# **Newer Design Guide Available**

Cisco Smart Business Architecture has become part of the Cisco Validated Designs program. For up-to-date guidance on the designs described in this guide, see http://cvddocs.com/fw/Aug13-134 For information about the Cisco Validated Design program, go to http://www.cisco.com/go/cvd





BYOD

SOLUTIONS

F

1111111

CISCO

SBA

## BYOD — Advanced Guest Wireless Access Deployment Guide

SMART BUSINESS ARCHITECTURE

February 2013 Series

## Preface

### **Who Should Read This Guide**

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

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

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

## **Release Series**

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

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

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

#### month year Series

For example, the series of guides that we released in February 2013 is the "February Series".

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

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

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

### **How to Read Commands**

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

Commands to enter at a CLI appear as follows:

configure terminal

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

ntp server 10.10.48.17

Commands with variables that you must define appear as follows:

#### class-map [highest class name]

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

#### Router# enable

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

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

100 100 100

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

interface Vlan64

ip address 10.5.204.5 255.255.2

### **Comments and Questions**

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

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

February 2013 Series

## Table of Contents

What's In This SBA Guide	.1
Cisco SBA Solutions	1
Route to Success	1
About This Guide	1
Introduction	2
Business Overview	2
Technical Overview	3

Deployment Details	5
Deploying Cisco ISE	5
Configuring Cisco ISE Sponsor Portal Services	8
Integrating the Cisco Wireless LAN Controller and Cisco ISE	. 12
Creating and Using Guest Accounts	. 18
Appendix A: Product List	.21
Appendix B: Changes	23

## What's In This SBA Guide

## **Cisco SBA Solutions**

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

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

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

## **Route to Success**

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

## **About This Guide**

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

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

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

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

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



## Introduction

### 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. 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 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 enduser applications to any user or any device at any time.

Other Cisco SBA Solutions guides addressing BYOD business problems include:

- BYOD—Design Overview
- BYOD—Internal Corporate Access Deployment Guide
- · BYOD—Identity and Authentication Deployment Guide
- BYOD—Remote Mobile Access Deployment Guide
- BYOD—Virtual Desktop 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 while they are onsite in order to gain access to authorized organizational resources, as well as VPN connectivity to their employer's network and the Internet, so they can be as productive as possible. However, by offering guests the same level of network access that the organization's users have, the organization is exposed to a significant risk.

Relying on a set group of internal users, such as receptionists and IT helpdesk staff, to create the guest accounts may not be as flexible as an organization requires. The group might not be available 24-hours per 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.

After a guest account has been created, you typically need to tell the guest the account details, the access instructions, and the acceptable-use policy. Dealing with this information when the guest arrives can take a lot of time. Additionally, a guest account often needs to change after it has been created. For example, 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**

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.

#### Dedicated guest wireless topology

## Internet Cisco ASA 4 0000000 Active Directory **Guest Wireless** LAN Controller A. .... Inside Network ISE 00000000 Wireless LAN 0000000 Controller Guest 1) Guest Traffic 2) Tunneled Traffic

➔ 3) Web Auth Redirect

#### Shared guest wireless topology



	4) RADIOS Request from WLC
$\longrightarrow$	5) LDAP Request
<b>*</b> · <b>-</b> · <b>-</b> · <b>*</b>	6) Authenticated Guest Traffic

## **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.

**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? U/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.



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.

cisco Identity Services Engine		ise-1 admin Logout Feedback
🛕 Home Operations 🔻 Policy 🔻 Adr	ministration 🔻	👓 Task Navigator 👻 📀
🔆 System 👰 Identity Management	Network Resources 🛃 Guest Management	
Deployment Licensing Certificates Lo	gging Maintenance Admin Access Settings	
License Operations	Current License 5 ise-1 Import new License File * License File C\Downloads\u00edse-base-license.lic Import Cancel	

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)



