Newer Cisco SBA Guides Available

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

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

SBA

SOLUTIONS

BYOD

BYOD—Virtual Desktop Access Deployment Guide

SMART BUSINESS ARCHITECTURE

August 2012 Series

Preface

Who Should Read This Guide

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

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

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

Release Series

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

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

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

month year Series

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

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

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

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

How to Read Commands

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

Commands to enter at a CLI appear as follows:

```
configure terminal
```

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

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

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

```
Router# enable
```

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

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

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

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

Comments and Questions

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

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

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

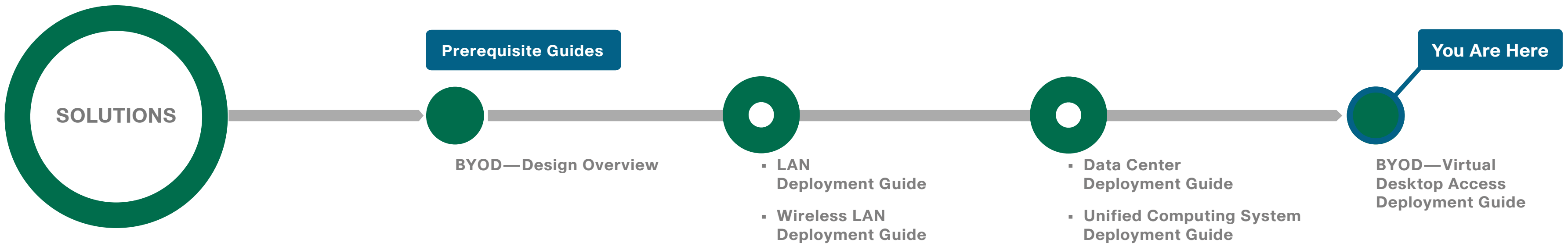
This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- 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


SOLUTIONS
Prerequisite Guides
BYOD—Design Overview
LAN Deployment Guide
Wireless LAN Deployment Guide
Data Center Deployment Guide
Unified Computing System Deployment Guide
You Are Here
BYOD—Virtual Desktop Access Deployment Guide

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 nontraditional devices, such as smart phones and tablets, and people bringing their own devices to access the network, organizations need to know how many of these devices are connecting. With this information, the organization can create policy to prevent connection by nontraditional devices, limit connection to approved devices, or make access to network resources easier for these nontraditional devices. This presents a challenge for IT organizations that seek to provide end-users with a consistent network access experience and the freedom to use any device, while still enforcing stringent security policies to protect corporate intellectual property. Further complicating the situation is delivering both consistent access and enforcing proper security policy based on the specific user-access scenario (wired, wireless, guest, local, branch, and remote users).

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

Other Cisco SBA Solutions guides addressing BYOD business problems include:

- *BYOD—Internal Corporate Access Deployment Guide*
- *BYOD—Identity and Authentication Deployment Guide*
- *BYOD—Advanced Guest Wireless Access Deployment Guide*
- *BYOD—Remote Mobile 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. Future projects will address additional use cases that focus on features that provide for things like device management and Security Group Access (SGA).

Technology Overview

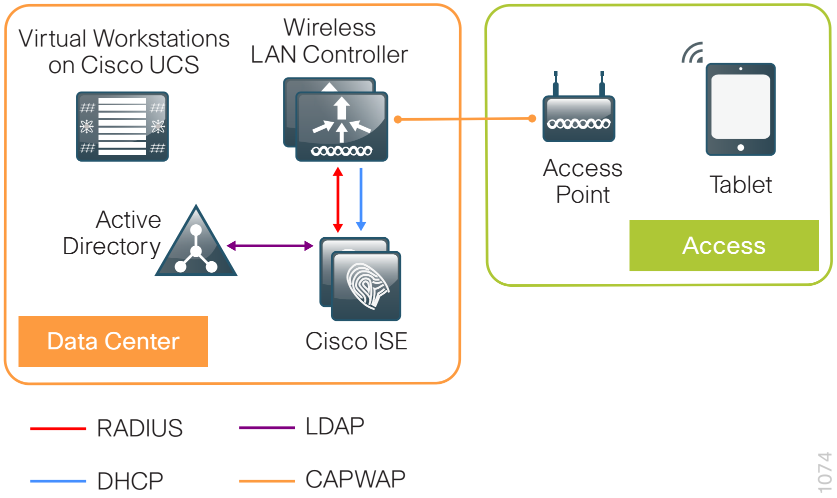
Cisco Identity Services Engine (ISE) is an identity and access control policy platform that enables enterprises to enforce compliance, enhance infrastructure security, and streamline their service operations. Cisco ISE is a core component of Cisco TrustSec. Its architecture allows an organization to 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 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.

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

Figure 1 - BYOD overview



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 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 allows 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 host names

Device	IP address	Host name
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

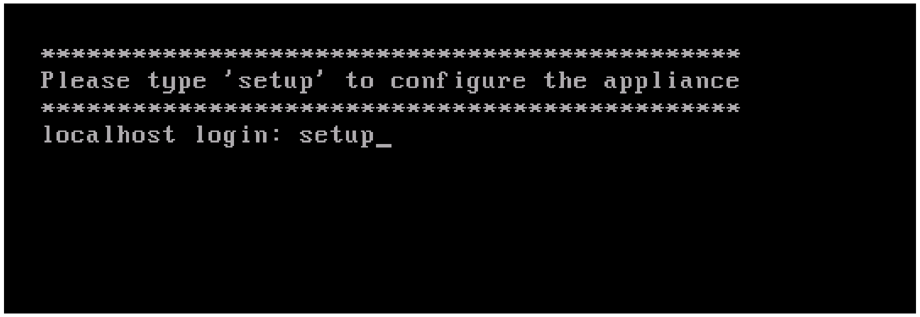
Process

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.



```
**********************************************
Please type 'setup' to configure the appliance
**********************************************
localhost login: setup_
```

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

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

Step 3: Enter DNS information.

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

Step 4: Configure time.

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

Tech Tip

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

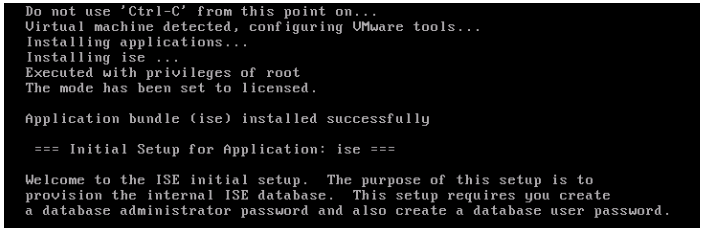
http://www.cisco.com/en/US/docs/security/ise/1.1/cli_ref_guide/ise_cli_app_a.html#wp1571855

