Cisco TrustSec How-To Guide: Cisco ISE Base Configuration and Bootstrapping

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

Current Document Version: 3.0

August 27, 2012

Table of Contents

Introduction

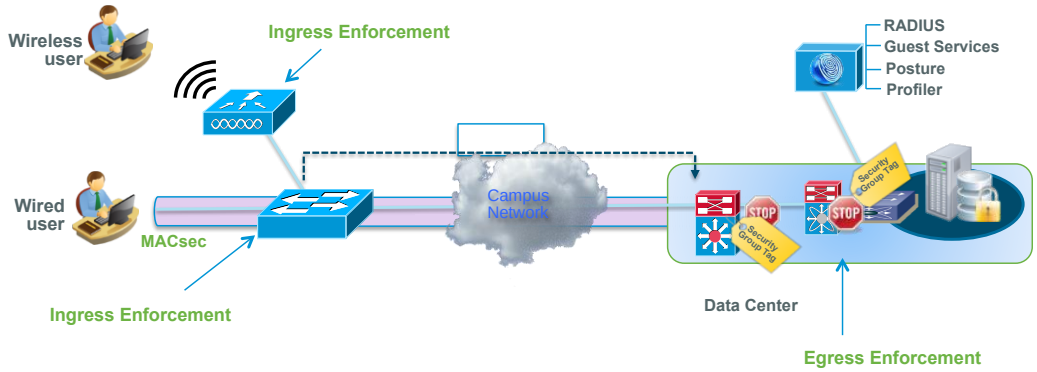
What Is the Cisco TrustSec System?

Cisco TrustSec®, a core component of the Cisco SecureX Architecture™, is an intelligent access control solution. Cisco 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 Cisco 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: Cisco TrustSec Architecture Overview

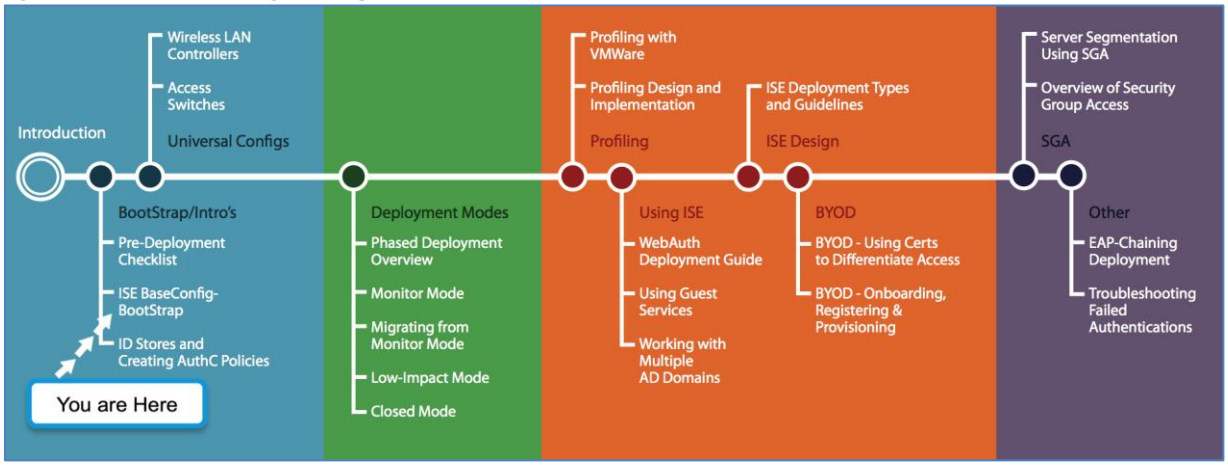


About the TrustSec How-To Guides

The TrustSec team is producing this series of How-To documents to describe best practices for Cisco TrustSec deployments. The documents in the series build on one another and guide the reader through a successful implementation of the Cisco 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 is 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 Cisco 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, Cisco 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 "Cisco TrustSec "certified". The Cisco TrustSec team strives to provide regular updates to these documents that will include new features as they become available, and are integrated into the Cisco TrustSec test plans, pilot deployments, and system revisions. (i.e., Cisco 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 Cisco TrustSec deployment as prescribed by Cisco best practices to help ensure a successful project deployment.

Initial Installation and Setup

Overview

This guide describes running the Cisco Identity Services Engine (ISE) Setup program to configure the Cisco ISE hardware appliances and virtual machine environments. While Cisco ISE comes preinstalled when ordered on a physical appliance, there are times when a physical appliance may need to be reinstalled (or reimaged). This How-To Guide can be used as a reference; we will demonstrate the step-by-step configuration in a later section.

Cisco ISE Installation and Setup

Procedure 1 Complete the Setup Dialog

Note: ISE will need to be freshly installed on the virtual machine. Installation consists of 1) booting from the ISE ISO image and 2) starting the installation process that installs the operating system and ISE application. For details on how to set up VMware, please refer to Installing the Cisco ISE System Software on a VMware Virtual Machine in the Cisco Identity Services Engine Hardware Installation Guide.

Note: After these two steps, the installation pauses and a setup dialog must be completed before the installation resumes and completes.

Step 1 Log in to the ise-1 virtual machine console.

```
********************************************
Please type 'setup' to configure the appliance
********************************************
localhost login:
```

Step 2 Enter **setup** at the login prompt to start the setup dialog.

```
Enter hostname[]: ise
Enter IP address []: 10.1.100.21
Enter IP default netmask[]: 255.255.255.0
Enter IP default gateway[]: 10.1.100.1
Enter default DNS domain[]: demo.local
Enter Primary nameserver[]: 10.1.100.10
Add/Edit another nameserver? Y/N : n
Enter Primary NTP server[time.nist.gov]: ntp.demo.local
Add/Edit secondary NTP server? Y/N : n
Enter system timezone[UTC]: <return>
Enter username[admin]: <return>
Enter password: default1A
Enter password again: default1A
Bringing up network interface...
Pinging the gateway...
Pinging the primary nameserver ...
Do not use 'Ctrl-C' from this point on...
Appliance is configured
Installing applications...
Installing ise ...
Generating configuration...

 === Initial Setup for Application: ise ===
Welcome to the ISE initial setup. The purpose of this setup is to provision the the internal ISE
database. This setup is non-interactive, and will take roughly 15 minutes to complete. Please be
patient.

Running database cloning script...
Running database network config assistant tool...
Extracting ISE database content...
Starting ISE database processes...
Restarting ISE database processes...
Creating ISE M&T session directory...
Performing ISE database priming...
Generating configuration...
Rebooting...
```

Note: The password policy is not explicitly stated, but a password of **default1A** will work.

Note: After completing the setup dialog, it may take roughly 45 minutes before the installation completes.

Note: It's preferred (but not required) to use all lower cases for host name and DNS domain name. Limit the host name to 15 characters if you are planning to join this ISE to an Active Directory domain.

Step 3 After the setup dialog is completed, the installation will continue and finish with a reboot. The installation is complete when you are presented with the following login prompt:

```
ise-1 login:
```

Procedure 2 Complete an ISE Installation

Step 1 Log in using the credentials you provided during the setup.

Note: You may continue using the VM console interface to access the ISE CLI, or you may use Secure Shell (SSH) Protocol. On a physical appliance, the serial port or the keyboard and video may be used to access the ISE CLI.

Step 2 Enter **show run** to confirm the setup settings.

Step 3 Configure a repository.

An ISE repository is a file storage location that can be used for copying files to and from ISE. You can use these repositories for various operations, such as patching or upgrading the ISE, backing up or restoring configuration, and creating a support bundle. The different repository types are shown in Table 1.

Table 1 ISE Repository Types

ISE Repository Types
cdrom: (read only)
ftp:
http: (read only)
https: (read only)
nfs:

Step 4 Configure an FTP repository on ISE.

```
ise-1/admin# config t
Enter configuration commands, one per line.  End with CNTL/Z.
ise-1/admin(config)# repository myFTP
ise-1/admin(config-Repository)# url ftp ftp.demo.local/
ise-1/admin(config-Repository)# user anonymous password plain admin@demo.local
ise-1/admin(config-Repository)# end
ise-1/admin# copy running-config startup-config
Generating configuration...
ise-1/admin#
```

Step 5 Confirm that ISE can communicate with the repository using the **show repository** command. (You should see a directory listing from the FTP server.)

```
ise-1/admin# show repository myFTP
<file list>
ise-1/admin#
```

Note: For this sample setup, the FTP server is on the admin PC and the FTP home directory is C:\Configs.

Step 6 Confirm that time synchronization is working.

