Campus 802.1X Authentication

Technology Design Guide

August 2014 Series

CISCO VALIDATED DESIGN

Table of Contents

Preface 1

CVD Navigator 2

  Use Cases 2

  Scope 2

  Proficiency 2

Introduction 3

  Technology Use Cases 3

    Use Case: Allowing Only Employees Access to the Network 3

    Use Case: Controlling the Services a User Can Access Based on Group Membership 3

  Design Overview 4

Deployment Details 6

  Enable Authentication 7

    Deploying Cisco Identity Services Engine 7

    Enabling ISE for Network Visibility 25

    Enabling Visibility to the Wired Network 28

    Enabling Visibility to the Wireless Network 30

    Deploying Digital Certificates 35

    Enabling 802.1X Authentication 45

    Configuring Group Policy Objects 58

    Deploying Cisco AnyConnect on Windows Endpoints 81

    Configuring Mac Workstations for 802.1X Authentication 91

    Configure Mac OS X Supplicant 94

  Enable Authorization 94

    Enabling Authorization for Wireless Access Points 95

    Modifying the MAB Authentication Policy 99

    Enabling Authorization for Wired Endpoints 101

    Enabling Authorization for Wireless Endpoints 106

    Modifying the Authorization Policy to be Closed 110

    Enabling EAP Chaining 112

    Enabling Downloadable Access Lists 133

    Enabling Security Group Access 141

    Monitoring Network Access 156

Appendix A: Product List 164

Appendix B: Changes 168

Preface

Cisco Validated Designs (CVDs) present systems that are based on common use cases or engineering priorities. CVDs incorporate a broad set of technologies, features, and applications that address customer needs. Cisco engineers have comprehensively tested and documented each design in order to ensure faster, more reliable, and fully predictable deployment.

CVDs include two guide types that provide tested design details:

- **Technology design guides** provide deployment details, information about validated products and software, and best practices for specific types of technology.
- **Solution design guides** integrate existing CVDs but also include product features and functionality across Cisco products and sometimes include information about third-party integration.

Both CVD types provide a tested starting point for Cisco partners or customers to begin designing and deploying systems.

CVD Foundation Series

This CVD Foundation guide is a part of the *August 2014 Series*. As Cisco develops a CVD Foundation series, the guides themselves are tested together, in the same network lab. This approach assures that the guides in a series are fully compatible with one another. Each series describes a lab-validated, complete system.

The CVD Foundation series incorporates wired and wireless LAN, WAN, data center, security, and network management technologies. Using the CVD Foundation simplifies system integration, allowing you to select solutions that solve an organization's problems—without worrying about the technical complexity.

To ensure the compatibility of designs in the CVD Foundation, you should use guides that belong to the same release. For the most recent CVD Foundation guides, please visit the CVD Foundation web site.

Comments and Questions

If you would like to comment on a guide or ask questions, please use the feedback form.

CVD Navigator

The CVD Navigator helps you determine the applicability of this guide by summarizing its key elements: the use cases, the scope or breadth of the technology covered, the proficiency or experience recommended, and CVDs related to this guide. This section is a quick reference only. For more details, see the Introduction.

Use Cases

This guide addresses the following technology use cases:

- **Allowing Only Employees Access to the Network**—An organization wants to require all devices accessing the network to be authenticated before being allowed access.
- **Controlling the Services a User Can Access Based on Group Membership**—An organization wants to correlate network access policies with business groups.

For more information, see the "Use Cases" section in this guide.

Scope

This guide covers the following areas of technology and products:

- LAN access layer switching
- Onsite and remote-site wireless LAN controllers
- Data center firewalls
- Management and user authentication, authorization, and policy

For more information, see the "Design Overview" section in this guide.

Proficiency

This guide is for people with the following technical proficiencies—or equivalent experience:

- **CCNP Routing and Switching**—3 to 5 years planning, implementing, verifying, and troubleshooting local and wide-area networks
- **CCNP Security**—3 to 5 years testing, deploying, configuring, maintaining security appliances and other devices that establish the security posture of the network
- **CCNP Wireless**—3 to 5 years designing, installing, and troubleshooting wireless LANs

Related CVD Guides

Campus Wired LAN Technology Design Guide

Campus Wireless LAN Technology Design Guide

To view the related CVD guides, click the titles or visit the CVD Foundation web site.

Introduction

Technology Use Cases

With an increasingly mobile workforce and a diverse number of platforms used to gain access to the network, organizations are looking for ways to monitor and control network access. An organization needs to know not only who is accessing their wired and wireless networks, but also when the networks were accessed and from where. In addition, with the wide adoption of devices such as smart phones and tablets and with people bringing their own devices to access the network, organizations need to know how many of these devices are connecting. With this information, the organization can create a policy to prevent connection by nontraditional devices, limit connection to approved devices, or make access to network resources easier for these nontraditional devices.

Organizations are being driven by industry and regulatory compliance (PCI, Sarbanes-Oxley) to be able to report on who is accessing the organization's information, where they are accessing it from, and what type of device they are using to access it. Government mandates such as Federal Information Processing Standard (FIPS) and Federal Information Security Management Act (FISMA) are also requiring agencies and entities working with government agencies to track this information. In some cases, an organization may choose to limit access to certain information in order to adhere to these regulations.

This information is also key data that can be used to generate advanced security policies. Organizations see this as a daunting task requiring the use of several advanced technologies and often delay implementing a solution simply because they don't know where to begin.

This guide is the first step in deploying a complete identity-based architecture. Future projects will address additional use cases that will focus on the features that will provide for things such as enforcement, guest access, and confidentiality.

Use Case: Allowing Only Employees Access to the Network

An organization wants to require all devices accessing the network to be authenticated before being allowed access.

This design guide enables the following network capabilities:

- Identify the types of devices accessing the network
- Authenticate by using 802.1X authentication on the wired and wireless networks for both users and devices
- Monitor the users and devices that are accessing the network, and when they are accessing the network

Use Case: Controlling the Services a User Can Access Based on Group Membership

An organization wants to correlate network access policies with business groups. However, employees can use one of several mobile devices to log in to the wireless network. Additionally, device IP addresses can change as employees move throughout the campus to attend meetings during the day.

This design guide enables the following network capabilities:

- Identify the types of devices accessing the network
- Limit access to the network using access lists and Security Group Tag Access Lists (SGACLs), based on the group to which the employee belongs

Design Overview

Cisco Identity Services Engine (ISE) is an identity and access control policy platform that enables organizations to enforce compliance, enhance infrastructure security, and streamline their service operations. Cisco ISE is a core component of Cisco TrustSec. Its architecture allows an organization to gather real-time contextual information from the network, users, and devices to make proactive policy decisions by tying identity into network elements such as access switches, wireless controllers, and VPN gateways. For more information about Cisco TrustSec, go to:

http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html

This deployment uses Cisco ISE as the authentication, authorization, and accounting server for the wired and wireless networks using RADIUS. Cisco ISE acts as a proxy to the existing Active Directory (AD) services to maintain a centralized identity store for all network services.

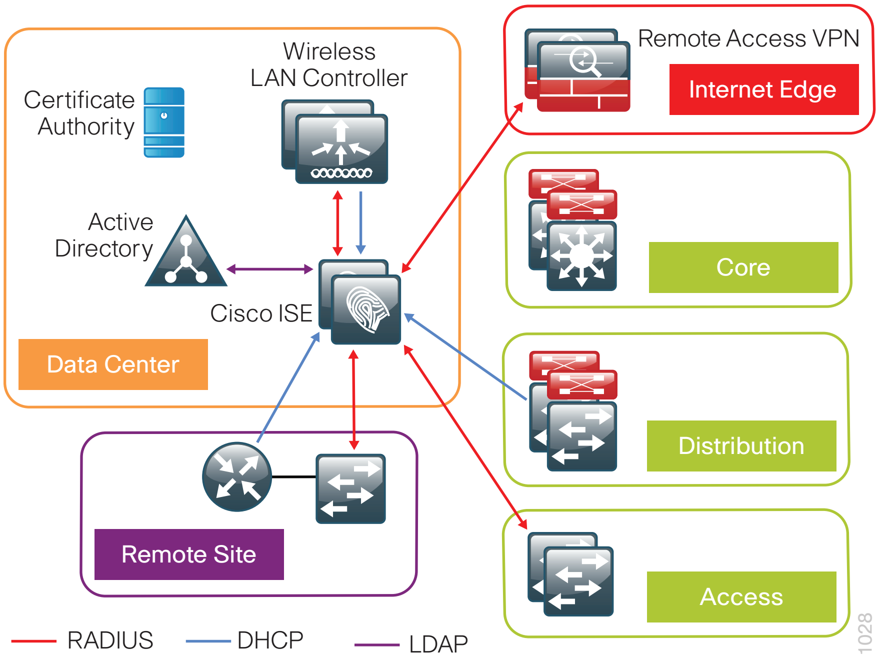
In addition to authentication, this deployment uses Cisco ISE to profile devices in order to determine the specific type of devices that are accessing the network. This is done by examining network traffic for certain criteria, based on certain characteristics. Cisco ISE currently has probes for Dynamic Host Configuration Protocol (DHCP), HTTP, RADIUS, Domain Name System (DNS), Simple Network Management Protocol (SNMP) traps and queries, Network Mapper (Nmap) scans, and Cisco IOS NetFlow. To analyze the traffic, the engine can be deployed as an inline policy enforcement device, or the traffic can be forwarded to the engine. As an example, the network infrastructure is configured to send DHCP and Cisco Discovery Protocol (CDP) data via RADIUS to Cisco ISE for analysis. The engine then evaluates the RADIUS data and can identify the device based off of the data in the RADIUS packet. For example, Cisco IP Phones are identified by their DHCP class identifier.

In the LAN, there are three modes for deploying Cisco TrustSec: monitor mode, low-impact mode, and closed mode. Cisco recommends a phased deployment model that can allow for limited impact on network access while gradually introducing authentication/authorization on the network. An organization's goals might be met by implementing only some of the overall functionality of Cisco TrustSec and a successful deployment does not require all three modes to be deployed. This document covers the deployment phases of monitor mode and low-impact mode both at the headquarters site and the remote sites, with Cisco ISE being centralized in the data center.

The deployment in use deploys two features within Cisco IOS on the switches in the access layer at both the headquarters sites as well as the remote sites. The first is MAC Authentication Bypass (MAB), which authenticates the device on the switch port by the MAC address. Monitor mode logs the MAC addresses that connect and grant access to any device that connects. The second feature is 802.1X open mode, which allows the switch port to give unrestricted access to the network even though authentication and authorization have not been performed. This enables the deployment of identity without affecting existing connectivity. This phased approach allows you to prepare for moving to another mode in the future. In addition to these features, this deployment also deploys the Security Group Access (SGA) features of Security Group Tags (SGT) and Security Group Exchange Protocol (SXP) in low-impact mode in order to enforce the access policy. Packets for a particular group are marked with an SGT in the TrustSec header. SXP is used to pass tagged packets across devices that do not support marking SGTs by binding the IP address of the device to the SGT and then passing the packets along to a device that does support SGTs. Devices then enforce a security policy using these tags.

You accomplish integrating Cisco ISE into the wireless network by using Cisco ISE as the RADIUS server for wireless 802.1X authentication, authorization, and accounting. You configure this on every wireless LAN controller (WLC) in the network, at both headquarters and the remote sites. The one exception is for the controller used for guest access. You can also configure the WLCs to forward DHCP requests to Cisco ISE in order to enable the profiling of wireless endpoints.

Figure 1 - Cisco ISE integration into CVD



Deployment Details

How to Read Commands

This guide uses the following conventions for commands that you enter at the command-line interface (CLI).

Commands to enter at a CLI prompt:

```
configure terminal
```

Commands that specify a value for a variable:

```
ntp server 10.10.48.17
```

Commands with variables that you must define:

```
class-map [highest class name]
```

Commands at a CLI or script prompt:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
police rate 10000 pps burst 10000
packets conform-action
```

Noteworthy parts of system output (or of device configuration files) are highlighted:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

The deployment described here bases all IP addressing off of the Campus Wired LAN Technology Design Guide. IP addresses used in this guide are examples; you should use addressing that is applicable to your architecture.

Cisco ISE has different personas, or modes, for which it can be configured: administration, policy service, and monitoring. For a standalone configuration where the appliance is all personas, the maximum number of endpoints that can be supported is 10,000—dependent upon the installation hardware. To support a greater number of endpoints, to add additional resiliency, or to distribute policy services, you divide the personas across multiple appliances. In this example, there are four nodes. Two nodes run both Administration and Monitoring personas: one is primary for these personas and one is secondary. Two additional nodes run the Policy Service persona. This configuration offers resiliency, and allows the deployment to scale to 10,000 endpoints, for some hardware choices. To scale beyond 10,000 endpoints, all personas must be deployed on dedicated appliances.

You can use shorthand references for the nodes. A node that runs the Administration persona is called a Policy Administration Node (PAN). A node that runs the Monitoring persona is called a Monitoring and Troubleshooting Node (MnT). A node that runs the Policy Service persona is called a Policy Service Node (PSN).

Table 1 - Cisco ISE node IP addresses and hostnames

Device Persona	Shorthand	IP address	Hostname
Cisco ISE primary Policy Administration Node and primary Monitoring and Troubleshooting node	Primary PAN/MnT	10.4.48.41	ise-1.cisco.local
Cisco ISE secondary Policy Administration Node and secondary Monitoring and Troubleshooting node	Secondary PAN/MnT	10.4.48.42	ise-2.cisco.local
Cisco ISE Policy Service Node	First PSN	10.4.48.43	ise-3.cisco.local
Cisco ISE additional Policy Service Node	Additional PSN	10.4.48.44	ise-4.cisco.local

Enable Authentication

PROCESS

Deploying Cisco Identity Services Engine

1. Install primary engine
2. Install the remaining nodes
3. Configure certificate trust list
4. Configure Cisco ISE deployment nodes
5. Add RADIUS profiling to the Cisco ISE deployment nodes
6. Install Cisco ISE license
7. Configure network devices in Cisco ISE
8. Configure Cisco ISE to use Active Directory

Procedure 1 Install primary engine

Step 1: Boot the Cisco ISE and then, at the initial prompt, enter **1**.

```
      Welcome to the Cisco Identity Services Engine Installer
      Cisco ISE Version: 1.2.1.198

Available boot options:
  [1] Cisco ISE Installation (keyboard/Monitor)
  [2] Cisco ISE Installation (Serial Console)
  [3] Recover administrator password (keyboard/Monitor)
  [4] Recover administrator password (Serial Console)
<Enter> Boot existing OS from hard disk.

Enter boot option and press <Enter>.
boot: 1
```

Step 2: At the localhost login prompt, enter **setup.** The installation begins.

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

Step 3: Enter the host name, IP address, subnet mask, and default gateway of the engine.

```
Enter hostname[]: ise-1
Enter IP address[]: 10.4.48.41
Enter IP netmask[]: 255.255.255.0
Enter IP default gateway[]: 10.4.48.1
```

Step 4: Enter DNS information.

```
Enter default DNS domain[]: cisco.local
Enter primary nameserver[]: 10.4.48.10
Add secondary nameserver? Y/N [N]: N
```

Step 5: Configure time.

```
Enter NTP server[time.nist.gov]: ntp.cisco.local
Add another NTP server? Y/N [N]: N
Enter system timezone[UTC]: PST8PDT
```

Tech Tip

Time zone abbreviations can be found in the Cisco Identity Services Engine CLI Reference Guide, Release 1.2.

Step 6: Configure secure shell access and the administrator account.

You must configure an administrator account in order to access to the CLI console. The password must have at least one uppercase character. You also enable SSH access to the CLI.

```
Enable SSH service? Y/N [N]: Y
Enter username[admin]: admin
Enter password: [password]
Enter password again: [password]
```

Tech Tip

The Cisco ISE administrator password expires by default every 45 days. You can reconfigure the default lifetime for administrator passwords. You can reset the password from the CLI by using SSH to issue the **application reset-password ise [user account]** command.

Cisco ISE completes the installation and reboots. This process takes from several minutes to over an hour, depending on available resources. Do not press **Control-C** during the installation, or the installation aborts.

The first ISE node is now installed.

Procedure 2 Install the remaining nodes

The procedure for setting up the remaining nodes is the same as for the first, with the only difference being the IP address and host name configured for the node. To set up the remaining nodes, follow Procedure 1, “Cisco ISE integration into CVD,” and use the values supplied in Table 1 for the remaining nodes.

Procedure 3 Configure certificate trust list

The nodes use public key infrastructure (PKI) to secure communications among them. Initially in this deployment, you use local certificates, and you must configure a trust relationship among all of the nodes. To do this, you import the local certificates from the secondary PAN/MnT and the two PSNs into the primary PAN/MnT.

Step 1: In your browser, connect to the secondary node GUI (Example: https://ise-2.cisco.local). If the browser displays any certificate warnings, acknowledge them and continue.

Step 2: Login using the administrator account previously created, and then in **Administration > System**, select **Certificates**.

Step 3: In the Local Certificates window, select the local certificate by selecting the box on the row containing the name of the secondary node, **ise-2.cisco.local**, and then click **Export**.

Step 4: Choose **Export Certificate Only**, and then click **Export.**

Step 5: When the browser prompts you to save the file to a location on the local machine, choose where to store the file and make a note of it. You will be importing this file into the primary PAN/MnT.

Step 6: In a browser, access the primary engine GUI (Example: https://ise-1.cisco.local).

Step 7: In **Administration > System**, select **Certificates**.

Step 8: In the Certificate Operations pane on the left, click **Certificate Store**, and then click **Import**.

Step 9: Next to Certificate File, click **Browse**, and then locate the certificate exported from the secondary engine. It has an extension of .pem. Click **Submit**.

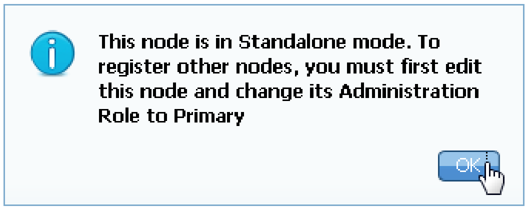
Step 10: Repeat this procedure for the remaining nodes, **ise-3.cisco.local** and **ise-4.cisco.local**, by importing the certificates from the additional nodes into **ise-1.cisco.local**.

Procedure 4 Configure Cisco ISE deployment nodes

You can configure the personas of Cisco ISE—Administration, Monitoring, and Policy Service—to run all on a single server or to be distributed amongst several servers. For this example installation, you deploy a pair of servers to run both the Administration persona and the Monitoring persona, with one serving as primary, the other serving as secondary, and another pair of servers to run the Policy Service persona.

Step 1: Connect and login to the server for the primary Administration and primary Monitoring personas (Example: https://ise-1.cisco.local).

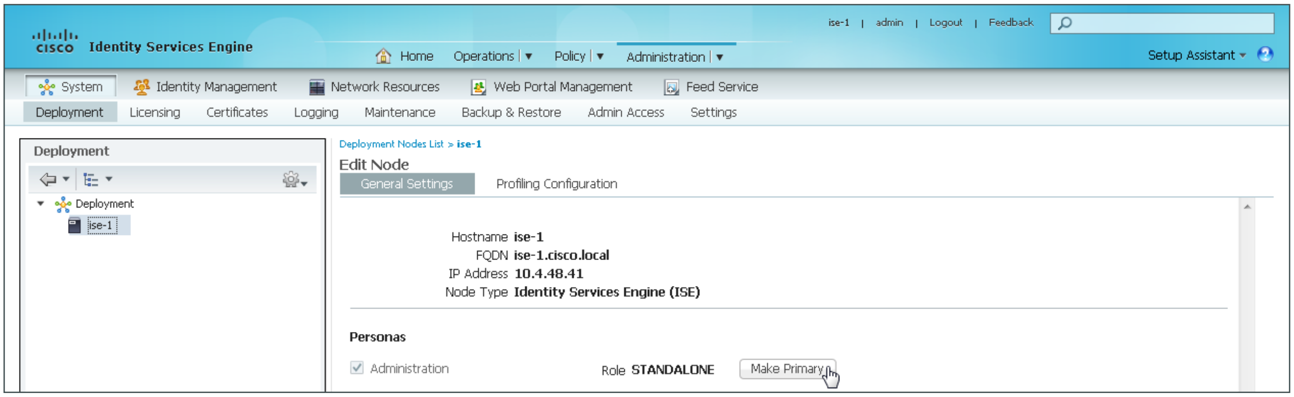
Step 2: From the **Administration** menu, choose **System**, and then choose **Deployment**. A message appears notifying you that the node is currently stand-alone. Click **OK**.


This node is in Standalone mode. To register other nodes, you must first edit this node and change its Administration Role to Primary

Step 3: In the **Deployment** pane on the left, expand **Deployment**. A list of the current deployment nodes appears.

Step 4: Click **ise-1**. This enables you to configure this deployment node.

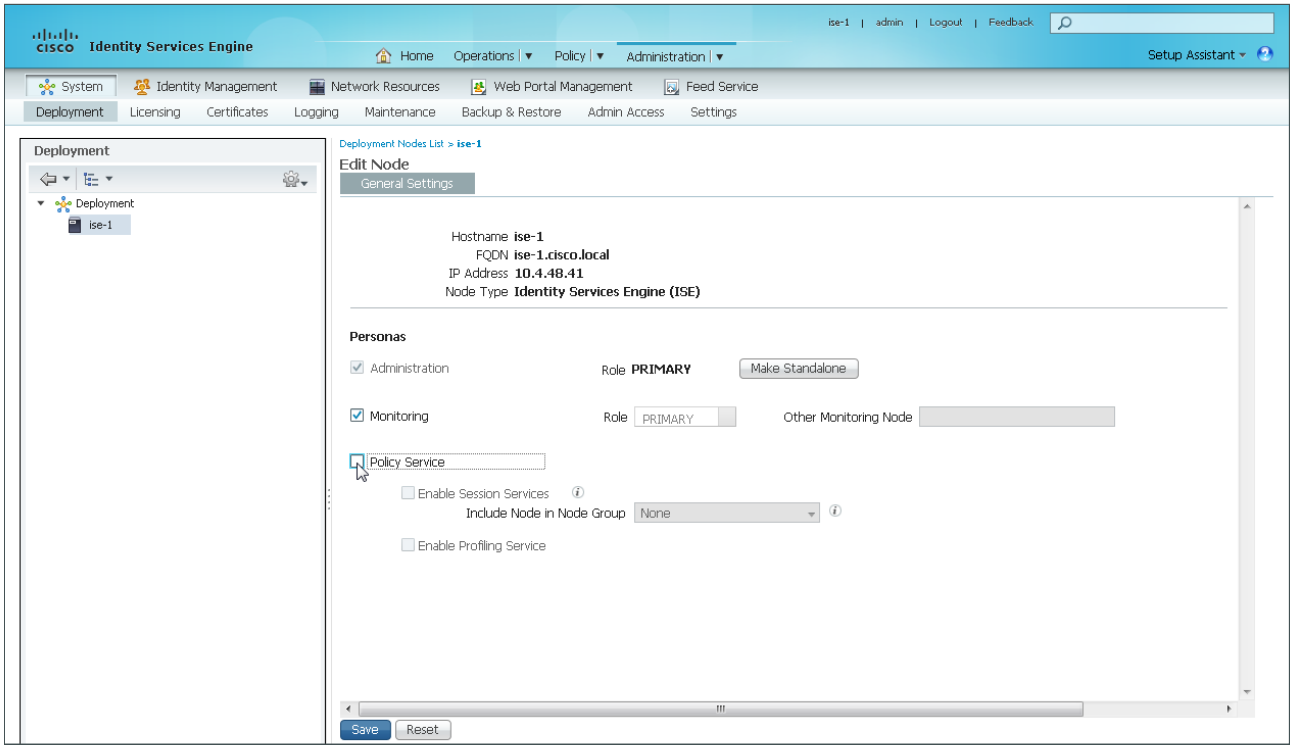
Step 5: On the General Settings tab, in the Personas section, next to the Administration Role, click **Make Primary**.



Hostname ise-1
FQDN ise-1.cisco.local
IP Address 10.4.48.41
Node Type Identity Services Engine (ISE)

☑ Administration Role STANDALONE

Step 6: In the Personas section, clear **Policy Service**, and then, at the bottom, click **Save**.



Hostname ise-1
FQDN ise-1.cisco.local
IP Address 10.4.48.41
Node Type Identity Services Engine (ISE)

☑ Administration Role PRIMARY

☑ Monitoring Role PRIMARY Other Monitoring Node

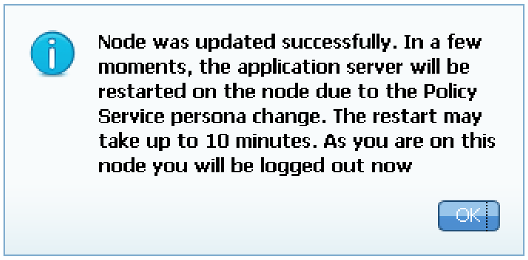
☐ Policy Service

☐ Enable Session Services

Include Node in Node Group None

☐ Enable Profiling Service

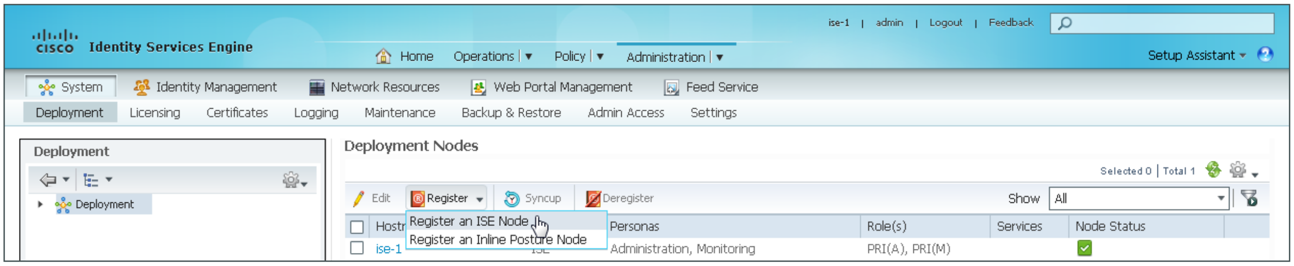
Step 7: You do not need acknowledge the notification that you will be logged out and the server will reboot to update the engine persona, because even without an acknowledgement, the reboot happens automatically.


Node was updated successfully. In a few moments, the application server will be restarted on the node due to the Policy Service persona change. The restart may take up to 10 minutes. As you are on this node you will be logged out now

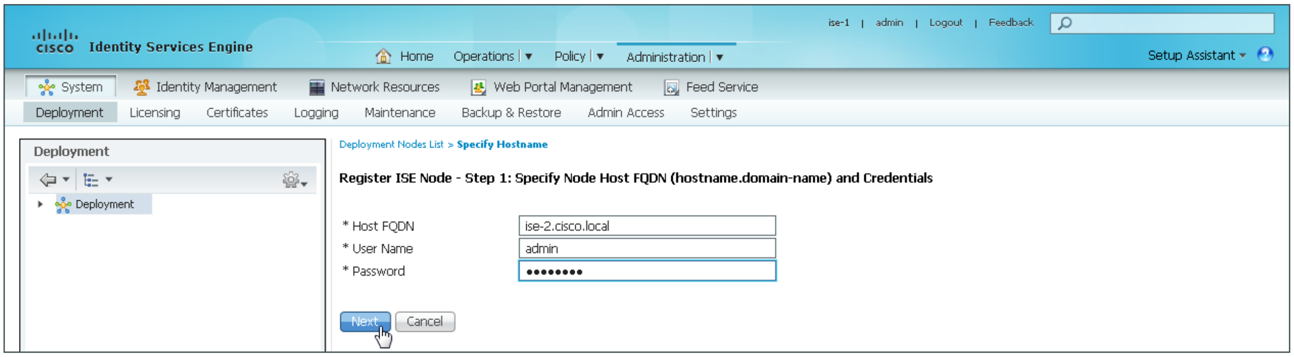
Step 8: After the server has finished rebooting, connect and login to the ISE primary PAN/MnT node (Example: https://ise-1.cisco.local).

Step 9: From the **Administration** menu, choose **System**, and then choose **Deployment**.

Step 10: Under **Deployment Nodes**, select **Register**, and then select **Register an ISE Node**.


cisco Identity Services Engine
ise-1 | admin | Logout | Feedback
Home Operations | ▾ Policy | ▾ Administration | ▾
Setup Assistant ▾
System Identity Management Network Resources Web Portal Management Feed Service
Deployment Licensing Certificates Logging Maintenance Backup & Restore Admin Access Settings
Deployment
Deployment
Deployment Nodes
Selected 0 | Total 1
Edit Register ▾ Syncup Deregister
Show All
Register an ISE Node
Register an Inline Posture Node
Hostr
Personas
Role(s)
Services
Node Status
ise-1
ISE
Administration, Monitoring
PRI(A), PRI(M)

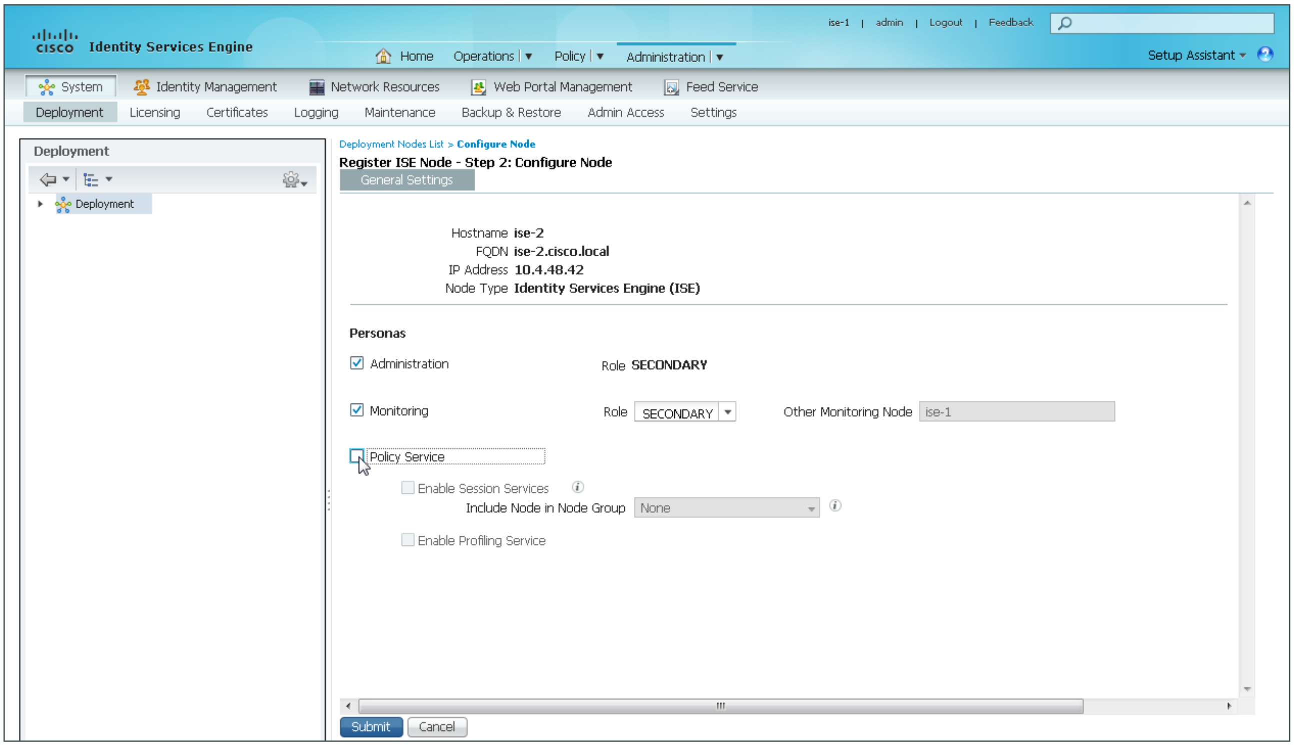
Step 11: Enter the secondary PAN/MnT node FQDN (Example: ise-2.cisco.local), User Name and Password credentials, and then click **Next**.


cisco Identity Services Engine
ise-1 | admin | Logout | Feedback
Home Operations | ▾ Policy | ▾ Administration | ▾
Setup Assistant ▾
System Identity Management Network Resources Web Portal Management Feed Service
Deployment Licensing Certificates Logging Maintenance Backup & Restore Admin Access Settings
Deployment
Deployment
Deployment Nodes List > Specify Hostname
Next
Cancel

Register ISE Node - Step 1: Specify Node Host FQDN (hostname.domain-name) and Credentials

* Host FQDN ise-2.cisco.local
* User Name admin
* Password ••••••••

Step 12: In Register ISE Node - Step 2: Configure Node, under General Settings, clear **Policy Service**, and then click **Submit**.



Identity Services Engine
ise-1 | admin | Logout | Feedback
Home Operations | ▾ Policy | ▾ Administration | ▾
Setup Assistant ▾
System Identity Management Network Resources Web Portal Management Feed Service
Deployment Licensing Certificates Logging Maintenance Backup & Restore Admin Access Settings
Deployment
Deployment
Deployment Nodes List > Configure Node
General Settings
Submit
Cancel

Register ISE Node - Step 2: Configure Node

Hostname ise-2
FQDN ise-2.cisco.local
IP Address 10.4.48.42
Node Type Identity Services Engine (ISE)

Personas

☑ Administration Role SECONDARY

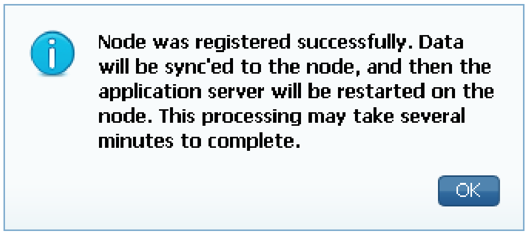
☑ Monitoring Role SECONDARY Other Monitoring Node ise-1

☐ Policy Service

☐ Enable Session Services
Include Node in Node Group None

☐ Enable Profiling Service

The newly added node registers to the primary PAN/MnT, and a success message is displayed.

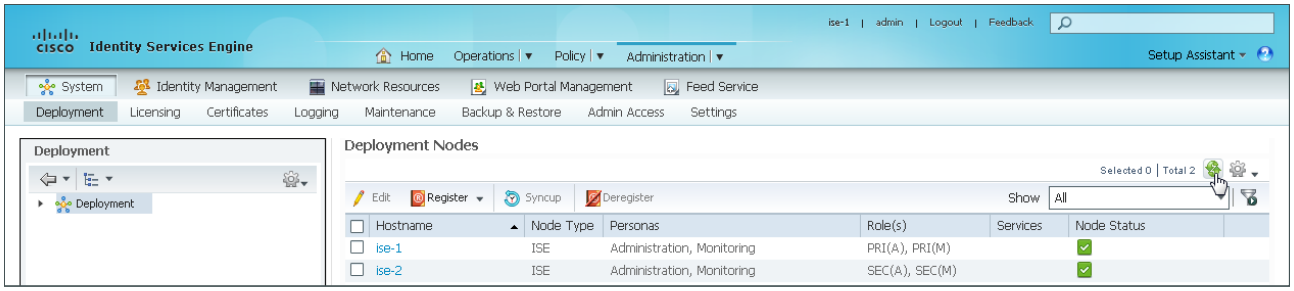


Node was registered successfully. Data will be sync'ed to the node, and then the application server will be restarted on the node. This processing may take several minutes to complete.

Step 13: Click **OK**. The node reboots. The Deployment Nodes list is displayed. This list is also available from the **Administration > System > Deployment**.

Step 14: Click the circular arrow button at the top right and refresh the Deployment Nodes view until you see a green checkmark for the additional server under Node Status.

The Administration and Monitoring servers are now synchronized.



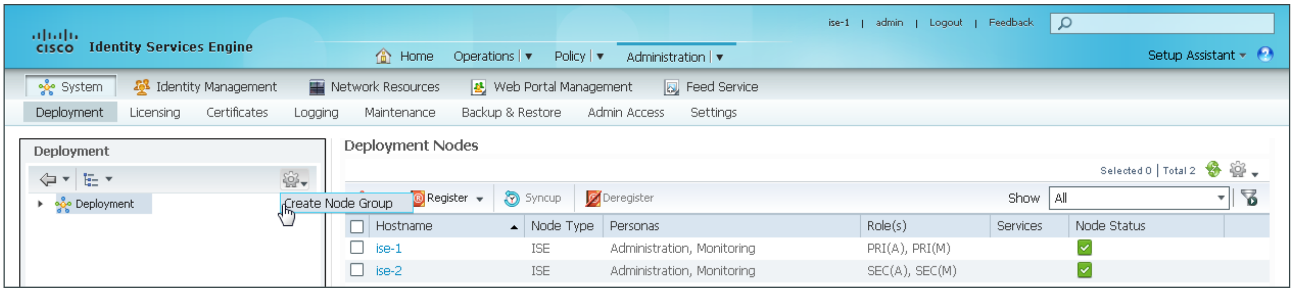
Identity Services Engine
ise-1 | admin | Logout | Feedback
Home Operations | ▾ Policy | ▾ Administration | ▾
Setup Assistant ▾
System Identity Management Network Resources Web Portal Management Feed Service
Deployment Licensing Certificates Logging Maintenance Backup & Restore Admin Access Settings
Deployment
Deployment
Deployment Nodes
Selected 0 | Total 2
Edit Register ▾ Syncup Deregister
Show All

☐	Hostname	Node Type	Personas	Role(s)	Services	Node Status
☐	ise-1	ISE	Administration, Monitoring	PRI(A), PRI(M)		✓
☐	ise-2	ISE	Administration, Monitoring	SEC(A), SEC(M)		✓

You now add the first PSN to the ISE deployment configuration.

Step 15: From the **Administration** menu, choose **System**, and then choose **Deployment**.

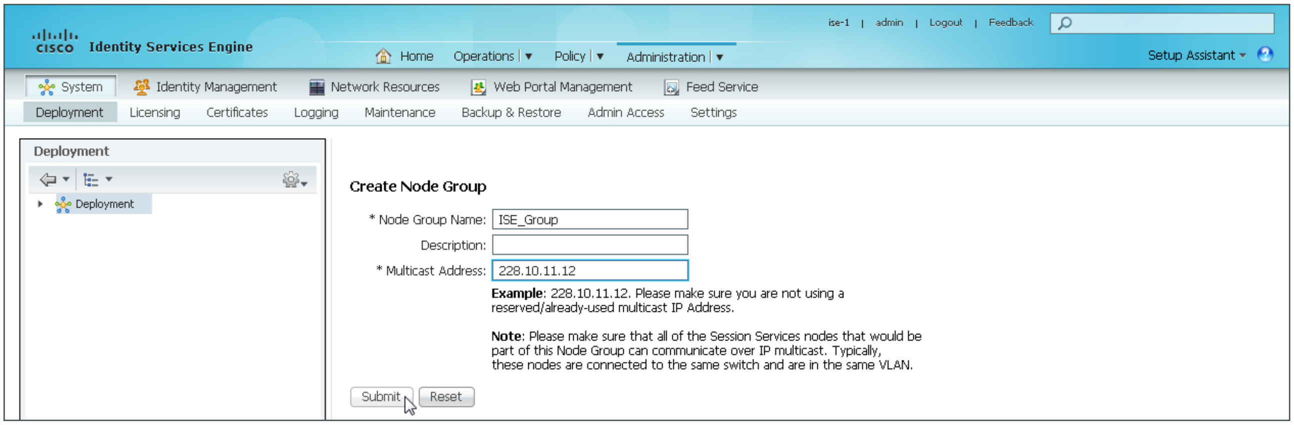
Step 16: In the Deployment pane, click the gear icon, and then select **Create Node Group**.



Hostname	Node Type	Personas	Role(s)	Services	Node Status
ise-1	ISE	Administration, Monitoring	PRI(A), PRI(M)		✓
ise-2	ISE	Administration, Monitoring	SEC(A), SEC(M)		✓

In order for the two Cisco ISE PSNs to replicate information efficiently and to support recovery of orphaned posture pending sessions, they must be in a node group. In this version of ISE, the nodes use IP multicast to distribute this information, so the nodes need to be able to communicate via IP multicast.

Step 17: Configure the node group with the node group name **ISE_Group** and the default multicast address of **228.10.11.12**, and then click **Submit**.



Create Node Group

* Node Group Name: ISE_Group

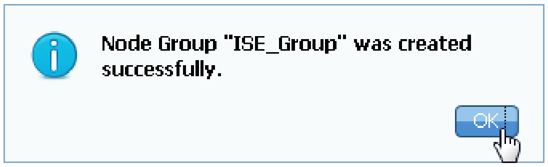
Description:

* Multicast Address: 228.10.11.12

Example: 228.10.11.12. Please make sure you are not using a reserved/already-used multicast IP Address.

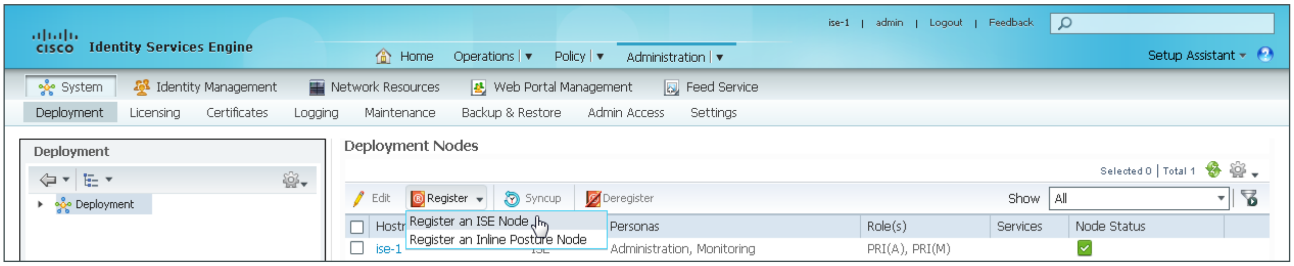
Note: Please make sure that all of the Session Services nodes that would be part of this Node Group can communicate over IP multicast. Typically, these nodes are connected to the same switch and are in the same VLAN.

Step 18: After the pop-up window lets you know the group was created successfully, click **OK**.

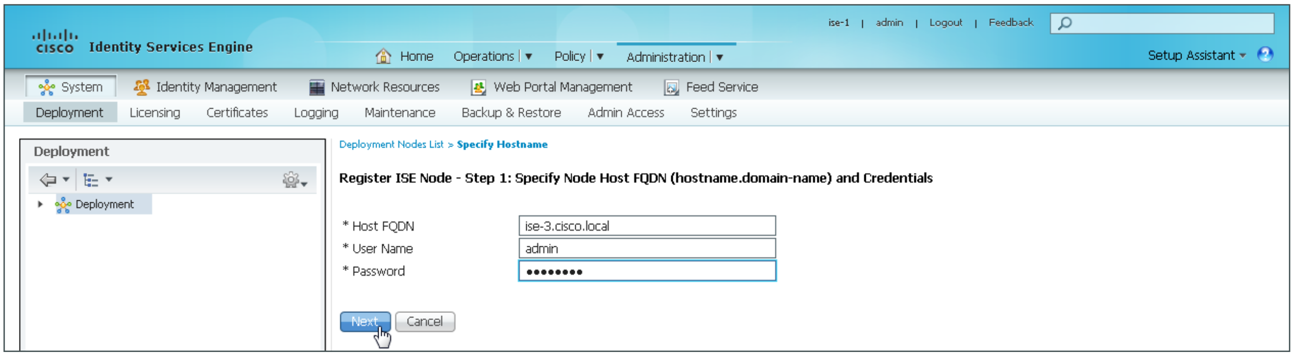


Node Group "ISE_Group" was created successfully.

Step 19: Under **Deployment Nodes**, select **Register**, and then select **Register an ISE Node**.



Step 20: Enter the first PSN FQDN (Example: ise-3.cisco.local), User Name and Password credentials, and then click **Next**.

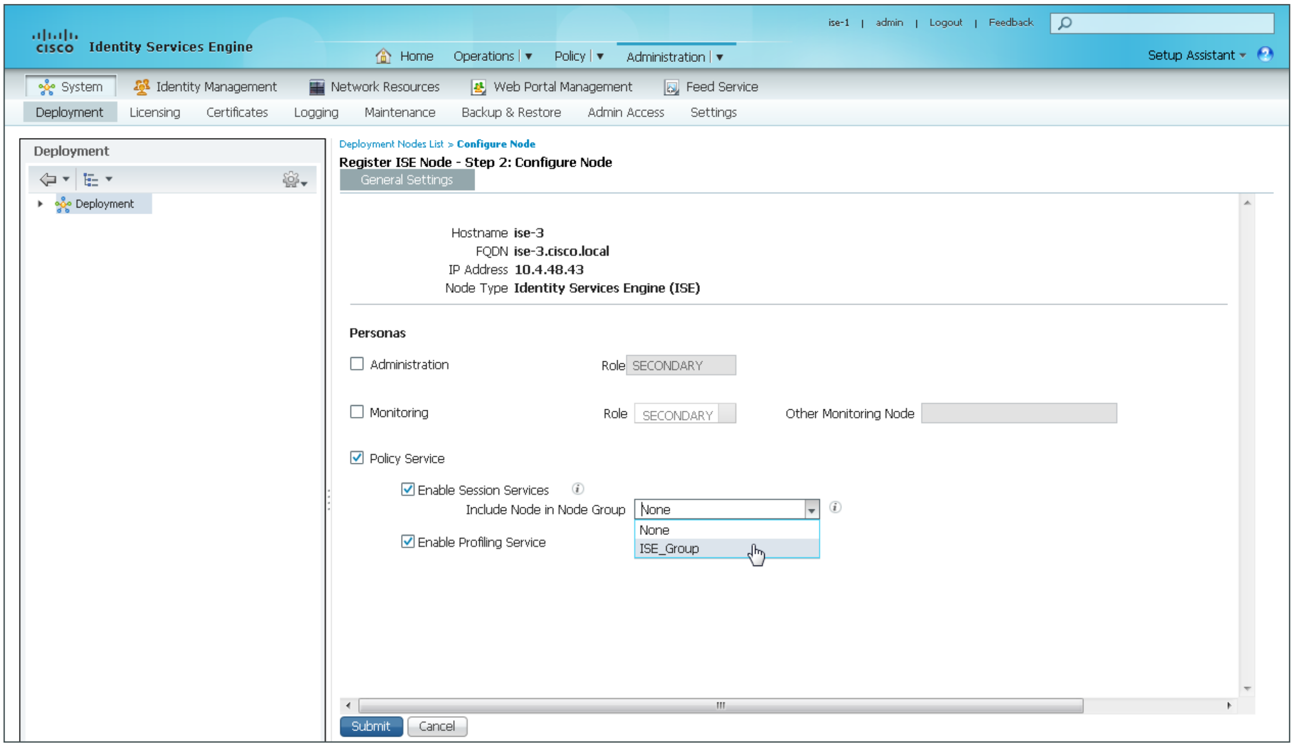


Register ISE Node - Step 1: Specify Node Host FQDN (hostname.domain-name) and Credentials

* Host FQDN ise-3.cisco.local
* User Name admin
* Password ••••••••

Step 21: In Register ISE Node - Step 2: Configure Node, under the General Settings tab in the Personas section, clear **Administration**, and clear **Monitoring.**

Step 22: Next to Include Node in Node Group in the drop-down list, select the node group you created (Example: ISE_Group), leave the other default selections, and then at the bottom, click **Submit**. The newly added node registers to the primary PAN, and a success message appears.



Register ISE Node - Step 2: Configure Node

Hostname ise-3
FQDN ise-3.cisco.local
IP Address 10.4.48.43
Node Type Identity Services Engine (ISE)

Personas

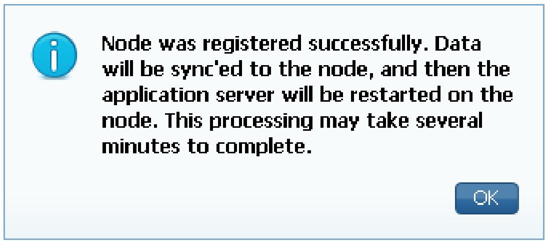
☐ Administration Role SECONDARY

☐ Monitoring Role SECONDARY Other Monitoring Node

☑ Policy Service

☑ Enable Session Services
Include Node in Node Group None

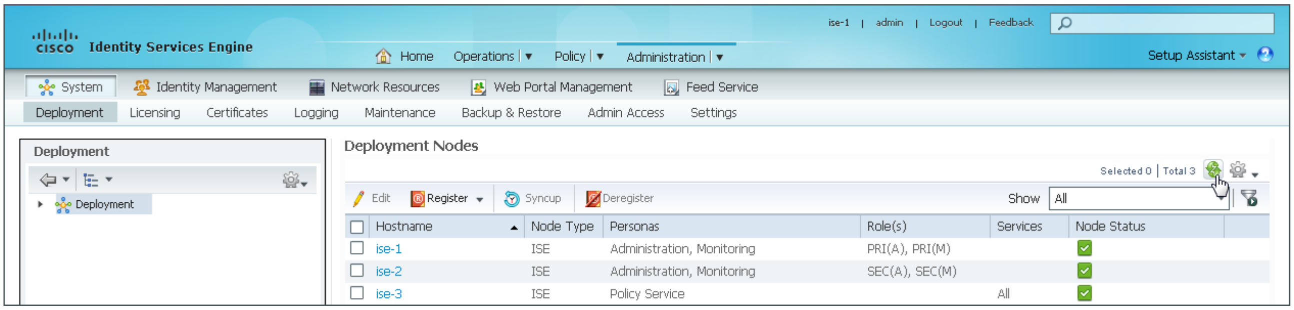
☑ Enable Profiling Service



Node was registered successfully. Data will be sync'ed to the node, and then the application server will be restarted on the node. This processing may take several minutes to complete.

Step 23: Click **OK**. The node reboots. The Deployment Nodes list is displayed. This list is also available from the **Administration > System > Deployment**. Click the circular arrow button at the top right and refresh the Deployment Nodes view until you see a green checkmark for the additional server under Node Status.

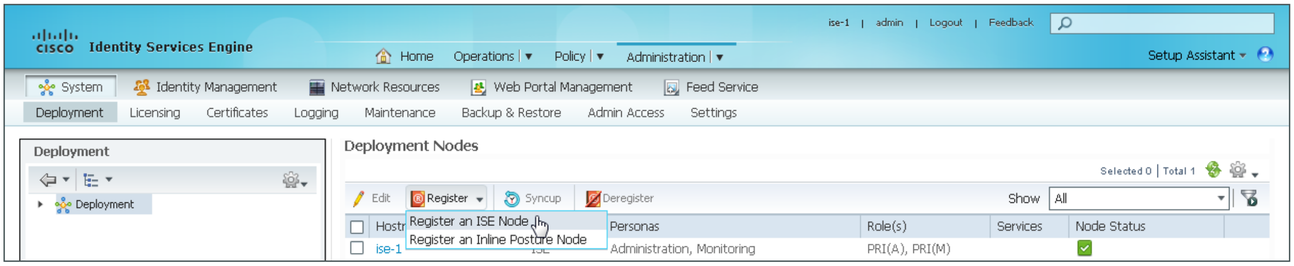
The primary PSN is now synchronized.



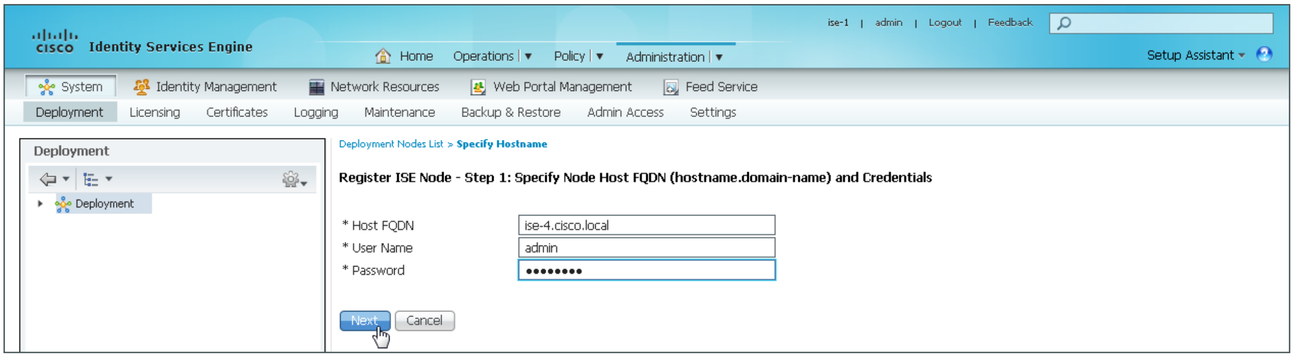
☐	Hostname	Node Type	Personas	Role(s)	Services	Node Status
☐	ise-1	ISE	Administration, Monitoring	PRI(A), PRI(M)		✓
☐	ise-2	ISE	Administration, Monitoring	SEC(A), SEC(M)		✓
☐	ise-3	ISE	Policy Service		All	✓

You now add the additional PSN in order to complete the ISE deployment configuration.

Step 24: Under **Deployment Nodes**, select **Register**, and then select **Register an ISE Node**.



Step 25: Enter the additional PSN FQDN (Example: ise-4.cisco.local) and User Name and Password credentials, and then click **Next**.

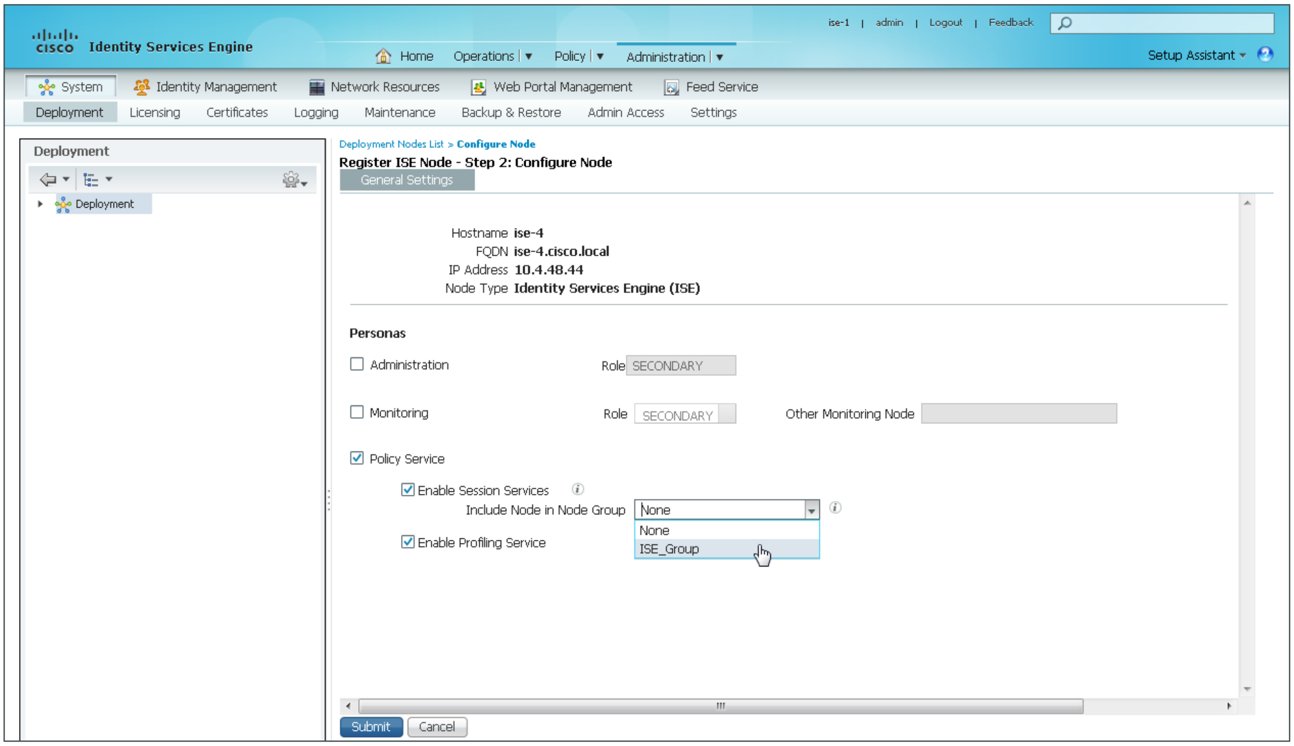


Register ISE Node - Step 1: Specify Node Host FQDN (hostname.domain-name) and Credentials

* Host FQDN: ise-4.cisco.local
* User Name: admin
* Password: ••••••••

Step 26: In Register ISE Node - Step 2: Configure Node, under the General Settings tab in the Personas section, clear **Administration** and **Monitoring.**

Step 27: Next to Include Node in Node Group in the drop-down list, select the node group you created (Example: ISE_Group), leave the other default selections, and then at the bottom, click **Submit**.


Identity Services Engine
ise-1 | admin | Logout | Feedback
Home Operations Policy Administration
Setup Assistant
System Identity Management Network Resources Web Portal Management Feed Service
Deployment Licensing Certificates Logging Maintenance Backup & Restore Admin Access Settings
Deployment
Deployment
Deployment Nodes List > Configure Node
General Settings
Submit
Cancel

Register ISE Node - Step 2: Configure Node

Hostname ise-4
FQDN ise-4.cisco.local
IP Address 10.4.48.44
Node Type Identity Services Engine (ISE)

Personas

☐ Administration Role SECONDARY

☐ Monitoring Role SECONDARY Other Monitoring Node

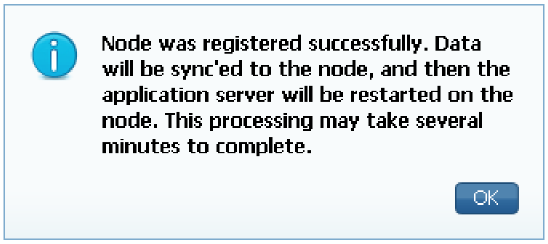
☑ Policy Service

☑ Enable Session Services

Include Node in Node Group None (None, ISE_Group)

☑ Enable Profiling Service

The newly added node registers to the primary PAN, and a success message appears.

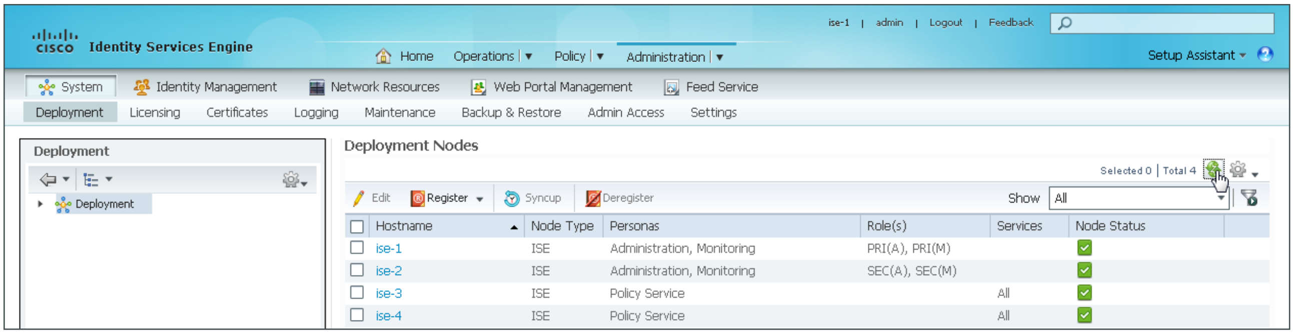


Node was registered successfully. Data will be sync'ed to the node, and then the application server will be restarted on the node. This processing may take several minutes to complete.

Step 28: Click **OK**. The node reboots.

The Deployment Nodes list is displayed. If you have navigated away while the node is booting, this list is also available from the **Administration > System > Deployment**. Click the circular arrow button at the top right and refresh the Deployment Nodes view until you see a green checkmark for the additional server under Node Status.

After a few minutes, all servers are synchronized.


Identity Services Engine
ise-1 | admin | Logout | Feedback
Home Operations Policy Administration
Setup Assistant
System Identity Management Network Resources Web Portal Management Feed Service
Deployment Licensing Certificates Logging Maintenance Backup & Restore Admin Access Settings
Deployment
Deployment
Deployment Nodes
Selected 0 | Total 4
Edit Register Syncup Deregister
Show All

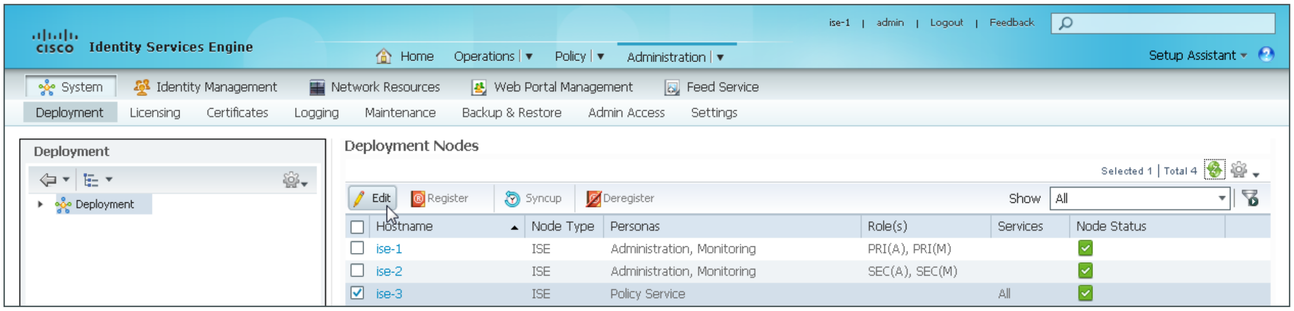
☐	Hostname	Node Type	Personas	Role(s)	Services	Node Status
☐	ise-1	ISE	Administration, Monitoring	PRI(A), PRI(M)		✓
☐	ise-2	ISE	Administration, Monitoring	SEC(A), SEC(M)		✓
☐	ise-3	ISE	Policy Service		All	✓
☐	ise-4	ISE	Policy Service		All	✓

Procedure 5 Add RADIUS profiling to the Cisco ISE deployment nodes

You now configure the methods that are used to profile network endpoints.

Step 1: Navigate to **Administration > System > Deployment**. The Deployment Nodes list is displayed.

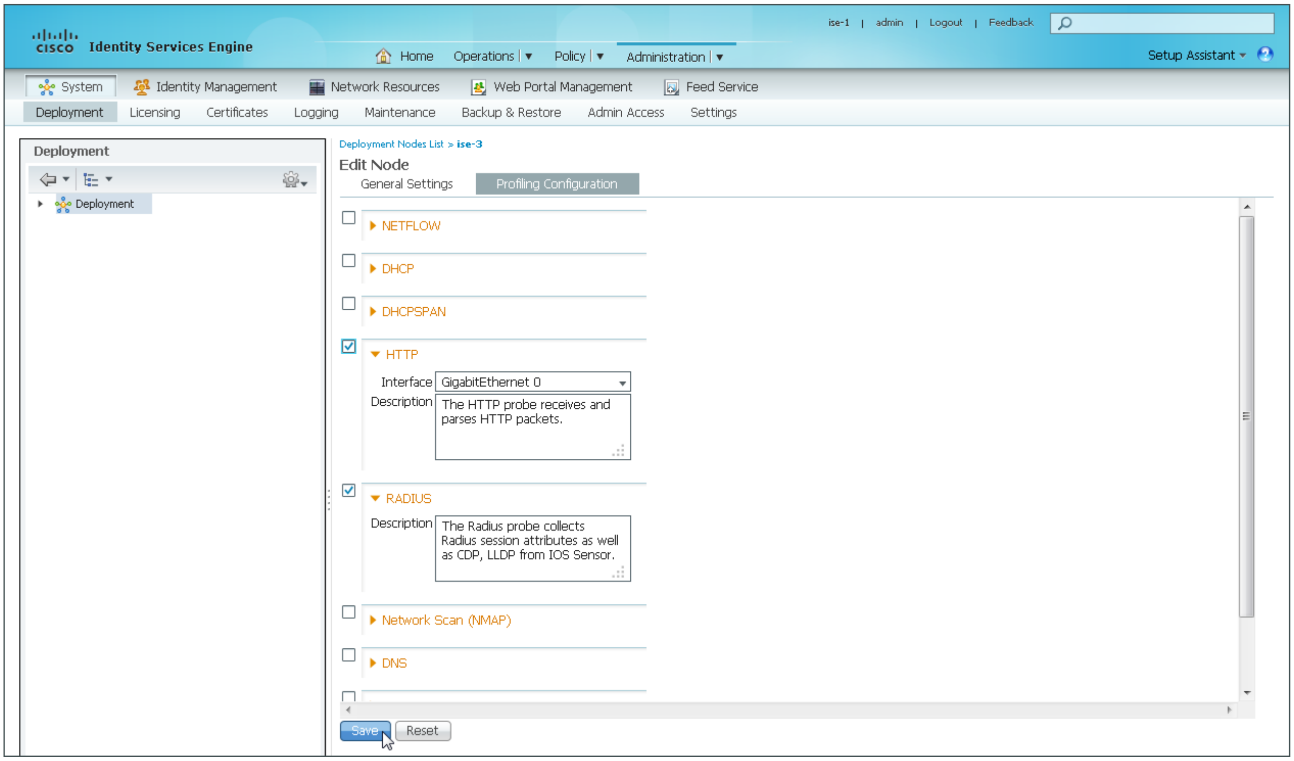
Step 2: Select the first PSN (Example: ise-3), and then click **Edit**.



☐	Hostname	Node Type	Personas	Role(s)	Services	Node Status
☐	ise-1	ISE	Administration, Monitoring	PRI(A), PRI(M)		✓
☐	ise-2	ISE	Administration, Monitoring	SEC(A), SEC(M)		✓
☑	ise-3	ISE	Policy Service		All	✓

Step 3: At the top, under Edit Node, select the **Profiling Configuration** tab.

Step 4: Select **HTTP**. Leave the default parameters unchanged.



☐ NETFLOW

☐ DHCP

☐ DHCPSPAN

☑ HTTP

Interface: GigabitEthernet 0

Description: The HTTP probe receives and parses HTTP packets.

☑ RADIUS

Description: The Radius probe collects Radius session attributes as well as CDP, LLDP from IOS Sensor.

☐ Network Scan (NMAP)

☐ DNS

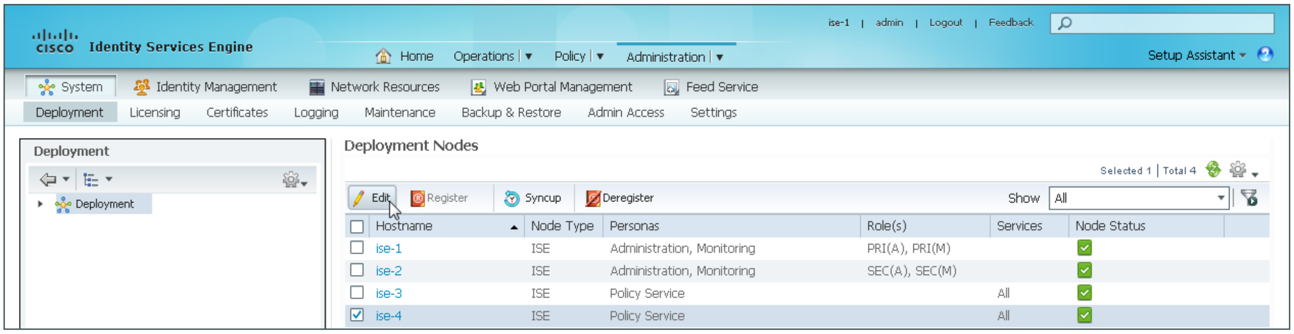
Step 5: Select **RADIUS**. Leave the default description unchanged, and then at the bottom, click **Save**.

The new policy configuration is saved.

Server Response
Node was updated successfully.

Step 6: Navigate to **Administration > System > Deployment**. The Deployment Nodes list is displayed.

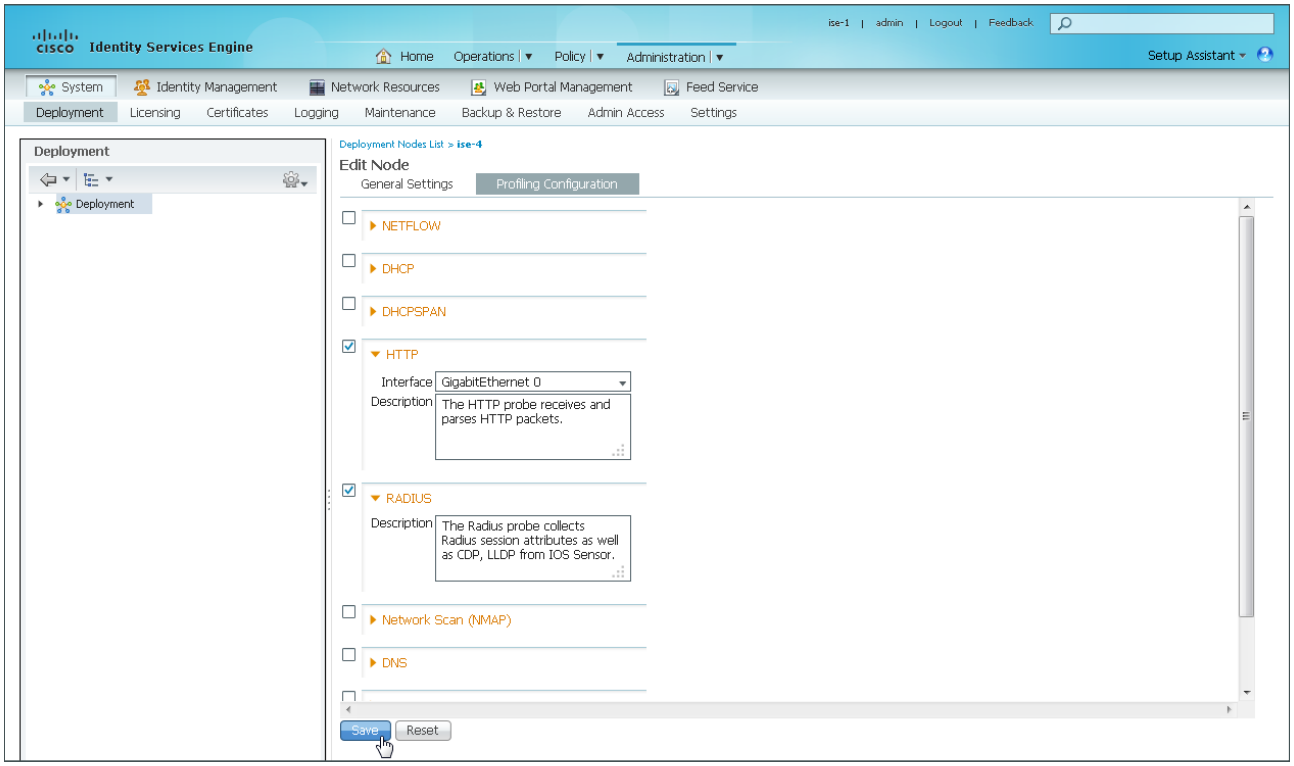
Step 7: Select the additional PSN (Example: ise-4), and then click **Edit**.



☐	Hostname	Node Type	Personas	Role(s)	Services	Node Status
☐	ise-1	ISE	Administration, Monitoring	PRI(A), PRI(M)		✓
☐	ise-2	ISE	Administration, Monitoring	SEC(A), SEC(M)		✓
☐	ise-3	ISE	Policy Service		All	✓
☑	ise-4	ISE	Policy Service		All	✓

Step 8: At the top, under Edit Node, select the Profiling Configuration tab.

Step 9: Select **HTTP**. Leave the default parameters unchanged.



☐ NETFLOW

☐ DHCP

☐ DHCPSPAN

☑ HTTP

Interface: GigabitEthernet 0

Description: The HTTP probe receives and parses HTTP packets.

☑ RADIUS

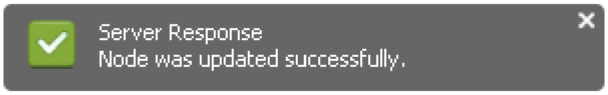
Description: The Radius probe collects Radius session attributes as well as CDP, LLDP from IOS Sensor.

☐ Network Scan (NMAP)

☐ DNS

Step 10: Select **RADIUS**. Leave the default description unchanged, and then at the bottom, click **Save**.

The new policy configuration is saved.



Server Response
Node was updated successfully.

You have now deployed all Cisco ISE nodes: a redundant pair of servers for the PAN/MnT personas and a redundant pair of servers for the PSN persona.

Tech Tip

After you have finished software installation, you should check the release notes to see if there are patches available to apply that are appropriate for the requirements of your organization. After you download any required patches, you can automatically distribute and apply them to all nodes by navigating to **Administration > System > Maintenance**, selecting **Patch Management,** and following the instructions.

Procedure 6 Install Cisco ISE license

Cisco ISE comes with a 90-day demo license for both the Base and Advanced packages. To go beyond 90 days, you need to obtain a license from Cisco. In a redundant configuration, you only need to install the license on the primary administration node.

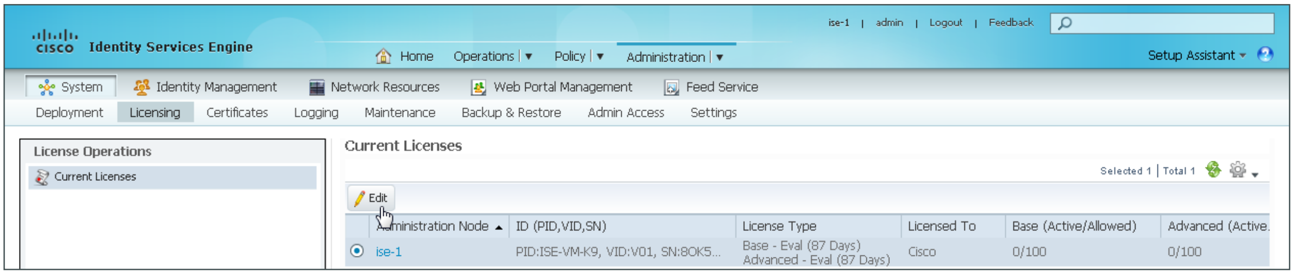
Tech Tip

When installing a Base license and an Advanced license, the Base license must be installed first.

Step 1: Navigate to **Administration > System > Licensing**.

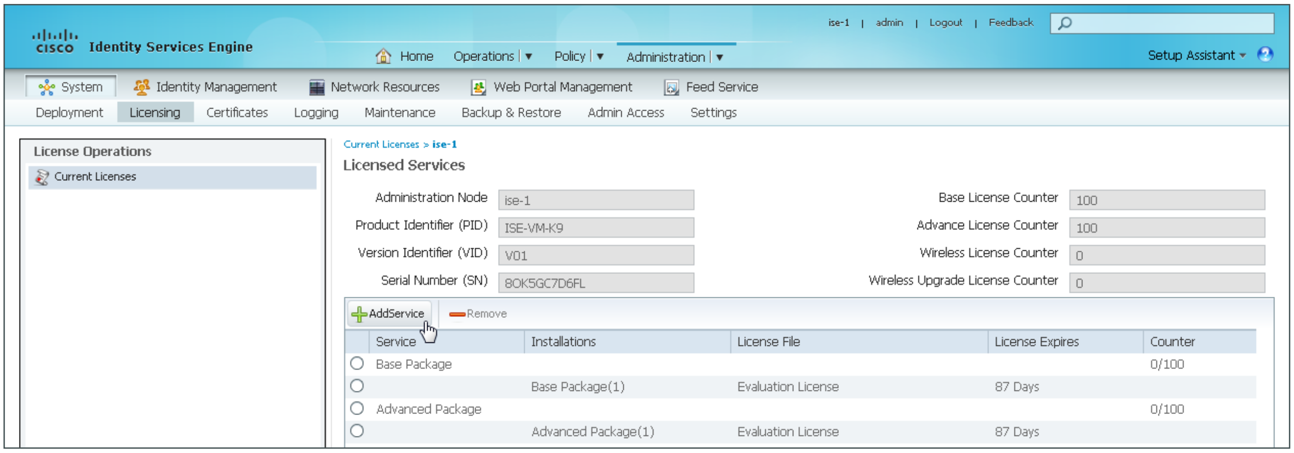
Notice that you only see one node here since only the primary administration node requires licensing.

Select the primary Cisco ISE server, and then click **Edit**. The Licensed Services details are displayed.



	Administration Node	ID (PID,VID,SN)	License Type	Licensed To	Base (Active/Allowed)	Advanced (Active.
●	ise-1	PID:ISE-VM-K9, VID:V01, SN:8OK5...	Base - Eval (87 Days) Advanced - Eval (87 Days)	Cisco	0/100	0/100

Step 2: Under Licensed Services, click **Add Service**.



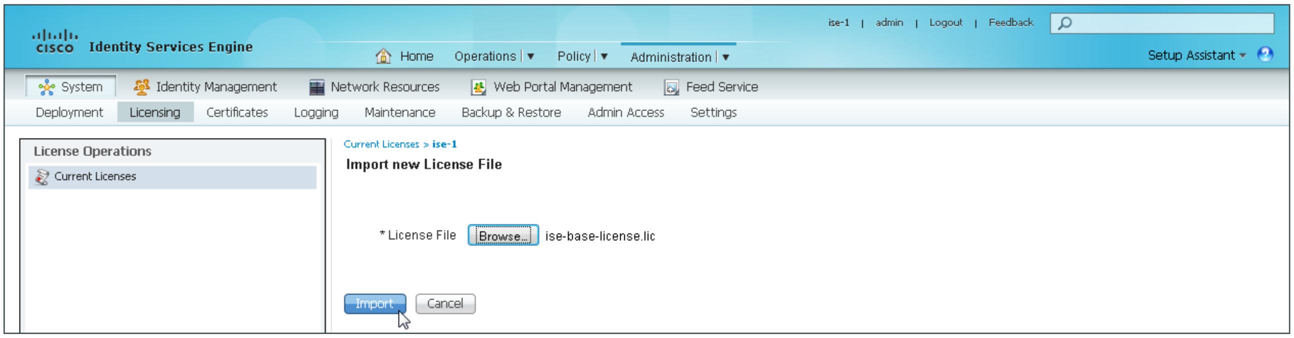
Current Licenses > ise-1

Licensed Services

Administration Node	ise-1	Base License Counter	100
Product Identifier (PID)	ISE-VM-K9	Advance License Counter	100
Version Identifier (VID)	V01	Wireless License Counter	0
Serial Number (SN)	8OK5GC7D6FL	Wireless Upgrade License Counter	0

	Service	Installations	License File	License Expires	Counter
○	Base Package				0/100
○		Base Package(1)	Evaluation License	87 Days	
○	Advanced Package				0/100
○		Advanced Package(1)	Evaluation License	87 Days	

Step 3: Click **Browse**, locate your license file, and then click **Import**.



Current Licenses > ise-1

Import new License File

* License File ise-base-license.lic

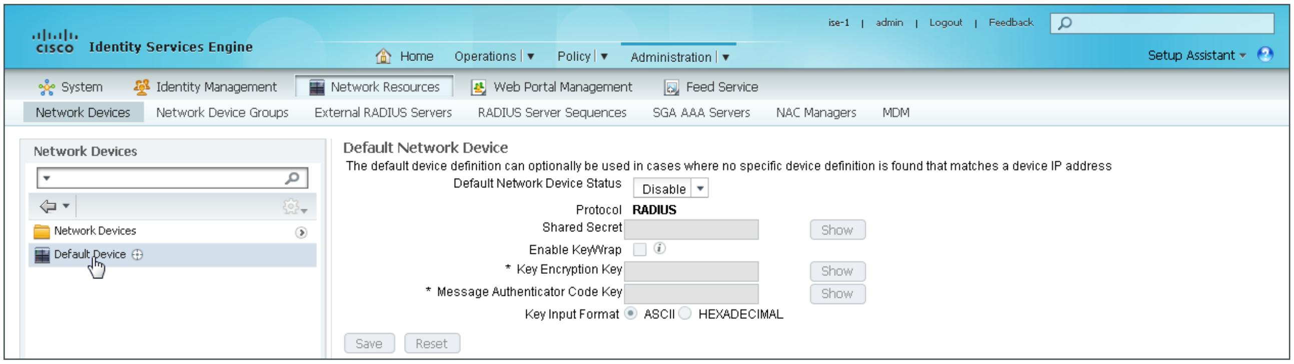
Step 4: If you have multiple licenses to install, repeat the process for each.

Procedure 7 Configure network devices in Cisco ISE

Configure Cisco ISE to accept authentication requests from network devices. RADIUS requires a shared secret key to enable encrypted communications. Each network device that will use Cisco ISE for authentication will need to have this key.

Step 1: Navigate to **Administration > Network Resources > Network Devices**.

In the left pane, click **Default Device**.



Default Network Device

The default device definition can optionally be used in cases where no specific device definition is found that matches a device IP address

Default Network Device Status: Disable

Protocol: RADIUS

Shared Secret

Enable KeyWrap ☐

* Key Encryption Key

* Message Authenticator Code Key

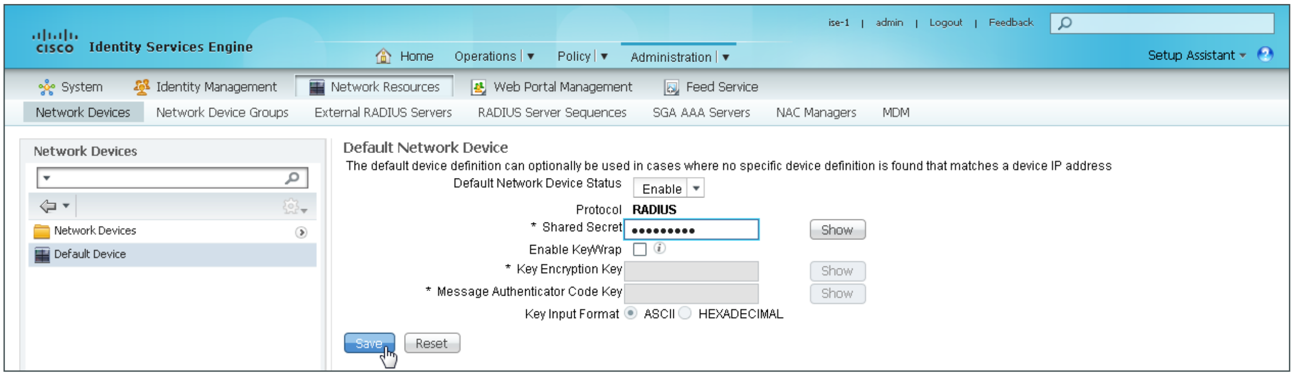
Key Input Format ● ASCII ○ HEXADECIMAL

Tech Tip

Each network device can be configured individually, or devices can be grouped by location, by device type, or by using IP address ranges. The other option is to use the Default Device to configure the parameters for devices that aren't specifically configured. All network devices in this example use the same key, so for simplicity, this example uses the Default Device.

Step 2: In the **Default Network Device Status** list, choose **Enable**.

Step 3: Enter the RADIUS shared secret, and then click **Save**. The default network device RADIUS key is now saved.



Default Network Device

The default device definition can optionally be used in cases where no specific device definition is found that matches a device IP address

Default Network Device Status: Enable

Protocol: RADIUS

* Shared Secret: ●●●●●●●●●

Enable KeyWrap ☐

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ● ASCII ○ HEXADECIMAL

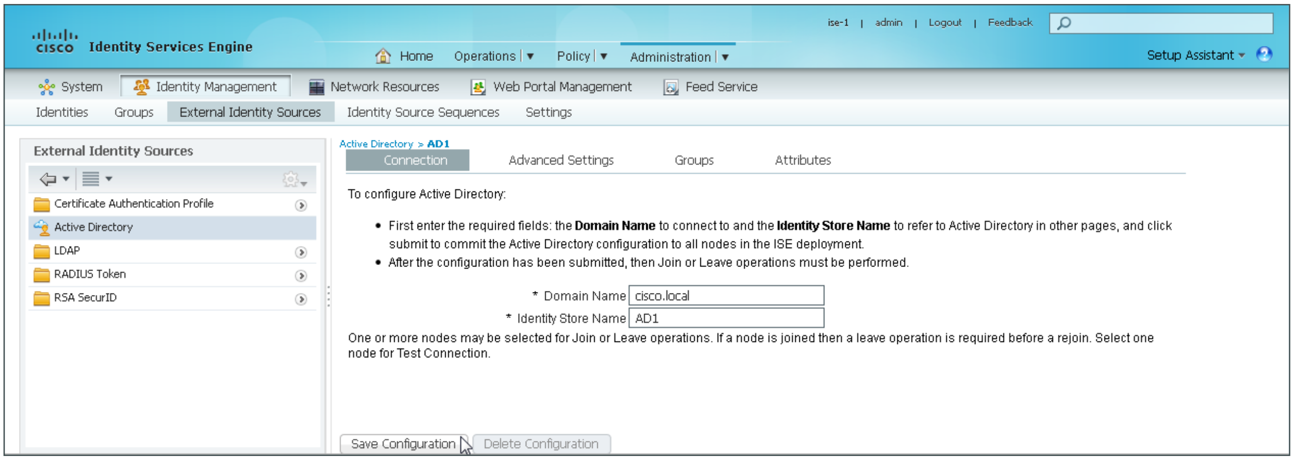
Procedure 8 Configure Cisco ISE to use Active Directory

Cisco ISE will use the existing AD server as an external authentication server. First, you must configure the external authentication server.

Step 1: Navigate to **Administration > Identity Management > External Identity Sources**.

Step 2: In the left panel, click **Active Directory**.

Step 3: On the Connection tab, enter the AD domain (for example, cisco.local) and the name of the server (for example, AD1), and then click **Save Configuration**.



To configure Active Directory:

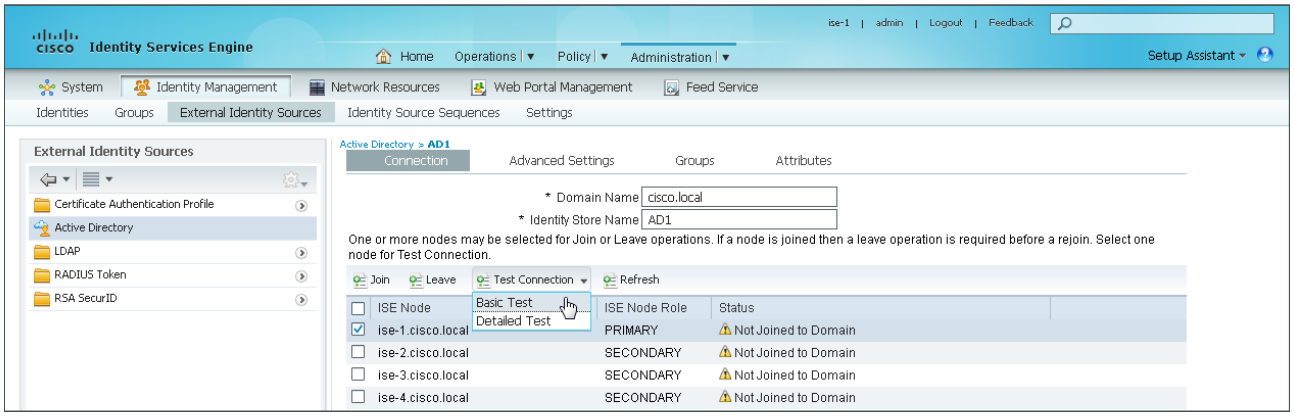
- First enter the required fields: the **Domain Name** to connect to and the **Identity Store Name** to refer to Active Directory in other pages, and click submit to commit the Active Directory configuration to all nodes in the ISE deployment.
- After the configuration has been submitted, then Join or Leave operations must be performed.

* Domain Name: cisco.local

* Identity Store Name: AD1

One or more nodes may be selected for Join or Leave operations. If a node is joined then a leave operation is required before a rejoin. Select one node for Test Connection.

Step 4: Verify these settings by selecting the box next to the node, clicking **Test Connection**, and then choosing **Basic Test**.



* Domain Name: cisco.local

* Identity Store Name: AD1

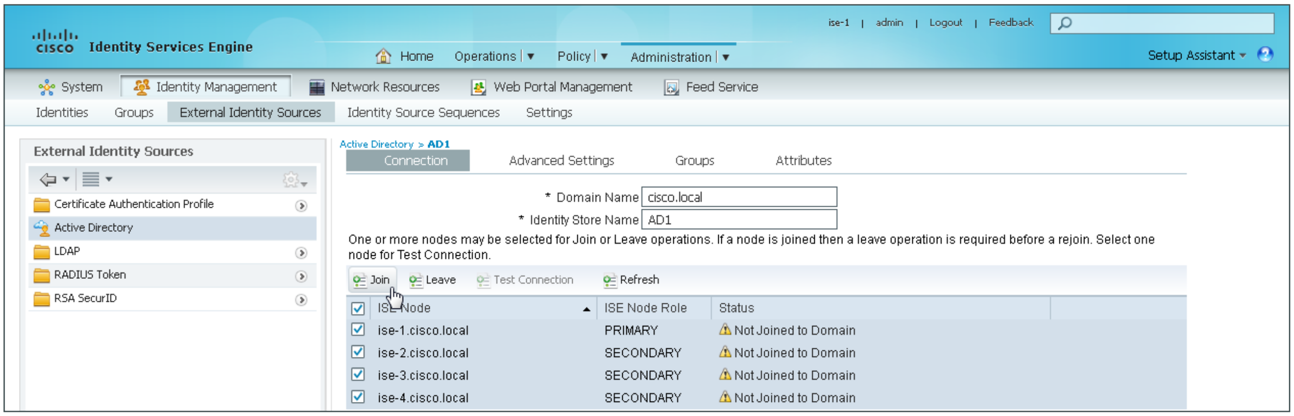
One or more nodes may be selected for Join or Leave operations. If a node is joined then a leave operation is required before a rejoin. Select one node for Test Connection.

☐	ISE Node	ISE Node Role	Status
☑	ise-1.cisco.local	PRIMARY	⚠ Not Joined to Domain
☐	ise-2.cisco.local	SECONDARY	⚠ Not Joined to Domain
☐	ise-3.cisco.local	SECONDARY	⚠ Not Joined to Domain
☐	ise-4.cisco.local	SECONDARY	⚠ Not Joined to Domain

Step 5: Enter the credentials for a domain user, and then click **OK**.

Step 6: A message appears letting you know whether or not the test was successful. Click **Close**.

Step 7: Select the box next each node, and then click **Join**.



* Domain Name: cisco.local

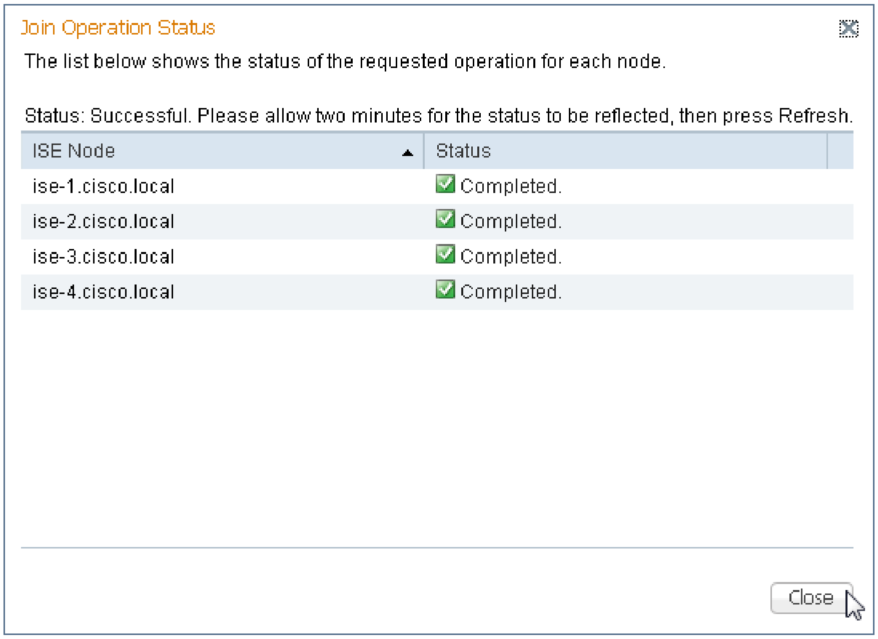
* Identity Store Name: AD1

One or more nodes may be selected for Join or Leave operations. If a node is joined then a leave operation is required before a rejoin. Select one node for Test Connection.

☑	ISE Node	ISE Node Role	Status
☑	ise-1.cisco.local	PRIMARY	⚠ Not Joined to Domain
☑	ise-2.cisco.local	SECONDARY	⚠ Not Joined to Domain
☑	ise-3.cisco.local	SECONDARY	⚠ Not Joined to Domain
☑	ise-4.cisco.local	SECONDARY	⚠ Not Joined to Domain

Step 8: Enter the credentials for a domain administrator account, and then click **OK**. Cisco ISE is now joined to the AD domain.

Step 9: After the message saying the join was successful, click **Close**.



Join Operation Status

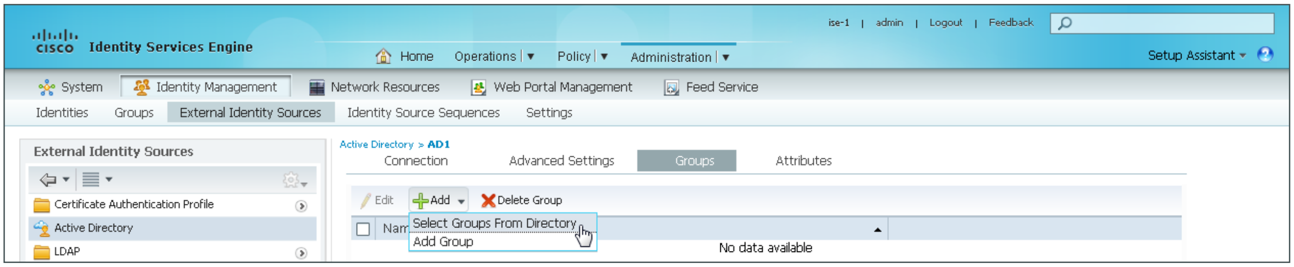
The list below shows the status of the requested operation for each node.

Status: Successful. Please allow two minutes for the status to be reflected, then press Refresh.

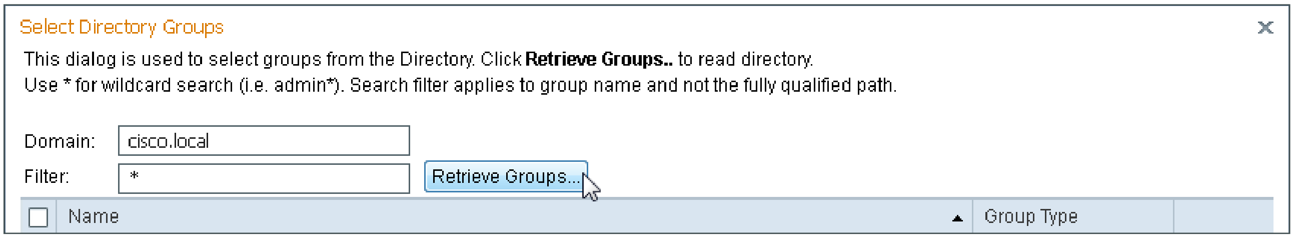
ISE Node	Status
ise-1.cisco.local	✓ Completed.
ise-2.cisco.local	✓ Completed.
ise-3.cisco.local	✓ Completed.
ise-4.cisco.local	✓ Completed.

Next, you select which groups from AD that Cisco ISE will use for authentication.

Step 10: At the top of the same pane, click the Groups tab, click **Add**, and then click **Select Groups from Directory**.



Step 11: Search for the groups you wish to add. The domain box is already filled in. The default filter is a wildcard to list all groups. Click **Retrieve Groups** to get a list of all groups in your domain.

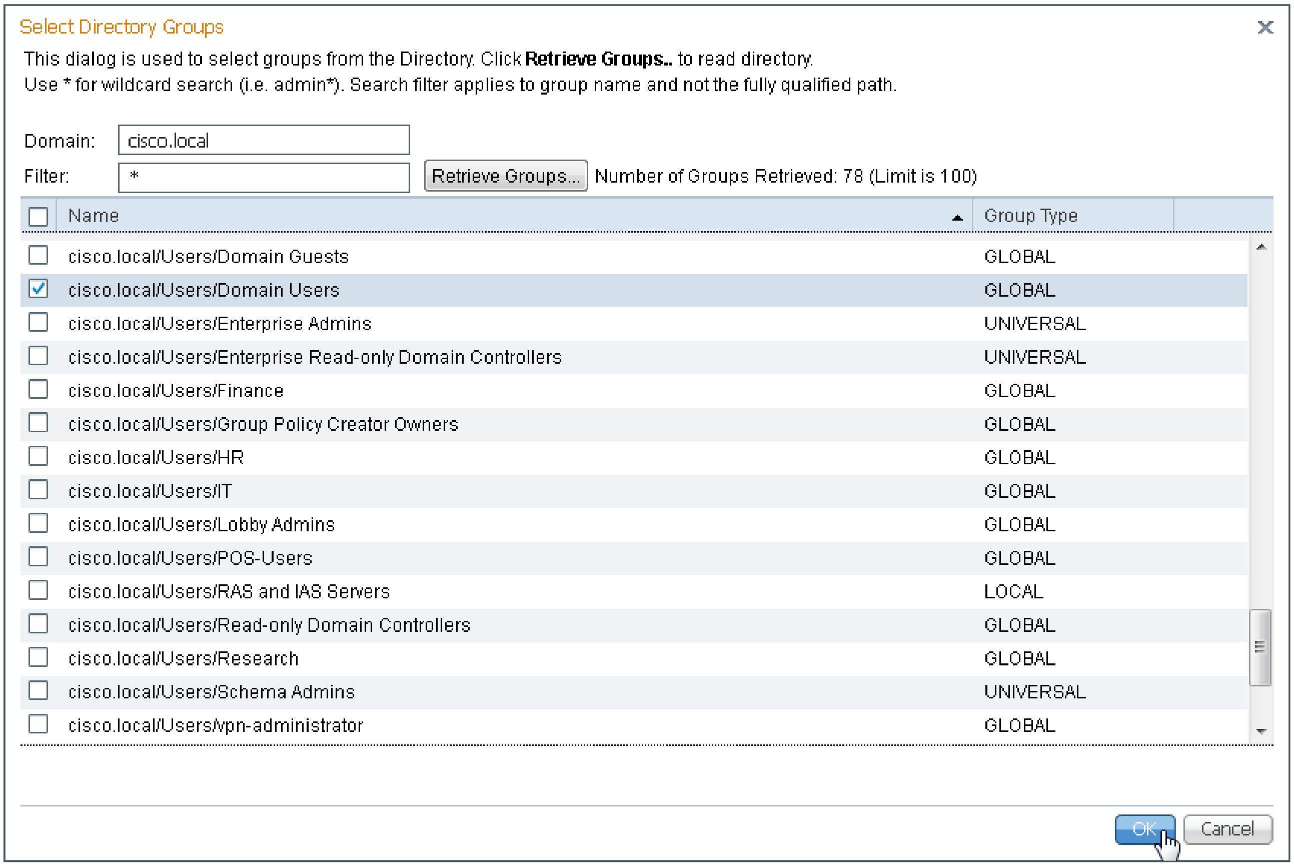


Select Directory Groups

This dialog is used to select groups from the Directory. Click **Retrieve Groups..** to read directory.
Use * for wildcard search (i.e. admin*). Search filter applies to group name and not the fully qualified path.

Domain: cisco.local
Filter: *

Step 12: Select the groups you want to use for authentication, and then click **OK**. For example, for all users in the domain, select the group **<domain>/Users/Domain Users**.



Select Directory Groups

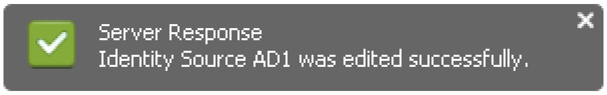
This dialog is used to select groups from the Directory. Click **Retrieve Groups..** to read directory.
Use * for wildcard search (i.e. admin*). Search filter applies to group name and not the fully qualified path.

Domain: cisco.local
Filter: *

Number of Groups Retrieved: 78 (Limit is 100)

☐	Name	Group Type
☐	cisco.local/Users/Domain Guests	GLOBAL
☑	cisco.local/Users/Domain Users	GLOBAL
☐	cisco.local/Users/Enterprise Admins	UNIVERSAL
☐	cisco.local/Users/Enterprise Read-only Domain Controllers	UNIVERSAL
☐	cisco.local/Users/Finance	GLOBAL
☐	cisco.local/Users/Group Policy Creator Owners	GLOBAL
☐	cisco.local/Users/HR	GLOBAL
☐	cisco.local/Users/IT	GLOBAL
☐	cisco.local/Users/Lobby Admins	GLOBAL
☐	cisco.local/Users/POS-Users	GLOBAL
☐	cisco.local/Users/RAS and IAS Servers	LOCAL
☐	cisco.local/Users/Read-only Domain Controllers	GLOBAL
☐	cisco.local/Users/Research	GLOBAL
☐	cisco.local/Users/Schema Admins	UNIVERSAL
☐	cisco.local/Users/vpn-administrator	GLOBAL

Step 13: Click **Save Configuration**. The AD configuration is saved.



Server Response
Identity Source AD1 was edited successfully.

PROCESS

Enabling ISE for Network Visibility

1. Configure MAC Authentication Bypass
2. Configure 802.1X for wired and wireless users

Cisco ISE now has a baseline configuration. The next step is to configure Cisco ISE with an authentication policy and to configure the switches for identity by using the IOS CLI.

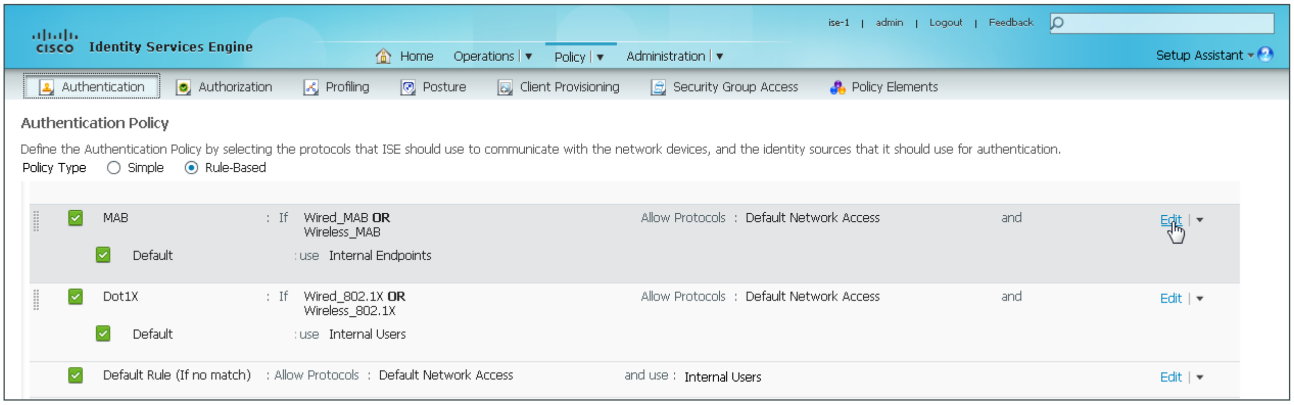
Procedure 1 Configure MAC Authentication Bypass

MAB allows you to configure specific machine MAC addresses on the switch to bypass the authentication process. For monitor mode, this is required, since you aren't enforcing authentication. You configure MAB to allow any MAC address to authenticate for both the wired and wireless networks.

Step 1: Navigate to **Policy > Authentication**. The Policy Type is Rule-Based.

There are already two preconfigured rules in place, MAB and Dot1X along with the default rule.

Step 2: For the MAB rule, click **Edit**.



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

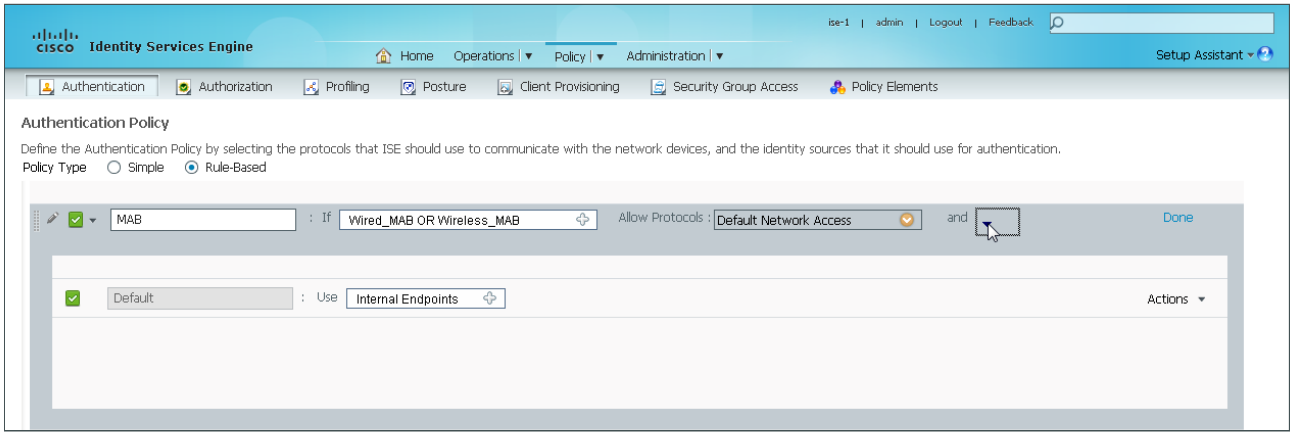
Policy Type ○ Simple ● Rule-Based

☑ MAB : If Wired_MAB **OR** Wireless_MAB Allow Protocols : Default Network Access and
☑ Default : use Internal Endpoints

☑ Dot1X : If Wired_802.1X **OR** Wireless_802.1X Allow Protocols : Default Network Access and
☑ Default : use Internal Users

☑ Default Rule (If no match) : Allow Protocols : Default Network Access and use : Internal Users

Step 3: For the MAB policy, click the black triangle to the right of the **and**. This brings up the identity store used for the MAB rule.



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

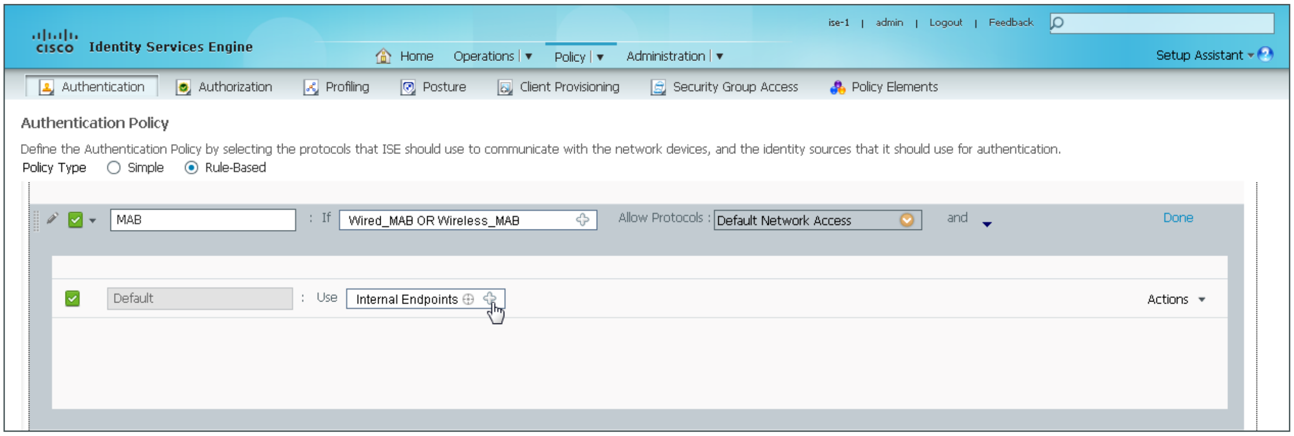
Policy Type ○ Simple ● Rule-Based

☑ MAB : If Wired_MAB OR Wireless_MAB Allow Protocols : Default Network Access and

☑ Default : Use Internal Endpoints

Next, you modify the default options on the Internal Users database, which is used for profiling.

Step 4: Next to Internal Endpoints, click the **+**.



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

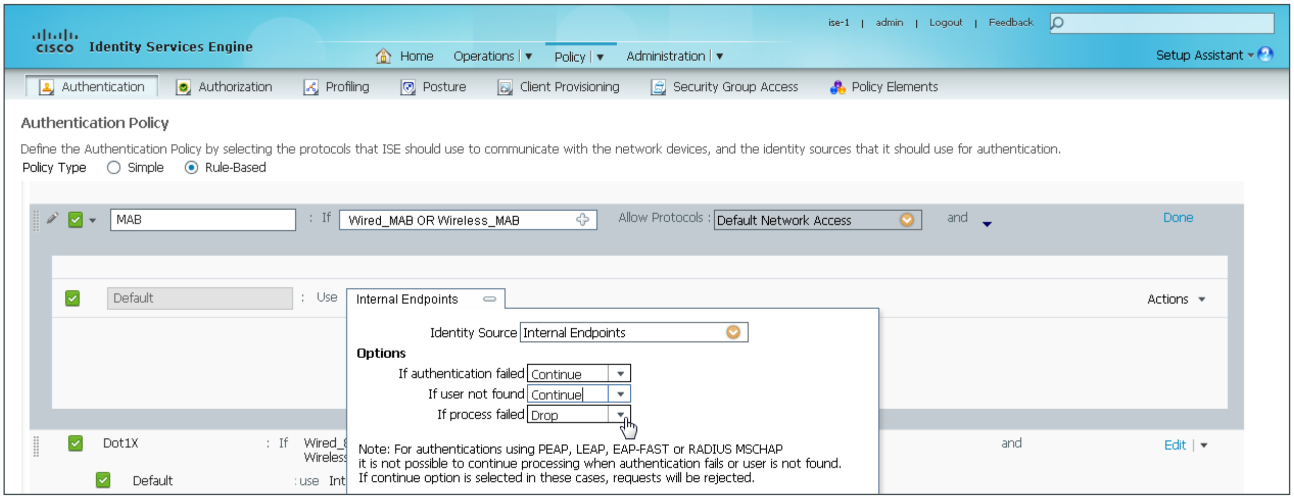
Policy Type ○ Simple ● Rule-Based

☑ MAB : If Wired_MAB OR Wireless_MAB Allow Protocols : Default Network Access and

☑ Default : Use Internal Endpoints

Step 5: In this example deployment, all endpoints are allowed to authenticate. Set the following values:

- If authentication failed—**Continue**
- If user not found—**Continue**
- If process failed—**Drop**



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type ○ Simple ● Rule-Based

☑ MAB : If Wired_MAB OR Wireless_MAB Allow Protocols : Default Network Access and

☑ Default : Use Internal Endpoints

Identity Source Internal Endpoints

Options

If authentication failed Continue

If user not found Continue

If process failed Drop

Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS MSCHAP it is not possible to continue processing when authentication fails or user is not found. If continue option is selected in these cases, requests will be rejected.

☑ Dot1X : If Wired_ Wireless and

☑ Default : use Int

Step 6: Click anywhere in the window in order to continue, and then at the bottom click **Save**.

Procedure 2 Configure 802.1X for wired and wireless users

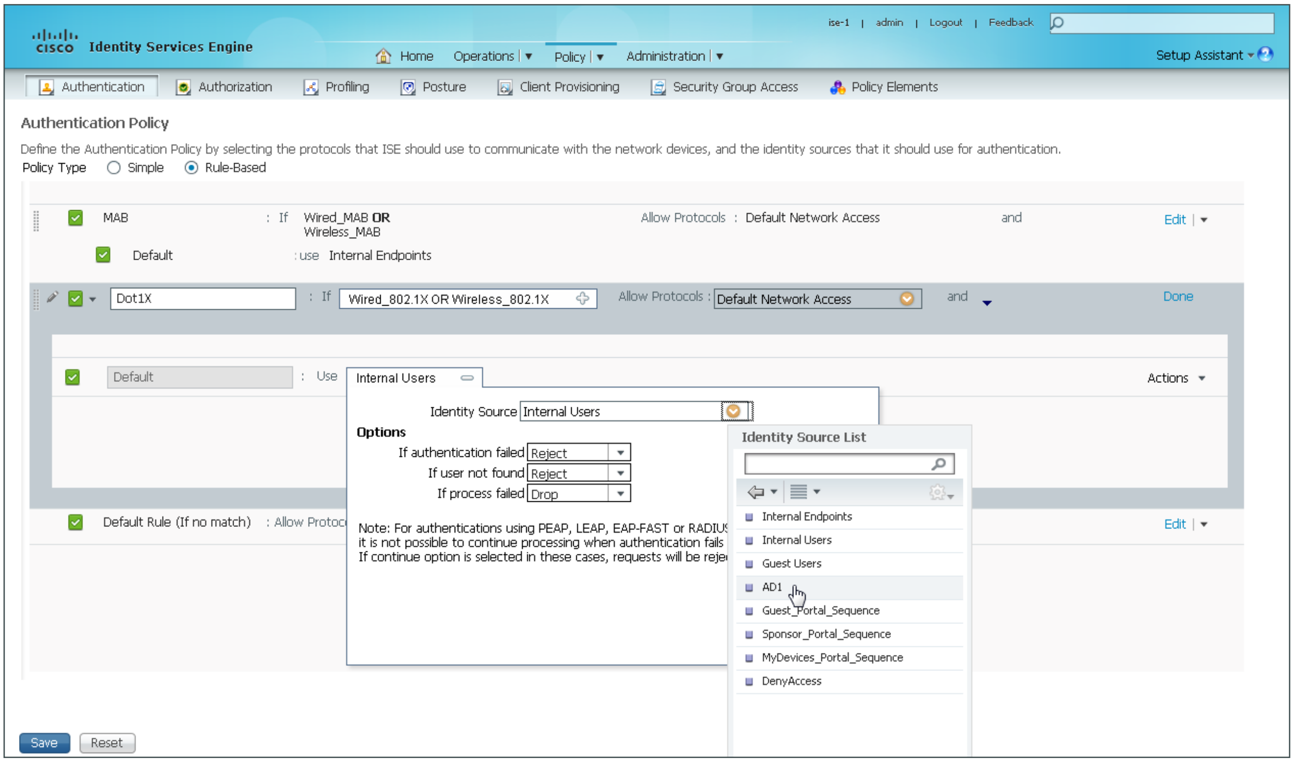
There is already a Dot1X rule configured on the engine. Although in this example deployment you aren't deploying any wired endpoints with 802.1X supplicants at this point, you should still configure this rule to prepare for the next phase of an identity deployment. The default identity store is the internal user database. For 802.1X, use the Active Directory server that you defined earlier.

Step 1: Navigate to **Policy > Authentication**.

Step 2: For the **Dot1X** rule, click **Edit**, and then click the black triangle to the right of the **and**. This brings up the identity store used for this rule.

Step 3: Next to Internal Users, click the **+** symbol. This enables you to edit the identity store and the parameters.

Step 4: In the **Identity Source** list, choose the previously defined AD server **AD1**.



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type ○ Simple ● Rule-Based

☑ MAB : If Wired_MAB **OR** Wireless_MAB Allow Protocols : Default Network Access and

☑ Default : use Internal Endpoints

☑ Dot1X : If Wired_802.1X OR Wireless_802.1X Allow Protocols : Default Network Access and

☑ Default : Use Internal Users

Identity Source Internal Users

Options

If authentication failed Reject

If user not found Reject

If process failed Drop

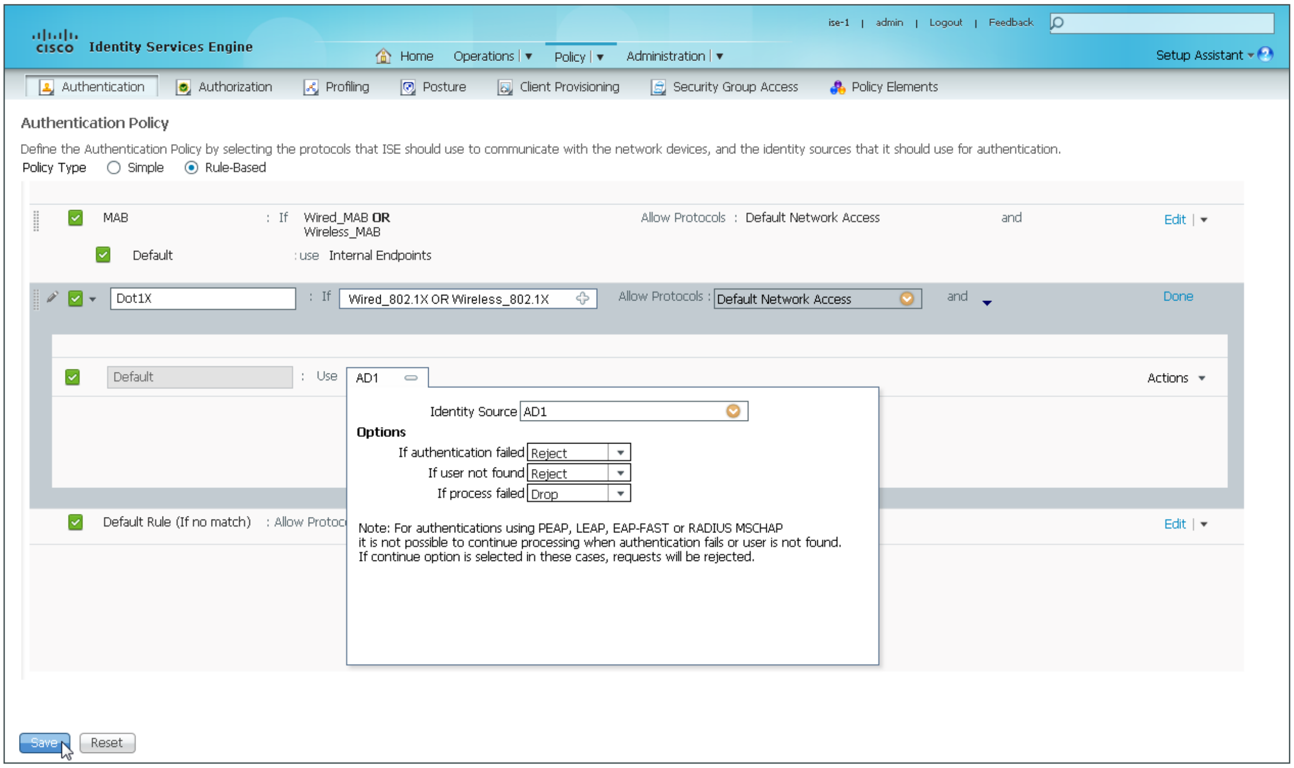
Note: For authentications using PEAP, LEAP, EAP-FAST or RADIU
it is not possible to continue processing when authentication fails
If continue option is selected in these cases, requests will be reje

☑ Default Rule (If no match) : Allow Protoc

Identity Source List

- Internal Endpoints
- Internal Users
- Guest Users
- AD1
- Guest_Portal_Sequence
- Sponsor_Portal_Sequence
- MyDevices_Portal_Sequence
- DenyAccess

Step 5: Do not change the default options for this identity source. Click anywhere in the window to continue, and then at the bottom click **Save**.



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type ○ Simple ● Rule-Based

☑ MAB : If Wired_MAB **OR** Wireless_MAB Allow Protocols : Default Network Access and

☑ Default : use Internal Endpoints

☑ Dot1X : If Wired_802.1X OR Wireless_802.1X Allow Protocols : Default Network Access and

☑ Default : Use AD1

Identity Source AD1

Options

If authentication failed Reject

If user not found Reject

If process failed Drop

Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS MSCHAP it is not possible to continue processing when authentication fails or user is not found. If continue option is selected in these cases, requests will be rejected.

☑ Default Rule (If no match) : Allow Protoc

PROCESS

Enabling Visibility to the Wired Network

1. Enable RADIUS in the wired access layer
2. Enable identity on the wired access ports
3. Disable port security timers

Procedure 1 Enable RADIUS in the wired access layer

Step 1: Identify switches in the access layer (enabling visibility), connect to the CLI of each access switch, and configure each with the following RADIUS and AAA global configuration commands.