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 ends.



```
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

Step 1: The procedure for setting up the remaining engines is the same as when setting up the primary engine, 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**.

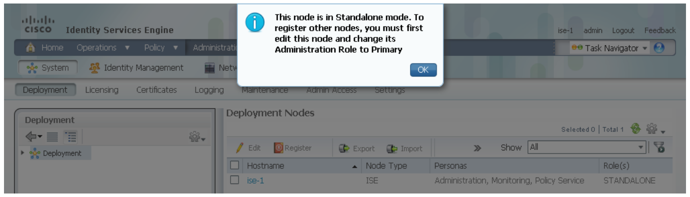
Step 10: Repeat this procedure for the remaining engines, ise-3.cisco.local and ise-4.cisco.local.

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 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**.


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

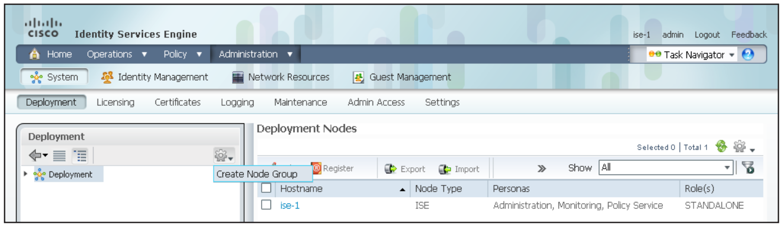
This node is in Standalone mode. To register other nodes, you must first edit this node and change its Administration Role to Primary

Deployment Nodes

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

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

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


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

Deployment Nodes

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

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

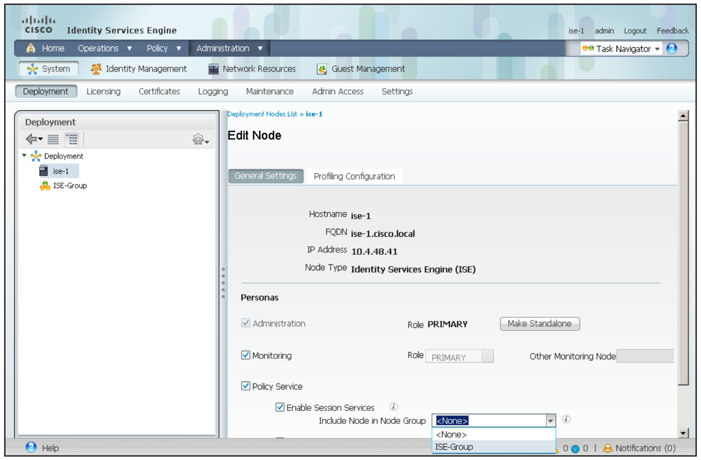
Step 5: A pop-up window lets you know the group was created successfully. Click **OK**.

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**.


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

Edit Node

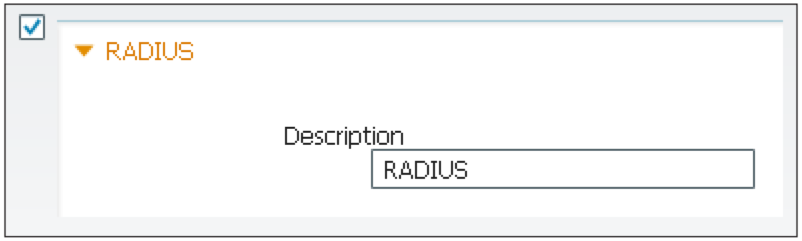
Hostname ise-1
FQDN ise-1.cisco.local
IP Address 10.4.48.41
Node Type Identity Services Engine (ISE)

Personas

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

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

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

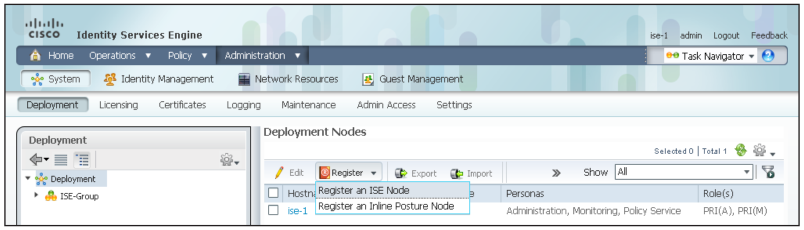


☑ RADIUS

Description RADIUS

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

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


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

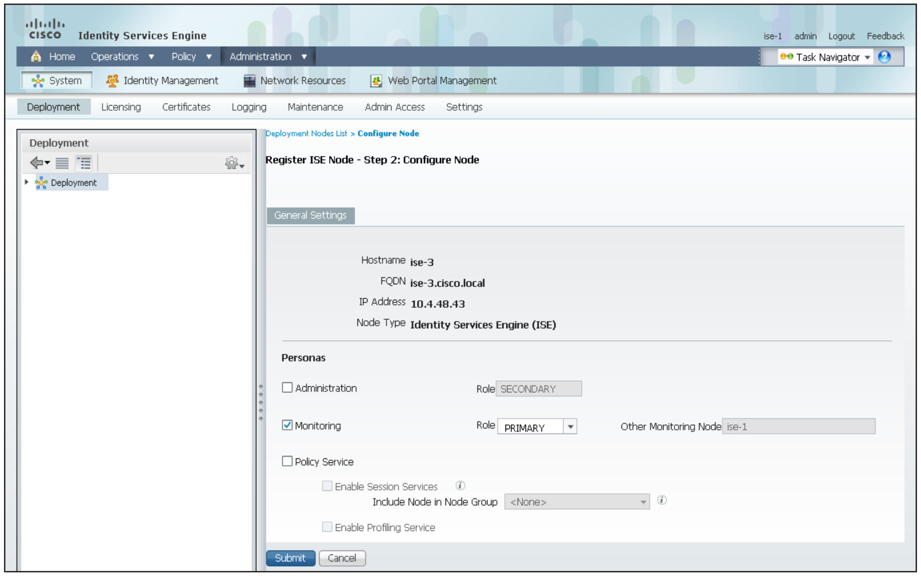
Deployment Nodes

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

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

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

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


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

Register ISE Node - Step 2: Configure Node

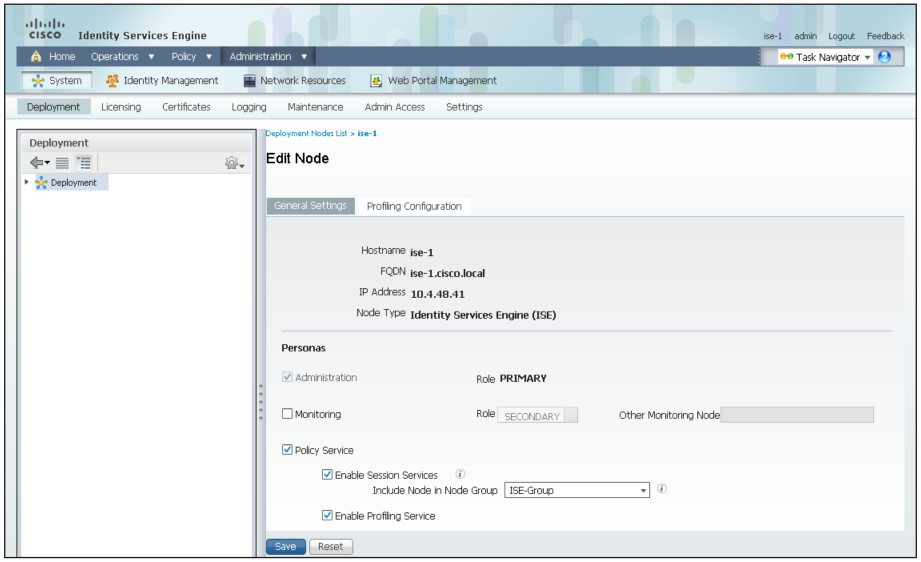
Hostname ise-3
FQDN ise-3.cisco.local
IP Address 10.4.48.43
Node Type Identity Services Engine (ISE)

Personas

□ Administration Role SECONDARY
☑ Monitoring Role PRIMARY Other Monitoring Node ise-1
□ Policy Service
□ Enable Session Services
Include Node in Node Group <None>
□ Enable Profiling Service

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

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


Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
System Identity Management Network Resources Web Portal Management
Deployment Licensing Certificates Logging Maintenance Admin Access Settings
Deployment
Deployment
Deployment Nodes List > ise-1
General Settings Profiling Configuration
Save Reset

Edit Node

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

Personas

☑ Administration Role PRIMARY

☐ Monitoring Role SECONDARY Other Monitoring Node

☑ Policy Service

☑ Enable Session Services
Include Node in Node Group ISE-Group

☑ Enable Profiling Service

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

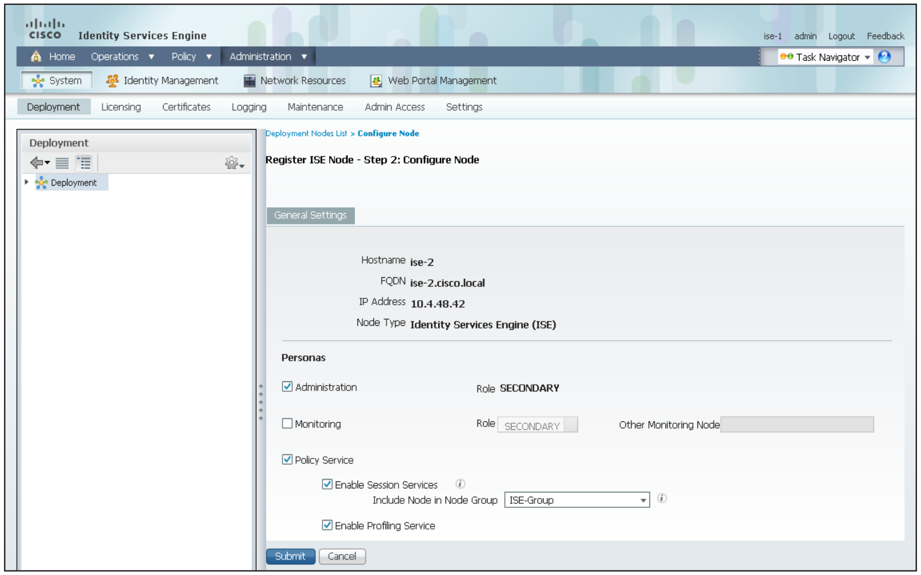
Step 19: In the Deployment Node window, click **Register**, and then choose **Register an ISE Node**.

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

Step 21: Select **Administration** and **Policy Service**.

Step 22: 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**.


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

Register ISE Node - Step 2: Configure Node

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

Personas

☑ Administration Role SECONDARY

☐ Monitoring Role SECONDARY Other Monitoring Node

☑ Policy Service

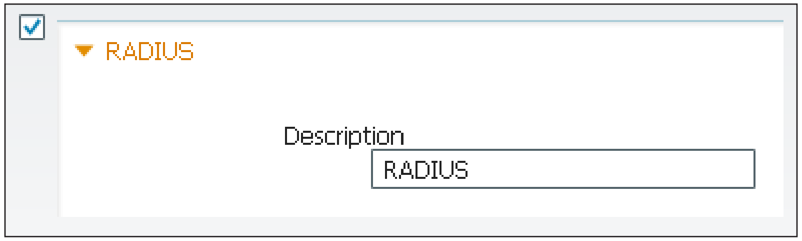
☑ Enable Session Services
Include Node in Node Group ISE-Group

☑ Enable Profiling Service

Step 24: Next, configure which methods are used to profile network endpoints for the secondary policy service node.

Step 25: In the **Deployment Nodes** list, choose **ise-2**.

Step 26: On the Profiling Configuration tab, select **RADIUS**, use the default parameters, and then click **Save**.



☑ RADIUS

Description RADIUS

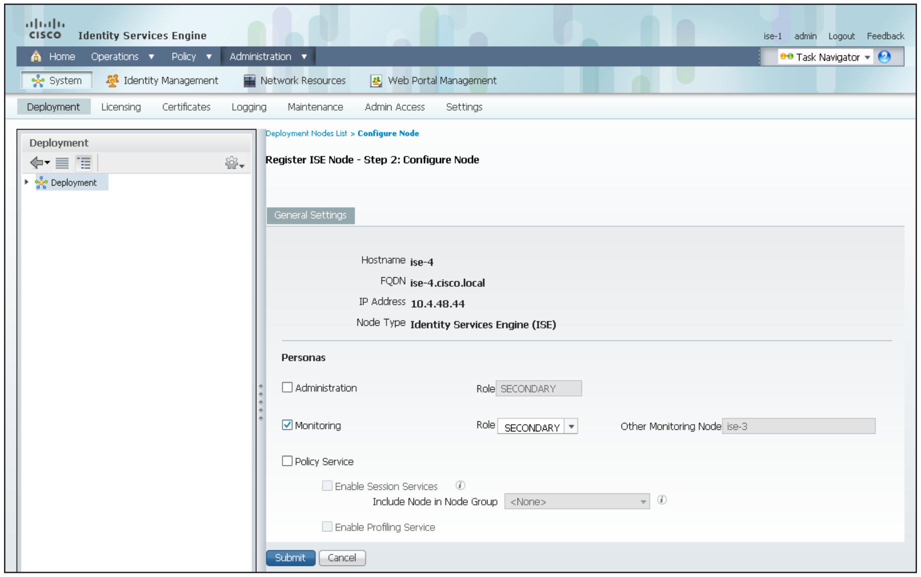
Step 27: In the Edit Node window, click **Deployment Nodes List**. The Deployment Nodes window appears.

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**.


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

Register ISE Node - Step 2: Configure Node

Hostname ise-4
FQDN ise-4.cisco.local
IP Address 10.4.48.44
Node Type Identity Services Engine (ISE)

□ Administration Role SECONDARY
☑ Monitoring Role SECONDARY Other Monitoring Node ise-3
□ Policy Service
□ Enable Session Services
Include Node in Node Group <None>
□ Enable Profiling Service

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

Procedure 5 Install Cisco ISE license

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

Tech Tip

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

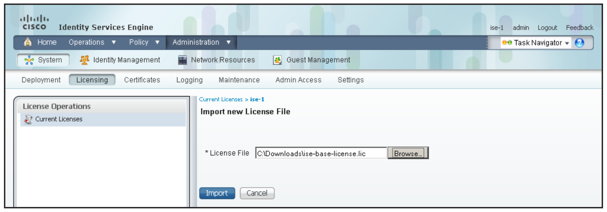
Step 1: Mouse over **Administration**, and then, from the System section of the menu, choose **Licensing**.

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

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

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

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


CISCO Identity Services Engine
ise-1 admin Logout Feedback
Home Operations ▾ Policy ▾ Administration ▾
Task Navigator ▾
System Identity Management Network Resources Guest Management
Deployment Licensing Certificates Logging Maintenance Admin Access Settings
License Operations
Current Licenses
Current Licenses > ise-1
Browse...
Import Cancel

Import new License File

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

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 needs to have this key.

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

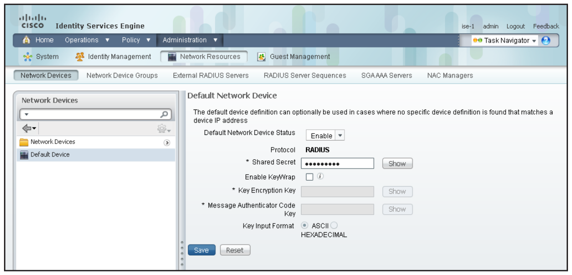
Step 2: In the left pane, click **Default Device**.

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

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

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



Default Network Device

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

Default Network Device Status: Enable

Protocol: RADIUS

* Shared Secret: •••••••••

Enable KeyWrap: □

* Key Encryption Key:

* Message Authenticator Code Key:

Key Input Format: ● ASCII ○ HEXADECIMAL

Procedure 7 Configure Cisco ISE to use Active Directory

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

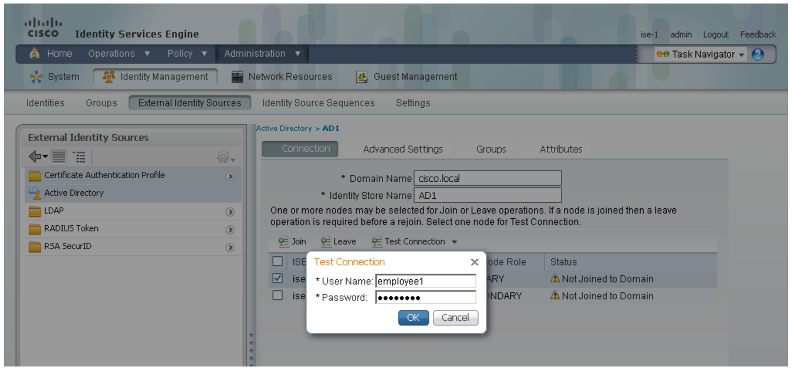
Step 1: Mouse over **Administration**, and then, from the Identity Management section of the menu, choose **External Identity Sources**.

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**.



* Domain Name: cisco.local

* Identity Store Name: AD1

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

Test Connection

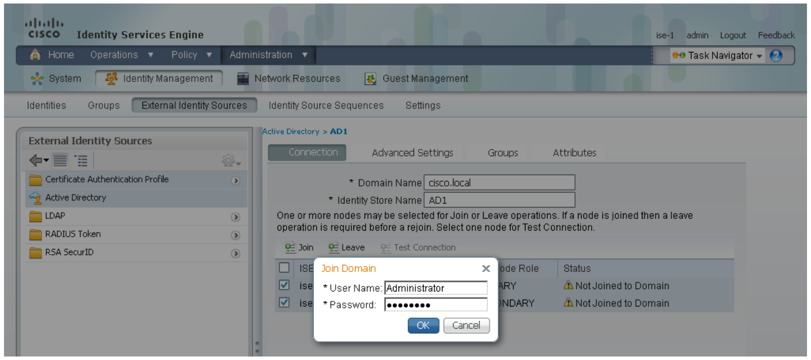
* User Name: employee1

* Password: •••••••••

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.



* Domain Name: cisco.local

* Identity Store Name: AD1

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

Join Domain

* User Name: Administrator

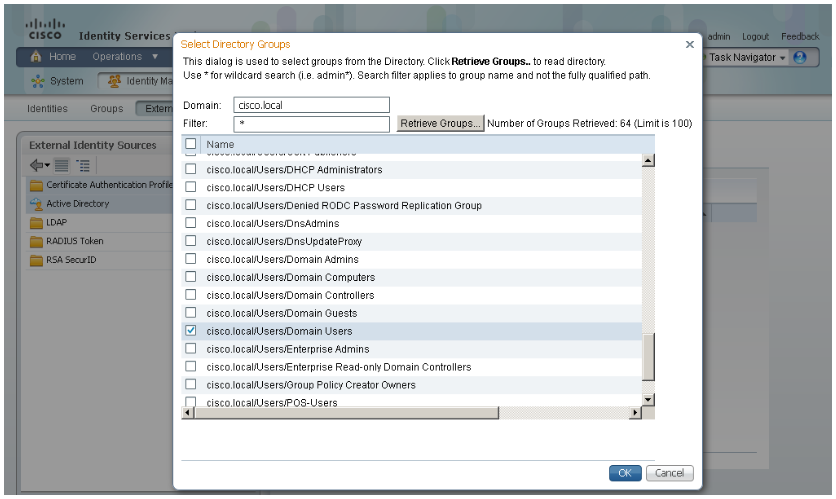
* Password: •••••••••

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

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

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

Step 11: Select the groups you want to use for authentication, and then click **OK**. For example, for all users in the domain, select the group **<domain>/Users/Domain Users**. In this example deployment, you add the groups for **cisco.local/Users/Finance**, **cisco.local/Users/HR**, **cisco.local/Users/IT**, and **cisco.local/Users/Research**.



Select Directory Groups

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

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

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

OK Cancel

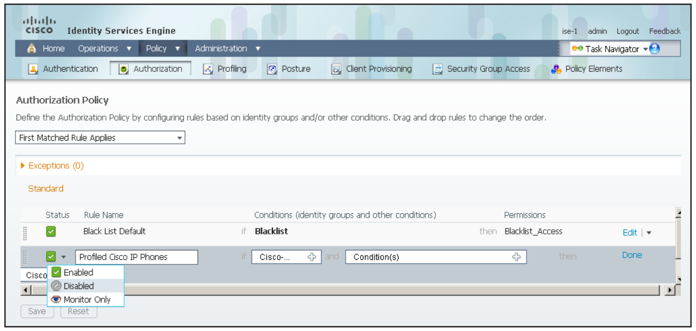
Step 12: Click **Save Configuration**.

Procedure 8 Disable IP Phone authorization policy

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

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

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


cisco Identity Services Engine
ise-1 admin Logout Feedback
Home Operations ▼ Policy ▼ Administration ▼
Task Navigator
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Enabled
Disabled
Monitor Only
Save Reset

Authorization Policy

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

First Matched Rule Applies

Exceptions (0)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
✓	Black List Default	if	**Blacklist**	then	Blacklist_Access	Edit
✓	Profiled Cisco IP Phones	if	Cisco-... and Condition(s)	then		Done

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 DHCP profiling

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

Procedure 1 Configure 802.1X for wireless endpoints

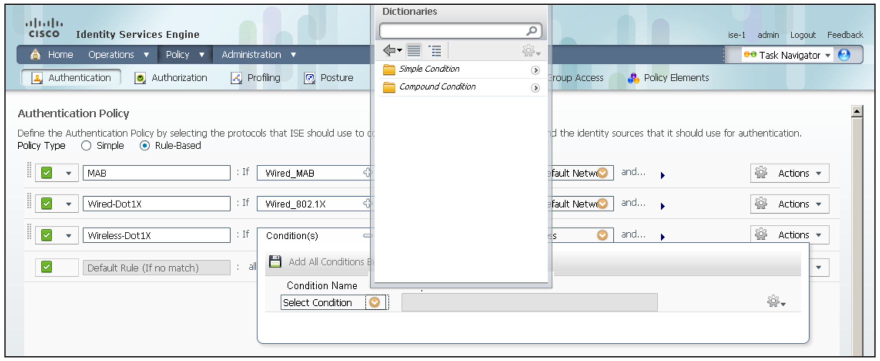
To differentiate wireless users in the authentication logs, create a rule to identify when wireless users authenticate.

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

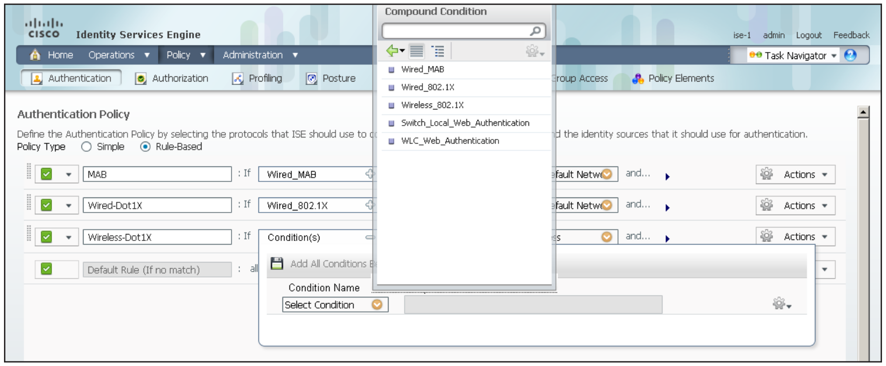
Step 2: For the Default Rule, click the **Actions** button, and then choose **Insert new row above**. A new rule, Standard Policy 1, is created.

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

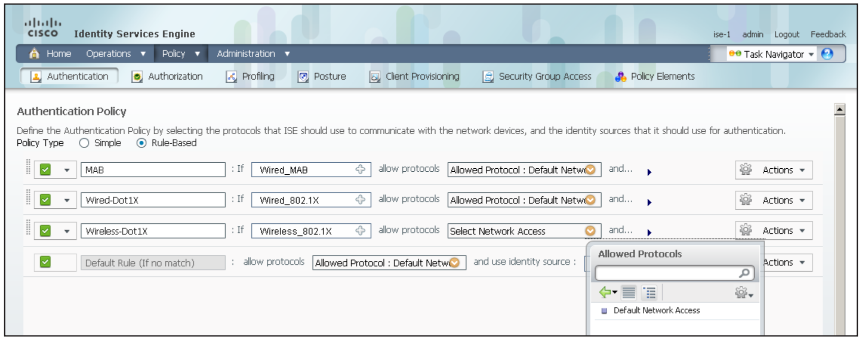
Step 4: In the **Select Condition** list, next to **Compound Condition**, click the **>** symbol.



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**.

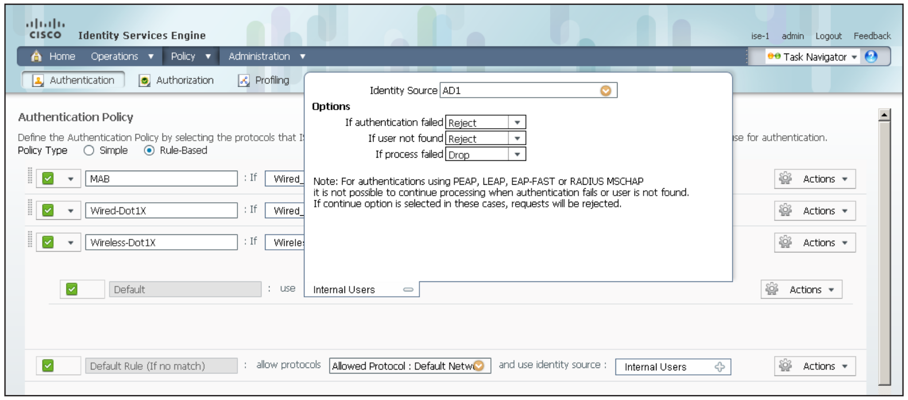

Identity Services Engine
Home
Operations
Policy
Administration
Authentication
Authorization
Profiling
Posture
Client Provisioning
Security Group Access
Policy Elements
Authentication Policy
Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network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

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

Step 8: Next to **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**.


Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
Authentication Authorization Profiling
Authentication Policy
Actions

Define the Authentication Policy by selecting the protocols that I… …se for authentication.

Policy Type ○ Simple ● Rule-Based

☑ MAB : If Wired_…

☑ Wired-Dot1X : If Wired_…

☑ Wireless-Dot1X : If Wirele…

☑ Default : use Internal Users

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

Identity Source AD1

Options

If authentication failed Reject

If user not found Reject

If process failed Drop

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

Procedure 2 Disable EAP-TLS on Cisco ISE

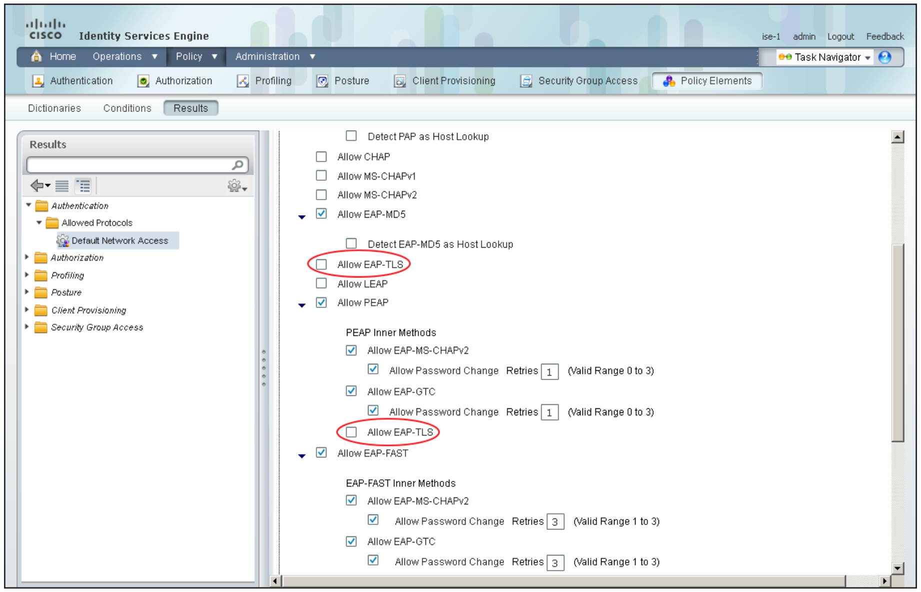
For wireless deployments that aren't currently using digital certificates, you need to disable EAP-TLS in order to allow clients to log in. You will be deploying digital certificates in a later phase of this deployment.

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**.


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

□ Detect PAP as Host Lookup

□ Allow CHAP

□ Allow MS-CHAPv1

□ Allow MS-CHAPv2

☑ Allow EAP-MD5

□ Detect EAP-MD5 as Host Lookup

□ Allow EAP-TLS

□ Allow LEAP

☑ Allow PEAP

PEAP Inner Methods

☑ Allow EAP-MS-CHAPv2

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

☑ Allow EAP-GTC

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

□ Allow EAP-TLS

☑ Allow EAP-FAST

EAP-FAST Inner Methods

☑ Allow EAP-MS-CHAPv2

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

☑ Allow EAP-GTC

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

Procedure 3 Add ISE as RADIUS authentication server

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

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

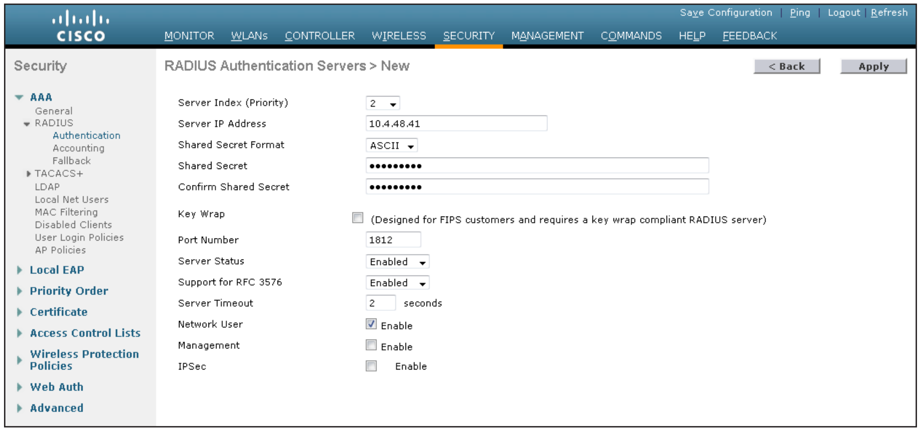
Step 2: On the menu bar, click **Security**.

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

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

Step 5: 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**.



RADIUS Authentication Servers > New

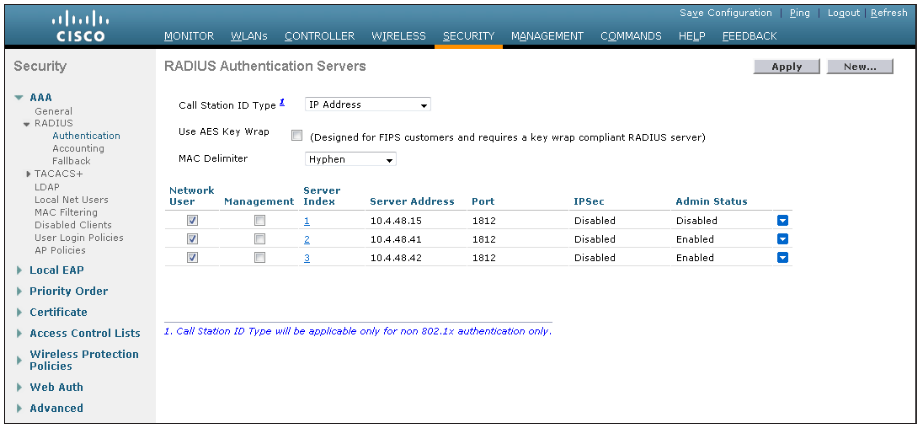
Server Index (Priority)	2
Server IP Address	10.4.48.41
Shared Secret Format	ASCII
Shared Secret	•••••••••
Confirm Shared Secret	•••••••••
Key Wrap	□ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server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

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

Step 8: 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 9: 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 10: On the RADIUS Authentication Servers screen, click **Apply**.



RADIUS Authentication Servers

Call Station ID Type [1]	IP Address
Use AES Key Wrap	□ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
MAC Delimiter	Hyphen

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

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

Procedure 4 Add ISE as RADIUS accounting server

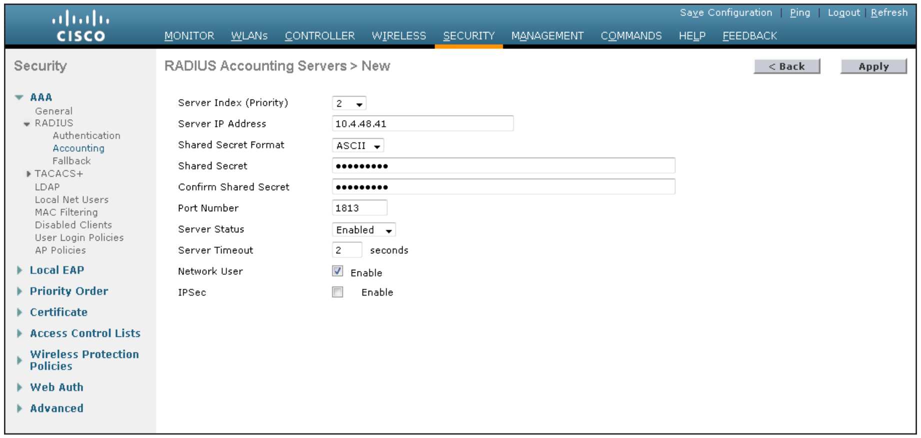
Perform this procedure for every wireless LAN controller (WLC) in the architecture, with the exception of the guest WLC in the DMZ.

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.**



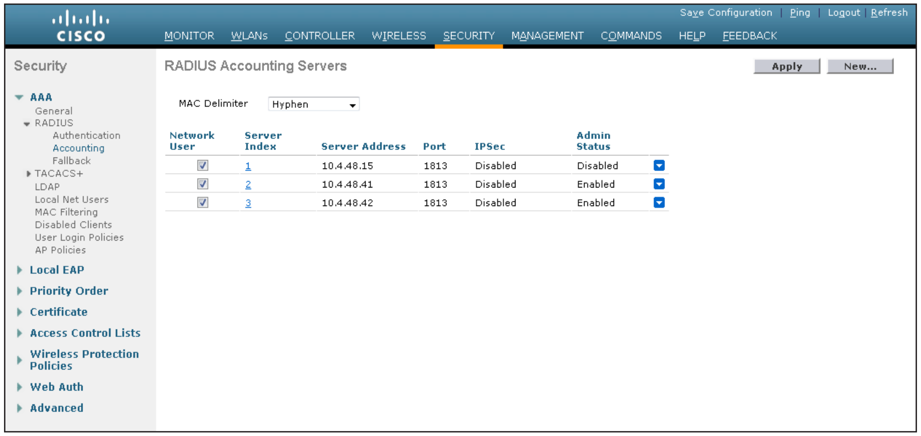
RADIUS Accounting Servers > New

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

Step 5: Repeat Step 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**.



RADIUS Accounting Servers

MAC Delimiter: Hyphen

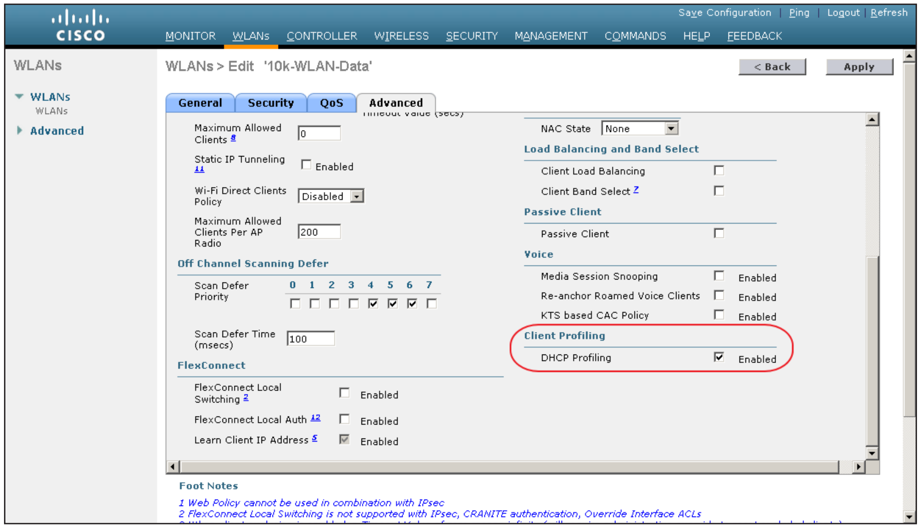
Network User	Server Index	Server Address	Port	IPSec	Admin Status
☑	1	10.4.48.15	1813	Disabled	Disabled
☑	2	10.4.48.41	1813	Disabled	Enabled
☑	3	10.4.48.42	1813	Disabled	Enabled

Procedure 5 Enable DHCP profiling

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

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

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


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General
Security
QoS
Advanced

WLANs > Edit '10k-WLAN-Data'

Maximum Allowed Clients [8]	0
Static IP Tunneling [11]	□ Enabled
Wi-Fi Direct Clients Policy	Disabled
Maximum Allowed Clients Per AP Radio	200

Off Channel Scanning Defer

Scan Defer Priority	0	1	2	3	4	5	6	7
	□	□	□	□	☑	☑	☑	□

Scan Defer Time (msecs): 100

FlexConnect

FlexConnect Local Switching [2]	□ Enabled
FlexConnect Local Auth [12]	□ Enabled
Learn Client IP Address [5]	☑ Enabled

NAC State: None

Load Balancing and Band Select

Client Load Balancing	□
Client Band Select [7]	□

Passive Client

Passive Client	□

Voice

Media Session Snooping	□ Enabled
Re-anchor Roamed Voice Clients	□ Enabled
KTS based CAC Policy	□ Enabled

Client Profiling

DHCP Profiling	☑ Enabled

Foot Notes

1 Web Policy cannot be used in combination with IPsec

2 FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs

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

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

Process

Enabling Authorization

1. Configure identity groups
2. Create profile to deny iPhones
3. Create authorization rule to deny iPhones
4. Create profiles for virtual desktops
5. Create authorization rules for VDI
6. Configure WLC for authorization

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 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 an iPhone. If the user is using an iPad or Android device, the user gets access to the VDI environment and the Internet.

Procedure 1 Configure identity groups

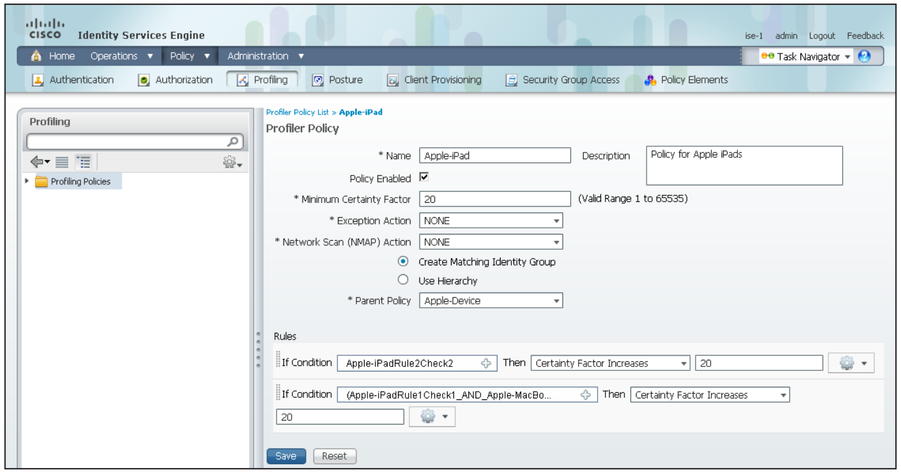
Cisco ISE has more in-depth options to give more details on the devices connecting to the network. To help identify the endpoints, identity groups are used to classify profiled endpoints. You use these identity groups to create authorization policies.

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**.



Profiler Policy

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

Rules

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

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 iPhones

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 iPhone access to the network. This policy is an example and can be modified to suit your environment.

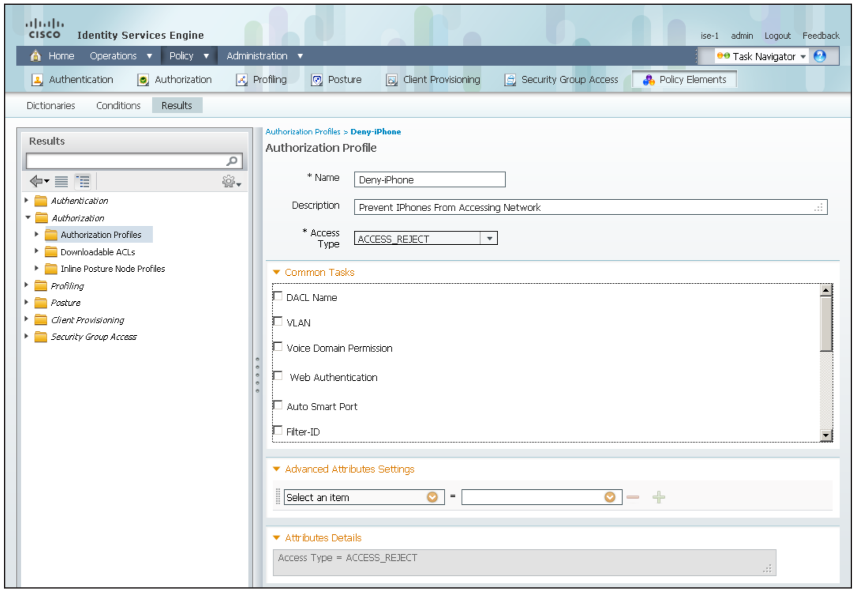
Step 1: On the menu bar, mouse over **Policy**, and then, in the Policy Elements section, choose **Results**.

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**.


Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Dictionaries Conditions Results
Results
Authentication
Authorization
Authorization Profiles
Downloadable ACLs
Inline Posture Node Profiles
Profiling
Posture
Client Provisioning
Security Group Access
Authorization Profiles > Deny-iPhone

Authorization Profile

* Name: Deny-iPhone

Description: Prevent IPhones From Accessing Network

* Access Type: ACCESS_REJECT

Common Tasks

□ DACL Name

□ VLAN

□ Voice Domain Permission

□ Web Authentication

□ Auto Smart Port

□ Filter-ID

Advanced Attributes Settings

Select an item =

Attributes Details

Access Type = ACCESS_REJECT

Procedure 3 Create authorization rule to deny iPhones

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 iPhones."

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

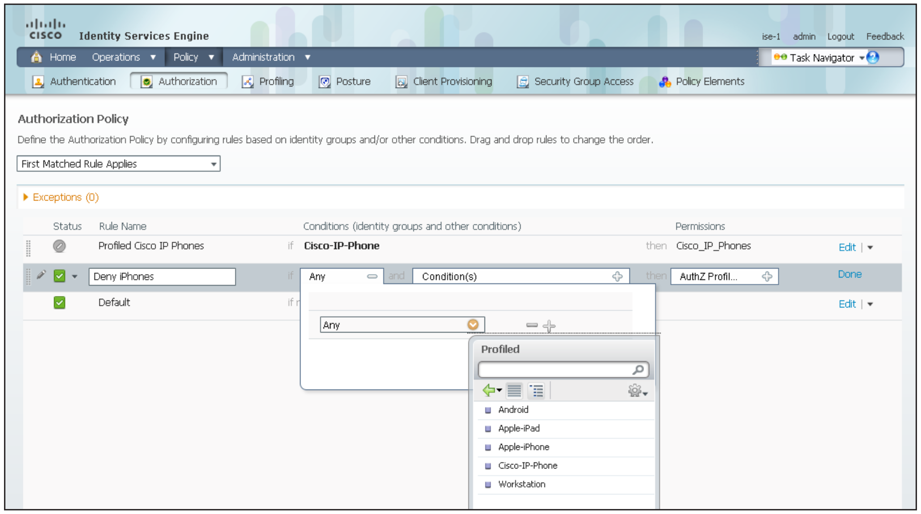
Step 2: At the end of the Default Rule, click the arrow, and then choose **Insert new rule above**. A new rule, "Standard Rule 1," is created.

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

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 **Apple-iPhone**.


Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Edit
Done
Profiled
Android
Apple-iPad
Apple-iPhone
Cisco-IP-Phone
Workstation

Authorization Policy

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

First Matched Rule Applies

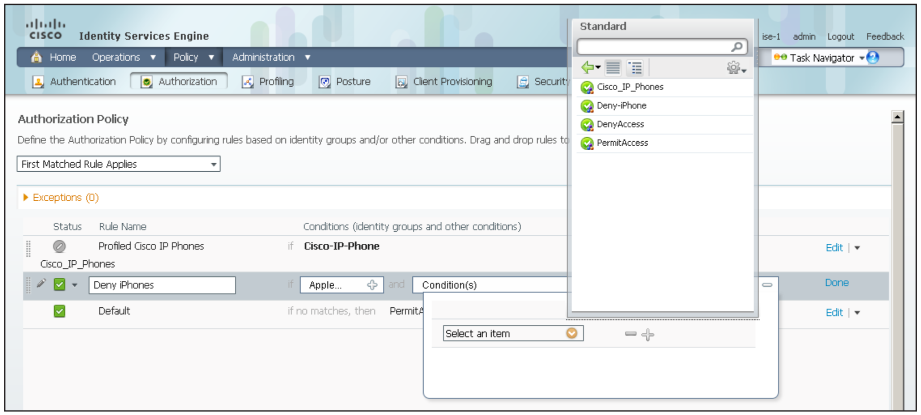
Exceptions (0)

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
	Profiled Cisco IP Phones	if	Cisco-IP-Phone	then	Cisco_IP_Phones
☑	Deny iPhones	if	Any and Condition(s)	then	AuthZ Profil...
☑	Default	if n			

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-iPhone authorization profile that was created in Procedure 2, "Create profile to deny iPhones."


Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
Authentication Authorization Profiling Posture Client Provisioning Securit
Standard
Cisco_IP_Phones
Deny-iPhone
DenyAccess
PermitAccess
Edit
Done
Select an item

Authorization Policy

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

First Matched Rule Applies

Exceptions (0)

Status	Rule Name		Conditions (identity groups and other conditions)
	Profiled Cisco IP Phones Cisco_IP_Phones	if	Cisco-IP-Phone
☑	Deny iPhones	if	Apple... and Condition(s)
☑	Default	if no matches, then	PermitA

Step 10: Click **Done**, and then click **Save**.

Procedure 4 Create profiles for virtual desktops

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. In this procedure, it is assumed that you have deployed a Virtual Desktop Infrastructure (VDI). The policy in this procedure pushes an access list to the WLC that allows access only to the VDI infrastructure and the Internet for users who are using either an iPad or an Android device. The access list can be deployed only 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.

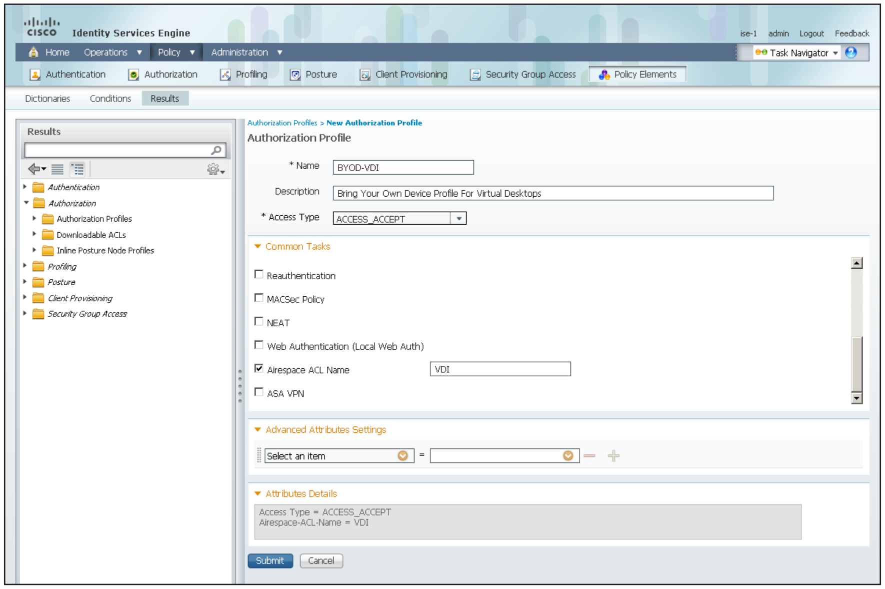
Step 1: On the menu bar, mouse over **Policy**, and then, in the Policy Elements section, choose **Results**.

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-VDI) and a description for the policy.

Step 5: 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 "VDI."



Identity Services Engine
ise-1 admin Logout Feedback
Home Operations ▾ Policy ▾ Administration ▾
Task Navigator ▾
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Dictionaries Conditions Results
Results
Authentication
Authorization
Authorization Profiles
Downloadable ACLs
Inline Posture Node Profiles
Profiling
Posture
Client Provisioning
Security Group Access
Authorization Profiles > New Authorization Profile
Authorization Profile
Common Tasks
Advanced Attributes Settings
Select an item
Attributes Details
Submit
Cancel

* Name: BYOD-VDI

Description: Bring Your Own Device Profile For Virtual Desktops

* Access Type: ACCESS_ACCEPT

□ Reauthentication

□ MACSec Policy

□ NEAT

□ Web Authentication (Local Web Auth)

☑ Airespace ACL Name: VDI

□ ASA VPN