Step 7 Immediately after the primary Network Time Protocol (NTP) server is configured, you will see that ISE is in an unsynchronized state.

```
ise-pap-1/admin# sho ntp
Primary NTP   : ntp.demo.local
unsynchronized
  time server re-starting
   polling server every 64 s
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 127.127.1.0     .LOCL.          10 l   14   64    7    0.000    0.000   0.001
 128.107.220.1   CHU_AUDIO(1)     4 u   14   64    7    0.773    0.528   0.431

Warning: Output results may conflict during periods of changing synchronization.
```

Step 8 After a few minutes, ISE should synchronize with the primary NTP server. The asterisk indicates which time server it has synchronized with.

```
ise-pap-1/admin# sho ntp
Primary NTP   : ntp.demo.local
synchronised to NTP server (128.107.220.1) at stratum 5
   time correct to within 459 ms
   polling server every 64 s
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
 127.127.1.0     .LOCL.          10 l   48   64  377    0.000    0.000   0.001
*128.107.220.1   CHU_AUDIO(1)     4 u   45   64  377    0.733    1.738   1.010
Warning: Output results may conflict during periods of changing synchronization.
```

Step 9 If you see that ISE has synchronized to the local machine (as shown below), this means that NTP time synchronization is not working.

```
ise-pap-1/admin# show ntp
Primary NTP   : ntp.demo.local
synchronised to local net at stratum 11
   time correct to within 10 ms
   polling server every 1024 s
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*127.127.1.0     .LOCL.          10 l    5   64  377    0.000    0.000   0.001
 128.107.220.1   .LOCL.           4 u 1026 1024  377    0.478  -866.81  60.476
Warning: Output results may conflict during periods of changing synchronization.
```

Note: Synchronization with the NTP server may not be immediate. You may need to wait 10 to 15 minutes for ISE to select the NTP server over the local clock.

ISE Web GUI Access

Overview

When you log in to the Cisco ISE web-based interface for the first time, you will be using the preinstalled evaluation license. You must use only the supported HTTPS-enabled browsers listed in the previous section. After you have installed Cisco ISE as described in this guide, you can log in to the Cisco ISE web-based interface.

Log In Using the Web-Based Interface

Procedure 1 Start a Web Session with ISE

Step 1 Open an HTTP-enabled browser window and browse to **http://ise.demo.local**.

Note: This URL was based on lab setup in the previous section. Please use http://<host name>.<domain name> to access the browsers. The HTTPS-enabled browsers are: Mozilla Firefox 2.6 and 9 and Microsoft Internet Explorer 8 and 9.

Step 2 The session will be redirected to the secure Cisco ISE login page: https://ise.demo.local/admin.

Step 3 On the login page, enter the username and password that you defined during setup.

Step 4 Click Login, and the Cisco ISE dashboard appears.

Note: The default web UI credentials are **admin/cisco**. On first login, you will be prompted to change the default password.

Figure 3 ISE Web Login

Certificates and Certificate Authorities

Overview

This guide demonstrates how to generate an ISE certificate, how the certificate authority (CA) issues a certificate to ISE, and how to install the certificates to ISE. While installing Cisco ISE, a default, self-signed certificate will be generated. Although sufficient for labs and demonstrations, it is not a good practice to put Cisco ISE into production with a self-signed certificate. To secure communications with ISE, whether the communication is authentication-related or for ISE management--for example, for configuration using the ISE web interface--X.509 certificates and certificate trust chains need to be configured to enable asymmetric encryption.

Note: Time synchronization is extremely important for certificate operations. Ensure that you have configured NTP and have the correct time.

Cisco ISE Configuration – Certificates and Trusting the CA

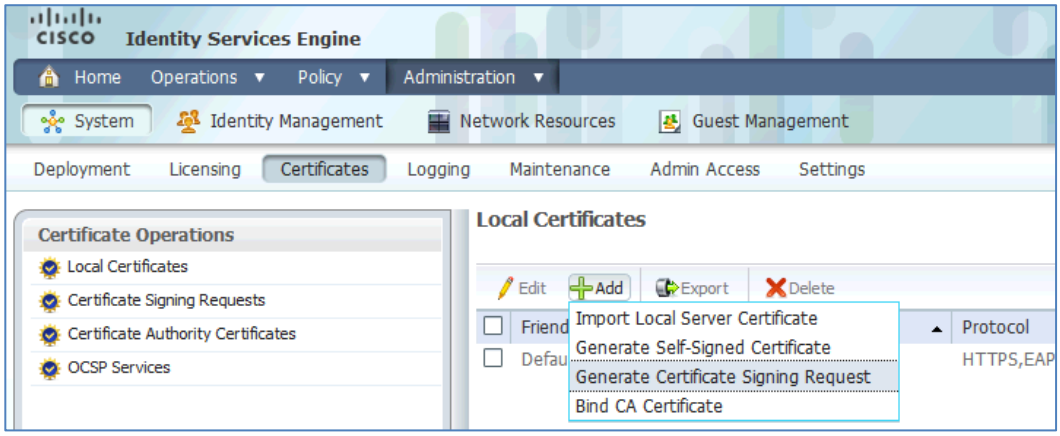
Note: For certificate chains: The entire chain should be imported successfully before the certificate request is created.

Procedure 1 Request a Certificate from the Certificate Authority.

Step 1 Go to Administration→ System → Certificates → Local Certificates.

Step 2 Click Add → Generate Certificate Signing Request.

Figure 4 Generate Certificate Request

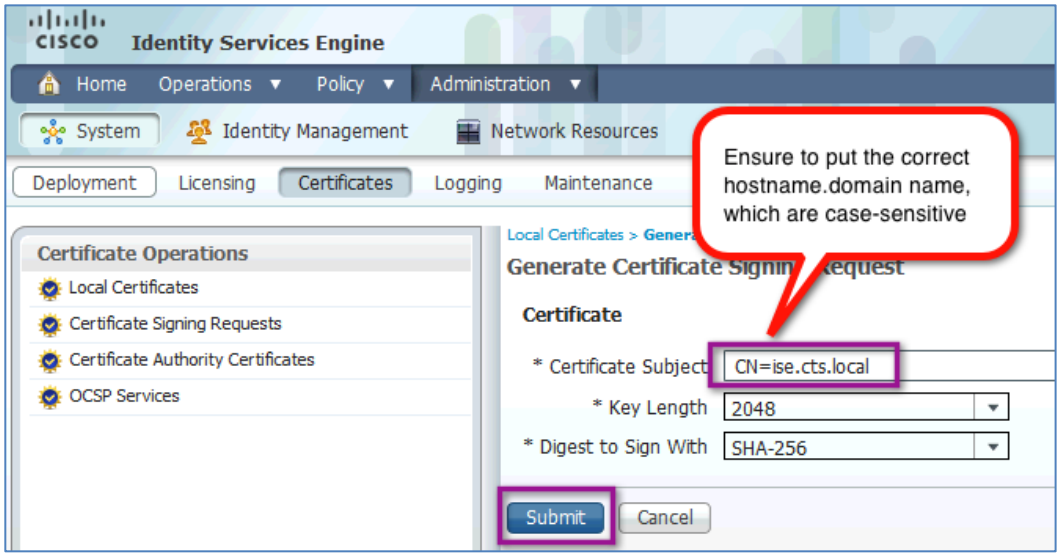


Step 3 Enter the fully qualified domain name (FQDN) for the Cisco ISE node into the Certificate Subject field.

Note: The example that includes additional fields for public CA are: CN=ise.cts.local, OU=SAMPG, O=Cisco, L=San Jose, ST=California, C=US

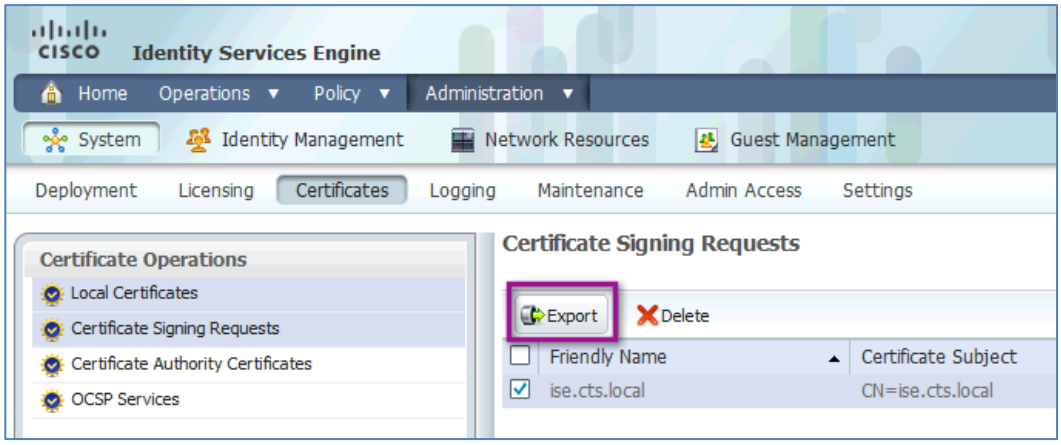
Step 4 Click Submit.

Figure 5 Certificate Details



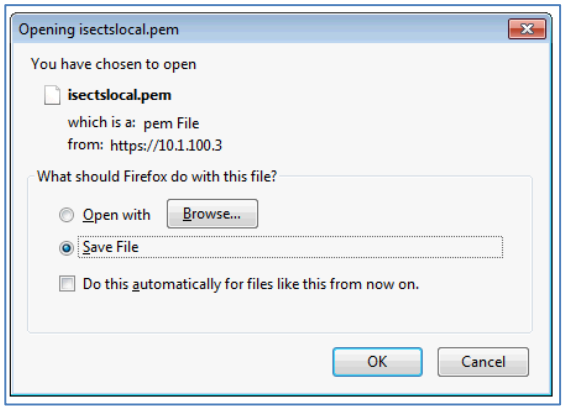
Step 5 Click Certificate Signing Requests and select your new request. Click Export.

Figure 6 Export Newly Created Certificate



Step 6 Save the .pem file to an easily accessible location.

