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 10.5.204.5 255.255.255.0
```

Comments and Questions

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

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

Table of Contents

What's In This SBA Guide

Cisco SBA Solutions

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

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

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

Route to Success

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

About This Guide

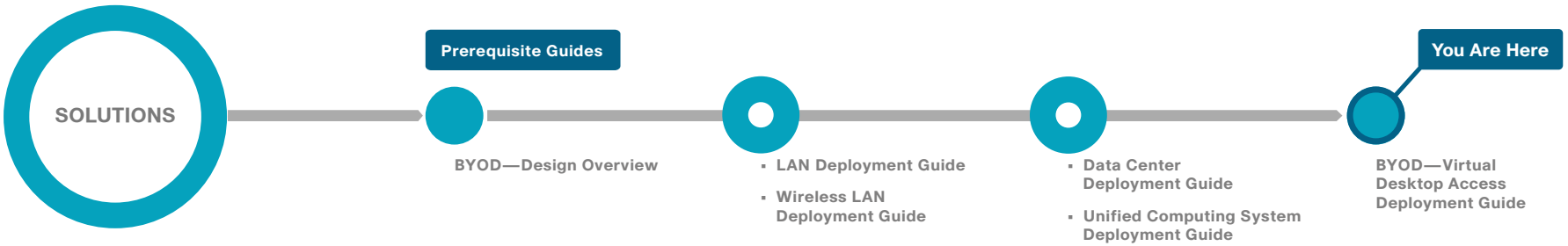
This *deployment guide* contains one or more deployment chapters, which each include the following sections:

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

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

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

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



Introduction

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.

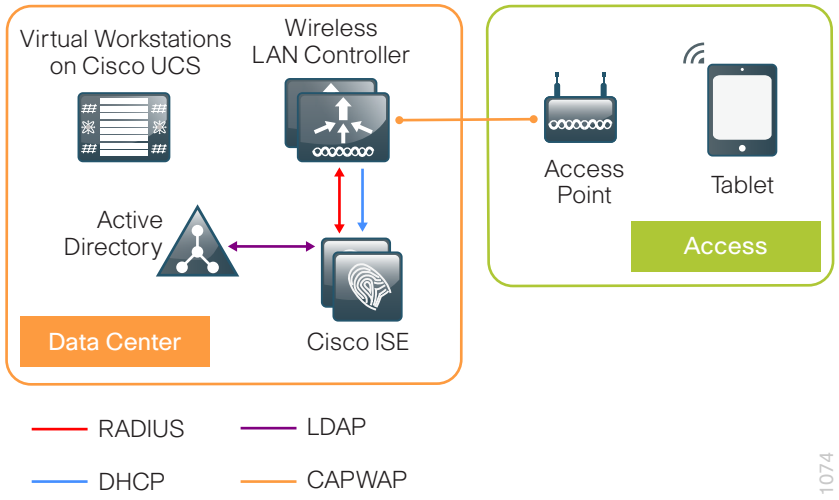
This deployment uses Cisco ISE as the authentication, authorization, and accounting server for wireless network users who connect using RADIUS. Cisco ISE acts as a proxy to the existing Active Directory (AD) services to maintain a centralized identity store for all network services.

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, closed—and 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

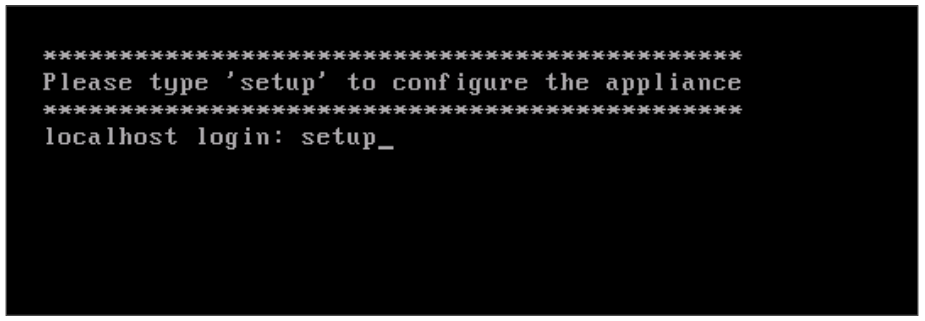
Process

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**.

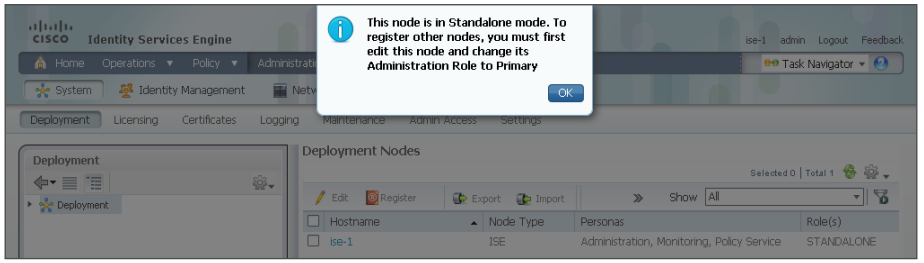
Step 10: Repeat this procedure for the remaining engines, ise-3.cisco.local and ise-4.cisco.local.

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.

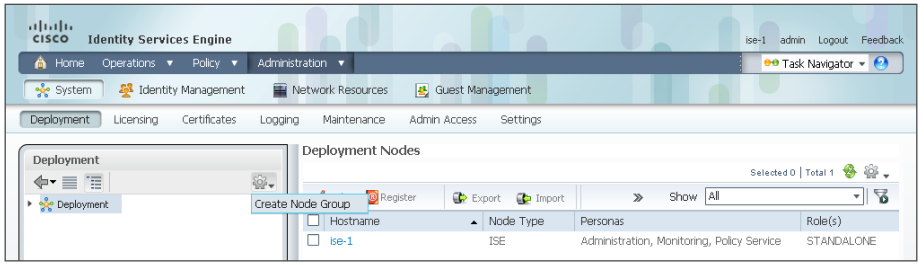
Step 1: Connect to http://ise-1.cisco.local.

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**.



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

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



Step 4: Configure the node group with the node group name ISE-Group and the default multicast address of 228.10.11.12, and then click **Submit**.

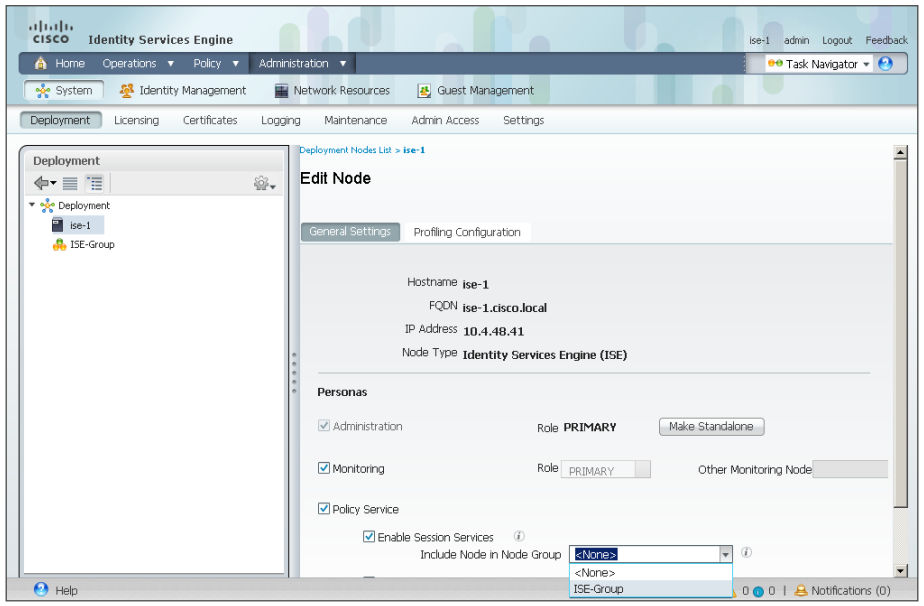
Step 5: A pop-up window lets you know the group was created successfully. Click **OK**.

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

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

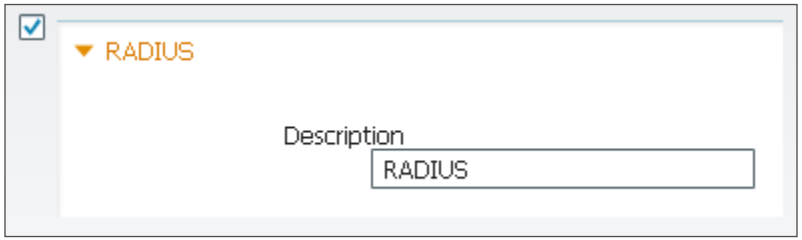
Step 8: On the General Settings tab, in the Personas section, next to the Administration Role, click **Make Primary**.

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

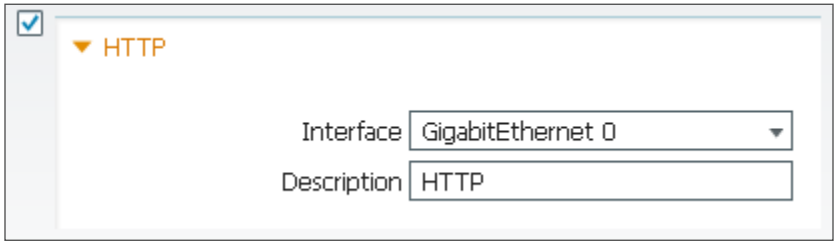


Next, you'll configure which methods are used to profile network endpoints.

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

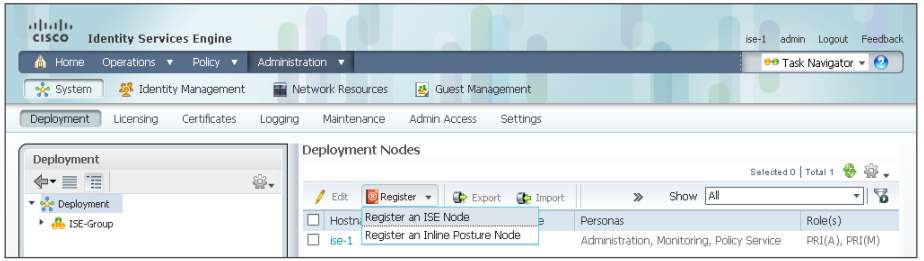


Step 11: Select **HTTP**, use the default parameters, and then click **Save**.



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

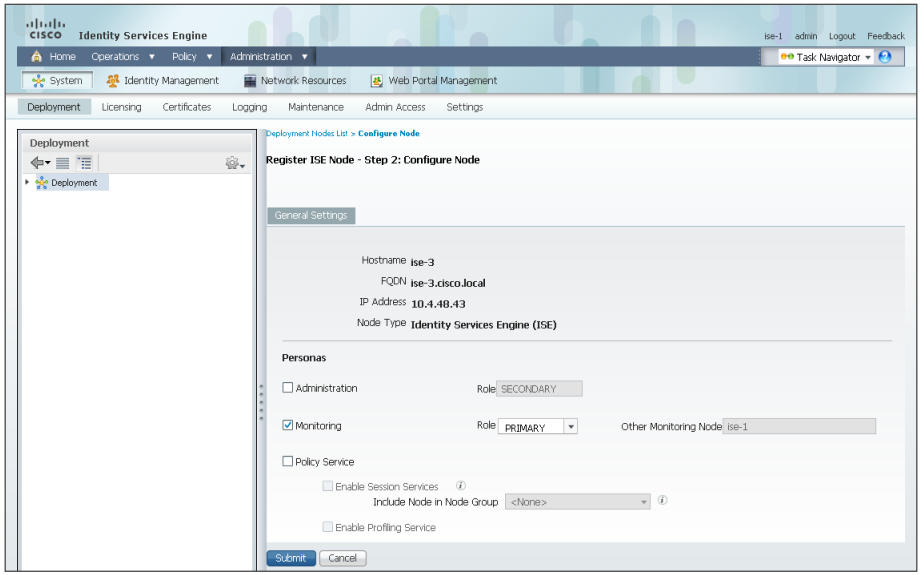
Step 13: Click **Register,** and then choose **Register an ISE Node**.



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**.

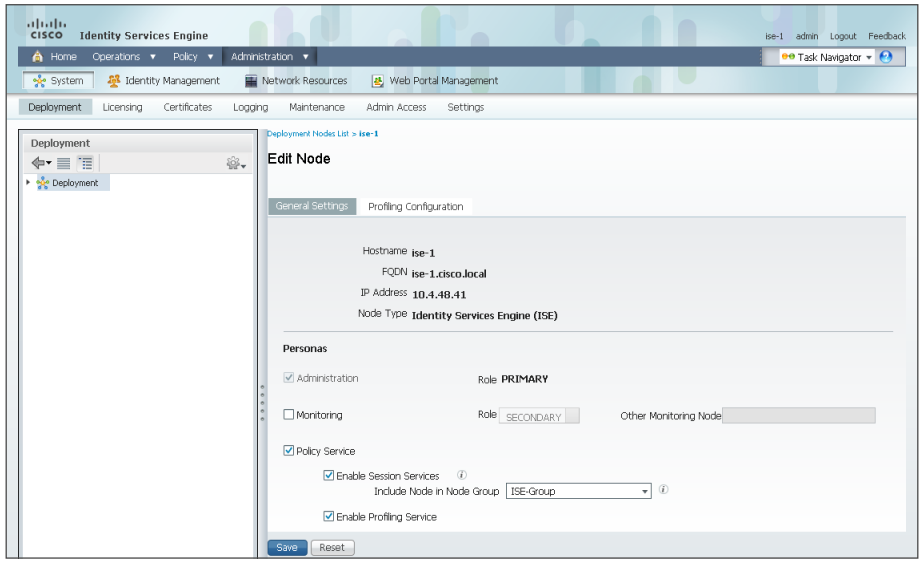
Step 15: Select **Monitoring**, and then in the **Role** list, choose **Primary**. Make sure **Administration** and **Policy Service** are not selected.

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



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.



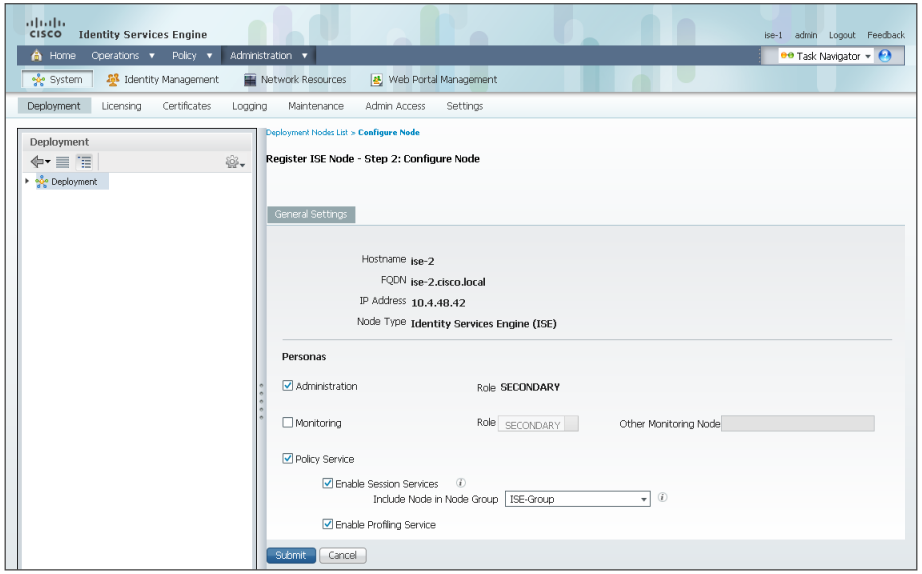
Step 19: Log in to the console, and then in the **Administration** menu, in the System section, choose **Deployment**.

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**.

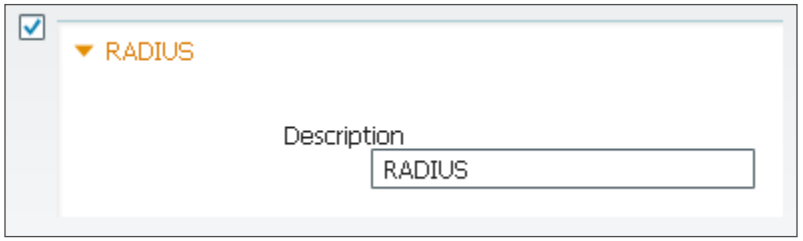
Step 23: Click **Submit**. The node registers, and a pop-up window displays letting you know that the process was successful. Click **OK**.



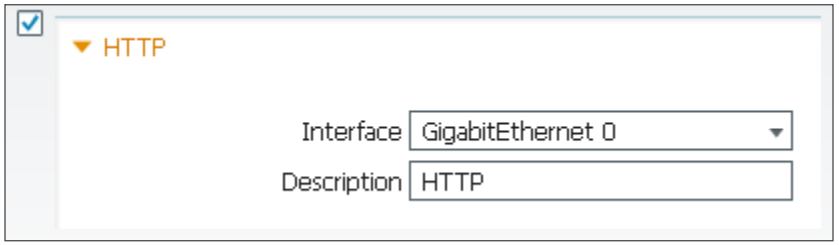
Next, you'll configure which methods are used to profile network endpoints for the secondary policy service node.

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

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



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



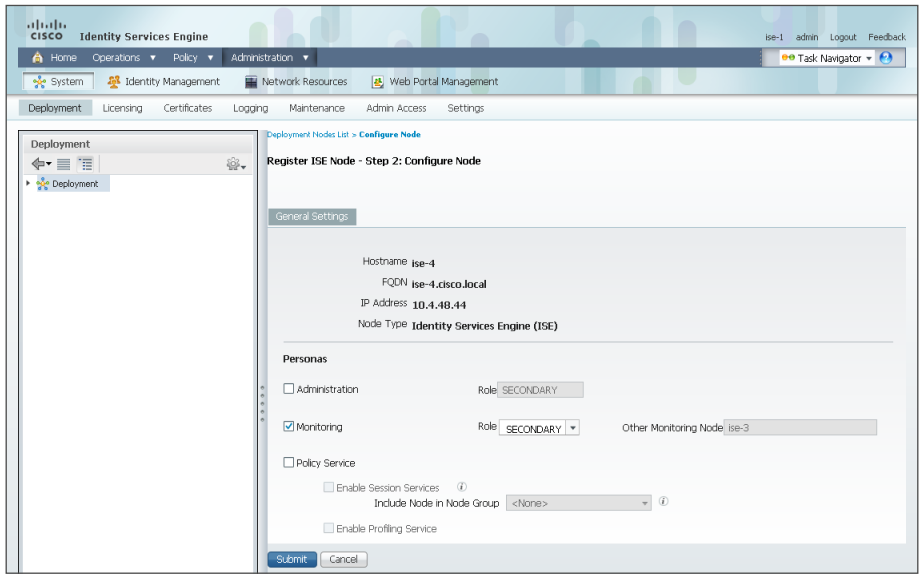
Step 27: In the Edit Node window, click **Deployment Nodes List**. The Deployment Nodes window appears.

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.

Tech Tip

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

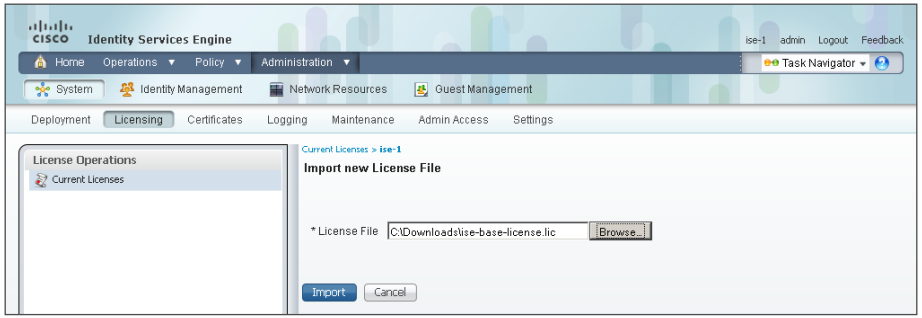
Step 1: Mouse over **Administration**, and then, from the System section of the menu, choose **Licensing**.

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

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

Step 3: Under Licensed Services, click **Add Service**.

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



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

Procedure 6 Configure network devices in Cisco ISE

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

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

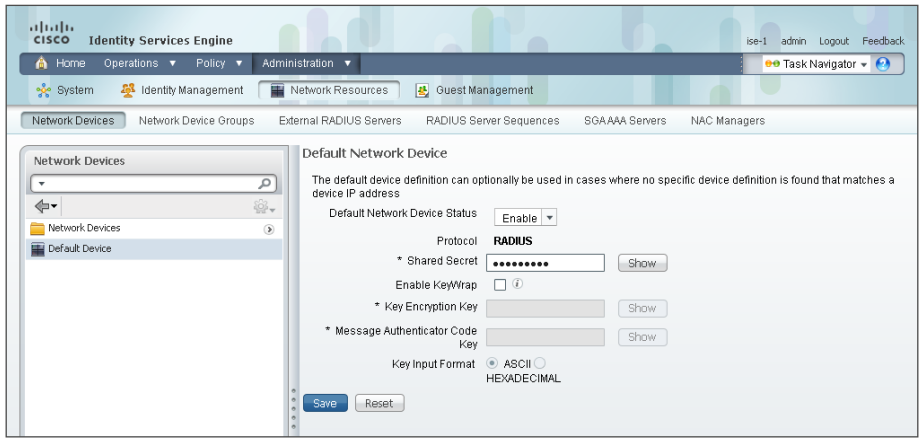
Step 2: In the left pane, click **Default Device**.

Tech Tip

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

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

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



Procedure 7 Configure Cisco ISE to use Active Directory

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

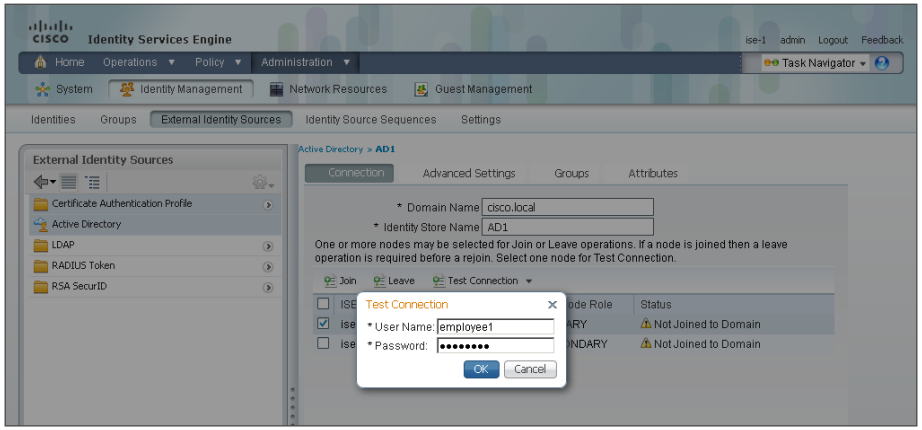
Step 1: Mouse over **Administration**, and then, from the Identity Management section of the menu, choose **External Identity Sources**.

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

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

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

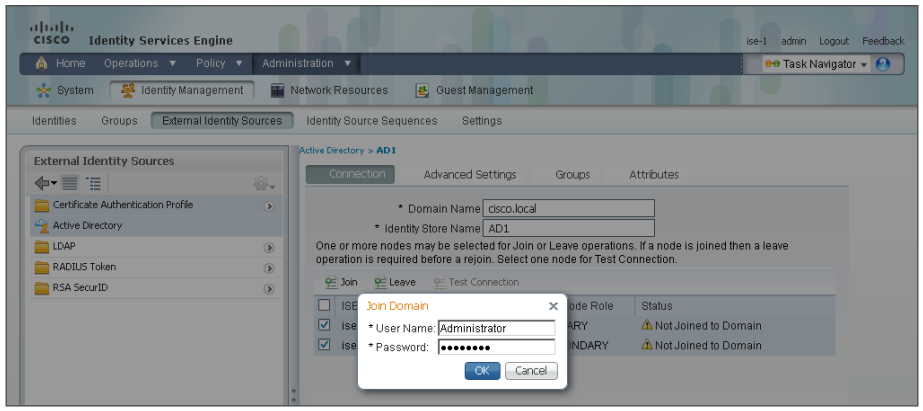
Step 5: Enter the credentials for a domain user, and then click **OK**.



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

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

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

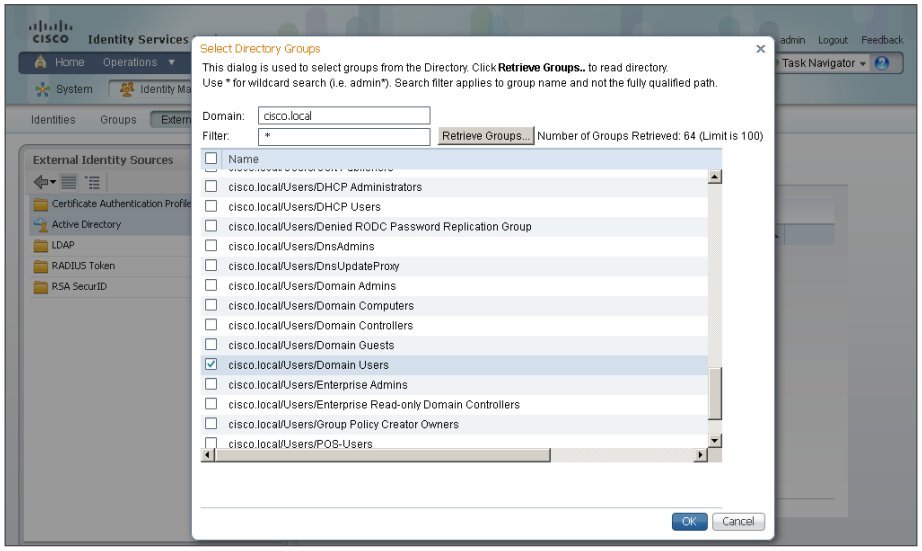


Next, you select which groups from AD that Cisco ISE will use for authentication.

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

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

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



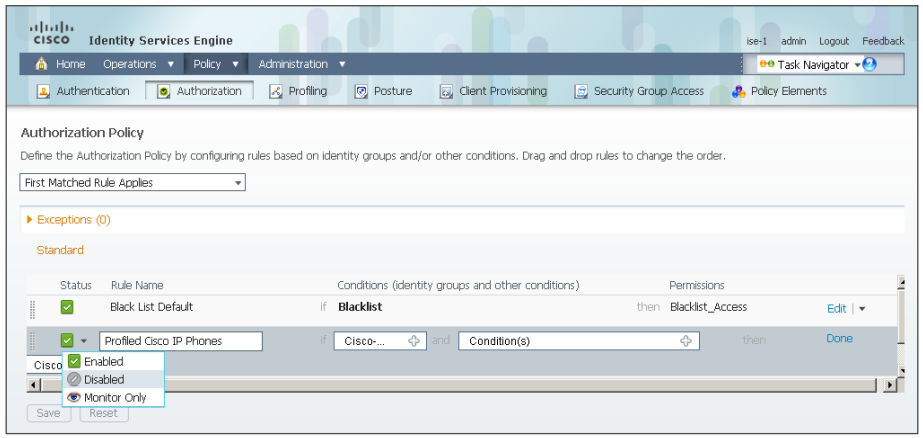
Step 12: Click **Save Configuration**.

Procedure 8 Disable IP Phone authorization policy

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

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

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



Process

Enabling Visibility to the LAN

1. Configure MAC Authentication Bypass
2. Configure 802.1X for wired users
3. Enable RADIUS in the access layer
4. Enable identity 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.

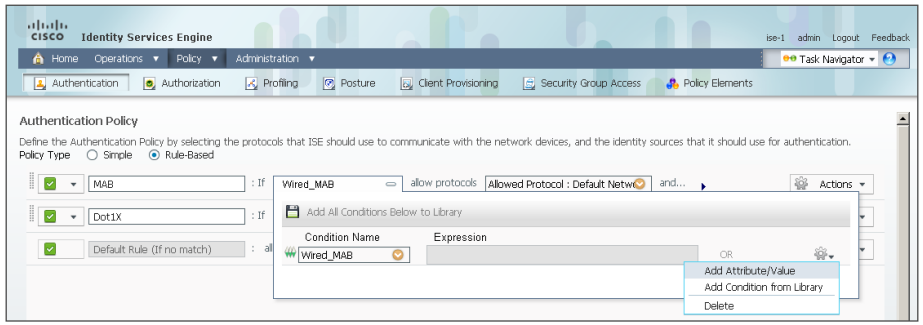
Procedure 1 Configure MAC Authentication Bypass

MAC Authentication Bypass (MAB) allows you to configure specific machine MAC addresses on the switch to bypass the authentication process. 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.

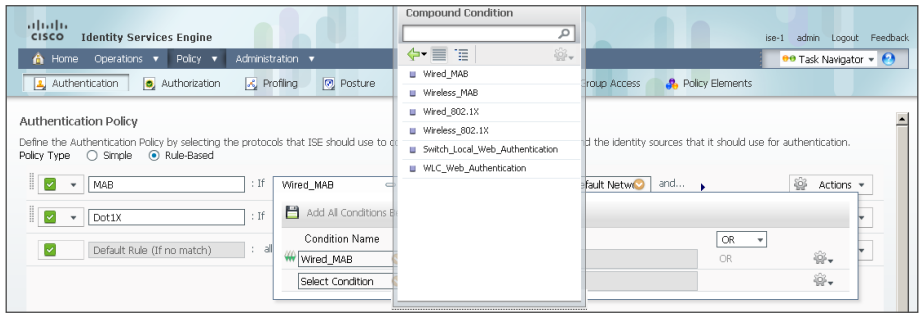
There are already two default rules in place, MAB and Dot1X.

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**.

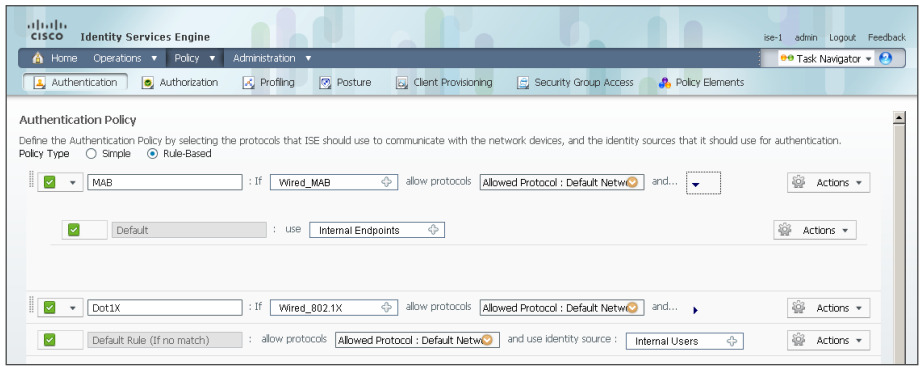


Step 3: In the **Select Condition** list, next to **Compound Condition**, click the > symbol.

Step 4: Choose **Wireless_MAB,** and then click anywhere to continue.



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.

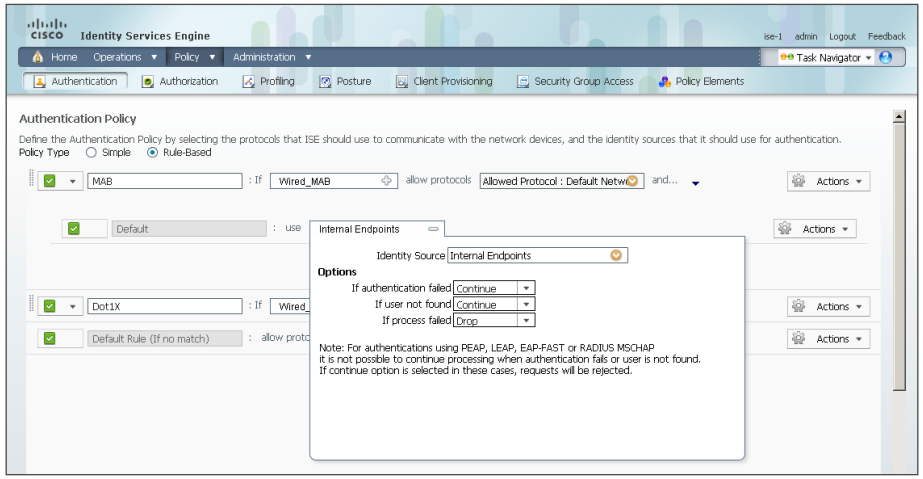


Next, you change the options on the Internal Users database, which is used for profiling.

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



Procedure 2 Configure 802.1X for wired users

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

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

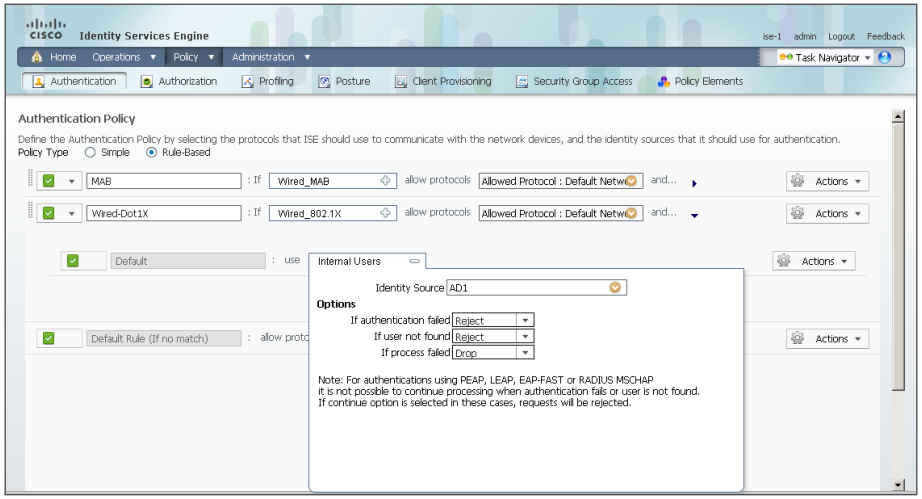
Step 2: To differentiate this from a wireless 802.1X rule, rename the rule Wired-Dot1X.

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

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

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

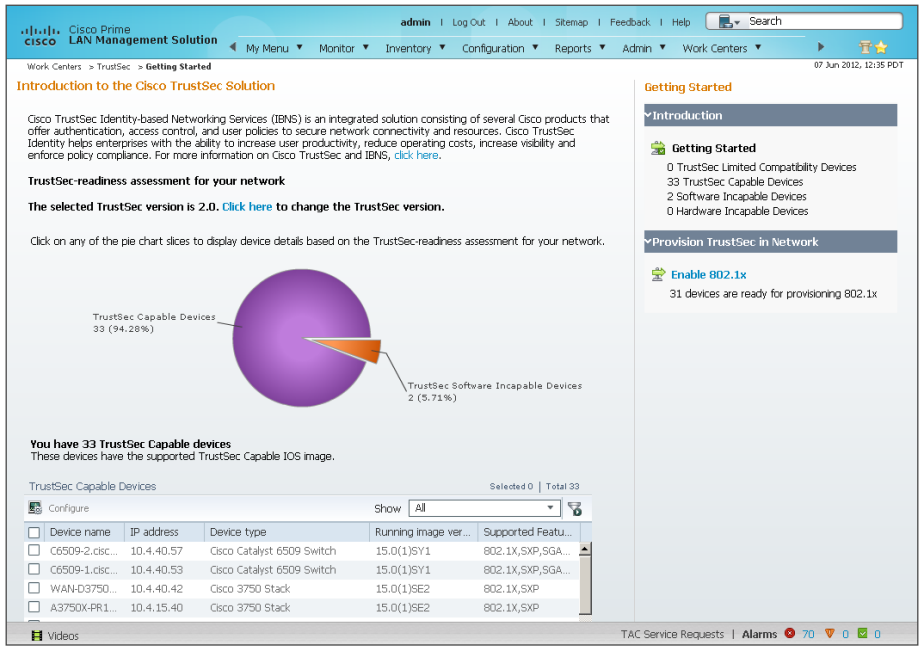
Step 5: In the **Identity Source** list, choose the previously defined AD server **AD1**, use the default options for this identity source, click anywhere in the window to continue, and then click **Save**.



Procedure 3 Enable RADIUS in the access layer

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

Step 2: Mouse over **Work Centers**, and then, from the TrustSec section, choose **Getting Started**. This shows the network's Cisco TrustSec-readiness assessment, which verifies that the software versions support the identity features and that the switches are capable of running RADIUS.



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**.

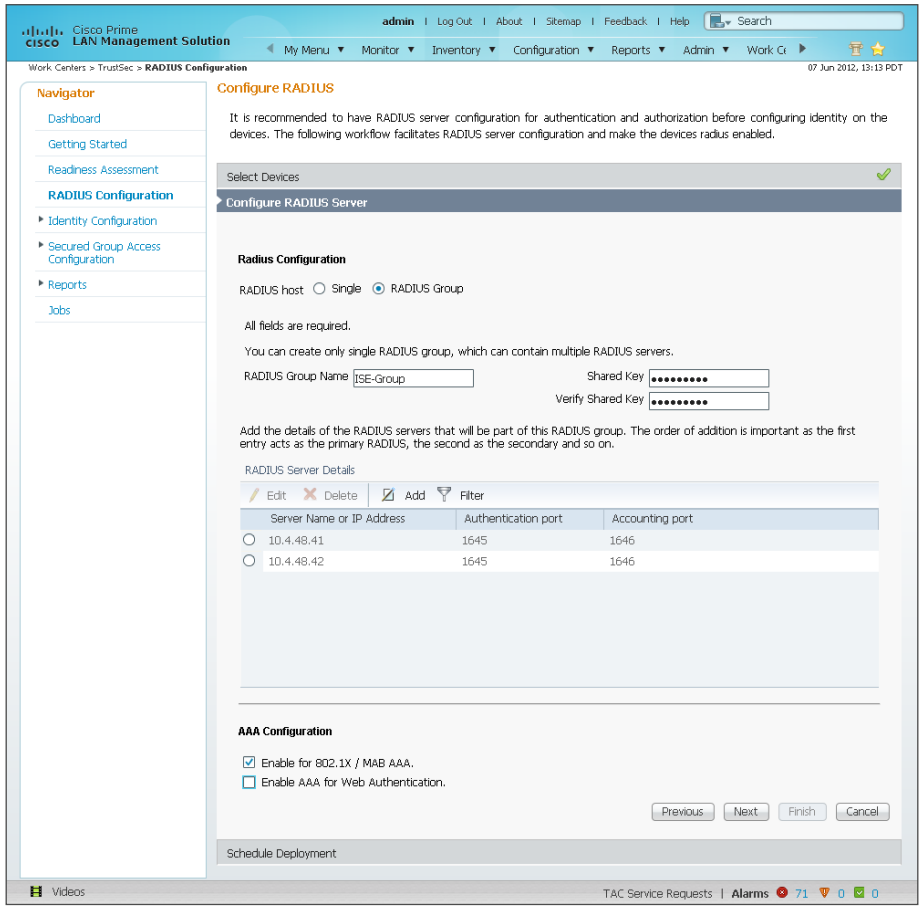
Step 5: On the Configure RADIUS page, select **RADIUS Group**, and in the **RADIUS Group Name** box, enter **ISE-Group**, and then in the **Shared Key** box, use the value used in previous procedures.

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**.



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

Tech Tip

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

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

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

Procedure 4 Enable identity and web authentication

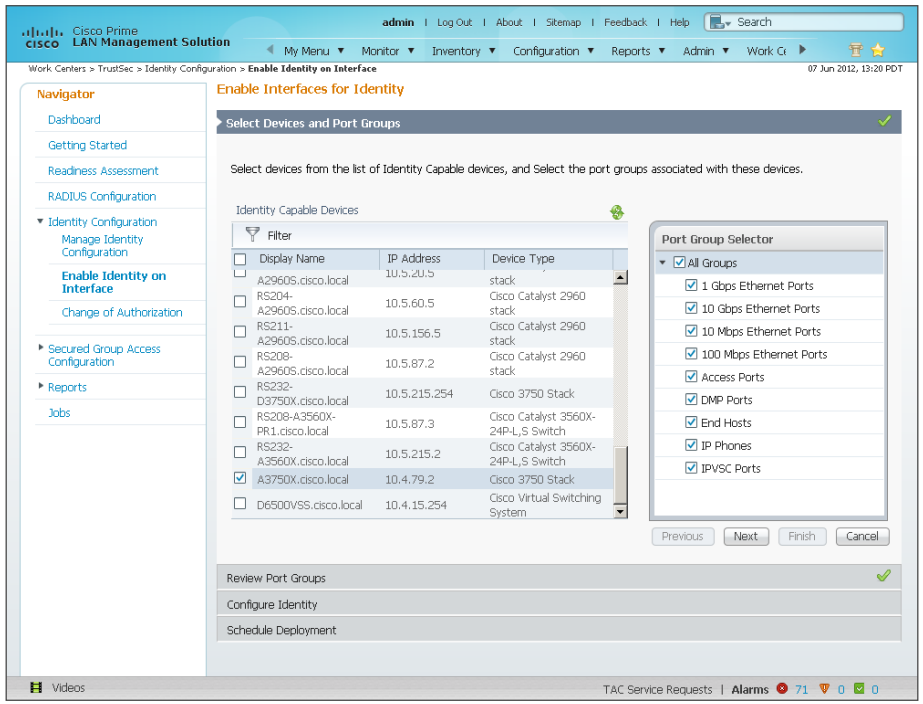
The identity configuration enables MAB on the switch. Web authentication allows users to access the network from a device that isn't configured for 802.1X and still be authenticated. The TrustSec Work Center supports configuring local web authentication, however, in this deployment you use centralized 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**.

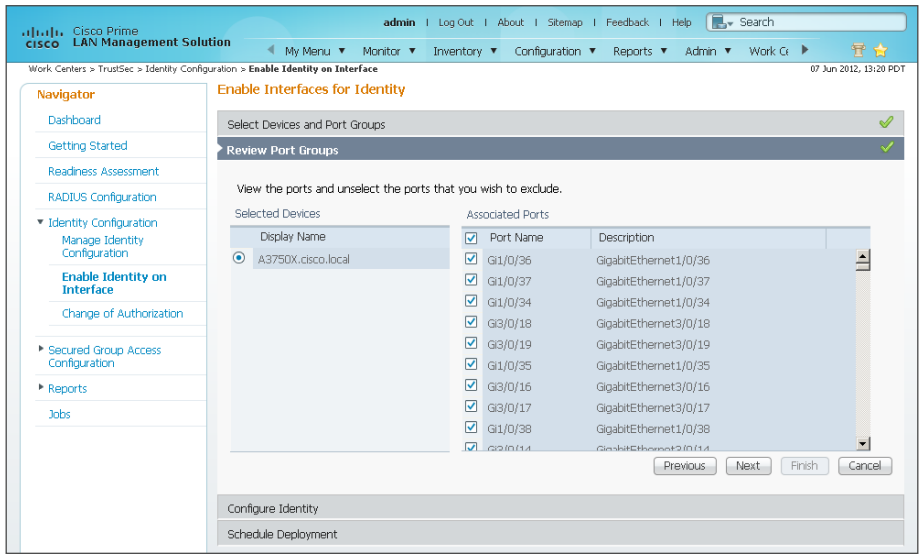
Step 2: In the Navigator pane, click **Enable Identity on Interfaces**.

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**.



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



Next, you configure monitor mode.

Step 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.

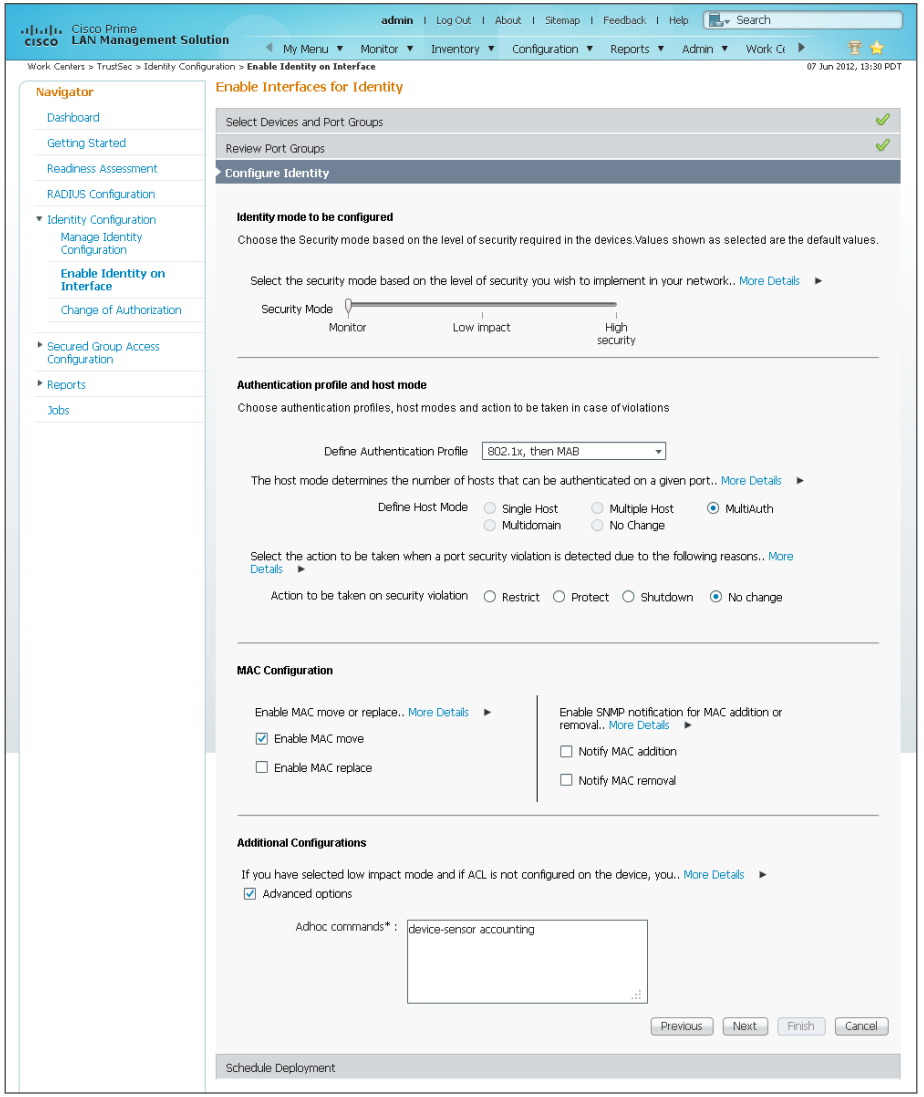
Step 9: In the Additional Configurations section, select **Advanced Options**.

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

