## 

# **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 Wireless LAN 802.1X Authentication Deployment Guide

SMART BUSINESS ARCHITECTURE

August 2012 Series

## Preface

### **Who Should Read This Guide**

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

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

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

### **Release Series**

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

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

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

#### month year Series

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

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

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

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

### **How to Read Commands**

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

configure terminal

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

ntp server 10.10.48.17

Commands with variables that you must define appear as follows:

#### class-map [highest class name]

Commands shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

#### Router# enable

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

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

100 100 100

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

interface Vlan64

ip address 10.5.204.5 255.255.25.0

#### **Comments and Questions**

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

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

August 2012 Series

## Table of Contents

What's In This SBA Guide	1
Cisco SBA Borderless Networks	1
Route to Success	1
About This Guide	1
Introduction	2
Business Overview	2
Technology Overview	2
Deployment Details	4
Enable Authentication	4
Deploying Cisco Identity Services Engine	4
Enabling Visibility to the LAN	11
Enabling Visibility to the Wireless Network	
Deploying Digital Certificates	
Enabling 802.1X Authentication	
Configuring Group Policy Objects	
Deploying Cisco AnyConnect on Windows Endpoints	41
Configuring Mac Workstations for 802.1X Authentication	
Enable Authorization	
Enabling Authorization for Cisco IP Phones	
Enabling Authorization for Wireless Access Points	
Modifying the MAB Authentication Policy	51
Enabling Authorization for Wired Endpoints	51
Enabling Authorization for Wireless Endpoints	
Modify Authorization Policy to be Closed	59
Monitoring Network Access	60

Appendix A: Product List	
Appendix B: Changes	

## What's In This SBA Guide

## **Cisco SBA Borderless Networks**

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

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

Cisco SBA Borderless Networks is a comprehensive network design targeted at organizations with up to 10,000 connected users. The SBA Borderless Network architecture incorporates wired and wireless local area network (LAN) access, wide-area network (WAN) connectivity, WAN application optimization, and Internet edge security infrastructure.

## **Route to Success**

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

## **About This Guide**

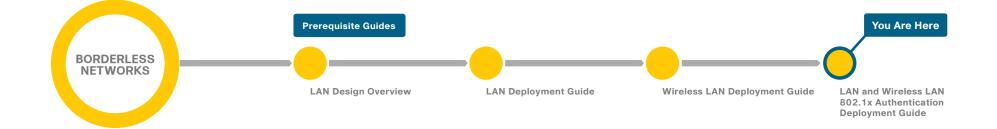
This *deployment guide* contains one or more deployment chapters, which each include the following sections:

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

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

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

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



## Introduction

## **Business Overview**

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

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

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

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

## **Technology Overview**

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

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

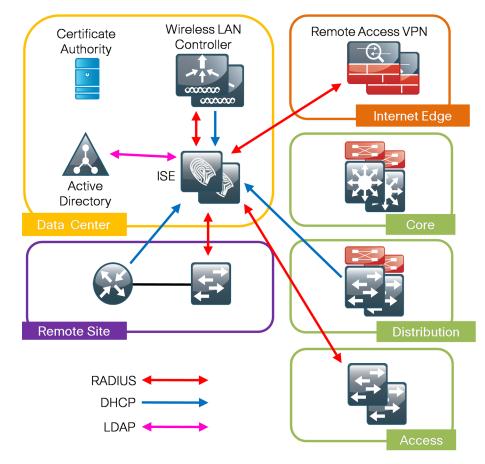
In addition to authentication, this deployment uses Cisco ISE to profile devices in order to determine the specific type of devices that are accessing the network. This is done by examining network traffic for certain criteria, based on certain characteristics. Cisco ISE currently has probes for Dynamic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

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

the remote sites, with Cisco ISE being centralized in the data center. The deployment in use deploys two features within Cisco IOS on the switches in the access layer at both the headquarters sites as well as the remote sites. The first is MAC Authentication Bypass (MAB), which authenticates the device on the switch port by the MAC address. Monitor mode logs the MAC addresses that connect and grant access to any device that connects. The second feature is 802.1X open mode, which allows the switch port to give unrestricted access to the network even though authentication and authorization have not been performed. This enables the deployment of identity without affecting existing connectivity. This phased approach allows you to prepare for moving to another mode in the future. In the organization, these switch configurations will be managed by Cisco Prime LAN Management Solution (LMS) 4.2 and the new TrustSec Work Center. Cisco Prime LMS simplifies the deployment of identity by performing a network-readiness assessment for an identity deployment, providing templates for the various modes-monitor, low-impact, closed-and providing a step-by-step wizard to configure the various components required.

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

Figure 1 - Cisco ISE integration into Cisco SBA



## **Deployment Details**

The deployment described here bases all IP addressing off of the *Cisco SBA—Borderless Networks LAN Deployment Guide*. Any IP addresses used in this guide are examples; you should use addressing that is applicable to your architecture.

Cisco ISE has different personas, or modes, for which it can be configured: administration, policy service, and monitoring. For a standalone configuration where the appliance is all personas, the maximum number of endpoints that can be supported is 2000. To support a greater number of endpoints, you will need to divide the personas across multiple appliances. In this example, there is a primary and secondary policy service and administration node and a primary and secondary monitoring node. This will allow the deployment to scale to 10,000 endpoints. If your deployment does not require support for more than 2000 endpoints, then you can just have a primary and secondary set of engines that support all the personas.

Table 1 - Cisco ISE engine IP addresses and hostnames

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

### **Enable Authentication**

#### Process

Deploying Cisco Identity Services Engine

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

#### **Procedure 1**

Set up initial primary engine

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

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

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

#### Step 3: Enter DNS information.

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

#### Step 4: Configure time.

Enter primary NTP server[time.nist.gov]: ntp.cisco.local
Add/Edit secondary NTP server? Y/N : n
Enter system timezone[UTC]: PST8PDT



#### **Tech Tip**

Time zone abbreviations can be found in the *Cisco Identity* Services Engine CLI Reference Guide, Release 1.1.x:

http://www.cisco.com/en/US/docs/security/ise/1.1/cli\_ref\_guide/ ise\_cli\_app\_a.html#wp1571855 Step 5: Configure an administrator account.

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

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

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

Do not use 'Ctrl-C' from this point on... Virtual machine detected, configuring UMware tools... Installing applications... Installing ise ... Executed with privileges of root The mode has been set to licensed. Application bundle (ise) installed successfully === Initial Setup for Application: ise === Welcome to the ISE initial setup. The purpose of this setup is to provision the internal ISE database. This setup requires you create a database administrator password and also create a database user password.

The primary engine is now installed.

#### **Procedure 2**

Set up the remaining engines

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

#### Procedure 3

**Configure certificate trust list** 

The engines use public key infrastructure (PKI) to secure communications between them. Initially in this deployment, you use local certificates, and you must configure a trust relationship between all of the engines. To do this, you need to import the local certificates from the secondary administration node and the two monitoring nodes into the primary administration node. **Step 1:** In your browser, connect to the secondary engine's GUI at http:// ise-2.cisco.local.

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

Step 3: In the Local Certificates window, select the local certificate by checking the box next to the name of the secondary engine, ise-2.cisco. local, and then click Export.

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

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

**Step 6:** In a browser, access the primary engine's GUI at http://ise-1.cisco. local.

Step 7: In Administration > System, select Certificates.

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

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

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

#### **Procedure 4**

Configure Cisco ISE deployment nodes

You can configure the personas of Cisco ISE—administration, monitoring, and policy service—to run all on a single engine or to be distributed amongst several engines. For this example installation, you will deploy a pair of engines for administration and policy service with one serving as primary and the other secondary and another pair of engines for monitoring with one serving as primary and the other secondary.

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

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



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

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

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 Nodes	
<b>◆</b> • ■ 1	8. ·	Selected D   Total 1   🍄 🙀 🖕
Deployment	Create Node Group Register & Export & Import > Show All	- 8
	Hostname   Node Type Personas	Role(s)
	ise-1 ISE Administration, Monitoring, Polic	cy 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, and then click Submit.

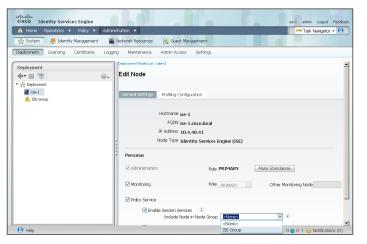
**Step 5:** A pop-up window lets you know the group was created successfully. Click **OK**.

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

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

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

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



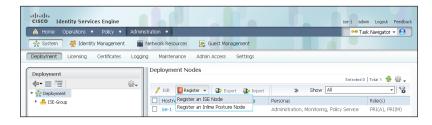
Next, you'll configure which methods are used to profile network endpoints.

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

<b>~</b>	▼ RADIUS		-
		Description RADIUS	

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

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



**Step 13:** Enter the IP address or host name of the primary monitoring Cisco ISE engine from Table 1 (in this example, ise-3.cisco.local) and the credentials for the admin account, and then click **Next**.

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

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

cisco Identity Services Engine		ise-1 admin Logout Feedback
🍐 Home Operations 🔻 Policy 🔻 Administr	ation 🔻	👓 Task Navigator 👻 🕗
👷 System 🛛 👰 Identity Management 🛛 🖀 N	twork Resources 🛛 🛃 Web Portal Management	
Deployment Licensing Certificates Logging	Maintenance Admin Access Settings	
Deployment	eployment Nodes List > Configure Node	
	egister ISE Node - Step 2: Configure Node	
	General Settings	
	Hostname ise-3	
	FQDN ise-3.cisco.local	
	IP Address 10.4.48.43	
	Node Type Identity Services Engine (ISE)	
	Personas	
e	Administration Role SECONDARY	
e e	Monitoring Role PRIMARY    Other Monitoring Node ise-1	
	Policy Service	
	Enable Session Services	
	Include Nade in Nade Group <none> + (1)</none>	
	Enable Profiling Service	
	Submit Cancel	

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

**Step 17:** Clear **Monitoring**, and then click **Save**. The node updates, and a message displays letting you know that the process was successful. Click **OK**. The node restarts.

cisco Identity Services Engine		ise-1 admin Logout Feedback
🋕 Home Operations 🔻 Policy 🔻 Administ	ration 🔻	👓 Task Navigator 👻 🕙
🔆 System 🛛 🖉 Identity Management 🖉 N	letwork Resources 🛛 🛃 Web Portal Management	
Deployment Licensing Certificates Logging	Maintenance Admin Access Settings	
Deployment	bapleyment Nodes Liti ⇒ Ise-1 Edit Node	
	General Settings Profiling Configuration	
	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 SECONDARY Other Monitoring Node	
	Policy Service	
	Enable Session Services (1) Include Node in Node Group ISE-Group (1)	
	Enable Profiling Service	
	Save Reset	

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

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

**Step 20:** Enter the IP address or host name of the secondary administration Cisco ISE from Table 1 (in this example, ise-2.cisco.local) and the credentials for the admin account, and then click **Next**.

Step 21: Select Administration and Policy Service. In the Administration section, in the Role list, choose Secondary, and then in the Policy Service section, in the Node Group list, choose ISE-Group.

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

cisco Identity Services Engine	ise-1 admin Logout Feedback
🛕 Home Operations 🔻 Policy 🔻 Adminis	stration 🔻 😶 Task Navigator 👻 🙆
🔆 System 🏾 👰 Identity Management	Network Resources 🛃 Web Portal Management
Deployment Licensing Certificates Loggin	ng Maintenance Admin Access Settings
Deployment	Deployment Nodes List > Configure Node
N. = :=	Register ISE Node - Step 2: Configure Node
heployment	
	General Settings
	Hostname Ise-2
	FQDN ise-2.cisco.local IP Address 10.4.48.42
	Node Type Identity Services Engine (ISE)
	Tode Type Identity Services Engine (15:)
	Personas
:	Administration Role SECONDARY
	Monitoring Role SECONDARY Other Monitoring Nade
	✓ Policy Service
	Enable Session Services ①     Include Node in Node Group ISE-Group      V
	✓ Enable Profiling Service
	Submit Cancel

**Step 23:** Next, you'll configure which methods are used to profile network endpoints for the secondary policy service node.

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

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

<b>V</b>	▼ RADIUS		
		Description	-
		RADIUS	_

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

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

**Step 28:** Enter the IP address or host name of the secondary monitoring Cisco ISE from Table 1 (in this example, ise-4.cisco.local) and the credentials for the admin account, and then click **Next**.

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

**Step 30:** Click **Submit**. The node registers, and a pop-up window displays letting you know that the process was successful. Click **OK**.

CISCO Identity Services Engine		ise-1 admin Logout Feedback
🋕 Home Operations 🔻 Policy 🔻 Admini	stration 🔻	👓 Task Navigator 👻 😢
🔆 System 🦉 Identity Management	Network Resources 🛃 Web Portal Management	
Deployment Licensing Certificates Loggin	ng Maintenance Admin Access Settings	
Deployment	Deployment Nodes Lit > Configure Node	
<ul> <li>← = :::: ::::::::::::::::::::::::::::::</li></ul>	Register ISE Node - Step 2: Configure Node	
	General Settings  Hostname Ise-4 FQDN Ise-4.cisco.local IP Address 10.4.48.44 Node Type Identity Services Engine (ISE)  Personas Administration Role SECONDARY Monitoring Role SECONDARY Other Monitoring Node Ise-3 Policy Service Enable Session Services Include Node in Node Group <none></none>	
	Enable Profiling Service  Submit Cancel	

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

#### Procedure 5

#### Install Cisco ISE license

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



#### **Tech Tip**

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

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

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

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

Step 3: Under Licensed Services, click Add Service.

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

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	
License Operations	Correct Lorenze - Nei- Import new License File - License File Circlownladdhre-bate-Ricense Ric (Browne)	
	Import Cancel	

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

#### Procedure 6

**Configure network devices in Cisco ISE** 

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

**Step 1:** Mouse over **Administration**, and then, from the Network Resources section of the menu, choose **Network Devices**.

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



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

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

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



#### **Procedure 7**

**Configure Cisco ISE to use Active Directory** 

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

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

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

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

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

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

🛕 Home Operations 🔻 Policy	<ul> <li>Adminis</li> </ul>	tration 🔻	\varTheta Task Navigator 👻 🧧
🔆 System 🛛 🖉 Identity Managem	ent 🔛 N	twork Resources 🛛 👪 Guest Management	
dentities Groups Edernal Ident	ity Sources	Identity Source Sequences Settings	
External Identity Sources		Active Directory > AD1	
<b>◆•</b>	@ <b>.</b>	Connection Advanced Settings Groups Attributes	
Certificate Authentication Profile	۲	* Domain Name cisco.local	
2 Active Directory		* Identity Store Name AD1	
LDAP	۲	One or more nodes may be selected for Join or Leave operations. If a node is joined	then a leave
RADIUS Token	۲	operation is required before a rejoin. Select one node for Test Connection.	
RSA SecurID	۲	9 Join 9 Leave 9 Test Connection -	
		ISE Test Connection × ode Role Status	
		VISE * User Name: employee1 ARY A Not Joined to E	omain
		Ise * Password: ••••••• INDARY A Not Joined to E	omain
		Cancel	

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

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

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

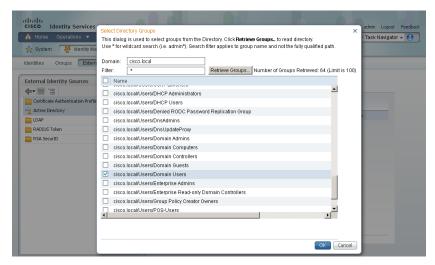
cisco Identity Services Engine		ise-1 admin Logout Feedback
🛕 Home Operations 🔻 Policy 🔻 Admi	nistration 🔻	\varTheta Task Navigator 👻 😢
🔆 System 🛛 🖉 Identity Management 🛛 📰	Network Resources 🛃 Guest Management	
Identities Groups External Identity Sources	Identity Source Sequences Settings	
External Identity Sources	Advanced Settings Groups Attributes	en a leave
	IDE         Join Doman         ×         pde Role         Status           V         ise         *User Name: Administrator         NRV         db. Not Joined to Dor           V         ise         *Password:         ••••••••         NDARY         db. Not Joined to Dor	

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

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

**Step 10:** Search for the groups you wish to add. The domain box is already filled in. The default filter is a wildcard to list all groups. Click **Retrieve Groups** to get a list of all groups in your domain.

Step 11: Select the groups you want to use for authentication, and then click OK. For example, for all users in the domain, select the group <domain>/ Users/Domain Users.



#### Step 12: Click Save Configuration.

#### Procedure 8

**Disable IP Phone authorization policy** 

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

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

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

🏠 Home Operations 🔻 Policy 🔻	Administration 🔻	😁 Task Navigator 👻
Authentication S Authorization	🔀 Profiling 🕐 Posture 🕞 Client Provisioning 🚍	Security Group Access 💦 🚯 Policy Elements
uthorization Policy		
	les based on identity groups and/or other conditions. Drag and drop	nies to change the order
rst Matched Rule Applies +		
Exceptions (0)		
Standard		
	Conditions (identity groups and other conditions)	Permissions
Standard	Conditions (dentity groups and other conditions) If <b>Blacklist</b>	Permissions then Blackist_Access Edit   •
Standard Status Rule Name	if Blacklist	then Blackist_Access Edit   +
Standard Status Rule Name Black List Default	if Blacklist	then Blackist_Access Edit   +

#### **Process**

Enabling Visibility to the LAN

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

Cisco ISE now has a baseline configuration. The next step is to configure Cisco ISE with an authentication policy and to configure the switches for identity by using Cisco Prime LMS 4.2 and the Cisco TrustSec Work Center.

#### Procedure 1

#### **Configure MAC Authentication Bypass**

MAC Authentication Bypass (MAB) allows you to configure specific machine MAC addresses on the switch to bypass the authentication process. For monitor mode, this is required, since you aren't enforcing authentication. MAB will be configured to allow any MAC address to authenticate.

