# Newer Cisco SBA Guides Available

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

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

# BYOD—Guest Wireless Access Deployment Guide

SMART BUSINESS ARCHITECTURE

February 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 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.

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 2011 are the "August 2011 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 forum at the bottom of one of the following sites:

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

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

An RSS feed is available if you would like to be notified when new comments are posted.

# Table of Contents


What's In This SBA Guide . . . . . 1
- About SBA . . . . . 1
- About This Guide . . . . . 1

Introduction . . . . . 2
- Business Overview . . . . . 2
- Technical Overview . . . . . 3

Deployment Details . . . . . 4
- Deploying Cisco ISE Server . . . . . 4
- Configuring Cisco ISE Sponsor Portal Services . . . . . 7
- Integrating the Cisco Wireless LAN Controller and Cisco ISE . . . . . 10
- Creating and Using Guest Accounts . . . . . 14

Appendix A: Product List . . . . . 17



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.

© 2012 Cisco Systems, Inc. All rights reserved.

# What's In This SBA Guide

## About SBA

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.

For more information, see the *How to Get Started with Cisco SBA* document:

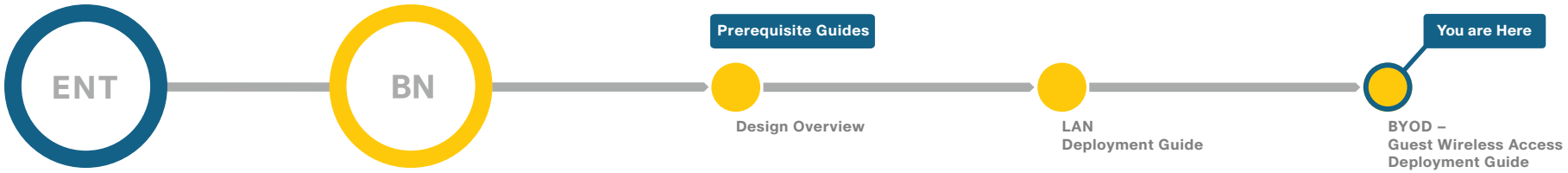
http://www.cisco.com/en/US/docs/solutions/Enterprise/Borderless_Networks/Smart_Business_Architecture/SBA_Getting_Started.pdf

## About This Guide

This *additional deployment guide* includes the following sections:

- **Business Overview**—The challenge that your organization faces. Business decision makers can use this section to understand the relevance of the solution to their organizations' operations.
- **Technology Overview**—How Cisco solves the challenge. Technical decision makers can use this section to understand how the solution works.
- **Deployment Details**—Step-by-step instructions for implementing the solution. Systems engineers can use this section to get the solution up and running quickly and reliably.

This guide presumes that you have read the prerequisites guides, as shown on the Route to Success below.




## Route to Success

To ensure your success when implementing the designs in this guide, you should read any guides that this guide depends upon—shown to the left of this guide on the route above. Any guides that depend upon this guide are shown to the right of this guide.

For customer access to all SBA guides: http://www.cisco.com/go/sba
For partner access: http://www.cisco.com/go/sbachannel

# Introduction

**Note**

This guide is based on the *Cisco SBA Borderless Networks Advanced Guest Wireless Deployment Guide*. The goal of this guide is to show you how a BYOD business problem can be solved by using Cisco Smart Business Architecture. Cisco has previously developed solutions to solve issues that are similar to the various BYOD business problems. Cisco SBA uses 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. This ranges from guest wireless access all the way to device authentication and identification. The goal is to provide a common work-environment regardless of the type of device being used. This could be through 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.

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." The distinction between a device used exclusively for "work" and a device used exclusively for "personal use" has evolved.

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

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

Other SBA Borderless Networks guides addressing BYOD business problems include:

- *BYOD—Internal Corporate Access Deployment Guide*
- *BYOD—Identification and Authentication Deployment Guide*
- *BYOD—Remote Mobile Device Access Deployment Guide*

## Business Overview

Organizations' facilities are frequently called upon to host a wide range of guest users including customers, partners, and vendors. Many of these users want network connectivity to gain access to authorized organizational resources as well as VPN connectivity to their employer's network and the Internet while they are onsite so they can be as productive as possible. However, offering guests the same level of network access that the organization's users have exposes the organization to a significant risk.

Relying on a set group of internal users, such as receptionists and IT helpdesk staff, to create all the guest accounts may not be as flexible as an organization requires. The group might not be available 24 hours a day to create accounts, or the turnaround time for creation of the accounts might be significant. The turnaround times tend to be most significant when the resources that create the accounts have a cost associated with them. For example, a helpdesk representative might spend time creating guest accounts only after all higher priority issues have been resolved.

Once a guest account has been created, how do you tell the guest the account details, the access instructions, and the acceptable use policy? Dealing with this information when the guest arrives onsite can take a lot of time. Also, what if a guest account needs to change after it has been created? You may want to extend the time on the guest account so you don't need to create a new one for the guest when it expires, or you may want to resend the account details to a guest if the information has been lost or forgotten.

## Technical Overview

The solution is Cisco Identity Services Engine (ISE) including sponsor portal. Cisco ISE is an identity and access control policy platform that enables enterprises to enforce compliance, enhance infrastructure security, and streamline their service operations. With the sponsor portal, users can quickly open a web connection to the server running Cisco ISE, authenticate with a Microsoft® Active Directory® user name 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 Cisco 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 proxies guest web authentication requests to the Cisco ISE server.

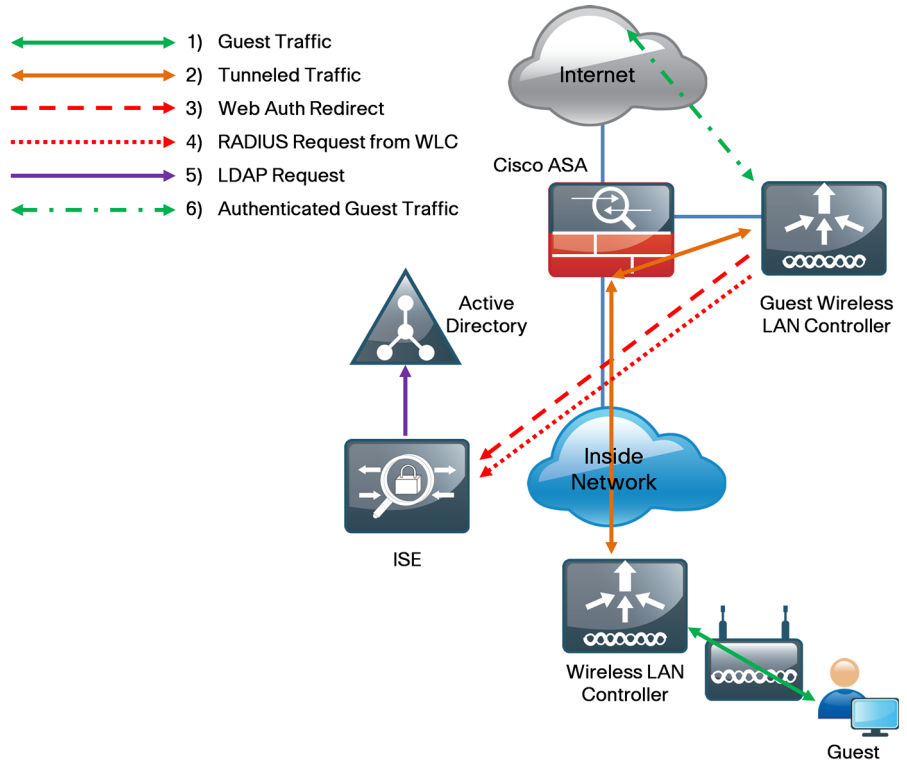
If the sponsor has a visitor coming the following day for a meeting, he can create a guest account and automatically email or Short Message Service (SMS) text message details to the visitor the night before, so if the guest arrives early, he can get connected while waiting for the meeting.