```
device-sensor accounting
```

Tech Tip

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.

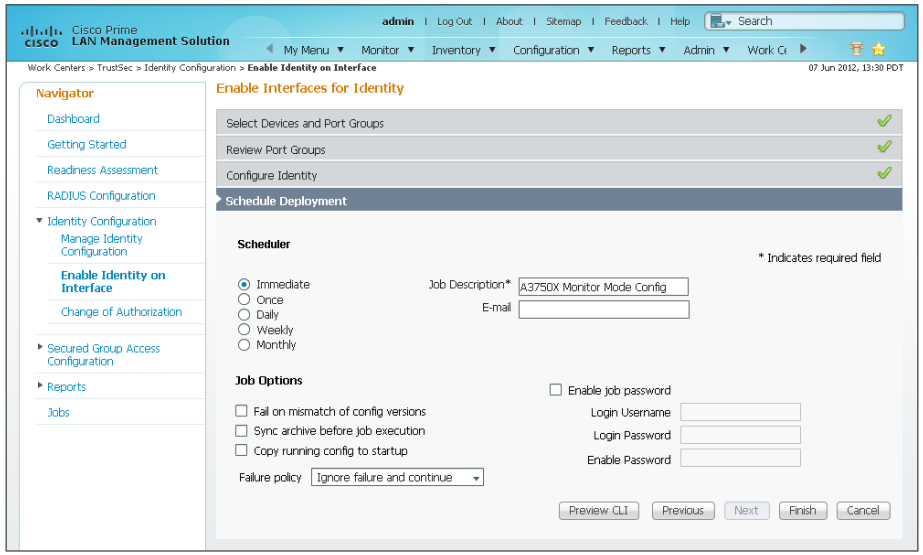


Identity configuration is complete. Next, you create a deployment job in order to deliver the configuration to the switch.

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**.



The global 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 pre-defined groups or by model.

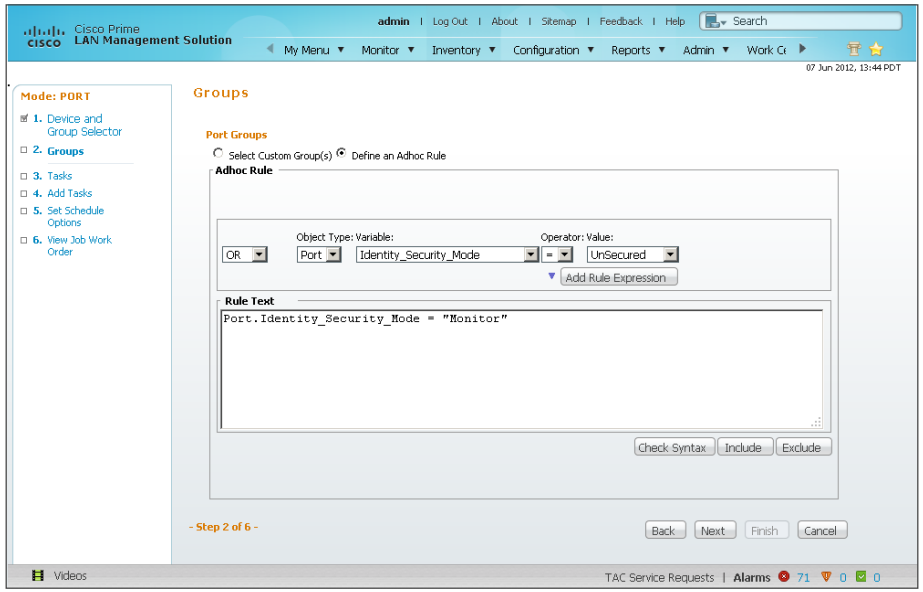
Step 6: Select **Define an Ad-Hoc Rule**. A new screen is displayed.

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**.

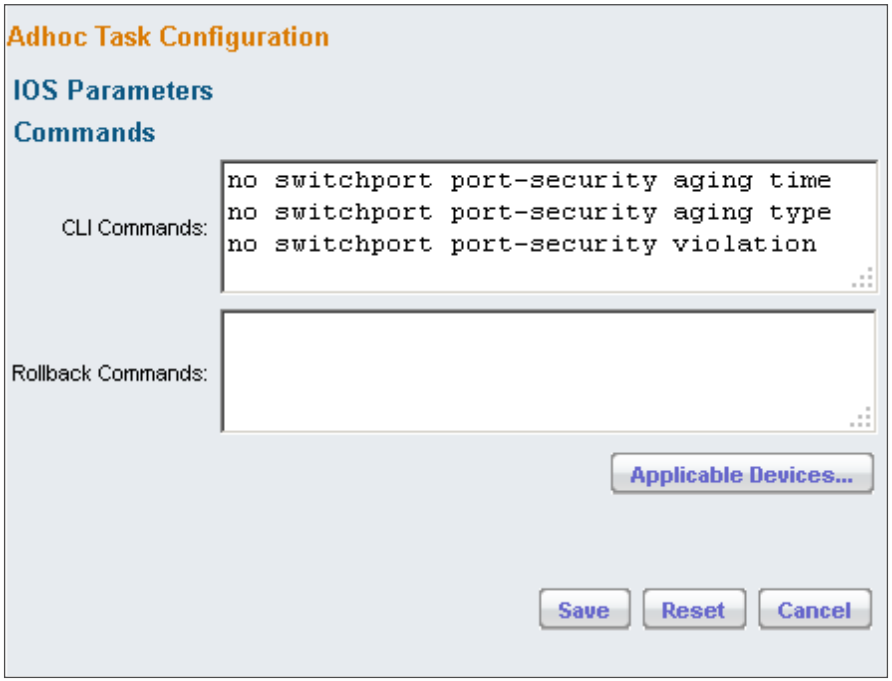


Step 11: In the Task Selector, select **Adhoc Task**, and then click **Next**.

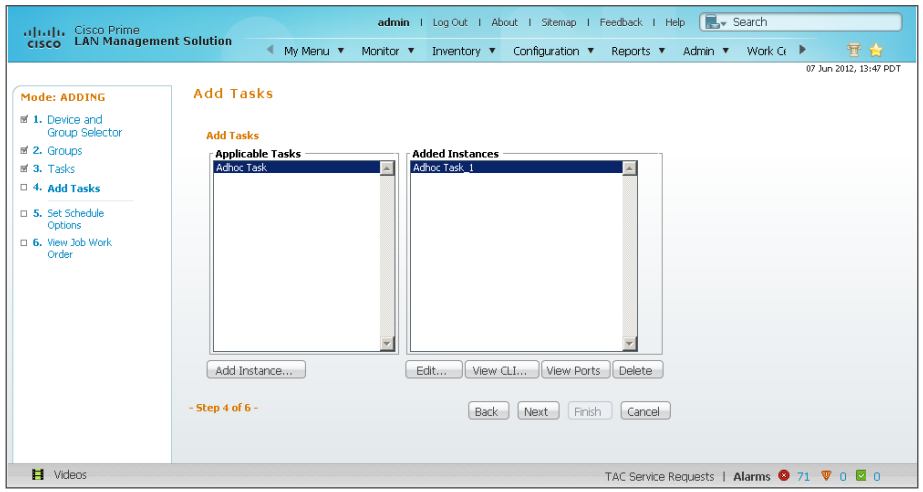
Step 12: Click **Add Instance**, and then, in the new window, enter the CLI commands necessary to remove the port security configuration.

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

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



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



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

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

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

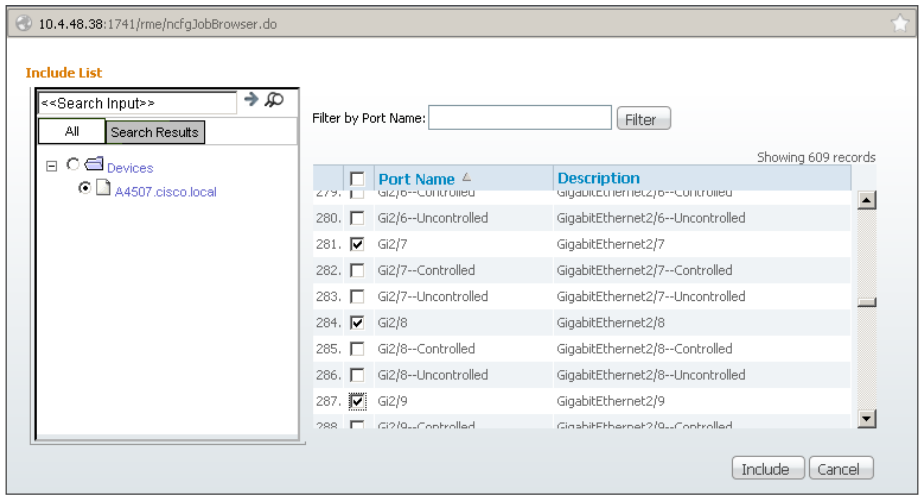
In this example, only one switch is being configured, but you can select multiple switches to accommodate a large deployment. The Group Selector allows you to choose switches by pre-defined groups or by model.

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.



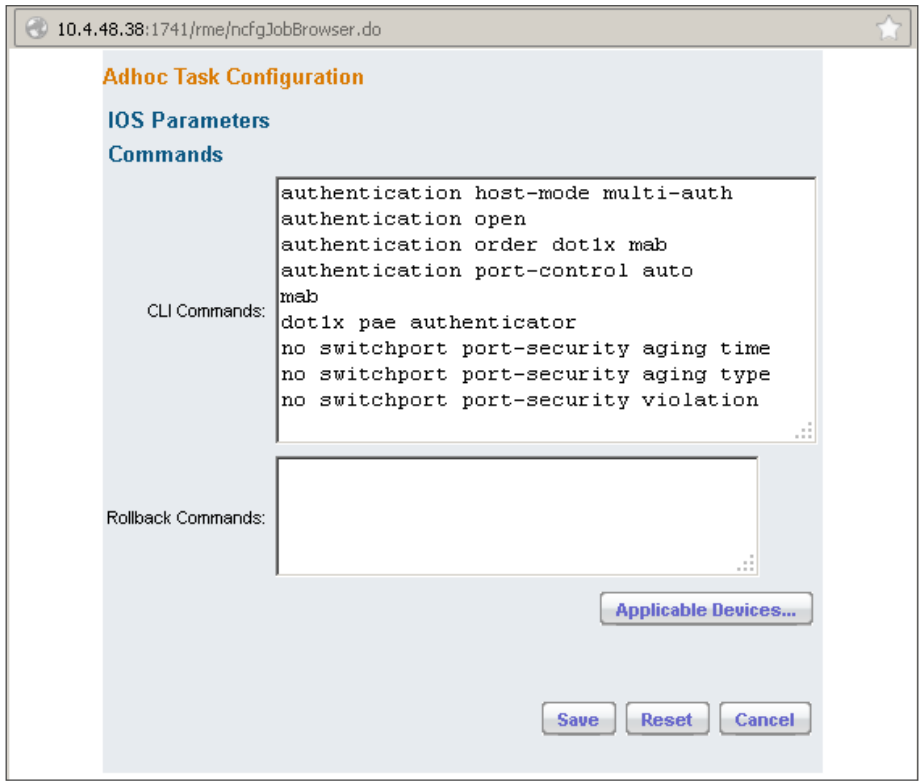
Step 21: Move to step 3 of the wizard by clicking **Next**.

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

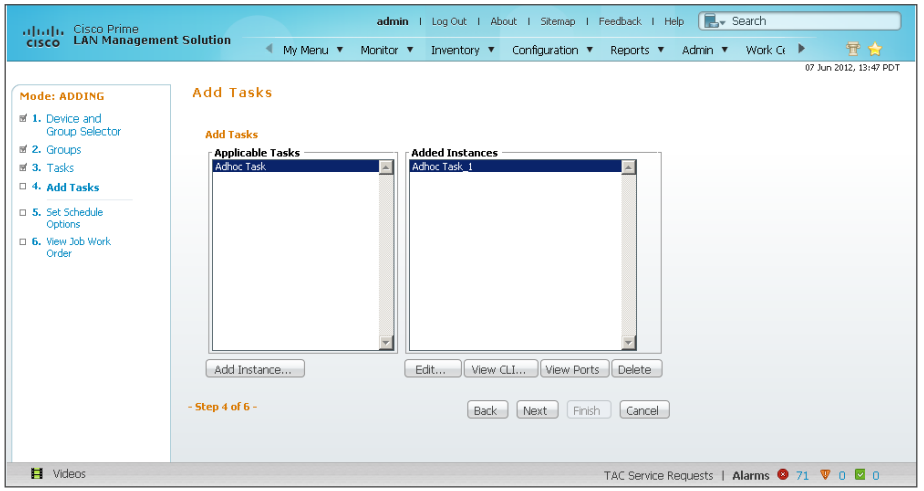
Step 23: Click **Add Instance**, and then, in the new window, enter the CLI commands necessary in order to enable monitor mode and remove the port security configuration.

```
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**.



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



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

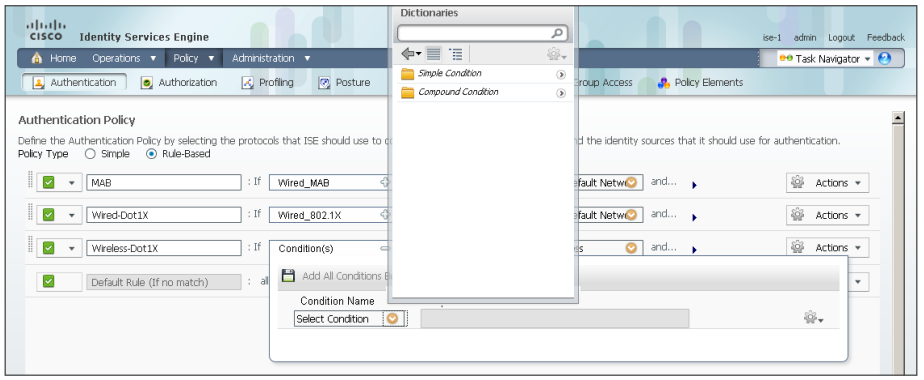
To differentiate wireless users in the authentication logs, create a rule to identify when wireless users authenticate.

Step 1: On the ISE console, Navigate to **Policy** > **Authentication** to open the Authentication Policy page.

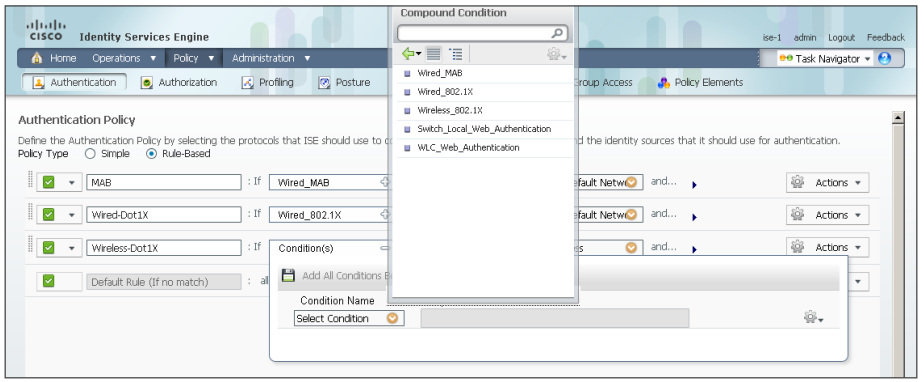
Step 2: For the Default Rule, click the **Actions** button, and then choose **Insert new row above**. A new rule, Standard Policy 1, is created.

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**.

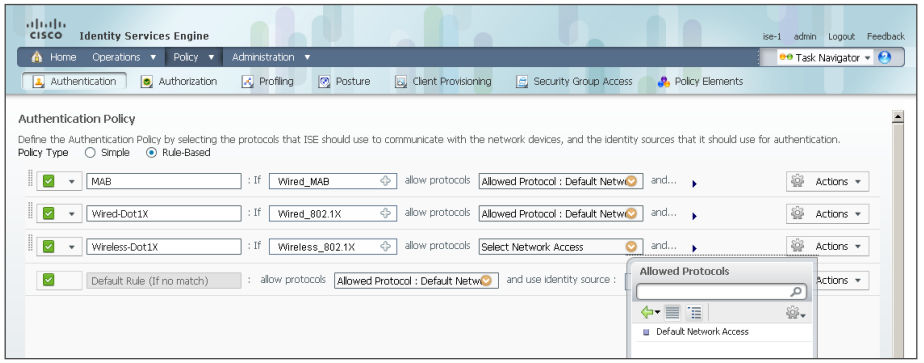
Step 4: In the **Select Condition** list, next to **Compound Condition**, click the > symbol.



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



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

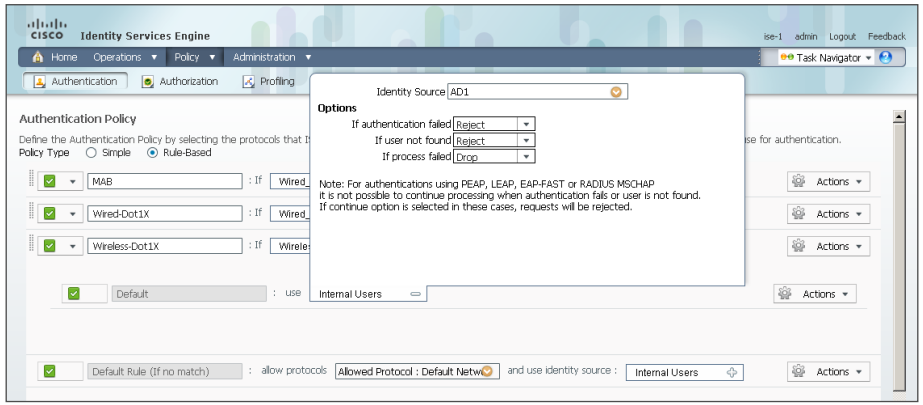


Step 7: For the **Wireless-Dot1X** rule, to the right of **and...**, click the black triangle. This displays the identity store used for this rule.

Step 8: Next to **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**.



Procedure 2 Disable EAP-TLS on Cisco ISE

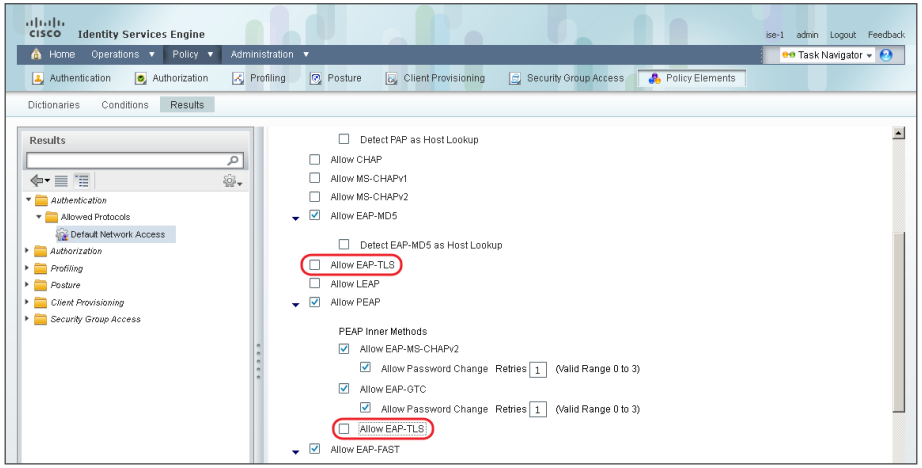
For wireless deployments that aren't currently using digital certificates, you need to disable EAP-TLS in order to allow clients to log in. You will be deploying digital certificates in a later phase of this deployment.

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

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

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

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



Procedure 3 Add ISE as RADIUS authentication server

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

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

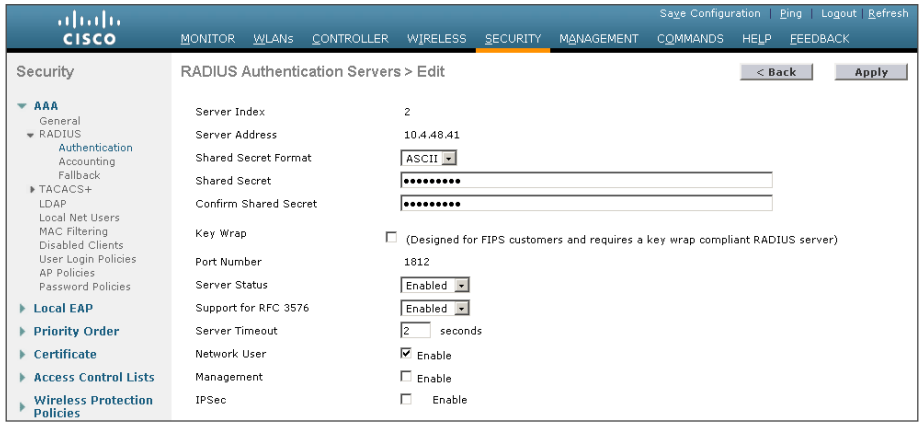
Step 2: On the menu bar, click **Security**.

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**.

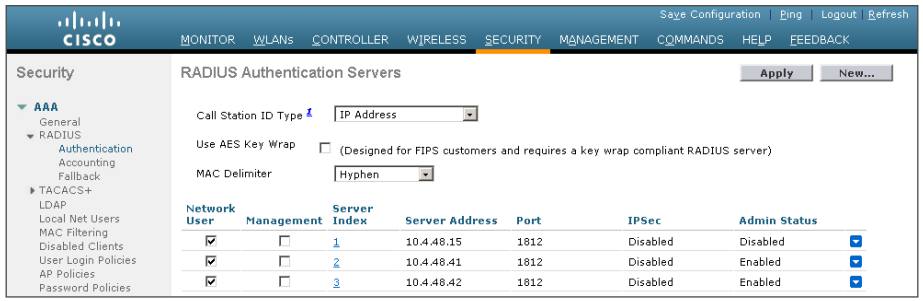


Step 7: Repeat Step 4 through Step 6 in order to add the secondary engine, 10.4.48.42, to the WLC configuration.

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**.



Procedure 4 Add ISE as RADIUS accounting server

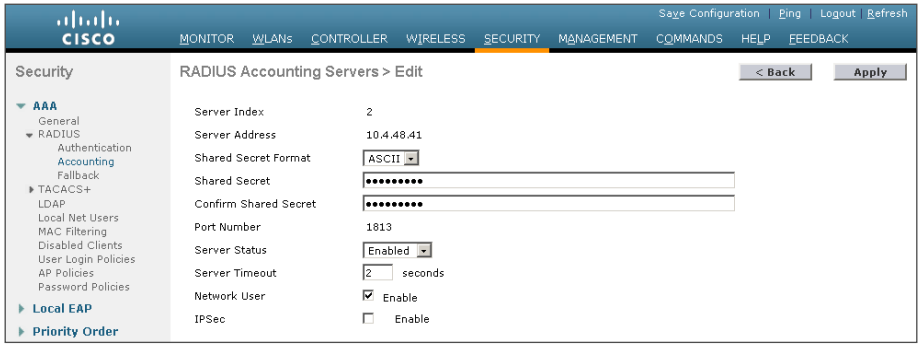
Perform this procedure for every wireless LAN controller (WLC) in the architecture, with the exception of the guest WLC in the DMZ.

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.

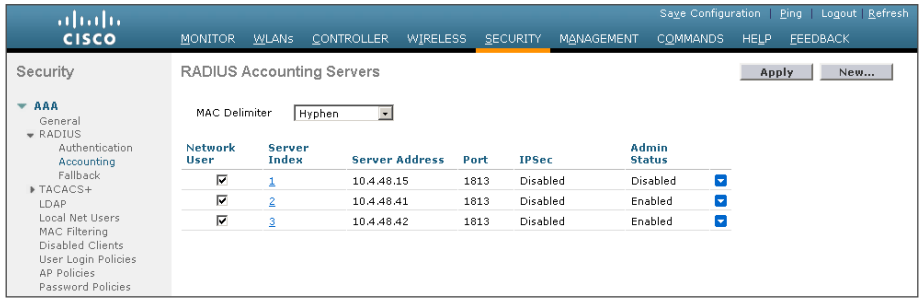
Step 4: In the **Server IP Address** box, enter **10.4.48.41**, enter your RADIUS shared secret, and then click **Apply.**



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

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

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



Procedure 5 Enable client profiling

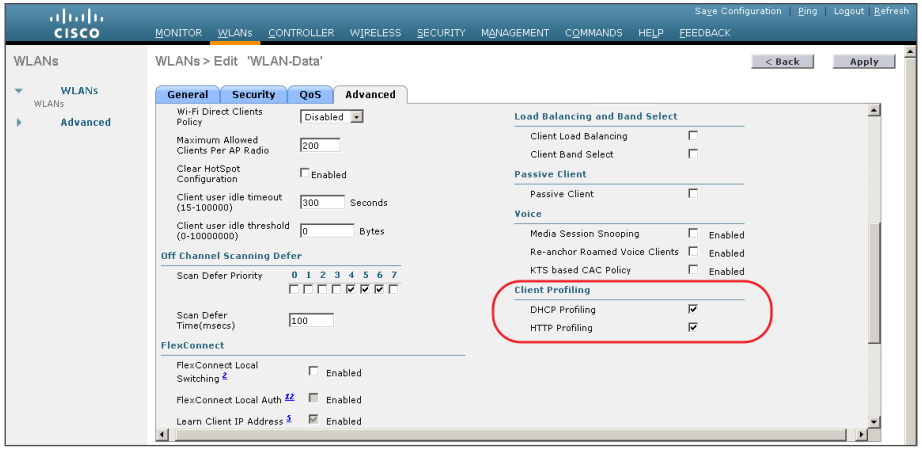
You need to enable DHCP profiling on the WLC in order to send DHCP and HTTP information to the engine for endpoint profiling.

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.

Procedure 1 Create authorization profile

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

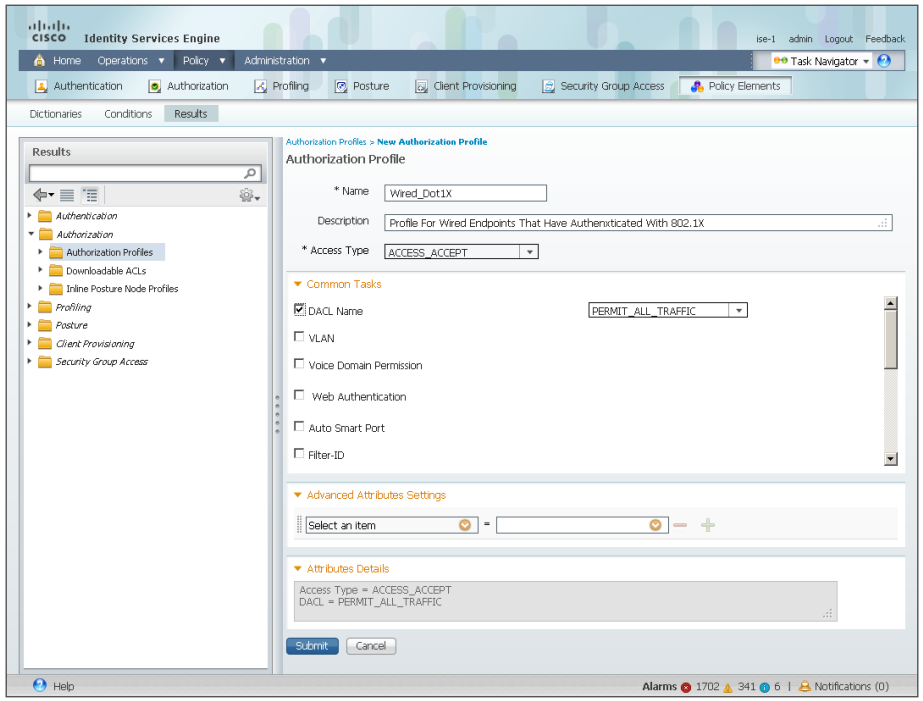
Step 1: On the ISE console, in the menu bar, mouse over **Policy**, and then in the Policy Elements section, choose **Results**.

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**.

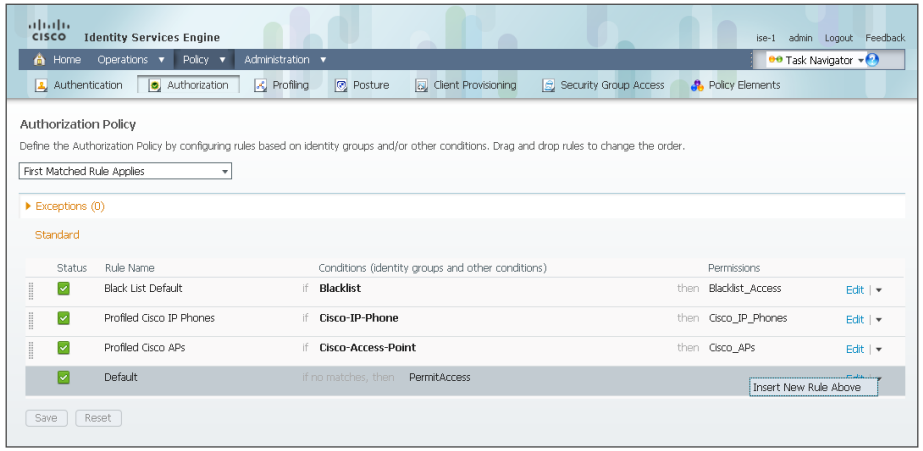


Procedure 2 Create authorization policy

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.

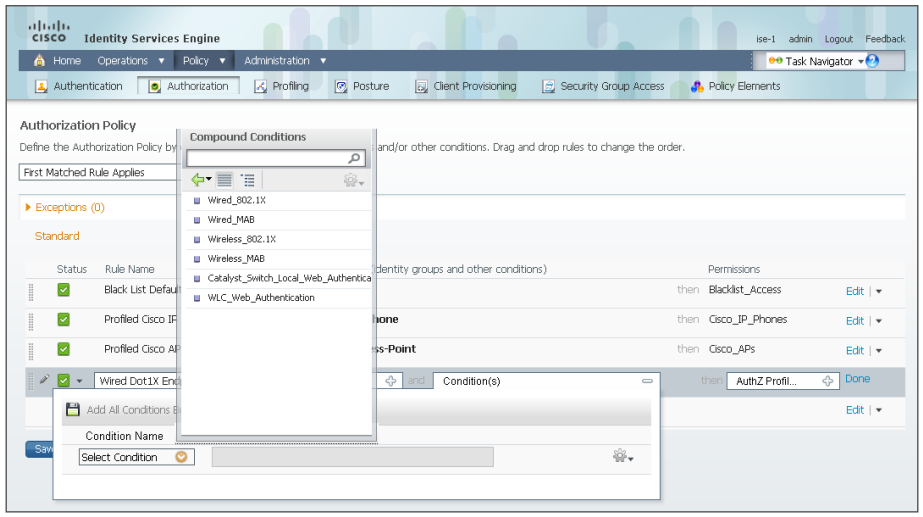


Step 3: Rename the rule **Wired Dot1X Endpoints**.

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

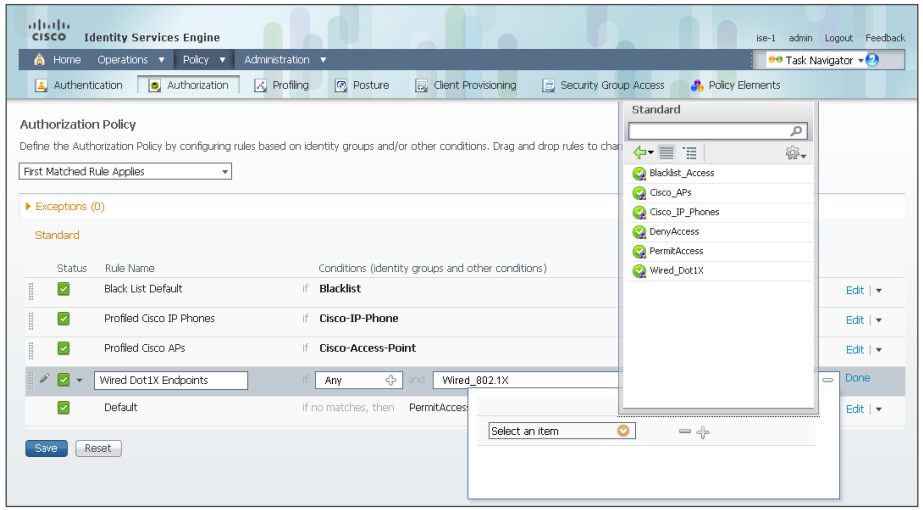
Step 5: Click **Select Existing Condition from Library**.

