# 



# Campus Wireless LAN

## Technology Design Guide

August 2014 Series

IIIII CISCO VALIDATED DESIGN

# Table of Contents

Preface	1
CVD Navigator	2
Use Cases	2
Scope	2
Proficiency	3
Introduction	4
Technology Use Cases	4
Use Case: Network Access for Mobile Devices	4
Use Case: Self-Administered Advanced Guest Wireless Access	4
Use Case: High Performance 802.11ac Access	5
Design Overview	5
Deployment Components	7
Wireless Design Models	9
High Availability	12
Multicast Support	12
Band Select	13
ClientLink	15
802.11ac Bandwidth Performance	16
802.11ac Channel Planning	17
Guest Wireless	22
Deployment Details	24
Configuring Cisco Secure ACS for Wireless Infrastructure Access	25
Deploying Redundant Cisco ISE Servers	32
Configuring On-Site AireOS Wireless Controllers	47
Configuring On-Site 5760 (IOS-XE) Wireless Controller	84
Configuring Controller Discovery and Access Point Connectivity	121
Configuring Remote-Site Wireless with Cisco FlexConnect	129
Follow Additional Best Practices	182
Configuring Guest Wireless: Shared Guest Controller	184
Configuring Guest Wireless: Dedicated Guest Controller	201
Configuring Cisco ISE Sponsor Portal Services	258
Configuring Cisco ASA Firewall and Cisco ISE for Guest Wireless	266
Creating and Using Guest Accounts	279
Appendix A: Product List	284
Appendix B: Changes	290

# Preface

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

CVDs include two guide types that provide tested design details:

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

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

## **CVD Foundation Series**

This CVD Foundation guide is a part of the *August 2014 Series*. As Cisco develops a CVD Foundation series, the guides themselves are tested together, in the same network lab. This approach assures that the guides in a series are fully compatible with one another. Each series describes a lab-validated, complete system.

The CVD Foundation series incorporates wired and wireless LAN, WAN, data center, security, and network management technologies. Using the CVD Foundation simplifies system integration, allowing you to select solutions that solve an organization's problems—without worrying about the technical complexity.

To ensure the compatibility of designs in the CVD Foundation, you should use guides that belong to the same release. For the most recent CVD Foundation guides, please visit the CVD Foundation web site.

## **Comments and Questions**

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

# CVD Navigator

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

## **Use Cases**

This guide addresses the following technology use cases:

- Network Access for Mobile Devices—At the headquarters and remote sites, mobile users require the same accessibility, security, quality of service (QoS), and high availability currently enjoyed by wired users.
- Self-Administered Advanced Guest Wireless Access-Authorized employees can administer a guest wireless network that supports time-based customized guest user accounts, multiple mobile device types, and guest authentication portals.
- High Performance 802.11ac Access—Many organizations are looking to leverage high-performance 802.11ac wireless networks for local and remote sites that require wire-like performance for HD video, high client density, and bandwidthintensive applications.

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

## Scope

This guide covers the following areas of technology and products:

- · Onsite, remote-site, and guest wireless LAN controllers
- Integration of 802.11ac using the Cisco AireOS wireless LAN controllers
- Integration of 802.11ac using the Cisco 5700 Series Wireless
   LAN controller
- 802.11ac channel planning, channel bonding and RF-based best practices
- Internet edge firewalls and demilitarized zone (DMZ) switching
- · Campus routing, switching, multicast and QoS
- High availability wireless using HA stateful switchover (HA SSO)
- Management of user authentication and policy using Cisco Identity Services Engine
- Cisco ISE integration with Microsoft Active Directory
- Integration of the above with the LAN and data center switching and Virtual Switching System (VSS)-based infrastructure
- Guest account authentication web portals using Cisco AireOS wireless LAN controllers
- Guest account sponsor portals using Cisco ISE with AireOS and IOS-XE 5760 Controller

## **Related CVD Guides** Campus CleanAir Technology cisco. VALIDATED **Design Guide** Campus Wired LAN cisco. **Technology Design Guide** VALIDATED DESIGN **Device Management** cisco. VALIDATED Using ACS Technology **Design Guide**

To view the related CVD guides, click the titles or visit the CVD Foundation web site.

## Proficiency

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

- CCNP Wireless-3 to 5 years designing, installing, and troubleshooting wireless LANs
- · CCNA Routing and Switching-1 to 3 years installing, configuring, and maintaining routed and switched networks
- CCNP Security—3 to 5 years testing, deploying, configuring, maintaining security appliances and other devices that establish the security posture of the network
- · VCP VMware-At least 6 months installing, deploying, scaling, and managing VMware vSphere environments

3

## **Technology Use Cases**

With the adoption of smartphones and tablets, the need to stay connected while mobile has evolved from a niceto-have to a must-have. The use of wireless technologies improves 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, wireless technology allows connectivity while we move about throughout the day.

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 wired networks have been. Given our reliance on mobility, network access for mobile devices, including guest wireless access, is essential.

#### **Use Case: Network Access for Mobile Devices**

At the headquarters and remote sites, the mobile user requires the same accessibility, security, quality of service (QoS), and high availability currently enjoyed by wired users.

This design guide enables the following network capabilities:

- Mobility within buildings or campus—Facilitates implementation of applications that require an always-on network and that involve movement within a campus environment.
- Secure network connectivity—Enables employees to be authenticated through IEEE 802.1X and Extensible Authentication Protocol (EAP), and encrypts all information sent and received on the WLAN.
- Simple device access—Allows employees to attach any of their devices to the WLAN using only their Microsoft Active Directory credentials.
- Voice services—Enables the mobility and flexibility of wireless networking to Cisco Compatible Extensions voice-enabled client devices.
- Consistent capabilities—Enables users to experience the same network services at main sites and remote offices.

#### Use Case: Self-Administered Advanced Guest Wireless Access

Most organizations host guest user-access services for customers, partners, contractors, and vendors. Often these services give guest users the ability to check their email and other services over the Internet.

This design guide enables the following network capabilities:

- · Allows Internet access for guest users and denies them access to corporate resources
- · Allows groups of users called sponsors to create and manage guest user accounts
- Enables the use of shared and dedicated guest controller architectures

#### Use Case: High Performance 802.11ac Access

With the adoption of 802.11ac devices and the explosive growth of mobile devices, many organizations are employing 802.11ac to support both higher performance and increased client densities. A well understood fact today is that many more people carry Wi-Fi-enabled devices on a daily basis. What is not commonly realized is that the number of Wi-Fi devices per person is also increasing. To address these trends, an increasing number of organizations are deploying 802.11ac. The result is a dramatically improved client experience—similar to that of wired Gigabit Ethernet in many cases.

This design guide enables the following 802.11ac capabilities:

- Introduces 802.11ac on Cisco AireOS and IOS-XE 5760 Wireless LAN Controllers
- Introduces the Cisco Aironet 3700 Series Access Point, which supports 802.11ac
- Introduces 802.11ac support for the Cisco Aironet 3600 Series Access Point
- · Provides guidance on 802.11ac channel planning and the use of Dynamic Channel Assignment
- Provides guidance on RF considerations in mixed 802.11 deployments
- · Introduces 80-MHz channels through the use of 802.11ac channel bonding

### **Design 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.

The benefits of this deployment include:

- **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 Validated Design (CVD) deployment uses a controller-based wireless design. Centralizing configuration and control on Cisco wireless LAN controllers (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.

5

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 controller-based 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.



Figure 1 - Wireless overview

6

#### **Deployment Components**

The CVD 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 CVD release:

- Cisco 2500 Series Wireless LAN Controller–This Cisco AireOS-based 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 Cisco AireOS-based controller supports up to 500 lightweight access points and 7000 clients, making it ideal for large-site and multi-site WLAN deployments. High availability is supported through Stateful Switchover (SSO), which provides subsecond controller failover without requiring the wireless client to re-authenticate.
- Cisco WiSM2–The Cisco Wireless Services Module 2 (WiSM2) for the Cisco Catalyst 6500 series switch is a Cisco AireOS-based controller supporting up to 1000 access points in a service module form factor. When coupled with the Cisco Sup720 or Sup2T supervisor module in the 6500-E or 6500 non-E chassis, the WiSM2 provides the rich set of features available within the AireOS-based family of controllers. High availability is supported through SSO, which provides sub-second controller failover without requiring the wireless client to re-authenticate.
- Cisco 5760 Series Wireless LAN Controller—The Cisco 5760 is designed for 802.11ac networks with up to 60 Gbps of capacity, supporting up to 1000 access points and 12,000 clients per controller. This is accomplished through the Cisco Unified Access Data Plan application-specific integrated circuit (ASIC). The 5760 provides investment protection in a proven high performance and scalable architecture.
- 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 requirements to deploy the Cisco FlexConnect solution in remote-site networks. High availability is supported through SSO, which provides sub-second controller failover without requiring the wireless client to re-authenticate.

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 access-point 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 is 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 downloads its configuration and synchronizes 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 CVD wireless design is based on Cisco generation 2 wireless access points, which offer robust wireless coverage with up to nine times the throughput of 802.11a/b/g and 802.11ac networks (1600, 2600 3600 and 3700). The following access points are included in this CVD release:

 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 CVD release includes two Cisco CleanAir access points:

- Cisco Aironet 2600 Series Access Points with Cisco CleanAir technology create a self-healing, selfoptimizing 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 high-performance 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.

This CVD release includes two 802.11ac access points:

- Cisco Aironet 3600 Series Access Point using the 802.11ac Wave 1 Adaptive Radio Module (AIR-RM30000AC-x-K9). Installing the 802.11ac adaptive radio module for the Cisco Aironet 3600 Series Access Point provides enterprise-class reliability and wired-network-like performance by supporting three spatial streams and 80-MHz wide channels for a maximum data rate of 1.3 Gbps.
- Cisco Aironet 3700 Series access point delivers 802.11ac performance of up to 1.3G bps, enabling a new generation of Wi-Fi clients such as smartphones, tables and high-performance laptops with 802.11ac support. The 3700 Series supports 4x4 MIMO with 3 spatial streams (with 802.3at PoE+) along with Cisco CleanAir technology and robust security capabilities.

For more information about Cisco CleanAir, see the Campus CleanAir Technology Design Guide.

8

#### **Wireless Design Models**

Cisco Unified Wireless networks support two major campus design models: Local mode 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 can be connected to a data center services block as described in this guide or can be connected to a LAN distribution layer at the site. Wireless traffic between wireless LAN clients and the LAN is tunneled by using the Control and Provisioning of Wireless Access Points (CAPWAP) protocol between the controller and the access point.





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.

9

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 controller-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 comprises a data center.
- 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 a Cisco 2500, 5500, WiSM2 or 5700 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.

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's native VLAN is used for all CAPWAP communication between the access point and the controller. This mode of operation is referred to as FlexConnect local switching and is the mode of operation described in this guide.

The other mode of operation, which is not discussed in this guide, is called *FlexConnect centrally switched*. In this mode, a majority of the traffic is tunneled back to the centrally located wireless LAN controller, allowing the administrator to configure access control lists (ACLs) to selectively switch some local traffic.





Cisco FlexConnect can also tunnel traffic back to the centralized 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. In a shared controller model, both local-mode and FlexConnect configured access points share a common controller. Shared controller architecture requires that the wireless LAN controller support both Flex-Connect local switching and local mode. The wireless LAN controllers that support both within this CVD are the Cisco WiSM2, 5500, and 2500 Series Wireless Controllers.

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. If you don't meet the requirements for a shared controller, you can deploy a dedicated controller pair by using a Cisco 5500, WiSM2 or 2500 Series Wireless LAN Controller, Cisco vWLC, or Cisco Flex 7500 Series Cloud Controller. The controller should reside in the data center. 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 Validated 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) in Cisco AireOS release 7.3 and client Stateful Switchover (Client SSO) in Cisco AireOS release 7.5, the resiliency of the wireless network continues to improve. Now that these two features (AP SSO and client SSO) are available within a single Cisco AireOS controller release, they will collectively be referred to as high availability SSO (HA SSO). By adopting the cost effective HA SSO licensing model, Cisco wireless deployments can improve the availability of the wireless network with controller recovery times in the sub-second range during a WLC disruption. In addition, HA SSO allows the resilient WLC to be cost-effectively licensed as a standby resilient controller with its access point (AP) license count being automatically inherited from its paired primary WLC. This is accomplished by purchasing a standby resilient controller using the HA SKU available for the Cisco 5500, 7500 and WiSM2 Series WLCs. Support for HA SSO within the WiSM2 controller family requires that both WiSM2 WLCs are deployed in one of the following ways:

- Within a Cisco Catalyst 6500 Series Switch pair configured for VSS operation as described in this guide.
- Within the same Cisco Catalyst 6500 Series Switch chassis.
- Within a different Cisco Catalyst 6500 Series Switch chassis when the Layer 2 redundancy VLAN is extended.

Operational and policy benefits also improve as the configuration and software upgrades of the primary WLC are automatically synchronized to the resilient standby WLC.

The following table shows which controllers support the HA SSO Feature

WLC model	HA SSO	N+1 redundancy	Link aggregation group (LAG)
vWLC	No	Yes	Yes (Through VMWare)
2500	No	Yes	Yes
5500	Yes	Yes	Yes
WiSM2	Yes	Yes	N/A
5760	Yes1	Yes	Yes
7500 Flex	Yes	Yes	Yes

Table 1 - High availability feature support

Note:

1. The Cisco 5760 Series Wireless LAN Controller supports AP SSO using the stacking cable.

#### **Multicast Support**

Video and voice applications continue to grow 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.

This guide fully supports multicast transmission for the onsite controller through the use of multicast-multicast mode (MC-MC). *Multicast-multicast mode* uses a multicast IP address in order to more efficiently communicate multicast streams to access points that have wireless users subscribing to a particular multicast group. MC-MC mode is supported on the Cisco 2500, 5500, WiSM2, and 5760 Series Wireless LAN Controllers.

Remote sites that utilize the Cisco Flex 7500 Series Cloud Controller or Cisco vWLC using Cisco FlexConnect in local switching mode can also benefit from the use of multicast-based applications. Multicast in remote sites leverage 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 each of the wireless design models described in this guide, the multicast support that users are accustomed to on a wired network is available wirelessly for those applications and wireless users that require it.

#### **Band Select**

Over time with the advent of consumer devices operating in the 2.4GHz industrial, scientific and medical band (ISM) band, the level of noise resulting in interference in this band has grown considerably. Likewise, many of the wireless devices available today are dual band and can operate in either the 2.4 GHz or 5 GHz band.

