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/Aug13-355 For information about the Cisco Validated Design program, go to http://www.cisco.com/go/cvd





11 11-1-1-1 CISCO BORDERLESS NETWORKS DEPLOYMENT GUIDE SBA

Wireless LAN 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 Borderless Networks	1
Route to Success	1
About This Guide	1
Introduction	2
Business Overview	2
Technology Overview	2

Deployment Details9
Configuring the RADIUS Server: Cisco Secure ACS
Configuring the RADIUS Server: Windows Server 2008
Configuring On-Site Wireless Controllers25
Configuring Remote-Site Wireless with Cisco FlexConnect46
Configuring Guest Wireless: Shared Guest Controller73
Configuring Guest Wireless: Dedicated Guest Controller
Appendix A: Product List
Appendix B: Changes

What's In This SBA Guide

Cisco SBA Borderless Networks

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 Borderless Networks is a comprehensive network design targeted at organizations with up to 10,000 connected users. The SBA Borderless Network architecture incorporates wired and wireless local area network (LAN) access, wide-area network (WAN) connectivity, WAN application optimization, and Internet edge security infrastructure.

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

Business Overview

In today's modern society, people are increasingly mobile in all aspects of their life. With the adoption of smartphones and tablets, the need to stay connected while mobile has evolved from a nice-to-have to a must-have. The use of wireless technologies can improve our effectiveness and efficiency by allowing us to stay connected, regardless of the location or platform being used. As an integrated part of the conventional wired network design that provides connectivity while users are stationary, wireless technology allows connectivity while we are going about our daily responsibilities. Wireless technologies have the capabilities to turn cafeterias, home offices, classrooms, and our vehicles into meeting places with the same effectiveness as being connected to the wired network. In fact, the wireless network has in many cases become more strategic in our lives than that of our wired networks of yesterday. Given the dependency of wireless networks on wired infrastructure, both are equally important in an overall end-to-end architecture.

Technology Overview

This deployment uses a wireless network in order to provide ubiquitous data and voice connectivity for employees and to provide wireless guest access for visitors to connect to the Internet.

Regardless of their location within the organization, on large campuses, or at remote sites, wireless users can have a similar experience when connecting to voice, video, and data services.

Benefits

- Productivity gains through secure, location-independent network access—Measurable productivity improvements and communication.
- Additional network flexibility—Hard-to-wire locations can be reached without costly construction.
- **Cost effective deployment** Adoption of virtualized technologies within the overall wireless architecture.

- Easy to manage and operate—From a single pane of glass, an organization has centralized control of a distributed wireless environment.
- **Plug-and-play deployment**—Automatic provisioning when an access point is connected to the supporting wired network.
- Resilient, fault-tolerant design—Reliable wireless connectivity in mission-critical environments, including complete RF-spectrum management.
- Support for wireless users—Bring your Own Device (BYOD) design models.
- Efficient transmission of multicast traffic— Support for many group communication applications, such as video and push-to-talk.

This Cisco Smart Business Architecture (SBA) deployment uses a controllerbased wireless design. Centralizing configuration and control on the Cisco wireless LAN controller (WLC) allows the wireless LAN (WLAN) to operate as an intelligent information network and support advanced services. This centralized deployment simplifies operational management by collapsing large numbers of managed endpoints.

The following are some of the benefits of a centralized wireless deployment:

- Lower operational expenses—A controller-based, centralized architecture enables zero-touch configurations for lightweight access points. Similarly, it enables easy design of channel and power settings and real-time management, including identifying any RF holes in order to optimize the RF environment. The architecture offers seamless mobility across the various access points within the mobility group. A controllerbased architecture gives the network administrator a holistic view of the network and the ability to make decisions about scale, security, and overall operations.
- Improved Return on Investment—With the adoption of virtualization, wireless deployments can now utilize a virtualized instance of the wireless LAN controller, reducing the total cost of ownership by leveraging their investment in virtualization.
- Easier way to scale with optimal design—As the wireless deployment scales for pervasive coverage and to address the ever-increasing

density of clients, operational complexity starts growing exponentially. In such a scenario, having the right architecture enables the network to scale well. Cisco wireless networks support two design models, local mode for campus environments and Cisco FlexConnect for lean remote sites.





Deployment Components

The Cisco SBA WLAN deployment is built around two main components: Cisco wireless LAN controllers and Cisco lightweight access points.

Cisco Wireless LAN Controllers

Cisco wireless LAN controllers are responsible for system-wide WLAN functions, such as security policies, intrusion prevention, RF management, quality of service (QoS), and mobility. They work in conjunction with Cisco lightweight access points to support business-critical wireless applications. From voice and data services to location tracking, Cisco wireless LAN controllers provide the control, scalability, security, and reliability that network managers need to build secure, scalable wireless networks—from large campus environments to remote sites.

Although a standalone controller can support lightweight access points across multiple floors and buildings simultaneously, you should deploy controllers in pairs for resiliency. There are many different ways to configure controller resiliency; the simplest is to use a primary/secondary model where all the access points at the site prefer to join the primary controller and only join the secondary controller during a failure event. However, even when configured as a pair, wireless LAN controllers do not share configuration information. Each wireless LAN controller must be configured separately.

The following controllers are included in this release of Cisco SBA:

- Cisco 2500 Series Wireless LAN Controller—This controller supports up to 75 lightweight access points and 1000 clients. Cisco 2500 Series Wireless LAN Controllers are ideal for small, single-site WLAN deployments.
- Cisco 5500 Series Wireless LAN Controller—This controller supports up to 500 lightweight access points and 7000 clients, making it ideal for large-site and multi-site WLAN deployments.
- Cisco Virtual Wireless LAN Controller—vWLCs are compatible with ESXi 4.x and 5.x and support up to 200 lightweight access points across two or more Cisco FlexConnect groups and 3000 clients total. Each vWLC has a maximum aggregate throughput of 500 Mbps when centrally switched with additional capacity achieved horizontally through the use of mobility groups. The virtualized appliance is well suited for small and medium-sized deployments utilizing a FlexConnect architecture.
- Cisco Flex 7500 Series Cloud Controller—Cisco Flex 7500 Series
 Cloud Controller for up to 6000 Cisco access points supports up to
 64,000 clients. This controller is designed to meet the scaling require ments to deploy the Cisco FlexConnect solution in remote-site networks.

Because software license flexibility allows you to add additional access points as business requirements change, you can choose the controller that will support your needs long-term, but you purchase incremental accesspoint licenses only when you need them.

Cisco Lightweight Access Points

In the Cisco Unified Wireless Network architecture, access points are *lightweight*. This means they cannot act independently of a wireless LAN controller (WLC). The lightweight access points (LAPs) have to first discover the WLCs and register with them before the LAPs service wireless clients. There are two primary ways that the access point can discover a WLC:

- Domain Name System (DNS)—When a single WLC pair is deployed in an organization, the simplest way to enable APs to discover a WLC is by creating a DNS entry for cisco-capwap-controller that resolves to the management IP addresses of WLCs.
- Dynamic Host Configuration Protocol (DHCP)—Traditionally, when multiple WLC pairs are deployed in an organization, DHCP Option 43 was used to map access points to their WLCs. Using Option 43 allows remote sites and each campus to define a unique mapping.

As the access point communicates with the WLC resources, it will download its configuration and synchronize its software or firmware image, if required.

Cisco lightweight access points work in conjunction with a Cisco wireless LAN controller to connect wireless devices to the LAN while supporting simultaneous data-forwarding and air-monitoring functions. The Cisco SBA wireless design is based on Cisco 802.11n wireless access points, which offer robust wireless coverage with up to nine times the throughput of 802.11a/b/g networks. The following access points are included in this release of Cisco SBA:

 Cisco Aironet 1600 Series Access Points are targeted for small and medium enterprises seeking to deploy or migrate to 802.11n technology at a low price point. The access point features a 3x3 MIMO radio with support for two spatial-streams.

Wireless networks are more than just a convenience; they are mission-critical to the business. However, wireless operates in a shared spectrum with a variety of applications and devices competing for bandwidth in enterprise environments. More than ever, IT managers need to have visibility into their wireless spectrum to manage RF interference and prevent unexpected downtime. Cisco CleanAir provides performance protection for 802.11n networks. This silicon-level intelligence creates a self-healing, self-optimizing wireless network that mitigates the impact of wireless interference. This release of Cisco SBA includes two Cisco CleanAir access points:

- Cisco Aironet 2600 Series Access Points with Cisco CleanAir technology create a self-healing, self-optimizing wireless network. By intelligently avoiding interference, they provide the high-performance 802.11n connectivity for mission-critical mobility and performance protection for reliable application delivery.
- Cisco Aironet 3600 Series Access Points with Cisco CleanAir technology deliver more coverage for tablets, smart phones, and highperformance laptops. This next-generation access point is a 4x4 MIMO, three-spatial-stream access point, resulting in up to three times more availability of 450 Mbps rates and performance optimization for more mobile devices.

For more information on Cisco CleanAir, please read the Cisco SBA— Borderless Networks Wireless LAN CleanAir Deployment Guide.

Design Models

Cisco Unified Wireless networks support two major design models: localmode and Cisco FlexConnect.

Local-Mode Design Model

In a local-mode design model, the wireless LAN controller and access points are co-located. The wireless LAN controller is connected to a LAN distribution layer at the site, and traffic between wireless LAN clients and the LAN is tunneled in Control and Provisioning of Wireless Access Points (CAPWAP) protocol between the controller and the access point.

Figure 2 - Local-mode design model



A local-mode architecture uses the controller as a single point for managing Layer 2 security and wireless network policies. It also enables services to be applied to wired and wireless traffic in a consistent and coordinated fashion.

In addition to providing the traditional benefits of a Cisco Unified Wireless Network approach, the local-mode design model meets the following customer demands:

- Seamless mobility—In a campus environment, it is crucial that users remain connected to their session even while walking between various floors or adjacent buildings with changing subnets. The local control-ler-based Cisco Unified Wireless network enables fast roaming across the campus.
- Ability to support rich media—As wireless has become the primary mode of network access in many campus environments, voice and video applications have grown in significance. The local-mode design model enhances robustness of voice with Call Admission Control (CAC) and multicast with Cisco VideoStream technology.
- Centralized policy—The consolidation of data at a single place in the network enables intelligent inspection through the use of firewalls, as well as application inspection, network access control, and policy enforcement. In addition, network policy servers enable correct classification of traffic from various device types and from different users and applications.

If any of the following are true at a site, you should deploy a controller locally at the site:

- The site has a LAN distribution layer.
- The site has more than 50 access points.
- The site has a WAN latency greater than 100 ms round-trip to a proposed shared controller.

In a deployment with these characteristics, use either a Cisco 2500 or 5500 Series Wireless LAN Controller. For resiliency, the design uses two wireless LAN controllers for the campus, although you can add more wireless LAN controllers in order to provide additional capacity and resiliency to this design.

Cisco FlexConnect Design Model

Cisco FlexConnect is a wireless solution for remote-site deployments. It enables organizations to configure and control remote-site access points from the headquarters through the WAN, without deploying a controller in each remote site.

Figure 3 - Cisco FlexConnect design model



If all of the following are true at a site, deploy Cisco FlexConnect at the site:

- The site LAN is a single access-layer switch or switch stack.
- The site has fewer than 50 access points.
- The site has a WAN latency less than 100 ms round-trip to the shared controller.

The Cisco FlexConnect access point can switch client data traffic out its local wired interface and can use 802.1Q trunking in order to segment multiple WLANs. The trunk native VLAN is used for all CAPWAP communication between the access point and the controller.

Cisco FlexConnect can also tunnel traffic back to the controller, which is specifically used for wireless guest access.

You can use a shared controller pair or a dedicated controller pair in order to deploy Cisco FlexConnect.

If you have an existing local-mode controller pair at the same site as your WAN aggregation, and if the controller pair has enough additional capacity to support the Cisco FlexConnect access points, you can use a shared deployment. In a shared deployment, the controller pair supports both local-mode and Cisco FlexConnect access points concurrently.

If you don't meet the requirements for a shared controller, you can deploy a dedicated controller pair by using Cisco 5500 Series Wireless LAN Controller, virtual wireless LAN controller, or Cisco Flex 7500 Series Cloud Controller. The controller should reside in and be connected to the server room or data center switches. For resiliency, the design uses two controllers for the remote sites, although you can add more controllers in order to provide additional capacity and resiliency to this design.

High Availability

As mobility continues to increase its influence in all aspects of our personal and professional lives, availability continues to be a top concern. The Cisco SBA design models continue to support high availability through the use of resilient controllers within a common mobility group.

With the advent of access point stateful switchover (AP SSO), the resiliency of the wireless network continues to improve. By adopting the cost effective AP SSO licensing model, Cisco wireless deployments can improve the availability of the wireless network with recovery times in the sub-second range during a WLC disruption. In addition, AP SSO allows the resilient WLC to be cost-effectively licensed as a standby controller with its access point (AP) license count being automatically inherited from its paired primary WLC.

Operational and policy benefits also improve as the configuration and software upgrades of the primary WLC are automatically synchronized to the resilient standby WLC. Support for AP SSO is available on Cisco 5500 Series Wireless LAN Controllers and on Cisco Flex 7500 Series Cloud Controllers.

Multicast Support

Video and voice applications are growing exponentially as smartphones, tablets, and PCs continue to be added to wireless networks in all aspects of our daily life. Multicast is required in order to enable the efficient delivery of certain one-to-many applications, such as video and push-to-talk group communications. By extending the support of multicast beyond that of the campus and data center, mobile users can now use multicast-based applications.

The Cisco SBA design modes now fully support multicast transmission for the onsite controller through the use of Multicast-Multicast mode. *Multicast-Multicast mode* uses a multicast IP address in order to communicate multicast streams to access points that have wireless users subscribing to a particular multicast group. Multicast-Multicast mode is supported on both the Cisco 2500 and 5500 Series Wireless LAN Controllers.

Remote sites that utilized the Cisco Flex 7500 Series Cloud Controller or vWLC using Cisco FlexConnect in local switching mode can also benefit from the use of multicast-based applications. Multicast in Cisco SBA remote sites leverages the underlying WAN and LAN support of multicast traffic. When combined with access points in FlexConnect mode using local switching, subscribers to multicast streams are serviced directly over the WAN or LAN network with no additional overhead being placed on the Wireless LAN Controller.

In all Cisco SBA wireless design models, the multicast support that users are accustomed to on a wired network is available wirelessly for those applications and user groups that require it.

Guest Wireless

Using the organization's existing WLAN for guest access provides a convenient, cost-effective way to offer Internet access for visitors and contractors. The wireless guest network provides the following functionality:

- Provides Internet access to guests through an open wireless Secure Set Identifier (SSID), with web access control.
- Supports the creation of temporary authentication credentials for each guest by an authorized internal user.
- Keeps traffic on the guest network separate from the internal network in order to prevent a guest from accessing internal network resources.
- · Supports both local-mode and Cisco FlexConnect design models.

Figure 4 - Cisco SBA wireless overview



You can use a shared controller pair or a dedicated controller in the Internet demilitarized zone (DMZ) in order to deploy a wireless guest network.

If you have one controller pair for the entire organization and that controller pair is connected to the same distribution switch as the Internet edge firewall, you can use a shared deployment. In a shared deployment, a VLAN is created on the distribution switch in order to logically connect guest traffic from the WLCs to the DMZ. The VLAN will not have an associated Layer 3 interface or switch virtual interface (SVI), and the wireless clients on the guest network will point to the Internet edge firewall as their default gateway.

If you don't meet the requirements for a shared deployment, you can use Cisco 5500 or 2500 Series Wireless LAN Controllers in order to deploy a dedicated guest controller. The controller is directly connected the Internet edge DMZ, and guest traffic from every other controller in the organization is tunneled to this controller.

In both the shared and dedicated guest wireless design models, the Internet edge firewall restricts access from the guest network. The guest network is only able to reach the Internet and the internal DHCP and DNS servers.

Notes

Deployment Details

This deployment guide uses certain standard design parameters and references various network infrastructure services that are not located within the wireless LAN (WLAN). These parameters are listed in the following table. In the "Site-specific values" column, enter the values that are specific to your organization.

Table 1 -	Universal	design	parameters
-----------	-----------	--------	------------

Network service	Cisco SBA values	Site-specific values
Domain name	cisco.local	
Active Directory, DNS server, DHCP server	10.4.48.10	
Network Time Protocol (NTP) server	10.4.48.17	
SNMP read-only community	cisco	
SNMP read-write community	cisco123	

Many organizations use the RADIUS protocol to authenticate users to both their wired and wireless networks. These access control systems (ACS) often integrate to a common local directory which contains specific information regarding the user. Common examples include an LDAP based user directory as well as Microsoft's Active Directory.

In addition to providing user authentication services, network components such as switches, wireless LAN controllers, routers, firewalls and so forth require administrative authentication and authorization when used by the network administrator to perform maintenance and configuration support.

In order to provide a customizable granular authorization list for network administrators as to the level of commands that they are permitted to execute, the TACACS+ (Terminal Access Control Access Control System) protocol is commonly used. Both TACACS+ and RADIUS protocols are available when deploying the Cisco Secure ACS solution.

If your organization has an existing Microsoft RADIUS server that is used to authenticate end user access for remote VPN, dial-up modem and so forth, it may be a good choice to deploy the wireless user authentication using the existing Microsoft RADIUS server. If however, your organization requires both TACACS+ for administrative access and RADIUS for wireless user authentication, the Cisco Secure ACS solution is the recommend choice. Cisco Secure ACS interfaces directly to an existing Microsoft Active Directory eliminating the need to define users in two separate authentication repositories.

If you don't require a comprehensive ACS system that spans the entire organization's management and user access, a simple RADIUS server can be used as an alternative to Cisco Secure ACS.

Process

Configuring the RADIUS Server: Cisco Secure ACS

- 1. Create the wireless device type group
- 2. Create the TACACS+ shell profile
- 3. Modify the device admin access policy
- 4. Create the network access policy
- 5. Modify the network access policy
- 6. Create the network device
- 7. Enable the default network device

For information about configuring the RADIUS server on Windows Server 2008, skip to the next process.

Cisco Secure Access Control System (ACS) is the centralized identity and access policy solution that ties together an organization's network access policy and identity strategy. Cisco Secure ACS operates as a centralized authentication, authorization, and accounting (AAA) server that combines user authentication, user and administrator access control, and policy control in a single solution.

Cisco Secure ACS 5.3 uses a rule-based policy model, which allows for security policies that grant access privileges based on many different attributes and conditions in addition to a user's identity.

This guide assumes that you have already configured Cisco Secure Access Control System (ACS). Only the procedures required to support the integration of wireless into the deployment are included. Full details on Cisco Secure ACS configuration are included in the Cisco SBA—Borderless Networks Device Management using ACS Deployment Guide.

Tech Tip

It has been found that certain browsers may render Cisco Secure ACS differently. In some cases, a browser may omit fields that are required for proper configuration. It is recommended that you refer to the following Secure ACS 5.3 release notes in order to obtain a list of supported browsers: http://www.cisco.com/en/US/ docs/net_mgmt/cisco_secure_access_control_system/5.3/release/ notes/acs_53_rn.html#wp222016

Procedure 1

Create the wireless device type group

Step 1: Navigate to the Cisco Secure ACS Administration Page. (Example: https://acs.cisco.local)

Step 2: In Network Resources > Network Device Groups > Device Type, click Create.

Step 3: In the Name box, enter a name for the group. (Example: WLC)

Step 4: In the Parent box, select All Device Types, and then click Submit.

Network Resources >	Network Device Groups > Devi	ice Type > Create		
Device Group Name: Description:	WLC			
	All Device Types		Select	
Required field	elds			
Submit Can	cel			

Procedure 2

Create the TACACS+ shell profile

You must create a shell profile for the WLCs that contains a custom attribute that assigns the user full administrative rights when the user logs in to the WLC.

Step 1: In Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles, click Create.

Step 2: On the General tab, In the **Name** box, enter a name for the wireless shell profile. (Example: WLC Shell)

Step 3: On the Custom Attributes tab, in the Attribute box, enter role1.

Step 4: In the Requirement list, choose Mandatory.

Step 5: In the Value box, enter ALL, and then click Add.

Step 6: In the Attribute Value drop down, select Static

Step 7: Click Submit.

eral Common Tasks mon Tasks Attributes		tration > Shell Profiles > Edit: "W	LC Shell*			
mon Tasks Attributes	Custom Attributes					
mon Tasks Attributes	Custom Attributes					
						- 1
					_	
pole	Requirement	Value			-	
					=	
					-	
ually Entered						
bute	Requirement	Value				
1	Mandatory	ALL			^	
					=	
					-	
dd A Edit V	Replace A Delete					
ute:						
uirement Mandatory 🖣	•					
]					
3.						
			-			
aquired fields						- 11
t Cancel						
	ibule ually Entered ubule s1 stdt A Edit V (suite uitement Mandatory • or equired fields	ibule Requirement ually Entered Ubule Requirement ibule Requirement ind A EditV (Replace A) Delete oute: uirement. Mandatory eequired fields	ibule Requirement Value ually Entered Usule Requirement Value I Mandatory ALL Mandatory ALL Usule State equired fields	ibule Requirement Value ually Entered Usule Requirement Value at Mandatory ALL define Edity Replace A Delete oute: uirement Mandatory +	ibule Requirement Value ualty Entered Usule Requirement Value at Mandatory ALL And A Edit V Replace A Delete oute: uirement Mandatory •	ibule Requirement Value ually Entered Ubule Requirement Value Ubule Requirement Value I Mandatory ALL U Edit V Replace A Delete Dute: urement Mandatory • urement Man

Procedure 3

Modify the device admin access policy

First, you must exclude WLCs from the existing authorization rule.

Step 1: In Access Policies > Default Device Admin > Authorization, click the Network Admin rule.

Step 2: Under Conditions, select NDG:Device Type, and in the filter list, choose not in.

Step 3: In the box to the right of the filter list, select All Device Types:WLC, and then click OK.

General Name: Network Admin	Status: Enabled		
The Custor	mize button in the lower	right area of the policy rules scree vailable here for use in policy rules	
Conditions			
Identity Group:	in •	 All Groups:Network Admins 	Select
NDG:Location:	-ANY-		
NDG:Device Type:	not in	 All Device Types:WLC 	Select
Time And Date:	-ANY-		
Results			
Shell Profile: Level 15		Select	
OK Cancel			Н

Next, you create a WLC authorization rule.

Step 4: In Access Policies > Default Device Admin > Authorization, click Create.

Step 5: In the **Name** box, enter a name for the WLC authorization rule. (Example: WLC Admin)

Step 6: Under Conditions, select Identity Group, and in the box, select All Groups:Network Admins.

Step 7: Select NDG:Device Type, and in the box, select All Device Types:WLC.

Step 8: In the Shell Profile box, select WLC Shell, and then click OK.

Step 9: Click Save Changes.

General			
Name: WLC Admin	Status:	Enabled 👻 \Theta	
		e lower right area of the policy rules s s are available here for use in policy	
Conditions			
Identity Group:	in	✓ All Groups:Network Admins	Select
NDG:Location:	-ANY-		
NDG:Device Type:	in	✓ All Device Types:WLC	Select
Time And Date:	-ANY-		
Results			
Shell Profile: WLC She	11	Select	
K Cancel			Help

Procedure 4

Create the network access policy

Step 1: In Access Policies > Access Services, click Create.

Step 2: In the Name box, enter a name for the policy. (Example: Wireless LAN)

Step 3: In the Based on Service Template box, select Network Access - Simple, and then click Next.

Access Policies > Access Services > Crea	ate						
General Allowed Protocols							
Step 1 - General							
General							
Name: Wireless LAN							
Description:							
Access Service Policy Structure							
Based on service template	Network A	Access - Simple	Select				
Based on existing service			Select				
O User Selected Service Type	Network A	Access 👻					
				Back	Next	Finish	Cancel

Step 4: On the Allowed Protocols pane, ensure Allow PEAP and Allow EAP-Fast are selected, and then click Finish.

Step 5: On the "Access Service created successfully. Would you like to modify the Service Selection policy to activate this service?" message, click **Yes**.

Step 6: On the Service Selection Rules pane, click Customize.

cisco Cisco Secure A	cs					acsadmin acs (Prin	
► S My Workspace	Access R	Policies	> Acces	s Services > Service Selectio	n Rules		
In the sources	O SI	nale n	esult sele	ection 💿 Rule based resi	ult selection		
With the second seco	Servi	ce Se	lection P	olicy			
Policy Elements	Filter	Staf	tus	▼ Match if: Eq	juals 👻	▼ Clear Filter Go ▼	
Access Policies Access Services			Status	Name	Protocol	Conditions Compound Condition	Results Service
Service Selection Rules O Default Device Admin	1	13		Remote Access VPN	match Radius	NDG:Device Type in All Device Types:ASA	Remote Access VPN
Default Network Access	2		0	Rule Wireless RADIUS	-ANY-	(RADIUS-IETF:Service-Type match Framed And RADIUS-IETF:NAS-Port-Type match Wireless - IEEE 802.11)	Wireless LAN
O Remote Access VPN O Wireless LAN	3		•	Rule-1	match Radius	-ANY-	Default Network Access
Identity	4		Θ	Rule-2	match Tacacs	-ANY-	Default Device Admin
Authorization Max User Session Policy Max Session User Settings Max Session Oroup Settings 							
Monitoring and Reports	- Louis	8	Default		If no rules defined	or no enabled rule matches.	DerwAccess
System Administration		ate		uplicate 🔹 (Edit) [Deli			Customize Hit Count
	Sav	re Cha	anges	Discard Changes			

Step 7: Using the arrow buttons, move Compound Condition from the Available list to the Selected list, and then click OK.

Customize Conditions Available:	Selected:	
ACS Host Name Device Filter Device IP Address Device Port Filter End Station Filter NDG:Device Type NDG:Location Time And Date UseCase	Protocol Compound Condition	
OK Cancel		

Step 8: On the Service Selection Rules pane, select the default RADIUS rule.

🕨 😚 My Workspace		ccess Policies > Access Services > Wireless LAN > Authorization									
Network Resources		Standa	nd Pol	icy <mark>Exce</mark>	eption Policy						
B Users and Identity Stores		Netw	ork Ac	cess Au	thorization Poli	cy					
Policy Elements Access Policies		Filte	r: Stat	us	¥ Ma	tch if: Equals	•	Clear Filter Go	▽		
Access Services Service Selection Rules	Â		V	Status	Name	NDG:Location	Condition Time And Date	NDG:Device Type	Results Authorization Profiles	Hit Count	
O Default Device Admin O Default Network Access O Remote Access VPN Wireless LAN		1	V	۲	WLC Access	-ANY-	-ANY-	in All Device Types:WLC	Permit Access	0	
Identity Authorization		**		Default		If no rules defin	ed or no enabled r	ule matches.	Permit Access	0	
Max User Session Policy Max Session User Settings Monitoring and Reports	•	Cre	ate	• D	uplicate 🔹 🤇	Edit) Delete	∧] Move to]	<u>×</u>	Custom	ize Hit Count	
System Administration	-1	8.00	ve Cha	naoc	Discard C	hangaa					

Next, you create a new rule for wireless client authentication.

Step 9: Click Create > Create Above.

Step 10: In the **Name** box, enter a name for the rule. (Example: Rule Wireless RADIUS)

- Step 11: Under Conditions, select Compound Condition.
- Step 12: In the Dictionary list, choose RADIUS-IETF.
- Step 13: In the Attribute box, select Service-Type.
- Step 14: In the Value box, select Framed, and then click Add V.
- Step 15: Under Current Condition Set, click And > Insert.
- Step 16: In the Attribute box, select NAS-Port-Type.
- Step 17: In the Value box, select Wireless IEEE 802.11, and then click Add V.

Step 18: Under Results, in the Service list, choose Wireless LAN, and then click OK.

General
Name: Rule Wireless RADIUS Status: Enabled 👻 \Theta
The Customize button in the lower right area of the policy rules screen controls which
policy conditions and results are available here for use in policy rules.
Conditions
Protocol: -ANY-
Compound Condition:
Condition:
Dictionary: Attribute:
RADIUS-IETF NAS-Port-Type Select
Operator: Value:
match
Select
Current Condition Set:
Add V Edit A Replace V
And
RADIUS-IETF:Service-Type match Framed
And >RADIUS-IETF:NAS-Port-Type match Wireless - IEEE 802.11
Or>•
Delete Preview
Results
Service: Wireless LAN

Step 19: On the Service Selection Rules pane, click Save Changes.

Procedure 5

Modify the network access policy

First, you must create an authorization rule that allows the WLCs to use RADIUS in order to authenticate clients.

Step 1: Navigate to Access Policies > Wireless LAN > Identity.

Step 2: In the Identity Source box, select AD then Local DB, and then click Save Changes.

Access Policies >	Access Services > Default Network Acces	ss > Identity		
Single result	It selection 🔘 Rule based result sele	ction		
Identity Source	AD then Local DB	Select		
	Advanced Options			
Save Changes	Discard Changes			

Step 3: Navigate to Access Policies > Wireless LAN > Authorization.

Step 4: On the Network Access Authorization Policy pane, click Customize.

Step 5: Using the arrow buttons, move NDG:Device Type from the Available list to the Selected list, and then click OK.

Step 6: In Access Policies > Wireless LAN > Authorization, click Create.

Step 7: In the Name box, enter a name for the rule. (Example: WLC Access)

Step 8: Under Conditions, select NDG:Device Type, and then in the box, select All DeviceTypes:WLC.

Step 9: In the Authorization Profiles box, select Permit Access, and then click OK.

General		
Name: WLC Access	Status: Enal	abled 👻 😌
		wer right area of the policy rules screen controls which
policy cond	litions and results are	re available here for use in policy rules.
Conditions		
NDG:Location:	-ANY-	
Time And Date:	-ANY-	Ť
NDG:Device Type:	in	✓ All Device Types:WLC Select
Identity Group:	-ANY-	
Results		
Authorization Profiles:		
Permit Access	<u> </u>	
		You may select multiple authorization profiles. Attributes defined in multiple profiles will use the value from the first
	=	profile defined.
	-	
Select Deselect		
Select Deselect		
OK Cancel		Не

Step 10: Click Save Changes.

Procedure 6

Create the network device

The TACACS+ shell profile that is required when managing the controllers with AAA must be applied to the controllers. This requires that for each controller and/or AP-SSO controller pair in the organization; you create a network device entry in Cisco Secure ACS.

If you are configuring a 2500 series WLC which does not support AP-SSO, you will need to include both of their IP addresses in this step to authorize them to use the ACS authentication services.

Step 1: In Network Resources > Network Devices and AAA Clients, click Create.

Step 2: In the Name box, enter the device host name. (Example: WLC-1)

Step 3: In the Device Type box, select All Device Types:WLC.

Step 4: In the **IP** box, enter the WLCs management interface IP address. (Example: 10.4.46.64)

Step 5: Select TACACS+.

Step 6: Enter the TACACS+ shared secret key. (Example: SecretKey)

Step 7: Select RADIUS.

Step 8: Enter the RADIUS shared secret key, and then click **Submit**. (Example SecretKey)



Procedure 7

Enable the default network device

Access points, when they are configured for Cisco FlexConnect operation and when the controller is unavailable, can authenticate wireless clients directly to Cisco Secure ACS. Enable the default network device for RADIUS in order to allow the access points to communicate with Secure ACS without having a network device entry.

Step 1: Navigate to Network Resources > Default Network Device.

Step 2: In the Default Network Device Status list, choose Enabled.

Next, you must show the RADIUS configuration.

Step 3: Under Authentication Options, click the arrow next to RADIUS.

Step 4: In the **Shared Secret** box, enter the secret key that is configured on the organization's access points, and then click **Submit**. (Example: SecretKey)

ne default device d 9 address.	enniuon can optionally be used in cases where he	o specific device definition is found that matches a device	
efault Network Dev	ice Status: Enabled 👻 \Theta		
etwork Device Gr	oups		
_ocation	All Locations	Select	
Device Type	All Device Types	Select	
uthentication Opt TACACS+	ons		
Shared Secret	Pagrati/au		
	nect Device		
	CACS+ Single Connect Support		
	Draft Compliant Single Connect Support		
RADIUS			
Shared Secret	SecretKey		
CoA port: 170	0		I
Enable Ke	eyWrap		
Key Encryptio	n Key:		
Message Auth	enticator Code Key:		
Key Input For	nat 🔿 ASCII 🔍 HEXADECIMAL		
= Required fields			

Process

Configuring the RADIUS Server: Windows Server 2008

- 1. Install services
- 2. Adding the Certification Authority snap-in
- 3. Certificate Enrollment Wizard

For information about configuring the RADIUS server on Cisco Secure ACS, use the previous process instead.

The following procedures describe the steps required in order to enable RADIUS authentication for the WLC deployment. In this guide, the Windows Server 2008 Enterprise Edition has already been installed.

Tech Tip

This procedure assumes that this is the first certificate authority (CA) in your environment. If it's not, you either don't need to install this role or you can configure this server as a subordinate CA instead.

Procedure 1

Install services

Step 1: Join the server to your existing domain (Example:cisco.local), and then restart.

Step 2: After the server restarts, open Server Manager.

Step 3: Navigate to Roles >Add Roles. The Add Roles Wizard opens.

Step 4: Follow the instructions in the wizard. Note the following:

On the Server Roles page, select Active Directory Certificate Services
 and Network Policy and Access Services.



- On the Role Services page, select Network Policy Server and Access Services, and then for Active Directory Certificate Services (AD CS), leave the default Certification Authority role service selected. You may not be able to select the Network Policy and Access Services option if it has already been installed previously.
- On the Setup Type page, for Active Directory Certificate Services, choose Enterprise.
- On the CA Type page, choose Root CA.

Follow the rest of the instructions in the wizard, making any changes you want or just leaving the default values as appropriate. Note that there is a warning at the end of the wizard, stating that the name of this server cannot be changed after installing the AD CS role.

Now that you have a root CA and an NPS server on your domain, you can configure the domain.

Procedure 2

Adding the Certification Authority snap-in

Step 1: Open an MMC console, and then click File > Add/Remove Snap-in.

Step 2: Choose Certificates from the available snap-ins.