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

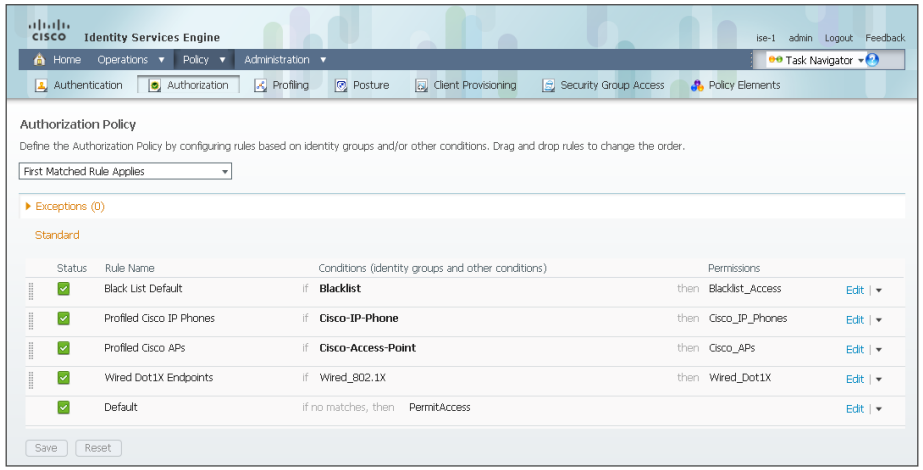


Step 7: Under the Permissions column, next to AuthZ Profile, click the **+** symbol.

Step 8: In the list, next to Standard, click the **>** symbol, and then choose **Wired_Dot1X**.



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



Procedure 3 Enable low-impact mode

You will now configure the switches for low-impact mode 802.1X using Cisco Prime LMS 4.2 and the Cisco TrustSec Work Center. You need to create an access list to limit what traffic is permitted on a port before it is authenticated. You 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.

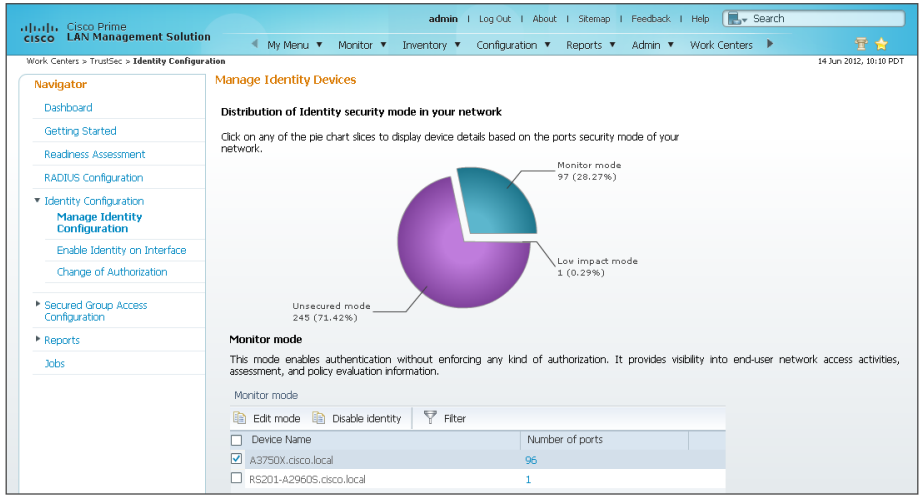
Step 1: Connect to Cisco Prime LMS with a web browser, for example: https://lms.cisco.local.

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

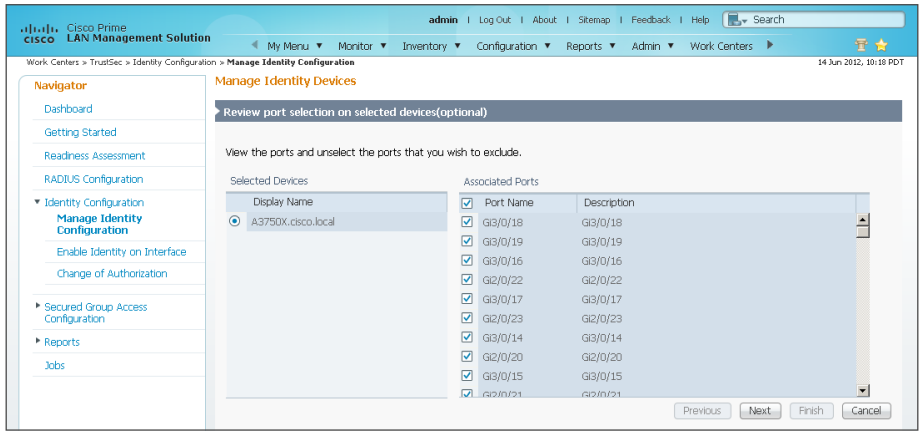
Step 3: In the Navigator panel on the left, click **Manage Identity Configuration**.

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**.



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:

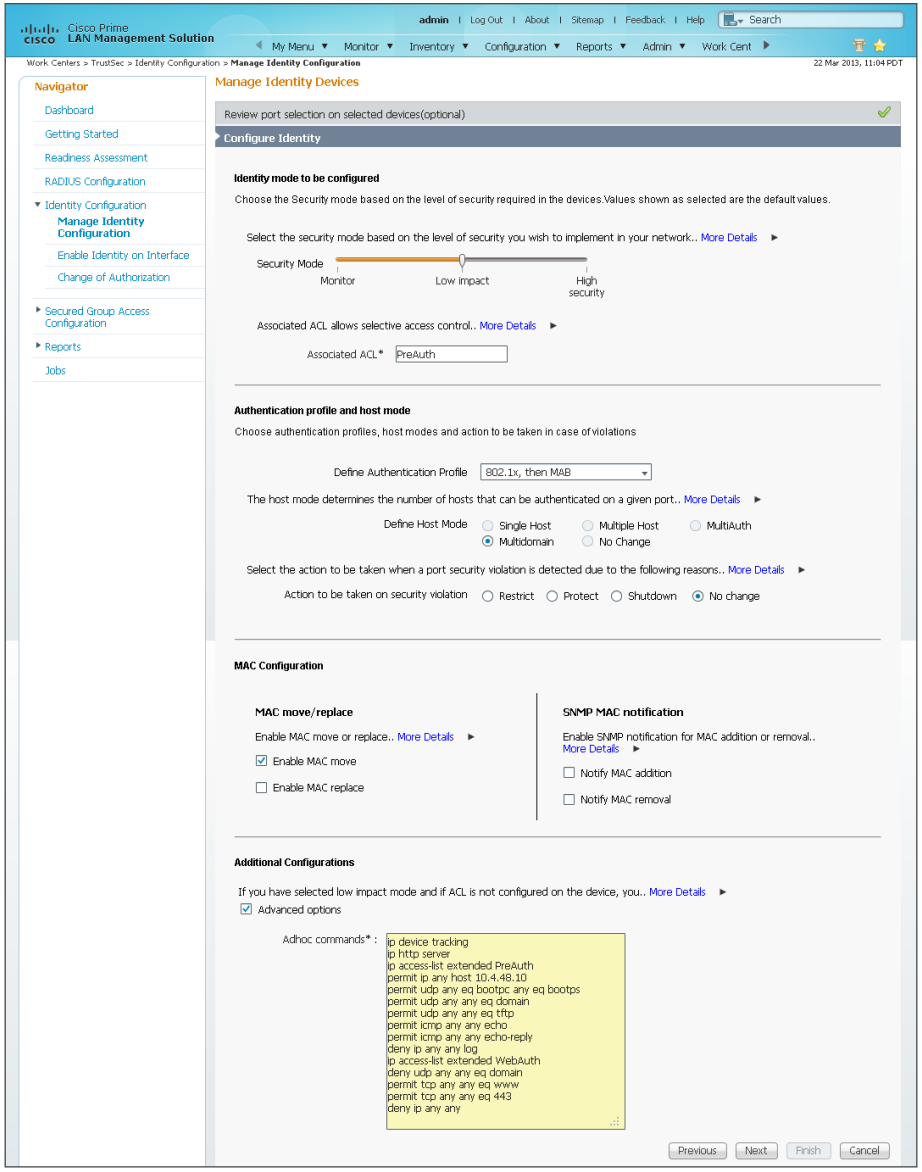
- Define Authentication Profile—**802.1X, then MAB**
- Define Host Mode—**Multidomain**
- Action to be taken on security violation—**No Change**

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 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
```



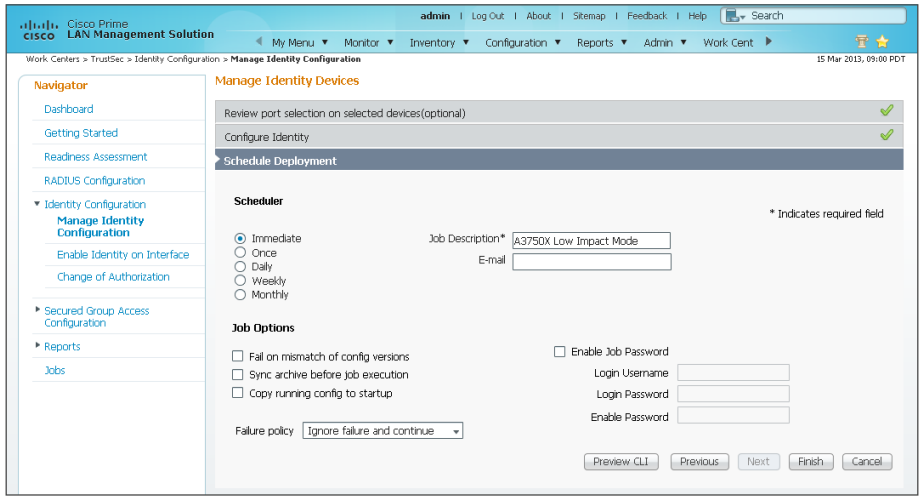
Tech Tip

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 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**.



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

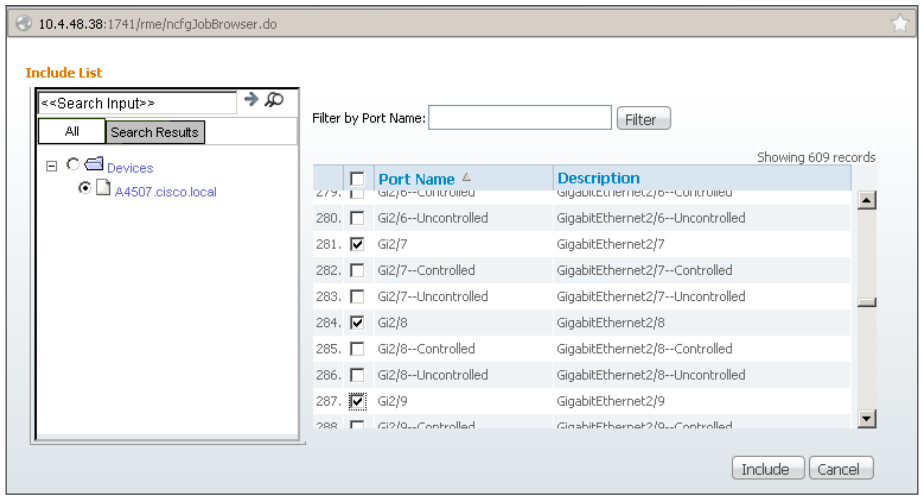
In this example, only one switch is being configured, but you can select multiple switches to accommodate a large deployment. The Group Selector allows you to choose switches by pre-defined groups or by model.

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.



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

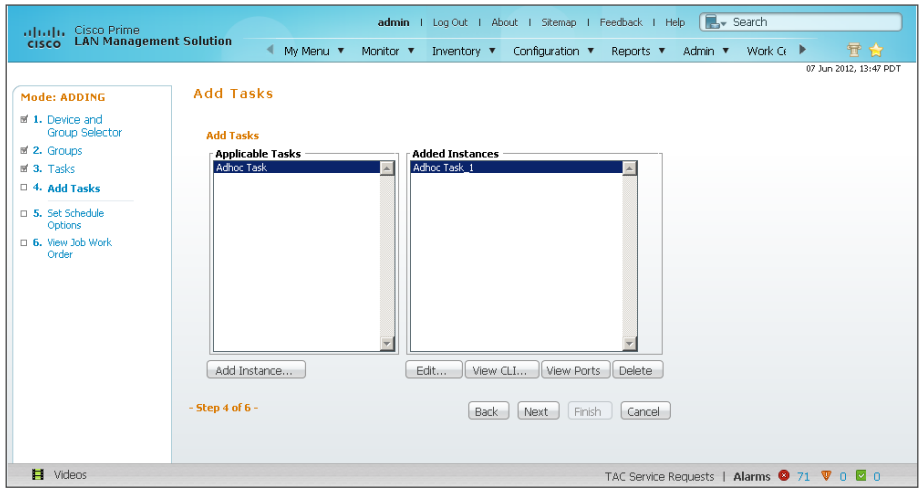
Step 22: In the Task Selector, select **Adhoc Task**, and then click **Next**.

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**.

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



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.

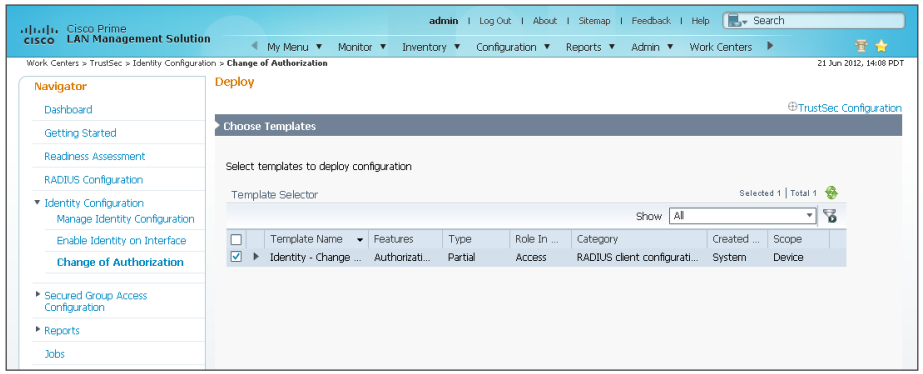
Procedure 5 Enable change of authorization

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**.

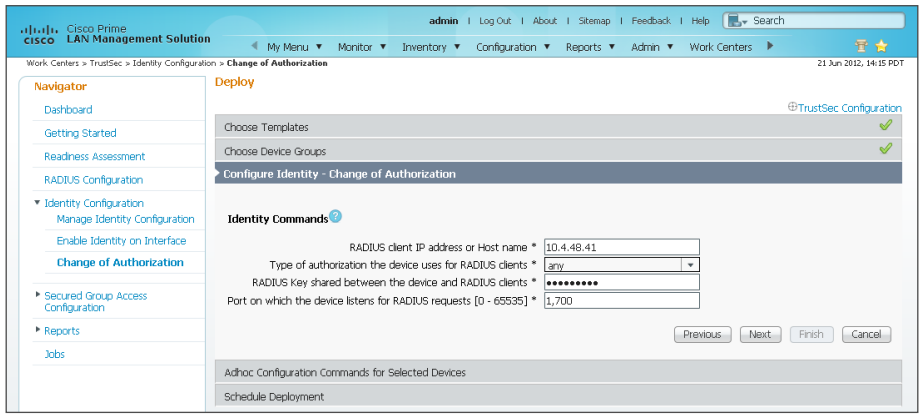
Step 2: In the Navigator panel on the left, click **Change of Authorization**.

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



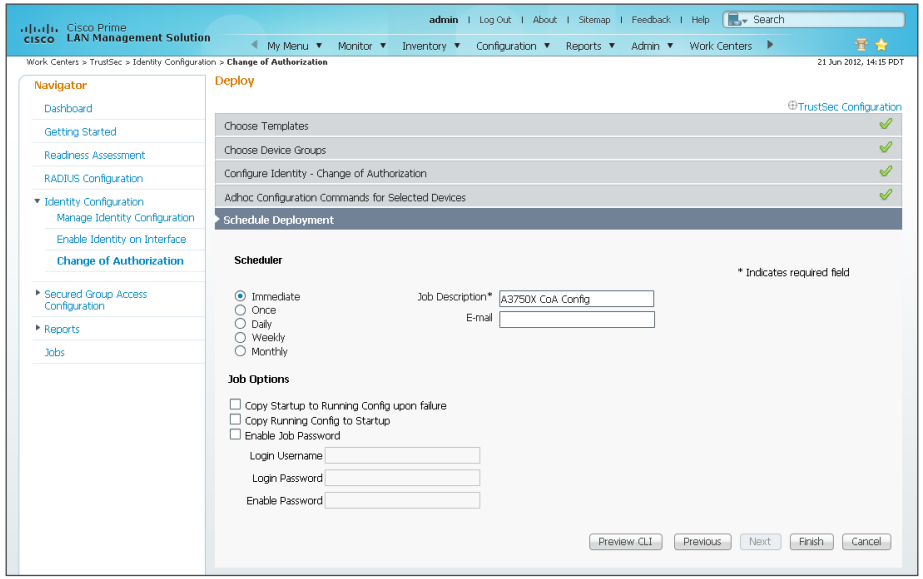
Step 4: In the Device Selector, expand **All Devices**, select the switches you want to enable for CoA, and then click **Next**.

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



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

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



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

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