#### **Procedure 4**

**Configure 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.

cisco Identity Services Engine	ise-1 admin Logout Feedback
👌 Home Operations 🔻 Policy 🔻 Admini	stration 🔹 😶 Task Navigator 🔹 😢
🔆 System 🖉 Identity Management 🕋 N	letwork Resources 🛛 🛃 Web Portal Management
Identities Groups External Identity Sources	Identity Source Sequences Settings
External Identity Sources	Connection       Advanced Settings       Groups       Attributes         To configure Active Directory: <ul> <li>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 cites, submit the active Directory configuration to all nodes in the ISE deployment.</li> <li>After the configuration has been submitted, then Join or Leave operations must be performed.</li> <li> <ul> <li></li></ul></li></ul>
	Save Configuration Delete Configuration
🕑 Help	Alarms 👩 0 🛕 0 🕦 0   😝 Notifications (0)

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.

CISCO Identity Services Engine		ise-1 admin Logout Feedback
🛕 Home Operations 🔻 Policy 🔻 A	dministration 🔻	🕶 Task Navigator 👻 🚷
system 🛃 Identity Management	Network Resources 🛛 👪 Guest Management	
Identities Groups External Identity Source	es Identity Source Sequences Settings	
External Identity Sources	Active Directory > AD1 Connection Advanced Settings Groups Attributes  Domain Name cisco.local	
DAP	One or more nodes may be selected for Join or Leave operations. If a node is joined their	n a leave operation
RADIUS Token	is required before a rejoin. Select one node for Test Connection.	
RSA SecurID	Oct 2 Join Q Leave Q Test Connection	
	ISE Node   ISE Node Status	
	✓ ise-1 STANDALONE ▲ Not Joined to Do	main
	Join Domain × • User Name: Administrator • Password: OK Cancel	

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.

Home Operations System Mome Methods	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.
Identities Groups Extern	Domain: discolocal Filter: * Retrieve Groups Number of Groups Retrieved: 64 (Limit is 100)
External Identity Sources	Name     Siscalocal/Users/DHCP Administrators     discalocal/Users/DHCP Isarce
Active Directory	discloted/sers/Dnied RODC Password Replication Group     discloted/Users/Dnied RODC Password Replication Group     discloted/Users/DnsAdmins
RADIUS Token	ciscolocal/Users/DonsUpdatProxy ciscolocal/Users/Domain Admins ciscolocal/Users/Domain Computers
	cisco local/Users/Domain Controllers     cisco local/Users/Domain Guests
	discolocal/Users/Emterprise Read-only Domain Controllers     discolocal/Users/Emterprise Read-only Domain Controllers
	cisco.local/Users/Group Policy Creator Owners
	OK Cancel







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.



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.

cisco Identity Services Engine		ise-5 admin Logout Feedback
🏠 Home Operations 🔻 Policy 🔻 Ad	istration 👻	👓 Task Navigator 👻 👩
🔆 System 🦉 Identity Management	Network Resources Keb Portal Management	
Sponsor Group Policy Sponsor Groups S	ings	
Settings	Portal Theme  * Login Page Logo Use Default * cisco_header_log  * Login Page Background Image Use Default * pageBackground Banner Logo Use Default * pageBackground * Default * pageBackground * pageBackground * Default * Default * Default * pageBackground * Default * pageBackground * Default * Default * Default * Default * Default * Default * pageBackground * Default * pageBackground * Default	io.png jpg jpo.png jpo f f f f k d color unless the background image is hy Devices Portal.
	Save Reset	
🕗 Help	Alar	rms 🚳 185 🛕 0 🕤 0   Notifications (0)

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.

