



Cisco TrustSec How-To Guide: ISE Profiling Design Guide

For Comments, please email: howtoguides@external.cisco.com

Document Version: 3.0

August 23, 2012

Table of Contents

Table of Contents	2
Introduction	4
What Is the Cisco TrustSec System?.....	4
About the TrustSec How-To Guides.....	4
<i>What does it mean to be "TrustSec Certified"?</i>	5
Cisco ISE Profiling Services	6
Solution Overview	6
Policy Architecture and Components	6
Scenario Overview	7
<i>Network Topology</i>	7
<i>Components</i>	7
Profiling Service Requirements	9
Licensing.....	9
Appliance Requirements	9
Network Requirements.....	9
Profiling Services Global Configuration	10
ISE Profiling Global Configuration.....	10
<i>Configure Global Profiling Settings</i>	10
<i>Enable ISE Profiling Services</i>	10
Configuring Probes	12
Probe Overview.....	12
Probe Configuration	12
<i>Profiling Using the RADIUS Probe</i>	13
<i>Configuring the RADIUS Probe</i>	13
<i>Profiling Using the SNMP Trap Probe</i>	18
<i>Configuring the SNMP Trap Probe</i>	18
<i>Profiling Using the SNMP Query Probe</i>	23
<i>Configuring the SNMP Query Probe</i>	26
<i>Profiling Using the DHCP and DHCP SPAN Probes</i>	30
<i>Configuring the DHCP and DHCP SPAN Probes</i>	33
<i>Profiling Using the HTTP Probe</i>	39
<i>Configuring the HTTP Probe</i>	42
<i>Profiling Using the DNS Probe</i>	52
<i>Configuring the DNS Probe</i>	53
<i>Profiling Using the NetFlow Probe</i>	56
<i>Configuring the NetFlow Probe</i>	58
<i>Profiling Using Network Scan (NMAP) Probe</i>	66
<i>Configuring the NMAP Probe</i>	68
Device Sensor	76
Device Sensor Overview	76
Device Sensor Details.....	76
<i>Device Sensor Requirements</i>	77
<i>Configuring Device Sensor for ISE Profiling</i>	78

Configuring Profiling Policies	88
Profiling Policy Configuration Overview	88
Profiling Conditions	88
<i>Dictionary Attributes</i>	89
<i>Configuring Profiling Conditions</i>	90
Profiling Policies and Rules	91
<i>Profiling Policy Rule Actions</i>	92
Endpoint Identity Groups	96
<i>Profiling Policy Hierarchy</i>	97
Profiling and Authorization Policy	100
Profile Transitions and Change of Authorization	101
<i>Change of Authorization (CoA)</i>	102
Profiling Design and Best Practices	107
Profiling Design Considerations	107
<i>Profiling Known Device Types</i>	107
<i>Profiling Unknown Device Types</i>	108
<i>Access Policy and Device Configuration Impact on Profiling</i>	109
Probe Selection Best Practices	110
<i>Probe Attributes</i>	110
<i>The Unofficial Guide to Probe Selection</i>	112
Profiling Plan	116
Summary of Profiling Best Practices and Recommendations	117
Appendix A: References	118
Cisco TrustSec System:	118
Device Configuration Guides:	118

Introduction

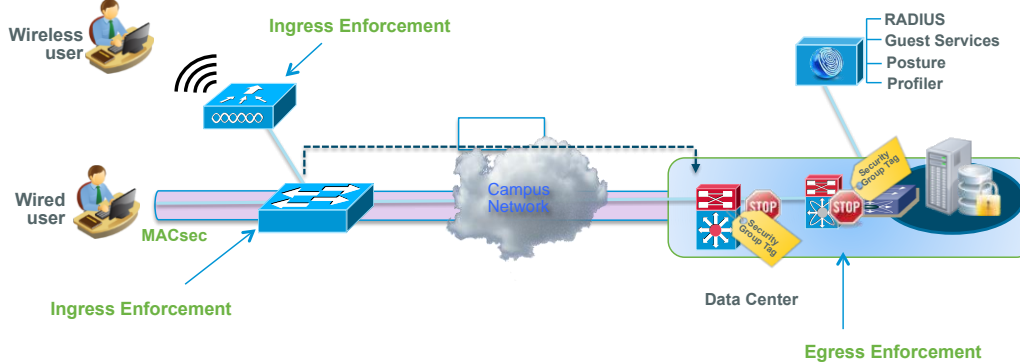
What Is the Cisco TrustSec System?

Cisco TrustSec®, a core component of the Cisco SecureX Architecture™, is an intelligent access control solution. TrustSec mitigates security risks by providing comprehensive visibility into who and what is connecting across the entire network infrastructure, and exceptional control over what and where they can go.

TrustSec builds on your existing identity-aware access layer infrastructure (switches, wireless controllers, and so on). The solution and all the components within the solution are thoroughly vetted and rigorously tested as an integrated system.

In addition to combining standards-based identity and enforcement models, such as IEEE 802.1X and VLAN control, the TrustSec system it also includes advanced identity and enforcement capabilities such as flexible authentication, Downloadable Access Control Lists (dACLs), Security Group Tagging (SGT), device profiling, posture assessments, and more.

Figure 1: TrustSec Architecture Overview

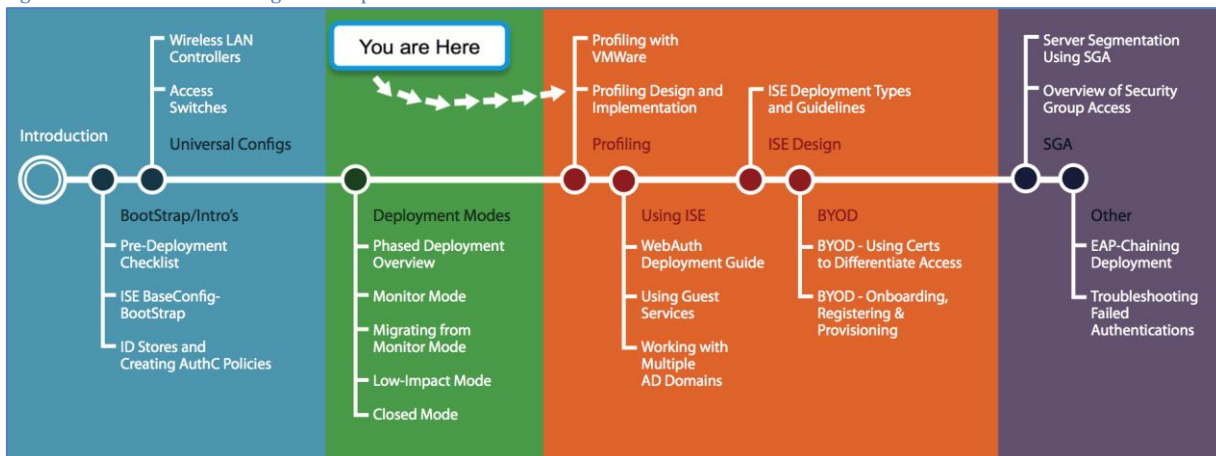


About the TrustSec How-To Guides

The TrustSec team is producing this series of How-To documents to describe best practices for TrustSec deployments. The documents in the series build on one another and guide the reader through a successful implementation of the TrustSec system. You can use these documents to follow the prescribed path to deploy the entire system, or simply pick the single use-case that meets your specific need.

Each guide in this series comes with a subway-style “You Are Here” map to help you identify the stage the document addresses and pinpoint where you are in the TrustSec deployment process (Figure 2).

Figure 2: How-To Guide Navigation Map



What does it mean to be ‘TrustSec Certified’?

Each TrustSec version number (for example, TrustSec Version 2.0, Version 2.1, and so on) is a certified design or architecture. All the technology making up the architecture has undergone thorough architectural design development and lab testing. For a How-To Guide to be marked “TrustSec certified,” all the elements discussed in the document must meet the following criteria:

- Products incorporated in the design must be generally available.
- Deployment, operation, and management of components within the system must exhibit repeatable processes.
- All configurations and products used in the design must have been fully tested as an integrated solution.

Many features may exist that could benefit your deployment, but if they were not part of the tested solution, they will not be marked as “TrustSec certified”. The TrustSec team strives to provide regular updates to these documents that will include new features as they become available, and are integrated into the TrustSec test plans, pilot deployments, and system revisions. (i.e., TrustSec 2.2 certification).

Additionally, many features and scenarios have been tested, but are not considered a best practice, and therefore are not included in these documents. As an example, certain IEEE 802.1X timers and local web authentication features are not included.

Note: Within this document, we describe the recommended method of deployment, and a few different options depending on the level of security needed in your environment. These methods are examples and step-by-step instructions for TrustSec deployment as prescribed by Cisco best practices to help ensure a successful project deployment.

Cisco ISE Profiling Services

Solution Overview

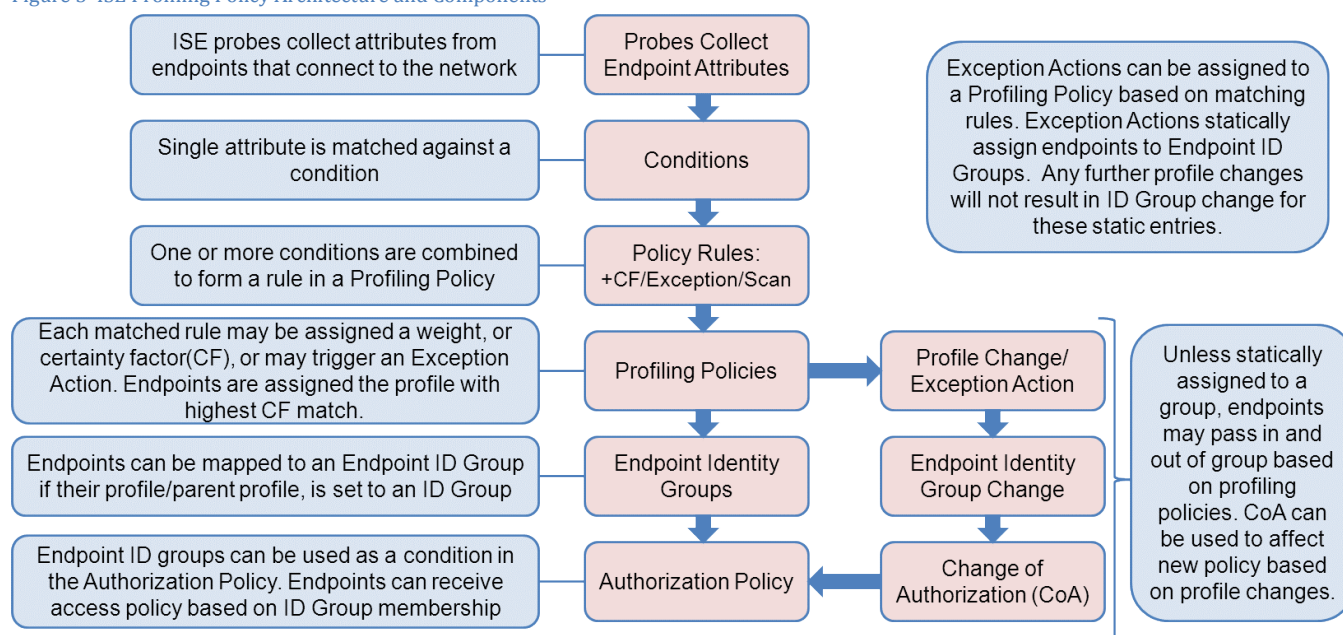
Cisco ISE Profiling Services provides dynamic detection and classification of endpoints connected to the network. Using MAC addresses as the unique identifier, ISE collects various attributes for each network endpoint to build an internal endpoint database. The classification process matches the collected attributes to prebuilt or user-defined conditions, which are then correlated to an extensive library of profiles. These profiles include a wide range of device types, including mobile clients (iPads, Android tablets, Blackberry phones, and so on), desktop operating systems (for example, Windows 7, Mac OS X, Linux, and others), and numerous nonuser systems such as printers, phones, cameras, and game consoles.

Once classified, endpoints can be authorized to the network and granted access based on their profile. For example, endpoints that match the IP phone profile can be placed into a voice VLAN using MAC Authentication Bypass (MAB) as the authentication method. Another example is to provide differentiated network access to users based on the device used. For example, employees can get full access when accessing the network from their corporate workstation but be granted limited network access when accessing the network from their personal iPhone.

Policy Architecture and Components

Figure 3 highlights the general policy architecture and key components for Cisco ISE Profiling Services. The configuration process begins with the enablement of specific probes on an ISE appliance running the Policy Service persona. There are different probes that are responsible for collecting different types of endpoint attributes. These attributes are matched to conditions which can then match rules in across a library of device types, or profiles. Based on a generic weighting scale, each matching condition can be assigned a different weight, or certainty factor (CF) that expresses the relative value that the condition contributes to classification of the device to a specific profile. Although conditions may match in multiple profiles, the profile for which the endpoint has the highest cumulative CF is the one assigned to the endpoint.

Figure 3 ISE Profiling Policy Architecture and Components



To expose the profile to the ISE Authorization Policy, administrators must configure the profile via simple checkbox to create a matching Identity Group. This simple process allows the profile to be selected in the form of an Endpoint Identity Group as a condition in the Authorization Policy.

Profiles can change as new attributes are learned or previously learned attributes are overwritten. Changes can also occur as a result of changes in the Profiling Policy. In some cases, the transition may be automatic—for example, from a generic HP device to a more specific profile such as an HP-Color-LaserJet-4500. In other cases, an administrator may want to make a deliberate action to bypass the default policy in the form of an Exception Action. Exception Actions allow static assignment of an endpoint to a specific Profiling Policy such that further attributes collection or correlation has no impact on the profile and optional Identity Group assigned.

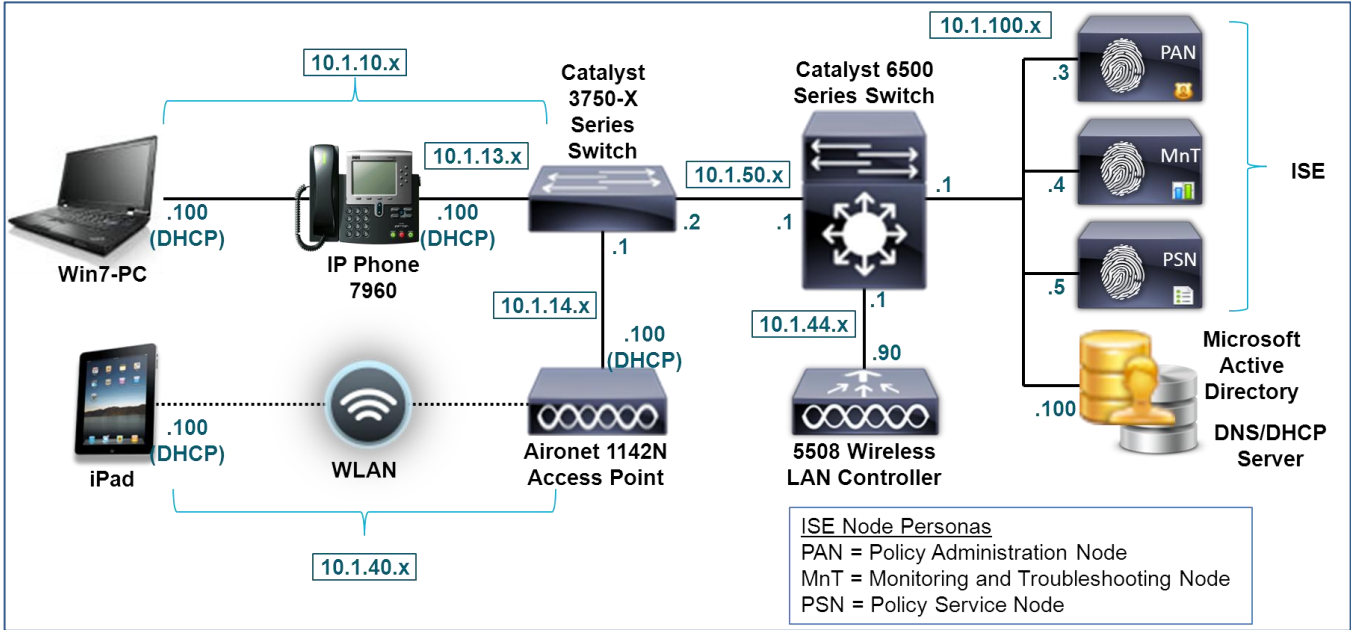
In each case above—profile transition and Exception Action—it may be desirable to allow ISE to enforce a new access policy for the endpoint based on the new profile assignment. RADIUS Change of Authorization (CoA) is the facility to accomplish this task in ISE. By sending CoA requests to the access device to which the endpoint is connected, ISE can require that the host be reevaluated against the Authentication and Authorization policy.

Scenario Overview

Network Topology

Figure 4 depicts the high-level network topology used in this guide. While all the scenarios pictured in Figure 1 are part of the overall TrustSec architecture, this document will focus on the wired and wireless user scenarios for profiling. ISE Profiling Services are not currently supported for the remote access VPN use case due to the lack of MAC address information from the VPN gateway required to correlate profiling data to unique endpoints.

Figure 4 ISE Profiling Topology



Components

Table 1 lists the hardware and software components were used in the writing of this guide.

Table 1: Cisco TrustSec 2.0 System Tested Components

Component	Hardware	Features Tested	Software Release
Cisco Identity Services Engine (ISE)	Cisco UCS C200 M2 server running VMware ESXi4.1	Integrated AAA, policy server, and profiling services	Cisco ISE Software Version 1.1.1 (Base and Advanced Feature Licenses)
Cisco Catalyst 3000 Series Switches	Cisco Catalyst 3560 Series	Basic Identity features including MAC Authentication Bypass (MAB), Local WebAuth (LWA), Central WebAuth (CWA), 802.1X authentication, and Change of Authorization (CoA). Profiling support services including Simple Network Management Protocol (SNMP), RADIUS, Dynamic Host Configuration Protocol DHCP Relay, and URL Redirection.	Cisco IOS® Software Release 12.2(55)SE3 (IP Base)
	Cisco Catalyst 3750-X Series	Basic Identity features including MAB, LWA, CWA, 802.1X authentication, and CoA. Profiling support services including SNMP, RADIUS, DHCP Relay, URL Redirection and Device Sensor.	Cisco IOS Software Release 15.0(1)SE2 (IP Base)

Component	Hardware	Features Tested	Software Release
Cisco Catalyst 6000 Series Switches	Cisco Catalyst 6500 Series Supervisor Engine 720 Policy Feature Card 3A (PFC3A)	Profiling support services including Cisco NetFlow Version 5 and Version 9 export, DHCP Relay, and Switched Port Analyzer/Remote Switched Port Analyzer (SPAN/RSPAN).	Cisco IOS Software Release 12.2(33)SXJ2 (Advanced IP Services)
Cisco Wireless LAN Controller (WLC)	Cisco 5508 Wireless LAN Controller	Basic Identity features including MAB, LWA, CWA, 802.1X authentication, and CoA. Profiling support services including SNMP, RADIUS, DHCP Relay, and URL Redirection.	Cisco Unified Wireless Network Software Release 7.2.103.0
Cisco Wireless Access Point	Cisco Aironet® Lightweight Access Point 1142N	Endpoint authenticated using MAB and authorization policy based on profile attributes	Cisco Lightweight Access Point Software Release 12.4(25e)JA
Cisco IP Phone	Cisco Unified IP Phone 7960	Endpoint authenticated using MAB and authorization policy based on profile attributes	Cisco IP Phone 7940 and 7960 firmware release 8.1(1.0)
Workstation	VMware Guest	Endpoint authenticated using MAB, LWA, CWA, and 802.1X and authorization policy based on profile attributes.	Windows 7
Tablet	Apple iPad (G1)	Endpoint authenticated using MAB, LWA, CWA, and 802.1X and authorization policy based on profile attributes.	iOS 5.0.1
Smartphone	Motorola DROIDX	Endpoint authenticated using MAB, LWA, CWA, and 802.1X and authorization policy based on profile attributes.	Android 2.3.4

Note: Cisco ISE Profiling Services is the key feature validated in this guide. Other TrustSec features were primarily deployed to support the configuration and testing of profiling services.

The devices and versions shown in the table are those specifically used during the guide testing and documentation process and are not reflective of all the devices that support TrustSec and ISE Profiling Services. For a more comprehensive listing of TrustSec-enabled devices and recommended versions, please go to <http://www.cisco.com/go/trustsec>.

Profiling Service Requirements

Licensing

ISE Profiling requires one of the following licenses to be installed on the Policy Administration node (PAN):

- Advanced Endpoint license (for wired or wireless deployments)
- Wireless Only license (for wireless only deployments)

One Advanced Endpoint license is required for each endpoint that is actively authenticated to the network and where profiling data is used to make an Authorization Policy decision. Not taking into account other services, such as posture assessment, that may require an Advanced Endpoint license, endpoints that are statically assigned to a profile do not consume an Advanced license. It is possible to profile multiple endpoints and have visibility into connected devices and their classification without requiring an Advanced Endpoint license for each if the profile information is not used to authorize the endpoint. The minimum number of Advanced Endpoint or Wireless Only licenses is 100.

Appliance Requirements

ISE Profiling Services can only run on an ISE appliance configured for the Policy Service persona. Table 2 shows general guidance for the number of active endpoints that can be profiled by an appliance dedicated to the Policy Service. Sizing for VMware-based appliances is based on matching or exceeding the equivalent specifications for hardware-based appliances.

Table 2 ISE Appliance Sizing

ISE Appliance	Maximum Endpoints	EPS Profiled (Profiling existing endpoints)	EPS Saved (Profiling new endpoints)
ACS1121/NAC3315/ISE3315	3000	43	33
NAC3355/ISE3355	6000	Not available	Not available
NAC3395/ISE3395	10,000	100	5
VMware	3000/6000/10,000	VMware configuration dependent	VMware configuration dependent

Additionally, each appliance is limited in the rate at which it can process new events per second (EPS). This value is dependent on whether the profiling data received is for a newly discovered endpoint or for an existing endpoint. The profiling rate for existing endpoints is shown in the EPS Profiled column in Table 2. The rate at which newly discovered endpoints are added to the database and profiled is shown in the EPS Saved column.

ISE Profiling Services can be scaled by distributing the service across multiple ISE appliances. An ISE Policy Service node that is running Profiling Services may also be a member of a node group used to cluster Policy Services behind a load balancer.

Network Requirements

ISE Profiling Services uses various collectors, or probes, to collect attributes about connected endpoints. Some of these probes require specific support by the network infrastructure, access devices, or possibly the endpoints. These requirements will be called out in greater detail in the sections that cover specific probes, but it is important to understand that some probes may not be usable if the appropriate data is not made available from the network or the endpoints.

Profiling Services Global Configuration

ISE Profiling Global Configuration

This section reviews the process for globally enabling ISE Profiling Services on a Policy Service node and configuring global profiling parameters.

Configure Global Profiling Settings

Procedure 1 Configure Global Profiling Settings from the Policy Administration Node

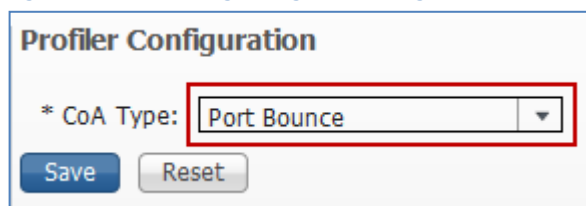
Step 1 Access the ISE administrative interface of the primary Policy Administration node (PAN) using a supported web browser and your admin credentials: **https://<ISE_PAN_FQDN_or_IP>**

Step 2 Navigate to Administration → System → Settings. Select Profiling from the left-hand-side (LHS) pane.

Step 3 From the right-hand side (RHS) pane, choose the default CoA type to be used for profiling transitions and Exception Actions (Figure 5).

If the goal is visibility only, leave the default value of No CoA. Otherwise, select Port Bounce. This will help ensure that even clientless endpoints will go through complete reauthorization process, including an IP address refresh, if needed. If multiple endpoints are detected on the switchport, ISE will revert to using the Reauth option to avoid service disruption of other connected devices.

Figure 5 Global Profiling Settings: CoA Configuration



The screenshot shows the 'Profiler Configuration' section of the ISE administrative interface. It features a dropdown menu for '* CoA Type:' with 'Port Bounce' selected. The dropdown is highlighted with a red rectangle. Below the dropdown are 'Save' and 'Reset' buttons.

Enable ISE Profiling Services

Procedure 1 Enable Profiling Services on the Policy Service Node

Step 1 Go to Administration → System → Deployment and select the Policy Service node to perform profiling from list of deployed nodes on the RHS pane.

Step 2 Under the General Settings tab, verify that the node persona called Policy Service is selected and that Enable Profiling Service is also selected (Figure 6).

Figure 6 Enabling Profiler Services on the Policy Service Node

General Settings Profiling Configuration

Hostname **ise-psn-1**
FQDN **ise-psn-1.cts.local**
IP Address **10.1.100.5**
Node Type **Identity Services Engine (ISE)**

Personas

☐ Administration Role **SECONDARY**

☐ Monitoring Role **SECONDARY** Other Monit

☒ **Policy Service**

☒ Enable Session Services **Include Node in Node Group** **<None>**

☒ **Enable Profiling Service**

Procedure 2 Access and View the Profiling Configuration Page

Step 1 Click the Profiling Configuration tab. View the various probes that can be enabled and configured simply by checking the appropriate box and selecting optional probe parameters (Figure 7).

Figure 7 Probe Configuration

General Settings Profiling Configuration

☐ ▶ **NETFLOW**

☐ ▶ **DHCP**

☐ ▶ **DHCPSPAN**

☐ ▶ **HTTP**

☐ ▶ **RADIUS**

☐ ▶ **Network Scan (NMAP)**

☐ ▶ **DNS**

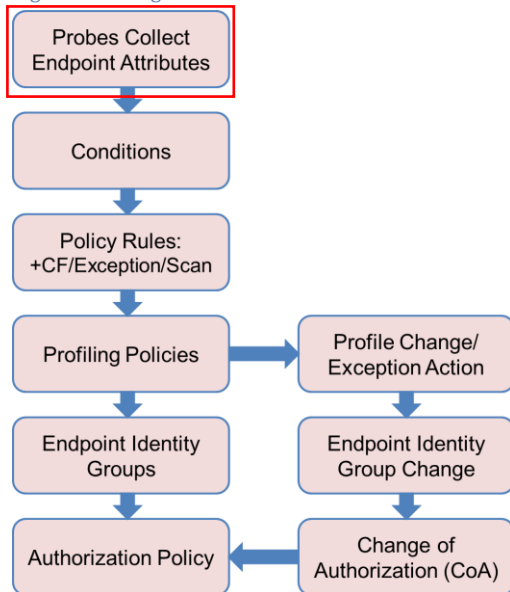
☐ ▶ **SNMPQUERY**

☐ ▶ **SNMPTRAP**

Step 2 Whenever you make changes to the profiling configuration, be sure to click Save at the bottom of page to commit the changes.

Configuring Probes

Figure 8: Configuration Flow: Probes and Attribute Collection



Probe Overview

An ISE probe is the component of ISE Profiling Services that collects endpoint attributes. Each probe uses different collection methods and can gather unique information about endpoints. Consequently, some probes are better suited than others to classify certain device types, or may be preferred based on the particular environment.

ISE supports the following probes:

- RADIUS
- SNMP Trap
- SNMP Query
- DHCP
- DHCP SPAN
- DNS
- HTTP
- NetFlow
- Network Scan (NMAP)

As suggested by their names, some probes such as DHCP and DHCP SPAN, for example, are uniquely capable of collecting certain attributes; in this example, DHCP attributes and associated option fields in DHCP packets. The choice between DHCP and DHCP SPAN will depend on whether the particular network environment supports the relay of DHCP traffic to the ISE Policy Service node, or if use of a Switch Port Analyzer (SPAN) method is better suited to network topology and capabilities of the infrastructure. This guide includes detailed guidance on probe selection under the individual sections for each probe.

Each probe type varies in how simple or difficult it is to enable. Each probe type also has varying levels of impact to the network or endpoints based on the protocols used and how they are deployed. Finally, each probe varies in the value of the data it produces and its applicability to classifying the specific endpoints of interest in the network. This guide reviews how each probe is configured and deployed and also aims to provide an overall understanding of each probe's deployment difficulty, network impact, and relative profiling value based on type of deployment.

Probe Configuration

ISE probes are enabled on ISE Policy Service nodes configured for Profiling Services. This section reviews the steps to enable the various ISE probes to collect different endpoint attributes. Working configuration examples of supporting network

infrastructure will also be provided along with the expected output from both the infrastructure and ISE administrative interface.

Profiling Using the RADIUS Probe

The RADIUS probe collects RADIUS attributes sent by RADIUS clients (including wired access switches and wireless controllers) to the RADIUS server (the ISE Policy Service node running Session Services). Standard RADIUS ports include UDP/1645 or UDP/1812 for authentication and authorization, and ports UDP/1646 and UDP/1813 for RADIUS accounting.

Note: The RADIUS probe does not listen directly to RADIUS traffic, but rather listens and parses RADIUS attributes sent in syslog to the Monitoring node on default UDP port 20514. Captured RADIUS profile attributes are then forwarded to an internal logger on default UDP port 30514.

The RADIUS probe also collects Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP), and DHCP attributes sent in RADIUS accounting packets using the Device Sensor feature. This feature is covered in detail later (see the [Device Sensor](#) section). Figure 9 shows the topology of our RADIUS probe example.

Figure 9 RADIUS Probe Example

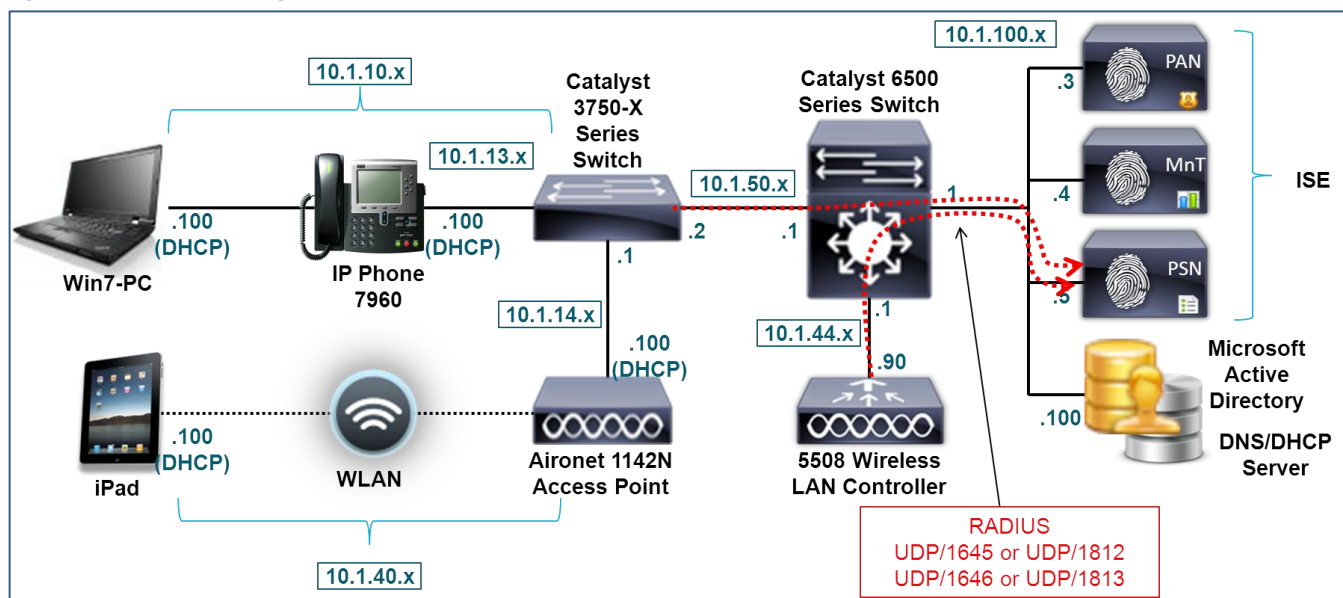


Table 3 shows common attributes collected using the RADIUS probe.

Table 3: Sample RADIUS Attributes

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

Although dependent on the access device configuration, Calling-Station-ID is commonly the MAC address of the connecting endpoint. This attribute provides immediate benefit in quickly identifying a unique endpoint based on MAC address as it connects to the network and authenticates. It also provides information on the vendor network adapter based on the Organizationally Unique Identifier (OUI) taken from the first three bytes of the MAC address.

The Framed-IP-Address present in RADIUS accounting packets provides the IP address of the connecting endpoint. This attribute combined with Calling-Station-ID gives ISE the critical IP-to-MAC binding required to support other probes that rely on IP address such as DNS, HTTP, Cisco NetFlow, and NMAP.

Configuring the RADIUS Probe

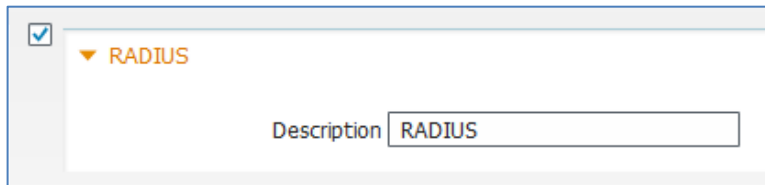
The RADIUS probe is one of the simplest probes to enable and deploy since the network access devices are already configured to send RADIUS packets to the ISE Policy Service node running Session Services for network authentication and authorization.

Procedure 1 Enable the RADIUS Probe in ISE

Step 1 Go to Administration→System→Deployment. From list of deployed nodes on the RHS pane, select the Policy Service node to perform profiling.

Step 2 Select the Profiling Configuration tab and check the box to enable the RADIUS probe. The probe is automatically enabled on the interfaces configured for RADIUS services (Figure 10).

Figure 10 RADIUS Probe Configuration



Step 3 Click Save to commit the change.

Step 4 Repeat the steps in this procedure for all other Policy Service nodes configured with Profiling Services.

Procedure 2 Verify Access Device Is Configured in ISE

This guide assumes that the network access devices have already been configured in ISE under Administration→Network Resources→Network Devices for standard RADIUS communications.

Procedure 3 Verify That Access Devices Are Configured to Send RADIUS to ISE PSN

This guide assumes that the network access devices have already been configured for RADIUS authentication, authorization, and accounting to the ISE Policy Service node (PSN). Here is a sample RADIUS configuration for a wired switch:

```
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
ip radius source-interface <Interface>
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server host <ISE_PSN_Address> auth-port 1812 acct-port 1813 key xxx
radius-server vsa send accounting
radius-server vsa send authentication
```

Figure 11 shows a sample RADIUS server configuration for a wireless controller. To access this configuration page, go to Security→AAA→RADIUS→Authentication in the WLC web administrative interface.

Figure 11 Global RADIUS Server Configuration for Wireless Controller Example

Security

AAA

- General
- RADIUS
 - Authentication
 - Accounting
 - Fallback
- TACACS+
- LDAP
- Local Net Users
- MAC Filtering
- Disabled Clients
- User Login Policies
- AP Policies
- Password Policies

RADIUS Authentication Servers

Call Station ID Type: **System MAC Address**

Use AES Key Wrap: ☐ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

MAC Delimiter: **Hyphen**

Network User	Management	Server Index	Server Address	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2	10.1.100.5	1812	Disabled	Enabled
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	3	10.1.100.6	1812	Disabled	Enabled
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	4	10.1.100.7	1812	Disabled	Enabled
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	5	10.1.101.3	1812	Disabled	Enabled

Best Practice: As shown in Figure 11, be sure to set the Call Station ID Type to System MAC Address to allow profiling of non-802.1X clients. This will ensure that ISE is able to add the endpoint to the database and associate other profile data received to this same endpoint based on known MAC address.

Similar entries should be present under the RADIUS accounting configuration for the wireless controller (Figure 12).

Figure 12 Global RADIUS Accounting Configuration for Wireless Controller Example

Security

AAA

- General
- RADIUS
 - Authentication
 - Accounting
 - Fallback
- TACACS+
- LDAP
- Local Net Users
- MAC Filtering
- Disabled Clients

RADIUS Accounting Servers

MAC Delimiter: **Hyphen**

Network User	Server Index	Server Address	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	2	10.1.100.5	1813	Disabled	Enabled
<input checked="" type="checkbox"/>	3	10.1.100.6	1813	Disabled	Enabled
<input checked="" type="checkbox"/>	4	10.1.100.7	1813	Disabled	Enabled
<input checked="" type="checkbox"/>	5	10.1.101.3	1813	Disabled	Enabled

Each WLAN should also be configured to designate the appropriate ISE Policy Service node(s) (Figure 13).

Figure 13 WLAN RADIUS Configuration for Wireless Controller Example

WLANs > Edit 'employee'

General **Security** **QoS** **Advanced**

Layer 2 **Layer 3** **AAA Servers**

Select AAA servers below to override use of default servers on this WLAN

Radius Servers

Radius Server Overwrite interface: ☐ Enabled

	Authentication Servers	Accounting Servers
Server 1	<input checked="" type="checkbox"/> Enabled IP:10.1.100.5, Port:1812	<input checked="" type="checkbox"/> Enabled IP:10.1.100.5, Port:1813
Server 2	None	None
Server 3	None	None

Step 1 Authenticate a new endpoint to the network.

Step 2 Go to the ISE Policy Administration node and navigate to Administration→Identity Management→Identities.

Step 3 Select Endpoints from the LHS pane.

Step 4 Find and select the MAC address of the newly connected endpoint to display the attributes captured by the RADIUS probe.

Numerous attributes can be captured. The sample output in Figure 14 highlights just four: **Calling-Station-ID**, **EndPointSource**, **Framed-IP-Address**, and **OUI**.