```
aaa server radius dynamic-author
  client 10.4.48.41 server-key [key]
  client 10.4.48.42 server-key [key]
  auth-type any
```

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.

Process

Enabling Authorization for Wireless Endpoints

1. Configure WLC for authorization

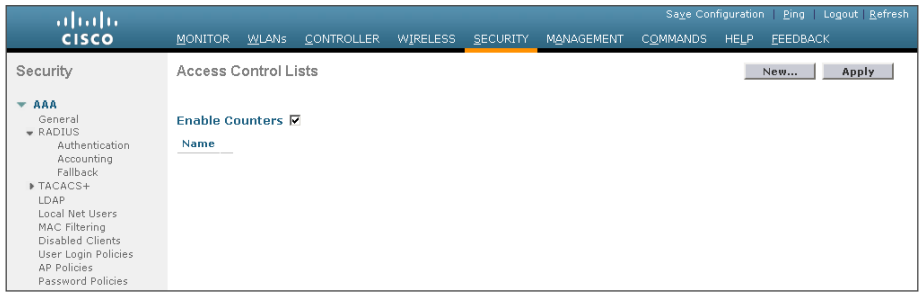
Procedure 1 Configure WLC for authorization

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**.

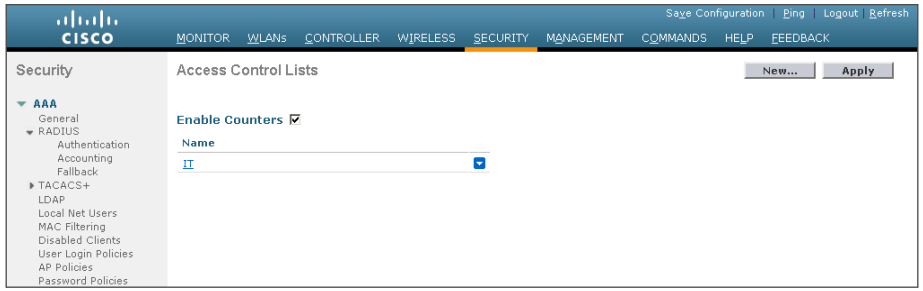
Step 3: In the left pane, expand **Access Control Lists**, and then click **Access Control Lists**.



Step 4: Click **New**.

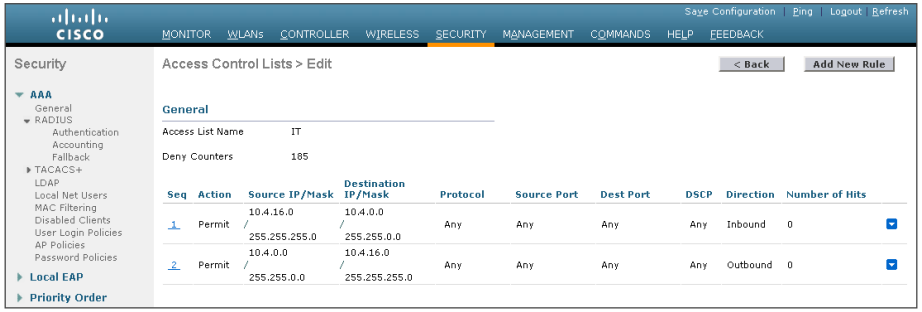
Step 5: Name the access list, and then click **Apply**.

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



Step 7: Click **Add New Rule**.

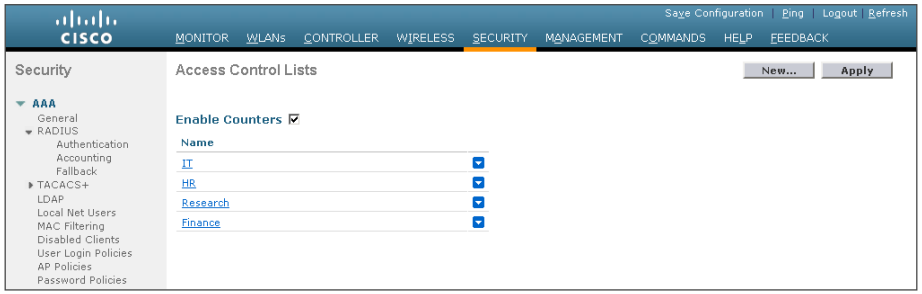
Step 8: Create a new access list rule based on your security policy, and then click **Apply**. In our example deployment, members of the IT group are only allowed access to the internal network (10.4.0.0/16) from their personal devices.



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.

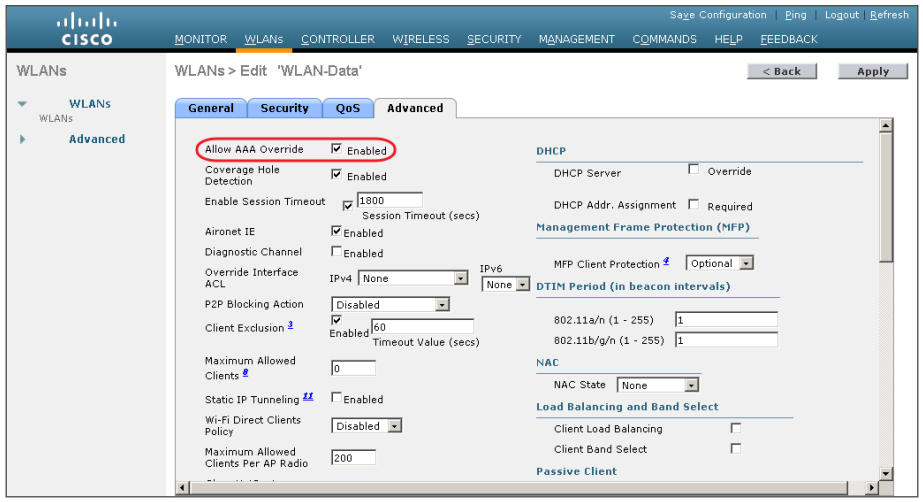


Next, you enable the WLC to allow Cisco ISE to use RADIUS to override the current settings, so that the access list can be applied to the wireless LAN.

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**.



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

Process

Enabling Authorization Policy

1. Configure identity groups
2. Create profile to deny BlackBerry phones
3. Create authorization rule
4. Create downloadable access lists
5. Create profiles for user groups
6. Create authorization rules for user groups

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

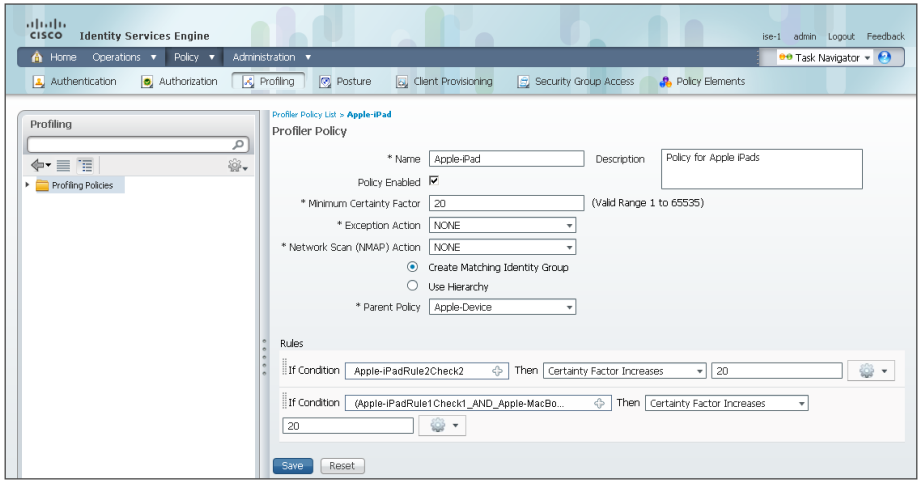
Cisco ISE has more in-depth options to give more details on the devices connecting to the network. To help identify the endpoints, identity groups are used to classify profiled endpoints. You use these identity groups to create authorization policies.

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**.



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.

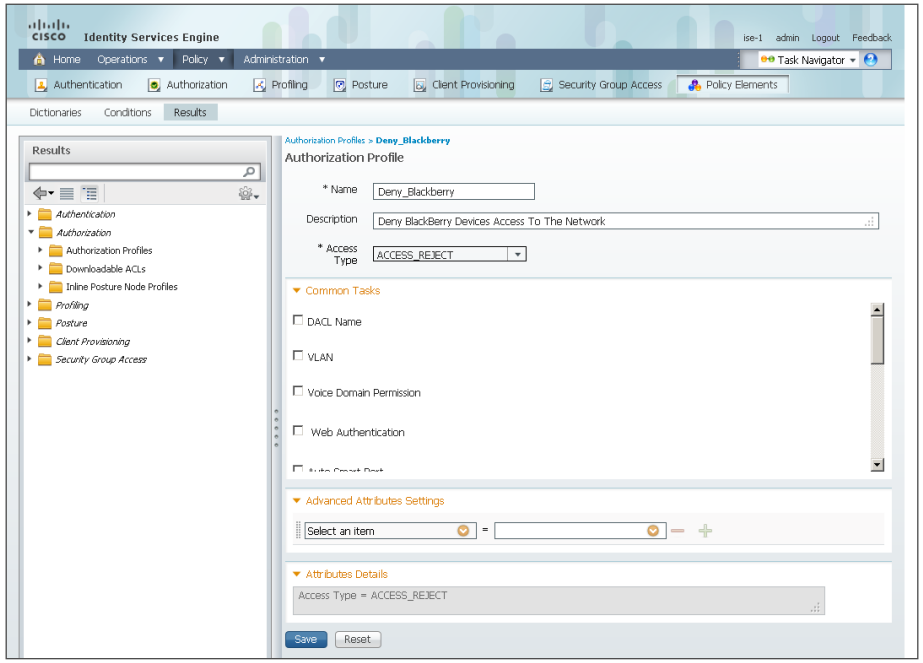
Step 1: On the menu bar, mouse over **Policy**, and then, in the Policy Elements section, choose **Results**.

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**.

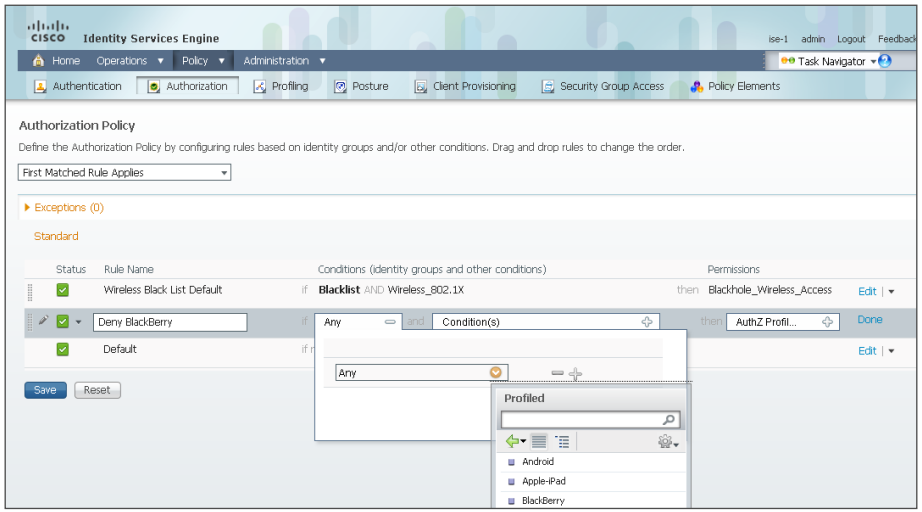
Step 2: At the end of the Default Rule, click the arrow, and then choose **Insert new rule above**. A new rule, "Standard Rule 1," is created.

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**.



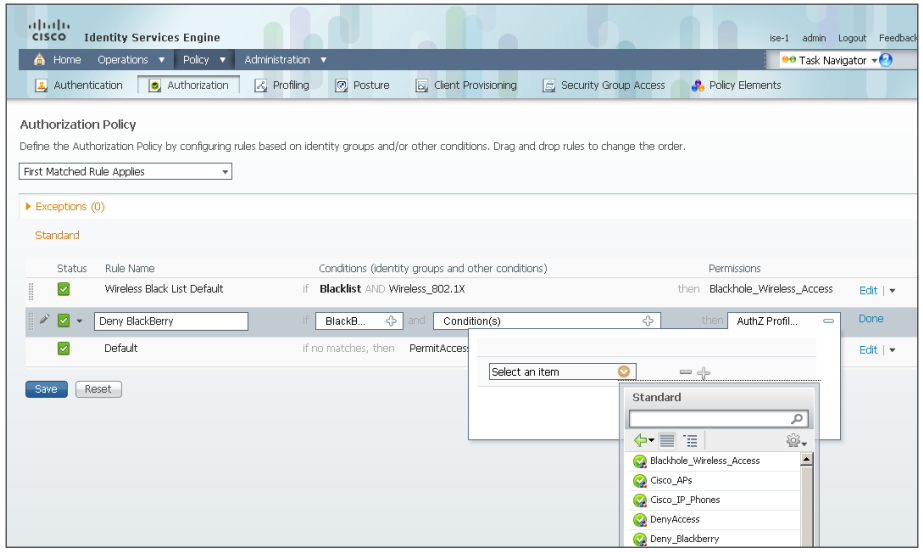
Tech Tip

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."



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**.

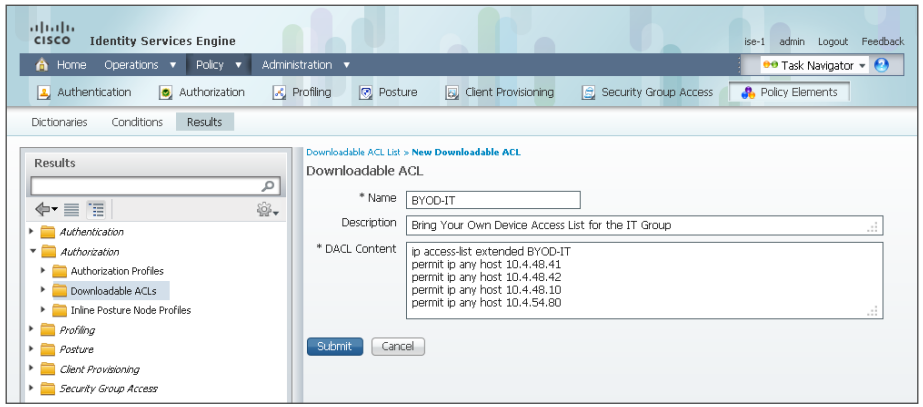
Step 2: In the left pane, double-click **Authorization,** and then select **Downloadable ACLs**.

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**.



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**.

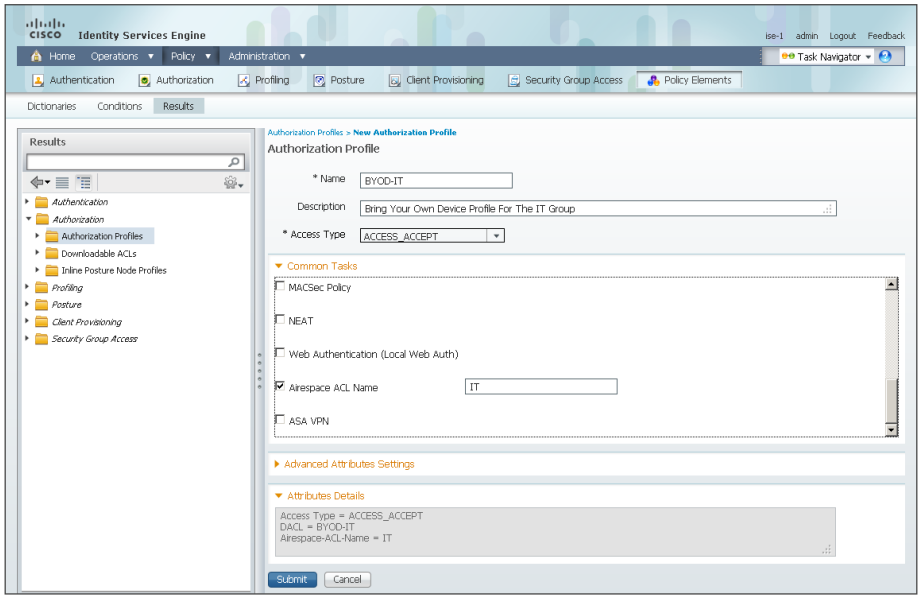
Step 2: In the left pane, double-click **Authorization**, and then select **Authorization Profiles**.

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.



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.

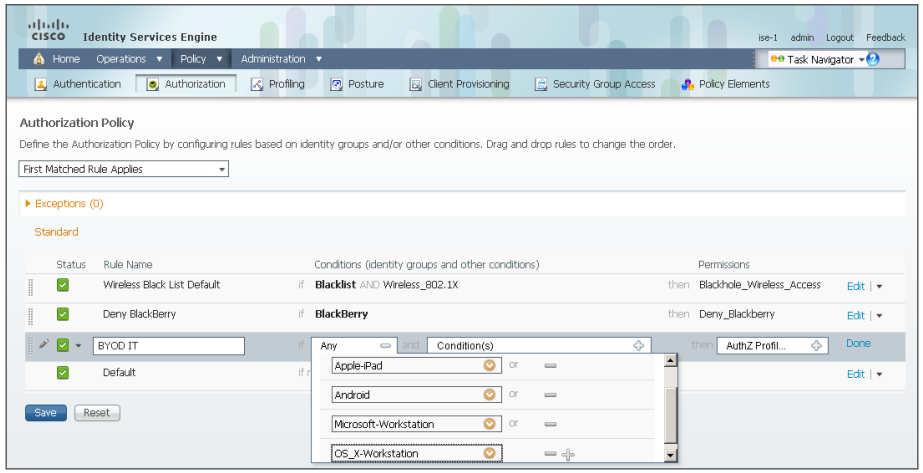
Step 11: In the list, next to Endpoint Identity Groups, choose the > symbol.

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**.

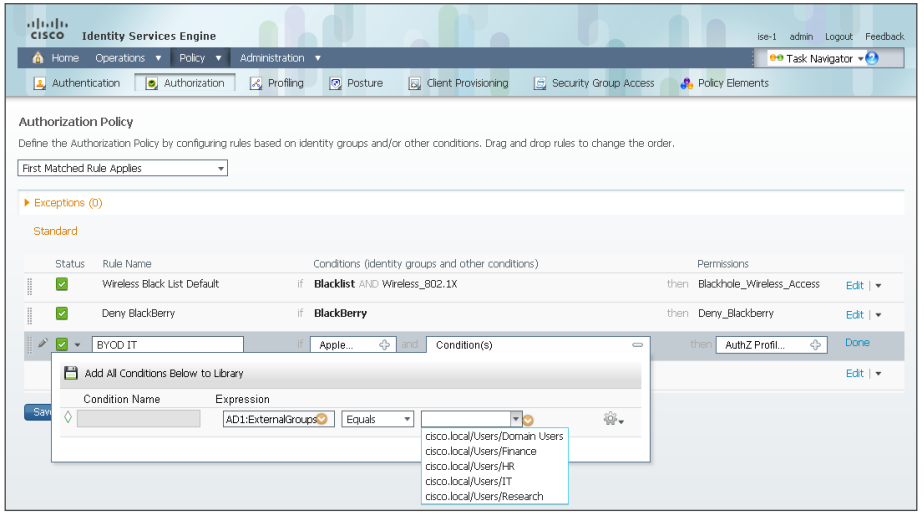


Step 16: In the **Condition(s)** list, click the **+** symbol, and then click **Create New Condition (Advance Option)**.

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**.

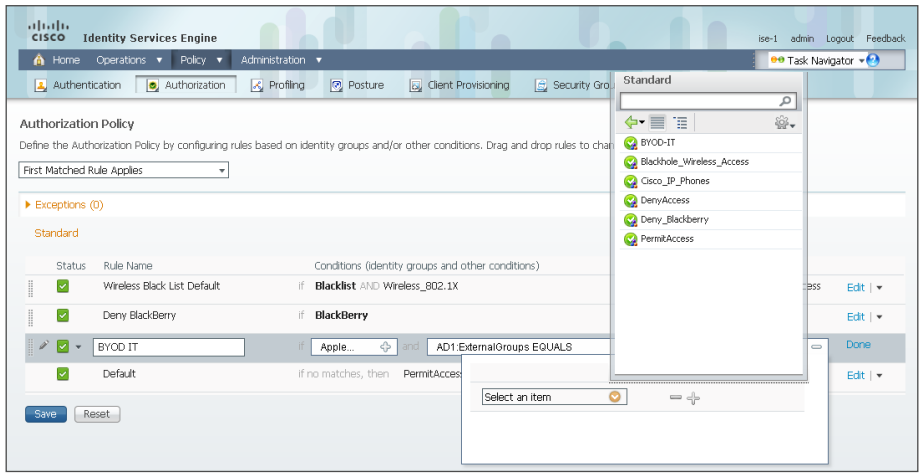
Step 19: In the first drop-down list, choose **Equals**, and then, in the second drop-down list, choose **cisco.local/Users/IT**.



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

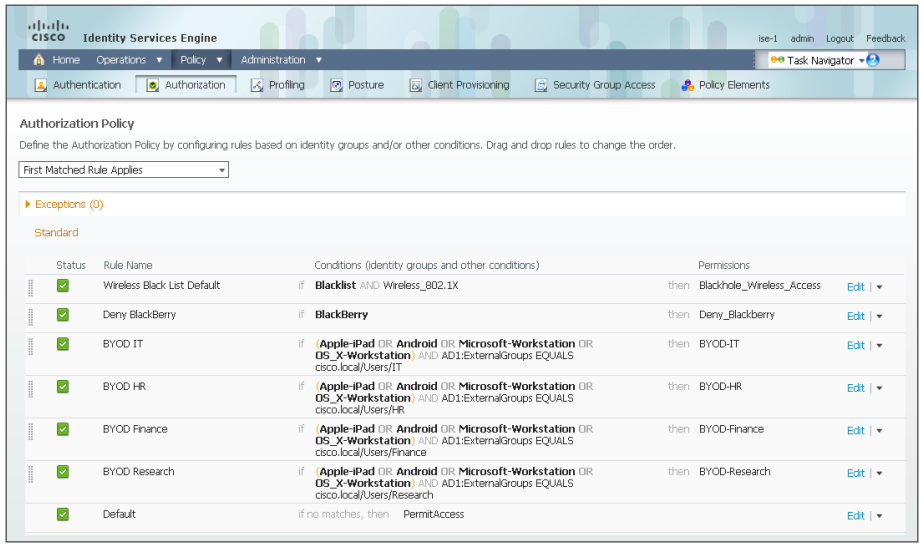
Step 21: In the Select an item list, next to Standard, click the > symbol.

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.



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.

Process

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.

Reader Tip

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

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

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

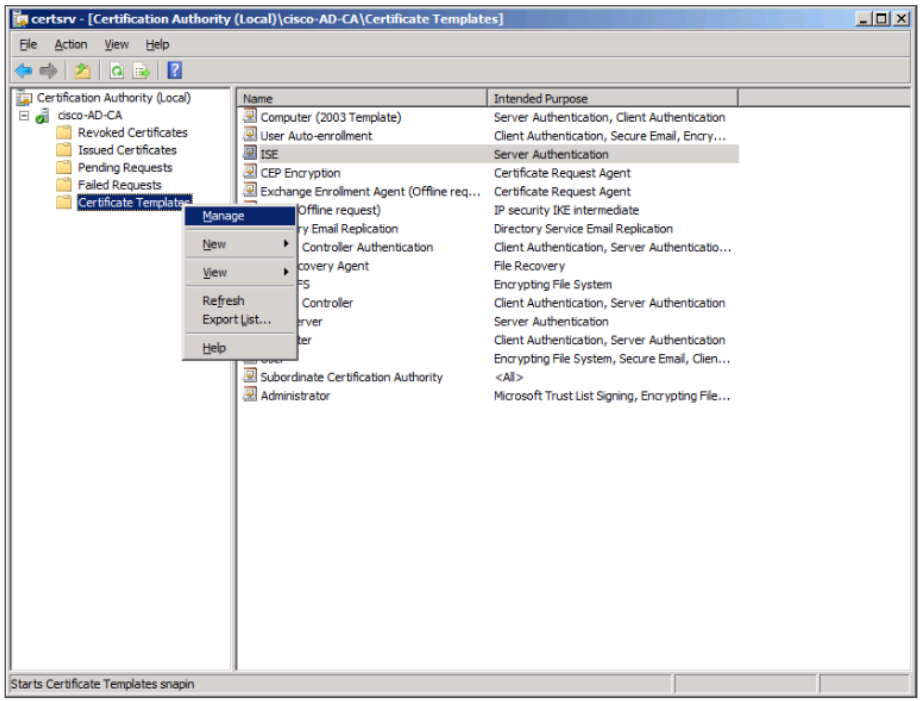
http://support.microsoft.com/kb/2483564

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**.

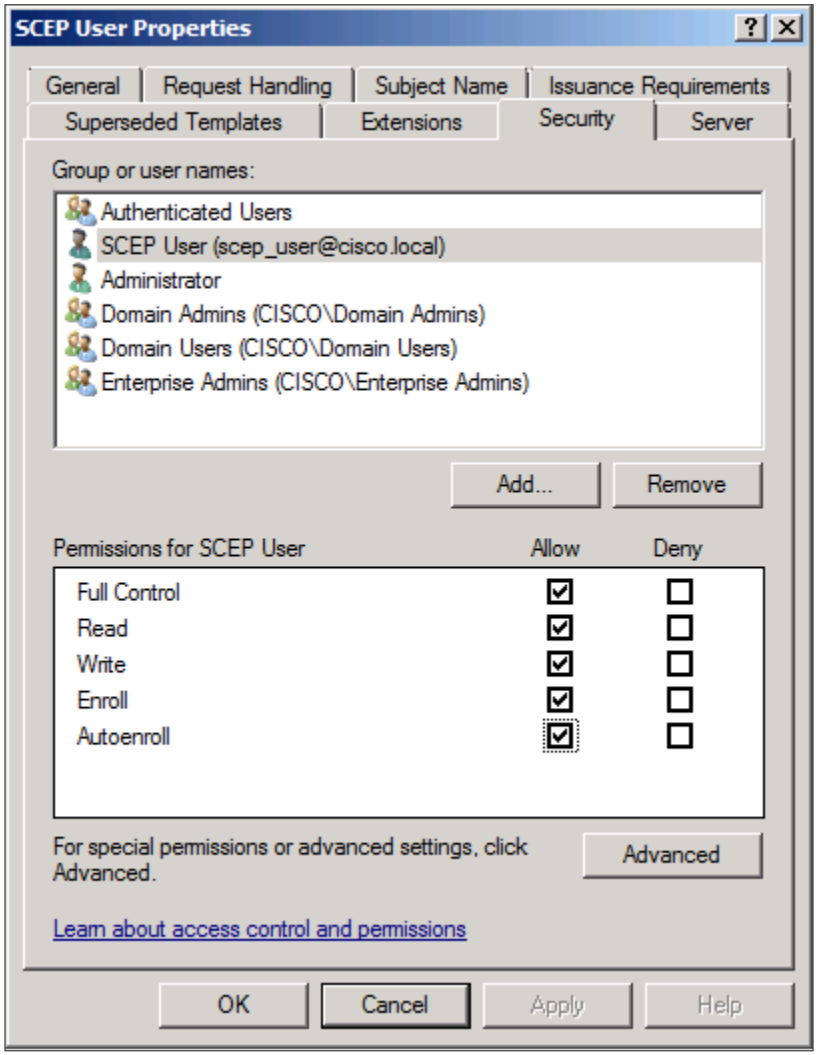
For compatibility with Windows XP, make sure that Windows 2003 Server Enterprise is selected.

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.



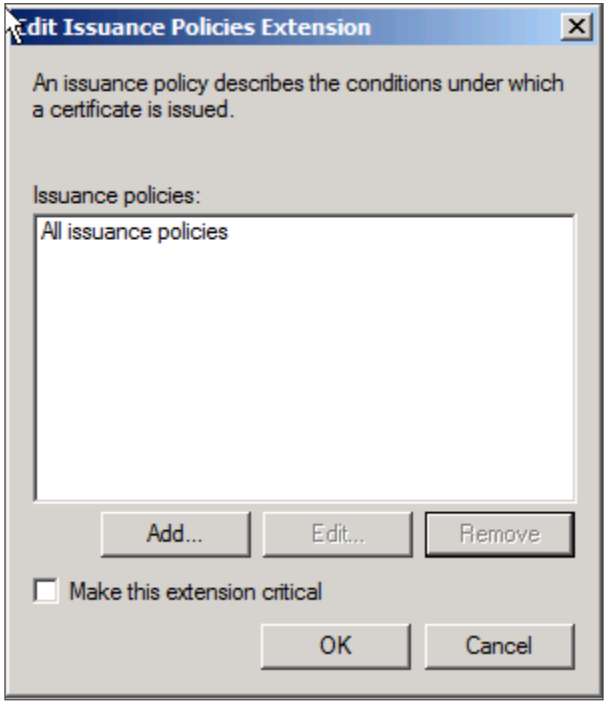
Step 8: On the Subject Name tab, select **Supply in the request**.

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**.

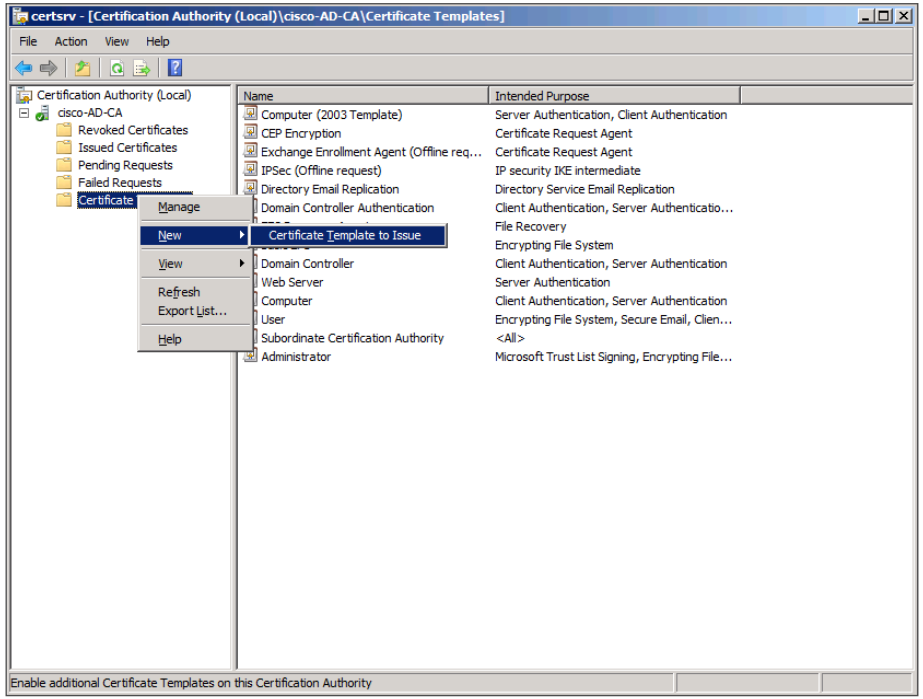


Step 13: Click **OK**.

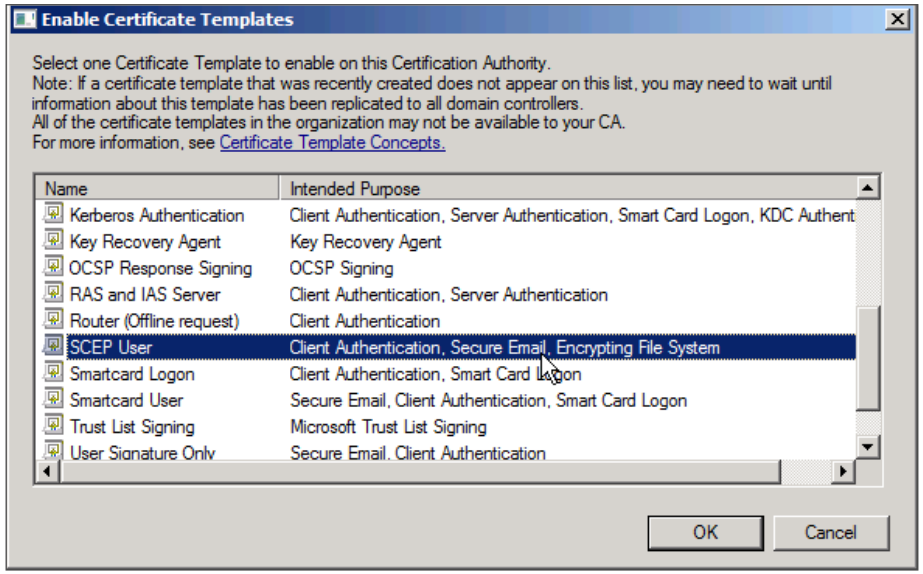
Step 14: Use the defaults for the remaining tabs, click **Apply**, and then click **OK**.

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**.



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



Procedure 3 Edit registry

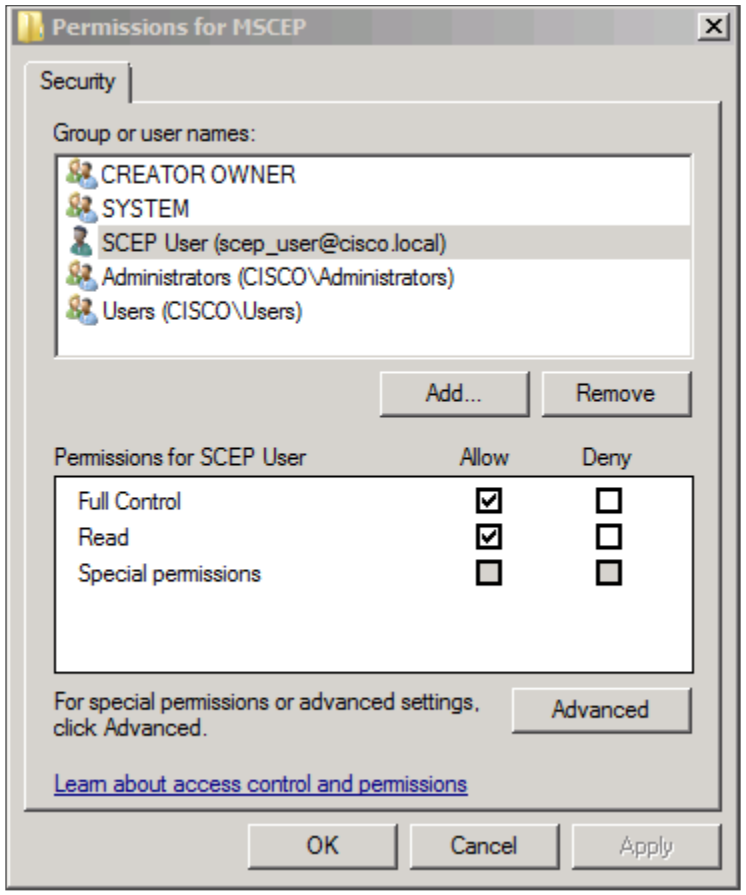
There are a few changes that need to be made to the registry to support auto-enrollment in order to complete the installation.

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**.

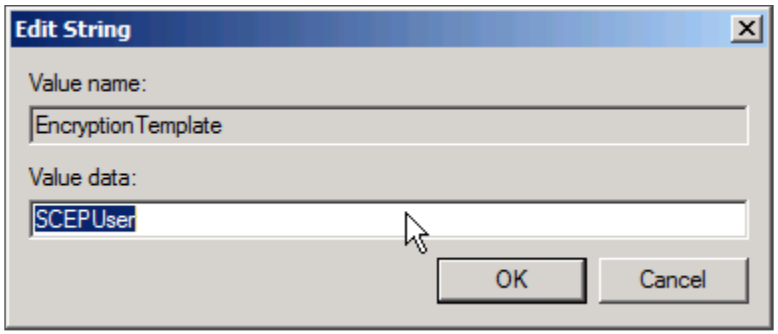
Step 3: Select the user that you created for SCEP during installation, in the Allow section select **Full Control**, and then click **OK**.



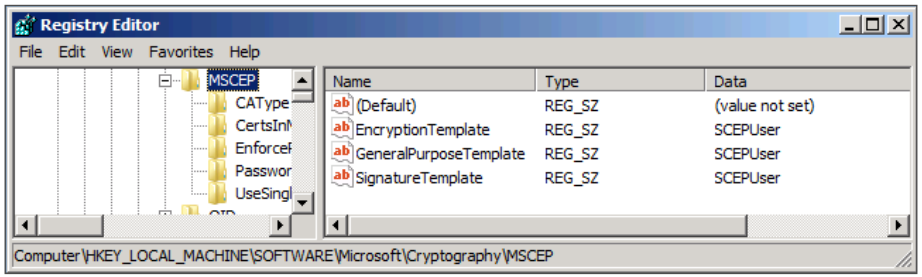
Step 4: There are three values for certificate templates in the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP key that need to point to the template that you created in Procedure 2. Those values are EncryptionTemplate, GeneralPurposeTemplate, and SignatureTemplate.

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**.



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

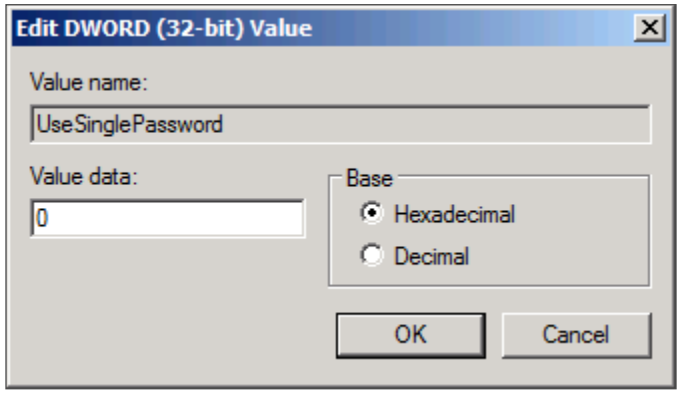


You will need to disable the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\UseSinglePassword key.

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.



Procedure 4 Install trusted root certificate for domain

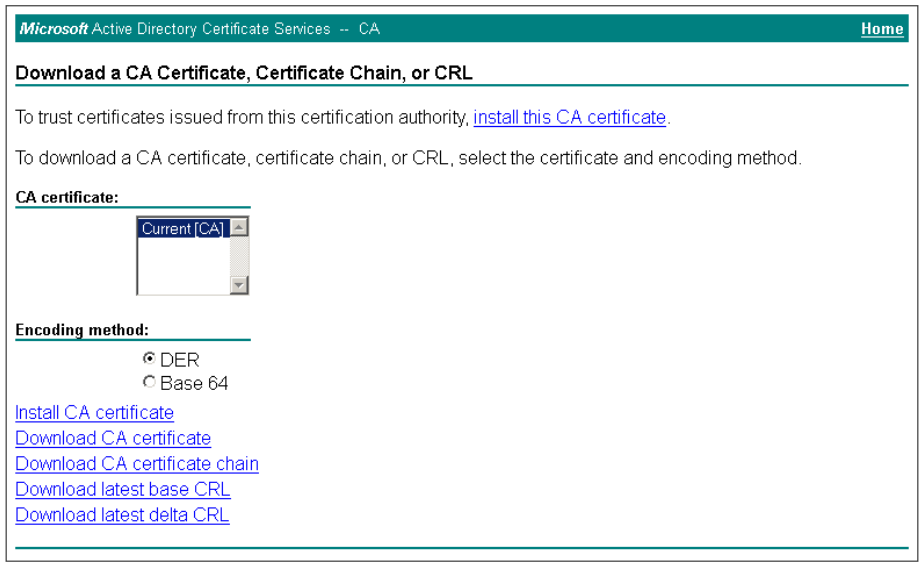
Install a trusted root certificate on the AD controller in order to distribute it to the clients so that certificates from the CA server will be trusted.

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.

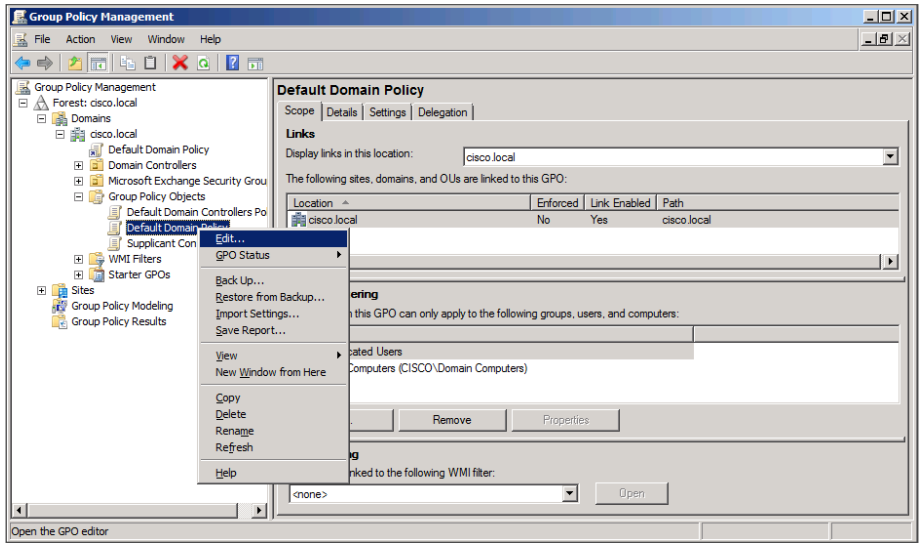
Step 4: Click **Download CA Certificate,** and then save the certificate file on the AD controller.



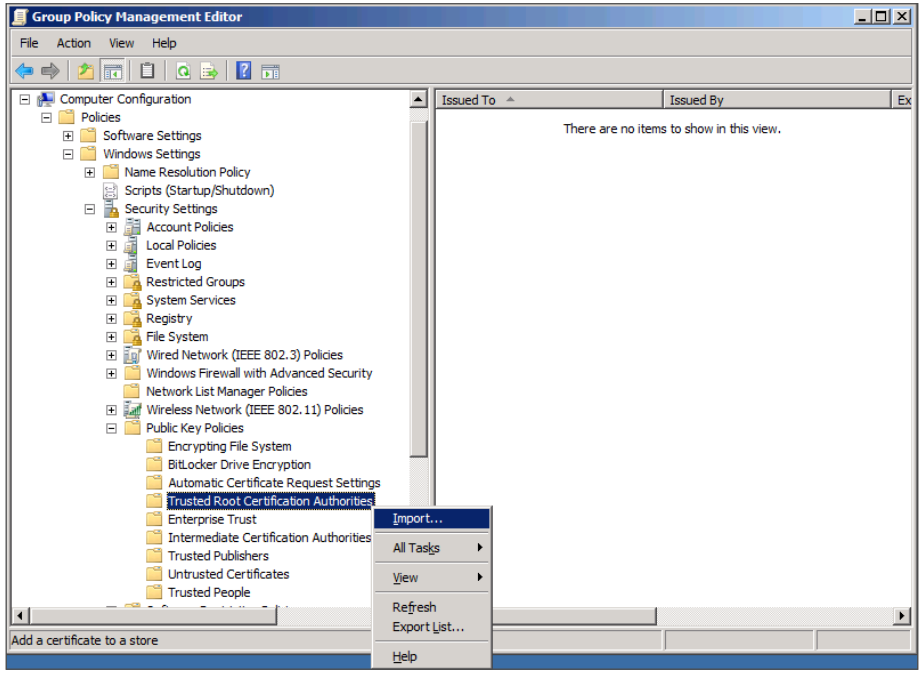
Step 5: On the CA console, navigate to **Start** > **Administrative Tools** > **Group Policy Management**.

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

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

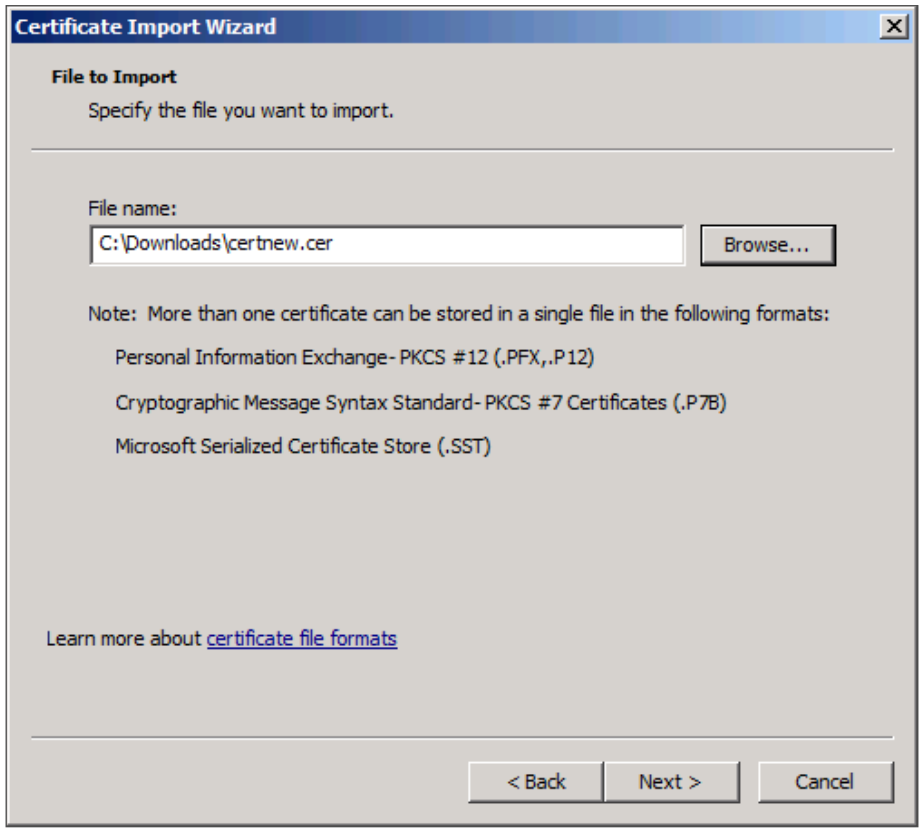


Step 8: Navigate to **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Public Key Policies,** right-click **Trusted Root Certification Authorities,** and then choose **Import**. The Certificate Import Wizard launches.



Step 9: Click **Next**.

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



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

Step 12: Click **Finish.** The certificate imports.

Step 13: Click **OK** to close the wizard.