ahah			
cisco Identity Services Engine			ise-5 admin Logout Feedba
Adminis	tration 🗸		•• Task Navigator • 🧑
🔆 System 🖉 Identity Management	Network Resources 🛃 Web Portal Manager	nent	
Identities Groups External Identity Sources	Identity Source Sequences Settings		
dentity Source Sequences List > Sponsor_Portal_Sequence			
dentity Source Sequence			
<ul> <li>Identity Source Sequence</li> </ul>			
* Name Sponsor Portal Sequence			
Description A Built-in Identity Sequence For The S	ponsor Portal		
		vq	
<ul> <li>Cerunicate based Autrientication</li> </ul>			
Select Certificate Authentication Profile			
<ul> <li>Authentication Search List</li> </ul>			
A set of identity sources that will be acces	ed in sequence until first authentication succeeds		
Available Internal Endpoints	Selected		
arcentar Eropoints	> Internal Users	$\overline{}$	
	<	~	
	>>	V	
	~	¥	
Advanced Search List Settings			
A THE REPORT OF A THE REPORT O			
Selectine action to be performed it a selected identity store cannot be accessed for authemication			
Do not access other stores in the sequence and set of a Automication status automic to ProcessEffOF			
O Lear as a ne rase, was not norm and horized to the lief zone and the sednence			
Save			
			Alarma A 196 + 0 A   Notficitions (0)
Ca ush			Marine V 100 2 0 0 0 1 Nochcabons (0)

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**.

ululu CISCO Identity Services Engine				
Administration V Administration V				
🔆 System 🛛 🖉 Identity Manage	ment 📱 Network Resources 📳 Web Portal Management			
Sponsor Group Policy Sponsor G	roups Settings			
Sponsor Group List > New Sponsor Group Sponsor Group	const Balas Tran Balfas			
General Additionzation cev	es quest roles i líne Prones			
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 99999999)			
* Maximum Duration of Account	1 Days (Valid Range 1 to 99999999)			
Submit Cancel				

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 B	elow to Library
Condition Name	Expression Select Attribute AD1

**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 C then SponsorAllAccounts	
and	Add All Conditions Below	to Library	
	Condition Name	Expression	
and	◊	AD1:ExternalGroups Equals  Equals  Cisco.local/Ur Cisco.local/Ur Cisco.local/Users/Domain Users	<b>∦</b> •

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

Stat	us Policy Name	Identity Groups	Other Conditions	Sponsor Groups
-	Manage All Accounts	If Any	AD1:ExternalGroups EQUALS cisco.local	수 then SponsorAllAccounts 수
-	Manage Group Accounts	If SponsorGroupAccounts	d Condition(s)	♦ then SponsorGroupGrpAccounts
-	Manage Own Accounts	If SponsorOwnAccounts	승 and Condition(s)	승 then SponsorGroupOwnAccounts 수

#### 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.

CISCO Identity Services Engine	
🛕 Home Operations 🗸 Policy 🚽 Admi	nistration 🚽
🔆 🔆 System 🦉 Identity Management	Network Resources Web Portal Management
Sponsor Group Policy Sponsor Groups Se	ttings
Settings	Multi-Portal Configuration List > DefaultGuestPortal
General	Multi-Portal
Sponsor	
My Devices	General Operations Customization Authentication
▼ Guest	Authentication Type
E Details Policy	<ul> <li>Guest</li> </ul>
Language Template	Central Web Auth
<ul> <li>Multi-Portal Configurations</li> </ul>	O Both
E DefaultGuestPortal	Identity Store Sequence Guest_Portal_Sequence
E Portal Policy	
Password Policy	
Time Profiles	
Username Policy	• •

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).

🔁 Add Netwo	rk Object	×
Name:	internal_ISE-1	
Type:	Host	•
IP Address:	10.4.48.41	
Description:	ISE 1 Server	
NAT		
iner i		~
	OK Cancel Help	

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

insert Access	Rule								
Interface:	Any 🔹								
Action: 💿 Pern	nit 💿 Deny								
Source Criteria									
Source:	192.168.19.0/24								
User:									
Security Group:									
Destination Crite	ria								
Destination:	internal_ISE-1								
Security Group:									
Service:	udp/1812,udp/1813								
Description:	Allow WLC to connect to ISE								
📝 Enable Loggi	☑ Enable Logging								
Logging Leve	el: Default 🗸								
More Options	*								
	OK Cancel Help								

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

📑 Insert Access	Rule
Interface:	Any 🗸
Action: 💿 Pern	nit 💿 Deny
Source Criteria	
Source:	192.168.28.0/22
User:	
Security Group:	
Destination Crite	ria
Destination:	internal_ISE-1
Security Group:	
Service:	tcp/8443
Description:	guest client web auth access to ISE
📝 Enable Loggi	ng
Logging Leve	al: Default 👻
More Options	*
	OK Cancel Help

