## 

# **Newer Cisco SBA Guides Available**

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

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



BYOD

-

SOLUTIONS

111111

CISCO

SBA

## BYOD—Identity and Authentication Deployment Guide

SMART BUSINESS ARCHITECTURE

August 2012 Series

## Preface

## **Who Should Read This Guide**

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

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

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

## **Release Series**

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

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

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

#### month year Series

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

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

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

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

## **How to Read Commands**

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

Commands to enter at a CLI appear as follows:

configure terminal

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

ntp server 10.10.48.17

Commands with variables that you must define appear as follows:

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

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

#### Router# enable

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

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

100 100 100

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

interface Vlan64

ip address 10.5.204.5 255.255.255.0

### **Comments and Questions**

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

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

August 2012 Series

## Table of Contents

What's In This SBA Guide	1
Cisco SBA Solutions	1
Route to Success	1
About This Guide	1
Introduction	2
Business Overview	2
Technology Overview	3

Deployment Details	5
Enable Authentication	5
Deploying Cisco Identity Services Engine	5
Enabling Visibility to the LAN	12
Enabling Visibility to the Wireless Network	19
Deploying Digital Certificates	
Enabling 802.1X Authentication	
Configuring Group Policy Objects	
Deploying Cisco AnyConnect on Windows Endpoints	
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	
Enabling Authorization for Wired Endpoints	
Enabling Authorization for Wireless Endpoints	
Modify Authorization Policy to be Closed	61
Monitoring Network Access	62
Appendix A: Product List	68
Appendix B: Changes	71

## What's In This SBA Guide

## **Cisco SBA Solutions**

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

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

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

## **Route to Success**

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

## **About This Guide**

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

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

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

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

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



## Introduction

### Note

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

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

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

The distinction between a work device and a personal device has evolved. This evolution of mobile device usage and the introduction of mobile devices into the workplace has caused a paradigm shift in how IT views what qualifies as a network "end point device" and also what it means to "be at work." An organization needs to know not only who is accessing their wired and wireless networks, but also when the networks are accessed and from where. In addition, with the wide adoption of nontraditional devices, such as smart phones and tablets, and people bringing their own devices to access the network, organizations need to know how many of these devices are connecting. With this information, the organization can create policy to prevent connection by nontraditional devices, limit connection to approved devices, or make access to network resources easier for these non-traditional devices. This presents a challenge for IT organizations that seek to provide end-users with a consistent network access experience and the freedom to use any device, while still enforcing stringent security policies to protect corporate intellectual property. Further complicating the situation is delivering both consistent access and enforcing proper security policy based on the specific user-access scenario (wired, wireless, guest, local, branch, and remote users).

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

Other Cisco SBA Solutions guides addressing BYOD business problems include:

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

## **Business Overview**

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

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

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

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

## **Technology Overview**

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

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

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

In the LAN, there are three modes for deploying Cisco TrustSec: monitor mode, low-impact mode, and closed mode. Cisco recommends a phased deployment model that can allow for limited impact on network access while gradually introducing authentication/authorization on the network. An organization's goals might be met by only implementing some of the overall functionality of Cisco TrustSec and a successful deployment does not require all three modes to be deployed. This document covers the deployment phases of monitor mode and low-impact mode both at the headquarters site and the remote sites, with Cisco ISE being centralized in the data center. The deployment in use deploys two features within Cisco IOS on the switches in the access layer at both the headquarters sites as well as the remote sites. The first is MAC Authentication Bypass (MAB), which authenticates the device on the switch port by the MAC address. Monitor mode logs the MAC addresses that connect and grant access to any device that connects. The second feature is 802.1X open mode, which allows the switch port to give unrestricted access to the network even though authentication and authorization have not been performed. This enables the deployment of identity without affecting existing connectivity. This phased approach allows you to prepare for moving to another mode in the future. In the organization, these switch configurations will be managed by Cisco Prime LAN Management Solution (LMS) 4.2 and the new TrustSec Work Center. Cisco Prime LMS simplifies the deployment of identity by performing a network-readiness assessment for an identity deployment, providing templates for the various modes-monitor, low-impact, closed-and providing a step-by-step wizard to configure the various components required.

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





Notes	

## **Deployment Details**

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

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

Table 1 - Cisco ISE engine IP addresses and hostnames

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

#### **Enable Authentication**

#### Process



Deploying Cisco Identity Services Engine

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

#### **Procedure 1**

#### Set up initial primary engine

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

**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... Uirtual 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.



**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**.

Hone Cpectors Policy +	Administrati	This node is in Stand register other nodes edit this node and ch Administration Role	alone mode. To , you must first hange its to Primary	ise1 d	idmin Logout Feedback Task Navigator 👻 🙆
Deployment Licensing Certificates	Logging Mainter	ance Admin Access	Settings	Selecte	d0   Total 1 🛞 🏭 🖕
≪ar ≣ ⊞ .	Edit     Hostn     Ise-1	Register 🕞 Ex	port C Import Node Type ISE	> Show All Personas Administration, Monitoring, Policy Service	Role(s) STANDALONE

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

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

cisco Identity Services Engine			ise-	1 admin Logout Feedback
🛕 Home Operations 🔻 Policy 🔻	Administration 🔻			👐 Task Navigator 👻 🕗 🔵
🔆 System 🦉 Identity Management	Network Resources	🛃 Guest Management		
Deployment Licensing Certificates	Logging Maintenance .	Admin Access Settings		
Deployment	Deployment Node	25		
	161		Se	lected 0   Total 1   🛞 🥁
<ul> <li>See Deployment</li> </ul>	Create Node Group	er 💮 Export 🚱 Import	>> Show All	- 6
	Hostname	<ul> <li>Node Type</li> </ul>	Personas	Role(s)
	ise-1	ISE	Administration, Monitoring, Policy Ser	vice 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**.

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 🔻 Admir	istration 🔻	👓 Task Navigator 👻 🕗
🔆 System 🛛 🖉 Identity Management	Network Resources 🛛 🛃 Web Portal Management	
Deployment Licensing Certificates Logo	ng Maintenance Admin Access Settings	
Deployment	Deployment Nodes List > Cenfigure Node	
<b>∲-</b> ■ 1 	Register ISE Node - Step 2: Configure Node	
Deployment		
	General Settings	
	Hostname ise-3	
	FQDN ise-3.cisco.local	
	IP Address 10.4.48.43	
	Node Type Identity Services Engine (ISE)	
	Personas	
	Administration Role SECONDARY	
	Monitoring Role PRIMARY   Other Monitoring Node ise-1	
	Policy Service	
	Enable Session Services	
	Include Nade in Nade Group <none> * (i)</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 🔻 Admini	stration 🔻	👓 Task Navigator 👻 😢
🔆 System 🦉 Identity Management 🖀	Network Resources 🛛 🧕 Web Portal Management	
Deployment Licensing Certificates Loggin	ig Maintenance Admin Access Settings	
Deployment	Daployment Hodes List > 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	
	Prable Session Services (1)     Include Node in Node Group ISE-Group + (1)	
	C 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 🔻 Administ	tration 🔻 😶 Task Navigator 👻 🙆
🔆 System 🏾 👰 Identity Management 🛛 🚔 N	Vetwork Resources 🛛 🛃 Web Portal Management
Deployment Licensing Certificates Logging	g Maintenance Admin Access Settings
Deployment	Deployment Nodes List > Configure Node
	Register ISE Node - Step 2: Configure Node
Septorment	
	General Settings
	Hostname ise-2
	FQDN ise-2.cisco.local
	IP Address 10.4.48.42
	Node Type Identity Services Engine (ISE)
	Personas
	Administration Role SECONDARY
°.	Monitoring Role SECONDARY Other Monitoring Node
	✓ Policy Service
	Enable Session Services      Include Node in Node Group     ISE-Group     ISE-Group     I
	✓ 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	-
		RADIOS	_

**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 List > Configure Node	
\$•• = = **	Register ISE Node - Step 2: Configure Node	
* Set Depoyment	General Setting:         Hosthame ise-4         FQDN ise-4.disco.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         Include Node in Node Group       Include Node in Node Group         Enable Section Service         Enable Profing 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 🔻 A	iministration 💌	👓 Task Navigator 👻 🕗
🔆 System 🖉 Identity Management	Network Resources 🦉 Guest Management	
Deployment Ucensing Certificates I	ogging Maintenance Admin Access Settings	
License Operations	Conset Learners a best I Import new License File  * License File [CDownload/steebase-icense lic ]  (Inport ]  Consel	

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	🔹 🔹 Adminis	tration 🔻	😝 Task Navigator 👻 🥑
🔆 System 🛛 🌺 Identity Managen	nent 📰 N	etwork Resources 🛛 🛃 Guest Management	
dentities Groups External Ider	tity Sources	Identity Source Sequences Settings	
External Identity Sources		Adve Directory > AD1 Connection Advanced Settings Groups Attributes	
Certificate Authentication Profile	•	* Domain Name cisco.local	
Active Directory		* Identity Store Name AD1	
LDAP	۲	One or more nodes may be selected for Join or Leave operations. If a node is join	d then a leave
RADIUS Token	۲	operation is required before a rejoin. Select one node for lest Connection.	
RSA SecurID	۲	9 Join 9 Leave 9 Test Connection +	
		ISE Test Connection X ode Role Status	
		Ise * User Name: employee1 ARY 🛆 Not Joined to	Domain
		Ise * Password: ••••••••     INDARY AND Joined to     CK Cancel	Domain

**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.

cifcilia CISCO Identity Services Engine	ise-1 admin Logout Feedback
💧 Home Operations 🔻 Policy 🔻 Adm	iinistration 🔻 🧶 😥
🔆 System 🛛 🖉 Identity Management	Network Resources 🛃 Guest Management
Identities Groups External Identity Sources	Identity Source Sequences Settings
External Identity Sources	Connection Advanced Settings Groups Attributes   Domain Name (dsco.local  I dentity Store Name (AD) One or more onder may be setted for Join or Leave operations. If a note is joined then a leave
RADIUS Token	operation is required before a rejoin. Select one node for Test Connection.
RSA SecurID 🛞	9 Join 9 Leave 9 Test Connection
	ISE     Join Domain     ×     bde Rote     Status       V     ise     *User Name, Administrator     RY     At Not Joined to Domain       V     ise     *Password;     ************************************

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.

Poine Operators • Point) • P	auninskakon •	00 Task Naviga	itur 🕶
Authentication SAuthorization	K Profiling R Posture Client Provisioning	Security Group Access 💦 🐥 Policy Elements	
uthorization Policy			
tine the Authorization Policy by configuring rule	is based on identity groups and/or other conditions. Drag and dr	to rules to change the order.	
has been been been been been been been bee			
Ist Matched Rule Applies +			
Exceptions (0)			
Exceptions (0)			
Exceptions (0) Standard			
Exceptions (0) Standard Status Rule Name	Conditions (identity groups and other conditions)	Permissions	
Exceptions (0) Standard Status Rule Name Black List Default	Conditions (identity groups and other conditions) If <b>Blacklist</b>	Permissions then Blackist_Access Er	idit   🕶
Exceptions (0) Standard Status Rule Name Black Let Default Status Profiled Gron IP Phones	Conditions (identity groups and other conditions) If Blackint If Classe	Permissions then Blackist_Access E	dit   🕶 one
Exceptions (0) Standard Status Rule Name Block List Default C Floffed Gisco IP Phones Course Researched	Conditions (identity groups and other conditions) If Blackbot If Cisco	Permissions then Blackist_Access Er	idit   🕶 one



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 Feedba
🛕 Home Operations 🔻 Policy 🔻 Administration 💌	👓 Task Navigator 👻 🕙
🛃 Authentication 🛛 Authonization 🔀 Profiling 🕜 Posture 🗔 Clent Provisioning 🚍 Security Group Access 🔥 Policy Elements	
Authentication Policy	2
Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use Policy Type O Smide	for authentication.
MAB : If Wired_MAB $\diamondsuit$ allow protocols [Allowed Protocol : Default Netwoo] and 🗸	🖗 Actions 👻
Default : US8 Internal Endpoints 💠	🖗 Actions 🔻
Dot1X : If Wired_802.1X 🔶 allow protocols Allowed Protocol : Default Netwoo and ,	🖗 Actions 👻
Default Rule (If no match) : allow protocols Allowed Protocol : Default Netwool and use identity source : Internal Users 🔶	🖗 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:** n this example deployment, all endpoints are allowed to authenticate. Set the following values, click anywhere in the window in order to continue, and then click **Save**:

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

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 I Policy Type Simple O Rule-Based	SE should use to communicate with the network devices, and the identity sources that it should u	se for authentication.
Default : use	AMAB	Actions *
Image: Contrast of the state of the sta	In a differituation and Logitize + If user not found (contrue + If process failed ( <u>Nop</u> + Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS MSCHAP It is not possible contribute processing when authentication fails or user is not found. If contrues option is selected in these cases, requests will be rejected.	Actions *

#### 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**.

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 Policy Type O Simple I Rule-Based	e protocols that ISE should use to communicate with the network devices, and the identity sources that it should use	for authentication.
MAB	: If Wired_MAB I allow protocols Allowed Protocol : Default: Netwo and	🚔 Actions 👻
Wired-Dot1X	: If Wired_802.1X 🔶 allow protocols Allowed Protocol : Default Netwoo and 🗸	🖗 Actions 👻
Default	: uee internal Users  Identity Source AD1 Options	🖗 Actions 🔻
Default Rule (If no match)	If authentication failed <u>Reject</u> : alow proto If user not found <u>Reject</u> If process failed <u>Drop</u> *	🚔 Actions 💌
	Note: For authenticators using PEAP, LEAP, PAP-TAST or RADIUS MSCHAP it is not possible to continue processing when authentication fails or user is not found. If continue option is selected in these cases, requests will be rejected.	

