# **Newer Design Guide Available**

Cisco Smart Business Architecture has become part of the Cisco Validated Designs program. For up-to-date guidance on the designs described in this guide, see http://cvddocs.com/fw/Aug13-142 For information about the Cisco Validated Design program, go to http://www.cisco.com/go/cvd







# BYOD—Virtual Desktop Access Deployment Guide

SMART BUSINESS ARCHITECTURE

February 2013 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 February 2013 is the "February 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 10.5.204.5 255.255.2

## **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.

February 2013 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
Deploying Cisco Identity Services Engine	5
Enabling Visibility to the LAN	13
Enabling Visibility to the Wireless Network	24
Enabling Authorization	
Enabling Authorization for Wired Endpoints	
Enabling Authorization for Wireless Endpoints	
Enabling Authorization Policy	
Enable Device Provisioning	43
Deploying Digital Certificates	43
Configuring Self-Provisioning	
Enabling Security Group Access	
Monitoring Network Access	

Appendix A: Product List	0
Appendix B: Changes	)3

# 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

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 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 these devices, limit connection to approved devices, or make access to network resources easier for these 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—Identity and Authentication Deployment Guide
- BYOD—Advanced Guest Wireless Access Deployment Guide
- BYOD—Remote Mobile Access Deployment Guide
- · BYOD—Internal Corporate Access Deployment Guide

# **Business Overview**

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

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

This guide is the first step in deploying an architecture for accommodating users who bring their own devices to access the network. The first phase is to allow users to access the network with their personal device using their existing network credentials. After authentication, the device is granted access to the portions of the network required to access the Virtual Desktop Infrastructure (VDI). VDI allows a client to access a virtual desktop hosted in the data center. This allows the user to access the same desktop from a variety of different endpoints. This simplifies network policies by providing a common environment for users and then applying policy centrally in the data center. This guide assumes that the VDI environment has already been installed in the data center and the clients are configured. The second phase is to provision the device with a digital certificate and network configuration prior to gaining network access. Once provisioned, the device has full network access. The next phase is to limit access to the network based on the user's Active Directory group membership by using both standard access lists as well as using Security Group Access.

# **Technology Overview**

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

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

In addition to using Cisco ISE for authentication, you can use Cisco ISE to profile devices to determine the specific type of devices that are accessing the network. This is done by examining network traffic for certain criteria based on certain characteristics. Cisco ISE currently has probes for Dynamic Host Configuration Protocol (DHCP), HTTP, RADIUS, Domain Name System (DNS), Simple Network Management Protocol (SNMP) traps and queries, 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 data sent via RADIUS and can identify the device based off of the data in the RADIUS packet. For example, Cisco IP phones are identified by a 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 and authorization on the network. An organization's goals might be met by implementing only some of the overall functionality of Cisco TrustSec and a successful deployment does not require all three modes to be deployed. This document covers the deployment phases of monitor mode and low-impact mode both at the headquarters site and the remote sites, with Cisco ISE being centralized in the data center. To support BYOD, the deployment uses web-based authentication for devices that are not 802.1X-capable. The deployment in use deploys two features within Cisco IOS on the switches in the access layer at both the headquarters sites as well as the remote sites. The first is MAC Authentication Bypass (MAB), which authenticates the device on the switch port by the MAC address. Monitor mode logs the MAC addresses that connect and grant access to any device that connects. The second feature is 802.1X open mode, which allows the switch port to give unrestricted access to the network even though authentication and authorization have not been performed. This enables the deployment of identity without affecting existing connectivity. This phased approach allows you to prepare for moving to another mode in the future. In addition to these features, this deployment also deploys the Security Group Access (SGA) features of Security Group Tags (SGT) and Security Group Exchange Protocol (SXP) in low-impact mode in order to enforce the access policy. Packets for a particular group are marked with an SGT in the TrustSec header. SXP is used to pass tagged packets across devices that do not support marking SGTs by binding the IP address of the device to the SGT and then passing the packets along to a device that does support SGTs. Devices then enforce a security policy using these tags. In the organization, these switch configurations will be managed by Cisco Prime LAN Management Solution (LMS) 4.2 and the new TrustSec Work Center, Cisco Prime LMS simplifies the deployment of identity by performing a network-readiness assessment for an identity deployment, providing templates for the various modes-monitor, low-impact, closedand providing a step-by-step wizard to configure the various components required.

You integrate Cisco ISE into the wireless network by using Cisco ISE as the AAA server for wireless 802.1X authentication, authorization, and accounting. After successful authentication, the user is redirected to the device registration portal in order to initiate the provisioning process for the device. You configure this on every wireless LAN controller (WLC) in the network, at both headquarters and the remote sites that have local controllers. The one exception is for the controller used for guest access.

#### Figure 1 - BYOD overview



# 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

#### Process



Deploying Cisco Identity Services Engine

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

#### Procedure 1

Set up initial primary engine

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

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

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

#### Step 3: Enter DNS information.

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

#### Step 4: Configure time.

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



#### Tech Tip

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

http://www.cisco.com/en/US/docs/security/ise/1.1/cli\_ref\_guide/ ise\_cli\_app\_a.html#wp1571855

Step 5: Configure an administrator account.

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

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

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

Application bundle (ise) installed successfully

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

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

The primary engine is now installed.

#### Procedure 2

Set up the remaining engines

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

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

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

#### **Procedure 4**

**Configure Cisco ISE deployment nodes** 

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

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

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

• Home     Operations     ▼     Policy     ▼     Admin	This node is in Standalone mode. To register other nodes, you must first edit this node and change its Administration Role to Primary Netv	ise-1 admin Lopout Peedback
Deployment Licensing Certificates Loggin	g Maintenance Admin Access Settings	
Deployment	Deployment Nodes	Selected 0   Total 1 🛭 🏀 🎡 🖕
Server	🖊 Edit 🔯 Register 🔀 Export 🔂 Import	» Show All 🔹
	Hostname 🔺 Node Type Pers	sonas Role(s)
	ise-1 ISE Adm	ninistration, Monitoring, Policy Service STANDALONE

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

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

cisco Identity Services Engine			is	e- <mark>1 a</mark> dmin Logout Feedback
💧 Home Operations 🔻 Policy 🔻	Administration 🔻			👓 Task Navigator 👻 🚷
😽 System 🛛 👰 Identity Management	📰 Network Resources 🛛 🛃	Guest Management		
Deployment Licensing Certificates	Logging Maintenance Admir	n Access Settings		
Deployment	Deployment Nodes			
	<u>ي</u>			Selected O   Total 1   🚳 🖕
Deployment	Create Node Group	🕞 Export 🛛 🚱 Import	≫ Show All	- 6
**	Hostname	<ul> <li>Node Type</li> </ul>	Personas	Role(s)
	ise-1	ISE	Administration, Monitoring, Policy S	ervice 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: Select HTTP, use the default parameters, and then click Save.

HTTP		
	Interface GigabitEthernet 0	-
	Description HTTP	
		_

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

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

cisco Identity Services Engine		ise-1 admin Logout Feedback
🛕 Home Operations 🔻 Policy 🔻 Admin	nistration 🔻	👓 Task Navigator 👻 🕗
🔆 System 🦉 Identity Management	Network Resources 🛛 🛃 Guest Management	
Deployment Licensing Certificates Loggi	ing Maintenance Admin Access Settings	
Deployment	Deployment Nodes	
<b>♦•</b> = 1		Selected 0   Total 1   🍪 🖕
▼ Seployment	🖉 Edit 🔯 Register 👻 🎲 Export 🐲 Import 🔉 Show	All 🔻 😽
A ISE-Group	Hostn, Register an ISE Node e Personas	Role(s)
	ise-1 Register an Inline Posture Node Administration, Monitor	ing, Policy Service PRI(A), PRI(M)

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

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

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

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 Logg	ng Maintenance Admin Access Settings
Deployment	Deployment Nodes List > Configure Node
<b>€-</b> ■ 1 ⊗-	Register ISE Node - Step 2: Configure Node
A 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 Be-1
	Policy Service
	Enable Session Services
	Include Nade in Node Group <none> + (1)</none>
	Enable Profiling Service
	Submit Cancel

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

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

aliulia CISCO Identity Services Engine 1841	admin Logout Feedback
🛕 Home Operations 🔻 Policy 🔻 Administration 💌 🧧 🚥	Task Navigator 👻 😢
👷 System 🛛 🖉 Identity Management 📲 Network Resources 🛛 🛃 Web Portal Management	
Deployment Licensing Certificates Logging Maintenance Admin Access Settings	
Deployment ↓ ★ Deployment ↓ ★ Deployment	
General Settings Profiling Configuration	
Hostname <sub>(se-1</sub> FQCN ise-1.cisco.local	
IP Address 10.4.48.41	
Nade Type Identity Services Engine (ISE)	
Personas	
Administration     Role PRIMARY	
Monitoring Role SECONDARY Other Monitoring Node	
Policy Service	
Enable Session Services	
Crable Profiling Service     Save Reset	

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

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

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

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

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

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	g Maintenance Admin Access Settings	
Deployment	Deployment Nodes List > Configure Node	
	Register ISE Node - Step 2: Configure Node	
Merce State Sta		
	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     ID	
	☑ Enable Profiling Service	
	Submit Cancel	

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

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

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

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

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

✓	▼ HTTP		
		Interface GigabitEthernet 0	•
		Description HTTP	

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

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

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

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

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



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

#### **Procedure 5**

Install Cisco ISE license

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



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 🔻 Adm	inistration 🔻	👓 Task Navigator 👻 🚷
🔆 System 🛛 🖉 Identity Management 📲	Network Resources 🛃 Guest Management	
Deployment Licensing Certificates Log	iging Maintenance Admin Access Settings	
License Operations	Current License File  * License File C:Downloads\u00e4se-base-license.lic Browse_ Cancel	

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

#### Procedure 6

#### **Configure network devices in Cisco ISE**

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

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

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



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





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.

cisco Identity Services Engine		ise-1 admin Logout Feedback
💧 Home Operations 🔻 Policy 🔻 Admi	nistration 🔻	\varTheta \varTheta Task Navigator 👻 🚷
🔆 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       cisco.local              • Identity Store Name       AD1         One or more nodes may be selected for Join or Leave operations. If a node is joined the operation is required before a rejoin. Select one node for Test Connection.            @ Join       Eleave       @ Test Connection *             @ Join          @ Leave       @ Test Connection *             @ Password:          @ Cancel </th <th>nain</th>	nain

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

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

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



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

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

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

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

cisco Identity Services	
	Select Directory Groups × admin Logout Feedback
💧 Home Operations 🔻	This dialog is used to select groups from the Directory. Click Retrieve Groups to read directory. 🕴 Task Navigator 👻 😢
🔆 System 🛛 😤 Identity Ma	Use * for wildcard search (i.e. admin*). Search filter applies to group name and not the fully qualified path.
Identities Groups	Domain: cisco.local
	Filter: * Retrieve Groups Number of Groups Retrieved: 64 (Limit is 100)
External Identity Sources	Name
<b>◆-</b> ■ '≣	Cisco Incal/Users/DHCP Artministrators
Certificate Authentication Profile	Cisco.local/Users/DHCP Users
Active Directory	cisco.local/Users/Denied RODC Password Replication Group
EDAP LDAP	cisco.local/Users/DnsAdmins
RADIUS Token	cisco.local/Users/DnsUpdateProxy
RSA SecurID	cisco.local/Users/Domain Admins
	Cisco.local/Users/Domain Computers
	Cisco.local/Users/Domain Controllers
	Cisco.local/Users/Domain Guests
	Cisco.local/Users/Domain Users
	cisco.local/Users/Enterprise Admins
	cisco.local/Users/Enterprise Read-only Domain Controllers
	cisco.local/Users/Group Policy Creator Owners
	⊂ cisco.local/Users/POS-Users
	OK Cancel

Step 12: Click Save Configuration.

**Procedure 8** 

**Disable IP Phone authorization policy** 

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

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

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

🛕 Home Operations 🔻 Policy 🔻 Adm	inistration 🔻	ee Ta	sk Navigator 🔫 🕗
🔺 Authentication 🛛 🧕 Authorization 🛛 🤀	Profiling 👰 Posture 🗔 Client Provisioni	ing 🔄 Security Group Access 💦 🐥 Policy El	ements
uthorization Policy			
fine the Authorization Policy by configuring rules b	ased on identity groups and/or other conditions. Dra	ag and drop rules to change the order.	
st Matched Rule Applies			
Exceptions (0)			
Standard			
	Conditions (identity groups and other co	anditions) Permissions	
Status Rule Name			Edit   👻
	if Blacklist	then Blacklist_Access	Luic 1 -
Black List Default		_	Done
Black List Default	if Blacklist	_	

#### Process

Enabling Visibility to the LAN

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

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



**Configure MAC Authentication Bypass** 

MAC Authentication Bypass (MAB) allows you to configure specific machine MAC addresses on the switch to bypass the authentication process. You configure MAB to allow any MAC address to authenticate for both the wired and wireless networks.

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

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

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

cisco Identity Services Engine		ise-1 admin Logout Feedback
🏠 Home Operations 🔻 Policy 🔻 Adminis	tration 🔻	👓 Task Navigator 👻 🕗
🚨 Authentication 🛛 🧕 Authorization 🔀 P	offing 🛛 🧑 Posture 🕞 Client Provisioning 🔄 Security Group Access 🔒	Policy Elements
Authentication Policy Define the Authentication Policy by selecting the protoc Policy Type O Simple O Rule-Based	ols that ISE should use to communicate with the network devices, and the identity sources           Wired_MAB         allow protocols         Allowed Protocol : Default Netwool         and	
Dot1X : If	Add All Conditions Below to Library	v
Default Rule (If no match) : a	Condition Name Expression	OR 谷 🗸
		Add Condition from Library Delete

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

Step 4: Choose Wireless\_MAB, and then click anywhere to continue.

CISCO Identity Services Engine	Compound Condition	ise-1 admin Logout Feedback				
🏠 Home Operations 🔻 Policy 🔻 Administration 🔻	🔶 🔲 📜 👘	🕫 Task Navigator 👻 😢				
Authentication 💿 Authorization 🔀 Profiling 🥂 Posture	Wired_MAB	roup Access				
Authentication Policy	Image: Section of the protocols that ISE should use to mple @ Rule-Based     Wred_MAB     Image: Section of the protocols that ISE should use to mple @ Rule-Based       Image: Section of the protocols that ISE should use to mple @ Rule-Based     If     Wired_MAB					
	Constants       Policy       Administration         Constants       Policy       Policy         Constants       Policy       Policy         Constants       Policy       Policy         Policy       Policy       Policy         Constants       Policy       Policy         Policy       Policy       Policy					
	Switch_Local_Web_Authentication	a the identity sources that it should use for authentication.				
hentication Policy          w Wrefess_002.1X         w Wrefess_002.1X         w Wrefess_002.1X         w Wrefess_002.1X         w Smple         w Rule-Based         w WLC_Web_Authentication         w WLC_Web_Authentication         w WLC_Web_Authentication         w WLC_Web_Authentication         w WLC_Web_Authentication         wull         w WLC_Web_Authentication         wull         web_authentication         wull         wull         web_authentication         wull         wull         web_authentication         wull         wull						
MAB : If Wired_MAB <		fault Netw📀 and 🕨 🚇 Actions 💌				
Dot1X : If Add Al Conditions	Wred_MAB     Wred_MAB					
Condition Name		OR 💌				
Default Rule (If no match) : all Wired_MAB		OR 🙀 🎽				
Select Condition	C					
	[]					

**Step 5:** For the MAB policy, click the black triangle to the right of the and.... This brings up the identity store used for the MAB rule.

cisco Identity Services Engine		ise-1 admin Logout Feedb
🏠 Home Operations 🔻 Policy 🔻	Administration 🔻	👓 Task Navigator 👻 😢
Authentication  Authentication  Authentication  C Profiling  Posture  C Clent Provisioning  C Security Group Access  Policy Elements  Authentication  Policy  Policy Policy Policy  Policy  Policy  Policy Policy Policy  Policy		
Authentication Policy		
	protocols that ISE should use to communicate with the network devices, and the identity sources that it should use i	for authentication.
Authentication Policy         Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.         Policy Type O Simple O Rule-Based         Image: If Wired_MAB       alow protocol: Allowed Protocol: Default Netwoo and         Image: I		
Default	: use Internal Endpoints 💠	🚔 Actions 💌
Dot1X	: If Wired_802.1X  allow protocols Allowed Protocol : Default Netwo and	👙 Actions 💌
Default Rule (If no match)	: allow protocols Allowed Protocol : Default Netw 📀 and use identity source : Internal Users 💠	🙀 Actions 🔻

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

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

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

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





**Configure 802.1X for wired users** 

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

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

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

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

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

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

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

Home Operations 🔻 Policy 🔻 Adminis	ation 🔻	😶 Task Navigator 👻 🌔
🛃 Authentication 🛛 🧕 Authorization 🔀 F	offing 🕐 Posture 🕞 Clent Provisioning 📄 Security Group Access 🔒 Policy Elements	
thentication Policy ne the Authentication Policy by selecting the proto y Type O Simple O Rule-Based	is that ISE should use to communicate with the network devices, and the identity sources that it should u	ise for authentication.
MAB : If	Wired_MAB 🔶 allow protocols Allowed Protocol : Default Netw 2 and 🖡	👾 Actions 💌
Wired-Dot1X : If	Wired_802.1X 🔶 allow protocols Allowed Protocol : Default Netwoo and 🖕	🖗 Actions 🔻
Default	: USP Internal Users  Identity Source AD1 Options If authentication failed Reject	🎡 Actions 🔻
Default Rule (if no match) : a	W prote         If user not found [Reject *           If process failed [Drop *           Note: For authentications using PEAP_HAST 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.	🖗 Actions 👻

#### **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.



**Tech Tip** 

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

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

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

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

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

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

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

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

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

ululu Cisco Prime	adm	in I Log Out I About I Sitema	ap I Feedback I Help 🕞 📕 Search	
CISCO LAN Management Sol	ation 🔹 My Menu 🔻 Monitor	▼ Inventory ▼ Configuratio	n 🔻 Reports 🔻 Admin 🔻 Work Ge	🕨 🔮 🚖
Work Centers > TrustSec > RADIUS Con				07 Jun 2012, 13:13 PDT
Navigator	Configure RADIUS			
Dashboard			ntication and authorization before configu	ring identity on the
Getting Started	devices. The following workflow fa	cilitates RADIUS server configuration	on and make the devices radius enabled.	
Readiness Assessment	Select Devices			Ś
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 mult	iple RADIUS servers.	
	RADIUS Group Name ISE-Group	)	Shared Key	
		Ver	ify Shared Key	
		ervers that will be part of this RAD 5, the second as the secondary an	IUS group. The order of addition is importa id so on.	nt as the first
	/ Edit 🗙 Delete 🛛 🗹	Add Ϋ Filter		
	Server Name or IP Address	Authentication port	Accounting port	
	0 10.4.48.41	1645	1646	
	0 10.4.48.42	1645	1646	
	AAA Configuration  C Enable for 902.1X / MAB AA  Enable AAA for Web Authen  Schedule Deployment		Previous Next	Finish Cancel
H Videos			TAC Service Requests   Alarms 🛽	71 🖤 0 🖬 0

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**.

#### **Procedure 4**

**Enable identity and web authentication** 

The identity configuration enables MAB on the switch. Web authentication allows users to access the network from a device that isn't configured for 802.1X and still be authenticated. The TrustSec Work Center supports configuring local web authentication, however, in this deployment you use centralized web authentication. During the MAB authentication, there is a default rule that will send the client a URL redirect to the centralized web authentication login portal. This is configured in Cisco ISE.

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

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

**Step 3:** In the **Filter** list, choose the switch that was previously configured for RADIUS.

Step 4: In the Port Group Selector pane, select All Groups, and then click Next.

Navigator	Enab	le Interfaces for Ide	entity			
Dashboard	Sele	ct Devices and Port Gr	ouns			~
Getting Started			antipo -			
Readiness Assessment	Sele	ect devices from the list o	of Identity Capable (	devices, and Select the por	t group:	s associated with these devices.
RADIUS Configuration						
<ul> <li>Identity Configuration</li> </ul>		entity Capable Devices			-	
Manage Identity	4	🖗 Filter				Port Group Selector
Configuration		Display Name	IP Address	Device Type		▼ ✓ All Groups
Enable Identity on Interface		A2960S.cisco.local	10.5.20.5	stack		1 Gbps Ethernet Ports
Change of Authorization		RS204- A2960S.cisco.local	10.5.60.5	Cisco Catalyst 2960 stack		✓ 10 Gbps Ethernet Ports
		RS211- A2960S.cisco.local	10.5.156.5	Cisco Catalyst 2960 stack		✓ 10 Mbps Ethernet Ports
<ul> <li>Secured Group Access Configuration</li> </ul>		RS208-	10.5.87.2	Cisco Catalyst 2960		✓ 100 Mbps Ethernet Ports
		A2960S.cisco.local RS232-	10.5.87.2	stack		Access Ports
Reports		RS232- D3750X.cisco.local	10.5.215.254	Cisco 3750 Stack		DMP Ports
Jobs		RS208-A3560X- PR1.cisco.local	10.5.87.3	Cisco Catalyst 3560X- 24P-L,S Switch		End Hosts
		RS232- A3560X.cisco.local	10.5.215.2	Cisco Catalyst 3560X- 24P-L,S Switch		✓ IP Phones
		A3750X.cisco.local	10.4.79.2	Cisco 3750 Stack		✓ IPVSC Ports
		D6500VSS.cisco.local	10.4.15.254	Cisco Virtual Switching System	-	
						Previous Next Finish Cancel
	Revie	ew Port Groups				<del>ا</del>
	Conf	igure Identity				
	Sche	dule Deployment				

**Step 5:** Select the check boxes next to the ports for which you want to enable identity, and then click **Next**.

/ork Centers > TrustSec > Identity Confi	-					07 Jun 2012, 13	
Navigator Enable Interfaces for Identity							
Dashboard	Select Devices and Port Groups						
Getting Started							
Readiness Assessment							
RADIUS Configuration	Vi	ew the ports and unselect the	ports that you	wish to exclude.			
<ul> <li>Identity Configuration</li> </ul>	Se	lected Devices	As	sociated Ports			
Manage Identity		Display Name	✓	Port Name	Description		
Configuration	۲	A3750X.cisco.local	✓	Gi1/0/36	GigabitEthernet1/0/36	<u> </u>	
Enable Identity on Interface			<b>V</b>	Gi1/0/37	GigabitEthernet1/0/37		
Change of Authorization			$\checkmark$	Gi1/0/34	GigabitEthernet1/0/34		
change of Authorization			$\checkmark$	Gi3/0/18	GigabitEthernet3/0/18		
Secured Group Access			<ul> <li>✓</li> </ul>	Gi3/0/19	GigabitEthernet3/0/19		
Configuration			✓	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		
				69/0/17	GiaphitEthorpot2/0/14	•	
					Previous Next Fin	nish Cance	
	Car	figure Identity					

Next, you configure monitor mode.

Step 6: In the Identity mode to be configured section, move the Security Mode slider to Monitor, which is the default.

**Step 7:** 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 8: In the MAC Configuration section, make sure only Enable MAC Move is selected.

Step 9: In the Additional Configurations section, select Advanced Options.

Step 10: In the Adhoc commands box, enter the following command, and then click Next.

device-sensor accounting



For device profiling, you need to enable the Cisco 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*. This feature is not supported on the Cisco Catalyst 2960S access layer switches. If you want to use device profiling in the access layer, you will need to deploy Cisco Catalyst 3560, 3750, or 4500 Series Switches.

uluulu Cisco Prime	admin I Log Out I About I Sitemap I Feedback I Help 📳 Search				
cisco LAN Management Solu	🔍 My Mienu 👻 Monitor 👻 Inventory 👻 Configuration 👻 Reports V. Admin V. Work Ct. 💌 🔡 🔀				
Work Centers > TrustSec > Identity Config					
Navigator	Enable Interfaces for Identity				
Dashboard	Select Devices and Port Groups				
Getting Started	Review Port Groups				
Readiness Assessment	Configure Identity				
RADIUS Configuration					
<ul> <li>Identity Configuration</li> <li>Manage Identity</li> <li>Configuration</li> </ul>	Identity mode to be configured Choose the Security mode based on the level of security required in the devices. Values shown as selected are the default values.				
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				
<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				
	Define Authentication Profile 802.1x, then MAB +				
	The host mode determines the number of hosts that can be authenticated on a given port More Details				
Define Host Mode Single Host Multiple Host Multiple Host MultiAuth Multiplemin No Change					
	Select the action to be taken when a port security violation is detected due to the following reasons More Details  Action to be taken on security violation  Restrict  Protect  Shutdown  No change				
	MAC Configuration				
	Enable MAC move or replace More Details   Enable SMMD notification for MAC addition or removal More Details   Enable MAC move  In able MAC replace  Notify MAC addition  Notify MAC addition				
	Additional Configurations				
	If you have selected low impact mode and if ACL is not configured on the device, you More Details  Advanced options				
	Adhoc commands*: device-sensor accounting				
	Previous Next Finish Cancel				
	Schedule Deployment				

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

Step 11: 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.

uluulu Cisco Prime		Log Out I Abo	ut I Sitemap I Feedba	:k i Help 📳	Search	
CISCO LAN Management Solut	🔍 My Menu 🔻 Monitor 🔻 🛛	Inventory 🔻	Configuration 🔻 Repo	ts 🔻 Admin 🔻	Work Ge 🕨	훈 🚖
Work Centers > TrustSec > Identity Config					07 J	un 2012, 13:30 PDT
Navigator	Enable Interfaces for Identity					
Dashboard	Select Devices and Port Groups					<ul> <li>✓</li> </ul>
Getting Started	Review Port Groups					<ul> <li>✓</li> </ul>
Readiness Assessment	Configure Identity					<b>V</b>
RADIUS Configuration	Schedule Deployment					
<ul> <li>Identity Configuration</li> <li>Manage Identity</li> <li>Configuration</li> </ul>	Scheduler				* Indicates re	auired field
Enable Identity on Interface	Immediate     J     Once		A3750X Monitor Mode (	ionfig		
Change of Authorization	O Daily O Weekly	E-mail				
<ul> <li>Secured Group Access Configuration</li> </ul>	Monthly					
Reports	Job Options		🗌 Enable job pas	sword		
Jobs	Fail on mismatch of config versions		Login Use	rname		
	Sync archive before job execution		Login Pas	sword		
	Copy running config to startup		Enable Pas	sword		
	Failure policy Ignore failure and conti	nue 👻				
			Preview CLI	Previous	Next Finish	Cancel

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

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

aaa authentication dot1x default group ISE-Group aaa authorization network default group ISE-Group aaa authorization configuration default group ISE-Group aaa accounting dot1x default start-stop group ISE-Group radius-server vsa send accounting radius-server vsa send authentication

authentication mac-move permit dot1x system-auth-control

device-sensor accounting

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

#### interface [interface]

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

#### Procedure 5

**Disable port security timers** 

The current Cisco SBA design incorporates the use of port security to provide a level of security and prevent rogue devices from being connected. However, TrustSec 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 TrustSec each have their own set of timers. The conflict causes TrustSec 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. A new screen is displayed.