Figure 14 RADIUS Probe Attributes Example

Endpoint	
* MAC Address	00:1A:70:38:B6:66
* Policy Assignment	Cisco-Device
Static Assignment	<input type="checkbox"/>
* Identity Group Assignment	Profiled
Static Group Assignment	<input type="checkbox"/>
Attribute List	
ADDomain	cts.local
AccSessionID	ise-psn-1/123830140/32632
Airespace-Wlan-Id	1
AuthState	Authenticated
AuthenticationIdentityStore	AD1
AuthenticationMethod	MSCHAPV2
AuthorizationPolicyMatchedRule	Employee_NoPosture
CPMSessionID	0a012c5a000005954f98e8cc
Called-Station-ID	cc-ef-48-0c-99-a0
Calling-Station-ID	00-1a-70-38-b6-66
DestinationIPAddress	10.1.100.5
DestinationPort	1812
Device IP Address	10.1.44.90
Device Type	Device Type#All Device Types#Wireless
EapAuthentication	EAP-MSCHAPV2
EapTunnel	PEAP
EndPointMACAddress	00-1A-70-38-B6-66
EndPointMatchedProfile	Cisco-Device
EndPointPolicy	Cisco-Device
EndPointProfilerServer	ise-psn-1
EndPointSource	RADIUS Probe
ExternalGroups	cts.local/users/employees\,cts.local/users/domain users\,cts.local/builtin/users
Framed-IP-Address	10.1.40.100
IdentityAccessRestricted	false
IdentityGroup	Profiled
IdentityPolicyMatchedRule	Default
Location	Location#All Locations#North_America#RTP
MACAddress	00:1A:70:38:B6:66
MatchedPolicy	Cisco-Device
MessageCode	3000
NAS-IP-Address	10.1.44.90
NAS-Identifier	Cisco_0c:99:a4
NAS-Port	1
NAS-Port-Type	Wireless - IEEE 802.11
NetworkDeviceGroups	Device Type#All Device Types#Wireless, Location#All Locations#North_America#RTP
NetworkDeviceName	wlc5508
OUI	Cisco-Linksys, LLC
PolicyVersion	22
PostureAssessmentStatus	NotApplicable
RequestLatency	1
Response	{User-Name=CTS\employee1; State=ReauthSession:0a012c5a000005954f98e8cc; Class=CACS:0a012c5a000005954f98e8cc; ise-psn-1/123830140/32632; Termination-Action=RADIUS-Request; cisco-av-pair=ACS:CiscoSecure-Defined-ACL=#ACSACL#-IP-PERMIT_ALL_TRAFFIC-4f57e406; MS-MPPE-Send-Key=7d:90:04:93:07:bc:92:1e:a5:4d:97:6f:39:51:02:6e:eb:39:46:35:4f:e4:76:06:27:58:96:98:b4:b5:51:cb; MS-MPPE-Recv-Key=ac:0e:b6:a9:6f:c7:72:5d:cf:fe:9d:8b:9d:95:7a:8c:c6:2c:a7:54:1f:ee:3e:40:ed:53:48:d6:68:78:38:e8; Airespace-ACL-Name=PERMIT_ALL_TRAFFIC; }
SelectedAccessService	Default Network Access
SelectedAuthenticationIdentityStores	AD1, Internal Users
SelectedAuthorizationProfiles	Employee
Service-Type	Framed
StaticAssignment	false
StaticGroupAssignment	false
TimeToProfile	20
Total Certainty Factor	20
User-Name	CTS\employee1
attribute-52	00:00:00:00
attribute-53	00:00:00:00
cisco-av-pair	audit-session-id=0a012c5a000005954f98e8cc
ip	10.1.40.100

The Calling-Station-ID populates the **MACaddress** attribute. Additionally, the vendor OUI of the network adapter is determined to be **Cisco-Linksys**. In this example, the network adapter is a Linksys Wireless USB adapter. Conditions that match OUI are common entries in Profiling Policy rules. In some cases, such as a Nintendo or Sony game console, it may be all that is required to classify the endpoint.

The Framed-IP-Address value populates the **ip** attribute. We now have an IP-to-MAC address binding for this endpoint.

The **EndPointSource** attribute specifies the source of the last profile attribute update. In this case, it is the RADIUS probe that provided the last update to this endpoint record.

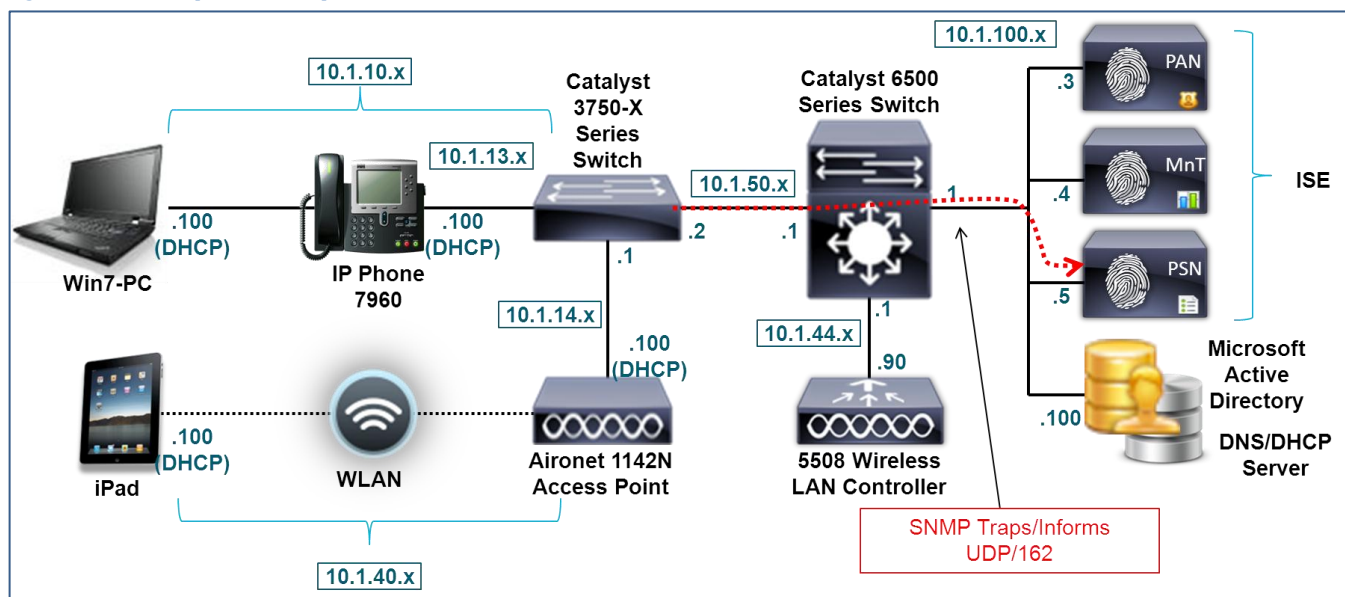
Additional RADIUS attributes can be used for profiling but since most of these are available directly to the Authorization Policy for creating policy conditions and rules, the focus is on the ones noted above.

Profiling Using the SNMP Trap Probe

The SNMP Trap probe is used to alert ISE Profiling Services to the presence (connection or disconnection) of a network endpoint and to trigger an SNMP Query probe.

To use the SNMP Trap probe, the access devices to which endpoints connect must be configured to send SNMP Traps to the ISE Policy Service node configured for Profiling Services. Figure 15 shows the topology for our example SNMP Trap probe.

Figure 15 SNMP Trap Probe Example



If the RADIUS probe is already enabled, the SNMP Trap probe is likely not needed since RADIUS Accounting Start messages can also trigger the SNMP Query probe. The primary use case for this probe would be for a predeployment discovery phase whereby RADIUS has yet to be configured for network authentication. Another use case would be to integrate environments that do not rely on RADIUS, such as Cisco NAC Appliance Release 4.9 and later.

Configuring the SNMP Trap Probe

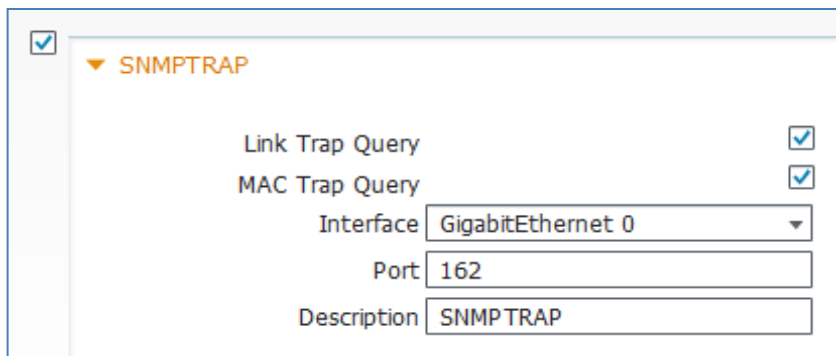
To use the SNMP Trap probe, it must first be enabled in ISE. As previously noted, the access devices to which endpoints connect must be configured to send SNMP Traps to the ISE Policy Service node configured for Profiling Services. ISE must also be configured to accept and process traps from these network access devices.

Procedure 1 Enable the SNMP Trap Probe in ISE

Step 1 Go to Administration→System→Deployment and select the Policy Service node to perform profiling from list of deployed nodes on the RHS pane.

Step 2 Select the Profiling Configuration tab and check the box to enable the SNMP Trap probe (Figure 16).

Figure 16 SNMPTRAP Probe Configuration

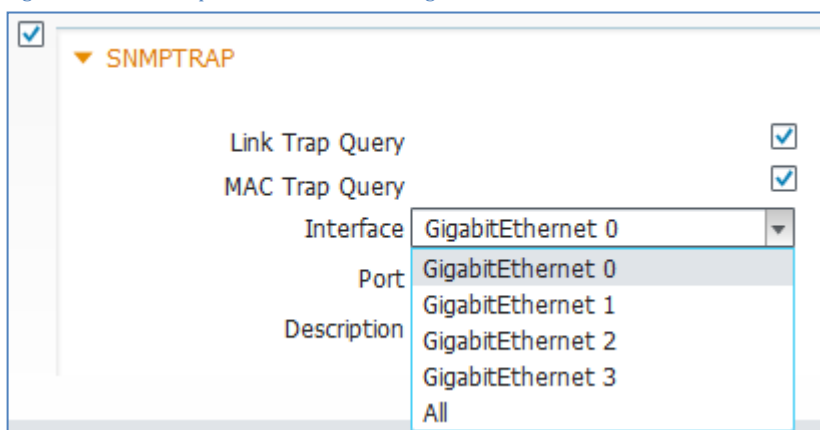


The image shows a configuration form for an SNMPTRAP probe. At the top left, there is a checked checkbox. Below it is a section header 'SNMPTRAP' with a downward arrow. The form contains the following fields: 'Link Trap Query' with a checked checkbox, 'MAC Trap Query' with a checked checkbox, 'Interface' with a dropdown menu showing 'GigabitEthernet 0', 'Port' with a text box containing '162', and 'Description' with a text box containing 'SNMPTRAP'.

Step 3 Check the boxes labeled Link Trap Query and MAC Trap Query to enable the probe to respond to each trap type.

Step 4 Verify the ISE PSN interface used to receive traps. In most cases this will be the default GigabitEthernet 0 interface although it is possible to process traps received on other interfaces or to select All interfaces.

Figure 17: SNMP Trap Probe—Interface Configuration



The image shows the same configuration form as Figure 16, but with the 'Interface' dropdown menu open. The dropdown list shows the following options: 'GigabitEthernet 0', 'GigabitEthernet 1', 'GigabitEthernet 2', 'GigabitEthernet 3', and 'All'. The 'Link Trap Query' and 'MAC Trap Query' checkboxes are checked. The 'Port' is set to '162' and the 'Description' is 'SNMPTRAP'.

If you decide to process traps on other interfaces, make sure those interfaces are enabled and have an IP address assigned. These addresses must be configured in the access devices at the SNMP host trap target.

Step 5 Click Save to commit the change.

Step 6 Repeat the steps in this procedure for all other Policy Service nodes configured with Profiling Services.

Procedure 2 Add the Network Access Device to ISE

Typically, all network access devices that authenticate endpoints via RADIUS will be configured in ISE, but use of the SNMP Trap probe often implies that access devices are not yet configured for RADIUS. If these access devices are not yet configured, you must add the access devices that will be sending SNMP traps to ISE.

Step 1 Go to Administration→Network Resources→Network Devices and click Add in the RHS pane.

Step 2 Enter the device name and IP address information (Figure 18). The IP address should include the IP address that will source SNMP traps. In simple configurations, there may be only one management IP address on the switch. In other cases, there can be multiple IP addresses and by default SNMP will typically use the IP address of the egress interface. If necessary, enter all possible IP addresses that access devices may use to source SNMP packets.

Figure 18 Network Device Configuration

Network Devices List > New Network Device

Network Devices

* Name

Description

* IP Address: /

* IP Address: /

Best Practice: If supported by the access device, use loopback interfaces for management traffic. Be sure to take advantage of options such as **source-interface** to set the specific interface and IP address that will source management traffic. This will provide a uniform address for all management traffic and also prevent connectivity failures if a specific interface is down.

Step 3 Check the SNMP Settings box.

Step 4 Specify SNMP Version used by the access device and enter the SNMP RO Community string for SNMP versions 1 and 2c, or else enter the SNMPv3 credentials and configuration, as appropriate to the access device (Figure 19).

Step 5 Verify that the boxes for Link Trap Query and MAC Trap Query are selected. These settings allow ISE to accept or ignore SNMP traps received from specific access devices, or to accept only a specific type of trap.

Figure 19 Network Device Configuration—SNMP Traps

☒ ▼ SNMP Settings

* SNMP Version

* SNMP RO Community

SNMP Username

Security Level

Auth Protocol

Auth Password

Privacy Protocol

Privacy Password

* Polling Interval seconds (Valid Range 600 to 86400)

Link Trap Query ☒

MAC Trap Query ☒

Originating Policy Services Node

Step 6 Save the changes once complete.

Step 7 Repeat the steps above for each access device that will send SNMP traps to the ISE Policy Service nodes.

Procedure 3 Configure Access Devices to Send SNMP Traps to ISE Policy Service Node

Step 1 Go to the management console of the access device and verify that it is configured to send SNMP traps to the ISE Policy Service node running Profiling Services and enabled with the SNMP Trap probe.

Here is an example configuration from a Catalyst switch running Cisco IOS to send SNMP LinkUp/LinkDown traps as well as MAC Notification traps:

```
interface <Endpoint_Interface>
  snmp trap mac-notification added
  snmp trap mac-notification removed
!
mac address-table notification change
mac address-table notification mac-move
!
snmp-server trap-source <Interface>
snmp-server enable traps snmp linkdown linkup
snmp-server enable traps mac-notification change move
snmp-server host <ISE_PSN_IP_address> version 2c ciscoro
```

Note: Cisco ISE does not currently support SNMP traps from the Wireless LAN Controller.

Procedure 4 Verify SNMP Trap Probe Data

The SNMP Trap probe cannot populate endpoint attributes based on LinkUp or LinkDown traps alone as there is no associated MAC address in these traps. They primarily signal the interface on which link has been established or lost. However, MAC Notification traps do include the MAC address of the endpoint and can therefore provide updates to the ISE Internal Endpoints database.

Step 1 Delete the endpoint from Administration→Identity Management→Identities→Endpoints.

Step 2 Disconnect and then reconnect a wired client from the access switch configured for SNMP traps.

Step 3 Go to the ISE Policy Administration node and navigate to Administration → Identity Management → Identities.

Step 4 Select Endpoints from the LHS pane.

Step 5 Find and select the MAC address of the newly connected endpoint to display the attributes captured by the SNMP Trap probe (Figure 20).

Figure 20 SNMP Trap Probe Attributes Example

Endpoint	
* MAC Address	00:50:56:A0:0B:3A
* Policy Assignment	VMWare-Device
Static Assignment	<input type="checkbox"/>
* Identity Group Assignment	Profiled
Static Group Assignment	<input type="checkbox"/>
Attribute List	
EndPointPolicy	VMWare-Device
EndPointProfilerServer	ise-psn-1
EndPointSource	SNMPTrap Probe
IdentityGroup	Profiled
MACAddress	00:50:56:A0:0B:3A
MacStatus	02
MatchedPolicy	VMWare-Device
NADAddress	10.1.50.2
OUI	VMware, Inc.
PolicyVersion	22
StaticAssignment	false
StaticGroupAssignment	false
TimeToProfile	19
Timestamp	58963997
Total Certainty Factor	10
Vlan	10
dot1dBasePort	1

Key attributes highlighted include **EndPointSource**, **MACAddress**, and **OUI**.

EndPointSource confirms that the SNMP Trap probe is the source of the information.

Note: In the example shown in Figure 20, all other probes were disabled and endpoint deleted from ISE database prior to running the test.

MACAddress was learned from the MAC Notification trap information and the vendor OUI was determined by correlating against ISE's OUI database. In this example, we can see that the client is running VMware, which uses a virtual network adapter.

As an optional verification that SNMP traps are being sent by the access switch, debug logging can be enabled to view the SNMP Link and MAC Notification traps as they are sent. The output below is from a Catalyst switch with the following debug enabled:

- **debug snmp packets**
- **debug mac-notification**

In the following example, upon enabling the switchport connected to a Cisco IP phone and Windows 7 PC connected to that phone, SNMP LinkUp traps are sent for both the phone and PC to the ISE PSN followed by MAC Notification traps for both. Only the traps related to the PC with MAC address 00:50:56:A0:0B:3A are highlighted.

```

Apr 26 16:53:06.735: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
Apr 26 16:53:06.743: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan13, changed state to up
Apr 26 16:53:06.743: SNMP: Queuing packet to 10.1.100.5
Apr 26 16:53:06.743: SNMP: V2 Trap, reqid 296, errstat 0, erridx 0
  sysUpTime.0 = 58970958
  snmpTrapOID.0 = snmpTraps.4
  ifIndex.10 = 10
  ifDescr.10 = Vlan10
  ifType.10 = 53
  lifEntry.20.10 = up
  
```

```

Apr 26 16:53:06.861: SNMP: Queuing packet to 10.1.100.5
Apr 26 16:53:06.861: SNMP: V2 Trap, reqid 299, errstat 0, erridx 0
sysUpTime.0 = 58970970
snmpTrapOID.0 = snmpTraps.4
ifIndex.13 = 13
ifDescr.13 = Vlan13
ifType.13 = 53
lifEntry.20.13 = up
Apr 26 16:53:06.995: SNMP: Packet sent via UDP to 10.1.100.5
Apr 26 16:53:07.246: SNMP: Packet sent via UDP to 10.1.100.5
Apr 26 16:53:08.706: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to up
Apr 26 16:53:09.713: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/1,
changed state to up
Apr 26 16:53:09.713: SNMP: Queuing packet to 10.1.100.5
Apr 26 16:53:09.713: SNMP: V2 Trap, reqid 302, errstat 0, erridx 0
sysUpTime.0 = 58971255
snmpTrapOID.0 = snmpTraps.4
ifIndex.10101 = 10101
ifDescr.10101 = GigabitEthernet1/0/1
ifType.10101 = 6
lifEntry.20.10101 = up
Apr 26 16:53:09.964: SNMP: Packet sent via UDP to 10.1.100.5
Apr 26 16:53:12.280: MN: Enqueue MAC 0050.56a0.0b3a on port 1 vlan 10
MN: New Shadow entry..

Apr 26 16:53:12.280: MN : MAC Notify event for 0050.56a0.0b3a on port 1 vlan 10

Apr 26 16:53:12.456: MN: Enqueue MAC 0030.94c4.528a on port 1 vlan 10
MN: Got the last shadow entry..Index 11

Apr 26 16:53:12.456: MN : MAC Notify event for 0030.94c4.528a on port 1 vlan 10
MN: Shadow entry for Despatch..
Despatching trap for Index 2 Time: 58971575
MN: Wrapping history queue..

Apr 26 16:53:12.925: SNMP: Queuing packet to 10.1.100.5
Apr 26 16:53:12.925: SNMP: V2 Trap, reqid 305, errstat 0, erridx 0
sysUpTime.0 = 58971577
snmpTrapOID.0 = cmnMacChangedNotification
cmnHistMacChangedMsg.1 =
01 00 0A 00 50 56 A0 0B 3A 00 01 01 00 0A 00 30
94 C4 52 8A 00 01 00
cmnHistTimestamp.1 = 58971575
Apr 26 16:53:13.177: SNMP: Packet sent via UDP to 10.1.100.5
Apr 26 16:53:23.587: MN: Enqueue MAC 0030.94c4.528a on port 1 vlan 13
MN: New Shadow entry..

Apr 26 16:53:23.604: MN : MAC Notify event for 0030.94c4.528a on port 1 vlan 13
MN: Shadow entry for Despatch..
Despatching trap for Index 2 Time: 58972696
MN: Wrapping history queue..

Apr 26 16:53:24.132: SNMP: Queuing packet to 10.1.100.5
Apr 26 16:53:24.132: SNMP: V2 Trap, reqid 308, errstat 0, erridx 0
sysUpTime.0 = 58972697
snmpTrapOID.0 = cmnMacChangedNotification
cmnHistMacChangedMsg.1 =
01 00 0D 00 30 94 C4 52 8A 00 01 00
cmnHistTimestamp.1 = 58972696
Apr 26 16:53:24.384: SNMP: Packet sent via UDP to 10.1.100.5

```

For reference, in addition to the debug logging available on the access devices, ISE also supports its own debug logging. Debugging is beyond the scope of this guide, although an alternative method to validate the information received by ISE is to use the built-in TCP Dump utility found under Operations→Troubleshoot→Diagnostic Tools→General Tools. This tool will allow ISE to capture SNMP traffic from the access device to the specified ISE Policy Service node interface (the one enabled with the SNMP Trap probe). This information can then be downloaded and displayed in human-readable format, or else in a standard packet capture format for import into a common packet analyzer such as Wireshark.

Profiling Using the SNMP Query Probe

The SNMP Query probe is used to send queries (or SNMP Get requests) to access devices and optionally to other infrastructure devices to collect relevant endpoint data stored in their SNMP MIBs. There are two general types of SNMP queries that the ISE Policy Service node performs:

- **lldpRemoteSystemsData** (Wired only)
- **cLApEntry** (WLC only)
- **cldcClientEntry** (WLC only)

If multiple Policy Service nodes have SNMP Query enabled, SNMP polling of network devices is distributed among all available PSNs unless specific PSNs are configured to poll a given network device.

Address Resolution Protocol (ARP) table information is also collected during this polled query to build the IP-MAC ARP Cache table in ISE. In environments where endpoints are connected to Layer 2-only switchports, it may be desirable to configure upstream Layer 3 devices (for example, branch routers or Layer 3 distribution switches) as ISE network access devices if they contain the ARP table information for the endpoints. This may be required to provide IP-to-MAC binding information in deployments that do not have RADIUS configured on the access devices or in which DHCP probes are not able to collect this data. In the example topology (Figure 21), the Cisco Catalyst 6500 Series Switch may be polled to acquire ARP information for the wireless clients or for a downstream Layer 2 switch (not displayed).

Interface Query

Interface queries are triggered by either a RADIUS Accounting Start packet (requires RADIUS probe) or an SNMP LinkUp/MAC Notification trap (requires SNMP Trap probe).

Best Practice: To simplify the deployment and to reduce traffic overhead due to SNMP traps, when possible, use the RADIUS probe to trigger SNMP Query based on RADIUS Accounting Start messages.

Whereas System Queries read the access device MIBs, Interface Queries request the MIBs or portions of MIBs that concern only a particular interface for which the trap is received. These triggered queries retrieve the following data from the access device:

- Interface data (ifIndex, ifDesc, etc)
- Port and VLAN data
- Session Data (if interface type is Ethernet)
- CDP data (Cisco devices)
- LLDP data

Some of the key profiling attributes collected during the triggered Interface Query include the Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) tables. CDP and LLDP are link protocols that allow the switch to dynamically learn attributes of the connected endpoint. Many devices, including IP video equipment, network infrastructure, and Cisco appliances, support these protocols. Most major IP phone manufacturers support CDP or LLDP. Consequently, many endpoints can be classified based on this information alone. Additionally, there are numerous CDP/LLDP agents available on a broad range of client operating systems at minimal or no charge.

The following output shows a sample of the type of information you can collect using SNMP Query to collect CDP data for connected endpoints.

```
cat3750x#show cdp neighbor detail
-----
Device ID: APc471.fe34.197a
Entry address(es):
  IP address: 10.1.14.100
Platform: cisco AIR-LAP1142N-A-K9, Capabilities: Trans-Bridge
Interface: GigabitEthernet1/0/2, Port ID (outgoing port): GigabitEthernet0
Holdtime : 123 sec

Version :
Cisco IOS Software, C1140 Software (C1140-K9W8-M), Version 12.4(25e)JA, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Fri 27-Jan-12 21:45 by prod_rel_team

advertisement version: 2
Duplex: full
Power drawn: 15.400 Watts
Power request id: 1358, Power management id: 2
Power request levels are:15400 14500 0 0 0
```

```

Management address(es) :

-----
Device ID: SEP003094C4528A
Entry address(es):
  IP address: 10.1.13.100
Platform: Cisco IP Phone 7960, Capabilities: Host Phone Two-port Mac Relay
Interface: GigabitEthernet1/0/1, Port ID (outgoing port): Port 1
Holdtime : 162 sec
Second Port Status: Up

Version :
P00308010100

advertisement version: 2
Duplex: full
Power drawn: 6.300 Watts
Management address(es) :

-----

```

Configuring the SNMP Query Probe

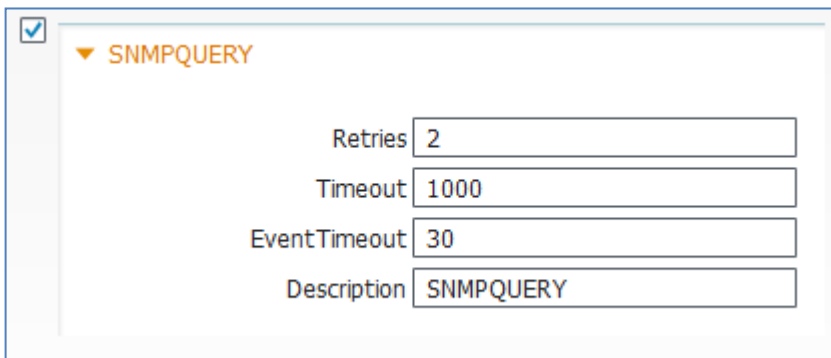
To use the SNMP Query probe, the network device must be configured to accept SNMP requests from the ISE Policy Service node using a Read-Only (RO) community. ISE must also have the SNMP device configured as a network device along with appropriate SNMP community strings. For a triggered query to occur, either the RADIUS probe or SNMP Trap probe must be enabled and associated components must be configured correctly. Finally, to retrieve CDP or LLDP information, the endpoint must support CDP or LLDP and either or both of these protocols must be enabled on the access switch.

Procedure 1 Enable the SNMP Query Probe in ISE

Step 1 Go to Administration→System→Deployment and select the Policy Service node to perform profiling from list of deployed nodes on the RHS pane.

Step 2 Select the Profiling Configuration tab and check the box to enable the SNMP Query probe (Figure 22).

Figure 22 SNMP Query Probe Configuration



☒ **SNMPQUERY**

Retries: 2

Timeout: 1000

EventTimeout: 30

Description: SNMPQUERY

Note: No interface needs to be configured for the SNMP Query probe. SNMP queries will be sent to access devices based on the appliance routing table.

Step 3 Leave the default values for Retries, Timeout, and Event Timeout:

- **Timeout** (in milliseconds) specifies the amount of time to wait for an SNMP response.
- **Retries** specifies the number of times the Policy Service node will attempt to establish an SNMP session after an initial failed attempt.
- **EventTimeout** (in seconds) specifies the time to wait after a RADIUS Accounting Start or SNMP Trap trigger before sending a batched query to the access device.

Step 4 For triggered interface queries, verify that RADIUS probe is enabled. If RADIUS is not configured on the network access devices, verify that the SNMP Trap probe is enabled.

Step 5 Click Save to commit the change.

Step 6 Repeat the steps in this procedure for all other Policy Service nodes configured with Profiling Services.

Procedure 2 Configure the Network Device in ISE (Network Resources)

Typically, all network access devices that authenticate endpoints via RADIUS will be configured in ISE, so all that must be done is to verify the SNMP settings for each. If configuring SNMP Query probe for a network that does not have RADIUS authentication deployed, you must add each access device —and optionally select Layer 3 devices (for ARP information) — to the list of ISE network devices.

Step 1 Go to Administration→Network Resources→Network Devices. If the device to be queried using SNMP is already present, simply select the device from the list, or else click Add from the RHS pane.

Step 2 For new devices, enter the device name and IP address information.

Step 3 In the SNMP Settings box, specify the SNMP Version used by the access device and enter the SNMP RO Community string for SNMP versions 1 and 2c, or else enter the SNMPv3 credentials and configuration as appropriate to the access device (Figure 23).

Figure 23 Network Access Device Configuration: SNMP Query

SNMP Settings

* SNMP Version 2c

* SNMP RO Community ciscoro

SNMP Username

Security Level

Auth Protocol

Auth Password Show

Privacy Protocol

Privacy Password Show

* Polling Interval 3,600 seconds (Valid Range 600 to 86400)

Link Trap Query ☒

MAC Trap Query ☒

Originating Policy Services Node

None

ise-psn-1

ise-psn-2

Step 4 For System (polled) Queries, set the Polling Interval and Originating Policy Services Node:

- **Polling Interval:** In general, a longer polling interval is recommended in networks that have RADIUS or DHCP probes deployed because the reliance on ARP information is reduced.
- **Originating Policy Services Node:** Each PSN with the SNMP Query probe enabled will appear in the list. Select the optimal Policy Service node to perform periodic polling of the network device. This will usually be the PSN closest to the network device in terms of network bandwidth.

Step 5 For Interface (triggered) Queries that rely on SNMP traps, be sure one or both of the Trap Query options are set.

Note: The Originating Policy Services Node setting does not apply to Interface queries as those are always sent by the PSN that received the trigger, such as RADIUS Accounting Start or SNMP Trap message.

Step 6 Save the changes once complete.

Step 7 Repeat the steps above for each access device that must be queried using SNMP by the ISE Policy Service nodes.

Procedure 3 Configure Wired Access Devices to Accept SNMP Queries from the ISE PSN

Step 1 Go to the management console of the wired access device and verify that it is configured to support SNMP Read-Only requests from the ISE Policy Service nodes with the SNMP Query probe enabled.

Here is an example configuration from a Cisco Catalyst switch running IOS to support SNMPv2c queries from ISE PSN using the read-only community string **ciscoro**:

```
snmp-server community ciscoro RO
snmp-server community ciscorw RW
```

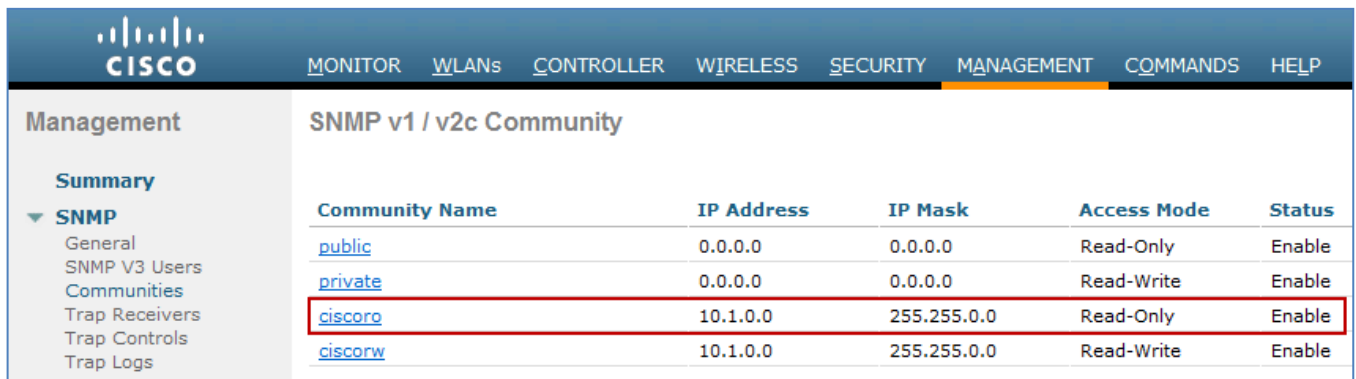
Procedure 4 Configure Wireless Access Devices to Accept SNMP Queries from the ISE PSN

Step 1 Go to the web admin interface of the Wireless LAN Controller and verify that it is configured to support SNMP Read-Only requests from the ISE Policy Service nodes with the SNMP Query probe enabled.

Step 2 Go to Management→SNMP→Communities→SNMP v1 / v2c Community and configure one or more read-only community strings used by the ISE Policy Service nodes that may query this device.

Figure 24 shows an example configuration from a WLC configured to support SNMPv2c queries from ISE PSN using the read-only community string **ciscoro**:

Figure 24 SNMP Configuration for Wireless Controller Example



Community Name	IP Address	IP Mask	Access Mode	Status
public	0.0.0.0	0.0.0.0	Read-Only	Enable
private	0.0.0.0	0.0.0.0	Read-Write	Enable
ciscoro	10.1.0.0	255.255.0.0	Read-Only	Enable
ciscorw	10.1.0.0	255.255.0.0	Read-Write	Enable

If SNMPv3 is deployed, be sure to configure the appropriate settings under Management→SNMP→SNMP V3 Users.

Procedure 5 Configure Access Devices to support CDP and LLDP

Step 1 To retrieve CDP and LLDP information from connected hosts, make sure the access device is configured to receive these protocols on the switchports. Although CDP is typically enabled by default on Cisco devices, LLDP is not. Therefore, be sure enable LLDP globally if wish to collect this information using the SNMP Query probe.

```
cdp run
interface <Endpoint_Interface>
  cdp enable
!
lldp run
interface <Endpoint_Interface>
  lldp receive
  lldp transmit
```

Note: The Wireless LAN Controller does not support CDP/LLDP for wireless clients.

Procedure 6 Verify SNMP Query Probe Data

Step 1 Delete the endpoint from Administration→Identity Management→Identities→Endpoints.

Step 2 Disconnect and then reconnect the endpoint from the access device configured for SNMP access by ISE.

Step 3 Go to the ISE Policy Administration node and navigate to Administration→Identity Management→Identities.

Step 4 Select Endpoints from the LHS pane.

Step 5 Find and select the MAC address of the newly connected endpoint to display the attributes captured by the SNMP Query probe.

The example shown in Figure 25 is taken using only the SNMP Trap and SNMP Query probes to highlight the attributes collected using SNMP Query. The key attributes highlighted include the **EndPointSource**, the **cdpCacheAddress**, and **cdpCachePlatform**:

- **EndPointSource** informs us that the last profiling update came from the SNMP Query probe.
- The **cdpCacheAddress** provides the IP address and allows binding between the IP and MAC address.
- The **cdpCachePlatform** attribute provides a detailed description of the connected endpoint—in this example, a Cisco AIR-LAP1142N-A-K9 which is the Cisco Aironet 1142N wireless access point.

Figure 25 SNMP Query Probe Attributes Example

Endpoint

* MAC Address **C4:71:FE:34:19:7A**

* Policy Assignment Cisco-Access-Point

Static Assignment ☐

* Identity Group Assignment Cisco-Access-Point

Static Group Assignment ☐

Attribute List

EndPointPolicy	Cisco-Access-Point
EndPointProfilerServer	ise-psn-1
EndPointSource	SNMPQuery Probe
IdentityGroup	Cisco-Access-Point
MACAddress	C4:71:FE:34:19:7A
MatchedPolicy	Cisco-Access-Point
NADAddress	10.1.50.2
OUI	Cisco Systems
PolicyVersion	22
StaticAssignment	false
StaticGroupAssignment	false
TimeToProfile	24
Total Certainty Factor	20
Vlan	14
VlanName	WIRELESS
cdpCacheAddress	10.1.14.100
cdpCacheCapabilities	T
cdpCacheDeviceId	APc471.fe34.197a
cdpCachePlatform	cisco AIR-LAP1142N-A-K9
cdpCacheVersion	Cisco IOS Software, C1140 Software (C1140-K9W8-M), Version 12.4(25e)JA, RELEASE SOFTWARE Copyright (c) 1986-2012 by Cisco Systems, Inc. Compiled Fri 27-Jan-12 21:45 by prod_rel_team
dot1xAuthAuthControlledPortControl	3
dot1xAuthAuthControlledPortStatus	2
ifDescr	GigabitEthernet1/0/2
ifIndex	10102
ifOperStatus	1
ip	10.1.14.100
port	2

Step 6 To verify the expected attribute data, you can use the following commands from the access switch console:

```
switch# show cdp neighbor detail
switch# show lldp neighbor detail
```

Profiling Using the DHCP and DHCP SPAN Probes

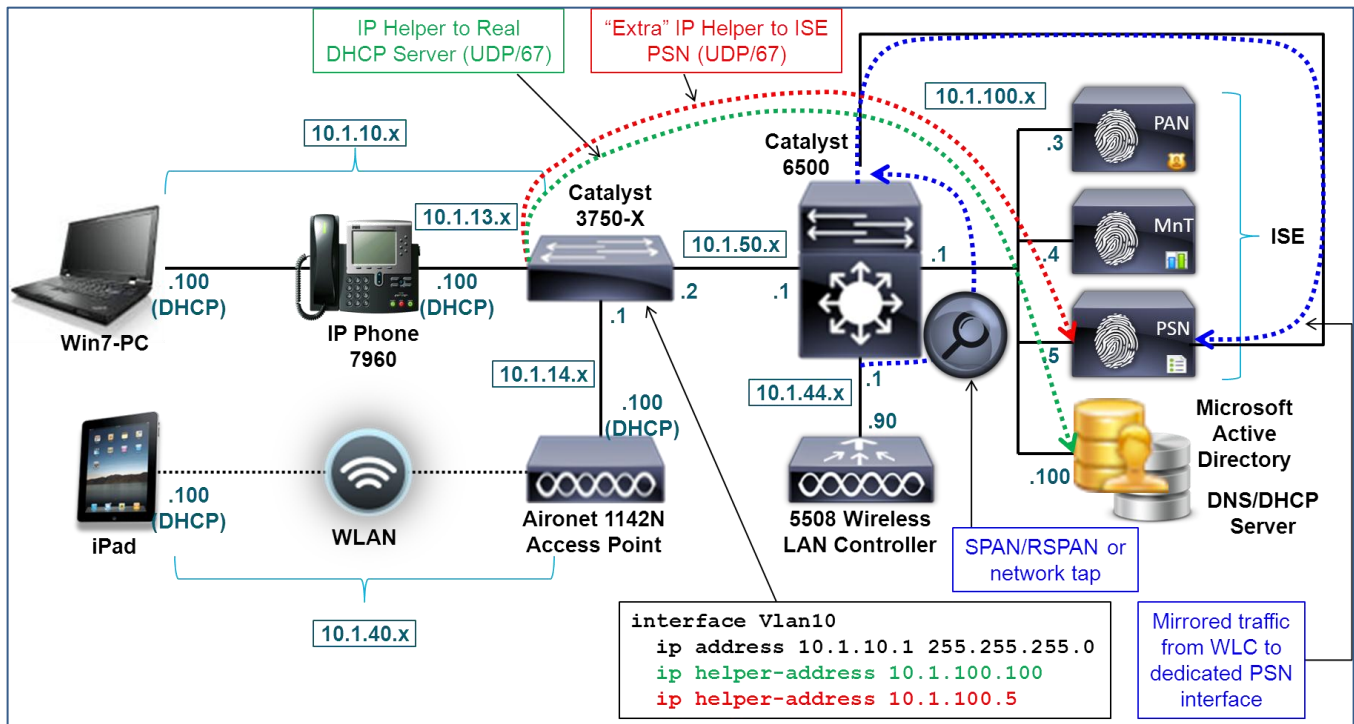
As the name implies, the DHCP probes collect attributes from DHCP packets. DHCP attributes can be collected using one or both of the following:

- DHCP Probe
- DHCP SPAN Probe

DHCP Probe

The DHCP Probe is intended for use with methods where the DHCP request is sent directly to the ISE Policy Service node, for example, as the result of DHCP Relay functions in the network. A common DHCP Relay in Cisco networks is the **ip helper-address** command applied to Layer 3 interfaces that are the gateway for local DHCP clients. Figure 26 shows an example topology using the DHCP probe.

