



CVD



BYOD—Identity and Authentication

SOLUTION DESIGN GUIDE

August 2013



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	4
Use Case: Controlling the Services a User Can Access Based on Group Membership	4
Design Overview	4
Deployment Details	6
Enable Authentication	6
Deploying Cisco Identity Services Engine	6
Enabling Visibility to the LAN	18
Enabling Visibility to the Wireless Network	34
Deploying Digital Certificates	39
Enabling 802.1X Authentication	48
Configuring Group Policy Objects	56
Deploying Cisco AnyConnect on Windows Endpoints	72
Configuring Mac Workstations for 802.1X Authentication	77
Configure Mac OS X Supplicant	80
Enable Authorization	80
Enabling Authorization for Cisco IP Phones	80
Enabling Authorization for Wireless Access Points	81
Modifying the MAB Authentication Policy	84
Enabling Authorization for Wired Endpoints	85
Enabling Authorization for Wireless Endpoints	97
Modifying the Authorization Policy to be Closed	100
Enabling EAP Chaining	102
Enabling Downloadable Access Lists	111
Enabling Security Group Access	116
Monitoring Network Access	130
Appendix A: Product List	141

Preface

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

CVDs include two guide types that provide tested and validated design and deployment 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 or reference existing CVDs, but also include product features and functionality across Cisco products and may 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 using their own setup and configuration.

How to Read Commands

Many CVD guides tell you how to use a command-line interface (CLI) to configure network devices. This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

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

Commands at a CLI or script prompt appear as follows:

```
Router# enable
```

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

```
police rate 10000 pps burst 10000 packets conform-action set-discard-class-  
transmit 48 exceed-action transmit
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

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

Comments and Questions

If you would like to comment on a guide or ask questions, please use the [feedback form](#).

For the most recent CVD guides, see the following site:

<http://www.cisco.com/go/cvd>

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**—A customer 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**—A customer 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 following site:
<http://www.cisco.com/go/cvd>

Introduction

There is a trend in the marketplace today that is often referred to as *Bring Your Own Device* (BYOD). BYOD is a spectrum of business problems that can be solved in various ways. These range from accessing guest wireless networks to providing device authentication and identification. The goal is to provide a common work environment, regardless of the type of device being used. This could be accomplished by providing a virtualized desktop or by allowing users to self-register devices for use on the network.

Organizations are experiencing an unprecedented transformation in the network landscape. In the past, IT typically provided network resources only to corporate-managed PCs, such as laptops and desktops. Today, employees are requiring access from both corporate managed and unmanaged devices, including mobile devices like smart phones and tablets. This rapid proliferation of mobile devices capable of supporting applications drastically increases workforce mobility and productivity, but it also presents an enormous challenge to IT organizations seeking to enforce security policies across a growing population of devices, operating systems, and connectivity profiles.

The distinction between a work device and a personal device has evolved. This evolution of mobile device usage and the introduction of mobile devices into the workplace has caused a paradigm shift in how IT views what qualifies as a network “end point device” and also what it means to “be at work.”

An organization needs to know not only who is accessing their wired and wireless networks, but also when the networks are accessed and from where. In addition, with the wide adoption of nontraditional devices, such as smart phones and tablets, and 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 policy to prevent connection by nontraditional devices, limit connection to approved devices, or make access to network resources easier for these non-traditional devices. This presents a challenge for IT organizations that seek to provide end-users with a consistent network access experience and the freedom to use any device, while still enforcing stringent security policies to protect corporate intellectual property. Further complicating the situation is delivering both consistent access and enforcing proper security policy based on the specific user-access scenario (wired, wireless, guest, local, branch, and remote users).

To balance the productivity gains versus the security risks, IT needs to implement a solution that allows for seamless on-boarding of users and devices, simplicity of on-going operations, and the ability to extend end-user applications to any user or any device at any time.

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

A customer 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

A customer 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.

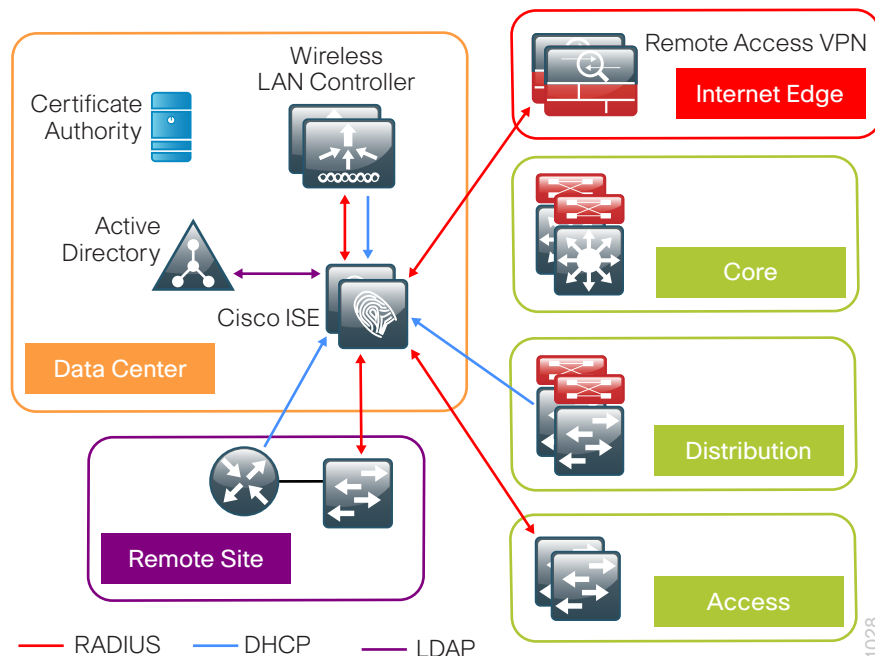
This deployment uses Cisco ISE as the authentication, authorization, and accounting server for the wired and wireless networks using RADIUS. Cisco ISE acts as a proxy to the existing Active Directory (AD) services to maintain a centralized identity store for all network services.

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 Name 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. In the organization, these switch configurations will be managed by Cisco Prime LAN Management Solution (LMS) 4.2 and the new TrustSec Work Center. Cisco Prime LMS simplifies the deployment of identity by performing a network-readiness assessment for an identity deployment, providing templates for the various modes—monitor, low-impact, closed—and providing a step-by-step wizard to configure the various components required.

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

The deployment described here bases all IP addressing off of the [Campus Wired LAN Design Guide](#). Any 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 2000. To support a greater number of endpoints, you will need to divide the personas across multiple appliances. In this example, there is a primary and secondary policy service and administration node and a primary and secondary monitoring node. This will allow the deployment to scale to 10,000 endpoints. If your deployment does not require support for more than 2000 endpoints, then you can just have a primary and secondary set of engines that support all the personas.

Table 1 - Cisco ISE engine IP addresses and hostnames

Device	IP address	Hostname
Primary Cisco ISE administration and policy service node	10.4.48.41	ise-1.cisco.local
Secondary Cisco ISE administration and policy service node	10.4.48.42	ise-2.cisco.local
Primary Cisco ISE monitoring node	10.4.48.43	ise-3.cisco.local
Secondary Cisco ISE monitoring node	10.4.48.44	ise-4.cisco.local

Enable Authentication

Deploying Cisco Identity Services Engine

PROCESS

1. Set up initial primary engine
2. Set up the remaining engines
3. Configure certificate trust list
4. Configure Cisco ISE deployment nodes
5. Install Cisco ISE license
6. Configure network devices in Cisco ISE
7. Configure Cisco ISE to use Active Directory
8. Disable IP Phone authorization policy

Procedure 1 Set up initial primary engine

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

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

Step 2: Enter the host name, IP address, subnet mask, and default router of the engine.

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

Step 3: Enter DNS information.

```
Enter default DNS domain[: cisco.local  
Enter primary nameserver[: 10.4.48.10  
Add/Edit another nameserver? Y/N : n
```

Step 4: Configure time.

```
Enter primary NTP server[time.nist.gov]: ntp.cisco.local  
Add/Edit secondary NTP server? Y/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 1.1.x](#).

Step 5: Configure an administrator account.

You must configure an administrator account in order to access to the CLI console. This account is not the same as the one used to access the GUI.

```
Enter username[admin]: admin
Enter password: [password]
Enter password again: [password]
```

Cisco ISE completes the installation and reboots. This process takes several minutes. You are asked to enter a new database administrator password and a new database user password during the provisioning of the internal database. Do not press **Control-C** during the installation, or the installation aborts.

```
Do not use 'Ctrl-C' from this point on...
Virtual machine detected, configuring VMware tools...
Installing applications...
Installing ise ...
Executed with privileges of root
The mode has been set to licensed.

Application bundle (ise) installed successfully

=== Initial Setup for Application: ise ===

Welcome to the ISE initial setup. The purpose of this setup is to
provision the internal ISE database. This setup requires you create
a database administrator password and also create a database user password.
```

The primary engine is now installed.

Procedure 2 Set up the remaining engines

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

Procedure 3 Configure certificate trust list

The engines use public key infrastructure (PKI) to secure communications between them. Initially in this deployment, you use local certificates, and you must configure a trust relationship between all of the engines. To do this, you need to import the local certificates from the secondary administration node and the two monitoring nodes into the primary administration node.

Step 1: In your browser, connect to the secondary engine’s GUI at <http://ise-2.cisco.local>.

Step 2: In **Administration > System**, select **Certificates**.

Step 3: In the Local Certificates window, select the local certificate by selecting the box next to the name of the secondary engine, **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 engine.

Step 6: In a browser, access the primary engine’s GUI at <http://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 the Certificate File box, click **Browse**, and then locate the certificate exported from the secondary engine. It has an extension of .pem. Click **Submit**.

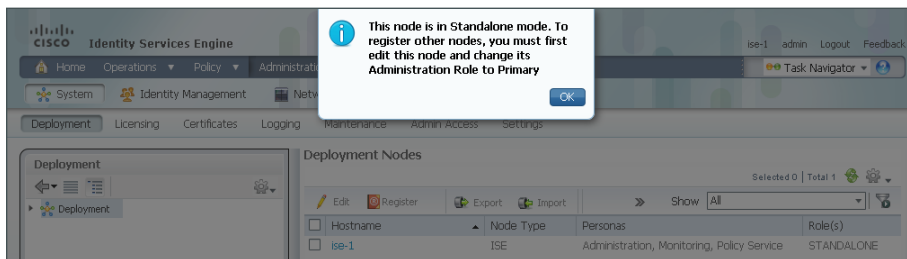
Step 10: Repeat this procedure for the remaining engines, ise-3.cisco.local and ise-4.cisco.local.

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 engine or to be distributed amongst several engines. For this example installation, you will deploy a pair of engines for administration and policy service with one serving as primary and the other secondary and another pair of engines for monitoring with one serving as primary and the other secondary.

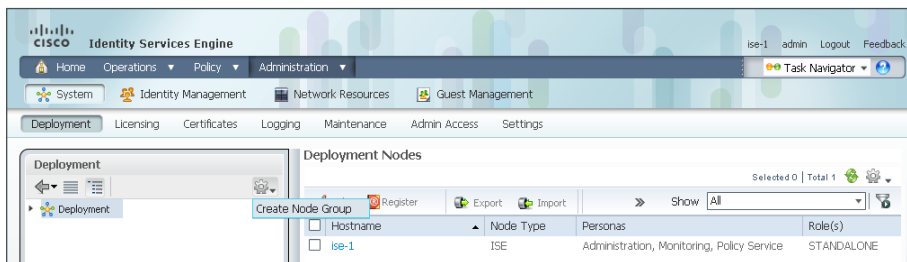
Step 1: Connect to <http://ise-1.cisco.local>.

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**.



Step 3: In the Deployment pane, click the gear icon, and then select **Create Node Group**.

In order for the two Cisco ISE devices to share policy and state information, they must be in a node group. The nodes use IP multicast to distribute this information, so they need to be able to communicate via IP multicast.



Step 4: 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**.

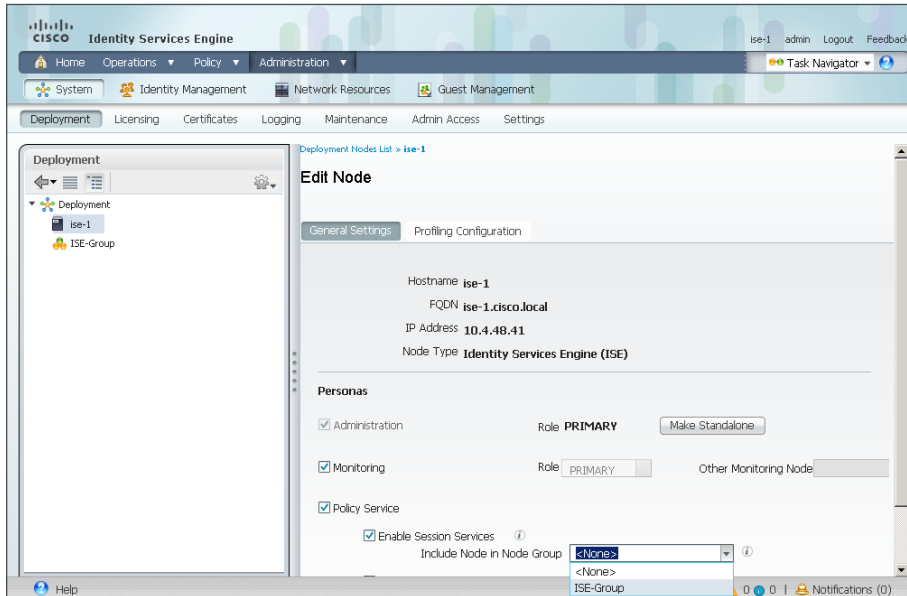
Step 5: A pop-up window lets you know the group was created successfully. Click **OK**.

Step 6: In the **Deployment** pane on the left, expand **Deployment**. A list of the current deployment nodes appears.

Step 7: Click **ise-1**. This enables you to configure this deployment node.

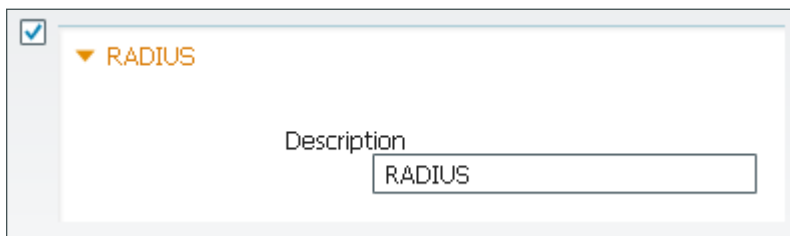
Step 8: On the General Settings tab, in the Personas section, next to the Administration Role, click **Make Primary**.

Step 9: In the Include Node in Node Group list, choose **ISE-Group**.

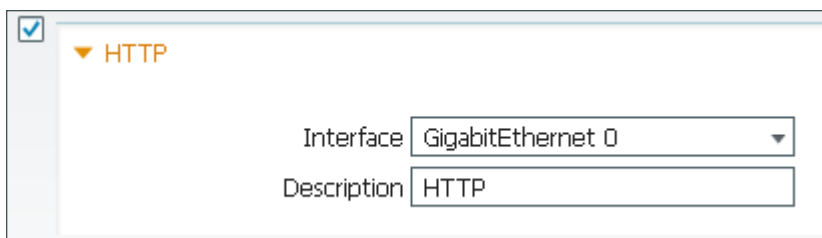


Next, you'll configure which methods are used to profile network endpoints.

Step 10: On the Profiling Configuration tab, select **RADIUS**, use the default parameters, and then click **Save**.

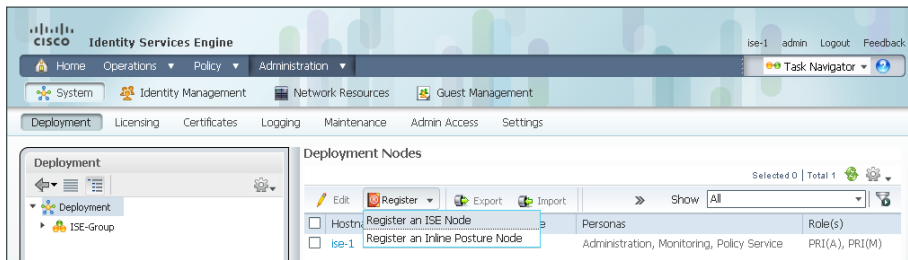


Step 11: Select **HTTP**, use the default parameters, and then click **Save**.



Step 12: In the Edit Node window, click **Deployment Nodes List**. The Deployment Nodes window appears.

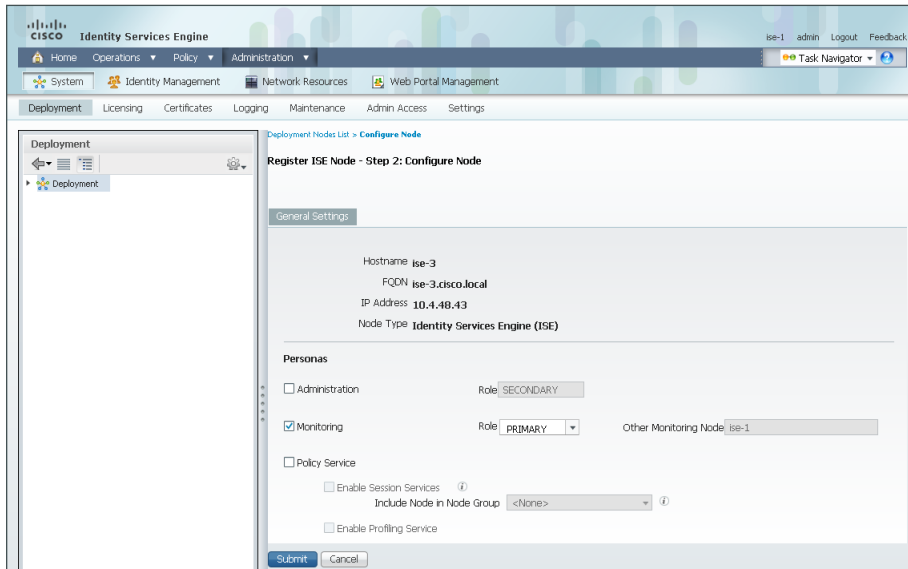
Step 13: Click **Register**, and then choose **Register an ISE Node**.



Step 14: Enter the IP address or host name of the primary monitoring Cisco ISE engine from Table 1 (in this example, ise-3.cisco.local) and the credentials for the admin account, and then click **Next**.

Step 15: Select **Monitoring**, and then in the **Role** list, choose **Primary**. Make sure **Administration** and **Policy Service** are not selected.

Step 16: Click **Submit**. The node registers, and a pop-up window displays letting you know that the process was successful. Click **OK**.



Step 17: In the Deployment Node window, click **ise-1**.

Step 18: Clear **Monitoring**, and then click **Save**. The node updates, and a message displays letting you know that the process was successful. Click **OK**. The node restarts.

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The left sidebar shows the 'Deployment' menu. The main content area is titled 'Edit Node' and shows the configuration for a node named 'ise-1'. The node type is 'Identity Services Engine (ISE)'. The role is set to 'PRIMARY'. The 'Monitoring' checkbox is unchecked. The 'Policy Service' checkbox is checked, and 'Enable Session Services' is also checked, with 'ISE-Group' selected in the 'Include Node in Node Group' dropdown. The 'Enable Profiling Service' checkbox is also checked. The 'Save' button is visible at the bottom.

Step 19: Log in to the console, and then in the **Administration** menu, in the System section, choose **Deployment**.

Step 20: In the Deployment Node window, click **Register**, and then choose **Register an ISE Node**.

Step 21: Enter the IP address or host name of the secondary administration Cisco ISE from Table 1 (in this example, ise-2.cisco.local) and the credentials for the admin account, and then click **Next**.

Step 22: Select only **Administration** and **Policy Service**. In the Administration section, in the **Role** list, choose **Secondary**, and then in the Policy Service section, in the **Node Group** list, choose **ISE-Group**.

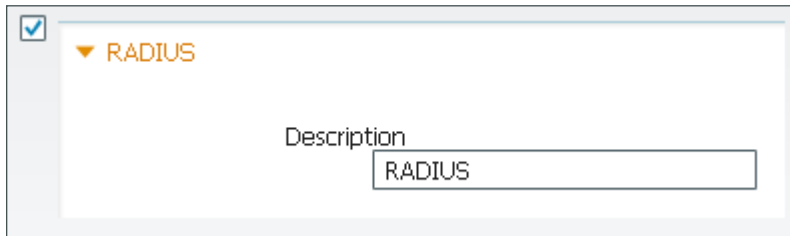
Step 23: Click **Submit**. The node registers, and a pop-up window displays letting you know that the process was successful. Click **OK**.

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The left sidebar shows the 'Deployment' menu. The main content area is titled 'Register ISE Node - Step 2: Configure Node'. The node type is 'Identity Services Engine (ISE)'. The role is set to 'SECONDARY'. The 'Monitoring' checkbox is unchecked. The 'Policy Service' checkbox is checked, and 'Enable Session Services' is also checked, with 'ISE-Group' selected in the 'Include Node in Node Group' dropdown. The 'Enable Profiling Service' checkbox is also checked. The 'Submit' button is visible at the bottom.

Next, you'll configure which methods are used to profile network endpoints for the secondary policy service node.

Step 24: In the **Deployment Nodes** list, click **ise-2**.

Step 25: On the Profiling Configuration tab, select **RADIUS**, and use the default parameters.



A screenshot of a configuration window for RADIUS. On the left, there is a checked checkbox and a dropdown menu showing 'RADIUS'. To the right, there is a 'Description' label followed by a text input field containing the word 'RADIUS'.

Step 26: Select **HTTP**, use the default parameters, and then click **Save**.



A screenshot of a configuration window for HTTP. On the left, there is a checked checkbox and a dropdown menu showing 'HTTP'. To the right, there are two fields: 'Interface' with a dropdown menu showing 'GigabitEthernet 0', and 'Description' with a text input field containing 'HTTP'.

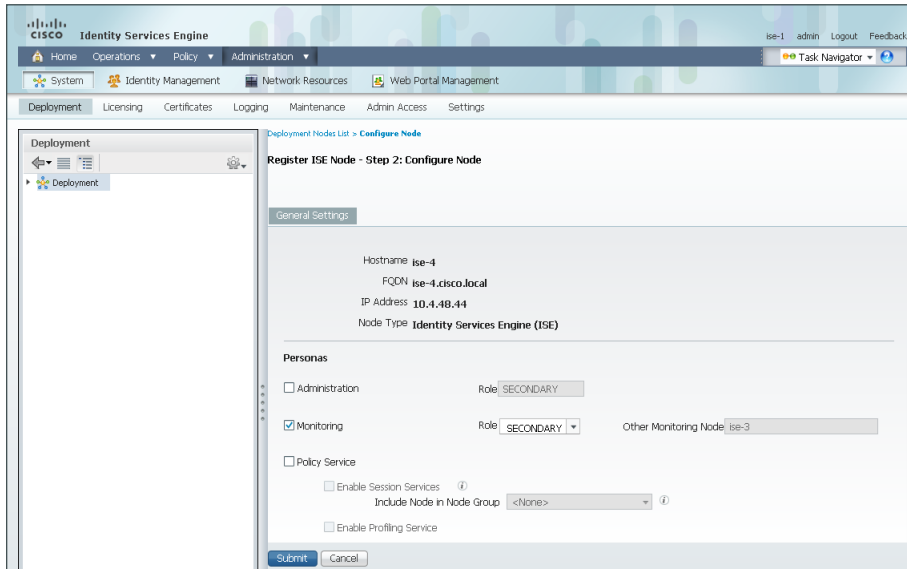
Step 27: In the Edit Node window, click **Deployment Nodes List**. The Deployment Nodes window appears.

Step 28: In the Deployment Nodes window, click **Register**, and then choose **Register an ISE Node**.

Step 29: Enter the IP address or host name of the secondary monitoring Cisco ISE from Table 1 (in this example, ise-4.cisco.local) and the credentials for the admin account, and then click **Next**.

Step 30: Select **Monitoring**, and then in the **Role** list, choose **Secondary**. Make sure **Administration** and **Policy Service** are not selected.

Step 31: Click **Submit**. The node registers, and a pop-up window displays letting you know that the process was successful. Click **OK**.



You have now deployed all Cisco ISE nodes: a pair of redundant administration and policy service nodes and a pair of redundant monitoring nodes.

Procedure 5 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.

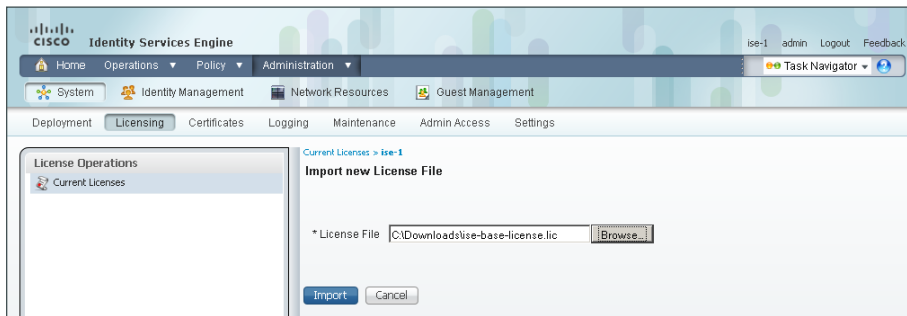
Step 1: Mouse over **Administration**, and then, from the System section of the menu, choose **Licensing**.

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

Step 2: Click the name of the Cisco ISE server. This enables you to edit the license details.

Step 3: Under Licensed Services, click **Add Service**.

Step 4: Click **Browse**, locate your license file, and then click **Import**.



Step 5: If you have multiple licenses to install, repeat the process for each.

Procedure 6 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: Mouse over **Administration**, and then, from the Network Resources section of the menu, choose **Network Devices**.

Step 2: In the left pane, click **Default Device**.

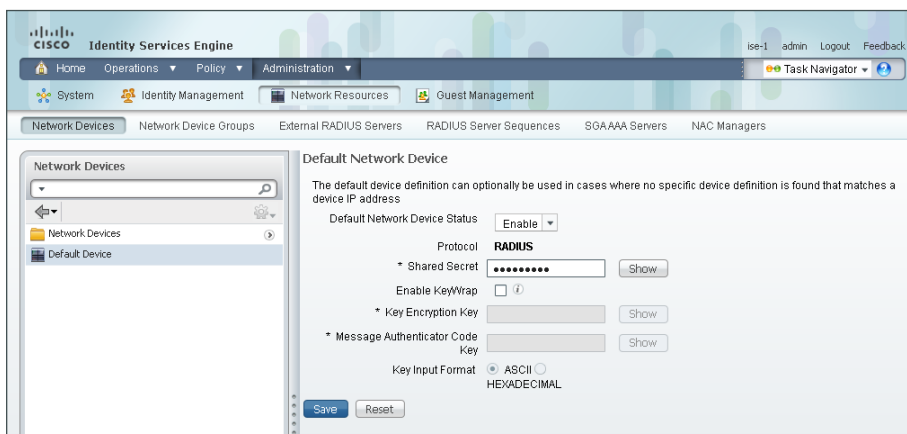


Tech Tip

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

Step 4: Enter the RADIUS shared secret, and then click **Save**.



Procedure 7 Configure Cisco ISE to use Active Directory

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

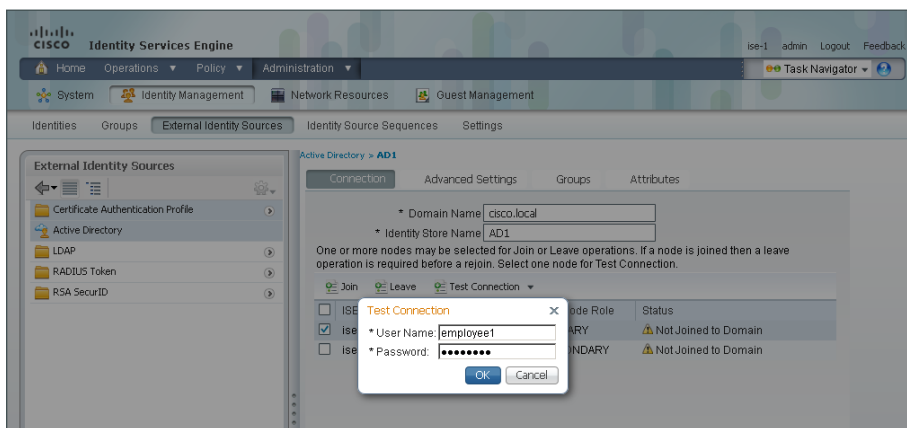
Step 1: Mouse over **Administration**, and then, from the Identity Management section of the menu, choose **External Identity Sources**.

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**.

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

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

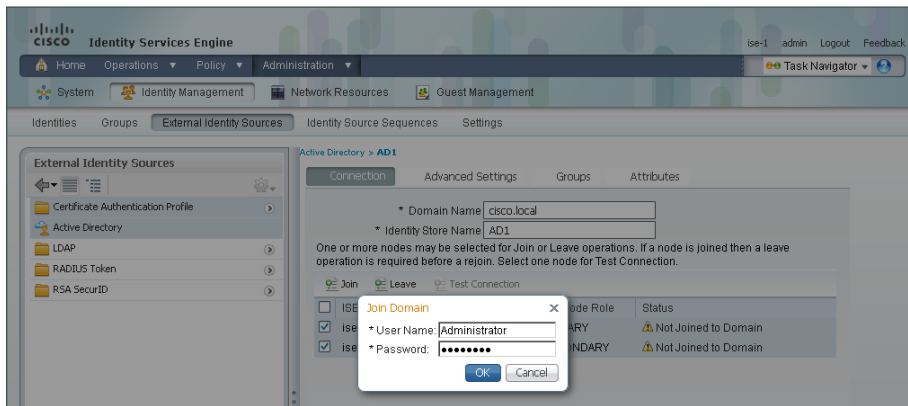


Step 6: A message appears letting you know whether or not the test was successful. Click **Close**.

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

Step 8: Enter the credentials for a domain administrator account. Cisco ISE is now joined to the AD domain.

Step 9: A message appears letting you know whether or not the join was successful. Click **Close**.

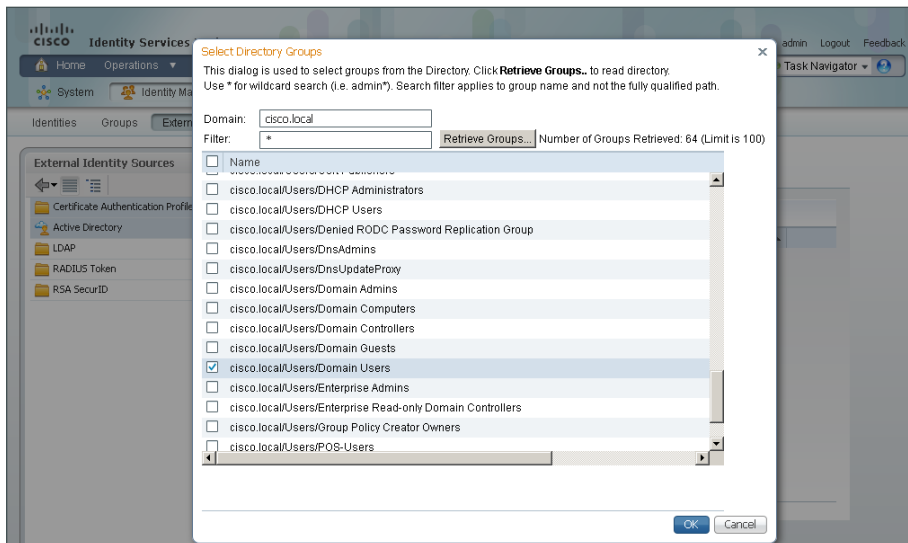


Next, you select which groups from AD that Cisco ISE will use for authentication.

Step 10: 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.

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**.



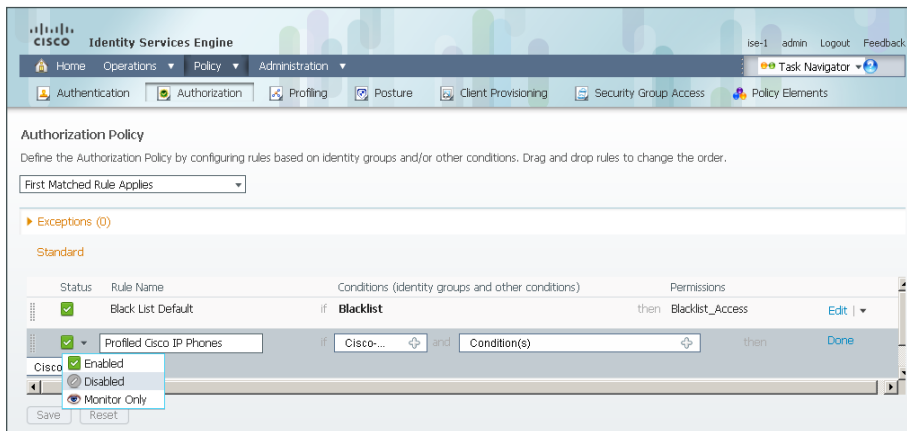
Step 13: Click **Save Configuration**.

Procedure 8 Disable IP Phone authorization policy

There is a default policy in place for Cisco IP Phones that have been profiled. This profile applies a downloadable access list on the port to which the phone is connected. Since there is no policy enforcement taking place at this point, this rule should be disabled.

Step 1: On the menu bar, mouse over **Policy**, and then click **Authorization**.

Step 2: For the **Profiled Cisco IP Phones** rule, click **Edit**, click the green check mark icon, choose **Disabled**, click **Done**, and then click **Save**.



PROCESS

Enabling Visibility to the LAN

1. Configure MAC Authentication Bypass
2. Configure 802.1X for wired users
3. Enable RADIUS in the access layer
4. Enable identity
5. Disable port security timers
6. Configure identity on Catalyst 4500

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 Cisco Prime LMS 4.2 and the Cisco TrustSec Work Center.

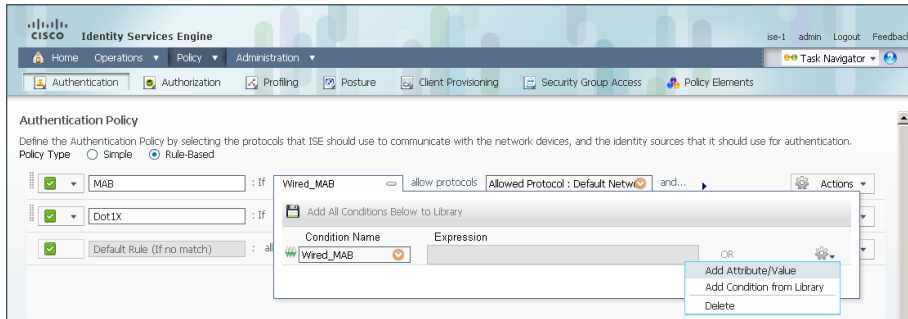
Procedure 1 Configure MAC Authentication Bypass

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: Mouse over **Policy**, and then choose **Authentication**. The Policy Type is Rule-Based.

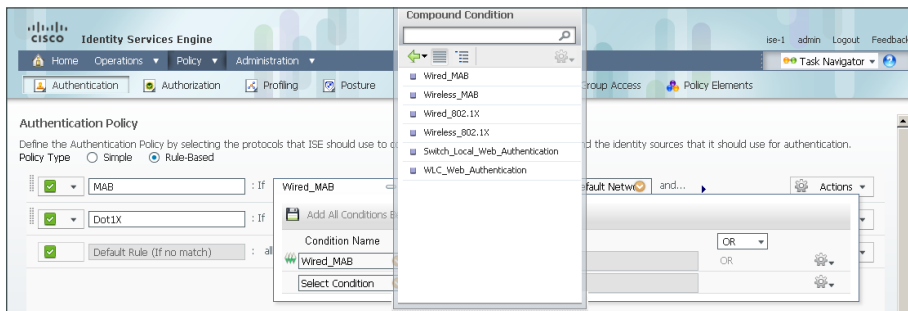
There are already two default rules in place, MAB and Dot1X.

Step 2: Next to Wired_MAB, click the + symbol. To the right of the Wired_MAB condition name, click the gear symbol, and then choose **Add Condition from Library**.

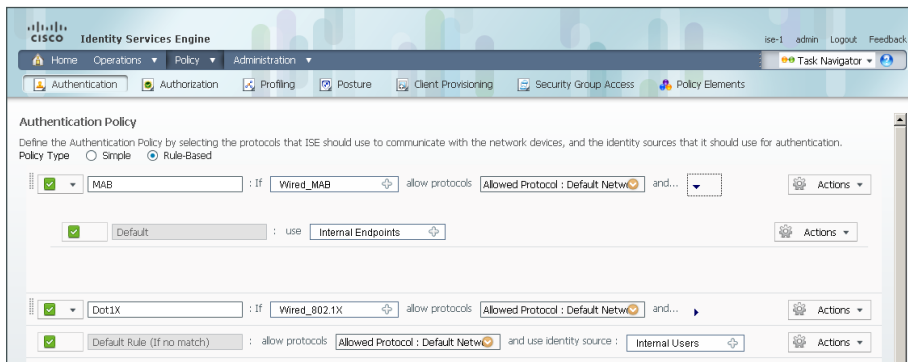


Step 3: In the **Select Condition** list, next to Compound Condition, click the > symbol.

Step 4: Choose **Wireless_MAB**, and then click anywhere to continue.



Step 5: 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.

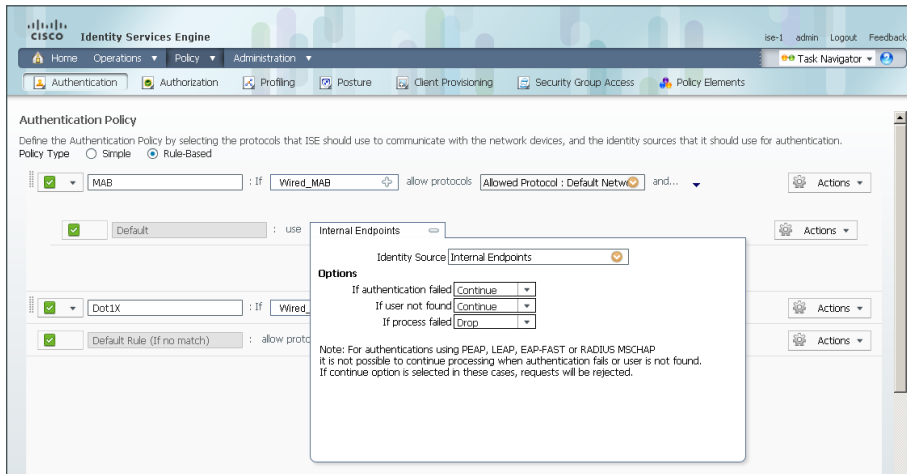


Next, you change the options on the Internal Users database, which is used for profiling.

Step 6: Next to Internal Endpoints, click the +.

Step 7: In this example deployment, all endpoints are allowed to authenticate. Set the following values, click anywhere in the window in order to continue, and then click **Save**:

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



Procedure 2 Configure 802.1X for wired 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.

Step 1: Mouse over **Policy**, and then, from the menu, choose **Authentication**.