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

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

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

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

Cisco Prime	admin i Log Out i About i Sitemap i Feedback i Help 🕞 Search
CISCO LAN Manager	Wy Menu • Monitor • Inventory • Configuration • Reports • Admin • Work CE • 11 👾
Mode: PORT	07 Jun 2012, 13:44 F Groups
f 1. Device and Group Selector	Port Groups
2. Groups	○ Select Custom Group(s) <sup>⊙</sup> Define an Adhoc Rule
<ol> <li>Tasks</li> <li>Add Tasks</li> </ol>	Adhoc Rule
5. Set Schedule Options	
6. View Job Work Order	Object Type: Variable: Operator: Value: OR  Port  Identity_Security_Mode V / Add Rule Expression
	r Rule Text
	Port.Identity_Security_Mode = "Monitor"
	Check Syntax Include Exclude
	- Step 2 of 6 - Back Next Frish Cancel
Videos	TAC Service Requests   Alarms 🙆 71 🦁 0 💆 0

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

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

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

no switchport port-security violation

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

Adhoc Task Confi	igur	ation				
<b>IOS Parameters</b>						
Commands						
CLI Commands:	no	switchport	port-security port-security port-security	aging	type	
Rollback Commands:						
			Ар	plicable D	evices	
			Save	Reset	Cancel	

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



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

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

Procedure 6

**Configure identity on the Catalyst 4500** 

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

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

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

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

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

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

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

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

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

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

radius-server vsa send accounting radius-server vsa send authentication

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

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

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

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

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

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

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

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

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

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



#### Tech Tip

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

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

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

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

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

< <search input="">&gt;</search>	Filter by Port Name:	Filter	
All Search Results			
<ul> <li>C   Devices</li> <li>A4507.cisco.local</li> </ul>	279. C Gizzo-Controlled	Showing 609 rec Description Gligablication	ord
	280. 🔲 Gi2/6Uncontrolled	GigabitEthernet2/6Uncontrolled	
	281. 🗹 Gi2/7	GigabitEthernet2/7	
	282. 🔲 Gi2/7Controlled	GigabitEthernet2/7Controlled	
	283. 🔲 Gi2/7Uncontrolled	GigabitEthernet2/7Uncontrolled	
	284. 🔽 Gi2/8	GigabitEthernet2/8	
	285. 🔲 Gi2/8Controlled	GigabitEthernet2/8Controlled	
	286. 🔲 Gi2/8Uncontrolled	GigabitEthernet2/8Uncontrolled	
	287. 🗹 Gi2/9	GigabitEthernet2/9	
	288 Gi2/9Controlled	GigabitEtherpet2/0_Controlled	-

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

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

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

authentication host-mode multi-auth authentication open authentication order dot1x mab authentication port-control auto mab dot1x pae authenticator no switchport port-security aging time no switchport port-security aging type no switchport port-security violation **Step 24:** Click **Applicable Devices**, select the switch to which you want to apply this configuration, click **Close**, and then click **Save**.

3 10.4.	48.38:1741/rme/ncfgJ	lobBrowser.do	
	Adhoc Task Conf	iguration	
	IOS Parameters		
	Commands		
	CLI Commands:	authentication host-mode multi-auth authentication open authentication order dot1x mab authentication port-control auto mab dot1x pae authenticator no switchport port-security aging time no switchport port-security aging type no switchport port-security violation	
	Rollback Commands:	::. ::. ::.	
		Applicable Devices Save Reset Cancel	

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

Cisco Prime		admin I Log Out I About I Sitemap I Feedback I Help  🗮 Search
CISCO LAN Manageme	t Solution 🔸 My Menu 🔻	Monitor 🔻 Inventory 🔻 Configuration 🔻 Reports 🔻 Admin 🔻 Work C( 🕨 🛛 管 😭
Mode: ADDING #1 Device and Group Selector #2 . Groups #3 . Tasks -4 . Add Tasks -5 . Set Schedule Options -6 . Wew Job Work Order	Add Tasks AddTasks Applicable Tasks Achoc Task Achoc Task Achoc Task Achoc Task Achoc Task Achoc Task	07 Jun 2012, 13:47 PA
H Videos		TAC Service Requests   Alarms 🝳 71 🦁 0 💆 0

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

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

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

#### Process

Enabling Visibility to the Wireless Network

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

To authenticate wireless clients, you need to configure the wireless LAN controllers (WLC) to use the new Cisco ISE servers as RADIUS servers for authentication and accounting. The existing entry is disabled so that if there are any issues after moving to Cisco ISE, you can quickly restore the original configuration. Additionally, you configure the WLCs for DHCP profiling so that profiling information can be obtained from the DHCP requests from these clients and sent to the Cisco ISE.

#### Procedure 1

**Configure 802.1X for wireless endpoints** 

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

**Step 1:** On the ISE console, 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.

սիսիս	Dictionaries	
CISCO Identity Services Engine	(م	ise-1 admin Logout Feedback
🛕 Home Operations 🔻 Policy 🔻 Administration 🔻	<b>∲•</b>	😐 Task Navigator 👻 😢
Authentication 💿 Authorization 📈 Profiling 🦁 Posture	Simple Condition 💿	roup Access
	Compound Condition 💿	
Authentication Policy		-
Define the Authentication Policy by selecting the protocols that ISE should use to a Policy Type O Simple   Rule-Based		d the identity sources that it should use for authentication.
MAB : If Wired_MAB		and , 🔯 Actions 💌
Wired-Dot1X : If Wired_802.1X		fault Netwoo and , 🕸 Actions 👻
Wireless-Dot1X : If Condition(s)		s 📀 and 🕨 🎡 Actions 🔻
Default Rule (If no match) : al Add Al Conditions of Conditions of Conditions of Select Condition	•	۰ ۵۰



cisco Identity Services Engine	Compound Condition		ise-1 admin Logout Feedba
🛕 Home Operations 🔻 Policy 🔻 Administration 💌	🔶 📲 📜 🚳 🍕		👓 Task Navigator 👻 😢
🛓 Authentication 💿 Authorization 🔀 Profiling 🕐 Posture	Wired_MAB Wired_802.1X	roup Access 🤱 Policy Elements	
Authentication Policy Define the Authentication Policy by selecting the protocols that ISE should use to o Policy Type  O Simple   Rule-Based	Wireless_802.1X  Switch_Local_Web_Authentication  WLC_Web_Authentication	d the identity sources that it should use	for authentication.
MAB : If Wired_MAB		and 🕨	🖗 Actions 🔻
Wired-Dot1X : If Wired_802.1X		əfault Netw📀 🛛 and 🕨	👙 Actions 🔻
Wireless-Dot1X : If Condition(s) Condition		e <mark>s 📀</mark> and 🕨	🖗 Actions 🔻
Default Rule (If no match) : al Conditions Condition Name Select Condition C			× چ

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

Authentication  Authorization Authorization Authorization Authorization Authorization Policy by selecting tr y Type Simple Rule-Based		Posture 💽 Client Prov		Security Grou		Policy Eler sources that it sh		itication.
e the Authentication Policy by selecting th	ne protocols that ISE shou	uld use to communicate wit	th the netwo	ork devices, and th	he identity	sources that it sh	iould use for auther	ntication.
e the Authentication Policy by selecting th	ne protocols that ISE shou	uld use to communicate wit	th the netwo	ork devices, and th	he identity	sources that it sh	ould use for auther	ntication.
	ie protocois triat ise snou	uid use to communicate wit	in the netwo	ork devices, and ti	ne identity	sources that it sh	iouid use for auther	nucation.
						1	-00	
MAB 🔹	: If Wired_MAB	allow protoc	OIS Allowed	d Protocol : Defaul	It Netw 💟	and 🕨		Actions 🔻
Wired-Dot1X	: If Wired 802.1X	allow protoc	ols Allowed	d Protocol : Defaul	lt Netw📀	and	100	Actions 💌
Vireless-Dot1X	: If Wireless_802	.1X 🔶 allow protoc	ols Select f	Network Access	0	and 🕨	<u>ģ</u>	Actions 🔻
					ſ	Allowed Protoco	ols	7
Default Rule (If no match)	: allow protocols	Allowed Protocol : Default N	vletw 💟 🛛 ar	nd use identity sou	urce :		م	Actions 👻
						<b>∲-</b> ∎ '≣		
						Default Network		,

**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 Set Identity Source, 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**.

cisco Identity Services Engine		ise-1 admin Logout Feedback
💧 Home Operations 🔻 Policy 🔻 Administration 🖲	,	👓 Task Navigator 👻 😢
🛃 Authentication 💿 Authorization 🔀 Profiling	Identity Source AD1	]
Authentication Policy Define the Authentication Policy by selecting the protocols that I Policy Type O Simple Rule-Based	Options If authentication failed Reject * If user not found Reject * If process failed Drop *	se for authentication.
MAB : If Wired	Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS MSCHAP It is not possible to continue processing when authentication fails or user is not found.	🖗 Actions 🔻
Wired-Dot1X : If Wired	If continue option is selected in these cases, requests will be rejected	👙 Actions 💌
Wireless-Dot1X : If Wirele		🖗 Actions 💌
Default : use	Internal Users 🗢	Actions *
Default Rule (If no match) : allow proto	ccols Allowed Protocol : Default Netwo	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 🔻 Ad	ministration 🔻	👓 Task Navigator 👻 📀
🛓 Authentication 💿 Authorization 🔀	Profiling 🕐 Posture 🕟 Client Provisioning 🔄 Security Group Access 🔒 Policy Elements	
Dictionaries Conditions Results		
Results		<u>م</u>

Procedure 3

Add ISE as RADIUS authentication server

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

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

Step 2: On the menu bar, click Security.

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

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

Step 5: 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.

uluilu cisco	MONITOR WLANS (		WIRELESS	SECURITY	MANAGEMENT	Sa <u>v</u> e Configu C <u>O</u> MMANDS		Logout   <u>R</u> efresh EDBACK
Security	RADIUS Authentica	_	_	Jecolari	Management	COMMANDS	< Back	Apply
<ul> <li>▼ AAA</li> <li>General</li> <li>▼ RADIUS</li> <li>Authentication</li> <li>Accounting</li> </ul>	Server Index Server Address Shared Secret Format		2 10.4.48.41 ASCII •					
Fallback TACACS+ LDAP	Shared Secret Confirm Shared Secret	:	•••••					
Local Net Users MAC Filtering Disabled Clients User Login Policies	Key Wrap Port Number		(Designed for 1812	FIPS custom	ers and requires a	key wrap compl	ant RADIUS s	erver)
AP Policies Password Policies	Server Status Support for RFC 3576		Enabled •					
Priority Order	Server Timeout		2 second	s				
<ul> <li>Certificate</li> <li>Access Control Lists</li> </ul>	Network User Management		Enable Enable					
<ul> <li>Wireless Protection</li> <li>Policies</li> </ul>	IPSec		🗌 Enable					

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

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

**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.

 cısco	MONITOR	<u>W</u> LANs <u>C</u>	ONTROLLER	WIRELESS ;	ECURITY	MANAGEMENT	Sa <u>v</u> e Configu C <u>O</u> MMANDS		g Logout <u>R</u> efresh EEDBACK
Security	RADIUS	Authenticat	ion Server	s				Apply	New
AAA     General     ADIUS     Adventication     Accounting     Fallback     TACACS+			IP Addres (Designed Hyphen		rs and requi	ires a key wrap con	npliant RADIUS	server)	
LDAP Local Net Users	Network User	Management	Server Index	Server Addre:	s Port	IPS	ec	Admin Sta	atus
MAC Filtering Disabled Clients	V		1	10.4.48.15	1812	Dis	abled	Disabled	
User Login Policies	V		2	10.4.48.41	1812	Dis	abled	Enabled	
AP Policies Password Policies	V		3	10.4.48.42	1812	Dis	abled	Enabled	



Add ISE as RADIUS accounting server

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

Step 1: On the menu bar, click Security.

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

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

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

սիսիս							ration   <u>P</u> ing   l	.ogout <u>R</u> efresh
CISCO	MONITOR WLANS		WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDE	ACK
Security	RADIUS Accountin	ng Servers >	Edit				< Back	Apply
▼ AAA General ▼ RADIUS Authentication Accounting	Server Index Server Address Shared Secret Format	2 10.4.4 t ASCI						
Accounting Fallback TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies Local EAP Priority Order	Shared Secret Confirm Shared Secret Port Number Server Status Server Timeout Network User IPSec	et	ed v seconds					

**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.

ىرايىرانى cısco	MONITOR	<u>W</u> LANS <u>C</u> O	NTROLLER WIRELE	SS <u>s</u> ec	URITY M <u>A</u> NAC	EMENT C <u>O</u> MM	ANDS	HELP FEEDBACK
Security	RADIUS A	ccounting	Servers					Apply New
▼ AAA General ▼ RADIUS	MAC Delim	iter Hyphe	en 🔽					
Authentication Accounting	Network User	Server Index	Server Address	Port	IPSec	Admin Status		
Fallback TACACS+		1	10.4.48.15	1813	Disabled	Disabled		
LDAP		2	10.4.48.41	1813	Disabled	Enabled		
Local Net Users		3	10.4.48.42	1813	Disabled	Enabled		
MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies								

#### **Procedure 5**

**Enable client profiling** 

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

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

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

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

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



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

## **Enabling Authorization**

The network infrastructure is now configured for 8021.X authentication in monitor mode. Upon successful authentication, the endpoint is granted full network access. However, monitor mode allows for endpoints that fail 802.1X to access the network by using MAB. This is a good point in the deployment to stop to verify that devices can access the network by using existing credentials.

The next step would be to deploy some form of authorization to control what authenticated endpoints can access on the network. This next phase is called *low-impact mode*. In low-impact mode, endpoints are authenticated with either 802.1X or MAB. MAB is used for devices that require network access but either don't support 802.1X or don't have 802.1X configured. After authentication, the endpoint is given full access to the network, but prior to authentication, the endpoint will only have access to the services necessary for authentication.

#### Process

Enabling Authorization for Wired Endpoints

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

You will enable authorization for wired endpoints that authenticate using 802.1X. 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 ISE console, in the menu bar, mouse over **Policy**, and then in the Policy Elements section, choose **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, choose **PERMIT\_ALL\_TRAFFIC**, and then click **Submit**.

cisco Identity Services Engine ▲ Home Operations ▼ Policy ▼ Admir	ise-1 admin Logout Fe	_
🛃 Authentication 🛛 🧕 Authorization 🔀	Profiling 🕜 Posture 👩 Client Provisioning 🚊 Security Group Access 🛛 🐥 Policy Elements	
Dictionaries Conditions Results		
Results         Image: Control of the second secon	Authorization Profile  * Name Wred_Dot1X Description Profile  * Name Ved_Dot1X Description Profile Common Tasks  Common Tasks Common Ta	
🕙 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 choose Authorization.

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

	Home	Operations   Policy   Admi	inistration 🔻			👓 Task M	lavigator + 🕗
4	Authenti	cation 🧕 Authorization 🛛 🧭	Profiling 💽 Postur	e 👩 Client Provisioning	🚊 Security Group Access	🚯 Policy Elements	
	orizatio	a Dolicy					
		orization Policy by configuring rules ba	and an identify maynes	nd/ex other conditions. Drog o	ad dean o las ka alaman kina andar		
			ased on identity groups a	nd/or other conditions. Urag ar	nd drop rules to change the order.		
st	Matched R	ule Applies 🔹 🔻					
Eх	ceptions (						
st	andard						
	Status	Rule Name	Conditions (id	entity groups and other condit	ions)	Permissions	
	<b>~</b>	Black List Default	if Blacklist		the	n Blacklist_Access	Edit   👻
	<b>~</b>	Profiled Cisco IP Phones	if Cisco-IP-Pho	one	the	n Gisco_IP_Phones	Edit   👻
		Profiled Cisco APs	f Cisco-Access	-Point	the	n Cisco APs	Edit   🔻
		Troned Geo Al 5	ODED ACCES	- Conte			Earc
		Default		en PermitAccess		Insert New R	
						Insert New R	ule Above

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

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

Step 5: Click Select Existing Condition from Library.

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

🛕 Home 🛛 Operations 🔻	Policy 🔻 Administration 🔻				👓 Task	: Navigator + 🕗
Authentication	thorization 🔀 Profiling	💽 Postu	re 📃 Client Provisioning 🚊 Security Grou	p Access	Policy Elements	
uthorization Policy efine the Authorization Policy by	Compound Conditions	٩	and/or other conditions. Drag and drop rules to chan	ge the order.		
irst Matched Rule Applies	↓ Wired 802.1X	\$\$* <b>•</b>				
<ul> <li>Exceptions (0)</li> </ul>	Wired_MAB					
Standard	Wireless_802.1X					
Status Rule Name	Wireless_MAB		lentity groups and other conditions)		Permissions	
🛛 🛛 🔤 Black List Default	Catalyst_Switch_Local_Web_ WLC_Web_Authentication	Authentica		then	Blacklist_Access	Edit   👻
Profiled Cisco IF	wcc_web_Mddienceddon	h	one	then	Cisco_IP_Phones	Edit   🗸
Profiled Cisco AP			s-Point	then	Cisco_APs	Edit   👻
🖉 🗹 👻 Wired Dot1X End				-	then AuthZ Profil	🔶 Done
Add All Conditions B						Edit   👻
Condition Name						
Select Condition			é	P+		

**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.

🔒 Home Operations 🔻 Policy 🔻 Admir	nistration 🔻	••• Task Na	avigator 🔫 🕗
🛓 Authentication 🛛 🙍 Authorization 🔀	Profiling 💽 Posture 🔂 Client Provisioning 🔄 Security Gro	up Access 💦 🚯 Policy Elements	
thorization Policy		Standard	
	sed on identity groups and/or other conditions. Drag and drop rules to cha		
st Matched Rule Applies			
r Matchieu Rule Applies *		Blacklist_Access     Gisco_APs	
Exceptions (0)		Cisco_IP_Phones	
Standard		C DenyAccess	
		RermitAccess	
Status Rule Name	Conditions (identity groups and other conditions)	G 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 🗇 and Wired_802:1X	-	👝 Done
🗹 Default	If no matches, then PermitAcces		Edit   🗸
	Select an item	o -+	

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

	_	entity Services Engine					Logout Feedb
-	_		iministration 🔻				Navigator 🛛 🕑
1	Authenti	cation 🧕 Authorization	🔀 Profiling 💽 Posture	Client Provisioning	Security Group Access	Policy Elements	
	norizatio	a Dolicy					
		orization Policy by configuring rules	based on identity groups and	or other conditions. Drag an	d drop rules to change the order		
			based of fidericity groups and	or other conditions, brag ar	ia arop rales to change the order		
rst	Matched R	ule Applies 🔻					
Ð	ceptions (						
SI	tandard						
	Status	Rule Name	Conditions (ident	ity groups and other conditi	ons)	Permissions	
	<b>~</b>	Black List Default	if Blacklist		ti	nen Blacklist_Access	Edit   🕶
		Profiled Cisco IP Phones	if Cisco-IP-Phone		ti	nen <b>Cisco_IP_Phones</b>	Edit   🗸
	-						
	<b>~</b>	Profiled Cisco APs	if Cisco-Access-Pe	pint		nen Cisco_APs	Edit   🔻
	<b></b>	Wired Dot1X Endpoints	If Wired_802.1X		ti	nen Wired_Dot1X	Edit   🕶
		Default	if no matches, then	PermitAccess			Edit   👻
			in no matchoy alon	P OIT II CACCOSS			Eulit   *

#### **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 want to enable only what is required for the port to go through the authentication process. Typically, this means allowing DHCP, DNS, and TFTP to support Preboot Execution Environment, and access to the AD domain controller. For troubleshooting, you also allow ICMP echo and echo-reply traffic. You deny all other traffic and log the denials in order to determine if there is legitimate traffic that is getting denied, and then make changes to the access list.

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

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

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

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

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



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

sco LAN Management Solution	n 🔹 My Menu 🔻 Monitor 🔻	Inventory V Configuration V	Reports 🔻 Admin 🔻 Wor	k Centers 🕨	e 🕁			
ork Centers » TrustSec » Identity Configurati		Inventory • Configuration •	Reports • Autrin • Won	K Cericers 💌 14 Jun 2012				
Navigator	Manage Identity Devices							
Dashboard	Review port selection on selected	devices(optional)						
Getting Started								
Readiness Assessment	View the ports and unselect the port	s that you wish to exclude.						
RADIUS Configuration	Selected Devices	Associated Ports						
<ul> <li>Identity Configuration</li> </ul>	Display Name	Port Name	Description					
Manage Identity Configuration	<ul> <li>A3750X.cisco.local</li> </ul>	GI3/0/18	Gi3/0/18	1	-			
Enable Identity on Interface		Gi3/0/19	Gi3/0/19	1	_			
		✓ Gi3/0/16	Gi3/0/16					
Change of Authorization		Gi2/0/22	Gi2/0/22					
Secured Group Access		GI3/0/17	GI3/0/17					
Configuration		✓ Gi2/0/23	GI2/0/23					
Reports		Gi3/0/14	Gi3/0/14					
Jobs		✓ Gi2/0/20	Gi2/0/20					
3003		GI3/0/15	Gi3/0/15					
		retinicia 🔽	GI2/0/21		-			

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

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

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

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

**Step 10:** In the Additional Configurations section, select **Advanced Options**.

Step 11: In the Adhoc commands box, enter the following commands, and then click Next.

ip device tracking ip http server ip access-list extended PreAuth permit ip any host 10.4.48.10 permit udp any eq bootpc any eq bootps permit udp any any eq domain permit udp any any eq tftp permit icmp any any echopermit icmp any any echo-reply deny ip any any log ip access-list extended WebAuth deny udp any any eq domain permit tcp any any eq www permit tcp any any eq 443 deny ip any any

#### **Tech Tip**

The WebAuth ACL is used to redirect web traffic to the Cisco ISE to launch the web authentication portal. The logic of this ACL is slightly different than a regular ACL. The permitted traffic is the traffic you want to redirect and the denied traffic is the traffic that will pass normally. This ACL name is passed to the switch from Cisco ISE via RADIUS and invoked when the user authenticates.

	admin   LogOut   Ab	out I Sitemap I Feedback I Help 🕞 Search
cisco Prime Cisco LAN Management Solution	n 🔹 My Menu 🔻 Monitor 🔻 Inventory 🔻 Configurati	
Work Centers > TrustSec > Identity Configuration	ion > Manage Identity Configuration	22 Mar 2013, 11:04 PDT
Navigator	Manage Identity Devices	
Dashboard	Review port 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</li> <li>Configuration</li> </ul>	Choose the Security mode based on the level of security required Select the security mode based on the level of security you w	
Enable Identity on Interface	Security Mode	
Change of Authorization	Monitor Low impact	High
<ul> <li>Secured Group Access Configuration</li> </ul>	Associated ACL allows selective access control. More Details	security
Reports		
Jobs	Associated ACL* PreAuth	
	Choose authentication profiles, host modes and action to be take Define Authentication Profile B02.1x, th The host mode determines the number of hosts that can be. Define Host Mode Select the action to be taken when a port security violation S Action to be taken on security violation Action to be taken on security violation MAC Configuration	an MAB  uthenticated on a given port More Details  ost  Multiple Host Multiputh  No Change  detected due to the following reasons More Details
	MAC move/replace	SNMP MAC notification
	Enable MAC move or replace More Details 🕨 🕨	Enable SNMP notification for MAC addition or removal.
	Enable MAC move	More Details
	Enable MAC replace	Notify MAC addition
		Notify MAC removal
	Additional Configurations	
	If you have selected low impact mode and if ACL is not configur Advanced options	ed on the device, you More Details 🕨
	Adhoc commands*: ip device tracking ip https:rev to accessist extended PreAuth permit ip any host 10.4.48.10 permit tudp any eq bootpc any c permit tudp any any eq domain permit tudp any any eq domain permit tudp any any eq domain permit tudp any any log ip accessist extended Webbut deny tudp any any eq dvas permit tip any any eq dvas deny tip any any eq 443 deny tip any any eq 443	н "
		Previous Next Finish Cancel

Step 12: 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.

ululu 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 Cent 🕨 👘	
Work Centers > TrustSec > Identity Configurati	ion > Manage Identity Configuration 15 Mar 2013, 09	:00 PDT
Navigator	Manage Identity Devices	
Dashboard	Review port selection on selected devices(optional)	<b>V</b>
Getting Started	Configure Identity	<b>V</b>
Readiness Assessment	Schedule Deployment	
RADIUS Configuration		
<ul> <li>Identity Configuration</li> </ul>	Scheduler	
Manage Identity Configuration	Indicates required fie     Job Description* A3750X Low Impact Mode	10
Enable Identity on Interface		
Change of Authorization	O Daly Chiles	
<ul> <li>Secured Group Access Configuration</li> </ul>	Job Dations	
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	
	Enable Password	
	Failure policy Ignore failure and continue	
	Preview CLI Previous Next Finish Can	el

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

ip device tracking

ip http server

ip access-list extended PreAuth

permit ip any host 10.4.48.10

permit udp any eq bootpc any eq bootps

permit udp any any eq domain

permit udp any any eq tftp

permit icmp any any echo

permit icmp any any echo-reply

deny ip any any log

ip access-list extended WebAuth deny udp any any eq domain permit tcp any any eq www permit tcp any any eq 443

deny ip any any

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

#### interface [interface]

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

#### **Procedure 4**

**Enable low impact mode on Catalyst 4500** 

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

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

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

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

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

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

Step 6: In the Task Selector, expand All Tasks, select Adhoc, and then click Next.
Step 7: Click Add Instance, and then, in the new window, enter the CLI commands necessary to configure low impact mode.

ip device tracking ip http server ip access-list extended PreAuth permit ip any host 10.4.48.10 permit udp any eq bootpc any eq bootps permit udp any any eq domain permit udp any any eq tftp permit icmp any any echo permit icmp any any echo-reply deny ip any any log ip access-list extended WebAuth deny udp any any eq domain permit tcp any any eq www permit tcp any any eq 443 deny ip any any



# **Tech Tip**

The WebAuth ACL is used to redirect web traffic to the Cisco ISE to launch the web authentication portal. The logic of this ACL is slightly different than a regular ACL. The permitted traffic is the traffic you want to redirect and the denied traffic is the traffic that will pass normally. This ACL name is passed to the switch from Cisco ISE via RADIUS and invoked when the user authenticates

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

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

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

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

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

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

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

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

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

# **Tech Tip**

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

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

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

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

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

10.4.48.38:1741/rme/ncfgJobBrowser.do Include List		÷
< <search input="">&gt; → ⊅</search>	Filter by Port Name:	Filter
		Showing 609 records
A4507.cisco.local	Z79. BazyoControlled	Description Glyablicatientet2/bcontrolled
	280. 🔲 Gi2/6Uncontrolled	GigabitEthernet2/6Uncontrolled
	281. 🔽 Gi2/7	GigabitEthernet2/7
	282. 🔲 Gi2/7Controlled	GigabitEthernet2/7Controlled
	283. 🔲 Gi2/7Uncontrolled	GigabitEthernet2/7Uncontrolled
	284. 🔽 Gi2/8	GigabitEthernet2/8
	285. 🔲 Gi2/8Controlled	GigabitEthernet2/8Controlled
	286. 🔲 Gi2/8Uncontrolled	GigabitEthernet2/8Uncontrolled
	287. 🔽 Gi2/9	GigabitEthernet2/9
	288 🗖 Gi2/QControlled	GinabitEthernet2/0Controlled
•	L.	Include Cancel

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

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

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

ip access-group PreAuth in authentication host-mode multi-domain **Step 24:** Click **Applicable Devices**, select the switch to which you want to apply this configuration, click **Close**, and then click **Save**.

Adhoc Task Conf	igui	auun					
IOS Parameters							
Commands							
CLI Commands:	no	switchport	port-securi port-securi port-securi	ity	aging	type	
							.:
Rollback Commands:							
			(	Ap	plicable D	evices.	
			Save		Reset	Cance	1

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

uluulu Cisco Prime		admin   Log Out   About   Sitemap   Feedback   Help 🕞 Search
CISCO LAN Manageme	nt Solution 🧹 My Menu 🔻 M	Monitor 🔻 Inventory 🔻 Configuration 🔻 Reports 🔻 Admin 🔻 Work Ce 🕨 📑 😭
Mode: ADDING If 1. Device and Group Selector If 2. Groups If 3. Tasks 4. Add Tasks 5. Set Schedule Options 6. Gene Schedule Options 6. Verv Job Work Order	Add Tasks Add Tasks Addic Task Ad	Added Instances Added Instances Contraction Contractio
H Videos		TAC Service Requests   Alarms 🙆 71 🔍 0 💆 0

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

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

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

# Procedure 5 Enable ch

# Enable change of authorization

Authorization requires the use of RADIUS Change of Authorization (CoA) in order to change the state of the port after authentication. This is not enabled by default, and you will need to enable it. You can do this by using the TrustSec Work Center of Cisco Prime LMS 4.2.