Figure 7 Saving .pem File



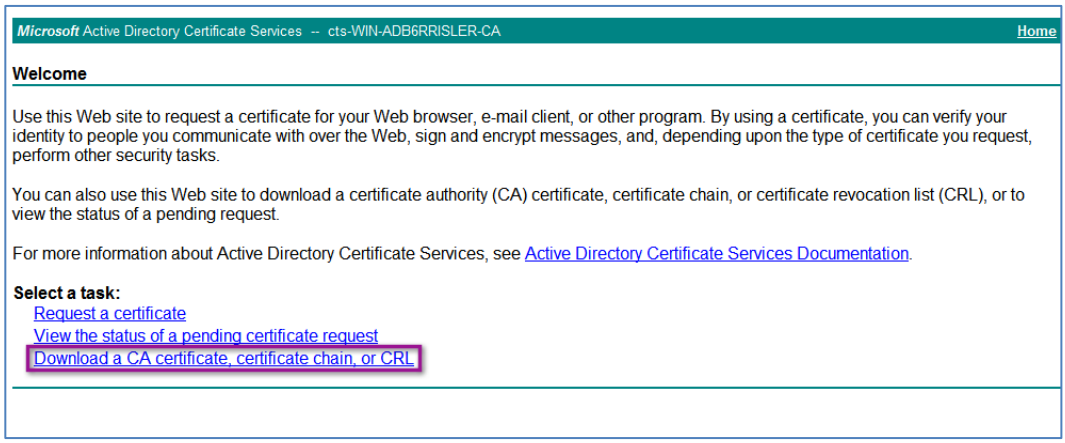
Procedure 2 Download the CA Root Certificate and Issue a Certificate

Step 1 Browse to your CA.

Step 2 Click the link titled "Download a CA certificate, certificate chain, or CRL."

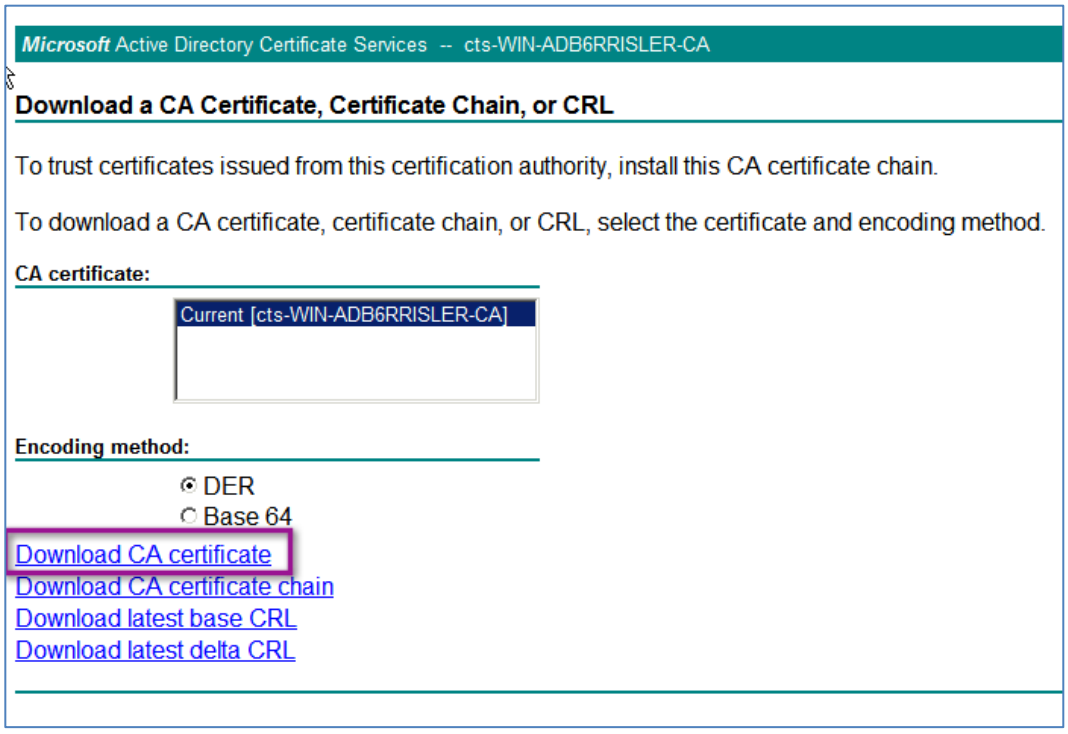
Note: We are using a Microsoft CA; therefore, we are browsing to http://ad.cts.local/certsrv/. Depending on the CA in your organization, the certificate request will follow a different procedure. When using the Microsoft CA, it has been noted that using Internet Explorer will provide a better experience.

Figure 8 Download a CA Certificate



Step 3 Click Download CA certificate.

Figure 9 Select Certificate and Encoding Method



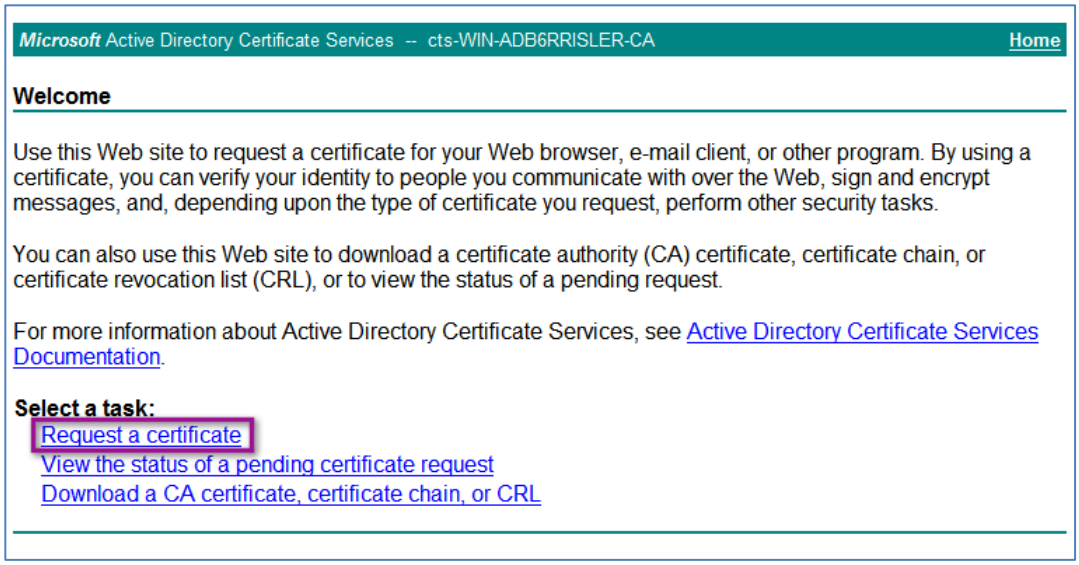
Step 4 Save the resulting .cer file in a location that can be easily accessed.

Cisco Best Practice: Name the file something unique, such as **RootCert.cer.**

Step 5 Click Home, in the upper right corner.

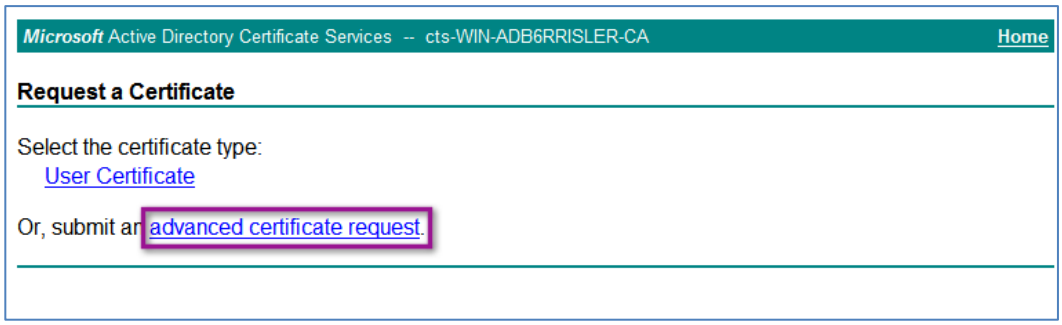
Step 6 Click Request a certificate.

Figure 10 Request a Certificate



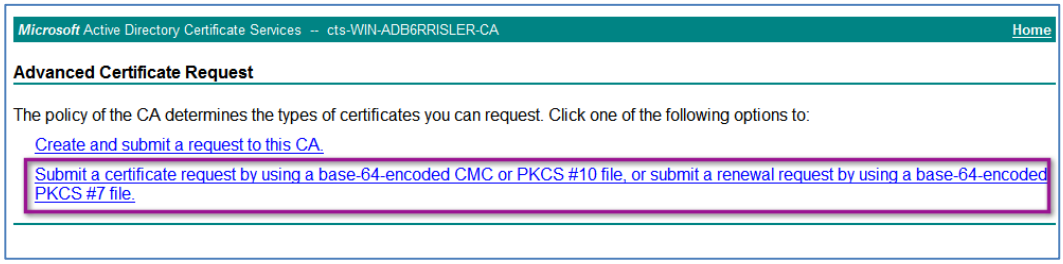
Step 7 Click advanced certificate request.

Figure 11 Advanced Certificate Request



Step 8 Select the option titled "Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoder PKCS #7 file."