#### **Procedure 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**.

ork Centers > TrustSec > RADIUS Con	figuration			07 Jun 2012, 13:13
Navigator	Configure RADIUS			
Dashboard	It is recommended to have RADIU	JS server configuration for authentic	cation and authorization before configurin	ng identity on the
Getting Started	devices. The following workflow far	clitates RADIUS server configuration	and make the devices radius enabled.	
Readiness Assessment	Select Devices			4
RADIUS Configuration	Configure RADIUS Server			
Identity Configuration				
<ul> <li>Secured Group Access Configuration</li> </ul>	Radius Configuration			
Reports	RADIUS host 🔿 Single 💿 RA	DIUS Group		
Jobs				
	All fields are required.			
	You can create only single RADI	US group, which can contain multiple	RADIUS servers.	
	DADUIC Concern Manual		Shared Key	
	KADIOS GIOUP Name ISE-Group			
	Add the details of the RADIUS sentry RADIUS action of the RADIUS sentry acts as the primary RADIUS	Verify : envers that will be part of this RADIUS i, the second as the secondary and s	Shared Key	t as the first
	Add the details of the RADIUS se entry acts as the primary RADIUS RADIUS Server Details	Verify : ervers that will be part of this RADIUS , the second as the secondary and s Add Y Filter	Shared Key	t as the first
	Add the details of the RADIUS set entry acts as the primary RADIUS RADIUS Server Details V Edt X Delete Z Server Name or IP Address	Verify : where that will be part of this RADIUS; the second secondary and s Add V Filter Authentication port	Shared Key	t as the first
	Add the details of the RADIUS se entry acts as the primary RADIUS RADIUS Server Details	Verify where that will be part of this RADIUS t, the second as the secondary and s Add T Filter Authentication port 1645	Shared Key	t as the first
	Add the details of the RADUS sec entry acts as the primary RADUS RADUS Server Details Server Name or IP Address 0 10.4.48.41 0 10.4.48.42	Verity: wers that will be part of this RADUU t, the second as the secondary and s Add ♀ Filter Authentization port 1645 1645	Shared Key	t as the first
	Add the data's of the RADUS sector with the test of the RADUS are entry acts as the primary RADUS RADUS are entry acts as the primary RADUS RADUS Sector Paddess  RADUS Sector P	Autoritation Action	Previous. Next. P	t as the first

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**.

	Enab	le Interfaces for Ide	entity				
Navigator	crido	ie internaces for for					
Dashboard	Sele	ct Devices and Port G	oups				
Getting Started							
Readiness Assessment	Sele	act devices from the list	of Identity Capable (	devices, and Select the port	group	s associated with these devices.	
RADIUS Configuration							
<ul> <li>Identity Configuration</li> </ul>	Ide	entity Capable Devices			+		
Manage Identity	4	🖗 Filter				Port Group Selector	
Configuration		Display Name	IP Address	Device Type		▼ All Groups	
Enable Identity on Interface	-	A29605.cisco.local	10.5.20.5	stack	-	✓ 1 Gbps Ethernet Ports	
Change of Authorization		A2960S.cisco.local	10.5.60.5	usco Catalyst 2960 stack		✓ 10 Gbps Ethernet Ports	
			RS211-	10.5.156.5	Cisco Catalyst 2960		✓ 10 Mbps Ethernet Ports
<ul> <li>Secured Group Access</li> <li>Configuration</li> </ul>		RS208-	10 5 07 0	Gisco Catalyst 2960		✓ 100 Mbps Ethernet Ports	
comparator i		A2960S.cisco.local	10.3.67.2	stack		Access Ports	
<ul> <li>Reports</li> </ul>		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- 24PJ IS Switch		End Hosts	
		RS232- A3560X.cisco.local	10.5.215.2	Cisco Catalyst 3560X- 24P-L,S Switch		IP Phones     In the second seco	
	<b>V</b>	A3750X.cisco.local	10.4.79.2	Gisco 3750 Stack		E Proc Ports	
		D6500VSS.cisco.local	10.4.15.254	Cisco Virtual Switching System	-		
						Previous Next Finish Can	
	Revis	ew Part Groups					
	Conf	igure Identity					
	Sche	adule Denlovment					

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

Work Centers > TrustSec > Identity Conf	iguration > Enal	ole Identity on Interfa	e					07 Jun 2012, 13:2
Navigator	Enable I	interfaces for Id	entity					
Dashboard	Select E	evices and Port Grou	ups					9
Getting Started	Review	Port Groups						ş
Readiness Assessment								
RADIUS Configuration	View 1	the ports and unsele	ct the ports that y	/ou v	wish to exclude.			
<ul> <li>Identity Configuration</li> </ul>	Select	ed Devices		Ass	ociated Ports			
Manage Identity	D	isplay Name		✓	Port Name	Description		
Configuration	• A:	8750X.cisco.local		✓	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 Addibited of				✓	Gi3/0/18	GigabitEthernet3/0/18		
Secured Group Access				✓	Gi3/0/19	GigabitEthernet3/0/19		
Configuration				<ul><li>✓</li></ul>	Gi1/0/35	GigabitEthernet1/0/35		
Reports				⊻	Gi3/0/16	GigabitEthernet3/0/16		
Jobs					Gi3/0/17	GigabitEthernet3/0/17		
					Gi1/0/38	GigabitEthernet1/0/38		
					GIDINIA	GiashitEthornot2 (0 (14	Next F	inish Cancel
						Previous		Cancer

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*.

ISCO LAN Management Sol	ution 🔹 My Manu 🗴 Monitor 🗶 Invantory 🔻 Configuration 🔻 Reports 🔻 Admin 🗶 Work G. 🕨 🤫 🛀
/ork Centers > TrustSec > Identity Confi	iguration > Enable Identity on Interface 07 Jun 2012, 13:30
Navigator	Enable Interfaces for Identity
Dashboard	Select Devices and Port Groups
Getting Started	Review Port Groups
Readiness Assessment	Configure Identity
RADIUS Configuration	soning as a workey
<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.
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 Mode V Monitor Low impact High
<ul> <li>Secured Group Access Configuration</li> </ul>	security
Reports	Authentication profile and host mode
Jobs	Choose authentication profiles, host modes and action to be taken in case of violations
	LIFOURCE LIFERENT LIFERENT LIFERENT

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**.

Lulu, Cisco Prime	admin   Log Out   Ab	out I Sitemap I Feedback I Help 💽 🖉 Search
isco LAN Management Sol	ution 🔍 My Menu 🔻 Monitor 🔻 Inventory 🔻	Configuration 🔻 Reports 🔻 Admin 🔻 Work Ce 🕨 👘 😭
Vork Centers > TrustSec > Identity Confi	guration > Enable Identity on Interface	07 Jun 2012, 13:30 F
Navigator	Enable Interfaces for Identity	
Dashboard	Select Devices and Port Groups	✓
Getting Started	Review Part 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 Monitor Mode Config
Change of Authorization	O Daily E-ma	
<ul> <li>Secured Group Access Configuration</li> </ul>	O Monthly	
Reports	Job Options	Enable job password
Jobs	Fail on mismatch of config versions	Login Username
	<ul> <li>Sync archive before job execution</li> </ul>	Login Password
	Copy running config to startup	Epshia Parsword
	Failure policy Ignore failure and continue 👻	
		Preview 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.

uluulu, Cisco Prime	admin   Log Out   About   Stemap   Feedback   Help 🔣 Search
	🖣 My Menu 🔻 Manitar 🔻 Inventory 🔻 Configuration 🔻 Reports 🔻 Admin 🔻 Work Ce 🕨 🏥 😭 07 Jun 2012, 13:44 P
Mode: PORT	Groups
f 1. Device and Group Selector	Port Groups
2. Groups	O Select Custom Group(s)  ☉ Define an Adhoc Rule
a 3. Tasks	Adhoc Rule
4. Add Tasks	
5. Set Schedule Options	
G. View Job Work	Object Type: Variable: Operator: Value:
Order	OR  Port  Identity_Security_Mode UnSecured UnSecured
	Add Rule Expression
	Rule Text
	Port.Identity_Security_Mode = "Monitor"
	Charle Suntay Linck da Eveluda
	- Step 2 of 6 - Back Next Frish 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	gur	ation					
<b>IOS Parameters</b>							
Commands							
CLI Commands:	no no no	switchport switchport switchport	port-secur: port-secur: port-secur:	ity ity ity	aging aging violat	time type ion	
							.::
Rollback Commands:							:
			(	Ар	plicable D	evices.	_
			`				_
			Save		Reset	Cance	

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

Julia L. Cisco Prime	admin i Log Out i About i Sitemap i Feedback i Help 🔣 v Search
cisco LAN Manageme	nt Solution 🔹 My Menu 🔻 Monitor 🔻 Inventory 🔻 Configuration 🔻 Reports 🔻 Admin 🔻 Work Gr 🕨 🛛 🚼 😭
Mode: ADDING 1. Device and Group Selector # 2. Groups # 3. Tasks 4. Add Tasks 5. Set Schedule Options 6. Siven Job Work Order	Of An 2012, 13-0 PC Add Tasks Add Tasks Adjoint Tasks Add Instance. Add Instance. Add Instance. Edt View Cli View Ports Delete - Step 4 of 6- Back Next Frich Cancel
H Videos	TAC Service Requests   Alarms 🔍 71 🔻 0 💆 0

**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.

als als		_		Dictionaries			
cisco I	dentity Services Engine				P		ise-1 admin Logout Feedback
💧 Home	Operations 🔻 Policy 🔻	Adminis	tration 🔻	<b>◆•</b> ■ 18 6	ŝi≁		👓 Task Navigator 👻 😢
Authen	tication . Authorization	R P	ofina 💿 Posture	🚞 Simple Candition	۲		
		14		Compound Condition	۲		
Authenticat	ion Policy						×
Define the Aut	hentication Policy by selecting the	protoc	ols that ISE should use to o	10		d the identity sources that it should use	for authentication.
Policy Type	<ul> <li>Simple          <ul> <li>Rule-Based</li> <li>Rule-Based</li> </ul> </li> </ul>						
	MAB	: If	Wired_MAB			fault Netw📀 🛛 and 😱	🖗 Actions 👻
	Ward Debty	· TE	105md 002.4V			Ku da Amari 🧑 Insel	Sill Antione -
	WIED-DOLTX		valled_802.1X 4				SP ACOURS *
	Wireless-Dot1X	: If	Condition(s)			s 📀 and 🕨	🎡 Actions 👻
			💾 ådd åll Conditions F				
	Default Rule (If no match)	: a	Our divisor Name				
			Condition Name	0		J	- 10k
			Desce contaidorn	<u>× 1</u> )			
			l				

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

CISCO Identity Services Engine	Compound Condition  ise-1 admin Logut Feedback
💧 Home Operations 🔻 Policy 🔻 Administration 💌	🔄 👘 Task Navigator 🗸 😣
🛃 Authentication 💿 Authorization 🧟 Profiling 💽 Posture	Wred_MAB Toup Access Wred_802.1X
Authentication Policy Define the Authentication Policy by selecting the protocols that ISE should use to Policy Type O Simple ③ Rule-Based	Wreless_802.1X     Switch_Local_Web_Authentication     d the identity sources that it should use for authentication.
MAB : If Wired_MAB	efault Netwoo
Wired_B02.1X <	afault Netwo and 🖌 🚳 Actions 💌
Wireless-Dot1X : If Condition(s)	s 📀 and 🕨 🔯 Actions 💌
Default Rule (If no match) : al Add Al Conditions Condition Name Select Condition Name	

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

A Home Operations - Policy -	Administration 👻			90 Tack Navinator 💌
Authentication	🔀 Profiling 🖉 Posture 🕞 Cl	ent Provisioning 🚊 Security Group Access	Policy Elements	Task Nangator -
.rthentication Policy afine the Authentication Policy by selecting dicy Type ○ Simple ◎ Rule-Based	he protocols that ISE should use to commun	icate with the network devices, and the identit	y sources that it should use for a	uthentication.
MAB	: If Wired_MAB 🔶 allow	w protocols Allowed Protocol : Default Netwo	and	🖗 Actions *
Wired-Dot1X	: If Wired_802.1X 🔶 allow	w protocols Allowed Protocol : Default Netwo	and	🖗 Actions 👻
Wireless-Dot1X	: If Wireless_802.1X 🔶 allow	w protocols Select Network Access	and	🚔 Actions 🔻
Default Rule (If no match)	: allow protocols Allowed Protocol :	Default Netw and use identity source :	Allowed Protocols	Actions +
			<b>∲-</b> ■ :≣	
			Default Network Access	

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

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

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

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

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 Bindle Based  MAB : If Wired  Wired-Dot1X : If Wired  Wireds-Dot1X : If Wired  Wireds-Dot1X : If Wired	Identity Source AD1	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**.

cisco Identity Services Engine		ise-1 admin Logout Feedback
🏠 Home Operations 🔻 Policy 🔻 Adn	inistration 🔻	👓 Task Navigator 👻 📀
🛃 Authentication 🛛 🧔 Authorization 🔀	Profiling 🖉 Posture 🕞 Client Provisioning 📄 Security Group Access 🔒 Policy Elements	)
Dictionaries Conditions Results		
Results	<ul> <li>Delect PAP as Host Lookup</li> <li>Allow HAP</li> <li>Allow MS-CHAPv1</li> <li>Allow MS-CHAPv2</li> <li>✓ Allow EAP-MD5</li> <li>Detect EAP-MD5 as Host Lookup</li> <li>Allow EAP-T03</li> <li>Allow EAP-T03</li> <li>Allow EAP-T03</li> <li>Y Allow EAP-MD5</li> <li>PEAP Inner Methods</li> <li>✓ Allow EAP-MS-CHAPv2</li> <li>✓ Allow EAP-MS-CHApv2</li> <li>✓ Allow EAP-T03</li> <li>✓ Allow EAP-GTC</li> <li>✓ Allow EAP-GTC</li> <li>✓ Allow FAP-GTC</li> <li>✓ Allow FAP-GTC</li> <li>✓ Allow Fastword Change Retries 3 (Valid Range 1 to 3)</li> </ul>	ے 

