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.

LAN and WLAN 802.1X Deployment Guide

SMART BUSINESS ARCHITECTURE

February 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 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.

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 2011 are the "August 2011 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 forum at the bottom of one of the following sites:

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

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

An RSS feed is available if you would like to be notified when new comments are posted.

Table of Contents

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

What's In This SBA Guide

About SBA

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.

For more information, see the *How to Get Started with Cisco SBA* document:

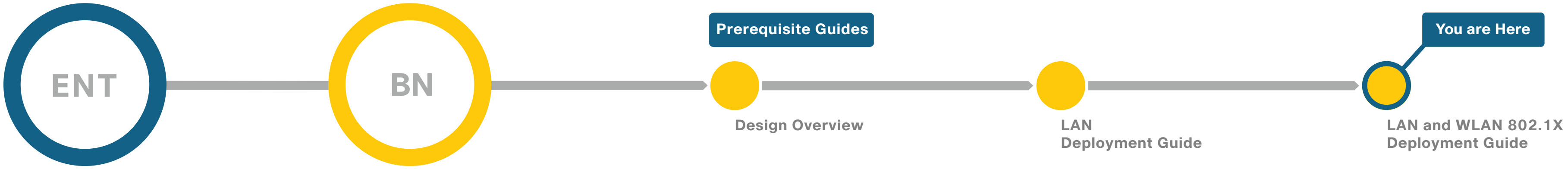
http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Smart_Business_Architecture/SBA_Getting_Started.pdf

About This Guide

This *additional deployment guide* includes the following sections:

- Business Overview—The challenge that your organization faces. Business decision makers can use this section to understand the relevance of the solution to their organizations' operations.
- Technology Overview—How Cisco solves the challenge. Technical decision makers can use this section to understand how the solution works.
- Deployment Details—Step-by-step instructions for implementing the solution. Systems engineers can use this section to get the solution up and running quickly and reliably.

This guide presumes that you have read the prerequisites guides, as shown on the Route to Success below.



Route to Success

To ensure your success when implementing the designs in this guide, you should read any guides that this guide depends upon—shown to the left of this guide on the route above. Any guides that depend upon this guide are shown to the right of this guide.

For customer access to all SBA guides: http://www.cisco.com/go/sba
For partner access: http://www.cisco.com/go/sbachannel

Introduction

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 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.

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 like 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 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 like enforcement, guest access, and confidentiality.

Technology Overview

Cisco Identity Services Engine (ISE) is an identity and access control policy platform that enables enterprises 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 like access switches, wireless controllers, and VPN gateways.

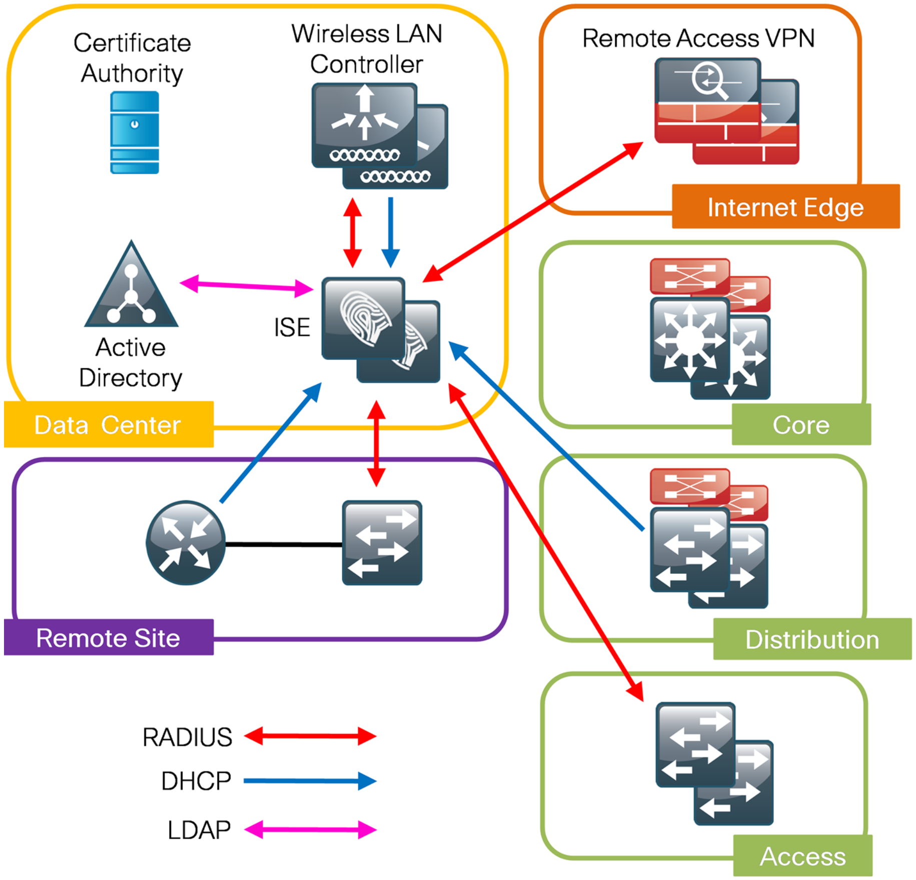
This deployment uses Cisco ISE as the authentication and accounting server for the wired and wireless networks as well as for remote access VPN users who connect using RADIUS. Cisco ISE acts as a proxy to the existing Active Directory (AD) services to maintain a centralized identity store for all network services.

In addition to authentication, this deployment uses Cisco ISE to profile devices 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, and 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 copies of the DHCP requests to Cisco ISE for analysis. The engine then evaluates the DHCP request and can identify the device based off of the data in the request. For example, Cisco IP Phones are identified by their DHCP class identifier.

In the LAN, there are three modes for deploying TrustSec: monitor mode, authenticated mode, and enforcement mode. Cisco recommends a phased deployment model that can allow for limited impact on network access while gradually introducing authentication/authorization on the network. This document covers the deployment of monitor mode both at the headquarters site and the remote sites, with Cisco ISE being centralized in the data center. The monitor mode deployment in use deploys two features within 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 us to prepare for moving to another mode (for instance, authenticated or enforcement) in the future. In the organization, these switch configurations will be managed by Cisco LAN Management Solution (LMS) 4.1 and the new Identity WorkCenter. Cisco LMS simplifies the deployment of identity by performing a network readiness assessment for an identity deployment, providing templates for the various modes—monitor, authenticated, enforcement—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 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 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 SBA for Enterprise Organizations – Borderless Networks LAN Deployment Guide. Any IP addresses used in this guide are examples; you should use addressing that is applicable to your architecture.

Device	IP address	Hostname
Primary Cisco ISE	10.4.48.41	Ise-1.cisco.local
Secondary Cisco ISE	10.4.48.42	ise-2.cisco.local

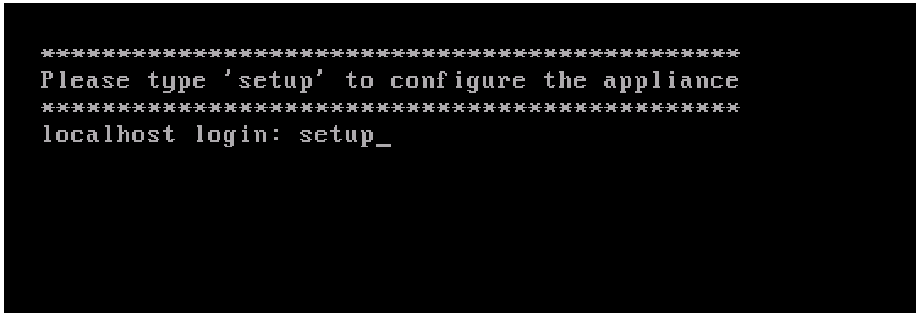
Process

Deploying Identity Services Engine

1. Set up initial primary engine
2. Set up the secondary engine
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

Timezone abbreviations can be found in the Cisco Identity Services Engine CLI Reference Guide, Release 1.1:

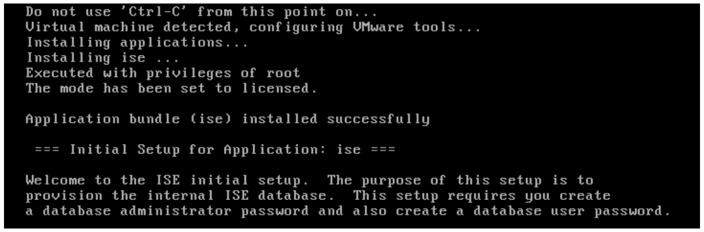
http://www.cisco.com/en/US/docs/security/ise/1.1/cli_ref_guide/ise_cli_app_a.html#wp1571855

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 will be 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 it will abort the installation.



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

Application bundle (ise) installed successfully

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

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

The primary engine is now installed.

Procedure 2 Set up the secondary engine

The procedure for setting up the secondary engine 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 secondary engine, follow Procedure 1 and use the values supplied in the table for the secondary engine.

Procedure 3 Configure certificate trust list

The two 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 the primary and secondary engines. To do this, you need to import the local certificate from the secondary engine into the primary engine.

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 Authority Certificates,** and then click **Add**.

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

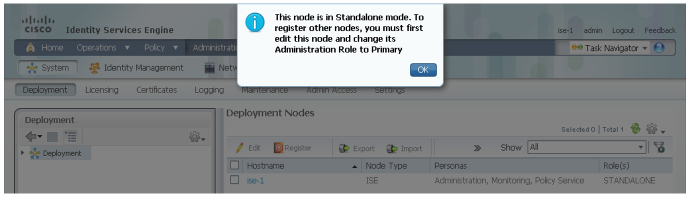
Step 10: Click **Submit**.

Procedure 4 Configure Cisco ISE deployment nodes

You can configure the functions 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 primary engine that performs all three functions and a secondary engine that acts as a backup for the primary.

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.

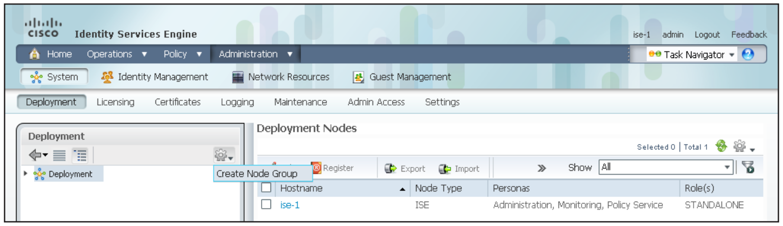

cisco Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administratio
Task Navigator
System Identity Management Netw
Deployment Licensing Certificates Logging Maintenance Admin Access Settings
Deployment
Deployment Nodes
Selected 0 | Total 1
Edit Register Export Import Show All
OK

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

Hostname	Node Type	Personas	Role(s)
ise-1	ISE	Administration, Monitoring, Policy Service	STANDALONE

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.


cisco Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
System Identity Management Network Resources Guest Management
Deployment Licensing Certificates Logging Maintenance Admin Access Settings
Deployment
Deployment
Create Node Group
Deployment Nodes
Selected 0 | Total 1
Register Export Import Show All

Hostname	Node Type	Personas	Role(s)
ise-1	ISE	Administration, Monitoring, Policy Service	STANDALONE

Step 4: Configure the node group with the node group name ISE-Group and the default multicast address of 228.10.11.12.

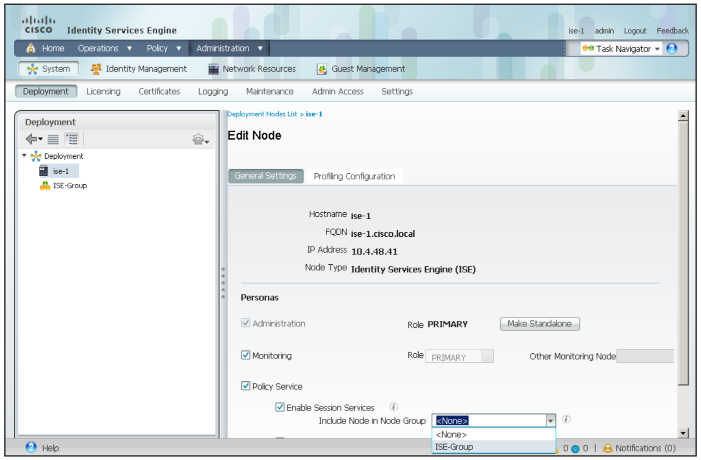
Step 5: Click **Submit**. A pop-up window lets you know the group was created successfully. Click **OK**.

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: Under the Personas section on the General Settings tab, click **Make Primary**, which is next to the Administration Role.

Step 9: Include this node in the ISE-Group node group by choosing it from the pull-down menu.


cisco Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
System Identity Management Network Resources Guest Management
Deployment Licensing Certificates Logging Maintenance Admin Access Settings
Deployment
Deployment
ise-1
ISE-Group
Deployment Nodes List > ise-1
Edit Node
General Settings
Profiling Configuration
Make Standalone
Help
Notifications (0)

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

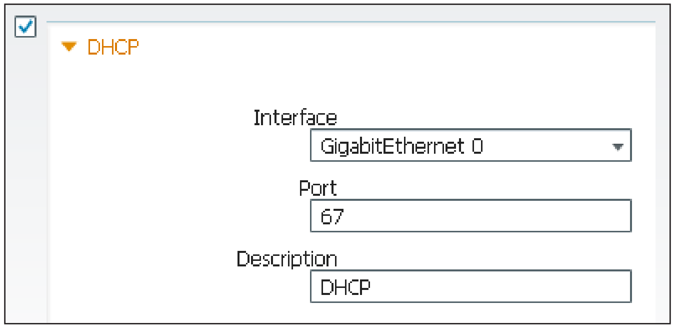
Personas

☑ Administration Role PRIMARY
☑ Monitoring Role PRIMARY Other Monitoring Node
☑ Policy Service
☑ Enable Session Services
Include Node in Node Group <None>
<None>
ISE-Group

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

Step 10: Click the **Profiling Configuration** tab.

Step 11: This example uses DHCP and RADIUS. Select the box next to each to enable these methods, use the default parameters, and then click **Save**.

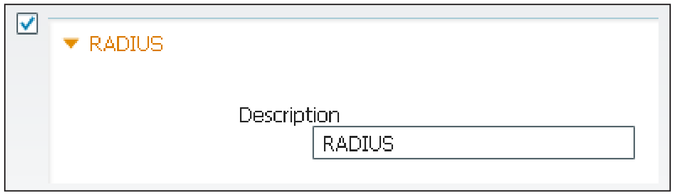


☑ DHCP

Interface: GigabitEthernet 0

Port: 67

Description: DHCP

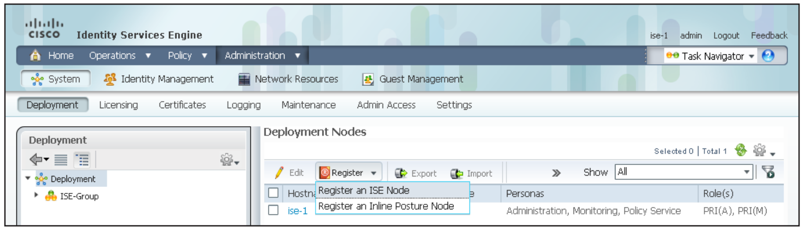


☑ RADIUS

Description: RADIUS

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

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


cisco Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
System Identity Management Network Resources Guest Management
Deployment Licensing Certificates Logging Maintenance Admin Access Settings
Deployment
Deployment
ISE-Group
Edit Register Export Import
Register an ISE Node
Register an Inline Posture Node

Deployment Nodes

Selected 0 | Total 1

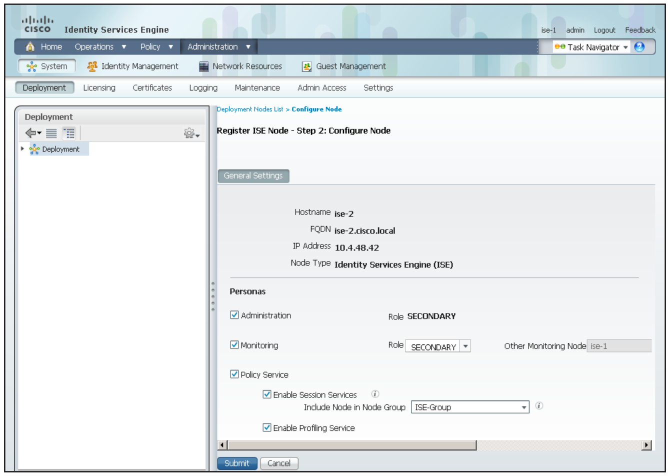
Show: All

☐	Hostname	Personas	Role(s)
☐	ise-1	Administration, Monitoring, Policy Service	PRI(A), PRI(M)

Step 14: Enter the IP address or host name of the secondary Cisco ISE and the credentials for the admin account, and then click **Next**.

Step 15: Configure ise-2 to be the secondary engine in the group by making sure that all the boxes are selected to enable all personas and that this unit is the secondary. Choose the node group **ISE-Group** from the drop-down list.

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


cisco Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
System Identity Management Network Resources Guest Management
Deployment Licensing Certificates Logging Maintenance Admin Access Settings
Deployment
Deployment
Deployment Nodes List > Configure Node
General Settings
Submit
Cancel

Register ISE Node - Step 2: Configure Node

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

Personas

☑ Administration — Role: SECONDARY

☑ Monitoring — Role: SECONDARY — Other Monitoring Node: ise-1

☑ Policy Service

☑ Enable Session Services

Include Node in Node Group: ISE-Group

☑ Enable Profiling Service

Step 17: In the Deployment Nodes window, click **ise-2,** click the **Profiling Configuration** tab, and then configure the DHCP and RADIUS options in the same way you did for the primary engine.

Step 18: Click **Save**.

Both Cisco ISE units are now configured as a redundant pair.

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.

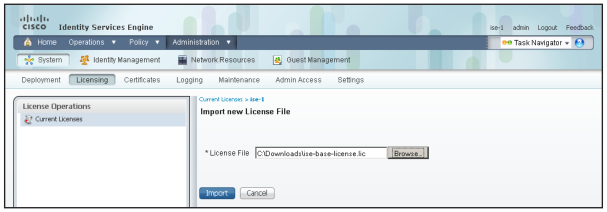
Step 1: Mouse over **Administration**, and then, from the System section of the menu, choose **Licensing**.

Notice that you only see one node here since the secondary node does not require 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 to locate your license file, and then click **Import**.



Current Licenses > ise-1

Import new License File

* License File C:\Downloads\ise-base-license.lic

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

Tech Tip

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

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**.

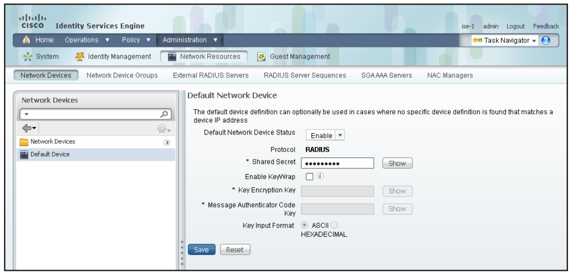
Step 2: In the left pane, click **Default Device**.

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 our network devices have to use the same key, so for simplicity, this example uses the Default Device.

Step 3: Enable Default Network Device Status by choosing **Enable** from the pull-down menu.

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



Default Network Device

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

Default Network Device Status Enable

Protocol **RADIUS**

* Shared Secret ●●●●●●●●●

Enable KeyWrap □

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ● ASCII ○ HEXADECIMAL

Procedure 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.

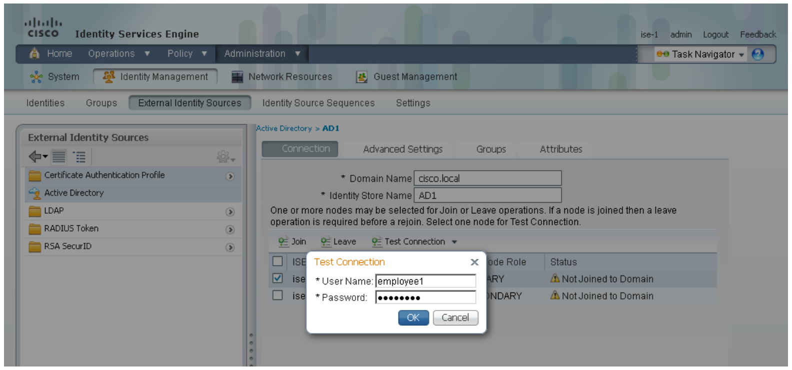
Step 1: Mouse over **Administration**, and then, from the Identity Management section of the menu, choose **External Identity Sources**.

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

Step 3: On the Connection tab, configure the connection to the AD server by entering 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, and then clicking **Test Connection** and choosing **Basic Test**.

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


Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
System Identity Management Network Resources Guest Management
Identities Groups External Identity Sources Identity Source Sequences Settings
External Identity Sources
Certificate Authentication Profile
Active Directory
LDAP
RADIUS Token
RSA SecurID
Active Directory > AD1
Connection Advanced Settings Groups Attributes
Join Leave Test Connection
ISE ode Role Status
OK Cancel

* Domain Name: cisco.local
* Identity Store Name: AD1

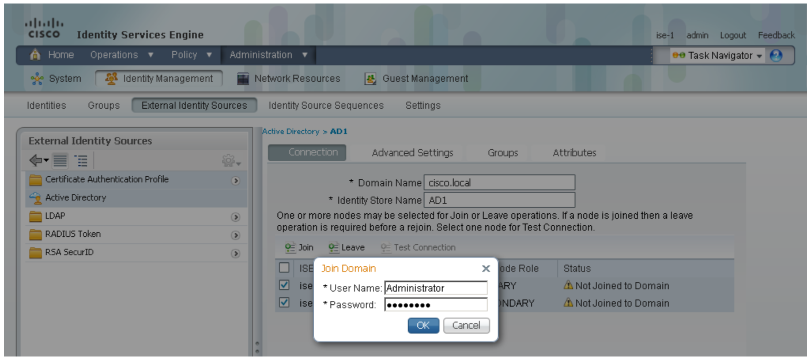
One or more nodes may be selected for Join or Leave operations. If a node is joined then a leave operation is required before a rejoin. Select one node for Test Connection.

	ISE	ode Role	Status
☑	ise	ARY	⚠ Not Joined to Domain
□	ise	NDARY	⚠ Not Joined to Domain

Test Connection
* User Name: employee1
* Password: ●●●●●●●●●

Step 6: Select the box next each node, and then click **Join**.

Step 7: Enter the credentials for a domain administrator account. The Cisco ISE is now joined to the AD domain.


Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
System Identity Management Network Resources Guest Management
Identities Groups External Identity Sources Identity Source Sequences Settings
External Identity Sources
Certificate Authentication Profile
Active Directory
LDAP
RADIUS Token
RSA SecurID
Active Directory > AD1
Connection Advanced Settings Groups Attributes
Join Leave Test Connection
ISE ode Role Status
OK Cancel

* Domain Name: cisco.local
* Identity Store Name: AD1

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

	ISE	ode Role	Status
☑	ise	ARY	⚠ Not Joined to Domain
☑	ise	NDARY	⚠ Not Joined to Domain

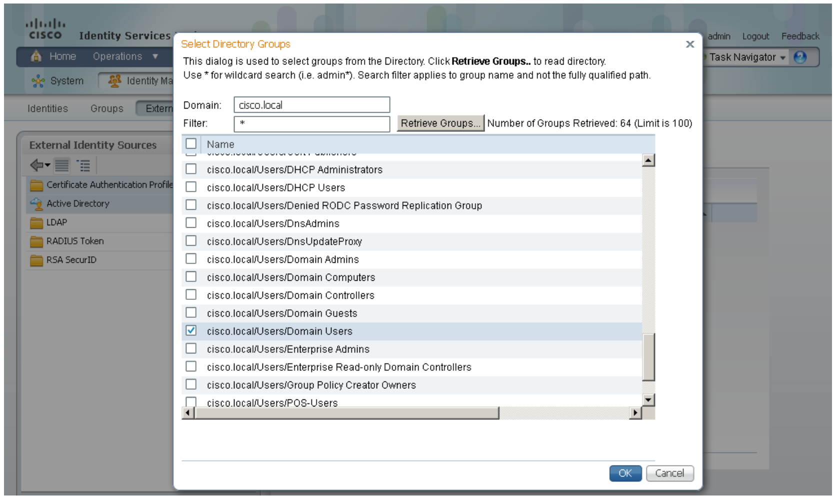
Join Domain
* User Name: Administrator
* Password: ●●●●●●●●●

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

Step 8: Click the **Groups** tab, click **Add,** and then click **Select Groups from Directory**.

Step 9: Search for the groups you wish to add. The domain field 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 10: Select the groups you want to use for authentication, and then click **OK**. For example, for all users in the domain, select the group <domain>/Users/Domain Users.



Select Directory Groups

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

Domain: cisco.local
Filter: *
Number of Groups Retrieved: 64 (Limit is 100)

□	Name
□	cisco.local/Users/DHCP Administrators
□	cisco.local/Users/DHCP Users
□	cisco.local/Users/Denied RODC Password Replication Group
□	cisco.local/Users/DnsAdmins
□	cisco.local/Users/DnsUpdateProxy
□	cisco.local/Users/Domain Admins
□	cisco.local/Users/Domain Computers
□	cisco.local/Users/Domain Controllers
□	cisco.local/Users/Domain Guests
☑	cisco.local/Users/Domain Users
□	cisco.local/Users/Enterprise Admins
□	cisco.local/Users/Enterprise Read-only Domain Controllers
□	cisco.local/Users/Group Policy Creator Owners
□	cisco.local/Users/POS-Users

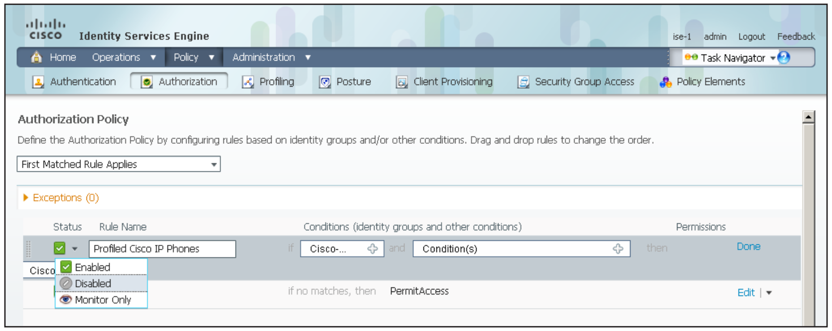
Step 11: Click **Save Configuration**.

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, this rule should be disabled.

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

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



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Profiled Cisco IP Phones	if Cisco-... and Condition(s)	then
	Cisco	if no matches, then	PermitAccess

✓ Enabled
Disabled
Monitor Only

Process

Enabling Visibility to the LAN

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

Cisco ISE is now configured for identity. The next step is to configure the switches for identity by using Cisco LMS 4.1 and the Identity Workcenter.

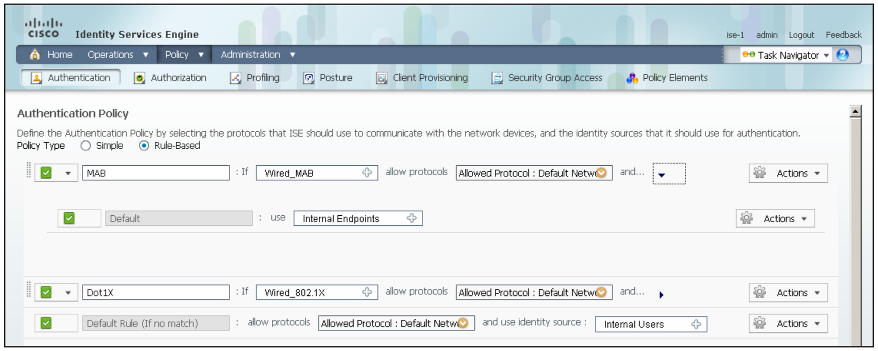
Procedure 1 Configure MAC Authentication Bypass

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: Use the default MAB policy. Click the black triangle to the right of the **and...** of the MAB rule. This brings up the identity store used for the MAB rule.


Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Actions

Authentication Policy

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

Policy Type ○ Simple ● Rule-Based

☑ MAB : If Wired_MAB allow protocols Allowed Protocol : Default Netw and...

☑ Default : use Internal Endpoints

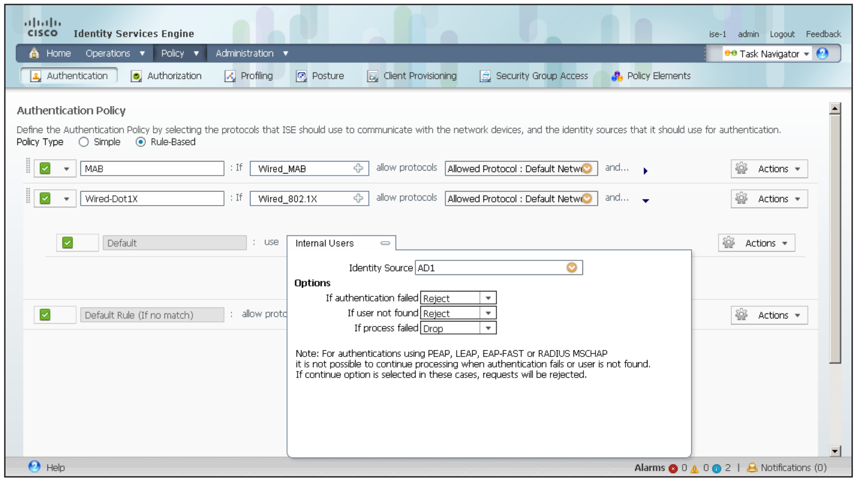
☑ Dot1X : If Wired_802.1X allow protocols Allowed Protocol : Default Netw and...