```
Access Type = ACCESS_ACCEPT
Airespace-ACL-Name = VDI
```

Step 6: Click **Submit**.

Procedure 5 Create authorization rules for VDI

The following steps describe how to create an authorization rule that uses the profile created in Procedure 4, "Create profiles for virtual desktops."

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 VDI.

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

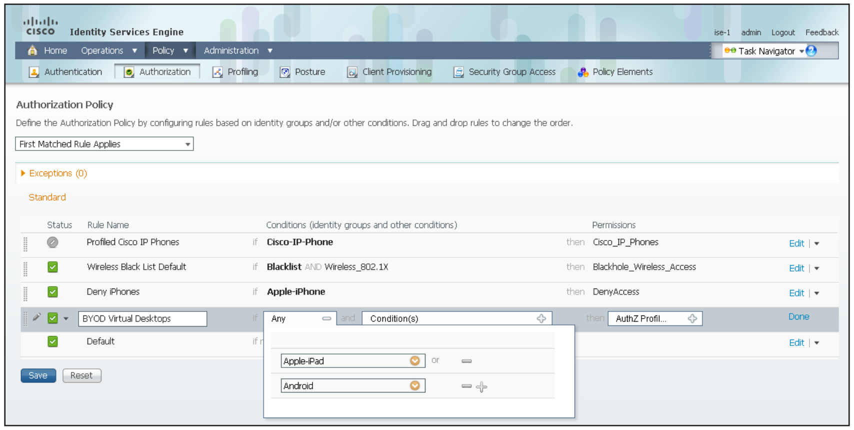
Step 5: In the list, next to Endpoint Identity Groups, choose the **>** symbol.

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**.


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

Authorization Policy

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

First Matched Rule Applies

Exceptions (0)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones	Edit
✓	Wireless Black List Default	if	**Blacklist** AND Wireless_802.1X	then	Blackhole_Wireless_Access	Edit
✓	Deny iPhones	if	**Apple-iPhone**	then	DenyAccess	Edit
✓	BYOD Virtual Desktops	if	Any and Condition(s)	then	AuthZ Profil...	Done
✓	Default	if r				Edit

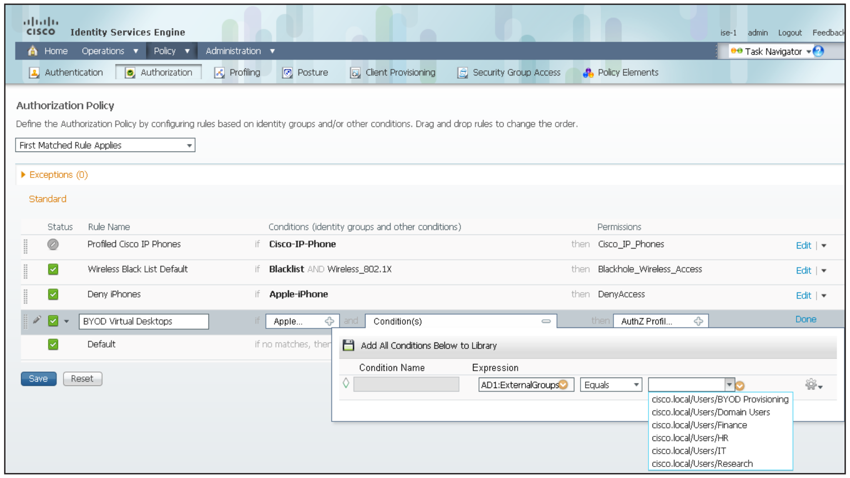
Apple-iPad or
Android

Step 10: In the **Condition(s)** list, click the **+** symbol, and then click **Create New Condition (Advance Option)**.

Step 11: Under Expression, next to Select Attribute, click the arrow. The menu opens.

Step 12: Next to AD1, click the > symbol, and then choose **ExternalGroups**.

Step 13: In the first drop-down list, choose **Equals**, and then, in the second drop-down list, choose **cisco.local/Users/Domain Users**.


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

Authorization Policy

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

First Matched Rule Applies

Exceptions (0)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones	Edit
✓	Wireless Black List Default	if	**Blacklist** AND Wireless_802.1X	then	Blackhole_Wireless_Access	Edit
✓	Deny iPhones	if	**Apple-iPhone**	then	DenyAccess	Edit
✓	BYOD Virtual Desktops	if	Apple... and Condition(s)	then	AuthZ Profil...	Done
✓	Default	if no matches, then				

Add All Conditions Below to Library

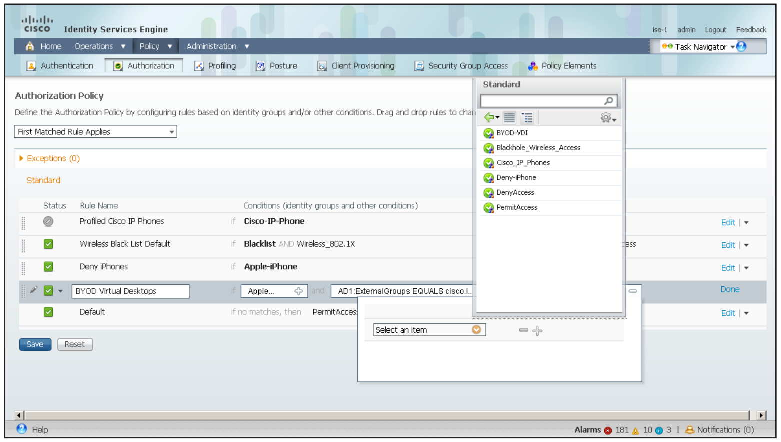
Condition Name	Expression		
	AD1:ExternalGroups	Equals	

cisco.local/Users/BYOD Provisioning
cisco.local/Users/Domain Users
cisco.local/Users/Finance
cisco.local/Users/HR
cisco.local/Users/IT
cisco.local/Users/Research

Step 14: In the Permissions section, next to AuthZ Profile(s), click the **+** symbol.

Step 15: In the Select an item list, next to Standard, click the > symbol.

Step 16: Select the BYOD-VDI authorization profile that was created in Procedure 4, “Create profiles for virtual desktops.”


Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Save Reset
Help
Alarms 181 10 3 | Notifications (0)

Authorization Policy

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

First Matched Rule Applies

Exceptions (0)

Standard

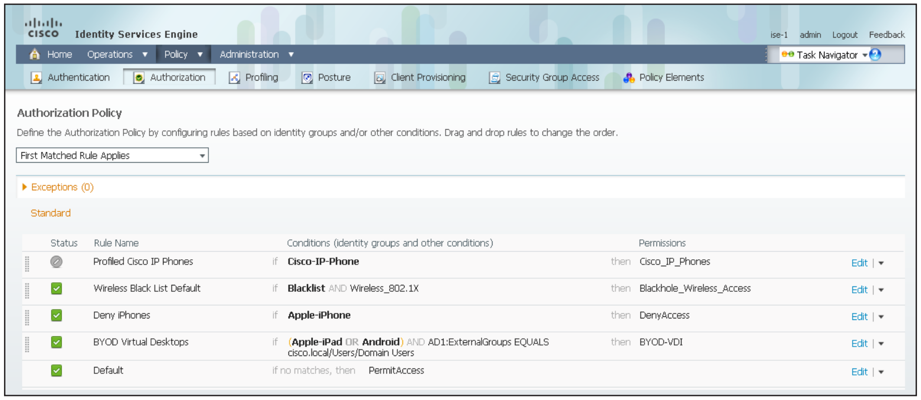
Status	Rule Name		Conditions (identity groups and other conditions)	
	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	Edit
✓	Wireless Black List Default	if	**Blacklist** AND Wireless_802.1X	Edit
✓	Deny iPhones	if	**Apple-iPhone**	Edit
✓	BYOD Virtual Desktops	if	Apple... and AD1:ExternalGroups EQUALS cisco.l...	Done
✓	Default	if no matches, then	PermitAcces	Edit

Select an item

Standard

BYOD-VDI
Blackhole_Wireless_Access
Cisco_IP_Phones
Deny-iPhone
DenyAccess
PermitAccess

Step 17: Click **Done**, and then click **Save**.


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

Authorization Policy

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

First Matched Rule Applies

Exceptions (0)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
⊘	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones	Edit | ▾
☑	Wireless Black List Default	if	**Blacklist** AND Wireless_802.1X	then	Blackhole_Wireless_Access	Edit | ▾
☑	Deny iPhones	if	**Apple-iPhone**	then	DenyAccess	Edit | ▾
☑	BYOD Virtual Desktops	if	(**Apple-iPad** OR **Android**) AND AD1:ExternalGroups EQUALS cisco.local/Users/Domain Users	then	BYOD-VDI	Edit | ▾
☑	Default	if no matches, then	PermitAccess			Edit | ▾

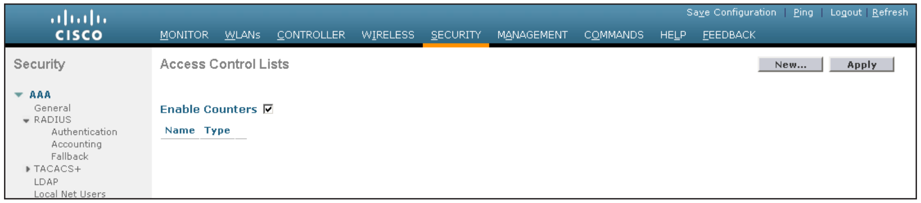
Procedure 6 Configure WLC for authorization

Configure every WLC in the environment, with the exception of the guest WLC in the DMZ, with access lists to support this newly defined policy. The ACL that is referenced by the VDI authorization profile needs to be defined on the WLC. When the clients on 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**.


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Security
AAA
General
RADIUS
Authentication
Accounting
Fallback
TACACS+
LDAP
Local Net Users
New... Apply

Access Control Lists

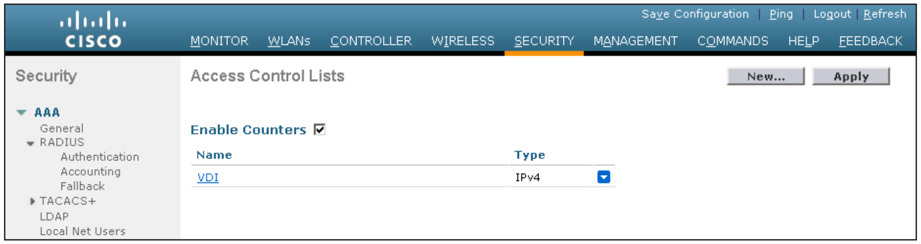
Enable Counters ☑

Name Type

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.


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Security
AAA
General
RADIUS
Authentication
Accounting
Fallback
TACACS+
LDAP
Local Net Users
New... Apply

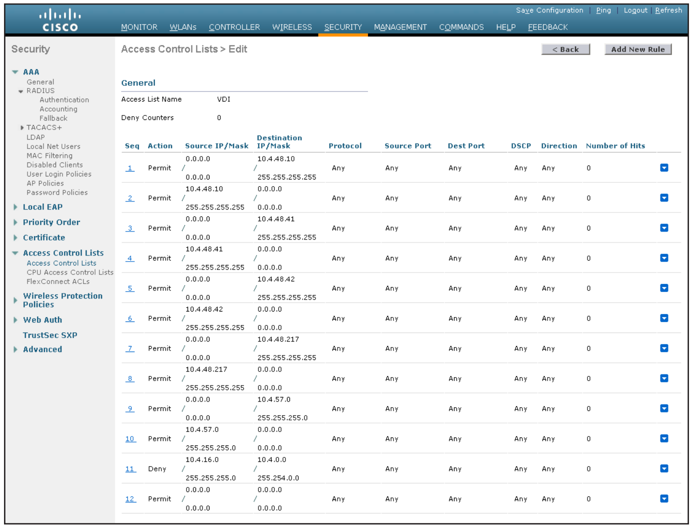
Access Control Lists

Enable Counters ☑

Name	Type
VDI	IPv4

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

Step 8: Create a new access list rule based on your security policy, and then click **Apply**. Create additional rules to complete the policy. In this example deployment, the access list allows only access to services required to use the VDI client on the user's personal device and no other internal resources. The policy also allows for access to the Internet.



Access Control Lists > Edit

General

Access List Name VDI

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	10.4.48.10 / 255.255.255.255	Any	Any	Any	Any	Any	0
2	Permit	10.4.48.10 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0
3	Permit	0.0.0.0 / 0.0.0.0	10.4.48.41 / 255.255.255.255	Any	Any	Any	Any	Any	0
4	Permit	10.4.48.41 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0
5	Permit	0.0.0.0 / 0.0.0.0	10.4.48.42 / 255.255.255.255	Any	Any	Any	Any	Any	0
6	Permit	10.4.48.42 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0
7	Permit	0.0.0.0 / 0.0.0.0	10.4.48.217 / 255.255.255.255	Any	Any	Any	Any	Any	0
8	Permit	10.4.48.217 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0
9	Permit	0.0.0.0 / 0.0.0.0	10.4.57.0 / 255.255.255.0	Any	Any	Any	Any	Any	0
10	Permit	10.4.57.0 / 255.255.255.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0
11	Deny	10.4.16.0 / 255.255.255.0	10.4.0.0 / 255.254.0.0	Any	Any	Any	Any	Any	0
12	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0

Tech Tip

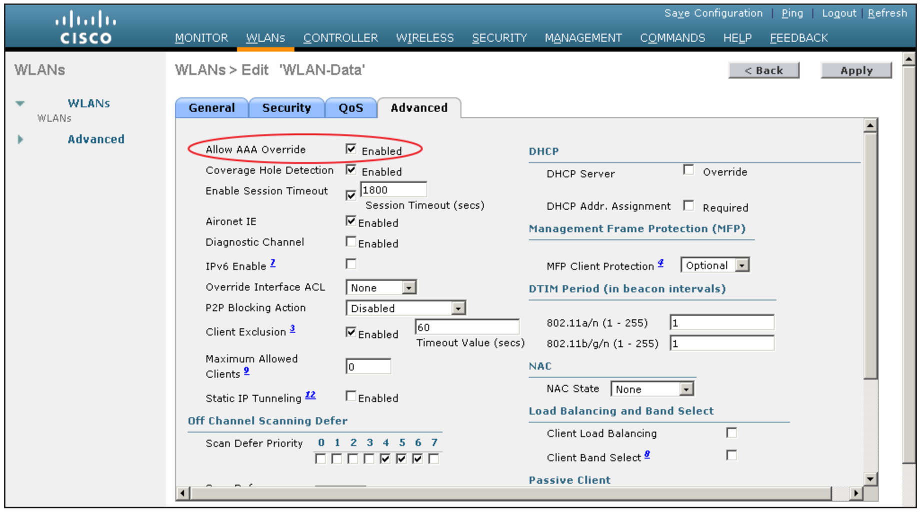
The access list needs to have entries for the traffic in both directions, so make sure you have pairs of access list rules for both inbound and outbound traffic. Also, there is an implicit "deny all" rule at the end of the access list so any traffic not explicitly permitted is denied.

Next, you 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 9: On the menu bar, click **WLANs**.

Step 10: Click the WLAN ID of the wireless network that the wireless personal devices are accessing.

Step 11: Click **Advanced**, and then select **Allow AAA Override**.



WLANs > Edit 'WLAN-Data'

Allow AAA Override ☑ Enabled
Coverage Hole Detection ☑ Enabled
Enable Session Timeout ☑ 1800 Session Timeout (secs)
Aironet IE ☑ Enabled
Diagnostic Channel □ Enabled
IPv6 Enable 7 □
Override Interface ACL None
P2P Blocking Action Disabled
Client Exclusion 3 ☑ Enabled 60 Timeout Value (secs)
Maximum Allowed Clients 9 0
Static IP Tunneling 12 □ Enabled

Off Channel Scanning Defer
Scan Defer Priority 0 □ 1 □ 2 □ 3 □ 4 ☑ 5 ☑ 6 ☑ 7 □

DHCP
DHCP Server □ Override
DHCP Addr. Assignment □ Required

Management Frame Protection (MFP)
MFP Client Protection 4 Optional

DTIM Period (in beacon intervals)
802.11a/n (1 - 255) 1
802.11b/g/n (1 - 255) 1

NAC
NAC State None

Load Balancing and Band Select
Client Load Balancing □
Client Band Select 8 □

Passive Client

Step 12: Click **Apply**, and then click **Save Configuration.**

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 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

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

Reader Tip

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

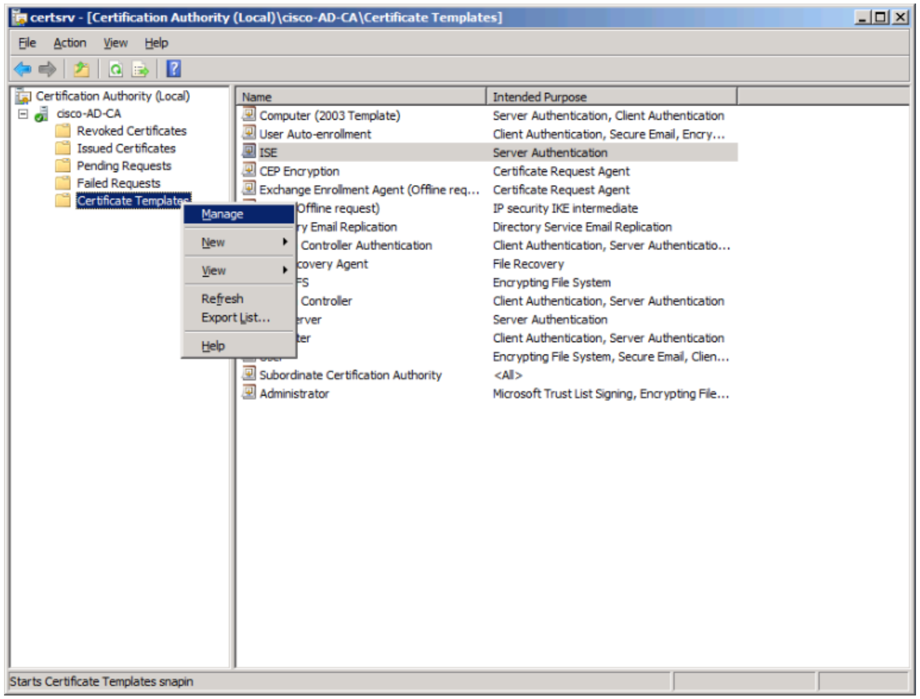
http://technet.microsoft.com/en-us/library/cc772393%28WS.10%29.aspx

Procedure 2 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.



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

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

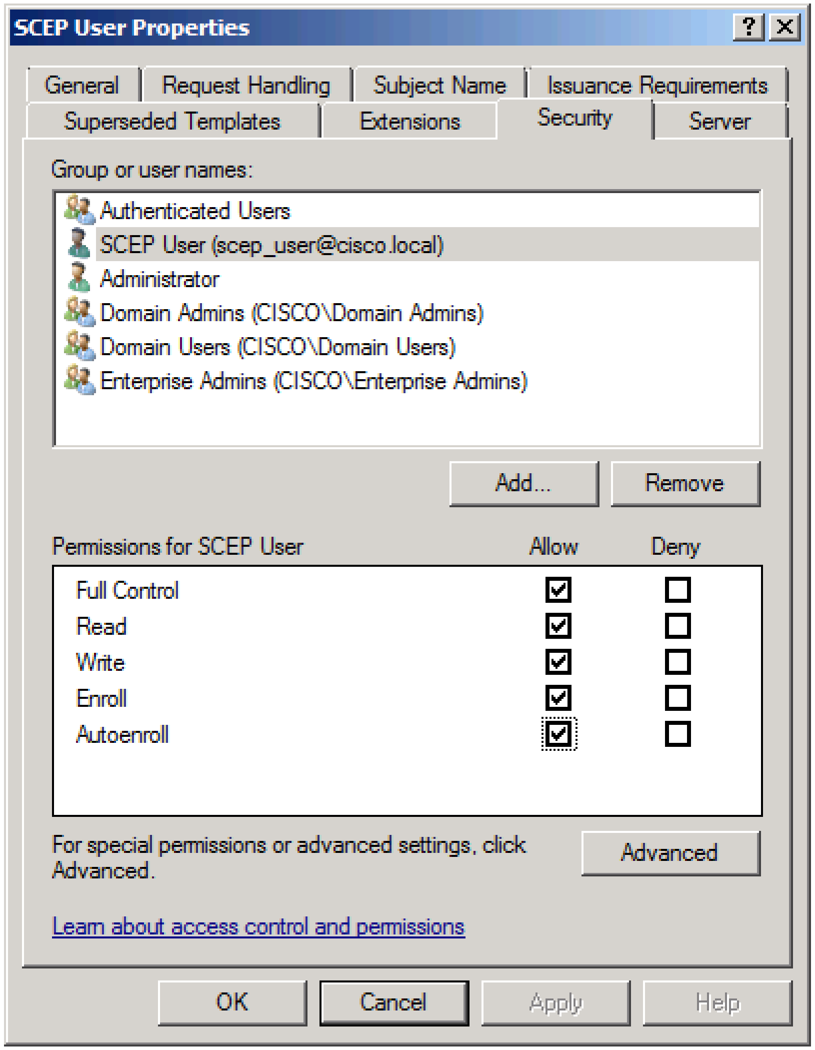
For compatibility with Windows XP, make sure that Windows 2003 Server Enterprise is selected.

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.



Group or user names:

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

Permissions for SCEP User	Allow	Deny
Full Control	☑	□
Read	☑	□
Write	☑	□
Enroll	☑	□
Autoenroll	☑	□

For special permissions or advanced settings, click Advanced.

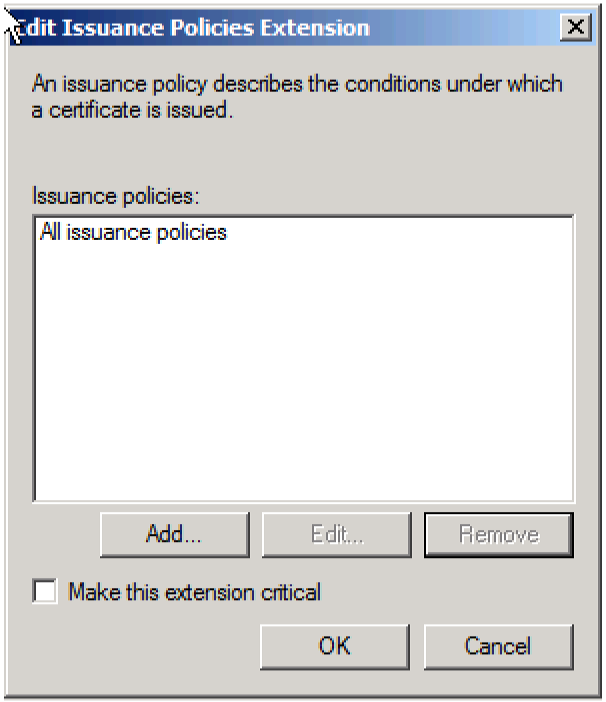
Step 8: On the Subject Name tab, select **Supply in the request**.

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**.



An issuance policy describes the conditions under which a certificate is issued.

Issuance policies:

All issuance policies

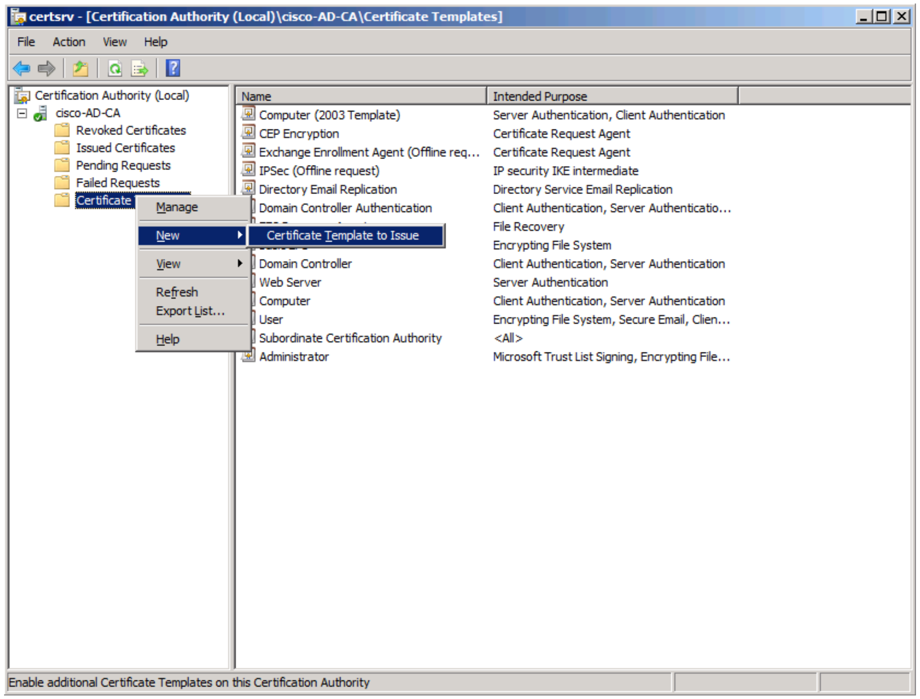
□ Make this extension critical

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**.

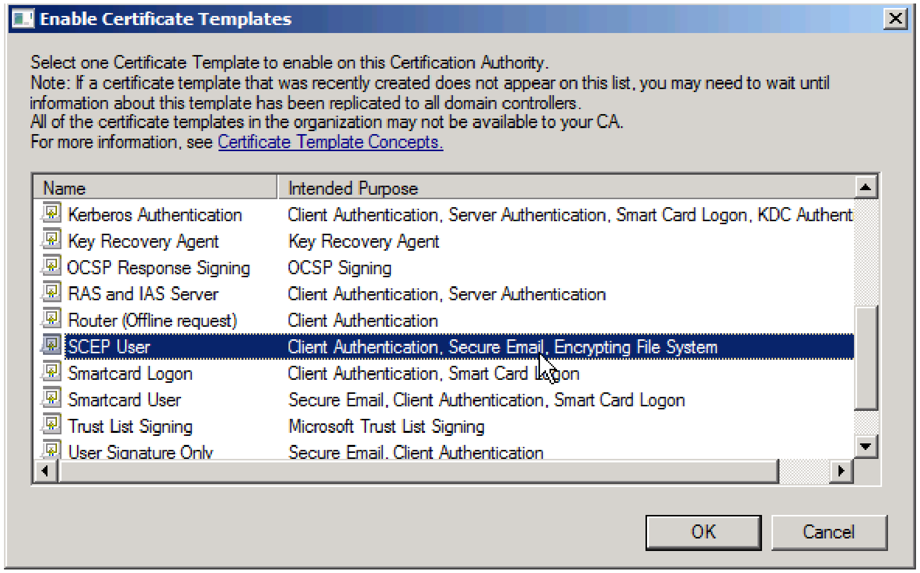


certsrv - [Certification Authority (Local)\cisco-AD-CA\Certificate Templates]

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

Enable additional Certificate Templates on this Certification Authority

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



Enable Certificate Templates

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

Name	Intended Purpose
Kerberos Authentication	Client Authentication, Server Authentication, Smart Card Logon, KDC Authent
Key Recovery Agent	Key Recovery Agent
OCSP Response Signing	OCSP Signing
RAS and IAS Server	Client Authentication, Server Authentication
Router (Offline request)	Client Authentication
SCEP User	Client Authentication, Secure Email, Encrypting File System
Smartcard Logon	Client Authentication, Smart Card Logon
Smartcard User	Secure Email, Client Authentication, Smart Card Logon
Trust List Signing	Microsoft Trust List Signing
User Signature Only	Secure Email, Client Authentication

Procedure 3 Edit registry

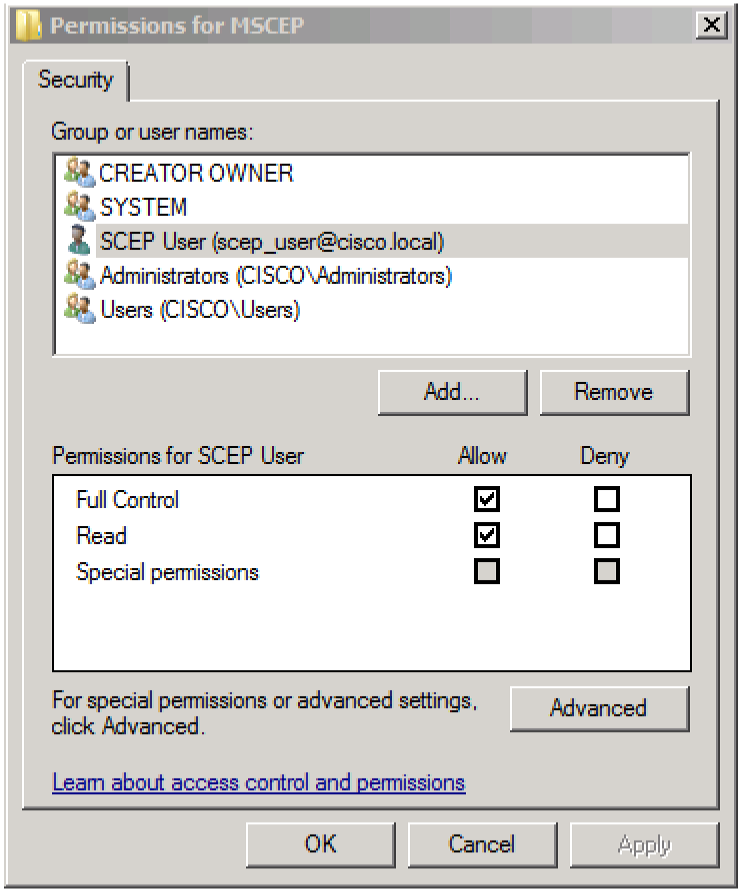
There are a few changes that need to be made to the registry to support auto-enrollment in order to complete the installation.

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**.



Group or user names:

- CREATOR OWNER
- SYSTEM
- SCEP User (scep_user@cisco.local)
- Administrators (CISCO\Administrators)
- Users (CISCO\Users)

Permissions for SCEP User	Allow	Deny
Full Control	☑	□
Read	☑	□
Special permissions	□	□

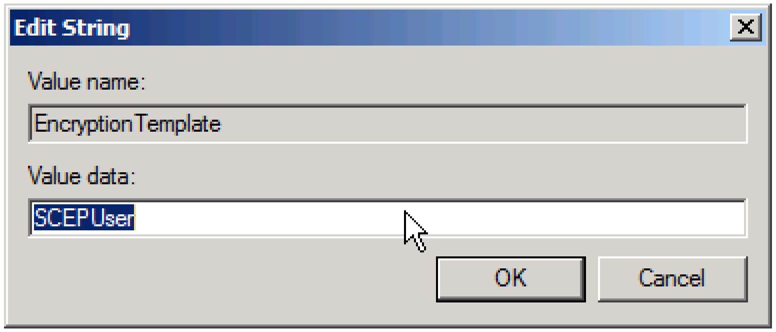
For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

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**.

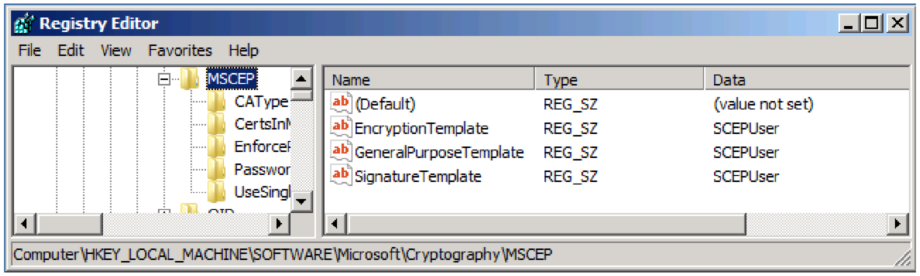
Step 6: In the Value Data box, enter the name of the template created in Procedure 2, and then click **OK**.



Value name: EncryptionTemplate

Value data: SCEPUser

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



Name	Type	Data
(Default)	REG_SZ	(value not set)
EncryptionTemplate	REG_SZ	SCEPUser
GeneralPurposeTemplate	REG_SZ	SCEPUser
SignatureTemplate	REG_SZ	SCEPUser

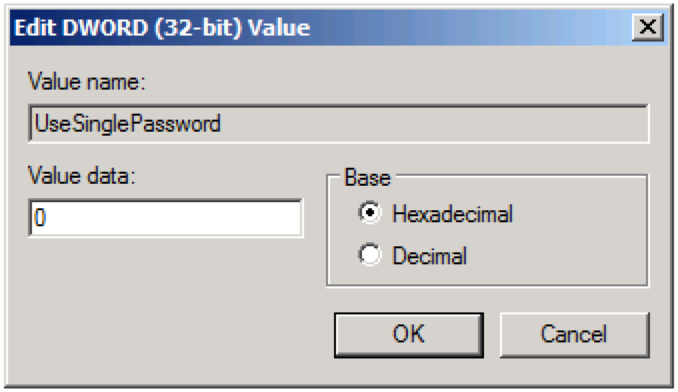
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP

Next, disable the HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\UseSinglePassword key.

Step 8: Click **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\UseSinglePassword**.

Step 9: Right-click **UseSinglePassword**, and then choose **Modify**.

Step 10: In the Value data box, enter **0**, and then click **OK**.


Edit DWORD (32-bit) Value

Value name: UseSinglePassword

Value data: 0

Base: ● Hexadecimal ○ Decimal

Procedure 4 Install trusted root certificate for domain

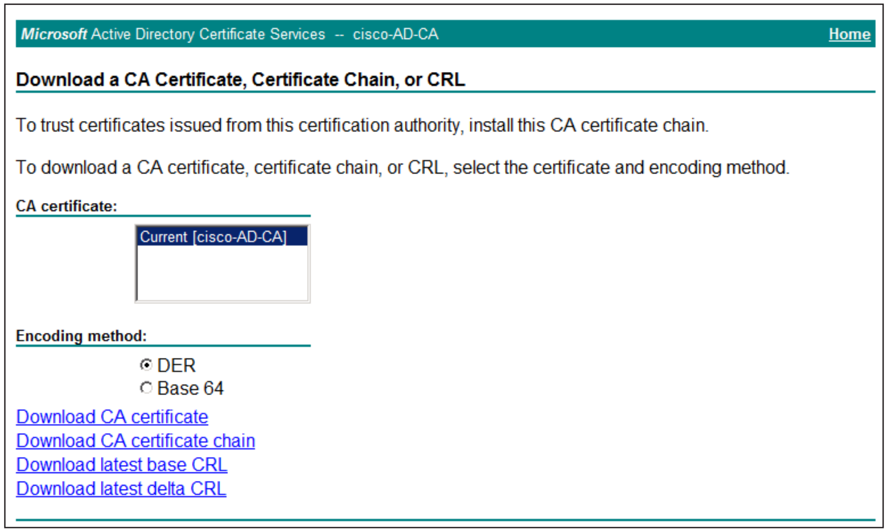
Install a trusted root certificate on the AD controller in order to distribute it to the clients so that certificates from the CA server will be trusted.

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

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

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

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


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

Download a CA Certificate, Certificate Chain, or CRL

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

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

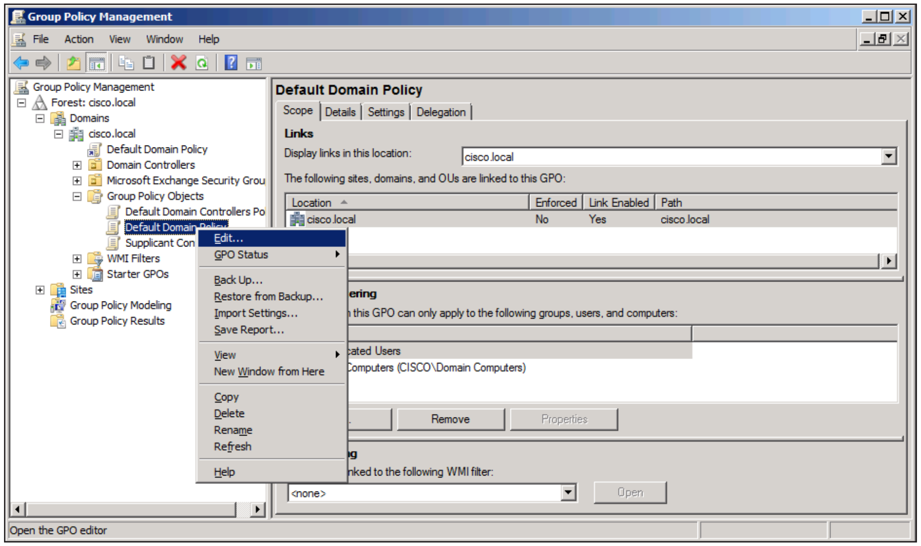
CA certificate: Current [cisco-AD-CA]

Encoding method: ● DER ○ Base 64

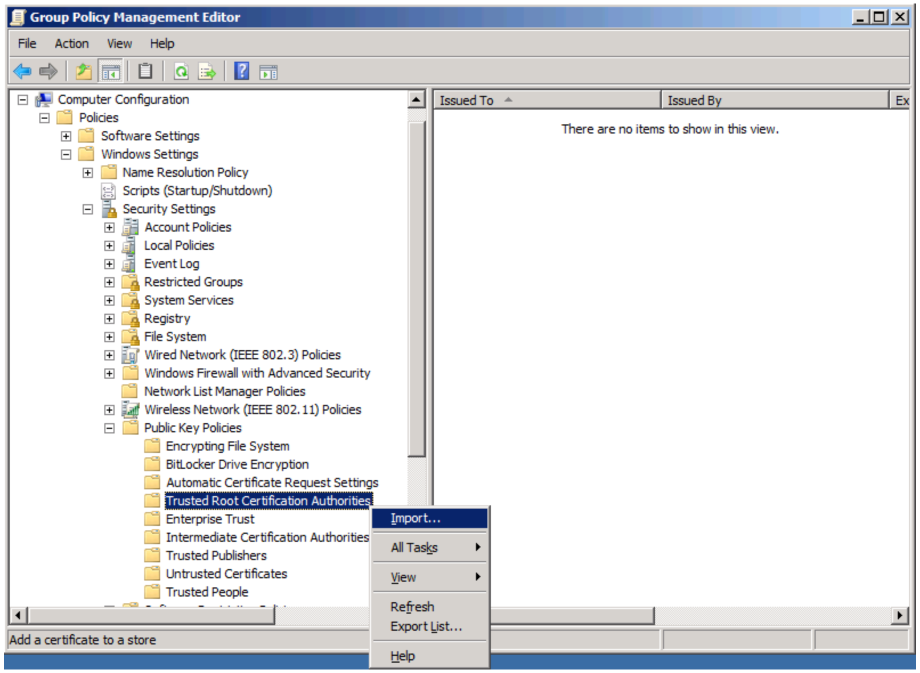
Step 5: On the CA console, navigate to **Start > Administrative Tools > Group Policy Management**.

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

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

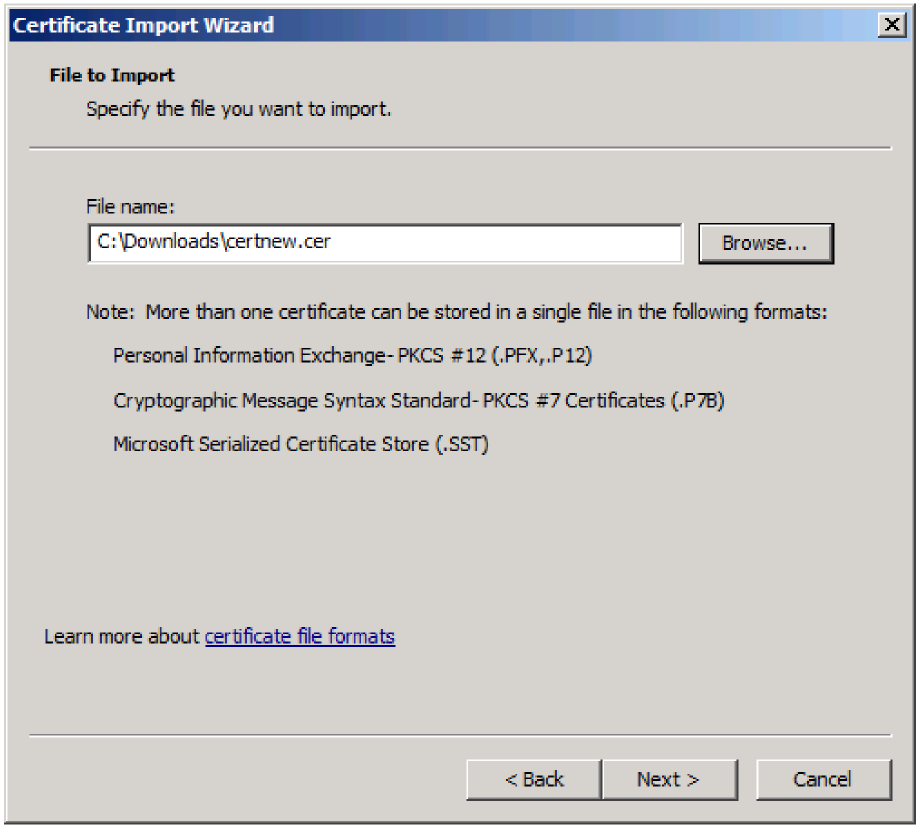


Step 8: Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies,** right-click **Trusted Root Certification Authorities,** and then choose **Import**. The Certificate Import Wizard launches.


Group Policy Management Editor
File Action View Help
Computer Configuration
Policies
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Encrypting File System
BitLocker Drive Encryption
Automatic Certificate Request Settings
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Trusted People
Import...
All Tasks
View
Refresh
Export List...
Help
Issued To
Issued By
Ex
There are no items to show in this view.
Add a certificate to a store

Step 9: Click **Next**.

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


Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

C:\Downloads\certnew.cer

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

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

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

Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

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

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

Step 13: Click **OK**. The wizard closes.

Procedure 5 Install trusted root on AD server

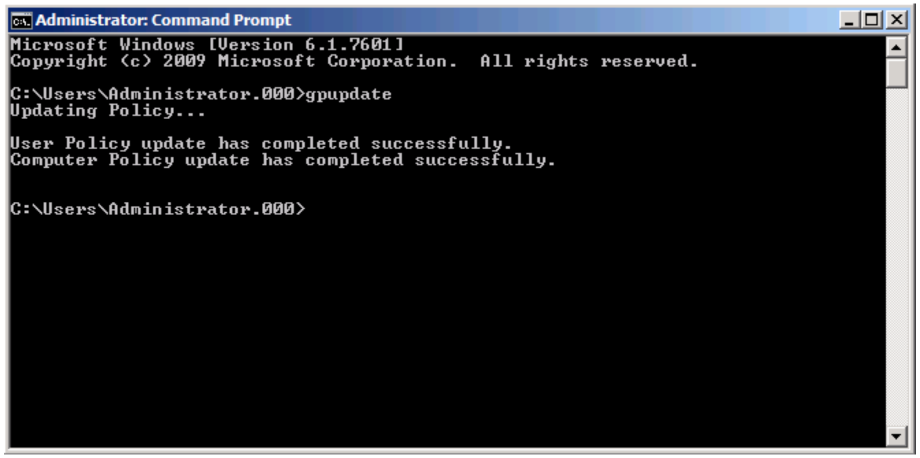
In addition to configuring AD server to distribute the trusted root certificate to workstations, you need to install the certificate directly on the AD server. A group policy object (GPO) update takes care of this automatically. In this procedure, you force the update to run immediately.

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

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

Step 3: Update the group policy.

