BYOD–Advanced Guest Wireless Access

SOLUTION DESIGN GUIDE

August 2013

Table of Contents

Preface

Cisco Validated Designs (CVDs) provide the framework for systems design based on common use cases or current engineering system priorities. They incorporate a broad set of technologies, features, and applications to address customer needs. Cisco engineers have comprehensively tested and documented each CVD in order to ensure faster, more reliable, and fully predictable deployment.

CVDs include two guide types that provide tested and validated design and deployment details:

- Technology design guides provide deployment details, information about validated products and software, and best practices for specific types of technology.
- Solution design guides integrate or reference existing CVDs, but also include product features and functionality across Cisco products and may include information about third-party integration.

Both CVD types provide a tested starting point for Cisco partners or customers to begin designing and deploying systems using their own setup and configuration.

How to Read Commands

Many CVD guides tell you how to use a command-line interface (CLI) to configure network devices. 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 at a CLI or script prompt appear as follows:

```
Router# enable
```

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

```
police rate 10000 pps burst 10000 packets conform-action set-discard-class-
transmit 48 exceed-action transmit
```

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 feedback form.

For the most recent CVD guides, see the following site:

http://www.cisco.com/go/cvd

CVD Navigator

The CVD Navigator helps you determine the applicability of this guide by summarizing its key elements: the use cases, the scope or breadth of the technology covered, the proficiency or experience recommended, and CVDs related to this guide. This section is a quick reference only. For more details, see the Introduction.

Use Cases

This guide addresses the following technology use cases:

- Self-Administered Advanced Guest Wireless Access—An authorized employee can administer a guest wireless network that supports time-based customized guest user accounts, multiple mobile BYOD device types, and guest authentication portals.

For more information, see the “Use Cases” section in this guide.

Scope

This guide covers the following areas of technology and products:

- Onsite, remote-site, and guest wireless LAN anchor controllers
- Internet edge firewalls and demilitarized zone (DMZ) switching
- Management and user authentication using Cisco Identity Services Engine (ISE)
- Cisco ISE integration with Microsoft Active Directory
- Guest account sponsor portals using Cisco ISE and a Cisco wireless LAN controller (WLC)

For more information, see the “Design Overview” section in this guide.

Proficiency

This guide is for people with the following technical proficiencies—or equivalent experience:

- CCNA Routing and Switching—1 to 3 years installing, configuring, and maintaining routed and switched networks
- CCNA Security—1 to 3 years installing, monitoring, and troubleshooting network devices to maintain integrity, confidentiality, and availability of data and devices
- CCNP Wireless—3 to 5 years designing, installing, and troubleshooting wireless LANs

Related CVD Guides

Campus Wireless LAN Technology Design Guide

BYOD—Identity and Authentication Solution Design Guide

To view the related CVD guides, click the titles or visit the following site: http://www.cisco.com/go/cvd

Introduction

The goal of this guide is to show you how a BYOD business problem can be solved by using this Cisco Validated Design (CVD). Cisco has previously developed solutions to solve issues that are similar to the various BYOD business problems. This CVD uses the Cisco Identity Services Engine to solve the BYOD problem of providing guest wireless access.

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

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

The distinction between a work device and a personal device has evolved. This evolution of mobile device usage and the introduction of mobile devices into the workplace has caused a paradigm shift in how IT views what qualifies as a network “end point device” and also what it means to “be at work.”

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

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

Technology Use Case

Guest wireless networks used to be confined to public spaces and other forums that required a simple click to consent to the user policy. Today however, guest wireless networks can be found within enterprises, commercial spaces, hospitals, and universities, and they can provide Internet access without accountability, which is an increasing concern. The challenges associated with advanced guest wireless networks is no longer the number and placement of access points, or even the bandwidth required to support the wireless users. Instead, enterprises need an advanced wireless authentication solution that improves the on-ramping experience for the numerous BYOD devices being used while at the same time satisfies the security concerns of the organization.

Typically, visitors and guests expect these types of organizations to provide Internet access on an individual, as-needed basis. Security teams within these organizations require accountability as to who and what types of BYOD devices are being used on the guest wireless network. When a visitor no longer needs Internet access, the security team should automatically suspend the guest account.

Ideally, the solution is self-supporting, eliminating the need for IT staff to configure each guest user account. A sponsor specifies information about the guest, providing information about the duration of the guest's visit, the guest's company name, preferred language, email addresses, and cell phone number. After this information is collected, it is used to build a temporary guest user account that satisfies the security requirements of the organization and also streamlines the guest's on-boarding process.

By combining the Cisco Identity Services Engine (ISE) with the Cisco Unified Wireless architecture, wireless guest users and the BYOD devices that they use can be easily identified, providing the organization with the ability to self-administer a secure and scalable advanced guest wireless network.

Use Case: Self-Administered Advanced Guest Wireless Access

Some organizations may choose to allow authorized employees to create and administer individualized guest wireless Internet access accounts with unique account activation and suspension times. In this scenario, the organization needs to automatically provide guest users with specific account logon information via email or SMS text messaging. The organization securely isolates wireless guest users from accessing the organization's network and supports multiple BYOD device types.

This design guide enables the following capabilities:

- Self-administered guest account using an authorized sponsor—Employees who have been granted Sponsor authority in Active Directory may access the Identity Services Engine web-based sponsor portal.
- Individual customized guest user accounts—Each guest wireless account created has specific account activation and suspension times, facilitating a wide range of custom access requirements.
- BYOD device support—Administrators can use the Cisco Identity Services Engine can to classify the types of devices being used, allowing them to apply specific policies.
- Guest user isolation—Wireless guest user traffic is tunneled between the organization's wireless LAN controller (WLC) that provides wireless access and a shared or dedicated Internet-facing wireless LAN controller that provides secure guest Internet access.
- Consistent guest access capabilities—Guest wireless users experience the same network experience at both the main sites as well as remote locations.
- Guest user account notification—Guest users are automatically notified via email and/or SMS text messages about their guest user account information.

Design Overview

Cisco Identity Services Engine (ISE) is an identity and access-control policy platform that enables organizations to enforce compliance, enhance infrastructure security, and streamline their service operations. With the included sponsor portal, you can quickly open a web connection to the server running Cisco ISE, authenticate with a Microsoft Active Directory username and password, and create a guest account. The entire process is quick, easy, and involves no additional staff or costs.

Cisco ISE is deployed by organizations in their networks to manage all the different aspects of identity, including guest access. Cisco ISE includes a complete provisioning and reporting system that provides temporary network access for guests, visitors, contractors, consultants, and customers. Integrating Cisco ISE into the guest wireless network is accomplished by using ISE as the RADIUS server for authentication and accounting. Cisco ISE works alongside the Cisco wireless LAN controller (WLC), which provides the enforcement point for guest access and serves as a proxy for guest web authentication requests to the ISE server.

If the sponsor has a visitor coming for a meeting the following day, he can create a guest account and automatically send an email or Short Message Service (SMS) text message with account details to the visitor the night before. If the guest arrives early, she can get connected while waiting for the meeting.

When guest accounts are created, they are stored within the built-in database of the Cisco ISE server. When a guest user connects to the wireless guest network by using the guest Secure Set Identifier (SSID), their traffic is tunneled from the WLC that controls the AP they are using to the guest WLC in the demilitarized zone (DMZ) of the Internet edge component. The guest WLC then uses a web authorization redirect to point the guest user to the Cisco ISE guest login page. The guest WLC uses the credentials supplied to Cisco ISE by the guest user, and then uses those credentials in a RADIUS request to the Cisco ISE server to retrieve other information, like connection time. Cisco ISE verifies the supplied credentials against its own internal database, where guest information is stored.

The Cisco ISE server provisions the guest account for the amount of time that is specified when the account is created. Upon expiry of the account, Cisco ISE sends a RADIUS message that notifies the WLC of the amount of valid time that remains on the account before the WLC must remove the user.

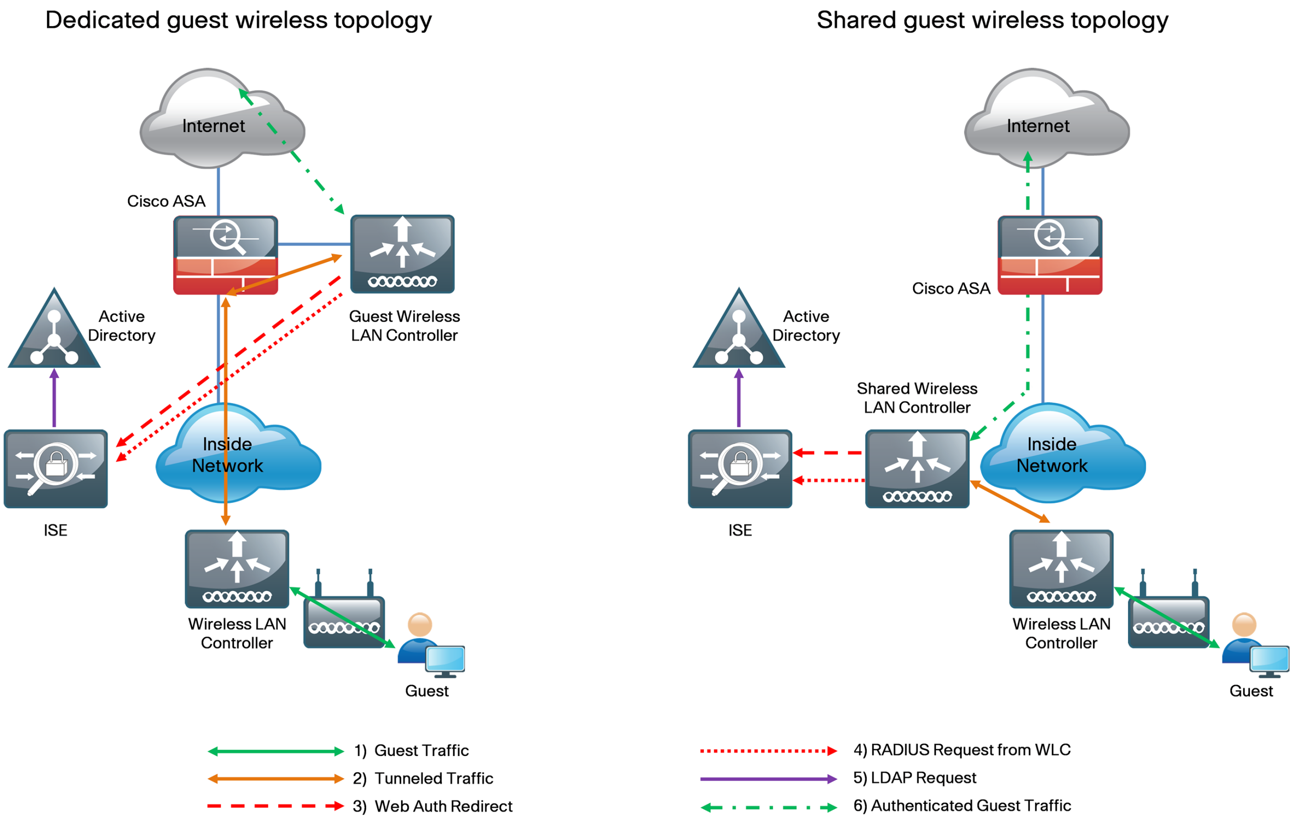
Risk is minimized because the guest account gives access only to the Internet, not the internal network. Sponsors can also suspend a guest account. Normally this feature is used in the event of malicious use of the account, but the organization could have a policy that requires suspension of the guest account as soon as the visitor leaves.

Because reporting is an important aspect of any guest access system, the whole process is recorded for audit purposes. If your organization gets a phone call from the security team at another company, and they explain that they were attacked at a specific time and date by an IP address that belongs to your organization’s guest wireless deployment, you can use Cisco ISE to get a full audit trail of who had that IP address, when they logged in and out, and who created the account.

There are two deployment models used for guest wireless access, as illustrated in Figure 1:

- Dedicated guest model, in which the guest WLC resides in the DMZ and handles only guest users.
- Shared guest model, in which the WLC supports both internal staff and guests, and resides in the internal network.