				Selected snap-ins:	
nap-in	Vendor	-		Console Root	Edit Extensions
ActiveX Control	Microsoft Cor				Remove
Authorization Manager	Microsoft Cor				Komovo
Certificates	Microsoft Cor	=			
Component Services	Microsoft Cor				Move Up
Computer Managem	Microsoft Cor				
🖁 Device Manager	Microsoft Cor		id >		Move Down
Disk Management	Microsoft and		10 × DI		
Event Viewer	Microsoft Cor				
Folder	Microsoft Cor				
Group Policy Object	Microsoft Cor				
IP Security Monitor	Microsoft Cor				
IP Security Policy M	Microsoft Cor				
Link to Web Address	Microsoft Cor	-			Advanced
. <u>.</u>				L	
scription:					

Step 3: On the Certificates snap-in page, select **Computer account**, and then click **Next**.

Certificates snap-in			×
This snap-in will always manage certificates for:			
C My user account			
C Service account			
Computer account			
	< Back	Next >	Cancel

Step 4: On the Select Computer page, select Local computer, and then click Finish.

Select Computer	×
Select the computer you want this snap-in to manage.	
This snap-in will always manage:	
 Local computer: (the computer this console is running on) 	
C Another computer: Browse	
Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.	
< Back Finish Cance	

Next, add the Certification Authority snap-in.

Step 5: On the Add or Remove Snap-ins dialog box, in the **Available snapins** list, choose **Certification Authority**, click **Add** >, choose **Local computer** and then click **Finish**.

		_	Selected snap-ins:	
	Vendor	<u> </u>	Console Root	Edit Extensions
Active Directory Do	Microsoft Cor		Certificate Templates	
Active Directory Site	Microsoft Cor		Certificates (Local Computer)	Remove
Active Directory Use	Microsoft Cor		Certification Authority (Local)	
ActiveX Control	Microsoft Cor			Move Up
ADSI Edit	Microsoft Cor			
Authorization Manager	Microsoft Cor			Move Down
Certificate Templates	Microsoft Cor	Add >		
Certificates	Microsoft Cor			
Certification Authority	Microsoft Cor			
Component Services	Microsoft Cor			
Computer Managem	Microsoft Cor			
Device Manager	Microsoft Cor			
DHCP	Microsoft Cor			• d
Disk Management	Microsoft and	•		Advanced
cription:				
cripcion;				

Step 6: On the Add or Remove Snap-ins dialog box, choose **Certificate Templates** in the available snap-ins list which will add the RAS/IAS template.

Step 7: Click Ok to complete the process of adding snap-ins.

Step 8: Expand Certificates (Local Computers) > Personal, right-click Certificates, and then click Request new certificate.



Procedure 3

Certificate Enrollment Wizard

Step 1: Follow the instructions in Certificate Enrollment wizard. Click **Next** to advance past the Before You Begin introductory page. Select **Active Directory Enrollment Policy** as the Enrollment policy for this certificate request.



Step 2: Select Domain Controller and Domain Controller Authentication as the type of certificates that are being requested, and then click **Enroll**.

Console1 - [Console Root\Certificates (Loc					_ 🗆
File Action View Favorites Window H	telp				
🗢 🔿 📶 🔲 🚨 🖬 🔟					
	Dijert Type		- O ×	Actions	
Certificates (Local Computer) Personal				Personal	_
🗉 🎬 Trusted Root Certification Authorities	Certificate Enrollment			More Actions	
Enterprise Trust Trust Intermediate Certification Authorities				Certificates	
🗉 🧮 Trusted Publishers	Request Certificates			More Actions	
	You can request the following types of certifi	cates. Select the certificates you want to request,	and then click Enroll.		
Trusted People Remote Desktop	Active Directory Enrollment Pol	icy		1	
Certificate Enrolment Requests Smart Card Trusted Roots	Directory Email Replication	🗘 STATUS: Available	Details 🛞		
Trusted Devices Gertification Authority (Local)	Domain Controller	(i) STATUS: Available	Details 🛞		
🗉 🗟 Certificate Templates	Domain Controller Authentication	🗘 STATUS: Available	Details 🛞		
	IPSec (Offline request)	📣 STATUS: Available	Details 🛞		
	A More information is required to e	nroll for this certificate. Click here to configure sett	ings.	1	
	Web Server	(i) STATUS: Available	Details 🛞	1	
	A More information is required to e	nroll for this certificate. Click here to configure sett	ings.		
	Show all templates				
	Learn more about <u>certificates</u>				
		[Enrol Cancel		
· · ·				1	
Personal store contains 6 certificates.					

Step 3: Once the Certificate request has been completed successfully, select **Finish**.

🚟 Console1 - [Console Root\Certificates (Lo						_ 🗆 ×
🚟 File Action View Favorites Window	Help					_ 6 ×
🗢 🔿 🙇 📅 📋 💁 🛃 📷						
Console Root	Object Tune			1	Actions	
Certificates (Local Computer) Personal	📫 🤇 🛄 Cer	tificate Enrollment			Personal	-
Personal Trusted Root Certification Authorities Enterprise Trust	📮 Cer	tificate Enrollment			More Actions	•
Citerprise indec Intermediate Certification Authorities Trusted Publishers		Certificate Installation Results			Certificates	*
Christel Packers Certificates Certification Authorit Trusted People		The following certificates have been enrolled a	nd installed on this computer.		More Actions	•
Trusted People Tested People Tested People Tested People		Active Directory Enrollment Polic	v			
Certificate Enrolment Requests Smart Card Trusted Roots		Domain Controller	🖌 STATUS: Succeeded	Details 🛞		
Trusted Devices Trusted Devices Certificate Templates Certificate Templates		III Doman Controler Authentication	✓ STATUG: Succeeded	Detals®		
()				Finish		
Personal store contains 6 certificates.						

Step 4: Navigate to **Certificate Authority (Local)** > **Issued Certificates**, and then verify that the Certificate Templates folder appears.

File Action View Help					
Certification Authority (Local)	Request ID	Requester Name CISCO\ADY\$	Binary Certificate	Certificate Template Domain Controller Authentication (1.3.6.1.4	Se 57
Revoked Certificates Issued Certificates Issued Certificates Pending Requests Failed Requests Certificate Templates	i⊒]3	CISCO (ADY\$		Domain Controller (DomainController)	57
			ŀ\$		

Step 5: Right click on the **Certificate Templates** folder, and in the right pane, right-click **RAS and IAS Server**, and then click **Duplicate Template**.

Recentificate Templates (Directory Email Replication	Windows Server 2003 Ent	115	Certificate Templat 🔺
	Real Domain Controller	Windows 2000	4.1	More Actions
	Domain Controller Authentication	Windows Server 2003 Ent	110	More Actions
	EFS Recovery Agent	Windows 2000	6.1	RAS and IAS Server
	🚇 Enrollment Agent	Windows 2000	4.1	
	🖳 Enrollment Agent (Computer)	Windows 2000	5.1	More Actions
	Rechange Enrollment Agent (Offline request)	Windows 2000	4.1	
	Real Exchange Signature Only	Windows 2000	6.1	
	🗷 Exchange User	Windows 2000	7.1	
	🗷 IPSec	Windows 2000	8.1	
	🚇 IPSec (Offline request)	Windows 2000	7.1	
	Rerberos Authentication	Windows Server 2003 Ent	110	
	Rey Recovery Agent	Windows Server 2003 Ent	105	
	Response Signing	Windows Server 2008 Ent	101	
	RAS and TAC Comment	Windows Server 2003 Ent	101	
	Root Ce Duplicate Template	Windows 2000	5.1	
	Reenroll ANCertificate Holders	Windows 2000	4.1	
	R Smartca All Tasks	Windows 2000	6.1	
	🗟 Smartca	Windows 2000	11.	
	Subordi Properties	Windows 2000	5.1	
	R Trust Li Help	Windows 2000	3.1	
	R User	Windows 2000	3.1	
	🚇 User Signature Only	Windows 2000	4.1	
	•			

Step 6: Select Windows Server 2008 Enterprise, and then click OK.



Step 7: In the **Template display name** box, enter a valid display name, select **Publish Certificate in Active Directory**, click **Apply**, and then close the MMC console.

operties	of New Templa	ite		
Issuance	Requirements	Superseded Tem	plates Extensio	ns Security
General	Request Hand	ling Cryptograp	hy Subject Na	me Server
Template	display name:			
Copy of	RAS and IAS Ser	ver for NPS		
Minimum	Supported CAs:	Windows Server:	2008 Enterprise	
Template				
_	ASandIASServer	forNPS		
leopyon	7.501101715561761	iona o		
Validity p	eriod:	Renewa	l period:	
	years 💌	6	weeks 💌	
		N		
	sh certificate in A	6		
_				
	o not automaticai irectory	ly reenroll if a dupli	cate certificate ex	ists in Active
For a	utomatic renewal ew kev cannot be	of smart card certi	ficates, use the ex	disting key
1 4 1 6	w key cannot be	Ciealeu		
		1		
	OK	Cancel	Apply	Help

Step 8: Open the Network Policy Server administrative console by navigating to Start > Administrative Tools > Network Policy Server.

Step 9: Right-click the parent node NPS (Local), click Register server in Active Directory, click OK to authorize this computer to read users' dial-in properties from the domain, and then click OK again.

File Action	View Help				
😓 🔿 🛛 🚾 🛛	?				
NPS (Local)		PS (Local)			
	Import Configuration Export Configuration		rted		
. E Solution → Networ → Networ → Network . Accoun . Accoun . Accoun . Accoun	Start NPS Service Stop NPS Service Register server in Act		olicy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection utherritication, and connection request authorization.		
	Properties	ive birectory	nfiguration		
	View +		ation scenario from the list and then click the link below to open the scenario wizard.		
	Help		iration scenario from the list and then click the link below to open the scenario wizard.		
		Network Ac When you con NAP-capable c	ss Protection (NAP) cess Protection (NAP) igue NFS as a NAP health policy server, you create health policies that allow NPS to validate the configuration of lient computer solarion that are not compliant with health policy can be placed on a crk and automatically updated to bring them into compliance. NAP Learn more		
		Advanced C Templates	onfiguration 🗸		
		Templates	Configuration		

Step 10: With the NPS (Local) node still selected, select RADIUS server for 802.1X Wireless or Wired Connections, and then click Configure 802.1X.

Network Policy Server	
File Action View Help	
🗇 🔿 🖬	
NPS (Loca) RADUS Clients and Servers Solution Accounting Accounting Templates Management	NPS (Local) Getting Started
	Standard Configuration Select a configuration scenario from the list and then click the link below to open the scenario wizard.
	RADIUS server for 802 1X Wieless or Wied Connections Network Access Protection (NAP) BABILIS server for 802 1X Wieless or Wied Connections RADIUS server for 802 NV Network Access prints and authenticating switches (also called RADIUS clients).
	Configure 802.1X Learn more
	Advanced Configuration
	Templates Configuration
]

Step 11: In the Configure 802.1X wizard, under Type of 802.1X connections, select **Secure Wireless Connections**, and in the **Name** box, enter an appropriate name for the policies that you want to create, and then click **Next**.

NPS (Local)	
Getting Started	
Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request authorization.	
Standard Configuration	
Select a configuration scenario from the list and then click the link below to open the scenario wizard.	
RADIUS server for 802.1X Wireless or Wired Connections	
BADILLE converter 902-1X litical convertions	
Select 802.1X Connections Type	
Type of 802.1X connections: Secure Wireless Connections When you deploy 802.1X wireless access points on your network, NPS can authenticate and authorize connection requests made by wireless clients connecting through the access points. Secure Wirel (Ethernet) Connections When you deploy 802.1X authenticating switches on your network, NPS can authenticate and authorize connection requests made by Ethernet clients connecting through the switches. Mame: This default text is used as part of the name for each of the policies created with this wizard. You can use the Mature text is used as part of the name for each of the policies created with this wizard. You can use the Mature text is used as part of the name for each of the policies created with this wizard. You can use the Mature text is used as part of the name for each of the policies created with this wizard. You can use the Mature text is used as part of the name for each of the policies created with this wizard. 	
default text or modify it .	
	: CAs i
Previous Next Finish Cancel	

Step 12: Add each of the wireless LAN controllers as RADIUS clients. Click **Add** and in the **Friendly name** box, enter a name for the controller (for example, WLC5508), provide the IP address or DNS entry for SBAthe controller. Provide the Shared Secret (Example SecretKey) and then click **OK**.

ttings		
Select an existing to	emplate:	
		V
Name and Address — Friendly name:		
WLC5508		
Address (IP or DNS):		
10.4.46.64		Verify
Shared Secret Select an existing Sha None	ared Secrets template:	
secret, click Generate	ared secret, click Manual. To autor . You must configure the RADIUS hared secrets are case-sensitive.	matically generate a shared client with the same shared
secret, click Generate secret entered here. S	. You must configure the RADIUS	matically generate a shared client with the same shared
secret, click Generate secret entered here. S • Manual	 You must configure the RADIUS ihared secrets are case-sensitive. 	matically generate a shared client with the same shared
secret, click Generate secret entered here. S • Manual	 You must configure the RADIUS ihared secrets are case-sensitive. 	matically generate a shared client with the same shared
secret, click Generate secret entered here. S Manual Shared secret:	e: You must configure the RADIUS ihared secrets are case-sensitive. Generate	natically generate a shared client with the same shared
secret, click Generate secret entered here. S • Manual Shared secret:	e: You must configure the RADIUS ihared secrets are case-sensitive. Generate	matically generate a shared client with the same shared

Step 13: Click Next.

Step 14: On the Configure an Authentication Method page, in the Type box, select Microsoft: Protected EAP (PEAP), and then click Configure.

Configure 802.	1X					
	Configur	e an Au	thentica	tion Meth	od	
Select the EAP	type for this polic	y.				
Type (based	on method of	access and	network ca	nfiguration):		
Microsoft: Prote	ected EAP (PEA	P)			•	Configure
					ß	
			Previous	Next	Finish	Cancel
		_				

Step 15: In the **Certificate issued** list, ensure that the certificate you enrolled in Step 5 is selected, and then click **OK**.

dit Protected EAP Pro	perties	×
	e server should use to prove its ident igured for Protected EAP in Connecti :ertificate.	
Certificate issued	AD.cisco.local	_
Friendly name:		
Issuer:	AD.cisco.local	
Expiration date:	3/15/2016 2:26:19 PM	
 Enable Fast Reconne Disconnect Clients wi Eap Types 		
Secured password (EAP	-MSCHAP v2)	Move Up
		Move Down
· · · ·	dit Remove OK	

Step 16: If you would like to use a group that you have already created, in Specify User Groups, click **Add**, select the desired group, and then skip to Step 18.

If you would like to create a new group, continue with this procedure.

Step 17: Navigate to Start > Administrative Tools > Active Directory Users and Computers. In the Active Directory Users and Computers window, right-click **cisco.local**, and then navigate to **New** > **Group**. Create a group called **SBA-Users**.

	1 8	<u>k 🖬 🔻 </u> 8	8	
Active Directory Users and Comput Saved Queries Interpret Control Change Domain Controller Change Domain Controller Poperations Masters Properties Help	Comp Secur d Ser Comp Conta Group InetC mSMC Organ Printe User	Container Container Container container uuter act brgPerson aging-PSPs 2 Queue Alias inzational Unit	Description Default container for upgr Default container for secu Default container for secu Default container for man Default container for upgr]

Step 18: Create a user named **WirelessUser**, and then add it to the group created in the previous step.

BA-Users Properties	5	? >
General Members	Member Of Managed By	
Members:		
Name	Active Directory Domain Services Folder	
💄 Wireless User		
Add	Remove	
Add	nemove	

Step 19: Click **Next**, and then click **Add**. This enables use of an Active Directory group in order to help secure your wireless network

Tech Tip

It is recommended that you add both the machine accounts and user accounts to this group in order to allow the machine to authenticate before the user logs in).

Select Group	<u>? ×</u>
Select this object type:	
Group	Object Types
From this location:	
cisco.local	Locations
Enter the object name to select (<u>examples</u>):	
SBA-Users	Check Names
1	
Advanced OK	Cancel

Step 20: On the next step of the wizard, configure VLAN information or accept the default settings, and then click **Next**.

Step 21: Click Finish. This completes the configuration of 802.1X.

Configure 802.	LX				×
		New IEEE 802. Inections and I			nd
You have succe	essfully created the follo	wing policies and config	ured the followin	ng RADIUS clien	ts.
 To change the 	onfiguration details in yo e configuration, click Pre onfiguration and close th		Configuration D)etails.	
Connection F	equest Policy:				
Network Polic Secure Wireless	xies:				
Configuration De	<u>itails</u>				

Step 22: Restart the Network Policy Server service, and then navigate to NPS (Local) > Policies.

Note that the wizard has created a Connection Request Policy and a Network Policy containing the appropriate settings in order to authenticate your wireless connection.

🞭 Network Policy Server					
File Action View Help					
🗢 🔿 🖄 📅 🚺					
NPS (Local) RADIUS Clients and Servers ADIUS Clients RADIUS Clients Remote RADIUS Server G Policies	Network Policies Network policies allow you to designate who is authorized to under which they can or cannot connect.	o connect i	to the network and t	he circumstance	95
Connection Request Polici	Policy Name	Status	Processing Order	Access Type	S
Health Policies	Secure Wireless Connections	Enabled	1	Grant Access	U
Network Access Protection	Connections to Microsoft Routing and Remote Access server	Enabled	<u>aaaaaa</u>	Deny Access	U
Accounting	Connections to other access servers	Enabled	1000000	Deny Access	U
Templates Management					
	o Secure Wireless Connections				
	Conditions - If the following conditions are met:				
	Condition Value				
	NAS Port Type Wireless - Other OR Wireless - IEEE 802.11				
	Windows Groups CISCO\SBA-Users				
	Settings - Then the following settings are applied:				
	Setting Value				-
	Extensible Authentication Protocol Configuration Configured				
	•				-

Step 23: If you want to remove the less secure authentication methods and increase the encryption methods in the network policy, continue with this procedure.

If you would like to use the default authentication and encryption methods, skip to the next process.

Step 24: Under the Network Policies node, open the properties of the newly created policy.

Step 25: On the Constraints tab, under Less secure authentication methods, clear all of the check boxes.

onstraints:	<u></u>
Constraints Authentication Methods	Allow access only to those clients that authenticate with the specified methods.
Marken State S	EAP types are negotiated between NPS and the client in the order in which they are listed. EAP Types:
Day and time restrictions NAS Port Type	Microsoft: Protected EAP (PEAP)
	Add E.dt Remove
	Morosoft Encrypted Authentication version 2 (MS-CHAP-v2) Use can change password alter it has expired Morosoft Encrypted Authentication (MS-CHAP)
	User can change password after it has expired
	Encrypted authentication (CHAP) Unencrypted authentication (PAP, SPAP)
	Allow clients to connect without negotiating an authentication method Perform machine health check only

Step 26: On the Settings tab, click **Encryption**, clear all check boxes except **Strongest encryption (MPPE 128-bit)**, and then click **OK**.

verview Conditions Constraints Setti	ngs
Configure the settings for this network polic conditions and constraints match the co	 inection request and the policy grants access, settings are applied.
Settings:	
RADIUS Attributes Standard	The encryption settings are supported by computers running Microsoft Routing and Remote Access Service.
Vendor Specific Network Access Protection	If you use different network access servers for dial-up or VPN connections, ensure that the encryptions settings you select are supported by your servers.
NAP Enforcement	If No encryption is the only option selected, traffic from access clients to the network access server is not secured by encryption. This configuration is not recommended.
Routing and Remote Access	
Allocation Protocol (BAP)	Basic encryption (MPPE 40-bit) Strong encryption (MPPE 56-bit)
Encryption	Strongest encryption (MPPE 128-bit) No encryption
	OK Cancel App

Step 27: Restart the Network Policy Server service.

Process

Configuring On-Site Wireless Controllers

- 1. Configure the switch for the WLC
- 2. Connecting the redundancy port
- 3. Configure the WLC platform
- 4. Configure the time zone
- 5. Configure SNMP
- 6. Limit which networks can manage the WLC
- 7. Configure wireless user authentication
- 8. Configure management authentication
- 9. Enable multicast support
- 10. Create the WLAN data interface
- 11. Create the wireless LAN voice interface
- 12. Configure the data wireless LAN
- 13. Configure the voice wireless LAN
- 14. Configure the resilient controller
- 15. Configure controller discovery
- 16.Connect the access points
- 17. Configure access points for resiliency

In an on-site local-mode deployment, the wireless LAN controller and access points are co-located. The wireless LAN controller is connected to a LAN distribution layer at the site, and traffic between wireless LAN clients and the LAN is tunneled in Control and Provisioning of Wireless Access Points (CAPWAP) protocol between the controller and the access point.

If you are deploying remote access points using FlexConnect, skip this section and proceed to the FlexConnect section of the guide.

This deployment guide supports both Cisco 5500 and 2500 Series WLCs for use in an on-site local-mode design. When installing 5500 Series WLCs, a high availability feature known as access point stateful switchover (AP SSO) is available. In this high availability mode, the resilient, or *secondary*, WLC uses the redundancy port in order to negotiate with its configured primary WLC and assumes the AP license count along with the configuration of the primary WLC.

In AP SSO mode, configuration synchronization and keep-alive monitoring occurs over a dedicated redundancy port (labeled as RP) using a dedicated straight through Ethernet cable.

The Cisco 2500 Series WLCs do not support the AP SSO feature and instead must be peered by using a mobility group in order to achieve resiliency. Unlike AP-SSO paired Wireless LAN Controllers, each Cisco 2500 Series WLC has a unique IP address on the management interface.

Table 2 - Cisco on-site wireless controller parameters checklist

Parameter	Cisco SBA values primary controller	Cisco SBA values resilient controller (optional)	Site-specific values
Controller parameters			
Switch interface number	1/0/3, 2/0/3	1/0/4, 2/0/4	
VLAN number	146	146	
Time zone	PST -8 0	PST -8 0	
IP address	10.4.46.64/24	10.4.46.65/242	
Default gateway	10.4.46.1	10.4.46.1	
Redundant management IP address (AP SSO) ¹	10.4.46.741	10.4.46.751	
Redundancy port connectivity (AP SSO) ¹	Dedicated Ethernet cable ¹	Dedicated Ethernet cable ¹	
Hostname	WLC-1	WLC-2 ²	
Local administrator username and password	admin/C1sco123	admin/C1sco123	
Mobility group name	CAMPUS	CAMPUS	
RADIUS server IP address	10.4.48.15	10.4.48.15	
RADIUS shared key	SecretKey	SecretKey	
Management network (optional)	10.4.48.0/24	10.4.48.0/24	
TACACS server IP address (optional)	10.4.48.15	10.4.48.15	
TACACS shared key (optional)	SecretKey	SecretKey	
Wireless data network parameters			
SSID	WLAN-Data	WLAN-Data	
VLAN number	116	116	
Default gateway	10.4.16.1	10.4.16.1	
Controller interface IP address	10.4.16.5/22	10.4.16.6/22	
Wireless voice network parameters			
SSID	WLAN-Voice	WLAN-Voice	
VLAN number	120	120	
Default gateway	10.4.20.1	10.4.20.1	
Controller interface IP address	10.4.20.5/22	10.4.20.6/22	

Notes:

1. AP SSO is only supported on the Cisco 5500 Series WLC.

2. The resilient Cisco 2500 Series WLC will require an IP address, as AP SSO is not supported on this platform.

```
Procedure 1
```

Step 1: On the LAN distribution switch, create the wireless VLANs that you are connecting to the distribution switch. The management VLAN can contain other Cisco appliances and does not have to be dedicated to the WLCs.

vlan 116 name WLAN_Data vlan 120 name WLAN_Voice vlan 146 name WLAN Mgmt

Step 2: Configure a switched virtual interface (SVI) for each VLAN. This enables devices in the VLAN to communicate with the rest of the network.

interface Vlan116 description Wireless Data Network ip address 10.4.16.1 255.255.252.0 no shutdown ! interface Vlan120 description Wireless Voice Network ip address 10.4.20.1 255.255.252.0 no shutdown ! interface Vlan146 description Wireless Management Network ip address 10.4.46.1 255.255.255.0 no shutdown

Step 3: On both the server room distribution and access switches, create the wireless management and data VLAN's.

vlan 116 name WLAN_Data vlan 120 name WLAN_Voice vlan 146 name WLAN_Mgmt **Step 4:** On the server room distribution switch, configure two uplink ports and an EtherChannel trunk to the server room access switches.

interface Port-channel12
description EtherChannel Link to Server Room Switch
switchport
switchport trunk allowed vlan 116,120,146
switchport mode trunk
logging event link-status
flowcontrol receive on
no shutdown

interface range tenGigabitEthernet [port 1],tenGigabitEthernet

[port 2]

description Link to Server Room Switch
switchport trunk allowed vlan 116,120,146
switchport mode trunk
channel group 12
logging event link-status
logging event trunk-status
no shutdown

Step 5: On the server room access switches, configure two ports and an EtherChannel trunk that connects to the server room distribution switch.

interface range GigabitEthernet1/1/1, GigabitEthernet2/1/1
description Link to Distribution Switch
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 116,120,146
switchport mode trunk
logging event link-status
logging event trunk-status
logging event bundle-status
macro apply EgressQoS
channel-protocol lacp
channel-group 1 mode active
no shutdown

interface Port-channel1
 description EtherChannel Link to Distribution Switch

switchport trunk encapsulation dot1q
switchport trunk allowed vlan 116,120,146
switchport mode trunk
logging event link-status
no shutdown

Step 6: Configure an 802.1Q trunk to be used for the connection to the WLCs. This permits Layer 3 services to all the networks defined on the WLC. The VLANs allowed on the trunk are limited to only the VLANs that are active on the WLC.

If you are deploying the Cisco Catalyst 4500 Series LAN distribution switch, you do not need to use the **switchport trunk encapsulation dot1q** command in the following configurations.

```
interface GigabitEthernet [port 1]
description To WLC Port 1
interface GigabitEthernet [port 2]
description To WLC Port 2
1
interface range GigabitEthernet [port 1], GigabitEthernet
[port 2]
  switchport
 macro apply EgressQoS
  channel-group [number] mode on
  logging event link-status
  logging event trunk-status
  logging event bundle-status
interface Port-channel [number]
description To WLC
 switchport trunk encapsulation dotlq
 switchport trunk allowed vlan 116,120,146
 switchport mode trunk
 logging event link-status
 no shutdown
```

Procedure 2

Connecting the redundancy port

If you are using a Cisco 2500 Series WLC, skip this procedure. If you are using a Cisco 5500 Series WLC and you wish to enable the high availability AP SSO feature, continue with this procedure. When using the high availability feature known as access point stateful switchover (AP SSO), a dedicated special-purpose port is available on the Cisco 5500 Series WLC. This port is located on the in the lower left of the front panel.

Step 1: Connect an ordinary Ethernet cable between the primary and standby WLC, as shown below.



Procedure 3

Configure the WLC platform

After the WLC is physically installed and powered up, you will see the following on the console. If you do not see this, press "-" a few times to force the wizard to back up to the previous step.

Welcome to the Cisco Wizard Configuration Tool

Use the '-' character to backup

Would you like to terminate autoinstall? [yes]: YES

Step 1: Enter a system name. (Example: WLC-1)

System Name [Cisco_7e:8e:43] (31 characters max): WLC-1

Step 2: Enter an administrator username and password.

Tech Tip

Use at least three of the following four classes in the password: lowercase letters, uppercase letters, digits, or special characters.

Enter Administrative User Name (24 characters max): **admin** Enter Administrative Password (24 characters max): ***** Re-enter Administrative Password : *****

Step 3: If you are deploying a Cisco 5500 Series Wireless LAN Controller, use DHCP for the service port interface address.

Service Interface IP address Configuration [none] [DHCP]: DHCP

Step 4: Enable the management interface.

Enable Link Aggregation (LAG) [yes][NO]: **YES** Management Interface IP Address: **10.4.46.64** Management Interface Netmask: **255.255.0** Management interface Default Router: **10.4.46.1** Management Interface VLAN Identifier (0 = untagged): **146**

Tech Tip

If you are configuring the 2500 series Wireless LAN Controllers, you will need to configure both WLC's individually as they do not support AP-SSO and are therefore managed and configured separately. (Example: 10.4.46.64 for WLC-1 and 10.4.46.65 for WLC-2)

Step 5: Enter the default DHCP server for clients. (Example: 10.4.48.10)

Management Interface DHCP Server IP Address: 10.4.48.10

Step 6: If you are deploying a Cisco 5500 Series Wireless LAN Controller enable AP SSO to enable high availability.

Enable HA [yes][NO]: YES Configure HA Unit [PRIMARY][secondary]: PRIMARY

Redundancy Management IP Address: 10.4.46.74 Peer Redundancy Management IP Address: 10.4.46.75

Step 7: The virtual interface is used by the WLC for mobility DHCP relay, guest web authentication and intercontroller communication. Enter an IP address that is not used in your organization's network. (Example: 192.0.2.1)

Virtual Gateway IP Address: 192.0.2.1

Step 8: If you are configuring a Cisco 2500 Series Wireless LAN Controller, enter a multicast address for delivery of IP multicast traffic by using the multicast-multicast method. This multicast address will be used by each AP in order to listen for incoming multicast streams from the wireless LAN controller. (Example: 239.1.1.1)

Multicast IP Address: 239.1.1.1

Step 9: Enter a name for the default mobility and RF group. (Example: CAMPUS)

Mobility/RF Group Name: CAMPUS

Step 10: Enter an SSID for the WLAN that supports data traffic. You will be able to leverage this later in the deployment process.

Network Name (SSID): WLAN-Data Configure DHCP Bridging Mode [yes][NO]: NO

Step 11: Enable DHCP snooping.

Allow Static IP Addresses {YES][no]: NO

Step 12: Do not configure the RADIUS server now. You will configure the RADIUS server later by using the GUI.

Configure a RADIUS Server now? [YES][no]: NO

Step 13: Enter the correct country code for the country where you are deploying the WLC.

Enter Country Code list (enter 'help' for a list of countries)
[US]: US

Step 14: Enable all wireless networks.

Enable 802.11b network [YES][no]: **YES** Enable 802.11a network [YES][no]: **YES** Enable 802.11g network [YES][no]: **YES** **Step 15:** Enable the radio resource management (RRM) auto-RF feature. This helps you keep your network up and operational.

Enable Auto-RF [YES][no]: YES

Step 16: Synchronize the WLC clock to your organization's NTP server.

Configure a NTP server now? [YES][no]:YES Enter the NTP server's IP address: 10.4.48.17 Enter a polling interval between 3600 and 604800 secs: 86400

Step 17: Save the configuration. If you respond with **no**, the system restarts without saving the configuration, and you have to complete this procedure again. Please wait for the "Configuration saved!" message before power-cycling the Wireless LAN Controller.

Configuration correct? If yes, system will save it and reset. [yes][NO]: YES Configuration saved! Resetting system with new configuration

Step 18: After the WLC has reset, log in to the Cisco Wireless LAN Controller Administration page by using the credentials defined in Step 2. (Example: https://wlc-1.cisco.local/)



Configure the time zone

Step 1: Navigate to Commands > Set Time.

Step 2: In the **Location** list, choose the time zone that corresponds to the location of the WLC.

Step 3: Click Set Timezone.

ululu cisco	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>s</u> ecurity	MANAGEMENT		nfiguration HE <u>L</u> P	<u>P</u> ing Logout <u>F</u> EEDBACK	<u>R</u> efresh
Commands Download File	Set Time						Set	Date and 1	Fime Set Tim	iezone
Upload File Reboot	Current T Date	ime	Tue May 31 11:07	7:38 2011						
Config Boot Scheduled Reboot 			Month Day		May 31 👻	•				
Reset to Factory Default Set Time			Year		2011					
Login Banner	Time		Hour		11 -					
			Minutes Seconds		7 38					
	Timezone									
			Delta Location ¹		hours 0 -8:00) Pacific	mins 0 Time (US and Cana	da) 👻			
	Foot Note									
	1. Automatic	ally sets d	aylight savings tim	e where used.						

Procedure 5 Configure SNMP

- Step 1: In Management > SNMP > Communities, click New.
- Step 2: Enter the Community Name. (Example: cisco)
- Step 3: Enter the IP Address. (Example: 10.4.48.0)
- Step 4: Enter the IP Mask. (Example: 255.255.255.0)
- Step 5: In the Status list, choose Enable, and then click Apply.

cisco	MONITOR	WLANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	Sa <u>v</u> e Cor C <u>O</u> MMANDS	nfiguration Ping Lo HELP <u>F</u> EEDBACK	gout <u>R</u> efresh
Management	SNMP v1	/ v2c Co	ommunity > N	ew				< Back	Apply
Summary SIMP General SIMP V3 Users Communities Trap Deceivers Trap Controls Trap Logs HTTP-HTTPS Telnet-SSH Serial Port Local Management Users User Sessions Logs Mgmt Via Wireless Software Activation Tech Support	Communi IP Addres IP Mask Access M Status	55	cisco 10.4.48.0 225.255.255.255.0 Read Only v Enable v						

- Step 6: In Management > SNMP > Communities, click New.
- Step 7: Enter the Community Name. (Example: cisco123)
- Step 8: Enter the IP Address. (Example: 10.4.48.0)
- Step 9: Enter the IP Mask. (Example: 255.255.255.0)
- Step 10: In the Access Mode list, choose Read/Write.

Step 11: In the Status list, choose Enable, and then click Apply.

սիսիս									
cisco	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP <u>F</u> EEDBACI	<
Management	SNMP v1	/ v2c Co	ommunity > N	ew				< Back	Apply
Summary SNMP General SNMP V3 Users Communities Trap Receivers Trap Controls	Communi IP Addres IP Mask Access M Status	s	cisco123 10.4.48.0 255.255.255.0 Read/Write • Enable •						
Trap Logs HTTP-HTTPS									
Telnet-SSH Serial Port									
Local Management Users									
User Sessions Logs									
Mgmt Via Wireless Software Activation 									
Tech Support									

Step 12: Navigate to Management > SNMP > Communities.

Step 13: Point to the blue box for the **public** community, and then click **Remove**.

Step 14: On the "Are you sure you want to delete?" message, click OK.