#### 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.

									Logout   <u>R</u> efresh
CISCO	MONITOR WLANS		WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	EEEDBACK	
Security AAA General RADIUS	RADIUS Authention Server Index (Priori Server IP Address	cation Servers	s > New 2 • 10.4.48.41					< Back	Apply
Authentication Accounting Fallback TACACS+ LDAP Confirm Shared Secret		at ret	ASCII -						
Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies	Key Wrap Port Number		(Designed fo	r FIPS custom	ers and requires a	key wrap compl	iant RAD	IUS server)	
<ul> <li>Local EAP</li> <li>Priority Order</li> </ul>	Server Status Support for RFC 357	6	Enabled •						
Certificate     Access Control Lists	Server Timeout Network User Management		Z secon Z Enable	as					
Wireless Protection     Policies     Web Auth     Advanced	IPSec		Enable Enable						

**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.

ahaha										Logout <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs <u>C</u> C	ONTROLLER	WIRELESS S	BECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	EEEDBACK	
Security	RADIUS	Authenticati	on Server:	s					Apply	New
▼ AAA General ▼ RADIUS Authentication	Call Sta Use AE	tion ID Type 🕹 S Key Wrap 👔	IP Address	▼	rs and requir	es a key wran co	moliant RADIUS	server)		
Accounting 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	✓		1	10.4.48.15	1812	Dis	abled	Disable	d 🔽	
User Login Policies	<b>V</b>		2	10.4.48.41	1812	Dis	abled	Enabled	t 🔽	
AP Policies	$\checkmark$		3	10.4.48.42	1812	Dis	abled	Enabled	1 🔽	
Local EAP										
Priority Order										
Certificate				1.4						
Access Control Lists	I. Call Sta	ion ID Type will t	be applicable	only for non 802.3	l× authentica	tion only.				
Wireless Protection     Policies										
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.

ahaha							Configuration   Ping   Logout Refresh
CISCO	MONITOR <u>W</u> LANS		WIRELESS SECU	RITY M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>E</u> EEDBACK
Security	RADIUS Accountin	ng Servers >	New				< Back Apply
AAA     Ganerol     RADJUS     Authentication     Accounting     Falback     TACACS+     LoAP     Local Net Users     MAC Filtering     Disabled Clients     User Login Policies     AP Policies	Server Index (Priority Server IP Address Shared Secret Format Shared Secret Confirm Shared Secre Port Number Server Status Server Timeout	2 - 10.4.4 - ASCII 	8.41 •••• •••• ed •				
Local EAP	Network User	📝 En-	able				
Priority Order	IPSec		nable				
Certificate							
Access Control Lists							
<ul> <li>Wireless Protection</li> <li>Policies</li> </ul>							
Web Auth							
Advanced							

**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.

ahaha							Say	e Configuration   <u>P</u> ing   Logout   <u>R</u> efresh
CISCO		<u>W</u> LANS <u>C</u> ON	TROLLER WIRELE	SS <u>S</u> E	CURITY MANAGEM	IENT C <u>O</u> MMAN	IDS HEL	P <u>E</u> EEDBACK
Security	RADIUS A	counting S	ervers					Apply New
▼ RADIUS Authentication Accounting	Network User	Server Index	Server Address	Port	IPSec	Admin Status		
Fallback TACACS+		1	10.4.48.15	1813	Disabled	Disabled		
LDAP	$\checkmark$	2	10.4.48.41	1813	Disabled	Enabled		
Local Net Users MAC Filtering		3	10.4.48.42	1813	Disabled	Enabled		
Disabled Clients User Login Policies AP Policies								
▶ Local EAP								
Priority Order								
▶ Certificate								
Access Control Lists								
Wireless Protection     Policies								
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**.

ahaha		Sa <u>v</u> e Configuration   <u>P</u> ing   Logout <u>R</u> efresh
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY	MANAGEMENT COMMANDS HELP EEEDBACK
WLANs	WLANs > Edit '10k-WLAN-Data'	< Back Apply
▼ WLANs WLANs	General Security QoS Advanced	
Advanced	Maximum Allowed 0	NAC State None 💌
	Static IP Tunneling  Enabled	Client Load Balancing
	Wi-Fi Direct Clients Disabled -	Client Band Select Z
	Maximum Allowed Clients Per AP Radio	Passive Client
	Off Channel Scanning Defer	Voice
	Scan Defer 0 1 2 3 4 5 6 7	Media Session Snooping 📃 Enabled
	Priority	Re-anchor Roamed Voice Clients 🗖 Enabled
		KTS based CAC Policy Enabled
	Scan Defer Time 100 (msecs)	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 2 FlexConnect Local Switching is not supported with IPsec, CRANIT	E 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, https://ca.cisco.local/certsrv.

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

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

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

Microsoft Active Directory Certificate Services cisco-AD-CA	<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:  Current [cisco-AD-CA] Encoding method:	
© DER © Base 64	
Download CA certificate Download CA certificate chain Download latest base CRL Download latest delta CRL	

Step 5: On the 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						_ B ×
(= =) 🖄 🖬 🖕 🗂 🗙 🖉	2 🛛 🖬						,,
Group Policy Management Group Policy Management Group Policy Management Group Policy Group Policy Group Policy Objects Group Policy Objects Default Domain Policy Group Policy Objects Default Domain	Y         Default I Scope           S         Display Imit Display Imit Security Grou           Security Grou         The follow           Controllers Po         Location           Security Grou         Security Grou	bomain Policy etails Settings Delegatio is in this location: ing sites, domains, and OUs local	n   cisco.local are linked to th	is GPO: Enforced No	Link Enabled Yes	Path cisco.local	¥
WALFUIL COMBUT Supplicant Con WMI Filters B WMI Filters B Stater GPOs Stes Group Policy Modeling Group Policy Results	Edit GPO Status Back Up Restore from Backup Import Settings Save Report	ering this GPO can only apply	y to the followin	g groups, us	ers, and comp	uters:	
-	<u>V</u> iew New <u>W</u> indow from Here	cated Users     Computers (CISCO\Doma	in Computers)				
	<u>C</u> opy Delete Rena <u>m</u> e Re <u>f</u> resh	. Remov	/e	Propertie	8		,
	Help	nked to the following WI	Al filter:				
	<pre>(none)</pre>			•	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	x
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	1

**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 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	Selected 0   Total 1   😵 🛶
😴 Local Certificates	/ Edit -Add  Export  XDelete	Show Al 🔹 😼
Certificate Signing Requests     Certificate Store	Friend Import Local Server Certificate	Issued By Valid From
SCEP CA Profiles	Defau Generate Seni-signed Certificate HTTPS,EAP ise-1.cisco.local Generate Certificate Signing Request	ise-1.cisco.local Fri, 3 Aug 2012
OCSP Services	Bind CA Certificate	

**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 🔻 Admi	nistration 🔻	👓 Task Navigator 👻 😢
🔆 System 🛛 🖉 Identity Management	Network Resources 🛛 🔹 Web Portal Management	
Deployment Licensing Certificates Log	jing Maintenance Admin Access Settings	
Dertificate Operations Cocil Certificates Certificate Spring Reguests Certificate Stree SCEP CA Profiles OCSP Services	Load Certificate Signing Request Generate Certificate Signing Request Certificate Subject [OI=sel.cisco.local * Certificate Subject [OI=sel.cisco.local * Certificate Subject [OI=sel.cisco.local * Digest to Sign With [SHA:256 * 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 Feedback			
🛕 Home Operations 🔻 Policy 🔻 Admini	tration 🔻	😁 Task Navigator 👻 🙆			
🔆 System 🖉 Identity Management 📓	Network Resources 🛛 🛃 Web Portal Management				
Deployment Licensing Certificates Loggin	Deployment Licensing Certificates Logging Maintenance Admin Access Settings				
Certificate Operations	Certificate Signing Requests	Selected 1   Total 1 😵 🚳 🕳			
🔵 Local Certificates	Chillionat Violate	Show All			
🚭 Certificate Signing Requests	Grothour Vicense	310# 41 10			
💩 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			
🔹 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 Hor
Submit a Cert	ificate Request or Renewal Request
To submit a sav by an external s	red request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated source (such as a Web server) in the Saved Request box.
Saved Request:	
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	uhtfohiv95CtuWCpHC72nUgeOifBrySECJudYB62 LbP/xwsXjIX4pLo8Xcf312DTbbw2c0ZX9bOdIffn COURFqV2woWuRs3c0c2QR16fhPHY3rpgcQUAhfA KQv134XMCW/eF12/UQ1JTF3yuhn/HytvcXGM1KD0 XHg13E90AKtnB4FHhESUN15t5xX0hhC05643Cut END CERTIFICATE REQUEST
Certificate Temp	late: Web Server
Additional Attrib	utes:
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.

cisco Identity Services Engine			ise-1 admin Logout Feedback
🍐 Home Operations 🔻 Policy 🔻 Admir	nistration 🔻		😬 Task Navigator 👻 🕗
🔆 System 🦉 Identity Management 📲	Network Resources 🛃 Web Portal Management		
Deployment Licensing Certificates Logg	ing Maintenance Admin Access Settings		
Certificate Operations	Certificate Store		Selected D   Total 4   🍪 🖕
Certificate Signing Requests	🖌 Edit 🕂 Import 🔂 Export 🗙 Delete		Show Al 🔹 😼
G Certificate Store	Friendly Name	<ul> <li>Issued To</li> <li>Issued By</li> </ul>	Valid From Expiration Dat
SCEP CA Profiles	ise-1.cisco.local#ise-1.cisco.local#00001	ise-1.cisco.local ise-1.cisco.local	Fri, 3 Aug 2012 Sat, 3 Aug 20
OCSP Services	ise-2	ise-2.cisco.local ise-2.cisco.local	Fri, 3 Aug 2012 Sat, 3 Aug 20
-	ise-3	ise-3.cisco.local ise-3.cisco.local	Fri, 3 Aug 2012 Sat, 3 Aug 20
	ise-4	ise-4.cisco.local ise-4.cisco.local	Fri, 3 Aug 2012 Sat, 3 Aug 20

**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 🔻 Adminis	ration 🔻	👓 Task Navigator 👻 🕗
🔆 System 🖉 Identity Management 📲	letwork Resources 🛛 🛃 Web Portal Management	
Deployment Licensing Certificates Loggin	Maintenance Admin Access Settings	
Certificate Operations	Local Certificates	Selected 0   Total 1   🚳 🖕
Catificate Stating Requests	/Edit -Add Export XDelete	Show All 👻 😼
Certificate Store	Friend Import Local Server Certificate Friend Certificate Frotocol Issued To	Issued By Valid From
SCEP CA Profiles	Defau Generate Sen-signed Ceronicate HTTPS,EAP ise-1.cisco.local Generate Certificate Signing Request	ise-1.cisco.local Fri, 3 Aug 2012
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	histration 💌	😶 Task Navigator 👻 📀
🔆 System 🦉 Identity Management	Network Resources 🛛 🛃 Web Portal Management	
Deployment Licensing Certificates Logg	ing Maintenance Admin Access Settings	
Certificate Operations	Load Certificates > Bind CA Signed Certificate Bind CA Signed Certificate	
🔹 Certificate Signing Requests	Certificate	
Scertificate Store	* Certificate File C\Downloads\JSEcert.cer Browse	
SCEP CA Profiles	Friendly Name 0	
CLSP services	Inable Validation of Certificate Extensions (accept only valid certificate)	
	Protocol	
	<ul> <li>☑ If you can also that be protected in the control of the tent wing</li> <li>☑ Management Interface: Use certificate to authenticate the web server (GUI)</li> </ul>	
	Override Policy	
	Replace     A catificate being imported may be determined to aheady exist in the system when it has either the     rundher as an existing catificate. In such a case, selection of the "Replace Certificate" option will allow     replaced while retaining the existing protocol selections for the carolinate.	same Subject or Issuer and serial 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.

cisco Identity Services Engine				ise-1	admin Logout Feedback
🏠 Home Operations 🔻 Policy 🔻 Admir	histration 🔻				Task Navigator 👻 😢
🔆 System 🛛 🖉 Identity Management	Network Resources 🛛 🛃 Web Portal Management				
Deployment Licensing Certificates Logg	ing Maintenance Admin Access Settings				
Certificate Operations	Local Certificates			Select	ed 1   Total 2 🥵 🚳 _
😨 Local Certificates	4-2 9-11 (2-2 1 ) March				
🔹 Certificate Signing Requests	/ Edit +Add Export ADelete			Show AI	<u>۵</u>
💩 Certificate Store	Friendly Name	<ul> <li>Protocol</li> </ul>	Issued To	Issued By	Valid From
	Default self-signed server certificate	HTTPS	ise-1.cisco.local	ise-1.cisco.local	Fri, 3 Aug 2012
SCEP CA Profiles	En perduic permagned perven conducto				

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 Feedback				
🛕 Home Operations 🔻 Policy 🔻 Admin	😁 Task Navigator 👻 🕗				
🔆 System 🖉 Identity Management 🖀 Network Resources 🛃 Web Partal Management					
Deployment Licensing Certificates Logging Maintenance Admin Access Settings					
Certificate Operations	Certificate Signing Requests	Salastad 4   Tatal 4 🚳 🚳			
🔹 Local Certificates					
🔹 Certificate Signing Requests	Export X Delete	Show All 👻 🎽			
💩 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			
🔹 OCSP Services					

Step 7: Click Delete, and then click OK.

