Newer Cisco SBA Guides Available

This guide is part of an older series of Cisco Smart Business Architecture designs. To access the latest Cisco SBA Guides, go to http://www.cisco.com/go/sba

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

BYOD—Identity and Authentication Deployment Guide

SMART BUSINESS ARCHITECTURE

August 2012 Series

Preface

Who Should Read This Guide

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

Release Series

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

The Release Notes for a series provides a summary of additions and changes made in the series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

month year Series

For example, the series of guides that we released in August 2012 are the "August 2012 Series".

You can find the most recent series of SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

How to Read Commands

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). 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 shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

```
Router# enable
```

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

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100
100 100 100
```

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 SBA feedback form.

If you would like to be notified when new comments are posted, an RSS feed is available from the SBA customer and partner pages.

Table of Contents

What's In This SBA Guide

Cisco SBA Solutions

Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.

Cisco SBA Solutions are designs for specific problems found within the most common technology trends. Often, Cisco SBA addresses more than one use case per solution because customers adopt new trends differently and deploy new technology based upon their needs.

Route to Success

To ensure your success when implementing the designs in this guide, you should first read any guides that this guide depends upon—shown to the left of this guide on the route below. As you read this guide, specific prerequisites are cited where they are applicable.

About This Guide

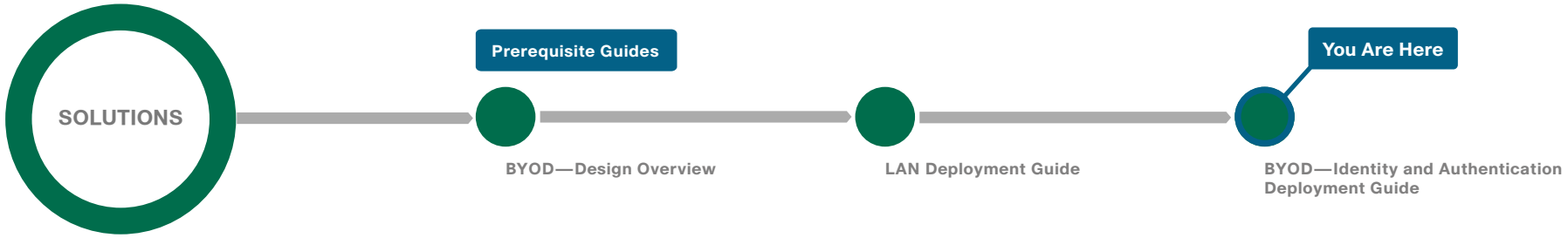
This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- **Business Overview**—Describes the business use case for the design. Business decision makers may find this section especially useful.
- **Technology Overview**—Describes the technical design for the business use case, including an introduction to the Cisco products that make up the design. Technical decision makers can use this section to understand how the design works.
- **Deployment Details**—Provides step-by-step instructions for deploying and configuring the design. Systems engineers can use this section to get the design up and running quickly and reliably.

You can find the most recent series of Cisco SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel



Introduction

Note

This guide is based on the *Cisco SBA—Borderless Networks LAN and Wireless LAN 802.1X Deployment Guide*. The goal of this guide is to show you how a BYOD business problem can be solved by using Cisco Smart Business Architecture. Cisco has previously developed solutions to solve issues that are similar to the various BYOD business problems. Cisco SBA uses 802.1X to solve the BYOD problem of identifying, authenticating, and authorizing devices.

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.

Other Cisco SBA Solutions guides addressing BYOD business problems include:

- *BYOD—Internal Corporate Access Deployment Guide*
- *BYOD—Advanced Guest Wireless Deployment Guide*
- *BYOD—Remote Mobile Access Deployment Guide*

Business Overview

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 nontraditional 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.

Technology 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.

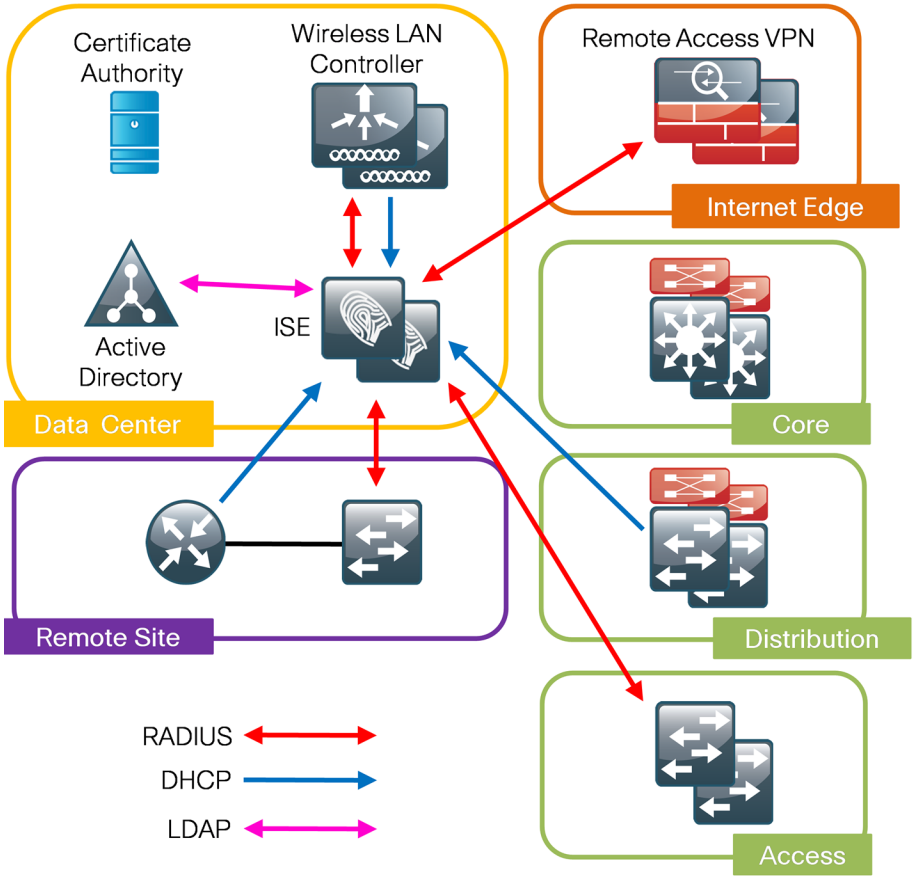
This deployment uses Cisco ISE as the authentication, authorization, and accounting server for the wired and wireless networks using RADIUS. Cisco ISE acts as a proxy to the existing Active Directory (AD) services to maintain a centralized identity store for all network services.

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 only implementing 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 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 Cisco SBA



Notes

Deployment Details

The deployment described here bases all IP addressing off of the *Cisco SBA—Borderless Networks LAN Deployment 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

Process

Deploying Cisco Identity Services Engine

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

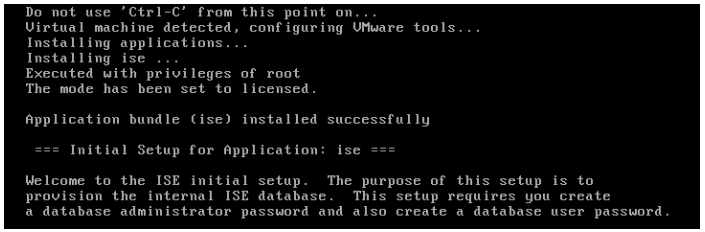
Time zone abbreviations can be found in the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1.x*: http://www.cisco.com/en/US/docs/security/ise/1.1/cli_ref_guide/ise_cli_app_a.html#wp1571855

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.



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 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 checking 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**.

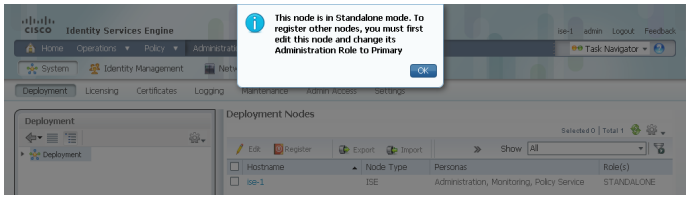
Step 10: Repeat this procedure for the remaining engines, ise-3.cisco.local and ise-4.cisco.local.

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.

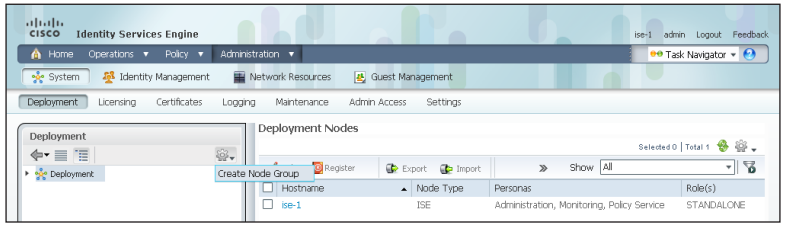
Step 1: Connect to http://ise-1.cisco.local.

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**.

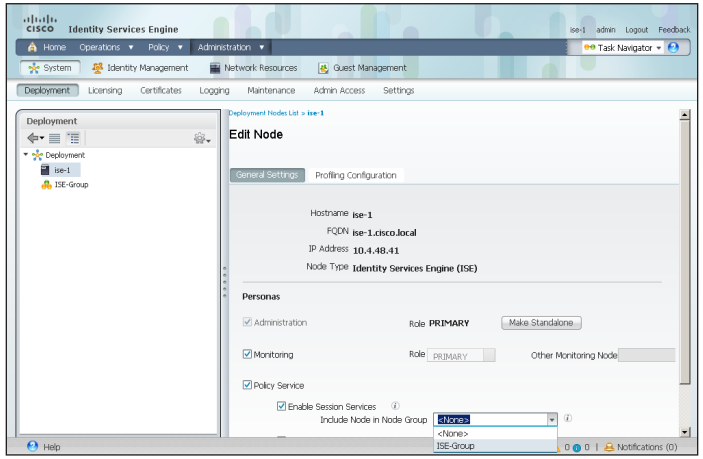
Step 5: A pop-up window lets you know the group was created successfully. Click **OK**.

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.

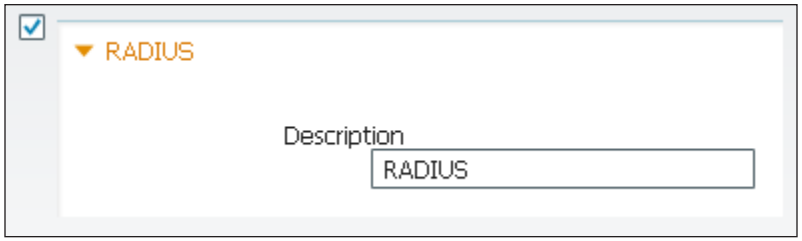
Step 8: On the General Settings tab, in the Personas section, next to the Administration Role, click **Make Primary**.

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



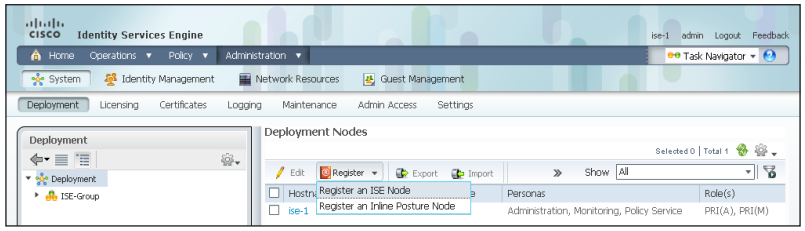
Next, you'll configure which methods are used to profile network endpoints.

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



Step 11: In the Edit Node window, click **Deployment Nodes List**. The Deployment Nodes window appears.

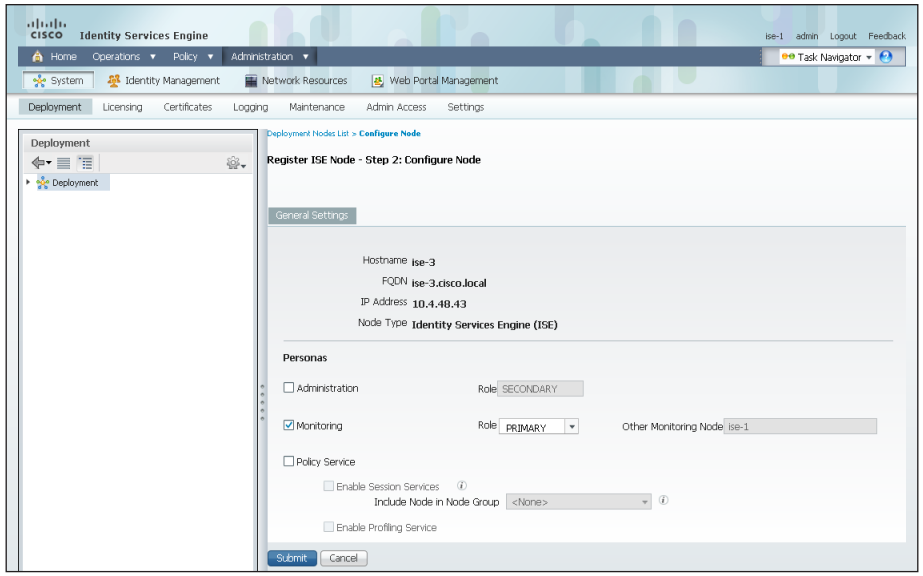
Step 12: Click **Register,** and then choose **Register an ISE Node**.



Step 13: 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**.

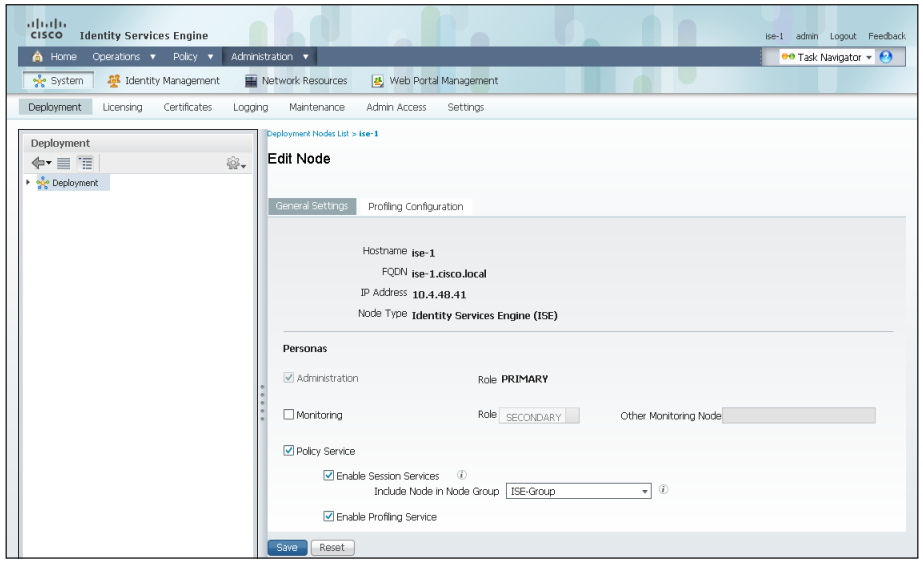
Step 14: Select **Monitoring**, and then in the **Role** list, choose **Primary**. Make sure **Administration** and **Policy Service** are not selected.

Step 15: Click **Submit**. The node registers, and a pop-up window displays letting you know that the process was successful. Click **OK**.



Step 16: In the Deployment Node window, click **ise-1**.

Step 17: 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.



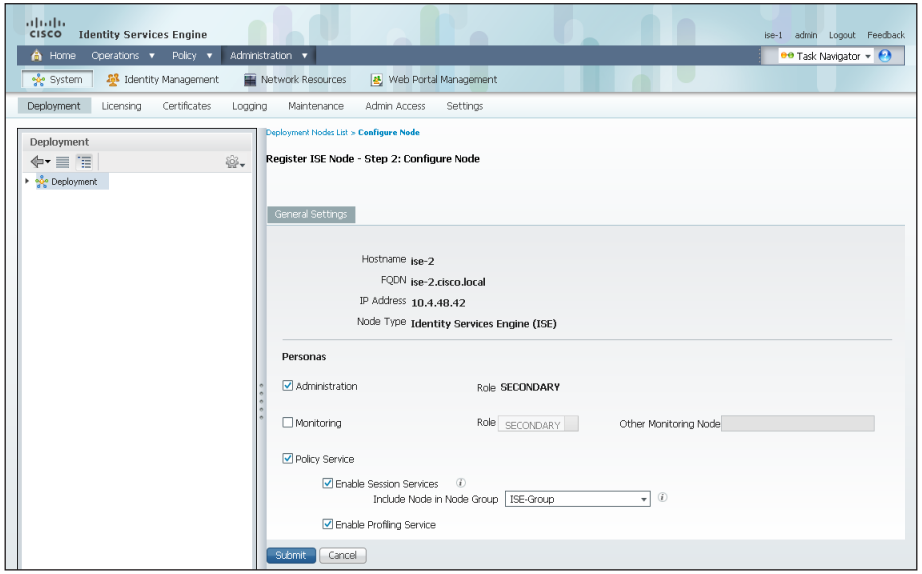
Step 18: Log in to the console, and then in the **Administration** menu, in the System section, choose **Deployment**.

Step 19: In the Deployment Node window, click **Register**, and then choose **Register an ISE Node**.

Step 20: 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 21: Select **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**.

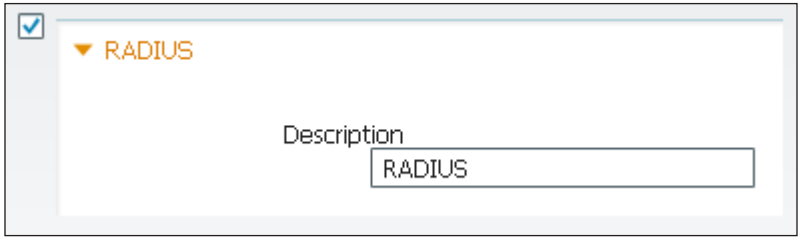
Step 22: Click **Submit**. The node registers, and a pop-up window displays letting you know that the process was successful. Click **OK**.



Step 23: 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**, use the default parameters, and then click **Save**.



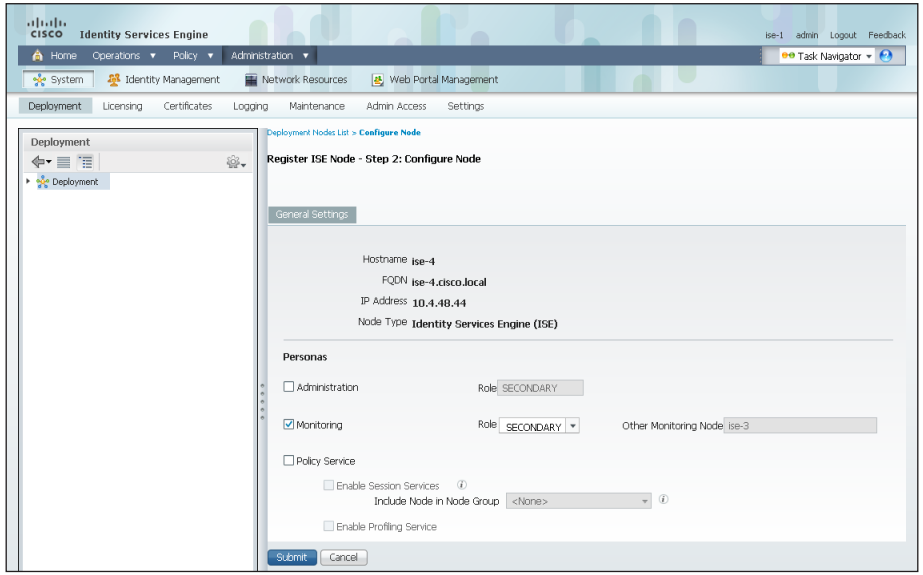
Step 26: In the Edit Node window, click **Deployment Nodes List**. The Deployment Nodes window appears.

Step 27: In the Deployment Nodes window, click **Register**, and then choose **Register an ISE Node**.

Step 28: 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 29: Select **Monitoring**, and then in the **Role** list, choose **Secondary**. Make sure **Administration** and **Policy Service** are not selected.

Step 30: 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.

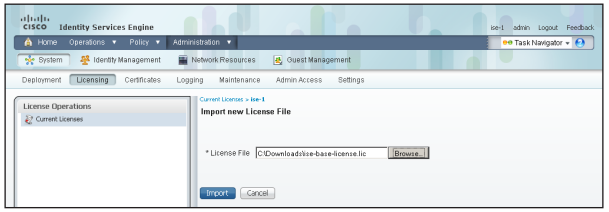
Step 1: Mouse over **Administration**, and then, from the System section of the menu, choose **Licensing**.

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**.



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**.

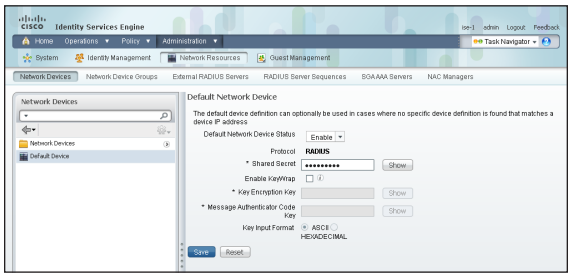
Step 2: In the left pane, click **Default Device**.

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 have to 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.

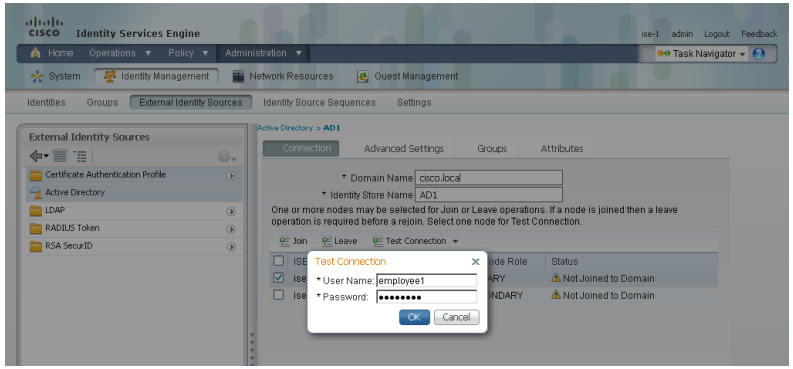
Step 1: Mouse over **Administration**, and then, from the Identity Management section of the menu, choose **External Identity Sources**.

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**.

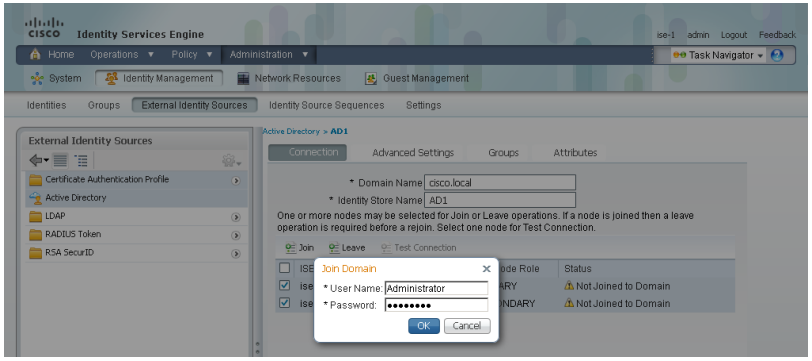
Step 5: Enter the credentials for a domain user, and then click **OK**.



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.

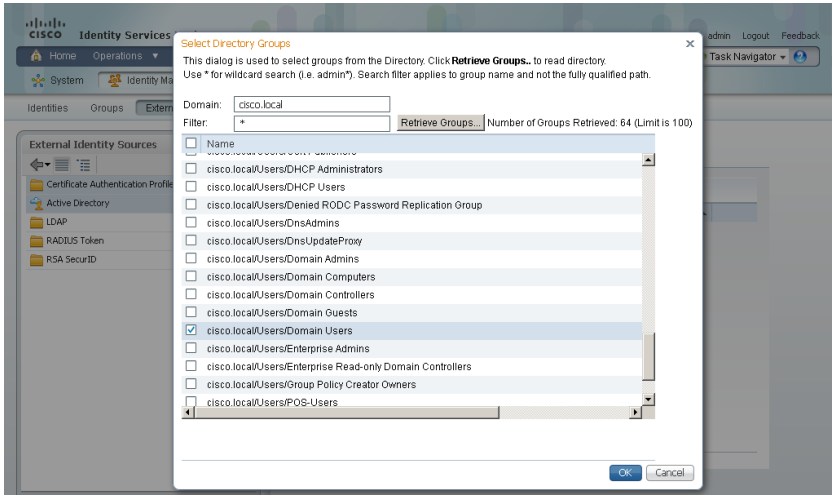


Next, you select which groups from AD that Cisco ISE will use for authentication.

Step 9: Click the Groups tab, click **Add**, and then click **Select Groups from Directory**.

Step 10: 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 11: 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**.



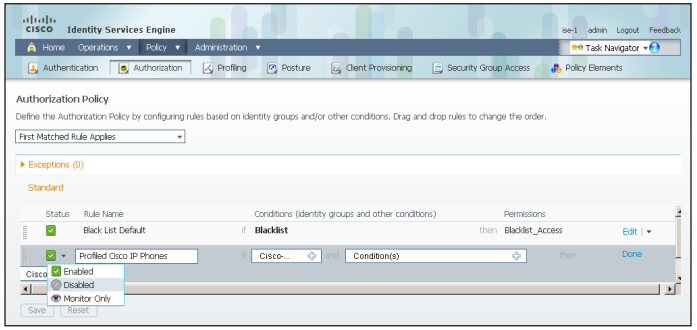
Step 12: Click **Save Configuration**.

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

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.

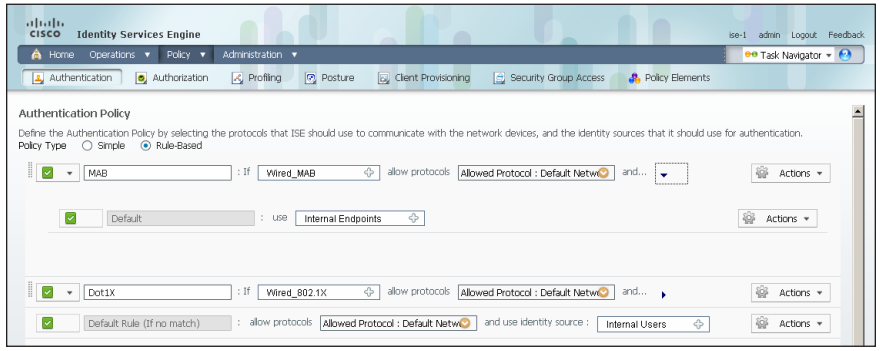
Procedure 1 Configure MAC Authentication Bypass

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. MAB will be configured to allow any MAC address to authenticate.

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: 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.

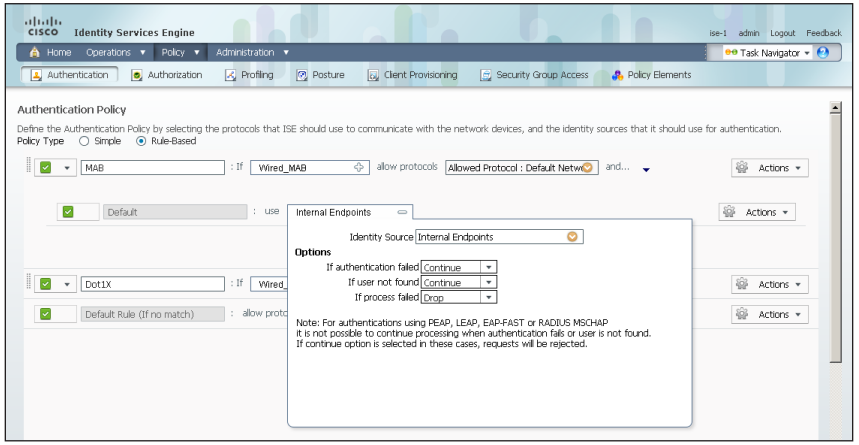


Next, you change the options on the Internal Users database, which is used for profiling.

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

Step 4: n 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**.

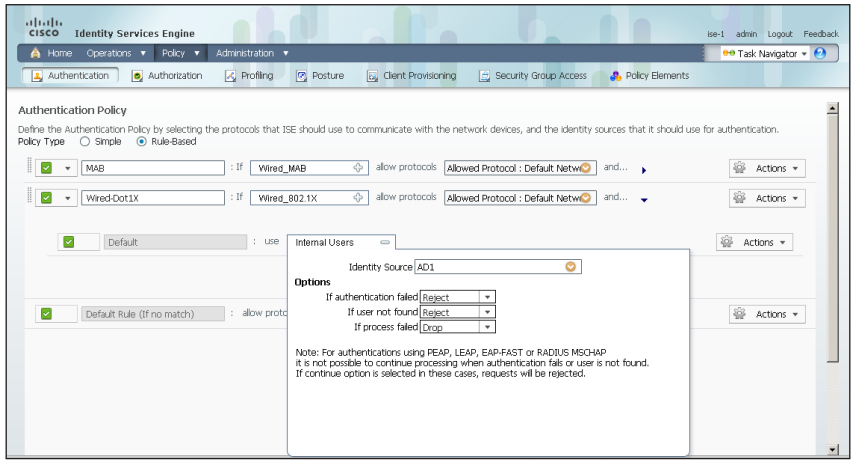
Step 2: To differentiate this from a wireless 802.1X rule, rename the rule Wired-Dot1X.

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.

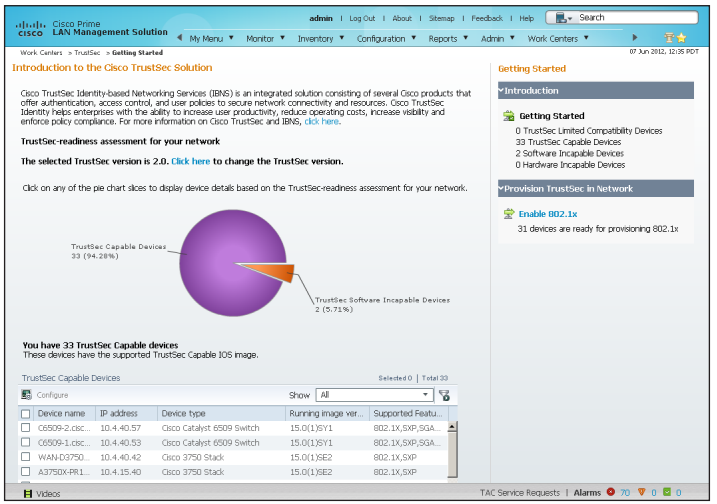
Step 5: In the **Identity Source** list, choose the previously defined AD server **AD1**, use the default options for this identity source, click anywhere in the window to continue, and then click **Save**.



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.



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**.

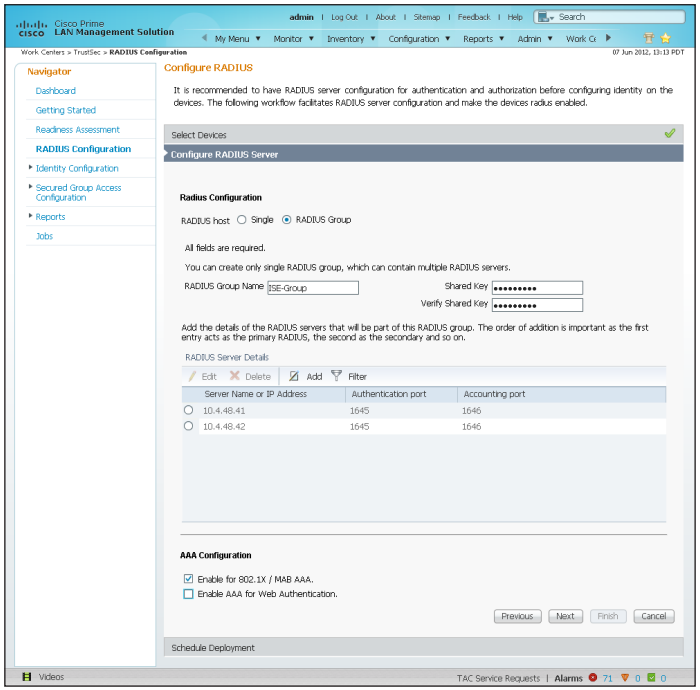
Step 5: On the Configure RADIUS page, select **RADIUS Group**, and in the **RADIUS Group Name** box, enter **ISE-Group**, and then in the **Shared Key** box, use the value used in previous procedures.

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**.



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**.

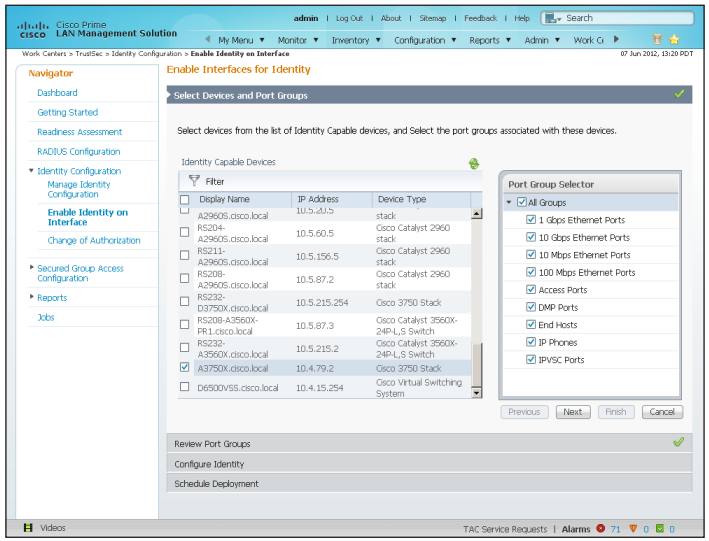
Procedure 4 Enable identity

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.

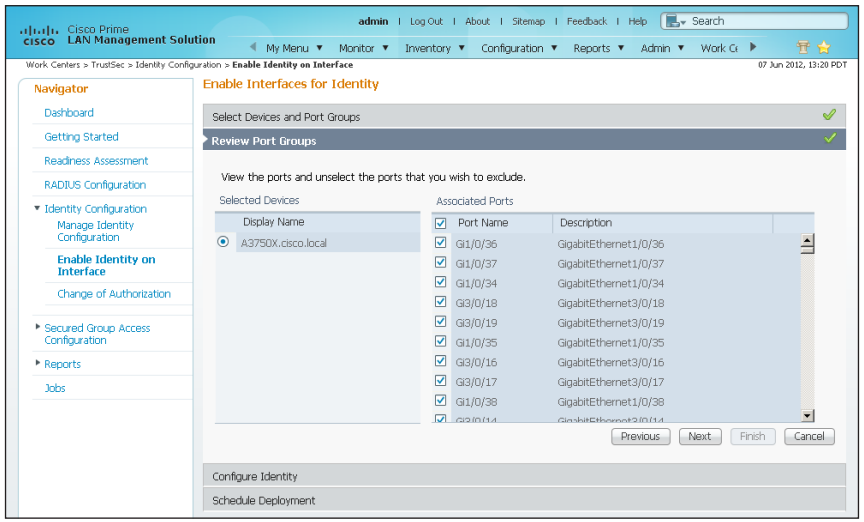
Step 1: Mouse over **Work Centers**, and then, under the TrustSec section, choose **Identity Configuration**.

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

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



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**

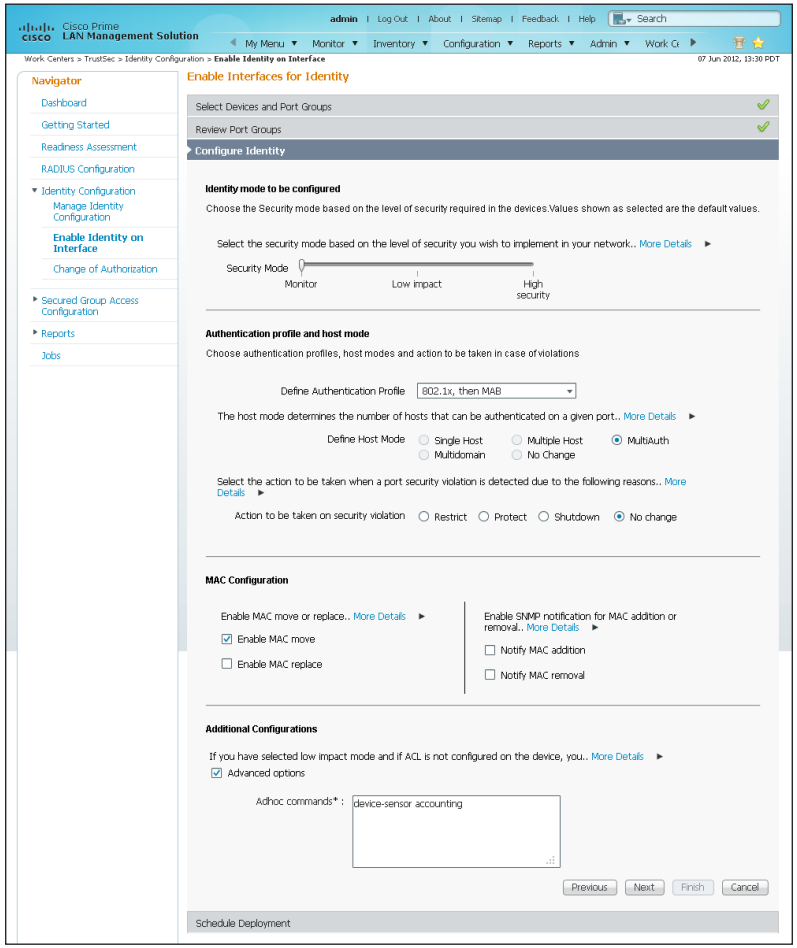
Step 7: In the MAC Configuration section, make sure only **Enable MAC Move** is selected.

Step 8: 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 *LAN Deployment Guide*.

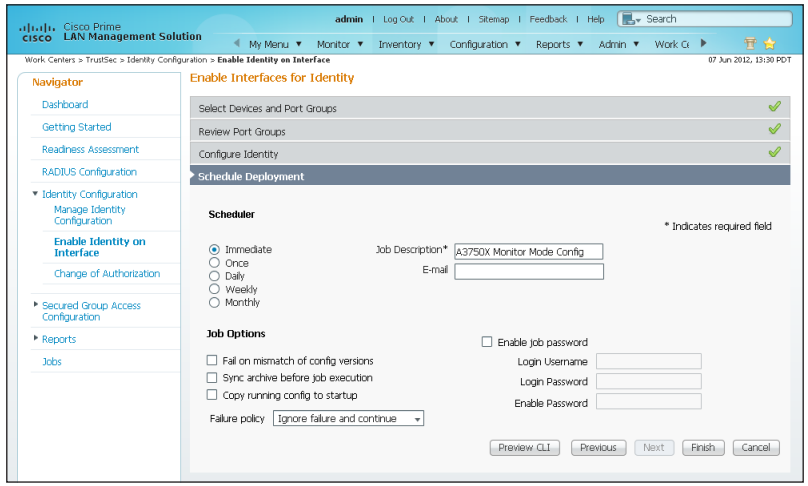


Identity configuration is complete. Next, you create a deployment job in order to deliver the configuration to the switch.

Step 9: 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.