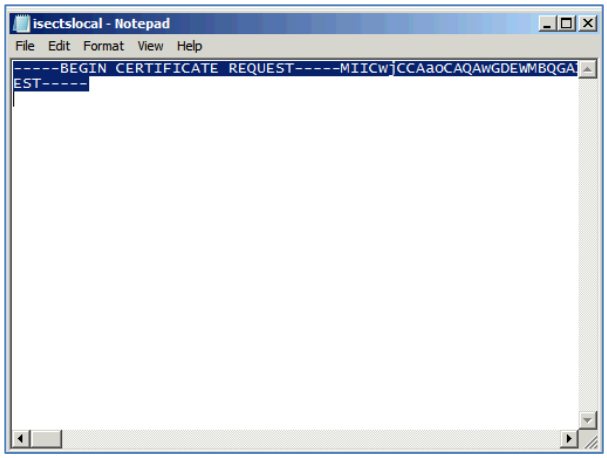
Figure 12 Select the Certificate Request Option



Step 9 Using NotePad or another text editor, open the .pem file saved in Procedure 2.

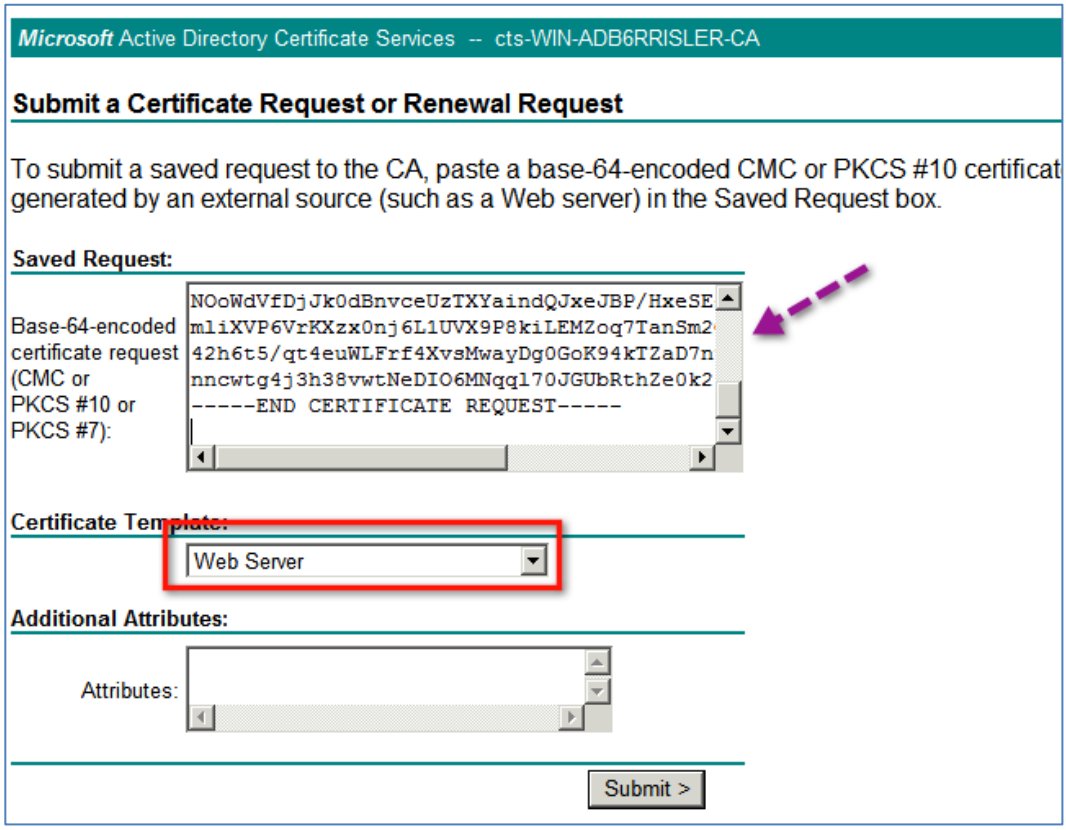
Step 10 Highlight the entire contents of the file and select Edit → Copy.

Figure 13 Copy the Certificate



Step 11 Paste the contents from the certificate request .pem file into the Saved Request text box in the CA window. The Certificate Template should be set to Web Server**.**

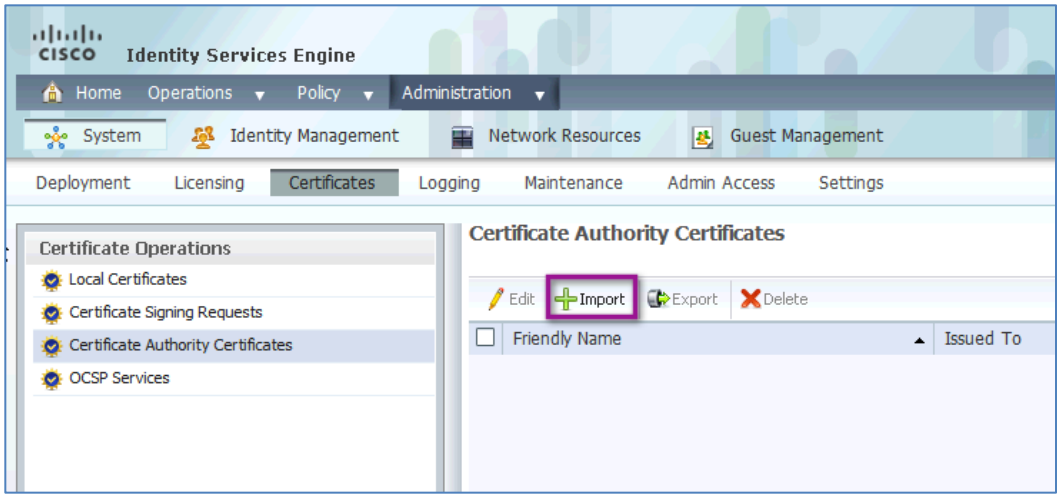
Figure 14 Submit a Certificate Request



Step 12 In the Cisco ISE administrative interface, navigate to Administration → System → Certificates → Certificate Authority Certificates.

Step 13 Click Import.

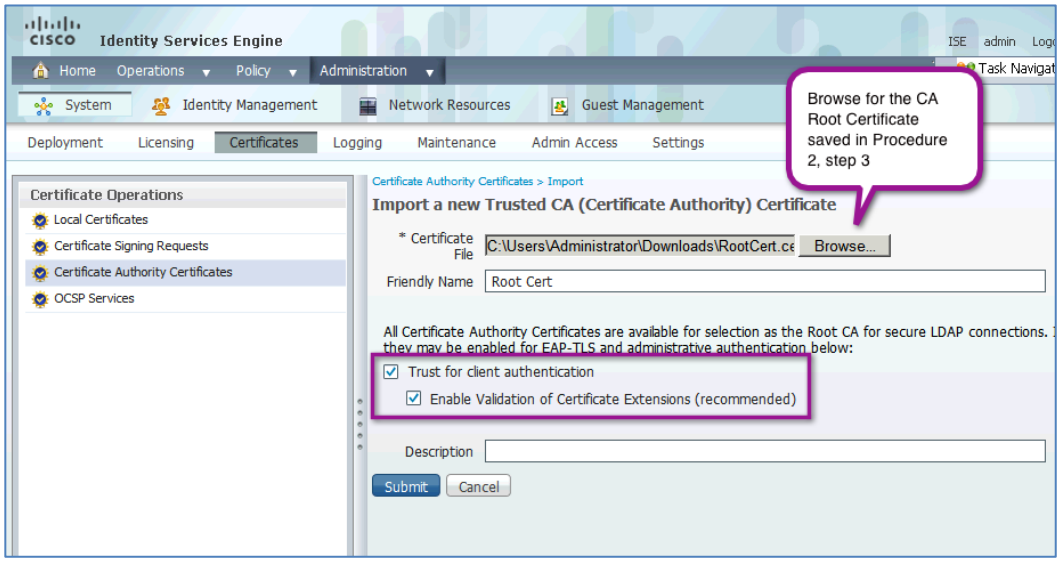
Figure 15 Import the Certificate



Step 14 Browse for the CA root certificate saved in Procedure 3, Step 3.

Step 15 Select the checkbox titled "Trust for client authentication," and then the box titled "Enable Validation of Certificate Extensions."

Figure 16 Trust with EAP-TLS



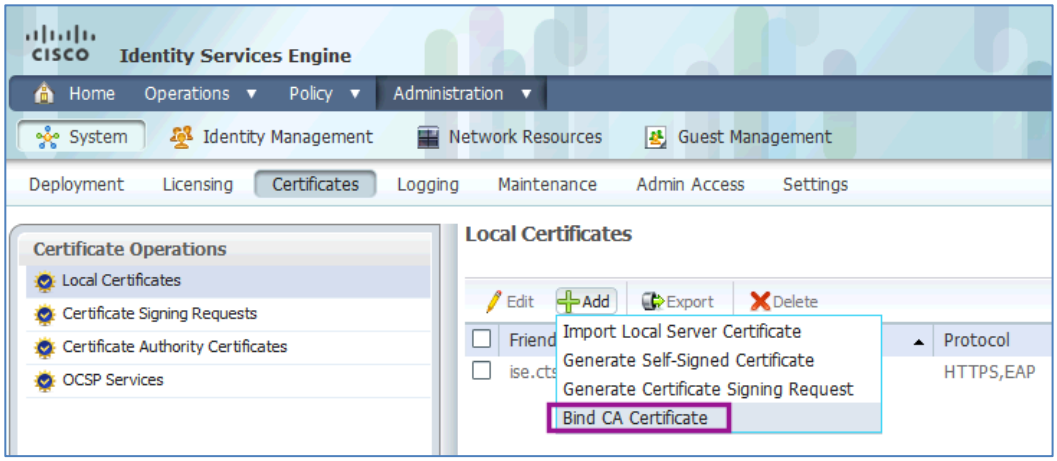
Step 16 Click Submit.