Step 15: Repeat Step 13 and Step 14 for the **private** community string. You should only have the read-write and read-only community strings as shown below.

սիսիս									ogout <u>R</u> efres
CISCO	MONITOR WLANS	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK	
Management	SNMP v1 / v2c C	ommunity							New
Summary									
▼ SNMP	Community Name		IP Address	IP Mask	Access M	tode Status			
General	cisco		10.4.48.0	255.255.25	5.0 Read-On	y Enable			
SNMP V3 Users Communities	cisco123		10.4.48.0	255.255.25	5.0 Read-Wr	te Enable			
Trap Receivers									
Trap Controls									
Trap Logs									
HTTP-HTTPS									
Telnet-SSH									
Serial Port									
Local Management Users									
User Sessions									
Logs									
Mgmt Via Wireless									
Software Activation									
Tech Support									
Free Support									

(Optional)

In networks where network operational support is centralized, you can increase network security by using an access control list in order to limit the networks that can access your controller. In this example, only devices on the 10.4.48.0/24 network are able to access the controller via Secure Shell (SSH) Protocol or Simple Network Management Protocol (SNMP).

Step 1: In Security > Access Control Lists > Access Control Lists, click New.

Step 2: Enter an access control list name (Example: ACL-Rules), select **IPv4** as the ACL type, and then click **Apply**.

Step 3: In the list, choose the name of the access control list you just created, and then click Add New Rule.

Step 4: In the window, enter the following configuration details, and then click **Apply**.

- · Sequence-1
- · Source-10.4.48.0 / 255.255.255.0
- · Destination—Any
- · Protocol-TCP
- Destination Port—HTTPS
- · Action—Permit



Step 5: Repeat Step 3 through Step 4 using the configuration details in the following table.

Table 3 - Access Rule configuration values

Sequence	Source	Destin ation	Protocol	Destina tion port	Action
2	10.4.48.0/ 255.255.255.0	Any	TCP	Other/22	Permit
3	Any	Any	TCP	HTTPS	Deny
4	Any	Any	TCP	Other/22	Deny
5	Any	Any	Any	Any	Permit



Step 6: In Security > Access Control Lists > CPU Access Control Lists, select Enable CPU ACL.

Step 7: In the **ACL Name** list, choose the ACL you created in Step 2, and then click **Apply**.


Step 1: In Security > AAA > RADIUS > Authentication, click New.

Step 2: Enter the Server IP Address. (Example: 10.4.48.15)

Step 3: Enter and confirm the Shared Secret. (Example: SecretKey)

Step 4: To the right of Management, clear Enable, and then click Apply.

Security	RADIUS Authentication S	ervers > New < Back Apply
 AAA General RADIUS Authentication Accounting Falback TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies 	Server Index (Priority) Server IP Address Shared Secret Format Shared Secret Confirm Shared Secret Key Wrap Port Number Server Status Support for RFC 3576 Server Timeout	1 • 10.4.48.15 • ASCII • • ••••••••••••••••••••••••••••••••••••
Local EAP	Network User	2 seconds
 Priority Order Certificate Access Control Lists Wireless Protection Policies Web Auth TrustSec SXP Advanced 	Management IPSec	Enable

Step 5: In Security > AAA > RADIUS > Accounting, click New.

Step 6: Enter the Server IP Address. (Example: 10.4.48.15)

Step 7: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)

Security	RADIUS Accounting Se	ervers > New		< Back	Apply
 AAA General RADIUS Authentication Accounting Fallback TACACS+ LDAP LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies Password Policies Local EAP Prointy Order Certificate Access Fortection Policies Wireless Protection Advanced 	Server Index (Priority) Server IP Address Shared Secret Format Shared Secret Confirm Shared Secret Port Number Server Status Server Timeout Network User IPSec	1 • 10.48.15 ASCII • 10.48.15 IBI3 Enabled • 2 seconds Ø Enable Enable			

Procedure 8

Configure management authentication

(Optional)

You can use this procedure to deploy centralized management authentication by configuring the Authentication, Authorization and Accounting (AAA) service. If you prefer to use local management authentication, skip to Procedure 9.

As networks scale in the number of devices to maintain, the operational burden to maintain local management accounts on every device also scales. A centralized AAA service reduces operational tasks per device and provides an audit log of user access, for security compliance and root-cause analysis. When AAA is enabled for access control, it controls all management access to the network infrastructure devices (SSH and HTTPS). **Tech Tip**

Access to the standby WLC when in HOT STANDBY mode via the console port requires the locally configured administrator user ID and password. Because the standby WLC does not have full IP connectivity to the network, it is unable to communicate with the configured TACACS server.

Step 1: In Security > AAA > TACACS+ > Authentication, click New.

Step 2: Enter the Server IP Address. (Example: 10.4.48.15)

Step 3: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)



Step 4: In Security > AAA > TACACS+ > Accounting, click New.

Step 5: Enter the Server IP Address. (Example: 10.4.48.15)

Step 6: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)

CISCO		ROLLER WIRELESS SECURIT	- <u></u>	HELP FEEDBACK	
Security	TACACS+ Accounting	Servers > New		< Back	Apply
 ★ AAA General ▶ RADIUS ★ TACACS+ Authenitation Accounting Authorization LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Apsword Policies 	Server Index (Priority) Server IP Address Shared Secret Format Shared Secret Confirm Shared Secret Port Number Server Status Server Timeout	1 • • 10.4.48.15 ASCII • • • • • • • • • • • • • • • • • •			
Local EAP					
 Priority Order Certificate Access Control Lists Wireless Protection Policies Web Auth TrustSec SXP Advanced 					

Step 7: In Security > AAA > TACACS+ > Authorization, click New.

Step 8: Enter the Server IP Address. (Example: 10.4.48.15)

Step 9: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)

սիսիս						Sa <u>v</u> e Cor	figuration Ping Logout	l <u>R</u> efresh
cisco	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBACK	
Security • AAA General • RADIUS • TACACS+ Authentication	TACACS+ Author Server Index (Priorit Server IP Address Shared Secret Forma	ization Server	-			_		lpply
Accounting Authorization LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies	Shared Secret Confirm Shared Secr Port Number Server Status Server Timeout	et	49 Enabled • 5 second	ls				
 Local EAP Priority Order 								
 Certificate Access Control Lists Wireless Protection Policies 								
 Web Auth TrustSec SXP Advanced 								

Step 10: Navigate to Security > Priority Order > Management User.

Step 11: Using the arrow buttons, move TACACS+ from the Not Used list to the Used for Authentication list.

Step 12: Using the Up and Down buttons, move TACACS+ to be the first in the Order Used for Authentication list.

Step 13: Using the arrow buttons, move **RADIUS** to the **Not Used** list, and then click **Apply**.



Procedure 9

Enable multicast support

Some data and voice applications require the use of multicast in order to provide a more efficient means of communication typical in one-to-many communications. The Cisco SBA local mode design model tunnels all traffic between the AP and WLC. As a result, the WLC issues all multicast joins on behalf of the wireless client.

Step 1: In Controller > Multicast, select Enable Global Multicast Mode and Enable IGMP Snooping, and then click Apply.

alulu -											Lo <u>q</u> out <u>R</u> efresh
CISCO	MONITOR	<u>W</u> LANs		LER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK	
Controller	Multicast									l	Apply
General Inventory Interfaces Interface Groups Multicast Network Routes Redundancy Internal DHCP Server Mobility Management Ports NTP CDP PMIPv6 PMIPv6 Advanced	Enable IG IGMP Tim IGMP Que Enable ML MLD Time	obal Multic MP Snoopi eout (seco ry Interva D Snoopin out (secon ry Interval	ng nds) I (seconds) ig ids)	20 20 20 20							

Step 2: Navigate to Controller > General.

Step 3: If you are using Cisco 5500 Series wireless LAN controllers, in the **AP Multicast Mode** list, choose **Multicast**, and then in the box, enter the multicast IP address that is to be used for multicast delivery. (Example: 239.1.1) and then click **Apply**.

If you are using a Cisco 2500 Series wireless LAN controller, in the **AP Multicast Mode** box, enter the multicast IP address that was configured in Step 8 of the "Configure the WLC platform" procedure, and then click **Apply**.

cisco	MONITOR WLANS CONTROLLER	WIRELESS SECURITY	Save Configuration <u>P</u> ing Logout <u>B</u> efre M <u>A</u> NAGEMENT C <u>O</u> MMANDS HELP <u>E</u> EEDBACK
Controller	General		Apply
General	Name	WLC-1-Primary	
Inventory	802.3× Flow Control Mode	Disabled -	
Interfaces	LAG Mode on next reboot	Enabled V	(LAG Mode is currently enabled).
Interface Groups	Broadcast Forwarding	Disabled 🔻	,,
Multicast	AP Multicast Mode ⁴	Multicast - 239.1.1.1	Multicast Group Address
Network Routes	AP Fallback	Disabled -	
Redundancy	Fast SSID change	Disabled 👻	
Internal DHCP Server	Default Mobility Domain Name	CAMPUS	
Mobility Management	RF Group Name	CAMPUS	
Ports	User Idle Timeout (seconds)	300	
▶ NTP	ARP Timeout (seconds)	300	
CDP	Web Radius Authentication	PAP 👻	
PMIPv6	Operating Environment	Commercial (0 to 40 C)	
IPv6	Internal Temp Alarm Limits	0 to 65 C	
mDNS	WebAuth Proxy Redirection Mode	Disabled 👻	
Advanced	WebAuth Proxy Redirection Port	0	
Havancea	Global IPv6 Config	Enabled 👻	
	1. Multicast is not supported with Fle	xConnect on this platform.	

Procedure 10 **Create the WLAN data interface**

Configure the WLC to separate voice and data traffic, which is essential in any good network design in order to ensure proper treatment of the respective IP traffic, regardless of the medium it is traversing. In this procedure, you add an interface that allows devices on the wireless data network to communicate with the rest of your organization.

Step 1: In Controller>Interfaces, click New.

Step 2: Enter the Interface Name. (Example: Wireless-Data)

Step 3: Enter the VLAN Id, and then click Apply. (Example: 116)

CISCO MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Controller Interfaces > New < Back Apply General Interface Name wireless-data	սիսիս								nfiguration <u>P</u> ing	
General Interface Name wireless-data Inventory VLN Id 116 Interfaces Interface Groups Multicast Network Routes Internal DHCP Server Mobility Management Ports P NTP CDP	CISCO	MONITOR	<u>W</u> LANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBAC	<
Inventory VLAN Id II6 Interfaces Interface Groups Multicast Network Routes Internal DHCP Server Mobility Management Ports NTP CDP	Controller	Interface	s > New						< Back	Apply
	General Inventory Interfaces Interface Groups Multicast Network Routes Internal DHCP Server Mobility Management Ports NTP CDP	Interface	Name	wireless-data					< Back	Apply

Step 4: If you are deploying a Cisco 2500 Series Wireless LAN Controller, in the Port Number box, enter the number of the port that is connected to the LAN distribution switch. (Example: 1)

Step 5: In the IP Address box, enter the IP address assigned to the WLC interface. (Example: 10.4.16.5)

Step 6: Enter the Netmask. (Example: 255.255.252.0)

Step 7: In the Gateway box, enter the IP address of the VLAN interface defined in Procedure 1. (Example: 10.4.16.1)

Step 8: In the Primary DHCP Server box, enter the IP address of your organization's DHCP server (Example: 10.4.48.10), and then click Apply.

،، ،،، ،، cısco	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	Sa <u>v</u> e Cor C <u>O</u> MMANDS	nfiguration <u>P</u> ing Logout <u>R</u> ef HELP <u>F</u> EEDBACK
Controller	Interfaces > Edit						< Back Apply
General							
Inventory	General Informati	on					
Interfaces	Interface Name	wireles	data				
Interface Groups	MAC Address		7:69:dd:6f				
Multicast	Hine Address	001241	//.09.00.01				
Network Routes	Configuration						
Internal DHCP Server	Guest Lan						
Mobility Management	Quarantine						
Ports NTP	Quarantine Vlan Id	0					
CDP	Physical Informat	ion					
Advanced	The interface is attac	hed to a LAG.					
F Advanced	Enable Dynamic AP Management						
	Interface Address						
	VLAN Identifier	116					
	IP Address	10.4.16.5					
	Netmask	255.255.2	52.0				
	Gateway	10.4.16.1					
	DHCP Information						
	Primary DHCP Serve	r i	10.4.48.10				
	Secondary DHCP Ser	ver					
	Access Control Lis	t					
	ACL Name	1	none 👻				
	Note: Changing the Inte temporarily disabled an some clients.						



Tech Tip

To prevent DHCP from assigning wireless clients addresses that conflict with the WLC's addresses, exclude the addresses you assign to the WLC interfaces from DHCP scopes.

Create the wireless LAN voice interface

You must add an interface that allows devices on the wireless voice network to communicate with the rest of the organization.

Step 1: In Controller>Interfaces, click New.

Step 2: Enter the Interface Name. (Example: wireless-voice)

Step 3: Enter the VLAN Id, and then click Apply. (Example: 120)

սիսիս								ogout <u>R</u> efresł
cisco	MONITOR WLANS	<u>CONTROLLER</u>	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBACK	
Controller	Interfaces > Nev	N					< Back	Apply
General Inventory Interfaces Interface Groups Multicast Network Routes Internal DHCP Server Mobility Management Ports NTP CDP Advanced	Interface Name VLAN Id	wireless-voice						

Step 4: If you are deploying a Cisco 2500 Series Wireless LAN Controller, in the Port Number box, enter the number of the port that is connected to the LAN distribution switch. (Example: 1)

Step 5: In the IP Address box, enter the IP address assigned to the WLC interface. (Example: 10.4.20.5)

Step 6: Enter the Netmask. (Example: 255.255.252.0)

Step 7: In the Gateway box, enter the IP address of the VLAN interface defined in Procedure 1. (Example: 10.4.20.1)

Step 8: In the Primary DHCP Server box, enter the IP address of your organization's DHCP server (Example: 10.4.48.10), and then click Apply.

սիսիս								nfiguratio	on <u>P</u> ing L	ogout <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	
Controller	Interface	s > Edit							< Back	Apply
General										
Inventory	General I	nformat	ion							
Interfaces Interface Groups	Interface	Name	wireless	-voice						
Multicast	MAC Add	ress	00:24:9	97:69:dd:6f						
Network Routes	Configura	tion								
Internal DHCP Server	Guest Lar	ı								
Mobility Management	Quarantir									
Ports NTP	Quarantir	ne Vlan Id	0							
CDP	Physical 1	[nformat	ion							
Advanced		namic AP	ched to a LAG.							
	Interface	Address								
	VLAN Ide	ntifier	120							
	IP Addres	s	10.4.20.5							
	Netmask		255.255.2	52.0						
	Gateway		10.4.20.1							
	DHCP Inf	ormation	ı							
	Primary D	HCP Serve	r :	0.4.48.10						
	Secondar	y DHCP Se	rver							
	Access Co	ontrol Lis	it							
	ACL Nam	e		none 🔻		_				
		disabled an	erface parameters Id thus may result							

Tech Tip

To prevent DHCP from assigning wireless clients addresses that conflict with the WLC's addresses, exclude the addresses you assign to the WLC interfaces from DHCP scopes.

Configure the data wireless LAN

Wireless data traffic can tolerate delay, jitter, and packet loss more efficiently than wireless voice traffic. Applications that require a one-to-many communication model may require the use of multicast-based transmission. Generally, for the data WLAN, it is recommended to keep the default QoS settings and segment the data traffic onto the data wired VLAN.

Step 1: Navigate to WLANs.

Step 2: Click the WLAN ID number of the SSID created in Procedure 3. (Example: WLAN-Data)

	MONITOR WLANS CONTROLLER WIRELESS SEC	Saye Configuration Ping Logout Befresh URITY MANAGEMENT COMMANDS HELP <u>F</u> EEDBACK
WLANs	WLANs	Entries 1 - 1 of 1
WLANs	Current Filter: None [Change Filter] [Clear Filter]	Create New Go
Advanced	ULAN ID Type Profile Name	Admin WLAN SSID Status Security Policies
	1 WLAN WLAN-Data	WLAN-Data Enabled [WPA2][Auth(802.1X)]

Step 3: On the General tab, in the **Interface/Interface Group(G)** list, choose the interface created in Procedure 10. (Example: wireless-data)

Step 4: If you want to enable multicast on the WLAN-Data wireless LAN, select **Multicast VLAN Feature**, and then in the **Multicast Interface** list, choose the WLAN data interface. (Example: wireless-data)

Step 5: Click Apply.

cisco	Sage Configuration Eng Logout								
WLANs	WLANs > Edit 'WLAN-Data'	y							
WLANS	General Security QoS Advanced	_							
Advanced	Profile Name WLAN-Data								
	Type WLAN								
	SSID WLAN-Data								
	Status V Enabled								
	Security Policies [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)								
	Radio Policy All								
	Interface/Interface Group(G) wireless-data								
	Multicast Vlan Feature V Enabled								
	Multicast Interface wireless-data								
	Broadcast SSID								
	Foot Notes								
	Web Policy cannot be used in combination with IPsec ProcConnect Local Switching in not supported with IPsec, CRAINTE authentication, Override Interface ACLS ProcConnect Local Switching in not supported with IPsec, CRAINTE authentication, Override Interface ACLS Clear MEP: so to alconate the support of the support and the support and the support of the support Science MEP: so to alconate Local Switching is enabled Switching Interface ACLS Switching								
	12 Max-associated-idents feature is not supported with RecConnect Local Authentication. 13 VLM based central subthing is not supported with RecConnect Local Authentication. 14 Enabling glx-randomize will prevent clients from decrypting broadcast and multicast packets. 15 Fast Transition is supported with WH2 and open socurity policy 16 A value of zaro (0) indicasts that the value specified in the selected QoS profile will take effect.								

Configure the voice wireless LAN

Wireless voice traffic is different from data traffic in that it cannot effectively handle delay and jitter as well as packet loss. Multicast may be required for some voice applications that require a one-to-many method of communication. One common example of a multicast voice use-case is a group-based push-to-talk, which is more efficient via multicast than over traditional unicast transmissions.

To configure the voice WLAN, change the default QoS settings to Platinum and segment the voice traffic onto the voice wired VLAN.

Step 1: On the WLANs page, in the list, choose Create New, and then click Go.

uluilu cisco	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY MANAGEMENT		uration <u>P</u> ing Logout <u>R</u> efre
WLANs	WLANs				Entries 1 - 1 of 1
WLANS	Current Filter: Non	[Change Filter] [Clear I	Filter] Crea	ate New 👻	Go
Advanced	WLAN ID Type	Profile Name	WLAN SSID	Admin Status	Security Policies
	1 WLAN	WLAN-Data	WLAN-Data	Enabled	[WPA2][Auth(802.1X)]

Step 2: Enter the Profile Name. (Example: Voice)

Step 3: In the **SSID** box, enter the voice WLAN name, and then click **Apply**. (Example: WLAN-Voice)



Step 4: On the General tab, next to Status, select Enabled.

Step 5: In the **Interface/Interface Group(G)** list, choose the interface created in Procedure 11. (Example: wireless-voice)

Step 6: If you want to enable multicast on the WLAN-Voice wireless LAN, select **Multicast VLAN Feature**, and then in the **Multicast Interface** list, choose the WLAN voice interface. (Example: wireless-voice)

Step 7: Click Apply.

cisco	Sage Configuration Eing Logout Befr MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK							
WLANs	WLANs>Edit 'WLAN-Voice' <back apply<="" td=""></back>							
WLANs WLANs	General Security QoS Advanced							
Advanced	Profile Name WLAN-Voice							
	Type WLAN							
	SSID WLAN-Voice							
	Status 🗹 Enabled							
	Security Policies [WPA2][Auth(802.1%)] (Modifications done under security tab will appear after applying the changes.)							
	Radio Policy All 🗸							
	Interface/Interface Group(G) wireless-voice 👻							
	Multicast Vlan Feature 🔽 Enabled							
	Multicast Interface wireless-voice Broadcast SSID Fnabled							
	Broadcast SSID 🗹 Enabled							
	Foot Notes							
	1 Web Policy cannot be used in combination with IPsec 2 Rescioned Load Switching is not supported with IPsec, CANNITE authentication, Override Interface ACLs 2 Control Control 3 Clance MPF is not active unless WM22 is configured 5 Learn Clent IP is configured only when Faccioned Load Switching is enabled 5 Learn Clent IP is configured only when Faccioned Load Switching is anabled							
	6 WMM and open or AES security should be enabled to support higher 11n rates 8 Value zero imples there is no retriction on maximum checks allowed. 9 MAC Filtering is not supported with flexConnect Local authentication 10 MAC Filtering should be enabled.							
	11 Guest tunneling, Local switching, DKP: Required should be disabled. 12 Max-sociated-clents teature is not supported with RecConnect Local Authentication. 13 VLAN based central switching is not supported with RecConnect Local Authentication. 14 Rebuilding dis-nardonnics will prevent clents from decrytopi provadost and multicast packets.							
	15 Fast Transition is supported with WPA2 and open security policy 16 A value of zero (0) indicates that the value specified in the selected QoS profile will take effect.							

February 2013 Series

Step 8: On the QoS tab, in the Quality of Service (QoS) list, choose Platinum (voice), and then click Apply.

uluili. cisco	Saye Configuration Bing Logout Befre MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
/LANs	WLANs > Edit 'Voice' < Back Apply
WLANS WLANS	General Security QoS Advanced
	Quality of Service (QoS) Platinum (voice) WHM WMM Policy Allowed 7920 AP CAC Enabled 7920 Client CAC Enabled
	Foot Notes 1 Web Policy cannot be used in combination with IPsec 2 H-REAP Local Switching is not supported with IPsec (CAMITE authentication 3 Wine client exclusion is enabled, a Timouci Value of zero means infinity (will require administrative override to reset excluded clients) 4 Client MTP is not active unless WRA2 is configured 5 Learn Client IP is configurable only when HeRAP Local Switching is enabled 6 WMM and coen or AES security should be enabled to support higher 11n rates 7 Multicast Should Be Enabled For IPV6. 8 Band Select is configurable only when Realize Policy is set to XII'. 9 Value zero implies there is no restriction on maximum clients allowed. 10 MAC Filtering is not supported with HREAP Local authentication 11 MAC Filtering Should be enabled. 12 Guest turnelling, Local switching, DICP Required should be disabled. 13 Max-associated-clients facture is non supported with HREAP Local authentication.

Procedure 14

Configure the resilient controller

If you are configuring Cisco 2500 Series WLCs, AP SSO is not supported. You should therefore complete this procedure in order to join multiple controllers to a mobility group. If you are configuring Cisco 5500 Series WLCs, AP SSO is supported, and you should skip this procedure.

The local-mode design model can support lightweight access points across multiple floors and buildings simultaneously, in all deployment scenarios, you should deploy multiple controllers at each site, for resiliency.

This design, not based on AP SSO, uses two independently licensed controllers. The first is the primary controller to which access points normally register. The secondary controller, also called the *resilient controller*, provides resiliency in case the primary controller fails. Under normal operation, no access points register to the resilient controller.

Even when configured as a pair, controllers do not share configuration information as they do when using AP SSO, so you must configure each controller separately. Because it is possible for a wireless client in your network to roam from an access point joined to one controller to an access point joined to another controller, both controllers should be deployed in the same mobility group.

A mobility group is a set of controllers, identified by the same mobility group name that defines the realm of seamless roaming for wireless clients. By creating a mobility group, you can enable multiple controllers in a network to dynamically share information and forward data traffic when intercontroller or intersubnet roaming occurs. Controllers in the same mobility group can share the context and state of client devices as well as their list of access points so that they do not consider each other's access points as rogue devices. With this information, the network can support intercontroller WLAN roaming and controller redundancy.

Step 1: Repeat Procedure 3 through Procedure 13 for the resilient controller.

Step 2: On the primary controller, navigate to Controller > Mobility Management > Mobility Groups. The MAC address, IP address, and mobility group name for the local controller are shown.

սիսիս	MONITOR	WLANs	CONTROLLER	WIRELECC	CECURITY	MANACEMENT	Sa <u>v</u> e Co COMMANDS	nfiguration HELP		ogout <u>R</u> efresh
CISCO Controller	MONITOR Static Mo		oup Members	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	_	FEEDBACK	EditAll
General Inventory	Local M	obility Gro	CAMPUS							
Interfaces	MAC Ad	dress	IP Address	Group N	ame M	lulticast IP	Status			
Interface Groups Multicast	00:24:9	7:69:dd:60	10.4.46.64	CAMPUS	0	.0.0.0	Up			
Network Routes										
Internal DHCP Server										
 Mobility Management Mobility Groups Mobility Anchor Config Multicast Messaging 										
Ports										
▶ NTP										
▶ CDP										
Advanced										

Step 3: On the resilient controller, navigate to Controller > Mobility Management > Mobility Groups, and then click New.

Step 4: In the **Member IP Address** box, enter the IP address of the primary controller. (Example: 10.4.46.64)

Step 5: In the **Member MAC Address** box, enter the MAC address of the primary controller, and then click **Apply**.

սիսիս								figuration Ping L	.ogout <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBACK	
Controller	Mobility	Group M	ember > New	,				< Back	Apply
General Inventory		Member IP Address 10.4.46.64 Member MAC Address 00:24:97:69:dd:60							
Interfaces Interface Groups Multicast	Group N	ame	CAMPUS						
Network Routes									
 Mobility Management Mobility Groups Mobility Anchor Config Multicast Messaging 									
Ports									
▶ NTP									
► CDP									
Advanced									

Step 6: On the primary controller, navigate to Controller > Mobility Management > Mobility Groups, and then click New.

Step 7: In the Member IP Address box, enter the IP address of the resilient controller. (Example: 10.4.46.65)

Step 8: In the Member MAC Address box, enter the MAC address of the resilient controller, and then click Apply.



Step 9: On each controller, click Save Configuration, and then click OK.

Step 10: Navigate to Controller > Mobility Management > Mobility

Groups on each controller, and then verify that connectivity is up between all the controllers by examining the mobility group information. In the Status column, all controllers should be listed as **Up**.

սիսիս								nfiguration		Logout <u>R</u> e
cisco	MONITOR	WLANs	<u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK	:
Controller	Static Mo	bility Gro	oup Members	S				,	lew	EditAl
General Inventory	Local M	obility Grou	up CAMPUS	;						
Interfaces	MAC Ad	dress	IP Address	Group Na	me M	ulticast IP	Status			
Interface Groups	00:24:9	7:69:dd:60	10.4.46.64	CAMPUS	0.	0.0.0	Up			
Multicast Network Routes	00:24:9	7:69:a7:20	10.4.46.65	CAMPUS	0.	0.0.0	Up			
Internal DHCP Server										
Mobility Management Mobility Groups Mobility Anchor Config Multicast Messaging										
Ports										
NTP										
CDP										
Advanced										

Procedure 15

Configure controller discovery

You have three options to configure controller discovery, depending on the number of controller pairs and the type of DHCP server you've deployed.

If you have only one controller pair in your organization, complete Option 1 of this procedure. If you have deployed multiple controller pairs in your organization and you use Cisco IOS software in order to provide DHCP service, complete Option 2. If you have deployed multiple controller pairs in your organization and you use a Microsoft DHCP server, complete Option 3.

DHCP Option 43 maps access points to their controllers. Using DHCP Option 43 allows remote sites and each campus to define a unique mapping.

Figure 5 - Flow chart of WLC discovery configuration options



Option 1. Only one WLC pair in the organization

Step 1: Configure the organization's DNS servers (Example: 10.4.48.10) to resolve the **cisco-capwap-controller** host name to the management IP address of the controller. (Example: 10.4.46.64) The cisco-capwap-controller DNS record provides bootstrap information for access points that run software version 6.0 and higher.

Step 2: If the network includes access points that run software older than version 6.0, add a DNS record to resolve the host name **cisco-lwapp-controller** to the management IP address of the controller.

Option 2. Multiple WLC pairs in the organization: Cisco IOS DHCP server

In a network where there is no external, central-site DHCP server, you can provide DHCP service with Cisco IOS software. This function can also be useful at a remote site where you want to provide local DHCP service and not depend on the WAN link to an external, central-site DHCP server.

Step 1: Assemble the DHCP Option 43 value.

The hexadecimal string is assembled as a sequence of the Type + Length + Value (TLV) values for the Option 43 suboption, as follows:

- Type is always the suboption code 0xf1.
- *Length* is the number of controller management IP addresses times 4, in hexadecimal.
- Value is the IP address of the controller listed sequentially, in hexadecimal.

For example, suppose there are two controllers with management interface IP addresses 10.4.46.64 and 10.4.46.65. The type is 0xf1. The length is 2 * 4 = 8 = 0x08. The IP addresses translate to 0a042e40 (10.4.46.64) and 0a042e41(10.4.46.65). When the string is assembled, it yields **f1080a042e400a042e41**.

Step 2: On the network device, add Option 43 to the pre-existing data network DHCP Pool.

ip dhcp pool [pool name]
 option 43 hex f1080a042e400a042e41

Option 3. Multiple WLC pairs in the organization: Microsoft DHCP server

This procedure shows how the Microsoft DHCP server is configured in order to return vendor-specific information to the lightweight Cisco Aironet 1600, 2600, and 3600 Series Access Points used in this deployment guide. The vendor class identifier for a lightweight Cisco Aironet access point is specific to each model type. To support more than one access point model, you must create a vendor class for each model type.

Table 4 - Vendor class identifiers

Access point	Vendor class identifier
Cisco Aironet 1600 Series	Cisco AP c1600
Cisco Aironet 2600 Series	Cisco AP c2600
Cisco Aironet 3600 Series	Cisco AP c3600

Step 1: Open the DHCP Server Administration Tool or MMC.

Step 2: Navigate to DHCP > ad.cisco.local, right-click IPv4, and then click Define Vendor Classes.



Step 3: In the DHCP Vendor Classes dialog box, click Add.



Step 4: In the New Class dialog box, enter a **Display Name**. (Example: Cisco Aironet 1600 AP)

Step 5: In the ASCII section, enter the vendor class identifier for the appropriate access point series from Table 4, and then click **OK**. (Example: Cisco AP c1600)

Step 6: In the DHCP Vendor Classes dialog box, click Close.

😲 DHCP	_ _ _ _ _ _ _
File Action View Help	
🗢 🔿 🗡 📰 🗶 🖼 🧟 📾	
P Name	Actions
	ad.cisco.local 🔺
 IPv4 ■ IPv6 IPv6 	More Actions
DHCP Vendor Classes	? ×
Available classes:	
Name Description	Add
Mii Mii Mii	? × Edit
Mi Display name:	lemove
Cis Cis Cis	
Cis Description:	
Cis Cis	
Cis ID: Binary: ASC	
0000 43 69 73 63 6F 20 41 50 Cisco A 0008 20 63 31 36 30 30 c1600	P Close
OK Car	

Step 7: Right-click the IPV4 DHCP server soot, and then click Set Predefined Options.

Step 8: In the **Option Class** list, choose the class created in Step 4, and then click **Add**.

Predefined Options	and Values 🔹 💽 🗙
Option class:	Cisco Aironet 1600 AP
Option name:	<u> </u>
	Add Edit Delete
Description:	
Value	
	OK Cancel

Step 9: In the Option Type dialog box, enter a Name. (Example: Option 43)

Step 10: In the Data Type list, choose IP Address.

Step 11: Select Array.

Step 12: In the Code box, enter 241, and then click OK.

Change Option	Name ? 🗙
Class:	Cisco Aironet 1600 AP
<u>N</u> ame:	Option 43
Data type:	IP Address 🔽 🗹 Array
<u>C</u> ode:	241
D <u>e</u> scription:	
	OK Cancel

The vendor class and suboption are now programmed into the DHCP server. Now, you need to define the vendor-specific information for the DHCP scope.

Step 13: Choose the DHCP scope that you will be installing Access Points on then right-click **Scope Options**, and then click **Configure Options**.

Step 14: Click the Advanced tab, and in the Vendor class list, choose the class created in Step 4.

Step 15: Under Available Options, select 241 Option 43.

Step 16: In the **IP address** box, enter the IP address of the primary controller's management interface, and then click **Add**. (Example: 10.4.46.64)

Scope Options	?
General Advanced	
Vendor class:	Cisco Aironet 1600 AP
User class:	Default User Class
Available Options 241 Option 43	Description
✓ Data entry Server name:	>
	Resolve
IP address:	Add
10.4.46.64	Remove
	Up
	Down
,	
	OK Cancel Apply

Step 17: If you are not using the AP SSO feature, repeat Step 13 through Step 16 for the resilient controller, and then click **Apply**. (Example: 10.4.46.65)

Procedure 16 Connect the access points

On the LAN access switch, the switch interfaces that are connected to the access points use the standard access switchport configuration, with the exception of the QoS policy that you configure in this procedure.

Step 1: Configure the interface where the access point will be connected to trust the QoS marking from the access point.

interface GigabitEthernet [port]

description Access Point Connection

switchport access vlan 100

switchport voice vlan 101

switchport host

macro apply EgressQoS

switchport port-security maximum 11

switchport port-security

switchport port-security aging time 2

switchport port-security aging type inactivity

switchport port-security violation restrict

ip arp inspection limit rate 100

ip dhcp snooping limit rate 100

ip verify source

Procedure 17

Configure access points for resiliency

Step 1: For access points that are connecting to a WLC that is not using AP-SSO, it is necessary to configure these access points with the IP addresses of each of the non AP-SSO controllers. If you are installing access points that will connect to a pair of WLC's using AP-SSO, please skip this step.

Step 2: On the primary controller, navigate to Wireless, and then select the desired access point.

Step 3: Click the High Availability tab.