```
aaa group server radius ISE-Group
 server 10.4.48.41
 server 10.4.48.42

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

authentication mac-move permit
dot1x system-auth-control
device-sensor accounting
radius-server host 10.4.48.41
radius-server host 10.4.48.42
radius-server key [key]
```

The interface commands added at the completion of this procedure 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 Cisco SBA design 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.

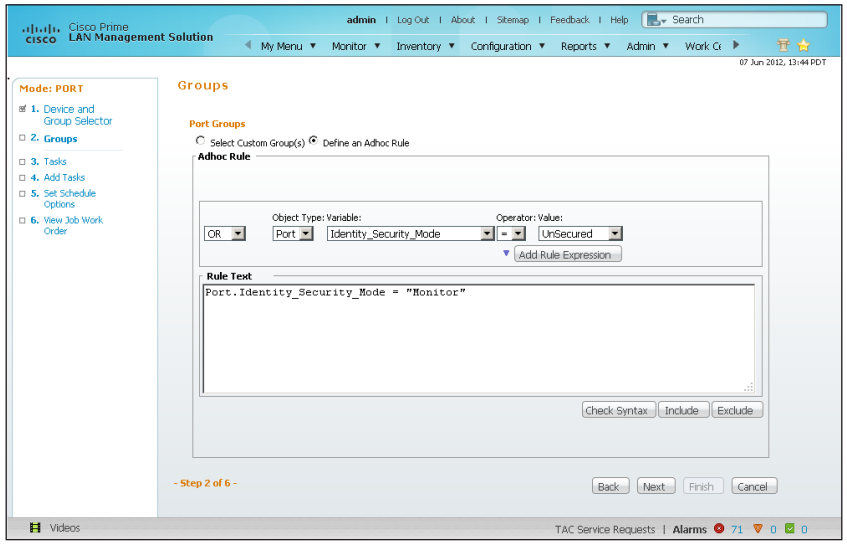
Step 6: Select **Define an Ad-Hoc Rule**. This brings up a new screen.

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, select **Monitor**.

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

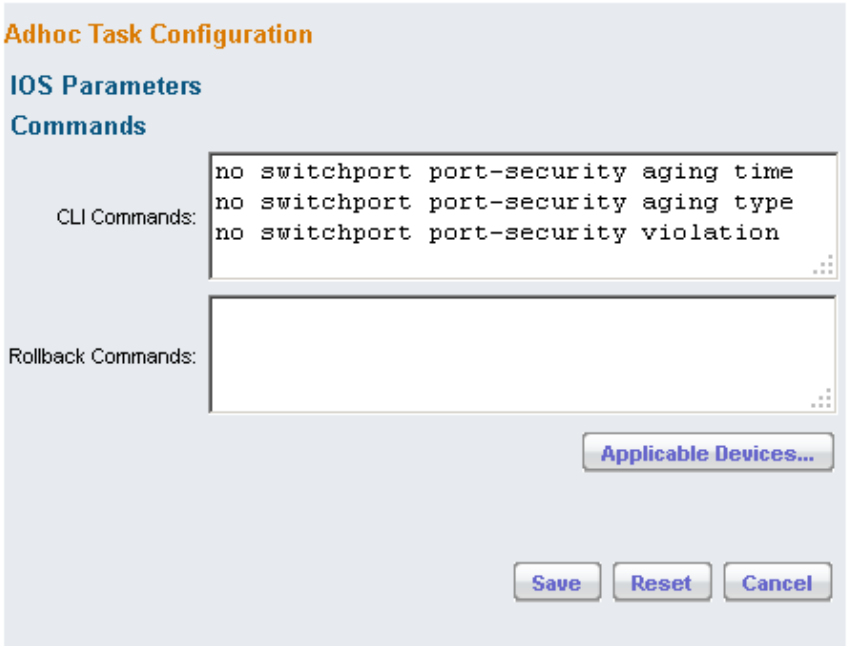


Step 11: In the Task Selector, select **Adhoc Task**, and then click **Next**.

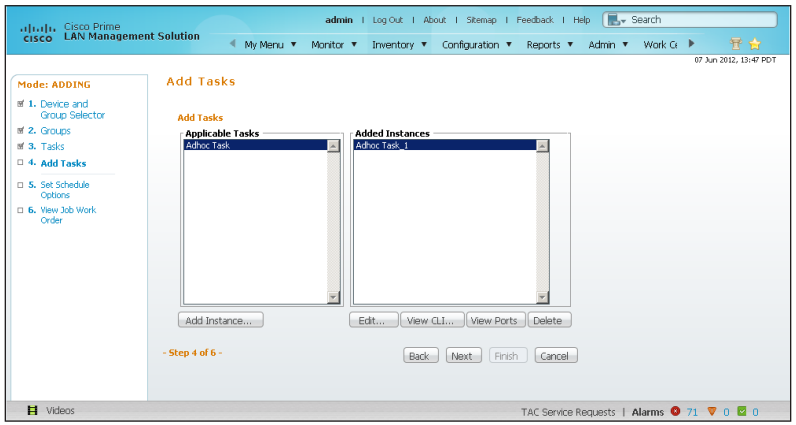
Step 12: Click **Add Instance**, and then, in the new window, enter the CLI commands necessary to remove the port security configuration.

```
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**.



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**.

Process

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 DHCP 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

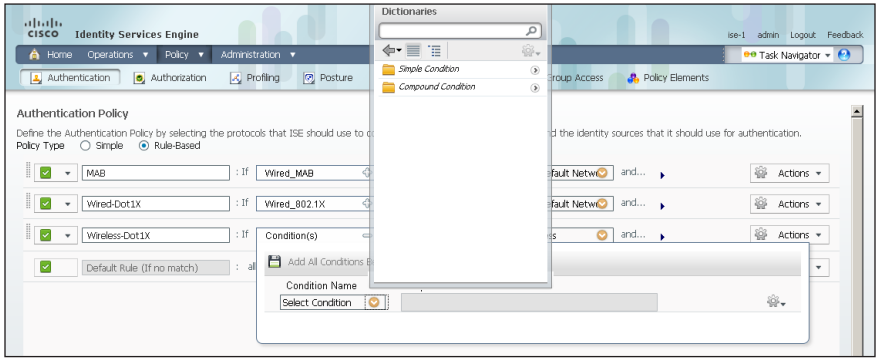
To differentiate wireless users in the authentication logs, create a rule to identify when wireless users authenticate.

Step 1: Navigate to **Policy** > **Authentication** to open the Authentication Policy page.

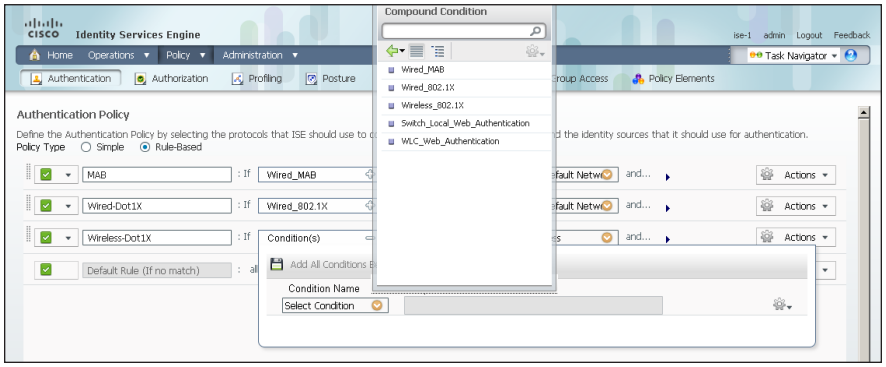
Step 2: For the Default Rule, click the **Actions** button, and then choose **Insert new row above**. A new rule, Standard Policy 1, is created.

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**.

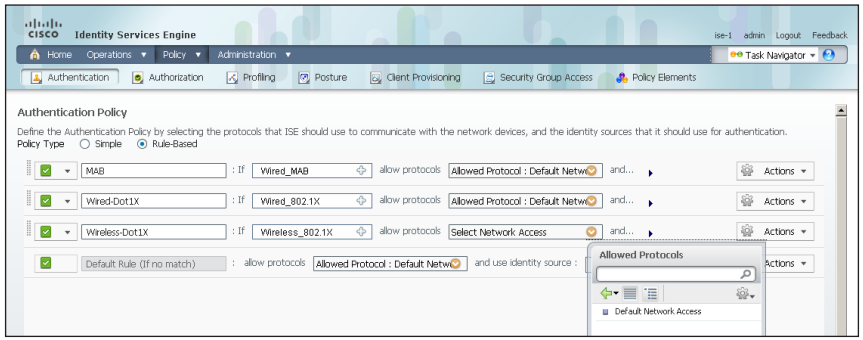
Step 4: In the **Select Condition** list, next to **Compound Condition**, click the **>** symbol.



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**.

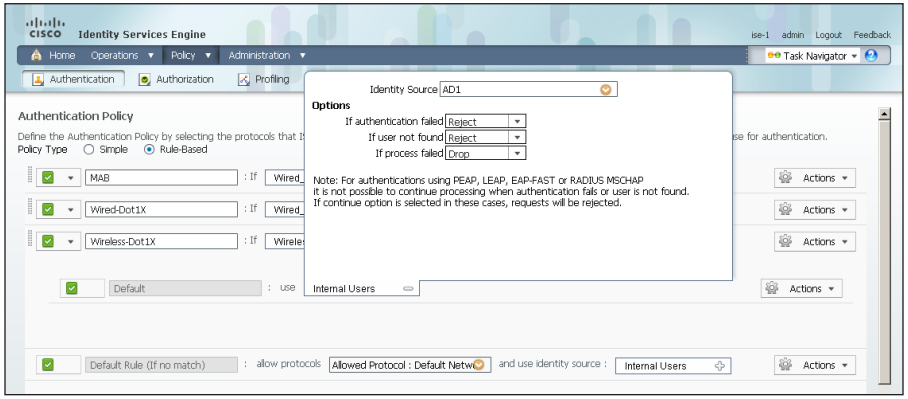


Step 7: For the **Wireless-Dot1X** rule, to the right of **and...**, click the black triangle. This displays the identity store used for this rule.

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

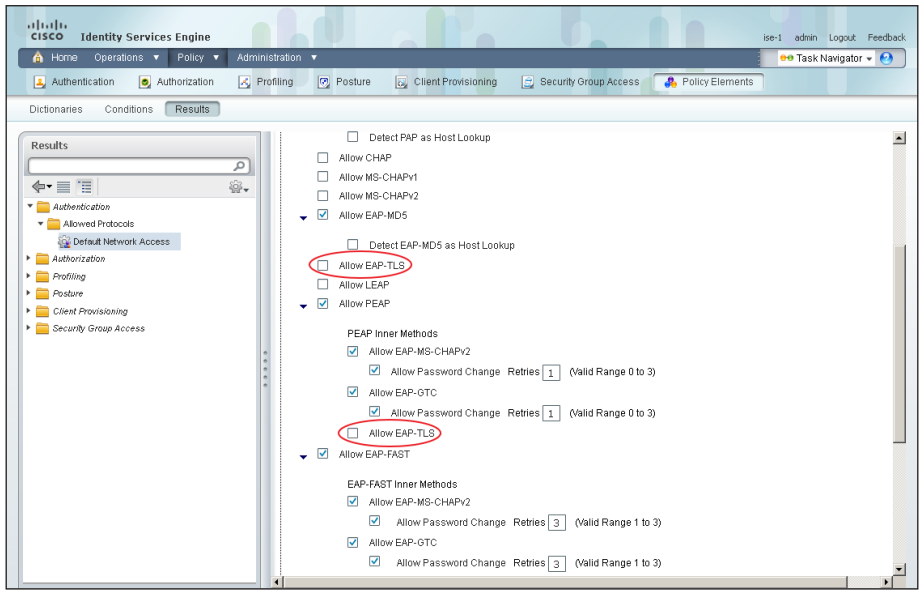
For wireless deployments that aren't currently using digital certificates, you need to disable EAP-TLS in order to allow clients to log in. You will be deploying digital certificates in a later phase of this deployment.

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.

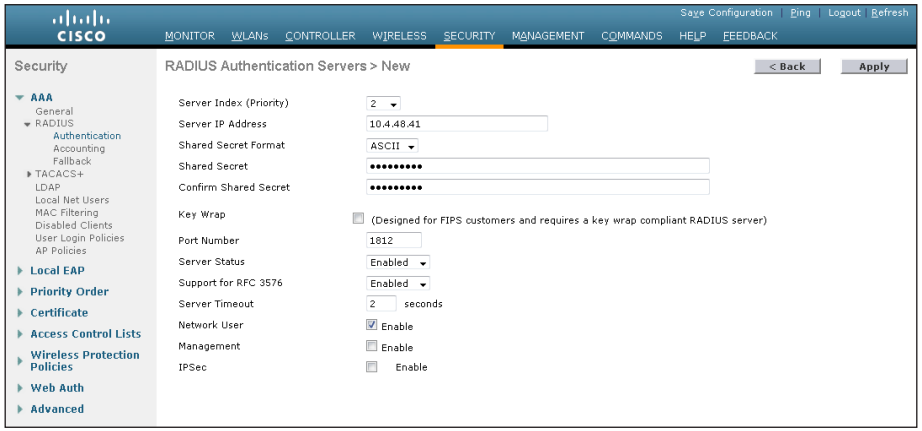
Step 2: On the menu bar, click **Security**.

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**.

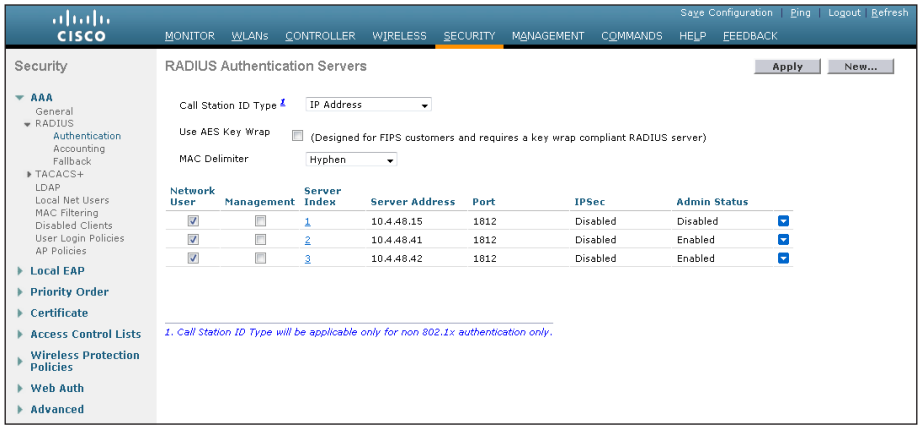


Step 7: Repeat Step 4 through Step 6 to add the secondary engine, 10.4.48.42, to the WLC configuration.

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**.



Procedure 4 Add Cisco ISE as RADIUS accounting server

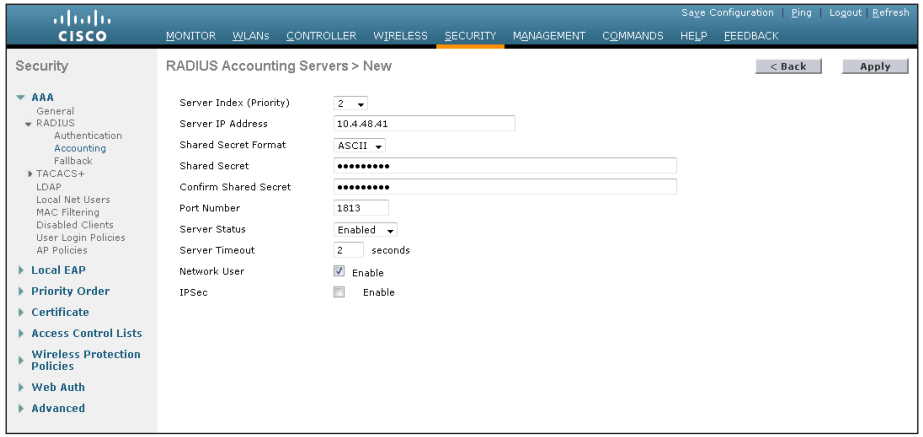
Perform this procedure for every wireless LAN controller (WLC) in the architecture, with the exception of the standalone guest WLC, if you have deployed one.

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.