```
gpupdate
```


Administrator: Command Prompt

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

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

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


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

Procedure 6 Request a certificate for ISE from the CA

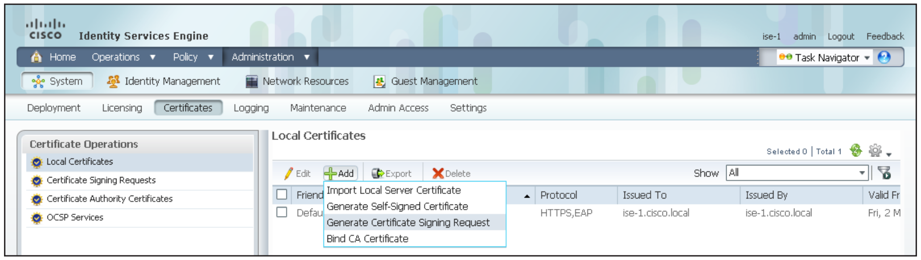
In order to obtain a certificate from the CA, Cisco ISE needs to generate a signing request that will be used by the CA to generate a certificate.

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**.

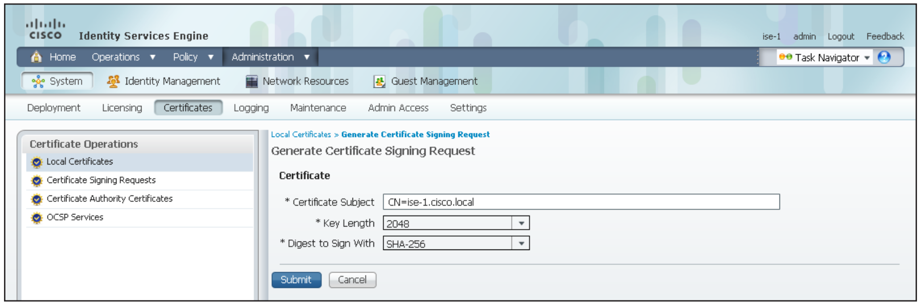


Local Certificates

Selected 0 | Total 1

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

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**.



Generate Certificate Signing Request

Certificate

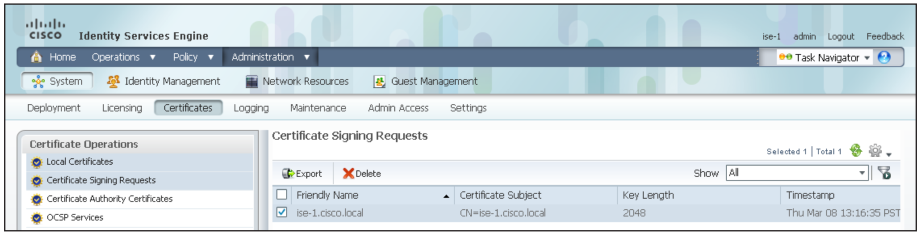
* Certificate Subject: CN=ise-1.cisco.local

* Key Length: 2048

* Digest to Sign With: SHA-256

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**.



Certificate Signing Requests

Selected 1 | Total 1

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

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

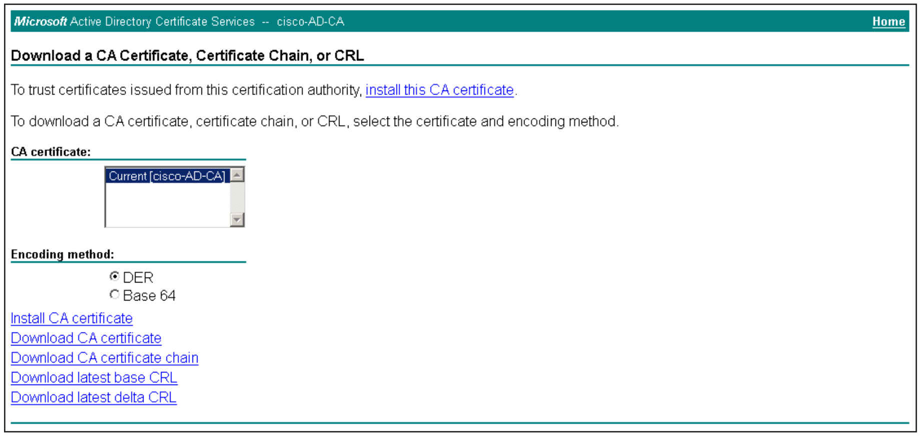
Procedure 7 Download CA root certificate

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.


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

Download a CA Certificate, Certificate Chain, or CRL

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

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

CA certificate: Current [cisco-AD-CA]

Encoding method:

● DER
○ Base 64

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

Procedure 8 Issue certificate for Cisco ISE

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

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

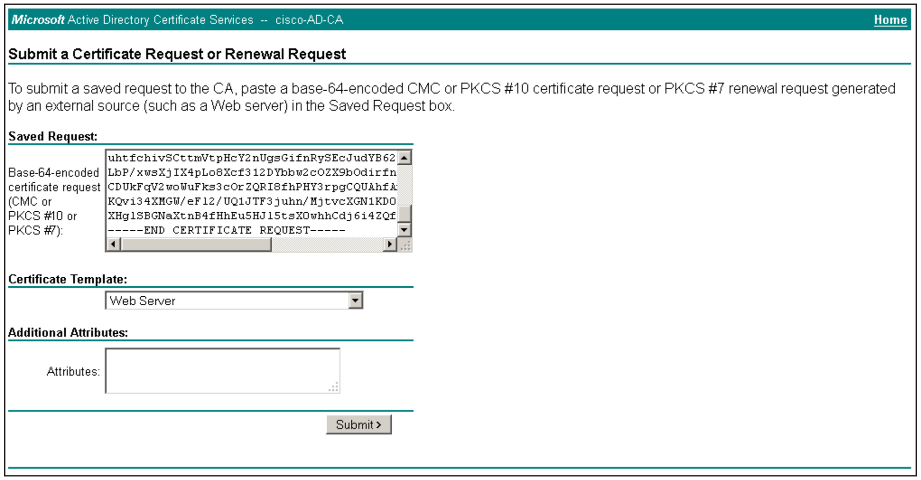
Step 3: Click **advanced certificate request**.

Step 4: In a text editor, such as Notepad, open the certificate file saved in Procedure 6, "Request a certificate for ISE from the CA."

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

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

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


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

Submit a Certificate Request or Renewal Request

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

Saved Request:

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

```
uhtfchivSCttmVtpHcY2nUgsGifnRySEcJudYB62
LbP/xwsXjIX4pLo8Xcf312DYbbw2cOZX9bOdirfn
CDUkFqV2woWuFks3cOrZQRI8fhPHY3rpgCQUAhfA
KQvi34XMGW/eF12/UQ1JTF3juhn/MjtvcXGN1KDO
XHg1SBGNaXtnB4fHhEu5HJ15tsXOwhhCdj6i4ZQf
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

Additional Attributes:

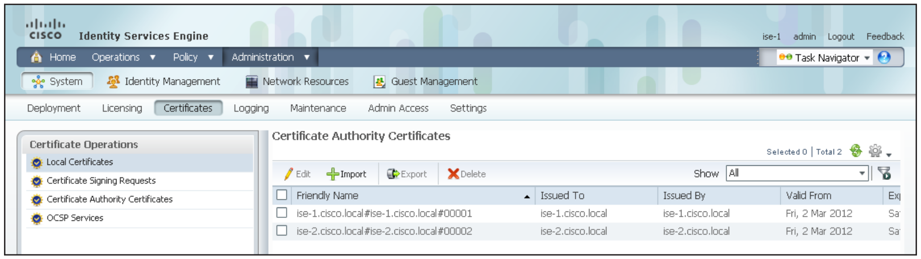
Attributes:

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**.



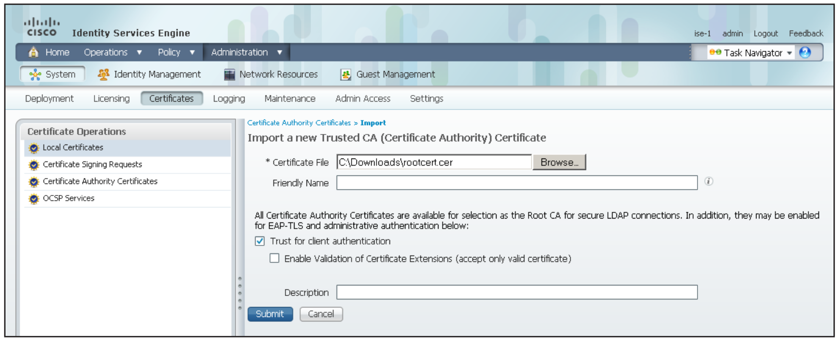
Certificate Authority Certificates

Selected 0 | Total 2

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

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

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



Import a new Trusted CA (Certificate Authority) Certificate

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

Friendly Name:

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

☑ Trust for client authentication

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

Description:

Procedure 10 Configure SCEP

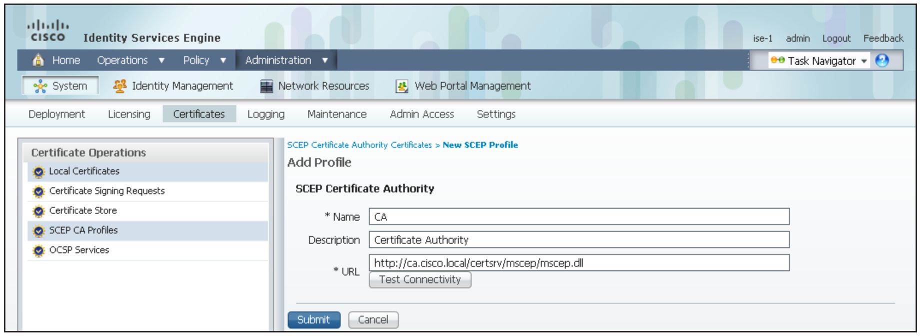
To support self-provisioning, you need to configure Cisco ISE to support SCEP, in order to enable Cisco ISE to obtain and then provision certificates for clients.

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**.


cisco Identity Services Engine
ise-1 admin Logout Feedback
Home Operations ▾ Policy ▾ Administration ▾
Task Navigator ▾
System Identity Management Network Resources Web Portal Management
Deployment Licensing Certificates Logging Maintenance Admin Access Settings
Certificate Operations
Local Certificates
Certificate Signing Requests
Certificate Store
SCEP CA Profiles
OCSP Services
SCEP Certificate Authority Certificates > New SCEP Profile
Add Profile
SCEP Certificate Authority
Test Connectivity
Submit
Cancel

* Name: CA

Description: Certificate Authority

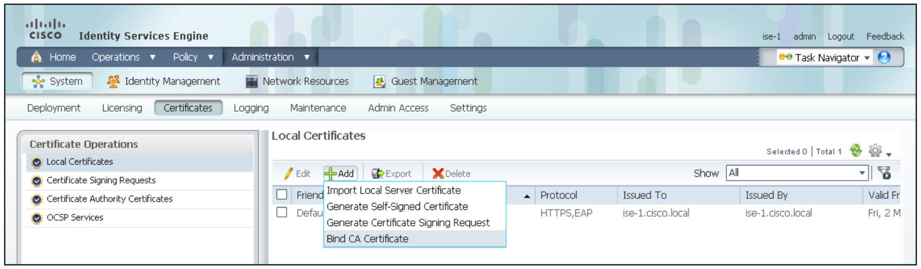
* URL: http://ca.cisco.local/certsrv/mscep/mscep.dll

Procedure 11 Install local certificate in Cisco ISE

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

Step 2: Click **Local Certificates**.

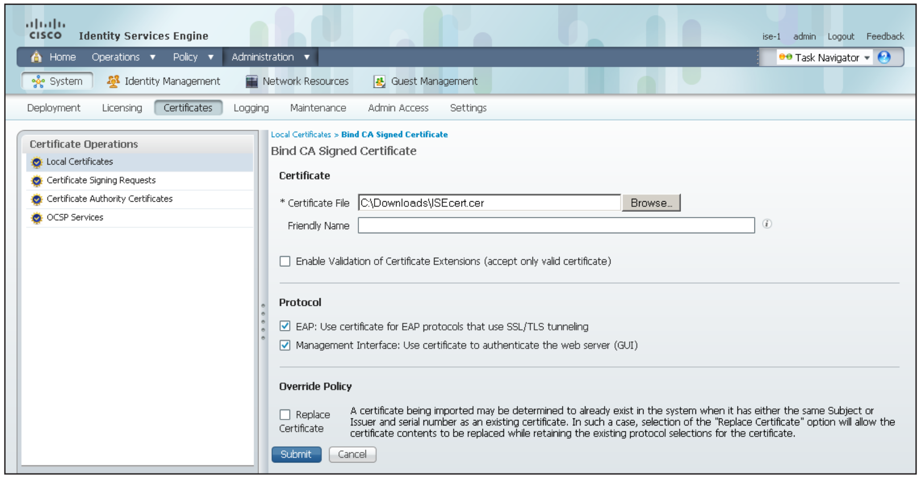
Step 3: Click **Add,** and then choose **Bind CA Certificate**.


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

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

Step 4: Click **Browse** and locate the certificate saved from Procedure 8, "Issue certificate for Cisco ISE."

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


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

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

Friendly Name:

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

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

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

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

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

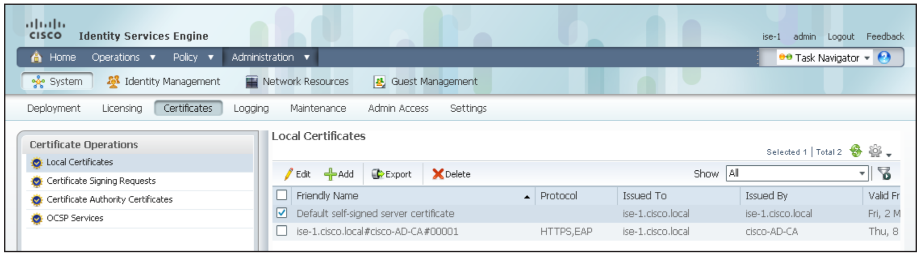
Procedure 12 Delete old certificate and request

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.


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

Local Certificates

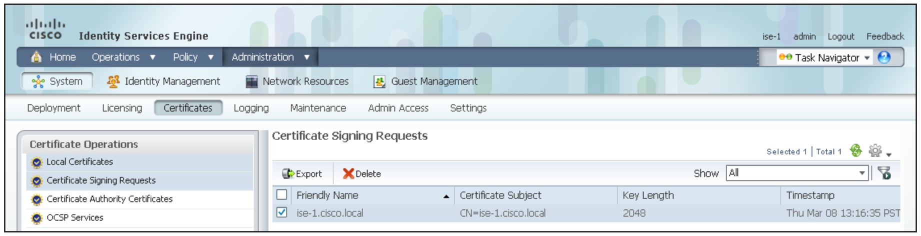
Selected 1 | Total 2

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

Step 4: Click **Delete,** and then click **OK**.

Step 5: Click **Certificate Signing Requests**.

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


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

Certificate Signing Requests

Selected 1 | Total 1

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

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

Process

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 authentication profile
6. Create native supplicant profile
7. Define provisioning policy
8. Modify authentication policy
9. Create authorization profile
10. Configure provisioning authorization rule
11. Create Android authorization profile
12. Create Android provisioning rule
13. Create 802.1X authorization rule
14. Modify default rule
15. Configure WLCs
16. Create profiles for user groups
17. Create authorization rules for user groups
18. Delete wireless 802.1X rule
19. Configure WLC for authorization
20. Provision an Apple iPad
21. Provision an Android tablet

Next, you configure Cisco ISE to provision digital certificates and the 802.1X supplicant for 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.

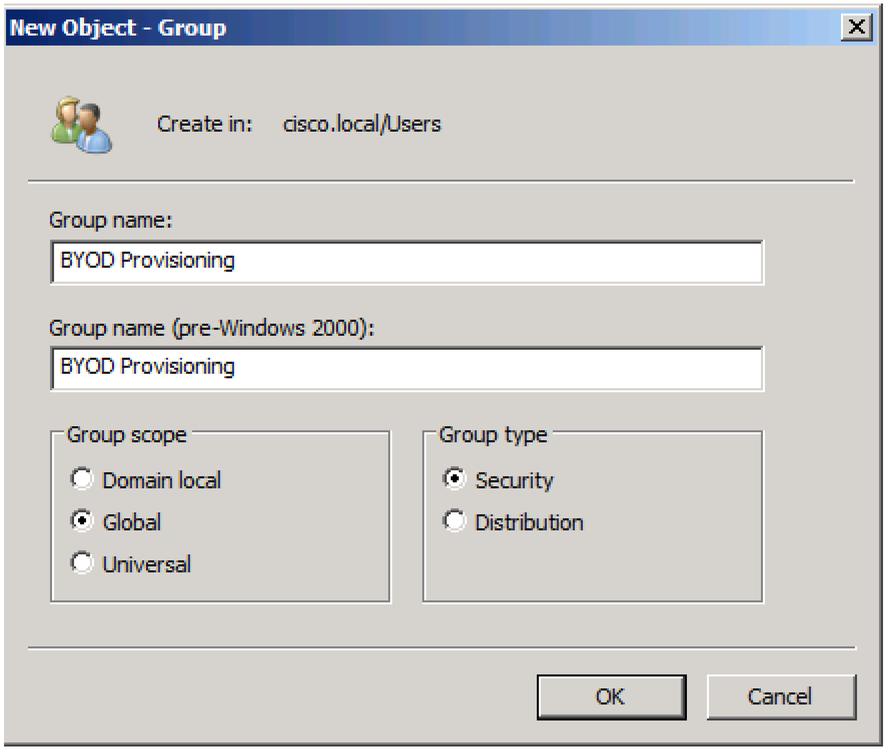
Procedure 1 Create AD group for provisioning

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, choose **New**, and then select **Group**.

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



New Object - Group

Create in: cisco.local/Users

Group name:
BYOD Provisioning

Group name (pre-Windows 2000):
BYOD Provisioning

Group scope
○ Domain local
● Global
○ Universal

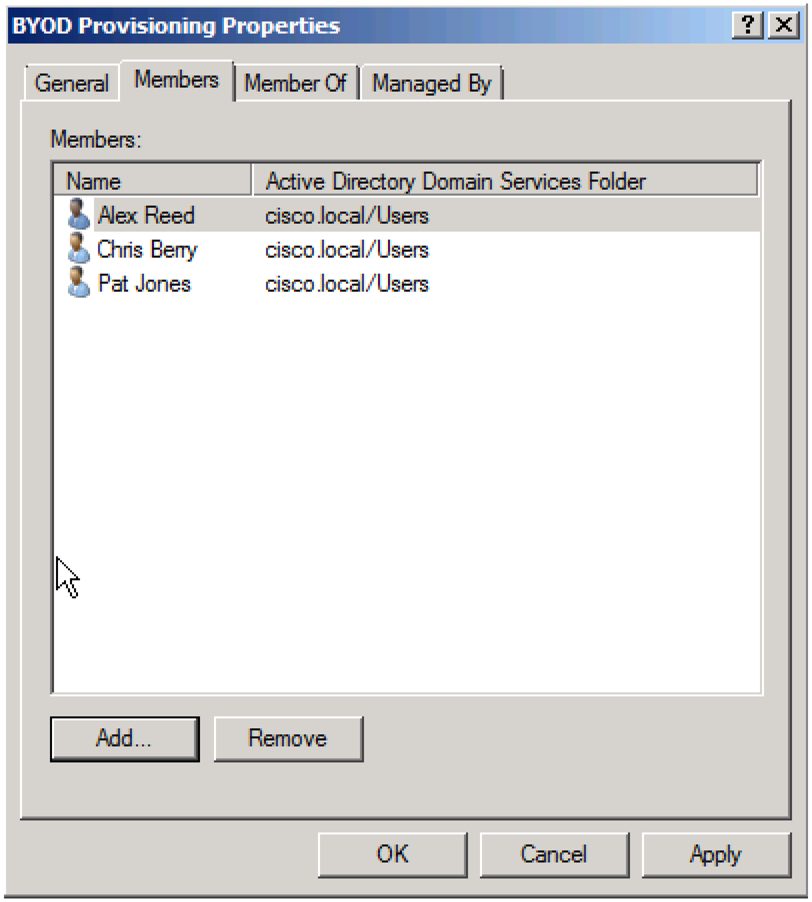
Group type
● Security
○ Distribution

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

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

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

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



BYOD Provisioning Properties

Members:

Name	Active Directory Domain Services Folder
Alex Reed	cisco.local/Users
Chris Berry	cisco.local/Users
Pat Jones	cisco.local/Users

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.

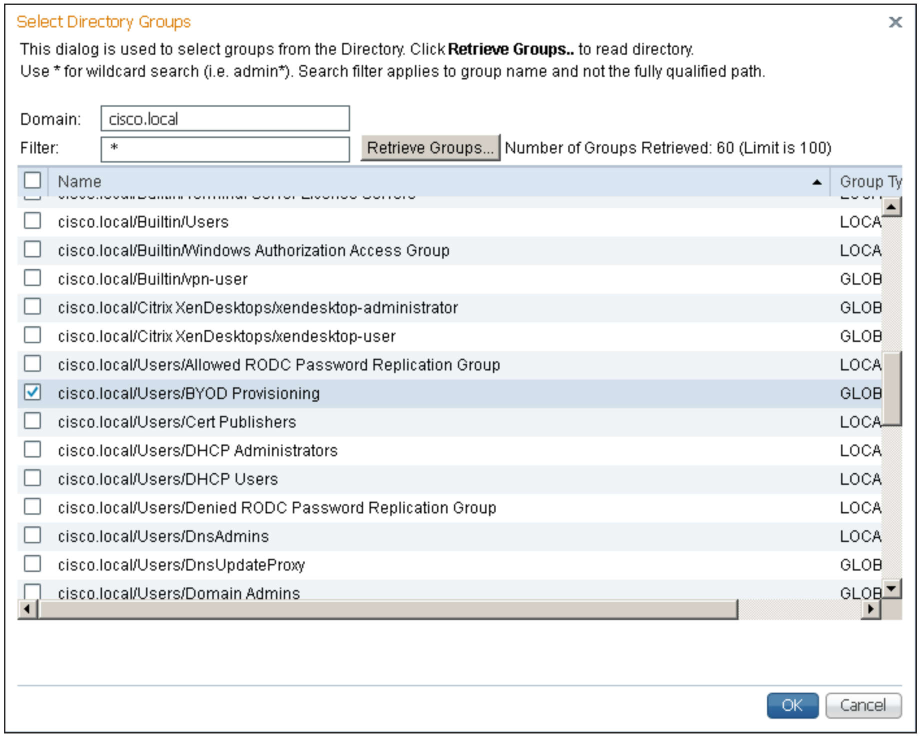
Step 2: On the menu bar, mouse over **Administration**, and then, in the Identity Management section, select **External Identity Sources**.