Procedure 3 Install the New Local Certificate

Now that the CA root certificate is trusted, it is time to replace the self-signed certificate with the CA-issued certificate, and delete the completed certificate-signing request (CSR).

Step 1 From Administration → System → Certificates → Local Certificates, click Add → Bind CA Certificate.

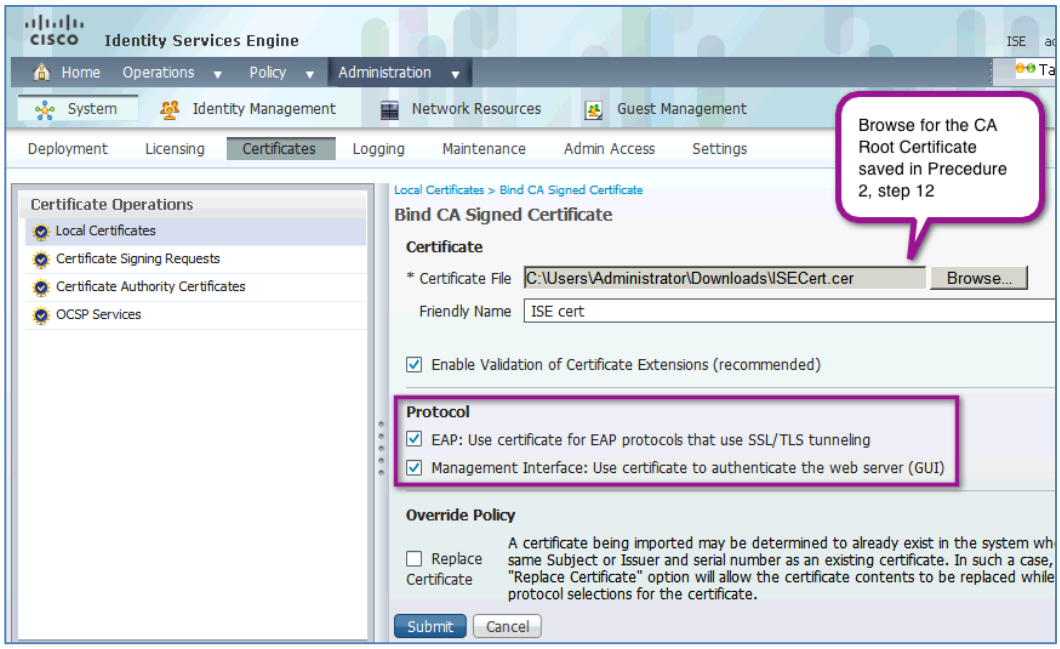
Figure 17 Bind CA Certificate



Step 2 Browse for the certificate issued by the CA for Cisco ISE. Select the EAP and Management Interface checkboxes.

Step 3 Click Submit.

Figure 18 Bind CA Signed Certificate Selection



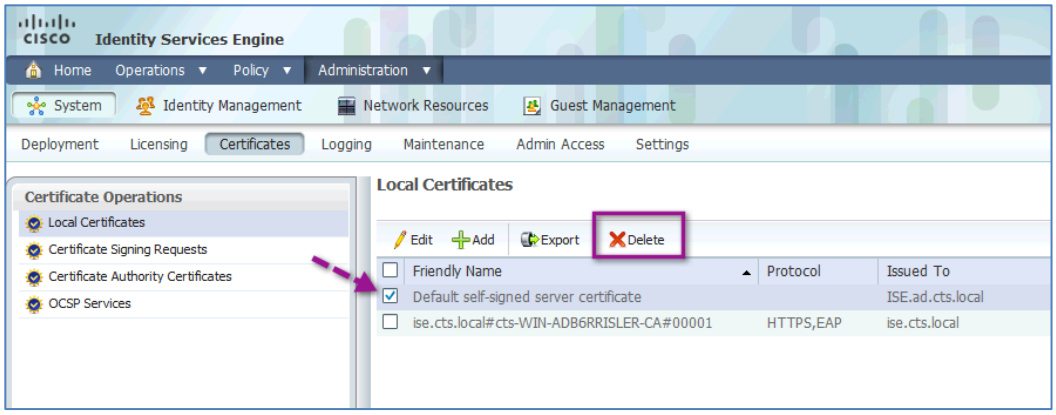
Note: If you did not create the certificate signing request (CSR) with the same host name as the Cisco ISE server (or did not use the same domain name), then you will receive an error message. Delete the old CSR or simply change the host name and start again.

Procedure 4 Clean Up Old Certificates and CSRs

Step 1 Select the checkbox titled "Default self-signed server certificate."

Step 2 Click Delete.

Figure 19 Delete Old Certificate

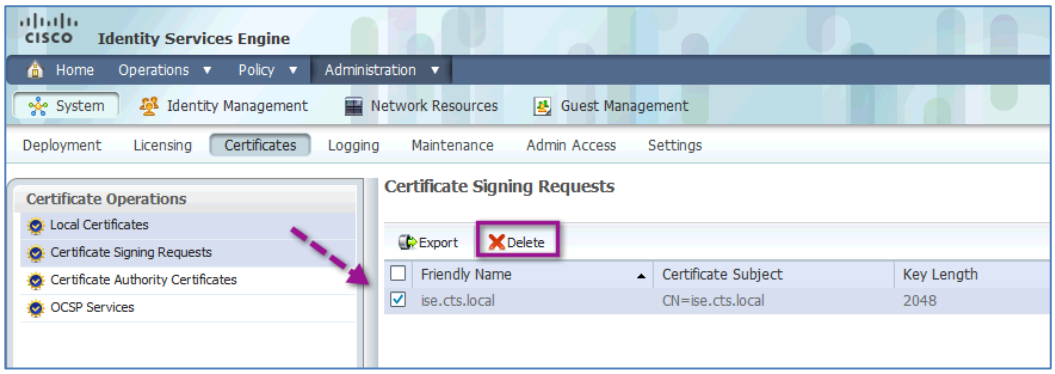


Step 3 Click Certificate Signing Requests.

Step 4 Select the CSR.

Step 5 Click Delete.

Figure 20 Delete Old Signing Request



Add Network Devices

Overview

Any switch or Wireless LAN Controller (WLC) that may be sending RADIUS requests to Cisco ISE to authenticate and authorize network clients should be added to Cisco ISE. Cisco ISE provides a default device that may be configured to allow any network device to send RADIUS requests, but it is not a good security practice to use this feature.

In order to provide a thorough level of policy creation, as well as detailed levels of reporting, it is recommended to add all devices individually to Cisco ISE and to use network device groups (NDGs) to organize those network devices.

Note: For bulk import of network devices and assignment of those devices to their respective NDGs, Cisco ISE provides an import/export mechanism. See the Cisco ISE User Guide (http://www.cisco.com/en/US/docs/security/ise/1.1/user_guide/ise_admin.html) for more detailed instructions.

Cisco ISE Configuration – Add Network Devices

Procedure 1 Configure Network Device Groups

NDGs are powerful tools when used appropriately. Cisco ISE has the power to use any number of attributes when it makes policy decisions. NDG membership is one such attribute that can be used as a policy condition. An example could be the creation of an NDG for switches, another for VPN devices, and a third group for WLCs.

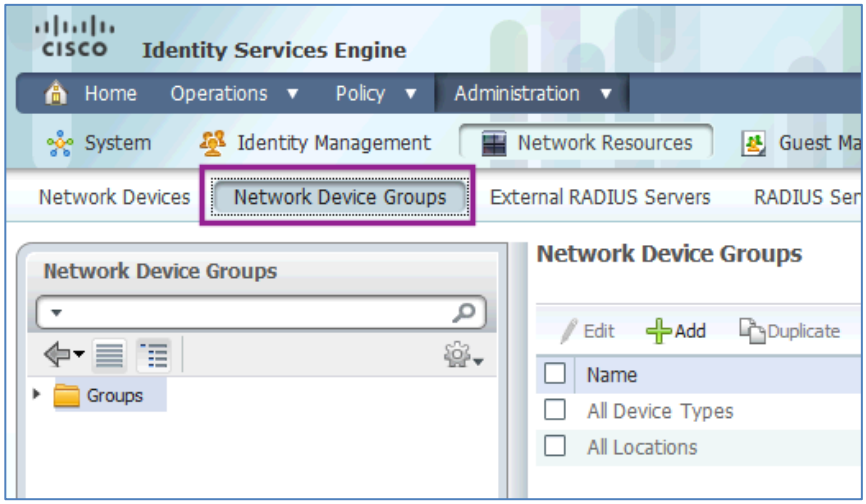
Cisco Best Practice: At a minimum, always use NDGs for device types and location.

Step 1 Go to Administration → Network Resource → Network Device Groups.