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

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

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

Lulu Cisco Prime						admin I I	.og Out I About	I Sitemap	I Feedback I F	ielp 🔛 🚽 Se	arch	
ISCO LAN Management Solutio	n	€ м	ly Menu 🔻	Monite	or 🔻 Inven	tory 🔻 C	onfiguration 🔻	Reports 🔻	Admin 🔻 V	/ork Centers	<b>F</b>	
Vork Centers > TrustSec > Identity Configurat	ion > Chane	e of A	Authorizatio	n							21	Jun 2012, 14:08
Navigator	Deploy	1										
Dashboard											⊕TrustS	ec Configurati
Getting Started	> Choo	se Te	mplates									
Readiness Assessment	Color	t torr	winter to d		nfiguration							
RADIUS Configuration	Selec	t tem	ipiates to c	ерюу со	inguration							_
<ul> <li>Identity Configuration</li> </ul>	Tem	plate	Selector							Selec	ed 1   Total 1	9
Manage Identity Configuration									Show All		- F	õ
Enable Identity on Interface		Т	"emplate N	ame 👻	Features	Туре	Role In	Category		Created	Scope	
Change of Authorization		▶ 1	dentity - Cł	nange	Authorizati	. Partial	Access	RADIUS c	lient configurati	. 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**.

	admin   Log Out   About   Sitemap   Feedback   Help 📗 🚽 Search
cisco LAN Management Solution	n 🔹 🤇 My Menu 🔻 Manitor 🔻 Inventory 🔻 Configuration 🔻 Reports 🔻 Admin 🔻 Work Centers 🕨 🛛 🗄 😭
Work Centers > TrustSec > Identity Configuration	on > 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</li> <li>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 *
Secured Group Access Configuration	RADIUS Key shared between the device and RADIUS clients *  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.

uluulu. Cisco Prime	admin I Log Out I About I Sitemap I Feedback I Help 🕞 - Search	
cisco Prime Cisco LAN Management Solution	🔍 🔍 My Menu 🔻 Monitor 🔻 Inventory 🔻 Configuration 🔻 Reports 🔻 Admin 🔻 Work Centers 🕨	
Work Centers > TrustSec > Identity Configuration		21 Jun 2012, 14:15 PD
Navigator	Deploy	
Dashboard		ustSec Configuration
Getting Started	Choose Templates	S
Readiness Assessment	Choose Device Groups	<b>\$</b>
RADIUS Configuration	Configure Identity - Change of Authorization	<b>V</b>
<ul> <li>Identity Configuration</li> </ul>	Adhoc Configuration Commands for Selected Devices	I.
Manage Identity Configuration	Schedule Deployment	
Enable Identity on Interface		
Change of Authorization	Scheduler * Indicates requi	ired field
<ul> <li>Secured Group Access Configuration</li> </ul>	Immediate Job Description* [A3750X CoA Config     Once E-mail     Daty	
Reports	O Weekly	
Jobs	O Monthly	
	Job Options	
	Copy Startup to Running Config upon failure     Copy Running Config to Startup     Enable Dassword     Login Password     Enable Password	
	Preview CLI Previous Next Fin	nish Cancel

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

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

aaa server radius dynamic-author

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

# Procedure 6

Enable CoA on Catalyst 4500

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

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

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

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

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

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

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

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

aaa server radius dynamic-author

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

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

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

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

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

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



Procedure 1

**Configure WLC for authorization** 

Configure every WLC in the environment, with the exception of the guest WLC in the DMZ, with access lists to support these newly defined policies. Each ACL that is referenced by the authorization profiles needs to be defined on the WLC. When the clients in the campus, and at remote sites with a local controller, connect to the WLC and authenticate, Cisco ISE passes a RADIUS attribute requesting the ACL be applied for this client.

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

Step 2: On the menu bar, click Security.

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

ahaha								n   <u>P</u> ing   Logout   <u>R</u> ef
cisco	MONITOR M	⊻LANs <u>C</u> ONTF	ROLLER W <u>I</u> RI	ELESS <u>S</u> ECURIT	Y M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	EEEDBACK
Security	Access Cor	ntrol Lists						New Apply
AAA     General     KADIUS     Authentication     Accounting     Fallback     TACACS+     LoAP     Local Net Users     MAC Filtering     Disabled Clients     User Login Policies     AP Policies     Password Policies	Enable Cour	nters						

#### Step 4: Click New.

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

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

սիսիս									n   <u>P</u> ing   Logout   <u>R</u> efresh
CISCO	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Security	Access C	ontrol Li	ists						New Apply
AAA     General     KADIUS     Authentcation     Accounting     Fallback     TACACS+     LDAP     Local Net Users     MAC Filtering     Disabled Clients     User Login Policies     AP Policies     Password Policies	Enable Co Name II	ounters R	2		٠				

Step 7: Click Add New Rule.

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

uluili. cisco	MONI	TOR <u>w</u>	LANS <u>C</u> ONTROLL	ER WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS		Configuration EEDBACK	<u>P</u> ing   Logout   <u>F</u>	<u>⊰</u> efresh
Security	Acce	ss Con	trol Lists > Edit						< Back	Add New Ru	le
AAA     General     RADIUS     Authentication     Accounting     Fallback		e <b>ral</b> s List Nam Counters	e IT 185								
<ul> <li>TACACS+ LDAP Local Net Users</li> </ul>		Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
MAC Filtering Disabled Clients User Login Policies AP Policies	Ŧ	Permit	10.4.16.0 / 255.255.255.0	10.4.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0	
Policies Password Policies Local EAP	_2_	Permit	10.4.0.0 / 255.255.0.0	10.4.16.0 / 255.255.255.0	Any	Any	Any	Any	Outbound	0	
Priority Order											

P

# Tech Tip

The access list needs to have entries for the traffic in both directions, so make sure you have pairs of access list rules for both inbound and outbound traffic. Also, there is an implicit "deny all" rule at the end of the access list so any traffic not explicitly permitted is denied.

**Step 9:** Repeat Step 4 through Step 8 in this procedure for each access list that you defined in the authorization profiles in Cisco ISE.

սիսիս					Sa <u>v</u> e Con	figuration <u>P</u> ing Logout <u>R</u> efresh
cisco	MONITOR WLANS C	ONTROLLER WIRELE	SS <u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBACK
Security	Access Control List	s				New Apply
▼ AAA General ▼ RADIUS Authentication	Enable Counters 🗹					
Accounting Fallback	Ш					
▶ TACACS+	HR					
LDAP Local Net Users	Research					
MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies	<u>Finance</u>					

Next, you enable the WLC to allow Cisco ISE to use RADIUS to override the current settings, so that the access list can be applied to the wireless LAN.

Step 10: On the menu bar, click WLANs.

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

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

ululu cisco	Save Configuration   Ping   Logout   MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK	<u>R</u> efresh
WLANS		pply
WLANS WLANS Advanced	General       Security       QoS       Advanced         Allow AAA Override	•

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



If you want to provide differentiated access for the BYOD devices, you must create an authorization policy. This example describes how to create a policy based on the user's AD group and also by the type of device that

is connecting. The user authenticates by using their AD credentials but gets different levels of access based on the type of device being used. The policy described here denies all access to anyone using a BlackBerry device. If the user is using a Windows, Mac OS X, iPad, or Android device, the user gets limited access based on their AD group.

# Procedure 1 Configure identity groups

Cisco ISE has more in-depth options to give more details on the devices connecting to the network. To help identify the endpoints, identity groups are used to classify profiled endpoints. You use these identity groups to create authorization policies.

The example below shows how this is done for an Apple iPad. The procedure for other types of devices is similar.

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

# Step 2: Click Apple-iPad.

Step 3: Select Create Matching Identity Group, and then click Save.

cisco Identity Services Engine	ise-1 admin Logout Feedback
💧 Home Operations 🔻 Policy 🔻 Admir	nistration 🔻 🕘
🛃 Authentication 🛛 🧕 Authorization 🔀	Profiling 🕐 Posture 👵 Client Provisioning 📄 Security Group Access 🔥 Policy Elements
Profiling	Police Policy       * Name       Apple-Pad       Description       Policy for Apple Pads         Policy Enabled       ▼            * Monrum Certainty Factor       20       (Vald Range 1 to 65535)       *         * Network Scan (NMAP) Action       NONE       ▼         • Oraste Matching Identity Group       •       •         • Vertice Heardby       *       *         • Use Hierardby       *       •         • If Condition       Apple-PadRule2Check2 ◆       Then       Certainty Factor Increases ▼         20       ·       •         Excel       #       #       *         • Reset       *       #       *

This can be done for other endpoint types as needed. In this example deployment, this procedure was also performed for Android and Apple iPhone. You can 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 2

#### **Create profile to deny BlackBerry phones**

In an authorization profile, you define the permissions to be granted for network access. An organization may decide that they don't want to allow certain devices on the network at all, regardless of whether the user has valid credentials or not. The policy created in this procedure denies any BlackBerry phones access to the network. This policy is an example and can be modified to suit your environment.

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

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

Step 3: Click Add.

Step 4: Enter a name and description for the policy you are adding.

Step 5: In the Access Type list, choose ACCESS\_REJECT, and then click Submit.



# **Procedure 3**

**Create authorization rule** 

An authorization rule is part of the overall authorization policy. The authorization rule links the identity profile to the authorization profile. The following steps describe how to create an authorization rule that uses the profile created in Procedure 2, "Create profile to deny BlackBerry phones."

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

**Step 2:** At the end of the Default Rule, click the arrow, and then choose **Insert new rule above**. A new rule, "Standard Rule 1," is created.

Step 3: Rename "Standard Rule 1" to "Deny BlackBerry."

Step 4: In the Conditions section, next to Any, click the + symbol.

Step 5: In the list, next to Endpoint Identity Groups, choose the > symbol.

Step 6: Next to Profiled, click the > symbol, and then click BlackBerry.

iliulu cisco Identity Services Engine		ise-1 admin Logout Feedback
🍐 Home Operations 🔻 Policy 🔻 Administration		👓 Task Navigator 🔫 🕗
🛃 Authentication 💽 Authorization 🔀 Profiling	💿 Posture 🔄 Client Provisioning 🔄 Security Group Access	noticy Elements
Authorization Policy		
Define the Authorization Policy by configuring rules based on ide	entity groups and/or other conditions. Drag and drop rules to change the order	
First Matched Rule Applies		
Exceptions (0)		
Standard		
Status Rule Name	Conditions (identity groups and other conditions)	Permissions
Wireless Black List Default if	Blacklist AND Wireless_802.1X to	hen Blackhole_Wireless_Access Edit   +
🖉 👻 👻 Deny BlackBerry	Any and Condition(s)	then AuthZ Profil 💠 Done
🗹 Default if r		Edit   🕶
	Any 📀 — 🔶	
Save Reset	Profiled	
	Android	-
	BlackBerry	

Tech Tip

You will need to have followed Procedure 1, "Configure identity groups," to create an authorization profile for BlackBerry devices for the profile to be shown as a choice in the Endpoint Identity Groups list.

**Step 7:** In the Permissions section, next to AuthZ Profile(s), click the + symbol.

Step 8: In the Select an item list, next to Standard, choose the > symbol.

**Step 9:** Choose the Deny\_BlackBerry authorization profile that was created in Procedure 2, "Create profile to deny BlackBerry phones."

cisco Identity Services Engine		ise-1 admin Logout Feedback
🛕 Home Operations 🔻 Policy 🔻 Administ	ration 🔻	😁 Task Navigator 🔫 🕗
🚨 Authentication 🛛 🙍 Authorization 🔀 Pr	ofiling 💿 Posture 🕞 Client Provisioning 📑 Security Group	o Access Access Policy Elements
Authorization Policy Define the Authorization Policy by configuring rules based [First Matched Rule Apples v]	d on identity groups and/or other conditions. Drag and drop rules to chang	ge the order.
<ul> <li>Exceptions (0)</li> <li>Standard</li> </ul>		
Status Rule Name	Conditions (identity groups and other conditions)	Permissions
Wireless Black List Default	if Blacklist AND Wireless_802.1X	then Blackhole_Wireless_Access Edit   -
🖉 🗹 👻 Deny BlackBerry	if BlackB 💠 and Condition(s)	🔶 then AuthZ Profil 🗢 Done
Default	if no matches, then PermitAcces	Edit   🕶
Save	Select an item	Standard Standa

Step 10: Click Done, and then click Save.

**Procedure 4** 

**Create downloadable access lists** 

An organization may decide to allow employees to bring in their own devices and use them on the corporate network. However, they may wish to apply some access controls to limit which parts of the network the user is allowed to access from their personal device. This can be based on the AD group to which the user belongs and also which services the user will need, such as access to a virtualized desktop. For wired devices, the access list is defined in Cisco ISE and it is pushed to the switch.

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

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

Step 3: Click Add.

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

**Step 5:** In the DACL Content section, enter an access list using standard Cisco IOS syntax.

# Step 6: Click Submit.

cisco Identity Services Engine				ise-1 admin Logout	Feedback
🏠 Home Operations 🔻 Policy 🔻 Ac	minis	stration 🔻		👓 Task Navigator 🕚	- 🕗
🚨 Authentication 🛛 🧕 Authorization	K F	Profiling 💽 Postu	ire 👩 Client Provisioning 🚊 Security Group Access	🔒 Policy Elements	
Dictionaries Conditions Results					
Results	-	Downloadable ACL List : Downloadable A * Name Description * DACL Content	New Downloadable ACL CL BYOD-IT Bring Your Own Device Access List for the IT Group ip access-list extended BYOD-IT permit ip any host 10.4.48.41 permit pany host 10.4.48.10 permit pin any host 10.4.58.10		
Profiling     Control     Contro     Control     Control     Control     Control     Control		Submit Cano	a		

## Procedure 5

#### **Create profiles for user groups**

The policy in this procedure pushes an access list to the switch or WLC for users in the IT group. The access list can only be deployed for access points in the campus or at remote sites that have a local WLC. This policy is an example and can be modified to suit your environment.

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

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

Step 3: Click Add.

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

**Step 5:** In the Common Task section, select **DACL Name**, and then choose the access list defined in Procedure 4, "Create downloadable access lists." In this example deployment, the ACL is **BYOD-IT**.

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

cisco Identity Services Engine	ise-1 admin Logout Feedback
💧 Home Operations 🔻 Policy 🔻 Adminis	stration 🔹 😐 Task Navigator 🔹 🥹
🛃 Authentication 🛛 🧕 Authorization 🔀 F	Profiling 👩 Posture 🔊 Client Provisioning 🔄 Security Group Access 🔒 Policy Elements
Dictionaries Conditions Results	
Results  Authorization  Composition  Composition	Authorization Profile           * Name       EVOOLT         Description       Error Yure         * Access Type       Access Type         • Common Tasks           • Marced Act Nume       IT         • Advanced Act Putters Settings           • Access Type = ACCESS_ACCEPT           • Advanced Act Putters Settings           • Access Type = ACCESS_ACCEPT           • Complementary           • Complementary

#### Step 7: Click Submit.

Procedure 6

**Create authorization rules for user groups** 

The following steps describe how to create an authorization rule that uses the profile created in Procedure 5, "Create profiles for user groups."

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

**Step 2:** At the end of the Default Rule, click the arrow, and then select **Insert new rule above**. A new rule, Standard Rule 1, is created.

Step 3: Rename Standard Rule 1 to BYOD IT.

Step 4: In the Conditions section, next to Any, click the + symbol.

Step 5: In the list, next to Endpoint Identity Groups, choose the > symbol.

Step 6: Next to Profiled, click the > symbol, and then select Apple-iPad.

Step 7: Next to Apple-iPad, click the + symbol.

Step 8: In the list, next to Endpoint Identity Groups, choose the > symbol.

Step 9: Next to Profiled, click the > symbol, and then choose Android.

Step 10: Next to Android, click the + symbol.

Step 11: In the list, next to Endpoint Identity Groups, choose the > symbol.

**Step 12:** Next to Profiled, click the > symbol, and then choose **Microsoft-Workstation**.

Step 13: Next to Microsoft-Workstation, click the + symbol.

Step 14: In the list, next to Endpoint Identity Groups, choose the > symbol.

Step 15: Next to Profiled, click the > symbol, and then choose OS\_X-Workstation.



Step 16: In the Condition(s) list, click the + symbol, and then click Create New Condition (Advance Option).

**Step 17:** Under Expression, next to Select Attribute, click the arrow. The menu opens.

Step 18: Next to AD1, click the > symbol, and then choose ExternalGroups.

**Step 19:** In the first drop-down list, choose **Equals**, and then, in the second drop-down list, choose **cisco.local/Users/IT**.

cisco Identity Services Engine	ise-1 admin Logout Feedback
🚯 Home Operations 🔻 Policy 💌 Administration 💌	👓 Task Navigator 👻
📕 Authentication 💽 Authorization 🔀 Profiling 💿 Posture 🔂 Client Provisioning 💿 Security Group	Access Access Access
Authorization Policy Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to chang First Matched Rule Apples	e the order.
Exceptions (0) Standard Status Rule Name Conditions (identity groups and other conditions)	Permissons
Wireless Black List Default         if         Blacklist AND Wireless_802.1X	then Blackhole_Wireless_Access Edit   •
Deny BlackBerry if BlackBerry	then Deny_Blackberry Edit   •
BYOD IT if Apple 💠 and Condition(s)	- then AuthZ Profil 💠 Done
Add Al Conditions Below to Library Condition Name Expression Condition Name Expression Condition Name Expression Condition Name Expression Cisco.local/Users/Domain Users Cisco.local/Users/Inance C	Edt   •

**Step 20:** In the Permissions section, next to AuthZ Profile(s), click the **+** symbol.

Step 21: In the Select an item list, next to Standard, click the > symbol.

**Step 22:** Select the BYOD-IT authorization profile that was created in Procedure 5, "Create profiles for user groups."



Step 23: Click Done, and then click Save.

**Step 24:** For each group that you want to define a policy for, repeat Procedure 5, "Create profiles for user groups" and Procedure 6, "Create authorization rules for user groups." In the example deployment described here, you need to create policies for the Finance, HR, and Research groups.

		Operations V Policy V Ac	ministration	-				👓 Task Navi	antor -
				_				-	Jator +
2	Authenti	cation 🧕 Authorization	🛃 Profiling	💽 Posture	🗟 Client Provisioning	🚊 Security Group Access	- *	Policy Elements	
	norization	,							
ìn	e the Auth	orization Policy by configuring rules	based on ide	ntity groups and/	or other conditions. Drag ar	d drop rules to change the orc	Jer.		
st	Matched R	ule Applies 👻							
Ē)	ceptions (	0)							
51	andard								
	Status	Rule Name		Conditions (identi	ity groups and other conditi	ons)		Permissions	
	<b>~</b>	Wireless Black List Default	if	Blacklist AND W	ireless_802.1X		then	Blackhole_Wireless_Access	Edit   🕶
		Deny BlackBerry	if	BlackBerry			then	Deny_Blackberry	Edit   🕶
	<b>~</b>	BYOD IT	if	(Apple-iPad OR	Android OR Microsoft-W	orkstation OR	then	BYOD-IT	Edit   🗸
	_			OS_X-Workstat cisco.local/Users/.	ion) AND AD1:ExternalGrou IT	ips EQUALS			
		BYOD HR	if		Android OR Microsoft-W	orkstation OR	then	BYOD-HR	Edit   🗸
				OS_X-Workstat cisco.local/Users/	ion) AND AD1:ExternalGrou	ips EQUALS			Lost 1 -
	<b>~</b>	BYOD Finance	if		⊣ĸ Android OR Microsoft-W	Industation OD	Manag	BYOD-Finance	
	<u>~</u>	BTOD Hinarite			ion) AND AD1:ExternalGrou		unen	B roo-minance	Edit   🔻
		BYOD Research	if		Android OR Microsoft-W	orkstation OR	then	BYOD-Research	Edit I 👻
					ion) AND AD1:ExternalGrou				Lut   *

# **Enable Device Provisioning**

Cisco ISE allows you to provision a device for network access by deploying digital certificates and configuring the 802.1X supplicant. Digital certificates are a Cisco best practice when deploying 802.1X, as they provide a higher level of assurance than just a username and password. In this example deployment, you deploy digital certificates to Microsoft Windows, Apple Mac OS X, Apple iOS, and Google Android devices. The certificate authority (CA) you use is the one built into Windows Server 2008 Enterprise, and you enable it on the existing Active Directory (AD) server.



Deploying Digital Certificates

- 1. Install certificate authority
- 2. Create template for auto-enrollment
- 3. Edit registry
- 4. Install trusted root certificate for domain
- 5. Install trusted root on AD server
- 6. Request a certificate for ISE from the CA
- 7. Download CA root certificate
- 8. Issue certificate for Cisco ISE
- 9. Install trusted root certificate in ISE
- 10. Configure SCEP
- 11. Install local certificate in Cisco ISE
- 12. Delete old certificate and request

#### **Procedure 1**

#### Install certificate authority

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

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



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

Be sure to install all the latest patches and hotfixes. There are two hotfixes that are required for this deployment, which can be found at the following links:

http://support.microsoft.com/kb/2633200

http://support.microsoft.com/kb/2483564

# **Procedure 2**

**Create template for auto-enrollment** 

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

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

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



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

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

Step 4: In the template properties window, click General, and then enter a name for the template.

Step 5: 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 6: Select Requests can use any CSP available on the subject's computer, and then click OK.

**Step 7:** On the Security tab, click the user created to run SCEP, and then make sure **Allow** is selected for all options: Full Control, Read, Write, Enroll, and Autoenroll.

SCEP User Properties	? ×
	uance Requirements   urity Server
Group or user names:	
& Authenticated Users	
SCEP User (scep_user@cisco.local)	
& Domain Admins (CISCO\Domain Admins) & Domain Users (CISCO\Domain Users)	
Enterprise Admins (CISCO\Enterprise Admins)	
Add	Remove
Permissions for SCEP User Allow	v Deny
Full Control	
Read	
Write	
Enroll	i i i
Autoenroll	
	, <u> </u>
For special permissions or advanced settings, click	Advanced
Advanced.	
Learn about access control and permissions	
OK Cancel Appl	y Help

Step 8: On the Subject Name tab, select Supply in the request.

**Step 9:** On the Extensions tab, click **Application Policies**, and then make sure Client Authentication is listed.

**Step 10:** Click **Basic Constraints**, and then make sure the subject is an end-entity. These are both default settings so they shouldn't need to be modified.

Step 11: Click Issuance Policies, and then click Edit.

Step 12: Click Add, choose All issuance policies, and then click OK.

dit Issuance Policies	Extension	<u>&gt;</u>	<
An issuance policy desc a certificate is issued.	ribes the condit	ions under which	
Issuance policies:			
All issuance policies			
Add	E dit	Remove	
Make this extension	critical		
	ОК	Cancel	
		·	

Step 13: Click OK.

Step 14: Use the defaults for the remaining tabs, click Apply, and then click OK.

Step 15: Close the Certificate Templates Console.

Step 16: In the Certificate Authority console, right-click Certificate Templates, and then navigate to New > Certificate Template to Issue.

ile Action View Help	(Local)\cisco-AD-CA\Certificate Template		
• 🔿 🖄 🞑 😖 👔			
Certification Authority (Local) Gertification Authority (Local) Gerco-AD-CA Revoked Certificates Pending Requests Pailed Requests Certificate Manage <u>New</u> <u>View</u> Refresh Export List <u>Help</u>	Name         Computer (2003 Template)         CEP Encryption         Exchange Enrollment Agent (Offline req         IPSec (Offline request)         Directory Email Replication         Domain Controller Authentication         Certificate Template to Issue         Domain Controller         Web Server         Computer         User         Subordinate Certification Authority         Administrator	Intended Purpose Server Authentication, Clent Authentication Certificate Request Agent IP security IKE intermediate Directory Service Email Replication Client Authentication, Server Authenticatio File Recovery Encrypting File System Client Authentication, Server Authentication Server Authentication Server Authentication Encrypting File System, Secure Email, Clien <ai> Microsoft Trust List Signing, Encrypting File</ai>	

# Step 17: Choose the previously defined template, and then click OK.

🔜 Enable Certificate Templates X Select one Certificate Template to enable on this Certification Authority. Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers. All of the certificate templates in the organization may not be available to your CA. For more information, see Certificate Template Concepts. ٠ Name Intended Purpose Revenue Authentication Client Authentication, Server Authentication, Smart Card Logon, KDC Authent Rev Recovery Agent Key Recovery Agent Response Signing OCSP Signing RAS and IAS Server Client Authentication, Server Authentication Router (Offline request) Client Authentication SCEP User Client Authentication, Secure Email, Encrypting File System Smartcard Logon Client Authentication, Smart Card Ligon Smartcard User Secure Email, Client Authentication, Smart Card Logon 🗷 Trust List Signing Microsoft Trust List Signing 🖳 User Signature Only Secure Email. Client Authentication OK Cancel

#### Procedure 3

**Edit registry** 

There are a few changes that need to be made to the registry to support auto-enrollment in order to complete the installation.

Step 1: On the certificate authority, navigate to Start > Run, enter regedit, and then click OK. The Windows Registry Editor opens.

During the installation of the Network Device Enrollment Service, you created a user for the Simple Certificate Enrollment Protocol (SCEP). This user needs to have full access to the HKEY\_LOCAL\_MACHINE\SOFTWARE\ Microsoft\Cryptography\MSCEP key.

# Step 2: Right-click HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\ Cryptography\MSCEP, and then select Permissions.

**Step 3:** Select the user that you created for SCEP during installation, in the Allow section select **Full Control**, and then click **OK**.

Permissions for MSCEP			×
Security			
Group or user names:			
& CREATOR OWNER			
SYSTEM SCEP User (scep_user@cisco	.local)		
& Administrators (CISCO\Adminis	-		
& Users (CISCO\Users)			
[	Add	Remove	
-	////	- Hellove	
Permissions for SCEP User	Allow	Deny	
Full Control			
Read Special permissions			
For special permissions or advanced	d settings,	Advanced	
click Advanced.	_		
Learn about access control and per	missions		
ОК	Cancel	Apply	

**Step 4:** There are three values for certificate templates in the HKEY\_ LOCAL\_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP key that need to point to the template that you created in Procedure 2. Those values are EncryptionTemplate, GeneralPurposeTemplate, and SignatureTemplate.

Step 5: Right click EncryptionTemplate, and then choose Modify.

**Step 6:** In the Value Data box, enter the name of the template created in Procedure 2, and then click **OK**.

Edit String				×
Value name:				
Encryption Template				
Value data:				
SCEPUser	2			
		OK	Cancel	

**Step 7:** Repeat Step 4 and Step 5 for GeneralPurposeTemplate and SignatureTemplate.

🎲 Registry Editor				
File Edit View Favorites Help				
CAType	Name (Default) (Defa	Type REG_SZ REG_SZ REG_SZ REG_SZ	Data (value not set) SCEPUser SCEPUser SCEPUser	
Computer HKEY_LOCAL_MACHINE\SOFTWAR	<ul> <li>◄</li> <li>■</li> <li>■</li></ul>	:EP		Þ

You will need to disable the HKEY\_LOCAL\_MACHINE\SOFTWARE\ Microsoft\Cryptography\MSCEP\UseSinglePassword key.

# Step 8: Click on HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\ Cryptography\MSCEP\UseSinglePassword.

Step 9: Right click on UseSinglePassword value, and then choose Modify.

# Step 10: In the Value Data box, enter 0 and then click OK.

Edit DWORD (32-bit) Value	×
Value name:	
UseSinglePassword	
Value data:	Base
0	Hexadecimal
	C Decimal
	OK Cancel

#### **Procedure 4**

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 CA	<u>Home</u>
Download a CA Certificate, Certificate Chain, or CRL	
To trust certificates issued from this certification authority, install this CA certificate.	
To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.	
CA certificate:	
Current (CA)	
© DER	
C Base 64	
Install CA certificate	
Download CA certificate	
Download CA certificate chain	
Download latest base CRL	
Download latest delta CRL	

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

Step 6: Expand 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 He	lp	_ 8 ×
🧇 🔿 🖄 🖬 🖡 🖄 🕺		
Group Policy Management Group Policy Management Group Policy Management Group Policy Group Policy Group Policy Group Policy Group Policy Group Policy Default Domain Controllers Group Policy Default Domain Controllers	Default Domain Policy           Scope         Details         Settings         Delegation           Links         Display links in this location:         Gisco local           cscurity Group         The following sites, domains, and OUs are linked to this GPO:         Enforced           Introllers Po         Enforced         No.         Yes	×
-	Refresh g Help nked to the following WMI filter:	
	cone>	
•		
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.