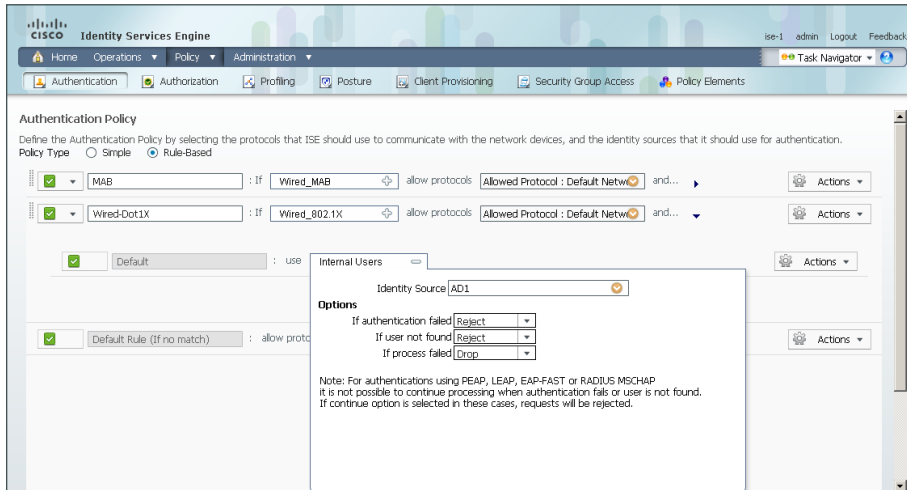
Step 2: Rename the rule **Wired-Dot1X**. This differentiates the rule from a wireless 802.1X rule.

Step 3: For the **Wired-Dot1X** rule, click the black triangle to the right of the **and....** This brings up the identity store used for this rule.

The default identity store is the internal user database. For 802.1X, use the Active Directory server that you defined earlier.

Step 4: Next to Internal Users, click the **+** symbol. This enables you to edit the identity store and the parameters.

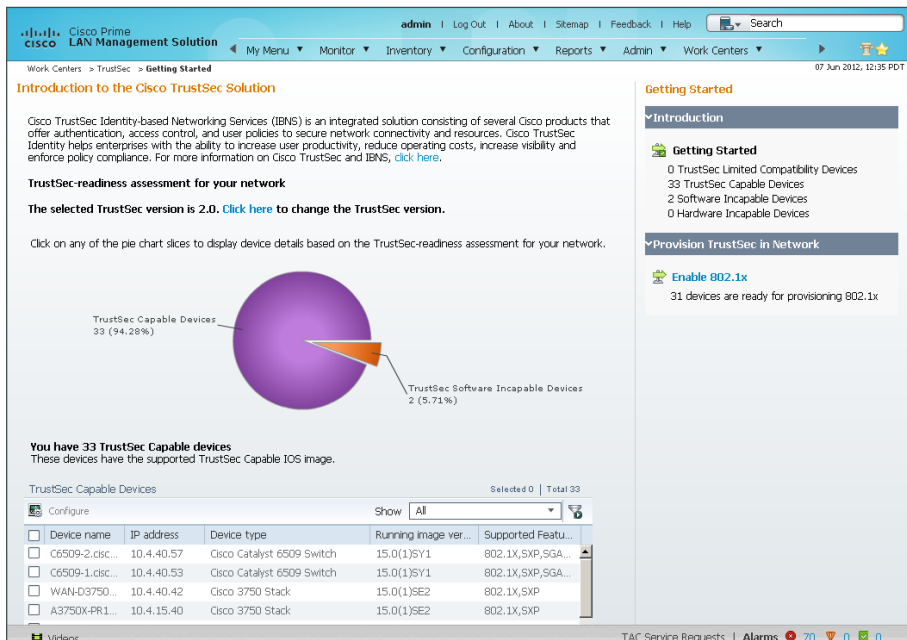
Step 5: In the **Identity Source** list, choose the previously defined AD server **AD1**, use the default options for this identity source, click anywhere in the window to continue, and then click **Save**.



Procedure 3 Enable RADIUS in the access layer

Step 1: In a web browser, connect to Cisco Prime LMS, for example: <https://lms.cisco.local>.

Step 2: Mouse over **Work Centers**, and then, from the TrustSec section, choose **Getting Started**. This shows the network's Cisco TrustSec-readiness assessment, which verifies that the software versions support the identity features and that the switches are capable of running RADIUS.





Tech Tip

Cisco Prime LMS 4.2 supports TrustSec 2.0 features. The TrustSec 2.0 feature set did not include support for the Cisco Catalyst 4500 Series Switches. Alternate procedures are listed in this guide for configuring these switches.

Next, you configure identity by enabling RADIUS on the switch.

Step 3: Mouse over **Work Centers**, and then, from the TrustSec section, choose **RADIUS Configuration**.

Step 4: In the RADIUS-capable devices table, select the switches for which you want to enable RADIUS, and then click **Next**.

Step 5: On the Configure RADIUS page, select **RADIUS Group**, and in the **RADIUS Group Name** box, enter **ISE-Group**, and then in the **Shared Key** box, use the value used in previous procedures.

Step 6: In the RADIUS Server Details section, click **Add**.

Step 7: In the pop-up window, for the RADIUS server IP address, enter **10.4.48.41**, and then click **Save and add another**.

Step 8: For the second RADIUS server, enter **10.4.48.42**, and then click **Save**. The RADIUS server group has been configured.

Step 9: In the AAA Configuration section, make sure that only **Enable for 802.1X / MAB AAA** is selected. A message about not configuring AAA for web authentication appears. Click **OK**.

Configure RADIUS

It is recommended to have RADIUS server configuration for authentication and authorization before configuring identity on the devices. The following workflow facilitates RADIUS server configuration and make the devices radius enabled.

Select Devices ✓

Configure RADIUS Server

Radius Configuration

RADIUS host ☐ Single ☒ RADIUS Group

All fields are required.

You can create only single RADIUS group, which can contain multiple RADIUS servers.

RADIUS Group Name Shared Key
 Verify Shared Key

Add the details of the RADIUS servers that will be part of this RADIUS group. The order of addition is important as the first entry acts as the primary RADIUS, the second as the secondary and so on.

RADIUS Server Details

Server Name or IP Address	Authentication port	Accounting port
<input type="radio"/> 10.4.48.41	1645	1646
<input type="radio"/> 10.4.48.42	1645	1646

AAA Configuration

☒ Enable for 802.1X / MAB AAA.
☐ Enable AAA for Web Authentication.

Schedule Deployment

Step 10: On the Configure RADIUS page, click **Next**.



Tech Tip

You can review the CLI commands that will be pushed to the switch by clicking **Preview CLI**.

Step 11: Enter a job description, and then click **Finish**. Deployment begins immediately.

Step 12: When you receive the message regarding the addition of AAA commands, click **Yes**, and then on the pop-up window generated after the job is created, click **OK**.

Procedure 4 Enable identity

The identity configuration enables monitor mode on the switch. This enables both 802.1X and MAC Authentication Bypass (MAB); however, no authentication policy is enabled. This allows the ports to be monitored with no disruption to current network activity.

Step 1: Mouse over **Work Centers**, and then, under the TrustSec section, choose **Identity Configuration**.

Step 2: In the Navigator pane, click **Enable Identity on Interfaces**.

Step 3: In the **Filter** list, choose the switch that was previously configured for RADIUS, in the **Port Group Selector** pane, select **All Groups**, and then click **Next**.

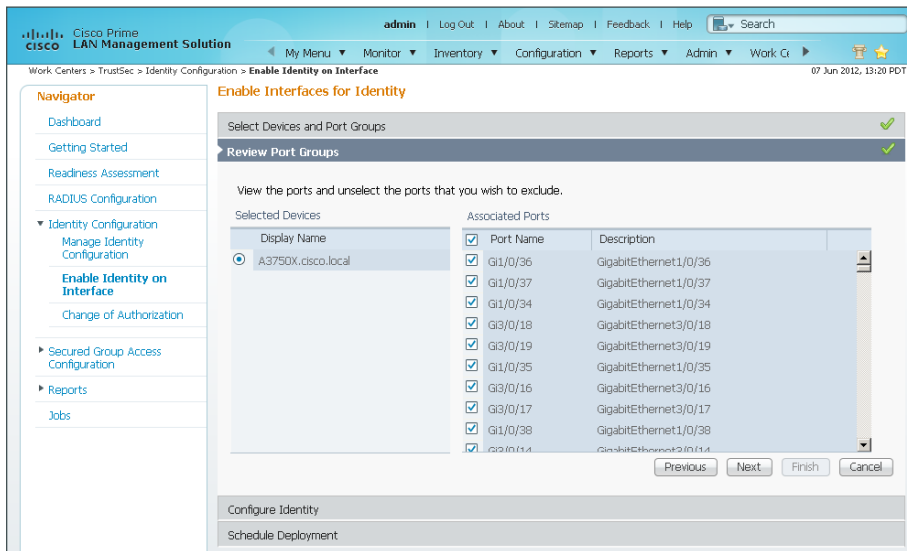
The screenshot displays the Cisco Prime LAN Management Solution web interface. The top navigation bar includes links for 'admin', 'Log Out', 'About', 'Sitemap', 'Feedback', and 'Help'. The main content area is titled 'Enable Interfaces for Identity' and features a 'Select Devices and Port Groups' section. This section contains a table of 'Identity Capable Devices' with columns for 'Display Name', 'IP Address', and 'Device Type'. The device 'A3750X.cisco.local' is selected. To the right, the 'Port Group Selector' pane shows a list of port groups, with 'All Groups' selected. The bottom of the page includes a 'Review Port Groups' section and a 'Schedule Deployment' button. The status bar at the bottom indicates 'TAC Service Requests' and 'Alarms'.

Display Name	IP Address	Device Type
A2960S.cisco.local	10.5.20.5	stack
RS204-A2960S.cisco.local	10.5.60.5	Cisco Catalyst 2960 stack
RS211-A2960S.cisco.local	10.5.156.5	Cisco Catalyst 2960 stack
RS208-A2960S.cisco.local	10.5.87.2	Cisco Catalyst 2960 stack
RS232-D3750X.cisco.local	10.5.215.254	Cisco 3750 Stack
RS208-A3560X-PR1.cisco.local	10.5.87.3	Cisco Catalyst 3560X-24P-L,S Switch
RS232-A3560X.cisco.local	10.5.215.2	Cisco Catalyst 3560X-24P-L,S Switch
<input checked="" type="checkbox"/> A3750X.cisco.local	10.4.79.2	Cisco 3750 Stack
D6500VSS.cisco.local	10.4.15.254	Cisco Virtual Switching System

Port Group Selector:

- ☒ All Groups
- ☒ 1 Gbps Ethernet Ports
- ☒ 10 Gbps Ethernet Ports
- ☒ 10 Mbps Ethernet Ports
- ☒ 100 Mbps Ethernet Ports
- ☒ Access Ports
- ☒ DMP Ports
- ☒ End Hosts
- ☒ IP Phones
- ☒ IPVSC Ports

Step 4: Select the check boxes next to the ports for which you want to enable identity, and then click **Next**.



Next, you configure monitor mode.

Step 5: In the Identity mode to be configured section, move the **Security Mode** slider to **Monitor**, which is the default.

Step 6: In the Authentication profile and host mode section, set the following values:

- Define Authentication Profile—**802.1X**, then **MAB**
- Define Host Mode—**MultiAuth**
- Action to be taken on security violation—**No Change**

In the MAC Configuration section, make sure only **Enable MAC Move** is selected.

Step 7: In the Additional Configurations section, select **Advanced Options**, and then in the **Adhoc commands** box, enter the following command, and then click **Next**.

```
device-sensor accounting
```



Tech Tip

For device profiling, you need to enable the IOS Sensor feature on the switch to include DHCP and CDP information in the RADIUS messages sent from the switch to Cisco ISE. The IOS Sensor feature relies on information from the DHCP snooping feature that was enabled in the [Campus Wired LAN Design Guide](#). This feature is not supported on the Cisco Catalyst 2960S access layer switches. If you want to use device profiling in the access layer, you will need to deploy Cisco Catalyst 3560, 3750, or 4500 Series Switches.

The screenshot displays the 'Enable Identity on Interface' configuration page in the Cisco Prime LAN Management Solution. The page is divided into several sections:

- Enable Interfaces for Identity:** Includes 'Select Devices and Port Groups' and 'Review Port Groups', both marked with green checkmarks.
- Configure Identity:**
 - Identity mode to be configured:** A slider for 'Security Mode' is positioned between 'Monitor' and 'Low impact', with 'High security' at the end. A 'More Details' link is available.
 - Authentication profile and host mode:** 'Define Authentication Profile' is set to '802.1x, then MAB'. The 'Define Host Mode' section has 'MultiAuth' selected. Below, 'Action to be taken when a port security violation is detected' has 'No change' selected.
 - MAC Configuration:** 'Enable MAC move or replace' has 'Enable MAC move' checked. 'Enable SNMP notification for MAC addition or removal' has 'Notify MAC addition' and 'Notify MAC removal' unchecked.
 - Additional Configurations:** 'Advanced options' is checked. The 'Adhoc commands*' field contains the text 'device-sensor accounting'.

At the bottom, there are buttons for 'Previous', 'Next', 'Finish', and 'Cancel', and a 'Schedule Deployment' button.

Identity configuration is complete. Next, you create a deployment job in order to deliver the configuration to the switch.

Step 8: In the **Job Description** box, enter a description, click **Finish**, and then click **OK**.



Tech Tip

You can review the CLI commands that will be pushed to the switch by clicking **Preview CLI**.

The global commands added to the switch configuration at the completion of the previous two procedures are as follows.

```
radius-server host 10.4.48.41 auth-port 1645 acct-port 1646
radius-server host 10.4.48.42 auth-port 1645 acct-port 1646
radius-server key [key]
aaa group server radius ISE-Group
  server 10.4.48.41 auth-port 1645 acct-port 1646
  server 10.4.48.42 auth-port 1645 acct-port 1646
```

```
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
```

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

The interface commands added at the completion of the previous two procedures are as follows.

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

Procedure 5 Disable port security timers

The current CVD incorporates the use of port security to provide a level of security and prevent rogue devices from being connected. However, 802.1X also provides this functionality and there can be conflicts when both are enabled on a port at the same time. This is particularly true of inactivity timers since both port security and 802.1X each have their own set of timers. The conflict causes 802.1X to re-authenticate every time the port security time out is reached. To avoid this issue, port security timers need to be disabled.

Step 1: Connect to the Cisco Prime LMS server by browsing to <https://lms.cisco.local>.

Step 2: Navigate to **Configuration > Tools > NetConfig**. This opens the Job Browser.

Step 3: Click **Create**. This enables you to configure a new job.

Step 4: Select **Port based**, and then click **Go**.

Step 5: In the tree, next to All Devices, click the + symbol, select the switch you are configuring, and then click **Next**.



Tech Tip

In this example, only one switch is being configured, but you can select multiple switches to accommodate a large deployment. The Group Selector allows you to choose switches by pre-defined groups or by model.

Step 6: Select **Define an Ad-Hoc Rule**. A new screen is displayed.

Step 7: For the ad-hoc rule, in the **Object Type** list, choose **Port**.

Step 8: In the **Variable** list, choose **Identity_Security_Mode**.

Step 9: In the **Operator** list, choose **=**, and then in the **Value** list, choose **Monitor**.

Step 10: Click **Add Rule Expression**, and then click **Next**.

The screenshot shows the Cisco Prime LAN Management Solution interface. The main content area is titled "Groups" and "Port Groups". It displays the "Adhoc Rule" configuration page. The "Object Type: Variable" dropdown is set to "Port", and the "Operator: Value" dropdown is set to "UnSecured". The "Rule Text" area contains the expression "Port.Identity_Security_Mode = \"Monitor\"". The "Add Rule Expression" button is visible. The page is titled "Groups" and "Port Groups". The left sidebar shows a navigation menu with "Groups" selected. The bottom status bar shows "TAC Service Requests | Alarms 71 0 0 0".

Step 11: In the Task Selector, select **Adhoc Task**, and then click **Next**.

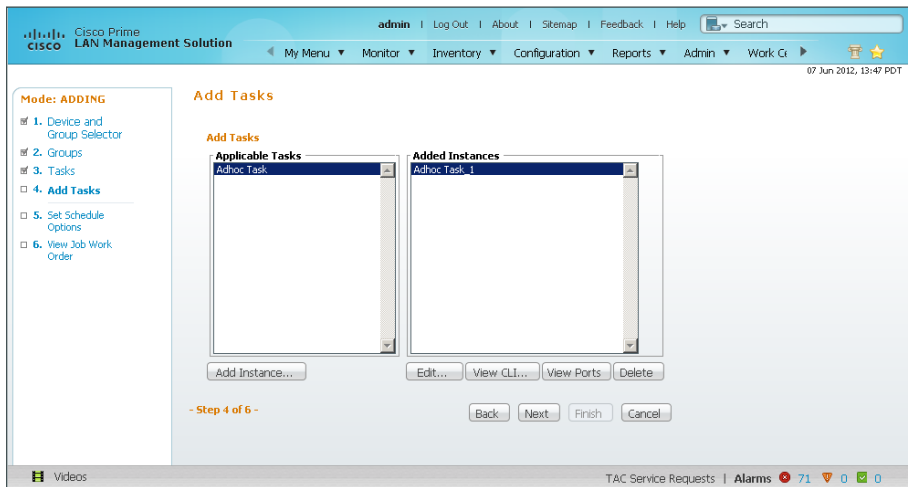
Step 12: Click **Add Instance**, and then, in the new window, enter the CLI commands necessary to remove the port security configuration.

```
no switchport port-security aging time
no switchport port-security aging type
no switchport port-security violation
```

Step 13: Click **Applicable Devices**, select the switch to which you want to apply this configuration, click **Close**, and then click **Save**.

The screenshot shows the "Adhoc Task Configuration" window. The "IOS Parameters" section is expanded, showing the "Commands" tab. The "CLI Commands" text area contains the commands: "no switchport port-security aging time", "no switchport port-security aging type", and "no switchport port-security violation". The "Rollback Commands" text area is empty. The "Applicable Devices..." button is visible. The "Save", "Reset", and "Cancel" buttons are at the bottom.

Step 14: After returning to the Add Tasks window, click **Next**.



Step 15: Fill in a description for the job, and then click **Next**. The job is submitted for immediate deployment.

Step 16: Click **Finish**, and then when you receive a notice that the job was submitted successfully, click **OK**.

Procedure 6 Configure identity on Catalyst 4500

Cisco TrustSec Work Center supports TrustSec 2.0 features, but does not support Cisco Catalyst 4500. However, Catalyst 4500 does support all of the features in use. You have to configure these by using the NetConfig feature of Cisco LMS. This procedure covers enabling RADIUS, configuring 802.1X in monitor mode, and disabling port security.

Step 1: Connect to the Cisco Prime LMS server by browsing to <https://lms.cisco.local:1741>.

Step 2: Mouse over **Configuration**, and then, from the Tools section, choose **NetConfig**.

Step 3: In the NetConfig Job Browser, click **Create**.

Step 4: Select **Device Based** for the NetConfig Job Type, and then click **Go**.

Step 5: In the Device Selector, expand **All Devices**, select the devices where you want to enable identity.

Step 6: In the Task Selector, expand **All Tasks**, select **Adhoc**, and then click **Next**.

Step 7: Click **Add Instance**, and then, in the new window, enter the CLI commands necessary to configure identity.

```
radius-server host 10.4.48.41 auth-port 1645 acct-port 1646
radius-server host 10.4.48.42 auth-port 1645 acct-port 1646
radius-server key [key]
aaa group server radius ISE-Group
    server 10.4.48.41 auth-port 1645 acct-port 1646
    server 10.4.48.42 auth-port 1645 acct-port 1646

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

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

Step 8: Click **Applicable Devices**, select the switch to which you want to apply this configuration, and then click **Close**.

Step 9: For the command mode, choose **Config**, and then click **Save**.

Step 10: After returning to the Add Tasks window, click **Next**.

Step 11: Fill in a description for the job, and then click **Next**. The job is submitted for immediate deployment.

Step 12: Click **Finish**, and then when you receive a notice that the job was submitted successfully, click **OK**.

Step 13: Navigate to **Configuration > Tools > NetConfig**. This opens the Job Browser.

Step 14: Click **Create**. This enables you to configure a new job.

Step 15: Select **Port based**, and then click **Go**.

Step 16: In the tree, next to All Devices, click the **+** symbol, select the switch you are configuring, and then click **Next**.



Tech Tip

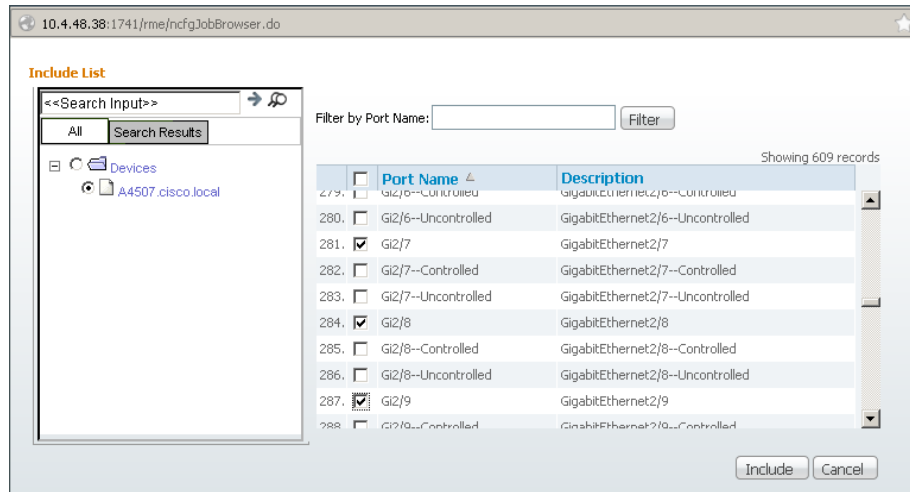
In this example, only one switch is being configured, but you can select multiple switches to accommodate a large deployment. The Group Selector allows you to choose switches by pre-defined groups or by model.

Step 17: Select **Define an Ad-Hoc Rule**. A new screen is displayed.

Step 18: For the ad-hoc rule, in the **Rule text** section, click **Include**.

Step 19: In the Include List section, expand **Devices**, and then select the switch you want to configure for identity.

Step 20: Choose the ports you want to configure for identity, and then click **Include**. The window closes.



Step 21: Move to step 3 of the wizard by clicking **Next**.

Step 22: In the Task Selector, select **Adhoc Task**, and then click **Next**.

Step 23: Click **Add Instance**, and then, in the new window, enter the CLI commands necessary in order to enable monitor mode and remove the port security configuration.

```
authentication host-mode multi-auth
authentication open
authentication order dot1x mab
authentication port-control auto
mab
dot1x pae authenticator
no switchport port-security aging time
no switchport port-security aging type
no switchport port-security violation
```


Step 24: Click **Applicable Devices**, select the switch to which you want to apply this configuration, click **Close**, and then click **Save**.

10.4.48.38:1741/rme/ncfgJobBrowser.do

Adhoc Task Configuration

IOS Parameters

Commands

CLI Commands:

```
authentication host-mode multi-auth
authentication open
authentication order dot1x mab
authentication port-control auto
mab
dot1x pae authenticator
no switchport port-security aging time
no switchport port-security aging type
no switchport port-security violation
```

Rollback Commands:

[Applicable Devices...](#)

[Save](#) [Reset](#) [Cancel](#)

Step 25: After returning to the Add Tasks window, click **Next**.

Cisco Prime LAN Management Solution

admin | Log Out | About | Sitemap | Feedback | Help | Search

My Menu | Monitor | Inventory | Configuration | Reports | Admin | Work Cr

07 Jun 2012, 13:47 PDT

Add Tasks

Mode: ADDING

- # 1. Device and Group Selector
- # 2. Groups
- # 3. Tasks
- ☒ 4. Add Tasks
- ☐ 5. Set Schedule Options
- ☐ 6. View Job Work Order

Applicable Tasks	Added Instances
Adhoc Task	Adhoc Task-1

[Add Instance...](#) [Edit...](#) [View CLI...](#) [View Ports](#) [Delete](#)

- Step 4 of 6 -

[Back](#) [Next](#) [Finish](#) [Cancel](#)

Videos

TAC Service Requests | Alarms 71 0 0

Step 26: Fill in a description for the job, and then click **Next**. The job is submitted for immediate deployment.

Step 27: Click **Finish**, and then when you receive a notice that the job was submitted successfully, click **OK**.

Step 28: Repeat this procedure for each Cisco Catalyst 4500 switch where you need to configure identity.

Enabling Visibility to the Wireless Network

1. Configure 802.1X for wireless endpoints
2. Disable EAP-TLS on Cisco ISE
3. Add ISE as RADIUS authentication server
4. Add Cisco ISE as RADIUS accounting server
5. Enable client profiling

To authenticate wireless clients, you need to configure the wireless LAN controllers (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 Configure 802.1X for wireless endpoints

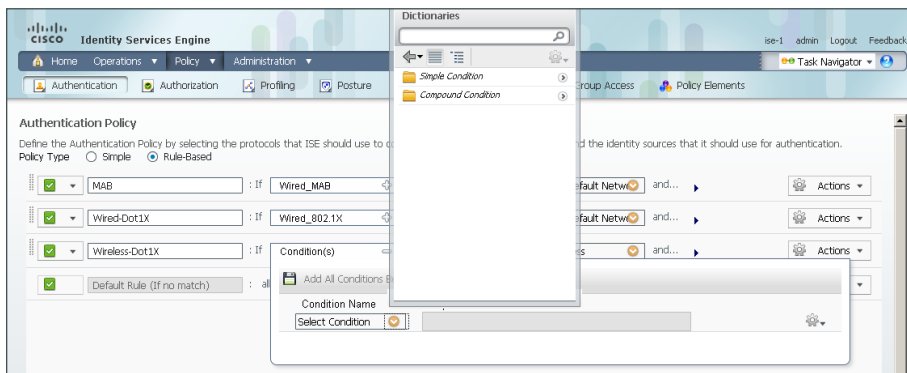
To differentiate wireless users in the authentication logs, create a rule to identify when wireless users authenticate.

Step 1: In a browser, access the primary engine's GUI at <http://ise-1.cisco.local> and navigate to **Policy > Authentication** to open the Authentication Policy page.

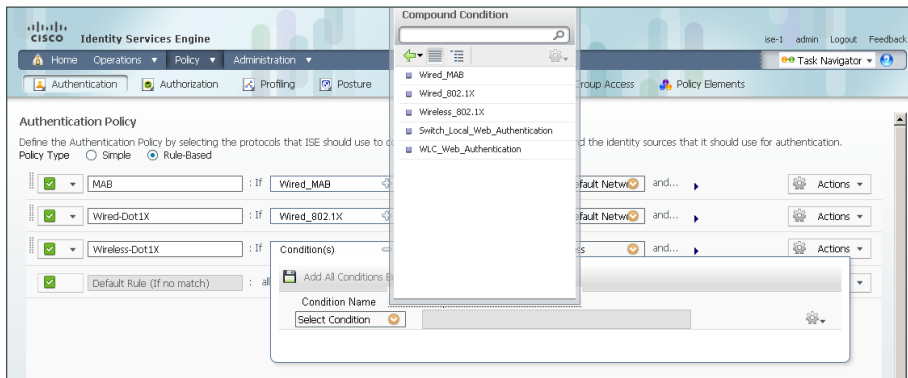
Step 2: For the Default Rule, click the **Actions** button, and then choose **Insert new row above**. A new rule, Standard Policy 1, is created.

Step 3: Rename Standard Policy 1 to **Wireless-Dot1X**. In the **Condition(s)** box, click the **+** symbol, and then choose **Select Existing Condition from Library**.

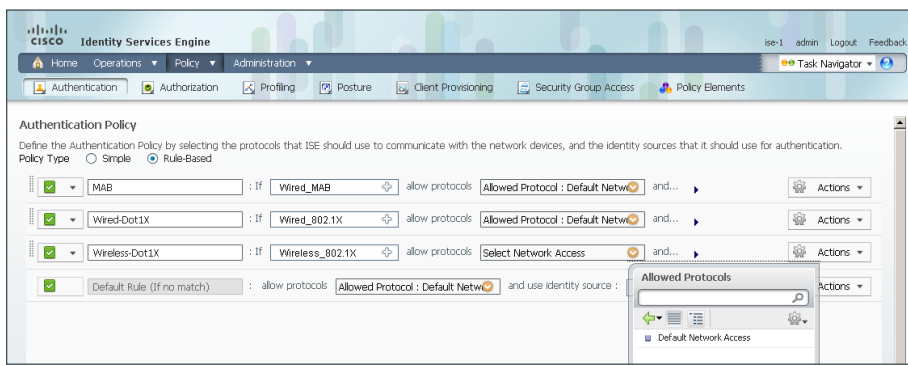
Step 4: In the **Select Condition** list, next to Compound Condition, click the **>** symbol.



Step 5: Choose **Wireless_802.1X**, and then click anywhere to continue.



Step 6: In the **Select Network Access** list, next to Allowed Protocols, click the > symbol, and then select **Default Network Access**.

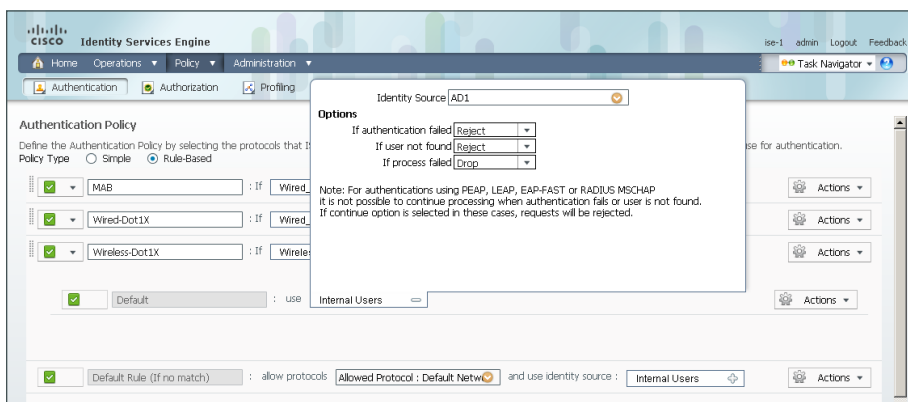


Step 7: For the **Wireless-Dot1X** rule, to the right of and..., click the black triangle. This displays the identity store used for this rule.

Step 8: Next to Internal Users, click the + symbol.

Step 9: In the **Identity Source** list, choose the previously defined AD server, for example, AD1.

Step 10: Use the default options for this identity source, continue by clicking anywhere in the window, and then click **Save**.



Procedure 2 Disable EAP-TLS on Cisco ISE

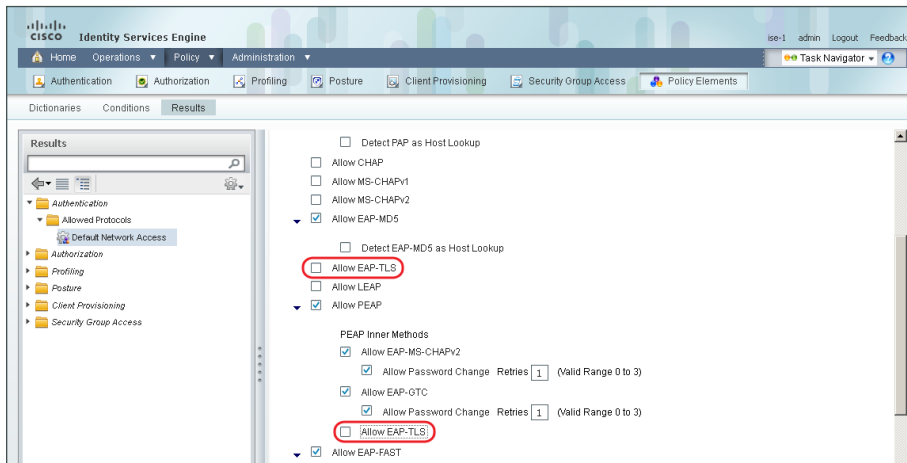
For wireless deployments that aren't currently using digital certificates, you need to disable EAP-TLS in order to allow clients to log in. You will be deploying digital certificates in a later phase of this deployment.

Step 1: On the menu bar, mouse over **Policy**, and then, from the Policy Elements section of the menu, choose **Results**.

Step 2: In the left pane, double-click **Authentication**. This expands the options.

Step 3: Double-click **Allowed Protocols**, and then select **Default Network Access**.

Step 4: Clear the global **Allow EAP-TLS** check box and under the PEAP settings, clear the **Allow EAP-TLS** check box, and then click **Save**.



Procedure 3 Add ISE as RADIUS authentication server

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

Step 1: Navigate to the WLC console by browsing to <https://wlc1.cisco.local>.

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

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

Step 4: Click **New**. A new server is added.

Step 5: In the **Server IP Address** box, enter **10.4.48.41**, and then enter your RADIUS shared secret.

Step 6: Next to Management, clear the **Enable** box, and then click **Apply**.

Security > RADIUS Authentication Servers > Edit

Server Index: 2

Server Address: 10.4.48.41

Shared Secret Format: ASCII

Shared Secret: [REDACTED]

Confirm Shared Secret: [REDACTED]

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

Port Number: 1812

Server Status: Enabled

Support for RFC 3576: Enabled

Server Timeout: 2 seconds

Network User: ☒ Enable

Management: ☐ Enable

IPSec: ☐ Enable

Step 7: Repeat Step 4 through Step 6 in order to add the secondary engine, 10.4.48.42, to the WLC configuration.

After adding Cisco ISE as a RADIUS server, disable the current RADIUS server in use. By disabling the server instead of deleting it, you can easily switch back if needed. Perform this procedure for every wireless LAN controller (WLC) in the architecture with the exception of the standalone guest WLC, if you have deployed one.

Step 8: On the RADIUS Authentication Servers screen, click the Server Index of the original RADIUS server, and then, for Server Status, select **Disabled**. Click **Apply**.

Step 9: On the RADIUS Authentication Servers screen, click **Apply**.

Security > RADIUS Authentication Servers

Call Station ID Type: IP Address

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

MAC Delimiter: Hyphen

Network User	Management	Server Index	Server Address	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	<input type="checkbox"/>	1	10.4.48.15	1812	Disabled	Disabled
<input checked="" type="checkbox"/>	<input type="checkbox"/>	2	10.4.48.41	1812	Disabled	Enabled
<input checked="" type="checkbox"/>	<input type="checkbox"/>	3	10.4.48.42	1812	Disabled	Enabled

Procedure 4 Add Cisco ISE as RADIUS accounting server

Perform this procedure for every wireless LAN controller (WLC) in the architecture, 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**.

Step 3: Click **New**. This adds a new server.

Step 4: In the **Server IP Address** box, enter **10.4.48.41**, enter your RADIUS shared secret, and then click **Apply**.

Security > RADIUS Accounting Servers > Edit

Server Index: 2

Server Address: 10.4.48.41

Shared Secret Format: ASCII

Shared Secret: [masked]

Confirm Shared Secret: [masked]

Port Number: 1813

Server Status: Enabled

Server Timeout: 2 seconds

Network User: ☒ Enable

IPSec: ☐ Enable

< Back Apply

Step 5: Repeat Step 3 through Step 4 in order to add the secondary engine, 10.4.48.42, to the WLC configuration.

Step 6: On the RADIUS Accounting Servers screen, click the Server Index of the original RADIUS server, and then, for Server Status, select **Disabled**. Click **Apply**.

Step 7: On the RADIUS Accounting Servers screen, click **Apply**.

Security > RADIUS Accounting Servers

MAC Delimiter: Hyphen

Network User	Server Index	Server Address	Port	IPSec	Admin Status
<input checked="" type="checkbox"/>	1	10.4.48.15	1813	Disabled	Disabled
<input checked="" type="checkbox"/>	2	10.4.48.41	1813	Disabled	Enabled
<input checked="" type="checkbox"/>	3	10.4.48.42	1813	Disabled	Enabled

Apply New...

Procedure 5 Enable client profiling

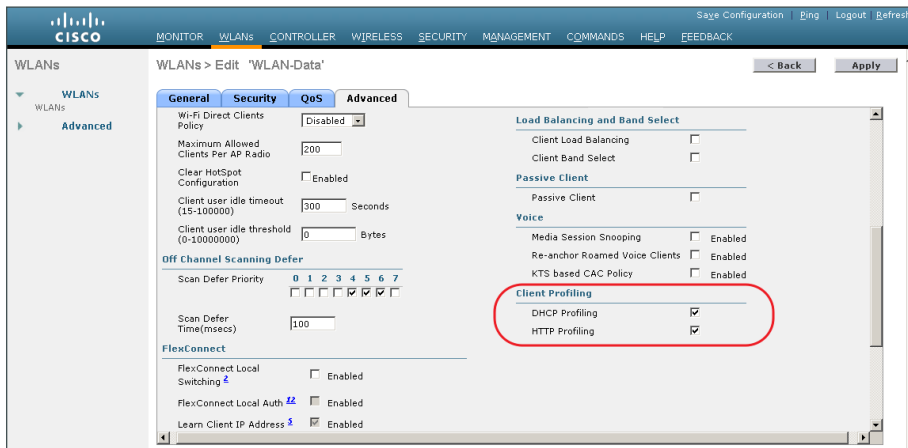
You need to enable client profiling on the WLC in order to send DHCP and HTTP information to the engine for endpoint profiling.

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

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

Step 3: When the message appears about enabling DHCP Req'd and disabling Local Auth, click **OK**.

Step 4: In the Client Profiling section, select **HTTP Profiling**, and then click **Apply**.



Step 5: When a message appears saying that the WLANs need to be disabled, click **OK**.

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.

Deploying Digital Certificates

PROCESS

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 the next 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 will be deploying digital certificates to Microsoft Windows XP and Windows 7 endpoints as well as to Apple Mac OS X devices. The certificate authority (CA) you will be using is the one built into Windows Server 2008 Enterprise, and you will install it as a standalone server.

Procedure 1 Install certificate authority

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

Step 1: Install an enterprise root certificate authority on a Windows 2008 R2 Enterprise server.



Reader Tip

For more information about installing a certificate authority, see the [Microsoft Windows Server 2008 Active Directory Certificate Services Step-by-Step Guide](#).

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, launch a web browser, and then connect to the certificate authority at the following:

<https://ca.cisco.local/certsrv>

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 AD controller.

Microsoft Active Directory Certificate Services -- 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 [CA]

Encoding method:

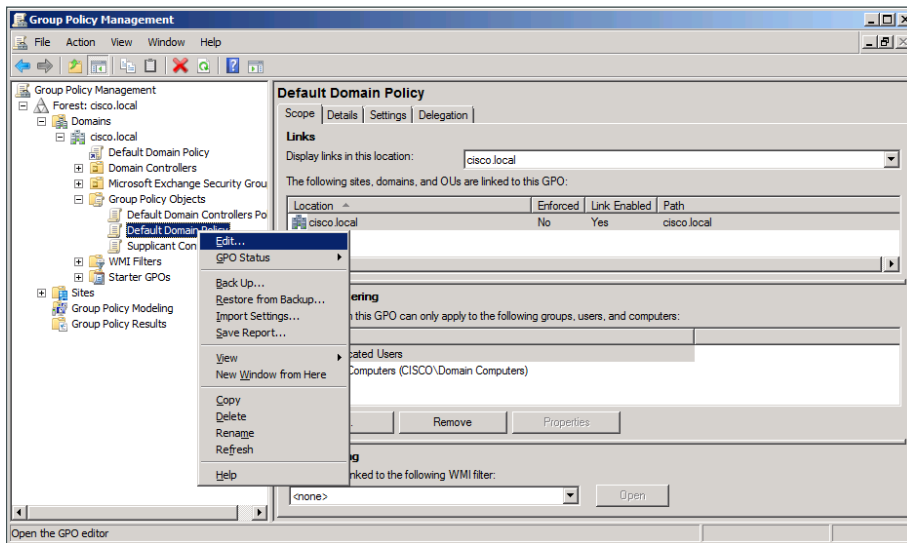
☒ DER
☐ Base 64

[Install CA certificate](#)
[Download CA certificate](#)
[Download CA certificate chain](#)
[Download latest base CRL](#)
[Download latest delta CRL](#)

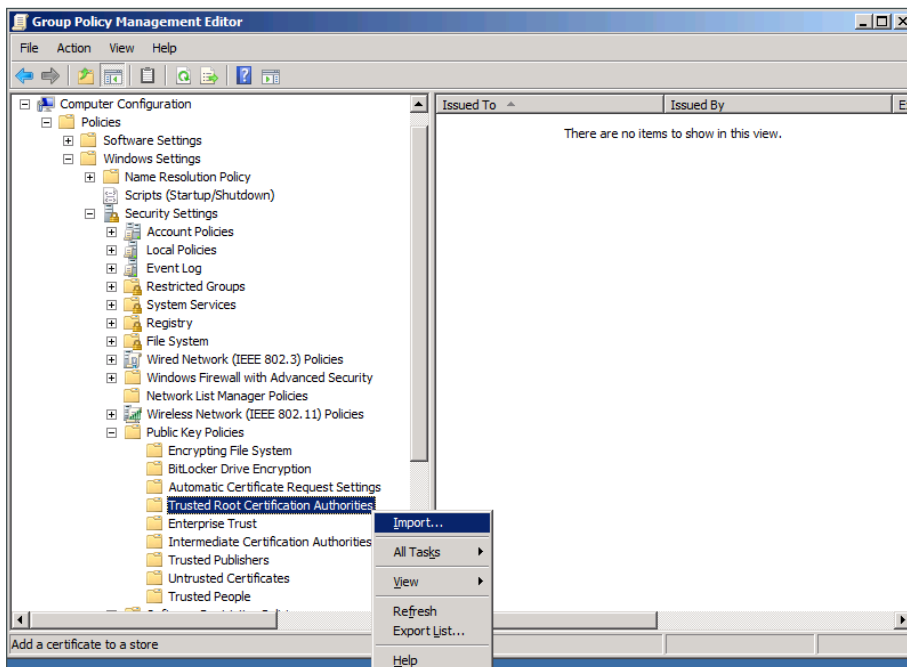
Step 5: On the AD console, navigate to **Start > Administrative Tools > Group Policy Management**.

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

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

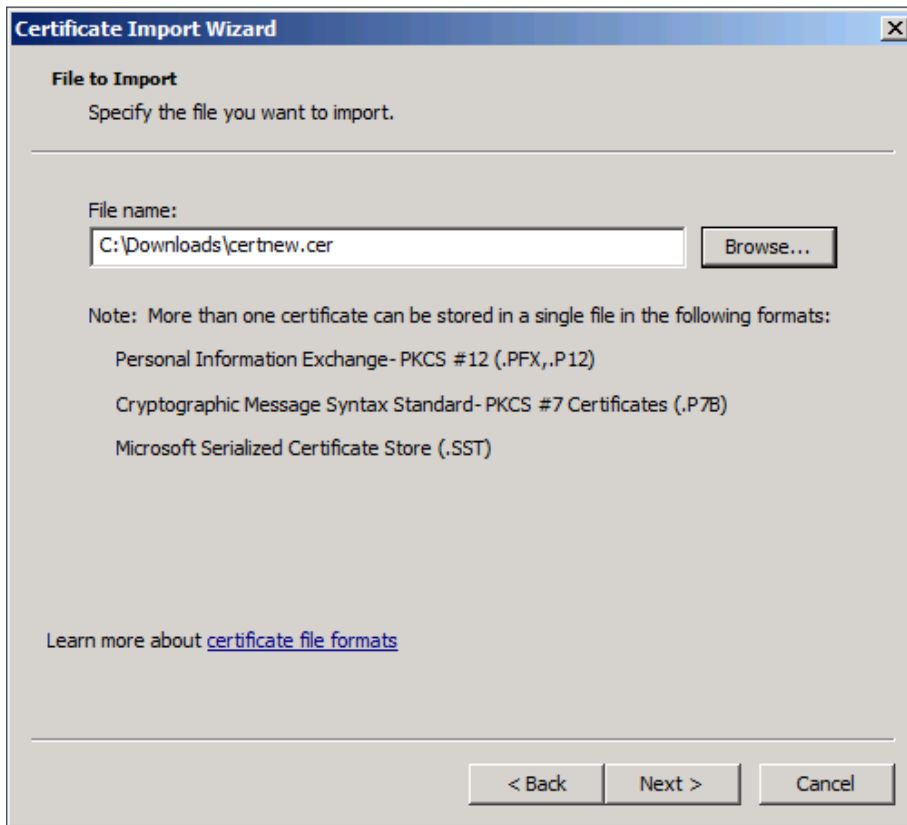


Step 8: Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies**, right-click **Trusted Root Certification Authorities**, and then choose **Import**. The Certificate Import Wizard launches.



Step 9: Click **Next**.

Step 10: Click **Browse**, locate the trusted root certificate saved in Step 2, and then click **Next**.



Step 11: Place the certificate in the Trusted Root Certification Authorities certificate store, and then click **Next**.

Step 12: Click **Finish**. The certificate imports.

Step 13: Click **OK** to close the wizard.

Procedure 3 Install trusted root on AD server

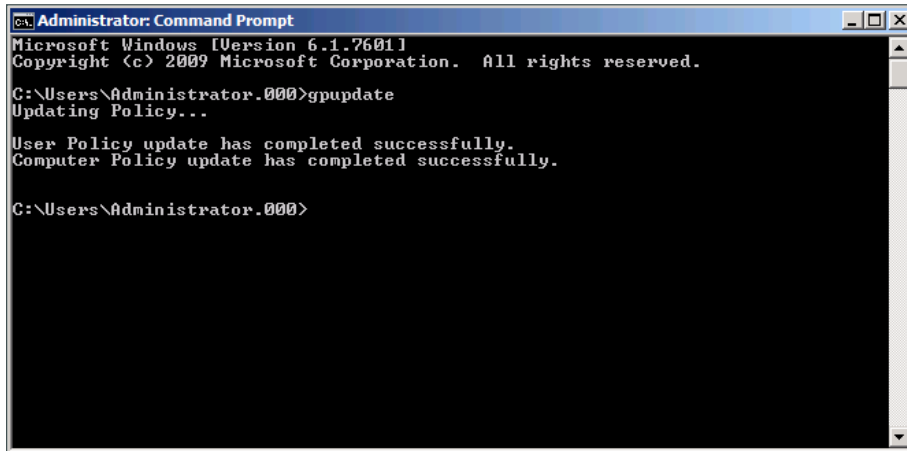
In addition to configuring AD server to distribute the trusted root certificate to workstations, you need to install the certificate directly on the AD server. A group policy object (GPO) update takes care of this automatically. In this procedure, you will force the update to run immediately.

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



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.000>gpupdate
Updating Policy...

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

C:\Users\Administrator.000>
```