Figure 1 - Guest wireless topologies



Dedicated guest wireless topology

Shared guest wireless topology

Deployment Details

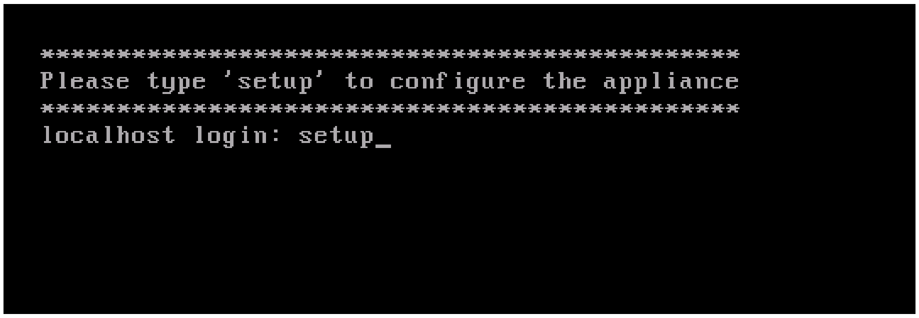
PROCESS

Deploying Cisco ISE

1. Perform initial setup of Cisco ISE
2. Install the Cisco ISE license
3. Configure network devices in Cisco ISE
4. Configure Cisco ISE to use Active Directory

Procedure 1 Perform initial setup of Cisco ISE

Step 1: Boot 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 Cisco ISE.

```
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 Domain Name System (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 the time.

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

Reader Tip

For time zone abbreviations, see the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1*, here:

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 the CLI console. This account is not the same as the one used to access the GUI.

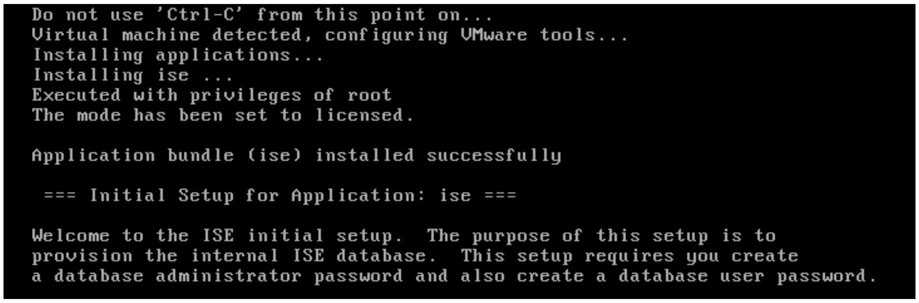
```
Enter username[admin]: admin
Enter password: [password]
Enter password again: [password]
```

Cisco ISE completes the installation and reboots. This process takes several minutes.

Step 6: During the provisioning of the internal database, when you are asked, enter a new database administrator password and a new database user password. Enter a password greater than 11 characters for the database administrator password. (Example: C1sco123C1sco123)

Tech Tip

Do not press Control-C during the installation, or it will end the installation.



```
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 Cisco ISE virtual appliance is now installed.

Procedure 2 Install the 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.

Step 1: In your browser, enter **http://ise-1.cisco.local**. The Cisco ISE GUI opens.

Step 2: On the menu bar, mouse over **Administration**, and then, in the System section, choose **Licensing**.

Notice that you see only one node here because the secondary node does not require licensing.

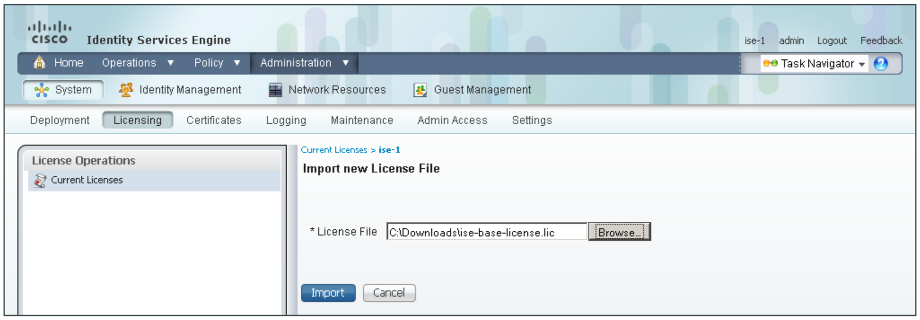
Step 3: Click the name of the Cisco ISE server. This allows you to edit the license details.

Step 4: Under Licensed Services, click **Add Service**.

Tech Tip

When installing a Base license and an Advanced license, you must install the Base license first.

Step 5: Locate your license file by clicking **Browse**, and then click **Import**.



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

Step 6: If you have multiple licenses to install, repeat the process for each.

Procedure 3 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 uses Cisco ISE for authentication needs to have this key.

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

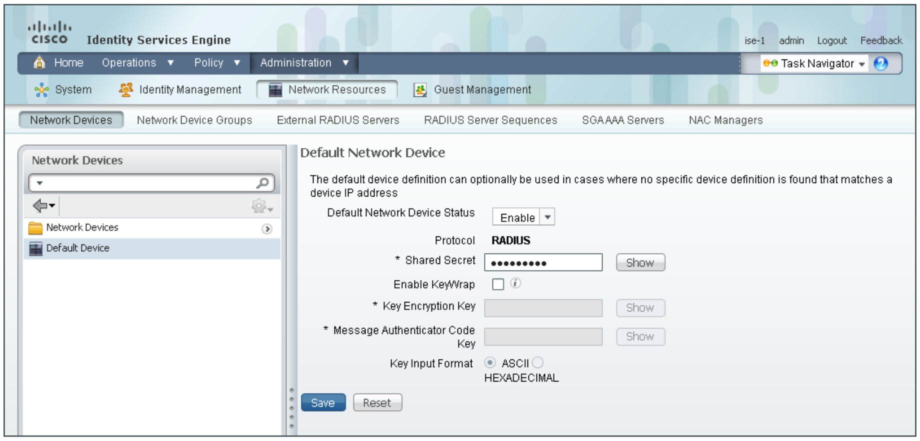
Step 2: In the left pane, click **Default Device**.

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 of Cisco's network devices 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: In the **Shared Secret** box, enter the RADIUS shared secret, and then click **Save**. (Example: SecretKey)


Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
System Identity Management Network Resources Guest Management
Network Devices Network Device Groups External RADIUS Servers RADIUS Server Sequences SGA AAA Servers NAC Managers
Network Devices
Network Devices
Default Device
Save Reset

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: ●●●●●●●●● Show

Enable KeyWrap: □

* Key Encryption Key: Show

* Message Authenticator Code Key: Show

Key Input Format: ● ASCII ○ HEXADECIMAL

Procedure 4 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.

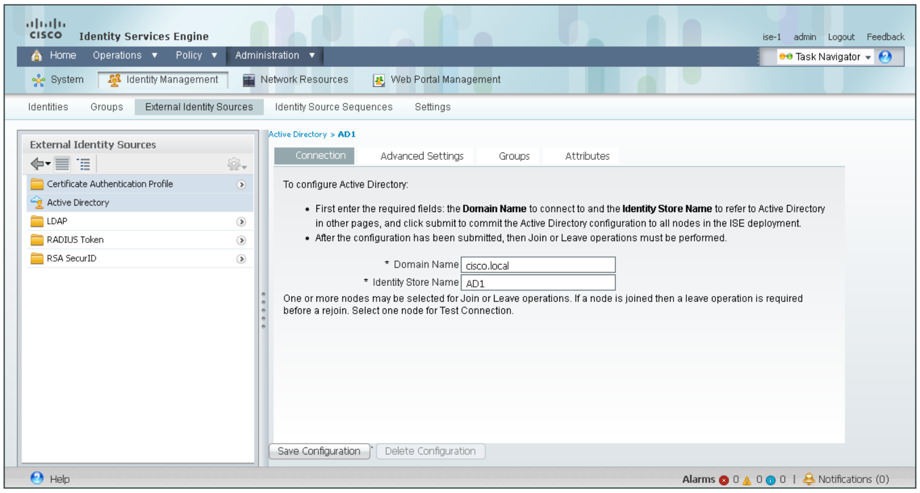
Step 1: On the menu bar, mouse over **Administration**, and then, in the Identity Management section, choose **External Identity Sources**.

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

Step 3: On the Connection tab, configure the connection to the AD server by entering the AD domain (example: cisco.local), the name of the server (example: AD1), and then click **Save Configuration**.

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

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


Identity Services Engine
ise-1 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
System Identity Management Network Resources Web Portal Management
Identities Groups External Identity Sources Identity Source Sequences Settings
External Identity Sources
Certificate Authentication Profile
Active Directory
LDAP
RADIUS Token
RSA SecurID
Active Directory > AD1
Connection Advanced Settings Groups Attributes
Save Configuration Delete Configuration
Help
Alarms 0 0 0 | Notifications (0)

To configure Active Directory:

- First enter the required fields: the **Domain Name** to connect to and the **Identity Store Name** to refer to Active Directory in other pages, and click submit to commit the Active Directory configuration to all nodes in the ISE deployment.
- After the configuration has been submitted, then Join or Leave operations must be performed.

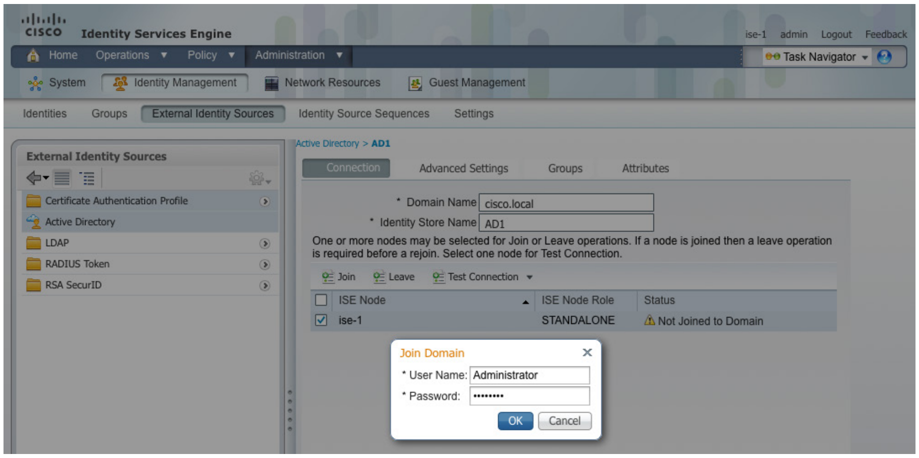
* Domain Name: cisco.local

* 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.

Step 6: Select the node, and then click **Join**.

Step 7: Enter the credentials for a domain administrator account. Cisco ISE is now joined to the AD domain.



Active Directory > AD1

* 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.

☐	ISE Node	ISE Node Role	Status
☑	ise-1	STANDALONE	⚠ Not Joined to Domain

Join Domain

* User Name: Administrator

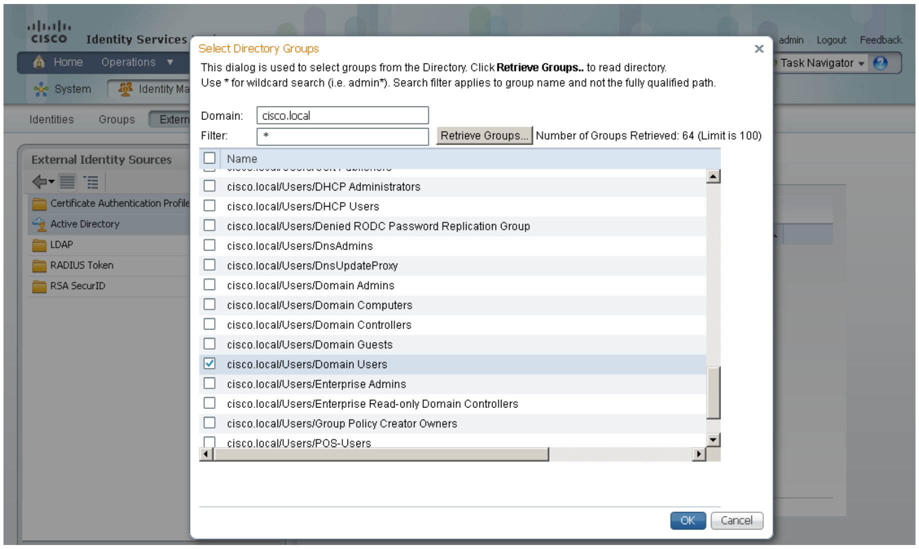
* Password: ••••••••

Next, select the groups from AD that Cisco ISE uses for authentication.