**Step 1:** Mouse over **Policy**, and then choose **Authentication**. The Policy Type is Rule-Based.

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

**Step 2:** For the MAB policy, click the black triangle to the right of the **and...**. This brings up the identity store used for the MAB rule.

cisco Identity Services Engine		ise-1 admin Logout Feedbac
🚖 Home Operations 🔻 Policy 🔻	Administration 🔻	👓 Task Navigator 👻 😢
Authentication 🧕 Authorization	🛃 Profiling 💿 Posture 🕞 Clent Provisioning 📄 Security Group Access 🔥 Policy Elements	
Authentication Policy Define the Authentication Policy by selecting th Policy Type Simple Rule-Based	e protocols that ISE should use to communicate with the network devices, and the identity sources that it should use f	or authentication.
Default	: USB Internal Endpoints 💠	Actions *
Dot1X	: If Wired_802.1X 🕀 allow protocols Allowed Protocol : Default Netwo and 🕨	🖗 Actions 🕶
Default Rule (If no match)	: allow protocols Allowed Protocol : Default Netwo	🙀 Actions 🔻

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

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

**Step 4:** In this example deployment, all endpoints are allowed to authenticate. Set the following values, click anywhere in the window in order to continue, and then click **Save**:

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

cisco 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	
Policy Type O Simple   Rule-Based	SE should use to communicate with the network devices, and the identity sources that it should	
MAB : If Wired	MAB    AMA	🖗 Actions 💌
DottX : If Wired	If authentication failed <u>Contruue</u> * If users not found <u>Contruue</u> * If process failed <u>Conc</u> * Note: For authentications using PEAP, LEAP, EAPFAST or RADIUS MSCHAP it is not possible to contrue processing when authentication fails or user is not found. If contruue option is selected in these cases, requests will be rejected.	ه Actors •       ه Actors •

#### Procedure 2

**Configure 802.1X for wired users** 

There is already a Dot1X rule configured on the engine. Although in this example deployment you aren't deploying any wired endpoints with 802.1X supplicants at this point, you should still configure this rule to prepare for the next phase of an identity deployment.

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

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

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

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

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

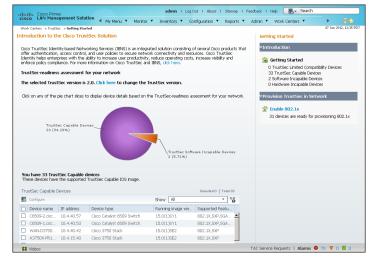
**Step 5:** In the **Identity Source** list, choose the previously defined AD server **AD1**, use the default options for this identity source, click anywhere in the window to continue, and then click **Save**.

🛕 Home Operations 🔻 Policy 💌	Administration 🔻				👓 Task Navigator 👻
Authentication S Authorization	🛃 Profiling	🖸 Posture 🕞 Client Provisioning	🚊 Security Group Access	🐥 Policy Elements	
uthentication Policy					
efine the Authentication Policy by selecting t	he protocols that I	SE should use to communicate with the ne	twork devices, and the identity so	surces that it should use	for authentication.
MAB	: If Vired_	MAB 🔶 allow protocols Allo	wed Protocol : Default Netw📀	and	🖗 Actions 💌
Wired-Dot1X	: If Wired_	802.1X 🕀 allow protocols Allo	wed Protocol : Default Netw📀	and 🚽	🖗 Actions 💌
Default	: use	Internal Users			🎡 Actions 🔻
		Identity Source AD1	0		
		Options If authentication failed Reject	¥		
Default Rule (If no match)	: allow proto		* *		🚔 Actions 👻
		Note: For authentications using PEAP, LE			
		it is not possible to continue processing If continue option is selected in these ca	when authentication fails or user is	not found.	

#### **Procedure 3**

Enable RADIUS in the access layer

**Step 1:** In a web browser, connect to Cisco Prime LMS, for example: https:// Ims.cisco.local. **Step 2:** Mouse over **Work Centers**, and then, from the TrustSec section, choose **Getting Started**. This shows the network's Cisco TrustSec-readiness assessment, which verifies that the software versions support the identity features and that the switches are capable of running RADIUS.



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

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

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

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

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

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

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

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

sco LAN Management Solut	ion 🚽 My Menu 🔻 Monitor 🔻 Ir	wentory V Configuration	▼ Reports ▼ Admin ▼ Work Cr ▶	
/ork Centers > TrustSec > RADIUS Config		,,		un 2012, 13:13
Navigator	Configure RADIUS			
Dashboard	It is recommended to have RADIUS serv	er configuration for authentic	ation and authorization before configuring ide	ntity on the
Getting Started	devices. The following workflow facilitates	RADIUS server configuration	and make the devices radius enabled.	
Readiness Assessment	Select Devices			<b>v</b>
RADIUS Configuration	Configure RADIUS Server			
Identity Configuration				
<ul> <li>Secured Group Access Configuration</li> </ul>	Radius Configuration			
Reports	RADIUS host 🔿 Single 💿 RADIUS G	Broup		
Jobs				
	All fields are required.			
	You can create only single RADIUS gro	up, which can contain multiple	RADIUS servers.	
	RADIUS Group Name ISE-Group		Shared Key	
		Verify:	Shared Key	
	🖊 Edit 🗙 Delete 🛛 🛛 Add	🝸 Filter		
	Server Name or IP Address	Authentication port	Accounting port	
	O 10.4.48.41	1645	1646	
	0 10.4.48.42	1645	1646	
	AAA Configuration			
	<ul> <li>Enable for 802.1X / MAB AAA.</li> <li>Enable AAA for Web Authentication</li> </ul>	n.		
		n.	Previous Next Finish	Cancel

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



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

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



**Enable identity** 

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

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

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

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

/ork Centers > TrustSec > Identity Conf	,	le Interfaces for Ide				07 Jun 2012, 1
Navigator	Chido	in memory lot for fac				
Dashboard	Sele	ct Devices and Port Gr	oups			
Getting Started						
Readiness Assessment	Sele	act devices from the list o	of Identity Capable	devices, and Select the por	t group	is associated with these devices.
RADIUS Configuration						
<ul> <li>Identity Configuration</li> </ul>		entity Capable Devices			-	
Manage Identity		🕈 Filter				Port Group Selector
Configuration		Display Name	IP Address 10.5.20.5	Device Type		▼ All Groups
Enable Identity on Interface		A2960S.cisco.local RS204-	10.5.20.5	stack Cisco Catalyst 2960	-	✓ 1 Gbps Ethernet Ports
Change of Authorization		A2960S.cisco.local	10.5.60.5	stack		✓ 10 Gbps Ethernet Ports
		RS211- A2960S.cisco.local	10.5.156.5	Cisco Catalyst 2960 stack		✓ 10 Mbps Ethernet Ports
<ul> <li>Secured Group Access Configuration</li> </ul>		RS208-	10.5.87.2	Cisco Catalyst 2960		✓ 100 Mbps Ethernet Ports
<ul> <li>Reports</li> </ul>		A2960S.cisco.local RS232-		stack		Access Ports
		D3750X.cisco.local	10.5.215.254	Cisco 3750 Stack		DMP Ports
Jobs		RS208-A3560X- PR1.cisco.local	10.5.87.3	Cisco Catalyst 3560X- 24P-L,S Switch		End Hosts
		RS232- A3560X.cisco.local	10.5.215.2	Cisco Catalyst 3560X- 24P-L,S Switch		IP Phones     IPVSC Ports
		A3750X.cisco.local	10.4.79.2	Cisco 3750 Stack		PARC HOLD
		D6500VSS.cisco.local	10.4.15.254	Cisco Virtual Switching System	-	
						Previous Next Finish Canc
	Revi	ew Part Groups				
	Cont	figure Identity				
	Sche	edule Deplovment				

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

ork Centers > TrustSec > Identity Confi	guration > Enable Identity on Interface				07 Jun 2012, 13:
Navigator	Enable Interfaces for Identity				
Dashboard	Select Devices and Port Groups				
Getting Started	Review Port Groups				
Readiness Assessment					
RADIUS Configuration	View the ports and unselect the	ports that you	wish to exclude.		
<ul> <li>Identity Configuration</li> </ul>	Selected Devices	Ass	ociated Ports		
Manage Identity	Display Name	<b>V</b>	Port Name	Description	
Configuration	<ul> <li>A3750X.cisco.local</li> </ul>	$\checkmark$	Gi1/0/36	GigabitEthernet1/0/36	-
Enable Identity on Interface		✓	Gi1/0/37	GigabitEthernet1/0/37	_
Change of Authorization		✓	Gi1/0/34	GigabitEthernet1/0/34	
change of Addioit2ation		✓	Gi3/0/18	GigabitEthernet3/0/18	
Secured Group Access		$\checkmark$	Gi3/0/19	GigabitEthernet3/0/19	
Configuration		✓	Gi1/0/35	GigabitEthernet1/0/35	
Reports		✓	Gi3/0/16	GigabitEthernet3/0/16	
lobs		$\checkmark$	Gi3/0/17	GigabitEthernet3/0/17	
		$\checkmark$	Gi1/0/38	GigabitEthernet1/0/38	
			GI2/0/14	GiashitEthorpot2/0/14	•
				Previous Next F	inish Cance
	Configure Identity				

Next, you configure monitor mode.

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

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

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

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

**Step 8:** In the Additional Configurations section, select **Advanced Options**, and then in the **Adhoc commands** box, enter the following command, and then click **Next**.

device-sensor accounting



#### **Tech Tip**

For device profiling, you need to enable the IOS Sensor feature on the switch to include DHCP and CDP information in the RADIUS messages sent from the switch to Cisco ISE. The IOS Sensor feature relies on information from the DHCP snooping feature that was enabled in the *LAN Deployment Guide*.

	iguration > Enable Identity on Interface 07 Jun 2012,
Navigator	Enable Interfaces for Identity
Dashboard	Select Devices and Port Groups
Getting Started	Review Part Groups
Readiness Assessment	Configure Identity
RADIUS Configuration	
<ul> <li>Identity Configuration</li> </ul>	Identity mode to be configured
Manage Identity Configuration	Choose the Security mode based on the level of security required in the devices. Values shown as selected are the default values are the default values and the security mode based on the level of security required in the devices.
Enable Identity on Interface	Select the security mode based on the level of security you wish to implement in your network More Details >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
Change of Authorization	Security Made
<ul> <li>Secured Group Access Configuration</li> </ul>	Monitor Low impact High security
Reports	Authentication profile and host mode
Jobs	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
	Select the action to be taken when a port security violation is detected due to the following reasonsMore Detait: ► Action to be taken on security violation
	MAC Configuration
	Enable MAC move or replace More Details   Enable SNMP notification for MAC addition or removal More Details
	Enable MAC move     Notify MAC addition
	Enable MAC replace     Notify MAC removal
	Additional Configurations
	If you have selected low impact mode and if AQ, is not configured on the device, you More Details > Advanced options
	Adhoc commands* : device-sensor accounting

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

Step 9: In the Job Description box, enter a description, click Finish, and then click OK.

### **Tech Tip**

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

IIII. Cisco Prime	admin   Log Out   About   Sitema	ip I Feedback I Help 🕞 ▼ Search
ISCO LAN Management Sol	My Menu   Monitor  Inventory  Configuration	
Work Centers > TrustSec > Identity Confi	guration > Enable Identity on Interface	07 Jun 2012, 13:30 P
Navigator	Enable Interfaces for Identity	
Dashboard	Select Devices and Port Groups	✓
Getting Started	Review Port Groups	✓
Readiness Assessment	Configure Identity	✓
RADIUS Configuration	Schedule Deployment	
<ul> <li>Identity Configuration Manage Identity Configuration</li> </ul>	Scheduler	* Indicates required field
Enable Identity on Interface	Immediate     Job Description*     A3750X Mo	onitor Mode Config
Change of Authorization	O Daily E-mail	
<ul> <li>Secured Group Access Configuration</li> </ul>	Monthly	
Reports	Job Options	nable job password
Jobs	Fail on mismatch of config versions	Login Username
	Sync archive before job execution	Login Password
	Copy running config to startup	Enable Password
	Failure policy Ignore failure and continue	
	P	review CLI Previous Next Finish Cancel

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

aaa group server radius ISE-Group
server 10.4.48.41
server 10.4.48.42

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

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

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

#### interface [interface]

authentication host-mode multi-auth authentication open authentication order dot1x mab authentication port-control auto mab

dot1x pae authenticator

#### Procedure 5

#### Disable port security timers

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

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

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

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

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

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

## **Tech Tip**

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

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

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

Step 8: In the Variable list, choose Identity\_Security\_Mode.

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

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

cisco LAN Manager	admin I Log Out I About I Sitemap I Feedback I Help 🔣 - Search
CISCO ENVIRIANDE	🔨 My Menu 🔻 Manitor 🔻 Inventory 👻 Configuration 🔻 Reports 👻 Admin 🔻 Work Ce 🕨 📅 😭
Mode: PORT	Groups
ef 1. Device and Group Selector	Port Groups
2. Groups	C Select Custom Group(s)      Define an Adhoc Rule     Adhor Rule
3. Tasks	Adhoc Kule
<ul> <li>4. Add Tasks</li> <li>5. Set Schedule Options</li> </ul>	
G. View Job Work     Order	Object Type: Variable: Operator: Value: OR  Port V Identity_Security_Mode V Add Rule Expression
	<pre>route Test Port.Identity_Security_Mode = "Nonitor"</pre>
	- Step 2 of 6 - Back Next Findh Cancel
H Videos	TAC Service Requests   Alarms 👁 71 🔻 0 🖬 0

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

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

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

no switchport port-security violation

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

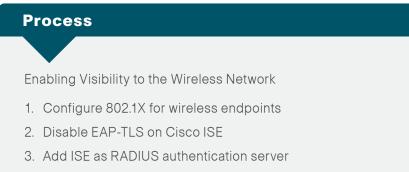
Adhoc Task Confi	igur	ation				
<b>IOS Parameters</b>						
Commands						
CLI Commands:	no no no	switchport	port-securit port-securit port-securit	y aging	type	
						.::
Rollback Commands:						
			A	pplicable [	)evices	
			Save	Reset	Cancel	

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

July Cisco Prime	admin i Log Out i About i Sitemap i Feedback i Help 🔣 🖶 Search	
cisco LAN Manageme	t Solution 🛛 🔨 My Menu 🔻 Monitor 🔻 Inventory 🔻 Configuration 🔻 Reports 🔻 Admin 🔻 Work Gr 🕨 🛛 😤 🗧	
Mode: ADDING d' 1. Device and Group Selector d' 3. Tasks 4. Add Tasks 5. Se Soledde Options 6. View Job Work Order	Add tasks Add instance Add instance Back Next Frich Cancel	
H Videos	TAC Service Requests   Alarms 🔮 71 🔻 0 💆 0	5

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

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



- 4. Add Cisco ISE as RADIUS accounting server
- 5. Enable DHCP profiling

To authenticate wireless clients, you need to configure the wireless LAN controllers (WLC) to use the new Cisco ISE servers as RADIUS servers for authentication and accounting. The existing entry is disabled so that if there are any issues after moving to Cisco ISE, you can quickly restore the original

configuration. Additionally, you configure the WLCs for DHCP profiling so that profiling information can be obtained from the DHCP requests from these clients and sent to the Cisco ISE.

#### Procedure 1

**Configure 802.1X for wireless endpoints** 

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

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

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

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

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

ahah			Dictionaries		
	ervices Engine		٩		ise-1 admin Logout Feedback
🛕 Home Operation	ns 🔻 Policy 🔻 Administ	ration 🔻	🔶 📃 📜 🐘		👓 Task Navigator 👻 😢
Authentication	Authorization K Pr	ofiling 👩 Posture	Simple Condition 💿	roup Access	
		- L.a	Compound Condition 3		
Authentication Policy					<u> </u>
	Policy by selecting the protoc	ols that ISE should use to o	c .	d the identity sources that it should us	e for authentication.
Policy Type 🔿 Simple	<ul> <li>Rule-Based</li> </ul>				
MAB 👻	: If	Wired_MAB	>	fault Netw📀 🛛 and 😱	🎡 Actions 👻
Vired-Dot	HIX : If	Wired 802.1X		and	🖗 Actions 👻
II WIRD-DO		Wired_802.1X %			SP ALOURS *
🛛 🔻 Wireless-D	Oot1X : If	Condition(s) =	2	es 📀 and 🕨	🎡 Actions 👻
		Add All Conditions B			
Default Ru	ule (If no match) : all				· · · · · · · · · · · · · · · · · · ·
		Condition Name Select Condition	⊙]		ŵ-
		Select condition	<u>V </u> ];		24.4

Step 5: Choose Wireless\_802.1X, and then click anywhere to continue.

Wired_802.1X Wireless_802.1X Switch_Local_Web_Authentication	Froup Access 🔒 Policy Elements	
Wired_802.1X Wireless_802.1X Switch_Local_Web_Authentication		
Switch_Local_Web_Authentication		
WCC_Web_Addrenication	nd the identity sources that it should us	se for authentication.
	efault Netw📀 🛛 and 🕨	🎡 Actions 👻
	əfault Netw📀 🛛 and 🕨	🎡 Actions 👻
	s 📀 and 🕨	🖗 Actions 👻
		*
]		\
]		and

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

🏠 Home Operations 🔻 Policy 🔻	Administration 🔻				😶 Tas	Navigator 👻
Authentication	🔀 Profiling 🛛 💇 Posture	🛃 Client Provisioning	🚊 Security Group Access	Policy Elements		
Authentication Policy lefine the Authentication Policy by selecting olicy Type O Simple O Rule-Based				_		
MAB	: If Wired_MAB		wed Protocol : Default Netwo	and 🕨	÷	Actions 👻
Wired-Dot1X	: If Wired_802.1X	allow protocols Allo	wed Protocol : Default Netw 📀	and 🕨	- 	Actions 💌
Wireless-Dot1X	: If Wireless_802.1X	🔶 allow protocols Sele	ict Network Access	] and 🕨	- 	Actions 💌
Default Rule (If no match)	: allow protocols Allowed	Protocol : Default Netwo	and use identity source :	Allowed Protocols	٩	Actions 👻

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

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

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

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

Authentication Authorization Poling Authentication Policy Define the Authentication Policy by selecting the protocols that I Define the Authentication Policy by selecting the protocols that I Define the Authentication Policy By selecting the protocols that I Define the Authentication Policy By selecting the protocols that I Define the Authentication Policy By selecting the protocols that I Define the Authentication Policy By selecting the protocols that I Define the Authentication Policy By selecting the protocols that I Define the Authentication Policy By selecting the protocols that I Define the Authentication Policy By selecting the protocols that I Define the Authentication Policy By selecting the protocols that I Define the Authentication Policy By selecting the protocols that I Define the Authentication Policy By selecting the protocols that I Define the Authentication Policy By selecting the protocols that I Define the Authentication Policy By selecting the protocols that I Define the Authentication Policy By selecting the protocols that I Define the Authentication Policy By selecting the protocols that I Define the Authentication Policy By selecting the protocols that I Define the Authentication Policy By selecting the protocols that I Define the Authentication Policy By selecting the protocols that I Define the Authentication Policy By selecting the protocols that I Define the Authentication Policy By selecting the Policy By selecting t	If process failed Drop *	se for authentication.
Default : use     Default Rule (If no match) : allow proto	Internal Users  Col: Allowed Protocol : Default Netwood and use identity source : Internal Users	Actions

**Procedure 2** 

#### Disable EAP-TLS on Cisco ISE

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

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

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

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

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

🛕 Home Operations 🔻 Policy 🔻		e-1 admin Logout Feedback
Authentication Authorization	🔀 Profiling 🎯 Posture 🕞 Client Provisioning 📄 Security Group Access 🏾 🌲 Policy Elements	
Results	Detect PAP as Host Lookup Allow CHAP Allow MS-CHAP1 Allow MS-CHAP2 Allow BAP-MD5 Detect EAP-MD5 as Host Lookup Detect EAP-MD5 as Host Lookup Allow EAP-M5 Detect EAP-MD5 as Host Lookup Allow EAP-M5 Allow EAP-M5-CHAPv2	

#### Procedure 3

Add ISE as RADIUS authentication server

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

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

Step 2: On the menu bar, click Security.