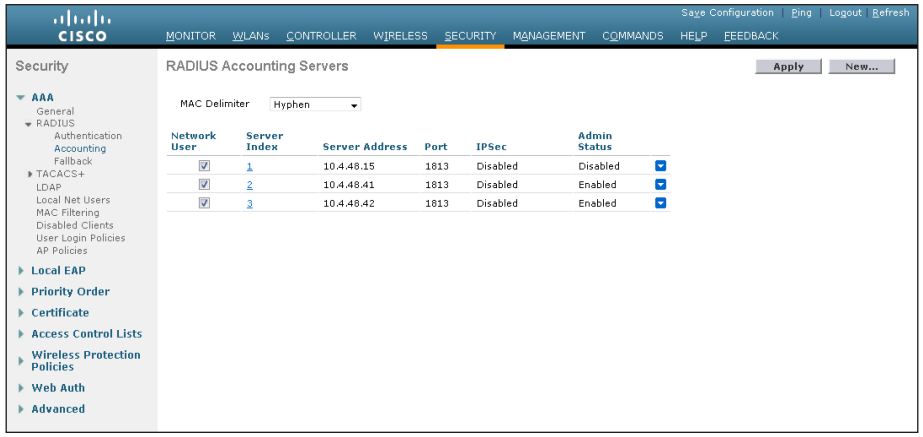
Step 4: In the **Server IP Address** box, enter **10.4.48.41**, enter your RADIUS shared secret, and then click **Apply.**



Step 5: Repeat Step 3 through Step 4 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**.

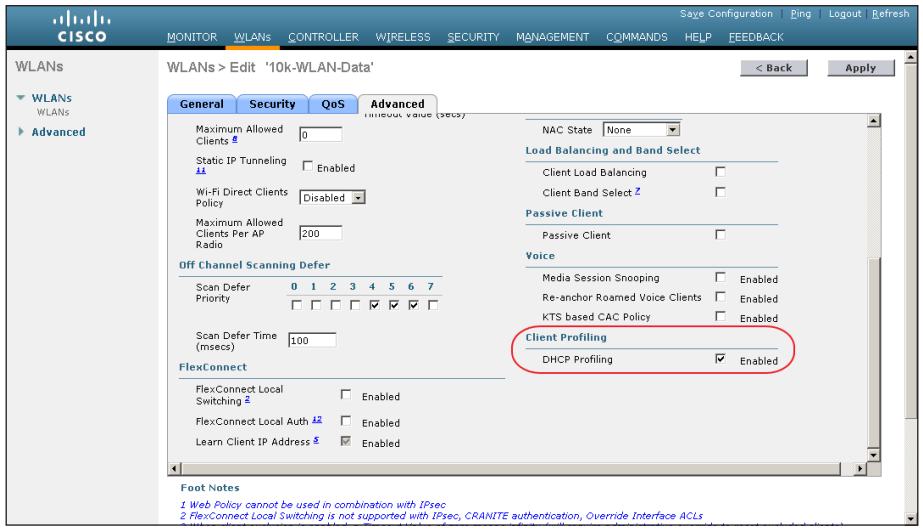


Procedure 5 Enable DHCP profiling

You need to enable DHCP profiling on the WLC in order to send DHCP 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 Reqd and disabling Local Auth, click **OK**, and then click **Apply**.

Step 4: 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.

Process

Deploying Digital Certificates

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

In 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 enable it on the existing Active Directory (AD) server.

Procedure 1 Install certificate authority

Step 1: Install an enterprise root certificate authority on the AD 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:

http://technet.microsoft.com/en-us/library/cc772393%28WS.10%29.aspx

Procedure 2 Install trusted root certificate for domain

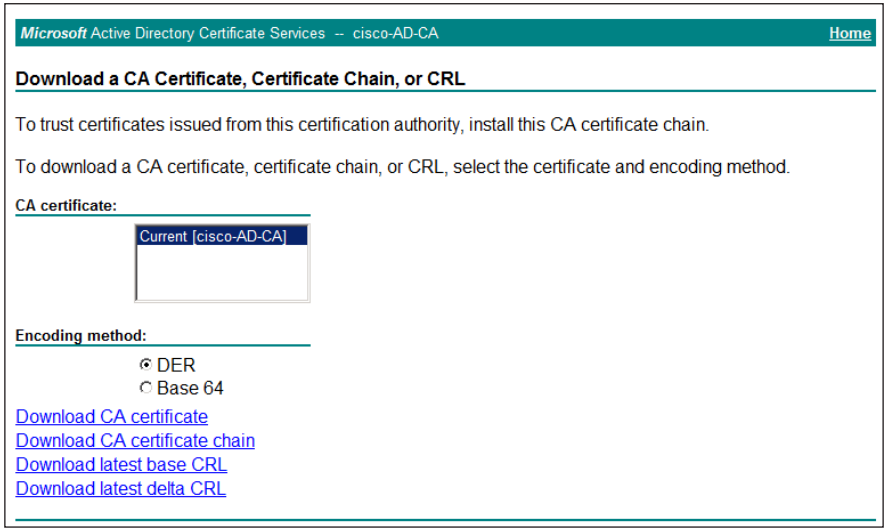
Install a trusted root certificate on the AD controller in order to distribute it to the clients so that certificates from the CA server will be trusted.

Step 1: On the CA console, launch a web browser, and then connect to the certificate authority, 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.

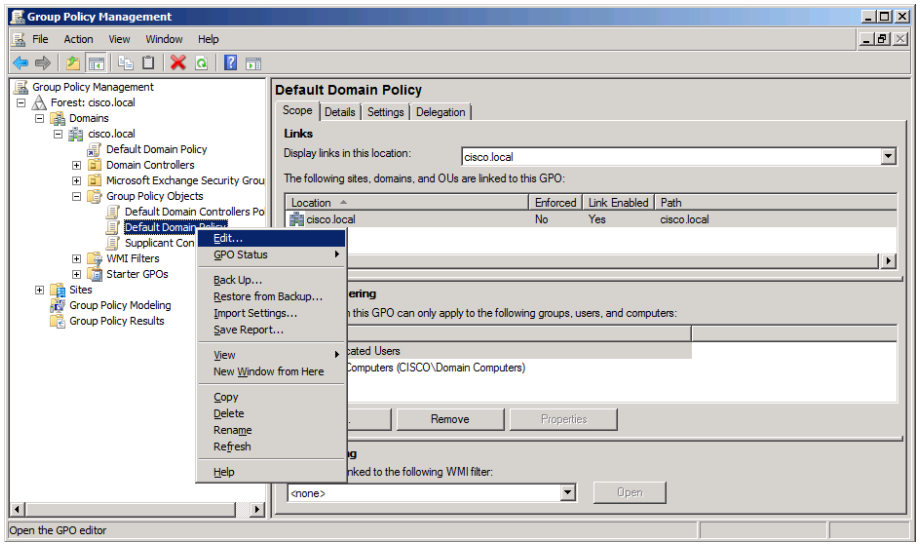
Step 4: Click **Download CA Certificate,** and then save the certificate file on the AD controller.



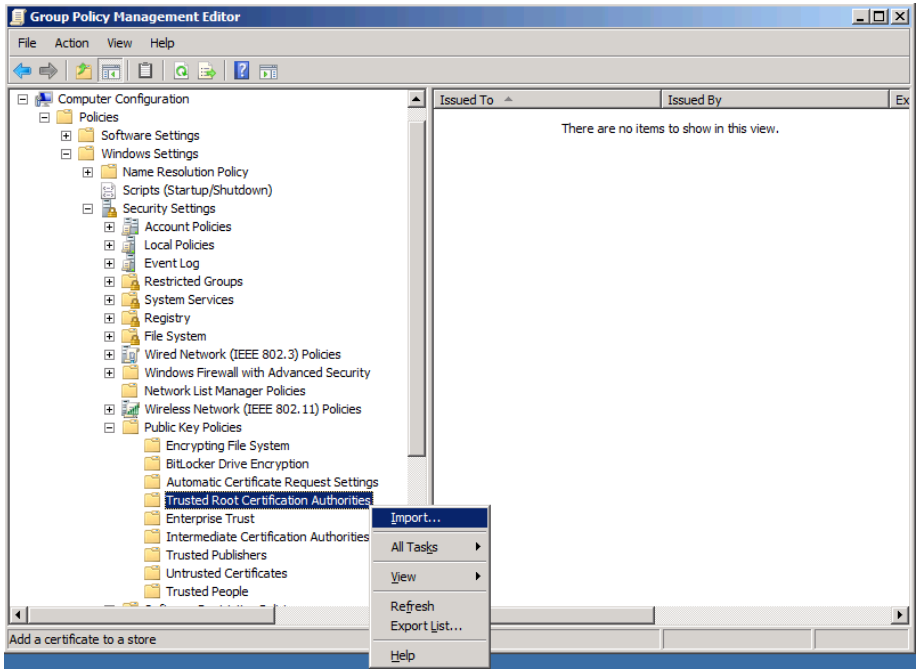
Step 5: On the AD console, navigate to **Start** > **Administrative Tools** > **Group Policy Management**.

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

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

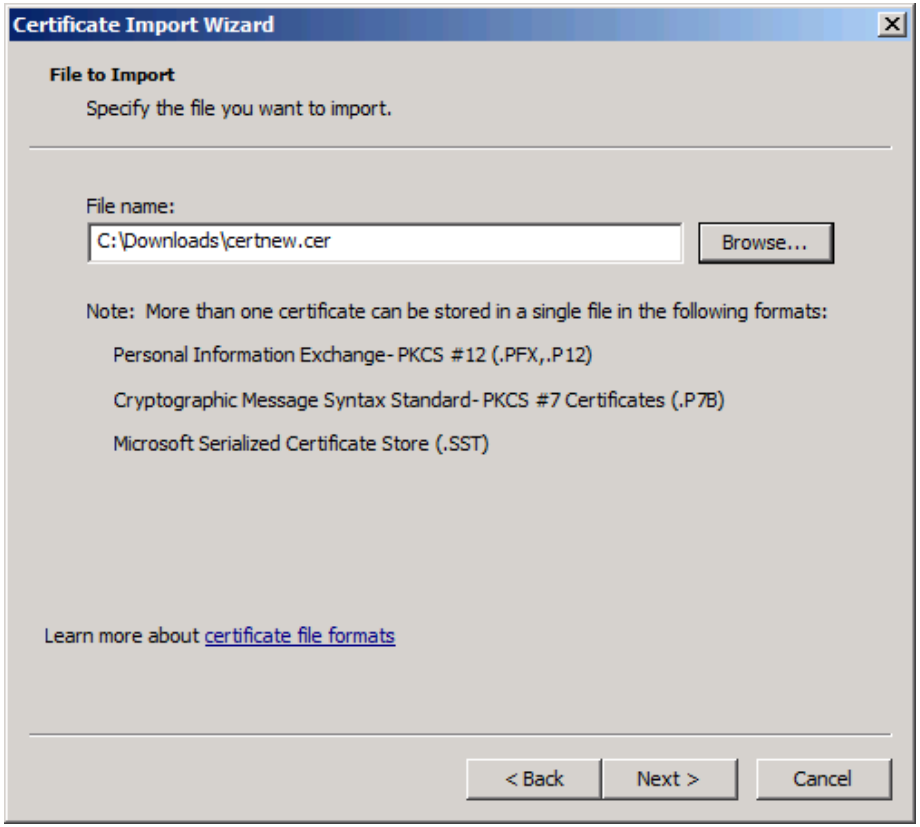


Step 8: Navigate to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Public Key Policies,** right-click **Trusted Root Certification Authorities,** and then choose **Import**. The Certificate Import Wizard launches.



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

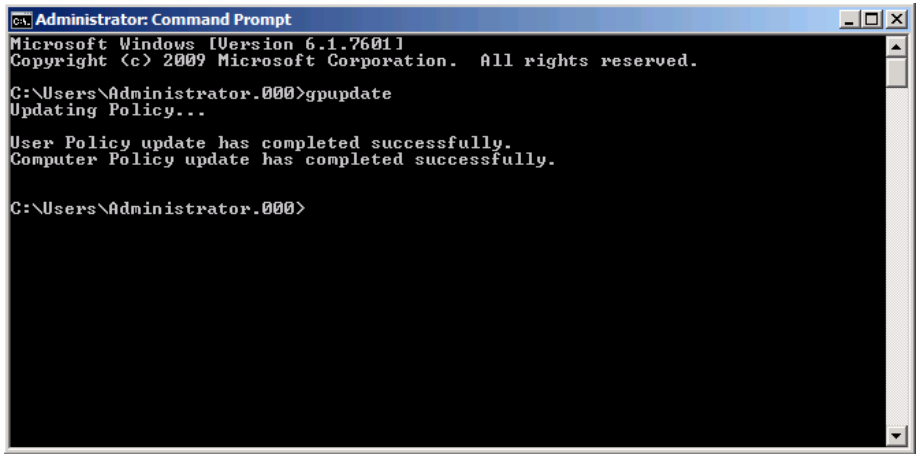
In addition to configuring AD server to distribute the trusted root certificate to workstations, you need to install the certificate directly on the AD server. A group policy object (GPO) update takes care of this automatically. In this procedure, you will force the update to run immediately.

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.

```
gpupdate
```



Procedure 4 Request a certificate for ISE from the CA

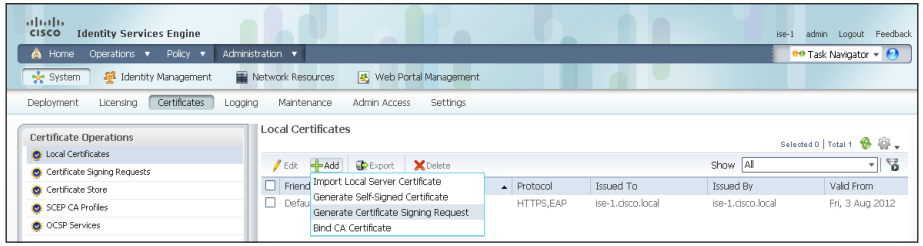
In order to obtain a certificate from the CA, Cisco ISE needs to generate a signing request that will be used by the CA to generate a certificate.

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

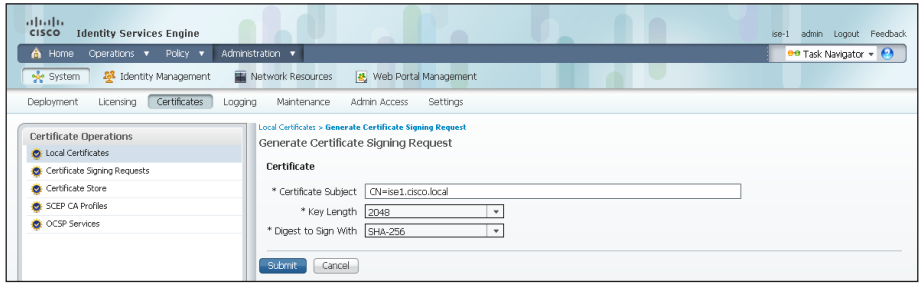
Step 2: Mouse over **Administration**, and then, from the System section of the menu, choose **Certificates**.

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

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

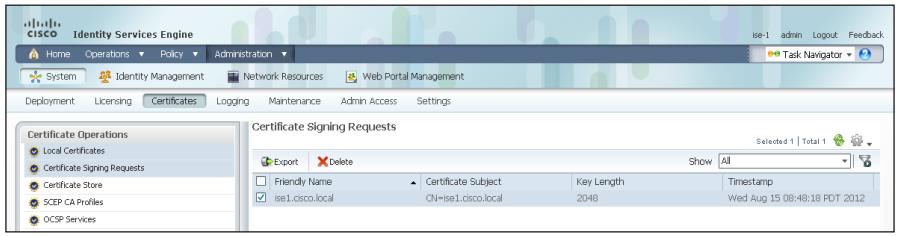


Step 5: In the **Certificate Subject** box, after the "CN=", enter the fully qualified domain name (FQDN) of the Cisco ISE server, and then click **Submit**.



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.

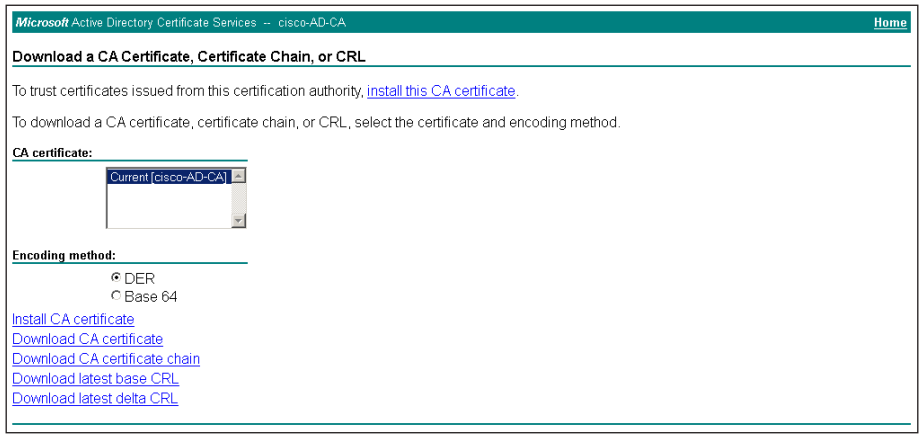
Procedure 5 Download CA root certificate

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**.

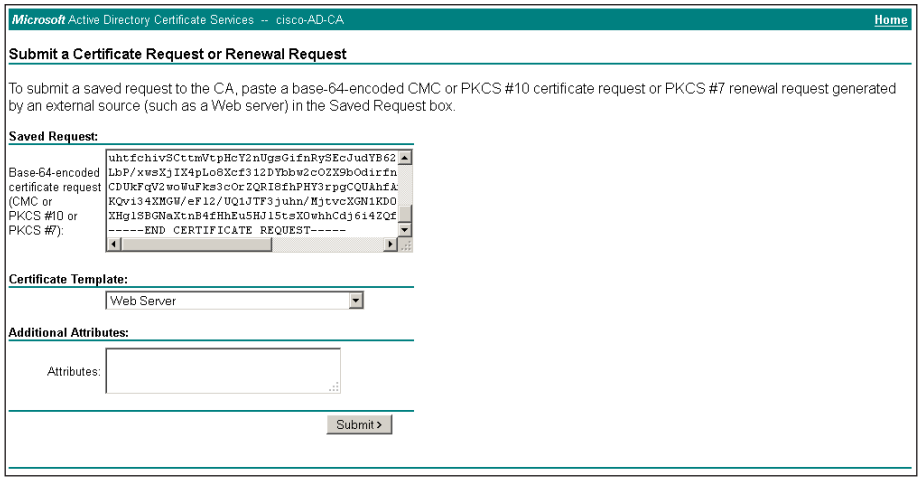
Step 3: Click **advanced certificate request**.

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**.

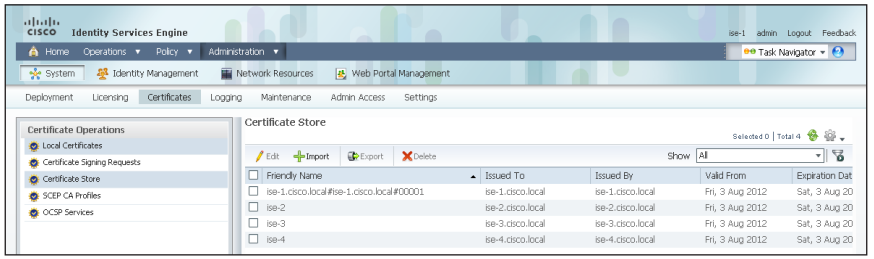


Step 8: Select **DER encoded**, and then click **Download certificate.** The certificate saves to your local machine.

Procedure 7 Install trusted root certificate in Cisco ISE

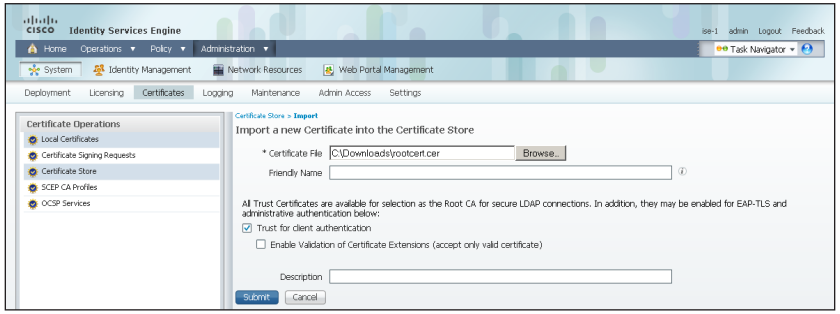
Step 1: In the Cisco ISE interface, mouse over **Administration**, and then, from the System section of the menu, choose **Certificates**.

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



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**.

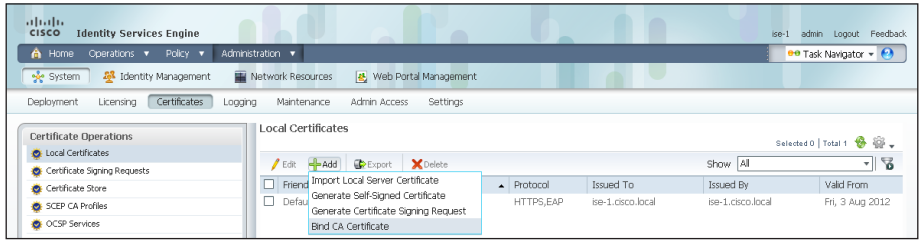


Procedure 8 Install local certificate in Cisco ISE

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

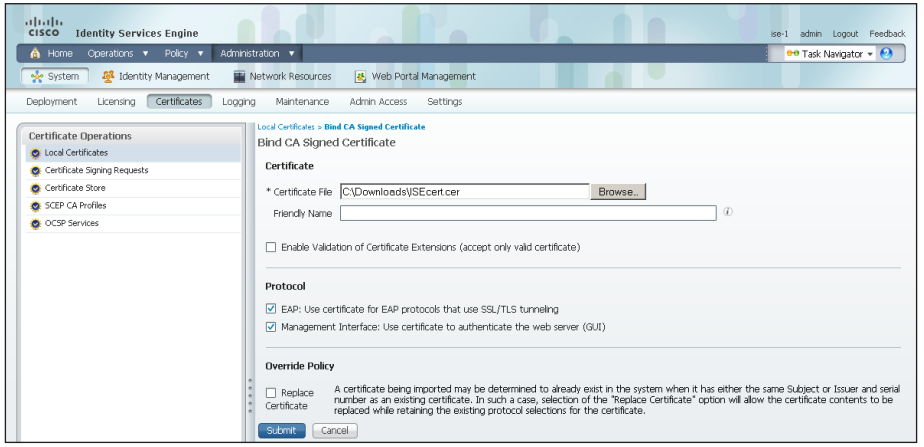
Step 2: Click **Local Certificates**.

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



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**.

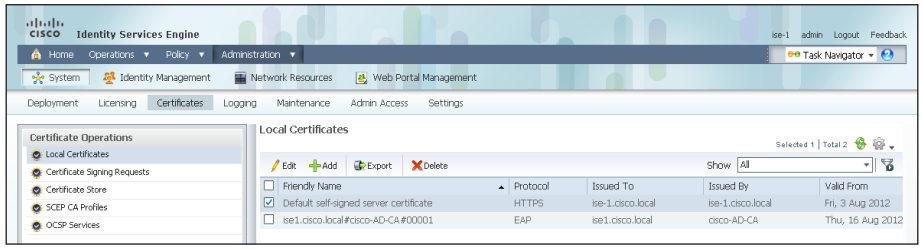
Procedure 9 Delete old certificate and request

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**.

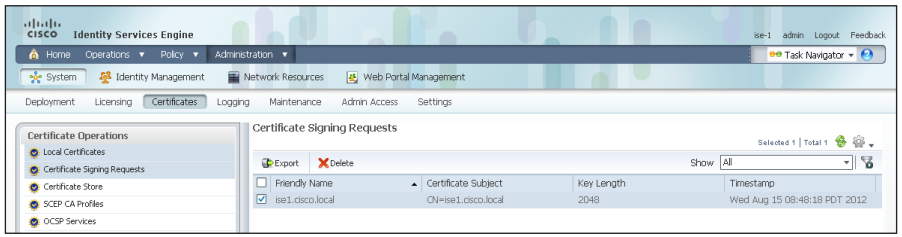
Step 3: Select the box next to the self-signed certificate. This is the certificate issued by the Cisco ISE appliance and not the certificate issued by the CA that was just imported.



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 Cisco ISE policies
2. Enable certificates
3. Enable EAP-TLS

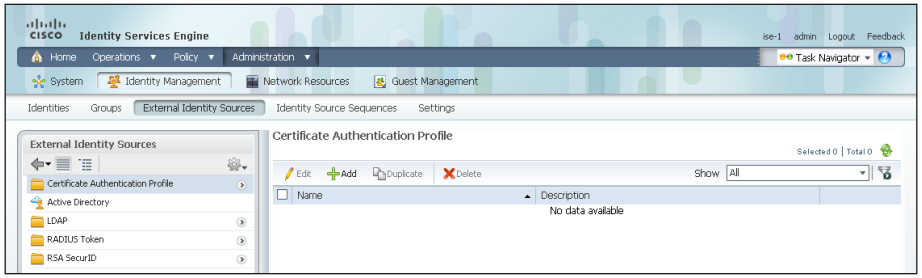
You will configure Cisco ISE policies to support 802.1X authentication using digital certificates for both wired and wireless users.

Procedure 1 Create Cisco ISE policies

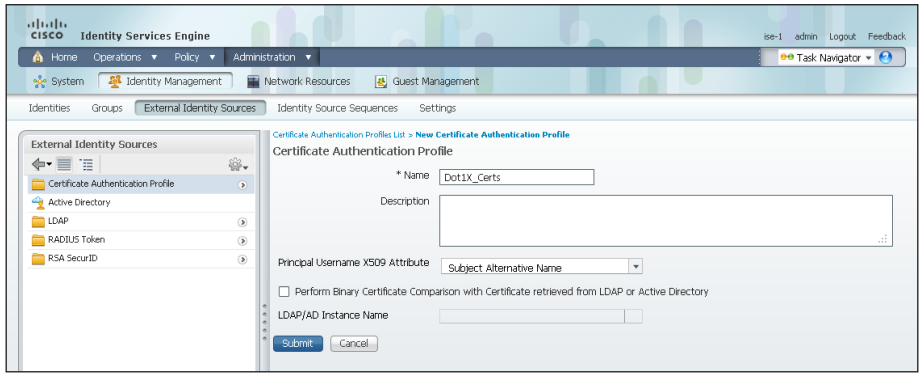
An authentication profile is used to determine how a certificate will be used for authentication.

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**.

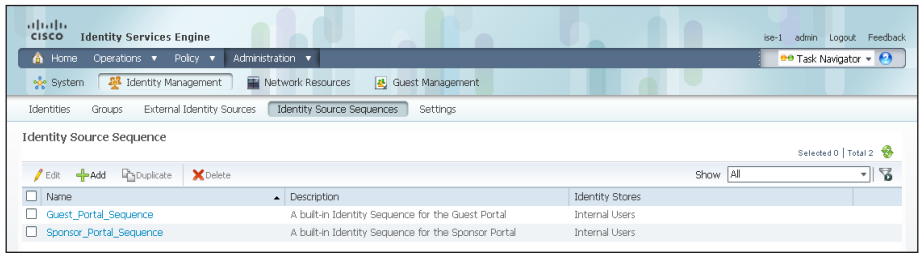


Step 3: Give the profile a meaningful name, and in the **Principal Username X509 Attribute** list, choose **Subject Alternative Name**, and then click **Submit**.