Step 8: Click the **Groups** tab, click **Add**, and then click **Select Groups from Directory**.

Step 9: Search for the groups 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 10: Select the groups you want to use for authentication, and then click **OK**. For example, if you want to select all users in the domain, select the group <domain>/Users/Domain Users.



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.

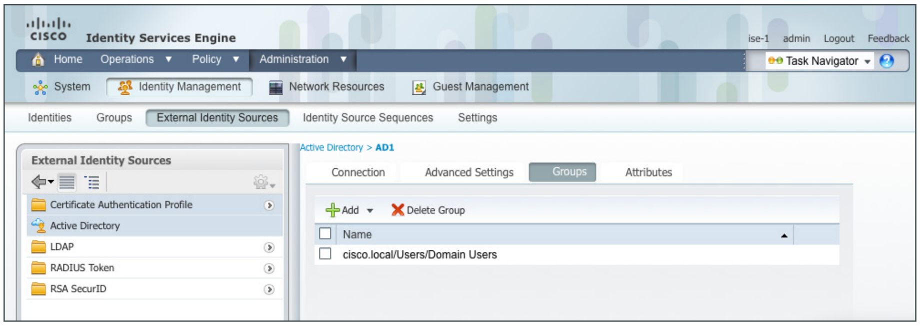
Domain: cisco.local

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

Step 11: Click **OK** and then click **Save Configuration**.



cisco.local/Users/Domain Users

PROCESS

Configuring Cisco ISE Sponsor Portal Services

1. Configure sponsor settings
2. Configure guest settings

A sponsor portal provides a web-based interface to privileged users, or sponsors, within an organization that allows you to create guest accounts. This process covers the steps required to customize the sponsor portal and to configure general sponsor settings, which govern how sponsors access customized web portals for the creation and management of guest accounts.

Setting up the portal is a two-part task. First you need to configure sponsor settings, or specify who can create guest accounts, and then you need to configure guest settings.

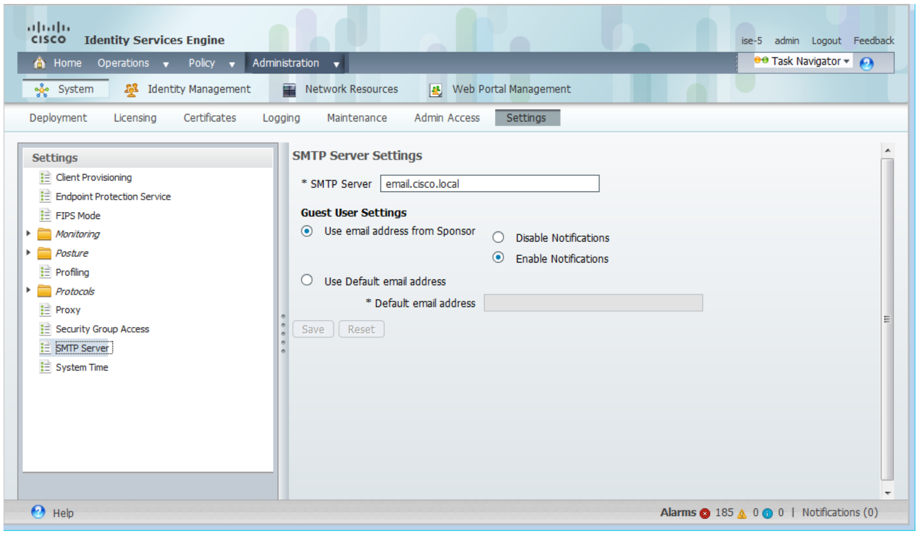
Procedure 1 Configure sponsor settings

A sponsor group defines which privileges are available to the sponsor after the sponsor has been authenticated. These privileges determine the menu options that are available, the guest accounts that can be managed, and the network access privileges that can be granted to a guest through role assignment and time restrictions. Organizations should set up sponsor groups according to their own policy. The privileges that are assignable are:

- SponsorAllAccounts—The sponsor in this group can manage all guest accounts.
- SponsorGroups—The sponsor in this group can manage all guest accounts created by sponsors in the same sponsor group only.
- SponsorGroupOwnAccounts—The sponsor in this group can manage only guest accounts that the sponsor created.

For this deployment, new groups are not required because the SponsorAllAccounts default group is sufficient, but the following steps detail how to build a new group in order to show the different settings available when setting up groups.

Step 1: In the Cisco ISE admin management web interface, navigate to **Administration > System > Settings > SMTP Server**, and then enter the location of the SMTP server that should be used to send guest wireless account notifications after creation. Emails can be sourced from either the sponsor's email address or from a global address. After entering the SMTP server information, click **Save**.


Identity Services Engine
ise-5 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
Settings
Client Provisioning
Endpoint Protection Service
FIPS Mode
Monitoring
Posture
Profiling
Protocols
Proxy
Security Group Access
SMTP Server
System Time
Help
Alarms 185 0 0 | Notifications (0)

SMTP Server Settings

* SMTP Server: email.cisco.local

Guest User Settings

● Use email address from Sponsor

○ Disable Notifications

● Enable Notifications

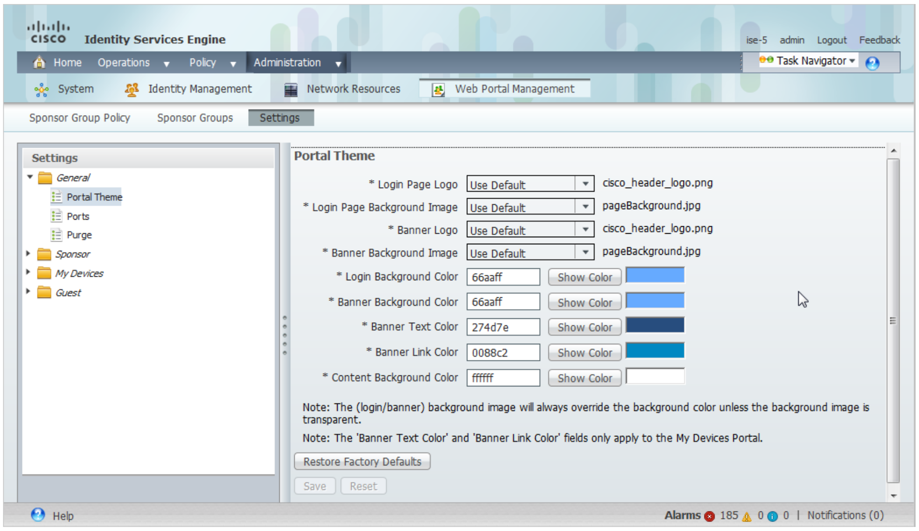
○ Use Default email address

* Default email address:

Save Reset

Step 2: Navigate to **Administration > Web Portal Management > Settings**, double-click **General**, and then, in the list, choose **Portal Theme**.

This page defines the sponsor portal layout and is where you configure customizations for the portal page.


Identity Services Engine
ise-5 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
Portal Theme
Ports
Purge
Sponsor
My Devices
Guest
Help
Alarms 185 0 0 | Notifications (0)

Portal Theme

* Login Page Logo: Use Default — cisco_header_logo.png

* Login Page Background Image: Use Default — pageBackground.jpg

* Banner Logo: Use Default — cisco_header_logo.png

* Banner Background Image: Use Default — pageBackground.jpg

* Login Background Color: 66aaff — Show Color

* Banner Background Color: 66aaff — Show Color

* Banner Text Color: 274d7e — Show Color

* Banner Link Color: 0088c2 — Show Color

* Content Background Color: ffffff — Show Color

Note: The (login/banner) background image will always override the background color unless the background image is transparent.

Note: The 'Banner Text Color' and 'Banner Link Color' fields only apply to the My Devices Portal.

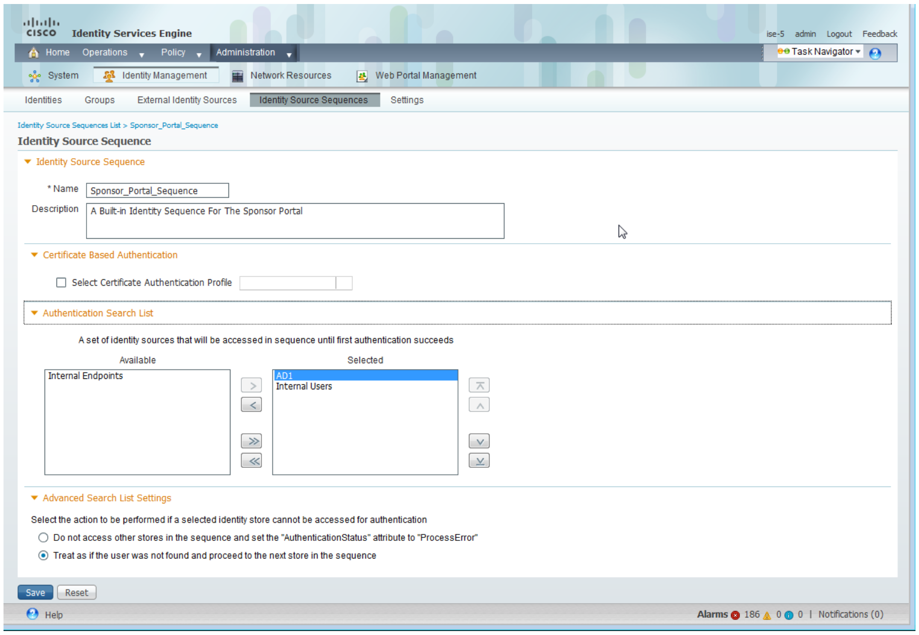
Restore Factory Defaults

Save Reset

Step 3: Navigate to **Administration > Identity Management > Identity Source Sequences**, and then click **Sponsor_Portal_Sequences**.

Step 4: In the **Available** list, choose the AD identity store, **AD1**, and then move it to the top of the **Selected** list.

This forces Sponsor authentication to use the AD database first and the Internal Users database second.


Identity Services Engine
ise-5 admin Logout Feedback
Home Operations Policy Administration
Task Navigator
System Identity Management Network Resources Web Portal Management
Identities Groups External Identity Sources Identity Source Sequences Settings
Identity Source Sequences List > Sponsor_Portal_Sequence
Save Reset
Help
Alarms 186 0 0 | Notifications (0)

Identity Source Sequence

Identity Source Sequence

* Name: Sponsor_Portal_Sequence

Description: A Built-in Identity Sequence For The Sponsor Portal

Certificate Based Authentication

□ Select Certificate Authentication Profile

Authentication Search List

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

Available	Selected
Internal Endpoints	AD1 Internal Users

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"

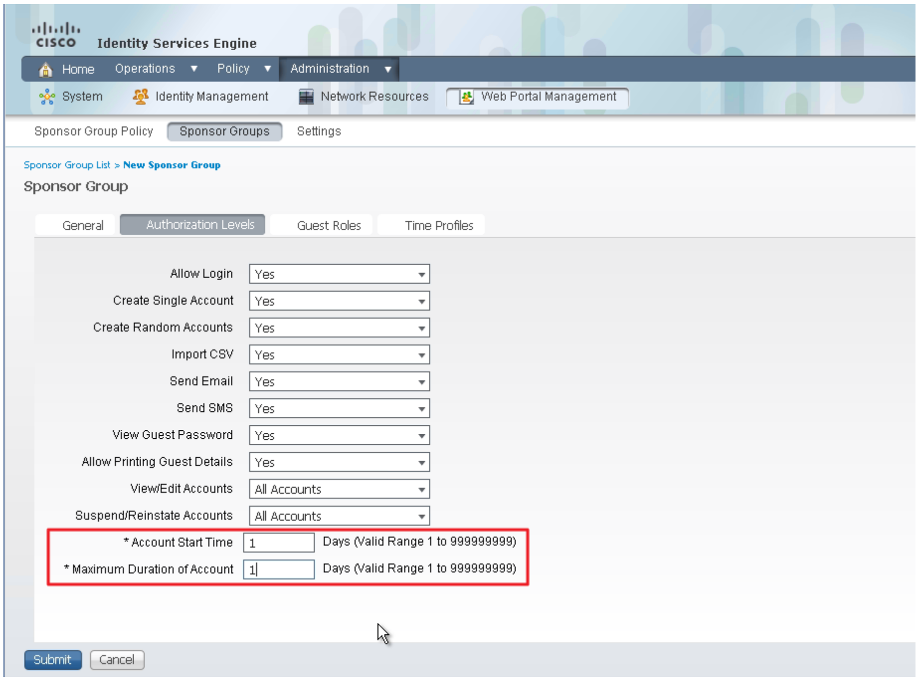
● Treat as if the user was not found and proceed to the next store in the sequence

Step 5: Click **Save**.