Step 4: In the **Primary Controller** box, enter the name and management IP address of the primary controller. (Example: WLC-1 / 10.4.46.64)

Step 5: In the **Secondary Controller** box, enter the name and management IP address of the resilient controller, and then click **Apply**. (Example: WLC-2 / 10.4.46.65)

սիսիս									Logout <u>R</u> efre:
CISCO	MONITOR WLANS	CONTRO	DLLER WIREL	ESS <u>S</u> ECURITY	′ M <u>A</u> N	NAGEMENT C	OMMANDS H	IELP FEEDBACK	(
Wireless	All APs > Details	for A45	07-1141N					< Back	Apply
 Access Points All APs 	General Crede	entials	Interfaces	High Availat	bility	Inventory	Advanced		
		Nam	e	Man	agemer	nt IP Address			
802.11b/g/n Global Configuration	Primary Controller	WLC			4.46.64				
Advanced	Secondary Contro Tertiary Controller		-2	10	4.46.65				
Mesh	reitary controller								
HREAP Groups 802.11a/n	AP Failover Priorit	Low	•						
▶ 802.11b/g/n									
Media Stream									
Country Timers									
QoS									
	Foot Notes								
	1 DNS server IP Add	ess and t	he Domain name	can be set only aft	ter a vali	id static IP is pus	hed to the AP.		

Process

Configuring Remote-Site Wireless with Cisco FlexConnect

- 1. Install the vWLC for FlexConnect designs
- 2. Configure the console port on the vWLC
- 3. Configure the vWLC network adapters
- 4. Configure the data center switches
- 5. Configure the LAN distribution switch
- 6. Connecting the redundancy port
- 7. Configure the WLC platform
- 8. Configure the time zone
- 9. Configure SNMP
- 10. Limit which networks can manage the WLC
- 11. Configure wireless user authentication
- 12. Configure management authentication
- 13. Configure the resilient WLC
- 14. Configure mobility groups
- 15. Configure the data wireless LAN
- 16.Configure the voice wireless LAN
- 17. Configure controller discovery
- 18.Configure the remote-site router
- 19. Configure the remote-site switch for APs
- 20.Enable licensing on the vWLC
- 21. Configure the AP for Cisco FlexConnect
- 22.Configure access points for resiliency
- 23.Configure Cisco FlexConnect groups

There are two methods of deploying remote site wireless LAN controllers, shared and dedicated:

- A shared WLC has both remote-site access points and local, on-site access points connected to it concurrently. Use a shared WLC when the number of access points matches the available capacity of the co-located WLCs near the WAN headend, and the WAN headend is co-located with a campus.
- A dedicated WLC only has remote-site access points connected to it. Use a dedicated WLC pair, such as Cisco Flex 7500 Series Cloud Controller using AP SSO, when you have a large number of access points or remote sites. Alternately, for smaller deployments, the use of the vWLC is a cost-effective option, provided that you do not exceed 200 APs across two or more Cisco FlexConnect groups or exceed 3000 wireless clients per vWLC. You also use this option when the co-located WLCs near the WAN headend don't have the necessary capacity or the WAN headend is not co-located with a campus.

If you are using a shared WLC, this deployment guide assumes that you have already deployed the WLC following the instructions in the "Configuring On-Site Wireless Controllers" process. To deploy remote-site wireless in a shared controller deployment, skip to Procedure 15.

If you are using a dedicated WLC, perform all the procedures in this process in order to deploy remote-site wireless.

Table 5 - Cisco remote-site wireless controller parameters checklist

Parameter	Cisco SBA values	Cisco SBA values	
	primary controller	resilient controller not using AP SSO	Site-specific values
Controller parameters			
Switch interface number	1/0/3, 2/0/3	1/0/4, 2/0/4	
VLAN number	146	146	
Time zone	PST -80	PST -8 0	
IP address	10.4.46.68/24	10.4.46.69/24	
Default gateway	10.4.46.1	10.4.46.1	
Hostname	WLC-RemoteSites-1	WLC-RemoteSites-2	
Mobility group name	REMOTES	REMOTES	
RADIUS server IP address	10.4.48.15	10.4.48.15	
RADIUS shared key	SecretKey	SecretKey	
Management network (optional)	10.4.48.0/24	10.4.48.0/24	
TACACS server IP address (optional)	10.4.48.15	10.4.48.15	
TACACS shared key (optional)	SecretKey	SecretKey	
Remote site parameters			
Wireless data SSID	WLAN-Data	WLAN-Data	
Wireless data VLAN number	65	65	
Wireless voice SSID	WLAN-Voice	WLAN-Voice	
Wireless voice VLAN number	70	70	
Default gateway	10.4.20.1	10.4.20.1	
Controller interface IP address	10.4.20.5/22	10.4.20.6/22	

Install the vWLC for FlexConnect designs

The virtual Wireless LAN controller (vWLC) is ideal for small to medium deployments where virtualized compute services are available within the data center and the AP design model is using local switching using Cisco FlexConnect.



The vWLC requires two physical network interface cards (NICs), one dedicated to the management interface and one for wireless client traffic. To provide full switch fabric redundancy, four physical NICs are required and are grouped into two pairs by using NIC teaming.

If you are installing a virtual wireless LAN controller (vWLC), you must complete the following steps in order to install it using the downloaded Open Virtual Archive (OVA) file available online from Cisco. If you are using another WLC to support your remote sites, you can skip to Procedure 5 "Configure the LAN distribution switch."

Step 1: Begin by preparing the VMware host machine networking environment. On the physical host machine, in vCenter, create three virtual switches (vSwitch0, vSwitch1, and vSwitch2), as follows:

- On vSwitch0, allocate two physical NIC interfaces. These will be used to provide management access to the vWLC (Example: management network mapped to VLAN ID: 148)
- On vSwitch1 allocate two physical interfaces that will be used to provide wireless VLAN access for each WLAN created on the vWLC. (Example: wireless VLANs mapped to VLAN ID: All 4095)
- On vSwitch2, no physical interfaces need to be allocated unless the service port will be used in the future. Failure to define this interface may result in the wrong interface's vSwitches being used for the wireless data VLANs. The configuration of the service port is required in

the event that the service port needs to be used for maintenance and support functions during the controller's lifecycle.

File Edit View Inventory Administration Plug-ins Help				
🖸 🔝 🏠 Home 🕨 👩 Inv	rentory 🕨 🎁 Hosts and Clusters	Search Inventory		
Police Police Police Police 10k 10k 10k 10k 10k 10k 10k		0.0, 623860 Evaluation (25 days remaining)		
A				

Next, you install the vWLC OVA file obtained from Cisco.

In vCenter, select the physical machine, click **File**, and then click **Deploy** OVF Template.



Step 2: Complete the Deploy OVF Template wizard. Note the following:

- On the Source page, select the downloaded vWLC OVA file that you obtained from Cisco.
- On the Name and Location page, provide a unique name for the virtual Wireless LAN controller. (Example: vWLC-1)

Specify a name and loca	ation for the deployed template
Source OVF Template Details Name and Location Storage Disk Format Network Mapping Ready to Complete	Name: [vwLC-1] The name can contain up to 80 characters and it must be unique within the inventory folder.
	Inventory Location:

Step 3: On the Storage page, select the storage destination of the virtual machine.

<u>Source</u> OVF Template Details	Select a destination s	torage for the virtu			
<u>Vame and Location</u> Storage	VM Storage Profile:	Drive Type	Capacity Provisioned		Thin Pro
Disk Format Network Mapping	Openfiler(Soft		9.09 TB 6.07 TB	3.04 TB NFS	Support
Ready to Complete	₿ R5200-E5X82_	Non-SSD	1.63 TB 1004.00	1.63 TB VMF55	5 Support
	Disable Storage Select a datastore:	DR5 for this virtua	machine		2

Step 4: On the Disk Format page, select Thick Provision Lazy Zeroed.

Deploy O¥F Template Disk Format			-
In which format do you	want to store the virtual disks?		
	_		
Source	Datastore:	RS200-ESXi2_Local	
OVF Template Details Name and Location			
Storage	Available space (GB):	1672.5	
Disk Format			
Network Mapping			
Ready to Complete	Thick Provision Lazy	Zeroed	
	C Thick Provision Eage	r Zeroed	
	C Thin Provision		
	< min Provision		

Step 5: On the Network Mapping page, in the **Destination Networks** list, choose the network defined on the VM host machine that will be used on the vWLC management interface. (Example: Server VLAN 1)

🛃 Deploy OVF Template			
Network Mapping What networks should the	he deployed template use?		
Source OVF Template Details Name and Location	Map the networks used in this OVF	template to networks in your inventory	
Storage	Source Networks	Destination Networks	
Disk Format	VM Network	Server VLAN 1	•
Network Mapping Ready to Complete		Server VLAN 1 Server VLAN 2 WLAN Service Port Wireless VLANs	
	Description:		
	The VM Network		A. V

Step 6: On the Ready to Complete page, review the settings, and then press **Finish**. Deployment of the OVA file begins, and it may take a few minutes to complete.

His chose and options ye	u want to use?		
Source OVF Template Details Name and Location Storage Disk Format Network Mapping Ready to Complete	When you click Finish, the depl Deployment settings: OVF file: Download size: Size on disk: Name: Folder: Host/Cluster: Datastore: Disk provisioning: Network Mapping: Network Mapping:	oyment task will be started. C:\A5_CTVM_7_4_1_42.ova 161.7 MB 8.2 GB WUC-1 RS200 Data Center rs200-esxi2.dsco.local RS200-EsX2_local Thick Provision Lazy Zeroed "VM Network" to "Server VLAN 1"	
Help		≤Back Finish	Cancel

Procedure 2

Configure the console port on the vWLC

When the vWLC starts, the Console tab within vSphere will display a repetitive message stating to press any key in order to make the Console tab the default terminal for console messages from the vWLC. If a key is not pressed during the vWLC startup, console communication to the vWLC through the vSphere client's console window will not be possible. This can be a problem when troubleshooting IP connectivity issues, for example, and console access is required. For this reason, in this procedure, you create a virtual serial port. This will ensure access to the vWLC console through the use of a standard Telnet client.

Step 1: In vCenter, select the newly added vWLC (Example: vWLC-1), click **Edit virtual machine settings**, and then in the Virtual Machine Properties dialog box, click **Add**.



Step 2: Complete the Add Hardware wizard. Note the following:

• On the Device Type page, select Serial Port.

√€		perties	
Hare	dware Options Resources P	rofiles VServices	Virtual Machine Version: 7
-			Memory Configuration
L.,	🚱 Add Hardware		×
Ha		you wish to add to your virtual machine	37
	Device Type Select Port Type	Choose the type of device you w	ish to add.
	Select Output File	Serial Port	Information
0	Ready to Complete	Parallel Port	This device can be added to this Virtual Machine.
		Floppy Drive	
		CD/DVD Drive	
l E		USB Device (unavailable)	
		PCI Device (unavailable)	
		Ethernet Adapter	
		SCSI Device	
	<u></u>	1	
	Help		≤Back Next ≥ Cancel

• On the Select Port Type page, select Connect via Network.



On the Network Backing page, select Server (VM listens for connection), and then in the Port URI box, enter telnet://[Host Machine IP Address]:[Unique TCP Port]. (Example: telnet://10.5.24.101:9292) This configures IP address and TCP port number that are used access the console port via Telnet.

	WLC-1 - Virtual Machine Proper		Machine Version: 7
Har	dware Options Resources Profi	vircual vircual	Machine Version: 7
	🚱 Add Hardware		×
	Network Serial Port Setting How should this serial port Select Port Type Select Network Backing Ready to Complete		
		Use Virtual Serial Port Concentrator vSPC URI: Device Status C Connect at power on I/O Mode Vield CPU on poll Allow the guest operating system to use this serial port in polled mode rather than in interrupt mode.	
	Help	_≤Back Next ≥	Cancel

• On the Ready to Complete page, review the settings, and then click **Finish**.

Step 3: On the Virtual Machine Properties dialog box, click **OK**. The new serial port has been successfully configured.



Procedure 3

Configure the vWLC network adapters

Configure the network adapters that will be used for the WLAN service port and the wireless VLAN interfaces. In this procedure, four physical NIC interfaces are used in two EtherChannel pairs, and each interface in a pair connects to separate redundant switches.

Step 1: In the Virtual Machine Properties dialog box, select Network adapter 1, and then in the Network label list, choose WLAN Service Port.

Step 2: Select Network adapter 2, and in the Network label list, choose Wireless VLAN, and then press OK.

lardware Options Resources Pro	erties files vServices	Virtual Machine Version
Show All Devices	Add Remove	Device Status
Hardware Hardware CPUs Video card Video card Video Card Video Card CD/DVD drive 1 Floppy drive 1 Serial port 1	Summary 2048 MB 1 Video card Restricted LSI Logic Parallel Virtual Disk (Rs200-E5x02_Local) v WLAN Service Port Wireless VLANs Floppy 1 teinet://10.5.24.101:92	Connect at power on Adapter Type Current adapter: E1000 MAC Address D0:50:56:a2:5d:84 Automatic Autom

Step 3: Start the virtual wireless LAN controller for the first time by selecting virtual machine just installed in the left column, and pressing the **Power on the virtual machine option shown within the console tab.** Within the Console tab you are prompted to "Press any key to use this terminal as the default terminal." You do not need to press any key as access via the serial port that was created in Procedure 2 will be used.

🚱 vCenter.cisco.local - vSphere Client				
Bie Edit Wegt Equentory Administration Bie	pine Belp			
🖸 🔯 📩 Hone 🕨 🛃 Inventory	Hosts and Clusters		Search Inventory	0
Contractional and a second seco		A point of a static of a stati		
Bronot Tasks			Name, Target or Status contains: *	Osy
Name Target	Status Details	Initiated by Venter Server Requested Start Time	Completed Time	053
Name Target Power On virtual mech M VMLC-1	Completed	CISCOLISTING	10/31/2012 12:50:01	

Tech Tip

In the event that you are unable to use Telnet to connect to the serial port defined for the vWLC, you can restart the vWLC and press any key during the initial boot up in order to use the VMware console port as the access method.

Using a Telnet client, such as Putty, access the vWLC console port by connecting via Telnet to the IP address and TCP port defined in the Add Hardware wizard in the previous procedure.

🕵 PuTTY Configuration	
Category:	
🖃 Session	Basic options for your PuTTY session
Logging	Specify the destination you want to connect to
Keyboard	Host <u>N</u> ame (or IP address) <u>P</u> ort
Bell	10.5.24.101 9292
- Features ⊡- Window	Connection type: Ra <u>w</u> Ielnet Rlogin <u>S</u> SH Serial
Appearance Behaviour Translation Selection Colours Connection Data Proxy Telnet Rlogin SSH Serial	Load, save or delete a stored session Sav <u>e</u> d Sessions
	Default Settings Load Save Delete
About	Close window on e <u>x</u> it: Always Never Only on clean exit Open Cancel
About	

Procedure 4

Configure the data center switches

When using a dedicated design controller model with the Cisco Flex 7500 Series Cloud Controller, the controller resides within the data center. This procedure configures the data center Cisco Nexus switch for connectivity to the redundant Flex 7500 Series Cloud Controllers using redundant Ethernet ports configured for link aggregation (LAG). For the virtual Wireless LAN Controller, these steps are performed for the VM host machine during the deployment of the VM environment.

Step 1: On the primary data center Cisco Nexus switch (Example: DC5596UPa), create the wireless management VLAN that you are going to use to connect the redundant Cisco Flex 7500 Series Cloud Controller.

Vlan **146**

name WLAN Mgmt

Step 2: On the primary data center Cisco Nexus switch (Example: DC5596UPa), create wireless port channels for the primary and resilient Cisco Flex 7500 Series Cloud Controller.

- interface port-channel**65**
- description Link to WLC7500-1
 switchport mode trunk
 switchport trunk allowed vlan 146
 no shutdown
 interface port-channel66
 description Link to WLC7500-2
 switchport mode trunk
 switchport trunk allowed vlan 146
 no shutdown

Step 3: Configure a switched virtual interface (SVI) for the VLAN. This enables devices in the VLAN to communicate with the rest of the network.

interface Vlan146
 no shutdown
 description Wireless Management Network
 no ip redirects
 ip address 10.4.46.2/24
 ip router eigrp 100
 ip passive-interface eigrp 100

ip pim sparse-mode
hsrp 146
priority 110
ip 10.4.46.1

Step 4: Configure two ports on the data center switch as a trunk port. These two ports will be connected to the redundant ports on the primary Cisco Flex 7500 Series Cloud Controller.

interface Ethernet103/1/1
 description Links to 7500-1
 switchport mode trunk
 switchport trunk allowed vlan 146
 channel-group 65
 no shutdown
interface Ethernet104/1/1
 description link to 7500-1
 switchport mode trunk
 switchport trunk allowed vlan 146
 channel-group 65
 no shutdown

Step 5: Configure two ports on the data center switch as a trunk port. These two ports will be connected to the redundant ports on the resilient Cisco Flex 7500 Series Cloud Controller.

interface Ethernet103/1/2
 description link to 7500-2
 switchport mode trunk
 switchport trunk allowed vlan 146
 channel-group 66
 no shutdown
interface Ethernet104/1/2
 description link to 7500-2
 switchport mode trunk
 switchport trunk allowed vlan 146
 channel-group 66
 no shutdown

Step 6: Repeat this procedure for the redundant Cisco Nexus data center switch (Example: DC5596UPb). Failure to define these on both Cisco Nexus switches results in a configuration inconsistency and prevents the ports from coming active.

Procedure 5

Configure the LAN distribution switch

Step 1: On the LAN distribution switch, create the wireless management VLAN that you are connecting to the distribution switch.

vlan **146**

name WLAN_Mgmt

Step 2: Configure a switched virtual interface (SVI) for the VLAN so devices in the VLAN can communicate with the rest of the network.

interface Vlan146
description Wireless Management Network
ip address 10.4.46.1 255.255.255.0
no shutdown

Step 3: For interface configuration in this procedure, an 802.1Q trunk is used for the connection to the WLCs. This allows the distribution switch to provide the Layer 3 services to all of the networks defined on the WLC. The VLANs allowed on the trunk are reduced to only the VLANs that are active on the WLC.

If you are deploying the Cisco Catalyst 4500 Series LAN distribution switch, you do not need to use the **switchport trunk encapsulation dot1q** command in the following configurations.

If you are deploying a Cisco Flex 7500 Series Cloud Controller, configure a 10-Gigabit distribution switch interface as a trunk. Note that when deploying a Cisco Flex 7500 Series Cloud Controller, it should not be connected to a Cisco Catalyst 3750-X Series distribution switch.

interface TenGigabitEthernet [number]
description To WLC port 1
switchport trunk encapsulation dotlq
switchport trunk allowed vlan 146
switchport mode trunk
macro apply EgressQoS

logging event link-status
logging event trunk-status
no shutdown

If you are deploying a Cisco 5500 Series Wireless LAN Controller, configure at least two distribution switch interfaces as an EtherChannel trunk.

interface GigabitEthernet [port 1]

description To WLC Port 1

interface GigabitEthernet [port 2]

description To WLC Port 2

```
!
```

interface range GigabitEthernet [port 1], GigabitEthernet

[port 2]

switchport

macro apply EgressQoS
channel-group [number] mode on

logging event link-status

logging event trunk-status

logging event bundle-status

```
!
```

interface Port-channel [number]

description **To WLC**

switchport trunk encapsulation dot1q
switchport trunk allowed vlan 146
switchport mode trunk
logging event link-status
no shutdown

Procedure 6

Connecting the redundancy port

If you are using a Cisco vWLC, skip this procedure. If you are using a Cisco 7500 Series WLC and you wish to enable the high availability AP SSO feature, continue with this procedure. When using the high availability feature known as access point stateful switchover (AP SSO), a dedicated special-purpose port is available on the Cisco 7500 Series WLC. This port is located on the rear panel.

Step 1: Connect an ordinary Ethernet cable between the primary and standby WLC, as shown below.



Procedure 7

Configure the WLC platform

If you are installing a vWLC, the console port may be accessed by using a Telnet client as configured in Procedure 2. Alternately, you can use the VMware Console tab within vSphere in order to access the vWLC if the vSphere console was selected as the default terminal when the vWLC was started.

After the WLC is installed and powered on, you will see the following on the console:

Welcome to the Cisco Wizard Configuration Tool Use the '-' character to backup Would you like to terminate autoinstall? [yes]: **YES**

Step 1: Enter a system name. (Example: WLC-RemoteSites-1)

System Name [Cisco_d9:3d:66] (31 characters max): WLC-RemoteSites-1

Step 2: Enter an administrator username and password.

Tech Tip

Use at least three of the following four classes in the password: lowercase letters, uppercase letters, digits, or special characters.

Enter Administrative User Name (24 characters max): admin Enter Administrative Password (24 characters max): ***** Re-enter Administrative Password : *****

Step 3: Use DHCP for the service port interface address.

Service Interface IP address Configuration [none] [DHCP]: DHCP

Step 4: Enter the IP address and subnet mask for the management interface.

If you are deploying a Cisco 5500 Series WLC or Cisco Flex Series Cloud Controller, configure at least two interfaces as an EtherChannel trunk.

Enable Link Aggregation (LAG) [yes][NO]: YES

Management Interface IP Address: 10.4.46.68

Management Interface Netmask: 255.255.255.0

Management interface Default Router: 10.4.46.1

Management Interface VLAN Identifier (0 = untagged): 146

If you are deploying a virtual Wireless LAN Controller, select port 1 as the management interface port.

Management Interface Port Num [1 to 1]: 1

Step 5: Enter the default DHCP server for clients. (Example: 10.4.48.10)

Management Interface DHCP Server IP Address: 10.4.48.10

Step 6: If you are deploying a Cisco 7500 Series Wireless LAN Controller as a primary WLC in an AP-SSO redundant pair, complete the following steps to enable AP SSO on the primary.

Enable HA [yes][NO]: YES Configure HA Unit [PRIMARY][secondary]: PRIMARY Redundancy Management IP Address: 10.4.46.78 Peer Redundancy Management IP Address: 10.4.46.79

Step 7: If you are deploying a Cisco 7500 Series Wireless LAN Controller as a secondary WLC in an AP-SSO redundant pair, complete the following steps to enable AP SSO on the secondary

Enable HA [yes][NO]: YES Configure HA Unit [PRIMARY][secondary]: secondary Redundancy Management IP Address: 10.4.46.79 Peer Redundancy Management IP Address: 10.4.46.78 **Step 8:** The virtual interface is used by the WLC for mobility DHCP relay and intercontroller communication. Enter an IP address that is not used in your organization's network. (Example: 192.0.2.1)

Virtual Gateway IP Address: 192.0.2.1

Step 9: Enter a name for the default mobility and RF group. (Example: REMOTES)

Mobility/RF Group Name: REMOTES

Step 10: Enter an SSID for the WLAN that supports data traffic. You will be able to leverage this later in the deployment process.

Network Name (SSID): WLAN-Data Configure DHCP Bridging Mode [yes][NO]: NO

Step 11: Enable DHCP snooping.

Allow Static IP Addresses {YES][no]: NO

Step 12: Do not configure the RADIUS server now. You will configure the RADIUS server later by using the GUI.

Configure a RADIUS Server now? [YES][no]: NO

Step 13: Enter the correct country code for the country where you are deploying the WLC.

Enter Country Code list (enter 'help' for a list of countries)
[US]: US

Step 14: Enable all wireless networks.

Enable 802.11b network [YES][no]: **YES** Enable 802.11a network [YES][no]: **YES** Enable 802.11g network [YES][no]: **YES**

Step 15: Enable the RRM auto-RF feature. This helps you keep your network up and operational.

Enable Auto-RF [YES][no]: YES

Step 16: Synchronize the WLC clock to your organization's NTP server.

Configure a NTP server now? [YES] [no]:YES

Enter the NTP server's IP address: 10.4.48.17

Enter a polling interval between 3600 and 604800 secs: $\mathbf{86400}$

Step 17: Save the configuration. If you respond with **no**, the system will restart without saving the configuration, and you will have to complete this procedure again.

Configuration correct? If yes, system will save it and reset. [yes][NO]: **YES**

Configuration saved!

Resetting system with new configuration

Step 18: After the WLC has restarted, access the console port on the WLC and configure it to automatically convert the APs to Cisco FlexConnect mode as they register.

config ap autoconvert flexconnect

Step 19: Log in to the Cisco Wireless LAN Controller Administration page by using the credentials defined in Step 2. (Example: https://WLC-RemoteSites-1.cisco.local/)

Procedure 8 Configure the time zone

Step 1: Navigate to Commands > Set Time.

Step 2: In the **Location** list, choose the time zone that corresponds to the location of the WLC.

Step 3: Click Set Timezone.

սիսիս										Logout <u>R</u> efresl
CISCO	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBA	ACK
Commands	Set Time						Set	Date and	Time	Set Timezone
Download File Upload File Reboot	Current T Date	ime	Tue May 31 11:07	7:38 2011						
Config Boot Scheduled Reboot			Month		May	•		_		
Reset to Factory Default			Day Year		31 ¥ 2011					
Set Time										
Login Banner	Time							_		
			Hour		11 👻					
			Minutes		7					
			Seconds		38					
	Timezone									
			Delta		hours 0	mins 0				
			Location ¹	(GMT	-8:00) Pacific	Time (US and Can	ada) •	·		
	Foot Note	25								
	1. Automati	cally sets d	aylight savings tim	e where used.						

Procedure 9

Configure SNMP

Step 1: In Management > SNMP > Communities, click New.

Step 2: Enter the Community Name. (Example: cisco)

Step 3: Enter the IP Address. (Example: 10.4.48.0)

Step 4: Enter the IP Mask. (Example: 255.255.255.0)

Step 5: In the Status list, choose Enable, and then click Apply.

սիսիս							Sa <u>v</u> e Cor	nfiguratio	n <u>P</u> ing L	o <u>q</u> out <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK	
Management	SNMP v1	/ v2c Co	ommunity > N	ew					< Back	Apply
Summary SNNP General SNNP V3 Users Communities Trap Receivers Trap Controls Trap Logs HTTP-HTTPS Telnet-SSH Serial Port Local Management Users Users User Sessions > Logs	Communi IP Addres IP Mask Access Mi Status	ty Name s	cisco 10.4.48.0 255.255.255.0 Read Only v Enable v					_		
Mgmt Via Wireless > Software Activation > Tech Support										

Step 6: In Management > SNMP > Communities, click New.

Step 7: Enter the Community Name. (Example: cisco123)

Step 8: Enter the IP Address. (Example: 10.4.48.0)

Step 9: Enter the IP Mask. (Example: 255.255.255.0)

Step 10: In the Access Mode list, choose Read/Write.

Step 11: In the Status list, choose Enable, and then click Apply.

uluili. cisco	MONITOR WLANS	<u>C</u> ONTROLLER	WIRELESS	SECURITY	M <u>A</u> NAGEMENT	Sa <u>v</u> e Co C <u>O</u> MMANDS	nfiguratio HE <u>L</u> P	n <u>P</u> ing Logout <u>R</u> efresh <u>F</u> EEDBACK
Management Summary T SNMP	SNMP v1 / v2c Co Community Name IP Address						_	< Back Apply
General SNMP V3 Users Communities Trap Receivers Trap Controls Trap Logs	IP Mask Access Mode Status	255.255.255.0 Read/Write V Enable V						
HTTP-HTTPS Telnet-SSH								
Serial Port Local Management Users								
User Sessions Logs								
Mgmt Via Wireless Software Activation								
Tech Support								

Step 12: Navigate to Management > SNMP > Communities.

Step 13: Point to the blue box for the **public** community, and then click **Remove**.

Step 14: On the "Are you sure you want to delete?" message, click OK.

Step 15: Repeat Step 13 and Step 14 for the private community. You should only have the read-write and read-only community strings as shown below.

սիսիս								Sa <u>v</u> e Co	nfiguratio	n <u>P</u> ing	Logout <u>R</u> efresh
CISCO	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	SECURITY	M <u>A</u> NAGE	MENT	COMMANDS	HELP	FEEDBAC	ж
Management	SNMP v1	/ v2c Co	ommunity								New
Summary											
▼ SNMP	Communit	y Name		IP Address	IP Mask	A	ccess Mo	de Statu	5		
General	cisco			10.4.48.0	255.255.2	55.0 R	ead-Only	Enable			
SNMP V3 Users Communities	cisco123			10.4.48.0	255.255.2	55.0 R	ead-Write	Enable			
Trap Receivers											
Trap Controls											
Trap Logs											
HTTP-HTTPS											
Telnet-SSH											
Serial Port											
Local Management Users											
User Sessions											
Logs											
Mgmt Via Wireless											
Software Activation											
Tech Support											

Procedure 10

(Optional)

In networks where network operational support is centralized you can increase network security by using an access control list in order to limit the networks that can access your controller. In this example, only devices on the 10.4.48.0/24 network are able to access the controller via SSH or SNMP.

Step 1: In Security > Access Control Lists > Access Control Lists, click New.

Step 2: Enter an access control list name, and then click Apply.

Step 3: In the list, choose the name of the access control list you just created, and then click Add New Rule.

Step 4: In the window, enter the following configuration details, and then click **Apply**.

- Sequence-1
- · Source-10.4.48.0 / 255.255.255.0
- Destination—Any
- · Protocol-TCP
- Destination Port—HTTPS
- Action—Permit

սիսիս									ıt <u>R</u> efre
CISCO	MONITOR WLANS	<u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK	
Security	Access Control L	ists > Rules >	New					< Back	Apply
► AAA	Sequence	1							
Local EAP				IP Addr		Netmask			
Priority Order	Source	IP Address	•	10.4.4	8.0	255.255.255.0			
Certificate	Destination	Any	-						
 Access Control Lists Access Control Lists 	Protocol	TCP	•						
CPU Access Control Lists FlexConnect ACLs	Source Port	Any	-						
Wireless Protection Policies	Destination Port	HTTPS	•						
Web Auth	DSCP	Any	•						
TrustSec SXP									
Advanced	Direction	Any	•						
	Action	Permit	•						

Step 5: Repeat Step 3 through Step 4 four more times, using the configuration details in the following table.

Sequence	Source	Destin ation	Protocol	Destin ation port	Action
2	10.4.48.0/ 255.255.255.0	Any	TCP	Other/22	Permit
3	Any	Any	TCP	HTTPS	Deny
4	Any	Any	TCP	Other/22	Deny
5	Any	Any	Any	Any	Permit

uluilu cisco	MON	TOR M	LANS <u>C</u> O	ONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK			Sage Conf	iguration [2ing Logout <u>R</u> e
Security	Acce	ess Con	trol Lists	> Edit									< Bac	. A	idd New Rule
AAA Local EAP Priority Order	Gene	e ral s List Nam		ACL-Rules											
 Certificate 		Counters		0											
 Access Control Lists Access Control Lists CPU Access Control 		Action	Source I			Destination IP/Mask		Protoco		Source Port	Dest Port	DSCP	Direction	Number of Hits	
Lists FlexConnect ACLs	1	Permit	10,4,48.0	/ 255	.255.255.0	0.0.0.0	/ 0.0.0.0	TCP	,	Any	HTTPS	Any	Any	0	
Wireless Protection	2	Permit	10,4,48.0	/ 255	.255.255.0	0.0.0.0	/ 0.0.0.0	TCP	,	Any	22	Any	Any	0	
Policies	3	Deny	0.0.0.0	/ 0.0	0.0	0.0.0.0	/ 0.0.0.0	TCP	,	Any	HTTPS	Any	Any	0	
Web Auth	4	Deny	0.0.0.0	/ 0.0	0.0	0.0.0.0	/ 0.0.0.0	TCP	,	Any	22	Any	Any	0	
TrustSec SXP	5	Permit	0.0.0.0	/ 0.0	0.0	0.0.0.0	/ 0.0.0.0	Any	,	Any	Any	Any	Any	0	
Advanced															

Step 6: In Security > Access Control Lists > CPU Access Control Lists, select Enable CPU ACL.

Step 7: In the ACL Name list, choose the ACL you just created, and then click Apply.

Procedure 11 Configure wireless user authentication

Step 1: In Security > AAA > RADIUS > Authentication, click New.

Step 2: Enter the Server IP Address. (Example: 10.4.48.15)

Step 3: Enter and confirm the Shared Secret. (Example: SecretKey)

Step 4: To the right of Management, clear Enable, and then click Apply.

ດໄທໄທ cisco	MONITOR WLANS CONTROL	LER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Security	RADIUS Authentication Se	ervers > New <a> Apply
AAA	Server Index (Priority)	1 -
General RADIUS	Server IP Address	10.4.48.15
Authentication Accounting	Shared Secret Format	ASCII 👻
Fallback	Shared Secret	••••••
TACACS+ LDAP	Confirm Shared Secret	•••••
Local Net Users	Key Wrap	(Designed for FIPS customers and requires a key wrap compliant RADIUS server)
MAC Filtering Disabled Clients	Port Number	1812
User Login Policies	Server Status	Enabled 🔻
AP Policies Password Policies	Support for RFC 3576	Enabled 👻
Local EAP	Server Timeout	2 seconds
Priority Order	Network User	C Enable
Certificate	Management	Enable
Access Control Lists	IPSec	Enable Enable
Wireless Protection Policies		
Web Auth		
TrustSec SXP		
Advanced		

Step 5: In Security > AAA > RADIUS > Accounting, click New.

Step 6: Enter the Server IP Address. (Example: 10.4.48.15)

Step 7: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)

(Optional)

You can use this procedure to deploy centralized management authentication by configuring an authentication, authorization and accounting (AAA) service. If you prefer to use local management authentication, skip to Procedure 13.

As networks scale in the number of devices to maintain, the operational burden to maintain local management accounts on every device also scales. A centralized Authentication, Authorization and Accounting (AAA) service reduces operational tasks per device and provides an audit log of user access for security compliance and root-cause analysis. When AAA is enabled for access control, it controls all management access to the network infrastructure devices (SSH and HTTPS).

Step 1: In Security > AAA > TACACS+ > Authentication, click New.

Step 2: Enter the Server IP Address. (Example: 10.4.48.15)

Step 3: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)



Step 4: In Security > AAA > TACACS+ > Accounting, click New.

Step 5: Enter the Server IP Address. (Example: 10.4.48.15)

Step 6: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)

cisco	MONITOR WLANS CONT	ROLLER WIRELESS SECUR	TY MANAGEMENT	COMMANDS	HELP FEEDBACK	
Security	TACACS+ Accounting	Servers > New			< Back	Apply
AAA General FADIUS FADIUS TACKCS+ Authentication Accounting Authorization LOAP Local Net Users MAC Filtering Diabled Clients User Login Policies Password Policies Password Policies Password Policies	Server Index (Priority) Server IP Address Shared Secret Format Shared Secret Confirm Shared Secret Port Number Server Status Server Timeout	1 • 10.4.48.15 ASCII • 49 Enabled • 5 seconds				
Priority Order						
Certificate						
Access Control Lists						
Wireless Protection Policies						
Web Auth						
TrustSec SXP						
Advanced						

Step 7: In Security > AAA > TACACS+ > Authorization, click New.