Procedure 4 Request a certificate for ISE from the CA

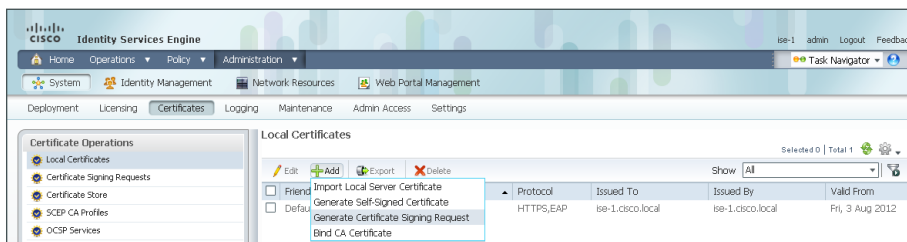
In order to obtain a certificate from the CA, Cisco ISE needs to generate a signing request that will be used by the CA to generate a certificate.

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

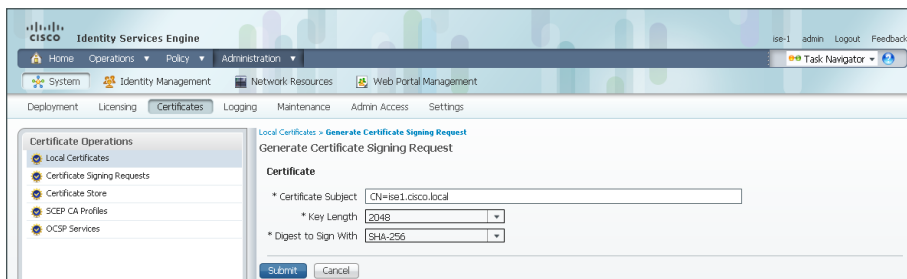
Step 2: Mouse over **Administration**, and then, from the System section of the menu, choose **Certificates**.

Step 3: Under **Certificate Operations**, select **Local Certificates**.

Step 4: Click **Add**, and then choose **Generate Certificate Signing Request**.

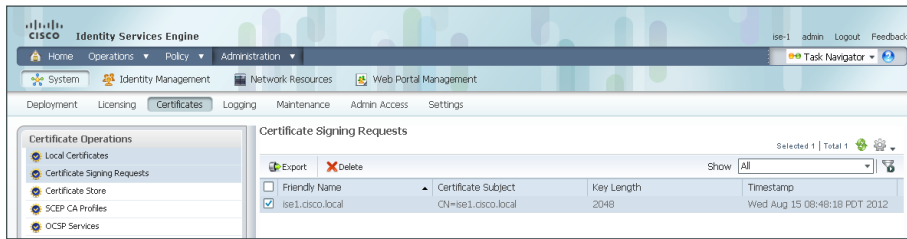


Step 5: In the **Certificate Subject** box, after the "CN=", enter the fully qualified domain name (FQDN) of the Cisco ISE server, and then click **Submit**.



Step 6: On the message acknowledging that the certificate was successfully generated, click **OK**.

Step 7: Click **Certificate Signing Requests**, select the check box next to the new request, and then click **Export**.



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

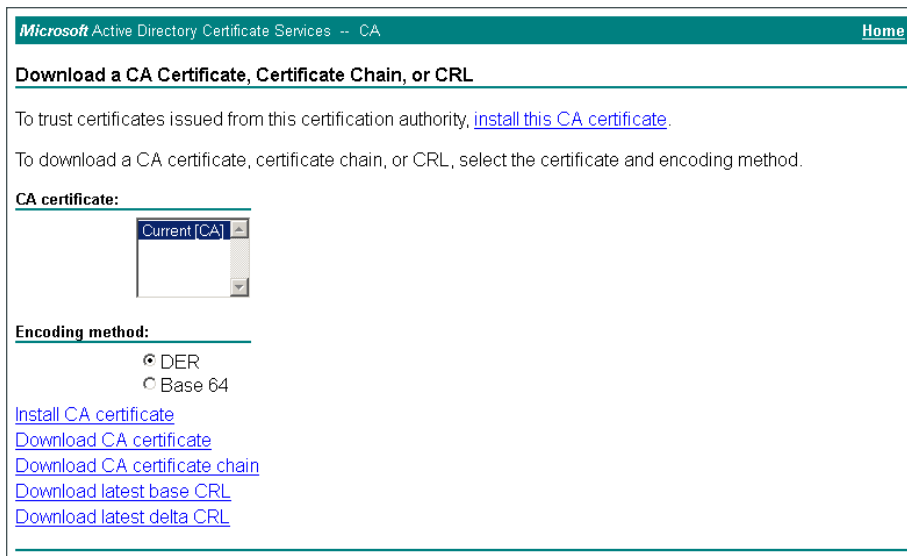
Procedure 5 Download CA root certificate

Step 1: Browse to <https://ca.cisco.local/certsrv>.

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.



Procedure 6 Issue certificate for Cisco ISE

Step 1: Click **Home**. The CA's home screen displays.

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

Step 3: Click **advanced certificate request**.

Step 4: In a text editor, such as Notepad, open the certificate file 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**.

The screenshot shows the "Submit a Certificate Request or Renewal Request" page in the Microsoft Active Directory Certificate Services console. The page has a teal header with "Microsoft Active Directory Certificate Services -- CA" and a "Home" link. Below the header, the title "Submit a Certificate Request or Renewal Request" is displayed. A paragraph explains that users can submit a saved request, a base-64-encoded CMC or PKCS #10 certificate request, or a PKCS #7 renewal request. The "Saved Request:" section contains a text area with a base-64-encoded certificate request. Below this, the "Certificate Template:" section has a dropdown menu set to "Web Server". The "Additional Attributes:" section has a text area for attributes. A "Submit >" button is at the bottom right.