When guest accounts are created, they are stored within the Cisco ISE server built-in database. When a guest user connects to the wireless guest network by using the Guest Secure Set Identifier (SSID), their traffic gets tunneled from whichever WLC controls the AP they are using to the guest WLC in the 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 uses those credentials in a RADIUS request to the Cisco ISE server to retrieve other information like connection time, etc. Cisco ISE verifies the supplied credentials against its own internal database where guest information is stored.

Cisco ISE Server provisions the guest account for the amount of time specified when the account is created. Upon expiry of the account, Cisco ISE sends a RADIUS message that notifies the Cisco 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 access to 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 Server to get a full audit trail of who had that IP address, when they logged in and out, and who created the account.



# Deployment Details

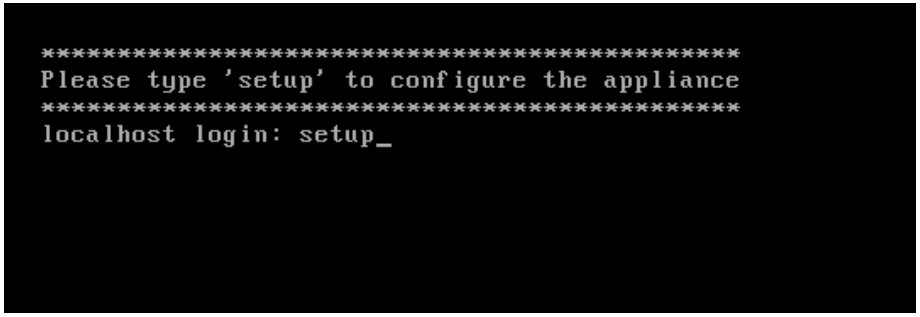
## Process

Deploying Cisco ISE Server

1. Perform initial setup of Cisco ISE
2. Install 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 the Cisco ISE and at the initial prompt, enter **setup.** The installation begins.




**Step 2:** Enter the host name, IP address, subnet mask, and default router of the 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 primary NTP server[time.nist.gov]: ntp.cisco.local
Add/Edit secondary NTP server? Y/N : n
Enter system timezone[UTC]: PST8PDT
```

### Tech Tip

Timezone abbreviations can be found in the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1*:

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 will be 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 it will abort 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.
```

Cisco ISE is now installed.

## Procedure 2 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 will need to obtain a license from Cisco.

**Step 1:** In your browser, connect to the ISE's GUI at http://ise-1.cisco.local.

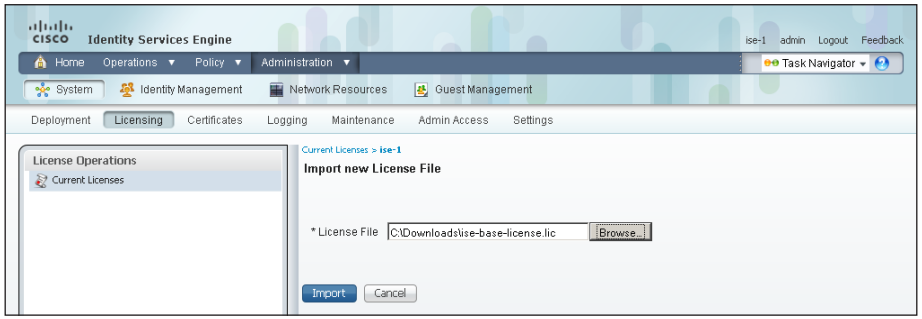
**Step 2:** Mouse over **Administration.** The drop-down menu appears. Under System, choose **Licensing**.

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

**Step 3:** Click the name of the Cisco ISE server to edit the license details.

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

**Step 5:** Click **Browse,** locate your license file, and then click **Import**.




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

### Tech Tip

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

## 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:** Mouse over **Administration**. The drop-down menu appears. Under Network Resources, choose **Network Devices**.

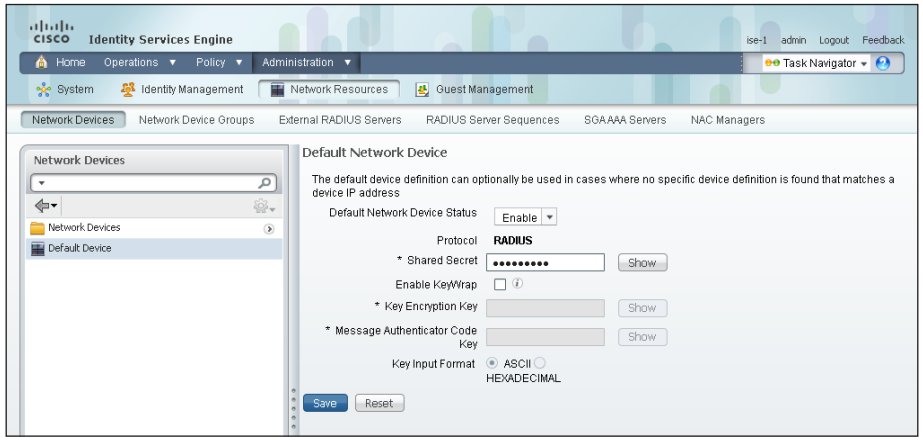
**Step 2:** In the left pane, click **Default Device**.

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

**Step 3:** Enable Default Network Device Status by choosing **Enable** from the pull-down menu.

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




## 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.

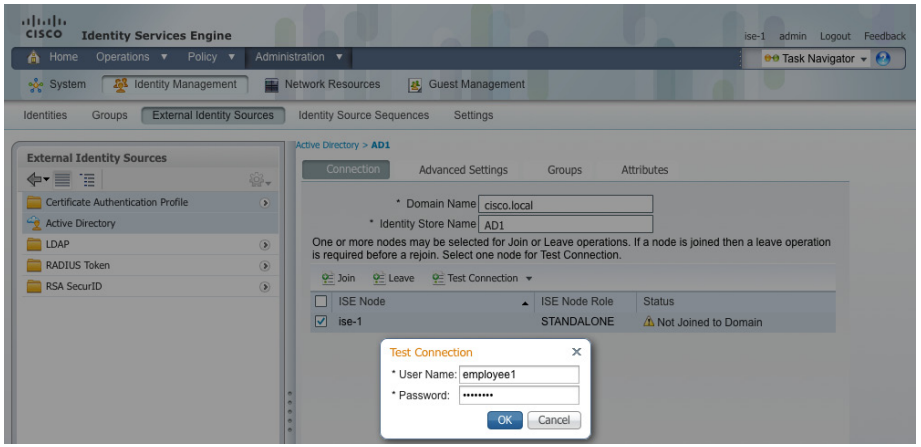
**Step 1:** Mouse over **Administration**, and then, from the Identity Management section of the menu, choose **External Identity Sources**.