☑ Default Rule (If no match) : allow protocols Allowed Protocol : Default Netw and use identity source : Internal Users

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

Step 3: Click the **+** next to **Internal Endpoints**. In this example deployment, we are allowing all endpoints to authenticate. If the MAC address isn't found in the database, you need to bypass authentication and continue. For the authentication failed and user not found options, choose **Continue** from the pull-down menu.

Step 4: Click anywhere in the window to continue, and then click **Save**.


Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Actions
Help
Alarms 0 0 2 | Notifications (0)

Authentication Policy

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

Policy Type ○ Simple ● Rule-Based

☑ MAB : If Wired_MAB allow protocols Allowed Protocol : Default Netw and...

☑ Wired-Dot1X : If Wired_802.1X allow protocols Allowed Protocol : Default Netw and...

☑ Default : use Internal Users

Identity Source AD1

Options

If authentication failed Reject

If user not found Reject

If process failed Drop

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

☑ Default Rule (If no match) : allow proto

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**.

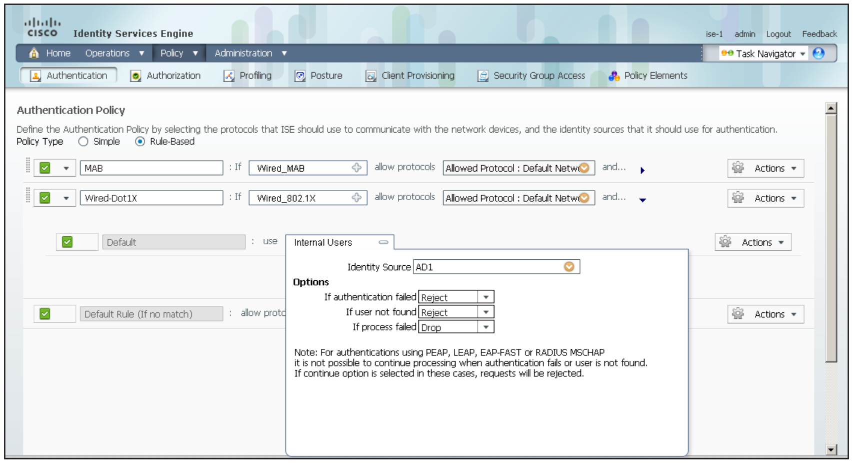
Step 3: Click the black triangle to the right of the **and...** of the Wired-Dot1X rule. This brings up the identity store used for this rule.

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

Step 4: Click the **+** symbol next to **Internal Users**. This enables you to edit the identity store and the parameters.

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

Step 6: Click **Save**.


Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Actions

Authentication Policy

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

Policy Type ○ Simple ● Rule-Based

☑ MAB : If Wired_MAB allow protocols Allowed Protocol : Default Netw and...

☑ Wired-Dot1X : If Wired_802.1X allow protocols Allowed Protocol : Default Netw and...

☑ Default : use Internal Users

Identity Source AD1

Options

If authentication failed Reject

If user not found Reject

If process failed Drop

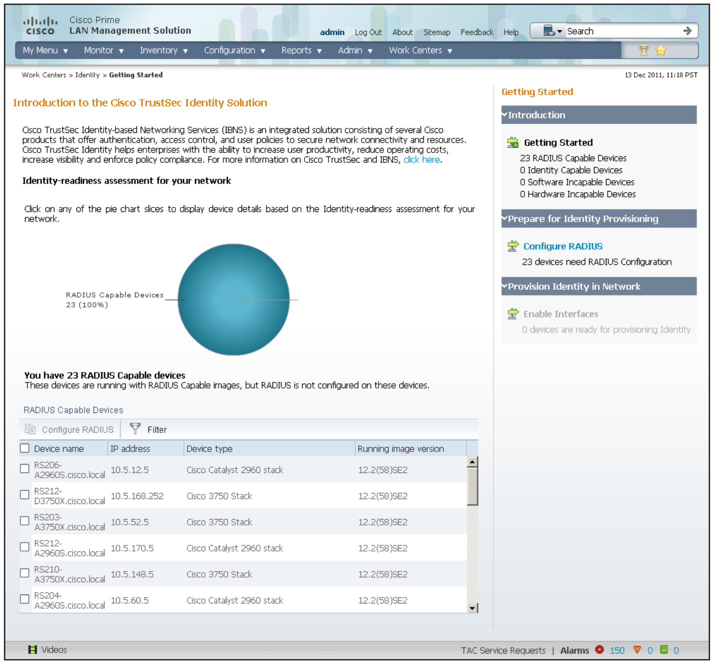
Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS MSCHAP it is not possible to continue processing when authentication fails or user is not found. If continue option is selected in these cases, requests will be rejected.

☑ Default Rule (If no match) : allow proto

Procedure 3 Enable RADIUS in the access layer

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

Step 2: Mouse over **Workcenters**, and then, from the Identity section, choose **Getting Started**. This shows the network's Identity Readiness Assessment, which verifies that the software versions support the identity features and that the switches are capable of running RADIUS.


Cisco Prime
LAN Management Solution
admin Log Out About Sitemap Feedback Help
Search
My Menu Monitor Inventory Configuration Reports Admin Work Centers
Work Centers > Identity > Getting Started
13 Dec 2011, 11:18 PST
RADIUS Capable Devices
23 (100%)
Configure RADIUS
Filter
Videos
TAC Service Requests | Alarms 150 0 0

Introduction to the Cisco TrustSec Identity Solution

Cisco TrustSec Identity-based Networking Services (IBNS) is an integrated solution consisting of several Cisco products that offer authentication, access control, and user policies to secure network connectivity and resources. Cisco TrustSec Identity helps enterprises with the ability to increase user productivity, reduce operating costs, increase visibility and enforce policy compliance. For more information on Cisco TrustSec and IBNS, click here.

Identity-readiness assessment for your network

Click on any of the pie chart slices to display device details based on the Identity-readiness assessment for your network.

You have 23 RADIUS Capable devices
These devices are running with RADIUS Capable images, but RADIUS is not configured on these devices.

RADIUS Capable Devices

Device name	IP address	Device type	Running image version
RS206-A2960S.cisco.local	10.5.12.5	Cisco Catalyst 2960 stack	12.2(58)SE2
RS212-D3750X.cisco.local	10.5.168.252	Cisco 3750 Stack	12.2(58)SE2
RS203-A3750X.cisco.local	10.5.52.5	Cisco 3750 Stack	12.2(58)SE2
RS212-A2960S.cisco.local	10.5.170.5	Cisco Catalyst 2960 stack	12.2(58)SE2
RS210-A3750X.cisco.local	10.5.148.5	Cisco 3750 Stack	12.2(58)SE2
RS204-A2960S.cisco.local	10.5.60.5	Cisco Catalyst 2960 stack	12.2(58)SE2

Getting Started

Introduction

Getting Started
23 RADIUS Capable Devices
0 Identity Capable Devices
0 Software Incapable Devices
0 Hardware Incapable Devices

Prepare for Identity Provisioning

Configure RADIUS
23 devices need RADIUS Configuration

Provision Identity in Network

Enable Interfaces
0 devices are ready for provisioning Identity

Next, configure identity by enabling RADIUS on the switch.

Step 3: In the RADIUS-capable devices table, select the switches for which you want to enable RADIUS, and then click **Configure RADIUS**.

Step 4: Select the **RADIUS Group** button, and then fill in the fields. Enter **ISE-Group** for the RADIUS group name, and then use the value used in previous procedures for the Shared Key.

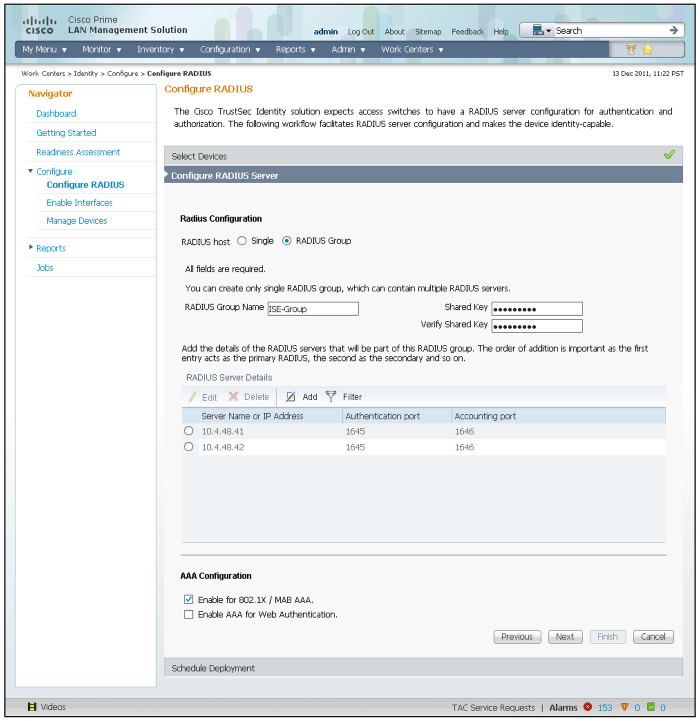
Step 5: In the RADIUS Server Details section, click **Add**.

Step 6: In the pop-up window, enter **10.4.48.41** for the RADIUS server IP address, and then click **Save and add another**.

Step 7: Enter **10.4.48.42** for the second RADIUS server, and then click **Save.** The RADIUS server group has been configured.

Step 8: In the AAA Configuration section, make sure that only **Enable for 802.1X / MAB AAA** is selected. A warning message about not configuring AAA for Web authentication appears. Click **OK**.

Step 9: Click **Next** to proceed to the next step.



Configure RADIUS

The Cisco TrustSec Identity solution expects access switches to have a RADIUS server configuration for authentication and authorization. The following workflow facilitates RADIUS server configuration and makes the device identity-capable.

Radius Configuration

RADIUS host ○ Single ● RADIUS Group

All fields are required.

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

RADIUS Group Name: ISE-Group
Shared Key: ●●●●●●●●●
Verify Shared Key: ●●●●●●●●●

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

RADIUS Server Details

Server Name or IP Address	Authentication port	Accounting port
10.4.48.41	1645	1646
10.4.48.42	1645	1646

AAA Configuration

☑ Enable for 802.1X / MAB AAA.
□ Enable AAA for Web Authentication.

Tech Tip

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

Step 10: Enter a job description, and then click **Finish** to deploy immediately.

Step 11: When you receive the warning regarding the addition of AAA commands, click **Yes**, and then click **OK** on the pop-up window generated after the job is created.

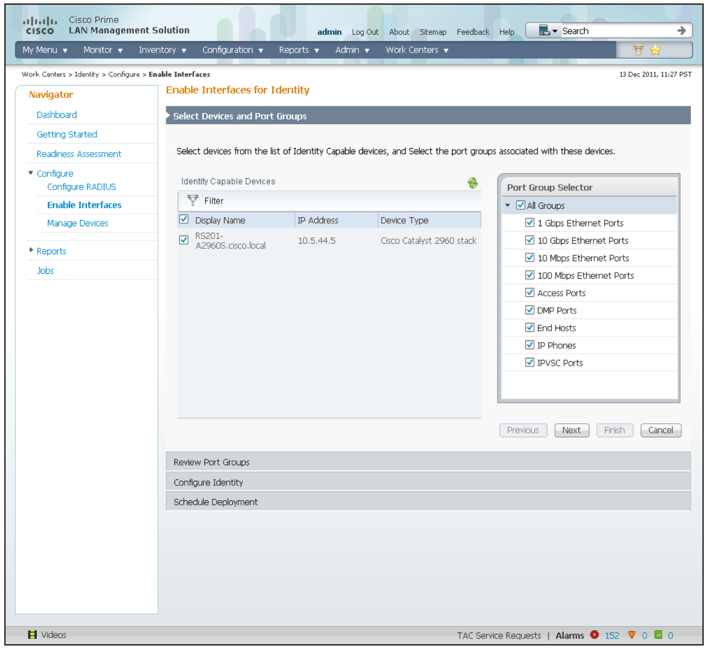
Procedure 4 Enable identity

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 Identity section, choose **Configure**.

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

Step 3: Choose the switch that was previously configured for RADIUS from the list, select **All Groups** in the port group selector, and then click **Next**.



Enable Interfaces for Identity

Select Devices and Port Groups

Select devices from the list of Identity Capable devices, and Select the port groups associated with these devices.

Identity Capable Devices

☑	Display Name	IP Address	Device Type
☑	RS201-A2960S.cisco.local	10.5.44.5	Cisco Catalyst 2960 stack

Port Group Selector

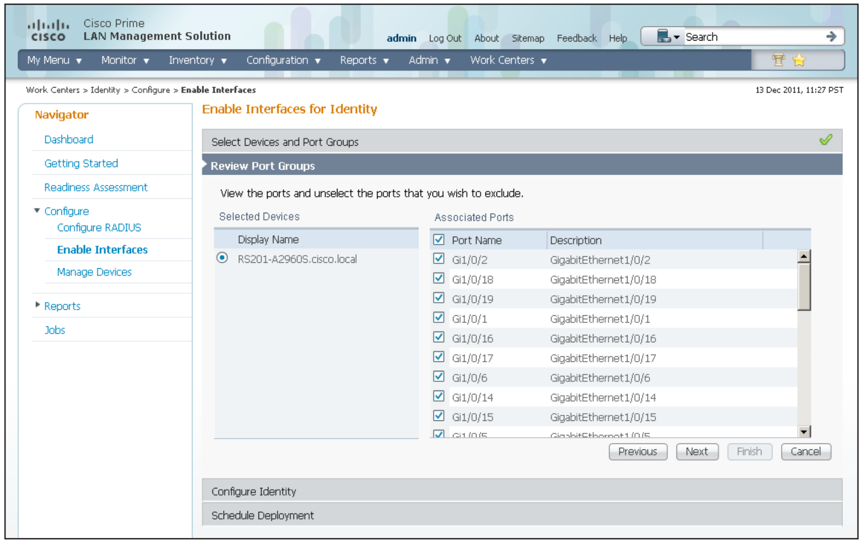
- ☑ All Groups
  - ☑ 1 Gbps Ethernet Ports
  - ☑ 10 Gbps Ethernet Ports
  - ☑ 10 Mbps Ethernet Ports
  - ☑ 100 Mbps Ethernet Ports
  - ☑ Access Ports
  - ☑ DMP Ports
  - ☑ End Hosts
  - ☑ IP Phones
  - ☑ IPVSC Ports

Review Port Groups

Configure Identity

Schedule Deployment

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



Enable Interfaces for Identity

Select Devices and Port Groups ✓

Review Port Groups

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

Selected Devices

	Display Name
●	RS201-A2960S.cisco.local

Associated Ports

☑	Port Name	Description
☑	Gi1/0/2	GigabitEthernet1/0/2
☑	Gi1/0/18	GigabitEthernet1/0/18
☑	Gi1/0/19	GigabitEthernet1/0/19
☑	Gi1/0/1	GigabitEthernet1/0/1
☑	Gi1/0/16	GigabitEthernet1/0/16
☑	Gi1/0/17	GigabitEthernet1/0/17
☑	Gi1/0/6	GigabitEthernet1/0/6
☑	Gi1/0/14	GigabitEthernet1/0/14
☑	Gi1/0/15	GigabitEthernet1/0/15
☑	Gi1/0/5	GigabitEthernet1/0/5

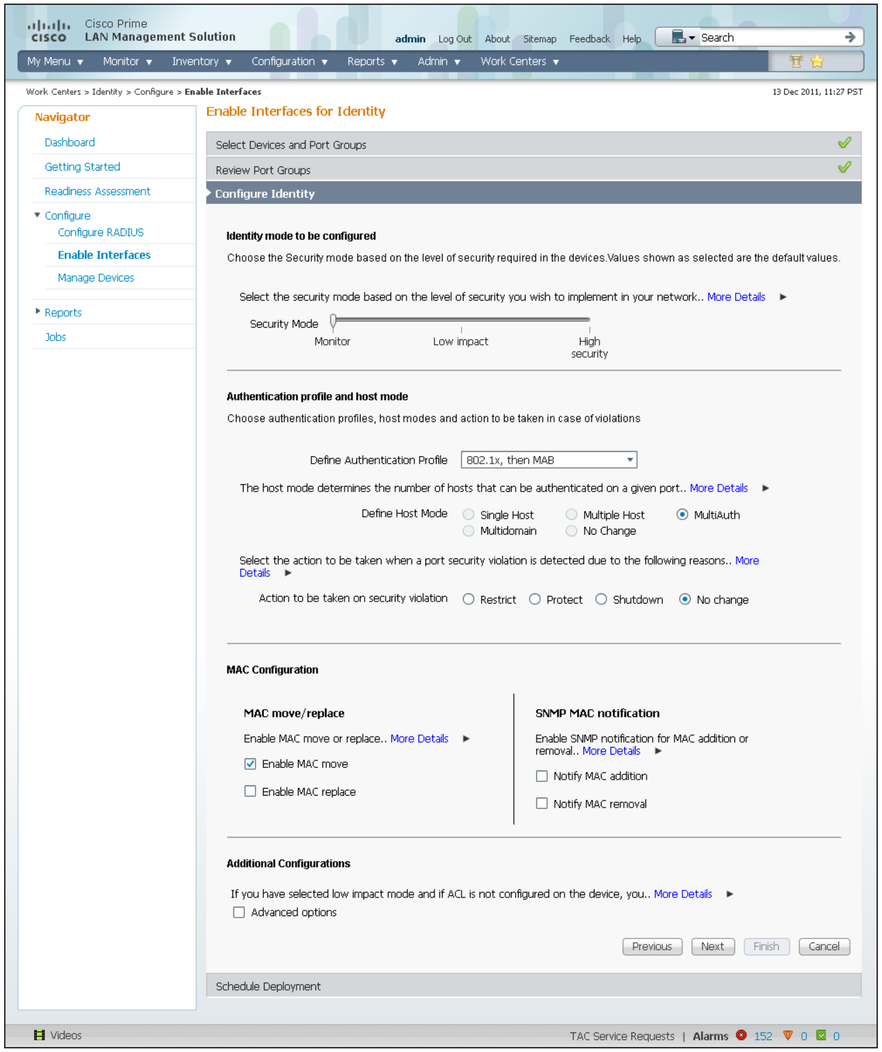
Configure Identity

Schedule Deployment

Next, configure monitor mode.

Step 5: Move the Security Mode slider to **Monitor**, which is the default.

Step 6: In the Authentication Profile section, select **802.1X, then MAB** in the Define Authentication Profile slider, make sure **MultiAuth** is selected in the Define Host Mode section and **No Change** is selected for Action to be taken on security violation, and then, in the MAC Configuration section, make sure only **Enable MAC Move** is selected.



Work Centers > Identity > Configure > Enable Interfaces 13 Dec 2011, 11:27 PST

Enable Interfaces for Identity

Select Devices and Port Groups ✓

Review Port Groups ✓

Configure Identity

Identity mode to be configured

Choose the Security mode based on the level of security required in the devices.Values shown as selected are the default values.

Select the security mode based on the level of security you wish to implement in your network.. More Details ▸

Security Mode: Monitor — Low impact — High security

Authentication profile and host mode

Choose authentication profiles, host modes and action to be taken in case of violations

Define Authentication Profile: 802.1x, then MAB

The host mode determines the number of hosts that can be authenticated on a given port.. More Details ▸

Define Host Mode: ○ Single Host ○ Multiple Host ● MultiAuth ○ Multidomain ○ No Change

Select the action to be taken when a port security violation is detected due to the following reasons.. More Details ▸

Action to be taken on security violation: ○ Restrict ○ Protect ○ Shutdown ● No change

MAC Configuration

MAC move/replace

Enable MAC move or replace.. More Details ▸

☑ Enable MAC move

□ Enable MAC replace

SNMP MAC notification

Enable SNMP notification for MAC addition or removal.. More Details ▸

□ Notify MAC addition

□ Notify MAC removal

Additional Configurations

If you have selected low impact mode and if ACL is not configured on the device, you.. More Details ▸

□ Advanced options

Schedule Deployment

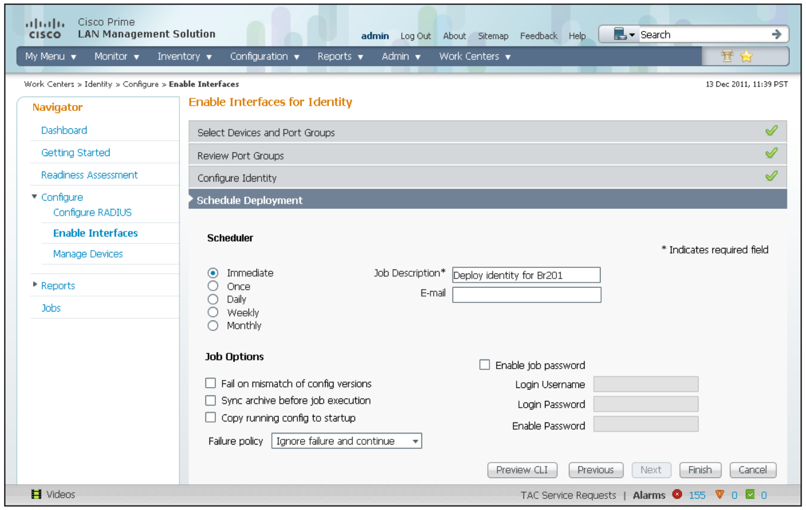
Step 7: Click **Next**. Identity configuration is complete.

Next, you must create a deployment job in order to deliver the configuration to the switch.

Step 8: Give the deployment job a description in the Job Description field, and then click **Finish** to submit the job. Click **OK**.

Tech Tip

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



Work Centers > Identity > Configure > Enable Interfaces 13 Dec 2011, 11:39 PST

Enable Interfaces for Identity

Select Devices and Port Groups ✓

Review Port Groups ✓

Configure Identity ✓

Schedule Deployment

Scheduler

* Indicates required field

● Immediate ○ Once ○ Daily ○ Weekly ○ Monthly

Job Description*: Deploy identity for Br201

E-mail:

Job Options

□ Fail on mismatch of config versions

□ Sync archive before job execution

□ Copy running config to startup

Failure policy: Ignore failure and continue

□ Enable job password

Login Username

Login Password

Enable Password

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
```

```
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 LMS server by browsing to https://lms.cisco.local.

Step 2: Mouse over **Configuration**, and then choose **NetConfig** under the Tools heading. 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: Click the **+** symbol next to the **All Devices** tree, 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.

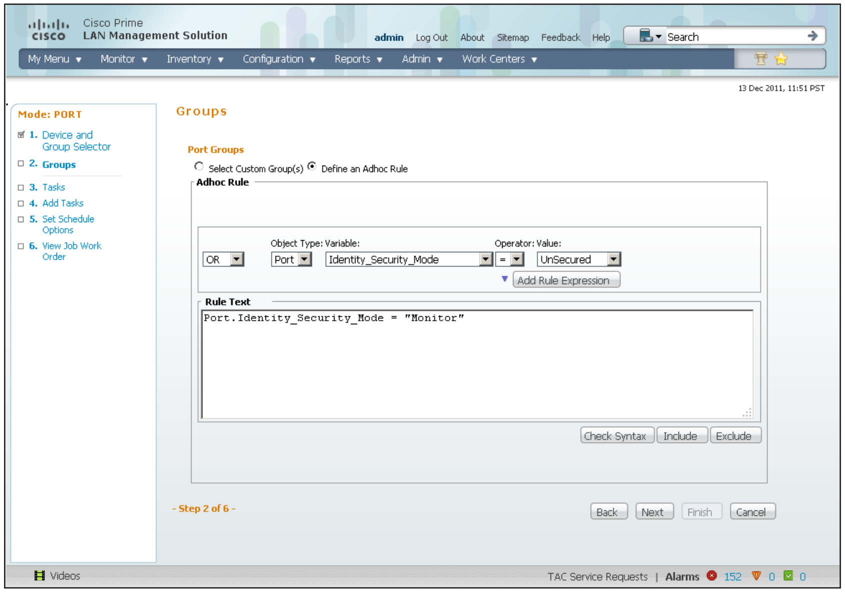
Step 6: Select **Define an Ad-Hoc Rule**. This brings up a new screen.

Step 7: For the ad-hoc rule, select **Port** for the object type.

Step 8: From the Variable drop-down menu, choose **Identity_Security_Mode**.

Step 9: For the Operator, choose **=,** and for the Value, select **Monitor**.

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



Cisco Prime
LAN Management Solution
admin Log Out About Sitemap Feedback Help
Search
My Menu Monitor Inventory Configuration Reports Admin Work Centers
13 Dec 2011, 11:51 PST
Mode: PORT
☑ 1. Device and Group Selector
□ 2. Groups
□ 3. Tasks
□ 4. Add Tasks
□ 5. Set Schedule Options
□ 6. View Job Work Order
Check Syntax
Include
Exclude
Back
Next
Finish
Cancel
Videos
TAC Service Requests | Alarms 152 0 0

Groups

Port Groups

○ Select Custom Group(s) ● Define an Adhoc Rule

Adhoc Rule

	Object Type:	Variable:	Operator:	Value:
OR	Port	Identity_Security_Mode	=	UnSecured

Add Rule Expression

Rule Text

```
Port.Identity_Security_Mode = "Monitor"
```

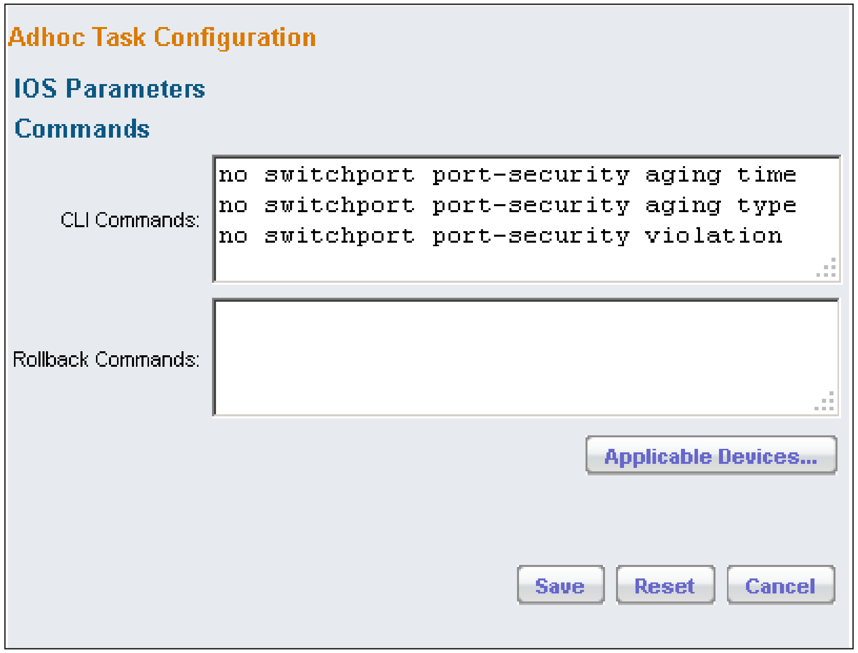
- Step 2 of 6 -

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

Step 12: Click **Add Instance**, and then, in the new window, add 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 apply this configuration to, click **Close**, and then click **Save**.



Adhoc Task Configuration

IOS Parameters

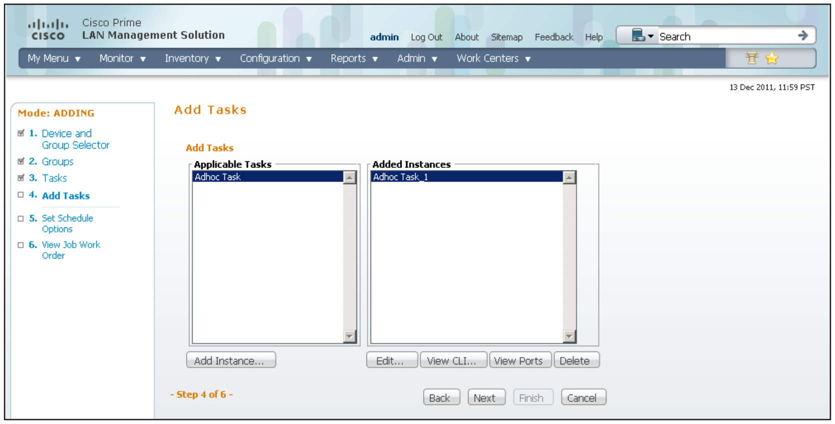
Commands

CLI Commands:

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

Rollback Commands:

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



Step 15: Fill in a description for the job, and then click **Next** to submit the job for immediate deployment.

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

Procedure 6 Configure profiling for the LAN

One of the ways Cisco ISE profiles endpoints is by examining DHCP requests that are sent from the device. In order to forward these requests to the engine, a helper address needs to be configured on the router interface of the network of the host. A helper address takes the broadcast packet and makes it a directed broadcast to the address specified.

Step 1: Connect to the console of the default router for the endpoint.

Step 2: At the CLI, enter the following commands.

```
Router#ena
Router#conf terminal
Router(config)#interface [interface]
Router(config-if)#ip helper-address 10.4.48.41
Router(config-if)#ip helper-address 10.4.48.42
Router(config-if)#exit
Router(config)#exit
Router#copy running-config startup-config
```

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. Disable the original RADIUS server
5. Add ISE as RADIUS accounting server
6. Add secondary DHCP server on WLC

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 with Cisco ISE as a secondary DHCP server so that profiling information can be obtained from the DHCP requests from these clients.