Microsoft Active Directory Certificate Services -- 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):

```
+m1q/yM44JX50YD2YIOH1YKhE3Ru966HdIjGaB3y
fcWzjIloM1JJ1x0kNaXerhitwiU3z4NuvBnqdl0p
W6UFu4SoMSbINYqoW56HoJfiX1t38PeQptQ&euH0
RepCm2VVz9F6BK9QOlngJ2JkSSINQkG0d93uPmPO
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

Additional Attributes:

Attributes:

[Submit >](#)

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

Procedure 7 Install trusted root certificate in Cisco ISE

Step 1: In the Cisco ISE interface, mouse over **Administration**, and then, from the System section of the menu, choose **Certificates**.

Step 2: Click **Certificate Store**, and then click **Import**.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes "Home", "Operations", "Policy", and "Administration". The "Administration" menu is expanded, showing "System", "Identity Management", "Network Resources", and "Web Portal Management". The "System" menu is further expanded, showing "Deployment", "Licensing", "Certificates", "Logging", "Maintenance", "Admin Access", and "Settings". The "Certificates" menu is selected, and the "Certificate Store" page is displayed. The page shows a table of certificates with columns for "Friendly Name", "Issued To", "Issued By", "Valid From", and "Expiration Date". There are four certificates listed, all issued to "ise-1.cisco.local" and issued by "ise-1.cisco.local". The "Valid From" date is "Fri, 3 Aug 2012" and the "Expiration Date" is "Sat, 3 Aug 2020".

Friendly Name	Issued To	Issued By	Valid From	Expiration Date
ise-1.cisco.local#ise-1.cisco.local#00001	ise-1.cisco.local	ise-1.cisco.local	Fri, 3 Aug 2012	Sat, 3 Aug 2020
ise-2	ise-2.cisco.local	ise-2.cisco.local	Fri, 3 Aug 2012	Sat, 3 Aug 2020
ise-3	ise-3.cisco.local	ise-3.cisco.local	Fri, 3 Aug 2012	Sat, 3 Aug 2020
ise-4	ise-4.cisco.local	ise-4.cisco.local	Fri, 3 Aug 2012	Sat, 3 Aug 2020

Step 3: Click **Browse**, and then locate the root CA certificate saved in Procedure 5, “Download CA root certificate.”

Step 4: Select **Trust for client authentication**, and then click **Submit**.

The screenshot shows the 'Import' form in the Cisco ISE interface. The left sidebar lists 'Certificate Operations' with 'Local Certificates' selected. The main area is titled 'Import a new Certificate into the Certificate Store'. It contains a 'Certificate File' field with a 'Browse...' button, a 'Friendly Name' field, and a section for 'All Trust Certificates'. The 'Trust for client authentication' checkbox is checked. Below it is an unchecked checkbox for 'Enable Validation of Certificate Extensions (accept only valid certificate)'. A 'Description' field is at the bottom, followed by 'Submit' and 'Cancel' buttons.

Procedure 8 Install local certificate in Cisco ISE

Step 1: In the Cisco ISE interface, mouse over **Administration**, and then, from the System section of the menu, choose **Certificates**.

Step 2: Click **Local Certificates**.

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

The screenshot shows the 'Local Certificates' page in the Cisco ISE interface. The left sidebar shows 'Local Certificates' selected under 'Certificate Operations'. The main area has a toolbar with 'Edit', 'Add', 'Export', and 'Delete' buttons. The 'Add' button is highlighted, and a dropdown menu is open showing options: 'Import Local Server Certificate', 'Generate Self-Signed Certificate', 'Generate Certificate Signing Request', and 'Bind CA Certificate'. Below the menu is a table with columns: 'Protocol', 'Issued To', 'Issued By', and 'Valid From'. The table contains one entry with 'HTTPS,EAP' in the Protocol column, 'ise-1.cisco.local' in the Issued To column, 'ise-1.cisco.local' in the Issued By column, and 'Fri, 3 Aug 2012' in the Valid From column.

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 **Management Interface**. When you receive a message that selecting the Management Interface check box will require the Cisco ISE appliance to restart, click **OK**, and then click **Submit**.

Step 6: When you receive a message that the Cisco ISE appliance will restart, click **OK**.

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: In the Cisco ISE interface, mouse over **Administration**, and then, in the System section, choose **Certificates**.

Step 2: Click **Local Certificates**.

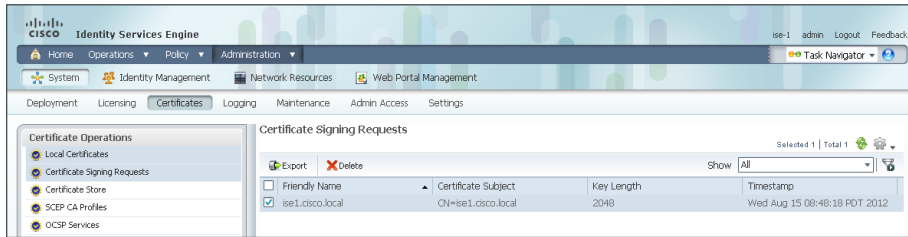
Step 3: Select the box next to the self-signed certificate. This is the certificate issued by the Cisco ISE appliance and not the certificate issued by the CA that was just imported.

Friendly Name	Protocol	Issued To	Issued By
<input checked="" type="checkbox"/> Default self-signed server certificate		ise1.cisco.local	ise1.cisco.local
<input type="checkbox"/> ise-1.cisco.local#CA	HTTPS,EAP	ise-1.cisco.local	CA

Step 4: Click **Delete**, and then click **OK**.

Step 5: Click **Certificate Signing Requests**.

Step 6: Select the box next to the certificate signing request that was created in Procedure 4, “Request a certificate for ISE from the CA.”



Step 7: Click **Delete**, and then click **OK**.

PROCESS

Enabling 802.1X Authentication

1. Create user authentication policies
2. Create machine authentication policies
3. Enable certificates
4. Enable EAP-TLS

You will configure Cisco ISE policies to support 802.1X authentication using digital certificates for both wired and wireless users.

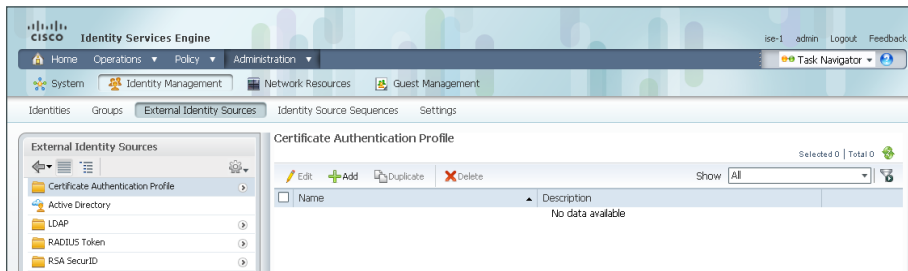
Procedure 1

Create user authentication policies

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

Step 1: In Cisco ISE, mouse over **Administration**, and then, in the Identity Management section, choose **External Identity Sources**.

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



Step 3: Give the profile a meaningful name, and in the **Principal Username X509 Attribute** list, choose **Subject Alternative Name**.

Step 4: Select **Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory**, and then, in the **LDAP/AD Instance Name** list, choose previously defined AD server **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 be able to use it for policy decisions.

Step 5: Click **Submit**.

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 6: Click **Identity Source Sequences**, and then click **Add**.

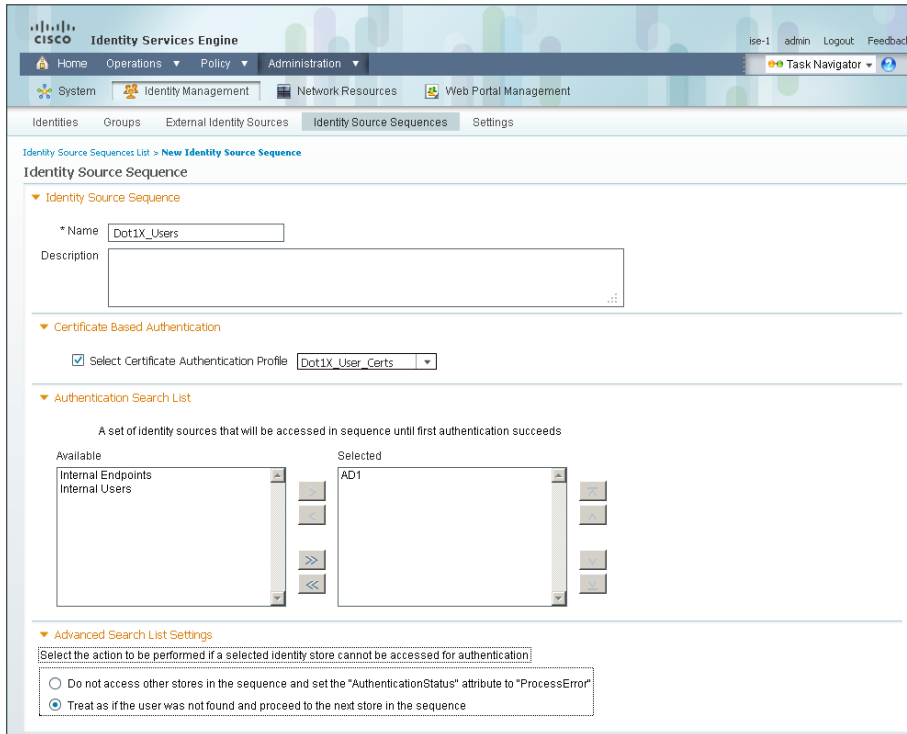
Name	Description	Identity Stores
Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal	Internal Users
Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal	Internal Users

Step 7: Give the sequence a meaningful name.

Step 8: In the Certificate Based Authentication section, select **Select Certificate Authentication Profile**, and then choose the profile created in Step 2 through Step 5.

Step 9: In the Authentication Search List section, in the **Available** list, double-click the AD server. It moves into the **Selected** list.

Step 10: 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 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	AD1
Internal Users	

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 will create an authentication profile for machine authentication using certificates.

Step 1: In Cisco ISE, mouse over **Administration**, and then, in the Identity Management section, choose **External Identity Sources**.

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

Step 3: Give the profile a meaningful name, and in the **Principal Username X509 Attribute** list, choose **Common Name**.

Step 4: Click **Submit**.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. The left sidebar shows 'External Identity Sources' with options like 'Certificate Authentication Profile', 'Active Directory', 'LDAP', 'RADIUS Token', and 'RSA SecurID'. The main form is titled 'Certificate Authentication Profile' and contains fields for 'Name' (Dot1X_Machine_Certs), 'Description', 'Principal Username X509 Attribute' (Common Name), and a checkbox for 'Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory'. The 'Submit' button is at the bottom.

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 5: Click **Identity Source Sequences**, and then click **Add**.

Step 6: Give the sequence a meaningful name.

Step 7: In the Certificate Based Authentication section, select **Select Certificate Authentication Profile**, and then choose the profile created in Step 2 through Step 4.

Step 8: In the Authentication Search List section, in the **Available** list, double-click the AD server. It moves into the **Selected** list.

Step 9: 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**.

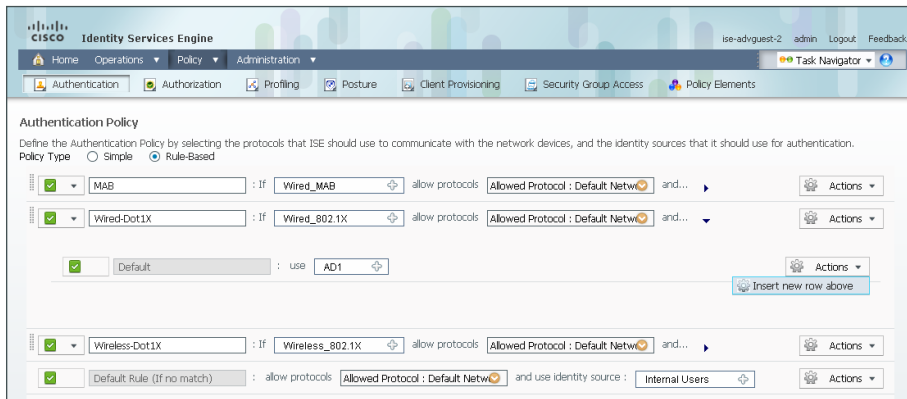
The screenshot shows the Cisco Identity Services Engine (ISE) interface for creating a new identity source sequence. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. The left sidebar shows 'Identity Source Sequences' with a 'New Identity Source Sequence' link. The main form is titled 'Identity Source Sequence' and contains sections for 'Identity Source Sequence' (Name: Dor1X_Machines), 'Certificate Based Authentication' (Select Certificate Authentication Profile: Dot1X_Machine_Certs), 'Authentication Search List' (Available: Internal Endpoints, Internal Users; Selected: AD1), and 'Advanced Search List Settings' (Treat as if the user was not found and proceed to the next store in the sequence).

Procedure 3 Enable 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 both wired and wireless users.

Step 1: Mouse over **Policy**, and then choose **Authentication**.

Step 2: For the **Wired-Dot1X** rule, to the right of and..., click the black triangle. This brings up the identity store used for this rule. Next to the Default rule, in the **Actions** list, choose **Insert new rule above**.



Step 3: Give the rule a name, and then next to the Enter Condition box, click the box symbol. The Expression Builder opens.

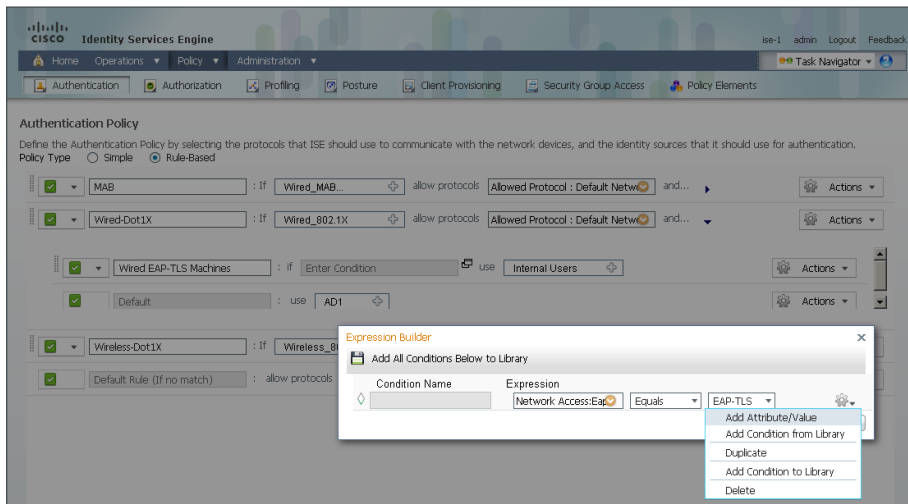
Step 4: Click **Create New Condition (Advance Option)**.

Step 5: In the **Expression** list, next to **Select Attribute**, click the arrow.

Step 6: Next to Network Access, click the arrow, and then choose **EapAuthentication**.

Step 7: In the second list, choose **Equals**, and in the last list, choose **EAP-TLS**.

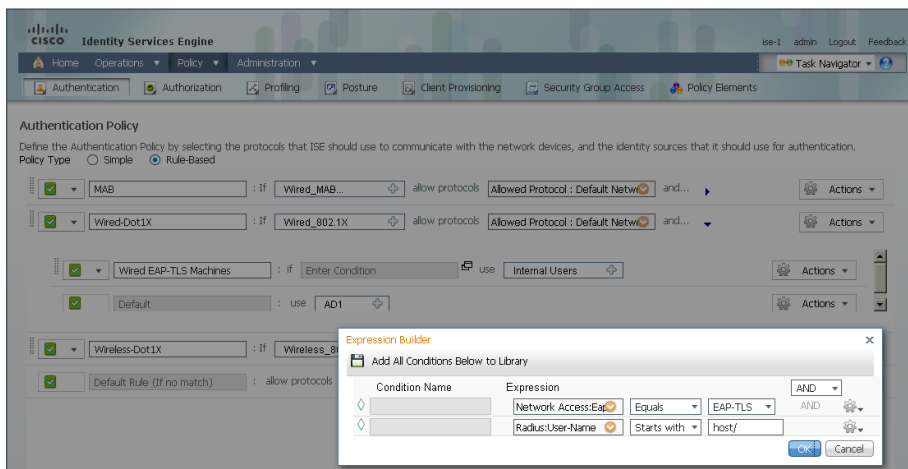
Step 8: Click the gear icon at the end of the condition, and then choose **Add Attribute/Value**.



Step 9: In the **Expression** list, next to Select Attribute, click the arrow.

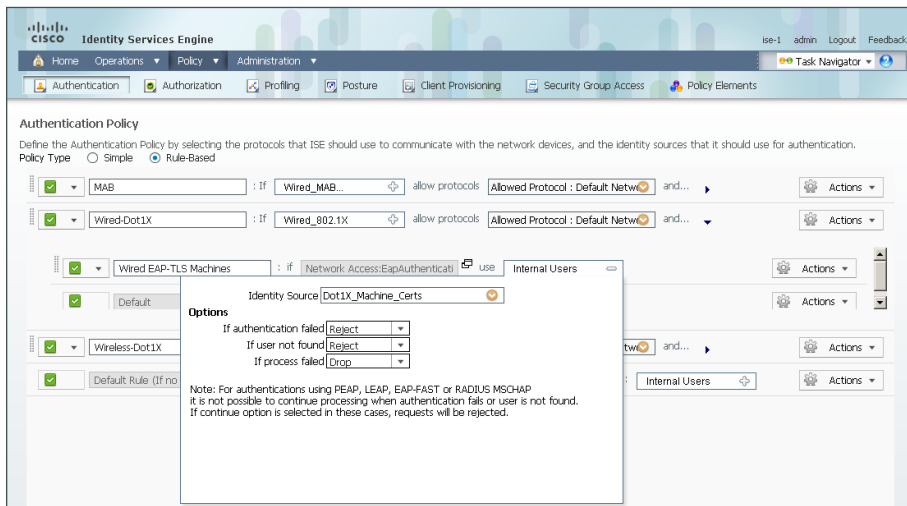
Step 10: Next to Radius, click the arrow, and then select **User-name**.

Step 11: In the second list, choose **Starts with**, and in the last box, type **host/** and then click **OK**.



Step 12: Next to Internal Users, click the + symbol.

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,” use the default options for this identity source, and then click anywhere in the window to continue.



You now create a rule for wired user authentication.

Step 14: Next to the Default rule, in the **Actions** list, choose **Insert new rule above**.

Step 15: Give the rule a name, and then next to the Enter Condition box, click the box symbol. The Expression Builder opens.

Step 16: Click **Create New Condition (Advance Option)**.

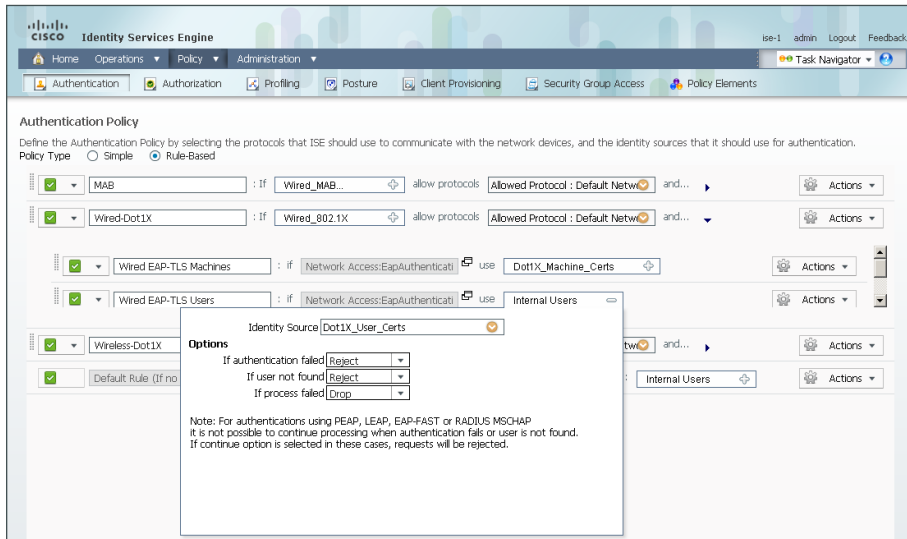
Step 17: In the **Expression** list, next to Select Attribute, click the arrow.

Step 18: Next to Network Access, click the arrow, and then choose **EapAuthentication**.

Step 19: In the second list, choose **Equals**, and in the last list, choose **EAP-TLS**, and then click **OK**.

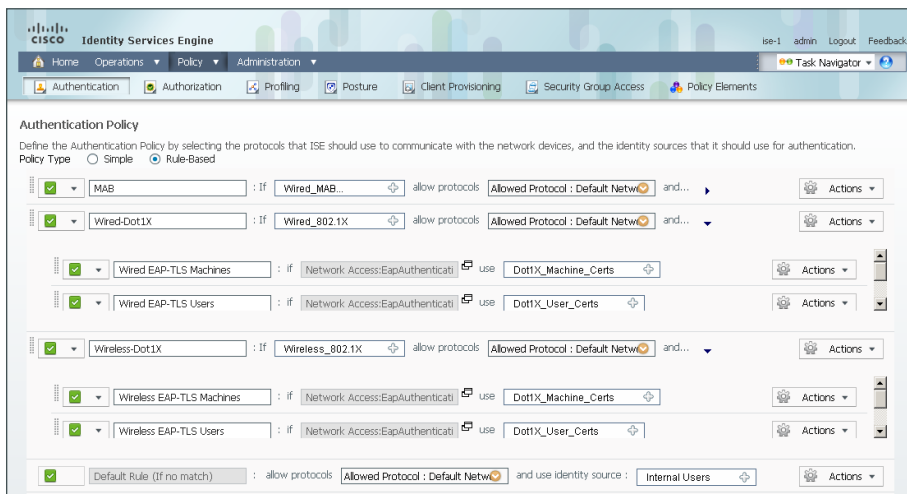
Step 20: Next to Internal Users, click the **+** symbol.

Step 21: In the **Identity Source** list, choose the identity source sequence for machine authentication that you created in Procedure 1, “Create user authentication policies,” use the default options for this identity source, and then click anywhere in the window to continue.



Step 22: Click **Save**.

Step 23: Repeat Step 2 through Step 22 for the Wireless-Dot1X rule.



Procedure 4 Enable EAP-TLS

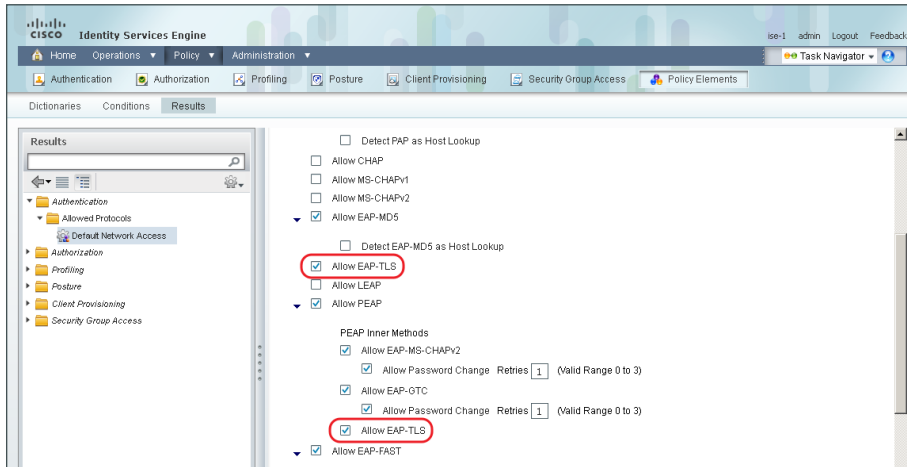
In a previous section, you disabled EAP-TLS. Now that you are using digital certificates, you need to re-enable it.

Step 1: On the menu bar, mouse over **Policy**, and then in the Policy Elements section, choose **Results**.

Step 2: In the left pane, double-click **Authentication**. This expands the options.

Step 3: Double-click **Allowed Protocols**, and then choose **Default Network Access**.

Step 4: Select the global **Allow EAP-TLS** check box and, under the PEAP settings, select the **Allow EAP-TLS** check box, and then click **Save**.



PROCESS

Configuring Group Policy Objects

1. Create template for workstations
2. Create template for user auto-enrollment
3. Configure GPOs for wired endpoints
4. Configure GPOs for wireless endpoints

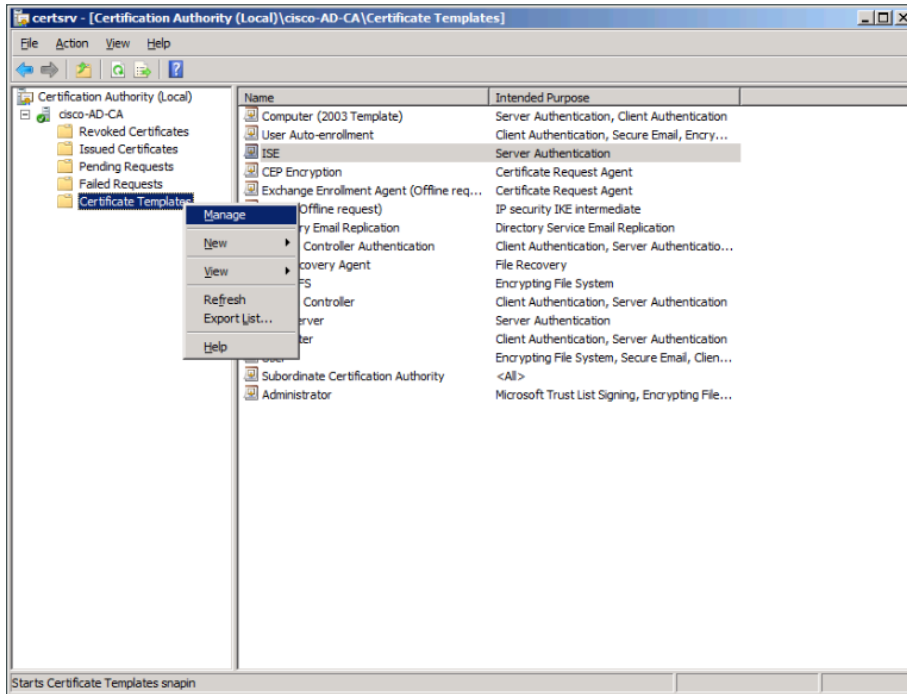
In this deployment, you will be using group policy objects (GPOs) to distribute certificates and to configure the native 802.1X supplicant for Windows XP and later endpoints that are members of the domain. Machine certificates are distributed when the machine joins the domain, and user certificates are 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 will apply to all users, but you could create a new policy object and apply it to a subset of users if you prefer.

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

Step 2: Expand the CA server, right-click **Certificate Templates**, and then choose **Manage**. The Certificate Templates Console opens.



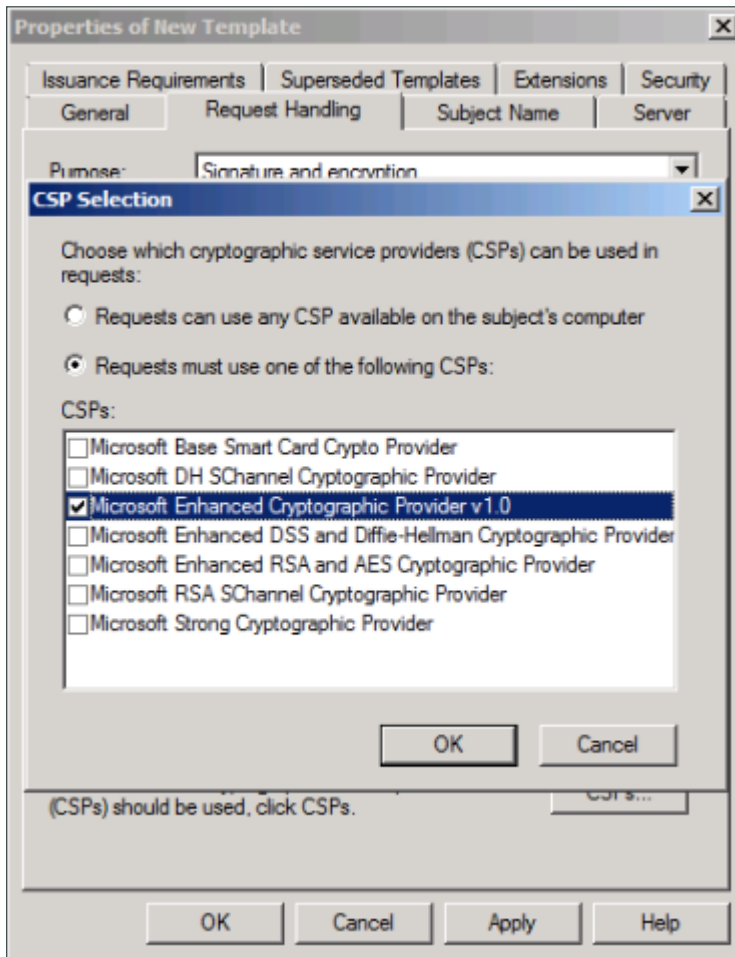
Step 3: Right-click the Computer template, and then choose **Duplicate Template**.

Step 4: For compatibility, make sure that **Windows 2003 Server Enterprise** is selected.

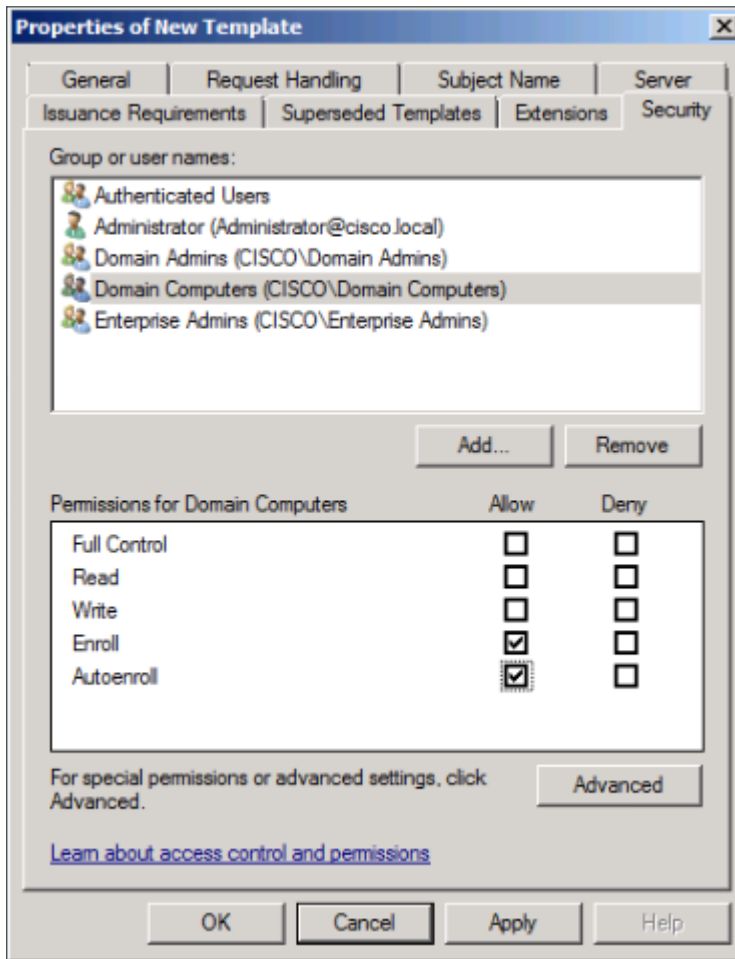
Step 5: In the Properties of New Template window, click the **General** tab, and then give the template a name.

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

Step 7: Select **Requests** must use one of the following CSPs and **Microsoft Enhanced Cryptographic Provider v1.0**, and then click **OK**.



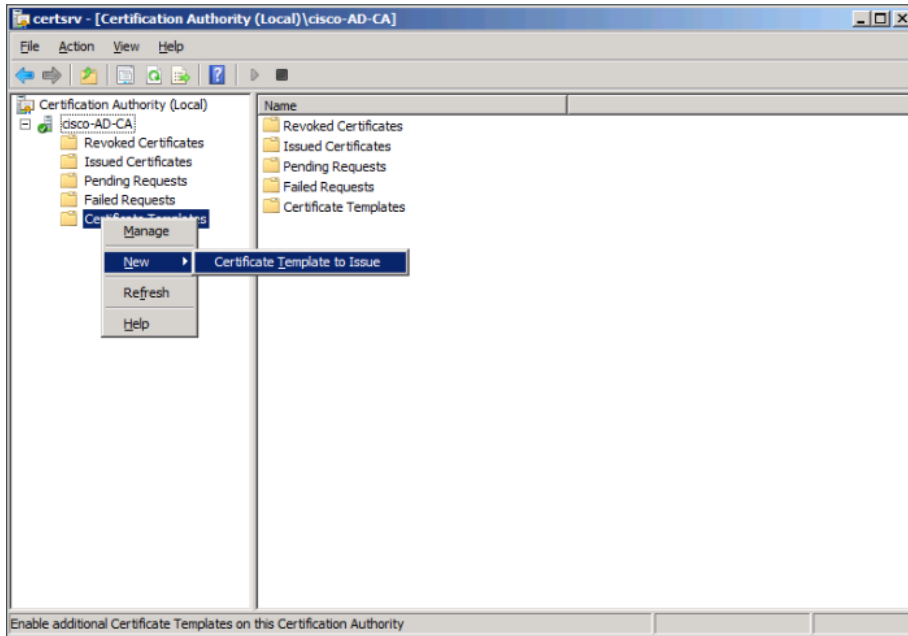
Step 8: On the Security tab, click **Domain Computers**, and then for both **Enroll** and **Autoenroll**, make sure **Allow** is selected.



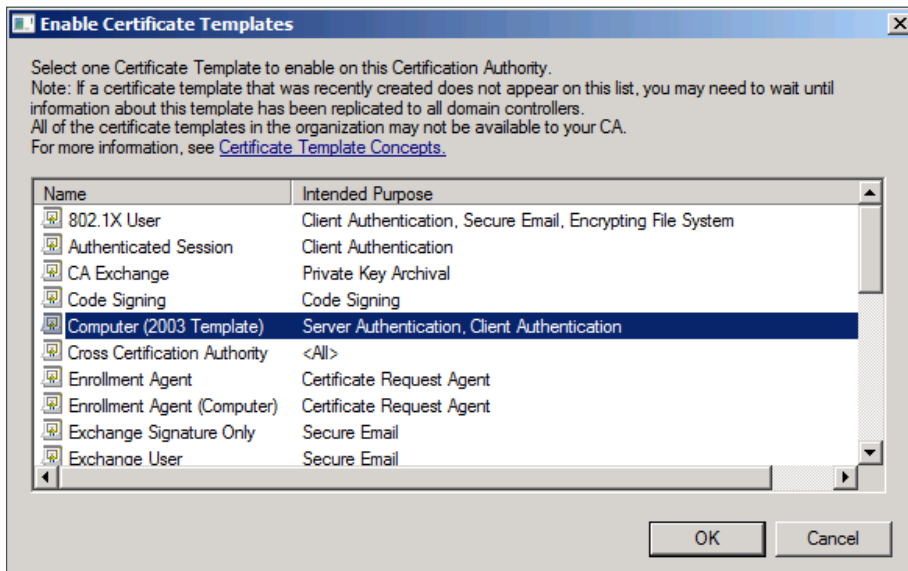
Step 9: Use the defaults for the remaining tabs, and then click **OK**.

Step 10: Close the Certificate Templates Console.

Step 11: In the Certificate Authority console, right-click **Certificate Templates**, and then choose **New > Certificate Template to Issue**.



Step 12: Choose the previously defined template, and then click **OK**.



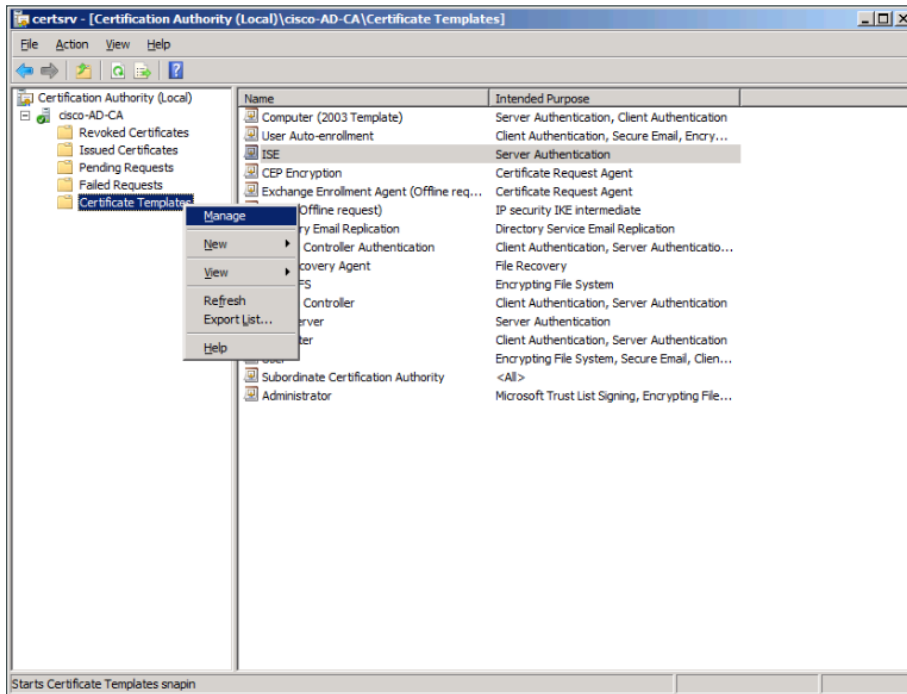
When machines join the domain or when the GPO policy is refreshed (the default period is 90 minutes), the machine receives a machine certificate to allow for 802.1X machine authentication.

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: Expand the CA server, right-click **Certificate Templates**, and then choose **Manage**. The Certificate Templates Console opens.



Step 3: Right-click the User template, and then choose **Duplicate Template**.

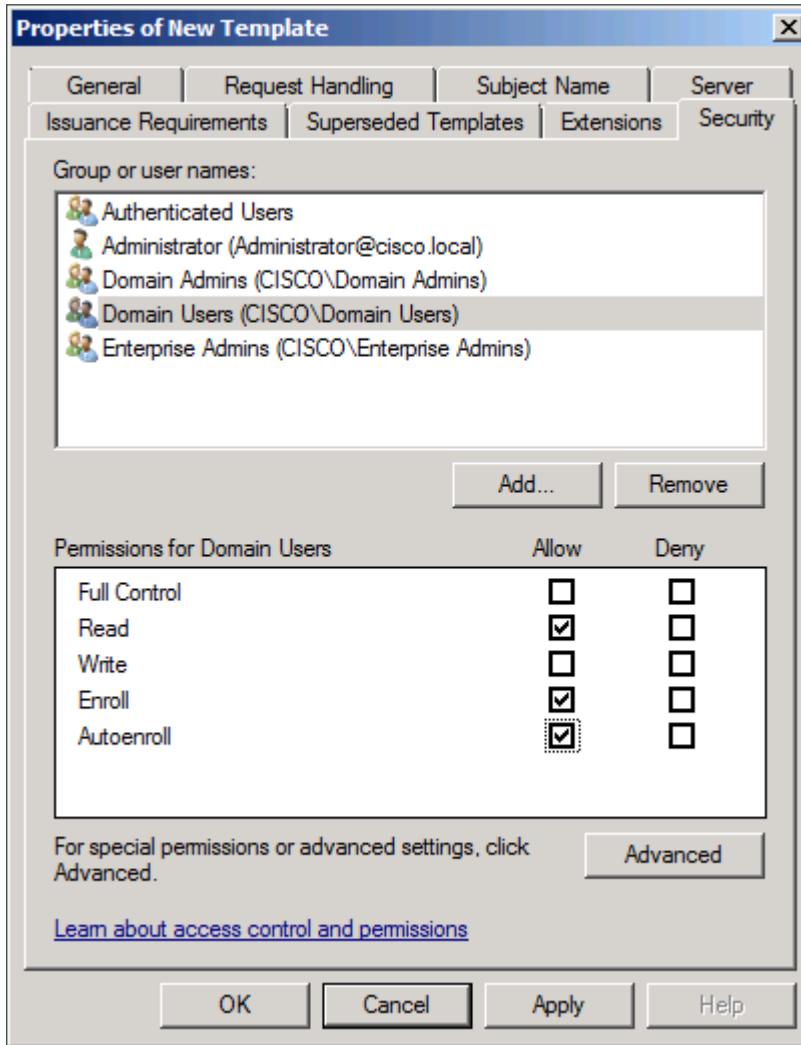
Step 4: For compatibility with Windows XP, make sure that **Windows 2003 Server Enterprise** is selected.

Step 5: In the Properties of New Template window, click the **General** tab, and then give the template a name.

Step 6: On the Request Handling tab, select **Allow private key to be exported**, make sure **Enroll subject without requiring any user input** is selected, and then click **CSPs**.

Step 7: Select **Requests must use one of the following CSPs** and **Microsoft Enhanced Cryptographic Provider v1.0**, and then click **OK**.

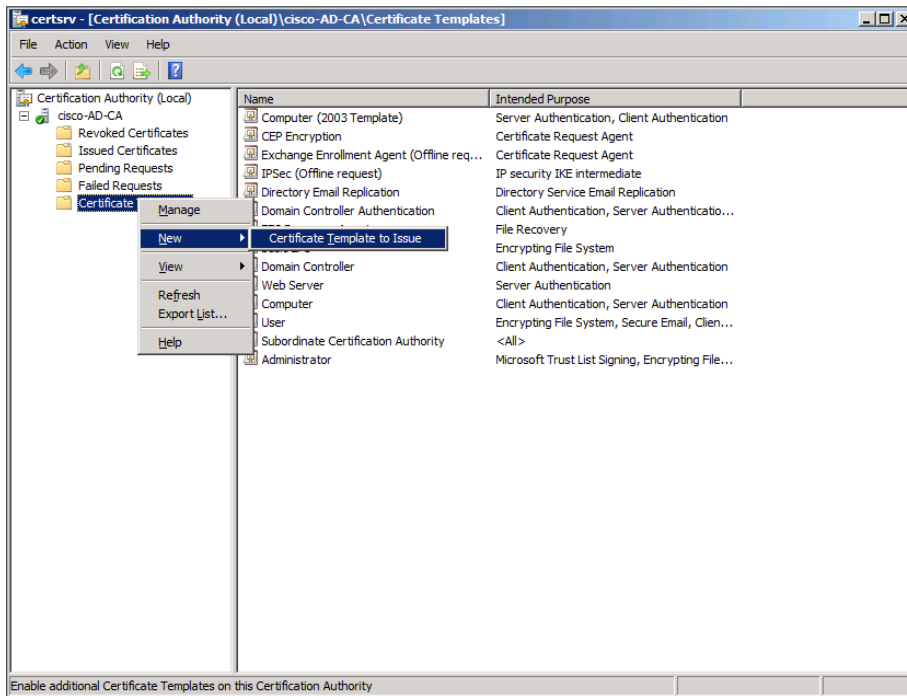
Step 8: On the Security tab, click **Domain Users**, and then for **Read**, **Enroll**, and **Autoenroll**, make sure **Allow** is selected.



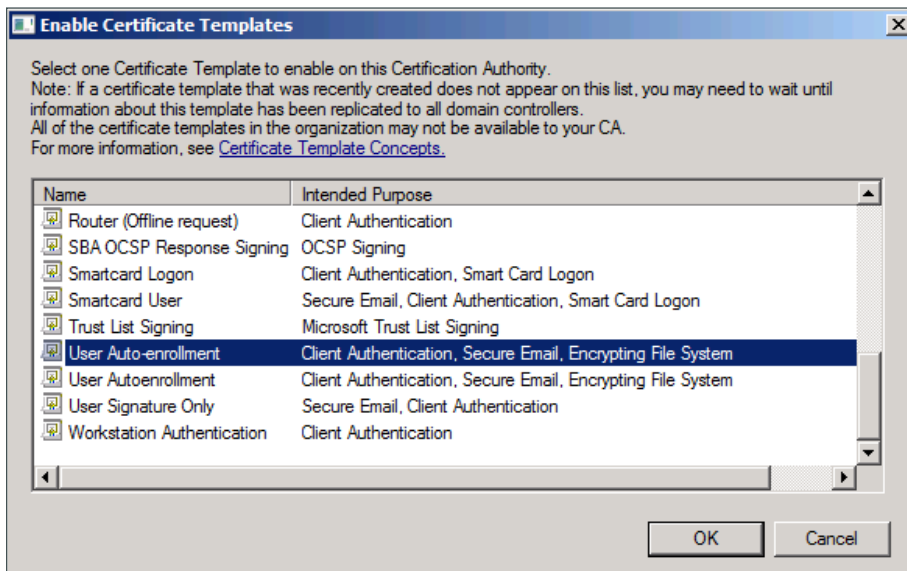
Step 9: Use the defaults for the remaining tabs, and then click **OK**.

Step 10: Close the Certificate Templates Console.

Step 11: In the Certificate Authority console, right-click **Certificate Templates**, and then choose **New > Certificate Template to Issue**.



Step 12: Choose the previously defined template, and then click **OK**.



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 3 Configure GPOs for wired endpoints

This deployment uses GPOs to configure the 802.1X supplicant on wired endpoints running Windows XP SP3 and higher.

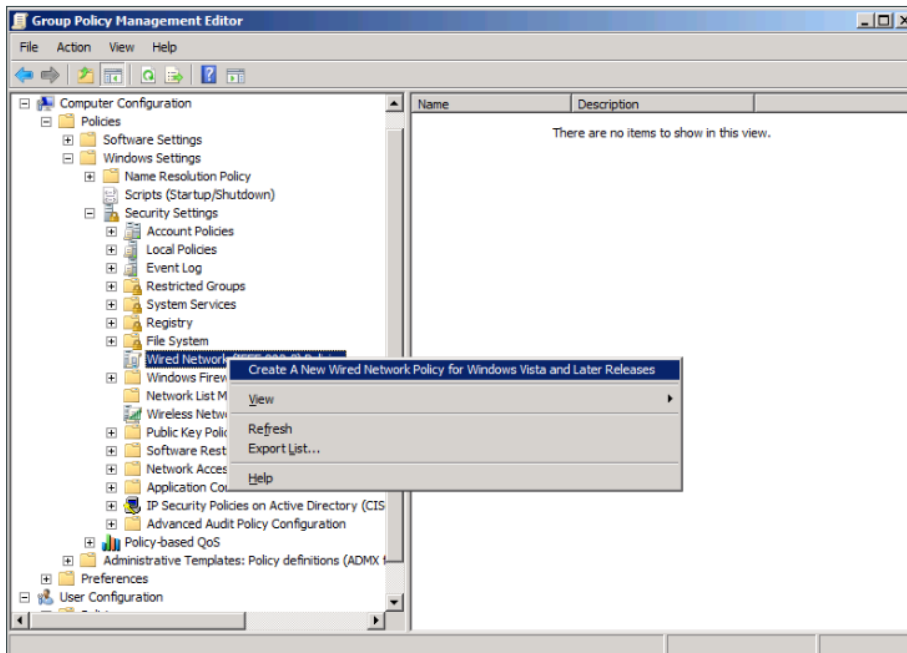
Step 1: On the CA console, navigate to **Start > Administrative Tools > Group Policy Management**.

Step 2: Expand **Forest > Domain > local domain > Group Policy Objects**.

Step 3: Right-click **Default Domain Policy** and click **Edit**. The Group Policy Management Editor opens.

Step 4: In the Group Policy Management Editor, navigate to **Computer Configuration > Policies > Windows Settings > Security Settings**.

Step 5: Right-click **Wired Network (IEEE 802.3e) Policies**, and then choose **Create a New Wired Network Policy for Windows Vista and Later Releases**.



Step 6: On the General tab, give the policy a name and description, and then make sure **Use Windows Wired Auto Config service for clients** is selected.

Step 7: On the Security tab, make sure **Enable of IEEE 802.1X authentication for network access** is selected.

Step 8: In the **Network Authentication Method** list, choose **Microsoft: Smart Card or other certificate**.

Step 9: In the **Authentication Mode** list, choose **User or computer authentication**.

Step 10: Click **Properties**.

Step 11: Make sure **Use a certificate on this computer** is selected, and then make sure **Use simple certificate selection** and **Validate server certificate** are selected.

Step 12: In the **Trusted Root Certification Authorities** list, next to the root certificate for the CA, select the check box.

Step 13: Click **OK**. The certificate properties window closes.

Step 14: In the policy properties window, click **Apply**, and then click **OK** again.

Procedure 4 Configure GPOs for wireless endpoints

This deployment uses GPOs to configure the 802.1X supplicant for wireless endpoints running Windows XP SP3 and higher.

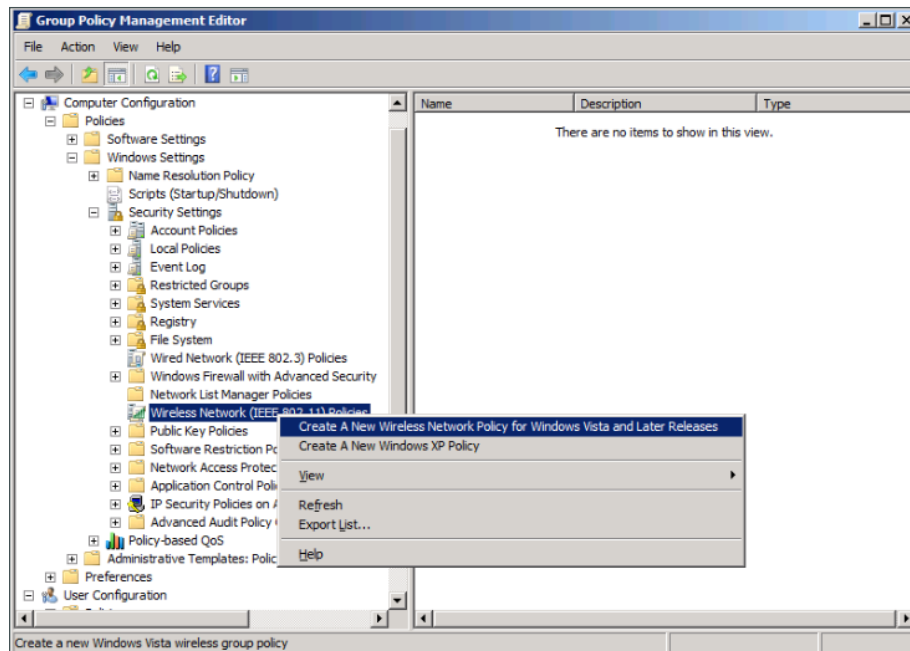
Step 1: On the CA console, navigate to **Start > Administrative Tools > Group Policy Management**.

Step 2: Expand **Forest > Domain > local domain > Group Policy Objects**.

Step 3: Right-click **Default Domain Policy**. The Group Policy Management Editor opens.

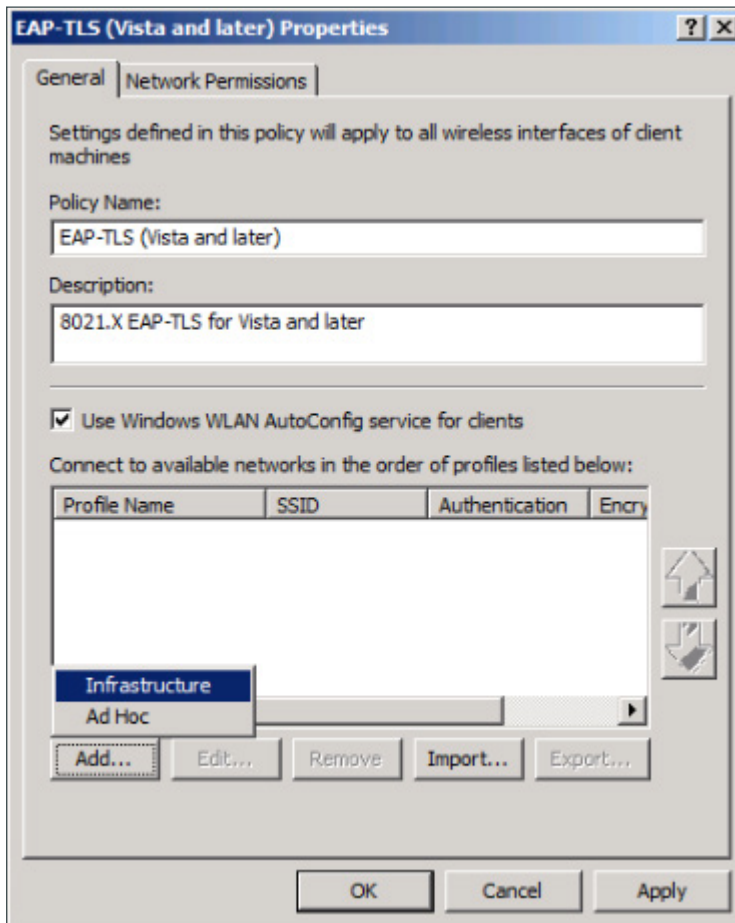
Step 4: In the Group Policy Management Editor, navigate to **Computer Configuration > Policies > Windows Settings > Security Settings**.

Step 5: Right-click **Wireless Network (IEEE 802.11) Policies**, and then choose **Create a New Wireless Network Policy for Windows Vista and Later Releases**.



Step 6: On the General tab, give the policy a name and description, and then make sure **Use Windows WLAN AutoConfig service for clients** is selected.

Step 7: Click **Add**, and then choose **Infrastructure**.

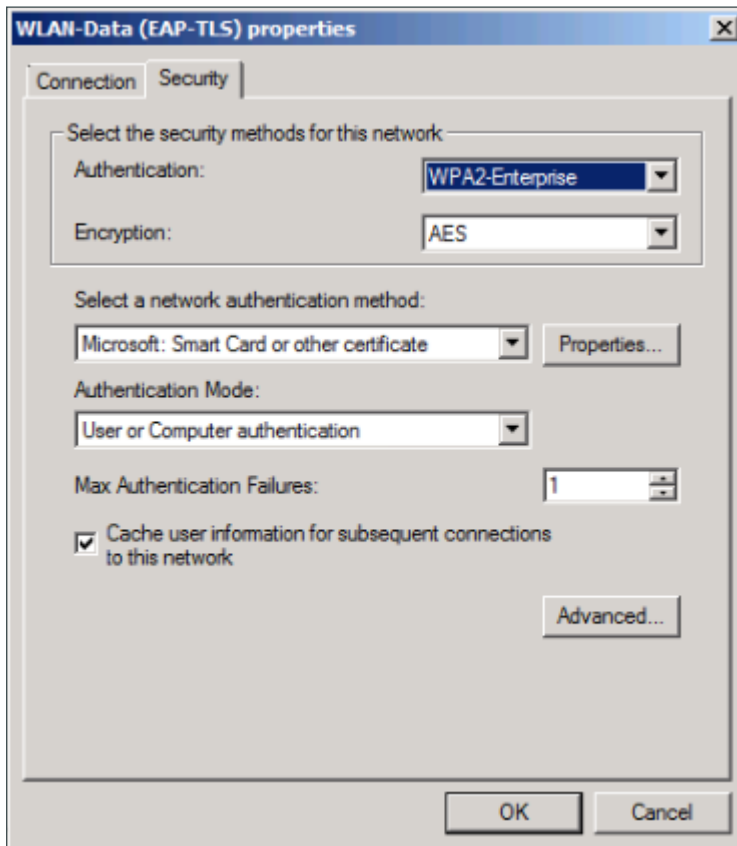


Step 8: Give the profile a name, enter the name of the SSID for the wireless network, and then click **Add**.

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

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: Make sure **Use a certificate on this computer** is selected, and then make sure **Use simple certificate selection** and **Validate server certificate** are selected.

Step 14: In the **Trusted Root Certification Authorities** list, next to the root certificate for the CA, select the check box.

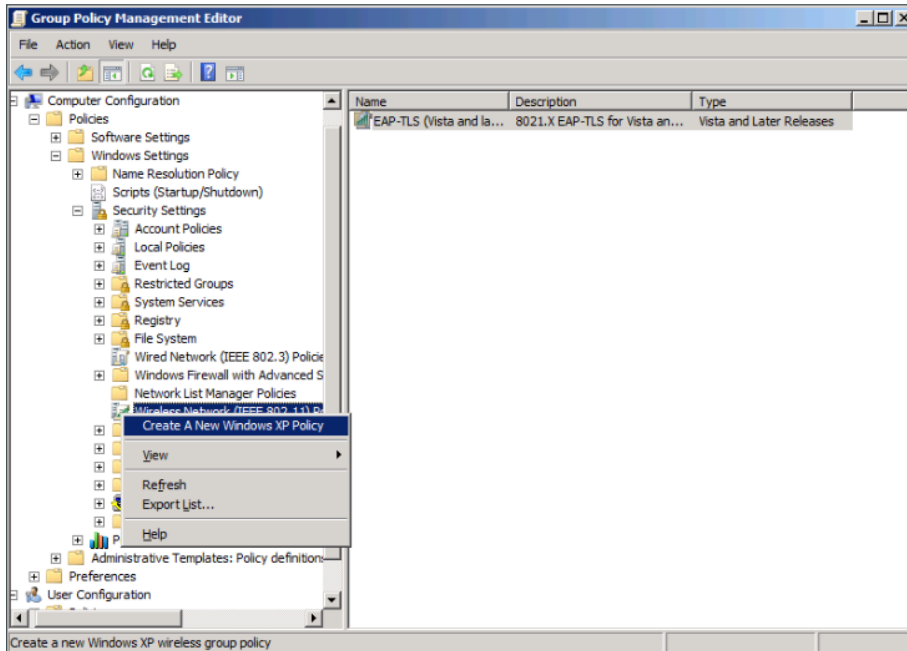
Step 15: Click **OK**. The certificate properties window closes.

Step 16: Click **OK**. The profile properties window closes.

Step 17: In the policy properties window, click **Apply**, and then click **OK**.

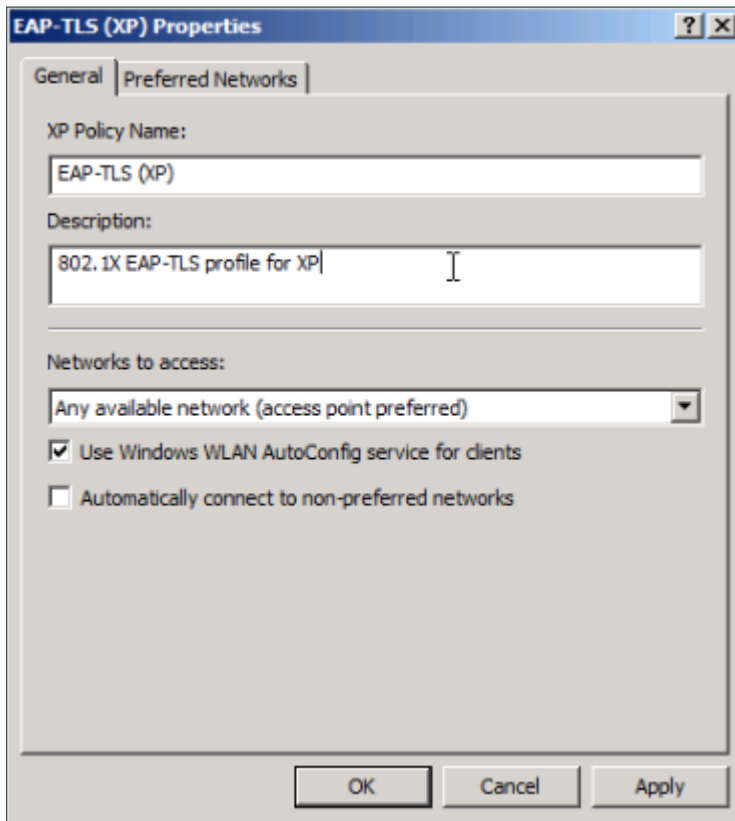
Next, you create a policy for Windows XP clients.

Step 18: Right-click **Wireless Network (IEEE 802.11) Policies**, and then choose **Create a New Windows XP Policy**.



Step 19: On the General tab, give the policy a name and description, and then make sure **Use Windows WLAN AutoConfig service for clients** is selected.

Step 20: In the **Networks to access** list, choose **Any available network (access point preferred)**.



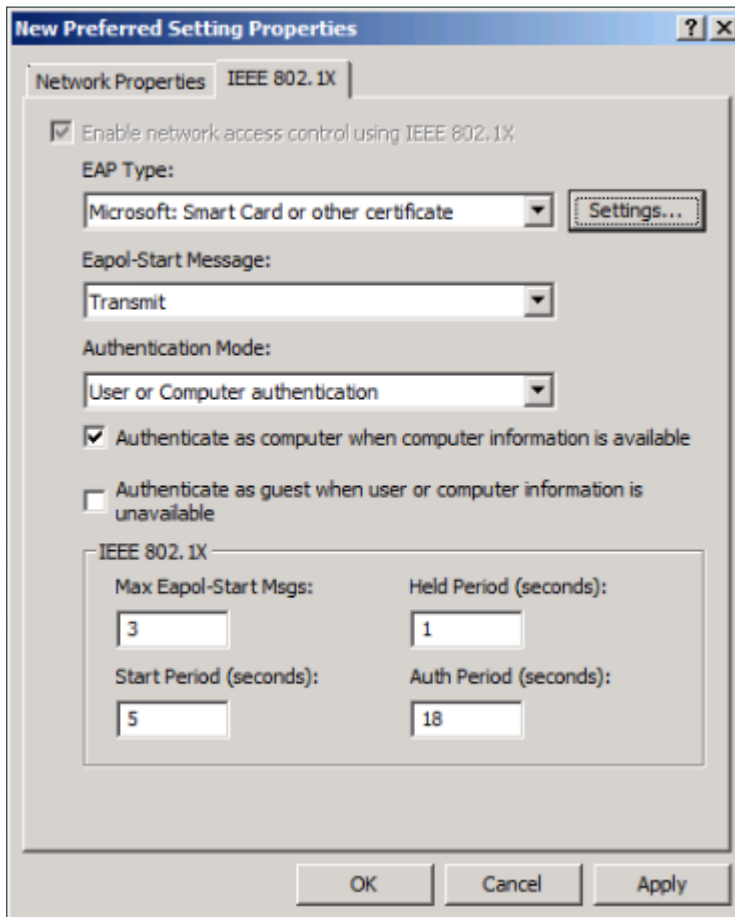
Step 21: On the **Preferred Networks** tab, click **Add**, and then select **Infrastructure**.

Step 22: Enter the SSID for the network and give a description.