🗐 Group Policy Management Editor								<u>_     ×</u>
File Action View Help								
🗢 🔿 🖄 📰 📋 🙆 🎰 🔽 🗊								
🖃 👰 Computer Configuration		Issued To	<u>ه</u>		1	(ssued By		E
🖃 🧰 Policies				-		to show in this vi		
🕀 🚞 Software Settings				Inere are no	items t	to snow in this vi	iew.	
🖃 🚞 Windows Settings								
Image: The second se								
Scripts (Startup/Shutdown)								
🖃 🚡 Security Settings								
🕀 📑 Account Policies								
🕀 📑 Local Policies								
🕀 📑 Event Log								
🕀 📴 Restricted Groups								
🕀 📴 System Services								
🕀 📴 Registry								
🗉 🔂 File System								
🛨 🛐 Wired Network (IEEE 802.3) Policies								
Windows Firewall with Advanced Security								
Network List Manager Policies								
<ul> <li>Wireless Network (IEEE 802.11) Policies</li> </ul>								
🖃 🧰 Public Key Policies								
Encrypting File System								
BitLocker Drive Encryption								
Automatic Certificate Request Settings								
Trusted Root Certification Authorities								
Enterprise Trust	Import							
Intermediate Certification Authorities	411-22							
Trusted Publishers	All Tas <u>k</u> s	•						
Untrusted Certificates	View	•						
Trusted People	-							
	Re <u>f</u> resh							
Add a certificate to a store	Export Li	ist						
Idd a certificate to a store	Help							
	Tielp							

Step 9: Click Next.

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



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

Step 12: Click Finish. The certificate imports.

Step 13: Click OK to close the wizard.



Install trusted root on AD server

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

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

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

Step 3: Update the group policy.

C: <> gpupdate



#### Procedure 6

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 Feedba
🛕 Home Operations 🔻 Policy 💌 Adr	ministration 🔻			•	) Task Navigator 👻 📀
🔆 System 🦉 Identity Management	🖀 Network Resources 🛛 🛃 Web Portal Management				
Deployment Licensing Certificates Lo	gging Maintenance Admin Access Settings				
Certificate Operations	Local Certificates			Selec	ted 0   Total 1 😵 🎡 ,
Local Certificates     Certificate Signing Requests	/Edit -Add @Export XDelete			Show All	- 8
S Certificate Store	Friend Import Local Server Certificate	Protocol	Issued To	Issued By	Valid From
SCEP CA Profiles	Defau Generate Self-Signed Certificate Generate Certificate Signing Request	HTTPS,EAP	ise-1.cisco.local	ise-1.cisco.local	Fri, 3 Aug 2012
🜞 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	ging Maintenance Admin Access Settings	
Certificate Operations Confricte Signing Requests Certificate Size Certificate Size Certificate Size Size CA Profiles OCSP Services	Local Certificate Signing Request Generate Certificate Signing Request Certificate Certificate Subject ON=sel.cisco.local Key Length 2D49 Key Length Dots Key Length Context Key Length Context Key Length Context Key Length Key Length Context Key Length	
	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 Feedb
🚖 Home Operations 🔻 Policy 💌 A	vdministration 💌	🕶 Task Navigator 👻 😣
🔆 System 🛛 🖉 Identity Management	🖀 Network Resources 🛛 🗿 Web Portal Management	
Deployment Licensing Certificates L	Logging Maintenance Admin Access Settings	
Certificate Operations	Certificate Signing Requests	Saladad e I Talait e 🦓 🎊
Certificate Operations		Selected 1   Total 1 😵 🎡 🖕
	Certificate Signing Requests	Selected 1   Total 1 👙 🎡 🕳
🔹 Local Certificates		
🔹 Local Certificates 🚭 Certificate Signing Requests	∰rExport XDelete	Show All

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



**Download CA root certificate** 

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

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

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

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

Microsoft Active Directory Certificate Services CA	<u>Home</u>
Download a CA Certificate, Certificate Chain, or CRL	
To trust certificates issued from this certification authority, install this CA certificate.	
To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.	
CA certificate:	
Encoding method: © DER	
O Base 64	
Install CA certificate Download CA certificate Download CA certificate chain Download latest base CRL Download latest delta CRL	

Procedure 8

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 6, "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 CA Home
Submit a Certi	ficate Request or Renewal Request
	red request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or wal request generated by an external source (such as a Web server) in the Saved Request box.
Saved Request:	
	+miq/yM44JXSOYD2YIOH1YKhE3Ru966HdIjGaB3y       fc%zjiloMiJJiXOKNaXerhit#U3z4MnvBnqdlop       W6UFu4SoMSbINYqoW56HoJfiX1t38PeQptQAeuH0       RepCmZVVz9F6BK9QOlngJZJKSSINQk6Gd33uPmP0      END CERTIFICATE REQUEST       Image:
Additional Attrib	utes:
Attributes:	
	Submit >

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

# **Procedure 9**

Install trusted root certificate in ISE

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

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

🏠 Home Operations 🔻 Policy 🔻 🖌	Administration 🔻			👓 Task f	Navigator 👻 😢
🔆 System 🛛 👰 Identity Management	📑 Network Resources 🛛 🛃 Web Portal Managemen				
Deployment Licensing Certificates I	Logging Maintenance Admin Access Settings				
Certificate Operations	Certificate Store				
Certificate Operations	Certificate Store			Selected 0   T	'otal 4 😵 🎡 ,
🔹 Local Certificates	Certificate Store		Sh	Selected 0   T	
🔹 Local Certificates 🔹 Certificate Signing Requests		<ul> <li>Issued To</li> </ul>	Sh Issued By		otal 4 😵 🎡 . 🗾 🔹 🕅 Expiration (
🔹 Local Certificates 💇 Certificate Signing Requests 🕵 Certificate Store	✓ EditImportExport XDelete	▲ Issued To ise-1.cisco.local	-	now All	<ul> <li>Expiration (</li> </ul>
💇 Local Certificates 💇 Certificate Signing Requests 💇 Certificate Store 💇 SCEP CA Profiles	Edit Import Export XDelete     Friendly Name		Issued By	ow All Valid From	Expiration I Sat, 3 Aug
Local Certificates     Certificate Signing Requests     Certificate Store	Edit      ♣Import      �PExport      XDelete     Priendly Name     ise-1.cisco.local#00001	ise-1.cisco.local	Issued By ise-1.cisco.local	ow All Valid From Fri, 3 Aug 2012	- 9

**Step 3:** Click **Browse**, and then locate the root CA certificate saved in Procedure 7, "Download CA root certificate."

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

cisco Identity Services Engine	se-1 admin Logout Feedback
🛕 Home Operations 🔻 Policy 🔻 Administra	ation 🔹 😐 Task Navigator 👻 🕗
🔆 System 🏾 🖉 Identity Management 🛛 🖀 Ne	stwork Resources 😹 Web Portal Management
Deployment Licensing Certificates Logging	Maintenance Admin Access Settings
Certificate Enerations	Certificate Store > Import Import a new Certificate into the Certificate Store * Certificate File [C\Downloads/potcert.cer   Browse.
Certificate Store     SCEP CA Profiles	Friendly Name 0
CCSP Services	All Trust Certificates are available for selection as the Root CA for secure LDAP connections. In addition, they may be enabled for EAP-TLS and administrative authentication below:
	Trust for client authentication Trust for client authentication Cathenesis (accept only valid certificate)
	Description

## Procedure 10 Configu

Configure SCEP

To support self-provisioning, you need to configure Cisco ISE to support SCEP, in order to enable Cisco ISE to obtain and then provision certificates for clients.

**Step 1:** On the menu bar, mouse over **Administration**, and then, in the System section, choose **Certificates**.

**Step 2:** In the Certificate Operations pane, click **SCEP CA Profiles**, and then click **Add**.

**Step 3:** Enter a profile name and description, and then enter the URL for the SCEP service. For this deployment, the URL is http://ca.cisco.local/certsrv/mscep/mscep.dll.

Step 4: Click Submit.



Procedure 11

**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 Log	jout Feedba
🛕 Home Operations 🔻 Policy 💌 A	dministration 💌	😶 Task Navig	jator 👻 😢
🔆 System 🛛 👰 Identity Management	🖀 Network Resources 🛛 🛃 Web Portal Management		
Deployment Licensing Certificates L	ogging Maintenance Admin Access Settings		
Certificate Operations	Local Certificates		
		Selected 0   Total	😔 🎡 🗸
💇 Local Certificates	/Edit -Add - Export XDelete	Selected 0   Total - Show All	• 😵 •
	Event Import Local Server Certificate	Show All	
🔹 Local Certificates 🔹 Certificate Signing Requests	Transit Lord Course Carthering	Show All Issued By Valid	- 8

**Step 4:** Click **Browse** and locate the certificate saved from Procedure 8, "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 💌 Admi	istration 🔻	👓 Task Navigator 👻 🕗
🔆 System 🛛 👰 Identity Management 🛛 📲	Network Resources 🛛 🛃 Web Portal Management	
Deployment Licensing Certificates Logo	ng Maintenance Admin Access Settings	
Certificate Operations	Local Cettficate > Dind CA Signed Certificate Bind CA Signed Certificate Certificate	
Cerbificate Store     SCEP CA Profiles     OCSP Services	Certificate File C\Downloads\USEcert.cer     Filendy Name	
		same Subject or Issuer and serial the certificate contents to be

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

# Procedure 12

• 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 Feedba
🏠 Home Operations 🔻 Policy 💌 A	ministration 🔻	🕶 Task Navigator 👻 😢
🔆 System 🛛 🖉 Identity Management	🗑 Network Resources 🛛 🛃 Web Portal Management	
Deployment Licensing Certificates L	igging Maintenance Admin Access Settings	
Certificate Operations	Local Certificates	Selected O   Total 2   🍪 🤹
Certificate Signing Requests	✓ Cdit ♣Add @Export XDelete	Show All
S Certificate Store	Friendly Name     Protocol	Issued To Issued By
SCEP CA Profiles	Default self-signed server certificate	ise1.cisco.local ise1.cisco.local
OCSP Services	ise-1.cisco.local#CA HTTPS,EAP	ise-1.cisco.local CA

Step 4: Click Delete, and then click OK.

# Step 5: Click Certificate Signing Requests.

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

cisco Identity Services Engine				ise-1 admin Logout Feedback
🛕 Home Operations 🔻 Policy 💌 Admi	nistration 🔻			👓 Task Navigator 👻 🕗
😽 System 🦉 Identity Management 🛛	🖥 Network Resources 🛛 🛃 Web F	Portal Management		
Deployment Licensing Certificates Logo	ging Maintenance Admin Acce	ss Settings		
Certificate Operations	Certificate Signing Reques	ts		Selected 1   Total 1 😵 🎬 🖕
🙊 Local Certificates	a			
🔹 Certificate Signing Requests	Export XDelete			Show All
💩 Certificate Store	Friendly Name	<ul> <li>Certificate Subject</li> </ul>	Key Length	Timestamp
SCEP CA Profiles	✓ ise1.cisco.local	CN=ise1.cisco.local	2048	Wed Aug 15 08:48:18 PDT 2012
S OCSP Services				

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

Next, you configure Cisco ISE to provision digital certificates and the 802.1X supplicant for Microsoft Windows, Apple OS X, Apple iOS and Google Android devices. To do this, you create a client provisioning profile for each operating system you wish to provision, and then apply this profile to the authentication profile. You also create a new authorization profile for these devices.

# Process



Configuring Self-Provisioning

- 1. Create AD group for provisioning
- 2. Enable AD group in Cisco ISE
- 3. Enable EAP-TLS
- 4. Enable self-provisioning portal
- 5. Create user authentication policies
- 6. Create native supplicant profile
- 7. Define provisioning policy
- 8. Modify wired authentication policy
- 9. Modify wireless authentication policy
- 10. Create wired authorization profiles
- 11. Configure wired provisioning authorization
- 12. Create wireless authorization profile
- 13. Configure wireless provisioning auth. rule
- 14. Create Android authorization profile
- 15. Create Android provisioning rule
- 16.Create wired 802.1X authorization rule
- 17. Create wireless 802.1X authorization rule
- 18. Modify default rule
- 19. Configure WLCs
- 20.Enable captive portal bypass
- 21. Create authorization rules for user groups
- 22.Delete 802.1X rules
- 23. Provision a Windows workstation
- 24. Provision a Mac OS X workstation
- 25.Provision an Apple iPad
- 26.Provision an Android tablet

### Procedure 1

#### **Create AD group for provisioning**

To simplify the deployment, you create a group in Active Directory for users that are allowed to perform self-provisioning.

Step 1: Open the AD server console, and then navigate to Start > Administrative Tools > Active Directory Users and Computers.

Step 2: From the Action menu, click New, and then select Group.

Step 3: Enter a name for the group, and then click OK.

New Object - Group	×
Create in: cisco.local/l	Users
Group name:	
BYOD Provisioning	
Group name (pre-Windows 2000):	
BYOD Provisioning	
Group scope	Group type
C Domain local	Security
Global	O Distribution
C Universal	
	OK Cancel

**Step 4:** Double-click the group name. This opens the group properties window and allows you to add users to the group.

Step 5: Click the Members tab, and then click Add.

**Step 6:** Enter the users you wish to add, and then click **OK**.

Step 7: Click Apply, and then click OK.

BYOD Provisioning Pr	operties	? ×
General Members	Member Of Managed By	
Members:		
Name	Active Directory Domain Services Folder	
👗 Alex Reed	cisco.local/Users	
	cisco.local/Users	
👗 Pat Jones	cisco.local/Users	
		- U
Add	Remove	
	OK Cancel A	pply

#### Procedure 2

• Enable AD group in Cisco ISE

You must now configure Cisco ISE to use this new group for authentication.

Step 1: In your browser, enter https://ise-1.cisco.local.

**Step 2:** On the menu bar, mouse over **Administration**, and then, in the Identity Management section, select **External Identity Sources**.

Step 3: In the left pane, click Active Directory, and then select Groups.

# Step 4: Click Add, and then choose Select Groups From Directory.

**Step 5:** Search for the group you wish to add. The domain field is already filled in. The default filter is a wildcard to list all groups. You can click **Retrieve Groups** if you want to get a list of all groups in your domain.

**Step 6:** Select the group you want to use for BYOD provisioning, and then click **OK**.

This dialog is used to select groups from the Directory. Click Retrieve Groups to read directory.         Use * for wildcard search (i.e. admin*). Search filter applies to group name and not the fully qualified path.         Domain:       cisco.local         Filter:       *	
Domain: cisco.local	
Filter: * Retrieve Groups Number of Groups Retrieved: 60 (Limit is 100)	
Name Group T	y
	1
Cisco.local/Builtin/Windows Authorization Access Group LOCA	
Cisco.local/Builtin/vpn-user GLOB	
cisco.local/Citrix XenDesktops/xendesktop-administrator GLOB	
cisco.local/Citrix XenDesktops/xendesktop-user GLOB	
Cisco.local/Users/Allowed RODC Password Replication Group	11
✓ cisco.local/Users/BYOD Provisioning GLOB	Ш
Cisco.local/Users/Cert Publishers LOCA	1
Cisco.local/Users/DHCP Administrators LOCA	
Cisco.local/Users/DHCP Users LOCA	
Cisco.local/Users/Denied RODC Password Replication Group LOCA	
Cisco.local/Users/DnsAdmins LOCA	
Cisco.local/Users/DnsUpdateProxy GLOB	
Cisco.local/Users/Domain Admins GLOB	1
	1
	-
OK	

**Procedure 3** 

**Enable EAP-TLS** 

In a previous section, you disabled EAP-TLS. Now that you are using digital certificates, you need to 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	bel a	dmin Logout Feedback
🏠 Home Operations 🔻 Policy 🔻 Adm	ninistration 🔻 😐 😶	Task Navigator 👻 😢
🛃 Authentication 🛛 🧕 Authorization 🔀	Profiling 🖗 Posture 🕞 Client Provisioning 🔄 Security Group Access 🔒 Policy Elements	
Dictionaries Conditions Results		
Persuits       Image: Second Seco		

**Procedure 4** 

• Enable self-provisioning portal

Self-provisioning uses the guest web portal, and you need to modify the default guest portal to support self-provisioning.

**Step 1:** From the **Administration** menu, in the Web Portal Management section, select **Settings**.

Step 2: In the Settings section, double-click Guest, double-click Multi-Portal Configurations, and then click DefaultGuestPortal. Step 3: On the Operations tab, make sure Enable Self-Provisioning Flow is selected, and then click Save.



Procedure 5

**Create user authentication policies** 

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

**Step 1:** On the menu bar, mouse over **Administration**, and then, in the Identity Management section, choose **External Identity Sources**.

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



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

cisco Identity Services Engine		ise-1 admin Logout Feedback
🛕 Home Operations 🔻 Policy 🔻 Admi	nistration 🔻	👓 Task Navigator 👻 😣
🔆 System 🏾 👰 Identity Management	Network Resources 🛃 Web Portal Management	
Identities Groups External Identity Sources	Identity Source Sequences Settings	
External Identity Sources	Certificte Authentication Profile Lid > New Certificate Authentication Profile Certificate Authentication Profile * Name Dot1X_User_Certs Description Principal Username X509 Attribute Common Name Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active LDAP/AD Instance Name Stampt Cancel	्रती Pirectory

#### Step 4: Click Submit.

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

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

IlII. cisco Identity Services Engine			ise-1 admin Logout Feedba
🔥 Home Operations 🔻 Policy 🔻	Administration 🔻		👓 Task Navigator 👻 🕙
🔆 System 🦉 Identity Management	🖀 Network Resources 🛛 🛃 Guest Management		
dentities Groups External Identity So	urces Identity Source Sequences Settings		
lentity Source Sequence			Selected 0   Total 2 🥳
/ Edit 🕂 Add 🖓 Duplicate 🗙 Delete		Show All	- 6
Name	<ul> <li>Description</li> </ul>	Identity Stores	
Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal	Internal Users	

Step 6: Give the sequence a meaningful name.

**Step 7:** In the Certificate Based Authentication section, select **Select Certificate Authentication Profile**, and then choose the profile created in Step 2 through Step 3.

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

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

cisco Identity Services Engine ise-1 admin Logout Feed
🏠 Home Operations 🔻 Policy 👻 Administration 💌 🤒 😶 Task Navigator 👻
🔆 System 🛛 👰 Identity Management 📲 Network Resources 🛛 🛃 Web Portal 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_Users
Description
Certificate Based Authentication     Select Certificate Authentication Profile Dot1X_User_Certs     Authentication Search List     A set of identity sources that will be accessed in sequence until first authentication succeeds
Available Selected
Internal Endpoints Internal Users
Advanced Search List Settings
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 6

Create native supplicant profile

You need to create a native supplicant profile for each operating system that is used for self-provisioning.

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

Step 2: In the Results section, double-click Client Provisioning, and then click Resources.

# Step 3: Click Add, and then choose Native Supplicant Profile.

🛕 Home Operations 🔻 Policy 🔹	Admin	istration 🔻				👓 Task Navigator 👻 🌔
🔺 Authentication 🛛 🧕 Authorization	🛃 Pr	ofiling 🦉	💈 Posture 🛛 🔂 Client Provisio	ning 🛛 🚊 Security Group A	Access 🔒 Polic	cy Elements
Dictionaries Conditions Results						
Results		Resource	25			Selected 0   Total 2
=	2	/ Edit	+Add - BDuplicate 🗙 D	elete	Show All	- F
		Nam	Agent resources from Cisco site	slete Type	Show All	- ▼ F
		Nam	Agent resources from Cisco site Agent resources from local disk	7		
Authentication		Nam	Agent resources from Cisco site Agent resources from local disk ISE Posture Agent Profile	Туре	Version	Last Update
Authentication     Authorization     Defining		Nam	Agent resources from Cisco site Agent resources from local disk	Type WinSPWizard	Version 1.0.0.19	Last Update 2012/05/15 13:07:30
		Nam	Agent resources from Cisco site Agent resources from local disk ISE Posture Agent Profile	Type WinSPWizard	Version 1.0.0.19	Last Update 2012/05/15 13:07:30

Step 4: Enter a name and description for the profile.

**Step 5:** Enter the SSID for your wireless network.

Step 6: In the Allowed Protocol list, choose TLS, for the remaining options, use the default values, and then click Submit.

cisco Identity Services Engine				ise-1 admin Logout Feedback
🛕 Home Operations 🔻 Policy 🔻 Adm	inistration 🔻			😶 Task Navigator 👻 🕗
💄 Authentication 🛛 🧕 Authorization 🔀 F	Profiling 💽 Posture 🛛	🖌 Client Provisioning 🛛 🚊 Securit	ty Group Access	Policy Elements
Dictionaries Conditions Results				
Results ♪ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓	Native Supplicant Profile > New St Native Supplicant Profi			
Authentication	* Name	EAP-TLS Profile		
Authorization     Profiling     Posture	Description	EAP-TLS Native Supplicant Profile		
Client Provisioning	* Operating System	ALL 💠		
E Resources	* Connection Type	<ul> <li>✓ Wired</li> <li>✓ Wireless</li> </ul>		
	*SSID	WLAN-Data		
	Security	WPA2 Enterprise 🔹		
	* Allowed Protocol	TLS 🔹		
	* Key Size	1024 💌	۲	
	Submit Cancel			

#### **Procedure 7**

#### **Define provisioning policy**

You create a provisioning policy for each operating system in order to determine which supplicant profile to apply.

Step 1: On the menu bar, mouse over Policy, and then choose Client Provisioning.

Step 2: Click Add.

Step 3: Enter a name for the rule.

**Step 4:** In the Operating Systems section, click the + symbol, and then select **Apple iOS All**.



**Step 5:** Next to Result, click the + symbol, and then select the profile created in Procedure 6.

A Home Operations V Policy V Administration V
🛃 Authentication 🛛 👩 Authorization 🧭 Profiling 👘 Posture 🛛 🙀 Client Provisioning 📄 Security Group Access 👘 🦺 Policy Elements
Authentication Authonization Profiling Posture Center Provisioning Security Group Access Policy Elements Define the Clent Provisioning Policy to determine what users will receive upon login and user session initiation: Provisioning Policy and Policy Elements Provisioning Policy Elements Define the Clent Provisioning Policy to determine what users will receive upon login and user session initiation: Provisioning Policy to determine what users will receive upon login and user session initiation: Provisioning Policy Elements Provide the Clent Provisioning Policy to determine what users will receive upon login and user session initiation: Provisioning Policy Elements Provide the Clent Provisioning Policy to determine what users will receive upon login and user session initiation: Provisioning Policy Elements Provide Policy Elements Rule Name Identity Groups Operating Systems Other Conditions Results Results Provide Policy If Any Provide Policy Pol

Step 6: Click Actions, and then select Insert new policy below.

**Step 7:** Create a rule for Android devices by repeating Step 3 through Step 5.

Next, create a rule for Windows devices.

Step 8: Click Actions, and then select Insert new policy below.

Step 9: Enter a name for the rule.

**Step 10:** In the Operating Systems section, click the + symbol, and then select **Windows All**.

Step 11: Next to Result, click the + symbol.

**Step 12:** In the **Config Wizard** list in the Native Supplicant Configuration section, click the gear icon, and choose **Download Resource**.

cisco Identity Services Engine				ise-1 admin Logout Feedback
🛕 Home Operations 🔻 Policy 💌 Administration 💌				👓 Task Navigator 👻 🕙
🛃 Authentication 💿 Authorization 🔀 Profiling	🕐 Posture 🛛 🕞 Client Prov	isioning 📑 Security Gro.	up Access 💦 🐥 Policy Elements	
Client Provisioning Policy				<b>_</b>
Define the Client Provisioning Policy to determine what users will re For Agent Configuration: version of agent, agent profile, agent con For Native Supplicant Configuration: wizard profile and/or wizard.	ceive upon login and user session pliance module, and/or agent o	nitiation: stomization nackade ConfigWizard		
·		<b>↓</b>	P Besuits	
	erating Systems Other C pple iO 💠 and Condi	Clear Selection	Results     Download Resource     We Upload Resource	💠 🏰 Actions 👻
Android If Any 🗇 and A	ndroid 🔶 and Condi		EAP-TLS Profile	🔶 🎬 Actions 🔻
Windows If Any 🔶 and N	Vindow 🔶 and Condi		Result 🗢	🕸 Actions 👻
Agent Configuration	1			
Agent:	Choose an Agent		ory	
Profile:	Choose a Profile			
Compliance Module:	Choose a Compliance Mod			
Agent Customization Pac	kage: Choose a Customization P			
Native Supplicant D	onfiguration			
Config Wizard: Choose a	Config Wizard (	2		
Wizard Profile: Choose a	Wizard Profile (	2		
				_

**Step 13:** Choose the latest version of the WinSPWizard and click **Save**. This downloads the most current wizard.

Name	<ul> <li>Type</li> </ul>	Version	Description
U Marie MacusxAgent 4.9.0.654	MacusxAgent	4.9.0.654	Posture Agent for Mac USX (15E
MacOsXAgent 4.9.0.655	MacOsXAgent	4.9.0.655	Posture Agent for Mac OSX (ISE
MacOsXAgent 4.9.0.659	MacOsXAgent	4.9.0.659	Posture Agent for Mac OS X v4
MacOsXSPWizard 1.0.0.11	MacOsXSPWizard	1.0.0.11	Supplicant Provisioning Wizard fo
MacOsXSPWizard 1.0.0.18	MacOsXSPWizard	1.0.0.18	Supplicant Provisioning Wizard fo
NACAgent 4.9.0.37	NACAgent	4.9.0.37	Windows Agent (ISE 1.0MR only)
NACAgent 4.9.0.37	NACAgent	4.9.0.37	Windows Agent (ISE 1.1 releas
NACAgent 4.9.0.42	NACAgent	4.9.0.42	Windows Agent (ISE 1.1.1 or la
NACAgent 4.9.0.47	NACAgent	4.9.0.47	Windows Agent with Win8 OS s
NACAgent 4.9.0.51	NACAgent	4.9.0.51	Windows Agent (ISE 1.1.3 Rele
WebAgent 4.9.0.20	WebAgent	4.9.0.20	Web Agent (ISE 1.0MR only)
WebAgent 4.9.0.24	WebAgent	4.9.0.24	Web Agent (ISE 1.1.1 or later)
WebAgent 4.9.0.27	WebAgent	4.9.0.27	Web Agent with Win8 OS supp
WebAgent 4.9.0.28	WebAgent	4.9.0.28	Web Agent (ISE 1.1.3 release)
WinSPWizard 1.0.0.22	WinSPWizard	1.0.0.22	Supplicant Provisioning Wizard fo
WinSPWizard 1.0.0.23	WinSPWizard	1.0.0.23	SP Wizard for Windows with Wi
✓ WinSPWizard 1.0.0.28	WinSPWizard	1.0.0.28	Supplicant Provisioning Wizard fo

Step 14: Next to Result, click the + symbol.

**Step 15:** In the **Config Wizard** list in the Native Supplicant Configuration section, choose **WinSPWizard**.

**Step 16:** In the **Wizard Profile** list in the Native Supplicant Configuration section, choose the profile created in Procedure 6, "Create native supplicant profile."

	Policy 🔻 Administration 🔻				👓 Task Navigator 🔻
🛓 Authentication 🛛 🧕 Au	thorization 🔀 Profiling 💽	Posture 🔂 Client Provisioning 🤶	Security Group Access	Policy Elements	
nt Provisioning Policy					
ne the Client Provisioning Polic		e upon login and user session initiation:			
Agent Configuration: version o Native Supplicant Configuratior	f agent, agent profile, agent compile 1: wizard profile and/or wizard.	ince module, and/or agent customization par	ckage.		
Rule Name	Identity Groups Opera	ting Systems Other Conditions	R	esults	
Apple iOS	If Any 🗇 and App	e iO 💠 and Condition(s)	🔶 then 🛛 E	AP-TLS Profile 🔶	🙀 Actions 🕶
-					
Android	If Any 🔶 and And	roid 🔶 and Condition(s)	🚓 then E	AP-TLS Profile 🔶	🚔 Actions 🔻
Vindows	If Any 🔶 and Win	dow 🔶 and Condition(s)	🔶 then 🛛 F	esult 🗢	🖗 Actions 🔻
	Agent Configuration				
	Agent:		S Upgrade Mandatory		
	Profile:		0		
	Compliance Module:	· ·	0		
	Agent Customization Packag	e: Choose a Customization Package	0		
	Native Supplicant Conf	quiration			
	Config Wizard: WinSPWizard	5			

Next, create a rule for Mac OS devices.