Process
Enabling 802.1X Authentication
1. Create Cisco ISE policies
2. Enable certificates
3. Enable EAP-TLS

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

#### Procedure 1

**Create Cisco ISE policies** 

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

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

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

cisco Identity Services Engine		ise-1 admin Logout Feedback
💧 Home Operations 🔻 Policy 🔻 Admin	istration 🔻	😬 Task Navigator 👻 🕑
🔆 System 🦉 Identity Management 🔳	Network Resources 🛛 🖉 Guest Management	
Identities Groups External Identity Sources	Identity Source Sequences Settings	
External Identity Sources	Certificate Authentication Profile	Selected 0   Total 0 😽
<b>⊕</b> • <b>≡ ≡ ⊗</b> •	/Edit -Add Choupicate XDelete Show	All
Certificate Authentication Profile 📀	Name • Description	
Active Directory	No data available	
🚞 LDAP 💿		
RADIUS Token ()		
RSA SecurID 📀		

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

cisco Identity Services Engine		ise-1 admin Logout Feedback
🏠 Home Operations 🔻 Policy 🔻 Admin	istration 🔻	😁 Task Navigator 👻 🕗
🔆 System 🛛 🖉 Identity Management	Network Resources 🛛 🛃 Guest Mar	nagement
Identities Groups External Identity Sources	Identity Source Sequences Sett	tings
External Identity Sources           External Identity Sources           Image: Sources           <	Certificate Authentication Profiles List > New 6 Certificate Authentication Pro * Name Description	Certificate Anthentication Profile file Dot1X_Certs
RSA SecurID ()	Principal Username X509 Attribute	Subject Alternative Name
	Perform Binary Certificate Compa	arison with Certificate retrieved from LDAP or Active Directory
	LDAP/AD Instance Name	
	Submit Cancel	

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.

cisco Identity Services Engine			ise-1 admin Logout Feedback
💧 Home Operations 🔻 Policy 🔻 Administra	tion 🔻		😬 Task Navigator 👻 🕙
🔆 System 🛛 👰 Identity Management 🛛 🗑 Net	twork Resources 🛛 🛃 Guest Management		
Identities Groups External Identity Sources	Identity Source Sequences Settings		
Identity Source Sequence			Selected 0   Total 2 😵
/ Edit 🕂 Add 🖓 Duplicate 🗙 Delete		Show All	- 8
Name .	Description	Identity Stores	
Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal	Internal Users	
Sponsor_Portal_Sequence	A built-In Identity Sequence for the Sponsor Portal	Internal Users	

**Step 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: List > New Identity Source Sequence	-
Identity Source Sequence	
Identity Source Sequence	
* Name Dot1X_Certificates	
Description	
Certificate Based Authentication	
Select Certificate Authentication Profile Dot1X_Certs	
▼ Authentication Search List	
A set or identity sources that will be accessed in sequence until hirst authentication succeeds	
Internal Endpoints AD1	
Internal Users	
v ×	
▼ Advanced Search List Settions	
Select the action to be performed if a selected identity store cannot be accessed for authentication	
O 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.

clico Identity Services Engine	ise-1 admin Logout Feedback
🛕 Home Operations 🔻 Policy 🔻 Administration 💌	👓 Task Navigator 👻 😢
📃 Authentication 🖉 Authorization 🧭 Profiling 🕐 Posture 👦 Client Provisioning 🔄 Security Group Access 🔒 Policy Elements	
Authentication Policy Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use Policy Type O Simple O Rule-Based	for authentication.
MAB       : If       Wired_MAB       allow protocols       Allowed Protocol : Default Netwool and         Wired-Dot1X       : If       Wired_802.1X       allow protocols       Allowed Protocol : Default Netwool and	🖗 Actions 🔻
	🚔 Actions 🔻
Image: Control of the second secon	Actions *

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-1 admin Logout Feedback
🛕 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 the Policy Type Simple Skule-Based MAB Viried-Dot1X Viried-Dot1X Viried-Dot1X	protocols that ISE should use to communicate with the network devices, and the identity sources that it should use           : If         Wired_MAB         allow protocols         Allowed Protocol : Default Netwood         and ,           : If         Wired_B021X         allow protocols         Allowed Protocol : Default Netwood         and ,           : If         Wired_B021X         allow protocols         Allowed Protocol : Default Netwood         and ,           : If         Wireless_6021X         allow protocols         Allowed Protocol : Default Netwood         and ,	for authentication.
Default     Default Rule (If no match)	Use AD1	Actions      Actions      Actions      Actions      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.

allalla Network Access	
cisco Identity Services Engine	o admin Logout Feedbac
A Home Operators + Porcy + Administration +	👾 Task Navigator 👻 🧐
🛃 Authentication 💿 Authorization 🥳 Profiling 💮 Posture 🔂 Clent Provisioning 🚍 Security Group 🗉 AuthenticationMetho	d
Device IP Address	
Authentication Policy EapAuthentication	
Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the	hentication.
Policy Type O Simple   Rule-Based  ISE Host Name	
MAR : If Wired MAR I alow protocols allowed Protocol : Default )	ili Actions *
Protocol	
🛛 🔹 Wired-Dot1X : If Wired_802.1X 💠 allow protocols Allowed Protocol : Default N 🗮 UseCase	🖗 Actions 👻
UserName	
I Wireless-Dot1X : If Wireless_802,1X ↔ allow protocols (Allowed Protocol : Default ).	i Actions +
Expression Builden	×
Eab.TLS : If Enter Co	
Condition Name Expression	
Default : use AD1 V Select Attribute O	
	CK Cancel
Default Duty (framework) · Show postcoric Research Default Statute Default Statute (Section 2016)	A SS tations -
Default Rule (If no match)	

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

ahah		
CISCO Identity Services Engine		ise-1 admin Logout Feedbac
A Home Operations • Policy •	Acministration V	😽 Task Navigator 👻 🥶
Authentication S Authorization	🔣 Profiling 🖉 Posture 👵 Client 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	for authentication.
MAB	: If Wired_MAB     Allow protocols Allowed Protocol : Default Netwood and	🖗 Actions *
Vired-Dot1X	: If Wired_802.1X	🖗 Actions +
Vireless-Dot1X	: If Wireless_802.1X  alow protocols Allowed Protocol : Default Netwo and	Actions +
EAP-TLS	; if Enter Co	
Default	Condition Name Expression  Condition Name (Network AccessEster) Equals  EAP-TLS	▼ @+
		OK Cancel
Default Rule (If no match)	: allow protocols Allowed Protocol : Default Netwool and use identity source : Internal Users 🔶 .	💮 Actions 👻

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.

	Administration	ee Task Navigator •
Authentication   💽 Authoriza	ion 💪 Profing 🖉 Posture 👦 Clent Provisioning 🚍 Security Group Access 🚑 Policy Bernenis	
rentication Policy re the Authentication Policy by selec v Type Simple Bulg-Bas	ting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should used	se for authentication.
<ul> <li>M48</li> </ul>	: If <u>Wined_MAB</u> (allow protocols <u>Allowed Protocol</u> : Default Netwo) and	🖗 Actions •
Vired-Dot1X	: If Wired_802.1X	Actions *
Vireless-Dot1X	: If Wireless_802.1X 💠 allow protocols [Allowed Protocol : Default Netwo] and 🗸	🚯 Actions *
EAP-TLS	: if Televerk Access Explutionticati 🖉 use Internal Users	Actions •
EAP-TLS	If Network Access Exploritmentation      Ø Loo Internal Users      Identify Scarse [Coll L_Centric date     Identify Scarse [Coll L_Centric date     Identify Scarse [Coll L_Centric date	Actions •
EAP-TLS Default Default Rule (If no	I I meneni kons Eduarimentari 9 uni interna Users ⊂ Idareti Suna Cotti, Certikute: O Italianto talo ( <u>leget →</u> I fauren talo ( <u>leget →</u> I fauren talo ( <u>leget →</u>	Actions •
EAP-TLS     Default Op/     Opfault Rule (If no	If Tennesk Kosse Episiufvantice ♥ us Tetema Uters      totor Source Cost L, carificate     Ta and rescans rate ( <u>Sease +</u> If an orth cost ( <u>Sease +</u> If an orthogon ( <u>Sease +</u> If an orth cost ( <u>Sease +</u> If an orthown ( <u>Sease +</u> If an orthown ( <u>Sease +</u>	Actions •

#### 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**.

cisco Identity Services Engine	ie-1 admin Logout Fee	edback
🏠 Home Operations 🔻 Policy 🔻 Ar	dministration 🔻 😶 Task Navigator 👻 (	0
💄 Authentication 🛛 🧕 Authorization 🖉	🕻 Profiling 🕐 Posture 👼 Client Provisioning 🚍 Security Group Access 🚺 Policy Elements	
Dictionaries Conditions Results		
Results	Allow MS-CHAPY1 Allow MS-CHAPy2 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-GTC Allow Password Change Retries 1 (Valid Range 0 to 3) Allow EAP-GTC Allow EAP-FAST EAP-FAST Inner Methods Allow EAP-MD5-CHAPV2 Allow EAP-MD5-CHAPV2 Allow EAP-FAST EAP-FAST Inner Methods Allow EAP-MD5-CHAPV2 Allow EAP-MD5-CHAPV3 Allow EAP-MD5-CHAP	
🕗 Help	Alarms 🔕 0 🛕 0 💿 2   🚑 Notifications (	0)



- 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

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.

🗽 certsrv - [Certification Aut	thority (Local)\ci	isco-AD-CA\Certificate Template	es]	
Eile Action View Help				
🗢 🔿 🖄 🙆 😹				
Certification Authority (Joca)	Name Comp Comp Cosp Cosp Escha Cep E Excha Manage New New New Refresh Export List Help Cosp Cosp Cep E Cosp Cep E Cosp Cep E Cosp Cep E Cosp Cep E Cosp Cep E Cep E Cosp Cep E Cep E Cosp Cep E Cep E Cep E Cosp Cep E Cep E Cosp Cep E Cosp Cep E Cep E Cosp Cep E Cep E Cosp Cep E Cosp Cep E Cosp Cep E Cosp Cep E Cosp Cep E Cep Cep E Cep E Cep Cep E Cep Cep E Cep Cep Cep Cep Cep Cep Cep Cep Cep Cep	uter (2003 Template) uto-enrollment naye Enrollment Agent (Offine req Offine request) Y Email Replication Controller Authentication covery Agent =5 Controller ter ter dinate Certification Authority sistator	Intended Purpose Server Authentication, Client Authentication Client Authentication, Secure Email, Encry Server Authentication Certificate Request Agent Certificate Request Agent 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>	
Starts Certificate Templates snapi				

**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:
C Requests can use any CSP available on the subject's computer
Requests must use one of the following CSPs:
CCD <sub>e</sub> .
<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.

Properties of N	ew Template					×
General Issuance Requ	Request Ha irements   Su	andling   perseded Ter	Subject nplates	Name Extensi	ions S	Server   Security
Group or user	names: ated Users					-
Administre	ator (Administra Admins (CISCO)	tor@cisco.loc Domain Admi	al) ns)			_
Sector Company	Computers (CISC e Admins (CISC	CO\Domain C O\Enterprise	omputers) Admins)	)		
	D : C		Add.		Remo	ove
Full Control	r Domain Comp	uters	A		Denj	<u>/</u>
Read				H	H	
Write						
Enroll				$\checkmark$		
Autoenroll				$\mathbf{\nabla}$		
For special per Advanced.	missions or adv	vanced setting	gs, click		Advanc	ed
	ок	Cancel	A	pply		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	(Local)\cisco-AD-CA]	
<u>File Action View H</u> elp		
🗢 🔿 🙎 🖺 📓 🙆 🚺		
Certification Authority (Local)           Idsco-AD-CA           Revoked Certificates           Issued Certificates           Pending Requests           Failed Requests           Manage           New           Certific           Leip	Name       Issued Certificates       Issued Certificates       Pending Requests       Failed Requests       Certificate Templates	
Enable additional Certificate Templates on	this Certification Authority	J J

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

1	Enable Certificate Templates	;	×
i	Select one Certificate Template to e Note: If a certificate template that w information about this template has All of the certificate templates in the For more information, see <u>Certificate</u>	enable on this Certification Authority. ras 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. <u>e Template Concepts.</u>	
I	Name	Intended Purpose	•
I	🚇 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	
	Reference Certification Authority	<al></al>	
	風 Enrollment Agent	Certificate Request Agent	
	🐵 Enrollment Agent (Computer)	Certificate Request Agent	
	風 Exchange Signature Only	Secure Email	
	🖳 Exchange User	Secure Email	<u> </u>
		OK Canc	el

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.

🗽 certsrv - [Certification Au	thority (	(Local)\ci	sco-AD-CA\Certificate Templat	es]	
Eile Action View Help					
🗢 🧼 🖄 🔯 🛃 👔					
Certification Authority (Local)	l) Name	Name		Intended Purpose	
🖃 🦪 cisco-AD-CA		Compu	iter (2003 Template)	Server Authentication, Client Authentication	
Revoked Certificates		🖳 User A	uto-enrollment	Client Authentication, Secure Email, Encry	
Paodios Paquests		ISE .		Server Authentication	
Eailed Requests		CEP Er	ncryption	Certificate Request Agent	
Certificate Template		Exchai	nge Enrolment Agent (Offline req	Certificate Request Agent	
	Manag	e	Offine request)	IP security IKE intermediate	
	New	•	Controller Authentication	Client Authentication Server Authentication	
	2		covery Agent	File Decovery	
	View	•	ES	Encrypting File System	
	Refres	h	Controller	Client Authentication, Server Authentication	
	Export Li	tList erver		Server Authentication	
	Hele	ter ter	ter	Client Authentication, Server Authentication Encrypting File System, Secure Email, Clien	
	Helb				
		Subore	linate Certification Authority	<all></all>	
		🚇 Admini	strator	Microsoft Trust List Signing, Encrypting File	
Starts Certificate Templates snapir	n	,			

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	2
General Request Handling Subject Nam Issuance Requirements Superseded Templates Exte	e Server ensions Security
Group or user names:	
Authenticated Users         Administrator (Administrator@cisco.local)         Domain Admins (CISCO\Domain Admins)         Domain Users (CISCO\Domain Users)         Enterprise Admins (CISCO\Enterprise Admins)	
Add Permissions for Domain Users Allow	Remove Deny
Full Control	
Read	
Write	
Enroll  Autoenroll	
For special permissions or advanced settings, click Advanced.	Advanced
OK Cancel 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.