Step 6: Navigate to **Administration > Web Portal Management > Sponsor Groups**, and then click **Add**.

Step 7: Give the new group a name (example: OrganizationSponsorAllGroup).

Step 8: On the Authorization Levels tab, set Account Start Time to **1 Day**, and then set Maximum Duration of Account to **1 Day**.


Identity Services Engine
Home Operations Policy Administration
System Identity Management Network Resources Web Portal Management
Sponsor Group Policy Sponsor Groups Settings
Sponsor Group List > New Sponsor Group
General Authorization Levels Guest Roles Time Profiles
Submit Cancel

Sponsor Group

Allow Login	Yes
Create Single Account	Yes
Create Random Accounts	Yes
Import CSV	Yes
Send Email	Yes
Send SMS	Yes
View Guest Password	Yes
Allow Printing Guest Details	Yes
View/Edit Accounts	All Accounts
Suspend/Reinstate Accounts	All Accounts
* Account Start Time	1 Days (Valid Range 1 to 999999999)
* Maximum Duration of Account	1 Days (Valid Range 1 to 999999999)

Step 9: In the Guest Roles section, select **SponsorAllAccount**.

Step 10: On the **Time Profiles** tab, choose **DefaultFirstLogin**.

Step 11: Click **Submit.**

Next, you configure policies that define the sponsor group that is assigned to a sponsor, based on login credentials and other conditions.

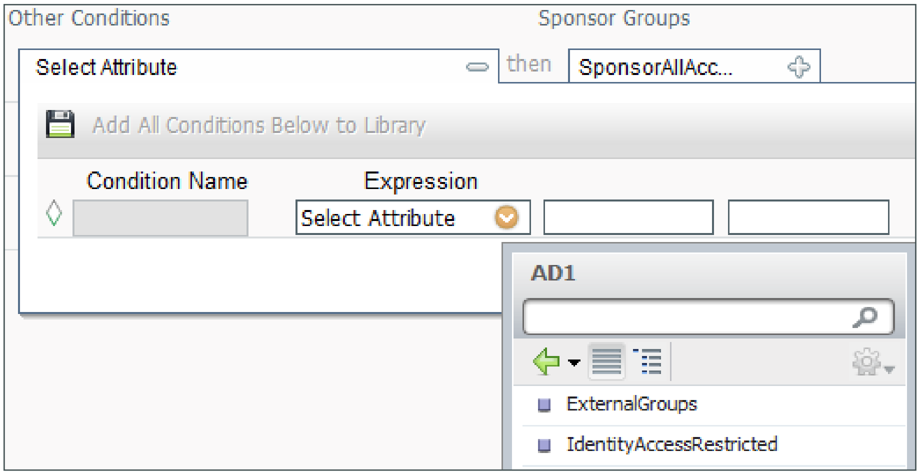
Step 12: Navigate to **Administration > Web Portal Management > Sponsor Group Policy**.

Step 13: Next to Manage All Accounts, next to Identity Groups, click the **+** symbol, and then choose **Any**.

Step 14: Next to Other Conditions, click the **+** symbol, and then select **Create New Condition**.

Step 15: Under Expression, next to Select Attribute, click the arrow. The menu opens.

Step 16: Next to AD1, click the **>** symbol, and then choose **ExternalGroups**.



Other Conditions

Sponsor Groups

Select Attribute then SponsorAllAcc...

Add All Conditions Below to Library

Condition Name

Expression

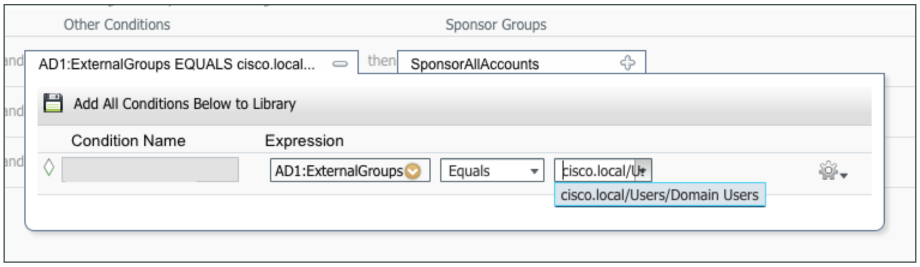
Select Attribute

AD1

ExternalGroups

IdentityAccessRestricted

Step 17: In first drop-down list, choose **Equals**, and then, in the second drop-down list, choose the AD group **yourdomain.local/Domain Users** which was added earlier in Step 8 of Procedure 4.



Other Conditions

Sponsor Groups

and AD1:ExternalGroups EQUALS cisco.local... then SponsorAllAccounts

and Add All Conditions Below to Library

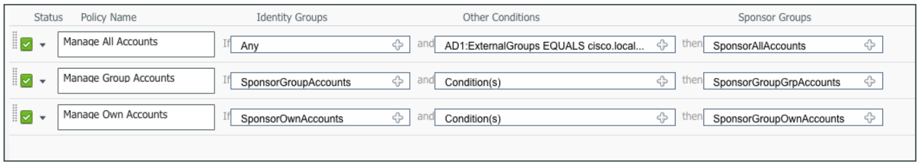
Condition Name

Expression

and AD1:ExternalGroups Equals cisco.local/U

cisco.local/Users/Domain Users

Step 18: In the **Sponsor Groups** list, ensure the default, **SponsorAllAccounts**, is selected, and then click **Save**.



Status	Policy Name		Identity Groups		Other Conditions		Sponsor Groups
☑	Manage All Accounts	If	Any	and	AD1:ExternalGroups EQUALS cisco.local...	then	SponsorAllAccounts
☑	Manage Group Accounts	If	SponsorGroupAccounts	and	Condition(s)	then	SponsorGroupGrpAccounts
☑	Manage Own Accounts	If	SponsorOwnAccounts	and	Condition(s)	then	SponsorGroupOwnAccounts

Procedure 2 Configure guest settings

In order to perform web-based authentication, guest users need a portal that allows the user to enter their login credentials, and also provides optional services, like password changes, device registration, or self-service account creation.

Step 1: Navigate to **Administration > Web Portal Management > Settings**, and then, in the Settings section, expand **Guest**.

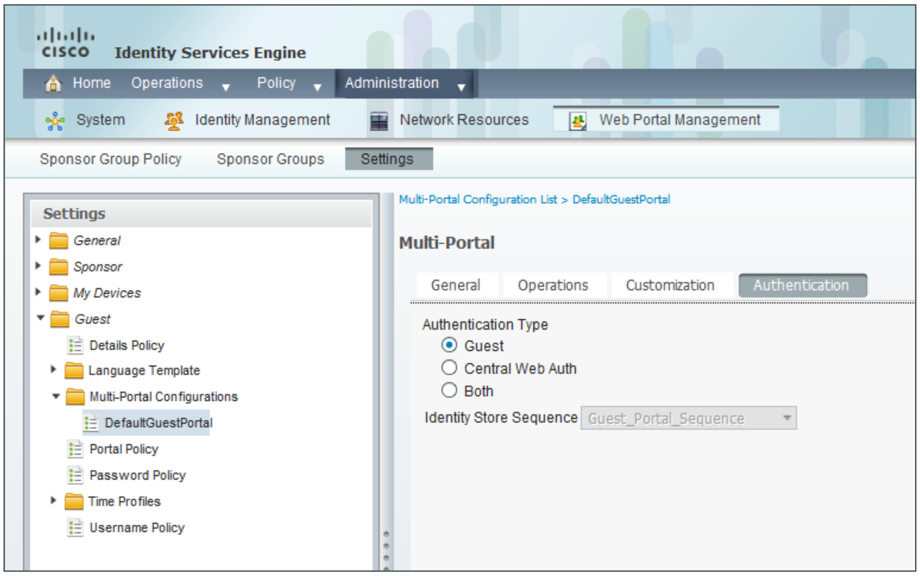
Tech Tip

The Details Policy option allows you to configure required guest account information. This can be changed from the default to fit a required security policy, as needed.

Step 2: On the left-hand panel, select **Multi-Portal Configurations**, and then click **DefaultGuestPortal**.

Step 3: On the Authentication tab, in the **Authentication Type** list, choose **Guest**. The Guest setting uses only the internal guest user database, which stores sponsor-created guest accounts.

Step 4: Click **Save**.



Authentication Type
● Guest
○ Central Web Auth
○ Both

Identity Store Sequence: Guest_Portal_Sequence

Specific security policies may also require changing password or username policy. You can do this by using the appropriate selections in this panel.

PROCESS

Integrating the Cisco Wireless LAN Controller and Cisco ISE

1. Configure a firewall policy
2. Configure the wireless LAN controller

Procedure 1 Configure a firewall policy

If there is a firewall between the guest WLC and the Cisco ISE server, you need to allow UDP/1812 and UDP/1813.

Step 1: Connect to the Internet edge firewall by using Cisco ASDM.

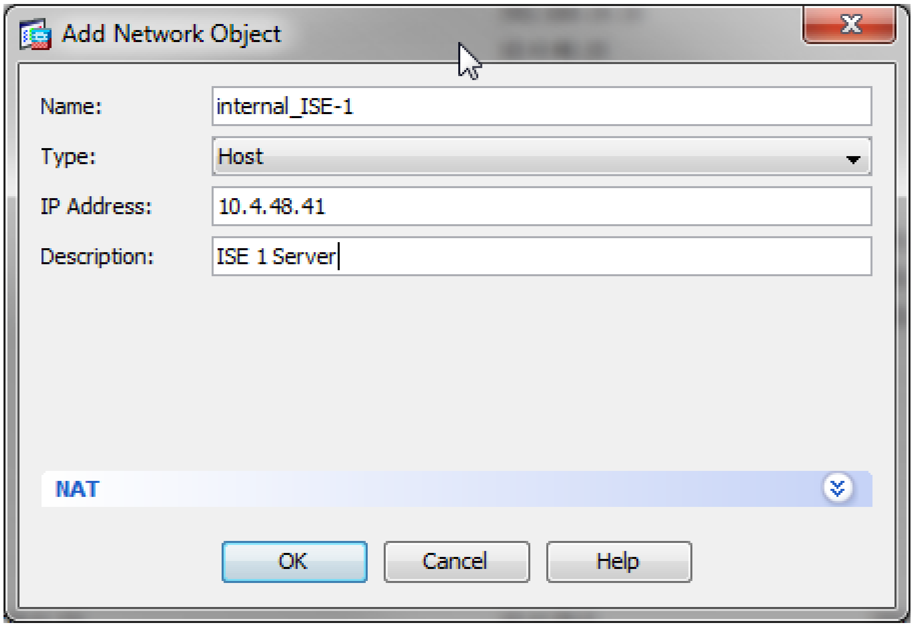
Step 2: Navigate to **Configuration > Firewall > Objects > "Network Objects/Groups"**.

Step 3: Click **Add**, and then click **Network Object**.

Step 4: In the **Name** box, enter the object name of the Cisco ISE server (example: internal_ISE-1).

Step 5: In the **Type** list, choose **Host**.

Step 6: In the **IP Address** box, enter the IP address of the Cisco ISE server (example: 10.4.48.41).



Name: internal_ISE-1
Type: Host
IP Address: 10.4.48.41
Description: ISE 1 Server

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

Step 8: Navigate to **Configuration > Firewall > Access Rules**.