By default there are two top-level NDG types: All Device Types and All Locations. These types are a good start for most deployments. Your deployment may need to create multiple location sub-groups. The possibilities are virtually limitless (see the sample hierarchy that follows).

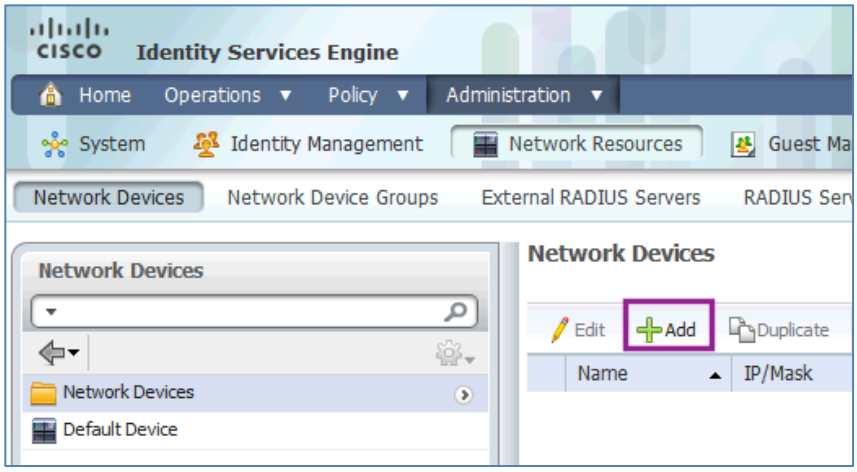
The group structure is hierarchical. With an example group structure of: All Locations → North America → US → SJC → Building M → 1st Floor, you can use any level of the group hierarchy in your policy. In other words, you can select "US" in your policy and get every device in every group underneath "US."

Figure 21 Network Device Groups



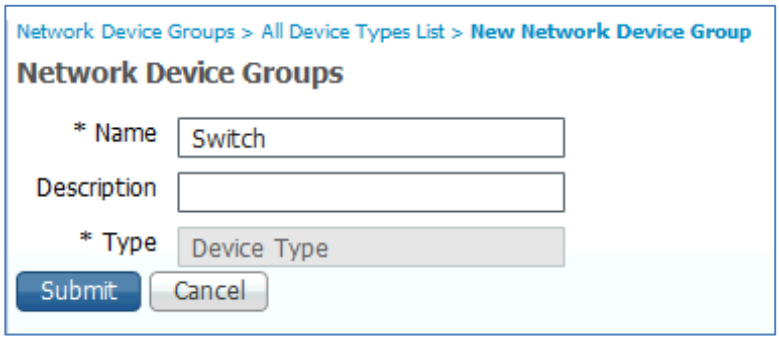
Step 2 Select Network Devices. Click Add.

Figure 22 Add Network Devices



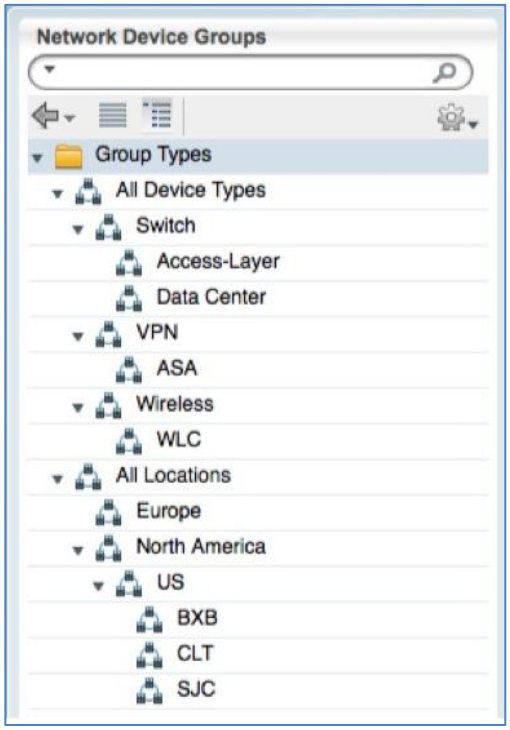
Step 3 Enter the name **Switch** in the Name field and click Submit.

Figure 23 Add a Switch



Step 4 Repeat the process to create your desired NDG hierarchy. Figure 24 depicts an example hierarchy.

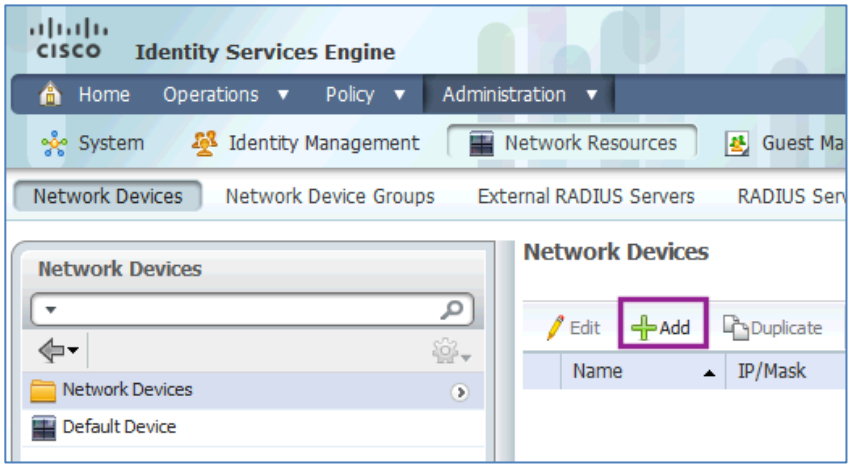
Figure 24 Group Types



Procedure 2 Add Network Device

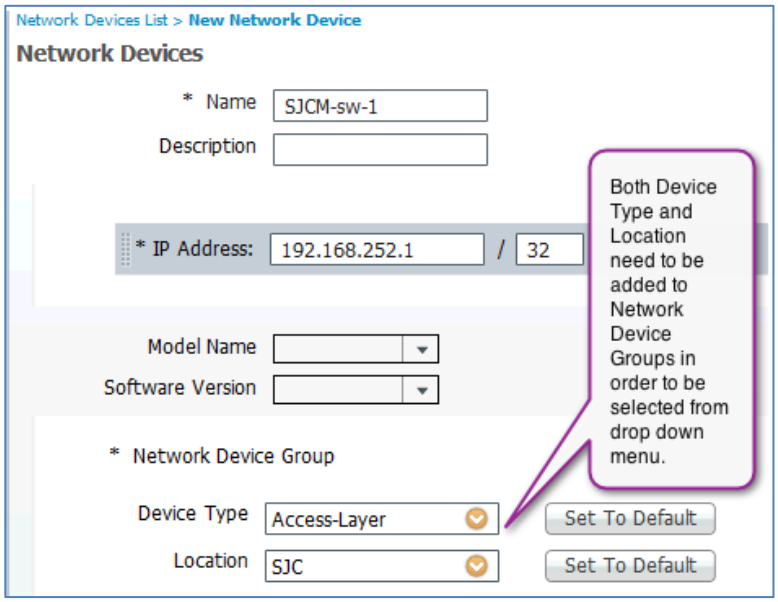
Step 1 Go to Administration → Network Resources → Network Devices and click Add.

Figure 25 Network Devices



Step 2 Fill out the Name, IP Address, and Network Device Group fields.

Figure 26 Network Device Details



Step 3 Repeat for all network devices (also known as "policy enforcement points").

Note: For bulk administration, network devices may be imported via CSV file. See the Cisco ISE User Guide (http://www.cisco.com/en/US/docs/security/ise/1.1/user_guide/ise_admin.html) for more information.

Table 2 Network Devices

Section	Purpose
General Settings	
Name	Use a name that is easy to distinguish later. The name will display in all monitoring, dashboards, and reporting.
Description	Optional
IP Address	Must match the source interface chosen for RADIUS communication in the switch configuration section. Best practice is to use

Section	Purpose
	loopback interfaces for management.
Model Name	Optional
Software Version	Optional
Network Device Group	
Location	Be as specific as possible.
Device Type	Be as specific as possible.
Authentication Settings	
Protocol	Will be prepopulated as RADIUS.
Shared Secret	Must match the RADIUS key configured on the switch.
SNMP Settings (used for device profiling)	
SNMP Version	Select the version in use in your organization.
SNMP RO Community	SNMP is used only for device profiling purposes. Cisco ISE will probe the switch for contents of Cisco Discovery Protocol tables, Link Layer Discovery Protocol (LLDP) tables, and more.
SNMP Username	Used with SNMPv3 – must match the configuration on the switch.
Security Level	Used with SNMPv3 – must match the configuration on the switch.
Auth Protocol	Used with SNMPv3 – must match the configuration on the switch.
Privacy Protocol	Used with SNMPv3 – must match the configuration on the switch.
Polling Interval	It is not recommended to change the default polling interval: 3,600 sec
Link Trap Query	Configures Cisco ISE to accept linkup and linkdown SNMP traps from the switch. Leave this checkbox selected.
MAC Trap Query	Configures Cisco ISE to accept mac-address-table type traps from the switch. Leave this checkbox selected.
Security Group Access (SGA): Not used at this stage of our deployment guide. This will be revisited in the SGA section.	
Device Configuration Deployment: Not used at this stage of our deployment guide. This will be revisited in the SGA section.	