certsrv - [Certification Authority ]	(Local)\cisco-AD-CA\Certificate Template	es]	
File Action View Help			
🗢 🔿 🙍 🧟 📓			
Certification Authority (Local) disco-AD-CA Revoked Certificates Failed Requests Certificate Certificate Manage New Yew Refresh Export List Help	Name            Computer (2003 Template)             Computer (2003 Template)             Computer forollment Agent (Offline req             IPSec (Offline request)             Directory Email Replication             Domain Controller Authentication             Meb Server             Computer             User             Subordinate Certification Authority             Subordinate Certification Authority	Intended Purpose Server Authentication, Client Authentication Certificate Request Agent Certificate Request Agent IP security IKE intermediate Directory Service Email Replication Client Authentication, Server Authentication Encrypting File System Client Authentication, Server Authentication Encrypting File System, Secure Email, Clien CAI> Microsoft Trust List Signing, Encrypting File	
Enable additional Certificate Templates on t	this Certification Authority		

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> ×

Name	Intended Purpose	<b></b>
Router (Offline request)	Client Authentication	
SBA OCSP Response Signing	OCSP Signing	
風 Smartcard Logon	Client Authentication, Smart Card Logon	
風 Smartcard User	Secure Email, Client Authentication, Smart Card Logon	
風 Trust List Signing	Microsoft Trust List Signing	
🚇 User Auto-enrollment	Client Authentication, Secure Email, Encrypting File System	
風 User Autoenrollment	Client Authentication, Secure Email, Encrypting File System	
風 User Signature Only	Secure Email, Client Authentication	
R Workstation Authentication	Client Authentication	
. 1		
<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			
🗯 🔿 🗾 🖬 🖻 📑 📔 🖬			
E Computer Configuration     Policies	Name	Description	
Software Settings     Windows Settings	The	re are no items to show in this vi	ew.
Name Resolution Policy     Scripts (Startup/Shutdown)     Scripts (Startup/Shutdown)     Scripts Seturity Settings     Local Policies     Local Policies     Event Log     Restricted Groups     Restricted Groups     Restricted Forester Anew Wred Network     Windows Firew     Network List M	Policy for Windows Vista and	Later Releases	
Image: Wireless Network           Image: Big Display Software Rest           Image: Big Display Software Re			
Application Col Elep      Application Col Elep      Advine Directory (CIS      Advine Adult Policy Configuration      Advinistrative Templates: Policy definitions (ADMX +      Advinistrative Templates: Policy definitions (ADMX +      Our 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.

	later) Properties		?
eneral Network P	Permissions		
Settings defined in machines	this policy will apply to	all wireless interface	es of dient
EAP-TLS (Vista ar	nd later)		
Description:			
8021.X EAP-TLS	for Vista and later		
Connect to availab	WLAN AutoConfig serv de networks in the ord	ice for clients er of profiles listed be	elow:
		a al ar ar	-
Profile Name	SSID	Authentication	Encry
Infrastructure Ad Hoc	dit, Remove	Authentication	Encry

**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				
🗢 🔿 🔰 📰 💁 🗟 🖬				
🛛 👰 Computer Configuration 📃	Name	Description	Туре	
Policies	EAP-TLS (Vista and la	8021.X EAP-TLS for Vista an	Vista and Later Release	s
E Software Settings				
Windows Settings				
Image: State Resolution Policy				
Scripts (Startup/Shutdown)				
Security Settings				
🗄 📑 Account Policies				
E Local Policies				
🗉 📺 Event Log				
E Arestricted Groups				
🗉 📑 System Services				
🗉 📴 Registry				
🕀 🣴 File System				
Wired Network (IEEE 802.3) Policie				
Windows Firewall with Advanced S				
Network List Manager Policies				
Mirelace Naturek (TEEE 802-11) Dr				
Create A New Windows XP Policy				
🛨 🔄 View 🕨				
E Refresh				
T F Export List				
🕀 📊 P Help				
🗉 🧾 Administrative Templates: Policy definition:	T			
Preferences				
🔥 User Configuration 📃 🚽				
reate 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).

EAP-TLS (XP) Properties	? ×
General Preferred Networks	
XP Policy Name:	
EAP-TLS (XP)	
Description:	
802.1X EAP-TLS profile for XP	
1	1
Networks to access:	
Any available network (access point preferred)	-
☑ Use Windows WLAN AutoConfig service for clients	
Automatically connect to non-preferred networks	
OK Cancel Apply	·

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.

New Preferred Setting Properties
Network Properties IEEE 802.1X
Enable network access control using IEEE 802.1X
EAP Type:
Microsoft: Smart Card or other certificate Settings
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 Earol-Start Meas: 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**.

mart Card or other Certificate Properties	2
When connecting:	
C Use my smart card	
<ul> <li>Use a certificate on this computer</li> </ul>	
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	-
I →	
View Certificate	
Do not prompt user to authorize new servers or trusted certific	ation
Use a different user name for the connection	
OK Can	cel

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.

#### 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.

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

🔇 Cisco AnyConnect Secure Mobility Client Install Selector	. 🗆 🗡
Select the AnyConnect 3.0.08057 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 Serv	vices
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.

Policy Profile:ili	ty Client\Network Acces	s Manager\system\o	configuration.xml
Network			
Name	Media Type	Group*	
wired	Wired	Global	
			Add
			Edit
			Delete
* A network in	group 'Global' is a member of <i>all</i> gro	oups.	
1			

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.

Access Manager Networks		
Profile:Ility Client\Network A	ccess Manager\system\configuration.xml	Made Tons
ork Groups		Fedra Type
Unprotected Identity Pattern:	[username]@[domain]	Connection Type
		Machine Auth
		Credentials
		User Auth
User Credentials		Credentials
Use Single Sign On Credentials		
Description Conductorial		
Prompt for Credentials		
Remember Forever	110-	
Remember while Oser is i	Logged On	
O Never Remember		
Certificate Sources	Remember Smart Card Pin	
Smart Card or OS certificates	Remember Forever	
Sinar Card of OS Cer uncates	Remember while User is Logged On	
Smart Card certificates only	Neuro Demerikan	
	Never Remember	
< [		

Procedure 4 Create

**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.

Client Policy Authentication Policy	Profile:ility Client\Netwo	ork Access Manager\system\configuration.xml		
Networks Network Groups	Name: Group Membership In group: In all groups (Global)	Wireless-TLS (auto-generated)	Media Type Security Level	
	<ul> <li>Choose Your Network Media</li> <li>Wired (802.3) Network</li> <li>Select a wired network if the ethermet cable.</li> <li>Wi-FI (wireless) Network</li> <li>Select a WFI network if the radio connection to an Acce SSID (max 32 chars):</li> <li>Association Timeout (sec)</li> </ul>	e endstations will be connecting to the network with a traditional endstations will be connecting to the network via a wireless ss Point. WLAN-Data Hidden Network 5		
	Common Settings Script or application on each user's Connection Timeout (sec.) 40	s machine to run when connected. Browse Local Machine		

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

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

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

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

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

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

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

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

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

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

#### Process



Configuring Mac Workstations for 802.1X Authentication

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

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

#### Procedure 1

#### Install root certificate on Mac OS X

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

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

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

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

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

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

#### Step 6: Click Always Trust.



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

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

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

🔀 cisco-Al	D-CA	
Certificate	cisco-AD-CA Root certificate authority Expires: Tuesday, October 18, 20 This root certificate is not trust	16 1:27:28 PM ET red
	Hide Certificate	Don't Trust Always Trust

#### Procedure 2

• Request user certificate

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

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

Keychain Access File Edit	View Window Help
About Keychain Access	Keychain Access
Preferences ೫,	Q
Keychain First Aid 🔍 🕱 A	
Certificate Assistant	Open
Ticket Viewer ℃#K	Create a Certificate
Services	Create a Certificate Authority Create a Certificate For Someone Else as a Certificate Authority
Hide Keychain Access #H	Request a Certificate From a Certificate Authority
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**.

	Certificate Information Enter information for the certificate you are requesting. Click Continue to request a certificate from the CA.
Ce	User Email Address: taylorsmith@cisco.local  Common Name: Taylor Smith CA Email Address: Request is: Emailed to the CA Saved to disk Let me specify key pair information
	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 D	irectory Certificate Services cisco-AD-CA	Home
Submit a Certif	ïcate Request or Renewal Request	
To submit a save generated by ar	ed request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request external source (such as a Web server) in the Saved Request box.	
Saved Request:		
Base-64-encoded c certificate request 1 (CMC or F PKCS #10 or F PKCS #7):	mcBeRIR4XgBiml2vzL161lD1qAgXy1VNk51J3ov kaRmV1E8MgptbolaJ33gmHF14OsanrhwanSDL IFV49197X0PzpK1BkKosUd0CMOrEBolistEjD00n StondOdaLUXgrameQC3/QydyaybaryhE5YE05Gpr GeC63cqXNBDQqzAjJCJ0E9sdBn9rE293HN07E7ue 	
Certificate Templa	te:	
0	User 🗘	
Additional Attribut	les:	
Attributes:		
	(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.

00	Add Certificates
Certificate	Do you want to add the certificate(s) from the file "certnew.cer" to a keychain?
View Cert	Keychain: login 🛟
Procedur	e 3 Configure Mac OS X supplicant
Step 1: On y	our 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.

00	Network	
Show All		٩
🛜 AirPort		
AirPort TCP/IP	DNS WINS 802.	1X Proxies Ethernet
	Status: Con	inected (Turn AirPort Off)
e 1	User Name:	
	Password:	
	Authentication:	Enable Protocol TTLS TLS EAP-FAST
		Configure
		Configure Trust
+ -	Wireless Network: Security Type:	WPA2 Enterprise
Add User Profile	now AirPort status in	
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 TCF	P/IP DNS	WINS	802.1	LX P	roxies	Ethernet	)—
User Profiles							
🗹 WLAN-Data		User	Name:	taylor	smith		
		Pase	sword:		•••		
				Alw	ays pror	npt for pas	sword
		Authenti	cation:	Enable	Protoco	ol	
					TTLS		(
					PEAP		
				⊻	TLS		-
					EAP-F	AST	Ť
				Confi	gure	]	
				$\square$	Configu	ure Trust	
	Wi	reless Ne	twork:	WLAN	-Data		-
_	_	Security	Type:	WPA2	Enterpr	rise	*
_							

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	inistr	ation 🔻 🤒 🤒 💀 Task Navigator 👻 😣
🚨 Authentication 🛛 💿 Authorization 🔀	Pro	filing 👩 Posture 👩 Client Provisioning 🔄 Security Group Access 🦳 🦺 Policy Elements
Profiling		Profiler Policy Lit > Cisco-Access-Point Profiler Policy  * Name Cisco-Access-Point Description Policy for all Cisco Access Points
	0000	Rules If Condition Cisco-Access-PointRule1Check1   Then Certainty Factor Increases   10

#### 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.

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
Dictionaries Conditions Results	
Results	Authorization Profile  * Name Goso_APS Description Profile  * Common Tasks  Description Common Tasks Data Name PERMIT_ALL_TRAFFIC  VLAN Voice Domain Permission VLAN VOICE VLAN VLAN VLAN VLAN VLAN VLAN VLAN VLAN
🕙 Help	Alarms 😆 1702 🔬 0 🚳 6   🔒 Notifications (0)

#### 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.

cisco Identity	Services Engine					ise-1 ad	min Logout F	eedback
🛕 Home Operat	ions 🔻 Policy 🔻 Administratio	on 🔻				👓 Tas	sk Navigator 🔫	3
💄 Authentication	💿 Authorization 🔣 Profilm	ng 💽 Posture	🗔 Client Provisioning	🚊 Security Group Access	🔒 P	olicy Elements		
Authorization Polic	y							
Define the Authorization	n Policy by configuring rules based on	identity groups and/o	r other conditions. Drag and	d drop rules to change the ord	er.			
First Matched Rule App	iles 🔹							
Exceptions (0)								
Standard								
Standard								
Status Rule I	Name	Conditions (identit	y groups and other condition	ons)	P	ermissions		
Black	List Default	if Blacklist			then <b>B</b>	lacklist_Access	Edit	•
Profile	ed Cisco IP Phones	if Cisco-IP-Phone			then O	isco_IP_Phones	Edit	*
🗹 Defau	lt		PermitAccess			Insert Nev	v Rule Above	-
Save Reset								

#### 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.

cisco Identity Services Engine		ise-1 admin Logout Feedback
🚖 Home Operations 🔻 Policy 🔻 Administration 💌		😁 Task Navigator 👻 🕗
🛃 Authentication 🛛 Authorization 🔀 Profiling 💿 Posture 設 Client Provisi	Profiled	A Policy Elements
Authorization Policy	∲•	
Define the Authorization Policy by configuring rules based on identity groups and/or other conditions.	u Android	
First Matched Rule Annlies	■ Apple-Pad	
	Cisco-Access-Point	
Exceptions (0)	Cisco-IP-Phone	
Standard	Workstation	
Status Rule Name Conditions (identity groups and other		Permissions
Black List Default if Blacklist		en Blacklist_Access Edit   🕶
Profiled Cisco IP Phones if Cisco-IP-Phone		n Gisco_IP_Phones Edit   •
Profiled Cisco APs if Any - and Condition(s		then AuthZ Profil 💠 Done
Default if r		Edit   🗸
Save Reset	<b>&gt;</b> = ⊹	

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

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



Step 9: Click Done, and then click Save.

uluulu cisco	' Ide	entity Services Engine	ise-1 admi	n Logout Feedback
🍐 Hor	me (	Operations 🔻 Policy 🔻 Administra	on 🔻 😽 😽 😽 😽 et al.	Navigator 🔫 🕗
💄 Aut	thentic	ation 🧕 Authorization 🔣 Profi	ng 🕜 Posture 🧕 Client Provisioning 📄 Security Group Access 🔥 Policy Elements	
Authoriz	zation	Policy		
Define the	e Autho	rization Policy by configuring rules based o	n identity groups and/or other conditions. Drag and drop rules to change the order.	
First Matri	hed Ru	le ânnlies 👻		
TESCHACO		in Applies		
Except	tions (O	)		
Standa	ard			
Sta	atus	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 Cisco_APs	Edit   🕶
<b>~</b>		Default	If no matches, then PermitAccess	Edit   🕶
Save	Res	et		



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.

cisco Identity Services Engine		ise-1 admin Logout Feedback
Administratio     Authentication     Authentication     Authentication	) 🔹	ee Task Navigator 👻 🕗
Authentication Policy Define the Authentication Policy by selecting the protocols th Policy Type ③ Smple ④ Rule-Based	at ISE should use to communicate with the network devices, and the identity so <u>MAB</u> $\$ allow protocols <u>Allowed Protocol</u> : <u>Default Netw</u> and	urces that it should use for authentication.
Default : use     Vired-Dot1X : If Wired     Vired-Dot1X : If Wired     Vired-S-Dot1X : If Wired	Internal Endpoints Identity Source Internal Endpoints Options If authentication failed <u>Reject * If user not found Reject * If process failed (prop * Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS MSCHAP </u>	کې Actions ۲
Default Rule ((f no match) : allow prot	It is not possible to continue processing when authentication fails or user is not If continue option is selected in these cases, requests will be rejected.	found.