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

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

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

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

սիսիս cisco	MONITOR WLANS	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	Sa <u>x</u> e ( HELP	Configuration <u>P</u> ing <u>E</u> EEDBACK	Logout <u>R</u> efresh
Security	RADIUS Authenti	cation Server	s > New					< Back	Apply
<ul> <li>AAA         General         <ul> <li>RADIUS</li> <li>Authentication             Accounting             Fallback</li>             TACACS+             LoAP             Local Net Users             MAC Filtering             Disabled Clients             User Login Policies             AP Policies</ul></li>             Local EAP             Priority Order             Certificate             Access Control Lists             Wireless Protection             Policies             Wehauth             Advanced </ul>	Server Index (Prior) Server IP Address Shared Secret Form Shared Secret Confirm Shared Secret Key Wrap Port Number Server Status Support for RFC 353 Server Timeout Network User Management IPSec	at ret	2 v 10.4.48.41 ASCII v Cossigned fo 1812 Enabled v Enabled v Enable Enable Enable		ers and requires a	key wrap compl	iant RAD	IUS server)	

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

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

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

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

սիսիս										Logout <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs <u>C</u> C	NTROLLER	WIRELESS S	BECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	EEEDBACK	
Security	RADIUS	Authenticati	on Servers	6					Apply	New
▼ AAA General ▼ RADIUS		tion ID Type 💈	IP Address	•						
Authentication Accounting	Use AES	S Key Wrap	(Designed	for FIPS customer	rs and requi	es a key wrap co	mpliant RADIUS	server)		
Fallback	MAC De	limiter	Hyphen	•						
▶ TACACS+ LDAP Local Net Users	Network User	Management	Server Index	Server Addres	ss Port	IPS	iec	Admin	Status	
MAC Filtering Disabled Clients	$\checkmark$		1	10.4.48.15	1812	Dis	abled	Disable	d 🔽	
User Login Policies AP Policies	<b>V</b>		2	10.4.48.41	1812	Dis	abled	Enabled		
Local EAP	1		3	10.4.48.42	1812	Dis	abled	Enabled	t 🔽	
Priority Order										
Certificate				1.4						
Access Control Lists	1. Call Stat	ion ID Type will t	e applicable (	only for non 802.1	ix authentici	ttion only.				
<ul> <li>Wireless Protection</li> <li>Policies</li> </ul>										
Web Auth										
Advanced										

#### Procedure 4

Add Cisco ISE as RADIUS accounting server

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

Step 1: On the menu bar, click Security.

Step 2: In the left pane, under the RADIUS section, click Accounting.

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

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

սիսիս							Configuration   Ping	Logout   <u>R</u> efresh
CISCO	MONITOR WLANS CONT	ROLLER WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	EEEDBACK	
Security	RADIUS Accounting Se	rvers > New					< Back	Apply
AAA     General     RADIUS     Authentication     Accounting     Fallback     TACACS+     LOAP     Local Net Users     MAC Filtering     Disabled Clients     User Login Policies     AP Policies     Local EAP	Server Index (Priority) Server IP Address Shared Secret Format Shared Secret Confirm Shared Secret Port Number Server Status Server Timeout Network User	2 • 10.4.48.41 ASCII • 1813 Enabled • 2 seconds V Enable						
<ul> <li>Priority Order</li> <li>Certificate</li> <li>Access Control Lists</li> <li>Wireless Protection Policies</li> <li>Web Auth</li> <li>Advanced</li> </ul>	IPSec	Enable						

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

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

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

սիսիս							Sa	<u>ve</u> Configuration <u>P</u> ing Logout <u>R</u> efresh
CISCO	MONITOR	<u>W</u> LANS <u>C</u> (	ONTROLLER WIREL	ESS <u>s</u> ec	CURITY MANAGE	MENT C <u>O</u> MMAI	IDS HE	LP EEEDBACK
Security	RADIUS A	ccounting	Servers					Apply New
AAA     General     RADIUS	MAC Delim	iter Hyph	ien 👻					
Authentication Accounting	Network User	Server Index	Server Address	Port	IPSec	Admin Status		
Fallback TACACS+	$\checkmark$	1	10.4.48.15	1813	Disabled	Disabled		
LDAP Local Net Users	<b>V</b>	2	10.4.48.41	1813	Disabled	Enabled		
MAC Filtering Disabled Clients User Login Policies AP Policies	V	3	10.4.48.42	1813	Disabled	Enabled		
Local EAP								
Priority Order								
▶ Certificate								
Access Control Lists								
<ul> <li>Wireless Protection</li> <li>Policies</li> </ul>								
▶ Web Auth								
Advanced								

#### Procedure 5

#### Enable DHCP profiling

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

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

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

CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY	( MANAGEMENT COMMANDS HELP EEEDBACK	
/LANs	WLANs > Edit '10k-WLAN-Data'	< Back	Apply
WLANs WLANs	General Security QoS Advanced		_
Advanced	Maximum Allowed 0	NAC State None 💌	-
	Static IP Tunneling	Load Balancing and Band Select	
		Client Load Balancing 📃	
	Wi-Fi Direct Clients Disabled 💌	Client Band Select Z	
	Maximum Allowed	Passive Client	
	Clients Per AP 200 Radio	Passive Client	
	Off Channel Scanning Defer	Voice	
	Scan Defer 0 1 2 3 4 5 6 7	Media Session Snooping 📃 Enabled	
		Re-anchor Roamed Voice Clients 🔲 Enabled	
		KTS based CAC Policy Enabled	
	Scan Defer Time 100	Client Profiling	
	FlexConnect	DHCP Profiling 🔽 Enabled	
	FlexConnect Local Enabled	-	
	FlexConnect Local Auth 💶 🗖 Enabled		
	Learn Client IP Address 💈  Enabled		
	•		
	Foot Notes		
	1 Web Policy cannot be used in combination with IPsec	TE authentication, Override Interface ACLs	

**Step 3:** When the message appears about enabling DHCP Reqd and disabling Local Auth, click **OK**, and then click **Apply**.

**Step 4:** When a message appears saying that the WLANs need to be disabled, click **OK**.

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

#### Process



Deploying Digital Certificates

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

In the next phase of deployment, you configure the infrastructure to support the use of digital certificates for user and machine authentication. Using digital certificates when deploying 802.1X is a Cisco best practice. In this example deployment, you will be deploying digital certificates to Microsoft Windows XP and Windows 7 endpoints as well as to Apple Mac OS X devices. The certificate authority (CA) you will be using is the one built into Windows Server 2008 Enterprise, and you will enable it on the existing Active Directory (AD) server.

#### **Procedure 1**

#### Install certificate authority

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

#### **Reader Tip**

For more information about installing a certificate authority, see the Microsoft Windows Server 2008 Active Directory Certificate Services Step-by-Step Guide:

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

#### Procedure 2

Install trusted root certificate for domain

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

**Step 1:** On the CA console, launch a web browser, and then connect to the certificate authority, http://ca.cisco.local/certsrv.

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

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

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

Microsoft Active Directory Certificate Services cisco-AD-CA	<u>Home</u>							
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:								
Encoding method: © DER © Base 64								
Download CA certificate Download CA certificate chain Download latest base CRL Download latest delta CRL								

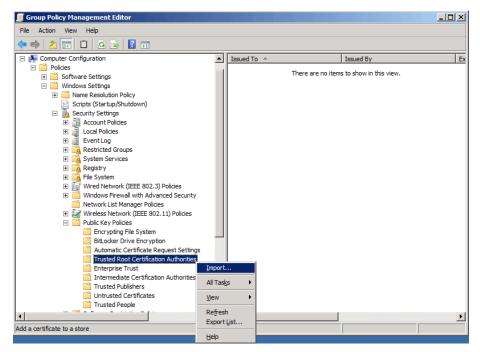
Step 5: On the AD console, navigate to Start > Administrative Tools > Group Policy Management.

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

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

🧾 Group Policy Management							_ 🗆 🗵
File Action View Window H	Help						_ 8 ×
♦ ≥	2 🖬						,
Group Policy Management Group Policy Management Group Policy Management Group Policy Management Group Policy Modeling Group Policy Modeling Group Policy Modeling Group Policy Modeling	y Default Scope   Links Display li Security Grou Controllers Po	ering     this GPO can only appl     tated Users	cisco.local are linked to thi y to the following	Enforced No	Link Enabled Yes	cisco.local	×
	Copy Delete Rena <u>m</u> e Refresh	Remov		Propertie	8		
- -	Help	nked to the following WI	All filter:	•	Open		
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.



Step 9: Click Next.

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

Certificate Import Wizard	×
File to Import	
Specify the file you want to import.	
	_
File name:	
C:\Downloads\certnew.cer Browse	
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 <u>certificate file formats</u>	
< Back Next > Cancel	

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

Step 12: Click Finish. The certificate imports.

Step 13: Click OK to close the wizard.

#### Procedure 3

#### Install trusted root on AD server

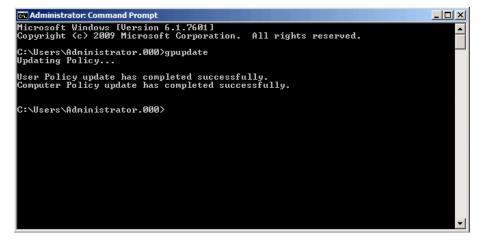
In addition to configuring AD server to distribute the trusted root certificate to workstations, you need to install the certificate directly on the AD server. A group policy object (GPO) update takes care of this automatically. In this procedure, you will force the update to run immediately.

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

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

Step 3: Update the group policy.

gpupdate



**Procedure 4** 

Request a certificate for ISE from the CA

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

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

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

Step 3: Under Certificate Operations, select Local Certificates.

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

cisco Identity Services Engine		ise-1 admin Logout Fee
🛕 Home Operations 🔻 Policy 💌 A	administration 🔻	😷 Task Navigator 👻 🕻
🔆 System 🦉 Identity Management	🖀 Network Resources 🛛 🛃 Web Portal Management	
Deployment Licensing Certificates L	Logging Maintenance Admin Access Settings	
Certificate Operations	Local Certificates	Selected 0   Total 1 🥵 🗟
Certificate Operations		Selected 0   Total 1 😵 🤤
	/Edt -Add @Export XDelete	Selected D   Total 1 😵 🎡 Show 🔠 💌
🔹 Local Certificates	/Edt = Add @>Export ★Delete	
🔹 Local Certificates 🔹 Certificate Signing Requests		Show Al V

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

cisco Identity Services Engine		ise-1 admin Logout Feedback
🛕 Home Operations 🔻 Policy 🔻 Adm	inistration 🔻	👓 Task Navigator 👻 😢
😽 System 🛛 🖉 Identity Management 👔	Network Resources 🛛 🛃 Web Portal Management	
Deployment Licensing Certificates Log	ging Maintenance Admin Access Settings	
Dertificate Operations Coal Certificates Coefficate Signing Requests Certificate Store Signing Certificate Store Signing Certificate Store Coefficient Store	Locd Cartificate & Generate Certificate Signing Request Generate Certificate Subject Certificate * Certificate Subject ON=sel.cisco.local * Key Length 2048 * Digest to Sign With 2048 *	
	Submit Cancel	

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

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

cisco Identity Services Engine					ise-1 admin Logout Feedba
🛕 Home Operations 🔻 Policy 🔻 Admir	nistration 🔻				👓 Task Navigator 👻 😢
🔆 System 🛛 👰 Identity Management 🛛 🖀	Network Resour	ces 🛛 🛃 Web Portal N	lanagement		
Deployment Licensing Certificates Logg	ing Maintenan	ce Admin Access	Settings		
Certificate Operations	Certificate \$	Signing Requests			Selected 1   Total 1 😵 🏭 🕳
Local Certificates     Certificate Signing Requests	Export	XDelete			Show Al 🔹 🐨
Certificate Store	Friendly I	Name 🖌	Certificate Subject	Key Length	Timestamp
SCEP CA Profiles	ise1.cisco	o.local	CN=ise1.cisco.local	2048	Wed Aug 15 08:48:18 PDT 2012
OCSP Services					

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

**Procedure 5** 

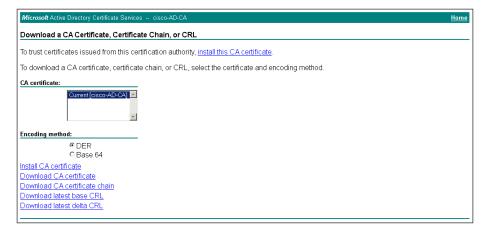
**Download CA root certificate** 

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

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

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

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



Procedure 6

Issue certificate for Cisco ISE

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

Step 2: Click Request a certificate.

Step 3: Click advanced certificate request.

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

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

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

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

Microsoft Active	Directory Certificate Services cisco-AD-CA <u>Horr</u>
Submit a Certi	ficate Request or Renewal Request
by an external s	ed request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated ource (such as a Web server) in the Saved Request box.
Base-64-encoded certificate request	uhtEchivSCttmVtpHe72nUgsG1fnRySEcJud7B62 LbP/xws3jIX4pLoBxcf312DYDbv2cOZSD0G1rfn CDUFqV2vBuVERs3ccZQERBfbHY3pgC0Uhft KQv134XNGW/eF12/UQ1JTF3juhn/HjvvcXGN1KD0 XHg1SBGNA%tnBffHhZuSBJ15csX0whhcdj6142Q2
Certificate Templ	ate: Web Server ▼
Additional Attribu	ites:
Attributes:	
	Submit>

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

**Procedure 7** 

Install trusted root certificate in Cisco ISE

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

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

🛕 Home Operations 🔻 Policy 🔻 A	Administration 🔻			👓 Task I	Navigator 👻 🕙
🔆 System 🛛 👰 Identity Management	📷 Network Resources 🛛 🛃 Web Portal Manageme	nt			
Deployment Licensing Certificates L	Logging Maintenance Admin Access Settings				
	0.115 1.01				
Cortificato Operations	Certificate Store				
Certificate Operations	Certificate Store			Selected 0   1	otal 4 😵 🎡 🖕
🔹 Local Certificates	/ Edt -Fimport Export XDelete		Sh	Selected 0   1	otal 4 👻 🔽
🔹 Local Certificates 🔹 Certificate Signing Requests		<ul> <li>Issued To</li> </ul>	Sh Issued By		
🔹 Local Certificates 🏩 Certificate Signing Requests 😋 Certificate Store	✓ Edt	Issued To     ise-1.cisco.local		ow Al	Expiration Date
Local Certificates     Certificate Signing Requests     Certificate Store     SCEP CA Profiles	Fidt ↓ Import		Issued By	ow All Valid From	Expiration D Sat, 3 Aug 2
Local Certificates     Certificate Signing Requests     Certificate Store	Edit Import Debet     Friendly Name     ise-1.cisco.local#56e-1.cisco.local#00001	ise-1.cisco.local	Issued By ise-1.cisco.local	w Al Vaid From Fri, 3 Aug 2012	- 8

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

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



**Procedure 8** 

Install local certificate in Cisco ISE

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

#### Step 2: Click Local Certificates.

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

cisco Identity Services Engine				ise-1	admin Logout Feedback
🛕 Home Operations 🔻 Policy 🔻 Admi	istration 🔻			••	Task Navigator 👻 🕗
🔆 System 🛛 🖉 Identity Management	Network Resources 🛛 🛃 Web Portal Management				
Deployment Licensing Certificates Logo	ng Maintenance Admin Access Settings				
Certificate Operations	Local Certificates			Select	ed 0   Total 1 😵 🚳 🖕
🔹 Local Certificates	/ Edit -Add Export XDelete			Show Al	1 2
🔹 Certificate Signing Requests				SIDW M	. 0
🙍 Certificate Store	Friend Import Local Server Certificate	<ul> <li>Protocol</li> </ul>	Issued To	Issued By	Valid From
SCEP CA Profiles	Defau Generate Self-Signed Certificate Generate Certificate Signing Request	HTTPS,EAP	ise-1.cisco.local	ise-1.cisco.local	Fri, 3 Aug 2012
S OCSP Services	Bind CA Certificate				

**Step 4:** Click **Browse** and locate the certificate saved from Procedure 6, "Issue certificate for Cisco ISE." **Step 5:** In the Protocol section, select both **EAP** and **Management Interface**. When you receive a message that selecting the Management Interface check box will require the Cisco ISE appliance to restart, click **OK**, and then click **Submit**.

cisco Identity Services Engine		ise-1 admin Logout Feedback
🛕 Home Operations 🔻 Policy 🔻 Admir	istration 💌	👓 Task Navigator 👻 🕙
🔆 System 🦉 Identity Management 📲	Network Resources 🛛 🛃 Web Portal Management	
Deployment Licensing Certificates Loggi	ng Maintenance Admin Access Settings	
Certificate Operations	Loci Cofficate » Eller Configued Certificate Bind CA Signed Certificate Certificate	
Certificate Signing Requests     Store		
SCEP CA Profiles	* Certificate File C\Downloads\JSEcert.cer Browse Filendly Name 0	
OCSP Services	mencely warte	
	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     A cettificate being imported may be determined to aheady exist in the system when it has either the     certificate     Certi	same Subject or Issuer and serial v the certificate contents to be
	Submit Cancel	

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

#### **Procedure 9**

Delete old certificate and request

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

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

Step 2: Click Local Certificates.