Step 23: In the **Authentication** list, choose **WPA2**, and then in the **Encryption** list, choose **AES**.

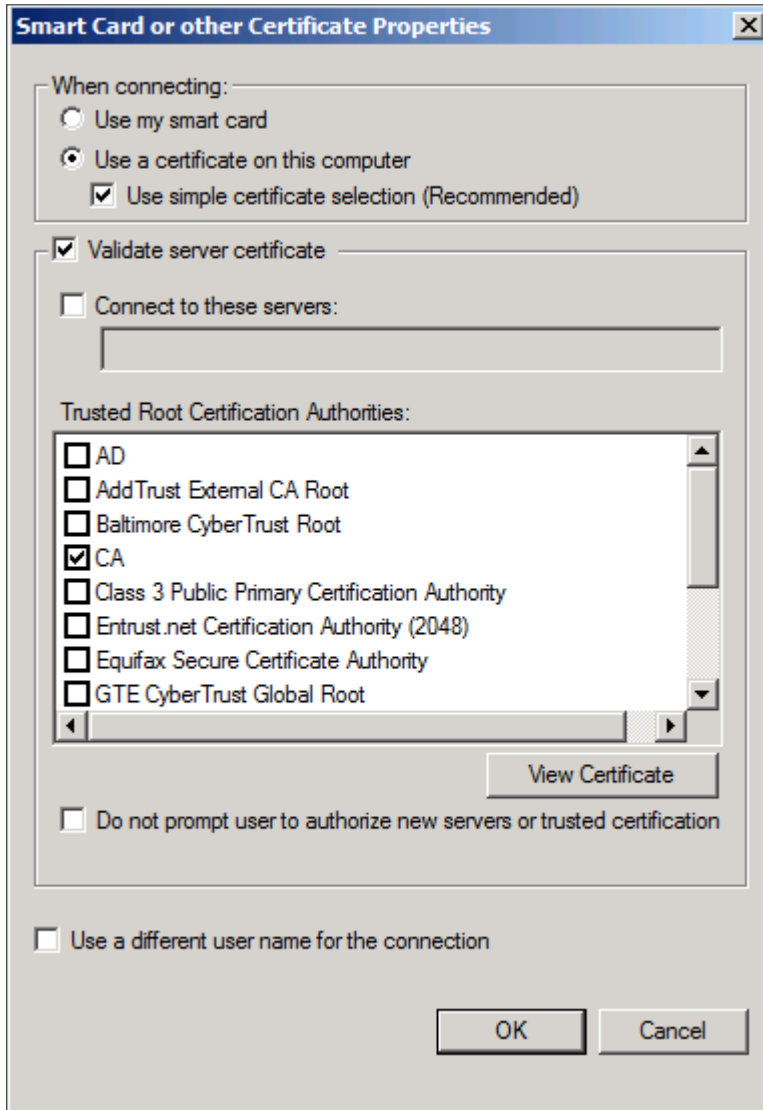
Step 24: On the **IEEE 802.1X** tab, in the **EAP type** list, choose **Microsoft: Smart Card or other certificate**.

Step 25: In the **Authentication Mode** list, choose **User or Computer authentication**.



Step 26: Click **Settings**, make sure **Use a certificate on this computer** is selected, and then make sure **Use simple certificate selection** and **Validate server certificate** are selected.

Step 27: In the **Trusted Root Certification Authorities** list, next to the root certificate for the CA, select the check box, and then click **OK**.



Step 28: In the profile properties window, click **Apply**, and then click **OK**.

Step 29: In the policy properties window, click **Apply**, and then click **OK**.

At this point, all endpoints running Windows XP SP3 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.

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 3.1 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 3.1 as your 802.1X supplicant on Windows endpoints, you need to download the latest version from Cisco.com along with the Profile Editor. The client is distributed as an ISO image and will need to either be burned to a disk or mounted as a disk image by using a utility that provides this function. You need to be logged in as an administrator to install AnyConnect Secure Mobility Client.

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=3.1.02040>



Tech Tip

To deploy the Cisco AnyConnect Secure Mobility Client to multiple workstations with the same policy, you can create a customized installation package. You need to copy all the files from the installation disk to a folder on the hard drive, for example, C:\AnyConnect. Then, follow the procedure above to edit the profile. Copy the file (C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\configuration.xml) to C:\AnyConnect\Profiles\nam\configuration.xml.

Copy the contents of C:\AnyConnect to some form of removable media, for instance, CD, DVD, USB drive, etc. You can then take this new installer package and run the installation on a workstation. The custom configuration file is loaded and ready for use.

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**, and then clear all of the other check boxes.



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

Step 4: Click **Accept**. This accepts the license agreement.

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

Procedure 2 Install Profile Editor

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

The installation requires Java Runtime Environment 1.6 or higher. If you don't have it installed, you are prompted to install it.

Step 2: If you are prompted to install Java Runtime Environment 1.6 or higher, click **Next**. This installs it.

Step 3: Click **Next**. The installation of Profile Editor continues.

Step 4: Click **Typical**, and then click **Install**.

Step 5: Click **Finish**. The installation completes.

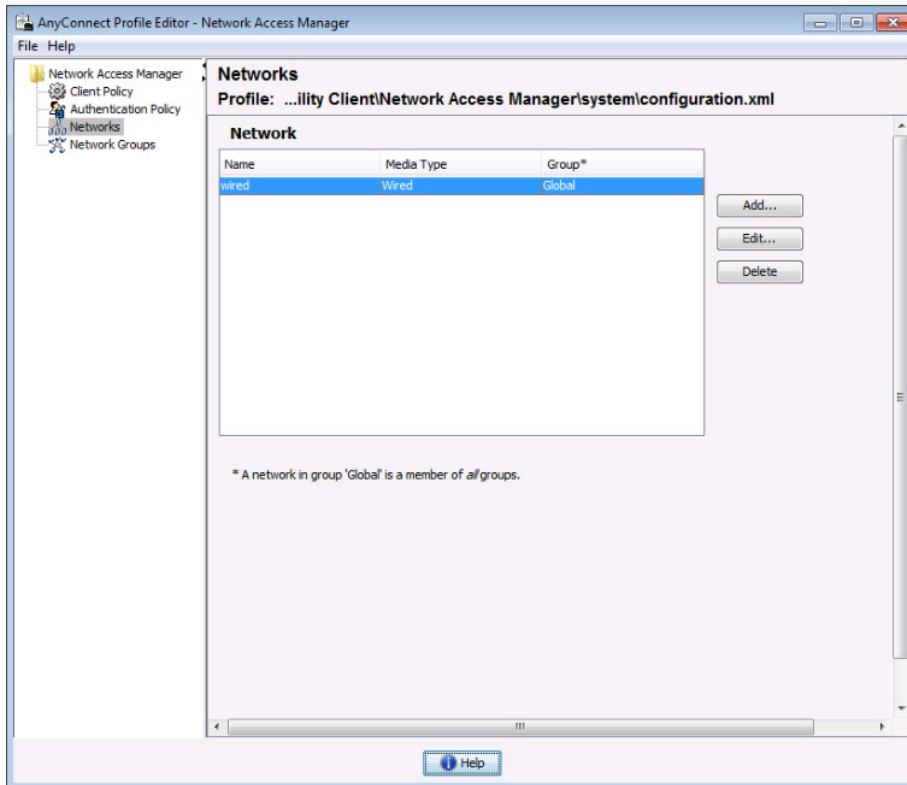
Procedure 3 Create wired profile

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 then select **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\configuration.xml**.

Step 3: Click **Networks**.

Step 4: Select the wired profile, and then click **Edit**.



Step 5: Enter a name for the profile, and then click **Next**.

Step 6: Select **Authenticating Network**, and then click **Next**.

Step 7: Select **Machine and User Connection**, and then click **Next**.

Step 8: For the machine authentication method, select **EAP-TLS**, and then click **Next**.

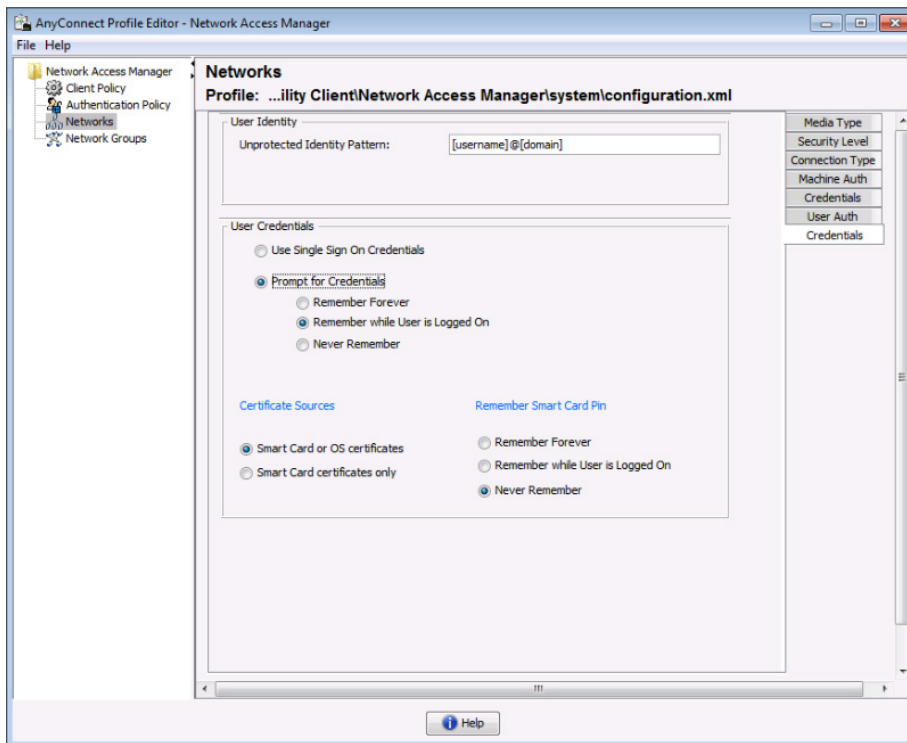
Step 9: For machine identity, enter an unprotected identity pattern. In this deployment, use **host.[domain]**, and then click **Next**.

Step 10: For the user authentication method, select **EAP-TLS**, and then click **Next**.

Step 11: For user identity, enter an unprotected identity pattern. In this deployment, use **[username]@[domain]**.

Step 12: In the User Credentials section, select **Prompt for Credentials**, and then select **Remember while User is Logged On**.

Step 13: Under **Certificate Sources**, select **Smart Card or OS certificates**, and then click **Done**.

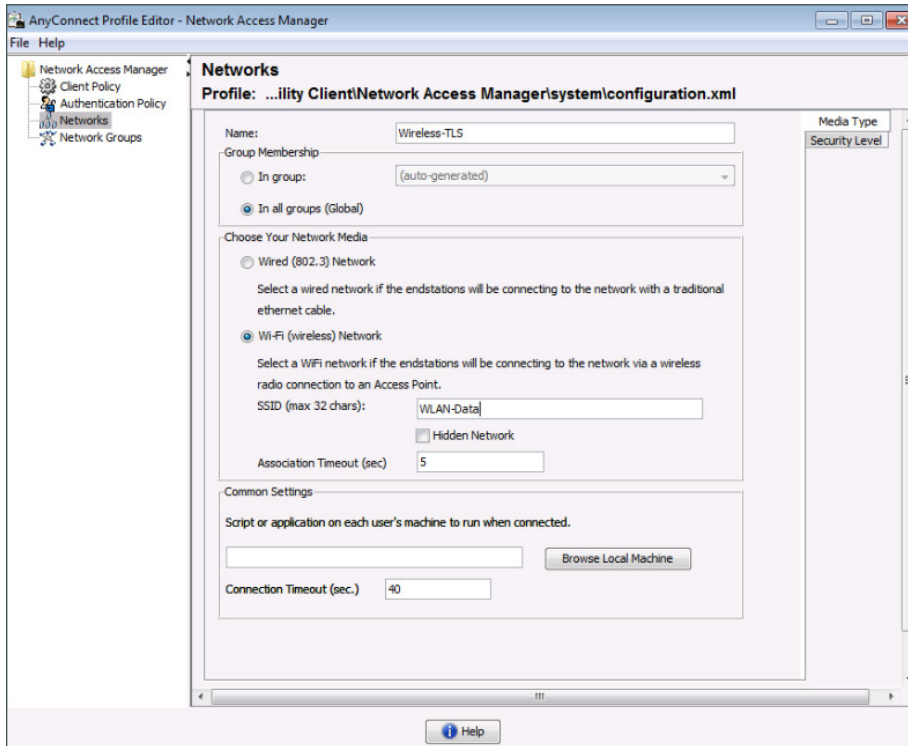


Procedure 4 Create wireless profile

Step 1: In the Profile Editor, click **Add**. This creates a new wireless profile.

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

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



Step 4: Select **Authenticating Network**, for the association mode, choose **WPA2 Enterprise (AES)**, and then click **Next**.

Step 5: Select **Machine and User Connection**, and then click **Next**.

Step 6: For the machine authentication method, select **EAP-TLS**, and then click **Next**.

Step 7: For machine identity, enter an unprotected identity pattern. In this deployment, use **host.[domain]**, and then click **Next**.

Step 8: For the user authentication method, select **EAP-TLS**, and then click **Next**.

Step 9: For user identity, enter an unprotected identity pattern. In this deployment, use **[username]@[domain]**.

Step 10: In the User Credentials section, select **Prompt for Credentials**, and then select **Remember while User is Logged On**.

Step 11: Under **Certificate Sources**, select **Smart Card or OS certificates**, and then click **Done**.

Step 12: From the **File** menu, choose **Save**. This updates the configuration file.

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 MAC Authentication Bypass (MAB).

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 would do this for Mac OS X 10.8.

Procedure 1 Install root certificate on Mac OS X

To install a trusted root certificate on Mac OS X 10.8, you need to manually request the certificate from the CA and install the certificate in the keychain.

Step 1: On the Mac, browse to the CA at <http://ca.cisco.local/certsrv>.

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.

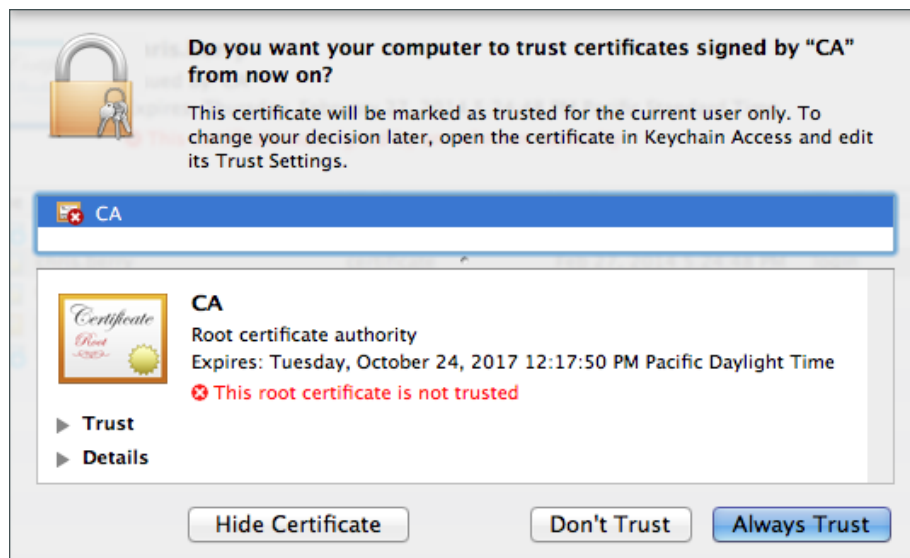
Step 5: Locate the certificate file, and then double-click it. This launches the Keychain Access utility.

Step 6: Click **Always Trust**.



Tech Tip

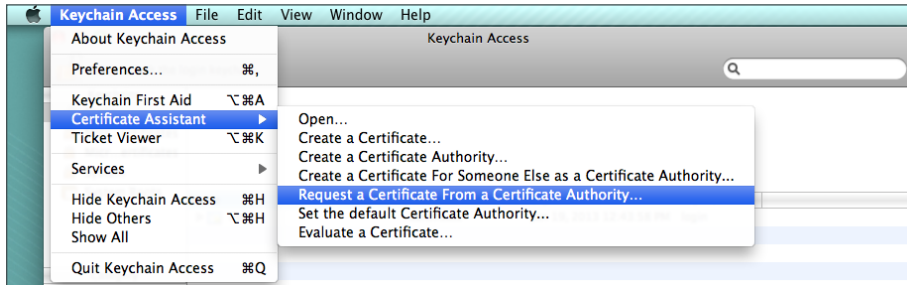
You may be prompted for credentials of a user with permission to change the certificate trust settings.



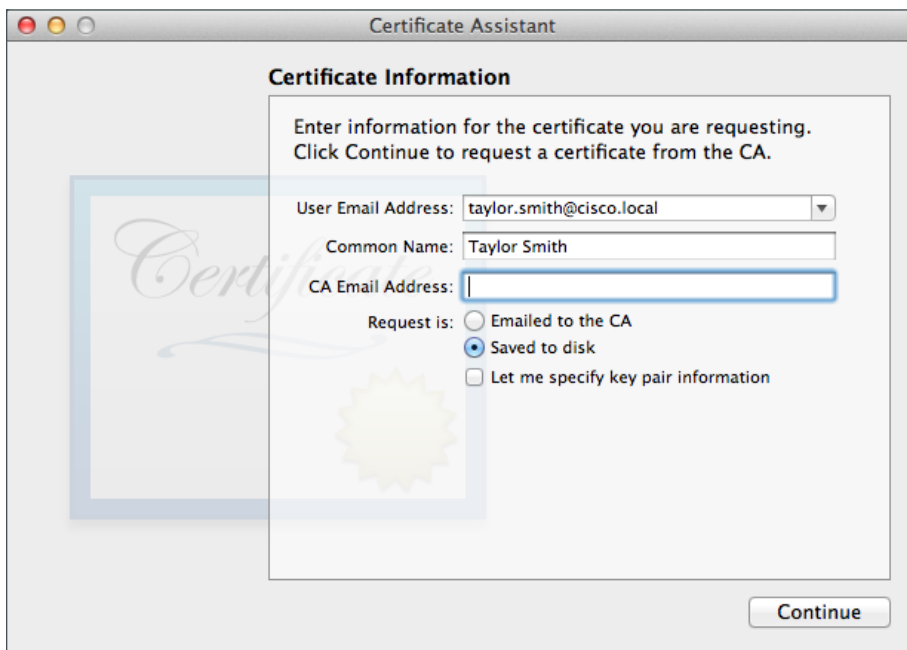
Procedure 2 Request user certificate

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 the 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**.



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

Step 4: Click **Done**.

Step 5: On the Mac, browse to <http://ca.cisco.local/certsrv>.

Step 6: 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 7: Click **Request a certificate**.

Step 8: Click **advanced certificate request**.

Step 9: In a text editor, such as TextEdit, open the certificate request file saved in Step 3.

Step 10: Select all the text, and then copy it to the clipboard.

Step 11: In the browser, on the Submit a Certificate Request or Renewal Request page, in the **Saved Request** box, paste the certificate contents.

Step 12: In the **Certificate Template** list, choose **User**, and then click **Submit**.

Step 13: Select **DER encoded**, and then click **Download certificate**. This saves the certificate.

Step 14: 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 10.8, you will 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 802.1X 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 would be to deploy some form of authorization to control what authenticated endpoints can access on the network. This next phase is called *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 will identify with device profiling. Any other device will have 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 will only have access to the services necessary for authentication.

PROCESS

Enabling Authorization for Cisco IP Phones

1. Enable Cisco IP Phone policy

There is a built-in policy in Cisco ISE for Cisco IP Phones that was disabled in a previous section. You will enable this policy and create an authorization profile for Cisco IP Phones.

Procedure 1

Enable Cisco IP Phone policy

Step 1: Connect to <http://ise-1.cisco.local>.

Step 2: From the Policy menu, select **Authorization**.

Step 3: For the Profiled Cisco IP Phones rule, click **Edit**.

Step 4: Click the grey circle icon at the front of the rule, and then choose **Enabled**.

Step 5: Click **Done**, and then click **Save**.

Enabling Authorization for Wireless Access Points

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

You will create an authorization profile for wireless access points (APs) that is similar to the one for Cisco IP Phones.

Procedure 1 Create an identity group

Step 1: On the menu bar, mouse over **Policy**, and then select **Profiling**.

Step 2: In the **endpoint policies** list, choose **Cisco-Access-Point**.

Step 3: Make sure **Create Matching Identity Group** is selected, and then click **Save**.

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. The 'Policy' menu is expanded, showing 'Authentication', 'Authorization', 'Profiling', 'Posture', 'Client Provisioning', 'Security Group Access', and 'Policy Elements'. The 'Profiling' tab is selected. On the left, a tree view shows 'Profiling Policies' expanded. The main area displays the configuration for the 'Cisco-Access-Point' policy. The 'Name' is 'Cisco-Access-Point' and the 'Description' is 'Policy for all Cisco Access Points'. The 'Policy Enabled' checkbox is checked. The 'Minimum Certainty Factor' is set to 10. The 'Exception Action' is set to 'NONE'. The 'Network Scan (NMAP) Action' is set to 'NONE'. The 'Create Matching Identity Group' radio button is selected, and the 'Use Hierarchy' radio button is unselected. The 'Parent Policy' is 'Cisco-Device'. The 'Rules' section shows two rules: 'Cisco-Access-PointRule1Check1' with a 'Then' action of 'Certainty Factor Increases' and a value of 10, and 'Cisco-Access-PointRule3Check3' with a 'Then' action of 'Certainty Factor Increases' and a value of 10. At the bottom, there are 'Save' and 'Reset' buttons.

Procedure 2 Create authorization profile

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

Step 1: On the menu bar, mouse over **Policy**, and then in the Policy Elements section, select **Results**.

Step 2: In the panel on the left, double-click **Authorization**, and then double-click **Authorization Profiles**.

Step 3: Click **Add**.

Step 4: Name the profile **Cisco_APs** and give a description.

Step 5: Select **DACL Name** and in the list, make sure **PERMIT_ALL_TRAFFIC** is selected, and then click **Submit**.

The screenshot shows the 'New Authorization Profile' configuration page in the Cisco Identity Services Engine (ISE) web interface. The 'Name' field is set to 'Cisco_APs' and the 'Description' is 'Profile For Cisco Access Points'. The 'Access Type' is set to 'ACCESS_ACCEPT'. Under 'Common Tasks', 'DACL Name' is checked and set to 'PERMIT_ALL_TRAFFIC'. The 'Attributes Details' section shows 'Access Type = ACCESS_ACCEPT' and 'DACL = PERMIT_ALL_TRAFFIC'. The 'Submit' button is visible at the bottom.

Procedure 3 Create authorization policy

Step 1: On the menu bar, mouse over **Policy**, and then select **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.

The screenshot shows the 'Authorization Policy' configuration page in the Cisco Identity Services Engine (ISE) web interface. The 'First Matched Rule Applies' dropdown is set to 'First Matched Rule Applies'. The 'Exceptions (0)' section is expanded, showing a table with three rules: 'Black List Default', 'Profiled Cisco IP Phones', and 'Default'. The 'Default' rule is highlighted, and the 'Insert New Rule Above' button is visible.

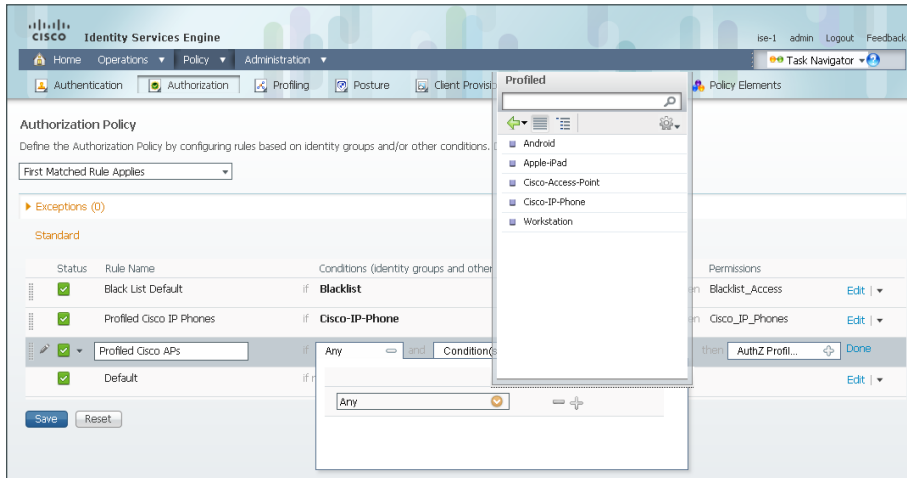
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions	
✓	Black List Default	if Blacklist	then Blacklist_Access	Edit ▼
✓	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones	Edit ▼
✓	Default	if no matches, then	PermitAccess	Edit ▼

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

Step 4: For the new rule, in the Conditions column, next to **Any**, click the **+** symbol.

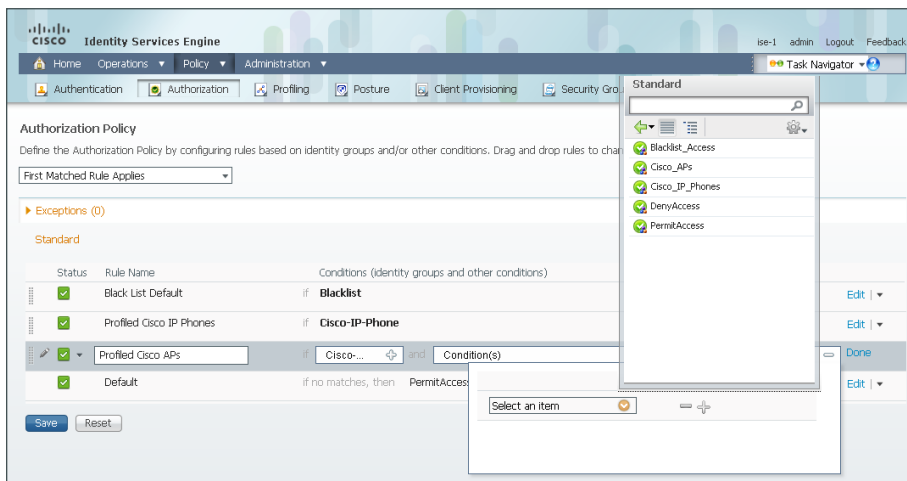
Step 5: From the list, next to **Endpoint Identity Groups**, click the > symbol and then next to **Profiled**, click the > symbol.

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

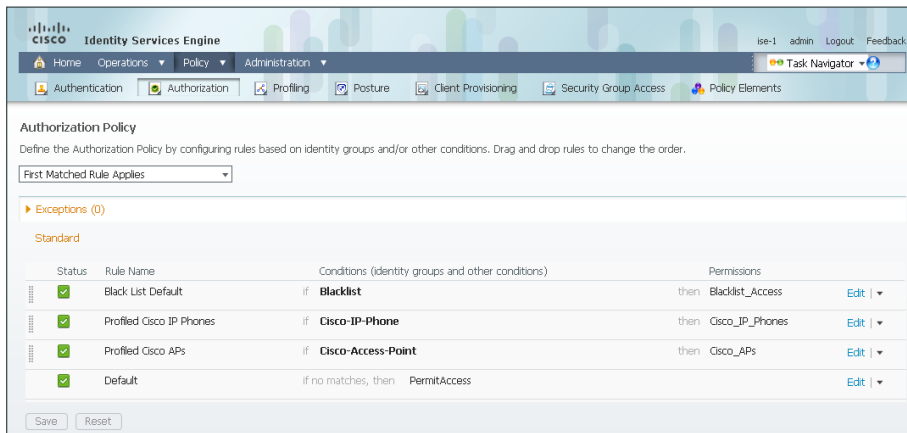


Step 7: Under the Permissions column, next to **AuthZ Profile**, click the + symbol.

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



Step 9: Click **Done**, and then click **Save**.



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 will be implementing low-impact mode, you need to modify the MAB policy to reject endpoints that fail authentication. This change works with the authorization policies for Cisco IP Phones and access points to be the only devices allowed on the network without performing 802.1X authentication.

Procedure 1

Modify MAB authentication rule

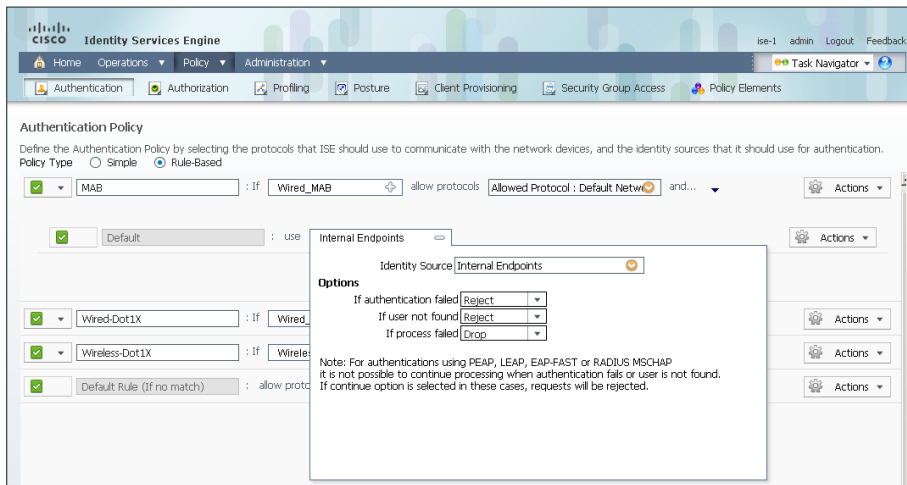
Step 1: On the menu bar, mouse over **Policy**, and then select **Authentication**.

Step 2: On the **MAB** rule, to the right of the and..., click the black triangle. This displays the identity store for this rule.

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

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

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



Enabling Authorization for Wired Endpoints

PROCESS

1. Create authorization profile
2. Create authorization policy
3. Enable low-impact mode
4. Enable low impact mode on Catalyst 4500
5. Enable change of authorization
6. Enable CoA on Catalyst 4500

You will enable authorization for wired endpoints that authenticate using digital certificates. At this stage, once authenticated, the endpoint will be 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 will create a profile for wired endpoints to permit full access.

Step 1: On the menu bar, mouse over **Policy**, and then in the Policy Elements section, select **Results**.

Step 2: In the panel on the left, double-click **Authorization**, and then double-click **Authorization Profiles**.

Step 3: Click **Add**.

Step 4: Name the profile **Wired_Dot1X** and give a description.

Step 5: Select **DACL Name** and in the list, make sure **PERMIT_ALL_TRAFFIC** is selected, and then click **Submit**.

Procedure 2 Create authorization policy

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

Step 1: On the menu bar, mouse over **Policy**, and then select **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.

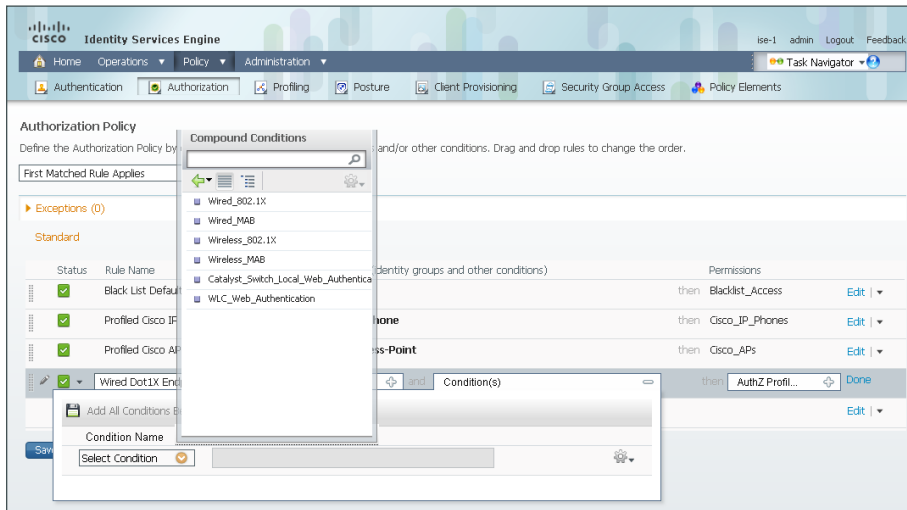
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Black List Default	if Blacklist	then Blacklist_Access
✓	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
✓	Profiled Cisco APs	if Cisco-Access-Point	then Cisco_APs
✓	Default	if no matches, then	PermitAccess

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

Step 4: For the new rule, in the Conditions column, next to Condition(s), click the **+** symbol.

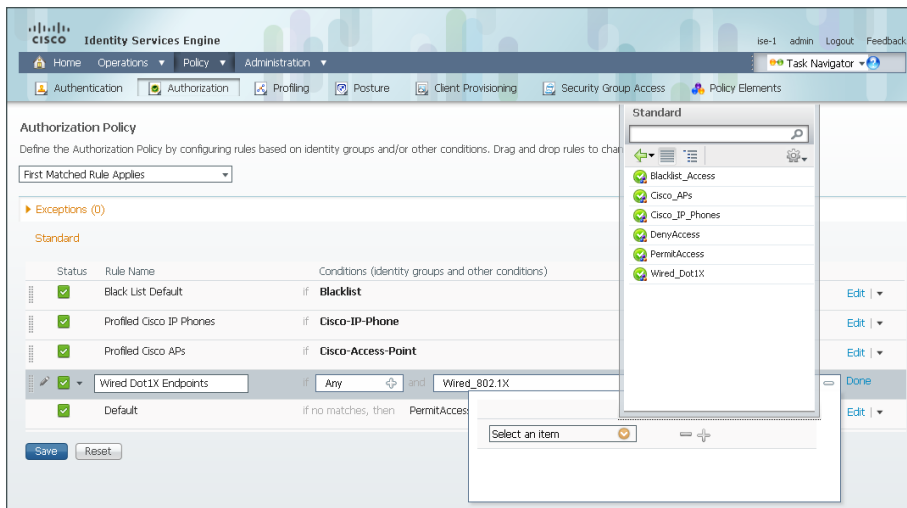
Step 5: Click **Select Existing Condition from Library**.

Step 6: In the list, next to Compound Conditions, click the > symbol, and then choose **Wired_802.1X**.

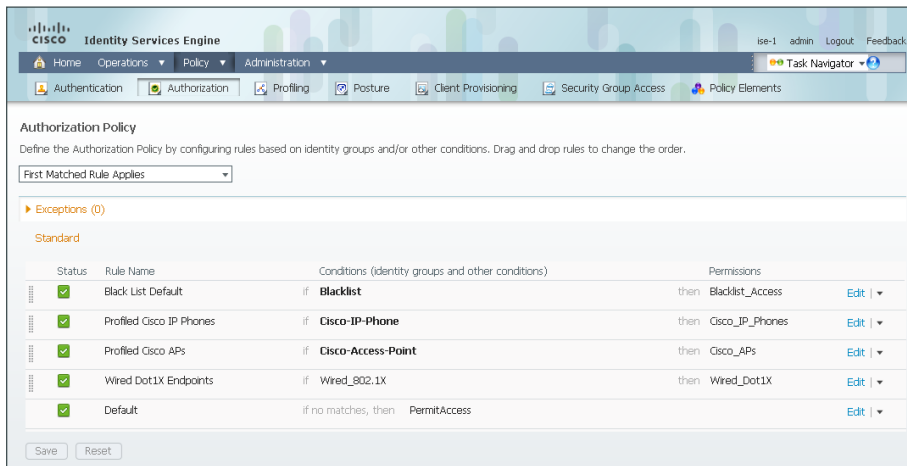


Step 7: Under the Permissions column, next to AuthZ Profile, click the + symbol.

Step 8: In the list, next to Standard, click the > symbol, and then choose **Wired_Dot1X**.



Step 9: Click **Done**, and then click **Save**.



Procedure 3 Enable low-impact mode

You will now configure the switches for low-impact mode 802.1X using Cisco Prime LMS 4.2 and the Cisco TrustSec Work Center. You need to create an access list to limit what traffic is permitted on a port before it is authenticated. You only want to enable what is required for the port to go through the authentication process. Typically, this means allowing DHCP, DNS, and TFTP to support Preboot Execution Environment, and access to the AD domain controller. For troubleshooting, you also allow ICMP echo and echo-reply traffic. You deny all other traffic and log the denials in order to determine if there is legitimate traffic that is getting denied and then make changes to the access list.

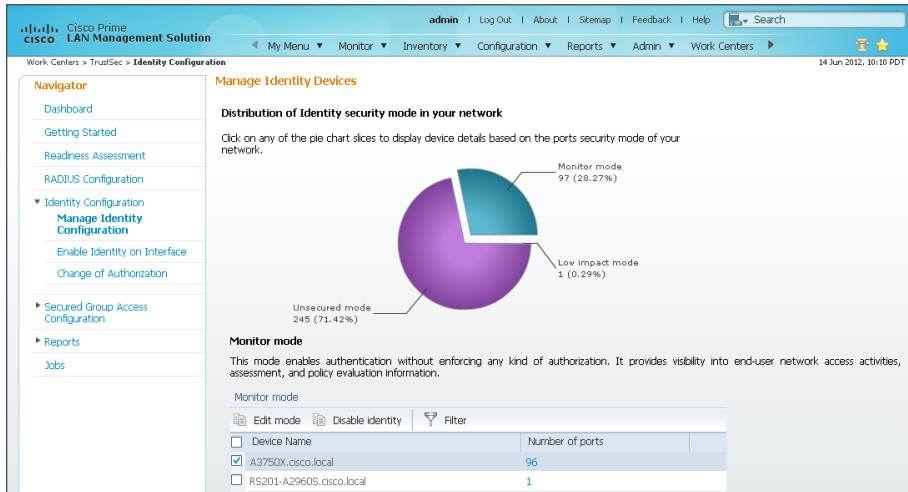
Step 1: Connect to Cisco Prime LMS with a web browser, for example: <https://lms.cisco.local>.

Step 2: Mouse over **Work Centers** and in the TrustSec section, click **Identity Configuration**.

Step 3: In the Navigator panel on the left, click **Manage Identity Configuration**.

Step 4: In the pie chart, click the Monitor Mode slice. A list of the devices that have ports configured for this mode appears.

Step 5: Select each switch with ports that you wish to move from monitor mode to low-impact mode, and then click **Edit Mode**.



Step 6: Select the check boxes next to the ports that you want to edit, and then click **Next**.

Manage Identity Devices

Review port selection on selected devices(optional)

View the ports and unselect the ports that you wish to exclude.

Selected Devices	Associated Ports																								
<table border="1"> <thead> <tr> <th>Display Name</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="radio"/> A3750X.cisco.local</td> </tr> </tbody> </table>	Display Name	<input checked="" type="radio"/> A3750X.cisco.local	<table border="1"> <thead> <tr> <th>Port Name</th> <th>Description</th> </tr> </thead> <tbody> <tr><td><input checked="" type="checkbox"/> G3/0/18</td><td>G3/0/18</td></tr> <tr><td><input checked="" type="checkbox"/> G3/0/19</td><td>G3/0/19</td></tr> <tr><td><input checked="" type="checkbox"/> G3/0/16</td><td>G3/0/16</td></tr> <tr><td><input checked="" type="checkbox"/> G2/0/22</td><td>G2/0/22</td></tr> <tr><td><input checked="" type="checkbox"/> G3/0/17</td><td>G3/0/17</td></tr> <tr><td><input checked="" type="checkbox"/> G2/0/23</td><td>G2/0/23</td></tr> <tr><td><input checked="" type="checkbox"/> G3/0/14</td><td>G3/0/14</td></tr> <tr><td><input checked="" type="checkbox"/> G2/0/20</td><td>G2/0/20</td></tr> <tr><td><input checked="" type="checkbox"/> G3/0/15</td><td>G3/0/15</td></tr> <tr><td><input checked="" type="checkbox"/> G2/0/21</td><td>G2/0/21</td></tr> </tbody> </table>	Port Name	Description	<input checked="" type="checkbox"/> G3/0/18	G3/0/18	<input checked="" type="checkbox"/> G3/0/19	G3/0/19	<input checked="" type="checkbox"/> G3/0/16	G3/0/16	<input checked="" type="checkbox"/> G2/0/22	G2/0/22	<input checked="" type="checkbox"/> G3/0/17	G3/0/17	<input checked="" type="checkbox"/> G2/0/23	G2/0/23	<input checked="" type="checkbox"/> G3/0/14	G3/0/14	<input checked="" type="checkbox"/> G2/0/20	G2/0/20	<input checked="" type="checkbox"/> G3/0/15	G3/0/15	<input checked="" type="checkbox"/> G2/0/21	G2/0/21
Display Name																									
<input checked="" type="radio"/> A3750X.cisco.local																									
Port Name	Description																								
<input checked="" type="checkbox"/> G3/0/18	G3/0/18																								
<input checked="" type="checkbox"/> G3/0/19	G3/0/19																								
<input checked="" type="checkbox"/> G3/0/16	G3/0/16																								
<input checked="" type="checkbox"/> G2/0/22	G2/0/22																								
<input checked="" type="checkbox"/> G3/0/17	G3/0/17																								
<input checked="" type="checkbox"/> G2/0/23	G2/0/23																								
<input checked="" type="checkbox"/> G3/0/14	G3/0/14																								
<input checked="" type="checkbox"/> G2/0/20	G2/0/20																								
<input checked="" type="checkbox"/> G3/0/15	G3/0/15																								
<input checked="" type="checkbox"/> G2/0/21	G2/0/21																								

Step 7: In the Identity mode to be configured section, move the **Security Mode** slider to **Low impact**, and then in the **Associated ACL** box, enter **PreAuth**.

Step 8: . In the Authentication profile and host mode section, set the following values:

- Define Authentication Profile—**802.1X, then MAB**
- Define Host Mode—**Multidomain**
- Action to be taken on security violation—**No Change**

Step 9: In the MAC Configuration section, make sure only **Enable MAC Move** is selected.

Step 10: In the Additional Configurations section, select **Advanced Options**. In the **Adhoc commands** box, enter the following commands, and then click **Next**.