Procedure 1 Configure 802.1X for wireless endpoints

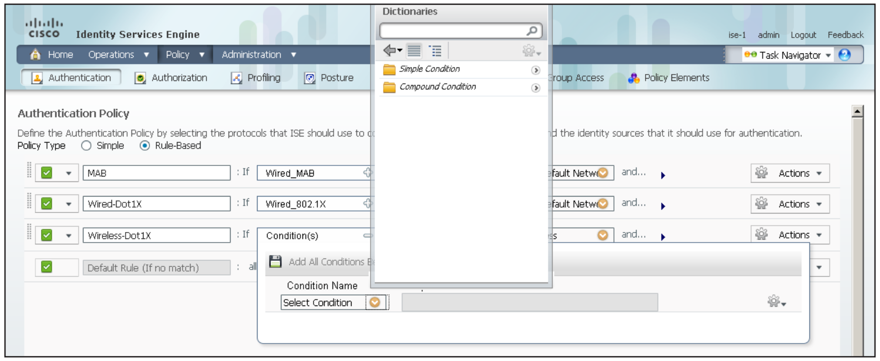
To differentiate wireless users in the authentication logs, create a rule to identify when wireless users authenticate.

Step 1: Navigate to the **Authentication Policy** tab, mouse over **Policy**, and then, from the menu, choose **Authentication**.

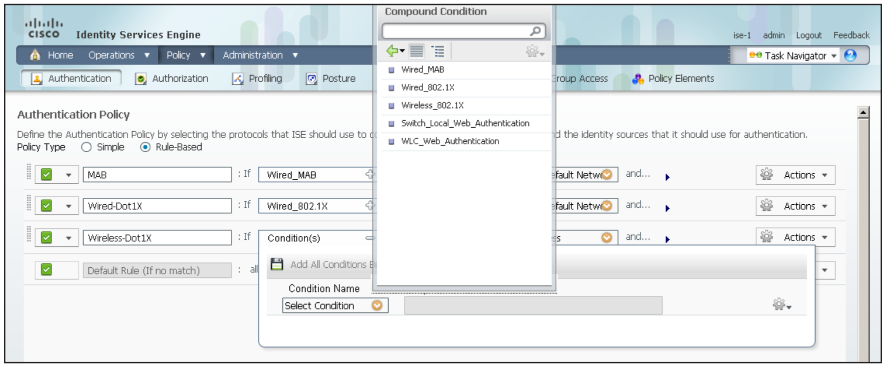
Step 2: Click the **Actions** button for the Default Rule, and then choose **Insert new row above**. A new rule, Standard Policy 1, is created.

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

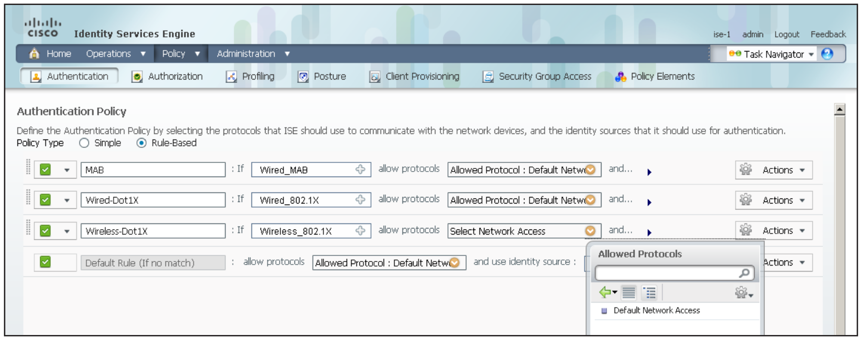
Step 4: In the Select Condition pull-down list, click the > symbol next to **Compound Condition**.


Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
Authentication Authorization Profiling Posture
Group Access Policy Elements
Authentication Policy
Define the Authentication Policy by selecting the protocols that ISE should use to c... d the identity sources that it should use for authentication.
Policy Type ○ Simple ● Rule-Based
MAB : If Wired_MAB ...fault Netw and...
Wired-Dot1X : If Wired_802.1X ...fault Netw and...
Wireless-Dot1X : If Condition(s) ...s and...
Default Rule (If no match) : al
Actions
Add All Conditions B
Condition Name
Select Condition
Dictionaries
Simple Condition
Compound Condition

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


Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
Authentication Authorization Profiling Posture
Group Access Policy Elements
Authentication Policy
Define the Authentication Policy by selecting the protocols that ISE should use to c... d the identity sources that it should use for authentication.
Policy Type ○ Simple ● Rule-Based
MAB : If Wired_MAB ...fault Netw and...
Wired-Dot1X : If Wired_802.1X ...fault Netw and...
Wireless-Dot1X : If Condition(s) ...s and...
Default Rule (If no match) : al
Actions
Add All Conditions B
Condition Name
Select Condition
Compound Condition
Wired_MAB
Wired_802.1X
Wireless_802.1X
Switch_Local_Web_Authentication
WLC_Web_Authentication

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

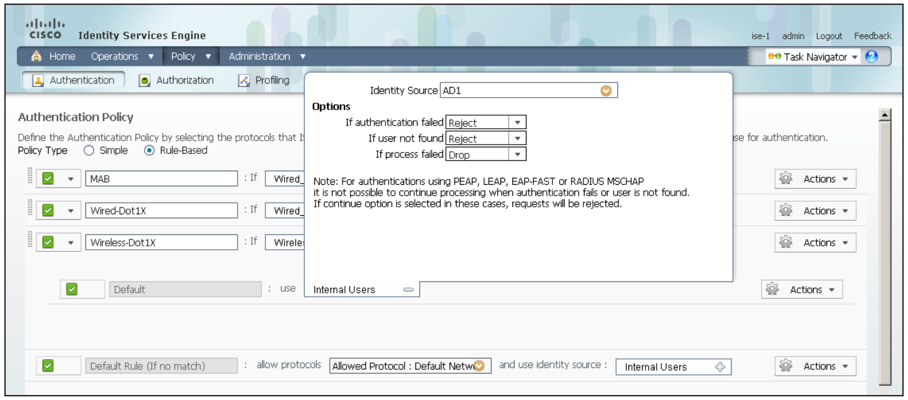

Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Authentication Policy
Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.
Policy Type ○ Simple ● Rule-Based
MAB : If Wired_MAB allow protocols Allowed Protocol : Default Netw and...
Wired-Dot1X : If Wired_802.1X allow protocols Allowed Protocol : Default Netw and...
Wireless-Dot1X : If Wireless_802.1X allow protocols Select Network Access and...
Default Rule (If no match) : allow protocols Allowed Protocol : Default Netw and use identity source :
Actions
Allowed Protocols
Default Network Access

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

Step 8: Click the + symbol next to **Set Identity Source**.

Step 9: In the Identity Source drop-down 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**.


Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
Authentication Authorization Profiling
Authentication Policy
Define the Authentication Policy by selecting the protocols that I... se for authentication.
Policy Type ○ Simple ● Rule-Based
MAB : If Wired_
Wired-Dot1X : If Wired_
Wireless-Dot1X : If Wireles
Default : use Internal Users
Default Rule (If no match) : allow protocols Allowed Protocol : Default Netw and use identity source : Internal Users
Actions

Identity Source AD1

Options

If authentication failed Reject

If user not found Reject

If process failed Drop

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

Procedure 2 Disable EAP-TLS on Cisco ISE

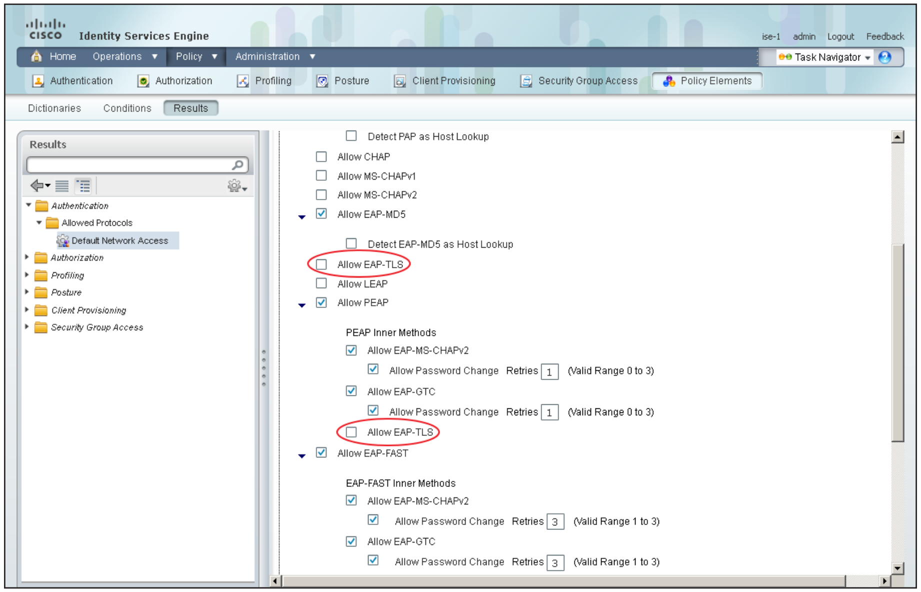
For wireless deployments that aren't currently using digital certificates, you need to disable EAP-TLS to allow clients to log in. You will be deploying digital certificates in a later phase of this deployment.

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**.


Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Dictionaries Conditions Results
Results
Authentication
Allowed Protocols
Default Network Access
Authorization
Profiling
Posture
Client Provisioning
Security Group Access

- □ Detect PAP as Host Lookup
- □ Allow CHAP
- □ Allow MS-CHAPv1
- □ Allow MS-CHAPv2
- ☑ Allow EAP-MD5
  - □ Detect EAP-MD5 as Host Lookup
- □ Allow EAP-TLS
- □ Allow LEAP
- ☑ Allow PEAP
  - PEAP Inner Methods
  - ☑ Allow EAP-MS-CHAPv2
    - ☑ Allow Password Change Retries 1 (Valid Range 0 to 3)
  - ☑ Allow EAP-GTC
    - ☑ Allow Password Change Retries 1 (Valid Range 0 to 3)
  - □ Allow EAP-TLS
- ☑ Allow EAP-FAST
  - EAP-FAST Inner Methods
  - ☑ Allow EAP-MS-CHAPv2
    - ☑ Allow Password Change Retries 3 (Valid Range 1 to 3)
  - ☑ Allow EAP-GTC
    - ☑ Allow Password Change Retries 3 (Valid Range 1 to 3)

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 guest WLC in the demilitarized zone (DMZ).

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

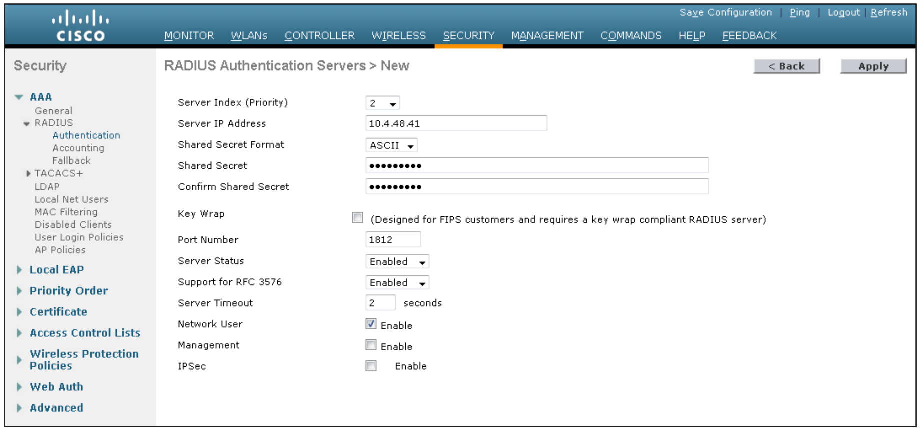
Step 2: On the menu bar, click **Security**.

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

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

Step 5: Enter **10.4.48.41** for the IP address of the new server and your RADIUS shared secret.

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



RADIUS Authentication Servers > New

Server Index (Priority)	2
Server IP Address	10.4.48.41
Shared Secret Format	ASCII
Shared Secret	•••••••••
Confirm Shared Secret	•••••••••
Key Wrap	□ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server Timeout	2 seconds
Network User	☑ Enable
Management	□ Enable
IPSec	□ Enable

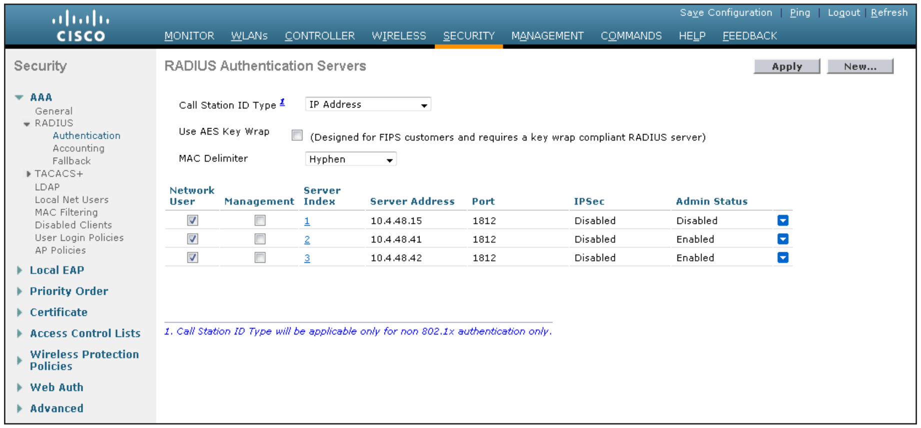
Step 7: Repeat Steps 4 through 6 to add the secondary engine, 10.4.48.42, to the WLC configuration.

Procedure 4 Disable the original RADIUS server

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 guest WLC in the DMZ.

Step 1: 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 2: On the RADIUS Authentication Servers screen, click **Apply**.



RADIUS Authentication Servers

Call Station ID Type [1] IP Address

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

MAC Delimiter Hyphen

Network User	Management	Server Index	Server Address	Port	IPSec	Admin Status
☑	☐	1	10.4.48.15	1812	Disabled	Disabled
☑	☐	2	10.4.48.41	1812	Disabled	Enabled
☑	☐	3	10.4.48.42	1812	Disabled	Enabled

1. Call Station ID Type will be applicable only for non 802.1x authentication only.

Procedure 5 Add ISE as RADIUS accounting server

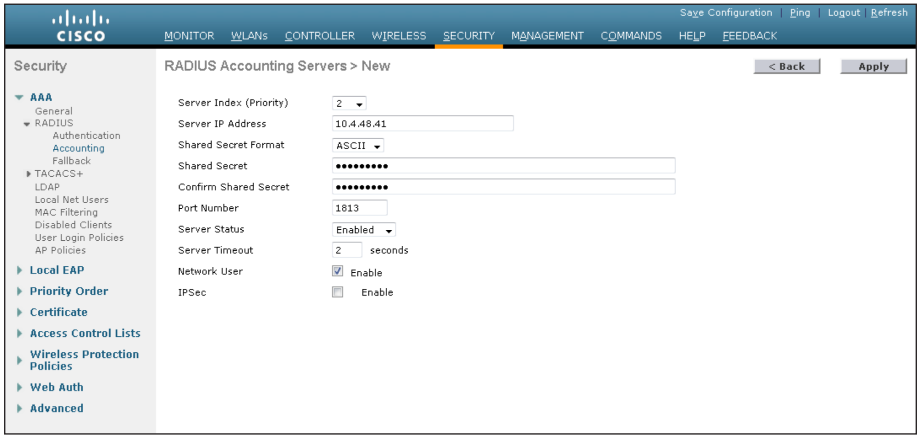
Perform this procedure for every wireless LAN controller (WLC) in the architecture, with the exception of the guest WLC in the DMZ.

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: Enter **10.4.48.41** for the IP address of the new server and your RADIUS shared secret, and then click **Apply.**



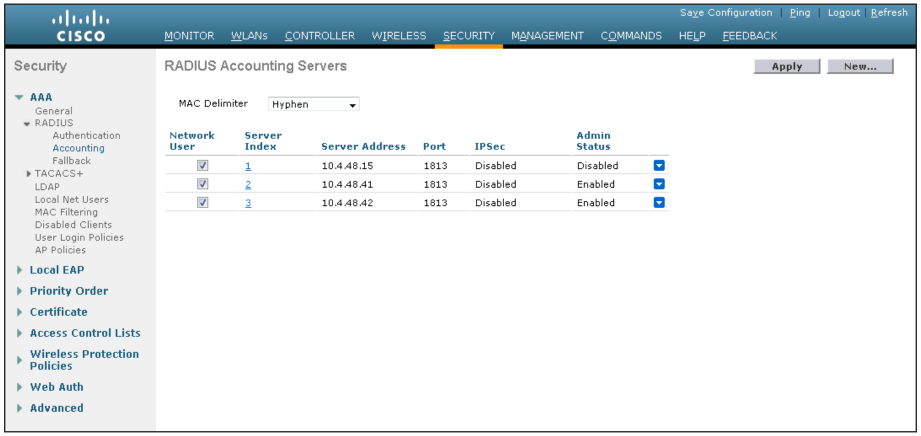
RADIUS Accounting Servers > New

Server Index (Priority)	2
Server IP Address	10.4.48.41
Shared Secret Format	ASCII
Shared Secret	•••••••••
Confirm Shared Secret	•••••••••
Port Number	1813
Server Status	Enabled
Server Timeout	2 seconds
Network User	☑ Enable
IPSec	☐ Enable

Step 5: Repeat 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**.



RADIUS Accounting Servers

MAC Delimiter Hyphen

Network User	Server Index	Server Address	Port	IPSec	Admin Status
☑	1	10.4.48.15	1813	Disabled	Disabled
☑	2	10.4.48.41	1813	Disabled	Enabled
☑	3	10.4.48.42	1813	Disabled	Enabled

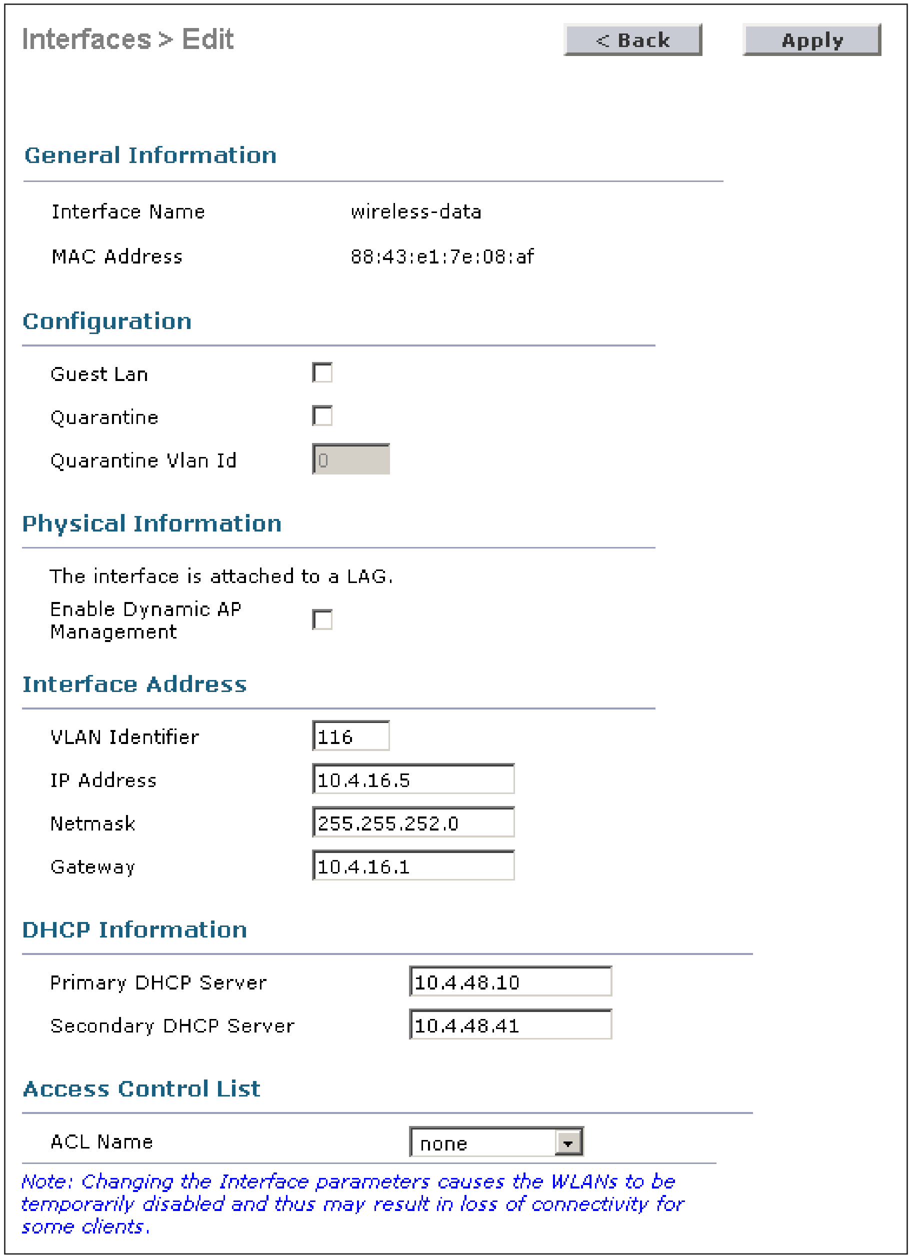
Procedure 6 Add secondary DHCP server on WLC

You need to add a secondary DHCP server to the WLC configuration in order to send DHCP requests to the engine for endpoint profiling.

Step 1: On the WLC, navigate to **Controller > Interfaces**. Select the interface for the clients you wish to monitor.

Step 2: In the DHCP Information section, add the Cisco ISE server as the Secondary DHCP Server, and then click **Apply**.

Step 3: When the warning appears with a message about the WLANs needing to be disabled, click **OK**.



General Information

Interface Name	wireless-data
MAC Address	88:43:e1:7e:08:af

Configuration

Guest Lan	□
Quarantine	□
Quarantine Vlan Id	0

Physical Information

The interface is attached to a LAG.

Enable Dynamic AP Management	□

Interface Address

VLAN Identifier	116
IP Address	10.4.16.5
Netmask	255.255.252.0
Gateway	10.4.16.1

DHCP Information

Primary DHCP Server	10.4.48.10
Secondary DHCP Server	10.4.48.41

Access Control List

ACL Name	none

Note: Changing the Interface parameters causes the WLANs to be temporarily disabled and thus may result in loss of connectivity for some clients.

Step 4: Click **Save Configuration**, and then click **OK**.

The network infrastructure is now enabled for monitoring the network to determine what types of devices are connecting. Additionally, authentication using ISE was 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 ISE
7. Install trusted root certificate in ISE
8. Install local certificate in 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.

Tech Tip

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

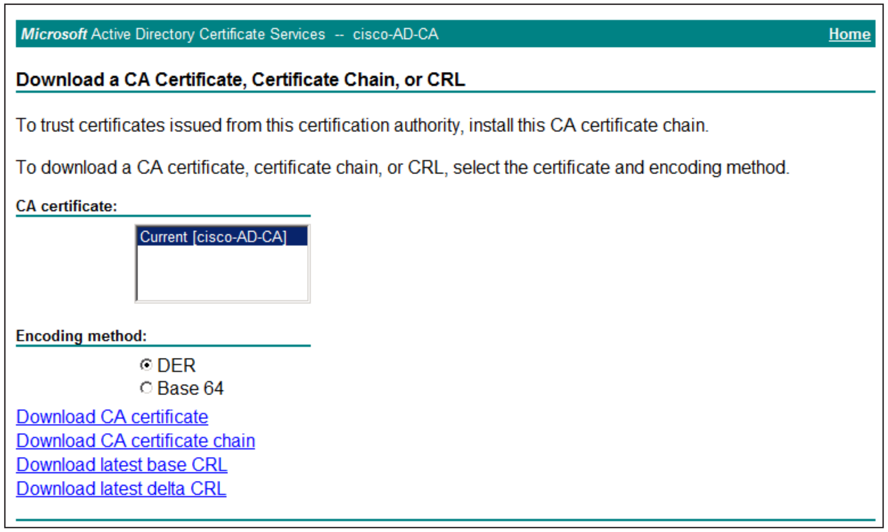
Install a trusted root certificate on the AD controller to distribute it to the clients so that certificates from the CA server will be trusted.

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.



Microsoft Active Directory Certificate Services -- cisco-AD-CA

Home

Download a CA Certificate, Certificate Chain, or CRL

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

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

CA certificate:

Current [cisco-AD-CA]

Encoding method:

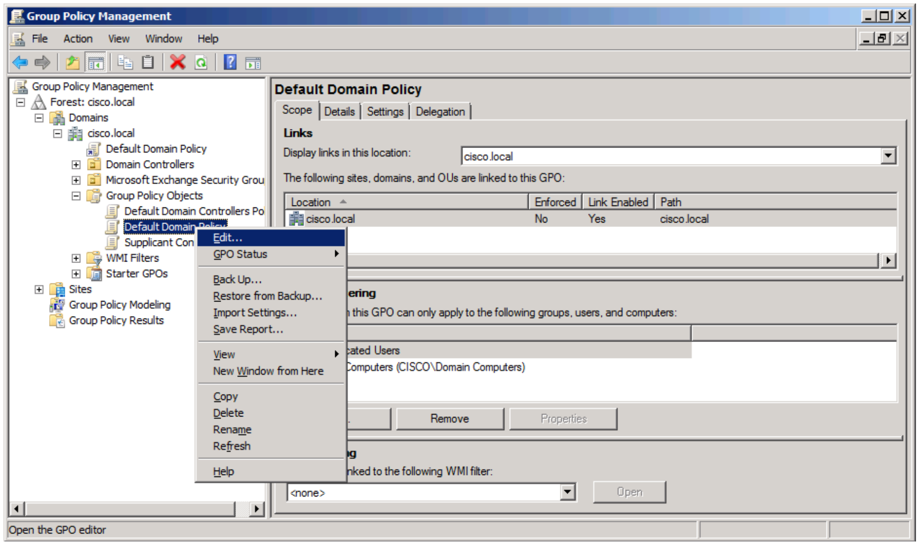
● DER
○ Base 64

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

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

Step 6: Expand the **Forest**, **Domain**, local domain, and **Group Policy Objects**.

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



Default Domain Policy

Links

Display links in this location: cisco.local

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

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

ering

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

cated Users
Computers (CISCO\Domain Computers)

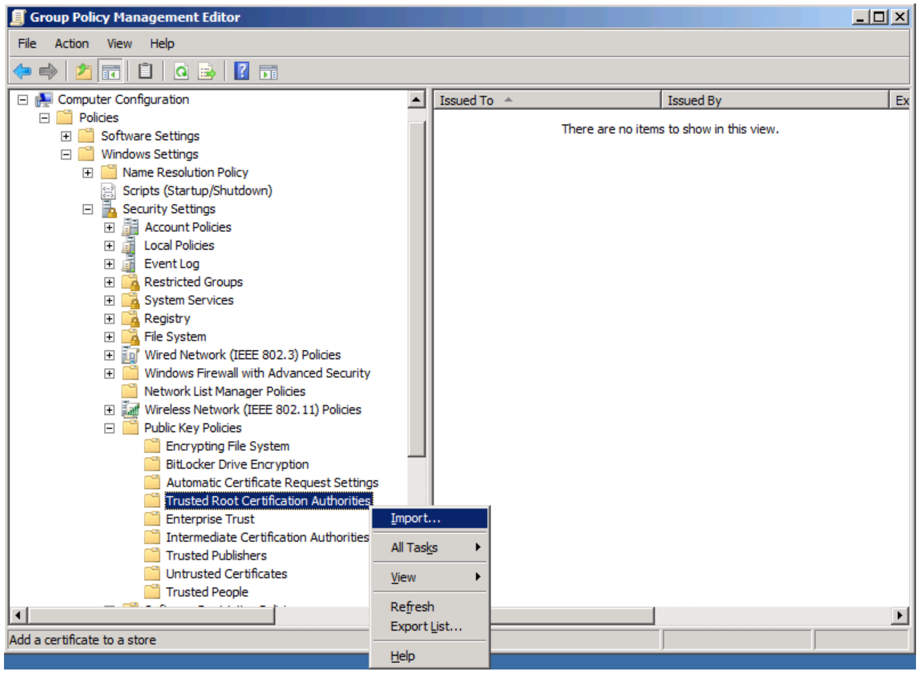
g

nked to the following WMI filter:

<none>

Open the GPO editor

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.

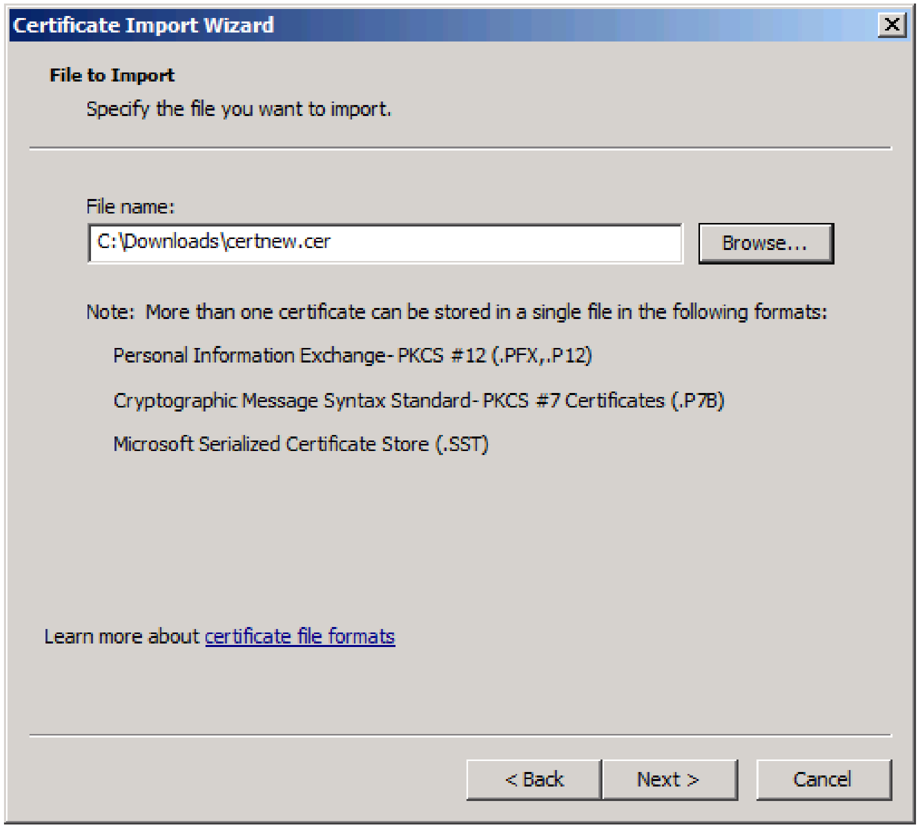


There are no items to show in this view.