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

			admin Logout Feedb
🏠 Home Operations 🔻 Policy 🔻 Ad	dministration 🔻	•	🖲 Task Navigator 👻 🕙
🔆 System 🛛 🖉 Identity Management	🖬 Network Resources 🛛 🔮 Web Portal Management		
Deployment Licensing Certificates Li	ogging Maintenance Admin Access Settings		
Certificate Operations	Local Certificates		
Certificate Operations			ted 1   Total 2 😵 🎡 🖕
	Local Certificates	Selec	ted 1   Total 2 😵 🏭 🕇
🔹 Local Certificates 🚭 Certificate Signing Requests			
🔹 Local Certificates	✓Edk ♣Add ⊕Export XDelete	Show All	- 6

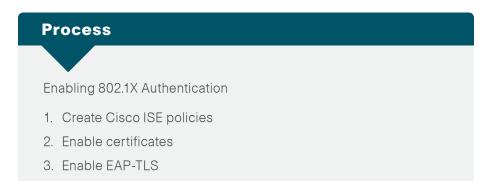
Step 4: Click Delete, and then click OK.

#### 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."

cisco Identity Services Engine		ise-1 admin Logout Feedbac
🏠 Home Operations 🔻 Policy 🔻 Adm	inistration 🔻	👓 Task Navigator 👻 🕗
🔆 System 🛛 👰 Identity Management	Network Resources 🛛 🚇 Web Portal Management	
Deployment Licensing Certificates Log	ging Maintenance Admin Access Settings	
Certificate Operations	Certificate Signing Requests	Selected 1   Total 1 😵 🎡 🖕
🧔 Local Certificates		
🔹 Certificate Signing Requests	Export XDelete	Show All 🔹 😽
S Certificate Store	Friendly Name 🔺 Certificate Subject Key Length	Timestamp
SCEP CA Profiles	✓ ise1.cisco.local CN=ise1.cisco.local 2048	Wed Aug 15 08:48:18 PDT 2012

Step 7: Click Delete, and then click OK.



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

#### Procedure 1

**Create Cisco ISE policies** 

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

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

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

nt 🔛 📰 Ne						👓 Task Navigator 🔻
- IVC	stwork Resources	🛃 Guest M	anagement			
y Sources	Identity Source Se	quences Se	ttings			
	Certificate Auth	entication Pr	ofile			Selected 0   Total 0
	/ Edit 🕂 Add		XDelete		Show	• Ila
	Name			<ul> <li>Description</li> </ul>		
۲				No data avalabic		
				No data available		
	· ·	Certificate Auth	Certificate Authentication Pr	Certificate Authentication Profile	Certificate Authentication Profile	Certificate Authentication Profile

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

🏠 Home Operations 🔻 Policy 🖲	Admir	istration 🔻		👓 Task Navigator 👻 😢
🔆 System 🛛 👰 Identity Manageme	nt 🔳	Network Resources 🛛 🍇 Guest Mana	agement	
Identities Groups External Identit	y Sources	Identity Source Sequences Settin	ngs	
External Identity Sources	ي. ب ب	Certificate Authentication Profiles Lits > New C Certificate Authentication Profi * Name [ Description		
RADIUS Token	•	Principal Username X509 Attribute	Subject Alternative Name	

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

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

🏠 Home Operations 🔻 Policy 🔻	Administration 🔻			👓 Task Navigator 👻 🔮
🔆 System 🛛 👰 Identity Management	🖀 Network Resources 🛛 🚇 Guest Management			
Identities Groups External Identity So	purces Identity Source Sequences Settings			
dentity Source Sequence				
lentity Source Sequence				Selected 0   Total 2 🤞
dentity Source Sequence	3		Show All	Selected 0   Total 2 🥞
/ Edit + Add Duplicate XDelete		Identity Stores	Show All	
dentity Source Sequence		Identity Stores Internal Users	Show All	

**Step 5:** Give the sequence a meaningful name.

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

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

Step 8: In the Advanced Search List Settings section, select Treat as if the user was not found and proceed to the next store in the sequence, and then click Submit.

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 Sequence: Ut > New Identity Source Sequence Identity Source Sequence	<b>A</b>
Identity Source Sequence	
*Name Dot1X_Certificates	
Description	
Certificate Based Authentication  Select Cartificate Authentication Profile Dot1X Certs    Authentication Search List  A set of identity sources that will be accessed in sequence until first authentication succeeds	
Available Selected	
Internal Endpoints A AD1 AD1	
▼ Advanced Search List Settings	
Select the action to be performed if a selected identity store cannot be accessed for authentication	
Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"	
Treat as if the user was not found and proceed to the next store in the sequence	

Procedure 2

#### Enable certificates

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

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

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

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

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

Interview Services Engine     Identity Services Engine     A Home Operators      Policy      Administration     Authoritization     Authorization     Policy     Policy     Policy     Policy     Policy     Posture     Q     Q     Q     Q     Control	ise-1 admin Logout Feedback 99 Task Navigator v 🕑 Ioning 🔄 Security Group Access 🔥 Polcy Elements
Authentication Policy         Define the Authentication Policy by selecting the protocols that ISE should use to communicate with Policy Type O Single Rule-Based         Image: I	S Allowed Protocol : Default Netwo
it is not possible to continue proc	ject v ject v Actions v

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

**Step 5:** For the **Wireless-Dot1X** rule, to the right of **and...**, click the black triangle. This brings up the identity store used for this rule. Next to the **Default** rule, in the **Actions** list, choose **Insert new rule above**.

cisco Identity Services Engine	ise-t admin Logout Feedback
🛕 Home Operations 🔻 Policy 🔻 Administration 👻	😬 Task Navigator 👻 🕙
🔒 Authentication 💿 Authorization 🔀 Profiling 👩 Posture 🛼 Clent Provisioning 🚊 Security Group Access 🔥 Policy Bernents	
Authentication Policy Defen 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  policy Tope Sime Sime Bessed	ior authentication.
MAB : If Wired_MAB $\diamondsuit$ alow protocols [Alowed Protocol : Default Netwoo] and	🖗 Actions *
Wired_Dot1X : If Wired_802.1X 💠 allow protocols Allowed Protocol : Default Netwo and 🕨	🎡 Actions 💌
Wrieless-Dot1X : If Wrieless_802.1X 🔶 allow protocols Allowed Protocol : Default Netwood and 🗸	🖗 Actions *
Default : use AD1 4	Actions *
Default Rule (If no match) : allow protocols Allowed Protocol : Default Netwo and use identity source : Internal Users 🔶	🖗 Actions 💌

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

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

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

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

cisco Identity Services Engine	Net	work Access	admin Logout Feedbaci
	Administration 🔻	(م بالا	Task Navigator + 😢
Authentication	🔀 Profiling 🛛 Posture 👵 Client Provisioning 📄 Security Group ( 💷 4	AuthenticationMethod	
Authentication Policy		Device IP Address EapAuthentication	
	protocols that ISE should use to communicate with the network devices, and the	EapTunnel	entication.
Policy Type 🔿 Simple 💿 Rule-Based		ISE Host Name	
MAB	If Wired MAB I alow protocols Allowed Protocol : Default N	NetworkDeviceName Protocol	🖗 Actions 👻
Vired-Dot1X		UseCase	Actions *
	u (	UserName	ST WOODS
Wireless-Dot1X	: If Wireless_802.1X I allow protocols Allowed Protocol : Default I		Actions -
	Expression Builder		×
EAP-TLS	: if Enter Co		
Default	Condition Name Expression Select Attribute O		1 
L Deraur		·	OK Cancel
Default Rule (If no match)	: allow protocols Allowed Protocol : Default Netwool and use identity source :	Internal Users	
Deraul( Kule (if ho match)	and the restored provided Protocol - Default NetWool and the restory source -	Internal Users 💠	Actions *

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

	Administration 🔻				🕫 Task Navigator 🔻
🛓 Authentication 🛛 🧕 Authorization	n 🔀 Profiling 🛛 🕅	Posture 🖳 Client Provisioning	😭 Security Group Access	🔒 Policy Elements	
thentication Policy					
fine the Authentication Policy by selecting icy Type   Simple  Rule-Based	the protocols that ISE sho	ould use to communicate with the n	network devices, and the identity st	surces that it should use to	or authentication.
MAB -	: IfWAB	allow protocols All	owed Protocol : Default Netw 📀	and 🕨	🖗 Actions 👻
Vired-Dot1X	: If Wired 802.1	x c alow protocok	owed Protocol : Default Netw	and	Actions +
					37 AC000 -
	: If Wireless 80	alow protocols	owed Protocol : Default Netwo	and 🖕	🚳 Actions 🕶
Vireless-Dot1X	Wireless_80				
Wireless-Dot1X	vireless_80	Expression Builder			×
······		Expression Builder	Library		×
Vireless-Dot1X	: If Enter G	Expression Builder			×
······		Expression Builder	Expression	ak • EAP-TLS •	

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

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

🛕 Home Operations 🔻 🛛	Nolicy 🔻 Administration 💌	👓 Task Navigator 🔻
🛓 Authentication 🛛 🧕 Aut	norization 🔀 Profiling 🖄 Posture 🕞 Client Provisioning 🔄 Security Group Access 🚓 Policy Bernents	
	whething the products that EE should use to communicate with the network devices, and the dentity sources that it should use to whether and the state of the st	ar authentication.
	: If Network accessEpauthentical 9 use InternalUsers	Actions *
	If shows left log →      If shows left log →      If anyons log →      If anyons left log →      If anyons left log →      If anyons left log →      If anyons log →      If an	WF ALCOID *

#### Step 13: Click Save.

#### Procedure 3 Enable EAP-TLS

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

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

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

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

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

A Hone       Operations       Policy       Administration       ere Task Navigator       ()         Authentication       Authentication       Authentication       Prodling       Posture       Client Provisioning       Security Group Access       Policy Elements         Dictionaries       Conditions       Results       ()       Allow MS-CHAPy1       Allow KS-CHAPy2       ()       Allow EAP-MDS         Image: Authentication       Image: Authentication       ()       Datase EAP-MDS as Host Lookup       ()       Allow EAP-MDS         Image: Authentication       Image: Authentication       ()       Allow EAP-MDS       ()	cisco Identity Services Engine	ise-1 admin Logout Feedback
Dictionaries       Conditions       Results         Results       Allow MS-CHAPv1         Allow MS-CHAPv2       Allow KS-CHAPv2         Allow Access       Allow EAP-MD5 as Host Lookup         Advectation       Detect EAP-MD5 as Host Lookup         Allow EAP-MD5       Detect EAP-MD5 as Host Lookup         Advectation       Detect EAP-MD5 as Host Lookup         Allow EAP-MD5       Detect EAP-MD5 as Host Lookup         Allow EAP-MD5       Detect EAP-MD5 as Host Lookup         Allow EAP-MD5       Allow EAP-MD5         Allow EAP-MD5       Allow EAP-MD5         Allow EAP-MD5       Allow EAP-MD5         Allow EAP-MD5       Allow EAP-MD5         Allow EAP-MD5-CHAPv2       Y         Allow FAP-TIS       Allow Password Change Retries 1         Allow FAP-TIS       Y         Allow FAP-GTC	🛕 Home Operations 🔻 Policy 🔻 Av	rministration 🔻 😽 Task Navigator 👻 😢
Results       Allow MS-CHAPY1         Allow MS-CHAPY2       Allow KS-CHAPy2         Allow KAccess       Allow EAP-MD5 as Host Lookup         Allow KAccess       Allow EAP-MD5         Allow EAP-MD5       Detect EAP-MD5 as Host Lookup         Allow EAP-MD5       Allow EAP-MD5         Allow EAP-MD5       Allow EAP-MD5         Allow EAP-MS-CHAP/2       Y Allow EAP-MS-CHAP/2         Allow EAP-MS-CHAP/2       Y Allow Password Change Retries 1 (Valid Range 0 to 3)         Allow EAP-MS-CHAP/2       Y Allow EAP-MS-CHAP/2         Y Allow EAP-MS-CHAP/2       Y Allow FAP-MS-CHAP/2         Y Allow EAP-MS-CHAP/2       Y Allow Password Change Retries 1 (Valid Range 1 to 3)         Y Allow PAP-GTC       Y Allow Password Change Retries 3 (Valid Range 1 to 3)         Y Allow Password Change Retries 3 (Valid Range 1 to 3)       Y Ual W Password Change Retries 3 (Valid Range 1 to 3)	🛓 Authentication 💿 Authorization 🖉	Profiling 🖉 Posture 👼 Client Provisioning 🚔 Security Group Access 🚺 Policy Elements
New Protocols            • Adversification             • Proving             • Proving <td>Dictionaries Conditions Results</td> <td></td>	Dictionaries Conditions Results	
		Allow H3-CHAPv2 Allow EAP-MD5 Detect EAP-MD5 as Host Lookup Allow EAP-TL3 Allow EAP-TL3 Allow EAP-TL3 Allow EAP-M3-CHAPv2 Allow Password Change Retries 1 (Valid Range 0 to 3) Allow EAP-GTC Allow EAP-GTC Allow EAP-FAST EAP-FAST Inner Methods Allow EAP-M3-CHAPv2 Allow Password Change Retries 3 (Valid Range 1 to 3) Allow EAP-M3-CHAPv2 Allow EAP-M3-CHAPv2 Allow Password Change Retries 3 (Valid Range 1 to 3) Allow EAP-M3-CHAPv2 Allow EAP-M3-CHAPv3 Allow EAP-M3-CHAPv3 Allow EAP-M3-CHAPv3 Allow EAP-M3-CHAPv3 Allow EAP-M3-CHAPv3 Allow EAP-M3-CHAPv3 Allow EAP-M3-CHAPv3 Allow EAP-M3-CHAPv3 Allow EAP-M3 Allow EAP-M3
	🕗 Help	Alarms 🔕 0 🛕 0 🕦 2   🔒 Notifications (0)



Configuring Group Policy Objects

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

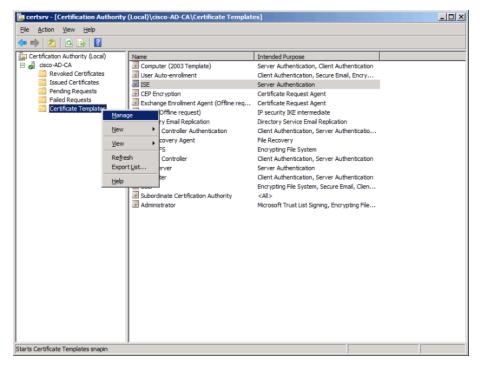
In this deployment, you will be using group policy objects (GPOs) to distribute certificates and to configure the native 802.1X supplicant for Windows XP and later endpoints that are members of the domain. Machine certificates are distributed when the machine joins the domain, and user certificates are deployed to the endpoint where the user logs in to the domain. The steps in this example deployment describe how to edit the Default Domain Policy so that it will apply to all users, but you could create a new policy object and apply it to a subset of users if you prefer.

#### Procedure 1 Create template for workstations

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

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

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



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

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

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

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

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

Properties of New Template
Issuance Requirements Superseded Templates Extensions Security General Request Handling Subject Name Server
Pumose: Signature and encryption
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:
<ul> <li>Microsoft Base Smart Card Crypto Provider</li> <li>Microsoft DH SChannel Cryptographic Provider</li> <li>✓ Microsoft Enhanced Cryptographic Provider v 1.0</li> <li>Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Provider</li> <li>Microsoft Enhanced RSA and AES Cryptographic Provider</li> <li>Microsoft RSA SChannel Cryptographic Provider</li> <li>Microsoft Strong Cryptographic Provider</li> </ul>
OK Cancel
(CSPs) should be used, click CSPs.
OK Cancel Apply Help

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

operties of N	lew Temp	late				
General Issuance Req		est Handling		ect Name s   Exten		Server Security
& Domain	icated User trator (Admir Admins (CI: Computers	s nistrator@cisco. SCO\Domain Ar (CISCO\Domair CISCO\Enterpri	dmins) n Compute			
Permissions fr Full Contro Read Write Enroll Autoenroll		Computers	Ad	Allow	Ren De	3
Advanced.		r advanced set	-	k	Advan	ced
	ОК	Cancel		Apply	1	Help

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.

🙀 certsrv - [Certification Authority	r (Local)\cisco-AD-CA]	
<u>File Action View H</u> elp		
🗢 🔿 🙍 📓 📓 👔		
Refresh Help	Name         Revoked Certificates         Pending Requests         Pailed Requests         Certificate Templates	
Enable additional Certificate Templates on	n this Certification Authority	

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

ormation about this template has	vas recently created does not appear on this list, you may need to wait until been replicated to all domain controllers. organization may not be available to your CA.	
r more information, see <u>Certificate</u>		
lame	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></all>	
Enrollment Agent	Certificate Request Agent	
Enrollment Agent (Computer)	Certificate Request Agent	
Exchange Signature Only	Secure Email	
Exchange User	Secure Email	A
		1

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

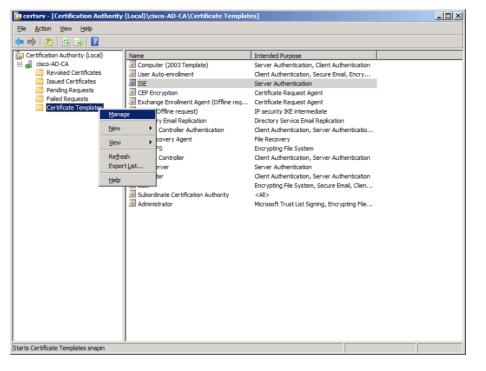
#### **Procedure 2**

**Create template for user auto-enrollment** 

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

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

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



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

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

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

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

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

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

roperties of New Template		
General Request Handling Issuance Requirements Superseded	Subject Nam	
Group or user names:	remplates   Ext	ensions Security
Authenticated Users Administrator (Administrator@cisco Domain Admins (CISCO\Domain A Domain Users (CISCO\Domain Us Enterprise Admins (CISCO\Enterprise	dmins) ers)	
Permissions for Domain Users	Add	Remove Deny
Full Control		
Read Write		
Enroll		H
Autoenroll		ā
For special permissions or advanced se Advanced.		Advanced
OK Cance	Apply	Help

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.