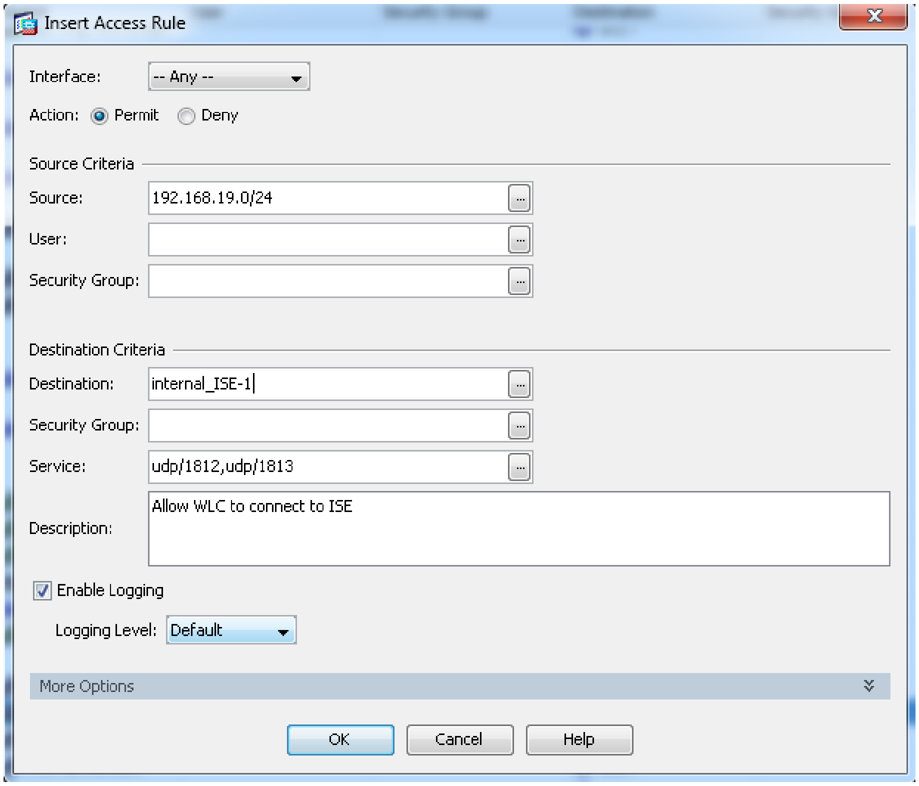
If you are using the shared deployment model, in which the WLC resides on the internal network, skip to Step 12. If you are using the dedicated deployment model, in which the WLC resides on the DMZ, continue to the next step.

Step 9: Click the rule that denies DMZ-network access to the internal networks.

Step 10: Click **Add**, and then click **Insert**. A new access rule is inserted before the deny rule that was selected.

Step 11: Enter the following access rule details, and then click **OK**.

- Source—**192.168.19.0/24**. This is the IP address for the guest Cisco Wireless LAN Controller management network.
- Destination—**internal_ISE-1**. This is the object name of the Cisco ISE server.
- Service—**udp/1812, udp/1813**



Interface: -- Any --

Action: ● Permit ○ Deny

Source Criteria

Source: 192.168.19.0/24

User:

Security Group:

Destination Criteria

Destination: internal_ISE-1

Security Group:

Service: udp/1812,udp/1813

Description: Allow WLC to connect to ISE

☑ Enable Logging

Logging Level: Default

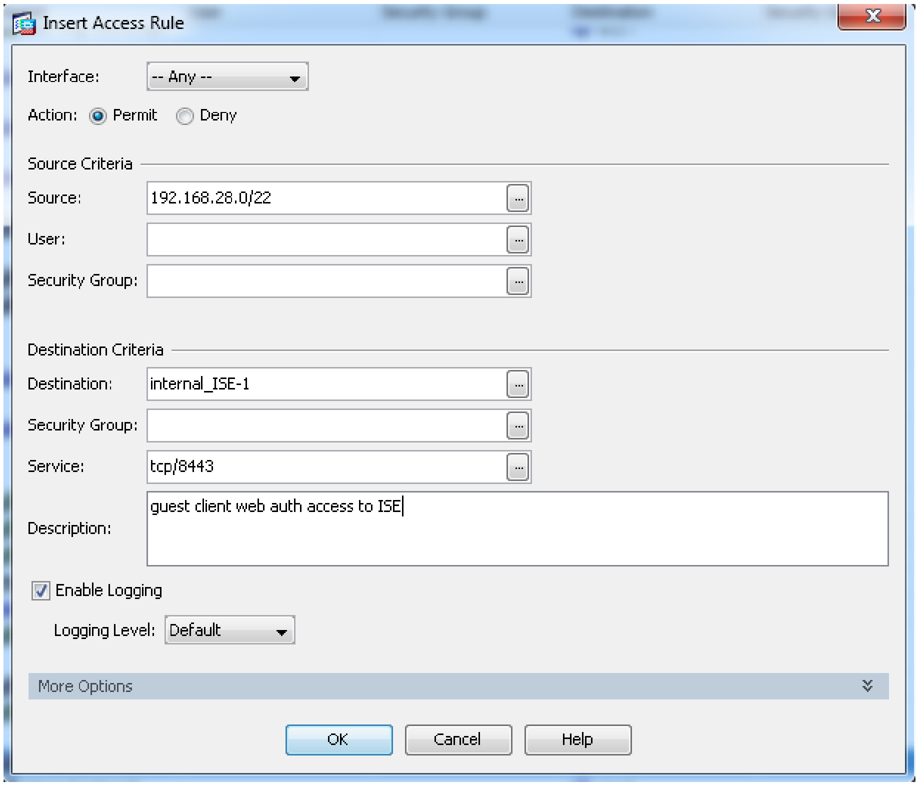
Guest client IP addresses need access through the firewall to the Cisco ISE server for web authentication attempts.

Step 12: Click the rule that denies DMZ-guest-network access to the DMZ-networks and the internal-network.

Step 13: Click **Add**, and then click **Insert**. A new access rule is inserted before the deny rule that is currently selected.

Step 14: Enter the following access rule details:

- Source—**192.168.28.0/22**. This is the network IP address for the DMZ guest network.
- Destination—**internal_ISE-1**
- Service—**tcp/8443**



Interface: -- Any --

Action: ● Permit ○ Deny

Source Criteria

Source: 192.168.28.0/22

User:

Security Group:

Destination Criteria

Destination: internal_ISE-1

Security Group:

Service: tcp/8443

Description: guest client web auth access to ISE

☑ Enable Logging

Logging Level: Default

Step 15: Click **OK**, click **Apply**, and then click **Save**.

Procedure 2 Configure the wireless LAN controller

Step 1: In your browser, enter the address of the guest anchor WLC management interface (example: https://guest-wlc), and then log in.

Step 2: Navigate to **Security > AAA > RADIUS > Authentication**. From here, you can add the Cisco ISE server as an authentication server in the WLC.

Step 3: If you are using the dedicated WLC model, ensure that the RADIUS servers that are already configured on this WLC are either disabled or removed; this ensures that Cisco ISE is used for guest user authentication. If you are using the shared model, there could possibly be other defined AAA servers.

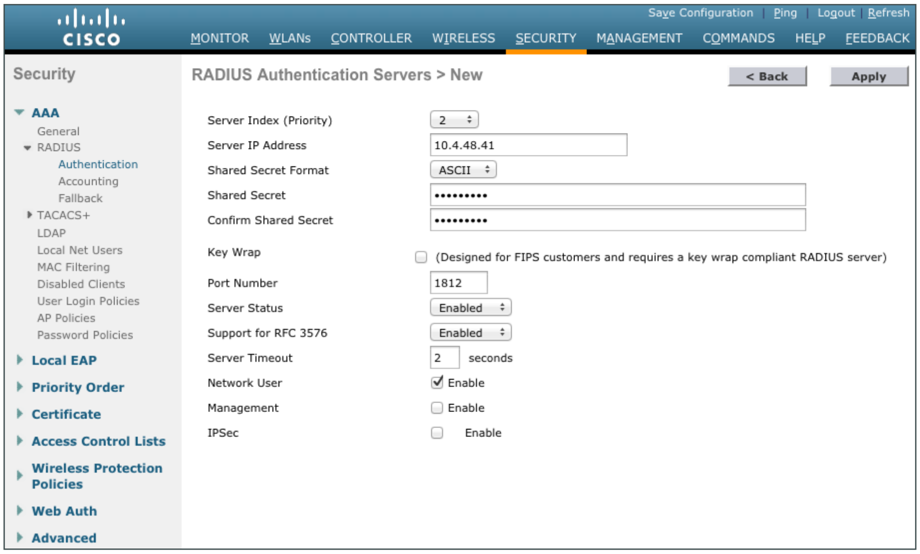
Step 4: Click **New**.

Step 5: Enter **10.4.48.41**. This is the IP Address for the server running Cisco ISE.

Step 6: In the **Shared Secret** box, enter a shared secret (Example: SecretKey).

Step 7: In the **Confirm Shared Secret** box, re-enter the shared secret. (Example: SecretKey)

Step 8: Next to Management, clear the **Enable** check 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

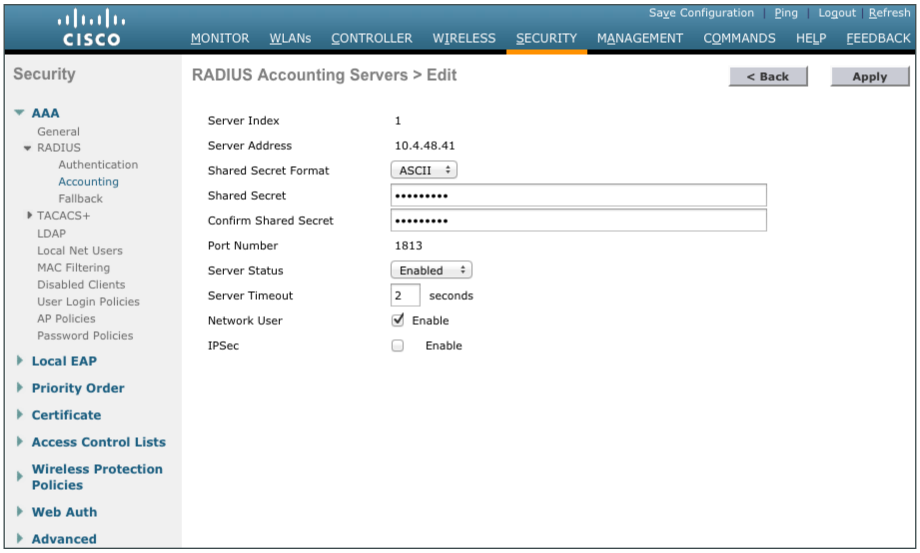
Step 9: Navigate to **Security > AAA > RADIUS > Accounting**. From here, you can add the guest server as an accounting server in the WLC.

Step 10: Click **New**.

Step 11: In the **Server Address** box, enter **10.4.48.41**. This is the IP address of the Cisco ISE server.

Step 12: In the **Shared Secret** box, enter a shared secret. (Example: SecretKey)

Step 13: In the **Confirm Shared Secret** box, re-enter the shared secret.



RADIUS Accounting Servers > Edit

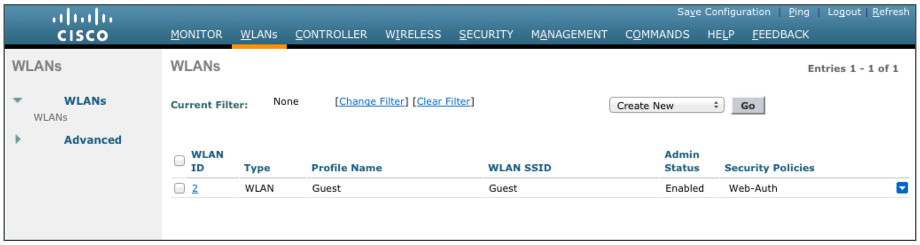
Server Index	1
Server Address	10.4.48.41
Shared Secret Format	ASCII
Shared Secret	•••••••••
Confirm Shared Secret	•••••••••
Port Number	1813
Server Status	Enabled
Server Timeout	2 seconds
Network User	☑ Enable
IPSec	□ Enable

Step 14: Click **Apply**.

Step 15: On the menu bar, click **WLANs**.

Step 16: In order to modify the Web Authentication Type later in the procedure, you must disable the WLANs using Web-Auth as an authentication method.

Step 17: Next to Guest, select the check box.