Step 8: Enter the Server IP Address. (Example: 10.4.48.15)

Step 9: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)

սիսիս						Sa <u>v</u> e Cor	nfiguration Ping	Logout <u>R</u> efresh
cisco	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBAC	к
Security	TACACS+ Autho	orization Serve	rs > New				< Back	Apply
AAA General AAAAI General Adotus TACACS+ Authentication Accounting Authorization LDAP Local Het Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies	Server Index (Prior Server IP Address Shared Secret Forn Shared Secret Confirm Shared Se Port Number Server Status Server Timeout	nat	1 • 10.4.48.15 ASCII • ••••••• 49 Enabled • 5 second	ls				
Local EAP								
Priority Order								
Certificate								
Access Control Lists								
Wireless Protection Policies								
Web Auth								
TrustSec SXP								
Advanced								

Step 10: Navigate to Security > Priority Order > Management User.

Step 11: Using the arrow buttons, move TACACS+ from the Not Used list to the Used for Authentication list.

Step 12: Using the Up and Down buttons, move TACACS+ to be the first in the Order Used for Authentication list.

Step 13: Using the arrow buttons, move **RADIUS** to the **Not Used** list, and then click **Apply**.

սիսիս										ogout <u>R</u> efresh
CISCO	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK	
Security	Priority C	Order > N	/lanagement l	Jser						Apply
 AAA Local EAP Priority Order Management User Certificate Access Control Lists Wireless Protection Policies Web Auth TrustSec SXP Advanced 	RADIU	Used JS	second priority th	en user will be	authenticated a	Up Dowr				

Procedure 13 Configure the resilient WLC

Step 1: This design uses two WLCs. The first is the primary WLC, and the access points register to it. The second WLC provides resiliency in case the primary WLC fails. Under normal operation, there will not be any access points registered to this WLC. Repeat Procedure 5 through Procedure 10 to configure the resilient AP-SSO secondary WLC.



Configure mobility groups

In the event that you are using two WLCs using AP SSO mode of operation (Cisco 5500 Series WLCs or Cisco Flex 7500 Series Cloud Controllers), you should skip this procedure. If you are using two or more WLCs without AP SSO (vWLCs), then complete this procedure in order to create a mobility group.

Step 1: On the primary controller, navigate to Controller > Mobility Management > Mobility Groups. The MAC address, IP address, and mobility group name for the local controller are shown on the Static Mobility Group Members page.

սիսիս						nfiguration Ping	Logout <u>R</u> efresh
cisco	MONITOR WLAN	Is <u>C</u> ONTROLLER	WIRELESS SE	CURITY MANAGEMENT	COMMANDS	HELP FEEDBACH	¢
Controller	Static Mobility	Group Member	s			New	EditAll
General Inventory	Local Mobility	Group REMOT	ES				
Interfaces	MAC Address	IP Address	Group Name	Multicast IP	Status		
Interface Groups	40:55:39:f6:1d	40 10.4.46.68	REMOTES	0.0.0.0	Up		
Multicast							
Network Routes							
Internal DHCP Server							
 Mobility Management Mobility Groups Mobility Anchor Config Multicast Messaging 							
Ports							
▶ NTP							
► CDP							
Advanced							

Step 2: On the resilient controller, navigate to Controller > Mobility Management > Mobility Groups, and then click New.

Step 3: In the **Member IP Address** box, enter the IP address of the primary controller. (Example: 10.4.46.68)

Step 4: In the Member MAC Address box, enter the MAC address of the primary controller, and then click Apply.

Step 5: On the primary controller, navigate to Controller > Mobility Management > Mobility Groups, and then click New.

Step 6: In the **Member IP Address** box, enter the IP address of the resilient controller. (Example: 10.4.46.69)

Step 7: In the Member MAC Address box, enter the MAC address of the resilient controller, and then click Apply.



Step 8: On each controller, click Save Configuration, and then click OK.

Step 9: Navigate to Controller > Mobility Management > Mobility Groups,

and then verify that connectivity is up between all the controllers by examining the mobility group information. In the Status column, all controllers should be listed as **Up**.

արտիս						nfiguration Ping	
CISCO	MONITOR WLANS	CONTROLLER	WIRELESS SECURI	TY M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP FEEDBACH	
Controller	Static Mobility G	roup Members	\$			New	EditAll
General			-				
Inventory	Local Mobility Gr	oup REMOTE	S				
Interfaces	MAC Address	IP Address	Group Name	Multicast IP	Status		
Interface Groups	40:55:39:f6:1d:40	10.4.46.68	REMOTES	0.0.0.0	Up		
Multicast Network Routes	00:24:97:69:a8:a	0 10.4.46.69	REMOTES	0.0.0.0	Up		
Internal DHCP Server							
 Mobility Management Mobility Groups Mobility Anchor Config Multicast Messaging 							
Ports							
NTP							
CDP							
Advanced							

Procedure 15

Configure the data wireless LAN

Wireless data traffic can handle delay, jitter, and packet loss more efficiently than wireless voice traffic. For the data WLAN, keep the default QoS settings and segment the data traffic onto the data wired VLAN.

Step 1: Navigate to WLANs.

Step 2: Click the WLAN ID number of the data SSID.

Step 3: On the General Tab, to the right of Status, select **Enabled** and then click **Apply**.

ululu cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u>	DNTROLLER WIRELESS SE		Sa <u>v</u> e Configurati MANDS HELP	on <u>P</u> ing Logout <u>R</u> efresh <u>F</u> EEDBACK
WLANs	WLANs				Entries 1 - 1 of 1
WLANS	Current Filter: None	[Change Filter] [Clear Filter]	Create Ne	ew 🔻 Go	2
Advanced	WLAN ID Type	Profile Name	WLAN SSID	Admin Status See	curity Policies
	1 WLAN	WLAN-Data	WLAN-Data	Enabled [W	PA2][Auth(802.1X)]

Step 4: On the Advanced tab disable mDNS Snooping as this is not supported with FlexConnect Local Switching. Next, enable FlexConnect Local Switching by selecting **Enabled**, and then click **Apply**.

սիսիս		gout <u>R</u> efr
cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK	
WLANs	WLANs>Edit 'WLAN-Data-RS201'	Apply
 ₩LANs WLANs Advanced 	General Security QoS Advanced (15:100000) Jow Jow Media Session Snooping Enabled Client uprid th treshold 0 Bytes Re-anchor Reamed Vaice Clients Enabled Off Channel Scanning Defer KTS based CAC Policy Enabled Scan Defer Prority 0 1 2 4 5 7 DHCP Profiling DHCP Profiling Image: Comparison of the second s	
	Scan Dafer HTTP Profiling Time(msecs) 100 mDNS FlexConnect mDNS Snooping Enabled	
	FlexConnect Local IV Switching & IV FlexConnect Local Auth Enabled Learn Client IP Address & IV Van based Central Enabled Switching Enabled	н
	Central DHCP Processing C Inabled Override DNS Enabled	-

Procedure 16

Configure the voice wireless LAN

Wireless voice traffic is unique among other types of data traffic in that it cannot effectively handle delay and jitter or packet loss. To configure the voice WLAN, change the default QoS settings to Platinum and segment the voice traffic onto the voice wired VLAN.

Step 1: On the WLANs page, in the list, choose Create New, and then click Go.

	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY MANAGEMENT	Sa <u>v</u> e Configur C <u>O</u> MMANDS HE	ation <u>P</u> ing Logout <u>R</u> efresh LP <u>F</u> EEDBACK
WLANS WLANS	WLANs Current Filter: Not	e [Change Filter] [Clear	Filter] Cru	ate New 👻	Entries 1 - 1 of 1
Advanced	U Type ID Type 1 WLAN	Profile Name WLAH-Data	WLAN SSID WLAN-Data		Security Policies [WPA2][Auth(802.1X]]

Step 2: Enter the Profile Name. (Example: Voice)

Step 3: In the **SSID** box, enter the voice WLAN name, and then click **Apply**. (Example: WLAN-Voice)

uluili. cisco	MONITOR WLANS	<u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	Sa <u>v</u> e Cor C <u>O</u> MMANDS	figuration <u>Ping</u> L HELP <u>F</u> EEDBACK	
WLANS WLANS WLANS Advanced	WLANS > New Type Profile Name SSID ID	WLAN Voice WLAN 2	-Voice				< Back	Apply

Step 4: On the Advanced tab disable mDNS Snooping as this is not supported with FlexConnect Local Switching. Next, enable FlexConnect Local Switching by selecting **Enabled**, and then click **Apply**.

uludu cisco	Saye Configuration Monitor <u>w</u> lanis <u>c</u> ontroller wireless security management commands help eeedback	<u>Ping</u> Logout <u>R</u> efre
WLANs	WLANs>Edit 'Voice'	Apply
WLANs Advanced	General Security Q45 Advanced 100000) 300 Basive Client 00 Client user idle threshold (0) 0 Passive Client 0	*
	10000000) Voice Voice	
	Scan Defer Priority 0 I Z 3 4 5 6 7 Re-anchor Reamed Voice Clients Enabled Image: Comparison of the second se	
	Scan Defer Time 100 Client Profiling	
	FlexConnect HTTP Profiling	П
	FlexConnect Local Image: Connect Local Image: Conne	
Vlan ba Switchit Central	Learn Client IP Address # Enabled Vian based Central Switching ## Enabled	E
	Central DHCP Processing Enabled	
	Override DNS Enabled NAT-PAT Enabled	
	€ [•

Step 5: On the QoS tab, in the Quality of Service (QoS) list, choose Platinum (voice), and then click Apply.

ւվովո cisco	MONITOR WLANS CONT	OLLER WIRELESS S	ECURITY MANAGEMENT	COMMANDS HEL	P EEEDBACK	Sa <u>v</u> e Configuration <u>P</u> ing Logout <u>B</u> e
WLANs	WLANs > Edit 'Voice'					< Back Apply
 ₩LANS ₩LASS Advanced 	General Security Quality of Service (QoS) Application Visibility AUX Profile Netflow Monitor Override Per-User Band Average Data Rate Burt Date Beh Average Real-Time Rate Burt Seal-Time Rate Burt Seal-Time Rate	QoS Advanced Plathnum (voice) Enabled none width Contracts (kbp DownStream UpStre 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0				8
	Override Per-SSID Band	width Contracts (kbp	s) #			
	Average Data Rate Burst Data Rate	DownStream UpStre 0 0 0 0		77		

Step 6: On the General tab, to the right of Status, select **Enabled**, and then click **Apply**.

սիսիս cisco	MONITOR WLANS CONTRO	LLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK	Sa <u>v</u> e Configuration <u>P</u> ing Logout <u>R</u> efre
/LANs	WLANs > Edit 'Voice'		< Back Apply
WLANS WLANS	General Security Q	DS Advanced	
Advanced	Profile Name	Voice	
	Туре	WLAN	
	SSID	WLAN-Voice	
	Status	I Enabled	
	Security Policies	[WPA2][Auth(882.1X)] (Modifications done under security tab will appear after applying the changes.)	
	Radio Policy	All	
	Interface/Interface Group(G	management 👻	
	Multicast Vlan Feature	Enabled	
	Broadcast SSID	Enabled	
	NAS-ID	WLC-RemoteSites-1	

Procedure 17

Configure controller discovery

You have three options to configure controller discovery, depending on the number of controller pairs and the type of DHCP server you've deployed.

If you have only one controller pair in your organization, complete Option 1 of this procedure.

If you have deployed multiple controller pairs in your organization and you use Cisco IOS software in order to provide DHCP service, complete Option 2. If you have deployed multiple controller pairs in your organization and you use a Microsoft DHCP server, complete Option 3.

Figure 6 - Flow chart of WLC discovery configuration options



Option 1. Only one WLC pair in the organization

If AP SSO is being used, the WLC pair is represented by a single IP address, that being the management address of the primary WLC. The resilient secondary controller will assume the IP address of the primary in the event the primary WLC fails.

Step 1: Configure the organization's DNS servers (Example: 10.4.48.10) to resolve the **cisco-capwap-controller** host name to the management IP address of the controller. (Example: 10.4.46.64) The cisco-capwap-controller DNS record provides bootstrap information for access points that run software version 6.0 and higher.

Step 2: If the network includes access points that run software older than version 6.0, add a DNS record to resolve the host name **cisco-lwapp-controller** to the management IP address of the controller.

Option 2. Multiple WLC pairs in the organization: Cisco IOS DHCP server

In a network where there is no external central site DHCP server you can provide DHCP service with Cisco IOS software. This function can also be useful at a remote-site where you want to provide local DHCP service and not depend on the WAN link to an external central-site DHCP server.

Step 1: Assemble the DHCP Option 43 value.

The hexadecimal string is assembled as a sequence of the Type + Length + Value (TLV) values for the Option 43 suboption, as follows:

- Type is always the suboption code 0xf1.
- Length is the number of controller management IP addresses times 4 in hex.
- · Value is the IP address of the controller listed sequentially in hex.

For example, suppose there are two controllers with management interface IP addresses, 10.4.46.64 and 10.4.46.65. The type is 0xf1. The length is 2 * 4 = 8 = 0x08. The IP addresses translate to 0a042e44 (10.4.46.68) and 0a042e45(10.4.46.69). When the string is assembled, it yields f1080a042e440a042e45.

Step 2: On the network device, add Option 43 to the pre-existing data network DHCP Pool.

ip dhcp pool [pool name]
 option 43 hex [f1080a042e440a042e45]

Option 3. Multiple WLC pairs in the organization: Microsoft DHCP server

This procedure shows how the Microsoft DHCP server is configured to return vendor-specific information to the lightweight Cisco Aironet 1600, 2600, and 3600 Series Access Points used in this deployment guide. The vendor class identifier for a lightweight Cisco Aironet access point is specific to each model type. To support more than one access point model, you must create a vendor class for each model type.

Table 6 - Vendor class identifiers

Access point	Vendor class identifier
Cisco Aironet 1600 Series	Cisco AP c1600
Cisco Aironet 2600 Series	Cisco AP c2600
Cisco Aironet 3600 Series	Cisco AP c3600

Step 1: Open the DHCP Server Administration Tool or MMC.

Step 2: Navigate to DHCP > ad.cisco.local, right-click IPv4, and then click Define Vendor Classes.

Y DHCP		-	E ×
File Action View Help			
(= =) 🖄 📷 💥 🔛 🍳 📄 🔢 📷			
PHCP id.csco.local i	Name	Actions	
ad.cisco.local	IPv4 IPv6	ad.cisco.local	-
Display Statistics	1940	More Actions	•
New Scope			
New Superscope New Multicast Scope			
Define User Classes			
Define Vendor Classes			
Reconcile All Scopes			
Set Predefined Options			
Refresh			
Properties			
Help			
		1	
		1	
		1	
Define vendor specific option classes	1	,	
L			

Step 3: In the DHCP Vendor Classes dialog box, click Add.

Name	Description	A <u>d</u> d
Microsoft Windows 20 Microsoft Windows 98 Microsoft Options	Microsoft vendor-specific option Microsoft vendor-specific option Microsoft vendor-specific option	Edit

Step 4: In the New Class dialog box, enter a **Display Name**. (Example: Cisco Aironet 1600 AP)

Step 5: In the ASCII section, enter the vendor class identifier for the appropriate access point series from Table 6, and then click **OK**. (Example: Cisco AP c1600)

Step 6: In the DHCP Vendor Classes dialog box, click Close.

🖞 DHCP	_ 🗆 ×
File Action View Help	
💠 🏟 🖄 📷 💥 🖹 🖻 😹 🔢 🖬	
PHCP Name Actions	
ad.cisco.local	-
E E E E E E	•
DHCP Vendor Classes	
Available classes:	
Name Description Add	
Mi New Class	
Mi Display name: Cis Cisco Aironet 1600 AP	
Cis	
Cis Description:	
L~ ID: Binary: ASUI:	
0000 43 69 73 63 67 20 41 50 CISED AF 0008 20 63 31 36 30 30 CISED AF C1600	
OK Cancel	

Step 7: Right-click the IPV4 DHCP server root, and then click Set Predefined Options.

Step 8: In the Option Class list, choose the class you just created, and then click Add.

Predefined Options a	nd ¥alues	? ×
Option class:	Cisco Aironet 1600 AP	▼
Option name:		•
	Add Edit	Delete
Description:		
- Value		
	ОК	Cancel

Step 9: In the Option Type dialog box, enter a Name. (Example: Option 43)

Step 10: In the Data Type list, choose IP Address.

Step 11: Select Array.

Step 12: In the Code box, enter 241, and then click OK.

Change Option Name 🔹 🔋 🗙		
Class:	Cisco Aironet 1600 AP	
<u>N</u> ame:	Option 43	
Data type:	IP Address 🔽 🗹 Array	
<u>C</u> ode:	241	
D <u>e</u> scription:	l	
	OK Cancel	

The vendor class and suboption are now programmed into the DHCP server. Now, you need to define the vendor-specific information for the DHCP scope.

Step 13: Choose the DHCP that you will be installing access points on then Right-click **Scope Options**, and then click **Configure Options**.

Step 14: Click the **Advanced** tab, and then in the **Vendor class** list, choose the class you created in this procedure. (Example: Cisco Aironet 1600 AP)

Step 15: Under Available Options, select 241 Option 43.

Step 16: In the **IP address** box, enter the IP address of the primary controller's management interface, and then click **Add**. (Example: 10.4.46.68)

Scope Options	? ×
General Advanced	
Vendor class:	Cisco Aironet 1600 AP
User class:	Default User Class
Available Options 241 Option 43	Description
^I Data entry Server name:	Resolve
IP address:	
	Add
10.4.46.68	Remove
	Up
	Down
	OK Cancel Apply

Step 17: If you are not using AP-SSO, it is necessary to repeat Step 16 for the resilient controller, and then click **Apply**. (Example: 10.4.46.69)

Configure the remote-site router

Remote-site routers require additional configuration in order to support wireless VLANs. If you have a single WAN remote-site router, complete Option 1 of this procedure. If you have dual remote-site routers, complete Option 2.

Option 1. Single WAN remote-site router

Step 1: Create wireless data and voice sub-interfaces on the router's interface that connects to the access layer switch. The interface will be a physical interface when the connection is a single link, and it will be a logical port-channel interface when the connection is EtherChannel.

interface GigabitEthernet0/2.65
description Wireless Data
encapsulation dot1Q 65
ip address 10.5.42.1 255.255.255.0
ip helper-address 10.4.48.10
ip pim sparse-mode
!
interface GigabitEthernet0/2.70
description Wireless Voice
encapsulation dot1Q 70
ip address 10.5.43.1 255.255.255.0
ip helper-address 10.4.48.10
ip pim sparse-mode

Step 2: If application optimization is deployed at the remote site as described in the *Cisco SBA—Borderless Networks Application Optimization Deployment Guide*, configure Web Cache Communication Protocol (WCCP) redirection on the router's wireless data interface.

interface GigabitEthernet0/2.65
description Wireless Data
ip wccp 61 redirect in

Step 3: If the network does not have a central-site DHCP server, configure the Cisco IOS software DHCP service on the router.

ip dhcp excluded-address 10.5.42.1 10.5.42.10

ip dhcp excluded-address 10.5.43.1 10.5.43.10

ip dhcp pool WLAN-Data
network 10.5.42.0 255.255.255.0
default-router 10.5.42.1
domain-name cisco.local
dns-server 10.4.48.10
ip dhcp pool WLAN-Voice
network 10.5.43.0 255.255.255.0
default-router 10.5.43.1
domain-name cisco.local
dns-server 10.4.48.10

Option 2. Dual WAN remote-site routers

Step 1: On the primary router, create wireless data and voice sub-interfaces on the interface that connects to the access layer switch. The interface will be a physical interface when the connection is a single link, and it will be a logical port-channel interface when the connection is EtherChannel.

interface GigabitEthernet0/2.65 description Wireless Data encapsulation dot1Q 65 ip address 10.5.42.2 255.255.255.0 ip helper-address 10.4.48.10 ip pim dr-priority 110 ip pim sparse-mode standby version 2 standby 1 ip 10.5.42.1 standby 1 priority 110 standby 1 preempt standby 1 authentication md5 key-string cisco123 standby 1 track 50 decrement 10 T interface GigabitEthernet0/2.70 description Wireless Voice encapsulation dot1Q 70 ip address 10.5.43.2 255.255.255.0 ip helper-address 10.4.48.10 ip pim dr-priority 110 ip pim sparse-mode
standby version 2
standby 1 ip 10.5.43.1
standby 1 priority 110
standby 1 preempt
standby 1 authentication md5 key-string cisco123
standby 1 track 50 decrement 10

Step 2: On the secondary router, create wireless data and voice sub-interfaces on the interface that connects to the access layer switch. The interface will be a physical interface when the connection is a single link, and a logical port-channel interface when the connection is EtherChannel.

```
interface GigabitEthernet0/2.65
description Wireless Data
encapsulation dot10 65
 ip address 10.5.42.3 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 105
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.42.1
 standby 1 priority 105
 standby 1 preempt
 standby 1 authentication md5 key-string cisco123
T.
interface GigabitEthernet0/2.70
description Wireless Voice
encapsulation dot10 70
 ip address 10.5.43.3 255.255.255.0
 ip helper-address 10.4.48.10
 ip pim dr-priority 105
 ip pim sparse-mode
 standby version 2
 standby 1 ip 10.5.43.1
 standby 1 priority 105
 standby 1 preempt
 standby 1 authentication md5 key-string cisco123
```

Step 3: If application optimization is deployed at the remote site as described in the *Cisco SBA—Borderless Networks Application Optimization Deployment Guide*, configure WCCP redirection on both the primary and secondary router.

interface GigabitEthernet0/2.65
description Wireless Data
ip wccp 61 redirect in

Procedure 19

Configure the remote-site switch for APs

Before remote-site switches can offer the appropriate trunk behavior to access points configured for Cisco FlexConnect wireless switching, you must reconfigure the switch interfaces connected to the access points. For consistency and modularity, configure all WAN remote sites that have a single access switch or switch stack to use the same VLAN assignment scheme.

Step 1: On the remote-site switch, create the data and voice wireless VLANs.

vlan 65 name WLAN_Data vlan 70 name WLAN_Voice

Step 2: Configure the existing interface where the router is connected to allow the wireless VLANs across the trunk. If there are two routers at the site, configure both interfaces.

interface GigabitEthernet 1/0/24
switchport trunk allowed vlan add 65,70

Step 3: Reset the switch interface where the wireless access point will connect to its default configuration.

default interface GigabitEthernet 1/0/23

Step 4: Configure the interface to which the access point will connect to allow a VLAN trunk for remote-site VLANs.

Tech Tip

The Inter-Switch Link trunking protocol is supported on Cisco Catalyst 3750-X Series Switches but not supported on Cisco Catalyst 2960s and 4500 Series Switches. As such, you do not need to specify the trunk encapsulation type on Catalyst 2960 and 4500 Series switches, but you do need to specify it on Catalyst 3750 Series switches.

interface GigabitEthernet 1/0/23

description FlexConnect Access Point Connection
switchport trunk encapsulation dot1q
switchport trunk native vlan 64
switchport trunk allowed vlan 64,65,70
switchport mode trunk
switchport port-security maximum 255
spanning-tree portfast trunk
macro apply EgressQoS

Procedure 20

Enable licensing on the vWLC

The Wireless LAN Controller virtual Appliance OVA includes a temporary 60-day license that includes 200 access points. After you acquire a permanent license from licensing@cisco.com, you must install and activate it, using the same steps below. To activate the demo license included with the vWLC deployment, complete the following steps.



Tech Tip

Failure to activate the demo licenses will result in the inability for the access point to register with the vWLC

Step 1: On the vWLC, navigate to Management > Software Activation > Licensing.

Step 2: Change the Priority to **High** using the Set Priority button and press **Apply**.

Step 3: Accept the License and click OK and Apply.

Step 4: Reboot the vWLC by navigating to Commands > Reboot > Save and Reboot.

Procedure 21

Configure the AP for Cisco FlexConnect

Step 1: Connect the access point to the remote-site switch, and then wait for the light on the access point to turn a solid color.

Step 2: On the WLC's web interface, navigate to Wireless > Access Points.

Step 3: Select the AP Name of the access point you want to configure.

Step 4: If the access points were not previously registered to the WLC prior to issuing the **autoconvert** command in Step 18 of Procedure 7, skip this step.

If the access points were registered to the WLC prior to issuing the **autoconvert** command, on the General tab, in the **AP Mode** list, choose **FlexConnect**, and then click **Apply**. Wait for the access point to reboot and reconnect to the controller. This should take approximately three minutes.

CISCO	MONITOR	WLANS CONTR	OLLER WIRELE	SS <u>S</u> ECURITY	MANAGEMENT	COMMANDS	HELP FEEDBACK	
ireless	All APs > I	Details for AP	4d3.ca42.309	d			< Back	Apply
Access Points	General	Credentials	Interfaces	High Availabilit	y Inventor	y Advanced		
Radios 802.11a/n 802.11b/a/n	General				Versions			
Global Configuration	AP Name	e	AP44d3.ca42.309d		Primary So	ftware Version	7.2.104.16	
Advanced	Location		default location		Backup Sof	ftware Version	0.0.0.0	
Mesh	AP MAC	Address	44:d3:ca:42:30:90		Predownloa	ad Status	None	
RF Profiles	Base Ra	dio MAC	64:d9:89:42:28:e0)	Predownloa	aded Version	None	
FlexConnect Groups	Admin S	tatus	Enable 👻		Predownloa	ad Next Retry Tim	e NA	
FlexConnect ACLs	AP Mode		FlexConnect -		Predownloa	ad Retry Count	NA	
802.11a/n	AP Sub I	Mode	None 🔻		Boot Versio	on	12.4.2.4	
802.11b/g/n	Operatio	inal Status	REG		IOS Version	n	12.4(20120312:1	34417)\$
Media Stream	Port Nur	nber	LAG		Mini IOS Ve	ersion	7.0.114.214	
Country	Venue G	iroup	Unspecified	•	IP Config			
Timers	Venue T	ype	Unspecified 👻		IP Address		10.4.128.10	
QoS	Venue N	lame			Static IP			
	Languag	e						
		Spectrum	18551F89B90500F	6FC39DDA8279C16D	Time Statistic	cs		
	Interface	е кеу			UP Time		0 d, 00 h 46 m 45	s
					Controller A	Associated Time	0 d, 00 h 45 m 35	s
					Controller /	Association Latenc	y 0 d, 00 h 01 m 09	s
	Hardware	Reset		Set to Fa	ctory Defaults			
		a hardware reset o	n this AP	defaul	configuration on th ts ar All Config	iis AP and reset it	to factory	
				Clea	ar Config Except	Static IP		
	Foot Note							

Step 5: In Wireless > Access Points, select the same access point as in Step 3.

Step 6: On the FlexConnect tab, select VLAN Support.

Step 7: In the **Native VLAN ID** box, enter the trunk's native VLAN number as configured in Procedure 17, and then click **Apply**. (Example: 64)

 ahahas s 								Logout <u>R</u> efr
CISCO	MONITOR WI	LANS <u>C</u> ONTR	OLLER WIREL	ESS <u>S</u> ECURITY	MANAGEMENT	COMMANDS H	IELP <u>F</u> EEC	DBACK
Vireless	All APs > Det	tails for RS2	01-CAP3602I				< Back	Apply
 Access Points All APs Radios	General	Credentials	Interfaces	High Availabilit	y Inventory	FlexConnect	Advanc	ced
Global Configuration Advanced Mesh RF Profiles FlexConnect Groups HacConnect ACLs 802.11a/n 802.11a/n 802.11b/g/n Media Stream Country Timers QoS	Support Native VLAN ID FlexConnec Group Nam PreAuthentic	e Not Conngu ation Access (abAuthentication AP idst	Control Lists	8				
	Foot Notes 1 DNS server	IP Address and	the Domain name	can be set only afte	er a valid static IP i	s pushed to the AP.		

Step 8: Click VLAN Mappings.

Step 9: For the data WLAN, in the **VLAN ID** box, enter the VLAN number from Procedure 17. (Example: 65)

Step 10: For the voice WLAN, in the **VLAN ID** box, enter the VLAN number from Procedure 17, and then click **Apply**. (Example: 70)

սիսիս cısco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	Sa <u>v</u> e Configu C <u>O</u> MMANDS	ration HELP	<u>Ping</u> Logout <u>R</u> efr <u>F</u> EEDBACK
Wireless	All APs >	RS201-0	CAP3602I > VL	AN Mappir	igs			< Back	Apply
Access Points All APs Radios 802.11a/n	AP Name Base Rad		S201-CAP3602I 4:d9:89:47:14:20						
802.11b/g/n Global Configuration	WLAN Id	SSID			VLAN ID				
Advanced	1	WLAN-Data			65				
Mesh RF Profiles	2	WLAN-Voice			70				
FlexConnect Groups	Centrally	switched	Wlans						
FlexConnect ACLs	WLAN Id		SSID	VLAN ID					
 802.11a/n 802.11b/g/n 	AP level \	LAN ACL	Mapping						
Media Stream	Vlan Id	Ingr	ess ACL	Egress A	CL				
Country	146	none	-	none 🔻					
Timers	Crown Iou		CL Mapping						
QoS	Vlan Id		ess ACL	Egress A	CL				

Procedure 22

Configure access points for resiliency

If you are using the AP SSO high availability feature on a Cisco 5500 Series WLC or Cisco Flex 7500 Series Cloud Controller, you can skip this procedure, as the resilient controller automatically tracks the primary controller and assumes its IP address in the event of a failure. The AP SSO feature is not available on the virtual wireless LAN controller (vWLC).

Step 1: On the primary WLC, navigate to **Wireless**, and then select the desired access point. If the access point is not listed, check the resilient WLC.

Step 2: Click the High Availability tab.

Step 3: In the **Primary Controller** box, enter the name and management IP address of the primary WLC. (Example: WLC-RemoteSites-1 / 10.4.46.68)

Step 4: In the **Secondary Controller** box, enter the name and management IP address of the resilient WLC, and then click **Apply**. (Example: WLC-RemoteSites-2 / 10.4.46.69)

cisco	Save Configuration Ping Logout	<u>R</u> ef
Vireless	All APs > Details for R\$201-CAP36021 < Back Appl	y
Access Points	General Credentials Interfaces High Availability Inventory FlexConnect Advanced	
 Radios 802.11a/n 802.11b/g/n 	Name Management IP Address	
Global Configuration	Primary Controller WLC-RemoteSites-1 10.4.46.68	
Advanced	Secondary Controller WLC-RemoteSites-2 10.4.46.69	
Mesh	Tertiary Controller	
RF Profiles		
FlexConnect Groups FlexConnect ACLs	AP Failover Priority Low	
802.11a/n		
802.11b/g/n		
Media Stream		
Country		
Timers		
QoS		
	Foot Notes	
	1 DNS server IP Address and the Domain name can be set only after a valid static IP is pushed to the AP.	



Configure Cisco FlexConnect groups

Step 1: On the WLC, navigate to Wireless > FlexConnect Groups, and then click New.

Step 2: In the **Group Name** box, enter a name that will allow you to associate the group with the remote site, and then click **Apply**. (Example: Remote-Site 1)

Step 3: Under Group Name, click the group you just created.

Step 4: Under Add AP, select Select APs from current controller.

Step 5: In the AP Name list, choose an access point that is located at the site, and then click Add.

Step 6: Repeat the previous step for every access point at the site.

Step 7: Under AAA, enter the Server IP Address, Shared Secret and then click Add, then click Apply.

Step 8: Repeat Procedure 23 for each remote site.

Process

Configuring Guest Wireless: Shared Guest Controller

- 1. Configure the distribution switch
- 2. Configure the firewall DMZ interface
- 3. Configure Network Address Translation
- 4. Configure guest network security policy
- 5. Create the guest wireless LAN interface
- 6. Configure the guest wireless LAN
- 7. Create the lobby admin user account
- 8. Create guest accounts

Procedure 1

Configure the distribution switch

The VLAN used in the following configuration examples is:

Guest Wireless—VLAN 1128, IP: 192.168.28.0/22

switchport trunk allowed vlan add 1128

Step 1: On the LAN distribution switch, for Layer 2 configuration, create the guest wireless VLAN.

vlan **1128**

name Guest_Wireless

Step 2: Configure the interfaces that connect to the Internet edge firewalls by adding the wireless VLAN.

interface GigabitEthernet1/0/24
description IE-ASA5540a Gig0/1
!
interface GigabitEthernet2/0/24
description IE-ASA5540b Gig0/1
!
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24

Step 3: Configure the interfaces that connect to the WLCs by adding the wireless VLAN.

```
interface Port-channel [WLC #1 number]
description WLC-1 LAG
!
interface Port-channel [WLC #2 number]
description WLC-2 LAG
!
interface range Port-channel [WLC #1 number], Port-channel
[WLC #2 number]
switchport trunk allowed vlan add 1128
```

Procedure 2

Configure the firewall DMZ interface

Typically, the firewall *DMZ* is a portion of the network where traffic to and from other parts of the network is tightly restricted. Organizations place network services in a DMZ for exposure to the Internet; these services are typically not allowed to initiate connections to the inside network, except for specific circumstances.

The guest DMZ is connected to Cisco Adaptive Security Appliances (ASA) on the appliances' internal Gigabit Ethernet interface via a VLAN trunk. The IP address assigned to the VLAN interface on the appliance is the default gateway for that DMZ subnet. The internal distribution switch's VLAN interface does not have an IP address assigned for the DMZ VLAN.

Table 7 - Cisco ASA DMZ interface information

Interface Label	IP Address & Netmask	VLAN	Security Level	Name
GigabitEthernet0/ 0.1128	192.168.28.1/22	1128	10	dmz-guests

Step 1: Login to the Internet Edge firewall using Cisco Adaptive Security Device Manager (Cisco ASDM).

Step 2: Navigate to Configuration -> Device Setup ->Interfaces.

Step 3: On the Interface pane, click Add > Interface.