File     Action     View     Help       Image: State of the state of	Continuation Authority	(Local)) sicco AD (A) Contificato Tomplat		
Certification Authority (Local)       Name       Intended Purpose         Image: Server Authority (Local)       Image: Server Authority (Local)       Server Authority (Local)         Image: Server Authority (Local)       Image: Server Authority (Local)       Server Authority (Local)         Image: Server Authority (Local)       Image: Server Authority (Local)       Server Authority (Local)         Image: Server Authority (Local)       Image: Server Authority (Local)       Server Authority (Local)         Image: Server Authority       Image: Server Authority (Server Authority)       Image: Server Authority (Server Authority)         Image: Server Authority (Server Authority)       Image: Server Authority (Server Authority)       Server Authority (Server Authority)         Image: Server Authority (Server Authority)       Image: Server Authority (Server Authority)       Server Authority         Image: Server Authority       Image: Server Authority       Server Authority       Server Authority         Image: Server Authority       Image: Server Authority       Server Authority       Server Authority         Image: Server Authority       Image: Server Authority       Server Authority       Server Authority         Image: Server Authority       Server Authority       Server Authority       Server Authority         Image: Server Authority       Server Authority       Server Authority       Server Authority </th <th></th> <th>(Local) (CSCO-AD-CA (Certificate Templat</th> <th><u>c)</u></th> <th></th>		(Local) (CSCO-AD-CA (Certificate Templat	<u>c)</u>	
Image: Subscription       Computer (2003 Template)       Server Authentication, Client Authentication         Image: Subscription       Certificates       Server Authentication, Client Authentication         Image: Subscription       Certificate Request Agent       Image: Subscription         Image: Subscription       Directory Environment Agent (Offline request)       IP security INE Intermediate         Image: Subscription       Directory Environment Agent (Offline request)       IP security INE Intermediate         Image: Subscription       Directory Environment Authentication       Directory Service Enail Replication         Image: Subscription       Certificate Implate to Issue       File Recovery         Image: Subscription       Domain Controller       Client Authentication, Server Authentication         Image: Subscription       Subscription Authentication       Server Authentication         Image: Subscription       Subscription Authentication       Server Authentication         Image: Subscription       Subscription Authentication Authentication       Server Authentication         Image: Subscription       Subscription Authentication Authentication       Server Authentication         Image: Subscription       Subscription Authentication Authentication       Server Authentication         Image: Subscription       Subscription Authonity <ali></ali>	🗢 🔿 🖄 🙆 🗟			
	Certification Authority (Local) Certification Authority (Local) Certificates Certificates Pending Requests Certificate Certificate Manage New View Refresh Export List	Computer (2003 Template) Computer (2003 Template) Computer (2003 Template) Computer Agent (Offine req PSec (Offine request) Demain Controller Authentication Controller Authentication Computer User User User User User User User Us	Server Authentication, Client Authentication Certificate Request Agent Certificate Request Agent IP security IKE intermediate Directory Service Email Replication Client Authentication, Server Authenticatio File Recovery Encrypting File System Client Authentication, Server Authentication Server Authentication, Server Authentication Client Authentication, Server Authentication Encrypting File System, Secure Email, Clien <al></al>	

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

#### Enable Certificate Templates

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 <u>Certificate Template Concepts.</u> X

Name	Intended Purpose	<b></b>
Router (Offline request)	Client Authentication	
BA OCSP Response Signing	OCSP Signing	
風 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	
Reference Workstation Authentication	Client Authentication	
		<b>_</b>
<u>  •  </u>		
	ОК	Cancel

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

#### **Procedure 3**

**Configure GPOs for wired endpoints** 

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

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

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

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

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

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

📕 Group Policy Management Editor			
File Action View Help			
🗢 🔿 🗾 🖬 💁 🔽 🖬			
🖃 👰 Computer Configuration 📃	Name	Description	
Policies	The	ere are no items to show in this vi	PW.
Windows Settings     Mame Resolution Policy			
Scripts (Startup/Shutdown)			
Security Settings			
Account Policies			
T Local Policies			
🕀 📑 Event Log			
Restricted Groups			
🕀 📴 System Services			
🕀 📴 Registry			
🗉 📴 File System			
Wired Network Create A New Wired Network	Policy for Windows Vista and	Later Releases	
1 Windows Firev			
Network List M View		•	
Public Key Polic Refresh			
Software Rest Export List			
E Network Acces			
Application Co. Help			
IP Security Policies on Active Directory (CIS)			
Advanced Audit Policy Configuration			
🕀 🍌 Policy-based QoS			
🗉 🚞 Administrative Templates: Policy definitions (ADMX 🕮			
Preferences			
🖃 🕵 User Configuration			
▲ >			
			· ·

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

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

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

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

Step 10: Click Properties.

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

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

Step 13: Click OK to close the certificate properties window.

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

## Procedure 4

**Configure GPOs for wireless endpoints** 

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

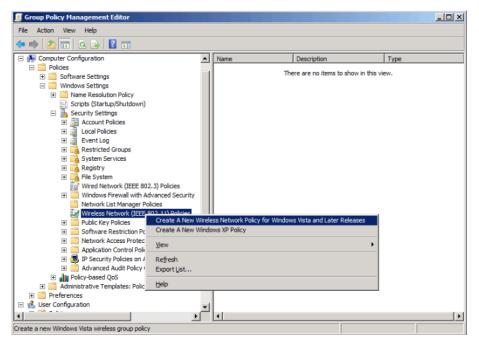
Step 1: On the CA console, navigate to Start > Administrative Tools > Group Policy Management.

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

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

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

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



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

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

P-TLS (Vista and lat	er) Properties		?
General Network Perm	nissions		
Settings defined in this machines	s policy will apply to	all wireless interface	es of dient
Policy Name: EAP-TLS (Vista and la	iter)		_
Description:			
8021.X EAP-TLS for	/ista and later		
Use Windows WLA Connect to available n			elow:
Infrastructure Ad Hoc Add Edit	, Remove	Import Expo	₽ 
	ОК	Cancel	Apply

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

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

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

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

WLAN-Data (EAP-TLS) properties	×
Connection Security	
Select the security methods for this network	
Authentication: WPA2-Enterprise	
Encryption: AES	
Select a network authentication method:	
Microsoft: Smart Card or other certificate   Properties	
Authentication Mode:	
User or Computer authentication	
Max Authentication Failures:	
Cache user information for subsequent connections to this network	
Advanced	
OK Cancel	

Step 12: Click Properties.

Step 13: Make sure Use a certificate on this computer is selected, and then make sure Use simple certificate selection and Validate server certificate are selected.

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

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

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

Next, you create a policy for Windows XP clients.

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

Group Policy Management Editor				
File Action View Help				
⊨ 🔿 🖄 📰 🖻 🗟 🖬				
E Computer Configuration	Name	Description	Туре	[
🖃 🧰 Policies	EAP-TLS (Vista and la	8021.X EAP-TLS for Vista an	Vista and Later Releases	
Software Settings				
🖃 🧮 Windows Settings				
Image: Second Seco				
Scripts (Startup/Shutdown)				
🖃 🚋 Security Settings				
🗉 📑 Account Policies				
1 🚡 Local Policies				
Event Log				
Restricted Groups				
E System Services				
Registry				
File System				
Wired Network (IEEE 802.3) Policie				
Windows Firewall with Advanced S				
Network List Manager Policies				
Wireless Network (TEEE 802-11) Pr	l .			
Create A New Windows XP Policy				
t t ⊻iew ↓				
🗉 🧧 Refresh				
± 🛃 Export List				
H =	-			
🛨 📊 P Help				
E Administrative Templates: Policy definitions	T			
Preferences				
🛃 User Configuration 🔤				
eate a new Windows XP wireless group policy				

**Step 18:** On the General tab, give the policy a name and description, and then make sure **Use Windows WLAN AutoConfig service for clients** is selected.

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

AP-TLS (XP) Properties	? ×
General Preferred Networks	
XP Policy Name:	
EAP-TLS (XP)	
Description:	
802.1X EAP-TLS profile for XP	
	-1
Networks to access:	
Any available network (access point preferred)	•
Vise Windows WLAN AutoConfig service for clients	
Automatically connect to non-preferred networks	
OK Cancel Ap;	oly

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

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

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

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

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

ew Preferred Setting Properties
Network Properties IEEE 802.1X
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: Held Period (seconds):
3 1
Start Period (seconds): Auth Period (seconds):
5 18
· · · · · · · · · · · · · · · · · · ·
OK Cancel Apply

Step 25: Click Settings.

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

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

nart Card or other Certificate Properties	2
When connecting:	
C Use my smart card	
Use a certificate on this computer	
Use simple certificate selection (Recommended)	
Validate server certificate	
Connect to these servers:	_
J 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	•
View Certificate	1
Do not prompt user to authorize new servers or trusted certificat	ion
Use a different user name for the connection	
OK Cano	el

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

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

At this point, all endpoints running Windows XP SP3 and later will have a 802.1X supplicant configuration pushed to them the next time they log in to the domain or after the GPO policy is refreshed.

#### Process

Deploying Cisco AnyConnect on Windows Endpoints

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

Cisco AnyConnect Secure Mobility Client 3.0 can be used as an 802.1X supplicant on Windows endpoints, using the Network Access Manager module. In this example deployment, the Network Access Manager is configured with both wired and wireless profiles using digital certificates.

#### Procedure 1 Install Cisco AnyConnect

To use Cisco AnyConnect Secure Mobility Client 3.0 as your 802.1X supplicant on Windows endpoints, you need to download the latest version from Cisco.com along with the Profile Editor. The client is distributed as an ISO image and will need to either be burned to a disk or mounted as a disk image by using a utility that provides this function. You need to be logged in as an administrator to install AnyConnect Secure Mobility Client.

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

http://www.cisco.com/cisco/software/release.html?mdfid=283000185&flow id=17001&softwareid=282364313&release=3.0.08057&relind=AVAILABLE&r ellifecycle=&reltype=latest

#### Tech Tip

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

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

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

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

Select the AnyConnect 3.0.08057 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
Install Selected

**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.



Install Profile Editor

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

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

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

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

Step 4: Click Typical, and then click Install.

Step 5: Click Finish. The installation completes.

Procedure 3

Create wired profile

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

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

Step 3: Click Networks.

ss Manager , Networks cy ation Policy Profile:ili	ty Client\Network Acces	s Manager\system\c	onfiguration.xml	
Proups Network				
Name	Media Type	Group*		
wired	Wired	Global	Add	
			Edit	
			Delete	
* A network in	group 'Global' is a member of all gro	oups.		

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

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

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

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

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

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

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

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

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

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

ky cation Policy Profile:ility Client\Network Ac	ccess Manager\system\configuration.xml	
User Identity		Media Type
Groups Unprotected Identity Pattern:	[username]@[domain]	Security Level
		Connection Type
		Machine Auth
		Credentials
User Credentials		User Auth
Use Single Sign On Credentials		Credentials
Prompt for Credentials		
Remember Forever		
Remember while User is L	logged On	
Never Remember		
Certificate Sources	Remember Smart Card Pin	
<ul> <li>Smart Card or OS certificates</li> </ul>	Remember Forever	
	Remember while User is Logged On	
Smart Card certificates only	-	
	<ul> <li>Never Remember</li> </ul>	
•	III	

#### Procedure 4 Create wireless profile

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

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

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

ess Manager , Networks licy Profile:ility Clie	ent\Network Access Manager\system\configuration.xml	
5	Wireless-TLS	Media Type
Groups Name: Group Membership		Security Level
In group:	(auto-generated)	
	N.L.D.	
In all groups (G		
Choose Your Network	Media	
Wired (802.3) I	Network	
Select a wired r	network if the endstations will be connecting to the network with a traditional	
ethernet cable.		
Wi-Fi (wireless)	) Network	
Select a WiFi ne	etwork if the endstations will be connecting to the network via a wireless	
radio connectio	on to an Access Point.	
SSID (max 32 c	thars): WLAN-Data	
	Hidden Network	
Association Tim	eout (sec) 5	
Common Settings		
Script or application o	on each user's machine to run when connected.	
	Browse Local Machine	
Connection Timeout (	(sec.) 40	
1		
•		

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

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

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

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

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

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

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

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

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

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

#### Process

Configuring Mac Workstations for 802.1X Authentication

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

If you have Apple Mac endpoints, you have to manually obtain a certificate and configure 802.1X authentication. The example deployment shows how you would do this for Mac OS X 10.6.

#### Procedure 1

Install root certificate on Mac OS X

To install a trusted root certificate on Mac OS X 10.6, you need to manually request the certificate from the CA and install the certificate in the keychain.

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

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

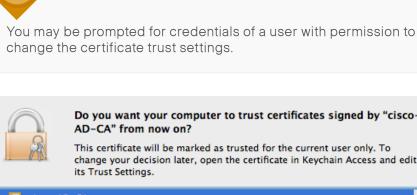
Step 3: Make sure the current certificate is selected and the DER encoding method is selected.

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

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

#### Step 6: Click Always Trust.

**Tech Tip** 



#### 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-Al	D-CA	
Certificate Generation Details	cisco-AD-CA Root certificate authority Expires: Tuesday, October 1 This root certificate is not	
	Hide Certificate	Don't Trust Always Trust



0

**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.

;	Keychain Access File Edit	View Window Help
	About Keychain Access	Keychain Access
I	Preferences ೫,	٩
	Keychain First Aid て第A	
P	Certificate Assistant	Open
	Ticket Viewer て第K	Create a Certificate
	Services	Create a Certificate Authority Create a Certificate For Someone Else as a Certificate Authority
l	Hide Keychain Access #H	Request a Certificate From a Certificate Authority
l	Hide Others \\#H	Set the default Certificate Authority
	Show All	Evaluate a Certificate
	Quit Keychain Access #Q	

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

0	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			
B	Common Name: Taylor Smith			
Oera	CA Email Address:			
	Request is: O Emailed to the CA			
	• Saved to disk			
	Let me specify key pair information			
	Continue			

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

Step 4: Click Done.

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

**Step 6:** Authenticate to the CA as the user for which you wish to obtain a certificate.



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

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

Step 8: Click advanced certificate request.

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

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

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

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

#### Microsoft Active Directory Certificate Services -- cisco-AD-C

#### 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:	
	rmGBqRlR4XgBimH2wZiM611DiqAqXy1VMk5IJ3ov
Base-64-encoded	okaRmWiE6Mpqrb0olA3Z9mWFHf+QsanrhwwmsxDL
	1FV49197X0PzpKiBkkOsUdOtMOrEE0ilstEjD0Qn
(CMC or	H2vnd0QdsuLYq+meqQC3/Qqw3eyn4bIYEQp5GpsT
PKCS #10 or	6eCoSzqxNBDQqzAjcJoGE9sdBn9rE293HNQFzFue *
PKCS #7):	A P
O	
Certificate Templ	
	User 🗘
Additional Attribution	utes:
Attributes:	
	Cubally
	(Submit >)

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

**Step 14:** In Finder, locate the saved certificate, and then double-click it. The Keychain Access utility imports the certificate.

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

$\Theta \cap \cap$	Add Certificates
Certificate	Do you want to add the certificate(s) from the file "certnew.cer" to a keychain?
	Keychain: login 🗘
View Cer	tificates Cancel Add

#### Procedure 3

**Configure Mac OS X supplicant** 

Step 1: On your Mac, launch System Preferences.

- Step 2: Double-click Network.
- Step 3: Click Advanced, and then click the 802.1X tab.
- Step 4: Click the + symbol, and then select Add User Profile.

Show All	Q
🛜 AirPort	
AirPort TCP/IP DNS WINS 802.1X Proxies	Ethernet
Status Connected	Turn Annon On
User Name:	
Password:	
Authentication: Enable Protocol	
EAP-F/	AST
Configure	
Configu	ure Trust
Wireless Network:	•
+ - Security Type: WPA2 Enterpr	rise 🗘
Add User Profile Add Login Window Profile Add System Profile	Cancel OK

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

- Step 6: In the Authentication section, select TLS, and then click Configure.
- Step 7: Select the certificate for this user, and then click Continue.

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

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

AirPort TCP/IP	DNS WINS 802.1	X Proxies Ethernet
User Profiles		
🗹 WLAN-Data	User Name:	taylorsmith
	Password:	•••••
	C	Always prompt for password
	Authentication:	Enable Protocol
		□ PEAP ✓ TLS
		EAP-FAST
		Configure
	(	Configure Trust
	Wireless Network:	WLAN-Data
_	Security Type:	WPA2 Enterprise

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

Repeat this process for all Mac OS X endpoints to deploy certificates and to enable 802.1X authentication. On the wireless network, any device that doesn't have a certificate uses PEAP to gain access to the network. Monitor mode is running on the wired network, so endpoints that aren't configured for 802.1X still get access by using MAC Authentication Bypass (MAB).

## **Enable Authorization**

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

The next step would be to deploy some form of authorization to control what authenticated endpoints can access the network. This next phase is called *low-impact mode*. In low-impact mode, endpoints are authenticated with either 802.1X or MAB. MAB is used for devices that require network access but either don't support 802.1X or don't have 802.1X configured. In this example, we are using MAB to authenticate IP phones and wireless access points that we will identify with device profiling. Any other device will have to successfully authenticate with 802.1X, or it will not have access to the network. After authentication, the endpoint is given full access to the services necessary for authentication.

### Process

Enabling Authorization for Cisco IP Phones

1. Enable Cisco IP Phone policy

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

#### Procedure 1

Enable Cisco IP Phone policy

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

Step 2: From the Policy menu, select Authorization.

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

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

Step 5: Click Done, and then click Save.

#### Process

Enabling Authorization for Wireless Access Points

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

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

#### **Procedure 1**

**Create an identity group** 

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

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

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

cisco Identity Services Engine	ise-1 admin Logout Feedback
💧 Home Operations 🔻 Policy 🔻 Adm	nistration 🔹 😐 Task Navigator 👻 🕗
🛃 Authentication 🛛 👩 Authorization 🗌	Profiling 🕜 Pasture 👩 Client Provisioning 📄 Security Group Access 🔥 Policy Elements
Profiling	Profiler Policy       * Name       Cisco-Access-Point       Description       Policy for all Cisco Access Points         Policy Enabled       V      if         * 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         Parent Policy       Gisco-Access-PointFluie1Check1       Then         If Condition       Cisco-Access-PointRule3Check3       Then         If       Condition       Cisco-Access-PointRule3Check3       Then         Store       Reset       •       •

#### Procedure 2 Create authorization profile

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

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

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

Step 3: Click Add.