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

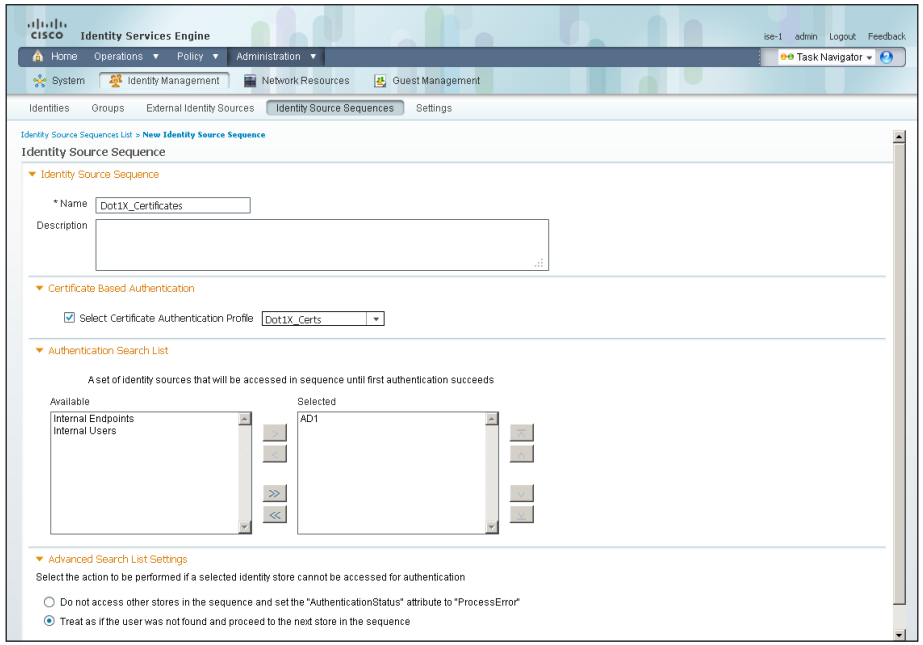


Step 5: Give the sequence a meaningful name.

Step 6: In the Certificate Based Authentication section, select **Select Certificate Authentication Profile**, and then choose the profile created previously.

Step 7: In the Authentication Search List section, in the **Available** list, double-click the AD server. It moves into the **Selected** list.

Step 8: 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**.



Procedure 2 Enable certificates

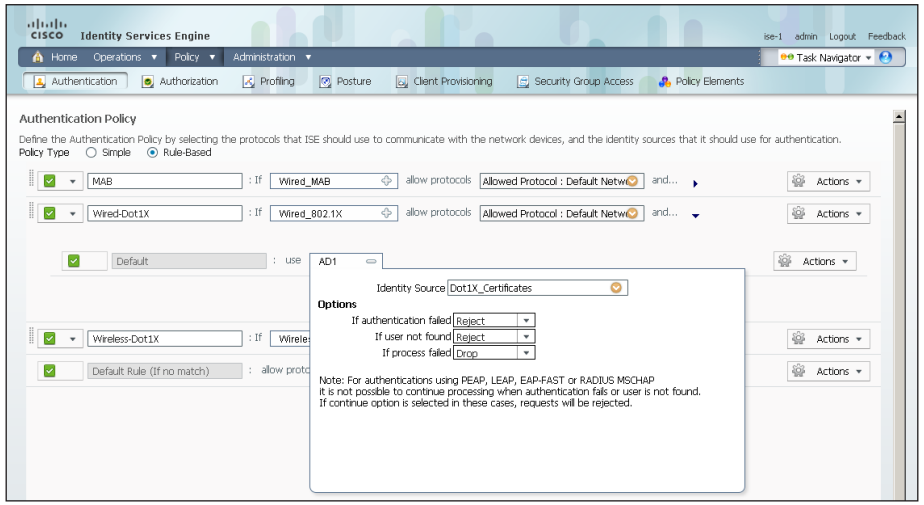
Now that you have created a certificate authentication profile and identity source sequence for digital certificates, you need to enable the 802.1X authentication policies for both wired and wireless users.

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.

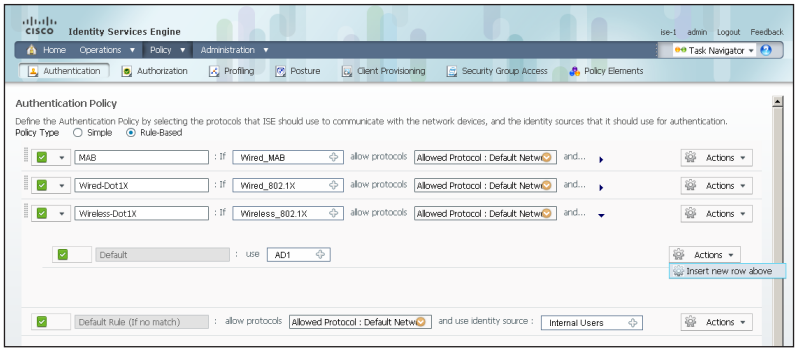
Step 3: Next to the AD1 identity store entry, click the **+** symbol.

Step 4: In the **Identity Source** list, choose the identity source sequence created in Procedure 1, "Create Cisco ISE policies," use the default options for this identity source, and then click anywhere in the window to continue.



Next, for wireless users, you modify the authentication policy to first check if the client is using EAP-TLS and then, if not, to allow them to use an authentication method, such as Protected Extensible Authentication Protocol (PEAP), that uses a user name and password for credentials. This allows users who haven't gotten certificates yet to still access the network. Once they connect to the network, Windows clients get their certificates pushed to them, and other endpoints can manually obtain a certificate.

Step 5: For the **Wireless-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**.

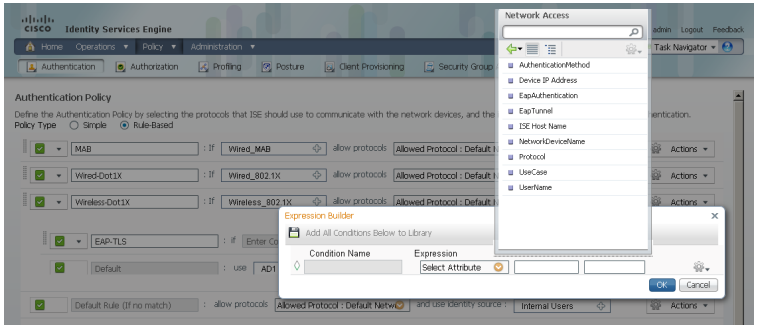


Step 6: Give the rule a name, and then next to the **Enter Condition** box, click the **+** symbol. The Expression Builder opens.

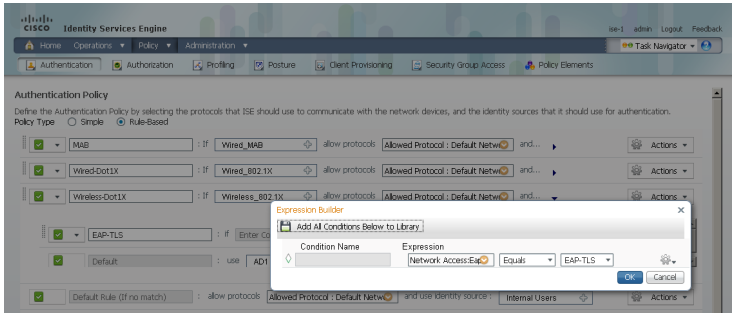
Step 7: Click **Create New Condition (Advance Option)**.

Step 8: In the **Expression** list, next to **Select Attribute**, click the arrow.

Step 9: Next to **Network Access**, click the arrow, and then select **EapAuthentication**.

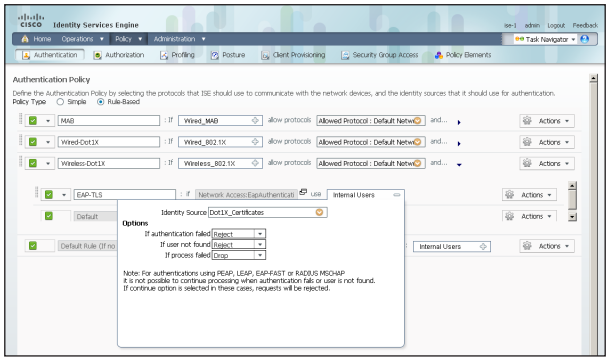


Step 10: In the second list, choose **Equals,** and in the last list, choose **EAP-TLS**, and then click **OK**.



Step 11: Next to **Internal Users**, click the **+** symbol.

Step 12: In the **Identity Source** list, choose the identity source sequence created in Procedure 1, "Create Cisco ISE policies," use the default options for this identity source, and then click anywhere in the window to continue.



Step 13: Click **Save**.

Procedure 3 Enable EAP-TLS

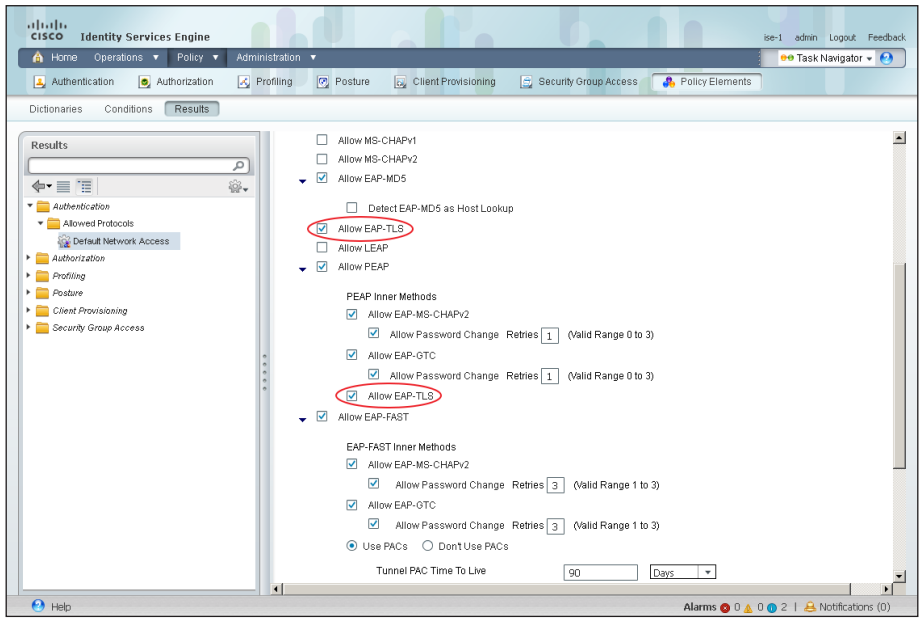
In a previous section, you disabled EAP-TLS. Now that you are using digital certificates, you need to re-enable it.

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

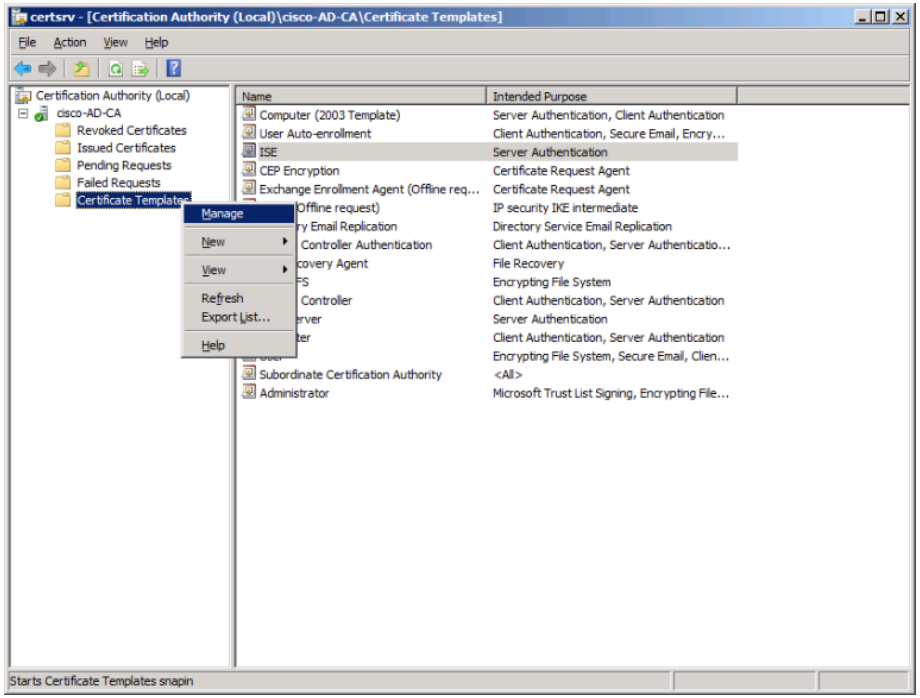
certificates are deployed to the endpoint where the user logs in to the domain. The steps in this example deployment describe how to edit the Default Domain Policy so that it will apply to all users, but you could create a new policy object and apply it to a subset of users if you prefer.

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.



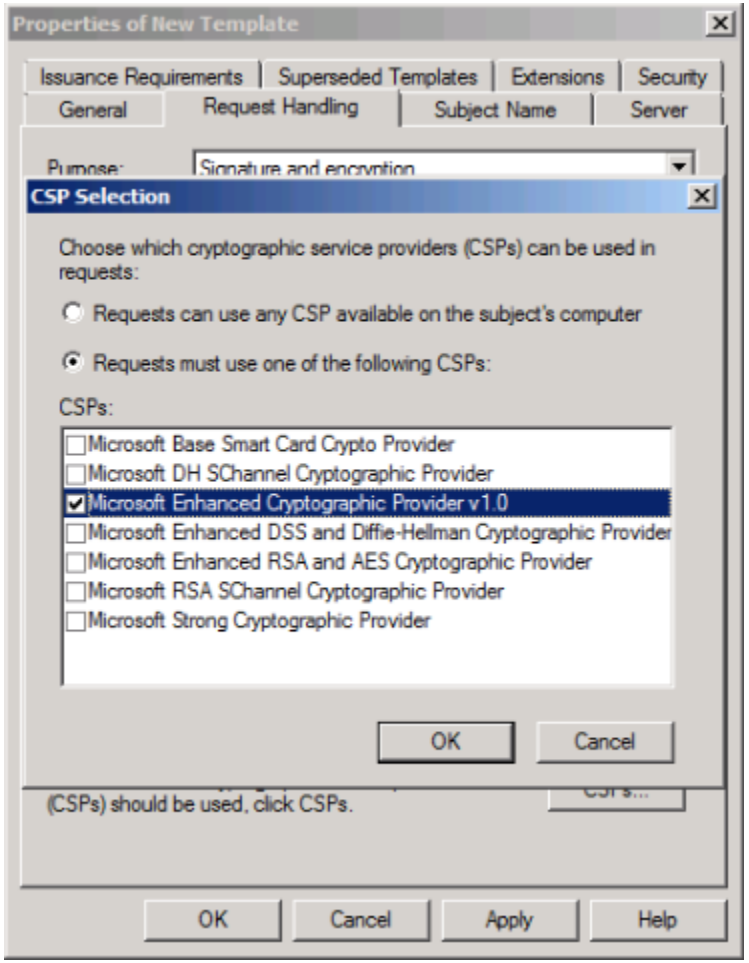
Step 3: Right-click the Computer template, and then choose **Duplicate Template**.

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

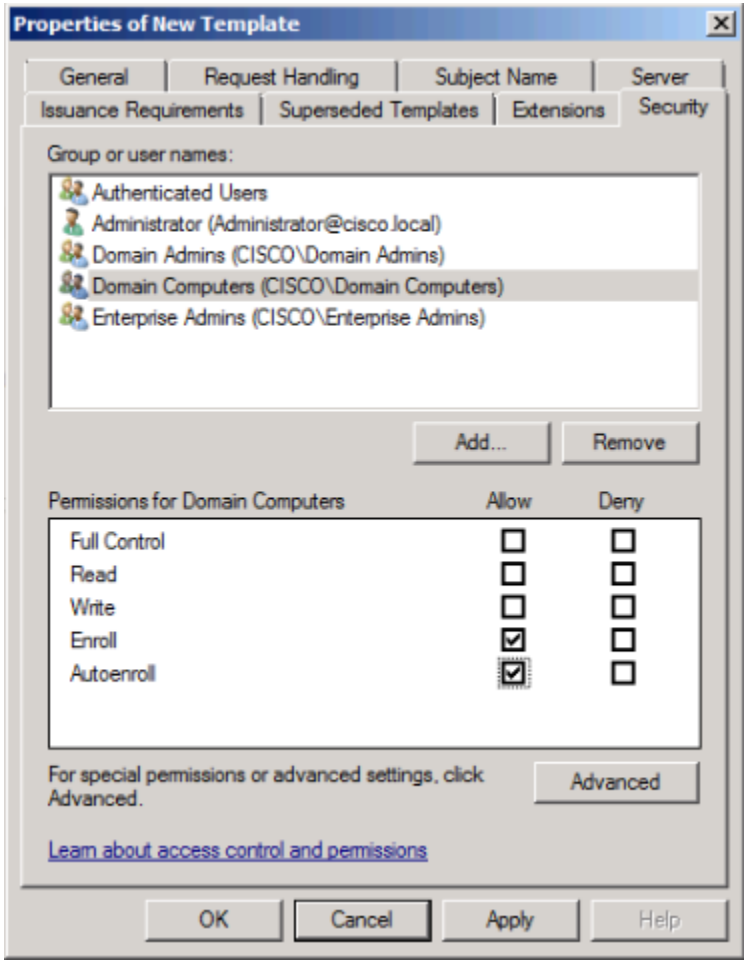
Step 5: In the Properties of New Template window, click the General tab, and then give the template a name.

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**.



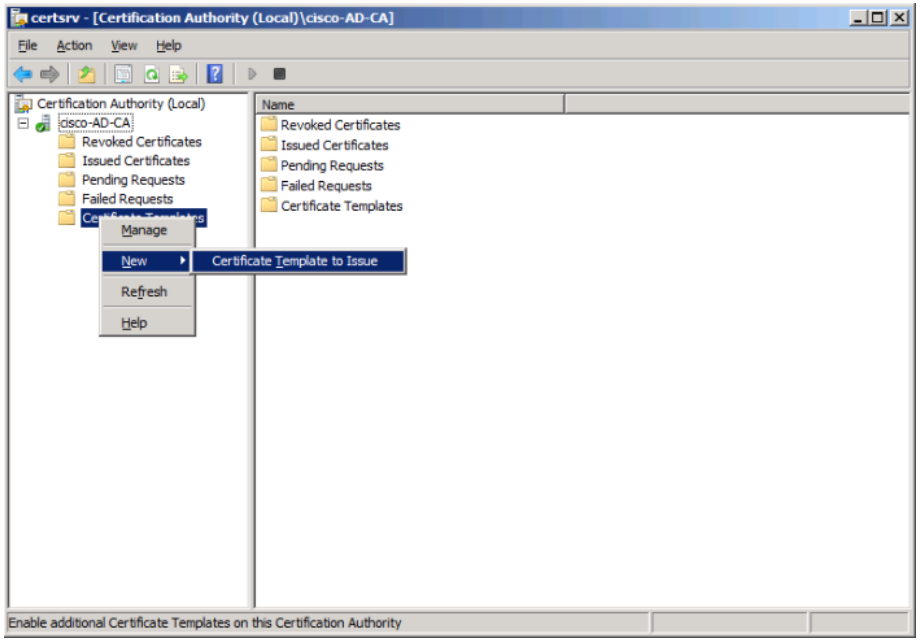
Step 8: On the Security tab, click **Domain Computers,** and then for both **Enroll** and **Autoenroll**, make sure **Allow** is selected.



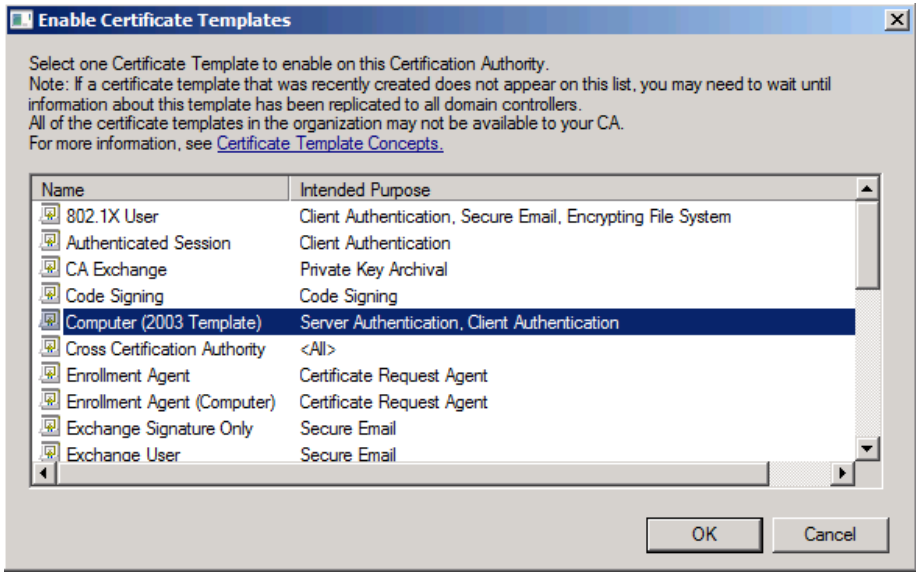
Step 9: Use the defaults for the remaining tabs, and then click **OK**.

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**.



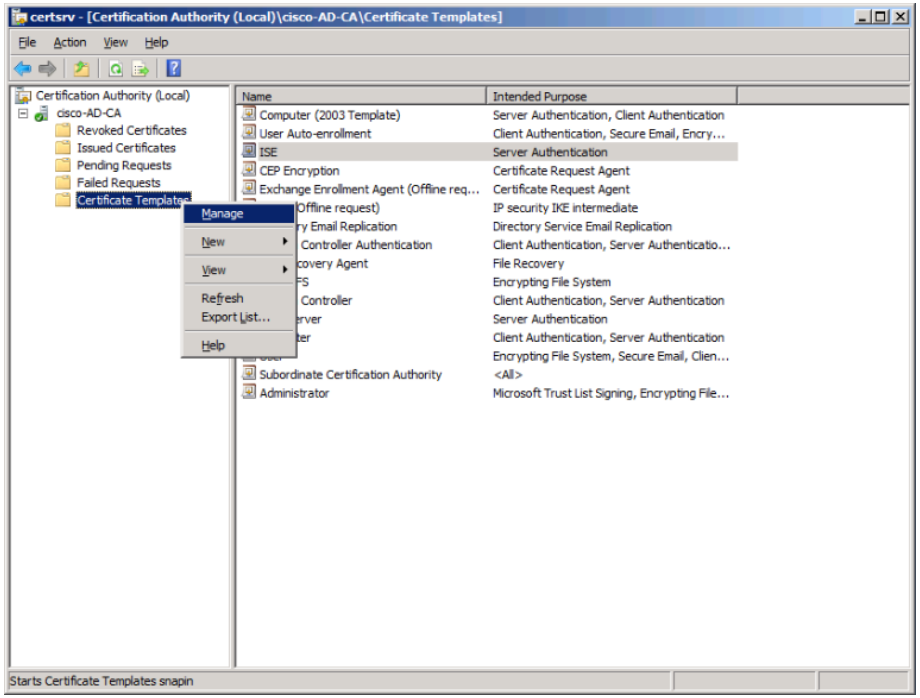
When machines join the domain or when the GPO policy is refreshed (the default period is 90 minutes), the machine receives a machine certificate to allow for 802.1X machine authentication.

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**.

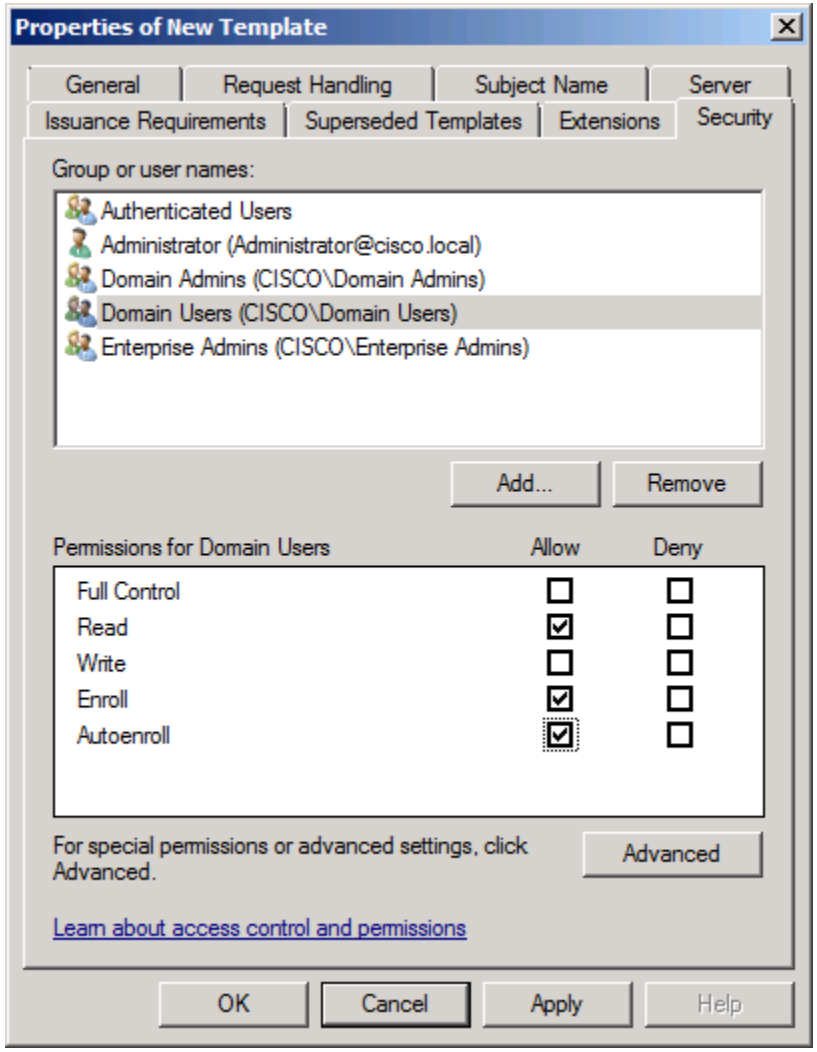
Step 4: For compatibility with Windows XP, make sure that **Windows 2003 Server Enterprise** is selected.

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**.

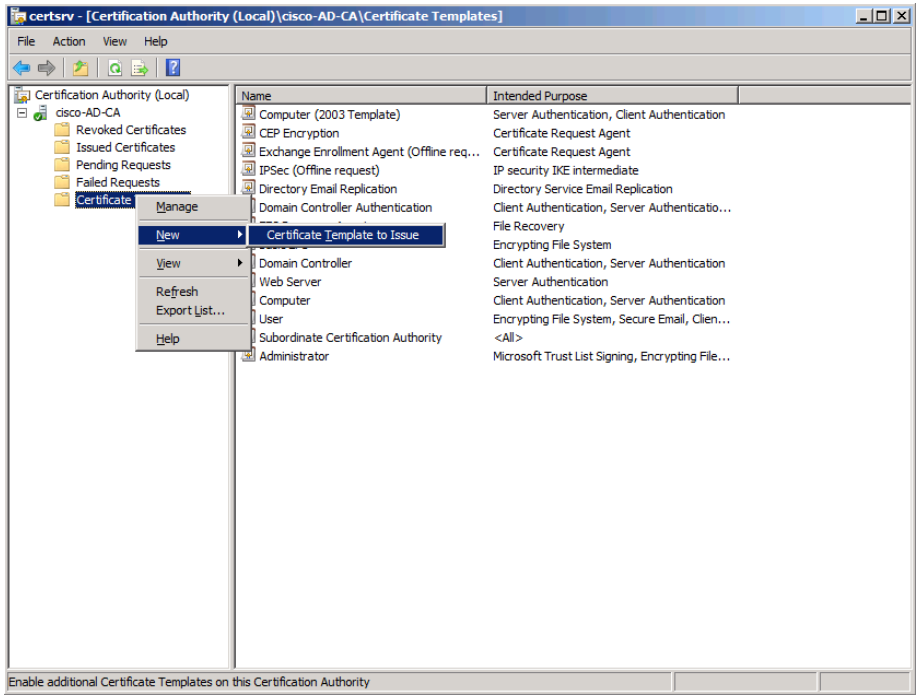
Step 8: On the Security tab, click **Domain Users**, and then for **Read**, **Enroll**, and **Autoenroll**, make sure **Allow** is selected.