With critical business class devices, it would be advantageous to influence these devices to utilize the 5 GHz band with the objective of much lower interference and therefore a better user experience.

Many dual-band wireless devices will first send a probe request on the 2.4 GHz band looking for a 2.4 GHz access point within range. Subsequent to this 2.4 GHz probe request, the wireless device will send out a 5 GHz probe a few milliseconds later looking for a 5 GHz access point. In dual-band wireless networks, the 2.4 GHz probe response will be received first by the wireless device followed by the 5GHz probe response. Most times, the wireless device will then connect using the 2.4 GHz band even though a 5 GHz probe response was received after the 2.4 GHz probe response.

Band Select delays the probe response to the 2.4 GHz probe by a few hundred milliseconds, allowing the AP to determine if the wireless device is a dual-band device. A dual-band wireless device is detected when a 2.4 GHz and 5 GHz probe is received from the same device. By delaying the 2.4 GHz probe response and providing the 5 GHz probe response prior to the 2.4 GHz probe response, it is possible to influence the wireless client to connect to the preferred 5 GHz band.

Band Select for voice and video devices is not recommended because it introduces delay in responding to probe requests in the 2.4 GHz band. For real-time streaming devices that are moving from a 5 GHz area into a 2.4 GHz covered area, or clients that are roaming between 2.4 GHz access points, this delay could result in momentary disruption of connectivity. With data-only based traffic flows, this delay is negligible and generally does not impact application access.

The Band Select algorithm uses a number of default values to determine if a wireless client is in fact dual-band capable. There are also times when a dual-band client will disable a particular radio based on the user deciding to disable it for any number of reasons.

The following table lists the values and their meaning. These values are used by default on both Cisco AireOS and Cisco IOS-XE wireless LAN controllers. It is not recommend that these values be changed, but are provided here with their definitions.

Table 2 -	Band Select default	values and	usage
-----------	---------------------	------------	-------

Field name	Default value	Purpose
Probe Cycle Count	2	The number of client 2.4 GHz probe requests to wait until determining that the client is capable of only 2.4 GHz
Scan Cycle Period Threshold (ms)	200	The number of milliseconds that represents one client probe cycle
Age Out Suppression (seconds)	20	The number of seconds to wait to hear a client probe before removing the client from the Band Select table
Age Out Dual Band (seconds)	60	The number of seconds to wait to hear a 5 GHz probe from a dual-band client before marking the client as uni-band only
Acceptable Client RSSI (dBm)	-80	The minimum received signal strength indication (RSSI) value that must be met from a client probe before sending a probe response

Figure 4 - Band Select-Impacts to real-time applications





Wireless deployments that mix data, voice, and real-time services on a single SSID should not use Band Select on that WLAN. This includes voice applications such as Jabber, Facetime and Skype among other real-time applications.

#### ClientLink

ClientLink uses beam forming to improve the Signal-to-Noise Ratio (SNR) for all wireless clients and is not limited to those which support the 802.11n standard. These performance improvements in the downstream direction (AP → wireless client) enable better throughput by reducing retransmissions and facilitating higher data rates. Furthermore, by reducing the time any given wireless client is using the RF channel, overall performance of the wireless network in both the uplink and downlink direction is improved.

ClientLink version 2.0 is enabled by default and is supported by second generation access points such as the Cisco Aironet 1600, 2600 and 3600 Series. Cisco ClientLink 3.0 is supported on the Cisco Aironet 3700 Series Access Points and is also enabled by default. Legacy ClientLink (version 1.0) is supported only on first generation access points such as the Cisco Aironet 1140, 3500, 1250, and 1260 Series and is disabled by default. On a given WLC, ClientLink is enabled on an entire radio band (802.11b | 802.11a) or an AP basis.

Figure 5 - ClientLink optimization



#### 802.11ac Bandwidth Performance

There has been no other time in the evolution of Wi-Fi based wireless technology that has seen such significant performance improvements than with the introduction of 802.11ac. Beginning in 1997 the original 802.11 standard yielded a theoretical physical layer (PHY) performance of 2 Mbps. Today, with the introduction of 802.11ac Wave 1 with 3 Spatial Streams (3SS), the theoretical maximum PHY performance jumps to 1.3 Gbps.

Year	Technology	Theoretical PHY performance	Expected user performance <sup>1</sup>
1997	802.11	2 Mbps	1 Mbps
1999	802.11b	11 Mbps	6 Mbps
1999	802.11a	54 Mbps	25 Mbps
2003	802.11g	54 Mbps	25 Mbps
2003	802.11a/g	54 Mbps	13-25 Mbps
2007	802.11n	450 Mbps w/ 3SS	180-220 Mbps
2013	802.11ac Wave 1	1.3Gbps w/ 3SS	up to 750 Mbps
Future	802.11ac Wave 2	2.4-3.5 Gbps	To be determined

Table 3 - 802.11ac Bandwidth performance

Note:

1. In b/g mixed environment the user experience can be expected to be 13 Mbps.

Actual wireless performance is a function of a number of variables including distance, spectrum quality, wireless adapter, wireless adapter interface (USB 2.0, USB 3.0), BSS/cell load, wireless driver efficiency, number of spatial streams, device type (battery vs. AC powered), number of and placement of antenna, transmission direction (uplink/downlink), channel selection vs. power (UNII-3 and UNII-2 over UNII 1) and the overall RF environment among others. Be aware that different types of 802.11ac wireless clients are not equal. Some battery-powered devices are purposely built with only 1 transmitter to conserve the battery, while other AC-powered devices may have 3 spatial streams but have a poorly performing interface (USB 2.0) or inefficient driver. Additionally, consider adjacent mixed cells using 802.11a resulting in longer channel usage due to lower transmit speed. When 40 MHz bonded adjacent 802.11a/n is deployed with misaligned primary channel, the benefits of the Clear Carrier Assessment mechanism are not realized.

The 802.11ac Wave 1 specification includes a number of technologies, as detailed in the following, which are responsible for this significant performance improvement.

- 802.11ac is implemented only in the quieter and less crowded 5 GHz band, so it's not possible to have a 2.4 GHz 802.11ac implementation.
- 802.11n used 64QAM, allowing for 6 bits to be transmitted per symbol. 802.11ac expands significantly
  on these gains by employing a 256 QAM allowing 8 bits per symbol and a fourfold increase in
  performance. In simplest terms, Quadrature Amplitude Modulation (QAM) is a modulation technique that
  uses waveform phase and amplitude to encode data. With 256 QAM there are 256 symbols, resulting in
  higher throughput.
- Channel width has been expanded allowing 20, 40, and 80 MHz wide channels in 802.11ac Wave 1; and 20, 40, 80, 80+80, and 160 MHz in Wave 2.
- Beamforming was first available with 802.11n, but has been enhanced and included in the 802.11ac specification. This technology allows the access point to *beam steer* or direct a concentration of signals at the receiver that combine to effectively increase the quality and signal level at the receiver. It gets even better in Wave 2 of 802.11ac, where multiuser beam forming allows a single access point to transmit to 4 wireless clients at the same time and on the same frequency, allowing each client to have its own dedicated spatial stream.

#### 802.11ac Channel Planning

Channel assignment when using Radio Resource Management (RRM) and Dynamic Channel Assignment (DCA) is simpler then it was in the early days of 802.11. As such there are some things to consider before making the decision to bond channels. While this guide assumes a greenfield deployment, network administrators of existing wireless environments may want to move more cautiously.

If your environment today is limited to the standard 20 MHz wide channels, it is recommended that you use a phased rather than direct approach when you switch to 80 MHz wide channels. The initial step would be to enable a Dynamic Frequency Selection (DFS) channel set if it is not already enabled. Using DFS channels requires you to scan the access point scan for the use of radar, and if it is detected, move to another channel or reduce the transmit power. By enabling the DFS channels, a wider range of RF spectrum is available as permitted by your regulatory domain. This in turn enables greater channel bonding choices by DCA.

With DFS channels enabled, four 80-MHz channels and eight 40-MHz channels are available in the U.S.

Number of channels available	U.S.	EU	China	India	Japan	Russia
20MHz channels	18	16	5	13	19	16
40MHz channels	8	8	2	6	9	8
80MHz channels	4	4	1	3	4	4

#### Table 4 - Worldwide 5GHz channel availability

#### Tech Tip

DFS channels (e.g., 120-128) are unusable because the standard mandates a 10 minute quiet period before becoming the channel master device after the detection of radar. Environments that employ the use of DFS channels should take this into consideration.

The following lists a few of the considerations for 40 MHz and 80 MHz wide channel usage:

- Density of AP deployment
- Channel isolation
- · Mixed cell environments
- Adjacent mixed cell and proper 802.11ac primary channel selection
- · Consumer wireless device support of DFS channel set
- · Increased transmit power in UNII-2 and UNII-3 bands
- Increased battery usage in UNII-2 and UNII-3 bands

#### i Tech Tip

The approved spectrum within each regulatory domain evolves over time. Please verify the current channel availability in your regulatory domain.

With the advent of 80MHz wide channels in 802.11ac Wave 1, and the upcoming 160MHz wide channels in Wave 2, there are some considerations regarding channel planning. The spectrum available in the U.S. is shown below.





The number of 20 MHz channels in the 5 GHz band is plentiful, but this can quickly change as 80 MHz and 160 MHz (Wave 2) are deployed within the enterprise.

Figure 6 explains the effects of 40 MHz and 80 MHz channel selections.

As has been the case since the inception of RF-based data communication, the elimination RF interference as well as co-channel interference must be considered in the channel planning process.

The 802.11ac standard allows for the backward compatibility with 802.11n or 802.11a clients in a number of aspects. Beacons are always transmitted in the primary 20MHz channel, allowing legacy clients to discover the wireless network. To aid in the elimination of co-channel interference, the 802.11ac standard has a 20 MHz multi-channel based enhanced Request to Send (RTS) and Clear to Send (CTS) mechanism.

The worst case scenario is an 802.11ac AP configured for 80 MHz wide channel using channel 36 as its primary 20 MHz sub-channel. In this scenario, the 80 MHz wide 802.11ac channel comprises sub-channels 36, 40, 44 and 48–any one of which could be shared by an adjacent 802.11a/n access point. Before transmitting, the 802.11ac access point transmits an RTS on each of the four 20 MHz sub-channels comprising the 80 MHz bonded channel. An adjacent AP upon hearing this will send a CTS back and mark its channel as busy, temporarily preventing it from transmitting. In the best case, the result is a successfully transmitted and interference free 80 MHz wide transmissions.

In the event however that a nearby AP is already transmitting when the RTS is sent, the CTS will not be received. In that case, the 802.11ac access point only transmits on the 20 MHz sub-channels that it received the CTS, and in doing so avoids the generation of co-channel interference, resulting in temporarily reduced throughput.

The goal of effective 802.11ac RF channel planning is the same as it has always been—to avoid co-channel interference whenever possible. In doing so, the entire 40 MHz or 80 MHz-wide bonded channels can transmit using each of their sub-channels, improving performance in the service area. In 802.11ac environments where there are 802.11a and/or 802.11an service areas (aka mixed cell), the selection of the primary channel is critical in order to allow the Clear Carrier Assessment process to listen before transmitting. In general however, most 802.11ac implementations do not listen solely to the primary channel but will instead listen to the entire 80MHz channel before beginning a transmission.

Because of the complexities involved, mixed cell, Unlicensed National Information Infrastructure (UNII) channels, client types and various regulatory domain limitations, and channel planning and the manual assignment of channels should be performed by an experienced wireless network engineer. In most other cases, allowing DCA and RRM to make the necessary channel assignments will provide optimum 802.11ac results.

While most 802.11ac networks rely on the DCA process to automatically select the channel assignment, Figure 7 graphically shows one possible channel planning strategy. As of this writing, this is all of the regulatory domains with the exception of China, which is limited to one 80 MHz channel.

i Tech Tip				
The naming standard below for bonded channel cells shows the starting channel, the channel offset for the primary 20 MHz channel, and the channel offset for the secondary 40 MHz channel. Figure 7 is meant to illustrate the considerations involved in effective channel selection. Note the selection of Channel 44 as the primary channel used in the bonded channels. This ensures proper Clear Carrier Assessment functionality providing optimum performance.				
<b>40 MHz 802.11a/n Channel Naming Examples</b> (Primary channel)+1 40+1 = Primary 20 on 40, Secondary 20 on 44 (Primary channel)-1 40-1 = Primary 20 on 40, Secondary 20 on 36				
80 MHz 802.11ac Channel Naming Examples (Primary channel)+1 [+2] 36+1[+2] = Primary 20 on 36, Secondary 20 on 40, Secondary 40 on 44 and 48				
(Primary channel)-1 [+2] 40-1[+2] = Primary 20 on 40, Secondary 20 on 36, Secondary 40 on 44 and 48				
(Primary channel)+1 [- 2] 44+1[-2] = Primary 20 on 44, Secondary 20 on 48, Secondary 40 on 36 and 40				
(Primary channel)-1[-2] 48-1[-2] = Primary 20 on 48, Secondary 20 on 44, Secondary 40 on 36 and 40				





The utilization of 802.11ac channel allocation depends greatly on the wireless clients being served. For example, a deployment where most of the wireless devices are legacy 20 MHz based 802.11a or 40 MHz 802.11n. In the channel strategy describe previously, the plan is to lay out 80 MHz channels with no overlap. But if most of the clients are not yet capable of 802.11ac, it is possible to overlap 802.11ac channels.

Each 80MHz channel is comprised of a primary and secondary 20 MHz sub-channel, as shown in the following figure.



Figure 8 - 802.11ac Overlapping channel in mixed client environments

By using Clear Carrier Assessment, an access point which needs to transmit to a client first listens to its primary channel. If a carrier signal is detected with a signal at or above its prescribed Clear Carrier Assessment threshold values, it will lose the contention and hold off transmitting. This listen-before-talking allows 802.11ac to co-exist with other non-802.11ac wireless clients.

Protocol	Primary	Secondary 20 MHz	Secondary 40 MHz
802.11a	-82dBm	-	-
802.11n	-82dBm	-62 dBm (20 dB liberty)	-
802.11ac	-82dBm	-72 dBm (10 dB liberty)	-76 to -79 (3-6 dB liberty)

In the preceding table, all three protocols have equal contention on the primary channel. Any primary operating within a secondary 20 or 40 will lose contention and any secondary 20 operating in a secondary 40 will win contention over the other secondary.

With Radio Resource Management (RRM), Transmit Power Control (TPC), and Dynamic Channel Assignment (DCA), the process of channel selection can be both automated and optimized. In the implementation section of this guide, enabling 80MHz channels using DCA for all 802.11ac access points in the network is described.