#### 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.



**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.

cisco Identity Services Engine	ise-1 admin Logout Fee	edback
Home Operations      Policy      Admi     Authentication     Authentication	stration V et ask Navigator V	2
Dictionaries Conditions Results		
Results         Image: Second	Authorization Profile  Authorization Profile  * Name Wred_DOIX Description Profile For Wred_Endpoints That Have Authenuticated With 802.1X  * Access Type ACCESS ACCEPT  Common Tasks DACL Name PERMIT_ALL_TRAFFIC VLAN Voice Domain Permission Web Authentication Auto Smart Port Fitter-ID  Advanced Attributes Settings Second Attributes Settings Second Attributes Settings Second Attributes Settings Second Tasks Common Tasks	
🥶 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.

cis	ili. co Id	entity Services Engine					ise-1 ad	lmin Logout F	eedback
â	Home	Operations 🔻 Policy 🔻 Administrat	tion 🔻				😶 Ta	sk Navigator 🔫	3
4	Authentio	ation 🛛 🧕 Authorization 🛛 🔀 Profi	ling 💽 Posture	🛃 Client Provisioning	🚊 Security Group Access		Policy Elements		
Auth	orization	Policy							
Define	the Auth	rization Policy by configuring rules based o	n identity groups and/i	or other conditions. Drag an	id drop rules to change the orde	er.			
First N	latched Ri	le Annies 👻	, , , , , , , , , , , , , , , , , , , ,						
Tisci		an Apples +							
Exc	eptions ((	)							
Sta	ndard								
	Status	Rule Name	Conditions (identi	ty groups and other condition	ons)		Permissions		
	<ul> <li>Image: A set of the set of the</li></ul>	Black List Default	if Blacklist			then	Blacklist_Access	Edit	*
1		Profiled Cisco IP Phones	if Cisco-IP-Phone			then	Cisco_IP_Phones	Edit	•
	<b>~</b>	Profiled Cisco APs	If Cisco-Access-Po	int		then	Cisco_APs	Edit	•
		Default		PermitAccess			Insert Net	w Rule Above	7
Sav	e Re	set							

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.

cisco Identity Services	Engine		ise-1 admin Logout Feedback
🛕 Home Operations 🔻	Policy 🔻 Administration 🔻		🕶 Task Navigator 🚽 😔
🔔 Authentication 🛛 💽 Au	thorization 🔣 Profiling 🖉 Pos	ure 👩 Client Provisioning 📄 Security Group Access	Policy Elements
Authorization Policy Define the Authorization Policy by First Matched Rule Applies	Compound Conditions	and/or other conditions. Drag and drop rules to change the or	der.
Exceptions (0)     Standard	Wired_802.1X     Wired_MAB     Wireless 802.1X		
Status Rule Name	Wireless_MAB     Catalyst_Switch_Local_Web_Authentica	dentity groups and other conditions)	Permissions
Profiled Cisco IF	WLC_Web_Authentication	ione	then Cisco_IP_Phones Edit   +
Profiled Cisco AP		ss-Point	then Cisco_APs Edit   •
Add All Conditions B		Contained (c)	Edit   •
Sav Condition Name Select Condition	2		

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.

cisco Identity Services Engine		ise-1 admin Logout Feedback
🍐 Home Operations 🔻 Policy 🔻 Administrat	tion 🔻	😁 Task Navigator 🛛 🚱
🛃 Authentication 🛛 🧕 Authorization 🔀 Profi	ling 🕜 Posture 🗟 Client Provisioning 🔄 Security Grou	p Access 3 Policy Elements
Authorization Policy Define the Authorization Policy by configuring rules based of First Matched Rule Applies	in identity groups and/or other conditions. Drag and drop rules to cha	Standard
Exceptions (0)		Cisco_APs
P Exceptions (0)		Cisco_IP_Phones
Standard		2 DenyAccess
Status Rule Name	Conditions (identity groups and other conditions)	Wired_Dot1X
Black List Default	if Blacklist	Edit   🕶
Profiled Cisco IP Phones	if Cisco-IP-Phone	Edit   🕶
Profiled Cisco APs	if Cisco-Access-Point	Edit   🕶
🖉 🗹 👻 Wired Dot1X Endpoints	if Any I Wired_802.1X	c Done
🗹 Default	if no matches, then PermitAcces	Edit   •
Save Reset	Select an item (	2 — ÷

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

oli cis	ilii sco Id	entity Services Engine				ise-1 a	admin Logout Feedback
á	Home	Operations 🔻 Policy 🔻 Admini	stration 🔻			90 T	ask Navigator 🛛 🕗
4	Authentio	ation 💽 Authorization 🔀 F	Profiling 💽 Posture	🛃 Client Provisioning	🚊 Security Group Access 💦 👌	Policy Elements	
Auth	orization	Policy					
Define	e the Auth	prization Policy by configuring rules base	ad on identity groups and/o	or other conditions. Drag an	d drop rules to change the order.		
First	Matched Ri	Je Applies 🔹					
► Ex	ceptions ((	))					
St	andard						
	Status	Rule Name	Conditions (identit	ty groups and other conditio	ons)	Permissions	
1	<b>V</b>	Black List Default	if Blacklist		then	Blacklist_Access	Edit   👻
	<b>~</b>	Profiled Cisco IP Phones	if Cisco-IP-Phone		then	Cisco_IP_Phones	Edit   👻
		Profiled Cisco APs	if Cisco-Access-Po	int	then	Cisco_APs	Edit   👻
	<b>~</b>	Wired Dot1X Endpoints	if Wired_802.1X		then	Wired_Dot1X	Edit   👻
		Default	if no matches, then	PermitAccess			Edit   👻
		set					
58	Ve Ke	SBL					

#### **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**.

July L. Cisco Prime						adm	in I	Log Out I About	I Sitemap	I Feedback	I Help	🖳 🖉 Sear	:h	
cisco LAN Management Solution	•	<b>∢</b> (	My Menu	<ul> <li>Moniti</li> </ul>	or 🔻	Inventory	•	Configuration 🔻	Reports 🔻	Admin 🔻	Work	Centers 🕨		
Work Centers > TrustSec > Identity Configuration	on » Man	age Id	lentity Con	figuration									14	Jun 2012, 10:18 PDT
Navigator	Mana	ge I	dentity	Devices										
Dashboard	Revi	ew p	ort selec	tion on se	lected	devices(o	otion	al)						
Getting Started														
Readiness Assessment	Viev	, the	ports and	unselect th	he port	s that you v	wish t	o exclude.						
RADIUS Configuration	Sel	acted	Devices				As	sociated Ports						
<ul> <li>Identity Configuration</li> </ul>		Disp	olay Name				✓	Port Name	Descript	ion				
Manage Identity Configuration	۲	A37	50X.cisco.	local			✓	Gi3/0/18	GI3/0/18	3				-
Enable Identity on Interface							✓	Gi3/0/19	Gi3/0/19	9				_
Changes of Authorization								Gi3/0/16	Gi3/0/16	6				
change of Authorization							☑	Gi2/0/22	Gi2/0/22	2				
Secured Group Access							☑	Gi3/0/17	GI3/0/17	r.				
Configuration							✓	Gi2/0/23	Gi2/0/23	3				
Reports							✓	Gi3/0/14	Gi3/0/14	ŧ.				
Jobs							✓	Gi2/0/20	Gi2/0/20	)				
							✓	Gi3/0/15	Gi3/0/15	5				
								GI2/0/21	GI2/0/21					•
											Previou	lis Next	Finish	Cancel

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

Lulu, Cisco Prime	admin I Log Out I About I Sitemap I Feedback I Help 🔣 - Search
ISCO LAN Management Solution	My Menu 🔻 Monitor 🔻 Inventory 🔻 Configuration 🔻 Reports 🗶 Admin 🔻 Work Centers 💌 🛛 🝸 🚖
Vork Centers > TrustSec > Identity Configuration >	> Manage Identity Configuration 14 Aug 2012, 12:12 PD
Navigator	Manage Identity Devices
Dashboard	Review part selection on selected devices(optional)
Getting Started	Configure Identity
Readiness Assessment	
RADIUS Configuration	Identity mode to be configured
<ul> <li>Identity Configuration</li> <li>Manage Identity Configuration</li> </ul>	Choose the Security mode based on the level of security required in the devices. Values shown as selected are the default values.
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 Mode Monitor Low Impact High
Secured Group Access Configuration	security
Reports	Associated ACL allows selective access control More Details 🕨
Jobs	Associated ACL* PreAuth
	Authentication profile and host mode Choose authentication profiles, host modes and action to be taken in case of violations
	Define Authentication Profile 802.1X, then MAB
	The best mode determines the number of bosts that can be authenticated on a diven part. More Details
	eine nusk wude
	Select the action to be taken when a port security violation is detected due to the following reasons. More Details  Action to be taken on security violation  Restrict  Protect  Shuttdown  No change
	MAC Configuration
	MAC move/replace SNMP MAC notification
	Enable MAC move or replace More Details   Enable SNMP notification for MAC addition or removal More
	Enable MAC move
	Enable MAC replace
	Notify MAC removal
	Additional Configurations If you have selected low impact mode and if AQL is not configured on the device, you More Details
	Advanced options
	Adhoc commands": p accessibit extended PreAuth permit udp any eq bootpc any eq bootps permit udp any en eq doman permit luop any any eq tho permit luop any any eq echo- permit luop any any eq echo-reply
	Previous Next Firsh Cancel
	Schedule Deployment

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

**Tech Tip** 

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

Julualu, Cisco Prime	admin   Lo	ng Out I About I Sitemap I Feedback I Help 🕞 🖡 Sea	rch
cisco LAN Management Solution	🔨 My Menu 🔻 Monitor 🔻 Inventory 🔻 Co	nfiguration 🔻 Reports 🔻 Admin 🔻 Work Centers 🕨	• 🗄 😭
Work Centers > TrustSec > Identity Configuration	n > Manage Identity Configuration		14 Jun 2012, 12:18 PDT
Navigator	Manage Identity Devices		
Dashboard	Review port selection on selected devices(optional)		<b>\$</b>
Getting Started	Configure Identity		<b>V</b>
Readiness Assessment	Schedule Deployment		
RADIUS Configuration			
<ul> <li>Identity Configuration</li> <li>Manage Identity Configuration</li> </ul>	Scheduler     Job Descripti	00* A3750Y Authenticated Mode	* Indicates required field
Enable Identity on Interface	O Once	mail	
Change of Authorization	O Daily O Weekly O Monthly		
<ul> <li>Secured Group Access Configuration</li> </ul>	Job Options		
Reports	Fail on mismatch of config versions	Enable Job Password	
Jobs	Sync archive before job execution	Login Username	
	Copy running config to startup	Login Password	
	Failure policy Ignore failure and continue 💌	Enable Password	
		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



**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.

uluulu. Cisco Prime				adm	iin I Log Ou	t I About	I Sitemap I	Feedback	i Help 📳 Si	earch	
ISCO LAN Management Solutio	n 🔳	My Menu 🔻	Monitor 🔻	Inventory	▼ Configu	ration 🔻	Reports 🔻	Admin 🔻	Work Centers	•	문 🗧
Work Centers > TrustSec > Identity Configurat	ion > Change	of Authorization									21 Jun 2012, 14:0
Navigator	Deploy										
Dashboard										⊕Trus	tSec Configura
Getting Started	Choose	e Templates									
Readiness Assessment	Colort	templates to de	nlov configu	ration							
RADIUS Configuration	Jelect	cempiaces to de	pioy coringo	100011							
<ul> <li>Identity Configuration</li> </ul>	Temp	late Selector						_	Selec	ted 1   Total 1	*
Manage Identity Configuration								Show A		*	6
Enable Identity on Interface		Template Na	me 👻 Fe	atures	Туре	Role In	Category		Created	Scope	
Change of Authorization	>	Identity - Cha	ange Au	ithorizati	Partial	Access	RADIUS cl	ient configur	ati System	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**.

uluulu. Cisco Prime	admin I Log Out I About I Sitemap I Feedback I Help 🕞 Search
cisco LAN Management Solution	🔍 🔨 My Menu 🔻 Monitor 🔻 Inventory 🔻 Configuration 🔻 Reports 🔻 Admin 🔻 Work Centers 🕨 🛛 📅 🚖
Work Centers > TrustSec > Identity Configuration	n > Change of Authorization 21 Jun 2012, 14:15 PDT
Navigator	Deploy
Dashboard	OrrustSec Configuration
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 client IP address or Host name * 10.4.48.41
Change of Authorization	Type of authorization the device uses for RADIUS clients *
k Son red Group Arrow	RADIUS Key shared between the device and RADIUS clients *
Configuration	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.

alialia Cisco Prime	admin I Log Out I About I Sitemap I Feedback I Help 🛛 📕 🖉 Search	
CISCO LAN Management Solutio	🗖 🔍 🧹 My Menu 🔻 Monitor 🔻 Inventory 🔻 Configuration 🔻 Reports 🔻 Admin 🔻 Work Centers 🕨	
Work Centers > TrustSec > Identity Configurat	con > Change of Authorization 2	1 Jun 2012, 14:15 PDT
Navigator	Deploy	
Dashboard	⊕Trust	Sec Configuration
Getting Started	Choose Templates	<i>S</i>
Readiness Assessment	Choose Device Groups	<ul> <li>Image: A start of the start of</li></ul>
RADIUS Configuration	Configure Identity - Change of Authorization	<ul> <li>✓</li> </ul>
<ul> <li>Identity Configuration</li> </ul>	Adhoc Configuration Commands for Selected Devices	S
Manage Identity Configuration	Schedule Deployment	
Enable Identity on Interface		
Change of Authorization	Scheduler * Indicates require	d field
Sacured Group Access Configuration     Reports     Jobs	Immediate Job Description* A3750X CoA Config     Once E-mail     Daly     Weekly     Monthly  Job Options     Copy Startup to Ruming Config upon failure     Copy Naming Config to Startup     Inside to Bassword     Login Username     Login Password     Enable Dessword	
	Preview CLI Previous Next Prish	Cancel

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

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

aaa server radius dynamic-author

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



- 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.