```
radius server ise-3
 address ipv4 10.4.48.43 auth-port 1812 acct-port 1813
 key [radius key]
radius server ise-4
 address ipv4 10.4.48.44 auth-port 1812 acct-port 1813
 key [radius key]
aaa group server radius ISE_GROUP
 server name ise-3
 server name ise-4

aaa authentication dot1x default group ISE_GROUP
aaa authorization network default group ISE_GROUP
aaa authorization configuration default group ISE_GROUP
aaa accounting dot1x default start-stop group ISE_GROUP

radius-server vsa send accounting
radius-server vsa send authentication
```

Tech Tip

For consistency among this guide and other CVD guides, the guides standardized on these well-known TCP ports for RADIUS authentication and accounting: 1812 and 1813. The Cisco Identity Services Engine supports both the older IOS default of 1645/1646 ports and the newer standardized 1812/1813 ports.

Procedure 2 Enable identity on the wired access ports

Step 1: Connect to the CLI of each access switch, and configure each with the following identify global configuration commands. The device-sensor command is not available on all switches.

```
authentication mac-move permit
dot1x system-auth-control
device-sensor accounting
```

Tech Tip

The device sensor functionality is only available for switches that use specific software versions and feature sets. If available, it should be enabled to add additional profiling visibility by gathering data gleaned from traffic coming from endpoints.

To make configuration easier when the same configuration is applied to multiple interfaces on the switch, use the **interface range** command. This command allows you to issue a command once and have it apply to many interfaces at the same time. Since most of the interfaces in the access layer are configured identically, it can save a lot of time. For example, the following command allows you to enter commands on all 24 interfaces (Gig 0/1 to Gig 0/24) simultaneously.

```
interface range GigabitEthernet 0/1-24
```

Step 2: Connect to the CLI of each access switch, and configure all host access ports on each with the following commands. These commands should not be configured on infrastructure-facing ports, such as uplinks.

```
interface range [interface type] [port number]-[port number]
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab
 authentication port-control auto
 mab
 dot1x pae authenticator
```

Procedure 3 Disable port security timers

The Campus Wired LAN Technology Design Guide incorporates the use of port security to provide a level of security and prevent rogue devices from being connected. However, 802.1X also provides similar functionality and there can be conflicts when both are enabled on a port at the same time. As an example, both port security and 802.1X each have their own set of inactivity timers. Enabling both simultaneously causes 802.1X to re-authenticate every time the port security timeout is reached. To avoid this issue, disable port security.

Step 1: Enter the CLI commands necessary to remove the port security configuration.

```
interface range [interface type] [port number]-[port number]
 no switchport port-security aging time
 no switchport port-security aging type
 no switchport port-security violation
 no switchport port-security
```

PROCESS

Enabling Visibility to the Wireless Network

1. Disable EAP-TLS on Cisco ISE
2. Add ISE as RADIUS authentication server
3. Add Cisco ISE as RADIUS accounting server
4. Enable client profiling

To authenticate wireless clients, you need to configure the WLC to use the new Cisco ISE servers as RADIUS servers for authentication and accounting. The existing entry is disabled so that if there are any issues after moving to Cisco ISE, you can quickly restore the original configuration. Additionally, you configure the WLCs for DHCP profiling so that profiling information can be obtained from the DHCP requests from these clients and sent to the Cisco ISE.

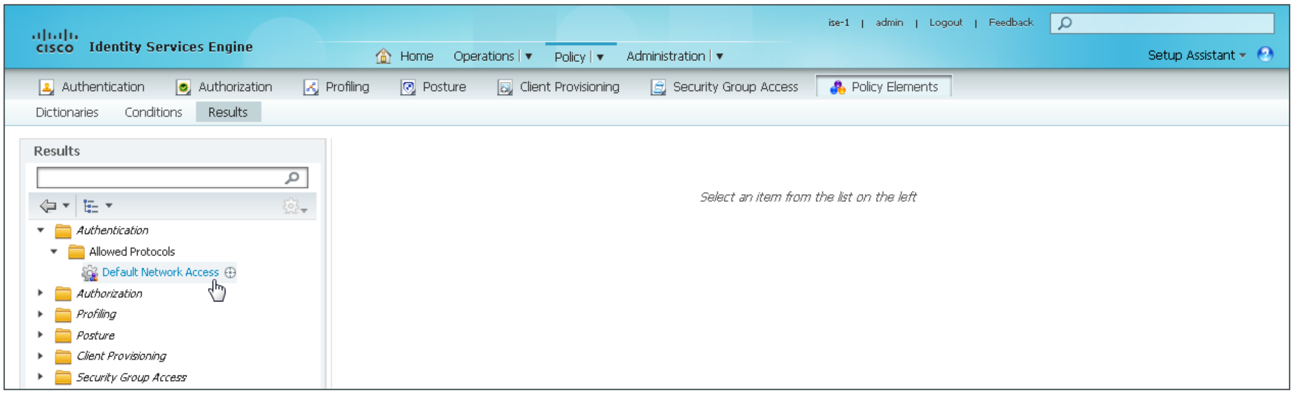
Procedure 1 Disable EAP-TLS on Cisco ISE

For wireless deployments that aren't currently using digital certificates, you need to disable EAP-TLS in order to allow clients to log in. You will be deploying digital certificates in a later phase of this deployment.

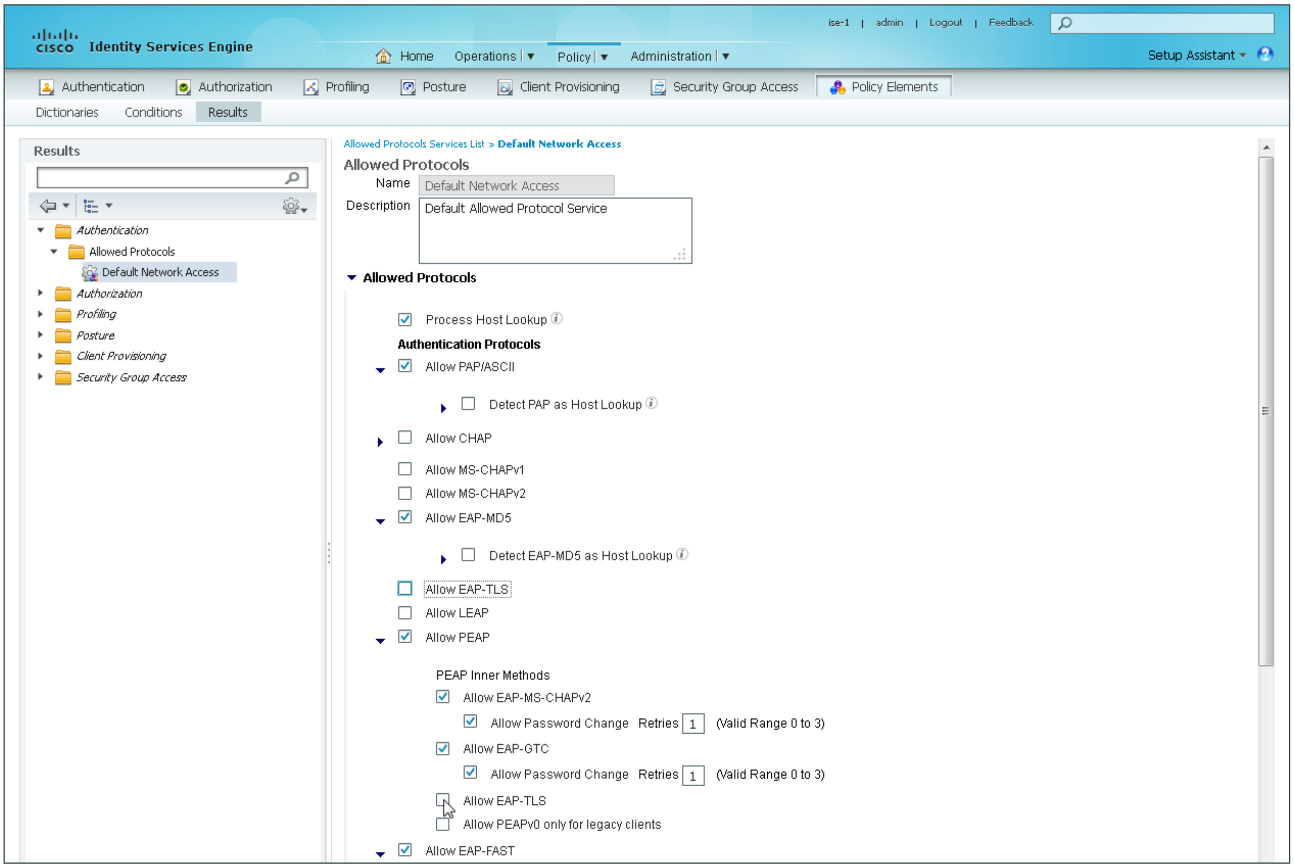
Step 1: Connect and login to the ISE primary administration and monitoring node (Example: http://ise-1.cisco.local).

Step 2: In the top menu, navigate to **Policy > Policy Elements > Results**.

Step 3: In the left pane, navigate to **Authentication > Allowed Protocols**, and then select **Default Network Access**.



Step 4: Under **Allowed Protocols > Authentication Protocols**, clear **Allow EAP-TLS.**



Allowed Protocols

Name: Default Network Access

Description: Default Allowed Protocol Service

Allowed Protocols

☑ Process Host Lookup

Authentication Protocols

☑ Allow PAP/ASCII
  ☐ Detect PAP as Host Lookup
☐ Allow CHAP
☐ Allow MS-CHAPv1
☐ Allow MS-CHAPv2
☑ Allow EAP-MD5
  ☐ Detect EAP-MD5 as Host Lookup
☐ Allow EAP-TLS
☐ Allow LEAP
☑ Allow PEAP
  PEAP Inner Methods
  ☑ Allow EAP-MS-CHAPv2
    ☑ Allow Password Change Retries 1 (Valid Range 0 to 3)
  ☑ Allow EAP-GTC
    ☑ Allow Password Change Retries 1 (Valid Range 0 to 3)
  ☐ Allow EAP-TLS
  ☐ Allow PEAPv0 only for legacy clients
☑ Allow EAP-FAST

Step 5: Under **Allowed Protocols > Authentication Protocols > Allow PEAP**, clear **Allow EAP-TLS**, and then at the bottom, click **Save**.

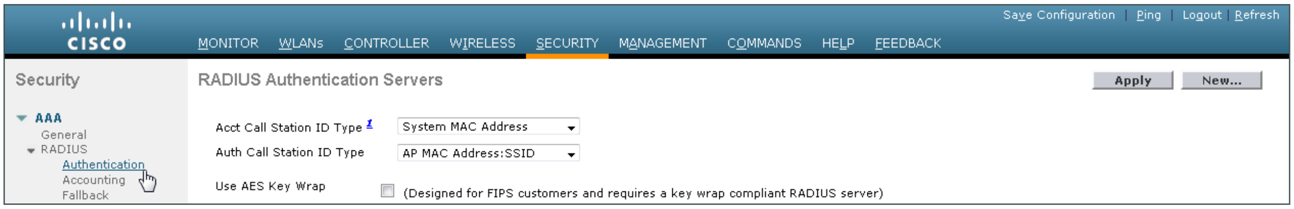
Procedure 2 Add ISE as RADIUS authentication server

Perform this procedure for every wireless LAN controller with the exception of the standalone guest WLC, if you have deployed one.

Step 1: Use a web browser to connect and login to the WLC console (Example: https://wlc1.cisco.local).

Step 2: On the top menu bar, click **Security**.

Step 3: In the left pane, under the **AAA > RADIUS** section, click **Authentication**.



RADIUS Authentication Servers

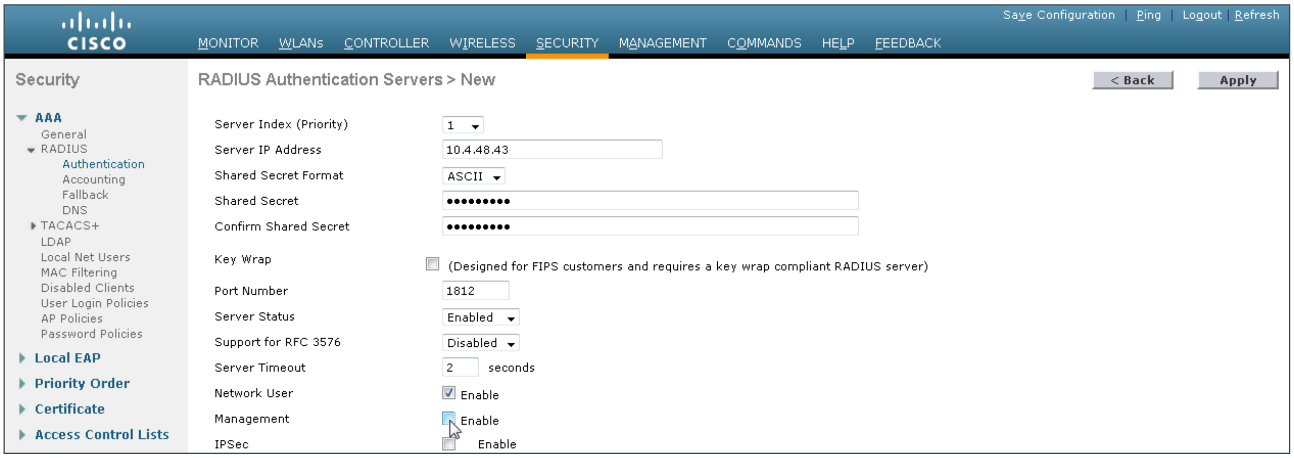
Acct Call Station ID Type: System MAC Address
Auth Call Station ID Type: AP MAC Address:SSID
Use AES Key Wrap ☐ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Step 4: Do not make changes to any preexisting RADIUS servers yet. Click **New**. You can now configure a new RADIUS Authentication server.

Step 5: In the **Server IP Address** box, enter your primary ISE policy service node IP address, **10.4.48.43**.

Step 6: In the **Shared Secret** box, enter your RADIUS shared secret, and then in the **Confirm Shared Secret** box, re-enter it.

Step 7: Next to Management, clear **Enable**, and then click **Apply**.



RADIUS Authentication Servers > New

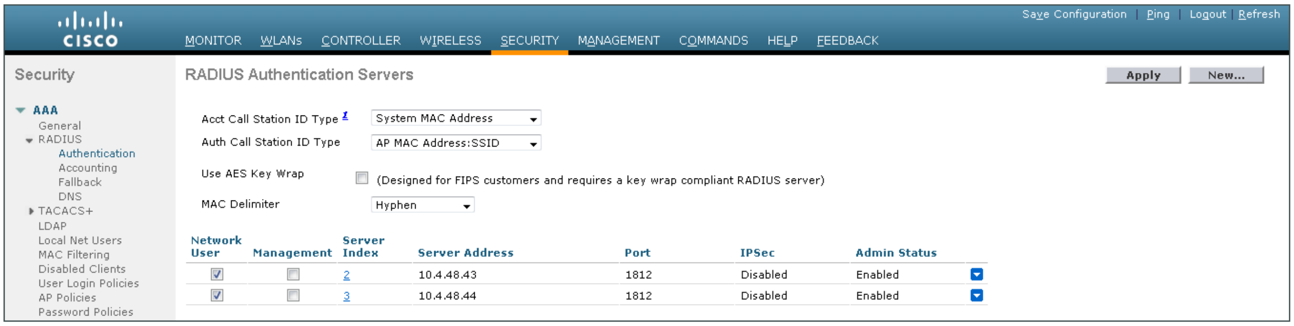
Server Index (Priority): 1
Server IP Address: 10.4.48.43
Shared Secret Format: ASCII
Shared Secret: •••••••••
Confirm Shared Secret: •••••••••
Key Wrap: ☐ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number: 1812
Server Status: Enabled
Support for RFC 3576: Disabled
Server Timeout: 2 seconds
Network User: ☑ Enable
Management: ☐ Enable
IPSec: ☐ Enable

Step 8: Repeat Step 4 through Step 7 in order to add the additional ISE policy service node **10.4.48.44** to the WLC configuration.

If a RADIUS server was previously configured on the WLC, you disable the preexisting RADIUS server. By disabling the server instead of deleting it, you can easily switch back, if needed. You perform this step for every WLC, with the exception of the standalone guest WLC, if you have deployed one.

Step 9: If you have a preexisting RADIUS server, on the RADIUS Authentication Servers screen under Server Index, click the number of the preexisting RADIUS server. On the Edit screen, change **Server Status** to **Disabled**, and then click **Apply**.

You are returned to the RADIUS Authentication Servers screen, where you can see the Admin Status for the preexisting server is Disabled.



RADIUS Authentication Servers

Acct Call Station ID Type: System MAC Address
Auth Call Station ID Type: AP MAC Address:SSID
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
☑	☐	2	10.4.48.43	1812	Disabled	Enabled
☑	☐	3	10.4.48.44	1812	Disabled	Enabled

Repeat this procedure for every remaining WLC, with the exception of the standalone guest WLC, if you have deployed one.

Procedure 3 Add Cisco ISE as RADIUS accounting server

Perform this procedure for every WLC, with the exception of the standalone guest WLC, if you have deployed one.

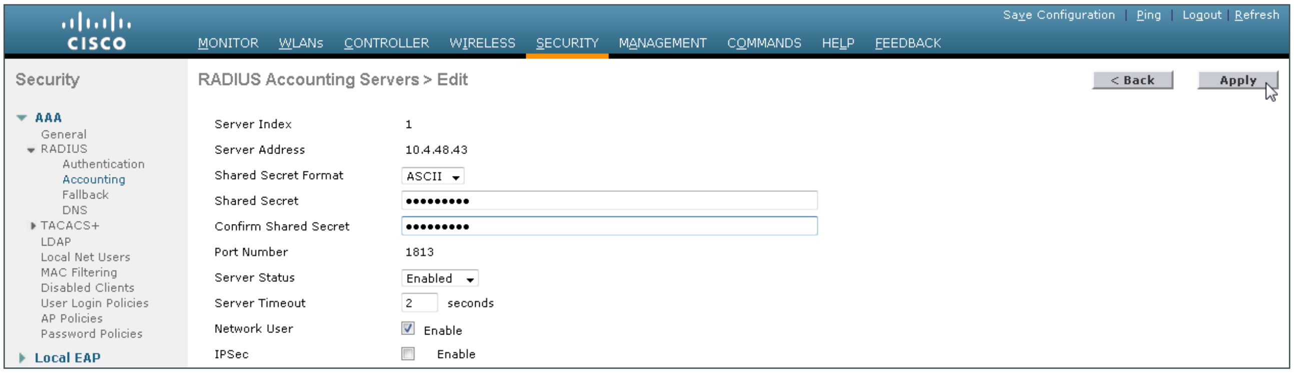
Step 1: On the menu bar, click **Security**.

Step 2: In the left pane, under the RADIUS section, click **Accounting**. Do not make changes to any preexisting RADIUS servers yet.

Step 3: Click **New**. You can now configure a new RADIUS accounting server.

Step 4: In the **Server IP Address** box, enter your primary ISE policy service node IP address, **10.4.48.43.**

Step 5: In the **Shared Secret** box, enter your RADIUS shared secret, and then in the **Confirm Shared Secret** box, re-enter it.



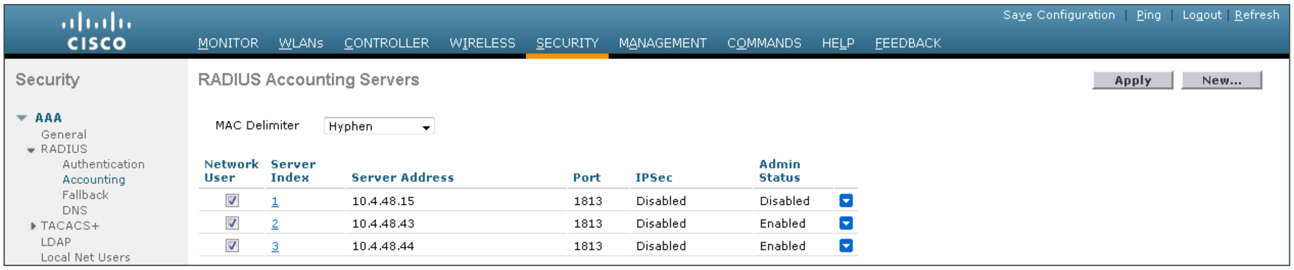
RADIUS Accounting Servers > Edit

Server Index: 1
Server Address: 10.4.48.43
Shared Secret Format: ASCII
Shared Secret: •••••••••
Confirm Shared Secret: •••••••••
Port Number: 1813
Server Status: Enabled
Server Timeout: 2 seconds
Network User: ☑ Enable
IPSec: ☐ Enable

Step 6: Repeat Step 3 through Step 4 and add the additional ISE policy service node **10.4.48.44** to the WLC configuration.

Step 7: If you have a preexisting RADIUS server, on the RADIUS Accounting Servers screen under Server Index, click the number of the preexisting RADIUS server. On the Edit screen, change **Server Status** to **Disabled**, and then click **Apply**.

You are returned to the RADIUS Accounting Servers screen, where you can see the Admin Status for the preexisting server is Disabled.



Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Security
AAA
General
RADIUS
Authentication
Accounting
Fallback
DNS
TACACS+
LDAP
Local Net Users
Apply
New...

RADIUS Accounting Servers

MAC Delimiter: Hyphen

Network User	Server Index	Server Address	Port	IPSec	Admin Status
☑	1	10.4.48.15	1813	Disabled	Disabled
☑	2	10.4.48.43	1813	Disabled	Enabled
☑	3	10.4.48.44	1813	Disabled	Enabled

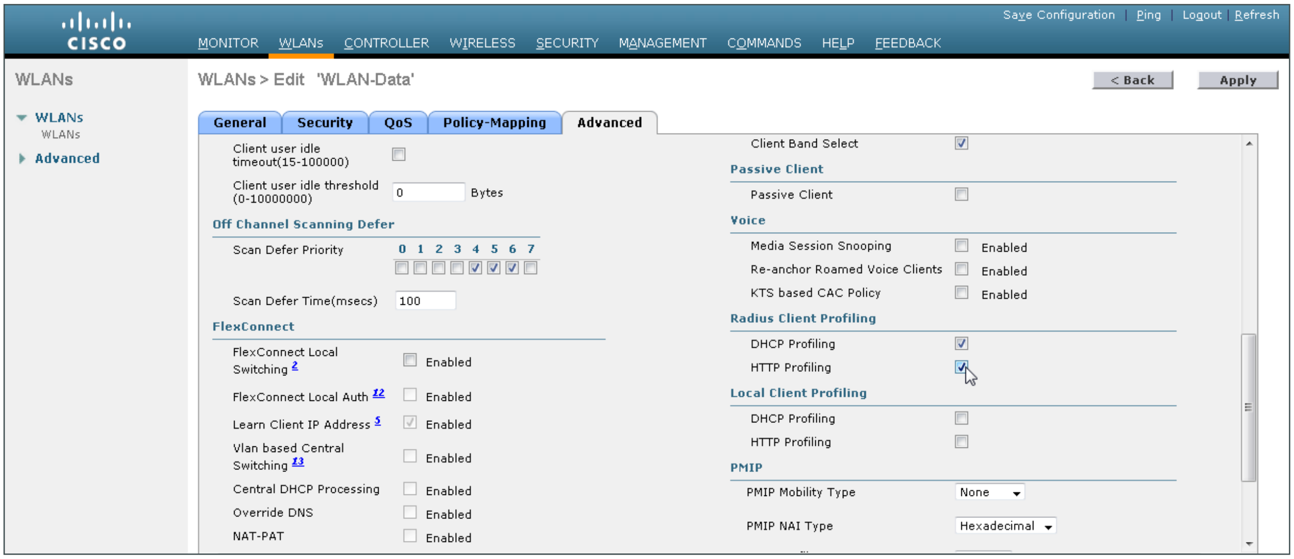
Procedure 4 Enable client profiling

You need to enable client profiling on the WLC in order to send DHCP and HTTP information to the engine for endpoint profiling.

Step 1: On the WLC, navigate to **WLANs**, and then select the WLAN ID underlined number for an SSID you wish to monitor.

Step 2: On the Advanced tab, in the Radius Client Profiling section, select **DHCP Profiling.**

Step 3: Select **HTTP Profiling,** click **Apply**, and then click **OK** in order to acknowledge there may be a WLAN connectivity disruption.



Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General
Security
QoS
Policy-Mapping
Advanced

WLANs > Edit 'WLAN-Data'

Client user idle timeout(15-100000) ☐

Client user idle threshold (0-10000000) 0 Bytes

Off Channel Scanning Defer

Scan Defer Priority 0 ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☑ 5 ☑ 6 ☑ 7 ☐

Scan Defer Time(msecs) 100

FlexConnect

FlexConnect Local Switching [2] ☐ Enabled

FlexConnect Local Auth [12] ☐ Enabled

Learn Client IP Address [5] ☑ Enabled

Vlan based Central Switching [13] ☐ Enabled

Central DHCP Processing ☐ Enabled

Override DNS ☐ Enabled

NAT-PAT ☐ Enabled

Client Band Select ☑

Passive Client

Passive Client ☐

Voice

Media Session Snooping ☐ Enabled

Re-anchor Roamed Voice Clients ☐ Enabled

KTS based CAC Policy ☐ Enabled

Radius Client Profiling

DHCP Profiling ☑

HTTP Profiling ☑

Local Client Profiling

DHCP Profiling ☐

HTTP Profiling ☐

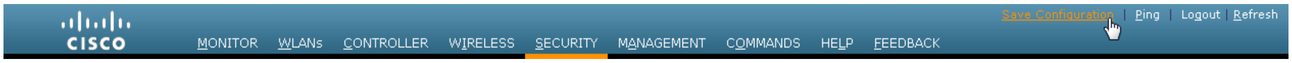
PMIP

PMIP Mobility Type None

PMIP NAI Type Hexadecimal

The network infrastructure is now enabled for monitoring the network to determine what types of devices are connecting. Additionally, authentication using Cisco ISE is enabled for the wireless network. This is a good place in the deployment to test the deployment and monitor network access. Some organizations may not need to implement the next phase and choose to stop here.

Step 4: At the top right, click **Save Configuration**, and then click **OK** to confirm.



The configuration updates are now saved.

Repeat this procedure for every remaining WLC with the exception of the standalone guest WLC, if you have deployed one.

PROCESS

Deploying Digital Certificates

1. Install certificate authority
2. Install trusted root certificate for domain
3. Install trusted root on AD server
4. Request a certificate for ISE from the CA
5. Download CA root certificate
6. Issue certificate for Cisco ISE
7. Install trusted root certificate in Cisco ISE
8. Install local certificate in Cisco ISE
9. Delete old certificate and request

In this phase of deployment, you configure the infrastructure to support the use of digital certificates for user and machine authentication. Using digital certificates when deploying 802.1X is a Cisco best practice. In this example deployment, you deploy digital certificates to Microsoft Windows 7 and Windows 8 endpoints as well as to Apple Mac OS X devices. The certificate authority (CA) you use is the one built into Windows Server 2012 Enterprise.

Procedure 1 Install certificate authority

There are six different role services that can be installed when configuring the certificate authority. For this deployment, you install all of them.

Step 1: Install an enterprise root certificate authority on a Windows 2012 Enterprise server.

Reader Tip

Active Directory Certificate Services installation guidance is available from Microsoft, described in Microsoft's Test Lab Guide: Deploying an AD CS Two-Tier PKI Hierarchy.

Procedure 2 Install trusted root certificate for domain

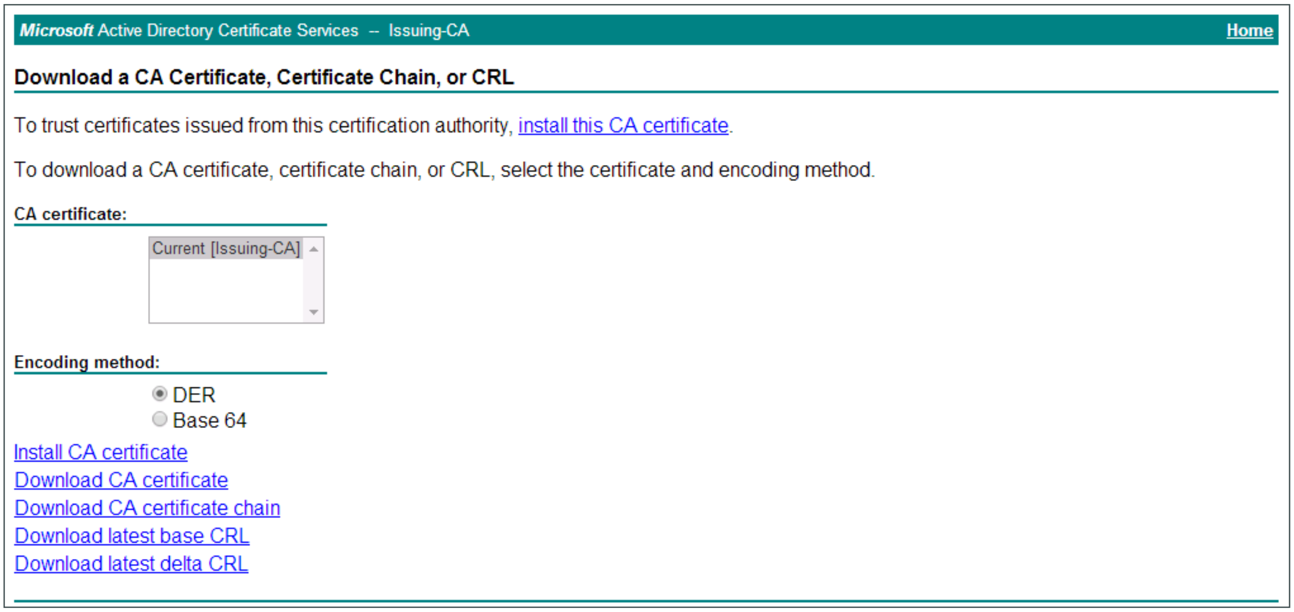
Install a trusted root certificate on the AD controller in order to distribute it to the clients so that certificates from the CA server will be trusted.

Step 1: On the console of the AD controller (Example: ad.cisco.local), launch a web browser, and then connect to the certificate authority at the following address:
https://**ca.cisco.local**/certsrv

Step 2: Click **Download a CA certificate, certificate chain, or CRL**.

Step 3: Verify that the current certificate is selected and the **DER** encoding method is selected.

Step 4: Click **Download CA Certificate**, and then save the certificate file (obtained from the CA) on to the AD controller.


Microsoft Active Directory Certificate Services -- Issuing-CA
Home

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [Issuing-CA]

Encoding method:

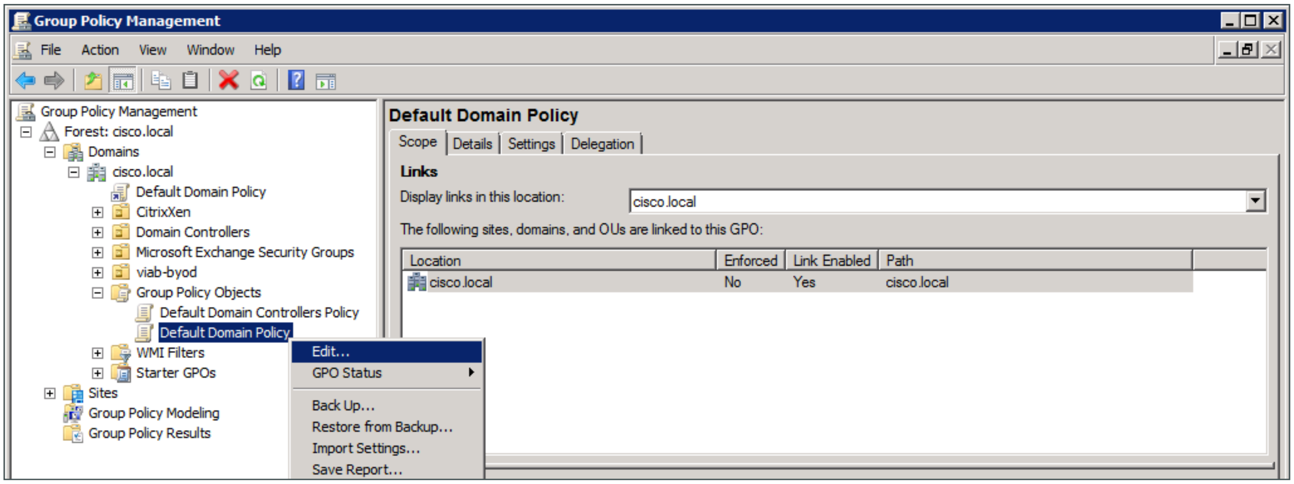
● DER
○ Base 64

Install CA certificate
Download CA certificate
Download CA certificate chain
Download latest base CRL
Download latest delta CRL

Step 5: On the AD console, navigate to **Start > Administrative Tools > Group Policy Management**.

Step 6: Expand **Forest: [local forest]** > Domains > **[local domain]** > Group Policy Objects.

Step 7: Right-click **Default Domain Policy**, and then choose **Edit**.



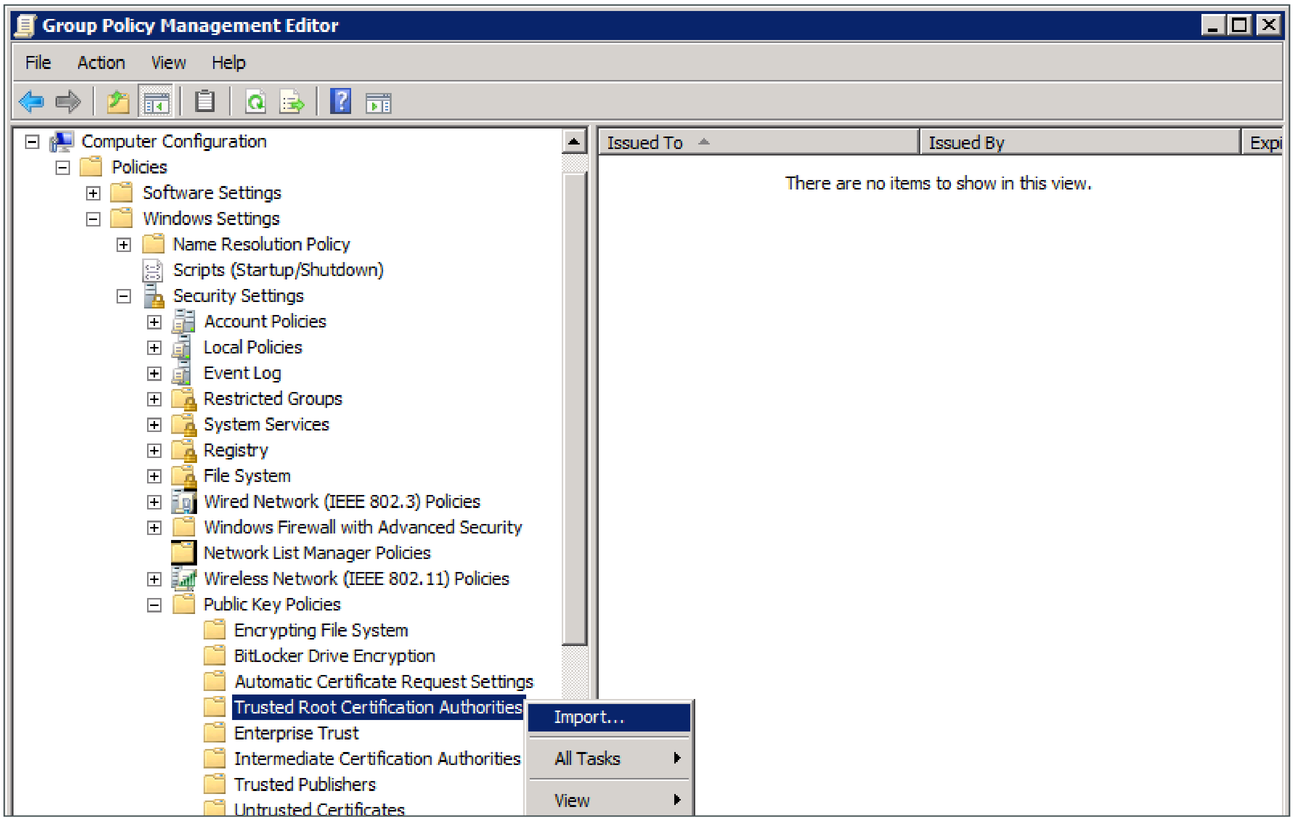
Display links in this location: cisco.local

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
cisco.local	No	Yes	cisco.local

The Group Policy Management Editor displays.

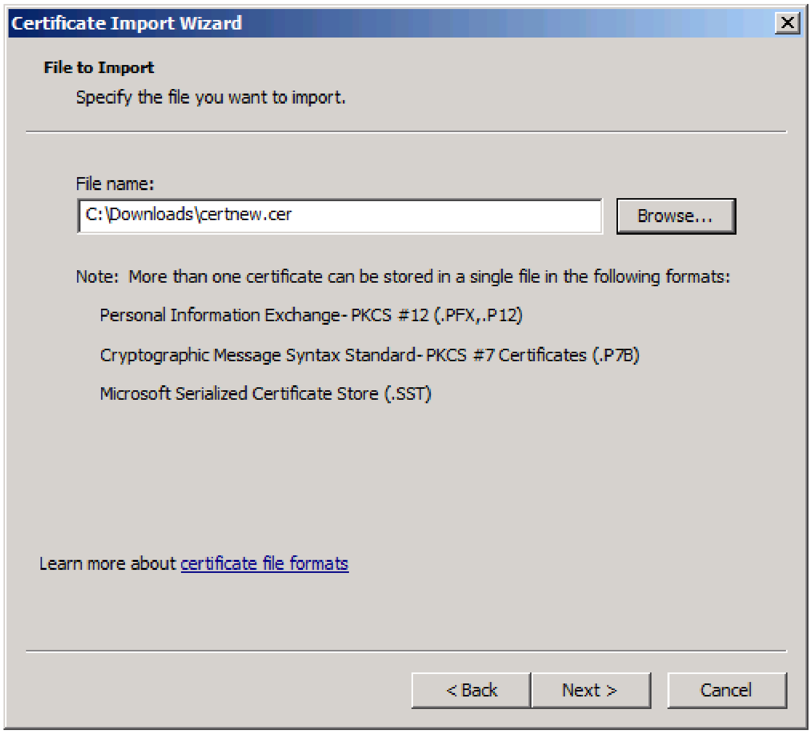
Step 8: Within the Group Policy Management Editor, navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies**, right-click **Trusted Root Certification Authorities**, and then choose **Import**.



There are no items to show in this view.

The Certificate Import Wizard launches.

Step 9: Click **Next**, click **Browse**, locate the trusted root certificate saved in Step 2, and then click **Next**.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

C:\Downloads\certnew.cer

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

Step 10: Place the certificate in the Trusted Root Certification Authorities certificate store, and then click **Next**.

Step 11: Click **Finish**. The certificate imports.

Step 12: Click **OK** to close the wizard.

Procedure 3 Install trusted root on AD server

In addition to configuring the AD server to distribute the trusted root certificate to workstations, you need to install the certificate directly onto the AD server. A group policy object (GPO) update takes care of this automatically. In this procedure, you will force the update to run immediately.

Step 1: On the AD console, navigate to **Start > Run**.

Step 2: Type **cmd**, and then press **Enter**. A command window opens.

Step 3: Update the group policy.

```
C:\> gpupdate
Updating policy. . .

User Policy update has completed successfully.
Computer Policy update has completed successfully.