Figure 26 DHCP Probe Example



In the diagram, the Cisco Catalyst 3750-X has both an Employee Data VLAN 10 and a Voice VLAN 13. Under the interface configuration for each Switched Virtual Interface (SVI) is an **ip helper-address** command to forward local DHCP broadcast packets to the actual DHCP server at 10.1.100.100 (highlighted in green in Figure 26). This is the server that will respond to DHCP requests. Under the same interfaces, another **ip helper-address** command is configured to point to the ISE PSN interface enabled with the DHCP probe (highlighted in red). The ISE Policy Service node will not reply to these packets, but the goal is simply to send a copy of the requests to ISE for parsing of DHCP attributes.

It is possible to configure multiple IP Helper targets on Cisco devices to allow multiple ISE Policy Service nodes to receive copies of the DHCP requests.

Note: ISE DHCP probes can parse traffic from both a DHCP Relay and a DHCP Proxy. A key difference between these methods is that DHCP Relay via **ip helper-address** command is capable of sending traffic to multiple destinations, thus allowing multiple real DHCP servers and ISE Policy Services nodes to receive a copy of the DHCP requests. DHCP Proxy, on the other hand, will send the request to only the primary DHCP server and only fall back to other configured DHCP targets if a valid response is not received. Although possible to configure the ISE nodes as the first entry to allow fallback to the actual DHCP server, such an implementation will delay the time required for an endpoint to acquire an IP address. This can impact the user experience, but may also result in the client timing out as it waits for a response.

DHCP SPAN Probe

The DHCP SPAN probe is intended for use when traffic is mirrored to an interface on the ISE Policy Service node using methods such as Switch Port Analyzer (SPAN), Remote SPAN (RSPAN), or network taps. This method is primarily used when the basic DHCP probe using DHCP Relay is not available or possible.

Best Practice: For any given flow of DHCP traffic, only one probe should be selected to collect the attributes from that traffic. There is limited value in using both DHCP (IP Helper) and DHCP SPAN probes to collect attributes from the same DHCP traffic.

If available, it is recommended to use the DHCP probe rather than the DHCP SPAN probe. Sending only DHCP packets via DHCP Relay reduces the overall traffic load on the ISE Policy Service node to inspect and parse attributes from DHCP packets.

The DHCP SPAN probe can also be used to capture DHCP traffic from local subnet broadcasts, whereas use of DHCP Probe can capture only the DHCP traffic that is relayed by an upstream gateway. This may be necessary when the Layer 3 gateway is also the DHCP Server for local clients. The Cisco IOS DHCP server will not relay DHCP for a segment if it is also configured to serve DHCP for that subnet.

The sample topology illustrates the use of SPAN or network tap to copy packets from wireless clients connected to the WLC to a dedicated interface on the Policy Service node (highlighted in blue in Figure 26). A dedicated interface is needed because SPAN destination ports may have special properties that restrict the sending and receiving of normal traffic destined to the PSN. Additionally, we do not want mirrored traffic to cause congestion on other critical interfaces of the PSN such as RADIUS. Using SPAN methods, it is possible to send more data to the SPAN port than it can handle, resulting in packet drops or delay of critical traffic.

DHCP Attributes

Both the DHCP and DHCP SPAN probes deliver the same key profiling attributes to ISE. These include some of the following:

- **dhcp-class-identifier**
- **dhcp-user-class-id**
- **dhcp-client-identifier**
- **dhcp-message-type**
- **dhcp-parameter-request-list**
- **dhcp-requested-address**
- **host-name**
- **domain-name**
- **client-fqdn**

Since DHCP provides both a MAC address (**dhcp-client-identifier**) and an IP address (**dhcp-requested-address**), it is also capable of establishing IP-to-MAC address bindings for the ISE ARP cache table. This is useful in supporting other probes that rely on IP address rather than MAC address. To apply and save the attributes they provide about a specific endpoint into the ISE database, the IP address needs to be correlated to a specific endpoint based on its MAC address.

In addition to **dhcp-client-identifier** and **dhcp-requested-address**, other key attributes include **dhcp-class-identifier**, **dhcp-user-class-id**, and **dhcp-parameters-request-list**. The class identifier is often used to convey platform or OS information. Class identifier as well as User Class ID may be customized on some client operating systems like Mac OS and Microsoft Windows, respectively, to be used as unique corporate identifiers for profiling or to return unique scope values by the DHCP server.

The **dhcp-parameters-request-list** offers a potentially unique indicator of the device type since the values and sequence of parameters requested are often unique to a single or limited set of device types. For example, a **dhcp-parameters-request-list** value of 1, 3, 6, 15, 119, 252 represents an Apple iOS device such as an iPad, iPod, or iPhone.

If a standard hostname, domain name, or Fully Qualified Domain Name (FQDN) naming convention is deployed to specific endpoints, these attributes can be used to classify them. For example, if all Windows XP clients are assigned a name such as **jsmith-winxp**, the **host-name** attribute or **client-fqdn** attribute can be used in a condition to classify Windows XP endpoints. Similarly, if there is a convention to populate the **host-name** for corporate endpoints to something like **jsmith-corp-dept**, then this attribute can be used to validate a corporate asset.

Caution must be taken to not confuse profile attributes as identity, but attributes can add a certain level of credence that the endpoint is a certain type. For example, the Authorization Policy can be used with profiling to deny full access privileges to employees where the **host-name** attribute of their PC (as indicated by matching Endpoint Identity group) does **not** include expected values.

In general, DHCP offers many profiling benefits and will often be a cornerstone for classifying a large percentage of endpoints in any environment as most endpoints provide a DHCP “fingerprint” with detailed platform information.

Configuring the DHCP and DHCP SPAN Probes

To use the DHCP probe, the access devices (or next hop gateway for Layer 2-only access devices) must be configured to send DHCP Relay or DHCP Proxy packets to the ISE PSN configured for Profiling Services. To use the DHCP SPAN probe, the network must send copies of the network traffic, preferably a filtered subset of traffic containing DHCP only, to the ISE PSN through a dedicated interface.

Another requirement for either DHCP-based probe to be effective is that endpoints of interest must obtain their IP address using DHCP. This may seem obvious, but many customers may have clientless devices that have static IP address assignments. In those cases, it may be possible to deploy static DHCP reservations to allow endpoint to keep a specific IP address while also allowing centralized management of IP addressing and support for ISE profiling via DHCP.

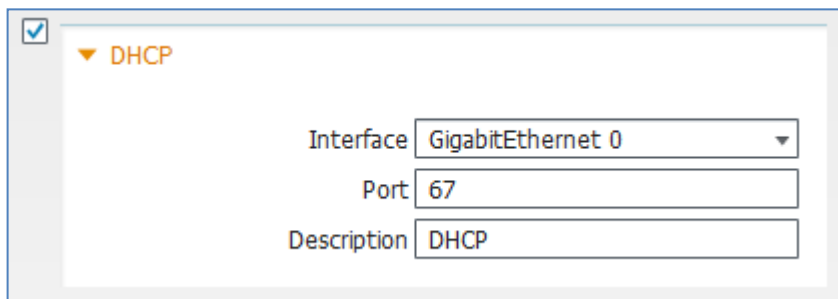
Procedure 1 Enable DHCP Probes in ISE

Step 1 Go to Administration→System→Deployment and select the Policy Service node to perform profiling from list of deployed nodes on the RHS pane.

Step 2 Select the Profiling Configuration tab.

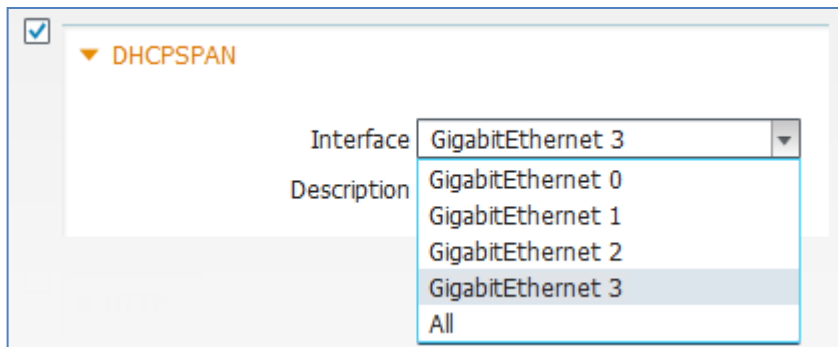
- To add support for the DHCP probe (for use with IP Helper, for example), check the box labeled DHCP as shown in the upper left corner of Figure 27.

Figure 27 DHCP Probe Configuration



- To add support for the DHCP SPAN probe (for use with SPAN or other port mirroring solution), check the box labeled DHCPSPAN (Figure 28).

Figure 28 DHCP Probe Configuration—Interfaces



Step 3 Select the interface to be used for collecting DHCP traffic.

- For use with IP Helper (DHCP Relay), the interface used is often the default interface used for Session Services. However, in larger environments where higher volumes of DHCP traffic are expected, you may want to use a dedicated interface—for example, GigabitEthernet 1, 2, or 3.
- For use with mirrored traffic (SPAN/RSPAN/taps), this should be a dedicated interface.

Step 4 Click Save to commit the changes.

Step 5 Repeat the steps in this procedure for all other Policy Service nodes configured with Profiling Services.

Note: Because of the requirements for traffic mirroring, it may not be possible or feasible to configure multiple Policy Service nodes to receive SPAN. If mirroring the same traffic flows, it may not be desirable to forward the same traffic to multiple Policy Service nodes. Although adding some redundancy, doing so can greatly increase the load on the ISE nodes and result in unnecessary duplication of profiling data which must be correlated and synced across other nodes.

Procedure 2 Add the Network Device to ISE (Network Resources)

There are no specific steps required to complete this procedure. Although access devices supporting RADIUS or SNMP may already be added to the list of ISE Network Devices (under Administration→Network Resources→Network Devices), it is not required that a network device be added to ISE solely for the purpose of forwarding of DHCP to the DHCP probe or DHCP SPAN probe.

Procedure 3 Configure ISE Policy Service Node Interface to Receive DHCP Relay Packets (DHCP Probe Only)

If the DHCP Probe is enabled on the default GigabitEthernet 0 interface, this procedure is complete. If another interface is to be used to receive DHCP Relay traffic, complete the following steps.

Step 1 Physically connect the desired interface to a network switchport.

Step 2 Access the ISE PSN console (CLI). Enable the appropriate interface and assign a valid IP address as shown in Figure 29.

Figure 29 DHCP Relay Configuration for Access Switch Example

```
ise-psn-1/admin# conf t
Enter configuration commands, one per line. End with CNTL/Z.
ise-psn-1/admin(config)# interface GigabitEthernet 3
ise-psn-1/admin(config-GigabitEthernet)# ip address 10.1.99.100 255.255.255.0

Changing the IP may result in undesired side effects on
any installed application(s).
Are you sure you want to proceed? Y/N [N]: Y
ISE M&T Log Processor is not running.
ISE M&T Log Collector is not running.
ISE M&T Alert Process is not running.
Stopping ISE Application Server...
ISE M&T Session Database is not running.
Stopping ISE Database processes...
Starting ISE Database processes...
ISE M&T Session Database is not running.
Starting ISE Application Server...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise-psn-1/admin(config-GigabitEthernet)# _
```

Step 3 Verify all processes are in a running state as instructed.

Step 4 Verify the configuration of the newly configured interface and that it is enabled (NOT in shutdown) by using the **show running-config** command (Figure 30).

Figure 30 Verify DHCP Relay Configuration for Access Switch Example

```
ise-psn-1/admin# show running-config
Generating configuration...
?
hostname ise-psn-1
?
ip domain-name cts.local
?
interface GigabitEthernet 0
  ip address 10.1.100.5 255.255.255.0
  ipv6 address autoconfig
?
interface GigabitEthernet 1
  shutdown
  ipv6 address autoconfig
?
interface GigabitEthernet 2
  shutdown
  ipv6 address autoconfig
?
interface GigabitEthernet 3
  ip address 10.1.99.100 255.255.255.0
  ipv6 address autoconfig
?
ip name-server 10.1.100.100
--More--
```

Step 5 Verify connectivity to the new ISE probe interface by sending an ICMP ping from a network device that needs to relay DHCP.

Step 6 Save changes using the CLI command **copy running-config startup-config**.

Procedure 4 Configure ISE Policy Service Node Interface to Receive SPAN Traffic (DHCP SPAN Probe Only)

Step 1 Physically connect the desired interface to the appropriate SPAN destination port or network tap interface.

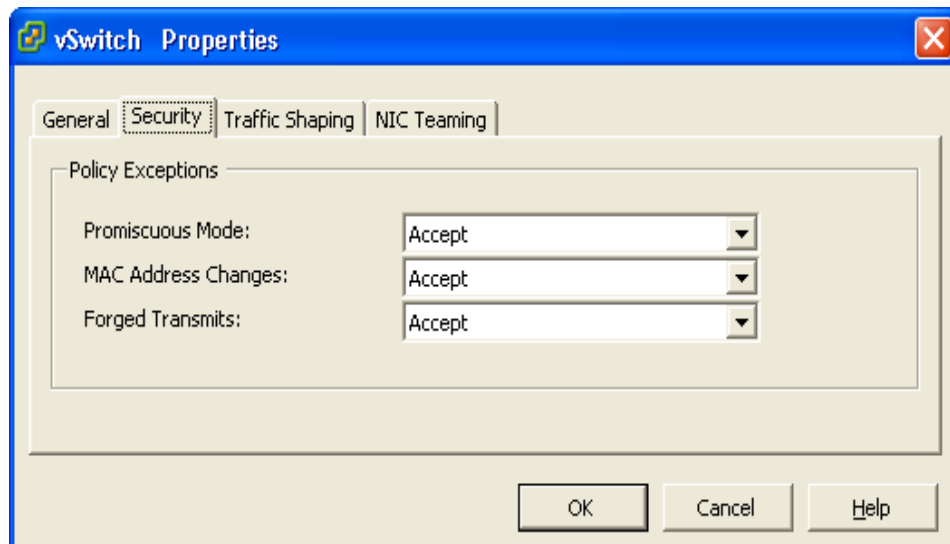
Step 2 Access the ISE PSN console (CLI). Enable the appropriate interface by simply entering **no shutdown** while in configuration mode for the desired interface.

Step 3 Save changes using the ISE CLI command **copy running-config startup-config**.

Note: For Policy Service Nodes Running on VMware Appliance

To use a dedicated interface for profiling, it is assumed that additional virtual interfaces were configured for the virtual appliance. If not completed at the time of install, it will be necessary to shut down the ISE node and update the hardware and networking configuration of the ESX appliance for the required interface(s) before continuing with the ISE configuration.

Additionally, to accept SPAN/mirror traffic on the ISE DHCP SPAN interface, the VMware appliance requires promiscuous mode to be set on the virtual switch interface. To enable this mode, go to VMware Host→Configuration→Hardware→Networking→vSwitch→Security and set Promiscuous Mode: Accept (Default = Reject), as follows:



Procedure 5 Configure Wired Access Devices to Relay DHCP Packets to the ISE PSN (DHCP Probe Only)

Step 1 Go to the management console of the Cisco Catalyst switch or router. Under each routed interface that connects to an endpoint subnet where DHCP traffic originates, add the following commands:

```
interface <Endpoint_VLAN>
ip helper-address <ISE_PSN_address>
```

The address specified should be to the PSN interface with the DHCP Probe enabled. For redundancy, you can add more IP Helper statements to relay DHCP to other Policy Service nodes, but the recommendation is to keep this at a minimum to reduce traffic duplication because each PSN will process the traffic received.

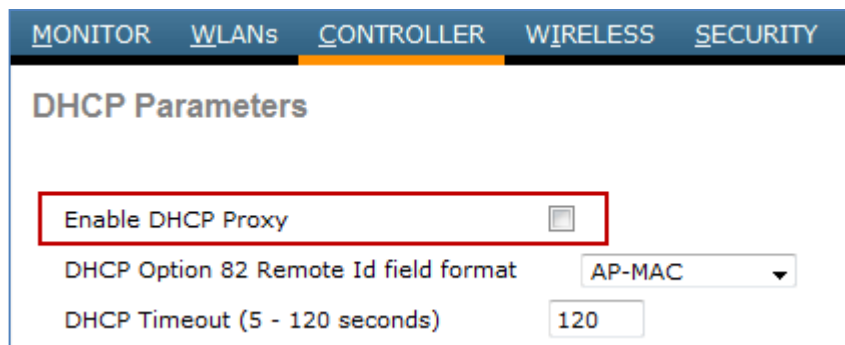
Procedure 6 Configure Wireless Access Devices to Relay DHCP Packets to the ISE PSN (DHCP Probe Only)

It is recommended that you configure WLCs in DHCP Bridging mode rather than DHCP Proxy mode so that all DHCP packets are forwarded from the wireless clients to the ISE PSN.

Step 1 Go to the web administrative interface of the Cisco Wireless LAN Controller or Wireless Services Module. Navigate to Controller→Advanced→DHCP→DHCP Parameters.

Step 2 If the checkbox labeled Enable DHCP Proxy is selected, deselect/uncheck it (Figure 31).

Figure 31 DHCP Relay Configuration for Wireless Controller Example



Step 3 For each WLAN configured on the WLC using DHCP, be sure the upstream gateway is configured to relay DHCP to the ISE Policy Service node as described in the previous procedure.

Procedure 7 Configure Network Devices to Send Copies of DHCP Traffic to the PSN (DHCP SPAN Probe only)

There are multiple ways to mirror traffic to the ISE Policy Service node. This procedure will show one common way using basic SPAN on a Cisco Catalyst switch.

Step 1 Determine the interface(s) or VLAN(s) that will be the source of DHCP traffic. Certain chokepoints such as the egress interface of a WLC or connection to DHCP server(s) can make ideal places to capture all client DHCP packets.

In the following example, interface GigabitEthernet 1/1 is a trunk connection to a Cisco 5500 Series Wireless LAN Controller. Interface GigabitEthernet 2/37 is a switchport connection to a Cisco UCS® server running VMware ESXi 4.1. The ESX server hosts an ISE virtual appliance configured as a Policy Services node with Profiling enabled. Interface GigabitEthernet 2/37 is link to a virtual interface linked to the ISE PSN as Gigabit Ethernet 3.

```
interface GigabitEthernet1/1
description WLC5508 ETH0 (Port 1)
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 40-44
switchport mode trunk

interface GigabitEthernet2/37
description UCS1 SPAN (port 3 of 4)
switchport
```

Step 2 Configure SPAN to capture all inbound and outbound traffic on the 5500 Series switch connection and forward to the ISE PSN connection. To do this, interface GigabitEthernet 1/1 is set as the SPAN source and interface GigabitEthernet 2/37 is the destination. Since ISE does not need to see tagged packets, 802.1Q trunking is not enabled on the switchport.

```
cat6500(config)# monitor session 1 source interface gigabitEthernet 1/1 both
cat6500(config)# monitor session 1 destination interface gigabitEthernet 2/37
```

Step 3 Verify the configuration and save.

```
cat6500# show monitor session 1
Session 1
-----
Type                : Local Session
Source Ports        :
    Both             : Gi1/1
Destination Ports    : Gi2/37

Egress SPAN Replication State:
Operational mode     : Centralized
Configured mode      : Centralized (default)
```

Procedure 8 Verify DHCP Probe Data

Step 1 Delete the endpoint from Administration→Identity Management→Identities→Endpoints.

Step 2 Disconnect and then reconnect the endpoint from the access device where the gateway interface has IP Helper forwarding DHCP to the ISE PSN.

Step 3 Go to the ISE Policy Administration node and navigate to Administration→Identity Management→Identities.

Step 4 Select Endpoints from the LHS pane.

Find and select the MAC address of the newly connected endpoint to display the attributes captured by the DHCP probe (Figure 32). The example shown is taken using only the DHCP probe to highlight the attributes collected using DHCP.

Figure 32 DHCP Probe Attributes Example

Endpoint List > 00:30:94:C4:52:8A

Endpoint

* MAC Address **00:30:94:C4:52:8A**

* Policy Assignment Cisco-IP-Phone ▼

Static Assignment ☐

* Identity Group Assignment Cisco-IP-Phone ▼

Static Group Assignment ☐

Attribute List

EndPointPolicy	Cisco-IP-Phone
EndPointProfilerServer	ise-psn-1
EndPointSource	DHCP Probe
IdentityGroup	Cisco-IP-Phone
MACAddress	00:30:94:C4:52:8A
MatchedPolicy	Cisco-IP-Phone
OUI	Cisco Systems, Inc.
PolicyVersion	22
StaticAssignment	false
StaticGroupAssignment	false
TimeToProfile	24
Total Certainty Factor	30
chaddr	00:30:94:c4:52:8a
ciaddr	0.0.0.0
dhcp-class-identifier	Cisco Systems, Inc. IP Phone CP-7960
dhcp-client-identifier	01:00:30:94:c4:52:8a
dhcp-message-type	DHCPDISCOVER
dhcp-parameter-request-list	1, 66, 6, 3, 15, 150, 35
dhcp-requested-address	10.1.13.100
flags	0x8000
giaddr	10.1.13.1
hlen	6
hops	1
host-name	SEP003094C4528A
htype	Ethernet (10Mb)
ip	10.1.13.100
op	BOOTREQUEST
secs	0
yiaddr	0.0.0.0

The key attributes highlighted include:

- **EndPointSource**
- **OUI**

- **dhcp-class-identifier**
- **dhcp-client-identifier**
- **dhcp-parameter-request-list**
- **dhcp-requested-address**

The **EndPointSource** shows that the DHCP probe was the source of last attribute update.

The **dhcp-client-identifier** typically provides the MAC address, which in turn provides the vendor OUI information through correlation from the MAC Address-OUI mapping table.

The **dhcp-requested-address** is the IP address requested by the endpoint. Along with the **dhcp-client-identifier**, this provides the binding between the IP and MAC address.

The **dhcp-class-identifier** often provides a unique platform-specific attribute and in some cases provides a detailed description of the connected endpoint—in this example, Cisco Systems, Inc. IP Phone CP-7960.

The **dhcp-parameter-request-list** also indicates that the endpoint is a Cisco IP phone since the exact sequence 1, 66, 6, 3, 15, 150, 35, 151 is typically used only by certain Cisco IP phones.

In summary, one or more attributes can classify network endpoints using DHCP. As explained later in the [Device Sensor](#) section of this guide, Cisco offers the capability to collect DHCP and other information using a local classification technology referred to as Device Sensor. This feature makes it possible to collect DHCP attributes even when it is not possible through IP Helper or SPAN techniques. This solution offers a much more scalable approach to endpoint attribute collection and classification.

Profiling Using the HTTP Probe

Web browsers typically identify themselves, including application type, operating system, software vendor, and software revision by submitting a characteristic identification string to the web server. In HTTP, this is transmitted in an HTTP request-header field known as **User-Agent**.

The **User-Agent** is the primary attribute collected using the HTTP probe. ISE profiling captures the web browser information from the **User-Agent** attribute, as well as other HTTP attributes from the request messages, and adds 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.

The two methods used to send HTTP traffic to the HTTP probe include the following:

- URL Redirection
- SPAN (and other traffic mirroring methods)

The HTTP probe listens to communication from web browsers on both port 80 and port 8080. Both the URL Redirection and SPAN methods provide the **User-Agent** attribute to the HTTP probe.

HTTP Probe Using URL Redirection

ISE uses URL redirection for a number of user session services including Central WebAuth (CWA), Local WebAuth (LWA), Device Registration WebAuth (DRW), Client Provisioning, Posture Assessment, and Native Supplicant Provisioning (NSP). In each of these use cases, the endpoint's web browser is redirected to the ISE Policy Service node. During this process, it is possible for ISE to capture the **User-Agent** attribute.

The sample topology in Figure 33 illustrates the use of URL redirection as a part of the initial authorization of the endpoint, ISE can send a URL redirect to the access device (highlighted in green in Figure 33). When the client opens a web browser, they are redirected to the Policy Service node (highlighted in red) for a specified service such as Central WebAuth.

ISE sends URL Redirect to access device as RADIUS authorization result

Endpoint opens browser; redirected to PSN on TCP/8443 (default port)

Win7-PC

IP Phone 7960

iPad

WLAN

Aironet 1142N Access Point

Catalyst 3750-X

Catalyst 6500

5508 Wireless LAN Controller

ISE

PAN

MnT

PSN

Microsoft Active Directory

DNS/DHCP Server

SPAN/RSPAN or network tap

Mirrored traffic from WLC to dedicated PSN interface

cisco-av-pair = url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cwa

URL redirection can also be initiated as a RADIUS authorization from ISE to the network access device. An example of a URL redirect triggered by a RADIUS authorization is Central WebAuth whereby the access device helps facilitate the redirection, but the actual session is established between the client and the ISE Policy Service node and is tracked via a unique session ID.

To use the HTTP probe without URL redirection, the optional method is to copy, or mirror, web traffic to an interface on the ISE Policy Service node using methods such as SPAN, RSPAN, or network taps. This method is primarily used when URL redirection is not feasible or possible.

If URL redirection is not applicable, for example in a Cisco NAC Appliance deployment that does not use RADIUS-based authentication, or in an endpoint discovery phase where RADIUS has yet to be deployed to the access devices, the SPAN method is the preferred method as it still allows capture of the **User-Agent** without RADIUS or URL redirection as a requirement.

HTTP Probe and IP-to-MAC Address Binding Requirement

40

learned **User-Agent** attribute. Consequently, it is required to learn the IP-to-MAC address binding via another probe **prior** to collecting HTTP data. Probes that can be used to provide this information include the following:

- RADIUS (via the **Framed-IP-Address** attribute)
- DHCP (via the **dhcp-requested-address** attribute)
- SNMP Query (via SNMP polling)

There are special HTTP profiling scenarios that offer exceptions to the IP-to-MAC binding requirement. These include:

- URL Redirection with Client Provisioning
- URL Redirection with Central WebAuth

URL Redirection with Client Provisioning

Client Provisioning (CP) is the ISE session service that provides dynamic download of agent and configuration files to the endpoint to enable Posture Agent and Native Supplicant Provisioning (NSP) services. Client Provisioning relies on URL redirection. During the CP process, the Policy Service node must determine the client OS through its user agent to know which provisioning policy to apply. For example, if the endpoint is detected as a Windows client, the Windows posture agent should be selected for posture support. Similarly, if the endpoint is detected as an Android client, the Supplicant Provisioning files for an Android client should be installed on the endpoint.

When the Client Provisioning service learns the **User-Agent** attribute, ISE uses this knowledge by updating the profiling service with this information. Additionally, since Client Provisioning is part of an active session, ISE is able to apply this information to the MAC address (**Calling-Station-ID**) retrieved from the session cache. It is therefore possible to fully profile many endpoints using this process alone.

URL Redirection with Central WebAuth

Central WebAuth (CWA) relies on URL redirection. During the CWA process, the HTTP probe is able to capture the **User-Agent** attribute from the redirected HTTPS packets after decryption on the Policy Services node. Similar to Client Provisioning service, the guest flow is part of an active session from which ISE is able to retrieve the MAC address (**Calling-Station-ID**) from the session cache. This process allows HTTP probe to learn the **User-Agent** and associated MAC address required to populate the endpoint database.

In general, the HTTP probe provides a high level of fidelity for detecting client OS types via **User-Agent**. The HTTP probe is recommended when a policy based on operating system is required, particularly for wireless environments where customers often need to provide differentiated access based on whether the endpoint is a personal or corporate asset.

In both scenarios—URL redirect with CP and URL redirect with CWA—ISE is able to apply the **User-Agent** attribute to a MAC address without a pre-existing IP-to-MAC address binding. HTTP SPAN methods always require a preexisting IP-to-MAC binding entry unless the mirrored traffic is taken from a segment that is Layer 2 adjacent to the endpoint. In this particular case, the packet source MAC address is that of the actual endpoint, and can be used to update the endpoint database accordingly.

Best Practice: To acquire the **User-Agent**, use URL redirection with the HTTP probe for CWA use cases. Profiling using URL redirection with Client Provisioning is automatic when the Posture Agent or Native Supplicant Provisioning service is required, but in some cases, it may be desirable to deliberately trigger CP even if Posture or Supplicant Provisioning is not required. This can be accomplished through redirection to CWA (with posture agent enabled) or to Client Provisioning and Posture (CPP) services (Posture Discovery) when the endpoint profile is set to Unknown or incomplete. The goal is to capture the **User-Agent** in the process and allow resulting Posture Status to trigger a Change of Authorization (CoA). Upon reconnection, a new Authorization Policy rule can be assigned based on a more refined profile match.

As noted, URL redirection is generally preferred over HTTP SPAN as it allows the Policy Service node to acquire the **User-Agent** attribute with minimal traffic load versus packet mirroring methods; in some special cases allows profiling without first populating an ARP cache. Additionally, URL redirection based on RADIUS authorization simplifies high-availability scenarios because the redirect is always sent to the same PSN that terminated the RADIUS traffic.

However, there are some scenarios, such as access devices without RADIUS deployed, where SPAN method may be the only feasible option.

Configuring the HTTP Probe

To use the HTTP probe with redirected traffic, the access device must be capable of redirecting HTTP traffic to ISE either directly (for example, through Local WebAuth) or via a RADIUS authorization. For RADIUS-based redirection, ISE must be configured with an Authorization Policy rule to return the Cisco attribute value pair (AVP) for **url-redirect** as an authorization result.

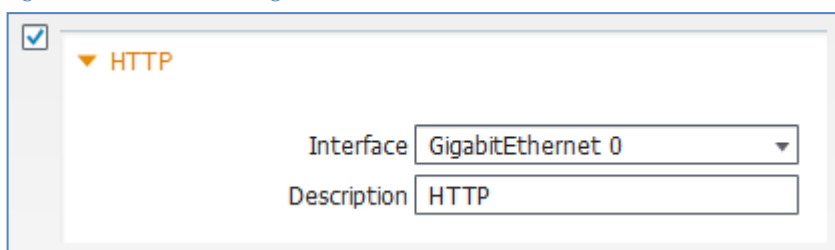
To use the HTTP probe with SPAN, the network must send copies of the network traffic, preferably a filtered subset of traffic containing HTTP only, to the ISE PSN through a dedicated interface.

Procedure 1 Enable HTTP Probe in ISE

Step 1 Go to Administration→System→Deployment and select the Policy Service node to perform profiling from list of deployed nodes on the RHS pane.

Step 2 Select the Profiling Configuration tab. To add support for the HTTP probe, select the box labeled HTTP (Figure 34).

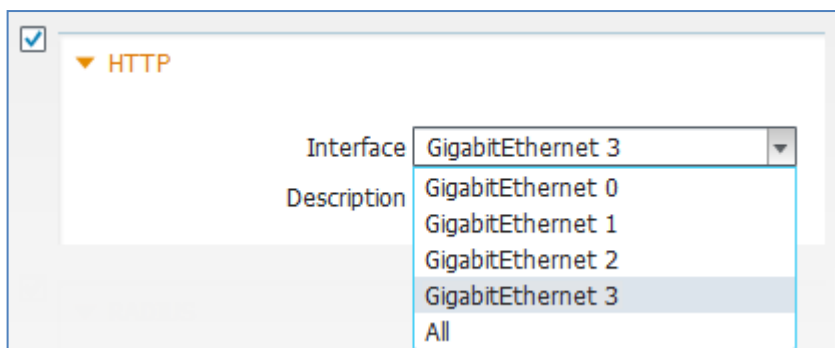
Figure 34: HTTP Probe Configuration



Step 3 Select the interface to be used for collecting HTTP traffic.

- For use with URL redirection, the interface used should be GigabitEthernet 0, the same interface used for Session Services such as RADIUS, Web Authentication, Posture, and so on.
- For use with mirrored traffic (SPAN/RSPAN/taps), this should be a dedicated interface (Figure 35).

Figure 35 HTTP Probe Configuration—Interfaces



Step 4 Click Save to commit the changes.

Step 5 Repeat the steps in this procedure for all other Policy Service nodes configured with Profiling Services.

Note: Due to the requirements for traffic mirroring, it may not be possible or feasible to configure multiple Policy Service nodes to receive SPAN. If mirroring the same traffic flows, then it may not be desirable to forward the same traffic to multiple Policy Service nodes. Although adding some redundancy, doing so can greatly increase the load on the ISE nodes and result in unnecessary duplication of profiling data which must be correlated and synced across other nodes.

Procedure 2 Add the Network Device to ISE (Network Resources)

There are no specific steps required to complete this procedure. When URL redirection is the method used to capture HTTP data, the network access device must already be configured to support RADIUS-based authentication, so no additional steps are required to add or edit the network access device.

When SPAN is the method used to capture HTTP data, there is no specific requirement to add the access device to ISE if it is not performing RADIUS-based authentication.

Procedure 3 Configure ISE Policy Service Node Interface to Receive Redirected HTTP Traffic

There are no specific steps required to complete this procedure. When URL redirection is used, the HTTP probe should be enabled on the default GigabitEthernet 0 interface. Therefore, no additional interface configuration is required.

Procedure 4 Configure ISE Policy Service Node Interface to Receive HTTP SPAN Traffic

When SPAN is used, the HTTP probe should be configured on a dedicated SPAN interface to receive HTTP traffic. To configure a dedicated SPAN interface on ISE, complete the following steps:

Step 1 Physically connect the desired interface to the appropriate SPAN destination port or network tap interface.

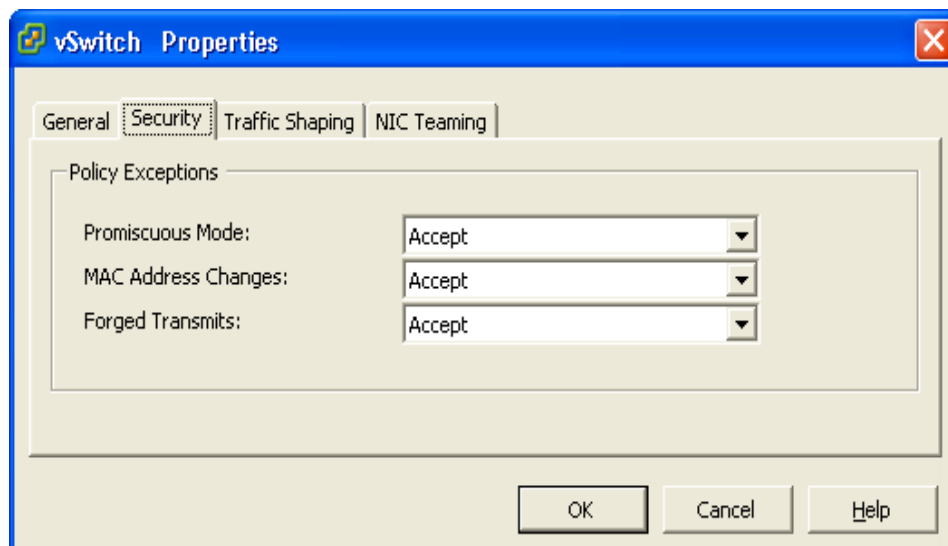
Step 2 Access the ISE PSN console (CLI). Enable the appropriate interface by simply entering **no shutdown** while in configuration mode for the desired interface.

Step 3 Save changes using the ISE CLI command **copy running-config startup-config**

Note: For Policy Service Nodes Running on VMware Appliance

To use a dedicated interface for profiling, it is assumed that additional virtual interfaces were configured for the virtual appliance. If not completed at the time of install, it will be necessary to shut down the ISE node and update the hardware and networking configuration of the ESX appliance for the required interface(s) before continuing with the ISE configuration.

Additionally, to accept SPAN/mirror traffic on the ISE DHCP SPAN interface, the VMware appliance requires promiscuous mode to be set on the virtual switch or interface. To enable this mode, go to VMware Host→Configuration→Hardware→Networking→vSwitch→Security and set Promiscuous Mode: Accept (Default = Reject), as follows:



Procedure 5 Configure Wired Access Devices to Redirect HTTP Packets to the ISE PSN

Access device configuration to support URL redirection for specific services including CWA, Posture, or Supplicant Provisioning is beyond the scope of this guide. In summary, essential commands to support redirection based on RADIUS authorization using a Cisco Catalyst switch will be similar to the following:

Step 1 Under global configuration mode, enable HTTP and optionally HTTPS servers.

Step 2 Configure the redirect ACL that is referenced in the ISE RADIUS authorization to specify traffic eligible for redirection.

```
ip http server
ip http secure-server
ip access-list extended REDIRECT-ACL
deny tcp any any <PSN_IP_address>
permit tcp any any eq http
permit tcp any any eq https
```

For traffic initiated by the client, Catalyst switches can support redirection of both HTTP and HTTPS traffic. The traffic redirected to ISE is always HTTPS.

Procedure 6 Configure Wireless Access Devices to Redirect HTTP Packets to the ISE PSN

Access device configuration to support URL redirection for specific services, including CWA, Posture, or Supplicant Provisioning, is beyond the scope of this guide. In summary, essential steps to support redirection based on RADIUS authorization using a Wireless LAN Controller will be similar to the following example:

Step 1 Under Security→AAA→RADIUS→Authentication→(RADIUS Server)→Edit, verify that Support for RFC 3576 is set to Enabled (Figure 36).