Procedure 5 Install trusted root on AD server

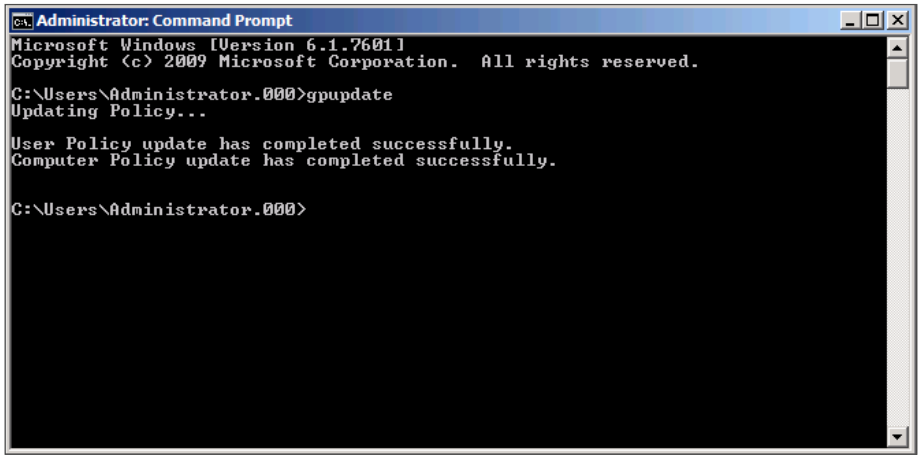
In addition to configuring AD server to distribute the trusted root certificate to workstations, you need to install the certificate directly on the AD server. A group policy object (GPO) update takes care of this automatically. In this procedure, you will force the update to run immediately.

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

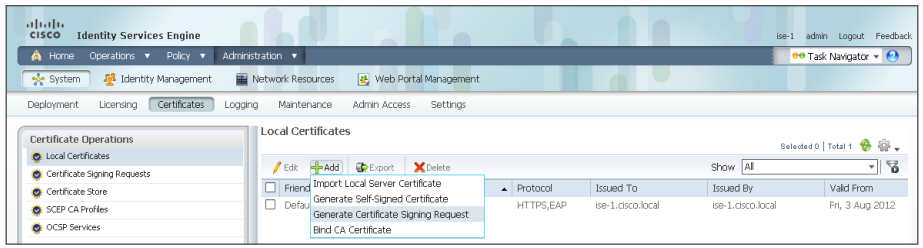
In order to obtain a certificate from the CA, Cisco ISE needs to generate a signing request that will be used by the CA to generate a certificate.

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

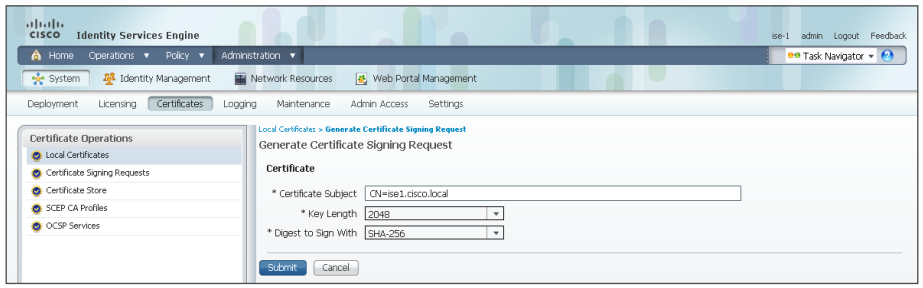
Step 2: Mouse over **Administration**, and then, from the System section of the menu, choose **Certificates**.

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

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

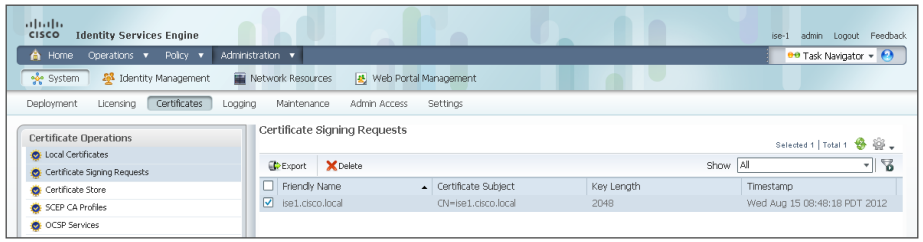


Step 5: In the **Certificate Subject** box, after the "CN=", enter the fully qualified domain name (FQDN) of the Cisco ISE server, and then click **Submit**.



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

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



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

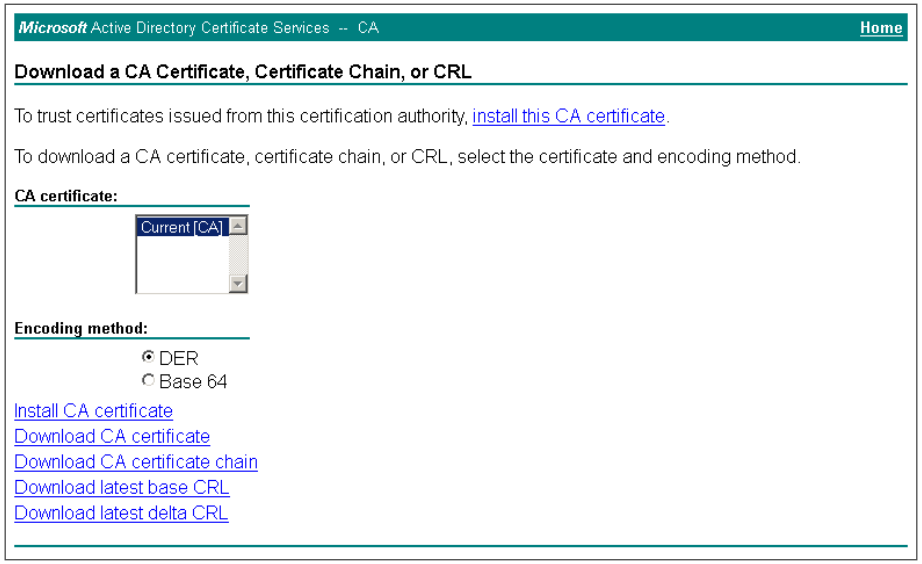
Procedure 7 Download CA root certificate

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

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

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

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



Procedure 8 Issue certificate for Cisco ISE

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

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

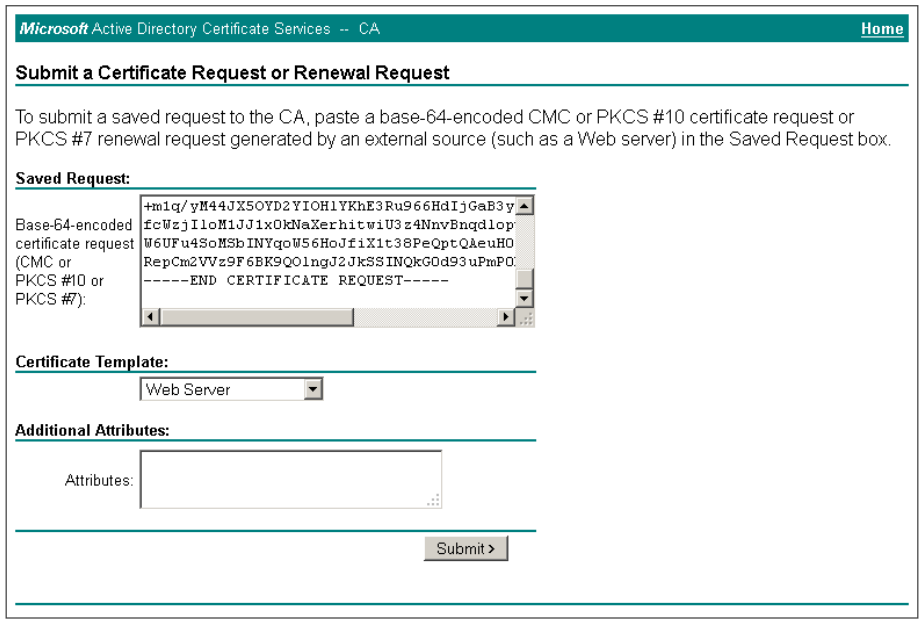
Step 3: Click **advanced certificate request**.

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**.

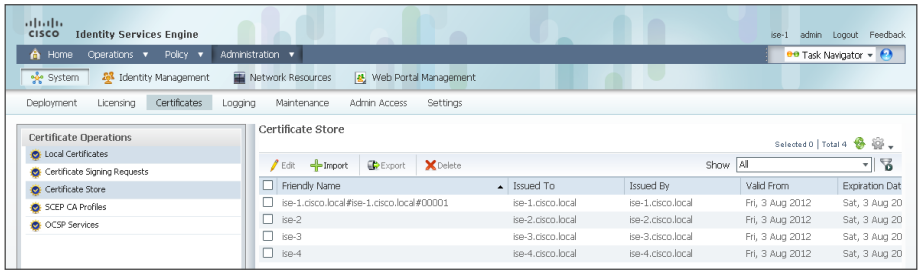


Step 8: Select **DER encoded**, and then click **Download certificate.** The certificate saves to your local machine.

Procedure 9 Install trusted root certificate in ISE

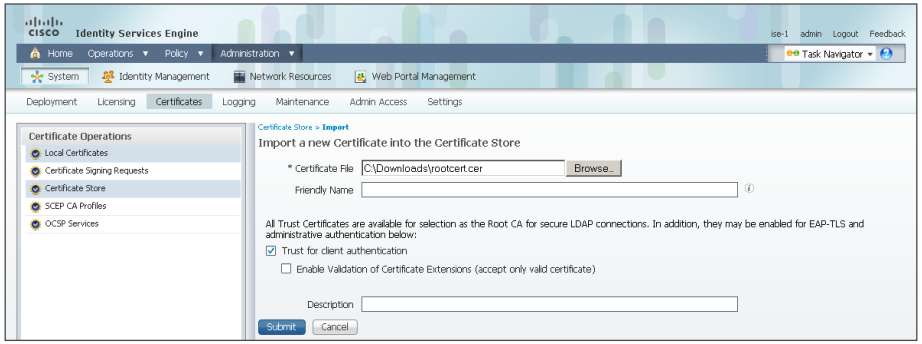
Step 1: In the Cisco ISE interface, mouse over **Administration**, and then, from the System section of the menu, choose **Certificates**.

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



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**.



Procedure 10 Configure SCEP

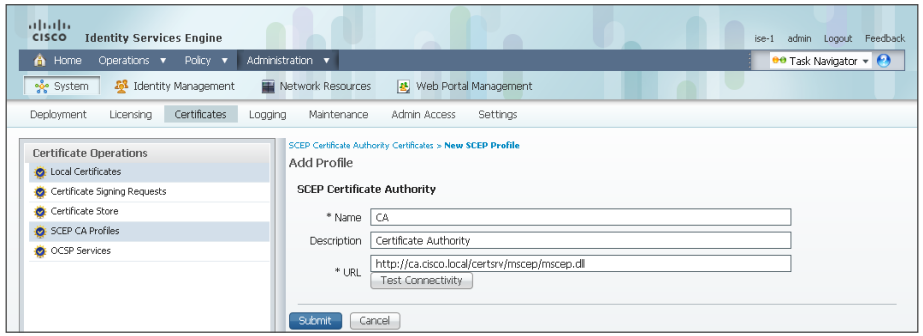
To support self-provisioning, you need to configure Cisco ISE to support SCEP, in order to enable Cisco ISE to obtain and then provision certificates for clients.

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**.

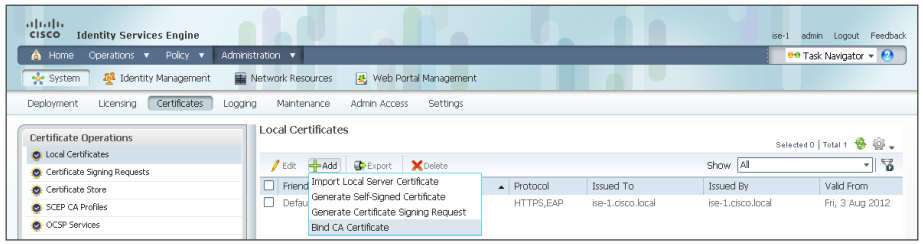


Procedure 11 Install local certificate in Cisco ISE

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

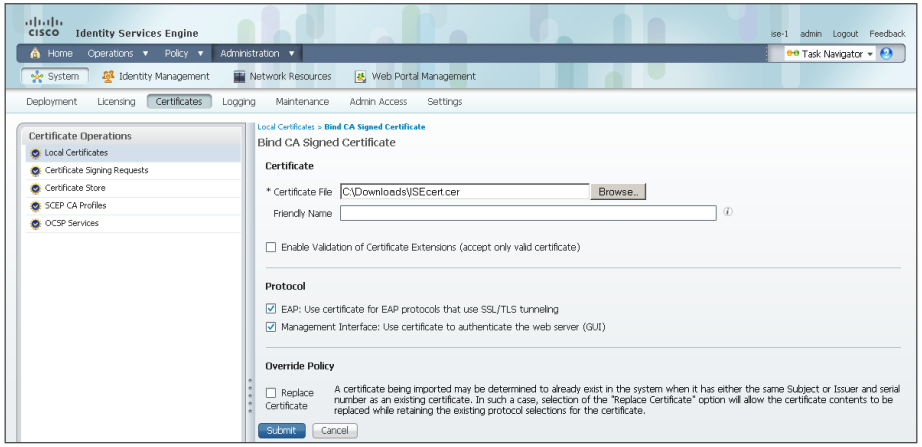
Step 2: Click **Local Certificates**.

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



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**.



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

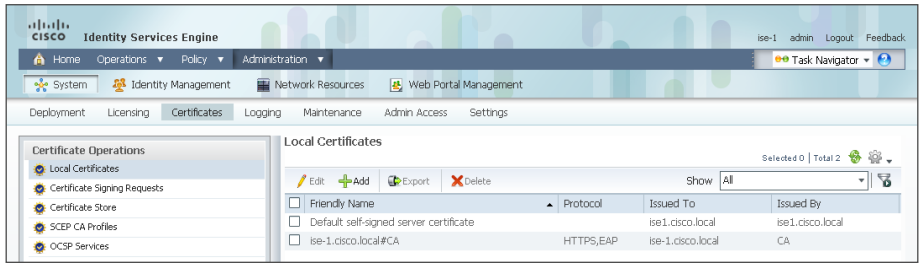
Procedure 12 Delete old certificate and request

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**.

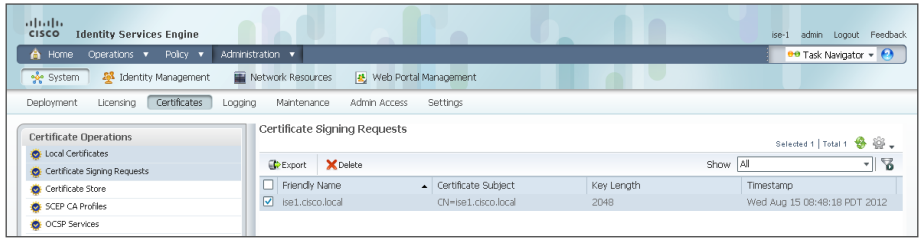
Step 3: Select the box next to the self-signed certificate. This is the certificate issued by the Cisco ISE appliance and not the certificate issued by the CA that was just imported.



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."



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

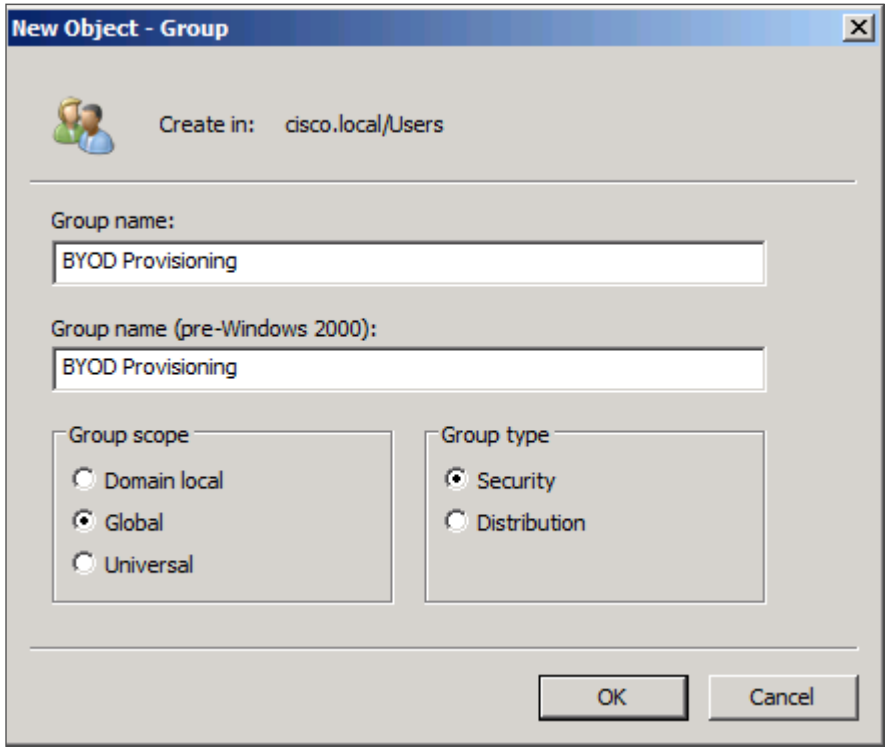
Procedure 1 Create AD group for provisioning

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**.

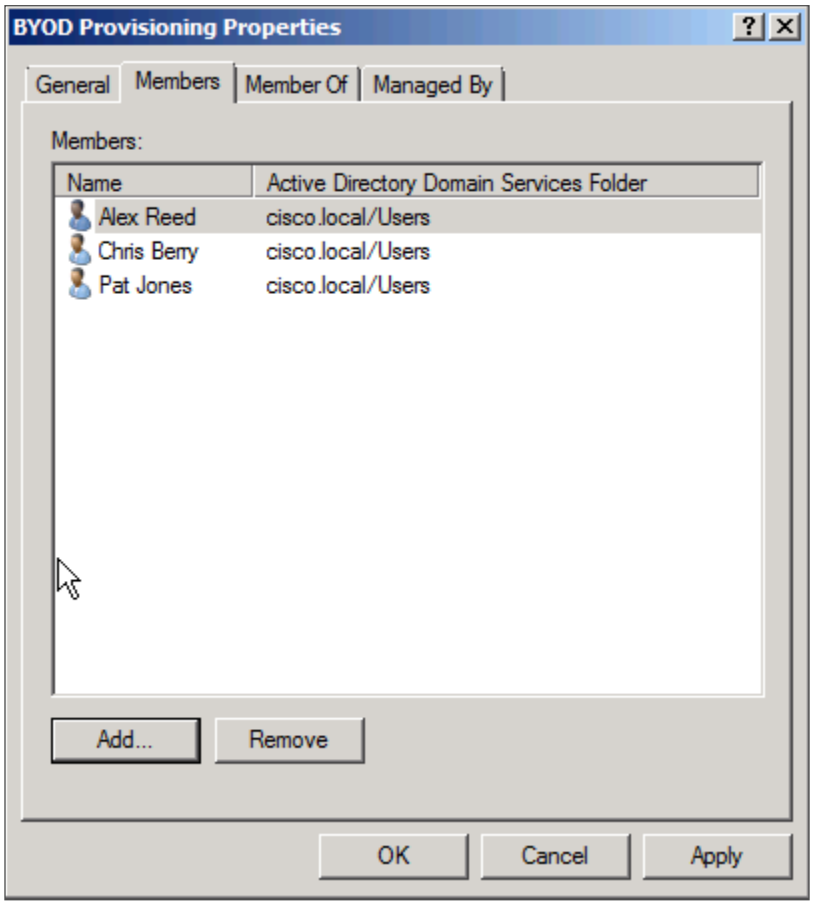


Step 4: Double-click the group name. This opens the group properties window and allows you to add users to the group.

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**.



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.

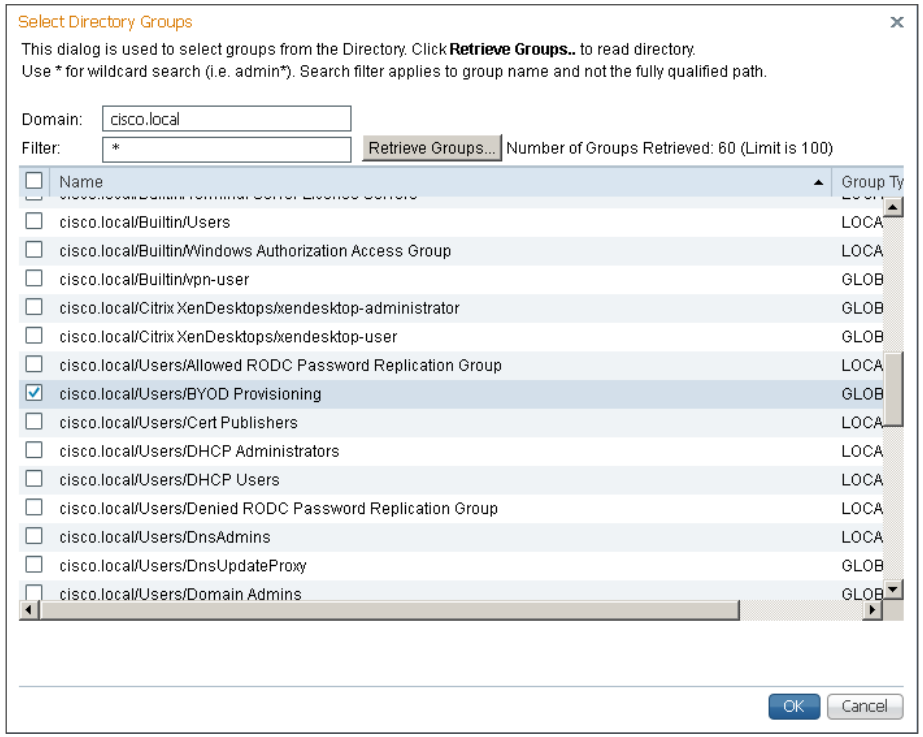
Step 2: On the menu bar, mouse over **Administration**, and then, in the Identity Management section, select **External Identity Sources**.

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**.



Procedure 3 Enable EAP-TLS

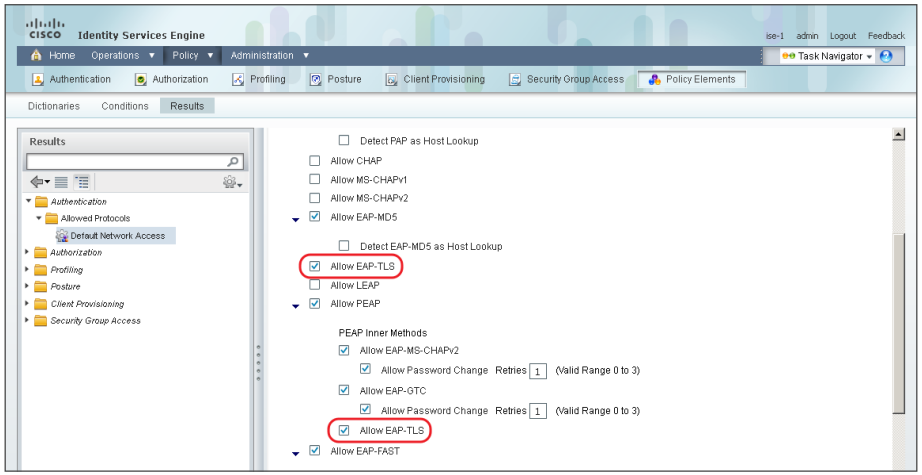
In a previous section, you disabled EAP-TLS. Now that you are using digital certificates, you need to enable it.

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**.



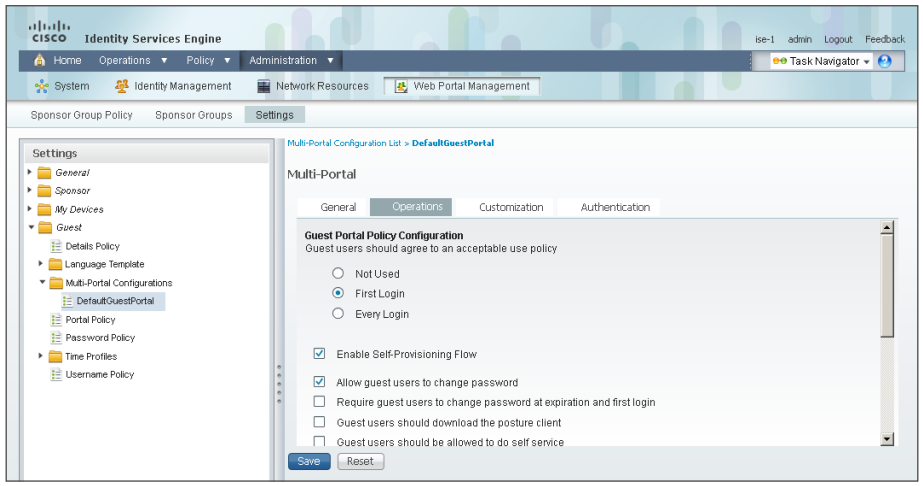
Procedure 4 Enable self-provisioning portal

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**.

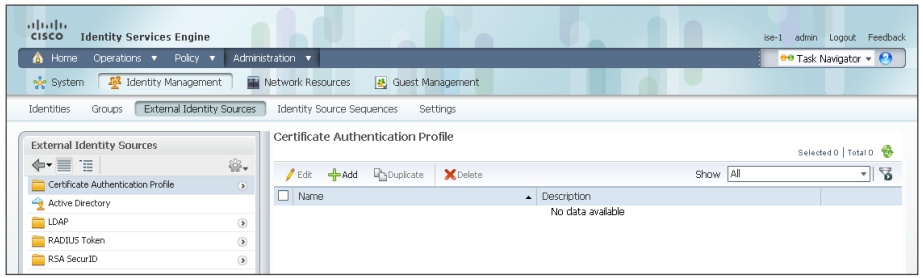


Procedure 5 Create user authentication policies

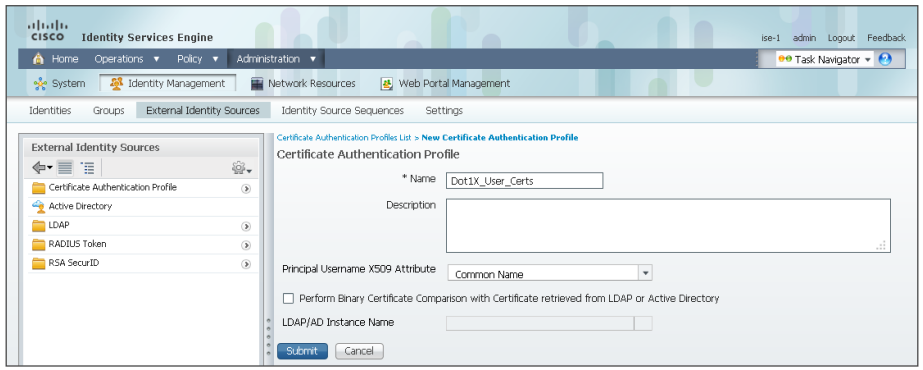
An authentication profile is used to determine how a certificate will be used for authentication. You will create an authentication profile for user authentication using certificates.

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**.



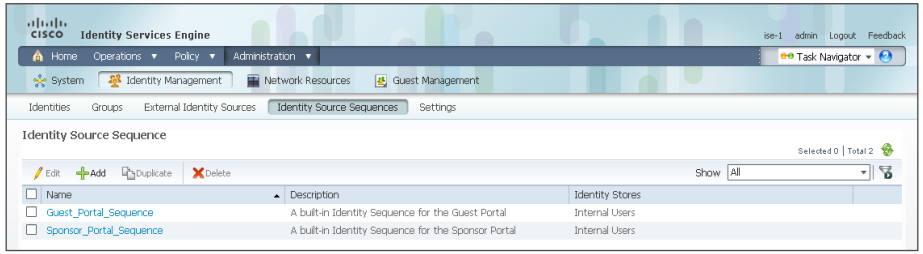
Step 3: Enter a name for the profile, and then, in the **Principal Username X509 Attribute** list, choose **Common Name**.



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**.

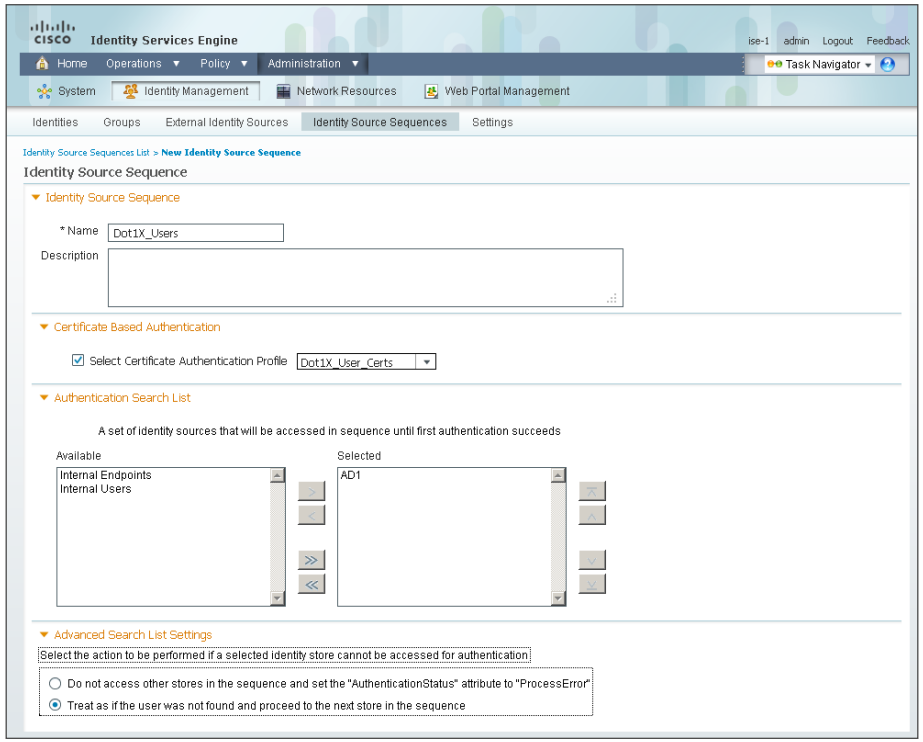


Step 6: Give the sequence a meaningful name.

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**.



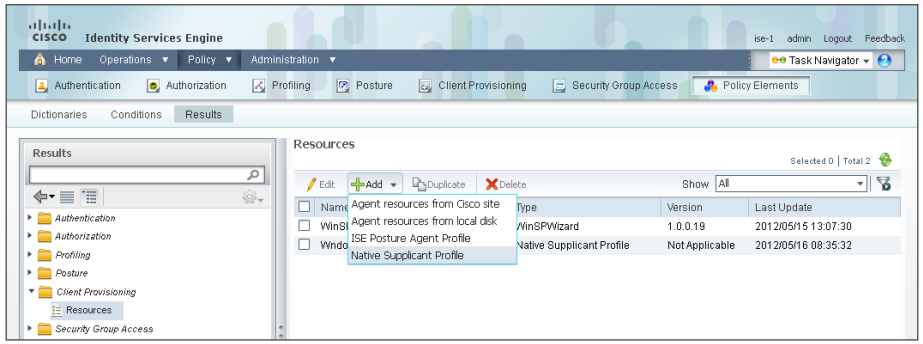
Procedure 6 Create native supplicant profile

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**.

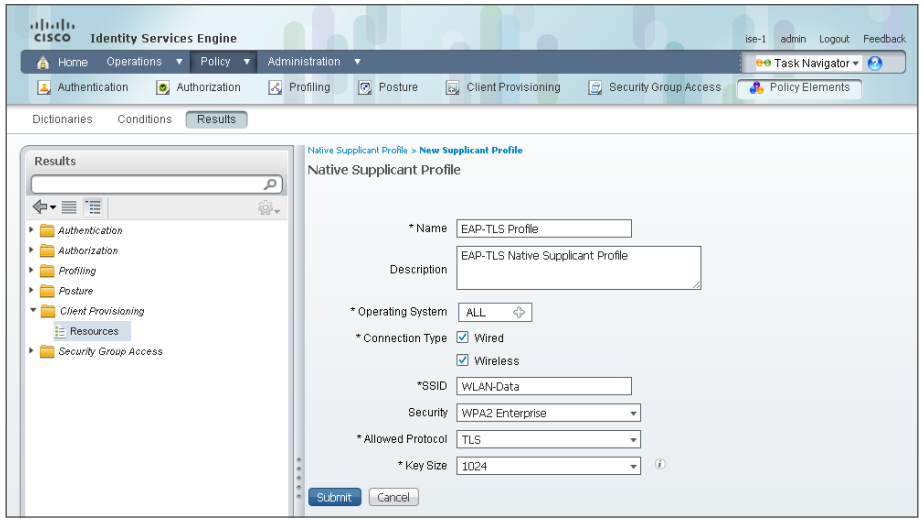
Step 3: Click **Add**, and then choose **Native Supplicant Profile**.



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**.



Procedure 7 Define provisioning policy

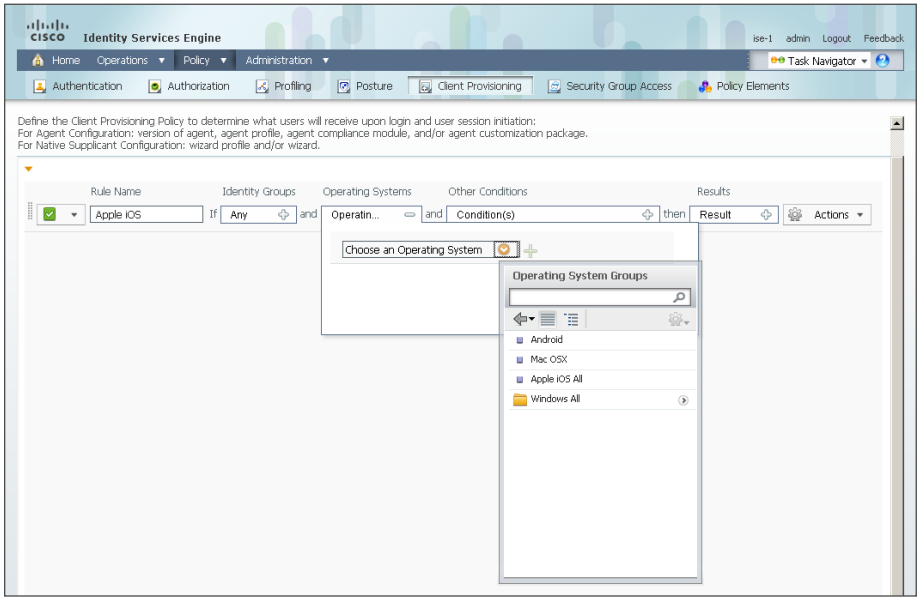
You create a provisioning policy for each operating system in order to determine which supplicant profile to apply.

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

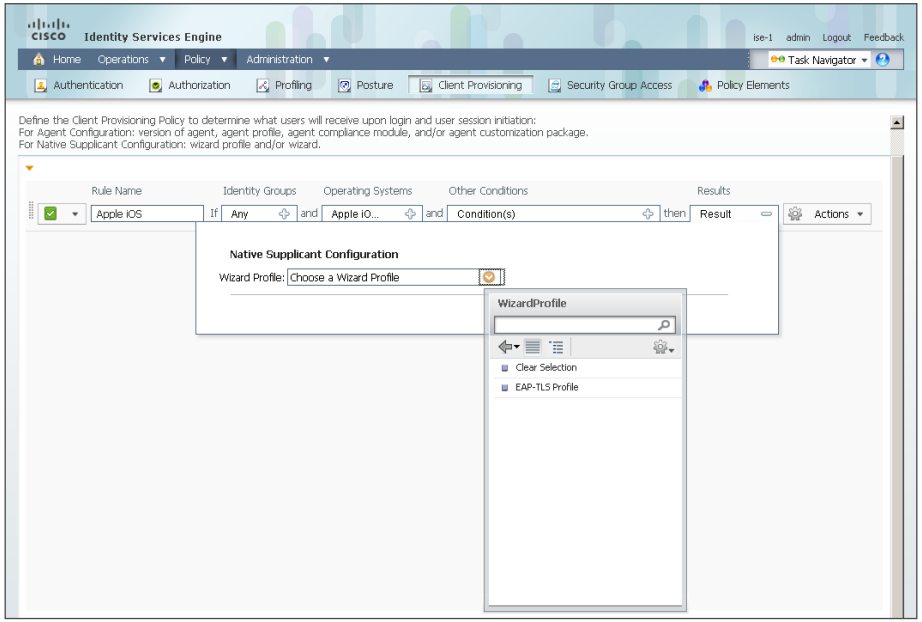
Step 2: Click **Add**.

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.



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.

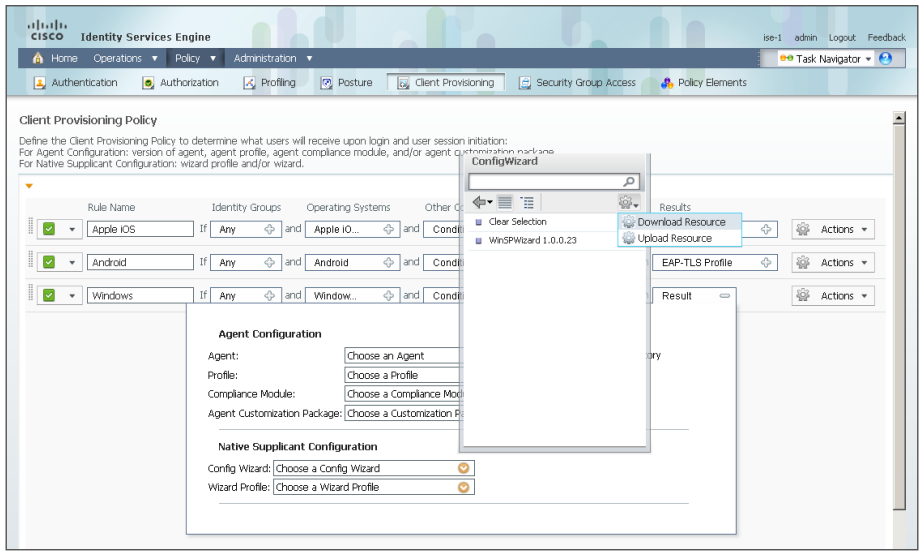
Step 8: Click **Actions**, and then select **Insert new policy below**.

Step 9: Enter a name for the rule.

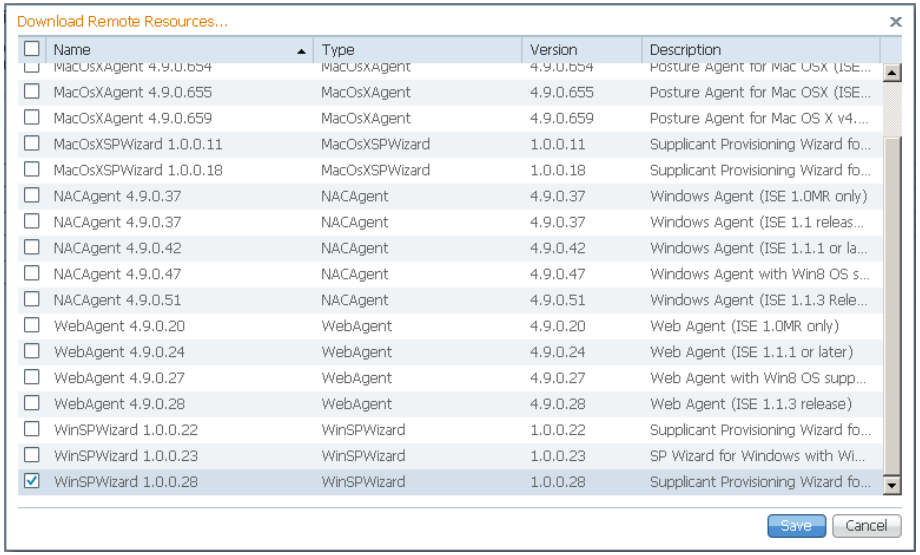
Step 10: In the Operating Systems section, click the **+** symbol, and then select **Windows All**.

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**.



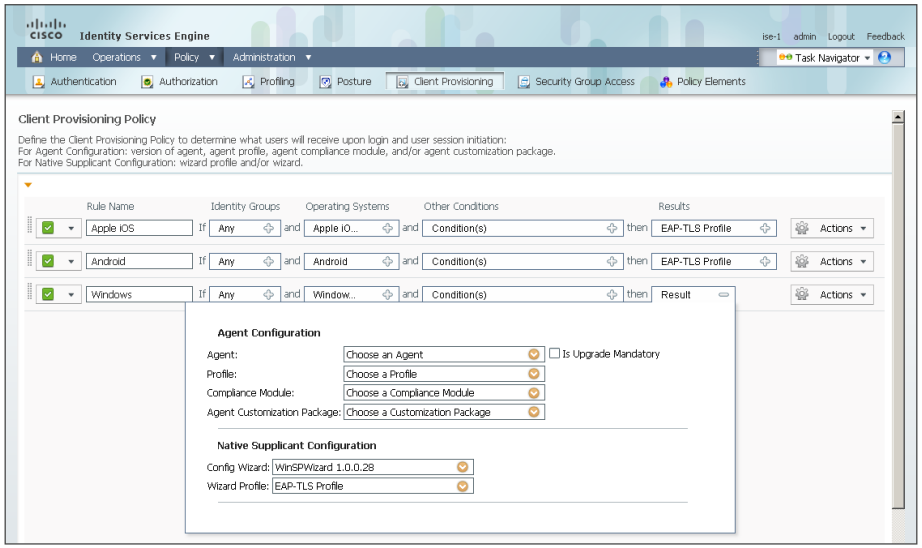
Step 13: Choose the latest version of the WinSPWizard and click **Save**. This downloads the most current wizard.



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."



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.

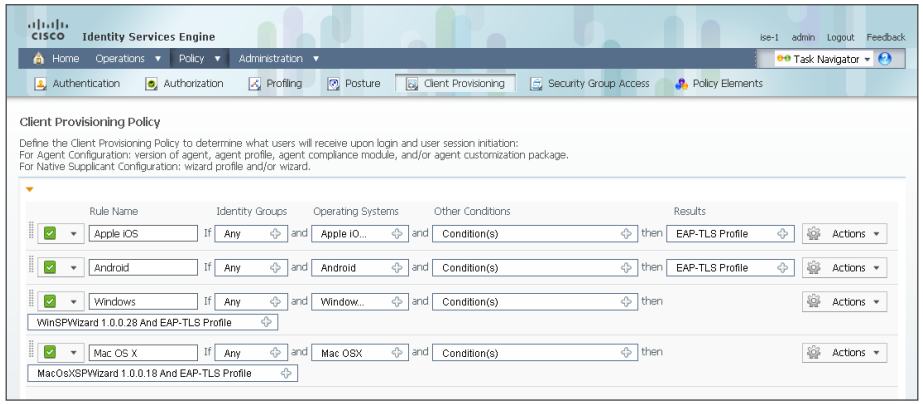
Step 21: In the **Config Wizard** list in the Native Supplicant Configuration section, click the gear icon, and choose **Download Resource**.

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**.



Procedure 8 Modify wired authentication policy

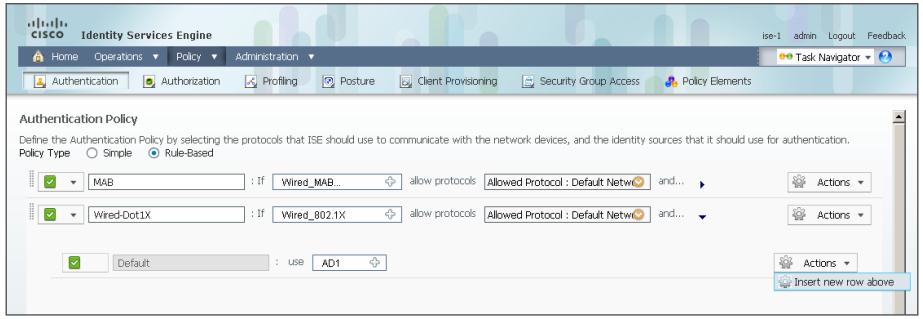
Now that you have created a certificate authentication profile and identity source sequence for digital certificates, you need to enable the 802.1X authentication policies for wired users.

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**.

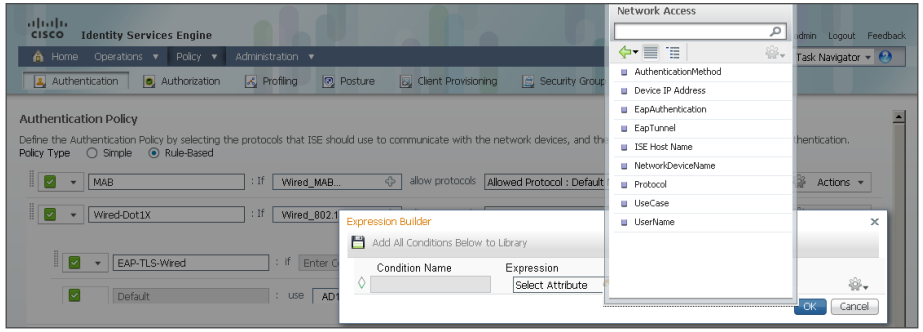