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**.



Select Directory Groups

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

Domain: cisco.local

Filter: *

Number of Groups Retrieved: 60 (Limit is 100)

□	Name	Group Ty
□	cisco.local/Builtin/Users	LOCA
□	cisco.local/Builtin/Windows Authorization Access Group	LOCA
□	cisco.local/Builtin/vpn-user	GLOB
□	cisco.local/Citrix XenDesktops/xendesktop-administrator	GLOB
□	cisco.local/Citrix XenDesktops/xendesktop-user	GLOB
□	cisco.local/Users/Allowed RODC Password Replication Group	LOCA
☑	cisco.local/Users/BYOD Provisioning	GLOB
□	cisco.local/Users/Cert Publishers	LOCA
□	cisco.local/Users/DHCP Administrators	LOCA
□	cisco.local/Users/DHCP Users	LOCA
□	cisco.local/Users/Denied RODC Password Replication Group	LOCA
□	cisco.local/Users/DnsAdmins	LOCA
□	cisco.local/Users/DnsUpdateProxy	GLOB
□	cisco.local/Users/Domain Admins	GLOB

Procedure 3 Enable EAP-TLS

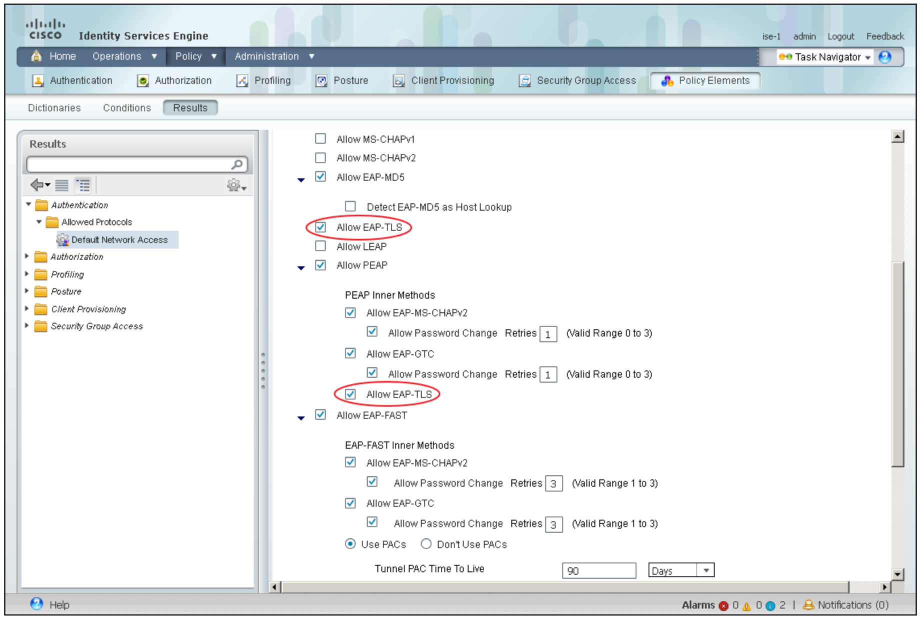
In a previous section, you disabled EAP-TLS. Now that you are using digital certificates, you need to enable it.

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**.



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

□ Allow MS-CHAPv1
□ Allow MS-CHAPv2
☑ Allow EAP-MD5
□ Detect EAP-MD5 as Host Lookup
☑ Allow EAP-TLS
□ Allow LEAP
☑ Allow PEAP

PEAP Inner Methods
☑ Allow EAP-MS-CHAPv2
☑ Allow Password Change Retries 1 (Valid Range 0 to 3)
☑ Allow EAP-GTC
☑ Allow Password Change Retries 1 (Valid Range 0 to 3)
☑ Allow EAP-TLS
☑ Allow EAP-FAST

EAP-FAST Inner Methods
☑ Allow EAP-MS-CHAPv2
☑ Allow Password Change Retries 3 (Valid Range 1 to 3)
☑ Allow EAP-GTC
☑ Allow Password Change Retries 3 (Valid Range 1 to 3)
● Use PACs ○ Don't Use PACs
Tunnel PAC Time To Live 90 Days

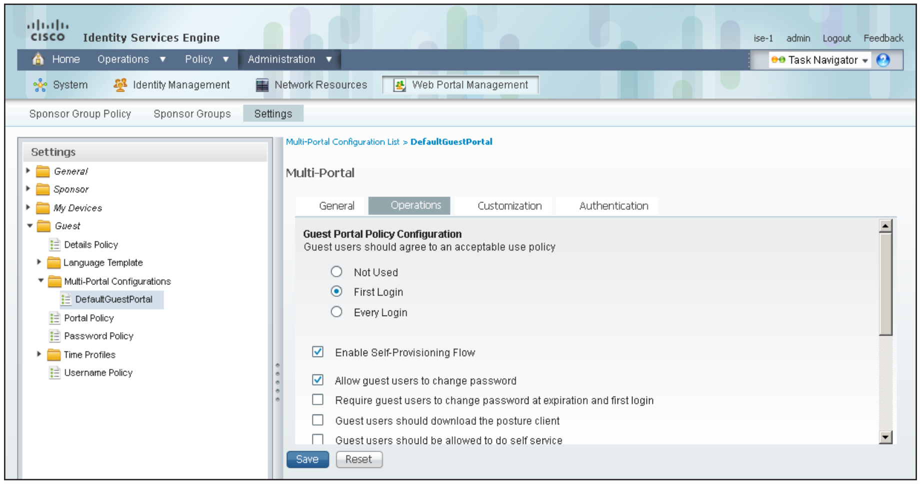
Procedure 4 Enable self-provisioning portal

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**.


Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
System Identity Management Network Resources Web Portal Management
Sponsor Group Policy Sponsor Groups Settings
Settings
General
Sponsor
My Devices
Guest
Details Policy
Language Template
Multi-Portal Configurations
DefaultGuestPortal
Portal Policy
Password Policy
Time Profiles
Username Policy

Multi-Portal Configuration List > DefaultGuestPortal

Multi-Portal

General | Operations | Customization | Authentication

Guest Portal Policy Configuration
Guest users should agree to an acceptable use policy

○ Not Used
● First Login
○ Every Login

☑ Enable Self-Provisioning Flow

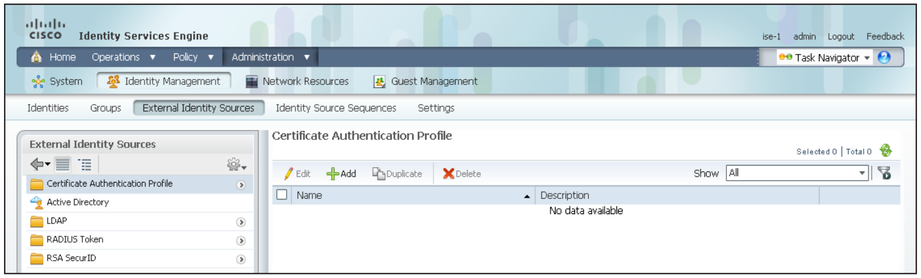
☑ Allow guest users to change password
□ Require guest users to change password at expiration and first login
□ Guest users should download the posture client
□ Guest users should be allowed to do self service

Save Reset

Procedure 5 Create authentication profile

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**.

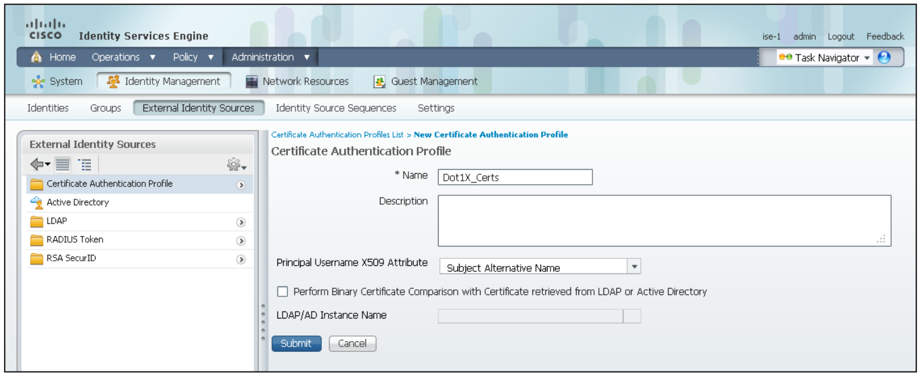

Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
System Identity Management Network Resources Guest Management
Identities Groups External Identity Sources Identity Source Sequences Settings
External Identity Sources
Certificate Authentication Profile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

Certificate Authentication Profile

Selected 0 | Total 0

Name	Description
No data available	

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


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

Certificate Authentication Profiles List > New Certificate Authentication Profile

Certificate Authentication Profile

* Name: Dot1X_Certs

Description:

Principal Username X509 Attribute: Subject Alternative Name

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

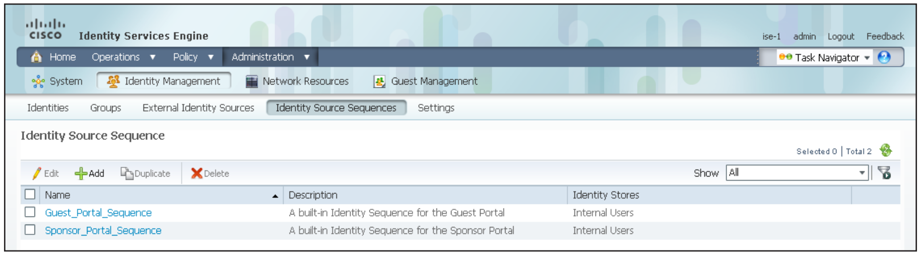
LDAP/AD Instance Name:

Submit Cancel

Step 4: Click **Submit**.

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

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


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

Identity Source Sequence

Selected 0 | Total 2

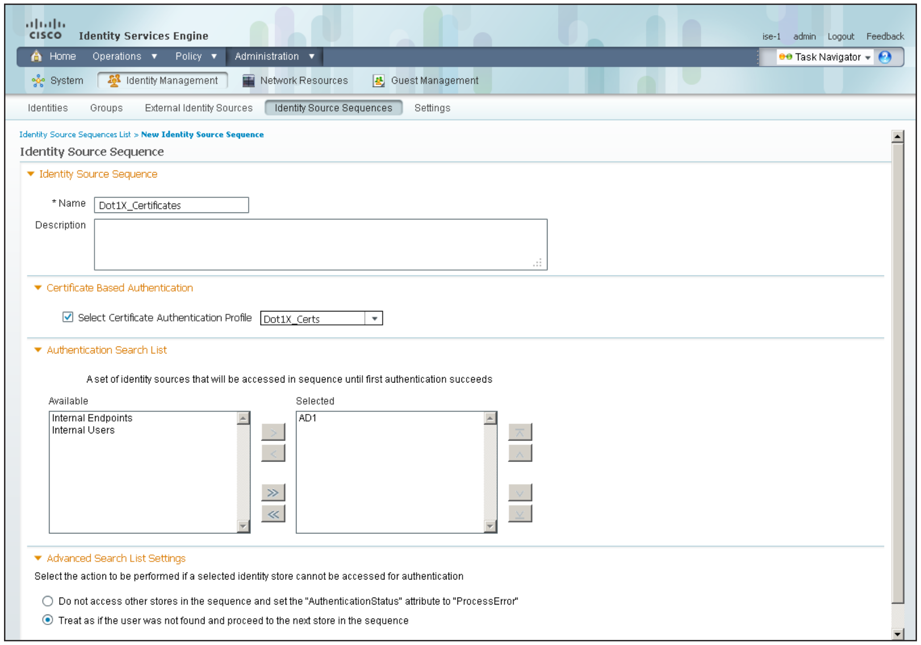
Name	Description	Identity Stores
Guest_Portal_Sequence	A built-in Identity Sequence for the Guest Portal	Internal Users
Sponsor_Portal_Sequence	A built-in Identity Sequence for the Sponsor Portal	Internal Users

Step 6: Enter a name for the sequence.

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

Step 8: In the Authentication Search List section, 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**.


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

Identity Source Sequences List > New Identity Source Sequence

Identity Source Sequence

Identity Source Sequence

* Name Dot1X_Certificates

Description

Certificate Based Authentication

☑ Select Certificate Authentication Profile Dot1X_Certs

Authentication Search List

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

Available	Selected
Internal Endpoints Internal Users	AD1

Advanced Search List Settings

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

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

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

Step 10: Click **Submit**.

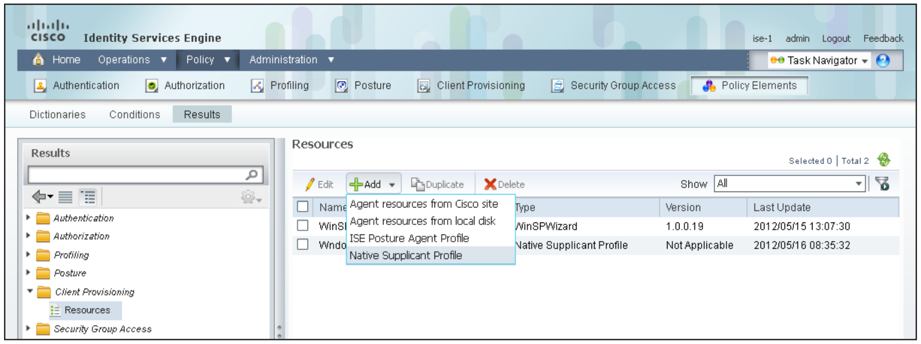
Procedure 6 Create native supplicant profile

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**.


Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Dictionaries Conditions Results
Results
Authentication
Authorization
Profiling
Posture
Client Provisioning
Resources
Security Group Access
Edit Add Duplicate Delete
Show All
Agent resources from Cisco site
Agent resources from local disk
ISE Posture Agent Profile
Native Supplicant Profile

Resources

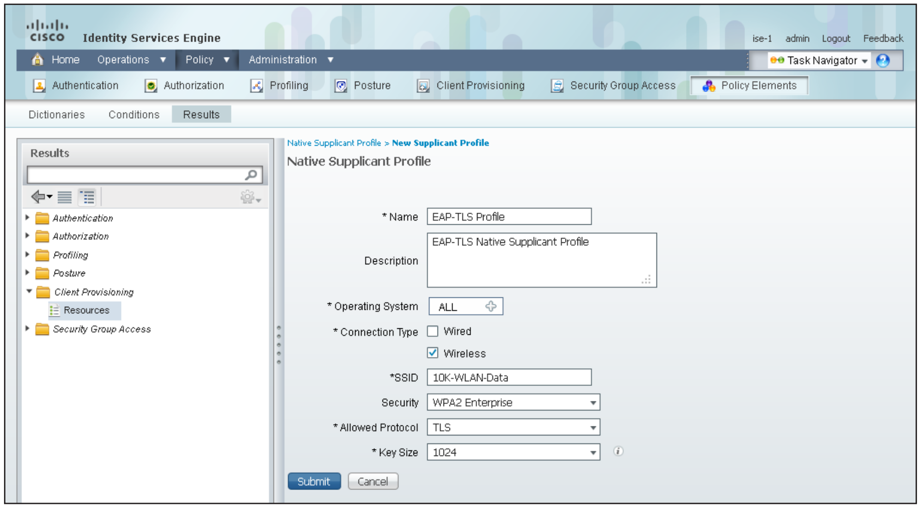
Selected 0 | Total 2

☐	Name	Type	Version	Last Update
☐	WinS	WinSPWizard	1.0.0.19	2012/05/15 13:07:30
☐	Wndo	Native Supplicant Profile	Not Applicable	2012/05/16 08:35:32

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**.


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

Native Supplicant Profile > New Supplicant Profile

Native Supplicant Profile

* Name EAP-TLS Profile

Description EAP-TLS Native Supplicant Profile

* Operating System ALL

* Connection Type ☐ Wired

☑ Wireless

*SSID 10K-WLAN-Data

Security WPA2 Enterprise

* Allowed Protocol TLS

* Key Size 1024

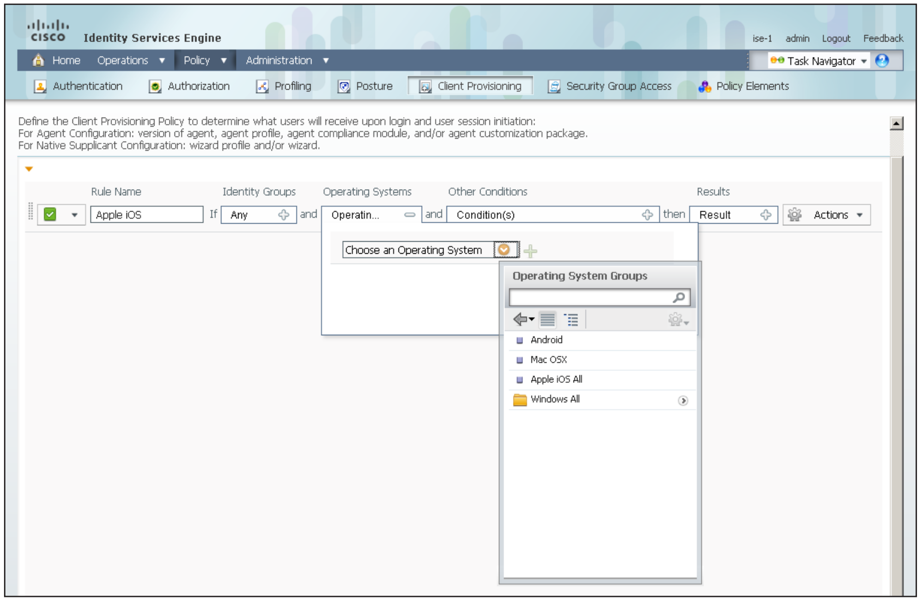
Procedure 7 Define provisioning policy

You create a provisioning policy for each operating system (in this example, Apple iOS and Google Android) in order to determine which supplicant profile to apply.

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

Step 2: Enter a name for the rule.

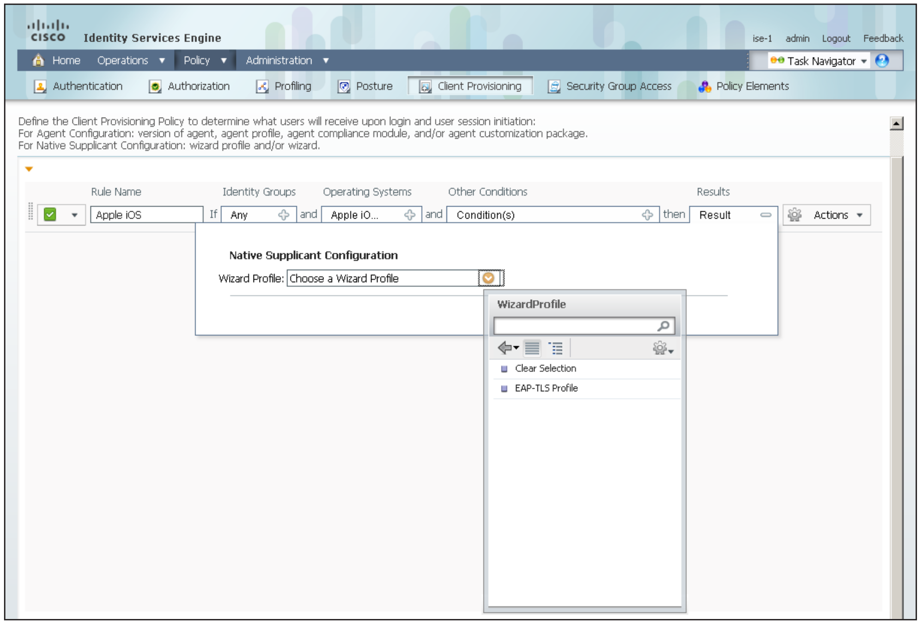
Step 3: In the Operating Systems section, click the **+** symbol, and then select **Apple iOS All**.


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

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard.

Rule Name		Identity Groups		Operating Systems		Other Conditions		Results	
Apple iOS	If	Any	and	Operatin...	and	Condition(s)	then	Result	Actions

Step 4: Next to Result, click the **+** symbol, and then select the profile created in Procedure 6.


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

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard.

Rule Name		Identity Groups		Operating Systems		Other Conditions		Results	
Apple iOS	If	Any	and	Apple iO...	and	Condition(s)	then	Result	Actions

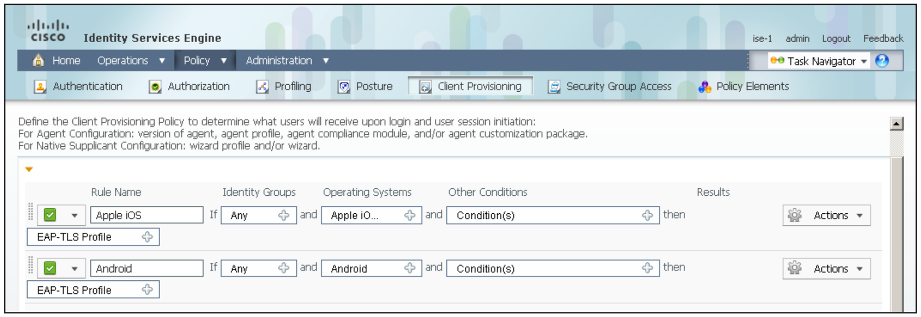
Native Supplicant Configuration

Wizard Profile: Choose a Wizard Profile

Step 5: Click **Actions**, and then select **Insert new policy below**.

Step 6: Create a rule for Android devices by repeating Step 1 through Step 3.

Step 7: Click **Save**.


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

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard.

Rule Name		Identity Groups		Operating Systems		Other Conditions		Results	
Apple iOS	If	Any	and	Apple iO...	and	Condition(s)	then	EAP-TLS Profile	Actions
Android	If	Any	and	Android	and	Condition(s)	then	EAP-TLS Profile	Actions

Procedure 8 Modify authentication policy

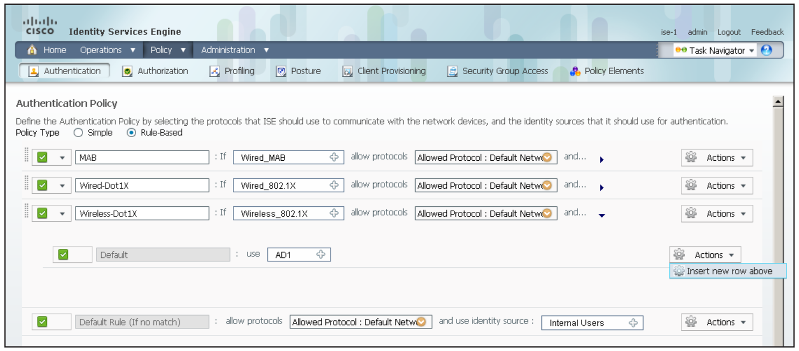
Now that you have created a certificate authentication profile and identity source sequence for digital certificates, you need to enable the 802.1X authentication policies for wireless users.

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 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: 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**.


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

Authentication Policy

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

Policy Type ○ Simple ● Rule-Based

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

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

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

☑ Default : use AD1 Actions

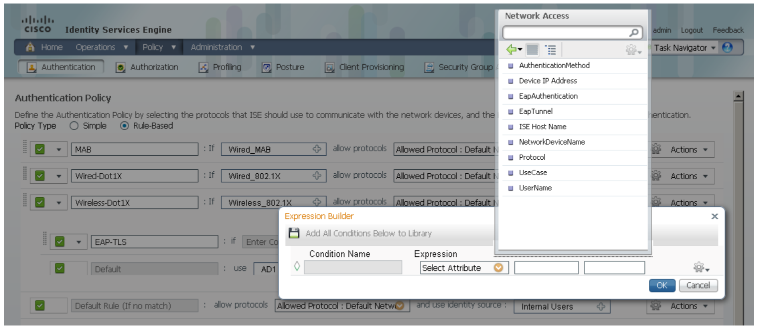
☑ Default Rule (If no match) : allow protocols Allowed Protocol : Default Netw and use identity source : Internal Users Actions

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

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

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

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



Authentication Policy

Policy Type ○ Simple ● Rule-Based

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

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

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

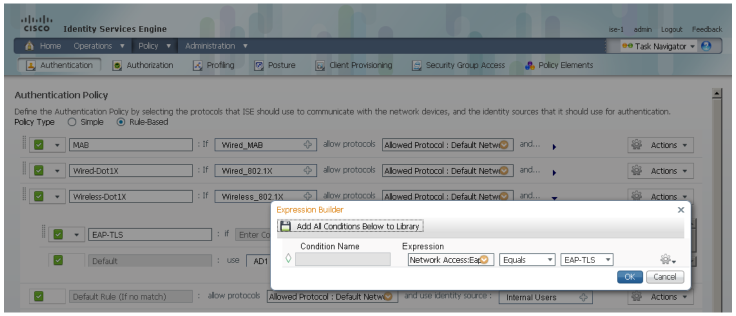
☑ EAP-TLS : if Enter Co

☑ Default : use AD1

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

Condition Name | Expression: Select Attribute

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


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

Authentication Policy

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

Policy Type ○ Simple ● Rule-Based

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

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

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

☑ EAP-TLS : if Enter Co

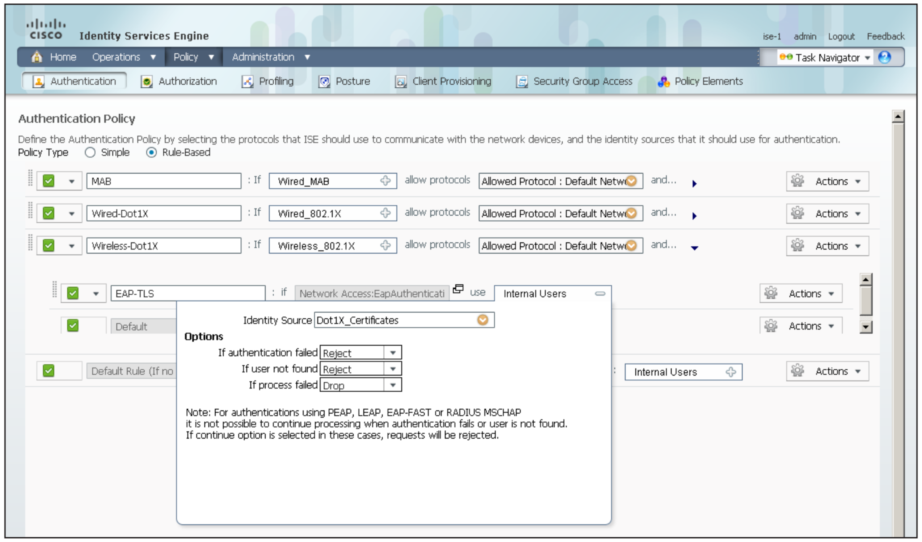
☑ Default : use AD1

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

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

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

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


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

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.
Policy Type ○ Simple ● Rule-Based

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

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

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

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

☑ Default

☑ Default Rule (If no : Internal Users

Identity Source Dot1X_Certificates

Options
If authentication failed Reject
If user not found Reject
If process failed Drop

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

Step 11: Click **Save**.

Procedure 9 Create 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**.

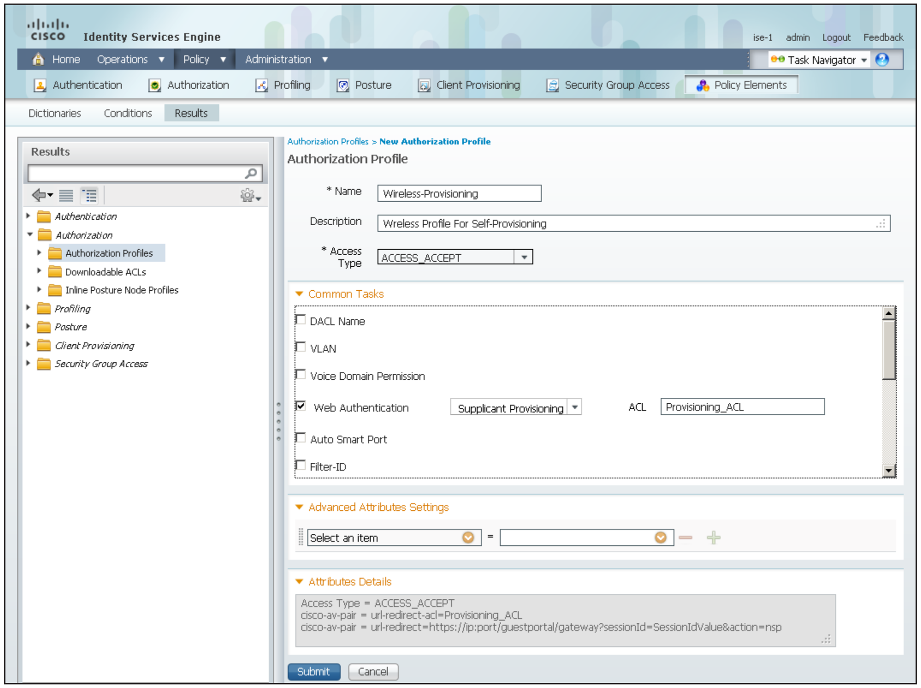
Step 4: Enter a name and description for the profile.

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**.


Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Dictionaries Conditions Results
Results
Authentication
Authorization
Authorization Profiles
Downloadable ACLs
Inline Posture Node Profiles
Profiling
Posture
Client Provisioning
Security Group Access
Authorization Profiles > New Authorization Profile
Common Tasks
Advanced Attributes Settings
Select an item
Attributes Details
Submit
Cancel

Authorization Profile

* Name Wireless-Provisioning

Description Wreless Profile For Self-Provisioning

* Access Type ACCESS_ACCEPT

□ DACL Name
□ VLAN
□ Voice Domain Permission
☑ Web Authentication Supplicant Provisioning ACL Provisioning_ACL
□ Auto Smart Port
□ Filter-ID

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-acl=Provisioning_ACL
cisco-av-pair = url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=nsp
```

Procedure 10 Configure provisioning authorization 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 BYOD Virtual Desktops 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.

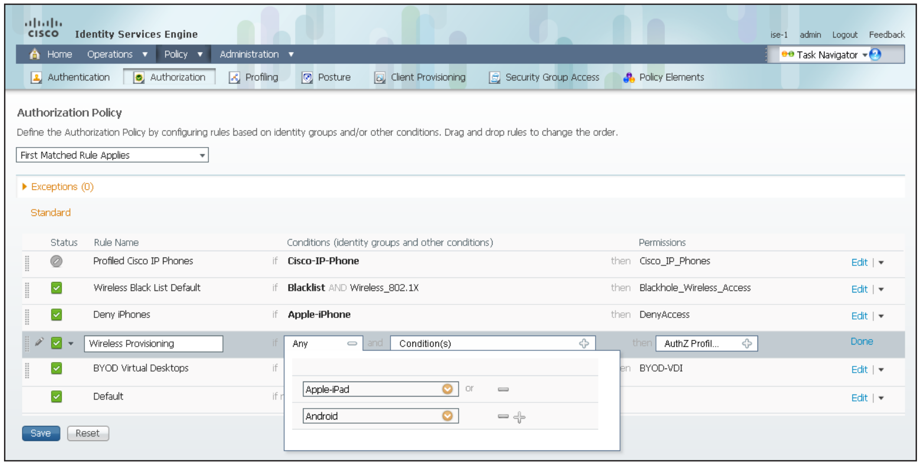
Step 5: In the list, next to Endpoint Identity Groups, click the **>** symbol, and then, next to Profiled, click the **>** symbol.

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**.



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

Authorization Policy

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

First Matched Rule Applies

Exceptions (0)

Standard

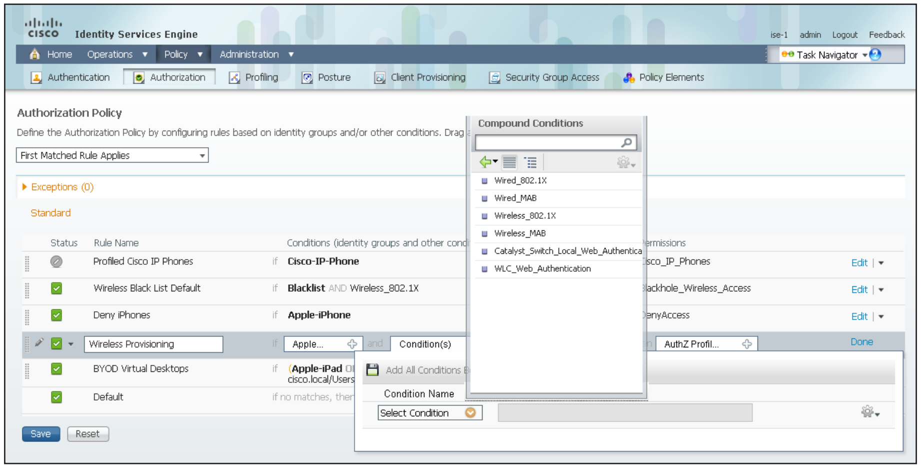
Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones	Edit | ▾
☑	Wireless Black List Default	if	**Blacklist** AND Wireless_802.1X	then	Blackhole_Wireless_Access	Edit | ▾
☑	Deny iPhones	if	**Apple-iPhone**	then	DenyAccess	Edit | ▾
☑	Wireless Provisioning	if	Any and Condition(s)	then	AuthZ Profil...	Done
☑	BYOD Virtual Desktops	if		then	BYOD-VDI	Edit | ▾
☑	Default	if				Edit | ▾

Apple-iPad or

Android

Step 10: In the **Condition(s)** list, click the **+** symbol, and then click **Select Existing Condition from Library**.

Step 11: In the list, next to Compound Conditions, click the **>** symbol, and then choose **Wireless_802.1X**.



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

Authorization Policy

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

First Matched Rule Applies

Exceptions (0)

Standard

Status	Rule Name		Conditions (identity groups and other cond	Permissions	
	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	sco_IP_Phones	Edit | ▾
☑	Wireless Black List Default	if	**Blacklist** AND Wireless_802.1X	ackhole_Wireless_Access	Edit | ▾
☑	Deny iPhones	if	**Apple-iPhone**	enyAccess	Edit | ▾
☑	Wireless Provisioning	if	Apple... and Condition(s)	AuthZ Profil...	Done
☑	BYOD Virtual Desktops	if	(**Apple-iPad** O cisco.local/Users		
☑	Default		if no matches, then		

Compound Conditions

- Wired_802.1X
- Wired_MAB
- Wireless_802.1X
- Wireless_MAB
- Catalyst_Switch_Local_Web_Authentica
- WLC_Web_Authentication

Add All Conditions

Condition Name

Select Condition

Step 12: At the end of the rule, click the gear icon, and then select **Add Attribute/Value**.

Step 13: Next to Select Attribute, click the arrow. The menu opens.

Step 14: Next to Network Access, click the **>** symbol, and then choose **EapTunnel**.

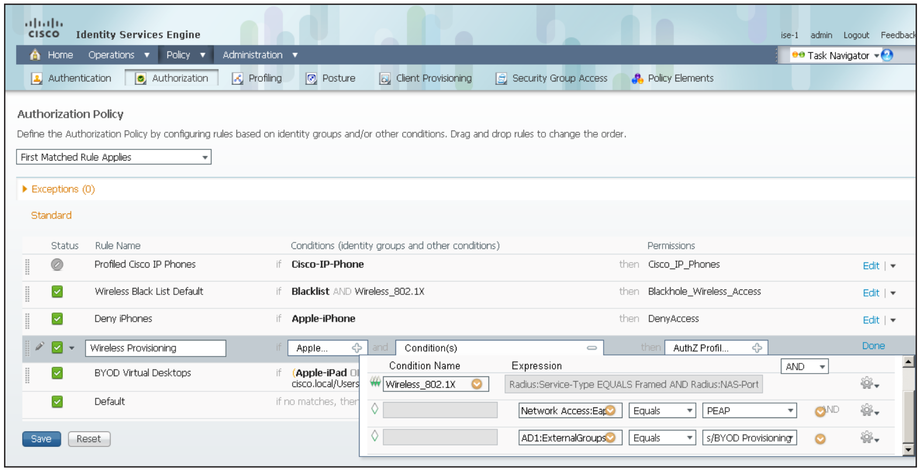
Step 15: Under Expression, in the first list, choose **Equals**, and then, in the second list, choose **PEAP**.

Step 16: At the end of this rule, click the gear icon, and then select **Add Attribute/Value**.

Step 17: Next to Select Attribute, click the arrow. The menu opens.

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

Step 19: Under Expression, in the first list, choose **Equals**, and then, in the second list, choose the BYOD group created in Procedure 2.



Authorization Policy

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

First Matched Rule Applies

▸ Exceptions (0)

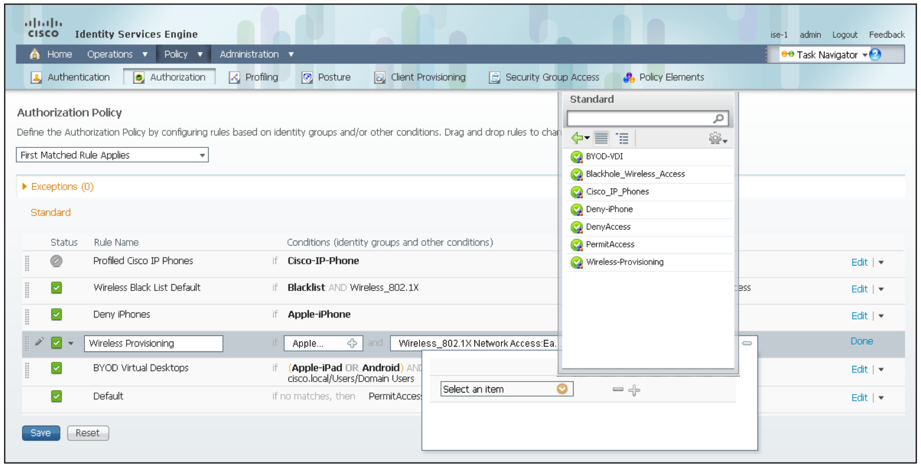
Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
⊘	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones	Edit | ▾
☑	Wireless Black List Default	if	**Blacklist** AND Wireless_802.1X	then	Blackhole_Wireless_Access	Edit | ▾
☑	Deny iPhones	if	**Apple-iPhone**	then	DenyAccess	Edit | ▾
☑	Wireless Provisioning	if	Apple... and Condition(s)	then	AuthZ Profil...	Done
☑	BYOD Virtual Desktops	if	(**Apple-iPad** O… cisco.local/Users			
☑	Default	if no matches, then				

Condition Name	Expression			AND
Wireless_802.1X	Radius:Service-Type EQUALS Framed AND Radius:NAS-Port			
	Network Access:Ea…	Equals	PEAP	AND
	AD1:ExternalGroups	Equals	s/BYOD Provisioning	

Step 20: Next to AuthZ Profile(s), click the **+** symbol, and then, next to Select an item, click the arrow.

Step 21: Next to Standard, click the **>** symbol, and then choose the authorization profile created in Procedure 9.



Authorization Policy

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

First Matched Rule Applies

▸ Exceptions (0)

Standard

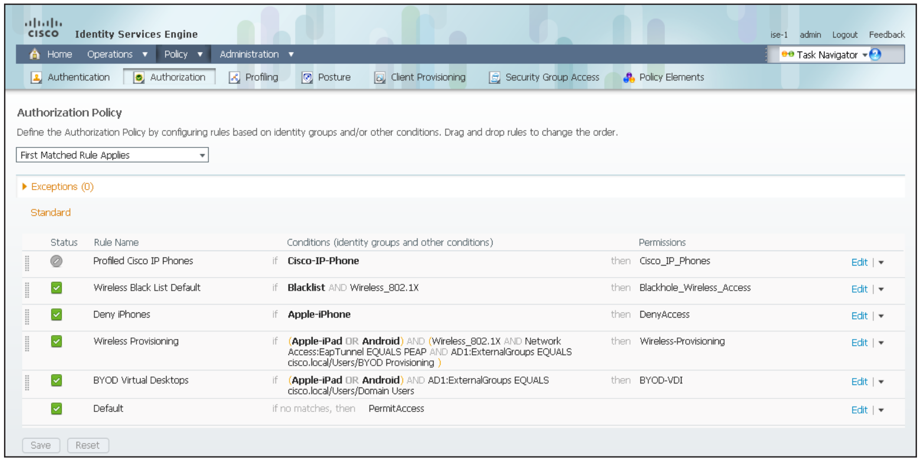
Status	Rule Name		Conditions (identity groups and other conditions)	
⊘	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	Edit | ▾
☑	Wireless Black List Default	if	**Blacklist** AND Wireless_802.1X	Edit | ▾
☑	Deny iPhones	if	**Apple-iPhone**	Edit | ▾
☑	Wireless Provisioning	if	Apple... and Wireless_802.1X Network Access:Ea...	Done
☑	BYOD Virtual Desktops	if	(**Apple-iPad** OR **Android**) AN… cisco.local/Users/Domain Users	Edit | ▾
☑	Default	if no matches, then	PermitAcces…	Edit | ▾

Standard

- BYOD-VDI
- Blackhole_Wireless_Access
- Cisco_IP_Phones
- Deny-iPhone
- DenyAccess
- PermitAccess
- Wireless-Provisioning

Select an item

Step 22: Click **Done**, and then click **Save**.



Authorization Policy

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

First Matched Rule Applies

▸ Exceptions (0)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
⊘	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones	Edit | ▾
☑	Wireless Black List Default	if	**Blacklist** AND Wireless_802.1X	then	Blackhole_Wireless_Access	Edit | ▾
☑	Deny iPhones	if	**Apple-iPhone**	then	DenyAccess	Edit | ▾
☑	Wireless Provisioning	if	(**Apple-iPad** OR **Android**) AND (Wireless_802.1X AND Network Access:EapTunnel EQUALS PEAP AND AD1:ExternalGroups EQUALS cisco.local/Users/BYOD Provisioning)	then	Wireless-Provisioning	Edit | ▾
☑	BYOD Virtual Desktops	if	(**Apple-iPad** OR **Android**) AND AD1:ExternalGroups EQUALS cisco.local/Users/Domain Users	then	BYOD-VDI	Edit | ▾
☑	Default	if no matches, then	PermitAccess			Edit | ▾

Procedure 11 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**.

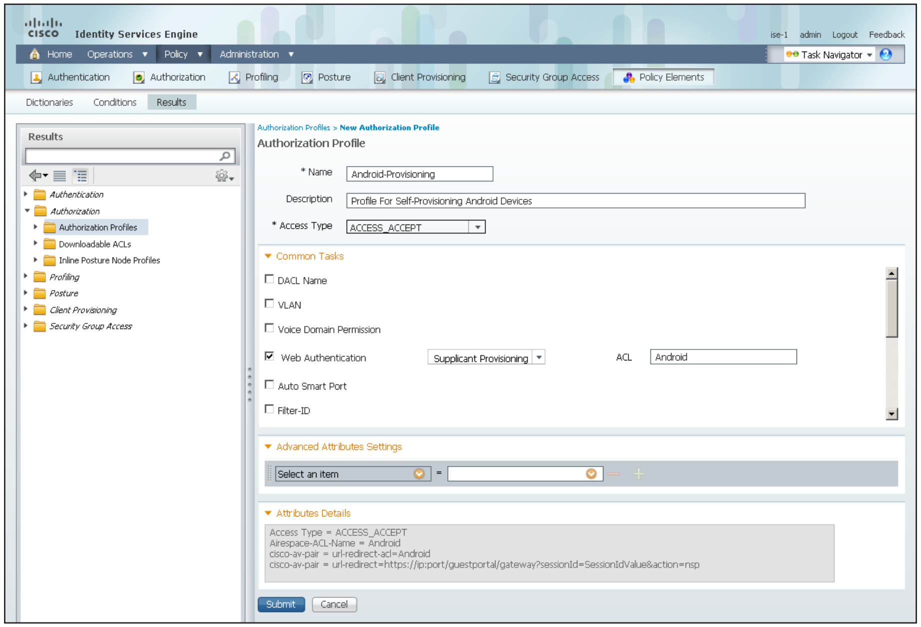
Step 4: Enter a name and description for the profile.

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**.


Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Dictionaries Conditions Results
Results
Authentication
Authorization
Authorization Profiles
Downloadable ACLs
Inline Posture Node Profiles
Profiling
Posture
Client Provisioning
Security Group Access
Authorization Profiles > New Authorization Profile
Submit Cancel

Authorization Profile

* Name: Android-Provisioning

Description: Profile For Self-Provisioning Android Devices

* Access Type: ACCESS_ACCEPT

Common Tasks

☐ DACL Name

☐ VLAN

☐ Voice Domain Permission

☑ Web Authentication — Supplicant Provisioning — ACL: Android

☐ Auto Smart Port

☐ Filter-ID

Advanced Attributes Settings

Select an item =

Attributes Details

```
Access Type = ACCESS_ACCEPT
Airespace-ACL-Name = Android
cisco-av-pair = url-redirect-acl=Android
cisco-av-pair = url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=nsp
```

Procedure 12 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 10.

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 11.

Step 12: Click **Done**, and then click **Save**.

Procedure 13 Create 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 14 Modify default rule

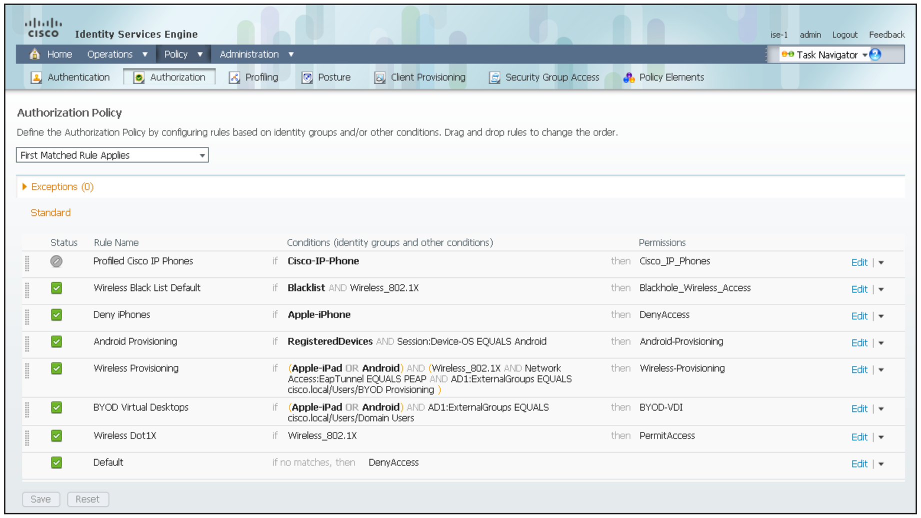
The last step is to modify the default rule to deny network access to any device that has not matched an existing authorization rule.

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**.


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

Authorization Policy

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

First Matched Rule Applies

Exceptions (0)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
⊘	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones	Edit | ▾
☑	Wireless Black List Default	if	**Blacklist** AND Wireless_802.1X	then	Blackhole_Wireless_Access	Edit | ▾
☑	Deny iPhones	if	**Apple-iPhone**	then	DenyAccess	Edit | ▾
☑	Android Provisioning	if	**RegisteredDevices** AND Session:Device-OS EQUALS Android	then	Android-Provisioning	Edit | ▾
☑	Wireless Provisioning	if	(**Apple-iPad** OR **Android**) AND (Wireless_802.1X AND Network Access:EapTunnel EQUALS PEAP AND AD1:ExternalGroups EQUALS cisco.local/Users/BYOD Provisioning)	then	Wireless-Provisioning	Edit | ▾
☑	BYOD Virtual Desktops	if	(**Apple-iPad** OR **Android**) AND AD1:ExternalGroups EQUALS cisco.local/Users/Domain Users	then	BYOD-VDI	Edit | ▾
☑	Wireless Dot1X	if	Wireless_802.1X	then	PermitAccess	Edit | ▾
☑	Default	if no matches, then	DenyAccess			Edit | ▾

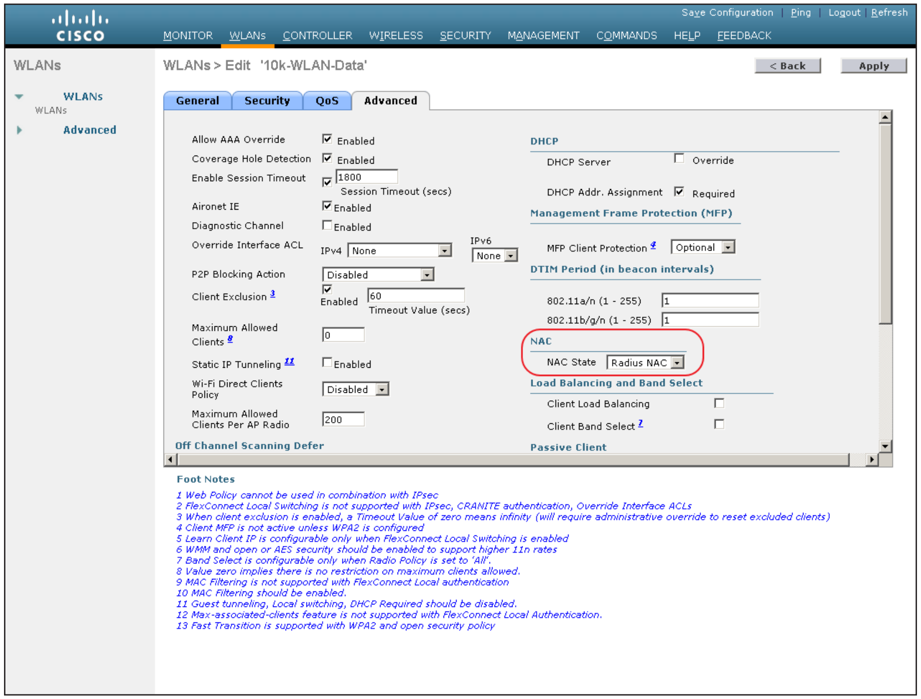
Procedure 15 Configure WLCs

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**.


cisco
Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
< Back
Apply
General Security QoS Advanced

WLANs > Edit '10k-WLAN-Data'

Allow AAA Override ☑ Enabled

Coverage Hole Detection ☑ Enabled

Enable Session Timeout ☑ 1800 Session Timeout (secs)

Aironet IE ☑ Enabled

Diagnostic Channel □ Enabled

Override Interface ACL IPv4 None IPv6 None

P2P Blocking Action Disabled

Client Exclusion [3] ☑ Enabled 60 Timeout Value (secs)

Maximum Allowed Clients [8] 0

Static IP Tunneling [11] □ Enabled

Wi-Fi Direct Clients Policy Disabled

Maximum Allowed Clients Per AP Radio 200

Off Channel Scanning Defer

DHCP

DHCP Server □ Override

DHCP Addr. Assignment ☑ Required

Management Frame Protection (MFP)

MFP Client Protection [4] Optional

DTIM Period (in beacon intervals)

802.11a/n (1 - 255) 1

802.11b/g/n (1 - 255) 1

NAC

NAC State Radius NAC

Load Balancing and Band Select

Client Load Balancing □

Client Band Select [7] □

Passive Client

Foot Notes

1 Web Policy cannot be used in combination with IPsec
2 FlexConnect Local Switching is not supported with IPsec, CRANITE authentication, Override Interface ACLs
3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients)
4 Client MFP is not active unless WPA2 is configured
5 Learn Client IP is configurable only when FlexConnect Local Switching is enabled
6 WMM and open or AES security should be enabled to support higher 11n rates
7 Band Select is configurable only when Radio Policy is set to 'All'.
8 Value zero implies there is no restriction on maximum clients allowed.
9 MAC Filtering is not supported with FlexConnect Local authentication
10 MAC Filtering should be enabled.
11 Guest tunneling, Local switching, DHCP Required should be disabled.
12 Max-associated-clients feature is not supported with FlexConnect Local Authentication.
13 Fast Transition is supported with WPA2 and open security policy

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**.

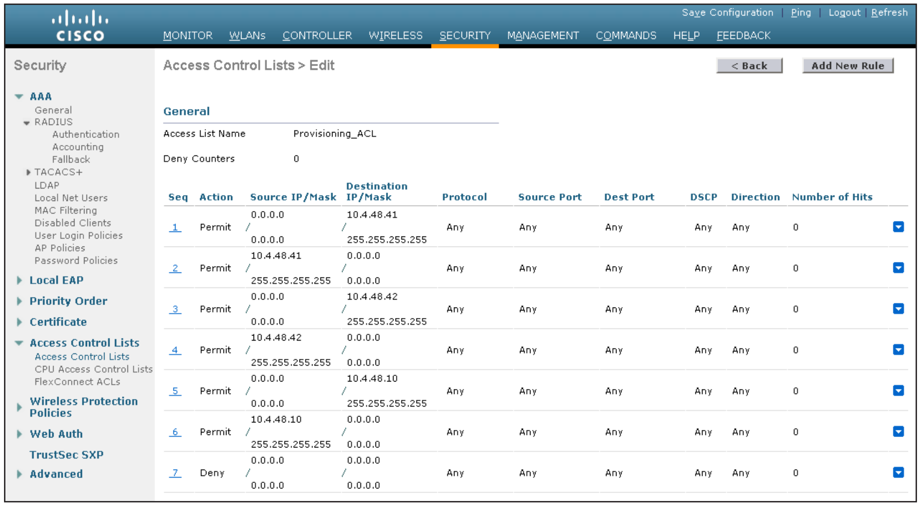
Step 6: Click **New**.

Step 7: Name the access list the same name that was used in Procedure 9, 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.



Access Control Lists > Edit

General

Access List Name: Provisioning_ACL

Deny Counters: 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	10.4.48.41 / 255.255.255.255	Any	Any	Any	Any	Any	0
2	Permit	10.4.48.41 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0
3	Permit	0.0.0.0 / 0.0.0.0	10.4.48.42 / 255.255.255.255	Any	Any	Any	Any	Any	0
4	Permit	10.4.48.42 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0
5	Permit	0.0.0.0 / 0.0.0.0	10.4.48.10 / 255.255.255.255	Any	Any	Any	Any	Any	0
6	Permit	10.4.48.10 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0
7	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0

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 11, and then click **Apply**.

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

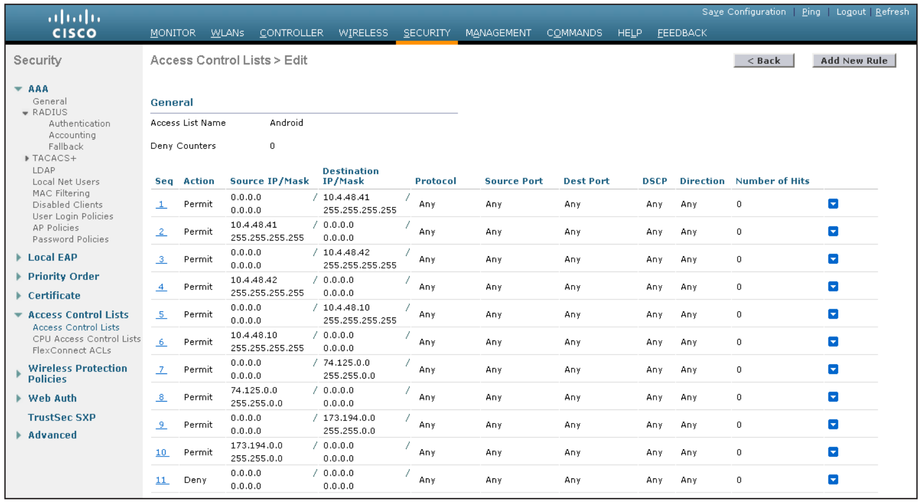
Step 15: Click **Add New Rule**.

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**.



Access Control Lists > Edit

General

Access List Name: Android

Deny Counters: 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	10.4.48.41 / 255.255.255.255	Any	Any	Any	Any	Any	0
2	Permit	10.4.48.41 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0
3	Permit	0.0.0.0 / 0.0.0.0	10.4.48.42 / 255.255.255.255	Any	Any	Any	Any	Any	0
4	Permit	10.4.48.42 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0
5	Permit	0.0.0.0 / 0.0.0.0	10.4.48.10 / 255.255.255.255	Any	Any	Any	Any	Any	0
6	Permit	10.4.48.10 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0
7	Permit	0.0.0.0 / 0.0.0.0	74.125.0.0 / 255.255.0.0	Any	Any	Any	Any	Any	0
8	Permit	74.125.0.0 / 255.255.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0
9	Permit	0.0.0.0 / 0.0.0.0	173.194.0.0 / 255.255.0.0	Any	Any	Any	Any	Any	0
10	Permit	173.194.0.0 / 255.255.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0
11	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0

Procedure 16 Create profiles for user groups

The current policy permits full network access to any device that was provisioned. Devices that have not been provisioned are limited to accessing the virtual desktop infrastructure and the Internet. To refine the policy further, limit the parts of the network the employee can access with a provisioned device, based on their AD group.

The policy in this procedure pushes an access list to the WLC that allows only access to the Internet and part of the internal network for users in the IT group, who are using either an iPad or an Android device. The access list can be deployed only 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.

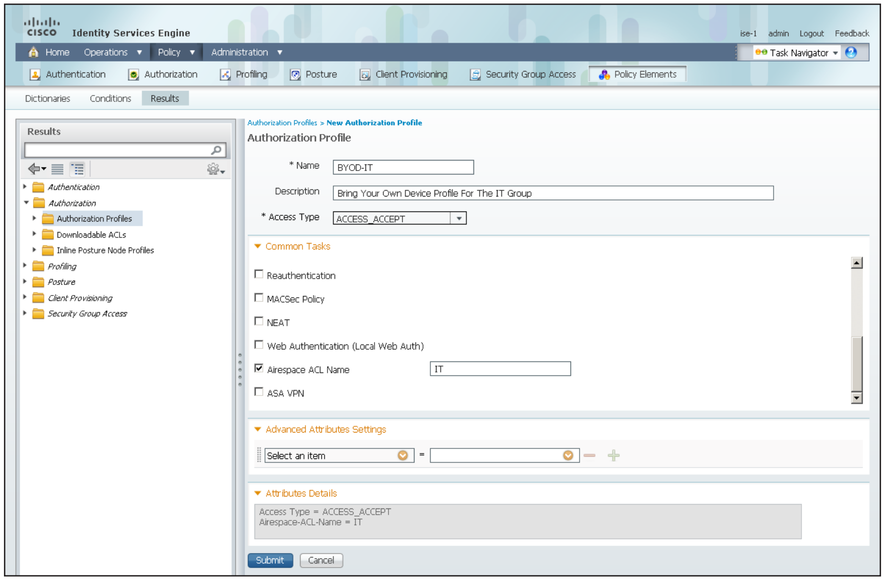
Step 2: On the menu bar, mouse over **Policy**, and then, in the Policy Elements section, choose **Results**.

Step 3: In the left pane, double-click **Authorization,** and then select **Authorization Profiles**.

Step 4: Click **Add**.

Step 5: Enter a name (example: BYOD-IT-Provisioned) and a description for the policy.

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


cisco Identity Services Engine
ise-1 admin Logout Feedback
Home Operations ▾ Policy ▾ Administration ▾
Task Navigator ▾
Authentication Authorization Profiling Posture Client Provisioning Security Group Access Policy Elements
Dictionaries Conditions Results
Results
Authentication
Authorization
Authorization Profiles
Downloadable ACLs
Inline Posture Node Profiles
Profiling
Posture
Client Provisioning
Security Group Access
Authorization Profiles > New Authorization Profile
Authorization Profile
Common Tasks
Advanced Attributes Settings
Select an item
Attributes Details
Submit
Cancel

* Name: BYOD-IT

Description: Bring Your Own Device Profile For The IT Group

* Access Type: ACCESS_ACCEPT

□ Reauthentication

□ MACSec Policy

□ NEAT

□ Web Authentication (Local Web Auth)

☑ Airespace ACL Name: IT

□ ASA VPN