Add a certificate to a store

Step 9: Click **Next**.

Step 10: Click **Browse**, locate the trusted root certificate saved in Step 4, and then click **Next**.



File to Import

Specify the file you want to import.

File name: C:\Downloads\certnew.cer

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

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

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

Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

Step 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**.

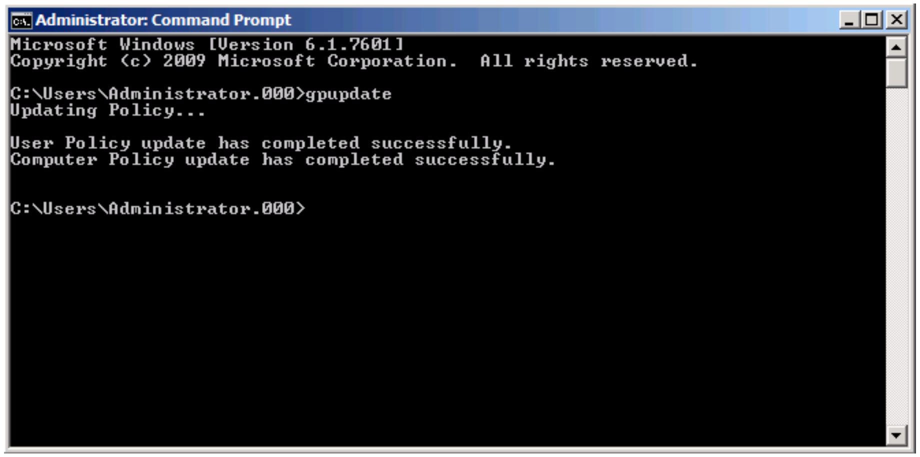
Procedure 3 Install trusted root on AD server

In addition to installing the trusted root certificate on the AD server to be distributed to workstations, you need to install it on the AD server directly. A 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 to open a command window.

Step 3: Type **gpupdate**. The group policy updates.



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

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

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


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

Procedure 4 Request a certificate for ISE from the CA

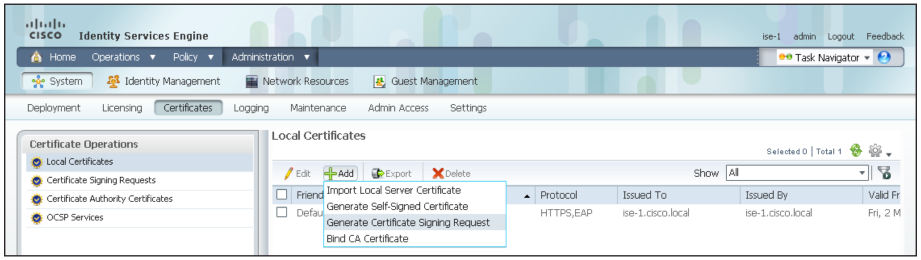
In order to obtain a certificate from the CA, Cisco ISE needs to generate a signing request that will be used by the CA to generate a certificate.

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

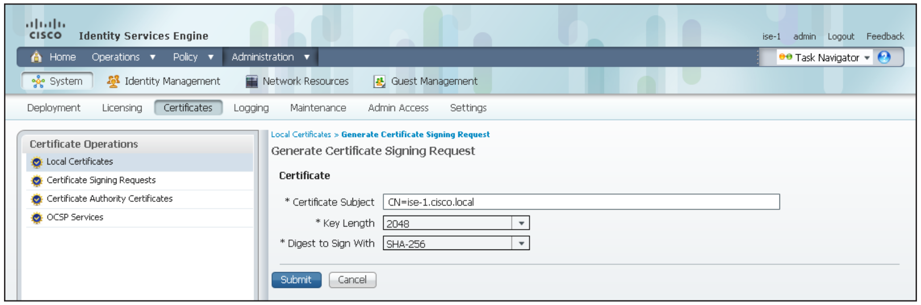
Step 2: Mouse over **Administration**, and then, from the System section of the menu, choose **Certificates**.

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

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


cisco Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
System Identity Management Network Resources Guest Management
Deployment Licensing Certificates Logging Maintenance Admin Access Settings
Certificate Operations
Local Certificates
Certificate Signing Requests
Certificate Authority Certificates
OCSP Services
Local Certificates
Selected 0 | Total 1
Edit Add Export Delete
Show All
Import Local Server Certificate
Generate Self-Signed Certificate
Generate Certificate Signing Request
Bind CA Certificate
Friend
Defau
Protocol
Issued To
Issued By
Valid Fr
HTTPS,EAP
ise-1.cisco.local
ise-1.cisco.local
Fri, 2 M

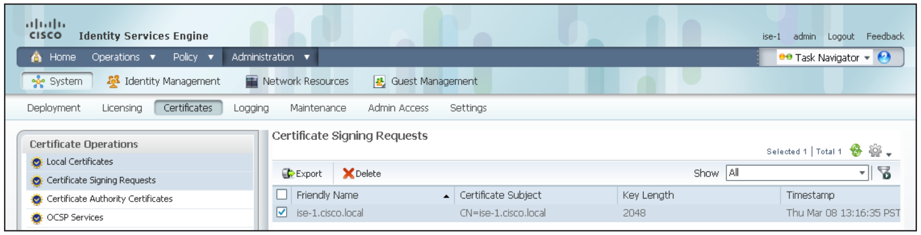
Step 5: Enter the fully qualified domain name (FQDN) of the Cisco ISE server in the Certificate Subject field after the "CN=", and then click **Submit**.


cisco Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
System Identity Management Network Resources Guest Management
Deployment Licensing Certificates Logging Maintenance Admin Access Settings
Certificate Operations
Local Certificates
Certificate Signing Requests
Certificate Authority Certificates
OCSP Services
Local Certificates > Generate Certificate Signing Request
Generate Certificate Signing Request
Certificate
Submit
Cancel

* Certificate Subject: CN=ise-1.cisco.local
* Key Length: 2048
* Digest to Sign With: SHA-256

Step 6: Click **OK.** This acknowledges the certificate was generated successfully.

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


cisco Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
System Identity Management Network Resources Guest Management
Deployment Licensing Certificates Logging Maintenance Admin Access Settings
Certificate Operations
Local Certificates
Certificate Signing Requests
Certificate Authority Certificates
OCSP Services
Certificate Signing Requests
Selected 1 | Total 1
Export Delete
Show All

	Friendly Name	Certificate Subject	Key Length	Timestamp
☑	ise-1.cisco.local	CN=ise-1.cisco.local	2048	Thu Mar 08 13:16:35 PST

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

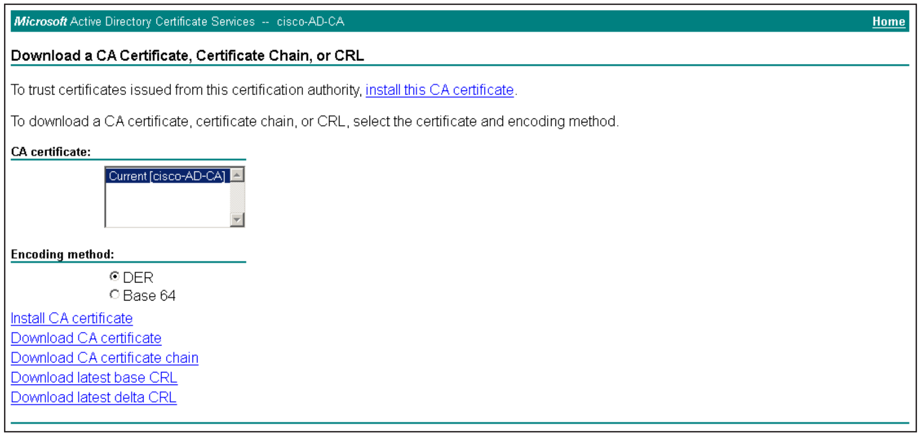
Procedure 5 Download CA root certificate

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.



Microsoft Active Directory Certificate Services -- cisco-AD-CA **Home**

Download a CA Certificate, Certificate Chain, or CRL

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

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

CA certificate:

Current [cisco-AD-CA]

Encoding method:

● DER
○ Base 64

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

Procedure 6 Issue certificate for ISE

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

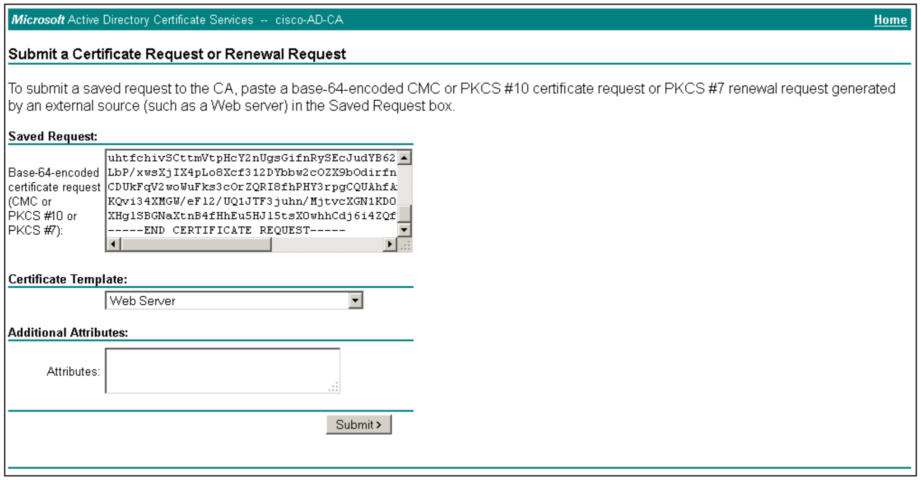
Step 2: Click **Request a certificate**.

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

Step 4: Open the certificate file saved in Procedure 4, "Request a certificate for ISE from the CA," in a text editor, such as Notepad. Select all the text and copy it to the clipboard.

Step 5: Paste the contents into the text box in the Saved Request section of the certificate request that is open in the browser.

Step 6: From the Certificate Template drop-down list, choose **Web Server**, and then click **Submit**.



Microsoft Active Directory Certificate Services -- cisco-AD-CA **Home**

Submit a Certificate Request or Renewal Request

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

Saved Request:

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

```
uhtfchivSCttmVtpHcY2nUgsGifnRySEcJudYB62
LbP/xwsXjIX4pLo8Xcf312DYbbw2cOZX9bOdirfn
CDUkFqV2woWuFks3cOrZQRI8fhPHY3rpgCQUAhfA
KQvi34XMGW/eFl2/UQ1JTF3juhn/MjtvcXGN1KDO
XHglSBGNaXtnB4fHhEu5HJl5tsXOwhhCdj6i4ZQf
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

Additional Attributes:

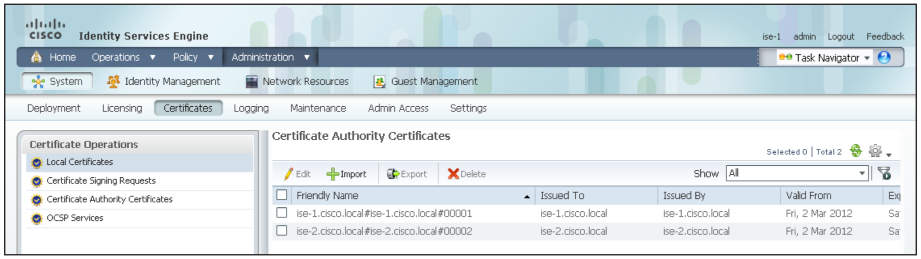
Attributes:

Step 7: Select **DER encoded**, and then click **Download certificate.** The certificate saves to your local machine.

Procedure 7 Install trusted root certificate in 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 Authority Certificates,** and then click **Import**.

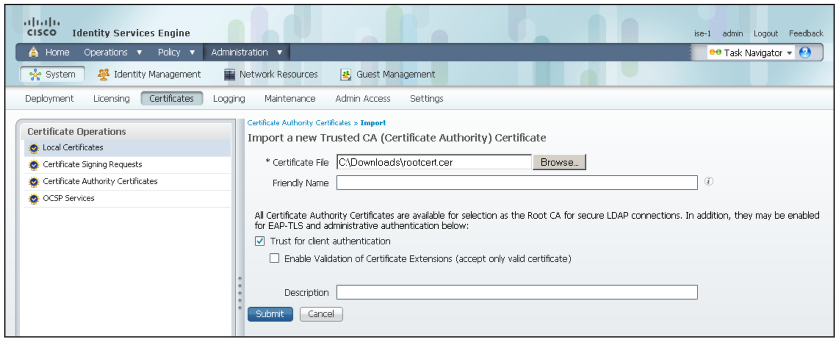

Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
System Identity Management Network Resources Guest Management
Deployment Licensing Certificates Logging Maintenance Admin Access Settings
Certificate Operations
Local Certificates
Certificate Signing Requests
Certificate Authority Certificates
OCSP Services
Selected 0 | Total 2
Edit Import Export Delete
Show All

Certificate Authority Certificates

	Friendly Name	Issued To	Issued By	Valid From	Ex
□	ise-1.cisco.local#ise-1.cisco.local#00001	ise-1.cisco.local	ise-1.cisco.local	Fri, 2 Mar 2012	Sa
□	ise-2.cisco.local#ise-2.cisco.local#00002	ise-2.cisco.local	ise-2.cisco.local	Fri, 2 Mar 2012	Sa

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**.


Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
System Identity Management Network Resources Guest Management
Deployment Licensing Certificates Logging Maintenance Admin Access Settings
Certificate Operations
Local Certificates
Certificate Signing Requests
Certificate Authority Certificates
OCSP Services
Certificate Authority Certificates > Import
Browse...
Submit
Cancel

Import a new Trusted CA (Certificate Authority) Certificate

* Certificate File: C:\Downloads\rootcert.cer

Friendly Name:

All Certificate Authority Certificates are available for selection as the Root CA for secure LDAP connections. In addition, they may be enabled for EAP-TLS and administrative authentication below:

☑ Trust for client authentication

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

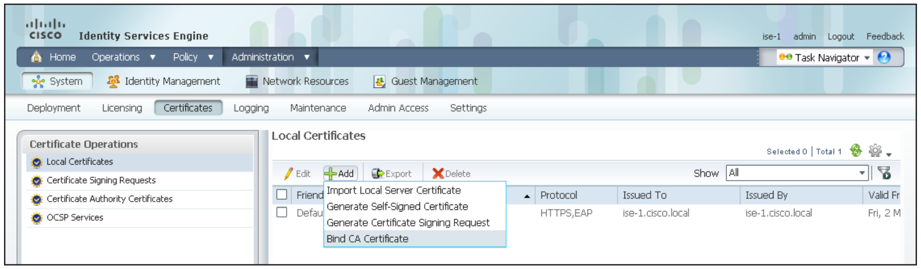
Description:

Procedure 8 Install local certificate in 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**.

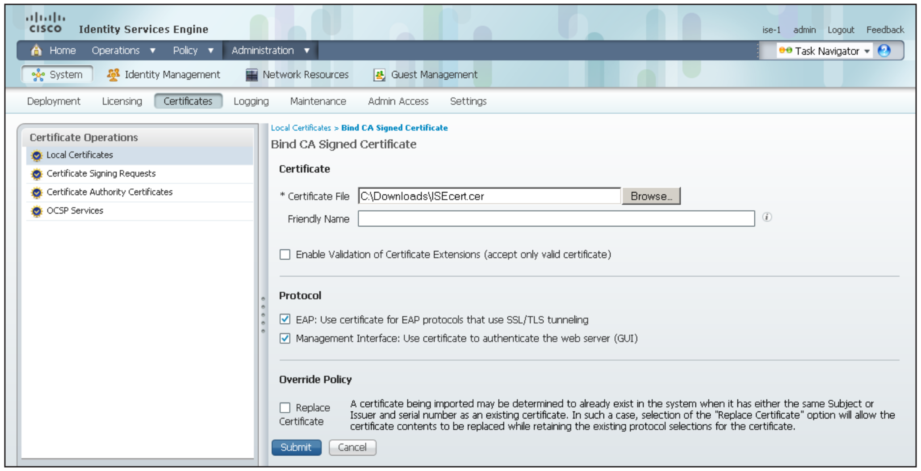

Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
System Identity Management Network Resources Guest Management
Deployment Licensing Certificates Logging Maintenance Admin Access Settings
Certificate Operations
Local Certificates
Certificate Signing Requests
Certificate Authority Certificates
OCSP Services
Selected 0 | Total 1
Edit Add Export Delete
Show All
Import Local Server Certificate
Generate Self-Signed Certificate
Generate Certificate Signing Request
Bind CA Certificate

Local Certificates

	Friend	Protocol	Issued To	Issued By	Valid Fr
□	Defau	HTTPS,EAP	ise-1.cisco.local	ise-1.cisco.local	Fri, 2 M

Step 4: Click **Browse** and locate the certificate saved from Step 1, "Issue certificate for ISE."

Step 5: In the Protocol section, select both the EAP and Management Interface check boxes. When you receive a warning that checking the Management Interface box will require the Cisco ISE appliance to restart, click **OK**, and then click **Submit**.


Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
System Identity Management Network Resources Guest Management
Deployment Licensing Certificates Logging Maintenance Admin Access Settings
Certificate Operations
Local Certificates
Certificate Signing Requests
Certificate Authority Certificates
OCSP Services
Local Certificates > Bind CA Signed Certificate
Browse...
Submit
Cancel

Bind CA Signed Certificate

Certificate

* Certificate File: C:\Downloads\ISEcert.cer

Friendly Name:

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

Protocol

☑ EAP: Use certificate for EAP protocols that use SSL/TLS tunneling

☑ Management Interface: Use certificate to authenticate the web server (GUI)

Override Policy

□ Replace Certificate — A certificate being imported may be determined to already exist in the system when it has either the same Subject or Issuer and serial number as an existing certificate. In such a case, selection of the "Replace Certificate" option will allow the certificate contents to be replaced while retaining the existing protocol selections for the certificate.

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

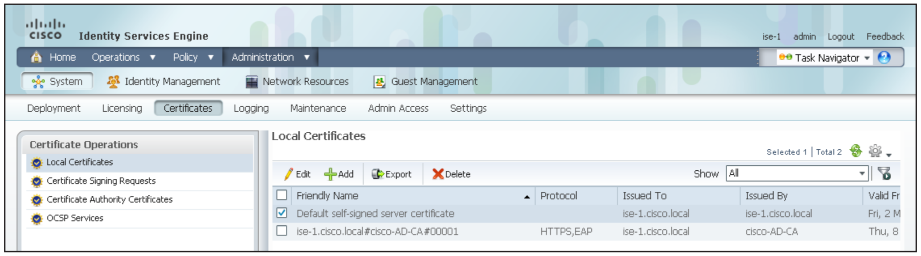
Procedure 9 Delete old certificate and request

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

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

Step 2: Click **Local Certificates**.

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

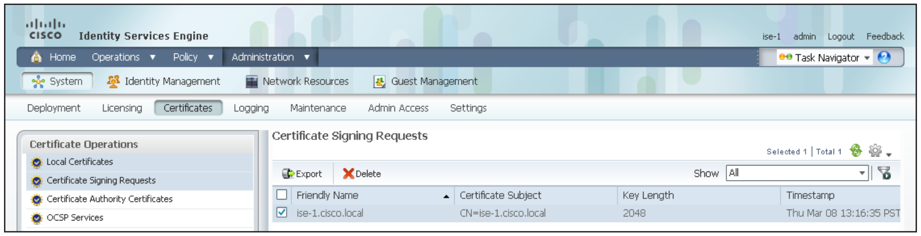


	Friendly Name	Protocol	Issued To	Issued By	Valid Fr
☑	Default self-signed server certificate		ise-1.cisco.local	ise-1.cisco.local	Fri, 2 M
□	ise-1.cisco.local#cisco-AD-CA#00001	HTTPS,EAP	ise-1.cisco.local	cisco-AD-CA	Thu, 8

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.”



	Friendly Name	Certificate Subject	Key Length	Timestamp
☑	ise-1.cisco.local	CN=ise-1.cisco.local	2048	Thu Mar 08 13:16:35 PST

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

Process

Enable 802.1X authentication

1. Create ISE policies
2. Enable certificates
3. Enable EAP-TLS

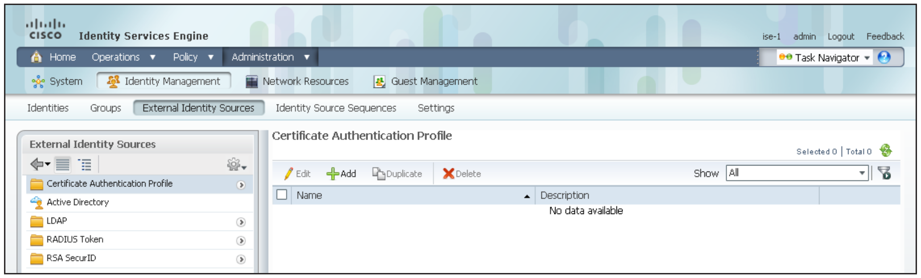
You will configure ISE policies to support 802.1X authentication using digital certificates for both wired and wireless users.

Procedure 1 Create 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**.

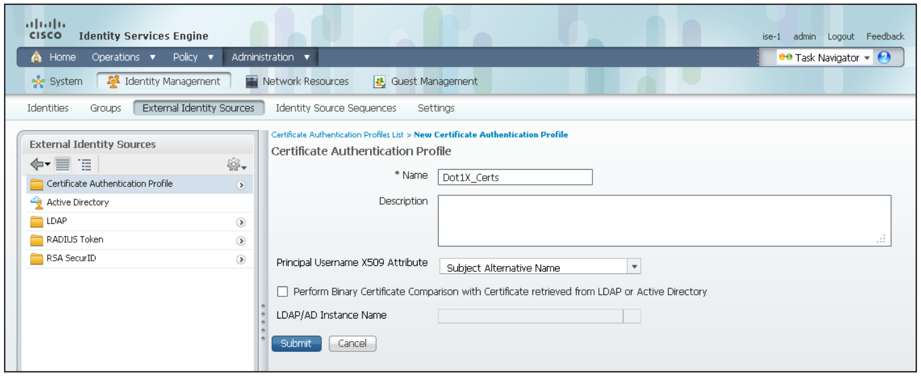
Step 2: In the left pane, click **Certificate Authentication Profile,** and then click **Add**.



	Name	Description
□		

No data available

Step 3: Give the profile a meaningful name, and then, from the Principal Username X509 Attribute drop-down list, choose **Subject Alternative Name**.



cisco Identity Services Engine
ise-1 admin Logout Feedback
Home Operations ▾ Policy ▾ Administration ▾
Task Navigator ▾
System Identity Management Network Resources Guest Management
Identities Groups External Identity Sources Identity Source Sequences Settings
External Identity Sources
Certificate Authentication Profile
Active Directory
LDAP
RADIUS Token
RSA SecurID

Certificate Authentication Profiles List > **New Certificate Authentication Profile**

Certificate Authentication Profile

* Name: Dot1X_Certs

Description:

Principal Username X509 Attribute: Subject Alternative Name ▾

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

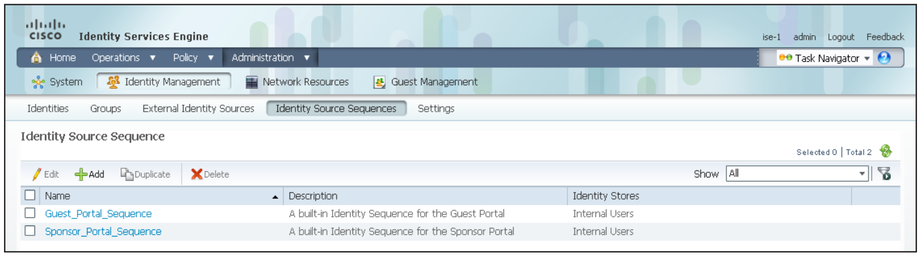
LDAP/AD Instance Name:

Submit Cancel

Step 4: 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 5: Click **Identity Source Sequences**, and then click **Add**.



cisco Identity Services Engine
ise-1 admin Logout Feedback
Home Operations ▾ Policy ▾ Administration ▾
Task Navigator ▾
System Identity Management Network Resources Guest Management
Identities Groups External Identity Sources Identity Source Sequences Settings
Edit Add Duplicate Delete
Show All

Identity Source Sequence

Selected 0 | Total 2

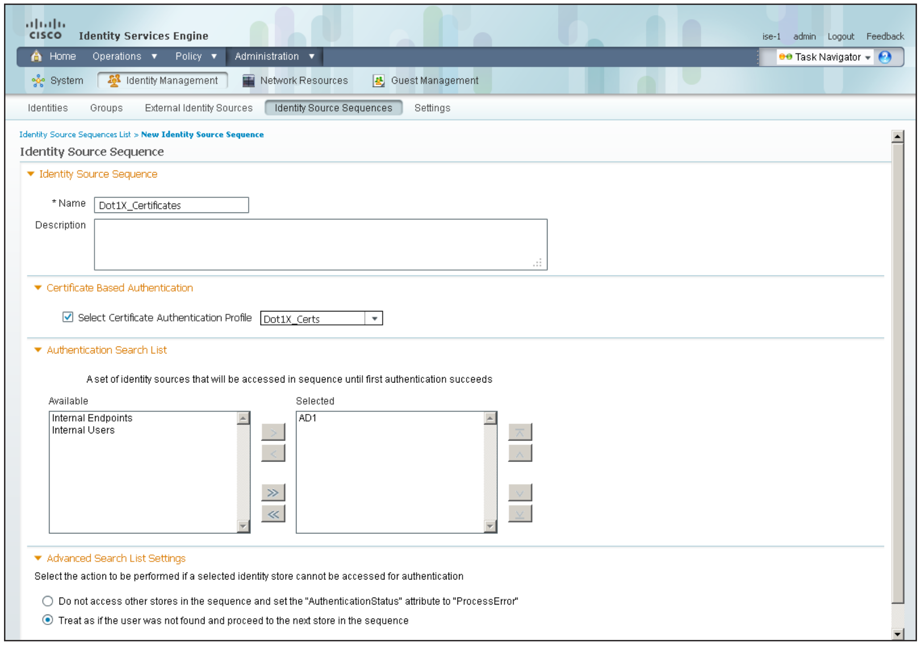
□	Name	Description	Identity Stores
□	Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal	Internal Users
□	Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal	Internal Users

Step 6: Give the sequence a meaningful name.

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

Step 8: In the Authentication Search List section, double-click the AD server from the **Available** list to move it to the **Selected** list.

Step 9: In the Advanced Search List Settings section, select **Treat as if the user was not found and proceed to the next store in the sequence**.



cisco Identity Services Engine
ise-1 admin Logout Feedback
Home Operations ▾ Policy ▾ Administration ▾
Task Navigator ▾
System Identity Management Network Resources Guest Management
Identities Groups External Identity Sources Identity Source Sequences Settings

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

Identity Source Sequence

▾ Identity Source Sequence

* Name: Dot1X_Certificates

Description:

▾ Certificate Based Authentication

☑ Select Certificate Authentication Profile: Dot1X_Certs ▾

▾ Authentication Search List

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

Available: Internal Endpoints, Internal Users

Selected: AD1

▾ Advanced Search List Settings

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

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

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

Step 10: Click **Submit**.

Procedure 2 Enable certificates

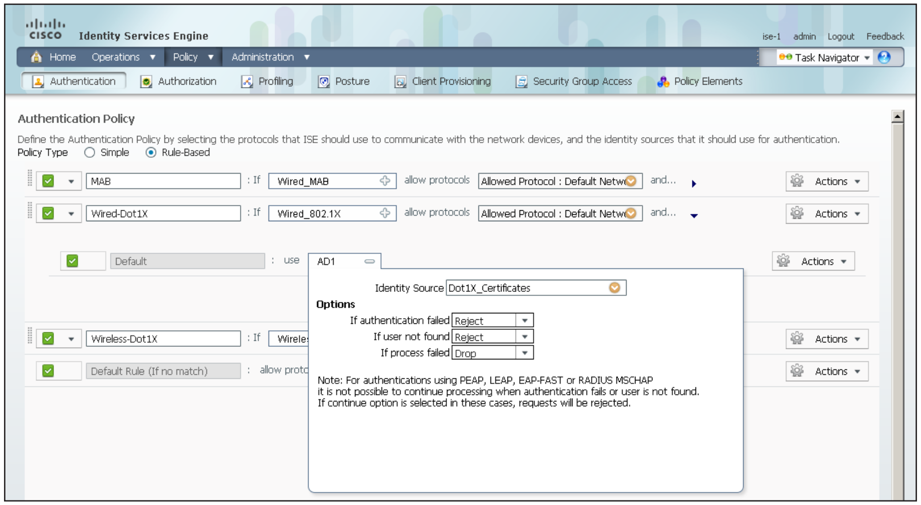
Now that you have created a certificate authentication profile and identity source sequence for digital certificates, you need to enable the 802.1X authentication policies for both wired and wireless users.

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

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

Step 3: Click the **+** symbol next to the AD1 identity store entry.

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



Authentication Policy

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

Policy Type ○ Simple ● Rule-Based

☑ MAB : If Wired_MAB allow protocols Allowed Protocol : Default Netw and...

☑ Wired-Dot1X : If Wired_802.1X allow protocols Allowed Protocol : Default Netw and...

☑ Default : use AD1

Identity Source Dot1X_Certificates

Options

If authentication failed Reject

If user not found Reject

If process failed Drop

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

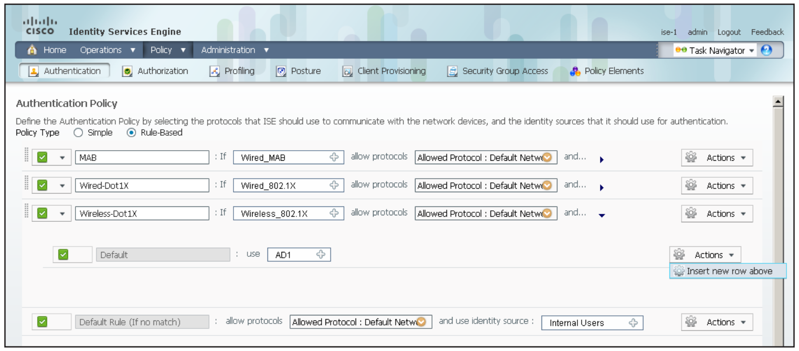
☑ Wireless-Dot1X : If Wireles

☑ Default Rule (If no match) : allow proto

For wireless users, you should 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 like 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 will get their certificates pushed to them and other endpoints can manually obtain a certificate.

Step 5: Click the black triangle to the right of the **and...** of the Wireless-Dot1X rule. This brings up the identity store used for this rule.

Step 6: In the Actions drop-down list next to the Default rule, choose **Insert new rule above**.



Authentication Policy

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

Policy Type ○ Simple ● Rule-Based

☑ MAB : If Wired_MAB allow protocols Allowed Protocol : Default Netw and...

☑ Wired-Dot1X : If Wired_802.1X allow protocols Allowed Protocol : Default Netw and...

☑ Wireless-Dot1X : If Wireless_802.1X allow protocols Allowed Protocol : Default Netw and...

☑ Default : use AD1

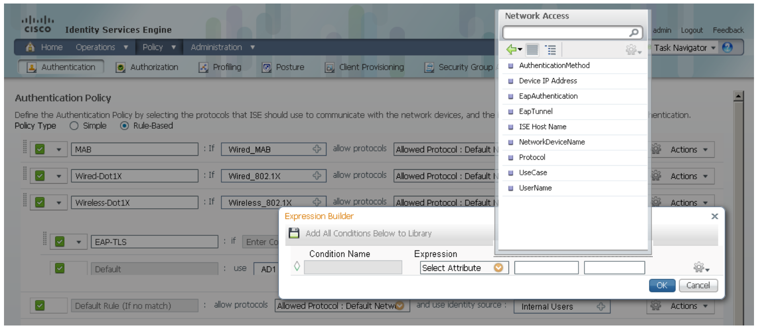
☑ Default Rule (If no match) : allow protocols Allowed Protocol : Default Netw and use identity source : Internal Users

Step 7: Give the rule a name, and then open the expression builder by clicking the symbol next to the **Enter Condition** box.

Step 8: Click **Create New Condition (Advance Option)**.

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

Step 10: Click the arrow next to Network Access, and then select **EapAuthentication**.



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the ihentication.

Policy Type ○ Simple ● Rule-Based

☑ MAB : If Wired_MAB allow protocols Allowed Protocol : Default N

☑ Wired-Dot1X : If Wired_802.1X allow protocols Allowed Protocol : Default N

☑ Wireless-Dot1X : If Wireless_802.1X allow protocols Allowed Protocol : Default N

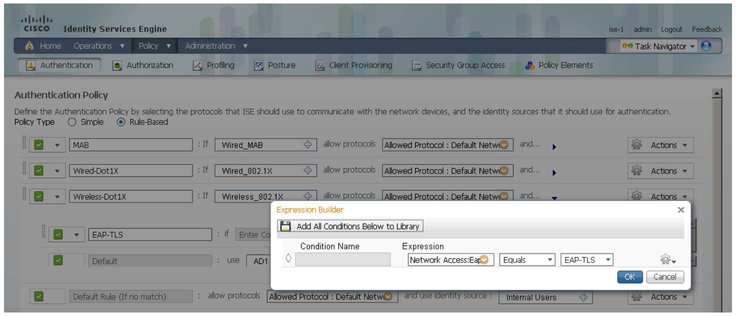
☑ EAP-TLS : if Enter Co

☑ Default : use AD1

Condition Name | Expression: Select Attribute

☑ Default Rule (If no match) : allow protocols Allowed Protocol : Default Netw and use identity source : Internal Users

Step 11: In the second drop-down list, choose **Equals,** and in the last drop-down list, choose **EAP-TLS**, and then click **OK**.


Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Actions
Add All Conditions Below to Library
OK Cancel

Authentication Policy

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

Policy Type ○ Simple ● Rule-Based

☑ MAB : If Wired_MAB allow protocols Allowed Protocol : Default Netw… and…

☑ Wired-Dot1X : If Wired_802.1X allow protocols Allowed Protocol : Default Netw… and…

☑ Wireless-Dot1X : If Wireless_802.1X allow protocols Allowed Protocol : Default Netw… and…

☑ EAP-TLS : if Enter Co…

☑ Default : use AD1

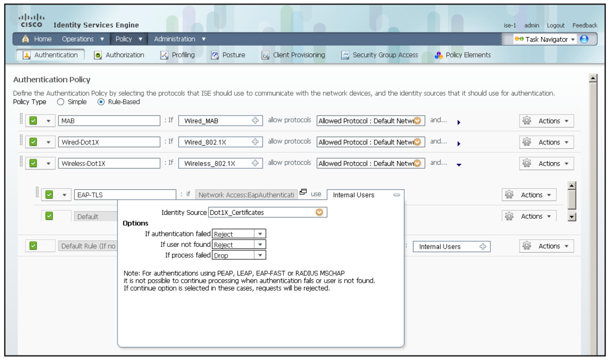
☑ Default Rule (If no match) : allow protocols Allowed Protocol : Default Netw… and use identity source : Internal Users

Expression Builder

Condition Name | Expression: Network Access:Eap… Equals EAP-TLS

Step 12: Click the **+** symbol next to Internal Users.

Step 13: In the Identity Store drop-down list, choose the identity source sequence created in Procedure 1, “Create ISE policies,” use the default options for this identity source, and then click anywhere in the window to continue.


Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Actions

Authentication Policy

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

Policy Type ○ Simple ● Rule-Based

☑ MAB : If Wired_MAB allow protocols Allowed Protocol : Default Netw… and…

☑ Wired-Dot1X : If Wired_802.1X allow protocols Allowed Protocol : Default Netw… and…

☑ Wireless-Dot1X : If Wireless_802.1X allow protocols Allowed Protocol : Default Netw… and…

☑ EAP-TLS : if Network Access:EapAuthenticati use Internal Users

☑ Default

☑ Default Rule (If no … Internal Users

Identity Source Dot1X_Certificates

Options

If authentication failed Reject

If user not found Reject

If process failed Drop

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

Step 14: Click **Save**.

Procedure 3 Enable EAP-TLS

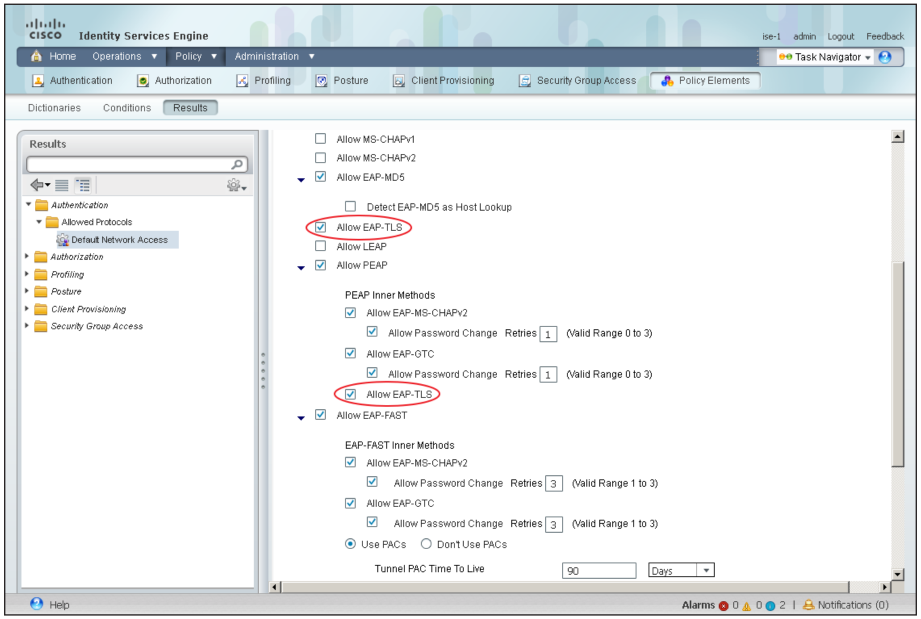
In a previous section, you disabled EAP-TLS. Now that you are using digital certificates, you need to re-enable it.

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**.


Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Dictionaries Conditions Results
Results
Authentication
Allowed Protocols
Default Network Access
Authorization
Profiling
Posture
Client Provisioning
Security Group Access
Help
Alarms 0 0 2 | Notifications (0)

□ Allow MS-CHAPv1

□ Allow MS-CHAPv2

☑ Allow EAP-MD5

□ Detect EAP-MD5 as Host Lookup

☑ Allow EAP-TLS

□ Allow LEAP

☑ Allow PEAP

PEAP Inner Methods

☑ Allow EAP-MS-CHAPv2

☑ Allow Password Change Retries 1 (Valid Range 0 to 3)

☑ Allow EAP-GTC

☑ Allow Password Change Retries 1 (Valid Range 0 to 3)

☑ Allow EAP-TLS

☑ Allow EAP-FAST

EAP-FAST Inner Methods

☑ Allow EAP-MS-CHAPv2

☑ Allow Password Change Retries 3 (Valid Range 1 to 3)

☑ Allow EAP-GTC

☑ Allow Password Change Retries 3 (Valid Range 1 to 3)

● Use PACs ○ Don't Use PACs

Tunnel PAC Time To Live 90 Days

Process

Configure 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

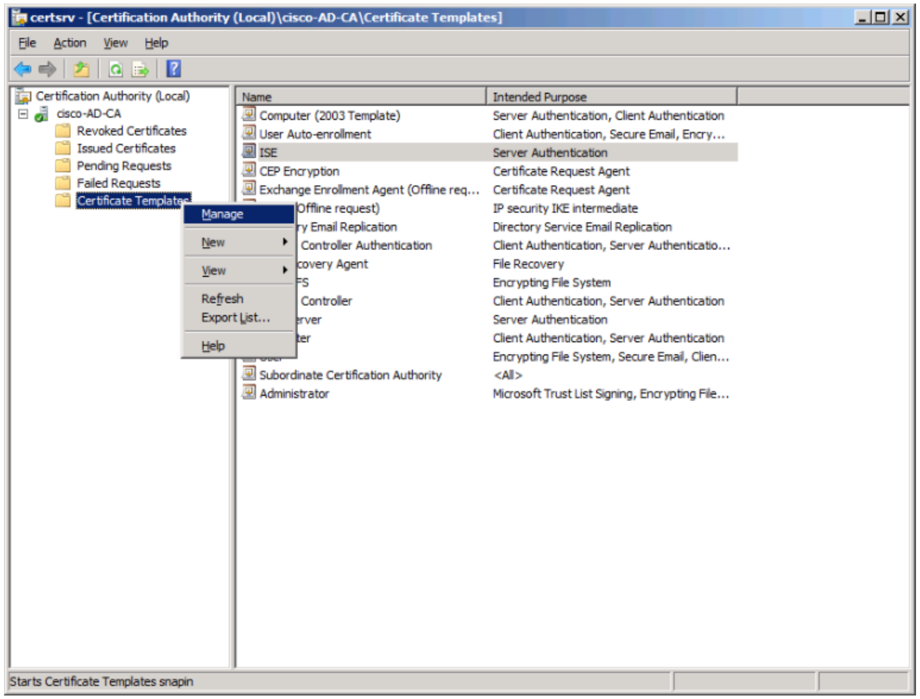
In this deployment you will be using Group Policy Objects (GPOs) to distribute certificates and to configure the native 802.1X supplicant for Windows XP and later endpoints that are members of the domain. Machine certificates are distributed when the machine joins the domain and user certificates are 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.



Name	Intended Purpose
Computer (2003 Template)	Server Authentication, Client Authentication
User Auto-enrollment	Client Authentication, Secure Email, Encry...
ISE	Server Authentication
CEP Encryption	Certificate Request Agent
Exchange Enrollment Agent (Offline req...	Certificate Request Agent
Offline request)	IP security IKE intermediate
y Email Replication	Directory Service Email Replication
Controller Authentication	Client Authentication, Server Authenticatio...
covery Agent	File Recovery
FS	Encrypting File System
Controller	Client Authentication, Server Authentication
rver	Server Authentication
ter	Client Authentication, Server Authentication
[illegible]	Encrypting File System, Secure Email, Clien...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting File...

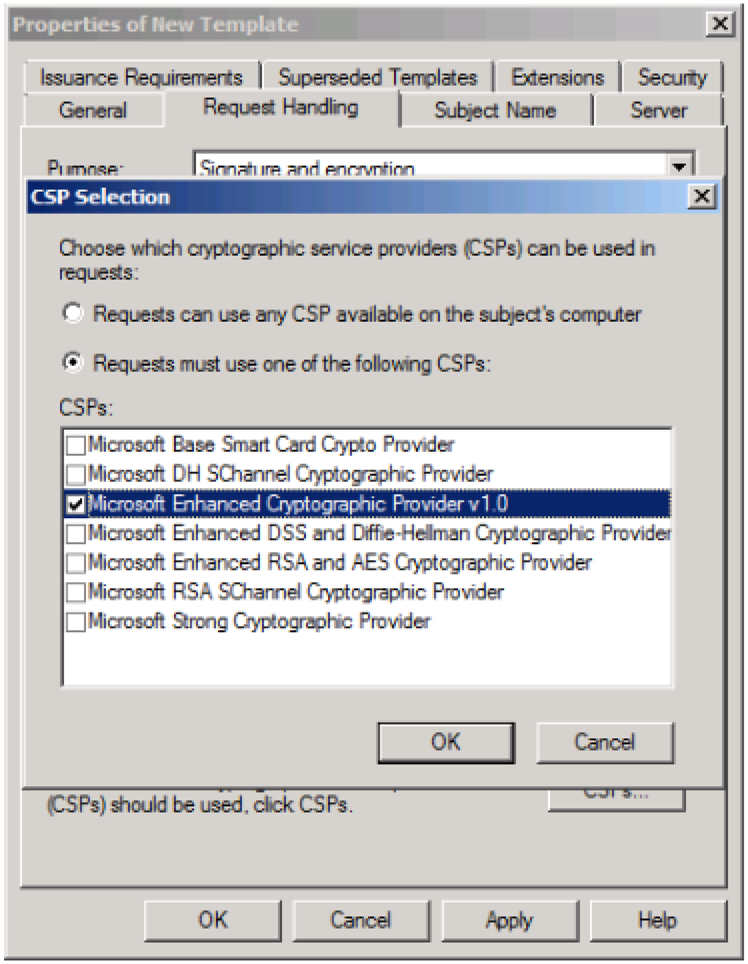
Step 3: Right-click the Computer template, and then choose **Duplicate Template**.

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

Step 5: In the template properties 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**.



Purpose: Signature and encryption

(CSPs) should be used, click CSPs.

CSP Selection

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

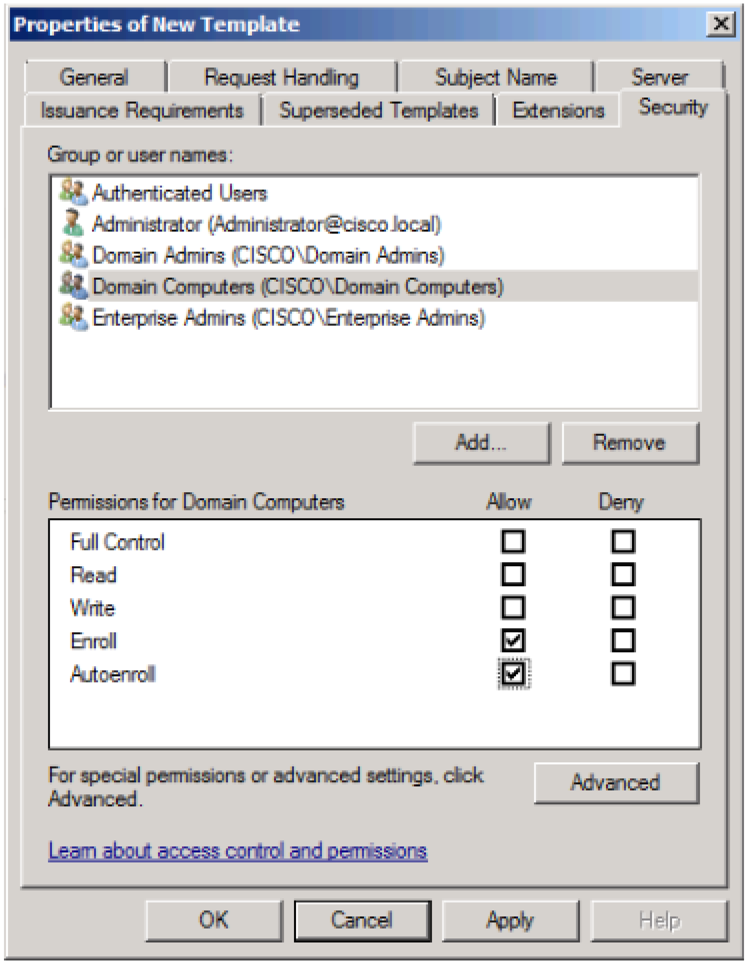
○ Requests can use any CSP available on the subject's computer

● Requests must use one of the following CSPs:

CSPs:

□ Microsoft Base Smart Card Crypto Provider
□ Microsoft DH SChannel Cryptographic Provider
☑ Microsoft Enhanced Cryptographic Provider v1.0
□ Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Provider
□ Microsoft Enhanced RSA and AES Cryptographic Provider
□ Microsoft RSA SChannel Cryptographic Provider
□ Microsoft Strong Cryptographic Provider

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



Group or user names:

- Authenticated Users
- Administrator (Administrator@cisco.local)
- Domain Admins (CISCO\Domain Admins)
- Domain Computers (CISCO\Domain Computers)
- Enterprise Admins (CISCO\Enterprise Admins)