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

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

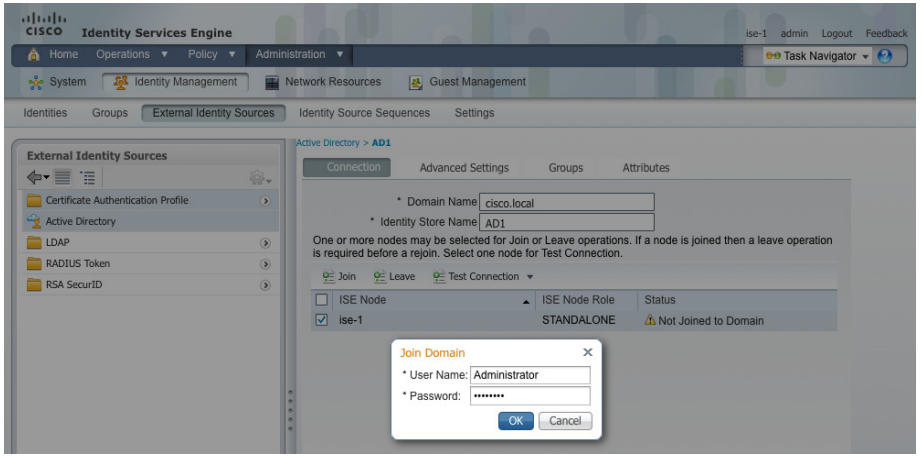
**Step 4:** Verify these settings by selecting the box next to the node, and then clicking **Test Connection** and choosing **Basic Test**.

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




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

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

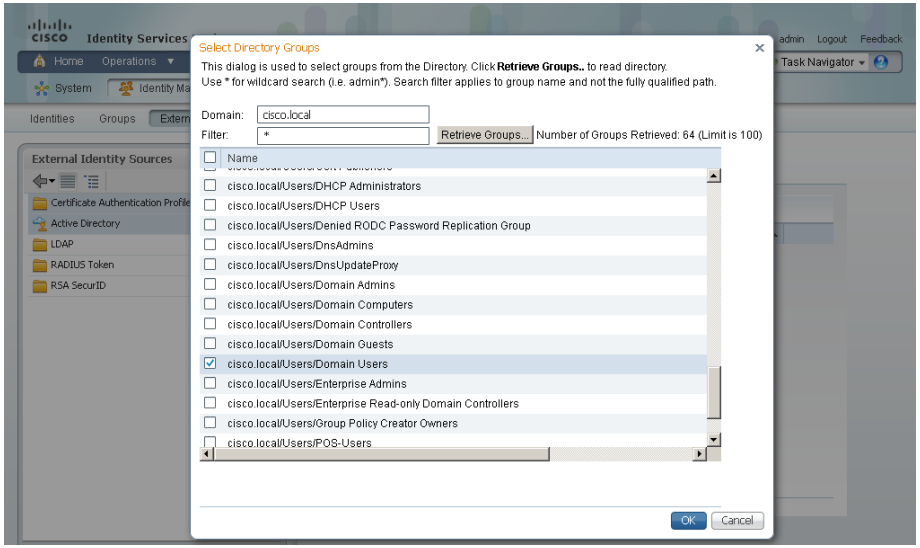


Next, select the groups from AD that Cisco ISE will use for authentication.

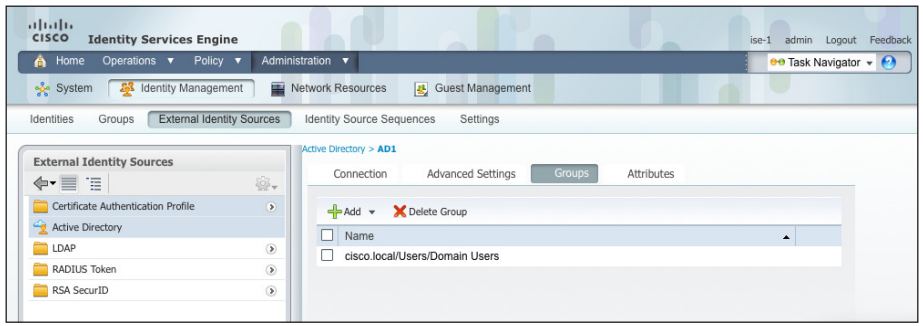
**Step 8:** Click the **Groups** tab, click **Add,** and then click **Select Groups from Directory**.

**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. Click **Retrieve Groups** 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, for all users in the domain, select the group <domain>/Users/Domain Users.




**Step 11:** Click **Save Configuration**.




## 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 (sponsors) within an organization that allows creation of guest user accounts. This process covers the required steps to customize the sponsor portal and to configure general sponsor settings that govern how sponsors access customized web portals for the creation and management of guest user accounts.

Setting up the portal is a two-part task: configuring sponsor (who can create guest accounts) settings and configuring guest settings.

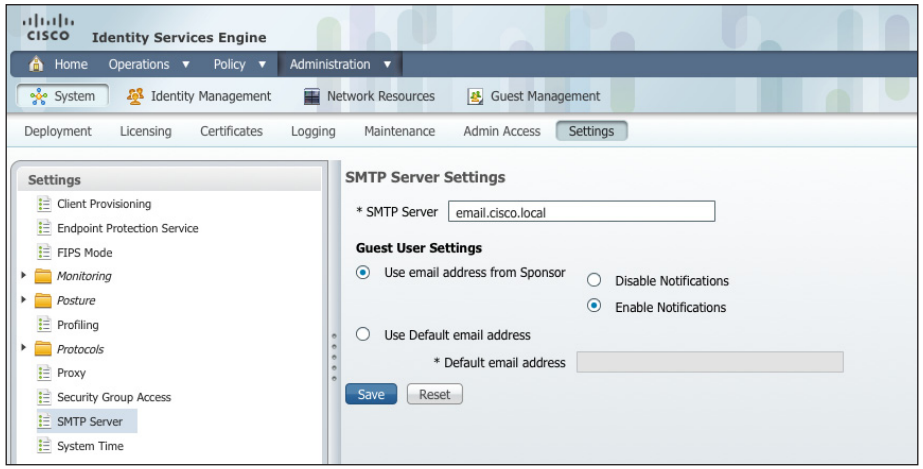
## Procedure 1 Configure sponsor settings

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

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

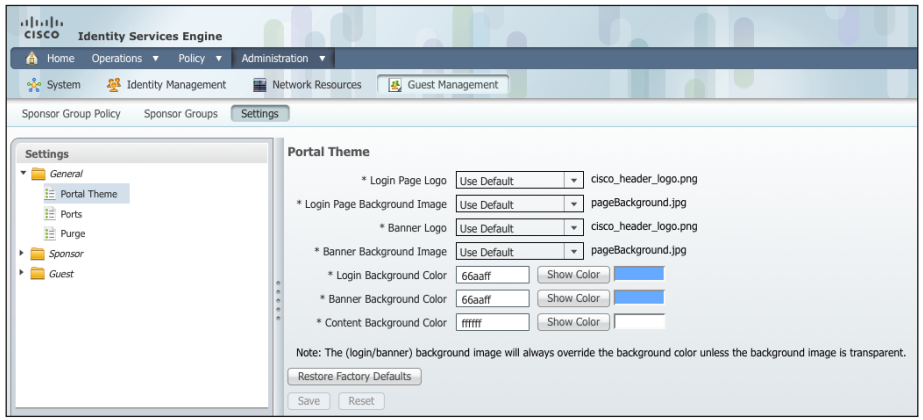
For this deployment, new groups will not be required because the SponsorAllAccounts default group is sufficient, but the following steps detail how to build a new group in order to show the different settings available when setting up groups.