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

Procedure 2	Configure	the wireless	LAN controlle
-------------	-----------	--------------	---------------

**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.

ahaha		Sa <u>v</u> e Configuration Ping Logout <u>R</u> efresh
CISCO	MONITOR WLANS CONTROLI	ER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Security	RADIUS Authentication Se	rvers > New < Back Apply
<ul> <li>AAA</li> <li>General</li> <li>RADIUS</li> <li>Authentication</li> <li>Accounting</li> <li>Fallback</li> </ul>	Server Index (Priority) Server IP Address Shared Secret Format Shared Secret	2 * 10.4.48.41 ASCII *
<ul> <li>TACACS+ LDAP Local Net Users MAC Filtering</li> </ul>	Confirm Shared Secret Key Wrap	Obesigned for FIPS customers and requires a key wrap compliant RADIUS server)
Disabled Clients User Login Policies AP Policies Password Policies	Port Number Server Status Support for RFC 3576	1812 Enabled ‡ Enabled ‡
Local EAP	Server Timeout	2 seconds
Priority Order     Certificate	Network User Management	Enable     Enable
Access Control Lists	IPSec	Enable
Wireless Protection     Policies		
<ul> <li>Web Auth</li> <li>Advanced</li> </ul>		

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.

alialia.					Sa <u>v</u> e Co	onfiguration P	ing Log	gout <u>R</u> efresh
cisco	<u>m</u> onitor <u>w</u> l	.ANs <u>C</u> ONTROLL	.ER W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK
Security	RADIUS Acc	ounting Serve	rs > Edit			< Bac	k	Apply
<ul> <li>AAA</li> <li>General</li> <li>RADIUS</li> <li>Authentication</li> <li>Accounting</li> <li>Fallback</li> <li>TACACS+</li> <li>LOAP</li> <li>LOAP</li> <li>Local Net Users</li> <li>MAC Filtering</li> <li>Disabled Clients</li> <li>User Login Policies</li> <li>AP Policies</li> </ul>	Server Index Server Addres Shared Secret Confirm Share Port Number Server Status Server Timeou Network User	is Format ( ed Secret [ ut [	1 10.4.48.41 ASCII ÷ 1813 Enabled ÷ 2 seconds ✓ Enable					
Password Policies	IPSec	(	Enable					
P LOCALEAP								
Priority Order								
Access Control Lists								
Wireless Protection     Policies								
Web Auth								
Advanced								

#### 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.

راریان cısco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	Sa <u>v</u> e C <u>O</u> MMANDS	Configur HE <u>L</u> P	ation Ping Logout FEEDBACK	:   <u>R</u> efres
WLANs	WLANs								Entries 1	- 1 of 1
WLANs         Current Filter:         None         [Change Filter]         Create New         E           WLANs         WLANs         Go         Go						o				
Advanced		Туре	Profile Name		WLAN S	SID	Admin Status	Secu	irity Policies	
	0.0	MIAN	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.

ululu cisco	Saye Configuration Bing Logout MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	<u>R</u> efr
WLANs	WLANs > Edit 'Guest' <back app<="" td=""><td>ly</td></back>	ly
WLANS WLANS	General Security QoS Advanced	_
Advanced	Allow AAA Override V Enabled DHCP	Î
	Enable Session Timeout [2] 1800 DHCP Server Override Session Timeout (secs) DHCP Addr. Assignment Required	
	Arronet IE IZ Enabled Management Frame Protection (MFP) Diagnostic Channel Enabled	
	IPv6 Enable Z     MFP Client Protection ± Optional •       Override Interface ACL     None •       DTIM Period (in beacon intervals)	E
	P2P Blocking Action Disabled	
	Client Exclusion 2 Client Ex	
	Maximum Allowed Clients 2 0 NAC Static IP Tunneling 12 Enabled NAC State None	
	Off Channel Scanning Defer Load Balancing and Band Select	
	Scan Defer         0         1         2         3         4         5         6         7         Client Load Balancing           Priority         Image: Client Stand Select #         Image: Client Band Band #         Image	
	Scan Defer Time 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.