```
Access Type = ACCESS_ACCEPT
Airespace-ACL-Name = IT
```

Step 7: Click **Submit**.

Procedure 17 Create authorization rules for user groups

The following steps describe how to create an authorization rule that uses the profile created in Procedure 16, “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 BYOD Virtual Desktops 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 Virtual Desktops rule created earlier.

Step 3: Rename “Standard Rule 1” to **BYOD IT Provisioned**.

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 Network Access, click the > symbol, and then choose **EapAuthentication**.

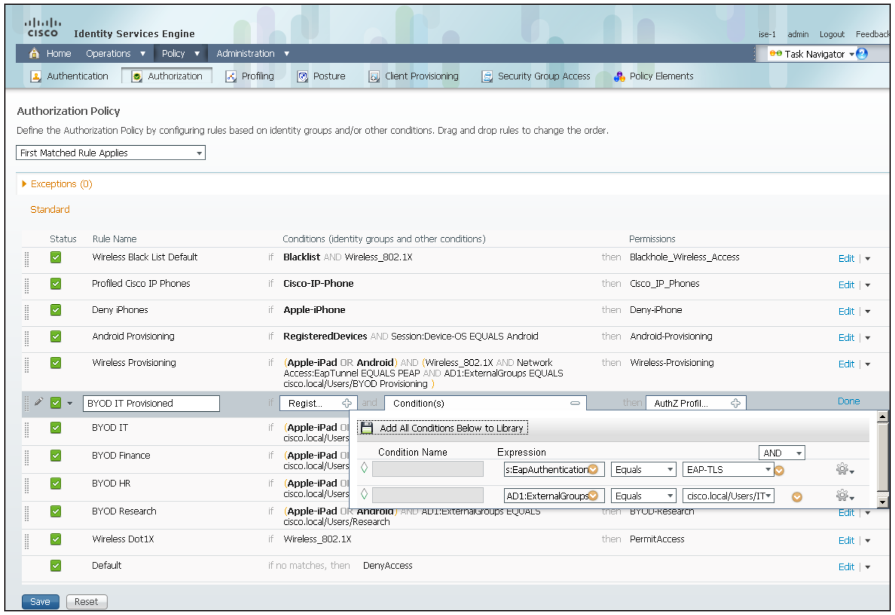
Step 9: Under Expression, in the first list, choose **Equals**, and then, in the second list, choose **EAP-TLS**.

Step 10: At the end of this rule, click the gear icon, and then select **Add Attribute/Value**.

Step 11: Next to Select Attribute, click the arrow. This opens the menu.

Step 12: Next to AD1, click the > symbol, and then choose **ExternalGroups**.

Step 13: Under Expression, in the first list, choose **Equals**, and then, in the second list, choose the IT group.


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

Authorization Policy

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

First Matched Rule Applies

Exceptions (0)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
☑	Wireless Black List Default	if	**Blacklist** AND Wireless_802.1X	then	Blackhole_Wireless_Access	Edit | ▾
☑	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones	Edit | ▾
☑	Deny iPhones	if	**Apple-iPhone**	then	Deny-iPhone	Edit | ▾
☑	Android Provisioning	if	**RegisteredDevices** AND Session:Device-OS EQUALS Android	then	Android-Provisioning	Edit | ▾
☑	Wireless Provisioning	if	(**Apple-iPad** OR **Android**) AND (Wireless_802.1X AND Network Access:EapTunnel EQUALS PEAP AND AD1:ExternalGroups EQUALS cisco.local/Users/BYOD Provisioning)	then	Wireless-Provisioning	Edit | ▾
☑	BYOD IT Provisioned	if	Regist... and Condition(s)	then	AuthZ Profil...	Done
☑	BYOD IT	if	(**Apple-iPad** O cisco.local/Users			
☑	BYOD Finance	if	(**Apple-iPad** O cisco.local/Users			
☑	BYOD HR	if	(**Apple-iPad** O cisco.local/Users			
☑	BYOD Research	if	(**Apple-iPad** OR **Android**) AND AD1:ExternalGroups EQUALS cisco.local/Users/Research	then	BYOD-Research	Edit | ▾
☑	Wireless Dot1X	if	Wireless_802.1X	then	PermitAccess	Edit | ▾
☑	Default	if no matches, then	DenyAccess			Edit | ▾

Add All Conditions Below to Library

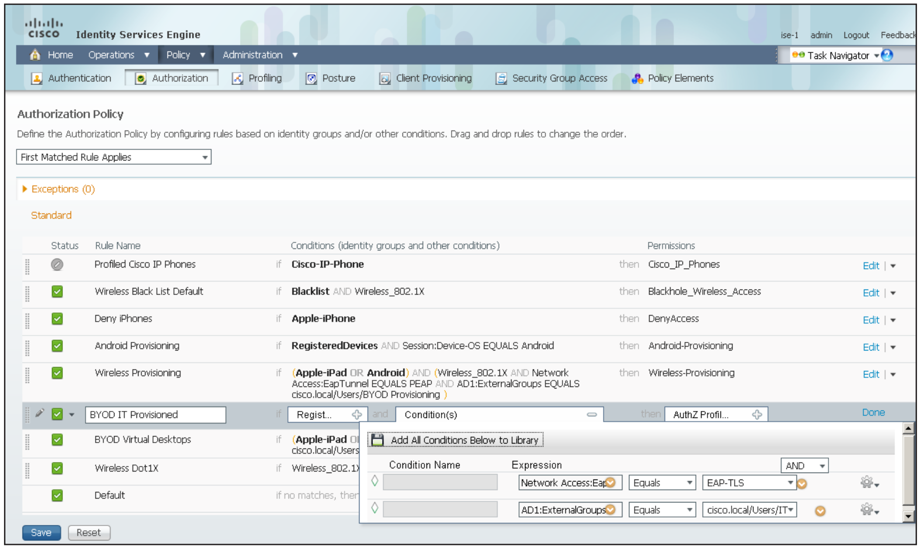
Condition Name	Expression			AND
	s:EapAuthentication	Equals	EAP-TLS	
	AD1:ExternalGroups	Equals	cisco.local/Users/IT	

Save Reset

Step 14: Next to AuthZ Profile(s), click the + symbol, and then, next to Select an item, click the arrow.

Step 15: Next to Standard, click the > symbol, and then choose the authorization profile BYOD-IT.

Step 16: Click **Done**, and then click **Save**.


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

Authorization Policy

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

First Matched Rule Applies

Exceptions (0)

Standard

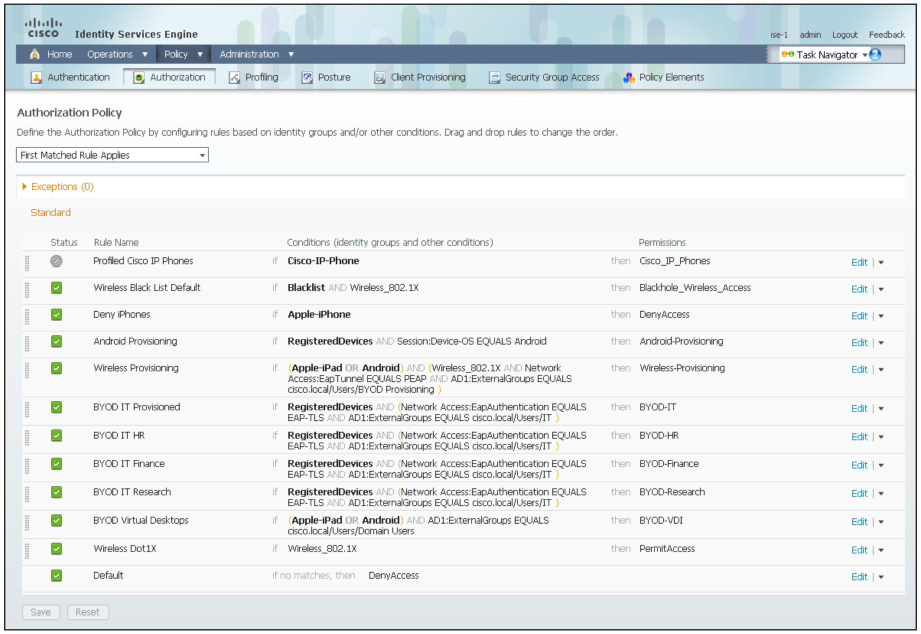
Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
⊘	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones	Edit | ▾
☑	Wireless Black List Default	if	**Blacklist** AND Wireless_802.1X	then	Blackhole_Wireless_Access	Edit | ▾
☑	Deny iPhones	if	**Apple-iPhone**	then	DenyAccess	Edit | ▾
☑	Android Provisioning	if	**RegisteredDevices** AND Session:Device-OS EQUALS Android	then	Android-Provisioning	Edit | ▾
☑	Wireless Provisioning	if	(**Apple-iPad** OR **Android**) AND (Wireless_802.1X AND Network Access:EapTunnel EQUALS PEAP AND AD1:ExternalGroups EQUALS cisco.local/Users/BYOD Provisioning)	then	Wireless-Provisioning	Edit | ▾
☑	BYOD IT Provisioned	if	Regist... and Condition(s)	then	AuthZ Profil...	Done
☑	BYOD Virtual Desktops	if	(**Apple-iPad** O cisco.local/Users			
☑	Wireless Dot1X	if	Wireless_802.1X			
☑	Default	if no matches, then				

Add All Conditions Below to Library

Condition Name	Expression			AND
	Network Access:Eap	Equals	EAP-TLS	
	AD1:ExternalGroups	Equals	cisco.local/Users/IT	

Save Reset

Step 17: 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.


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

Authorization Policy

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

First Matched Rule Applies ▾

▸ Exceptions (0)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions	
⊘	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones	Edit | ▾
☑	Wireless Black List Default	if	**Blacklist** AND Wireless_802.1X	then	Blackhole_Wireless_Access	Edit | ▾
☑	Deny iPhones	if	**Apple-iPhone**	then	DenyAccess	Edit | ▾
☑	Android Provisioning	if	**RegisteredDevices** AND Session:Device-OS EQUALS Android	then	Android-Provisioning	Edit | ▾
☑	Wireless Provisioning	if	(**Apple-iPad** OR **Android**) AND (Wireless_802.1X AND Network Access:EapTunnel EQUALS PEAP AND AD1:ExternalGroups EQUALS cisco.local/Users/BYOD Provisioning)	then	Wireless-Provisioning	Edit | ▾
☑	BYOD IT Provisioned	if	**RegisteredDevices** AND (Network Access:EapAuthentication EQUALS EAP-TLS AND AD1:ExternalGroups EQUALS cisco.local/Users/IT)	then	BYOD-IT	Edit | ▾
☑	BYOD IT HR	if	**RegisteredDevices** AND (Network Access:EapAuthentication EQUALS EAP-TLS AND AD1:ExternalGroups EQUALS cisco.local/Users/IT)	then	BYOD-HR	Edit | ▾
☑	BYOD IT Finance	if	**RegisteredDevices** AND (Network Access:EapAuthentication EQUALS EAP-TLS AND AD1:ExternalGroups EQUALS cisco.local/Users/IT)	then	BYOD-Finance	Edit | ▾
☑	BYOD IT Research	if	**RegisteredDevices** AND (Network Access:EapAuthentication EQUALS EAP-TLS AND AD1:ExternalGroups EQUALS cisco.local/Users/IT)	then	BYOD-Research	Edit | ▾
☑	BYOD Virtual Desktops	if	(**Apple-iPad** OR **Android**) AND AD1:ExternalGroups EQUALS cisco.local/Users/Domain Users	then	BYOD-VDI	Edit | ▾
☑	Wireless Dot1X	if	Wireless_802.1X	then	PermitAccess	Edit | ▾
☑	Default	if no matches, then	DenyAccess			Edit | ▾

Procedure 18 Delete wireless 802.1X rule

Now that you have created specific authorization rules, you need to delete the generic, catch-all rule 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 Wireless Dot1X rule, click the black triangle, and then select **Delete**.

Step 3: Verify that you want to delete the rule, click **Delete**, and then click **Save**.

Procedure 19 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 on 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**.

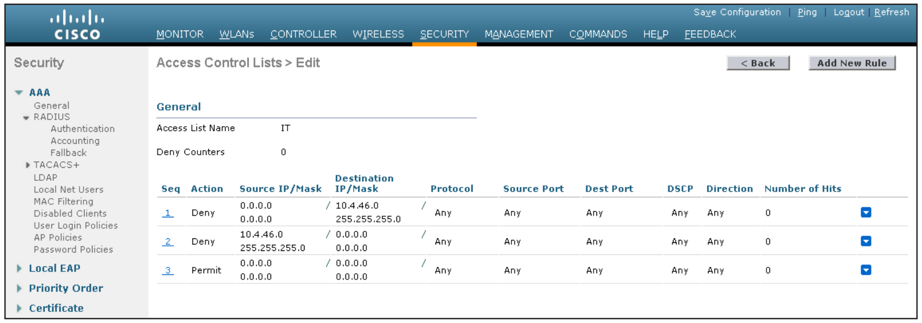
Step 4: Click **New**.

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**. Create additional rules to complete the policy. In our example deployment, users in the IT group are prevented from accessing a section of the internal network, but are allowed to access the rest of the internal network and the Internet.



Access Control Lists > Edit

General

Access List Name IT

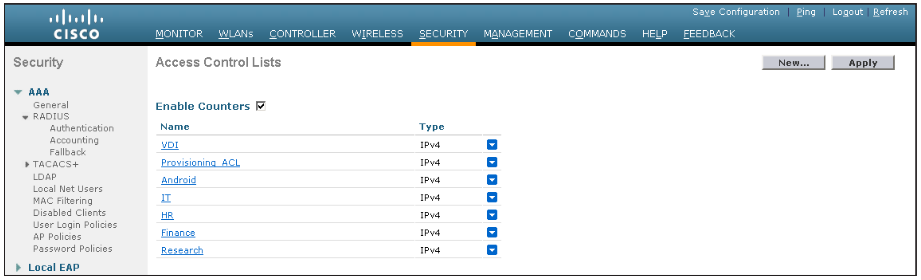
Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Deny	0.0.0.0 / 0.0.0.0	10.4.46.0 / 255.255.255.0	Any	Any	Any	Any	Any	0
2	Deny	10.4.46.0 / 255.255.255.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0
3	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0

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 3 through Step 8 in this procedure for each access list that you defined in the authorization profiles in Cisco ISE.



Access Control Lists

Enable Counters ☑

Name	Type
VDI	IPv4
Provisioning_ACL	IPv4
Android	IPv4
IT	IPv4
HR	IPv4
Finance	IPv4
Research	IPv4

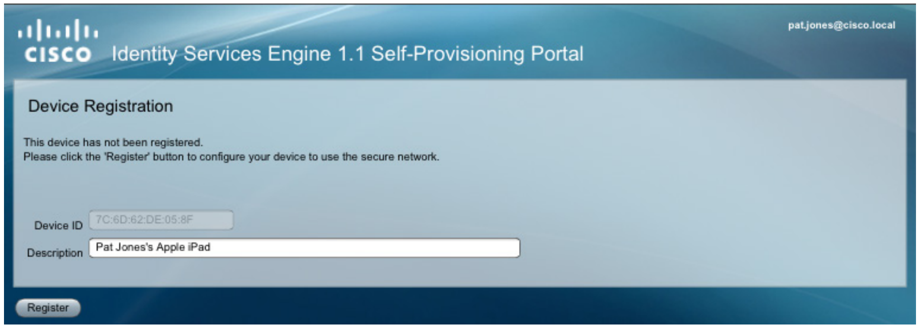
Procedure 20 Provision an Apple iPad

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.

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

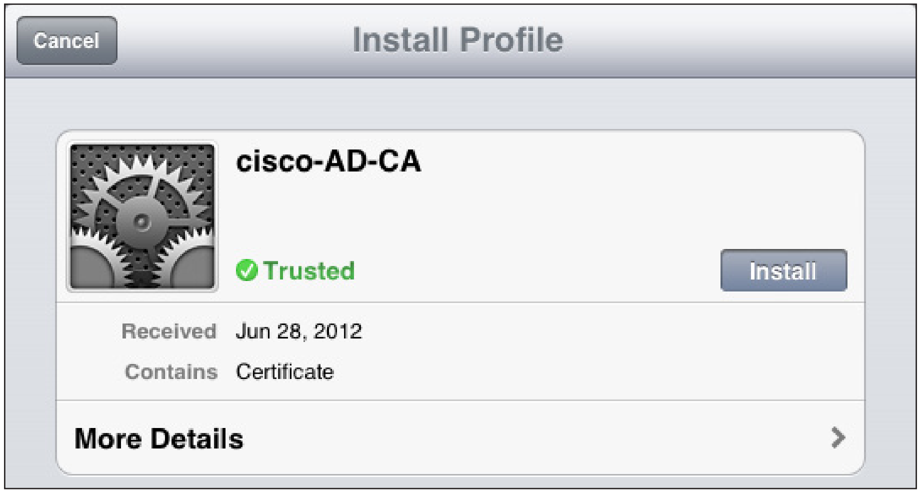


Device Registration

This device has not been registered.
Please click the 'Register' button to configure your device to use the secure network.

Device ID: 7C:6D:62:DE:05:8F
Description: Pat Jones's Apple iPad

Step 4: Click **Install**. The trusted root certificate from the CA installs.



cisco-AD-CA

✓ Trusted

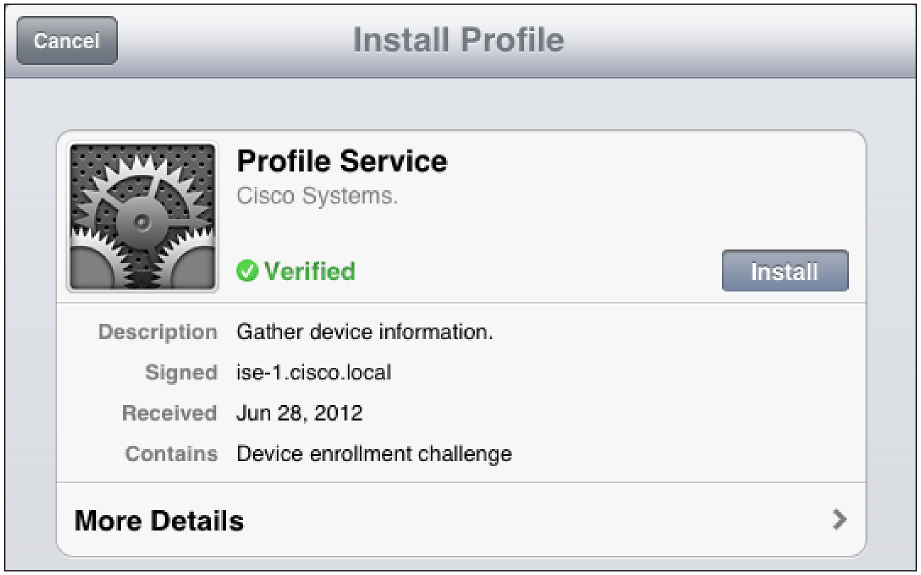
Received: Jun 28, 2012
Contains: Certificate

Step 5: On the warning message that appears, click **Install**.

Step 6: Click **Done**. The Safari and the Self-Provisioning Portal displays.

Step 7: Click **Register**.

Step 8: To install the user certificate, click **Install**.



Profile Service
Cisco Systems.
Verified

Description Gather device information.
Signed ise-1.cisco.local
Received Jun 28, 2012
Contains Device enrollment challenge

Step 9: On the warning message that appears, click **Install Now**. The profile installs.

Step 10: Click **Done**.

You now need to manually connect to the wireless network using the new profile.

Step 11: On the iPad, open **Settings**, and then choose **Wi-Fi**.

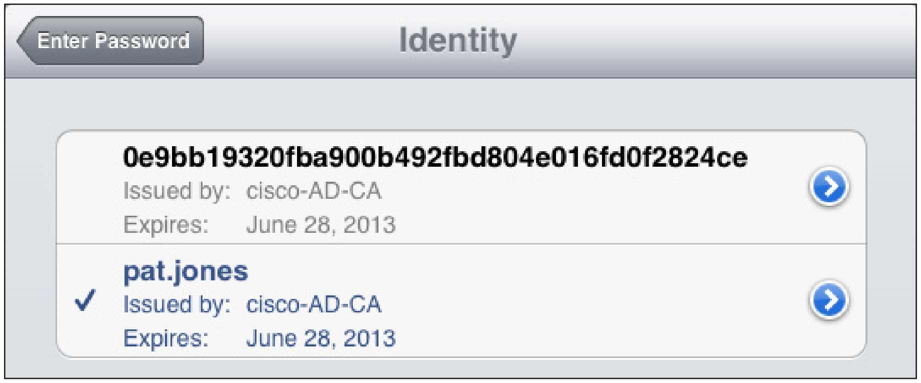
Step 12: Next to the network, click the blue arrow, click **Forget this Network**, and then, on the verification message, click **Forget**.

Step 13: Return to the wireless settings by clicking **Wi-Fi**, and then select the network from the list.

Step 14: Click **Mode**, and then select **EAP-TLS**.

Step 15: Enter the username, and then click **Identity**.

Step 16: Choose the profile for the user, and then click **Enter Password**. You are returned to the previous screen.



0e9bb19320fba900b492fbd804e016fd0f2824ce
Issued by: cisco-AD-CA
Expires: June 28, 2013

✓ pat.jones
Issued by: cisco-AD-CA
Expires: June 28, 2013

Step 17: Click **Join**. You are connected to the network using EAP-TLS and the newly provisioned certificate.

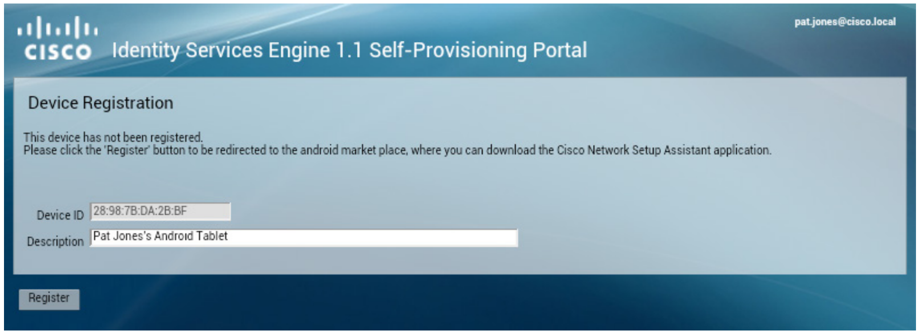
Procedure 21 Provision an Android tablet

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**.



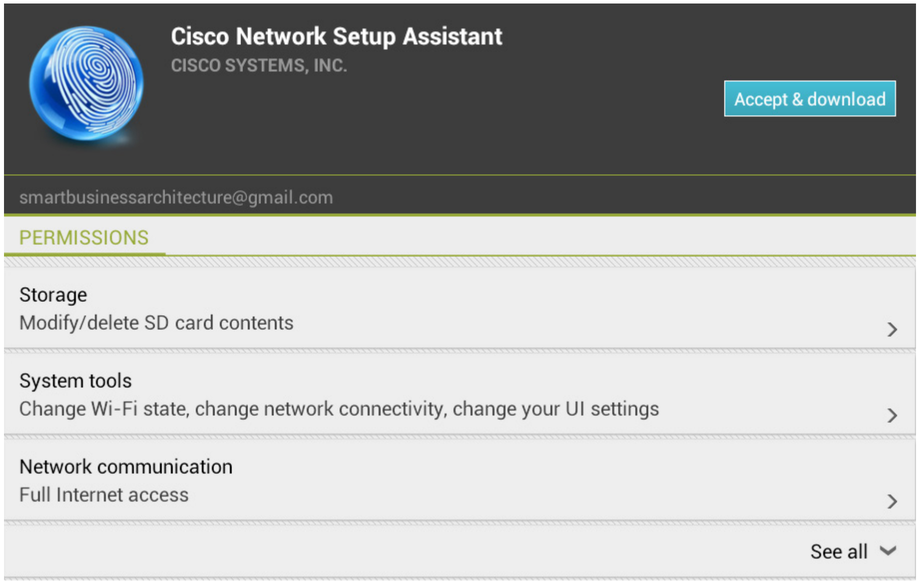
Device Registration

This device has not been registered.
Please click the 'Register' button to be redirected to the android market place, where you can download the Cisco Network Setup Assistant application.

Device ID 28:98:7B:DA:2B:BF
Description Pat Jones's Android Tablet

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

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



Cisco Network Setup Assistant
CISCO SYSTEMS, INC.

smartbusinessarchitecture@gmail.com

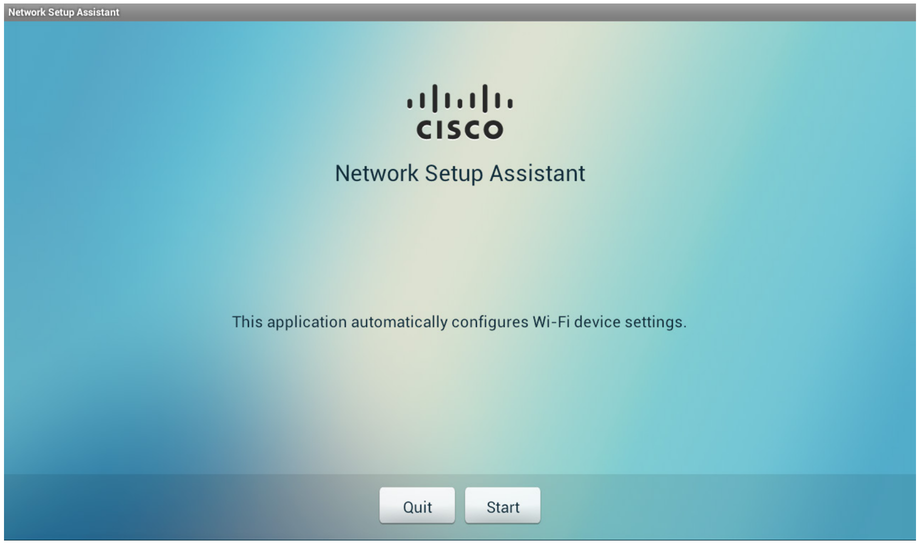
PERMISSIONS

Storage
Modify/delete SD card contents

System tools
Change Wi-Fi state, change network connectivity, change your UI settings

Network communication
Full Internet access

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

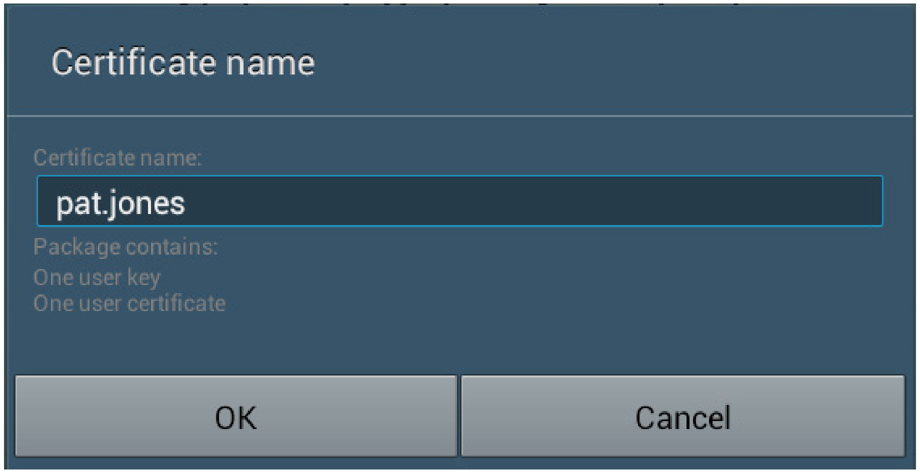


Network Setup Assistant

Network Setup Assistant

This application automatically configures Wi-Fi device settings.

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

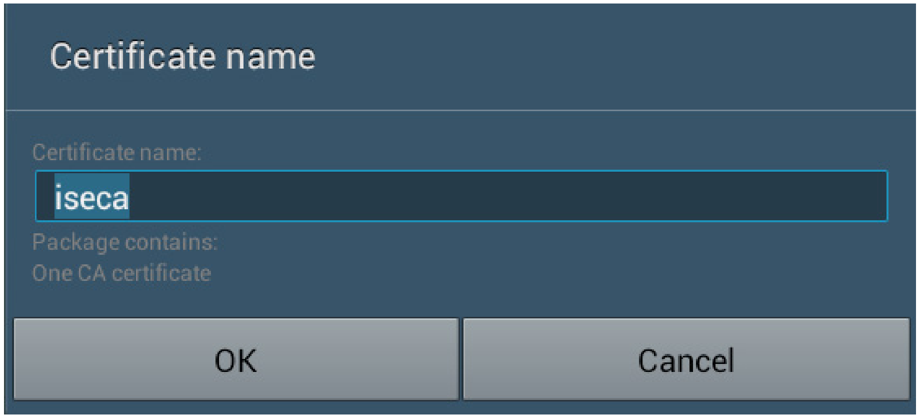


Certificate name

Certificate name: pat.jones

Package contains:
One user key
One user certificate

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



Certificate name

Certificate name: iseca

Package contains:
One CA certificate

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

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

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

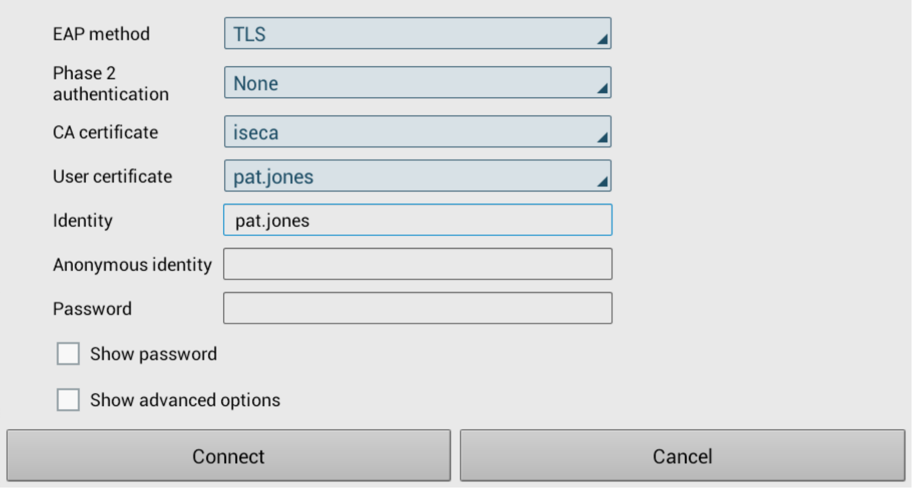
Step 12: Select the network from the list. This allows you to configure the options for connecting.

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

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

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

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



EAP method	TLS
Phase 2 authentication	None
CA certificate	iseca
User certificate	pat.jones
Identity	pat.jones
Anonymous identity	
Password	

□ Show password

□ Show advanced options

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.

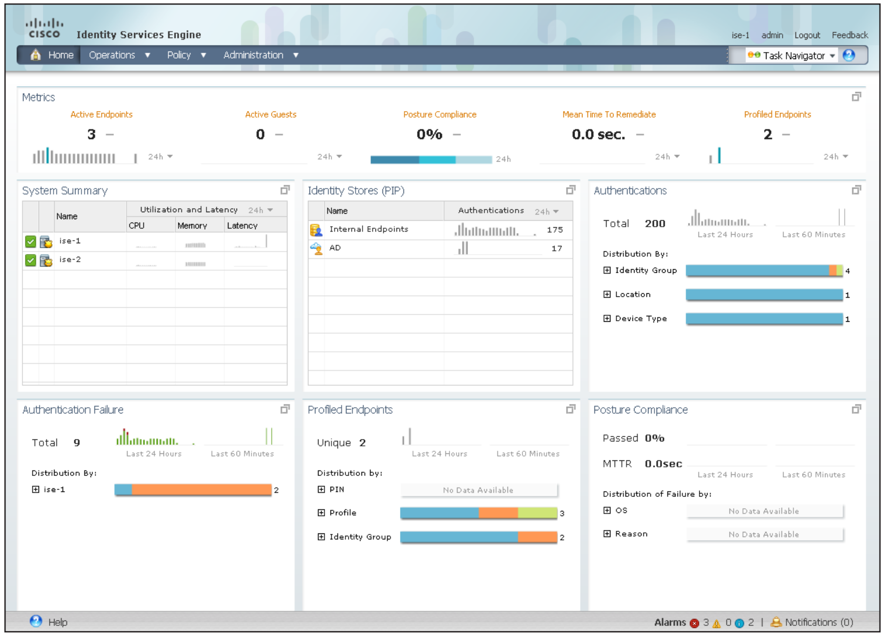
Cisco ISE is now configured to authenticate users and to profile endpoints based on RADIUS and DHCP information. The reporting capabilities of Cisco ISE allow you to determine what type of device is connecting to your network, when it connects, and where it connects from. Also, you will know who is connecting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



Metrics

Active Endpoints	Active Guests	Posture Compliance	Mean Time To Remediate	Profiled Endpoints
3 –	0 –	0% –	0.0 sec. –	2 –

System Summary

	Name	Utilization and Latency 24h ▾		
		CPU	Memory	Latency
☑	ise-1			
☑	ise-2			

Identity Stores (PIP)

Name	Authentications 24h ▾
Internal Endpoints	175
AD	17

Authentications

Total 200

Distribution By:

⊞ Identity Group	4
⊞ Location	1
⊞ Device Type	1

Authentication Failure

Total 9

Distribution By:

⊞ ise-1	2

Profiled Endpoints

Unique 2

Distribution by:

⊞ PIN	No Data Available
⊞ Profile	3
⊞ Identity Group	2

Posture Compliance

Passed 0%

MTTR 0.0sec

Distribution of Failure by:

⊞ OS	No Data Available
⊞ Reason	No Data Available

Procedure 2 Configure identity groups

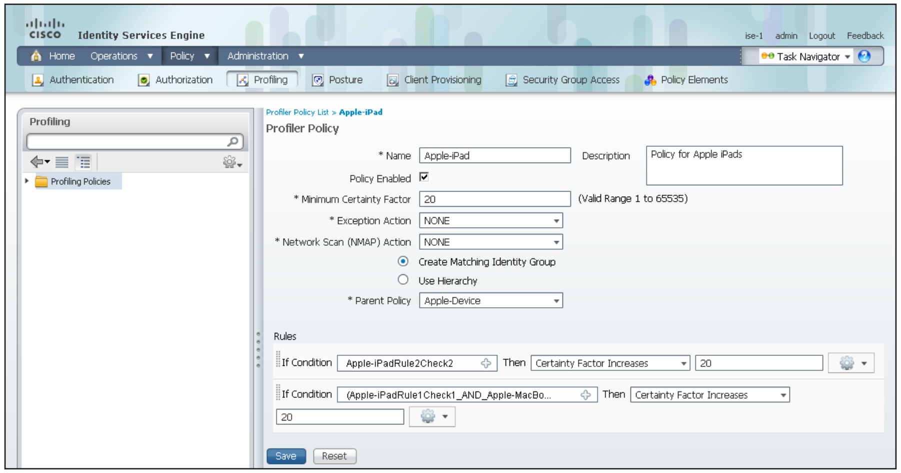
Cisco ISE has more in-depth reporting options to give more details on the devices connecting to the network. To identify the endpoints, you can use identity groups to classify profiled endpoints and to generate reports.

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**.



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

Profiler Policy List > Apple-iPad

Profiler Policy

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

Rules

If Condition Apple-iPadRule2Check2 Then Certainty Factor Increases 20

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

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

Procedure 3 Add a custom profile

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

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

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

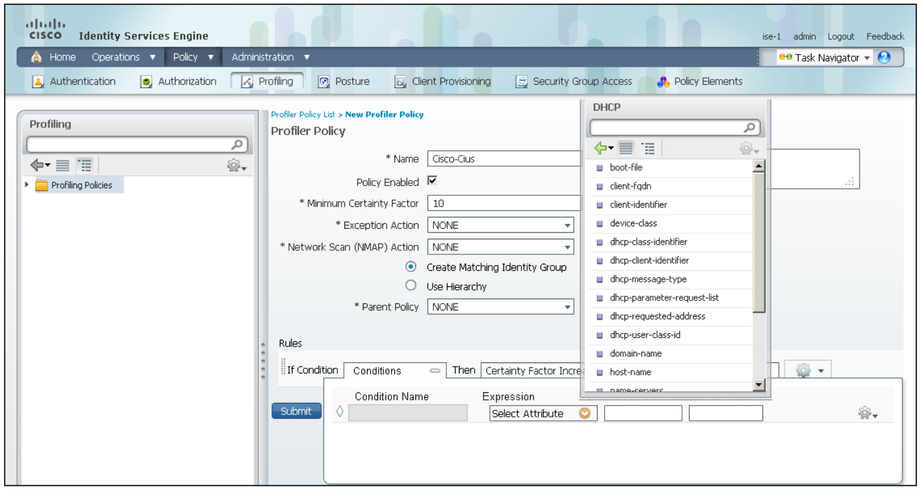
Step 2: Mouse over **Policy**, and then, from the drop-down menu, choose **Profiling**.

Step 3: Click **Create**.

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

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

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



Profiler Policy List > New Profiler Policy

Profiler Policy

* Name: Cisco-Cius

Policy Enabled ☑

* Minimum Certainty Factor: 10

* Exception Action: NONE

* Network Scan (NMAP) Action: NONE

● Create Matching Identity Group

○ Use Hierarchy

* Parent Policy: NONE

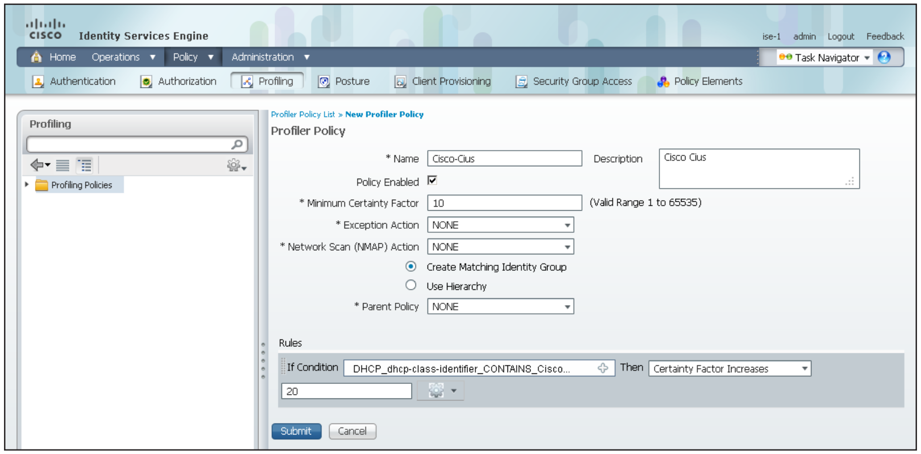
Rules

If Condition: Conditions Then: Certainty Factor Incre

Condition Name | Expression: Select Attribute

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

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



Profiler Policy List > New Profiler Policy

Profiler Policy

* Name: Cisco-Cius Description: Cisco Cius

Policy Enabled ☑

* Minimum Certainty Factor: 10 (Valid Range 1 to 65535)

* Exception Action: NONE

* Network Scan (NMAP) Action: NONE

● Create Matching Identity Group

○ Use Hierarchy

* Parent Policy: NONE

Rules

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

20

Procedure 4 Examining the authentication log

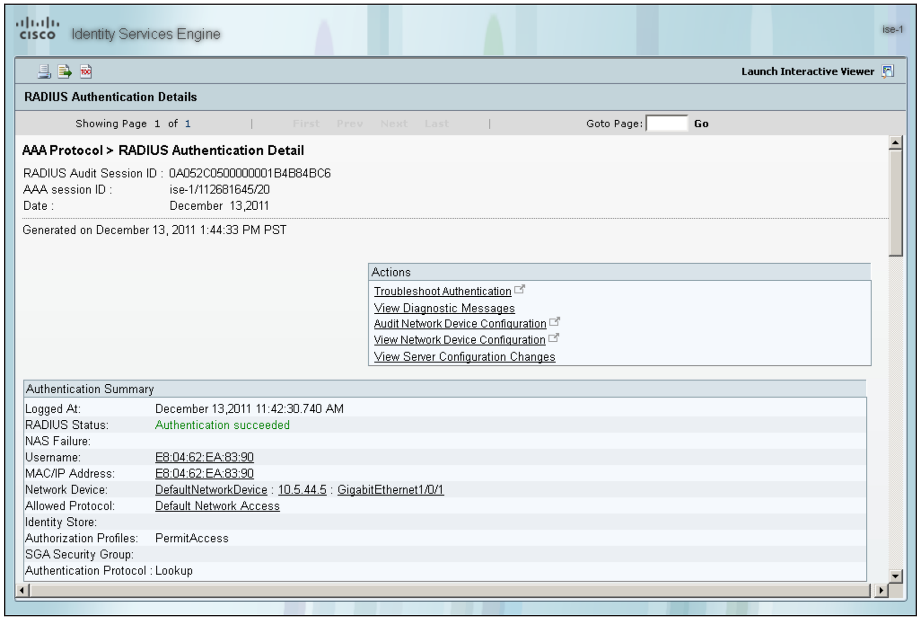
Step 1: On the menu bar, mouse over **Operations**, and then choose **Authentications**. The authentication log displays. The default option is to display the last 20 records from the last 24 hours.

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

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

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

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


Identity Services Engine
ise-1
Launch Interactive Viewer
RADIUS Authentication Details
Showing Page 1 of 1 | First Prev Next Last | Goto Page: Go

AAA Protocol > RADIUS Authentication Detail

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

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

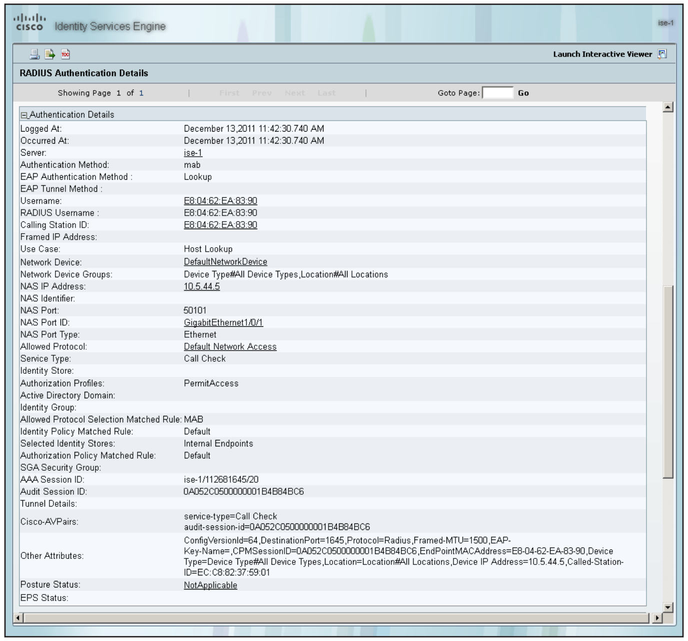
Actions

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

Authentication Summary

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

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


Identity Services Engine
ise-1
Launch Interactive Viewer
RADIUS Authentication Details
Showing Page 1 of 1 | First Prev Next Last | Goto Page: Go

Authentication Details

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

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

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

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

Procedure 5 Create custom authentication reports

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

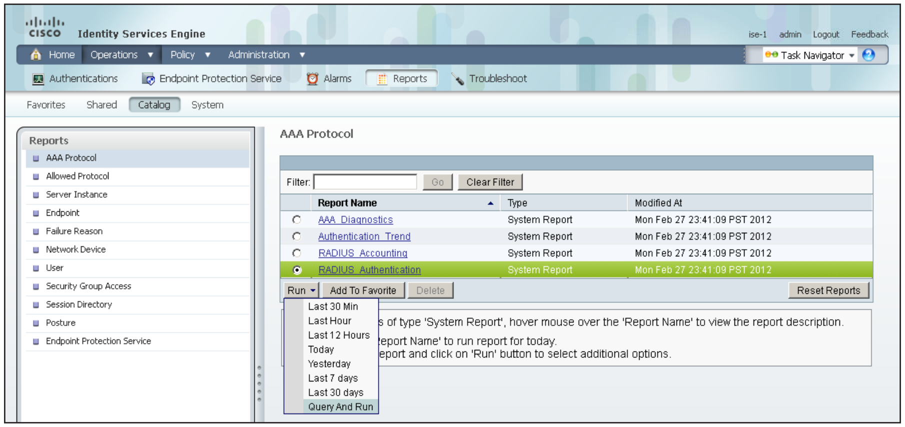
Step 1: On the menu bar, mouse over **Operations**, and then, in the Reports section, choose **Catalog**.

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

Step 3: Select **RADIUS Authentication**.

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

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

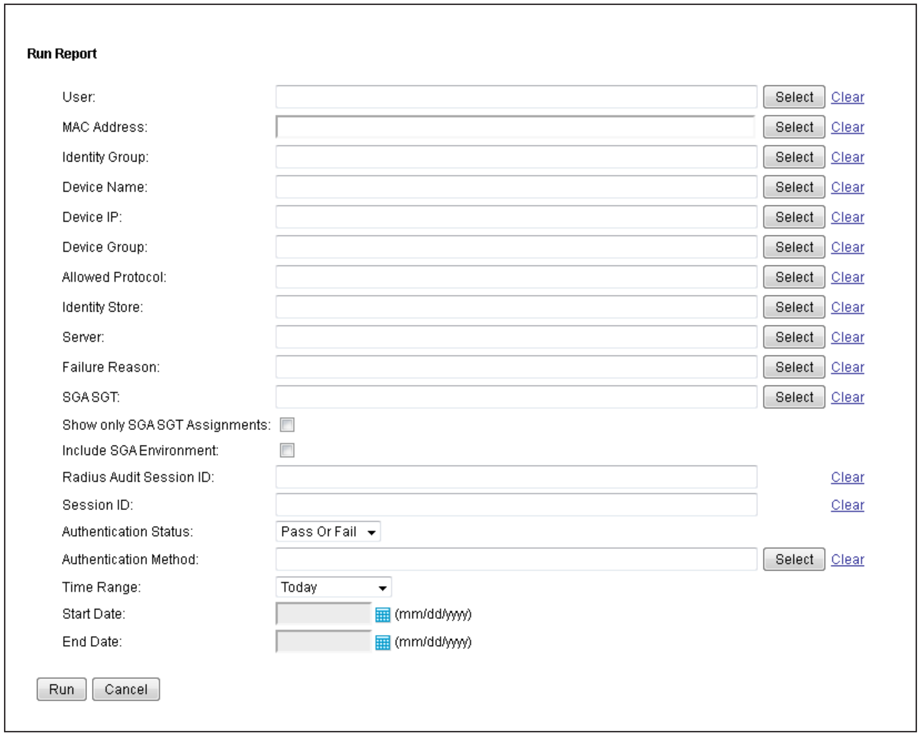


	Report Name	Type	Modified At
○	AAA_Diagnostics	System Report	Mon Feb 27 23:41:09 PST 2012
○	Authentication_Trend	System Report	Mon Feb 27 23:41:09 PST 2012
○	RADIUS_Accounting	System Report	Mon Feb 27 23:41:09 PST 2012
●	RADIUS_Authentication	System Report	Mon Feb 27 23:41:09 PST 2012

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

Step 6: If you want to select a time range that is not listed, choose **Query and Run**. All the parameters available for the report display. After choosing the parameters you want, click **Run** to generate the report.

Figure 2 - RADIUS report parameters



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

Procedure 6 Identify endpoints

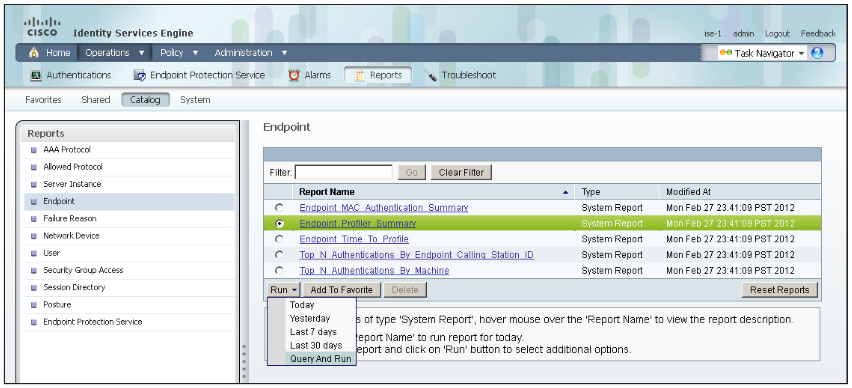
Using information gleaned from the RADIUS and DHCP requests, Cisco ISE can identify what types of devices are connecting to the network. This can assist in determining the network security policy based on the type of device that is in use.

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.



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

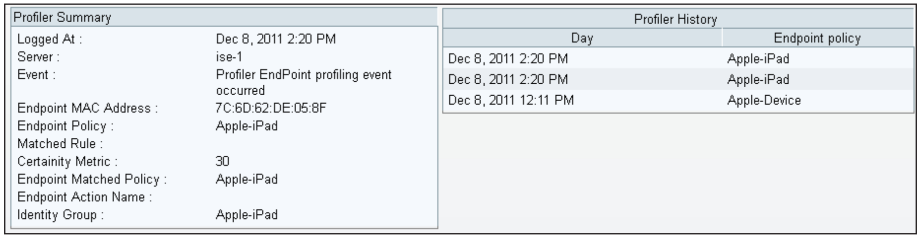
s of type 'System Report', hover mouse over the 'Report Name' to view the report description.

eport Name' to run report for today.
eport and click on 'Run' button to select additional options.

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

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

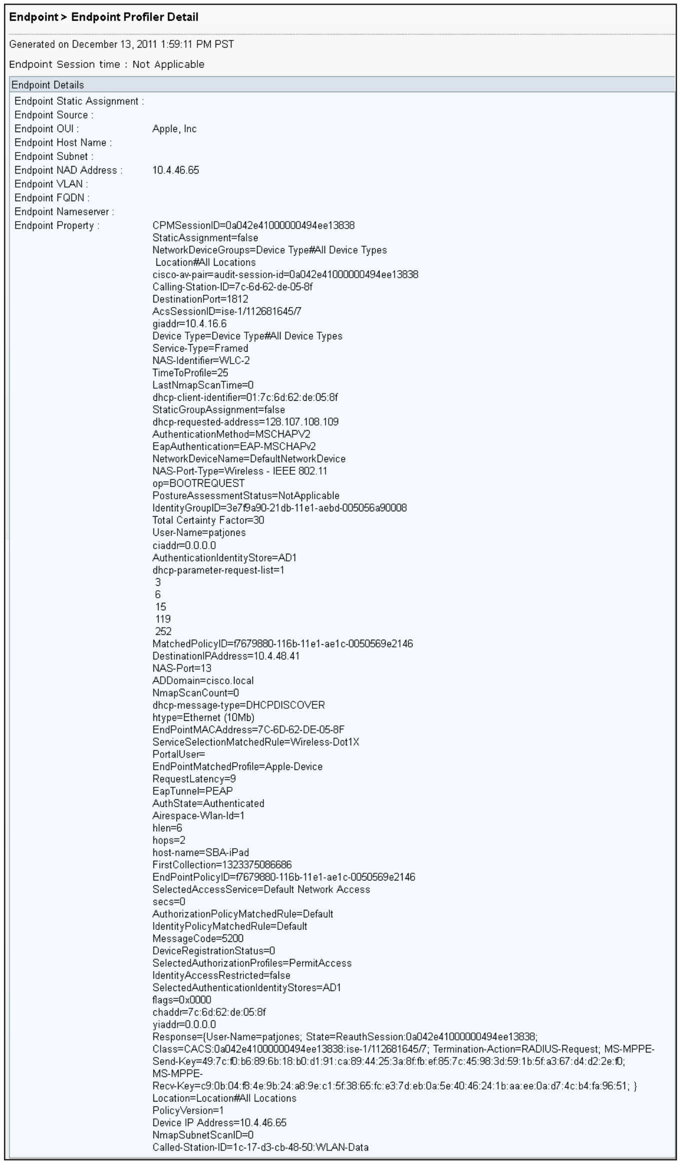
Figure 3 - Endpoint profile summary



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

Profiler History	
Day	Endpoint policy
Dec 8, 2011 2:20 PM	Apple-iPad
Dec 8, 2011 2:20 PM	Apple-iPad
Dec 8, 2011 12:11 PM	Apple-Device

Figure 4 - Endpoint Details



Endpoint > Endpoint Profiler Detail

Generated on December 13, 2011 1:59:11 PM PST

Endpoint Session time : Not Applicable