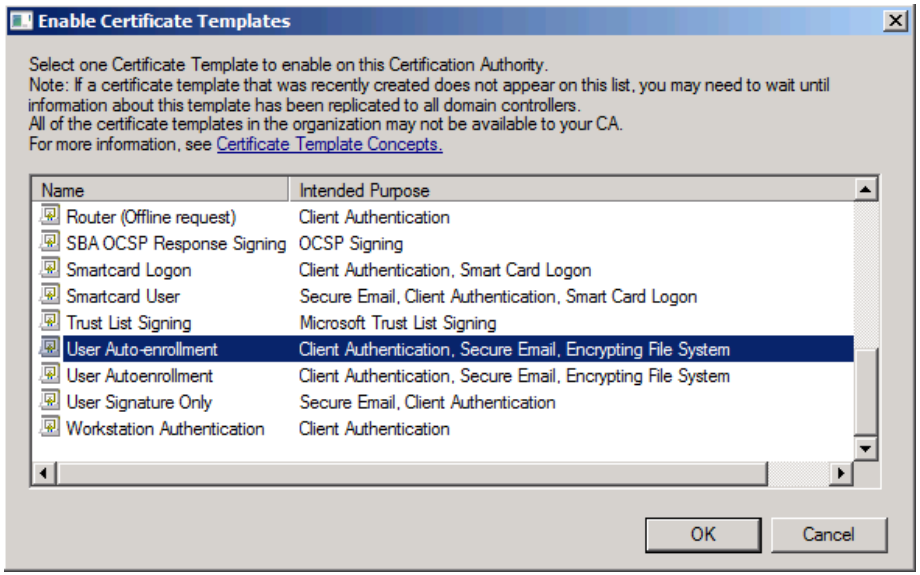
Step 9: Use the defaults for the remaining tabs, and then click **OK**.

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.

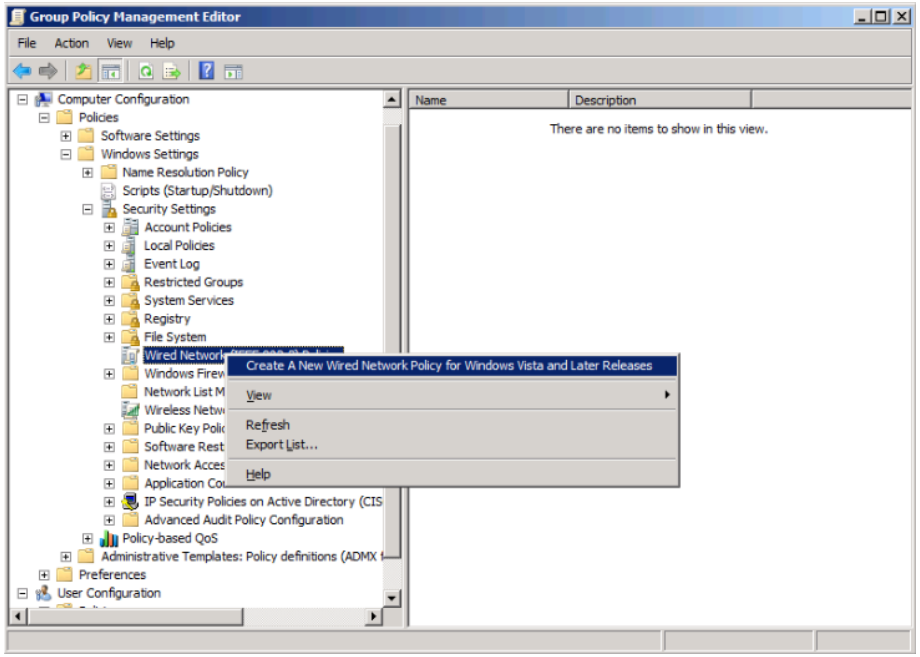
Step 1: On the CA console, navigate to **Start** > **Administrative Tools** > **Group Policy Management**.

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

Step 3: Right-click **Default Domain Policy.** 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** to close the certificate properties window.

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.

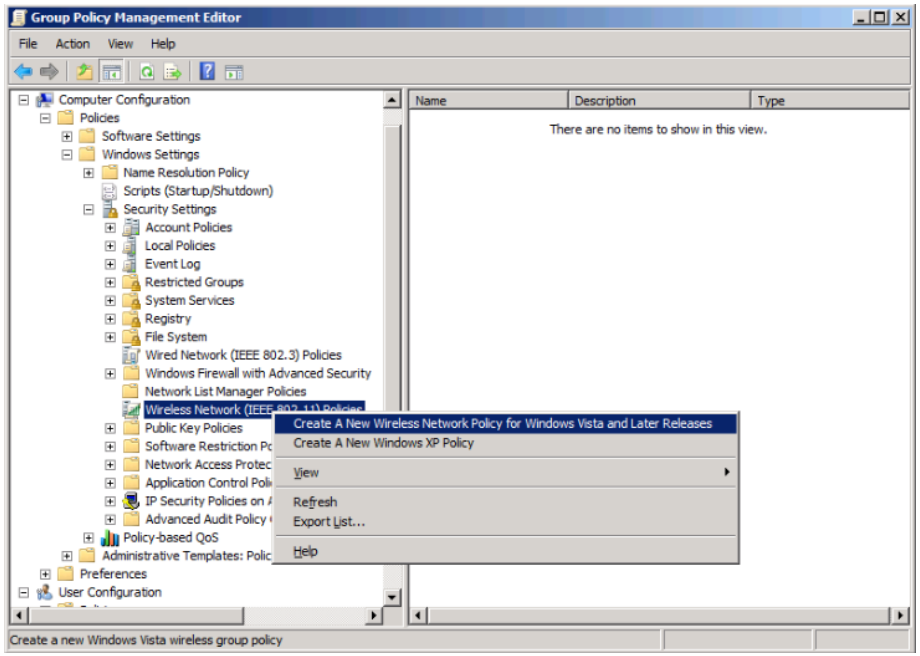
Step 1: On the CA console, navigate to **Start** > **Administrative Tools** > **Group Policy Management**.

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

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

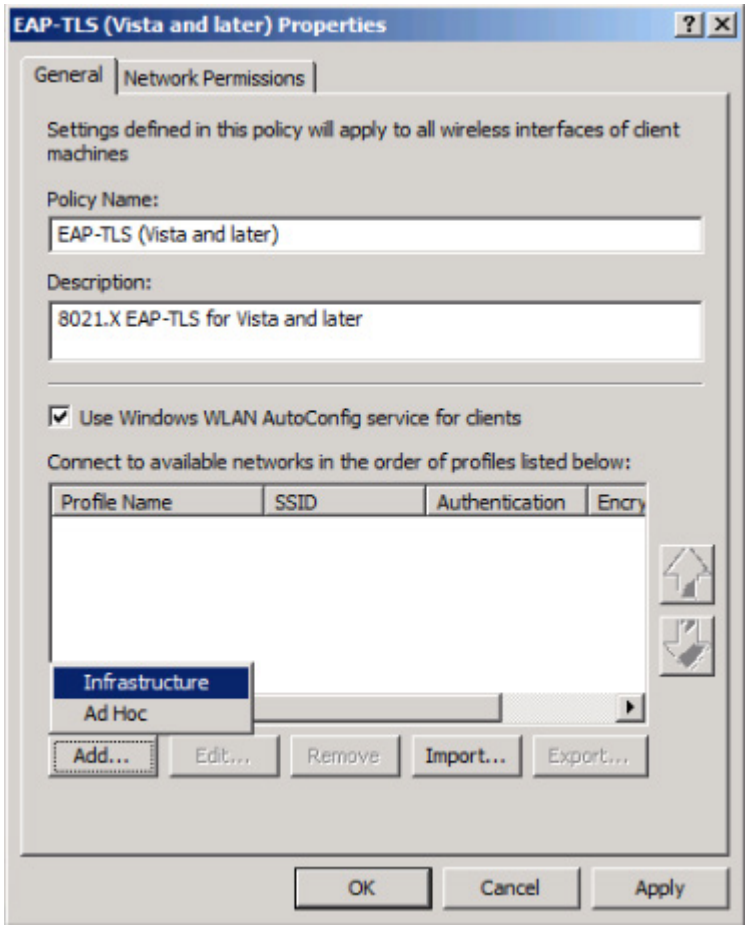
Step 4: In the Group Policy Management Editor, navigate to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings**.

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**.

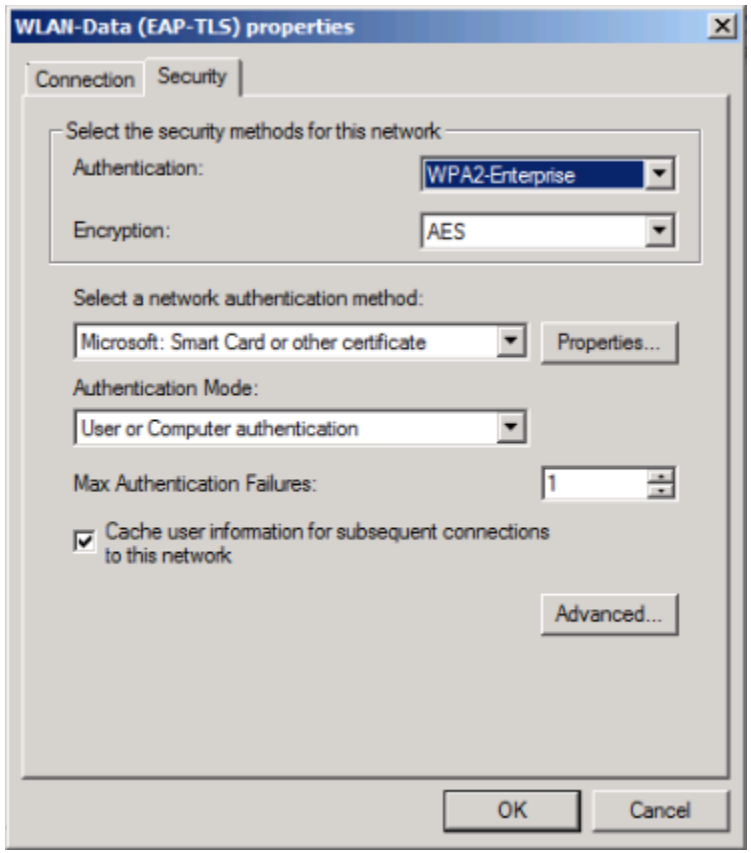


Step 8: Give the profile a name, enter the name of the SSID for the wireless network, and then click **Add**.

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.

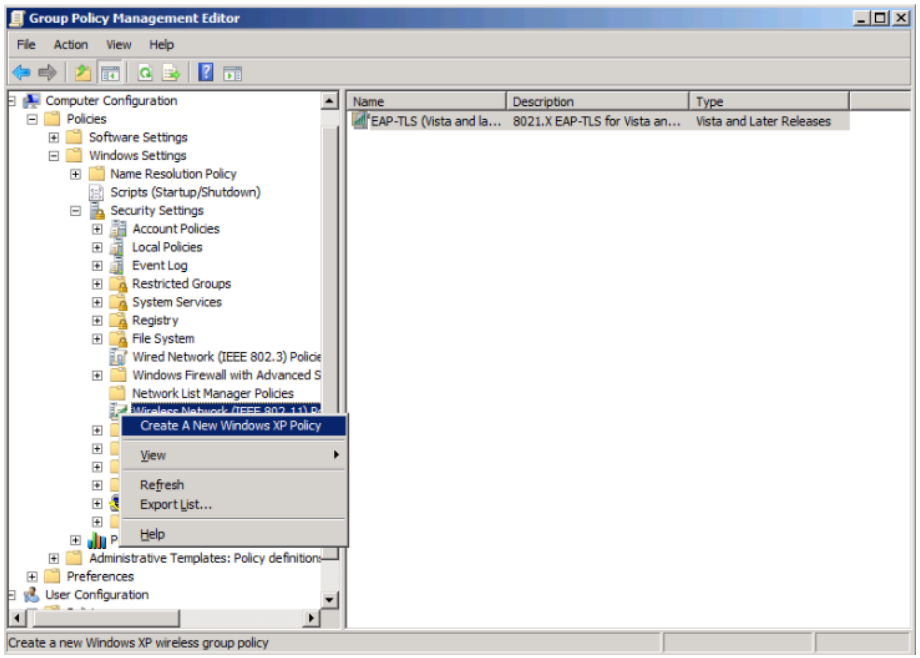
Step 14: In the **Trusted Root Certification Authorities** list, next to the root certificate for the CA, select the check box.

Step 15: Click **OK** to close the certificate properties window and then click **OK** to close the profile properties window.

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

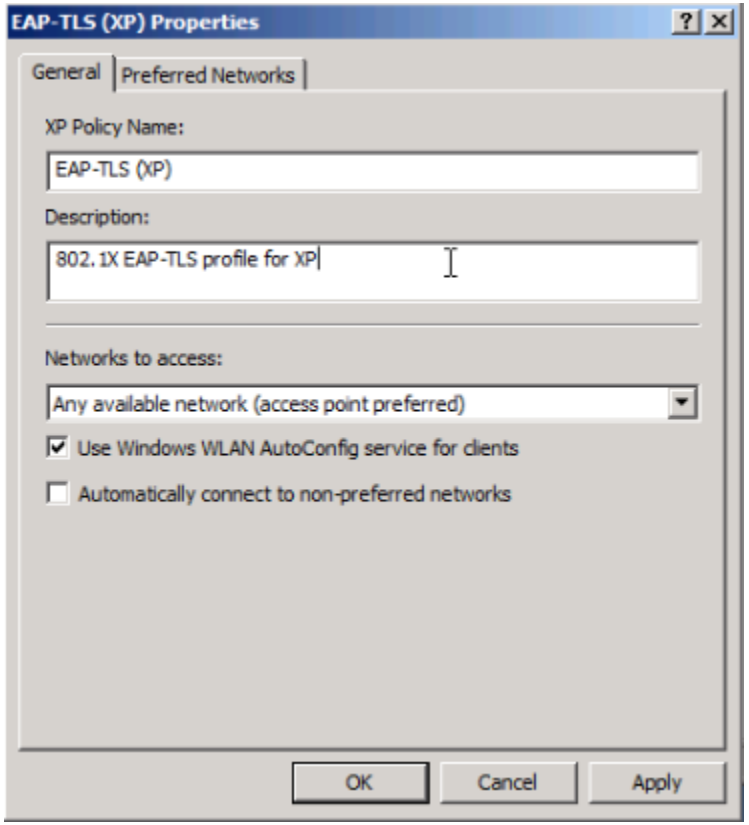
Next, you create a policy for Windows XP clients.

Step 17: Right-click **Wireless Network (IEEE 802.11) Policies**, and then choose **Create a New Windows XP Policy**.



Step 18: 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 19: In the **Networks to access** list, choose **Any available network (access point preferred)**.



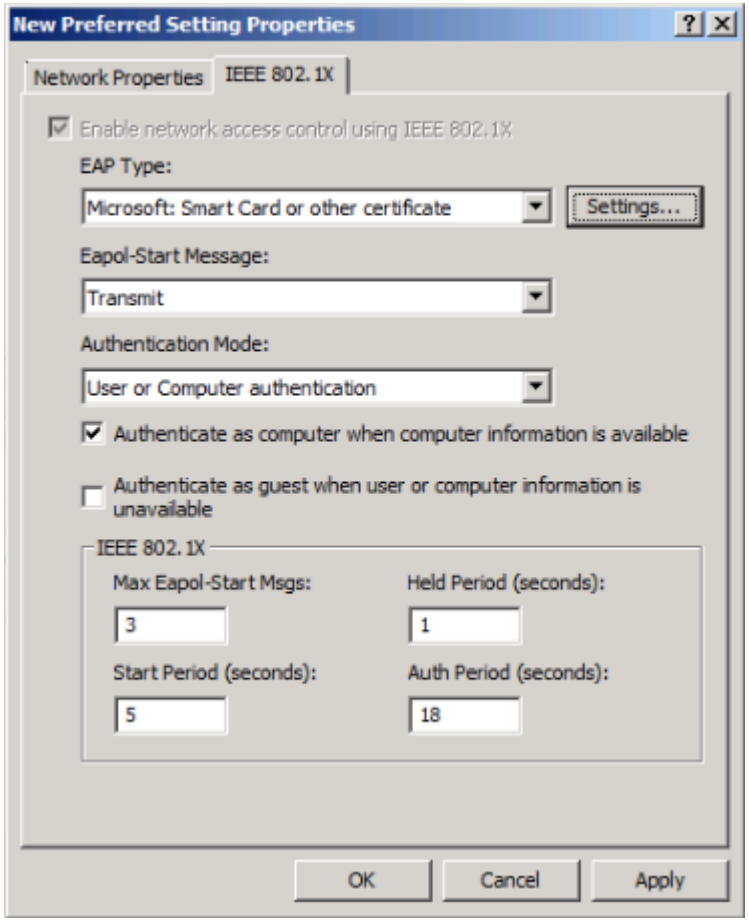
Step 20: On the Preferred Networks tab, click **Add,** and then select **Infrastructure**.

Step 21: Enter the SSID for the network and give a description.

Step 22: In the **Authentication** list, choose **WPA2**, and then in the **Encryption** list, choose **AES**.

Step 23: On the IEEE 802.1X tab, in the **EAP type** list, choose **Microsoft: Smart Card or other certificate**.

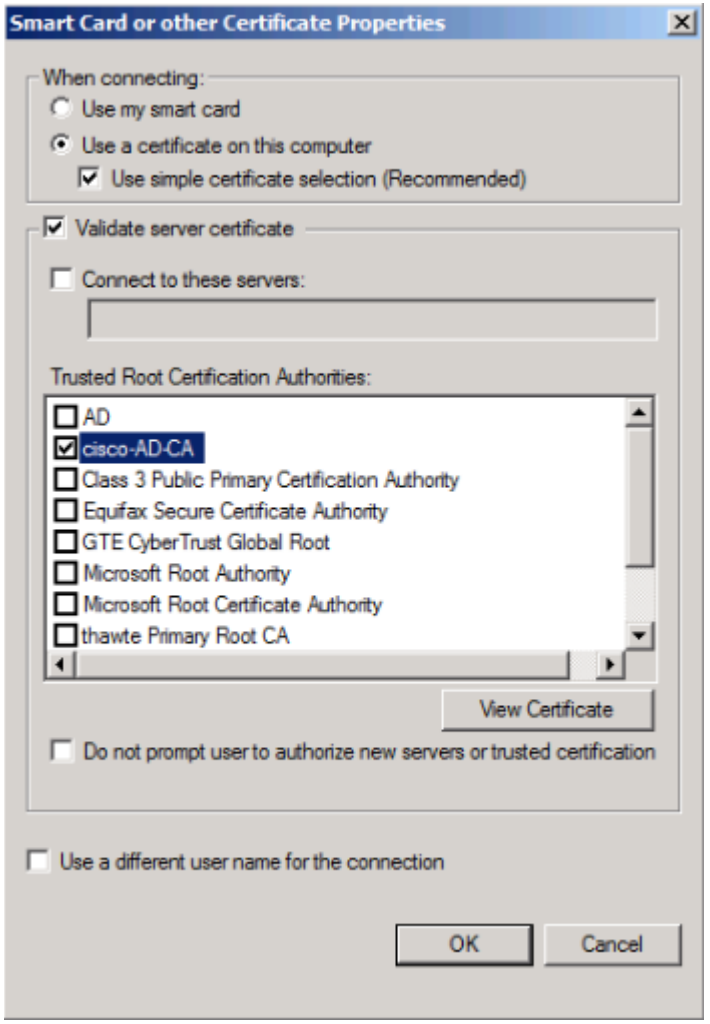
Step 24: In the **Authentication Mode** list, choose **User or Computer authentication**.



Step 25: Click **Settings**.

Step 26: 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.

Process

Deploying Cisco AnyConnect on Windows Endpoints

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

Cisco AnyConnect Secure Mobility Client 3.0 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 3.0 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://www.cisco.com/cisco/software/release.html?mdfid=283000185&flowid=17001&softwareid=282364313&release=3.0.08057&relind=AVAILABLE&rellifecycle=&reltype=latest

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** to accept 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.

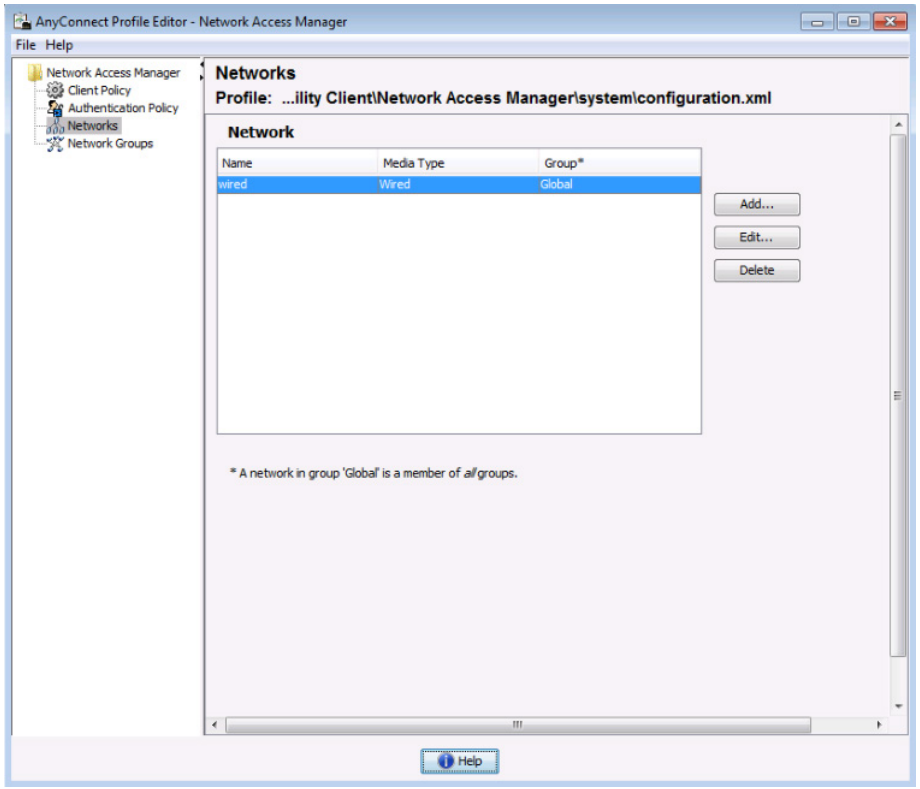
Procedure 3 Create wired profile

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**.

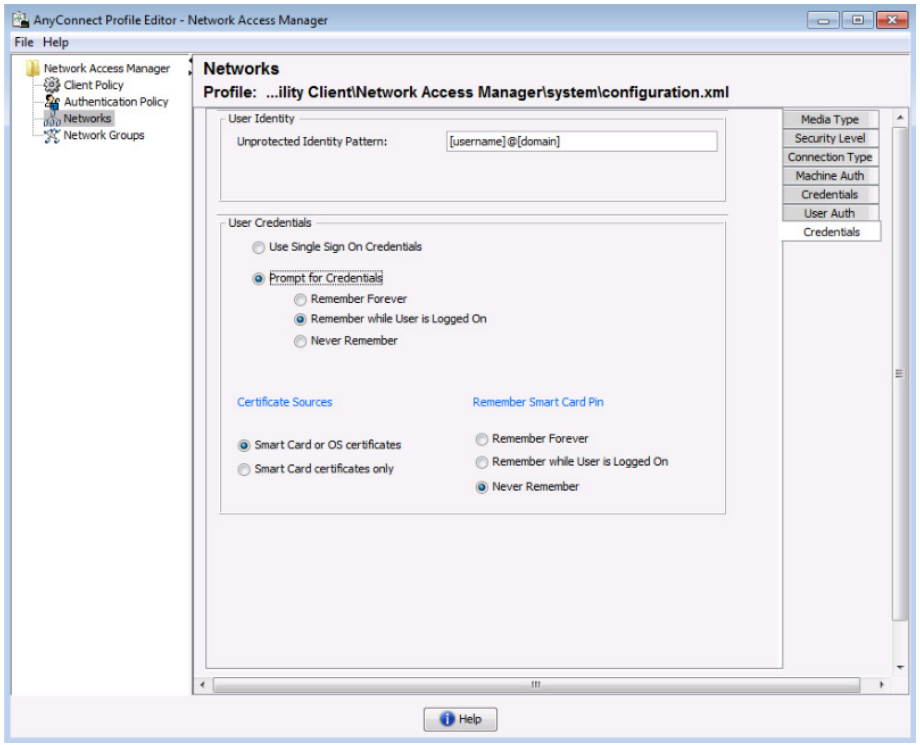
Step 9: For machine identity, enter an unprotected identity pattern. In this deployment, use **host.[domain]**, and then click **Next**.

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**.

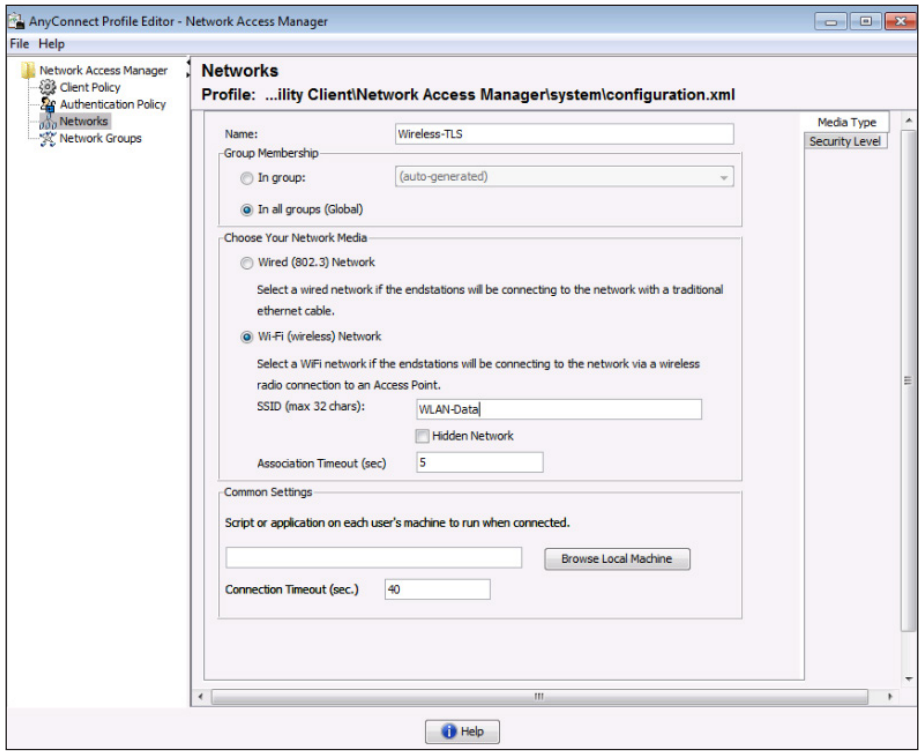


Procedure 4 Create wireless profile

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).

Process

Configuring Mac Workstations for 802.1X Authentication

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

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 10.6.

Procedure 1 Install root certificate on Mac OS X

To install a trusted root certificate on Mac OS X 10.6, 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.

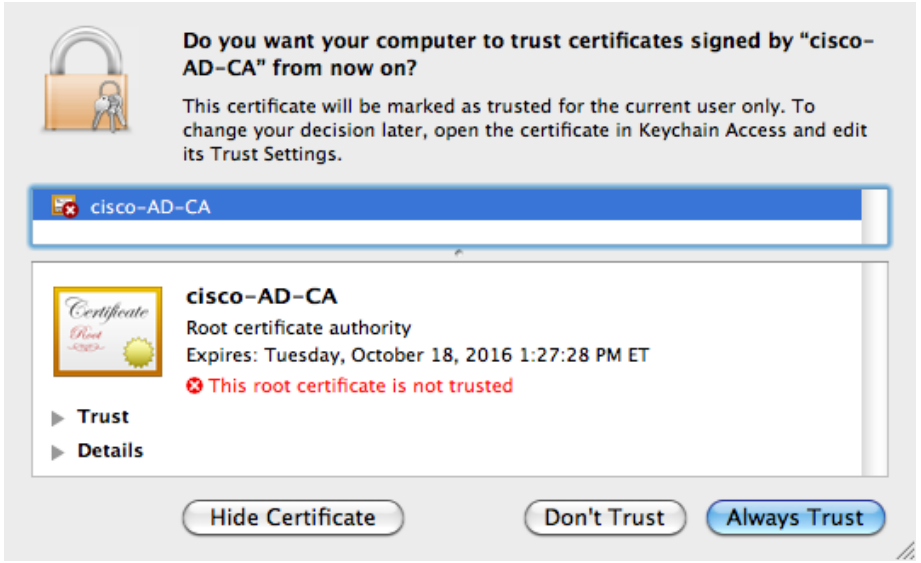
Step 4: Click **Download CA Certificate,** and then save the certificate file.