Step 17: Click Actions, and then select Insert new policy below.

Step 18: Enter a name for the rule.

**Step 19:** In the Operating Systems section, click the + symbol, and then select **Mac OSX**.

Step 20: Next to Result, click the + symbol.

**Step 21:** In the **Config Wizard** list in the Native Supplicant Configuration section, click the gear icon, and choose **Download Resource**.

**Step 22:** Choose the latest version of the MacOsXSPWizard and click **Save**. This downloads the most current wizard.

Step 23: Next to Result, click the + symbol.

Step 24: In the Native Supplicant Configuration section, in the Config Wizard list, choose MacOsXSPWizard.

**Step 25:** In the Native Supplicant Configuration section, in the **Wizard Profile** list, choose the profile created in Procedure 6, "Create native supplicant profile," and then click **Save**.

	Operations •	Policy 🔻	Administration	•						😶 Task I	Vavigator 👻
🛓 Authe	entication 🧕	Authorization	🔀 Profiling	💽 Postu	e 🗔 Ci	ent Provisioning	🧕 Security G	oup Access	🔒 Policy Element	s	
ent Prov	isioning Policy										
Agent Co	infiguration: versio	n of agent, ager	t profile, agent i	compliance mo		er session initiation agent customizati					
Native Su	ipplicant Configura	ition: wizard profi	e and/or wizard.								
	Rule Name	Ider	tity Groups	Operating Sy	stems	Other Conditions			Results		
-	Apple iOS	If An	y 💠 and	Apple iO	4) and	Condition(s)		<>> then	EAP-TLS Profile	\$	Actions 👻
-	Android	If An	y 🔶 and	Android	💠 and	Condition(s)		🔶 then	EAP-TLS Profile	\$ \$	Actions 🔻
	Windows	If An	y 🔶 and	Window	4> and	Condition(s)		then		<u>i</u>	Actions 👻
-		EAP-TLS Profile	¢								
	izard 1.0.0.28 And										

### Procedure 8

Modify wired authentication policy

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 wired users.

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

For wired users, you should modify the authentication policy to first check if the client is using EAP-TLS and then, if not, to allow them to use an authentication method such as Protected Extensible Authentication Protocol (PEAP) that uses a username and password for credentials. This allows users who haven't gotten certificates yet to still access the network. When they connect to the network, the provisioning process pushes a certificate to the device.

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

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

🏠 Home Operations 🔻 Policy	<ul> <li>Administ</li> </ul>	ration 🔻							👓 Tasi	Navigator 👻
🛃 Authentication 🛛 🧕 Authorizat	tion 🔀 Pr	ofiling 🛛 💽 Pi	osture	🛃 Client Provisio	ning 🚊 Sec	urity Group Access	🔷 🐥 Po	licy Elements		
thentication Policy										
ine the Authentication Policy by select	tion the sectors	ale that ICC should		mener minutes with t	na nakundu davia	an and the identity	an see a	and the selection class of	en far a daar	tion times.
		us triat the should	u use to co	initiate with t	ne network devit	es, and the identity	sources o	iac ic sriuulu u:		iucauuri.
licy Type ( Simple 💿 Rule-Base	ed .									
							_			
	ed : If	Wired_MAB	¢	allow protocols	Allowed Protoc	ol : Default Netw📀	and	•	- 	Actions 🔻
MAB	: If		-	- ·			_			
licy Type O Simple   Rule-Base MAB Wired-Dot1X		Wired_MAB Wired_802.1X	\$ \$	- ·		ol : Default Netw© ol : Default Netw©	_		\$	Actions 👻
MAB	: If		-	- ·			_			
MAB	: If		-	- ·			_			

**Step 4:** Enter a name for the rule, and then, next to Enter Condition, click the symbol. This opens the expression builder.

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

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

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

uludu. CISCO Identity Services Engine	Network Access	admin Logout Feedback
🛕 Home Operations 🔻 Policy 🔻 Administration 💌	🔶 🔳 📜 👘	Task Navigator 👻 😢
🔍 Authentication 💽 Authorization 🔣 Profiling 💿 Posture 🕟 Client Provisioning 🗟 Security Group	AuthenticationMethod	
	Device IP Address	
Authentication Policy	EapAuthentication	
	EapTunnel	thentication.
Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the Policy Type O Simple  Rule-Based	ISE Host Name	inentication.
	NetworkDeviceName	
If Wired_MAB 🔶 allow protocols Allowed Protocol : Default	Protocol	🐕 Actions 👻
Wired-Dot1X : If Wired 802.1	UseCase	
Wired_Bot1X : If Wired_802.1 Expression Builder	UserName	×
💾 Add All Conditions Below to Library		
EAP-TLS-Wired : If Enter C Condition Name Expression		
Select Attribute		
Default : use   AD1		OK Cancel

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



**Step 9:** Next to Internal Users, click the + symbol.

**Step 10:** In the **Identity Store** list, choose the identity source sequence created in Step 5 of Procedure 5, "Create user authentication policies," use the default options for this identity source, and then click anywhere in the window to continue.

cijulju CISCO Identity Services Engine	ise-1 admin Logout Feedback
🛕 Home Operations 🔻 Policy 🔻 Administration 💌	👓 Task Navigator 👻 😢
📕 Authentication 🛛 Authorization 🔀 Profiling 🕜 Posture 🗔 Client Provisioning 🔄 Security Group Access 💦 🔒 Policy Elements	
Authentication Policy         Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use to communicate with the network devices, and the identity sources that it should use to communicate with the network devices, and the identity sources that it should use to communicate with the network devices, and the identity sources that it should use to communicate with the network devices, and the identity sources that it should use to communicate with the network devices, and the identity sources that it should use to communicate with the network devices, and the identity sources that it if wired_802.1X allow protocols Allowed Protocol: Default Network and a	Actions •

Step 11: Click Save.

# Procedure 9

**Modify wireless authentication policy** 

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 wireless users.

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

For wireless users, you should modify the authentication policy to first check if the client is using EAP-TLS and then, if not, to allow them to use an authentication method like PEAP that uses a username and password for credentials. This allows users who haven't gotten certificates yet to still access the network. When they connect to the network, the provisioning process pushes a certificate to the device.

**Step 2:** To the right of the "and..." on the Wireless-Dot1X rule, click the black triangle. This opens the identity store used for this rule.

Step 3: Next to 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 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-Eased	for authentication.
MAB : If Wired_MAB	🖗 Actions 🕶
🛛 🖌 🛛 Wired-Dot1X : If 🛛 Wired_802.1X 🔶 allow protocols Allowed Protocol : Default Netw 🖉 and 🕨	😂 Actions 🔻
🛛 🔹 🛛 Wireless-Dot1X : If 🛛 Wireless_802.1X 🔶 allow protocols 🛛 Allowed Protocol : Default Netwood 🖌 and 🗸	👙 Actions 👻
Default : use AD1 🔶	Actions
Default Rule (If no match) : allow protocols Allowed Protocol : Default Netwo and use identity source : Internal Users 💠	🚔 Actions 👻

**Step 4:** Enter a name for the rule, and then, next to Enter Condition, click the symbol. This opens the expression builder.

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

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

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



Step 8: In the first list, choose Equals, in the second list, choose EAP-TLS, and then click OK.



Step 9: Next to Internal Users, click the + symbol.

**Step 10:** In the **Identity Store** list, choose the identity source sequence created in Step 5 of Procedure 5, "Create user authentication policies," use the default options for this identity source, and then click anywhere in the window to continue.

cisco Identity Services En	gine Participant Parti	ise-1 admin Logout Feedback
🛕 Home Operations 🔻 Pol	icy 🔻 Administration 🔻	😬 Task Navigator 👻 🕗
🚨 Authentication 🛛 🧕 Author	rization 🔀 Profiling 🖉 Posture 🛃 Clent Provisioning 🔄 Security Group Access 🔒 Policy Elements	
Polcy Type O Simple O Rule-B	: If       Wired_MAB       allow protocols       Allowed Protocol : Default NetwO       and ,         : If       Wired_802.1X       allow protocols       Allowed Protocol : Default NetwO       and ,         : If       Wireless_802.1X       allow protocols       Allowed Protocol : Default NetwO       and ,         : If       Wireless_802.1X       allow protocols       Allowed Protocol : Default NetwO       and ,         : If       Network Access:Expluthenticati       G       use       Internal Users       Internal Users	x authentication.

# Step 11: Click Save.

#### Procedure 10

## **Create wired authorization profiles**

Create authorization profiles in order to configure the access switch to redirect the client to the Cisco ISE provisioning page when the client authenticates to the network without a certificate and also to provision the device with a certificate.

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

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

Step 3: Click Add.

Step 4: Enter a name and description for the profile.

Step 5: Select DACL Name and then, in the list, choose PERMIT\_ALL\_TRAFFIC.

Step 6: Select Web Authentication, and then, in the list, choose Centralized.

**Step 7:** Enter the name of the ACL that will be applied to the switch. This was configured when you enabled low-impact mode in Procedure 3 and Procedure 4 of the "Enabling Authorization for Wired Endpoints" section.

Step 8: In the Redirect list, choose Default.

Step 9: Click Submit.



Step 10: Click Add.

Step 11: Enter a name and description for the profile.

Step 12: Select Web Authentication, and then, in the list, choose Supplicant Provisioning.

**Step 13:** Enter the name of the ACL that will be applied to the switch. This was configured when you enabled low-impact mode in Procedure 3 and Procedure 4 of the "Enabling Authorization for Wired Endpoints" section.

# Step 14: Click Submit.

cisco Identity Services Engine	ise-1 admin Logout Feedback
🏠 Home Operations 🔻 Policy 🔻 Adminis	stration 🔻 😽 😔
🛃 Authentication 💿 Authorization 🔣 P	rofling 🕐 Posture 🗔 Client Provisioning 📄 Security Group Access 🚺 Policy Elements
Dictionaries Conditions Results	
Dictonaries Conditions Results	Addocation Profile > New Authorization Profile  * Name Vired-Provisioning Description Wred Profile For Self-Provisioning * Access Type Access_AccepT  Common Tasks VLAN Common Tasks VLAN Voice Domain Permission Web Authentication Supplicant Provisioning ACL WebAuth Auto Smart Port  Media Cate Settings Setting
	Submit Cancel

Procedure 11

**Configure wired provisioning authorization** 

Next, you configure authorization rules to apply the authorization profile created in the previous step to provision devices not using certificates on the wired network. You will create one policy to allow wired devices that don't have 802.1X supplicants configured to access the network, but they will be redirected to the provisioning portal. The second policy you create is used after the user and device register on the portal and start the provisioning process.

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

**Step 2:** At the end of the first BYOD rule, click the black triangle, and then select **Insert New Rule Above**. A new rule, Standard Rule 1, is created above the BYOD rules that were created earlier.

Step 3: Rename Standard Rule 1 to Wired BYOD.

Step 4: In the Condition(s) list, click the + symbol, and then choose Select Existing Condition from Library.

**Step 5:** In the list, next to Compound Conditions, click the > symbol, and then choose **Wired\_MAB**.

**Step 6:** Next to AuthZ Profile(s), click the + symbol, and then, next to Select an item, click the arrow.

**Step 7:** Next to Standard, click the > symbol, and then choose the authorization profile created in Step 4 of Procedure 10, "Create wired authorization profiles."

#### Step 8: Click Done.

**Step 9:** At the end of the newly created rule, click the black triangle, and then select **Insert New Rule Above**. A new rule, Standard Rule 1, is created above the new rule.

Step 10: Rename Standard Rule 1 to Wired Provisioning.

Step 11: In the Conditions column, next to Any, click the + symbol.

**Step 12:** In the list, next to Endpoint Identity Groups, click the > symbol, and then, next to Profiled, click the > symbol.

Step 13: Choose Microsoft-Workstation.

**Step 14:** Next to Microsoft\_Workstation, click the + symbol.

Step 15: In the list, next to Endpoint Identity Groups, click the > symbol.

# Step 16: Next to Profiled, click the > symbol, and then choose OS\_X-Workstation.

		Administration	·			< Navigator 👻 🕑
🛓 Authent	cation 🧕 Authorization	🛃 Profiling	🖉 Posture 🕞 Client Provisioning 📄 Security Group Acce	ess 🦳 🔒	Policy Elements	
thorizatio ine the Auth st Matched F	orization Policy by configuring ru	iles based on id	entity groups and/or other conditions. Drag and drop rules to change the	order.		
Exceptions (	0)					
Standard						
Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
<b>~</b>	Wireless Black List Default	if	Blacklist AND Wireless_802.1X	then	Blackhole_Wireless_Access	Edit   👻
	Profiled Cisco IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phones	Edit   🕶
<b>~</b>	Profiled Cisco APs	if	Cisco-Access-Point	then	Cisco_APs	Edit   🕶
	Deny BlackBerry	if	BlackBerry	then	Deny_BlackBerry	Edit   🕶
1 🗹 🔹	Wired Provisioning	if	Any 🗢 and Condition(s) 💠	1	hen 🛛 AuthZ Profil 💠	Done
1	Wired BYOD	if		en	Wired-BYOD	Edit   🔻
	BYOD IT	if	Microsoft-Workstation Or -	en	BYOD-IT	Edit   🕶
	BYOD HR	if	OS_X-Workstation 📀 🤤 🕁	en	BYOD-HR	Edit   🕶
	BYOD Finance	if	cisco.local/Users/HR (Apple-iPad OR Android OR Microsoft-Workstation OR OS_X-Workstation) NND AD1:ExternalGroups EQUALS cisco.local/Users/Finance	then	BYOD-Finance	Edit   🕶
	BYOD Research	if	(Apple-iPad OR Android OR Microsoft-Workstation OR	then	BYOD-Research	Edit   🗸

Step 17: In the Condition(s) list, click the + symbol, and then choose Select Existing Condition from Library.

**Step 18:** In the list, next to Compound Conditions, click the > symbol, and then choose **Wired\_MAB**.

🟠 Home Operations 🔻	Policy 🔻 Administration 🔹	,				90 T	ask Navigator 👻	0
Authentication	ithorization 🔣 Profiling	💽 Posture	🕞 Client Provisioning	🚊 Security Group A	.ccess 🔗 🦧	Policy Elements		
uthorization Policy efine the Authorization Policy by	and an other or dear large and any balance							
	Compound Conditions	uty groups and/	ir other conditions, brag an	ia arop rules to change i	the order.			
irst Matched Rule Applies		P						
Exceptions (0)	<b>↓</b> • ■ 1≣							
Standard	Wired_802.1X	10. T						
Stanuaru	Wired_MAB							
Status Rule Name	Wireless_802.1X	jidenti	y groups and other condition	ons)		Permissions		
🔽 🛛 Wireless Black Li	Wireless_MAB	ND W	eless_802.1X		then	Blackhole_Wireless_Access	Edit	
Profiled Cisco IF	Catalyst_Switch_Local_Web	Authentica			then	Cisco IP_Phones	Edit I •	
	WLC_Web_Authentication						Eur	
Profiled Cisco Al	EAP-Chaining-User-and-Mach	nine-Cert ss-Pc	int		then	Cisco_APs	Edit	
🗹 Deny BlackBerry					then	Deny_BlackBerry	Edit	
🖉 🔽 👻 🛛 Wired Provisionin		\$	and Select Attribute		-	then 🛛 AuthZ Profil 🔶	Done	
🖉 💾 Add All Conditions B					then	Wired-BYOD	Edit   •	
Condition Name					then	BYOD-IT	Edit	
	2			- A9-∓				

**Step 19:** At the end of this rule, click the gear icon, and then select **Add Attribute/Value**.

Step 20: Next to Select Attribute, click the arrow. The menu opens.

Step 21: Next to AD1, click the > symbol, and then choose ExternalGroups.

**Step 22:** Under Expression, in the first list, choose **Equals**, and then, in the second list, choose the BYOD group created in Procedure 2, "Enable AD group in Cisco ISE."

	perations 🔻 Policy 🔻	Administration 🔻						al Nazartan 🙆
					_			ask Navigator 👻
🛓 Authentica	tion 🧕 Authorization	n 🔀 Profiling	💽 Posture 🛛 🔂 Client	Provisioning 🚊 Sec	curity Group Access		Policy Elements	
uthorization I	,							
efine the Authori	zation Policy by configurin	g rules based on ident	tity groups and/or other cond	itions. Drag and drop rule	as to change the on	der.		
First Matched Rule	e Applies ,	-						
<ul> <li>Exceptions (0)</li> </ul>								
Standard								
	Rule Name		onditions (identity groups and				Permissions	
	Wireless Black List Default	if B	lacklist AND Wireless_802.1X			then	Blackhole_Wireless_Access	Edit   🕶
	Profiled Cisco IP Phones	if D	isco-IP-Phone			then	Cisco_IP_Phones	Edit   🗸
	Profiled Cisco APs	if C	isco-Access-Point			then	Cisco_APs	Edit   🖛
I I	Deny BlackBerry	if B	lackBerry			then	Deny_BlackBerry	Edit   🕶
								-
🖉 🗸 👻 V	vired Provisioning	if	Micros 🔶 and Con	dition(s)	-		then AuthZ Profil 🔶	Done
	-	brany			-	then	Wired-BYOD	Edit   🕶
	All Conditions Below to Li							
🖉 💾 Add								
🖉 💾 Add	dition Name E	Expression	UALS Call Check AND Radius:N	AND -		then	BYOD-IT	Edit   🔻

**Step 23:** Next to AuthZ Profile(s), click the + symbol, and then, next to Select an item, click the arrow.

**Step 24:** Next to Standard, click the > symbol, and then choose the authorization profile created in Step 11 of Procedure 10, "Create wired authorization profiles."

🏠 Home	Operations 🔻 Policy 🔻 Ad	ministration					😶 Task I	Navigator + 🕗
🔔 Auther	ntication 💽 Authorization [	🔨 Profiling	💽 Posture 🛛 🗔 Client	: Provisioning	🚊 Security Grou	up Access 🥼 🦺 Policy Elements		
	on Policy thorization Policy by configuring rules	based on ide	entity groups and/or other con	ditions. Drag and c	frop rules to chan		۹ ا	
Exceptions Standard	s (D)					Cisco_IP_Phones Cisco_IP_Phones DenyAccess Deny BlackBerry	-	
Status	s Rule Name Wireless Black List Default	16	Conditions (identity groups an Blacklist AND Wireless 802.1		.)	Deny_iPhones     PermitAccess		Table 1
	Profiled Osco IP Phones		Cisco-IP-Phone	^		User+Machine-Cert	BSS	Edit   •
<b>_</b>	Profiled Cisco APs	if	Cisco-Access-Point			Wired-MAB		Edit   🕶
	Deny BlackBerry	if	BlackBerry			Wired_Dot1X		Edit   🕶
# 🗹 🕶	Wired Provisioning Wired BYOD	if	Micros I and Wir	ed_MAB AD1:Exter	malGroups EQ	Wireless-Provisioning     Wireless_Dot1X	<sup>©</sup>	Done Edit   •
	BYOD IT	if	(Apple-iPad OR Android OF OS_X-Workstation) AND AD cisco.local/Users/IT	Select an it	tem 🤇	2 -+		Edit   🕶
	BYOD HR	if	(Apple-iPad OR Android OF OS_X-Workstation) AND AD cisco.local/Users/HR	R / D1				Edit   🕶

# Step 25: Click Done, and then click Save.

		lministration		g 🔄 Security Group Access 🦳	Policy Elements	👓 Task Navigator 👻
horizati	on Policy					
	thorization Policy by configuring rules b	based on ide	ntity groups and/or other conditions. Drag	and drop rules to change the order.		
xceptions	(0)					
tandard						
Status	Rule Name		Conditions (identity groups and other cond	itions)	Permissions	
<b>V</b>	Wireless Black List Default	if	Blacklist AND Wireless_802.1X	then	Blackhole_Wireless_Access	Edit   👻
	Profiled Cisco IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phones	Edit   👻
<b>~</b>	Profiled Cisco APs	if	Cisco-Access-Point	then	Cisco_APs	Edit   🕶
<b>~</b>	Deny BlackBerry	if	BlackBerry	then	Deny_BlackBerry	Edit   🕶
<b>~</b>	Wired Provisioning	if	(Microsoft-Workstation OR OS_X-Work AND AD1:ExternalGroups EQUALS cisco.lo )	kstation) AND (Wired_MAB then cal/Users/BYOD Provisioning	Wired-Provisioning	Edit   🕶
<b>~</b>	Wired BYOD	if	Wired_MAB	then	Wired-BYOD	Edit   👻
<b>~</b>	BYOD IT		(Apple-iPad OR Android OR Microsoft- OS_X-Workstation) AND AD1:ExternalGr cisco.local/Users/IT	Workstation OR then then the	BYOD-IT	Edit   🕶
	BYOD HR		(Apple-iPad DR Android DR Microsoft- OS_X-Workstation) AND AD1:ExternalGr cisco.local/Users/HR	Workstation OR then oups EQUALS	BYOD-HR	Edit   🗸
2	BYOD Finance		(Apple-iPad DR Android DR Microsoft- DS_X-Workstation) AND AD1:ExternalGr clsco.local/Users/Finance	Workstation DR then oups EQUALS	BYOD-Finance	Edit   🕶
<b>×</b>	BYOD Research		(Apple-iPad OR Android OR Microsoft- OS_X-Workstation) AND AD1:ExternalGr cisco.local/Users/Research	Workstation OR then oups EQUALS	BYOD-Research	Edit   🕶
<b></b>	Default	if n	o matches, then PermitAccess			Edit   •

# Procedure 12

#### **Create wireless authorization profile**

Next, you create an authorization profile to configure the WLC to redirect the client to the Cisco ISE provisioning page when the client authenticates to the wireless network without a certificate.

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

Step 2: In the Results pane, double-click Authorization, and then click Authorization Profiles.

Step 3: Click Add.

Step 4: Enter a name and description for the profile.

Step 5: Select Web Authentication, and then, in the list, choose Supplicant Provisioning.

**Step 6:** Enter the name of the ACL that will be applied to the WLC. You will configure this ACL on the WLC later in this guide.

**Step 7:** Select **Airespace ACL Name**, and then enter the name of the ACL that will be applied to the WLC. This is the same ACL used in Step 6.

#### Step 8: Click Submit.

🏠 Home Operations 🔻 Policy 🔻 Admi	istration 🔻	Navigator 👻 😢
🛃 Authentication 🛛 👩 Authorization 🔣	Profiling 💿 Posture 🕞 Client Provisioning 🚊 Security Group Access 🦂 🦺 Policy Elements	
Dictionaries Conditions Results		
Results  P  Authonization  Authonization  Authonization  Authonization  Authonization  Authonization  Authonization  Authonization  Posture  Authonization  Client Providening  Security Group Access	Authorization Profile  Authorization Profile  * Name Wireless-Provisioning Description Wireless Profile For Self-Provisioning  * Access Access Access Accept  Common Tasks  Access Type * Access Accept  Access Type * Acce	

# Procedure 13

Configure wireless provisioning auth. rule

Next, you configure authorization rules to apply the authorization profile created in the previous step to provision devices not using certificates on the wireless network.

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

**Step 2:** At the end of the first BYOD rule, click the black triangle, and then select **Insert New Rule Above**. A new rule, Standard Rule 1, is created above the BYOD rules that were created earlier.

# Step 3: Rename Standard Rule 1 to Wireless Provisioning.

**Step 4:** In the Conditions column, next to Any, click the **+** symbol.

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

Step 6: Choose Apple-iPad.

Step 7: Next to Apple-iPad, click the + symbol.

Step 8: In the list, next to Endpoint Identity Groups, choose the > symbol.

- Step 9: Next to Profiled, click the > symbol, and then choose Android.
- Step 10: Next to Android, click the + symbol.

Step 11: In the list, next to Endpoint Identity Groups, choose the > symbol.

**Step 12:** Next to Profiled, click the > symbol, and then choose **Microsoft-Workstation**.

Step 13: Next to Microsoft-Workstation, click the + symbol.

Step 14: In the list, next to Endpoint Identity Groups, choose the > symbol.

# Step 15: Next to Profiled, click the > symbol, and then choose OS\_X-Workstation.

💄 Authenti	cation 🛛 👩 Authorization 🔀				
		Profiling	💽 Posture 🕞 Client Provisioning 📄 Security Group Ar	ccess 🕜 🐥 Policy Elements	
uthorizatio	Dolicu				
		xed on ide	ntity groups and/or other conditions. Drag and drop rules to change t	the order	
st Matched R					
Exceptions (	0)				
Standard					
Status	Rule Name		Conditions (identity groups and other conditions)	Permissions	
<b>~</b>	Wireless Black List Default	if	Blacklist AND Wireless_802.1X	then Blackhole_Wireless_Access	Edit   🕶
<b>~</b>	Profiled Gsco IP Phones	if	Cisco-IP-Phone	then Cisco_IP_Phones	Edit   👻
<b>~</b>	Profiled Cisco APs	if	Cisco-Access-Point	then Cisco_APs	Edit   👻
<b>~</b>	Deny BlackBerry	if	BlackBerry	then Deny_BlackBerry	Edit   👻
	Wired Provisioning	if	(Microsoft-Workstation OR DS_X-Workstation) AND (Wired_MA AND AD1:ExternalGroups EQUALS cisco.local/Users/BYOD Provisionin)	VB then Wired-Provisioning g	Edit   🕶
	Wired BYOD	if	Wired_MAB	then Wired-BYOD	Edit   👻
# 🛃 👻	Wireless Provisioning	if	Apple and Condition(s)	수 then AuthZ Profil 수	5 Done
	BYOD IT	if	Apple-Pad 💿 or 🕳	en BYOD-IT	Edit   🕶
	BYOD HR	if	Apple-Pad O ar and Android O ar and Android	en BYOD-HR	Edit   🕶
	BYOD Finance	if	Microsoft-Workstation 📀 ar 😑	en BYOD-Finance	Edit   🕶
			OS X-Workstation		

Step 16: In the Condition(s) list, click the + symbol, and then click Select Existing Condition from Library.
**Step 17:** In the list, next to Compound Conditions, click the > symbol, and then choose **Wireless\_802.1X**.

	Authenti			•			👓 Task Navigator 👻 🕙
uth		ication 🧕 Authorization 🔀	Profiling	Posture 🔂 Client Provisioning	g 🔄 Security Group Access 🦳 🐥	Policy Elements	
	orizatio	n Dolicy					
			ased on id	entity groups and/or other conditions. Drag	and drop rules to change the order.		
irst I	Aatched R	tule Applies v					
Ex	ceptions (						
Sta	andard				Compound Conditions		
	Status	Rule Name		Conditions (identity groups and other con	٩	Permissions	
		Wireless Black List Default	if	Blacklist AND Wireless_802.1X	🔶 🗐 📜 👘	Blackhole_Wireless_Access	Edit   👻
		Profiled Cisco IP Phones	if	Cisco-IP-Phone	U Wired_802.1X	Cisco IP Phones	Edit   👻
	_				Wired_MAB		Eurc   •
	<b>~</b>	Profiled Cisco APs	if	Cisco-Access-Point	Wreless_MAB	Cisco_APs	Edit   👻
	~	Deny BlackBerry	if	BlackBerry	Catalyst_Switch_Local_Web_Authentica	Deny_BlackBerry	Edit   👻
		Wired Provisioning	if	(Microsoft-Workstation OR OS_X-Wo	WLC_Web_Authentication	Wired-Provisioning	Edit   👻
	_			AND AD1:ExternalGroups EQUALS cisco.	EAP-Chaining-User-and-Machine-Cert	-	
	<b>~</b>	Wired BYOD	if	Wired_MAB		Wired-BYOD	Edit   👻
	<b>-</b>	Wireless Provisioning	if	Apple I and Condition(s)		en AuthZ Profil 💠	Done
1		BYOD IT					
	<u>~</u>	BIODII		OS_X-Workst	2		
		BYOD HR		Condition Name			ŵ.,
	_			OS X-Workst Select Condition	2		499 <del>v</del>

**Step 18:** At the end of the rule, click the gear icon, and then select **Add Attribute/Value**.

Step 19: Next to Select Attribute, click the arrow. The menu opens.