Step 4: In the **Hardware Port** list, choose the interface that is connected to the internal LAN distribution switch. (Example: GigabitEthernet0/0)

Step 5: In the **VLAN ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1128)

Step 6: In the **Subinterface ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1128)

Step 7: Enter an Interface Name. (Example: dmz-guests)

Step 8: In the Security Level box, enter a value of 10.

Step 9: Enter the interface IP Address. (Example: 192.168.28.1)

Step 10: Enter the interface **Subnet Mask**, and then click **OK**. (Example: 255.255.252.0)

🔂 Add Interface
General Advanced IPv6
Hardware Port: GigabitEthernet0/1 -
VLAN ID: 1128
Subinterface ID: 1128
Interface Name: dmz-guests
Security Level: 10
Dedicate this interface to management only
Channel Group:
IP Address
© Use Static IP ○ Obtain Address via DHCP ○ Use PPPoE
IP Address: 192.168.28.1
Subnet Mask: 255.255.252.0 -
Description:
OK Cancel Help

Step 11: Navigate to Configuration > Device Management > High Availability > Failover.

Step 12: On the Interfaces tab, in the **Standby IP address** column, enter the IP address of the standby unit for the interface you just created. (Example: 192.168.28.2)

Step 13: Select Monitored, and then click Apply.

Interface Name	Name	Active IP Address	Subnet Mask/ Prefix Length	Standby IP Address	Monitored
GigabitEthernet0/0.300	inside	3 10.4.24.30	255.255.255.224	3 10.4.24.29	
GigabitEthernet0/1.1116	dmz-web	3 192.168.16.1	255.255.255.0	3 192.168.16.2	
<u></u>		🖳 2001:db8:	64	📇 2001:db8:a:	
GigabitEthernet0/1.1117	dmz-email	3 192.168.17.1	255.255.255.0	3 192.168.17.2	
GigabitEthernet0/1.1118	dmz-dmvpn	3 192.168.18.1	255.255.255.0	3 192.168.18.2	
GigabitEthernet0/1.1119	dmz-wlc	3 192.168.19.1	255.255.255.0	3 192.168.19.2	
GigabitEthernet0/1.1123	dmz-management	3 192.168.23.1	255.255.255.0	3 192.168.23.2	
GigabitEthernet0/1.1128	dmz-guests	192.168.28.1	255.255.252.0	92.168.28.2	
GigabitEthernet0/3.16	outside-16	3 172.16.13	255.255.255.0	3 172.16.130	
L		🖳 2001:db8:	64	📇 2001:db8:a::2	
GigabitEthernet0/3.17	outside-17	3 172.17.13	255.255.255.0		
Management0/0	IPS-mgmt				V

Step 14: At the bottom of the window, click **Apply**. This saves the configuration.

Procedure 3

Configure Network Address Translation

The DMZ network uses private network (RFC 1918) addressing that is not Internet-routable, so the firewall must translate the DMZ address of the guest clients to an outside public address.

Step 1: Navigate to Configuration > Firewall > Objects > Network Objects/Groups.

Step 2: Click Add > Network Object.

Step 3: In the Add Network Object dialog box, in the **Name** box, enter a description for the guest network. (Example: dmz-guests-network-ISPa)

Step 4: In the Type list, choose Network.

Step 5: In the **IP Address** box, enter the guest DMZ network address. (Example: 192.168.28.0)

- Step 6: Enter the guest DMZ netmask. (Example: 255.255.252.0)
- Step 7: Click the two down arrows. The NAT pane expands.
- Step 8: Select Add Automatic Address Translation Rules.
- Step 9: In the Type list, choose Dynamic PAT (Hide).

Step 10: In the **Translated Addr** list, choose the interface name for the primary Internet connection. (Example: outside-16)

📴 Add Network	: Object
Name:	dmz-guest-network-ISPa
Туре:	Network
IP Version:	IPv4
IP Address:	192.168.28.0
Netmask:	255.255.252.0
Description:	DMZ outside PAT address for ISPa
NAT	*
🚺 Add Autom	atic Address Translation Rules
Туре:	Dynamic PAT (Hide) 👻
Translated A	ddr: outside-16
Use one-	to-one address translation
PAT Pool	Translated Address:
Round	Robin
Extend	d PAT uniqueness to per destination instead of per interface
Transl	ate TCP and UDP ports into flat range 1024-65535 📃 Include range 1-1023
Fall throu	ugh to interface PAT(dest intf): IPS-mgmt 🚽
📃 Use IPv6	i for interface PAT
	Advanced
	OK Cancel Help

Step 11: Click Advanced.

Step 12: In the **Destination Interface** list, choose the interface name for the primary Internet connection, and then click **OK**. (Example: outside-16)

屆 Advanced NAT Settin	ngs 🔀					
Translate DNS repli	es for rule					
Disable Proxy ARP	Disable Proxy ARP on egress interface					
Lookup route table	to locate egress interface					
Interface						
Source Interface:	Any 👻					
Destination Interface:	outside-16 👻					
Service						
Protocol:	rœ≻ tcp 👻					
Real Port:						
Mapped Port:						
OK	Cancel Help					

Step 13: In the Add Network Object dialog box, click OK.



Step 1: Navigate to Configuration > Firewall > Access Rules.

Step 2: Click the rule that denies traffic from the DMZ toward other networks.

First, you enable the guests to communicate with the DNS and DHCP servers in the data center.

IP ip

🔞 Denv

Step 3: Click Add > Insert.

24 🔽 🛤 dmz-networks

Step 4: In the Interface list, choose Any.

Step 5: In the **Source** list, choose the network object automatically created for the guest DMZ. (Example: dmz-guests-network/22)

Step 6: In the **Destination** list, choose the network object for the DNS server. (Example: internal-dns)

Step 7: In the Service list, enter udp/domain, tcp/domain, and then click OK.

📴 Insert Access	Rule
Interface:	Any 🔹
Action: 💿 Pern	nit 🔘 Deny
Source Criteria	
Source:	dmz-guests-network/22
User:	
Security Group:	
Destination Crite	ria
Destination:	internal-dns -
Security Group:	
Service:	udp/domain, tcp/domain
Description:	Allow Guest Wireless users to resolve DNS names.
🔽 Enable Loggi	ng
Logging Leve	l: Default 👻
More Options	*
	OK Cancel Help

Step 8: Click Add > Insert.

Step 9: In the Interface list, choose Any.

Step 10: In the **Source** list, choose the network object automatically created for the guest DMZ. (Example: dmz-guests-network/22)

Step 11: In the **Destination** list, choose the network object for the DHCP server. (Example: internal-dhcp)

Step 12: In the Service list, enter udp/bootps, and then click OK.

🔂 Add Access I	Rule	x
Interface:	Any 👻	
Action: 💿 Pern	mit 💿 Deny	
Source Criteria		_
Source:	dmz-guests-network/22	
User:		
Security Group:		
Destination Crite	eria	-
Destination:	internal-dhcp 💼	
Security Group:		
Service:	udp/bootps	
Description:	Allow Hosts on DMZ Guest Network access to DHCP server for IP address assignment.	
📝 Enable Logg	ing	
Logging Leve	el: Default 🗸	
More Options		*
	OK Cancel Help	

Next, you enable the guests to communicate with the web servers in the DMZ.

Step 13: Click Add > Insert.

Step 14: In the Interface list, choose Any.

Step 15: In the **Source** list, choose the network object automatically created for the guest DMZ. (Example: dmz-guests-network/22)

Step 16: In the **Destination** list, choose the network object automatically created for the web DMZ. (Example: dmz-web-network/24)

Step 17: In the Service list, enter tcp/http, tcp/https, and then click OK.

insert Access	Rule
Interface:	Any 🔹
Action: 💿 Pern	nit 💿 Deny
Source Criteria	
Source:	dmz-guests-network/22
User:	
Security Group:	
Destination Crite	
Destination:	dmz-web-network/24
Security Group:	
Service:	tcp/http, tcp/https
Description:	All wireless guest users access to DMZ based webservers, possibly for walled garden access
📝 Enable Loggi	ing
Logging Leve	el: Default 👻
More Options	*
	OK Cancel Help

Next, you remove the guest's ability communicate with other internal and DMZ devices.

Step 18: Click Add > Insert.

Step 19: In the Interface list, choose Any.

Step 20: To the right of Action, select Deny.

Step 21: In the **Source** list, choose the network object automatically created for the guest DMZ. (Example: dmz-guests-network/22)

Step 22: In the **Destination** list, choose the network objects for the internal and DMZ networks, and then click **OK**. (Example: internal-network, dmz-networks)

둴 Edit Access F	ule 🔀
Interface:	Any
Action: 🔘 Pern	nit 💿 Deny
Source Criteria -	
Source:	dmz-guests-network/22
User:	
Security Group:	
Destination Crite	
Destination:	dmz-networks, internal-network
Security Group:	
Service:	ip m
Description:	Deny traffic from the wireless guest network to the internal and dmz resources
🔽 Enable Loggi	ng
Logging Leve	l: Default 👻
More Options	*
	OK Cancel Help

Next, you enable the guests to communicate with the Internet.

Step 23: Click Add > Insert.

Step 24: In the Interface list, choose Any.

Step 25: In the **Source** list, choose the network object automatically created for the guest DMZ, click **OK**, and then click **Apply**. (Example: dmz-guests-network/22)

insert Access	s Rule
Interface:	Any 🗸
Action: 🧿 Perr	nit 💿 Deny
Source Criteria	
Source:	dmz-guests-network/22
User:	
Security Group:	
Destination Crite	eria
Destination:	any
Security Group:	
Service:	ip
Description:	Allow Wireless DMZ users access to the internet
📝 Enable Logg	ing
Logging Leve	el: Default 👻
More Options	*
	OK Cancel Help

Procedure 5

Create the guest wireless LAN interface

The guest wireless interface is connected to the DMZ of the Cisco ASA 5500 Series Adaptive Security Appliances. This allows guest wireless traffic only to and from the Internet. All traffic, regardless of the controller that the guest initially connects to, is tunneled to the guest WLC and leaves the controller on this interface. To easily identify the guest wireless devices on the network, use an IP address range for these clients that are not part of your organization's regular network. This procedures adds an interface that allows devices on the guest wireless network to communicate with the Internet.

Step 1: In Controller>Interfaces, click New.

Step 2: Enter the Interface Name. (Example: Wireless-Guest)

Step 3: Enter the VLAN Id, and then click Apply. (Example: 1126)

սիսիս						Sa <u>v</u> e Cor	nfiguration <u>P</u> ing I	.ogout <u>R</u> efres
CISCO	MONITOR WL	LANS <u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBACK	
Controller	Interfaces >	New					< Back	Apply
General Inventory Interfaces Interface Groups Multicast Network Routes Internal DHCP Server Mobility Management Ports NTP CDP Advanced	Interface Nam VLAN Id	ne Wireless-Guest						

Step 4: In the **IP Address** box, enter the IP address you want to assign to the WLC interface. (Example: 192.168.28.5)

Step 5: Enter the Netmask. (Example: 255.255.252.0)

Step 6: In the **Gateway** box, enter the IP address of the firewall's DMZ interface, defined in Procedure 2. (Example: 192.168.28.1)

Step 7: In the **Primary DHCP Server** box, enter the IP address of your organization's DHCP server, and then click **Apply**. (Example: 10.4.48.10)

սիսիս						Sa <u>v</u> e (Configuration	<u>P</u> ing L	.ogout <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Controller	Interfaces	s > Edit					< Back		Apply
General Inventory Interfaces Interface Groups Multicast Network Routes Internal DHCP Server Mobility Management Ports NTP CDP IPv6 Advanced	General I Interface MAC Add Configura Guest Lar Quarantir Quarantir Physical I The interf Enable Dp Interface VLAN Ide IP Addres Netmask Gateway DHCP Info Primary D Secondar Access Co Acc Nam	nformatic Name ress tion ne e Vlan Id nformatic ace is attac ynamic AP I Address ntifier s ormation DHCP Serve y DHCP Serve y DHCP Serve g DHCP Serve Ser	wireless 88:43:4 88:43:4 0 0 0 0 0 0 0 0 0 0 0 0 0	28 28 2.166.28.5 2.166.28.5 2.166.28.1 2.166.28.1 0.4.48.10 0.4.48.10		· 	_ < Back		Apply

Tech Tip

To prevent DHCP from assigning addresses to wireless clients that conflict with the WLC's addresses, exclude the addresses you assign to the WLC interfaces from DHCP scopes.

Procedure 6

Step 1: On the WLANs page, in the list, choose Create New, and then click Go.

cisco	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY MANAGEMENT		ration Ping Logout <u>R</u> efre ELP <u>F</u> EEDBACK
WLANs	WLANs				Entries 1 - 2 of 2
WLANS	Current Filter: Non	[Change Filter] [Clear Fi	ter] Cre	ate New 👻	Go
Advanced	WLAN ID Type	Profile Name	WLAN SSID	Admin Status	Security Policies
	1 WLAN	WLAN-Data	WLAN-Data	Enabled	[WPA2][Auth(802.1X)]
	2 WLAN	Voice	WLAN-Voice		[WPA2][Auth(802.1X)]

Step 2: Enter the Profile Name. (Example: Guest)

Step 3: In the **SSID** box, enter the guest WLAN name, and then click **Apply**. (Example: Guest)

սիսիս						Sa <u>v</u> e Co	nfiguration Ping Logout	<u>R</u> efresh
cisco	MONITOR WLAN	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBACK	
WLANs	WLANs > New						< Back Ap	oply
 WLANs WLANs ➤ Advanced 	Type Profile Name SSID ID	WLL Gue Gue	it it					

Step 4: On the General tab, in the **Interface/Interface Group(G)** list, choose the interface created in Procedure 5. (Example: wireless-guest)

MIL ANI-		
WLANs	WLANs > Edit 'Gues	< Back Appl
WLANS WLANS	General Security	QoS Advanced
Advanced	Profile Name	Guest
	Туре	WLAN
	SSID	Guest
	Status	Enabled
	Security Policies	[WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
	Radio Policy	All
	Interface/Interface Group(G)	wireless-guest 👻
	Multicast Vlan Feature	Enabled
	Broadcast SSID	V Enabled
	Foot Notes	
	2 H-REAP Local Switching 3 When client exclusion is 4 Client MFP is not active 5 Learn Client IP is config 6 WMM and open or AES 7 Multicast Should Be Ens	ed in combination with IPace in an supported with IPace, CDAVITE authentication in an supported with IPace, CDAVITE authentication unless WAA's configured within a WAA's configured accepts phong be enabled to support higher 11 rates be only when Analow Horky is set to XI.
	9 Value zero implies then 10 MAC Filtering is not su 11 MAC Filtering should b	is no restriction on maximum clients allowed. oported with HREAP Local authentication

Step 5: Click the Security tab, and then on the Layer 2 tab, in the Layer 2 Security list, choose None.

սիսիս	Saye Configuration Ping Logout Re	
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	
WLANs	WLANs > Edit 'Guest' Appl	y
WLANS WLANS	General Security QoS Advanced	
Advanced	Layer 2 Layer 3 AAA Servers	
	Leyer 2 Security ⁹ None IMMAC Filtering	
	Fond Notes Tech Notes 1 Web Relys cannot be used in combination with IPsec, CRANTE authentication 2. Hr4RAP Local Switching is not supported with IPsec, CRANTE authentication 3 Who cleans with evolution is anabided a Timeout Value of azero means infinity (will require administrative override to reset excluded clients). 4 Cleans MPI and active unless WAQ is combined 2. Second Switching is not active unless WAQ is combined to suscellation is enabled 6 Links 2. Second Switching is not active unless with AG is combined to suscellation is enabled 3. Who cleans are of AG is active whom Redo Folio (s) is set to VAI. 7 MUlticast Should be challed for IPV6. 8. Band Select is combiguited only whom Redo Folio (s) is set to VAI. 3. Second Science (S) is set to VAI. 3 Band Select is combination of whom Redo Folio (s) is set to VAI. 3. Second Science (S) is set to VAI. 1 MAC Filtering is the size is a constrained in uncommute cleans advined. 3. Second Science (S) is set to VAI. 1 MAC Filtering should be exclusive. 4. Second Science (S) is set to VAI. 3. Second Science (S) is set to VAI. 1 MAC Filtering should be exclusive. 5. Second Science (S) is set to VAI. 3. Second Science (S) is set to VAI. 1 MAC Filtering should be exclusive. 6. Second Science (S) is set to VAI. 3. Second Science (S) is set to VAI. 1 MAC Filtering should be exclusitere (S) is set to VAI. <td></td>	

Step 6: On the Layer 3 tab, select Web Policy, and then click OK.



Step 7: On the QoS tab, in the Quality of Service (QoS) list, choose Bronze (background), and then click Apply.

սիսիս	Sa <u>v</u> e Configuration <u>P</u> ing Logout <u>R</u> efres
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
LANs	WLANs > Edit 'Guest' < Back Apply
WLANS	General Security QoS Advanced
Advanced	
	Quality of Service (QoS) Bronze (background) WMM
	WMM Policy Allowed -
	7920 AP CAC Enabled
	7920 Client CAC
	Foot Notes
	1 Web Policy cannot be used in combination with IPsec
	2 H-REAP Local Switching is not supported with IPsec, CRANITE authentication
	3 When client exclusion is enabled, a Timeout Value of zero means infinity (will require administrative override to reset excluded clients) 4 Client MFP is not active unless WPA2 is configured
	5 Learn Client IP is configurable only when HREAP Local Switching is enabled
	6 WMM and open or AES security should be enabled to support higher 11n rates
	7 Multicast Should Be Enabled For IPV6. 8 Band Select is configurable only when Radio Policy is set to "All".
	 Solution and the state of the s
	10 MAC Filtering is not supported with HREAP Local authentication
	11 MAC Filtering should be enabled.
	12 Guest tunneling, Local switching, DHCP Required should be disabled.

Step 8: On the General tab, to the right of Status, select **Enabled**, and then click **Apply**.

սիսիս								nfiguration Ping	Logout <u>R</u> e
cisco	MONITOR	<u>W</u> LANs O	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP FEEDE	MCK
WLANs	WLANs > I	Edit 'Gue	est'					< Back	Appl
WLANS	General	Security	QoS	Advanced					
Advanced	Profile N	ame	Guest						
	Туре		WLAN						
	SSID		Guest						
	Status		🔽 Enab	ed					
	Security	Policies	[WPA2	[Auth(802.1X	31				
						will appear after ap	plying the chang	es.)	
	Radio Po	licy	All						
	Interface Group(G	e/Interface	manage	ment 👻					
		t Vian Feature	E Enabl	м					
	Broadcas		Enable Enable						
				-					
	Foot Note								
				rted with IPsec, Timeout Value o		hentication infinity (will require	administrative o	verride to reset ex	cluded clients)
				is configur ed when HREAP Loo	al Switching i	- apphied			
	6 WMM and	d open or AES	security should	ld be enabled t	o support high	er 11n rates			
			nabled For IPV	6. n Radio Policy i	c cet to 14//				
	9 Value zer	o implies the	re is no restric	tion on maximu	im clients alloi	ved.			
		tering is not s tering should		HREAP Local a	thentication				
		inneling, Loca	al switching, D	HCP Required s	hould be disat				
						Authentication.			

Procedure 7

Create the lobby admin user account

Typically, the lobby administrator is the first person to interact with your corporate guests. The lobby administrator can create individual guest user accounts and passwords that last from one to several days, depending upon the length of stay for each guest.

Step 1: In Management > Local Management Users, click New.

Step 2: Enter the username. (Example: Guest-Admin)

Step 3: Enter and confirm the password. (Example: C1sco123)

Step 4: In the User Access Mode list, choose LobbyAdmin, and then click Apply.

ent L	ent l	nt L	nt l	nt l	nt U	t U	Us	ser	rs	>	Ne	ew	v																									1	<	Ba	ck				A	ply
										G ••	iues	st-,	Ad			-																														
					U		Us			ers	G •	Gue	Guest	•••••	Guest-Admin																															



Create guest accounts

Now you can use the lobby administrator account to create usernames and passwords for partners, customers, and anyone else who is not normally granted access to your network.

Step 1: Using a web browser, open the WLC's web interface (for example, https://wlc-1.cisco.local/), and then log in using your LobbyAdmin account with the username **Guest-Admin** and password **C1sco123**.

Step 2: From the Lobby Ambassador Guest Management page, click New.

،، ،،، ،، cısco	Lobby Ambassador Guest Management	Logou	t Refresh H	lelp
Guest Management	Guest Users List	1	New	
	Items 0	to O	of O	
	User Name WLAN SSID Account Remaining Time Description			

Step 3: Create a new username and password, or allow the system to create a password automatically by selecting **Generate Password**.

iliilii cisco	Lobby Ambassador Gues	t Management	Logou	ıt Refresh Help
Guest Management	Guest Users List > N	ew	< Back	Apply
	User Name	partner		
	Generate Password	V		
	Password	••••••		
	Confirm Password	••••••		
	Lifetime	1 day Message from webpage		
	Guest User Role	The generated password for this user is BIN:54yY		
	WLAN SSID	Any WLAN		
	Description			

Step 4: Click Apply. The new user name and password are created.

With a wireless client, you can now test connectivity to the guest WLAN. Without any security enabled, you should receive an IP address, and after opening a web browser, you should be redirected to a web page to enter a username and password for Internet access, which will be available to a guest user for 24 hours.

Process

Configuring Guest Wireless: Dedicated Guest Controller

- 1. Configure the DMZ switch
- 2. Configure the firewall DMZ interface
- 3. Configure Network Address Translation
- 4. Create network objects
- 5. Configure WLC security policy
- 6. Configure guest network security policy
- 7. Configure the DMZ WLC
- 8. Configure the time zone
- 9. Configure SNMP
- 10. Limit which networks can manage the WLC
- 11. Configure management authentication
- 12. Create the guest wireless LAN interface
- 13. Configure the guest wireless LAN
- 14. Configure mobility groups
- 15. Create the lobby admin user account
- 16.Configure the internal WLCs for a guest
- 17. Create guest accounts

Procedure 1

Configure the DMZ switch

The VLANs used in the following configuration examples are:

- Guest Wireless—VLAN 1128, IP: 192.168.28.0/22
- · Wireless management—VLAN 1119, IP 192.168.19.0/24

Step 1: On the DMZ switch, create the wireless VLANs.

vlan 1119 name WLAN_Mgmt vlan 1128 name Guest Wireless

Step 2: Configure the interfaces that connect to the Internet firewalls as trunk ports and add the wireless VLANs.

interface GigabitEthernet1/0/24
description IE-ASA5545a Gig0/1
!
interface GigabitEthernet2/0/24
description IE-ASA5545b Gig0/1
!
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
switchport trunk encapsulation dot1q
switchport trunk allowed vlan add 1119, 1128
switchport mode trunk

- macro apply EgressQoS
- logging event link-status
- logging event trunk-status
- no shutdown

Step 3: This deployment uses Layer 2 EtherChannels in order to connect the WLCs to the DMZ switch. Connect the WLC EtherChannel uplinks to separate devices in the DMZ stack.

On the DMZ switch, the physical interfaces that are members of a Layer 2 EtherChannel are configured prior to configuring the logical port-channel interface. Doing the configuration in this order allows for minimal configuration because most of the commands entered to a port-channel interface are copied to its members' interfaces and do not require manual replication.

Configure two or more physical interfaces to be members of the EtherChannel. It is best if they are added in multiples of two.

Interface range **GigabitEthernet1/0/13**, **GigabitEthernet2/0/13** description DMZ-WLC-Guest-1

!

T

Interface range **GigabitEthernet 1/0/14, GigabitEthernet 2/0/14** description DMZ-WLC-Guest-2

interface range GigabitEthernet 1/0/13, GigabitEthernet 2/0/13
channel-group 12 mode on
macro apply EgressQoS
logging event link-status
logging event trunk-status
interface range GigabitEthernet 1/0/14, GigabitEthernet 2/0/14
channel-group 13 mode on
macro apply EgressQoS
logging event link-status
logging event trunk-status
logging event trunk-status
logging event bundle-status

Step 4: Configure trunks.

An 802.1Q trunk is used for the connection to the WLC, which allows the firewall to provide the Layer 3 services to all the VLANs defined on the access layer switch. The VLANs allowed on the trunk are reduced to only the VLANs that are active on the WLC.

interface Port-channel12
description DMZ-WLC-Guest-1
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1119,1128
switchport mode trunk
logging event link-status
no shutdown

interface Port-channel13

description DMZ-WLC-Guest-2
switchport trunk encapsulation dotlq
switchport trunk allowed vlan 1119,1128
switchport mode trunk
logging event link-status
no shutdown

Procedure 2

Configure the firewall DMZ interface

Typically, the firewall *DMZ* is a portion of the network where traffic to and from other parts of the network is tightly restricted. Organizations place network services in a DMZ for exposure to the Internet; these services are typically not allowed to initiate connections to the inside network, except for specific circumstances.

The various DMZ networks are connected to Cisco ASA on the appliances' Gigabit Ethernet interface via a VLAN trunk. The IP address assigned to the VLAN interface on the appliance is the default gateway for that DMZ subnet. The DMZ switch's VLAN interface does not have an IP address assigned for the DMZ VLAN.

Table 8 - Cisco ASA DMZ interface information

Interface Label	IP Address & Netmask	VLAN	Security Level	Name
GigabitEthernet0/ 1.1119	192.168.19.1/24	1119	50	dmz-wlc
GigabitEthernet0/ 1.1128	192.168.28.1/22	1128	10	dmz-guests

Step 1: Login to the Internet Edge firewall using Cisco ASDM.

Step 2: Navigate to **Configuration > Device Setup > Interfaces**, and then click the interface that is connected to the DMZ switch. (Example: GigabitEthernet0/1)

Step 3: Click Edit.

Step 4: Select Enable Interface, and then click OK.

Edit Interface
General Advanced IPv6
Hardware Port: GigabitEthernet0/1 Configure Hardware Properties
Interface Name:
Security Level:
Dedicate this interface to management only
Channel Group:
Enable Interface
IP Address
Use Static IP Obtain Address via DHCP Use PPPoE
IP Address:
Subnet Mask: 255.0.0.0 👻
Description:
OK Cancel Help

Step 5: On the Interface pane, click Add > Interface.

Step 6: In the **Hardware Port** list, choose the interface configured in Step 2 (Example: GigabitEthernet0/1)

Step 7: In the **VLAN ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1119)

Step 8: In the **Subinterface ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1119)

Step 9: Enter an Interface Name. (Example: dmz-wlc)

Step 10: In the Security Level box, enter a value of 50.

Step 11: Enter the interface IP Address. (Example: 192.168.19.1)

Step 12: Enter the interface **Subnet Mask**, and then click **OK**. (Example: 255.255.255.0)

🔂 Edit Interface
General Advanced IPv6
Hardware Port: GigabitEthernet0/1.1119 VLAN ID: 1119 Subinterface ID: 1119 Interface Name: dmz-wic Security Level: 50 Dedicate this interface to management only Channel Group: V Enable Interface
IP Address IP Address IP Address: 192.168.19.1 Subnet Mask: 255.255.255.0
Description: WLC DMZ Trunk to DMZ Switch OK Cancel Help

Step 13: Navigate to Configuration > Device Management > High Availability and Scalability > Failover.

Step 14: On the Interfaces tab, in the **Standby IP address** column, enter the IP address of the standby unit for the interface you just created. (Example: 192.168.19.2)

Step 15: Select Monitored, and then click Apply.

Interface Name	Name	Active IP Address	Subnet Mask/ Prefix Length	Standby IP Address	Monitored
GigabitEthernet0/0.300	inside	📇 10.4.24.30	255.255.255.224	📇 10.4.24.29	
GigabitEthernet0/1.1116	dmz-web	📇 192.168.16.1	255.255.255.0	4 192.168.16.2	
		📇 2001:db8:	64	📇 2001:db8:a:	
GigabitEthernet0/1.1117		📇 192.168.17.1		📇 192.168.17.2	
GigabitEthernet0/1.1118		📇 192.168.18.1		📇 192.168.18.2	
GigabitEthernet0/1.1119		🖳 192.168.19.1		🖳 192.168.19.2	
GigabitEthernet0/1.1123				📇 192.168.23.2	
GigabitEthernet0/1.1128		4 192.168.28.1		4 192.168.28.2	
GigabitEthernet0/3.16	outside-16	📇 172.16.13		📇 172.16.130	
		💐 2001:db8:		📇 2001:db8:a::2	
GigabitEthernet0/3.17	outside-17	📇 172.17.13	255.255.255.0	📇 172.17.130	
Management0/0	IPS-mgmt				

Step 16: At the bottom of the window, click **Apply**. This saves the configuration.

Step 17: Repeat Step 5 through Step 12 for the dmz-guests interface.

Procedure 3

Configure Network Address Translation

The DMZ network uses private network (RFC 1918) addressing that is not Internet-routable, so the firewall must translate the DMZ address of the guest clients to an outside public address.

Step 1: Navigate to Configuration > Firewall > Objects > Network Objects/Groups.

Step 2: Click Add > Network Object.

Step 3: In the Add Network Object dialog box, in the **Name** box, enter a description for the guest network. (Example: dmz-guests-network-ISPa)

Step 4: In the Type list, choose Network.

Step 5: In the **IP Address** box, enter the guest DMZ network address. (Example: 192.168.28.0)

Step 6: Enter the guest DMZ netmask. (Example: 255.255.252.0)

Step 7: Click the two down arrows. The NAT pane expands.

Step 8: Select Add Automatic Address Translation Rules.

Step 9: In the Type list, choose Dynamic PAT (Hide).

Step 10: In the **Translated Addr** list, choose the interface name for the primary Internet connection. (Example: outside-16)

🔄 Add Network	Object							
Name:	dmz-guest-network-ISPa							
Туре:	Network							
IP Version:	● IPv4							
IP Address:	192.168.28.0							
Netmask:	255.255.252.0 🗸							
Description:	DMZ outside PAT address for ISPa							
NAT	*							
🔽 Add Autom	atic Address Translation Rules							
Type:	Dynamic PAT (Hide) 👻							
Translated A	ddr: outside-16							
Use one-	Use one-to-one address translation							
PAT Pool Translated Address:								
Round	Robin							
Extend	d PAT uniqueness to per destination instead of per interface							
Transla	ate TCP and UDP ports into flat range 1024-65535 🗌 Include range 1-1023							
Fall through to interface PAT(dest intf): IPS-mgmt								
Use IPv6 for interface PAT								
	Advanced							
	OK Cancel Help							

Step 11: Click Advanced.

Step 12: In the **Destination Interface** list, choose the interface name for the primary Internet connection, and then click **OK**. (Example: outside-16)

Advanced NAT Settin	ngs 💽
Translate DNS repl	ies for rule
Interface	
Source Interface:	Any 👻
Destination Interface:	outside-16 🗸
ОК	Cancel Help

Step 13: In the Add Network Object dialog box, click OK.



Step 1: Navigate to Configuration > Firewall > Objects > Network Objects/Groups.

First, add a network object for the every internal WLC in your organization.

Step 2: Click Add > Network Object.

Step 3: In the Add Network Object dialog box, in the **Name** box, enter a description of the WLC. (Examples: internal-wlc-5508, internal-wlc-flex-7500)

Step 4: In the Type list, choose Host.

Step 5: In the **IP Address** box, enter the WLC's management interface IP address, and then click **OK**. (Example: 10.4.46.64, 10.4.46.68)

📴 Edit Networ	k Object	×
Name:	internal-wlc-5508	
Туре:	Host	•
IP Version:	IPv4	
IP Address:	10.4.46.64	
Description:	Internal 5508 WLC	
NAT		*
NO1		*
	OK Cancel Help	

Step 6: Repeat Step 2 through Step 5 for every WLC inside your organization.

🔁 Edit Network	Object	×
Name:	internal-wlc-flex-7500	
Туре:	Host	•
IP Version:	● IPv4	
IP Address:	10.4.46.68	
Description:	Internal FlexConnect 7500 WLC	
NAT		*
1961		~
	OK Cancel Help	

Next, to simplify security policy configuration, you create a network object group that contains every WLC inside your organization.

Step 7: Click Add > Network Object Group.

Step 8: In the Add Network Object Group dialog box, in the **Group Name** box, enter a name for the group. (Example: internal-wlc-group)

Step 9: In the Existing Network Objects/Groups pane, select every internal WLC, click **Add**, and then click **OK**.