```
ip device tracking
ip access-list extended PreAuth
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 log
```

The screenshot shows the 'Manage Identity Devices' configuration page in Cisco Prime LAN Management Solution. The page is divided into several sections:

- Security Mode:** A slider bar is set to 'Low impact' between 'Monitor' and 'High security'. Below it, 'Associated ACL' is set to 'PreAuth'.
- Authentication profile and host mode:** 'Define Authentication Profile' is set to '802.1x, then MAB'. 'Define Host Mode' has 'Multidomain' selected. 'Action to be taken on security violation' has 'No change' selected.
- MAC Configuration:** 'Enable MAC move or replace' is checked, with 'Enable MAC move' also checked. 'SNMP MAC notification' has 'Enable SNMP notification for MAC addition or removal' checked, with 'Notify MAC addition' and 'Notify MAC removal' also checked.
- Additional Configurations:** 'Advanced options' is checked. Below it, the 'Adhoc commands' box contains the following commands:

```
ip device tracking
ip http server
ip access-list extended PreAuth
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 log
```

At the bottom right, there are buttons for 'Previous', 'Next', 'Finish', and 'Cancel'.

Step 11: In the **Job Description** box, enter a description, and then click **Finish**. The job is submitted and a confirmation message appears. Click **OK**.



Tech Tip

You can review the CLI commands that will be pushed to the switch by clicking **Preview CLI**.

The global commands added to the switch configuration at the completion of this procedure are as follows.