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

Step 6: Click **Always Trust**.

Tech Tip

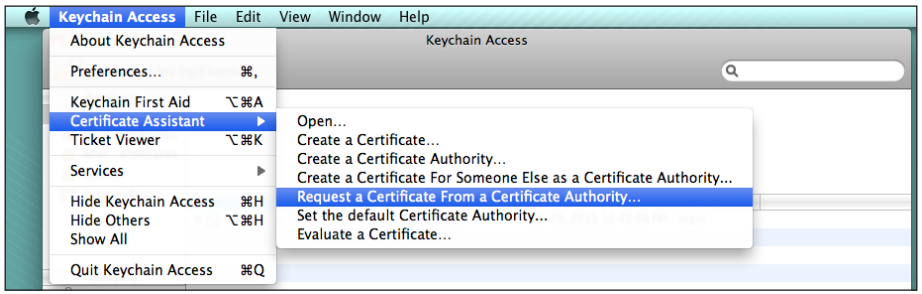
You may be prompted for credentials of a user with permission to change the certificate trust settings.



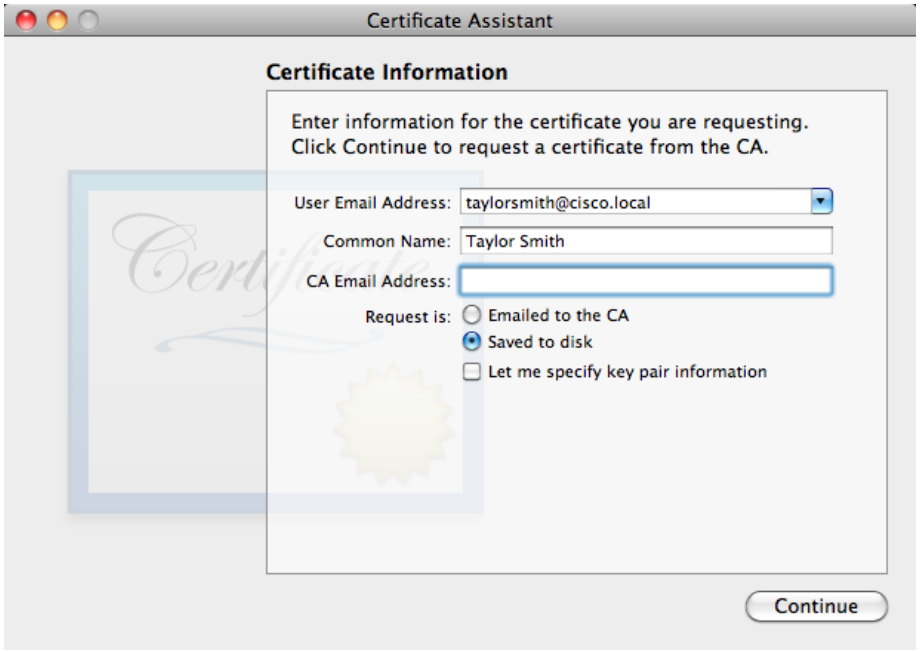
Procedure 2 Request user certificate

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 to go back to the main page of the CA.

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

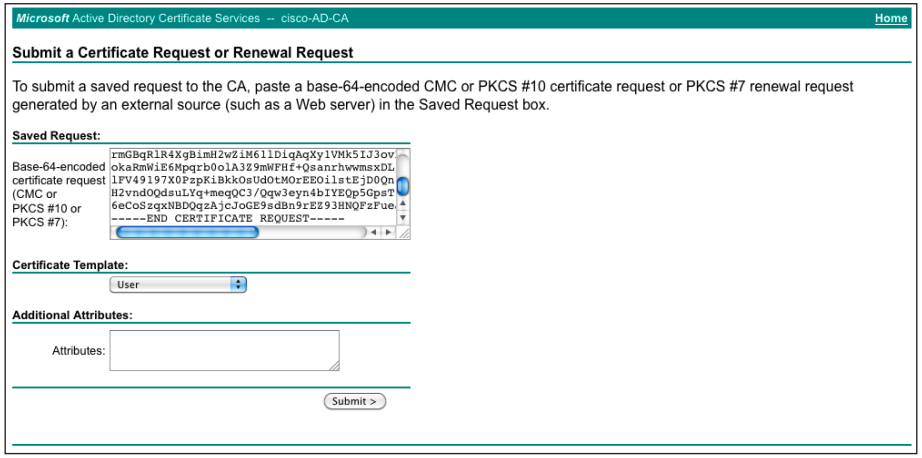
Step 8: Click **advanced certificate request**.

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.

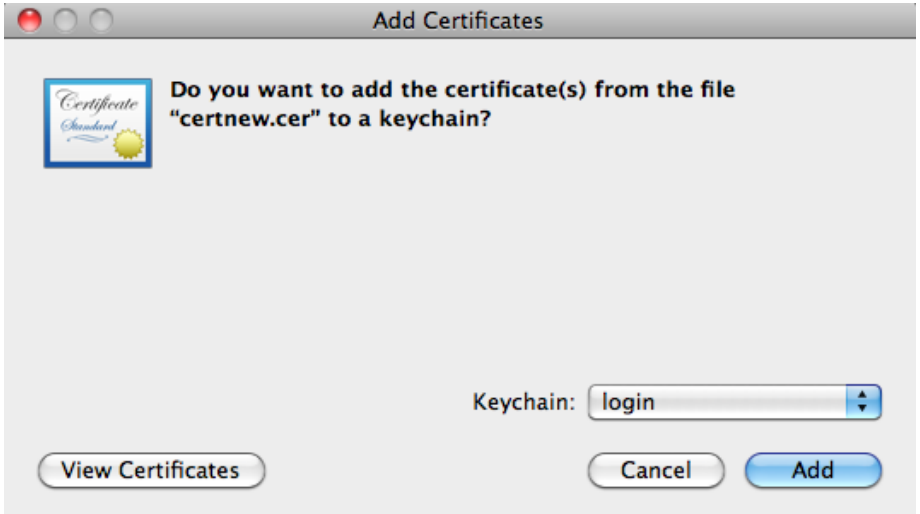
Step 12: In the **Certificate Template** list, choose **User,** and then click **Submit**.



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.

Step 15: In the **Keychain** list, choose **login**, and then click **Add**.



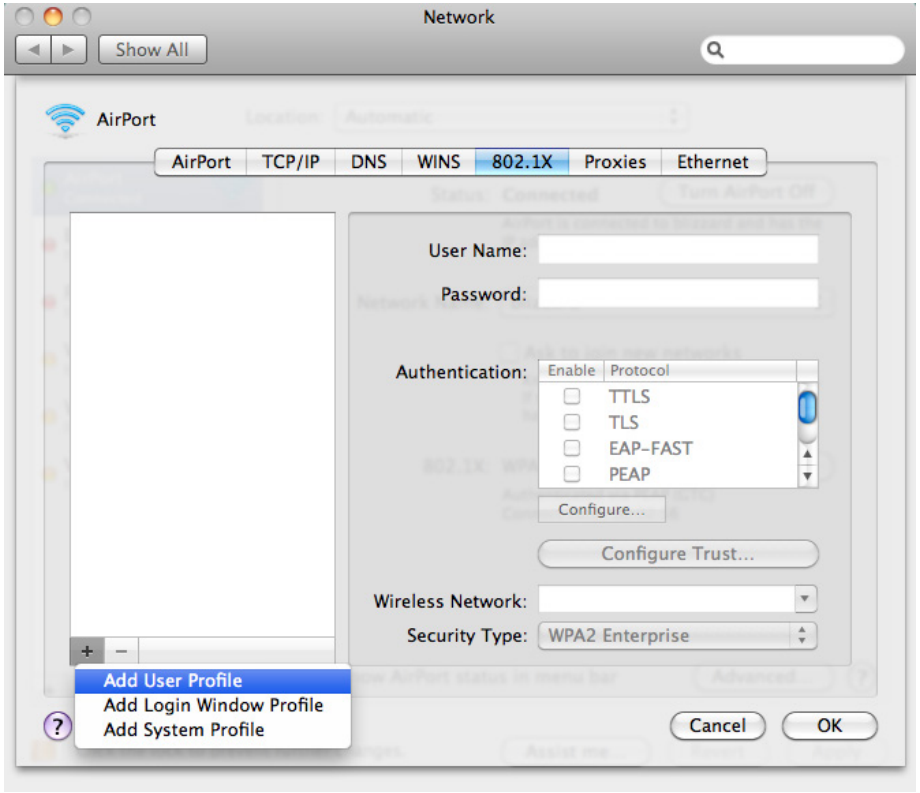
Procedure 3 Configure Mac OS X supplicant

Step 1: On your Mac, launch System Preferences.

Step 2: Double-click **Network**.

Step 3: Click **Advanced,** and then click the **802.1X** tab.

Step 4: Click the **+** symbol, and then select **Add User Profile**.



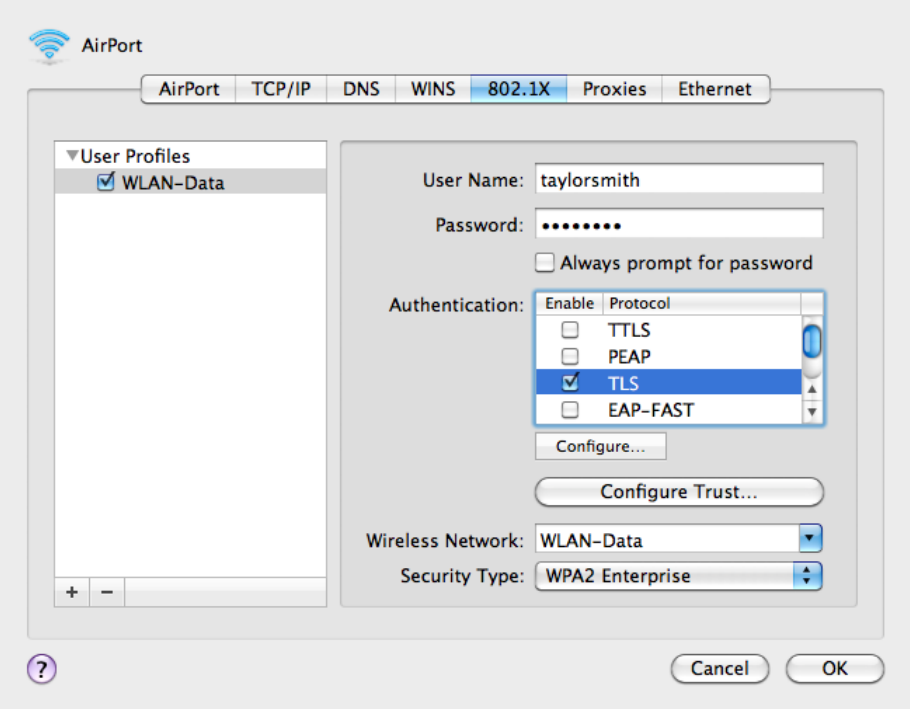
Step 5: Give the profile a name, and then enter your user name and password.

Step 6: In the Authentication section, select **TLS**, and then click **Configure**.

Step 7: Select the certificate for this user, and then click **Continue**.

Step 8: If you are using a wireless connection, in the **Wireless Network** list, choose the wireless network

Step 9: In the **Security Type** list, choose **WPA2 Enterprise**, and then click **OK**.



Step 10: Click **Apply**, and then exit System Preferences.

Repeat this process for all Mac OS X endpoints to deploy certificates and to enable 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).

Enable Authorization

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

The next step would be to deploy some form of authorization to control what authenticated endpoints can access 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 choose **Enabled**.

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

Process

Enabling Authorization for Wireless Access Points

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

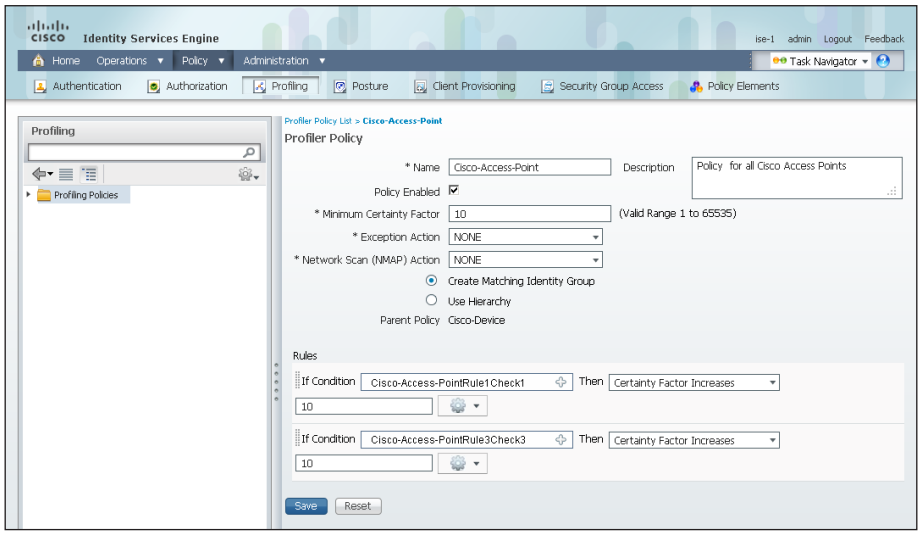
You will create an authorization profile for wireless access points (APs) that is similar to the one for Cisco IP Phones.

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, select **Cisco-Access-Point**.

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



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.

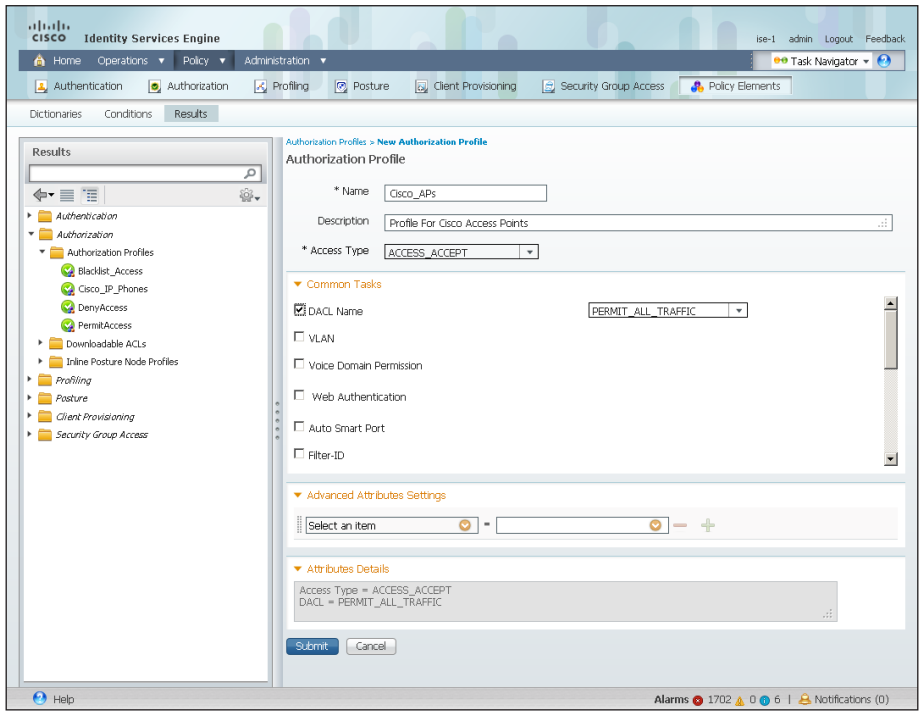
Step 1: On the menu bar, mouse over **Policy**, and then in the Policy Elements section, select **Results**.

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.

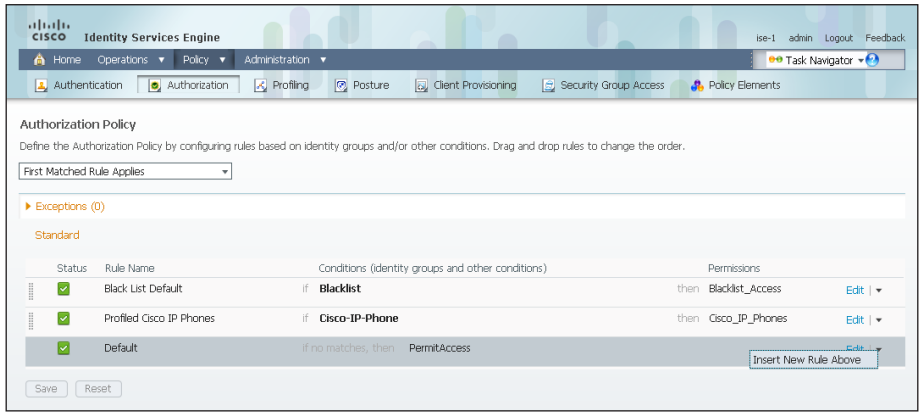
Step 5: Select **DACL Name** and in the list, make sure **PERMIT_ALL_TRAFFIC** is selected, and then click **Submit**.



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.

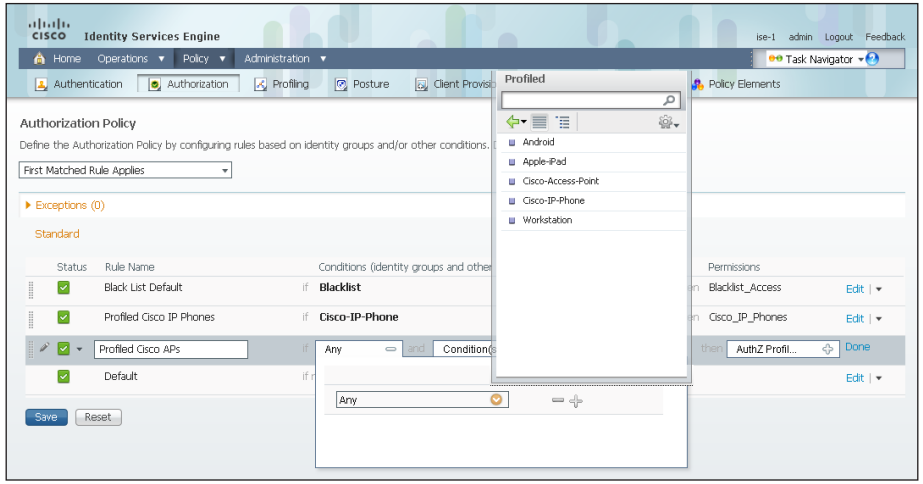


Step 3: Rename the rule **Profiled Cisco APs**.

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

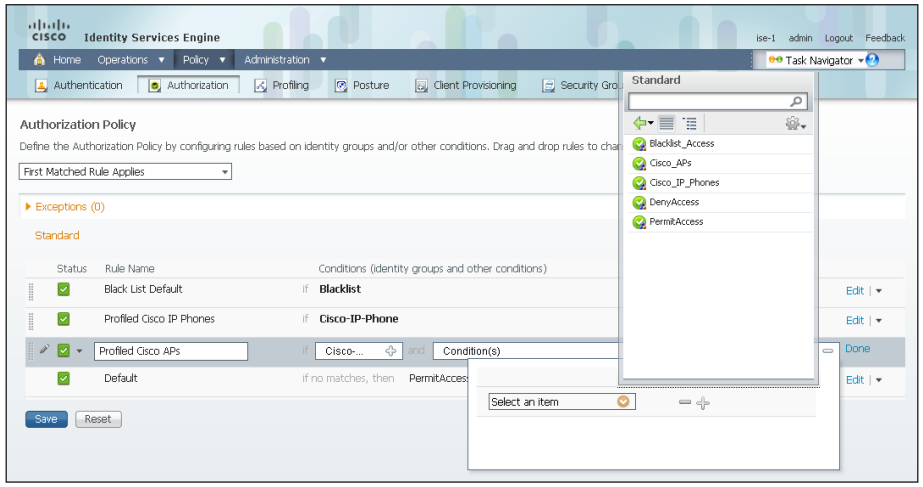
Step 5: From the list, next to **Endpoint Identity Groups**, click the **>** symbol and then next to **Profiled**, click the **>** symbol.

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

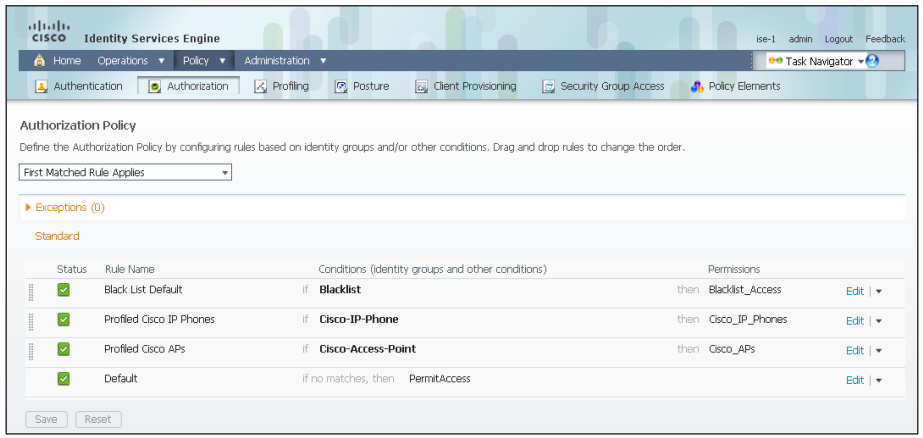


Step 7: Under the Permissions column, next to **AuthZ Profile**, click the **+** symbol.

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

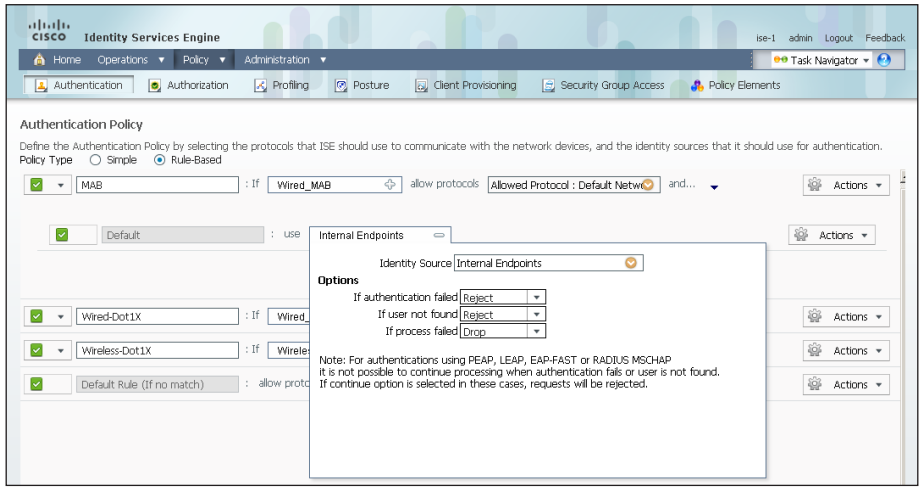
Step 1: On the menu bar, mouse over **Policy**, and then select **Authentication**.

Step 2: On the **MAB** rule, to the right of the **and...**, click the black. 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**.



Process

Enabling Authorization for Wired Endpoints

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

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.

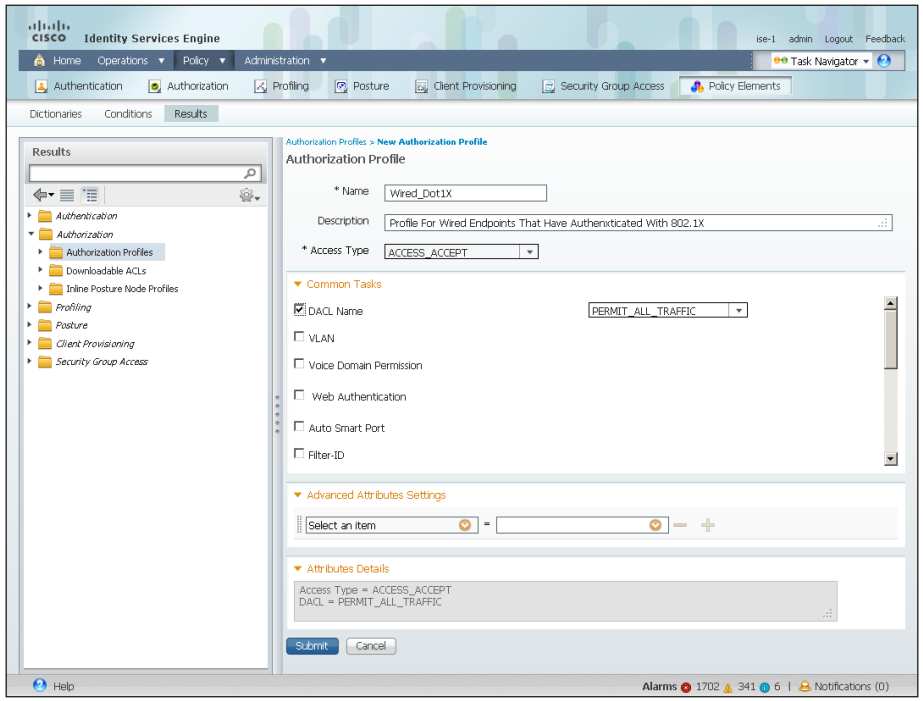
Step 1: On the menu bar, mouse over **Policy**, and then in the Policy Elements section, select **Results**.

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**.

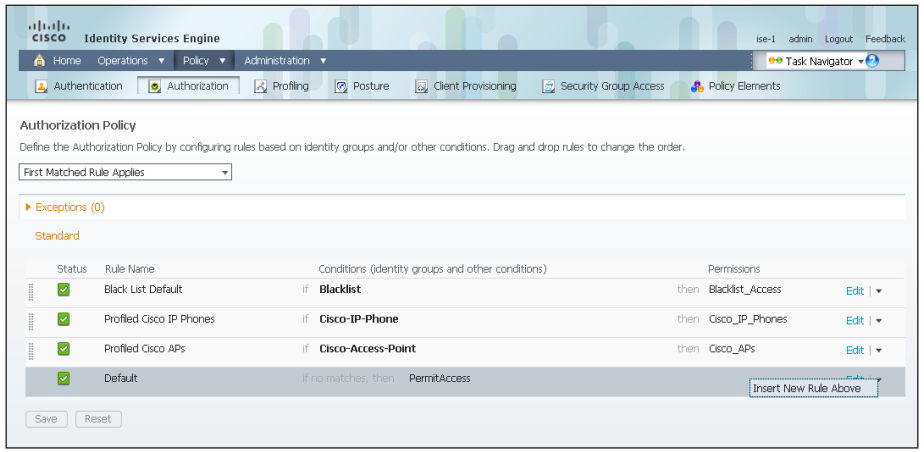


Procedure 2 Create authorization policy

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.