Step 4: Enter a name for the rule, and then, next to Enter Condition, click the symbol. This opens the expression builder.

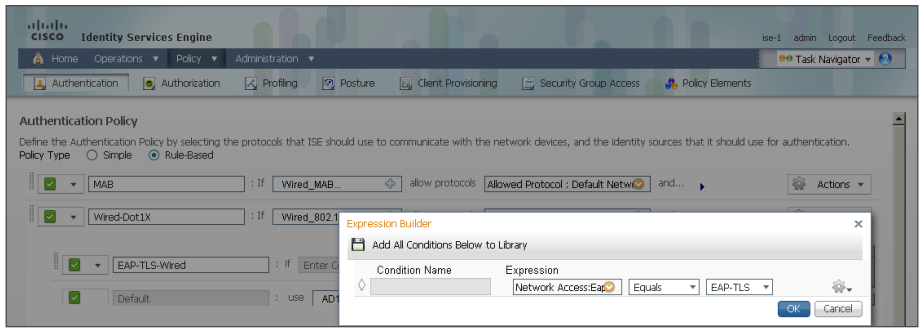
Step 5: Click **Create New Condition (Advance Option)**.

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

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

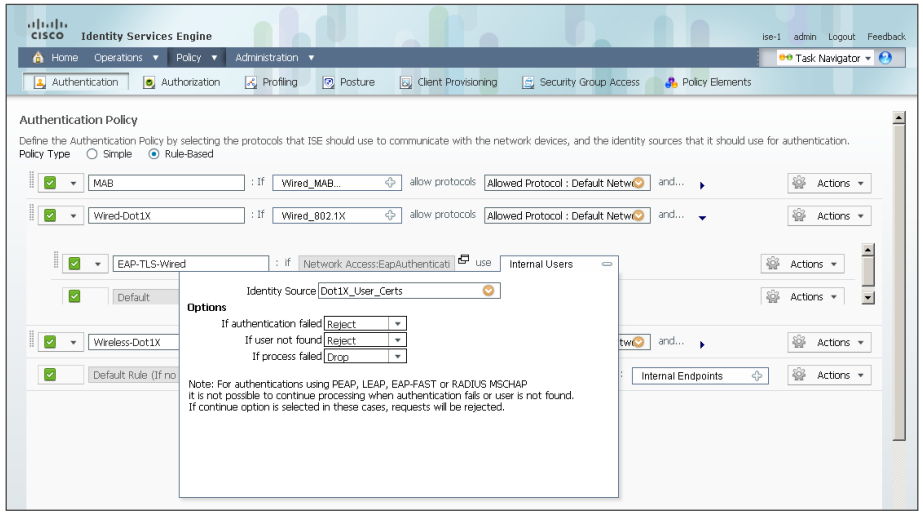


Step 8: In the first list, choose **Equals**, in the second list, choose **EAP-TLS**, and then click **OK**.



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.



Step 11: Click **Save**.

Procedure 9 Modify wireless authentication policy

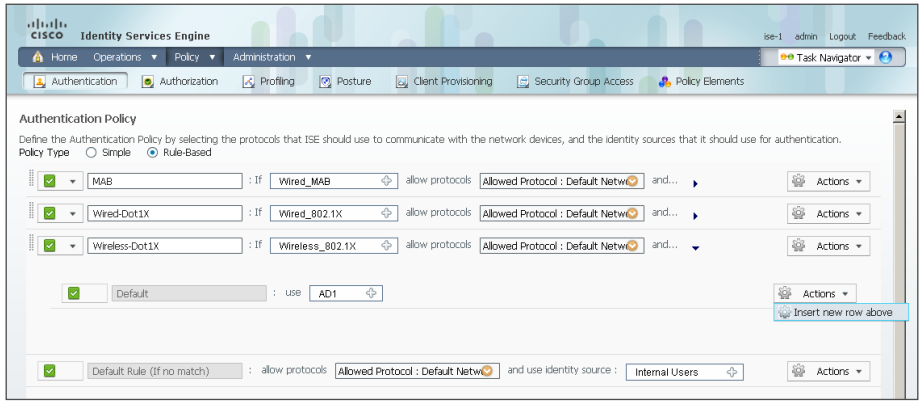
Now that you have created a certificate authentication profile and identity source sequence for digital certificates, you need to enable the 802.1X authentication policies for wireless users.

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**.

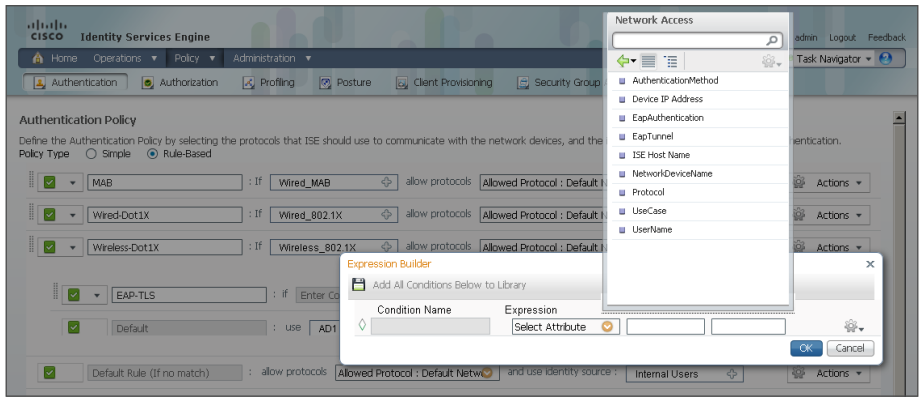


Step 4: Enter a name for the rule, and then, next to Enter Condition, click the symbol. This opens the expression builder.

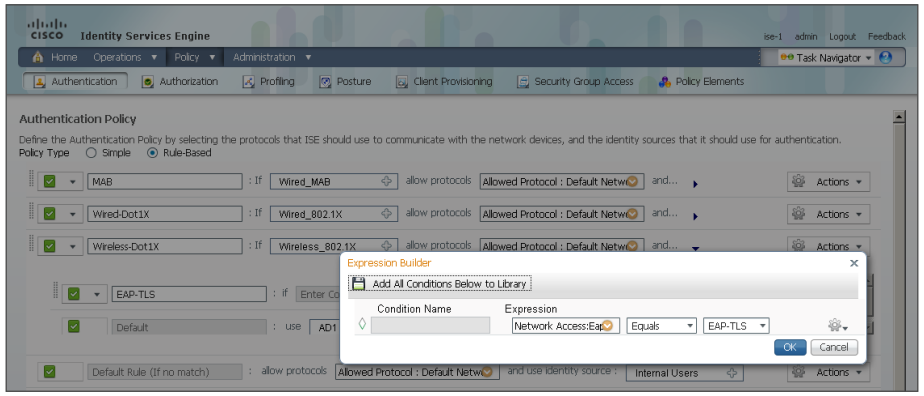
Step 5: Click **Create New Condition (Advance Option)**.

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

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

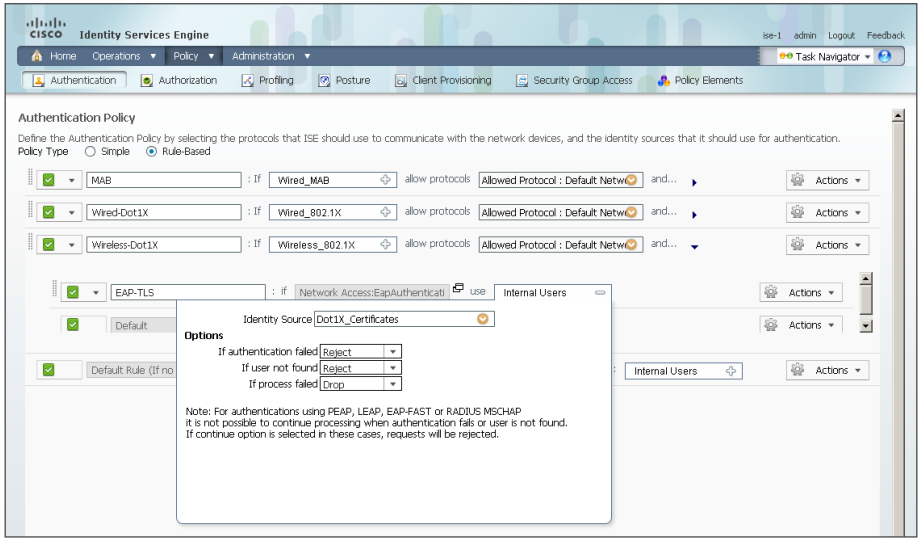


Step 8: In the first list, choose **Equals**, in the second list, choose **EAP-TLS**, and then click **OK**.



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.



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.

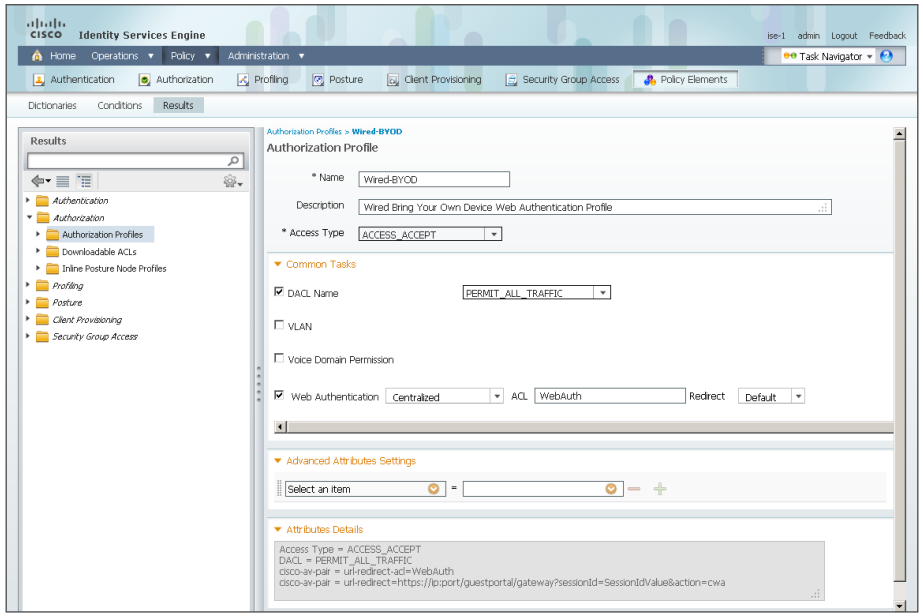
Step 5: Select **DACL Name** and then, in the list, choose **PERMIT_ALL_TRAFFIC**.

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**.



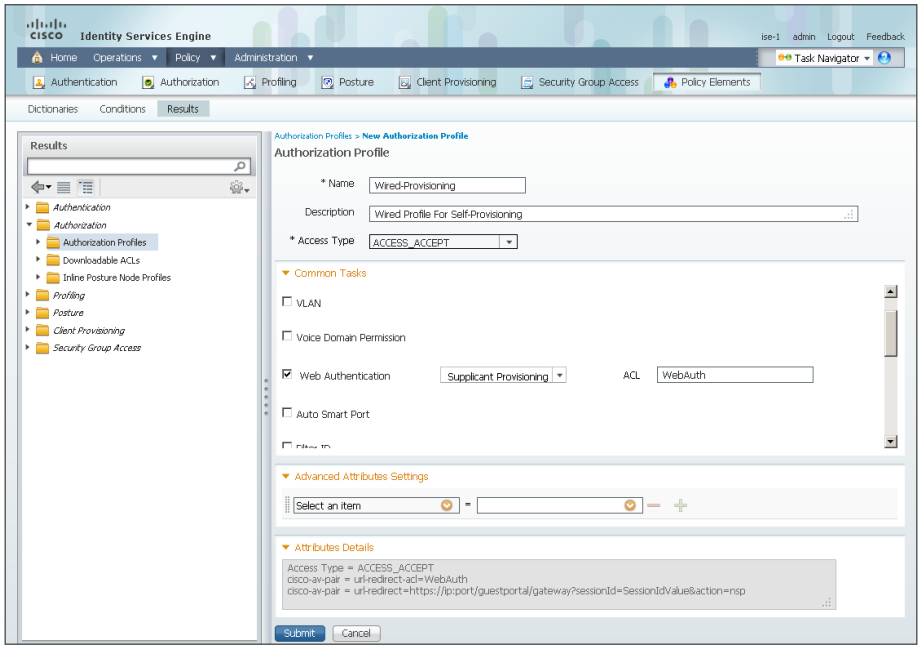
Step 10: Click **Add**.

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**.



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.

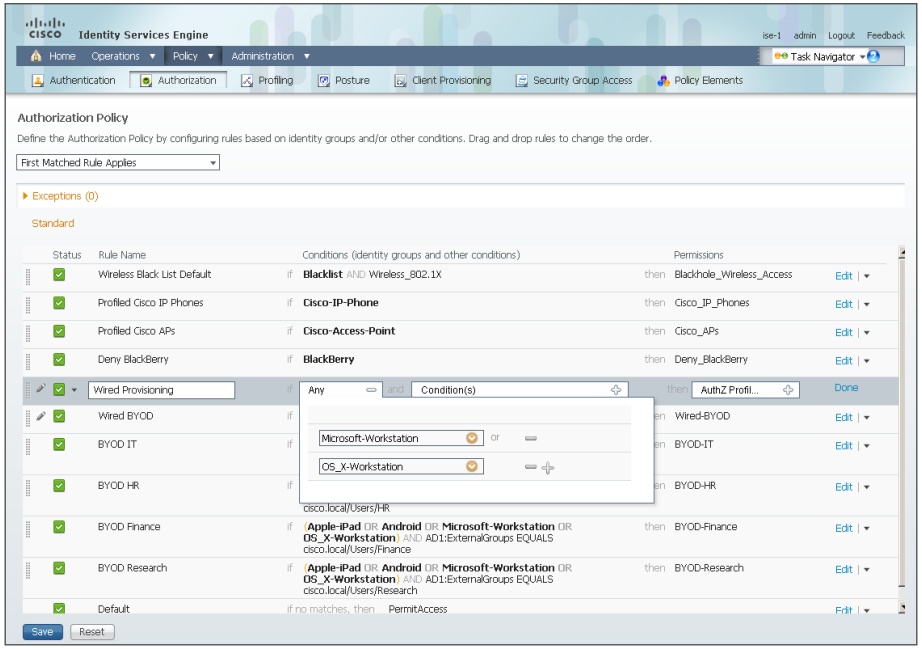
Step 12: In the list, next to Endpoint Identity Groups, click the **>** symbol, and then, next to Profiled, click the **>** symbol.

Step 13: Choose **Microsoft-Workstation**.

Step 14: Next to Microsoft_Workstation, click the **+** symbol.

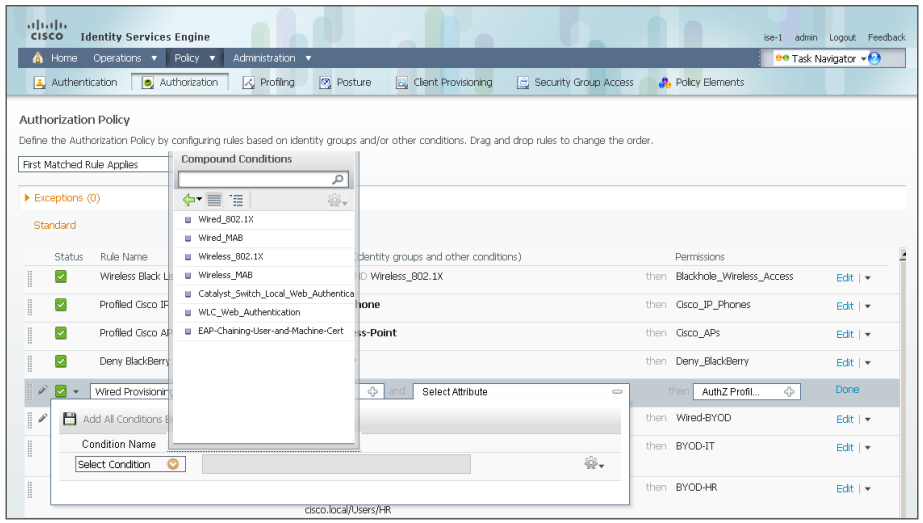
Step 15: In the list, next to Endpoint Identity Groups, click the **>** symbol.

Step 16: Next to Profiled, click the **>** symbol, and then choose **OS_X-Workstation**.



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**.

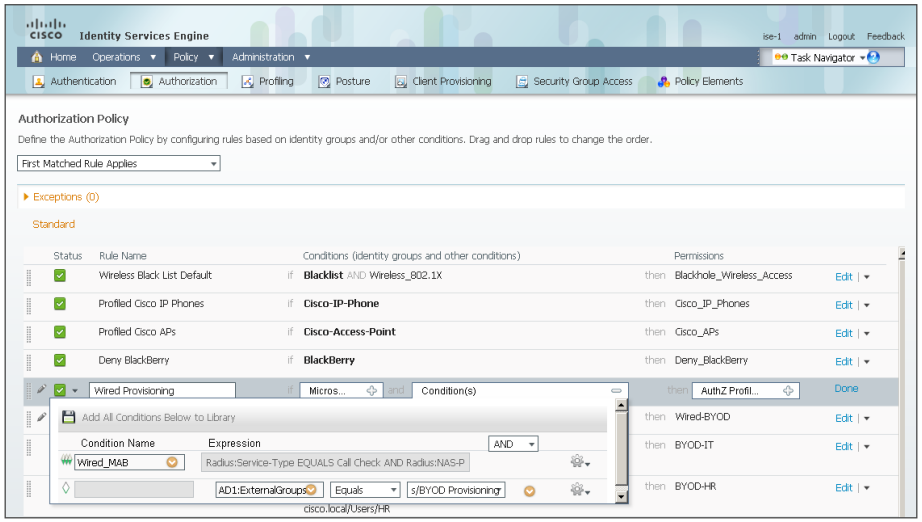


Step 19: At the end of this rule, click the gear icon, and then select **Add Attribute/Value**.

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

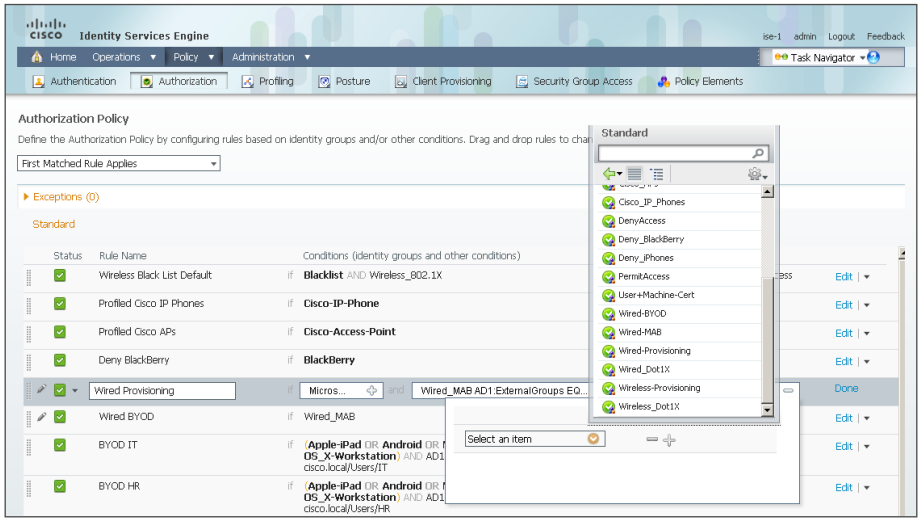
Step 21: Next to AD1, click the > symbol, and then choose **ExternalGroups**.

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."

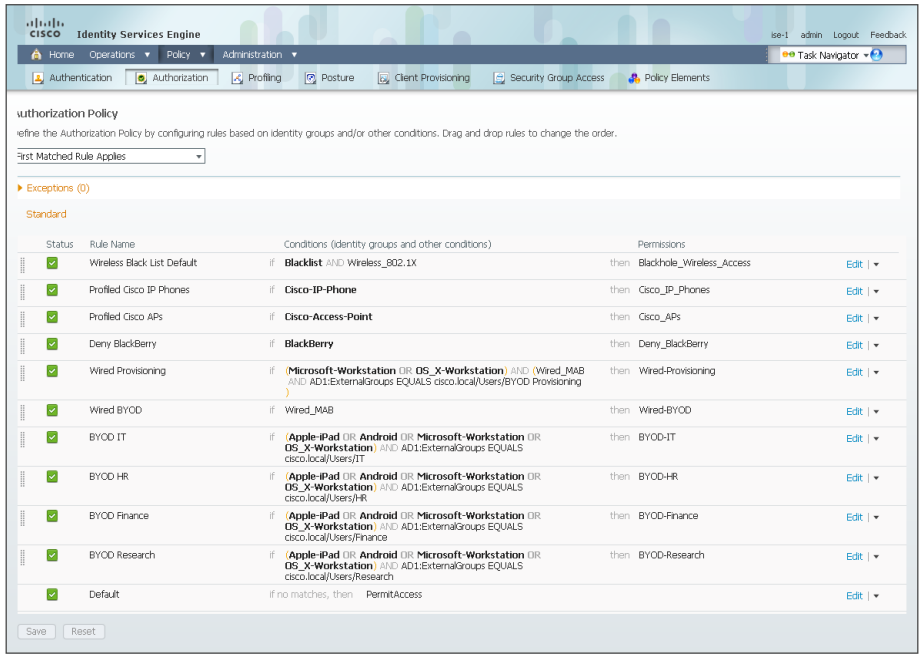


Step 23: Next to AuthZ Profile(s), click the + symbol, and then, next to Select an item, click the arrow.

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."



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



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**.

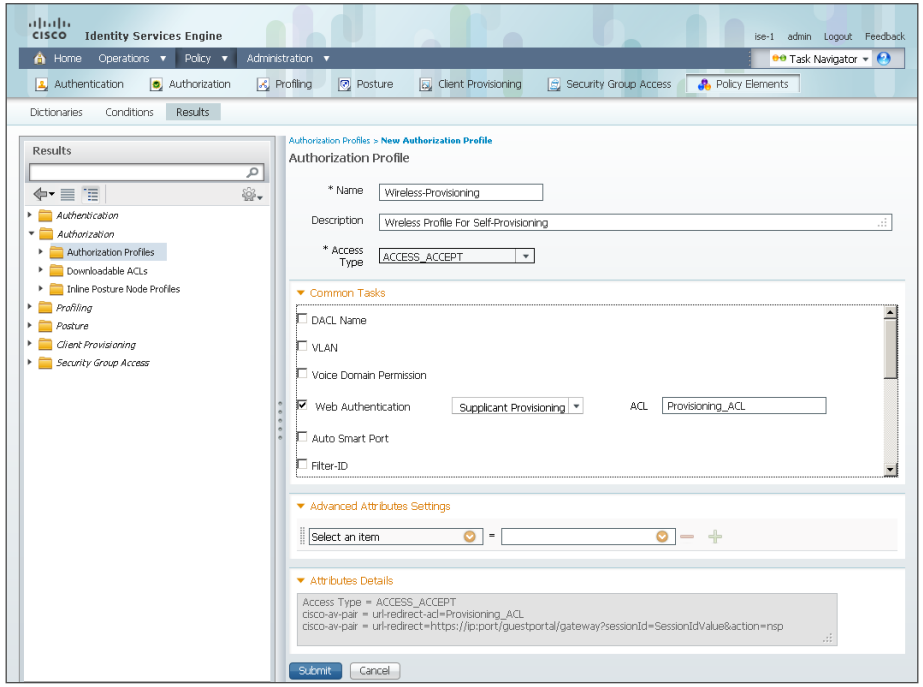
Step 4: Enter a name and description for the profile.

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**.



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.

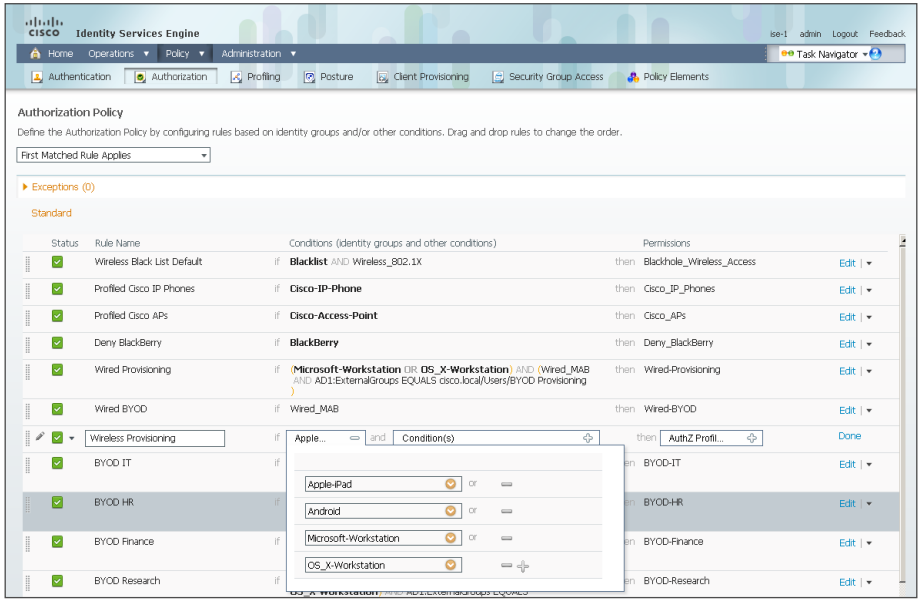
Step 11: In the list, next to Endpoint Identity Groups, choose the **>** symbol.

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

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

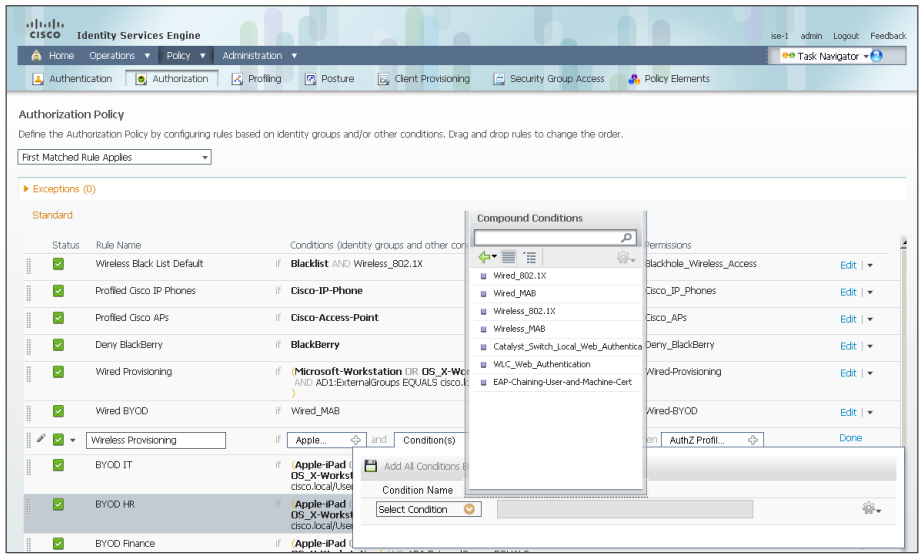
Step 14: In the list, next to Endpoint Identity Groups, choose the **>** symbol.

Step 15: Next to Profiled, click the **>** symbol, and then choose **OS_X-Workstation**.



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**.



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**.

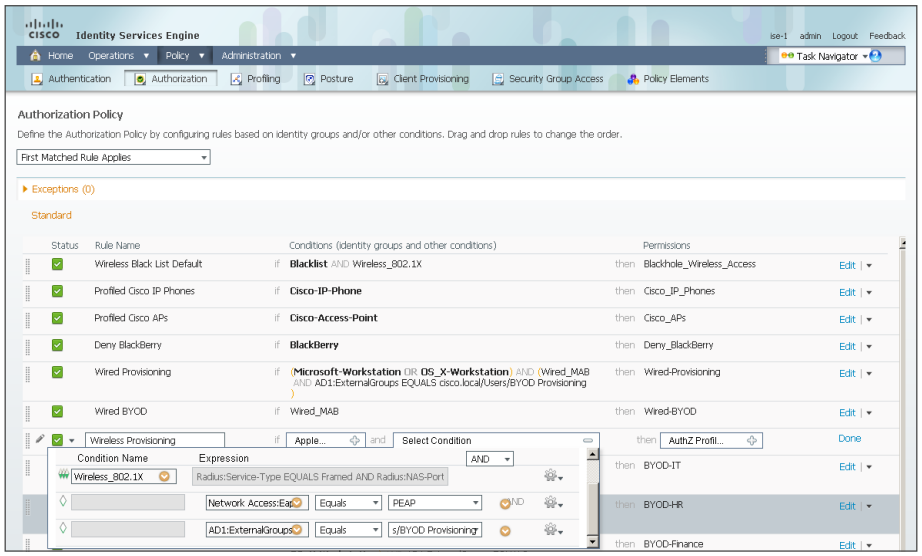
Step 21: Under Expression, in the first list, choose **Equals**, and then, in the second list, choose **PEAP**.

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.

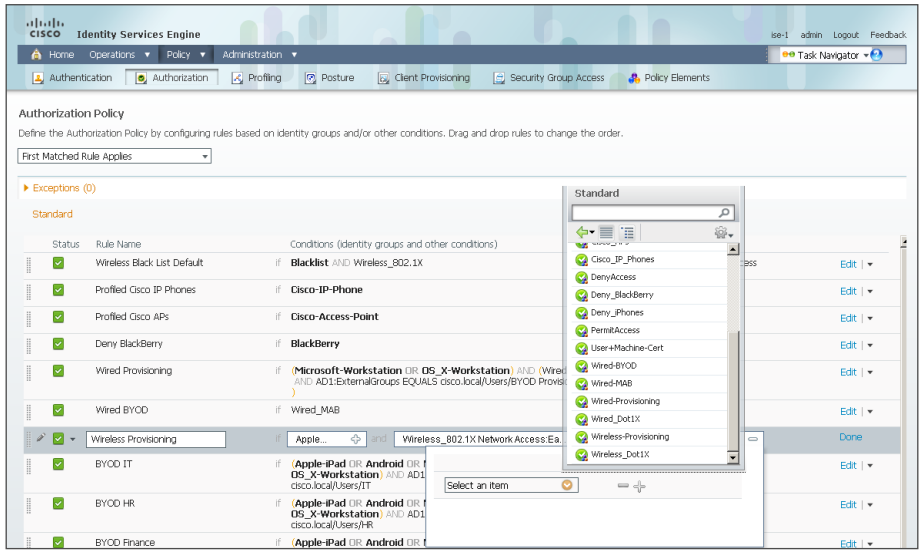
Step 24: Next to AD1, click the > symbol, and then choose **ExternalGroups**.

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

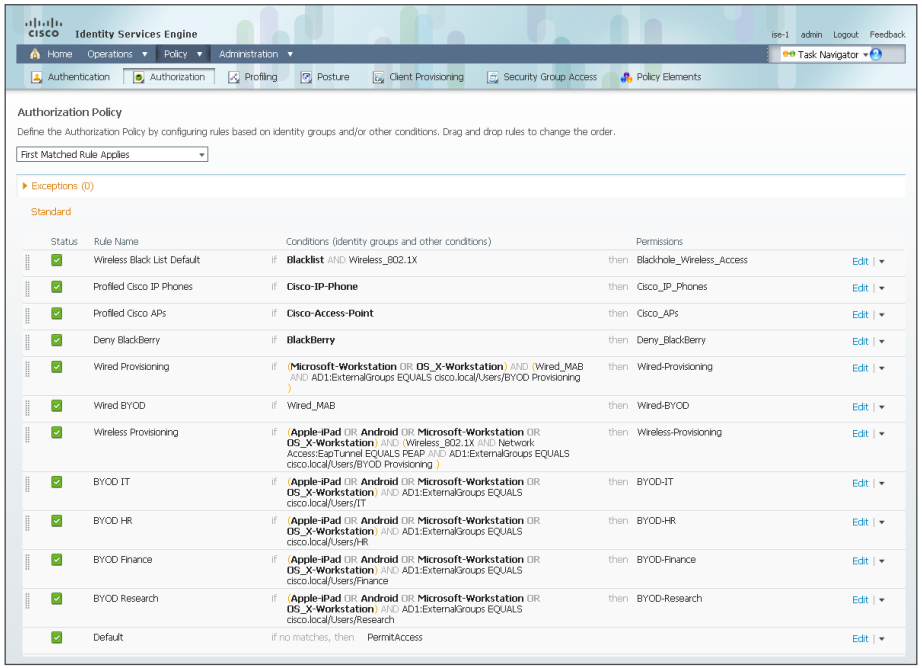


Step 26: Next to AuthZ Profile(s), click the **+** symbol, and then, next to Select an item, click the arrow.

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



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



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**.

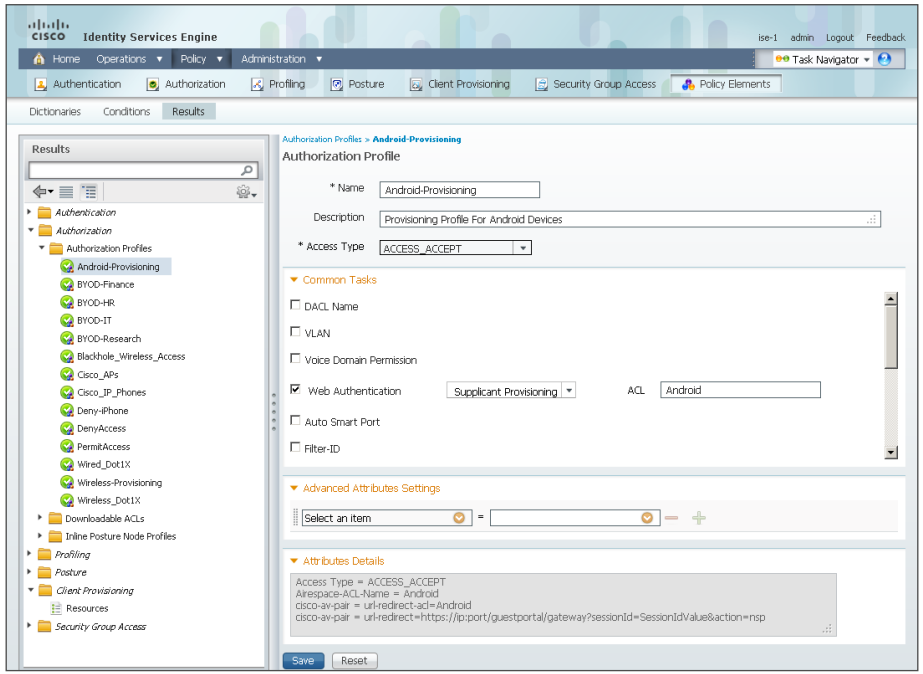
Step 4: Enter a name and description for the profile.

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**.

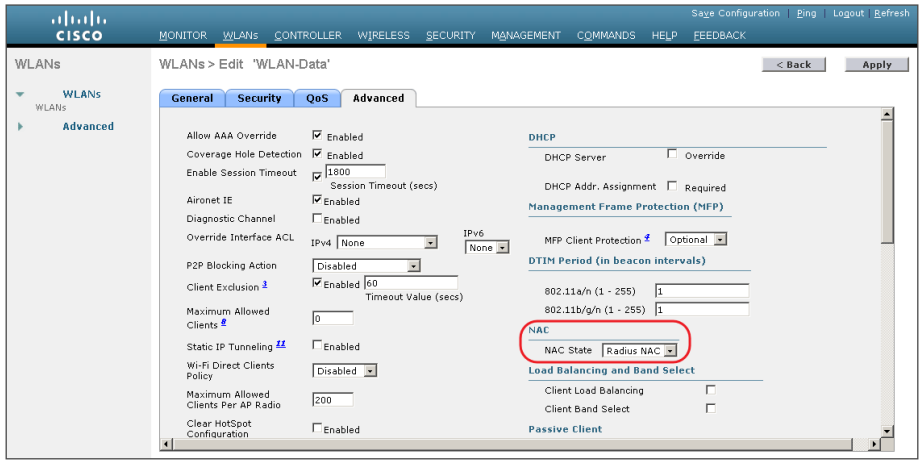
Procedure 19 Configure WLCs

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**.

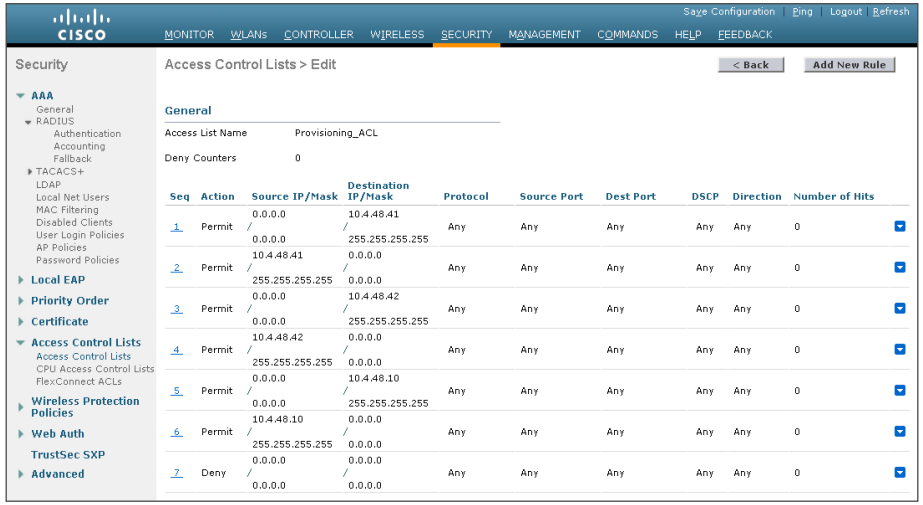
Step 6: Click **New**.

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.



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.

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.

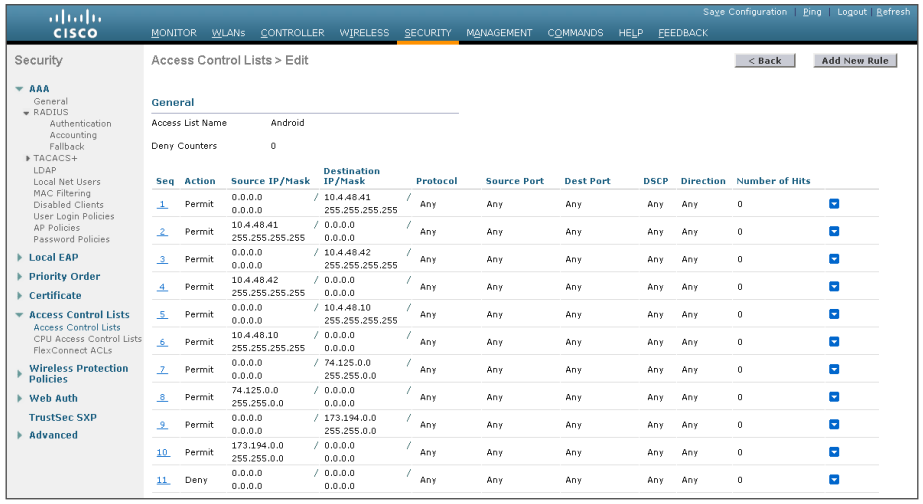
Step 15: Click **Add New Rule**.

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**.



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**.

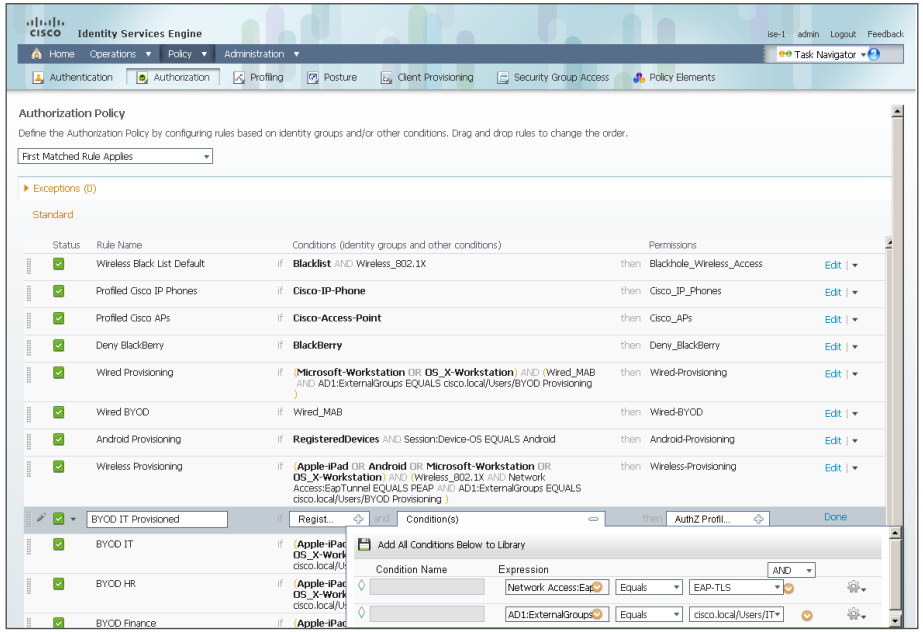
Step 10: Under Expression, in the first list, choose **Equals**, and then, in the second list, choose **EAP-TLS**.

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.



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**.

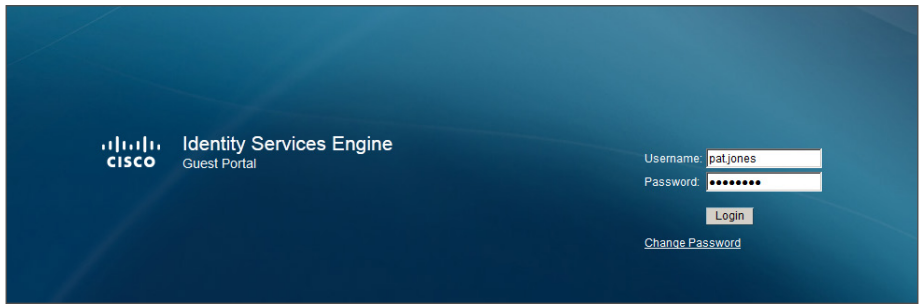
Procedure 23 Provision a Windows workstation

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

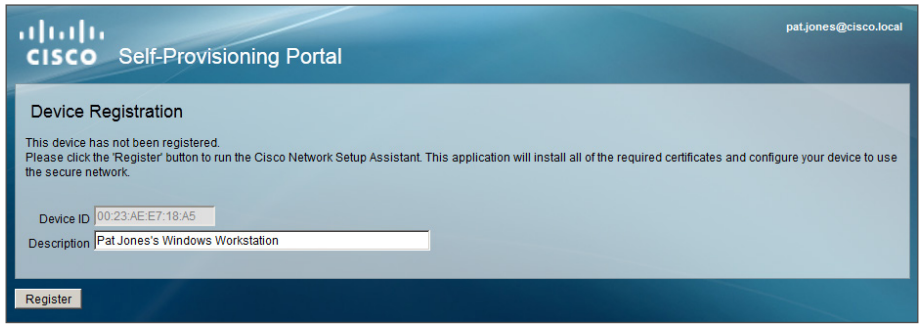
Step 1: From a Windows workstation, connect to the network by connecting an Ethernet cable for a wired connection. For wireless, open the Network control panel and choose the wireless network name. Use your username and password to connect to the wireless network.

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**.

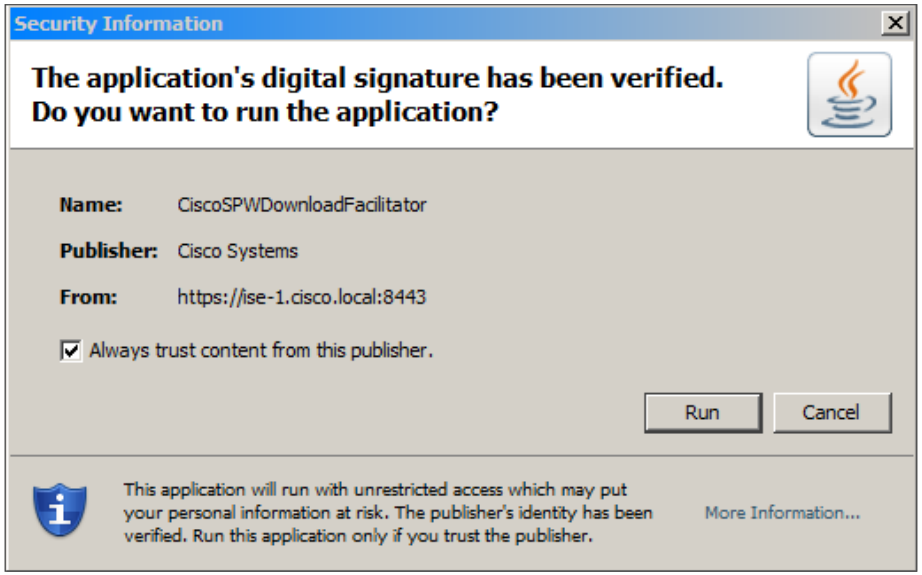


Step 4: The browser will then connect to the Self-Provisioning Portal. Enter a description of the device, and then click **Register**.

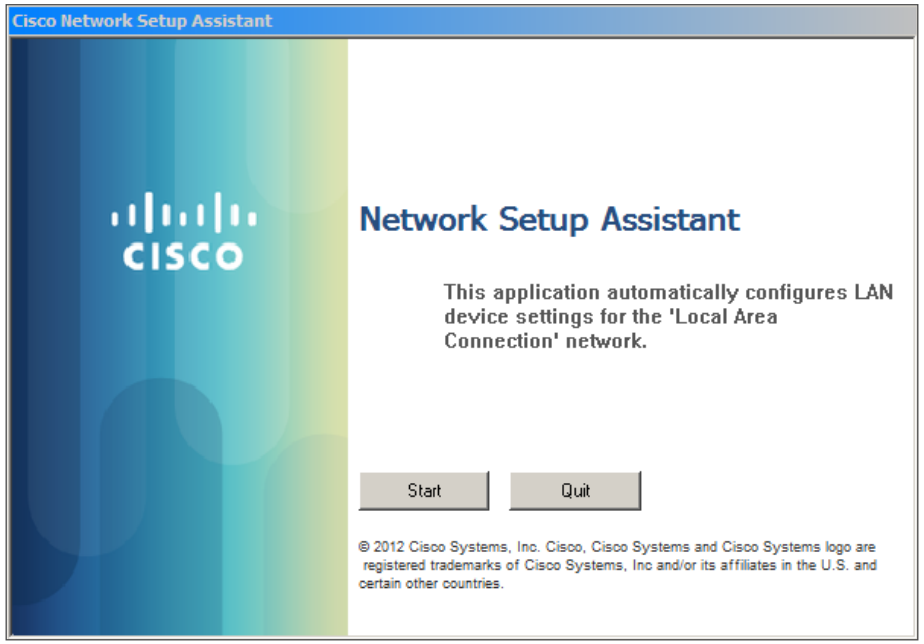


The provisioning process begins.

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



Step 6: Click **Start**.



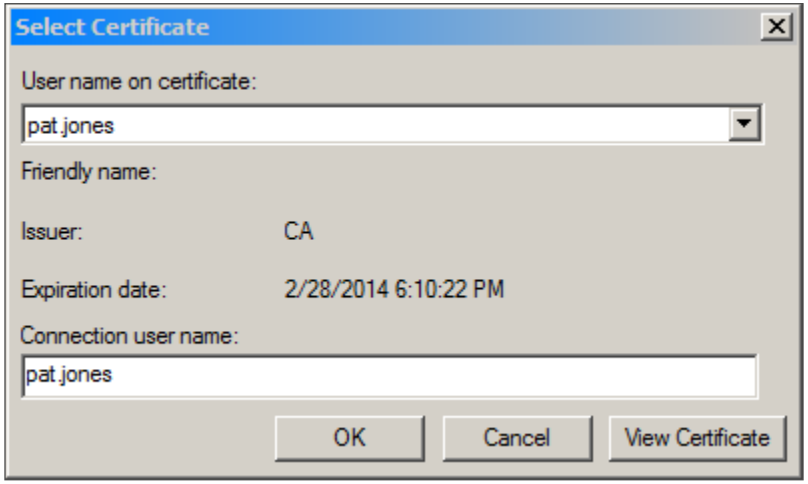
Step 7: As the Network Setup Assistant runs, you will be prompted to verify you want to install the root certificate. Click **Yes**.

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**.



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.

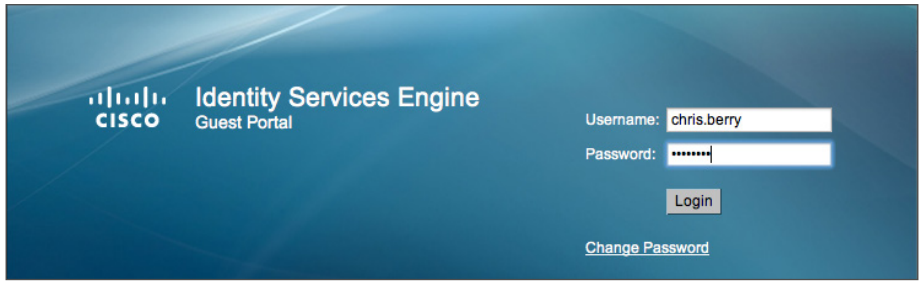
For wireless, open **System Preferences**, click **Network**, and then, in the **Network Name** list, choose your network. Use your username and password to connect to the wireless network.

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

The browser gets redirected to the Guest Portal.

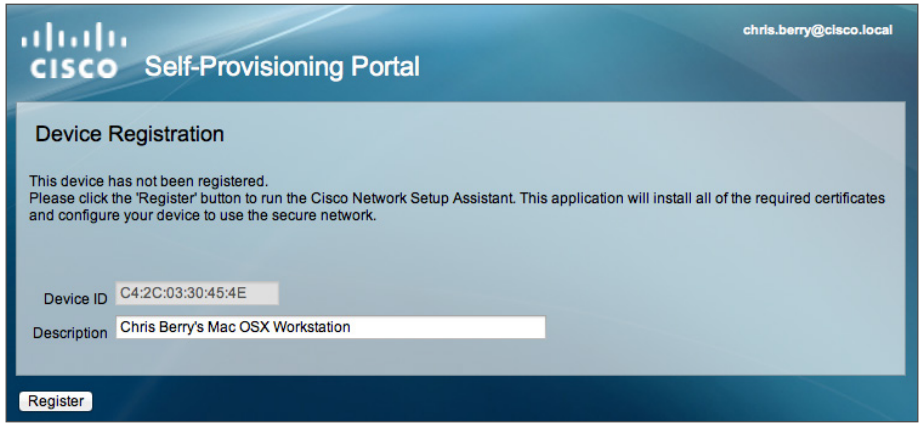
Step 3: Enter your username and password, and then click **Login**.

Step 4:



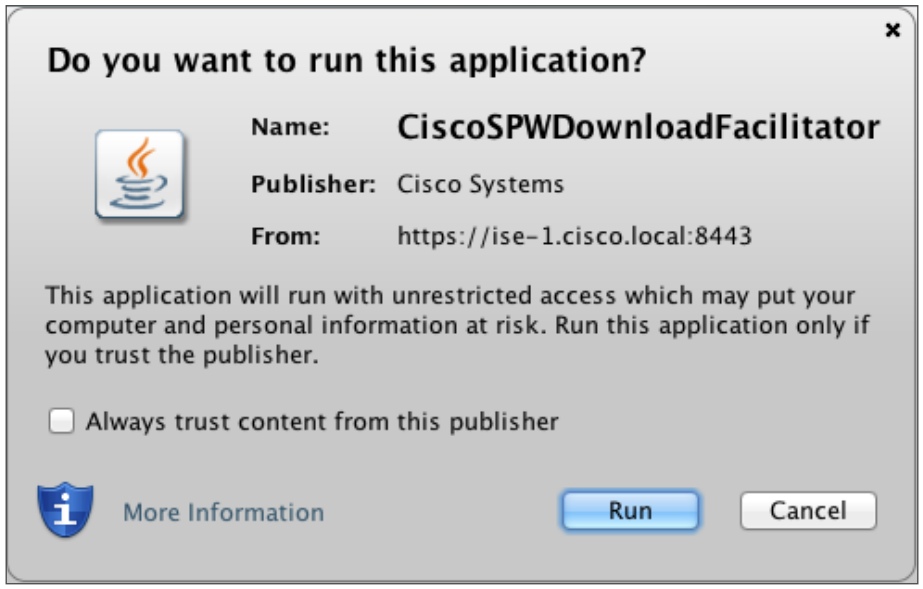
The browser will then connect to the Self-Provisioning Portal.

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



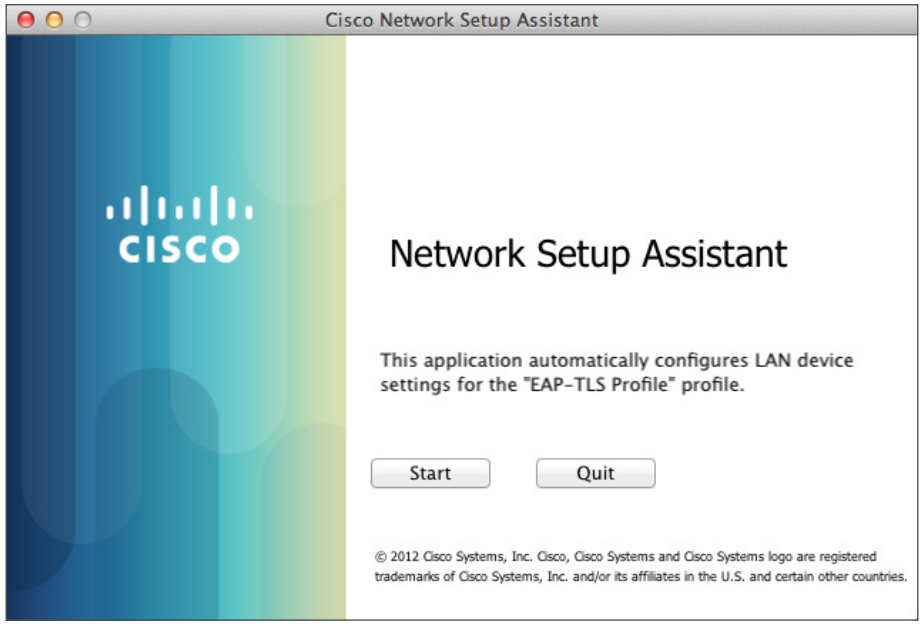
The provisioning process begins.

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**.