```
ip device tracking
ip access-list extended PreAuth
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 log
```

The interface commands added at the completion of this procedure are as follows.

```
interface [interface]
ip access-group PreAuth in
authentication host-mode multi-domain
```

Procedure 4 Enable low impact mode on Catalyst 4500

The TrustSec Work Center supports TrustSec 2.0 features, which does not include support for Cisco Catalyst 4500. However, Catalyst 4500 does support all of the features in use. You will have to configure these using the NetConfig feature of Cisco LMS. This procedure covers configuring 802.1X in low impact mode.

Step 1: Connect to the Cisco Prime LMS server by browsing to <https://lms.cisco.local:1741>.

Step 2: Mouse over **Configuration**, and then, from the Tools section, choose **NetConfig**.

Step 3: In the NetConfig Job Browser, click **Create**.

Step 4: Select **Device Based** for the NetConfig Job Type, and then click **Go**.

Step 5: In the Device Selector, expand **All Devices**, select the devices where you want to enable low impact mode.

Step 6: In the Task Selector, expand **All Tasks**, select **Adhoc**, and then click **Next**.

Step 7: Click **Add Instance**, and then, in the new window, enter the CLI commands necessary to configure low impact mode.

```
ip device tracking
ip access-list extended PreAuth
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 log
```

Step 8: Click **Applicable Devices**, select the switch to which you want to apply this configuration, and then click **Close**.

Step 9: For the command mode, choose **Config**, and then click **Save**.

Step 10: After returning to the Add Tasks window, click **Next**.

Step 11: Fill in a description for the job, and then click **Next**. The job is submitted for immediate deployment.

Step 12: Click **Finish**, and then when you receive a notice that the job was submitted successfully, click **OK**.

Step 13: Navigate to **Configuration > Tools > NetConfig**. This opens the Job Browser.

Step 14: Click **Create**. This enables you to configure a new job.

Step 15: Select **Port based**, and then click **Go**.

Step 16: In the tree, next to All Devices, click the **+** symbol, select the switch you are configuring, and then click **Next**.



Tech Tip

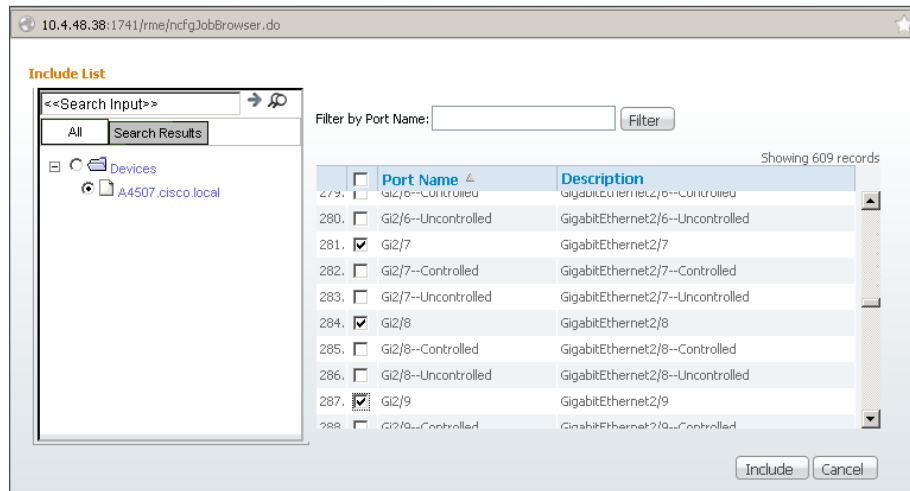
In this example, only one switch is being configured, but you can select multiple switches to accommodate a large deployment. The Group Selector allows you to choose switches by pre-defined groups or by model.

Step 17: Select **Define an Ad-Hoc Rule**. This brings up a new screen.

Step 18: For the ad-hoc rule, in the **Rule text** section, click **Include**.

Step 19: In the Include List section, expand **Devices**, and then select the switch you want to configure for low impact mode.

Step 20: Choose the ports you want to configure for low impact mode, and then click **Include**. The window closes.



Step 21: Move to step 3 of the wizard by clicking **Next**.

Step 22: In the Task Selector, select **Adhoc Task**, and then click **Next**.

Step 23: Click **Add Instance**, and then, in the new window, enter the CLI commands necessary in order to enable monitor mode and to remove the port security configuration.

```
ip access-group PreAuth in
authentication host-mode multi-domain
```

Step 24: Click **Applicable Devices**, select the switch to which you want to apply this configuration, click **Close**, and then click **Save**.

The screenshot shows the 'Adhoc Task Configuration' window with the 'IOS Parameters' tab selected. Under the 'Commands' section, there are two text areas: 'CLI Commands' and 'Rollback Commands'. The 'CLI Commands' area contains the text: `ip access-group PreAuth in` and `authentication host-mode multi-domain`. Below these areas is an 'Applicable Devices...' button. At the bottom of the window are 'Save', 'Reset', and 'Cancel' buttons.

Step 25: After returning to the Add Tasks window, click **Next**.

The screenshot shows the 'Add Tasks' window in the Cisco Prime LAN Management Solution. The left sidebar shows a navigation menu with 'Mode: ADDING' and steps 1 through 6. Step 4, 'Add Tasks', is currently selected. The main area is titled 'Add Tasks' and contains two panels: 'Applicable Tasks' and 'Added Instances'. The 'Applicable Tasks' panel shows 'Adhoc Task'. The 'Added Instances' panel shows 'Adhoc Task-1'. Below these panels are buttons for 'Add Instance...', 'Edit...', 'View CLI...', 'View Ports', and 'Delete'. At the bottom of the window are 'Back', 'Next', 'Finish', and 'Cancel' buttons. The status bar at the bottom indicates 'TAC Service Requests' and 'Alarms'.

Step 26: Fill in a description for the job, and then click **Next**. The job is submitted for immediate deployment.

Step 27: Click **Finish**, and then when you receive a notice that the job was submitted successfully, click **OK**.

Step 28: Repeat this procedure for each Cisco Catalyst 4500 where you need to configure low impact mode.

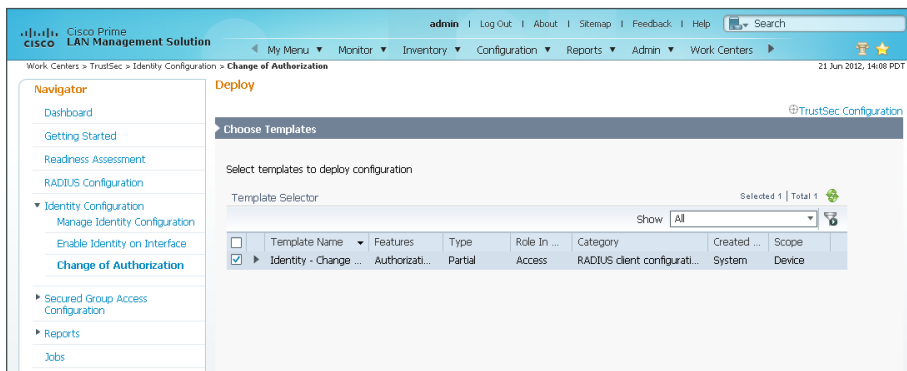
Procedure 5 Enable change of authorization

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, and you will need to enable it. You can do this by using the TrustSec Work Center of Cisco Prime LMS 4.2.

Step 1: In Cisco Prime LMS, mouse over **Work Centers**, and then, in the TrustSec section, click **Identity Configuration**.

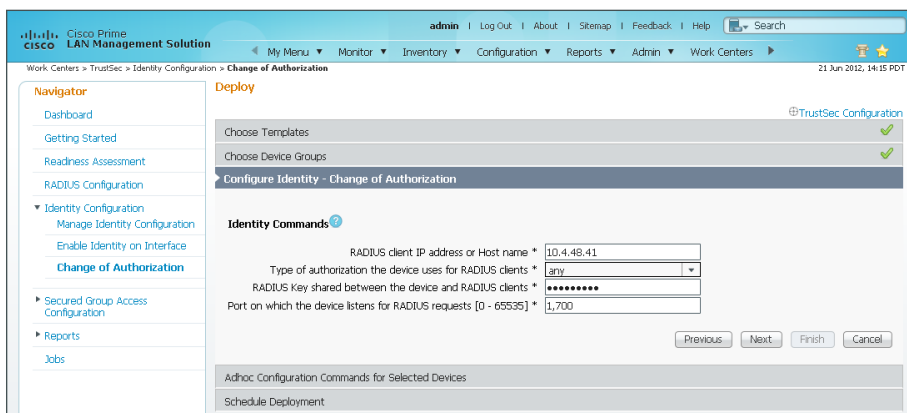
Step 2: In the Navigator panel on the left, click **Change of Authorization**.

Step 3: Select the built-in **Identity** template, and then click **Next**.



Step 4: In the Device Selector, expand **All Devices**, select the switches you want to enable for CoA, and then click **Next**.

Step 5: Enter the IP address of the primary Cisco ISE administration node, provide the RADIUS key, and then click **Next**.



Step 6: The Adhoc Configuration page allows you to add commands to the device in addition to the ones generated by the wizard. At this point, you don't need additional commands. Click **Next**.

Step 7: Give the job a description, and then click **Finish**.

The screenshot shows the Cisco Prime LMS interface for configuring a Change of Authorization (CoA) job. The left sidebar contains a 'Navigator' with links to various configuration areas. The main content area is titled 'Change of Authorization' and includes a 'Deploy' section with a table of configuration steps. Below this is the 'Schedule Deployment' section, which includes a 'Scheduler' with radio buttons for 'Immediate' (selected), 'Once', 'Daily', 'Weekly', and 'Monthly'. The 'Job Description' field contains 'A3750X CoA Config' and the 'E-mail' field is empty. There are also 'Job Options' checkboxes for 'Copy Startup to Running Config upon failure', 'Copy Running Config to Startup', and 'Enable Job Password'. At the bottom are buttons for 'Preview CLI', 'Previous', 'Next', 'Finish', and 'Cancel'.

Step 8: Repeat these steps for the secondary Cisco ISE administration node.

The global commands added to the switch configuration at the completion of this procedure are as follows.

```
aaa server radius dynamic-author
  client 10.4.48.41 server-key [key]
  client 10.4.48.42 server-key [key]
auth-type any
```

Procedure 6 Enable CoA on Catalyst 4500

The TrustSec Work Center supports TrustSec 2.0 features, which does not include support for Cisco Catalyst 4500. However, Catalyst 4500 does support all of the features in use. You will have to configure these using the NetConfig feature of Cisco LMS. This procedure covers configuring RADIUS change of authorization.

Step 1: Connect to the Cisco Prime LMS server by browsing to <https://lms.cisco.local:1741>.

Step 2: Mouse over **Configuration**, and then, from the Tools section, choose **NetConfig**.

Step 3: In the NetConfig Job Browser, click **Create**.

Step 4: Select **Device Based** for the NetConfig Job Type, and then click **Go**.

Step 5: In the Device Selector, expand **All Devices**, select the devices where you want to enable change of authorization.

Step 6: In the Task Selector, expand **All Tasks**, select **Adhoc**, and then click **Next**.

Step 7: Click **Add Instance**, and then, in the new window, enter the CLI commands necessary to enable change of authorization.

```
aaa server radius dynamic-author
  client 10.4.48.41 server-key [key]
  client 10.4.48.42 server-key [key]
auth-type any
```

Step 8: Click **Applicable Devices**, select the switch to which you want to apply this configuration, click **Close**, choose **Config** for the command mode, and then click **Save**.

Step 9: After returning to the Add Tasks window, click **Next**.

Step 10: Fill in a description for the job, and then click **Next**. The job is submitted for immediate deployment.

Step 11: Click **Finish**, and then when you receive a notice that the job was submitted successfully, click **OK**.

Step 12: Repeat this procedure for each Cisco Catalyst 4500 switch where you want to enable RADIUS change of authorization.

PROCESS

Enabling Authorization for Wireless Endpoints

1. Create authorization profile
2. Create authorization policy

You will enable authorization for wireless endpoints that authenticate using digital certificates. At this stage, once authenticated, the endpoint will be 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 will 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 will not need to define an access list at this point.

Step 1: In a browser, access the primary engine's GUI at <http://ise-1.cisco.local>. On the menu bar, mouse over **Policy**, and then in the Policy Elements section, select **Results**.

Step 2: In the panel on the left, double-click **Authorization**, and then double-click **Authorization Profiles**.

Step 3: Click **Add**.

Step 4: Name the profile **Wireless_Dot1X** and give a description.

Step 5: In the **Access Type** list, make sure **ACCESS_ACCEPT** is selected, and then click **Submit**.

Procedure 2 Create authorization policy

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

Step 1: On the menu bar, mouse over **Policy**, and then select **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.

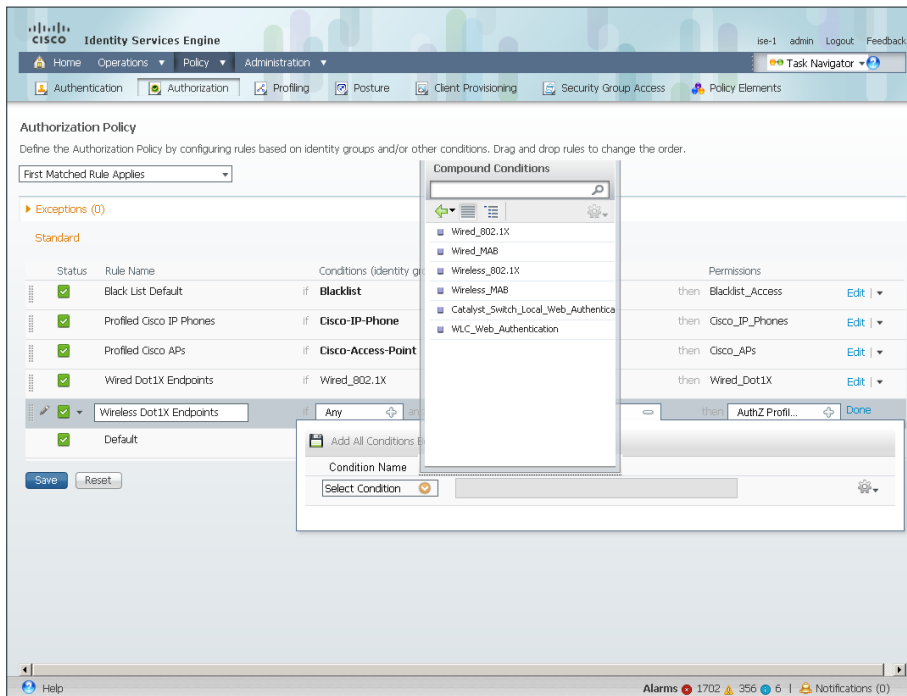
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Black List Default	if Blacklist	then Blacklist_Access
✓	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
✓	Profiled Cisco APs	if Cisco-Access-Point	then Cisco_APs
✓	Wired Dot1X Endpoints	if Wired_802.1X	then Wired_Dot1X
✓	Default	if no matches, then	PermitAccess

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.

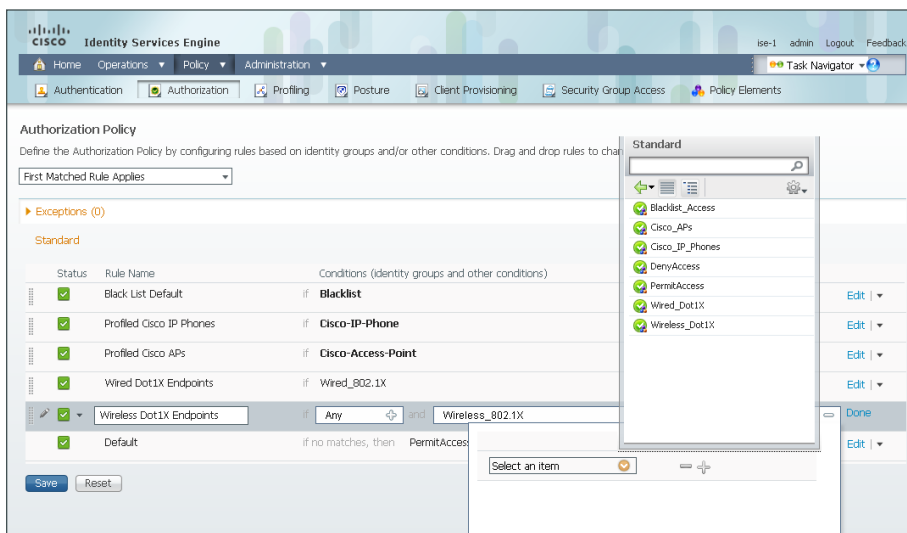
Step 5: Click **Select Existing Condition from Library**.

Step 6: In the list, next to Compound Conditions, click the > symbol, and then choose **Wireless_802.1X**.

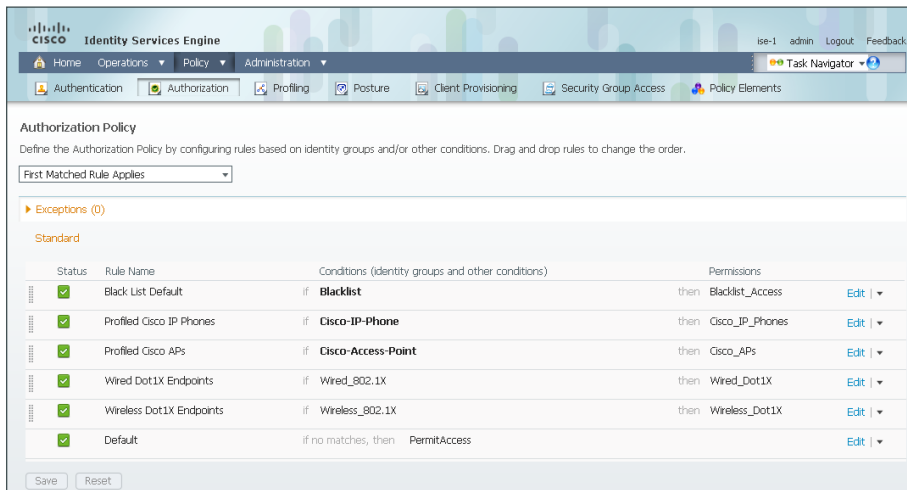


Step 7: Under the Permissions column, next to AuthZ Profile, click the + symbol.

Step 8: In the list, next to Standard, click the > symbol, and then choose **Wireless_Dot1X**.



Step 9: Click **Done**, and then click **Save**.



PROCESS

Modifying the Authorization Policy to be Closed

1. Modify default rule

The current authorization policy 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 would then just permit access to the network. Now that you have enabled low-impact mode, you will need to change this rule to deny access to any request that doesn't match one of the specific rules.

Procedure 1 Modify default rule

Step 1: On the menu bar, mouse over **Policy**, and then select **Authorization**.

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

Step 3: In the Conditions column, next to PermitAccess, click the **+** symbol.

Step 4: In the list, next to Standard, click the > symbol, and then choose **DenyAccess**.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The 'Authorization Policy' section is active, and the 'Standard' tab is selected. A dropdown menu is open, showing a list of policy elements. The 'DenyAccess' element is highlighted. The 'Default' rule is currently set to 'PermitAccess'.

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Black List Default	if Blacklist	then Blacklist_Access
<input checked="" type="checkbox"/>	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
<input checked="" type="checkbox"/>	Profiled Cisco APs	if Cisco-Access-Point	then Cisco_APs
<input checked="" type="checkbox"/>	Wired Dot1X Endpoints	if Wired_802.1X	then Wired_Dot1X
<input checked="" type="checkbox"/>	Wireless Dot1X Endpoints	if Wireless_802.1X	then Wireless_Dot1X
<input checked="" type="checkbox"/>	Default	if no matches, then	DenyAccess

Step 5: Click **Done**, and then click **Save**.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The 'Authorization Policy' section is active, and the 'Standard' tab is selected. The 'Default' rule is now set to 'DenyAccess'.

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Black List Default	if Blacklist	then Blacklist_Access
<input checked="" type="checkbox"/>	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
<input checked="" type="checkbox"/>	Profiled Cisco APs	if Cisco-Access-Point	then Cisco_APs
<input checked="" type="checkbox"/>	Wired Dot1X Endpoints	if Wired_802.1X	then Wired_Dot1X
<input checked="" type="checkbox"/>	Wireless Dot1X Endpoints	if Wireless_802.1X	then Wireless_Dot1X
<input checked="" type="checkbox"/>	Default	if no matches, then	DenyAccess

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

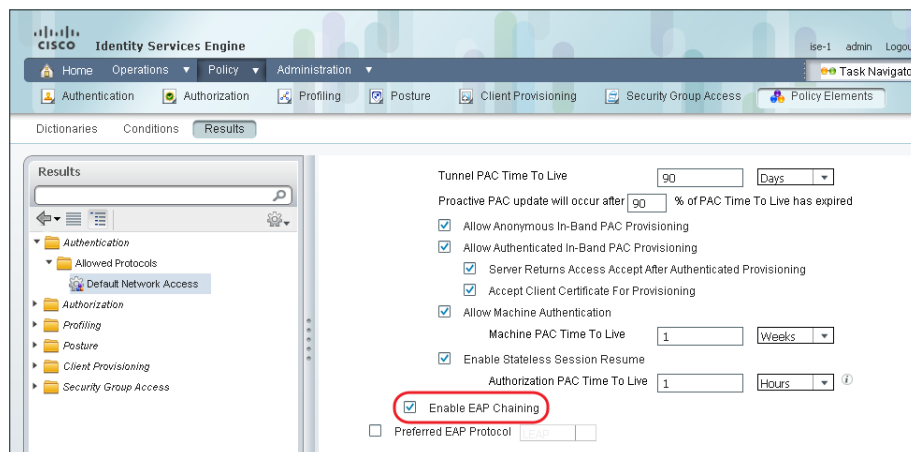
Step 1: Connect to <https://ise-1.cisco.local>.

Step 2: On the menu bar, mouse over **Policy**, and then, from the Policy Elements section of the menu, choose **Results**.

Step 3: In the left pane, double-click **Authentication**. This expands the options.

Step 4: Double-click **Allowed Protocols**, and then select **Default Network Access**.

Step 5: Select **Enable EAP Chaining**, and then click **Save**.



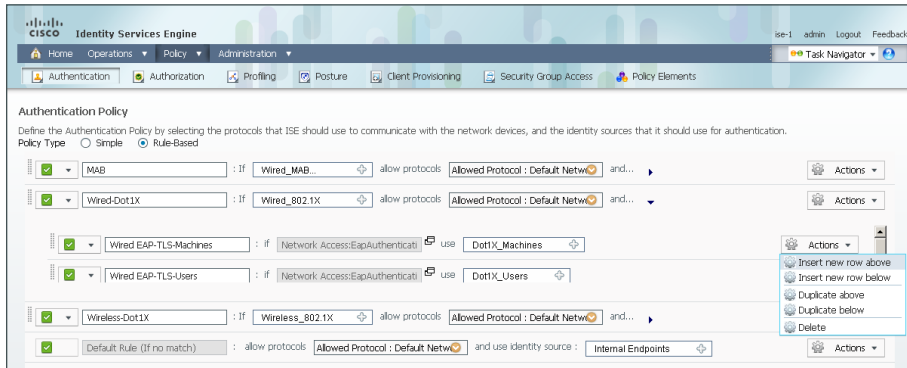
Procedure 2 Create authentication policy

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: Mouse over **Policy**, and then choose **Authentication**.

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

Step 3: Next to the first rule, in the **Actions** list, choose **Insert new row above**.



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

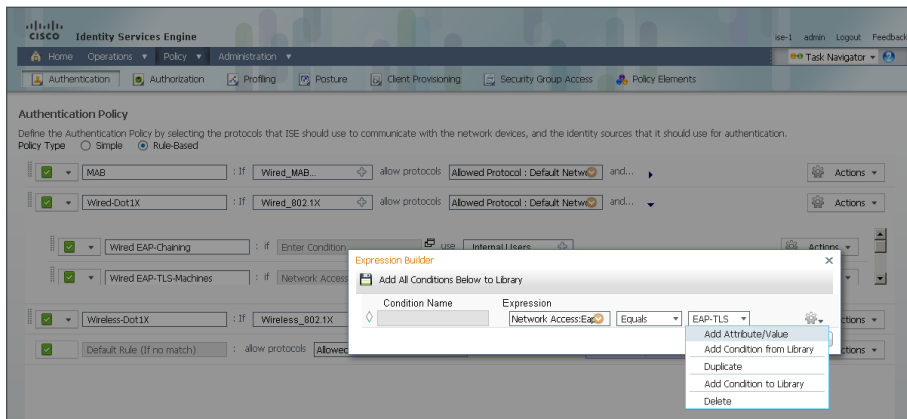
Step 5: Click **Create New Condition (Advance Option)**.

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

Step 7: Next to Network Access, click the arrow, and then select **EapAuthentication**.

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

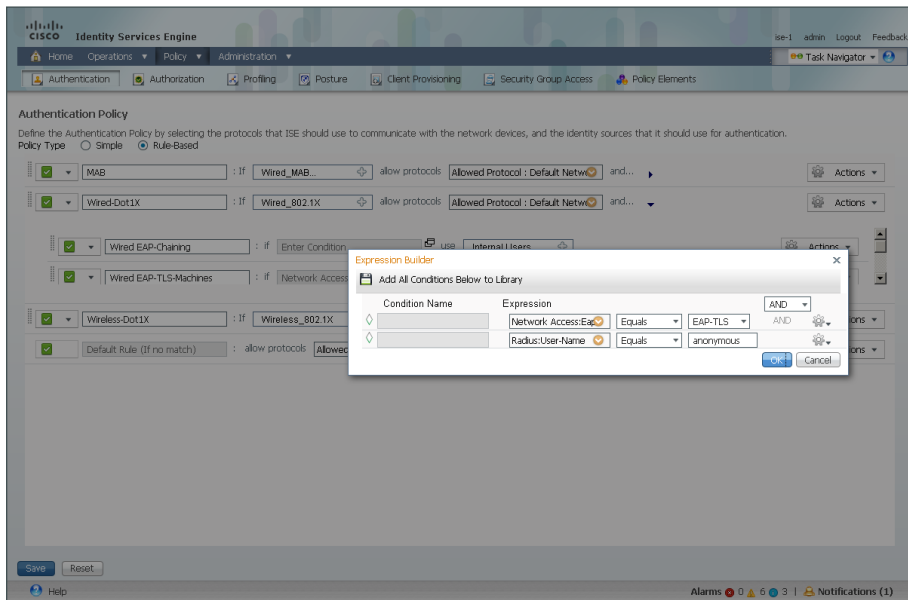
Step 9: Click the gear icon at the end of the condition, and then choose **Add Attribute/Value**.



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

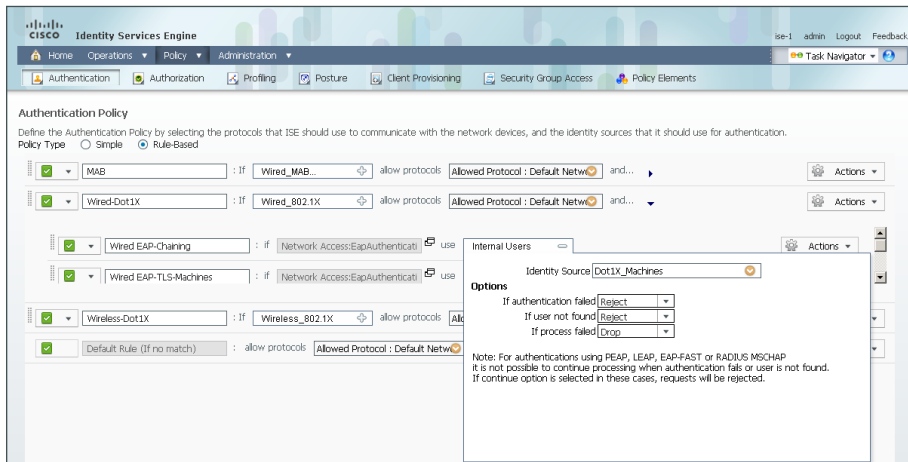
Step 11: Next to Radius, click the arrow, and then choose **User-name**.

Step 12: In the second list, choose **Equals**, and then in the last box, type **anonymous**, and then click **OK**.



Step 13: Next to Internal Users, click the **+** symbol.

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,” use the default options for this identity source, and then click anywhere in the window to continue.



Step 15: Click **Save**.

Step 16: Repeat Step 2 through Step 15 for the Wireless-Dot1X rule.

Procedure 3 Create authorization profile

An authorization profile defines the specific access policies granted to the device. You will 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 will allow you to modify the policy if you choose to make a more restrictive policy in the future.

Step 1: On the menu bar, mouse over **Policy**, and then in the Policy Elements section, click **Results**.

Step 2: In the panel on the left, double-click **Authorization**, and then double-click **Authorization Profiles**.

Step 3: Click **Add**.

Step 4: Name the profile **User+Machine-Cert** and give a description.

Step 5: Select **DACL Name** and in the list, choose **PERMIT_ALL_TRAFFIC**, and then click **Submit**.

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. The 'Policy' menu is expanded, showing 'Authentication', 'Authorization', 'Profiling', 'Posture', 'Client Provisioning', 'Security Group Access', and 'Policy Elements'. The 'Results' tab is selected in the 'Policy Elements' section. On the left, a tree view shows the hierarchy: 'Authentication' > 'Authorization' > 'Authorization Profiles'. The main content area is titled 'Authorization Profile' for 'User+Machine-Cert'. It includes fields for 'Name' (User+Machine-Cert), 'Description' (EAP Chaining Profile For User And Machine Certificates), and 'Access Type' (ACCESS_ACCEPT). Under 'Common Tasks', the 'DACL Name' checkbox is checked and set to 'PERMIT_ALL_TRAFFIC'. Other options like 'VLAN', 'Voice Domain Permission', 'Web Authentication', and 'Auto Smart Port' are unchecked. The 'Advanced Attributes Settings' section shows a 'Select an item' dropdown. The 'Attributes Details' section displays 'Access Type = ACCESS_ACCEPT' and 'DACL = PERMIT_ALL_TRAFFIC'. At the bottom are 'Save' and 'Reset' buttons.

Procedure 4 Create authorization rule

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

Step 1: On the menu bar, mouse over **Policy**, and then select **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.

Step 3: Rename the rule **EAP Chaining Machine andUser**.

Step 4: For the new rule, in the Conditions column, next to Condition(s), click the + symbol.

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

Step 6: Under Expression, next to Select Attribute, click the arrow. The menu opens.

Step 7: Next to Network Access, click the > symbol, and then choose **EapAuthentication**.

Step 8: In the first list, choose **Equals**, and then, in the second list, 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 rule, under Expression, next to Select Attribute, click the arrow. The menu opens.

Step 11: Next to Network Access, click the > symbol, and then choose **EapTunnel**.

Step 12: In the first list, choose **Equals**, and then, in the second list, choose **EAP-FAST**.

Step 13: Click the gear icon at the end of the rule, and then select **Add Attribute/Value**.

Step 14: In the new rule, under Expression, next to Select Attribute, click the arrow. The menu opens.

Step 15: Next to Network Access, click the > symbol, and then choose **EapChainingResult**.

Step 16: In the first list, choose **Equals**, and then, in the second list, choose **User and machine both succeeded** then click anywhere to continue.

Step 17: In the Permissions section, next to AuthZ Profile(s), click the + symbol.

Step 18: In the **Select an item** list, next to Standard, click the > symbol.

Step 19: Choose the User+Machine-Cert authorization profile that you created in Procedure 3, "Create authorization profile."

Step 20: Click **Done**, and then click **Save**.

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, you will create a wired profile for EAP Chaining.

Step 3: Click **Networks**, and then click **Add**.

Step 4: Enter a name for the profile, select **Wired (802.3) Network**, and then click **Next**.

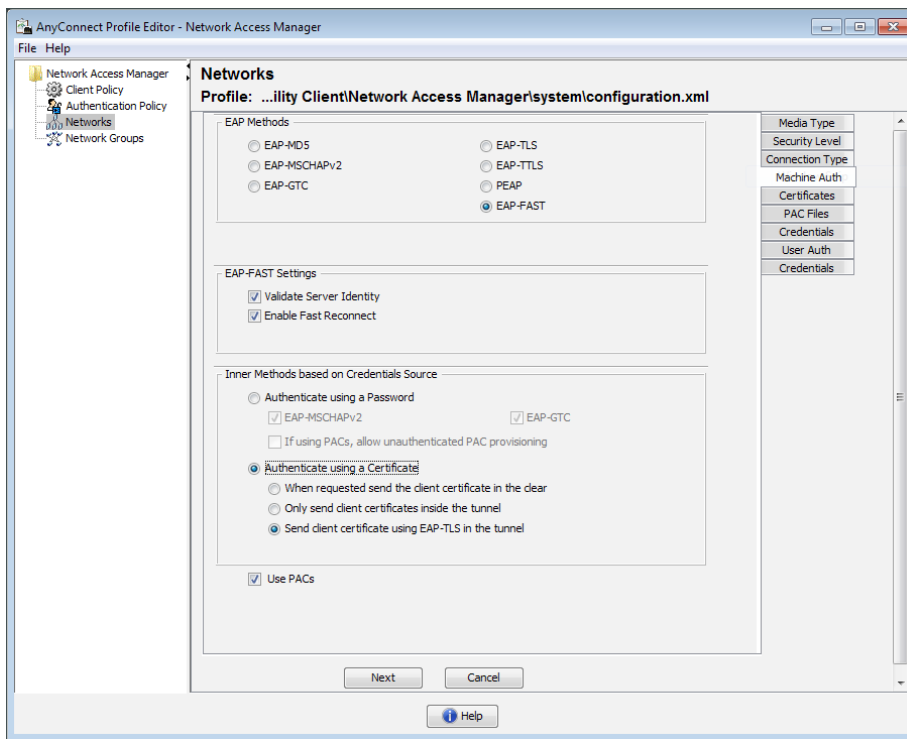
Step 5: Select **Authenticating Network**, and then click **Next**.

Step 6: Select **Machine and User Connection**, and then click **Next**.

Step 7: For the machine authentication method, select **EAP-FAST**.

Step 8: In the Inner Methods based on Credentials Source section, select **Authenticate using a certificate** and **Send client certificate using EAP-TLS in the tunnel**.

Step 9: Make sure **Use PACs** is selected, and then click **Next**.

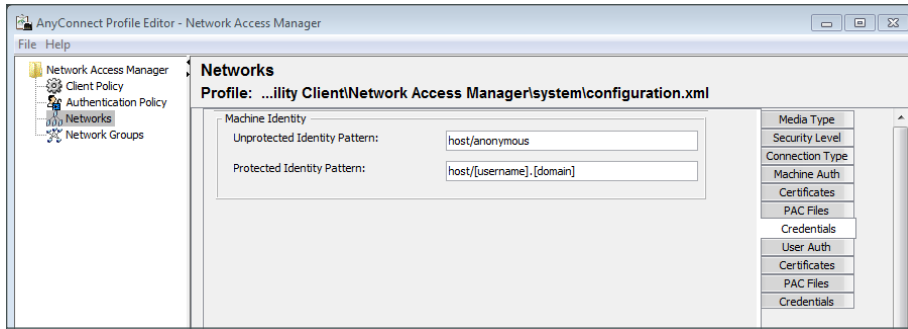


Step 10: For the Certificates tab, click **Next**. This accepts the default values.

Step 11: For the PAC Files tab, click **Next**. This accepts the default values.

Step 12: Enter an unprotected identity pattern. In this deployment, use **host/anonymous**.

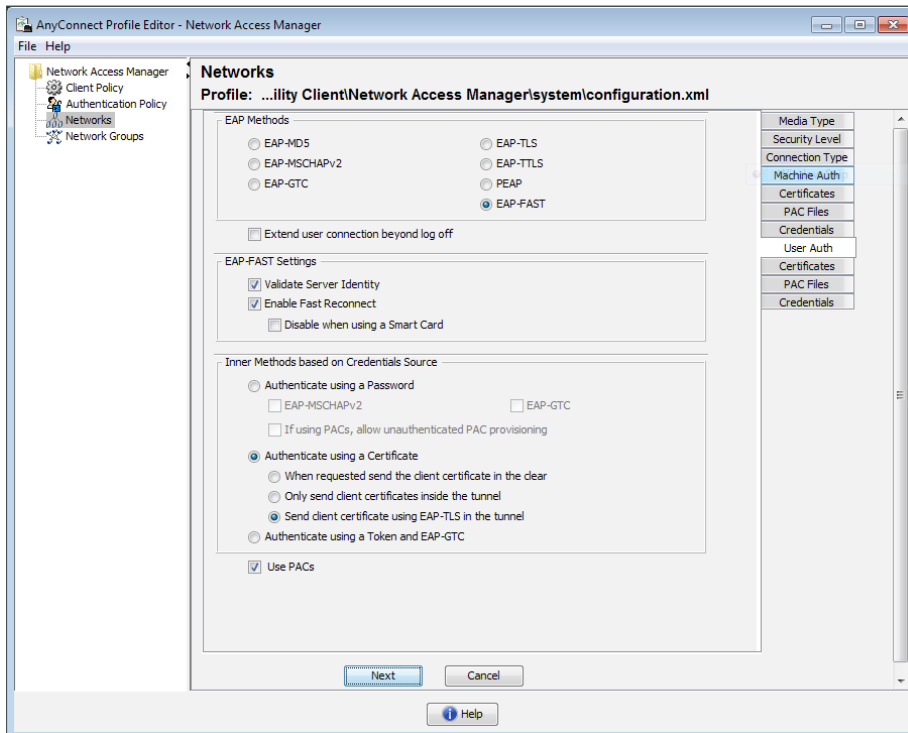
Step 13: Enter a protected identity pattern. In this deployment, use **host/[username].[domain]**, and then click **Next**.



Step 14: For the user authentication method, select **EAP-FAST**.

Step 15: In the Inner Methods based on Credentials Source section, select **Authenticate using a certificate** and **Send client certificate using EAP-TLS in the tunnel**.

Step 16: Make sure **Use PACs** is selected, and then click **Next**.



Step 17: For the Certificates tab, click **Next**. This accepts the default values.

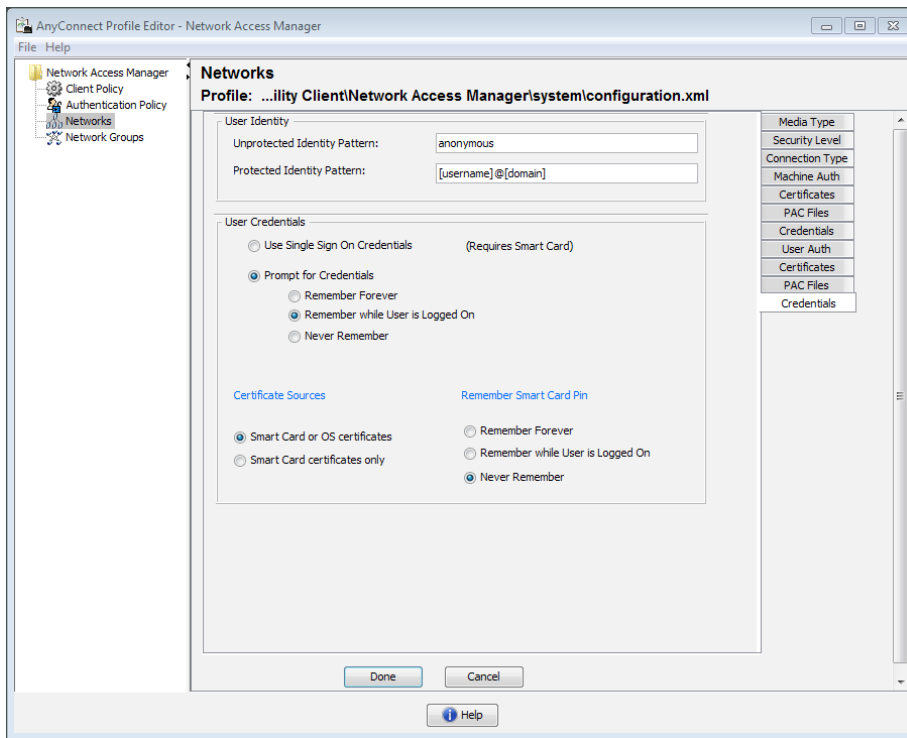
Step 18: For the PAC Files tab, click **Next**. This accepts the default values.

Step 19: Enter an unprotected identity pattern. In this deployment, use **anonymous**.

Step 20: Enter a protected identity pattern. In this deployment, use **[username]@[domain]**.

Step 21: In the User Credentials section, select **Prompt for Credentials**, and then select **Remember while User is Logged On**.

Step 22: Under **Certificate Sources**, select **Smart Card or OS certificates**, and then click **Done**.



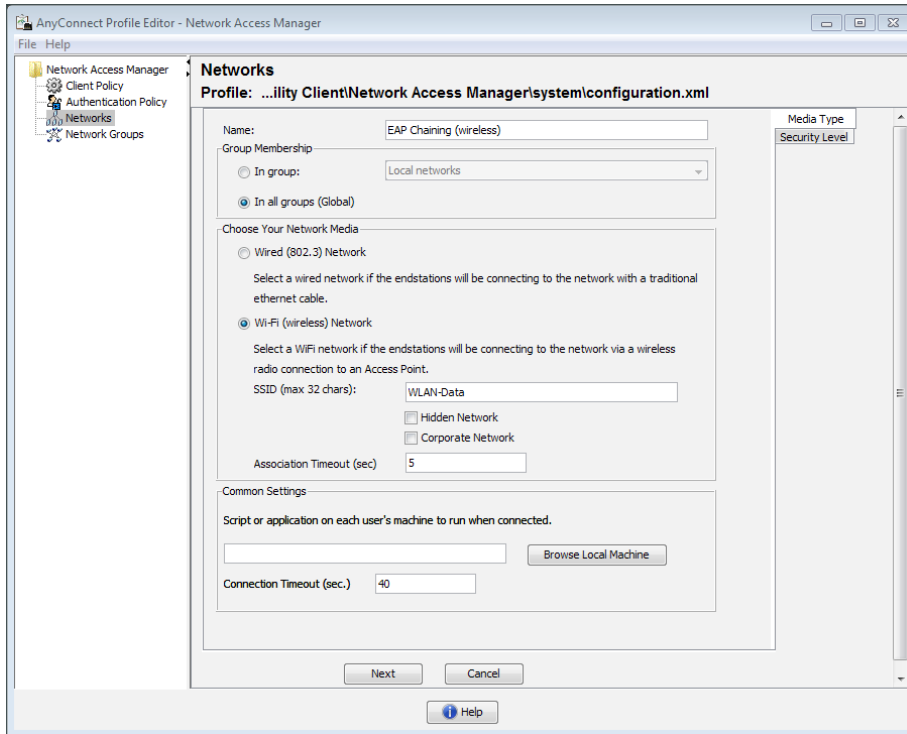
Procedure 6 Configure AnyConnect wireless profile

You will now create a wireless profile for EAP Chaining.

Step 1: Click **Networks**, and then click **Add**.

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**.



Step 4: Select **Authenticating Network**, choose **WPA2 Enterprise (AES)** for Association Mode, and then click **Next**.

Step 5: Select **Machine and User Connection**, and then click **Next**.

Step 6: For the machine authentication method, select **EAP-FAST**.

Step 7: In the Inner Methods based on Credentials Source section, select **Authenticate using a certificate** and **Send client certificate using EAP-TLS in the tunnel**.

Step 8: Make sure **Use PACs** is selected, and then click **Next**.

Step 9: For the Certificates tab, click **Next**. This accepts the default values.

Step 10: For the PAC Files tab, click **Next**. This accepts the default values.

Step 11: Enter an unprotected identity pattern. In this deployment, use **host/anonymous**.

Step 12: Enter a protected identity pattern. In this deployment, use **host/[username].[domain]**, and then click **Next**.

Step 13: For the user authentication method, select **EAP-FAST**.

Step 14: In the Inner Methods based on Credentials Source section, select **Authenticate using a certificate** and **Send client certificate using EAP-TLS in the tunnel**.

Step 15: Make sure **Use PACs** is selected, and then click **Next**.

Step 16: For the Certificates tab, click **Next**. This accepts the default values.

Step 17: For the PAC Files tab, click **Next**. This accepts the default values.

Step 18: Enter an unprotected identity pattern. In this deployment, use **anonymous**.

Step 19: Enter a protected identity pattern. In this deployment, use **[username]@[domain]**.

Step 20: In the User Credentials section, select **Prompt for Credentials**, and then select **Remember while User is Logged On**.

Step 21: Under **Certificate Sources**, select **Smart Card or OS certificates**, and then click **Done**.

Step 22: From the **File** menu, choose **Save**. This updates the configuration file.

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 Active Directory (AD) group. You will 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 engine's GUI at <http://ise-1.cisco.local>.

Step 2: Mouse over **Administration**, and then, from the Identity Management section of the menu, choose **External Identity Sources**.

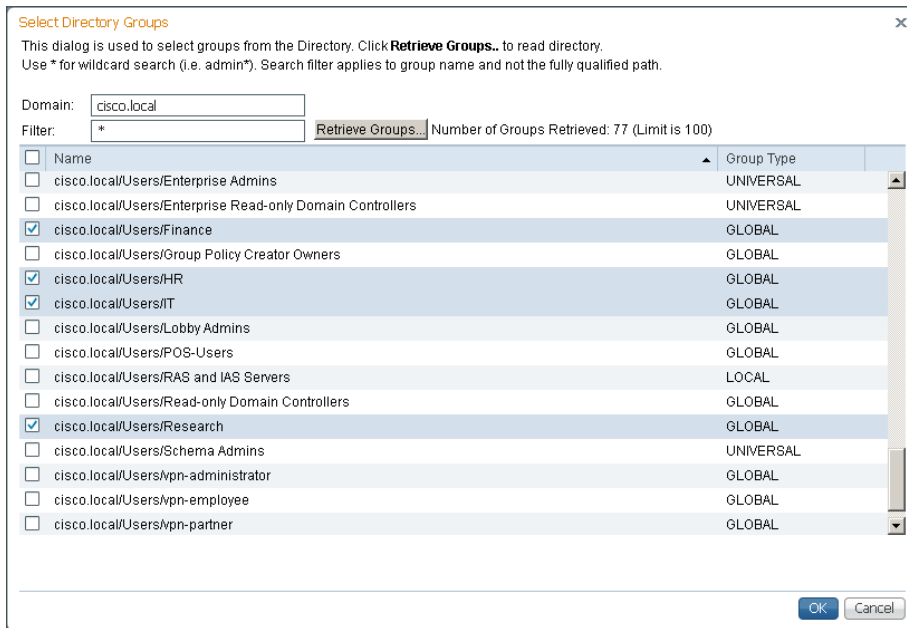
Step 3: In the left panel, click **Active Directory**.

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** 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



Step 7: Click **Save Configuration**.

Procedure 2 Create wired access list

You will need to create an access list to deploy on the switches that will limit what portions of the network members of the group can access. The access list will use standard IOS syntax.

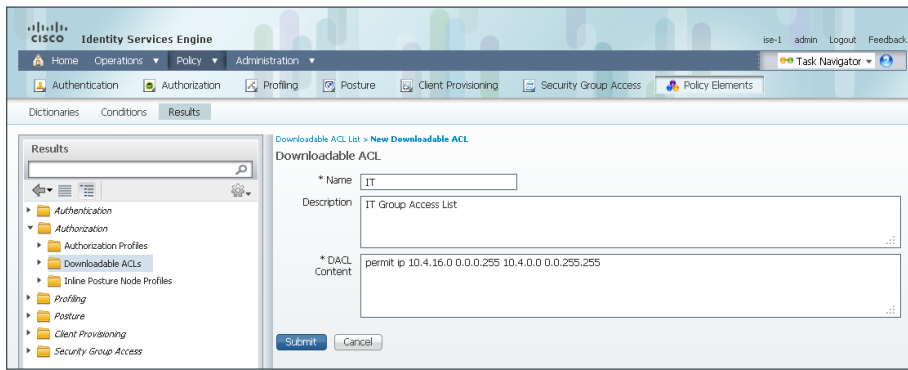
Step 1: On the menu bar, mouse over **Policy**, and then, in the Policy Elements section, choose **Results**.

Step 2: In the left pane, double-click **Authorization**, and then select **Downloadable ACLs**.

Step 3: Click **Add**.

Step 4: Enter a name (example: IT) and a description for the policy.

Step 5: In the DACL content section, enter the ACL by using IOS syntax, and then click **Submit**.



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: On the menu bar, mouse over **Policy**, and then, in the Policy Elements section, choose **Results**.

Step 2: In the left pane, double-click **Authorization**, and then select **Authorization Profiles**.

Step 3: Click **Add**.

Step 4: Enter a name (example: IT) and a description for the policy.

Step 5: In the Common Task section, select **DACL Name**, and then select the ACL that you configured in Procedure 2, “Create wired access list.” In the example, the ACL is “IT.”

Step 6: In the Common Task section, select **Airespace ACL Name**, and then enter the name of the ACL that you are applying to the WLC. In this example, the ACL is “IT.”

Step 7: Click **Submit**.

Procedure 4 Create authorization policy

Step 1: On the menu bar, mouse over **Policy**, and then click **Authorization**.

Step 2: 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.

Step 3: Rename Standard Rule 1 to **IT**.

Step 4: In the **Condition(s)** list, choose the **+** symbol, and then click **Create New Condition (Advance Option)**.

Step 5: Under Expression, next to Select Attribute, click the arrow. The menu opens.

Step 6: Next to AD1, click the > symbol, and then choose **ExternalGroups**.

Step 7: In the first list, choose **Equals**, and then, in the second list, choose **cisco.local/Users/IT**.

Step 8: In the Permissions section, next to AuthZ Profile(s), click the + symbol.

Step 9: In the **Select an item** list, next to Standard, choose the > symbol.

Step 10: Select the IT authorization profile that was created in Procedure 3, "Create authorization profile."

Step 11: Click **Done**, and then click **Save**.

Step 12: For each group that you want to define a policy for, repeat Procedure 2, "Create wired access list," Procedure 3, "Create authorization profile," and Procedure 4, "Create authorization policy." In this example deployment, you will create additional policies for the Finance, HR, and Research groups.

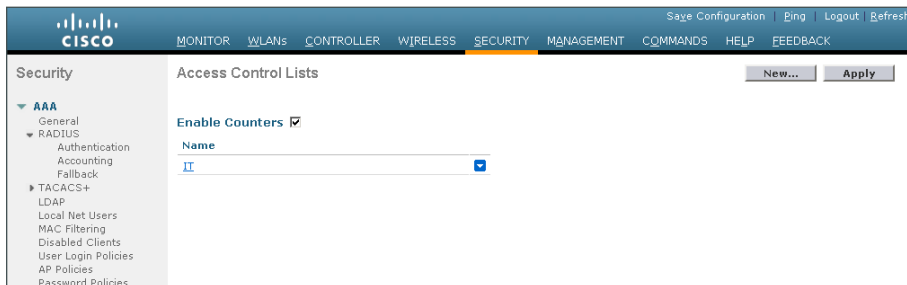
Procedure 5 Configure WLC for authorization

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 in the campus, and at remote sites with a local controller, connect to the WLC and authenticate, Cisco ISE passes a RADIUS attribute requesting the ACL be applied for this client.

Step 1: In your browser, enter <https://wlc1.cisco.local>. This takes you to the WLC console.

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

Step 3: In the left pane, expand **Access Control Lists**, and then click **Access Control Lists**.



Step 4: Click **New**.

Step 5: Name the access list, and then click **Apply**.

Step 6: Click the name in the list. This allows you to edit the newly created access list.

Step 7: Click **Add New Rule**.

Step 8: Create a new access list rule based on your security policy, and then click **Apply**. In our example deployment, members of the IT group are only allowed access to the internal network (10.4.0.0/16).

The screenshot shows the Cisco ISE Security configuration page. The left sidebar lists various security features, with 'AAA' expanded. The main content area is titled 'Access Control Lists > Edit'. It shows the 'General' tab for an access list named 'IT' with 185 deny counters. Below this is a table of rules:

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 9: Repeat Step 3 through Step 8 in this procedure for each access list that you defined in the authorization profiles in Cisco ISE.

The screenshot shows the Cisco ISE Security configuration page. The left sidebar lists various security features, with 'AAA' expanded. The main content area is titled 'Access Control Lists'. It shows the 'Enable Counters' checkbox checked. Below this is a table of rules:

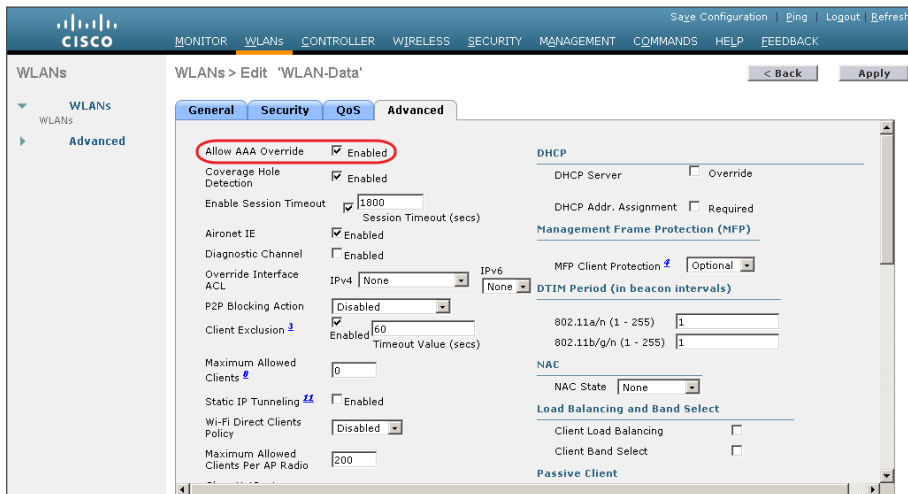
Name	Enable Counters
IT	<input checked="" type="checkbox"/>
HR	<input checked="" type="checkbox"/>
Research	<input checked="" type="checkbox"/>
Finance	<input checked="" type="checkbox"/>

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 10: On the menu bar, click **WLANs**.

Step 11: Click the WLAN ID of the wireless network that the wireless personal devices are accessing.

Step 12: Click **Advanced**, and then select **Allow AAA Override**.



Step 13: Click **Apply**, and then click **Save Configuration**.

Enabling Security Group Access

PROCESS

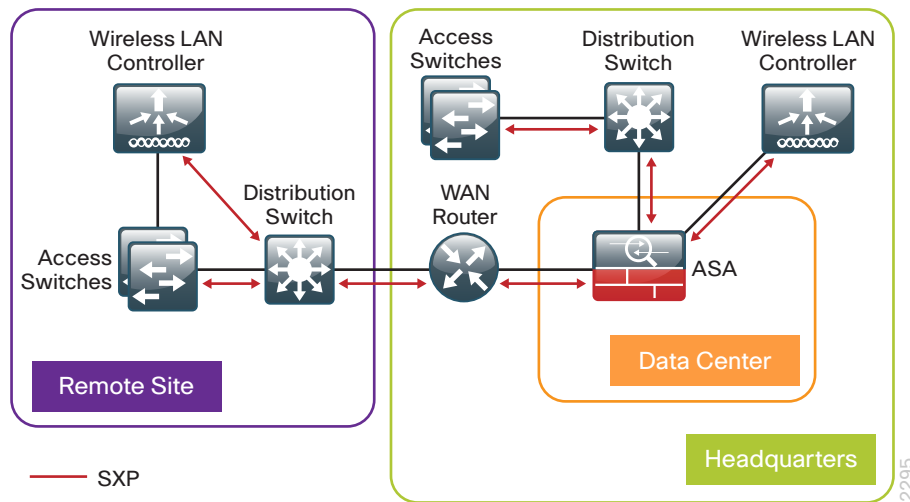
1. Define Security Group Tags
2. Add ASA as network device
3. Modify authorization policy
4. Configure SXP on IOS devices
5. Configure SXP on WLCs
6. Configure SXP on ASA
7. Configure firewall policy
8. Monitoring SGTs on Cisco ASA
9. Monitoring SGTs on the switches
10. Monitoring SGTs on the WLC

Security Group Access (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 Security Group Tags (SGT) and Security Group Access Control Lists (SGACL).

The SGT Exchange Protocol (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 of 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: In a browser, access the primary engine's GUI at <http://ise-1.cisco.local>.

Step 2: On the menu bar, mouse over **Policy**, and then in the Policy Elements section, select **Results**.

Step 3: In the panel on the left, double-click **Security Group Access**, and then click **Security Groups**.

Step 4: Click **Add**.

Step 5: Give the group a name and description, and then click **Submit**.

Step 6: Repeat Step 4 and Step 5 for each tag you wish to create. In this example deployment, you create tags for each of the following groups: Finance_Users, HR_Users, IT_Users, Research_Users, and Network_Devices.

Procedure 2 Add ASA as 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: On the menu bar, mouse over **Administration**, and then in the Network Resources section, click **Network Devices**.

Step 2: Click **Add**.

Step 3: Enter the hostname of the ASA appliance and give it a description.

Step 4: For the IP address, enter **10.4.53.126**.

Network Devices List > **New Network Device**

Network Devices

* Name

Description

* IP Address: /

Model Name

Software Version

* Network Device Group

Location

Device Type

Step 5: Select **Authentication Settings**.

Step 6: Enter the RADIUS shared secret.

☒ **Authentication Settings**

Enable Authentication Settings

Protocol **RADIUS**

* Shared Secret

Enable KeyWrap ☐ ⓘ

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ☒ ASCII ☐ HEXADECIMAL

Step 7: Select **Advanced TrustSec Settings**.

Step 8: In the Device Authentication Settings section, make sure **Use Device ID for SGA Identification** is selected, and enter a password.

Step 9: In the SGA Notifications and Updates section, accept the default values.

Advanced TrustSec Settings

Device Authentication Settings

Use Device ID for SGA Identification ☒

Device Id

* Password

SGA Notifications and Updates

* Download environment data every

* Download peer authorization policy every

* Reauthentication every ⓘ

* Download SGACL lists every

Other SGA devices to trust this device ☒

Notify this device about SGA configuration changes ☐

Step 10: In the Out of Band (OOB) SGA PAC section, click **Generate PAC**.

Step 11: Enter an encryption key and the PAC time to live, and then click **Generate PAC**.

Step 12: You are prompted to save the file to your local machine. 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 section, you created authorization policies that limited network access based on Active Directory group membership by using access lists. In this procedure, you will modify those policies to instead use SGTs.

Step 1: On the menu bar, mouse over **Policy**, and then click **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 to add a new permission.

Step 5: Expand the drop-down menu and click the **>** symbol next to Security Group.

Step 6: Select **IT_Users**.

Step 7: Click **Done**, and then click **Save**.

Step 8: Repeat Step 2 through Step 7 for each policy you need to modify to support SGTs. In this example deployment, you will edit the Finance, HR and Research policies.

Procedure 4 Configure SXP on IOS devices

Step 1: Connect to the Cisco Prime LMS server by browsing to <https://lms.cisco.local:1741>.

Step 2: Mouse over **Configuration**, and then, from the Tools section, choose **NetConfig**.

Step 3: In the NetConfig Job Browser, click **Create**.

Step 4: Select **Device Based** for the NetConfig Job Type, and then click **Go**.

Step 5: In the Device Selector, expand **All Devices**, and then select the devices where you want to enable SXP.

Step 6: In the Task Selector, expand **All Tasks**, select **Adhoc**, and then click **Next**.

Step 7: Click **Add Instance**, and then, in the new window, enter the CLI commands necessary to enable SXP.