Scription: Internal Wireless LAH Controllers Existing Network Objects/Groups: Members in Group: Name 1 IP Address Netmask Image: I	up Name	: internal-wlc-group							
Name IP Address Netmask	cription:	Internal Wireless LAN Cor	ntrollers						
Name IP Address Netmask Image: Participation of the partipation	Existing I	Network Objects/Groups:					Members in Group:		
Image: Second	Name	A1	IP Address	Netmask			Name	IP Address	NetmaskPrefix Len
• ## dm:-puest-network:15Pa 12:168.20.0 255.255.252.0 • ## dm:-pie-fragtool 192:168.10.0 255.255.248.0 ## dm:-pie-fragtool 192:168.10.0 192:168.10.0 ## dm:-pie-fragtool 192:168.10.0 192:168.10.0 ## dm:-pie-fragtool 192:168.10.0 192:168.10.0 ## dm:-pie-fragtool 192:168.10.0 192:168.10.0 192:168.10.10 ## dm:-pie-fragtool 192:168.10.10 192:168.10.10 ## dm:-pie-fragtool 192:168.10.10 192:168.10.10 194:168.10 194:168.10 194:168.10 194:168.10 194:168.10 194:168.10 194:168.10 194:168.10 194:168.10 194:168.10 194:168.10 194:168.10 194:168.10 194:10 194:168.10 194:168.10 194:168.10 194:11 4dd> 4dd> 4dd> 4dd> 194:168.11 4dd> 194:168.11 194:11 4dd> 194:168.11 194:11 194:11 4dd> 194:11 4dd> 194:11	la p	🖳 dm2-dmvnn-2	192.168.18.11				💬 🖳 internal-wic-flex-7500	10.4.46.68	
## dmc_met-metrodi 192.168.16.0.82-192 ## dmc_metworks 192.168.16.0.82-192 ## dmc_metworks 192.168.16.0. ## dmc_metworks 192.168.16.10.0 # dmc_metworks 192.17.17.10.1 # dmcdsde-metworks 192.17.17.130.10			192.168.28.0	255,255,252,0			🛄 📇 internal-wic-5508	10.4.46.64	
Add >>									
• • • • • • • • • • • • • • •			192.168.16.0	255.255.248.0					
Image: drive-webserver:FSPs 192,168.16.100 Image: drive-webserver:FSPs 192,168.10.100 Image: drive-drive-rSPs 172,17.130.10 Image: drive-drive-drive-rSPs 172,17.130.100 Image: drive-drive-drive-rSPs 172,17.130.100 Image: drive-drive-rSPs 172,17.130.100 Image: drive-drive-rSPs 172,17.130.100 Image: drive-drive-rSPs 172,17.130.100 Image: drive-drive-rSPs 172,17.130.100 Image: drive-rSPs 172,17.130.100 <			2001:db8:a:1::	64					
Image: decision of the second seco			192.168.16.100						
■ dre:webserver:1951 192.165.16.100 ■ dre:meharetwork: 10.4.0.0 255.254.0.0 ■ dre:meharetwork:Sps 12.1.6.1.30.1 E ■ dre:meharetwork:Dip:meharetwork:Sps 12.1.6.1.30.100 Image:meharetwork:Sps ■ dre:meharetwork:Object member: Note:meharetwork:Dip:meharet			192.168.16.111						
• #P Internal-network: 199 10.4.0.0 255,254.0.0 • # Internal-network: 199 10.4.0.0 255,254.0.0 • # Internal-network: 199 172,17,130.1 • # Outside-dmvpn-159 172,17,130.1 • # Outside-dmvpn-159 172,17,130.10 • #									
Bit Netmain-Network: 15Pa 10.4.0.0 255:254.0.0 Status Network: 15Pa 122.16:10.0.1 Image: 120.16 Status Network: 15Pa 122.16:10.0.1 Image: 120.16 Status Network: 15Pa 122.17:130.10 Image: 120.16 Status Network: 0bject member: Image: 120.16 Image: 120.16 Type: Hist Image: 120.16 IP Version: IP Version: Image: 120.16			10.4.0.0	255.254.0.0					
Social de webservertigtur, 2001 (168/sec.)111 # Social de dropp-1359 172.16.10.1 Social de dropp-1359 172.16.10.10 Social de vebserver-1359 172.16.10.100 Social de vebserver-1359 172.16.10.100 Social de vebserver-1359 172.16.10.100 Type: Host Previour #		internal-network-ISPa	10.4.0.0	255.254.0.0					
Image: solvide-dromportspine 172.16.130.1 Image: solvide-dromportspine 172.17.130.1 Image: solvide-dromportspine 0		internal-network-ISPb	10.4.0.0	255.254.0.0					
actsde-dmypr-ISPb 172.17.130.1 actsde-dmypr-ISPb 172.17.130.100 actsde-webserver-ISPb 172.17.130.100 actsde-webserver-ISPb 172.17.130.100 create new Network Object member: Name: (optional) Type: Host PV ersion:	5	dustide-webserver-isp	2001:db8:a::111						
Boutside TPre-dul :: 0 Control on the server-15Pe 172.17.180.100	8	🖳 outside-dmvpn-ISPa	172.16.130.1		-	Add >>			
@ outside TP-6-all :: U @ outside webserver-TSPb 172.16.130.100 + @ cotside webserver-TSPb 172.17.130.100 + Create new Network Object member: > > Name: (optional)	8	🖳 outside-dmvpn-ISPb	172.17.130.1						
• outside webserver-15Pb 172.17.130.100 • m • • create new Network Object member: Name: (optional) Type: Host IP Version: • IP Version:	3	🛱 outside-IPv6-all	8	0		<< Remove			
III > Greate new Network Object member: > Name: (optional)									
Create new Network Object member: Name: (optiona) Type: Host v IP Version: (a) IPv4 IPv6	(🖳 outside-webserver-ISPb	172.17.130.100		-				
Name: (optional)	•			Þ					
Type: Host v IP Version:	Create n	new Network Object member	:						
Type: Host v IP Version:									
IP Version:	ivame: (c								
	Туре:	Host			•				
IP Address:	IP Versio	on: 💿 IPv4 🖱 IPvé	;						
Ir Address:	m a data	-							
	r- Hadle	555.							
							•		,
							•		

Next, you create a network object group that contains the private DMZ address of every WLC in the DMZ. (Example: 192.168.19.54)

Step 10: Click Add > Network Object Group.

Step 11: In the Add Network Object Group dialog box, in the **Group Name** box, enter a name for the group. (Example: dmz-wlc-group)

Description:	Wireless LAN Controller	rs in the DMZ							
Existing I	Network Objects/Groups:				N	1ember	rs in Group:		
ame	A1	IP Address	Netmask			Name		IP Address	NetmaskPrefix Le
	dmz-wlc-network	192.168.19.0	255.255.255.0				dmz-wic-5508		
- <u>-</u>	inside-network	10.4.24.0	255.255.255.224				dmz-wic-2504-1	192.168.19.56	
<u>-</u>	outside-16-network	172.16.130.0	255.255.255.0			<u></u>	dmz-wic-2504-2	192.168.19.57	
	outside-16-network6	2001:db8:a::	64						
- -	outside-17-network	172.17.130.0	255.255.255.0						
- 🖪 d	dmz-dmvpn-1	192.168.18.10							
- 3 (dmz-dmvpn-2	192.168.18.11							
- 🚜 e	dmz-guest-network-ISPa	192.168.28.0	255.255.252.0						
- 🚜 🛛	dmz-ipv6-natpool	192.168.16.32-192		Ξ					
- 🛃 (dmz-networks	192.168.16.0	255.255.248.0						
		2001:db8:a:1::	64						
- 3 (dmz-webserver-ISPa	192.168.16.100							
	dmz-webserver-ispa-v6	192.168.16.111		-	Add >>				
		192.168.16.100			Mdd >>				
		10.4.0.0	255.254.0.0		<< Remove				
		10.4.0.0	255.254.0.0						
		10.4.0.0	255,254.0.0						
				Ŧ					
•			,						
🕤 Create n	ew Network Object memi	per:							
Name: (c	optional)								
Type:	Host			-					
IP Versio	n: 💿 IPv4 🔘 IF	Pv6							
IP Addre	55:								
						_			
						٠ 📃			

Step 12: Choose the primary WLC from the Existing Network Objects/ Groups pane, and then click **Add**. (Example: 192.168.19.54). If using the 5508 as the anchor controller, only the IP address of the primary WLC needs to be configured as this WLC model supports AP-SSO and the redundant pair use a single IP address.

Step 13: If using a 2504 as a guest anchor controller, both the primary and resilient WLC IP addresses are necessary as this WLC does not support AP-SSO. Choose the resilient WLC from the Existing Network Objects/ Groups pane, click **Add**, and then click **OK**. (Example: 192.168.19.56). You will also add the IP address of the secondary WLC's (Example: 192.168.19.57)

Step 14: The resilient Wireless LAN Controller when in standby mode when using AP-SSO uses the Redundancy Port to communicate with the NTP server. Since either of the WLC in AP-SSO mode could be in standby we need to create a network object that is used to identify the RP ports. create a Network Object for each of the WLC in the DMZ (Example: 192.168.19.54). Click Add > Network Object.

Step 15: In the Add Network Object dialog box, in the **Name** box, enter a description of the WLC. (Example: dmz-wlc-primary-5508-RP)

Step 16: In the Type list, choose Host.

Step 17: In the IP Address box, enter the primary WLC's RP interface IP address, and then click OK. (Example: 192.168.19.154)

🔁 Add Network	Object	×
Name:	dmz-wlc-primary-5508-RP	
Туре:	Host	•
IP Version:		
IP Address:	192.168.19.154	
Description:	Primary WLC Redundancy Port	
NAT		×
1961		Ť
	OK Cancel Help	

Step 18: Repeat for the resilient controllers Redundancy Port (Example 192.168.19.155)

💁 Add Networ	k Object	×
Name:	dmz-wlc-resilient-5508-RP	
Туре:	Host	-
IP Version:	IPv4 O IPv6	
IP Address:	192.168.19.155	
Description:	Resilient WLC Redundancy Port	
NAT		*
DIM I		Ŷ
	OK Cancel Help	

Step 19: Create a Network Object Group that will group the two Redundancy Ports (RP) on the WLCs.

Sroup Name:	dmz-wlc-RP-group							
Description:	DMZ Wireless LAN Contro	llers Redundancy Port Gr	oup					
Existing N	letwork Objects/Groups:					Members in Group:		
Name	×1	IP Address	Netmask			Name	IP Address	NetmaskPrefix
	duckide-16-network duckide-16-network6 duckide-17-network6 draz-dmypn-2 draz-dmypn-2 draz-guest-network-ISPa draz-guest-network-ISPa draz-networks draz-networks draz-webserver-ISPa draz-webserver-ISPa draz-webserver-ISPb draz-webserver-ISPb draz-webserver-ISPb draz-webserver-ISPb	192.168.16.32-192 192.168.16.0 2001:db8:a:1:: 192.168.16.100	255,255,255.0 64 255,255,255.0 255,255,255.0 255,255,252.0 255,255,248.0 64	E	Add >>	L, dm2+vk-primary-5508-PP 31. dm2+vk-resilent-5508-PP	192,168,19,154 192,168,19,155	
	dm2+wlc-5508 internal-aaa internal-dhcp 	192.168.19.54 10.4.48.15 10.4.48.10	·	Ŧ				
Type:	Host			•				
IP Version	i: 💿 IPv4 🔘 IPv6							
IP Addres	5:					4 111		

Step 20: In the Add Network Object Group dialog box, click OK.

Procedure 5 Configure WLC security policy

Step 1: Navigate to Configuration > Firewall > Access Rules.

Step 2: Click the rule that denies traffic from the DMZ toward other networks.

Next, you insert a new rule above the rule you selected that enables the WLCs in the DMZ to communicate with the AAA server in the data center for management and user authentication.

Step 3: Click Add > Insert.

24 🔽 📑 dmz-networks

🔞 Deny

IP ip

Step 4: In the Insert Access Rule dialog box, in the **Interface** list, choose **Any**.

Step 5: To the right of Action, select Permit.

Step 6: In the **Source** list, choose the network object group created in Step 7, "Create network objects." (Example: wlc-group)

Step 7: In the **Destination** list, choose the network object for the Cisco Secure ACS server with AAA services. (Example: internal-aaa)

Step 8: In the Service list, enter tcp/tacacs, udp/1812, udp/1813, and then click OK.

🔂 Add Access I	Rule
Interface:	Any 🗸
Action: 💿 Perr	nit 💿 Deny
Source Criteria	
Source:	dmz-wlc-group
User:	
Security Group:	
Destination Crite	ria
Destination:	internal-aaa
Security Group:	
Service:	tcp/tacacs, udp/1812, udp/1813
Description:	Allow DMZ based WLC's to communicate with the AAA/ACS Server on the internal network.
📝 Enable Logg	ing
Logging Leve	el: Default 🗸
More Options	*
	OK Cancel Help

Next, you must allow the WLCs in the DMZ to synchronize their time with the NTP server in the data center.

Step 9: Click Add > Insert.

Step 10: In the Internet Access Rule dialog box, in the Interface list, choose Any.

Step 11: To the right of Action, select Permit.

Step 12: In the **Source** list, choose the network object group created in Step 10 of Step 13, "Create network objects." (Example: dmz-wlc-group)

Step 13: In the **Destination** list, choose the network object for the NTP server. (Example: internal-ntp)

Step 14: In the Service list, enter udp/ntp, and then click OK.

📴 Edit Access R	ule 💌
Interface:	Any
Action: () Perm	ili 🔘 Deny
Source Criteria -	
Source:	dmz-wlc-group
User:	
Security Group:	
Destination Crite	ria
Destination:	internal-ntp
Security Group:	
Service:	udp/ntp
Description:	Allow WLC's to communicate with the NTP server locate din the data center.
🔽 Enable Loggii	ng
Logging Leve	l: Default 🗸
More Options	*
	OK Cancel Help

Next, you allow the WLCs in the DMZ to be able to download new software via FTP.

Step 15: Click Add > Insert.

Step 16: In the Internet Access Rule dialog box, in the Interface list, choose Any.

Step 17: To the right of Action, select Permit.

Step 18: In the **Source** list, choose the network object group created in Step 10 of Step 13, "Create network objects." (Example: dmz-wlc-group)

Step 19: In the Service list, enter tcp/ftp, tcp/ftp-data, and then click OK.

뒄 Add Access I	Rule
Interface:	Any 🔻
Action: 💿 Perr	nit 💿 Deny
Source Criteria	
Source:	dmz-wlc-group
User:	
Security Group:	· · · · · · · · · · · · · · · · · · ·
Destination Crite	ria —
Destination:	any
Security Group:	
Service:	tcp/ftp, tcp/ftp-data
Description:	Allow the WLC's to communicate with any FTP server.
🔽 Enable Logg	ing
Logging Leve	al: Default 🗸
More Options	*
	OK Cancel Help

Next, you enable the DMZ guest WLC to communicate with the WLCs inside the organization.

Step 20: Click Add > Insert.

Step 21: In the Interface list, choose Any.

Step 22: In the **Source** list, choose the network object group created in Step 10 of Step 13, "Create network objects." (Example: dmz-wlc-group)

Step 23: In the **Destination** list, choose the network object group created in Step 7 of Step 13, "Create network objects." (Example: internal-wlc-group)

Step 24: In the Service list, enter udp/16666, udp/5246, udp/5247, 97, and then click OK.

둴 Add Access I	Rule	x
Interface:	Any 🗸	
Action: 💿 Perr	nit 💿 Deny	
Source Criteria		
Source:	dmz-wlc-group	
User:		
Security Group:		
Destination Crite	ria	_
Destination:	internal-wic-group	
Security Group:		
Service:	udp/16666, udp/5246, udp/5247, 97	
Description:	Allow DMZ based WLC's to communicate with the internal WLC's	
📝 Enable Logg	ing	
Logging Leve	el: Default 👻	
More Options		×
	OK Cancel Help	

Next, you enable the guest WLC to communicate with the DHCP server inside your organization.

Step 25: Click Add > Insert.

Step 26: In the Interface list, choose Any.

Step 27: In the **Source** list, choose the network object group created in Step 10 of Step 13, "Create network objects." (Example: dmz-wlc-group)

Step 28: In the **Destination** list, choose the network object group for the internal DHCP server. (Example: internal-dhcp)

Step 29: In the Service list, enter udp/bootps, click OK, and then click Apply.

📴 Edit Access F	tule	
Interface:	Any	
Action: 💿 Pern	nit 💿 Deny	
Source Criteria		
Source:	dmz-wic-group ····	
User:		
Security Group:		
Destination Crite	ria	
Destination:	internal-dhcp	
Security Group:		
Service:	udp/bootps	
Description:	Allow DMZ WLC's to obtain IP address via internal DHCP server	
👿 Enable Loggi	ing	
Logging Leve	sl: Default 🗸	
More Options	*	
	OK Cancel Help	

Finally, enable the guest WLC configured for AP-SSO (5500 series) to communicate with the internal NTP server using its Redundancy Port (RP).

Step 30: Click Add > Insert.

Step 31: In the Interface list, choose Any.

Step 32: In the Source list, choose network group that was created for the WLC RP ports (Example: dmz-wlc-RP-group)

Step 33: In the Destination list, choose the network object group for the internal NTP server. (Example: internal-ntp)

Step 34: In the Service list, enter udp/ntp, click OK, and then click Apply.

둴 Edit Access R	tule	×
Interface:	Any	
Action: 💿 Perm	nit 💿 Deny	
Source Criteria -		_
Source:	dmz-wic-RP-group	
User:		
Security Group:		
Destination Crite	ria	
Destination:	internal-ntp	
Security Group:		
Service:	udp/ntp	
Description:	Allow Standby AP-SSO WLC's to communicate to internal NTP server using RP Port	
📝 Enable Loggi	ng	
Logging Leve	el: Default 🗸	
More Options	¥	
	OK Cancel Help	

Procedure 6

Configure guest network security policy

Step 1: Navigate to Configuration > Firewall > Access Rules.

Step 2: Click the rule that denies traffic from the DMZ toward other networks.

First, you configure an access rule in the firewall in order to enable the guest wireless users to communicate with the internal DNS and DHCP servers in the data center.

Step 3: Click Add > Insert.

24 🔽 🛃 dmz-networks

Step 4: In the Interface list, choose Any.

😢 Denv

IP iD

Step 5: In the **Source** list, select the network object automatically created for the guest DMZ. (Example: dmz-guests-network/22)

Step 6: In the **Destination** list, choose the network object for the DNS server. (Example: internal-dns)

Step 7: In the Service list, enter udp/domain, tcp/domain, and then click OK.

insert Access	Rule
Interface:	Any 🔹
Action: 💿 Pern	nit 🕜 Deny
Source Criteria -	
Source:	dmz-guests-network/22
User:	
Security Group:	
Destination Crite	ria
Destination:	internal-dns
Security Group:	
Service:	udp/domain, tcp/domain
Description:	Allow Guest Wireless users to resolve DNS names.
📝 Enable Loggi	ng
Logging Leve	l: Default 👻
More Options	*
	OK Cancel Help

Step 8: Click Add > Insert.

Step 9: In the Interface list, choose Any.

Step 10: In the **Source** list, choose the network object automatically created for the guest DMZ. (Example: dmz-guests-network/22)

Step 11: In the **Destination** list, choose the network object for the DHCP server. (Example: internal-dhcp)

Step 12: In the Service list, enter udp/bootps, and then click OK.

insert Access	Rule
Interface:	Any 🔹
Action: 💿 Perm	it 💿 Deny
Source Criteria -	
Source:	dmz-guests-network/22
User:	
Security Group:	
Destination Crite	ria
Destination:	internal-dhcp 💼
Security Group:	
Service:	udp/bootps
Description:	Allow wireless guest users to obtain an IP address from the internal DHCP server
🔽 Enable Loggi	ng
Logging Leve	l: Default 👻
More Options	*
	OK Cancel Help

Next, you enable the guests to communicate with the web servers in the DMZ.

Step 13: Click Add > Insert.

Step 14: In the Interface list, choose Any.

Step 15: In the **Source** list, choose the network object automatically created for the guest DMZ. (Example: dmz-guests-network/22)

Step 16: In the **Destination** list, choose the network object automatically created for the web DMZ. (Example: dmz-web-network/24)

Step 17: In the Service list, enter tcp/http, tcp/https, and then click OK.

📴 Insert Access	Rule
Interface:	Any 🔻
Action: 💿 Pern	nit 💿 Deny
Source Criteria	
Source:	dmz-guests-network/22
User:	
Security Group:	
Destination Crite	ria
Destination:	dmz-web-network/24
Security Group:	
Service:	tcp/http, tcp/https
Description:	All wireless guest users access to DMZ based webservers, possibly for walled garden access
📝 Enable Loggi	ng
Logging Leve	sl: Default 🗸
More Options	¥
	OK Cancel Help

Next, you remove the guests' ability communicate with other internal and DMZ devices.

Step 18: Click Add > Insert.

Step 19: In the Interface list, choose Any.

Step 20: To the right of Action, select Deny.

Step 21: In the **Source** list, choose the network object automatically created for the guest DMZ. (Example: dmz-guests-network/22)

Step 22: In the **Destination** list, choose the network objects for the internal and DMZ networks, and then click **OK**. (Example: internal-network, dmz-networks)

🔂 Edit Access R	ule	×
Interface:	Any	
Action: 🔘 Perm	nit o Deny	
Source Criteria -		
Source:	dmz-guests-network/22	
User:		
Security Group:		
Destination Crite	ria	-
Destination:	dmz-networks, internal-network	
Security Group:		
Service:	ip 💮	
Description:	Deny traffic from the wireless guest network to the internal and dmz resources]
📝 Enable Loggi	ng	
Logging Leve	l: Default 🔹	
More Options	*	
	OK Cancel Help	

Next, you enable the guests to communicate with the Internet.

Step 23: Click Add > Insert.

Step 24: In the Interface list, choose Any.

Step 25: In the **Source** list, choose the network object automatically created for the guest DMZ, click **OK**, and then click **Apply**. (Example: dmz-guests-network/22)

🚰 Insert Access	Rule
Interface:	Any 🔻
Action: 🧿 Perr	nit 💿 Deny
Source Criteria	
Source:	dmz-guests-network/22
User:	
Security Group:	
Destination Crite	ria
Destination:	any -
Security Group:	
Service:	ip
Description:	Allow Wireless DMZ users access to the internet
🔽 Enable Logg	ing
Logging Leve	al: Default 👻
More Options	*
	OK Cancel Help

Notes	

Procedure 7

Configure the DMZ wireless LAN controller by using the following values.

Table 9 - Cisco DMZ wireless controller parameters checklist

Parameter	Cisco SBA values primary controller	Cisco SBA values resilient controller not using AP SSO	Site-specific values
Controller parameters			-
Switch interface number	1/0/13, 2/0/13	1/0/14, 2/0/14	
VLAN number	1119	1119	
Time zone	PST -8 0	PST -8 0	
IP address	192.168.19.54/24	192.168.19.55/24 ¹	
Default gateway	192.168.19.1	192.168.19.1	
Redundant management IP address (AP SSO)	192.168.19.154	192.168.19.155	
Redundancy port connectivity (AP SSO)	Dedicated Ethernet cable	Dedicated Ethernet cable	
Hostname	DMZ-WLC-Guest-1	DMZ-WLC-Guest-2 ²	
Local administrator username and password	admin/C1sco123	admin/C1sco123	
Mobility group name	GUEST	GUEST	
RADIUS server IP address	10.4.48.15	10.4.48.15	
RADIUS shared key	SecretKey	SecretKey	
Management network (optional)	10.4.48.0/24	10.4.48.0/24	
TACACS server IP address (optional)	10.4.48.15	10.4.48.15	
TACACS shared key (optional)	SecretKey	SecretKey	
Wireless data network parameters			
SSID	Wireless-Guest	Wireless-Guest	
VLAN number	1128	1128	
Default gateway	192.168.28.1	192.168.28.1	
Controller interface IP address	192.168.28.5	192.168.28.6 ¹	

Notes:

- 1. If you're using AP SSO high availability, the IP address of the resilient WLC not required, as the secondary controller's management interface is offline until the primary fails. During this time, the IP address of the RP (Example: 192.168.19.155) is used for outbound communication to the NTP server and to monitor the status of its default gateway.
- 2. If using AP SSO, the resilient standby controller does not have a unique hostname, as it inherits the continuation of its paired primary WLC.

After the WLC is physically installed and powered up, you will see the following on the console:

Welcome to the Cisco Wizard Configuration Tool Use the '-' character to backup

Would you like to terminate autoinstall? [yes]: **YES**

Step 1: Enter a system name. (Example: GUEST-1)

System Name [Cisco_7e:8e:43] (31 characters max): DMZ-WLC-Guest

Step 2: Enter an administrator username and password.

Tech Tip

Use at least three of the following four classes in the password: lowercase letters, uppercase letters, digits, or special characters.

Enter Administrative User Name (24 characters max): admin Enter Administrative Password (24 characters max): ***** Re-enter Administrative Password : *****

Step 3: Use DHCP for the service port interface address.

Service Interface IP address Configuration [none] [DHCP]: DHCP

Step 4: Enable the management interface. If you are deploying a Cisco 5500 or 2500 Series Wireless LAN Controller, configure at least two interfaces as an EtherChannel trunk.

Enable Link Aggregation (LAG) [yes][NO]: YES

Management Interface IP Address: 192.168.19.54

Management Interface Netmask: 255.255.255.0

Management interface Default Router: 192.168.19.1

Management Interface VLAN Identifier (0 = untagged): 1119

Step 5: Enter the default DHCP server for clients. (Example: 10.4.48.10)

Management Interface DHCP Server IP Address: 10.4.48.10

Step 6: If you are deploying a Cisco 5500 Series Wireless LAN Controller and you want to enable AP SSO, enable high availability.

Secondary>

Redundancy Management IP Address: 192.168.19.154 Peer Redundancy Management IP Address: 192.168.19.155

Step 7: The virtual interface is used by the WLC for mobility DHCP relay and intercontroller communication. Enter an IP address that is not used in your organization's network. (Example: 192.0.2.1)

Virtual Gateway IP Address: 192.0.2.1

Step 8: If configuring a Cisco 2500 Series WLC, enter the multicast IP address for communication of multicast traffic by using the multicast-multicast method. This WLC does not support multicast using the multicast-unicast method.

Multicast IP Address: 239.40.40.40

Step 9: Enter a name for the default mobility and RF group. (Example: GUEST)

Mobility/RF Group Name: GUEST

Step 10: Enter an SSID for the WLAN that supports data traffic. You will be able to leverage this later in the deployment process.

Network Name (SSID): Guest Configure DHCP Bridging Mode [yes][NO]: NO

Step 11: Enable DHCP snooping.

Allow Static IP Addresses [YES][no]: NO

Step 12: Do not configure the RADIUS server now. You will configure the RADIUS server later by using the GUI.

Configure a RADIUS Server now? [YES][no]: NO

Step 13: Enter the correct country code for the country where you are deploying the WLC.

Enter Country Code list (enter 'help' for a list of countries)
[US]: US

Step 14: Enable all wireless networks.

Enable 802.11b network [YES][no]: **YES** Enable 802.11a network [YES][no]: **YES** Enable 802.11g network [YES][no]: **YES**

Step 15: Enable the RRM auto-RF feature. This helps you keep your network up and operational.

Enable Auto-RF [YES][no]: YES

Step 16: Synchronize the WLC clock to your organization's NTP server.

Configure a NTP server now? [YES][no]:YES

Enter the NTP server's IP address: 10.4.48.17

Enter a polling interval between 3600 and 604800 secs: 86400

Step 17: Save the configuration. If you enter **NO**, the system restarts without saving the configuration, and you have to complete this procedure again.

Configuration correct? If yes, system will save it and reset. [yes][NO]: **YES**

Configuration saved!

Resetting system with new configuration

Step 18: After the WLC has reset, log in to the Cisco Wireless LAN Controller Administration page by using the credentials defined in Step 2. (Example: https://dmz-wlc-guest.cisco.local/) Procedure 8

Configure the time zone

Step 1: Navigate to Commands > Set Time.

Step 2: In the **Location** list, choose the time zone that corresponds to the location of the WLC.

Step 3: Click Set Timezone.

սիսիս						Sa <u>v</u> e Cor	nfiguration Ping	Logout <u>R</u> efresh
cisco	MONITOR WLAP	is <u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDE	ACK
Commands	Set Time					Set	Date and Time	Set Timezone
Download File Upload File Reboot	Current Time	Tue May 31 11:0	7:38 2011					
Config Boot	Date	Month Day		May	•		_	
Reset to Factory Default Set Time		Year		31 ¥ 2011				
Login Banner	Time							
		Hour Minutes		11 • 7				
	Timezone	Seconds		38				
		Delta		hours 0	mins 0			
		Location ¹	(GMT	-8:00) Pacific	Time (US and Cana	da) 🗸		
	Foot Notes							
	1. Automatically set	s daylight savings tin	e where used.					

Procedure 9 Configure SNMP

- Step 1: In Management > SNMP > Communities, click New.
- Step 2: Enter the Community Name. (Example: cisco)
- Step 3: Enter the IP Address. (Example: 10.4.48.0)
- Step 4: Enter the IP Mask. (Example: 255.255.255.0)
- Step 5: In the Status list, choose Enable, and then click Apply.

cisco	MONITOR WI	LANS CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	HELP FI		gout <u>R</u> efres
Management	SNMP v1 / v2	2c Community > N	lew			< B	ack	Apply
Summary SMMP General SMMP V3 Users Communites Trap Receivers Trap Logs HTTP-HTTPS Telnet-SSH Serial Port Local Management Users User Sessions > Logs Mgmt Via Wireless > Software Activation > Tech Support	Community Nie IP Address IP Mask Access Mode Status	ame 10.4.48.0 255.255.255.0 Read Only • Enable •						

- Step 6: In Management > SNMP > Communities, click New.
- Step 7: Enter the Community Name. (Example: cisco123)
- Step 8: Enter the IP Address. (Example: 10.4.48.0)
- Step 9: Enter the IP Mask. (Example: 255.255.255.0)
- Step 10: In the Access Mode list, choose Read/Write.

Step 11: In the Status list, choose Enable, and then click Apply.

սիսիս							nfiguration Ping L	
CISCO	MONITOR WL	ANS <u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBACK	
Management	SNMP v1 / v2	c Community > N	lew				< Back	Apply
Summary SNMP General SNNP V3 Users Communities Trap Receivers Trap Controls Trap Logs	Community Nar IP Address IP Mask Access Mode Status	me cisco123 10.4.48.0 255.255.255.255.0 Read/Write Enable						
HTTP-HTTPS								
Telnet-SSH								
Serial Port								
Local Management Users								
User Sessions								
▶ Logs								
Mgmt Via Wireless Software Activation 								
Fech Support								

Step 12: Navigate to Management > SNMP > Communities. Point to the blue box for the public community, and then click Remove.

Step 13: On the "Are you sure you want to delete?" message, click OK.

Step 14: Repeat Step 12 and Step 13 for the private community.

cisco	MONITOR WI	LANs	CONTROLLER	WIRELESS	SECURITY	MANA	GEMENT	Sa <u>v</u> e COMMAND	Configurat 5 HELP		Logout <u>R</u> efr
Vanagement	SNMP v1 / v2		_	WINELEDD	<u>5</u> ccold11	11200	GENERI	C <u>o</u> rnikito.		TECODA	New
Summary SNMP	Community Na	ame		IP Address	IP Mask		Access M	ode Stat	us		
General	cisco			10.4.48.0	255.255.2	55.0	Read-Only	Ena	ble		
SNMP V3 Users Communities	cisco123			10.4.48.0	255.255.2		Read-Writ				
Trap Receivers Trap Controls Trap Logs											
HTTP-HTTPS											
Telnet-SSH											
Serial Port											
Local Management Users											
User Sessions											
Logs											
Mgmt Via Wireless											
Software Activation											
Tech Support											



(Optional)

In networks where network operational support is centralized, you can increase network security by using an access control list in order to limit the networks that can access your controller. In this example, only devices on the 10.4.48.0/24 network are able to access the device via SSH or SNMP.

Step 1: In Security > Access Control Lists > Access Control Lists, click New.

Step 2: Enter an access control list name, and then click Apply.

Step 3: In the list, choose the name of the access control list you just created, and then click Add New Rule.

Step 4: In the window, enter the following configuration details, and then click **Apply**.

- · Sequence-1
- · Source-10.4.48.0 / 255.255.255.0
- · Destination—Any
- · Protocol-TCP
- Destination Port—HTTPS
- Action—Permit



Step 5: Repeat Step 3 through Step 4, using the configuration details in the following table.

Table 10 - Rule configuration values

Sequence	Source	Destin ation	Protocol	Destin ation port	Action
2	10.4.48.0/ 255.255.255.0	Any	ТСР	Other/22	Permit
3	Any	Any	TCP	HTTPS	Deny
4	Any	Any	TCP	Other/22	Deny
5	Any	Any	Any	Any	Permit



Step 6: In Security > Access Control Lists > CPU Access Control Lists, select Enable CPU ACL.

Step 7: In the ACL Name list, choose the ACL you just created, and then click Apply.

Procedure 11

Configure management authentication

(Optional)

You can use this procedure to deploy centralized management authentication by configuring an authentication, authorization and accounting (AAA) service. If you prefer to use local management authentication, skip to Procedure 12.

As networks scale in the number of devices to maintain, the operational burden to maintain local management accounts on every device also scales. A centralized AAA service reduces operational tasks per device and provides an audit log of user access, for security compliance and root-cause analysis. When AAA is enabled for access control, it controls all management access to the network infrastructure devices (SSH and HTTPS).

Step 1: In Security > AAA > TACACS+ > Authentication, click New.

Step 2: Enter the Server IP Address. (Example: 10.4.48.15)

Step 3: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)



Step 4: In Security > AAA > TACACS+ > Accounting, click New.

Step 5: Enter the Server IP Address. (Example: 10.4.48.15)

Step 6: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)

Security	TACACS+ Accounting	Servers > New		< Back	Apply
 AAA General RADIUS TACACS+ Authentication Accounting Authorization LOAP LOAP LOAP LOAP Disabled Clients User Login Policies Password Policies Password Policies 	Server Index (Priority) Server IP Address Shared Secret Format Shared Secret Confirm Shared Secret Port Number Server Status Server Timeout	1 • 10.4.48.15 ASCII • 			
Priority Order					
Certificate					
Access Control Lists					
Wireless Protection Policies					
Web Auth					
TrustSec SXP					

Step 7: In Security > AAA > TACACS+ > Authorization, click New.

Step 8: Enter the Server IP Address. (Example: 10.4.48.15)

Step 9: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)

սիսիս			ave Configuration Ping Logout Refresh
CISCO Security	MONITOR WLANS CONTROLLER		ANDS HELP <u>F</u> EEDBACK ADDS HELP SEEDBACK
 AAA General PADIUS TACACS+ Authentication Accounting Authonization LDAP Local Net Users MAA Filtering Disabled Clients User Login Policies AP Policies Password Policies 	Server Index (Priority) Server IP Address Shared Secret Format Shared Secret Confirm Shared Secret Port Number Server Status Server Timeout	1 • 10.4.48.15 ASCII • ••••••• 49 Enabled • S seconds	
Local EAP Priority Order			
Certificate Access Control Lists Wreless Protection Policies Web Auth TrustSec SXP Advanced			

Step 10: Navigate to Security > Priority Order > Management User.

Step 11: Using the arrow buttons, move TACACS+ from the Not Used list to the Used for Authentication list.

Step 12: Using the Up and Down buttons, move TACACS+ to be the first in the Order Used for Authentication list.

Step 13: Use the arrow buttons to move **RADIUS** to the **Not Used** list, and then click **Apply**.



Tech Tip

If using Cisco Secure ACS in order to authenticate TACACS management access to the WLC, you must add the WLC as an authorized network access device. Failure to do so will prevent administrative access to the WLC by using the Secure ACS server.