Step 4: Name the profile Cisco\_APs and give a description.

**Step 5:** Select **DACL Name** and in the list, make sure **PERMIT\_ALL\_ TRAFFIC** is selected, and then click **Submit**.

🛃 Authentication 🧑 Authorization 🧭 Profiling 🕐 Posture 🕞 Client Provisioning 😁 Security Group Access 🚮 Policy Elements		ise-1 admin Logout Feet	_
Dictionanes contactors Resoluts		Proming M Posture M client Provisioning M Security Group Access	
Results     Authorization Profile     * Name        * Name	Results	Authorization Profile  *Name Gsco_APS Description Profile For Osco Access Points *Access Type Courses Accept Common Tasks C DACL Name PERMIT_ALL_TRAFFIC VLAN Voice Domain Permission Web Authentication Auto Smart Port Fiter-ID  Advanced Attributes Settings Select an item  Access Type - ACCESS_ACCEPT DACL = PERMIT_ALL_TRAFFIC: Submit Cancel	×

Procedure 3

#### **Create authorization policy**

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

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

	sco Id	lentity Services Engine					ise-1 admi	n Logout Feedbi
â	Home	Operations 🔻 Policy 🔻 .	Administration 🔻				👓 Task	Navigator 🛛 🕗
4	Authenti	cation 🧕 Authorization	🔀 Profiling 💽 Posture 🗔	Client Provisioning	🚊 Security Group Access	🐥 Pi	olicy Elements	
	orizatior							
əfine	e the Auth	orization Policy by configuring rul	es based on identity groups and/or oth	er conditions. Drag an	id drop rules to change the orde	r.		
irst I	Matched R	ule Applies 🔹						
• Ex	ceptions (	0)						
CH.	andard							
00								
	Status	Rule Name	Conditions (identity gro	ups and other conditir	ons)	Pe	ermissions	
		Black List Default	If Blacklist			then <b>B</b>	lacklist_Access	Edit   🕶
		Profiled Cisco IP Phones	if Cisco-IP-Phone			then <b>G</b>	isco_IP_Phones	Edit   🕶
		Default	if no matches, then Pern	nitAccess			Insert New	Rule Above
	-							
Sa	_	set						

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

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

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

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

💧 Home Operations 🔻 Policy 🔻 Administration			ise-1 ad	sk Navigator 👻 🕗
Authentication Authorization Profing	🖉 Posture 🔒 Client Provisio	Profiled	Policy Elements	sk havigator •
Authorization Policy Define the Authorization Policy by configuring rules based on ider First Matched Rule Applies *	ntity groups and/or other conditions. (	Android     Apple-Pad     Gsco-Access-Point		
Exceptions (0) Standard		Cisco-IP-Phone Workstation	-	
	Conditions (identity groups and other Blacklist		Permissions an Blacklist Access	Edit   🗸
	Cisco-IP-Phone		n Cisco_IP_Phones	Edit   🕶
🖋 🗹 🔹 Profied Cisco APs if	Any Condition(s		then AuthZ Profil	4) Done
Default if r     Save Reset	Any	<b>)</b> = ÷		Edit   •

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

Step 8: In the list, next to Standard, click the > symbol, and then choose Cisco\_APs.

🛕 Home Operations 🔹 Policy 🔹 Administration 🔹 🤨 Task Navigator 🌏
👢 Authentication 💽 Authorization 🔀 Profiling 🦻 Posture 👦 Client Provisioning 🚍 Security Gro
Authorization Policy 🔶 🐨 📳 🌚
Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to chan 🤬 Bladdist_Access
First Matched Rule Applies
Cisco_IP_Phones
Exceptions (0)     Q DenyAccess
Standard Q PermitAccess
Status Rule Name Conditions (identity groups and other conditions)
Black List Default if Blacklist
Profiled Cisco IP Phones If Cisco-IP-Phone Edit   🕶
Profiled Cisco APs if Cisco 4 and Condition(s)
Default if no matches, then PermitAcces
Select an item 📀 — 🜵
Save Reset

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

11) C19	 sco Id	lentity Services Engine				ise-1 admi	n Logout Feedback
â	Home	Operations 🔻 Policy 🔻	Administration 🔻			👓 Task	Navigator 🔫 🕙
4	Authenti	ication 💽 Authorization	🛃 Profiling 🛛 💽 Posture	🗔 Client Provisioning	📃 Security Group Access	🐥 Policy Elements	
Define		•	ules based on identity groups and/	or other conditions. Drag ar	nd drop rules to change the order.		
► Ex	ceptions (						
St	andard						
	Status	Rule Name	Conditions (identi	ty groups and other condit	ons)	Permissions	
		Black List Default	if Blacklist		the	n Blacklist_Access	Edit   👻
		Profiled Cisco IP Phones	if Cisco-IP-Phone		the	n Cisco_IP_Phones	Edit   🕶
	<b>V</b>	Profiled Cisco APs	if Cisco-Access-Po	bint	the	en Cisco_APs	Edit   👻
		Default	if no matches, then	PermitAccess			Edit   🕶
Sa	ve Re	eset					

#### Process

Modifying the MAB Authentication Policy

1. Modify MAB authentication rule

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

#### **Procedure 1**

Modify MAB authentication rule

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

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

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

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

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

India CISCO 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 sour Policy Type O Simple O Rule-Based	ces that it should use for authentication.
MAB : If Wired_MAB 🔶 allow protocols Allowed Protocol : Default Netwoo and	··· • Actions •
Default : use Internal Endpoints Udentity Source Internal Endpoints Options If authentication failed Rogect •	🖗 Actions 💌
Wired-Dot1X : If Wired If user not found Reject * If process failed Drop *	👾 Actions 🔻
Wireless-Dot1X     If Wirele     Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS MSCHAP     ti is not possible to continue processing when authentication fails or user is not f	Actions *
Default Rule (If no match) : allow proto	🖗 Actions 👻

#### Process

Enabling Authorization for Wired Endpoints

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

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

#### Procedure 1

#### **Create authorization profile**

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

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

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

Step 3: Click Add.

Step 4: Name the profile Wired\_Dot1X and give a description.

Step 5: Select DACL Name and in the list, make sure PERMIT\_ALL\_ TRAFFIC is selected, and then click Submit.

Authentication Authonization * Policy * Administration * * * * * * * * * * * * * * * * * * *	cisco Identity Services Engine	ise-1 admin Logout Feedba
Dectonates       Conditions         Results       Authorization Profile         *       Authorization Profile         *       Authorization Profile         *       Authorization Profile For Wred Endpoints That Have Authenvicated With 602.1X         *       Authorization Profile         *       Authorization         *       Common Tasks         *       Common Tasks         *       VuaN         Voice Domain Permission         *       Auto Smart Port         *       Filter-ID         *       Advanced Attributes Settings         Select an item       *         Actions Concel       Autore Control         *       Attributes Details         Access Type = ACCESS_ACCEPT	🛕 Home Operations 🔻 Policy 🔻 Admini	istration 🔻 😶 Task Navigator 👻 📀
Results <ul> <li>Authorization Profile</li> <li>Authorization Profile</li> <li>Name</li> <li>Description</li> <li>Profile For Wred Endpoints That Have Authenxticated With 802.1X</li> <li>Authorization Profiles</li> <li>Common Tasks</li> <li>Common Tasks</li> <li>Collext Provisioning</li> <li>Vulaw</li> <li>Vulaw</li></ul>	🛃 Authentication 🛛 👩 Authorization 🔀	Profiling 🛛 👰 Posture 👦 Client Provisioning 🔄 Security Group Access 🔒 Policy Elements
Results            • Authorization Profile         • Name         • Vired_Dot1X         Description         • Authorization Profile         • Name         Vired_Dot1X         Description         • Authorization Profile         • Access Type         Access Type         Access Type         Access Type         Access Type         Access Type         Access         • Common Tasks         • Common Tasks         • Collent Provisioning         • Security Group Access         • VuN         • Voice Domain Permission         • Web Authentication         Auto Smart Port         • Fite=:D         • Advanced Attributes Settings         [Select an Item         • - +         • Attributes Details         Access Type - ACCESS_ACCEPT	Dictionaries Conditions Results	
🕙 Help 🛛 🕹 Notifications (0)	Authentication  Authonization Profiles  Downloadable ACLs  Downloadable ACLs  Profiling  Profiling  Profiling  Caller Posture Node Profiles  Security Group Access	Authorization Profile  *Name Wred_Dot1X Description Profile For Wred Endpoints That Have Authenticated With 802.1X *Access Type Access Accept  Common Tasks  C Common Tasks  Description Permission  C Common Tasks  Description Permission  V VAN  Voice Domain Permission  Web Authentication  Web Authentication  Auto Smart Port  Fitter-ID  Advanced Attributes Settings  Defect an item  -  -  Attributes Details  Access Type + ACCESS_ACCEPT
	🕗 Help	Alarms 👩 1702 🛕 341 🌀 6   🚑 Notifications (0)

#### Procedure 2

**Create authorization policy** 

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

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

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

🏠 Home	Operations 🔻 Policy 🔻 Admin					Fask Navigator 🔫 🕗
ዿ Authen	tication 💽 Authorization 🔀	Profiling 🛛 💽 Posture	🔂 Client Provisioning	🚊 Security Group Access 📩	Policy Elements	
uthorizatio		1 11 10 11				
	horization Policy by configuring rules bas	sed on identity groups and,	for other conditions. Drag an	d drop rules to change the order.		
irst Matched	Rule Applies 👻					
Exceptions	(0)					
Standard						
Status	Rule Name	Conditions (ident	ity groups and other conditi	ons)	Permissions	
	Black List Default	if Blacklist		ther	Blacklist_Access	Edit   🕶
	Profiled Cisco IP Phones	if Cisco-IP-Phone	•	ther	Gisco_IP_Phones	Edit   🗸
	Profiled Cisco APs	if Cisco-Access-P	oint	ther	Cisco_APs	Edit   🕶
	Default		PermitAccess		Incort A	lew Rule Above
					Inserun	Iew Rule Above

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

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

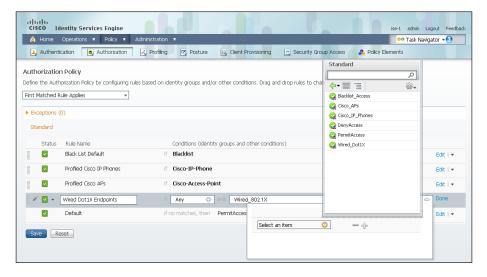
Step 5: Click Select Existing Condition from Library.

Step 6: In the list, next to Compound Conditions, click the > symbol, and then choose Wired\_802.1X.

🙆 Home Operations 🔻	Policy  Administration		_	👓 Task Nav	vigator 🔫 😢
🛓 Authentication 🛛 💿 A	ithorization 🔀 Profiling 💽 Posture	灵 Client Provisioning 🛛 📄 Security Group A	ccess 🥑	Policy Elements	
uthorization Policy afine the Authorization Policy b Irst Matched Rule Applies	Compound Conditions	other conditions. Drag and drop rules to change	the order.		
Exceptions (0) Standard	Wired_802.1X Wired_MAB Wirels_802.1X				
Status Rule Name	Catalyst_Switch_Local_Web_Authentica	groups and other conditions)	then	Permissions Blacklist_Access	Edit   •
Profiled Cisco II	hone		then	Cisco_IP_Phones	Edit   🕶
Profiled Cisco A	ss-Point		then	Cisco_APs	Edit   🕶
Wired Dot1X En	ф. 	d Condition(s)	-	then AuthZ Profil	수 Done
Saw Select Condition			-		Edit   🕶

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

Step 8: In the list, next to Standard, click the > symbol, and then choose Wired\_Dot1X.



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

	.1 1. 5 <b>CO</b> Id	entity Services Engine					ise-1	admin Logout	Feedback
â	Home	Operations 🔻 Policy 🔻	Administration	•			00	Task Navigator 👻	0
4	Authenti	cation 🧕 Authorization	🛃 Profiling	💽 Posture	🛃 Client Provisioning	🔄 Security Group Access	🚯 Policy Elements		
Auth	orization	1 Policy							
			ules based on ide	entity groups and/o	or other conditions. Drag an	d drop rules to change the order.			
		ule Applies 🔹							
mrst	Maluned K	ue applies 🔹							
► Ex	ceptions (	0)							
St	andard								
	Status	Rule Name		Conditions (identit	ty groups and other condition	ons)	Permissions		
	<ul> <li></li> </ul>	Black List Default	if	Blacklist		th	n Blacklist_Access	Edit	<b>v</b>
		Profiled Cisco IP Phones	if	Cisco-IP-Phone		th	en Cisco_IP_Phone	s Edit	•
1		Profiled Cisco APs	if	Cisco-Access-Po	bint	th	an <b>Cisco_APs</b>	Edit	•
1	<ul> <li>Image: A set of the set of the</li></ul>	Wired Dot1X Endpoints	if	Wired_802.1X		th	an Wired_Dot1X	Edit	<b>-</b>
		Default	if r	no matches, then	PermitAccess			Edit	-
Sa	ve Re	set							

#### **Procedure 3**

**Enable low-impact mode** 

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

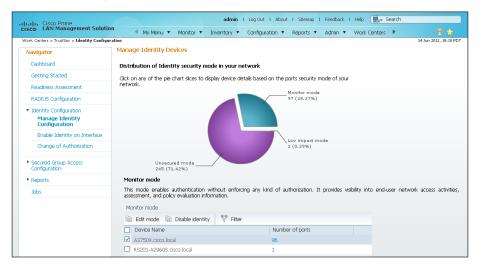
**Step 1:** Connect to Cisco Prime LMS with a web browser, for example: https://lms.cisco.local.

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

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

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

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



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

sco LAN Management Solutio	My Menu Y Monitor Y Inve	ntory 🔻 🤇	Ionfiguration 🔻	Reports 🔻 Admin	<ul> <li>Work Centers</li> </ul>	물 🚖
ork Centers » TrustSec » Identity Configura	, , ,					14 Jun 2012, 10:18 F
Navigator	Manage Identity Devices					
Dashboard	Review port selection on selected device	ces(optiona	l)			
Getting Started						
Readiness Assessment	View the ports and unselect the ports that	: you wish to	exclude.			
RADIUS Configuration	Selected Devices	Ass	ociated Ports			
<ul> <li>Identity Configuration</li> </ul>	Display Name	<b>V</b>	Port Name	Description		
Manage Identity Configuration	<ul> <li>A3750X.cisco.local</li> </ul>	✓	Gi3/0/18	Gi3/0/18		-
Enable Identity on Interface		✓	Gi3/0/19	Gi3/0/19		_
Change of Authorization			Gi3/0/16	Gi3/0/16		
		_	Gi2/0/22	Gi2/0/22		
Secured Group Access		_	Gi3/0/17	Gi3/0/17		
Configuration		$\checkmark$	Gi2/0/23	Gi2/0/23		
Reports			Gi3/0/14	Gi3/0/14		
Jobs		✓	Gi2/0/20	Gi2/0/20		
5555		✓	Gi3/0/15	Gi3/0/15		
			GI2/0/21	GI2/0/21		•

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

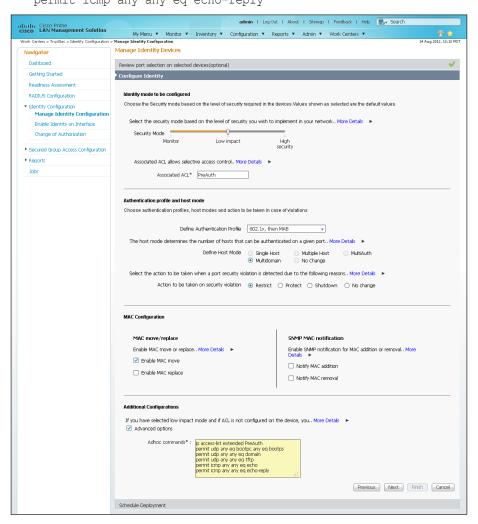
**Step 8:** In the Authentication profile and host mode section, set the following values:

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

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

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

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



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



switch by clicking **Preview CLI**.

ulu ulu - Cisco Prime	admin I Log Out I About I Sitemap I Feedback I Help  🔜 v Search	
(1.1.1), Cisco Prime CISCO LAN Management Solution	My Menu V Monitor Inventory Configuration Reports Admin Viork Centers	
Work Centers > TrustSec > Identity Configurati	ion > Manage Identity Configuration	14 Jun 2012, 12:18 PD
Navigator	Manage Identity Devices	
Dashboard	Review port selection on selected devices(optional)	Ś
Getting Started	Configure Identity	<b>V</b>
Readness Assessment	Schedule Deployment	
RADIUS Configuration		
<ul> <li>Identity Configuration</li> <li>Manage Identity</li> <li>Configuration</li> </ul>	Scheduler * Ind  Immediate Job Description* A3750X Authenticated Mode	icates required field
Enable Identity on Interface	Once	
Change of Authorization	O Dally Ennial	
<ul> <li>Secured Group Access Configuration</li> </ul>	Job Options	
Reports	Fail on mismatch of config versions  Fail on mi	
Jobs	Sync archive before job execution	
	Copy running config to startup Login Password	
	Falure policy Ignore failure and continue	
	Preview CLI Previous Next	Finish Cancel

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

ip access-list extended PreAuth
permit udp any eq bootpc any eq bootps
permit udp any any eq domain
permit udp any any eq tftp
permit icmp any any eq echo
permit icmp any any eq echo-reply
deny ip any any log
The interface commands added at the completion of this procedure are as
follows.