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

<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	COMMANDS	HE <u>L</u> P	<u>F</u> EEDBACK
Access C	Control L	ists > Rules >	New			l	< Back	Apply
Sequence		1						
Source		Any -	·			-		
Destination		IP Address 🔻	•	IP Addre 10.4.48	ess .0	Vetmask 255.255.255.0		
Protocol		Any	Ŧ					
DSCP		Any •	·					
Direction		Any •	·					
Action		Permit 🔻	·					



**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

MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK
Access C	control L	ists > Rules >	New			1	< Back	Apply
Sequence		2		IP Addre	ss N	letmask		
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 23, and then click Apply.

ANs > Edit 'GUEST V	ALIDATION'		I	< Back	Apply
eneral Security Q	oS Advanced				
Layer 2 Layer 3	AA Servers				
Laver 3 Security None	1				
Effort of occurring filterion	-				
Authentication					
C Passthrough					
C Conditional Web Redire	ct				
C Splash Page Web Redir	ect				
C On MAC Filter failure 10					
Preauthentication ACL	IPv4 Pre-Auth-for-External-Web-Server 💌	IPv6 None 💌	WebAuth FlexAcl No	ne 💌	
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 36.

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.

Layer 2 Layer 3 AAA Se Select AAA servers below to ove Radius Servers	rrvers			
Select AAA servers below to ove Radius Servers	rride use of default servers			
Radius Servers		on this WLAN		*
			LDAP Servers	
Radius Server Overwrite interfac	e 📃 Enabled		Server 1 None 🔻	
	Authentication Servers	Accounting Servers	Server 2 None -	
	Enabled	Enabled	Server 3 None 🔻	-
Server 1	IP:10.10.48.41, Port:1812	· IP:10.10.48.41, Port:1813 •		=
Server 2	None	• None •		
Padius Server Accounting	None	• None •		
Interim Update				
Local EAP Authentication				
Local EAP Authentication	abled			
Authentication priority order	for			
web datil user				
Not Used	Order Used For Aut	entication		
I DAP	RADIUS	Up		

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/go/sba)

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

uluilu cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Security	Web Log	in Page							
AAA     General     RADIUS     Authentication     Accounting     Fallback     TACACS+     LDAP     Local Net Users     MAC Filtering     Disabled Clients     User Login Policies     AP Policies     Password Policies	Web Auth Redirect I External 1	ventication URL after lo	Type Igin RL	E w ht	xternal (Redirec ww.cisco.com/g tps://ise-1.cisco	t to external server p/sba .local:8443/guestp	) : ortal/Login.action	1	
Local EAP									
<ul> <li>Priority Order</li> <li>Certificate</li> <li>Access Control Lists</li> <li>Wireless Protection Policies</li> <li>Web Auth</li> </ul>									
Web Auth     Web Login Page     Certificate     Advanced									

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**.

uluili. cisco	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY MANAGEMENT	COMMANDS HELP	EEDBACK	Sa⊻e Configuration
WLANs	WLANs					
WLANS WLANS	Current Filter: No	ne [Change filter] [Cl	lear filter]		Enable Selected 👻 🐻	
Advanced	WLAN ID Type	Profile Name	WLAN SSID		Admin Status Security Policies	
	VLAN	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.