#### **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





Both shared controller and dedicated controller pair deployment models within the Internet edge demilitarized zone (DMZ) are supported for wireless guest services within this CVD.

If you have a single 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 DMZ Guest VLAN will not have an associated Layer 3 interface or switch virtual interface (SVI). As such, each wireless client on the guest network will use 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 Cisco 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. Other controllers such as Cisco WiSM2 and Cisco 5760 Series Wireless LAN Controllers can provide guest anchoring services as described, but most organizations will use other WLC models and therefore these deployment models are not covered in this guide.

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.

# ITech TipIf you are using a Cisco IOS-XE based 5760 WLC with other Cisco AireOS controllers<br/>either as a Guest Anchor in the Internet edge or as a remote anchor within your<br/>campus, you must enable the New Mobility (Converged Access) feature. You can find<br/>this global configuration Controller > Mobility Management > Mobility Configuration.If you don't enable New Mobility (Converged Access), Mobility Peering cannot be<br/>established between the WLCs. This is because Cisco AireOS controllers use Ethernet<br/>over IP (EoIP) while Cisco IOS-XE controllers use CAPWAP (UDP 16666/16667). Once<br/>New Mobility (Converged Access) is enabled on the AireOS WLC, the time to detect<br/>a failure within an AireOS HA SSO configured WLC pair is increased significantly.<br/>Configuration synchronization, license inheritance, and software upgrades to the<br/>resilient backup WLC are unaffected.

This guide covers the use of the Cisco 5760 Series Wireless LAN Controller as an onsite centralized campus wireless LAN controller. The Cisco 5760 Unified Access Wireless LAN Controller can be deployed in a number of different models. With the introduction of Converged Access, a number of new features such as Mobility Controller (MC), Mobility Agent (MA), and Mobility Oracle (MO) have also been introduced.

The deployment model used in this CVD for the Cisco 5760 Series Wireless LAN Controller is similar to that of Cisco AireOS, namely Cisco Unified Wireless Network (CUWN). In the CUWN architecture, controllers maintain both the MC and MA functions on the controller. Future versions will begin to separate these functions in order to provide additional scaling capabilities. This approach is consistent with many enterprise deployments of the 5760 with the intention of moving the MA onto Cisco Catalyst 3850/3650 Series Switches as the access layer switches are upgraded.

# Deployment Details

How to Read Commands			
This guide uses the following convention commands that you enter at the comm interface (CLI).	ons for land-line	Commands at a C Router# <b>ena</b>	LI or script prompt: . <b>ble</b>
Commands to enter at a CLI prompt:		Long commands the Enter them as one	hat line wrap are underlined. command:
configure terminal		police rate	e 10000 pps burst 10000
Commands that specify a value for a va	ariable:	packets con	form-action
ntp server 10.10.48.17		Noteworthy parts of configuration files)	of system output (or of device are highlighted:
Commands with variables that you mus	st define:	interface Vl	an64
class-map <b>[highest class n</b>	ame]	ip address	10.5.204.5 255.255.255.0

This design 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.

Network service	CVD 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	

Table 6 - Universal design parameters

Many organizations use the 802.1X and RADIUS protocols to authenticate and impose user policy to both their wired and wireless networks. A local directory is commonly used that provides specific information regarding users' rights and privileges. Common examples include an LDAP-based user directory as well as perhaps the most popular Microsoft Active Directory.

In addition to providing user authentication services, network components such as switches, wireless LAN controllers, routers, firewalls require administrative authentication, authorization and accounting (AAA) when managed by the network administrator.

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 Terminal Access Control Access Control System (TACACS+) protocol is commonly used. Given the common usage for TACACS+ and its continued use for providing AAA services for network infrastructure components, Cisco Secure ACS is used in this deployment solely for controlling administrative access to the network control plane.

With the increase in end-user policy management as well as mobile device management, many organizations have begun to deploy the Cisco Identity Services Engine (ISE) as part of their BYOD strategy. Cisco ISE is a next-generation identity and access control policy platform providing secure wired, wireless and VPN access. While this guide does not provide design guidance for BYOD deployments, ISE has been introduced for basic wireless user authentication as well as sponsor-based guest wireless services. There are other Cisco Validated Designs that provide detailed information regarding the design and deployment considerations of BYOD.

The following table shows the security product and use within this guide.

Cisco security product	Network infrastructure access using TACACS+	Wireless network user access using RADIUS		
Cisco Secure ACS	Yes	No		
Cisco Identity Services Engine	No	Yes		

# Configuring Cisco Secure ACS for Wireless Infrastructure Access

- 1. Create the wireless device type group
- 2. Create the TACACS+ shell profile
- 3. Modify the device admin access policy
- 4. Define Cisco AireOS WLCs as TACACS+ network devices

This guide describes the configuration of Cisco Secure Access Control System (ACS) for the authentication by network administrators to the wireless network infrastructure using TACACS+. Wireless end user client authentication services are performed by Cisco Identity Services Engine (ISE).

Cisco Secure 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 5.5 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.



**PROCESS** 

The following procedures outline the additional configuration of a functional ACS server for wireless infrastructure access. For information about initial setup and installation of Cisco Secure ACS, please see the Device Management Using ACS Technology Design Guide.



**Step 1:** Navigate to the Cisco Secure ACS Administration page (Example: https://acs.cisco.local) and log in using the configured ACS Administrator userid and password (Example: **acsadmin/C1sco123**).

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: AireOS-WLC). In the Description box, provide a meaningful description of this device group.

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

Cisco Secure A EVAL(Days left: 364)	CS acsadmin acs (Primary : LogCollector) Log Out About Help
My Workspace      Metwork Resources	Network Resources > Network Device Groups > Device Type > Create
Network Device Groups     Location     Device Type     Network Devices and AAA Clients     Surver and Identity Stores     Sy Policy Elements	Name: AireOS-WLC     Description: Device Group for AireOS Wireless LAN Controllers X     Parent: All Device Types     Select     S = Required fields
La Access Policies      Monitoring and Reports      System Administration	Submit Cancel

Procedure 2 Create the TACACS+ shell profile

You must create a shell profile for the Cisco AireOS WLCs that contains a custom attribute that assigns the user full administrative rights when the user logs in to the WLC. The Cisco AireOS controllers included in this design are the Cisco Flex 7500, WiSM2, 5500, 2500 and the vWLC Series Wireless Controllers.

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: AireOS WLC Shell), and then in the Description box, enter a description.

Cisco Secure A CISCO EVAL(Days left: 364)	CS acsadmin acs (Primary : LogCollector) Log Out About Help
▶ 🧬 My Workspace	Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles > Create
Network Resources	
Users and Identity Stores	General Common Lasks Custom Attributes
Policy Elements	Name: AireOS WLC Shell
Date and Time Custom Network Conditions Network Access Device Administration Shell Profiles Command Sets Named Permission Objects Mantoring and Reports	Description: AireOS Based WLC Shell
System Administration	Submit Cancel

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

Step 4: In the Requirement list, choose Mandatory. In the Attribute Value list, choose Static.

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

Cisco Secure AC EVAL(Days left: 364)	S		acsadmin	acs (Primary : LogCollector)	About	Help
🕨 😚 My Workspace	olicy Elements > Authorization and Pe	ermissions > Device Admin	istration > Shell Profiles :	Create		
Image:						
Users and Identity Stores	General Common Tasks C	Custom Attributes				_
<ul> <li>Policy Elements</li> </ul>	Common Tasks Attributes	Requirement	Value		_	
Session Conditions Date and Time Custom     Network Conditions     Authorization and Permissions Network Access     Device Administration	Manually Entered					
Shell Profiles	Manually Entered					
Command Sets	Attribute F	Requirement	Value			
Access Policies						
Maritaina and Danata						
monitoring and Reports						
System Administration	Add A Edit V Re Attribute: role 1 Requirement: Mandatory V Attribute: Static V Value: Static V ALL e = Required fields	splace /\Delete	Bulk Edit	~		

Step 6: Click Submit.

Cisco Secure AC CISCO EVAL(Days left: 364)	CS		acsadmin	acs (Primary : LogCollector)	Log Out	About	Help
My Workspace	Policy Elements > Authorization and	d Permissions > Device Ad	ministration > Shell Profiles >	Create			
Horork Resources      Metwork Resources      Musers and Identity Stores	General Common Tasks	Custom Attributes					
Policy Elements	Common Tasks Attributes						
Session Conditions     Date and Time     Custom     Network Conditions     Authorization and Permissions     Network Access     Device Administration     Shell Profiles	Attribute Manually Entered	Requirement	Value				
Command Sets	Attribute	Requirement	Value				
Named Permission Objects     Access Policies	role1	Mandatory	ALL			^	
Monitoring and Reports							
System Administration						~	
	Add A Edit V Attribute: Requirement: Mandatory V Attribute Value: Static V e = Required fields	Replace A Delete	Bulk Edit	Ŷ			

Procedure 3 Modify the device admin access policy

You must exclude the Cisco AireOS WLCs from the existing default authorization rule.

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

cisco Cisco Secure A EVAL(Days left: 364)	CS				acsadmin acs	(Primary : LogCollector)	Log Out Ab	out	
► 💦 My Workspace	Access Poli	ies > Acce	ss Services > Defau	It Device Admin > Authorization					
Network Resources	Standard	Standard Policy Exception Policy							
Users and Identity Stores	Device /	dministra	tion Authorization	n Policy					
Policy Elements									
🔹 💺 Access Policies	Filler.	natus	▼ Watch i		• Olear I - Int			_	
Access Services     Service Selection Rules		Status	Name	Identity Group	NDG:Location	Conditions NDG:Device Type			
<ul> <li>O Default Device Admin Identity</li> </ul>	1 🗆		Network Admin	in All Groups:Network Admins	-ANY-	-ANY-			
Group Mapping Authorization	2	0	Helpdesk	in All Groups:Helpdesk	-ANY-	not in All Device Types	Security Devic	es	
Default Network Access									

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

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

General Name: Network Admin The Custom conditions a	Status: Enabled Status: Enable	
Conditions		
Identity Group:	in V All Groups:Network Admins Select	
NDG:Location:	-ANY-	
✓ NDG:Device Type:	not in V All Device Types:AireOS-WLC Select	
Time And Date:	-ANY-	
Shell Profile: Level15	Select	
OK Cancel	Н	elp

Next, create a Cisco AireOS 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 Cisco AireOS WLC authorization rule. (Example: AireOS 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:AireOS-WLC.

August 2014 Series

General Name: AireOS WLC Ac	Imin Status: Enab	right area of the policy rules scre	en controls which policy
conditions a	no results are available	e nere for use in policy rules.	
Conditions		All Crevers Naturals Admins	Solost
✓ Identity Group:	in 🗸		Select
NDG:Location:	-ANY-		
✓ NDG:Device Type:	in 🗸	All Device Types:AireOS-WLC	Select
Time And Date:	-ANY-		
Results Shell Profile: AireOS W	LC Shell	Select	
OK Cancel			Help

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

Step 9: Click Save Changes.

#### **Procedure 4** Define Cisco AireOS WLCs as TACACS+ network devices

For each Cisco AireOS-based controller and/or HA SSO controller pair in the organization, you must create a network device entry in Cisco Secure ACS.

If you are configuring a Cisco 2500 Series WLC pair that does not support HA SSO, you need to include both of their IP addresses in this step in order 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-5508), and then, in the **Description** box, enter a description (Example: 5508 WLC HA Pair).

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

Step 4: In the IP box, enter the WLCs management interface IP address. (Example: 10.4.175.66)

Step 5: Select TACACS+.

Step 6: In the Shared Secret box, enter the TACACS+ shared secret key. (Example: SecretKey)

Cisco Secure A EVAL(Days left: 363)	CS			ad	csadmin	acs (Primary : LogCollector)	Log Out	About	Help
My Workspace	Network Resources	> Network	k Devices and AAA Clients > Create						
Vetwork Resources     Network Device Groups     Location     Device Type	o Name: Description:	WLC-55	i08 LC HA Pair			]			^
Network Devices and AAA Clients	Location	ce Group	All Locations		Select				
Default Network Device External Proxy Servers	Device Type		All Device Types:AireOS-WLC		Select				
Services     Users and Identity Stores     So Policy Elements     La Access Policies	IP Address Single IP: 10.4.30	IP Addres	ss O IP Subnets O IP Range(s)	Authenti TACAC Shar	cation Op S+ 🔽 ed Secret:	SecretKey Hide	*		
<ul> <li>Monitoring and Reports</li> </ul>				8	Single Con	nect Device			
System Administration				•	Legacy IA	CACS+ Single Connect Suppor	t Ourset		
				DADIUS	TACAUS+	Dratt Compliant Single Connect	Support		
				<ul> <li>RADIU:</li> </ul>	• 🗆				
				Sha	red Secret	<u>5n</u>	ow		
				CoA	port: 170	- Alfana			
				Kev	Encountion	ywnap Kew			
				Mes	sane Auth	enticator Code Key:			
				Key	Input Forr	nat O ASCII  HEXADECIN	IAL		
	o = Required fir	elds							~
	<							>	
	Submit Can	cel							

**Step 7:** Repeat these steps for each of the Cisco AireOS-based Wireless LAN Controllers in your environment. This includes any AireOS-based guest anchor controllers located in the Internet edge. If you have multiple controllers that can be logically grouped, you can select IP ranges and define a number of individual IP addresses.

Cisco Secure A CISCO EVAL(Days left: 363)	CS	acsadmin	acs (Primary : LogCollector)	Log Out About	Help			
Interface       Network Resources > Network Device and AAA Clients > Create         Interview Resources > Network Resources > Network Device and AAA Clients > Create         Interview Resources > Network Resources > Network Device and AAA Clients > Create         Interview Review Review Resources > Network Resources > Network Device and AAA Clients > Create         Interview Review Revie		Select Se	admin acs (Primary : LogCollector) Log Cut Af Select Select Authentication Options • TACACS+ Shared Secret SecretKey Hi Single Connect Device • Legacy TACACS+ Single Connect Supp • TACACS+ Draft Compliant Single Connect • RADIUIS • RADIUS • RADIUS Shared Secret CoA port: 1700 • Enable KeyWrap Key Encryption Keyr Message Authenticator Code Key:					
	Submit Cancel		Shared Secret   CoA port 1700 Enable KeyWrap Key Encryption Key Message Authenticator Code Key Input Format ASCII	Key:	1 1			

#### Tech Tip

Devices that are not explicitly defined using the procedure above will use the Default Network Device setting. The Default Network Device setting was defined during the initial installation of Cisco Secure ACS. For more information, see the Device Management Using ACS Technology Design Guide. The TACACS+ Cisco AireOS shell profile is required when managing AireOS controllers with AAA and must be used for all AireOS-based controller authentication and authorization requests. Cisco IOS-based devices such as routers and switches expect to receive a TACACS+ attribute value (AV) pair priv-IvI = 15 when an administrator logs on. The same concept applies to AireOS devices, but instead of priv-IvI = 15 being returned, a value of role1 = ALL is returned to the AireOS-based WLC. With IOS-XE based wireless LAN controllers, however, this does not apply as Cisco 5760 Series Wireless Controller requires the IOS-based TACACS+ attribute value pair of priv-IvI = 15. As such, IOS-XE based WLCs must not be added using the process described above. By design, they will fall through the logic and use the default shell, which returns the expected IOS AV pair of priv-IvI = 15.