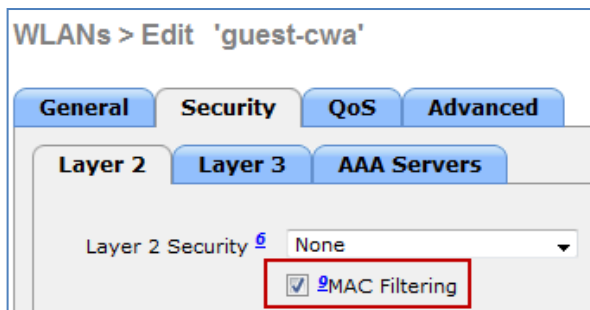
Figure 36 CoA Configuration for Wireless Controller Example

RADIUS Authentication Servers > Edit

Server Index	2
Server Address	10.1.100.5
Shared Secret Format	ASCII
Shared Secret	...
Confirm Shared Secret	...
Key Wrap	<input type="checkbox"/> (Designed for FIPS)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

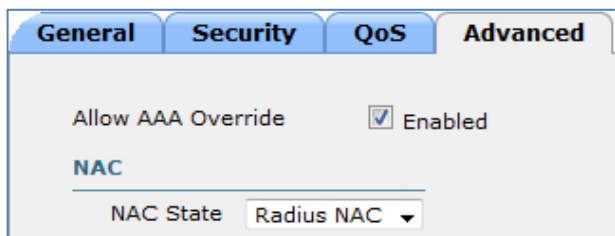
Step 2 Under WLANs→Edit (WLAN)→Security→Layer 2, configure the WLAN for MAC Filtering. Layer 2 and Layer 3 Security should be set to None (Figure 37).

Figure 37 MAC Filtering Configuration for Wireless Controller Example



Step 3 Under the Advanced tab, select Allow AAA Override and set the NAC State to RADIUS NAC (Figure 38).

Figure 38 RADIUS Authorization Configuration for Wireless Controller Example



For traffic initiated by the client, Cisco Wireless LAN Controllers support redirection of HTTP traffic only. Redirection of HTTPS traffic is not supported. The traffic redirected to ISE is always HTTPS.

Procedure 7 Configure ISE to Perform URL Redirection as a RADIUS Authorization

ISE configuration to support URL redirection for specific services, including CWA, Posture, or Supplicant Provisioning, is beyond the scope of this guide. In summary, essential steps to support redirection based on RADIUS authorization in the ISE Authorization Policy will be similar to the following example:

Step 1 From the ISE administration interface, go to Policy→Policy Elements→Results.

Step 2 Select Authorization→Authorization Profiles from the LHS pane, and then click Add from the RHS pane to add a new Authorization Profile named **Posture_Remediation**, as shown in Figure 39.

Figure 39 Authorization Profile for URL Redirection Configuration Example

Authorization Profiles > Posture_Remediation

Authorization Profile

* Name:

Description:

* Access Type:

▼ Common Tasks

☒ DACL Name:

☐ VLAN

☐ Voice Domain Permission

☒ Web Authentication: ACL:

☐ Auto Smart Port

▼ Advanced Attributes Settings

Select an item = +

▼ Attributes Details

```
Access Type = ACCESS_ACCEPT
DACL = POSTURE_REMEDIATION
cisco-av-pair = url-redirect-ac=ACL-POSTURE-REDIRECT
cisco-av-pair = url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=cpp
```

In the example shown in Figure 39, the Common Task labeled Web Authentication is select with the specific redirect selected as Posture Discovery. This will result in the endpoint being redirect to Client Provisioning and Posture services, or CPP. The redirect ACL is ACL-POSTURE-REDIRECT and must be preconfigured on the access device. The resulting RADIUS authorizations are highlighted in blue.

Step 3 Go to Policy→Authorization and add an Authorization Policy rule named **Employee_PreCompliant** that uses the new Authorization Profile for employees where the device type used is neither a workstation nor Apple iPad (see Figure 40).

Figure 40 Authorization Policy Rule for URL Redirection Example

<input checked="" type="checkbox"/>	Employee-Workstation	if	Workstation AND Employee	then	Employee AND SGT_Employee
<input checked="" type="checkbox"/>	Employee-iPad	if	Apple-iPad AND Employee	then	Employee_iPad AND SGT_Guest
<input checked="" type="checkbox"/>	Employee_PreCompliant	if	(Employee AND Session:PostureStatus NOT_EQUALS Compliant)	then	Posture_Remediation

In Figure 40 example, the rule labeled **Employee_PreCompliant** is deliberately placed **after** the previous rules to ensure that it is only matched in the event that the employee connects to network and the device type does not match one of the explicit Endpoint Identity Groups equal to **Workstation** or **Apple-iPad**. When the authenticated employee matches the Employee_PreCompliant rule, they are assigned the Authorization Profile named **Posture_Redirection**. This will return an RADIUS authorization to the access device to perform URL redirection to the Client Provisioning and Posture service.

Procedure 8 Configure Network Devices to Send Copies of HTTP Traffic to the ISE PSN

There are multiple methods to mirror traffic to the ISE Policy Service node. This procedure shows one common way using VACL Capture on a Cisco Catalyst switch. This method has the added benefit of being able to forward only select traffic of

interest to the ISE Policy Service node.

Best Practice: When available, utilize intelligent tap systems that support scalable traffic mirroring with filters to only send the required traffic to the ISE probe. This includes DHCP SPAN and HTTP probes that rely on SPAN methods to acquire profiling data. More advanced tap systems will support high availability for mirrored traffic.

Alternatively, when supported by the infrastructure, take advantage of intelligent SPAN techniques such as VACL Capture on the local switch, or VACL Capture/Redirect in conjunction with RSPAN, to allow selective capture of network traffic.

Step 1 Determine the interface(s) or VLAN(s) that will be the source of DHCP traffic. Certain chokepoints such as the egress interface of a WLC or connection to DHCP Server(s) can make ideal places to capture all client DHCP packets.

In the following example, VLANs 40-44 are trunked to the Cisco 5500 Series Wireless LAN Controller. GigabitEthernet 2/37 is a switchport connection to a Cisco UCS server running VMware ESXi 4.1. The ESX server hosts an ISE virtual appliance configured as a Policy Services node with profiling enabled. Interface GigabitEthernet 2/37 is link to a virtual interface linked to the ISE PSN as Gigabit Ethernet 3.

```
interface GigabitEthernet1/1
description WLC5508 ETH0 (Port 1)
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 40-44
switchport mode trunk

interface GigabitEthernet2/37
description UCS1 SPAN (port 3 of 4)
switchport
```

Step 2 Configure VACL Capture to match all HTTP traffic on VLANs 40-44 and forward to the ISE PSN connection.

- a. Configure an ACL to match only HTTP traffic and another to match all IP traffic, as follows:

```
cat6500(config)# ip access-list extended HTTP_TRAFFIC
cat6500(config-ext-nacl)# permit tcp any any eq www

cat6500(config)# ip access-list extended ALL_TRAFFIC
cat6500(config-ext-nacl)# permit ip any any
```

- b. Configure a VLAN access map with a sequence that sets the capture bit on traffic that matches the HTTP_TRAFFIC ACL. Configure another sequence in the same VLAN access map that forward all other traffic (matches the ALL_TRAFFIC ACL).

```
cat6500(config)# vlan access-map HTTP_MAP 10
cat6500(config-access-map)# match ip address HTTP_TRAFFIC
cat6500(config-access-map)# action forward capture

cat6500(config)# vlan access-map HTTP_MAP 20
cat6500(config-access-map)# match ip address ALL_TRAFFIC
cat6500(config-access-map)# action forward
```

- c. Configure a VLAN filter that applies the VLAN access map to VLANs 40, 41, 42, and 43, as follows:

```
cat6500(config)# vlan filter HTTP_MAP vlan-list 40-43
```

- d. Configure the capture port (Gi2/37) to include all matching traffic on VLANs 40, 41, 42, and 43, including traffic routed to upstream VLAN 100, as follows:

```
cat6500(config)# int Gi2/37
cat6500(config-if)# switchport capture allowed vlan 40-43,100
cat6500(config-if)# switchport capture
```


Procedure 9 Verify HTTP Probe Data Using URL Redirection (CWA Example)

Step 1 Delete the endpoint from Administration→Identity Management→Identities→Endpoints.

Step 2 Disconnect and then reconnect the endpoint from the access device configured to support HTTP redirection to the ISE PSN.

Step 3 Log in from the endpoint using web authentication.

Step 4 Go to the ISE Policy Administration node and navigate to Administration→Identity Management→Identities.

Step 5 Select Endpoints from the LHS pane.

Step 6 Find and select the MAC address of the newly connected endpoint to display the attributes captured by the HTTP probe.

The example in Figure 41 shows using only the HTTP probe to highlight the attributes collected using URL redirection.

Figure 41 HTTP Probe Attributes with URL Redirection—CWA Example

* MAC Address	00:50:56:A0:0B:3A
* Policy Assignment	Windows7-Workstation
Static Assignment	<input type="checkbox"/>
* Identity Group Assignment	Microsoft-Workstation
Static Group Assignment	<input type="checkbox"/>
Attribute List	
EndPointPolicy	Windows7-Workstation
EndPointSource	HTTP Probe
IdentityGroup	Microsoft-Workstation
MACAddress	00:50:56:A0:0B:3A
MatchedPolicy	Windows7-Workstation
OUI	VMware, Inc.
PolicyVersion	20
StaticAssignment	false
StaticGroupAssignment	false
Total Certainty Factor	60
User-Agent	Mozilla/5.0 (Windows NT 6.1; rv:11.0) Gecko/20100101 Firefox/11.0

The key attributes highlighted include:

- **EndPointSource**
- **MACAddress**
- **OUI**
- **User-Agent**

The example shown is taken using only the HTTP probe to highlight the attributes collected using URL redirection. This particular scenario allows the endpoint to be added to the Internal Endpoints database even without an IP-to-MAC address binding.

As you can see in Figure 41, the **EndPointSource** shows that the HTTP probe is the latest source for attribute updates.

MACAddress is the value obtained from the session cache. **OUI** is derived from the **MACAddress** value.

User-Agent is the critical data point that reveals that this VMware-based client is running the Windows 7 operating system.

Procedure 10 Verify HTTP Probe Data Using URL Redirection (Client Provisioning Example)

Step 1 Delete the endpoint from Administration→Identity Management→Identities→Endpoints.

Step 2 Disconnect and then reconnect the endpoint from the access device configured to support HTTP redirection to the ISE PSN.

Step 3 Attempt login from the endpoint.

Step 4 Navigate to Administration→Identity Management→Identities and select Endpoints from the LHS pane.

Step 5 Find and select the MAC address of the newly connected endpoint to display the attributes captured by the Client Provisioning service.

Figure 42 shows an example without any probes enabled to highlight the attributes collected using URL redirection with Client Provisioning.

Figure 42 HTTP Probe Attributes with URL Redirection—Client Provisioning Example

* MAC Address	7C:6D:62:E3:D5:05
* Policy Assignment	Apple-iPad
Static Assignment	<input type="checkbox"/>
* Identity Group Assignment	Apple-iPad
Static Group Assignment	<input type="checkbox"/>
Attribute List	
EndPointPolicy	Apple-iPad
EndPointProfilerServer	ise-psn-1
EndPointSource	CP
IdentityGroup	Apple-iPad
MACAddress	7C:6D:62:E3:D5:05
MatchedPolicy	Apple-iPad
OUI	Apple, Inc
PolicyVersion	20
StaticAssignment	false
StaticGroupAssignment	false
TimeToProfile	26
Total Certainty Factor	30
User-Agent	Mozilla/5.0 (iPad; CPU OS 5_0_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9A405 Safari/7534.48.3

The key attributes highlighted are similar to those in previous example with the exception of the **EndPointSource**, which is set to CP (Client Provisioning).

Procedure 11 Verify HTTP Probe Data using SPAN

Step 1 Delete the endpoint from Administration→Identity Management→Identities→Endpoints.

Step 2 Disconnect and then reconnect the endpoint from the access device configured.

Step 3 Open the web browser on the endpoint and attempt http access to any website.

Step 4 Navigate to Administration→Identity Management→Identities and select Endpoints from the LHS pane.

Step 5 Find and select the MAC address of the newly connected endpoint to display the attributes captured by the HTTP probe.

Figure 43 shows only the HTTP probe enabled to highlight the attributes collected using SPAN.

Figure 43 HTTP Probe Attributes with SPAN Example

Endpoint List > 7C:6D:62:E3:D5:05

Endpoint

* MAC Address **7C:6D:62:E3:D5:05**

* Policy Assignment Apple-iPad ▼

Static Assignment ☐

* Identity Group Assignment Apple-iPad ▼

Static Group Assignment ☐

Attribute List

Cookie	NID=59=eFjUh-KeyMVy3sJa6yME53u3iI1LDRrpolvqVVdInBu30HDIVTz; PREF=ID=14254f19b36df761:U=9b71d718247b1acd:FF=0:TM=1339
EndPointPolicy	Apple-iPad
EndPointProfilerServer	ise-psn-1
EndPointSource	HTTP Probe
Host	www.google.com
IdentityGroup	Apple-iPad
MACAddress	7C:6D:62:E3:D5:05
MatchedPolicy	Apple-iPad
OUI	Apple, Inc
PolicyVersion	22
StaticAssignment	false
StaticGroupAssignment	false
TimeToProfile	21
Total Certainty Factor	30
User-Agent	Mozilla/5.0 (iPad; CPU OS 5_0_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9A405 Safari/7534.48.3
ip	10.1.41.101

The key attributes include the same in previous examples as well as some new attributes:

- **Cookie** (truncated for display)
- **Host**

After the initial CWA process is completed, the output was similar to that using URL redirection. These additional attributes represent the capture of additional HTTP header information collected by normal client browsing activity. As these attributes change, ISE will be constantly updated. It is apparent that these numerous updates for attributes that may not be used can result in a much higher impact to the database update and synchronization process. This highlights again how capture of the **User-Agent** using the HTTP probe with URL redirection can be much more efficient than SPAN methods.

In summary, endpoints can be classified based on their operating system as determined by the **User-Agent** attribute. This attribute can be collected by the HTTP probe and in special cases by Client Provisioning services. Two general methods to collect HTTP traffic include URL redirection and SPAN techniques. In general, URL redirection is much more efficient, although SPAN may be the only option if profiling is required in an environment without RADIUS authentication enabled.

Profiling Using the DNS Probe

The DNS probe is used to acquire the DNS Fully Qualified Domain Name (FQDN) based on a reverse DNS lookup from the ISE Policy Service node once the IP address for an existing endpoint is learned. Therefore, the DNS probe cannot function unless the IP address is known.

The following probes can be used to determine the IP address of an endpoint:

- RADIUS Probe via Framed-IP-Address
- SNMP Probe via cdpCacheAddress
- HTTP Probe via SourceIP
- DHCP Probes via dhcp-requested-address

In addition to having a known IP address, the use of reverse DNS lookups has a number of other requirements to function:

- 1) In DNS, each endpoint requires an Address or **A** record (hostname) and a pointer or **PTR** record (IP address).
- 2) Assuming endpoints use DHCP, Dynamic DNS (DDNS) must be configured on the DHCP servers.
- 3) Depending on the DHCP server configuration, endpoints may require configuration to request dynamic updates.
- 4) ISE Policy Service nodes must be configured to resolve addresses from DNS servers that are dynamically updated.

Assuming DDNS is configured and working properly, the DNS probe can retrieve the FQDN. Otherwise, there will be no attribute added if the reverse lookup fails.

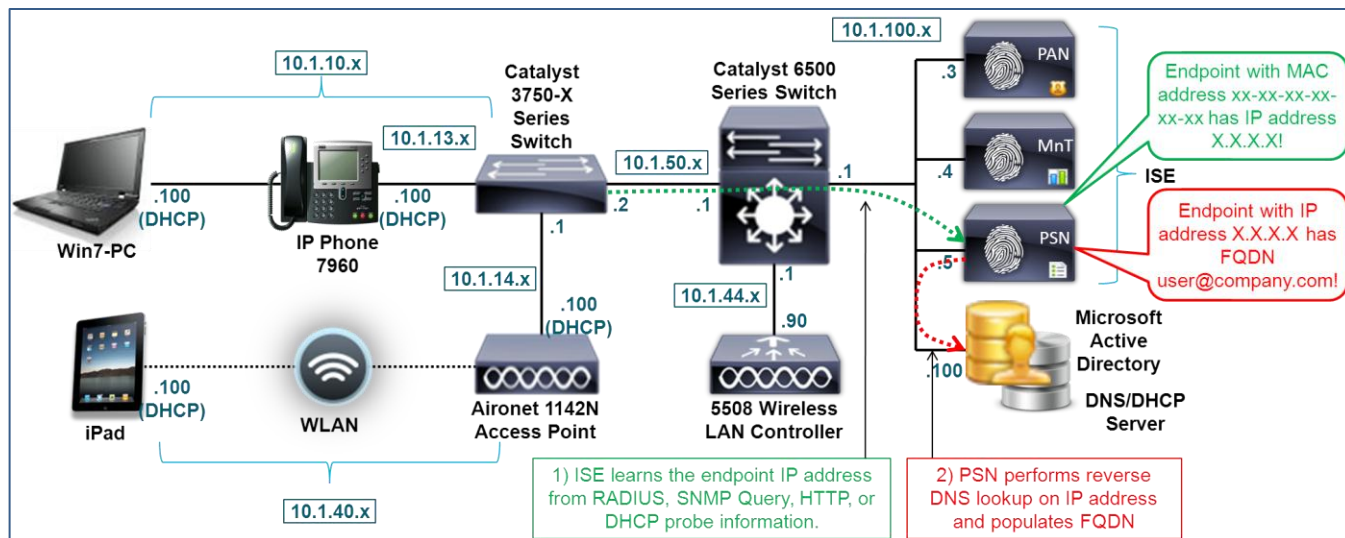
If a standard hostname, domain name, or FQDN naming convention is deployed to specific endpoints, these attributes can be used to classify them. For example, if all Windows XP clients are assigned a name such as **jsmith-winxp**, the **host-name** attribute or **client-fqdn** attribute can be used in a condition to classify Windows XP endpoints. Similarly, if the convention is to populate hostname for corporate endpoints to something like **jsmith-corp-dept**, that can be used to validate a corporate asset.

Caution must be taken to not confuse profile attributes as identity, but attributes can add a certain level of credence that the endpoint is a certain type. For example, the Authorization Policy can be used with profiling to deny full access privileges to employees where the host-name attribute of their PC (as indicated by matching Endpoint Identity group) does **not** include expected values. Note: This guide will discuss the relationship between profiles and Endpoint Identity groups in a later section.

As this discussion suggests, it may be possible to collect the FQDN or its components using other probes. Therefore, the use of the DNS probe may not be necessary if the same information, or portions of the FQDN, is already available by other means. However, DDNS can be configured to be more secure, thus making the information retrieved via a DHCP client packet less reliable than a reverse lookup to a trusted DNS server.

Figure 44 shows a sample topology using the DNS probe. As the figure shows, the ISE Policy Service node learns the IP address for an endpoint using one of multiple methods. The PSN then initiates a reverse lookup for the IP address. If response received, ISE Profiling services update the endpoint record with the FQDN attribute.

Figure 44 DNS Probe Example



Configuring the DNS Probe

To use the DNS probe, the DNS referenced by the ISE Policy Service node must be configured—either manually or dynamically using DDNS—to include host and reverse pointer records for each endpoint for which FQDN is to be retrieved.

Procedure 1 Enable DNS Probe in ISE

Step 1 Go to Administration→System→Deployment and select the Policy Service node to perform profiling from list of deployed nodes on the RHS pane.

Step 2 Select the Profiling Configuration tab.

- a. To add support for the DNS probe, select the box labeled DNS (Figure 45).

Figure 45: HTTP Probe Attributes with SPAN Example

There is no interface selection with the DNS probe as all probe queries are initiated by the ISE Policy Service node using the global routing table for reverse lookups to the locally configured DNS server(s).

- b. Leave the default value for Timeout. This value specifies the number of seconds the PSN waits for a reverse lookup response.

Step 3 Click Save to commit the changes.

Step 4 Repeat the steps in this procedure for all other Policy Service nodes configured with Profiling Services.

Procedure 2 Configure Probes to Obtain the Endpoint IP Address

Note: Configure Probes to Obtain the Endpoint IP Address In order for the DNS probe to perform a reverse DNS lookup for the FQDN, it must first learn the IP address of the endpoint from the SNMP Query, DHCP, DHCP SPAN, HTTP, or RADIUS probe. Refer to the appropriate section in this guide for details on the configuration of these probes.

Procedure 3 Configure ISE with DNS Servers for Reverse Address Lookups

When the ISE appliance is initially installed, a required configuration step is to configure one or more domain name servers.

Step 1 If required, update the list of DNS servers used by the ISE Policy Service nodes running Profiling Services using the ISE CLI command **ip name-server** in global configuration mode, as shown In Figure 46.

Figure 46 ISE Policy Service Node DNS Server Configuration Example

```
ise-pan-1/admin(config)# ip name-server ?
<A.B.C.D> Primary DNS server IP address
<A.B.C.D> DNS server 2 IP address
<A.B.C.D> DNS server 3 IP address
```

Step 2 To remove an entry, us the **no name-server** command.

Step 3 To save changes, exit global configuration mode and enter the command **copy running-config startup-config**.

Step 4 Repeat steps as required on remaining Policy Service nodes running Profiling Services.

Procedure 4 Verify DNS Probe Data

Step 1 Delete the endpoint from Administration→Identity Management→Identities→Endpoints.

Step 2 Disconnect and then reconnect the endpoint from the access device configured to support HTTP redirection to the ISE PSN.

Step 3 Go to the ISE Policy Administration node and navigate to Administration→Identity Management→Identities.

Step 4 Select Endpoints from the LHS pane.

Step 5 Find and select the MAC address of the newly connected endpoint to display the attributes captured by the HTTP probe.

The example in Figure 47 shows only the RADIUS, DHCP (IP Helper), and DNS probe enabled. RADIUS and DHCP are enabled as methods to acquire both the MAC address and IP address of the endpoint. These probes are also selected to compare similar data that can be collected using various probes.

The hash marks indicate sections where the output has been truncated for display purposes.

Figure 47 DNS Probe Attributes Example

Endpoint List > 00:50:56:A0:0B:3A

Endpoint

* MAC Address **00:50:56:A0:0B:3A**

* Policy Assignment Microsoft-Workstation ▼

Static Assignment ☐

* Identity Group Assignment Microsoft-Workstation ▼

Static Group Assignment ☐

Attribute List

ADDomain	cts.local
AcsSessionID	ise-psn-1/124936089/19986
EndPointMACAddress	00-50-56-A0-0B-3A
EndPointMatchedProfile	VMWare-Device
EndPointPolicy	Microsoft-Workstation
EndPointProfilerServer	ise-psn-1
EndPointSource	DNS Probe
ExternalGroups	cts.local/users/employees\,cts.local/users/domain users\,cts.local/builtin/users
FQDN	win7-pc.cts.local.
Framed-IP-Address	10.1.10.100
GroupsOrAttributesProcessFailure	true
IdentityGroup	Microsoft-Workstation
chaddr	00:50:56:a0:0b:3a
ciaddr	0.0.0.0
cisco-av-pair	audit-session-id=0A01320200000032046FD998, disc-cause-ext=No Reason, connect-pro
client-fqdn	00:00:00:77:69:6e:37:2d:70:63:2e:63:74:73:2e:6c:6f:63:61:6c
dhcp-class-identifier	MSFT 5.0
dhcp-client-identifier	01:00:50:56:a0:0b:3a
dhcp-message-type	DHCPREQUEST
dhcp-parameter-request-list	1, 15, 3, 6, 44, 46, 47, 31, 33, 121, 249, 43
dhcp-requested-address	10.1.10.100
flags	0x8000
giaddr	10.1.10.1
hlen	6
hops	1
host-name	win7-pc
htype	Ethernet (10Mb)
ip	10.1.10.100
op	BOOTREQUEST
secs	0
yiaddr	0.0.0.0

The key attributes highlighted in red include:

- **EndPointSource = DNS Probe**
- **FQDN = win7-pc.cts.local**

- **ip = 10.1.10.100**

EndPointSource reflects the last source of endpoint attributes.

The **FQDN** value is the result of a successful reverse lookup to the DNS server using the DNS probe.

The **ip** attribute is important to emphasize the requirement of obtaining this attribute in order for the DNS probe to function. In this example, either the RADIUS or DHCP probe could have updated this value.

Secondary attributes highlighted in orange include:

- **ADDomain = cts.local**
- **client-fqdn = 00:00:00:77:69:6e:37:2d:70:63:2e:63:74:73:2e:6c:6f:63:61:6c**
- **host-name = win7-pc**

ADDomain value is the domain name learned from RADIUS attributes using the RADIUS probe.

The **client-fqdn** attribute is the fully qualified domain name of the endpoint learned from the DHCP probe and is expressed in HEX format (Figure 48).

Figure 48 Hex to ASCII Conversion Example

The **host-name** attribute is the simple hostname of the endpoint learned from the DHCP probe.

This example illustrates that different probe attributes may supply similar information. Ultimately, the policy administrator must choose which attributes are the most useful to profiling endpoints and which probes are can best acquire this information. A comparison of probe and profiling methods will be discussed later in this guide.

Profiling Using the NetFlow Probe

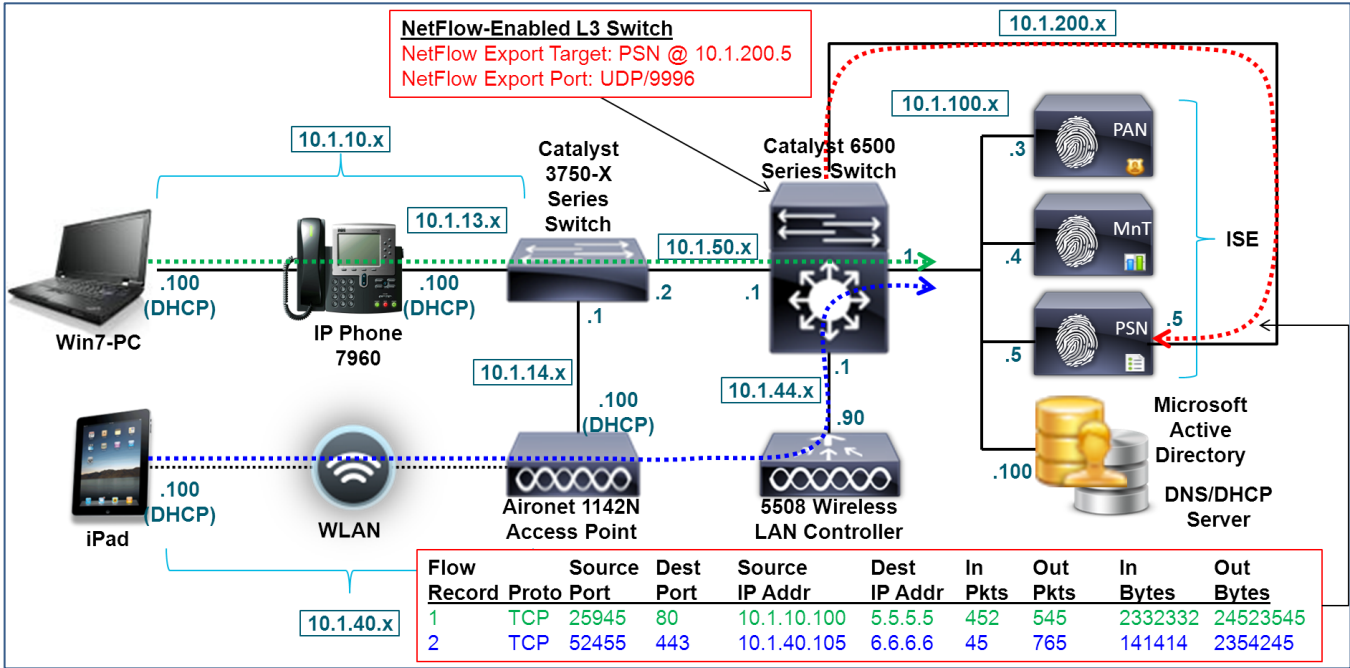
Cisco NetFlow is a form of telemetry exported from Cisco IOS Software-based routers and Layer 3 switches. NetFlow provides information about traffic passing through or directly to each NetFlow-enabled router or switch. NetFlow-enabled devices collect and export network flow data to collectors on a specified UDP port (default UDP/9996). A flow is a unidirectional stream of packets between a given source and destination and is uniquely identified by a combination of the following key fields:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Layer 3 protocol type
- ToS byte
- Input logical interface (ifIndex)

The ISE NetFlow probe is cable of receiving flow records from NetFlow Version 5 and Version 9-enabled devices to allow parsing of critical information for profiling purposes.

The sample topology in Figure 49 shows two different endpoints that have established traffic flows through a NetFlow-capable switch (Cisco Catalyst 6500 Series). The 6500 Series is configured to export the flows to the ISE Policy Services node on a dedicated interface with IP address 10.1.200.5 on UDP/9996. This interface is separate from the one that terminates user session services like RADIUS and Web Authentication.

Figure 49: NetFlow Probe Example



As you can see from the topology NetFlow must be enabled on routers or switches that are in the path of interesting traffic. For example, if traffic flows between segments within a remote branch must be collected, NetFlow deployed at a hub or central location will not offer the required visibility. Additionally, in order to collect specific traffic flows, that traffic must first be allowed on the network. Therefore, if network access is dependent on a profile that relies on NetFlow data, you need to determine how to best limit access while still allowing traffic required to complete profiling.

NetFlow Attributes

Table 4 shows some of the attributes collected by the NetFlow probe.

Table 4 NetFlow Probe Attributes

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

In ISE Profiling Services, NetFlow is typically used to identify endpoints based on the traffic they generate. Conversely, it can provide an indicator of anomalous behavior when specific endpoints appear to generate traffic that is not characteristic of that endpoint. For example, if an endpoint initially profiled as an IP phone began to suddenly start communicating to remote destinations on port 443 as reflected by NetFlow attributes, this would represent an anomalous condition and potential spoofing exploit. However, please note that the use of NetFlow with ISE Profiling Services is not to be positioned as an anti-spoofing feature or solution.

Focusing on the positive classification of endpoints, NetFlow is most useful in scenarios where general-purpose hardware may be used for mission-specific functions whereby the only information that uniquely classifies them is traffic-related. Examples of these types of devices include those used in manufacturing or healthcare industries. For example, a heart monitor in a hospital may use an embedded Windows OS or hardened Linux kernel using standard hardware technology, but

can run applications that communicate on very specific protocols, ports, and destinations. For these types of endpoints, NetFlow may be the only feasible option.

In general, it is not recommended to randomly enable NetFlow and/or use the NetFlow probe as an all-purpose profiling method. If not deployed with caution, NetFlow can have a negative impact on device resources depending on the platforms used, as well as on the NetFlow configuration and traffic volumes. NetFlow can also generate a high load on the ISE Policy Service nodes if large volumes of traffic are continuously sent from one or more sources. Unlike other ISE probes, the NetFlow probe does not support attribute filters to optimize data collection and database efficiency.

Where available on network devices, NetFlow Version 9 is recommended over Version 5 for NetFlow export to the ISE Policy Service node. Version 9 supports Flexible NetFlow and numerous enhancements for filtering flow data collected and exported to the NetFlow probe. Although sampled NetFlow can reduce overall traffic volume, sampling may not satisfy all profiling requirements because some scenarios may require that all flows be seen by the NetFlow probe.

NetFlow Probe and IP-to-MAC Address Binding Requirement

NetFlow records are based on communications between source and destination IP addresses. Since NetFlow traffic does not include the MAC address of the source or destination endpoint, it is critical that the ISE Policy Service node already have an IP-to-MAC address binding in its ARP cache table in order to properly correlate data sent to the NetFlow probe. In other words, if the endpoint is not already known to ISE by its MAC address **or** if there is not an associated IP address, profiling data learned by the NetFlow probe will be discarded since there is no endpoint to which it can apply the learned flow attributes. Consequently, you have to learn the IP-to-MAC address binding via another probe **prior** to collecting NetFlow data. Probes that can be used to provide this information include the following:

- RADIUS (via Framed-IP-Address)
- DHCP (via dhcp-requested-address)
- SNMP Query (via SNMP polling)

It should be noted that NetFlow Version 9 does support the option to include source and destination MAC addresses within the flow record, whereas version 5 does not. However, these reported MAC addresses are that of the adjacent nodes in the path, typically Layer 3 routers and switches, not the MAC address of endpoints more than one hop away. Unless the end systems are directly connected to the NetFlow device, this functionality offers little value.

Best Practice: Use of NetFlow for profiling can result in a potentially high volume of data being sent to ISE for parsing. Restrict the use of NetFlow to scenarios where other probes are insufficient. If required, NetFlow Version 9 is advocated to take advantage of filtering enhancements as found in Flexible NetFlow. Although ISE will not prevent the use of the default interface, it is highly recommended that NetFlow be exported to an ISE PSN interface dedicated to the NetFlow probe.

Configuring the NetFlow Probe

To use the NetFlow probe, network devices that are inline with traffic flows of interest must be NetFlow-capable and support NetFlow Version 5 or Version 9. A dedicated interface should be used on each ISE PSN that will be the target of NetFlow data.

Procedure 1 Enable NetFlow Probe in ISE

Step 1 Go to Administration→System→Deployment and select the Policy Service node to perform profiling from list of deployed nodes on the RHS pane.

Step 2 Select the Profiling Configuration tab and select the box to enable the NetFlow probe (Figure 50).

Step 3 Select the interface to be used for collecting NetFlow traffic. This should be a dedicated interface with a routable IP address (Figure 50)

Figure 50 NetFlow Probe Configuration

Step 4 Select the UDP port to listen for exported NetFlow. This value should be the same as that configured on the NetFlow export device. The default port is UDP/9996.

Step 5 Click Save to commit the changes.

Step 6 Repeat the steps in this procedure for all other Policy Service nodes configured with Profiling Services.

Note: Many NetFlow-capable routers and switches support only a single target for NetFlow export. Therefore, consideration must be taken into account regarding high availability. It is also recommended that all profile data for a given endpoint be received by the same Policy Service node. This may not always be possible due to network configuration and other limitations.

Procedure 2 Add the Network Device to ISE (Network Resources)

Access devices may also be capable of NetFlow but there is no specific requirement that other network devices capable of sending NetFlow to the NetFlow probe be configured as a network device in ISE.

Procedure 3 Configure ISE Policy Service Node Interface to Receive NetFlow Traffic

The NetFlow probe should be configured on a dedicated interface to receive NetFlow traffic. To configure a dedicated NetFlow interface on ISE, complete the following steps:

Step 1 Physically connect the desired interface to a network switchport.

Step 2 Access the ISE PSN console (CLI). Enable the appropriate interface and assign a valid IP address as shown in Figure 51.

Figure 51 ISE Probe Dedicated Interface Configuration Example

```
ise-psn-1/admin# conf t
Enter configuration commands, one per line. End with CNTL/Z.
ise-psn-1/admin(config)# interface GigabitEthernet 3
ise-psn-1/admin(config-GigabitEthernet)# ip address 10.1.99.100 255.255.255.0

Changing the IP may result in undesired side effects on
any installed application(s).
Are you sure you want to proceed? Y/N [N]: Y
ISE M&T Log Processor is not running.
ISE M&T Log Collector is not running.
ISE M&T Alert Process is not running.
Stopping ISE Application Server...
ISE M&T Session Database is not running.
Stopping ISE Database processes...
Starting ISE Database processes...
ISE M&T Session Database is not running.
Starting ISE Application Server...
Note: ISE Processes are initializing. Use 'show application status ise'
      CLI to verify all processes are in running state.
ise-psn-1/admin(config-GigabitEthernet)# _
```

Step 3 Verify all processes are in a running state as instructed.

Step 4 Verify the configuration of the newly configured interface and that it is enabled (NOT in shutdown) by using the **show running-config** command (Figure 52).

Figure 52 ISE Probe Dedicated Interface Verification Example

```
ise-psn-1/admin# show running-config
Generating configuration...
?
hostname ise-psn-1
?
ip domain-name cts.local
?
interface GigabitEthernet 0
  ip address 10.1.100.5 255.255.255.0
  ipv6 address autoconfig
?
interface GigabitEthernet 1
  shutdown
  ipv6 address autoconfig
?
interface GigabitEthernet 2
  shutdown
  ipv6 address autoconfig
?
interface GigabitEthernet 3
  ip address 10.1.99.100 255.255.255.0
  ipv6 address autoconfig
?
ip name-server 10.1.100.100
--More--
```

Step 5 Verify connectivity to the new probe interface by sending an ICMP ping from a network device that needs to export NetFlow data.

Step 6 Save changes using the CLI command **copy running-config startup-config**.

Step 7 Physically connect the desired interface to the appropriate SPAN destination port or network tap interface.

Note: For Policy Service Nodes Running on VMware Appliance

To use a dedicated interface for profiling, it is assumed that additional virtual interfaces were configured for the virtual appliance. If not completed at the time of install, it will be necessary to shut down the ISE node and update the hardware and networking configuration of the ESX appliance for the required interface(s) before continuing with the ISE configuration

Procedure 4 Configure NetFlow-Capable Switch/Router to Export NetFlow to the ISE PSN

NetFlow configuration is specific to the NetFlow-capable device. This procedure includes an example configuration for a Catalyst 6500 Series switch.

Step 1 Under global configuration mode, enable NetFlow, configure NetFlow Version 9 support, the interface IP address from which to source NetFlow data, and the Policy Service node to export data. Note the specification of the ISE default port of UDP 9996.

```
mls netflow interface
mls flow ip interface-full
mls nde sender
mls nde interface
ip flow-cache timeout active 1
ip flow-export source Vlan100
ip flow-export version 9
```

```
ip flow-export destination 10.1.100.5 9996
```

Note: In the preceding example, the Catalyst 6500 Series Switch has a Supervisor 720 where the Policy Feature Card (PFC) performs hardware-based NetFlow and flows punted to Multilayer Switch Feature Card (MSFC) are performed in software. The PFC must be configured to perform NetFlow Data Export (NDE) using the **mls nde sender** command.