```
cts sxp enable
cts sxp default password <password>
cts sxp default source-ip <IP-address-of-switch>
cts sxp connection peer <IP-address-of-peer> password default mode local
{speaker|listener}
```

Step 8: Click **Applicable Devices**, select the switch to which you want to apply this configuration, click **Close**, choose **Config** for the command mode, and then click **Save**.

Step 9: After returning to the Add Tasks window, click **Next**.

Step 10: Fill in a description for the job, and then click **Next**. The job is submitted for immediate deployment.

Step 11: Click **Finish**, and then when you receive a notice that the job was submitted successfully, click **OK**.

Step 12: Repeat this procedure for each IOS device where you need to configure SXP.

Procedure 5 Configure SXP on WLCs

Step 1: Navigate to the WLC console by browsing to <https://wlc1.cisco.local>.

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

Step 3: In the left pane, click **TrustSec SXP**.

Step 4: In the SXP State pull-down, select **Enabled**.

Step 5: Enter the default password. This password must match what is configured on the peer.

Step 6: Add a new peer by clicking **New**.

Step 7: Enter the IP address of the peer, and then click **Apply**. The SXP Configuration page appears.

Step 8: Click **Apply**.

The screenshot shows the Cisco ASA management console interface. The top navigation bar includes links for Save Configuration, Ping, Logout, and Refresh. The main menu on the left lists various configuration categories: AAA, RADIUS, TACACS+, LDAP, Local Net Users, MAC Filtering, Disabled Clients, User Login Policies, AP Policies, and Password Policies. The 'Security' tab is selected, and the 'SXP Configuration' page is displayed. The page shows the following configuration details:

- Total SXP Connections: 1
- SXP State: Enabled (dropdown menu)
- SXP Mode: Speaker
- Default Password: (masked with dots)
- Default Source IP: 10.5.87.10
- Retry Period: 120

Below the configuration fields is a table showing the SXP configuration details:

Peer IP Address	Source IP Address	Connection Status
10.5.87.1	10.5.87.10	Off

Buttons for 'Apply' and 'New...' are located at the top right of the configuration area.

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 at <https://DC-ASA5585X.cisco.local>, and then click **Run ASDM**.

Step 2: Navigate to **Configuration > Firewall > Identity by TrustSec**.

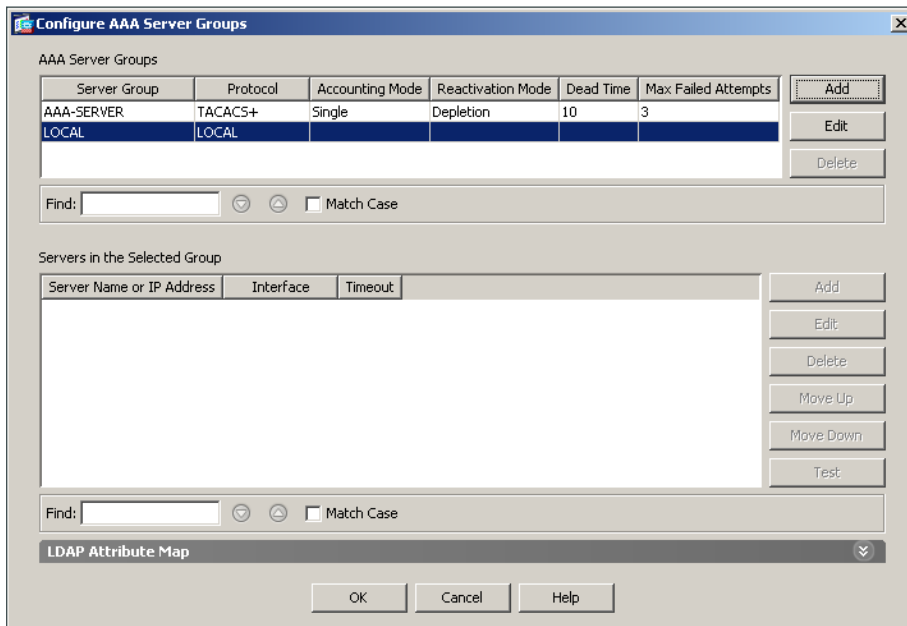
Step 3: Select **Enable SGT Exchange Protocol (SXP)**.

Step 4: For the Default Source field, 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**.

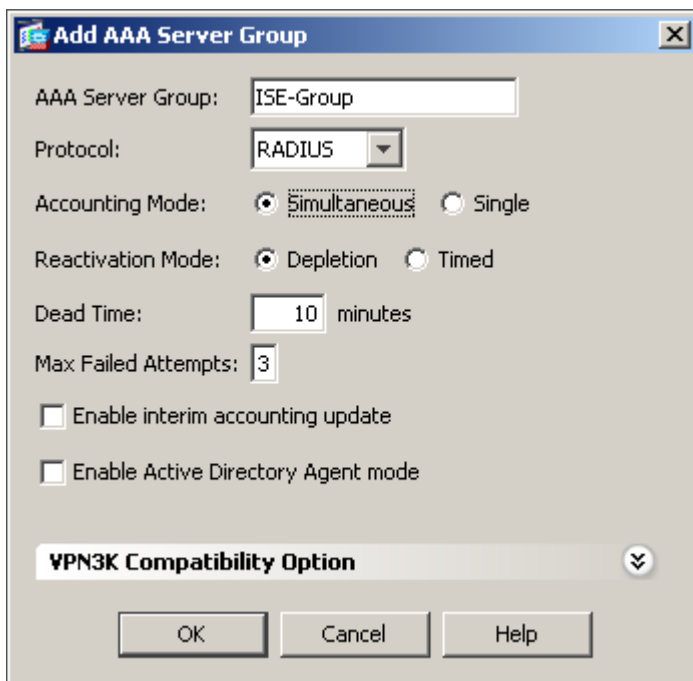


The 'Configure AAA Server Groups' window displays a table of existing server groups. The table has columns for Server Group, Protocol, Accounting Mode, Reactivation Mode, Dead Time, and Max Failed Attempts. It lists 'AAA-SERVER' (TACACS+, Single, Depletion, 10, 3) and 'LOCAL' (LOCAL, empty, empty, empty, empty). Buttons for Add, Edit, and Delete are on the right. Below the table is a 'Find' search bar with a 'Match Case' checkbox. The 'Servers in the Selected Group' section is empty, with buttons for Add, Edit, Delete, Move Up, Move Down, and Test. A second 'Find' search bar and 'Match Case' checkbox are below. At the bottom is an 'LDAP Attribute Map' dropdown and 'OK', 'Cancel', and 'Help' buttons.

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 field, enter **ISE-Group**.

Step 9: For Accounting Mode, select **Simultaneous**, and then click **OK**.

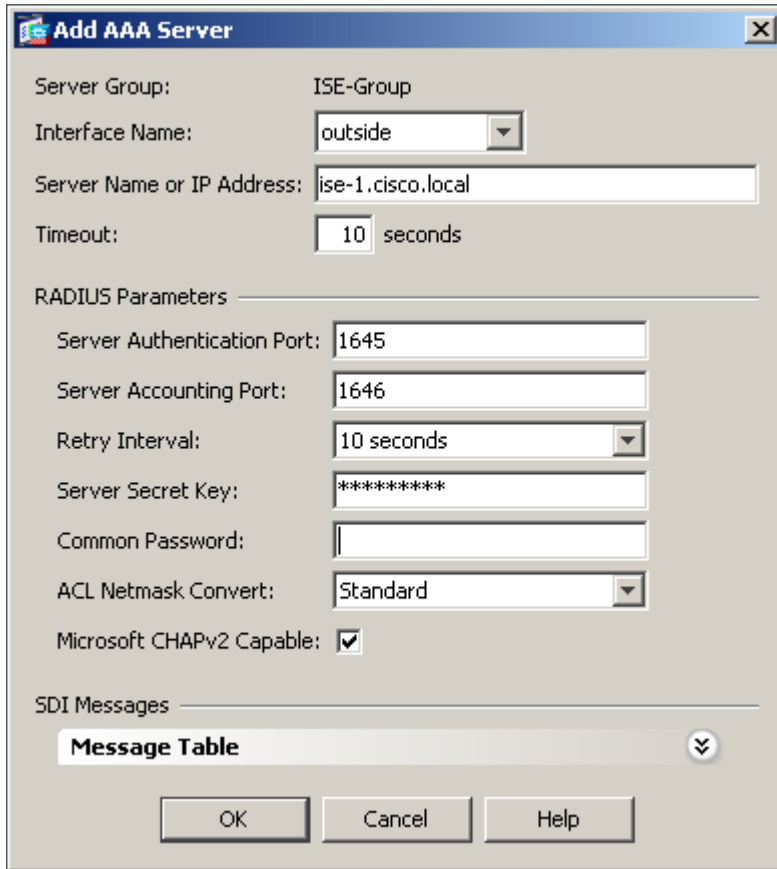


The 'Add AAA Server Group' window shows configuration fields. 'AAA Server Group' is 'ISE-Group'. 'Protocol' is 'RADIUS'. 'Accounting Mode' has 'Simultaneous' selected. 'Reactivation Mode' has 'Depletion' selected. 'Dead Time' is '10 minutes'. 'Max Failed Attempts' is '3'. There are checkboxes for 'Enable interim accounting update' and 'Enable Active Directory Agent mode'. At the bottom is a 'VPN3K Compatibility Option' dropdown and 'OK', 'Cancel', and 'Help' buttons.

Step 10: In the Selected Group section, for Servers, click **Add**.

Step 11: In the list, choose the firewall interface **outside**.

Step 12: In the RADIUS Parameters sections, enter the **Shared Secret Key**, accept the defaults for the remaining parameters, and then click **OK**.



The "Add AAA Server" dialog box is shown. It has a title bar with a close button. The fields are as follows:

- Server Group: ISE-Group
- Interface Name: outside (dropdown)
- Server Name or IP Address: ise-1.cisco.local
- Timeout: 10 seconds
- RADIUS Parameters section:
 - Server Authentication Port: 1645
 - Server Accounting Port: 1646
 - Retry Interval: 10 seconds (dropdown)
 - Server Secret Key: *****
 - Common Password: (empty)
 - ACL Netmask Convert: Standard (dropdown)
 - Microsoft CHAPv2 Capable: ☒
- SDI Messages section:
 - Message Table (dropdown)
- Buttons: OK, Cancel, Help

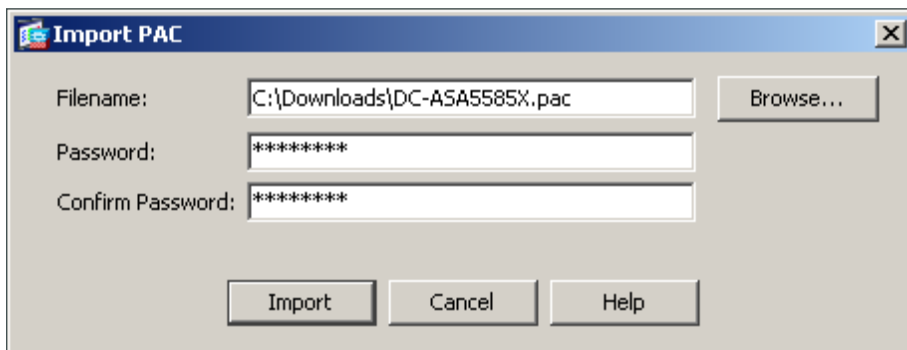
Step 13: Repeat Step 10 through Step 12 for the secondary Cisco ISE administration node, **ise-2.cisco.local**.

Step 14: Click **OK**. The Configure AAA Server Groups window closes.

Step 15: Click **Import PAC**.

Step 16: Click **Browse**, and then locate the PAC file you saved to your machine in Step 12, Procedure 2, "Add ASA as network device."

Step 17: Enter the PAC password, and then confirm it. Click **Import**.



The "Import PAC" dialog box is shown. It has a title bar with a close button. The fields are as follows:

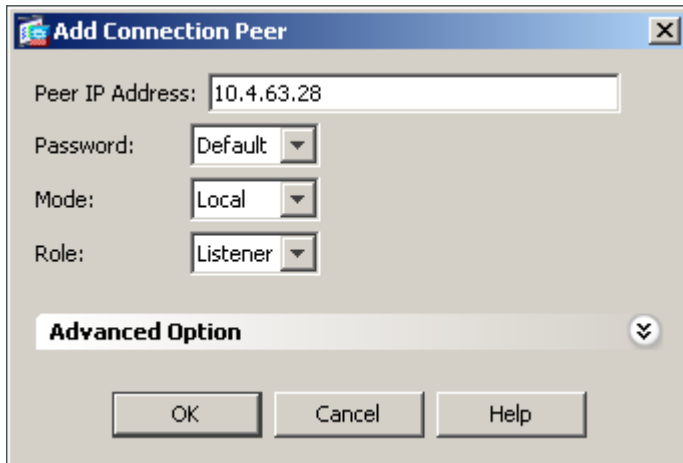
- Filename: C:\Downloads\DC-ASA5585X.pac
- Password: *****
- Confirm Password: *****
- Buttons: Import, Cancel, Help

Now you will add SXP peers to Cisco ASA.

Step 18: Click **Add**.

Step 19: Enter the IP address of the peer.

Step 20: For Password, choose **Default**, for Mode, choose **Local**, and for Role, choose **Listener**, and then click **OK**.

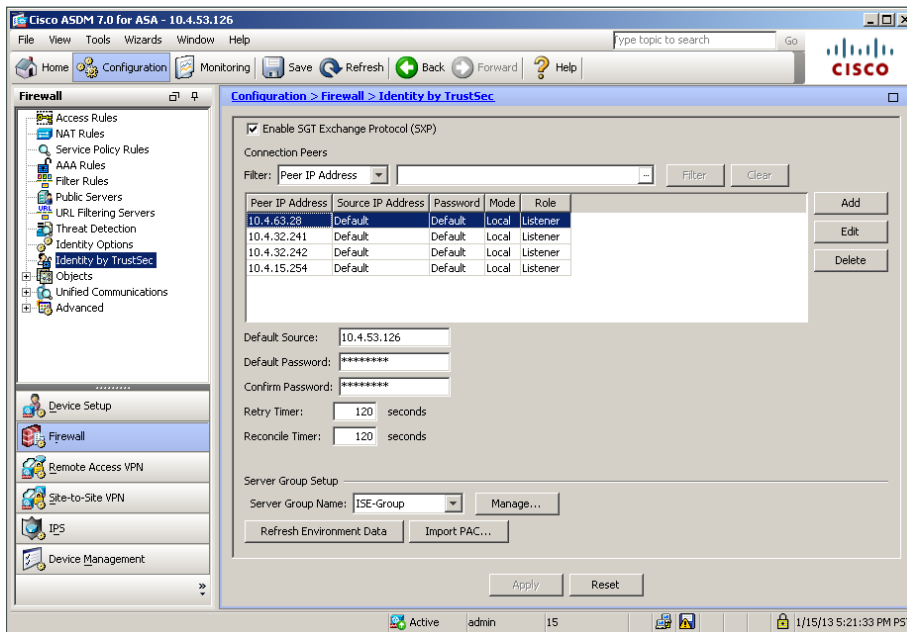


The 'Add Connection Peer' dialog box is shown. It contains the following fields and options:

- Peer IP Address: 10.4.63.28
- Password: Default (dropdown)
- Mode: Local (dropdown)
- Role: Listener (dropdown)
- Advanced Option: (toggle button, currently off)
- Buttons: OK, Cancel, Help

Step 21: Repeat Step 18 through Step 20 for each peer you need to add.

Step 22: Click **Apply**.



The Cisco ASDM 7.0 for ASA - 10.4.53.126 Configuration > Firewall > Identity by TrustSec window is shown. The 'Enable SGT Exchange Protocol (SXP)' checkbox is checked. The 'Connection Peers' table is displayed with the following data:

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

Below the table, the 'Default Source' is set to 10.4.53.126. The 'Default Password' and 'Confirm Password' fields are masked with asterisks. The 'Retry Timer' and 'Reconcile Timer' are both set to 120 seconds. The 'Server Group Setup' section shows 'Server Group Name' as ISE-Group. The 'Apply' button is highlighted.

Procedure 7 Configure firewall policy

In the [Data Center Design Guide](#), organizational servers were defined. In this procedure, you will create policy to limit access to each server based on SGTs. In this example, you will create a rule for the server for the IT group.

Step 1: In Cisco ASDM, navigate to **Configuration > Firewall > Access Rules**.

Step 2: Click **Add**.

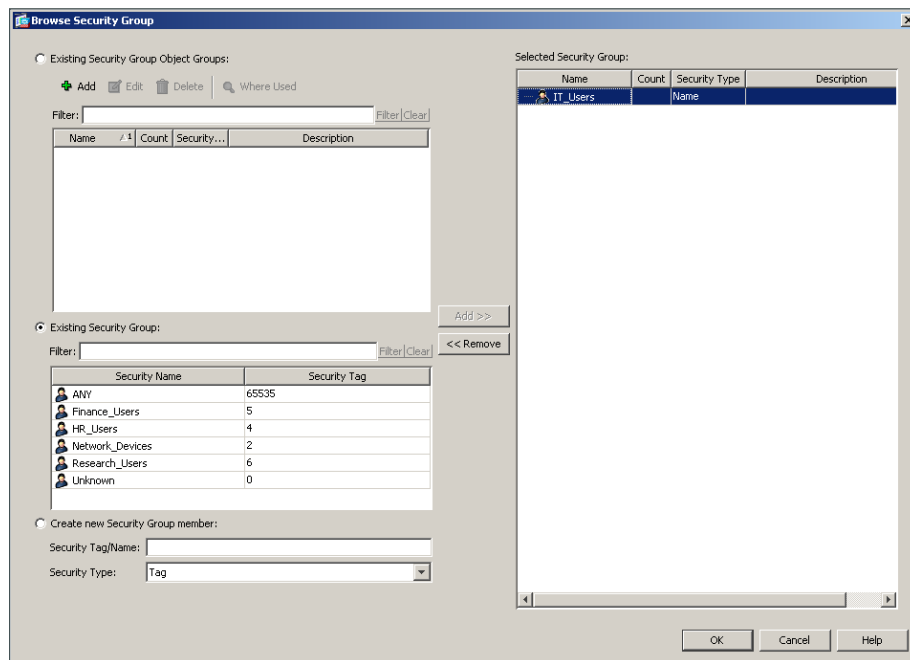
Step 3: From the Interface menu, choose **Any**.

Step 4: Select the **Permit** action.

Step 5: In the Source Criteria section, enter **any** for the Source, 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**.

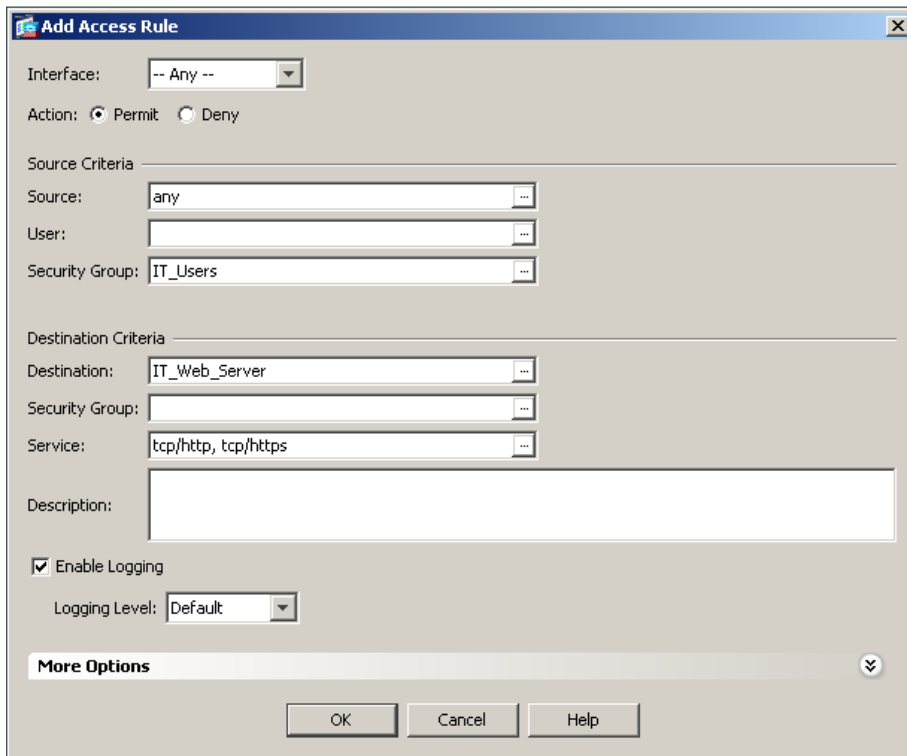


Step 8: Click **OK**. The Add Access Rule window opens.

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: For the service, enter **tcp/http, tcp/https**, and then click **OK**.



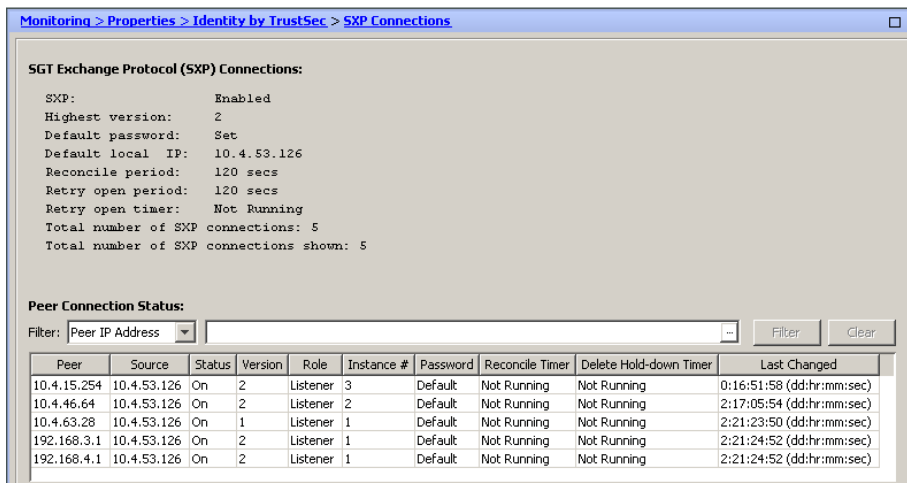
The 'Add Access Rule' dialog box is shown. It has a title bar with a close button. The 'Interface' dropdown is set to '-- Any --'. The 'Action' section has 'Permit' selected. The 'Source Criteria' section has 'Source' set to 'any', 'User' is empty, and 'Security Group' is 'IT_Users'. The 'Destination Criteria' section has 'Destination' set to 'IT_Web_Server', 'Security Group' is empty, and 'Service' is 'tcp/http, tcp/https'. The 'Description' field is empty. The 'Enable Logging' checkbox is checked, and 'Logging Level' is 'Default'. At the bottom, there is a 'More Options' button with a dropdown arrow, and 'OK', 'Cancel', and 'Help' buttons.

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 will use ASDM to verify 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.



The 'Monitoring > Properties > Identity by TrustSec > SXP Connections' window is shown. It displays the 'SGT Exchange Protocol (SXP) Connections' status and a table of 'Peer Connection Status'.

SGT Exchange Protocol (SXP) Connections:

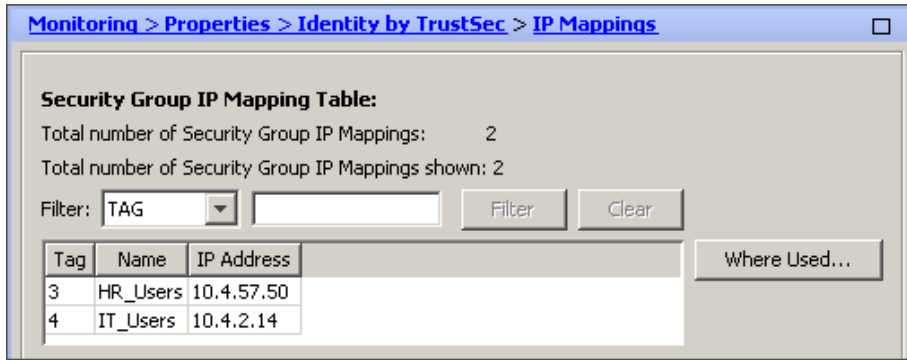
- SXP: Enabled
- Highest version: 2
- Default password: Set
- Default local IP: 10.4.53.126
- Reconcile period: 120 secs
- Retry open period: 120 secs
- Retry open timer: Not Running
- Total number of SXP connections: 5
- Total number of SXP connections shown: 5

Peer Connection Status:

Filter: Peer IP Address [] Filter Clear

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: 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.



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 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 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

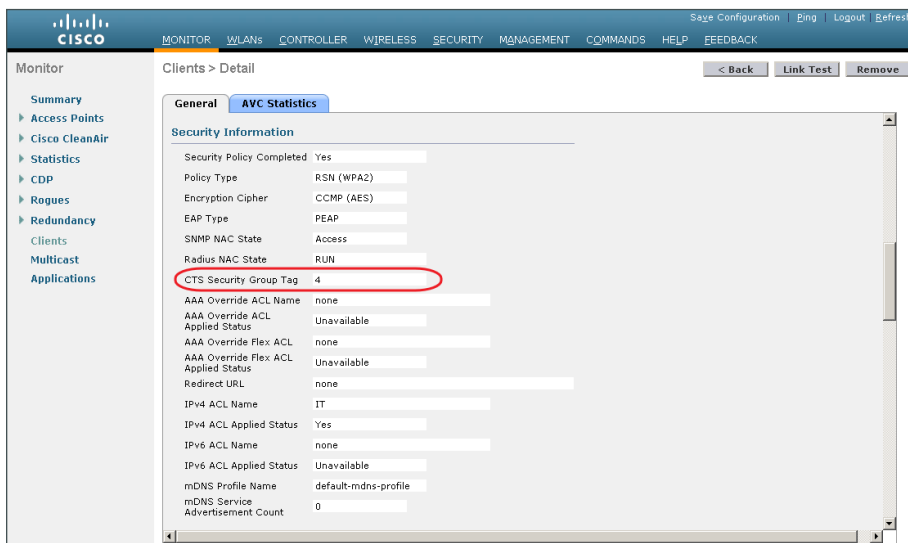
You use the GUI of the WLC to monitor the SGT assignments and SXP connections.

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.



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**.

Security 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
7. Create device-type reports

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.

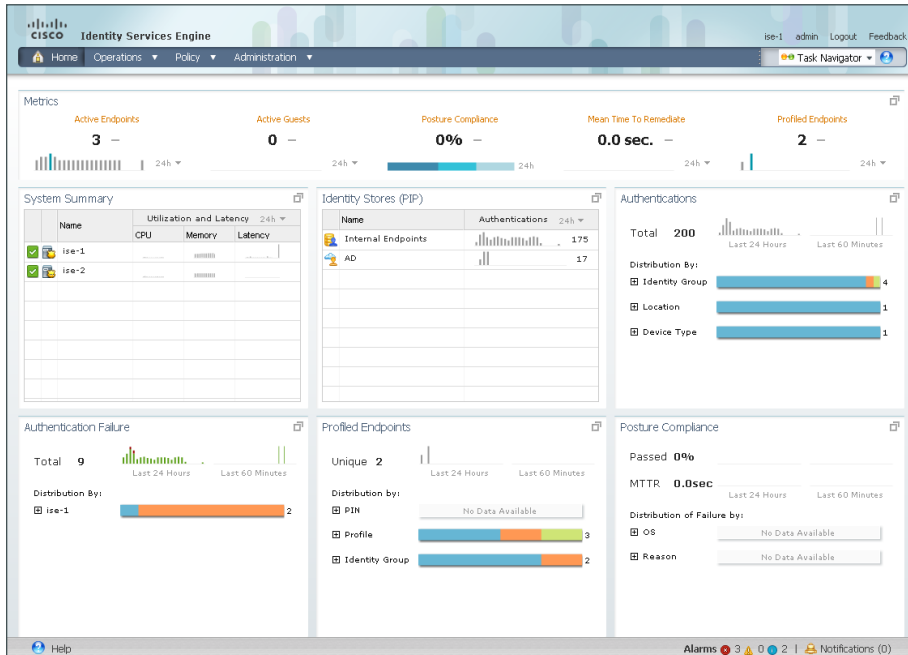
Cisco ISE is now configured to authenticate users and to profile endpoints based on RADIUS and DHCP information. The reporting capabilities of Cisco ISE allow you to determine what type of device is connecting to your network, when it connects, and where it connects from. Also, you will know who is connecting 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.



Procedure 2 Configure identity groups

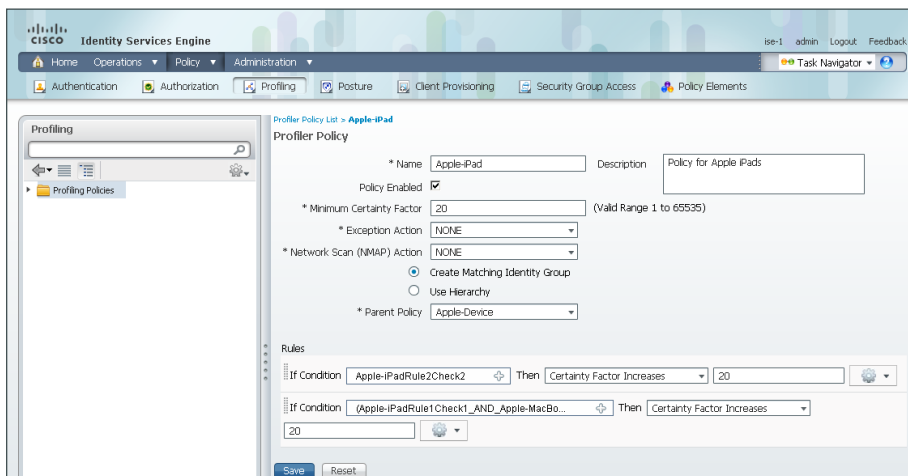
Cisco ISE has more in-depth reporting options to give more details on the devices connecting to the network. To help identify the endpoints, you can use identity groups to classify profiled endpoints and to generate reports.

The example below describes how to do this for an Apple iPad. The procedure for other types of devices is similar.

Step 1: In the menu bar, mouse over **Policy**, and then choose **Profiling**.

Step 2: Click **Apple-iPad**. This enables you to edit this policy.

Step 3: Select **Create Matching Identity Group**, and then click **Save**.



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: Connect to <https://ise-1.cisco.local>.

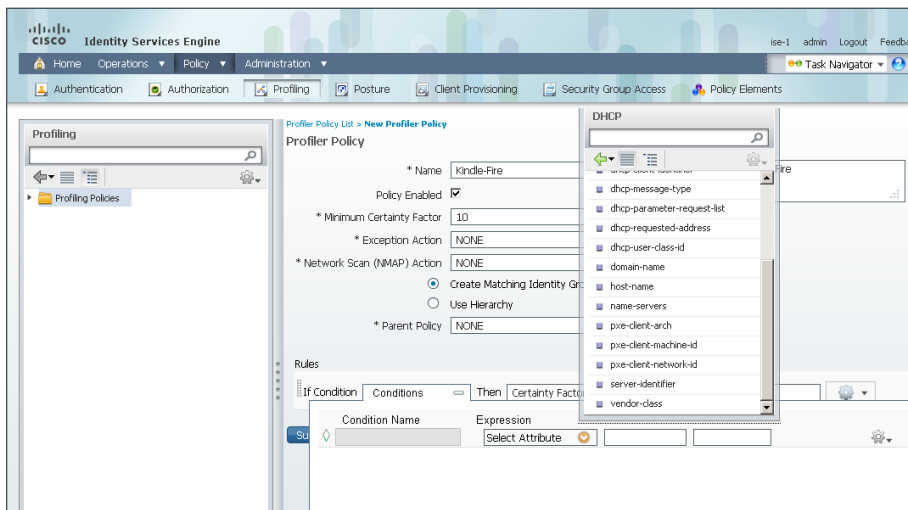
Step 2: Mouse over **Policy**, and then, from the drop-down menu, choose **Profiling**.

Step 3: Click **Add**.

Step 4: Give the policy the name **Kindle-Fire** and a description.

Step 5: In the rules section, next to Conditions, click the **+** symbol, and then click **Create New Condition (Advance Option)**.

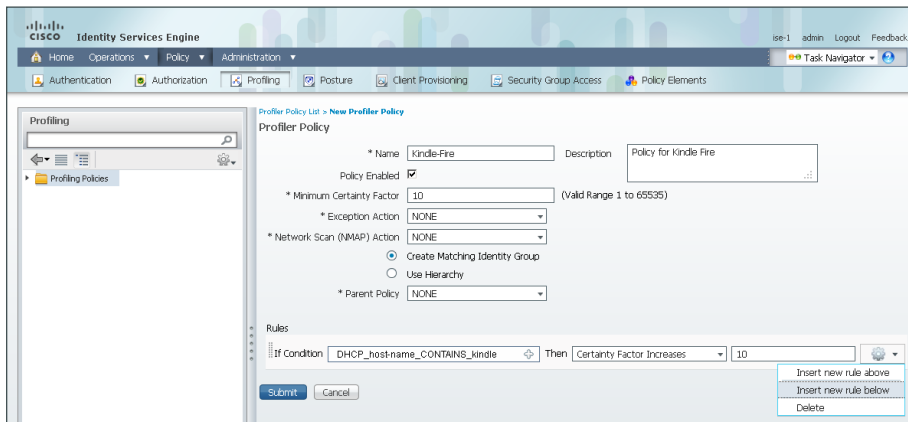
Step 6: In the **Expression** list, next to DHCP, click the **>** symbol, and then choose **host-name**.



Step 7: In the second list, choose **CONTAINS**, and then, in the final box, enter **kindle**.

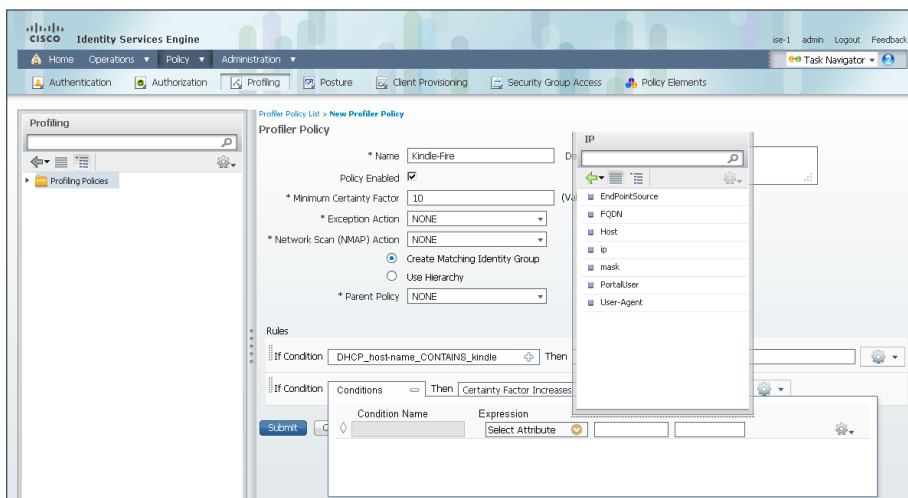
Step 8: Choose **Certainty Factor Increases**, and then set the value to **10**.

Step 9: Click the gear icon at the end of the rule, and then select **Insert new rule below**.



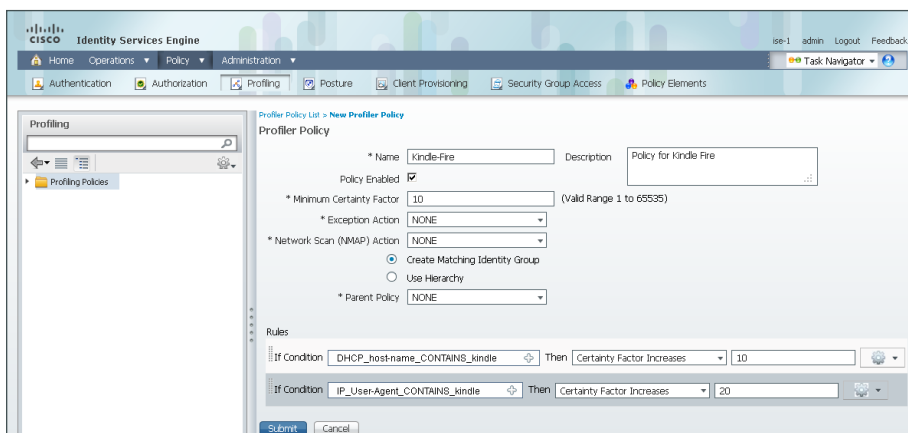
Step 10: Next to Conditions, click the + symbol, and then click **Create New Condition (Advance Option)**.

Step 11: In the **Expression** list, next to IP, click the > symbol, and then choose **User-Agent**.



Step 12: In the second list, choose **CONTAINS**, and then, in the final box, enter **kindle**.

Step 13: Choose **Certainty Factor Increases**, set the value to **20**, and then click **Submit**.



Procedure 4 Examining the authentication log

Step 1: On the menu bar, mouse over **Operations**, and then choose **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.

The screenshot displays the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes the Cisco logo and the text "Identity Services Engine". A "Launch Interactive Viewer" button is visible in the top right corner. The main content area is titled "RADIUS Authentication Details" and shows a single record for "AAA Protocol > RADIUS Authentication Detail". The record details include: "RADIUS Audit Session ID : 0a05570a0000039512b337", "AAA session ID : ise-1/144790336/4152", and "Date : February 28, 2013". Below this, it states "Generated on February 28, 2013 11:44:24 AM PST". An "Actions" menu is present with links: "Troubleshoot Authentication", "View Diagnostic Messages", "Audit Network Device Configuration", "View Network Device Configuration", and "View Server Configuration Changes". At the bottom, the "Authentication Summary" section provides a detailed log of the authentication process, including the logged-in time, RADIUS status (Authentication succeeded), NAS failure, username (pat.jones), MAC/IP address (40:30:04:24:EE:A9), network device (DefaultNetworkDevice : 10.5.87.10), allowed protocol (Default Network Access), identity store, authorization profiles (Finance_Users), SGA security group (Finance_Users), and authentication protocol (EAP-TLS).

Authentication Summary	
Logged At:	February 28, 2013 11:42:52 820 AM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	pat.jones
MAC/IP Address:	40:30:04:24:EE:A9
Network Device:	DefaultNetworkDevice : 10.5.87.10 :
Allowed Protocol:	Default Network Access
Identity Store:	
Authorization Profiles:	Finance_Users
SGA Security Group:	Finance_Users
Authentication Protocol:	EAP-TLS

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.

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.

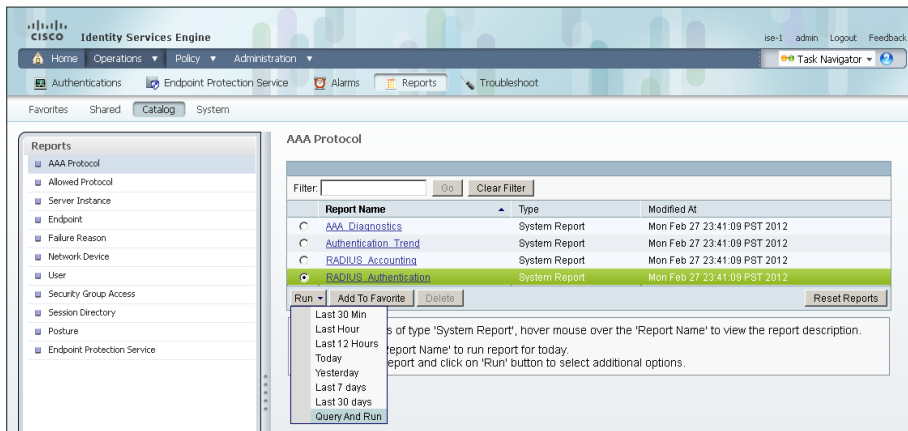
Step 1: On the menu bar, mouse over **Operations**, and then, in the Reports section, choose **Catalog**.

Step 2: In the left pane, select **AAA Protocol**.

Step 3: Select **RADIUS Authentication**.

Step 4: Click **Run**. Different time ranges for producing the default report are displayed.

Step 5: If you wish to use one of the default time ranges, choose that time range.



If you wish to select a time range that is not listed, choose **Query and Run**. All the parameters available for the report display.

Step 6: After choosing the parameters you want, click **Run** to generate the report.

Figure 2 - RADIUS report parameters

Run Report

User:

Select

Clear

MAC Address:

Select

Clear

Identity Group:

Select

Clear

Device Name:

Select

Clear

Device IP:

Select

Clear

Device Group:

Select

Clear

Allowed Protocol:

Select

Clear

Identity Store:

Select

Clear

Server:

Select

Clear

Failure Reason:

Select

Clear

SGASGT:

Select

Clear

Show only SGASGT Assignments:

☐

Include SGASGT Environment:

☐

Radius Audit Session ID:

Clear

Session ID:

Clear

Authentication Status:

Pass Or Fail

Authentication Method:

Select

Clear

Time Range:

Today

Start Date:

(mm/dd/yyyy)

End Date:

(mm/dd/yyyy)

Run

Cancel

Procedure 6 Identify endpoints

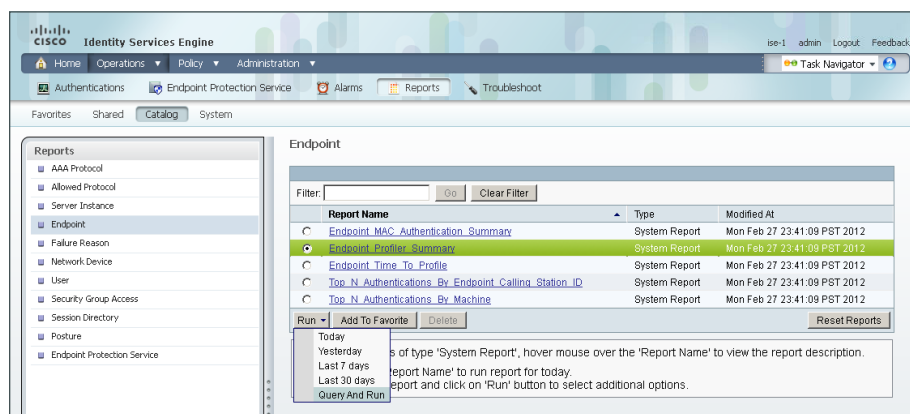
Using information gleaned from the RADIUS and DHCP requests, Cisco ISE can identify what types of devices are connecting to the network. This can assist in determining the network security policy based on the type of device that is in use.

Step 1: On the menu bar, mouse over **Operations**, and then, in the Reports section, choose **Catalog**.

Step 2: In the left pane, click **Endpoint**. This displays the available endpoint reports.

Step 3: Select **Endpoint Profiler Summary**, and then click **Run**.

Step 4: Select the desired time period to run the report.



Step 5: Once the report is generated, you can view the details of a profiled endpoint by clicking the magnifying glass icon.

The details given in the summary section are the MAC address, the endpoint policy, and the identity group for the endpoint. Additional details, such as IP address and network access devices, are available in the Endpoint Details section. For wireless and remote-access VPN endpoints that authenticated with RADIUS, the user name is also listed.

Figure 3 - Endpoint profile summary

Profiler Summary		Profiler History	
Logged At :	Feb 28, 2013 11:39 AM	Day	Endpoint policy
Server :	ise-1	Feb 28, 2013 11:39 AM	Apple-Device
Event :	Profiler is triggering Change Of Authorization Request	Feb 28, 2013 11:39 AM	Apple-iPad
Endpoint MAC Address :	40:30:04:24:EE:A9	Feb 27, 2013 1:39 PM	Apple-Device
Endpoint Policy :	Apple-iPad	Feb 27, 2013 1:39 PM	Apple-iPad
Certainty Metric :			
Endpoint Matched Policy :	Apple-iPad		
Identity Group :	Apple-iPad		

Figure 4 - Endpoint Details

Endpoint > Endpoint Profiler Detail	
Generated on February 28, 2013 5:01:30 PM PST	
Endpoint Session time : 383.67Seconds	
Endpoint Details	
Endpoint Static Assignment :	
Endpoint Source :	
Endpoint OUI :	Apple, Inc.
Endpoint Host Name :	
Endpoint Subnet :	
Endpoint NAD Address :	10.5.87.10
Endpoint VLAN :	
Endpoint FQDN :	
Endpoint Nameserver :	
Endpoint Property :	CPMSessionID=0a05570a00000038512fb262 Event-Timestamp=1362080368 NetworkDeviceGroups=Device Type#All Device Types Location#All Locations cisco-av-pair=audit-session-id=0a05570a00000038512fb262 dhcp-option=host-name=SBA-iPad2 nas-update=true Calling-Station-ID=40-30-04-24-ee-a9 DestinationPort=1812 AcctSessionID=ise-1/144790336/4148 Device Type=Device Type#All Device Types Service-Type=Framed NAS-Identifier=RS208-WLC2504 TimeToProfile=9 LastNmapScanTime=0 Acct-Delay-Time=0 AuthenticationMethod=MSCHAPV2 EapAuthentication=EAP-MSCHAPV2 NetworkDeviceName=DefaultNetworkDevice Tunnel-Type=(tag=0) VLAN NAS-Port-Type=Wireless - IEEE 802.11 RegistrationTimeStamps=0 Acct-Session-Id=512fb269/40-30-04-24-ee-a9/27 PostureAssessmentStatus=NotApplicable IdentityGroupID=1104cb0-237c-11e2-a044-005056a25d6d Total Certainty Factor=30 User-Name=pat.jones AuthenticationIdentityStore=AD1 MatchedPolicyID=70024e80-be86-11e1-ba69-0050568e002b DestinationIPAddress=10.4.48.41 NAS-Port=13 Class=CACS:0a05570a00000038512fb262:ise-1/144790336/4148 Acct-Session-Time=1 ADDomain=cisco.local NmapScanCount=0 EndPointMACAddress=40-30-04-24-EE-A9 Tunnel-Private-Group-ID=(tag=0) 104 ServiceSelectionMatchedRule=Wireless-Dot1X PortalUsers RequestLatency=2 Tunnel-Medium-Type=(tag=0) 802 EapTunnel=PEAP AuthState=Authenticated Airespace-Wlan-Id=1 Acct-Input-Octets=0 PostureStatus=Unknown Acct-Authentic=RADIUS host-name=SBA-iPad2 FirstCollector=1362080372532 EndPointPolicyID=70024e80-be86-11e1-ba69-0050568e002b SelectedAccessService=Default Network Access Acct-Status-Type=Interim-Update attribute-52=00:00:00:00 AuthorizationPolicyMatchedRule=Finance_SGT IdentityPolicyMatchedRule=Default MessageCode=3002 attribute-53=00:00:00:00 Acct-Input-Packets=0 Acct-Output-Octets=0 DeviceRegistrationStatus=notRegistered SelectedAuthorizationProfiles=Finance_Users Framed-MTU=1300 IdentityAccessRestricted=false SelectedAuthenticationIdentityStores=AD1 ExternalGroup=cisco.local/users/finance\ cisco.local/users/pos-users\ cisco.local/users/byod provisioning\ cisco.local/users/domain users\ cisco.local/built-in/users Response=[User-Name=pat.jones; State=ReauthSession:0a05570a00000038512fb262; Class=CACS:0a05570a00000038512fb262:ise-1/144790336/4148; Termination-Action=RADIUS-Request; cisco- av-pair=cts security-group-tag=0005-0; MS-MPPE: Send-Key=56:3c:a1:08:52:72:61:37:a3:4a:b1:f4:72:30:a9:41:f4:56:e8:d3:6c:ad:29:d1:f4:f1:67:05:37:b5:1b:bf; MS-MPPE: Recv-Key=e6:c9:e1:08:1a:ca:86:0f:1d:ae:c4:0b:59:8b:02:2f:5a:50:8a:34:4a:88:74:38:d1:96:82:ae:08:23:27:0c;] Location=Location#All Locations PolicyVersion=19 Device IP Address=10.5.87.10 State=37CPMSessionID=0a05570a00000038512fb262\;30SessionID=ise-1/144790336/4148\ NmapSubnetScanID=0 Acct-Output-Packets=0 Called-Station-ID=3c-ce-73-d9-9c-20

Procedure 7 Create device-type reports

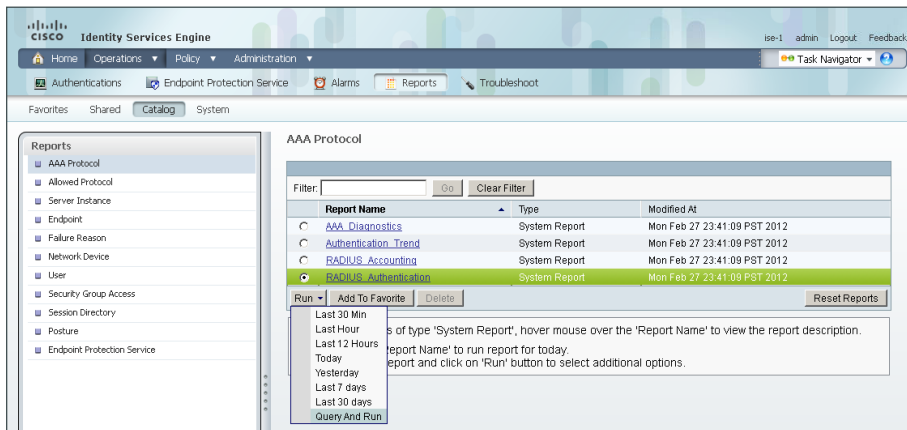
You can create reports to identify specific devices based on the identity groups configured previously. This example uses the group created to identify Apple iPads.

Step 1: On the menu bar, mouse over **Operations**, and then, in the Reports section, choose **Catalog**.

Step 2: In the left pane, click **AAA Protocol**.

Step 3: Select **RADIUS Authentication**.

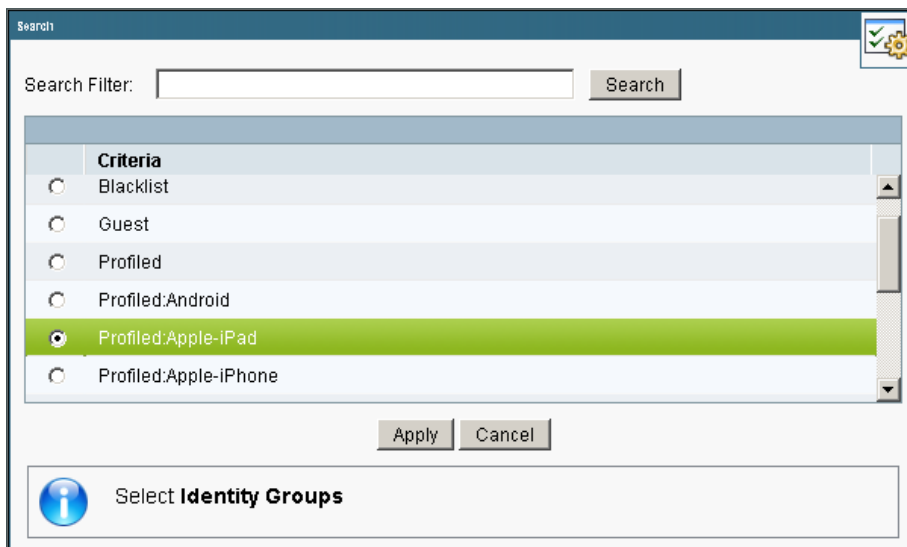
Step 4: Click **Run**, and then choose **Query and Run**.



Step 5: For the identity group you want to query, next the Identity Group field, click **Select**. A search window appears.

Step 6: Leave the search field empty, and then click **Search**. The search returns all groups.

Step 7: Select the group **Profiled:AppleiPad**, and then click **Apply**.



Step 8: Select a time range for the report, and then click **Run**. The report generates.

Figure 5 – Sample report

AAA Protocol > RADIUS Authentication

Identity Group : Profiled Apple-iPad

Authentication Status : Pass or Fail

Date : January 29, 2013 - February 27, 2013 ([Last 30 Minutes](#) | [Last Hour](#) | [Last 12 Hours](#) | [Today](#) | [Yesterday](#) | [Last 7 Days](#) | [Last 30 Days](#))

Generated on February 28, 2013 5:24:43 PM PST

✓=Pass

✗=Fail

=Click for details

=Mouse over item for additional information

Logged At	RADIUS Status	NAS Failure	Details	Event	Username	MAC/IP Address	Allowed Protocol	Service Type	Authentication Protocol
Feb 27, 13:39:24.237 PM	✓			Authentication succeeded	pat.jones	40.30.04.24:EE:A8	Default Network Access	Framed	PEAP (EAP-MSCHAPv2)
Feb 27, 13:39:17.342 PM	✓			Authentication succeeded	pat.jones	40.30.04.24:EE:A8	Default Network Access	Framed	PEAP (EAP-MSCHAPv2)

Appendix A: Product List

Network Management

Functional Area	Product Description	Part Numbers	Software
Identity Management	Cisco Identity Services Engine Virtual Appliance	ISE-VM-K9=	1.1.2.145
	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 3-year License for 2500 Endpoints	L-ISE-ADV3Y-2500=	
	Cisco ISE Advanced 3-year License for 3500 Endpoints	L-ISE-ADV3Y-3500=	
	Cisco ISE Advanced 3-year License for 5000 Endpoints	L-ISE-ADV3Y-5K=	
	Cisco ISE Advanced 3-year License for 10,000 Endpoints	L-ISE-ADV3Y-10K=	
Network Management	Cisco Prime Infrastructure 1.1	R-PI-1.1-K9	4.2
	Prime Infrastructure 1.1 Software – 50 Device Base License	R-PI-1.1-50-K9	
	Prime Infrastructure 1.1 Software – 100 Device Base License	R-PI-1.1-100-K9	
	Prime Infrastructure 1.1 Software – 500 Device Base License	R-PI-1.1-500-K9	
	Prime Infrastructure 1.1 Software – 1K Device Base License	R-PI-1.1-1K-K9	
	Prime Infrastructure 1.1 Software – 2.5K Device Base License	R-PI-1.1-2.5K-K9	
	Prime Infrastructure 1.1 Software – 5K Device Base License	R-PI-1.1-5K-K9	

LAN Access Layer

Functional Area	Product Description	Part Numbers	Software
Modular Access Layer Switch	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.4.0.SG(15.1-2SG) IP Base license
	Cisco Catalyst 4500 E-Series Supervisor Engine 7L-E	WS-X45-SUP7L-E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+ ports	WS-X4648-RJ45V+E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+,UPoE ports	WS-X4748-UPOE+E	
Stackable Access Layer Switch	Cisco Catalyst 3850 Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3850-48F	3.2.1SE(15.0-1EX1) IP Base license
	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 3750-X Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-48PF-S	15.0(2)SE2 IP Base license
	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	

Functional Area	Product Description	Part Numbers	Software
Standalone Access Layer Switch	Cisco Catalyst 3560-X Series Standalone 48 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-48PF-S	15.0(2)SE2 IP Base license
	Cisco Catalyst 3560-X Series Standalone 24 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-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	
Stackable Access Layer Switch	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-48FPD-L	15.0(2)SE2 LAN Base license
	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-48FPS-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-24PD-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-24PS-L	
	Cisco Catalyst 2960-S Series Flexstack Stack Module	C2960S-STACK	

Wireless LAN Controllers

Functional Area	Product Description	Part Numbers	Software
On Site, Remote Site, or Guest Controller	Cisco 5500 Series Wireless Controller for up to 500 Cisco access points	AIR-CT5508-500-K9	7.4.100.0
	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	7.4.100.0
	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 3600 Series Access Point Dual Band 802.11a/g/n and CleanAir with Internal Antennas	AIR-CAP3602I-x-K9	7.4.100.0
	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-10 and IPS SSP-10 bundle	ASA5585-S10P10XK9	ASA 9.0(1) IPS 7.1(7) 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-40 and IPS SSP-40 bundle	ASA5585-S40P40-K9	

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.

© 2013 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)