**Step 1:** Using 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.




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

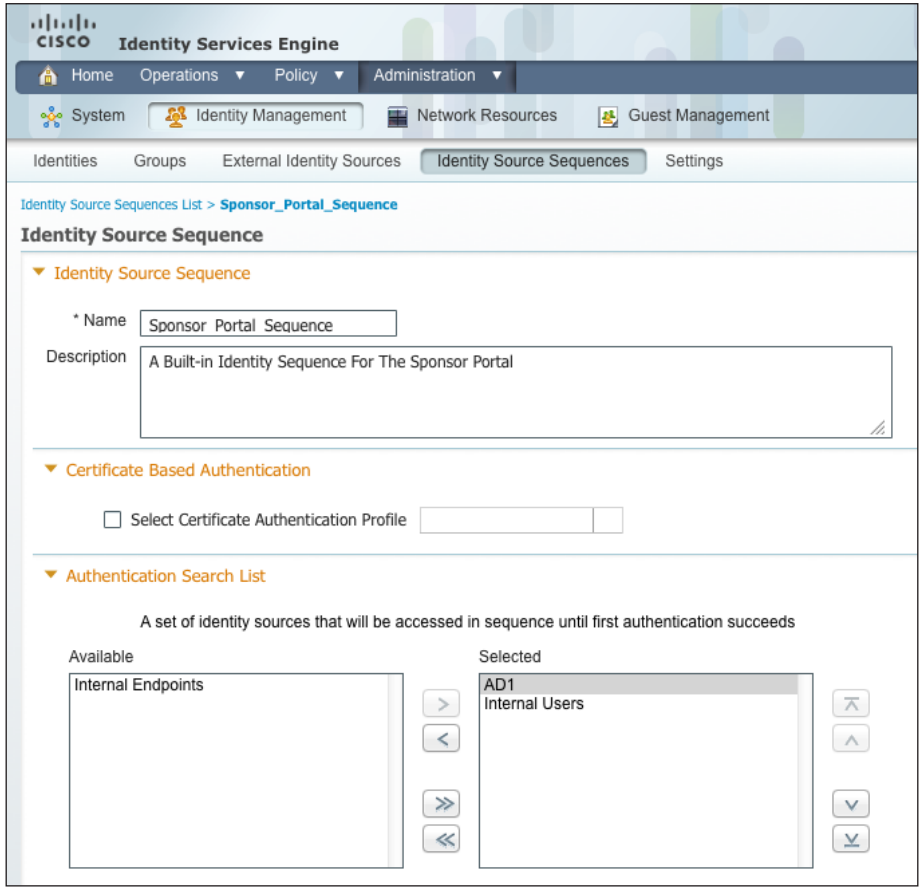
This page defines the sponsor portal layout and is where customizations for the portal page are configured.




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

**Step 4:** From the Available list, choose the Active Directory 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 then fall back to the Internal Users database.




**Step 5:** Click **Save.**

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

**Step 7:** Give the new group a name, for example, OrganizationSponsorAllGroup.

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

Step 9: Under **Guest Roles**, select **SponsorAllAccount**.

Step 10: For **Time Profile**, choose **DefaultFirstLogin**.

Step 11: Click **Submit.**

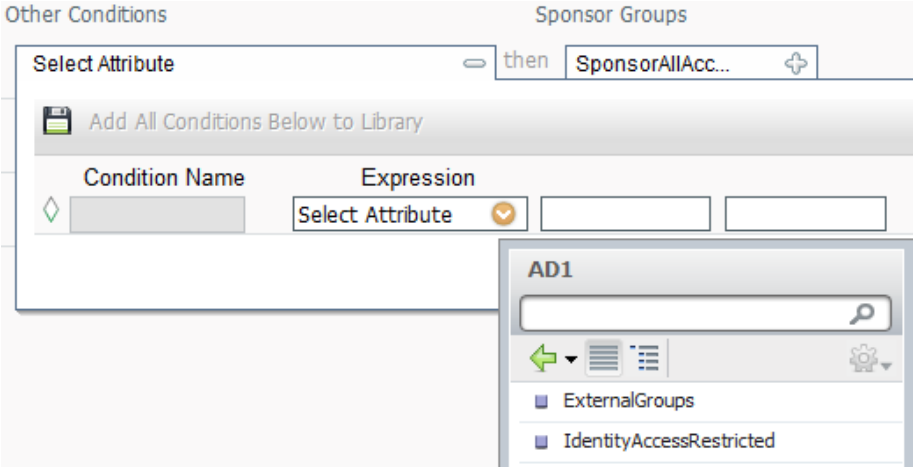
Next you will configure policies that define the sponsor group that is assigned to a sponsor, based on login credentials and other conditions.

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

Step 13: Click the plus sign on **Identity Groups** next to **Manage All Acounts,** and then choose **Any.**

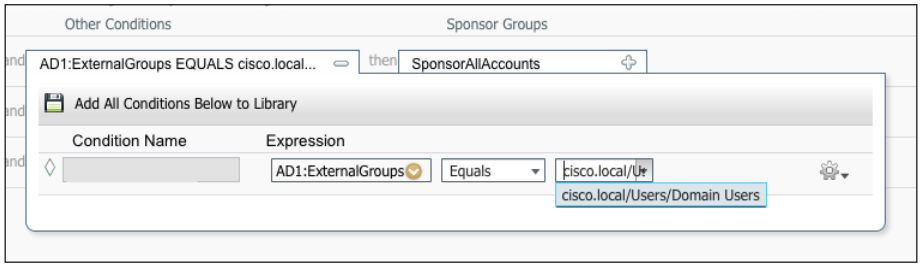
Step 14: Click the plus sign on **Other Conditions**, and then select **Create New Condition**.

Step 15: Under **Expression**, click **Select Attribute**, expand **AD1,** and then select **ExternalGroups**.

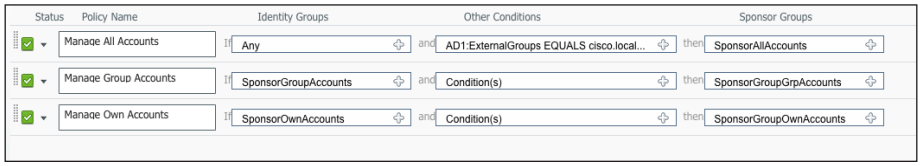



Step 16: In the second box in the **Expression**, select **Equals**.