Step 2 Optionally configure capture filters, as follows:

```
ip flow-capture ttl
ip flow-capture vlan-id
ip flow-capture ip-id
ip flow-capture mac-addresses
```

Step 3 Enable NetFlow on the ingress interfaces (endpoint-facing interfaces), as follows:

```
interface GigabitEthernet 2/47
description To cat3750x
ip address 10.1.50.1 255.255.255.0
ip flow ingress
!
interface Vlan40
description EMPLOYEE
ip address 10.1.40.1 255.255.255.0
ip helper-address 10.1.100.100
ip helper-address 10.1.100.5
ip flow ingress
!
interface Vlan41
description GUEST
ip address 10.1.41.1 255.255.255.0
ip helper-address 10.1.100.100
ip helper-address 10.1.100.5
ip flow ingress
```

IP Helper commands are also shown to highlight the configuration to support the DHCP probe, which is used to obtain IP-to-MAC address binding information. This allows the NetFlow probe to apply attributes based on the matching IP attribute.

Figure 53 illustrates the interfaces where NetFlow is applied as well as the destination for NetFlow Data Export (NDE). The goal is to capture traffic from wired endpoints connecting through the Cisco Catalyst 3750-X Series Switch as well wireless endpoints connecting through the Cisco 5500 Series Wireless LAN Controller.

The diagram illustrates a network topology with the following components and connections:

- Win7-PC:** Connected to the Catalyst 3750-X Series Switch via a blue line. IP address: 10.1.10.x. Subnet: .100 (DHCP).
- IP Phone 7960:** Connected to the Catalyst 3750-X Series Switch via a blue line. IP address: 10.1.13.x. Subnet: .100 (DHCP).
- iPad:** Connected to the WLAN access point via a blue line. IP address: .100 (DHCP).
- WLAN:** Connected to the Aironet 1142N Access Point via a blue line. Subnet: 10.1.40.x.
- Catalyst 3750-X Series Switch:** Connected to the Catalyst 6500 Series Switch via a blue line. IP address: 10.1.14.x. Subnet: .100 (DHCP).
- Aironet 1142N Access Point:** Connected to the Catalyst 6500 Series Switch via a blue line. IP address: 10.1.15.x. Subnet: .2.
- 5508 Wireless LAN Controller:** Connected to the Catalyst 6500 Series Switch via a blue line. IP address: 10.1.44.x. Subnet: .90.
- Catalyst 6500 Series Switch:** The central switch, connected to the ISE and Microsoft Active Directory/DNS/DHCP Server via a red line. IP address: 10.1.200.x. Subnet: .3.
- ISE (Identity Services Engine):** Contains three components: PAN, MnT, and PSN. The PSN component is connected to the Microsoft Active Directory/DNS/DHCP Server via a red line. IP address: 10.1.100.x. Subnet: .4.
- Microsoft Active Directory/DNS/DHCP Server:** Connected to the Catalyst 6500 Series Switch via a red line. IP address: 10.1.100.x. Subnet: .5.

IP Flow Ingress and Egress:

- Interface GigabitEthernet 2/47:** ip flow ingress (red line).
- Interface VLAN 40:** ip flow ingress (red line).
- ip flow-export destination 10.1.100.5 9996:** (red line).

Procedure 5 Verify NetFlow Probe Data

Step 1 Delete the endpoint from Administration→Identity Management→Identities→Endpoints.

Step 2 Disconnect and then reconnect the endpoint from the access device.

Step 3 Login from the endpoint and attempt generate sample traffic such as attempting web access using a browser.

Step 4 Go to the ISE Policy Administration node and navigate to Administration→Identity Management→Identities.

Step 5 Select Endpoints from the LHS pane.

Step 6 Find and select the MAC address of the newly connected endpoint to display the attributes captured by the NetFlow probe (Figure 54).

The example in Figure 54 highlights the attributes collected using NetFlow export. Additionally, the RADIUS and DHCP probes were enabled to ensure that IP-to-MAC bindings were acquired to support the NetFlow probe.

Figure 54 NetFlow Attributes Example

Endpoint List > 00:50:56:A0:0B:3A

Endpoint

* MAC Address **00:50:56:A0:0B:3A**

* Policy Assignment Windows7-Workstation ▼

Static Assignment ☐

* Identity Group Assignment Microsoft-Workstation ▼

Static Group Assignment ☐

Attribute List

EndPointProfilerServer	ise-psn-1
EndPointSource	NETFLOW Probe
ExternalGroups	cts.local/users/contractors\,cts.local/users/domain users\,cts.local/builtin/users
FIRST_SWITCHED	137839523
FLOW_SAMPLER_ID	0
FQDN	win7-pc.cts.local.
FragmentOffset	0
Framed-IP-Address	10.1.10.100
GroupsOrAttributesProcessFailure	true
INPUT_SNMP	49
IN_BYTES	1869
IN_PKTS	6
IPV4_DST_ADDR	173.37.144.208
IPV4_NEXT_HOP	172.16.1.1
IPV4_SRC_ADDR	10.1.10.100
IdentityGroup	Microsoft-Workstation
IdentityPolicyMatchedRule	Default
L4_DST_PORT	80
L4_SRC_PORT	53149
LAST_SWITCHED	137839715
Location	Location#All Locations#North_America#RTP
MACAddress	00:50:56:A0:0B:3A
MatchedPolicy	Windows7-Workstation
MessageCode	3002
NAS-IP-Address	10.1.50.2
NAS-Port	50101
NAS-Port-Id	GigabitEthernet1/0/1
NAS-Port-Type	Ethernet
NetworkDeviceGroups	Device Type#All Device Types#Wired, Location#All Locations#North_America#RTP
NetworkDeviceName	cat3750x
OUI	VMware, Inc.
OUTPUT_SNMP	52
PROTOCOL	6

The key attributes highlighted in red include:

- **EndPointSource** = NetFlow Probe
- **IPV4_DST_ADDR** = 173.37.144.208 (cisco.com)

- **IPV4_SRC_ADDR** = 10.1.10.100 (win7-pc)
- **L4_DST_PORT** = 80 (HTTP)
- **L4_SRC_PORT** = 53149
- **PROTOCOL** = 6 (TCP)

If flow capture statements are used, you may see the following additional attributes:

- **DST_VLAN/SRC_VLAN**
- **IN_SRC_MAC/OUT_DST_MAC**
- **MAX_TTL/MIN_TTL**

Step 7 To verify that NetFlow data is being collected, you can use the **show ip cache flow** and the **show mls netflow ip** commands. The following example uses the **show ip cache flow** command:

```
cat6503#show ip cache flow
```

Displaying software-switched flow entries on the MSFC in Module 1:

IP packet size distribution (348128 total packets):

1-32	64	96	128	160	192	224	256	288	320	352	384	416	448	480
.548	.342	.077	.005	.000	.000	.000	.000	.000	.000	.015	.000	.000	.000	.000
512	544	576	1024	1536	2048	2560	3072	3584	4096	4608				
.000	.000	.007	.000	.000	.000	.000	.000	.000	.000	.000				

IP Flow Switching Cache, 278544 bytes
 2 active, 4094 inactive, 15760 added
 251284 aged polls, 0 flow alloc failures
 Active flows timeout in 1 minutes
 Inactive flows timeout in 15 seconds

IP Sub Flow Cache, 33992 bytes
 6 active, 1018 inactive, 47280 added, 15760 added to flow
 0 alloc failures, 2775 force free
 1 chunk, 24 chunks added
 last clearing of statistics never

Protocol	Total Flows	Flows /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active(Sec) /Flow	Idle(Sec) /Flow
TCP-Telnet	44	0.0	91	42	0.0	14.4	7.8
TCP-WWW	1361	0.0	22	45	0.0	0.0	14.2
TCP-other	1602	0.0	25	51	0.0	0.1	13.6
UDP-DNS	128	0.0	1	70	0.0	0.0	15.4
UDP-NTP	1375	0.0	1	76	0.0	0.0	15.5
UDP-other	2880	0.0	3	338	0.0	3.8	15.4
ICMP	6985	0.0	34	30	0.0	0.4	13.4
IP-other	1383	0.0	13	65	0.0	58.3	2.0
Total:	15758	0.0	22	46	0.0	6.0	13.0

SrcIf	SrcIPaddress	DstIf	DstIPaddress	Pr	SrcP	DstP	Pkts
Gi2/47	10.1.50.2	Null	224.0.0.10	58	0000	0000	4
Gi2/47	10.1.13.1	Null	10.1.100.7	11	0043	0043	3

Displaying hardware-switched flow entries in the PFC (Active) Module 1:

SrcIf	SrcIPaddress	DstIf	DstIPaddress	Pr	SrcP	DstP	Pkts
Gi2/47	10.1.50.1	Gi2/47	10.1.50.2	58	0000	0000	0
Gi2/47	10.1.50.2	---	10.1.100.1	11	007B	007B	0
Gi2/47	10.1.50.2	---	10.1.50.1	58	0000	0000	0
Gi2/47	10.1.100.1	Gi2/47	10.1.50.2	11	007B	007B	0
Gi2/47	10.1.50.2	Vl100	10.1.100.5	11	CC9B	00A2	15
Gi2/47	10.1.13.1	Vl100	10.1.100.100	11	0043	0043	124
Gi2/47	10.1.13.1	Vl100	10.1.100.5	11	0043	0043	124
Gi2/47	10.1.13.1	Vl100	10.1.100.6	11	0043	0043	124
Gi2/47	10.1.50.2	---	224.0.0.10	58	0000	0000	84
Vl40	10.1.40.1	---	224.0.0.10	58	0000	0000	0
Gi2/47	10.1.50.2	Vl100	10.1.100.4	11	C8D5	5022	30
Gi2/47	10.1.13.1	---	10.1.100.7	11	0043	0043	0
Gi2/47	10.1.10.100	Vl100	10.1.100.100	11	CA72	0035	1
Gi2/47	10.1.50.2	Vl100	10.1.100.5	11	066E	0715	128

Vl41	10.1.41.1	---	224.0.0.10	58 0000 0000	0
Gi2/47	10.1.50.2	Vl100	10.1.100.5	11 06A4 7195	2
Gi2/47	10.1.50.2	Vl100	10.1.100.6	11 E6D7 00A2	15
Gi2/47	10.1.50.2	---	10.1.100.7	11 C748 00A2	0
Gi2/47	10.1.50.2	Vl100	10.1.100.5	11 066D 0714	6
Gi2/47	10.1.10.100	Vl100	10.1.100.100	11 E5CC 0035	1
Gi2/47	10.1.10.100	Vl100	10.1.100.100	11 DA8B 0035	1
Gi2/47	10.1.10.100	Vl100	10.1.100.100	11 C114 0035	1
Gi2/47	10.1.10.100	Vl100	10.1.100.100	11 FC03 0035	1
Gi2/47	10.1.10.100	Vl100	10.1.100.100	11 D295 0035	1
Gi2/47	10.1.10.100	Vl100	10.1.100.100	11 ED48 0035	1
Gi2/47	10.1.10.100	Vl100	10.1.100.100	11 E7E8 0035	1
Gi2/47	10.1.10.100	Vl100	10.1.100.100	11 D770 0035	1
Gi2/47	10.1.10.100	Vl100	10.1.100.100	11 D5AB 0035	1
--	0.0.0.0	---	0.0.0.0	00 0000 0000	31K

The following example uses **show mls netflow ip**:

```
at6503#show mls netflow ip
Displaying Netflow entries in Active Supervisor EARL in module 1
DstIP      SrcIP      Prot:SrcPort:DstPort  Src i/f      :AdjPtrPkts  Bytes
Age   LastSeen  Attributes
-----
10.1.50.2   10.1.100.1   udp :ntp      :ntp      Gi2/47      :0x00        0
43    20:26:48  L2 - Dynamic
10.1.44.90  10.1.14.100  udp :16792    :5246     Gi2/47      :0x03        359
35    20:27:26  L3 - Dynamic
10.1.100.100 10.1.13.1   udp :67       :67       Gi2/47      :0x04        1846
32    20:27:30  L3 - Dynamic
10.1.100.5   10.1.50.2   udp :52379    :162      Gi2/47      :0x015       2734
335   20:23:02  L3 - Dynamic
10.1.100.4   10.1.50.2   udp :51413    :20514    Gi2/47      :0x030       5286
334   20:23:58  L3 - Dynamic
10.1.100.5   10.1.50.2   udp :1646     :1813     Gi2/47      :0x04        2680
32    20:27:30  L3 - Dynamic
10.1.100.100 10.1.10.100  udp :51826    :dns      Gi2/47      :0x01        61
211   20:24:00  L3 - Dynamic
10.1.44.90  10.1.14.100  udp :16792    :5247     Gi2/47      :0x06        901
30    20:27:30  L3 - Dynamic
224.0.0.10  10.1.41.1   88  :0         :0         Vl41        :0x00        0
426   20:27:27  Multicast
10.1.100.5   10.1.50.2   udp :1700     :29077    Gi2/47      :0x02        132
335   20:23:56  L3 - Dynamic
10.1.100.6   10.1.50.2   udp :59095    :162      Gi2/47      :0x015       2734
335   20:23:02  L3 - Dynamic
10.1.100.7   10.1.50.2   udp :51016    :162      Gi2/47      :0x00        0
335   20:23:02  L3 - Dynamic
10.1.100.5   10.1.50.2   udp :1645     :1812     Gi2/47      :0x06        1365
270   20:23:56  L3 - Dynamic
10.1.100.100 10.1.10.100  udp :54699    :dns      Gi2/47      :0x01        64
211   20:24:00  L3 - Dynamic
10.1.100.1   10.1.50.2   udp :ntp      :ntp      Gi2/47      :0x00        0
43    20:26:48  L3 - Dynamic
17.172.232.209 10.1.40.101  tcp :61858    :443      Vl40        :0x02        173
17    20:27:14  L3 - Dynamic
17.172.232.209 10.1.40.101  tcp :61858    :443      Vl40        :0x00        0
17    20:27:14  L2 - Dynamic
10.1.40.101  17.172.232.209  tcp :443      :61858    Vl40        :0x00        0
17    20:27:14  L2 - Dynamic
0.0.0.0     0.0.0.0     0   :0         :0         --         :0x032283    20941051
1573  20:27:31  L3 - Dynamic
```

Step 8 To verify the NetFlow export configuration and that flows are being sent to the ISE Policy Service node, use the **show ip flow export** command, as follows:

```
cat6503# sh ip flow export
Flow export v9 is enabled for main cache
Export source and destination details :
VRF ID : Default
Source(1) 10.1.100.1 (Vlan100)
Destination(1) 10.1.99.5 (9996)
Version 9 flow records
```

```

20408 flows exported in 7635 udp datagrams
0 flows failed due to lack of export packet
0 export packets were sent up to process level
0 export packets were dropped due to no fib
0 export packets were dropped due to adjacency issues
0 export packets were dropped due to fragmentation failures
0 export packets were dropped due to encapsulation fixup failures
0 export packets were dropped enqueueing for the RP
0 export packets were dropped due to IPC rate limiting
0 export packets were dropped due to Card not being able to export

```

Profiling Using Network Scan (NMAP) Probe

The Network Scan probe is based on an embedded version of the open-source Network Mapper utility. Network Mapper (NMAP) is designed to scan large networks for connected endpoints, and then perform scans on individual hosts to detect their operating system (OS), OS version, and services (application names and versions).

Other ISE probes are considered “passive” in the sense that they do not directly interrogate the endpoint itself but rather rely on indirect methods of data collection such as parsing data generated by the device or from other network devices. The Network Scan probe is considered an “active” assessment mechanism since it communicates directly with the endpoint to obtain information from the source.

NMAP Probe Scan Operations

When the NMAP probe does a scan, it can perform one or more of the following NMAP operations:

- Operating System Scan
- SNMP Port Scan
- Common Ports Scan

The operating system (OS) scan is used to detect the OS and version of endpoint. This is an intensive operation.

The SNMP Port Scan tries to detect if UDP port 161 (SNMP daemon) and 162 (SNMP Trap) are open. If so, an SNMP query is initiated to the endpoint using a community string of **public** to collect additional information about the endpoint from the System MIB and others. This probe has proven especially useful in endpoints like network printers that have SNMP enabled by default with the default community string **public**.

Note: The NMAP probe can only use the default community string **public** to directly query endpoints. This value is currently not configurable.

This should not be confused with the SNMP Query probe which queries network devices, not endpoints, and has configurable SNMP settings under the Network Device settings.

The Common Ports Scan performs a scan of 15 common TCP and UDP ports, as shown in Table 5:

Table 5 NMAP Probe Common Ports Scan: TCP and UDP Ports

TCP Ports		UDP Ports	
Port	Service	Port	Service
21/tcp	ftp	53/udp	domain
22/tcp	ssh	67/udp	dhcp
23/tcp	telnet	68/udp	dhcp
25/tcp	smtp	123/udp	ntp
53/tcp	domain	135/udp	msrpc
80/tcp	http	137/udp	netbios-ns
110/tcp	pop3	138/udp	netbios-dgm
135/tcp	msrpc	139/udp	netbios-ssn

139/tcp	netbios-ssn		161/udp	snmp
143/tcp	imap		445/udp	microsoft-ds
443/tcp	https		500/udp	isakmp
445/tcp	microsoft-ds		520/udp	route
3306/tcp	mysql		631/udp	ipp
3389/tcp	ms-term-serv		1434/udp	ms-sql-m
8080/tcp	http-proxy		1900/udp	upnp

Note: The list of common ports scanned is not currently configurable.

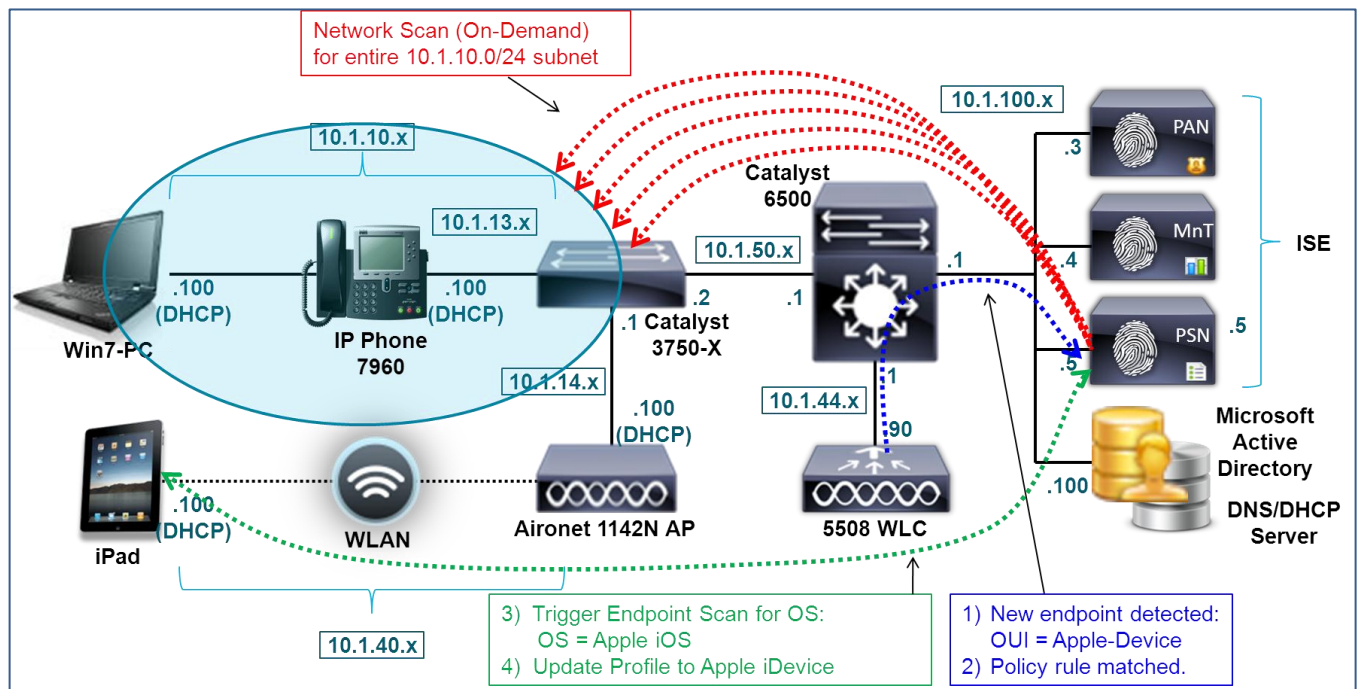
Administrators may choose to classify and secure endpoints differently based on services they run. For example, a Windows server running web services may require a specific authorization policy applied (dACL, VLAN, SGT) to ensure it is protected from non-HTTP requests. Conversely, a Windows or Linux workstation running a web server may need to be denied access or quarantined using similar authorization methods.

The NMAP probe can be initiated using one of two methods:

- Network Scan
- Endpoint Scan

The sample topology in Figure 55 depicts a Network Scan being initiated across the 10.1.10/24 subnet (highlighted in red).

Figure 55 NMAP Probe Example



NMAP Probe Network Scan

The Network Scan is an on-demand scan against one or multiple network endpoints. It is manually started by an admin user from the ISE Administration node. The probe does not even need to be enabled on the Policy Service node to run a manual Network Scan. The admin user simply specifies the IP subnet to scan and clicks the Run Scan button.

A Network Scan performs both an SNMP Port and Operating System scan. Since scans of large networks can be time consuming and add a load to the Policy Service node, it is recommended that the scope of the subnet be selected carefully. After initiating the scan, the admin user can click a link to navigate to a page where results are displayed.

NMAP Probe Endpoint Scan

An Endpoint Scan is a triggered scan of a single endpoint. It is automatically initiated based on a matching rule in the Profiling Policy. In order for the triggered scan to occur, the endpoint must match both the profile policy as well as the specified condition to which a Network Scan Action is assigned. The Network Scan Action is configurable per profile rule and defines the specific scan operations to be taken.

By default, there are three NMAP Actions which can be assigned as responses to a matching profile condition:

- **CommonPortsAndOS-scan** (Common Ports + OS scan)
- **OS-scan** (OS scan only)
- **SNMPPortsAndOS-scan** (SNMP Ports + OS scan)

The sample topology in Figure 55 depicts this process. A new endpoint is detected as a result of a recent probe event (shown in blue). Based on the profile data collected, the endpoint is known to be an Apple device based on OUI from its MAC address, but it is not known if the endpoint is a Mac OS X workstation, Apple iDevice, or other Apple endpoint. A policy rule is matched that triggers a pointed OS scan against the Apple device (shown in green). As a result, it is learned that the endpoint is running Apple iOS and its profile is updated to that of a mobile Apple device.

Endpoints that match the Unknown profile are automatically scanned using both an SNMP port and OS scan. This is not a configurable response. It is intended to allow ISE Profiling to quickly gain more information about any endpoint that is discovered but not profiled.

Note: Some endpoints have personal firewalls or other agent software enabled, which blocks attempts to scan the endpoint. These endpoints will yield little or no NMAP data. Additionally, any endpoints that have restricted network access may not be able to receive or reply to NMAP operations.

NMAP Probe and IP-to-MAC Address Binding Requirement

NMAP is based on a known IP address. If the NMAP probe collects attributes for an endpoint but cannot correlate that to a specific MAC address, that data is discarded. If the Policy Service node is on the same segment as the endpoint it is scanning, it can learn the IP-to-MAC address binding from its local ARP cache and add the endpoint directly into the Internal Endpoints database. Consequently, it is required to learn the IP-to-MAC address binding via another probe **prior** to collecting NMAP probe data. Probes that can be used to provide this information include the following:

- RADIUS (via Framed-IP-Address)
- DHCP (via dhcp-requested-address)
- SNMP Query (via SNMP polling)

Best Practice: During the discovery phase of an ISE deployment when ISE is not yet authenticating endpoints, the Network Scan can be run against larger network blocks to scan and detect endpoints along with any relevant OS and endpoint information. It is recommended that the SNMP Query probe also be enabled during this phase for all network devices that store endpoint ARP table information. This will allow discovery of endpoint MAC and IP addresses, including statically addressed endpoints. This, in turn, will support NMAP probe collection, as the PSN should now have MAC addresses for each IP address discovered during the Network Scan.

Configuring the NMAP Probe

As just described, there are two methods to run the NMAP probe—either as a manual, on-demand Network Scan or as an automatically triggered scan event for a single endpoint. The procedures to use each method will be covered separately.

Procedure 1 Run a Network Scan

Step 1 Go to Administration→System→Deployment and select the Policy Service node that will perform the Network Scan from list of deployed nodes on the RHS pane.

Step 2 Select the Profiling Configuration tab.

Step 3 To run a Network Scan, select the Network Scan (NMAP) option to expand its contents (Figure 56).

Figure 56: NMAP Probe

☐ **Network Scan (NMAP)**

Description

Manual Scan Subnet

[Click to see latest scan results](#)

Note: As shown in Figure 56, enabling the probe is not a requirement to perform a manual Network Scan.

Step 4 Enter the IP subnet address and mask to scan in the format shown in the example. The example shows that a Class C subnet (10.1.10.0) is entered along with the appropriate number of mask bits (24) for a Class C subnet.

Other subnet sizes can be selected, but consideration must be given to the scope of network and number of endpoints covered by the selection to reduce overall time and load to execute the scan.

Step 5 Click Run Scan.

Step 6 To cancel an active scan, click Cancel Scan. Otherwise select “Click to see latest scan results” to navigate directly to the Administration→Identity Management→Identities page. Even though you have navigated away from the page, scanning will continue until completed.

Step 7 From the Identities page select **Latest Network Scan Results** from the LHS pane. Depending on the progress of the scan, endpoints with positive scan results should appear on the RHS pane (Figure 57).

Figure 57 NMAP Network Scan Results Example

Latest Network Scan Results Endpoints				
Edit				
<input type="checkbox"/>	Endpoint Profile ▲	MAC Address	Profiler Server	Static Assignment
<input type="checkbox"/>	Cisco-Device	1C:DF:0F:8F:60:42	ise-psn-1	false
<input type="checkbox"/>	VMWare-Device	00:50:56:A0:0B:3A	ise-psn-1	false

Step 8 Click endpoint entries by MAC address to view the results, as shown in Figure 58. (The blue hash lines in Figure 58 indicate sections that have been removed for display purposes.)

Figure 58 NMAP Probe Attributes from Network Scan Example

Endpoint List > 00:50:56:A0:0B:3A

Endpoint

* MAC Address **00:50:56:A0:0B:3A**

* Policy Assignment **VMWare-Device**

Static Assignment ☐

* Identity Group Assignment **Profiled**

Static Group Assignment ☐

Attribute List

EndPointMACAddress	00-50-56-A0-0B-3A
EndPointMatchedProfile	VMWare-Device
EndPointPolicy	VMWare-Device
EndPointProfilerServer	ise-psn-1
EndPointSource	NMAP Probe
NmapSubnetScanID	4
OUI	VMware, Inc.
ip	10.1.10.100
operating-system	Microsoft Windows general purpose 2008

The selected endpoint is a Windows 7 PC. As you can see from the output of the manual Network Scan, NMAP has detected the general OS class (Windows 7 and Windows 2008 share common code bases), but insufficient information is available to further classify the endpoint beyond the current VMware profile that is based on a match to an OUI condition. The **EndPointSource** is shown as **NMAP Probe**. The ScanID refers to the ID assigned to the manual Network Scan event.

Note: It was necessary to disable the default Windows 7 Firewall settings to allow a successful scan from the NMAP probe.

Procedure 2 Configure the NMAP Probe for Endpoint Scanning

Step 1 Go to Administration→System→Deployment and select the Policy Service node to perform profiling from list of deployed nodes on the RHS pane.

Step 2 Select the Profiling Configuration tab and select the box labeled Network Scan (NMAP) (Figure 59).

Figure 59 NMAP Probe Configuration

☒ **Network Scan (NMAP)**

Description **NMAP**

Manual Scan Subnet

Run Scan **Cancel Scan**

[Click to see latest scan results](#)

Step 3 Click Save to commit the changes.




Step 4 Repeat the steps in this procedure for all other Policy Service nodes configured with Profiling Services.

Procedure 3 Review Network Scan (NMAP) Actions

Step 1 Go to Policy→Policy Elements→Results and select Profiling→Network Scan (NMAP) Actions from the LHS pane.

Step 2 Review the default NMAP Actions (Figure 60).

Figure 60 NMAP Scan Actions

Network Scan Actions	
 Edit	 Add
 Delete	
<input type="checkbox"/> Network Scan (NMAP) Action Name	Description
<input type="checkbox"/> CommonPortsAndOS-scan	Perform operating system and common ports detection (not SNMP).
<input type="checkbox"/> OS-scan	Perform operating system detection.
<input type="checkbox"/> SNMPPortsAndOS-scan	Perform operating system and SNMP ports detection. Used for 'Unknown' endpoints.

Additional NMAP Actions can be defined if required, although the most common options have been configured. For example, a new Scan Action named **CommonPorts** or **SNMPPorts** can be created to perform only a scan of Common Ports or SNMP Ports as part of a triggered response.

Procedure 4 Review the Configuration to Assign an NMAP Action to a Profiling Policy Condition

Step 1 Go to Policy→Profiling and select the Apple-Device profile from the list on the RHS pane (Figure 61).

Figure 61 Profiling Policy with NMAP Scan Action Example

Profiler Policy List > Apple-Device

Profiler Policy

* Name: Apple-Device Description: Generic policy for all Apple devices

Policy Enabled: ☒

* Minimum Certainty Factor: 10 (Valid Range 1 to 65535)

* Exception Action: NONE

* Network Scan (NMAP) Action: OS-scan

☐ Create Matching Identity Group

☒ Use Hierarchy

Parent Policy: ***NONE***

Rules

If Condition: Apple-DeviceRule1-SCAN Then: Take Network Scan Action

If Condition: Apple-DeviceRule1Check1 Then: Certainty Factor Increases 10

Step 2 The Apple-Device profile has two conditions. Click to the right of the second condition name to review the contents of the rule entry (Figure 62).

Figure 62 Profiling Policy Rule for NMAP Scan Example 1

Rules

If Condition: Apple-DeviceRule1-SCAN

If Condition: Apple-DeviceRule1Check1

Conditions Details

Name: Apple-DeviceRule1Check1

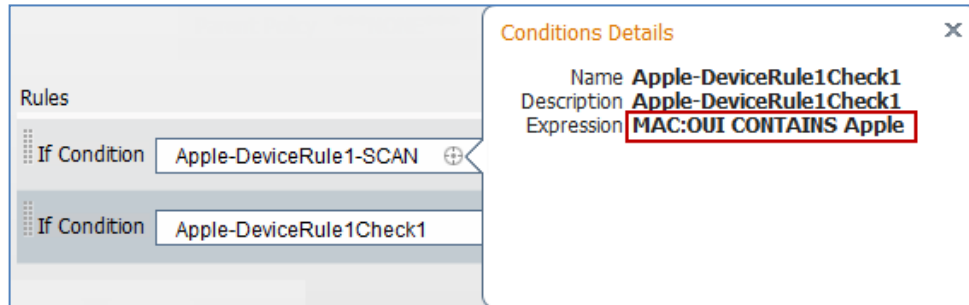
Description: Apple-DeviceRule1Check1

Expression: MAC:OUI CONTAINS Apple

This rule is used to match endpoints to this profile by increasing its certainty factor (CF). The condition matches if the OUI from MAC address matches “Apple”.

Step 3 Click to the right of the first condition name to review its contents (Figure 63).

Figure 63 Profiling Policy Rule for NMAP Scan Example 2



This rule is used to trigger an endpoint scan. The first condition is the same condition as used in the second rule. Therefore, any endpoint matching this profile based on the second condition will automatically match the first rule and trigger the selected Network Scan Action, which is OS-scan.

Individual rule entries can be added or removed by clicking the gear icon to the right of the existing rule table.

Step 4 When you finish reviewing or making changes, click Save at the bottom of the page to commit changes.

The intent of this procedure is to review how Network Scan Actions can be applied to a profile based on matching conditions. Profiling Policy configuration will be discussed in greater detail in the section [Configuring Profiling Policies](#).

Procedure 5 Verify NMAP Probe Data Based on a Triggered Endpoint Scan Action

Step 1 Delete the endpoint from Administration→Identity Management→Identities→Endpoints.

Step 2 Disconnect and then reconnect the endpoint from the access device configured to support profiling using the NMAP probe.

Step 3 Go to the ISE Policy Administration node and navigate to Administration→Identity Management→Identities.

Step 4 Select Endpoints from the LHS pane.

Step 5 Find and select the MAC address of the newly connected endpoint to display the attributes captured by the HTTP probe.

In the example in Figure 64, only the RADIUS and DHCP (IP Helper) probes are enabled in addition to the NMAP probe. These additional probes are used to discover new endpoints and to add them to the Internal Endpoints database along with appropriate MAC address and IP address information. This will help to ensure NMAP probe data is properly applied and not discarded.

Figure 64 NMAP Probe Attributes from Endpoint Scan Example 1

Endpoint List > 7C:6D:62:E3:D5:05

Endpoint

* MAC Address **7C:6D:62:E3:D5:05**

* Policy Assignment Apple-Device ▼

Static Assignment ☐

* Identity Group Assignment Profiled ▼

Static Group Assignment ☐

Attribute List

MACAddress	7C:6D:62:E3:D5:05
MatchedPolicy	Apple-Device
MessageCode	3001
NAS-IP-Address	10.1.44.90
NAS-Identifier	Cisco_0c:99:a4
NAS-Port	1
NAS-Port-Type	Wireless - IEEE 802.11
NetworkDeviceGroups	Device Type#All Device Types#Wireless, Location#All Locations#l
NetworkDeviceName	wlc5508
NmapScanCount	1
OUI	Apple, Inc

Step 6 The truncated output shows that an initial scan has been run against this endpoint (**NmapScanCount**), but the profile assignment to Apple is still based on the OUI. The scan is triggered based on the matching profile conditions for Apple-Device.

Step 7 After a brief period, the OS scan should complete. Exit and reselect the same endpoint to review any updated profiling attributes (Figure 65).

The key attributes highlighted include:

- **EndPointPolicy**
- **LastNmapScanTime**
- **NmapScanCount**
- **OUI**
- **operating-system**

Figure 65 NMAP Probe Attributes from Endpoint Scan Example 2

Endpoint List > 7C:6D:62:E3:D5:05

Endpoint

* MAC Address 7C:6D:62:E3:D5:05

* Policy Assignment Apple-iDevice

Static Assignment

* Identity Group Assignment Apple-iDevice

Static Group Assignment

Attribute List

EndPointMACAddress	7C-6D-62-E3-D5-05
EndPointMatchedProfile	Apple-iDevice
EndPointPolicy	Apple-iDevice
EndPointProfilerServer	ise-psn-1
EndPointSource	RADIUS Probe
ExternalGroups	cts.local/users/employees\,cts.local/users/domain users\
Framed-IP-Address	10.1.40.101
IdentityAccessRestricted	false
IdentityGroup	Apple-iDevice
IdentityPolicyMatchedRule	Default
LastNmapScanTime	2012-May-03 05:59:56 UTC
Location	Location#All Locations#North_America#RTP
MACAddress	7C:6D:62:E3:D5:05
MatchedPolicy	Apple-iDevice
NAS-Port-Type	Wireless - IEEE 802.11
NetworkDeviceGroups	Device Type#All Device Types#Wireless, Location#All L
NetworkDeviceName	wlc5508
NmapScanCount	2
OUI	Apple, Inc
PolicyVersion	22
PostureAssessmentStatus	NotApplicable
host-name	Apple-1pad
htype	Ethernet (10Mb)
ip	10.1.40.101
op	BOOTREQUEST
operating-system	Apple iOS general purpose 4.X (accuracy 93%)
secs	0

In this example, it is apparent that the NMAP scan completed. The **EndPointSource** attribute indicates that RADIUS made the last updates. This is possible, as the value will constantly change as different sources supply profiling data.

The **LastNmapScanTime** and **NmapScanCount** attributes are not really critical to device classification, but are highlighted to show attributes added by the NMAP probe.

The **OUI** attribute is Apple but now the profile assigned is that of Apple-iDevice instead of the more generic Apple-Device. This is due to a match on the triggered NMAP scan result, which revealed that the endpoint OS is Apple iOS. If you review the contents of the Apple-iDevice profile under Policy→Profiling, you can see that this profile can match on one of two conditions based on NMAP OS scan results (Figure 66).

Figure 66 Profiling Policy for Apple-iDevice

Profiler Policy List > **Apple-iDevice**

Profiler Policy

* Name: Description:

Policy Enabled: ☒

* Minimum Certainty Factor: (Valid Range 1 to 65535)

* Exception Action:

* Network Scan (NMAP) Action:

☒ Create Matching Identity Group
☐ Use Hierarchy

* Parent Policy:

Rules

- If Condition:
- If Condition:

Conditions Details

Name: **Apple-iOS-NMAP-Rule4Check1**
Description: **NMAP operating-system**
Expression: **NMAP:operating-system CONTAINS Apple iOS**

This profile matches if either the NMAP scan returns an **operating-system** attribute value containing Apple iOS or Apple iPhone OS. In this example, it matched on Apple iOS.

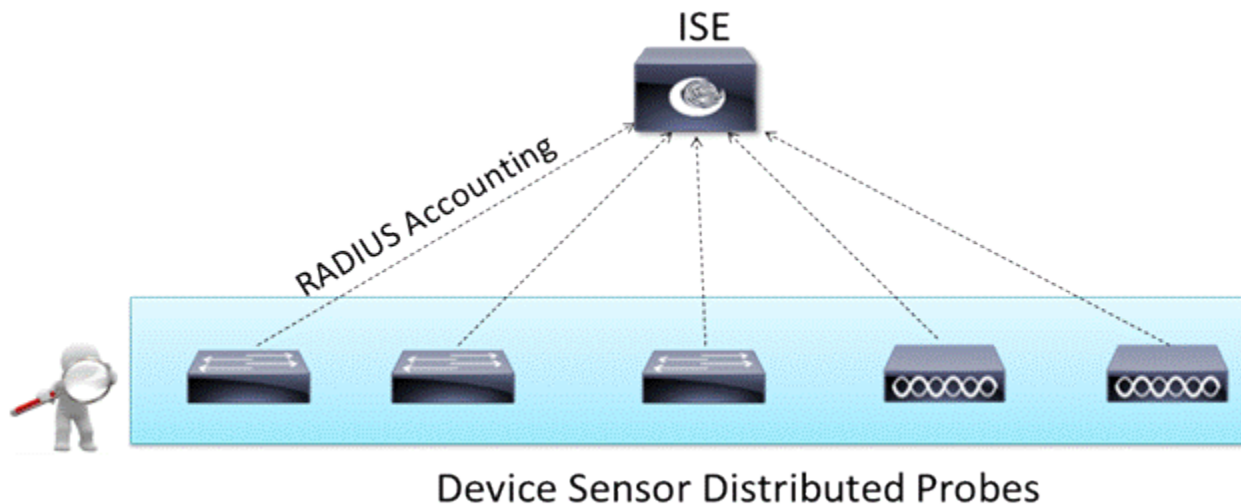
In summary, the NMAP probe can be useful in classifying endpoints based on their operating system as determined by the Operating System scan. Many clientless devices support SNMP agents that can be queried for device classification. Other devices can be classified based on their open ports, and policy may govern that certain devices running specific services should be granted more or less restrictive permissions. Independent of authorization policy assignments, each probe offers an additional level of visibility that can be invaluable to the operational and security management of the entire network.