Device Profiling

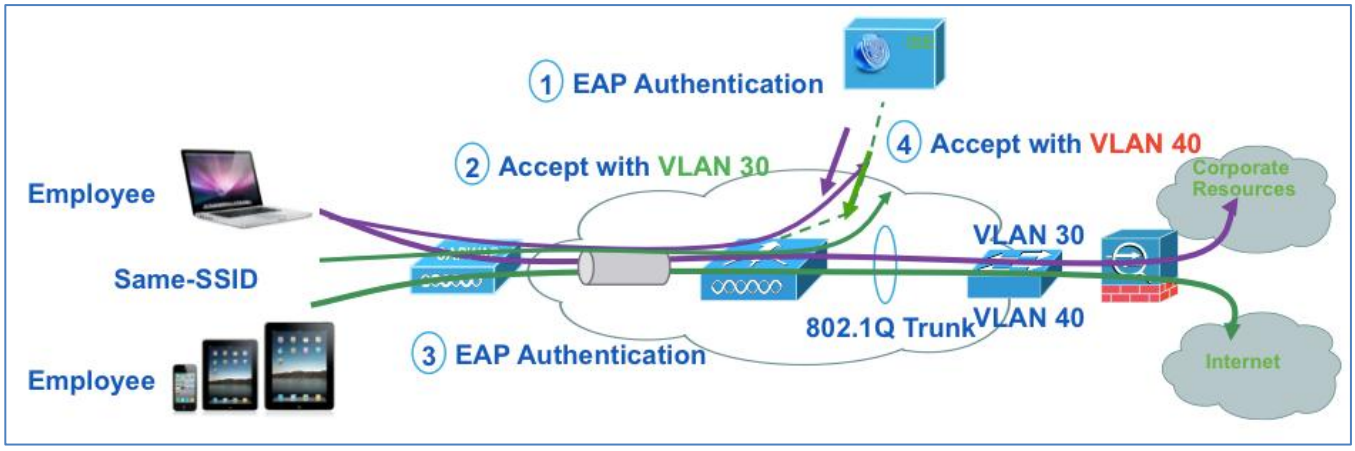
Overview

The Cisco ISE Profiler is responsible for endpoint detection and classification on the ISE platform. It uses an array of probes (sensors) that collect attributes about an endpoint and a policy-based mechanism that evaluates the attributes to match the endpoint with a predefined profile. The result of the collection and classification from the profiler are then used as conditions in the authentication and authorization policies. The classification result of profiling can be used to invoke a different authorization result.

Note: Please see the How-To-30-Profiling_Design_Guide for more details on the probes.

Figure 27 depicts an example of a differentiated device policy based on profiling.

Figure 27 Device Policy Based on Profiling



Users, using the same SSID, can be associated to different wired VLAN interfaces after EAP authentication.

- Employees using corporate laptops with their AD user ID assigned to VLAN 30 = full network access
- Employees using personal iPads/iPhones with their AD user ID assigned to VLAN 40 = Internet only

ISE Configuration – Enable Device Profiling Probes

At this stage we will enable profiling probes on the Cisco ISE device. In a distributed deployment, profiling probes would generally be enabled on all the Policy Services Nodes (PSNs), sometimes referred to as Policy Decision Points or PDPs. The specifics of which probes to enable (and where to enable them) can be complex and should be addressed in the high-level design process.

Note: This guide will not explain how to enable a NetFlow probe. NetFlow is a powerful tool, but its implementation must be thought out carefully. In certain Cisco TrustSec implementations, NetFlow will be crucial. However, an important aspect of NetFlow is understanding what data to send from the infrastructure. This configuration is out of the scope of this guide, but will be in either a specific follow-on guide or in a future version of a Cisco TrustSec implementation guide.

Procedure 1 Enable the Profiling Probes

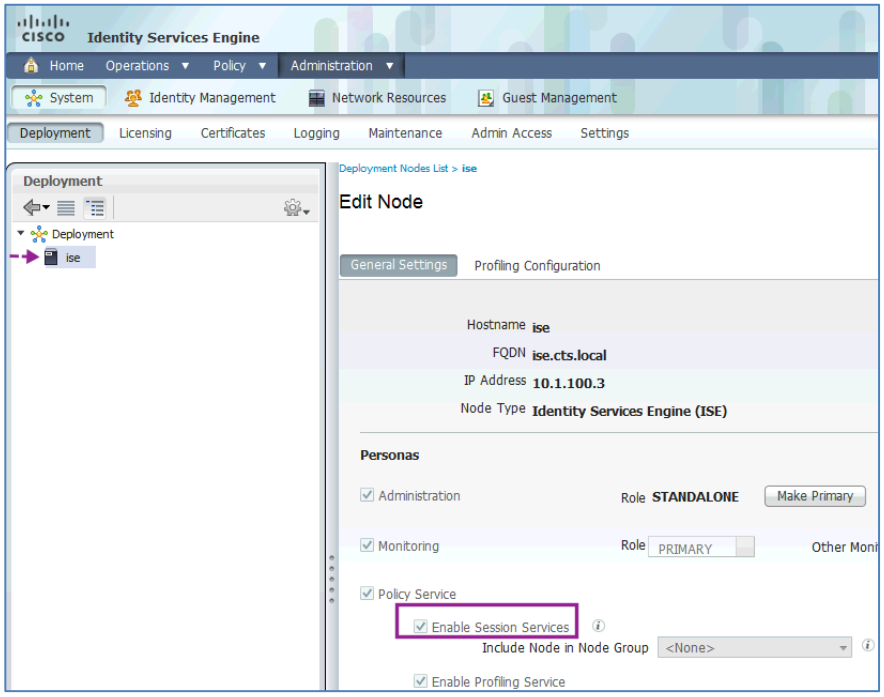
Step 1 Navigate to Administration → System → Deployment.

Step 2 Select the Policy Services Node.

This node may be a single Cisco ISE node, as depicted in Figure 28. If your Cisco TrustSec deployment is distributed, you should select one of the nodes configured for policy service. Repeat these steps for each PSN in the deployment.

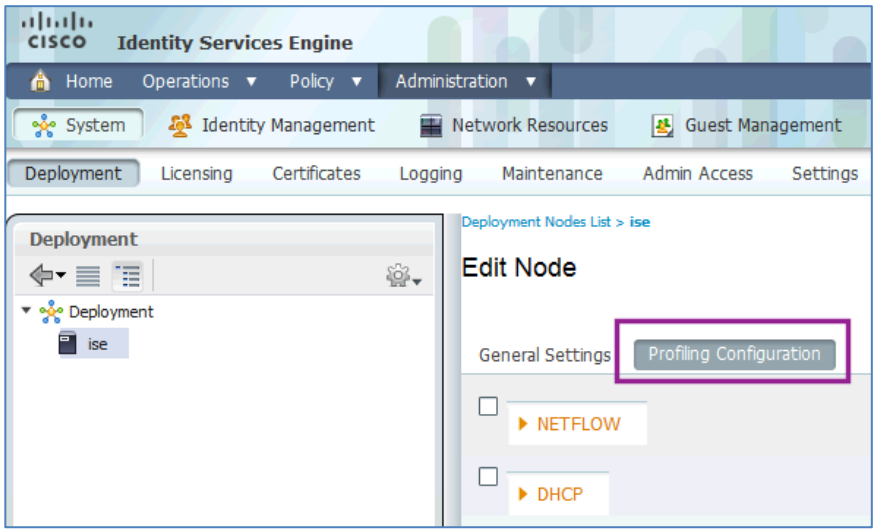
Step 3 Check Enable Session Service.

Figure 28 Select the Policy Services Node



Step 4 Click the Profiling Configuration tab.

Figure 29 Profiling Configuration

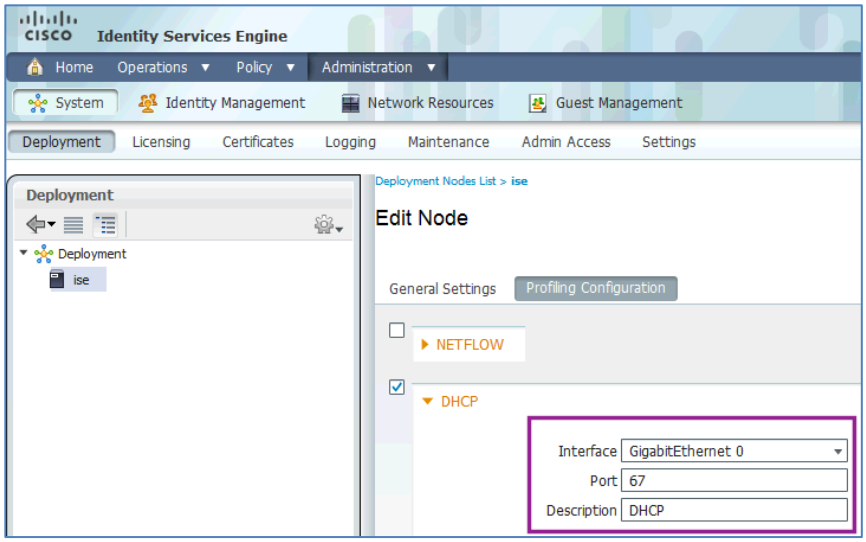


Step 5 Enable the checkbox for DHCP.