Step 17: In the third box, select the Active Directory group **Domain Users**.




Step 18: For **Sponsor Groups**, leave it at the default of **SponsorAllAccounts**.




Step 19: Click **Save.**

## Procedure 2 Configure guest settings

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

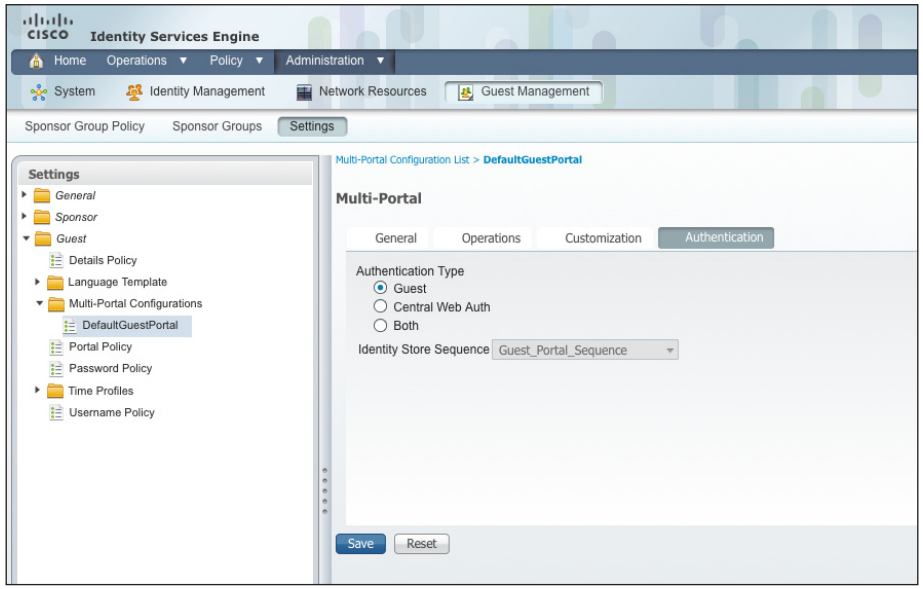
Step 1: Navigate to **Administration** > **Guest Management** > **Settings, and then** expand the **Guest** option in the left-hand panel.

### Tech Tip

The **Details Policy** option allows configuration of required Guest 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 > DefaultGuestPortal, and then, on** the **Authentication** tab, change it to **Guest**. The Guest setting uses only the internal guest user database, which stores sponsor-created guest accounts.

**Step 3:** Click **Save.**




Specific security policies may also require changing password or username policy. These activities are accomplished by using the appropriate selections in this same 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 Wireless LAN Controller 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.

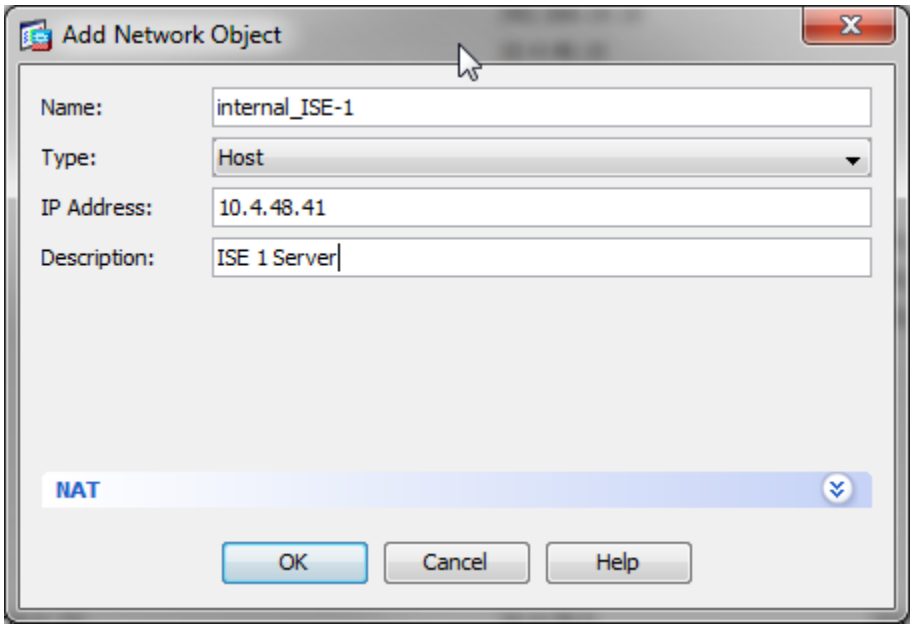
**Step 2:** Choose **Configuration > Firewall > Objects > Network Objects / Groups**.

**Step 3:** Choose **Add > Network Object**.

**Step 4:** In the name box, enter the name of the Cisco ISE server (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 (for example, 10.4.48.41).




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

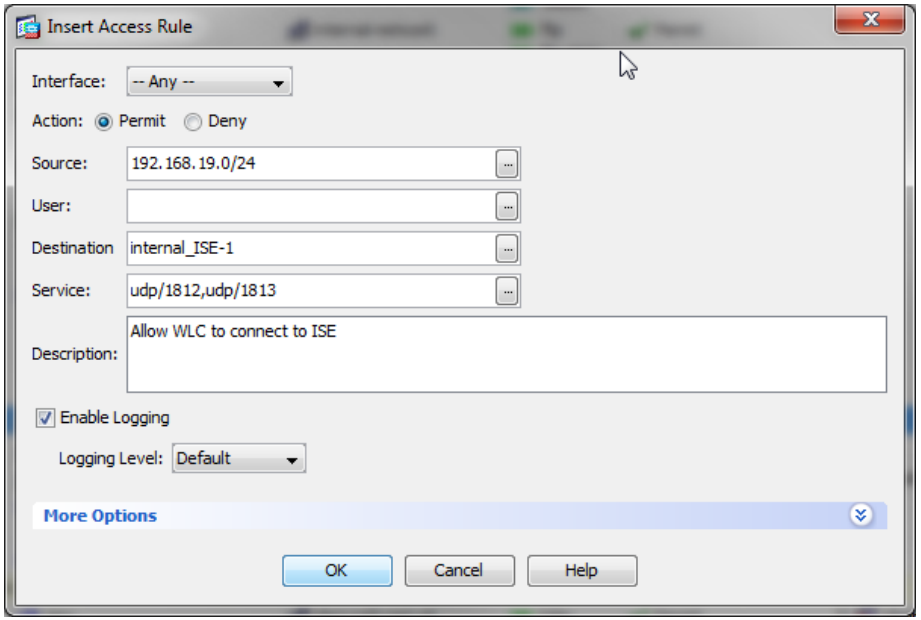
**Step 8:** Navigate to **Configuration** > **Firewall** > **Access Rules**.