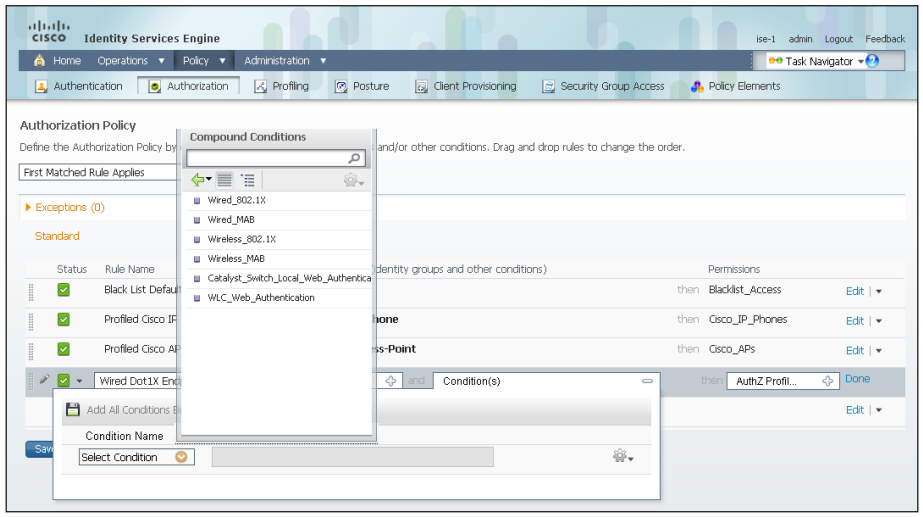


Step 3: Rename the rule Wired Dot1X Endpoints.

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

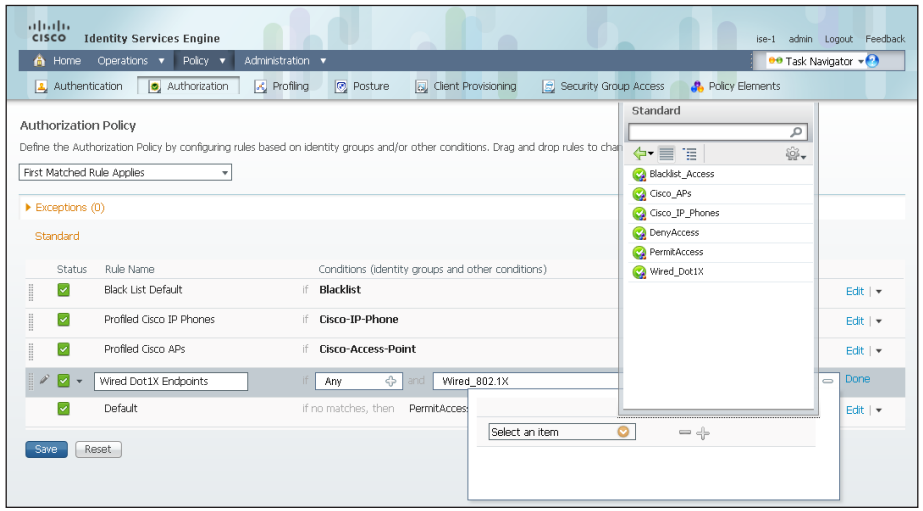
Step 5: Click **Select Existing Condition from Library**.

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

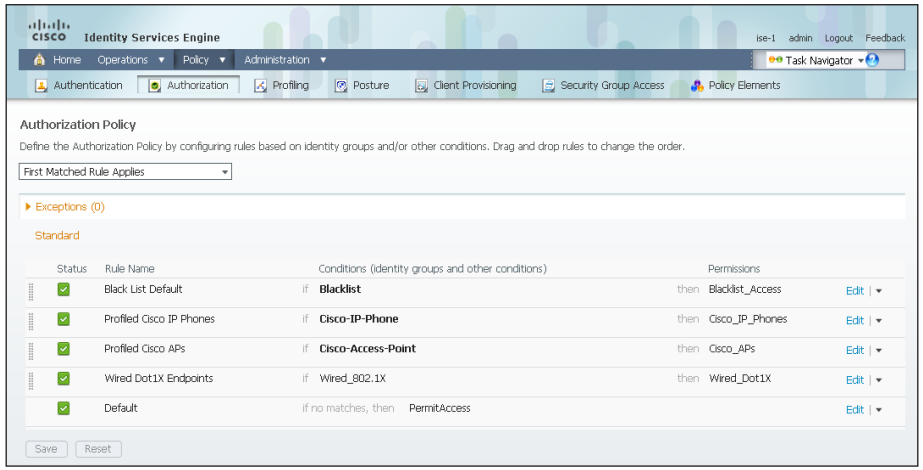


Step 7: Under the Permissions column, next to **AuthZ Profile**, click the **+** symbol.

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. 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.

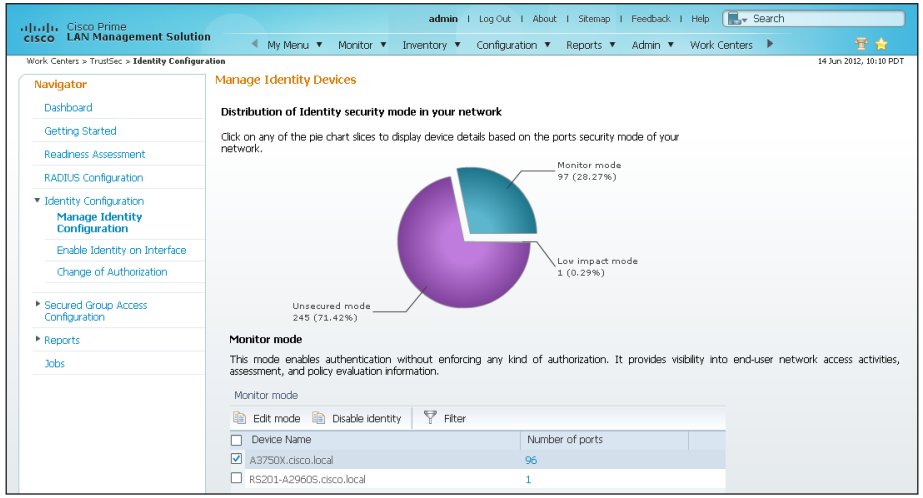
Step 1: Connect to Cisco Prime LMS with a web browser, for example: https://lms.cisco.local.

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

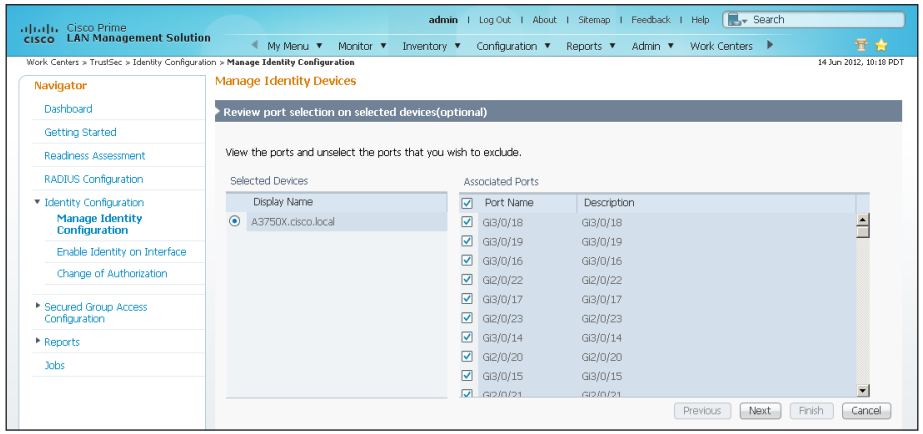
Step 3: In the Navigator panel on the left, click **Manage Identity Configuration**.

Step 4: In the pie chart, click on 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**.



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.

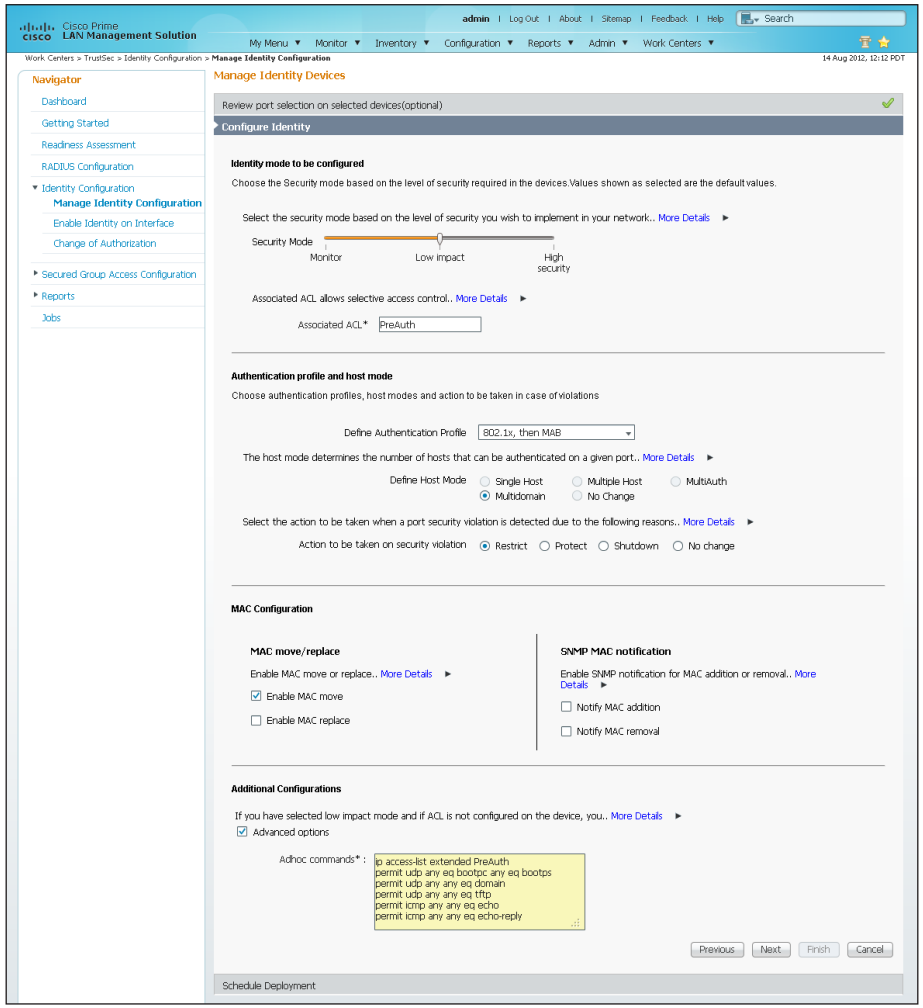
Step 8: In the Authentication profile and host mode section, set the following values:

- 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**.

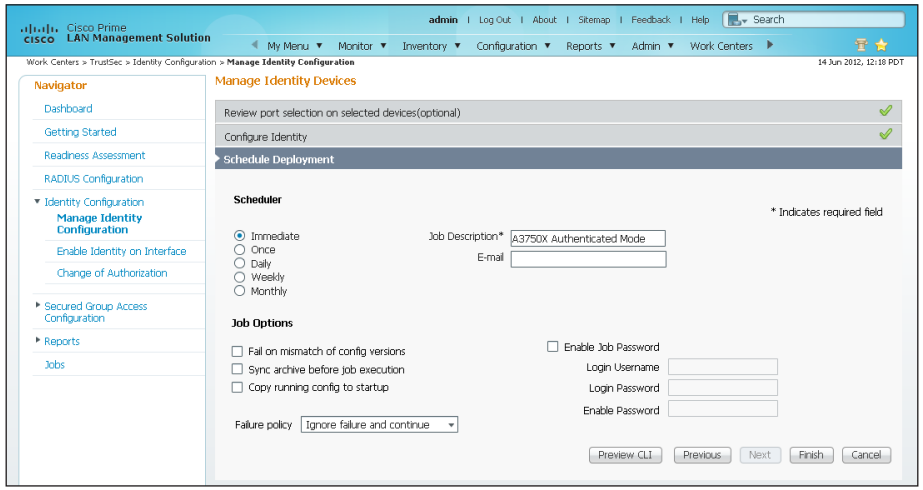
```
ip access-list extended PreAuth
permit udp any eq bootpc any eq bootps
permit udp any any eq domain
permit udp any any eq tftp
permit icmp any any eq echo
permit icmp any any eq echo-reply
```



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 access-list extended PreAuth
permit udp any eq bootpc any eq bootps
permit udp any any eq domain
permit udp any any eq tftp
permit icmp any any eq echo
permit icmp any any eq 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
```

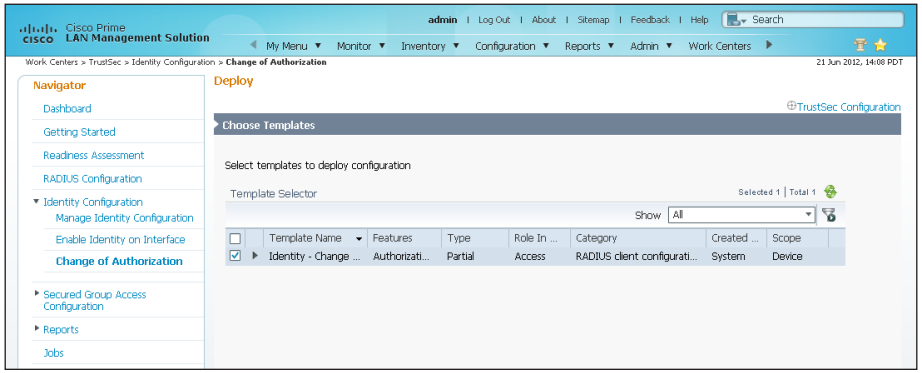
Procedure 4 Enable change of authorization

Authorization requires the use of RADIUS Change of Authorization (CoA) to change the state of the port after authentication. This is not enabled by default, and you will need to enable it. There is a wizard in Cisco Prime LMS 4.2 for this.

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

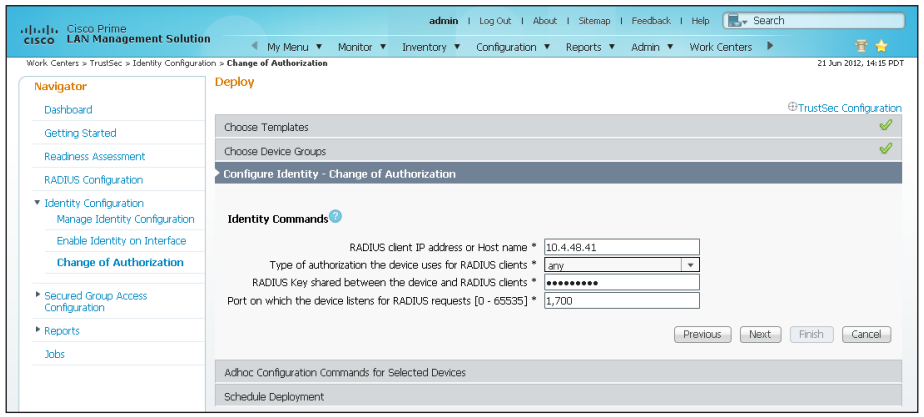
Step 2: In the Navigator panel on the left, click **Change of Authorization**.

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



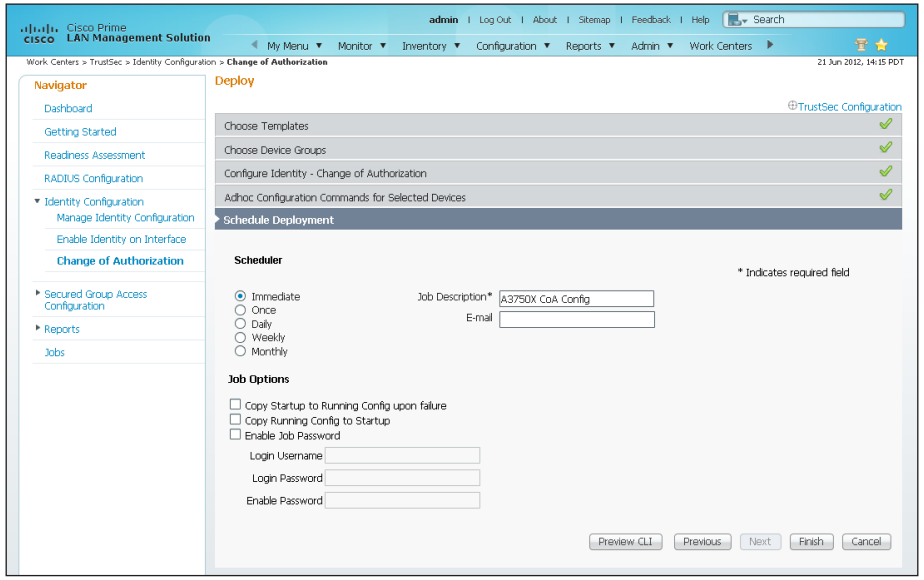
Step 4: In the Device Selector, expand **All Devices**, select the switches you want to enable for CoA, and then click **Next**.

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**.



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
```

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.

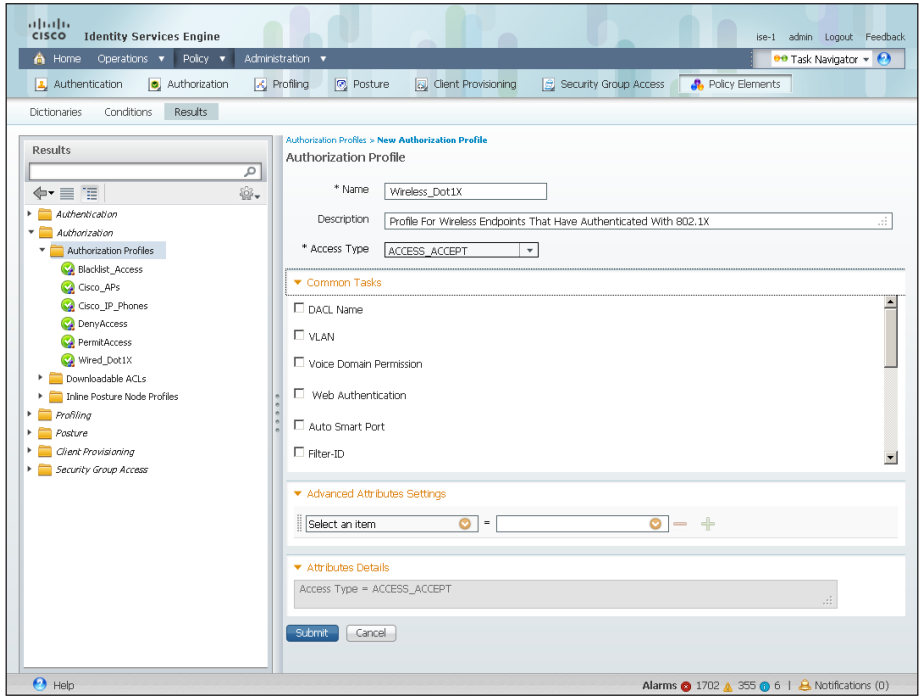
Step 1: On the menu bar, mouse over **Policy**, and then in the Policy Elements section, select **Results**.

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**.

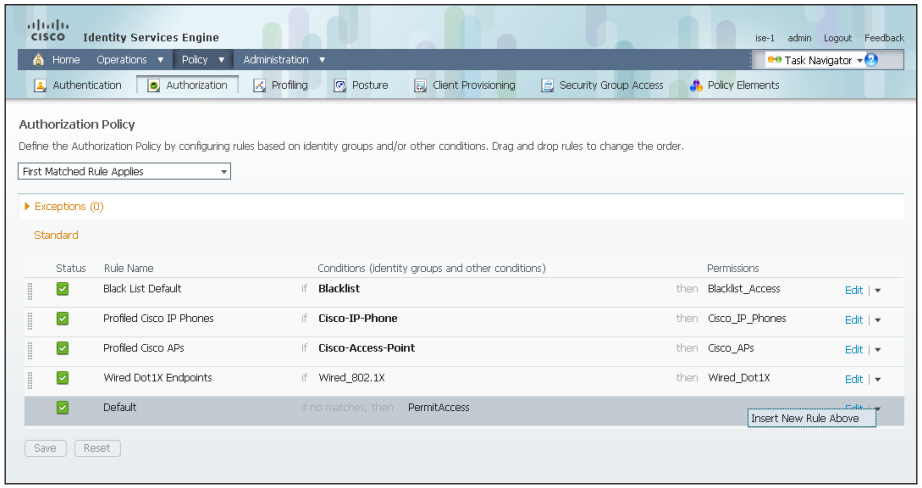


Procedure 2 Create authorization policy

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.

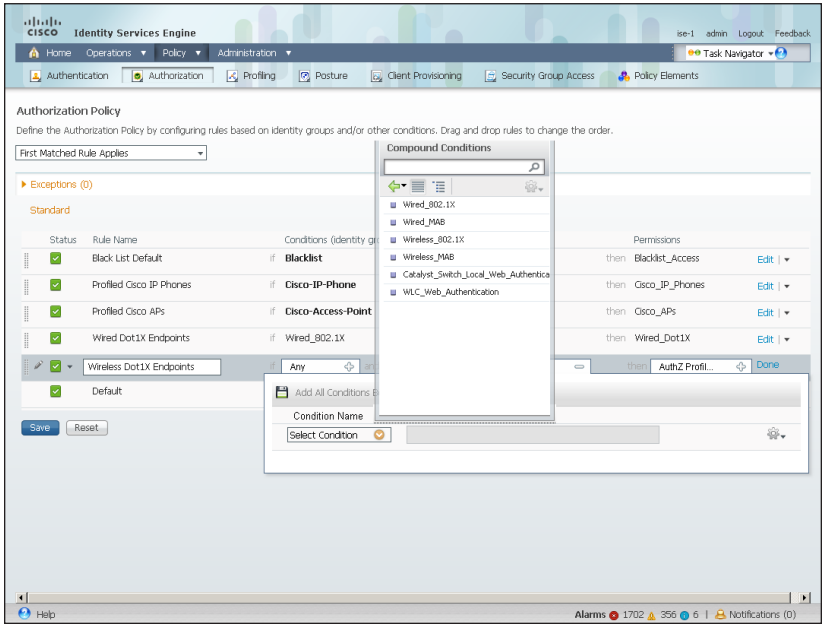


Step 3: Rename the rule **Wireless Dot1X Endpoints**.

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

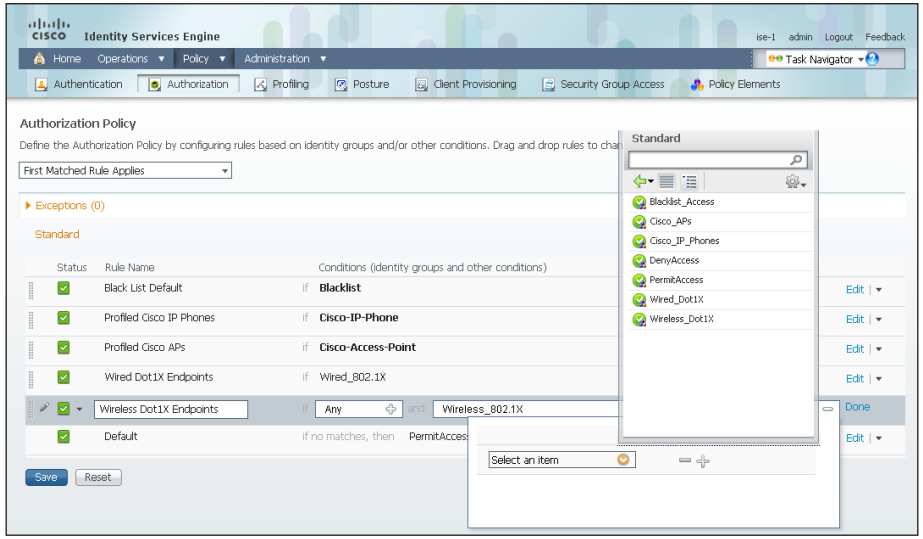
Step 5: Click **Select Existing Condition from Library**.

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

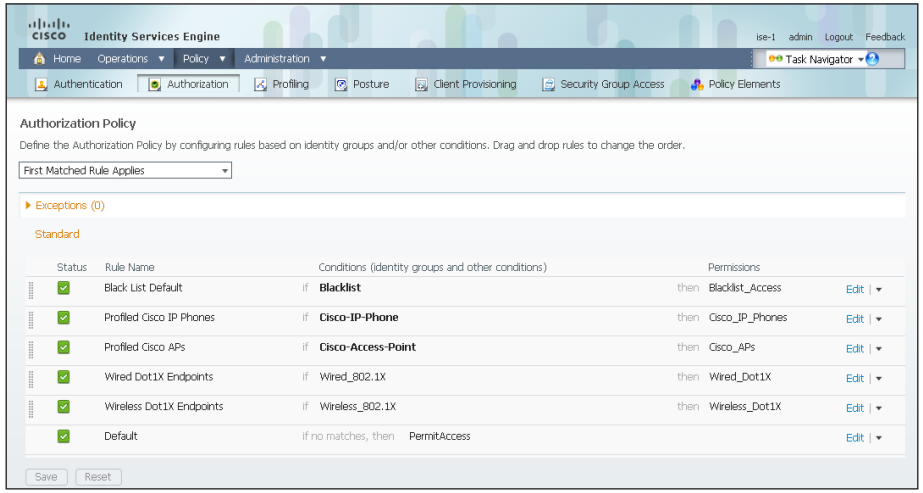


Step 7: Under the Permissions column, next to **AuthZ Profile**, click the + symbol.

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

Modify 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.

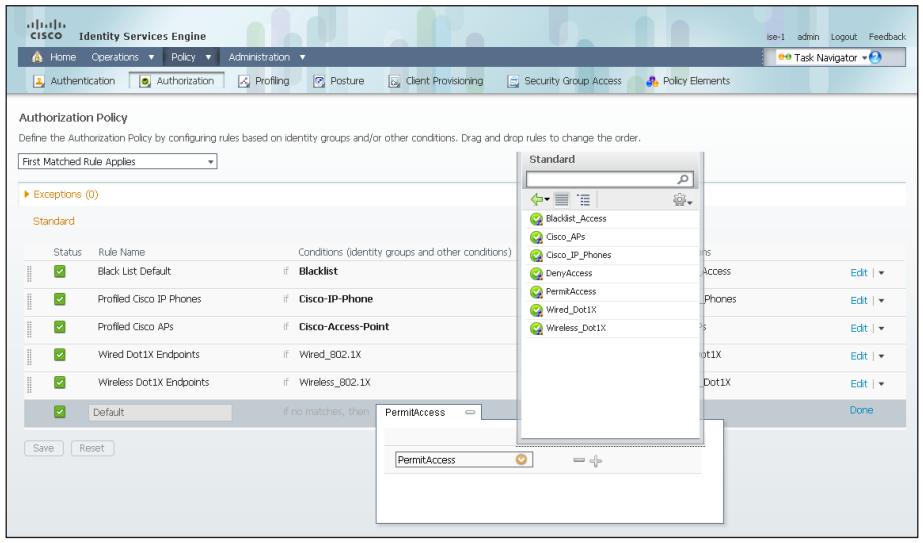
Procedure 1 Modify default rule

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

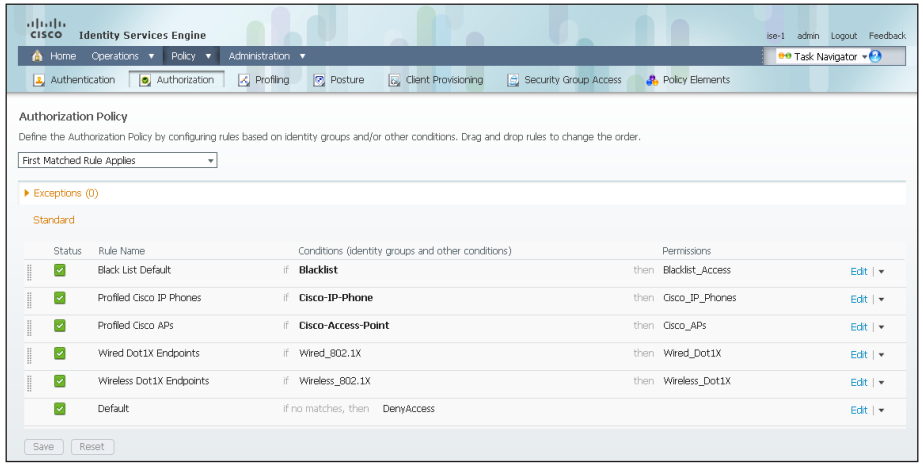
Step 2: For the default rule, click **Edit**.

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**.



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



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.