This is the DHCP IP Helper probe. It will listen to packets forwarded to it from the DHCP IP Helper configured on the switch or other Layer 3 device. The DHCP IP Helper probe will listen to traffic from the DHCP client to server only (DHCPDISCOVER and DHCPREQUEST).

Enable this probe on a particular interface or on all interfaces.

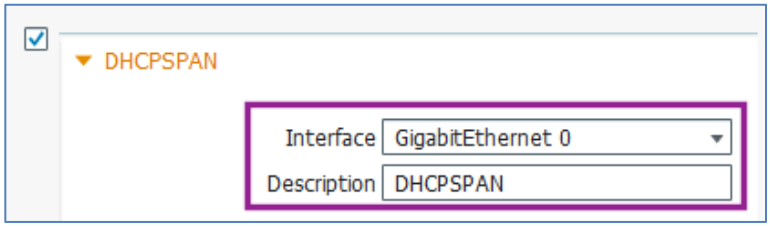
Figure 30 Enable DHCP



Step 6 Enable the checkbox for DHCPSPAN.

The DHCP Span probe will listen to packets forwarded to it from the switchport analyzer (SPAN) session configured on the switch. This probe will listen to all of the DHCP traffic.

Figure 31 Enable DHCPPSAN



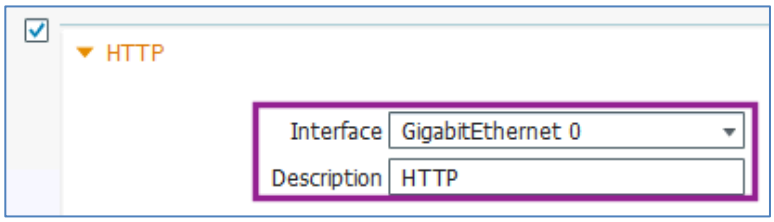
When a switchport is configured to be a SPAN destination, the port no longer functions normally. The interface connected to the SPAN destination port is expected to be in "promiscuous mode," meaning the interface is expected to be capturing all traffic that enters the port, and will not respond to directed communications.

With that understanding, it is recommended that one or more of the Cisco ISE server interfaces be set to promiscuous mode for the DHCPSPAN and HTTP probes. In this guide, we will dedicate the GigabitEthernet 1 interface to be a SPAN destination.

Note: When using an interface on the Cisco ISE other than GigabitEthernet 0, enter the CLI and type **no shutdown** at interface configuration mode to enable the interface. Please see the "Add Network Devices" procedure for the switch configuration. To configure the SPAN (monitor session) on the switchport, please see the "Configure the SPAN Session on the Switch" procedure.

Step 7 Enable the checkbox for HTTP.

Figure 32 Enable HTTP



The HTTP Span probe will listen for HTTP packets on the specified interface and parse them to augment endpoints with HTTP attributes. The HTTP probe will capture traffic emanating from the endpoint and going to port 80 to detect what user agent and other HTTP attributes are present within the HTTP request.

The HTTP data is important for, among other things, mobile device recognition. Use of HTTP will also require some design consideration and should be a part of the High-Level Design.

Step 8 Enable the checkbox for RADIUS.

The RADIUS probe will help detect endpoints based on RADIUS information. It is also used to receive profiling data from the device sensors in Cisco IOS routers and WLCs.

Figure 33 Enable RADIUS

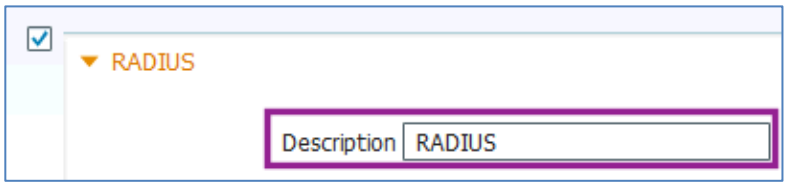


Table 3 lists known attributes collected by the RADIUS probe. The RADIUS probe helps detect endpoints based on RADIUS information.

Table 3 Attributes Collected by RADIUS Probe

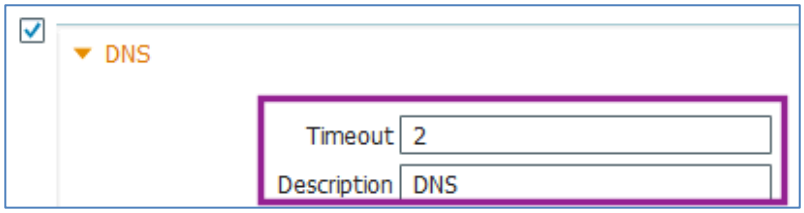
User-Name	Framed-IP-Address	Acct-Session-Time
NAS-IP Address	Calling-Station-ID	Acct-Terminate-Cause
NAS-Port	Acct-Session-ID	

Note: The RADIUS probe may also trigger DNS and SNMP Query collection events (if enabled).

Step 9 Enable the checkbox for DNS.

The DNS probe in your Cisco ISE deployment allows the profiler to look up an endpoint and get the fully qualified domain name (FQDN) of that endpoint.

Figure 34 Enable DNS



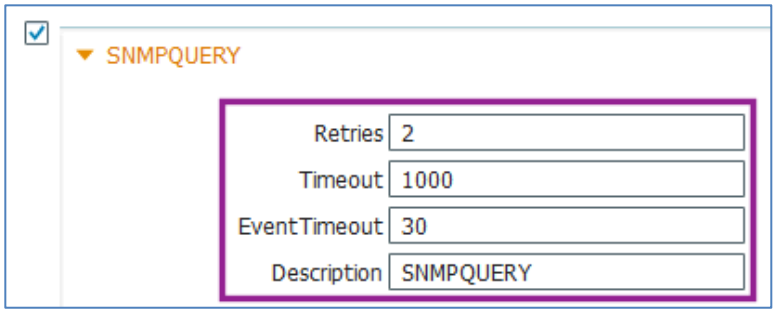
A reverse DNS lookup will be completed only when an endpoint detected by the DHCP, RADIUS, HTTP, and SNMP probes contains the respective attributes listed in Table 4. So, for DNS lookup, at least one of the probes listed in Table 4 needs to be enabled along with the DNS probe.

Table 4 Probes That Need to Be Enabled

Probes That Need to Be Enabled
DHCP IP Helper, DHCP Span – “dhcp-requested-address”
RADIUS Probe – “Framed-IP-Address”
SNMP Probe – “cdpCacheAddress”
HTTP Probe – “Source IP”

Step 10 Enable the checkbox for SNMPQUERY.

Figure 35 Enable SNMPQUERY



Note: When you configure SNMP settings on the network devices, you need to also ensure that Cisco Discovery Protocol is enabled on all the ports of the network devices. If you disable Cisco Discovery Protocol on any of these ports, you may not be able to profile properly because you will miss the Cisco Discovery Protocol information about all the connected endpoints.

The SNMPQuery probe polls all of the SNMP-enabled network devices at configured polling intervals. This feature requires the configuration of SNMP parameters in the Add Network Device section.

The SNMPQuery probe queries the following MIBS:

- System
- cdpCacheEntry
- cLApEntry (If device is WLC)
- cldcClientEntry (If device is WLC)

LinkUp/MAC Notification/RADIUS Acct Start event queries:

- Interface data (ifIndex, ifDesc, etc.)
- Port and VLAN data
- Session data (if interface type is Ethernet)
- Cisco Discovery Protocol data (if the device is a Cisco device)

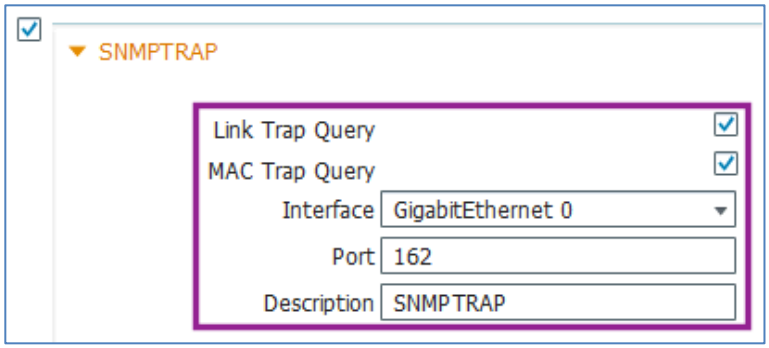
For distributed deployments, NAD polling is distributed among enabled SNMP query probes.

Note: SNMPTrap-triggered queries are queued to the same node for SNMP Query probe. If the local SNMP Query probe is not enabled, those queries are dropped.

Step 11 Enable the checkbox for SNMPTRAP.

The SNMP Trap receives information from the configured NADs that support MAC notification, linkup, linkdown, and informs. For SNMPTrap to be fully functional, you must also enable the SNMPQuery probe. The SNMPTrap probe receives information from the specific NADs when ports come up or go down and endpoints disconnect or connect to your network. The To make this feature functional, you must configure the NAD to send SNMP traps. Information received from the SNMP traps will not create a new endpoint in Cisco ISE, but can be used for profiling.

Figure 36 Enable SNMPTRAP



Note: SNMP informs are supported.

Step 12 Ensure the Link Trap Query and MAC Trap Query options are enabled and click Save.

Note: If you use VMware for the profiling, please refer to the ISE Base Configurations How-To Guide.

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