**Step 9:** Choose the rule that denies dmz-network access to the internal networks.

**Step 10:** Choose **Add** > **Insert**. This inserts a new access rule before the deny rule that was selected.

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

- Source—Enter the IP address for the guest Cisco Wireless LAN Controller management network: 192.168.19.0/24
- Destination—Enter the address of the ISE server: internal_ISE-1
- Service—udp/1812, udp/1813



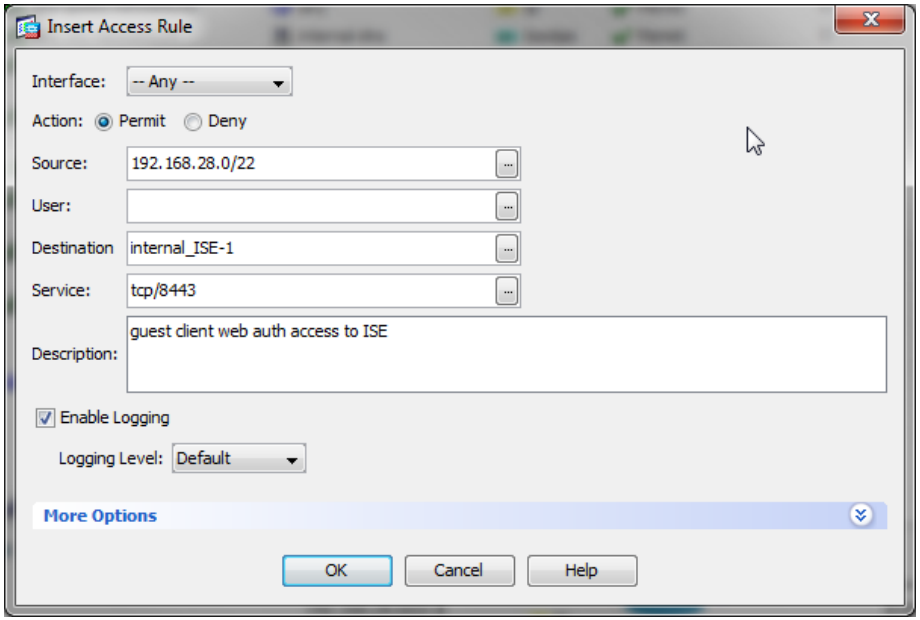

Guest client IP addresses need access through the firewall to the Cisco ISE server for web authentication attempts.

**Step 12:** Select the access rule that denies dmz-guest-network access to the dmz-networks and the internal-network.

**Step 13:** Choose **Add** > **Insert.** This inserts a new access rule before the deny rule that is currently selected.

**Step 14:** Enter access rule details in the following fields:

- Source—Enter the network IP address for the DMZ guest network: 192.168.28.0/22
- Destination—internal_ISE-1
- Service—tcp/8443




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

## Procedure 2 Configure the Wireless LAN Controller

**Step 1:** Browse to the guest anchor Cisco Wireless LAN Controller (WLC) management interface (for example https://guest-wlc) and login.

**Step 2:** Choose **Security** > **AAA** > **RADIUS** > **Authentication** to add the Cisco ISE server as an authentication server in the Cisco Wireless LAN Controller.

**Step 3:** Ensure that other RADIUS Authentication Servers already configured on this WLC are either disabled or removed to ensure that ISE is used for guest user authentication.

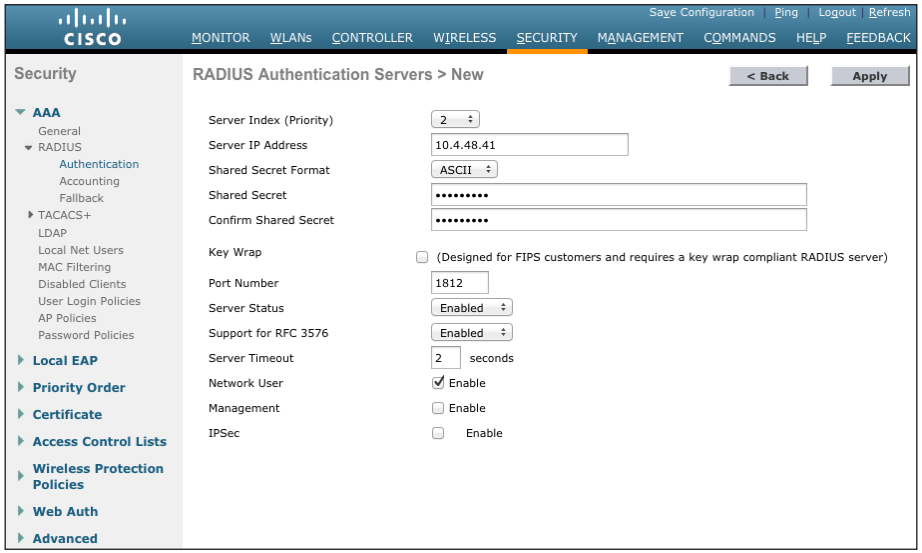
**Step 4:** Click **New**.

**Step 5:** Add the IP Address for the server running Cisco ISE Server: 10.4.48.41

**Step 6:** In the **Shared Secret** field, enter a shared secret.

**Step 7:** In the **Confirm** field, re-enter the shared secret.

**Step 8:** Clear the **Management Enable** check box, and then click **Apply**.




**Step 9:** Click **Apply**

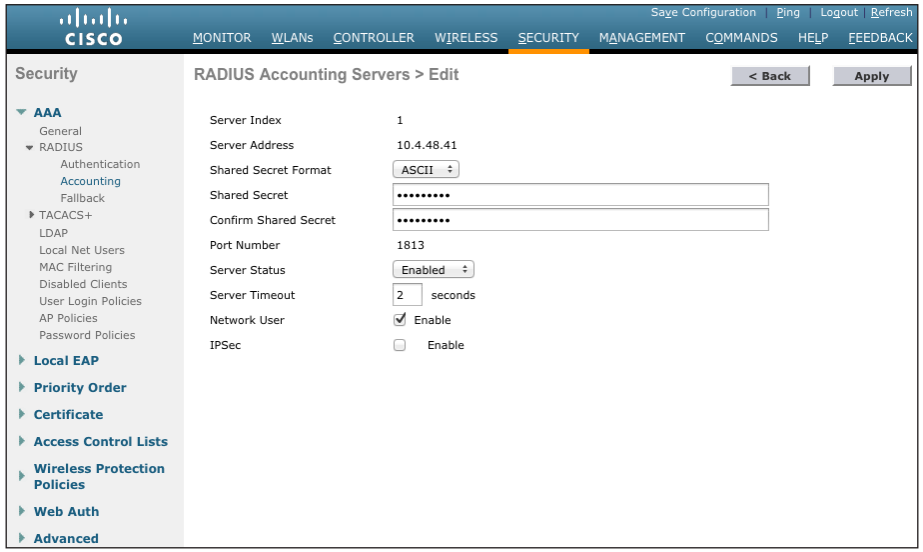
**Step 10:** Navigate to **Security** > **AAA** > **RADIUS** > **Accounting** to add the guest server as an accounting server in the Cisco Wireless LAN Controller.