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

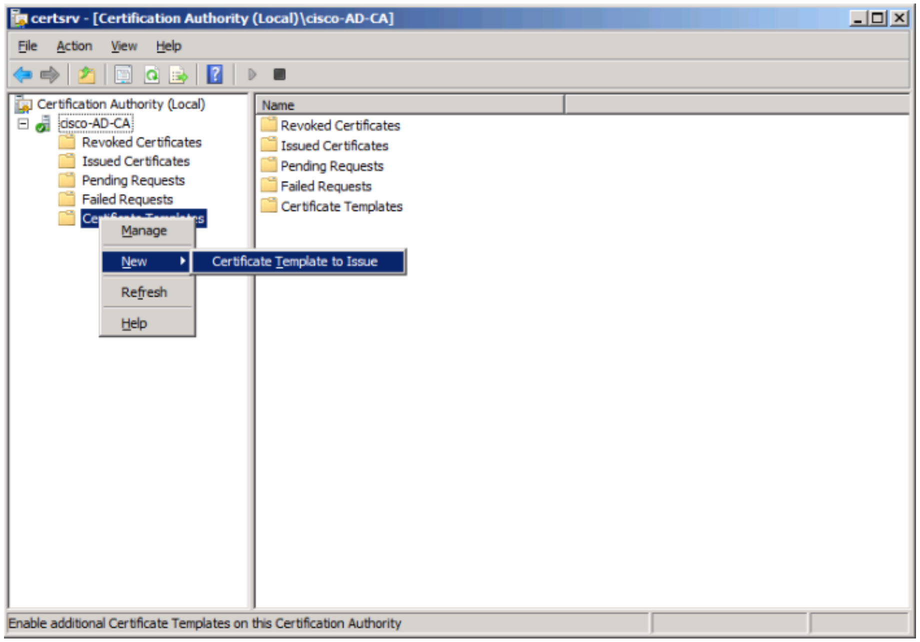
For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

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

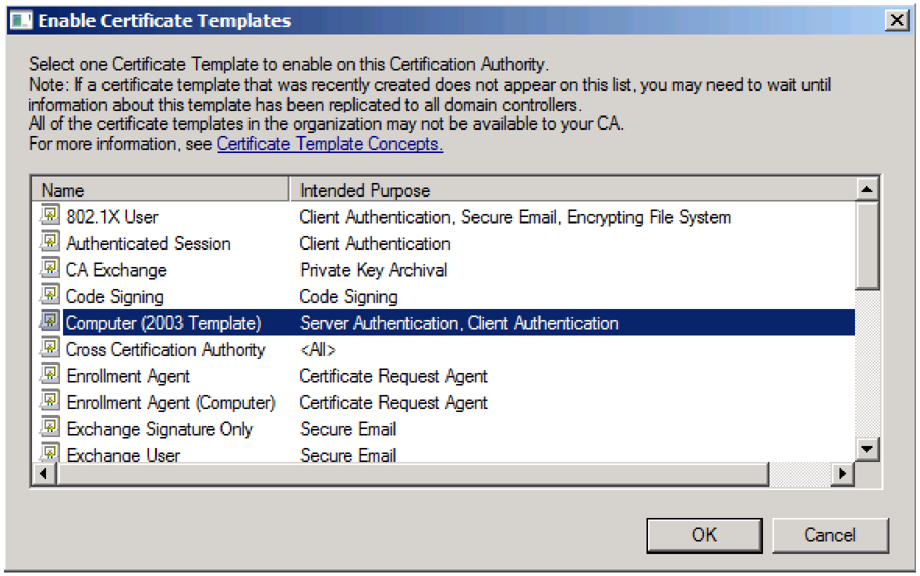
Step 10: Close the Certificate Templates Console.

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



Enable additional Certificate Templates on this Certification Authority

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



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

Name	Intended Purpose
802.1X User	Client Authentication, Secure Email, Encrypting File System
Authenticated Session	Client Authentication
CA Exchange	Private Key Archival
Code Signing	Code Signing
Computer (2003 Template)	Server Authentication, Client Authentication
Cross Certification Authority	<All>
Enrollment Agent	Certificate Request Agent
Enrollment Agent (Computer)	Certificate Request Agent
Exchange Signature Only	Secure Email
Exchange User	Secure Email

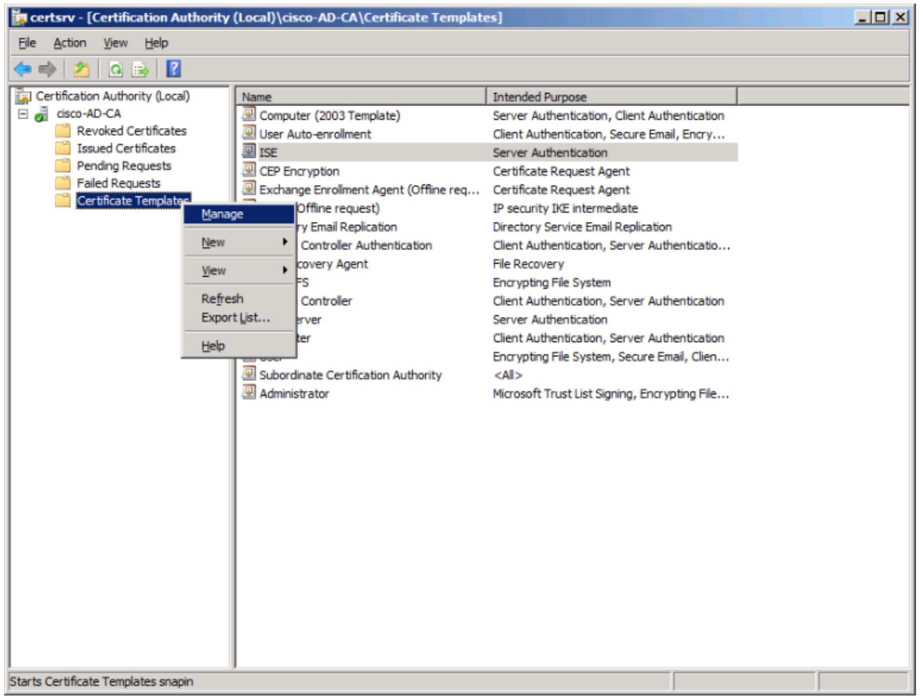
When machines join the domain or when the GPO policy is refreshed (the default period is 90 minutes), the machine receives a machine certificate to allow for 802.1X machine authentication.

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. You need to create a certificate template for these users to enable auto-enrollment.

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.



certsrv - [Certification Authority (Local)\cisco-AD-CA\Certificate Templates]

Name	Intended Purpose
Computer (2003 Template)	Server Authentication, Client Authentication
User Auto-enrollment	Client Authentication, Secure Email, Encry...
ISE	Server Authentication
CEP Encryption	Certificate Request Agent
Exchange Enrollment Agent (Offline req...	Certificate Request Agent
Offline request)	IP security IKE intermediate
y Email Replication	Directory Service Email Replication
Controller Authentication	Client Authentication, Server Authenticatio...
covery Agent	File Recovery
FS	Encrypting File System
Controller	Client Authentication, Server Authentication
rver	Server Authentication
ter	Client Authentication, Server Authentication
	Encrypting File System, Secure Email, Clien...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting File...

Starts Certificate Templates snapin

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

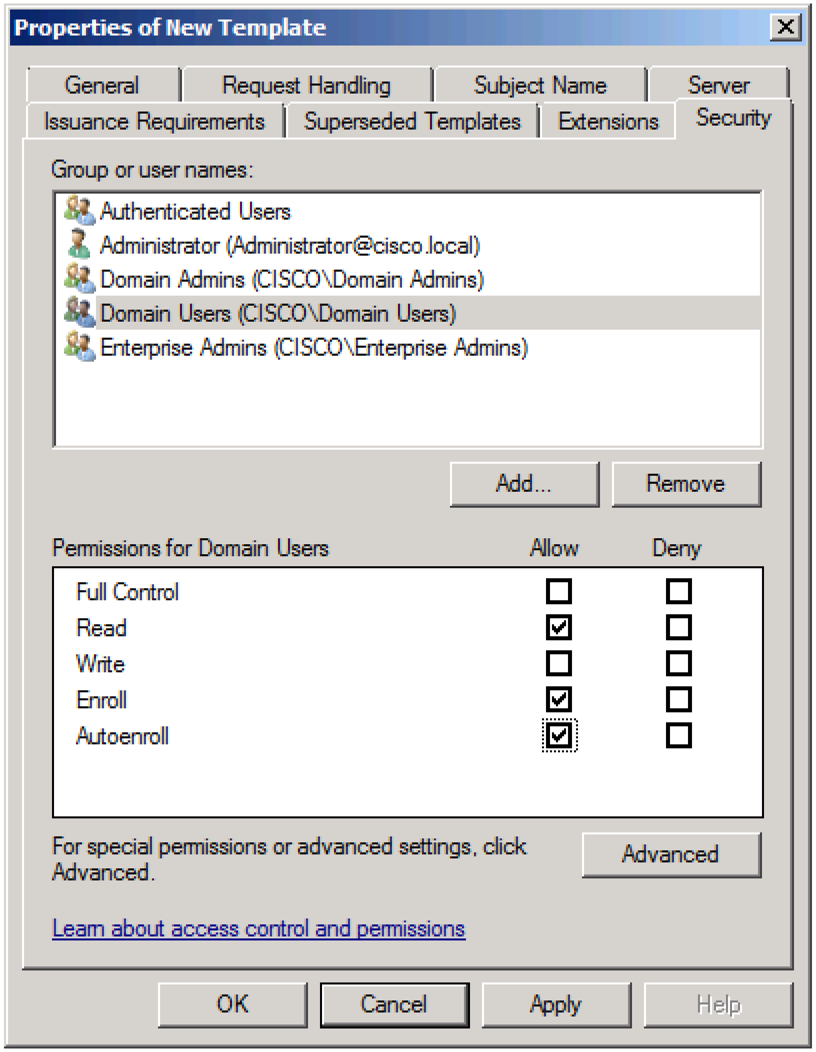
Step 4: For compatibility with Windows XP, make sure that **Windows 2003 Server Enterprise** is selected.

Step 5: In the template properties 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 make sure **Allow** is selected for **Read**, **Enroll,** and **Autoenroll**.



Properties of New Template

Group or user names:

- Authenticated Users
- Administrator (Administrator@cisco.local)
- Domain Admins (CISCO\Domain Admins)
- Domain Users (CISCO\Domain Users)
- Enterprise Admins (CISCO\Enterprise Admins)

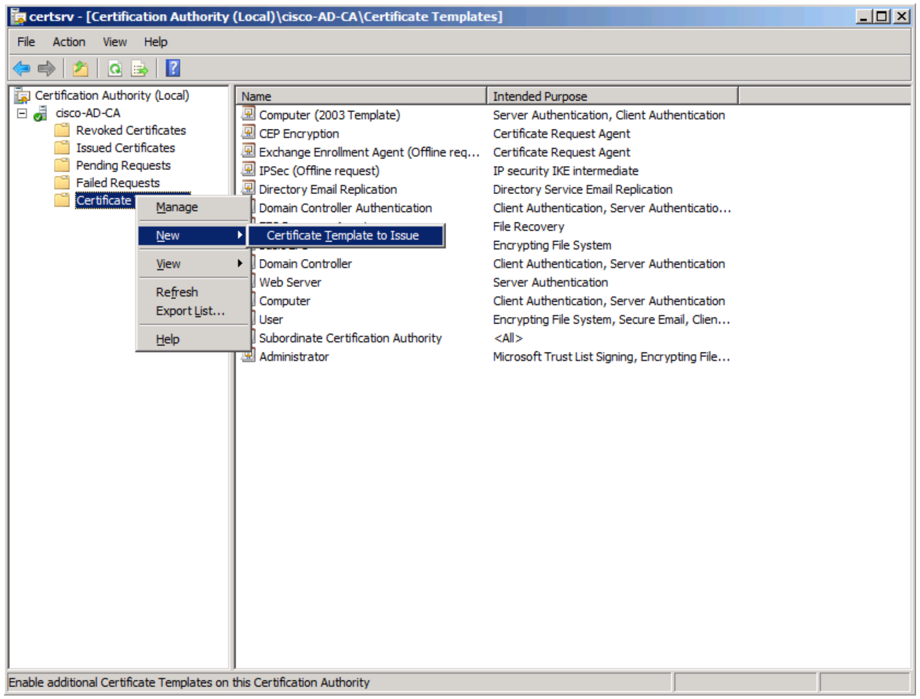
Permissions for Domain Users	Allow	Deny
Full Control	□	□
Read	☑	□
Write	□	□
Enroll	☑	□
Autoenroll	☑	□

For special permissions or advanced settings, click Advanced.

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

Step 10: Close the Certificate Templates Console.

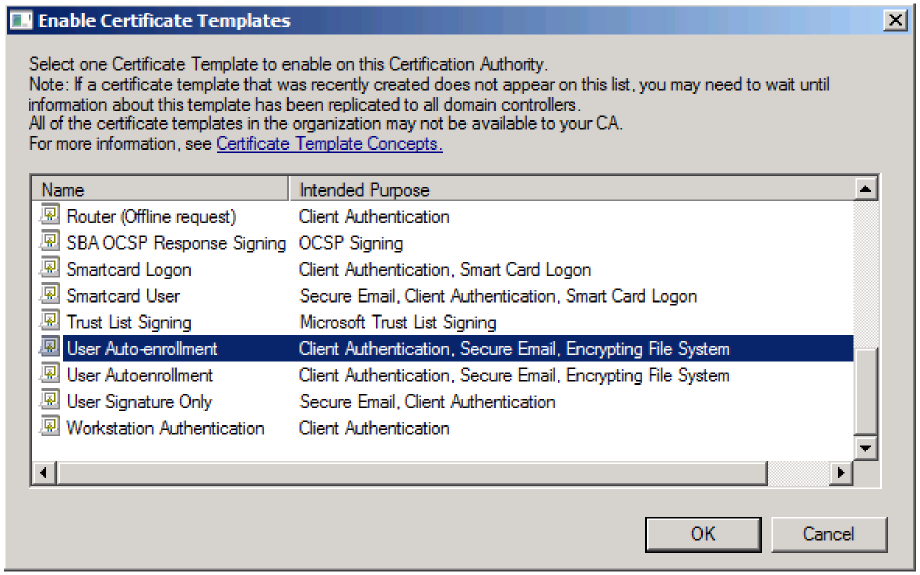
Step 11: In the Certificate Authority console, right-click **Certificate Templates**, and then choose **New > Certificate Template to Issue**.



Name	Intended Purpose
Computer (2003 Template)	Server Authentication, Client Authentication
CEP Encryption	Certificate Request Agent
Exchange Enrollment Agent (Offline req...	Certificate Request Agent
IPSec (Offline request)	IP security IKE intermediate
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authenticatio...
[illegible]	File Recovery
[illegible]	Encrypting File System
Domain Controller	Client Authentication, Server Authentication
Web Server	Server Authentication
Computer	Client Authentication, Server Authentication
User	Encrypting File System, Secure Email, Clien...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting File...

Enable additional Certificate Templates on this Certification Authority

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



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

Name	Intended Purpose
Router (Offline request)	Client Authentication
SBA OCSP Response Signing	OCSP Signing
Smartcard Logon	Client Authentication, Smart Card Logon
Smartcard User	Secure Email, Client Authentication, Smart Card Logon
Trust List Signing	Microsoft Trust List Signing
User Auto-enrollment	Client Authentication, Secure Email, Encrypting File System
User Autoenrollment	Client Authentication, Secure Email, Encrypting File System
User Signature Only	Secure Email, Client Authentication
Workstation Authentication	Client Authentication

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.

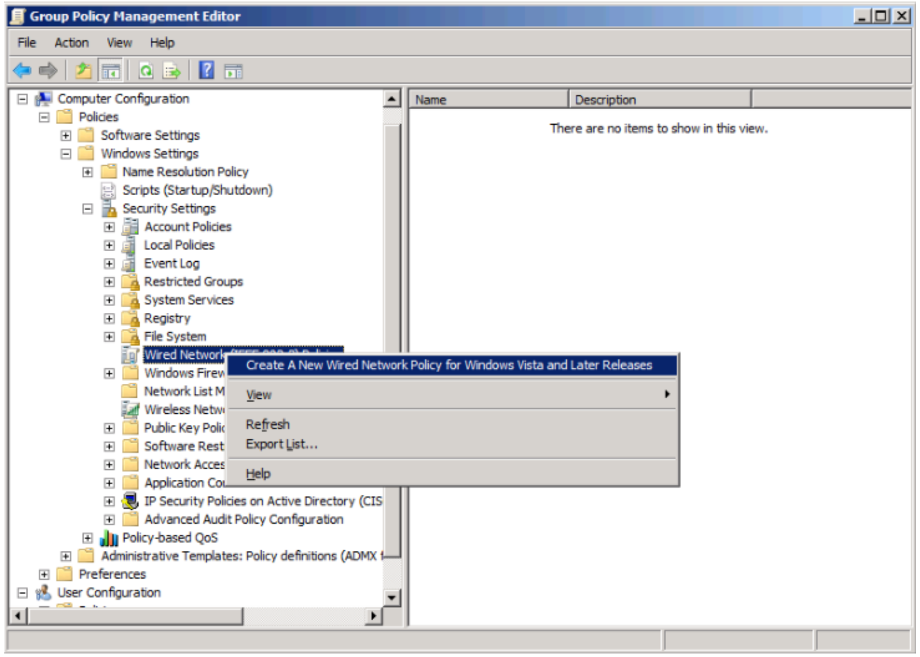
Step 1: On the CA console, navigate to **Start > Administrative Tools > Group Policy Management**.

Step 2: Expand the **Forest**, **Domain**, **local domain**, and **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**.



There are no items to show in this view.

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 drop-down list, choose **Microsoft: Smart Card or other certificate**.

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

Step 10: Click **Properties**.

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

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

Step 13: Click **OK**, 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.

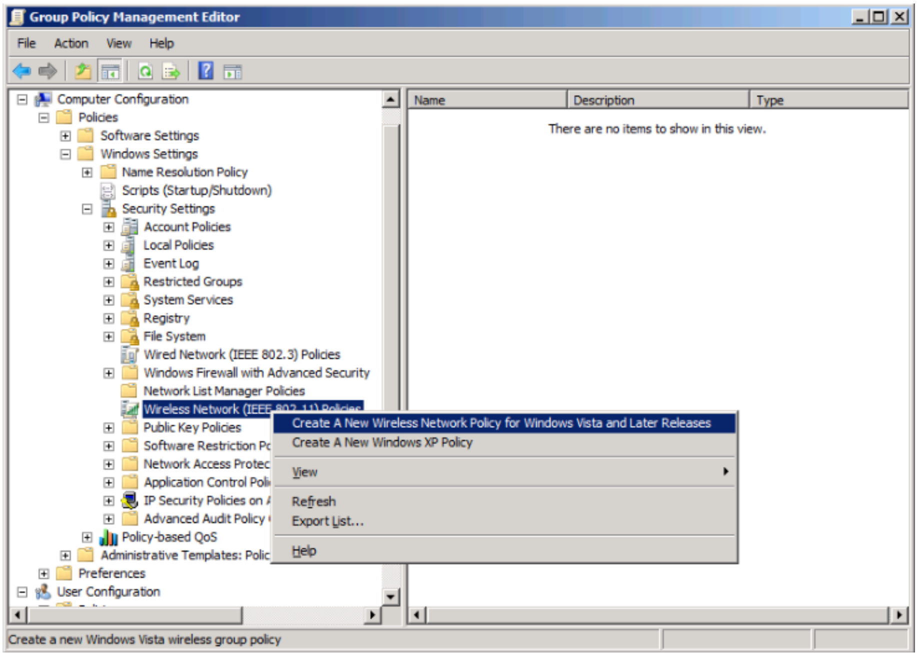
Step 1: On the CA console, navigate to **Start > Administrative Tools > Group Policy Management**.

Step 2: Expand the **Forest**, **Domain**, **local domain**, and **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**.

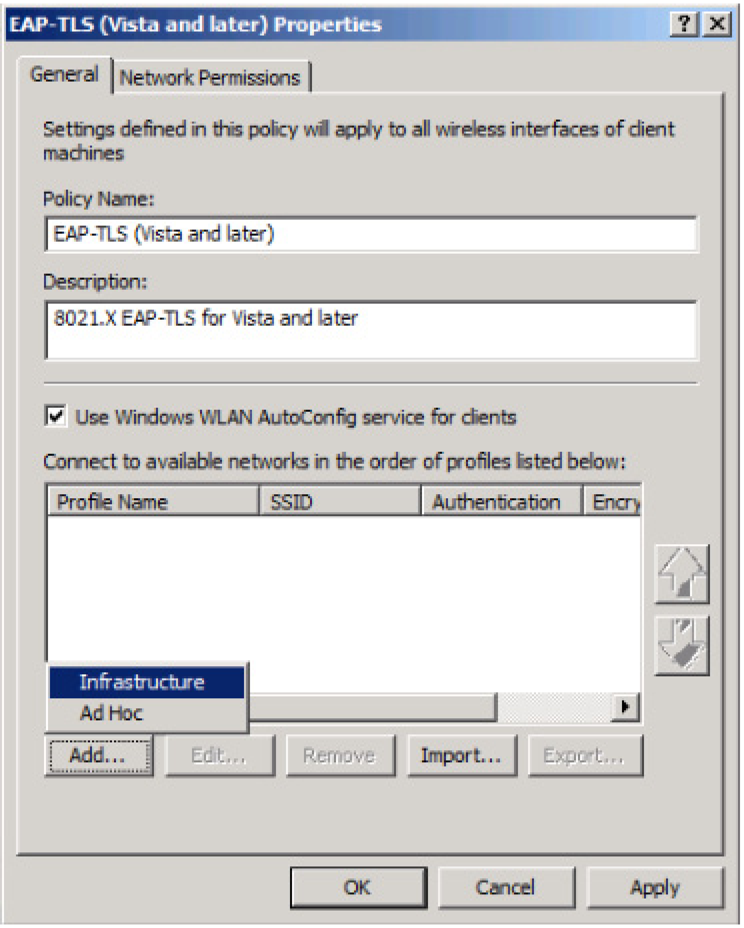


There are no items to show in this view.

Create a new Windows Vista wireless group policy

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**.



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

Policy Name: EAP-TLS (Vista and later)

Description: 8021.X EAP-TLS for Vista and later

☑ Use Windows WLAN AutoConfig service for clients

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

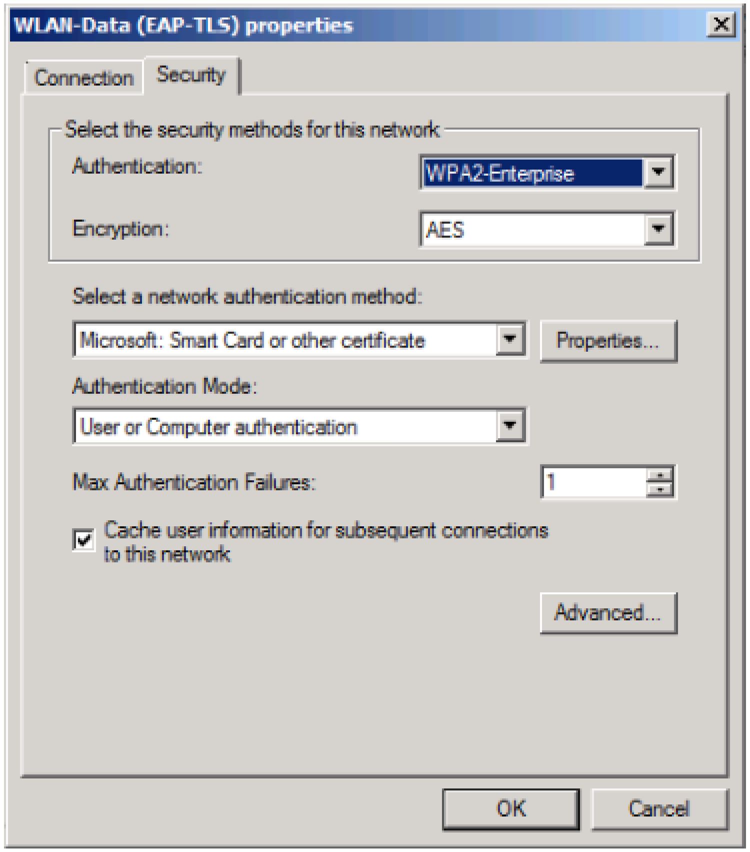
Step 8: Give the profile a name, enter the name of the SSID for the wireless network, and then click **Add**.

Step 9: Click the **Security** tab.

Step 10: In the **Authentication** drop-down list, choose **WPA2-Enterprise,** and then in the Encryption drop-down list, choose **AES**.

Step 11: In the Select a network authentication method drop-down list, choose **Microsoft: Smart Card or other certificate**.

Step 12: In the Authentication Mode drop-down list, choose **User or Computer authentication**.



WLAN-Data (EAP-TLS) properties

Select the security methods for this network

Authentication: WPA2-Enterprise

Encryption: AES

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

Authentication Mode: User or Computer authentication

Max Authentication Failures: 1

☑ Cache user information for subsequent connections to this network

Step 13: Click **Properties**.

Step 14: Make sure the **Use a certificate on this computer** option is selected, and then make sure the **Use simple certificate selection** and **Validate server certificate** check boxes are selected.

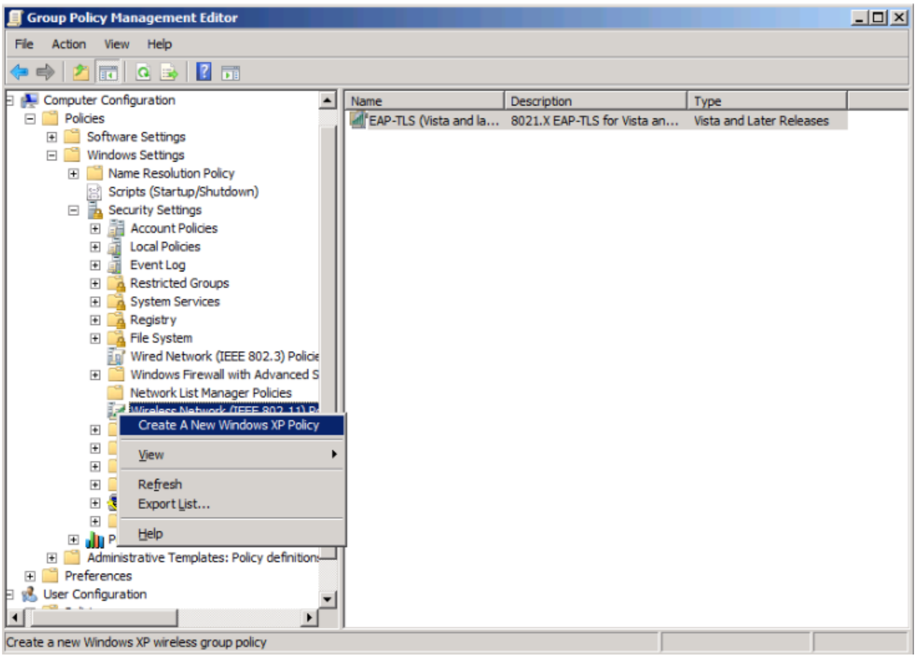
Step 15: In the Trusted Root Certification Authorities list, select the box next to the root certificate for the CA.

Step 16: Click **OK**, and then click **OK** again.

Step 17: Click **Apply,** and then click **OK**.

You also need to create a policy for Windows XP clients.

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



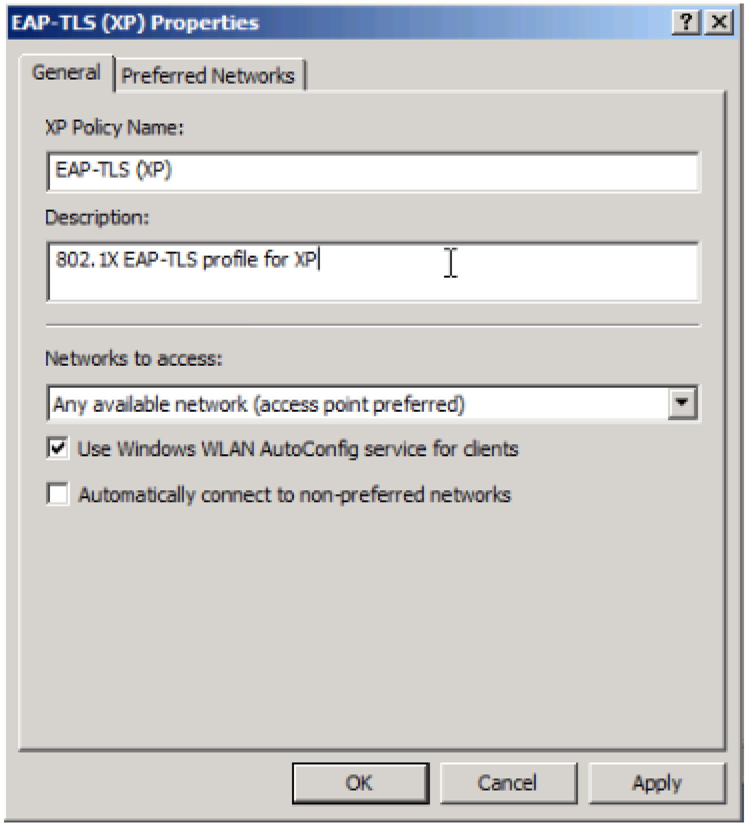
Group Policy Management Editor

Name	Description	Type
EAP-TLS (Vista and la...	8021.X EAP-TLS for Vista an...	Vista and Later Releases

Create a new Windows XP wireless group policy

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

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



XP Policy Name: EAP-TLS (XP)

Description: 802.1X EAP-TLS profile for XP

Networks to access: Any available network (access point preferred)

☑ Use Windows WLAN AutoConfig service for clients

☐ Automatically connect to non-preferred networks

Step 21: Click the **Preferred Networks** tab.

Step 22: Click **Add,** and then select **Infrastructure**.

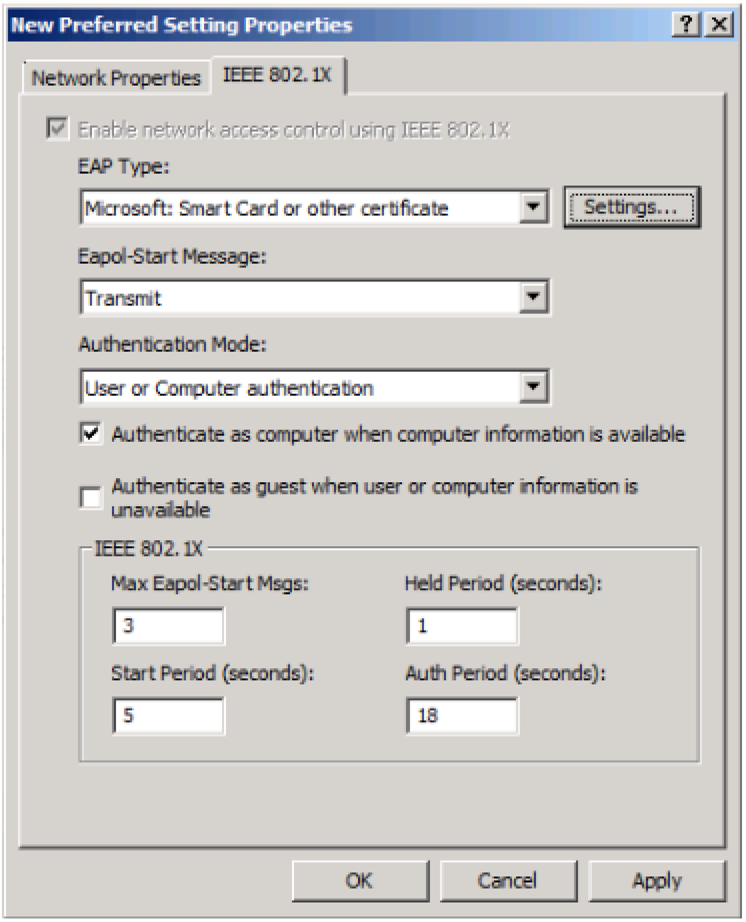
Step 23: Enter the SSID for the network and give a description.

Step 24: Select **WPA2** for Authentication and **AES** for Encryption.

Step 25: Click the **IEEE 802.1X** tab.

Step 26: In the EAP type list, choose **Microsoft: Smart Card or other certificate**.

Step 27: In the Authentication Mode list, choose **User or Computer authentication**.



☑ Enable network access control using IEEE 802.1X

EAP Type: Microsoft: Smart Card or other certificate

Eapol-Start Message: Transmit

Authentication Mode: User or Computer authentication

☑ Authenticate as computer when computer information is available

☐ Authenticate as guest when user or computer information is unavailable

IEEE 802.1X

Max Eapol-Start Msgs: 3

Held Period (seconds): 1

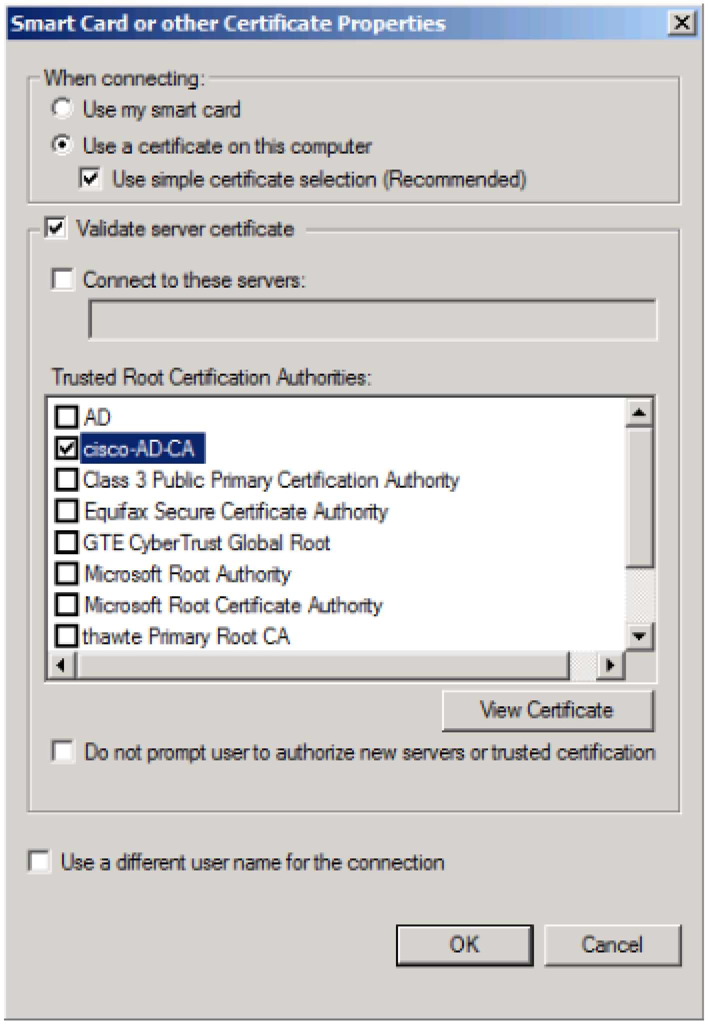
Start Period (seconds): 5

Auth Period (seconds): 18

Step 28: Click **Settings**.

Step 29: Make sure the **Use a certificate on this computer** option is selected, and then make sure the **Use simple certificate selection** and **Validate server certificate** check boxes are selected.

Step 30: In the Trusted Root Certification Authorities list, select the box next to the root certificate for the CA.



Smart Card or other Certificate Properties

When connecting:

○ Use my smart card

● Use a certificate on this computer

☑ Use simple certificate selection (Recommended)

☑ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

□ AD

☑ cisco-AD-CA

□ Class 3 Public Primary Certification Authority

□ Equifax Secure Certificate Authority

□ GTE CyberTrust Global Root

□ Microsoft Root Authority

□ Microsoft Root Certificate Authority

□ thawte Primary Root CA

□ Do not prompt user to authorize new servers or trusted certification

□ Use a different user name for the connection

Step 31: Click **OK**.

Step 32: Click **Apply,** and then click **OK.** The Profile Properties window displays.

Step 33: 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

Deploy AnyConnect on Windows endpoints

1. Install 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 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.

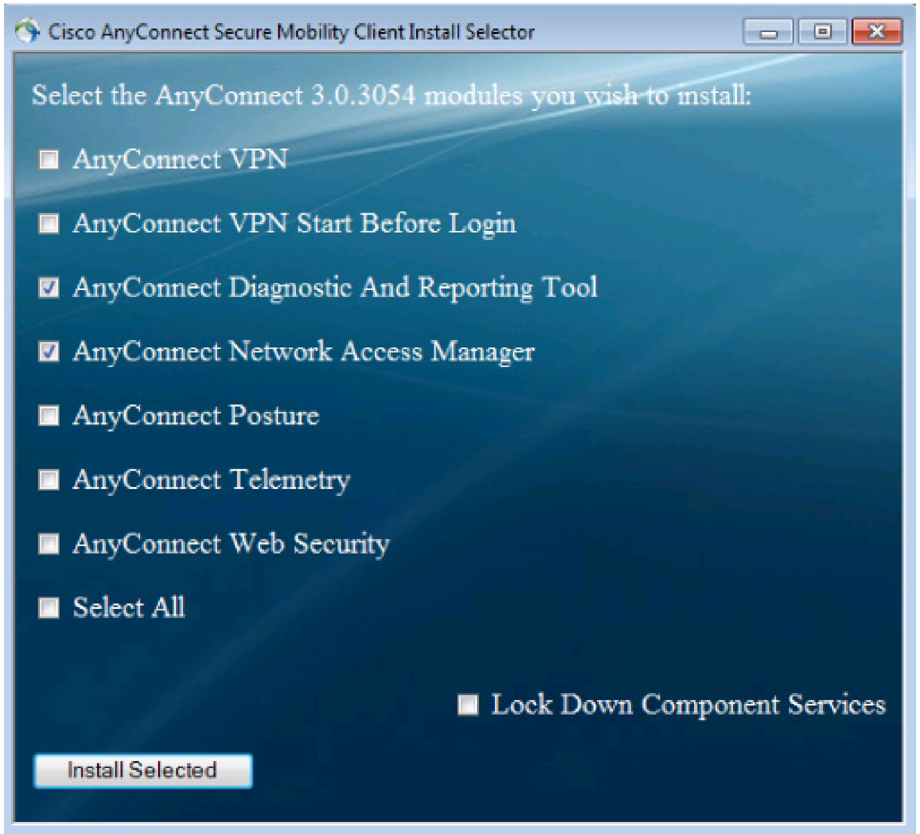
Reader Tip

The latest Cisco AnyConnect Secure Mobility client and Profile Editor can be downloaded from:

http://www.cisco.com/cisco/software/release.html?mdfid=283000185&flowid=17001&softwareid=282364313&release=3.0.5075&relind=AVAILABLE&rellifecycle=&reltype=latest

Step 1: Start the installer for the 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.



Cisco AnyConnect Secure Mobility Client Install Selector

Select the AnyConnect 3.0.3054 modules you wish to install:

☐ AnyConnect VPN

☐ AnyConnect VPN Start Before Login

☑ AnyConnect Diagnostic And Reporting Tool

☑ AnyConnect Network Access Manager

☐ AnyConnect Posture

☐ AnyConnect Telemetry

☐ AnyConnect Web Security

☐ Select All

☐ Lock Down Component Services

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

Step 4: Click **Accept** 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 will be 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.

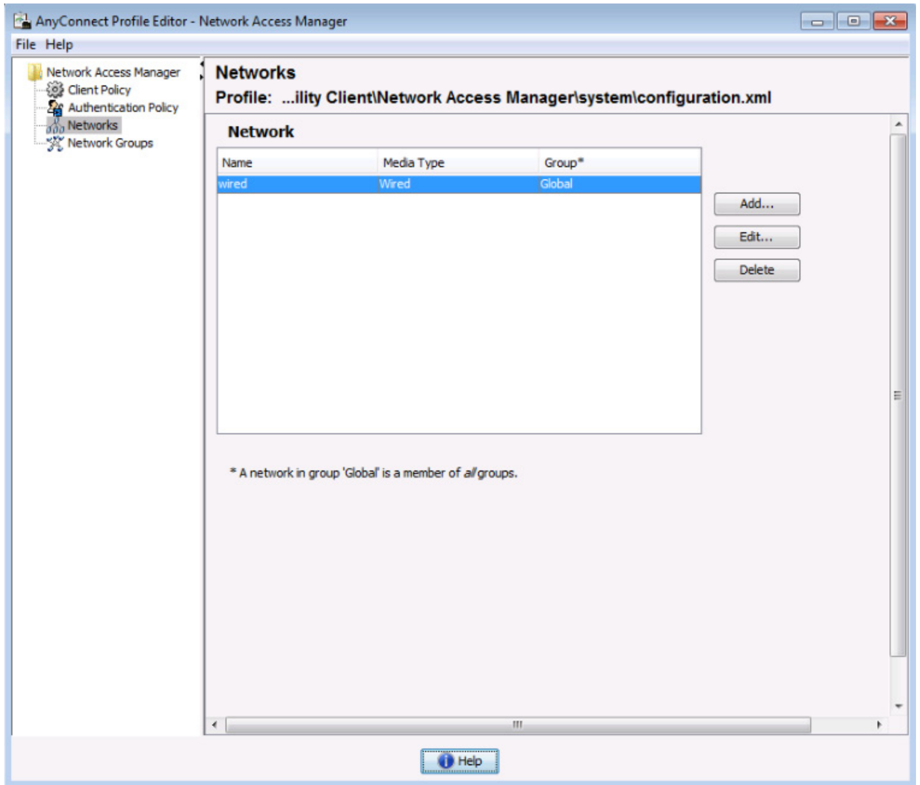
Procedure 3 Create wired profile

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 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**.



Networks

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

Network

Name	Media Type	Group*
wired	Wired	Global

* A network in group 'Global' is a member of *all* groups.

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 Authentication,** and then click **Next**.

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

Step 9: Enter an unprotected identity pattern for machine identity. In this deployment, use host.[domain].

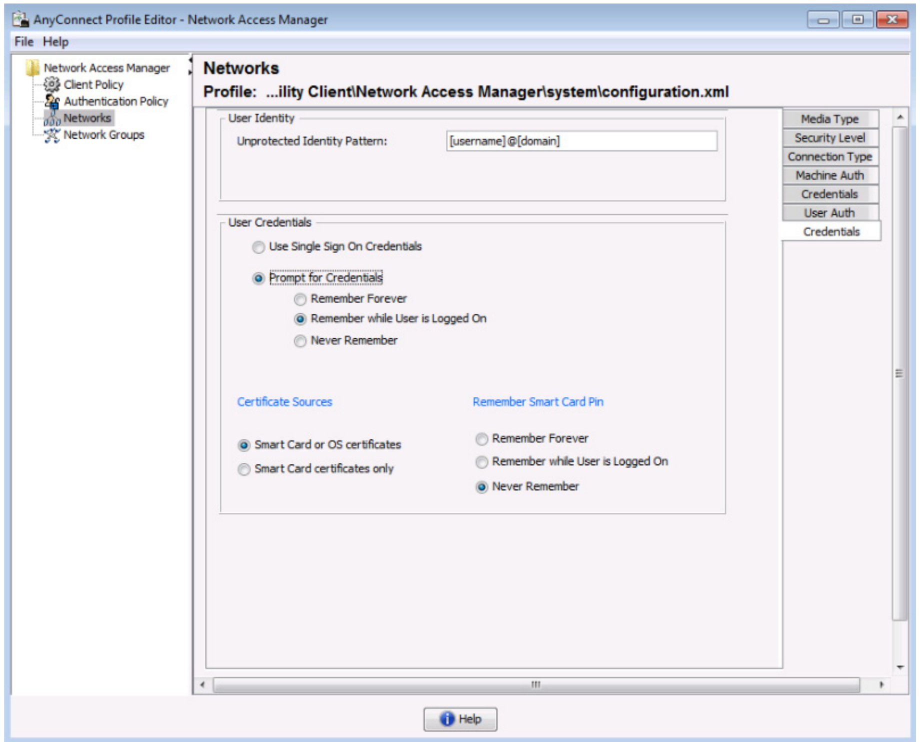
Step 10: Click **Next**.

Step 11: Select **EAP-TLS** as the user authentication method, and then click **Next**.

Step 12: Enter an unprotected identity pattern for user identity. In this deployment, use [username]@[domain].

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

Step 14: Select **Smart Card or OS certificates** as the certificate source, and then click **Done**.



Networks

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

User Identity

Unprotected Identity Pattern: [username]@[domain]

User Credentials

○ Use Single Sign On Credentials

● Prompt for Credentials

○ Remember Forever

● Remember while User is Logged On

○ Never Remember

Certificate Sources

● Smart Card or OS certificates

○ Smart Card certificates only

Remember Smart Card Pin

○ Remember Forever

○ Remember while User is Logged On

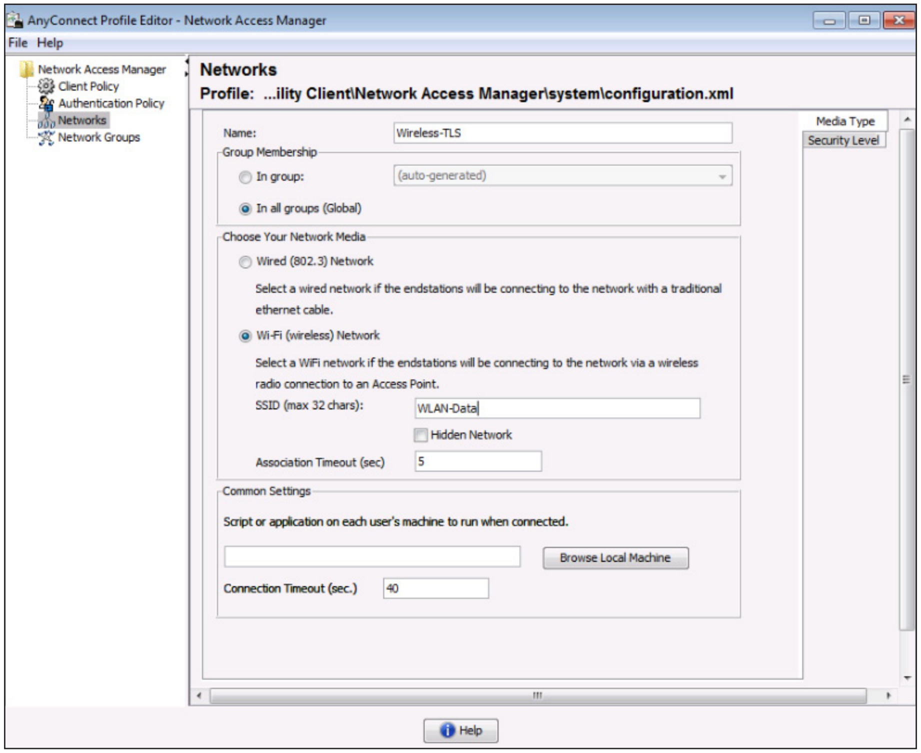
● Never Remember

Procedure 4 Create wireless profile

Step 1: 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 Network Media section, select **Wi-Fi (wireless) Network,** enter the **SSID** of the wireless network, and then click **Next**.



Networks

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

Name: Wireless-TLS

Group Membership

○ In group: (auto-generated)

● In all groups (Global)

Choose Your Network Media

○ Wired (802.3) Network

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

● Wi-Fi (wireless) Network

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

SSID (max 32 chars): WLAN-Data

□ Hidden Network

Association Timeout (sec) 5

Common Settings

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

Connection Timeout (sec.) 40

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

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

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

Step 7: Enter an unprotected identity pattern for machine identity. In this deployment, use host.[domain].

Step 8: Click **Next**.

Step 9: Select **EAP-TLS** as the user authentication method, and then click **Next**.

Step 10: Enter an unprotected identity pattern for user identity. In this deployment, use [username]@[domain].

Step 11: In the User Credentials section, select **Prompt for Credentials,** and then select **Remember while User is Logged On**.

Step 12: Select **Smart Card or OS certificates** as the certificate source, and then click **Done**.

Step 13: From the File menu, choose **Save**. This updates the configuration file.

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.

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

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

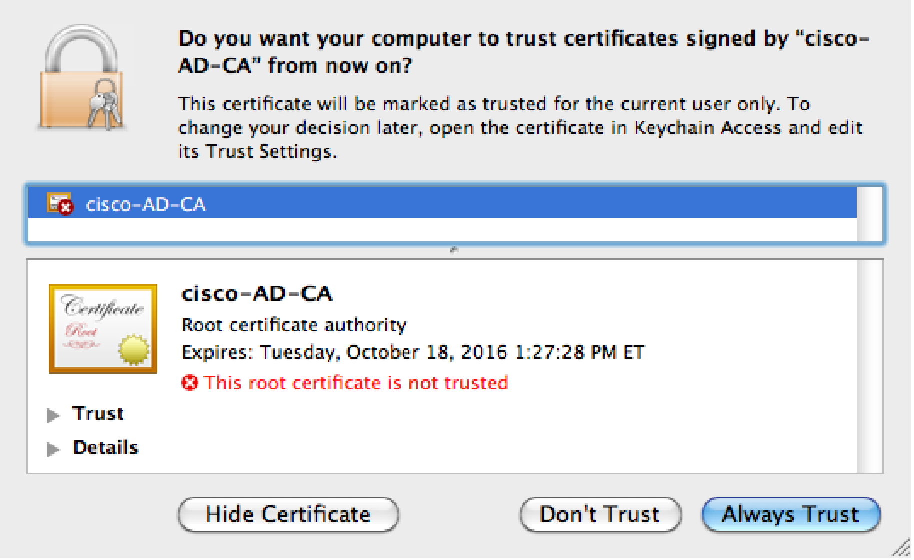
Step 3: Click **Download CA Certificate,** and then save the certificate file.

Step 4: Locate the certificate file, and then double-click it. This launches the Keychain Access utility.

Step 5: Click **Always Trust**.

Tech Tip

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



Do you want your computer to trust certificates signed by “cisco-AD-CA” from now on?

This certificate will be marked as trusted for the current user only. To change your decision later, open the certificate in Keychain Access and edit its Trust Settings.

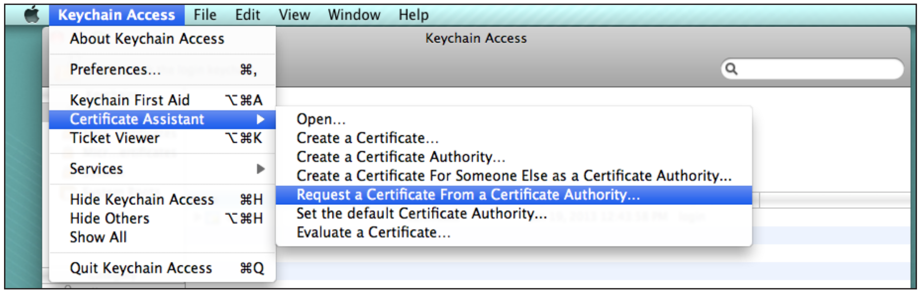
cisco-AD-CA

cisco-AD-CA
Root certificate authority
Expires: Tuesday, October 18, 2016 1:27:28 PM ET
This root certificate is not trusted

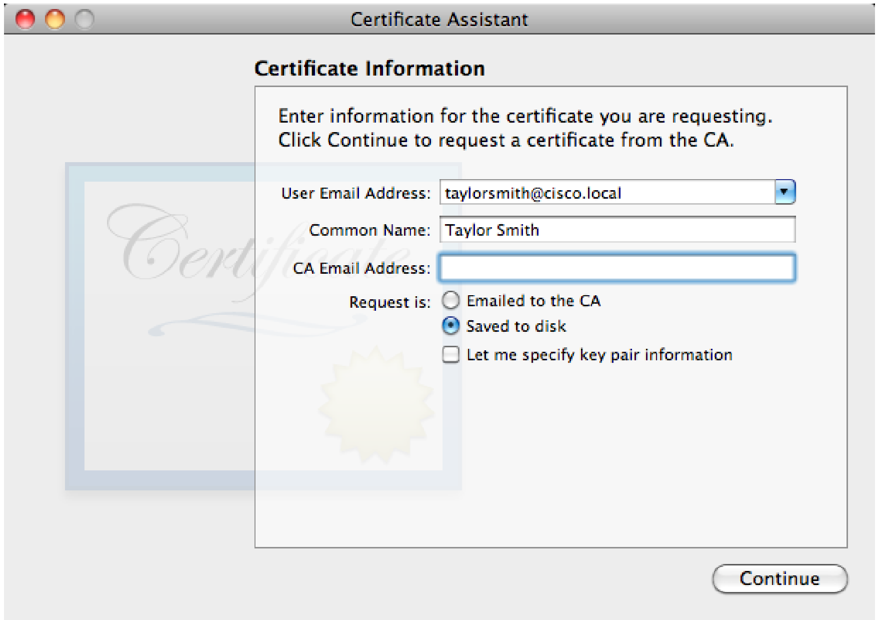
Procedure 2 Request user certificate

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 your email address and common name (typically the user’s first and last names), select **Saved to Disk**, and then click **Continue**.



Certificate Assistant

Certificate Information

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

User Email Address: taylorsmith@cisco.local
Common Name: Taylor Smith
CA Email Address:
Request is: ○ Emailed to the CA
● Saved to disk
□ Let me specify key pair information

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

Step 4: Click **Done**.

Step 5: On the Mac, browse to http://ca.cisco.local/certsrv. When you authenticate to the CA, be sure to authenticate 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.

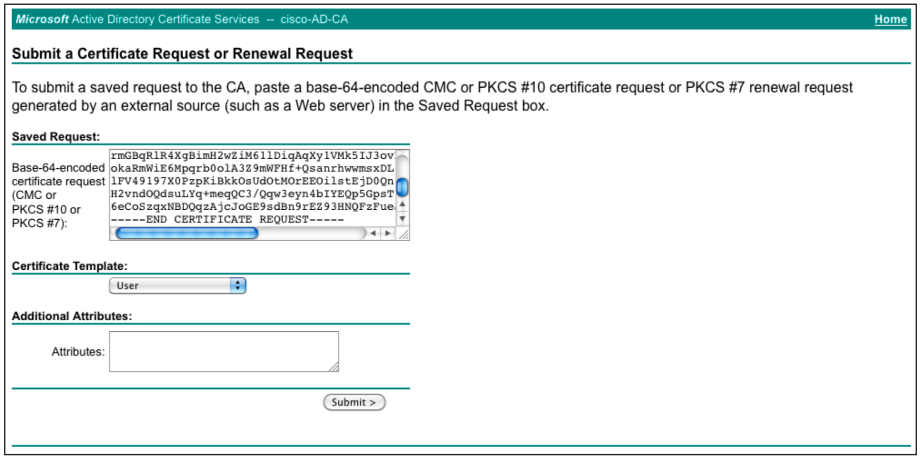
Step 6: Click **Request a certificate**.

Step 7: Click **advanced certificate request**.

Step 8: Open the certificate request file saved in Step 3 in a text editor, such as TextEdit, select all the text, and then copy it to the clipboard.

Step 9: Paste the contents into the text box in the Saved Request section of the certificate request that is open in the browser.

Step 10: In the Certificate Template drop-down list, choose **User,** and then click **Submit**.



Microsoft Active Directory Certificate Services -- cisco-AD-CA

Home

Submit a Certificate Request or Renewal Request

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

Saved Request:

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