C:\>
```

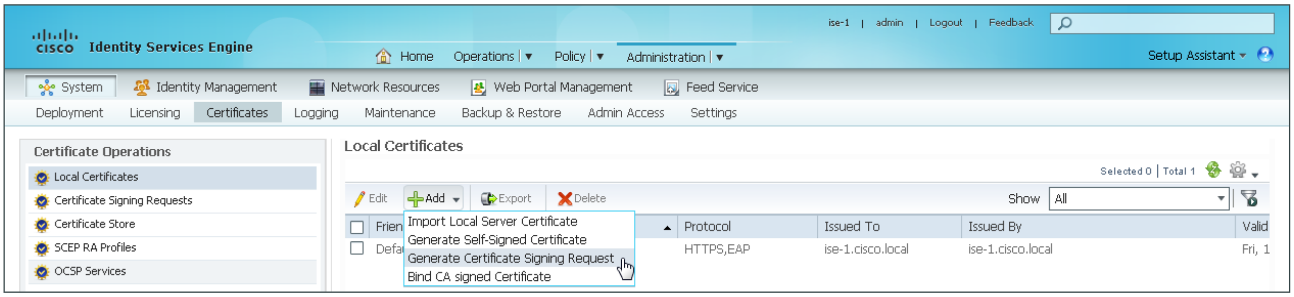
Procedure 4 Request a certificate for ISE from the CA

In order to obtain a certificate from the CA, Cisco ISE needs to generate a certificate signing request that will be used by the CA to generate the certificate for Cisco ISE.

Step 1: Connect to **https://ise-1.cisco.local**.

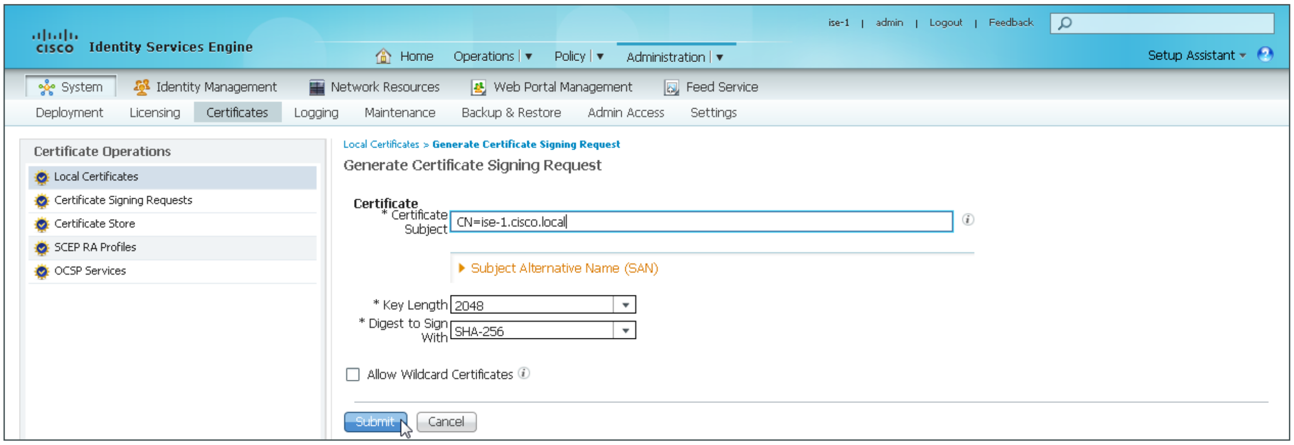
Step 2: Navigate to **Administration > System > Certificates**, and on the left, under Certificate Operations, select **Local Certificates**.

Step 3: Click **Add**, and then choose **Generate Certificate Signing Request**.



Frien	Protocol	Issued To	Issued By	Valid
Defa	HTTPS,EAP	ise-1.cisco.local	ise-1.cisco.local	Fri, 1

Step 4: In the **Certificate Subject** box, after the "CN=", enter the fully qualified domain name (FQDN) of the Cisco ISE server, and then click **Submit**.



* Certificate Subject: CN=ise-1.cisco.local

* Key Length: 2048

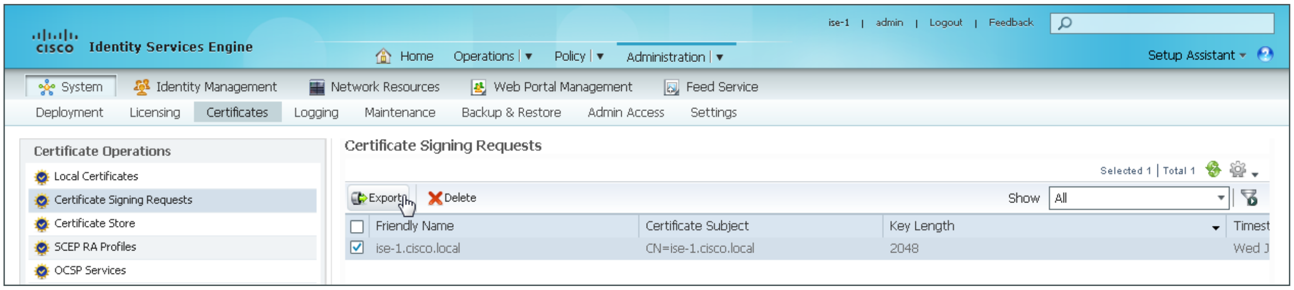
* Digest to Sign With: SHA-256

☐ Allow Wildcard Certificates

Step 5: On the message acknowledging that the certificate was successfully generated, click **OK**.

Step 6: On the left, under Certificate Operations, click **Certificate Signing Requests.**

Step 7: Select the check box next to the new request, and then click **Export**.



☐	Friendly Name	Certificate Subject	Key Length	Timest
☑	ise-1.cisco.local	CN=ise-1.cisco.local	2048	Wed J

Step 8: Save the file to your local machine. You use this file in a later procedure to generate a certificate on the CA for Cisco ISE.

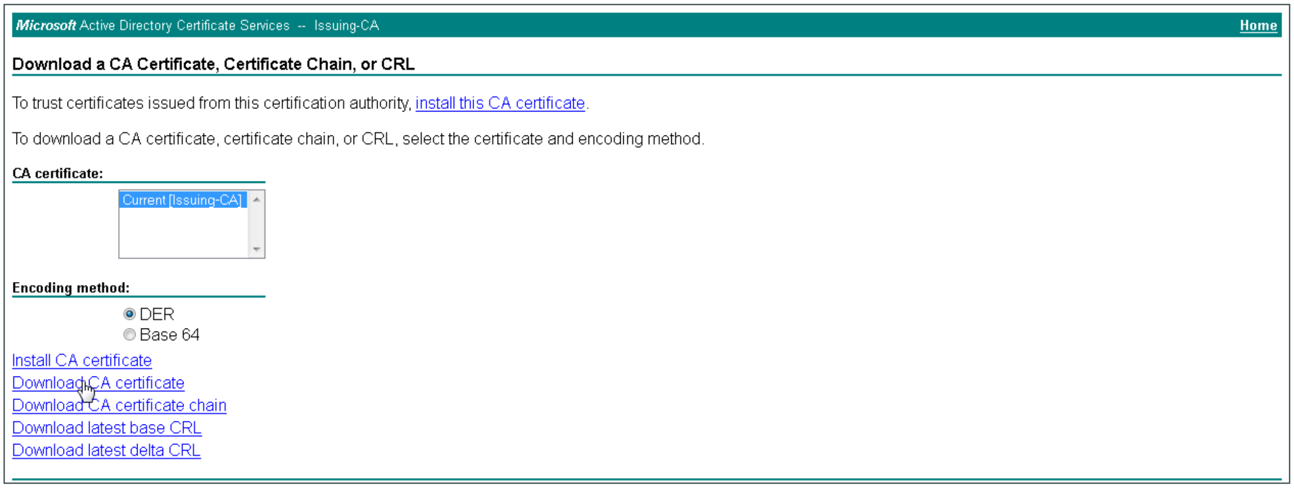
Procedure 5 Download CA root certificate

Step 1: Browse to **https://ca.cisco.local/certsrv**, and log in using an account with authority to generate certificates.

Step 2: Click **Download a CA certificate, certificate chain, or CRL**.

Step 3: Make sure the current certificate is selected and the **DER** encoding method is selected.

Step 4: Click **Download CA Certificate**, and then save the certificate file on the local machine.


Microsoft Active Directory Certificate Services -- Issuing-CA
Home

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate: Current [Issuing-CA]

Encoding method:

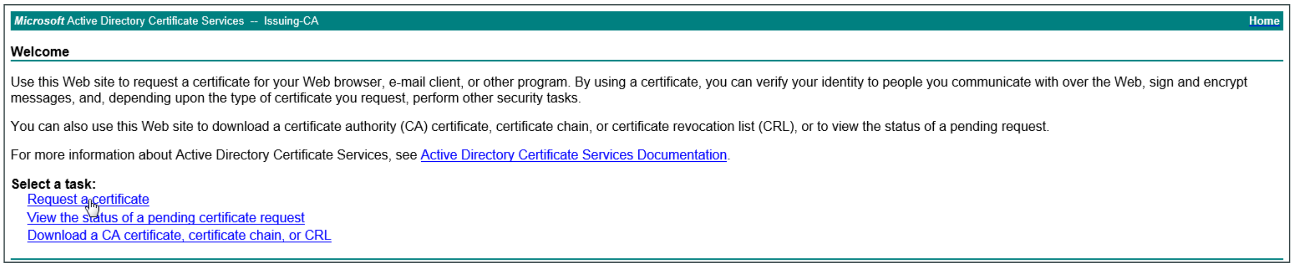
● DER
○ Base 64

Install CA certificate
Download CA certificate
Download CA certificate chain
Download latest base CRL
Download latest delta CRL

Procedure 6 Issue certificate for Cisco ISE

Step 1: At the top-right of the browser window, click **Home**. The CA's home screen displays.

Step 2: Click **Request a certificate**.



Microsoft Active Directory Certificate Services -- Issuing-CA

Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

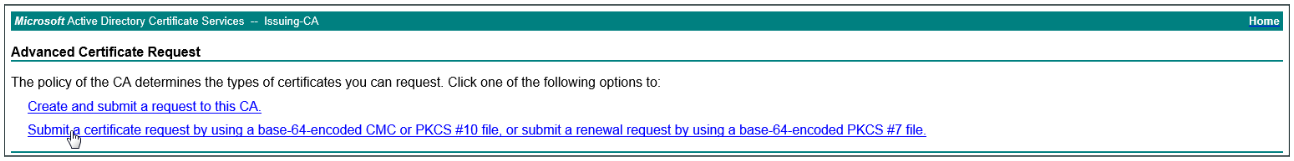
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:

Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

Step 3: Click the option that starts with **Submit a certificate request by using a base-64-encoded CMC**.



Microsoft Active Directory Certificate Services -- Issuing-CA

Home

Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

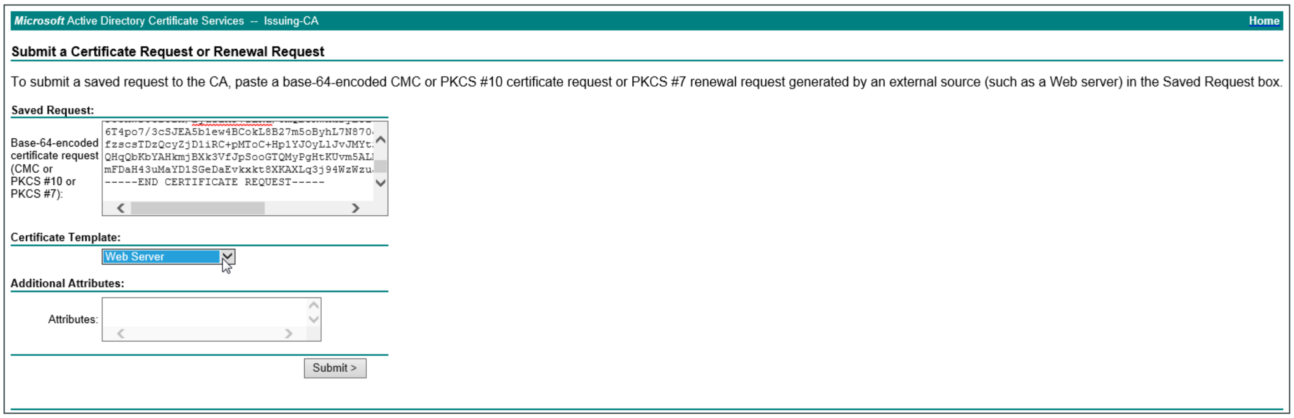
Create and submit a request to this CA.
Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

Step 4: In a text editor, such as Notepad, open the certificate file for ISE saved in Procedure 4, "Request a certificate for ISE from the CA."

Step 5: Select all the text, and then copy it to the clipboard.

Step 6: In the browser, on the Submit a Certificate Request or Renewal Request page, in the **Saved Request** box, paste the certificate contents.

Step 7: In the **Certificate Template** list, choose **Web Server**, and then click **Submit**.



Microsoft Active Directory Certificate Services -- Issuing-CA

Home

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
6T4po7/3cSJEA5b1ew4BCokL8B27m5oByhL7N870
fzscsTDzQcyZjD1iRC+pMToC+Hp1YJOyL1JvJMYt
QHqQbKbYAHkmjBXk3VfJpSooGTQMyPgHtKUvm5AL
mFDaH43uMaYD1SGeDaEvkxkt8XKAXLq3j94WzWzu
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

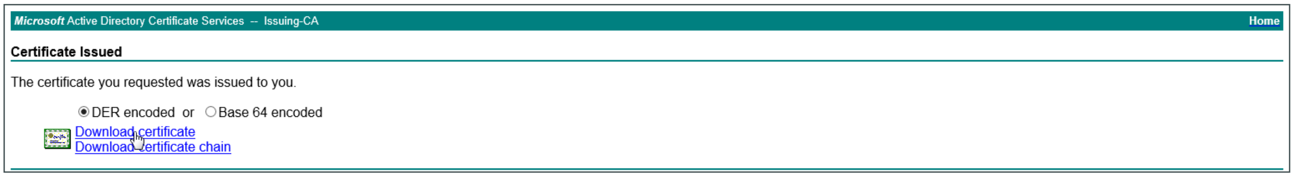
Web Server

Additional Attributes:

Attributes:

Submit >

Step 8: Select **DER encoded**, click **Download certificate**, and then save the certificate to your local machine.


Microsoft Active Directory Certificate Services -- Issuing-CA
Home

Certificate Issued

The certificate you requested was issued to you.

● DER encoded or ○ Base 64 encoded

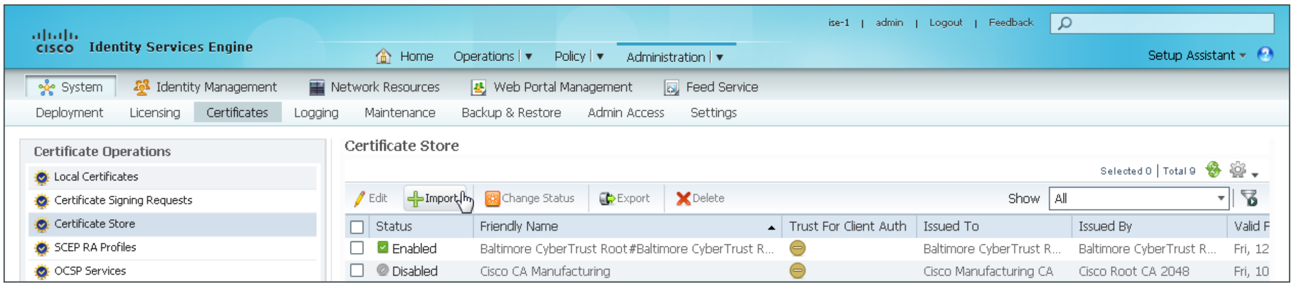
Download certificate
Download certificate chain

Procedure 7 Install trusted root certificate in Cisco ISE

Step 1: Connect to **https://ise-1.cisco.local**.

Step 2: Navigate to **Administration > System > Certificates.**

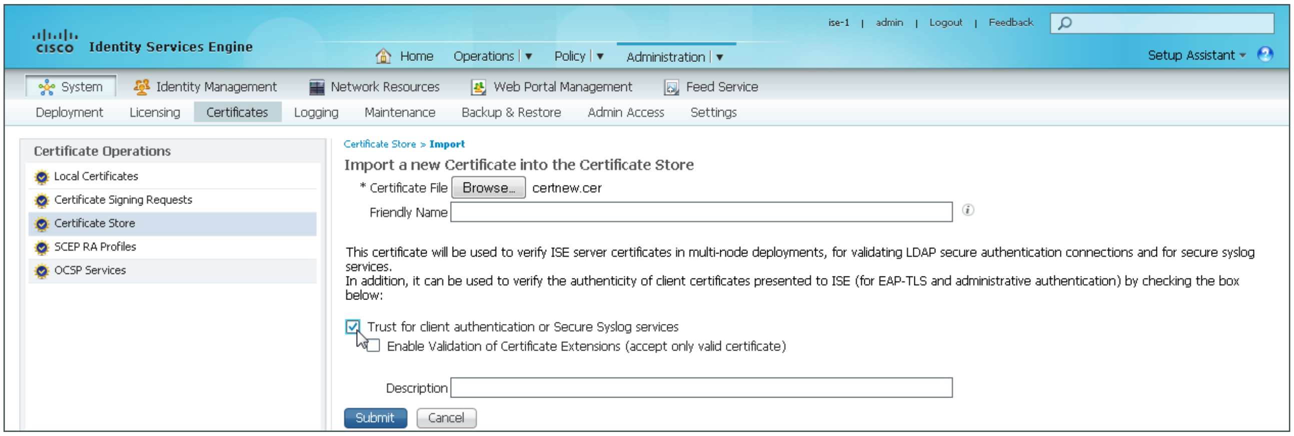
Step 3: On the left, under Certificate Operations, select **Certificate Store**, and then click **Import**.



☐	Status	Friendly Name	Trust For Client Auth	Issued To	Issued By	Valid F
☐	☑ Enabled	Baltimore CyberTrust Root#Baltimore CyberTrust R...	⊖	Baltimore CyberTrust R...	Baltimore CyberTrust R...	Fri, 12
☐	Disabled	Cisco CA Manufacturing	⊖	Cisco Manufacturing CA	Cisco Root CA 2048	Fri, 10

Step 4: Click **Browse**, and then locate and select the root CA certificate saved in Procedure 5, "Download CA root certificate."

Step 5: Select **Trust for client authentication**, and then click **Submit**. The certificate imports into the Certificate Store.



Import a new Certificate into the Certificate Store

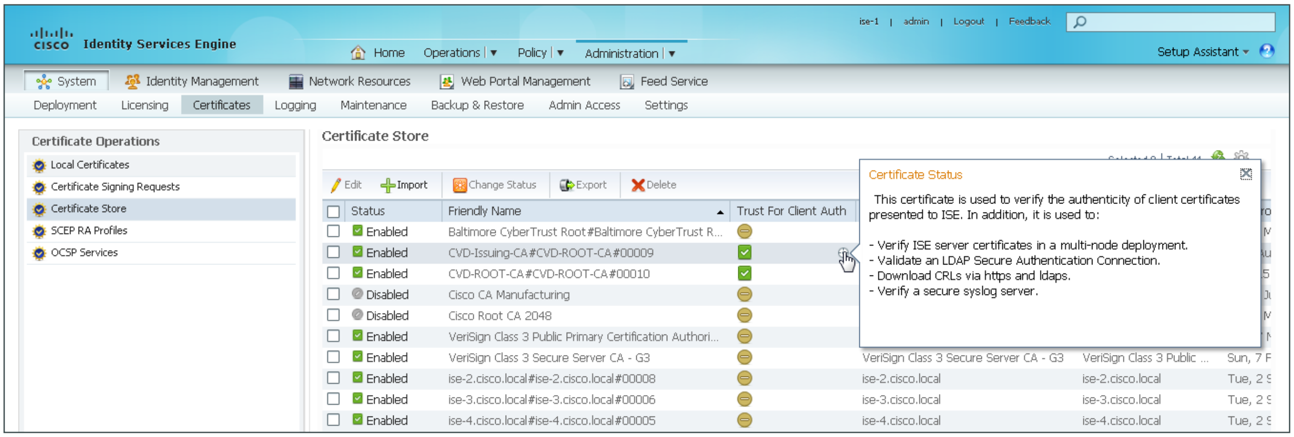
* Certificate File: certnew.cer

Friendly Name:

This certificate will be used to verify ISE server certificates in multi-node deployments, for validating LDAP secure authentication connections and for secure syslog services.
In addition, it can be used to verify the authenticity of client certificates presented to ISE (for EAP-TLS and administrative authentication) by checking the box below:

☑ Trust for client authentication or Secure Syslog services
☐ Enable Validation of Certificate Extensions (accept only valid certificate)

Description:



Certificate Store

☐	Status	Friendly Name	Trust For Client Auth			
☐	☑ Enabled	Baltimore CyberTrust Root#Baltimore CyberTrust R...	⊖			
☐	☑ Enabled	CVD-Issuing-CA#CVD-ROOT-CA#00009	☑			
☐	☑ Enabled	CVD-ROOT-CA#CVD-ROOT-CA#00010	☑			
☐	Disabled	Cisco CA Manufacturing	⊖			
☐	Disabled	Cisco Root CA 2048	⊖			
☐	☑ Enabled	VeriSign Class 3 Public Primary Certification Authori...	⊖			
☐	☑ Enabled	VeriSign Class 3 Secure Server CA - G3	⊖	VeriSign Class 3 Secure Server CA - G3	VeriSign Class 3 Public ...	Sun, 7 F
☐	☑ Enabled	ise-2.cisco.local#ise-2.cisco.local#00008	⊖	ise-2.cisco.local	ise-2.cisco.local	Tue, 2
☐	☑ Enabled	ise-3.cisco.local#ise-3.cisco.local#00006	⊖	ise-3.cisco.local	ise-3.cisco.local	Tue, 2
☐	☑ Enabled	ise-4.cisco.local#ise-4.cisco.local#00005	⊖	ise-4.cisco.local	ise-4.cisco.local	Tue, 2

Certificate Status

This certificate is used to verify the authenticity of client certificates presented to ISE. In addition, it is used to:

- Verify ISE server certificates in a multi-node deployment.
- Validate an LDAP Secure Authentication Connection.
- Download CRLs via https and ldaps.
- Verify a secure syslog server.

Tech Tip

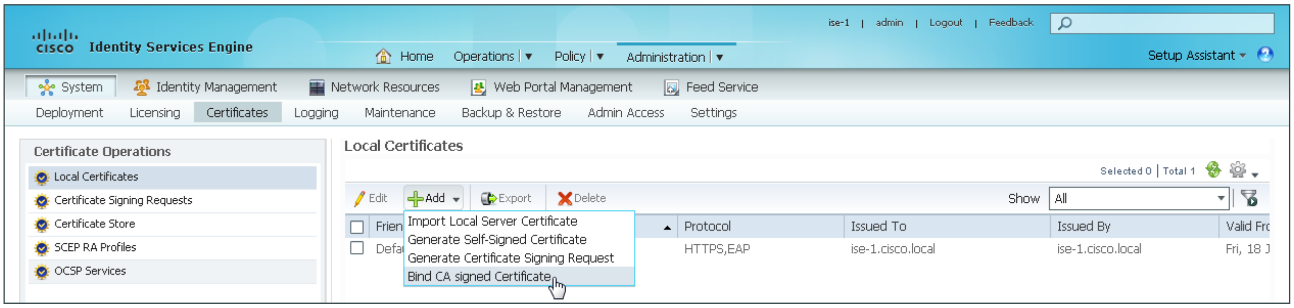
If you are obtaining a certificate from a subordinate certificate authority, then you also need to obtain the trusted root certificate from every CA in the certificate chain, install them individually into the ISE certificate store, and trust them for client authentication. In the above example, the server certificate for ISE was issued by CVD-Issuing-CA, which is subordinate to CVD-ROOT-CA, and both trusted root certificates are installed.

Procedure 8 Install local certificate in Cisco ISE

Step 1: Navigate to **Administration > System > Certificates**.

Step 2: On the left, under Certificate Operations, select **Local Certificates**.

Step 3: Click **Add**, and then choose **Bind CA Certificate**.



Local Certificates

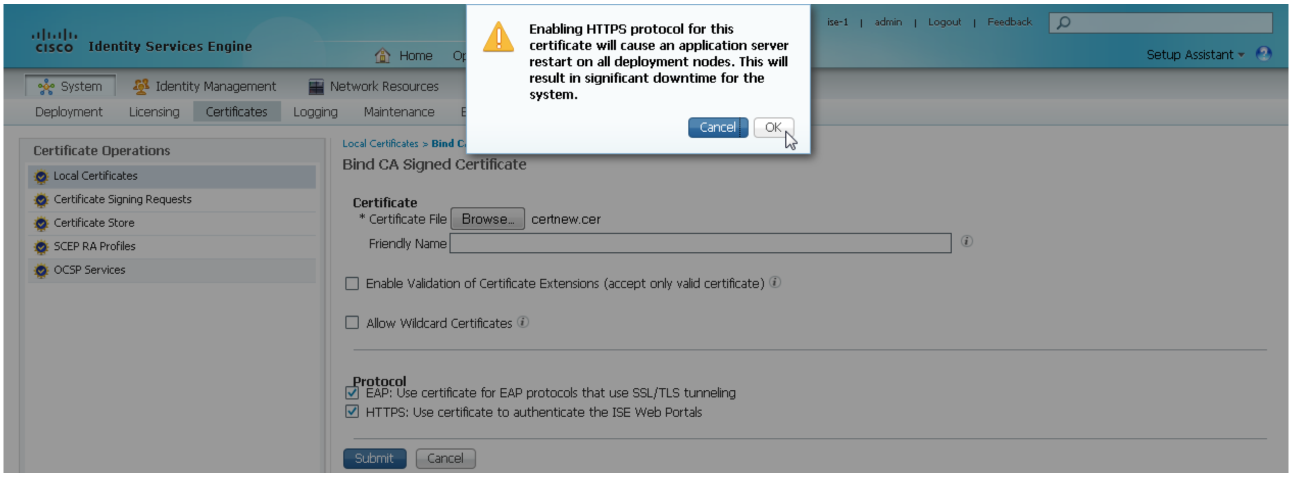
Show: All

☐	Frien	Protocol	Issued To	Issued By	Valid Fr
☐	Defa	HTTPS,EAP	ise-1.cisco.local	ise-1.cisco.local	Fri, 18 J

Step 4: Click **Browse** and locate the certificate saved from Procedure 6, “Issue certificate for Cisco ISE.”

Step 5: In the Protocol section, select both **EAP** and **HTTPS**. Selecting HTTPS requires the Cisco ISE server to restart, which displays a notification message.

Step 6: Click **OK** to acknowledge the notification, and then click **Submit**.



Enabling HTTPS protocol for this certificate will cause an application server restart on all deployment nodes. This will result in significant downtime for the system.

Bind CA Signed Certificate

Certificate
* Certificate File certnew.cer
Friendly Name

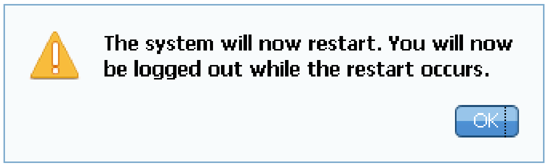
☐ Enable Validation of Certificate Extensions (accept only valid certificate)

☐ Allow Wildcard Certificates

Protocol
☑ EAP: Use certificate for EAP protocols that use SSL/TLS tunneling
☑ HTTPS: Use certificate to authenticate the ISE Web Portals

You are notified that the Cisco ISE appliance is restarting.

Step 7: Wait while the appliance restarts. You do not need to acknowledge the message.



The system will now restart. You will now be logged out while the restart occurs.

Procedure 9 Delete old certificate and request

Now that you have imported the local certificate into Cisco ISE, you need to delete the old self-signed certificate as well as the certificate signing request generated previously.

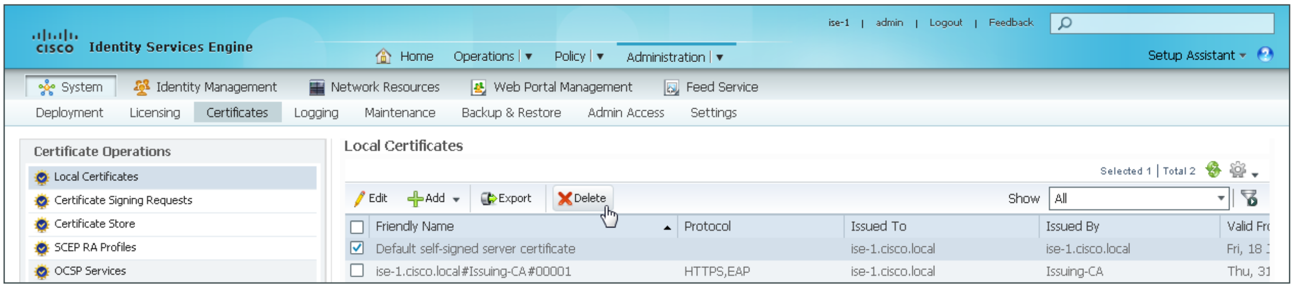
Step 1: After the server has finished booting, reconnect to **https://ise-1.cisco.local**.

Step 2: Navigate to **Administration > System > Certificates**.

Step 3: On the left, under Certificate Operations, select **Local Certificates**.

Step 4: Select the box next to the self-signed certificate. This is the certificate issued by the Cisco ISE appliance and not the certificate issued by the CA that was just imported.

Step 5: Click **Delete**, and then click **OK**.



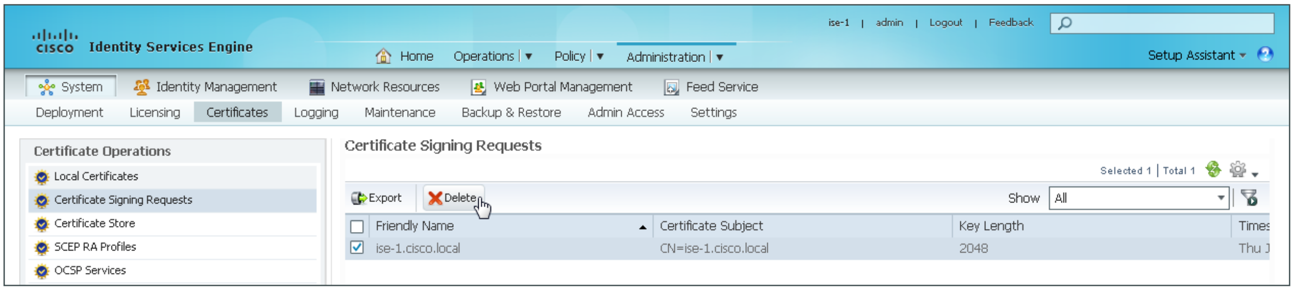
☐	Friendly Name	Protocol	Issued To	Issued By	Valid Fr
☑	Default self-signed server certificate		ise-1.cisco.local	ise-1.cisco.local	Fri, 18
☐	ise-1.cisco.local#Issuing-CA#00001	HTTPS,EAP	ise-1.cisco.local	Issuing-CA	Thu, 31

The obsolete self-signed certificate is deleted.

Step 6: On the left, under Certificate Operations, select **Certificate Signing Requests**.

Step 7: Select the box next to the certificate signing request that was created in Procedure 4, “Request a certificate for ISE from the CA.”

Step 8: Click **Delete**, and then click **OK**. The obsolete certificate signing request is deleted.



☐	Friendly Name	Certificate Subject	Key Length	Times
☑	ise-1.cisco.local	CN=ise-1.cisco.local	2048	Thu J

PROCESS

Enabling 802.1X Authentication

1. Create user authentication policies
2. Create machine authentication policies
3. Modify authentication policy to use certificates
4. Enable EAP-TLS

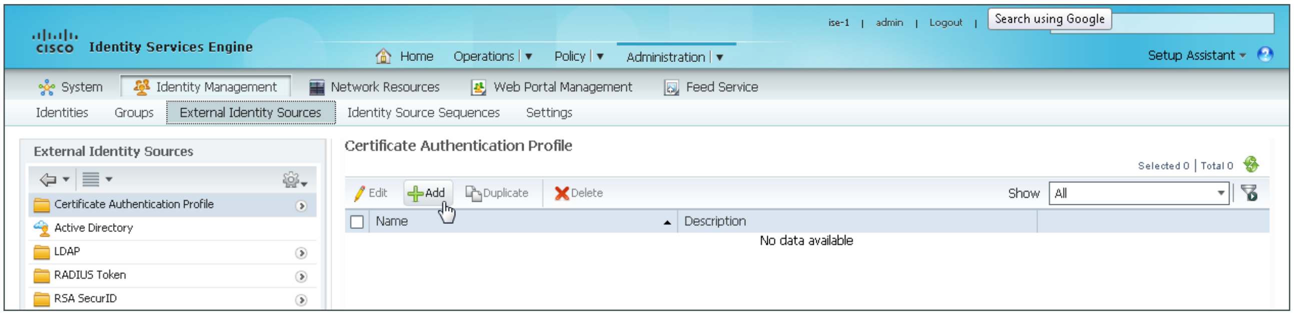
In this procedure, you configure Cisco ISE policies to support 802.1X authentication using digital certificates for both wired and wireless users.

Procedure 1 Create user authentication policies

An authentication profile is used to determine how a certificate will be used for authentication. You create an authentication profile for user authentication using certificates.

Step 1: In Cisco ISE, navigate to **Administration > Identity Management > External Identity Sources**.

Step 2: In the left pane, click **Certificate Authentication Profile**, and then click **Add**.



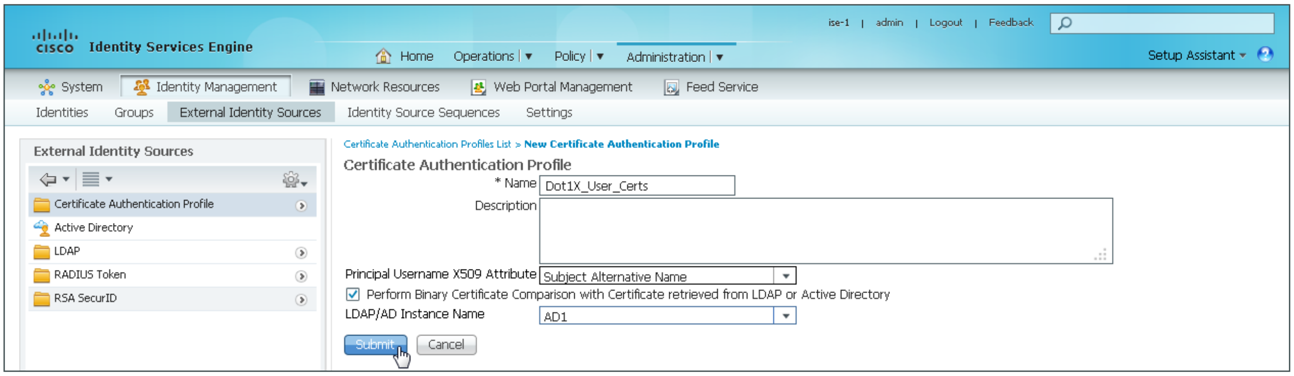
☐	Name	Description
		No data available

Step 3: Give the profile a meaningful name.

Step 4: In the **Principal Username X509 Attribute** list, choose **Subject Alternative Name**.

Step 5: Select **Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory.**

Step 6: In the **LDAP/AD Instance Name** list, choose previously defined AD server **AD1**, and then click Submit.


cisco Identity Services Engine
ise-1 | admin | Logout | Feedback
Home
Operations
Policy
Administration
Setup Assistant
System
Identity Management
Network Resources
Web Portal Management
Feed Service
Identities
Groups
External Identity Sources
Identity Source Sequences
Settings
External Identity Sources
Certificate Authentication Profile
Active Directory
LDAP
RADIUS Token
RSA SecurID
Certificate Authentication Profiles List > New Certificate Authentication Profile
Submit
Cancel

Certificate Authentication Profile

* Name: Dot1X_User_Certs

Description:

Principal Username X509 Attribute: Subject Alternative Name

☑ Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory

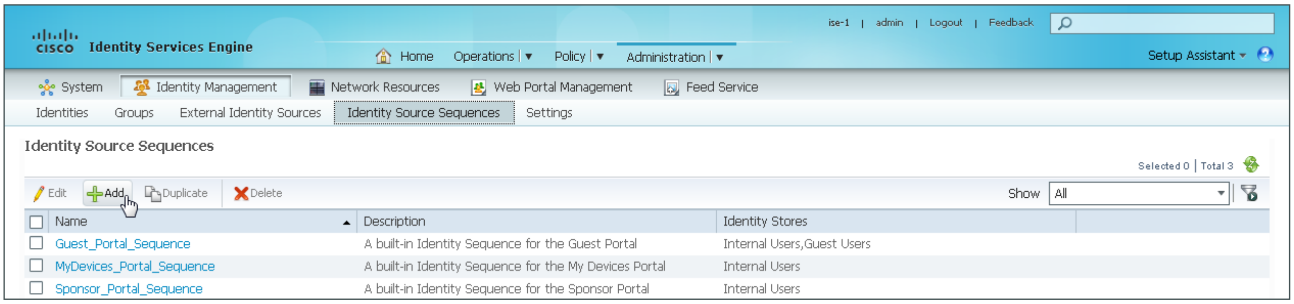
LDAP/AD Instance Name: AD1

Tech Tip

When using certificates for authentication, Cisco ISE does not need to proxy the authentication request to Active Directory. However, without contacting Active Directory, you won't get additional information about the user, such as group membership. By performing the certificate comparison with Active Directory, you can get that information and use it for policy decisions.

An identity source sequence allows certificates to be used as an identity store and also allows for a backup identity store if a primary identity store is unavailable.

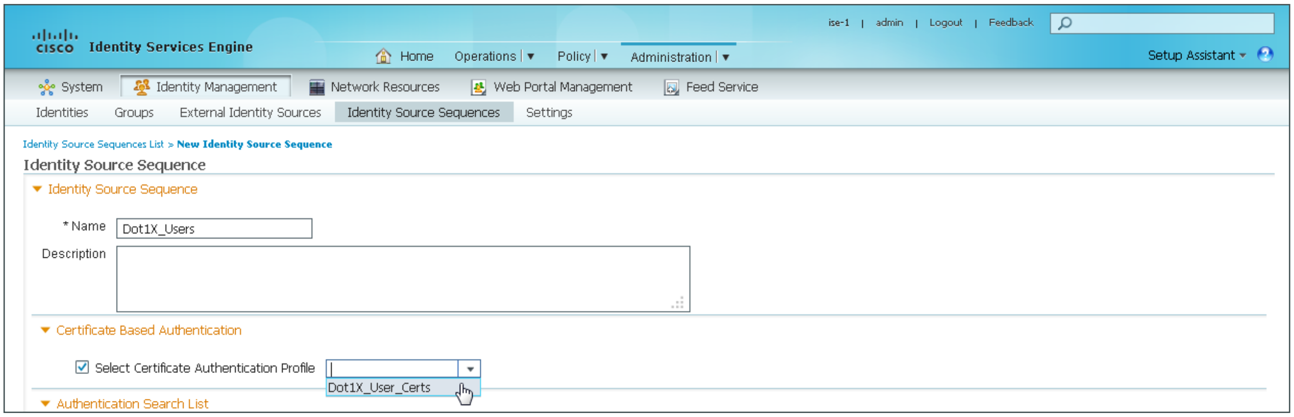
Step 7: At the top, click the **Identity Source Sequences** tab, and then click **Add**.



Identity Source Sequences

☐ Name	Description	Identity Stores
☐ Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal	Internal Users,Guest Users
☐ MyDevices_Portal_Sequence	A built-in Identity Sequence for the My Devices Portal	Internal Users
☐ Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal	Internal Users

Step 8: Give the sequence a meaningful name.



Identity Source Sequences List > **New Identity Source Sequence**

Identity Source Sequence

Identity Source Sequence

* Name Dot1X_Users

Description

Certificate Based Authentication

☑ Select Certificate Authentication Profile

Dot1X_User_Certs

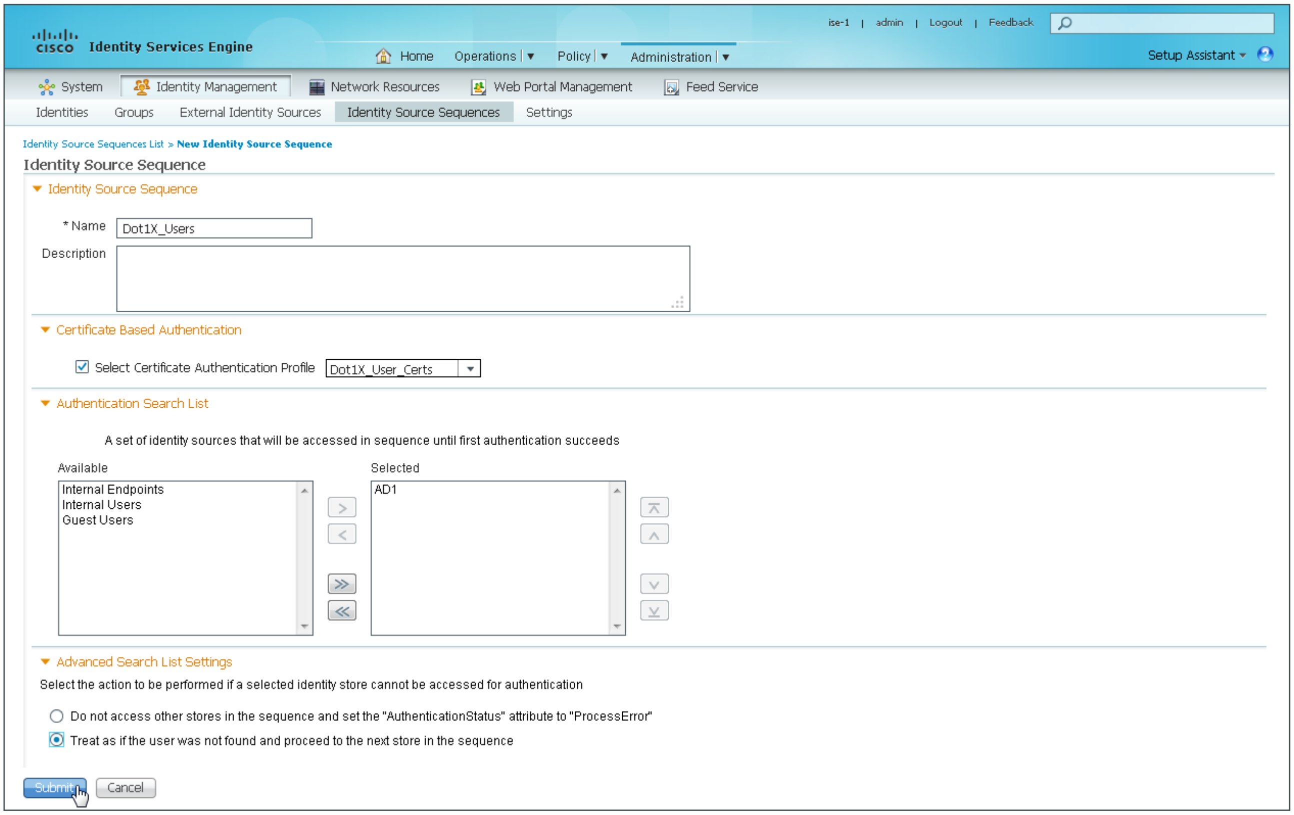
Authentication Search List

Step 9: In the Certificate Based Authentication section, select **Select Certificate Authentication Profile**.

Step 10: In the **Available** list, choose the profile created in Step 5.

Step 11: In the Authentication Search List section, in the **Available** list, double-click the AD server. It moves into the **Selected** list.

Step 12: In the Advanced Search List Settings section, select **Treat as if the user was not found and proceed to the next store in the sequence**, and then click **Submit**.



Identity Source Sequences List > **New Identity Source Sequence**

Identity Source Sequence

Identity Source Sequence

* Name Dot1X_Users

Description

Certificate Based Authentication

☑ Select Certificate Authentication Profile Dot1X_User_Certs

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
Internal Endpoints Internal Users Guest Users	AD1

Advanced Search List Settings

Select the action to be performed if a selected identity store cannot be accessed for authentication

○ Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"

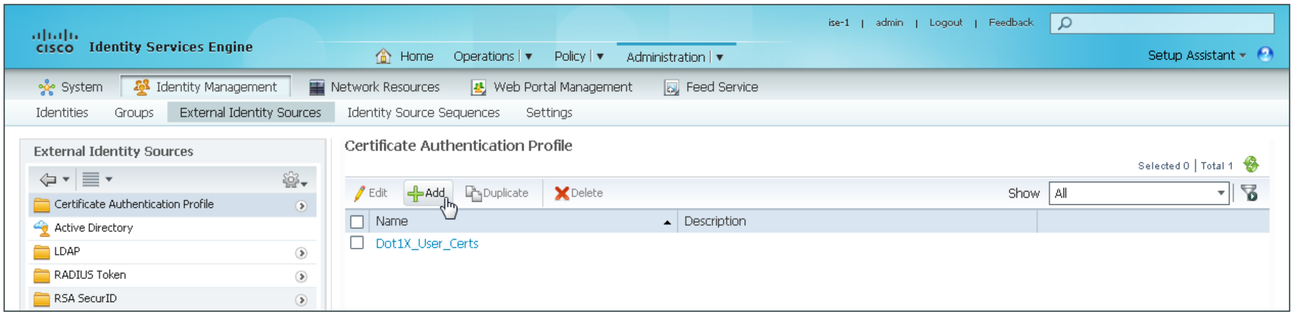
● Treat as if the user was not found and proceed to the next store in the sequence

Procedure 2 Create machine authentication policies

You create an authentication profile for machine authentication using certificates.

Step 1: In Cisco ISE, navigate to **Administration > Identity Management > External Identity Sources**.

Step 2: In the left pane, click **Certificate Authentication Profile,** and then click **Add**.

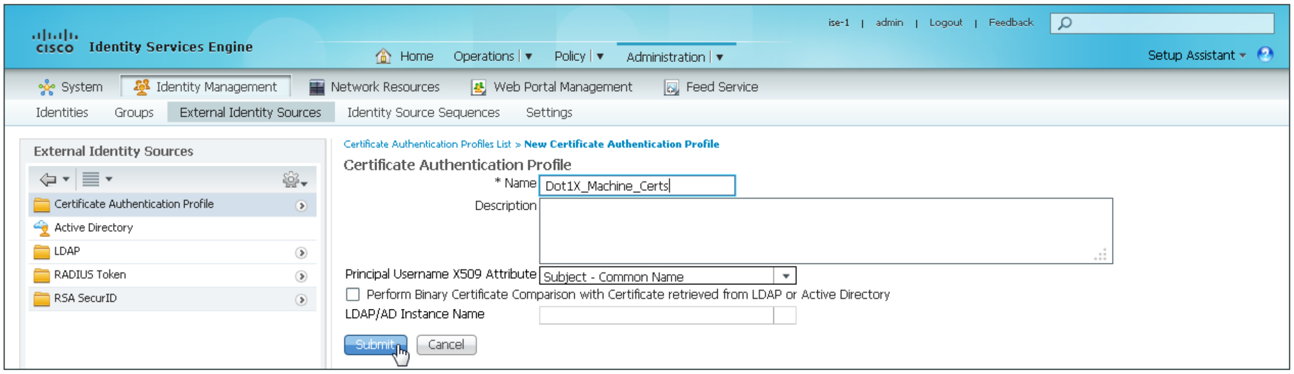

Identity Services Engine
ise-1 | admin | Logout | Feedback
Home Operations Policy Administration
Setup Assistant
System Identity Management Network Resources Web Portal Management Feed Service
Identities Groups External Identity Sources Identity Source Sequences Settings
External Identity Sources
Certificate Authentication Profile
Active Directory
LDAP
RADIUS Token
RSA SecurID
Certificate Authentication Profile
Selected 0 | Total 1
Edit Add Duplicate Delete
Show All

☐	Name	Description
☐	Dot1X_User_Certs	

Step 3: Give the profile a meaningful name.

Step 4: In the **Principal Username X509 Attribute** list, choose **Common Name**.

Step 5: Click **Submit**.


Identity Services Engine
ise-1 | admin | Logout | Feedback
Home Operations Policy Administration
Setup Assistant
System Identity Management Network Resources Web Portal Management Feed Service
Identities Groups External Identity Sources Identity Source Sequences Settings
External Identity Sources
Certificate Authentication Profile
Active Directory
LDAP
RADIUS Token
RSA SecurID
Certificate Authentication Profiles List > New Certificate Authentication Profile
Certificate Authentication Profile
Submit Cancel

* Name: Dot1X_Machine_Certs

Description:

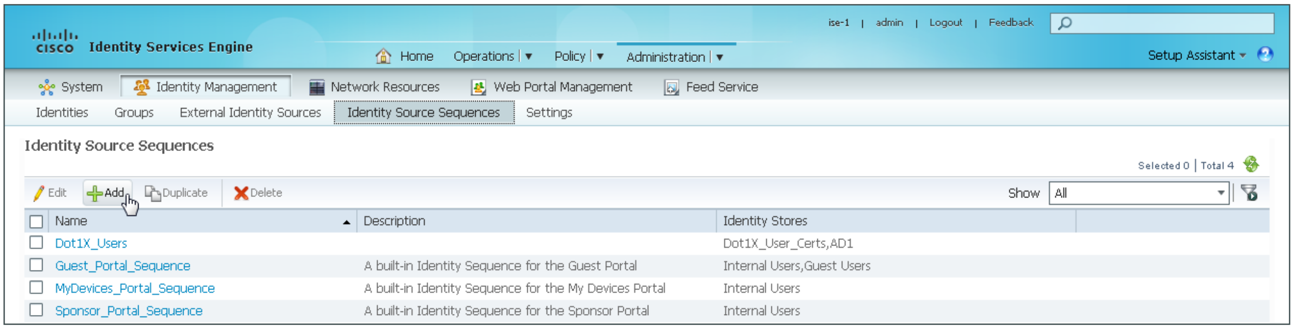
Principal Username X509 Attribute: Subject - Common Name

☐ Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory

LDAP/AD Instance Name:

An identity source sequence allows certificates to be used as an identity store and also allows for a backup identity store if the primary identity store is unavailable.

Step 6: At the top, click the **Identity Source Sequences** tab, and then click **Add**.

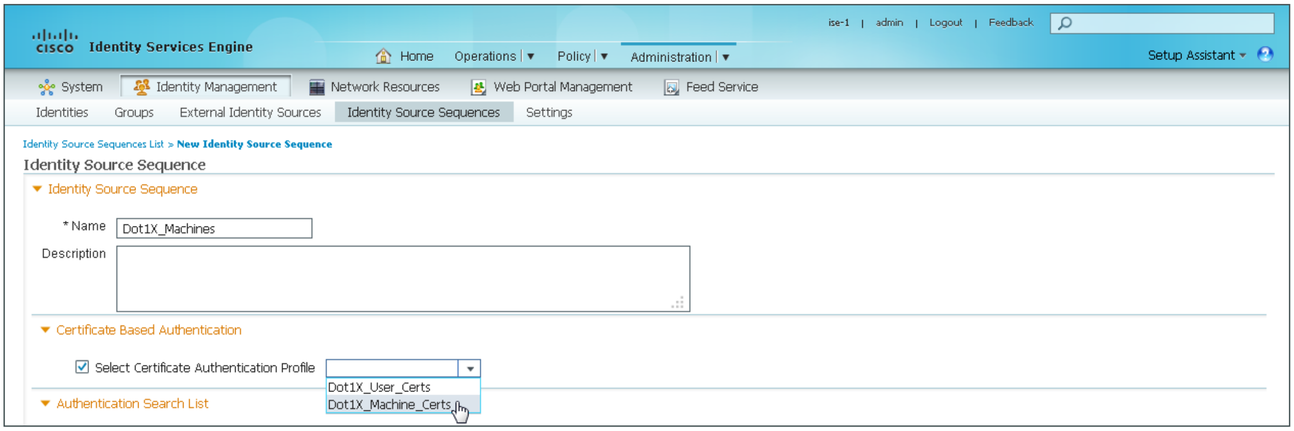

Identity Services Engine
ise-1 | admin | Logout | Feedback
Home Operations Policy Administration
Setup Assistant
System Identity Management Network Resources Web Portal Management Feed Service
Identities Groups External Identity Sources Identity Source Sequences Settings
Identity Source Sequences
Selected 0 | Total 4
Edit Add Duplicate Delete
Show All

☐	Name	Description	Identity Stores
☐	Dot1X_Users		Dot1X_User_Certs,AD1
☐	Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal	Internal Users,Guest Users
☐	MyDevices_Portal_Sequence	A built-in Identity Sequence for the My Devices Portal	Internal Users
☐	Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal	Internal Users

Step 7: Give the sequence a meaningful name.

Step 8: In the Certificate Based Authentication section, select **Select Certificate Authentication Profile**.

Step 9: In the **Select Certificate Authentication** list, choose the profile created in Step 5.



* Name: Dot1X_Machines

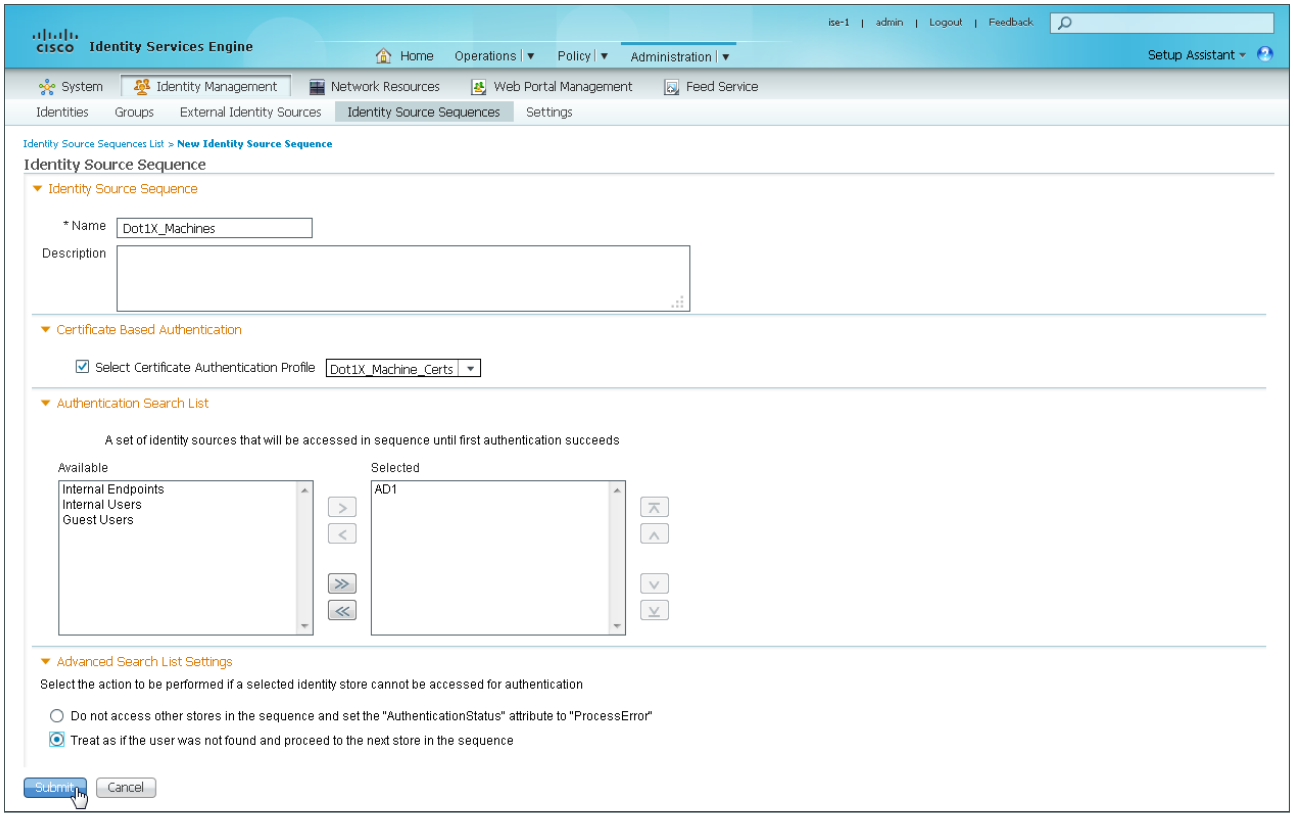
Description:

☑ Select Certificate Authentication Profile

Dot1X_User_Certs
Dot1X_Machine_Certs

Step 10: In the Authentication Search List section, in the **Available** list, double-click the AD server. It moves into the **Selected** list.

Step 11: In the Advanced Search List Settings section, select **Treat as if the user was not found and proceed to the next store in the sequence**, and then click **Submit**.



* Name: Dot1X_Machines

Description:

☑ Select Certificate Authentication Profile: Dot1X_Machine_Certs

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
Internal Endpoints Internal Users Guest Users	AD1

Select the action to be performed if a selected identity store cannot be accessed for authentication

○ Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"

● Treat as if the user was not found and proceed to the next store in the sequence

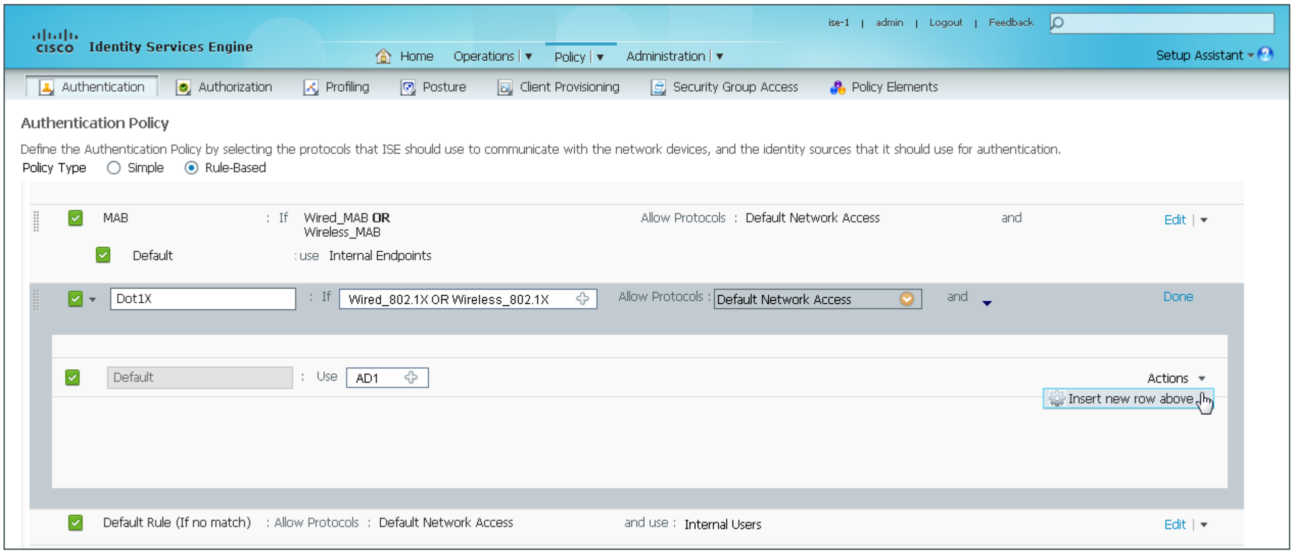
Procedure 3 Modify authentication policy to use certificates

Now that you have created certificate authentication profiles and identity source sequences for digital certificates, you need to enable the 802.1X authentication policies for machine authentication and user authentication for wired and wireless users.

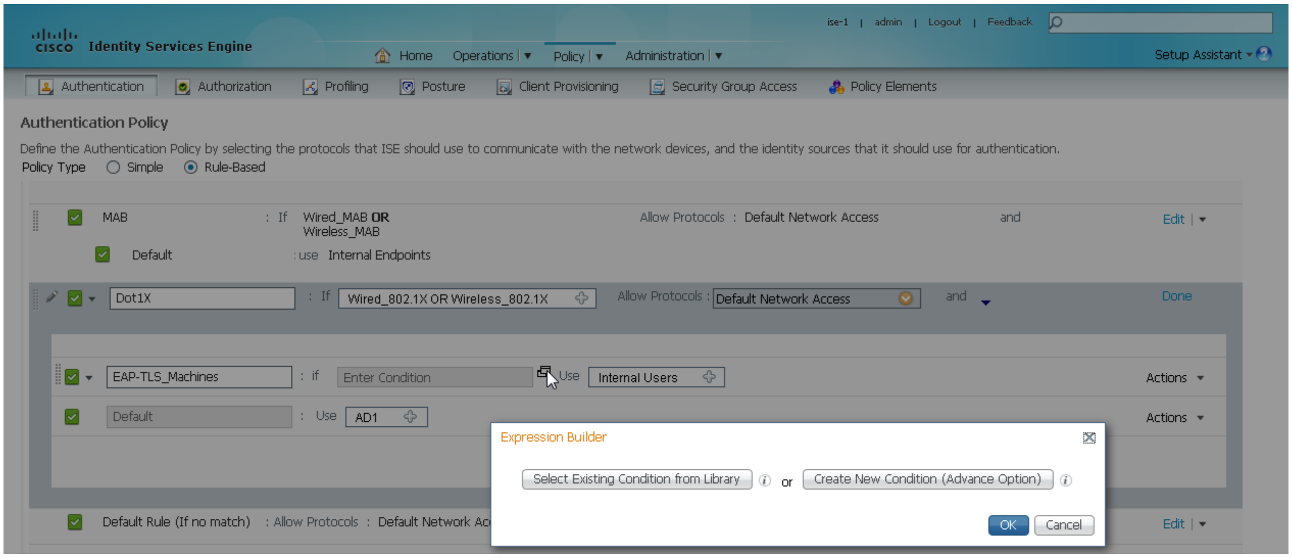
Step 1: Navigate to **Policy > Authentication**.

Step 2: In the Authentication Policy list of rules, on the right side of the **Dot1X** rule, click **Edit**. The details are revealed for the identity store used in this rule.

Step 3: In the same Dot1X rule, next to the Default row showing the identity store, click the **Actions** list, and then choose **Insert new row above**.

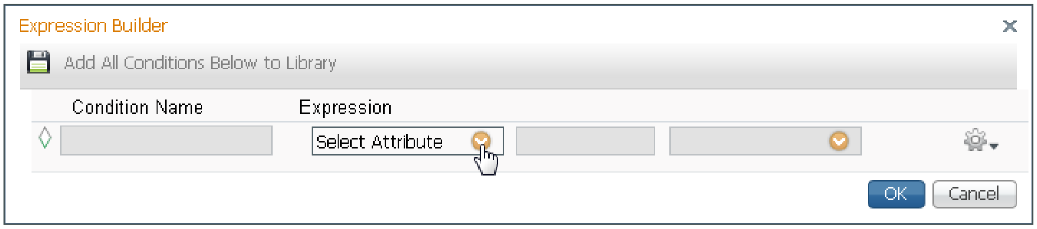

Identity Services Engine
ise-1 | admin | Logout | Feedback
Home
Operations
Policy
Administration
Setup Assistant
Authentication
Authorization
Profiling
Posture
Client Provisioning
Security Group Access
Policy Elements
Authentication Policy
Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.
Policy Type ○ Simple ● Rule-Based
MAB : If Wired_MAB OR Wireless_MAB Allow Protocols : Default Network Access and Edit
Default : use Internal Endpoints
Dot1X : If Wired_802.1X OR Wireless_802.1X Allow Protocols : Default Network Access and Done
Default : Use AD1 Actions
Insert new row above
Default Rule (If no match) : Allow Protocols : Default Network Access and use : Internal Users Edit

Step 4: Give the rule a name, and then next to the Enter Condition box, click the box symbol. The Expression Builder opens.

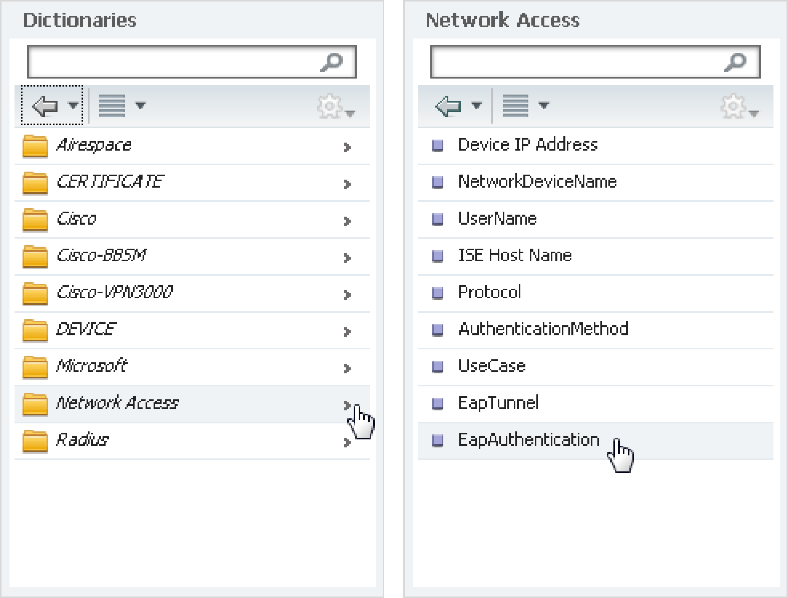

Identity Services Engine
ise-1 | admin | Logout | Feedback
Home
Operations
Policy
Administration
Setup Assistant
Authentication
Authorization
Profiling
Posture
Client Provisioning
Security Group Access
Policy Elements
Authentication Policy
Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.
Policy Type ○ Simple ● Rule-Based
MAB : If Wired_MAB OR Wireless_MAB Allow Protocols : Default Network Access and Edit
Default : use Internal Endpoints
Dot1X : If Wired_802.1X OR Wireless_802.1X Allow Protocols : Default Network Access and Done
EAP-TLS_Machines : if Enter Condition Use Internal Users Actions
Default : Use AD1 Actions
Default Rule (If no match) : Allow Protocols : Default Network Ac Edit
Expression Builder
Select Existing Condition from Library or Create New Condition (Advance Option)
OK
Cancel

Step 5: Click **Create New Condition (Advance Option)**.

Step 6: In the **Expression** list, next to **Select Attribute**, click the arrow**.**

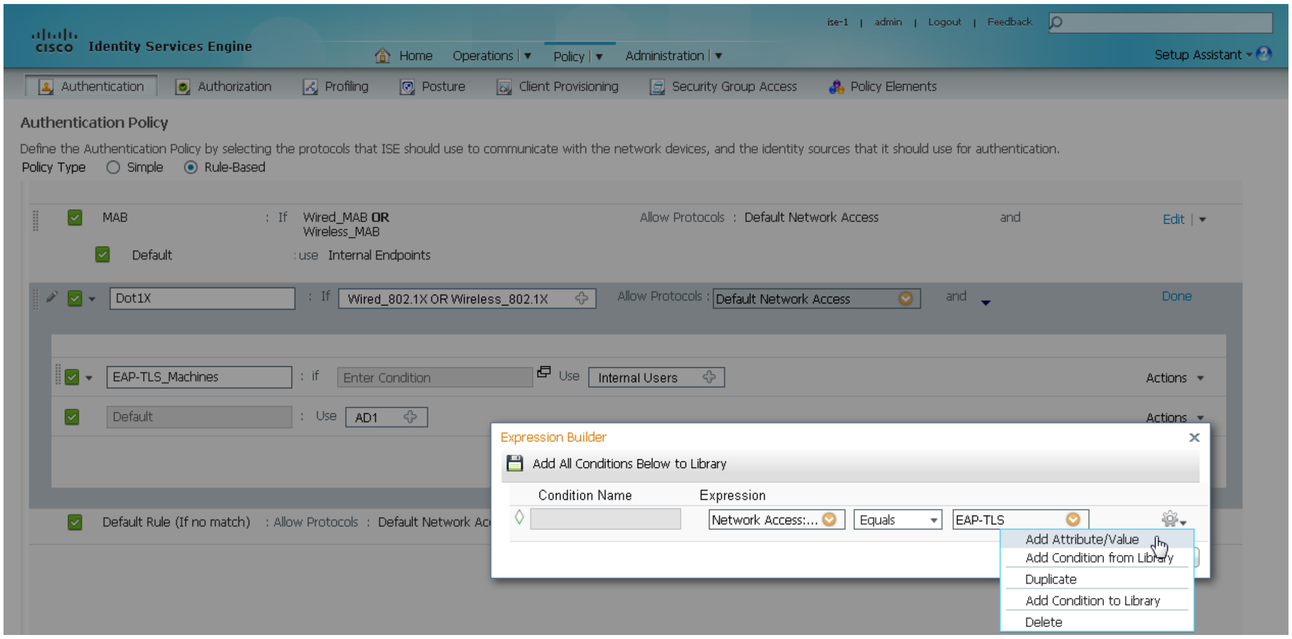


Step 7: Click Network Access, and then choose **EapAuthentication**.



Step 8: In the second list, choose **Equals,** and in the last list, choose **EAP-TLS**.

Step 9: Click the gear icon at the end of the condition, and then choose **Add Attribute/Value**.


Identity Services Engine
ise-1 | admin | Logout | Feedback
Home Operations Policy Administration
Setup Assistant
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Expression Builder
Add All Conditions Below to Library
Add Attribute/Value
Add Condition from Library
Duplicate
Add Condition to Library
Delete

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type ○ Simple ● Rule-Based

☑ MAB : If Wired_MAB OR Wireless_MAB Allow Protocols : Default Network Access and Edit

☑ Default : use Internal Endpoints

☑ Dot1X : If Wired_802.1X OR Wireless_802.1X Allow Protocols : Default Network Access and Done

☑ EAP-TLS_Machines : if Enter Condition Use Internal Users Actions

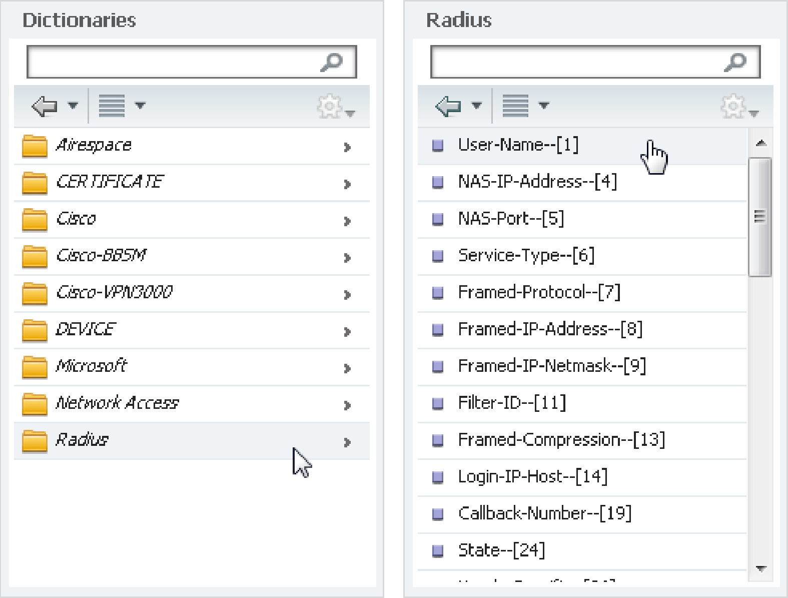
☑ Default : Use AD1 Actions

☑ Default Rule (If no match) : Allow Protocols : Default Network Ac

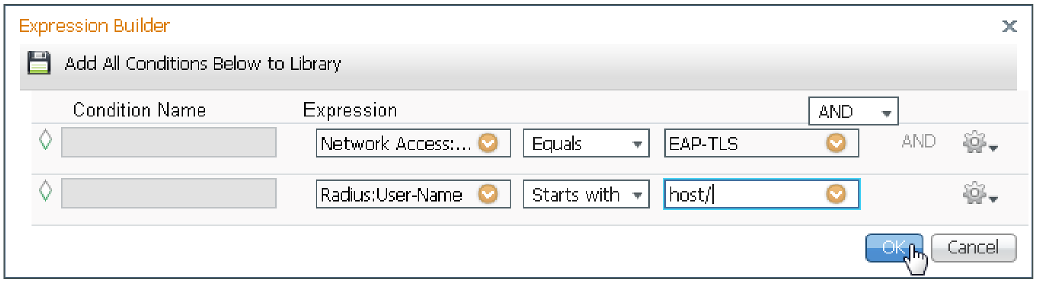
Condition Name	Expression		
	Network Access:...	Equals	EAP-TLS

Step 10: In the **Expression** list, next to Select Attribute, click the arrow.

Step 11: Select **Radius**, and then select **User-Name--[1]**.



Step 12: In the second list, choose **Starts with,** and in the last box, type **host/** and then click **OK**.

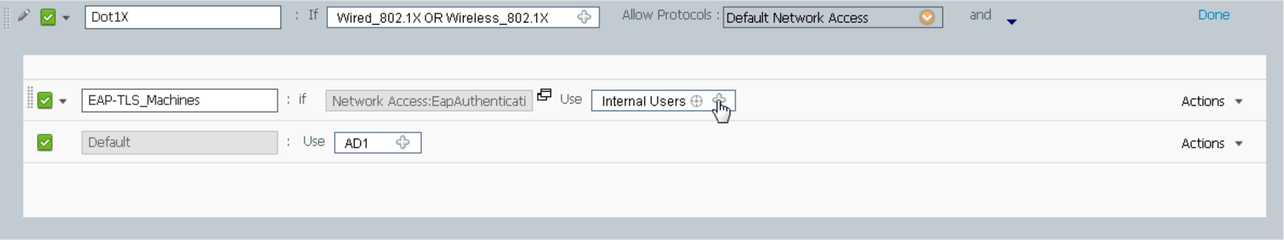


AND

Network Access:... Equals EAP-TLS AND

Radius:User-Name Starts with host/

Step 13: On the new row you are creating for the rule, next to Internal Users, click the **+** symbol.



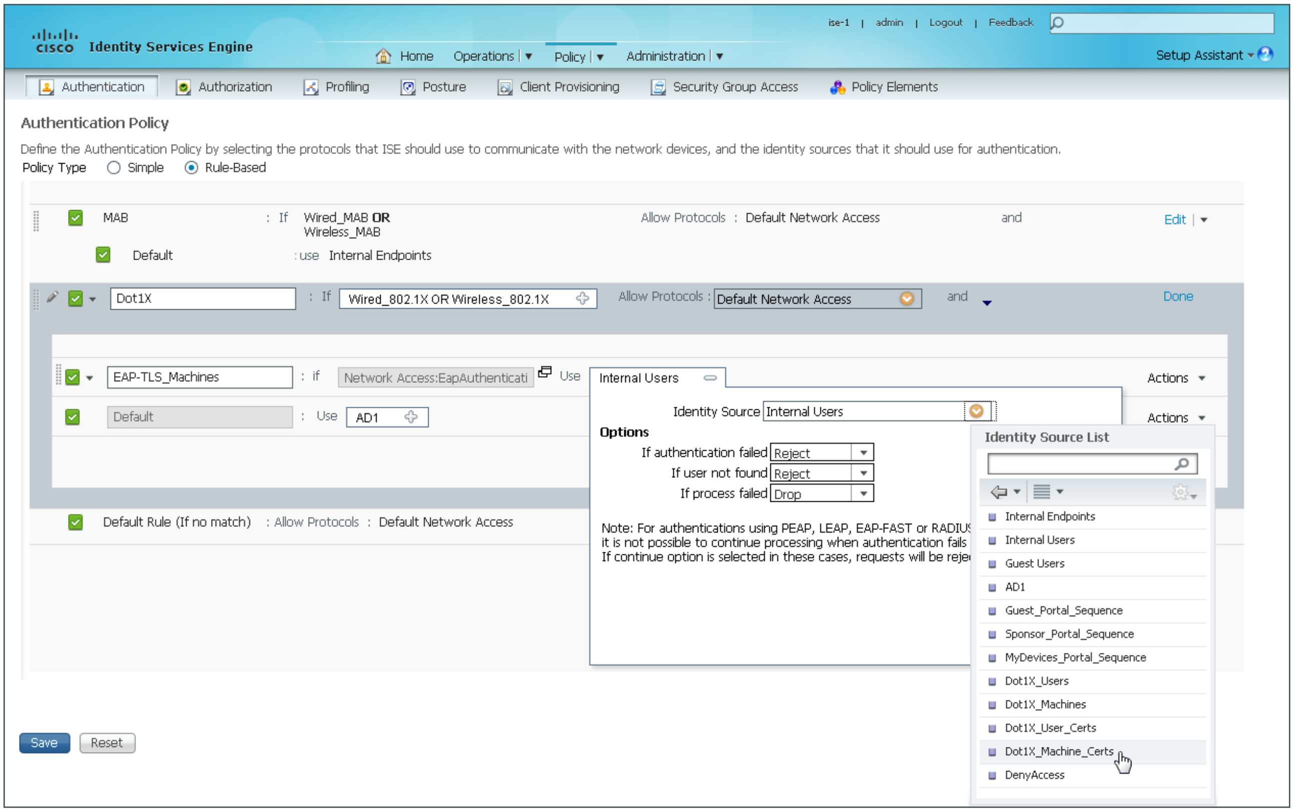
Dot1X : If Wired_802.1X OR Wireless_802.1X Allow Protocols : Default Network Access and

EAP-TLS_Machines : if Network Access:EapAuthenticati Use Internal Users

Default : Use AD1

Step 14: In the **Identity Source** list, choose the identity source sequence for machine authentication that you created in Procedure 2, "Create machine authentication policies."

Step 15: Use the default options for this identity source, and then click anywhere in the window to continue.


cisco Identity Services Engine
ise-1 | admin | Logout | Feedback
Home Operations Policy Administration
Setup Assistant
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Edit
Done
Actions
Actions
Save Reset
Identity Source List
Internal Endpoints
Internal Users
Guest Users
AD1
Guest_Portal_Sequence
Sponsor_Portal_Sequence
MyDevices_Portal_Sequence
Dot1X_Users
Dot1X_Machines
Dot1X_User_Certs
Dot1X_Machine_Certs
DenyAccess

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type ○ Simple ● Rule-Based

☑ MAB : If Wired_MAB **OR** Wireless_MAB Allow Protocols : Default Network Access and

☑ Default :use Internal Endpoints

☑ Dot1X : If Wired_802.1X OR Wireless_802.1X Allow Protocols : Default Network Access and

☑ EAP-TLS_Machines : if Network Access:EapAuthenticati Use Internal Users

☑ Default : Use AD1

☑ Default Rule (If no match) : Allow Protocols : Default Network Access

Identity Source Internal Users

Options

If authentication failed Reject

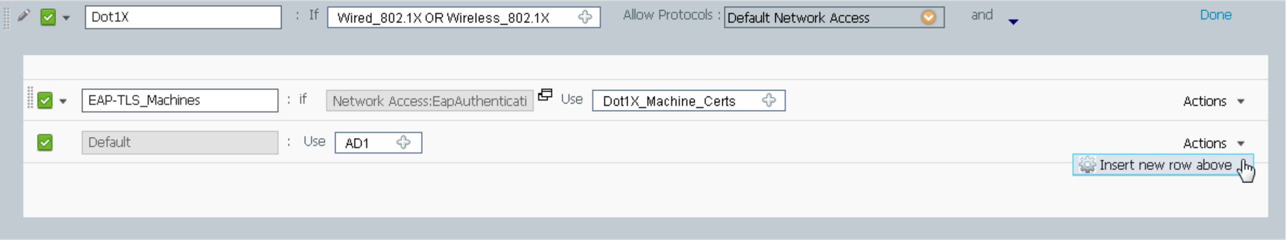
If user not found Reject

If process failed Drop

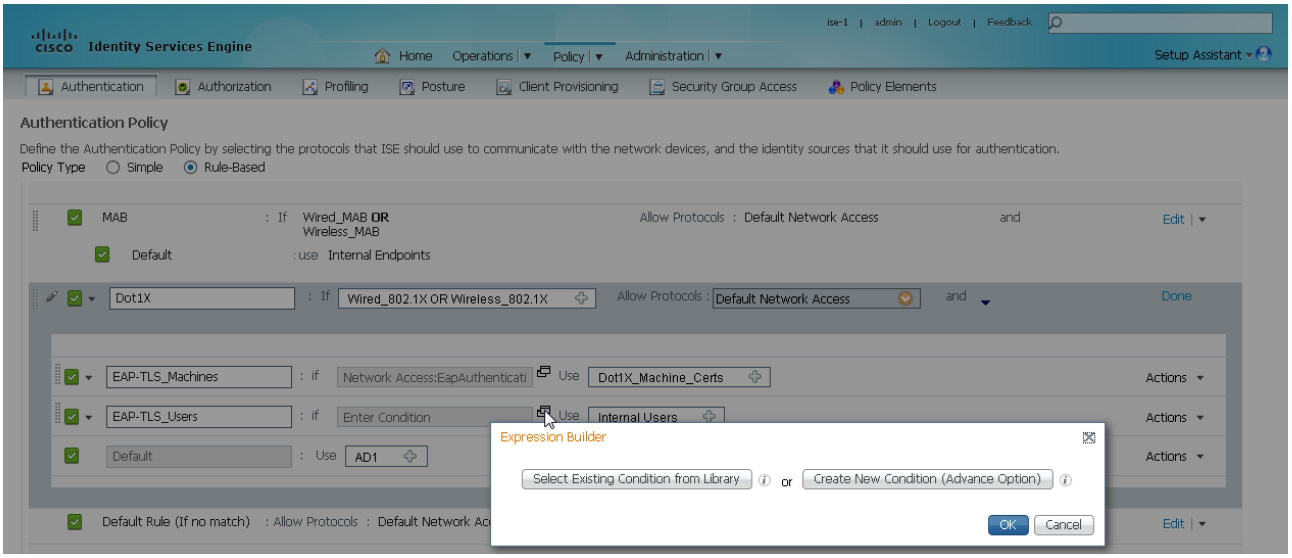
Note: For authentications using PEAP, LEAP, EAP-FAST or RADIU
it is not possible to continue processing when authentication fails
If continue option is selected in these cases, requests will be reje

You also create an additional row within the rule for user authentication.

Step 16: Next to the Default row showing the identity store, click the **Actions** list, and then choose **Insert new row above**.



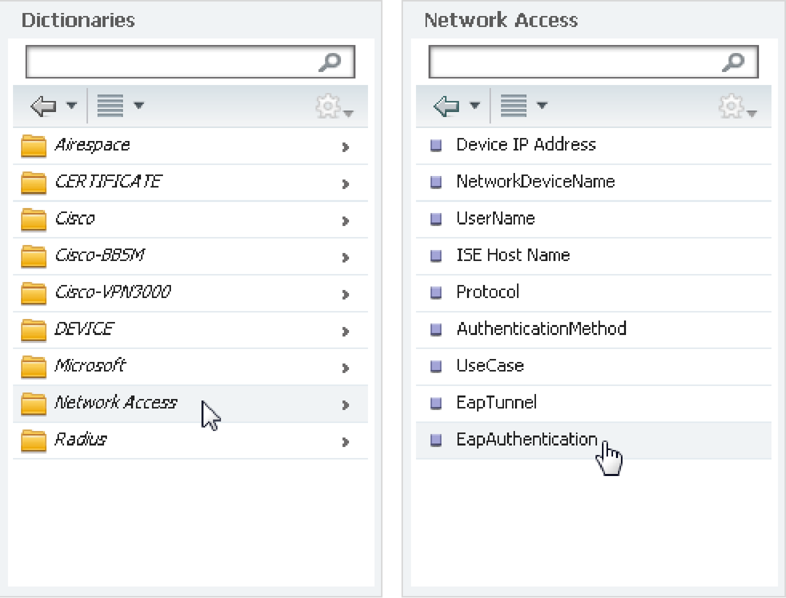
Step 17: Give the rule a name, and then next to the Enter Condition box, click the box symbol. The Expression Builder opens.


cisco Identity Services Engine
ise-1 | admin | Logout | Feedback
Home
Operations
Policy
Administration
Setup Assistant
Authentication
Authorization
Profiling
Posture
Client Provisioning
Security Group Access
Policy Elements
Authentication Policy
Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.
Policy Type ○ Simple ● Rule-Based
MAB : If Wired_MAB OR Wireless_MAB
Allow Protocols : Default Network Access
and
Edit
Default : use Internal Endpoints
Dot1X : If Wired_802.1X OR Wireless_802.1X
Allow Protocols : Default Network Access
and
Done
EAP-TLS_Machines : if Network Access:EapAuthenticati
Use Dot1X_Machine_Certs
Actions
EAP-TLS_Users : if Enter Condition
Use Internal Users
Actions
Default : Use AD1
Actions
Default Rule (If no match) : Allow Protocols : Default Network Ac
Edit
Expression Builder
Select Existing Condition from Library
or
Create New Condition (Advance Option)
OK
Cancel

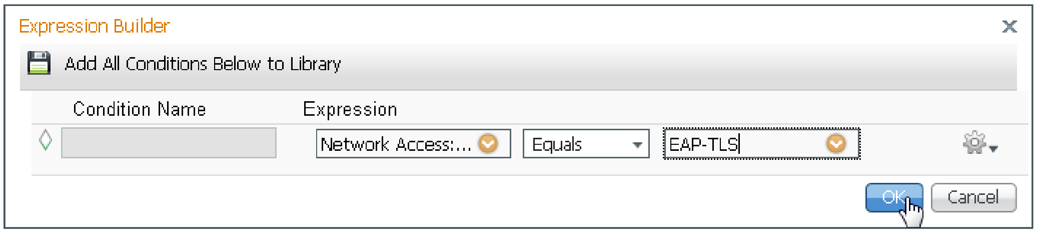
Step 18: Click **Create New Condition (Advance Option)**.

Step 19: In the **Expression** list, next to Select Attribute, click the arrow**.**

Step 20: Select **Network Access**, and then select **EapAuthentication**.

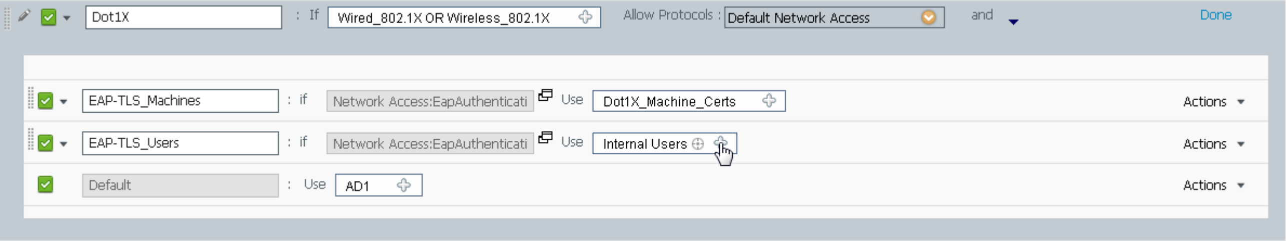


Step 21: In the second list, choose **Equals,** and in the last list, choose **EAP-TLS**, and then click **OK**.



Network Access:... | Equals | EAP-TLS

Step 22: On the new row you are creating for the rule, next to Internal Users, click the **+** symbol.



Dot1X : If Wired_802.1X OR Wireless_802.1X Allow Protocols : Default Network Access and

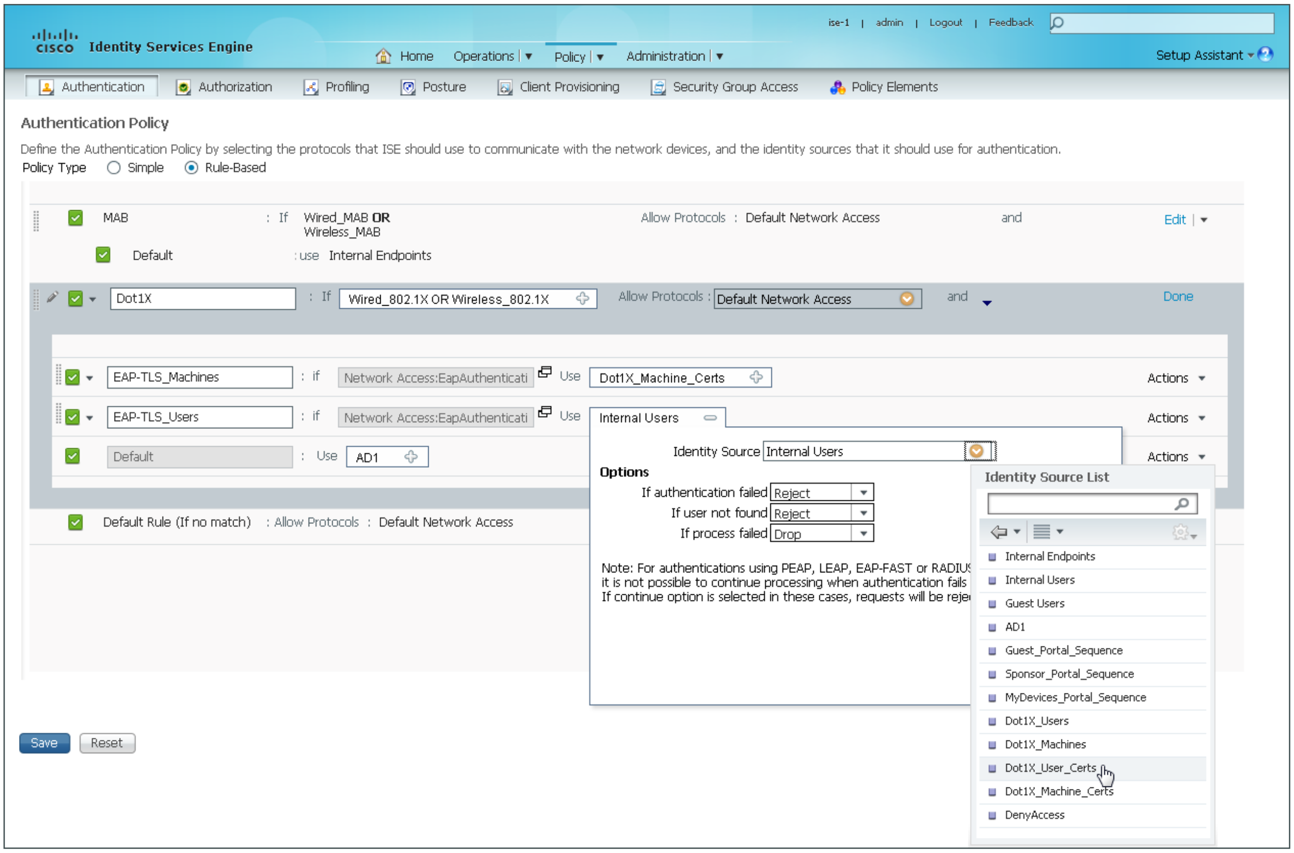
EAP-TLS_Machines : if Network Access:EapAuthenticati Use Dot1X_Machine_Certs

EAP-TLS_Users : if Network Access:EapAuthenticati Use Internal Users

Default : Use AD1

Step 23: In the **Identity Source** list, choose the identity source sequence for machine authentication that you created in Procedure 1, “Create user authentication policies.”

Step 24: Use the default options for this identity source, and then click anywhere in the window to continue.



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type ○ Simple ● Rule-Based

☑ MAB : If Wired_MAB **OR** Wireless_MAB Allow Protocols : Default Network Access and

☑ Default : use Internal Endpoints

☑ Dot1X : If Wired_802.1X OR Wireless_802.1X Allow Protocols : Default Network Access and

☑ EAP-TLS_Machines : if Network Access:EapAuthenticati Use Dot1X_Machine_Certs

☑ EAP-TLS_Users : if Network Access:EapAuthenticati Use Internal Users

☑ Default : Use AD1

☑ Default Rule (If no match) : Allow Protocols : Default Network Access

Identity Source Internal Users

Options

If authentication failed Reject

If user not found Reject

If process failed Drop

Note: For authentications using PEAP, LEAP, EAP-FAST or RADIU
it is not possible to continue processing when authentication fails
If continue option is selected in these cases, requests will be reje

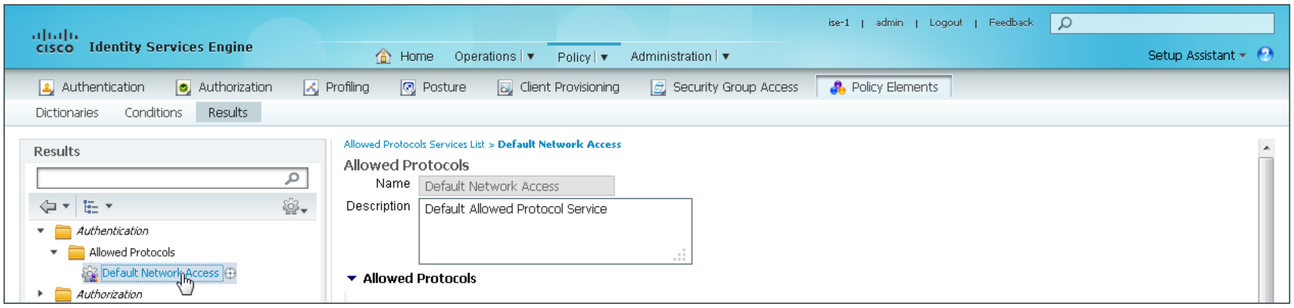
Step 25: Click **Save**. The authentication policy is now modified to use certificates.

Procedure 4 Enable EAP-TLS

In a previous section, you disabled EAP-TLS. Now that you have configured the policy to use digital certificates, you re-enable EAP-TLS for the authentication policy.

Step 1: Navigate to **Policy > Policy Elements > Results**.

Step 2: In the left pane, navigate to **Authentication** > **Allowed Protocols**, and then choose **Default Network Access**.



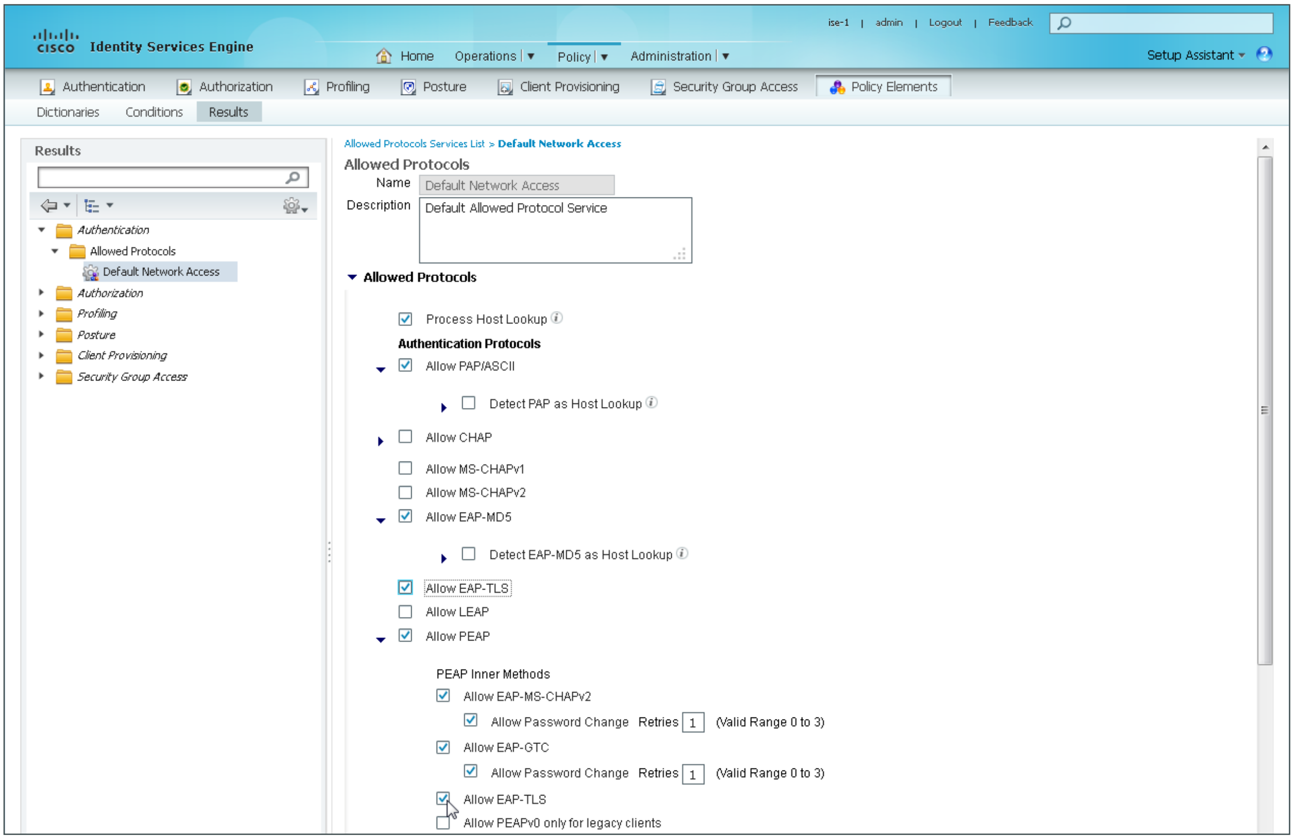
Allowed Protocols

Name Default Network Access

Description Default Allowed Protocol Service

Allowed Protocols

Step 3: In the main pane, under the Allowed Protocols > Authentication Protocols section, select **Allow EAP-TLS**.



Allowed Protocols

Name: Default Network Access

Description: Default Allowed Protocol Service

Allowed Protocols

☑ Process Host Lookup

Authentication Protocols

- ☑ Allow PAP/ASCII
  - ☐ Detect PAP as Host Lookup
- ☐ Allow CHAP
- ☐ Allow MS-CHAPv1
- ☐ Allow MS-CHAPv2
- ☑ Allow EAP-MD5
  - ☐ Detect EAP-MD5 as Host Lookup
- ☑ Allow EAP-TLS
- ☐ Allow LEAP
- ☑ Allow PEAP
  - PEAP Inner Methods
  - ☑ Allow EAP-MS-CHAPv2
    - ☑ Allow Password Change Retries 1 (Valid Range 0 to 3)
  - ☑ Allow EAP-GTC
    - ☑ Allow Password Change Retries 1 (Valid Range 0 to 3)
  - ☑ Allow EAP-TLS
  - ☐ Allow PEAPv0 only for legacy clients

Step 4: Under the Allowed Protocols> Authentication Protocols > Allow PEAP > PEAP Inner Methods section, select **Allow EAP-TLS**, leave the other default selections, and then at the bottom, click **Save**.