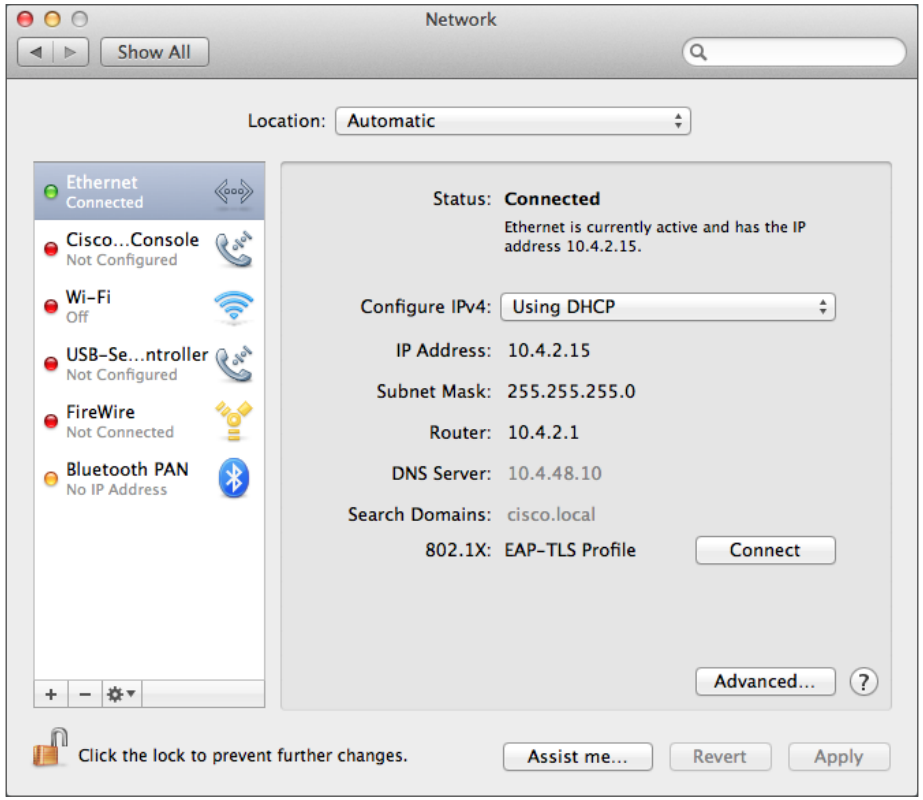
As the Network Setup Assistant runs, you will be prompted to verify you want to modify the system.

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**.

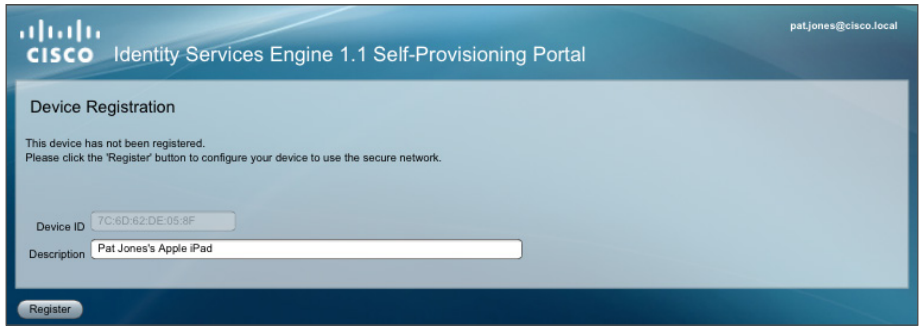


Procedure 25 Provision an Apple iPad

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

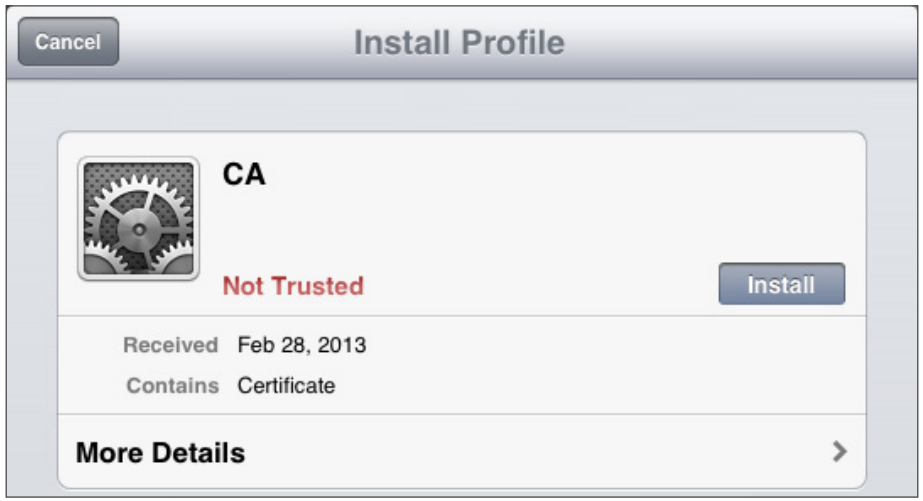
Step 1: From an iPad, connect to the wireless network by opening **Settings**, and then choosing the network from the list. Connect using your username and password.

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.

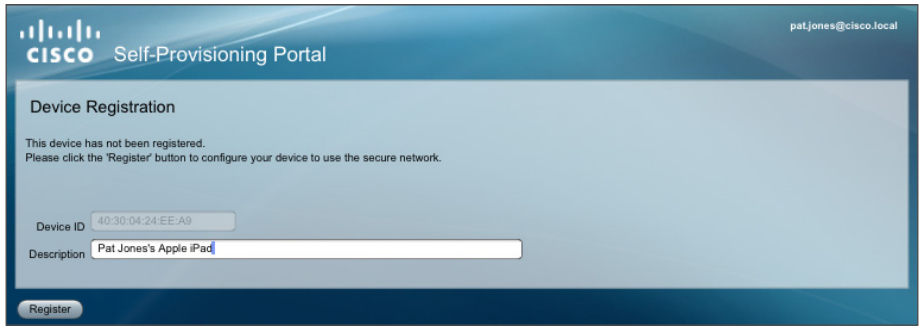
Step 3: Click **Install**. The trusted root certificate from the CA installs.



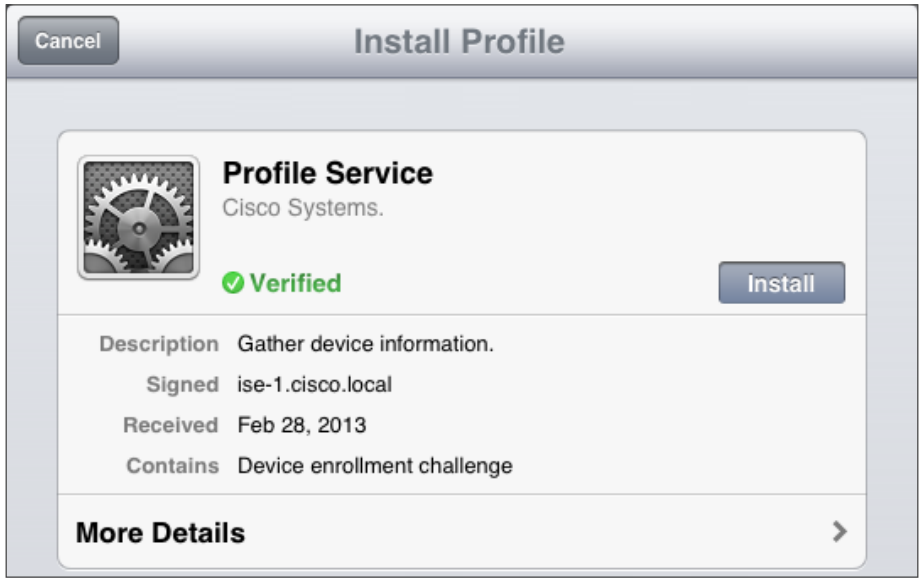
Step 4: On the warning message that appears, click **Install**.

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

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



Step 7: Click **Install**. The user certificate installs.



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.

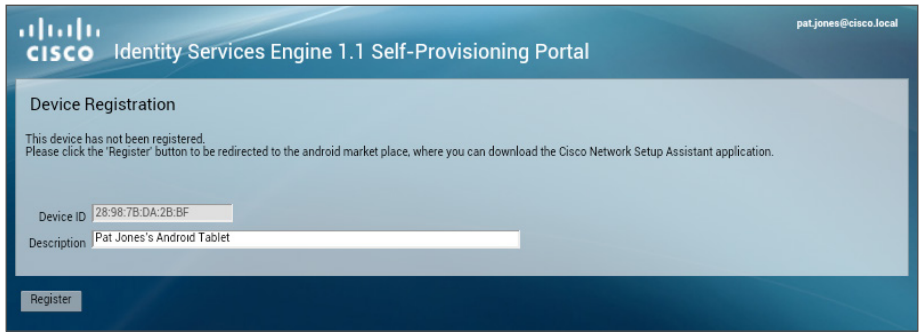
Procedure 26 Provision an Android tablet

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.

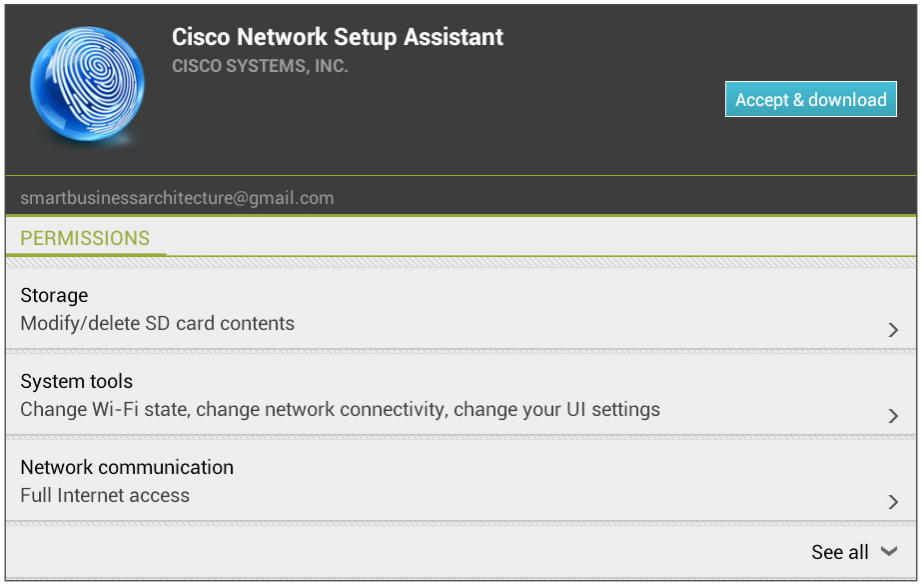
Step 2: Open the browser and browse to any site.

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

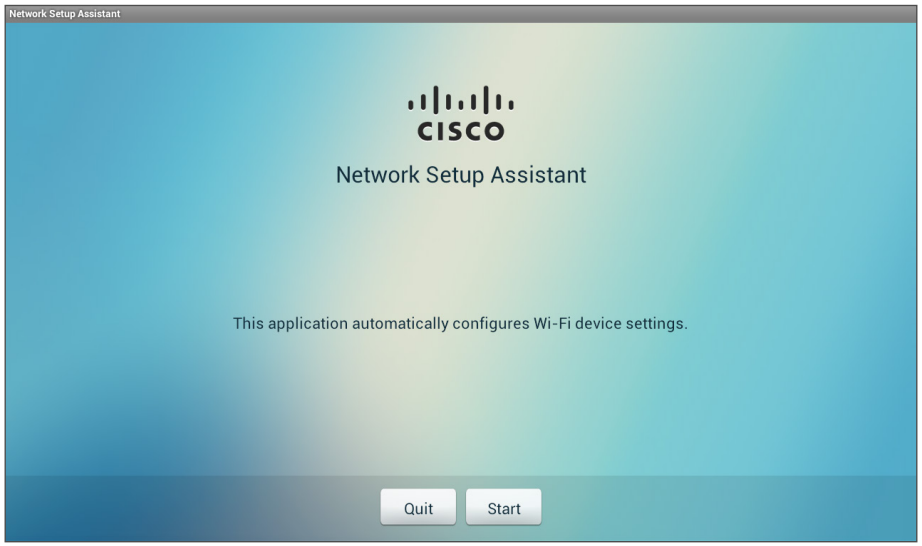


Step 4: Choose **Play Store**. The Google Play Store opens, where you can download the Cisco Network Setup Assistant.

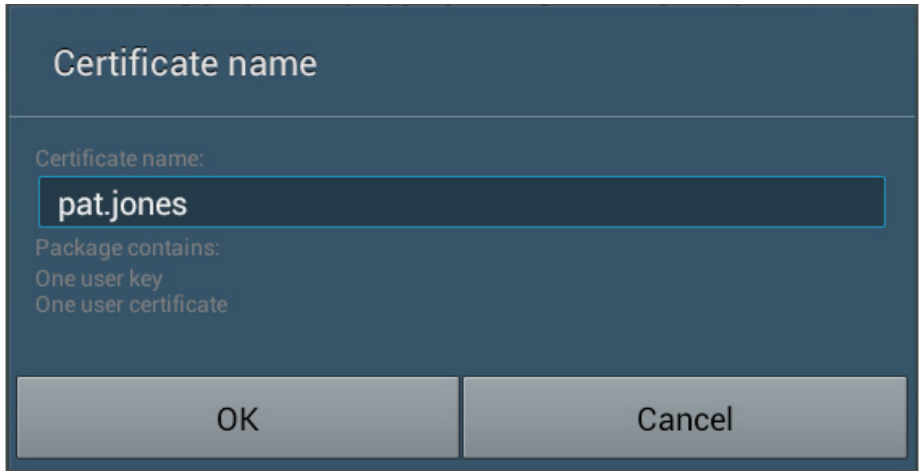
Step 5: In the Google Play Store, click **Download**, and then, on the verification window, click **Accept & download**. The Cisco Network Setup Assistant downloads.



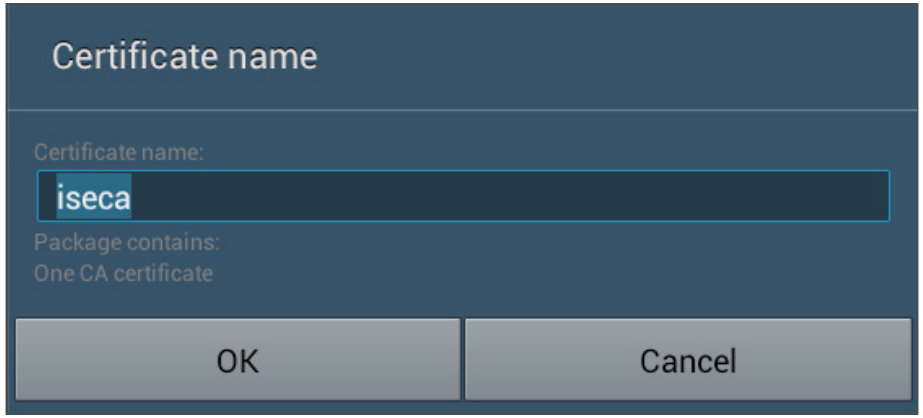
Step 6: Run the setup assistant by clicking **Open**, and then clicking **Start**.



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



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



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**.

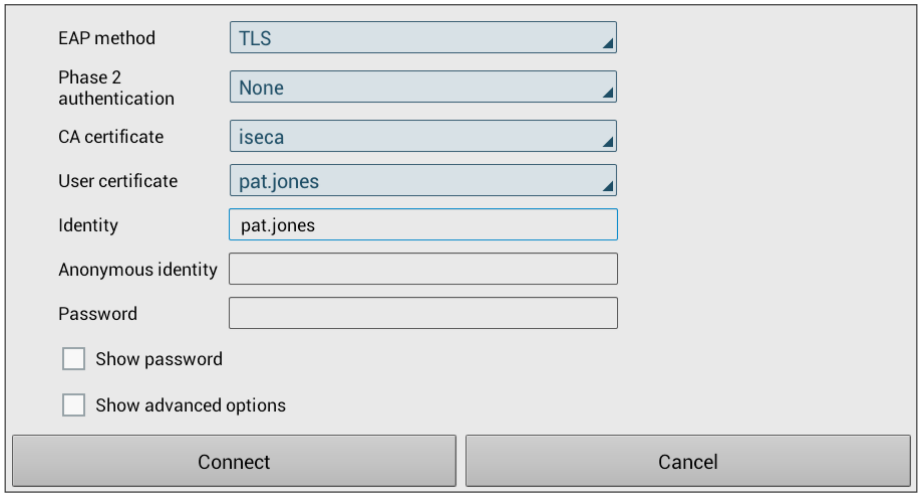
Step 12: Select the network from the list. This allows you to configure the options for connecting.

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**.



Process

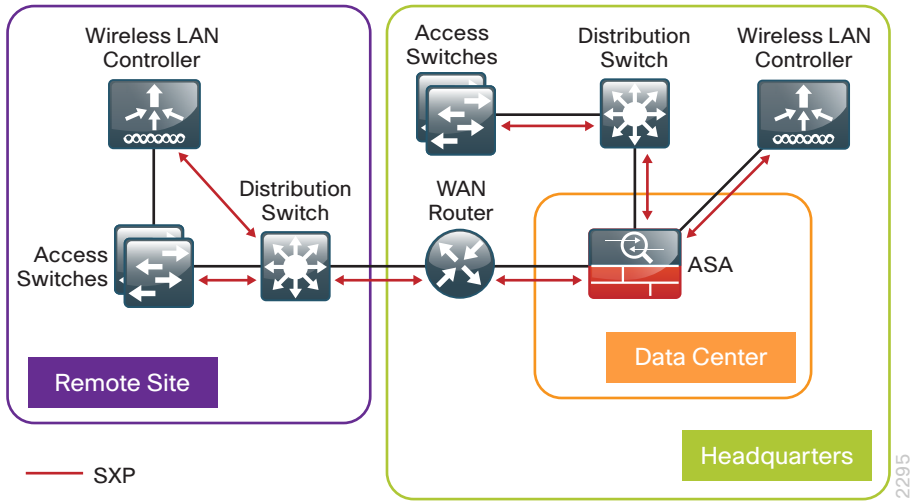
Enabling Security Group Access

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

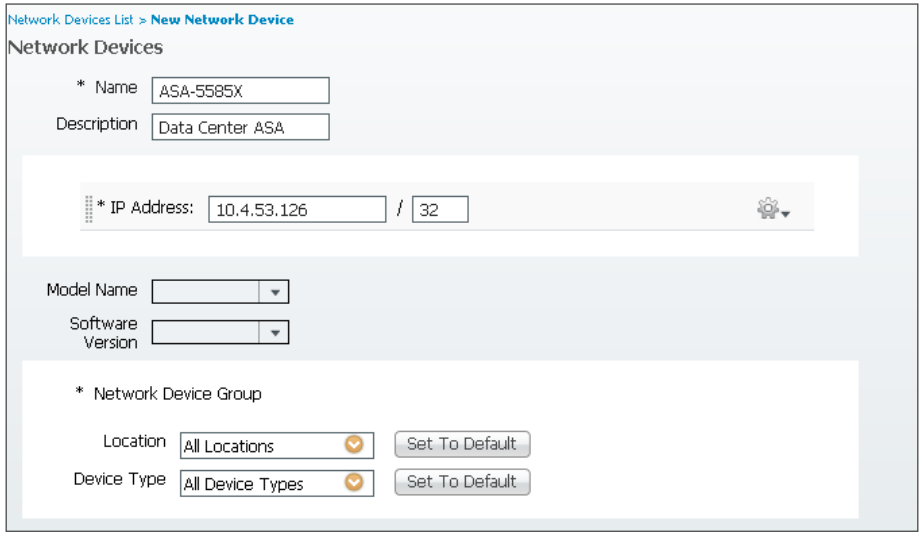
In order to allow Cisco ISE to provide SGT enforcement on Cisco ASA, the ASA appliance needs to be added as a network device in ISE.

Step 1: On the menu bar, mouse over **Administration**, and then in the Network Resources section, choose **Network Devices**.

Step 2: Click **Add**.

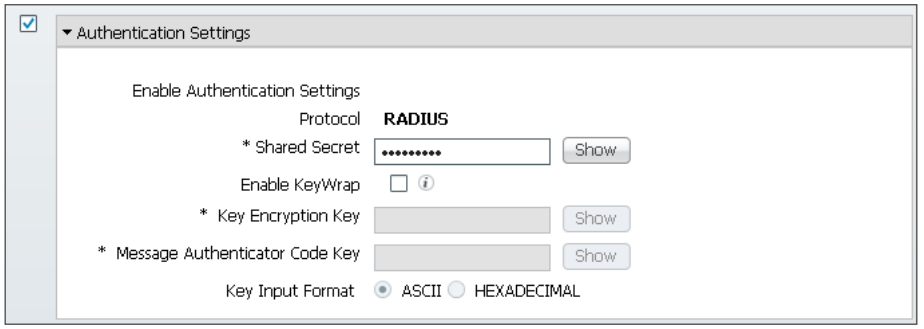
Step 3: Enter the hostname of the ASA appliance and give it a description.

Step 4: For the IP address, enter **10.4.53.126**.



Step 5: Select **Authentication Settings**.

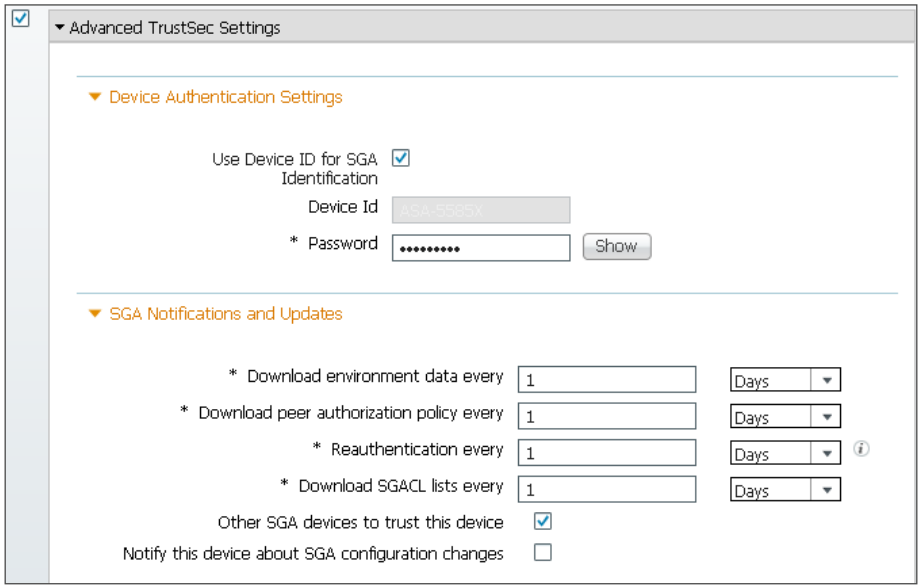
Step 6: Enter the RADIUS shared secret.



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.



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-profile 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 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**.

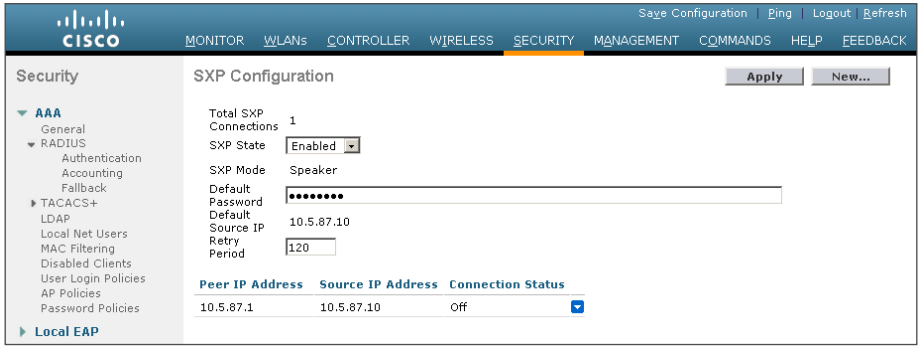
Step 4: In the **SXP State** list, choose **Enabled**.

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**.



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**.

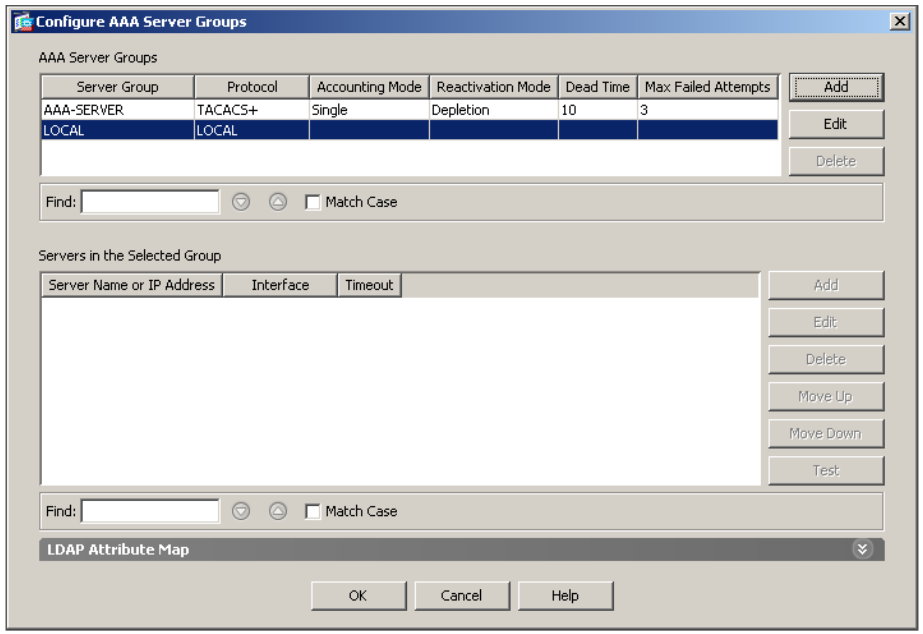
Step 3: Select **Enable SGT Exchange Protocol (SXP)**.

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.

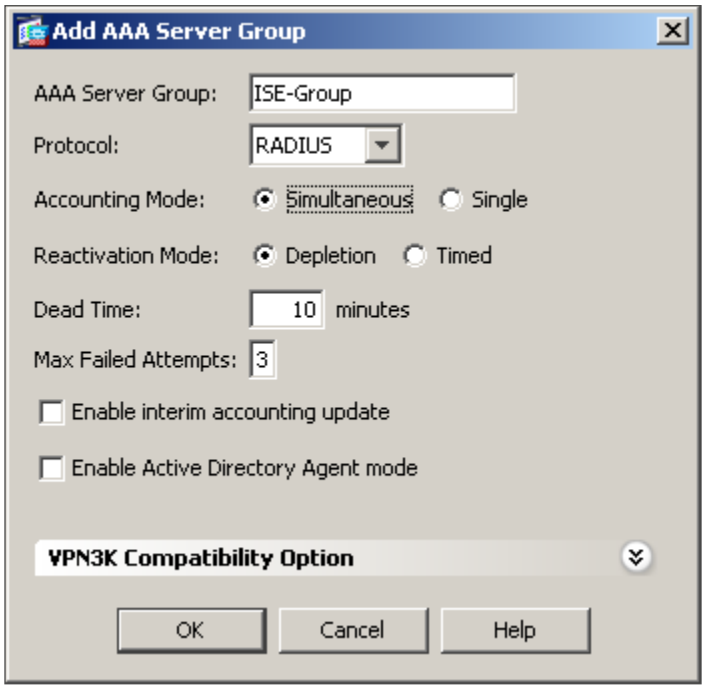
Step 6: In the Server Group Setup section, click **Manage**.

Step 7: In the Configure AAA Server Group window, click **Add**.



Step 8: In the **AAA Server Group** box, enter **ISE-Group**.

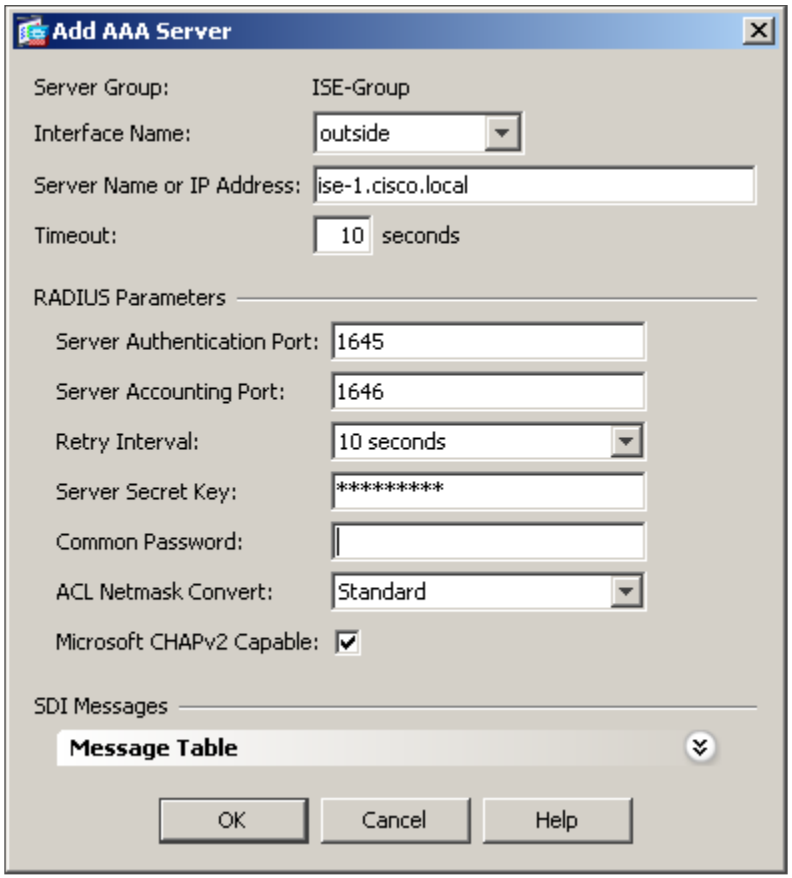
Step 9: For Accounting Mode, select **Simultaneous**, and then click **OK**.



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**.



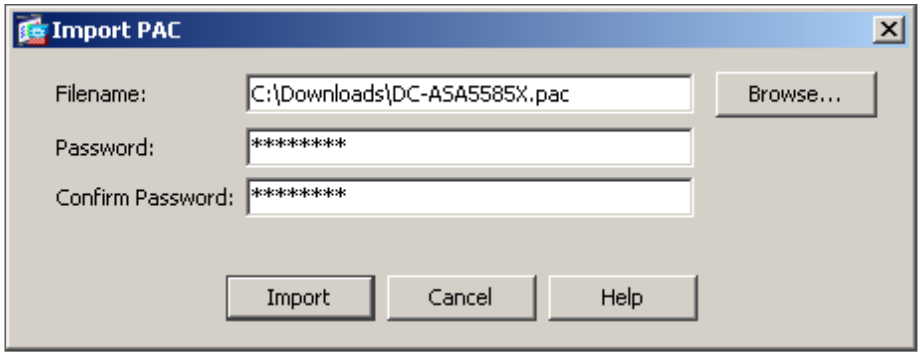
Step 13: Repeat Step 10 through Step 12 for the secondary Cisco ISE administration node, ise-2.cisco.local.

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**.

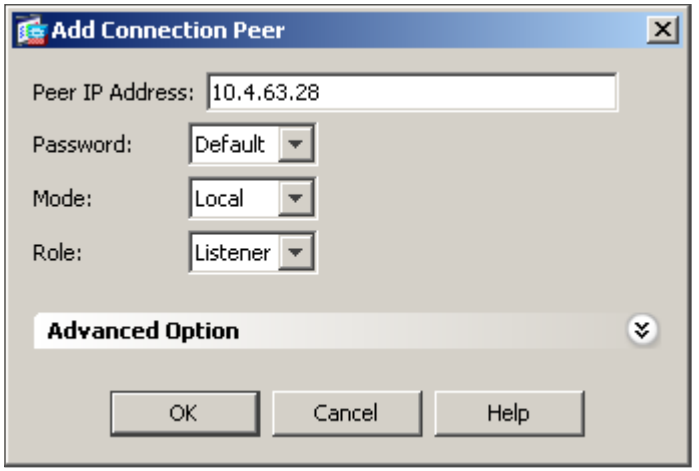


Next, you add SXP peers to Cisco ASA.

Step 18: Click **Add**.

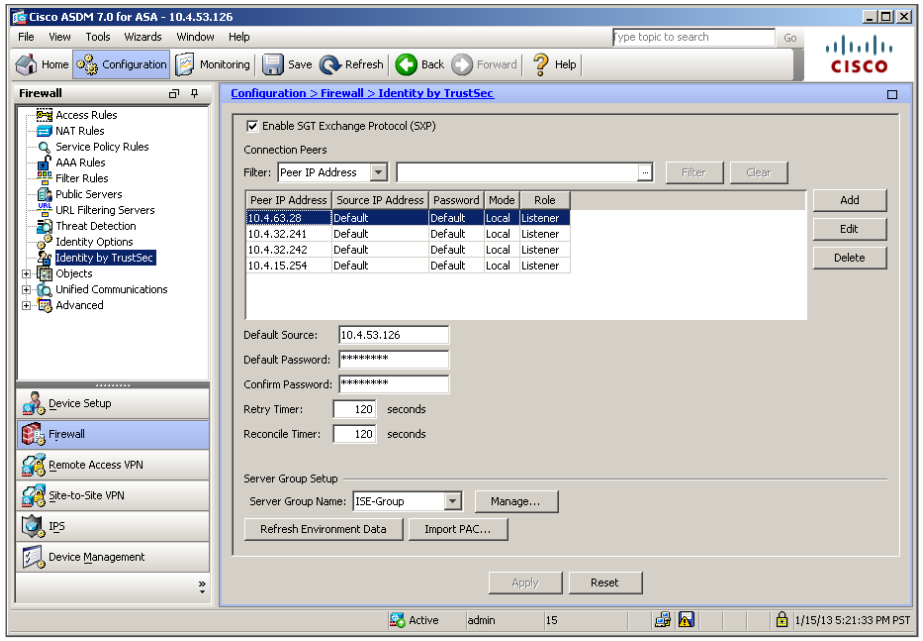
Step 19: Enter the IP address of the peer.

Step 20: For Password, choose **Default**, for Mode, choose **Local**, and for Role, choose **Listener**, and then click **OK**.



Step 21: Repeat Step 18 through Step 20 for each peer you need to add.

Step 22: Click **Apply**.



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**.

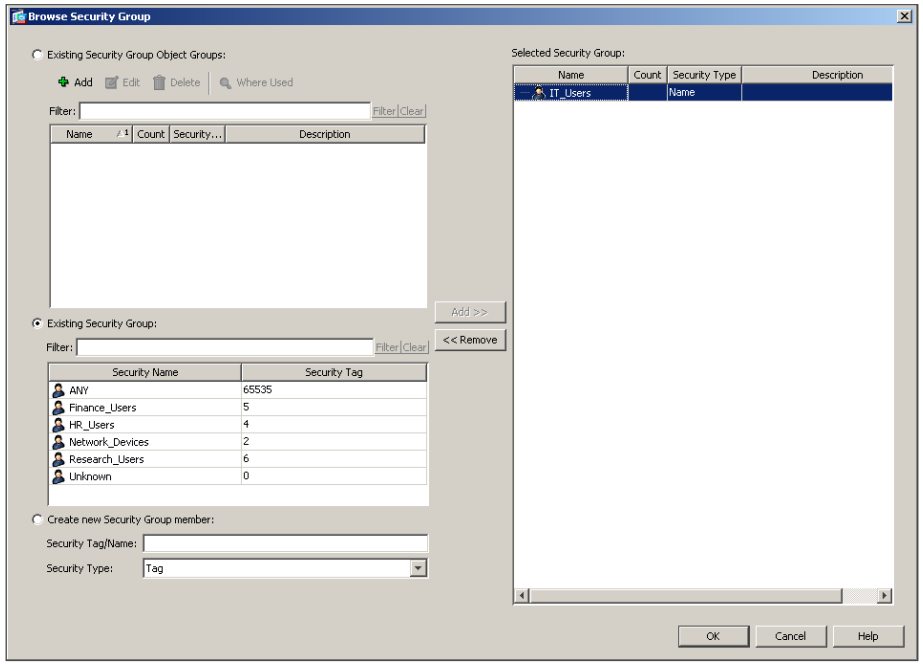
Step 3: From the Interface menu, choose **Any**.

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**.

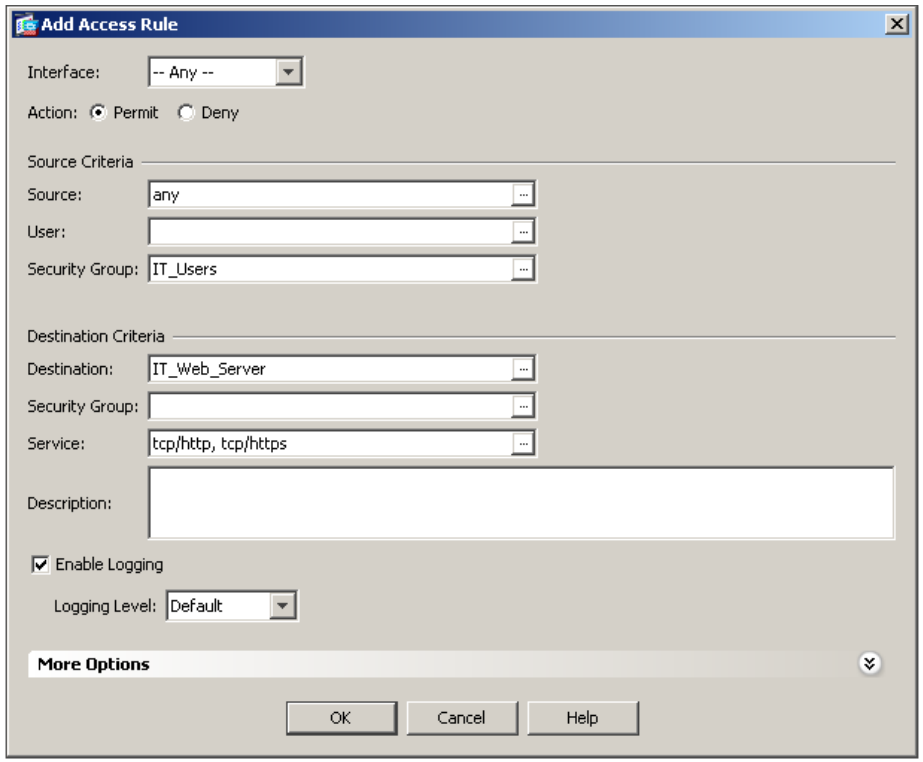


Step 8: Click **OK**. The Add Access Rule window opens.

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.

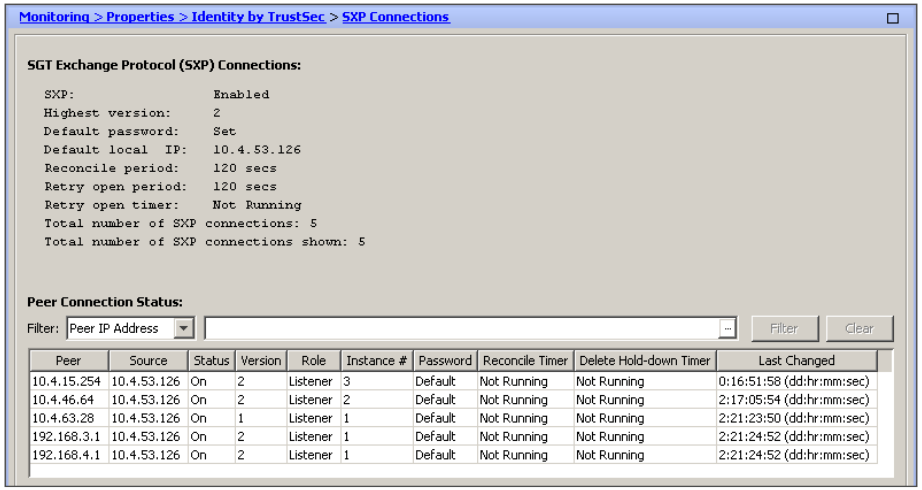


Step 12: Repeat Step 2 through Step 11 for each server that you wish to create an SGT policy for. In this deployment, the remaining groups are Finance, HR, and Research.

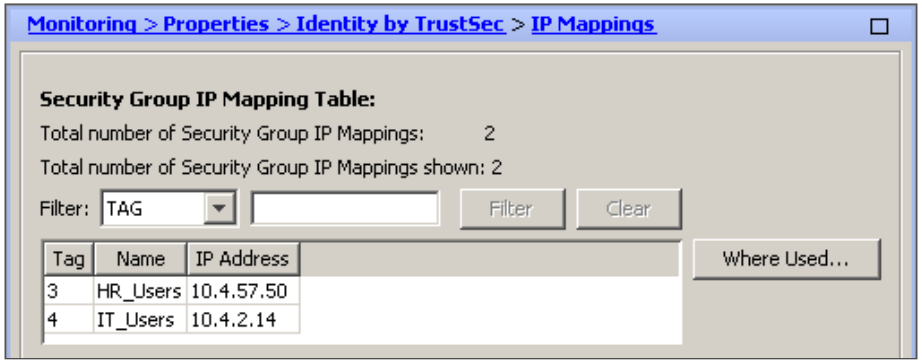
Procedure 9 Monitoring SGTs on Cisco ASA

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.



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.



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: default SXP password
Duration since last 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

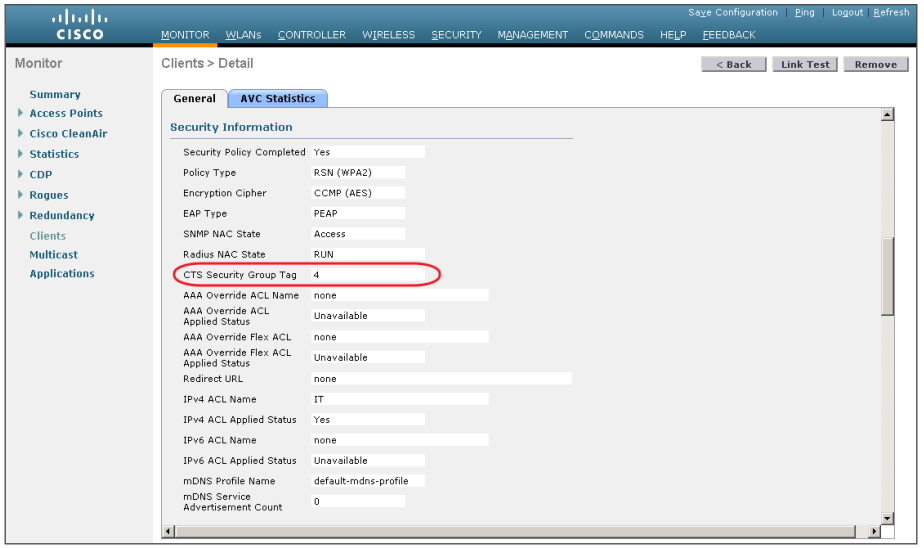
You use the GUI of the WLC to monitor the SGT assignments and SXP connections.

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.

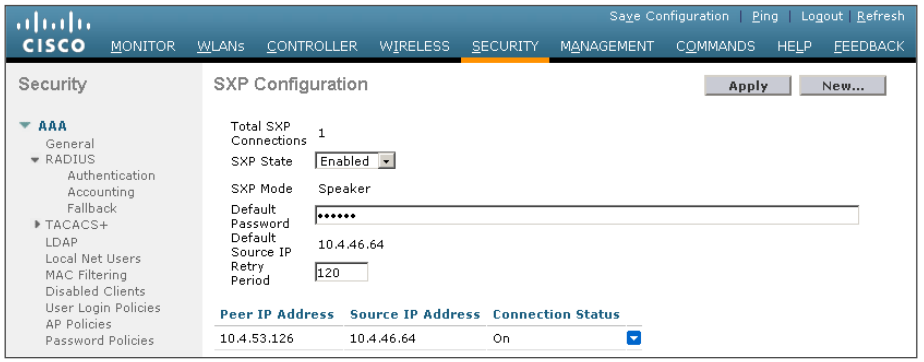
Step 3: Scroll down to the Security Information section.



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**.



Process

Monitoring Network Access

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

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

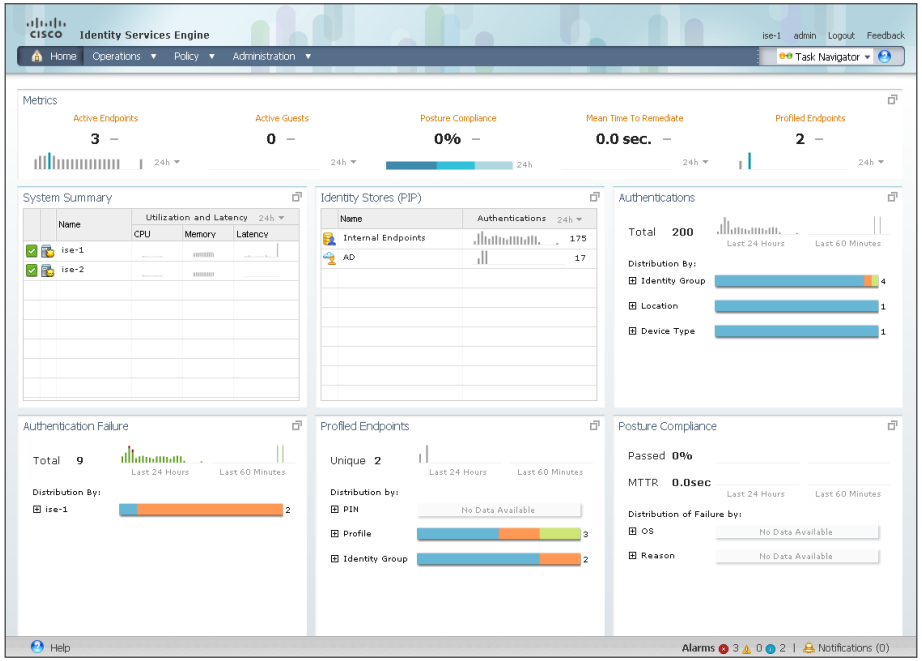
Cisco ISE is now configured to authenticate users and to profile endpoints based on RADIUS and DHCP information. The reporting capabilities of Cisco ISE allow you to determine what type of device is connecting to your network, when it connects, and where it connects from. Also, you will know who is connecting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

Procedure 1 View the Cisco ISE dashboard

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

Step 1: On the menu bar, click **Home**.

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



Procedure 2 Configure identity groups

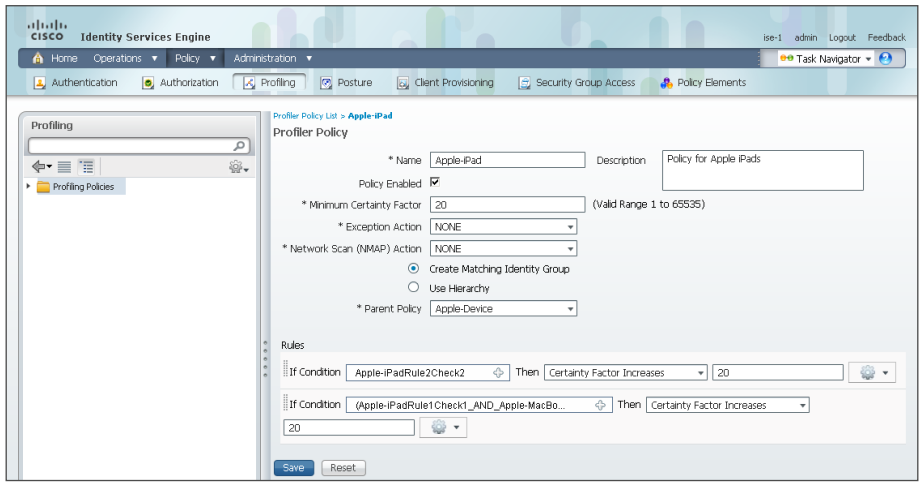
Cisco ISE has more in-depth reporting options to give more details on the devices connecting to the network. To help identify the endpoints, you can use identity groups to classify profiled endpoints and to generate reports.

The example below describes how to do this for an Apple iPad. The procedure for other types of devices is similar.

Step 1: In the menu bar, mouse over **Policy**, and then choose **Profiling**.

Step 2: Click **Apple-iPad.** This enables you to edit this policy.

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



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

Procedure 3 Add a custom profile

Although there are many pre-defined profiles, you may find that a device you want to profile doesn't have an existing profile. You can create a new one 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.