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**.

CISCO Identity Services Engine	ise-1 admin Logout Fe	edback
🚨 Authentication 🛛 🙍 Authorization 🔀	Profiling 🕜 Posture 👩 Client Provisioning 📄 Security Group Access 🦺 Policy Elements	
Dictionaries Conditions Results		
Results	Authorization Profile Authorization Profile * Name Vereless_Dot1X Description Profile For Wireless Endpoints That Have Authonticated With 802.1X * Access Type Access Type Access Accept  Common Tasks Common Tasks Common Tasks Authorization Auto Smart Port Riter-ID Auto Smart Port Riter-ID Auto Settings Setting Setting Setting Common Tasks Com	
😢 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.

cisco Id	lentity Services Engine					se-1 admin Logout	Feedback
💧 Home	Operations 🔻 Policy 🔻 Administra	ition 🔻				👓 Task Navigator	• 🕗
🛓 Authent	ication 🧕 Authorization 🔀 Prof	filing 🛛 💽 Posture	🔊 Client Provisioning	🚍 Security Group Access	🔒 Policy Elem	ients	
Authorizatio	n Policy						
Define the Auth	norization Policy by configuring rules based (	on identity groups and/c	r other conditions. Drag and	d drop rules to change the order	r.		
First Matched R	tule Applies 🔹						
Exceptions (	0)						
Standard							
Status	Rule Name	Conditions (identit	y groups and other conditio	ns)	Permissions	5	
	Black List Default	f Blacklist		t	then Blacklist_A	ICess Edit	-
	Profiled Cisco IP Phones	if Cisco-IP-Phone		t	then Cisco_IP_P	hones Edit	•
	Profiled Cisco APs	if Cisco-Access-Poi	int	t	then Cisco_APs	Edit	•
	Wired Dot1X Endpoints	if Wired_802.1X		t	then Wired_Dot	1X Edit	•
	Default		PermitAccess		Ir	nsert New Rule Above	-
Envo Pr							
[N	DEL						

#### 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.

ie the Auth Matched F	iorization Policy by configuring rules ba iule Applies •	ased on identity groups and/or	other conditions. Drag and drop rules to change Compound Conditions	the order.	
xceptions ( tandard	0)		. Wired_802.1X		
Status	Rule Name	Conditions (identity	gr Wireless 802.1X	Permissions	
	Black List Default	if Blacklist	Wireless_MAB	then Blacklist_Access	Edit   -
<b>~</b>	Profiled Cisco IP Phones	if Cisco-IP-Phone	Catalyst_Switch_Local_Web_Authentica WLC_Web_Authentication	then Gsco_IP_Phones	Edit   🕶
<b>~</b>	Profiled Cisco APs	If Cisco-Access-Poin	t	then Cisco_APs	Edit   🔻
	Wired Dot1X Endpoints	if Wired_802.1X		then Wired_Dot1X	Edit   +
× 🗹 ×	Wireless Dot1X Endpoints Default	f Any 🔶 a	n E	then AuthZ Profil	دې Done
ave Ri	aset	Select Condition	<b>O</b>		<b>₩</b> •

**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.

uli cis		dentity Services Engine								ise-1 admin	Logout	Feedback
á	Home	Operations 🔻 Policy 🔻	Administration	•						😶 Task N	avigator	-0
	Authen	tication 🧕 Authorization	🛃 Profiling	💽 Posture	词 Client Prov	visioning	🚊 Security Grou	up Access	🔒 Policy El	ements		
ê. eth	orizatio	n Doligu										
Define	the Aut	horization Bolicy by configuring	rules based on id	entity arouns and/	or other condition	ns. Drag and	dron rules to char	Standard				
Denne		- L - L	10/05 00500 0110	entry groups and,		ns, brag and				Q		
Hirst	Matched	Rule Applies *						<b></b>	1	<u>نۇ</u> ب		
► Ex	ceptions	(0)						😪 Blacklist_	Access			
~								Gisco_AP	;			
56	ariuaru							Gisco_IP	Phones			
	Status	Rule Name		Conditions (identi	ity groups and oth	her condition	s)	Q DenyAcc	55			
		Black List Default	if	Blacklist				😪 PermitAci	ess		Eď	lit   🖛
-	_							Wired_Do	61X			
	<u>~</u>	Profiled Cisco IP Phones	IŤ	Cisco-IP-Phone				Wireless_	Dot1X		Ed	it   ▼
		Profiled Cisco APs	if	Cisco-Access-Po	bint						Ed	lit   🕶
	<ul> <li></li> </ul>	Wired Dot1X Endpoints	if	Wired_802.1X							Ed	lit   🕶
	•	Wireless Dot1X Endpoints	if	Any 💠	and Wireles	s_802.1X				- 1	- Do	ne
	<b>~</b>	Default	if	no matches, then	PermitAcces						Ed	lit   🕶
Sa	/e	Reset				Select an	item 🤇	2 -	· -[-			

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

CIS	co Id	entity Services Engine		U.			ise-1 a	dmin Logout Fee
۵	Home	Operations 🔻 Policy 🔻	Administration 🔻				99 Ta	ask Navigator 🔫 🕗
4	Authenti	cation 🧕 Authorization	🛃 Profiling	💽 Posture	词 Client Provisioning	🚊 Security Group Access	🐥 Policy Elements	
uth	orization	a Policy						
efine	the Auth	orization Policy by configuring ru	iles based on ident	ity groups and/i	or other conditions. Drag an	nd drop rules to change the order		
irst N	Aatched R	ule Applies v			-			
Exc	eptions (	0)						
Sta	ndard							
				ker foll er				
	Status	Rule Name Black List Default	if B	arklist	ty groups and other condition	uris)	non Blackist Access	Edit La
	-	block bot boldart		dekiist			ICIT DUCKIST_ACCOST	Eurci
	<b>~</b>	Profiled Cisco IP Phones	if C	sco-IP-Phone		ti	nen Cisco_IP_Phones	Edit   🖛
	<ul> <li>Image: A set of the set of the</li></ul>	Profiled Cisco APs	if C	isco-Access-Pc	int	ti	nen Cisco_APs	Edit   •
		Wired Dot1X Endopints	if W	ired 802.1X		ti	nen Wired Dot1X	Edit I -
	_							Edit   -
	<b>~</b>	Wireless Dot1X Endpoints	if W	ireless_802.1X			nen Wireless_Dot1X	Edit   •

#### Process

Modify Authorization Policy to be Closed

1. Modify default rule

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

#### Procedure 1

Modify default rule

- Step 1: On the menu bar, mouse over Policy, and then select Authorization.
- Step 2: For the default rule, click Edit.

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

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

cisc	1. 0 Id	entity Services Engine					ise-1 admin Logout	Feedback
<u>(</u> ≜ ⊢	-lome	Operations 🔻 Policy 🔻 A	dministration 🔻				👓 Task Navigator 🔻	• 🕗
🚨 A	Authenti	cation 🧕 Authorization	🛃 Profiling 🛛 💽 Post.	re 👩 Client Provisioning	🔄 Security Group Access	🔒 Policy Elements		
Author Define the	rization he Auth	n Policy orization Policy by configuring rule	is based on identity groups	and/or other conditions. Drag a	nd drop rules to change the ord	ler.		
Those this	renoun	de Apples				2		
Exce	ptions (	0)			<b>⇔</b> •≡ :≡	- 60		
Stan	dard				Blacklist_Access			
					Gisco_APs			
	Status	Rule Name	Conditions (i	dentity groups and other condit	ions) 😪 Cisco_IP_Phones	ins		
	<ul> <li>Image: A set of the set of the</li></ul>	Black List Default	if Blacklist		C DenyAccess	Access	Edit	t   •
	<b>v</b>	Profiled Cisco IP Phones	f Cisco-IP-Ph	one	RermitAccess	Phones	Edit	tlv
-	_				Wired_Dot1X			
	<u>~</u>	Profiled Cisco APs	it Cisco-Acces	s-Point	Wireless_Dot1X	25	Edit	t∣▼
	<u>~</u>	Wired Dot1X Endpoints	if Wired_802.1	х		otix	Edit	t I 🕶
	<b>Z</b>	Wireless Dot1X Endpoints	if Wireless_803	2.1X		Dot1X	Edit	t   •
		Default		nen PermitAccess 👄			Dor	ne
Save	Re	set		PermitAccess	○ = 4			

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

A Home Operations  Policy Administration Administration Policy Po	<b>, </b>
💶 Authentication 🛛 Authorization 🔀 Profiling 🕐 Posture 🐻 Client Provisioning 😁 Security Group Access 💦 Apolog Elements	
Authorization Dalicu	
Autorization zavori e voice. Define the autorization Policy by configuring miles based on identity groups and/or other conditions. Drag and drop miles to change the order.	
Control of the Analysis of Control of the Control o	
TISLIMATURE ADJARS Y	
Exceptions (0)	
Standard	
Status Rule Name Conditions (identity groups and other conditions) Permissions	
Black List Default if Blacklist then Blacklist Elected Electronic State	c   •
Profiled Cisco IP Phones If Cisco-IP-Phone then Cisco_IP_Phones Education	t I 🕶
Profiled Clsco APs If Cisco-Access-Point than Clsco_APs Ex	t I 🕶
Wired Dot1X Endpoints if Wired_802.1X then Wired_Dot1X End	t I 🕶
Wireless Dot1X Endpoints if Wireless_802.1X then Wireless_Dot1X Endpoints	t I 🕶
Default if no matches, then DenyAccess	t I 🕶
Save Reset	

#### 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.

trics Active End; 3 —	oints		Active Guests 0 —	Posture 09	Compliance	Mean Ti O.C	ime To Remediate ) sec. —	Profiled E	ndpoints —
Name ise-1 ise-2	Utilizat CPU	Memory semantic semantic	Letency	24) * Identity Stores (PJP) Nane Tritemal Endpoints AD	24h Authentications allintinailleallea all	24h ¥ . 175 17	24h ¥ Authentications Total 200 Distribution By: El Identity Group El Location El Device Type	Lart 24 Hours	24h *
hentication Fail. otal <b>9</b> Istribution By: Ilse-1	re Illuttoutto Last 24 Ho	II Luurs L	CT III ast 60 Minutes 2	Profiled Endpoints Unique 2    Distribution by: E P1H E Profile E Identity Group	14 Hours Last 60 I No Data Available	Minutes 3 2	Posture Compliance Passed 0% MTTR 0.0sec Distribution of Failu E OS E Reason	2 Last 24 Hours <b>re by:</b> No Data Avai No Data Avai	Last 60 Minutes Iable

#### 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 🔻 Adm	istration 🔻	😁 Task Navigator 👻 🕗
🛃 Authentication 🛛 🧕 Authorization 🗌 🔀	Profiling 👩 Posture 👼 Client Provisioning 📑 Security Group Access 🚽	Policy Elements
Profiling ← ■ TH > Profiling Polices	Porfiler Policy       * Name Apple-Pad Description         * Name Apple-Pad Description       Policy Enabled         * Norme Certainty Factor 20       (Valid Range 1 to "Exception Action NONE *         * Network Scan (NMAP) Action NONE *       *         © Create Matching Identity Group       © Use Hierarchy         * Use Hierarchy       *         # Rules       If Condition Apple-IPadRule2Check2 ◆ Then Certainty Factor Increases         If Condition (Apple-IPadRule1Checkd_AND Apple-MacBo ◆) Then Certainty Factor Increases	Polcy for Apple Pads a 65535) • 20

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

#### Procedure 3

Add a custom profile

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

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

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

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

Identity Services Engine     Identity Services Engine     A Home Operations      Polcy      Admit     Authentication     Authentication	nistraton • Profiling 🕐 Posture 🕞 Client Provisioning 📑 Secur	ise-1 admin Logout Feedback 99 Task Navigator = 🕐 rity Group Access 🔒 Policy Elements
Profiling (	Polier Policy Lis > New Prelier Policy Profiler Policy * Name Gooo-Gus Policy Enabled  * Minimum Certainty Factor * Network Scan (NMAP) Action NONE * Network Scan (NMAP) Action NONE * Network Scan (NMAP) Action Use Heardry * Parent Policy Use Heardry * Parent Policy NONE Rules If Condition Conditions  Then Certainty Factor Select Attribut	DHCP

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.

cisco Identity Services Engine	ise-1 admin Logout Feedback
🛕 Home Operations 🔻 Policy 🔻 Adm	inistration 🔻 😐 Task Navigator 👻 🕗
🛓 Authentication 💿 Authorization 🔀	Profiling 👩 Posture 🐻 Client Provisioning 🔄 Security Group Access 🔥 Policy Elements
Profiling ↓ ↓ Profiling Policies ↓ ↓ Profiling Policies	Policy Policy Las New Polifier Pelicy Profiler Policy * Name Gisco-Glus Description Policy Enabled  Policy Ena
	Rules       If Condition       DHCP_dhcp-class-identifier_CONTAINS_Cisco.       20       20       Submit       Cancel