Device Sensor

Device Sensor Overview

Device Sensor is an access device feature that is currently supported on Cisco access switches and wireless controllers, such as Cisco Catalyst 3650 and 3750 Series and 4500 Series Switches. Device Sensor collects network information from connected endpoints through protocols such as Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP), and Dynamic Host Configuration Protocol (DHCP) and forwards this information to the ISE PSN in RADIUS accounting packets (Figure 67). ISE is able to collect and parse the profiling data using only the RADIUS probe.

Figure 67 Device Sensor Overview



Device Sensor Details

Device Sensor gathers raw endpoint data from network devices. The endpoint information that is gathered aids in completing the profiling capability of switches. The profiling capability of the access device consists of two parts:

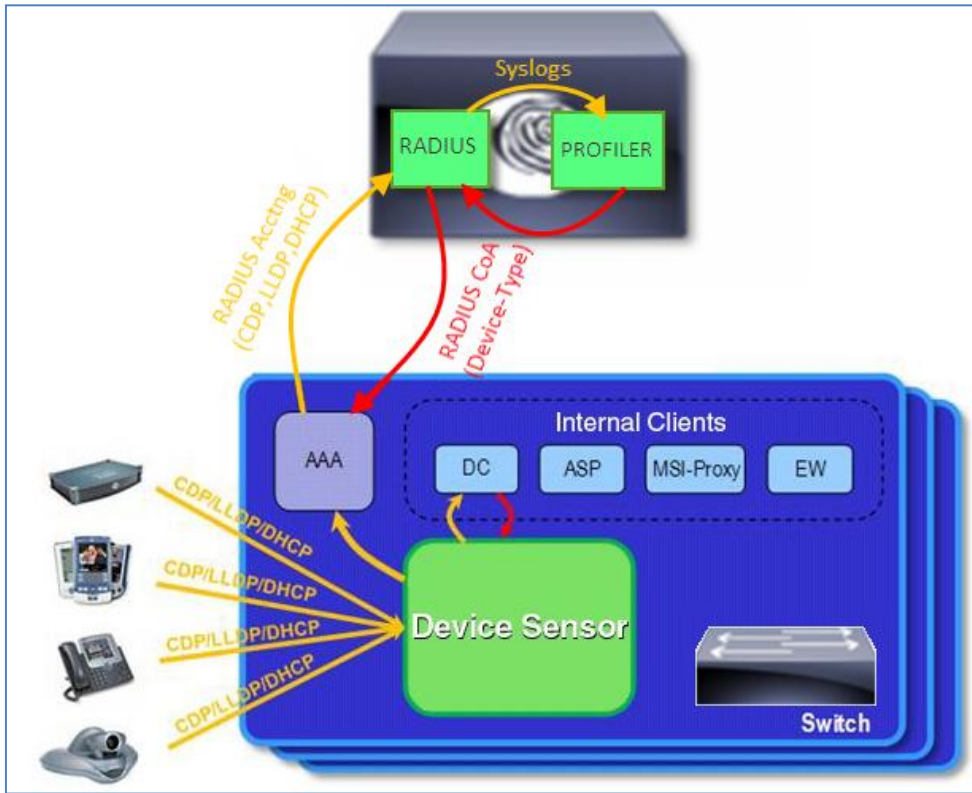
- Collector—Gathers endpoint data from network devices
- Analyzer—Processes the data and determines the type of device

The Device Sensor represents the embedded collector functionality of the access device such as a Cisco Catalyst switch or Cisco Wireless LAN Controller. Figure 68 shows the Device Sensor in the context of the profiling system and also depicts other possible consumers of the sensor data.

A switch or wireless controller with sensor capability gathers endpoint information from network devices using protocols such as CDP, LLDP, and DHCP, subject to statically configured filters, and makes this information available to its registered clients in the context of an access session. An access session represents an endpoint's connection to the network device.

The Device Sensor has internal and external clients. The internal clients include components such as the embedded Device Classifier (DC, or local analyzer), Cisco Auto SmartPorts (ASP), MSI-Proxy, and Cisco EnergyWise™ (EW). Device Sensor uses RADIUS accounting to send data to external clients such as the Identity Services Engine (ISE) Profiling “analyzer.”

Figure 68 Device Sensor Operation Details



Client notifications and accounting messages containing profiling data along with the session events, and other session-related data, such as MAC address and ingress port data, are generated and sent to the internal and external clients (ISE). By default, for each supported peer protocol, client notifications and accounting events are only generated where an incoming packet includes a profiling attribute, or type-length value (TLV), that has not previously been received in the context of a given session. You can enable client notifications and accounting events for all TLV changes, where either a new TLV has been received or a previously received TLV has been received with a different value using CLI commands.

The sensor limits the maximum device monitoring sessions to 32 per port (access ports and trunk ports). In other words, a maximum of 32 endpoints may be monitored per port. An inactivity timer will age out sessions older than 12 hours.

Device Sensor Requirements

Table 6 summarizes Device Sensor protocol support by access device and version.

Table 6 Device Sensor Requirements

Platform	CDP	LLDP	DHCP	HTTP	mDNS
Catalyst 3560/3750 Series Switches	15.0(1)SE1	15.0(1)SE1	15.0(1)SE1	-	-
Catalyst 4500 Series Switch	15.1(1)SG IOS-XE 3.3.0SG	15.1(1)SG IOS-XE 3.3.0SG	15.1(1)SG IOS-XE 3.3.0SG	-	15.1(1)SG IOS-XE 3.3.0SG
WLC/WiSM2 Wireless Controllers	-	-	7.2.110.0	7.3	-

Note: Be sure to reference the applicable Release Notes for your platform to verify software version and feature support. As an example, there are a number of Catalyst 3560 and 3750 switches that do not meet the requirements for Cisco IOS Software Release 15.0(1)SE1 and Device Sensor functionality.

Device Sensor feature support for the Catalyst 3560-C and 3560-CG Series Switches is provided in Cisco IOS Software Release 15.0(2)SE.

When Device Sensor is deployed on a Cisco wireless controller, DHCP profiling is enabled for all clients that join the WLANs configured for sensing. Both DHCP Proxy and Bridged modes are supported for client DHCP requests. Limitations in 7.2MR1 include the following:

- Standalone access points are not supported.
- Local Authentication with local switching is not supported.

In summary, the Device Sensor offers significant benefits in scaling data collection for ISE Profiling Services. With Device Sensors, data collection is highly distributed across the access layer, the points closest to the endpoint and source of data. Information is then selectively filtered at the point of origin and transmitted in RADIUS accounting packets to centralized Policy Service nodes for analysis and classification. This alleviates many of the design challenges and infrastructure requirements to capture this same data using traditional ISE probes.

Configuring Device Sensor for ISE Profiling

The Device Classifier collects information from MAC-OUI and protocols such as CDP, LLDP, and DHCP to identify devices. To collect CDP and LLDP information, CDP and LLDP must be enabled on the Catalyst switch. To make DHCP options information available to the DC, the DHCP Snooping feature must be enabled on the switch. The Cisco Wireless LAN Controller currently supports DHCP data only. Filters can then be defined which specify specific attributes and options to be sent to the analyzer (ISE). To send sensor data to ISE, the access device must have RADIUS accounting enabled. ISE must have the RADIUS probe enabled and properly configured.

Note: RADIUS accounting is required to forward sensor data to ISE. However, RADIUS authentication and authorization are not required to collect and send sensor data to ISE. Therefore, it is possible to use the Device Sensor for pre-ISE deployments during a network discovery phase when an organization is not yet ready to enable RADIUS authentication, even if only Monitor Mode. This support extends to deployments using ISE Profiling Services with Cisco NAC Appliance where RADIUS access control is not deployed.

Procedure 1 Enable RADIUS Probe in ISE

The steps for enabling the RADIUS probe have been covered in detail under the section [Configuring the RADIUS Probe](#). Refer to that section for proper enabling and configuration for the RADIUS probe.

One exception to the instructions provided in that section relates to use of Device Sensor in deployments that do not use RADIUS-based authentication and authorization. In this scenario, it is not expected that the access devices have been added to ISE, but since they need to communicate RADIUS accounting to ISE, it will be necessary to add all access devices that support Device Sensor under Administration→Network Resources→Network Devices.

Be sure that the IP address entered in ISE matches the value sourced by the access device for sending RADIUS. Also be certain that the RADIUS shared key matches the value configured on access devices. These steps are required to support reception of RADIUS accounting packets from the Device Sensor.

Procedure 2 Enable Profiling Protocols on Cisco Wired Switches

To collect CDP, LLDP, or DHCP attributes from the endpoint, the access switch needs to have these protocols enabled to allow it read and gather the associated attributes.

Step 1 Access the command console of an access switch with Device Sensor support.

Step 2 Enable the switch to support CDP.

- a. CDP is enabled globally on Cisco switches by default. If disabled, enable it using this global command:

```
cat3750x(config)# cdp run
```

- b. CDP is enabled on each switchport by default. If disabled, enable using the following interface command:

```
cat3750x(config-if)# cdp enable
```

Step 3 Verify CDP is working on the switch using the **show cdp neighbors** command as shown:

```
cat3750x# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID         Local Intrfce   Holdtme    Capability   Platform   Port ID
APc471.fe34.197a  Gig 1/0/2       137        T            AIR-LAP11  Gig 0
SEP003094C4528A  Gig 1/0/1       150        H P M        IP Phone   Port 1
cat6503.cts.local
                  Gig 1/0/24       140        R S I        WS-C6503   Gig 2/47
```

Here is the detailed view:

```
cat3750x# show cdp neighbors detail
-----
Device ID: APc471.fe34.197a
Entry address(es):
  IP address: 10.1.14.100
Platform: cisco AIR-LAP1142N-A-K9, Capabilities: Trans-Bridge
Interface: GigabitEthernet1/0/2, Port ID (outgoing port): GigabitEthernet0
Holdtime : 133 sec

Version :
Cisco IOS Software, C1140 Software (C1140-K9W8-M), Version 12.4(25e)JA, RELEASE
SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Fri 27-Jan-12 21:45 by prod_rel_team

advertisement version: 2
Duplex: full
Power drawn: 15.400 Watts
Power request id: 21756, Power management id: 2
Power request levels are:15400 14500 0 0 0
Management address(es):

-----
Device ID: SEP003094C4528A
Entry address(es):
  IP address: 10.1.13.100
Platform: Cisco IP Phone 7960, Capabilities: Host Phone Two-port Mac Relay
Interface: GigabitEthernet1/0/1, Port ID (outgoing port): Port 1
Holdtime : 147 sec
Second Port Status: Up

Version :
P00308010100

advertisement version: 2
Duplex: full
Power drawn: 6.300 Watts
Management address(es):

-----
Device ID: cat6503.cts.local
Entry address(es):
  IP address: 10.1.50.1
Platform: cisco WS-C6503, Capabilities: Router Switch IGMP
Interface: GigabitEthernet1/0/24, Port ID (outgoing port): GigabitEthernet2/47
Holdtime : 136 sec

Version :
Cisco IOS Software, s72033_rp Software (s72033_rp-ADVIPSERVICESK9_WAN-M), Versio
n 12.2(33)SXJ2, RELEASE SOFTWARE (fc4)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2011 by Cisco Systems, Inc.
Compiled Wed 14-Dec-11 19:51 by prod_rel_team

advertisement version: 2
VTP Management Domain: 'cts'
Duplex: full
Management address(es):
```

```
IP address: 10.1.50.1
```

Step 4 Enable the switch to support LLDP.

- a. LLDP is disabled globally on Cisco switches by default. To enable it enter the following global command:

```
cat3750x(config)# lldp run
```

- b. LLDP is enabled on each switchport by default. If disabled, enable using the following interface command:

```
cat3750x(config-if)# lldp receive
```

Step 5 Verify that LLDP is working on the switch using the **show lldp neighbors** command, as shown:

```
cat3750x# show lldp neighbors
Capability codes:
(R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
(W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID Local Intf Hold-time Capability Port ID
AVA4FF00E Gi1/0/9 120 B 0004.0d4f.f00e
AVAEC8C79 Gi1/0/10 120 B 0004.0dec.8c79
AVAF694AC Gi1/0/15 120 B 0004.0df6.94ac
AVAEC8C79 Gi1/0/17 120 B 0004.0dec.8c79

Total entries displayed: 4
```

Here is the detailed view:

```
cat3750x# show lldp neighbors detail
-----
Chassis id: 10.6.104.29
Port id: 0004.0d4f.f00e
Port Description - not advertised
System Name: AVA4FF00E
System Description - not advertised

Time remaining: 106 seconds
System Capabilities: B,T
Enabled Capabilities: B
Management Addresses:
IP: 10.X.104.29
OID:
1.3.6.1.4.1.6889.1.69.1.5.
Auto Negotiation - supported, enabled
Physical media capabilities:
Symm Pause(FD)
Pause(FD)
100base-TX(FD)
100base-TX(HD)
10base-T(FD)
10base-T(HD)
Media Attachment Unit type: 16
Vlan ID: - not advertised

MED Information:

MED Codes:
(NP) Network Policy, (LI) Location Identification
(PS) Power Source Entity, (PD) Power Device
(IN) Inventory

H/W revision: 4620D01B
F/W revision: b20d01b2_9_1.bin
S/W revision: a20d01b2_9_1.bin
Serial number: 051606020284
Manufacturer: Avaya
Model: 4620
```



```
Capabilities: NP, IN
Device type: Endpoint Class III
Network Policy(Voice): VLAN dot1p, tagged, Layer-2 priority: 6, DSCP: 46
Power requirements - not advertised
Location - not advertised

----<snip>----

Total entries displayed: 4
```

Step 6 Enable the switch to snoop DHCP. Enter the following commands in global configuration mode to enable DHCP Snooping on select access VLANs:

```
cat3750x(config)# ip dhcp snooping
cat3750x(config)# ip dhcp snooping vlan <VLANs>
```

At a minimum, access VLANs that connect endpoints to be profiled should be included in the list.

Step 7 To trust DHCP information that is sent from an interface connected directly or indirectly to a trusted DHCP server, use the following interface configuration command:

```
cat3750x(config)# interface <interface_to_DHCP_Server>
cat3750x(config-if)# ip dhcp relay information trusted
```

Step 8 Verify DHCP Snooping is enabled on the switch using the **show ip dhcp snooping** command, as shown:

```
cat3750x# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
10-14
DHCP snooping is operational on following VLANs:
10-14
Smartlog is configured on following VLANs:
none
Smartlog is operational on following VLANs:
none
DHCP snooping is configured on the following L3 Interfaces:

Insertion of option 82 is enabled
  circuit-id default format: vlan-mod-port
  remote-id: 1cdf.0f8f.6000 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enabled
Verification of giaddr field is enabled
DHCP snooping trust/rate is configured on the following Interfaces:

Interface                Trusted    Allow option    Rate limit (pps)
-----
-----
```

Step 9 Verify DHCP Snooping is working (binding tables are created for DHCP clients) on the switch using the **show ip dhcp snooping binding** command as shown:

```
cat3750x# show ip dhcp snooping binding
MacAddress                IpAddress        Lease(sec)  Type           VLAN  Interface
-----
00:30:94:C4:52:8A         10.1.13.100      691187      dhcp-snooping  13    GigabitEthernet1/0/1
00:50:56:A0:0B:3A         10.1.10.100      653260      dhcp-snooping  10    GigabitEthernet1/0/1
C4:71:FE:34:19:7A         10.1.14.100      653068      dhcp-snooping  14    GigabitEthernet1/0/2
Total number of bindings: 3
```

Step 10 Save your changes to the switch configuration.

Step 1 Define filters that select CDP, LLDP, or DHCP attributes to be included or excluded from data collection.

- a. Define a filter for CDP attributes starting in global configuration mode:

```
cat3750x(config)# device-sensor filter-list cdp list <my_cdp_list>
cat3750x(config-sensor-cdplist)# tlv name device-name
cat3750x(config-sensor-cdplist)# tlv name address-type
cat3750x(config-sensor-cdplist)# tlv name capabilities-type
cat3750x(config-sensor-cdplist)# tlv name platform-type
cat3750x(config)# device-sensor filter-spec cdp include list <my_cdp_list>
```

CDP TLV values can be entered by name or by number. Table 7 displays a list of CDP TLV names and corresponding descriptions available from the Cisco Catalyst 3750-X Series Switch console interface.

Table 7 Device Sensor: CDP TLV Names and Descriptions

CDP TLV Name	CDP TLV Description
address-type	Address Type
capabilities-type	Capabilities Type
cos-type	COS Type
device-name	Device Name
duplex-type	Duplex Type
external-port-id-type	External Port Id Type
ipprefix-type	IP Prefix Type
mgmt-address-type	Management Address Type
mtu-type	MTU Type
native-vlan-type	Native VLAN Type
platform-type	Platform Type
port-id-type	Port Id type
power-available-type	Power Available Type
power-request-type	External Port Id Type
power-type	Power Type
protocol-hello-type	Protocol Hello Type
trigger-type	Trigger Type
trust-type	Trust Type
twoway-connectivity-type	Twoway Connectivity Type
unidirectional-mode-type	Unidirectional Mode Type
version-type	Version Type
vtp-mgmt-domain-type	VTP Management Domain Type
vvid-type	VVID Type

- b. Define a filter for LLDP attributes starting in global configuration mode, as follows:

```
cat3750x(config)# device-sensor filter-list lldp list <my_lldp_list>
cat3750x(config-sensor-llldplist)# tlv name system-name
cat3750x(config-sensor-llldplist)# tlv name system-description
cat3750x(config)# device-sensor filter-spec lldp include list <my_lldp_list>
```

LLDP TLV values can be entered by name or number. Table 8 displays a list of LLDP TLV names and corresponding descriptions available from the Cisco Catalyst 3750-X Series Switch console interface.

Table 8 Device Sensor: LLDP TLV Names and Descriptions

LLDP Name	LLDP Description
chassis-id	Chassis Chassis Id
end-of-lldpdu	End Of LLDP
management-address	Management Address
port-description	Port Description
port-id	Port Id
system-capabilities	System Capabilities
system-description	System Description

system-name	System Name
time-to-live	Time To Live

- c. Define a filter for DHCP attributes starting in global configuration mode, as follows:

```
cat3750x(config)# device-sensor filter-list dhcp list my_dhcp_list
cat3750x(config-sensor-dhcplist)# option name host-name
cat3750x(config-sensor-dhcplist)# option name default-ip-ttl
cat3750x(config-sensor-dhcplist)# option name requested-address
cat3750x(config-sensor-dhcplist)# option name parameter-request-list
cat3750x(config-sensor-dhcplist)# option name class-identifier
cat3750x(config-sensor-dhcplist)# option name client-identifier
cat3750x(config)# device-sensor filter-spec dhcp include list my_dhcp_list
```

DHCP options can be entered by name or number. Table 9 displays a list of DHCP option names and corresponding descriptions available from the Cisco Catalyst 3750-X Series Switch console interface.

Table 9 Device Sensor: DHCP Option Names and Descriptions

DHCP Option Name	DHCP Option Description
class-identifier	Class Identifier
client-fqdn	Client FQDN
client-identifier	Client Identifier
default-ip-ttl	Default IP Time To Live
domain-name	Domain Name
host-name	Host Name
server-identifier	Server ID
user-class-id	User Class ID

Best Practice: The sample filters shown for CDP, LLDP, and DHCP provide reasonable selections for most use cases. To understand which attributes are available, use the show commands for CDP and LLDP to view which TLVs the endpoints in the network present and determine if any specific attributes will assist in uniquely classifying the endpoint. Device Sensor can also be deployed initially without filters to see which attributes are presented to ISE under Administration→Identity Management→Identities. Appropriate filters can be applied based on those determined to be required to match profiling conditions of customer endpoints.

Note: Entering a specific TLV or option value does not mean that this information is being transmitted by the endpoint. Filters are applied based on the attributes that the endpoint presents to switch or network. For example, if DHCP option client-fqdn is selected for inclusion by the filter, but that option is not requested by DHCP client, no information on that option will be available to Device Sensor or ISE.

- Step 2 Enable sensor data to be sent in RADIUS accounting, including all changes, as follows:

```
cat3750x(config)# device-sensor accounting
cat3750x(config)# device-sensor notify all-changes
```

- Step 3 Disable local analyzer to prevent duplicate updates from being sent to ISE:

```
cat3750x(config)# no macro auto monitor
cat3750x(config)# access-session template monitor
```

The embedded Device Classifier is enabled by default on Cisco switches, which programmatically enables Device Sensor. Therefore, Device Sensor is also enabled by default. When RADIUS authentication and accounting are enabled to send sensor data to ISE, a duplicate RADIUS accounting packet may be sent for each TLV change. This is due to the session monitoring by the local analyzer. To prevent duplicate accounting messages, the local analyzer must be disabled.

If RADIUS authentication is disabled (for example, in networks that are in a pre-ISE deployment/discovery phase or have implemented ISE Profiling Services with Cisco NAC Appliance), no sensor data will be sent if local analyzer disabled. To allow sensor data to be sent independent of the local analyzer, use the command **access-session template monitor**.

- Step 4 Configure the switch to send session accounting information to ISE using RADIUS accounting.

If RADIUS authentication and authorization have already been configured, this step should already be complete. Refer to the section [Configuring the RADIUS Probe](#) for additional details on configuring the switch for RADIUS communication with ISE.

If RADIUS/802.1X has not yet been deployed, be sure to include the following commands in the switch configuration:

```

cat3750x(config)# aaa new-model
cat3750x(config)# aaa accounting dot1x default start-stop group radius
cat3750x(config)# radius-server host <PSN_ip> auth-port <port> acct-port <port> key <shared-secret>
cat3750x(config)# radius-server vsa send accounting

```

Step 5 Verify that the Device Sensor is collecting profiling information.

Use the command **show device-sensor cache**, as follows, to verify that the Device Sensor is working properly:

```

cat3750x# show device-sensor cache all
Device: 0050.56a0.0b3a on port GigabitEthernet1/0/1
-----
Proto Type:Name                               Len Value
dhcp    55:parameter-request-list             14 37 0C 01 0F 03 06 2C 2E 2F 1F 21 79 F9 2B
dhcp    60:class-identifier                     10 3C 08 4D 53 46 54 20 35 2E 30
dhcp    12:host-name                           9 0C 07 77 69 6E 37 2D 70 63
dhcp    50:requested-address                   6 32 04 0A 01 0A 64
dhcp    61:client-identifier                   9 3D 07 01 00 50 56 A0 0B 3A

Device: 0012.d9e3.427e on port GigabitEthernet1/0/24
-----
Proto Type:Name                               Len Value
cdp     4:capabilities-type                     8 00 04 00 08 00 00 00 29
cdp     2:address-type                         17 00 02 00 11 00 00 00 01 01 01 CC 00 04 0A 01 32 01
cdp     6:platform-type                       18 00 06 00 12 63 69 73 63 6F 20 57 53 2D 43 36 35 30 33
cdp     1:device-name                         21 00 01 00 15 63 61 74 36 35 30 33 2E 63 74 73 2E
                                         6C 6F 63 61 6C

Device: c471.fe34.197a on port GigabitEthernet1/0/2
-----
Proto Type:Name                               Len Value
cdp     4:capabilities-type                     8 00 04 00 08 00 00 00 02
cdp     2:address-type                         17 00 02 00 11 00 00 00 01 01 01 CC 00 04 0A 01 0E 64
cdp     6:platform-type                       30 00 06 00 1E 63 69 73 63 6F 20 41 49 52 2D 4C 41
                                         50 31 31 34 32 4E 2D 41 2D 4B 39 20 20 20
cdp     1:device-name                         20 00 01 00 14 41 50 63 34 37 31 2E 66 65 33 34 2E 31 39 37 61
dhcp    50:requested-address                   6 32 04 0A 01 0E 64
dhcp    60:class-identifier                     16 3C 0E 43 69 73 63 6F 20 41 50 20 63 31 31 34 30
dhcp    55:parameter-request-list             10 37 08 01 06 0F 2C 03 21 96 2B
dhcp    12:host-name                           18 0C 10 41 50 63 34 37 31 2E 66 65 33 34 2E 31 39 37 61
dhcp    61:client-identifier                   9 3D 07 01 C4 71 FE 34 19 7A

Device: 0030.94c4.528a on port GigabitEthernet1/0/1
-----
Proto Type:Name                               Len Value
cdp     2:address-type                         17 00 02 00 11 00 00 00 01 01 01 CC 00 04 0A 01 0D 64
cdp     6:platform-type                       23 00 06 00 17 43 69 73 63 6F 20 49 50 20 50 68 6F
                                         6E 65 20 37 39 36 30
cdp     4:capabilities-type                     8 00 04 00 08 00 00 04 90
cdp     1:device-name                         19 00 01 00 13 53 45 50 30 30 33 30 39 34 43 34 35 32 38 41
dhcp    50:requested-address                   6 32 04 0A 01 0D 64
dhcp    55:parameter-request-list             9 37 07 01 42 06 03 0F 96 23
dhcp    60:class-identifier                     39 3C 25 43 69 73 63 6F 20 53 79 73 74 65 6D 73 2C
                                         20 49 6E 63 2E 20 49 50 20 50 68 6F 6E 65 20 43
                                         50 2D 37 39 36 30 00
dhcp    12:host-name                           18 0C 10 53 45 50 30 30 33 30 39 34 43 34 35 32 38 41 00
dhcp    61:client-identifier                   9 3D 07 01 00 30 94 C4 52 8A

```

Procedure 4 Configure Device Sensor on Cisco Wireless Controllers

Device Sensor for DHCP on supported wireless controllers can be enabled using the CLI or web administrative interface.

Step 1 To configure Device Sensor on the Cisco Wireless Controller via the CLI, enter the following command:

```
> config wlan profiling radius enable <wlan-id>
```

Device Sensor is enabled for all wireless clients on the specified WLAN.

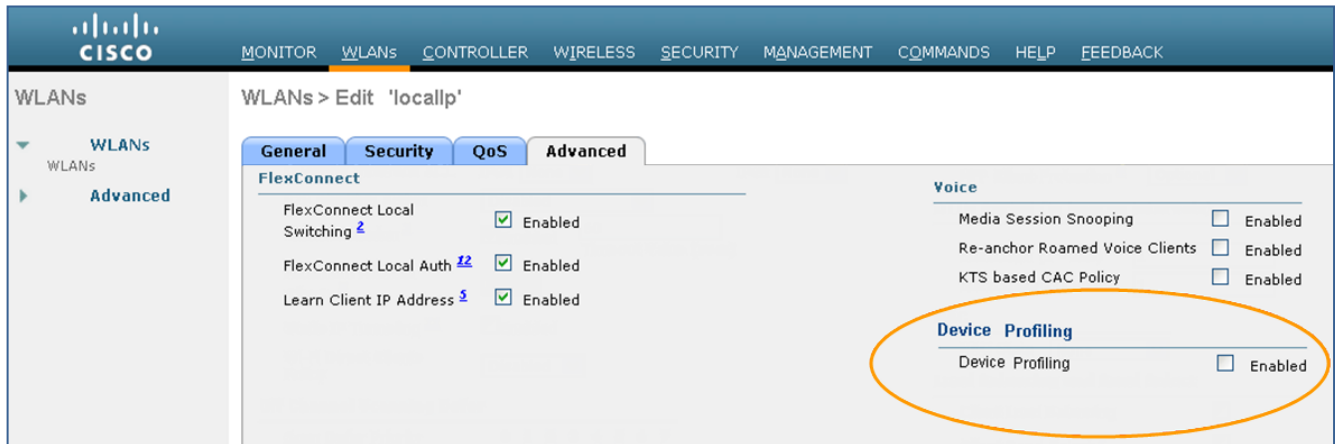
Step 2 Configure the wireless controller to send session accounting information to ISE using RADIUS accounting.

If RADIUS authentication and authorization have already been configured, this step should already be complete.

Refer to the section [Configuring the RADIUS Probe](#) for additional details on configuring the wireless controller for RADIUS communication with ISE.

Step 3 From the WLC web interface, go to WLANs→(WLAN-id)→Edit. The screen display in Figure 69 shows where to enable Device Sensor.

Figure 69 Device Sensor Configuration for Wireless Controller Example



Procedure 5 Verify Profiling using Device Sensor

Step 1 Delete the endpoint from Administration→Identity Management→Identities→Endpoints.

Step 2 Disconnect and then reconnect the endpoint from the access device configured to support profiling using the NMAP probe.

Step 3 Go to the ISE Policy Administration node and navigate to Administration→Identity Management→Identities.

Step 4 Select Endpoints from the LHS pane.

Step 5 Find and select the MAC address of the newly connected endpoint to display the attributes captured by the HTTP probe.

In Figure 70, only the RADIUS probe is enabled on the ISE Policy Service node. Key attributes highlighted include:

- **EndPointPolicy**
- **EndPointSource**
- **OUI**
- **CDP attributes (cdpCacheAddressType, cdpCacheCapabilities, cdpCacheId, cdpCachePlatform)**
- **DHCP attributes (dhcp-class-identifier, dhcp-client-identifier, dhcp-parameter-request-list, dhcp-requested-address, host-name)**

Figure 70 Device Sensor Attributes Example

Endpoint	
* MAC Address	00:30:94:C4:52:8A
* Policy Assignment	Cisco-IP-Phone-7960
Static Assignment	<input type="checkbox"/>
* Identity Group Assignment	Cisco-IP-Phone
Static Group Assignment	<input type="checkbox"/>
Attribute List	
AcsSessionID	ise-psn-1/125323864/12755
AuthState	Authenticated
CPMSessionID	0A010A010000000900036DFC
Called-Station-ID	1C-DF-0F-8F-60-01
Calling-Station-ID	00-30-94-C4-52-8A
Device IP Address	10.1.50.2
Device Type	Device Type#All Device Types#Wired
EndPointPolicy	Cisco-IP-Phone-7960
EndPointProfilerServer	ise-psn-1
EndPointSource	RADIUS Probe
Framed-IP-Address	10.1.13.100
IdentityGroup	Cisco-IP-Phone
Location	Location#All Locations#North_America#RTP
MACAddress	00:30:94:C4:52:8A
MatchedPolicy	Cisco-IP-Phone-7960
MessageCode	3002
NAS-IP-Address	10.1.50.2
NAS-Port	50101
NAS-Port-Id	GigabitEthernet1/0/1
NAS-Port-Type	Ethernet
NetworkDeviceGroups	Device Type#All Device Types#Wired, Location#All Locations#North_America#RTP
NetworkDeviceName	cat3750x
OUI	Cisco Systems, Inc.
PolicyVersion	22
RequestLatency	12
SelectedAccessService	Default Network Access
Service-Type	Framed
StaticAssignment	false
StaticGroupAssignment	false
TimeToProfile	24
Total Certainty Factor	145
attribute-151	A4117E8D
cdpCacheAddressType	00:00:00:01:01:01:cc:00:04:0a:01:0d:64
cdpCacheCapabilities	H;P;M
cdpCacheDeviceId	SEP003094C4528A
cdpCachePlatform	Cisco IP Phone 7960
cisco-av-pair	audit-session-id=0A010A010000000900036DFC, connect-progress=Call Up, cdp-tlv=cdpCacheAddressType=00:00:00:01:01:01:cc:00:04:0a:01:0d:64, cdp-tlv=cdpCachePlatform=Cisco IP Phone 7960, cdp-tlv=cdpCacheCapabilities=00:00:04:90, cdp-tlv=cdpCacheDeviceId=SEP003094C4528A, dhcp-address=10.1.13.100, dhcp-option=dhcp-parameter-request-list=1, 66, 6, 3, 15, 150, 35, dhcp-option=dhcp-class-identifier=Cisco System option=host-name=SEP003094C4528A, dhcp-option=dhcp-client-identifier=01:00:30:94:c4:52:8a
dhcp-class-identifier	Cisco Systems, Inc. IP Phone CP-7960
dhcp-client-identifier	01:00:30:94:c4:52:8a
dhcp-parameter-request-list	1, 66, 6, 3, 15, 150, 35
dhcp-requested-address	10.1.13.100
host-name	SEP003094C4528A
ip	10.1.13.100

If we use Device Sensor alone with **EndPointSource** set to RADIUS probe, we can see that **EndPointPolicy** is correctly matched to Cisco-IP-Phone-7960. The profiling attributes received from Device Sensor that contributed to the profile match include **OUI** = Cisco Systems, Inc., **cdpCachePlatform** = Cisco IP Phone 7960, and **dhcp-class-identifier** = Cisco Systems, Inc. IP Phone CP-7960.

Note that the CDP and DHCP attributes include only those specified by the filter, which shows how data collection is optimized. The Policy Service node was not required to parse and synchronize unneeded attributes across all Administration and Policy Service nodes in the ISE deployment. Based on the Device Sensor configuration, updates are received only when changes occur. SNMP Query and DHCP Probes, on the other hand, will update attributes upon each query or DHCP renewal.

Best Practice: Deploy ISE Profiling using Device Sensor when possible to greatly increase scalability and simplify overall management and profiling configuration. Device Sensor can be deployed across wired access switches and wireless controllers for both RADIUS-authenticated environments and other types of deployments such as a pre-ISE discovery phase or integration with NAC Appliance.

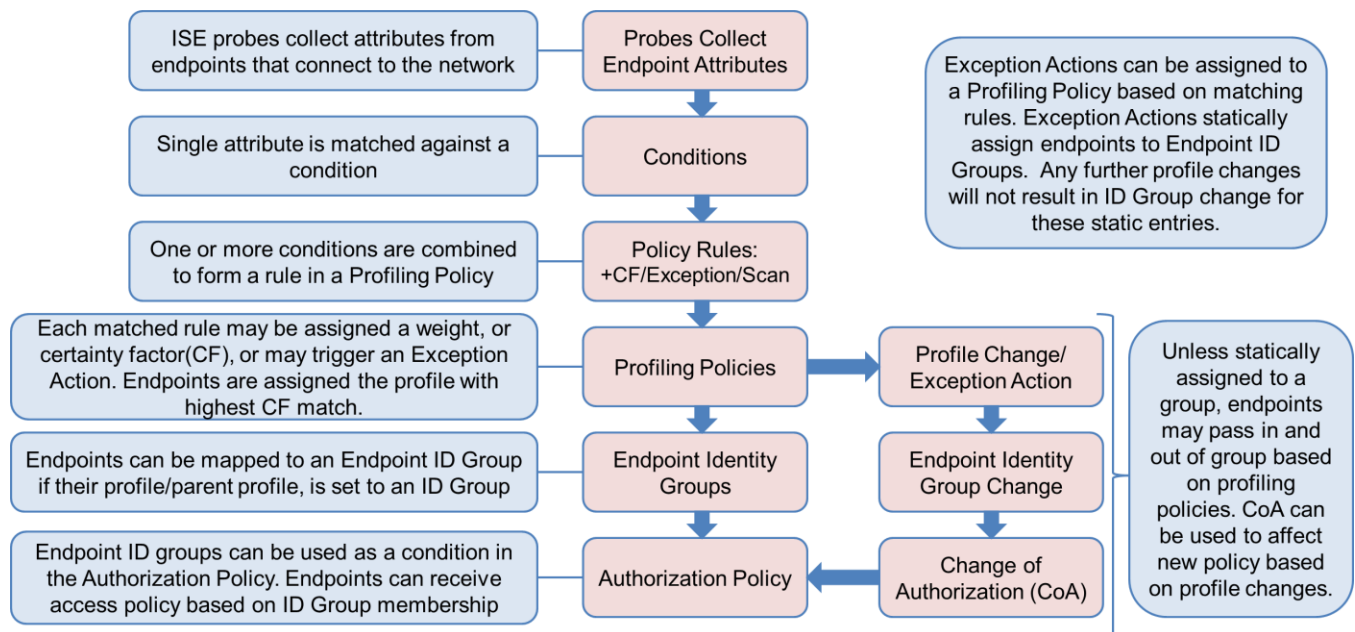
Configuring Profiling Policies

Profiling Policy Configuration Overview

Earlier in this guide, we introduced the high-level architecture of ISE Profiling Services, as shown in Figure 71. This can also serve as a general guideline for ISE Profiling configuration and overall process flow.

We just completed the first component in the flow—namely configuration of probes to collect endpoint attributes. In this section, we will continue through the remaining components to configure Profiling Policy and Authorization Policy to support customer profiling requirements.

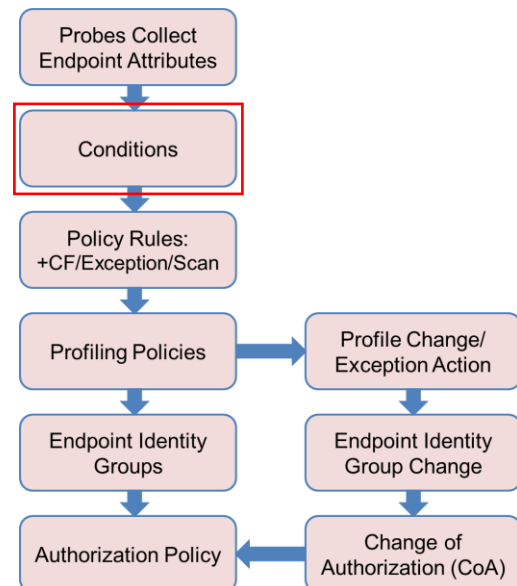
Figure 71: ISE Profiling Policy Configuration Flow



Profiling Conditions

Many profiling attributes can be collected by various ISE probes. Once attributes are collected by the ISE Policy Services nodes, the next step in the profiling process is to match these attributes to Profiling Conditions (Figure 72). Each condition represents a match to a supported attribute listed in the System Dictionary under Policy→Policy Elements→Dictionary.

Figure 72 Configuration Flow: Profiling Conditions



Dictionary Attributes

Table 10 presents the attributes listed in the System Dictionary under Policy→Policy Elements→Dictionary. These attributes are selectable when profiling conditions are created or modified under Policy→Policy Elements→Conditions→Profiling.