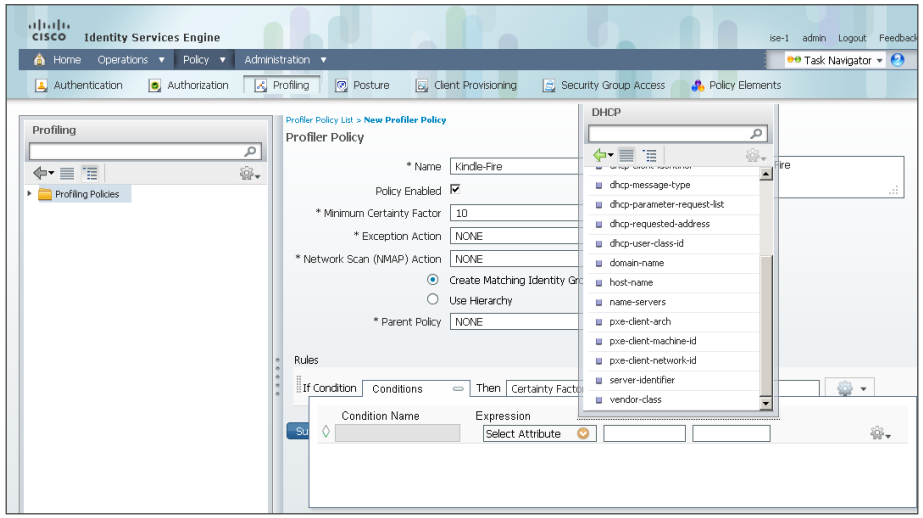
Step 2: Mouse over **Policy**, and then, from the drop-down menu, choose **Profiling**.

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)**.

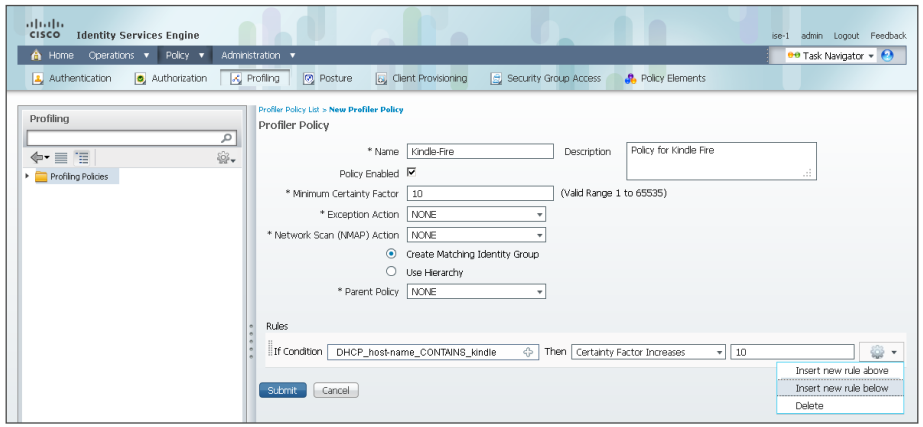
Step 6: In the **Expression** list, next to DHCP, click the **>** symbol, and then choose **host-name**.



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

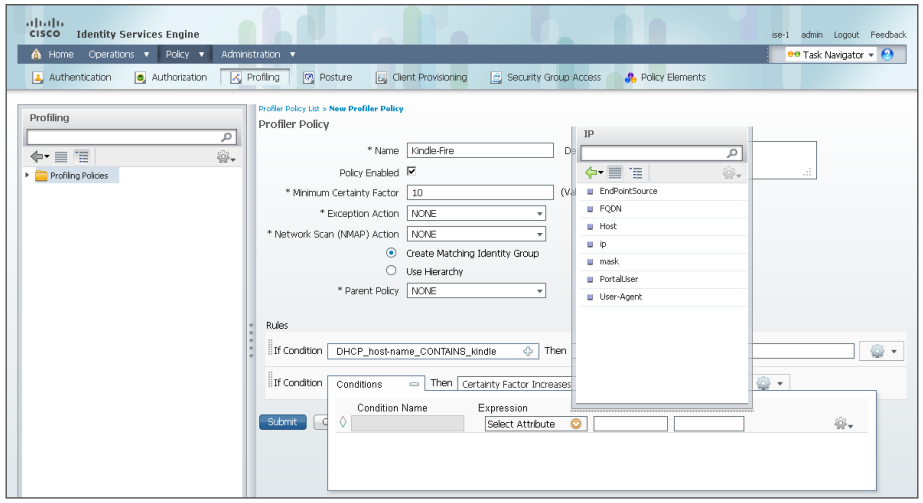
Step 8: Choose **Certainty Factor Increases**, and then set the value to **10**.

Step 9: Click the gear icon at the end of the rule, and then select **Insert new rule below**.



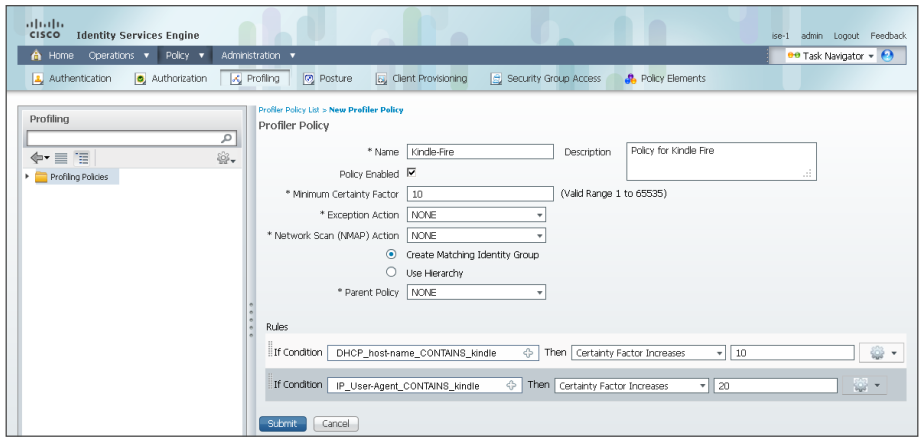
Step 10: Next to Conditions, click the **+** symbol, and then click **Create New Condition (Advance Option)**.

Step 11: In the **Expression** list, next to IP, click the **>** symbol, and then choose **User-Agent**.



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**.



Procedure 4 Examining the authentication log

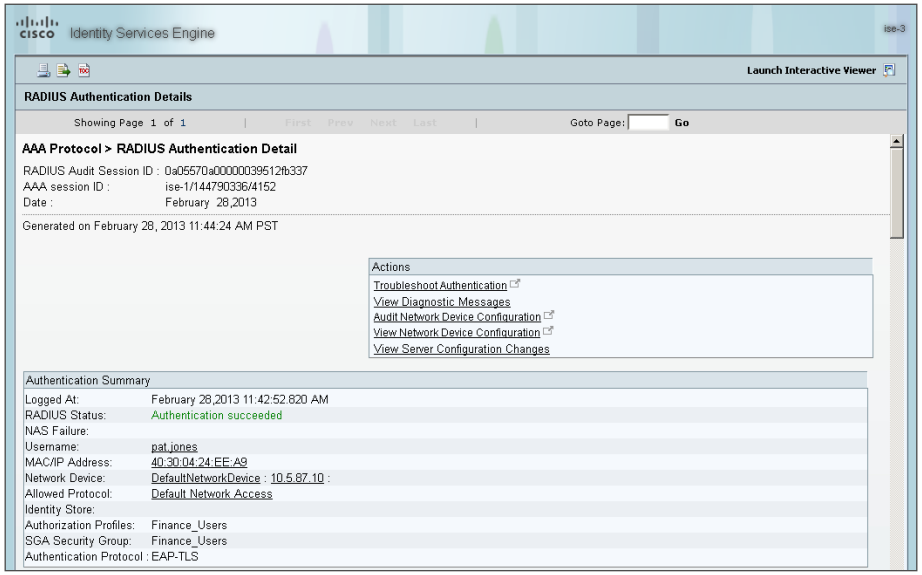
Step 1: On the menu bar, mouse over **Operations**, and then choose **Authentications**. The authentication log displays. The default option is to display the last 20 records from the last 24 hours.

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

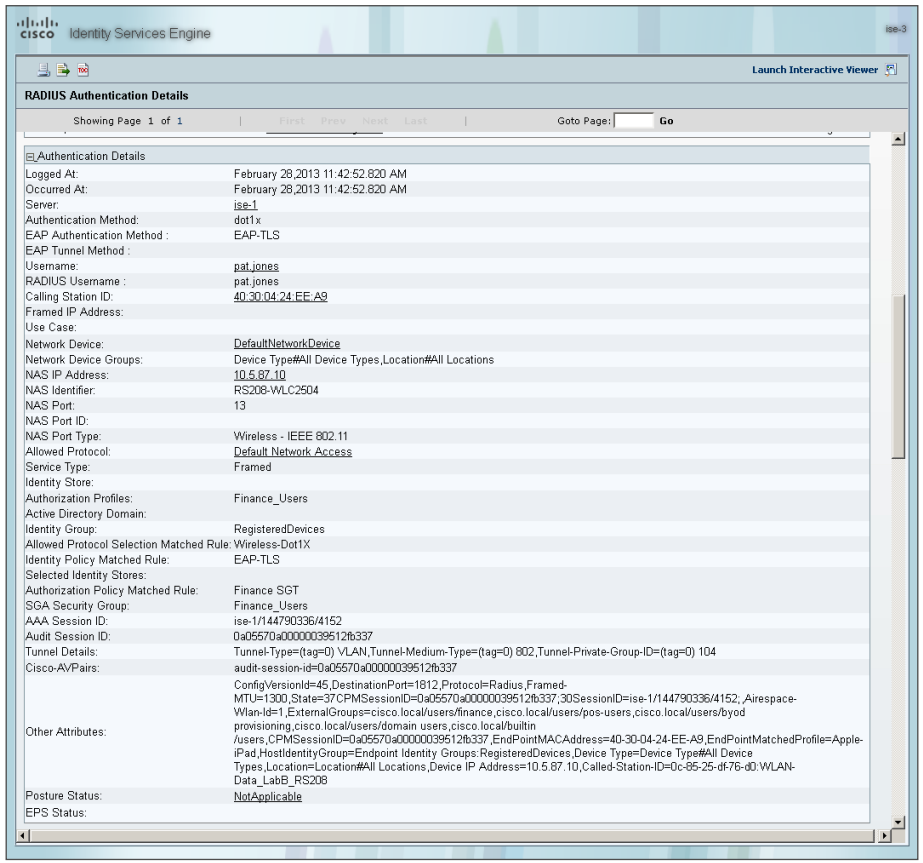
If the device was able to be profiled, that information is displayed.

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.



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



Similar data can be found for endpoints that have authenticated with 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.

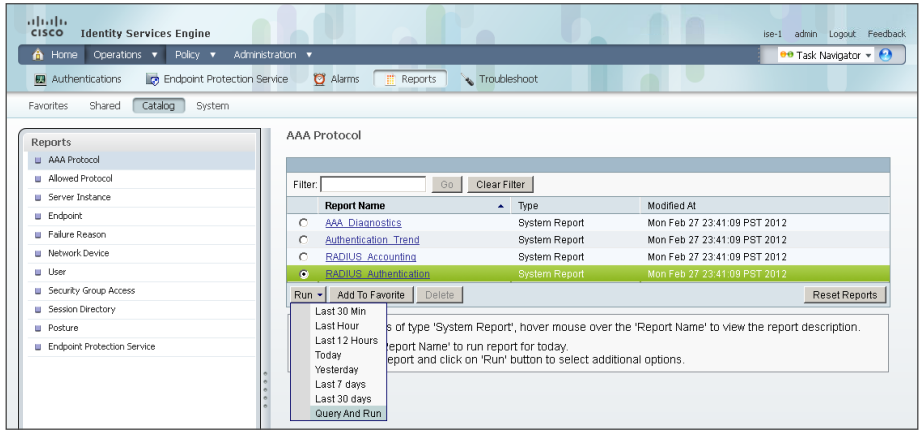
Step 1: On the menu bar, mouse over **Operations**, and then, in the Reports section, choose **Catalog**.

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

Step 3: Select **RADIUS Authentication**.

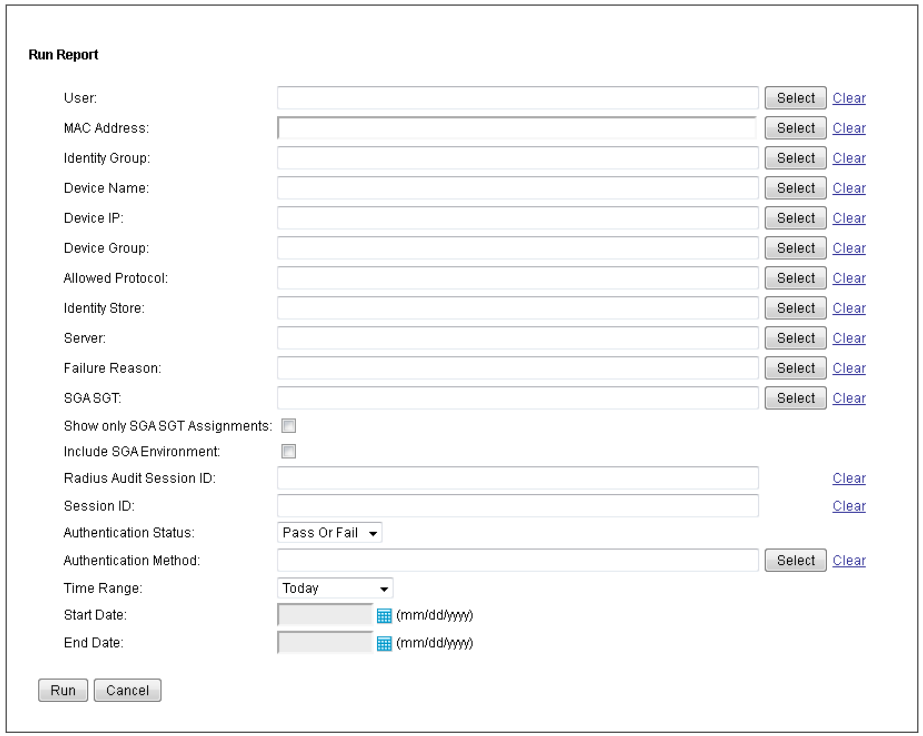
Step 4: Click **Run**. Different time ranges for producing the default report are displayed.

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



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

Figure 2 - RADIUS report parameters



Procedure 6 Identify endpoints

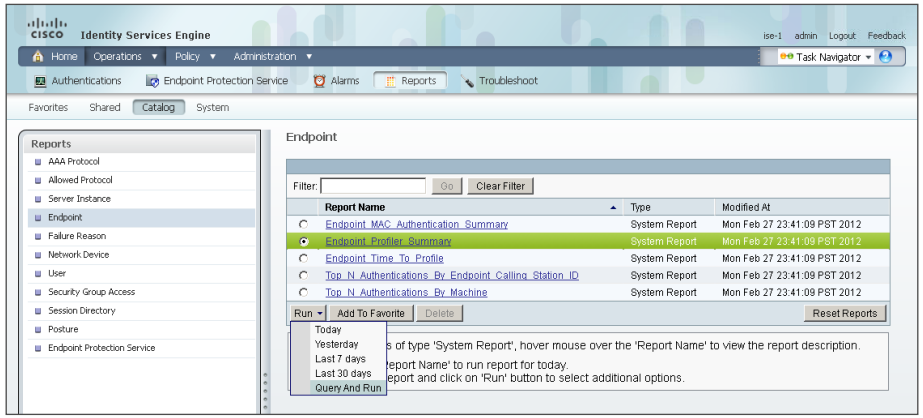
Using information gleaned from the RADIUS and DHCP requests, Cisco ISE can identify what types of devices are connecting to the network. This can assist in determining the network security policy based on the type of device that is in use.

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

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

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

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



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

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

Figure 3 - Endpoint profile summary

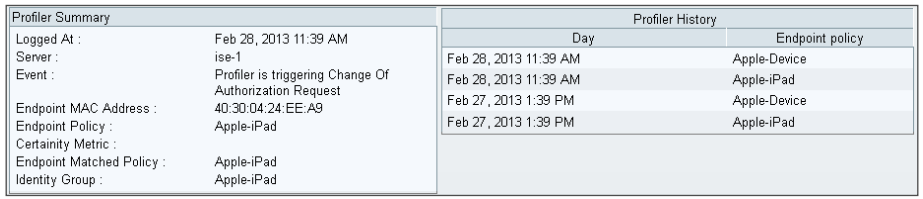


Figure 4 - Endpoint Details

Endpoint > Endpoint Profiler Detail

Generated on February 28, 2013 5:01:30 PM PST

Endpoint Session time : 383.67Seconds

Endpoint Details

Endpoint Static Assignment :	
Endpoint Source :	
Endpoint OUI :	Apple, Inc.
Endpoint Host Name :	
Endpoint Subnet :	
Endpoint NAD Address :	10.5.87.10
Endpoint VLAN :	
Endpoint FQDN :	
Endpoint Nameserver :	
Endpoint Property :	CPMSessionID=0a05570a00000038512fb262 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=00:00:00:00 AuthorizationPolicyMatchedRule=Finance SGT IdentityPolicyMatchedRule=Default MessageCode=3002 attribute-53=00:00:00:00 Acct-Input-Packets=0 Acct-Output-Octets=0 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:0a05570a00000038512fb262; Class=CACS:0a05570a00000038512fb262:ise-1/144790336/4148; Termination-Action=RADIUS-Request; cisco-av-pair=cts:security-group-tag=0005-0; MS-MPPE-Send-Key=56:3c:a1:08:52:72:61:37:a3:4a:b1:f4:72:30:a9:41:f4:56:e8:d3:6c:ad:29:d1:f4:f1:67:05:37:b5:1b:bf; MS-MPPE-Recv-Key=e6:c9:e1:08:1a: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 Called-Station-ID=3c-ce-73-d9-9c-20

Procedure 7 Create device-type reports

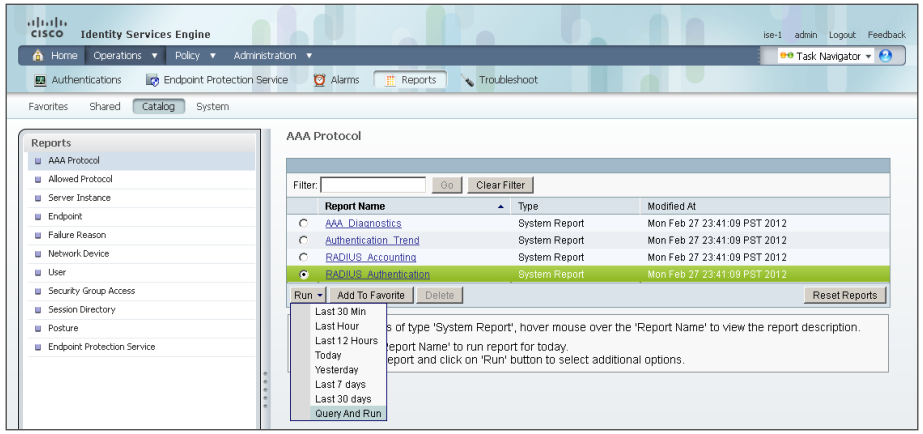
You can create reports to identify specific devices based on the identity groups configured previously. This example uses the group created to identify Apple iPads.

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

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

Step 3: Select **RADIUS Authentication**.

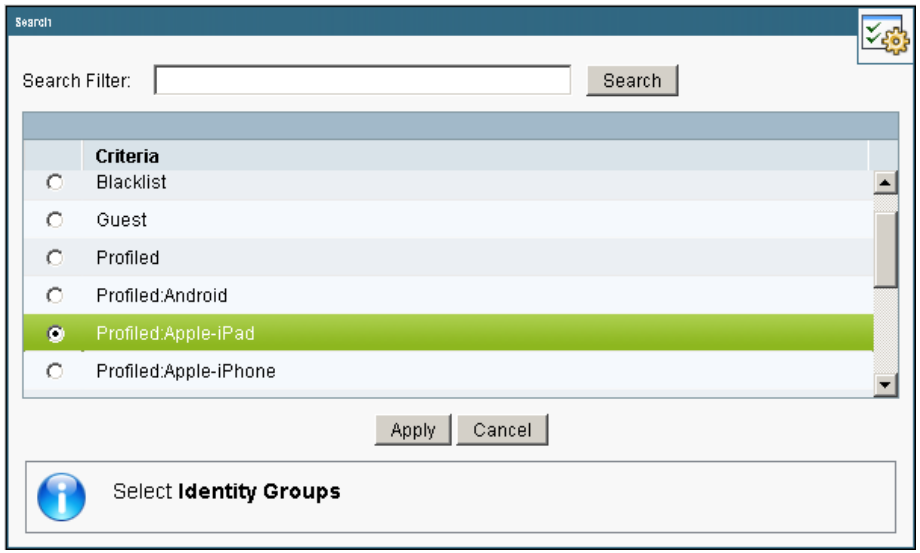
Step 4: Click **Run,** and then choose **Query and Run**.



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

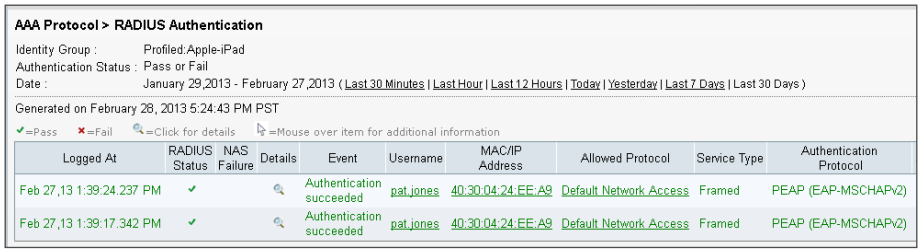
Step 6: Leave the search field empty, and then click **Select**. The search returns all groups.

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



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

Figure 5 - Sample report



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 Switch	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.3.0.SG(15.1-1SG) IP Base license
	Cisco Catalyst 4500 E-Series Supervisor Engine 7L-E	WS-X45-SUP7L-E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+ ports	WS-X4648-RJ45V+E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+,UPoE ports	WS-X4748-UPOE+E	

Functional Area	Product Description	Part Numbers	Software
Stackable Access Layer Switch	Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-48PF-S	15.0(2)SE IP Base license
	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-24P-S	
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
Standalone Access Layer Switch	Cisco Catalyst 3560-X Series Standalone 48 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-48PF-S	15.0(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 Guest Controller	Cisco 5500 Series Wireless Controller for up to 500 Cisco access points	AIR-CT5508-500-K9	7.4.100.0
	Cisco 5500 Series Wireless Controller for up to 250 Cisco access points	AIR-CT5508-250-K9	
	Cisco 5500 Series Wireless Controller for up to 100 Cisco access points	AIR-CT5508-100-K9	
	Cisco 5500 Series Wireless Controller for up to 50 Cisco access points	AIR-CT5508-50-K9	
	Cisco 5500 Series Wireless Controller for up to 25 Cisco access points	AIR-CT5508-25-K9	
	Cisco 5500 Series Wireless Controller for up to 12 Cisco access points	AIR-CT5508-12-K9	
	Cisco 5500 Series Wireless Controller for High Availability	AIR-CT5508-HA-K9	

Functional Area	Product Description	Part Numbers	Software
On Site Controller, Guest Controller	Cisco 2500 Series Wireless Controller for up to 50 Cisco access points	AIR-CT2504-50-K9	7.4.100.0
	Cisco 2500 Series Wireless Controller for up to 25 Cisco access points	AIR-CT2504-25-K9	
	Cisco 2500 Series Wireless Controller for up to 15 Cisco access points	AIR-CT2504-15-K9	
	Cisco 2500 Series Wireless Controller for up to 5 Cisco access points	AIR-CT2504-5-K9	

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	ASA5585-S40P40-K9	ASA 9.0(1) IPS 7.1(6) E4
	Cisco ASA 5585-X Security Plus IPS Edition SSP-20 and IPS SSP-20 bundle	ASA5585-S20P20X-K9	
	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	Nexus 1000V CPU License Qty-1	N1K-VLCPU-01=	4.2(1)SV2(1.1)
	Nexus 1000V VSM on Physical Media	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 self-provisioning 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.

SMART BUSINESS ARCHITECTURE

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

B-0000142-1 4/13