The service is updated to allow EAP-TLS.

PROCESS

Configuring Group Policy Objects

1. Create template for workstations
2. Create template for user auto-enrollment
3. Configure auto-enrollment for users
4. Configure auto-enrollment for domain computers
5. Configure GPOs for wired endpoints
6. Configure GPOs for wireless endpoints

In this deployment, you use group policy objects (GPOs) to distribute certificates and to configure the native 802.1X supplicant for Microsoft Windows endpoints that are members of the domain. Machine certificates are distributed when the machine joins the domain, and user certificates are deployed to the endpoint where the user logs in to the domain.

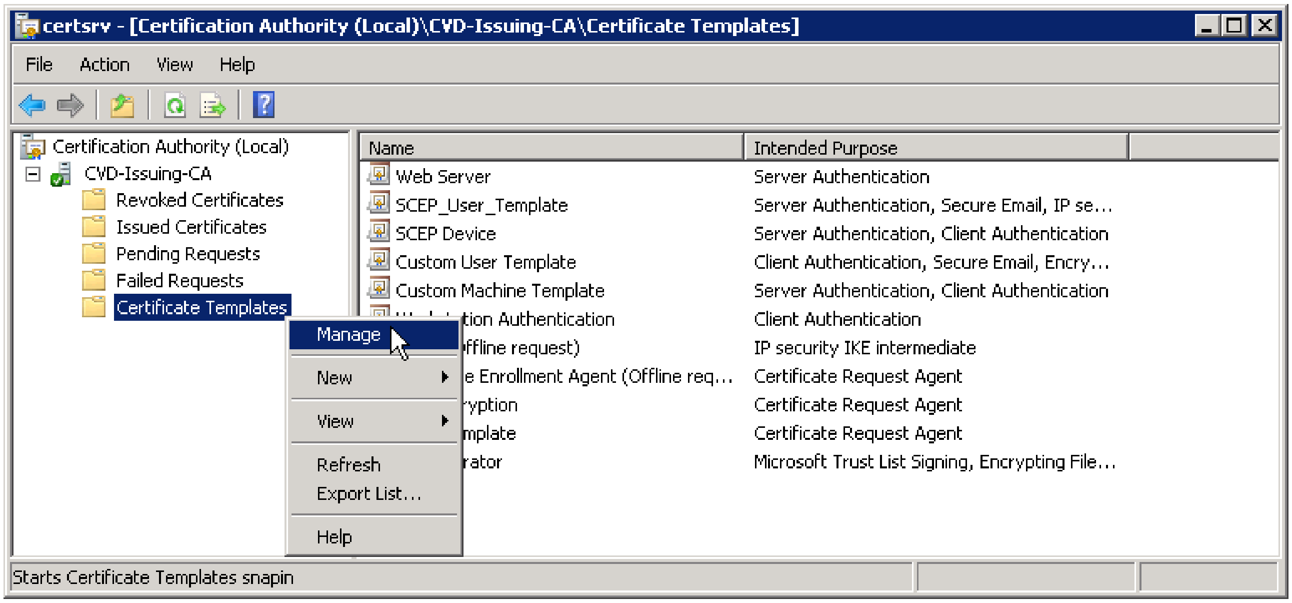
The steps in this example deployment describe how to edit the Default Domain Policy so that it applies to all users, but you could create a new policy object and apply it to a subset of users if you prefer. This configuration also assumes that the Default Domain Policy is applied to all Domain Computers, and therefore the computers are included for distribution of GPOs. If you create your own policy, then you need to apply the policy to distribute appropriately.

Procedure 1 Create template for workstations

You need to create a certificate template on the CA to be used to distribute machine certificates to workstations that join the Active Directory (AD) domain.

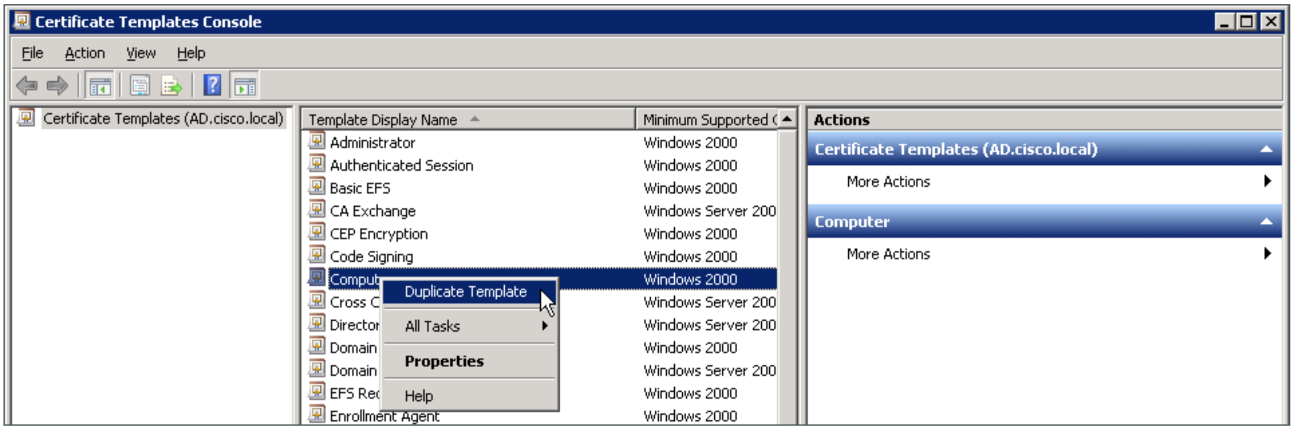
Step 1: Using a remote desktop connection, connect to the Microsoft CA console, navigate to **Start > Administrative Tools > Certification Authority**.

Step 2: In the left pane, expand the tree for the CA server, right-click **Certificate Templates**, and then choose **Manage**. The Certificate Templates Console opens.



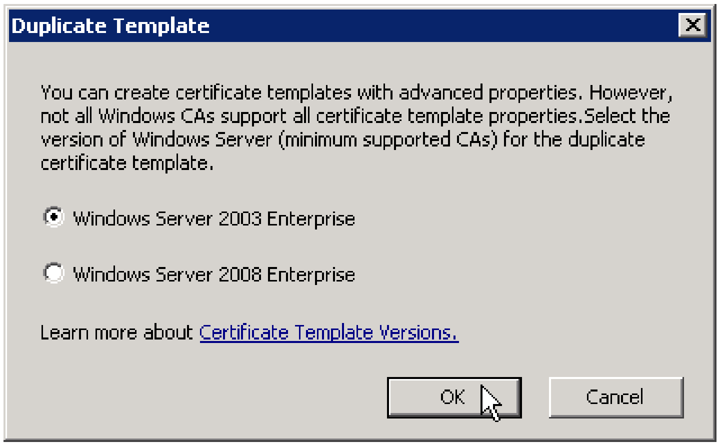
Name	Intended Purpose
Web Server	Server Authentication
SCEP_User_Template	Server Authentication, Secure Email, IP se...
SCEP Device	Server Authentication, Client Authentication
Custom User Template	Client Authentication, Secure Email, Encry...
Custom Machine Template	Server Authentication, Client Authentication
tion Authentication	Client Authentication
ffline request)	IP security IKE intermediate
e Enrollment Agent (Offline req...	Certificate Request Agent
yption	Certificate Request Agent
mplate	Certificate Request Agent
rator	Microsoft Trust List Signing, Encrypting File...

Step 3: Right-click the Computer template, and then choose **Duplicate Template**. The Duplicate Template window appears.


Certificate Templates Console
File
Action
View
Help
Certificate Templates (AD.cisco.local)
Duplicate Template
All Tasks
Properties
Help
Actions
Certificate Templates (AD.cisco.local)
More Actions
Computer
More Actions

Template Display Name	Minimum Supported (
Administrator	Windows 2000
Authenticated Session	Windows 2000
Basic EFS	Windows 2000
CA Exchange	Windows Server 200
CEP Encryption	Windows 2000
Code Signing	Windows 2000
Comput	Windows 2000
Cross C	Windows Server 200
Director	Windows Server 200
Domain	Windows 2000
Domain	Windows Server 200
EFS Rec	Windows 2000
Enrollment Agent	Windows 2000

Step 4: For compatibility, leave the default **Windows 2003 Server Enterprise** selection, and then click **OK**.



You can create certificate templates with advanced properties. However, not all Windows CAs support all certificate template properties.Select the version of Windows Server (minimum supported CAs) for the duplicate certificate template.

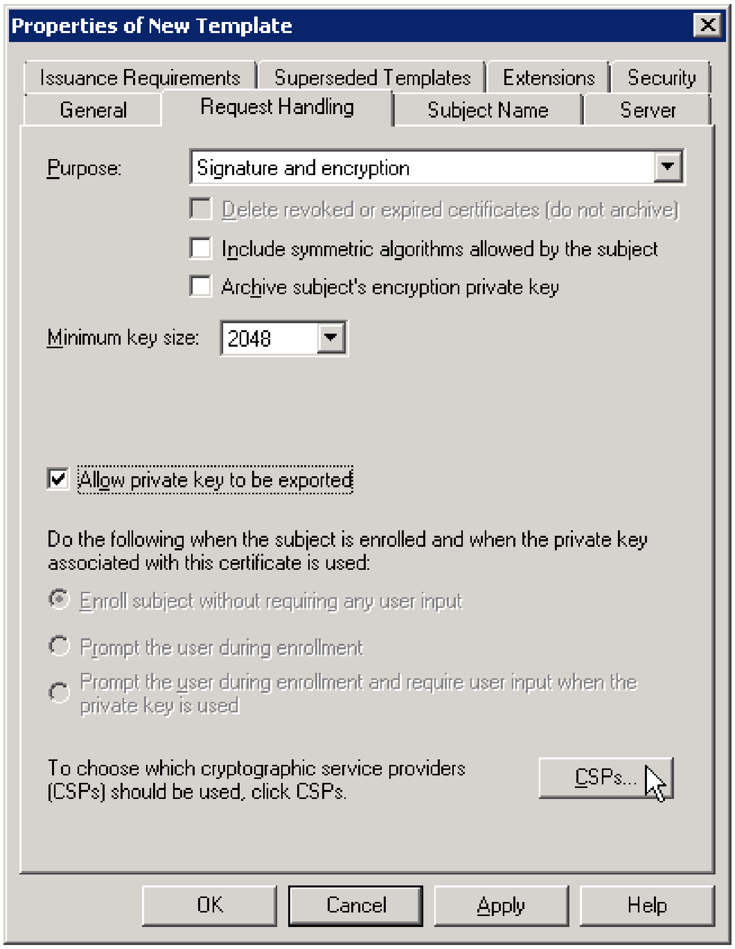
● Windows Server 2003 Enterprise

○ Windows Server 2008 Enterprise

Learn more about Certificate Template Versions.

Step 5: In the Properties of New Template window, click the **General** tab, and then give the new template a **Template display name**. (Example: Custom Machine Template) A similar **Template name** is automatically created.

Step 6: On the Request Handling tab, select **Allow private key to be exported**, and then click **CSPs**.



Properties of New Template

Purpose: Signature and encryption

☐ Delete revoked or expired certificates (do not archive)

☐ Include symmetric algorithms allowed by the subject

☐ Archive subject's encryption private key

Minimum key size: 2048

☑ Allow private key to be exported

Do the following when the subject is enrolled and when the private key associated with this certificate is used:

● Enroll subject without requiring any user input

○ Prompt the user during enrollment

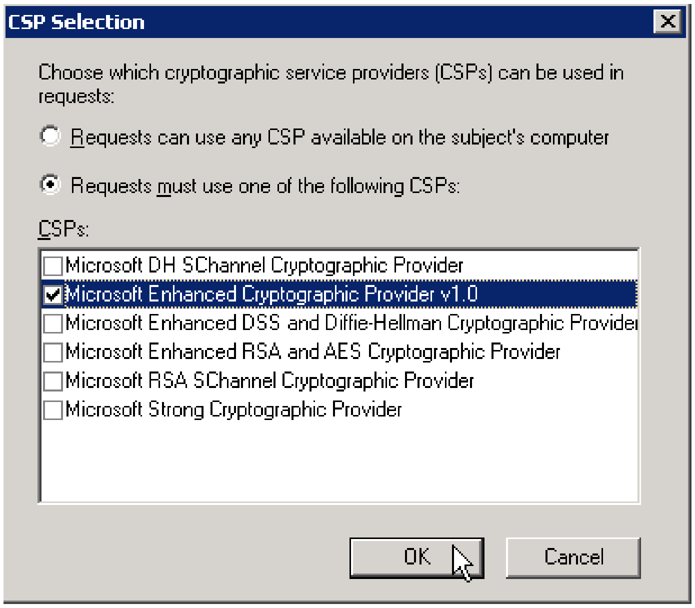
○ Prompt the user during enrollment and require user input when the private key is used

To choose which cryptographic service providers (CSPs) should be used, click CSPs.

Step 7: Select **Requests must use one of the following CSPs.**

Step 8: Select **Microsoft Enhanced Cryptographic Provider v1.0.**

Step 9: Clear all other selections, and then click **OK**.



CSP Selection

Choose which cryptographic service providers (CSPs) can be used in requests:

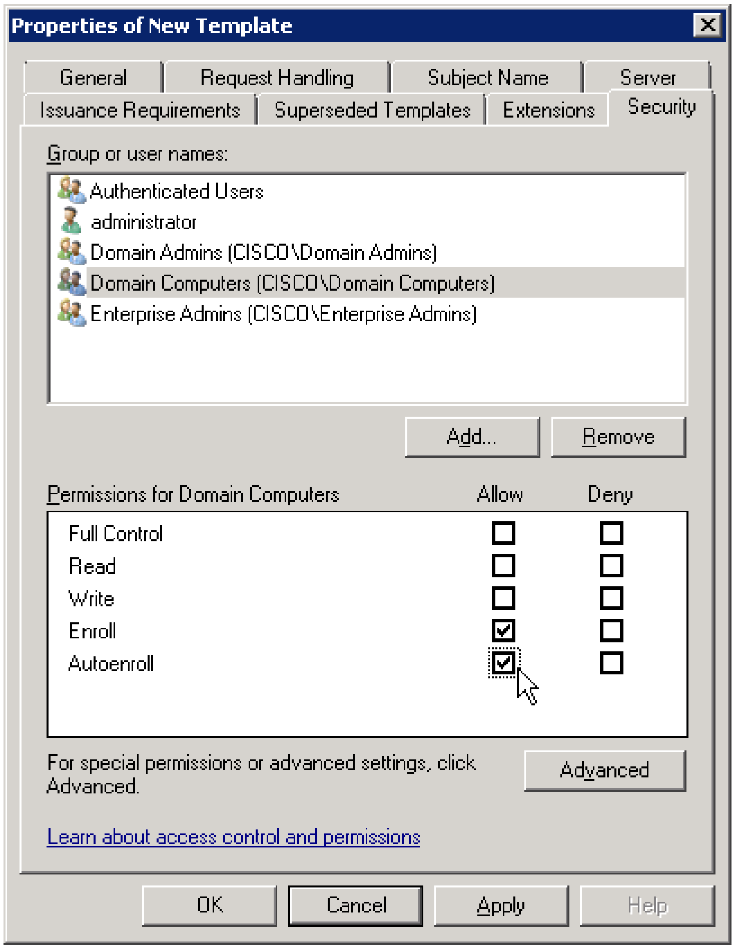
○ Requests can use any CSP available on the subject's computer

● Requests must use one of the following CSPs:

CSPs:

☐ Microsoft DH SChannel Cryptographic Provider
☑ Microsoft Enhanced Cryptographic Provider v1.0
☐ Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Provider
☐ Microsoft Enhanced RSA and AES Cryptographic Provider
☐ Microsoft RSA SChannel Cryptographic Provider
☐ Microsoft Strong Cryptographic Provider

Step 10: On the Security tab, click **Domain Computers**.



Properties of New Template

Group or user names:

- Authenticated Users
- administrator
- Domain Admins (CISCO\Domain Admins)
- Domain Computers (CISCO\Domain Computers)
- Enterprise Admins (CISCO\Enterprise Admins)

Permissions for Domain Computers	Allow	Deny
Full Control	☐	☐
Read	☐	☐
Write	☐	☐
Enroll	☑	☐
Autoenroll	☑	☐

For special permissions or advanced settings, click Advanced.

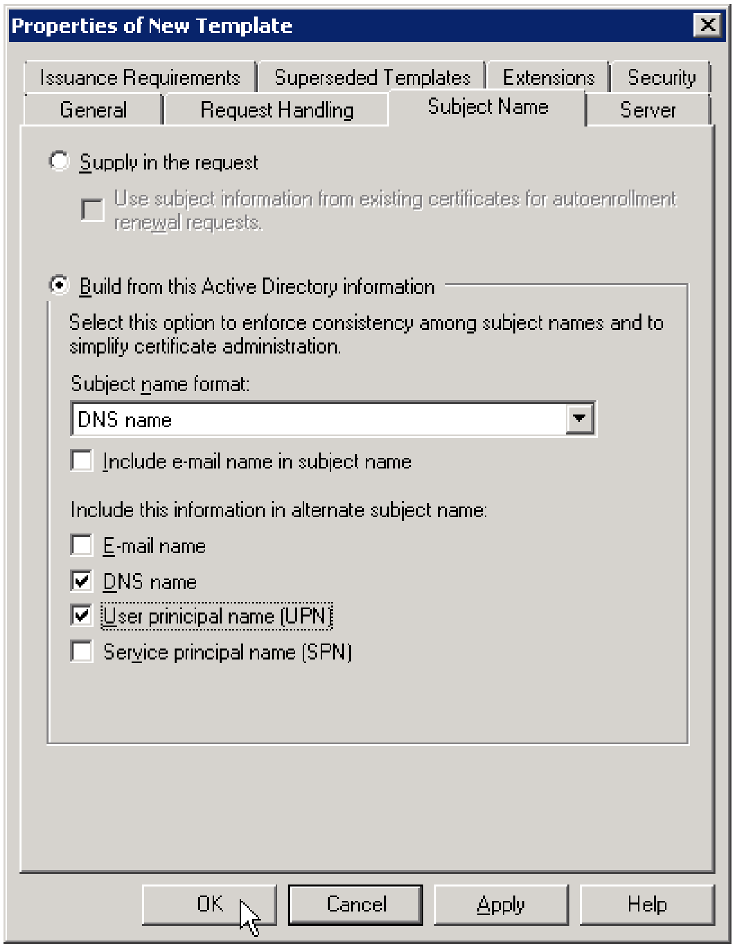
Learn about access control and permissions

Step 11: For both **Enroll** and **Autoenroll**, select **Allow**.

Step 12: On the Subject Name tab, configure the following values:

- Build from this Active Directory information—**Selected**
- Subject name format—**DNS name**
- DNS name—**Selected**
- User Principal name (UPN)—**Selected**

Leave the defaults for the remaining tabs, and then click **OK**



○ Supply in the request

☐ Use subject information from existing certificates for autoenrollment renewal requests.

● Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

DNS name

☐ Include e-mail name in subject name

Include this information in alternate subject name:

☐ E-mail name

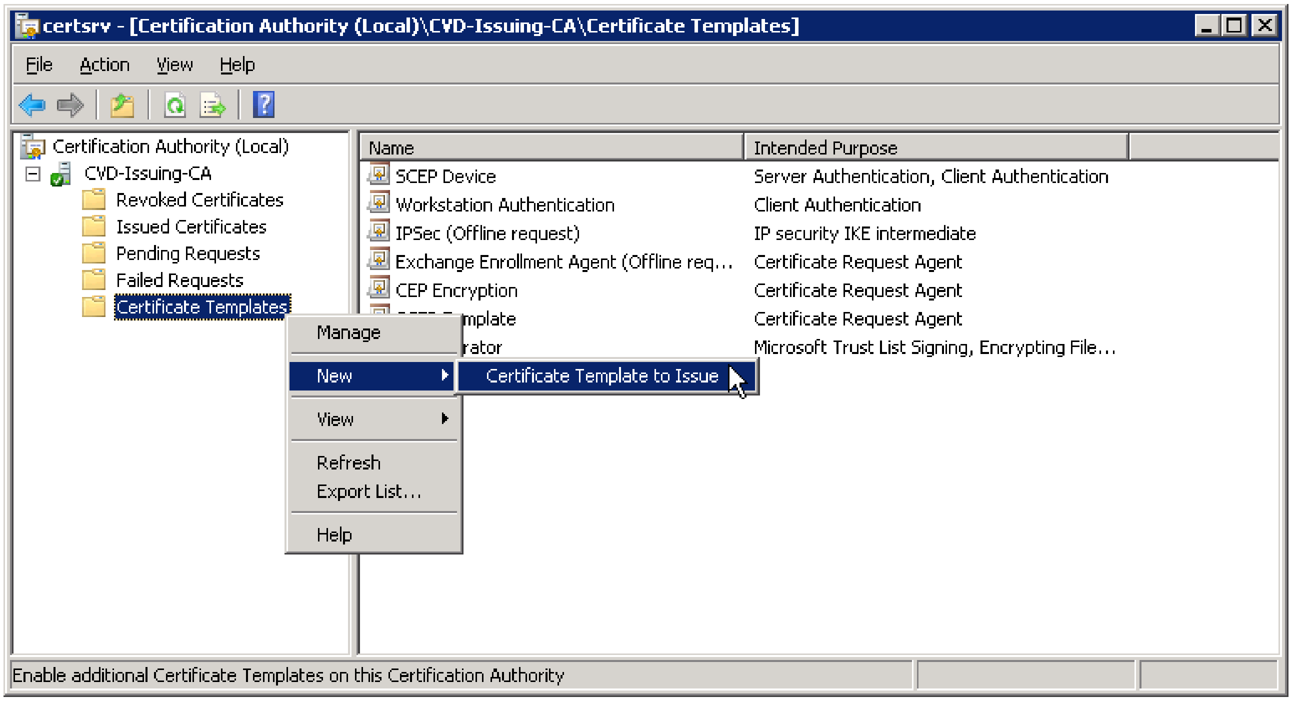
☑ DNS name

☑ User principal name (UPN)

☐ Service principal name (SPN)

Step 13: Close the Certificate Templates Console.

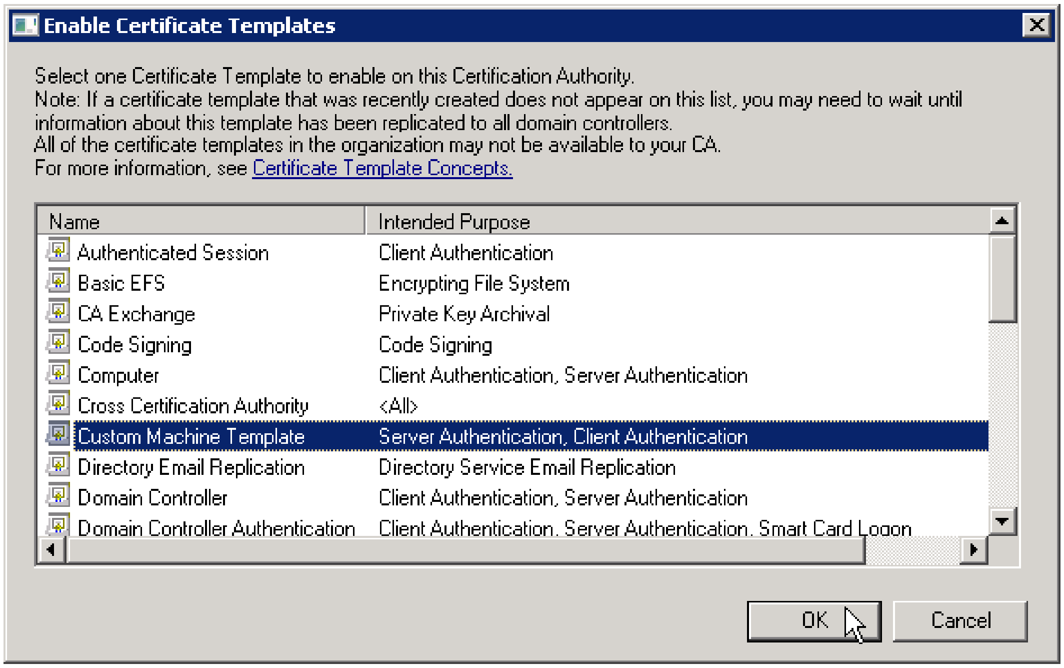
Step 14: In the Certificate Authority console, right-click **Certificate Templates**, and then choose **New > Certificate Template to Issue**.



Name	Intended Purpose
SCEP Device	Server Authentication, Client Authentication
Workstation Authentication	Client Authentication
IPSec (Offline request)	IP security IKE intermediate
Exchange Enrollment Agent (Offline req...	Certificate Request Agent
CEP Encryption	Certificate Request Agent
mplate	Certificate Request Agent
rator	Microsoft Trust List Signing, Encrypting File...

Enable additional Certificate Templates on this Certification Authority

Step 15: Choose the previously defined template, and then click **OK**.



Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to your CA.
For more information, see Certificate Template Concepts.

Name	Intended Purpose
Authenticated Session	Client Authentication
Basic EFS	Encrypting File System
CA Exchange	Private Key Archival
Code Signing	Code Signing
Computer	Client Authentication, Server Authentication
Cross Certification Authority	<All>
Custom Machine Template	Server Authentication, Client Authentication
Directory Email Replication	Directory Service Email Replication
Domain Controller	Client Authentication, Server Authentication
Domain Controller Authentication	Client Authentication, Server Authentication, Smart Card Logon

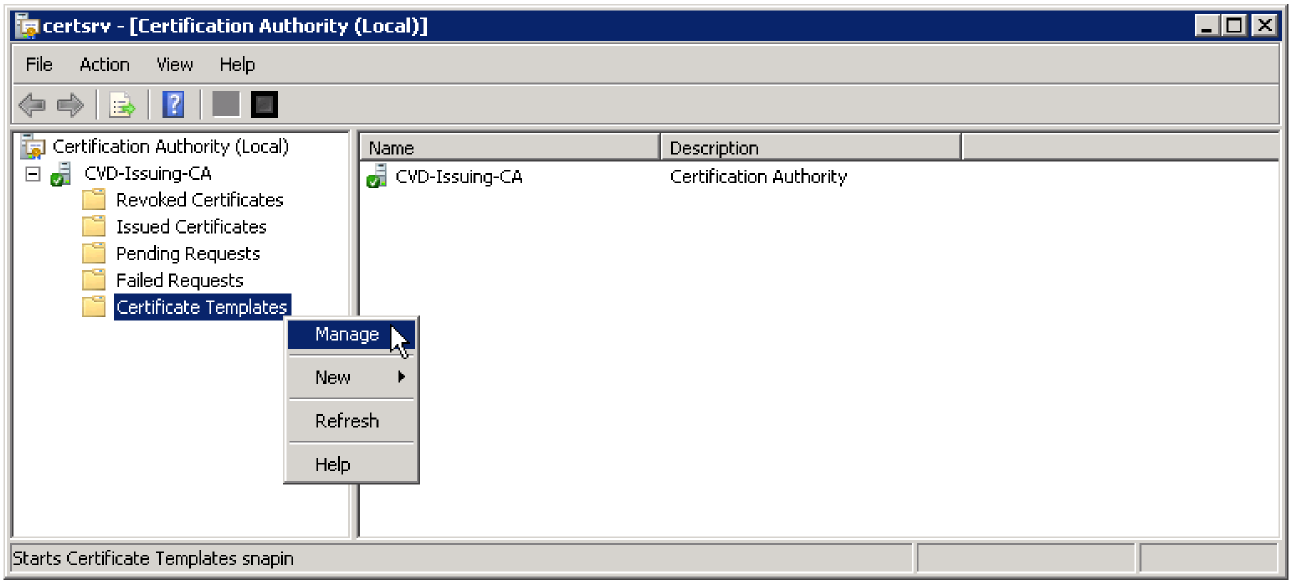
When machines join the domain or when the GPO policy is refreshed (the default period is 90 minutes), the machine receives a machine certificate to allow for 802.1X machine authentication.

Procedure 2 Create template for user auto-enrollment

This deployment uses group policy objects (GPOs) to have domain users auto-enroll to obtain a certificate when they log in to the domain. To enable auto-enrollment, you need to create a certificate template for these users.

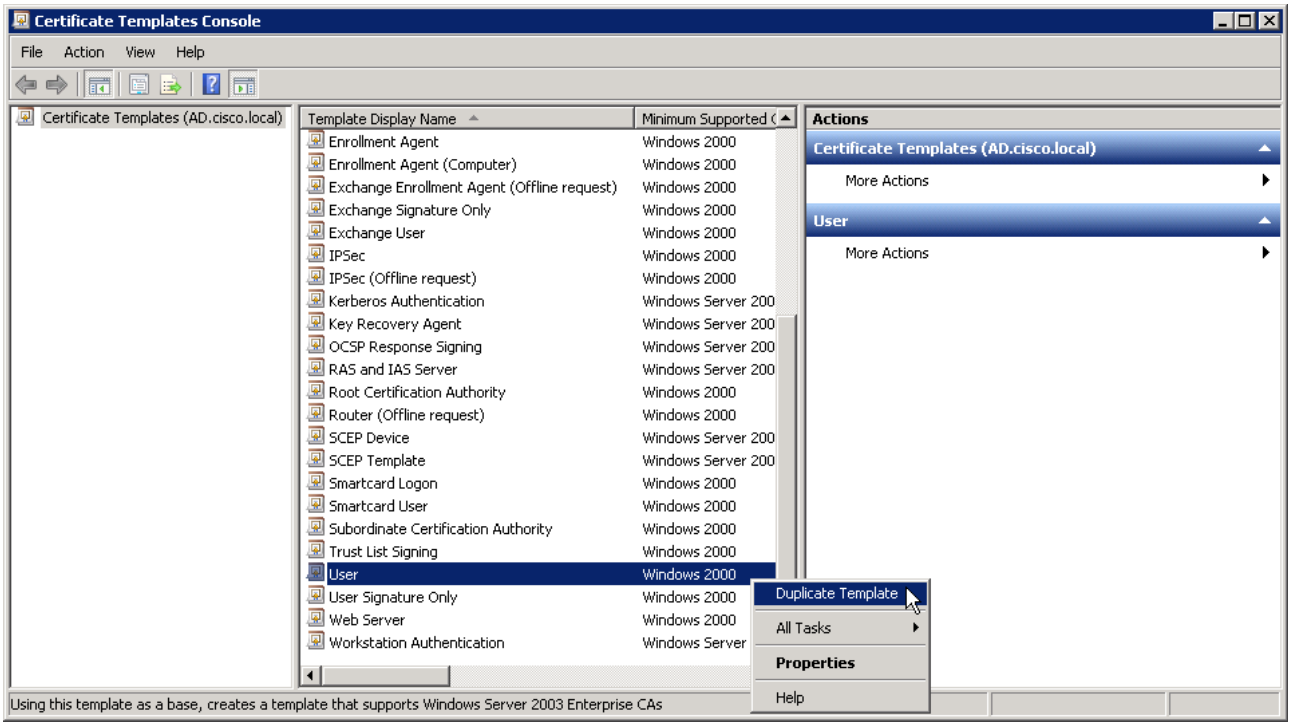
Step 1: On the CA console, navigate to **Start > Administrative Tools > Certification Authority**.

Step 2: In the left pane, expand the tree for the CA server, right-click **Certificate Templates**, and then choose **Manage**. The Certificate Templates Console opens.



Starts Certificate Templates snapin

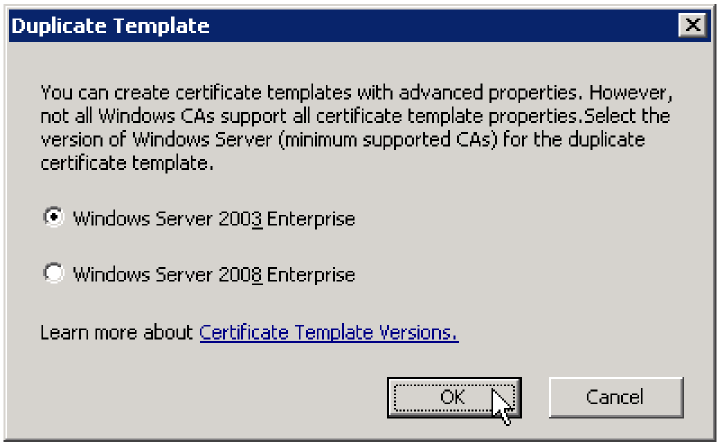
Step 3: Near the bottom of the template names, right-click the User template, and then choose **Duplicate Template**.


Certificate Templates Console
File
Action
View
Help
Certificate Templates (AD.cisco.local)
Actions
Certificate Templates (AD.cisco.local)
More Actions
User
More Actions
Duplicate Template
All Tasks
Properties
Help

Template Display Name	Minimum Supported (
Enrollment Agent	Windows 2000
Enrollment Agent (Computer)	Windows 2000
Exchange Enrollment Agent (Offline request)	Windows 2000
Exchange Signature Only	Windows 2000
Exchange User	Windows 2000
IPSec	Windows 2000
IPSec (Offline request)	Windows 2000
Kerberos Authentication	Windows Server 200
Key Recovery Agent	Windows Server 200
OCSP Response Signing	Windows Server 200
RAS and IAS Server	Windows Server 200
Root Certification Authority	Windows 2000
Router (Offline request)	Windows 2000
SCEP Device	Windows Server 200
SCEP Template	Windows Server 200
Smartcard Logon	Windows 2000
Smartcard User	Windows 2000
Subordinate Certification Authority	Windows 2000
Trust List Signing	Windows 2000
User	Windows 2000
User Signature Only	Windows 2000
Web Server	Windows 2000
Workstation Authentication	Windows Server

Using this template as a base, creates a template that supports Windows Server 2003 Enterprise CAs

Step 4: For compatibility, leave the default **Windows 2003 Server Enterprise** selection, and click **OK**.



You can create certificate templates with advanced properties. However, not all Windows CAs support all certificate template properties.Select the version of Windows Server (minimum supported CAs) for the duplicate certificate template.

● Windows Server 2003 Enterprise

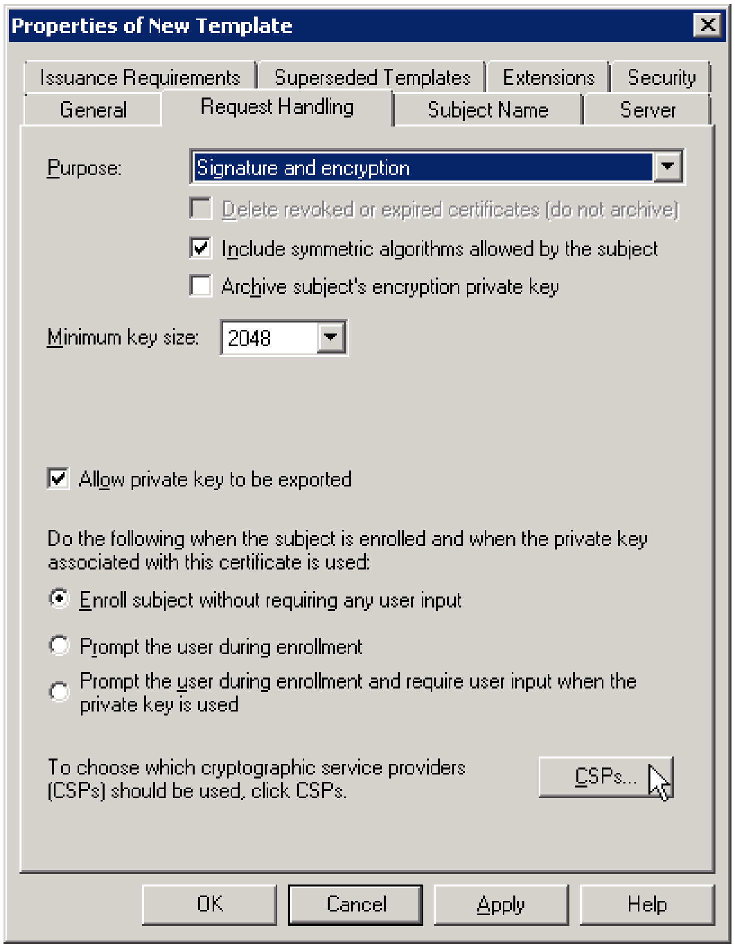
○ Windows Server 2008 Enterprise

Learn more about Certificate Template Versions.

Step 5: In the Properties of New Template window, click the **General** tab, and then give the new template a **Template display name**. (Example: Custom User Template) A similar **Template name** is automatically created.

Step 6: On the Request Handling tab, select **Allow private key to be exported.**

Step 7: Verify that **Enroll subject without requiring any user input** is selected, and then click **CSPs**.



Purpose: Signature and encryption

☐ Delete revoked or expired certificates (do not archive)

☑ Include symmetric algorithms allowed by the subject

☐ Archive subject's encryption private key

Minimum key size: 2048

☑ Allow private key to be exported

Do the following when the subject is enrolled and when the private key associated with this certificate is used:

● Enroll subject without requiring any user input

○ Prompt the user during enrollment

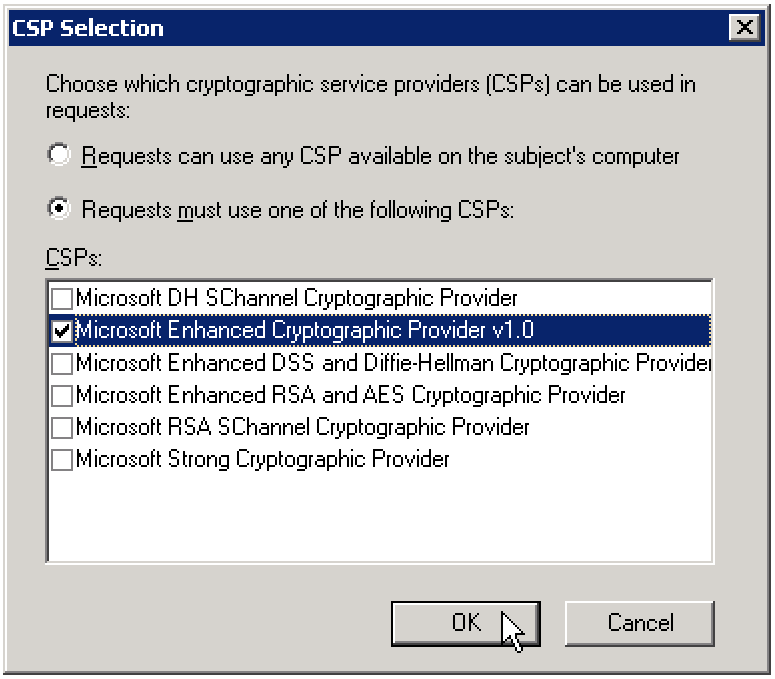
○ Prompt the user during enrollment and require user input when the private key is used

To choose which cryptographic service providers (CSPs) should be used, click CSPs.

Step 8: Select **Requests must use one of the following CSPs**.

Step 9: Select **Microsoft Enhanced Cryptographic Provider v1.0**.

Step 10: Clear all other selections, and then click **OK**.



Choose which cryptographic service providers (CSPs) can be used in requests:

○ Requests can use any CSP available on the subject's computer

● Requests must use one of the following CSPs:

CSPs:

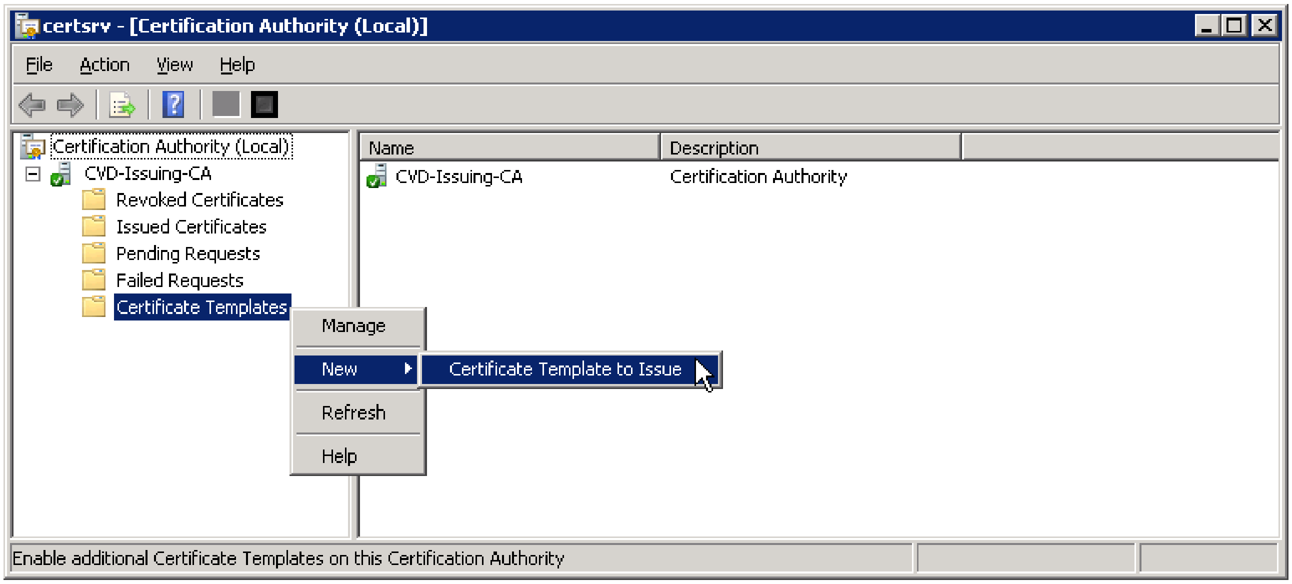
☐ Microsoft DH SChannel Cryptographic Provider
☑ Microsoft Enhanced Cryptographic Provider v1.0
☐ Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Provider
☐ Microsoft Enhanced RSA and AES Cryptographic Provider
☐ Microsoft RSA SChannel Cryptographic Provider
☐ Microsoft Strong Cryptographic Provider

Step 11: On the Security tab, click **Domain Users**.

Step 12: For **Read**, **Enroll,** and **Autoenroll**, select **Allow**. Leave the defaults for the remaining tabs, and then click **OK**.

Step 13: Close the Certificate Templates Console.

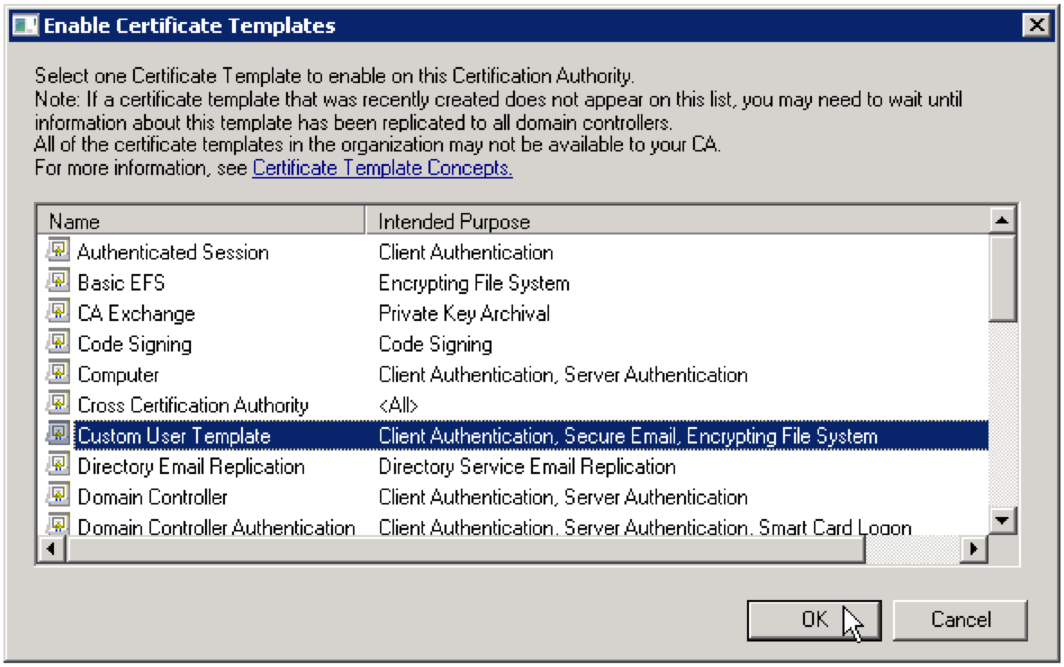
Step 14: In the Certificate Authority console, right-click **Certificate Templates**, and then choose **New > Certificate Template to Issue**.



Name	Description
CVD-Issuing-CA	Certification Authority

Enable additional Certificate Templates on this Certification Authority

Step 15: Choose the previously defined template, and then click **OK**.



Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to your CA.
For more information, see Certificate Template Concepts.

Name	Intended Purpose
Authenticated Session	Client Authentication
Basic EFS	Encrypting File System
CA Exchange	Private Key Archival
Code Signing	Code Signing
Computer	Client Authentication, Server Authentication
Cross Certification Authority	<All>
Custom User Template	Client Authentication, Secure Email, Encrypting File System
Directory Email Replication	Directory Service Email Replication
Domain Controller	Client Authentication, Server Authentication
Domain Controller Authentication	Client Authentication, Server Authentication, Smart Card Logon

Procedure 3 Configure auto-enrollment for users

Certificate auto-enrollment is not configured by default. You must enable this feature in AD to distribute user certificates to the authenticated user.

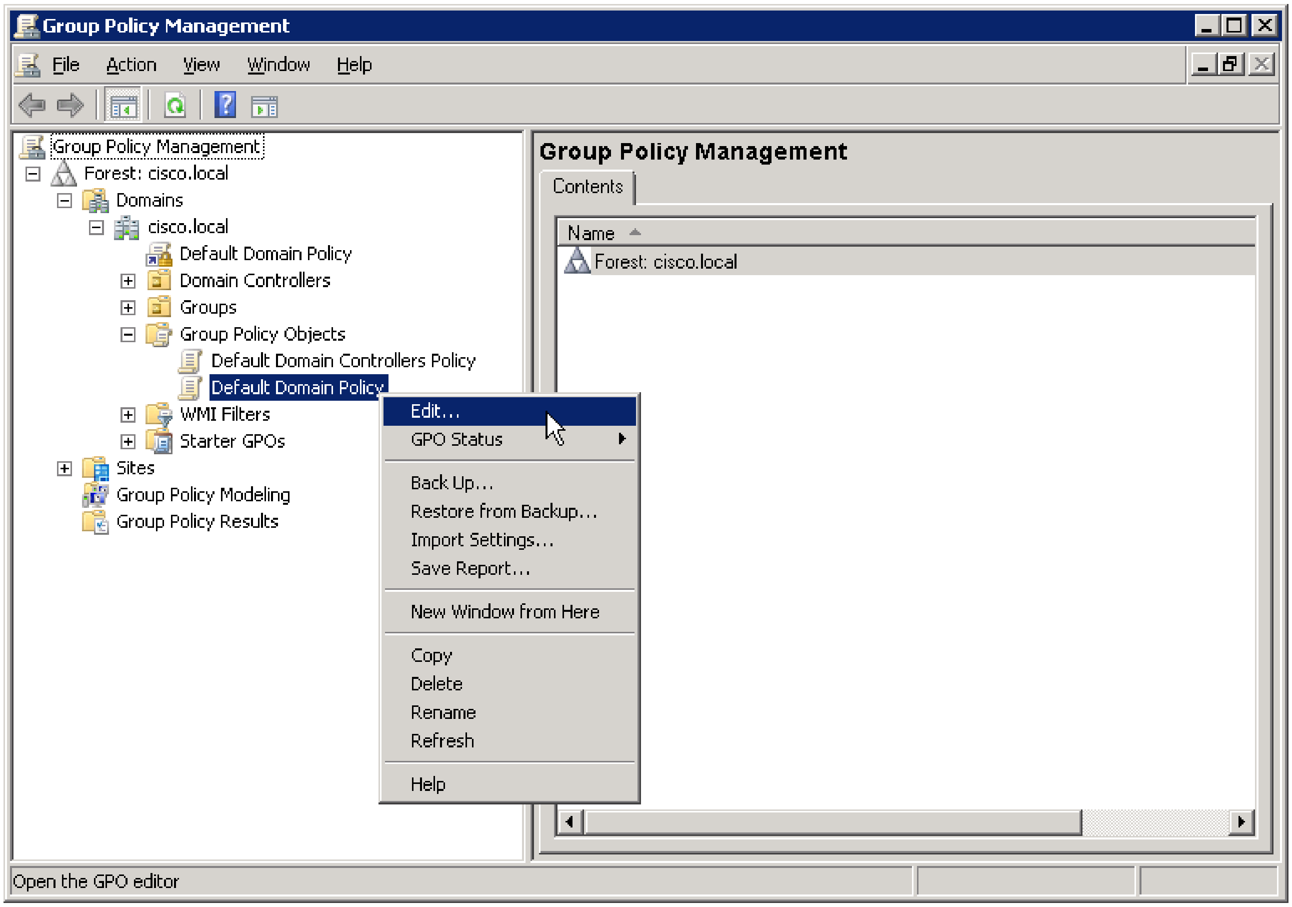
Step 1: On the AD console, navigate to **Start > Administrative Tools > Group Policy Management**.

Tech Tip

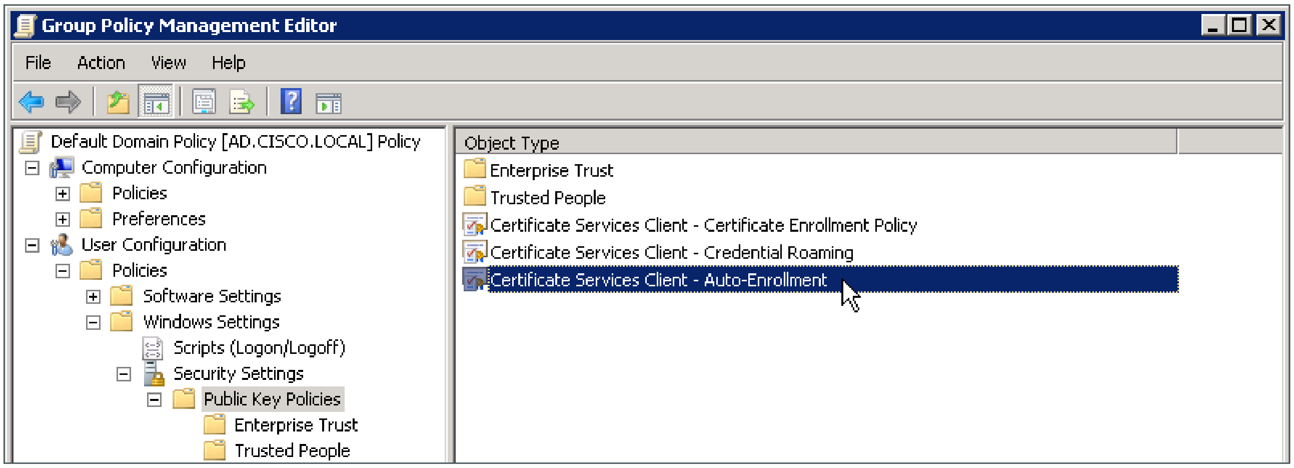
The Group Policy Management Console is not installed by default with the Windows Server installation. If it isn't available under Administrative Tools, see "Install the GPMC" at the following location:

http://technet.microsoft.com/en-us/library/cc725932.aspx

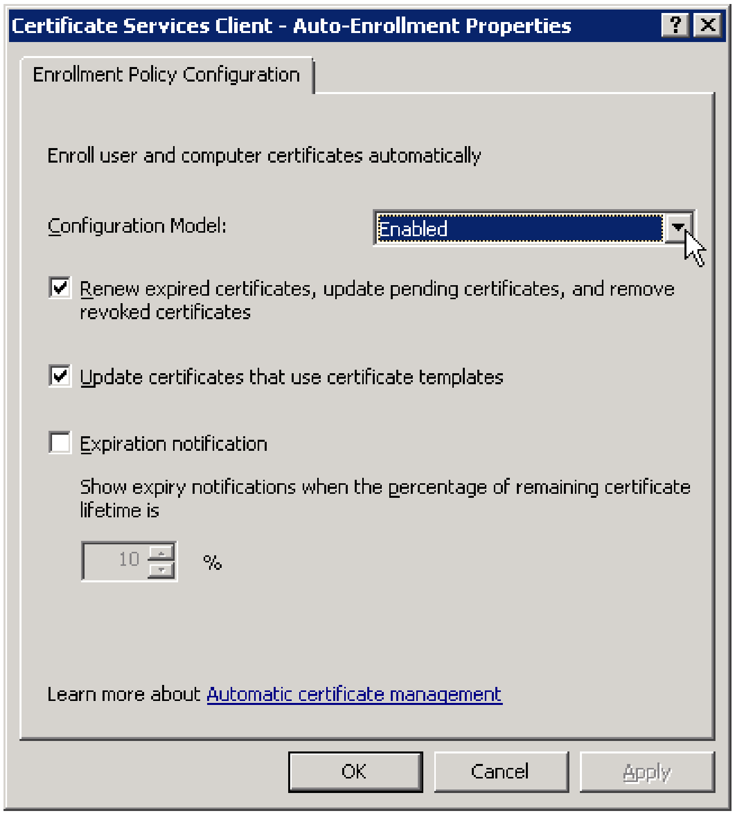
Step 2: In the left pane, expand **Forest: [local domain]** > **Domains** > **[local domain]** > **Group Policy Objects**, right-click **Default Domain Policy**, and then click **Edit**. The Group Policy Management Editor opens.



Step 3: In the Group Policy Management Editor, navigate to **User Configuration > Policies > Windows Settings > Security Settings**, click **Public Key Policies**, and then in the right panel double-click **Certificate Services Client - Auto-Enrollment**.



Step 4: In the Configuration Model list, choose **Enabled**, select the first two check boxes which start with **Renew** and **Update**, and then click **OK**.


Certificate Services Client - Auto-Enrollment Properties
Enrollment Policy Configuration
OK
Cancel
Apply

Enroll user and computer certificates automatically

Configuration Model: Enabled

☑ Renew expired certificates, update pending certificates, and remove revoked certificates

☑ Update certificates that use certificate templates

☐ Expiration notification

Show expiry notifications when the percentage of remaining certificate lifetime is 10 %

Learn more about Automatic certificate management

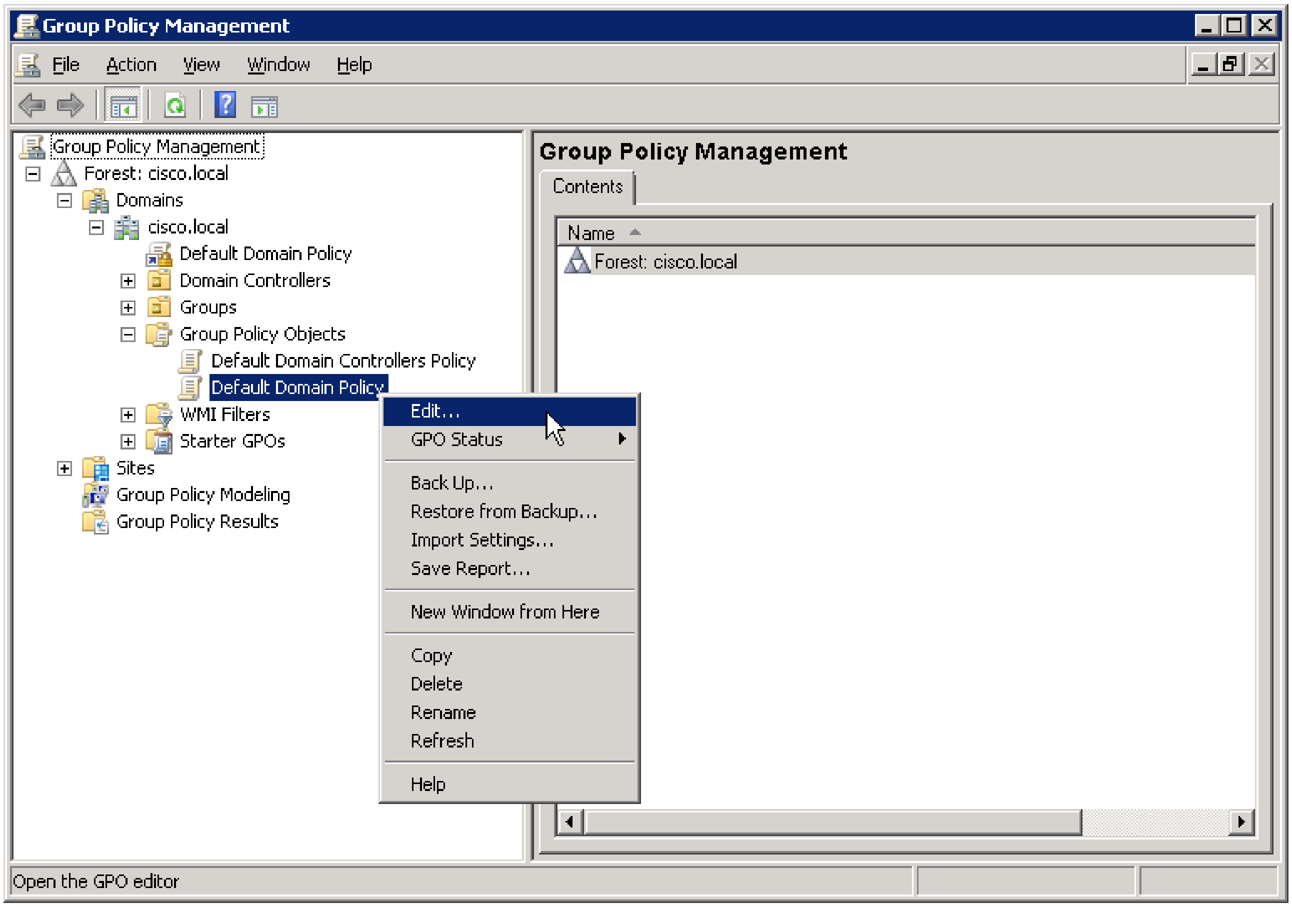
Users will have a certificate pushed to them the next time they log in to the domain or after the GPO policy is refreshed. If the user logs in to multiple endpoints, the certificate is deployed to each of them.

Procedure 4 Configure auto-enrollment for domain computers

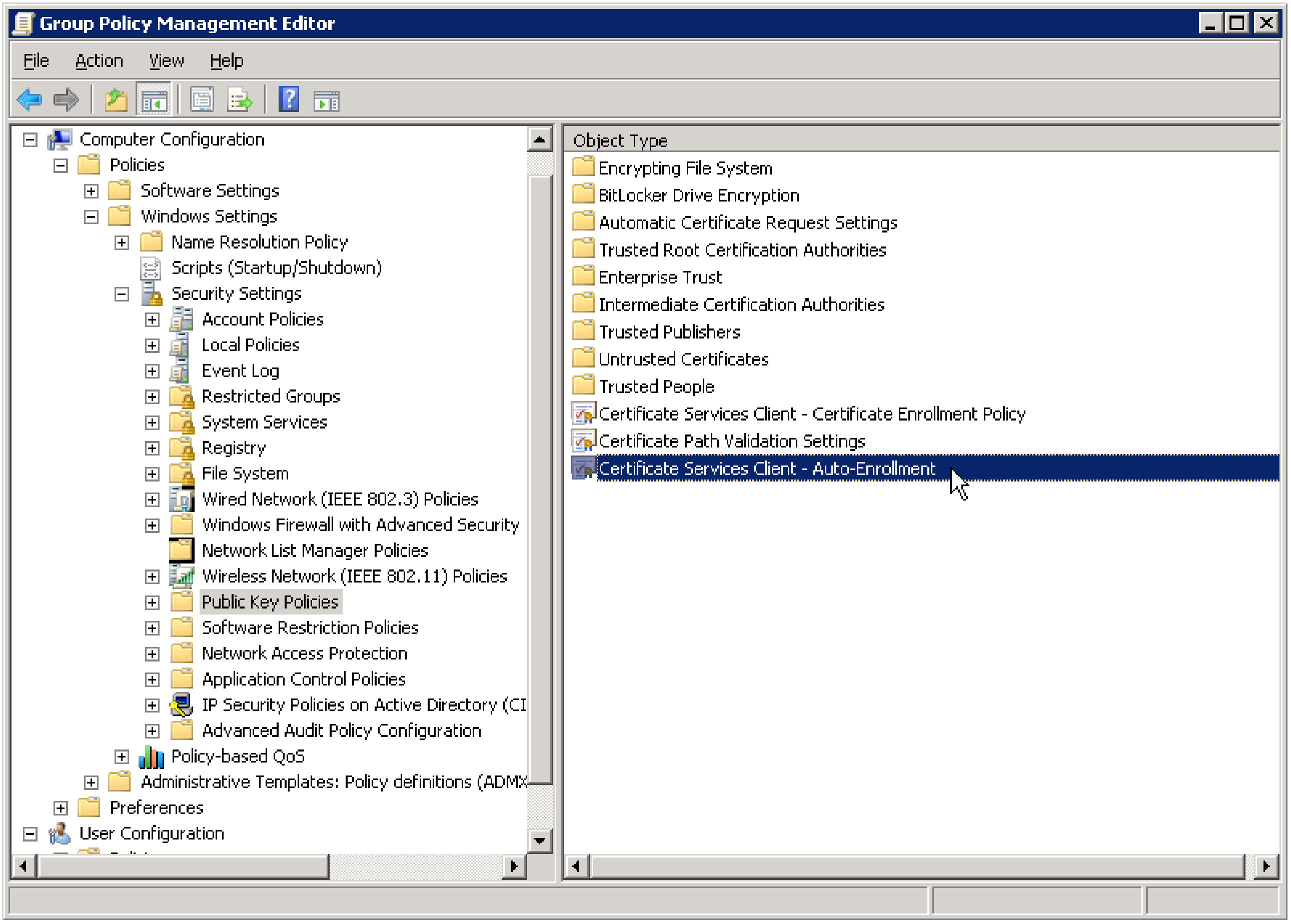
Certificate auto-enrollment is not configured by default. You must enable this feature in AD to distribute machine certificates to the computers in the domain.

Step 1: On the AD console, navigate to **Start > Administrative Tools > Group Policy Management**.

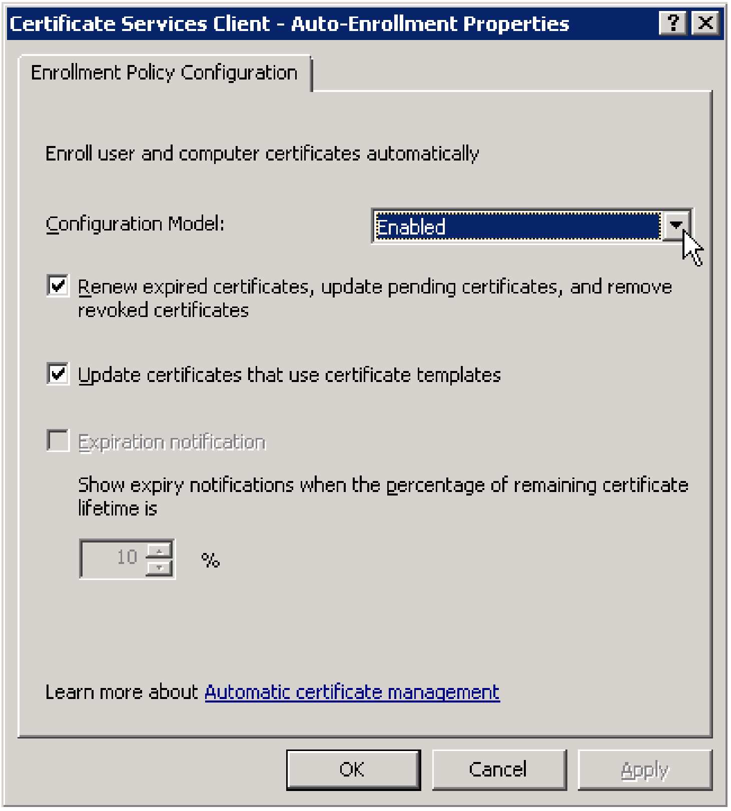
Step 2: In the left pane, expand **Forest: [local domain]** > **Domains** > **[local domain]** > **Group Policy Objects**, right-click **Default Domain Policy**, and then click **Edit**. The Group Policy Management Editor opens.



Step 3: In the Group Policy Management Editor, navigate to **Computer Configuration > Policies > Windows Settings > Security Settings**, click **Public Key Policies**, and then in the right panel double-click **Certificate Services Client - Auto-Enrollment**.


Group Policy Management Editor
File
Action
View
Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Directory (CI
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADMX
Preferences
User Configuration
Object Type
Encrypting File System
BitLocker Drive Encryption
Automatic Certificate Request Settings
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Trusted People
Certificate Services Client - Certificate Enrollment Policy
Certificate Path Validation Settings
Certificate Services Client - Auto-Enrollment

Step 4: In Configuration Model select **Enabled**, select the first two check boxes that start with **Renew** and **Update**, and then click **OK**.



Certificate Services Client - Auto-Enrollment Properties
Enrollment Policy Configuration
OK
Cancel
Apply

Enroll user and computer certificates automatically

Configuration Model: Enabled

☑ Renew expired certificates, update pending certificates, and remove revoked certificates

☑ Update certificates that use certificate templates

☐ Expiration notification

Show expiry notifications when the percentage of remaining certificate lifetime is 10 %

Learn more about Automatic certificate management

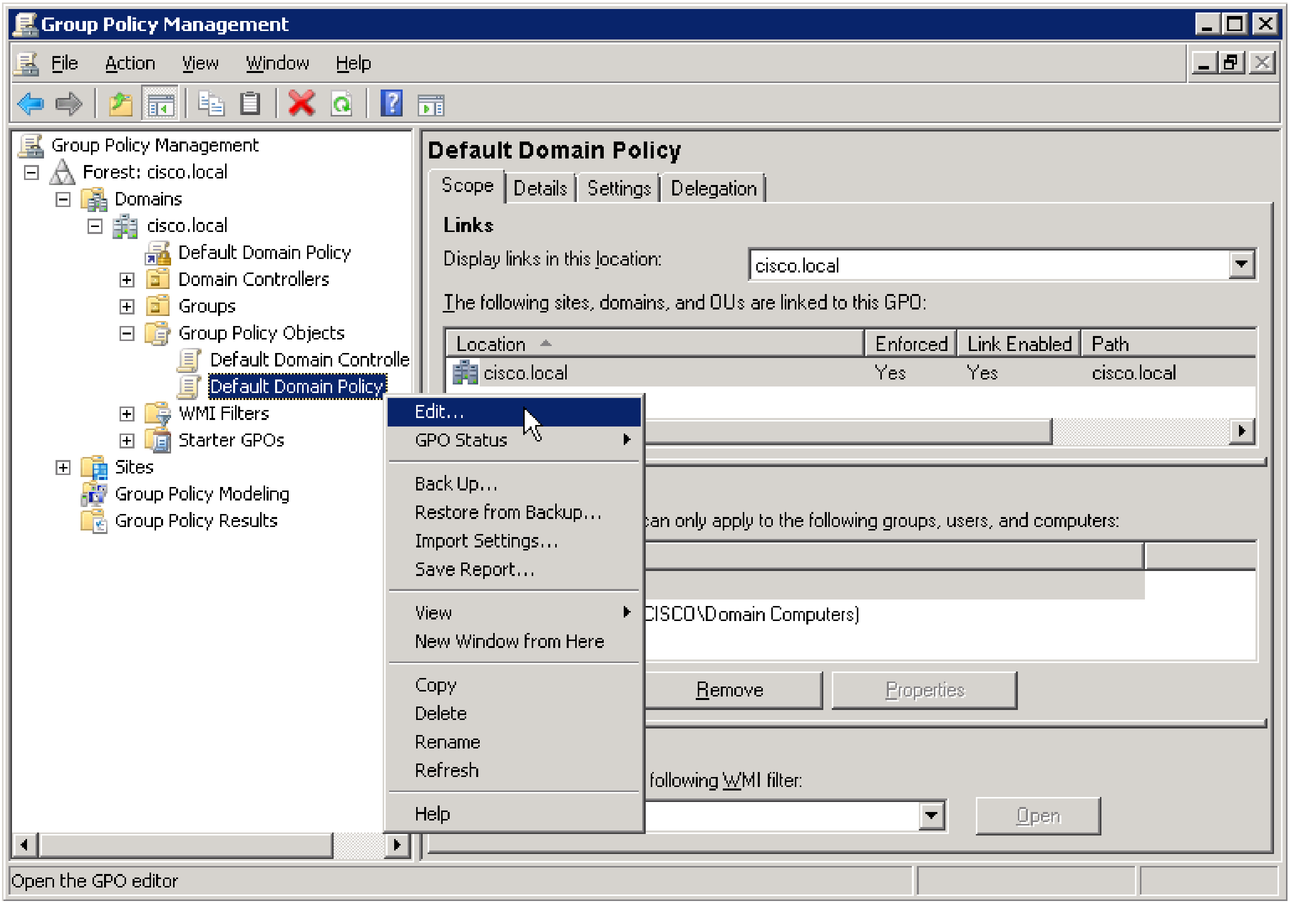
Domain computers will have a certificate pushed to them the next time they log in to the domain or after the GPO policy is refreshed.

Procedure 5 Configure GPOs for wired endpoints

This deployment uses GPOs to configure the 802.1X supplicant on wired endpoints running Microsoft Windows 7.

Step 1: On the AD console, navigate to **Start > Administrative Tools > Group Policy Management**.

Step 2: In the left pane, expand **Forest: [local domain]** > **Domains** > **[local domain]** > **Group Policy Objects**, right-click **Default Domain Policy**, and then click **Edit**. The Group Policy Management Editor opens.



Display links in this location: cisco.local

The following sites, domains, and OUs are linked to this GPO:

Location	Enforced	Link Enabled	Path
cisco.local	Yes	Yes	cisco.local

can only apply to the following groups, users, and computers:

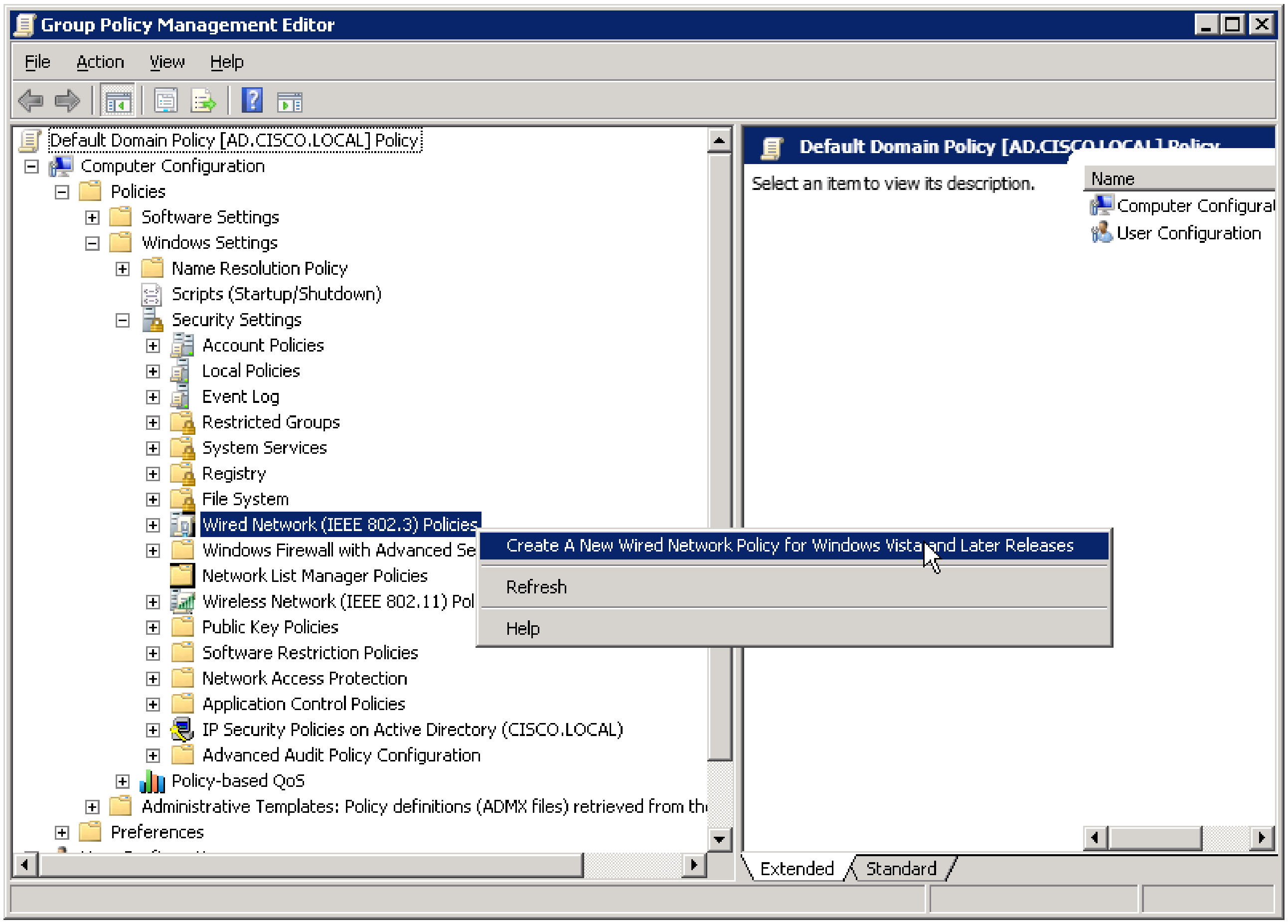
CISCO\Domain Computers)

following WMI filter:

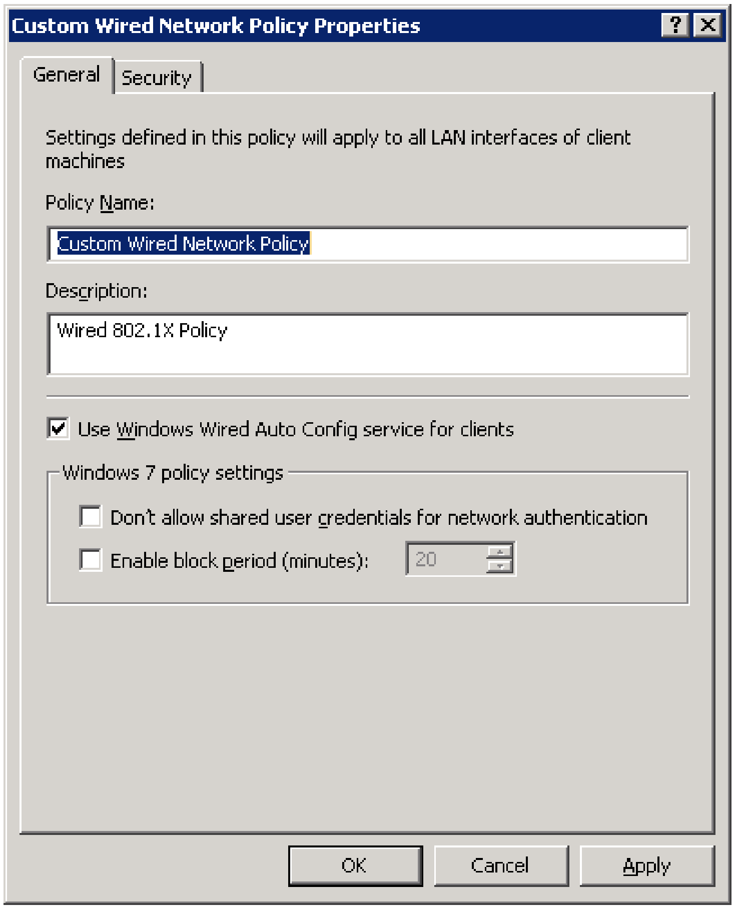
Open the GPO editor

Step 3: In the Group Policy Management Editor, navigate to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings**, right-click **Wired Network (IEEE 802.3) Policies**, and then choose **Create a New Wired Network Policy for Windows Vista and Later Releases**.

After the first time you have created this policy, the option to create a new wired policy is no longer displayed.


Group Policy Management Editor
File Action View Help
Default Domain Policy [AD.CISCO.LOCAL] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Se
Network List Manager Policies
Wireless Network (IEEE 802.11) Pol
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Directory (CISCO.LOCAL)
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADMX files) retrieved from th
Preferences
Create A New Wired Network Policy for Windows Vista and Later Releases
Refresh
Help
Default Domain Policy [AD.CISCO.LOCAL] Policy
Select an item to view its description.
Name
Computer Configural
User Configuration
Extended
Standard

Step 4: In the New Wired Network Policy Properties box, on the General tab, give the policy a name and description.



Settings defined in this policy will apply to all LAN interfaces of client machines

Policy Name: Custom Wired Network Policy

Description: Wired 802.1X Policy

☑ Use Windows Wired Auto Config service for clients

Windows 7 policy settings

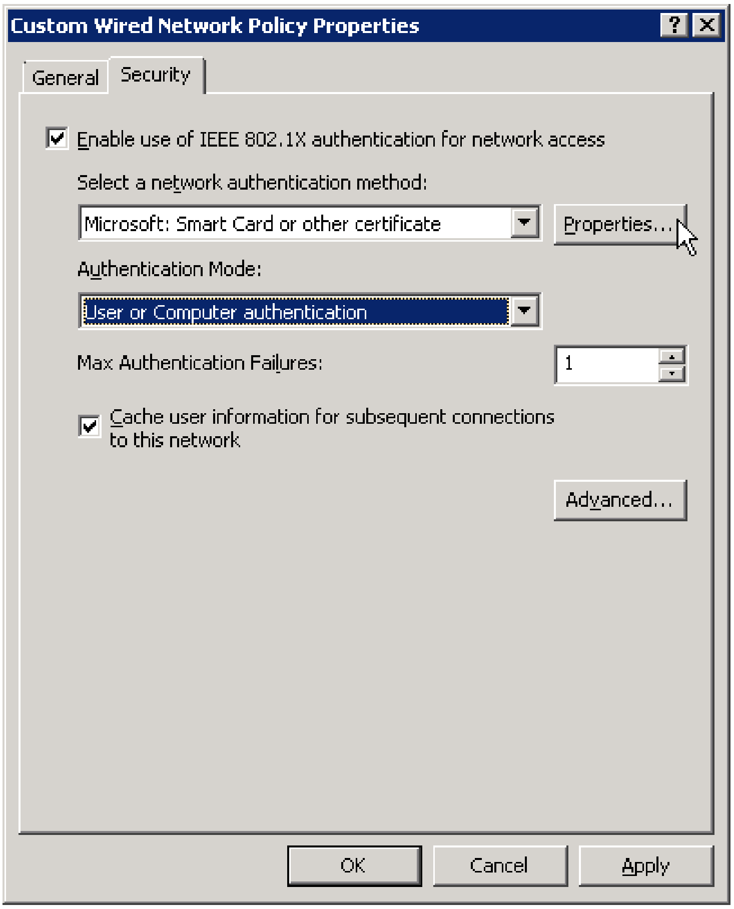
☐ Don't allow shared user credentials for network authentication

☐ Enable block period (minutes): 20

Step 5: Verify that **Use Windows Wired Auto Config service for clients** is selected.

Step 6: On the Security tab, verify that **Enable of IEEE 802.1X authentication for network access** is selected.

Step 7: In the **Select a Network Authentication Method** list, choose **Microsoft: Smart Card or other certificate**.


Custom Wired Network Policy Properties
General
Security
☑ Enable use of IEEE 802.1X authentication for network access
Select a network authentication method:
Microsoft: Smart Card or other certificate
Properties...
Authentication Mode:
User or Computer authentication
Max Authentication Failures:
1
☑ Cache user information for subsequent connections to this network
Advanced...
OK
Cancel
Apply

Step 8: In the **Authentication Mode** list, choose **User or computer authentication**.

Step 9: Click **Properties.**

Step 10: In Smart Card or other Certificate Properties, verify that the following settings are selected:

- **Use a certificate on this computer**
- **Use simple certificate selection (Recommended)**
- **Validate server certificate**

Step 11: In the **Trusted Root Certification Authorities** list, next to the root certificate for the CA, select the check box, and then click **OK**. The certificate properties window closes.

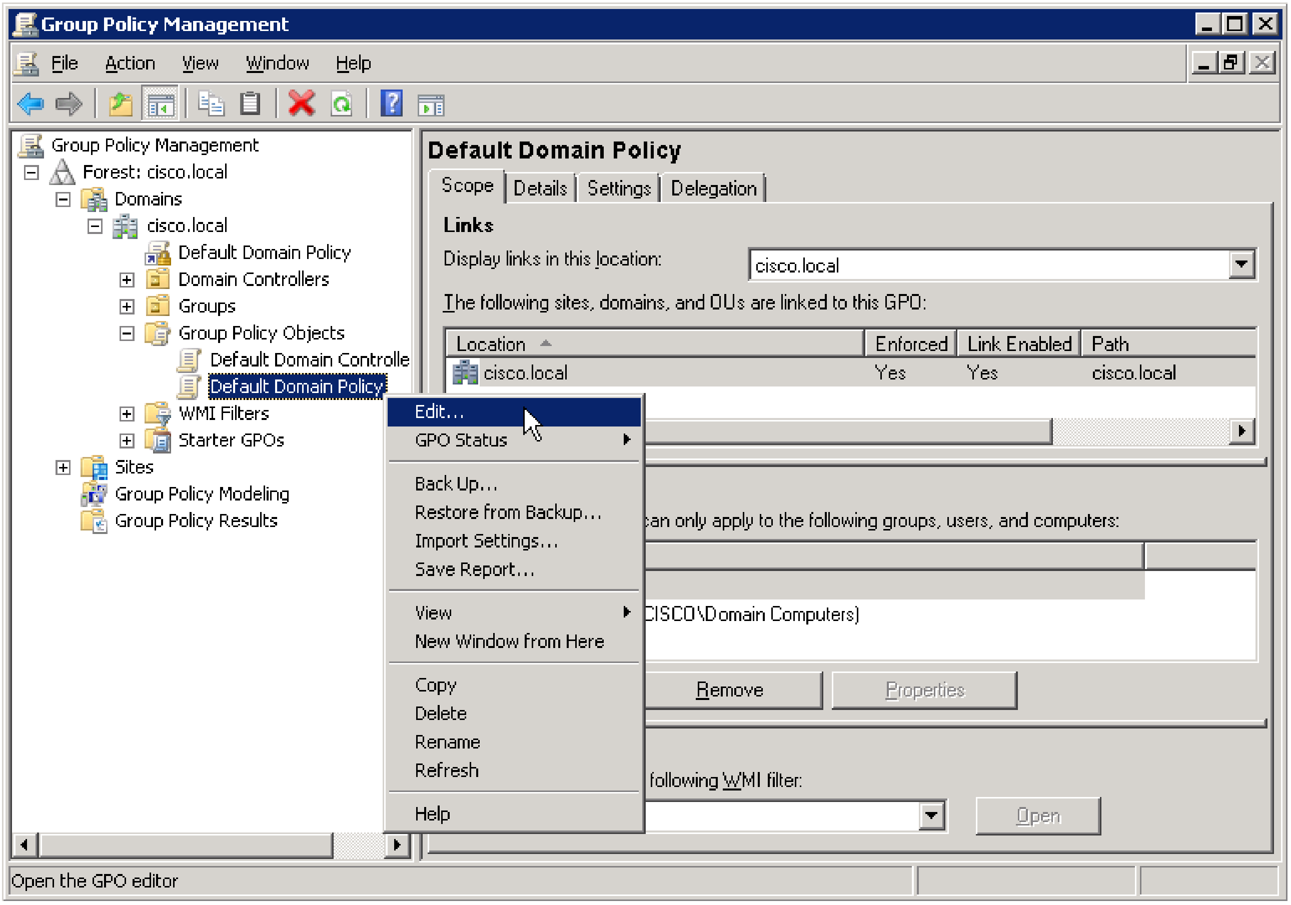
Step 12: In the policy properties window, click **Apply**, and then click **OK** again.

Procedure 6 Configure GPOs for wireless endpoints

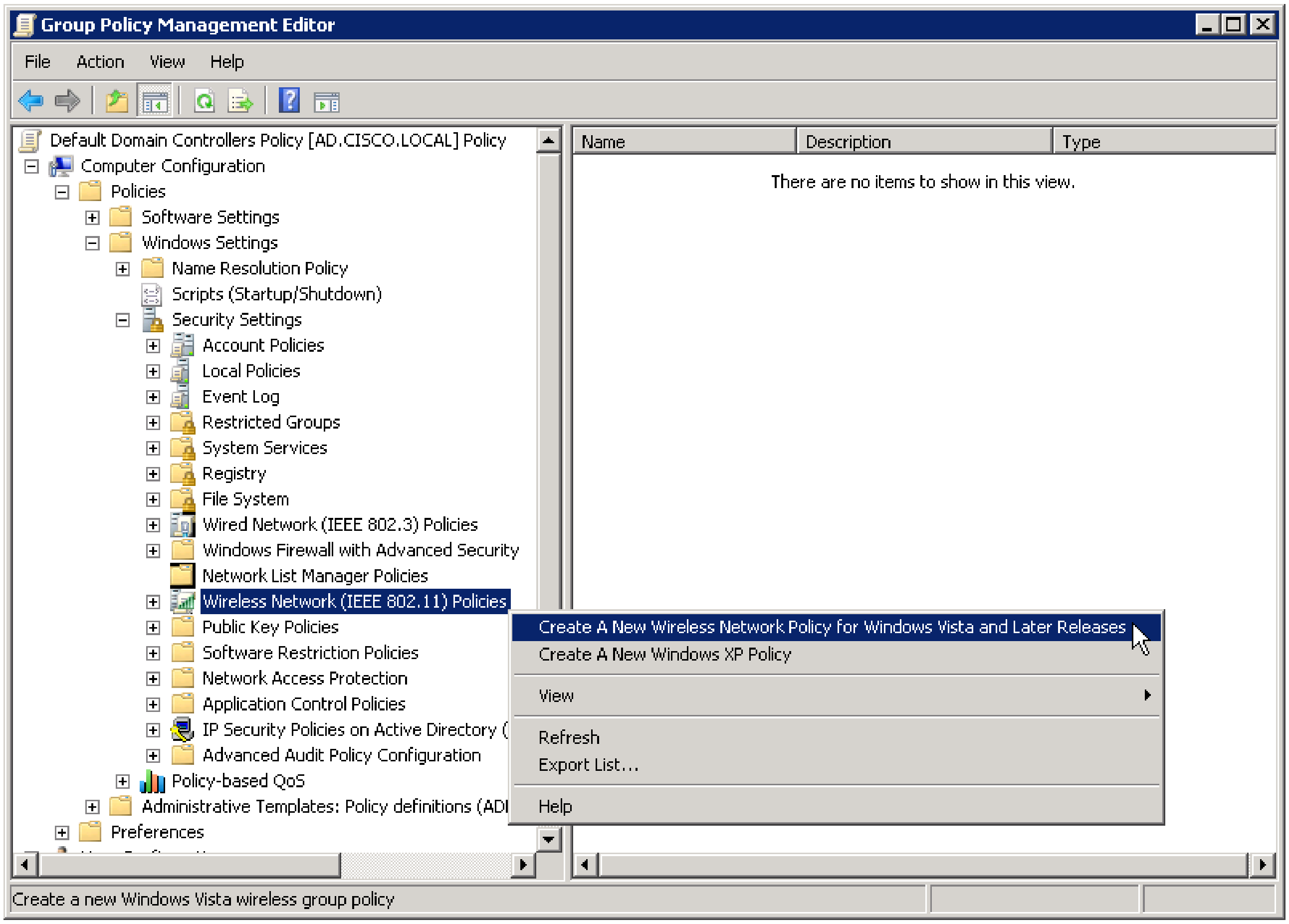
This deployment uses GPOs to configure the 802.1X supplicant for wireless endpoints running Windows 7.

Step 1: On the AD console, navigate to **Start > Administrative Tools > Group Policy Management**.

Step 2: In the left pane, expand **Forest: [local domain] > Domains > [local domain] > Group Policy Objects**, right-click **Default Domain Policy**, and then click **Edit**. The Group Policy Management editor opens.



Step 3: In the Group Policy Management Editor, navigate to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings**, right-click **Wireless Network (IEEE 802.11) Policies**, and then choose **Create a New Wireless Network Policy for Windows Vista and Later Releases**.


Group Policy Management Editor
File
Action
View
Help
Default Domain Controllers Policy [AD.CISCO.LOCAL] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Network Access Protection
Application Control Policies
IP Security Policies on Active Directory (
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates: Policy definitions (ADI
Preferences
Name
Description
Type
Create A New Wireless Network Policy for Windows Vista and Later Releases
Create A New Windows XP Policy
View
Refresh
Export List...
Help

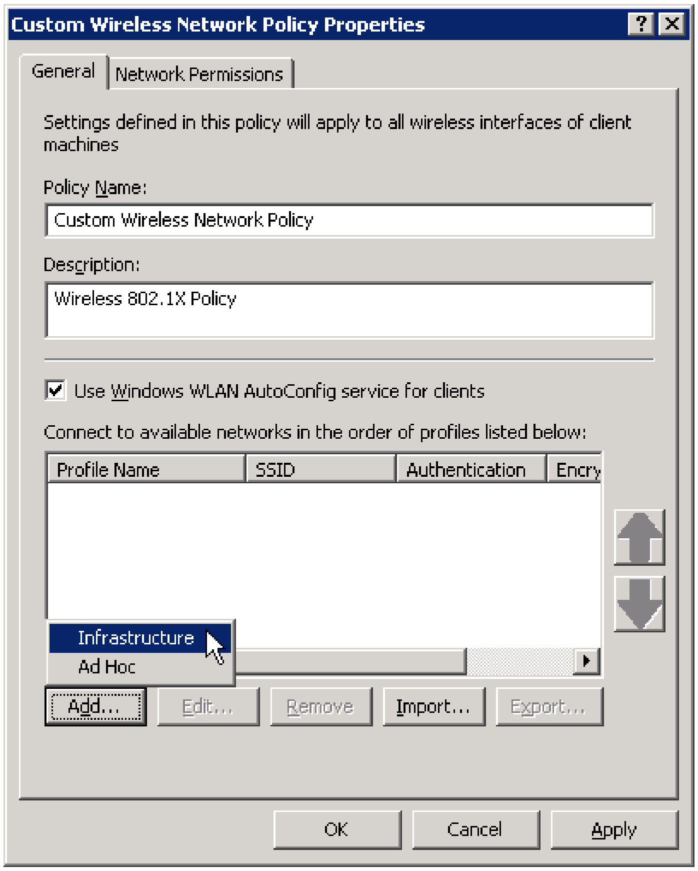
There are no items to show in this view.

Create a new Windows Vista wireless group policy

Step 4: In the Custom Wireless Network Policy Properties box, on the General tab, give the policy a name and description.

Step 5: Verify that **Use Windows WLAN AutoConfig service for clients** is selected.

Step 6: Click **Add**, and then choose **Infrastructure**.



Custom Wireless Network Policy Properties

Settings defined in this policy will apply to all wireless interfaces of client machines

Policy Name: Custom Wireless Network Policy

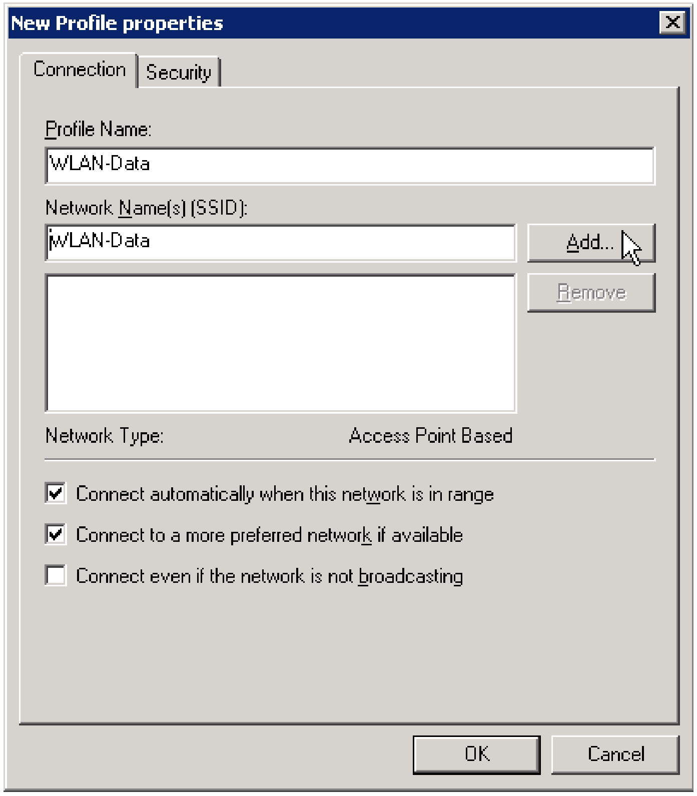
Description: Wireless 802.1X Policy

☑ Use Windows WLAN AutoConfig service for clients

Connect to available networks in the order of profiles listed below:

Profile Name	SSID	Authentication	Encry

Step 7: In the New Profile properties window, on the Connection tab, enter a **Profile Name.**



New Profile properties

Profile Name: WLAN-Data

Network Name(s) (SSID): WLAN-Data

Network Type: Access Point Based

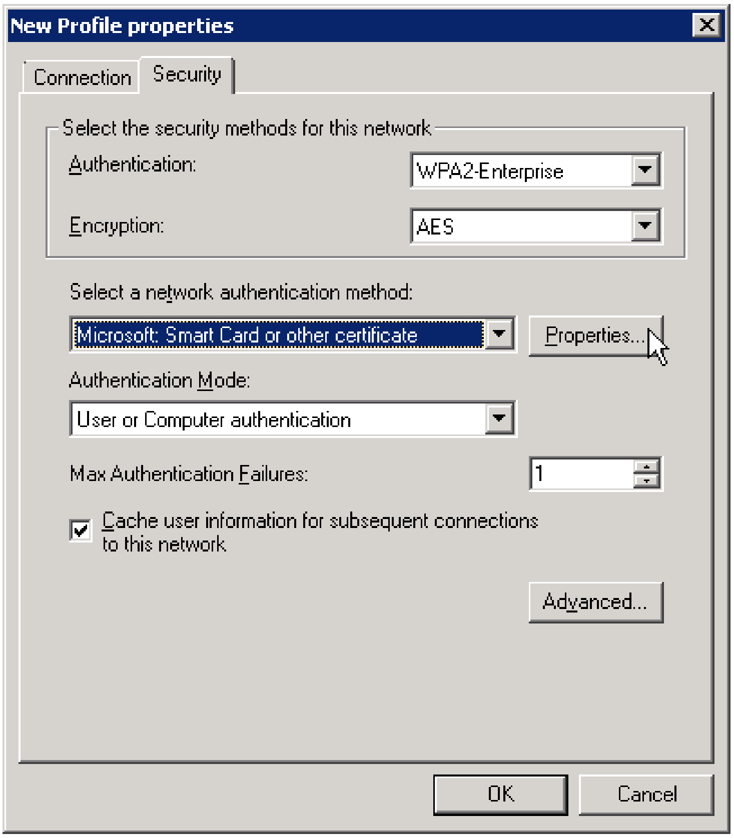
☑ Connect automatically when this network is in range

☑ Connect to a more preferred network if available

☐ Connect even if the network is not broadcasting

Step 8: In the **Network Name(s) (SSID)** box, enter the wireless network SSID, and then click **Add**.

Step 9: On the Security tab, in the **Authentication** list, choose **WPA2-Enterprise**, and then in the **Encryption** list, choose **AES**.


New Profile properties

Select the security methods for this network

Authentication: WPA2-Enterprise

Encryption: AES

Select a network authentication method: Microsoft: Smart Card or other certificate

Authentication Mode: User or Computer authentication

Max Authentication Failures: 1

☑ Cache user information for subsequent connections to this network

Step 10: In the **Select a network authentication method** list, choose **Microsoft: Smart Card or other certificate**.

Step 11: In the **Authentication Mode** list, choose **User or Computer authentication**.

Step 12: Click **Properties.**

Step 13: In the Smart Card or other Certificate Properties window, verify that the following settings are selected:

- **Use a certificate on this computer**
- **Use simple certificate selection (Recommended)**
- **Validate server certificate**

Step 14: In the **Trusted Root Certification Authorities** list, next to the root certificate for the CA, select the check box, and then click **OK**. The certificate properties window closes.

Step 15: Click **OK**. The profile properties window closes.

Step 16: In the policy properties window, click **Apply**, and then click **OK**.

At this point, all endpoints running Windows 7 (and later) will have a 802.1X supplicant configuration pushed to them the next time they log in to the domain or after the GPO policy is refreshed.

PROCESS

Deploying Cisco AnyConnect on Windows Endpoints

1. Install Cisco AnyConnect
2. Install Profile Editor
3. Create wired profile
4. Create wireless profile

Cisco AnyConnect Secure Mobility Client can be used as an 802.1X supplicant on Windows endpoints, using the Network Access Manager module. In this example deployment, the Network Access Manager is configured with both wired and wireless profiles using digital certificates.

Procedure 1 Install Cisco AnyConnect

To use Cisco AnyConnect Secure Mobility Client as your 802.1X supplicant on Windows endpoints, download the latest version along with the Profile Editor. The latest Cisco AnyConnect Secure Mobility client and Profile Editor can be downloaded from the following location:

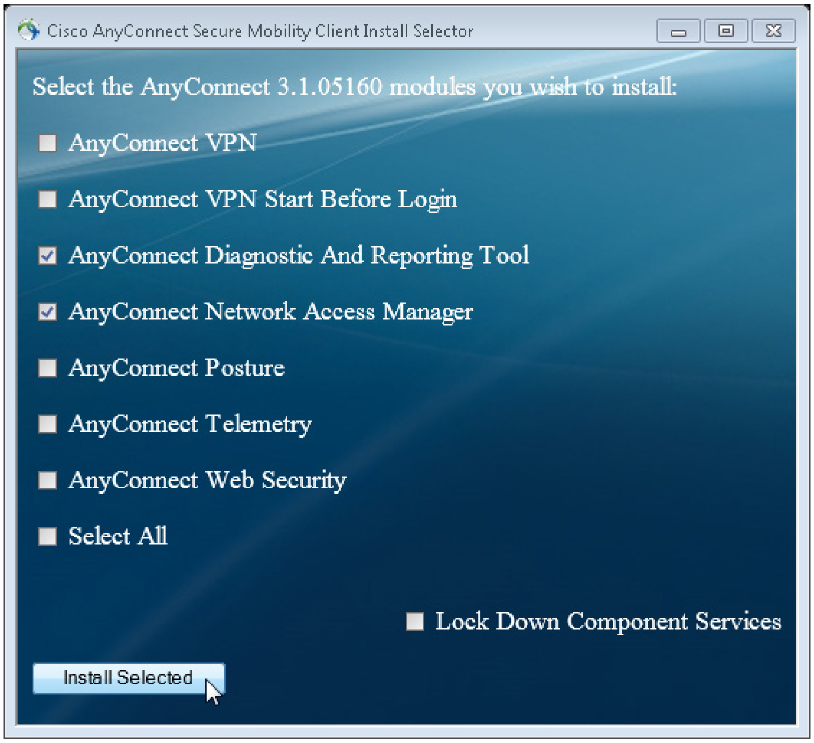
http://software.cisco.com/download/release.html?mdfid=283000185&softwareid=282364313&release=latest

The Windows client is distributed as an ISO image and should be burned to a disk or mounted as a disk image by using a utility that provides this function, such as the Virtual CD-ROM Control Panel from Microsoft. You must be logged in with administrator privileges in order to install AnyConnect Secure Mobility Client.

The client can also be distributed using the Cisco ASA platforms. The ISO distribution method is covered here, because the Cisco ASA distribution method is not available in every deployment situation.

Step 1: Start the installer for the Cisco AnyConnect Secure Mobility Client by launching the Setup program on the disk.

Step 2: Select **AnyConnect Diagnostic and Reporting Tool** and **AnyConnect Network Access Manager**, clear all of the other check boxes, and then click **Install Selected**.



Select the AnyConnect 3.1.05160 modules you wish to install:

☐ AnyConnect VPN
☐ AnyConnect VPN Start Before Login
☑ AnyConnect Diagnostic And Reporting Tool
☑ AnyConnect Network Access Manager
☐ AnyConnect Posture
☐ AnyConnect Telemetry
☐ AnyConnect Web Security
☐ Select All

☐ Lock Down Component Services

Step 3: Click **Install Selected**, verify the components selected to install, and then click **OK**.

Step 4: Click **Accept**. This accepts the license agreement, and the installation begins.

Step 5: After the installation completes, click **OK**. You may be asked to restart Windows to complete the installation.

Procedure 2 Install Profile Editor

Step 1: Locate the Profile Editor Installer downloaded previously, and then double-click it. The installation process starts.

Step 2: If you are prompted to install Java Runtime Environment, click **Next** to install it, and then click **Next** again**.** The installation of Profile Editor continues.

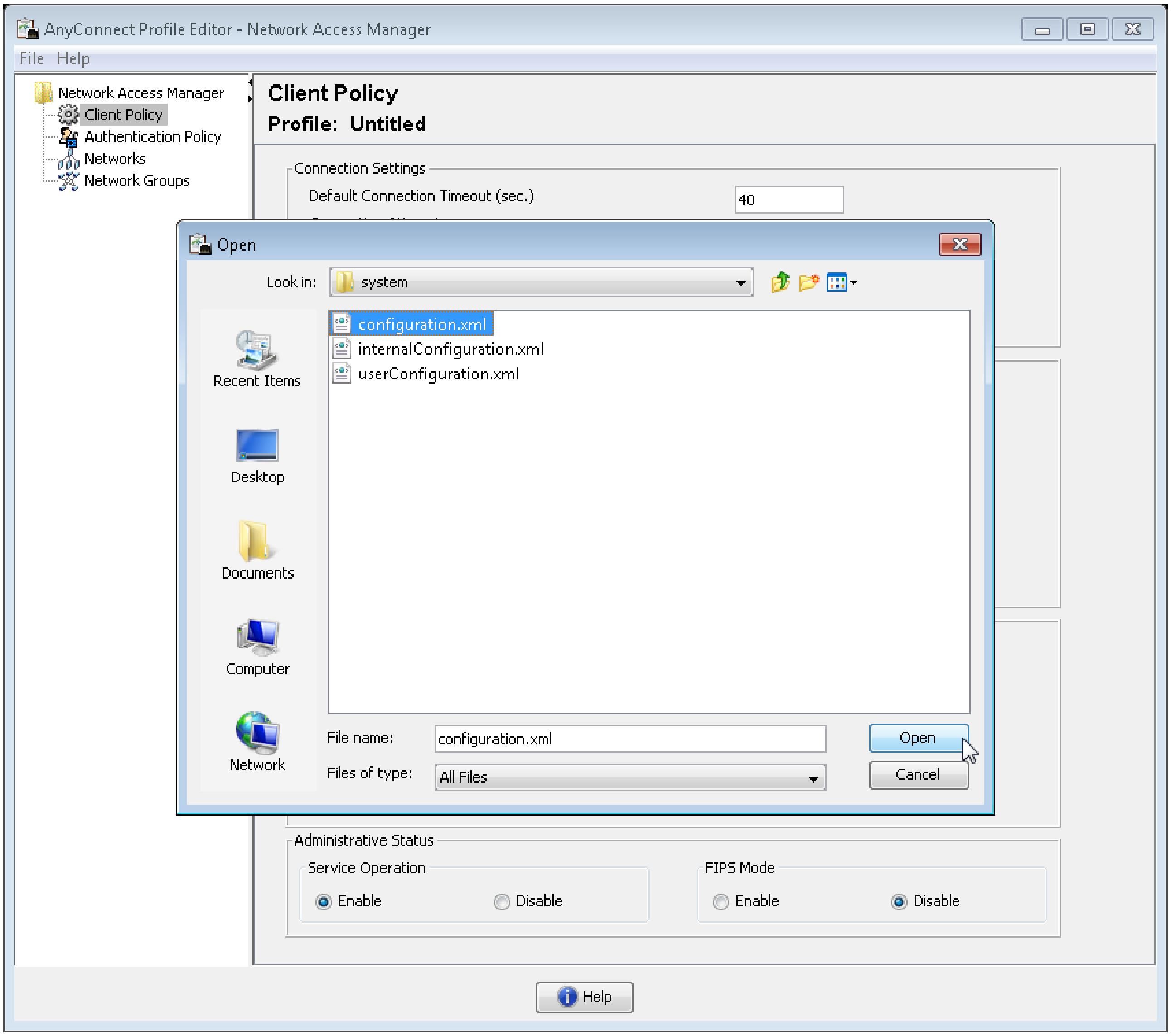
Step 3: Click **Typical**, and then click **Install**.

Step 4: On the Completing the Cisco AnyConnect Profile Editor Setup Wizard page, click **Finish**. The installation completes.

Procedure 3 Create wired profile

Step 1: Launch the Profile Editor by navigating to **Start > All Programs > Cisco > Cisco AnyConnect Profiler Editor > Network Access Manager Profile Editor**.

Step 2: From the **File** menu, choose **Open**, and select **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\configuration.xml**, and then click **Open**.



Default Connection Timeout (sec.) 40

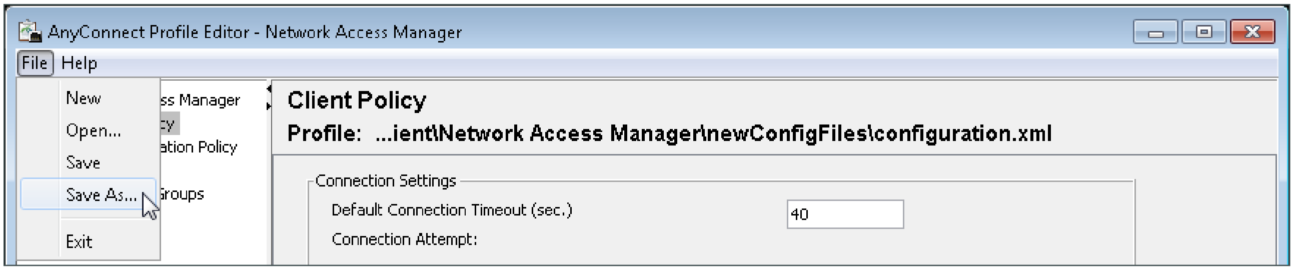
File name: configuration.xml

Files of type: All Files

Service Operation: ● Enable ○ Disable

FIPS Mode: ○ Enable ● Disable

Step 3: If you wish to keep a copy of the original default XML configuration file for later use should you want to be able to start from the beginning, then from the **File** menu, choose **Save As**, and then select **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\default-configuration.xml**. Before continuing, repeat Step 2 to open the original configuration.xml file again.



Client Policy

Profile: ...ient\Network Access Manager\newConfigFiles\configuration.xml

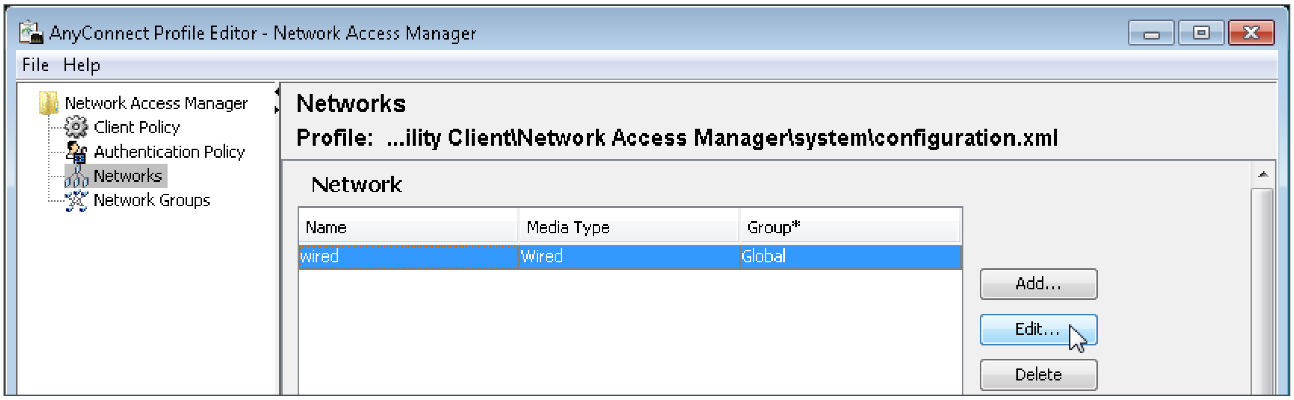
Connection Settings

Default Connection Timeout (sec.) 40

Connection Attempt:

Step 4: In the left panel, click **Networks**.

Step 5: Select the wired profile, and then click **Edit**.



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

Network

Name	Media Type	Group*
wired	Wired	Global

Step 6: Enter a name for the profile, and then click **Next**.

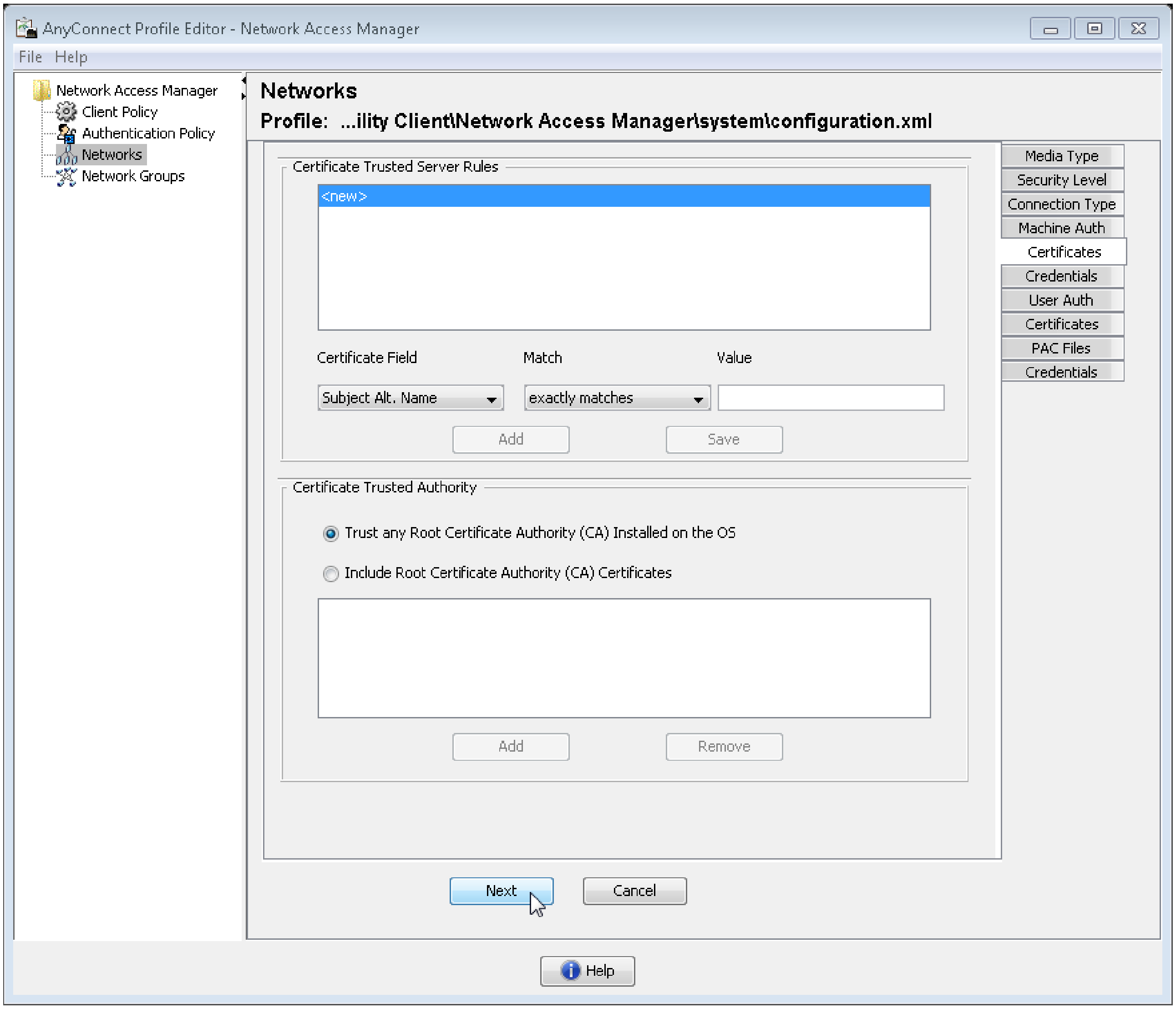
Step 7: On the Security Level tab, verify **Authenticating Network** is selected, and then click **Next**.

Step 8: On the Connection Type tab, verify **Machine and User Connection** is selected, and then click **Next**.

Step 9: On the Machine Auth tab, under EAP Methods, select **EAP-TLS**.

Step 10: Under EAP-TLS Settings, verify that **Validate Server Certificate** and **Enable Fast Reconnect** are selected, and then click **Next**.

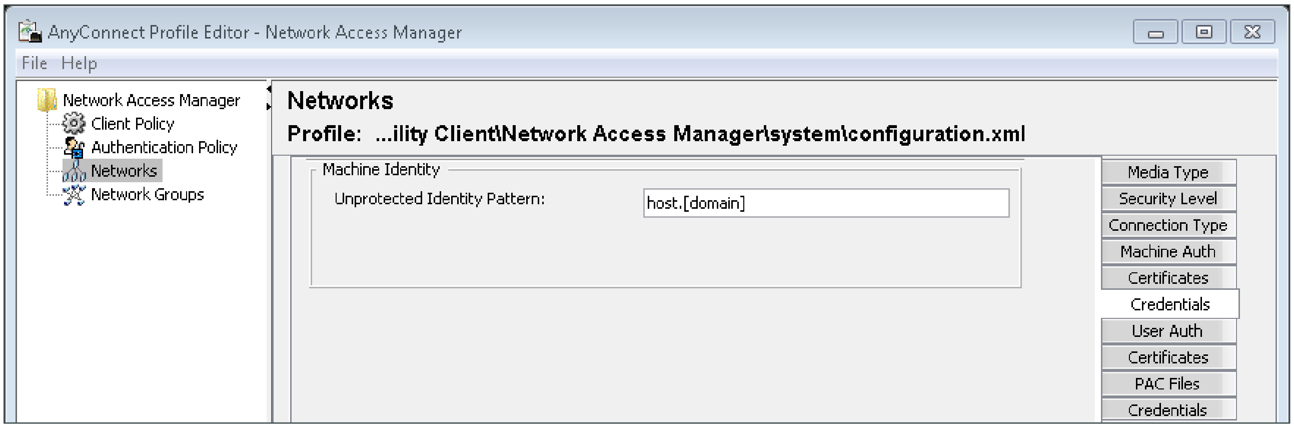
Step 11: Within the first of the two Certificates tabs, under Certificate Trusted Authority, verify that **Trust any Root Certificate Authority (CA) Installed on the OS** is selected, and then click **Next**.



● Trust any Root Certificate Authority (CA) Installed on the OS

○ Include Root Certificate Authority (CA) Certificates

Step 12: Within the first of two Credentials tabs, under Machine Identity, enter a value in the Unprotected Identity Pattern box. In this deployment, change to **host.[domain]**, and then click **Next**.

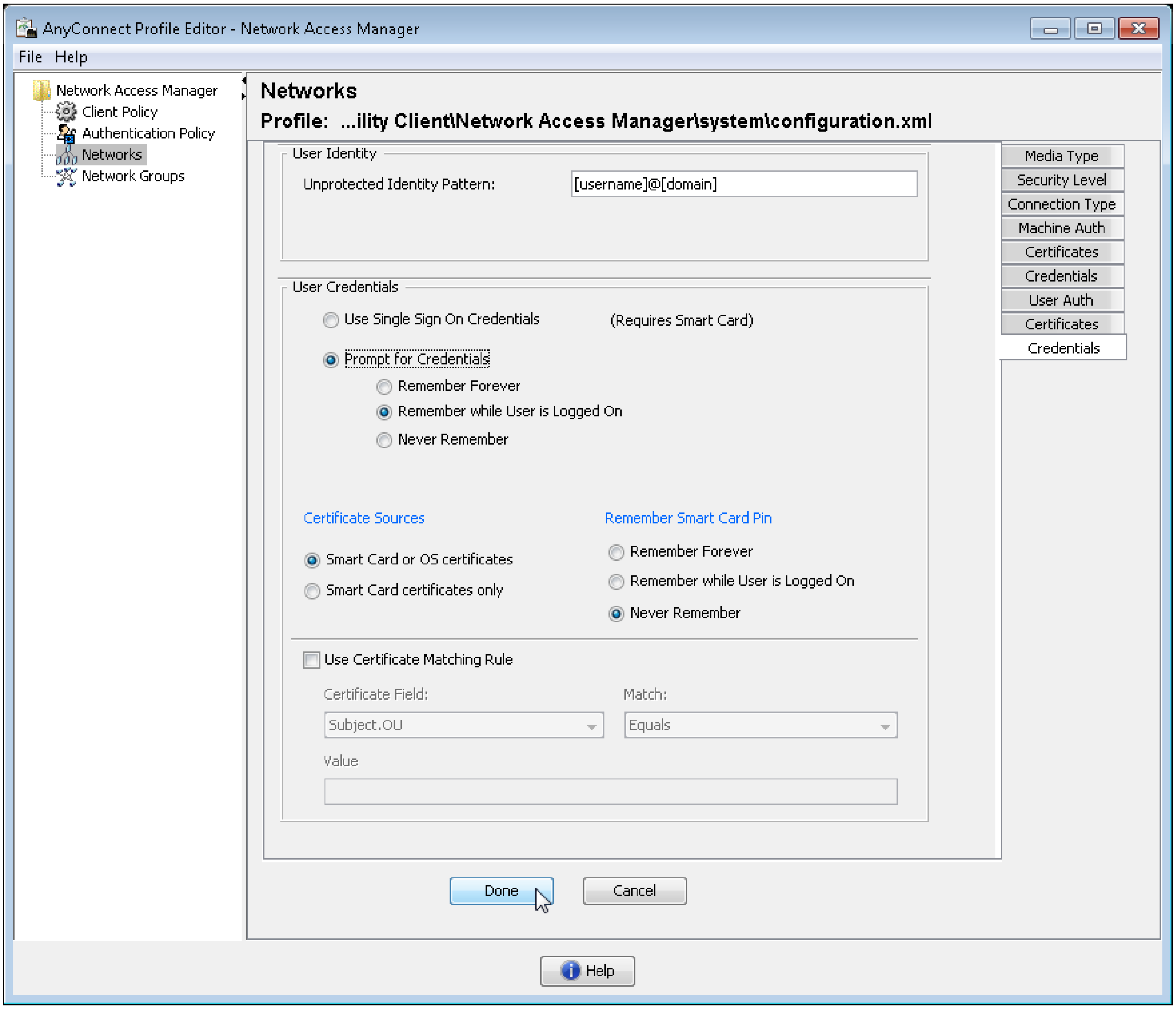


Unprotected Identity Pattern: host.[domain]

Step 13: On the User Auth tab, under EAP Methods, select **EAP-TLS**, under EAP-TLS Settings, verify **Validate Server Certificate** and **Enable Fast Reconnect** are selected, and then click **Next**.

Step 14: Within the second of two Certificates tabs, under Certificate Trusted Authority, verify **Trust any Root Certificate Authority (CA) Installed on the OS** is selected, and then click **Next**.

Step 15: Within the second of two Credentials tabs, under User Identity, enter an unprotected identity pattern. In this deployment, use **[username]@[domain]**. In the User Credentials section, select **Prompt for Credentials**, and then verify **Remember while User is Logged On** is selected.



AnyConnect Profile Editor - Network Access Manager

Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

User Identity

Unprotected Identity Pattern: [username]@[domain]

User Credentials

○ Use Single Sign On Credentials (Requires Smart Card)

● Prompt for Credentials

- ○ Remember Forever
- ● Remember while User is Logged On
- ○ Never Remember

Certificate Sources

● Smart Card or OS certificates

○ Smart Card certificates only

Remember Smart Card Pin

○ Remember Forever

○ Remember while User is Logged On

● Never Remember

☐ Use Certificate Matching Rule

Certificate Field: Subject.OU

Match: Equals

Value

Step 16: Under **Certificate Sources**, verify **Smart Card or OS certificates** is selected, and then click **Done**.

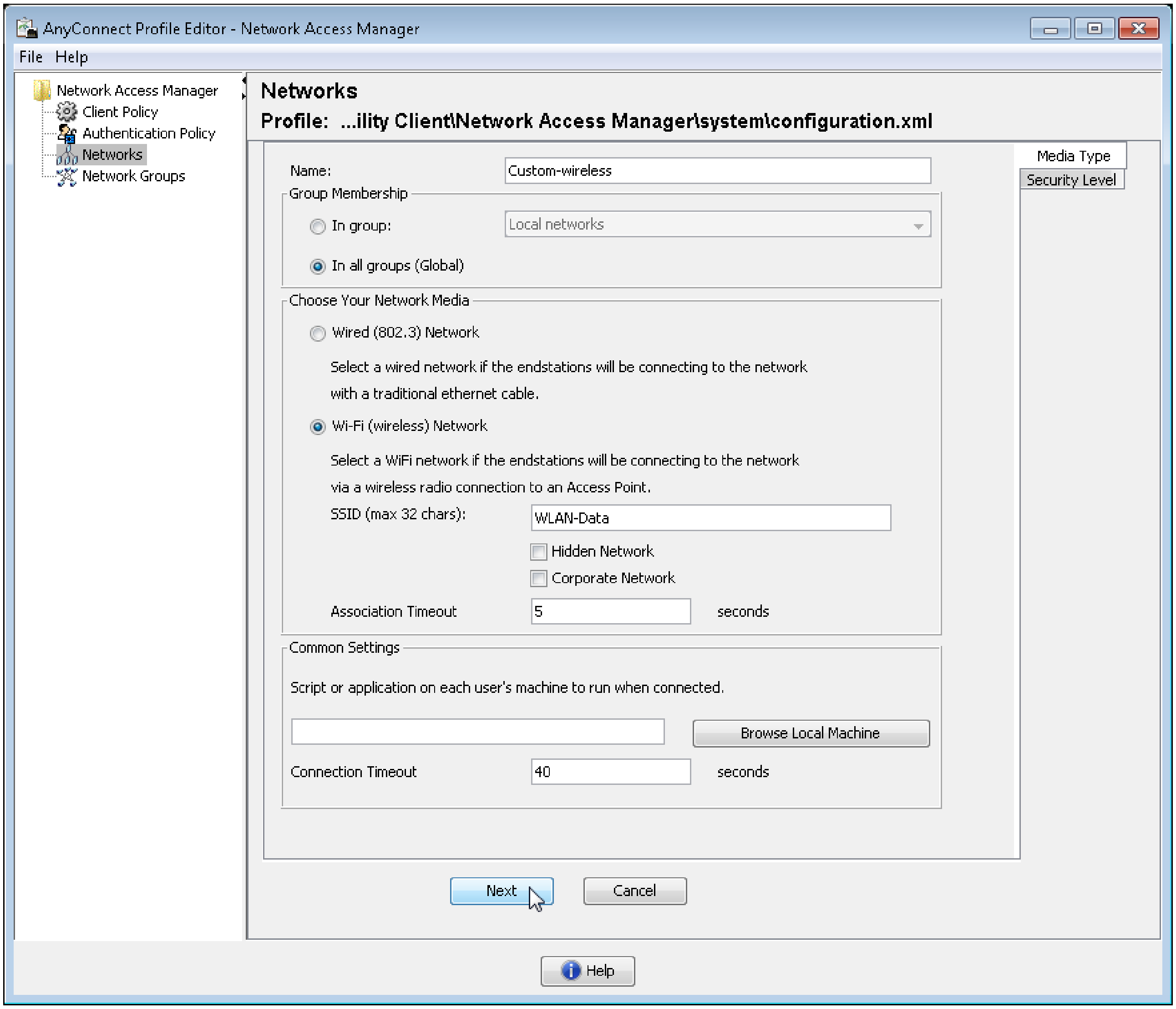
The default wired policy is now modified with your settings and name. If you edit the policy again, the tab selections can be different because of your updated selections.

Procedure 4 Create wireless profile

Step 1: In the Profile Editor, in the left pane click Networks, and then click **Add**. This creates a new profile that you customize for wireless.

Step 2: Enter a name for the profile, and then, for group membership, select **In all groups (Global)**.

Step 3: In the Media Type tab, under Choose Your Network Media, select **Wi-Fi (wireless) Network**, enter the **SSID** of the wireless network, and then click **Next**.



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

Name: Custom-wireless

Group Membership

○ In group: Local networks

● In all groups (Global)

Choose Your Network Media

○ Wired (802.3) Network

Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.

● Wi-Fi (wireless) Network

Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.

SSID (max 32 chars): WLAN-Data

☐ Hidden Network

☐ Corporate Network

Association Timeout 5 seconds

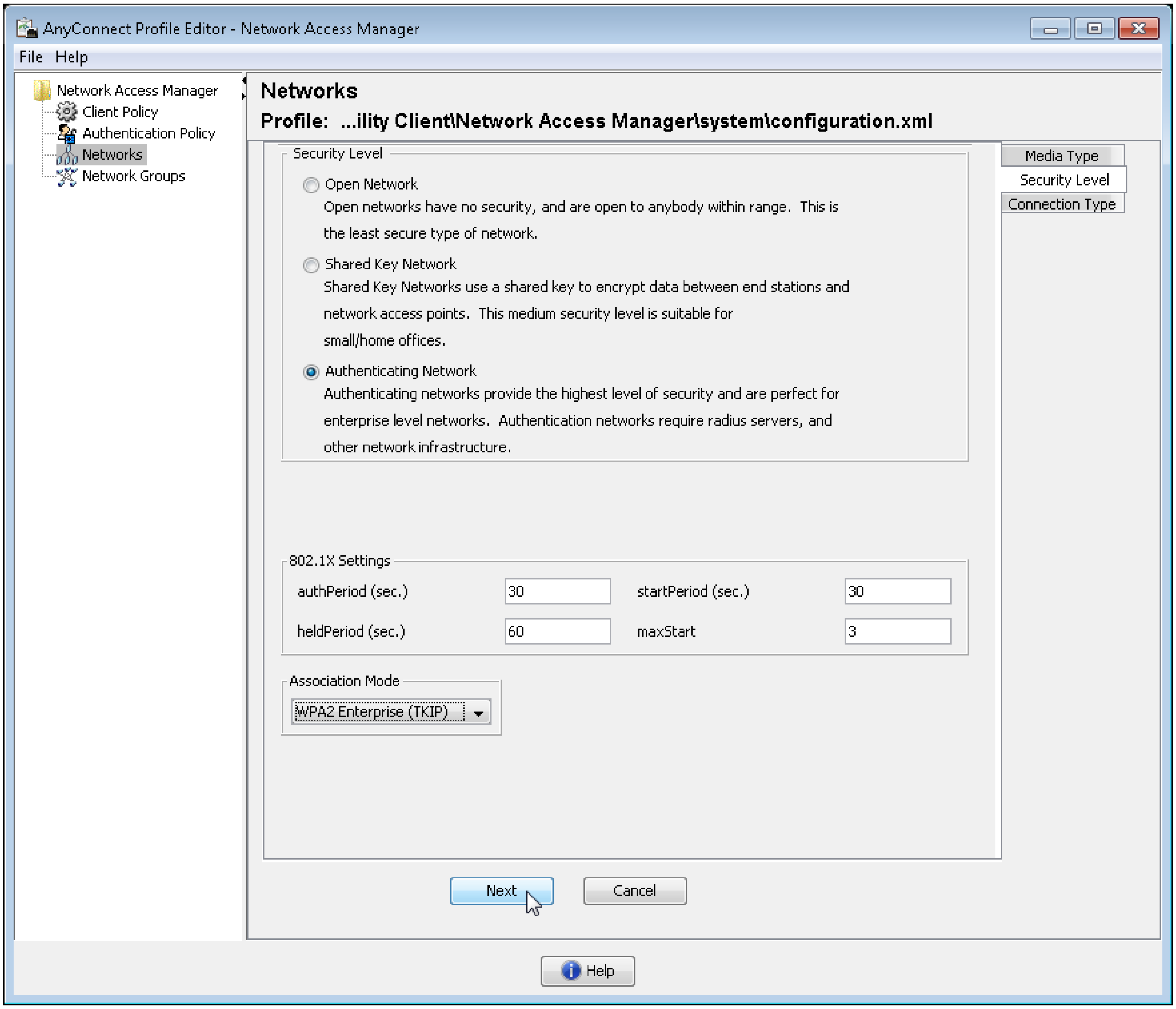
Common Settings

Script or application on each user's machine to run when connected.

Connection Timeout 40 seconds

Step 4: In the Security Level Tab, under Security Level, select **Authenticating Network**. Additional options are displayed.

Step 5: While remaining on the Security Level tab, under Association Mode, change the selection to **WPA2 Enterprise (AES)**, and then click **Next**.



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

Security Level

○ Open Network
Open networks have no security, and are open to anybody within range. This is the least secure type of network.

○ Shared Key Network
Shared Key Networks use a shared key to encrypt data between end stations and network access points. This medium security level is suitable for small/home offices.

● Authenticating Network
Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.

802.1X Settings

authPeriod (sec.)	30	startPeriod (sec.)	30
heldPeriod (sec.)	60	maxStart	3

Association Mode
WPA2 Enterprise (TKIP)

Step 6: In the Connection Type tab, under Network Connection Type, select **Machine and User Connection**, and then click **Next**.

Step 7: In the Machine Auth tab, under EAP Methods, select **EAP-TLS**, verify **Validate Server Certificate** and **Enable Fast Reconnect** are selected, and then click **Next**.

Step 8: In the Certificates tab, under Certificate Trusted Authority, verify **Trust any Root Certificate Authority (CA) Installed on the OS** is selected, and then click **Next**.

Step 9: In the first of the two Credentials tabs, under Machine Identity, enter a value in the Unprotected Identity Pattern box. In this deployment, change to **host.[domain]**, and then click **Next**.

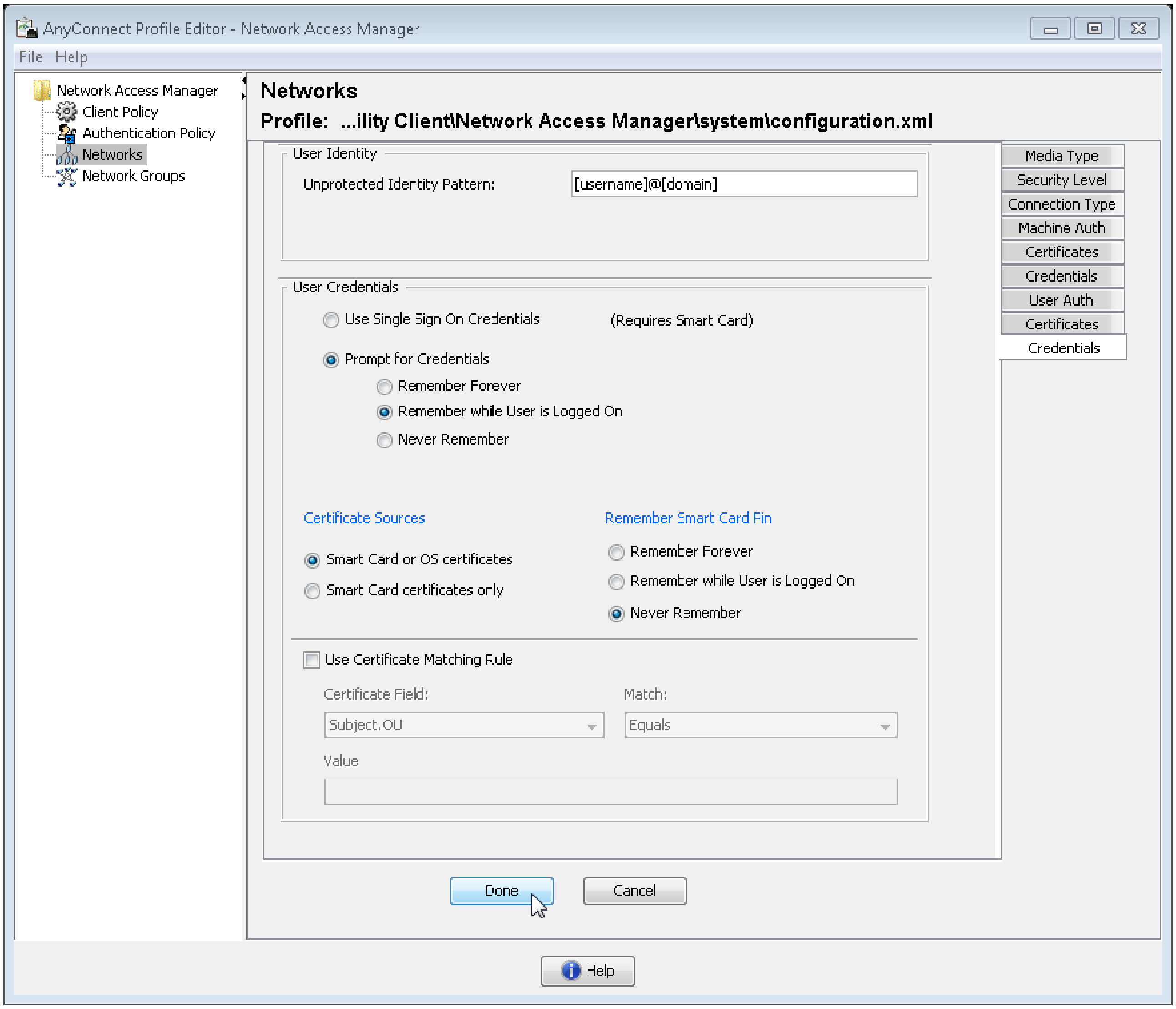
Step 10: In the User Auth tab, under EAP Methods, select **EAP-TLS**, verify **Validate Server Certificate** and **Enable Fast Reconnect** are selected, and then click **Next**.

Step 11: In the second of two Certificates tabs, under Certificate Trusted Authority, verify that **Trust any Root Certificate Authority (CA) Installed on the OS** is selected, and then click **Next**.

Step 12: In the second of the two Credentials tabs, under User Identity, enter an unprotected identity pattern. In this deployment, use **[username]@[domain]**.

Step 13: In the User Credentials section, select **Prompt for Credentials**, verify **Remember while User is Logged On** is selected.

Step 14: Under **Certificate Sources**, verify that **Smart Card or OS certificates** is selected, and then click **Done**.



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

User Identity

Unprotected Identity Pattern: [username]@[domain]

User Credentials

○ Use Single Sign On Credentials (Requires Smart Card)

● Prompt for Credentials

- ○ Remember Forever
- ● Remember while User is Logged On
- ○ Never Remember

Certificate Sources

● Smart Card or OS certificates

○ Smart Card certificates only

Remember Smart Card Pin

○ Remember Forever

○ Remember while User is Logged On

● Never Remember

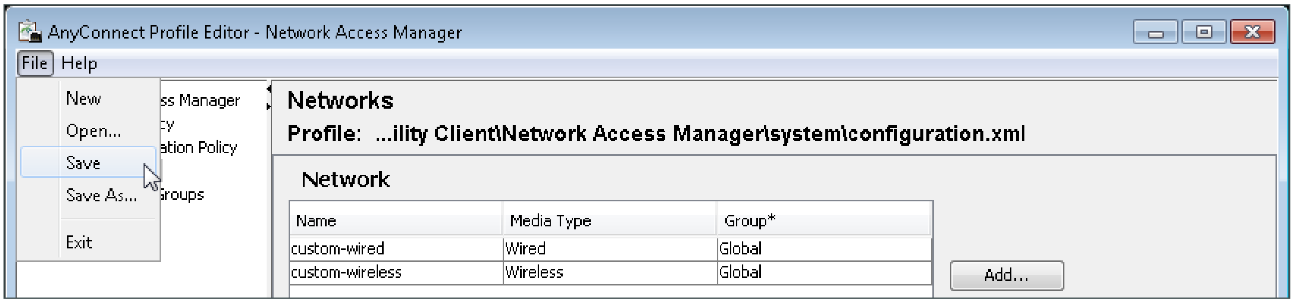
☐ Use Certificate Matching Rule

Certificate Field: Subject.OU

Match: Equals

Value

Step 15: From the **File** menu, choose **Save**. This updates the XML configuration file with the user-modified settings.



Profile: ...ility Client\Network Access Manager\system\configuration.xml

Name	Media Type	Group*
custom-wired	Wired	Global
custom-wireless	Wireless	Global

Tech Tip

When you deploy the Cisco AnyConnect Secure Mobility Client to multiple workstations, you can apply an identical policy by creating a customized installation package.

To create the package, copy all the files from the installation disk to a temporary folder (for example: **C:\AnyConnect**). Then follow the procedures to edit the profile. Copy the configuration file containing the profile edits from **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\configuration.xml** into the temporary folder location, **C:\AnyConnect\Profiles\nam\configuration.xml**.

Finally, copy the updated contents of the **C:\AnyConnect** temporary folder to removable media, such as, CD, DVD, USB drive, etc., and use the media for workstation installation. The custom configuration file is loaded and ready for use upon installation.

At this point, all Windows endpoints now have certificates deployed and are enabled to use 802.1X authentication. On the wireless network, any device that doesn't have a certificate uses PEAP to gain access to the network. Monitor mode is running on the wired network, so endpoints that aren't configured for 802.1X still get access by using MAB.

PROCESS

Configuring Mac Workstations for 802.1X Authentication

1. Install root certificate on Mac OS X
2. Request user certificate

If you have Apple Mac endpoints, you have to manually obtain a certificate and configure 802.1X authentication. The example deployment shows how you do this using Mac OS X 10.9.

Procedure 1 Install root certificate on Mac OS X

To install a trusted root certificate on Mac OS X, you manually request the certificate from the CA and install the certificate in the keychain.

Step 1: On the Mac, browse to the CA at **https://ca.cisco.local/certsrv**.

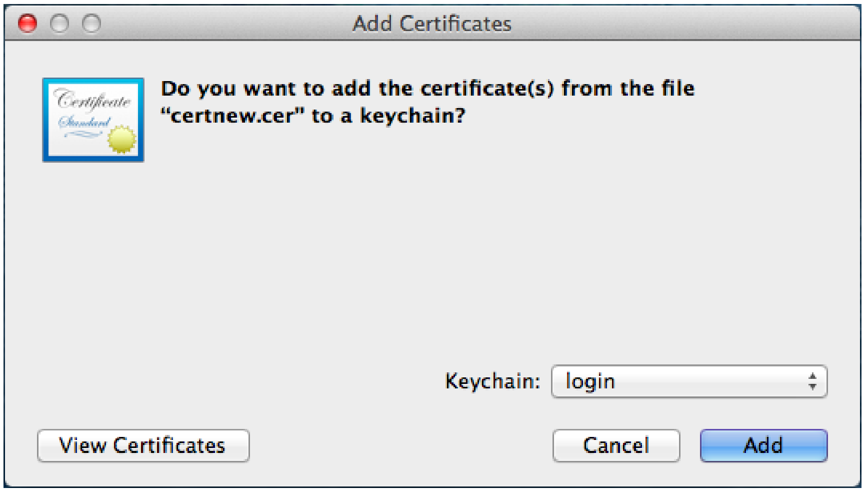
Step 2: Click **Download a CA certificate, certificate chain, or CRL**.

Step 3: Verify that the current certificate is selected.

Step 4: Verify that Encoding Method **DER** is selected.

Step 5: Click **Download CA Certificate**, and then save the certificate file.

Step 6: Locate the certificate file, and then double-click it. This launches the Keychain Access utility, and the Add Certificates dialog box appears.



Do you want to add the certificate(s) from the file “certnew.cer” to a keychain?

Keychain: login

Step 7: Click **Add**. The certificate is added to the machine.

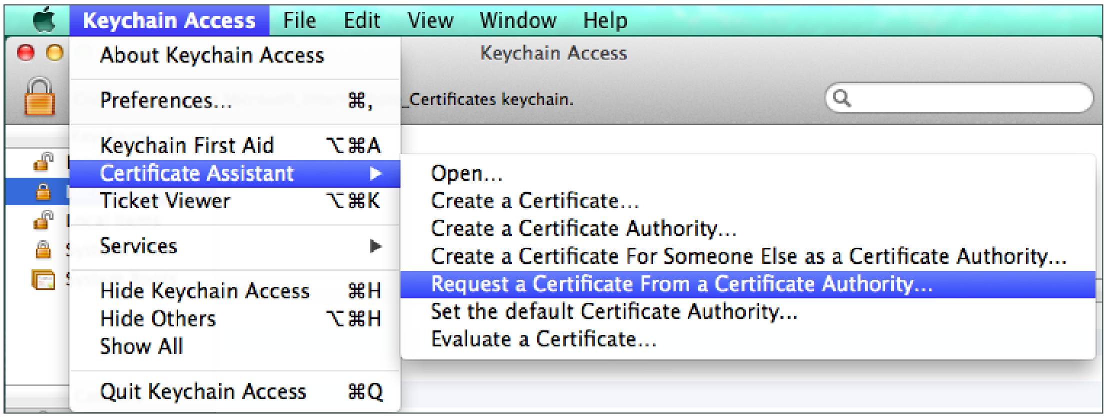
Tech Tip

You may be prompted for credentials of a user with permission to change the certificate trust settings.

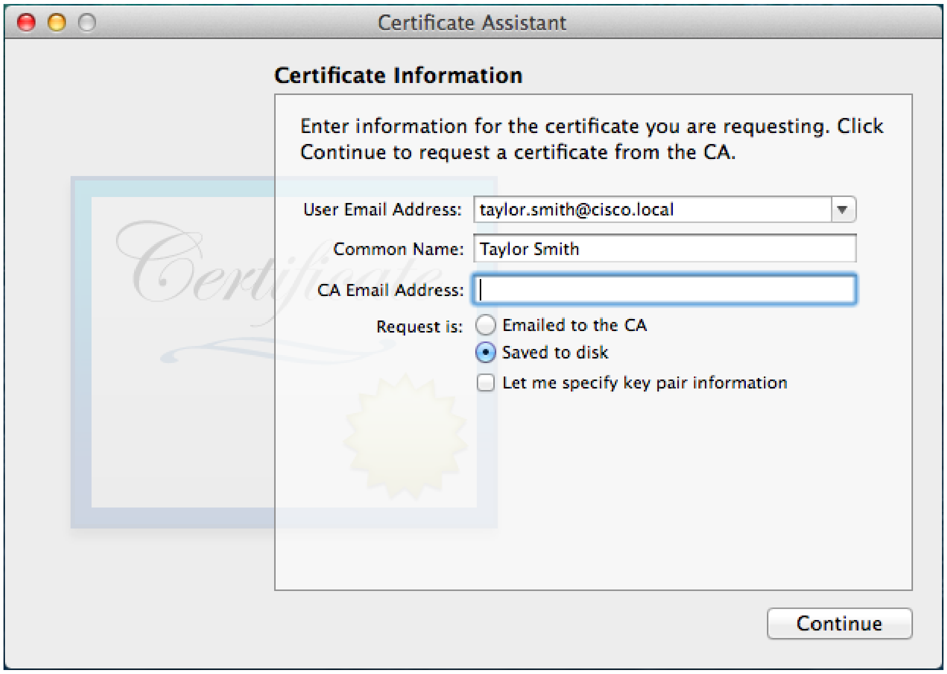
Procedure 2 Request user certificate

Next, you need to obtain a user certificate for the Mac. To do this, first you need to generate a certificate signing request, and then request the certificate from the CA.

Step 1: In the Keychain Access utility, from the **Keychain Access** menu, choose **Certificate Assistant > Request a Certificate from a Certificate Authority**.



Step 2: In Certificate Assistant, enter the Mac user's email address and common name (typically the user's first and last names), select **Saved to disk**, and then click **Continue**.



Certificate Information

Enter information for the certificate you are requesting. Click Continue to request a certificate from the CA.

User Email Address: taylor.smith@cisco.local

Common Name: Taylor Smith

CA Email Address:

Request is: ○ Emailed to the CA

● Saved to disk

☐ Let me specify key pair information

Step 3: Enter a file name and location, click **Save**, and then click **Done**.

Step 4: On the Mac, browse to **https://ca.cisco.local/certsrv**.

Step 5: Authenticate to the CA as the user for which you wish to obtain a certificate.

Tech Tip

If you still have the browser window open from when you downloaded the trusted root certificate, click **Home** in the upper right corner. This returns you to the main page of the CA.

Step 6: Click **Request a certificate**.

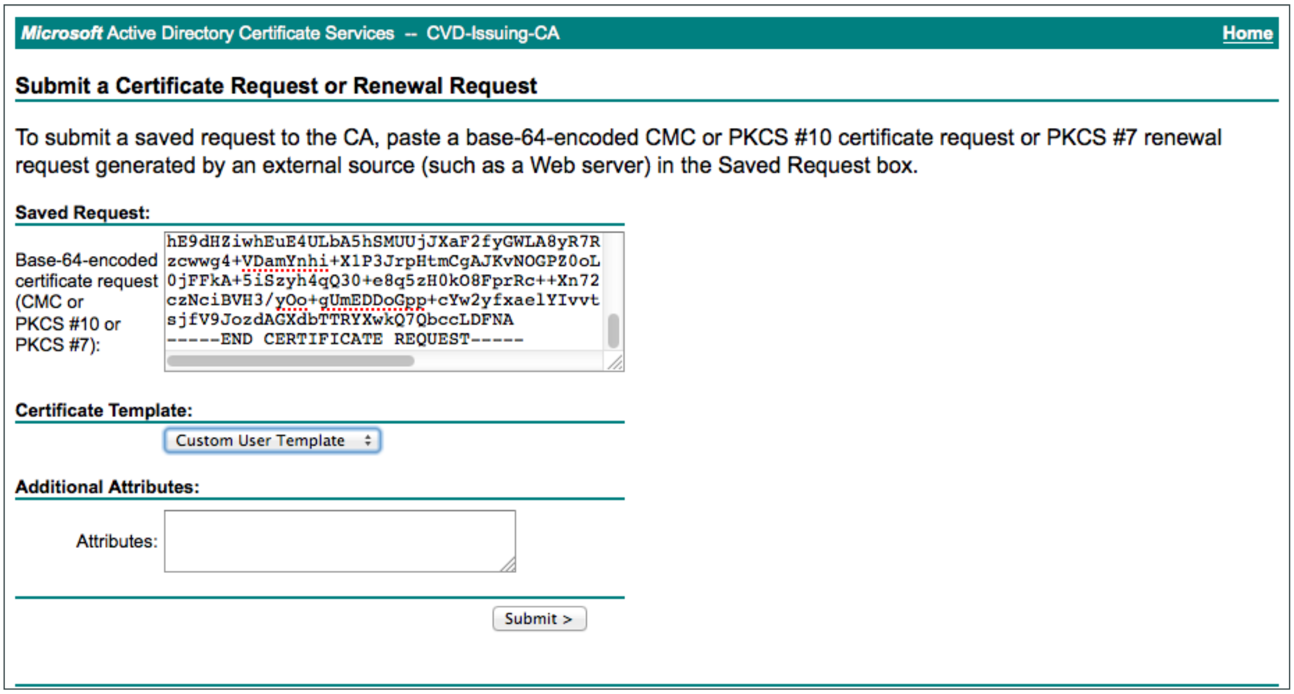
Step 7: Click the option that starts with **Submit a certificate request by use a base-64-encoded CMC or PKCS #10 file**.

Step 8: In a text editor, such as TextEdit, open the certificate request file saved in Step 3.

Step 9: Select all the text, and then copy it to the clipboard.

Step 10: In the browser, on the Submit a Certificate Request or Renewal Request page, in the **Saved Request** box, paste the certificate contents.

Step 11: In the **Certificate Template** list, choose **Custom User**, and then click **Submit**.



Microsoft Active Directory Certificate Services -- CVD-Issuing-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
hE9dHZiwhEuE4ULbA5hSMUUjJXaF2fyGWLA8yR7R
zcwwg4+VDamYnhi+X1P3JrpHtmCgAJKvNOGPZ0oL
0jFFkA+5iSzyh4qQ30+e8q5zH0kO8FprRc++Xn72
czNciBVH3/yOo+gUmEDDoGpp+cYw2yfxaelYIvvt
sjfV9JozdAGXdbTTRYXwkQ7QbccLDFNA
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Custom User Template

Additional Attributes:

Attributes:

Step 12: Select **DER encoded**, and then click **Download certificate**. This saves the certificate.

Step 13: In Finder, locate the saved certificate, and then double-click it. The Keychain Access utility imports the certificate.

Configure Mac OS X Supplicant

When accessing an 802.1X enabled network, Mac OS X will prompt you for a username and password. You will be connected to the network using PEAP and this will be stored in a configuration profile. To configure the 802.1X to use certificates and EAP-TLS in Mac OS X, you manually create a configuration profile. This process is documented in detail in the white paper 802.1X Authentication available from Apple.

Any device that doesn't have a certificate that wishes to use 802.1X will use PEAP to gain access to the network. Monitor mode is running on the wired network, so endpoints that aren't configured for 802.1X still get access by using MAC Authentication Bypass (MAB).

Enable Authorization

The network infrastructure is now configured for 8021.X authentication in monitor mode, and you have installed certificates on the endpoints and configured their 802.1X supplicants. Upon successful authentication, the endpoint is granted full network access. However, monitor mode allows for endpoints that fail 802.1X to access the network using MAB. This is a good point in the deployment to stop to verify that certificates are deployed to all endpoints and supplicants are configured correctly without impacting the users' network connectivity. You can monitor the logs to determine who is failing authentication and then correct those issues.

The next step is to deploy authorization to control network access from authenticated endpoints. The initial authorization deployment uses low-impact mode. In low-impact mode, endpoints are authenticated with either 802.1X or MAB. MAB is used for devices that require network access but either don't support 802.1X or don't have 802.1X configured. In this example, we are using MAB to authenticate IP phones and wireless access points that we identify with device profiling. Any other device has to successfully authenticate with 802.1X, or it will not have access to the network. After authentication, the endpoint is given full access to the network, but prior to authentication, the endpoint only has access to the services necessary for authentication.

PROCESS

Enabling Authorization for Wireless Access Points

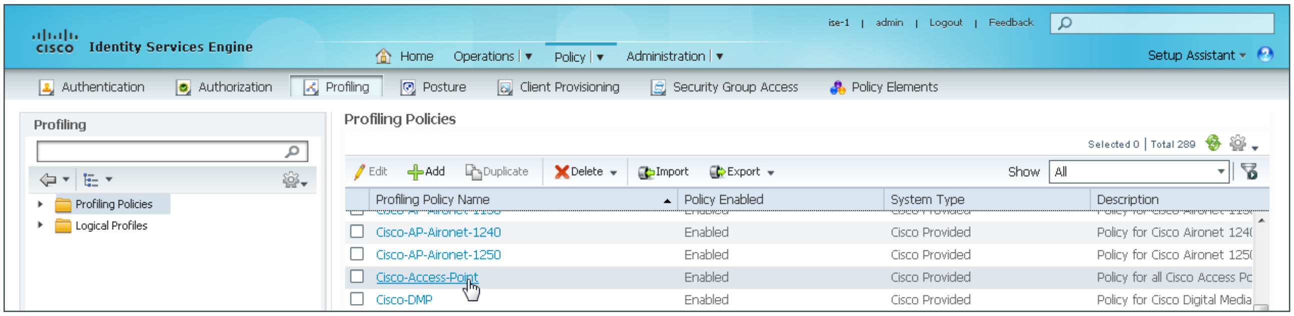
1. Create an identity group
2. Create authorization profile
3. Create authorization policy

You create an authorization profile for wireless access points (APs) that is similar to the one for Cisco IP Phones, which authorizes all traffic.

Procedure 1 Create an identity group

Step 1: In Cisco ISE, on the main menu bar, navigate to **Policy > Profiling**.

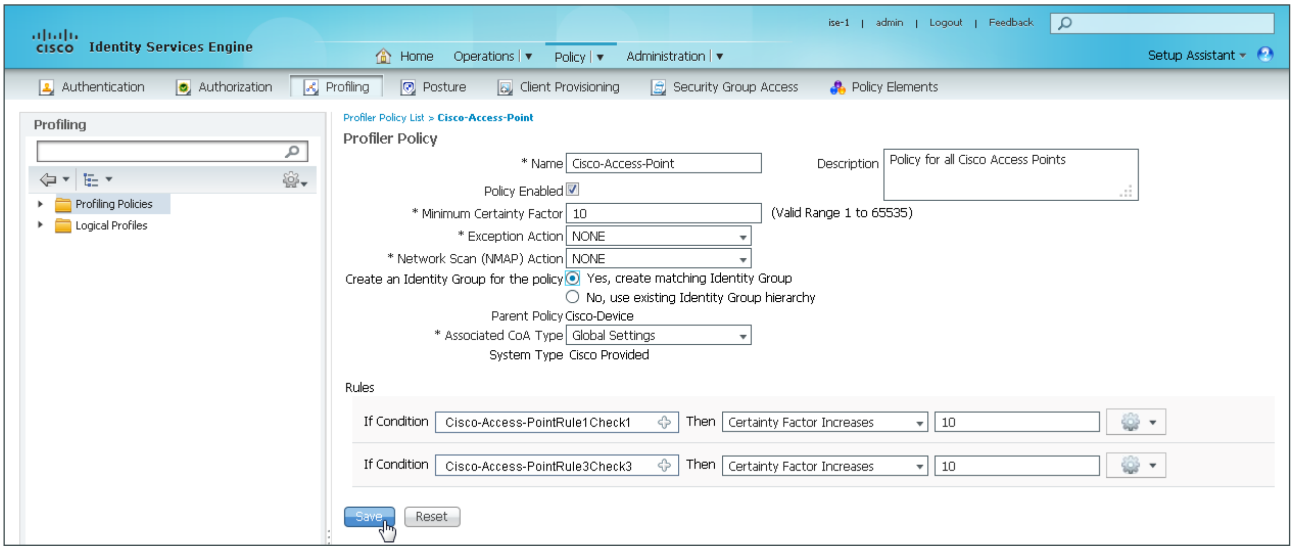
Step 2: In the left pane, verify that the Profiling Policies folder is selected.



Profiling Policy Name	Policy Enabled	System Type	Description
Cisco-AP-Aironet-1240	Enabled	Cisco Provided	Policy for Cisco Aironet 124
Cisco-AP-Aironet-1250	Enabled	Cisco Provided	Policy for Cisco Aironet 125
Cisco-Access-Point	Enabled	Cisco Provided	Policy for all Cisco Access P
Cisco-DMP	Enabled	Cisco Provided	Policy for Cisco Digital Media

Step 3: In the main Profiling Policies list in the Profiling Policy Name column, choose **Cisco-Access-Point**.

Step 4: In the Profiler Policy, for Create an Identity Group for the policy, select **Yes, create matching Identity Group**, and then click **Save**.



Profiler Policy

* Name Cisco-Access-Point
Description Policy for all Cisco Access Points
Policy Enabled ☑
* Minimum Certainty Factor 10 (Valid Range 1 to 65535)
* Exception Action NONE
* Network Scan (NMAP) Action NONE
Create an Identity Group for the policy ● Yes, create matching Identity Group
○ No, use existing Identity Group hierarchy
Parent Policy Cisco-Device
* Associated CoA Type Global Settings
System Type Cisco Provided

Rules

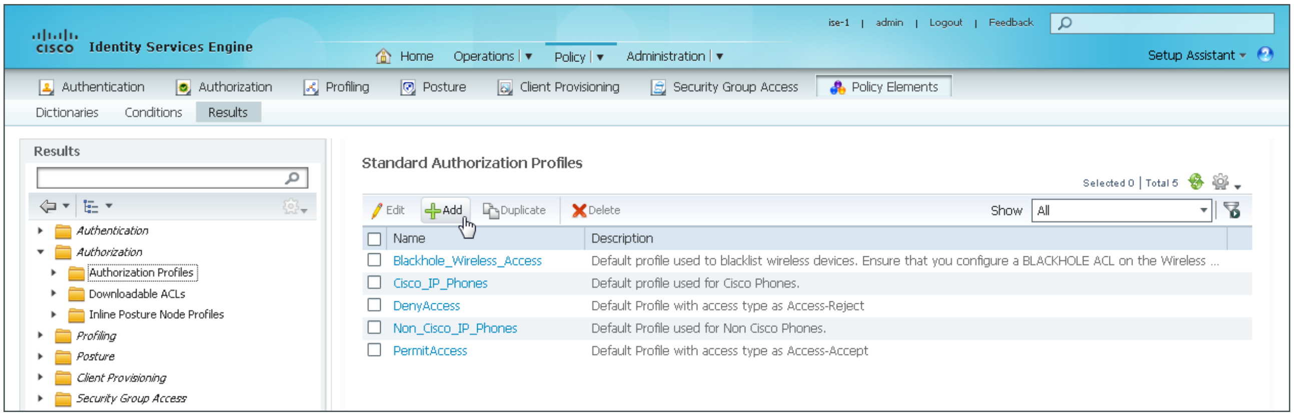
If Condition Cisco-Access-PointRule1Check1 Then Certainty Factor Increases 10
If Condition Cisco-Access-PointRule3Check3 Then Certainty Factor Increases 10

Procedure 2 Create authorization profile

An authorization profile defines the specific access policies granted to the device. You create a policy for access points to permit full access. Although there is already a similar built-in profile, creating a new one allows you to modify the policy if you choose to make a more restrictive policy in the future.

Step 1: In Cisco ISE, on the main menu bar, navigate to **Policy > Policy Elements > Results**.

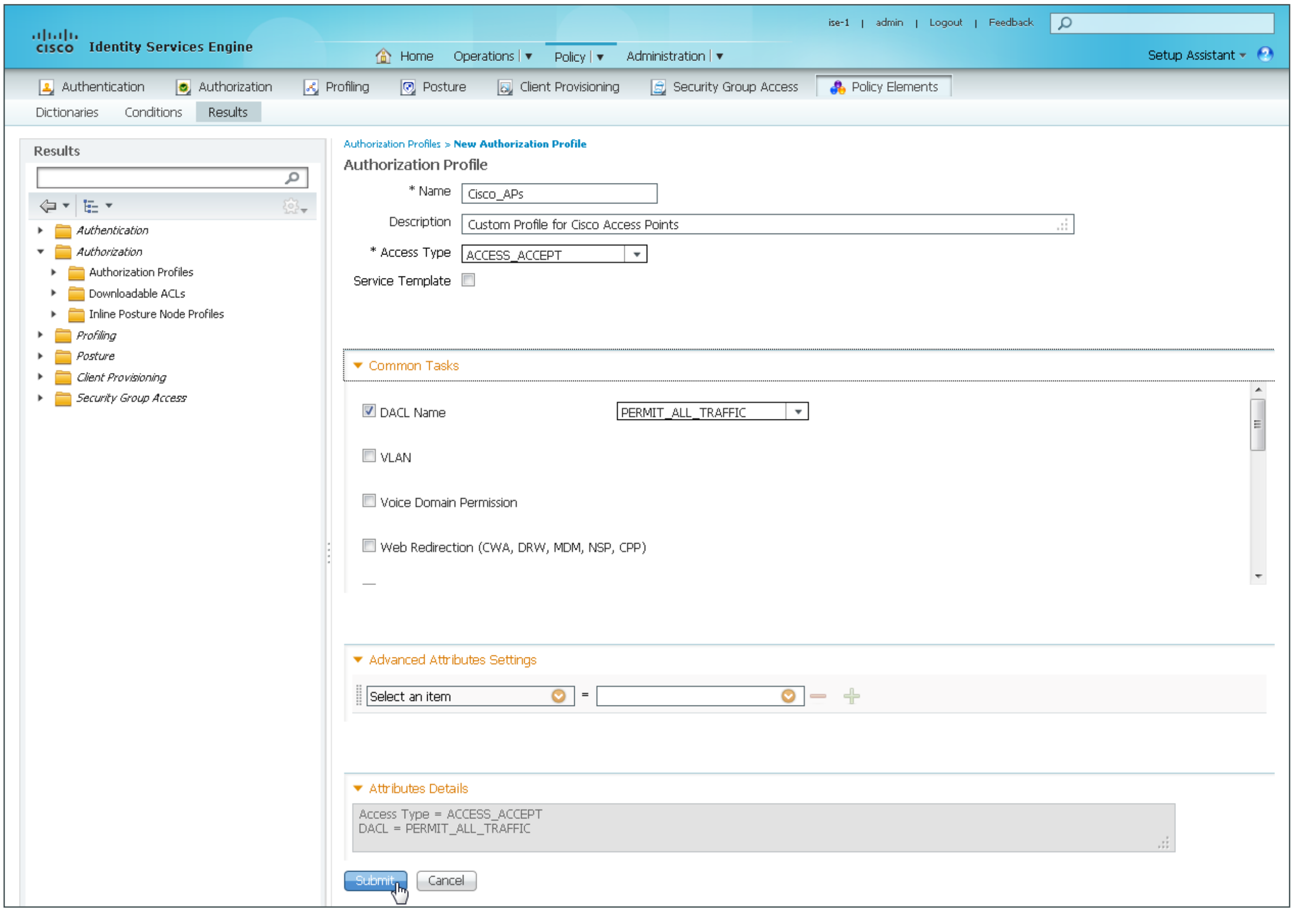
Step 2: In the left pane, navigate to **Authorization** > **Authorization Profiles**, next to the folder icon click the **Authorization Profiles** text, and then in the main Standard Authorization Profiles pane, click **Add**.


Identity Services Engine
ise-1 | admin | Logout | Feedback
Home Operations Policy Administration
Setup Assistant
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Dictionaries Conditions Results
Results
Authentication
Authorization
Authorization Profiles
Downloadable ACLs
Inline Posture Node Profiles
Profiling
Posture
Client Provisioning
Security Group Access
Selected 0 | Total 5
Edit Add Duplicate Delete
Show All

Standard Authorization Profiles

Name	Description
Blackhole_Wireless_Access	Default profile used to blacklist wireless devices. Ensure that you configure a BLACKHOLE ACL on the Wireless ...
Cisco_IP_Phones	Default profile used for Cisco Phones.
DenyAccess	Default Profile with access type as Access-Reject
Non_Cisco_IP_Phones	Default Profile used for Non Cisco Phones.
PermitAccess	Default Profile with access type as Access-Accept

Step 3: In the Authorization Profile, in the **Name** box, enter **Cisco_Aps**.


Identity Services Engine
ise-1 | admin | Logout | Feedback
Home Operations Policy Administration
Setup Assistant
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Dictionaries Conditions Results
Results
Authentication
Authorization
Authorization Profiles
Downloadable ACLs
Inline Posture Node Profiles
Profiling
Posture
Client Provisioning
Security Group Access
Authorization Profiles > New Authorization Profile
Advanced Attributes Settings
Select an item
Submit
Cancel

Authorization Profile

* Name: Cisco_APs

Description: Custom Profile for Cisco Access Points

* Access Type: ACCESS_ACCEPT

Service Template ☐

Common Tasks

☑ DACL Name: PERMIT_ALL_TRAFFIC

☐ VLAN

☐ Voice Domain Permission

☐ Web Redirection (CWA, DRW, MDM, NSP, CPP)

Attributes Details

Access Type = ACCESS_ACCEPT
DACL = PERMIT_ALL_TRAFFIC

Step 4: Enter a Description.

Step 5: Select **DACL Name**.

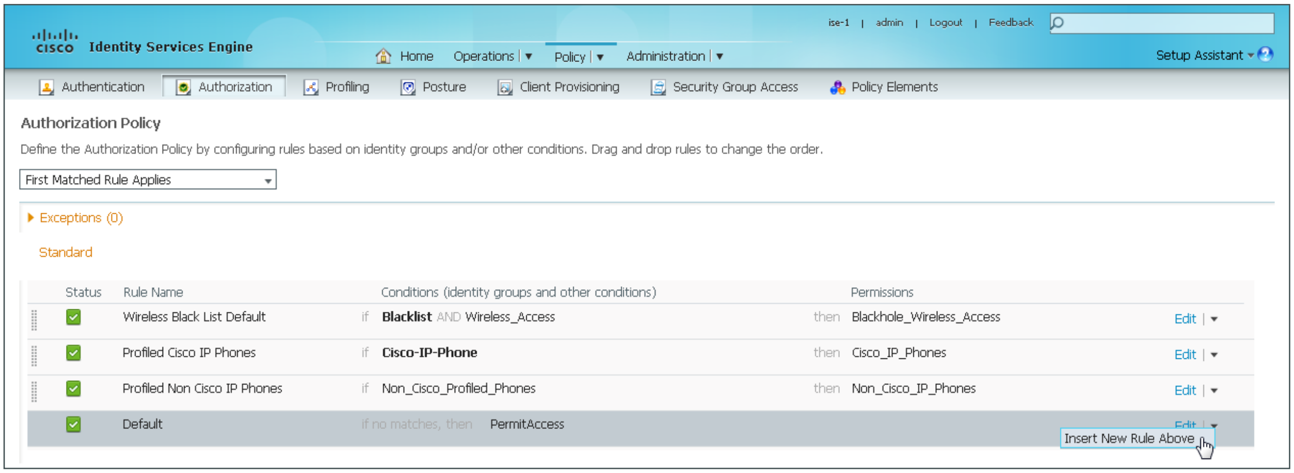
Step 6: In the **DACL Name** list, select **PERMIT_ALL_TRAFFIC**, and then click **Submit**.

The **Cisco_APs** profile is added to the list of standard authorization profiles.

Procedure 3 Create authorization policy

Step 1: In Cisco ISE, on the main menu bar, navigate to **Policy > Authorization**.

Step 2: For the Default rule, on the right, click the black triangle symbol, and then select **Insert New Rule Above**. A new rule named **Standard Rule 1** is created.

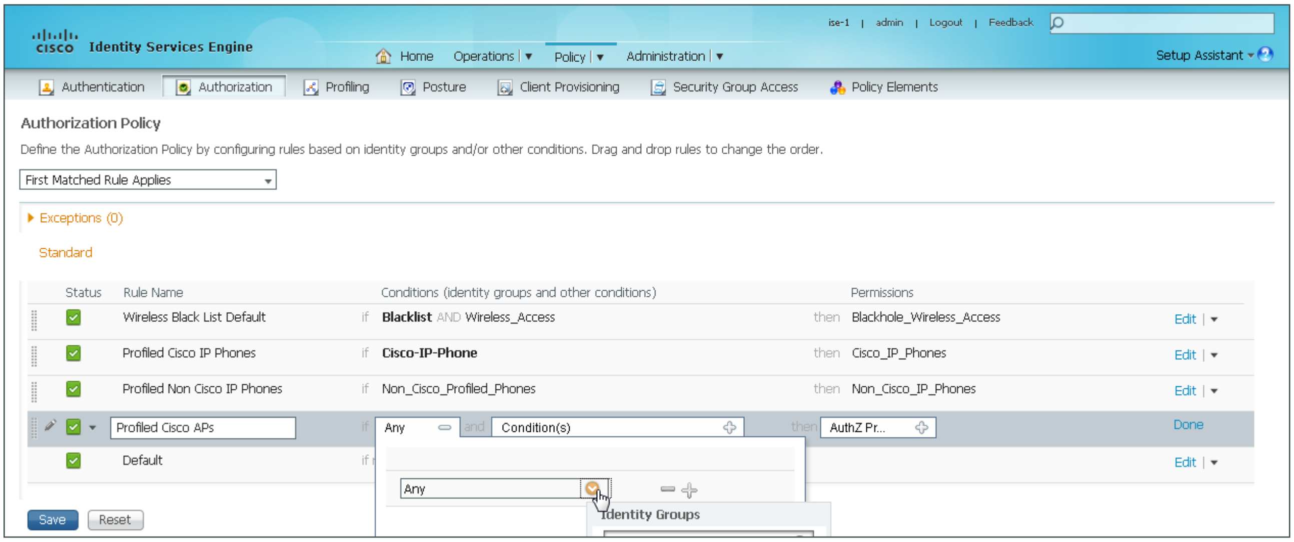


cisco Identity Services Engine
ise-1 | admin | Logout | Feedback
Home Operations | ▾ Policy | ▾ Administration | ▾
Setup Assistant ▾
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Authorization Policy
Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.
First Matched Rule Applies
Exceptions (0)
Standard
Insert New Rule Above

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
✓	Wireless Black List Default	if	**Blacklist** AND Wireless_Access	then	Blackhole_Wireless_Access	Edit | ▾
✓	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones	Edit | ▾
✓	Profiled Non Cisco IP Phones	if	Non_Cisco_Profiled_Phones	then	Non_Cisco_IP_Phones	Edit | ▾
✓	Default	if no matches, then	PermitAccess			Edit | ▾

Step 3: Rename the newly created rule **Profiled Cisco APs**.

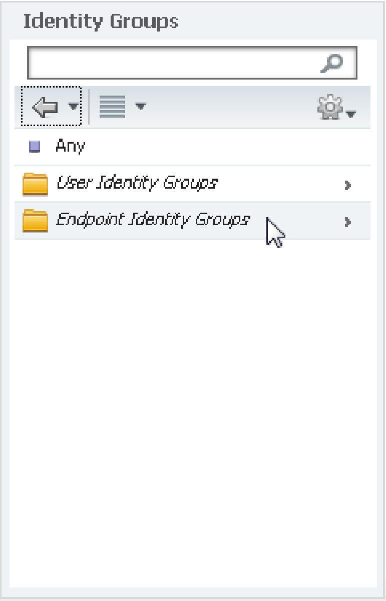
Step 4: In the Conditions column, next to **Any**, click the **+** symbol. A selection box opens.

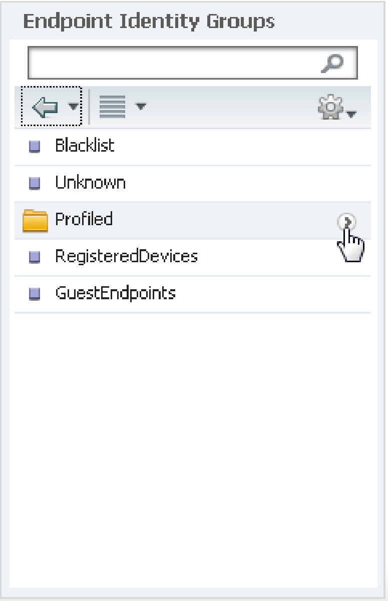


cisco Identity Services Engine
ise-1 | admin | Logout | Feedback
Home Operations | ▾ Policy | ▾ Administration | ▾
Setup Assistant ▾
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Authorization Policy
Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.
First Matched Rule Applies
Exceptions (0)
Standard
Any
Identity Groups
Save
Reset

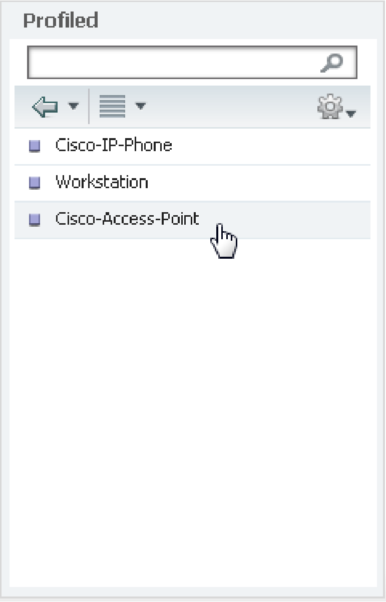
Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
✓	Wireless Black List Default	if	**Blacklist** AND Wireless_Access	then	Blackhole_Wireless_Access	Edit | ▾
✓	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones	Edit | ▾
✓	Profiled Non Cisco IP Phones	if	Non_Cisco_Profiled_Phones	then	Non_Cisco_IP_Phones	Edit | ▾
✓	Profiled Cisco APs	if	Any and Condition(s)	then	AuthZ Pr...	Done
✓	Default	if				Edit | ▾

Step 5: From the list, next to **Endpoint Identity Groups**, click the **>** symbol, and then next to Profiled, click the **>** symbol.



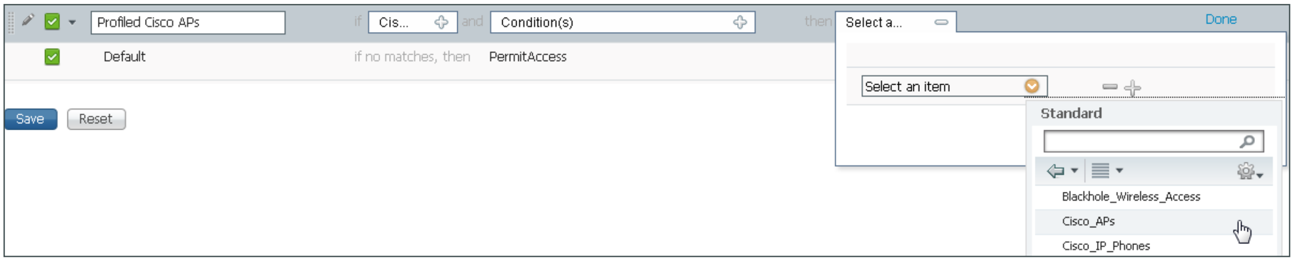


Step 6: Choose **Cisco-Access-Point**.

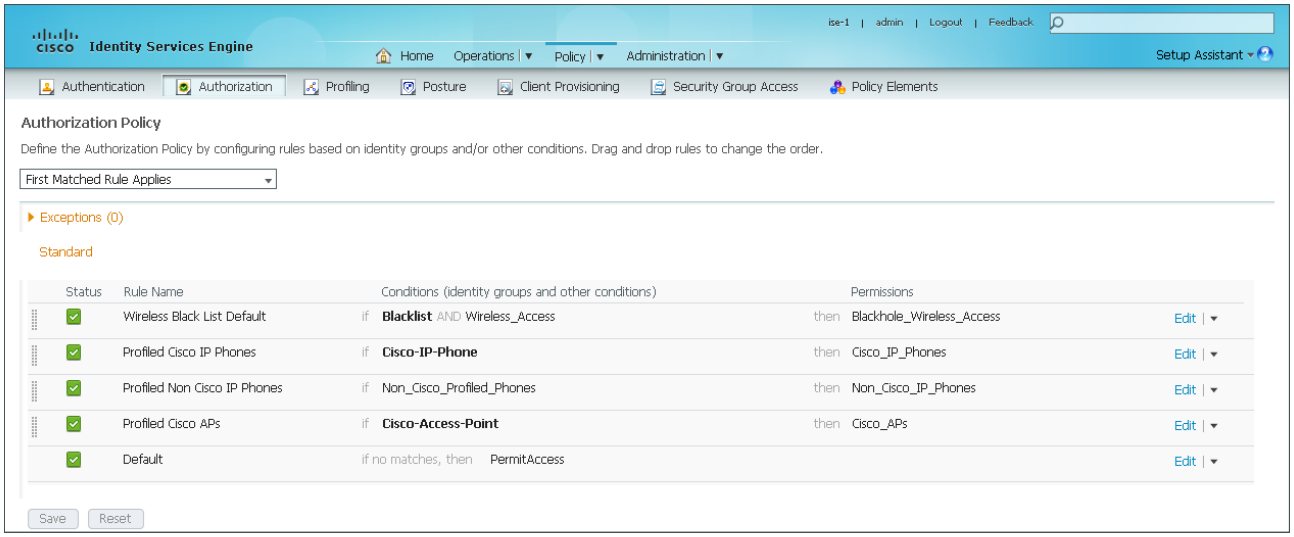


Step 7: Under the Permissions column, next to **AuthZ Profile**, click the **+** symbol.

Step 8: In the list, next to **Standard**, click the **>** symbol, and then choose **Cisco_APs**.



Step 9: On the rule, click **Done**, and then click **Save**. The updated Authorization Policy is displayed.



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)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
☑	Wireless Black List Default	if	**Blacklist** AND Wireless_Access	then	Blackhole_Wireless_Access	Edit | ▾
☑	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones	Edit | ▾
☑	Profiled Non Cisco IP Phones	if	Non_Cisco_Profiled_Phones	then	Non_Cisco_IP_Phones	Edit | ▾
☑	Profiled Cisco APs	if	**Cisco-Access-Point**	then	Cisco_APs	Edit | ▾
☑	Default	if no matches, then	PermitAccess			Edit | ▾

PROCESS

Modifying the MAB Authentication Policy

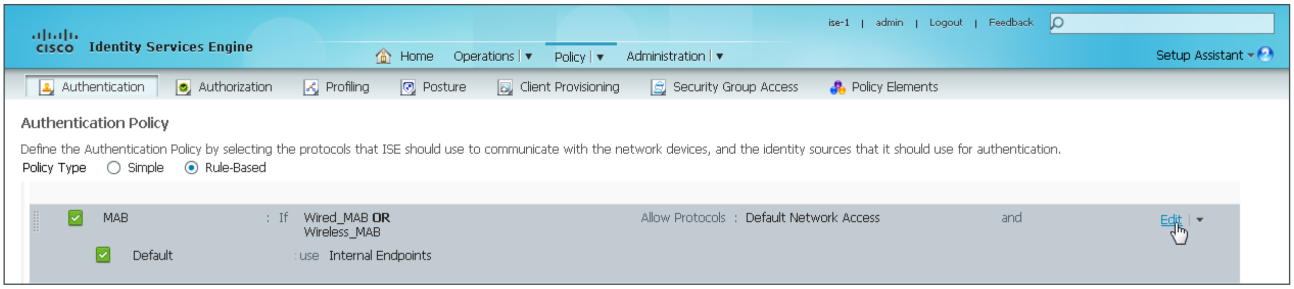
1. Modify MAB authentication rule

Because you have deployed monitor mode, the current MAB authentication policy allows endpoints access to the network even if they fail authentication. Now that you are implementing low-impact mode, you need to modify the MAB policy to reject endpoints that fail authentication. This change works with the authorization policies, which permit Cisco IP Phones and access points as the only devices authorized on the network without performing 802.1X authentication.

Procedure 1 Modify MAB authentication rule

Step 1: In Cisco ISE, on the main menu bar, navigate to **Policy** > **Authentication**.

Step 2: On the **MAB** rule, click **Edit**. This displays the identity store for this rule.



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

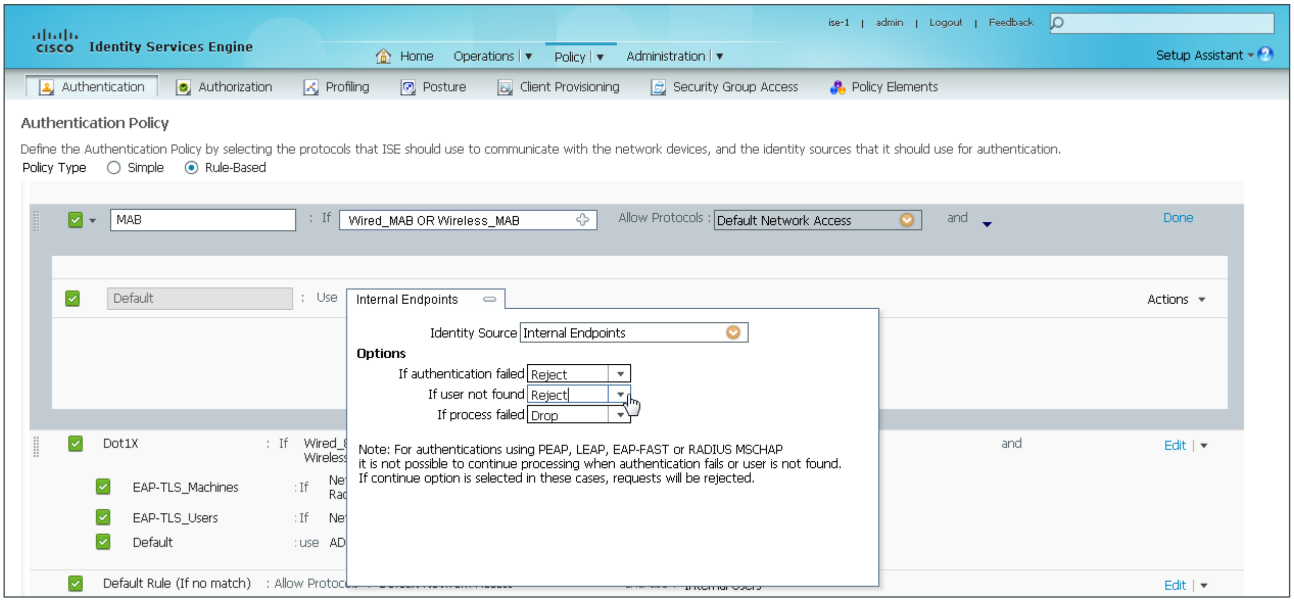
Policy Type ○ Simple ● Rule-Based

☑ MAB : If Wired_MAB OR Wireless_MAB Allow Protocols : Default Network Access and

☑ Default : use Internal Endpoints

Step 3: Next to Internal Endpoints, click the **+** symbol.

Step 4: In the **If authentication failed** and **If user not found** lists, choose **Reject**.



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type ○ Simple ● Rule-Based

☑ MAB : If Wired_MAB OR Wireless_MAB Allow Protocols : Default Network Access and

☑ Default : Use Internal Endpoints

Identity Source Internal Endpoints

Options

If authentication failed Reject

If user not found Reject

If process failed Drop

Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS MSCHAP it is not possible to continue processing when authentication fails or user is not found. If continue option is selected in these cases, requests will be rejected.

☑ Dot1X : If Wired_ Wireless and

☑ EAP-TLS_Machines : If Ne Rad

☑ EAP-TLS_Users : If Ne

☑ Default : use AD

☑ Default Rule (If no match) : Allow Protoco

Step 5: Click anywhere in the window to continue, and then click **Save**.

PROCESS

Enabling Authorization for Wired Endpoints

1. Create authorization profile
2. Create authorization policy
3. Enable low-impact mode and change of authorization

You enable authorization for wired endpoints that authenticate using digital certificates. At this stage, once authenticated, the endpoint is granted full access to the network. This policy can be modified if you choose a more restrictive policy in the future.

Procedure 1 Create authorization profile

An authorization profile defines the specific access policies granted to the device. You create a profile for wired endpoints to permit full access.

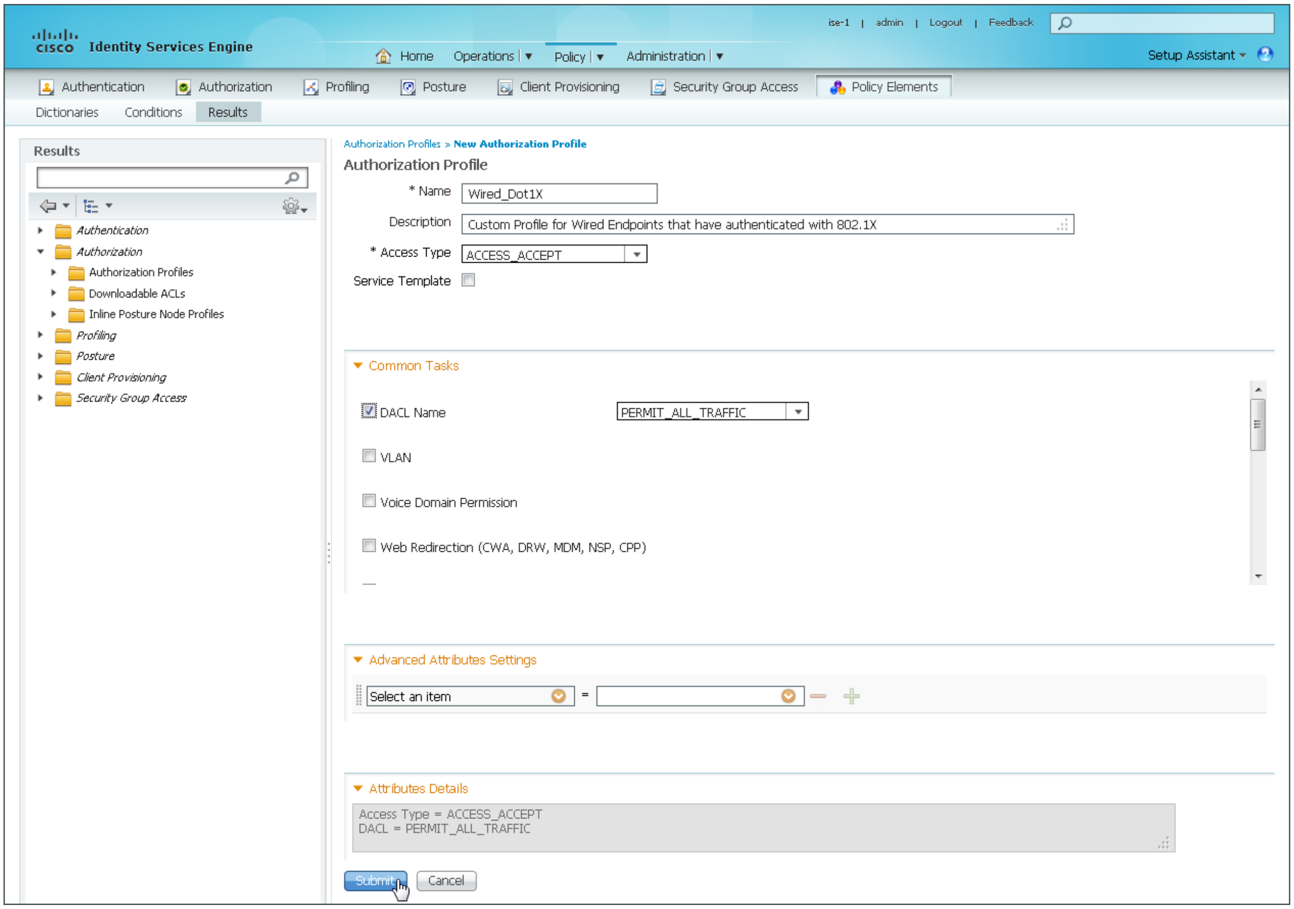
Step 1: In Cisco ISE, on the main menu bar, navigate to **Policy** > **Policy Elements** > **Results**.

Step 2: In left pane, navigate to **Authorization** > **Authorization Profiles.**

Step 3: Next to the folder icon, click the **Authorization Profiles** text.

Step 4: In the main Standard Authorization Profiles pane, click **Add**.

Step 5: In the Authorization Profile, add the Name **Wired_Dot1X.**



* Name: Wired_Dot1X

Description: Custom Profile for Wired Endpoints that have authenticated with 802.1X

* Access Type: ACCESS_ACCEPT

Service Template ☐

☑ DACL Name: PERMIT_ALL_TRAFFIC

☐ VLAN

☐ Voice Domain Permission

☐ Web Redirection (CWA, DRW, MDM, NSP, CPP)

Access Type = ACCESS_ACCEPT
DACL = PERMIT_ALL_TRAFFIC

Step 6: Add a Description.

Step 7: Select **DACL Name.**

Step 8: In the **DACL Name** list, select **PERMIT_ALL_TRAFFIC**, and then click **Submit**.

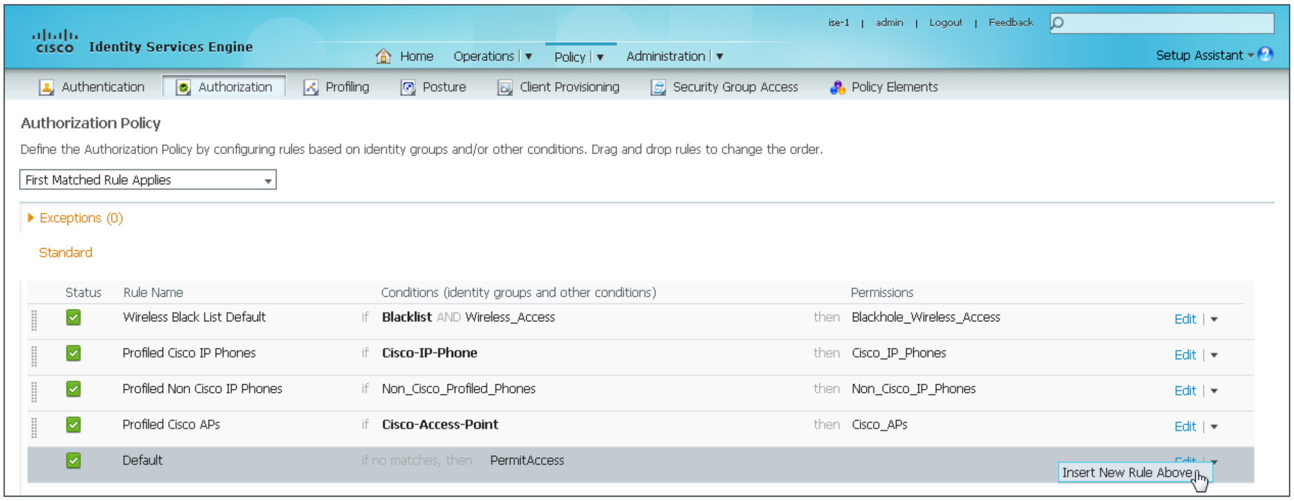
The **Wired_Dot1X** profile is added to the list of standard authorization profiles.

Procedure 2 Create authorization policy

Now you need to define an authorization policy for wired endpoints and apply the authorization profile.

Step 1: In Cisco ISE, on the main menu bar, navigate to **Policy > Authorization**.

Step 2: For the Default rule, on the right, click the black triangle symbol, and then select **Insert New Rule Above**. A new rule named **Standard Rule 1** is created.



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 ▾

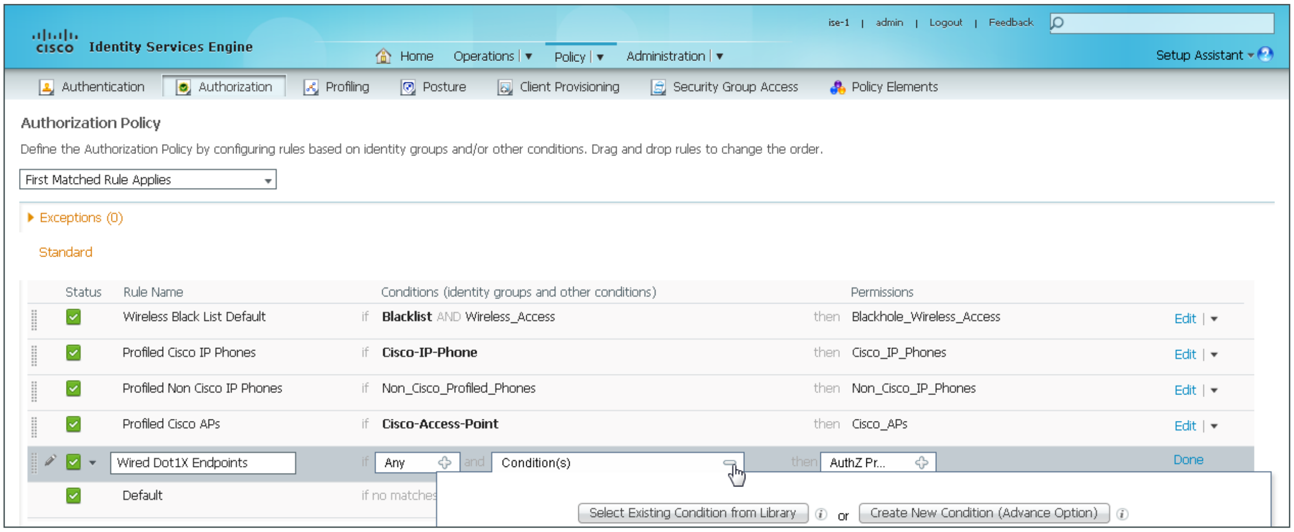
▸ Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions	
☑	Wireless Black List Default	if **Blacklist** AND Wireless_Access	then Blackhole_Wireless_Access	Edit | ▾
☑	Profiled Cisco IP Phones	if **Cisco-IP-Phone**	then Cisco_IP_Phones	Edit | ▾
☑	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones	Edit | ▾
☑	Profiled Cisco APs	if **Cisco-Access-Point**	then Cisco_APs	Edit | ▾
☑	Default	if no matches, then PermitAccess		Insert New Rule Above

Step 3: Rename the newly created rule **Wired Dot1X Endpoints.**

Step 4: In the **Conditions** column, next to **Condition(s)**, click the **+** symbol. A selection box opens.



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)

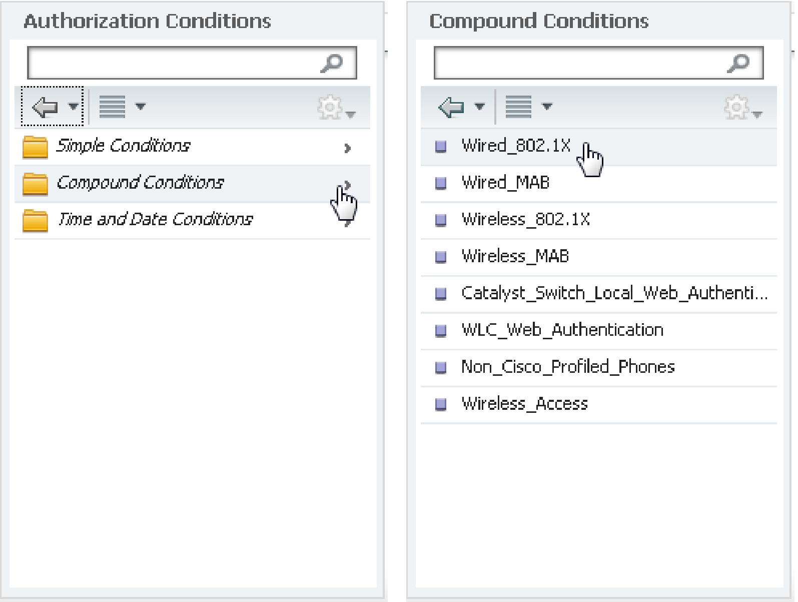
Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions	
☑	Wireless Black List Default	if **Blacklist** AND Wireless_Access	then Blackhole_Wireless_Access	Edit | ▾
☑	Profiled Cisco IP Phones	if **Cisco-IP-Phone**	then Cisco_IP_Phones	Edit | ▾
☑	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones	Edit | ▾
☑	Profiled Cisco APs	if **Cisco-Access-Point**	then Cisco_APs	Edit | ▾
☑ ▾	Wired Dot1X Endpoints	if Any and Condition(s)	then AuthZ Pr...	Done
☑	Default	if no matches		

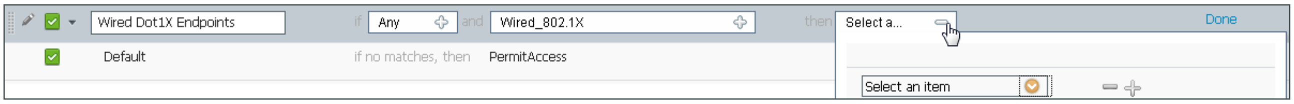
Select Existing Condition from Library
or
Create New Condition (Advance Option)

Step 5: Click **Select Existing Condition from Library**.

Step 6: In the Authorizations Conditions list, select **Compound Conditions**, click the **>** symbol, and then choose **Wired_802.1X**.

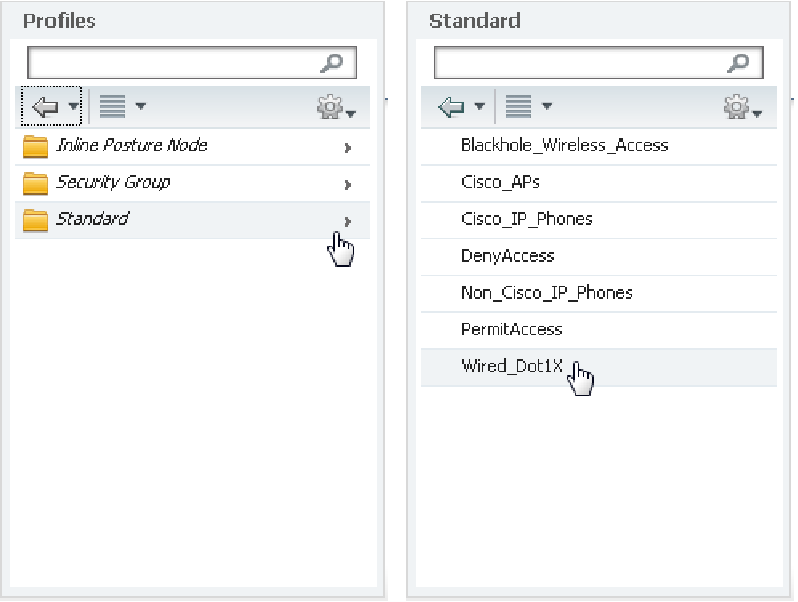


Step 7: Under the **Permissions** column, next to **AuthZ Profile**, click the **+** symbol. A selection box appears.

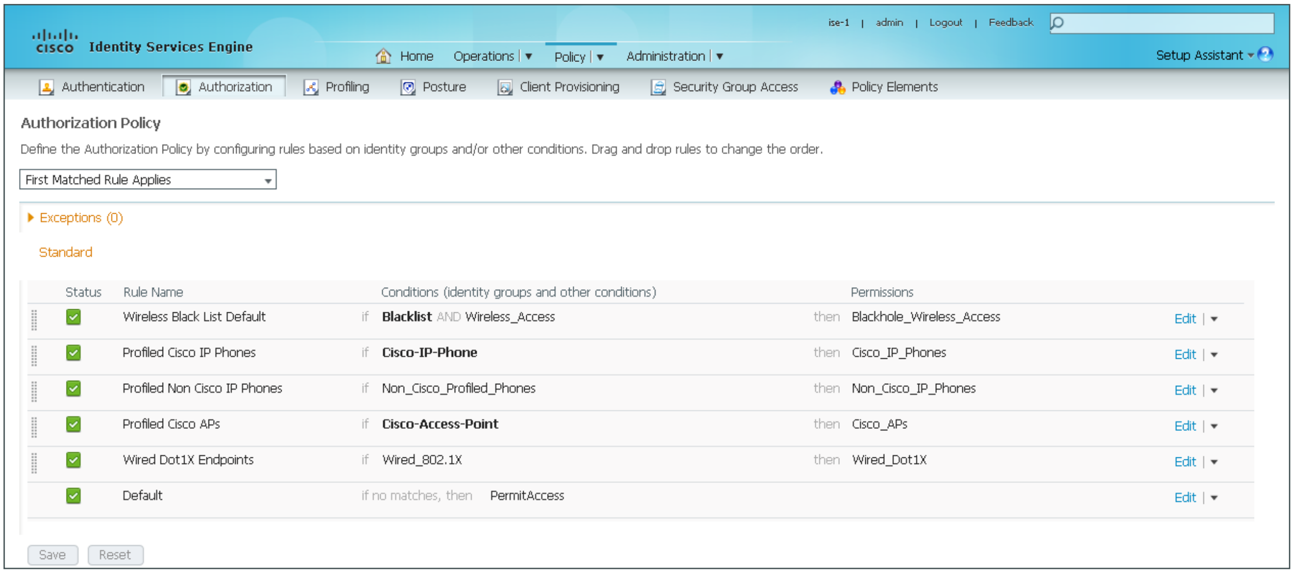

☑ Wired Dot1X Endpoints if Any and Wired_802.1X then Select a...

☑ Default if no matches, then PermitAccess

Step 8: In the **Select an item** list, select **Standard**, and then choose **Wired_Dot1X**.



Step 9: Click **Done**, and then click **Save**. The updated Authorization Policy is displayed.



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)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
☑	Wireless Black List Default	if	**Blacklist** AND Wireless_Access	then	Blackhole_Wireless_Access	Edit | ▾
☑	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones	Edit | ▾
☑	Profiled Non Cisco IP Phones	if	Non_Cisco_Profiled_Phones	then	Non_Cisco_IP_Phones	Edit | ▾
☑	Profiled Cisco APs	if	**Cisco-Access-Point**	then	Cisco_APs	Edit | ▾
☑	Wired Dot1X Endpoints	if	Wired_802.1X	then	Wired_Dot1X	Edit | ▾
☑	Default	if no matches, then	PermitAccess			Edit | ▾

Procedure 3 Enable low-impact mode and change of authorization

You now use the IOS CLI to configure the access switches for low-impact mode 802.1X.

You create an access list to limit traffic that is permitted on a port before it is authenticated, to allow only the traffic that is required for the port to go through the authentication process. Permitted traffic typically includes DHCP, DNS, TFTP for Preboot Execution Environment, and access to the AD domain controller. For troubleshooting, you also allow ICMP echo and echo-reply traffic. The list denies all other traffic.

Authorization requires the use of RADIUS Change of Authorization (CoA) in order to change the state of the port after authentication. This is not enabled by default, so you enable it.

On every access switch, perform the following configurations.

Step 1: Enable device tracking. Device tracking populates the dynamically learned IP address into the downloadable ACL.