```
rmGBqRlR4XgBimH2wZiM61lDiqAqXy1VMk5IJ3ov
okaRmWiE6Mpqrb0olA3Z9mWFHf+QsanrhwwmsxDL
lFV49197X0PzpKiBkkOsUdOtMOrEEOilstEjD0Qn
H2vndOQdsuLYq+meqQC3/Qqw3eyn4bIYEQp5GpsT
6eCoSzqxNBDQqzAjcJoGE9sdBn9rEZ93HNQFzFue
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

User

Additional Attributes:

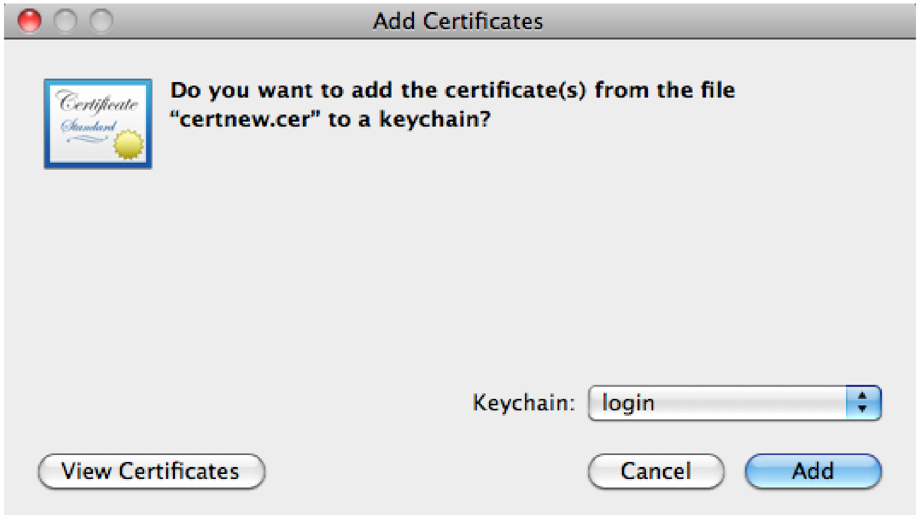
Attributes:

Submit >

Step 11: Select **DER encoded,** and then click **Download certificate**. This saves the certificate.

Step 12: Locate the saved certificate in Finder, and then double-click it to import it into the Keychain Access utility.

Step 13: In the Keychain drop-down list, choose **login**, and then click **Add**.



Add Certificates

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

Keychain: login

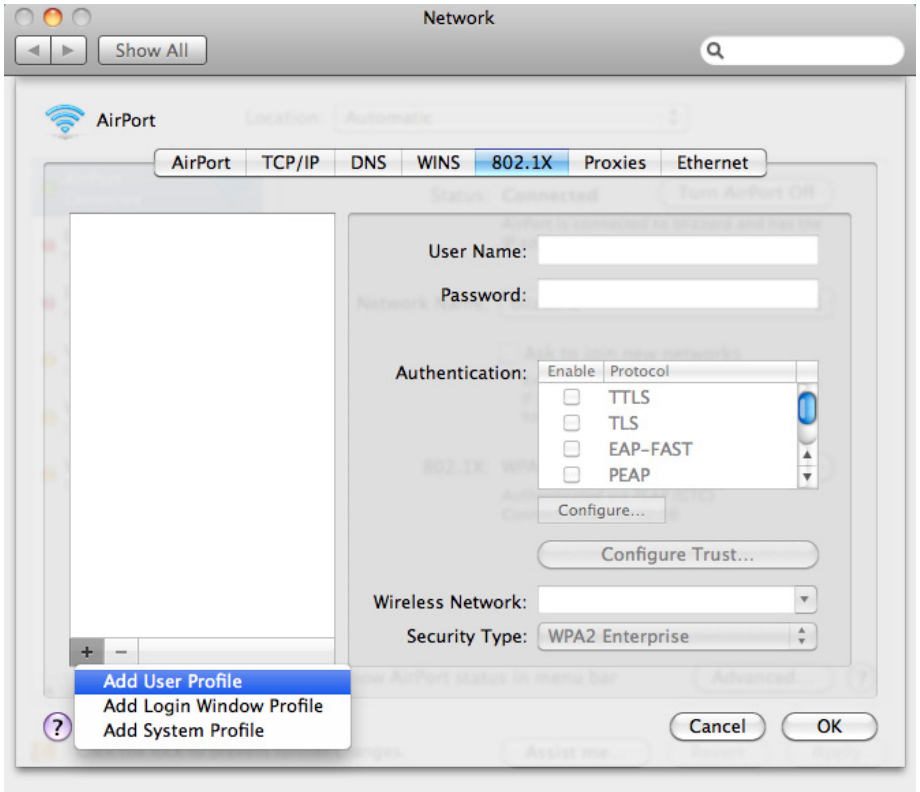
Procedure 3 Configure Mac OS X supplicant

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 select **Add User Profile**.



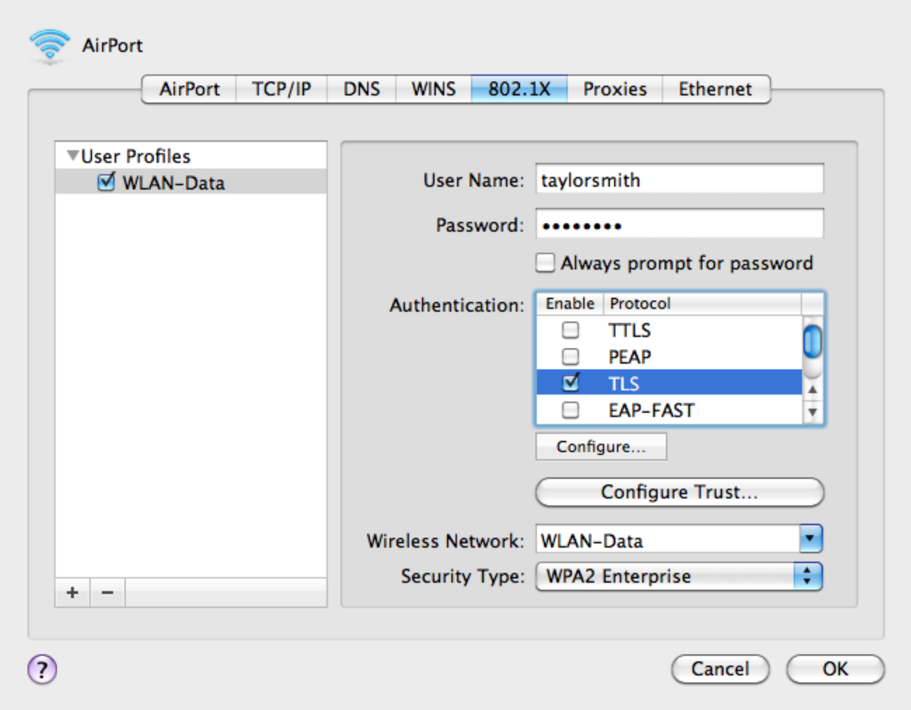
Security Type: WPA2 Enterprise

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: For wireless connections, choose the wireless network from the list, and then choose **WPA2 Enterprise** for the Security Type.



☑ WLAN-Data

User Name: taylorsmith

Password: ••••••••

□ Always prompt for password

Authentication:

Enable	Protocol
□	TTLS
□	PEAP
☑	TLS
□	EAP-FAST

Wireless Network: WLAN-Data

Security Type: WPA2 Enterprise

Step 9: Click **OK**, 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).

Process

Monitoring

1. 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

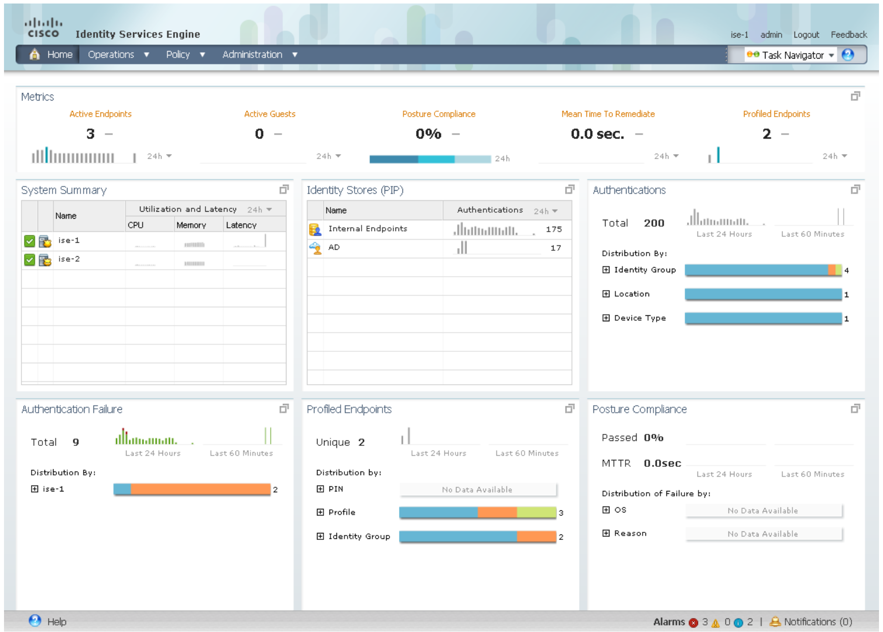
The configuration of the network infrastructure is complete. Now it's time to answer the what/when/where/who questions regarding network access by using the reporting functionality of Cisco ISE to gain a better understanding of current activity on the network .

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 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**. Each section can be expanded by clicking the upper-right corner.



Procedure 2 Configure identity groups

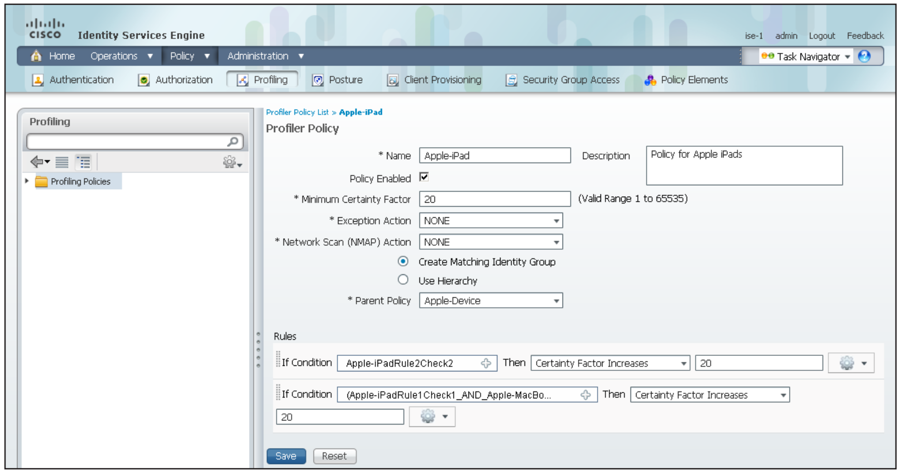
Cisco ISE has more in-depth reporting options to give more details on the devices connecting to the network. To help identify the endpoints, you can use identity groups to classify profiled endpoints and to generate reports.

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**.



Profiler Policy List > Apple-iPad

Profiler Policy

* Name: Apple-iPad
Description: Policy for Apple iPads
Policy Enabled ☑
* Minimum Certainty Factor: 20 (Valid Range 1 to 65535)
* Exception Action: NONE
* Network Scan (NMAP) Action: NONE
● Create Matching Identity Group
○ Use Hierarchy
* Parent Policy: Apple-Device

Rules

If Condition: Apple-iPadRule2Check2 Then: Certainty Factor Increases 20
If Condition: (Apple-iPadRule1Check1_AND_Apple-MacBo... Then: Certainty Factor Increases 20

You can repeat these steps for other endpoint types as needed. You can also investigate the rules used to profile the endpoint to understand the process. In the case of the Apple iPad, Cisco ISE uses two rules. One is based on DHCP information, and the other is based on HTTP.

Procedure 3 Add a custom profile

Although there are many pre-defined profiles, you may find that a device you want to profile doesn't have an existing profile. You can create a new one using unique characteristics of the device. Review some of the existing profiles to get an idea of the options and methods available to you for device profiling.

The example below creates a profile for the Cisco Cius using information obtained from the device's DHCP request.

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

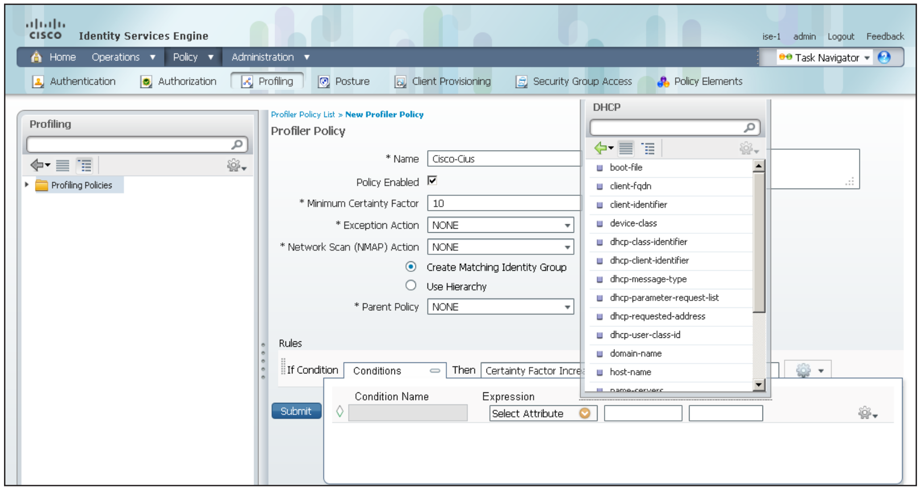
Step 2: Mouse over **Policy**, and then, from the drop-down menu, and choose **Profiling**.

Step 3: Click **Create**.

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 drop-down list, next to DHCP, click the **>** symbol, and then select **dhcp-class-identifier**.