#### 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.



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

![](_page_21_Picture_7.jpeg)

**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.

cisco Sponsor Porta	al	employee1	
Sponsor Home Settings Customization	Account Menagement > View AB Ouest Accounts > Onele Guest Account Create Guest Accounts First Name: David Last Name: Smith Email Address: dsmith/BganvMere.com Phone Number: 555-555-0100 +1 (555) 555-0100 Company Optional Data 1: Optional Data 2: Optional Data 4:		
Account Management     View Ouest Accounts     Create Single Account     Create Random Accounts     Import Accounts	Optional Data 5 • Group Role: Ouest • • Time Profile: DefaultOneHour • • Time Zone: PST8PDT • • Language Template for Email/SMS Notifications: English • • Required fields Submit Cancel		

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

cisco Sponsor Port	employeet Logod Help
▼ Sponsor	Account Management > View All Guest Accounts > Create Guest Account
Home Settings Customization	Successfully Created Guest Account: dsmith01
	Usename: dsmth01 Password: _FV78H88 First Name: David Last Name: Smth Company: Any Company Status: Any Company Status: Any Company Status: Any Company Company: Company Status: Company Status
+ Account Management	Optional Data 5:
View Guest Accounts	Group Role: Guest
Create Single Account Create Random Accounts Import Accounts	Time Profile: DefaultOneHour Time Zone: PSTPD/T © Account Starb Take: 2012-12-10.06.43.11 PST © Account Expiration Date: 2012-12-10.07.43.11 PST Language Template for Email/SMS Notifications: English Email: Print: Create Another Account: View All Accounts

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

- Sponsor	Sponsor > Settings Customizations	
Home Settings Customization	Settings Customizati	on
	Language Template:	English v
	Use Browser Locale:	
	Time Zone:	PST8PDT -
	Location:	
	Sponsor's Email Address:	
	Receive Email Confirmation:	
	Default Page to Show After Login:	Sponsor Portal: Getting Started -
	e = Required fields	
	Save Report	
<ul> <li>Account Management</li> </ul>	oave Reset	

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.

![](_page_22_Picture_11.jpeg)

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

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

![](_page_23_Picture_1.jpeg)

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.

![](_page_23_Picture_3.jpeg)

![](_page_23_Picture_4.jpeg)

### **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 Virutal 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	Cisco 5500 Series Wireless Controller for up to 500 Cisco access points	AIR-CT5508-500-K9	7.4.100.0
Guest Controller	Cisco 5500 Series Wireless Controller for up to 250 Cisco access points	AIR-CT5508-250-K9	
	Cisco 5500 Series Wireless Controller for up to 100 Cisco access points	AIR-CT5508-100-K9	
	Cisco 5500 Series Wireless Controller for up to 50 Cisco access points	AIR-CT5508-50-K9	
	Cisco 5500 Series Wireless Controller for up to 25 Cisco access points	AIR-CT5508-25-K9	
	Cisco 5500 Series Wireless Controller for up to 12 Cisco access points	AIR-CT5508-12-K9	
	Cisco 5500 Series Wireless Controller for High Availability	AIR-CT5508-HA-K9	
On Site Controller, Guest	Cisco 2500 Series Wireless Controller for up to 50 Cisco access points	AIR-CT2504-50-K9	7.4.100.0
Controller	Cisco 2500 Series Wireless Controller for up to 25 Cisco access points	AIR-CT2504-25-K9	
	Cisco 2500 Series Wireless Controller for up to 15 Cisco access points	AIR-CT2504-15-K9	
	Cisco 2500 Series Wireless Controller for up to 5 Cisco access points	AIR-CT2504-5-K9	

## 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)
	Cisco ASA 5525-X IPS Edition - security appliance	ASA5525-IPS-K9	IPS 7.1(6)E4
	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)SE IP Base license

## Appendix B: Changes

This appendix summarizes the changes to this guide since the previous Cisco SBA series.

- We upgraded Cisco ISE software to version 1.1.2
- We added Guest Anchor support for the 2500 Series Wireless LAN
   Controller

![](_page_26_Picture_4.jpeg)

### Feedback

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

![](_page_27_Picture_2.jpeg)

cisco.

Americas Headquarters Cisco Systems, Inc. San Jose, CA Asia Pacific Headquarters Cisco Systems (USA) Pte. Ltd. Singapore Europe Headquarters Cisco Systems International BV Amsterdam, The Netherlands

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

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITH-OUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR 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 OF USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS ON TO 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 CINSC.

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

© 2013 Cisco Systems, Inc. All rights reserved.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

#### B-0000134-1 2/13