```
ip device tracking
```

Step 2: Create an access list in order to restrict traffic before authentication.

```
ip access-list extended PreAuth
  remark Pre-authorization ACL customized for deployed environment
  permit ip any host 10.4.48.10
  permit udp any eq bootpc any eq bootps
  permit udp any any eq domain
  permit udp any any eq tftp
  permit icmp any any echo
  permit icmp any any echo-reply
  deny ip any any
```

Step 3: Enable RADIUS CoA.

```
aaa server radius dynamic-author
  client 10.4.48.43 server-key [radius key]
  client 10.4.48.44 server-key [radius key]
  auth-type any
```

Step 4: Apply authentication commands to the range of host interfaces.

```
interface range [interface type] [port number]-[port number]
 ip access-group PreAuth in
 authentication host-mode multi-domain
```

PROCESS

Enabling Authorization for Wireless Endpoints

1. Create authorization profile
2. Create authorization policy

You now enable authorization for wireless endpoints that authenticate using digital certificates. Once authenticated, the endpoint is granted full access to the network. This policy can be modified if you choose a more restrictive policy in the future.

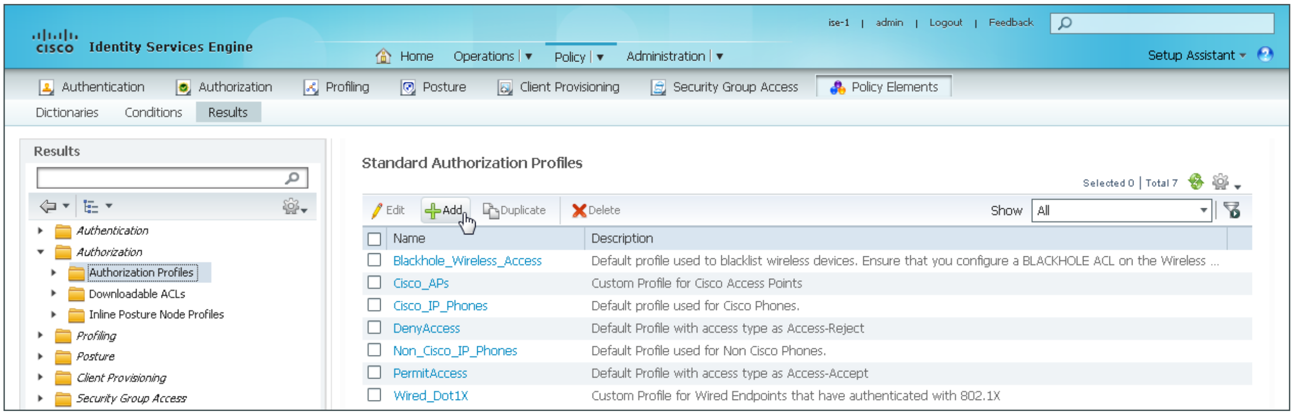
Procedure 1 Create authorization profile

An authorization profile defines the specific access policies granted to the device. You create a policy for wireless endpoints to permit full access. By default, a client is given full access when joining the wireless network, so you do not need to define an access list now.

Step 1: In a browser, access the primary Cisco ISE GUI, **http://ise-1.cisco.local**, and then on the main menu bar, navigate to **Policysection, > Policy Elements > Results**.

Step 2: In the left pane, navigate to **Authorization > Authorization Profiles.**

Step 3: Next to the folder icon, click the **Authorization Profiles** text, and then in the main Standard Authorization Profiles pane, click **Add**.



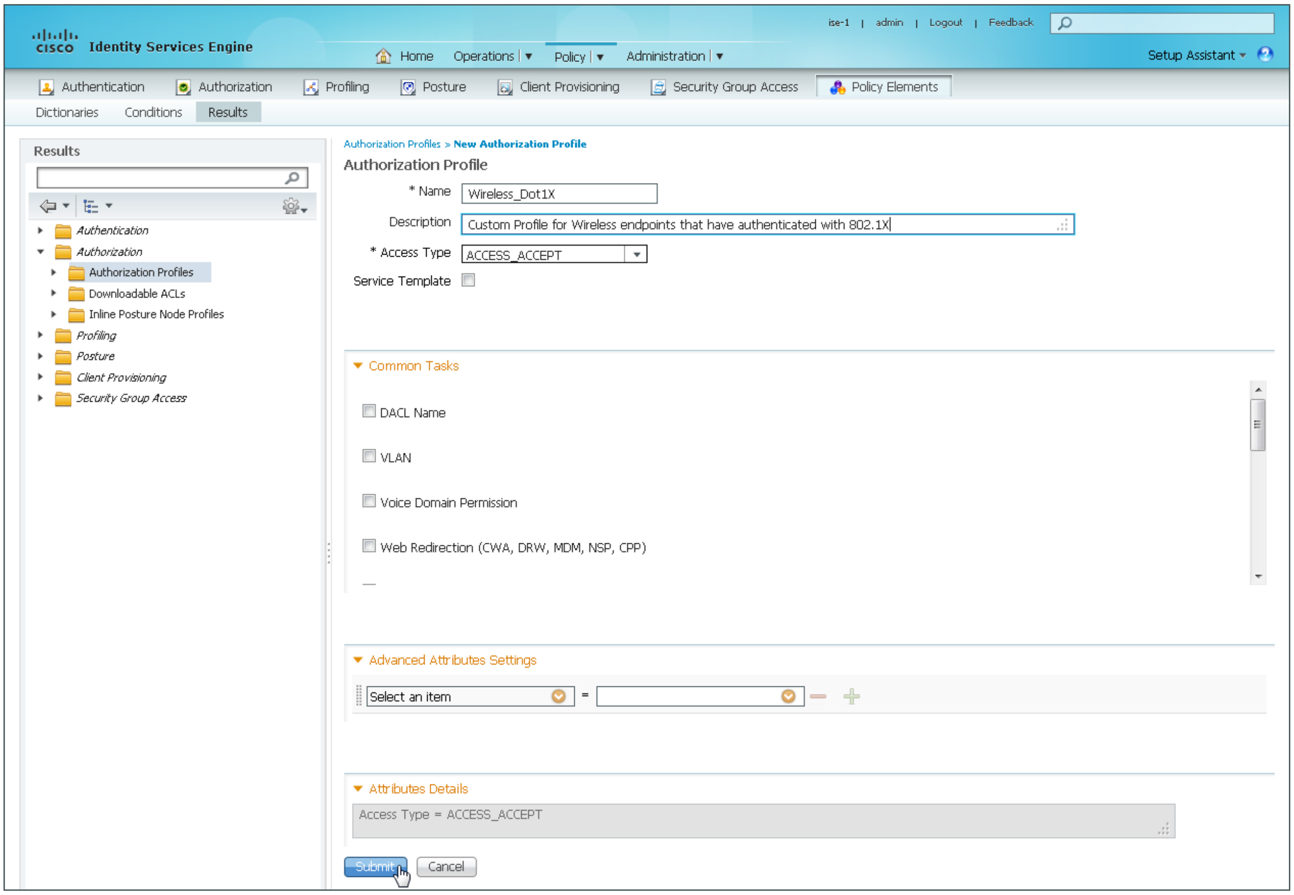
Standard Authorization Profiles

☐ Name	Description
☐ Blackhole_Wireless_Access	Default profile used to blacklist wireless devices. Ensure that you configure a BLACKHOLE ACL on the Wireless ...
☐ Cisco_APs	Custom Profile for Cisco Access Points
☐ Cisco_IP_Phones	Default profile used for Cisco Phones.
☐ DenyAccess	Default Profile with access type as Access-Reject
☐ Non_Cisco_IP_Phones	Default Profile used for Non Cisco Phones.
☐ PermitAccess	Default Profile with access type as Access-Accept
☐ Wired_Dot1X	Custom Profile for Wired Endpoints that have authenticated with 802.1X

Step 4: In the Authorization Profile, add the Name **Wireless_Dot1X**.

Step 5: Add a Description.

Step 6: In the **Access Type** list, verify that **ACCESS_ACCEPT** is selected, and then click **Submit**. The **Wireless_Dot1X** profile is added to the list of standard authorization profiles.



* Name: Wireless_Dot1X

Description: Custom Profile for Wireless endpoints that have authenticated with 802.1X

* Access Type: ACCESS_ACCEPT

Service Template: ☐

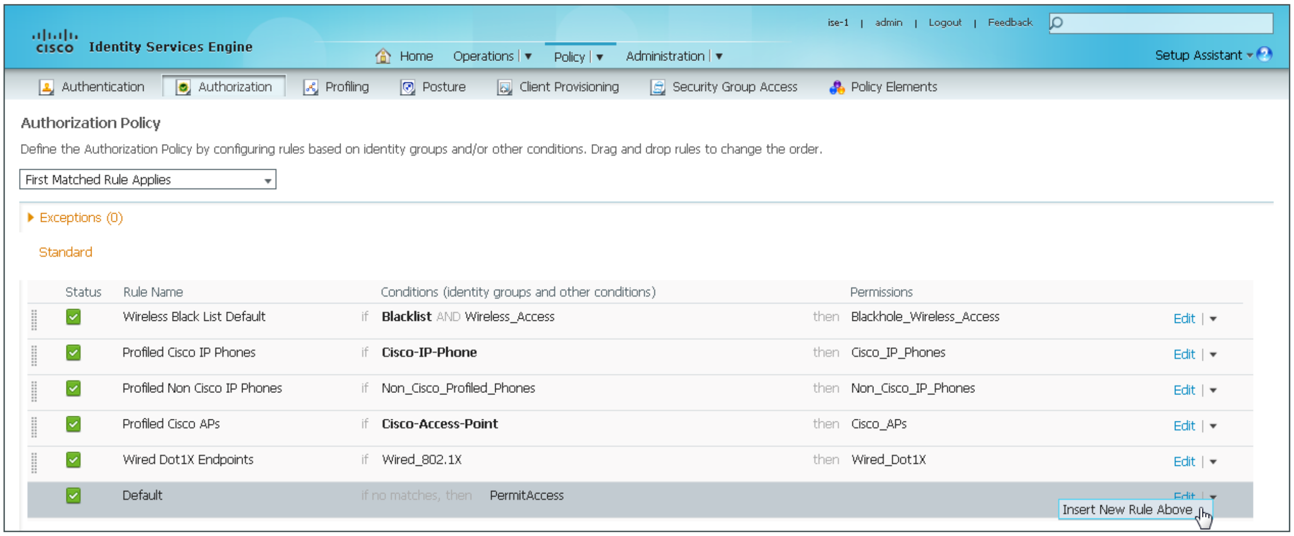
Attributes Details: Access Type = ACCESS_ACCEPT

Procedure 2 Create authorization policy

Now you need to define an authorization policy for wireless endpoints and apply the authorization profile.

Step 1: In Cisco ISE, on the main menu bar, navigate to **Policy > Authorization**.

Step 2: For the Default rule, on the right, click the black triangle symbol, and then select **Insert New Rule Above**. A new rule named **Standard Rule 1** is created.



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

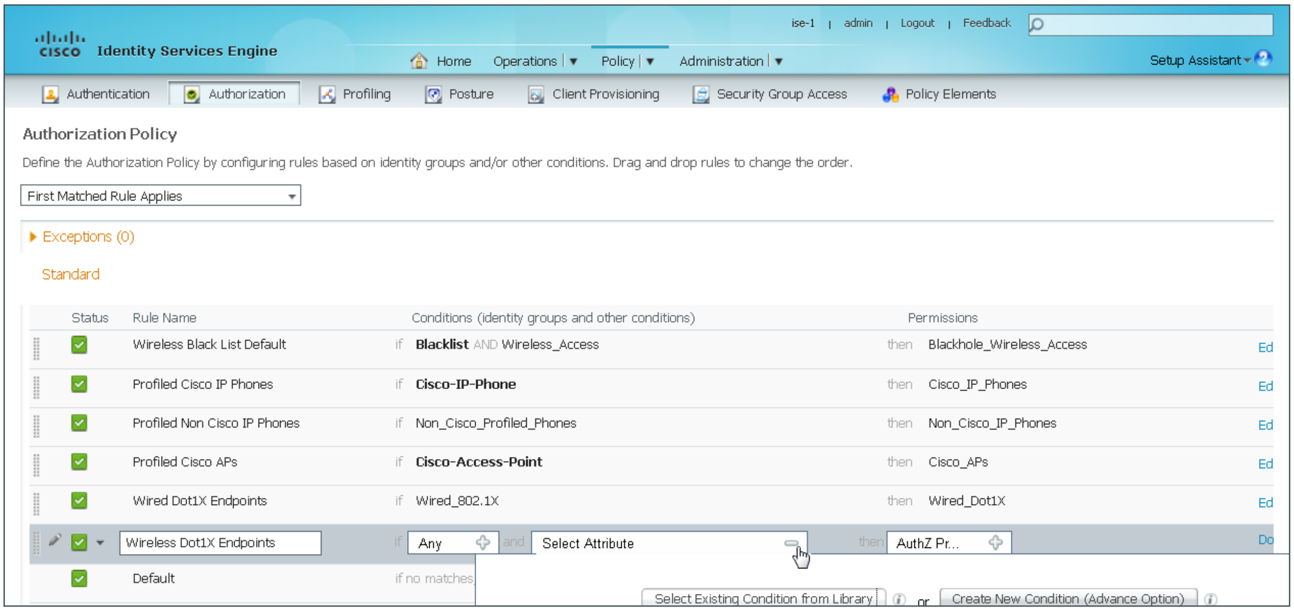
Exceptions (0)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
☑	Wireless Black List Default	if	**Blacklist** AND Wireless_Access	then	Blackhole_Wireless_Access	Edit | ▾
☑	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones	Edit | ▾
☑	Profiled Non Cisco IP Phones	if	Non_Cisco_Profiled_Phones	then	Non_Cisco_IP_Phones	Edit | ▾
☑	Profiled Cisco APs	if	**Cisco-Access-Point**	then	Cisco_APs	Edit | ▾
☑	Wired Dot1X Endpoints	if	Wired_802.1X	then	Wired_Dot1X	Edit | ▾
☑	Default	if no matches, then	PermitAccess			Edit | ▾

Step 3: Rename the rule **Wireless Dot1X Endpoints**.

Step 4: For the new rule, in the Conditions column, next to Condition(s), click the **+** symbol. A selection box opens.



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

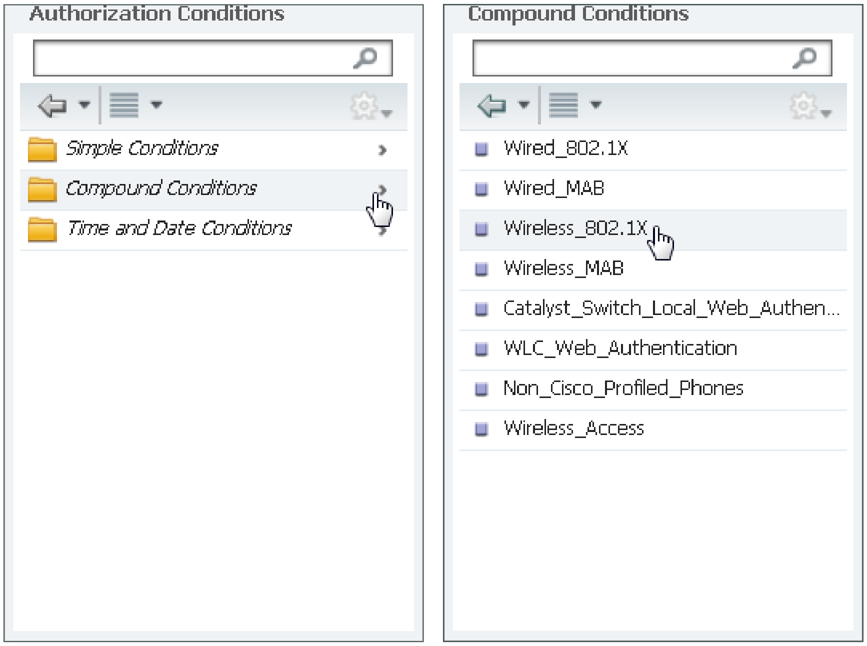
Exceptions (0)

Standard

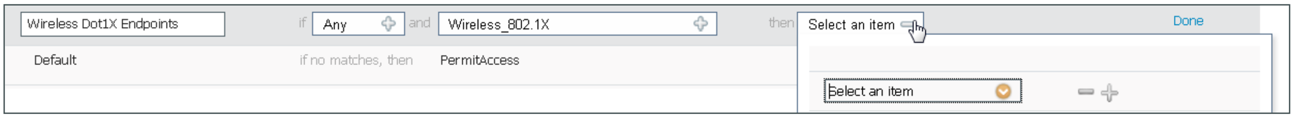
Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
☑	Wireless Black List Default	if	**Blacklist** AND Wireless_Access	then	Blackhole_Wireless_Access	Ed
☑	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones	Ed
☑	Profiled Non Cisco IP Phones	if	Non_Cisco_Profiled_Phones	then	Non_Cisco_IP_Phones	Ed
☑	Profiled Cisco APs	if	**Cisco-Access-Point**	then	Cisco_APs	Ed
☑	Wired Dot1X Endpoints	if	Wired_802.1X	then	Wired_Dot1X	Ed
☑	Wireless Dot1X Endpoints	if	Any and Select Attribute	then	AuthZ Pr...	Do
☑	Default	if no matches				

Step 5: Click **Select Existing Condition from Library**.

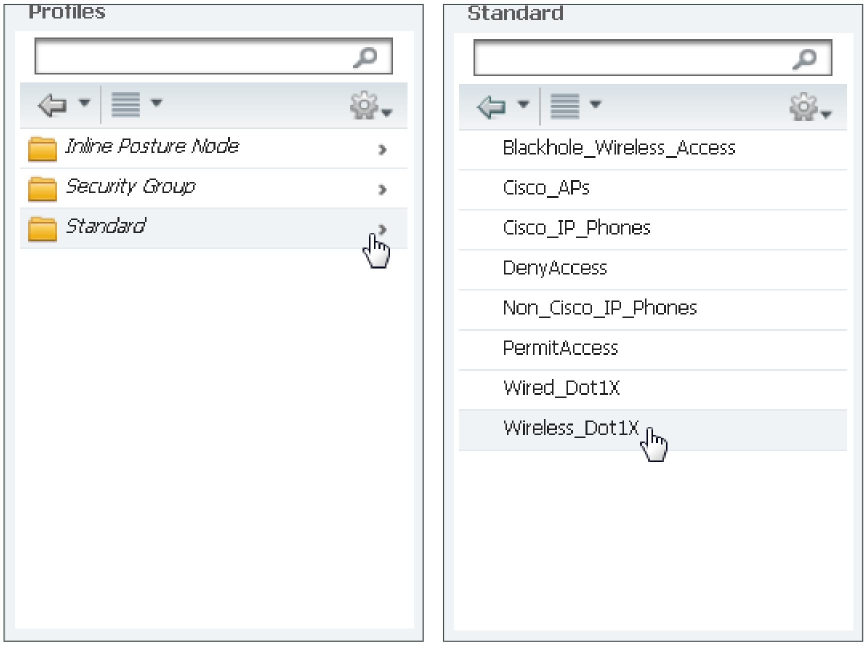
Step 6: In the Authorizations Conditions list, select Compound Conditions, and then choose **Wireless_802.1X**.



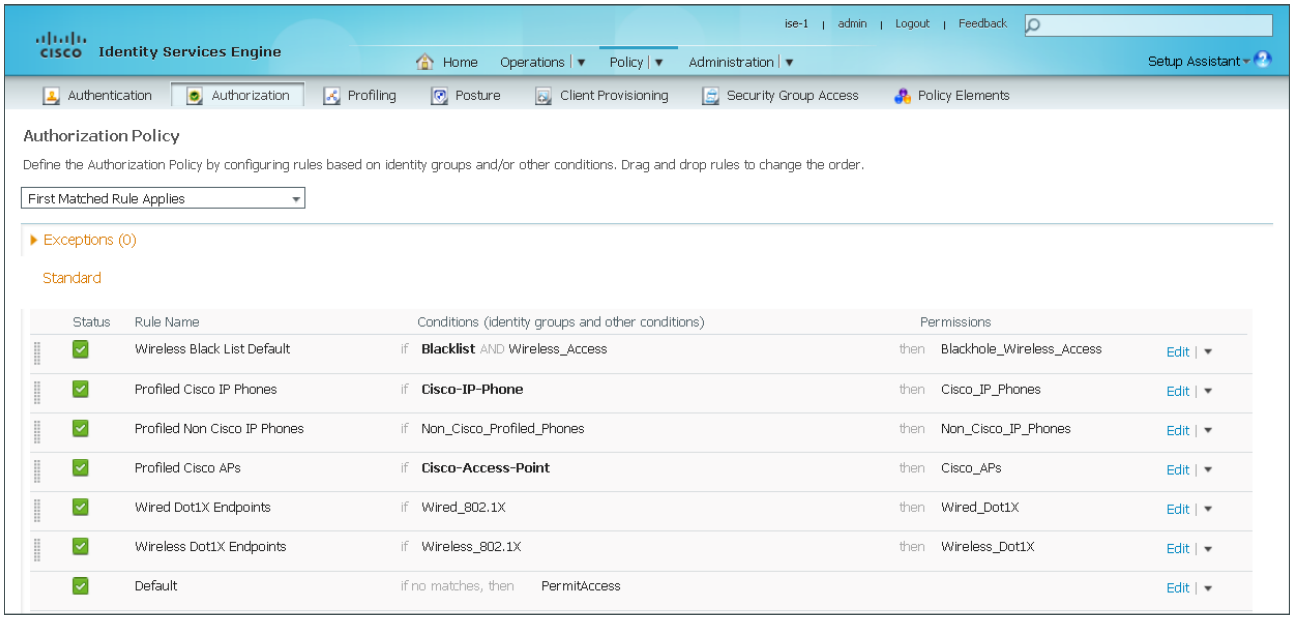
Step 7: Under the Permissions column, next to AuthZ Profile, click the **+** symbol. A selection box appears.



Step 8: In the Select Items list, select **Standard**, and then choose **Wireless_Dot1X**.



Step 9: Click **Done**, and then click **Save**. The updated Authorization Policy is displayed.



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)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
☑	Wireless Black List Default	if	**Blacklist** AND Wireless_Access	then	Blackhole_Wireless_Access	Edit | ▾
☑	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones	Edit | ▾
☑	Profiled Non Cisco IP Phones	if	Non_Cisco_Profiled_Phones	then	Non_Cisco_IP_Phones	Edit | ▾
☑	Profiled Cisco APs	if	**Cisco-Access-Point**	then	Cisco_APs	Edit | ▾
☑	Wired Dot1X Endpoints	if	Wired_802.1X	then	Wired_Dot1X	Edit | ▾
☑	Wireless Dot1X Endpoints	if	Wireless_802.1X	then	Wireless_Dot1X	Edit | ▾
☑	Default	if no matches, then	PermitAccess			Edit | ▾

PROCESS

Modifying the Authorization Policy to be Closed

1. Modify default rule

The authorization policy previously created is an open policy. The default rule at the end specifies that if an incoming authorization request doesn't match one of the specific rules defined, it permits access to the network. Because low-impact mode is enabled, you need to change this rule in order to deny access to any request that doesn't match one of the specific rules.

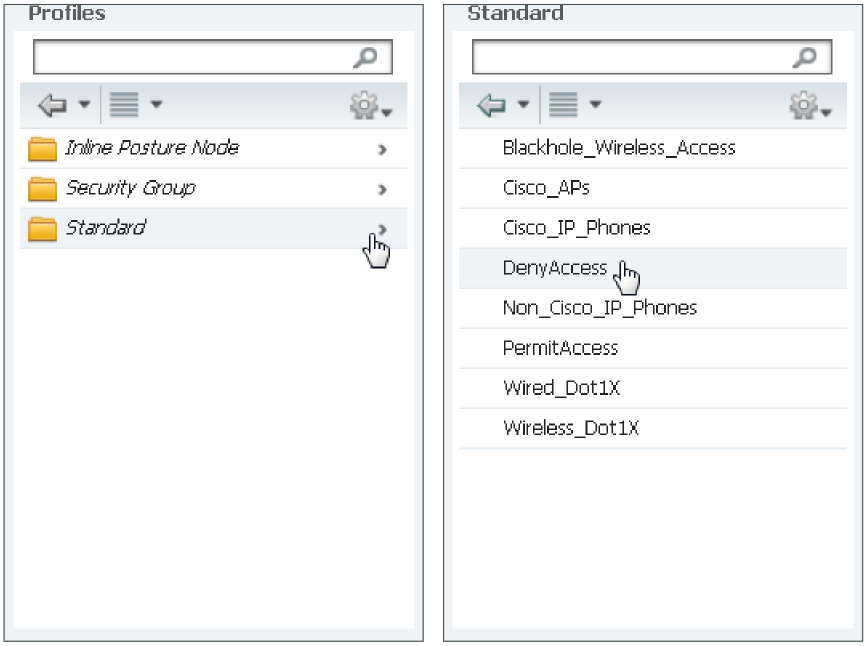
Procedure 1 Modify default rule

Step 1: In Cisco ISE, on the main menu bar, navigate to **Policy > Authorization**.

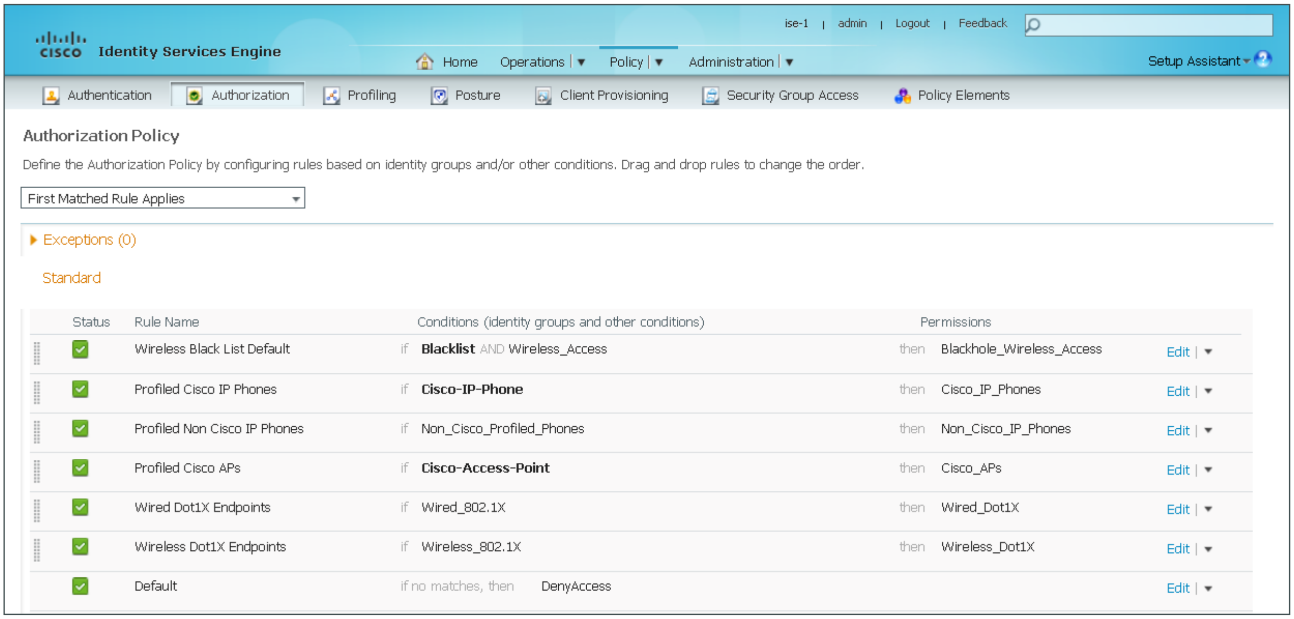
Step 2: In the row for the default rule, click **Edit**.

Step 3: In the Conditions column, next to PermitAccess, click the **+** symbol. A selection box opens.

Step 4: In the list, select **Standard**, and then choose **DenyAccess**.



Step 5: Click **Done**, and then click **Save**. The updated Authorization Policy is displayed.



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)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
☑	Wireless Black List Default	if	**Blacklist** AND Wireless_Access	then	Blackhole_Wireless_Access	Edit |
☑	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones	Edit |
☑	Profiled Non Cisco IP Phones	if	Non_Cisco_Profiled_Phones	then	Non_Cisco_IP_Phones	Edit |
☑	Profiled Cisco APs	if	**Cisco-Access-Point**	then	Cisco_APs	Edit |
☑	Wired Dot1X Endpoints	if	Wired_802.1X	then	Wired_Dot1X	Edit |
☑	Wireless Dot1X Endpoints	if	Wireless_802.1X	then	Wireless_Dot1X	Edit |
☑	Default	if no matches, then	DenyAccess			Edit |

PROCESS

Enabling EAP Chaining

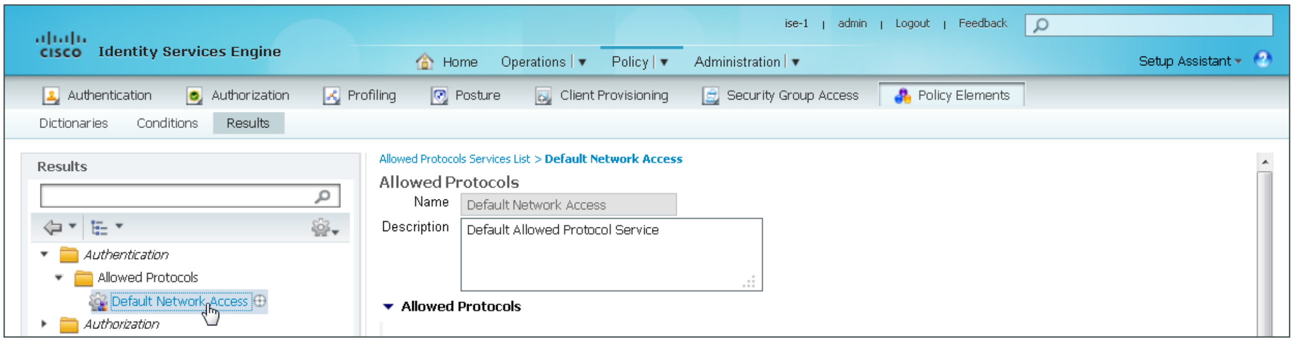
1. Enable EAP Chaining
2. Create authentication policy
3. Create authorization profile
4. Create authorization rule
5. Configure AnyConnect wired profile
6. Configure AnyConnect wireless profile

You have deployed both machine certificates and user certificates to Microsoft Windows workstations. However, only one of the certificates is used for authentication—the user certificate when a user is logged in and the machine certificate when one isn't. EAP Chaining allows you to authenticate using both certificates by using the Cisco AnyConnect Secure Mobility Client 3.1.

Procedure 1 Enable EAP Chaining

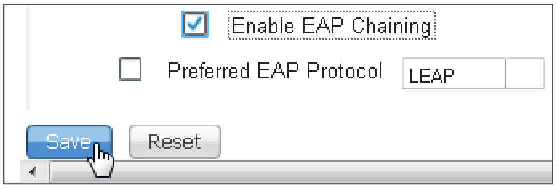
Step 1: Connect to the primary Cisco ISE GUI, **http://ise-1.cisco.local**, and then on the main menu bar, navigate to **Policy > Policy Elements > Results**.

Step 2: In the left pane, navigate to **Authentication > Allowed Protocols**, and then select **Default Network Access**.



Name: Default Network Access
Description: Default Allowed Protocol Service

Step 3: In the **Allowed Protocols** list, near the bottom of the Allow EAP-FAST section, select **Enable EAP Chaining**, and then click **Save**.



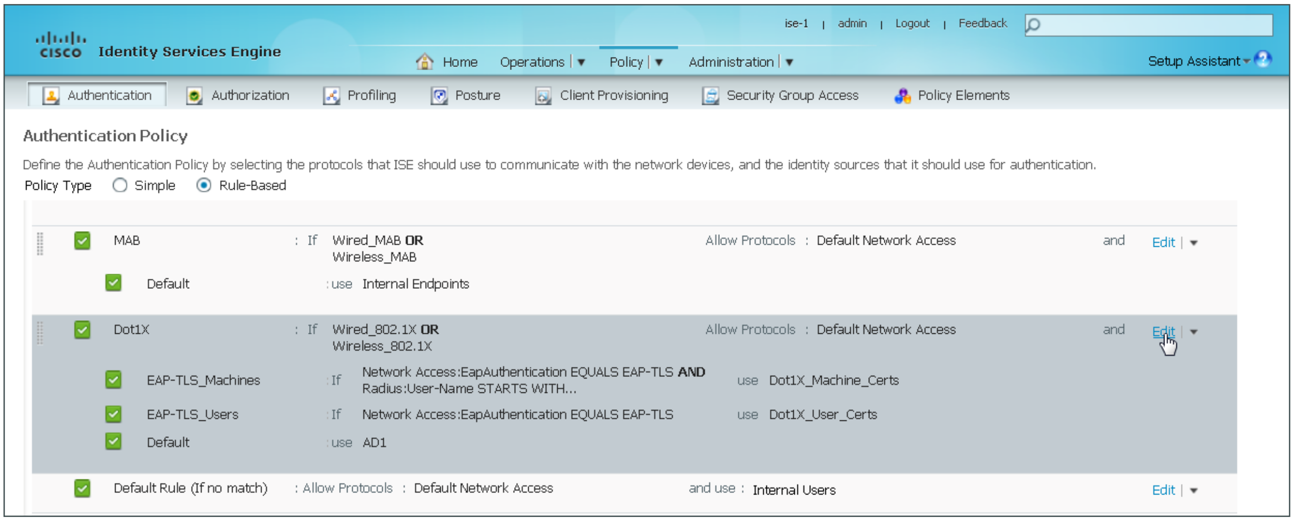
☑ Enable EAP Chaining
☐ Preferred EAP Protocol LEAP

Procedure 2 Create authentication policy

You have authentication rules defined for both machine and user authentication. You need to create a new rule for EAP chaining for both wired and wireless endpoints.

Step 1: Navigate to **Policy** > **Authentication**.

Step 2: In the row for the **Dot1X** rule, click **Edit**. The identity store used for this rule is displayed.



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type ○ Simple ● Rule-Based

☑ MAB : If Wired_MAB **OR** Wireless_MAB Allow Protocols : Default Network Access and Edit

☑ Default :use Internal Endpoints

☑ Dot1X : If Wired_802.1X **OR** Wireless_802.1X Allow Protocols : Default Network Access and Edit

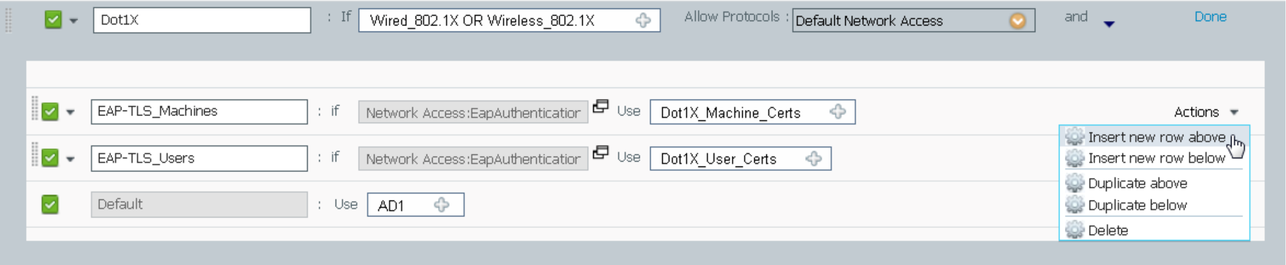
☑ EAP-TLS_Machines :If Network Access:EapAuthentication EQUALS EAP-TLS **AND** Radius:User-Name STARTS WITH... use Dot1X_Machine_Certs

☑ EAP-TLS_Users :If Network Access:EapAuthentication EQUALS EAP-TLS use Dot1X_User_Certs

☑ Default :use AD1

☑ Default Rule (If no match) : Allow Protocols : Default Network Access and use : Internal Users Edit

Step 3: Within the first sub-rule called EAP-TLS_Machines, in the **Actions** list at the right, choose **Insert new row above**.



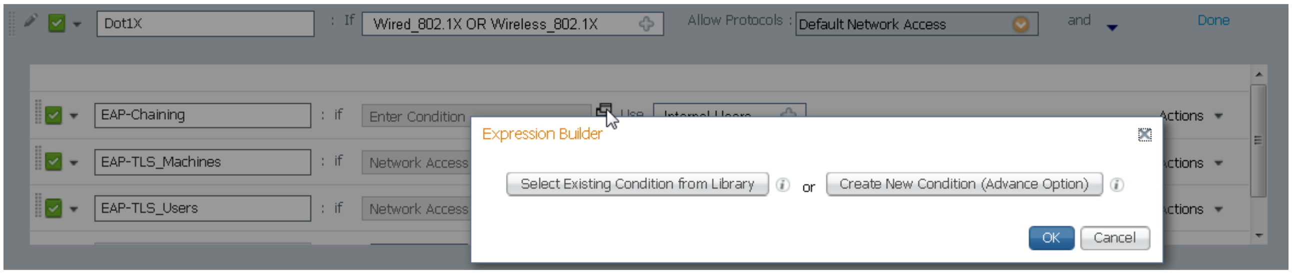
☑ Dot1X : If Wired_802.1X OR Wireless_802.1X Allow Protocols : Default Network Access and

☑ EAP-TLS_Machines : if Network Access:EapAuthenticatior Use Dot1X_Machine_Certs

☑ EAP-TLS_Users : if Network Access:EapAuthenticatior Use Dot1X_User_Certs

☑ Default : Use AD1

Step 4: Name the inserted rule **EAP-Chaining**, and then next to the Enter Condition box, click the box symbol. The Expression Builder opens.


Done
Actions
Expression Builder
Select Existing Condition from Library
or
Create New Condition (Advance Option)
OK
Cancel

☑ Dot1X : If Wired_802.1X OR Wireless_802.1X Allow Protocols : Default Network Access and

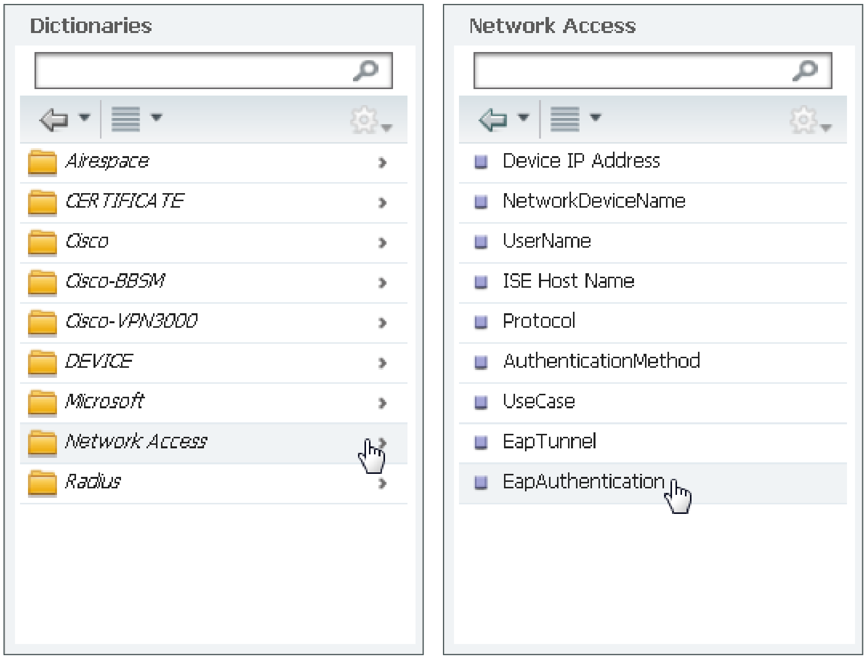
☑ EAP-Chaining : if Enter Condition Use Internal Users

☑ EAP-TLS_Machines : if Network Access

☑ EAP-TLS_Users : if Network Access

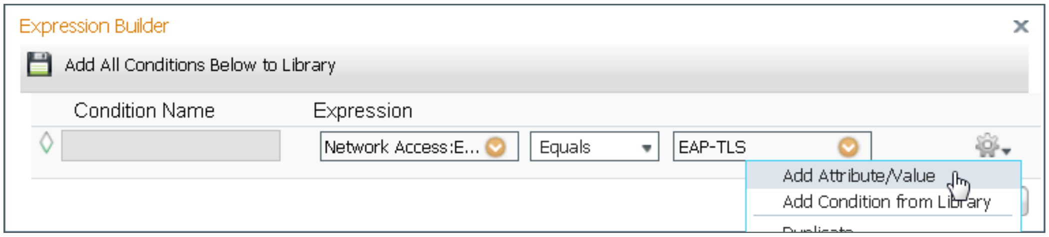
Step 5: Click **Create New Condition (Advance Option)**.

Step 6: In the **Expression** list, select **Network Access**, and then select **EapAuthentication**.



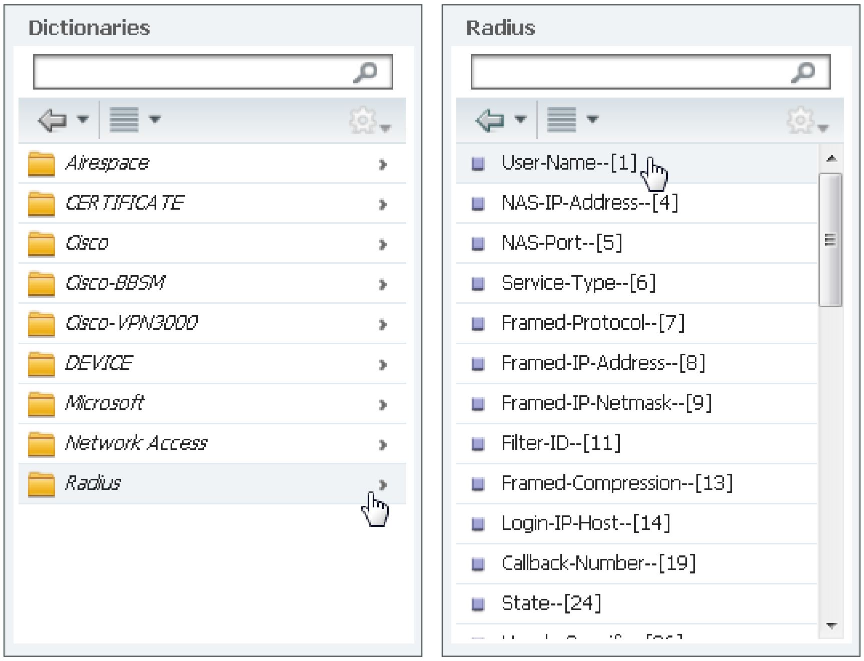
Step 7: In the second list, click **Equals.**

Step 8: **I**n the last list, choose **EAP-TLS**, click the gear icon at the end of the condition, and then choose **Add Attribute/Value**.


Expression Builder
Add All Conditions Below to Library
Condition Name
Expression
Add Attribute/Value
Add Condition from Library

Network Access:E... Equals EAP-TLS

Step 9: In the newly created row, in the Expression column, select **Radius**, click the arrow, and then choose **User-Name--[1]**.



Dictionaries

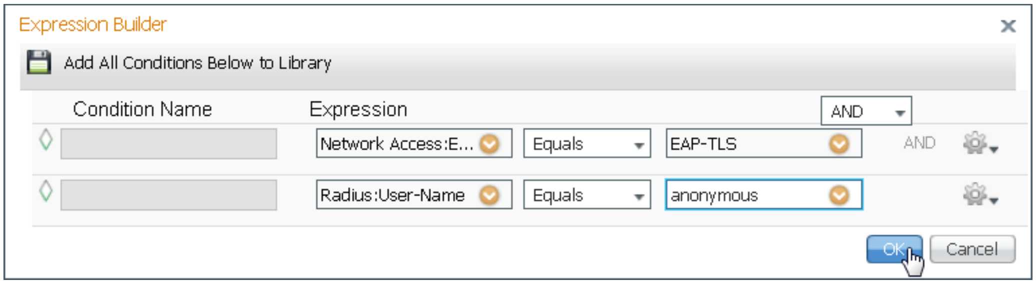
- Airespace
- CERTIFICATE
- Cisco
- Cisco-BBSM
- Cisco-VPN3000
- DEVICE
- Microsoft
- Network Access
- Radius

Radius

- User-Name--[1]
- NAS-IP-Address--[4]
- NAS-Port--[5]
- Service-Type--[6]
- Framed-Protocol--[7]
- Framed-IP-Address--[8]
- Framed-IP-Netmask--[9]
- Filter-ID--[11]
- Framed-Compression--[13]
- Login-IP-Host--[14]
- Callback-Number--[19]
- State--[24]

Step 10: In the next list, choose **Equals**.

Step 11: In the last box, type **anonymous**, and then click **OK**.

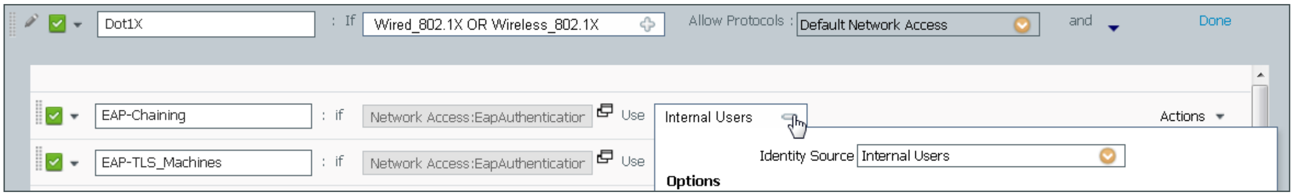


Expression Builder

Add All Conditions Below to Library

Condition Name	Expression			AND
	Network Access:E...	Equals	EAP-TLS	AND
	Radius:User-Name	Equals	anonymous	

Step 12: Next to Internal Users, click the **+** symbol. A selection box opens.



Dot1X : If Wired_802.1X OR Wireless_802.1X Allow Protocols : Default Network Access and

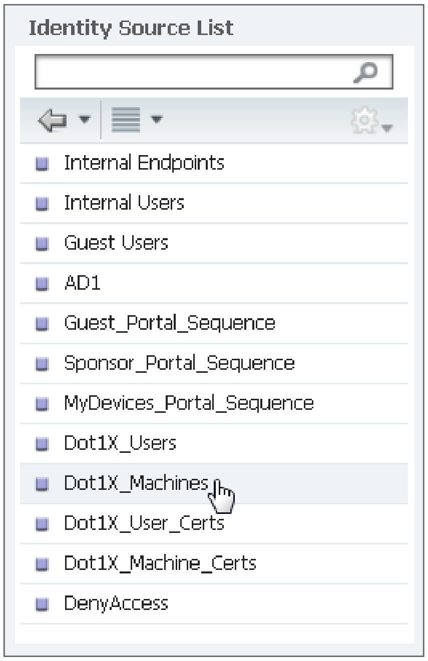
EAP-Chaining : if Network Access:EapAuthenticatior Use Internal Users

EAP-TLS_Machines : if Network Access:EapAuthenticatior Use

Identity Source Internal Users

Options

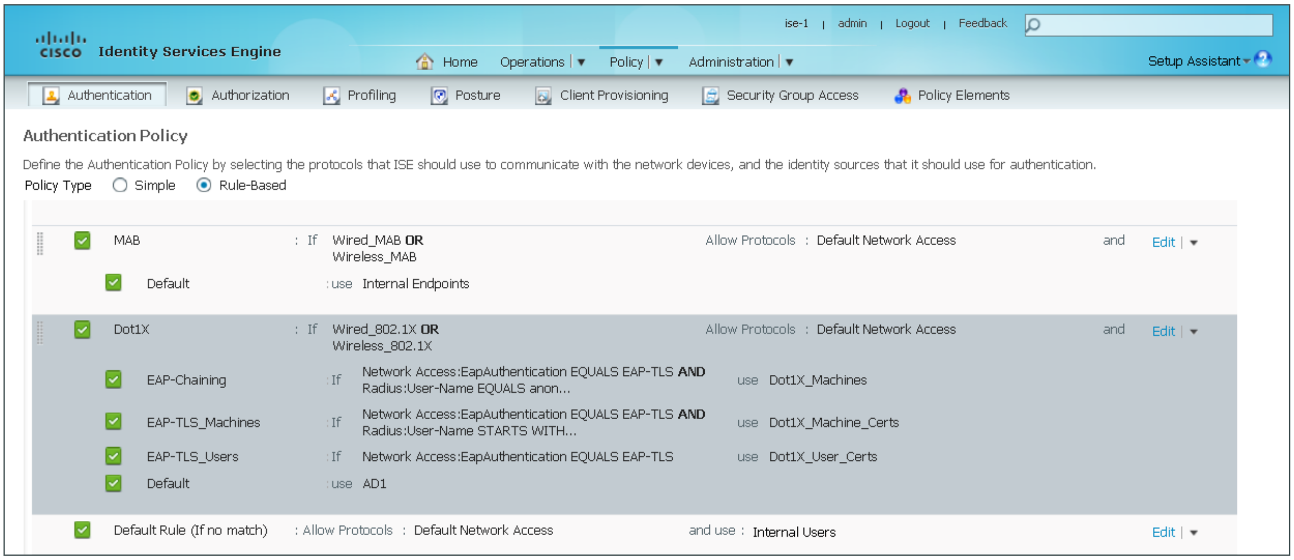
Step 13: In the **Identity Source** list, choose the identity source sequence for machine authentication that you created in Procedure 2, “Create machine authentication policies,”



Identity Source List

- Internal Endpoints
- Internal Users
- Guest Users
- AD1
- Guest_Portal_Sequence
- Sponsor_Portal_Sequence
- MyDevices_Portal_Sequence
- Dot1X_Users
- Dot1X_Machines
- Dot1X_User_Certs
- Dot1X_Machine_Certs
- DenyAccess

Step 14: Using the default options for this identity source, click anywhere in the window in order to continue, and then click **Save**. The updated Authentication Policy is displayed.



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type ○ Simple ● Rule-Based

☑ MAB : If Wired_MAB **OR** Wireless_MAB Allow Protocols : Default Network Access and
- ☑ Default : use Internal Endpoints

☑ Dot1X : If Wired_802.1X **OR** Wireless_802.1X Allow Protocols : Default Network Access and
- ☑ EAP-Chaining : If Network Access:EapAuthentication EQUALS EAP-TLS **AND** Radius:User-Name EQUALS anon... use Dot1X_Machines
- ☑ EAP-TLS_Machines : If Network Access:EapAuthentication EQUALS EAP-TLS **AND** Radius:User-Name STARTS WITH... use Dot1X_Machine_Certs
- ☑ EAP-TLS_Users : If Network Access:EapAuthentication EQUALS EAP-TLS use Dot1X_User_Certs
- ☑ Default : use AD1

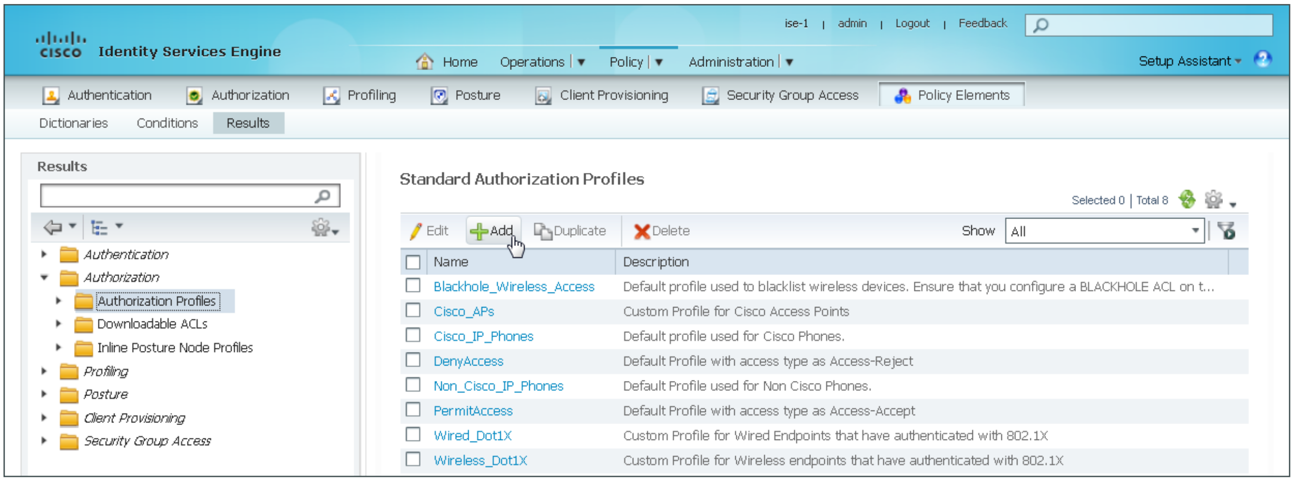
☑ Default Rule (If no match) : Allow Protocols : Default Network Access and use : Internal Users

Procedure 3 Create authorization profile

An authorization profile defines the specific access policies granted to the device. You create a policy to permit full access for devices that pass both user and machine authentication. Although there is already a built-in profile that permits full access, creating a new one allows you to modify the policy if you choose to make a more restrictive policy in the future.

Step 1: In Cisco ISE, on the main menu bar, navigate to **Policy > Policy Elements > Results**.

Step 2: In the left pane, navigate to **Authorization** > **Authorization Profiles**, next to the folder icon click the **Authorization Profiles** text, and then in the main Standard Authorization Profiles pane, click **Add**.



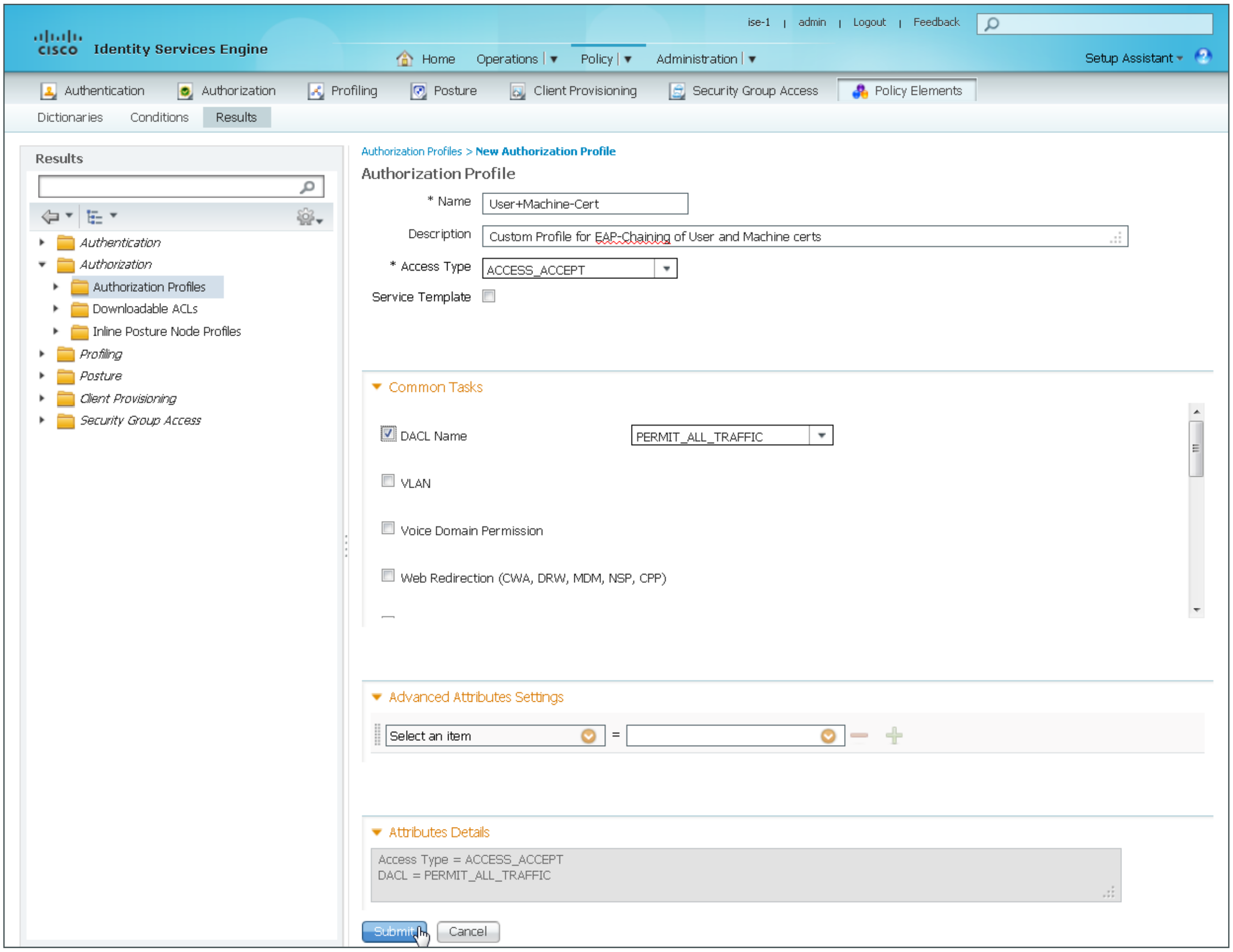
☐ Name	Description
☐ Blackhole_Wireless_Access	Default profile used to blacklist wireless devices. Ensure that you configure a BLACKHOLE ACL on t...
☐ Cisco_APs	Custom Profile for Cisco Access Points
☐ Cisco_IP_Phones	Default profile used for Cisco Phones.
☐ DenyAccess	Default Profile with access type as Access-Reject
☐ Non_Cisco_IP_Phones	Default Profile used for Non Cisco Phones.
☐ PermitAccess	Default Profile with access type as Access-Accept
☐ Wired_Dot1X	Custom Profile for Wired Endpoints that have authenticated with 802.1X
☐ Wireless_Dot1X	Custom Profile for Wireless endpoints that have authenticated with 802.1X

Step 3: In the Authorization Profile, add the Name **User+Macine-Cert**.

Step 4: Add a description.

Step 5: Select **DACL Name**.

Step 6: In the **DACL Name** list, choose **PERMIT_ALL_TRAFFIC**, and then click **Submit**.



Authorization Profile

* Name: User+Machine-Cert

Description: Custom Profile for EAP-Chaining of User and Machine certs

* Access Type: ACCESS_ACCEPT

Service Template ☐

Common Tasks

☑ DACL Name: PERMIT_ALL_TRAFFIC

☐ VLAN

☐ Voice Domain Permission

☐ Web Redirection (CWA, DRW, MDM, NSP, CPP)

Attributes Details

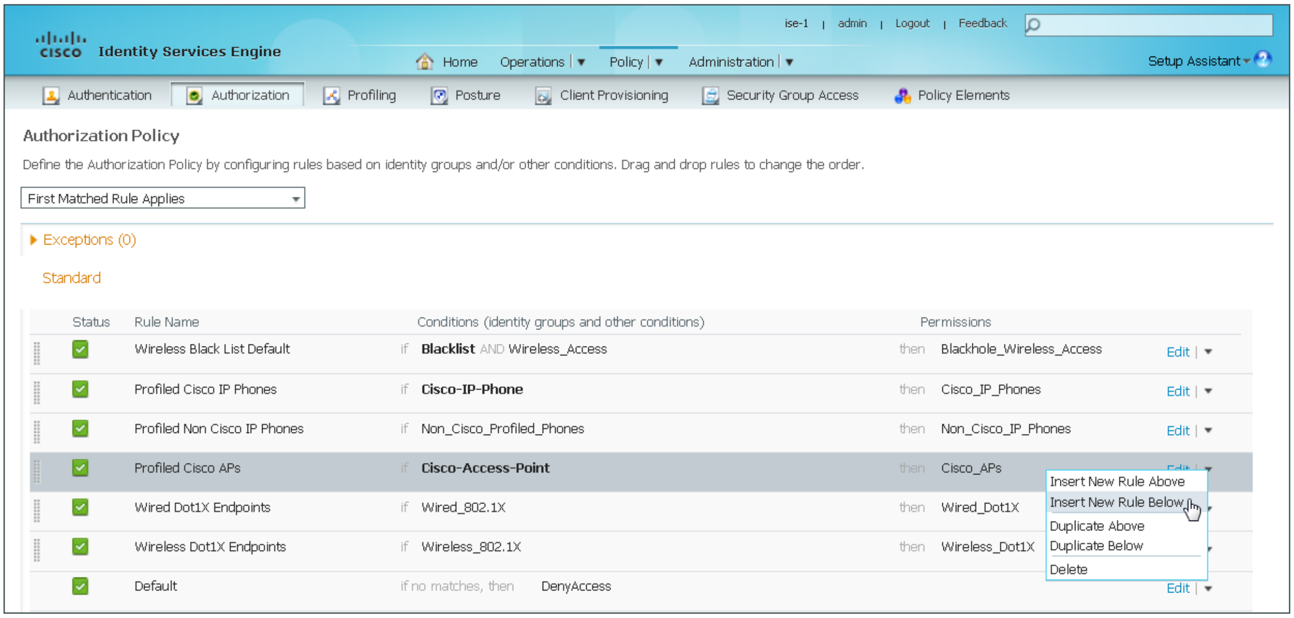
Access Type = ACCESS_ACCEPT
DACL = PERMIT_ALL_TRAFFIC

Procedure 4 Create authorization rule

Now you define an authorization policy and apply the authorization profile.

Step 1: In Cisco ISE, on the main menu bar, navigate to **Policy > Authorization**.

Step 2: For the Profiled Cisco APs rule, on the right, click the black triangle symbol, and then select **Insert New Rule Below**. A new rule named **Standard Rule 1** is created.



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

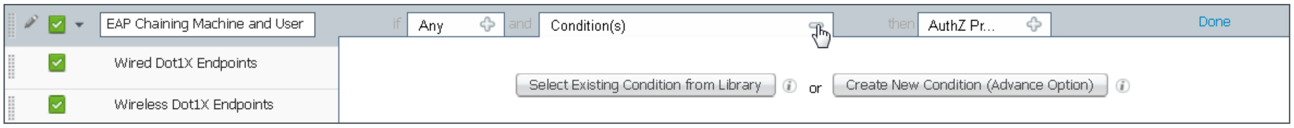
▸ Exceptions (0)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
☑	Wireless Black List Default	if	**Blacklist** AND Wireless_Access	then	Blackhole_Wireless_Access	Edit | ▾
☑	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones	Edit | ▾
☑	Profiled Non Cisco IP Phones	if	Non_Cisco_Profiled_Phones	then	Non_Cisco_IP_Phones	Edit | ▾
☑	Profiled Cisco APs	if	**Cisco-Access-Point**	then	Cisco_APs	Edit | ▾
☑	Wired Dot1X Endpoints	if	Wired_802.1X	then	Wired_Dot1X	
☑	Wireless Dot1X Endpoints	if	Wireless_802.1X	then	Wireless_Dot1X	
☑	Default	if no matches, then	DenyAccess			Edit | ▾

Step 3: Rename the rule **EAP Chaining Machine and User**.

Step 4: In the row for the new rule, in the Conditions column, next to Condition(s), click the **+** symbol. A selection box appears.



Done
Select Existing Condition from Library
or
Create New Condition (Advance Option)

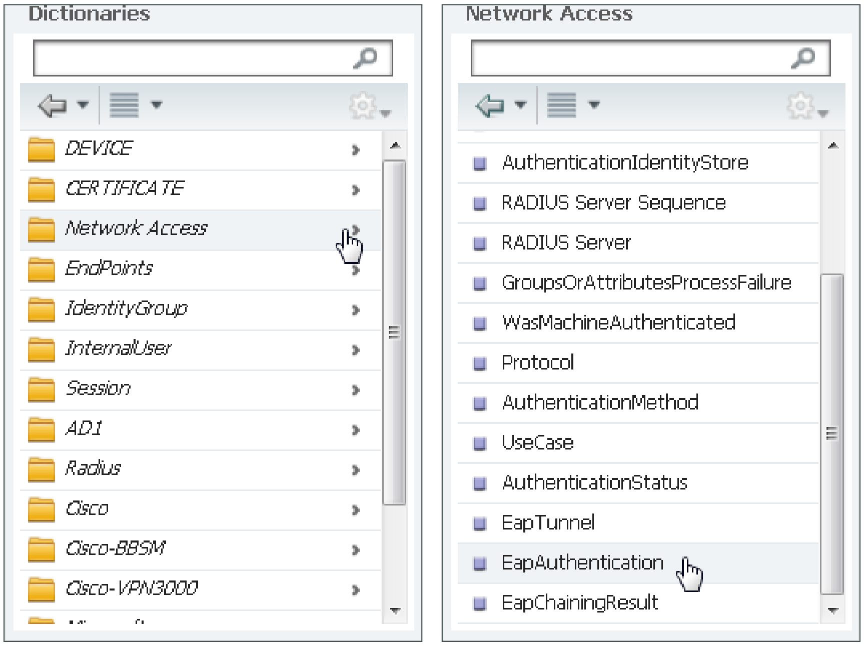
☑ EAP Chaining Machine and User | if Any and Condition(s) | then AuthZ Pr...

☑ Wired Dot1X Endpoints

☑ Wireless Dot1X Endpoints

Step 5: Click **Create New Condition (Advance Option)**.

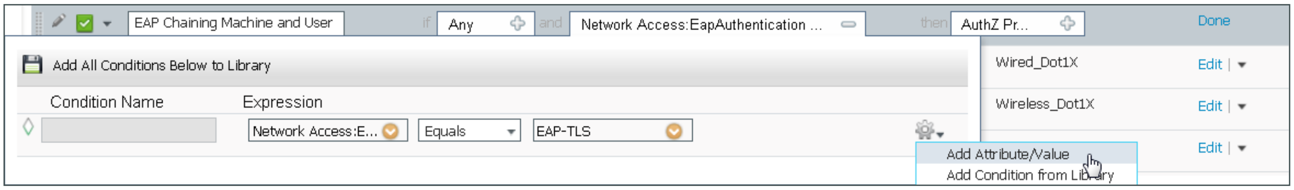
Step 6: In the Expression column, in the **Select Attribute** list, select **Network Access**, and then choose **EapAuthentication**.



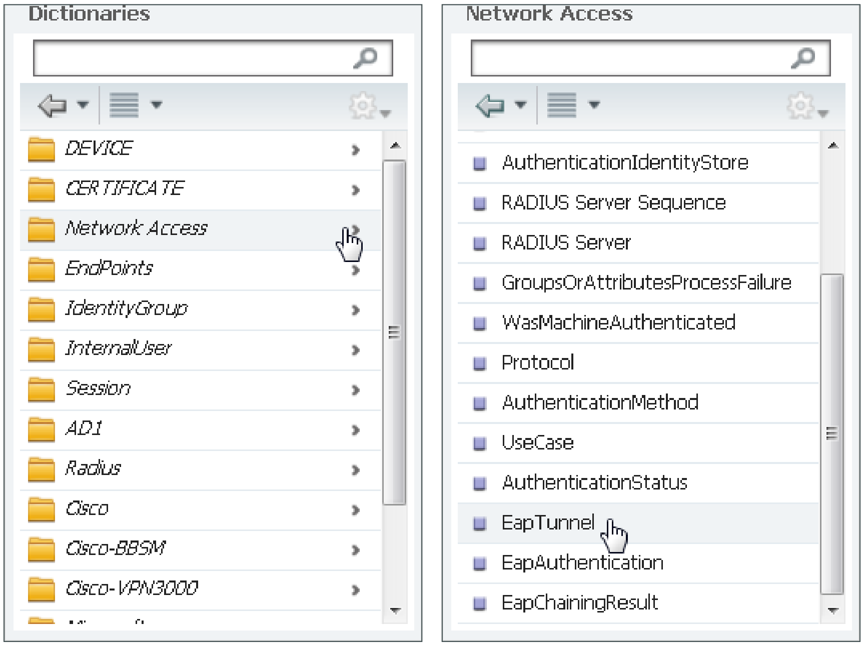
Step 7: In the next column, choose **Equals**.

Step 8: In the final column, choose **EAP-TLS**.

Step 9: Click the gear icon at the end of the rule, and then select **Add Attribute/Value**.



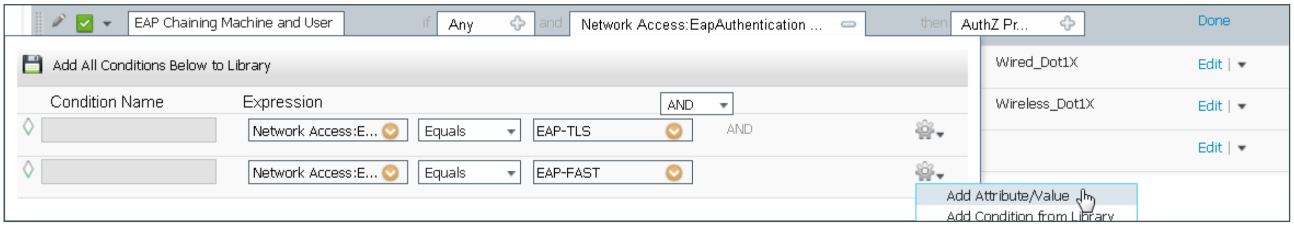
Step 10: In the new row, under the Expression column, in the Select Attribute list, click **Network Access**, and then click **EapTunnel**.



Step 11: In the next column, choose **Equals**.

Step 12: In the final column, choose **EAP-FAST**.

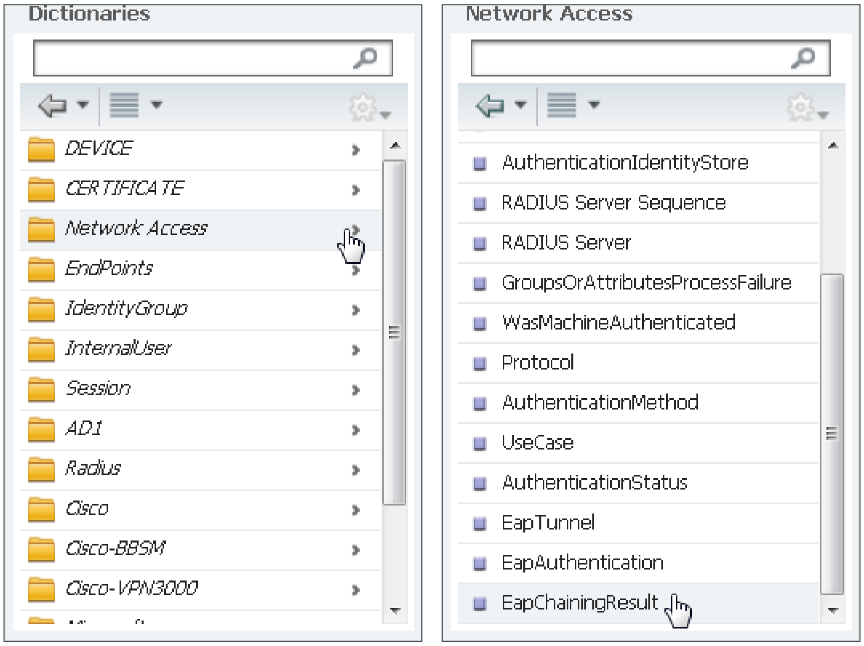
Step 13: Click the gear icon at the end of the rule, and then select **Add Attribute/Value**.


EAP Chaining Machine and User if Any and Network Access:EapAuthentication ... then AuthZ Pr...

Network Access:E... Equals EAP-TLS AND

Network Access:E... Equals EAP-FAST

Step 14: In the new row, under the Expression column, in the **Select Attribute** list, select **Network Access**, and then choose **EapChainingResult**.

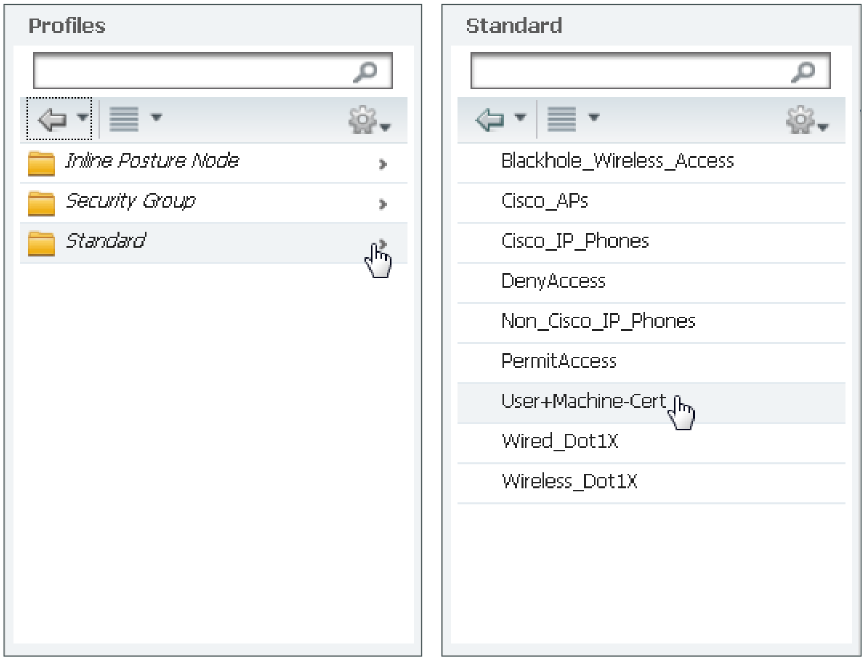


Step 15: In the next column, choose **Equals**.

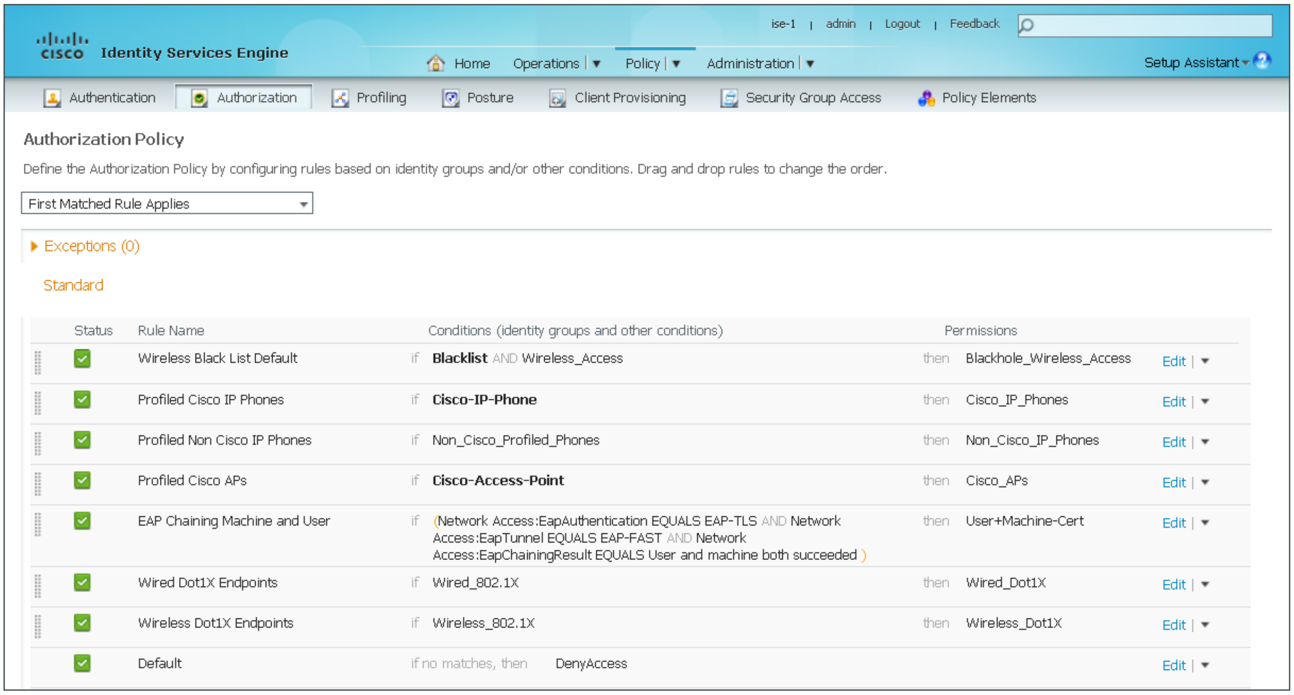
Step 16: In the final column, choose **User and machine both succeeded**, and then click anywhere in order to continue.

Step 17: In the Permissions section, next to AuthZ Profile(s), click the **+** symbol.

Step 18: In the **Select an item** list, click **Standard**, choose the **User+Machine-Cert** authorization profile that you created in Procedure 3, “Create authorization profile.”



Step 19: Click **Done**, and then click **Save**. The updated Authorization Policy is displayed.



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)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)		Permissions	
☑	Wireless Black List Default	if **Blacklist** AND Wireless_Access	then	Blackhole_Wireless_Access	Edit | ▾
☑	Profiled Cisco IP Phones	if **Cisco-IP-Phone**	then	Cisco_IP_Phones	Edit | ▾
☑	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then	Non_Cisco_IP_Phones	Edit | ▾
☑	Profiled Cisco APs	if **Cisco-Access-Point**	then	Cisco_APs	Edit | ▾
☑	EAP Chaining Machine and User	if (Network Access:EapAuthentication EQUALS EAP-TLS AND Network Access:EapTunnel EQUALS EAP-FAST AND Network Access:EapChainingResult EQUALS User and machine both succeeded)	then	User+Machine-Cert	Edit | ▾
☑	Wired Dot1X Endpoints	if Wired_802.1X	then	Wired_Dot1X	Edit | ▾
☑	Wireless Dot1X Endpoints	if Wireless_802.1X	then	Wireless_Dot1X	Edit | ▾
☑	Default	if no matches, then DenyAccess			Edit | ▾

Procedure 5 Configure AnyConnect wired profile

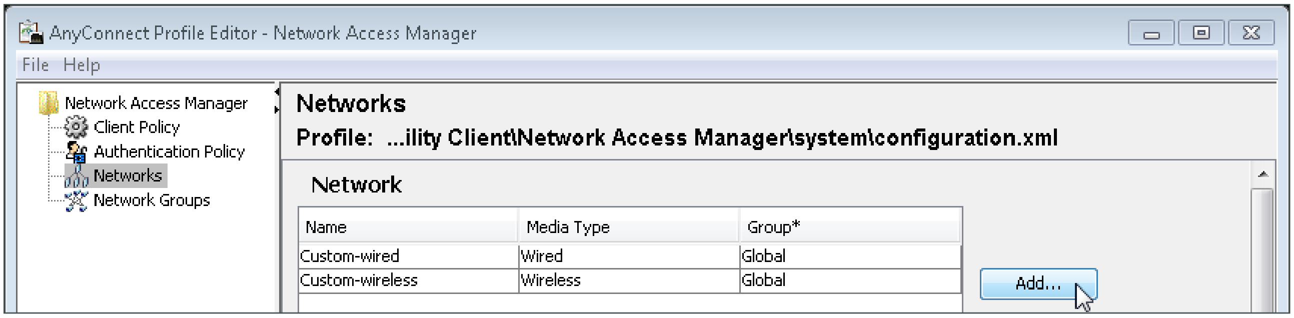
The AnyConnect client was installed in the process “Deploying Cisco AnyConnect on Windows Endpoints.” You now configure the Cisco AnyConnect Secure Mobility Client to use EAP Chaining.

Step 1: On the client running AnyConnect, Launch the Profile Editor by navigating to **Start > All Programs > Cisco > Cisco AnyConnect Profiler Editor > Network Access Manager Profile Editor**.

Step 2: From the **File** menu, choose **Open**, and then select **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\configuration.xml**.

First, create a wired profile for EAP Chaining.

Step 3: Click **Networks**, and then click **Add**.

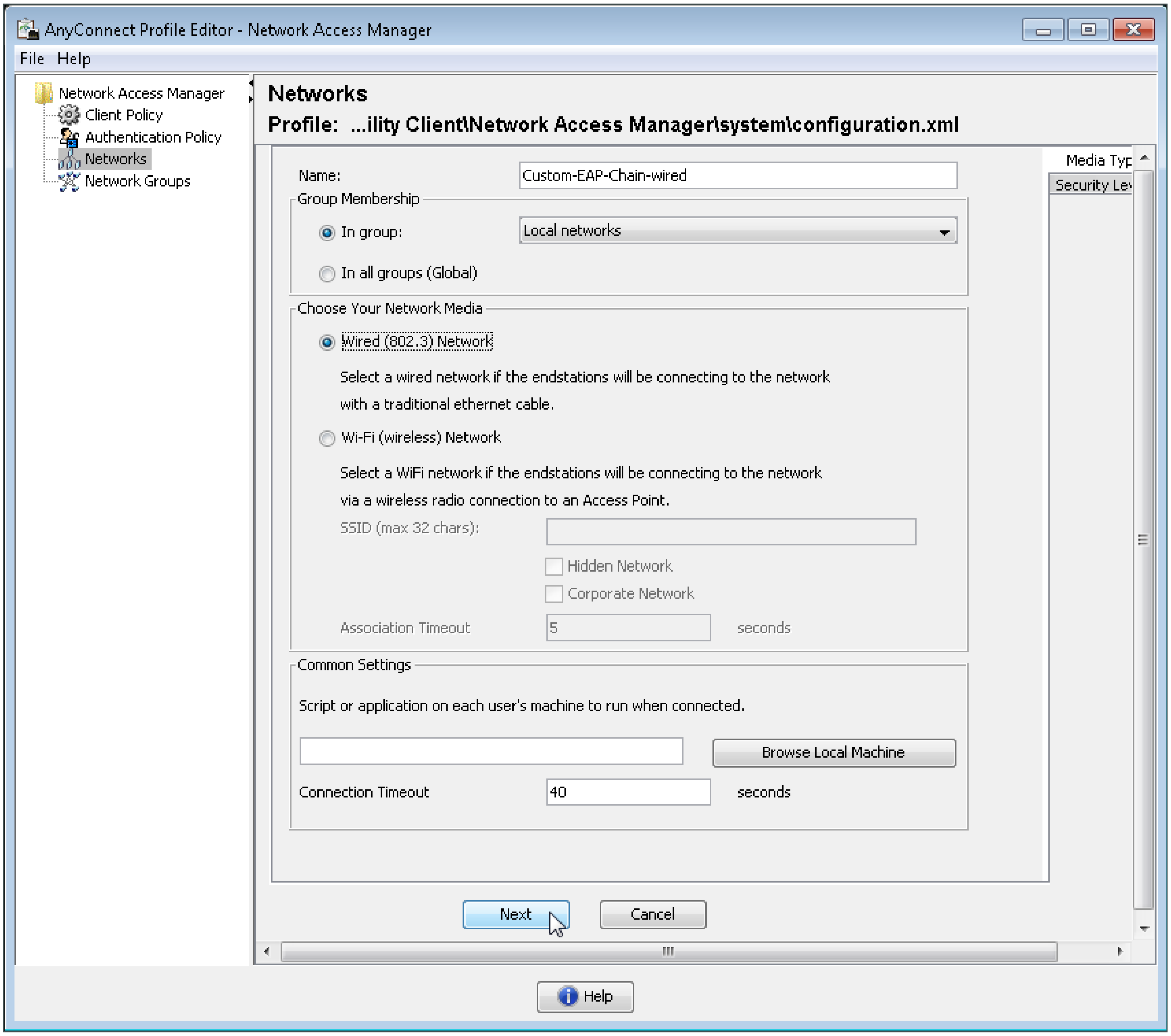


Profile: ...ility Client\Network Access Manager\system\configuration.xml

Name	Media Type	Group*
Custom-wired	Wired	Global
Custom-wireless	Wireless	Global

Step 4: Enter a name for the profile.

Step 5: In **Choose Your Network Media**, select **Wired (802.3) Network**, and then click **Next**.



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

Name: Custom-EAP-Chain-wired

Group Membership

● In group: Local networks

○ In all groups (Global)

Choose Your Network Media

● Wired (802.3) Network

Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.

○ Wi-Fi (wireless) Network

Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.

SSID (max 32 chars):

☐ Hidden Network

☐ Corporate Network

Association Timeout 5 seconds

Common Settings

Script or application on each user's machine to run when connected.

Connection Timeout 40 seconds

Step 6: Select **Authenticating Network**, and then click **Next**.

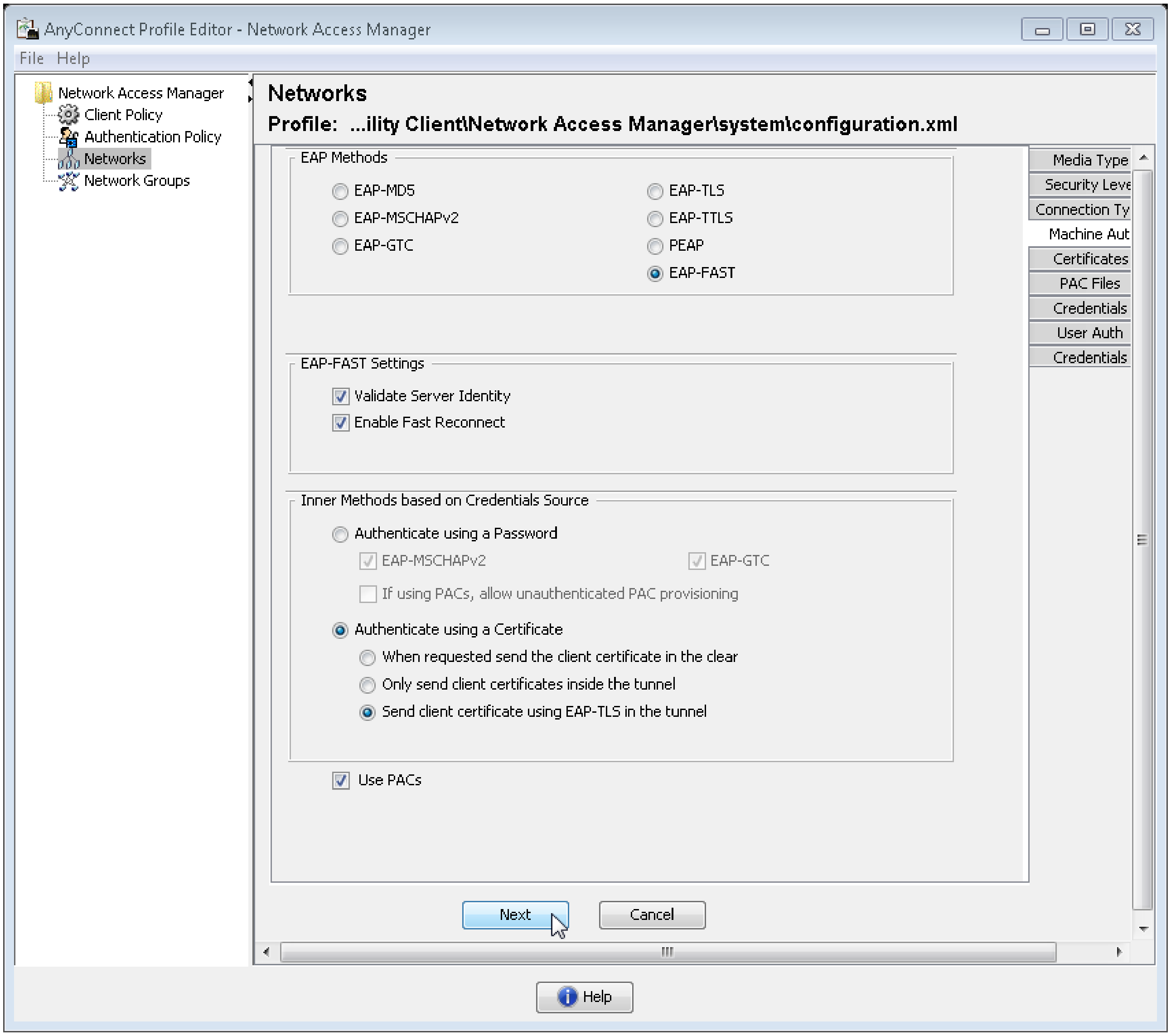
Step 7: For Network Connection Type, select **Machine and User Connection**, and then click **Next**.

Step 8: For the Machine Auth, in EAP Methods, select **EAP-FAST**.

Step 9: In the Inner Methods based on Credentials Source section, select **Authenticate using a certificate**.

Step 10: Select **Send client certificate using EAP-TLS in the tunnel**.

Step 11: Verify that **Use PACs** is selected, and then click **Next**.



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

EAP Methods

○ EAP-MD5
○ EAP-MSCHAPv2
○ EAP-GTC
○ EAP-TLS
○ EAP-TTLS
○ PEAP
● EAP-FAST

EAP-FAST Settings

☑ Validate Server Identity
☑ Enable Fast Reconnect

Inner Methods based on Credentials Source

○ Authenticate using a Password
☑ EAP-MSCHAPv2
☑ EAP-GTC
☐ If using PACs, allow unauthenticated PAC provisioning
● Authenticate using a Certificate
○ When requested send the client certificate in the clear
○ Only send client certificates inside the tunnel
● Send client certificate using EAP-TLS in the tunnel

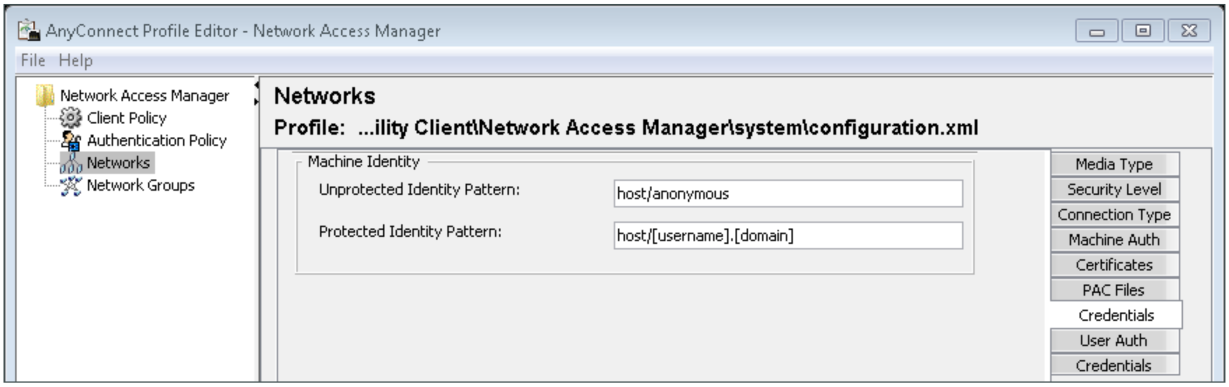
☑ Use PACs

Step 12: For the Certificates tab, click **Next**. This accepts the default values.

Step 13: For the PAC Files tab, click **Next**. This accepts the default values.

Step 14: For Credentials, in the Machine Identity section, enter an unprotected identity pattern **host/anonymous**.

Step 15: Enter a Protected Identity Pattern **host/[username].[domain]**, and then click **Next**.



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

Machine Identity

Unprotected Identity Pattern: host/anonymous

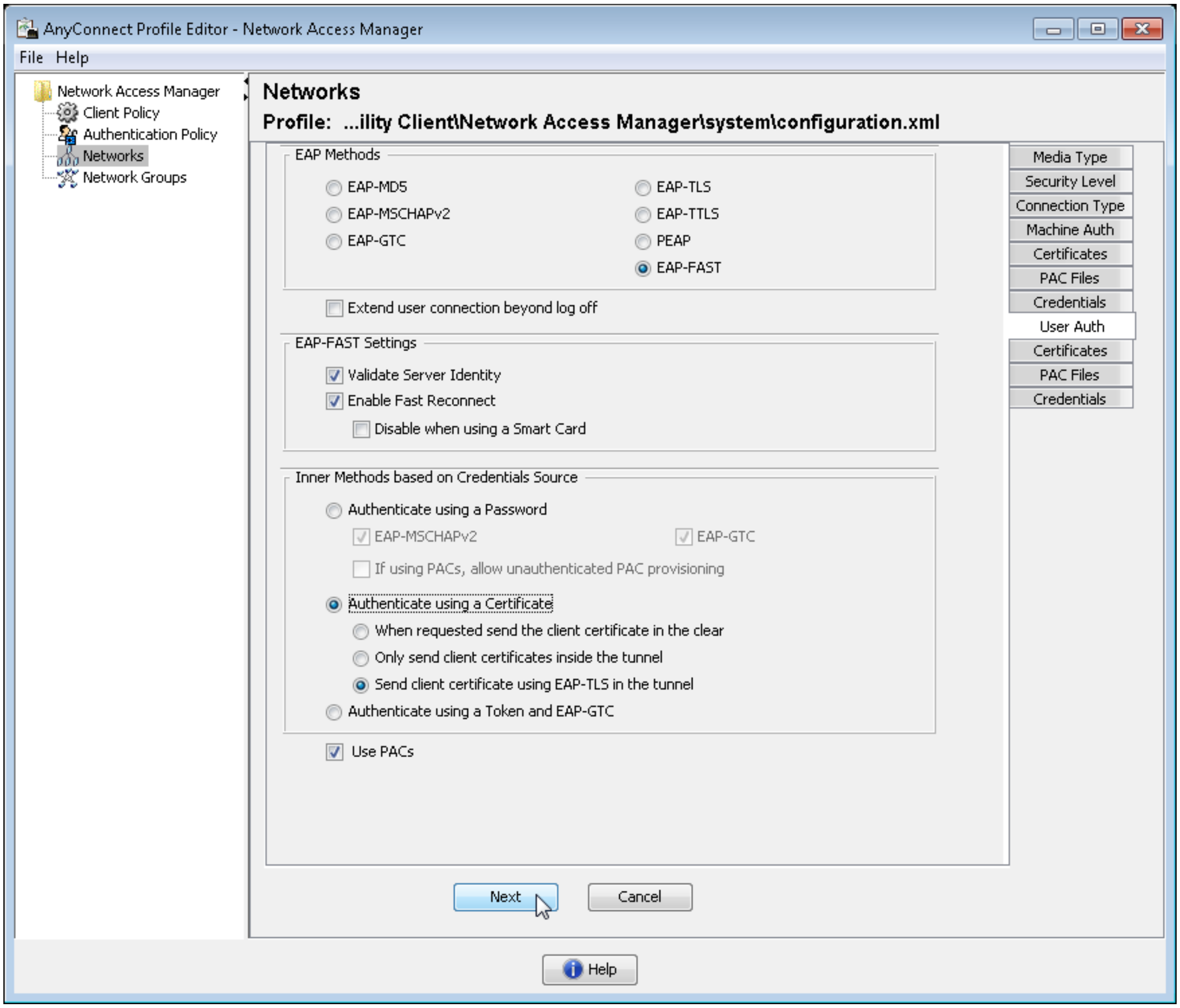
Protected Identity Pattern: host/[username].[domain]

Step 16: In User Auth, in the EAP Methods section, select **EAP-FAST**.

Step 17: In the Inner Methods based on Credentials Source section, select **Authenticate using a certificate**.

Step 18: Select **Send client certificate using EAP-TLS in the tunnel**.

Step 19: Verify that **Use PACs** is selected, and then click **Next**.



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

EAP Methods

○ EAP-MD5
○ EAP-MSCHAPv2
○ EAP-GTC
○ EAP-TLS
○ EAP-TTLS
○ PEAP
● EAP-FAST

☐ Extend user connection beyond log off

EAP-FAST Settings

☑ Validate Server Identity
☑ Enable Fast Reconnect
  ☐ Disable when using a Smart Card

Inner Methods based on Credentials Source

○ Authenticate using a Password
  ☑ EAP-MSCHAPv2 ☑ EAP-GTC
  ☐ If using PACs, allow unauthenticated PAC provisioning
● Authenticate using a Certificate
  ○ When requested send the client certificate in the clear
  ○ Only send client certificates inside the tunnel
  ● Send client certificate using EAP-TLS in the tunnel
○ Authenticate using a Token and EAP-GTC

☑ Use PACs

Step 20: For the Certificates tab, click **Next**. This accepts the default values.

Step 21: For the PAC Files tab, click **Next**. This accepts the default values.

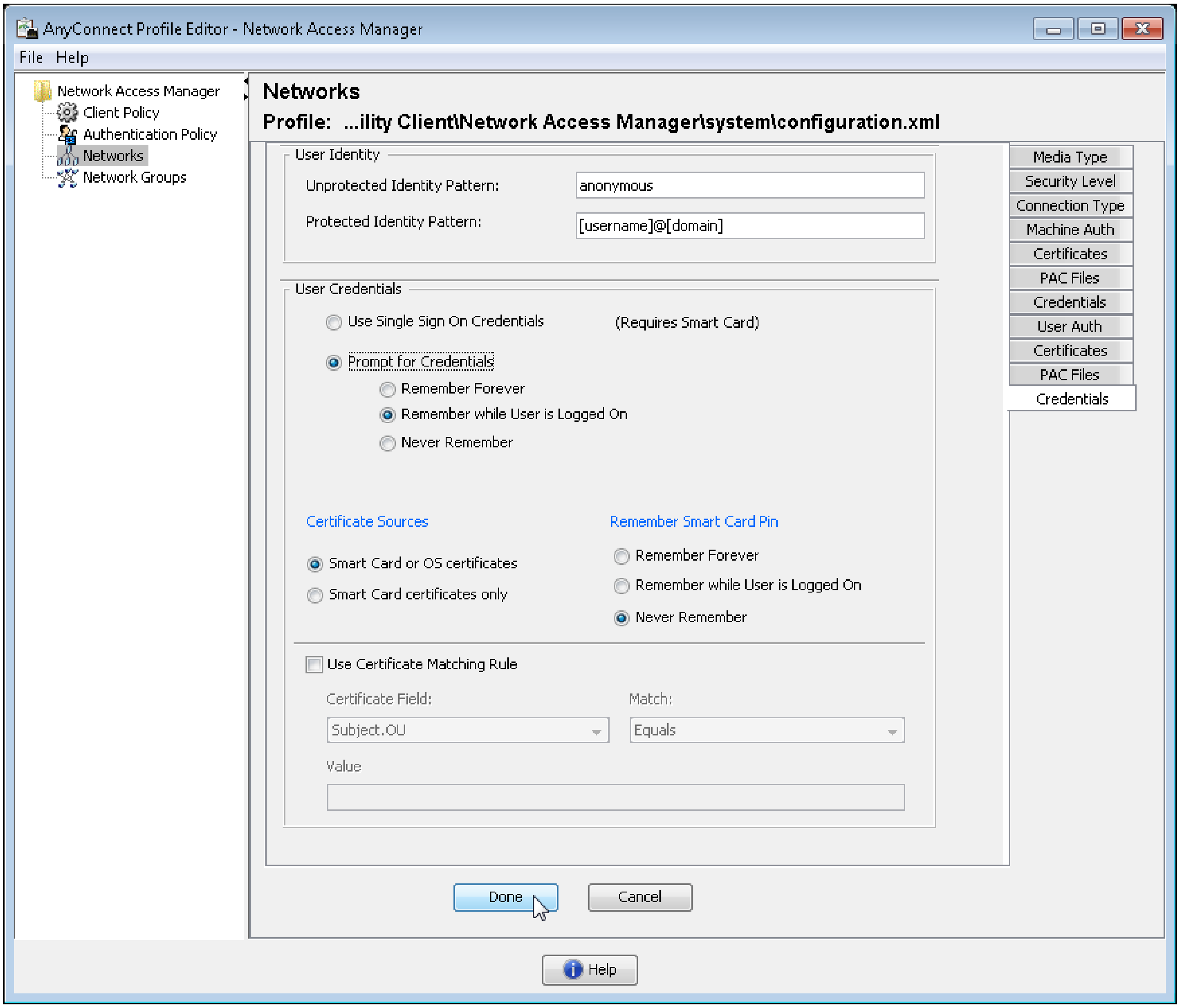
Step 22: In credentials, under User Identity, in the **Unprotected Identity Pattern** box**,** enter **anonymous**.

Step 23: For the protected identity pattern, enter **[username]@[domain]**.

Step 24: In the User Credentials section, select **Prompt for Credentials**.

Step 25: Select **Remember while User is Logged On**.

Step 26: Under **Certificate Sources**, select **Smart Card or OS certificates**, and then click **Done**.



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

User Identity

Unprotected Identity Pattern: anonymous

Protected Identity Pattern: [username]@[domain]

User Credentials

○ Use Single Sign On Credentials (Requires Smart Card)

● Prompt for Credentials

○ Remember Forever

● Remember while User is Logged On

○ Never Remember

Certificate Sources

● Smart Card or OS certificates

○ Smart Card certificates only

Remember Smart Card Pin

○ Remember Forever

○ Remember while User is Logged On

● Never Remember

☐ Use Certificate Matching Rule

Certificate Field: Subject.OU

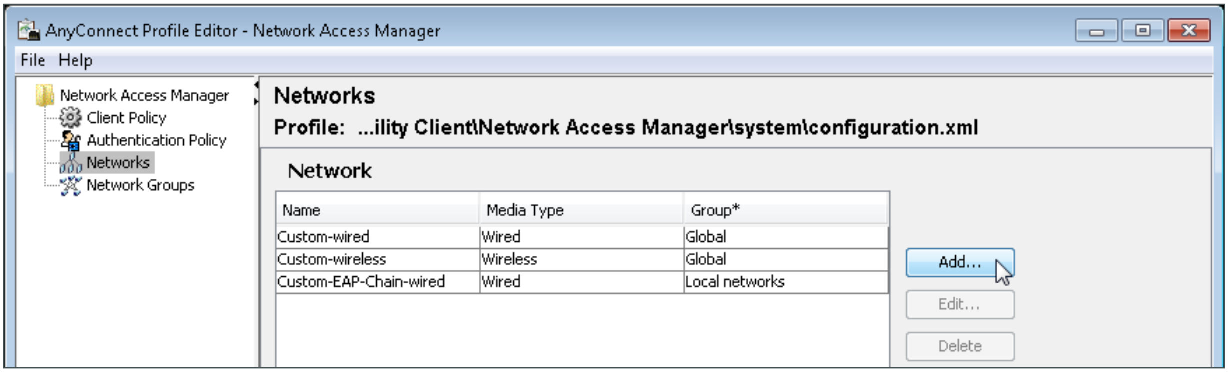
Match: Equals

Value

Procedure 6 Configure AnyConnect wireless profile

You now create a wireless profile for EAP Chaining.

Step 1: Click **Networks**, and then click **Add**.



Networks

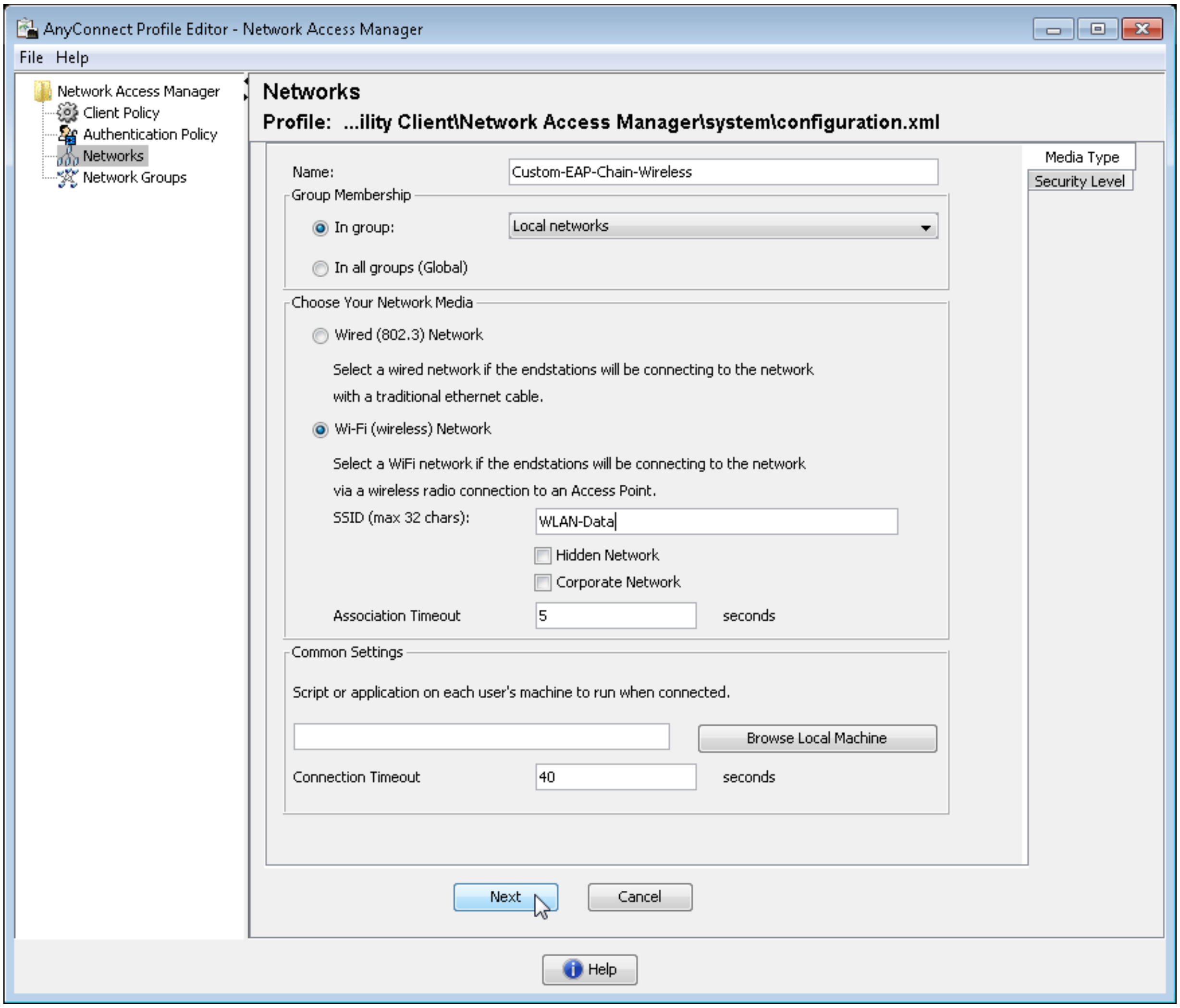
Profile: ...ility Client\Network Access Manager\system\configuration.xml

Network

Name	Media Type	Group*
Custom-wired	Wired	Global
Custom-wireless	Wireless	Global
Custom-EAP-Chain-wired	Wired	Local networks

Step 2: Enter a name for the profile.

Step 3: In the Choose Your Network Media section, select **Wi-Fi (wireless) Network**. For SSID, enter your wireless SSID, and then click **Next**.



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

Name: Custom-EAP-Chain-Wireless

Group Membership

● In group: Local networks

○ In all groups (Global)

Choose Your Network Media

○ Wired (802.3) Network

Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.

● Wi-Fi (wireless) Network

Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.

SSID (max 32 chars): WLAN-Data

☐ Hidden Network

☐ Corporate Network

Association Timeout 5 seconds

Common Settings

Script or application on each user's machine to run when connected.

Connection Timeout 40 seconds

Step 4: For Security Level, select **Authenticating Network**.

Step 5: For Association Mode, choose **WPA2 Enterprise (AES)**, and then click **Next**.

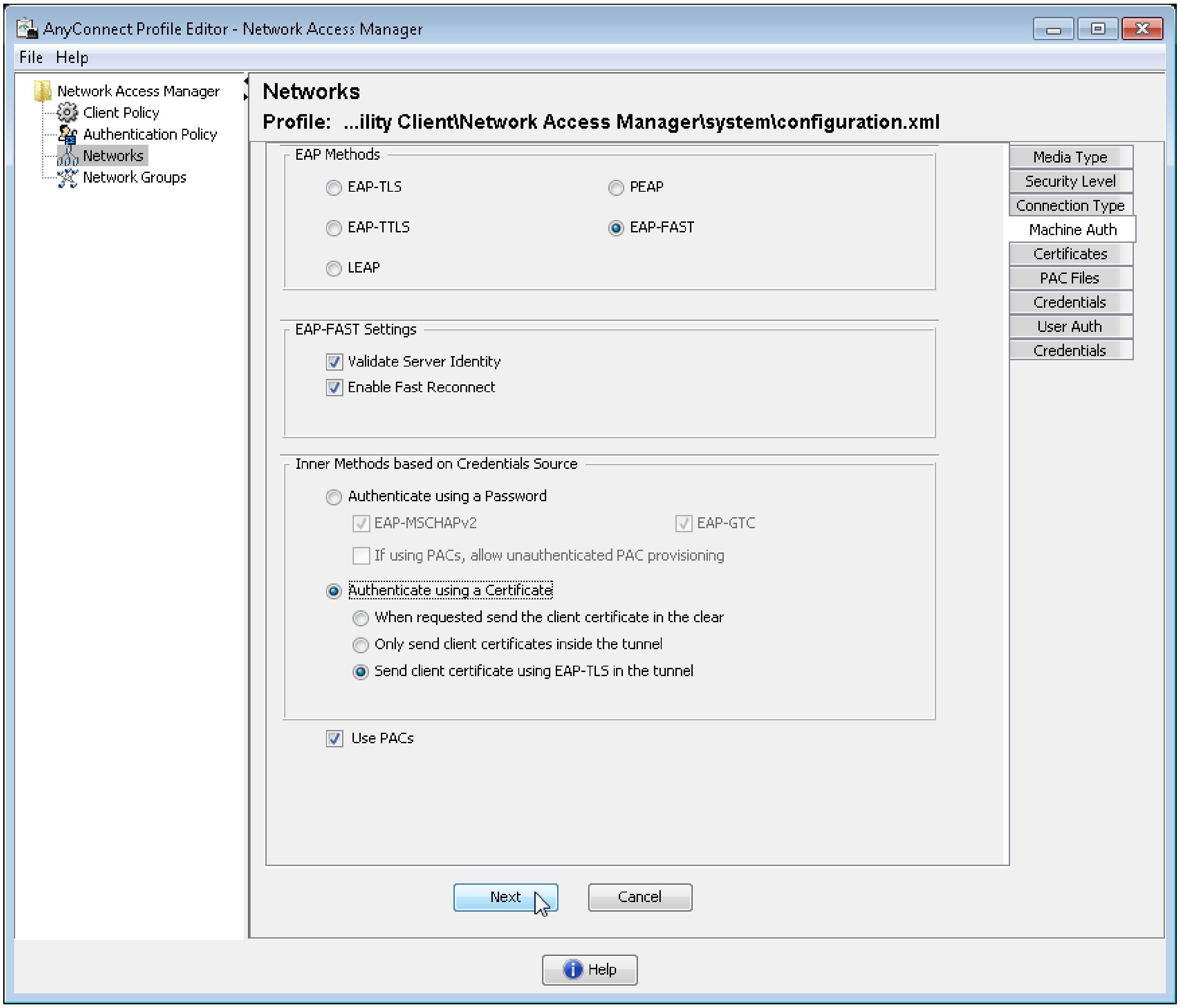
Step 6: For Network Connection Type, select **Machine and User Connection**, and then click **Next**.

Step 7: Under EAP Methods, select **EAP-FAST**.

Step 8: Under Inner Methods based on Credentials Source, select **Authenticate using a certificate**.

Step 9: Select **Send client certificate using EAP-TLS in the tunnel**.

Step 10: Verify that **Use PACs** is selected, and then click **Next**.



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

EAP Methods

○ EAP-TLS ○ PEAP

○ EAP-TTLS ● EAP-FAST

○ LEAP

EAP-FAST Settings

☑ Validate Server Identity

☑ Enable Fast Reconnect

Inner Methods based on Credentials Source

○ Authenticate using a Password

☑ EAP-MSCHAPv2 ☑ EAP-GTC

☐ If using PACs, allow unauthenticated PAC provisioning

● Authenticate using a Certificate

○ When requested send the client certificate in the clear

○ Only send client certificates inside the tunnel

● Send client certificate using EAP-TLS in the tunnel

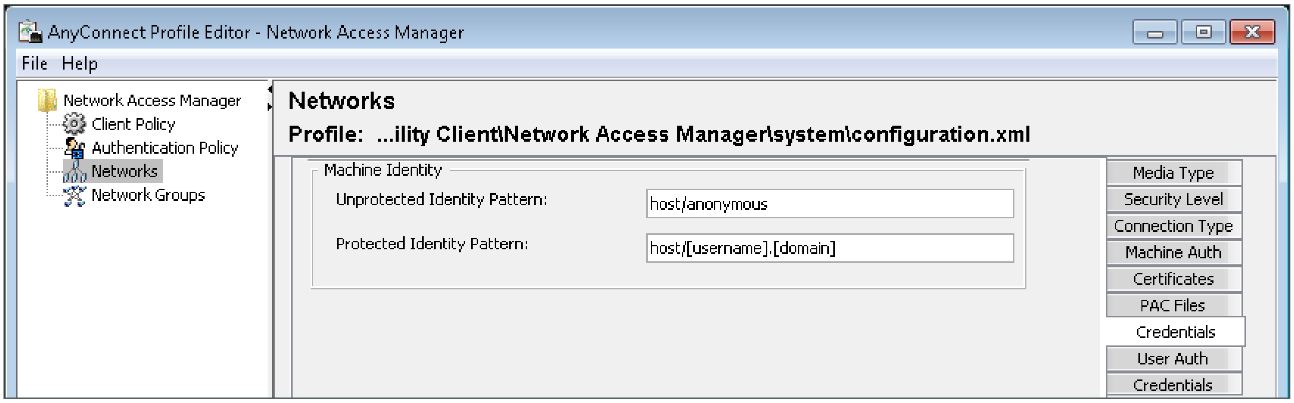
☑ Use PACs

Step 11: For the Certificates tab, click **Next**. This accepts the default values.

Step 12: For the PAC Files tab, click **Next**. This accepts the default values.

Step 13: For credentials, under Machine Identity, in the **Unprotected Identity Pattern** box, enter **host/anonymous**.

Step 14: In the **Protected Identity Pattern** box, enter **host/[username].[domain]**, and then click **Next**.



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

Machine Identity

Unprotected Identity Pattern: host/anonymous

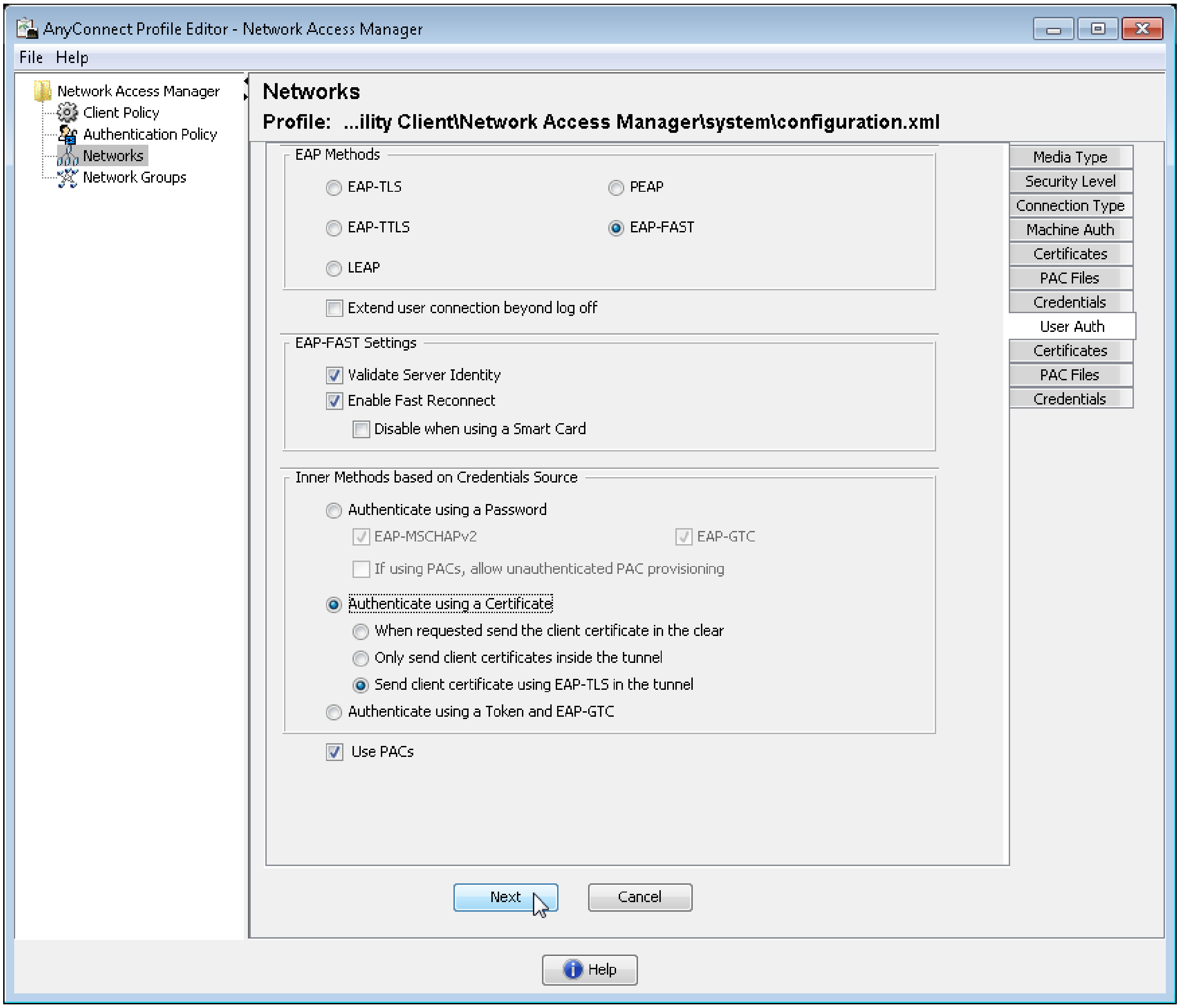
Protected Identity Pattern: host/[username].[domain]

Step 15: For User Auth, under EAP Methods, select **EAP-FAST**.

Step 16: Under Inner Methods based on Credentials Source, select **Authenticate using a certificate**.

Step 17: Select **Send client certificate using EAP-TLS in the tunnel**.

Step 18: Verify that **Use PACs** is selected, and then click **Next**.



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

EAP Methods

○ EAP-TLS ○ PEAP

○ EAP-TTLS ● EAP-FAST

○ LEAP

☐ Extend user connection beyond log off

EAP-FAST Settings

☑ Validate Server Identity

☑ Enable Fast Reconnect

☐ Disable when using a Smart Card

Inner Methods based on Credentials Source

○ Authenticate using a Password

☑ EAP-MSCHAPv2 ☑ EAP-GTC

☐ If using PACs, allow unauthenticated PAC provisioning

● Authenticate using a Certificate

○ When requested send the client certificate in the clear

○ Only send client certificates inside the tunnel

● Send client certificate using EAP-TLS in the tunnel

○ Authenticate using a Token and EAP-GTC

☑ Use PACs

Step 19: For the Certificates tab, click **Next**. This accepts the default values.

Step 20: For the PAC Files tab, click **Next**. This accepts the default values.

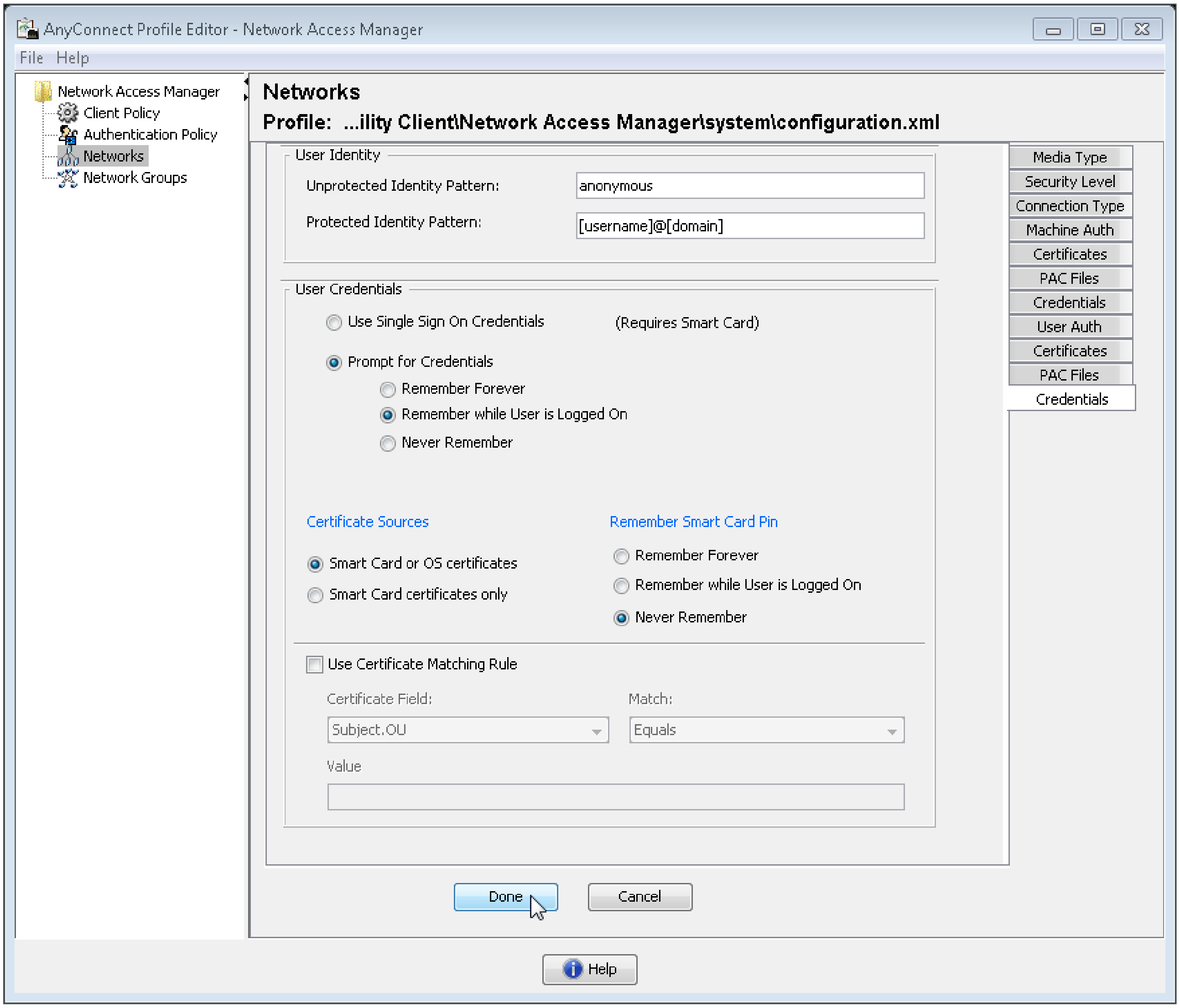
Step 21: For Credentials, under User Identity, in the **Unprotected Identity Pattern** box, enter **anonymous**.

Step 22: In the **Protected Identity Pattern** box, enter **[username]@[domain]**.

Step 23: In the User Credentials section, select **Prompt for Credentials**.

Step 24: Select **Remember while User is Logged On**.

Step 25: Under **Certificate Sources**, select **Smart Card or OS certificates**, and then click **Done**.



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

User Identity

Unprotected Identity Pattern: anonymous

Protected Identity Pattern: [username]@[domain]

User Credentials

○ Use Single Sign On Credentials (Requires Smart Card)

● Prompt for Credentials

- ○ Remember Forever
- ● Remember while User is Logged On
- ○ Never Remember

Certificate Sources

● Smart Card or OS certificates

○ Smart Card certificates only

Remember Smart Card Pin

○ Remember Forever

○ Remember while User is Logged On

● Never Remember

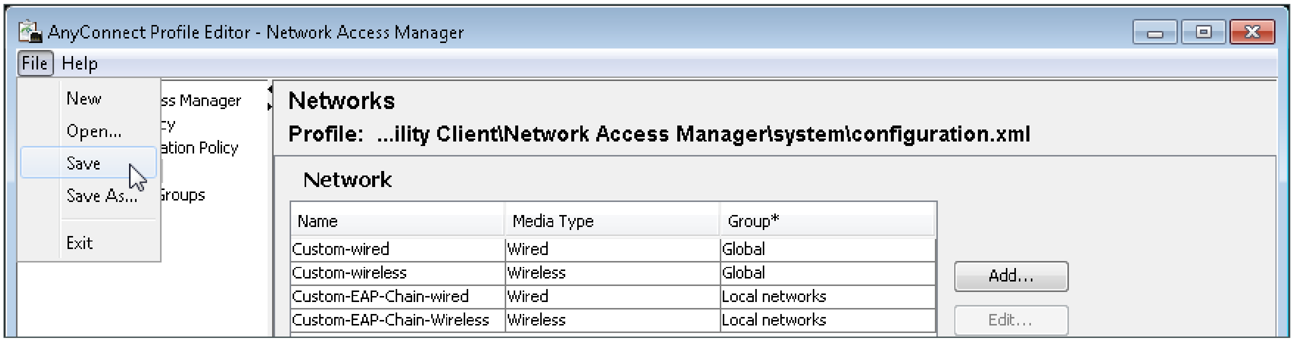
☐ Use Certificate Matching Rule

Certificate Field: Subject.OU

Match: Equals

Value

Step 26: From the **File** menu, choose **Save**.



Networks

Profile: ...ility Client\Network Access Manager\system\configuration.xml

Network

Name	Media Type	Group*
Custom-wired	Wired	Global
Custom-wireless	Wireless	Global
Custom-EAP-Chain-wired	Wired	Local networks
Custom-EAP-Chain-Wireless	Wireless	Local networks

This configuration file is updated with the new network configurations.

PROCESS

Enabling Downloadable Access Lists

1. Add Active Directory groups to ISE
2. Create wired access list
3. Create authorization profile
4. Create authorization policy
5. Configure WLC for authorization

You have now configured access for any user who authenticates successfully to be granted full access to the network. The next step will be to provide differentiated access to users based on their AD group. You create an authorization policy that verifies the user's AD group and then applies an access list to the switch or wireless access point for that user.

Procedure 1 Add Active Directory groups to ISE

Step 1: In a browser, access the primary Cisco ISE GUI, **http://ise-1.cisco.local**.

Step 2: On the main menu bar, navigate to **Administration > Identity Management > External Identity Sources**.

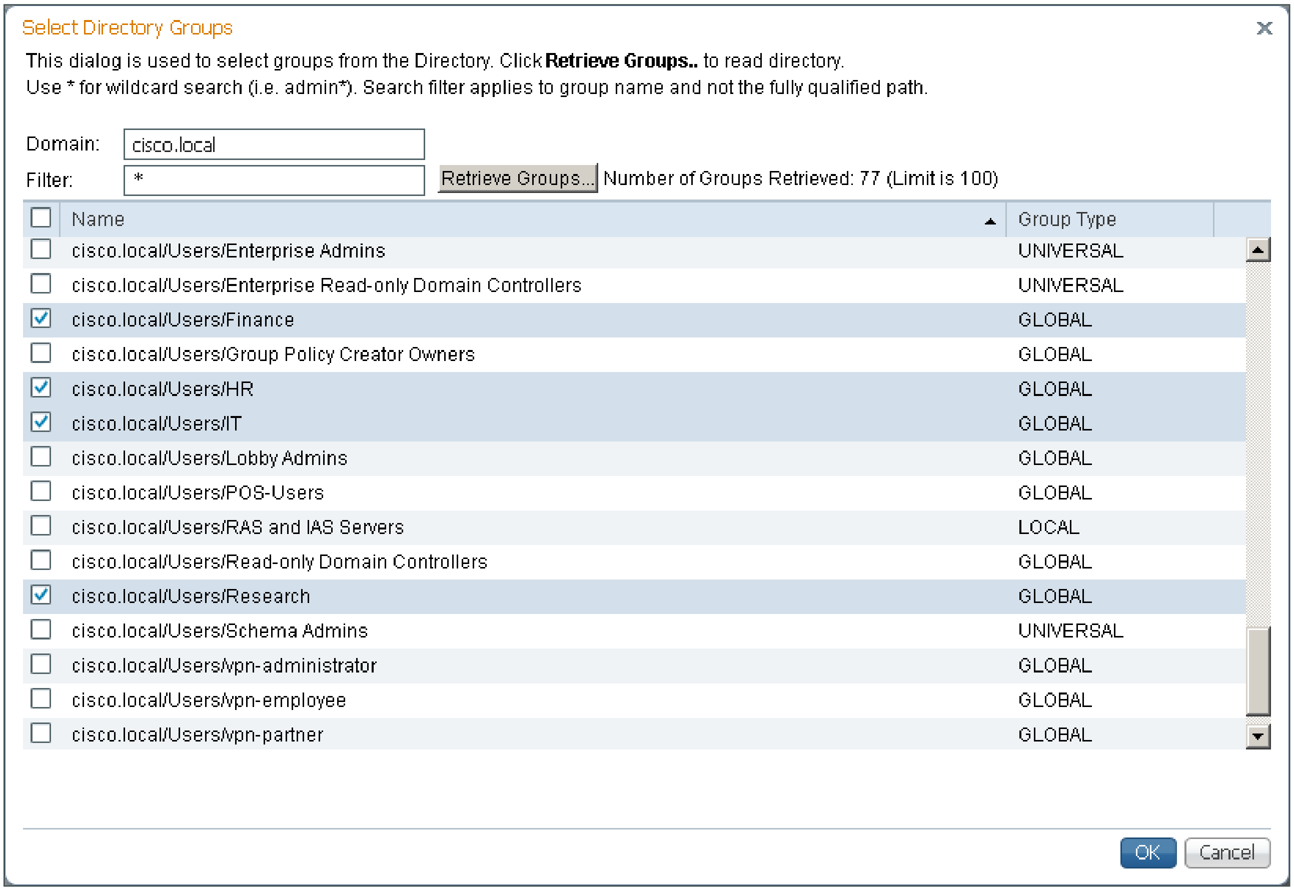
Step 3: In the left panel, click **Active Directory**.

Step 4: Click the Groups tab, click **Add**, and then click **Select Groups from Directory**.

Step 5: Search for the groups you wish to add. The domain box is already filled in. The default filter is a wildcard to list all groups. Click **Retrieve Groups** in order to get a list of all groups in your domain.

Step 6: Select the groups you want to use for authentication, and then click **OK**. In this example deployment, select the following groups:

- **cisco.local/Users/Finance**
- **cisco.local/Users/HR**
- **cisco.local/Users/IT**
- **cisco.local/Users/Research**



This dialog is used to select groups from the Directory. Click **Retrieve Groups..** to read directory.
Use * for wildcard search (i.e. admin*). Search filter applies to group name and not the fully qualified path.

Domain: cisco.local
Filter: *
Number of Groups Retrieved: 77 (Limit is 100)

☐	Name ▲	Group Type
☐	cisco.local/Users/Enterprise Admins	UNIVERSAL
☐	cisco.local/Users/Enterprise Read-only Domain Controllers	UNIVERSAL
☑	cisco.local/Users/Finance	GLOBAL
☐	cisco.local/Users/Group Policy Creator Owners	GLOBAL
☑	cisco.local/Users/HR	GLOBAL
☑	cisco.local/Users/IT	GLOBAL
☐	cisco.local/Users/Lobby Admins	GLOBAL
☐	cisco.local/Users/POS-Users	GLOBAL
☐	cisco.local/Users/RAS and IAS Servers	LOCAL
☐	cisco.local/Users/Read-only Domain Controllers	GLOBAL
☑	cisco.local/Users/Research	GLOBAL
☐	cisco.local/Users/Schema Admins	UNIVERSAL
☐	cisco.local/Users/vpn-administrator	GLOBAL
☐	cisco.local/Users/vpn-employee	GLOBAL
☐	cisco.local/Users/vpn-partner	GLOBAL

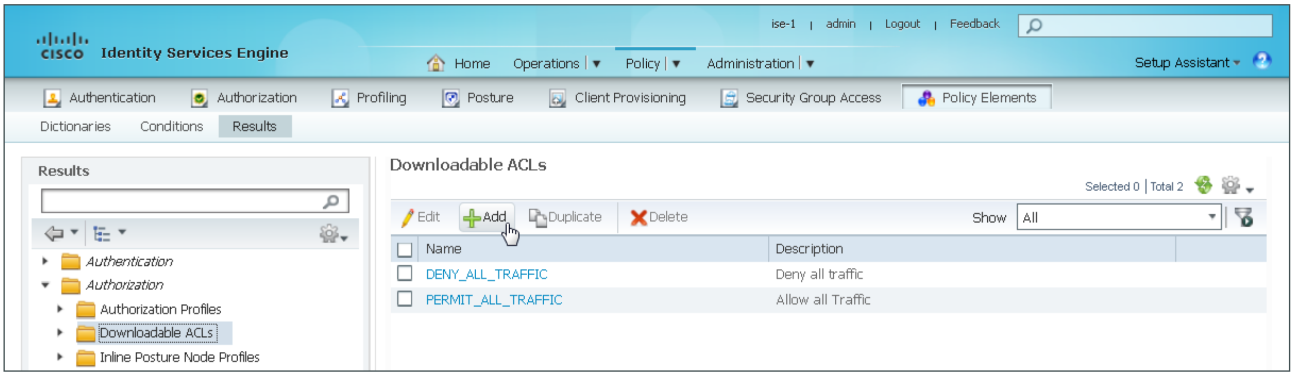
Step 7: Click **Save Configuration**.

Procedure 2 Create wired access list

You need to create an access control list to deploy on the switches, using standard IOS syntax. The ACL limits the portions of the network that members of a group can access.

Step 1: In Cisco ISE, on the main menu bar, navigate to **Policy > Policy Elements > Results**.

Step 2: In the left pane, navigate to **Authorization > Downloadable ACLs**, next to the folder icon click the **Downloadable ACLs** text, and then in the main pane, click **Add**.

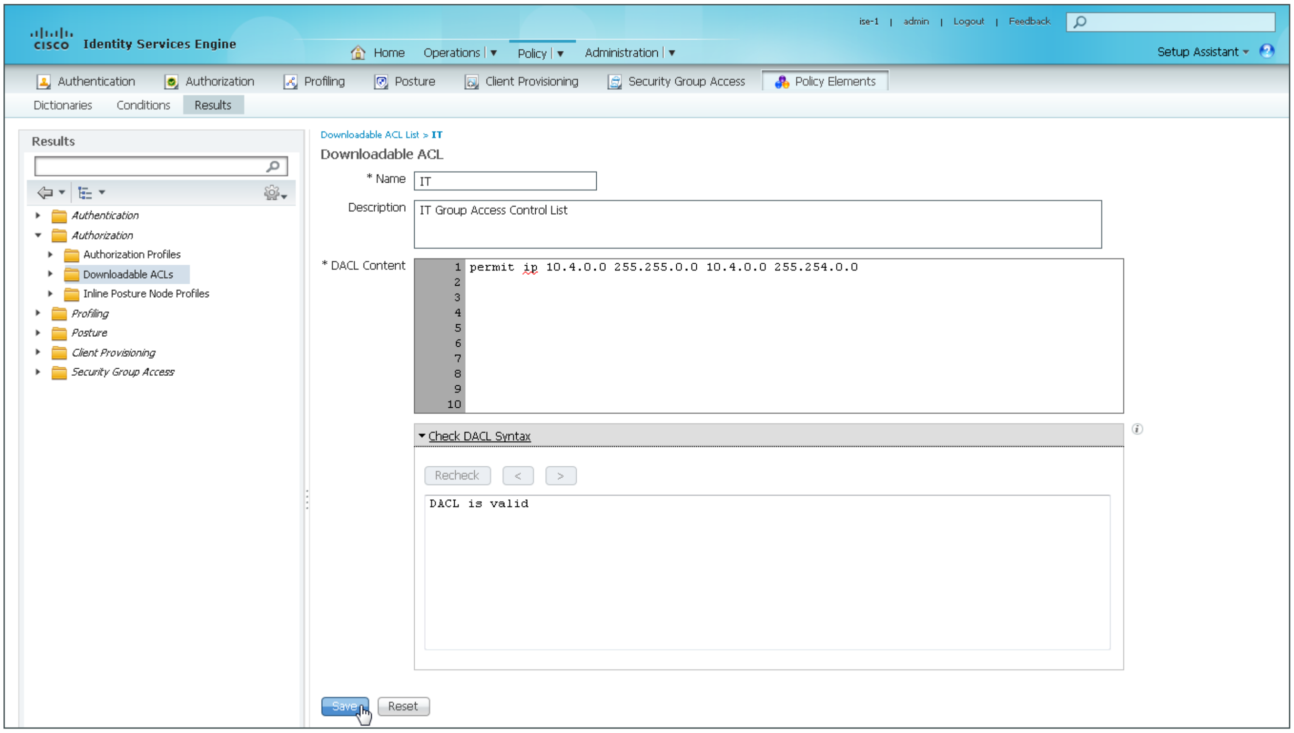


Name	Description
☐ DENY_ALL_TRAFFIC	Deny all traffic
☐ PERMIT_ALL_TRAFFIC	Allow all Traffic

Step 3: Enter a name (Example: IT) and a description for the policy.

Step 4: In the DACL content section, enter the ACL by using IOS syntax.

Step 5: Click **Check DACL Syntax** to validate, and then click **Submit**. The Downloadable ACL is now defined and ready to be referenced.



* Name: IT

Description: IT Group Access Control List

* DACL Content:

```
permit ip 10.4.0.0 255.255.0.0 10.4.0.0 255.254.0.0
```

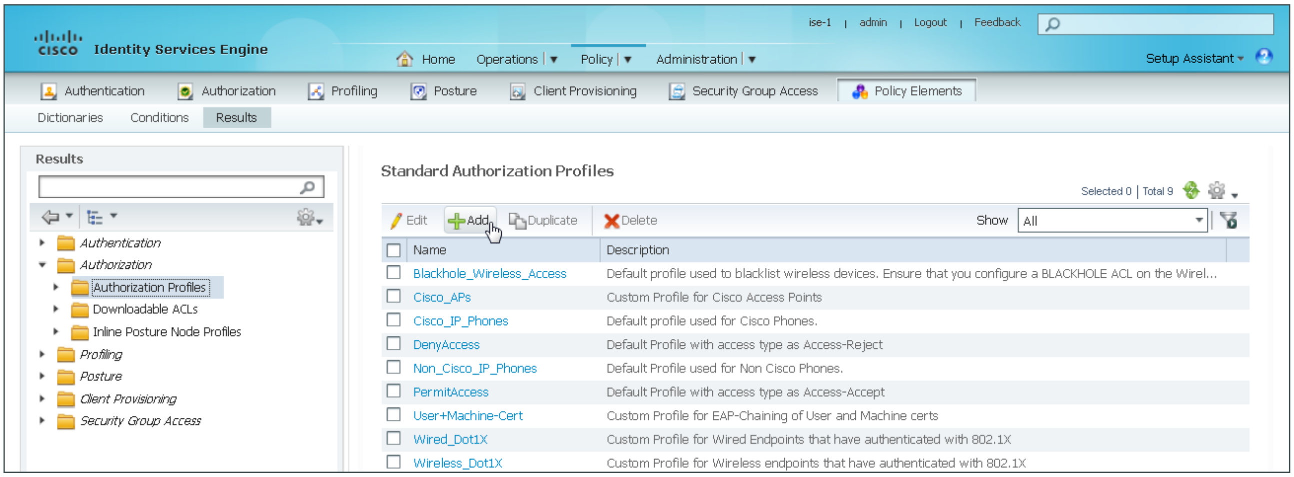
```
DACL is valid
```

Procedure 3 Create authorization profile

An authorization profile defines the specific access policies granted to the device. You will create a policy to apply an access list to the access device to limit what the endpoint has access to on the network.

Step 1: In Cisco ISE, on the main menu bar, navigate to **Policy > Policy Elements > Results**.

Step 2: In the left pane, navigate to **Authorization > Authorization Profiles**, next to the folder icon, click the **Authorization Profiles** text, and then in the main pane, click **Add**.



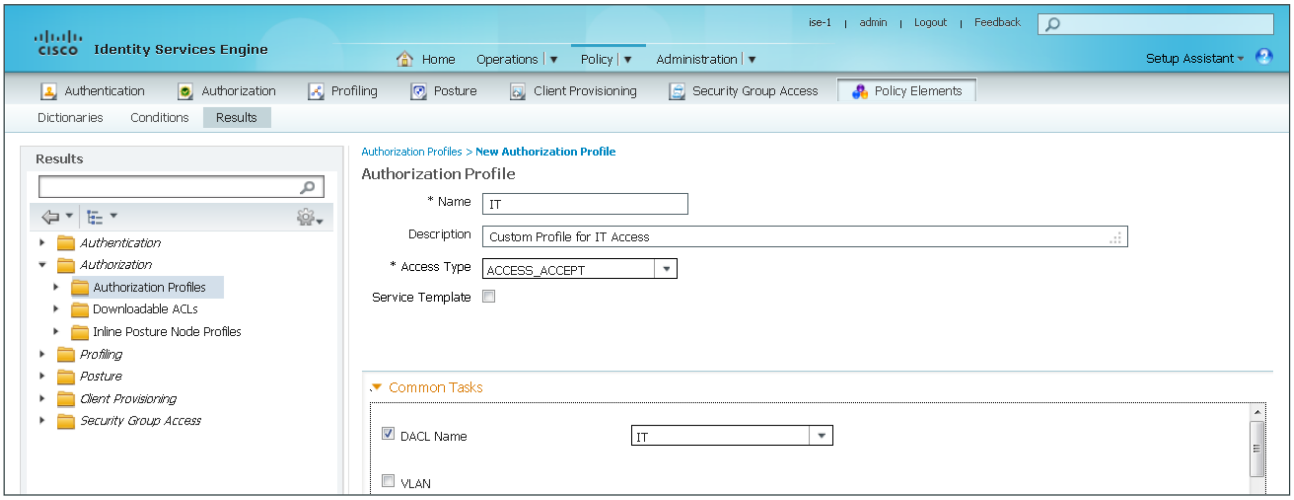
☐ Name	Description
☐ Blackhole_Wireless_Access	Default profile used to blacklist wireless devices. Ensure that you configure a BLACKHOLE ACL on the Wirel...
☐ Cisco_APs	Custom Profile for Cisco Access Points
☐ Cisco_IP_Phones	Default profile used for Cisco Phones.
☐ DenyAccess	Default Profile with access type as Access-Reject
☐ Non_Cisco_IP_Phones	Default Profile used for Non Cisco Phones.
☐ PermitAccess	Default Profile with access type as Access-Accept
☐ User+Machine-Cert	Custom Profile for EAP-Chaining of User and Machine certs
☐ Wired_Dot1X	Custom Profile for Wired Endpoints that have authenticated with 802.1X
☐ Wireless_Dot1X	Custom Profile for Wireless endpoints that have authenticated with 802.1X

Step 3: In the Authorization Profile, add the Name (Example: IT).

Step 4: Add a Description.

Step 5: In the Common Tasks section, select **DACL Name**.

Step 6: Select the ACL that you configured in Procedure 2, "Create wired access list" (Example: IT).



* Name: IT

Description: Custom Profile for IT Access

* Access Type: ACCESS_ACCEPT

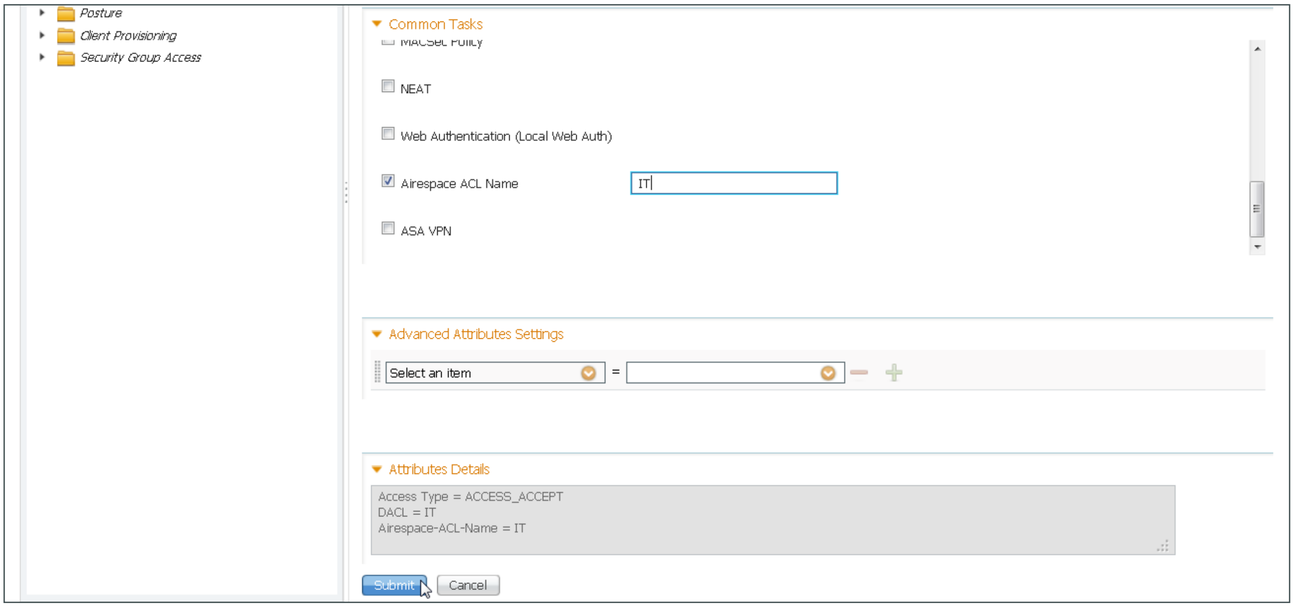
Service Template ☐

☑ DACL Name: IT

☐ VLAN

Step 7: In the Common Tasks section, scroll to view and select **Airespace ACL Name**.

Step 8: Enter the name of the ACL that you are applying to the WLC (Example: IT), and then click **Submit**. The profile you created is added to the Standard Authorization Profiles.



☐ NEAT

☐ Web Authentication (Local Web Auth)

☑ Airespace ACL Name: IT

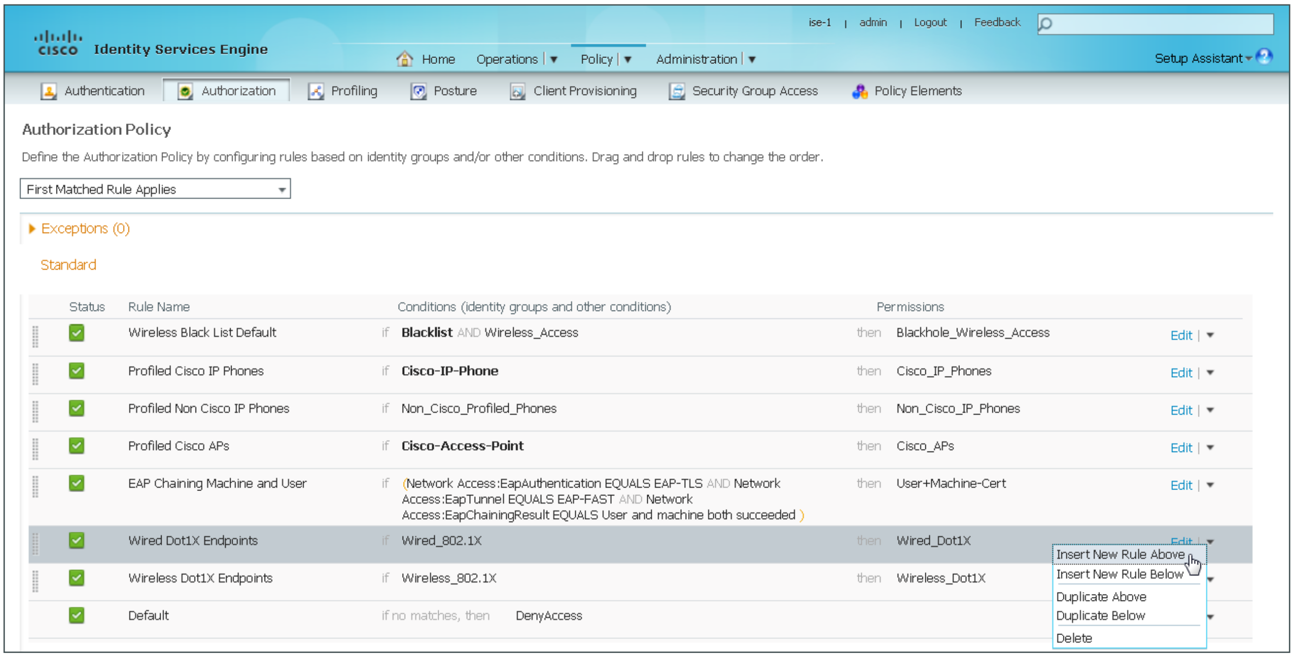
☐ ASA VPN

```
Access Type = ACCESS_ACCEPT
DACL = IT
Airespace-ACL-Name = IT
```

Procedure 4 Create authorization policy

Step 1: In Cisco ISE, on the main menu bar, navigate to **Policy > Authorization**.

Step 2: In the row for the Wired Dot1X Endpoints rule, on the right, click the black triangle symbol, and then select **Insert New Rule Above**. A new rule named **Standard Rule 1** is created.



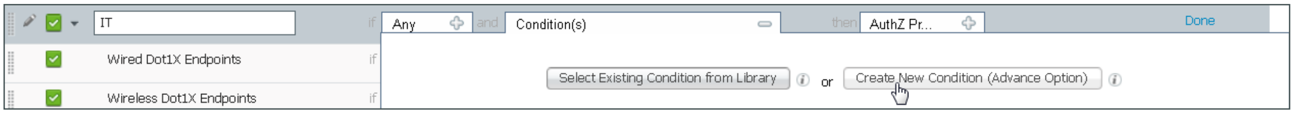
Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

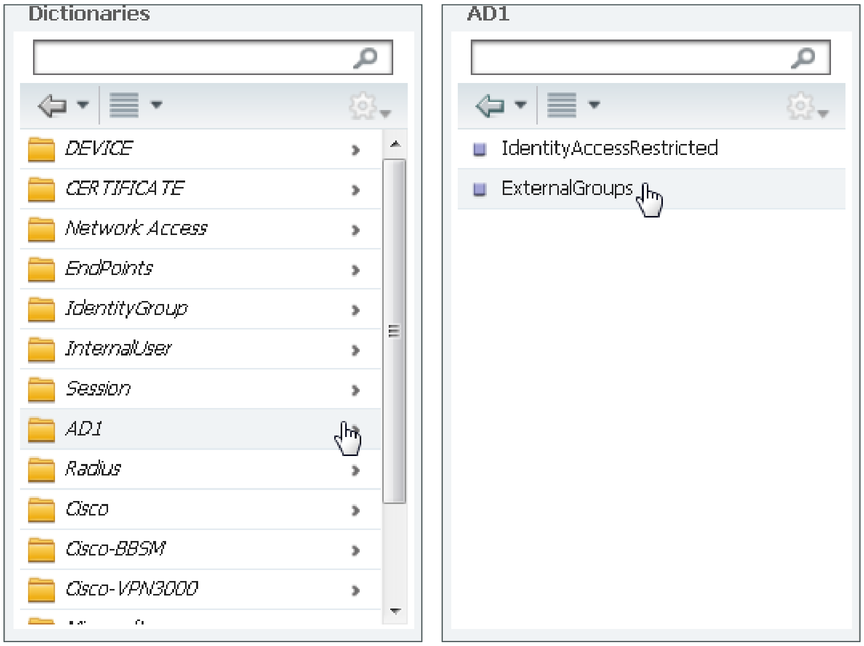
Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
✓	Wireless Black List Default	if	**Blacklist** AND Wireless_Access	then	Blackhole_Wireless_Access	Edit
✓	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones	Edit
✓	Profiled Non Cisco IP Phones	if	Non_Cisco_Profiled_Phones	then	Non_Cisco_IP_Phones	Edit
✓	Profiled Cisco APs	if	**Cisco-Access-Point**	then	Cisco_APs	Edit
✓	EAP Chaining Machine and User	if	(Network Access:EapAuthentication EQUALS EAP-TLS AND Network Access:EapTunnel EQUALS EAP-FAST AND Network Access:EapChainingResult EQUALS User and machine both succeeded)	then	User+Machine-Cert	Edit
✓	Wired Dot1X Endpoints	if	Wired_802.1X	then	Wired_Dot1X	Edit
✓	Wireless Dot1X Endpoints	if	Wireless_802.1X	then	Wireless_Dot1X	
✓	Default	if no matches, then	DenyAccess			

Step 3: Rename new rule to **IT**.

Step 4: In the **Condition(s)** list, choose the **+** symbol, and then click **Create New Condition (Advance Option)**.



Step 5: In the Expression column, in the **Select Attribute** list, select **AD1**, and then choose **ExternalGroups**.

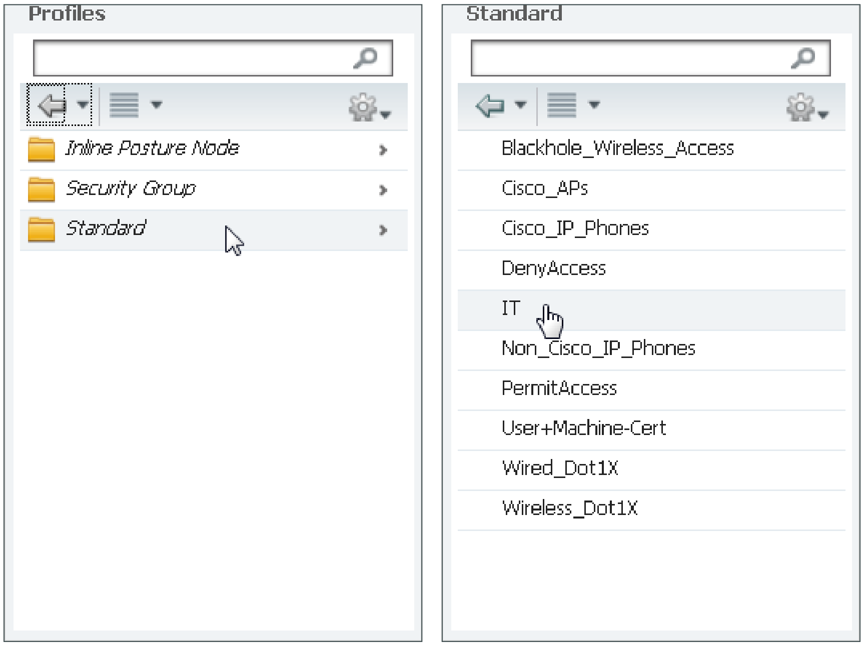


Step 6: In the next column, choose **Equals**.

Step 7: In the final column, choose **cisco.local/Users/IT**.

Step 8: In the Permissions column, next to AuthZ Profile(s), click the **+** symbol.

Step 9: In the **Select an item** list, select **Standard**, and then select the IT authorization profile that was created in Procedure 3, “Create authorization profile.”



Step 10: Click **Done**, and then click **Save**.

Step 11: For each group requiring a policy, repeat Procedure 2, “Create wired access list,” Procedure 3, “Create authorization profile,” and Procedure 4, “Create authorization policy.” In this example deployment, in addition to the IT policy, you create additional policies for the Finance, HR, and Research groups.

Procedure 5 Configure WLC for authorization

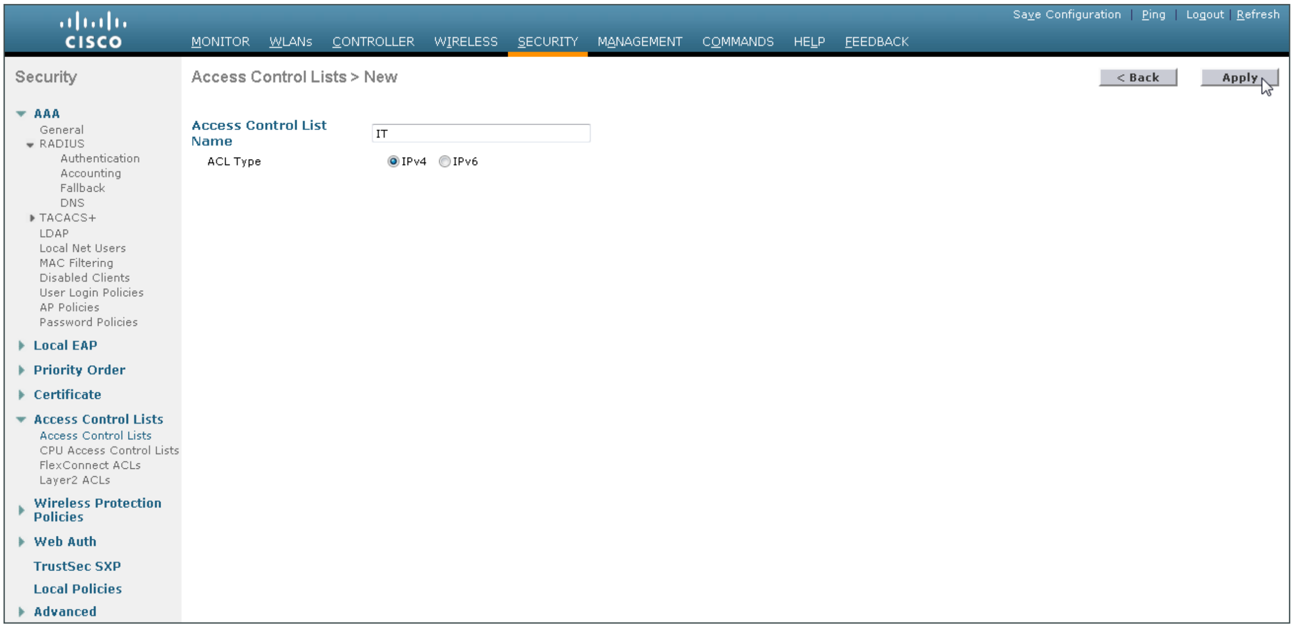
Configure every WLC in the environment, with the exception of the guest WLC in the DMZ, with access lists to support these newly defined policies. Each ACL that is referenced by the authorization profiles needs to be defined on the WLC. When clients connect to the WLC and authenticate, in the campus and at remote sites with a local controller, WLC Cisco ISE passes a RADIUS attribute requesting that the ACL be applied for this client.

Step 1: Use a web browser to connect and login to the WLC console (Example: https://wlc1.cisco.local).

Step 2: On the menu bar, click **Security**.

Step 3: In the left pane, expand **Access Control Lists**, click **Access Control Lists**, and then click **New**.

Step 4: Name the access list, and then click **Apply**.



Access Control Lists > New

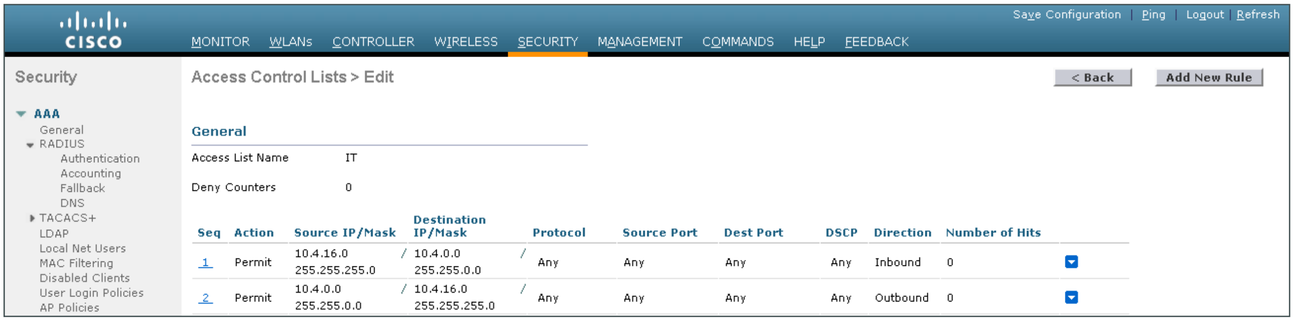
Access Control List Name: IT

ACL Type ● IPv4 ○ IPv6

Step 5: Click the name in the list. This allows you to edit the newly created access list.

Step 6: Click **Add New Rule**.

Step 7: Create a new access list rule based on your security policy, and then click **Apply**. In this example deployment, members of the IT group are only allowed access to the internal network (10.4.0.0/16).



Access Control Lists > Edit

General

Access List Name IT

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	10.4.16.0 / 255.255.255.0	10.4.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0
2	Permit	10.4.0.0 / 255.255.0.0	10.4.16.0 / 255.255.255.0	Any	Any	Any	Any	Outbound	0

Tech Tip

The access list needs to have entries for the traffic in both directions, so make sure you have pairs of access list rules for both inbound and outbound traffic. Also, there is an implicit "deny all" rule at the end of the access list so any traffic not explicitly permitted is denied.

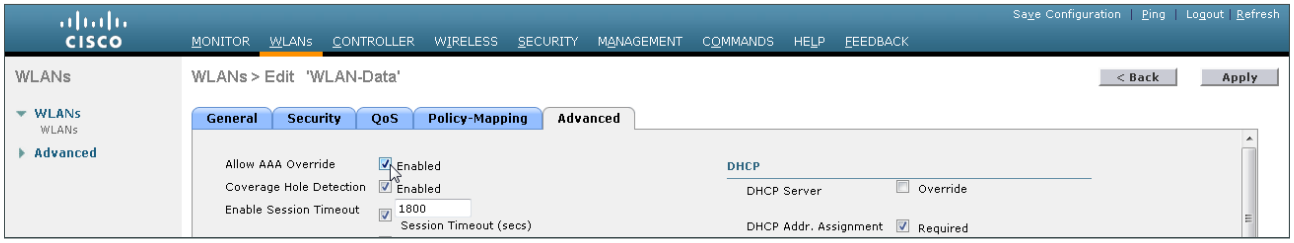
Step 8: For each access list that you defined in the authorization profiles in Cisco ISE, repeat Step 3 through Step 7 in this procedure.

Next, you enable WLC in order to allow Cisco ISE to use RADIUS to override the current settings, so that the access list can be applied to the wireless LAN.

Step 9: On the WLC menu bar, click **WLANs**.

Step 10: Click the WLAN ID of the wireless network that the wireless personal devices are accessing.

Step 11: Click **Advanced**, and then select **Allow AAA Override**.



WLANs > Edit 'WLAN-Data'

Allow AAA Override ☑ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)

DHCP
DHCP Server ☐ Override
DHCP Addr. Assignment ☑ Required

Step 12: Click **Apply**, and then click **Save Configuration.**

PROCESS

Enabling Security Group Access

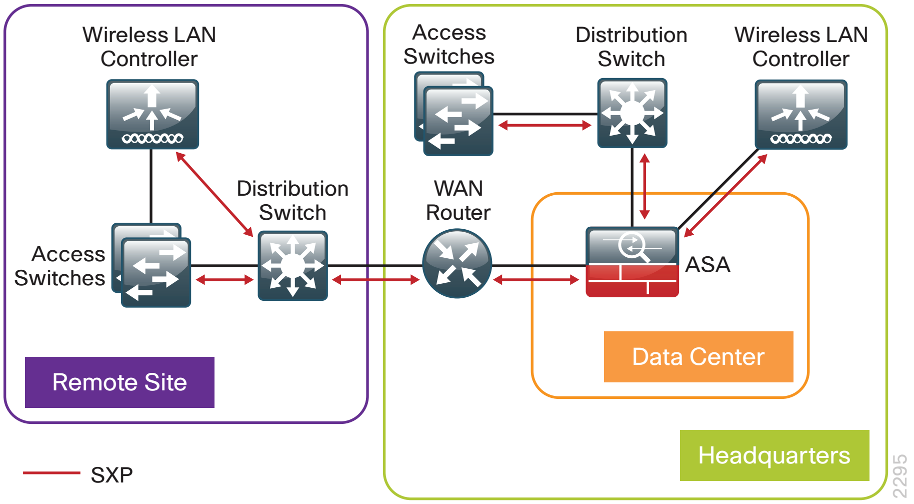
1. Define Security Group Tags
2. Add Cisco ASA as a network device
3. Modify authorization policy
4. Configure SXP on IOS devices
5. Configure SXP on WLCs
6. Configure SXP on ASA
7. Configure firewall policy
8. Monitoring SGTs on Cisco ASA
9. Monitoring SGTs on the switches
10. Monitoring SGTs on the WLC

SGA technology allows user identity information to be associated with their network traffic and then passed throughout the network. This information can then be used to enforce an access policy using SGT and SGACL.

SXP is used to propagate the IP-to-SGT bindings across network devices that do not support SGTs. In this example, we are passing SGT information from the access layer devices to Cisco ASA in the data center.

SXP establishes a peering relationship between two devices to exchange the IP-to-SGT bindings. There are two roles in the relationship: the speaker and the listener. The speaker passes the IP-to-SGT bindings to the listener. In our example, the access layer switch needs to pass these bindings to Cisco ASA in the data center. You could have the switch peer directly with the ASA appliance, however, that may not scale well in larger environments. It is a best practice to minimize the number or peers a device has by aggregating connections.

For example, campus access layer switches would peer with a distribution switch, which then would peer with the ASA appliance. Or, access layer switches at a remote site would peer with a distribution switch at the site, which would peer with the WAN aggregation router at the headquarters, which would then peer with the ASA appliance.



Procedure 1 Define Security Group Tags

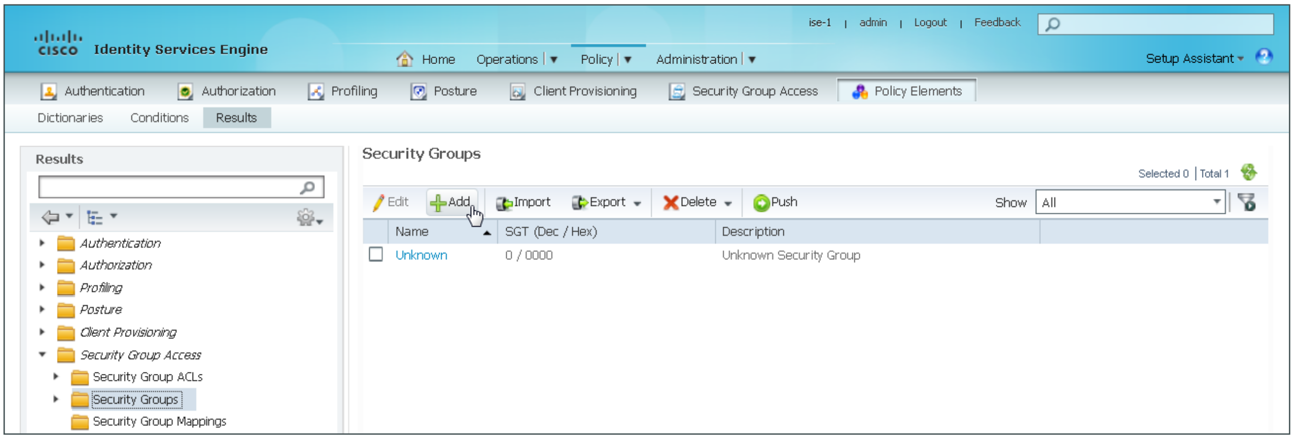
Step 1: Connect to the primary Cisco ISE GUI, **http://ise-1.cisco.local**.

Step 2: On the main menu bar, navigate to **Policy > Policy Elements > Results**.

Step 3: In the left pane, navigate to **Security Group Access > Security Groups**.

Step 4: Next to the folder icon, click the **Security Groups** text.

Step 5: In the main Security Groups pane, click **Add**.

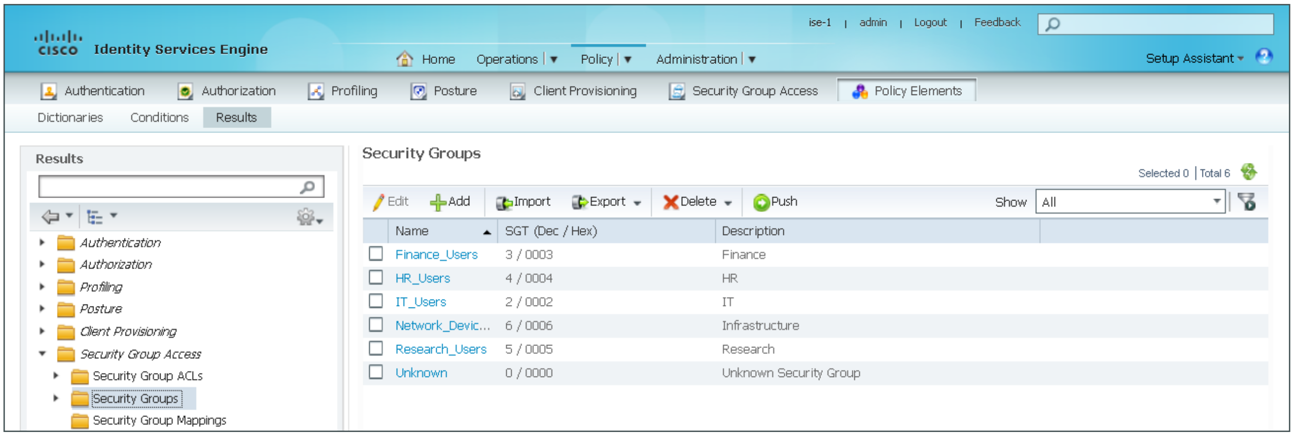


Name	SGT (Dec / Hex)	Description
☐ Unknown	0 / 0000	Unknown Security Group

Step 6: Give the group a name and description, and then click **Submit**.

Step 7: For each tag you wish to create, repeat Step 5 and Step 6. In this example deployment, you create tags for each of the following groups: IT_Users, Finance_Users, HR_Users, Research_Users, and Network_Devices.

The security groups are created.



Security Groups

Name	SGT (Dec / Hex)	Description
Finance_Users	3 / 0003	Finance
HR_Users	4 / 0004	HR
IT_Users	2 / 0002	IT
Network_Devic...	6 / 0006	Infrastructure
Research_Users	5 / 0005	Research
Unknown	0 / 0000	Unknown Security Group

Procedure 2 Add Cisco ASA as a network device

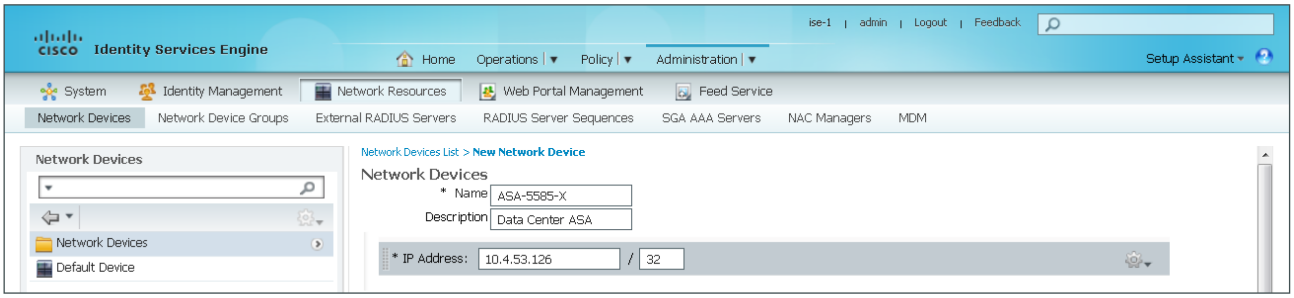
In order to allow Cisco ISE to provide SGT enforcement on Cisco ASA, the ASA appliance needs to be added as a network device in ISE.

Step 1: In Cisco ISE, on the main menu bar, navigate to **Administration > Network Resources, > Network Devices**, and then in the main Network Devices pane, click **Add**.

Step 2: Enter the ASA appliance name.

Step 3: Enter a Description.

Step 4: Enter the IP address (Example: ASA-5585-X, Data Center ASA, 10.4.53.126).



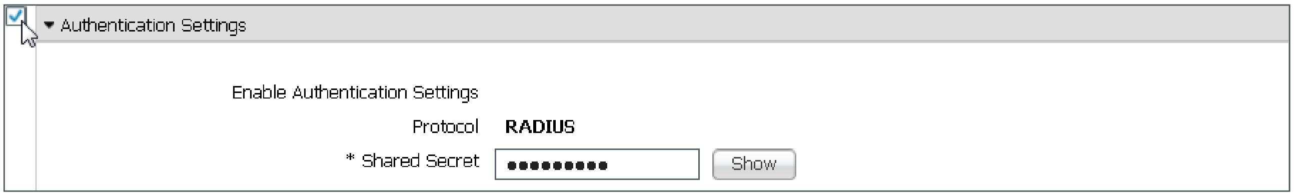
Network Devices

* Name ASA-5585-X

Description Data Center ASA

* IP Address: 10.4.53.126 / 32

Step 5: Select **Authentication Settings**, and then enter the RADIUS shared secret.



☑ Authentication Settings

Enable Authentication Settings

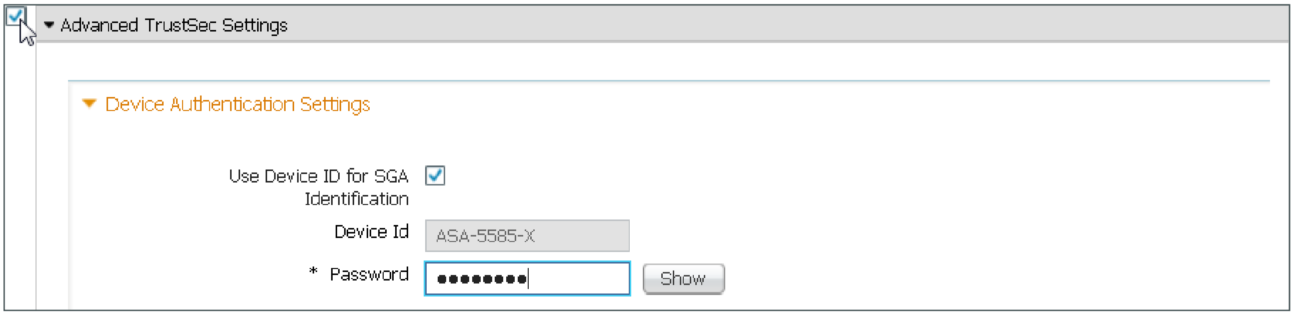
Protocol **RADIUS**

* Shared Secret ●●●●●●●●●●

Step 6: Select **Advanced TrustSec Settings**.

Step 7: In the Device Authentication Settings section, verify that **Use Device ID for SGA Identification** is selected.

Step 8: Enter a password.



☑ Advanced TrustSec Settings

Device Authentication Settings

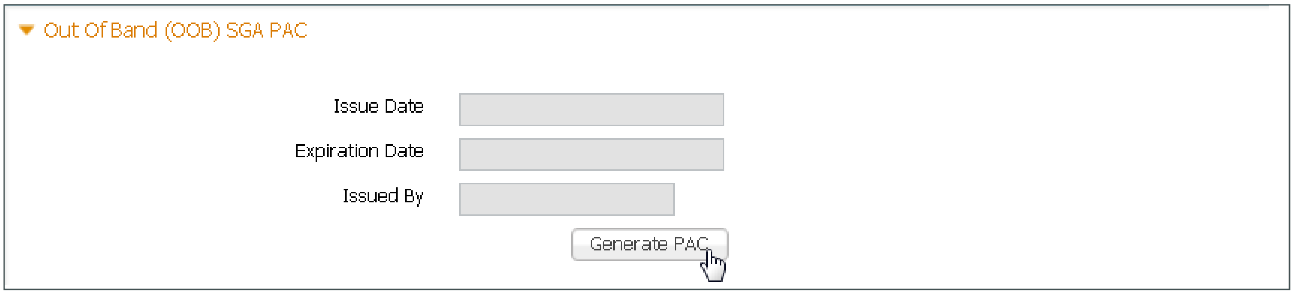
Use Device ID for SGA Identification ☑

Device Id: ASA-5585-X

* Password: ●●●●●●●●●

Step 9: In the SGA Notifications and Updates section, accept the default values.

Step 10: In the Out of Band (OOB) SGA PAC section, click **Generate PAC**.



Out Of Band (OOB) SGA PAC

Step 11: Enter an encryption key and the PAC time to live, and then click **Generate PAC**. You are prompted to save the file to your local machine.

Step 12: Choose a location, and then click **OK**.

Step 13: Click **Submit**.

Procedure 3 Modify authorization policy

In Procedure 4, “Create authorization policy,” of the previous process, you created authorization policies that limited network access based on Active Directory group membership by using access lists. In this procedure, you modify those policies to use SGTs instead.

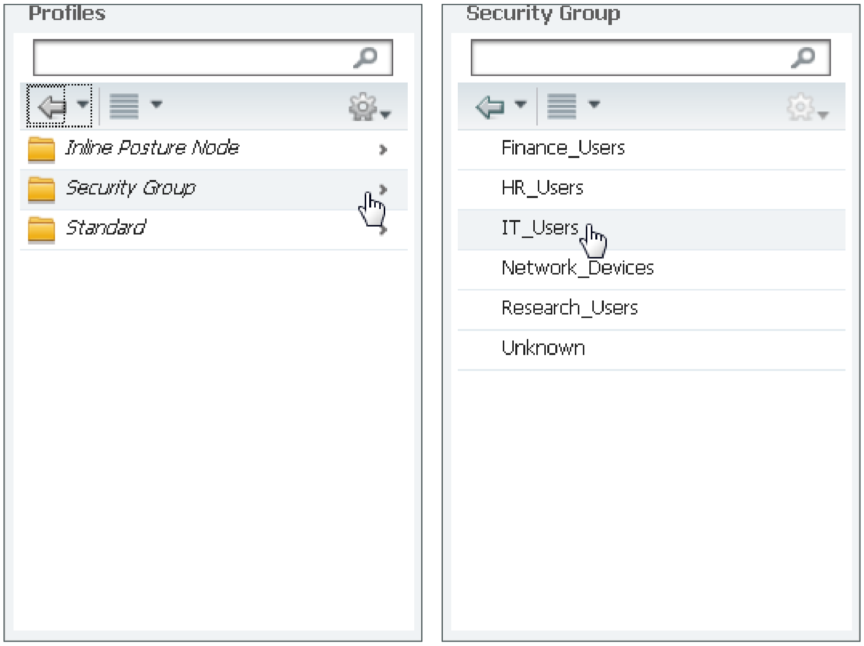
Step 1: In Cisco ISE, on the main menu bar, navigate to **Policy > Authorization**.

Step 2: For the IT rule, click **Edit**.

Step 3: In the Permissions column, click the **+** symbol next to IT.

Step 4: Click the **+** symbol in order to add a new permission.

Step 5: In the **Select an Item** list, select **Security Group**, and then select **IT_Users**.



Step 6: Click **Done**, and then click **Save**.

Step 7: For each policy you need to modify to support SGTs, repeat Step 2 through Step 6. In this example deployment, you modify the Finance, HR, and Research policies.

Procedure 4 Configure SXP on IOS devices

Next, you enable SXP by configuring the devices using the IOS CLI.

Step 1: On IOS devices in configuration mode, enable SXP.