**Step 20:** Next to Network Access, click the > symbol, and then choose **EapTunnel**.

**Step 21:** Under Expression, in the first list, choose **Equals**, and then, in the second list, choose **PEAP**.

**Step 22:** At the end of this rule, click the gear icon, and then select **Add Attribute/Value**.

Step 23: Next to Select Attribute, click the arrow. The menu opens.

Step 24: Next to AD1, click the > symbol, and then choose ExternalGroups.

**Step 25:** Under Expression, in the first list, choose **Equals**, and then, in the second list, choose the BYOD group created in Procedure 2.

	Operations 🔻 Policy 🔻 Admi	inistration 🔻		🕫 Task Navigator 👻 😢
💄 Authen	tication 🧕 Authorization 🔀	Profiling 👰 Posture 🕞 Client Provisioning 🔄 Security Group Access	s Policy Elements	
uthorizatio	on Policy			
		ased on identity groups and/or other conditions. Drag and drop rules to change the c	order.	
First Matched	Rule Applies 🔹			
	(D)			
Exceptions				
Standard				
Status	Rule Name	Conditions (identity groups and other conditions)	Permissions	
	Wireless Black List Default	if Blacklist AND Wireless_802.1X	then Blackhole_Wireless_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   👻
	Deny BlackBerry	if BlackBerry	then Deny_BlackBerry	Edit   🕶
	Wired Provisioning	If (Microsoft-Workstation OR DS_X-Workstation) AND (Wired_MAB AND AD1:ExternalGroups EQUALS disco.local/Users/BYOD Provisioning )	then Wired-Provisioning	Edit   🕶
	Wired BYOD	if Wired_MAB	then Wired-BYOD	Edit   👻
/ 🔽 🗸	Wireless Provisioning	if Apple 🔶 and Select Condition 🗢	then AuthZ Profil 🔶	Done
	Condition Name Expression	n AND  vice-Type EQUALS Framed AND Radius:NAS-Port	then BYOD-IT	Edit   👻
	neless_ouz.ix 🕥 noulus.del			

**Step 26:** Next to AuthZ Profile(s), click the **+** symbol, and then, next to Select an item, click the arrow.

**Step 27:** Next to Standard, click the > symbol, and then choose the authorization profile created in Procedure 12, "Create wireless authorization profile."

		Operations V Policy V Admin	nistration					Task Navigator 🕫 🕗
	A							ask tvangator -
	Authenti	cation 🧕 Authorization 🔀	Profiling	Posture 🕞 Client Provisio	oning 🚊 Security Group	p Access 💦 🐥 Policy Elements		
utba	orizatio	Dolicy						
			cod on id	entity groups and/or other conditions. I	Drag and drop rules to chang	the order		
			564 0114	shory groups and/or other contations.	prag and drop rules to chang	go the order.		
irst M	latched R	ule Applies 🔹						
Exc	eptions (					Standard		
							2	
Sta	ndard							
	Status	Rule Name		Conditions (identity groups and other	conditions)	The show the	*	
	<b></b>	Wireless Black List Default	if	Blacklist AND Wireless_802.1X		Gisco_IP_Phones	E BSS	Edit   👻
	~	Profiled Cisco IP Phones	16	Cisco-IP-Phone		San DenyAccess		
	<u>~</u>	Profiled Usco IP Phones	11	CISCO-1P-Phone		😪 Deny_BlackBerry		Edit   👻
	<b>~</b>	Profiled Cisco APs	if	Cisco-Access-Point		G Deny_Phones		Edit   👻
	<b>~</b>	Deny BlackBerry	if	BlackBerry		PermitAccess		Edit   👻
1	_					G User+Machine-Cert		Educ 1 -
	<b>~</b>	Wired Provisioning	if	(Microsoft-Workstation DR OS_X- AND AD1:ExternalGroups EQUALS ds	<ul> <li>Workstation) AND (Wred co.local/Users/BYOD Provisi</li> </ul>	Wired-MAB		Edit   👻
				)		Wired-Provisioning		
	×	Wired BYOD	if	Wired_MAB		Wired_Dot1X		Edit   👻
I 🖉	<b>-</b>	Wireless Provisioning		Apple 🔶 and Wireless_8	02.1X Network Access:Ea	Wireless-Provisioning		Done
	_					Wireless_Dot1X	-	
1	<u>~</u>	BYOD IT	if	(Apple-iPad OR Android OR 1 OS_X-Workstation) AND AD1	Ŀ			Edit   👻
				cisco.local/Users/IT	Select an item 🛛 🔇	-+		
		BYOD HR	if	(Apple-iPad OR Android OR 1				Edit   🔻

#### Step 28: Click Done, and then click Save.

cis 🏠			iministration	🖉 Posture 🕞 Client Provisioning	Security Group Access	Policy Elements	ise-1 admin Logout Fer
uth	orizatior the Auth	Policy		entity groups and/or other conditions. Drag a			
Exc	ceptions (i	)					
Sta	andard						
	Status	Rule Name Wireless Black List Default	if	Conditions (identity groups and other condit Blacklist AND Wireless_802.1X		Permissions Blackhole_Wireless_Access	Edit   •
	~	Profiled Cisco IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phones	Edit   •
	<b>~</b>	Profiled Cisco APs	if	Cisco-Access-Point	then	Cisco_APs	Edit
		Deny BlackBerry	if	BlackBerry	then	Deny_BlackBerry	Edit
	~	Wired Provisioning	if	(Microsoft-Workstation OR OS_X-Work AND AD1:ExternalGroups EQUALS clsco.loc	station) AND (Wired_MAB then al/Users/BYOD Provisioning	Wired-Provisioning	Edit   •
		Wired BYOD	if	Wired_MAB	then	Wired-BYOD	Edit
	<b>~</b>	Wireless Provisioning	lf	(Apple-iPad OR Android OR Microsoft-V OS_X-Workstation) AND (Wireless_802.1) Access:EapTunnel EQUALS PEAP AND AD1: cisco.local/Users/BYOD Provisioning )	X AND Network	Wireless-Provisioning	Edit   •
		BYOD IT	if	(Apple-iPad OR Android OR Microsoft-V OS_X-Workstation) AND AD1:ExternalGro cisco.local/Users/IT	Workstation OR then ups EQUALS	BYOD-IT	Edit   •
		BYOD HR	if	(Apple-iPad OR Android OR Microsoft-V OS_X-Workstation) AND AD1:ExternalGro cisco.local/Users/HR	Workstation OR then ups EQUALS	BYOD-HR	Edit   •
		BYOD Finance	if	(Apple-iPad DR Android DR Microsoft-V DS_X-Workstation) AND AD1:ExternalGro cisco.local/Users/Finance		BYOD-Finance	Edit   •
		BYOD Research	if	(Apple-iPad OR Android OR Microsoft-W OS_X-Workstation) AND AD1:ExternalGro cisco.local/Users/Research		BYOD-Research	Edit
	<b>~</b>	Default	if	no matches, then PermitAccess			Edit I

Procedure 14

#### **Create Android authorization profile**

For provisioning, an Android device must download a supplicant provisioning wizard from the Google Play store. Because of this, you need to add an authorization profile and an authorization rule for when the device is in the state where it has started the self-provisioning process but hasn't downloaded the wizard yet.

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

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

Step 3: Click Add.

Step 4: Enter a name and description for the profile.

## Step 5: Select Web Authentication, and then, in the list, choose Supplicant Provisioning.

**Step 6:** Enter the name of the ACL that will be applied to the WLC. You will configure this ACL on the WLC later in this guide.

**Step 7:** Select **Airespace ACL Name**, and then enter the name of the ACL that will be applied to the WLC. This is the same ACL used in Step 6.

#### Step 8: Click Submit.



**Procedure 15** 

**Create Android provisioning rule** 

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

**Step 2:** At the end of the wireless provisioning rule, click the black triangle, and then select **Insert New Rule Above**. This creates a new rule, Standard Rule 1, above the wireless provisioning rule created in Procedure 13, "Configure wireless provisioning auth. rule."

Step 3: Rename Standard Rule 1 to Android Provisioning.

Step 4: In the Conditions column, next to Any, click the + symbol.

**Step 5:** In the list, next to Endpoint Identity Groups, click the > symbol, and then select **RegisteredDevices**.

Step 6: In the Condition(s) list, click the + symbol, and then click Create New Condition (Advance Option).

Step 7: Next to Select Attribute, click the arrow. The menu opens.

Step 8: Next to Session, click the > symbol, and then choose Device-OS.

**Step 9:** Under Expression, in the first list, choose **Equals**, and then, in the second list, choose **Android**.

**Step 10:** Next to AuthZ Profile(s), click the **+** symbol, and then, next to Select an item, click the arrow.

**Step 11:** Next to Standard, click the > symbol, and then choose the authorization profile created in Procedure 14, "Create Android authorization profile."

Step 12: Click Done, and then click Save.

Procedure 16 Create wired 802.1X authorization rule

You need to create an authorization profile to grant devices full network access, which authenticates using certificates on the wired network.

**Step 1:** At the end of the default rule, click the black triangle, and then select **Insert New Rule Above**. A new rule, Standard Rule 1, is created.

Step 2: Rename Standard Rule 1 to Wired Dot1X.

**Step 3:** In the Conditions column, next to Condition(s), click the + symbol, and then click **Select Existing Condition from Library**.

**Step 4:** In the list, next to Compound Conditions, click the > symbol, and then choose **Wired\_802.1X**.

**Step 5:** Next to AuthZ Profile(s), click the + symbol, and then, next to Select an item, click the arrow.

Step 6: Next to Standard, click the > symbol, and then choose PermitAccess.

Step 7: Click Done, and then click Save.

## Procedure 17 Create wireless 802.1X authorization rule

You need to create an authorization profile to grant devices full network access, which authenticates using certificates.

**Step 1:** At the end of the default rule, click the black triangle, and then select **Insert New Rule Above**. A new rule, Standard Rule 1, is created.

Step 2: Rename Standard Rule 1 to Wireless Dot1X.

**Step 3:** In the Conditions column, next to Condition(s), click the + symbol, and then click **Select Existing Condition from Library**.

**Step 4:** In the list, next to Compound Conditions, click the > symbol, and then choose **Wireless\_802.1X**.

**Step 5:** Next to AuthZ Profile(s), click the + symbol, and then, next to Select an item, click the arrow.

**Step 6:** Next to Standard, click the > symbol, and then choose **PermitAccess**.

Step 7: Click Done, and then click Save.

Procedure 18 Modify default rule

The last step is to modify the default rule to deny network access to any device that has not matched an existing authorization rule.

Step 1: At the end of the default rule, click Edit.

Step 2: Next to PermitAccess, click the + symbol.

**Step 3:** Next to PermitAccess, click the arrow, next to Standard, click the > symbol, and then choose **DenyAccess**.

Step 4: Click Done, and then click Save.

#### Procedure 19 Configure WLCs

Next, you need to configure the WLCs to support device provisioning by defining ACLs that are applied to the controller, and to enable a posture state to be maintained to determine if a device has been provisioned. Perform this procedure for every WLC in the architecture, including controllers deployed at remote sites, with the exception of the guest WLC in the DMZ.

Step 1: In your browser, enter https://wlc1.cisco.local. The WLC console opens.

**Step 2:** Navigate to **WLANs**, and then select the WLAN ID for the SSIDs you wish to support device provisioning.

Step 3: Click Advanced, and then, in the NAC section, in the list, choose Radius NAC.



Step 4: Click Apply, and then, on the dialog box that appears, click OK.

Step 5: Navigate to Security, and in the pane on the left, expand Access Control Lists, and then click Access Control Lists.

#### Step 6: Click New.

**Step 7:** Name the access list the same name that was used in Procedure 12. "Create wireless authorization profile," and then click Apply.

Step 8: Click the name in the list. This allows you to edit the newly created access list.

#### Step 9: Click Add New Rule.

Step 10: Create a new access list rule based on your security policy, and then click Apply. In this example deployment, devices that need provisioning only require access to the primary and secondary Cisco ISE nodes, as well as the AD server that is providing DNS service. All other traffic is denied.

սիսիս								Sa <u>v</u> e Co	onfiguration	Ping   Logout   Re	efresh
cisco	<u>M</u> ONI	for <u>w</u>	LANS <u>C</u> ONTROLL	ER W <u>I</u> RELESS	<u>s</u> ecurity	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP <u>F</u>	EEDBACK		
Security	Acce	ss Con	trol Lists > Edit					1	< Back	Add New Rule	ð
▼ AAA General ▼ RADIUS	Gene										
Authentication Accounting Fallback TACACS+		: List Nam Counters	e Provisioni O	-							
LDAP Local Net Users	Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
MAC Filtering Disabled Clients User Login Policies AP Policies	1	Permit	0.0.0.0 / 0.0.0.0	10.4.48.41 / 255.255.255.255	Any	Any	Any	Any	Any	0	
Password Policies	2	Permit	10.4.48.41 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0	
<ul> <li>Priority Order</li> <li>Certificate</li> </ul>	3	Permit	0.0.0.0 / 0.0.0.0	10.4.48.42 / 255.255.255.255	Any	Any	Any	Any	Any	0	
<ul> <li>Access Control Lists Access Control Lists CPU Access Control Lists         </li> </ul>	4	Permit	10.4.48.42 / 255.255.255.255	0.0.0.0	Any	Any	Any	Any	Any	0	
FlexConnect ACLs	5	Permit	0.0.0.0 / 0.0.0.0	10.4.48.10 / 255.255.255.255	Any	Any	Any	Any	Any	0	
<ul> <li>Policies</li> <li>Web Auth</li> </ul>	<u>6</u>	Permit	10.4.48.10 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0	
FrustSec SXP Advanced	_7_	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0	



The access list needs to have entries for the traffic in both directions so make sure you have pairs of access list rules for both inbound and outbound traffic. Also, there is an implicit "deny all" rule at the end of the access list, so any traffic not explicitly permitted is denied.

Next, you need to create an ACL for Android provisioning.

#### Step 11: In the left pane, expand Access Control Lists, and then click Access Control Lists.

#### Step 12: Click New.

Step 13: Name the access list the same name that was used in Procedure 14, "Create Android authorization profile," and then click Apply.

Step 14: Click the name in the list. This allows you to edit the newly created access list.

#### Step 15: Click Add New Rule.

Android provisioning requires that you permit access to the Google Play store in addition to the primary and secondary ISE nodes and DNS server.



## **Tech Tip**

The actual addresses used for the Google Play store may change depending on your location due to the DNS and content distribution services used by Google. The address blocks 74.125.0.0/16 and 173.194.0.0/16 are owned by Google and the Play store has resolved to addresses in both. You should verify the correct address range to use for your environment.

#### Step 16: Create this new access list, and then click Apply.

սիսիս									Sa⊻e	Configuration   E	jing   Logout   <u>R</u> efresh
cisco	<u>M</u> ONI	TOR W	LANS <u>C</u> ONTROLL	.ER W <u>I</u> RELESS	SECURITY	MANAGEMENT	COMMANDS I	не <u>ц</u> р <u>е</u> ев	DBACK		
Security	Acce	ss Con	trol Lists > Edit							< Back	Add New Rule
✓ AAA General ✓ RADIUS Authentication Accounting Follback ▼ TACACS+		r <b>al</b> s List Nam Counters	e Android O								
LDAP Local Net Users	Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hit	s
MAC Filtering Disabled Clients User Login Policies	1	Permit	0.0.0.0	/ 10.4.48.41 255.255.255.255	/ Any	Any	Any	Any	Any	0	
AP Policies Password Policies	2	Permit	10.4.48.41 255.255.255.255	/ 0.0.0.0 / 0.0.0.0	/ Any	Any	Any	Any	Any	0	
▶ Local EAP	3	Permit	0.0.0.0	/ 10.4.48.42 255.255.255.255	/ Any	Any	Any	Any	Any	0	
<ul> <li>Priority Order</li> <li>Certificate</li> </ul>	4	Permit	10.4.48.42 255.255.255.255	/ 0.0.0.0 0.0.0.0	/ Any	Any	Any	Any	Any	0	
Access Control Lists     Access Control Lists	5	Permit	0.0.0.0	/ 10.4.48.10 255.255.255.255	/ Any	Any	Any	Any	Any	0	
CPU Access Control Lists FlexConnect ACLs	6	Permit	10.4.48.10 255.255.255.255	/ 0.0.0.0 0.0.0.0	/ Any	Any	Any	Any	Any	0	
Wireless Protection     Policies	7	Permit	0.0.0.0	/ 74.125.0.0 255.255.0.0	/ Any	Any	Any	Any	Any	0	
Web Auth	8	Permit	74.125.0.0 255.255.0.0	/ 0.0.0.0 0.0.0.0	/ Any	Any	Any	Any	Any	0	
TrustSec SXP Advanced	9	Permit	0.0.0.0	/ 173.194.0.0 255.255.0.0	/ Any	Any	Any	Any	Any	0	
,	<u>10</u>	Permit	173.194.0.0 255.255.0.0	/ 0.0.0.0 0.0.0.0	/ Any	Any	Any	Any	Any	0	
	<u>11.</u>	Deny	0.0.0.0 0.0.0.0	/ 0.0.0.0 0.0.0.0	Any	Any	Any	Any	Any	0	

#### Procedure 20

#### Enable captive portal bypass

When connecting to a wireless network with an Apple iOS device, the device sends a web request in order to initiate the process for logging into a wireless guest portal, such as at a hotel or public Wi-Fi hotspot. However, this can cause an issue when trying to use the redirect to the Cisco ISE provisioning portal from the WLC. To correct this, you configure the WLC to bypass the captive portal from the CLI of the WLC.

**Step 1:** Connect to the console of the WLC either directly using a console cable and terminal emulator or using SSH to the management IP address.

#### Step 2: Once connected, enter the command:

config network web-auth captive-bypass enable

**Step 3:** Reset the controller by using the **reset system** command for the new configuration to take effect.

**Step 4:** Repeat this procedure for every WLC in the architecture that will be used for BYOD.

#### Procedure 21

**Create authorization rules for user groups** 

Previously, you created authorization rules that limited which parts of the network an employee with a personal device could access, based on their AD group. The current policy permits full network access to any device that was provisioned.

Next, you create access rules for provisioned devices, which are similar to the rules created earlier for personal devices that haven't been provisioned. The provisioned devices use EAP-TLS and are registered, and you use that to create the policy. The ACLs have already been created on the WLCs, and you already have authorization profiles.

The policy in this procedure pushes an access list to the WLC for users in the IT group who are using a provisioned device. The access list can only be deployed for access points in the campus or at remote sites that have a local WLC. This policy is an example and can be modified to suit your environment.

Step 1: In your browser, enter https://ise-1.cisco.local.

Step 2: On the menu bar, mouse over Policy, and then choose Authorization.

**Step 3:** At the end of the first BYOD rule, click the black triangle, and then select **Insert New Rule Above**. This creates a new rule, Standard Rule 1, and puts it above the BYOD rules created earlier.

Step 4: Rename Standard Rule 1 to BYOD IT Provisioned.

Step 5: In the Conditions column, next to Any, click the + symbol.

**Step 6:** In the list, next to Endpoint Identity Groups, click the > symbol, and then select **RegisteredDevices**.

Step 7: In the Condition(s) list, click the + symbol, and then click Create New Condition (Advance Option).

Step 8: Next to Select Attribute, click the arrow. The menu opens.

**Step 9:** Next to Network Access, click the > symbol, and then choose **EapAuthentication**.

**Step 10:** Under Expression, in the first list, choose **Equals**, and then, in the second list, choose **EAP-TLS**.

Step 11: At the end of this rule, click the gear icon, and then select Add Attribute/Value.

Step 12: Next to Select Attribute, click the arrow. This opens the menu.

Step 13: Next to AD1, click the > symbol, and then choose ExternalGroups.

**Step 14:** Under Expression, in the first list, choose **Equals**, and then, in the second list, choose the IT group.

		tication 🧕 Authorization	🛃 Profiling	💽 Posture	🛃 Clent Provisioning	🚊 Security Group Access	Policy Elements	
h	orizatio	on Policy						
		horization Policy by configuring n	ules based on ic	entity groups and/o	ar other conditions. Drag ar	id drop rules to change the orr	der.	
: IV	latched	Rule Applies 🔹 🔻						
	eptions	(D)						
ita	ndard							
	Status	Rule Name		Conditions (identif	ty groups and other conditi	ons)	Permissions	
	<b>~</b>	Wireless Black List Default	if	Blacklist AND Wi	reless_802.1X		then Blackhole_Wireless_Access	Edit   🖛
	<b>~</b>	Profiled Cisco IP Phones	if	Cisco-IP-Phone			then Cisco_IP_Phones	Edit   🕶
	<u>~</u>	Profiled Cisco APs	if	Cisco-Access-Po	int		then Cisco_APs	Edit   🕶
	<ul> <li>Image: A second s</li></ul>	Deny BlackBerry	if	BlackBerry			then Deny_BlackBerry	Edit   🕶
		Wired Provisioning	if	(Microsoft-Work AND AD1:Extern	station OR OS_X-Works alGroups EQUALS cisco.loca	tation) AND (Wired_MAB I/Users/BYOD Provisioning	then Wired-Provisioning	Edit   👻
	<b>~</b>	Wired BYOD	if	Wired_MAB			then Wired-BYOD	Edit   🕶
		Android Provisioning	if	RegisteredDevic	es AND Session:Device-OS	EQUALS Android	then Android-Provisioning	Edit   🕶
	2	Wireless Provisioning	if	OS_X-Workstati Access:EapTunne	Android OR Microsoft-W ion) AND (Wireless_802.1) I EQUALS PEAP AND AD1:8 IYOD Provisioning )	AND Network	then Wireless-Provisioning	Edit   🕶
P	- 🗹	BYOD IT Provisioned	lf	Regist 🔶	and Condition(s)	-	then 🛛 AuthZ Profil 🔶	Done
		BYOD IT	if	(Apple-iPac OS_X-Work cisco.local/U:	Add All Conditions Below			
				coco.ocajo.	Condition Name	Expression		AND -

**Step 15:** Next to AuthZ Profile(s), click the + symbol, and then, next to Select an item, click the arrow.

**Step 16:** Next to Standard, click the > symbol, and then choose the authorization profile BYOD-IT.

Step 17: Click Done, and then click Save.

**Step 18:** For each group that you want to define a policy, repeat this procedure. In the example deployment described here, you need to create policies for the Finance, HR, and Research groups.

#### Procedure 22

Delete 802.1X rules

Now that you have created specific authorization rules, you need to delete the generic, catch-all rules that allowed any provisioned device full network access.

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

**Step 2:** At the end of the Wired Dot1X rule, click the black triangle, and then select **Delete**.

Step 3: Verify that you want to delete the rule by clicking Delete.

**Step 4:** At the end of the Wireless Dot1X rule, click the black triangle, and then select **Delete**.

**Step 5:** Verify that you want to delete the rule by clicking **Delete**, and then click **Save**.

Procedure 23

Provision a Windows workstation

The infrastructure has been configured to support self-provisioning for personally owned Microsoft Windows workstations using wired or wireless connections.

**Step 1:** From a Windows workstation, connect to the network by connecting an Ethernet cable for a wired connection. For wireless, open the Network control panel and choose the wireless network name. Use your username and password to connect to the wireless network.

Step 2: Once connected, open a web browser and browse to any site.

**Step 3:** The browser gets redirected to the Guest Portal. Enter your username and password, and then click **Login**.



**Step 4:** The browser will then connect to the Self-Provisioning Portal. Enter a description of the device, and then click **Register**.



The provisioning process begins.

**Step 5:** If a window displays asking if you want to run the application CiscoSPWDownloadFacilitator, click **Run**. This launches the Network Setup Assistant.

Security Inform	nation X
	ation's digital signature has been verified.
Name:	CiscoSPWDownloadFacilitator
Publisher:	Cisco Systems
From:	https://ise-1.cisco.local:8443
🔽 Always tr	rust content from this publisher.
	Run Cancel
your	application will run with unrestricted access which may put personal information at risk. The publisher's identity has been More Information ed. Run this application only if you trust the publisher.

#### Step 6: Click Start.



**Step 7:** As the Network Setup Assistant runs, you will be prompted to verify you want to install the root certificate. Click **Yes**.

Step 8: When the process completes, click Exit.

The workstation reauthenticates to the network and then prompts you that additional information is required to login.

**Step 9:** Click the message. This opens a window where you can select a certificate.

**Step 10:** Verify the certificate is the one that was just issued by the Network Setup Assistant, and then click **OK**.

Select Certificate		×
User name on certificate:		
pat.jones	•	
Friendly name:		
Issuer:	CA	
Expiration date:	2/28/2014 6:10:22 PM	
Connection user name:		
pat.jones		
	OK Cancel View Certificate	

Procedure 24

Provision a Mac OS X workstation

The infrastructure has been configured to support self-provisioning for personally owned Apple Mac OS X workstations using wired or wireless connections.

**Step 1:** From a Mac OS X workstation, connect to the network by connecting an Ethernet cable for a wired connection.

For wireless, open **System Preferences**, click **Network**, and then, in the **Network Name** list, choose your network. Use your username and password to connect to the wireless network.

Step 2: Once connected, open a web browser and browse to any site.

The browser gets redirected to the Guest Portal.

Step 3: Enter your username and password, and then click Login.

Step 4:



The browser will then connect to the Self-Provisioning Portal.

Step 5: Enter a description of the device, and then click Register.



The provisioning process begins.

**Step 6:** If a window displays asking if you want to run the application CiscoSPWDownloadFacilitator, click **Run**.



**Step 7:** On the warning that the file was downloaded from the Internet, click **Open**. This launches the Network Setup Assistant.

#### Step 8: Click Start.



As the Network Setup Assistant runs, you will be prompted to verify you want to modify the system.

**Step 9:** Enter your username and password, and then click **Modify Configuration**.

Step 10: When the process completes, click Exit.

The workstation connects using the new profile if it is configured for automatic 802.1X connections. **Step 11:** If the workstation is not configured for automatic 802.1X connections, open **System Preferences**, and then click **Network**. The profile is listed in the 802.1X section. Click **Connect**.

00		Network		
▲ ► Show All				Q.
	Location:	Automatic	;	
Connected	in the second se	Status:	Connected Ethernet is currently acti address 10.4.2.15.	ive and has the IP
e Wi-Fi	<u></u>	Configure IPv4:	Using DHCP	*
USB-Sentroller	6 star	IP Address:	10.4.2.15	
- FireWire		Subnet Mask:	255.255.255.0	
Not Connected	<b>2</b>	Router:	10.4.2.1	
Bluetooth PAN	8	DNS Server:	10.4.48.10	
		Search Domains:	cisco.local	
		802.1X:	EAP-TLS Profile	Connect
+ - &*				Advanced ?
Click the lock to p	revent further	changes.	Assist me	Revert Apply

#### Procedure 25

Provision an Apple iPad

The infrastructure has been configured to support self-provisioning for personally owned Apple iPads.

**Step 1:** From an iPad, connect to the wireless network by opening **Settings**, and then choosing the network from the list. Connect using your username and password.

Step 2: Once connected, open Safari and browse to any site.



Safari gets redirected to the Self-Provisioning Portal and then a window launches to start provisioning.



Step 3: Click Install. The trusted root certificate from the CA installs.

Step 4: On the warning message that appears, click Install.

Step 5: Click Done. The Self Provisioning Portal displays in Safari.

Step 6: Enter a description of the device, and then click Register.

CISCO Self-Provisioning Portal	pat.jones@cisco.local
Device Registration	
This device has not been registered.	
Please click the 'Register' button to configure your device to use the secure network.	
Device ID 40:30:04:24:EE:A9	
Description Pat Jones's Apple iPad	
Register	



Cancel	Install Profile	
yyyyyy	Cisco Systems.	
	Verified	Install
Desc	ription Gather device information.	
\$	Signed ise-1.cisco.local	
Re	ceived Feb 28, 2013	
Co	ntains Device enrollment challenge	
More	Details	>

**Step 8:** On the warning message that appears, click **Install Now**. The profile installs.

**Step 9:** Click **Done**. You are automatically reconnected to the wireless network using the new profile.

#### Procedure 26 Provision an Android tablet

The infrastructure has been configured to support self-provisioning for personally owned Google Android tablets.