**Step 11:** Click **New**.

**Step 12:** In the **Server IP Address** field, enter the IP address for the Cisco ISE server: 10.4.48.41

**Step 13:** In the **Shared Secret** field, enter a shared secret.

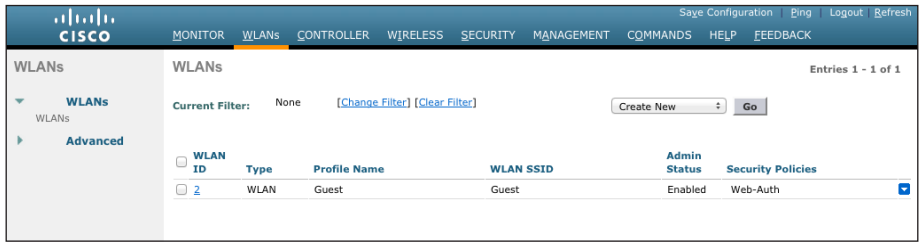
Step 14: In the **Confirm Shared Secret** field, re-enter the shared secret.




Step 15: Click **Apply**.

Step 16: Navigate to **WLANs**.

Step 17: To edit the WLAN, click the **WLAN ID** for the specific WLAN (in this case **2**).




Step 18: In order to modify the Web Authentication Type later in the procedure we must disable the WLANs using Web-Auth as an authentication method.

Step 19: Select the checkbox next to the **Guest** WLAN.

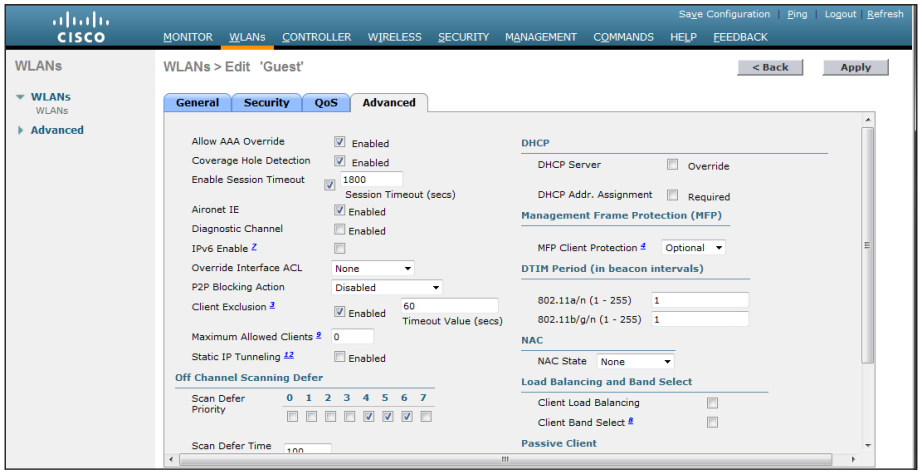
Step 20: Click the **Create New** dropdown and select **Disable Selected**.

Step 21: Click **Go**.

Step 22: Click **OK** to confirm disabling the selected WLANs.

Step 23: Click the **Advanced** tab.

Step 24: For **Allow AAA Override**, select **Enabled**. This allows the per client session time out to be set from the Cisco ISE Server.




Step 25: Click **Apply.**

When a guest wants to log in to the wireless network, they must be presented with a web-based login screen that authenticates them against the credentials stored on the Cisco ISE server 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 the Cisco ISE to retrieve the other options, like time, that are specific to this guest account login.

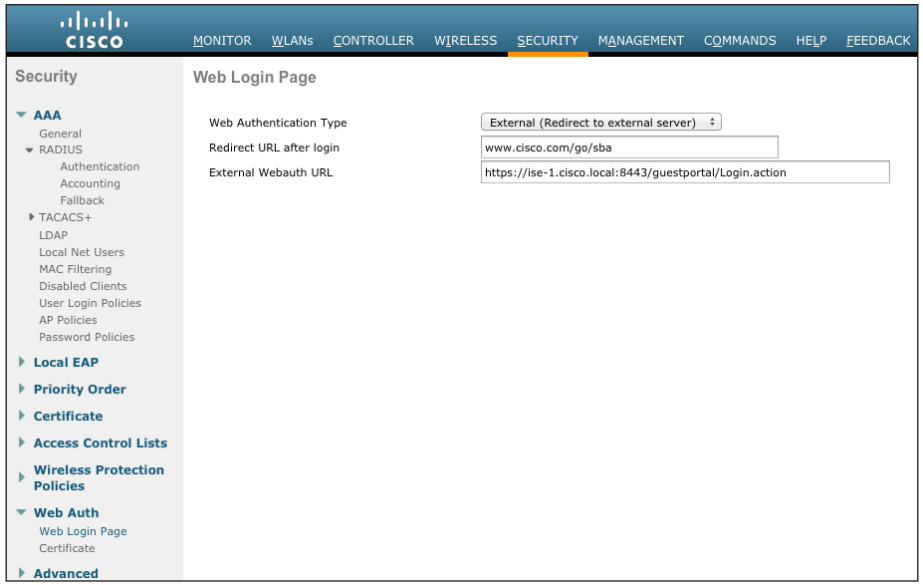
Step 26: Navigate to **Security > Web Auth > Web Login Page.**

Step 27: Change the **Web Authentication Type** to **External (Redirect to external server).**

Step 28: Change the **External Webauth URL** to the location of the Cisco ISE server's guest portal login page:
https://ise-1.cisco.local:8443/guestportal/Login.action