#### **Procedure 4**

**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.

cisco Identity Serv	vices Engine	ise-1
💷 🚔 🖻		Launch Interactive Viewer 🎦
RADIUS Authenticatio	on Details	
Showing Page	e 1 of 1   First Prev Next Last	Goto Page: Go
AAA Protocol > RAD	DIUS Authentication Detail	-
RADIUS Audit Session AAA session ID : Date :	ID: 0.4052C0500000001B4834BC6 ise-1/112681645/20 December 13,2011	
Generated on Decembe	er 13, 2011 1:44:33 PM PST	
	Actions Troubleshoot Authentication <sup>124</sup> <u>View Diagnostic Messages</u> Audit Network Device Confluxat View Network Device Confluxat View Server Configuration Cha	ation 12 Ilion 12 Inges
Authentication Summar	ary	
Logged At: RADIUS Status: NAS Failure:	December 13,2011 11:42:30.740 AM Authentication succeeded	
Username: MAC/IP Address: Network Device:	E8:04:62:EA:83:90 E8:04:62:EA:83:90 DefaultNetworkDevice : 10:5:44.5 : GigabitEthemet1/0/1	
Allowed Protocol: Identity Store:	Default Network Access	
SGA Security Group: Authentication Protocol	PermitAccess	
1		

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		
naged At:	December 13 2011 11:42:30 740 AM	٦.
Iccurred At	December 13 2011 11:42:30 740 AM	
Server	ise-1	
suthentication Method:	mah	
AP Authentication Method	Lookup	
AP Tunnel Method		
Isemame:	E8:04:62:EA:83:90	
ADIUS Username	F8 04 62 FA 83 90	
alling Station ID:	E8:04:62:EA:83:90	
ramed IP Address:		
Ise Case	Hest Lookup	
lationsk Davida:	DefaultNatworkDevice	
latwork Device Groune:	Device Type#Landowner	
IAS ID Addrage:	10.5 A/5	
AS Identifier	1000/7402	
AS Identifier.	60101	
AS FUIL	Sinki Sikawati Oti	
AS FULID.	Support Content of Con	
Mo Fort Type.	Enternet	
alowed Protocol.	Cell Charles	
lentitu Steen	Call Check	
entity store.	Develation	
uthonization Profiles: ctive Directory Domain:	PermitAccess	
dentity Group:		
Jlowed Protocol Selection Matched R	ule: MAB	
lentity Policy Matched Rule:	Default	
elected Identity Stores:	Internal Endpoints	
uthorization Policy Matched Rule: GA Security Group:	Default	
AA Session ID	ise-1/112681645/20	
udit Session ID:	DARS2CDSDDDDDD1B4E848C6	
unnel Details:		
	service.tvnettCall Check	
lisco-AVPairs:	audit-session-id=0A052C050000001B4B84BC6	
Other Attributes:	ConfigVersionId=64, DestinationPort=1645, Protocol=Radius, Framed-MTU=1500, EAP- Key-Namez, PMRSessionID=ADS/2C5000000001848246C5, AudPointMACAAdMorss=EB-04-62-EA-83-90, Device Type=Device Type#AII Device Types, Location=Location#AII Locations, Device IP Address=10.5.44.5, Called-Station- ID=EC:CR9.27.49.01	
fosture Status:	NotApplicable	
IPC Status:	100 prisons	

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.

cisco Identity Services Engine			ise-1 admin Logout Feedback					
🛕 Home Operations 🔻 Policy 🔹 Administration 🔹 🤒 😶 Task Navigator 🔹								
Authentications 🤯 Endpoint Protection S	iervice 💆 Alarms 📑 Reports 💊	Troubleshoot						
Favorites Shared Catalog System								
Reports  AAA Protocol  Alowed Protocol	AAA Protocol	Clear Filter						
Server Instance	Report Name	<ul> <li>Type</li> </ul>	Modified At					
Endpoint	AAA Diagnostics	System Report	Mon Feb 27 23:41:09 PST 2012					
Failure Reason	C Authentication Trend	System Report	Mon Feb 27 23:41:09 PST 2012					
Network Device	C RADIUS Accounting	System Report	Mon Feb 27 23:41:09 PST 2012					
User	RADIUS Authentication	System Report	Mon Feb 27 23:41:09 PST 2012					
Security Group Access	Run - Add To Favorite Delete		Reset Reports					
Session Directory	Last 30 Min							
Posture	Last Hour s of type 'System	Report', hover mouse over	the 'Report Name' to view the report description.					
Endpoint Protection Service	Last 12 Hours Today Yesterday Last 7 days Last 30 days Query And Run	n report for today. 'Run' button to select addit	ional options.					

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	<u>Clear</u>
Identity Group:		Select	<u>Clear</u>
Device Name:		Select	<u>Clear</u>
Device IP:		Select	Clear
Device Group:		Select	Clear
Allowed Protocol:		Select	Clear
Identity Store:		Select	Clear
Server:		Select	Clear
Failure Reason:		Select	Clear
SGASGT:		Select	Clear
Show only SGA SGT Assignments:			
Include SGA Environment:			
Radius Audit Session ID:			Clear
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			



**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.

cisco Identity Services Engine			ise-1 admin Logout Feedback
💧 Home Operations 🔻 Policy 🔻 Administ			😁 Task Navigator 👻 🥹
Authentications 🔯 Endpoint Protection Ser	vice 💆 Alarms 🧮 Reports 🍾 Troubleshoot		
Favorites Shared Catalog System			
Reports AAA Protocol Alowed Protocol	Endpoint		
Server Instance     Endpoint	Report Name     Endpoint MAC Authentication Summary	<ul> <li>Type</li> <li>System Report</li> </ul>	Modified At Mon Feb 27 23:41:09 PST 2012
Failure Reason     Network Device     User	Endpoint Profiler Summary     Endpoint Time To Profile     Ton N Authentications By Endpoint Calling Station ID	System Report System Report	Mon Feb 27 23:41:09 PST 2012 Mon Feb 27 23:41:09 PST 2012 Mon Feb 27 23:41:09 PST 2012
Security Group Access     Session Directory	C Top N Authentications By Machine	System Report	Mon Feb 27 23:41:09 PST 2012
Posture     Endpoint Protection Service	Today Yestinday Last 30 days Covery And Run	er the 'Report Name' I	to view the report description.

**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 :	7C:6D:62:DE:05:8F	Dec 8, 2011 12:11 PM	Apple-Device		
Endpoint Policy :	Apple-iPad				
Matched Rule :					
Certainity Metric :	30				
Endpoint Matched Policy :	Apple-iPad				
Endpoint Action Name :					
Identity Group :	Apple-iPad				

#### Figure 4 - Endpoint Details

Endpoint > Endpoint Profiler Detail						
Generated on December 13, 20	11 1:59:11 PM PST					
Endpoint Session time : Not	Applicable					
Endpoint Details						
Endpoint Static Assignment : Endpoint Source : Endpoint OUI : Endpoint Host Name :	Apple, Inc					
Endpoint Subnet : Endpoint NAD Address : Endpoint VLAN : Endpoint FQDN :	10.4.46.66					
Endpoint Nameserver : Endpoint Property :	CPMSessionID=0s042e41000000494ee13838 StaticAssignment=false					
	Location#All Locations Location#All Locations cisco-awpair=audit-session-id=0.a042e41000000494ee13838					
	Caling-station-ID=7 < 50-62-26-05-67 DestinationPort=1812 AcsSessionID=ise-1/112681645/7					
	giaddr≕10.4.16.6 Device Type≕Device Type#All Device Types Senice-Tyre=Framed					
	NAS-Identifier=WLC-2 TimeToProfile=25					
	LastNmapScan ImmeU dhcp-client-identlifier=011:7c:6d:62:de:05:8f StaticGroupAssignment=false					
	dhcp-requested-address=128.107.108.109 AuthenticationMethod=MSCHAPV2 Eachutheatister=EAD Method ADA					
	EapAintenintation=CAR-inscript=tz NetworkDeviceName=DefaultNetworkDevice NAS-Port-Type=Wireless - IEEE 802.11					
	op=BOOTREQUEST PostureAssessmentStatus=NotApplicable IdentityGroupID=3e7@e00-21db-11e1-aebd-005056a90008					
	Total Certainty Factor=30 User-Name=patjones					
	craderu.U.U.U AuthenticationIdentityStore=AD1 dhcp.parameter.reguest-list=1					
	3 '' ' 6					
	15 119 252					
	MatchedPolicyID=17679880-116b-11e1-ae1c-0050569e2146 DestinationIPAddress=10.4.48.41					
	ADDomain=cisco.local NmapScanCount=0					
	dhcp-message-type=DHCPDISCOVER htype=Ethemet (10Mb) E-dPuintMc didexer20 CD S2 DE 05 PE					
	EndFontMMA_Address/C-5D-52-DE-US-5F ServiceSelectionMatchedRule=Wireless-Dot1X PortalUser=					
	EndPointMatchedProfile=Apple-Device RequestLatency=9					
	AutiState=Authenticated Ariespace-Wian-Id=1					
	hlen=6 hops=2 hops=28A iBod					
	FirstCollection=1323375086686 EndPointPolicyID=f7679880-116b-11e1-ae1c-00505659e2146					
	SelectedAccessService=Detault Network Access secs=0 AuthorizationPolicvMatchedRule=Default					
	IdentityPolicyMatchedRule=Default MessageCode=5200					
	DeviceregistrationStatus=U SelectedAuthorizationProfiles=PermitAccess IdentityAccessRestricted=false					
	SelectedAuthenticationIdentityStores=AD1 flags=0x0000 chaldra=Z_c6H62_de/D5/8f					
	viadd=0.0.0 Response=(User-Name=patjones; State=ReauthSession:0a042e41000000494ee13838;					
	Class=CACS:0aU/2e41000000494e1383ise-1/11281164/7; Termination-Action=RADIUS-Request, MS-MPPE- Senk/Sey=437:0:1b 639.6b:18.0b.01.91.cc a89.44.25 as 6fb er687c.45.98.365.91.b 5fa.367.04.42.2e.0; MS-MPPE- Benck/Sey=610:0:16.46.9b:24.se.9e.c1.659.86.56.56.27.4e.0b;55.47.46.24.1b;se.91.e7.45.44.1c.95.11					
	Location=Location#All Locations Deation=Location=Location#All Locations PolicyVersion=1 PolicyVersion=1					
	Dence in Audiess-104.40.05 NmapSubnetScanD=0 Called-Station-ID=1c-17-d3-cb-48-50.WLAN-Data					

#### Procedure 7

#### **Create device-type reports**

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

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

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

Step 3: Select RADIUS Authentication.

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

a) Home Operations ▼ Policy ▼ Administra	tion v		••	* Task Navigator *
avorites Shared Catalog System	e 💆 Alams 📄 Repurts 💊	Troubleshout		
Reports	AAA Protocol			
Allowed Protocol	Filter. Go C	Slear Filter		
Server Instance	Report Name	<ul> <li>Type</li> </ul>	Modified At	
Bidpoint	C AAA Diagnostics	System Report	Mon Feb 27 23:41:09 PST 2012	
Pailure Reason	C Authentication Trend	System Report	Mon Feb 27 23:41:09 PST 2012	
Network Device	C RADIUS Accounting	System Report	Mon Feb 27 23:41:09 PST 2012	
User	RADIUS Authentication	System Report	Mon Feb 27 23:41:09 PST 2012	
Security Group Access	Run - Add To Favorite Delete			Reset Reports
Session Directory  Posture Endpoint Protection Service	Last 30 Min Last Hour s of type 'System F Last 12 Hours Today Yesterday	Report", hover mouse over n report for today. 'Run' button to select addi	the 'Report Name' to view the repo tional options.	rt description.

**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.

Search		~
		523
Search Filter:	Search	
Criteri	a	
O Blackli	st	▲
C Guest		
O Profile	d	
O Profile	d:Android	
💿 Profile	d:Apple-iPad	
O Profile	d:Apple-iPhone	-
	Apply Cancel	
Sele	ect Identity Groups	

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

Figure 5 - Sample report

AAA Protocol > Query and Run > RADIUS Authentication									
Showing Page	1 of 1					Goto Page:	Go		
AAA Protocol > RADIUS Authentication									
Identity Group : Profiled Apple-iPad Authentication Status : Pass or Fail Date : November 13,2011 - December 12,2011 ( <u>Last 30.Minutes   Last Hour   Last 12 Hours   Today   Yesterday   Last 7 Days</u>   Last 30 Days )									
Generated on December 13, 2011 2:28:15 PM PST									
✓=Pass X=Fail 4=Click for details 3=House over item for additional information									
Logged At	RADIUS N Status Fa	IAS ilure Details	Event	Username	MAC/IP Address	Allowed Protocol	Service Type	Authentication Method	Authentication Protocol
Dec 8,11 4:38:00.576 P	м 🖌	୍	Authentication succeeded	patjones	7C:6D:62:DE:05:8F	Default Network Access	Framed	dot1x	PEAP (EAP-MSCHAPv2)

# Appendix A: Product List

## **Network Management**

Functional Area	Product Description	Part Numbers	Software	
Identity Management	Cisco Identity Services Engine Virtual Appliance	ISE-VM-K9=	1.1.1.268	
	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) IP Base
	Cisco Catalyst 4500 E-Series Supervisor Engine 7L-E	WS-X45-SUP7L-E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+ ports	WS-X4648-RJ45V+E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+,UPoE ports	WS-X4748-UPOE+E	
Stackable Access Layer Switch	Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-48PF-S	15.0(1)SE2
	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 IP Base
	Cisco Catalyst 3560-X Series Standalone 24 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-24P-S	
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
Stackable Access Layer Switch	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-48FPD-L	15.0(1)SE2 LAN Base
	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-48FPS-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-24PD-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-24PS-L	
	Cisco Catalyst 2960-S Series Flexstack Stack Module	C2960S-STACK	

### **Wireless LAN Controllers**

Functional Area	Product Description	Part Numbers	Software
On Site, Remote Site, or Guest	Cisco 5500 Series Wireless Controller for up to 500 Cisco access points	AIR-CT5508-500-K9	7.2.110.0
Controller	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 IF CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY 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 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)