Save Configuration | Ping | Logout | Refresh
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs
WLANs
WLANs
Advanced
Create New
Go

WLANs

Entries 1 - 1 of 1

Current Filter: None [Change Filter] [Clear Filter]

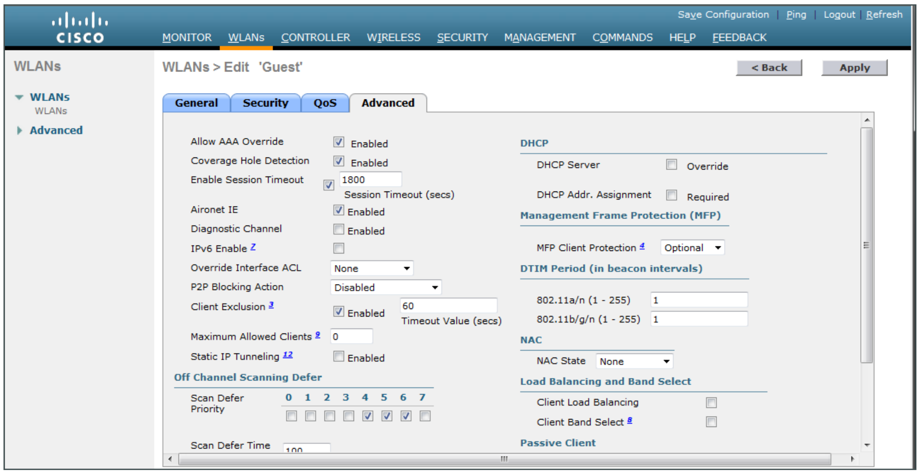
□	WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
□	2	WLAN	Guest	Guest	Enabled	Web-Auth

Step 18: Click the arrow next to Create New, in the list, choose **Disable Selected**, and then click **Go**.

Step 19: Click **OK**. This confirms that you want to disable the selected WLANs.

Step 20: Click the WLAN ID for the WLAN that you want to edit (example: 2).

Step 21: On the Advanced tab, next to Allow AAA Override, select **Enabled**. This allows the per-client session timeout to be set from the Cisco ISE server.


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 'Guest'

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
	□	□	□	□	☑	☑	☑	□

Scan Defer Time 100

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

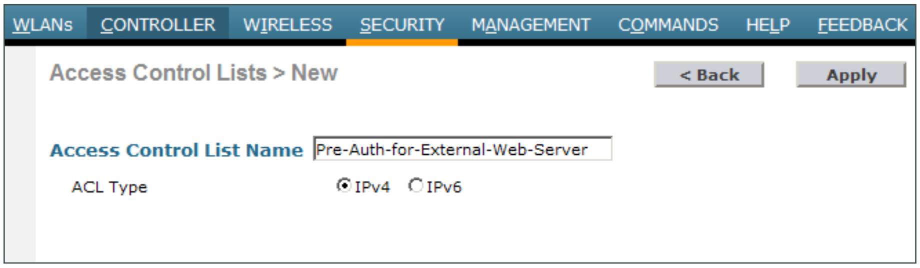
Step 22: Click **Apply**.

In order for the guest to have access to resources that they need before they authenticate, a pre-authentication ACL needs to be created that allows the guest access to DNS services and the Cisco ISE server.

Step 23: Navigate to **Security > Access Control Lists > Access Control Lists**.

Step 24: Click **New**. This allows you to create a new access control list.

Step 25: In the **Access Control List Name** box, enter a name for the ACL, and then click **Apply**.



Access Control List Name: Pre-Auth-for-External-Web-Server

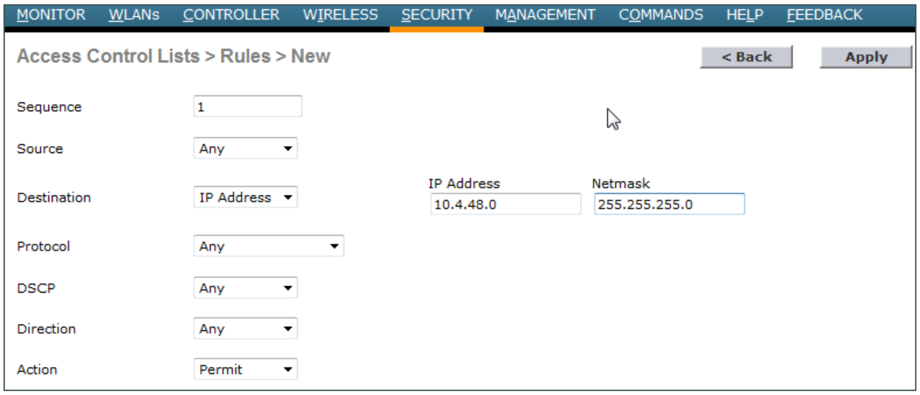
ACL Type: ● IPv4 ○ IPv6

Step 26: Click the name of the ACL.

Step 27: Click **Add New Rule**

Step 28: Enter the following information, and then click **Apply**. This defines an ACL that allows access to the management network. In this example, access is allowed to the 10.4.48.0 network, and access to specific resources is controlled on the Cisco ASA itself. This reduces the locations in which changes need to be made as the network evolves.

- Sequence—**1**
- Destination—**IP Address**
- IP Address—**10.4.48.0**
- Netmask—**255.255.255.0**
- Action—**Permit**



Sequence: 1

Source: Any

Destination: IP Address — IP Address: 10.4.48.0 — Netmask: 255.255.255.0

Protocol: Any

DSCP: Any

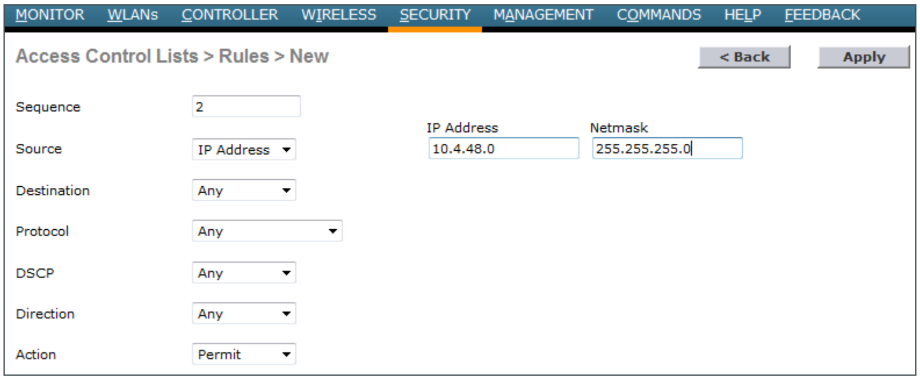
Direction: Any

Action: Permit

Step 29: Click **Add New Rule**.

Step 30: Enter the following information, and then click **Apply**. This defines another ACL entry in order to allow the return traffic from the 10.4.48.0 network to the guest clients.

- Sequence—**2**
- Source—**IP Address**
- IP Address—**10.4.48.0**
- Netmask—**255.255.255.0**
- Action—**Permit**



Access Control Lists > Rules > New

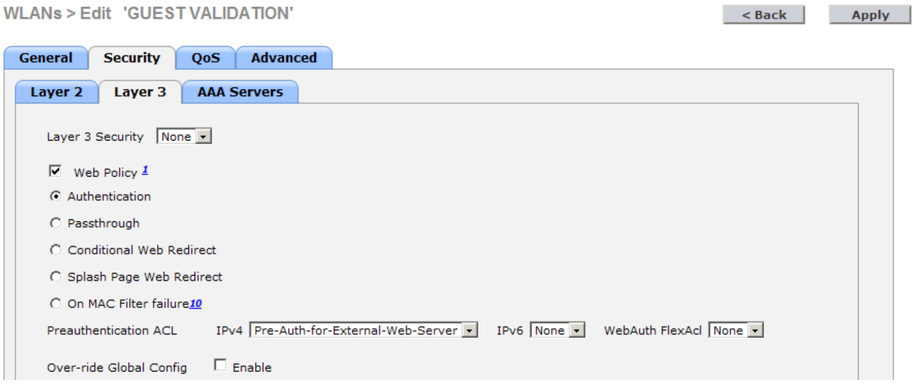
Sequence	2		
		IP Address	Netmask
Source	IP Address	10.4.48.0	255.255.255.0
Destination	Any		
Protocol	Any		
DSCP	Any		
Direction	Any		
Action	Permit		

Step 31: Navigate to **WLANs**.

Step 32: Click the WLAN ID for the specific guest WLAN. This allows you to edit the WLAN.

Step 33: Click **Security**, and then click **Layer 3**.

Step 34: On the Layer 3 tab, make sure **Web Policy** is selected, and then in the **IPv4** list, choose the ACL that was created in Step 25, and then click **Apply**.



WLANs > Edit 'GUEST VALIDATION'

Layer 3 Security None

☑ Web Policy 1

● Authentication

○ Passthrough

○ Conditional Web Redirect

○ Splash Page Web Redirect

○ On MAC Filter failure10

Preauthentication ACL IPv4 Pre-Auth-for-External-Web-Server IPv6 None WebAuth FlexAcl None

Over-ride Global Config □ Enable

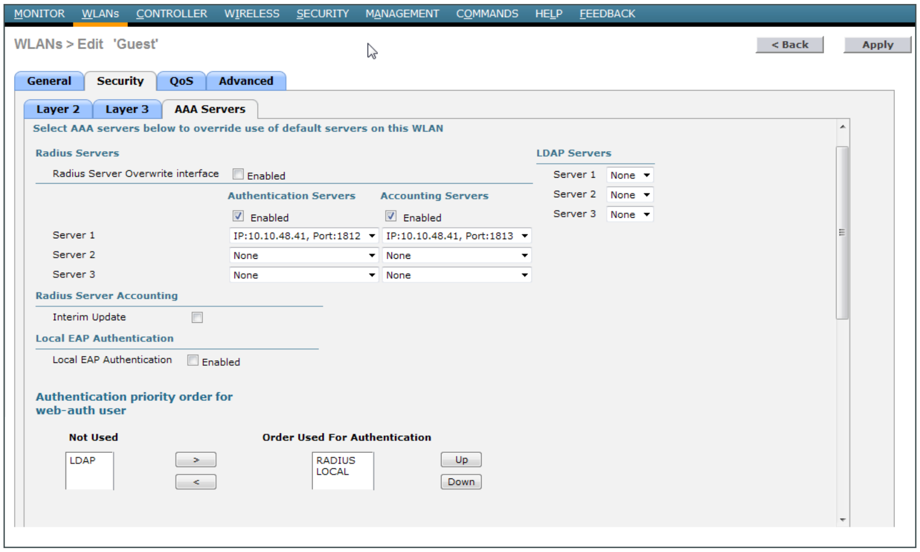
If you are using a shared deployment model, in which the WLC lives inside the firewall on the internal network and handles both guest users and internal users, continue to the next steps. If you are using a dedicated deployment model, in which the WLC resides on the DMZ and handles guest traffic only, skip to Step 38.

For this deployment, Cisco ISE is used only for guest traffic and not for the internal users. To support that, you need to set up the guest WLAN to use the Cisco ISE server for authentication.

Step 35: Navigate to **Security > AAA Servers**.

Step 36: Next to Server 1, in the **Authentication Servers** and **Accounting Servers** lists, choose the Cisco ISE server, 10.4.48.41.

Step 37: Under Authentication priority order for web auth user, in the **Order Used for Authentication** list, move **RADIUS** to the first position in the list, followed by **LOCAL**, and then ensure that **LDAP** is removed and then click **Apply**.



WLANs > Edit 'Guest'

Select AAA servers below to override use of default servers on this WLAN

Radius Servers

Radius Server Overwrite interface □ Enabled

	Authentication Servers	Accounting Servers
	☑ Enabled	☑ Enabled
Server 1	IP:10.10.48.41, Port:1812	IP:10.10.48.41, Port:1813
Server 2	None	None
Server 3	None	None

LDAP Servers

Server 1	None
Server 2	None
Server 3	None

Radius Server Accounting

Interim Update □

Local EAP Authentication

Local EAP Authentication □ Enabled

Authentication priority order for web-auth user

Not Used	Order Used For Authentication
LDAP	RADIUS LOCAL

When a guest wants to log in to the wireless network, they are presented with a web-based login screen that authenticates them against the credentials stored on the Cisco ISE server's internal database. To do this, any web session the guest begins must be redirected to the Cisco ISE server's web authentication URL to allow credential input. When the guest user enters their credentials, the WLC intercepts the credentials and the results, and uses them in a separate RADIUS request to Cisco ISE to retrieve the other options, such as time, that are specific to this guest account.