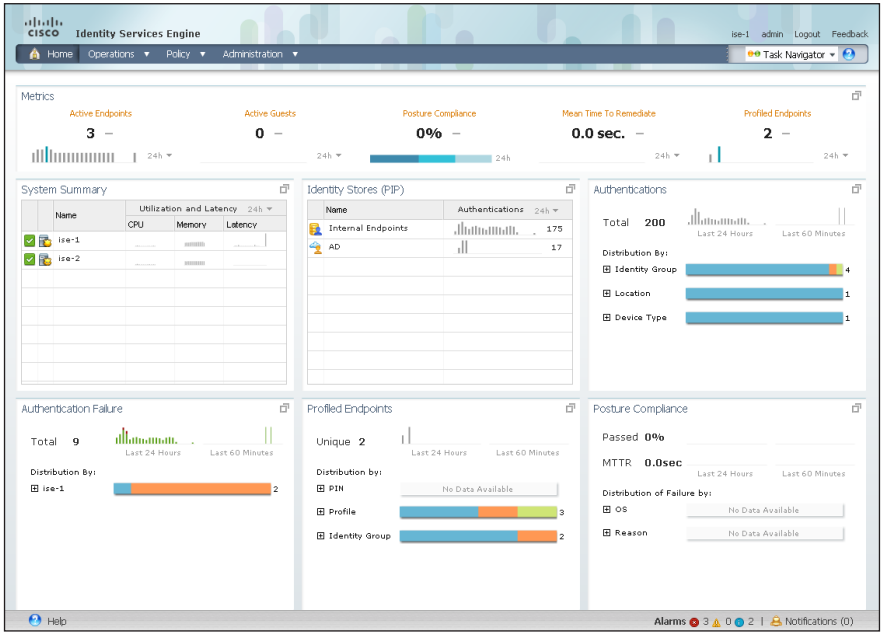
Cisco ISE is now configured to authenticate users and to profile endpoints based on RADIUS and DHCP information. The reporting capabilities of Cisco ISE allow you to determine what type of device is connecting to your network, when it connects, and where it connects from. Also, you will know who is connecting 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

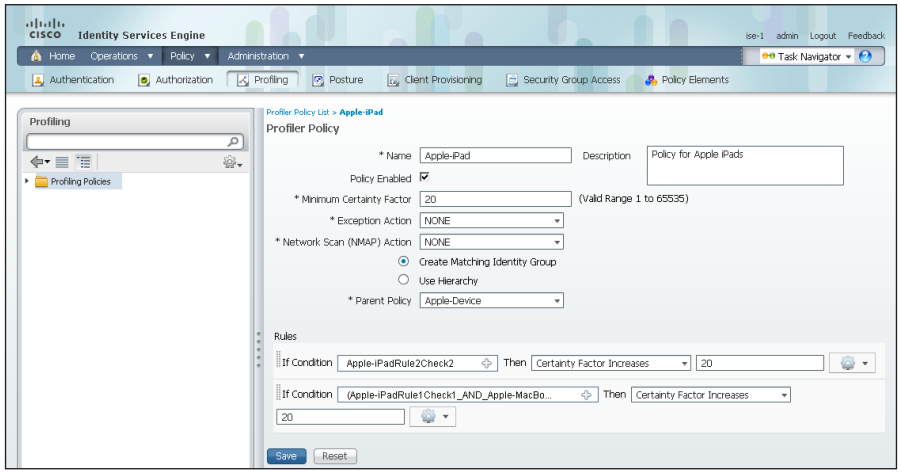
Cisco ISE has more in-depth reporting options to give more details on the devices connecting to the network. To help identify the endpoints, you can use identity groups to classify profiled endpoints and to generate reports.

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 Cisco Cius using information obtained from the device's DHCP request.

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

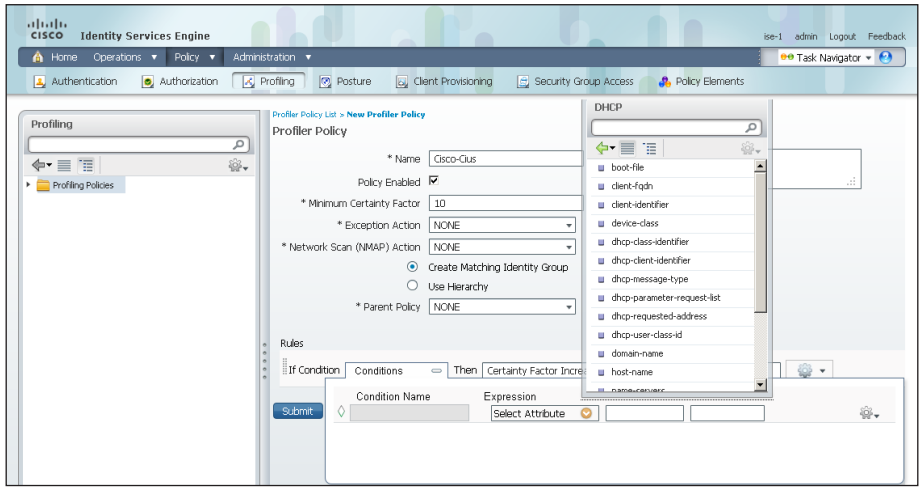
Step 2: Mouse over **Policy**, and then, from the drop-down menu, choose **Profiling**.

Step 3: Click **Add**.

Step 4: Give the policy the name **Cisco-Cius** and a description.

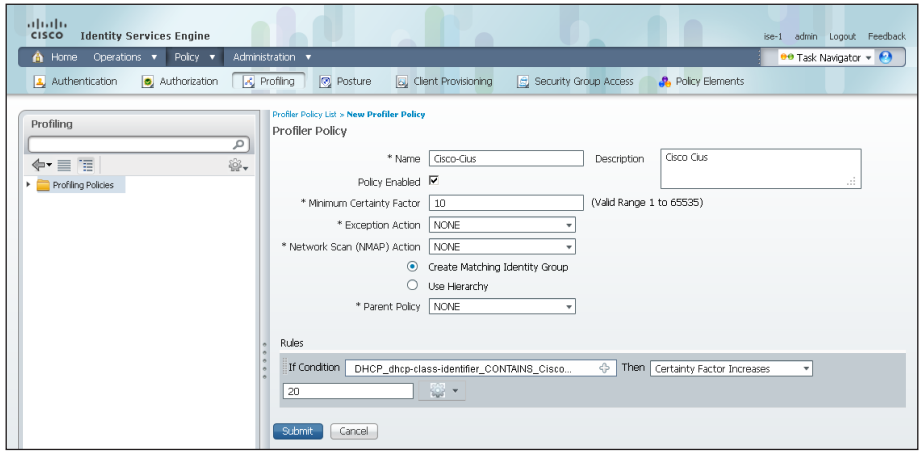
Step 5: In the rules section, next to **Conditions**, click the **+** symbol, and then click **Create New Condition (Advance Option)**.

Step 6: In the **Expression** list, next to **DHCP**, click the **>** symbol, and then select **dhcp-class-identifier**.



Step 7: In the second list, choose **CONTAINS**, and then, in the final box, enter **Cisco Cius**.

Step 8: Choose **Certainty Factor Increases**, set the value to **20**, and then click **Submit**.



Procedure 4 Examining the authentication log

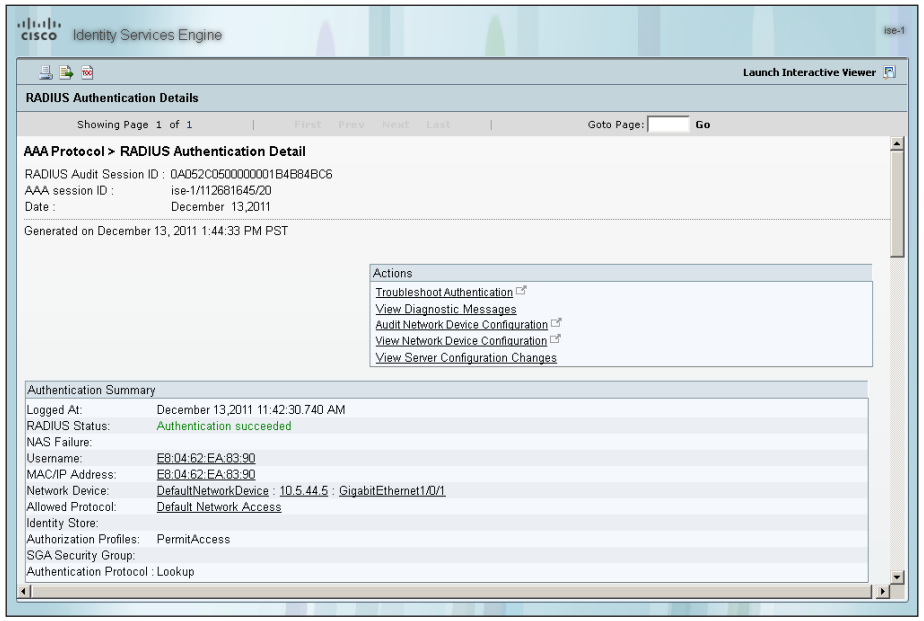
Step 1: On the menu bar, mouse over **Operations**, and then choose **Authentications**. The authentication log displays. The default option is to display the last 20 records from the last 24 hours.

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.

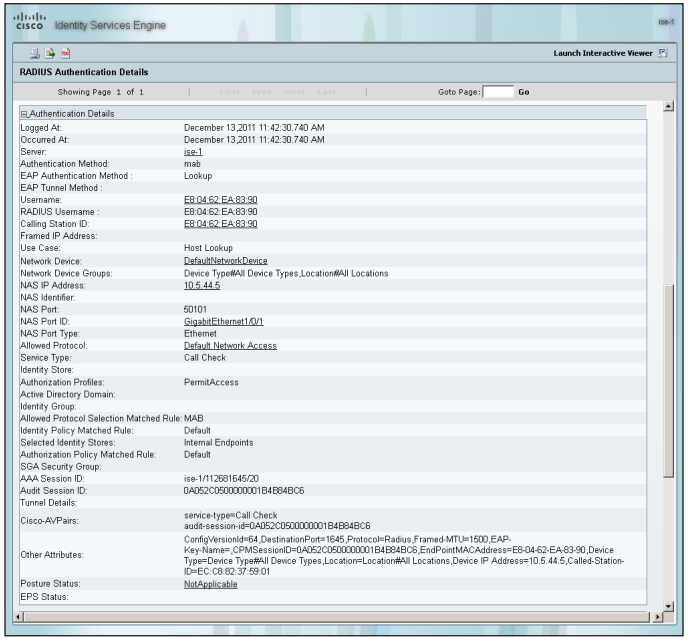
If the device was able to be profiled, that information is displayed.

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.



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.

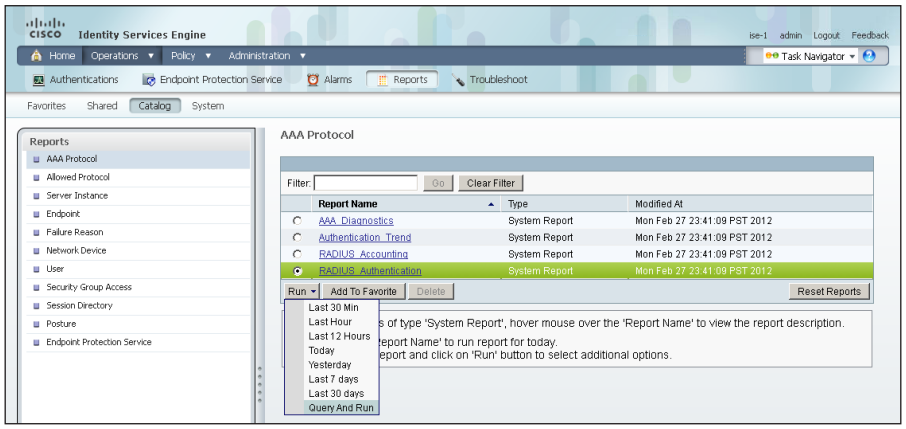
Step 1: On the menu bar, mouse over **Operations**, and then, in the Reports section, choose **Catalog**.

Step 2: In the left pane, select **AAA Protocol**.

Step 3: Select **RADIUS Authentication**.

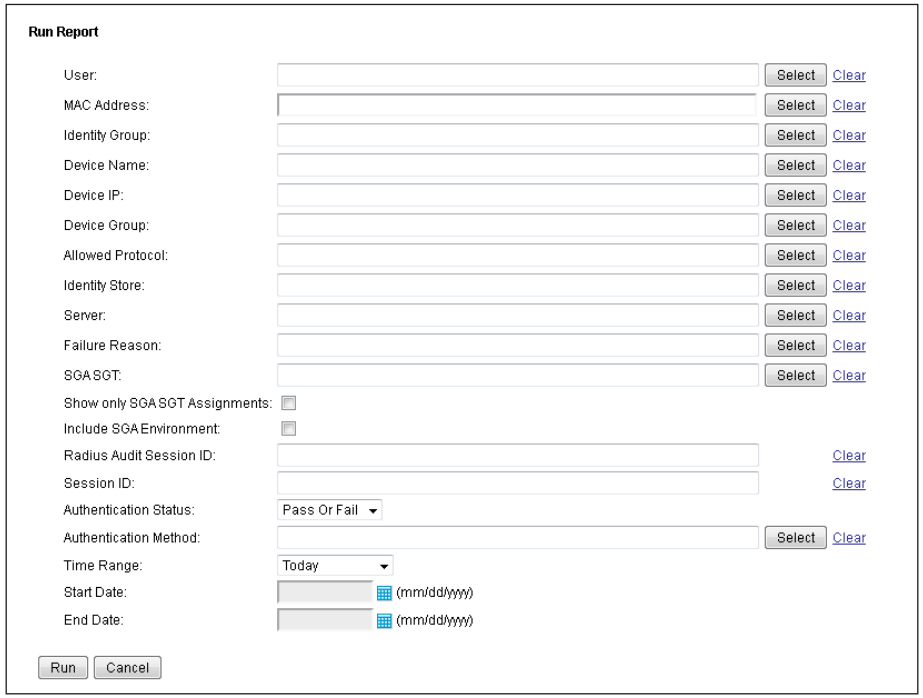
Step 4: Click **Run**. Different time ranges for producing the default report are displayed.

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. After choosing the parameters you want, click **Run** to generate the report.

Figure 2 - RADIUS report parameters



Procedure 6 Identify endpoints

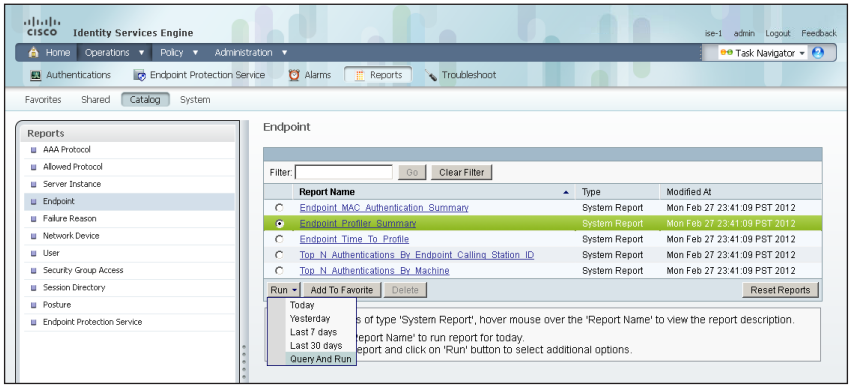
Using information gleaned from the RADIUS and DHCP requests, Cisco ISE can identify what types of devices are connecting to the network. This can assist in determining the network security policy based on the type of device that is in use.

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**.

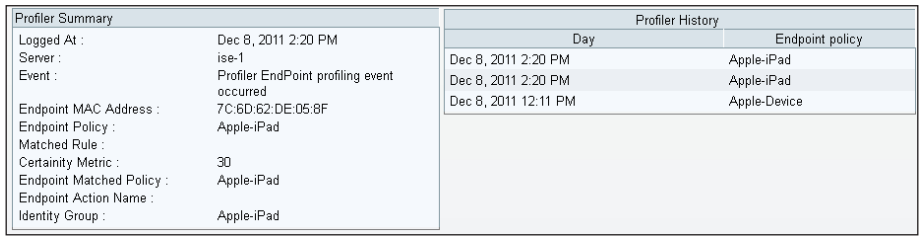
Step 4: Select the desired time period to run the report.



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	
Logged At :	Dec 8, 2011 2:20 PM
Server :	ise-1
Event :	Profiler EndPoint profiling event occurred
Endpoint MAC Address :	7C:6D:62:DE:05:8F
Endpoint Policy :	Apple-iPad
Matched Rule :	
Certainity Metric :	30
Endpoint Matched Policy :	Apple-iPad
Endpoint Action Name :	
Identity Group :	Apple-iPad

Profiler History	
Day	Endpoint policy
Dec 8, 2011 2:20 PM	Apple-iPad
Dec 8, 2011 2:20 PM	Apple-iPad
Dec 8, 2011 12:11 PM	Apple-Device

Figure 4 - Endpoint Details

Endpoint > Endpoint Profiler Detail

Generated on December 13, 2011 1:59:11 PM PST

Endpoint Session time : Not Applicable

Endpoint Details

Endpoint Static Assignment :
Endpoint Source :
Endpoint OUI : Apple, Inc
Endpoint Host Name :
Endpoint Subnet :
Endpoint NAD Address : 10.4.46.65
Endpoint VLAN :
Endpoint FQDN :
Endpoint Nameserver :
Endpoint Property : CPMSessionID=0a042e41000000494ee13838
StaticAssignment=false
NetworkDeviceGroups=Device Type#All Device Types
Location#All Locations
cisco-av-pair=audit-session-id=0a042e41000000494ee13838
Calling-Station-ID=7c-6d-62-de-05-8f
DestinationPort=1812
AcsSessionID=ise-1/112681645/7
giaddr=10.4.16.6
Device Type=Device Type#All Device Types
Service-Type=Framed
NAS-Identifier=WLC-2
TimeToProfile=25
LastNmapScanTime=0
dhcp-client-identifier=01:7c:6d:62:de:05:8f
StaticGroupAssignment=false
dhcp-requested-address=128.107.108.109
AuthenticationMethod=MSCHAPV2
EapAuthentication=EAP-MSCHAPv2
NetworkDeviceName=DefaultNetworkDevice
NAS-Port-Type=Wireless - IEEE 802.11
op=BOOTREQUEST
PostureAssessmentStatus=NotApplicable
IdentityGroupID=3e7f9a90-21db-11e1-aebd-005056a90008
Total Certainty Factor=30
User-Name=patjones
ciaddr=0.0.0.0
AuthenticationIdentityStore=AD1
dhcp-parameter-request-list=1
3
6
15
119
252
MatchedPolicyID=f7679880-116b-11e1-ae1c-0050569e2146
DestinationIPAddress=10.4.48.41
NAS-Port=13
ADDomain=cisco.local
NmapScanCount=0
dhcp-message-type=DHCPDISCOVER
htype=Ethernet (10Mb)
EndPointMACAddress=7C-6D-62-DE-05-8F
ServiceSelectionMatchedRule=Wireless-Dot1X
PortalUser=
EndPointMatchedProfile=Apple-Device
RequestLatency=9
EapTunnel=PEAP
AuthState=Authenticated
Airespace-Wlan-Id=1
hlen=6
hops=2
host-name=SBA-iPad
FirstCollection=1323375086686
EndPointPolicyID=f7679880-116b-11e1-ae1c-0050569e2146
SelectedAccessService=Default Network Access
secs=0
AuthorizationPolicyMatchedRule=Default
IdentityPolicyMatchedRule=Default
MessageCode=5200
DeviceRegistrationStatus=0
SelectedAuthorizationProfiles=PermitAccess
IdentityAccessRestricted=false
SelectedAuthenticationIdentityStores=AD1
flags=0x0000
chaddr=7c:6d:62:de:05:8f
yiaddr=0.0.0.0
Response={User-Name=patjones; State=ReauthSession:0a042e41000000494ee13838; Class=CACS:0a042e41000000494ee13838:ise-1/112681645/7; Termination-Action=RADIUS-Request; MS-MPPE-Send-Key=49:7c:f0:b6:89:6b:18:b0:d1:91:ca:89:44:25:3a:6f:fb:ef:85:7c:45:98:3d:59:1b:5f:a3:67:d4:d2:2e:f0; MS-MPPE-
Recv-Key=c9:0b:04:f9:4e:9b:24:a8:9e:c1:5f:38:65:fc:e3:7d:eb:0a:5e:40:46:24:1b:aa:ee:0a:d7:4c:b4:fa:96:51; }
Location=Location#All Locations
PolicyVersion=1
Device IP Address=10.4.46.65
NmapSubnetScanID=0
Called-Station-ID=1c-17-d3-cb-48-50:WLAN-Data

Procedure 7 Create device-type reports

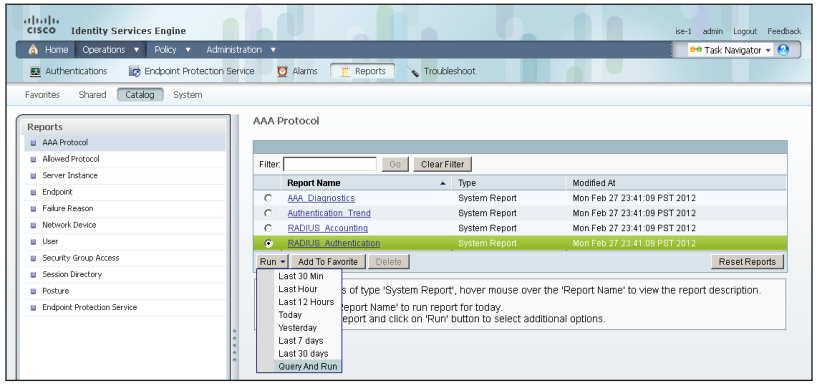
You can create reports to identify specific devices based on the identity groups configured previously. This example uses the group created to identify Apple iPads.

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**.

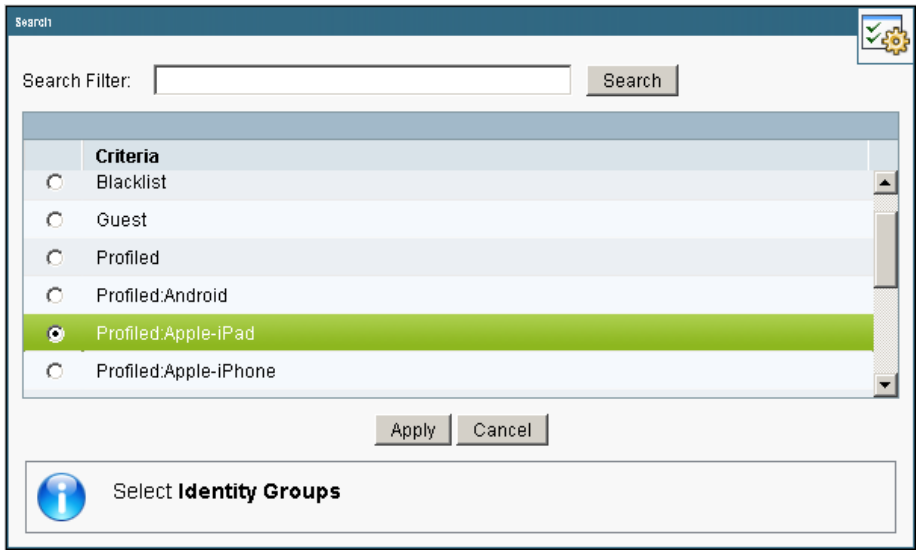
Step 4: Click **Run,** and then choose **Query and Run**.



Step 5: For the identity group you want to query, next the Identity Group field, click **Select**. A search window appears.

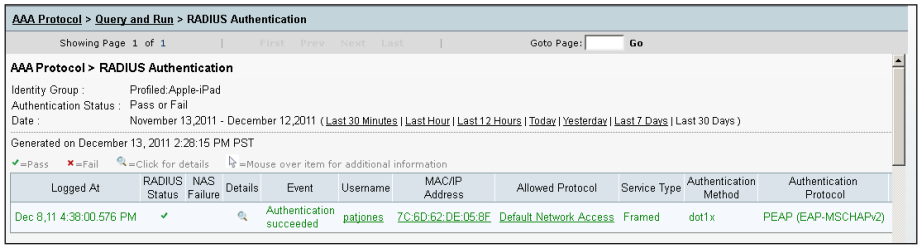
Step 6: Leave the search field empty, and then click **Search**. The search returns all groups.

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



Appendix A: Product List

Network Management

Functional Area	Product Description	Part Numbers	Software
Identity Management	Cisco Identity Services Engine Virtual Appliance	ISE-VM-K9=	1.1.1.268
	Cisco ISE Base License for 10,000 Endpoints	L-ISE-BSE-10K=	
	Cisco ISE Base License for 5000 Endpoints	L-ISE-BSE-5K=	
	Cisco ISE Base License for 3500 Endpoints Cisco ISE Base License for 2500 Endpoints	L-ISE-BSE-3500= L-ISE-BSE-2500=	
	Cisco ISE Advanced 3-year License for 10,000 Endpoints	L-ISE-ADV3Y-10K=	
	Cisco ISE Advanced 3-year License for 5000 Endpoints	L-ISE-ADV3Y-5K=	
	Cisco ISE Advanced 3-year License for 3500 Endpoints	L-ISE-ADV3Y-3500=	
	Cisco ISE Advanced 3-year License for 2500 Endpoints	L-ISE-ADV3Y-2500=	
Network Management	Cisco Prime Infrastructure 1.1	R-PI-1.1-K9	4.2
	Prime Infrastructure 1.1 Software – 5K Device Base Lic	R-PI-1.1-5K-K9	
	Prime Infrastructure 1.1 Software – 2.5K Device Base Lic	R-PI-1.1-2.5K-K9	
	Prime Infrastructure 1.1 Software – 1K Device Base Lic	R-PI-1.1-1K-K9	
	Prime Infrastructure 1.1 Software – 500 Device Base Lic	R-PI-1.1-500-K9	
	Prime Infrastructure 1.1 Software – 100 Device Base Lic	R-PI-1.1-100-K9	
	Prime Infrastructure 1.1 Software – 50 Device Base Lic	R-PI-1.1-50-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	3.3.0.SG(15.1-1SG) IP Base
	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 3750-X Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-48PF-S	15.0(1)SE2 IP Base
	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	
Standalone Access Layer Switch	Cisco Catalyst 3560-X Series Standalone 48 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-48PF-S	15.0(1)SE2 IP Base
	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(1)SE2 LAN Base
	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	7.2.110.0
	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	
On Site Controller	Cisco 2500 Series Wireless Controller for up to 50 Cisco access points	AIR-CT2504-50-K9	7.2.110.0
	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	

Appendix B: Changes

This appendix summarizes the changes to this guide since the previous Cisco SBA series.

- We upgraded the Cisco ISE appliances to software version 1.1.1.268.
- We upgraded the Cisco Wireless LAN Controllers to software version 7.2.110.0.
- We upgraded the Cisco Catalyst 2960-S Series, 3560-X Series, and 3750-X Series switches to Cisco IOS version 15.0(1)SE2.
- We upgraded the Cisco Catalyst 4500 E-Series switches to Cisco IOS XE version 3.3.0.SG (15.1-1SG).
- We upgraded Cisco Prime LMS to software version 4.2.
- We upgraded the Cisco ASA 5500 Series firewall to software version 8.6(1).
- We moved from a monitor mode deployment of 802.1X to a low-impact mode deployment, to include authorization, which enables denying network access to devices that do not authenticate, with an exception made for Cisco IP Phones and access points.
- We modified the ISE deployment such that it now consists of four appliances—a primary and secondary policy service and administration node and a primary and secondary monitoring node.
- We deployed the Device Sensor feature on the switches and wireless LAN controllers, to simplify the profiling configuration and eliminate the need to send copies of DHCP requests to the Cisco ISE appliances.

Notes

Feedback

Click here to provide feedback to Cisco SBA.

SMART BUSINESS ARCHITECTURE

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.

B-0000138-1 8/12