In this design, redundant Cisco ISE servers are used to provide wireless user authentication and replace Cisco Secure ACS for this purpose. Wireless user authentication uses the RADIUS protocol, and the following steps outline the installation process of the redundant ISE servers. The installation of ISE on the VMWare server was previously completed.

Table 8 -	Cisco ISE	enaine IP	addresses	and h	nostnames
10010 0	01000 101	ongino n	uuui 00000	anan	100011011100

Device	IP address	Hostname
Primary Cisco ISE administration and policy service node	10.4.48.41	ise-1.cisco.local
Redundant Cisco ISE administration and policy service node	10.4.48.42	ise-2.cisco.local



Step 1: Boot Cisco ISE, and then, at the initial prompt, enter setup. The installation begins.



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

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

Step 3: Enter Domain Name System (DNS) information.

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

Step 4: Configure the time.

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

#### CO Reader Tip

For time zone abbreviations, see entry for the **clock timezone** command in Appendix A of the *Cisco Identity Services Engine CLI Reference Guide, Release 1.2*, here: http://www.cisco.com/c/en/us/td/docs/security/ise/1-2/cli\_ref\_guide/ise\_cli/ise\_cli\_app\_a.html

**Step 5:** Configure an administrator account.

You must configure an administrator account in order to access the CLI console. This account is not the same as the one used to access the GUI.

```
Enable SSH Service? Y/N [N]: Y
Enter username[admin]: admin
Enter password: [password]
Enter password again: [password]
```

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



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

Do not use 'Ctrl-C' from this point on
Virtual machine detected, configuring VMware tools
Installing applications
Installing ise
Executed with privileges of root
The mode has been set to licensed.
Application bundle (ise) installed successfully
=== Initial Setup for Application: ise ===
Welcome to the ISE initial setup. The purpose of this setup is to
provision the internal ISE database. This setup requires you create
a database administrator password and also create a database user password.

The primary Cisco ISE virtual appliance is now installed.

#### **Procedure 2** Perform initial setup of redundant Cisco ISE server

The procedure for setting up a secondary redundant Cisco ISE server is the same as for the primary, with the only difference being the IP address and host name values configured for the engine.

**Step 1:** Set up the redundant ISE server by following Procedure 1, "Perform initial setup of primary Cisco ISE server" and using the values supplied in Table 8 for the redundant ISE server.

Procedure 3 Configure certificate trust list

The engines use public key infrastructure (PKI) to secure communications between them. Initially in this deployment, you use local certificates, and you must configure a trust relationship between both of the engines. To do this, you need to import the local certificates from the redundant Cisco ISE server into the primary Cisco ISE administration node.

August 2014 Series
Step 1: In your browser, connect to the secondary engine's GUI at http://ise-2.cisco.local. Select No when asked to run the setup assistant wizard.



Step 2: In Administration > System, select Certificates.

Step 3: In the Local Certificates window, select the local certificate by selecting the box next to the name of the secondary engine, **ise-2.cisco.local**, and then click **Export**.

abab					ise-2   admin   Logout	i Feedback		
cisco Identity Services Engine	Home Operations   • Policy   •	Administration   +					Setup A	Assistant + 🖸
🔆 System 🖉 Identity Management 🖀 N	etwork Resources 🛛 🛃 Web Portal Management	Feed Service						
Deployment Licensing Certificates Logg	ng Maintenance Backup & Restore Admin	Access Settings						
Certificate Operations	Local Certificates							
O Local Certificates							Selected 1   Total 1	😌 🗟 🗸
Certificate Signing Requests	/ Edit - Add - Delete					Show All		- 8
O Certificate Store	Friendly Name	<ul> <li>Protocol</li> </ul>	Issued To	Issued By	Valid From	Expiration Date	Expiration Status	
SCEP RA Profiles	Default self-signed server certificate	HTTPS,EAP	ise-2.cisco.local	ise-2.cisco.local	Thu, 20 Feb 2014	Fri, 20 Feb 2015		
OCSP Services								
\varTheta Help							Notific	cations (0)

Step 4: Choose Export Certificate Only, and then click Export.

			ise-2 (		Feedback		
cisco Identity Services Engine	🙆 Home Of	perations   • Policy   • Administration   •				Setup A	ssistant + 📀
System         Model         Identity Management         Network           Deployment         Licensing         Certificates         Logging	Nork Resources (#	Web Portel Messeement (102) Feed Service xport Certificate 'Default self-signed server certificate'	×				
Certificate Operations  Cocal Certificates  Certificate Stanka Revests	Local Certifica	Export Certificate Only     Export Certificate and Private Key			Show All	Selected 1   Total 1	***
Certificate Store SCEP RA Profiles	Friendly Nar	*Private Key Password *Confirm Password		ald From hu, 20 Feb 2014	Expiration Date Fn, 20 Feb 2015	Expiration Status	
CCSP Services		Warning: Eporting a private key is not a secure operation. It could lead to possible exposure of the functional secure operation. It could lead to possible exposure of the function of the f	Cancel				
🕘 Help						Notific	ations (0)

**Step 5:** When the browser prompts you to save the file to a location on the local machine, choose where to store the file and make a note of it. You will be importing this file into the primary engine.

alada					ise-2   admin   Logout	Feedback		
cisco Identity Services Engine	Home Operations + Policy +	Administration   +					Setup Ass	istant + 🖸
🔆 System 👰 Identity Management 🖀	Network Resources 🛛 🛃 Web Portal Management	Feed Service						
Deployment Licensing Certificates Log	ging Maintenance Backup & Restore Admin /	Access Settings						
Certificate Operations	Local Certificates							
O Local Certificates							Selected 1   Total 1	÷ 🖗 📲
Certificate Signing Requests	🖌 Edit 🚽 Add 👻 🔂 Export 🗙 Delete					Show All		- 8
Certificate Store	Friendly Name	<ul> <li>Protocol</li> </ul>	Issued To	Issued By	Valid From	Expiration Date	Expiration Status	
SCEP RA Profiles	Default self-signed server certificate	HTTPS,EAP	ise-2.cisco.local	ise-2.cisco.local	Thu, 20 Feb 2014	Fri, 20 Feb 2015		
OCSP Services								
Do you want to open o	or save Defaultselfsignedservercerti.pem f	from 10.4.48.42?			Open Save	e 🔻 Cance	el × Notificat	ions (0)

Step 6: In a browser, access the primary engine's GUI at http://ise-1.cisco.local.

#### Step 7: In Administration > System, select Certificates.

Step 8: In the Certificate Operations pane on the left, click Certificate Store, and then click Import.

**Step 9:** Next to the Certificate File box, click **Browse**, and then locate the certificate exported from the secondary engine. It has an extension of .pem.

Choose File to Upload						×
Computer	System (C:) 🕨 ISE Certificates	-	<b>4</b>	earch ISE	Certificates	٩
Organize  • New folder					•	0
<ul> <li>★ Favorites</li> <li>▲ Desktop</li> <li>↓ Downloads</li> <li>⊗ Recent Places</li> </ul>	] ISE2-Defaultselfsignedservercerti.pem					
Computer						
File name:	ISE2-Defaultselfsignedservercerti.pem	•	All File	es (*.*) en	Cancel	•

Step 10: You may enter a friendly name for the ISE2 server then click Submit.

abab		ise-1   admin   Logout   Feedback 🔎	
cisco Identity Services Engine	Home Operations        Policy        Administration		Setup Assistant 🛪 🕗
🔆 System 👰 Identity Management 📷	Network Resources 🛛 🛃 Web Portal Management 🔤 Feed Service		
Deployment Licensing Certificates Log	ging Maintenance Backup & Restore Admin Access Settings		
Certificate Operations	Certificate Store > Import Import a new Certificate into the Certificate Store		
Certificate Signing Requests	* Certificate File C:VSE CertificatesVSE2-Defaultselfsignedse( Browse		
Certificate Store	Friendly Name	0	
SCEP RA Profiles			
OCSP Services	This certificate will be used to verify ISE server certificates in multi-node deployments, for validating LDAF In addition, it can be used to verify the authenticity of client certificates presented to ISE (for EAP-TLS an	<sup>5</sup> secure authentication connections and for secure syslog services, d administrative authentication) by checking the box below:	
	Trust for client authentication or Secure Syslog services		
	Enable Validation of Certificate Extensions (accept only valid certificate)		
	Description		
	2		
	<		>
P Halo			Notifications (0)

**Procedure 4** Configure Cisco ISE deployment nodes

**Step 1:** You can configure the personas of Cisco ISE–administration, monitoring, and policy service–to run all on a single engine or to be distributed amongst several engines. This installation will run all services on the primary and redundant secondary ISE servers Connect to **http://ise-1.cisco.local**.

**Step 2:** From the **Administration** menu, choose **System**, and then choose **Deployment**. A message appears notifying you that the node is currently standalone. Click **OK**.



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

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

cisco Identity Services Engine				se <mark>-1 admin Logout Feedback</mark>
💧 Home Operations 🔻 Policy 🔻	Administration 🔻			👓 Task Navigator 🔻 😢
🔆 System 🛛 🖉 Identity Management	Network Resources	🛃 Guest Management		
Deployment Licensing Certificates	Logging Maintenance /	Admin Access Settings		
Danloumont	Deployment Node	es		
	262			Selected 0   Total 1 😵 🎡 🖕
Nor i i i i i i i i i i i i i i i i i i i	Create Node Group	er 🚯 Export 🚯 Import	> Show All	- 6
85 - Frit	- Hostname	<ul> <li>Node Type</li> </ul>	Personas	Role(s)
	ise-1	ISE	Administration, Monitoring, Policy	Service STANDALONE

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

cisco Identity Services Engine		ise-1 i admin i Logout i Feedback 🔎	
	Home Operations + Policy + Administration +		Setup Assistant + 🕐
🔆 System 🎽 Identity Management	🖀 Network Resources 🛛 🛃 Web Portal Management 👦 Feed Service		
Deployment Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings		
Deployment	Create Node Group     * Node Group Exercise     * Node Group Marker     * List Group Exercise     * Mulcast Address     * 228.00.11.13     *     * Mulcast Address     * 228.00.11.13     *     *     * Exercise Table Ta		
A Halo			Notifications (0)

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

**Step 6:** In the Deployment pane on the left, expand **Deployment**. A list of the current deployment nodes appears.

Step 7: Click ise-1. This enables you to configure this deployment node.

cisco Identity Services Engine	🙊 Home Operations i y Policy i y Administration i y	Freedback D Setup Assistant + 📀
e Help		Nobfications (0)

**Step 8:** On the General Settings tab, in the Personas section, next to the Administration Role, click **Make Primary**.

Step 9: In the Include Node in Node Group list, choose ISE\_Group.



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

On the Profiling Configuration tab, select RADIUS by placing a check mark as shown and then click Save.

ababa		ise-1   admin   Logout   Feedback
cisco Identity Services Engine	Home Operations + Policy + Administration +	Setup Assistant 🗸 😶
System         Identity Management           Deployment         Licensing         Certificates	Network Resources     Age Web Portal Management     Logging Maintenance Backup & Restore Admin Access Settings	
Deployment	Deployment Nodes List > ise-1.	â
	General Settings Profiling Configuration	
• 🐥 ISE_Group	□ ► NETFLOW	^
	bhcp	
	+ HITP	
	RADIUS Description CDF, LLF madus probe collects Radius CDF, LLF mas SC Sensor.	
	Network Scan (NMAP)	
	DNS	
	SNMPQUERY	
A Mala	SNMPTRAP	Y

Step 10: Select HTTP, use the default parameters, and then click Save.

abab		ise-1   admin   Logout   Feedback
cisco Identity Services Engine	Home Operations      Policy      Administration	Setup Assistant + 😶
System Version Certificates	Hetwork Resources     [e], Web Portal Management     [co] Feed Service     Logging Maintenance Backup & Restore Admin Access Settings	
Deployment	Deployment Nodes List > ise-1 E-dit Node	^
合• 用•	Several Settings Profiling Configuration	
<ul> <li>Colebonation</li> <li>Reg (Grap)</li> <li>set1</li> </ul>		^
	Process HTTP packets.      PRODIS     Description     Tos     Description     Tos     Description     Tos     Description     Provide produce produce packets     COP, LLDP from IOS Sensor.      P Intervenk Scan (MMAP)     PDIS	

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

cisco ruentity services Engine	🟠 Home Operations 💌 Policy 💌 Administration 🖃
🔆 System 🛛 👰 Identity Management	🞬 Network Resources 🛛 🛃 Web Portal Management 🛛 🗔 Feed Service
Deployment Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings
	General Settings Profiling Configuration Hostname ise-1 FQDN ise-1.cisco.local IP Address 10.4.48.41

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

ahaha	ise-1   admin   Lopout   F	edback P	
cisco Identity Services Engine	Administration   + Policy   + Administration   +		Setup Assistant 🕶 🕙
🔆 System 🦉 Identity Management	🖀 Network Resources 🛛 🛃 Web Portal Management 🛛 🙀 Feed Service		
Deployment Licensing Certificates	Logging Maintenance Backup & Restore Admin Access Settings		
Deployment	Deployment Nodes		
(a + H- +	8-		Selected 0   Total 1  🚭 🖕
* 🔆 Deployment	/ Edit Register - O Syncup Deregister	Show All	• 8
* 🐣 ISE_Group	Hose Register an ISE Node the Personas Role(s) Services Node Status		
ise-1	ise-1 ise Administration, Monitoring, Policy Service PRI(A), PRI(M) All		

**Step 13:** Enter the IP address or host name of the redundant Cisco ISE engine from Table 8 (in this example, ise-2.cisco.local) and the credentials for the admin account, and then click **Next**.