Step 38: Navigate to **Security > Web Auth > Web Login Page**.

Step 39: In the **Web Authentication Type** list, choose **External (Redirect to external server)**.

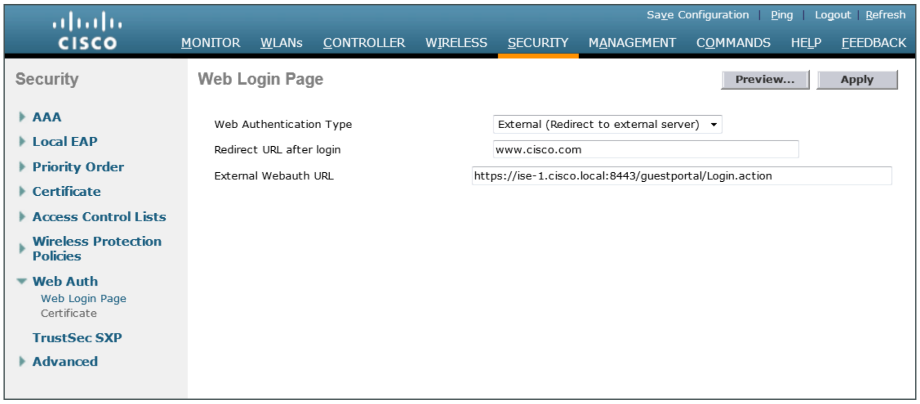
Step 40: If desired, in the **Redirect URL after login** field, enter a URL for the webpage that the user will be redirect to after they login. (Example www.cisco.com)

Step 41: In the **External Webauth URL** box, enter the following URL:

https://ise-1.cisco.local:8443/guestportal/Login.action

This is the location of the Cisco ISE server's guest portal login page.

Step 42: Click **Apply**, and then click **OK**. This confirms that the pre-authentication ACL has been configured.



Web Login Page

Web Authentication Type: External (Redirect to external server)

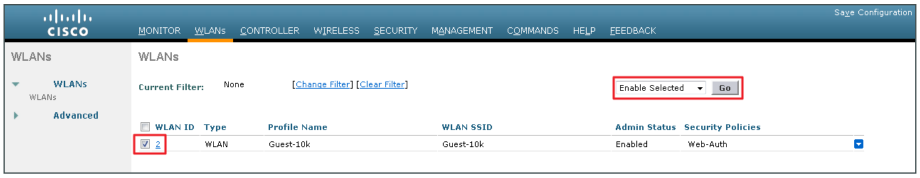
Redirect URL after login: www.cisco.com

External Webauth URL: https://ise-1.cisco.local:8443/guestportal/Login.action

Step 43: On the menu bar, navigate to **WLANs**.

Step 44: Select the check box for the Guest WLAN ID you want to edit (example: 2).

Step 45: Next to Create New, click the arrow, and then choose **Enable Selected**.



WLANs

Current Filter: None [Change Filter] [Clear Filter]

□ WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
☑ 2	WLAN	Guest-10k	Guest-10k	Enabled	Web-Auth

Step 46: Click **Go**, and then click **OK**.

Because of a change made in iOS device behavior (Apple iPhone, iPad, and iMac), you need to execute a command on the CLI of the WLC to allow those devices to be guests on the wireless network.

Step 47: Using SSH, navigate to the IP address of the WLC, and then log in with an administrator account.

Step 48: Enter the following command. This turns on captive bypass.

```
(Cisco Controller) >config network web-auth captive-bypass enable
```

Step 49: In the WLC GUI, on the right-hand side of the page, click **Save Configuration**.

Step 50: On the menu bar, navigate to **Commands**, and then click **Reboot**. The WLC reboots.

Step 51: If using a Cisco 2500 series WLC, repeat Procedure 2 for the resilient 2500 series WLC. This is necessary as the 2500 WLC does not support AP-SSO and the two controllers must be individually configured.

PROCESS

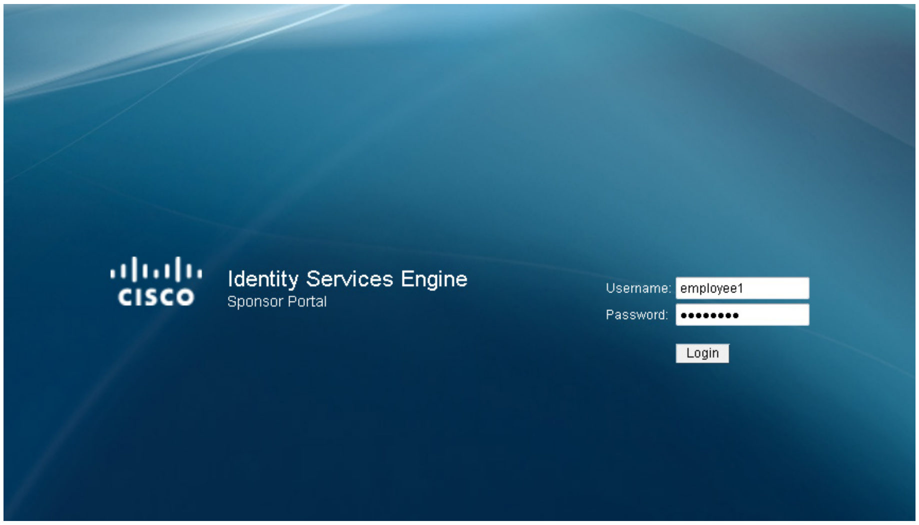
Creating and Using Guest Accounts

1. Use the Sponsor Portal
2. Use guest accounts

Procedure 1 Use the Sponsor Portal

To create the guest account, the authorized guest-user-account sponsor performs the following steps.

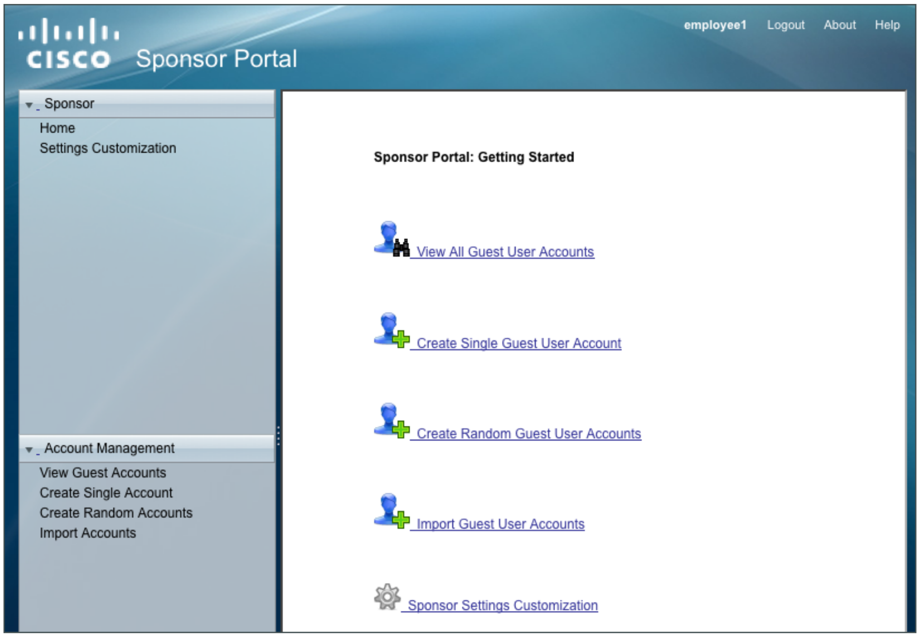
Step 1: In your browser, enter **https://ise-1.cisco.local:8443/sponsorportal**, and then log in to the Cisco ISE Sponsor Portal.



Username: employee1

Password: ••••••••

Step 2: Click **Create Single Guest User Account**.

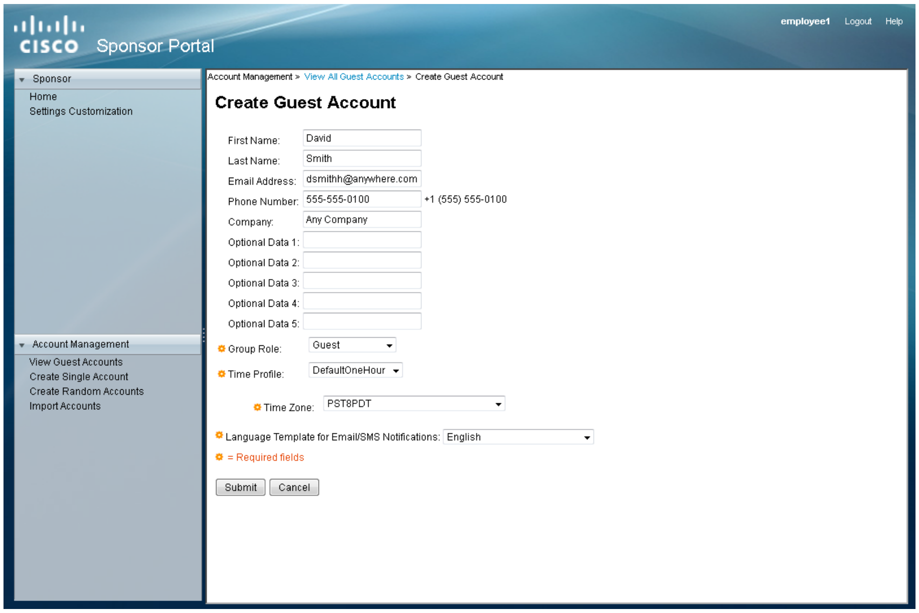


Sponsor Portal: Getting Started

- View All Guest User Accounts
- Create Single Guest User Account
- Create Random Guest User Accounts
- Import Guest User Accounts
- Sponsor Settings Customization

Step 3: Enter the information for the guest account as required by corporate policy (and the settings implemented in the "Configure Sponsor Portal" procedure in the "Configuring Cisco ISE Sponsor Portal Services" process). After you enter the required Guest User account info, click **Submit**.

Step 4: In this particular example, first and last name, email address, and company were entered by the sponsor.



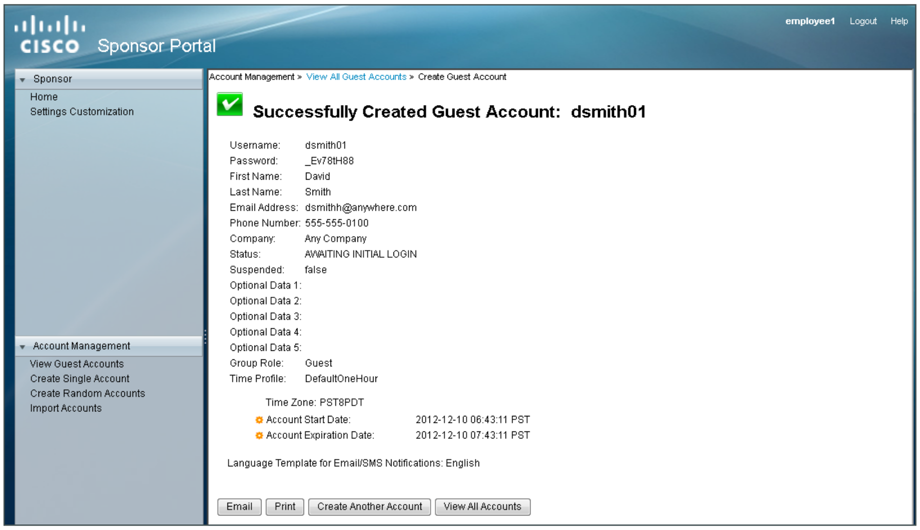
Account Management > View All Guest Accounts > Create Guest Account

Create Guest Account

First Name:	David
Last Name:	Smith
Email Address:	dsmithh@anywhere.com
Phone Number:	555-555-0100 +1 (555) 555-0100
Company:	Any Company
Optional Data 1:	
Optional Data 2:	
Optional Data 3:	
Optional Data 4:	
Optional Data 5:	
✱ Group Role:	Guest
✱ Time Profile:	DefaultOneHour
✱ Time Zone:	PST8PDT
✱ Language Template for Email/SMS Notifications:	English