#### interface [interface]

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

#### Procedure 4

#### **Enable change of authorization**

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

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

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

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

					ad	min I	Log Out I About	I Sitemap	Feedback	I Help	∎• S	earch		
cisco LAN Management Solution	•	< r	My Menu 🔻	Monitor	<ul> <li>Inventor</li> </ul>	у 🔻	Configuration 🔻	Reports 🔻	Admin 🔻	Work (	Centers	•		
Work Centers > TrustSec > Identity Configuration	on > Chanç	je of	Authorization									2	1 Jun 2012	2, 14:08 PDT
Navigator	Deploy	1												
Dashboard												⊕Trust	Sec Con	figuration
Getting Started	> Choo	se T	emplates											
Readness Assessment	Selec	t ter	mplates to de	nlov confi	ouration									
RADIUS Configuration														
<ul> <li>Identity Configuration</li> </ul>	Terr	plat	e Selector						_		Selec		-	
Manage Identity Configuration									Show A	1		•	8	
Enable Identity on Interface			Template Nar	ne 👻	Features	Type	Role In	Category		C	reated	Scope		
Change of Authorization	✓	•	Identity - Cha	inge	Authorizati	Partia	Access	RADIUS c	lient configur	ati S	ystem	Device		
<ul> <li>Secured Group Access Configuration</li> </ul>														
▶ Reports														
Jobs														

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

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

ujuju Cisco Prime	admin I Log Out I About I Sitemap I Feedback I Help 🕞 Search	٥,
cisco LAN Management Solution	🔨 My Menu 🔻 Monitor 🔻 Inventory 🔻 Configuration 🔻 Reports 🔻 Admin 🔻 Work Centers 🕨 🛛 📅 🚖	
Work Centers > TrustSec > Identity Configuration	In > Change of Authorization 21 Jun 2012, 14:15 P	эт
Navigator	Deploy	
Dashboard	+ TrustSec Configuration	n
Getting Started	Choose Templates	
Readiness Assessment	Choose Device Groups	
RADIUS Configuration	Configure Identity - Change of Authorization	
<ul> <li>Identity Configuration Manage Identity Configuration</li> </ul>	Identity Commands 🎯	
Enable Identity on Interface	RADIUS clent IP address or Host name * 10.4.48.41	
Change of Authorization	Type of authorization the device uses for RADIUS clients *	
	RADIUS Key shared between the device and RADIUS clients *	
<ul> <li>Secured Group Access Configuration</li> </ul>	Port on which the device listens for RADIUS requests [0 - 65535] * 1,700	
▶ Reports	Previous Next Finish Cancel	
Jobs		
	Adhoc Configuration Commands for Selected Devices	
	Schedule Deployment	

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

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

رابیاب Cisco Prime Cisco LAN Management Solutior	admin I Log Out I About I Sitemap I Feedback I Help 🔜 Search	
	My Menu 🔻 Monitor 🔹 Inventory 👻 Configuration 👻 Reports 👻 Admin 👻 Work Centers 🕨 👘	
Work Centers > TrustSec > Identity Configuration		15 PDT
Navigator	Deploy	
Dashboard	⊕TrustSec Configur	ration
Getting Started		<b>V</b>
Readiness Assessment	Choose Device Groups	<b>V</b>
RADIUS Configuration	Configure Identity - Change of Authorization	<b>V</b>
<ul> <li>Identity Configuration</li> </ul>	Adhoc Configuration Commands for Selected Devices	<b>V</b>
Manage Identity Configuration	Schedule Deployment	
Enable Identity on Interface		
Change of Authorization	Scheduler * Indicates required field	
Secured Group Access Configuration     Reports     Jobs	Immediate         Job Description*         A3750X CoA Config           O Once         Daily         E-mail           Weakly         Monthly	
	Job Options         Copy Startup to Running Config upon falure         Copy Running Config to Startup         Brable Job Password         Login Vassword         Enable Password         Enable Password         Preview CLI       Previous       Next       Enable       Cance	əl

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

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

aaa server radius dynamic-author

```
client 10.4.48.41 server-key [key]
client 10.4.48.42 server-key [key]
auth-type any
```

#### Process

Enabling Authorization for Wireless Endpoints

- 1. Create authorization profile
- 2. Create authorization policy

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

#### **Procedure 1**

#### **Create authorization profile**

An authorization profile defines the specific access policies granted to the device. You will create a policy for wireless endpoints to permit full access. By default, a client is given full access when joining the wireless network, so you will not need to define an access list at this point.

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

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

Step 3: Click Add.

Step 4: Name the profile Wireless\_Dot1X and give a description.

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

Identity Services Engine     Adm     Home Operations      Policy      Adm	ise-1 adnin Logout Fee	_
🛃 Authentication 💿 Authorization 🔀	Profiling 💿 Posture 🗔 Client Provisioning 📄 Security Group Access 🚺 Policy Elements	
Dictionaries Conditions Results		
Results         Image: Constraint of the state of th	Access Type Access Accept     Common Tasks     OACL Name     VLAN     Voice Domain Permission     Web Authentication     Auto Smart Port     Filter-ID     Advanced Attr butes Settings     [[Select an item ]] =     Advanced Attr butes Settings     [[Select an item ]] =     Attr butes Details     Access Type = ACCESS_ACCEPT    ;     Sumit;	
🕙 Help	Alarms 👩 1702 🔬 355 🍈 6 🕴 🚑 Notifications (0	))

#### Procedure 2

#### **Create authorization policy**

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

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

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

	Home	Operations 🔻 Policy 🔻 Admi	histration 🔻			👓 Task I	Navigator + 🕗
4	Authenti	ication 🧕 Authorization 🔀	Profiling 💽 Posture	🛃 Client Provisioning	📃 Security Group Access 💋 🕹	Policy Elements	
uth	orizatio	n Policy					
		norization Policy by configuring rules ba	sed on identity arouns and	f/or other conditions. Drag an	d dron rules to change the order		
			sea ornaenacy groups and	a) or other contactors, brag an	a arop raies to change the order.		
rst I	Aatched R	tule Applies 🔻					
• Ex	eptions (						
Sta	indard						
	Status	Rule Name	Conditions (iden	ntity groups and other condition	ons)	Permissions	
		Black List Default	if Blacklist		then	Blacklist_Access	Edit   🕶
	~	Profiled Cisco IP Phones	if Cisco-IP-Phon	e	then	Cisco_IP_Phones	Edit   👻
	<b>V</b>	Profiled Cisco APs	if Cisco-Access-F	Point	then	Cisco_APs	Edit   👻
	_		if Wired 802.1X		then	Wired_Dot1X	Edit   🗸
		Wired Dot1X Endpoints	in Miled_002111				

Step 3: Rename the rule Wireless Dot1X Endpoints.

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

Step 5: Click Select Existing Condition from Library.

Step 6: In the list, next to Compound Conditions, click the > symbol, and then choose Wireless\_802.1X.

		ased of hidenaty groups and of o	ther conditions. Drag and drop rules to change t Compound Conditions		
First Matched	I Rule Applies 👻				
Exceptions	; (0)		<b>∲-</b> ■ 18		
Standard			Wired_802.1X		
			Wired_MAB		
Status		Conditions (identity g		Permissions	
	Black List Default	if Blacklist	Wireless_MAB	then Blacklist_Access	Edit   •
	Profiled Gsco IP Phones	if Cisco-IP-Phone	Catalyst_Switch_Local_Web_Authentica WLC_Web_Authentication	then Gsco_IP_Phones	Edit
	Profiled Cisco APs	If Cisco-Access-Point		then Gsco_APs	Edit
	Wired Dot1X Endpoints	if Wired_802.1X		then Wired_Dot1X	Edit
1 🖉 🗹 🗸	Wireless Dot1X Endpoints	if Any 💠 an		then AuthZ Profil	💠 Done
	Default	Add All Conditions I	Ð		
		Condition Name			
Save	Reset	Select Condition	0		<u>نې</u> -

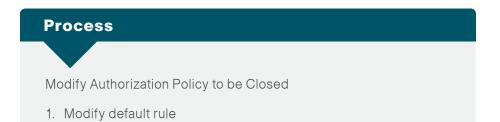
**Step 7:** Under the Permissions column, next to **AuthZ Profile**, click the + symbol.

Step 8: In the list, next to Standard, click the > symbol, and then choose Wireless\_Dot1X.

â	Home	Operations 🔻 Policy 🔻 Adr	ninistration 🔻				👓 Task Naviga	ator 🔫	9
4	Authent	ication 💽 Authorization 🛛	🖕 Profiling 🛛 💽 Posture	灵 Client Provisioning	📃 Security Grou	p Access 🥂 🐥 Policy Elem	ients		
ıth	orizatio	n Policy							
		norization Policy by configuring rules I	pased on identity groups and/	or other conditions. Drag ar	nd drop rules to chan	Standard			
rst N	latched F	Rule Applies 👻							
							- ∰.+		
Exc	eptions (	(0)				Garage Blacklist_Access			
Sta	ndard					Gisco_IP_Phones			
	Status	Rule Name	Conditions (idopt	ity groups and other condit	2007)	DenyAccess			
	Status	Black List Default	if Blacklist	ity groups and other condit	Uris j	PermitAccess		Edit	-
	_					😪 Wired_Dot1X		Eulit	
		Profiled Cisco IP Phones	f Cisco-IP-Phone			🤬 Wireless_Dot1X		Edit	Ŧ
	<b>~</b>	Profiled Cisco APs	if Cisco-Access-Pe	bint				Edit	Ŧ
	<b>~</b>	Wired Dot1X Endpoints	if Wired_802.1X					Edit	Ŧ
ø	•	Wireless Dot1X Endpoints	if Any 💠	and Wireless_802.1X			0	Done	
		Default	if no matches, then	PermitAcces:				Edit	Ŧ
				Select	an item 🔇	> -+			
Sav	e Re	eset							

Step 9: Click Done, and then click Save.

cisco Identity Services Engine		ise-1 admin Logout Feedback
🚖 Home Operations 🔻 Policy 🔻 Administra		🕶 Task Navigator 🔫 🕙
🛃 Authentication 🛛 👩 Authorization 🔀 Profi	ing 👩 Posture 🛛 Client Provisioning 🔄 Security Group Access	8 Policy Elements
Authorization Policy Define the Authorization Policy by configuring rules based of First Matched Rule Applies  Fits Matched Rule Applies Exceptions (0) Standard	n identity groups and/or other conditions. Drag and drop rules to change the ord	я.
Status Rule Name	Conditions (identity groups and other conditions)	Permissions
Black List Default	if Blacklist	then Blacklist_Access Edit   -
Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones Edit   -
Profiled Cisco APs	if Cisco-Access-Point	then Gisco_APs Edit   -
Wired Dot1X Endpoints	if Wired_802.1X	then Wired_Dot1X Edit   -
Wireless Dot1X Endpoints	if Wireless_802.1X	then Wireless_Dot1X Edit   -
✓ Default	if no matches, then PermitAccess	Edit   🕶
Save Reset		



The current authorization policy is an open policy. The default rule at the end specifies that if an incoming authorization request doesn't match one of the specific rules defined, it would then just permit access to the network. Now that you have enabled low-impact mode, you will need to change this rule to deny access to any request that doesn't match one of the specific rules.

#### Procedure 1

Modify default rule

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

Step 2: For the default rule, click Edit.

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

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

â	Home	Operations <b>v</b> Policy <b>v</b> Ad	ministration 🔻					👓 Task Navigati	or 📲 🕐
4	Authent	ication 🧕 Authorization	🖌 Profiling 🔤	🛐 Posture	🛃 Client Provisioning	Security Group Access	🔒 Policy Elements		
ıth	orizatio	n Policy							
		norization Policy by configuring rules	based on identity	groups and/or	other conditions. Drag and	I drop rules to change the ord	ar.		
st N	Matched F	Rule Applies 👻				Standard			
Exc	eptions (	(0)				<b>↓</b> •• ■ 1≣	- <u>(</u>		
Sta	indard					Gacklist_Access			
						Gisco_APs			
	Status	Rule Name			groups and other conditio		115		
		Black List Default	if Blac	:klist		Q DenyAccess	Access		Edit   🔻
	<ul> <li>Image: A set of the set of the</li></ul>	Profiled Cisco IP Phones	if Cisc	o-IP-Phone		PermitAccess	Phones		Edit   👻
		Profiled Cisco APs	f Cisc	o-Access-Poi	at	Wired_Dot1X	25		Edit I 👻
	_				R.	Wildess_DociA	í		cut ( *
	<b>~</b>	Wired Dot1X Endpoints	if Wire	ed_802.1X			ot1X		Edit   👻
	<b>~</b>	Wireless Dot1X Endpoints	if Wire	eless_802.1X			Dot1X		Edit   👻
		Default		atches, then	PermitAccess 🗢				Done
Sav	/e Ki	eset			PermitAccess	○ - +			
						v			

Step 5: Click Done, and then click Save.

	11	Operations V Policy V Admir								0
â			nistration 🔻		_		_	He las	k Navigator	
4	Authenti	cation 🧕 Authorization 🔀	Profiling 💽 Posture	🛃 Client Provisioning	Security Group Access	•	Policy Elements			
uth	orizatio	a Dolicy								
		iorization Policy by configuring rules ba	sed on identity grouns and/or	other conditions. Drag an	d dron rules to change the orde	ər.				
		ule Applies 🔹	ees en neer te product en ny er							
sti	Matched H	ule Applies 🔹								
Ex	ceptions (	0)								
Sta	andard									
	Status	Rule Name		groups and other conditi			Permissions			
	<ul> <li>Image: A set of the set of the</li></ul>	Black List Default	if Blacklist			then	Blacklist_Access		Ed	it∣▼
	<ul> <li>Image: A set of the set of the</li></ul>	Profiled Cisco IP Phones	if Cisco-IP-Phone			then	Gsco_IP_Phones		Ed	it I 👻
		Profiled Cisco APs	if Cisco-Access-Poir	nt		then	Cisco_APs		Ed	it∣▼
		Wired Dot1X Endpoints	if Wired 802.1X			de la seco	Wired Dot1X			
		WIND DULTY ENUDORIES	WIE0_802.1X			unen	Wied_DOUX		Ed	it∣▼
	<b>~</b>	Wireless Dot1X Endpoints	if Wireless_802.1X			then	Wireless_Dot1X		Ed	it   🔻
		Default	if no matches, then	DenyAccess					Ed	t I 👻

#### Process



Monitoring Network Access

- 1. View the Cisco ISE dashboard
- 2. Configure identity groups
- 3. Add a custom profile
- 4. Examining the authentication log
- 5. Create custom authentication reports
- 6. Identify endpoints
- 7. Create device-type reports

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

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

#### **Procedure 1**

View the Cisco ISE dashboard

The first place to view this information is on the Cisco ISE home dashboard. It gives a summary view of the health status of the servers in the group, how devices are authenticating, and what types of devices have been profiled.

Step 1: On the menu bar, click Home.

**Step 2:** If you want to view additional information for a section, click the upper-right corner of that section. The section expands.

cisco	Identity	Services		Administration				ise-1 admin Logout Feedback 👓 Task Navigator 💌 🕑
Metrics	Active Endp 3 —		÷	Active Guest	: Posture Com 0%		oon Time To Remediate 0.0 sec. — 24h ▼	Profiled Endpoints           2         -           1         24h ▼
		Utiliza	ttion and Lat	Latency	Identity Stores (PIP) Name Internal Endpoints AD	Authentications 24k ≠   hillini  hilli, 175     27		Last 24 Hours Last 60 Minutes
Total	ution By:	re Last 24 H		L <sup>T</sup> LLL ast 60 Minutes 2	Profiled Endpoints Unique 2 Distribution by: B PIN N B Profile B Identity Group	fours Last 60 Minutes	Passed 0% MTTR 0.0sec Distribution of Failur El OS El Reason	Last 24 Heurs Last 60 Minutes by: No Data Available No Data Available 0.30 00.2 [ Notificators (0)

#### 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.

cisco Identity Services Engine		ise-1 admin Logout Feedback
🛕 Home Operations 🔻 Policy 🔻 Admir	stration 🔻	👓 Task Navigator 🔻 🕙
🛃 Authentication 🛛 🧕 Authorization 🔀	Profiling 👩 Posture 👩 Client Provisioning 🔄 Security Group Access 💦 🐥 Policy Elements	
Profiling	Profiler Policy       * Name       Apple-Pad       Description       Policy for Apple Pads         Policy Finabled       Image: Pads       Policy for Apple Pads       Policy for Apple Pads         Policy Finabled       Image: Pads       Policy for Apple Pads       Policy for Apple Pads         * Minimum Certainty Factor       20       (Vaid Range 1 to 65555)       *         * Exception Action       NONE       Image: Pads       *         © Create Matching Identity Group       Use Herarchy       *       *         * Derent Policy       Apple-Device       Image: PadRule2Check2       Then Certainty Factor Increases       *         If Condutin       Apple-IPadRule2Check1_AND_Apple-MacBo       Then Certainty Factor Increases       *       20         Street       Reset       Reset       *       Reset       *	5 V

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

#### Procedure 3

Add a custom profile

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

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

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

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

Step 3: Click Add.

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

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

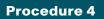
Step 6: In the Expression list, next to DHCP, click the > symbol, and then select dhcp-class-identifier.

Home Operations      Policy      Authentication     Authorization	Administration 🔹	👓 Task Navigator 👻 🕙
Profiling	Profiler Policy * Name CocoCus Policy * Name CocoCus Policy * Name CocoCus * both Policy * Name Policy * Name * Minimum Cartainty Factor * Exception Action * Exception Action * NONE * Network Scan (NMAP) Action © Create Matching Identity Group © Use Herachy * Parent Policy NONE * Rules	
	If Condition Conditions Then Certainty Factor Ince Condition Name Expression Select Attribute Condition Name Expression	

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

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

	ise-1 admin Logout Feedba Station • • • • • • • • • • • • • • • • • • •
Profiling	Profiler Policy       * Name       Gisco-Clus       Description       Clicco Clus         Policy Enabled       Image: Clicco Clus       Clicco Clus          * Policy Enabled       Image: Clicco Clus           * Winnum Certainty Factor       ID       (Vaid Range 1 to 65535)         * Network Scan (MAP) Action       NONE       Image: Clicco Clus          * Network Scan (MAP) Action       NONE       Image: Clicco Clus          © Create Matching Identity Group       Use Herarchy       *          * Network Scan (MAP) Action       NONE       Image: Clicco Clus          @ Create Matching Identity Group            @ Create Matching Identity Group            @ Create Matching Identity Group            @ Create Matching Identitier_CONTRINS_Clisco       Then Certainty Factor Increases          @ Create Matching Identitier_CONTRINS_Clisco       Then Certainty Factor Increases          @ Create Matching Identitier_CONTRINS_Clisco       Then Certainty Factor Increases          @ Create Matching Identitier_Contraints            @ Create



**Examining the authentication log** 

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

For devices that authenticated via MAB, the MAC address of the client is listed as the user name and the endpoint. For devices that authenticated via RADIUS over wireless or VPN, the user name is displayed.