راندان، cisco Identity Services Engine	🟠 Home Operat	ise-1   admin   Logout   Feedback	Setup Assistant • 2
🔆 System 🖉 Identity Management 🖀 No	etwork Resources 🛛 🛃 Web F	Portal Management 🕞 Feed Service	
Deployment Licensing Certificates Loggi	ng Maintenance Backup	& Restore Admin Access Settings	
Deployment	Deployment Nodes List > Specify	/ Hostname	
@• E• @•	Register ISE Node - Step	1: Specify Node Host FQDN (hostname.domain-name) and Cr	edentials
🔻 🐈 Deployment			
ISE_Group	* Host FQDN	ise-2.cisco.local	
ise-1	* User Name	admin	
	* Password	•••••	
	Next Cancel		
O Help			Notifications (0)

Step 14: Select only Administration and Policy Service. In the Administration section under Role list ensure Secondary is displayed. In the Policy Service section, in the Node Group list, Choose ISE\_Group.

diala	ise-1   admin   Logout   Feedback	
cisco Identity Services Engine	Administration   ▼	Setup Assistant +
🍹 System 🛛 👰 Identity Management 🛛 📑	Network Resources 🛛 🛃 Web Portal Management 🛛 🙀 Feed Service	
eployment Licensing Certificates Li	ogging Maintenance Backup & Restore Admin Access Settings	
eployment ₽ • E • @	Configuret Node     Configure Node     Configure Node     Configure Configure Node	
Peployment     BISE_Group     ise-1	Hostmane Ise-2 FQDN ise-2.cisco.local IP Address 10.4.48.42 Nod Type Learthy Services Engine (ISE)	^
	Personas  Administration Role SECONDARY	
	Monitoring Role SECONDARY Other Monitoring Node	
	Enable Session Services     Tocude Node in Node Group     Ise_Group     Tocude Node in Node Group     Tocude     Tocude Profiling Service     Ise_Group     Tocude	
	6	
	Submit Cancel	

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

cisco Identity Services Engine     System      Deployment Licensing Certificates Loopi	Home twork Resources	Node was regi will be sync'er application se node. This pro minutes to cor	istered successfully. Data d to the node, and then the rver will be restarted on the ocessing may take several mplete.	Logout   Feedback	۵)	Setup Assista	nt + 🕜
Deployment           Q= v         E v         Qave           *         M: Deployment         Y         N: SE: Group           ■         ISE: Group         B: se: 1         ISE: 1	Deployment N	Syncup Node Type ISE	Deregator Personas Administration, Monitoring, Policy Service	Sho Role(s) PRI(A), PRI(M)	Services All	ected 0   Total 2 😵 🕴	8
	11 86-2		Administration, Policy Service		All		
	<				Server Response Vode was registe	red successfully.	

**Step 16:** Verify that the sync of the resilient ISE node to the primary ISE node is completed. To refresh the status of the node group, select the green refresh arrows and verify that both nodes are operational.

cisco Identity Services Engine		A Home Oners	tione - Policy	a Administration I a	se-1   admin   Logout	Feedback	P Satur Assistant = P
System A Identity Management Deployment Licensing Certificates	Eoggin	twork Resources 🛃 Web	Portal Management	Feed Service in Access Settings			Jetup Assistant + •
Deployment	ŵ.	Deployment Nodes	🤡 Syncup 🛛 💆 [	Deregister		Show	Selected 0   Total 2
<ul> <li>ISE_Group</li> <li>ise-2</li> </ul>		Hostname	<ul> <li>Node Type ISE</li> </ul>	Personas Administration, Monitoring, Policy Service	Role(s) PRI(A), PRI(M)	Services	Node Status
ise-1		ise-2	ISE	Administration, Policy Service	SECONDARY(A)	All	

Procedure 5 Install the Cisco ISE license

Cisco ISE comes with a 90-day demo license for both the Base and Advanced packages. To go beyond 90 days, you need to obtain a license from Cisco.



Step 1: Access the Cisco ISE GUI in your browser entering the IP address or hostname for the Cisco ISE server that you just defined. (Example: https://ise-1.cisco.local or https://10.4.48.41)

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

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

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

Step 4: Under Licensed Services, click Add Service.



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

Image: System     M Identify Management     Textwork Resources     Web Portal Management     Textwork Resources     Textwork Res	tant v 🕗
License Operations Current Licenses Curr	
* License File Browse_	
Import	

Step 6: If you have multiple licenses to install such as an Advanced license, repeat the process for each license.

August 2014 Series

#### Procedure 6 Configure network devices in Cisco ISE

Configure Cisco ISE to accept authentication requests from network devices. RADIUS requires a shared secret key in order to enable encrypted communications. Each network device that uses Cisco ISE for authentication needs to have this key. By default, ISE will use the most specific device authentication credentials defined. As a general best practice, defining both a catch all Default Device setting as well as specific groups for the various wireless LAN controllers is recommended. This allows for the selection of specific policy selection that are then mapped to guest wireless as well as campus wireless users.

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

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



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

Step 4: In the Shared Secret box, enter the RADIUS shared secret, and then click Save. (Example: SecretKey)

alah	ise-1   admin   Logout   Feedback							
CISCO Identity Services Engine	Home Operations        Policy        Administration        Setup Assistant							
🔆 System 👹 Identity Management 🕢 🙀 Web Portal Management 🕞 Feed Service								
Network Devices Network Device Groups Exter	nal RADIUS Servers RADIUS Server Sequences SGA AAA Servers NAC Managers MDM							
Network Devices	Default Network Device							
<b>T</b>	The default device definition can optionally be used in cases where no specific device definition is found that matches a device IP address							
	Default Network Device Status Enable -							
Network Devices	Protocol RADIUS							
Default Device	* Shared Secret Show							
	: Enable KeyWrap 🔲 🕧							
	* Key Encryption Key Show							
	* Message Authenticator Code Key Show							
	Key Input Format 💿 ASCII 🔿							
	HEXADECIMAL							
	Save							
🕑 Help	Notifications (0)							

Next, create a Device group that contains the Anchor Guest wireless LAN controllers within the DMZ Internet edge. This will be used later when we define a policy that will be applied to authentication requests from guest users that will use the Sponsor Portal Identity Store, which, starting with Cisco ISE 1.2, is separate from the Internal identity store.

Step 5: Within Cisco ISE, navigate to Administration > Network Resources > Network Device Grou	ups.
--	------

altala cisco Identity Services Engine		Administration   🔻	
System Management     Metwork Device Groups      Hetwork Device Groups	Vetwork Resources  Vetwork Resources  RDIUS Server Sequer  RDIUS Server Sequer  RETWORK Device Groups  Let 4-Add Coportial Management  All Device Types  All Locations  Location	System     Deployment     Licensing     Certificates     Logring     Maritenance     Backup & Reistore     Admin Access     Settings     Network Resources     Network Resources     Network Revice Groups     External RADIUS Servers     RADIUS Servers     SGA AAA Servers     NAC Managers     NAC Managers     NAC Managers     NAC Managers     Not	<ul> <li>Identity Management Identities Groups External Identity Sources Identity Sources Settings</li> <li>Web Portal Management Sponsor Group Poky Sponsor Groups Settings</li> </ul>

**Step 6:** Expand **Groups** and **All Device Types**, and then add a new Device Type called **WLC-Guest** by selecting **+Add** as shown. This creates a new Device Type called WLC-Guest that will be used later in the configuration to trigger policy specific to wireless guest users.

cisco Identity Services Engine	Home Operations ▼ Policy ▼ Administration ▼
🔆 System 🥂 Identity Management 📰 Network Devices Network Device Groups	ietwork Resources 🛛 Web Portal Management 🕞 Feed Service External RADIUS Servers RADIUS Server Sequences SGA AAA Servers NAC Managers MDI
Network Device Groups          •       • <td>Network Device Groups &gt; All Device Types List &gt; New Network Device Group Network Device Groups * Name WLC-Guest Description Guest Wireless LAN Controllers * Type Device Type Submit Cancel</td>	Network Device Groups > All Device Types List > New Network Device Group Network Device Groups * Name WLC-Guest Description Guest Wireless LAN Controllers * Type Device Type Submit Cancel

Step 7: Navigate to Administration > Network Resources > Network Devices, and then select +Add. A new network device is added.

**Step 8:** On the Network Devices template that appears, provide a **Name** and **Description** for this set of wireless LAN controllers (WLCs).

**Step 9:** In the **IP Address** box, provide a network range that is inclusive of the WLC(s) within the DMZ. In this deployment, specify any WLC that resides in the Internet edge DMZ, specifically in the **192.168.19.0/24** network. You can be more or less specific depending on the number of WLC(s) within your Internet edge.

Step 10: Under Network Device Group > Device Type, select WLC-Guest, which was defined previously.

**Step 11:** Under **Authentication Settings**, disable the select **Enable KeyWrap**, and then, in the RADIUS **Shared Secret** box, enter the shared secret key (Example : SecretKey).

abab		ise-1   admin   Logsut   Feedback	٩
cisco Identity Services Engine	Home Operations      Policy      Administration      T		Setup Assistant 🛪 🕙
🔆 System 🛛 👰 Identity Management 🛛 🕋 Network I	Resources 🔣 Web Portal Management 👦 Feed Service		
Network Devices Network Device Groups External	RADIUS Servers RADIUS Server Sequences SGA AAA Servers NAC Managers MDM		
Interact Device Group         Letternd           Network Devices            ····································	BADBS Some         BADBS Some Sources         SGA AAA Some         NaC Manages         MCM           At Damaid         * Same         Generation         SGA AAA Some         NaC Manages         MCM           * Same         Generation         * Same         Generation         SGA AAA Some         NaC Manages         MCM           * Same         Generation         Generation         Generation         SGA AAA         Some         Generation         SGA AAA         Some         Generation         SGA AAA         Some         Generation         SGA AAAA         Some         Generation         SGA AAAA         Some         Generation         SGA AAAA         SGA AAAA         SGA AAAA         SGA AAAA         SGA AAAA         SGA AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA		ŵ-
	* Shared Secret Show		
	Enable KeyWrap		
	* Key Encryption Key Show		
	Key Innut Format   ASCTI HEYADECTMAI		
	Ney input rolline Constant Constants		
	SNMP Settings		

**Procedure 7** Configure Cisco ISE to use Active Directory

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

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

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

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

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

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

alah		ise	⊦1   admin   Logout   Feedback 📿 🔎	
CISCO Identity Services Engine	☆ Home Operations ▼ Policy	Administration	•	Setup Assistant 👻 🕗
🔆 System 🏾 🥂 Identity Management 🛛 🕋 Netwo	ork Resources 🛛 🛃 Web Portal Management	Feed Service		
Identities Groups External Identity Sources	Identity Source Sequences Settings			
External Identity Sources	Active Directory > AD Connection Advanced Settings * Domain Name	Groups Att	ributes	*
Active Directory	* Identity Store Name	AD1		
LDAP 3	One or more nodes may be selected for Join	or Leave operations. If a	node is joined then a leave operation is required before	e a rejoin.
RADIUS Token ()	Q= Join Q= Leave Q= Test Connection	😔 Refresh		
RSA SecurID ()	ISE Node	ISE Node Role	Status	
	ise-1.cisco.local	PRIMARY	Connected to: ad.cisco.local	
	ise-2.cisco.local	SECONDARY	Connected to: ad.cisco.local	=
	Save Configuration Delete Configuration	m		. ·
0		_		
<b>С</b> неір				wouncations (U)

**Step 6:** Select the nodes and then click **Join**. Enter the credentials for the domain administrator account (Example: administrator / c1sco123), and then click **OK**.

		ise	e-1   admin   Logout   Feedback 📿 🔎	
CISCO Identity Services Engine	👔 Home Operations 🔻 Po	licy   • Administration	Y	Setup Assistant 👻 🕗
💑 System 🏼 👰 Identity Management 🛛 🔤 Ne	etwork Resources 🛛 🙀 Web Portal Managem	ent 👩 Feed Service		
Identities Groups External Identity Sources	Identity Source Sequences Settings			
External Identity Sources	Active Directory > AD			
⟨ ] =	Connection Advanced Setting	is Groups Att		
Certificate Authentication Profile	* Domain N	ame cisco.local		
2 Active Directory	* Identity Store N	ame AD1		
EDAP 📀	One or more nodes may be selected for Select one node for Test Connection.	Join or Leave operations. If a	a node is joined then a leave operation is required	before a rejoin.
RADIUS Token 💿	Q= Join Q= Leave Q= Test Connectio	n 💓 Refresh		
RSA SecurID 📀		ISE Nodo Polo	Status	
		PRIMARY	Connected to: ad sizes local	
	ise-2.cisco.local	SECONDARY	Connected to: ad.cisco.local	
			_	
		oin Domain	×	
	•	User Name: Administrator		
		Password:	I	
		ок	Cancel	
	-			
	Save Configuration Delete Configura	tion		
🕑 Help				Notifications (0)

When the Cisco ISE nodes successfully join the domain, the following message displays.

		ise-1   admin   L	Logout   Feedback	
cisco Identity Services Engine	Home Operations      Police	y   🔻 Administration   👻		Setup Assistant 👻 🕗
💑 System 🏾 🌉 Identity Management 🛛 📷 f	vetwork Resources 🛛 🙀 Web Portal Management	t 🕞 Feed Service		
Identities Groups External Identity Sources	Join Operation Status		23	
External Identity Sources	The list below shows the status of the requested	operation for each node.		
	Status: Successful. Please allow two minutes for	the status to be reflected, then press Refre	esh.	
Castificate Authentication Drofin	ISE Node	Status		<u>^</u>
Certificate Authentication Prone	ise-1.cisco.local	Completed.		
	ise-2.cisco.local	Completed.	ration is required before a re	ioin.
PADING Telep				
I I I I I I I I I I I I I I I I I I I				
			xal	
			scal	
			Close	
	Cours Configuration Delate Configuration			
🕑 Help				Notifications (0)

Step 7: Click Close.

#### Procedure 8 Configure AD groups for Cisco ISE authentication

In order to provide Cisco ISE with a group of users to use the sponsor portal, select the AD group or groups that contain the users that the Sponsor Portal are provided. Choose all the users within the cisco.local domain as this set of users will also be used by ISE to authenticate non-guest users to the wireless network. Select a group that is more specific for the sponsor portal such as an AD group that contains all employees who fulfill the role of lobby ambassador within your organization.

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

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

Step 3: Click the Groups tab, click Add, and then click Select Groups from Directory.

**Step 4:** Within the list of groups, search for all of the groups you wish to add. The domain box is already filled in and does not need to be changed. The default filter is a wildcard to list all groups. If you want to get a list of all groups within your domain, click **Retrieve Groups**.