Step 29: Click **Apply.**

**Step 30:** Click **OK** to confirm that the preauthentication ACL has been configured.




**Step 31:** Navigate to **WLANs**.

**Step 32:** To edit the WLAN, click the **WLAN ID** for the specific WLAN (in this case **2**).

**Step 33:** Select the checkbox next to the **Guest** WLAN.

**Step 34:** Click the **Create New** dropdown and select **Enable Selected**.

**Step 35:** Click **Go**.

**Step 36:** Click **OK** to confirm enabling the selected WLANs.

## Process

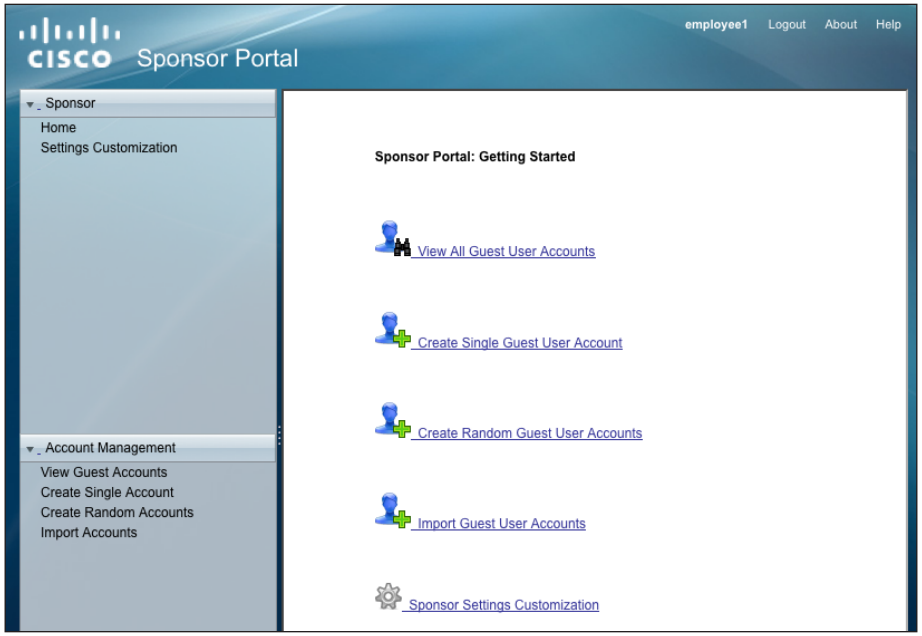
Creating and Using Guest Accounts

1. Use the Sponsor Portal
2. Use guest accounts

## Procedure 1 Use the Sponsor Portal

**Step 1:** Connect to the Cisco ISE Sponsor Portal by using a browser and login:

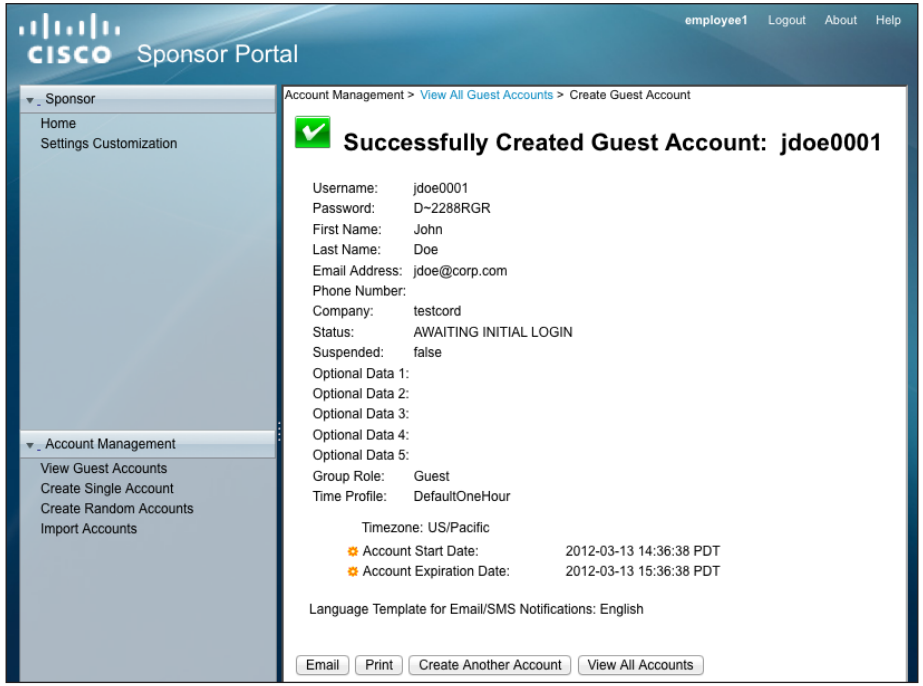
https://ise-1.cisco.local:8443/sponsorportal



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

Step 3: Enter the data as required by the policy implemented in the Sponsor Portal creation, and then click **Submit.**

The guest account and credentials will be returned if the account was successfully created.



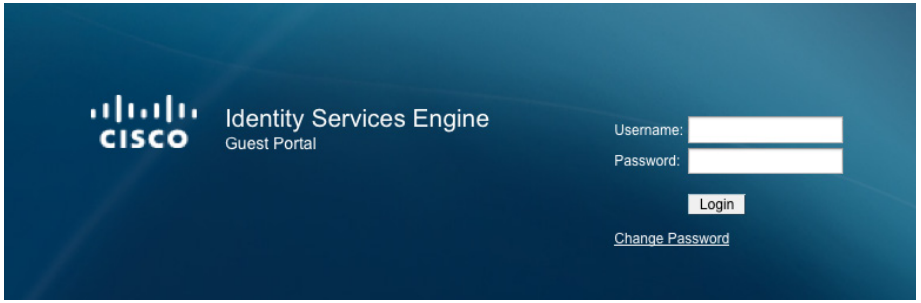

Step 4: If you want to customize sponsor account options, such as language and email notification, click **Settings Customization** on the left side of the main page.

## Procedure 2 Use guest accounts

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

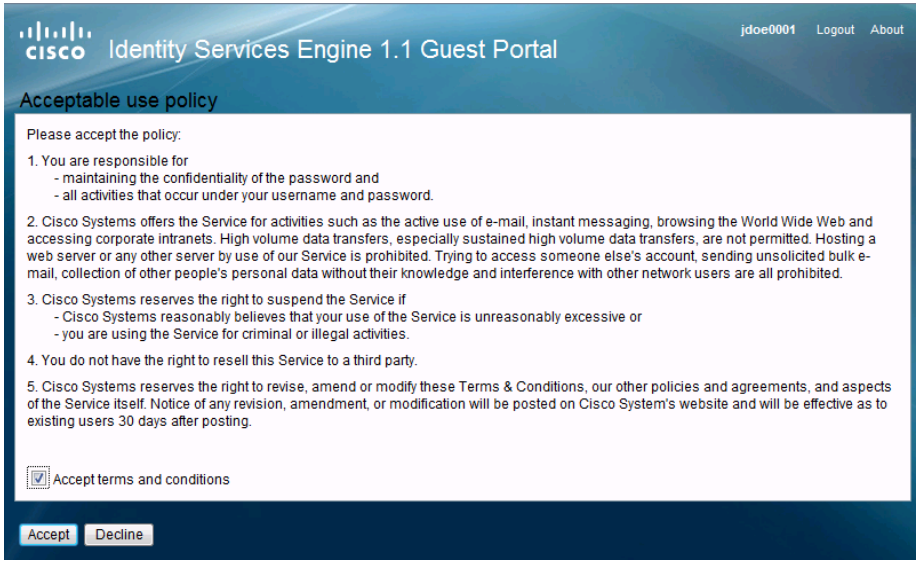
Step 1: Open up a browser and attempt to browse a known website.

Step 2: The browser is redirected to the Cisco ISE Guest Portal where the guest account credentials can be entered.




After entering guest credentials, the user is presented with the Acceptable Use Policy.

Step 3: Select **Accept terms and conditions,** and then click **Accept**.



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

**Notes**

# Appendix A: Product List

| Functional Area | Product | Part Numbers | Software Version |
|---|---|---|---|
| Authentication Services | Cisco ISE Server | ISE-VM-K9=<br>LS-ISE-AD5Y-W-100=<br>Cisco ISE 2500 Endpoint 5-Year Wireless Subscription License<br>LS-ISE-AD5Y-W-250=<br>Cisco ISE 2500 Endpoint 5-Year Wireless Subscription License<br>LS-ISE-AD5Y-W-500=<br>Cisco ISE 2500 Endpoint 5-Year Wireless Subscription License | 1.1.0.665 |
| Guest Wireless LAN Controller | 5508 Wireless LAN Controller | AIR-CT5508-100-K9<br>5508 Wireless LAN Controller with 100 AP license | 7.1.91.0 |

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

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

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

B-0000600-1 3/12