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

**Step 2:** In the details column of the MAB record, click the "paper with magnifying glass" icon. This displays detailed authentication information for the record.

In the Authentication Summary section, the network device lists the IP address and the port of the switch that the endpoint is connected to.

🔔 🚔 🖻					Launch Interactive Viewe	r Ş
RADIUS Authenticati	on Details					
Showing Pag	e 1 of 1   First		Goto Page:	Go		
AA Protocol > RAE	DIUS Authentication Detail					
RADIUS Audit Session NAA session ID : Date :	ID : 0A052C0500000001B4B84B0 ise-1/112681645/20 December 13,2011	26				
enerated on Decembe	er 13, 2011 1:44:33 PM PST					
		Actions				
		Troubleshoot Authentication				
		View Diagnostic Messages Audit Network Device Configuration				
		View Diagnostic Messages Audit Network Device Configuration View Network Device Configuration				
		View Diagnostic Messages Audit Network Device Configuration				
Authentication Summa	ary	View Diagnostic Messages Audit Network Device Configuration View Network Device Configuration				
Authentication Summa	ary December 13,2011 11:42:30.740	View Diagnostic Messages Audt Network Device Confluention <sup>™</sup> View Network Device Confluention <sup>™</sup> View Server Configuration Changes				
		View Diagnostic Messages Audt Network Device Confluention <sup>™</sup> View Network Device Confluention <sup>™</sup> View Server Configuration Changes				
Logged At:	December 13,2011 11:42:30.740	View Diagnostic Messages Audt Network Device Confluention <sup>™</sup> View Network Device Confluention <sup>™</sup> View Server Configuration Changes				
Logged At: RADIUS Status: NAS Failure: Username:	December 13,2011 11:42:30.740 Authentication succeeded E8:04:62:EA:83:90	View Diagnostic Messages Audt Network Device Confluention <sup>™</sup> View Network Device Confluention <sup>™</sup> View Server Configuration Changes				
Logged At: RADIUS Status: NAS Failure: Username:	December 13,2011 11:42:30.740 Authentication succeeded E8:04:62:EA:83:90 E8:04:62:EA:83:90	View Diagnostic Messages Audt Network Device Confluention <sup>™</sup> View Network Device Confluention <sup>™</sup> View Server Configuration Changes				
Logged At: RADIUS Status: NAS Failure: Username: MAC/IP Address: Network Device:	December 13,2011 11:42:30.740 Authentication succeeded E8:04:62:EA:83:90 E8:04:62:EA:83:90 DefaultNetworkDevice : 10.5.44:	View Diagnostic Messages Audt Network Device Confluention <sup>™</sup> View Network Device Confluention <sup>™</sup> View Server Configuration Changes				
Logged At: RADIUS Status: NAS Failure: Username: MAC/IP Address:	December 13,2011 11:42:30.740 Authentication succeeded E8:04:62:EA:83:90 E8:04:62:EA:83:90	View Diagnostic Messages Audt Network Device Confluention <sup>™</sup> View Network Device Confluention <sup>™</sup> View Server Configuration Changes				
Logged At: RADIUS Status: NAS Failure: Username: MAC/IP Address: Network Device: Allowed Protocol: Identity Store:	December 13,2011 11:42:30.740 Authentication succeeded E8:04:62:EA:83:90 DefaultNetworkDevice : 10.5.44. Default Network Access	View Diagnostic Messages Audt Network Device Confluention <sup>™</sup> View Network Device Confluention <sup>™</sup> View Server Configuration Changes				
Logged At: RADIUS Status: NAS Failure: Username: MAC/IP Address: Network Device: Allowed Protocol:	December 13,2011 11:42:30.740 Authentication succeeded E8:04:62:EA:83:90 DefaultNetworkDevice : 10.5.44. Default Network Access	View Diagnostic Messages Audt Network Device Confluention <sup>™</sup> View Network Device Confluention <sup>™</sup> View Server Configuration Changes				

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

🔔 🖴 🗃	Launch Interactive Vie	wer 🎦
RADIUS Authentication Details		
Showing Page 1 of 1	First Prev Next Last   Goto Page: Go	
∃_Authentication Details		
_ogged At:	December 13,2011 11:42:30.740 AM	
Dccurred At:	December 13,2011 11:42:30.740 AM	
Server:	ise-1	
Authentication Method:	mab	
AP Authentication Method :	Lookup	
AP Tunnel Method :		
/sername:	E8:04:62:EA:83:90	
ADIUS Username :	E8:04:62:EA:83:90	
alling Station ID:	E8:04:62:EA:83:90	
ramed IP Address:		
Ise Case	Host Lookup	
etwork Device:	DefaultNetworkDevice	
letwork Device Groups:	Device Type#All Device Types_Location#All Locations	
AS IP Address:	10.5.44.5	
AS Identifier:	103,443	
AS Part:	50101	
AS Port ID:	GigabitEthernet1/0/1	
IAS Port Type:	Ethemet	
llowed Protocol:	Default Network Access Call Check	
ervice Type:	Call Check	
lentity Store:		
uthorization Profiles:	PermitAccess	
ctive Directory Domain:		
lentity Group:		
llowed Protocol Selection Matched R		
lentity Policy Matched Rule:	Default	
elected Identity Stores:	Internal Endpoints	
uthorization Policy Matched Rule:	Default	
GA Security Group:		
AA Session ID:	ise-1/112681645/20	
udit Session ID:	0A052C050000001848848C6	
unnel Details:		
isco-AVPairs:	service-type=Call Check audit-session-id=0A052C050000001184B84BC6	
Other Attributes:	Config/Versionlefe4(Destination-Port=1645/Portocol=Radius,Framed-MTU=1500_EAP- Key-Name-C/MSessionII=D-Ad25C2000000001B48346C5_EndForMACAddress=E8-04-62-EA-83-90,Device Type=Portoc Type#AII Device Types_Location=Location#AII Locations_Device IP Address=10.5.44.5,Called-Station- DE=EC:68.25.789.01	
Posture Status:	NotApplicable	
PS Status		

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

#### Procedure 5

**Create custom authentication reports** 

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

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

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

#### Step 3: Select RADIUS Authentication.

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

**Step 5:** If you wish to use one of the default time ranges, choose that time range.

🛕 Home Operations 🔻 Policy 🔻 Admi	nistration	n 🔻				<del>90</del>	Task Navigator 👻 🕻
Authentications	Service	<u> </u>	🖞 Alarms 📑 Reports 💊	Trouble	eshoot		
Favorites Shared Catalog System							
Reports	1 1	AAA P	rotocol				
AAA Protocol	1						
<ul> <li>Allowed Protocol</li> </ul>		e					
Server Instance		Filter:		Clear F			
Endpoint			Report Name	*	Туре	Modified At	
Failure Reason		0	AAA Diagnostics		System Report	Mon Feb 27 23:41:09 PST 2012 Mon Feb 27 23:41:09 PST 2012	
Network Device		0	Authentication Trend RADIUS Accounting		System Report System Report	Mon Feb 27 23:41:09 PST 2012 Mon Feb 27 23:41:09 PST 2012	
User User		•	RADIUS Authentication		System Report	Mon Feb 27 23:41:09 PST 2012	
Security Group Access		_	· · · ·		Gystelli rtepoli		Denot Denote
Session Directory	4	Run -	ast 30 Min				Reset Reports
Posture		-		Report	" hover mouse over	the 'Report Name' to view the repor	t description
Endpoint Protection Service		L	ast 12 Hours eport Name' to ru				
			eport and click or		button to select addit	ional options.	
	•		esterday ast 7 days				

If you wish to select a time range that is not listed, choose **Query and Run**. All the parameters available for the report display. After choosing the parameters you want, click **Run** to generate the report.

Figure 2 - RADIUS report parameters

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

#### Procedure 6 Identify endpoints

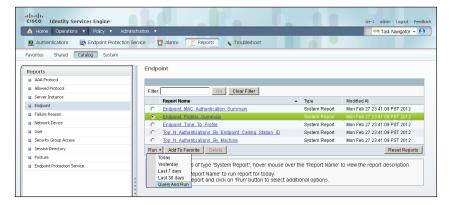
Using information gleaned from the RADIUS and DHCP requests, Cisco ISE can identify what types of devices are connecting to the network. This can assist in determining the network security policy based on the type of device that is in use.

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

**Step 2:** In the left pane, click **Endpoint**. This displays the available endpoint reports.

Step 3: Select Endpoint Profiler Summary, and then click Run.

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



**Step 5:** Once the report is generated, you can view the details of a profiled endpoint by clicking the magnifying glass icon.

The details given in the summary section are the MAC address, the endpoint policy, and the identity group for the endpoint. Additional details, such as IP address and network access devices, are available in the Endpoint Details section. For wireless and remote-access VPN endpoints that authenticated with RADIUS, the user name is also listed.

Figure 3 - Endpoint profile summary

Profiler Summary		Profiler History			
Logged At :	Dec 8, 2011 2:20 PM	Day	Endpoint policy		
Server :	ise-1	Dec 8, 2011 2:20 PM	Apple-iPad		
Event :	Profiler EndPoint profiling event	Dec 8, 2011 2:20 PM	Apple-iPad		
Endpoint MAC Address :	occurred 7C:6D:62:DE:05:8F	Dec 8, 2011 12:11 PM	Apple-Device		
Endpoint Policy : Matched Rule :	Apple-iPad				
Certainity Metric :	30				
Endpoint Matched Policy : Endpoint Action Name :	Apple-iPad				
Identity Group :	Apple-iPad				

#### Figure 4 - Endpoint Details

Endpoint > Endpoint Prof	iler Detail
Generated on December 13, 20	11 1:59:11 PM PST
Endpoint Session time : Not	t 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:	CPMSessionID=0a042e41000000494ee13838
Endpoint Property :	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-Identifie=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
	HostureAssessmentStatus=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
	15
	119
	252 MatchedPolicyID=17679880-116b-11e1-ae1c-0050569e2146
	Destination/PAddress=10.4.48.41
	NAS-Port=13
	ADDomain=cisco.local NmapScanCount=0
	dhcp-message-type=DHCPDISCOVER
	htype=Ethemet (10Mb)
	EndPointMACAddress=7C-6D-62-DE-05-8F ServiceSelectionMatchedRule=Wireless-Dot1X
	PortalUser=
	EndPointMatchedProfile=Apple-Device RequestLatency=9
	EapTunnel=PEAP
	AuthState=Authenticated
	Airespace-Wilan-Id=1 hlen=6
	hops=2
	host-name=SBA-iPad
	FirstCollection=1323375086686 EndPointPolicyID=17679880-116b-11e1-ae1c-0050569e2146
	SelectedAccessService=Default Network Access
	secs=0
	AuthorizationPolicyMatchedRule=Default IdentityPolicyMatchedRule=Default
	MessageCode=5200
	DeviceRegistrationStatus=0 SelectedAuthorizationProfiles=PermitAccess
	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:04:18:4e: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
	Called-Station-ID-TC-17-SD-CB-40-SD, WEDAVEData

#### Procedure 7

**Create device-type reports** 

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

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

Step 2: In the left pane, click AAA Protocol.

Step 3: Select RADIUS Authentication.

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

cisco Identity Services Engine			ise-1 admin Logout Feedback					
🛕 Home Operations 🔻 Policy 🔻 Admin	stration 🔻		😁 Task Navigator 👻 😣					
💆 Authentications 🛛 😿 Endpoint Protection S	ervice 💆 Alarms 📑 Reports 🍾 Trouble	shoot						
Favorites Shared Catalog System								
Reports  AAA Protocol  Alowed Protocol	AAA Protocol Filter: Go Clear Fi	Ner						
Server Instance	Report Name	Type Modified At						
Endpoint	O AAA Diagnostics	System Report Mon Feb 23	23:41:09 PST 2012					
Failure Reason	C Authentication Trend	System Report Mon Feb 23	23:41:09 PST 2012					
Network Device	C RADIUS Accounting		23:41:09 PST 2012					
User User	RADIUS Authentication	System Report Mon Feb 23	7 23:41:09 PST 2012					
Security Group Access	Run - Add To Favorite Delete		Reset Reports					
Session Directory	Last 30 Min							
Posture		', hover mouse over the 'Report Nam	e' to view the report description.					
Endpoint Protection Service	Last 12 Hours Today Port And Click on 'Run' Yesterday Last 7 days Query And Run	rt for today. button to select additional options.						

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

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

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

S	arch		٩,
	Bearch	Filter: Search	<u></u>
	_	Criteria	
	0	Blacklist	1
	0	Guest	
	0	Profiled	L
	0	Profiled:Android	
	۲	Profiled:Apple-iPad	
	0	Profiled:Apple-iPhone	
		Apply Cancel	-
	0	Select Identity Groups	

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

Figure 5 - Sample report

VAA Protocol > <u>Query and Run</u> > RADIUS Authentication										
Showing Pag	e 1 of 1						Goto Page:	Go		
AAA Protocol > RADIUS Authentication										
dentity Group : Profiled Apple-iPad Muthentication Status : Pass or Fail Jate : November 13,2011 - December 12,2011 ( <u>Last 30 Minutes   Last Hour   Last 12 Hours   Todav   Yesterdav   Last 7 Davs</u>   Last 30 Days )										
Generated on Decembe	er 13, 2011 2:2	28:15 PI	M PST							
✔=Pass ¥=Fail 🧐	=Click for d	etails	I≩ =Mo	use over item fo	r additional	information				
Logged At	Logged At Status Failure Details Event Username MAC/IP Allowed Protocol Service Type Authentication Authentication Protocol Proto									
Dec 8,11 4:38:00.576	PM 🖌		୍	Authentication succeeded	<u>patjones</u>	7C:6D:62:DE:05:8F	Default Network Access	Framed	dot1x	PEAP (EAP-MSCHAPv2)

Notes		

# Appendix A: Product List

## **Network Management**

Functional Area	Product Description	Part Numbers	Software	
Identity Management	Cisco Identity Services Engine Virtual Appliance	ISE-VM-K9=	1.1.1.268	
	Cisco ISE Base License for 10,000 Endpoints	L-ISE-BSE-10K=		
	Cisco ISE Base License for 5000 Endpoints	L-ISE-BSE-5K=		
	Cisco ISE Base License for 3500 Endpoints	L-ISE-BSE-3500=		
	Cisco ISE Base License for 2500 Endpoints	L-ISE-BSE-2500=		
	Cisco ISE Advanced 3-year License for 10,000 Endpoints	L-ISE-ADV3Y-10K=		
	Cisco ISE Advanced 3-year License for 5000 Endpoints	L-ISE-ADV3Y-5K=		
	Cisco ISE Advanced 3-year License for 3500 Endpoints	L-ISE-ADV3Y-3500=		
	Cisco ISE Advanced 3-year License for 2500 Endpoints	L-ISE-ADV3Y-2500=		
Network Management	Cisco Prime Infrastructure 1.1	R-PI-1.1-K9	4.2	
	Prime Infrastructure 1.1 Software – 5K Device Base Lic	R-PI-1.1-5K-K9		
	Prime Infrastructure 1.1 Software – 2.5K Device Base Lic	R-PI-1.1-2.5K-K9		
	Prime Infrastructure 1.1 Software – 1K Device Base Lic	R-PI-1.1-1K-K9		
	Prime Infrastructure 1.1 Software – 500 Device Base Lic	R-PI-1.1-500-K9		
	Prime Infrastructure 1.1 Software – 100 Device Base Lic	R-PI-1.1-100-K9		
	Prime Infrastructure 1.1 Software – 50 Device Base Lic	R-PI-1.1-50-K9		

## LAN Access Layer

Functional Area	Product Description	Part Numbers	Software	
Modular Access Layer Switch	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.3.0.SG(15.1-1SG)	
	Cisco Catalyst 4500 E-Series Supervisor Engine 7L-E	WS-X45-SUP7L-E	IP Base	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+ ports	WS-X4648-RJ45V+E		
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+,UPoE ports	WS-X4748-UPOE+E		
Stackable Access Layer Switch	Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-48PF-S	15.0(1)SE2	
	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-24P-S	IP Base	
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G		
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G		
Standalone Access Layer Switch	Cisco Catalyst 3560-X Series Standalone 48 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-48PF-S	15.0(1)SE2	
	Cisco Catalyst 3560-X Series Standalone 24 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-24P-S	IP Base	
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G		
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G		
Stackable Access Layer Switch	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-48FPD-L	15.0(1)SE2 LAN Base	
	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-48FPS-L		
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-24PD-L		
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-24PS-L		
	Cisco Catalyst 2960-S Series Flexstack Stack Module	C2960S-STACK		

## **Wireless LAN Controllers**

Functional Area	Product Description	Part Numbers	Software
On Site, Remote Site, or Guest Controller	Cisco 5500 Series Wireless Controller for up to 500 Cisco access points	AIR-CT5508-500-K9	7.2.110.0
	Cisco 5500 Series Wireless Controller for up to 250 Cisco access points	AIR-CT5508-250-K9	
	Cisco 5500 Series Wireless Controller for up to 100 Cisco access points	AIR-CT5508-100-K9	
	Cisco 5500 Series Wireless Controller for up to 50 Cisco access points	AIR-CT5508-50-K9	
	Cisco 5500 Series Wireless Controller for up to 25 Cisco access points	AIR-CT5508-25-K9	
	Cisco 5500 Series Wireless Controller for up to 12 Cisco access points	AIR-CT5508-12-K9	
On Site Controller	Cisco 2500 Series Wireless Controller for up to 50 Cisco access points	AIR-CT2504-50-K9	7.2.110.0
	Cisco 2500 Series Wireless Controller for up to 25 Cisco access points	AIR-CT2504-25-K9	
	Cisco 2500 Series Wireless Controller for up to 15 Cisco access points	AIR-CT2504-15-K9	
	Cisco 2500 Series Wireless Controller for up to 5 Cisco access points	AIR-CT2504-5-K9	

## Appendix B: Changes

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

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

#### Notes

### Feedback

Click here to provide feedback to Cisco SBA.



SMART BUSINESS ARCHITECTURE

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, WITH-OUT 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 DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY OF USE THE DESIGNS, EVEN 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 OF 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 ON ON TO 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.

© 2012 Cisco Systems, Inc. All rights reserved.



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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)