**Step 5:** Select the groups you want to use for authentication, and then click **OK**. For example, if you want to select all users in the domain, select the group <domain>/Users/Domain Users.

D Calast Dis	estern Creune	ise-1   admin   Logout	Feedback	Q	
o Identity Services E Seect Dre This dialog ystem A Identity Mana Use * for w	sctory Groups is used to select groups from the Direc wildcard search (i.e. admin*). Search filte	tory. Click Retrieve Groups. to read directory. r applies to group name and not the fully qualified path.		×	etup A
ties Groups Extern Domain:	cisco.local	Retrieve Groups Number of Groups Retrieved: 77 (Limit is 100)			
In identity sources	e		▲ Group T	Type	
C cisco	p.local/Users/Denied RODC Password R	Replication Group	LOCAL	A	
tilicate Authentication Profix	o.local/Users/DnsAdmins		LOCAL		
ive Directory cisco	o.local/Users/DnsUpdateProxy		GLOBA	L.	
P cisco	o.local/Users/Domain Admins		GLOBA	L.	
DIUS Token cisco	p.local/Users/Domain Computers		GLOBA	4	
SecurID cisco	p.local/Users/Domain Controllers		GLOBA	L	
Cisco	p.local/Users/Domain Guests		GLOBA	L.	
✓ cisco	o.local/Users/Domain Users		GLOBA	iL.	
Cisco	o.local/Users/Enterprise Admins		UNIVER	RSA	
Cisco	p.local/Users/Enterprise Read-only Dom-	ain Controllers	UNIVER	RSA	
C cisco	o.local/Users/Finance		GLOBA	L _	
Cisco	o.local/Users/Group Policy Creator Own	ers	GLOBA	L	
Cisco	p.local/Users/HR		GLOBA	L.	
Cisco	o.local/Users/IT		GLOBA	iL.	
< eiser	o local/Lisers/Lobby ∆rimins	m	GLOBA	•	
			ОКСа	ancel	
Help					Notif

Step 6: Click OK, and then click Save Configuration.

alah	ise-1   admin   Logout   Feedback	
CISCO Identity Services Engine	Home Operations      Policy      Administration	Setup Assistant 🕶 🕗
💑 System 🏼 👰 Identity Management 🛛 🖀 N	etwork Resources 🛛 👸 Web Portal Management 🛛 👼 Feed Service	
Identities Groups External Identity Sources	Identity Source Sequences Settings	
External Identity Sources	Adhe Divedory > AD Connection Advanced Settings Groups Attributes	
	Save Configuration Delete Configuration	
🛃 Help		Notifications (0)



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 services block in the data center 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 points.

This section covers the Cisco AireOS Wireless LAN Controllers operating in Cisco Unified Wireless Network (CUWN) mode. In this mode, both the Mobility Controller (MC) and Mobility Agent (MA) services are not separated and both remain on the WLC. Because the AireOS controllers for on-site local-mode deployment (Cisco WiSM2, 5508, 2504 Wireless Controllers) differ from that of the Cisco IOS-XE 5760 controller, the 5760 Series WLC configuration details are covered in the "Configuring On-Site 5760 (IOS-XE) Wireless Controller" section of this guide.

If you are deploying remote access points using Cisco FlexConnect, proceed to the "Configuring Remote-Site Wireless with Cisco FlexConnect" process.

This guide supports the Cisco 5760, WiSM2, 5500 and 2500 Series WLCs for use in an on-site local-mode design. When installing WiSM2 and 5500 Series WLCs, a high availability feature known as high availability Stateful Switchover (HA SSO) is available on these platforms. 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 HA SSO mode, configuration synchronization and keep-alive monitoring occurs over a dedicated redundancy port (labeled as RP) using either a dedicated straight through Ethernet cable, or a layer 2 connection that meets the HA SSO Redundancy Port requirements.

The Cisco 2500 Series WLC does not support the HA SSO feature and instead must be paired with the resilient WLC by using a mobility group in order to achieve resiliency. Unlike HA SSO paired Wireless LAN Controllers, each Cisco 2500 Series WLC has a unique IP address on the management interface and operates in a redundancy model referred to as N+1.

Parameter	CVD values primary controller	CVD values resilient controller	Site-specific values
Controller parameter	ers		
Switch interface number	1/0/3, 2/0/3	1/0/4, 2/0/4	
Management VLAN number	275	275	
Service Port VLAN number (WiSM2 Only)	1172	1172	
Redundancy Port VLAN number (WiSM2 only)	1173	1173	
Time zone	PST -8 0	PST -8 0	
IP address	10.4.175.64/24	10.4.175.65/24 <sup>3</sup>	
Default gateway	10.4.175.1	10.4.175.1	
Redundant manage- ment IP address (HA SSO) <sup>1</sup>	10.4.175.1641	10.4.175.1651	
Redundancy port connectivity (HA SSO) <sup>1</sup>	Dedicated Ethernet cable <sup>1</sup> Layer 2 network <sup>2</sup>	Dedicated Ethernet cable <sup>1</sup> Layer 2 network <sup>2</sup>	
Hostname	WLC-1	WLC-2 <sup>3</sup>	
Local administrator username and password	admin/C1sco123	admin/C1sco123	
Mobility group name	CAMPUS	CAMPUS	
Primary Cisco ISE RADIUS server IP address	10.4.48.41	10.4.48.41	
Secondary Cisco ISE RADIUS server IP address	10.4.48.42	10.4.48.42	
Network RADIUS shared key	SecretKey	SecretKey	
Management network	10.4.48.0/24	10.4.48.0/24	
ACS TACACS server IP address	10.4.48.15	10.4.48.15	
TACACS shared key	SecretKey	SecretKey	

Table 9 (continued) - Cisco on-site wireless controller parameters checklist

	CVD values	CVD values	
Parameter	primary controller	resilient controller	Site-specific values
Wireless data netw	ork parameters		
SSID	WLAN-Data	WLAN-Data	
VLAN number	116	116	
Default gateway	10.4.16.1	10.4.16.1	
WLC controller interface IP address	10.4.16.5/22	10.4.16.6/22	
Wireless voice netw	vork parameters		
SSID	WLAN-Voice	WLAN-Voice	
VLAN number	120	120	
Default gateway	10.4.20.1	10.4.20.1	
WLC controller interface IP address	10.4.20.5/22	10.4.20.6/22	

Notes:

- 1. HA SSO is only supported on the Cisco 5500, WiSM2, 7500 Series WLC.
- 2. HA SSO over Layer 2 network support is supported on Cisco 5500, WiSM2, and 7500 Series WLC provided the redundancy port round-trip time is less than 80 milliseconds
- 3. The resilient Cisco 2500 Series WLC will require an IP address, as HA SSO is not supported on this platform. Starting in Cisco AireOS release 7.6, N+1 redundancy using a high availability SKU is available on 2500 Series WLC.

# Procedure 1 Configure services block for the Cisco 2500, WiSM2 or 5500 Series WLC

The shared services block is comprised of two Cisco 6500 Series Switches configured as a Virtual Switching System (VSS) supporting wireless LAN controller services for campus-based wireless access. Use this procedure to configure connectivity for Cisco 2500, 5500 or WiSM2 series WLC within the VSS services block.

# Tech Tip

i

The wireless LAN controllers that provide Cisco FlexConnect services to remote sites (such as Cisco 7500 and vWLC Series Wireless Controllers) are not connected to the services block and remain within the data center access layer. The configuration of FlexConnect controllers for remote sites is covered in the "Configuring Remote-Site Wireless with Cisco FlexConnect" process later in this guide.

August 2014 Series

**Step 1:** Within the Cisco Catalyst 6500 VSS services block, create the wireless VLANs for connectivity to the data, voice, and wireless LAN controller VLANs. The management VLAN can contain other Cisco appliances and does not have to be dedicated to the WLCs.

```
vlan 116
  name WLAN_Data
exit
vlan 120
  name WLAN_Voice
exit
vlan 275
  name WLAN_Mgmt
exit
```

**Step 2:** Configure a switch 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
ip pim sparse-mode
no shutdown
T
interface Vlan120
description Wireless Voice Network
ip address 10.4.20.1 255.255.252.0
ip pim sparse-mode
no shutdown
T
interface Vlan275
description Wireless Management Network
ip address 10.4.175.1 255.255.255.0
ip pim sparse-mode
no shutdown
```

**Step 3:** Configure an 802.1Q trunk to be used for the connection to the appliance based wireless LAN controllers (2500 or 5500). This permits Layer 3 services for each of the networks defined on the WLC. The VLANs allowed on the trunk are limited to only the VLANs that are active on the WLC. The trunk is built using multiple Ethernet interfaces grouped into a logical PortChannel configuration for resiliency.

# i Tech Tip

If you are deploying a Cisco Catalyst 3750 Series LAN switch stack as a services block, you need to add the **switchport trunk encapsulation dot1q** command to the Port-channel configuration. Additionally, if you are using the 6500 with 1-Gigabit Ethernet ports, apply the EgressQoSOneGig macro instead of the EgressQoS macro. These macros are defined in the Campus Wired LAN Technology Design Guide.

```
interface GigabitEthernet [port 1]
description To WLC Port 1
interface GigabitEthernet [port 2]
description To WLC Port 2
Т
interface range GigabitEthernet [port 1], GigabitEthernet [port 2]
 switchport
 macro apply EgressQoS
 ! for 6500 with 1Gbps Ethernet, use:
  ! macro apply EgressQoSOneGig
 channel-group [number] mode on
 logging event link-status
 logging event trunk-status
 logging event bundle-status
L
interface Port-channel [number]
description To WLC
switchport trunk allowed vlan 116,120,275
switchport mode trunk
logging event link-status
no shutdown
```

**Step 4:** Repeat Step 3 for each of the appliance-based wireless LAN controllers (Cisco 2500 or 5500 Series Wireless Controllers) in your environment.

# Procedure 2 Connecting the redundancy port for Cisco 5500 Series WLC

If you are using a Cisco 5500 Series WLC pair and wish to enable the HA SSO feature, continue with this procedure. When using high availability, 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:** If you are connecting Cisco 5500 Series WLC RP ports directly using an ordinary Ethernet cable, connect it as shown in the following.

Primary AIR-CT5508-50-K9



Resilient AIR-CT5508-HA-K9

**Step 2:** If you are connecting Cisco 5500 Series WLC RP ports over an extended L2 network, the following requirements must be met:

- Round-trip time (RTT) latency on the redundancy link: 80 ms or less for the default keep-alive timeout or 80 percent of the configured keep-alive timeout
- Preferred maximum transmission unit (MTU) on the redundancy link of 1500 or above
- Bandwidth on the redundancy link: 60 Mbps or more

#### Coole States Vicies Control Coole States Vic

Primary AIR-CT5508-50-K9

Resilient AIR-CT5508-HA-K9

#### Procedure 3 Configure the switch for Cisco WiSM2 Series WLC

When using two Cisco WiSM2 Wireless LAN Controller service modules with HA SSO, the WiSM2 must conform to one of the following deployment topologies:

- Two Cisco WiSM2 WLCs on the same Cisco Catalyst 6500 Series chassis
- Two Cisco WiSM2 WLCs on different Cisco Catalyst 6500 Series chassis with the redundancy VLAN extended over the Layer 2 network and conforming to the same redundancy port (RP) requirements for bandwidth, latency, and MTU
- Two WiSM2 WLCs on different Cisco Catalyst 6500 Series chassis when configured using VSS

Because Cisco WiSM2 does not have a physical redundancy port, the VLAN used with the redundancy port must first be defined on the Cisco Catalyst 6500 Series VSS switch. If you are using a 6500 VSS and WiSM2, create the VLAN used for the redundancy port by using the following steps.

**Step 1:** Access the CLI of the Cisco Catalyst 6500 Series VSS Switch and create the redundancy VLAN for the Cisco WiSM2 Wireless LAN Controller.

vlan 1173 name WiSM2-RedundancyPort exit

August 2014 Series

Step 2: Create the Cisco WiSM2 service port and SVI for the service port VLAN.

```
vlan 1172
name WiSM2-Service-Port
exit
!
interface Vlan1172
ip address 172.16.10.1 255.255.255.0
exit
```

#### Tech Tip

Unlike the service port, the redundancy port for Cisco WiSM2 on the Cisco 6500 VSS chassis does not require a switch virtual interface (SVI). This is because the IP address used for the redundancy port is automatically assigned a unique IP address. The format of the address is 169.254.xx.yy, with the final two octets derived from the last two octets of the redundancy management IP address. This address is configured during the HA SSO configuration setup.

**Step 3:** Create a local DHCP scope for the service port on the Cisco Catalyst 6500 Series VSS and exclude the default gateway from the DHCP scope. This allows the Cisco WiSM2 to obtain an IP address for its service port automatically upon boot.

```
ip dhcp pool wism2-service-port
   network 172.16.10.0 255.255.255.0
   default-router 172.16.10.1
ip dhcp excluded-address 172.16.10.1 172.16.10.50
```

Step 4: Assign the service port and redundancy port VLAN.

```
wism service-vlan 1172
wism redundancy-vlan 1173
```

Step 5: Assign the allowed VLANs for data, voice, and management, and the native VLAN for the Cisco WiSM2.

```
wism switch 1 module 4 controller 1 allowed-vlan 116,120,275
wism switch 2 module 4 controller 1 allowed-vlan 116,120,275
wism switch 1 module 4 controller 1 native-vlan 275
wism switch 2 module 4 controller 1 native-vlan 275
```

Step 6: Configure the Cisco WiSM2 to trust DHCP and apply VLAN-based QoS.

wism switch 1 module 4 controller 1 qos trust dscp wism switch 2 module 4 controller 1 qos trust dscp wism switch 1 module 4 controller 1 qos vlan-based wism switch 2 module 4 controller 1 qos vlan-based



If you are using the Cisco WiSM2 with HA SSO enabled on a SUP2T, verify that you are running version 15.1(2)SY at a minimum. With versions prior to 15.1(2)SY the following workaround was used to prevent APs from re-registering during an HA SSO failover event.