✱ = Required fields

Step 5: If the account was successfully created, Cisco ISE displays the guest account and credentials. For testing purposes, write down the username that was automatically created (Example: dsmith01/_Ev78tH88)



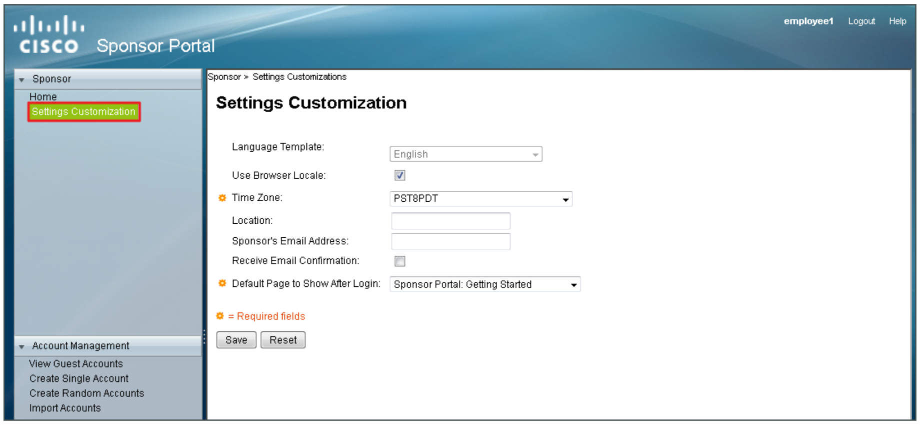
Successfully Created Guest Account: dsmith01

Username: dsmith01
Password: _Ev78tH88
First Name: David
Last Name: Smith
Email Address: dsmithh@anywhere.com
Phone Number: 555-555-0100
Company: Any Company
Status: AWAITING INITIAL LOGIN
Suspended: false
Optional Data 1:
Optional Data 2:
Optional Data 3:
Optional Data 4:
Optional Data 5:
Group Role: Guest
Time Profile: DefaultOneHour

Time Zone: PST8PDT
Account Start Date: 2012-12-10 06:43:11 PST
Account Expiration Date: 2012-12-10 07:43:11 PST

Language Template for Email/SMS Notifications: English

Step 6: If you want to customize sponsor account options, such as language and email notification, click **Settings Customization**.



Settings Customization

Language Template: English
Use Browser Locale: ☑
Time Zone: PST8PDT
Location:
Sponsor's Email Address:
Receive Email Confirmation: ☐
Default Page to Show After Login: Sponsor Portal: Getting Started

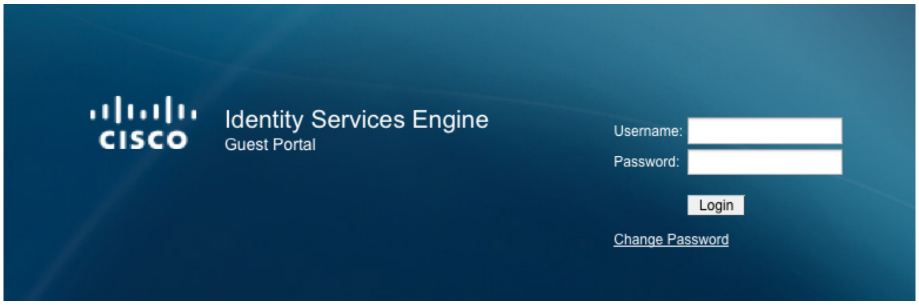
= Required fields

Procedure 2 Use guest accounts

For guests to be authenticated, they need to connect to the guest SSID and get an IP address in the 192.168.28.0/22 range.

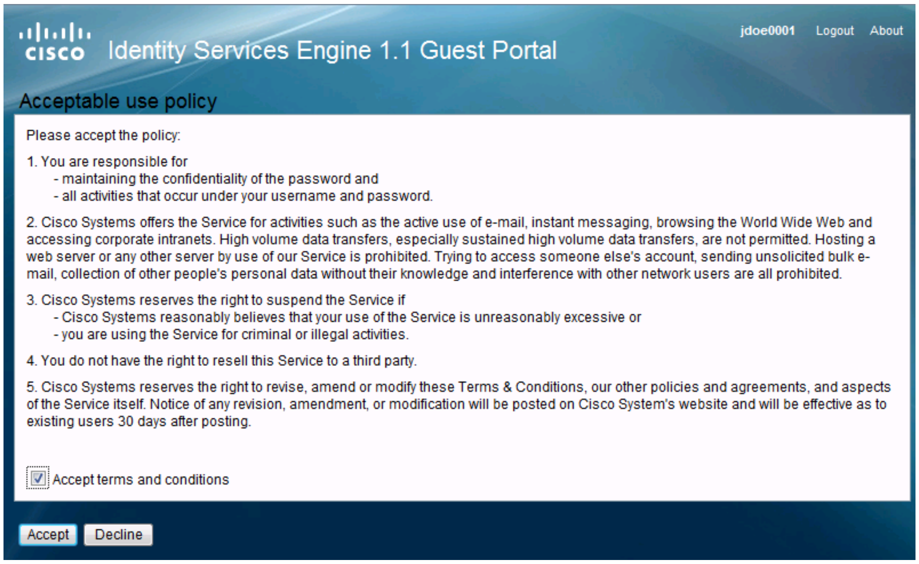
Step 1: From a wireless device, connect to the wireless guest network created. (Example: Guest)

Step 2: In the browser on the wireless device, browse to a known website (Example: http://www.cisco.com). The wireless guest machines browser is first redirected to the Cisco ISE Guest Portal, where the guest account credentials can be entered.



Step 3: Enter guest credentials. The Acceptable Use Policy opens.

Step 4: Select **Accept terms and conditions**, and then click **Accept**.



Please accept the policy:

1. You are responsible for
   - maintaining the confidentiality of the password and
   - all activities that occur under your username and password.

2. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited.

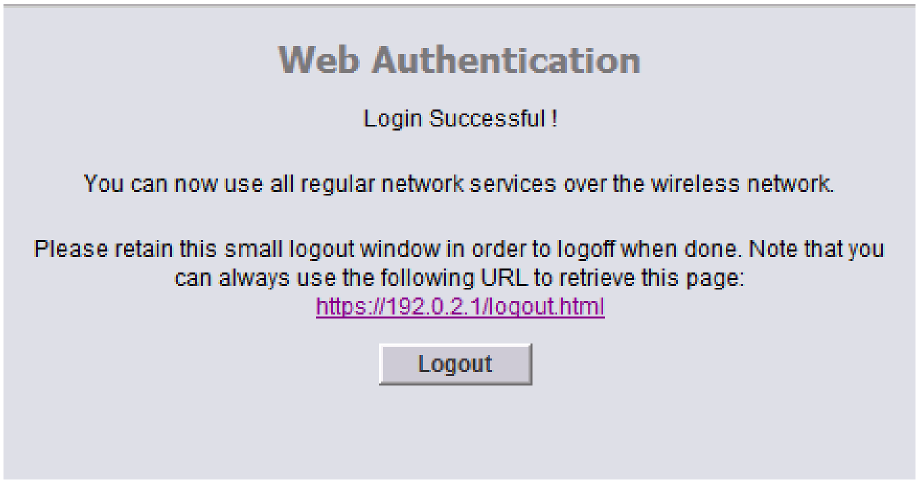
3. Cisco Systems reserves the right to suspend the Service if
   - Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or
   - you are using the Service for criminal or illegal activities.

4. You do not have the right to resell this Service to a third party.

5. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or modification will be posted on Cisco System's website and will be effective as to existing users 30 days after posting.

☑ Accept terms and conditions

The credentials have been successfully authenticated by Cisco ISE and the guest now has access as determined by the security policy implemented on the firewall.



Web Authentication

Login Successful !

You can now use all regular network services over the wireless network.

Please retain this small logout window in order to logoff when done. Note that you can always use the following URL to retrieve this page:
https://192.0.2.1/logout.html

Tech Tip

When using Internet Explorer, ensure that you have administrative authority to accept and install the digital certificate presented by the WLC using its configured virtual IP address of 192.0.2.1. By right clicking on the Internet Explorer ICON and selecting Run as Administrator you will be permitted to install the WLC certificate in the trusted root certificate store. Failure to do so will result in error 501 invalid certificate error messages. To avoid the use of certificates all together, issue the following command on the console port of each of the anchor WLC in the DMZ:

```
config network web-auth secureweb disable
```

Appendix A: Product List

Wireless LAN

Functional Area	Product Description	Part Numbers	Software
Cisco ISE Server	Cisco Identity Services Engine Virtual Appliance	ISE-VM-K9=	1.1.2.145
	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
Remote Site Controller	Cisco 7500 Series Wireless Controller for up to 6000 Cisco access points	AIR-CT7510-6K-K9	7.4.100.0
	Cisco 7500 Series Wireless Controller for up to 3000 Cisco access points	AIR-CT7510-3K-K9	
	Cisco 7500 Series Wireless Controller for up to 2000 Cisco access points	AIR-CT7510-2K-K9	
	Cisco Flex 7500 Series Wireless Controller for up to 1000 access points	AIR-CT7510-1K-K9	
	Cisco 7500 Series Wireless Controller for up to 500 Cisco access points	AIR-CT7510-500-K9	
	Cisco 7500 Series Wireless Controller for up to 300 Cisco access points	AIR-CT7510-300-K9	
	Cisco 7500 Series High Availability Wireless Controller	AIR-CT7510-HA-K9	
	Cisco Virtual Wireless Controller for up to 5 Cisco access points	L-AIR-CTVM-5-K9	
	Cisco Virtual Wireless Controller 25 Access Point Adder License	L-LIC-CTVM-25A	
	Cisco Virtual Wireless Controller 5 Access Point Adder License	L-LIC-CTVM-5A	
	Cisco Virtual Wireless Controller 1 Access Point Adder License	L-LIC-CTVM-1A	

Functional Area	Product Description	Part Numbers	Software
On Site, Remote Site, or Guest Controller	Cisco 5500 Series Wireless Controller for up to 500 Cisco access points	AIR-CT5508-500-K9	7.4.100.0
	Cisco 5500 Series Wireless Controller for up to 250 Cisco access points	AIR-CT5508-250-K9	
	Cisco 5500 Series Wireless Controller for up to 100 Cisco access points	AIR-CT5508-100-K9	
	Cisco 5500 Series Wireless Controller for up to 50 Cisco access points	AIR-CT5508-50-K9	
	Cisco 5500 Series Wireless Controller for up to 25 Cisco access points	AIR-CT5508-25-K9	
	Cisco 5500 Series Wireless Controller for up to 12 Cisco access points	AIR-CT5508-12-K9	
	Cisco 5500 Series Wireless Controller for High Availability	AIR-CT5508-HA-K9	
On Site Controller, Guest Controller	Cisco 2500 Series Wireless Controller for up to 50 Cisco access points	AIR-CT2504-50-K9	7.4.100.0
	Cisco 2500 Series Wireless Controller for up to 25 Cisco access points	AIR-CT2504-25-K9	
	Cisco 2500 Series Wireless Controller for up to 15 Cisco access points	AIR-CT2504-15-K9	
	Cisco 2500 Series Wireless Controller for up to 5 Cisco access points	AIR-CT2504-5-K9	

Internet Edge

Functional Area	Product Description	Part Numbers	Software
Firewall	Cisco ASA 5545-X IPS Edition - security appliance	ASA5545-IPS-K9	ASA 9.0(1) IPS 7.1(7)E4
	Cisco ASA 5525-X IPS Edition - security appliance	ASA5525-IPS-K9	
	Cisco ASA 5515-X IPS Edition - security appliance	ASA5515-IPS-K9	
	Cisco ASA 5512-X IPS Edition - security appliance	ASA5512-IPS-K9	
	Cisco ASA5512-X Security Plus license	ASA5512-SEC-PL	
	Firewall Management	ASDM	7.0(2)

Internet Edge LAN

Functional Area	Product Description	Part Numbers	Software
DMZ Switch	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 ports	WS-C3750X-24T-S	15.0(2)SE2 IP Base license

Feedback

Please use the feedback form to send comments and suggestions about this guide.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, 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.

B-0000134-1 08/13