```
Endpoint Details
 Endpoint Static Assignment :
 Endpoint Source :
 Endpoint OUI :              Apple, Inc
 Endpoint Host Name :
 Endpoint Subnet :
 Endpoint NAD Address :      10.4.46.65
 Endpoint VLAN :
 Endpoint FQDN :
 Endpoint Nameserver :
 Endpoint Property :         CPMSessionID=0a042e41000000494ee13838
                             StaticAssignment=false
                             NetworkDeviceGroups=Device Type#All Device Types
                              Location#All Locations
                             cisco-av-pair=audit-session-id=0a042e41000000494ee13838
                             Calling-Station-ID=7c-6d-62-de-05-8f
                             DestinationPort=1812
                             AcsSessionID=ise-1/112681645/7
                             giaddr=10.4.16.6
                             Device Type=Device Type#All Device Types
                             Service-Type=Framed
                             NAS-Identifier=WLC-2
                             TimeToProfile=25
                             LastNmapScanTime=0
                             dhcp-client-identifier=01:7c:6d:62:de:05:8f
                             StaticGroupAssignment=false
                             dhcp-requested-address=128.107.108.109
                             AuthenticationMethod=MSCHAPV2
                             EapAuthentication=EAP-MSCHAPv2
                             NetworkDeviceName=DefaultNetworkDevice
                             NAS-Port-Type=Wireless - IEEE 802.11
                             op=BOOTREQUEST
                             PostureAssessmentStatus=NotApplicable
                             IdentityGroupID=3e7f9a90-21db-11e1-aebd-005056a90008
                             Total Certainty Factor=30
                             User-Name=patjones
                             ciaddr=0.0.0.0
                             AuthenticationIdentityStore=AD1
                             dhcp-parameter-request-list=1
                              3
                              6
                              15
                              119
                              252
                             MatchedPolicyID=f7679880-116b-11e1-ae1c-0050569e2146
                             DestinationIPAddress=10.4.48.41
                             NAS-Port=13
                             ADDomain=cisco.local
                             NmapScanCount=0
                             dhcp-message-type=DHCPDISCOVER
                             htype=Ethernet (10Mb)
                             EndPointMACAddress=7C-6D-62-DE-05-8F
                             ServiceSelectionMatchedRule=Wireless-Dot1X
                             PortalUser=
                             EndPointMatchedProfile=Apple-Device
                             RequestLatency=9
                             EapTunnel=PEAP
                             AuthState=Authenticated
                             Airespace-Wlan-Id=1
                             hlen=6
                             hops=2
                             host-name=SBA-iPad
                             FirstCollection=1323375086686
                             EndPointPolicyID=f7679880-116b-11e1-ae1c-0050569e2146
                             SelectedAccessService=Default Network Access
                             secs=0
                             AuthorizationPolicyMatchedRule=Default
                             IdentityPolicyMatchedRule=Default
                             MessageCode=5200
                             DeviceRegistrationStatus=0
                             SelectedAuthorizationProfiles=PermitAccess
                             IdentityAccessRestricted=false
                             SelectedAuthenticationIdentityStores=AD1
                             flags=0x0000
                             chaddr=7c:6d:62:de:05:8f
                             yiaddr=0.0.0.0
                             Response={User-Name=patjones; State=ReauthSession:0a042e41000000494ee13838;
                             Class=CACS:0a042e41000000494ee13838:ise-1/112681645/7; Termination-Action=RADIUS-Request; MS-MPPE-
                             Send-Key=49:7c:f0:b6:89:6b:18:b0:d1:91:ca:89:44:25:3a:8f:fb:ef:85:7c:45:98:3d:59:1b:5f:a3:67:d4:d2:2e:f0;
                             MS-MPPE-
                             Recv-Key=c9:0b:04:f8:4e:9b:24:a8:9e:c1:5f:38:65:fc:e3:7d:eb:0a:5e:40:46:24:1b:aa:ee:0a:d7:4c:b4:fa:96:51; }
                             Location=Location#All Locations
                             PolicyVersion=1
                             Device IP Address=10.4.46.65
                             NmapSubnetScanID=0
                             Called-Station-ID=1c-17-d3-cb-48-50:WLAN-Data
```

Procedure 7 Create device-type reports

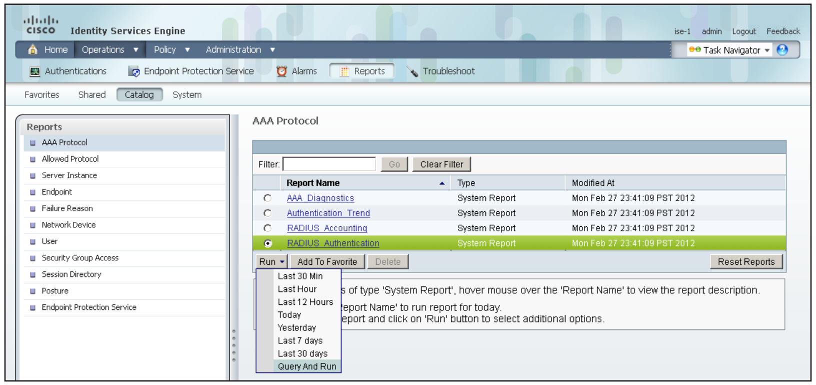
You can create reports to identify specific devices based on the identity groups configured previously. This example uses the group created to identify Apple iPads.

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



AAA Protocol

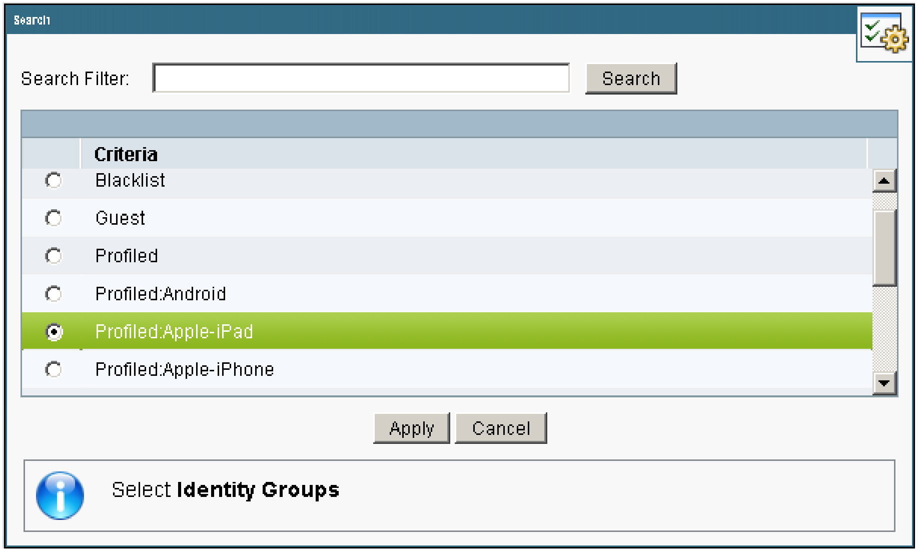
	Report Name	Type	Modified At
○	AAA_Diagnostics	System Report	Mon Feb 27 23:41:09 PST 2012
○	Authentication_Trend	System Report	Mon Feb 27 23:41:09 PST 2012
○	RADIUS_Accounting	System Report	Mon Feb 27 23:41:09 PST 2012
●	RADIUS_Authentication	System Report	Mon Feb 27 23:41:09 PST 2012

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

Step 5: 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**.

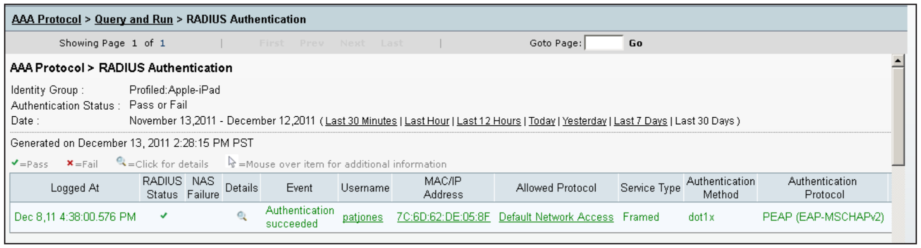


	Criteria
○	Blacklist
○	Guest
○	Profiled
○	Profiled:Android
●	Profiled:Apple-iPad
○	Profiled:Apple-iPhone

Select **Identity Groups**

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

Figure 5 - Sample report



AAA Protocol > RADIUS Authentication

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

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

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

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

Appendix A: Product List

Network Management

Functional Area	Product Description	Part Numbers	Software
Identity Management	Identity Services Engine Virtual Appliance	ISE-VM-K9=	1.1.1.268
	Cisco ISE Wireless 5-year License for 2500 Endpoints	LS-ISE-AD5Y-W-2500=	
	Cisco ISE Wireless 5-year License for 1000 Endpoints	LS- ISE- AD5Y-W-1K=	
	Cisco ISE Wireless 5-year License for 500 Endpoints	LS-ISE-AD5Y-W-500=	
	Cisco ISE Wireless 5-year License for 250 Endpoints	LS-ISE-AD5Y-W-250=	
	Cisco ISE Wireless 5-year License for 100 Endpoints	LS-ISE-AD5Y-W-100=	

Wireless LAN Controllers

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

Feedback

Click here to provide feedback to Cisco SBA.

SMART BUSINESS ARCHITECTURE

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

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

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.