```
port-channel hash-distribution fixed
```

**Step 7:** Reset the Cisco WiSM2 modules manually by removing and reinserting them into the Cisco Catalyst 6500 Series chassis or by using the following CLI commands.

hw-module switch 1 module 4 reset hw-module switch 2 module 4 reset

**Procedure 4** Configure the WLC Cisco AireOS platforms by using the Startup Wizard

After the WLC has been powered on and/or rebooted, you need to initially configure the Cisco AireOS WLC by using the CLI Startup Wizard.

Once connected, upon initial boot up of the WLC, you should see the following on the console. If you do not see this, press – a few times to force the startup wizard to back up to the previous step.

Welcome to the Cisco Wizard Configuration Tool Use the '-' character to backup

Step 1: Terminate the autoinstall process.

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

Step 2: Enter a system name. (Example: WLC-1)

System Name [Cisco 7e:8e:43] (31 characters max): WLC-1

Step 3: Enter an administrator username and password.



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

**Step 4:** If you are deploying the Cisco 5500 or WiSM2 Series Wireless LAN Controller, use DHCP for the service port interface address.

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

**Step 5:** If you are deploying the Cisco 5500 or 2500 Series Wireless LAN Controller, enable Link Aggregation (LAG).

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

**Step 6:** Enable the management interface. If you are configuring the secondary resilient controller in an HA controller pair, this IP address will only be in use during the first boot up of the WLC. Once the secondary resilient WLC downloads the configuration from the primary WLC, the secondary becomes a member of the HA controller pair. The secondary WLCs IP address is no longer used. In an N+1 configuration however, the secondary resilient controller is not part of the HA controller pair and will have its own unique IP address as configured.

Management Interface IP Address: 10.4.175.64 Management Interface Netmask: 255.255.255.0 Management interface Default Router: 10.4.175.1

**Step 7:** If you are configuring a Cisco WiSM2, the native VLAN is assigned on the Cisco 6500 VSS switch for the WiSM2. Configure the Management Interface VLAN Identifier as untagged. The tag for other devices is configured in the next step.

Management Interface VLAN Identifier (0 = untagged): 0

**Step 8:** If you are configuring a Cisco 5500 or 2500 Series WLC, you need to configure the Management Interface VLAN Identifier explicitly.

Management Interface VLAN Identifier (0 = untagged): 275

If you are configuring the Cisco 2500 Series Wireless LAN Controllers, you need to configure both WLCs individually as they do not support HA SSO and are therefore managed and configured separately. (Examples: 10.4.175.64 for WLC-1 and 10.4.175.65 for WLC-2)

Step 9: Enter the DHCP server for clients. (Example: 10.4.48.10)

Management Interface DHCP Server IP Address: 10.4.48.10

**Step 10:** If you are deploying a Cisco 5500 or WiSM2 Series Wireless LAN Controller, enable HA SSO. The 2500 Series Wireless LAN Controller does not support HA SSO.

Enable HA (Dedicated Redundancy Port is used by Default) [yes] [NO]: YES

If you are configuring the primary controller in an HA controller pair use the following values.

Configure HA Unit [PRIMARY][secondary]: **PRIMARY** Redundancy Management IP Address: **10.4.175.164** Peer Redundancy Management IP Address: **10.4.175.165** 

If you are configuring the secondary controller in an HA controller pair use the following values.

Configure HA Unit [PRIMARY][secondary]: **SECONDARY** Redundancy Management IP Address: **10.4.175.165** Peer Redundancy Management IP Address: **10.4.175.164** 

i

Tech Tip

**Step 11:** The virtual interface is used by the WLC for mobility DHCP relay, guest web authentication and inter-controller 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 12:** 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.)

```
Multicast IP Address: 239.1.1.1
```

i	Tech Tip
The r	multicast address must be unique for each controller or high availability controller
pair i	in the network. The multicast address entered is used as the source multicast
addre	ess, which the access points registered to the controller use for receiving wireless
user-	-based multicast streams.

Step 13: Enter a name for the default mobility and RF group. (Example: CAMPUS) Mobility/RF Group Name: CAMPUS

Step 14: Enter an SSID for the WLAN that supports data traffic. This is used later in the deployment process.

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

Step 15: Enable DHCP snooping.

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

Step 16: 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 Warning! The default WLAN security policy requires a RADIUS server. Please see documentation for more details.

Step 17: 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 18: 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 19:** 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 20: 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 21: Save the configuration.

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

The WLC resets and displays a **User:** login prompt.

```
(Cisco Controller)
Enter User Name (or 'Recover-Config' this one-time only to reset configuration to
factory defaults)
User:
```

If you configured the secondary 5500 or WiSM2 controller as a high availability controller pair, then the configuration for the secondary controller is complete. After the system reset finishes, the secondary controller downloads its configuration from the primary. Web access to the HA pair is obtained by using the IP address assigned to the management interfaces of the primary controller. Because no further steps in this procedure or process are used when configuring the secondary controller in an HA pair, you must use the following steps and procedures only for initial configuration of the primary controller.

# Procedure 5 Configure the time zone

Configuring the time and date of the WLC is critical, because certificate validation is performed using the date/ time as configured on the WLC. Improper date/time may prevent access points from successfully registering with the WLC. Ensure that the proper data and time has been obtained from the NTP server as configured in the Startup Wizard.

**Step 1:** Use a web browser to log in to the Cisco Wireless LAN Controller administration web page by using the credentials defined in Step 3. (Example: https://10.4.175.64)

Step 2: Navigate to Commands > Set Time.

Step 3: In the Location list, choose the time zone that corresponds to the location of the WLC.

Step 4: Click Set Time zone.

iiliiilii cisco	Sage Configuration Ping Logout Refresh
Commands Download File Upload File Reboot Config Boot Scheduled Reboot Reset to Factory	Set Time     Set Date and Time     Set Timezone       Current Time     Wed Oct 2 18:00:21 2013       Date       Month     October       Day     2
Default Set Time Login Banner Redundancy	Year 2013 Time Hour 18 • Minutes 0 Seconds 21
	Timezone Delta hours 0 mins 0 Location <sup>4</sup> [(GMT-8:00) Pacific Time (US and Canada)
	Foot Notes  1. Automatically sets daylight savings time where used.

**Step 5:** Press **OK** when prompted that continuing will cancel any scheduled system resets. Any scheduled system resets will be canceled as changing the time zone may cause a system reset at an undesirable time.

Message from webpage	3
The scheduled system reset will be cancelled. Are you sure you want to continue	
OK Cancel	

Procedure 6 Configure SNMP

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

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

Step 3: Enter the IP Address of your network management network. (Example: 10.4.48.0)

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

ahaha							Sa <u>v</u> e Cor	figuration   <u>P</u> ing   Logout   <u>R</u> ef	
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBACK	
CISCO Management Summary SNMP General SNMP V3 Users Communities Trap Receivers Trap Controls Trap Logs HTTP-HTTPS Telnet-SSH Serial Port Local Management Users User Sessions Logs	MONITOR SNMP v1 Communi IP Addres IP Mask Access Mc Status	WLANS / v2c Cc ty Name s	CONTROLLER pmmunity > N cisco 10.4.48.0 255.255.255.0 Read Only • Enable •	WIRELESS	SECURITY	MANAGEMENT	Saye Cor	ifiguration Ping Logout <u>P</u> et HELP FEEDBACK <back apply<="" td=""><td>resh</td></back>	resh
Software Activation     Tech Support									

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

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

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

Step 8: Enter the IP Address of your network management network. (Example: 10.4.48.0)

Step 9: Enter the IP Mask of your network management network. (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.

							Sa <u>v</u> e Cor	nfiguration   <u>P</u> ing	Logout <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs	<u>CONTROLLER</u>	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBAC	к
Management	SNMP v1	/ v2c Co	ommunity > N	ew				< Back	Apply
<ul> <li>Summary</li> <li>SNMP</li> <li>General</li> <li>SNMV V3 Users</li> <li>Communities</li> <li>Trap Receivers</li> <li>Trap Logs</li> <li>HTTP-HTTPS</li> <li>Telnet-SSH</li> <li>Serial Port</li> <li>Local Management</li> <li>User Sessions</li> <li>Logs</li> <li>Mgmt Via Wireless</li> <li>Software Activation</li> <li>Tech Support</li> </ul>	Communit IP Address IP Mask Access Mo Status	y Name ; de	iscol23 10.4.48.0 255.255.0 Read/Write ♥ Enable ♥					< back	Арріу

Step 12: Navigate to Management > SNMP > Communities.

Step 13: On the right side of the public community, point and click the blue down arrow, 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 have only the read-write and read-only community strings, as shown.

ahaha								Sa <u>v</u> e Con	iguratior	ı <u>P</u> ing	Logout   <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEM	1ent c <u>o</u>	MMANDS	HELP	FEEDBAC	<
Management	SNMP v1	/ v2c Co	ommunity								New
Summary											
▼ SNMP	Communit	y Name		10 4 49 0	IP Mask	ACC	cess mode	Status		-	
SNMP V3 Users	cisco123			10.4.48.0	255.255.25	55.0 Rez	ad-Write	Enable			
Communities											
Trap Controls											
Trap Logs											
HTTP-HTTPS											
Telnet-SSH											
Serial Port											
Local Management Users											
User Sessions											
▶ Logs											
Mgmt Via Wireless											
Software Activation											
Tech Support											

Step 16: Navigate to Management > SNMP > General and disable SNMP v3 Mode, then press Apply.

cisco	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>s</u> ecurity	M <u>a</u> nagement	C <u>O</u> MMANDS
Management	SNMP Sy	stem Su	immary				
Summary SNMP General SNMP V3 Users Communities Trap Receivers Trap Controls	Name Location Contact System D	escription	VWLC-F	roller			
Trap Logs HTTP-HTTPS	System O	bject ID	1.3.6.1.4.	1.9.1.1631			
Telnet-SSH Serial Port	SNMP Por Trap Port	t Number Number	161				
Local Management Users User Sessions Logs	SNMP v1 SNMP v2c SNMP v3	Mode Mode Mode	Disable Enable Disable				

Step 17: Navigate to Management > SNMP Communities > SNMP V3 Users.

**Step 18:** On the right side of the **default** User Name, point and click the blue down arrow, and then click **Remove**.

սիսիս					Sa <u>v</u> e C	onfiguration	<u>P</u> ing   L	ogout <u>R</u> efresh
CISCO MO	NITOR <u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	SECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK
Management	SNMP V3	Users						New
Summary								
▼ SNMP	User Name	Access	Level Au	th Protocol	Privacy Protoco	ol 👘		
General SNMP V3 Users	default	Readwrit	e HM	AC-SHA	AES	Remove	n	
Communities						(L		
Trap Receivers								
Trap Logs								
HTTP-HTTPS								
Telnet-SSH								
Serial Port								
Local Managemen Users	t							
User Sessions								
▶ Logs								
Mgmt Via Wireless	5							
Software Activation	on							
Frech Support								

Step 19: Press OK to confirm that you are sure you want to delete, then press Save Configuration.

- ahaha							Save Confi	guration 📋	Ping   L	ogout   <u>R</u> efresh
CISCO	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>s</u> ecuri	TY M <u>A</u> NAGE	MENT CC	MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK
Management	:	SNMP V3	Users							New
Summary										
▼ SNMP		User Name	Access I	Level Au	th Protoco	Privacy	Protocol			
General		default	Readwrit	e HM	IAC-SHA	AEC		-	-	
Communities						Message from	webpage		8	
Trap Receivers Trap Controls Trap Logs						Are	you sure you	ı want to dele	ete ?	
HTTP-HTTPS										
Telnet-SSH										
Serial Port							СК	C	ancel	
Local Manage Users	ment									
User Sessions										
Logs										
Mgmt Via Wir	eless									
Software Activ	vation									
Fech Support										
i Te	ech Tij	С								

### **Procedure 7** Limit which networks can manage the WLC

#### (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 https using SSL.

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

**Step 2:** Enter an access control list name (Example: ACL-Mgmt-Access-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

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

ahaha				Sa <u>v</u> e Configuration   <u>P</u> ing   Logout   <u>R</u> efresh
CISCO	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY MANAGEMENT	C <u>O</u> MMANDS HELP <u>F</u> EEDBACK
Security	Access Control Li	sts > Rules > New		< Back Apply
AAA     Local EAP     Priority Order     Certificate     Access Control Lists     Access Control Lists     CPU Access Control Lists     FlexConnect ACLs     Laver2 ACLs	Sequence Source Destination Protocol Source Port	1 IP Address • Any • TCP • Any •	IP Address 10.4.48.0	Netmask 255.255.255.0
Layer2 Acts Wireless Protection Policies Web Auth TrustSec SXP Local Policies Advanced	Destination Port DSCP Direction Action	HTTPS • Any • Any • Permit •		

Then click **Apply**.

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

Sequence	Source	Destination	Protocol	Source port	Destination port	Action
1	10.4.48.0/ 255.255.255.0	Any	ТСР	Any	HTTPS	Permit
2	10.4.48.0/ 255.255.255.0	Any	ТСР	Any	Other/22	Permit
3	Any	Any	ТСР	Any	HTTPS	Deny
4	Any	Any	TCP	Any	Other/22	Deny
5	Any	Any	Any	Any	Any	Permit

Table 10 - Access rule configuration values

սիսիս								Sa <u>v</u> e Configur	ation	<u>P</u> ing   Log	out <u>R</u> efresh
cisco	MONI	FOR <u>N</u>	LANS <u>C</u> ONTRO	DLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBA	CK
Security	Acce	Access Control Lists > Edit					< Back Add New Rule				Rule
► AAA											
Local EAP	Gene	ral									
Priority Order	Access	s List Nar	ne ACL-	Access-Rules							
Certificate	Deny (	Counters	0								
<ul> <li>Access Control Lists</li> <li>Access Control Lists</li> <li>CPU Access Control</li> </ul>	Seq	Action	Source IP/Mas	De k IP/	stination /Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
Lists FlexConnect ACLs Layer2 ACLs	1	Permit	10.4.48.0 255.255.255.0	/ 0.0 0.0	.0.0	ТСР	Any	HTTPS	Any	Any	0
Wireless Protection Policies	_2	Permit	10.4.48.0 255.255.255.0	/ 0.0 0.0	0.0.0 0.0.0	ТСР	Any	22	Any	Any	0
▶ Web Auth	3	Deny	0.0.0.0 0.0.0.0	0.0 / 0.0	0.0.0	TCP	Any	HTTPS	Any	Any	0
TrustSec SXP Local Policies	4	Deny	0.0.0.0	/ 0.0 0.0	.0.0	ТСР	Any	22	Any	Any	0
Advanced	_5	Permit	0.0.0.0 0.0.0.0	/ 0.0 0.0	1.0.0 1.0.0	Any	Any	Any	Any	Any	0

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.