**Step 1:** On an Android tablet, connect to the wireless network by opening **Settings**, selecting **Wi-Fi**, and then choosing the network from the list.

Step 2: Open the browser and browse to any site.

**Step 3:** In the Self-Provisioning Portal, enter a description of the device, and then click **Register**.



**Step 4:** Choose **Play Store**. The Google Play Store opens, where you can download the Cisco Network Setup Assistant.

**Step 5:** In the Google Play Store, click **Download**, and then, on the verification window, click **Accept & download**. The Cisco Network Setup Assistant downloads.

	Cisco Network Setup Assistant cisco systems, inc.	Accept & download
smartbusinessarc	nitecture@gmail.com	
PERMISSIONS		
Storage Modify/delete SE	) card contents	>
System tools Change Wi-Fi sta	ate, change network connectivity, change your UI settings	>
Network commu Full Internet acce		>
		See all 🐱

Step 6: Run the setup assistant by clicking Open, and then clicking Start.



#### Step 7: Click OK. The user certificate installs.

Certificate name						
Certificate name: pat.jones						
Package contains: One user key One user certificate						
ОК	Cancel					

Step 8: Click OK. The trusted root certificate installs.

Certificate name	
Certificate name: iseca Package contains: One CA certificate	
ОК	Cancel

Step 9: The tablet connects to the network using the new profile.

Step 10: If you need to connect to the network with the new profile manually, open Settings, and then select Wi-Fi.

Step 11: Choose the network from the list, and then click Forget.

**Step 12:** Select the network from the list. This allows you to configure the options for connecting.

#### Step 13: For EAP method, select TLS.

**Step 14:** For CA certificate, select the certificate that was installed in Step 8.

**Step 15:** For User certificate, select the certificate that was installed in Step 7.

**Step 16:** Enter the username that matches the certificate for Identity, and then click **Connect**.

EAP method	TLS	_	
Phase 2 authentication	None		
CA certificate	iseca	_	
User certificate	pat.jones		
Identity	pat.jones		
Anonymous identity			
Password			
Show password			
Show advanced	options		
Сог	nnect		Cancel

#### Process

Enabling Security Group Access

- 1. Define Security Group Tags
- 2. Add ASA as network device
- 3. Modify authorization policy
- 4. Configure SXP on IOS devices
- 5. Configure SXP and SGT on the Nexus 1000v
- 6. Configure SXP on WLCs
- 7. Configure SXP on ASA
- 8. Configure firewall policy
- 9. Monitoring SGTs on Cisco ASA
- 10. Monitoring SGTs on the switches
- 11. Monitoring SGTs on the WLC

Security Group Access (SGA) technology allows user identity information to be associated with their network traffic and then passed throughout the network. This information can then be used to enforce an access policy by using Security Group Tags (SGT) and Security Group Access Control Lists (SGACL).

The SGT Exchange Protocol (SXP) is used to propagate the IP-to-SGT bindings across network devices that do not support SGTs. In this example, we are passing SGT information from the access layer devices to Cisco ASA in the data center.

SXP establishes a peering relationship between two devices in order to exchange the IP-to-SGT bindings. There are two roles in the relationship: the speaker and the listener. The speaker passes the IP-to-SGT bindings to the listener. In our example, the access layer switch needs to pass these bindings to Cisco ASA in the data center. You could have the switch peer directly with the ASA appliance, however, that may not scale well in larger environments. It is a best practice to minimize the number or peers a device has by aggregating connections. For example, campus access layer switches would peer with a distribution switch, which then would peer with the ASA appliance. Or, access layer switches at a remote site would peer with a distribution switch at the site, which would peer with the WAN aggregation router at the headquarters, which would then peer with the ASA appliance. For the virtualized desktops, the Cisco Nexus 1000v is the access layer switch, and it peers directly with the Cisco ASA appliance in the data center.



**Procedure 1** 

**Define Security Group Tags** 

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

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

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

Step 4: Click Add.

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

**Step 6:** Repeat Step 4 and Step 5 for each tag you wish to create. In this example deployment, you create tags for each of the following groups: Finance\_Users, HR\_Users, IT\_Users, Research\_Users, and Network\_Devices.

#### Procedure 2

#### Add ASA as network device

In order to allow Cisco ISE to provide SGT enforcement on Cisco ASA, the ASA appliance needs to be added as a network device in ISE.

**Step 1:** On the menu bar, mouse over **Administration**, and then in the Network Resources section, choose **Network Devices**.

#### Step 2: Click Add.

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

Step 4: For the IP address, enter 10.4.53.126.

Network Devices List >	New Network Device	
Network Devic	es	
* Name Description	ASA-5585X Data Center ASA	
* IP A	ddress: 10.4.53.126 / 32	<b>₩</b> *
Model Name Software Version	•           •	
* Netwo	rk Device Group	
Locat Device Ty		

#### Step 5: Select Authentication Settings.

#### Step 6: Enter the RADIUS shared secret.

<ul> <li>Authentication Settings</li> </ul>		
Enable Authentication Settings		
Protocol	RADIUS	
* Shared Secret	•••••	Show
Enable KeyWrap	i)	
* Key Encryption Key		Show
* Message Authenticator Code Key		Show
Key Input Format	ASCII	MAL
	Enable Authentication Settings Protocol * Shared Secret Enable KeyWrap * Key Encryption Key * Message Authenticator Code Key	Enable Authentication Settings Protocol RADIUS * Shared Secret Enable KeyWrap  * Key Encryption Key

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

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

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

✓	▼ Advanced TrustSec Settings		
	<ul> <li>Device Authentication Settings</li> </ul>		
	Use Device ID for SGA 🗹 Identification		
	Device Id		
	* Password	Show	
	<ul> <li>SGA Notifications and Updates</li> </ul>		
	* Download environment data every	1	Days 💌
	* Download peer authorization policy every	1	Days 💌
	* Reauthentication every	1	Days 💌 👔
	* Download SGACL lists every	1	Days 🔻
	Other SGA devices to trust this device		
	Notify this device about SGA configuration changes	_	

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

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

**Step 12:** You are prompted to save the file to your local machine. Choose a location, click **OK**, and then click **Submit**.

#### Procedure 3 Modify authorization policy

In Procedure 6, "Create authorization rules for user groups" of the previous section, you created authorization policies that limited network access based on Active Directory group membership by using access lists. In this procedure, you modify those policies to instead use SGTs.

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

Step 2: For the IT rule, click Edit.

Step 3: In the Permissions column, next to IT, click the + symbol.

Step 4: Click the + symbol. This adds a new permission.

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

Step 6: Select IT\_Users.

Step 7: Click Done, and then click Save.

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

#### Procedure 4 Configure SXP on IOS devices

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

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

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

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

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

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

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

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

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

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

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

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

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

**Step 13:** Repeat this procedure for each Cisco IOS device where you need to configure SXP.

Procedure 5

**Configure SXP and SGT on the Nexus 1000v** 

The Cisco Nexus 1000v is used to support the virtualized desktops in the data center. You configure SXP to peer with Cisco ASA in the data center in order to share IP-SGT bindings. Each group is configured to use a port-pro-file on the switch that assigns the VLAN and SGT for the virtualized desktop.

Step 1: Access the console of the Nexus 1000v by using an ssh client and connecting to 10.4.63.28.

Step 2: Enter configuration mode and enter the following commands.

cts sxp enable cts sxp default password <password> cts sxp default source-ip 10.4.63.28 cts sxp connection peer 10.4.53.126 password default mode listener vrf management port-profile type vethernet IT\_VDI\_users vmware port-group switchport mode access switchport access vlan 157 cts sgt 3 no shutdown state enabled

**Step 3:** This example shows the configuration for a user in the IT group using the SGT value defined in Procedure 1, "Define Security Group Tags."

**Step 4:** Repeat this procedure for every group you wish to create an SGT policy for. In this deployment, the remaining groups are Finance, HR, and Research.

Procedure 6 C

Configure SXP on WLCs

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

Step 2: On the menu bar, click Security.

Step 3: In the left pane, click TrustSec SXP.

Step 4: In the SXP State list, choose Enabled.

**Step 5:** Enter the default password. This password must match what is configured on the peer.

Step 6: Add a new peer by clicking New.

**Step 7:** Enter the IP address of the peer, and then click **Apply**. The SXP Configuration page appears.

Step 8: Click Apply.

uluili. cisco	MONITOR WLANS	CONTROLLER W	IRELESS SECURIT		nfiguration   <u>P</u> ing COMMANDS H	Lo <u>g</u> out   <u>R</u> efrest ELP FEEDBACk
Security	SXP Configurati		TVELED2 2ECONT	MENROLMENT	Apply	New
AAA     General     KADUS     Authentication     Accounting     Fallback     TACACS+     LDAP     Loal Net Users     MAC Filtering     Disabled Clients     User Login Policies     AP Policies	SXP Mode Spe Default Password	bled  sker				

Procedure 7

Configure SXP on ASA

You now configure SXP on Cisco ASA and create a policy that limits access to servers in the data center based on the SGTs.

**Step 1:** In a browser, navigate to the Cisco ASA management console at https://DC-ASA5585X.cisco.local, and then click **Run ASDM**.

Step 2: Navigate to Configuration > Firewall > Identity by TrustSec.

Step 3: Select Enable SGT Exchange Protocol (SXP).

**Step 4:** In the **Default Source** box, enter the IP address of the interface of the Cisco ASA appliance used for management.

Step 5: Enter a password, and then verify it.

Step 6: In the Server Group Setup section, click Manage.

Step 7	7: In	the (	Configure	AAA	Server	Group	window,	click Add.
--------	-------	-------	-----------	-----	--------	-------	---------	------------

Server Group	Protocol	Accounting Mode	Reactivation Mode	Dead Time	Max Failed Attempts	Add
AA-SERVER	TACACS+	Single	Depletion	10	3	Edit
OCAL	LOCAL					
						Delete
Find:		Match Case				
insi j	0 0					
	_					
ervers in the Selected						
Server Name or IP Ad	dress Interfac	e Timeout				Add
						Edit
						Delete
						Move Up
						Move Down
						Test
					-	
Find:	$\odot$	🥅 Match Case				

Step 8: In the AAA Server Group box, enter ISE-Group.

Step 9: For Accounting Mode, select Simultaneous, and then click OK.

付 Add AAA Server	Group X
AAA Server Group:	ISE-Group
Protocol:	RADIUS
Accounting Mode:	💿 Simultaneous 🔿 Single
Reactivation Mode:	O Depletion O Timed
Dead Time:	10 minutes
Max Failed Attempts:	3
🔲 Enable interim ac	counting update
🔲 Enable Active Dir	ectory Agent mode
VPN3K Compatib	ility Option 🛛 🕹
ОК	Cancel Help

Step 10: In the Selected Group section, for Servers, click Add.

Step 11: In the list, choose the firewall interface outside.

**Step 12:** In the RADIUS Parameters sections, enter the **Shared Secret Key**, accept the defaults for the remaining parameters, and then click **OK**.

薩 Add AAA Server		×
Server Group: I	SE-Group	
Interface Name:	outside	
Server Name or IP Address:	se-1.cisco.local	
Timeout:	10 seconds	
RADIUS Parameters		
Server Authentication Port:	1645	
Server Accounting Port:	1646	
Retry Interval:	10 seconds	
Server Secret Key:	****	
Common Password:		
ACL Netmask Convert:	Standard	
Microsoft CHAPv2 Capable:		
SDI Messages		
Message Table		*
ОК	Cancel Help	

**Step 13:** Repeat Step 10 through Step 12 for the secondary Cisco ISE administration node, **ise-2.cisco.local**.

Step 14: Click OK. The Configure AAA Server Groups window closes.

Step 15: Click Import PAC.

**Step 16:** Click Browse, and then locate the PAC file you saved to your machine in Step 12 of Procedure 2, "Add ASA as network device."

Step 17: Enter the PAC password, confirm it, and then click Import.

🔂 Import PAC		×
Filename:	C:\Downloads\DC-ASA5585X.pac	Browse
Password:	*****	
Confirm Password:	****	
	Import Cancel Help	

Next, you add SXP peers to Cisco ASA.

Step 18: Click Add.

Step 19: Enter the IP address of the peer.

**Step 20:** For Password, choose **Default**, for Mode, choose **Local**, and for Role, choose **Listener**, and then click **OK**.

🚰 Add Connection Peer				
ess: 10.4.63.28				
Default 💌				
Local				
Listener 💌				
Ontion	*			
option	*			
OK Cancel Help				
	ess: 10.4.63.28  Default  Local  Listener  Option			

Step 21: Repeat Step 18 through Step 20 for each peer you need to add.

### Step 22: Click Apply.

🞼 Cisco ASDM 7.0 for ASA - 10.4.53.126				_ 🗆 🗙
File View Tools Wizards Window Help			Type topic to search	
Home 🗞 Configuration 🔯 Monitoring 📄 Save	🔇 Refresh 🔇 Back 🧲	Forward 🤗 Help		CISCO
Firewall a P Configuration :	Firewall > Identity by Tru	<u>stSec</u>		
Access Rules Access Rules Access Rules Connection Pe Access Rules Filter: Peer IF Filter: Peer IF				lear
Public Servers Deer TR 0.ddr	ss Source IP Address Passw	ord Mode Role		Add
URL Filtering Servers 10.4.63.28	Default Defaul			Edit
Jentity Options	Default Default Default			
Identity by TrustSec         10.4.32.242           Image: Contract of the section	Default Default			Delete
Unified Communications     Advanced				
Default Source	10.4.53.126			
Default Passwi	rd: *****			
Confirm Passw				
🔍 Device Colum				
	120 seconds			
Firewall Reconcile Time	: 120 seconds			
Remote Access VPN				
Server Group S		1		
	Name: ISE-Group	Manage		
🔍 🖭 Refresh En	ironment Data Import P	AC		
Device Management				
»		Apply	Reset	
	🔀 Active	admin 15	🗳 📐	🔒 1/15/13 5:21:33 PM PST

#### Procedure 8

#### **Configure firewall policy**

In the *Cisco SBA--Data Center Deployment Guide*, organizational servers were defined. In this procedure, you will create policy to limit access to each server based on SGTs. In this example, you will create a rule for the server for the IT group.

Step 1: In Cisco ASDM, navigate to Configuration > Firewall > Access Rules.

Step 2: Click Add.

Step 3: From the Interface menu, choose Any.

Step 4: Select the Permit action.

**Step 5:** In the Source Criteria section, enter **any** for the Source, and then click the ellipses at the end of Security Group.

### Step 6: Choose Existing Security Group.

Step 7: Select IT\_Users, and then click Add.

Add         i         Description           Filter:	Existing Security Group Object Gr	01001			Selected Security Group			
Filter         Filter         Add >>           Existing Security Group:         Filter (Clear)         Add >>           Filter         Filter (Clear)         Add >>           Filter (Clear)         Kenove         Add >>           Filter (Clear)         Kenove         Kenove							Security Type	Description
Filter:         Filter/Clear           Mame         / 1         Count         Security         Description           Existing Security Group:         Add >>         Add >>           Filter:         Filter/Clear            Security Name         Security Tag            Attr         65535         Filter/Clear           Filter:         Filter/Clear            Security Name         Security Tag            Attr         65535         Filter/Clear           Filter:         Filter/Clear            Security Name         Security Tag            Attr         65535         Filter/Clear           Filter:         Security Lisers         5           Filter/Lisers         5         Filter/Clear           Metwork, Devices         2         Filter/Clear           Research Lisers         6         Filter/Clear	💠 Add 🛛 Edit 🏢 Delete	🔍 Where Used				COUNT		Description
Existing Security Group:         Add >>           Filter:         Filter[Clear]           Security Name         Security Tag           ANY         65535           Finance Users         5           Filter[Clear]         Filter[Clear]           ANY         65535           Finance Users         5           Filter[Clear]         Security Tag           ANY         65535           Filter[Clear]         Security Tag           ANY         65           ANY         65	Filter:		Filter Clear					
Existing Security Group: Filter :	Name A1 Count Secur	ity	Description					
Existing Security Group: Filter: Filter: Clear  Security Name Security Tag  Any 65535  Finance_Users 5  Finance_Users 4  Network_Devices 2  Research_Users 6								
Existing Security Group: Filter :								
Existing Security Group: Filter :								
Existing Security Group: Filter :								
Existing Security Group: Filter: Filter: Clear  Security Name Security Tag  Any 65535  Finance_Users 5  Finance_Users 4  Network_Devices 2  Research_Users 6								
Existing Security Group: Filter :								
Existing Security Group: Filter :								
Existing Security Group:           Filter Clear           Security Name         Security Tag           ANY         655355           Any         Generity Liters         Security Tag           Any         Security Tag           Any         Security Name         Security Name           Any         Security Tag           Any         Security Security           Any         Security Security								
Existing Security Group: Filter :								
Existing Security Group: Filter: Filter: Clear  Security Name Security Tag  Any 65535  Finance_Users 5  Finance_Users 4  Network_Devices 2  Research_Users 6	1			add ss				
ANY         65535           ANY         65535           Finance_Users         5           Regular K_Users         4           Network_Devices         2           Research_Users         6				MUU //				
Security Name     Security Tag       ANY     65535       Finance_Users     5       Regular R_Users     4       Network_Devices     2       Research_Users     6	Existing Security Group:							
ANY         65535           Finance_Users         5           A RE_Users         4           Metwork_Devices         2           A Research_Users         6			ente Let	<< Remove				
Finance_Users         5           A R_Users         4           Network_Devices         2           A Research_Users         6			Filter Clear	<< Remove				
Finance_Users         5           A R_Users         4           Network_Devices         2           A Research_Users         6	Filter:			<< Remove				
Research_Lbers         4           Network_Devices         2           Research_Lbers         6	Filter: Security Name	65535		<< Remove				
Network, Devices         2           Research_Users         6	Filter: Security Name			<< Remove				
Research_Users 6	Filter: Security Name ANY Finance_Users	5		<< Remove				
Luknown 0	Filter: Security Name ANY Finance_Users HR_Users	5		<< Remove				
	Filter: Security Name ANY Finance_Users HR_Users Network_Devices	5 4 2		<< Remove				
	Filter: Security Name ANV Finance_Users He_Users Network_Devices Research_Users	5 4 2 6		<< Remove				
	Filter: Security Name ANY Finance_Users Her_Users Network_Devices Research_Users	5 4 2 6		< Remove				
Create new Security Group member:	Filters Security Name ANY A Rinance_Users A Re_Users Network_Devices Research_Users Linknown	5 4 2 6 0		<< Remove				
	Fitters Security Name ANY Fitters HR_Users Network_Devices Research_Users Unknown Create new Security Group memb	5 4 2 6 0		<< Remove				
Create new Security Group member: Security Tag/Name:	Fitters Security Name ANY Fitters HR_Users Network_Devices Research_Users Unknown Create new Security Group memb	5 4 2 6 0		<< Remove				
Security Tag/Name:	Fitters Security Name Any Fitnence_Users HR_Users Network_Devices Research_Users Unknown Create new Security Group memb Security Tag/Name:	5 4 2 6 0	Security Tag	<< Remove				
Security Tag/Name: Tag	Fitters Security Name Any Fitnence_Users HR_Users Network_Devices Research_Users Unknown Create new Security Group memb Security Tag/Name:	5 4 2 6 0	Security Tag	<< Remove				
Security Tag/Name:	Fitters Security Name Any Fitnence_Users HR_Users Network_Devices Research_Users Unknown Create new Security Group memb Security Tag/Name:	5 4 2 6 0	Security Tag	<< Remove	4			
Security Tag/Name: Security Type: Tag	Fitters Security Name Any Fitnence_Users HR_Users Network_Devices Research_Users Unknown Create new Security Group memb Security Tag/Name:	5 4 2 6 0	Security Tag	<< Remove	<u>د</u>			
Security Type: Tag	Fitters Security Name Any Fitnence_Users HR_Users Network_Devices Research_Users Unknown Create new Security Group memb Security Tag/Name:	5 4 2 6 0	Security Tag	<< Remove	4			Cancel Help

Step 8: Click OK. The Add Access Rule window opens.

**Step 9:** In the Destination Criteria section, click the ellipses for the Destination.

**Step 10:** Double-click **IT\_Web\_Server**, and then click **OK**. The Add Access Rule window appears.

Step 11: For the service, enter tcp/http, tcp/https, and then click OK.

🖆 Add Access Rule
Interface: Any
Action: 💿 Permit 🕐 Deny
Source Criteria
Source: any -
User:
Security Group: IT_Users
Destination Criteria
Destination: IT_Web_Server
Security Group:
Service: tcp/http, tcp/https
Description:
🔽 Enable Logging
Logging Level: Default
More Options 😵
OK Cancel Help

**Step 12:** Repeat Step 2 through Step 11 for each server that you wish to create an SGT policy for. In this deployment, the remaining groups are Finance, HR, and Research.

Procedure 9

**Monitoring SGTs on Cisco ASA** 

You will use ASDM to verify SXP is working properly and SGTs are being passed to Cisco ASA.

Step 1: In Cisco ASDM, navigate to Monitoring > Properties > Identity by TrustSec > SXP Connections. This shows all the current SXP connections to the ASA.

GT Exchanç	ge Protocol (	5XP) Co	nnection	ıs:							
SXP:		Ens	abled								
Highest version: 2											
Default	password:	Set									
Default	local IP:	10.	4.53.13	26							
Reconcil	le period:	120	) secs								
Retry op	en period:	120	) secs								
Retry open timer: Not Running											
Retry op	en timer:	Not	: Runnin	ng							
	en timer: umber of SX			-							
Total nu		(P conn	nections	s: 5	1: 5						
Total nu	umber of SX	(P conn	nections	s: 5	1: 5						
Total nu	umber of SX	(P conn	nections	s: 5	1: 5						
Total nu Total nu	umber of SX	(P conn	nections	s: 5	1: 5						
Total nu Total nu eer Connec	umber of SX umber of SX	(P conn	nections	s: 5	n: 5						
Total nu Total nu	umber of SX umber of SX	(P conn	nections	s: 5	n: 5					Filter	Clear
Total nu Total nu eer Connec	umber of SX umber of SX	(P conn (P conn	nections	s: 5		Password	Reconcile Timer	Delete Hold-down Timer		Filter	
Total nu Total nu eer Connec ker: Peer If Peer	umber of SX umber of SX ction Status: P Address	(P conn (P conn (P conn (P conn (P conn)	Nection:	s: 5 s shown	Instance #	Password	Reconcile Timer Not Running	Delete Hold-down Timer Not Running		st Chang	ed
Total nu Total nu eer Connec Iter: Peer IF Peer 0.4.15.254	umber of SX umber of SX ction Status: P Address	(P conn (P conn)(P conn (P conn)(P con	Version 2	s: 5 s shown Role	Instance #				La:	st Chang 8 (dd:hr:	ed :mm:sec)
Total nu Total nu eer Connec lter: Peer IF Peer 0.4.15.254 0.4.46.64	amber of SX amber of SX ction Status: P Address Source 10.4.53.126 10.4.53.126	(P conn (P conn)(P conn (P conn)(P con	Version 2	s: 5 s shown Role Listener	Instance # 3 2	Default	Not Running	Not Running	La:	st Chang 8 (dd:hr: 4 (dd:hr:	ed :mm:sec) :mm:sec)
Total nu Total nu eer Connec lter: Peer If Peer 0.4.15.254 0.4.46.64 0.4.63.28	Amber of SX           tion Status:           P Address           Source           10.4.53.126           10.4.53.126	CP conn CP conn CP conn Status On On On On	Version 2 2 1	s: 5 s shown Role Listener Listener	Instance # 3 2 1	Default Default	Not Running Not Running	Not Running Not Running	La: 0:16:51:5 2:17:05:5	st Chang 8 (dd:hr: 4 (dd:hr: 0 (dd:hr:	ed :mm:sec) :mm:sec) :mm:sec)

Step 2: In Cisco ASDM, navigate to Monitoring > Properties > Identity by TrustSec > IP Mappings. This shows all the current IP to SGT mappings passed to the ASA.

Monito	Monitoring > Properties > Identity by TrustSec > IP Mappings						
Secu	rity Group	) IP Mapping	g Table:				
Total r	number of S	Security Group	o IP Mappings:	2			
Total r	number of S	Security Group	o IP Mappings sho	wn: 2			
Filter:	TAG	<b>•</b>		Filter	Clear		
Tag	Name	IP Address				Where Used	
3	HR_Users	10.4.57.50					-
4	IT_Users	10.4.2.14					

#### Procedure 10

#### **Monitoring SGTs on the switches**

From the command line of the switch, you monitor SXP connections and the SGT assignments using a few show commands.

**Step 1:** Verify the SGT assigned to a switch port after user authorization on an access layer switch.

show authentication session interface <interface>

## A3750X#show authentication session interface GigabitEthernet 2/0/1

Interface:	GigabitEthernet2/0/1
MAC Address:	0050.56b9.007c
IP Address:	10.4.2.13
User-Name:	alex.reed
Status:	Authz Success
Domain:	DATA
Security Policy:	Should Secure
Security Status:	Unsecure
Oper host mode:	multi-auth
Oper control dir:	both
Authorized By:	Authentication Server
Vlan Policy:	N/A
SGT:	0004-0
Session timeout:	N/A
Idle timeout:	N/A
Common Session ID:	0A040F06000001778A321722
Acct Session ID:	0x00000B5D
Handle:	0xCB000178

**Step 2:** Verify the SXP connections on a switch. show cts sxp connections

#### D6500VSS**#show cts sxp connections** SXP : Enabled Highest Version Supported: 3 Default Password : Set Default Source IP: 10.4.15.254 Connection retry open period: 120 secs Reconcile period: 120 secs Retry open timer is not running

\_\_\_\_\_

Peer IP : 10.4.15.5 Source IP : 10.4.15.254 Conn status : On Conn version : 2 Local mode : SXP Listener Connection inst# : 4 TCP conn fd : 3 TCP conn password: default SXP password Duration since last state change: 11:20:31:22 (dd:hr:mm:sec)

#### -----

\_\_\_\_\_

Peer IP	:	10.4.15.6
Source IP	:	10.4.15.254
Conn status	:	On
Conn version	:	3
Local mode	:	SXP Listener
Connection inst#	:	6
TCP conn fd	:	1
TCP conn password	d:	default SXP password
Duration since la	as	t state change: 11:20:31:22 (dd:hr:mm:sec)

Peer IP : 10.4.53.126 Source IP : 10.4.15.254 Conn status : On Conn version : 2 Local mode : SXP Speaker Connection inst# : 1 TCP conn fd : 2 TCP conn password: default SXP password Duration since last state change: 11:20:31:22 (dd:hr:mm:sec)

\_\_\_\_\_

Peer IP : 10.4.79.5 Source IP : 10.4.15.254 Conn status : On Conn version : 3 Local mode : SXP Listener Connection inst# : 1 TCP conn fd : 4 TCP conn password: default SXP password Duration since last state change: 11:20:23:02 (dd:hr:mm:sec)

Total num of SXP Connections = 4

Procedure 11 Monitoring SGTs on the WLC

You use the GUI of the WLC to monitor the SGT assignments and SXP connections.

First, verify the SGT assigned to a client after user authorization on a WLC.

Step 1: In the web console, click Monitor, and then click Clients.

Step 2: Click the client MAC address. The Details window opens.

#### Step 3: Scroll down to the Security Information section.

	MONITOR WLANS CONT	ROLLER WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	Sa <u>v</u> e Configuration   <u>P</u> ing   Logout   <u>F</u> EEDBACK
Monitor	Clients > Detail					< Back Link Test Rei
Summary Access Points Cisco CleanAir	General AVC Statisti Security Information	<b>C5</b>				
<ul> <li>Statistics</li> </ul>	Security Policy Completed	Yes				
CDP	Policy Type	RSN (WPA2)				
Rogues	Encryption Cipher	CCMP (AES)				
Redundancy	EAP Type	PEAP				
Clients	SNMP NAC State	Access				
Multicast	Radius NAC State	RUN				
Applications	CTS Security Group Tag	4				
	AAA Override ACL Name	none				
	AAA Override ACL Applied Status	Unavailable				
	AAA Override Flex ACL	none				
	AAA Override Flex ACL Applied Status	Unavailable				
	Redirect URL	none				
	IPv4 ACL Name	IT				
	IPv4 ACL Applied Status	Yes				
	IPv6 ACL Name	none				
	IPv6 ACL Applied Status	Unavailable				
	mDNS Profile Name	default-mdns-profile				
	mDNS Service Advertisement Count	0				

Next, verify SXP connections from the WLC.