Table 10 Dictionary Attributes

RADIUS	MAC	SNMP	CDP	NetFlow	NMAP
Acct-Authentic	MACAddress	cafSessionAuthorizedBy	cdpCacheAddress	MAX_PKT_LENGTH	110-tcp
Acct-Delay-Time	OUI	cafSessionAuthUserName	cdpCacheCapabilities	MAX_TTL	123-udp
Acct-Input-Octets		cafSessionAuthVlan	cdpCacheDeviceId	MIN_PKT_LENGTH	135-tcp
Acct-Input-Packets		cafSessionClientMacAddress	cdpCachePlatform	MIN_TTL	135-udp
Acct-Interim-Interval		cafSessionDomain	cdpCacheVersion	nextHop	137-udp
Acct-Link-Count		cafSessionStatus		OUT_BYTES	138-udp
Acct-Multi-Session-Id	IP	clApIfMacAddress	LLDP	OUT_PKTS	139-tcp
Acct-Output-Octets	EndpointSource	clApIfName	lldpCacheCapabilities	output	139-udp
Acct-Output-Packets	FQDN	clApName	lldpCapabilitiesMapSupported	OUTPUT_SNMP	143-tcp
Acct-Session-Id	Host	clApNameServerAddress	lldpChassisId	prot	1434-udp
Acct-Session-Time	ip	clApNameServerAddressType	lldpManAddress	PROTOCOL	161-udp
Acct-Status-Type	mask	clApSshEnable	lldpPortDescription	sampling_interval	162-udp
Acct-Terminate-Cause	PortalUser	clApSysMacAddress	lldpPortId	src_as	1900-udp
Acct-Tunnel-Connection	User-Agent	clApTelnetEnable	lldpSystemCapabilitiesMapE	SRC_MAC	21-tcp
Acct-Tunnel-Packets-Lo	DHCP	clApTertiaryControllerAddress	lldpSystemDescription	SRC_MASK	22-tcp
Callback-ID	boot-file	clApTertiaryControllerAddress	lldpSystemName	SRC_TOS	23-tcp
Callback-Number	client-fqdn	clApUpTime	lldpTimeToLive	SRC_VLAN	25-tcp
Called-Station-ID	client-identifier	clApWipsEnable		srcaddr	3306-tcp
Calling-Station-ID	device-class	cldcAssociationMode		srcport	3389-tcp
CHAP-Challenge	dhcp-class-identifier	cldcClientAccessVLAN		sys_uptime	443-tcp
CHAP-Password	dhcp-client-identifier	cldcClientIPAddress		tcp_flag	445-tcp
Class	dhcp-message-type	cldcClientStatus		TCP_FLAGS	445-udp
Connect-Info	dhcp-parameter-request-list	dot1xAuthAuthControlledPo			500-udp
Digest-Attributes	dhcp-requested-address	dot1xAuthAuthControlledPo			520-udp
Digest-Response	dhcp-user-class-id	dot1xAuthSessionUserName			53-tcp
EAP-Key-Name	domain-name	hrDeviceDescr			53-udp
EAP-Message	host-name	hrDeviceStatus			631-udp
Egress-VLAN-Name	name-servers	ifDescr			67-udp
Egress-VLANID	pxe-client-arch	ifIndex			68-udp
Error-Cause	pxe-client-machine-id	ifOperStatus			80-tcp
Event-Timestamp	pxe-client-network-id	port			8080-tcp
Filter-ID	server-identifier	portifIndex			operating-syst
Framed-AppleTalk-Link	vendor-class	sysContact			
Framed-AppleTalk-Netv		sysDescr			
Framed-AppleTalk-Zone		sysLocation			
Framed-Compression		sysName			
Framed-IP-Address		sysObjectID			
(incomplete listing)		(incomplete listing)			

Configuring Profiling Conditions






Cisco ISE comes packaged with an extensive list of prebuilt profiling conditions used to build the large library of profiles in the Profiling Policy. At times it may be necessary to create a new custom condition or modify an existing one to suit a particular set of endpoints and a specific environment.

Procedure 1 Configure a Custom (User-Defined) Profiling Condition.

Step 1 Go to Policy→Policy Elements→Conditions and select Profiling from the LHS pane. Scroll through the list of conditions to get an understanding of the common attributes used to create conditions such as **OUI**, **dhcp-class-identifier**, **host-name**, **User-Agent**, and SNMP MIB data such as **cdpCachePlatform**, **lldpSystemDescription**, and **hrDeviceDescr**.

To illustrate the process for creating a custom profiling condition, we will use a real-world example. Under the list of Endpoints→Identities are endpoints that display the following (Figure 73):

Figure 73 Unknown Endpoints Example

Endpoints		
 Edit  Add  Delete  Import  Export		
Endpoint Profile	MAC Address	Static Assignment
<input type="checkbox"/> Unknown	00:C0:B7:65:1F:BC	false
<input type="checkbox"/> Unknown	00:C0:B7:68:31:E1	false

The two entries in diagram both show as Unknown profile; in addition, they share the same MAC prefix. Reviewing the detailed attributes for the first endpoint reveals the following (Figure 74):

Figure 74 NMAP Probe Attributes from Endpoint Scan Example 1

MACAddress	00:C0:B7:65:1F:BC
MatchedPolicy	Unknown
MessageCode	3000
NAS-IP-Address	10.1.50.2
NAS-Port	50108
NAS-Port-Id	GigabitEthernet1/0/8
NAS-Port-Type	Ethernet
NetworkDeviceGroups	Device Type#All Device Types#Wired, Location#All Locations#North_America#RTP
NetworkDeviceName	cat3750x
OUI	AMERICAN POWER CONVERSION CORP

Step 2 It is determined by direct inspection of the endpoint connected to GigabitEthernet1/0/8 or simple deduction from the OUI (American Power Conversion Corp) that these endpoints are SNMP Network Management connections for the APC Uninterruptible Power Systems (UPS) installed in the lab data center. Since there is no default condition in the library for these endpoints, we will create them and ultimately build a new policy to support all these devices throughout the network.

Step 3 Click Add from the RHS pane.

- In this example, the name **APC-OUICheck** is used to indicate the vendor and type of check.
- Enter description—**Custom OUI check for American Power Conversion Corp** in this example. We recommend that you add a unique identifier—the word “Custom” in this example—that will allow quick filtering and display of all user-defined conditions created.
- There are a number of categories under Type. For this check, the Type is **Mac** (Figure 75).

Figure 75 User-Defined Profiler Condition Example 1

Profiler Condition List > **New Profiler Condition**

Profiler Condition

* Name: APC-OUICheck Description: Custom OUI check for American Power Conversion Corp

* Type: Mac

* Attribute Name: DHCP
Mac
Snmp
IP
Radius
Netflow
CDP
LLDP
NMAP

* Operator:
* Attribute Value:
Submit Cancel

- d. Attribute Name is **OUI**.
- e. Operator is **EQUALS**.
- f. Attribute Value is the vendor name assigned to the OUI. In this example, it is **AMERICAN POWER CONVERSION CORP**.

Note: Be sure to use exact case when specifying Attribute Value strings.

In the example given, an Operator of MATCH with Attribute Value set to “AMERICAN POWER” or “AMERICAN POWER CONVERSION” could have optionally been used rather than an exact match (EQUALS).

In event that the OUI database lacks an entry for a particular MAC address prefix, it is possible to create a condition for the unknown OUI using the following settings:

- Type = **Mac**
 - Attribute Name = **MACAddress**
 - Operator = **CONTAINS**
 - Attribute Value = **XX:XX:XX** (3-byte prefix of the MAC address)
-

Figure 76 shows the final form of the user-defined profile condition.

Figure 76 User-Defined Profiler Condition Example 2

Profiler Condition List > **APC-OUICheck**

Profiler Condition

* Name: APC-OUICheck Description: Custom OUI check for American Power Conversion Corp

* Type: Mac

* Attribute Name: OUI

* Operator: EQUALS

* Attribute Value: AMERICAN POWER CONVERSION

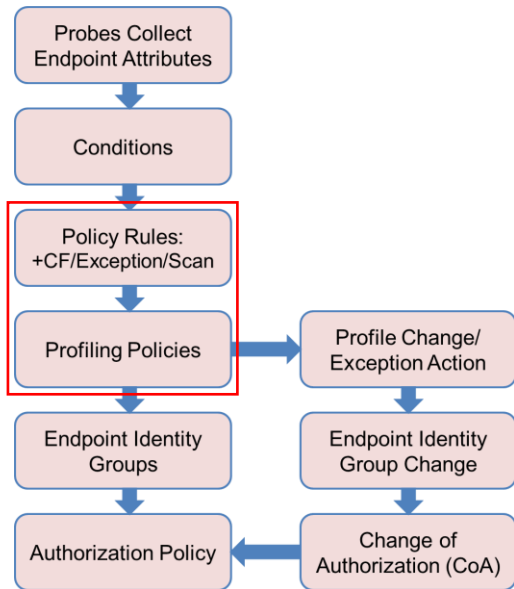
Submit Cancel

Step 4 Click the Submit button (or Save for successive edits) to commit changes.

Profiling Policies and Rules

A Profiling Policy, or profile, defines the policy rules that must match for an endpoint to be considered a profile match. The policy rules contain one or more conditions. If all the conditions of a rule are satisfied (using the AND operator), or if one condition of a rule is satisfied (using the OR operator), the specified action is taken. Figure 77 shows the Profiling Policy configuration flow.

Figure 77 Configuration Flow: Profiling Policy and Rules



Profiling Policy Rule Actions

The three supported Profiling Policy rule actions include:

- Certainty Factor Increases <X>
- Take Exception Action
- Take Network Scan Action

Certainty Factor (CF)

The simple Profiling Policy named Android is shown in Figure 78. This policy contains two rules. Each rule has a single condition that, if matched, takes the action Certainty Factor Increases 30. The CF is used to provide a generic weighting, or relative level of certainty, that an endpoint is a proper match for the profile per the matched condition(s).

The Minimum Certainty Factor is set to 30 for the Android profile. Therefore, if either rule matches, the endpoint is a candidate to be assigned to this profile. Since an endpoint can match multiple conditions and consequently multiple profiles simultaneously, the cumulative CF value must be calculated per matching profile.

Figure 78 Profiling Policy Example

Profiler Policy List > **Android**

Profiler Policy

* Name: Description:

Policy Enabled: ☒

* Minimum Certainty Factor: (Valid Range 1 to 65535)

* Exception Action:

* Network Scan (NMAP) Action:

☒ Create Matching Identity Group
☐ Use Hierarchy

* Parent Policy:

Rules

If Condition	<input type="text" value="AndroidRule1Check1"/>	+	Then	<input type="text" value="Certainty Factor Increases"/>	<input type="text" value="30"/>	
If Condition	<input type="text" value="AndroidRule1Check2"/>	+	Then	<input type="text" value="Certainty Factor Increases"/>	<input type="text" value="30"/>	

There are four Profiling Policy assignment criteria. The endpoint is assigned to a profile if all of the following conditions are met:

- 1) The policy must be enabled. (Policy Enabled checkbox must be checked/enabled).
- 2) Endpoint cumulative CF value for a profile meets the Minimum Certainty Factor.
- 3) The CF rating for the profile is higher than any other profile where 1 and 2 are also true.
- 4) The endpoint meets the Minimum CF for the parent profile (if profile is part of a hierarchy).

Per the first rule in the Android policy example shown in Figure 79, if an endpoint's **User-Agent** contains the string "Android", its CF for this profile is increased to 30. If the endpoint matches the second rule (DHCP **host-name** value contains the string "android"), that will also increase its CF for this profile to 30. If it matches the conditions for both rules, its CF will be 60.

Figure 79 Profiling Policy Rules Example

Profiler Policy List > **Android**

Profiler Policy

* Name Description

Policy Enabled ☒

* Minimum Certainty Factor (Valid Range 1 to 65535)

* Exception Action

* Network Scan (NMAP) Action

☒ Create Matching Identity Group
☐ Use Hierarchy

* Parent Policy

Rules

If Condition

If Condition

Save Reset

Conditions Details

Name **AndroidRule1Check1**
Description **AndroidRule1Check1**
Expression **IP:User-Agent CONTAINS Android**

Conditions Details

Name **AndroidRule1Check2**
Description **AndroidRule1Check2**
Expression **DHCP:host-name CONTAINS android**

Even with a CF of 60, it is technically possible for the endpoint to match the conditions of another policy where the CF value is greater than 60. If all other conditions are met, the endpoint would be assigned to that profile even though it met all conditions for the Android policy.

Typically, the CF values for predefined policies should be left at the default value. In some cases it may be necessary to modify the default values to ensure certain policies take precedence over others based on network policy or preference. In that case, increase the CF value for the applicable rules in the preferred policy the minimal amount to achieve your desired profiling goals.

Similarly, if you are creating new profiles, set initial CF values to a relatively low setting, say 10 or 20, then monitor policy assignments to validate desired outcome. If the initial values are set too high, it may not be possible for other profiles with a potentially closer alignment to the actual endpoint to ever be applied based on CF calculation if the rules for one profile are set with inordinately high CF values relative to other policies.

For example, if an endpoint matches a single rule for custom Profile_A which increases CF to a value of 100, then the endpoint may never be assigned to Profile_B where it matches four rules that increase the CF by only 20 each. It is even possible that the rule in Profile_A is identical to a rule in Profile_B, but has disparate CF values assigned. Therefore, it is a general recommendation to use consistent CF ratings across policy rules.

Best Practice: In general, it is recommended to keep the CF values at their default settings. If modification of default settings is required to ensure certain profile assignments take precedence, only increase the value of the rules in the preferred profile to minimal value to effect the desired policy assignment.

If create custom profiles, keep the initial values for CF relatively low, or at the same value set for other profiles.

Exception and NMAP Actions

The two other possible actions for matching rules include Take Network Scan Action and Take Exception Action. Take Network Scan Action allows the Policy Service node to trigger an NMAP scan against the endpoint per the setting of the Network Scan (NMAP) Action field. This function is covered in greater detail in the section [Profiling using Network Scan \(NMAP\) Probe](#).

Take Exception Action allows ISE to statically assign an endpoint to a policy based on the setting of the Exception Action field. This function is covered in greater detail in the [Exception Actions](#) section.

Both these actions can only be triggered if the endpoint matches the policy AND matches the specified condition. If the condition matches but the endpoint does not match the profile policy, action is not taken.

Also note that it is possible to match multiple rules in a policy such that multiple actions are taken. For example, it is possible to match a rule that increases the CF by 10 and match another rule such as Take Exception Action or Take Network Scan Action provided the policy also is matched.

Procedure 2 Configure a Custom (User-Defined) Profiling Policy

In this procedure, a custom Profiling Policy will be created for the lab APC UPS devices using the previously configured condition.


Step 1 Go to Policy→Profiling. Click Add from the menu of RHS pane.

Step 2 Enter the profile Name as APC-UPS.

Step 3 Enter the Description as **Custom profile for APC UPS Network Management module**. Similar to the description for the APC custom condition, using the keyword **Custom** will allow simple filtering for all user-defined policies based on this string.

Step 4 Keep the setting for Minimum Certainty Factor at its default value of 10.

Step 5 Select the radio button Use Hierarchy instead of the default setting Create Matching Identity Group.

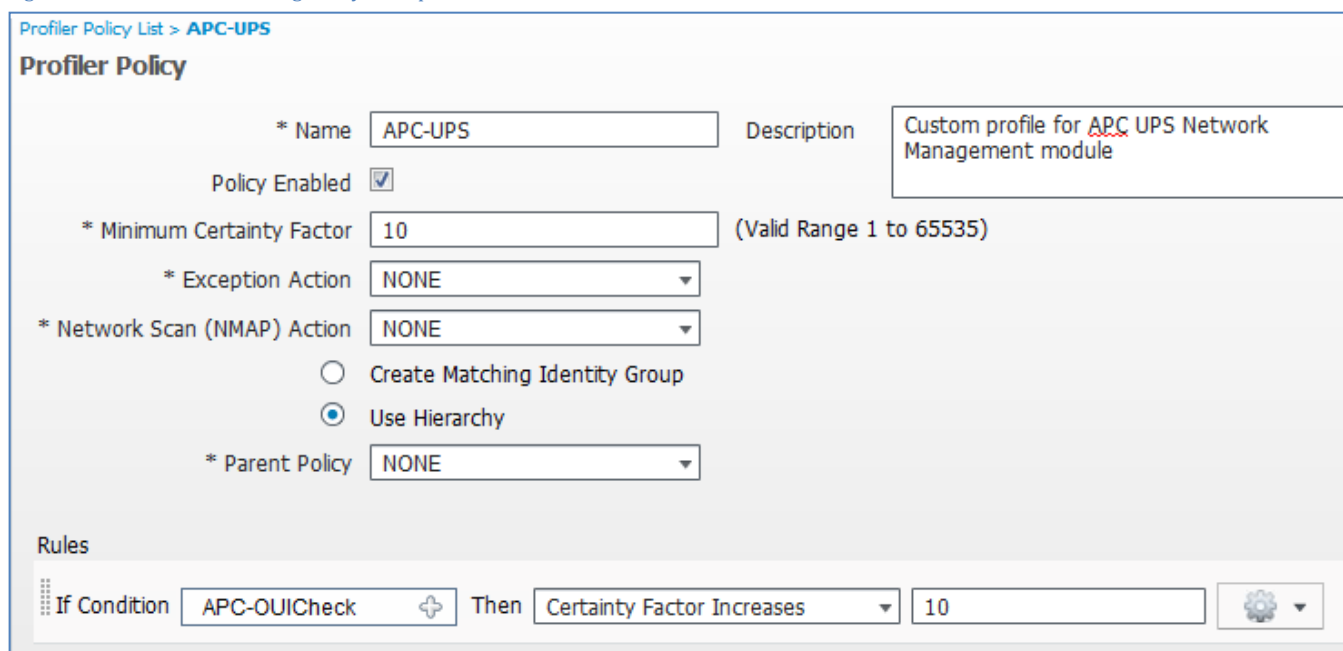
Step 6 Under Rules, click the  symbol next to Condition and choose Select Existing Condition from Library.

Step 7 Under Condition Name→Select Condition, select APC-OUICheck.

Note: As an alternative to creating the Profiling Condition first and then creating the Profiling Policy in a separate task, it would have also been possible to create the new condition from within the Profiling Policy itself using the option Create New Condition (Advanced Option). Once created, the new condition would appear as a named condition in the policy rule.

Step 8 Leave the default rule action Certainty Value Increases with the value of 10 (Figure 80).

Figure 80 User-Defined Profiling Policy Example



The screenshot shows the 'Profiler Policy' configuration window for a policy named 'APC-UPS'. The 'Name' field is 'APC-UPS' and the 'Description' is 'Custom profile for APC UPS Network Management module'. The 'Policy Enabled' checkbox is checked. The 'Minimum Certainty Factor' is set to 10, with a note '(Valid Range 1 to 65535)'. The 'Exception Action' and 'Network Scan (NMAP) Action' are both set to 'NONE'. Under the 'Identity Group' section, the 'Use Hierarchy' radio button is selected, while 'Create Matching Identity Group' is unselected. The 'Parent Policy' is set to 'NONE'. In the 'Rules' section, there is one rule: 'If Condition' is 'APC-OUICheck' (selected from a dropdown), 'Then' is 'Certainty Factor Increases' (selected from a dropdown), and the value is '10'. A gear icon is visible at the end of the rule configuration row.

Step 9 Click Submit to save changes.

Step 10 Go to Administration→Identity Management→Identities and select Endpoints from the LHS pane. The APC devices should no longer appear in the list as Unknown, but with the new matching Profiling Policy assignments, as shown in Figure 81.

Figure 81 Endpoints with User-Defined Profile Example

Endpoints		
<div><div>Edit</div><div>Add</div><div>Delete</div><div>Import</div><div>Export</div></div>		
Endpoint Profile	MAC Address	Static Assignment
<input type="checkbox"/> APC-UPS	00:C0:B7:68:31:E1	false
<input type="checkbox"/> APC-UPS	00:C0:B7:65:1F:BC	false

Step 11 Click APC-UPS for one of the endpoints in list (Figure 82).

Figure 82 Endpoint Detail with User-Defined Profile Example

Endpoint List > 00:C0:B7:68:31:E1

Endpoint

* MAC Address

00:C0:B7:68:31:E1

* Policy Assignment

APC-UPS

Static Assignment

☐

* Identity Group Assignment

Unknown

Static Group Assignment

☐

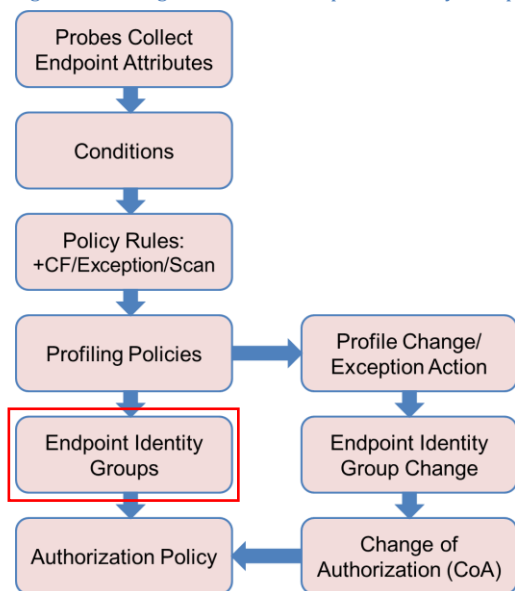
Note that the Policy Assignment is APC-UPS, but the Identity Group Assignment is set to Unknown. This is a result of the decision to change the default setting in the profile from Create Matching Identity Group to User Hierarchy. This option was chosen deliberately to illustrate the relationship between Profiling Policy and Endpoint Identity Groups.

Endpoint Identity Groups

Device profiling can be an invaluable tool for network and security administrators to gain a better understanding into what types of devices are connecting to the network. Beyond just visibility, in order to make an Authorization Policy decision based on an endpoint’s device classification, or Profiling Policy assignment, it is required that the profile be associated to an Endpoint Identity Group. ISE authorization policies do not currently accept raw profiling attributes or policy assignments as conditions, but it is possible to create Endpoint Identity Groups that are mapped to a Profiling Policy assignment. This allows an Authorization Policy to indirectly reference the endpoint’s Profiling Policy assignment as a rule condition.

Figure 83 shows the configuration flow for Endpoint Identity Groups.

Figure 83 Configuration Flow: Endpoint Identity Groups



To map a Profiling Policy to an Endpoint Identity Group, select the radio button labeled Create Matching Identity Group under the profile as shown in Figure 84.

Figure 84 Profiling Policy—Create Matching Identity Group Example

Profiler Policy List > **Android**

Profiler Policy

* Name: Description:

Policy Enabled: ☒

* Minimum Certainty Factor: (Valid Range 1 to 65535)

* Exception Action:

* Network Scan (NMAP) Action:

* ☒ Create Matching Identity Group
☐ Use Hierarchy

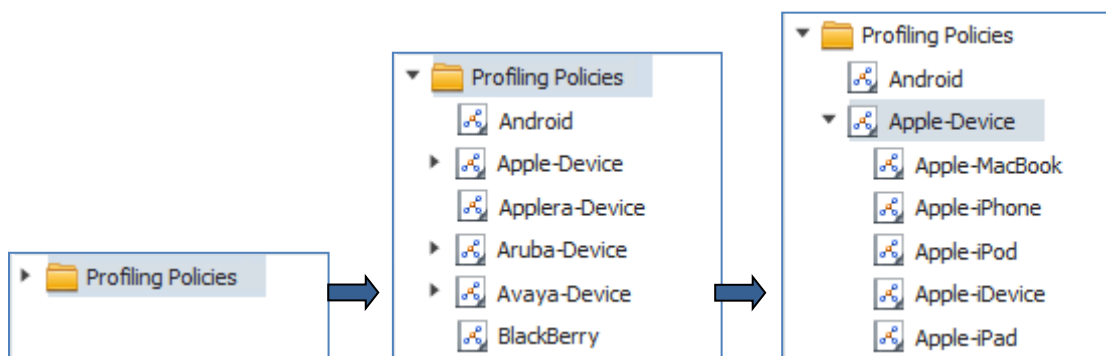
* Parent Policy:

Selection of the Create Matching Identity Group option is mutually exclusive of the Use Hierarchy setting, the default selection for most prebuilt profiles. In the Android policy example in Figure 84, the default setting was changed to create an Endpoint Identity Group based on the policy name. The default setting for user-defined profiles is to create a matching Identity Group.

Profiling Policy Hierarchy

The last criterion listed for matching a Profiling Policy is that the endpoint meets the minimum CF for the parent policy. This introduces the topic of hierarchy in the Profiling Policy. Unlike the Android profile which has Parent Policy set to NONE, as shown in the Figure 84, profiles such as the Apple-iPad and Apple-iPhone are child profiles with a parent profile of Apple-Device. To view the policy hierarchy, navigate to Policy→Profiling. Expand Profiling Policies from the LHS pane by clicking the right arrow symbol (▶) before the label. This will reveal all of the first-level policies (Figure 85).

Figure 85 Profiling Policy Hierarchy



Right-arrows in front of specific entries indicate the presence of child policies for those profiles. Per the above graphic, the Android policy has no children, whereas Apple-Device is a parent policy. Clicking the arrow reveals the child policies for Apple-Device.

The hierarchy is beneficial in organizing the display and management of policies. It also provides a method to define a set of common conditions for multiple child policies such that matching a child policy implies a match of a parent without having to repeatedly define those higher-level conditions under the more granular rules.

A common use of the hierarchy is to match on OUI. For example, all Apple Devices will have an OUI equal to Apple. Therefore, it is not necessary to repeat this condition for an iPad, iPod, iPhone, and so on. To match an Apple-iPhone profile requires that endpoint also have an Apple OUI. This is why use of the simple Firefox browser plugin named User Agent Switch, which mimics other browser **User-Agent** strings alone, will not pass the profile conditions for an Apple iPhone. Without an Apple MAC address, the parent condition fails the test. As noted earlier in this guide, profiling is not positioned as an anti-spoofing solution, but there are features of the solution that naturally thwart certain spoof activity.

The hierarchy is also beneficial to simplify the match of Identity Group assignments. If a parent policy is mapped to an Identity Group, it is not necessary to map all child policies to an Identity Group. For example, there are many prebuilt profiles for Cisco IP Phones. By creating a matching Identity Group for Cisco-IP-Phone (a default setting), it is possible to create an authorization policy based on this parent without requiring individual Identity Groups for each child policy. This can greatly simplify Authorization Policy rules. Unless individual IP phone models need special treatment, they can be treated uniformly through reference of the parent profile and Identity Group assignment.

Procedure 3 Create a Matching Identity Group for a Profiling Policy

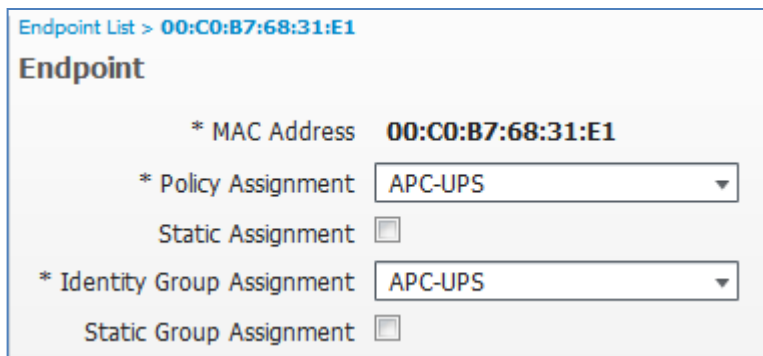
In this procedure, an Identity Group is created for the user-defined profile policy named APC-UPS.

Step 1 Go to Policy→Profiling and select APC-UPS from the list of profiles.

Step 2 Select the option Create Matching Identity Group and then click Save to commit changes.

Step 3 Return to the list of Internal Endpoints under Administration→Identity Management→Identities→Endpoints and again select one of the endpoints assigned to the APC-UPS profile (Figure 86).

Figure 86: Endpoint Identity Group for User-Defined Profile Example



Endpoint List > 00:C0:B7:68:31:E1

Endpoint

* MAC Address 00:C0:B7:68:31:E1

* Policy Assignment APC-UPS

Static Assignment ☐

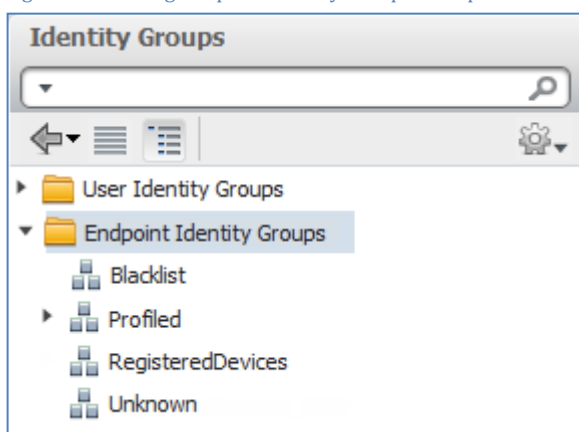
* Identity Group Assignment APC-UPS

Static Group Assignment ☐

Note: The Identity Group Assignment has changed from Unknown to APC-UPS.

Step 4 Go to Administration→Identity Management→Groups and click the arrow (▶) to the left of Endpoint Identity Groups in the LHS pane to expand its contents as shown in Figure 87.

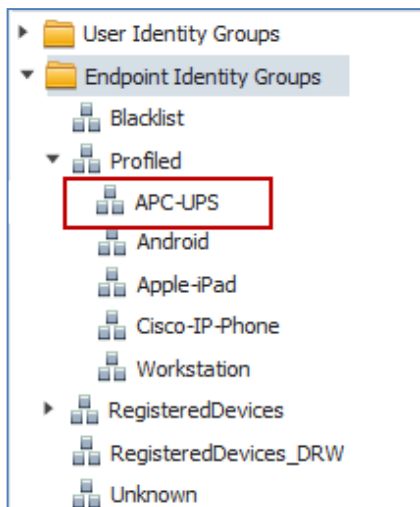
Figure 87 Viewing Endpoint Identity Groups Example 1



This list represents the default top-level Identity Group designations. By default, all endpoints assigned to profiling policies that do **not** have a matching Identity Group will be members of the Identity Group Unknown. All endpoints assigned to profiling policies with a matching Identity Group will appear as members of that Identity Group under the parent Identity Group Profiled. The Blacklist and RegisteredDevices group are special groups. Blacklist is used to identify endpoints denied network access. RegisteredDevices is used by MyDevicesPortal and Native Supplicant Provisioning to designate endpoints registered by network access users.

Step 5 Click ▶ to the left of Profiled to expand its contents (Figure 88):

Figure 88 Viewing Endpoint Identity Groups Example 2

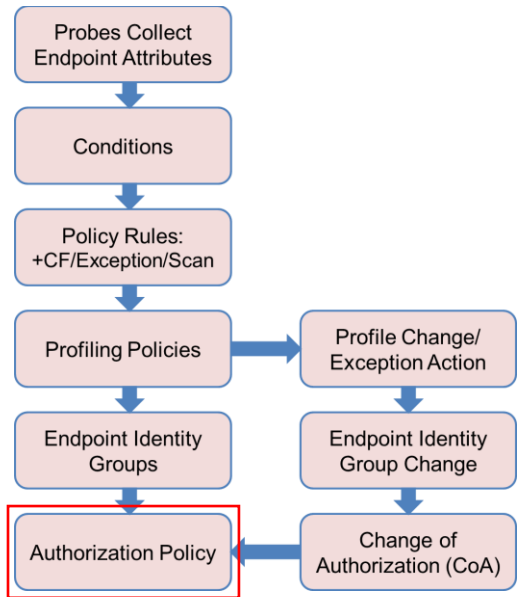


Note that there are some profiling policies that have matching Identity Groups by default, including Cisco-IP-Phone and Workstation. APC-UPS also appears in the list of Endpoint Identity Groups and is now selectable as a matching condition in an Authorization Policy rule.

Profiling and Authorization Policy

Authorization Policy defines the access permissions for endpoints that connect to the network based on matching rules. Authorization Policy rules specify the conditions that must be true for the endpoint before a specified permission is assigned. To assign policy to endpoints based on profiling, the endpoint must be assigned to a Profiling Policy that has a matching Identity Group. Figure 89 shows the configuration flow for Authorization Policies.

Figure 89 Configuration Flow: Authorization Policy



Using ISE Profiling Services to classify devices and assign them to Identity Groups allows ISE to apply different policies to a nonauthenticating endpoint such as a printer or IP phone using MAB, or to apply a different policy to an authenticated employee when connecting using a personal device such as an iPad versus a corporate workstation (Figure 90).

Figure 90 Authorization Policy Example

Authorization Policy				
Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.				
First Matched Rule Applies				
▶ Exceptions (0)				
Status	Rule Name	Conditions (identity groups and other conditions)		Permissions
✓	Profiled Cisco IP Phones	if	Cisco-IP-Phone	then Cisco_IP_Phones
✓	Employee_Personal_Device	if	Android OR Apple-iPad AND Employee	then Guest
✓	Employee_Corp_Device	if	Workstation AND Employee	then Employee

As depicted in the sample Authorization Policy, the Identity Group named Cisco-IP-Phone is used to assign special phone authorizations to endpoints that are profiled as Cisco IP phones. These endpoints are authenticated using MAB. The use of hierarchical policy also allows this policy to apply to any Cisco IP phones regardless of profile match to a specific IP phone model.

The Authorization Policy also highlights the use of profiling to uniquely authorize Employees who connect using a personal device, those classified as Apple-iPad or Android, to Internet-only access (Guest permissions), while at the same time Employees who connect via a workstation are granted full access (Employee permissions).

Procedure 4 Use an Endpoint Identity Group in the Authorization Policy

In this procedure, endpoints profiled as APC UPS devices will be assigned special permissions based on MAB authentication and Authorization Policy rule match to the Identity Group named APC-UPS.

Step 1 Go to Policy→Authorization and insert a new rule below the Profiled Cisco IP Phones rule named Profiled UPS Systems.

Step 2 Under the Identity Group condition, navigate to Endpoint Identity Groups→Profiled and select APC-UPS.

Step 3 Under Permissions, select the appropriate Authorization Profile such as UPS then click Save to commit the changes. The Policy Rule should appear similar to Figure 91.

Figure 91 Authorization Policy Configuration Example 1

Authorization Policy				
Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.				
First Matched Rule Applies				
▶ Exceptions (0)				
Status	Rule Name	Conditions (identity groups and other conditions)		Permissions
✓	Profiled Cisco IP Phones	if	Cisco-IP-Phone	then Cisco_IP_Phones
✓	Profiled UPS systems	if	APC-UPS	then UPS

Step 4 Validate that the Authorization Policy is working as expected by disconnecting and reconnecting the UPS device connections, or by simply resetting the connecting switchports by issuing **shut / no shut** commands under the appropriate interfaces.

Step 5 Go to Operations→Authentications to view the Live Authentications log. Entries similar to those in Figure 92 following should appear.

Figure 92 Authorization Policy Configuration Example 2

Live Authentications								
Add or Remove Columns		Refresh		Refresh Every 1 minute				
Time	Status	Details	Username	Endpoint ID	IP Address	Network Device	Authorization Profiles	Identity Group
May 07,12 06:35:17.230 AM	✓		00:C0:B7:65:1F:BC	00:C0:B7:65:1F:BC	172.16.1.48	cat3750x	UPS	Profiled:APC-UPS
May 07,12 06:35:01.802 AM	✓		#ACSACL#-IP-PERMI			cat3750x		
May 07,12 06:35:01.768 AM	✓		00:C0:B7:68:31:E1	00:C0:B7:68:31:E1	172.16.1.49	cat3750x	UPS	Profiled:APC-UPS

The log shows two endpoints profiled as APC-UPS being authenticated and authorized using the Authorization Profile named UPS. In this example, a downloadable ACL (dACL) is sent to the switch after the first endpoint is authorized. The second endpoint reuses the dACL that has already been downloaded, so there is no second dACL sent.

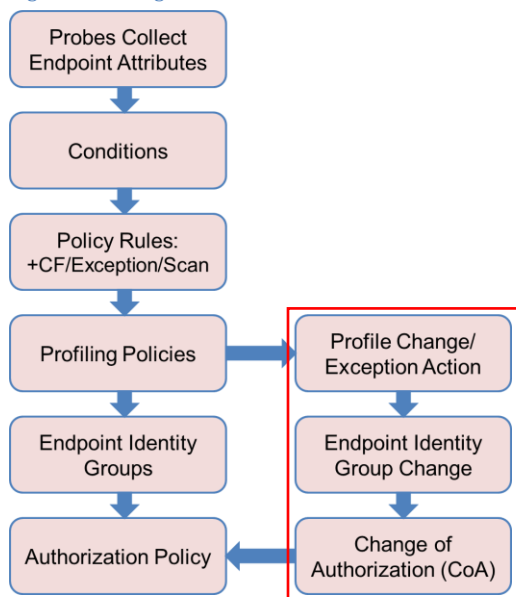
Profile Transitions and Change of Authorization

Through the course of profiling, it is possible that an endpoint will transition from the Unknown Identity Group to a more specific profile such as Apple-Device. In some cases it will transition directly to, for example, Apple-iPad, but it is also possible for transitions to occur in steps as new profile data is acquired from the network. Although not as common, it is possible for “negative” profiling data for an endpoint to cause a transition from a more-specific profile to a less-specific parent profile or a completely different profile altogether.

Regardless of the type of profile transition, often there is an associated change in the Endpoint Identity Group assignment that will apply a different Authorization Policy rule when a matching endpoint authenticates to the network. The challenge is how to effect a new authorization for an endpoint that is already authenticated and authorized to the network.

Figure 93 shows the configuration flow for profile transitions and Change of Authorization (CoA).

Figure 93 Configuration Flow: Profile Transitions and CoA



Change of Authorization (CoA)

CoA is a standards-based RADIUS feature (RFC 3576) that allows the RADIUS server (ISE) to initiate an unsolicited communication to the network access device (the RADIUS client) to update its access policy for an endpoint when certain state or policy changes occur. The update occurs without requiring that the endpoint initiate the reauthentication.

ISE Profiling Services trigger CoA under two primary conditions:

- Profile transition triggers an Exception Action.
- Profile transition results in a change to endpoint access per the Authorization Policy rules.

Exception Actions

By default, there are three predefined, nonconfigurable Exception Actions. Go to Policy→Policy Elements→Results→Profiling→Exception Action to see the list (Figure 94).