```
cts sxp enable
cts sxp default password [sxp password]
cts sxp default source-ip [Local IP address]
cts sxp connection peer [Peer IP address] password default mode local speaker
```

Step 2: For each IOS device where you need to configure SXP, repeat this procedure.

Procedure 5 Configure SXP on WLCs

Step 1: Navigate to the WLC console (Example: https://wlc1.cisco.local).

Step 2: On the menu bar, click **Security**.

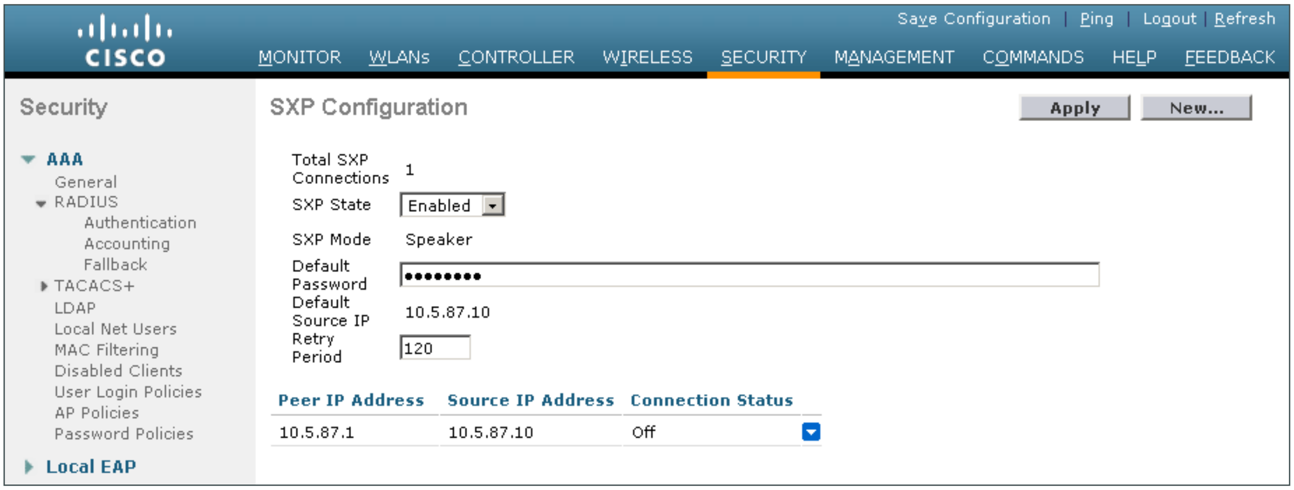
Step 3: In the left pane, click **TrustSec SXP**.

Step 4: In **SXP State**, select **Enabled**.

Step 5: Enter a Default Password, and then click Apply. This password must match what is configured on the peer.

Step 6: Click **New.**

Step 7: Enter the IP address of the new peer, and then click **Apply**. The SXP Configuration page appears.



SXP Configuration

Total SXP Connections 1
SXP State Enabled
SXP Mode Speaker
Default Password ●●●●●●●●●
Default Source IP 10.5.87.10
Retry Period 120

Peer IP Address	Source IP Address	Connection Status
10.5.87.1	10.5.87.10	Off

Step 8: Click **Apply**, and then at top, click **Save Configuration**.

Procedure 6 Configure SXP on ASA

You now configure SXP on Cisco ASA and create a policy that limits access to servers in the data center based on the SGTs.

Step 1: In a browser, navigate to the Cisco ASA management console (Example: https://DC-ASA5585X.cisco.local), and then click **Run ASDM**. You may be prompted to install a specific version of Java Runtime Engine.

Step 2: Navigate to **Configuration > Firewall > Identity by TrustSec**.

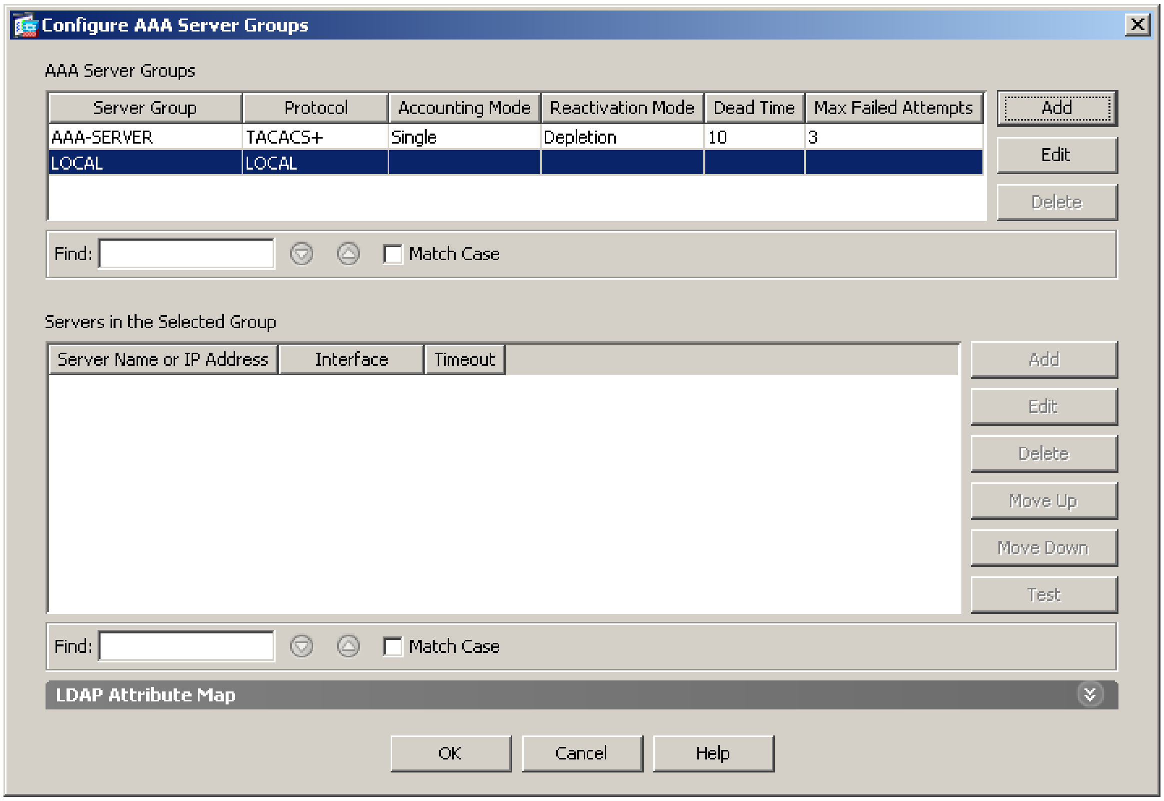
Step 3: Select **Enable SGT Exchange Protocol (SXP)**.

Step 4: In the **Default Source** box, enter the IP address of the interface of the Cisco ASA appliance used for management.

Step 5: Enter a password, and then verify it.

Step 6: In the Server Group Setup section, click **Manage**.

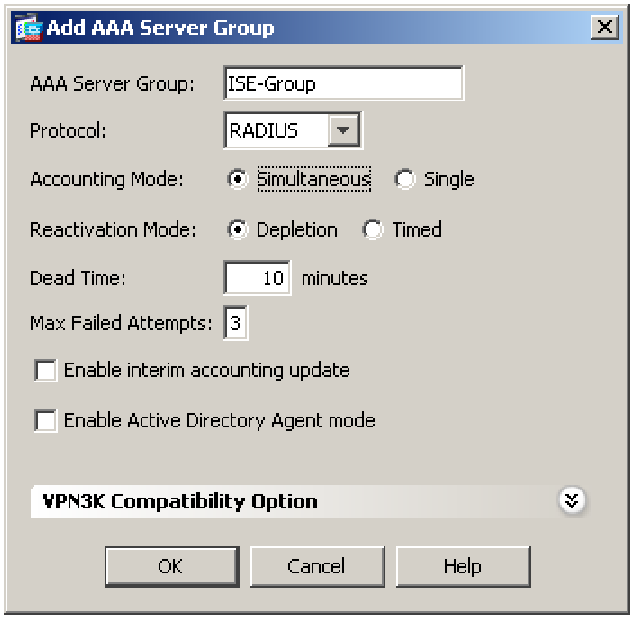
Step 7: In the Configure AAA Server Group window, click **Add**.



Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts
AAA-SERVER	TACACS+	Single	Depletion	10	3
LOCAL	LOCAL				

Step 8: In the AAA Server Group box, enter **ISE-Group**.

Step 9: For Accounting Mode, select **Simultaneous**, and then click **OK**.



AAA Server Group: ISE-Group
Protocol: RADIUS
Accounting Mode: ● Simultaneous ○ Single
Reactivation Mode: ● Depletion ○ Timed
Dead Time: 10 minutes
Max Failed Attempts: 3
☐ Enable interim accounting update
☐ Enable Active Directory Agent mode

Step 10: In the Servers in Selected Group section, click **Add**.

Step 11: In the **Interface Name** list, choose the firewall interface **outside**.

Step 12: In the **Server Name or IP Address** box, enter **ise-3.cisco.local**.

Step 13: In the RADIUS Parameters section, in **Server Authentication Port**, replace 1645 with **1812**.

Step 14: In **Server Accounting Port**, replace 1646 with **1813**.

Step 15: Enter the **Server Secret Key**.

Step 16: Accept the defaults for the remaining parameters, and then click **OK**.

Step 17: For the second Cisco ISE policy service node (**ise-4.cisco.local)**, repeat Step 10 through Step 13.

Step 18: Click **OK**. The Configure AAA Server Groups window closes.

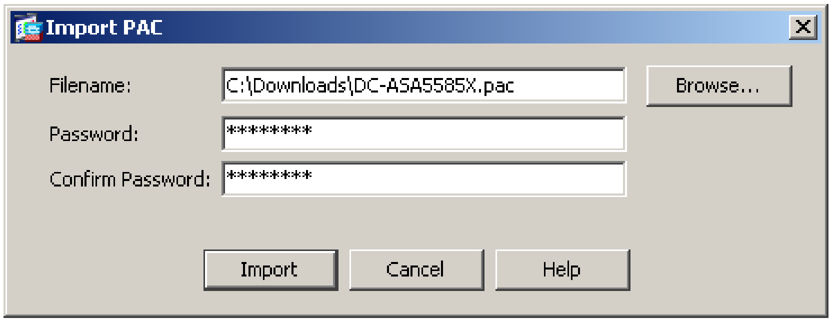
Step 19: Click **Import PAC**.

Step 20: Click **Browse**.

Step 21: Locate the PAC file you saved to your machine in Procedure 2, "Add Cisco ASA as a network device."

Step 22: Enter the PAC password, and then confirm it.

Step 23: Click **Import**.



Filename: C:\Downloads\DC-ASA5585X.pac
Password: ********
Confirm Password: ********

Step 24: When the import is complete, acknowledge the "PAC Imported Successfully" message.

Now you add SXP peers to Cisco ASA.

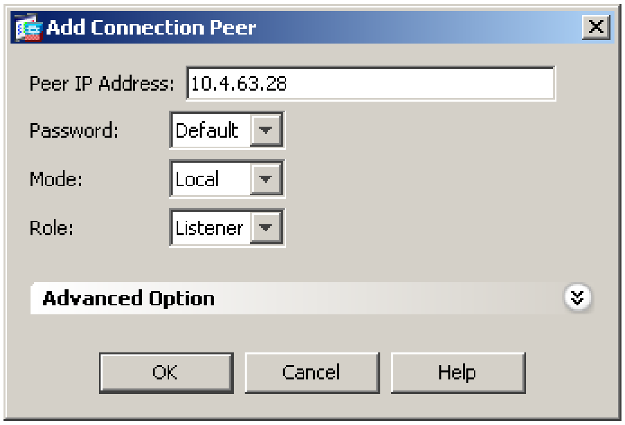
Step 25: Click **Add**.

Step 26: Enter the IP address of the peer.

Step 27: In the **Password** list, choose **Default**.

Step 28: In the Mode list, choose **Local**.

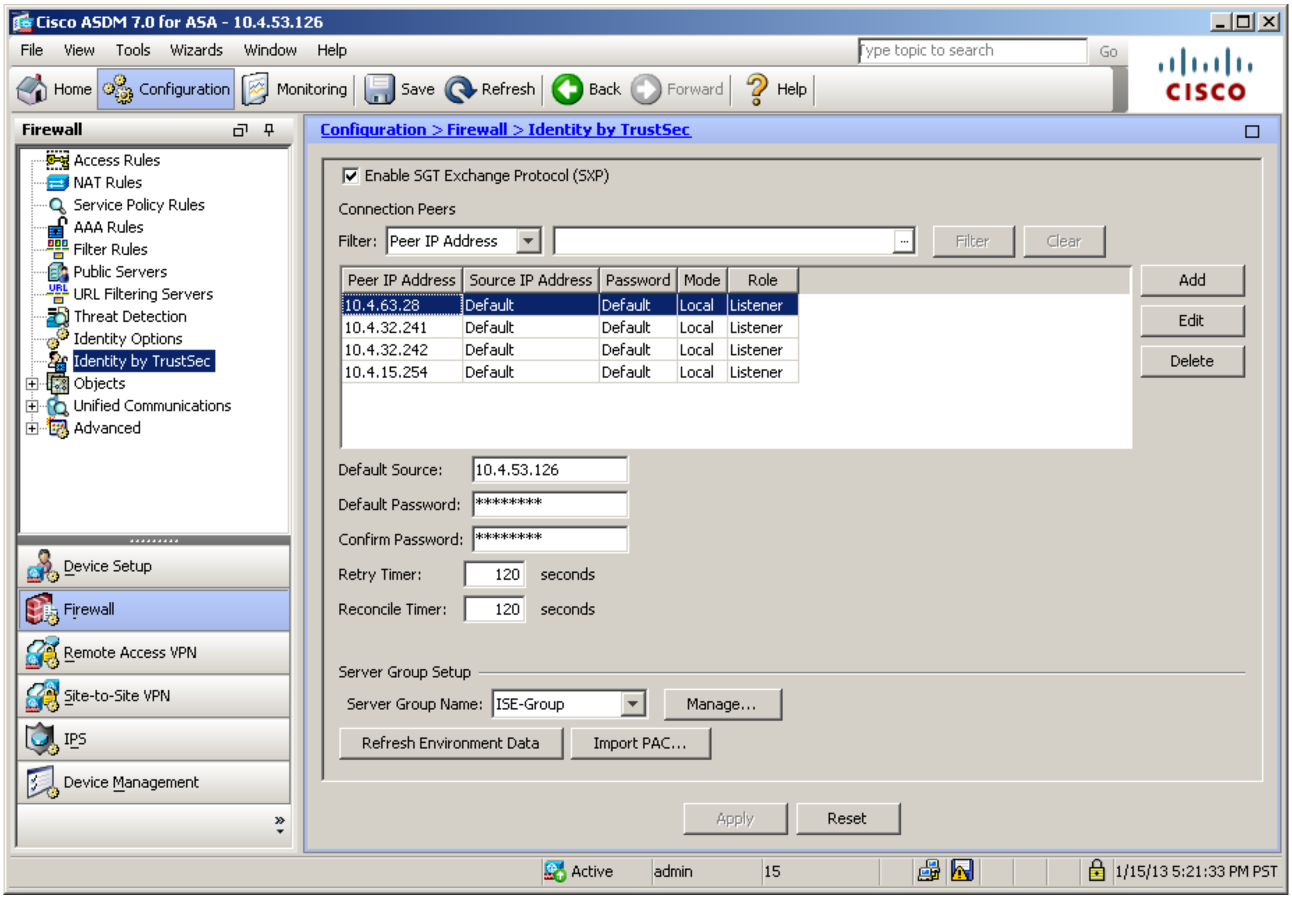
Step 29: In the **Role** list, choose **Listener**, and then click **OK**.



Peer IP Address: 10.4.63.28
Password: Default
Mode: Local
Role: Listener

Step 30: For each peer you need to add, repeat repeat Step 25 through 29.

Step 31: Click **Apply**.



☑ Enable SGT Exchange Protocol (SXP)

Connection Peers

Filter: Peer IP Address

Peer IP Address	Source IP Address	Password	Mode	Role
10.4.63.28	Default	Default	Local	Listener
10.4.32.241	Default	Default	Local	Listener
10.4.32.242	Default	Default	Local	Listener
10.4.15.254	Default	Default	Local	Listener

Default Source: 10.4.53.126
Default Password: ********
Confirm Password: ********
Retry Timer: 120 seconds
Reconcile Timer: 120 seconds

Server Group Setup
Server Group Name: ISE-Group

Procedure 7 Configure firewall policy

In the Data Center Technology Design Guide, organizational servers are defined. In this procedure, you create policy to limit access to each server based on SGTs. In this example, you create a rule for the server for the IT group.

Step 1: In Cisco ASDM, navigate to **Configuration** > **Firewall** > **Access Rules**.

Step 2: In the Access Rules pane, click **Add**.

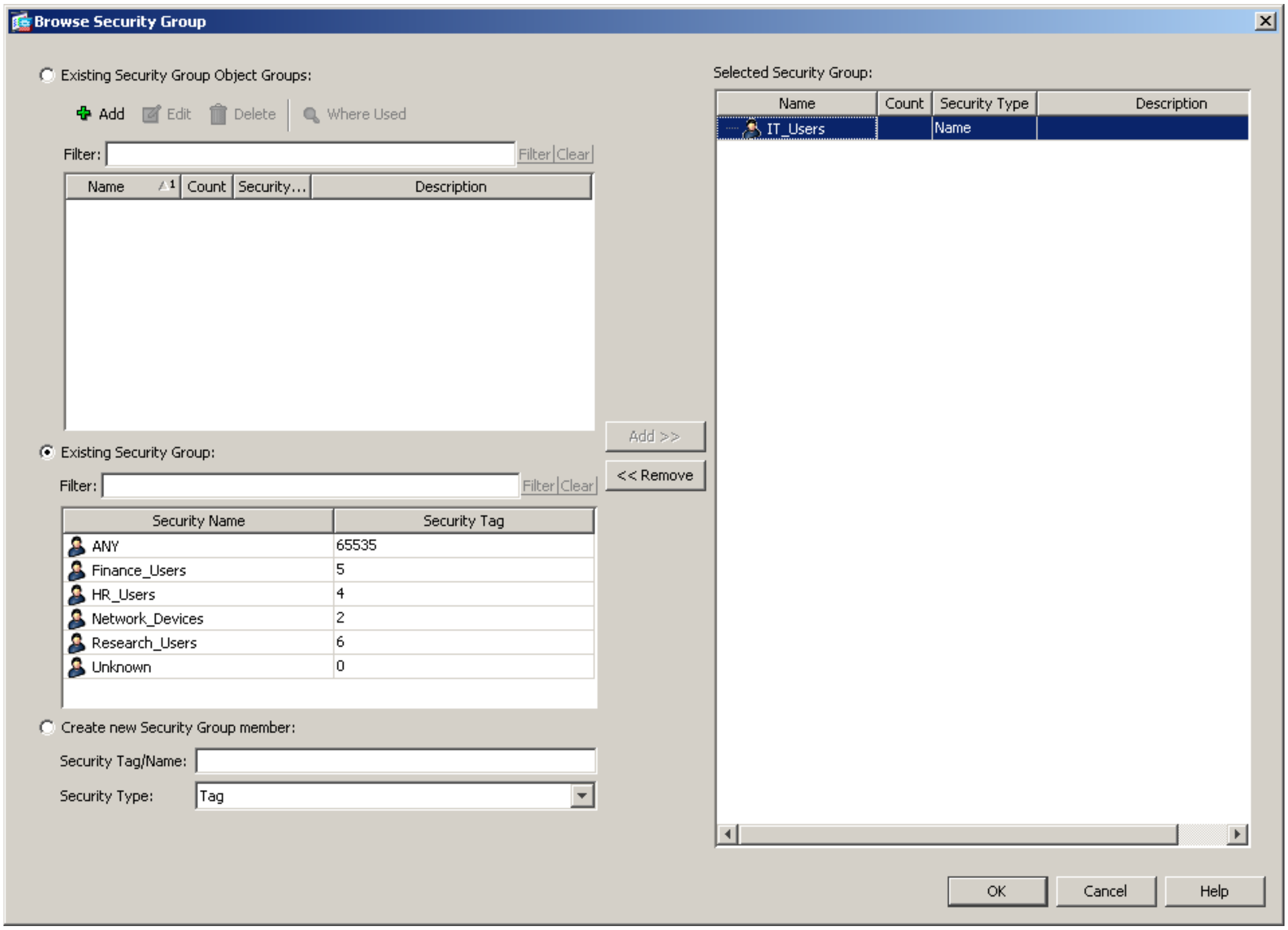
Step 3: From the Interface menu, choose **Any**.

Step 4: Select the **Permit** action.

Step 5: In the Source Criteria section, enter the source **any**, and then click the ellipses at the end of Security Group.

Step 6: Choose **Existing Security Group**.

Step 7: Select **IT_Users**, and then click **Add**.



○ Existing Security Group Object Groups:

Name	Count	Security...	Description

● Existing Security Group:

Security Name	Security Tag
ANY	65535
Finance_Users	5
HR_Users	4
Network_Devices	2
Research_Users	6
Unknown	0

○ Create new Security Group member:

Security Tag/Name:

Security Type: Tag

Selected Security Group:

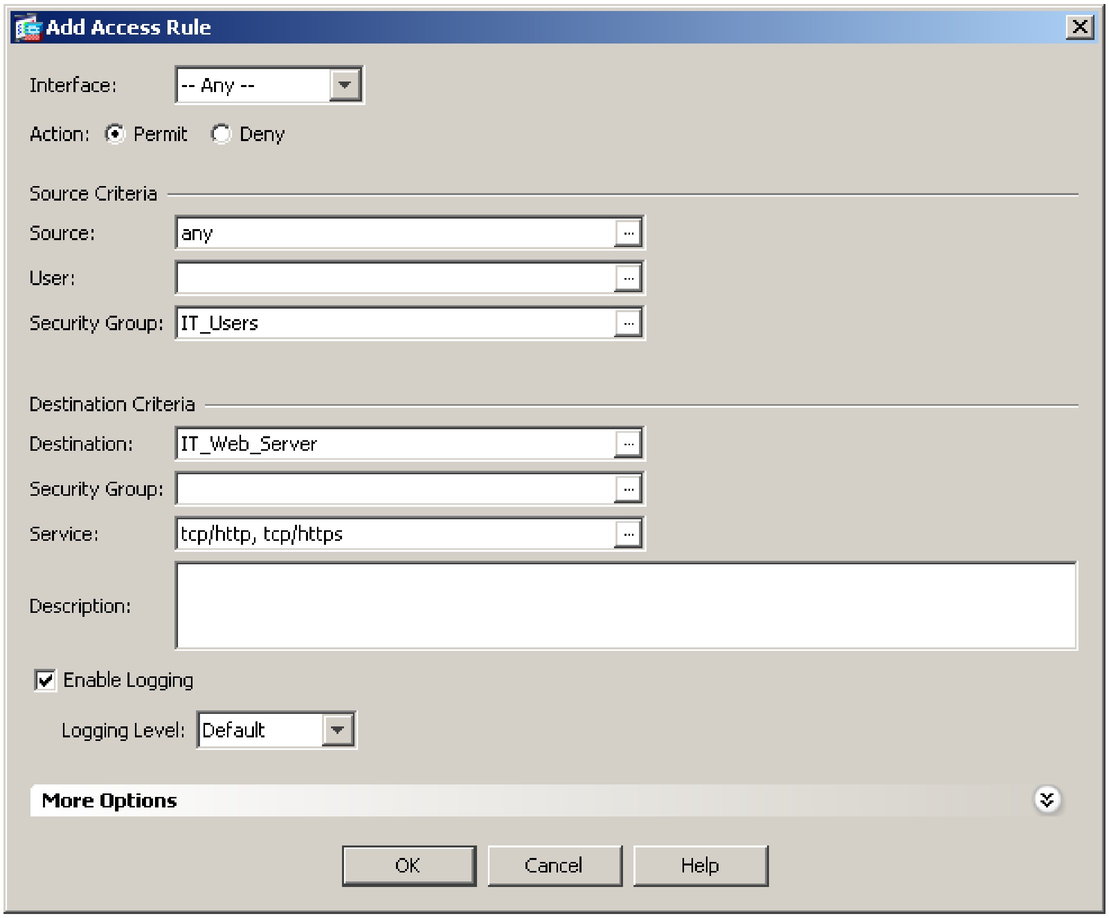
Name	Count	Security Type	Description
IT_Users		Name	

Step 8: Click **OK**. The Add Access Rule window opens.

Step 9: In the Destination Criteria section, click the ellipses for the Destination.

Step 10: Double-click **IT_Web_Server**, and then click **OK**. The Add Access Rule window appears.

Step 11: In the **Service** box, enter **tcp/http, tcp/https**, and then click **OK**.



Add Access Rule

Interface: -- Any --

Action: ● Permit ○ Deny

Source Criteria

Source: any

User:

Security Group: IT_Users

Destination Criteria

Destination: IT_Web_Server

Security Group:

Service: tcp/http, tcp/https

Description:

☑ Enable Logging

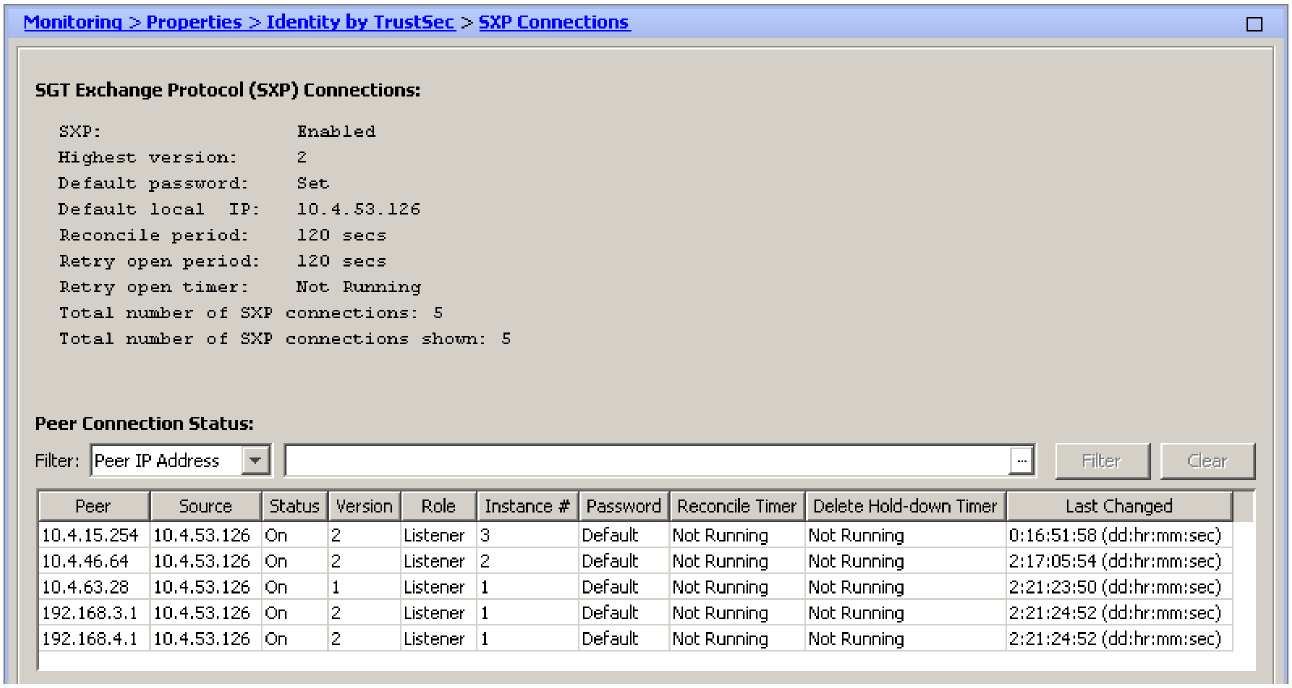
Logging Level: Default

Step 12: Repeat Step 2 through Step 11 for each server that you wish to create an SGT policy for. In this deployment, the remaining groups are Finance, HR, and Research.

Procedure 8 Monitoring SGTs on Cisco ASA

You use ASDM to verify that SXP is working properly and SGTs are being passed to Cisco ASA.

Step 1: In Cisco ASDM, navigate to **Monitoring > Properties > Identity by TrustSec > SXP Connections**. This shows all the current SXP connections to the ASA.



Monitoring > Properties > Identity by TrustSec > SXP Connections

SGT Exchange Protocol (SXP) Connections:

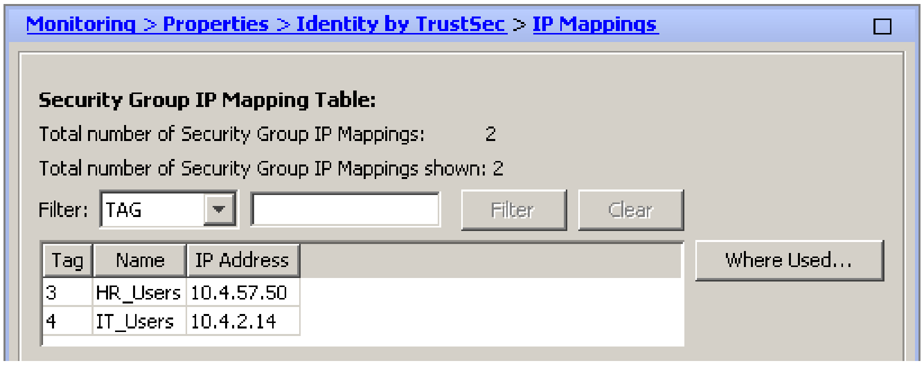
```
SXP:                  Enabled
Highest version:      2
Default password:     Set
Default local  IP:    10.4.53.126
Reconcile period:     120 secs
Retry open period:    120 secs
Retry open timer:     Not Running
Total number of SXP connections: 5
Total number of SXP connections shown: 5
```

Peer Connection Status:

Filter: Peer IP Address

Peer	Source	Status	Version	Role	Instance #	Password	Reconcile Timer	Delete Hold-down Timer	Last Changed
10.4.15.254	10.4.53.126	On	2	Listener	3	Default	Not Running	Not Running	0:16:51:58 (dd:hr:mm:sec)
10.4.46.64	10.4.53.126	On	2	Listener	2	Default	Not Running	Not Running	2:17:05:54 (dd:hr:mm:sec)
10.4.63.28	10.4.53.126	On	1	Listener	1	Default	Not Running	Not Running	2:21:23:50 (dd:hr:mm:sec)
192.168.3.1	10.4.53.126	On	2	Listener	1	Default	Not Running	Not Running	2:21:24:52 (dd:hr:mm:sec)
192.168.4.1	10.4.53.126	On	2	Listener	1	Default	Not Running	Not Running	2:21:24:52 (dd:hr:mm:sec)

Step 2: While at least one user is logged in using one of the security groups, in Cisco ASDM, navigate to **Monitoring > Properties > Identity by TrustSec > IP Mappings**. This shows all the current IP to SGT mappings passed to the ASA.



Monitoring > Properties > Identity by TrustSec > IP Mappings

Security Group IP Mapping Table:

Total number of Security Group IP Mappings: 2

Total number of Security Group IP Mappings shown: 2

Filter: TAG

Tag	Name	IP Address
3	HR_Users	10.4.57.50
4	IT_Users	10.4.2.14

Procedure 9 Monitoring SGTs on the switches

From the command line of the switch, you monitor SXP connections and the SGT assignments using a few show commands.

Step 1: Verify that the SGT assigned to a switch port after user authorization on an access layer switch.

```
show authentication session interface <interface>
```

```
A3750X#show authentication session interface GigabitEthernet 2/0/1
            Interface:  GigabitEthernet2/0/1
          MAC Address:  0050.56b9.007c
           IP Address:  10.4.2.13
            User-Name:  alex.reed
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  N/A
                  SGT:  0004-0
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0A040F06000001778A321722
      Acct Session ID:  0x00000B5D
               Handle:  0xCB000178
```

Step 2: Verify that the SXP connections on a switch.

```
show cts sxp connections
```

```
D6500VSS#show cts sxp connections
 SXP               : Enabled
 Highest Version Supported: 3
 Default Password : Set
 Default Source IP: 10.4.15.254
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is not running
----------------------------------------------
Peer IP          : 10.4.15.5
Source IP        : 10.4.15.254
Conn status      : On
Conn version     : 2
Local mode       : SXP Listener
Connection inst# : 4
```

```
TCP conn fd       : 3
TCP conn password: default SXP password
Duration since last state change: 11:20:31:22 (dd:hr:mm:sec)

----------------------------------------------
Peer IP           : 10.4.15.6
Source IP         : 10.4.15.254
Conn status       : On
Conn version      : 3
Local mode        : SXP Listener
Connection inst# : 6
TCP conn fd       : 1
TCP conn password: default SXP password
Duration since last state change: 11:20:31:22 (dd:hr:mm:sec)

----------------------------------------------
Peer IP           : 10.4.53.126
Source IP         : 10.4.15.254
Conn status       : On
Conn version      : 2
Local mode        : SXP Speaker
Connection inst# : 1
TCP conn fd       : 2
TCP conn password: default SXP password
Duration since last state change: 11:20:31:22 (dd:hr:mm:sec)

----------------------------------------------
Peer IP           : 10.4.79.5
Source IP         : 10.4.15.254
Conn status       : On
Conn version      : 3
Local mode        : SXP Listener
Connection inst# : 1
TCP conn fd       : 4
TCP conn password: default SXP password
Duration since last state change: 11:20:23:02 (dd:hr:mm:sec)


Total num of SXP Connections = 4
```

Procedure 10 Monitoring SGTs on the WLC

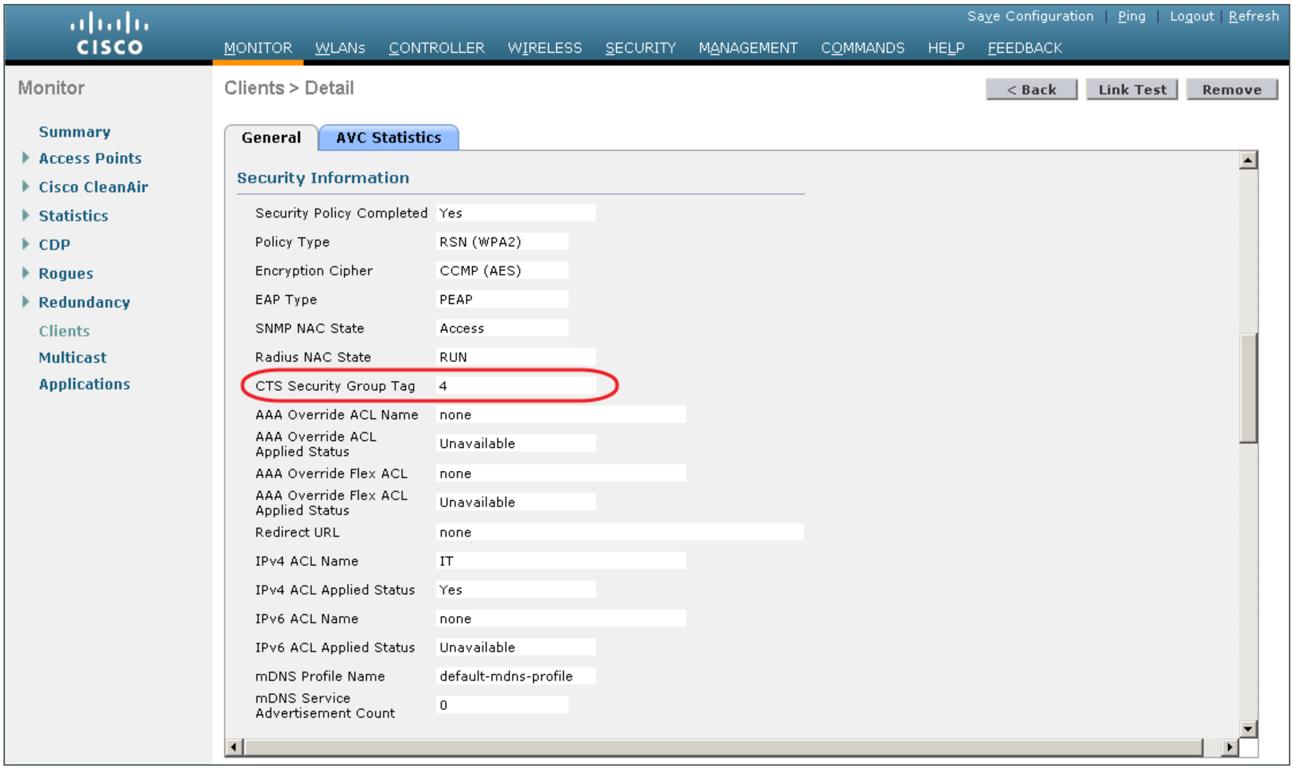
You use the GUI of the WLC to monitor the SGT assignments and SXP connections.

First, verify the SGT assigned to a client after user authorization on a WLC.

Step 1: In the web console, click **Monitor**, and then click **Clients.**

Step 2: Click the client MAC address. The Details window opens.

Step 3: Scroll down to the Security Information section.



Clients > Detail

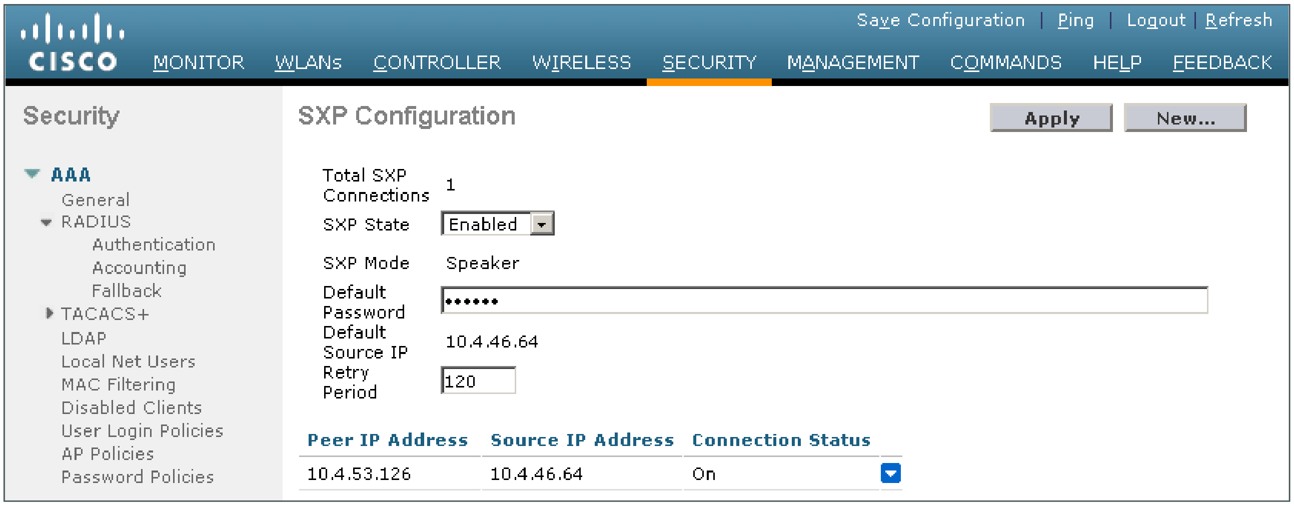
Security Information

Security Policy Completed	Yes
Policy Type	RSN (WPA2)
Encryption Cipher	CCMP (AES)
EAP Type	PEAP
SNMP NAC State	Access
Radius NAC State	RUN
CTS Security Group Tag	4
AAA Override ACL Name	none
AAA Override ACL Applied Status	Unavailable
AAA Override Flex ACL	none
AAA Override Flex ACL Applied Status	Unavailable
Redirect URL	none
IPv4 ACL Name	IT
IPv4 ACL Applied Status	Yes
IPv6 ACL Name	none
IPv6 ACL Applied Status	Unavailable
mDNS Profile Name	default-mdns-profile
mDNS Service Advertisement Count	0

Next, verify SXP connections from the WLC.

Step 4: In the web console, click **Security**.

Step 5: In the navigation pane on the left, click **TrustSec SXP**.



SXP Configuration

Total SXP Connections	1
SXP State	Enabled
SXP Mode	Speaker
Default Password	••••••
Default Source IP	10.4.46.64
Retry Period	120

Peer IP Address	Source IP Address	Connection Status
10.4.53.126	10.4.46.64	On

PROCESS

Monitoring Network Access

1. View the Cisco ISE dashboard
2. Configure identity groups
3. Add a custom profile
4. Examining the authentication log
5. Create custom authentication reports
6. Identify endpoints

The configuration of the network infrastructure is complete. Now it's time to answer the what, when, where, and who questions regarding network access by using the reporting functionality of Cisco ISE to gain a better understanding of current activity on the network.

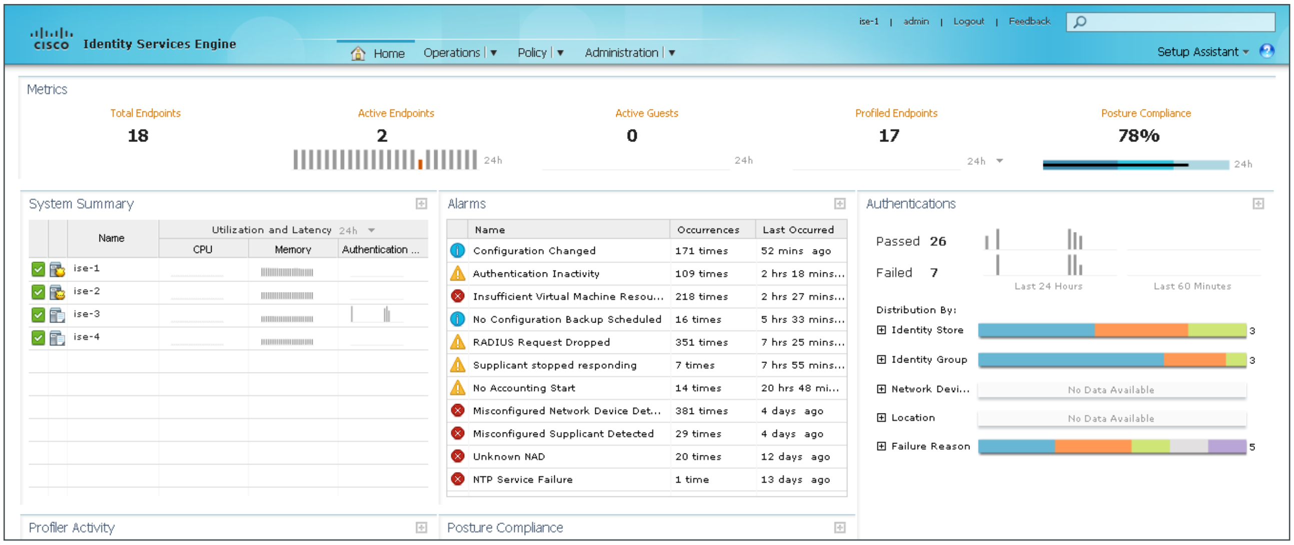
Cisco ISE is configured to authenticate users and to profile endpoints based on RADIUS and DHCP information. The reporting capabilities of Cisco ISE allow you to determine what type of device is connecting to your network, when it connects, and where it connects from. Also, you know who is connecting to your network and what authentication method was used.

Procedure 1 View the Cisco ISE dashboard

The first place to view this information is on the Cisco ISE home dashboard. It gives a summary view of the health status of the servers in the group, how devices are authenticating, and what types of devices have been profiled.

Step 1: On the menu bar, click **Home**.

Step 2: If you want to view additional information for a section, click the upper-right corner of that section. The section expands.



Total Endpoints	Active Endpoints	Active Guests	Profiled Endpoints	Posture Compliance
18	2	0	17	78%

Name	Occurrences	Last Occurred
Configuration Changed	171 times	52 mins ago
Authentication Inactivity	109 times	2 hrs 18 mins...
Insufficient Virtual Machine Resou...	218 times	2 hrs 27 mins...
No Configuration Backup Scheduled	16 times	5 hrs 33 mins...
RADIUS Request Dropped	351 times	7 hrs 25 mins...
Supplicant stopped responding	7 times	7 hrs 55 mins...
No Accounting Start	14 times	20 hrs 48 mi...
Misconfigured Network Device Det...	381 times	4 days ago
Misconfigured Supplicant Detected	29 times	4 days ago
Unknown NAD	20 times	12 days ago
NTP Service Failure	1 time	13 days ago

Passed 26

Failed 7

Procedure 2 Configure identity groups

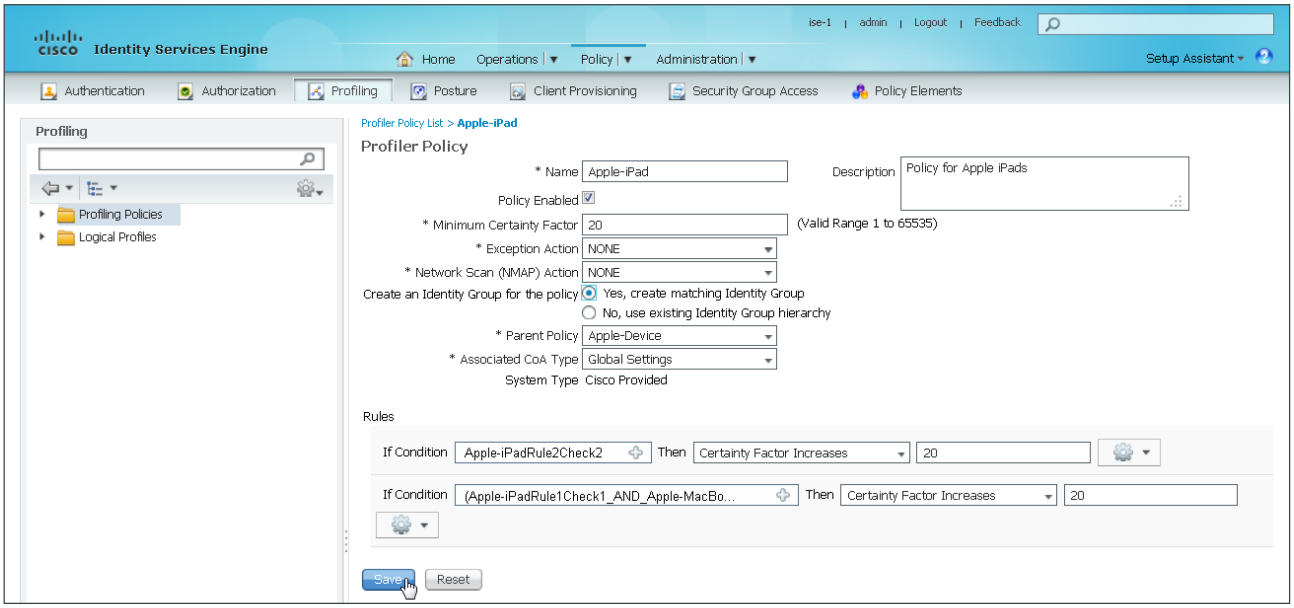
Cisco ISE has more in-depth reporting options to give more details on the devices connecting to the network. To help identify the endpoints, you can use identity groups to classify profiled endpoints and to generate reports.

The example below describes how to do this for an Apple iPad. The procedure for other types of devices is similar.

Step 1: In Cisco ISE, on the main menu bar, navigate to **Policy > Profiling**.

Step 2: Click the Policy Profiling name **Apple-iPad**. This enables you to edit this policy.

Step 3: Select **Create Matching Identity Group**, and then click **Save**.



Profiler Policy List > **Apple-iPad**

Profiler Policy

* Name Apple-iPad

Description Policy for Apple iPads

Policy Enabled ☑

* Minimum Certainty Factor 20 (Valid Range 1 to 65535)

* Exception Action NONE

* Network Scan (NMAP) Action NONE

Create an Identity Group for the policy ● Yes, create matching Identity Group

○ No, use existing Identity Group hierarchy

* Parent Policy Apple-Device

* Associated CoA Type Global Settings

System Type Cisco Provided

Rules

If Condition Apple-iPadRule2Check2 Then Certainty Factor Increases 20

If Condition (Apple-iPadRule1Check1_AND_Apple-MacBo... Then Certainty Factor Increases 20

You can repeat these steps for other endpoint types as needed. You can also investigate the rules used to profile the endpoint to understand the process. In the case of the Apple iPad, Cisco ISE uses two rules. One is based on DHCP information, and the other is based on HTTP.

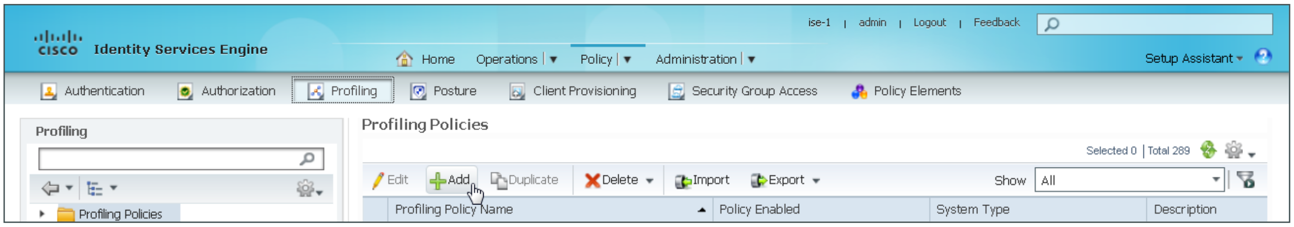
Procedure 3 Add a custom profile

Although there are many pre-defined profiles, you may find that a device you want to profile doesn't have an existing profile. You can create a new one using unique characteristics of the device. Review some of the existing profiles to get an idea of the options and methods available to you for device profiling.

The example below creates a profile for the Amazon Kindle Fire by using information obtained from the device's DHCP request and from HTTP requests.

Step 1: In Cisco ISE, on the main menu bar, navigate to **Policy > Profiling**.

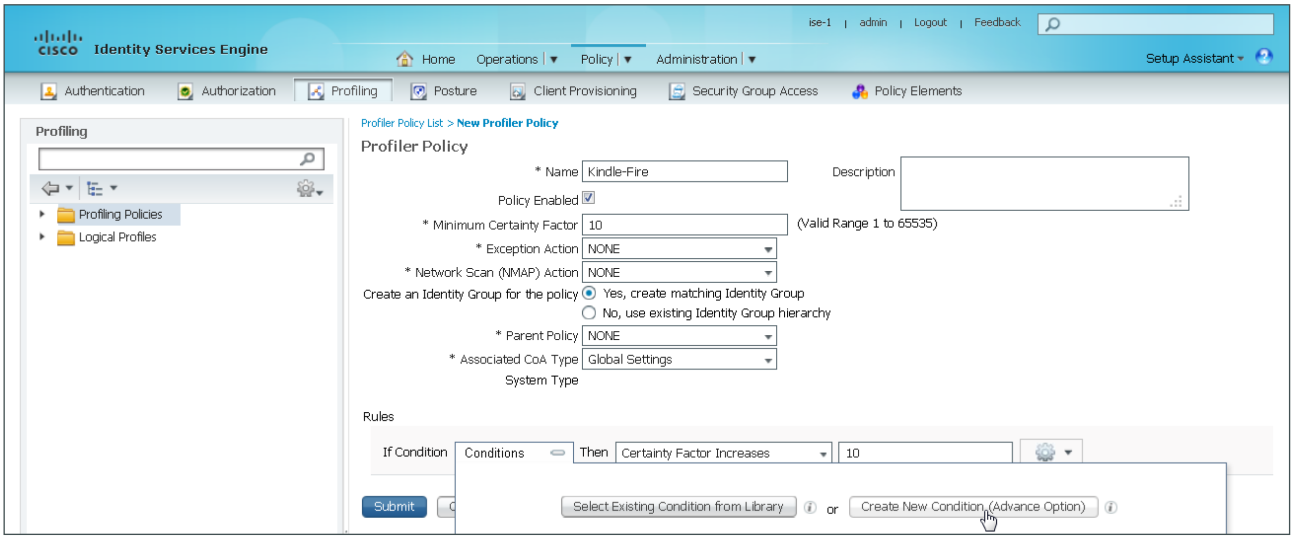
Step 2: Click **Add**.



Step 3: Enter the policy name **Kindle-Fire**.

Step 4: Enter a description.

Step 5: In the rules section, next to Conditions, click the **+** symbol, and then click **Create New Condition (Advance Option)**.



* Name: Kindle-Fire

Description:

Policy Enabled ☑

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

* Exception Action: NONE

* Network Scan (NMAP) Action: NONE

Create an Identity Group for the policy: ● Yes, create matching Identity Group ○ No, use existing Identity Group hierarchy

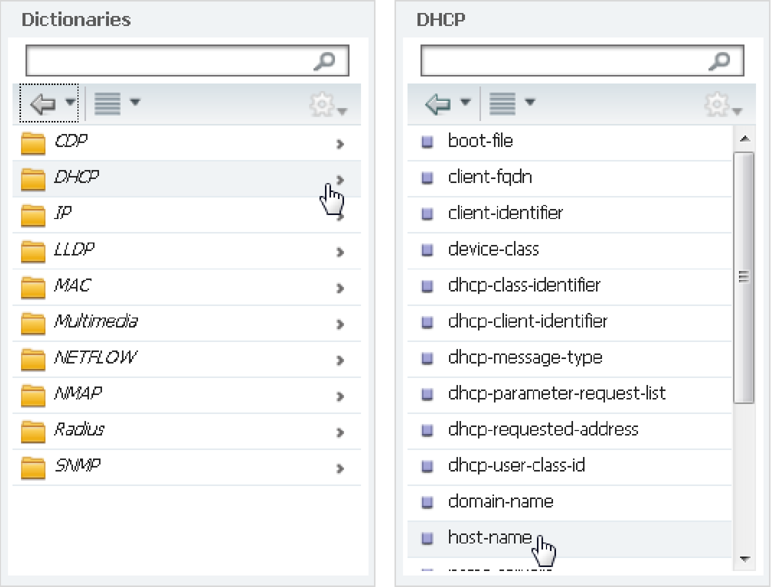
* Parent Policy: NONE

* Associated CoA Type: Global Settings

System Type

If Condition: Conditions Then: Certainty Factor Increases 10

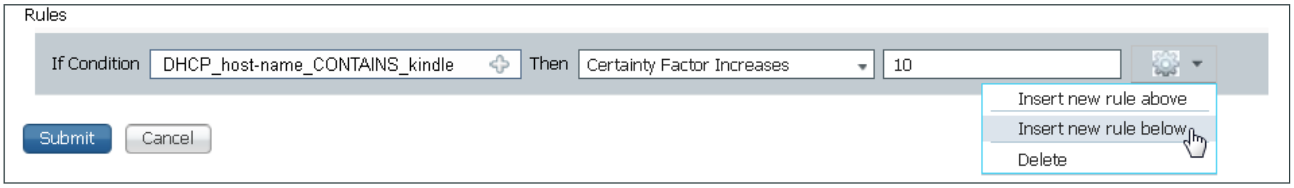
Step 6: In the **Expression** column, in the Selection List, choose **DHCP**, and then choose **host-name**.



Step 7: In the second column, choose **CONTAINS**, and then, in the box in the final column, enter **kindle**.

Step 8: Choose **Certainty Factor Increases**, and then set the value to **10**.

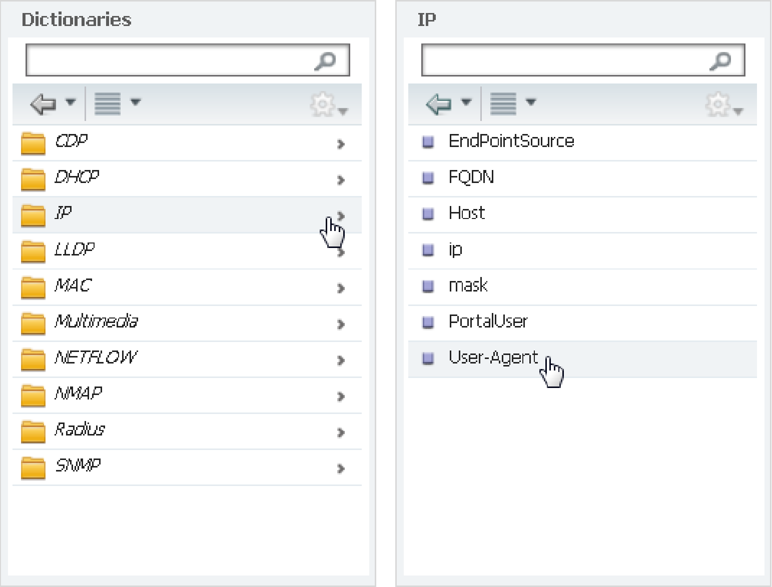
Step 9: Click the gear icon at the end of the rule, and then select **Insert new rule below**.


Rules

If Condition DHCP_host-name_CONTAINS_kindle Then Certainty Factor Increases 10

Step 10: Next to Conditions, click the **+** symbol, and then click **Create New Condition (Advance Option)**.

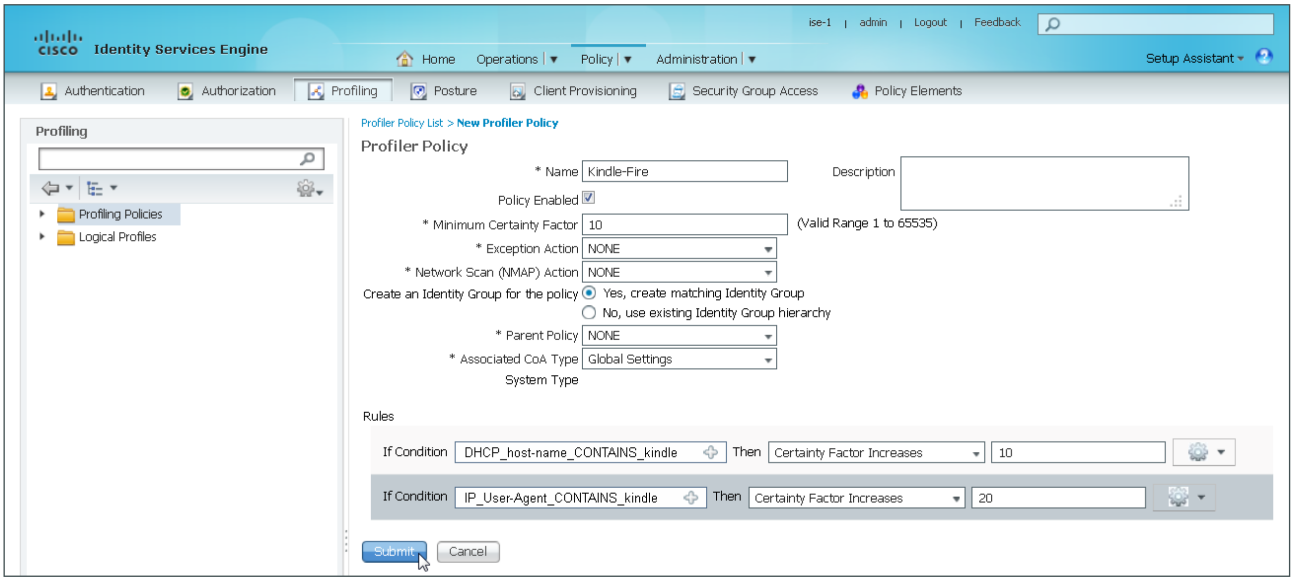
Step 11: In the **Expression** column in the **Select Attribute** list, select **IP**, and then choose **User-Agent**.



Step 12: In the next column, choose **CONTAINS**, and then, in the box in the final column, enter **kindle**.

Step 13: Choose **Certainty Factor Increases**.

Step 14: Set the certainty value to **20**, and then click **Submit**.



Profiler Policy

* Name Kindle-Fire

Description

Policy Enabled ☑

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

* Exception Action NONE

* Network Scan (NMAP) Action NONE

Create an Identity Group for the policy ● Yes, create matching Identity Group ○ No, use existing Identity Group hierarchy

* Parent Policy NONE

* Associated CoA Type Global Settings

System Type

Rules

If Condition DHCP_host-name_CONTAINS_kindle Then Certainty Factor Increases 10

If Condition IP_User-Agent_CONTAINS_kindle Then Certainty Factor Increases 20

Procedure 4 Examining the authentication log

Step 1: In Cisco ISE, on the main menu bar, navigate to **Operations > Authentications**. The authentication log displays. The default option is to display the last 20 records from the last 24 hours.

For devices that authenticated via MAB, the MAC address of the client is listed as the user name and the endpoint. For devices that authenticated via RADIUS over wireless or VPN, the user name is displayed.

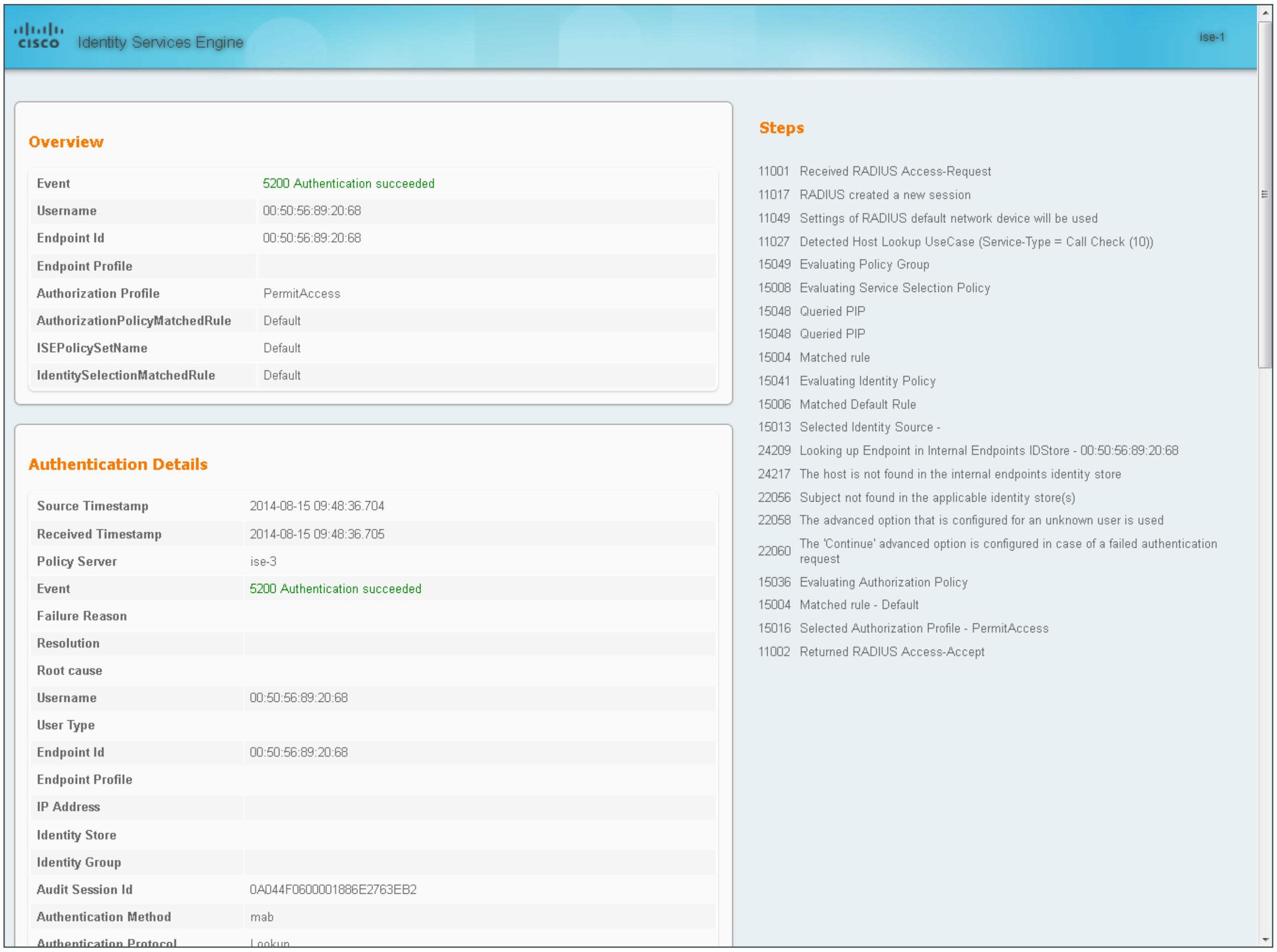
If the device was able to be profiled, that information is displayed.

Step 2: In the details column of the MAB record, click the “paper with magnifying glass” icon. This displays detailed authentication information for the record.

In the Authentication Summary section, the network device lists the IP address and the port of the switch that the endpoint is connected to.

You can find additional details, such as the identity group and identity policy, in the Authentication Details section.

Similar data can be found for endpoints that have authenticated with RADIUS. The user name is displayed in these records as well as the Extensible Authentication Protocol (EAP) method used.



Overview

Event	5200 Authentication succeeded
Username	00:50:56:89:20:68
Endpoint Id	00:50:56:89:20:68
Endpoint Profile	
Authorization Profile	PermitAccess
AuthorizationPolicyMatchedRule	Default
ISEPolicySetName	Default
IdentitySelectionMatchedRule	Default

Authentication Details

Source Timestamp	2014-08-15 09:48:36.704
Received Timestamp	2014-08-15 09:48:36.705
Policy Server	ise-3
Event	5200 Authentication succeeded
Failure Reason	
Resolution	
Root cause	
Username	00:50:56:89:20:68
User Type	
Endpoint Id	00:50:56:89:20:68
Endpoint Profile	
IP Address	
Identity Store	
Identity Group	
Audit Session Id	0A044F0600001886E2763EB2
Authentication Method	mab
Authentication Protocol	Lookup

Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
11049	Settings of RADIUS default network device will be used
11027	Detected Host Lookup UseCase (Service-Type = Call Check (10))
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15048	Queried PIP
15048	Queried PIP
15004	Matched rule
15041	Evaluating Identity Policy
15006	Matched Default Rule
15013	Selected Identity Source -
24209	Looking up Endpoint in Internal Endpoints IDStore - 00:50:56:89:20:68
24217	The host is not found in the internal endpoints identity store
22056	Subject not found in the applicable identity store(s)
22058	The advanced option that is configured for an unknown user is used
22060	The 'Continue' advanced option is configured in case of a failed authentication request
15036	Evaluating Authorization Policy
15004	Matched rule - Default
15016	Selected Authorization Profile - PermitAccess
11002	Returned RADIUS Access-Accept

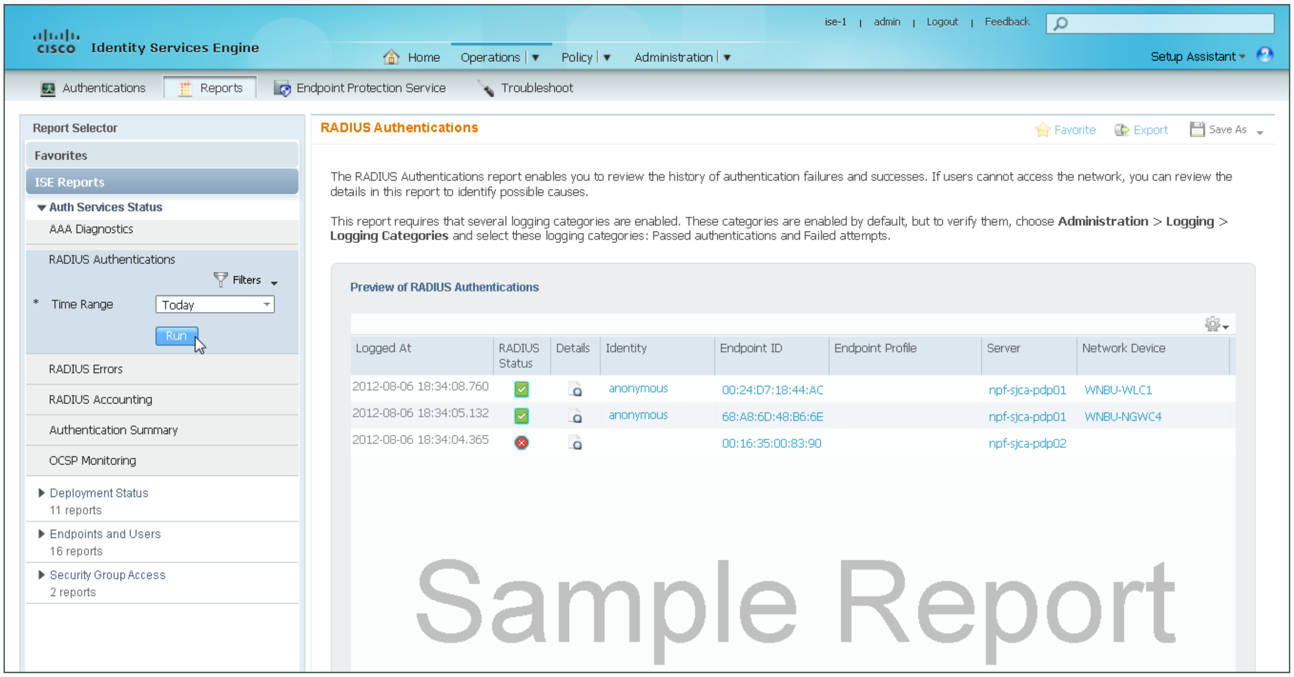
Procedure 5 Create custom authentication reports

The default authentication log view is limited to displaying only the most recent entries. To get in-depth reporting, you need to create a custom report.

Step 1: In Cisco ISE, on the main menu bar, navigate to **Operations > Reports > Catalog**.

Step 2: In the left pane, navigate to **Auth Services Status > RADIUS Authentications**.

Step 3: Select a time range. If you wish to select a time range that is not listed, choose **Custom**.



* Time Range: Today

RADIUS Authentications

The RADIUS Authentications report enables you to review the history of authentication failures and successes. If users cannot access the network, you can review the details in this report to identify possible causes.

This report requires that several logging categories are enabled. These categories are enabled by default, but to verify them, choose **Administration > Logging > Logging Categories** and select these logging categories: Passed authentications and Failed attempts.

Preview of RADIUS Authentications

Logged At	RADIUS Status	Details	Identity	Endpoint ID	Endpoint Profile	Server	Network Device
2012-08-06 18:34:08.760	☑		anonymous	00:24:D7:18:44:AC		npf-sjca-pdp01	WNBU-WLC1
2012-08-06 18:34:05.132	☑		anonymous	68:A8:6D:48:B6:6E		npf-sjca-pdp01	WNBU-NGWC4
2012-08-06 18:34:04.365	☒			00:16:35:00:83:90		npf-sjca-pdp02	

Step 4: Choose the filters you want.

Step 5: Choose parameters for those filters, and then click **Run**. The report generates.

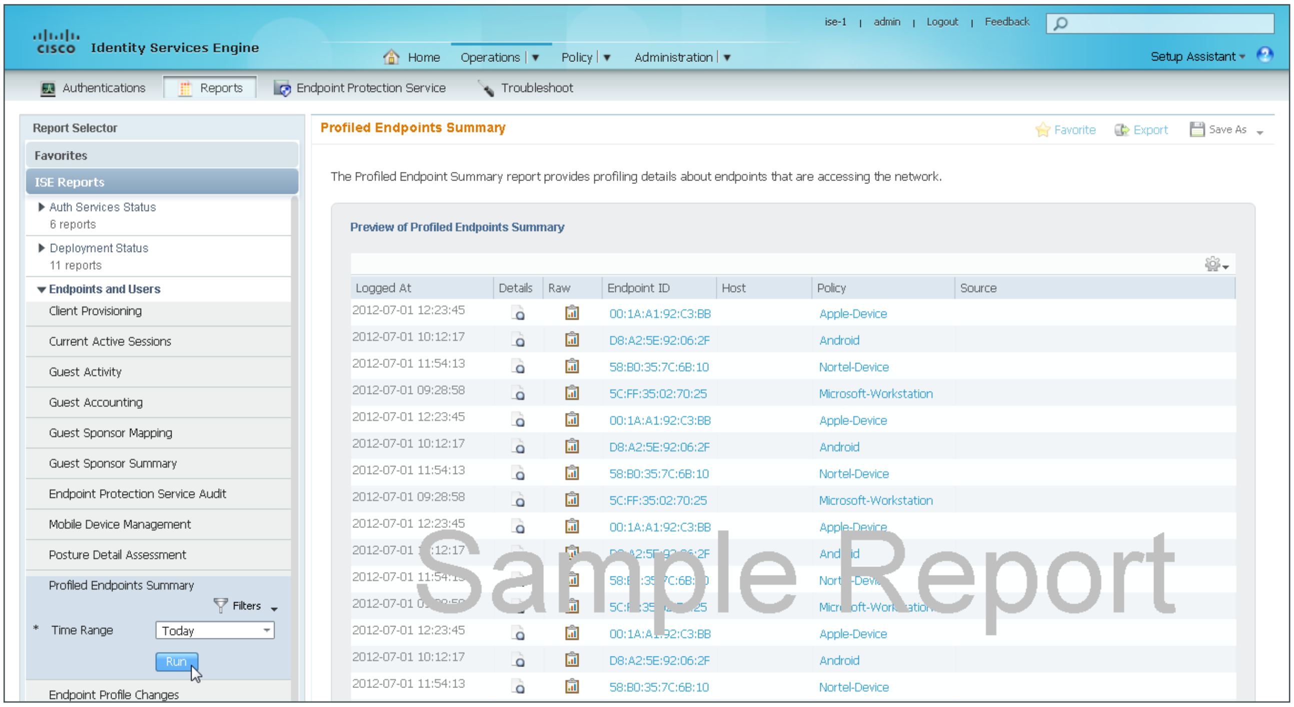
Procedure 6 Identify endpoints

Using information gleaned from the RADIUS and DHCP requests, Cisco ISE can identify what types of devices are connecting to the network. This can assist in determining the network security policy based on the type of device that is in use.

Step 1: In Cisco ISE, on the main menu bar, navigate to **Operations > Reports**.

Step 2: In the left pane, navigate to **Endpoints and Users**. This displays the available endpoint reports.

Step 3: Select **Profiled Endpoints Summary**, select the desired time period to run the report, and then click **Run**.



* Time Range: Today

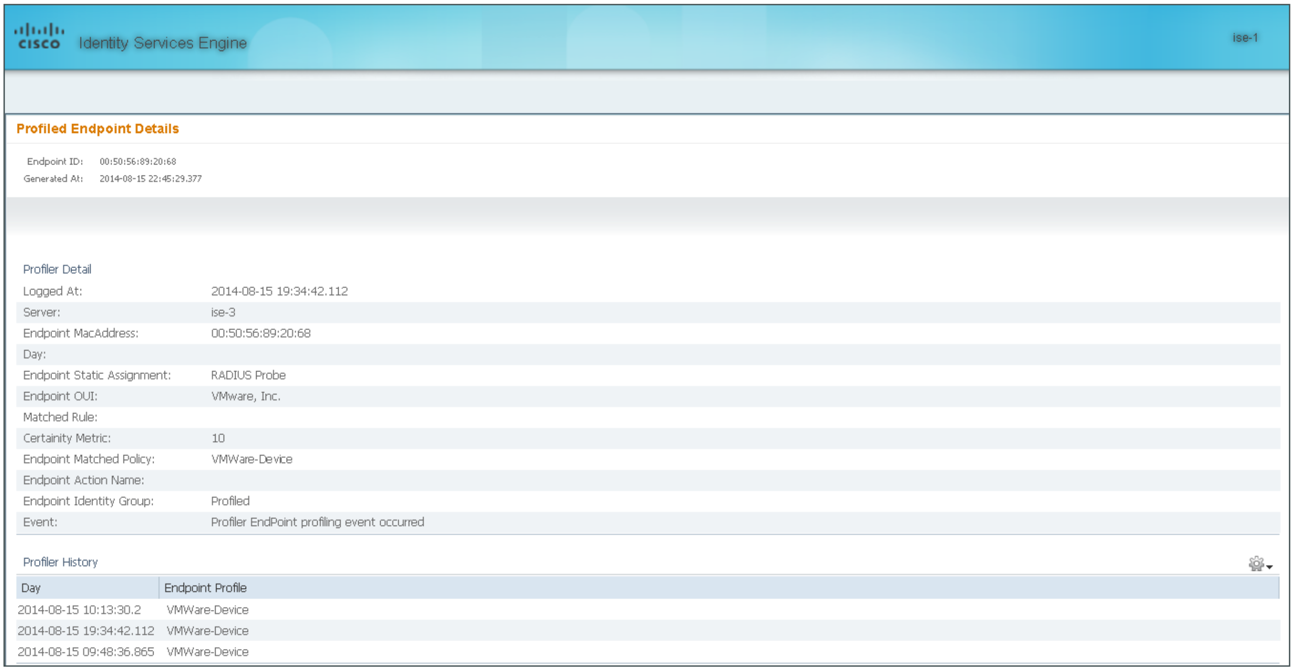
Profiled Endpoints Summary

The Profiled Endpoint Summary report provides profiling details about endpoints that are accessing the network.

Preview of Profiled Endpoints Summary

Logged At	Details	Raw	Endpoint ID	Host	Policy	Source
2012-07-01 12:23:45	🔍	📊	00:1A:A1:92:C3:BB		Apple-Device	
2012-07-01 10:12:17	🔍	📊	D8:A2:5E:92:06:2F		Android	
2012-07-01 11:54:13	🔍	📊	58:B0:35:7C:6B:10		Nortel-Device	
2012-07-01 09:28:58	🔍	📊	5C:FF:35:02:70:25		Microsoft-Workstation	
2012-07-01 12:23:45	🔍	📊	00:1A:A1:92:C3:BB		Apple-Device	
2012-07-01 10:12:17	🔍	📊	D8:A2:5E:92:06:2F		Android	
2012-07-01 11:54:13	🔍	📊	58:B0:35:7C:6B:10		Nortel-Device	
2012-07-01 09:28:58	🔍	📊	5C:FF:35:02:70:25		Microsoft-Workstation	
2012-07-01 12:23:45	🔍	📊	00:1A:A1:92:C3:BB		Apple-Device	
2012-07-01 [illegible]:12:17	[illegible]	📊	D[illegible]A2:5E[illegible]2F		And[illegible]id	
2012-07-01 11:54:1[illegible]	[illegible]	📊	58:[illegible]:35[illegible]7C:6B:[illegible]0		Nort[illegible]-Devi[illegible]	
2012-07-01 0[illegible]	[illegible]	📊	5C:[illegible]:35[illegible]25		Micr[illegible]oft-Work[illegible]ation[illegible]	
2012-07-01 12:23:45	🔍	📊	00:1A:A1:92:C3:BB		Apple-Device	
2012-07-01 10:12:17	🔍	📊	D8:A2:5E:92:06:2F		Android	
2012-07-01 11:54:13	🔍	📊	58:B0:35:7C:6B:10		Nortel-Device	

Step 4: Once the report is generated, you can view the details of a profiled endpoint by clicking the magnifying glass icon.



Profiled Endpoint Details

Endpoint ID: 00:50:56:89:20:68
Generated At: 2014-08-15 22:45:29.377

Profiler Detail

Logged At:	2014-08-15 19:34:42.112
Server:	ise-3
Endpoint MacAddress:	00:50:56:89:20:68
Day:	
Endpoint Static Assignment:	RADIUS Probe
Endpoint OUI:	VMware, Inc.
Matched Rule:	
Certainity Metric:	10
Endpoint Matched Policy:	VMWare-Device
Endpoint Action Name:	
Endpoint Identity Group:	Profiled
Event:	Profiler EndPoint profiling event occurred

Profiler History

Day	Endpoint Profile
2014-08-15 10:13:30.2	VMWare-Device
2014-08-15 19:34:42.112	VMWare-Device
2014-08-15 09:48:36.865	VMWare-Device

Appendix A: Product List

Network Management

Functional Area	Product Description	Part Numbers	Software
Identity Management	Cisco Identity Services Engine Virtual Appliance	ISE-VM-K9=	1.2.0.899–Cumulative Patch 8
	Cisco ISE Base License for 100 Endpoints	L-ISE-BSE-100=	
	Cisco ISE Base License for 250 Endpoints	L-ISE-BSE-250=	
	Cisco ISE Base License for 500 Endpoints	L-ISE-BSE-500=	
	Cisco ISE Base License for 1000 Endpoints	L-ISE-BSE-1K=	
	Cisco ISE Base License for 1500 Endpoints	L-ISE-BSE-1500=	
	Cisco ISE Base License for 2500 Endpoints	L-ISE-BSE-2500=	
	Cisco ISE Base License for 3500 Endpoints	L-ISE-BSE-3500=	
	Cisco ISE Base License for 5000 Endpoints	L-ISE-BSE-5K=	
	Cisco ISE Base License for 10,000 Endpoints	L-ISE-BSE-10K=	
	Cisco ISE Advanced Subscription License for 100 Endpoints	L-ISE-ADV-S-100=	
	Cisco ISE Advanced 3-year License for 100 Endpoints	ISE-ADV-3YR-100	
	Cisco ISE Advanced Subscription License for 250 Endpoints	L-ISE-ADV-S-250=	
	Cisco ISE Advanced 3-year License for 250 Endpoints	ISE-ADV-3YR-250	
	Cisco ISE Advanced Subscription License for 500 Endpoints	L-ISE-ADV-S-500=	
	Cisco ISE Advanced 3-year License for 500 Endpoints	ISE-ADV-3YR-500	
	Cisco ISE Advanced Subscription License for 1000 Endpoints	L-ISE-ADV-S-1K=	
	Cisco ISE Advanced 3-year License for 1000 Endpoints	ISE-ADV-3YR-1K	
	Cisco ISE Advanced Subscription License for 1500 Endpoints	L-ISE-ADV-S-1500=	
	Cisco ISE Advanced 3-year License for 1500 Endpoints	ISE-ADV-3YR-1500	
	Cisco ISE Advanced Subscription License for 2500 Endpoints	L-ISE-ADV-S-2500=	
	Cisco ISE Advanced 3-year License for 2500 Endpoints	ISE-ADV-3YR-2500	
	Cisco ISE Advanced Subscription License for 3500 Endpoints	L-ISE-ADV-S-3500=	
	Cisco ISE Advanced 3-year License for 3500 Endpoints	ISE-ADV-3YR-3500	
	Cisco ISE Advanced Subscription License for 5000 Endpoints	L-ISE-ADV-S-5k=	
	Cisco ISE Advanced 3-year License for 5000 Endpoints	ISE-ADV-3YR-5K	
	Cisco ISE Advanced Subscription License for 10,000 Endpoints	L-ISE-ADV-S-10K=	
	Cisco ISE Advanced 3-year License for 10,000 Endpoints	ISE-ADV-3YR-10K	

VPN Client

Functional Area	Product Description	Part Numbers	Software
VPN Client	Cisco AnyConnect Secure Mobility Client (Windows)	Cisco AnyConnect Secure Mobility Client	3.1.05160
	Cisco AnyConnect Secure Mobility Client (Mac OS X)	Cisco AnyConnect Secure Mobility Client	3.1.05160

LAN Access Layer

Functional Area	Product Description	Part Numbers	Software
Modular Access Layer Switch	Cisco Catalyst 4500E Series 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.3.1XO(15.1.1XO1) IP Base feature set
	Cisco Catalyst 4500E Supervisor Engine 8-E, Unified Access, 928Gbps	WS-X45-SUP8-E	
	Cisco Catalyst 4500E 12-port 10GbE SFP+ Fiber Module	WS-X4712-SFP+E	
	Cisco Catalyst 4500E 48-Port 802.3at PoE+ 10/100/1000 (RJ-45)	WS-X4748-RJ45V+E	
	Cisco Catalyst 4500E Series 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.5.3E(15.2.1E3) IP Base feature set
	Cisco Catalyst 4500E Supervisor Engine 7L-E, 520Gbps	WS-X45-SUP7L-E	
	Cisco Catalyst 4500E 48 Ethernet 10/100/1000 (RJ45) PoE+,UPoE ports	WS-X4748-UPOE+E	
	Cisco Catalyst 4500E 48 Ethernet 10/100/1000 (RJ45) PoE+ ports	WS-X4648-RJ45V+E	
Stackable Access Layer Switch	Cisco Catalyst 3850 Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3850-48F	3.3.3SE(15.0.1EZ3) IP Base feature set
	Cisco Catalyst 3850 Series Stackable 24 Ethernet 10/100/1000 PoE+ Ports	WS-C3850-24P	
	Cisco Catalyst 3850 Series 2 x 10GE Network Module	C3850-NM-2-10G	
	Cisco Catalyst 3850 Series 4 x 1GE Network Module	C3850-NM-4-1G	
	Cisco Catalyst 3650 Series 24 Ethernet 10/100/1000 PoE+ and 2x10GE or 4x1GE Uplink	WS-C3650-24PD	3.3.3SE(15.0.1EZ3) IP Base feature set
	Cisco Catalyst 3650 Series 24 Ethernet 10/100/1000 PoE+ and 4x1GE Uplink	WS-C3650-24PS	
	Cisco Catalyst 3650 Series Stack Module	C3650-STACK	
	Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-48PF-S	15.2(1)E3 IP Base feature set
	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-24P-S	
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
	Cisco Catalyst 2960-X Series 24 10/100/1000 Ethernet and 2 SFP+ Uplink	WS-C2960X-24PD	15.0(2)EX5 LAN Base feature set
Standalone Access Layer Switch	Cisco Catalyst 3650 Series 24 Ethernet 10/100/1000 PoE+ and 4x1GE Uplink	WS-C3650-24PS	3.3.3SE(15.01EZ3) IP Base feature set

Wireless LAN Controllers

Functional Area	Product Description	Part Numbers	Software
On Site, Remote Site, or Guest Controller	Cisco WiSM2 Series Wireless Controller for up to 1000 Cisco access points	WS-SVC-WISM2-K-K9	7.6.120.0
	Cisco WiSM2 Series Wireless Controller for up to 500 Cisco access points	WS-SVC-WISM2-5-K9	
	Cisco WiSM2 Series Wireless Controller for up to 300 Cisco access points	WS-SVC-WISM2-3-K9	
	Cisco WiSM2 Series Wireless Controller for up to 100 Cisco access points	WS-SVC-WISM2-1-K9	
	Cisco WiSM2 Series Wireless Controller for High Availability	WS-SVC-WISM2-HA-K9	
	Cisco 5500 Series Wireless Controller for up to 500 Cisco access points	AIR-CT5508-500-K9	
	Cisco 5500 Series Wireless Controller for up to 250 Cisco access points	AIR-CT5508-250-K9	
	Cisco 5500 Series Wireless Controller for up to 100 Cisco access points	AIR-CT5508-100-K9	
	Cisco 5500 Series Wireless Controller for up to 50 Cisco access points	AIR-CT5508-50-K9	
	Cisco 5500 Series Wireless Controller for up to 25 Cisco access points	AIR-CT5508-25-K9	
	Cisco 5500 Series Wireless Controller for up to 12 Cisco access points	AIR-CT5508-12-K9	
	Cisco 5500 Series Wireless Controller for High Availability	AIR-CT5508-HA-K9	
On Site Controller, Guest Controller	Cisco 2500 Series Wireless Controller for up to 50 Cisco access points	AIR-CT2504-50-K9	7.6.120.0
	Cisco 2500 Series Wireless Controller for up to 25 Cisco access points	AIR-CT2504-25-K9	
	Cisco 2500 Series Wireless Controller for up to 15 Cisco access points	AIR-CT2504-15-K9	
	Cisco 2500 Series Wireless Controller for up to 5 Cisco access points	AIR-CT2504-5-K9	

Wireless LAN Access Points

Functional Area	Product Description	Part Numbers	Software
Wireless Access Points	Cisco 3700 Series Access Point 802.11ac and CleanAir with Internal Antennas	AIR-CAP3702I-x-K9	7.6.120.0
	Cisco 3700 Series Access Point 802.11ac and CleanAir with External Antenna	AIR-CAP3702E-x-K9	
	Cisco 3600 Series Access Point Dual Band 802.11a/g/n and CleanAir with Internal Antennas	AIR-CAP3602I-x-K9	
	Cisco 3600 Series Access Point Dual Band 802.11a/g/n and CleanAir with External Antennas	AIR-CAP3602E-x-K9	
	Cisco 2600 Series Access Point Dual Band 802.11a/g/n and CleanAir with Internal Antennas	AIR-CAP2602I-x-K9	
	Cisco 2600 Series Access Point Dual Band 802.11a/g/n and CleanAir with External Antennas	AIR-CAP2602E-x-K9	
	Cisco 1600 Series Access Point Dual-band controller-based 802.11a/g/n with Internal Antennas	AIR-CAP1602I-x-K9	
	Cisco 1600 Series Access Point Dual-band controller-based 802.11a/g/n with External Antennas	AIR-CAP1602E-x-K9	

Data Center Services

Functional Area	Product Description	Part Numbers	Software
Firewall	Cisco ASA 5585-X Security Plus IPS Edition SSP-40 and IPS SSP-40 bundle	ASA5585-S40P40-K9	ASA 9.1(5) IPS 7.3(2) E4
	Cisco ASA 5585-X Security Plus IPS Edition SSP-20 and IPS SSP-20 bundle	ASA5585-S20P20X-K9	
	Cisco ASA 5585-X Security Plus IPS Edition SSP-10 and IPS SSP-10 bundle	ASA5585-S10P10XK9	

Appendix B: Changes

This appendix summarizes the changes Cisco made to this guide since its last edition.

- We upgraded Cisco ISE, Cisco IOS, and Cisco AireOS software, as shown in Appendix A: Product List.
- For clarity and conciseness, we ensured that all Cisco IOS deployments are shown exclusively with command line configurations.
- To be in alignment with the most common practices, we reconfigured the distribution across servers of Policy Administration Node, Monitoring and Troubleshooting Node, and Policy Service Node personas.

Feedback

Please use the feedback form to send comments and suggestions about this guide.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2014 Cisco Systems, Inc. All rights reserved.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

B-0000210-1 09/14