Step 4: In the web console, click Security.

Step 5: In the navigation pane on the left, click TrustSec SXP.

IIIIII CISCO <u>M</u> ONITOR	<u>W</u> LANS <u>C</u> ONTROLLE	R W <u>I</u> RELESS	<u>S</u> ECURITY	Sa <u>v</u> e Co M <u>A</u> NAGEMENT	nfiguration <u>P</u> ir C <u>O</u> MMANDS	ng Logout <u>R</u> efresh HE <u>L</u> P <u>F</u> EEDBACK
Security	SXP Configurati	on			Apply	New
AAA     General     KADIUS     Authentication     Accounting     Fallback     TACACS+     LDAP     Local Net Users     MAC Filtering     Disabled Clients     User Login Policies     AP Policies	SXP Mode Spea Default Password	• 46.64	ss Connect	ion Status		
Password Policies	10.4.53.126	10.4.46.64	On	-		

#### Process

Monitoring Network Access

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

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

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

#### **Procedure 1**

#### View the Cisco ISE dashboard

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

Step 1: On the menu bar, click Home.

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



#### **Procedure 2**

#### **Configure identity groups**

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

The example below describes how to do this for an Apple iPad. The procedure for other types of devices is similar.

Step 1: In the menu bar, mouse over Policy, and then choose Profiling.

Step 2: Click Apple-iPad. This enables you to edit this policy.

Step 3: Select Create Matching Identity Group, and then click Save.

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 Profiling Poldes Profiling Poldes	Profiler Policy       * Name       Apple-IPad         Profiler Policy       * Name       Apple-IPad       Description       Policy for Apple IPad         Policy Enabled       Image: The second	
	If Condition       (Apple-IPadRule1Checkt_AND_Apple-MacBo	<u>15 ¥</u>
	Save Reset	

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 by using unique characteristics of the device. Review some of the existing profiles to get an idea of the options and methods available to you for device profiling.

The example below creates a profile for the Amazon Kindle Fire by using information obtained from the device's DHCP request and from HTTP requests.

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

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

Step 3: Click Add.

Step 4: Give the policy the name Kindle-Fire and a description.

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

**Step 6:** In the **Expression** list, next to DHCP, click the > symbol, and then choose **host-name**.

cisco Identity Services Engine		ise-1 admin Logout Feedback
🚖 Home Operations 🔻 Policy 🔻 Admir	nistration 🔻	😷 Task Navigator 👻 🕗
🚨 Authentication 🛛 💿 Authorization 🔀	Profiling 💿 Posture 🕞 Client Provisioning 🔄 Sec	curity Group Access 🚽 🐥 Policy Elements
Profiling	Profile Policy UI > New Profile Policy Profile Policy * Name Kindle-Pre Policy Enabled * Minimum Certainty Factor * Metwork Scan (NMAP) Action NONE * Network Scan (NMAP) Action Use Herarchy * Parent Policy Use Herarchy * Parent Policy Use Herarchy * Parent Policy Use Herarchy * Condition Conditions Then Certainty Factor Set Condition Name Expression Set Set Set	name-servers     pxe-dient-arch     pxe-client-machine-id     pxe-client-network-id     pre-client-network-id

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

Step 8: Choose Certainty Factor Increases, and then set the value to 10.

Step 9: Click the gear icon at the end of the rule, and then select **Insert new** rule below.

cisco Identity Services Engine	ise-1 admin Logout Feedback
🛕 Home Operations 🔻 Policy 🔻 Admi	nistration 🔻 😐 Task Navigator 🗸 🕗
👢 Authentication 🛛 🧕 Authorization 🔣	Profiling 🕜 Posture 📙 Client Provisioning 📄 Security Group Access 🦺 Policy Bernents
Profiling P P P Profiling Polices	Profiler Policy       * Name       Kindle Fire       Description       Folicy for Kindle Fire         Policy Finaled       Viet
	Submit Cancel Insert new rule above Insert new rule above Insert new rule below Delete

Step 10: Next to Conditions, click the + symbol, and then click Create New Condition (Advance Option).

Step 11: In the Expression list, next to IP, click the > symbol, and then choose User-Agent.

👌 Home Operations 🔻 Policy 🔻 Admir	istration 🔻	👓 Task Navigator 👻 😢
🛓 Authentication 🛛 🧕 Authorization 🔣	Profiling 🕐 Posture 🕞 Client Provisioning 📄 Security Group Access 🦺 Policy Elements	
Profiling	Profiler Policy Profiler Policy *Name Kndle-Fire Policy Enabled  *Minnum Certainty Factor *Exception Action NONE *Network Scan (NAPA) Action NONE *Network Scan (NAPA) Action NONE *Deate Matching Identify Group Use Herardhy *Derent Policy NONE Use Herardhy *Derent Policy NONE User-Agent User-Agent User-Agent Condition Then Certainty Factor Increases Condition Name Expression Select Attribute	@ • @ •

Step 12: In the second list, choose CONTAINS, and then, in the final box, enter kindle.

Step 13: Choose Certainty Factor Increases, set the value to 20, and then click Submit.

cisco Identity Services Engine	ise-1 admin Logout Feedback
👌 Home Operations 🔻 Policy 🔻 Admir	istration 🔻 😐 Task Navigator 👻 🕗
👗 Authentication 🛛 🧕 Authorization 🔀	Profiling 🕜 Posture 👼 Client Provisioning 📄 Security Group Access 🔥 Policy Elements
Profiling → → Profiling Polces → Profiling Polces	Profiler Policy       * Name       Kndle-File       Description       Policy for Kindle File         Policy Enabled       Image: State Sta



**Examining the authentication log** 

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

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

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

**Step 2:** In the details column of a record, click the 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. There is additional information such as the authorization profile that was matched, the SGA security group assigned, and the authentication protocol.

🔔 🚔 🖻							Launch Interactive Viewer	r 🖪
RADIUS Authenticatio	n Details							
Showing Page	1 of 1   Fir				Goto Page:	Go		
AAA Protocol > RAD	IUS Authentication Detail							4
RADIUS Audit Session AAA session ID : Date :	ID : 0a05570a00000039512fb33 ise-1/144790336/4152 February 28,2013	17						
Generated on February	28, 2013 11:44:24 AM PST							
			Actions					
				n n 178				
			Troubleshoot Auth					
			View Diagnostic	rice Configuration 🖆				
				ice Configuration				
				figuration Changes				
Authentication Summa	γ							
Logged At:	February 28,2013 11:42:52.82	0 AM						
RADIUS Status:	Authentication succeeded							
NAS Failure:								
Usemame:	pat.jones							
	40:30:04:24:EE:A9							
MAC/IP Address:								
MAC/IP Address: Network Device:	DefaultNetworkDevice : 10.5.8	1 <u>7.10</u> :						
MAC/IP Address: Network Device: Allowed Protocol:		1 <u>7.10</u> :						
MAC/IP Address: Network Device: Allowed Protocol: Identity Store:	DefaultNetworkDevice : 10.5.8 Default Network Access	1 <u>7.10</u> :						
MAC/IP Address: Network Device: Allowed Protocol:	DefaultNetworkDevice : 10.5.8	1 <u>7.10</u> :						

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

	Launch Interactive Viewe
RADIUS Authentication Details	
Showing Page 1 of 1	First Prev Next Last Goto Page: Go
∃ Authentication Details	
_ogged At:	February 28,2013 11:42:52.820 AM
Docurred At:	February 28,2013 11:42:52:820 AM
Server:	ise-1
Authentication Method:	datix
EAP Authentication Method :	FAP-TI S
EAP Tunnel Method :	
Jsemame:	pat.jones
RADIUS Username :	pat.jones
Calling Station ID:	40:30:04:24:EE:A9
Framed IP Address:	
Jse Case:	
Network Device:	DefaultNetworkDevice
Network Device Groups:	Device Type#All Device Types Location#All Locations
VAS IP Address:	10.5.87.10
VAS In Address. VAS Identifier:	RS208-WLC2504
VAS Port:	13
VAS Port ID:	13
	No. 1 1977 000 14
NAS Port Type:	Wireless - IEEE 802.11
Allowed Protocol:	Default Network Access
Service Type:	Framed
dentity Store:	
Authorization Profiles:	Finance_Users
Active Directory Domain:	
dentity Group:	RegisteredDevices
Allowed Protocol Selection Matched R	(ule: Wireless-Dot1X
dentity Policy Matched Rule:	EAP-TLS
Selected Identity Stores:	
Authorization Policy Matched Rule:	Finance SGT
SGA Security Group:	Finance Users
AAA Session ID:	ise-1/144790336/4152
Audit Session ID:	0a05570a00000039512ftx337
Funnel Details:	Tunnel-Type=(tag=0) VLAN,Tunnel-Medium-Type=(tag=0) 802,Tunnel-Private-Group-ID=(tag=0) 104
Cisco-AVPairs:	audit-session-id=0a05570a00000039512fb337
Dther Attributes:	ConfigVersionId=45, DestinationPort=1812, Protocol=Radius, Framed. MTU=1300, State=37CPMSessionID=1362570400000039512h537; 30SessionID=ise-1/144790336/4152; Airespace- Wlan-Id=1, ExternalCroupsersion Local/users/finance, cisco Local/users/pos-users, cisco Local/users/byod provisioning, cisco Local/users/domain users, cisco Local/user/fox-users, cisco Local/users/byod provisioning, cisco Local/users/domain users, cisco Local/users/fox-users, cisco Local/users/byod provisioning, cisco Local/users/domain users, cisco Local/users/fox-users, cisco Local/users/byod provisioning, cisco Local/users/domain users, cisco Local/users/fox-users, cisco Local/users/byod provisioning, cisco Local/users/fox000000039612b537; EndPointMACAddress=40-30-04-24-EE-A9, EndPointMatchedProfile=Apple- iPad Hostidentity/Group=Endpoint Identity Groups Registere0Devices, Device Type=Device Type#AII Device Types_Location=Location#AII Locations, Device IP Address=10.5 87. 10, Called-Station-ID=0c-85-25-df.76-d0: WLAN- Data_LabB R5208
Posture Status:	NotApplicable
EPS Status:	Hor spin-sere

Similar data can be found for endpoints that have authenticated with MAB. The MAC address is displayed for these records as the identity.

#### Procedure 5

**Create custom authentication reports** 

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

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

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

Step 3: Select RADIUS Authentication.

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

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

🏠 Home Operations 🔻 Policy 🔻 Adr	ninistrati	on 🔻			00	Task Navigator 👻 😢
🙍 Authentications 🛛 🔯 Endpoint Protection	n Service	- 1	💆 Alarms 📑 Reports 🔪	Troubleshoot		
Favorites Shared Catalog System						
Reports		AAA F	Protocol			
Allowed Protocol     Server Instance		Filter	Go	Clear Filter		
Server inscance     Endpoint	- 11		Report Name	🔺 Туре	Modified At	
Endpoint     Ealure Reason	- 11	0	AAA Diagnostics	System Report	Mon Feb 27 23:41:09 PST 2012	
	- 11	0	Authentication Trend	System Report	Mon Feb 27 23:41:09 PST 2012	
Network Device	- 11	0	RADIUS Accounting	System Report	Mon Feb 27 23:41:09 PST 2012	
User User	- 11	۰	RADIUS Authentication	System Report	Mon Feb 27 23:41:09 PST 2012	
Security Group Access		Run	Add To Favorite Delete			Reset Reports
Session Directory		1 .	Last 30 Min			
Posture			Last Hour s of type 'System Last 12 Hours	Report', hover mouse over	the 'Report Name' to view the repor	t description.
Endpoint Protection Service			eport Name' to ru	un report for today. n 'Run' button to select addit	tional 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

User:		Select	) <u>Cle</u>
MAC Address:		Select	) <u>cı</u>
Identity Group:		Select	) <u>cı</u>
Device Name:		Select	) <u>cı</u>
Device IP:		Select	) <u>cı</u>
Device Group:		Select	) <u>cı</u>
Allowed Protocol:		Select	) <u>cı</u>
Identity Store:		Select	) <u>cı</u>
Server:		Select	) <u>cı</u>
Failure Reason:		Select	) <u>cı</u>
SGA SGT:		Select	) <u>cı</u>
Show only SGA SGT Assignments:			
Include SGAEnvironment:			
Radius Audit Session ID:			<u>Cl</u>
Session ID:			Cli
Authentication Status:	Pass Or Fail 👻		
Authentication Method:		Select	) <u>cı</u>
Time Range:	Today 🗸		
Start Date:	im (mm/dd/yyyy)		
End Date:	(mm/dd/yyy)		

#### Procedure 6

**Identify endpoints** 

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

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

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

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

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

🏠 Home Operations 🔻 Policy 🔻 Admir	istration 🔻		👓 Task Navigator 👻 😢
🔜 Authentications 🛛 🧔 Endpoint Protection :	Service 💆 Alarms 🧮 Reports 💊 Troubleshoot		
Favorites Shared Catalog System			
Reports	Endpoint		
AAA Protocol			
Allowed Protocol	Filter: Oo Clear Filter		
Server Instance	Report Name	<ul> <li>Type</li> </ul>	Modified At
W Endpoint	C Endpoint MAC Authentication Summary	System Report	Mon Feb 27 23:41:09 PST 2012
Failure Reason	Endpoint Profiler Summary	System Report	Mon Feb 27 23:41:09 PST 2012
Network Device	C Endpoint Time To Profile	System Report	Mon Feb 27 23:41:09 PST 2012
User User	C Top N Authentications By Endpoint Calling Station ID	System Report	Mon Feb 27 23:41:09 PST 2012
Security Group Access	O Top N Authentications By Machine	System Report	Mon Feb 27 23:41:09 PST 2012
Session Directory	Run - Add To Favorite Delete		Reset Reports
Posture	Today		
Endpoint Protection Service	Yesterday s of type 'System Report', hover mouse ov Last 7 days Last 30 days eport Name' to run report for today. eport and click on 'Run' button to select ac Query And Run		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		Prof	iler History
Logged At :	Feb 28, 2013 11:39 AM	Day	Endpoint policy
Server :	ise-1 Profiler is triggering Change Of	Feb 28, 2013 11:39 AM	Apple-Device
Event :		Feb 28, 2013 11:39 AM	Apple-iPad
Endpoint MAC Address :	Authorization Request 40:30:04:24:EE:A9	Feb 27, 2013 1:39 PM	Apple-Device
Endpoint Policy :	Apple-iPad	Feb 27, 2013 1:39 PM	Apple-iPad
Certainity Metric :			
Endpoint Matched Policy :	Apple-iPad		
Identity Group :	Apple-iPad		

#### Figure 4 - Endpoint Details

enerated on February 28, 201	3 5:01:30 PM PST
dpoint Session time : 38	
ndpoint Details	
indpoint Static Assignment :	
indpoint Source :	
ndpoint OUI :	Apple, Inc.
ndpoint Host Name :	
ndpoint Subnet :	
ndpoint NAD Address :	10.5.87.10
ndpoint VLAN :	
ndpoint FQDN :	
ndpoint Nameserver :	
ndpoint Property :	CPMSessionID=0a05570a0000038512fb262
	Event-Timestamp=1362080368
	NetworkDeviceGroups=Device Type#All Device Types Location#All Locations
	cisco-av-pair=audit-session-id=0a05570a00000038512fb262
	dhcp-option=host-name=SBA-iPad2
	nas-update=true
	Calling-Station-ID=40-30-04-24-ee-a9
	DestinationPort=1812
	AcsSessionID=ise-1/144790336/4148
	Device Type=Device Type#All Device Types
	Service-Type=Framed
	NAS-Identifier=RS208-WLC2504 TimeToProfile=9
	LastNmapScanTime=0
	Acct-Delay-Time=0
	AuthenticationMethod=MSCHAPV2
	EapAuthentication=EAP-MSCHAPv2
	NetworkDeviceName=DefaultNetworkDevice
	Tunnel-Type=(tag=0) VLAN
	NAS-Port-Type=Wireless - IEEE 802.11 RegistrationTimeStamp=0
	Acct-Session-Id=512fb26f/40:30:04:24:ee:a9/27
	PostureAssessmentStatus=NotApplicable
	IdentityGroupID=1104cba0-237c-11e2-a044-005056a25d6d
	Total Certainty Factor=30
	User-Name=pat.jones
	AuthenticationIdentityStore=AD1
	MatchedPolicyID=70024e80-be86-11e1-ba69-0050568e002b DestinationIPAddress=10.4.48.41
	NAS-Port=13
	Class=CACS:0a05570a00000038512fb262:ise-1/144790336/4148
	Acct-Session-Time=1
	ADDomain=cisco.local
	NmapScanCount=0
	EndPointMACAddress=40-30-04-24-EE-A9
	Tunnel-Private-Group-ID=(tag=0) 104
	ServiceSelectionMatchedRule=Wireless-Dot1X
	PortalUser= RequestLatency=2
	Tunnel-Medium-Type=(tag=0) 802
	EapTunnel=PEAP
	AuthState=Authenticated
	Airespace-Wlan-Id=1
	Acct-Input-Octets=0
	PostureStatus=Unknown
	Acct-Authentic=RADIUS
	host-name=SBA-iPad2
	FirstCollection=1362080372532 EndPointPolicyID=70024e80-be86-11e1-ba69-0050568e002b
	SelectedAccessService=Default Network Access
	Acct-Status-Type=Interim-Update
	attribute-52=00:00:00
	AuthorizationPolicyMatchedRule=Finance SGT
	IdentityPolicyMatchedRule=Default
	MessageCode=3002
	attribute-53=00:00:00
	Acct-Input-Packets=0
	Acct-Output-Octets=0 DeviceRegistrationStatus=notRegistered
	DeviceRegistrationStatus=notRegistered SelectedAuthorizationProfiles=Finance Users
	Framed-MTU=1300
	IdentityAccessRestricted=false
	SelectedAuthenticationIdentityStores=AD1
	ExternalGroups=cisco.local/users/finance\
	cisco.local/users/pos-users\
	cisco.local/users/byod provisioning\
	cisco.local/users/domain users\
	cisco.local/builtin/users Response={User-Name=pat.jones; State=ReauthSession:0a05570a00000038512/b262;
	Response={User-Name=pat.jones; State=ReauthSession:Ua055/Ua0U000036512fb252; Class=CACS:0a05570a00000038512fb262:ise-1/144790336/4148; Termination-Action=RADIUS-Request; cisco-
	class=CACS:uau55/uau000u0u36512fb2b2:lse-1/144/90336/4146; Termination-Action=RADIOS-Request; clsco- av-pair=cts:security-group-tag=0005-0; MS-MPPE-
	av-par=cts.secumy-group-tag=ouds-o, iniS-iniFPE- Send-Key=56:3cta1:08:52:72:61:37:a3:4a:b1:f4:72:30:a9:41:f4:56:e8:d3:6ctad:29:d1:f4:f1:67:05:37:b5:1b:bf;
	MS-MPPE-
	Recv-Key=e6ic9ie1:08:1a:ca:86:0f:1d:ae:c4:0b:59:8b:02:2f:5a:50:8a:34:4a:88:74:38:d1:96:82:ae:08:23:27:0c; }
	Location=Location#All Locations
	PolicyVersion=19
	Device IP Address=10.5.87.10
	State=37CPMSessionID=0a05570a00000038512fb262\;30SessionID=ise-1/144790336/4148\;
	NmapSubnetScanID=0 Acct-Output-Packets=0

#### 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.

Identity Services Engine     Identity Services Engine     Atmain Operations      Policy      Admin     Authentications     Policy	istration 🔹 Service 💆 Alarms 🏢 Reports 🔾	Troubleshoot		Logout Feedback Navigator • 📀
Favorites Shared Catalog System           Reports           W AAA Protocol	AAA Protocol			
Allowed Protocol     Server Instance	Filter:	Clear Filter		
Endpoint     Failure Reason     Network Device     User	Report Name     AAA Diagnostics     Authentication Trend     RADIUS Accounting     RADIUS Authentication	Type System Report System	Modified At Mon Feb 27 23:41:09 PST 2012 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 Posture	Run + Add To Favorite Delete Last 30 Min Last Hour s of type 'System	n Report', hover mouse over t		Reset Reports
Endpoint Protection Service	eport Name' to I	un report for today. n 'Run' button to select addit	ional options.	

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

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

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

Se	arch		J						
:	Gearch	Filter: Search	3						
		Criteria							
	0	Blacklist							
	0	Guest							
	0	Profiled							
	0	Profiled:Android							
	۲	Profiled:Apple-iPad							
	0	Profiled:Apple-iPhone							
	Apply Cancel								
	0	Select Identity Groups							

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

Figure 5 - Sample report

AAA Prot	AAA Protocol > RADIUS Authentication									
ldentity Group : Profiled:Apple-iPad Authentication Status : Pass or Fail Date : January 29,2013 - February 27,2013 ( <u>Last 30 Minutes   Last Hour   Last 12 Hours   Today   Yesterday   Last 7 Days</u>   Last 30 Days )										
	Generated on February 28, 2013 5:24:43 PM PST ✓ Pass ★=Fail = <pre>Set_All = Click for details = <pre>% = Mouse over item for additional information</pre></pre>									
Lo	ogged At	RADIUS Status	NAS Failure D	etails	Event	Username	MAC/IP Address	Allowed Protocol	Service Type	Authentication Protocol
Feb 27,13	1:39:24.237 PM				Authentication succeeded	<u>pat.jones</u>	40:30:04:24:EE:A9	Default Network Access	Framed	PEAP (EAP-MSCHAPv2)
Feb 27,13	1:39:17.342 PM			0	Authentication succeeded	pat.jones	40:30:04:24:EE:A9	Default Network Access	Framed	PEAP (EAP-MSCHAPv2

Notes		

# Appendix A: Product List

## **Network Management**

Functional Area	Product Description	Part Numbers	Software
Identity Management	Cisco Identity Services Engine Virtual Appliance	ISE-VM-K9=	1.1.2.145
	Cisco ISE Base License for 2500 Endpoints	L-ISE-BSE-2500=	
	Cisco ISE Base License for 3500 Endpoints	L-ISE-BSE-3500=	
	Cisco ISE Base License for 5000 Endpoints	L-ISE-BSE-5K=	
	Cisco ISE Base License for 10,000 Endpoints	L-ISE-BSE-10K=	
	Cisco ISE Advanced 3-year License for 2500 Endpoints	L-ISE-ADV3Y-2500=	
	Cisco ISE Advanced 3-year License for 3500 Endpoints	L-ISE-ADV3Y-3500=	
	Cisco ISE Advanced 3-year License for 5000 Endpoints	L-ISE-ADV3Y-5K=	
	Cisco ISE Advanced 3-year License for 10,000 Endpoints	L-ISE-ADV3Y-10K=	
Network Management	Cisco Prime Infrastructure 1.1	R-PI-1.1-K9	4.2
	Prime Infrastructure 1.1 Software – 50 Device Base License	R-PI-1.1-50-K9	
	Prime Infrastructure 1.1 Software – 100 Device Base License	R-PI-1.1-100-K9	
	Prime Infrastructure 1.1 Software – 500 Device Base License	R-PI-1.1-500-K9	
	Prime Infrastructure 1.1 Software – 1K Device Base License	R-PI-1.1-1K-K9	
	Prime Infrastructure 1.1 Software – 2.5K Device Base License	R-PI-1.1-2.5K-K9	
	Prime Infrastructure 1.1 Software – 5K Device Base License	R-PI-1.1-5K-K9	

## **LAN Access Layer**

Functional Area	Product Description	Part Numbers	Software
Modular Access Layer	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.3.0.SG(15.1-1SG)
Switch	Cisco Catalyst 4500 E-Series Supervisor Engine 7L-E	WS-X45-SUP7L-E	IP Base license
	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	

Functional Area	Product Description	Part Numbers	Software
Stackable Access Layer	Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-48PF-S	15.0(2)SE
Switch	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-24P-S	IP Base license
	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(2)SE IP Base license
	Cisco Catalyst 3560-X Series Standalone 24 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-24P-S	
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
Stackable Access Layer Switch	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-48FPD-L	15.0(2)SE LAN Base license
	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-48FPS-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-24PD-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-24PS-L	
	Cisco Catalyst 2960-S Series Flexstack Stack Module	C2960S-STACK	

## **Wireless LAN Controllers**

Functional Area	Product Description	Part Numbers	Software
On Site, Remote Site, or	Cisco 5500 Series Wireless Controller for up to 500 Cisco access points	AIR-CT5508-500-K9	7.4.100.0
Guest 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	
	Cisco 5500 Series Wireless Controller for High Availability	AIR-CT5508-HA-K9	

Functional Area	Product Description	Part Numbers	Software
On Site Controller, Guest	Cisco 2500 Series Wireless Controller for up to 50 Cisco access points	AIR-CT2504-50-K9	7.4.100.0
Controller	Cisco 2500 Series Wireless Controller for up to 25 Cisco access points	AIR-CT2504-25-K9	
	Cisco 2500 Series Wireless Controller for up to 15 Cisco access points	AIR-CT2504-15-K9	
	Cisco 2500 Series Wireless Controller for up to 5 Cisco access points	AIR-CT2504-5-K9	

## **Wireless LAN Access Points**

Functional Area	Product Description	Part Numbers	Software
Wireless Access Points	Cisco 3600 Series Access Point Dual Band 802.11a/g/n and CleanAir with Internal Antennas	AIR-CAP3602I-x-K9	7.4.100.0
	Cisco 3600 Series Access Point Dual Band 802.11a/g/n and CleanAir with External Antennas	AIR-CAP3602E-x-K9	
	Cisco 2600 Series Access Point Dual Band 802.11a/g/n and CleanAir with Internal Antennas	AIR-CAP2602I-x-K9	
	Cisco 2600 Series Access Point Dual Band 802.11a/g/n and CleanAir with External Antennas	AIR-CAP2602E-x-K9	
	Cisco 1600 Series Access Point Dual-band controller-based 802.11a/g/n with Internal Antennas	AIR-CAP1602I-x-K9	
	Cisco 1600 Series Access Point Dual-band controller-based 802.11a/g/n with External Antennas	AIR-CAP1602E-x-K9	

## **Data Center Services**

Functional Area	Product Description	Part Numbers	Software
Firewall	Cisco ASA 5585-X Security Plus IPS Edition SSP-40 and IPS SSP-40 bundle		ASA 9.0(1)
	Cisco ASA 5585-X Security Plus IPS Edition SSP-20 and IPS SSP-20 bundle	ASA5585-S20P20X-K9	IPS 7.1(6) E4
	Cisco ASA 5585-X Security Plus IPS Edition SSP-10 and IPS SSP-10 bundle	ASA5585-S10P10XK9	

## **Data Center Virtualization**

Functional Area	Product Description	Part Numbers	Software
Virtual Switch	al Switch Nexus 1000V CPU License Qty-1		4.2(1)SV2(1.1)
Nexus 1000V VSM on Physical Media N1		N1K-VSMK9-404S12=	

## 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 1.1.2.145.
- We upgraded the Cisco Wireless LAN Controllers to software version 7.4.100.1.
- We modified the Cisco 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 added BYOD support for wired devices.
- We deployed the DHCP Profiling feature on the wireless LAN controllers to simplify the profiling configuration and eliminate the need to send copies of DHCP requests to the Cisco ISE appliances.
- We added support for the provisioning of Microsoft Windows and Apple Mac OS X devices on both wired and wireless networks using the selfprovisioning portal feature in Cisco ISE. Provisioning includes configuring the 802.1X supplicant and deploying digital certificates.
- We added Security Group Access (SGA) support to our deployment, using Security Group Tags (SGT), Security Group Tag Exchange Protocol (SXP), and Security Group Firewall (SG-FW) to enforce our access policy.
- We added Cisco Nexus 1000v to the architecture in order to support using SGA with virtualized desktops.

## Notes

### Feedback

Please use the feedback form to send comments and suggestions about this guide.



cisco.

Americas Headquarters Cisco Systems, Inc. San Jose, CA Asia Pacific Headquarters Cisco Systems (USA) Pte. Ltd. Singapore Europe Headquarters Cisco Systems International BV Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

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

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

© 2013 Cisco Systems, Inc. All rights reserved.

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