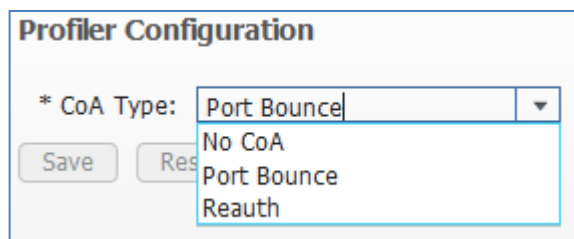
Figure 94 Exception Actions

<input type="checkbox"/> Profiler Action Name ▲	Description
<input type="checkbox"/> EndpointDelete	When endpoint is deleted or reassigned to the unknown profile.
<input type="checkbox"/> FirstTimeProfile	When an endpoint profile changes from unknown to known for the first time.
<input type="checkbox"/> StaticAssignment	When an endpoint has connected to the network and is now statically assigned.

- **EndpointDelete** sends a CoA when the endpoint is deleted or transitions from a Profiled profile to the Unknown profile (no Profiling Policy match).
- **FirstTimeProfile** generates a CoA when the endpoint transitions from the Unknown profile to a specific Profiling Policy assignment. This Exception Action does **not** trigger CoA if the endpoint transitions between known profiles, for example, for Apple-Device to Apple-iPod.
- **StaticAssignment** results in a CoA if an endpoint is statically assigned to a profile from a dynamic profile assignment. Once assigned to a static policy assignment, a new endpoint Profiling Policy cannot be assigned even if profiling attributes would normally dictate a transition.

The default CoA Type sent for each Exception Action is configured under global settings at **Administration→System→Settings→Profiling** (Figure 95).

Figure 95 Global Profiler CoA Configuration



The image shows a 'Profiler Configuration' window. It has a label '* CoA Type:' followed by a dropdown menu. The dropdown menu is open, showing three options: 'No CoA', 'Port Bounce', and 'Reauth'. 'Port Bounce' is the selected option. To the left of the dropdown are two buttons: 'Save' and 'Reset'.

Configuration of global profiling settings is covered in the [Configure Global Profiling Settings](#) section of this guide. The Port Bounce setting is reduced to the Reauth setting when multiple sessions are connected through the same switchport to minimize disruption to other sessions.

System-defined Exceptions Actions are not configurable and cannot be assigned as actions under the Profiling Policy. They are triggered automatically based on the defined transition. However, an administrator can define custom Exception Actions. These user-defined Exceptions can be used in a Profiling Policy to apply a static Profiling Policy assignment and specify if CoA is sent.

Automatic CoA on Profile Transition if Authorization Policy Change

Prior to Cisco ISE Software Release 1.1.1, Exception Actions were commonly used to enforce a CoA for inter-profile transitions—that is, from one known profile to another known profile, often with the undesirable side-effect of statically assigning an endpoint to a Profiling Policy. Starting in ISE 1.1.1, the ISE Policy Service node will issue a CoA whenever a profile transition results in change to endpoint access per the Authorization Policy rules. The decision logic is based on a change of Endpoint Identity Group where the Identity Group is used in Authorization Policy rule. This enhancement negates the need to use Exception Actions to address the use case to send CoA for inter-profile transitions. It also allows endpoints to maintain a dynamic profile assignment, thus allowing additional transitions based on profiling attributes and policy configuration.

User-defined Exception Actions are appropriate for statically assigning endpoints to a preferred policy assignment once a specific condition is met and optionally for preventing a CoA being sent on policy assignment. An example use case would be a critical network device such as a process control endpoint in a manufacturing facility, or a networked medical device in a healthcare facility. In these examples, the administrator may want to statically assign the endpoint to a policy and associated Identity Group. A static assignment through exception can prevent the risk that spurious profile data reverts and endpoint's profile and affects its network connectivity.

Procedure 5 Configure a Custom (User-Defined) Exception Action

In this procedure, an Exception Action is configured for a medical device to assign it to a static Profiling Policy once the specified conditions are matched. The example device is a Draeger M300, a portable wireless heart monitor.

Caution: Due to the inherent compliance factors involved with healthcare solutions, the goal of this example is strictly to illustrate the use of custom Exception Actions. It is not intended to validate the appropriateness of ISE Profiling Services as a method to secure network access for medical devices.

Step 1 Go to Policy→Profiling and select Draeger-M300 from the list. By default, this profile does not include a rule that references an Exception Action. Additionally, an Exception Action has not been defined (Figure 96).

Figure 96 Draeger-M300 Profiling Policy Example

Profiler Policy List > **Draeger-M300**

Profiler Policy

* Name Description

Policy Enabled ☒

* Minimum Certainty Factor (Valid Range 1 to 65535)

* Exception Action

* Network Scan (NMAP) Action

☐ Create Matching Identity Group

☒ Use Hierarchy

* Parent Policy

Rules

If Condition Then

Step 2 Add a new Exception Action.

- Go to Policy→Policy Elements→Results and click the arrow (▶) to the left of Profiling in the LHS pane to expand its contents.
- Select Exception Actions from the LHS pane and then click Add from the menu in RHS pane.
- A new Exception Action is added using the values shown in Figure 97.

Figure 97 User-Defined Exception Action Example

Profiler Exception Action List > **Draeger-M300**

Profiler Exception Action

* Name Description

COA Action ☒ Force COA

* Policy Assignment

In this example, no additional CoA will be sent upon static policy assignment to the profile Draeger-M300. This is the same profile previously shown.

Step 3 Return to the Draeger-M300 Profiling Policy under Policy→Profiling and complete the following steps to define an Exception Action for the profile:

- Set the Exception Action to Draeger-M300.
- Create a new rule with the identical conditions of the existing rule used to match the profile (Figure 98).

Figure 98 Profiling Policy Rules using User-Defined Exception Action Example 1

Rules

If Condition Then

If Condition Then

Condition Name	Expression	Logic
<input checked="" type="checkbox"/> Draeger-M300-PortC	Draeger-M300-PortCheck1	OR
<input checked="" type="checkbox"/> Draeger-M300-PortC	Draeger-M300-PortCheck2	OR
<input checked="" type="checkbox"/> Draeger-M300-PortC	Draeger-M300-PortCheck3	

- Change the action (Then) from default value, Certainty Factor Increases, to Take Exception Action. The resulting Profiling Policy should appear similar to the one in Figure 99.

Figure 99 Profiling Policy Rules using User-Defined Exception Action Example 2

Profiler Policy List > Draeger-M300

Profiler Policy

* Name: Description:

Policy Enabled: ☒

* Minimum Certainty Factor: (Valid Range 1 to 65535)

* Exception Action:

* Network Scan (NMAP) Action:

☐ Create Matching Identity Group

☒ Use Hierarchy

* Parent Policy:

Rules

If Condition	<input type="text" value="Draeger-M300-PortCheck1_OR_Draeger-M300..."/>	+	Then	<input type="text" value="Certainty Factor Increases"/>	<input type="text" value="20"/>
If Condition	<input type="text" value="Draeger-M300-PortCheck1_OR_Draeger-M300..."/>	+	Then	<input type="text" value="Take Exception Action"/>	

Step 4 Save changes.

In this example policy, we have used the same criteria that were used to assign the policy to the endpoint to also statically assign the endpoint to the policy. The Authorization Policy can use the fact that the parent policy called Draeger-Device has a matching Identity Group. Otherwise this policy can have an Identity Group assigned whereby the Authorization Policy will reference this specific profile.

Step 5 Configure a wired switch to support CoA. Use the **aaa server radius dynamic-author** command in global configuration mode as shown:

```
cat3750x(config)# aaa server radius dynamic-author
cat3750x(config-locsvr-da-radius)# client <ISE_PSN_IP_address> server-key <secret-key>
```

Add a separate client entry for each ISE Policy Service node that will communicate to the switch via RADIUS.

Step 6 Configure a wireless controller to support CoA.

- Under the WLC web administration interface, go to Security→AAA→RADIUS→Authentication. Under the RADIUS Server definition, ensure Support for RFC 3576 is enabled as shown in Figure 100.

Figure 100 CoA Configuration for Wireless Controller Example 1

RADIUS Authentication Servers > Edit

Server Index	2
Server Address	10.1.100.5
Shared Secret Format	ASCII ▾
Shared Secret	●●●
Confirm Shared Secret	●●●
Key Wrap	<input type="checkbox"/> (Designed for FIPS customers)
Port Number	1812
Server Status	Enabled ▾
Support for RFC 3576	Enabled ▾
Server Timeout	2 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

- b. Go to WLANs→(WLAN)→Edit→Advanced. For each WLAN to support CoA, Set Allow AAA Override to Enabled and set the NAC State to RADIUS NAC, as shown in Figure 101.

Figure 101 CoA Configuration for Wireless Controller Example 2

General Security QoS Advanced

Allow AAA Override <input checked="" type="checkbox"/> Enabled	DHCP
Coverage Hole Detection <input checked="" type="checkbox"/> Enabled	DHCP Server <input type="checkbox"/> Override
Enable Session Timeout <input checked="" type="checkbox"/> 1800 Session Timeout (secs)	DHCP Addr. Assignment <input type="checkbox"/> Required
Aironet IE <input checked="" type="checkbox"/> Enabled	Management Frame Protection (MFP)
Diagnostic Channel <input type="checkbox"/> Enabled	MFP Client Protection ⁴ Optional ▾
Override Interface ACL IPv4 None ▾ IPv6 None ▾	DTIM Period (in beacon intervals)
P2P Blocking Action Disabled ▾	802.11a/n (1 - 255) 1
Client Exclusion ³ <input checked="" type="checkbox"/> Enabled 60 Timeout Value (secs)	802.11b/g/n (1 - 255) 1
Maximum Allowed Clients ⁸ 0	NAC
Static IP Tunneling ¹¹ <input type="checkbox"/> Enabled	NAC State Radius NAC ▾
Wi-Fi Direct Clients Disabled ▾	

Step 7 Save changes as appropriate for each platform.

Profiling Design and Best Practices

The section discusses general profiling design and best practice recommendations for various deployments and use cases.

Profiling Design Considerations

When planning for ISE Profiling requirements, it is important to start with an understanding of the types of endpoints that require classification to support the network access policy. For example, if you know that a number of network devices of a particular type do not support 802.1X or web-based authentication, it is likely they may require MAB authentication with authorization based on device classification. It is important to list all the known device types that may require profiling for network access.

Profiling Known Device Types

During the ISE planning stage, identify endpoints requiring device classification (authorization based on profile attributes) and determine required attributes to profile these endpoints. If the type of devices requiring authorization is already known, the next step is to determine the attributes and associated probes required to adequately profile them.

Most popular endpoints have a prebuilt policy in the ISE Profile library. Determine attribute and probe requirements by reviewing these default ISE profiles. For example, knowing that Profile X contains conditions A, B, and C, you can deduce the required attributes and probes needed to collect that data. If there is no specific match in the Profile library, reference profiles for similar types of devices. Often the profiling requirements are similar for similar device types.

If there is no existing profile, probes can be temporarily enabled to collect attributes about an endpoint. Often by resetting the endpoint or disconnecting/reconnecting to the network, an administrator can capture the attributes available for the device upon normal startup. The attributes displayed in ISE often reveals the relevant attributes that can uniquely classify the endpoint. Some devices may require traffic analysis including packet capture to determine unique attributes for OUI, DHCP options, User Agent, TCP/UDP ports, or DNS naming.

The following example (Figure 102) shows how to look up attributes used to match on an Apple-iPod profile. It can be seen that this profile is based on either the DHCP attributes or **User-Agent**. Therefore, to profile Apple iPods, it is recommended that the DHCP and HTTP be used.

Figure 102 Profiling Conditions for Apple-iPod Example

The screenshot displays the 'Profiler Policy List > Apple-iPod' configuration page. The main form includes fields for Name (Apple-iPod), Description (Policy for Apple iPods), Policy Enabled (checked), Minimum Certainty Factor (20), Exception Action (NONE), and Parent Policy (Apple-Device). Below these are radio buttons for 'Create Matching Identity Group' and 'Use Hierarchy' (selected). A 'Rules' section shows a list of conditions: 'Apple-iPodRule3Check3' and 'Apple-iPodRule1Check1'. A 'Conditions Details' pop-up window is open for 'Apple-iPodRule1Check1', showing its Name, Description, and Expression: 'IP:User-Agent CONTAINS iPod; U; CPU iPhone OS'.

Looking at the Profile library (under Policy→Profiling) and also reviewing the Profiler Conditions (under Policy→Policy Elements→Conditions→Profiling) (Figure 103) can provide a reasonable understanding of the attributes used and probes required to profile those or similar endpoints.

Figure 103: Probes and Profiler Conditions

Profiler Check Name	Expression	Description
APC-OUICheck	OUI EQUALS AMERICAN POWER CONVERSI	Custom OUI check for American Power Conversion Corp
AndroidRule1Check1	User-Agent CONTAINS Android	AndroidRule1Check1
AndroidRule1Check2	host-name CONTAINS android	AndroidRule1Check2
Apple-DeviceRule1Check1	OUI CONTAINS Apple	Apple-DeviceRule1Check1
Apple-MacBookRule1Check1	User-Agent CONTAINS Macintosh	Apple-MacBookRuleCheck1
Apple-MacBookRule2Check1	User-Agent CONTAINS Mac OS	Apple-MacBookRuleCheck2
Apple-iOS-NMAP-Rule4Check1	operating-system CONTAINS Apple iOS	NMAP operating-system CONTAINS Apple iOS
Apple-iOS-NMAP-Rule5Check1	operating-system CONTAINS Apple iPhone OS	NMAP operating-system CONTAINS Apple iPhone OS
Apple-iPadRule1Check1	User-Agent CONTAINS iPad	Apple-iPadRule1Check1
Apple-iPadRule1Check3	User-Agent CONTAINS AppleWebKit	Apple-iPadRule1Check3
Apple-iPadRule2Check2	host-name CONTAINS iPad	Apple-iPadRule2Check2
Apple-iPhoneRule-TEST	User-Agent CONTAINS iPhone	Custom: Test
Apple-iPhoneRule1Check1	User-Agent CONTAINS iPhone;	Apple-iPhoneRule1Check1
Apple-iPhoneRule2Check1	host-name CONTAINS iPhone	Apple-iPhoneRule2Check1
Apple-iPodRule1Check1	User-Agent CONTAINS iPod;	Apple-iPodRule1Check1
Apple-iPodRule3Check3	host-name CONTAINS iPod	Apple-iPodRule3Check3
Applera-Check	OUI EQUALS Applera Holding B.V. Singapor	Check for Applera Holding B.V. Singapore Operations
Aruba-APRule1Check1	dhcp-class-identifier EQUALS ArubaAP	Aruba-APRule1Check1
Aruba-DeviceRuleCheck1	OUI CONTAINS ARUBA NETWORKS	Aruba-DeviceRuleCheck1
Avaya-DeviceRuleCheck1	OUI CONTAINS Avaya	Avaya-DeviceRuleCheck1
AvayaIPPhoneCheck	dhcp-class-identifier EQUALS ccp.avaya.com	Check for Avaya IP Phone
BlackBerryRule1Check1	OUI CONTAINS RIM	BlackBerryRule1Check1
BlackBerryRule2Check1	dhcp-class-identifier EQUALS BlackBerry	BlackBerryRule2Check1
BlackBerryRule3Check1	host-name CONTAINS BLACKBERRY	BlackBerryRule3Check1
Brother-Device-Descr	hrDeviceDescr CONTAINS Brother	SNMP hrDeviceDescr CONTAINS Brother
Brother-Device-OUI	OUI CONTAINS Brother	MAC OUI CONTAINS Brother
Brother-HL-3040CN-series_Check	hrDeviceDescr CONTAINS Brother HL-3040CN	hrDeviceDescr CONTAINS Brother HL-3040CN series
Brother-HL-5370DW-series_Check	hrDeviceDescr CONTAINS Brother HL-5370DW	hrDeviceDescr CONTAINS Brother HL-5370DW series

Once the key profiling attributes are known, determine the best option from available probes and other collection methods to gather the required profile data. Refer to the individual sections on ISE probe configuration for details on specific requirements to support each probe type. Additional recommendations on probe selection best practices are provided at the end of this section.

Profiling Unknown Device Types

The list of endpoints to be profiled may include networked printers, fax machines, phones, cameras, storage appliances, or any number of IP-enabled endpoints. Sometimes the list of critical devices will be readily known—for example, in environments with a large IP telephony deployment. In other cases, there may be a wide variety of unknown hosts where it is necessary to discover the endpoints first. A phased ISE deployment is a general best practice, starting with Monitor Mode. This will allow administrators to learn the type of endpoints that connect to the network and that would have been denied network access if switchports were placed into an enforcement mode.

Wireless does not have a “monitor mode,” but wireless profiling can still be used to classify endpoints that connect using 802.1X, Web Authentication, or MAC Filtering. Starting with Cisco Wireless LAN Controller Software Release 7.0.116.0, ISE supports profiling of wireless 802.1X endpoints. Starting with WLC Release 7.2.103.0, ISE supports profiling of wireless endpoints using MAC Filtering including those authenticated using Central WebAuth. This is due to support for CoA introduced for these WLAN authentication methods.

Prior to 7.2.103.0, it is still possible to profile the wireless clients, but ISE cannot apply CoA for profile transitions. It can, however, classify endpoints and optionally assign them to Endpoint Identity Groups for inventory (visibility) purposes. Additionally, Authorization Policy based on the current Identity Group assignment can be applied to endpoints upon reconnection to the wireless network. It simply cannot change authorization if a profile change is detected during an active session.

Best Practice: Be sure to set the Call Station ID Type shown in figure above to **System MAC Address** to allow profiling of non-802.1X clients. This will ensure that ISE is able to add the endpoint to the database and associate other profile data received to this same endpoint based on known MAC address.

If possible, deploy ISE Profiling in the early stages of the deployment. ISE can profile wired endpoints without network authentication or authorization to begin the discovery process. This can offer huge benefits in terms of visibility and understanding the types of endpoints trying to connect to the network. During these early stages, the ISE Profiling Policy can begin to evolve if the specific endpoint types requiring profiling for network access are not already clear.

Access Policy and Device Configuration Impact on Profiling

Profiling results may vary depending on the 802.1X deployment mode used (Open Authentication versus Closed Mode) and the order/priority of authentication methods configured on the access devices. For example, if the port is in Closed Mode, DHCP packets cannot be sent until port is authorized. If certain traffic is not sent, probes may not be able to collect the data needed to make a profiling decision. Use of Open Authentication (Monitor Mode and Low-Impact Mode) can allow certain traffic to pass prior to port authorization. Profiling can be accommodated in either scenario, but it is important to understand the implications of specific deployment modes on the ability and timing of attribute collection.

In the case of Flexible Authentication (FlexAuth), the order of authentication methods may also impact the timing of when attributes are collected and the profile assigned at the time of authorization. For example, if the order is set to perform MAB authentication first, 802.1X in Monitor or Low-Impact Modes, it is possible that ISE will have insufficient profile data to assign the desired policy upon initial connection. When the MAB lookup is performed, the endpoint may be still in an Unknown or generic Profiled Identity Group. If the order is set to perform 802.1X first, it may be possible to collect DHCP and other profiling attributes before 802.1X times out. MAB lookup may then succeed with the correct profile based on the additional attributes collected during initial connection.

Note: The impact to endpoint is typically only on first connection to network. Once an endpoint is profiled completely, ISE can use its Identity Group assignment to make an immediate policy match on successive reconnections to the network.

Another consideration is the overall access policy that is initially applied to the port or applied during intermediate or final authorization states. For example, when an endpoint first connects to the network, it may be granted access based on a port ACL (assuming Low-Impact Mode) or on an initial VLAN. If the endpoint is unknown and fails MAB lookup or its posture state is unknown, it may proceed to Central WebAuth or a Posture state, which places a new ACL on the port or VLAN assignment. Upon successful web authentication or remediation, the port may be authorized with a new ACL or VLAN. In each state, there will be different levels of network access. If profiling relies on collecting certain data, that access must be allowed.

A simple example is DHCP. If DHCP is not allowed, profiling that relies on data from DHCP probes may not be available. If Network Scan is used, but the port blocks access to the ports interrogated by the NMAP probe, again that information will not be available to make a profiling decision. This includes access to SNMP ports even if enabled on the endpoint. Additionally, the endpoint itself must allow the traffic. A common example is the use of NMAP to perform an OS scan. If a personal firewall blocks attempts to scan the endpoint, the probe will yield no results.

The use of the NetFlow probe can be particularly challenging because the endpoint must be allowed access to communicate on the network for NetFlow data to be collected. Therefore, policy must allow for the initial collection of data without assuming complete network access for any endpoint. One possible solution would be to profile endpoints in VLAN A, which disallows access to secured resources but does not block general access to the specified ports. Once profiled based on matching traffic, the endpoint can be reauthorized to VLAN B, which allows privileged access to the secured resources.

Another option is to initially allow the traffic but upon detection of uncharacteristic traffic, match a more specific profile that changes the port authorization. For example, if a process control endpoint communicates on an unexpected port, an Exception Action can be applied to assign the endpoint to a Quarantine Identity Group and policy. Again, ISE Profiling is not targeted to be an anti-spoofing solution, but may be used to enforce policy based on anomalous traffic or other profiling attributes. In environments that include critical devices, these will often be locked down or access limited to a known list of endpoints. In these cases, the value of profiling may be for visibility to ensure that all endpoints that match a specific Profiling Policy display attributes consistent with those device types.

The use of Exception Actions can be a tool in cases where a static policy assignment needs to be made. Realize however, that once an endpoint is statically assigned to a profile, only an administrator can change that assignment.

Probe Selection Best Practices

There are different probes that you can use for each deployment. This section focuses on the information made available by each probe and guides you in the probe selection process based on the type of deployment.

Probe Attributes

When determining which probes to enable in the network, it is helpful to understand which attributes can be collected by each probe. Table 11 summarizes the different probes, the key attributes collected, and the applicable use cases.

Table 11 Probes and Key Attributes

Probe	Key Profiling Attributes	Common Endpoint Profiling Use Cases
RADIUS	<ul style="list-style-type: none">• MAC Address (OUI)• IP Address	MAC Address→OUI = Indication of device vendor. Some endpoints can be profiled with this attribute alone if vendor only makes specific devices. Ex: Third-party IP phones, mobile devices, game consoles; MAC-to-IP bindings and probe support.
RADIUS w/Device Sensor	<ul style="list-style-type: none">• CDP/LLDP• DHCP	See SNMP probe for CDP/LLDP info See DHCP probe for DHCP info
SNMP	<ul style="list-style-type: none">• MAC Address/OUI• CDP/LLDP• ARP tables	Valuable for any vendor that uses CDP/LLDP. For example, Cisco IP phones, cameras, access points, appliances. DHCP (See DHCP probe info) MAC Address (see RADIUS probe) Polling of device ARP tables populates ISE MAC-to-IP bindings.
DHCP	<ul style="list-style-type: none">• DHCP	Unique vendor IDs for hardware and software. DHCP fingerprints for OS detection. Hostname/FQDN for common name patterns may indicate OS or device type. Additionally provides MAC-to-IP bindings to support other probes.
NMAP	<ul style="list-style-type: none">• Operating System• Common ports• Endpoint SNMP data	Operating system detection IF scanning not blocked by network/client FW. Offers classification of endpoints that run SNMP agents like network printers. Good for detecting endpoints that listen on the common UDP/TCP ports.
DNS	<ul style="list-style-type: none">• FQDN	Value will depend on whether common naming conventions used for hostname/DNS.
HTTP	<ul style="list-style-type: none">• User-Agent	Operating system detection; some browsers like Chrome may mask actual OS.
NetFlow	<ul style="list-style-type: none">• Protocol• Source/Dest IP• Source/Dest/Ports	Good for detecting mission-specific endpoints with unique traffic patterns or use general purpose hardware/software. May detect anomalous traffic for specific endpoints.

Table 12 provides a more detailed list of key attributes per probe. Other attributes may also be available per probe, but the following list highlights the most common or useful attributes for typical deployments.

Table 12 Probes and Profiling Attribute Details

Probe	Key Profiling Attributes
RADIUS	<ul style="list-style-type: none"> • Calling-Station-ID (OUI) • Framed-IP-Address
RADIUS w/Device Sensor	<ul style="list-style-type: none"> • cdpCachePlatform • cdpCacheAddress • cdpCacheCapabilities • lldpSystemDescription • lldpSystemName • dhcp-requested-address • dhcp-class-identifier • dhcp-client-identifier • dhcp-parameter-request-list • host-name • domain-name • client-fqdn
SNMP Query	<ul style="list-style-type: none"> • MACAddress(OUI) • MAC-IP (ARP) • cdpCachePlatform • cdpCacheAddress • cdpCacheCapabilities • lldpSystemDescription • lldpSystemName
DHCP	<ul style="list-style-type: none"> • dhcp-requested-address • dhcp-class-identifier • dhcp-client-identifier • dhcp-parameter-request-list • host-name • domain-name • client-fqdn
NMAP	<ul style="list-style-type: none"> • operating-system • tcp-x • udp-x • SNMP Attributes
DNS	<ul style="list-style-type: none"> • FQDN
HTTP	<ul style="list-style-type: none"> • User-Agent
NetFlow	<ul style="list-style-type: none"> • IPV4_DST_ADDR • IPV4_SRC_ADDR • PROTOCOL • L4_SRC_PORT • L4_DEST_PORT • MIN_TTL • MAX_TTL

Other	<ul style="list-style-type: none"> • PortalUser • EndPointSource • DeviceRegistrationStatus
-------	---

The Unofficial Guide to Probe Selection

As you consider which probe to select for particular use cases, it may be helpful to rate each probe based on generalized metrics that address the following questions:

- Which probes are the easiest or most difficult to deploy?
- Which probes have the least or highest impact to my network (in terms of traffic overhead, ISE server load, or additional components to support)?
- What is the general value that this probe adds to my ability to profile my endpoints?

Table 13 provides a legend for the metrics and ratings used in Tables 14, 15, and 16 to aid in probe selection for different use cases.

Table 13 Legend for Probe Ratings

Metric		Rating		
Name	Description	1	2	3
DDI	Deployment Difficulty Index	Easy	Medium	Difficult
NII	Network Impact Index	Low Impact	Medium Impact	High Impact
PVI	Probe Value Index	High Value	Medium Value	Low Value

Discovery Phase – Probe Best Practices

Table 14 provides recommended best practices and guidance for probe selection during the discovery phase of the ISE deployment. The assumption is that the network access devices have yet to be configured for RADIUS port authentication and authorization. Therefore, key probes such as the RADIUS probe will not be able to collect data related to network authentication.

These recommendations apply to other deployments that do not have RADIUS authentication enabled such as Cisco NAC Appliance installations where integration with ISE Profiling Services is required.

Table 14: Probe Selection—Discovery Phase

Probe (Method)	EDI	NII	PVI	Key Profiling Attributes	Notes
RADIUS	-	-	-	• N/A	Not applicable since ISE not in auth control plane .
RADIUS w/Device Sensor	2	1	1	• CDP/LLDP • DHCP	If network supports Device Sensor, you can use RADIUS accounting independent of auth control plane.
SNMPTrap	1	1	1	• LinkUp/Down Traps • MAC Notify Traps • Informs	Detect endpoints connections / trigger SNMPQuery probe
SNMPQuery	1	2	1	• MAC Address (OUI) • CDP/LLDP • ARP tables	Polling of device ARP tables populates ISE MA- to-IP bindings. Be careful of high SNMP Query traffic triggered by excessive RADIUS accounting updates due to reauth or interim updates.
DHCP (Helper)	2	1	1	• DHCP	Provides MAC-to-IP bindings. Network impact generally low, but be careful of low DHCP lease timers.
DHCP SPAN	2	3	1	• DHCP	Provides MAC-to-IP bindings
NMAP	1	2	2	• Operating System • Common ports • Endpoint SNMP data	SNMP data assumes UDP/161 open and public string. Relative value of NMAP will depend on customer network and whether OS detection is important factor in wired access policy.
DNS	1	1	2	• FQDN	Value will depend on whether common naming conventions are used.
HTTP (Redirect)	-	-	-	• N/A	Not applicable since ISE not in auth control plane.
HTTP (SPAN)	2	3	2	• User-Agent	Consider SPAN of key HTTP chokepoints like server or Internet edge using intelligent SPAN/tap solutions and/or VACL Capture.
NetFlow	3	3	2	• Protocol • Source/Dest IP • Source/Dest Ports	Recommended only for specific use cases, not general profiling.

Wired Network – Probe Best Practices

Table 15 provides recommended best practices and guidance for probe deployed in a wired network.

Table 15 Probe Selection—Wired Network

Probe (Method)	EDI	NII	PVI	Key Profiling Attributes	Notes
RADIUS	1	1	1	<ul style="list-style-type: none"> • MAC Address (OUI) • IP Address • User-Name, Others 	Fundamental probe for device detection and enabling other probes.
RADIUS w/Device Sensor	2	1	1	<ul style="list-style-type: none"> • CDP/LLDP • DHCP 	If running 3000 or 4000 Series access switches with Device Sensor support, then this is ideal and optimized method to collect select attributes.
SNMPTrap	1	1	3	<ul style="list-style-type: none"> • LinkUp/Down Traps • MAC Notify Traps • Informs 	Detect endpoints connections / trigger SNMP Query probe
SNMPQuery	1	2	1	<ul style="list-style-type: none"> • MAC Address (OUI) • CDP/LLDP • ARP tables 	Polling of device ARP tables populates ISE MAC-to-IP bindings; Be careful of high SNMP Query traffic triggered by excessive RADIUS Accounting updates due to re-auth or Interim Updates.
DHCP (Helper)	2	1	1	<ul style="list-style-type: none"> • DHCP attributes 	Provides MAC-to-IP Bindings; Be wary of low DHCP lease timers.
DHCP SPAN	2	3	1	<ul style="list-style-type: none"> • DHCP Attributes 	Provides MAC-to-IP Bindings
NMAP	1	2	2	<ul style="list-style-type: none"> • Operating System • Common ports • Endpoint SNMP data 	SNMP data assumes UDP/161 open and public string
DNS	1	1	2	<ul style="list-style-type: none"> • FQDN 	Value will depend on whether common naming conventions used
HTTP (Redirect)	2	1	2	<ul style="list-style-type: none"> • User Agent 	Value will depend on relative importance of OS for wired access.
HTTP (SPAN)	2	3	2	<ul style="list-style-type: none"> • User Agent 	Consider SPAN of key HTTP chokepoints like Internet edge; Leverage smart SPAN solutions and VACL Capture if possible
NetFlow	3	3	2	<ul style="list-style-type: none"> • Protocol • Source/Dest IP • Source/Dest Ports 	Recommended only for specific use cases, not general profiling

Wireless Network – Probe Best Practices

Table 16 provides recommended best practices and guidance for probe deployed in a wireless network.

Table 16 Probe Selection—Wireless Network

Probe (Method)	EDI	NII	PVI	Key Profiling Attributes	Notes
RADIUS	1	1	1	<ul style="list-style-type: none"> MAC Address (OUI) IP Address User-Name, Others 	Fundamental probe for device detection and enabling other probes
RADIUS w/Device Sensor	2	1	1	<ul style="list-style-type: none"> CDP/LLDP DHCP 	If running 3000 or 4000 Series access switches with Device Sensor support, then this is ideal and optimized method to collect select attributes.
SNMPTrap	1	1	3	<ul style="list-style-type: none"> LinkUp/Down Traps MAC Notify Traps Inform 	Detect endpoints connections / trigger SNMPQuery probe
SNMPQuery	1	2	1	<ul style="list-style-type: none"> MAC Address (OUI) CDP/LLDP ARP tables 	Polling of device ARP tables populates ISE MAC-to-IP bindings. Be careful of high SNMP Query traffic triggered by excessive RADIUS accounting updates due to reauth or interim updates.
DHCP (Helper)	2	1	1	<ul style="list-style-type: none"> DHCP 	Provides MAC-to-IP bindings. Be wary of low DHCP lease timers.
DHCP SPAN	2	3	1	<ul style="list-style-type: none"> DHCP 	Provides MAC-to-IP bindings.
NMAP	1	2	2	<ul style="list-style-type: none"> Operating System Common ports Endpoint SNMP data 	SNMP data assumes UDP/161 open and public string.
DNS	1	1	2	<ul style="list-style-type: none"> FQDN 	Value will depend on whether common naming conventions used.
HTTP (Redirect)	2	1	2	<ul style="list-style-type: none"> User Agent 	Value will depend on relative importance of OS for wired access.
HTTP (SPAN)	2	3	2	<ul style="list-style-type: none"> User Agent 	Consider SPAN of key HTTP chokepoints like Internet edge. Use smart SPAN solutions and VACL Capture if possible.
NetFlow	3	3	2	<ul style="list-style-type: none"> Protocol Source/Dest IP Source/Dest Ports 	Recommended only for specific use cases, not general profiling.

Profiling Plan

After reviewing the different types of endpoints that require device classification—for either visibility or network access based on device type—and agreeing on the best probes to collect the required data, the next step is to document the profiling plan. At a minimum, this plan should include all the devices to be profiled and how that profiling data will be used to authorize network access. The plan should also include the list of unique attributes required to classify each endpoint, the probe or method used to capture those attributes, and the specifics of the collection method. For example, will URL redirection or SPAN be used to capture HTTP? Where will the data be captured? Which PSNs will receive the data? Another critical aspect of the plan is how scalability and redundancy will be deployed.

Note: Profiling high availability and scalability, including load balancing, are beyond the scope of this document.

Table 17 shows a basic profiling plan for a sample company.

Table 17 Sample Profiling Plan

Device Profile	Where Used in Auth Policy Rules?	Unique Attributes	Probes Used	Collection Method
Cisco IP Phone	Cisco-IP-Phones (MAB)	OUI	RADIUS	RADIUS Authentication
		CDP	SNMP Query	Triggered by RADIUS Start
IP Camera	Cisco-IP-Cameras (MAB)	OUI	RADIUS	RADIUS Authentication
		CDP	SNMP Query	Triggered by RADIUS Start
Printer	Printers (MAB)	OUI	RADIUS	RADIUS Authentication
		DHCP Class Identifier	DHCP	IP Helper from local Layer 3 switch SVI
Point of Sale (PoS) Station (static IP)	POS (MAB)	MAC Address	RADIUS (MAC Address discovery)	RADIUS Authentication
		ARP Cache for MAC-to-IP mapping	SNMP Query	Triggered by RADIUS Start
		DNS name	DNS	Triggered by IP Discovery
Apple iDevice	Employee_Personal (802.1X/CWA)	OUI	RADIUS	RADIUS Authentication
		Browser User Agent	HTTP	Authorization Policy posture redirect to central Policy Service node cluster
		DHCP Class Identifier and MAC-to-IP mapping	DHCP	IP Helper from local Layer 3 switch SVI
Device X	Critical_Device_X (MAB)	MAC Address	RADIUS (MAC Address discovery)	RADIUS Authentication
		Requested IP Address for MAC-to-IP mapping	DHCP	RSPAN of DHCP Server ports to local Policy Service node
		Optional to acquire ARP Cache for MAC-to-IP mapping	SNMP Query	Triggered by RADIUS Accounting Start
		Traffic to Destination Port/IP	NetFlow	NetFlow export from Distribution 6500 switch to central Policy Service node

Summary of Profiling Best Practices and Recommendations

The following summarizes best practice recommendations for ISE Profiling:

- Use Device Sensors when possible to optimize data collection.
- When possible, ensure profile data for a given endpoint is sent to the same Policy Service node. Otherwise, there is a potential for excessive updates of endpoint data and contention by multiple PSNs.

In many cases, ISE handles this automatically:

- SNMP Queries will be issued by the same PSN that receives the RADIUS Accounting Start or SNMP trap packet.
- HTTP traffic resulting from URL redirection is sent to the PSN that is handling the RADIUS session.
- DHCP Helper can be sent to more than one PSN, so recommendation is to send to same PSNs as configured for RADIUS for particular access device.
- DNS queries are sent by the same PSN that learns the IP address. This PSN is typically the one that handles the RADIUS session and receives the IP address from either the Framed-IP-Address from RADIUS Accounting, dhcp-requested-address from DHCP, or triggered SNMP Query of cdpCacheAddress.
- Triggered NMAP Scans are sourced by the same PSN that receives the profiling data resulting in a policy rule match. For example, if an NMAP action is assigned to a profile rule condition based on OUI match, then the first PSN that receives the endpoint MAC address via RADIUS, DHCP, or other probe will be the one that sources the NMAP scan.

In other cases, such as using DHCP SPAN, HTTP SPAN, or NetFlow probe, it is not always possible to ensure traffic reaches the same PSN in a distributed deployment.

- HTTP Probe:

Use URL redirection instead of SPAN to centralize collection and reduce traffic load related to SPAN/RSPAN.

In general try to avoid data collection using HTTP SPAN. If used:

- Look for key traffic chokepoints such as the Internet edge or wireless controller connection
- Use intelligent SPAN/tap options or VACL Capture to limit amount of data sent to IS.

It can be difficult to provide high availability for SPAN without an intelligent network tap infrastructure.

- DHCP Probe:

Use DHCP Relays (IP Helpers) when possible.

In general, try to avoid data collection using DHCP SPAN. If used, make sure probe captures traffic to central DHCP Server.

Be aware that layer 3 devices serving DHCP will not relay DHCP for same network.

It can be difficult to provide high availability for SPAN without an intelligent network tap infrastructure.

- SNMP Probe:

Be careful of high SNMP traffic due to triggered RADIUS accounting updates as a result of high re-authentication (low session/re-auth timers) or frequent interim accounting updates.

For polled queries, be careful not to set polling interval too low. Be sure to set optimal PSN for polling in ISE network device configuration.

SNMP Traps are primarily useful for non-RADIUS deployments like integration with NAC Appliance, not for a network using RADIUS-based authentication and authorization.

- NetFlow: Use only for specific use cases. NetFlow has the potential for high load on network devices and PSN.

Appendix A: References

Cisco TrustSec System:

- <http://www.cisco.com/go/trustsec>
- http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

Device Configuration Guides:

Cisco Identity Services Engine User Guides:

http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

For more information about Cisco IOS Software, Cisco IOS XE Software, and Cisco NX-OS Software releases, please refer to following URLs:

- For Cisco Catalyst 2900 series switches:
http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 3000 series switches:
http://www.cisco.com/en/US/products/ps7077/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 3000-X series switches:
http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 4500 series switches:
http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 6500 series switches:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html
- For Cisco ASR 1000 series routers:
http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html
- For Cisco Wireless LAN Controllers:
http://www.cisco.com/en/US/docs/wireless/controller/7.0MR1/configuration/guide/wlc_cg70MR1.html