Create the guest wireless LAN interface

The guest wireless interface is connected to the DMZ of the Cisco ASA 5540 security appliance. This allows guest wireless traffic only to and from the Internet. All guest traffic, regardless of the controller to which the guest initially connects, is tunneled to the guest WLC and leaves the controller on this interface.

To easily identify the guest wireless devices on the network, use an IP address range for these clients that is not part of your organization's regular network. This procedure adds an interface that allows devices on the guest wireless network to communicate with the Internet.

Step 1: In Controller>Interfaces, click New.

Step 2: Enter the Interface Name. (Example: Wireless-Guest)

Step 3: Enter the VLAN Id, and then click Apply. (Example: 1128)

սիսիս							Sa <u>v</u> e Con	figuration	<u>P</u> ing	Logout <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	EEEDBAC	к
Controller	Interfaces	s > New						<	Back	Apply
General Inventory Interfaces Interface Groups Multicast Network Routes Redundancy Internal DHCP Server Molility Management Ports NTP CDP PMIPv6 PMIPv6 mDNS Advanced	Interface VLAN Id		Wireless-Guest 1128							

Step 4: In the **IP Address** box, enter the IP address to assign to the WLC interface. (Example: 192.168.28.5)

Step 5: Enter the Netmask. (Example: 255.255.252.0)

Step 6: In the **Gateway** box, enter the IP address of the firewall's DMZ interface defined in Procedure 2. (Example: 192.168.28.1)

Step 7: In the **Primary DHCP Server**, enter the IP address of your organization's DHCP server, and then click **Apply**. (Example: 10.4.48.10)

ahaha									Logout <u>R</u> efre	
cisco	MONITOR WLANS CO	ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	EEEDBACK		
Controller	Interfaces > Edit							< Back	Apply	Ţ
General										
Inventory	General Information									
Interfaces	Interface Name	wireless-	quest							
Interface Groups	MAC Address		:7e:0a:6f							
Multicast										
Network Routes	Configuration				_					
Redundancy	Guest Lan									
Finternal DHCP Server	Quarantine									
Mobility Management	Quarantine Vlan Id	0								
Ports	NAS-ID	DMZ-WLC-G	iuest							
▶ NTP	Enable DHCP Option 82									
▶ CDP	Physical Information									
▶ PMIPv6	The interface is attached	to a LAG.								
▶ IPv6	Enable Dynamic AP Management									
▶ mDNS	-									
Advanced	Interface Address									
	VLAN Identifier	1128								
	IP Address	192.168.28.								
	Netmask	255.255.255								
	Gateway	192.168.28.	1							
	DHCP Information									
	Primary DHCP Server	10	.4.48.10							
	Secondary DHCP Server									
	DHCP Proxy Mode	Gl	obal 👻							

Tech Tip

To prevent DHCP from assigning addresses to wireless clients that conflict with the WLC's addresses, exclude the addresses you assign to the WLC interfaces from DHCP scopes.



Configure the guest wireless LAN

Step 1: Navigate to WLANs.

Step 2: Hover over the blue list next to your guest WLAN, and then click **Mobility Anchors**.

Step 3: In the Switch IP Address (Anchor) list, choose (local).

Step 4: Click Mobility Anchor Create, and then click OK.

սիսիս						Save Configuration Ping Logout Refi			
CISCO	MONITOR WLANS	<u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK	
WLANs	Mobility Anchors	1						< Back	
WLANs WLANs	WLAN SSID	Guest							
Advanced	Switch IP Address (Anchor)			Data Path	C	ontrol Pat	h	
	Mobility Anchor Cr	eate							
	Switch IP Addres	s (Anchor)	(local)	-					

Step 5: Click Back.

Step 6: Click the **WLAN ID** of the SSID created in Procedure 7. (Example: Guest)

Step 7: On the General tab, in the **Interface/Interface Group(G)** list, choose the interface created in Procedure 12. (Example: wireless-guest)

ahaha								nfiguratio	n <u>P</u> ing	Logout <u>R</u> efresh		
CISCO	MONITOR	WLANS CO	NTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBAC			
WLANs	WLANs >	Edit 'Gue	sť						< Back	Apply		
WLANS WLANS	General	Security	QoS	Advanced								
Advanced	Profile N	lame	Guest									
	Туре		WLAN									
	SSID		Guest									
	Status		🔽 Enab	led								
	Security	Policies	[WPA2]	[Auth(802.1X	11							
				(Modifications done under security tab will appear after applying the changes.)								
	Radio Pr	olicy	All	-								
	Interfac Group(C	e/Interface 3)	wireless	-guest 👻								
	Multicas	t Vlan Feature	🔲 Enable	ed								
	Broadca	st SSID	🗹 Enable	ed								
	Foot Note		sed in combi	nation with IPse	~							
	2 H-REAP	Local Switching	is not suppo	rted with IPsec,	CRANITE aut							
		ent exclusion is FP is not active			f zero means i	nfinity (will require	administrative or	verride to	reset exclu	ded clients)		
				when HREAP Loc ild be enabled to								
	7 Multicast	Should Be End	abled For IPV	6.		er 11/1 races						
				n Radio Policy is tion on maximu		ved						
	10 MAC Fil	tering is not su	pported with	HREAP Local au								
		tering should b unneling, Local		HCP Required s	hould be disab	led.						
						Authentication.						

Step 8: Click the Security tab, and then on the Layer 2 tab, in the Layer 2 Security list, choose None.



Step 9: On the Layer 3 tab, select Web Policy, and then click OK.



Step 10: On the QoS tab, in the Quality of Service (QoS) list, choose Bronze (background), click Apply and then click OK.

🕒 🕗 🔻 🙋 https://19	2.168.19.54/screens/frameset.html							👻 😵 Ce	ertificate Error	
🚖 Favorites 🏾 🌈 DMZ-V	VLC-Guest									
սիսիս							Sa <u>v</u> e	Configuration Ping	Logout	
cisco	MONITOR WLANS COM	TROLLER WIR	ELESS SECURIT	MANAGEMENT	C <u>O</u> MMANDS	HELP	EEEDBACK			
WLANs	WLANs > Edit 'Guest							< Back	Apply	
WLANs WLANs	General Security	QoS Adva	inced							
Advanced									-	
	Quality of Service (QoS		sckground) 💌							
	Application Visibility	Enable	d							
	AVC Profile	none 🕶								
	Netflow Monitor	none 🔻								
	Override Per-User Ba	dwidth Contr	acts (kbps) 🖽							
		DownStream	UpStream							
	Average Data Rate	0	0							
	Burst Data Rate	0	0							
	Average Real-Time Rate	0	0							
	Burst Real-Time Rate	0	0							
	Clear	0	0							
	Ciedi									
	Override Per-SSID Ba	ndwidth Contr	acts (kbps) 🌆							
		DownStream	UpStream							
	Average Data Rate	0	0							
	Burst Data Rate	0	0						*	
	•			III					•	
	Foot Notes									
	1 Web Policy cannot be us 2 FlexConnect Local Switch	ing is not support	ed with IPsec, CRANI	TE authentication, C	verride Interface	ACLS				
	3 When client exclusion is 4 Client MPP is not active i	mabled, a Timeou nless WP42 is cor	it Value of zero mear dioured	is infinity (will requi	re administrative	override t	to reset excluded	l clients)		
	5 Learn Client IP is configurable only when FlexConnect Local Switching is enabled 6 WMM and paper or RES security should be enabled to support higher 11n rates									
	8 Value zero implies there is no restriction on maximum clients allowed.									
	10 MAC Eiltering should be	9 MAC Filtering is not supported with FlexConnect Local authentication 10 MAC Filtering - Analytic the enabled								
	11 Guest tunneling, Local : 12 Max-associated-clients	eature is not sup	corted with FlexConne	ict Local Authentica	tion.					
	13 VLAN based central swi 14 Enabling gtk-randomize	ching is not suppo	orted with FlexConner	t Local Authenticati	on.					
Procedure 14 Configure mobility groups

Step 1: If you are not using AP-SSO then you need to add each of the WLC's to the mobility group. On the guest controller, navigate to Controller > Mobility Management > Mobility Groups.

Step 2: On the Static Mobility Group Member page, note the MAC address, IP address, and mobility group name for the local controller. You need this information for the following steps.

🊖 Favorites 🛛 🏉 DMZ-WLC-	Guest									
.ılı.ılı. cısco		<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS 1	HELP FEEDBACK	Saye Configuration Ping Logout	t <u>R</u> efr
Controller	Static Mo	bility Gro	up Members						New	EditA
General Inventory	Local M	obility Gro	up GUEST							
Interfaces	MAC Ad	dress	IP Address	Group	o Name	Multicast IP	Hash Key		Status	
Interface Groups	88:43:e	:7e:0a:60	192.168.19.54	GUES	r	0.0.0	none		Up	
Multicast Network Routes Redundancy										
Internal DHCP Server										
 Mobility Management Mobility Groups Mobility Anchor Config Multicast Messaging Ports 										
▶ NTP										
▶ CDP										
▶ PMIPv6										
▶ IPv6										
▶ mDNS										
Advanced										

Step 3: On every controller in your organization that is not a resilient WLC and is providing DMZ guest access services, navigate to Controller > Mobility Management > Mobility Groups, and then click New.

Step 4: In the **Member IP Address** box, enter the IP address of the guest controller. (Example: 192.168.19.54 and/or 192.168.19.55 if not using AP-SSO)

Step 5: In the Member MAC Address box, enter the MAC address of the guest controller.

Step 6: In the **Group Name** box, enter the mobility group name configured on the guest controller, and then click **Apply**. (Example: GUEST)

C DMZ-WLC-Guest -								
🕞 🕗 🗢 🙋 https://192.168	1.19.54/screens/frameset.html						🔻 😵 Cer	tificate Error 🏼 🍫 🗙
🖕 Favorites 🛛 🏉 DMZ-WLC-	Guest							
սիսիս						Saye	Configuration Ping	Logout <u>R</u> efresh
CISCO	MONITOR WLANS CO	NTROLLER WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	НЕ <u>Г</u> Ь	EEEDBACK	
Controller	Mobility Group Memb	er > New					< Back	Apply
General Inventory Interfaces Interface Groups Multicast Network Routes ▶ Redundancy ▶ Internal OHCP Server ▼ Molitast Messaging Multicast Messaging Parts ▶ NTP ▶ CDP ▶ DMIP#o6 ▶ ImMIS ▶ mDNS ▶ Advanced	Member IP Address Member MAC Address Group Name Hash	192.16619.55						

Step 7: On the guest controller, navigate to Controller > Mobility Management > Mobility Groups, and then click New.

Step 8: In the **Member IP Address** box, enter the IP address of a campus or remote-site controller. (Example: 10.4.46.64)

Step 9: In the **Member MAC Address** box, enter the MAC address of the campus or remote-site controller.

Step 10: In the **Group Name** box, enter the mobility group name configured on the campus or remote-site controller, and then click **Apply**. (Example: CAMPUS)

🚖 Favorites 🛛 🏉 DMZ-WLC-	Guest								
	MONITOR WLANS CO	INTROLLER WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	EEEDBACK	Sage Configuration Bing	Logout <u>R</u> efn
Controller General	Mobility Group Memb	er > New						< Back	Apply
Inventory Interface Groups Multicast Network Routes > Redundancy > Internal DHCP Server Mobility Ananagement Mobility Ananagement	Member M-Adress Member MAC Adress Group Name Hash	10.4.46.64 88:43:e1:7e:08:a0 CAMPUS none							
Multicast Messaging Ports NTP									
NIP CDP PMIPv6 IPv6 mDNS Advanced									

Step 11: On each controller, click Save Configuration, and then click OK.

Step 12: Repeat Step 7 through Step 11 on every controller in your organization.

Step 13: Navigate to Controller > Mobility Management > Mobility

Groups, and then verify that connectivity is up between all the controllers by examining the mobility group information. In the Status column, all controllers should be listed as **Up**.

uludu cisco	MONITOR WLANS	<u>C</u> ONTROLLER	WIRELESS SECURITY	MANAGEMENT	COMMANDS HELP	<u>F</u> EEDBACK	Sa <u>v</u> e Configura	ition <u>P</u> ing	Logout <u>R</u> efresh
Controller	Static Mobility Gro	up Members					1	New	EditAll
General Inventory	Local Mobility Gro	up CAMPUS							
Interfaces	MAC Address	IP Address	Group Name	Multicast IP	Hash Key		Status		
Interface Groups	88:43:e1:7e:08:a0	10.4.46.64	CAMPUS	0.0.0	none		Up		
Multicast Network Routes	88:43:e1:7e:0a:60	192.168.19.54	GUEST	0.0.0.0	none		Up		
Redundancy									
Internal DHCP Server									
 Mobility Management Mobility Groups Mobility Anchor Config Multicast Messaging 									



Create the lobby admin user account

Typically, the lobby administrator is the first person to interact with your corporate guests. The lobby administrator can create individual guest user accounts and passwords that last from one to several days, depending upon the length of stay for each guest.

You have two options to configure the lobby admin user account.

If you have not deployed Cisco Secure ACS and TACACS+ for management access control to the controller, perform the steps in Option 1.

If you have deployed Cisco Secure ACS and TACACS+ for management access control to the controller, perform the steps in Option 2.

Option 1. Local lobby admin user account

Step 1: In Management > Local Management Users, click New.

Step 2: Enter the username. (Example: Guest-Admin)

Step 3: Enter and confirm the password. (Example: C1sco123)

Step 4: In the User Access Mode list, choose LobbyAdmin, and then click Apply.



Option 2. Centralized lobby admin user account

Create groups in the Cisco Secure ACS internal identity store for network device administrators and helpdesk users. Users in the network device administrator group have enable-level EXEC access to the network devices when they log in, while helpdesk users must type in the enable password on the device in order to get enable-level access.

Step 1: Within Microsoft Active Directory, it is assumed that a lobby ambassador group (Example: Lobby Admins) has been created. Within this group is each of the lobby ambassadors employees within the organization. (Example: Linda Lobby)

inda Lobby Propertie.	25			? ×
Dial-in Er Remote Desktop Ser General Address A		Sessions Personal Virtua Telephones (al Desktop	e control COM+ Member Of
Member of:				
Name	Active Directo	ry Domain Service	s Folder	
Domain Users	cisco.local/Us			
Lobby Admins	cisco.local/Us	ers		
1				
Add	Remove			
	Temove			
Primary group: D	omain Users			
	1 There is no	need to change F	rimary oroun	unless
Set Primary Group	🔄 you have N	facintosh clients o		
	application	s.		
	ок	Cancel /	Apply	Help

Step 2: In Cisco Secure ACS, navigate to Users and Identity Stores > External Identity Stores > Active Directory.

Step 3: Select the **Directory Groups** tab, and in the **Group Name** box, enter the lobby admin group (Example: cisco.local/Users/Lobby Admins), and then click **Add**.

The lobby admin group appears in the Selected Directory Groups list.

Cisco Secure A(Cisco EVAL(Days left: 323)	CS
▶ 😚 My Workspace	Users and Identity Stores > External Identity Stores > Active Directory
Hotwork Resources Jusers and Identity Stores Identity Groups	General Directory Groups Directory Attributes Directory groups must be selected on this page to be available as options in group mapping conditions in policy rules. Click Select foll aquive h adiato to be elect droups from the directory.
 Internal Identity Stores Users Hosts 	Selected Directory Groups:
External identity Stores LDAP Active Directory RSA Securit D Token Servers RADUE identity Servers Certificate Authentication Profile Identity Store Sequences	Group Name Crisco Local/Users/wpn-partner crisco Local/Users/wpn-partner E
Policy Elements	
Construction and Reports	
System Administration	Add A Edit V Replace A Deselect Select GroupName
	cisco.local/Users/Lobby Admins
	Example for group format: cisco.com/Users/Domain/Users 0 = Required fields
Monitoring and Reports	GroupName Cisco local/Users/Lobby Admins Example for group format : cisco cont/sers/Domain Users

Next, the Active Directory group that was just added to Cisco Secure ACS needs to be mapped to a Secure ACS policy.

Step 4: In Cisco Secure ACS, navigate to Access Policies > Access Services > Default Device Admin > Group Mapping, and then at the bottom of the screen, click Create.

Cisco Secure A	cs					
🕨 😚 My Workspace	Acces	is Polici	es > Acces	s Services	Default Device Admin > Group Mapping	
Ivelwork Resources	0	Single	result sel	ection 💿	Rule based result selection	
Users and Identity Stores	Gri	oup Ma	pping Pol	icy		
Policy Elements	Fil	ter: St	tatus		▼ Match if: Equals ▼ ▼ Clear Filter Go ▼	
K. Access Policies Access Services Service Selection Rules			Status	Name	Conditions Results Compound Condition Identity Group	Hit Count
O Default Device Admin	1	10	0	Rule-1	AD-AD1:ExternalGroups contains any cisco.local/Builtin/Network Device Admins All Groups:Network Admins	13100
Identity Grout Magting Authorization ◆ Default Network Access ◆ Remote Access VPN ◆ Writeless LAN Identity Authorization • Max Descision Policy Max Session Drart Settings Max Session Group Settings	:			I		
System Administration						
			Default		If no rules defined or no enabled rule matches. All Groups	18
		create	. ▼] D	uplicate	Edit Delete Move to	

Step 5: Under Conditions, select Compound Condition, in the Dictionary list, choose AD-AD1, and then in the Attribute box, click Select to select External Groups.

Step 6: Under the Value box, click Select.

Step 7: In the String Enum Definition dialog box, select the lobby admin Active Directory group (Example: cisco.local/Users/Lobby Admins), and then click **OK**.

String	Enum Definition	Showing 1-5 of 5 50	🝷 per page 😡
Filter:	▼ Match if: ▼		
	Enum Name		*
	cisco.local/Builtin/Network Device Admins		
	cisco.local/Users/vpn-administrator		
	cisco.local/Users/vpn-employee		
	cisco.local/Users/vpn-partner		
		🚺 🖣 Page	1 of 1 🕨 🕨
OK C	ancel		

Step 8: Under Current Condition Set, click **Add**. The new condition appears in the **Current Condition Set** box.

Condition: Dictionary:	Attribute:	
AD-AD1	▼ ExternalGroups Select	
Operator:	Value:	
contains any ▼	Select Deselect Clear	
Current Condition S	Set:	
	Add V Edit A Replace V	
And≥▼ Or>▼	AD-AD1 ExternalGroups contains any cisco local/Users/Lobby Ad	
Results		
nesuits		

Step 9: Under Results, click **Select**, and then select the Cisco Secure ACS identity group that will mapped to the Active Directory group specified in the Current Condition Set and then click **OK**.

Conditions		
🔽 Compound Co	ndition:	
Condition:		
Dictionary:	Attribute:	
AD-AD1	▼ ExternalGroups Select	
Operator:	Value:	
contains any 👻		
Current Condition	Select Clear	
	Add V Edit A Replace V	
	AD-AD1:ExternalGroups contains any cisco.local/Users/Lobby Ad	
And > • Or > •		
	Delete	
Results		
Identity Group: All (Broups:Lobby Admin	
	(Announced)	
Cancel		Hel

You must create a shell profile for the WLCs that contains a custom attribute that assigns the user lobby admin rights when the user logs in to the WLC.

Step 10: In Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles, click Create.

Step 11: Under the General tab, in the **Name** box, enter a name for the wireless shell profile. (Example: Lobby Admins)

Step 12: On the Custom Attributes tab, in the Attribute box, enter role1.

Step 13: In the Requirement list, choose Mandatory.

Step 14: In the Value box, enter LOBBY, and then click Add.

Favorites 🌈 Cisco Secure ACS							
Cisco Secure A Cisco EVAL(Days left: 324)					acsadmin	acs-1 (Primary)	
🕨 ổ My Workspace	Policy Elements > Auth	orization and F	ermissions > Device Admini	stration > Shell Profile	s > Create		
Interview Resources	General Corr	mon Tasks	Custom Attributes				
 B Users and Identity Stores 	Common Tasks						
Session Conditions	Attribute	Autodies	Requirement	Value			
Custom • Network Conditions • Authorization and Permissions • Network Access • Device Administration Shell Fondles Command Sets	Manually Entere	d					 •
 Named Permission Objects 	Attribute		Requirement Mandatory	Value			
Access Policies	TOTET		Manuatory	LOBBI			
Carlos Monitoring and Reports System Administration							•
	Add A	Edit V F	Replace A Delete				
	Requirement: M Attribute Value:	Static 🔻					
		.0BBY			^		

Step 15: Click Submit.

Next, you create a WLC authorization rule.

Step 16: In Access Policies > Default Device Admin > Authorization, click Create.

Step 17: In the **Name** box, enter a name for the WLC authorization rule. (Example: Lobby Admin)

Step 18: Under Conditions, select Identity Group, and then in the box, enter All Groups:Lobby Admins.

Step 19: Select NDG:Device Type, and then in the box, enter All Device Types:WLC.

Step 20: In the Shell Profile box, enter Lobby Admins, and then click OK.

Conditions		ults are available here for use in poli	-,
Identity Group:	in	 All Groups:Lobby Admins 	Select
NDG:Location:	-ANY-		
NDG:Device Type:	in	 All Device Types:WLC 	Select
Time And Date:	-ANY-		
Protocol:	-ANY-		
Shell Profile: Lobby Ac	Imins	Select	

Step 21: Click Save Changes.

Procedure 16

Configure the internal WLCs for a guest

When a client connects to the guest SSID, the client must be anchored to the controller in the DMZ. The guest clients' traffic is tunneled from the controller to which the access point is connected to the guest controller, where the access point is given an IP address for the DMZ. The clients' traffic is then redirected to the web authentication page located on the guest controller. The client will not be authorized to connect with any IP protocol until it presents credentials to this authentication page.

Step 1: On the WLANs page, in the list, choose Create New, and then click Go.

uluili. cisco		dller w <u>i</u> reless <u>s</u> ecurit		iguration <u>P</u> ing Logout <u>R</u> efresl HELP <u>F</u> EEDBACK
WLANs	WLANs			Entries 1 - 2 of 2
WLANS	Current Filter: None	Change Filter] [Clear Filter]	Create New -	Go
➢ Advanced		V-Data WL4	AN SSID Admin Status NI-Data Enabled NI-Voice Enabled	Security Policies [WPA2][Auth(802.1X)] [WPA2][Auth(802.1X)]

Step 2: Enter the Profile Name. (Example: Guest)

Step 3: In the **SSID** box, enter the guest WLAN name, and then click **Apply**. (Example: Guest)

սիսիս	Sa <u>v</u> e Configuration Ping Logout <u>R</u> efresh				
cisco	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBACK
WLANs	WLANs > New				< Back Apply
 WLANS WLANS Advanced 	Type Profile Name SSID ID	WLAN Guest Guest 3 V			

Step 4: Click the Security tab, and then on the Layer 2 tab, in the Layer 2 Security list, choose None.



Step 5: On the Layer 3 tab, select Web Policy.



Step 6: On the QoS tab, in the Quality of Service (QoS) list, choose Bronze (background), and then click Apply.

սիսիս	Sage Configuration	
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDB	ACK
WLANs	WLANs > Edit 'Guest'	ack App
♥ WLANS WLANS ▶ Advanced	Ceneral Security QoS Advanced Quality of Service (qoS) Branze (background) • Application Visibility Brabled AVC Profile none • Netflow Monitor none • Override Per-User Bandwidth Contracts (kbps) ⁴⁶	
	DownStream UpStream	
	Average Data Rate 0 0 Burst Data Rate 0 0 Average Real-Time Rate 0 0 Burst Real-Time Rate 0 0	
	Override Per-SSID Bandwidth Contracts (kbps) ^{#4} DownStream UpStream	
	Average Data Rate 0 0	•

Step 7: On the General tab, to the right of Status, select **Enabled**, and then click **Apply**.

uluulu cisco	Saye Configuration [Ping] Logout (Befr Monitor Wlans Controller Wireless Security Management Commands Help Feedback
WLANs	WLANs > Edit 'Guest' < Back Apply
WLANs	General Security QoS Advanced
Advanced	Profile Name Guest
	Type WLAN
	SSID Guest
	Status 🔽 Enabled
	Security Policies [WPA2][Auth(802.1X)] (Modifications done under security tab will appear after applying the changes.)
	Radio Policy All 👻
	Interface/Interface management - Group(G)
	Multicast Vian Feature 🔲 Enabled
	Broadcast SSID 🗹 Enabled
	Foot Notes
	2 H-HEAP Local Switching is not supported with IPsec, CRANUTE authentication 3 When clinet exclusion is enabled, a Timouci Vielue of zero means infinity (will require administrative override to reset excluded clients) 4 Client MFP is not excluse in sensible, a Timouci Vielue of zero means infinity (will require administrative override to reset excluded clients) 5 Learn Client IP is configurable only when HREAP Local Switching is enabled 6 WMM and open or AES security should be enabled to support higher 11n rates 7 Multicast Should Be Enabled for IPV6. 8 Band Select is configurable only when RREAP to JWI. 9 Value zero implies there is no restriction on maximum clients allowed.
	10 MAC Filtering is not supported with HREAP Local authentication 11 MAC Filtering should be enabled. 12 Guest Lunneling, Local switching, DHCP Required should be disabled. 13 Max-associate-clients fractions is not supported with HREAP Local Authentication.

Step 8: Click Back.

Step 9: Hover over the blue list next to your guest WLAN, and then click **Mobility Anchors**.

Step 10: In the **Switch IP Address (Anchor)** list, choose the IP address of the guest controller. (Example: 192.168.19.54)

Step 11: Click Mobility Anchor Create, and then click OK.

 cisco	MONITOR WLANS CONTRO	LER WIRELESS <u>S</u> E	CURITY MANAGEMENT		n <u>P</u> ing Logout <u>R</u> efresh EEDBACK
WLANS WLANS WLANS WLANS Advanced	MONITOR WLANS CONTRO Mobility Anchors WLAN SSID Guest-10k Switch IP Address (Anchor) 192.166.19.54 Mobility Anchor Create Switch IP Address (Anchor)	LER WIRELESS SE	Data Path up	COMMANDS HELP E	< Back

Step 12: Repeat Step 1through Step 10 for every internal controller in your organization.



Now you can use the lobby administrator account to create usernames and passwords for partners, customers, and anyone else who is not normally granted access to your network.

Step 1: Using a web browser, open the DMZ wireless LAN controller's web interface (for example, https://guest-1.cisco.local/), and then log in using your LobbyAdmin account with the username and password created in Active Directory. (Example: LindaLobby/c1sco123)

Step 2: From the Lobby Ambassador Guest Management page, click New.



Step 3: Create a new username and password, or allow the system to create a password automatically by selecting **Generate Password**.

،،۱،،۱،، cısco	Lobby Ambassador Gues	t Management	Logou	t Refresh Help
Guest Management	Guest Users List > No	ew	< Back	Apply
	User Name	partner		
	Generate Password	V		
	Password			
	Confirm Password	••••••		
	Lifetime	1 day Message from webpage		
	Guest User Role	The generated password for this user is BINc54yY		
	WLAN SSID			
	Description			

Step 4: Click Apply. The new user name and password are created.

With a wireless client, you can now test connectivity to the guest WLAN. Without any security enabled, you should receive an IP address, and after opening a web browser, you should be redirected to a web page to enter a username and password for Internet access, which will be available to a guest user for 24 hours.

Appendix A: Product List

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	
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	

Wireless LAN Access Points

Functional Area	Product Description	Part Numbers	Software
Wireless Access Points	Cisco 3600 Series Access Point Dual Band 802.11a/g/n and CleanAir with Internal Antennas	AIR-CAP3602I-x-K9	7.4.100.0
	Cisco 3600 Series Access Point Dual Band 802.11a/g/n and CleanAir with External Antennas	AIR-CAP3602E-x-K9	
	Cisco 2600 Series Access Point Dual Band 802.11a/g/n and CleanAir with Internal Antennas	AIR-CAP2602I-x-K9	
	Cisco 2600 Series Access Point Dual Band 802.11a/g/n and CleanAir with External Antennas	AIR-CAP2602E-x-K9	
	Cisco 1600 Series Access Point Dual-band controller-based 802.11a/g/n with Internal Antennas	AIR-CAP1602I-x-K9	
	Cisco 1600 Series Access Point Dual-band controller-based 802.11a/g/n with External Antennas	AIR-CAP1602E-x-K9	

Access Control

Functional Area	Product Description	Part Numbers	Software
Authentication Services	ACS 5.3 VMware Software and Base License	CSACS-5.3-VM-K9	5.3

Data Center Core

Functional Area	Product Description	Part Numbers	Software
Core Switch	Cisco Nexus 5596 up to 96-port 10GbE, FCoE, and Fibre Channel SFP+	N5K-C5596UP-FA	NX-OS 5.2(1)N1(1b)
	Cisco Nexus 5596 Layer 3 Switching Module	N55-M160L30V2	Layer 3 License
	Cisco Nexus 5548 up to 48-port 10GbE, FCoE, and Fibre Channel SFP+	N5K-C5548UP-FA	
	Cisco Nexus 5548 Layer 3 Switching Module	N55-D160L3	
Ethernet Extension	Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T (enhanced) Fabric Extender	N2K-C2248TP-E	—
	Cisco Nexus 2000 Series 48 Ethernet 100/1000BASE-T Fabric Extender	N2K-C2248TP-1GE	
	Cisco Nexus 2000 Series 32 1/10 GbE SFP+, FCoE capable Fabric Extender	N2K-C2232PP-10GE	

LAN Access Layer

Functional Area	Product Description	Part Numbers	Software
Modular Access Layer Switch	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.3.0.SG(15.1-1SG)
	Cisco Catalyst 4500 E-Series Supervisor Engine 7L-E	WS-X45-SUP7L-E	IP Base license
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+ ports	WS-X4648-RJ45V+E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+,UPoE ports	WS-X4748-UPOE+E	
Stackable Access Layer	Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-48PF-S	15.0(2)SE
Switch	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-24P-S	IP Base license
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
Standalone Access Layer Switch	Cisco Catalyst 3560-X Series Standalone 48 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-48PF-S	15.0(2)SE IP Base license
	Cisco Catalyst 3560-X Series Standalone 24 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-24P-S	
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
Stackable Access Layer Switch	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-48FPD-L	15.0(2)SE LAN Base license
	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-48FPS-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-24PD-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-24PS-L	
	Cisco Catalyst 2960-S Series Flexstack Stack Module	C2960S-STACK	

LAN Distribution Layer

Functional Area	Product Description	Part Numbers	Software
Modular Distribution Layer	Cisco Catalyst 6500 E-Series 6-Slot Chassis	WS-C6506-E	15.0(1)SY1
Virtual Switch Pair	Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4	VS-S2T-10G	IP Services license
	Cisco Catalyst 6500 16-port 10GbE Fiber Module w/DFC4	WS-X6816-10G-2T	
	Cisco Catalyst 6500 24-port GbE SFP Fiber Module w/DFC4	WS-X6824-SFP-2T	
	Cisco Catalyst 6500 4-port 40GbE/16-port 10GbE Fiber Module w/DFC4	WS-X6904-40G-2T	
	Cisco Catalyst 6500 4-port 10GbE SFP+ adapter for WX-X6904-40G module	CVR-CFP-4SFP10G	
Modular Distribution Layer	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.3.0.SG(15.1-1SG)
Switch	Cisco Catalyst 4500 E-Series Supervisor Engine 7-E, 848Gbps	WS-X45-SUP7-E	Enterprise Services
	Cisco Catalyst 4500 E-Series 24-port GbE SFP Fiber Module	WS-X4624-SFP-E	license
	Cisco Catalyst 4500 E-Series 12-port 10GbE SFP+ Fiber Module	WS-X4712-SFP+E	
Stackable Distribution Layer	Cisco Catalyst 3750-X Series Stackable 12 GbE SFP ports	WS-C3750X-12S-E	15.0(2)SE
Switch	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	IP Services license
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	

LAN Core Layer

Functional Area	Product Description	Part Numbers	Software
Modular Core Layer Switch	Cisco Catalyst 6500 E-Series 6-Slot Chassis	WS-C6506-E	15.0(1)SY1
	Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4	VS-S2T-10G	IP services license
	Cisco Catalyst 6500 24-port GbE SFP Fiber Module w/DFC4	WS-X6824-SFP-2T	
	Cisco Catalyst 6500 4-port 40GbE/16-port 10GbE Fiber Module w/DFC4	WS-X6904-40G-2T	
	Cisco Catalyst 6500 8-port 10GbE Fiber Module w/ DFC4	WS-X6908-10G-2T	

WAN Remote Site

Functional Area	Product Description	Part Numbers	Software
Modular WAN Remote-site Router	Cisco 3945 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3945-VSEC/K9	15.1(4)M5
	Cisco 3925 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3925-VSEC/K9	securityk9 license datak9 license
	Data Paper PAK for Cisco 3900 series	SL-39-DATA-K9	
	Cisco 2951 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2951-VSEC/K9	
	Cisco 2921 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2921-VSEC/K9	
	Cisco 2911 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2911-VSEC/K9	
	Data Paper PAK for Cisco 2900 series	SL-29-DATA-K9	
	1941 WAAS Express only Bundle	C1941-WAASX-SEC/K9	
	Data Paper PAK for Cisco 1900 series	SL-19-DATA-K9	
Fixed WAN Remote-site Router	Cisco 881 SRST Ethernet Security Router with FXS FXO 802.11n FCC Compliant	C881SRST-K9	15.1(4)M5 securityk9 license datak9 license

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 added the 7.4 release of firmware for all WLCs.
- We added the virtual Wireless LAN Controller (vWLC) for use in remote sites using Cisco FlexConnect.
- We added multicast support for sites with on-site controllers using the multicast-multicast method.
- We added Cisco Aironet1600 Series Access Points, replacing the Aironet 1040 Series APs.
- For Cisco 5500 and 7500 Series Wireless LAN Controller deployments, we added a new high availability feature called access point stateful switchover (AP SSO), which provides sub-second AP failover and automatic configuration synchronization between two wireless LAN controllers.
- We added link aggregation (LAG) support to the Cisco 2500 and 7500 Series Wireless LAN Controllers.
- We added guest anchor controller support for the Cisco 2500 Series Wireless LAN Controller by providing two choices of anchor controllers (2500 and 5500 Series wireless controllers).



Feedback

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



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-0000355-1 2/13