Profiler Policy List > New Profiler Policy

Profiler Policy

* Name: Cisco-Cius
Policy Enabled ☑
* Minimum Certainty Factor: 10
* Exception Action: NONE
* Network Scan (NMAP) Action: NONE
● Create Matching Identity Group
○ Use Hierarchy
* Parent Policy: NONE

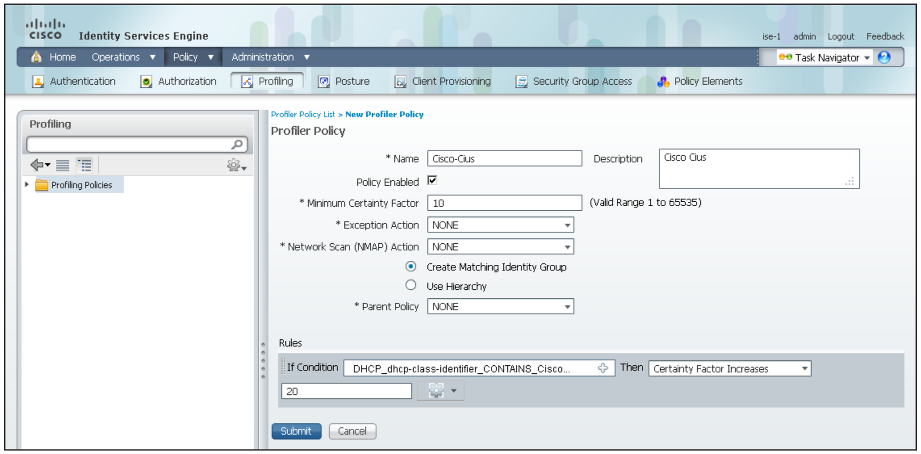
Rules

If Condition: Conditions Then: Certainty Factor Increa

Condition Name | Expression: Select Attribute

Step 7: In the second drop-down 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**.


Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Profiling
Profiling Policies
Submit
Cancel

Profiler Policy List > New Profiler Policy

Profiler Policy

* Name: Cisco-Cius
Description: Cisco Cius
Policy Enabled: ☑
* Minimum Certainty Factor: 10 (Valid Range 1 to 65535)
* Exception Action: NONE
* Network Scan (NMAP) Action: NONE
● Create Matching Identity Group
○ Use Hierarchy
* Parent Policy: NONE

Rules

If Condition DHCP_dhcp-class-identifier_CONTAINS_Cisco... Then Certainty Factor Increases
20

Procedure 4 Examining the authentication log

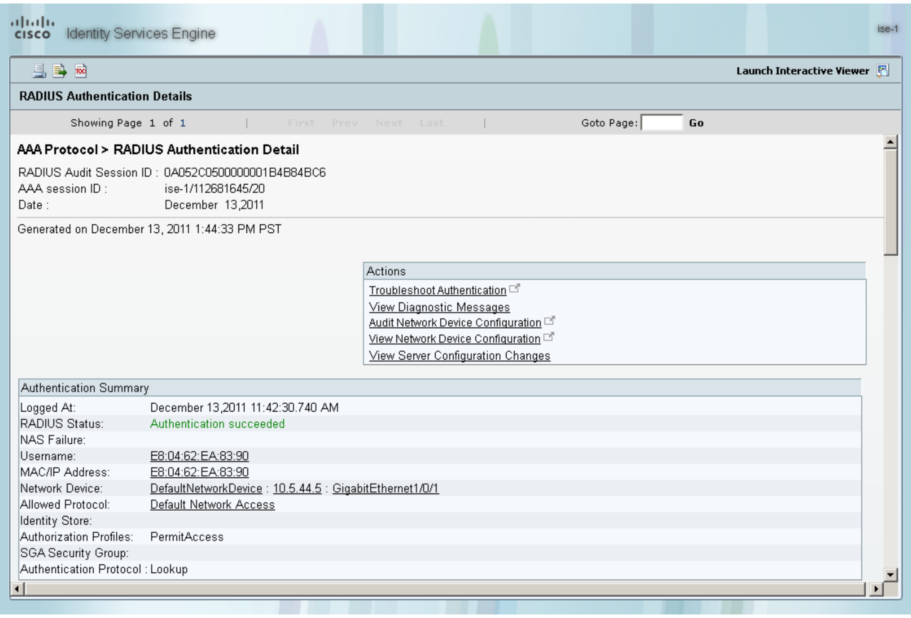
Step 1: On the menu bar, mouse over **Monitor**, and then choose **Authentications**. The authentication log displays. The default option is to display the last 20 records from the last 24 hours.

For devices that authenticated via MAB, the MAC address of the client is listed as the user name and the endpoint. For device 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.



RADIUS Authentication Details

AAA Protocol > RADIUS Authentication Detail

RADIUS Audit Session ID : 0A052C0500000001B4B84BC6
AAA session ID : ise-1/112681645/20
Date : December 13,2011

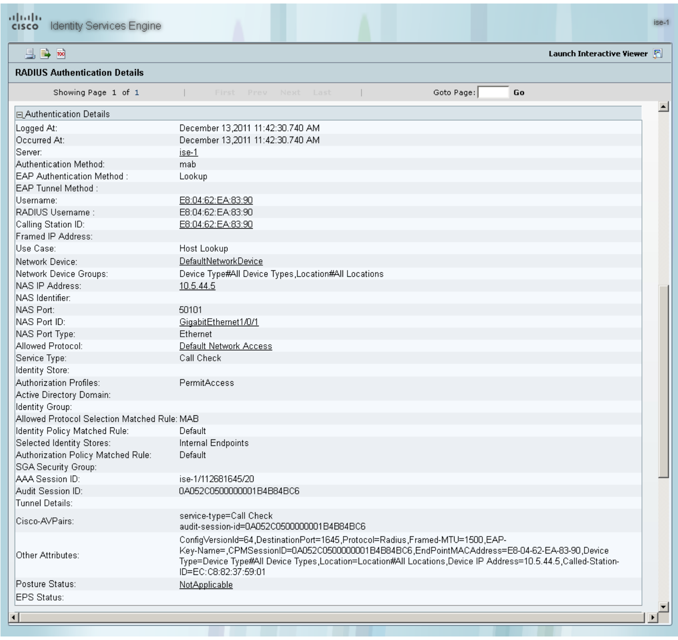
Generated on December 13, 2011 1:44:33 PM PST

Actions
Troubleshoot Authentication
View Diagnostic Messages
Audit Network Device Configuration
View Network Device Configuration
View Server Configuration Changes

Authentication Summary

Logged At:	December 13,2011 11:42:30.740 AM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	E8:04:62:EA:83:90
MAC/IP Address:	E8:04:62:EA:83:90
Network Device:	DefaultNetworkDevice : 10.5.44.5 : GigabitEthernet1/0/1
Allowed Protocol:	Default Network Access
Identity Store:	
Authorization Profiles:	PermitAccess
SGA Security Group:	
Authentication Protocol :	Lookup

You can find additional details, such as the Identity Group and Identity Policy, in the Authentication Details section.



RADIUS Authentication Details

Showing Page 1 of 1 | First Prev Next Last | Goto Page: Go

Authentication Details

Logged At:	December 13,2011 11:42:30.740 AM
Occurred At:	December 13,2011 11:42:30.740 AM
Server:	ise-1
Authentication Method:	mab
EAP Authentication Method :	Lookup
EAP Tunnel Method :	
Username:	E8:04:62:EA:83:90
RADIUS Username :	E8:04:62:EA:83:90
Calling Station ID:	E8:04:62:EA:83:90
Framed IP Address:	
Use Case:	Host Lookup
Network Device:	DefaultNetworkDevice
Network Device Groups:	Device Type#All Device Types,Location#All Locations
NAS IP Address:	10.5.44.5
NAS Identifier:	
NAS Port:	50101
NAS Port ID:	GigabitEthernet1/0/1
NAS Port Type:	Ethernet
Allowed Protocol:	Default Network Access
Service Type:	Call Check
Identity Store:	
Authorization Profiles:	PermitAccess
Active Directory Domain:	
Identity Group:	
Allowed Protocol Selection Matched Rule:	MAB
Identity Policy Matched Rule:	Default
Selected Identity Stores:	Internal Endpoints
Authorization Policy Matched Rule:	Default
SGA Security Group:	
AAA Session ID:	ise-1/112681645/20
Audit Session ID:	0A052C0500000001B4B84BC6
Tunnel Details:	

Cisco-AVPairs:	service-type=Call Check
	audit-session-id=0A052C0500000001B4B84BC6

Other Attributes:	ConfigVersionId=64,DestinationPort=1645,Protocol=Radius,Framed-MTU=1500,EAP-Key-Name=,CPMSessionID=0A052C0500000001B4B84BC6,EndPointMACAddress=E8-04-62-EA-83-90,Device Type=Device Type#All Device Types,Location=Location#All Locations,Device IP Address=10.5.44.5,Called-Station-ID=EC:C8:82:37:59:01
Posture Status:	NotApplicable
EPS Status:	

Similar data can be found for endpoints that have authenticated with RADIUS. The user name is displayed in these records as well the EAP method used.

Procedure 5 Create custom authentication reports

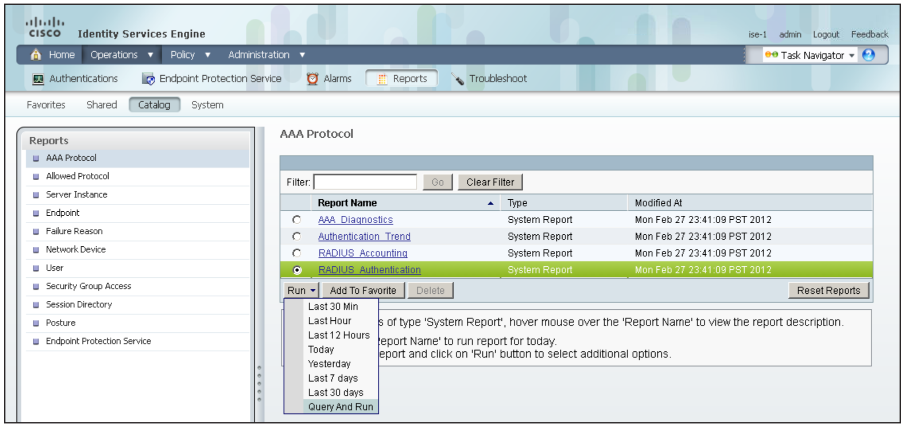
The default authentication log view is limited to displaying only the most recent entries. To get in-depth reporting, you need to create a custom report.

Step 1: On the menu bar, mouse over **Monitor**, 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. For time ranges not listed, choose **Query and Run**.



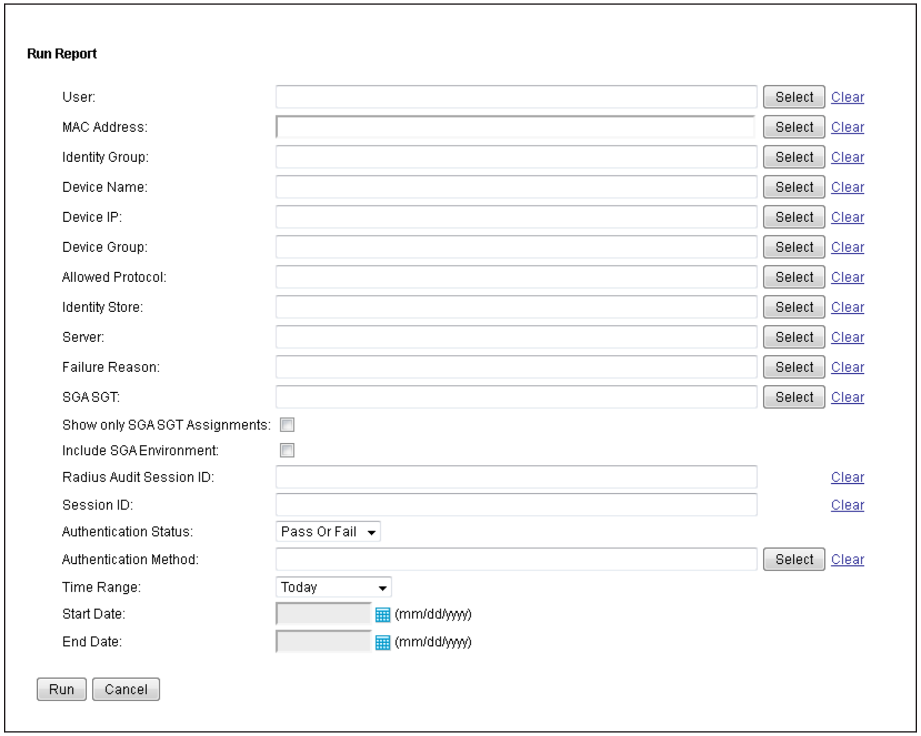
AAA Protocol

	Report Name	Type	Modified At
○	AAA_Diagnostics	System Report	Mon Feb 27 23:41:09 PST 2012
○	Authentication_Trend	System Report	Mon Feb 27 23:41:09 PST 2012
○	RADIUS_Accounting	System Report	Mon Feb 27 23:41:09 PST 2012
●	RADIUS_Authentication	System Report	Mon Feb 27 23:41:09 PST 2012

s of type 'System Report', hover mouse over the 'Report Name' to view the report description.
eport Name' to run report for today.
eport and click on 'Run' button to select additional options.

Step 5: If you 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



Run Report

User:		Select	Clear
MAC Address:		Select	Clear
Identity Group:		Select	Clear
Device Name:		Select	Clear
Device IP:		Select	Clear
Device Group:		Select	Clear
Allowed Protocol:		Select	Clear
Identity Store:		Select	Clear
Server:		Select	Clear
Failure Reason:		Select	Clear
SGA SGT:		Select	Clear
Show only SGA SGT Assignments:	□		
Include SGA Environment:	□		
Radius Audit Session ID:			Clear
Session ID:			Clear
Authentication Status:	Pass Or Fail		
Authentication Method:		Select	Clear
Time Range:	Today		
Start Date:	(mm/dd/yyyy)		
End Date:	(mm/dd/yyyy)		

Procedure 6 Identify endpoints

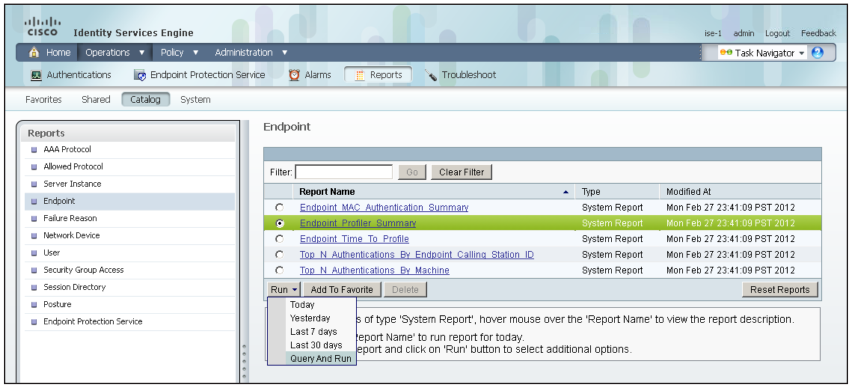
Using information gleaned from the RADIUS and DHCP requests, Cisco ISE can identify what types of devices are connecting to the network. This can assist in determining network security policy based on the type of device that is in use.

Step 1: On the menu bar, mouse over **Monitor**, 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.



Endpoint

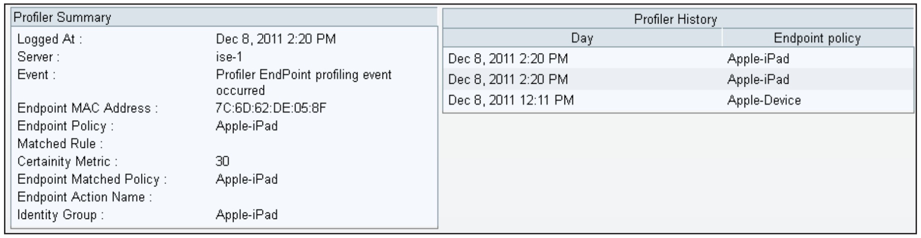
	Report Name	Type	Modified At
○	Endpoint_MAC_Authentication_Summary	System Report	Mon Feb 27 23:41:09 PST 2012
●	Endpoint_Profiler_Summary	System Report	Mon Feb 27 23:41:09 PST 2012
○	Endpoint_Time_To_Profile	System Report	Mon Feb 27 23:41:09 PST 2012
○	Top_N_Authentications_By_Endpoint_Calling_Station_ID	System Report	Mon Feb 27 23:41:09 PST 2012
○	Top_N_Authentications_By_Machine	System Report	Mon Feb 27 23:41:09 PST 2012

s of type 'System Report', hover mouse over the 'Report Name' to view the report description.
eport Name' to run report for today.
eport and click on 'Run' button to select additional options.

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

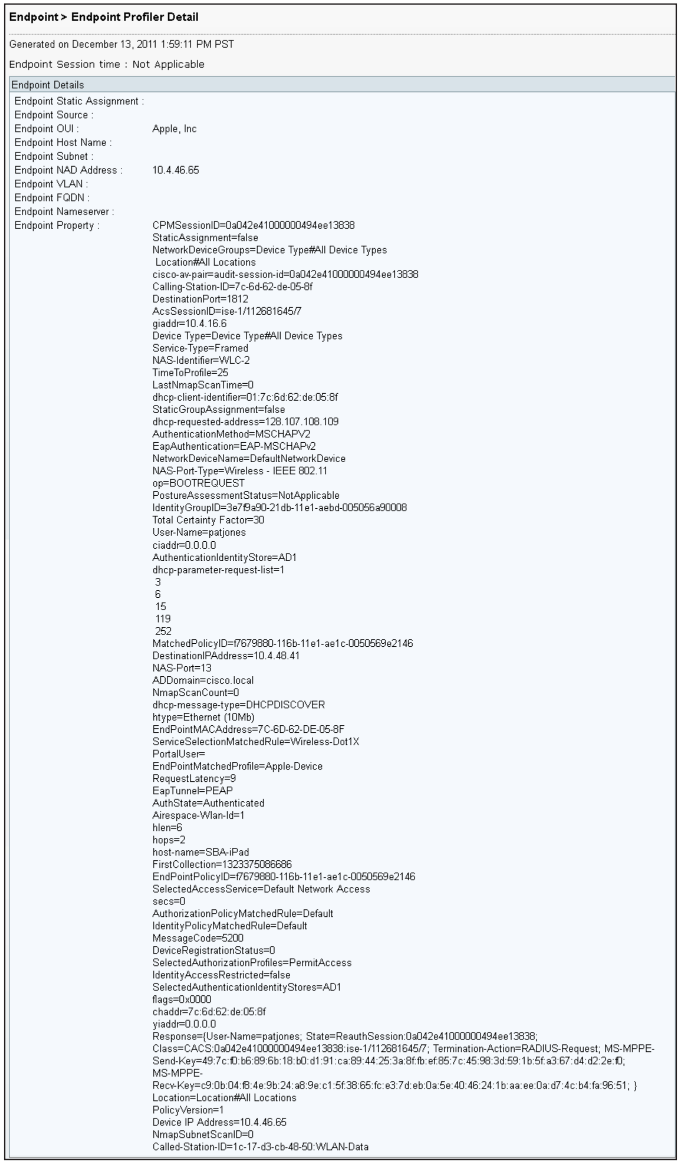


Profiler Summary	
Logged At :	Dec 8, 2011 2:20 PM
Server :	ise-1
Event :	Profiler EndPoint profiling event occurred
Endpoint MAC Address :	7C:6D:62:DE:05:8F
Endpoint Policy :	Apple-iPad
Matched Rule :	
Certainity Metric :	30
Endpoint Matched Policy :	Apple-iPad
Endpoint Action Name :	
Identity Group :	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:8f:fb:ef:85:7c:45:98:3d:59:1b:5f:a3:67:d4:d2:2e:f0;
                            MS-MPPE-
                            Recv-Key=c9:0b:04:f8:4e: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

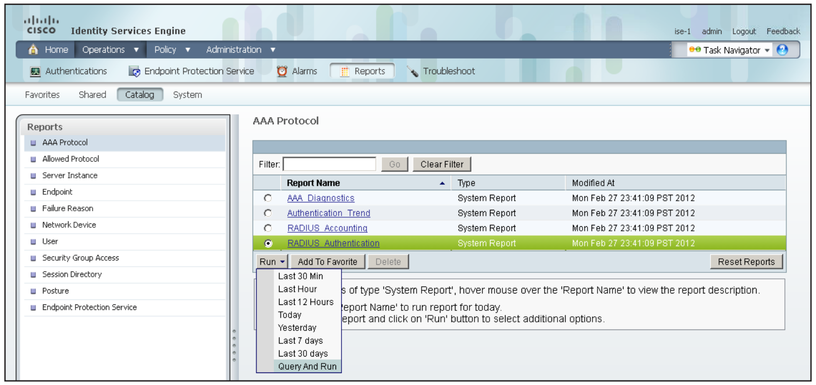
You can create reports to identify specific devices based on the identity groups configured previously. This example uses the group created to identify Apple iPads.

Step 1: On the menu bar, mouse over **Monitor**, 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 choose **Query and Run**.



AAA Protocol

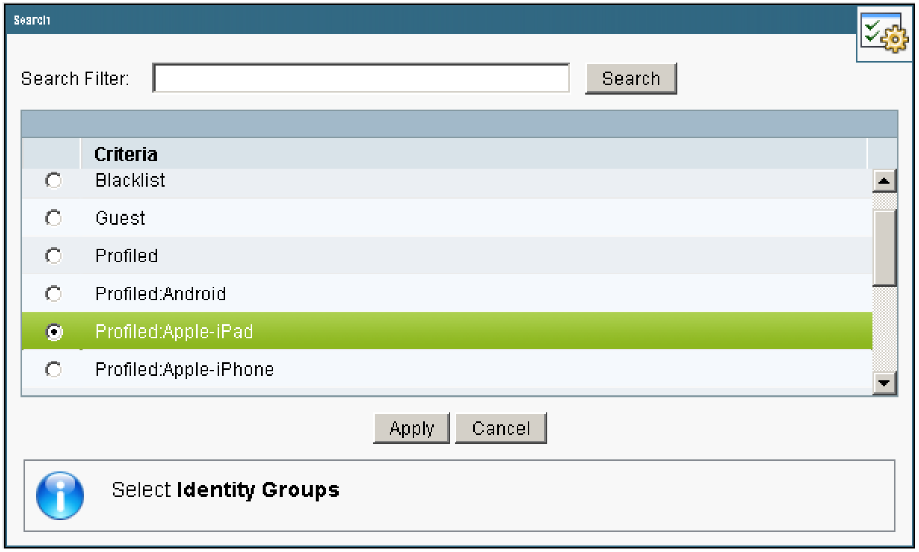
	Report Name	Type	Modified At
○	AAA_Diagnostics	System Report	Mon Feb 27 23:41:09 PST 2012
○	Authentication_Trend	System Report	Mon Feb 27 23:41:09 PST 2012
○	RADIUS_Accounting	System Report	Mon Feb 27 23:41:09 PST 2012
●	RADIUS_Authentication	System Report	Mon Feb 27 23:41:09 PST 2012

s of type 'System Report', hover mouse over the 'Report Name' to view the report description.
eport Name' to run report for today.
eport and click on 'Run' button to select additional options.

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

Step 6: Leave the search field empty and click **Select** to search all groups.

Step 7: Select the group **Profiled:AppleiPad**, and then click **Apply**.

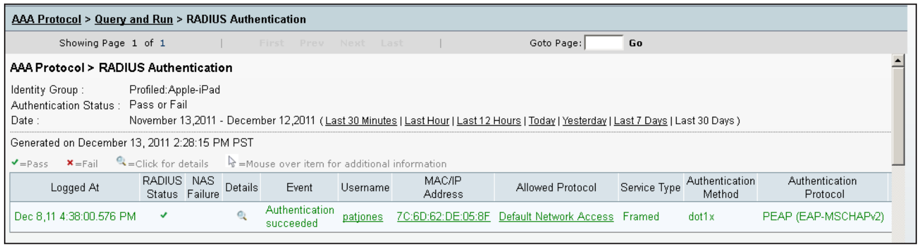


	Criteria
○	Blacklist
○	Guest
○	Profiled
○	Profiled:Android
●	Profiled:Apple-iPad
○	Profiled:Apple-iPhone

Select **Identity Groups**

Step 8: Select a time range for the report, and then click **Run.** The report generates.

Figure 5 - Sample report



AAA Protocol > RADIUS Authentication

Identity Group : Profiled:Apple-iPad
Authentication Status : Pass or Fail
Date : November 13,2011 - December 12,2011 (Last 30 Minutes | Last Hour | Last 12 Hours | Today | Yesterday | Last 7 Days | Last 30 Days)

Generated on December 13, 2011 2:28:15 PM PST

✓=Pass ✗=Fail 🔍=Click for details =Mouse over item for additional information

Logged At	RADIUS Status	NAS Failure	Details	Event	Username	MAC/IP Address	Allowed Protocol	Service Type	Authentication Method	Authentication Protocol
Dec 8,11 4:38:00.576 PM	✓		🔍	Authentication succeeded	patjones	7C:6D:62:DE:05:8F	Default Network Access	Framed	dot1x	PEAP (EAP-MSCHAPv2)

Appendix A: Product List

The following products and software versions have been validated for the Cisco Smart Business Architecture.

Functional Area	Product	Part Numbers	Software Version
Network Management	Cisco Identity Services Engine Virtual Appliance	ISE-VM-K9= L-ISE-BSE-2500= Cisco Identity Services Engine 2500 EndPoint Base License L-ISE-BSE-3500= Cisco Identity Services Engine 3500 EndPoint Base License L-ISE-BSE-5K= Cisco Identity Services Engine 5000 EndPoint Base License L-ISE-BSE-10K= Cisco Identity Services Engine 10000 EndPoint Base License L-ISE-ADV3Y-2500= Cisco ISE 2500 EndPoint 3Year Advanced Subscription License L-ISE-ADV3Y-3500= Cisco ISE 3500 EndPoint 3Year Advanced Subscription License L-ISE-ADV3Y-5K= Cisco ISE 5000 EndPoint 3Year Advanced Subscription License L-ISE-ADV3Y-10K= Cisco ISE 10000 EndPoint 3Year Advanced Subscription License	1.1.0.665

Functional Area	Product	Part Numbers	Software Version
Network Management	Cisco Prime LAN Management Solution	LMS-4.1-100-K9 LMS 4.1, networks of up to 100 devices LMS-4.1-500-K9 LMS 4.1, networks of 100 to 500 devices LMS-4.1-1K-K9 LMS 4.1, networks of 500 to 1000 devices LMS-4.1-2.5K-K9 LMS 4.1, networks of 1000 to 2500 devices	4.1
Access Layer for PC, phones, APs, other devices	Catalyst 2960S Stackable Ethernet 10/100/1000 ports with PoE+ and Stack Module	WS-C2960S-24PD-L Catalyst 2960S 24 GigE PoE+, 2 x 10G SFP+ LAN Base WS-C2960S-48FPD-L Catalyst 2960S 48 GigE PoE +, 2 x 10G SFP+ LAN Base WS-C2960S-24PS-L Catalyst 2960S 24 GigE PoE+, 4 x SFP LAN Base WS-C2960S-48FPS-L Catalyst 2960S 48 GigE PoE+, 4 x SFP LAN Base C2960S-STACK= Catalyst 2960S Flexstack Stack Module	12.2(58)SE1

Functional Area	Product	Part Numbers	Software Version
Access Layer for PC, phones, APs, other devices	Catalyst 3560X Ethernet 10/100/1000 ports with PoE+ and Uplink Module	WS-C3560X-24P-S Catalyst 3750 24 10/100/1000T PoE + and IPB Image WS-C3560X-48PF-S Catalyst 3750 48 10/100/1000T Full PoE + and IPB Image C3KX-NM-1G Catalyst 3750X 1Gig SFP Uplink Module C3KX-NM-10G Catalyst 3750X 10Gig SFP+ Uplink Module	12.2(58)SE1
Access Layer for PC, phones, APs, other devices	Catalyst 3750X Stackable Ethernet 10/100/1000 ports with PoE+ and Uplink Module	WS-C3750X-24P-S Catalyst 3750 24 10/100/1000T PoE + and IPB Image WS-C3750X-48PF-S Catalyst 3750 48 10/100/1000T Full PoE + and IPB Image C3KX-NM-1G Catalyst 3750X 1Gig SFP Uplink Module C3KX-NM-10G Catalyst 3750X 10Gig SFP+ Uplink Module	12.2(58)SE1
Access Layer for PC, phones, APs, other devices	Catalyst 4507R+E Dual Supervisors Dual Power Supplies	WS-C3750X-24P-S Catalyst 3750 24 10/100/1000T PoE + and IPB Image WS-C3750X-48PF-S Catalyst 3750 48 10/100/1000T Full PoE + and IPB Image C3KX-NM-1G Catalyst 3750X 1Gig SFP Uplink Module C3KX-NM-10G Catalyst 3750X 10Gig SFP+ Uplink Module	12.2(54)SG1

Functional Area	Product	Part Numbers	Software Version
VPN (Internet Edge 5K)	ASA 5510 or ASA 5520 or ASA 5540	ASA5510-AIP10-SP-K9 ASA5520-AIP20-K9 ASA5540-AIP40-K9	8.4.1
VPN (Internet Edge 10K)	2x ASA 5520 and 500 SSL seats or 2x ASA 5540 and 1000 SSL seats	ASA5520-SSL500-K9 ASA5540-SSL1000-K9	8.4.1
Wireless LAN	5508 Wireless LAN Controller	AIR-CT5508-100-K9 5508 Wireless LAN Controller with 100 AP license	7.1.91.0

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-0000137-1 3/12