```
Procedure 8 Configure wireless user authentication using Cisco ISE
```

In this design, the RADIUS authentication service is provided by the Cisco Identity Services Engine (ISE). The Cisco ACS server is used solely for network administrative access to the WLC using TACACS+.

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

Step 2: Enter the Server IP Address. (Example: 10.4.48.41)

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

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

			Sa <u>v</u> e Configura	ation <u>P</u> ing Logout <u>R</u> efresh
cisco	MONITOR WLANS CONTR	ROLLER WIRELESS SECURITY	MANAGEMENT COMMANDS	HELP EEEDBACK
Security	RADIUS Authentication S	Servers > New		< Back Apply
<ul> <li>AAA         <ul> <li>General</li> <li>RADIUS</li> <li>Authentication Accounting</li> <li>Fallback</li> <li>DNS</li> </ul> </li> <li>TACACS+         <ul> <li>LDAP</li> <li>Local Net Users</li> <li>MAC Filtering</li> <li>Disabled Clients</li> <li>User Login Policies</li> </ul> </li> <li>Priority Order</li> <li>Certificate</li> <li>Access Control Lists</li> <li>Wireless Protection Policies</li> <li>Weeb Auth</li> <li>TrustSec SXP</li> <li>Local Policies</li> <li>Advanced</li> </ul>	Server Index (Prionty) Server IP Address Shared Secret Format Shared Secret Confirm Shared Secret Key Wrap Port Number Server Status Support for RFC 3576 Server Timeout Network User Management IPSec	1 • 10.4.48.41 ASCII • • • • • • • • • • • • • •	stomers and requires a key wrap oc	mpliant RADIUS server)

**Step 5:** Repeat the Step 1 through Step 4 in the above process to add the secondary Cisco ISE authentication server (Example: 10.4.48.42), then press apply followed by click Save Configuration.

Step 6: In Security > AAA > RADIUS > Accounting, click New.

Step 7: Enter the ISE Server IP Address. (Example: 10.4.48.41)

Step 8:	Enter and	confirm the	Shared Secret,	and then click	Apply.	(Example:	SecretKey)
---------	-----------	-------------	----------------	----------------	--------	-----------	------------

ahaha			Sa <u>v</u> e Configura	tion <u>P</u> ing Logout <u>R</u> efresh
cisco	MONITOR WLANS CONTRO	DLLER WIRELESS SECURITY MA	NAGEMENT COMMANDS	HELP EEEDBACK
Security	RADIUS Accounting Serve	ers > New		< Back Apply
AAA     General     KADIUS     Authentication     Accounting     Fallback     DNS     TACACS+     LDAP     Local Net Users     MAC Filtering     Disabled Clients     User Login Policies     AP Policies     Paesword Policies	Server Index (Priority) Server IP Address Shared Secret Format Shared Secret Confirm Shared Secret Port Number Server Status Server Status Server Timeout	1 • 10.4.48.41 ASCII • 1813 Enabled • 2 seconds		
Local EAP	IPSec	Enable		
Priority Order				
Certificate				
Access Control Lists				
Wireless Protection Policies				
Web Auth				
TrustSec SXP				
Local Policies				
Advanced				

**Step 9:** Repeat Step 6 through Step 8 to add the secondary Cisco ISE accounting server (Example 10.4.48.42), click **Apply**, and then click **Save Configuration**.



# (Optional)

You can use this procedure to deploy centralized management authentication by configuring the authentication, authorization and accounting (AAA) service. If you use local management authentication, skip to Procedure 10, "Enable multicast support."

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). TACACS+ services are provided by Cisco ACS.

# i 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. This is because the standby WLC does not have an active management interface and it is therefore unable to communicate with the configured TACACS+ server directly.

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)

սիսիս						Sa <u>v</u> e Configura	ation   <u>P</u> i	ng   Logout   <u>R</u> efresh
CISCO	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	EEEDBACK
Security	TACACS+ Authen	tication Serve	rs > New			1	< Back	Арріу
General = RADIUS	Server Index (Prior	ity)	1 •					
Authentication	Server IP Address		10.4.48.15					
Fallback	Shared Secret Form	nat	ASCII 👻					
DNS = TACACS+	Shared Secret		•••••					
Authentication	Confirm Shared Se	cret	•••••					
Accounting Authorization	Port Number		49					
DNS	Server Status		Enabled	•				
Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies	Server filleout		J seco	nas				
Local EAP								
Priority Order								
Certificate								
Access Control Lists								
Wireless Protection     Policies								
Web Auth								
TrustSec SXP								
Local Policies								
Advanced								

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

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

սիսիս						Sa <u>v</u> e Configur	ation   <u>P</u>	ing Lo <u>q</u> out <u>R</u> efresh
cisco	MONITOR WLAN	CONTROLLER	. WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
Security	TACACS+ Accor	unting Servers	> New			1	< Back	Αρρίγ
AAA     General     General     Authentication     Acubentication     Accounting     Fallback     DNS     TACACS+     Authentication     Accounting     Authorization     DNS     LDAP     Local Net Users     MAC Filtering     Disabled Clients     User Login Policies     Password Policies     Local EAP     Priority Order     Certificate     Access Control Lists     Wireless Protection     Policies     Wireless Protection     Policies     Web Auth     TrustSec SXP	Server Index (Pri Server IP Addres Shared Secret Fo Shared Secret Confirm Shared S Port Number Server Status Server Timeout	ority) 1 s 10 ecret •• Er 5	A448.15     SCII      mabled      seconds					
Local Policies Advanced								

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

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)

ahaha							Sa <u>v</u> e Configura	ation   <u>I</u>	2ing   Logout   <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
Security	TACACS	Authori	zation Server	s > New				< Back	Apply
General General RADIUS Authentication Accounting Fallock DNS TACACS+ Authentication Accounting Authorization DNS LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies	Server IF Shared S Shared S Confirm S Port Nur Server S Server Ti	ndex (Priori ecret Form Secret Form Secret Shared Sec Shared Sec Shared Sec Shared Sec Shared Sec	ty) nat	1 • 10.4.48.15 ASCII • 49 Enabled • 5 seco	nds				
Local EAP									
Priority Order									
Certificate									
Access Control Lists									
Wireless Protection Policies									
Web Auth									
TrustSec SXP									
Local Policies									
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							Save Configura		ong   Logout   <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
Security	Priority C	order > N	lanagement U	ser					Αρρίγ
<ul> <li>AAA</li> <li>Local EAP</li> <li>Priority Order Management User</li> <li>Certificate</li> <li>Access Control Lists</li> </ul>	Authentic Not RADIU	Used IS	>	Order	Used for Auth TACACS+ LOCAL	entication	n		
<ul> <li>Wireless Protection Policies</li> <li>Web Auth TrustSec SXP Local Policies</li> <li>Advanced</li> </ul>	MONITOR WLANS CONTROLLER Priority Order > Management Us Authentication Not Used RADIUS C If LOCAL is selected as second priority the LOCAL only if first priority is unreachable.			en user will be	authenticated	against			

**Step 14:** Verify that TACACS+ authentication is functioning properly by logging off the wireless LAN controller and logging back on. If you are unable to logon, verify that the WLC has been added to the ACS server properly by reviewing the ACS Section called Configuring Cisco Secure ACS for Wireless Infrastructure Access above.

# Procedure 10 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 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.

The various multicast streams can be delivered to the APs in one of two manners. The first is called Multicast-Unicast, and in this mode each multicast stream is converted to unicast and sent to the access points with wireless clients who have requested the multicast stream. When many users across many access points are requesting the same stream, the WLC must replicate each frame of the multicast stream, convert it into a unique unicast format, and replicate it for each access point with an associated multicast subscriber. For large numbers of access points and subscribed multicast users, the frame replication is highly inefficient.

A better method (and the only method for a Cisco 2504 Series WLC) is to use multicast-multicast (MC-MC) mode. In MC-MC mode the multicast stream is converted to a unique controller-to-AP multicast flow. The underlying campus infrastructure, which must be configured for multicast, will facilitate that this MC-MC flow reach each AP that has subscribed wireless users requesting a multicast stream. The end result is a much more scalable and efficient method for handling multicast flows across the campus network.

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

սիսիս								ation   [	ing   Logout   <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
Controller	Multicast								Apply
General									
Inventory	Enable G	ilobal Multi	cast Mode	1					
Interfaces	Enable I	GMP Snoop	bing						
Interface Groups	IGMP Tim	neout (sec	onds) 60						
Multicast	IGMP Qu	ery Interv	al (seconds) 20						
Network Routes	Enable M	1LD Snoop	ing 📃						
Redundancy	MLD Time	eout (seco	nds) 60						
Internal DHCP Server	MLD Oue	rv Interva	l (seconds) 20						
Mobility Management									
Ports									
▶ NTP									
▶ CDP									
PMIPv6									
▶ IPv6									
mDNS									
Advanced									

Step 2: Navigate to Controller > General.

**Step 3:** If you are using Cisco 5500 or WiSM2 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: 239.1.1.1), and then click **Apply**.



**Step 4:** 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 12 of the "Configure the WLC Cisco AireOS platform" procedure, and then click **Apply**.

սիսիս							Sa <u>v</u> e Configur	ation   <u> </u>	<u>P</u> ing   Lo <u>q</u> out   <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
Controller	General								Apply
General Inventory Interfaces Interface Groups Multicast Network Routes Redundancy Internal DHCP Server Mobility Management Ports NTP CDP PMIPv6 IPv6 MDNS Advanced	Name 802.3x Flov LAG Mode of Broadcast F AP Multicas AP Fallback Fast SSID of Default Mot RF Group N User Idle Ti ARP Timeou Web Radius WebAuth P Mode WebAuth P Mode WebAuth P Mode I Pode I Pod HA SKU sec 1. Multicast	v Contro on next rt Forwardi : : : : : : : : : : : : : : : : : : :	I Mode reboot ing t main Name seconds) ids) itication jirection Port ips 2 unit upported with Files there is no restr	WLC-1       Disabled       Enabled       Visabled       Multicast       Enabled       WiSM2       300       300       Disabled       O       Disabled       O       Enabled       ViSM2       Side       Side       Side       ViSM2       Side       Side       Disabled       Connect on th       Connect on th	239.1.1.1	(LAG Multicast Gr	Mode is currenth	v enable4	<u>аџру</u>

Procedure 11 Create the WLAN data interface

Configure the WLC to separate voice and data traffic, which is essential 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)

սիսիս							Sa <u>v</u> e Configur	ation   <u>P</u>	ing Logout <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
Controller	Interfaces	s > New					1	< Back	Apply
General Inventory Interfaces Interface Groups Multicast Network Routes Redundancy Internal DHCP Server Mobility Management Ports NTP CDP	Interface VLAN Id	Name	Wireless-Data 116				_		
mDNS									
Advanced									

Step 4: In the IP Address box, enter the IP address assigned to the WLC interface. (Example: 10.4.16.5)

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

**Step 6:** In the **Gateway** box, enter the IP address of the VLAN interface defined in Procedure 1. (Example: 10.4.16.1)

**Step 7:** 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**.

արտիս								Sage Configuration Ping Logout Refr	esh
cisco	MONITOR WLANS	<u>C</u> ONTROLLER W	IRELESS SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	EEEDBACK		
Controller	Interfaces > Edit							< Back Apply	~
Garant									1
General									
Interfaces	General Informati	ion							
Interface Groups	Interface Name	wireless-dat	ta						
Multicast	MAC Address	6c:20:56:20	c:0f:2f						
Network Routes									
Redundancy	Configuration								
Internal DHCP Server	Guest Lan								
Mobility Management	Quarantine								
Ports	Quarantine Vlan Id	0							
▶ NTP	NAS-ID	WiSM2							
► CDP	Physical Informat	ion							
PMIPv6	The interface is attac	hed to a LAG.							
▶ IPv6	Enable Dynamic AP M	Management 🗌							
mDNS									
Advanced	Interface Address								
	VLAN Identifier	116							
	IP Address	10.4.16	.5						
	Netmask	255.255	5.252.0						
	Gateway	10.4.16	.1						1
	DHCP Information								
	Primary DHCP Serve	r	10.4.48.10						
	Secondary DHCP Ser	ver							
	DHCP Proxy Mode		Global 🗸						
	Enable DHCP Option	82							4

i	Tech Tip
To pre WLC's scope	event DHCP from assigning wireless clients addresses that conflict with the s addresses, exclude the addresses you assign to the WLC interfaces from DHCP es on the DHCP server.

**Procedure 12** 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)

ահահե										Save Configuration Ping	Logout <u>R</u> efresh
CISCO	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK		
Controller	Interfaces	s > New								< Back	Apply
General Inventory Interfaces Interface Groups Multicast Network Routes Network Routes Internal DHCP Server Mobility Management Ports NTP COP NTP NTP PORS	Interface VLAN Id	Name	wireless-voice 120		×						
Advanced											

Step 4: In the IP Address box, enter the IP address assigned to the WLC interface. (Example: 10.4.20.5)

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

**Step 6:** In the **Gateway** box, enter the IP address of the VLAN interface defined in Procedure 1. (Example: 10.4.20.1)

**Step 7:** 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**.

արտիս									Save Configuration		Logout R	efresh
CISCO	MONITOR WLA	Ns <u>C</u> ONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK				
Controller	Interfaces > E	dit							< Bao	:k	Apply	
General												
Inventory												
Interfaces	General Inform	nation										
Interface Groups	Interface Name	wireles	s-voice									
Multicast	MAC Address	6c:20:	56:2c:0f:2f									
Network Routes	Configuration											
Redundancy	Curatilar											
Internal DHCP Server	Guest Lan											
Mobility Management	Quarantine Vlan	Id 0										
Ports	NAS-ID	WiSM2										
▶ NTP	1010 10	THO IL										
► CDP	Physical Infor	nation										
▶ PMIPv6	The interface is	attached to a LAG.										
▶ IPv6	Enable Dynamic	AP Management 🗌										
▶ mDNS	Interface Add	066										
Advanced	Interface Addi	655			_							
	VLAN Identifier	120										
	IP Address	10.	1.20.5									
	Netmask	255	.255.252.0									
	Gateway	10.	+.20.1									- 1
	DHCP Informa	tion										
	Primary DHCP S	erver	10.4.48.	10 ×								
	Secondary DHC	Server										
	DHCP Proxy Mor	le	Global	~								
	Enable DHCP Op	tion 82										


## **Procedure 13** Configure the data wireless LAN for multicast

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 4. (Example: WLAN-Data)

սիսիս		Sa <u>v</u> e Configuration <u>P</u> ing Logout <u>R</u> efresh
CISCO	MONITOR WLANS CONTROLLER WIRELESS SE	CURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs	Entries 1 - 1 of 1
WLANS	Current Filter: None [Change Filter] [Clear Filter	Create New  Go
Advanced	WLAN	Admin
	- ID Type Profile Name	WLAN SSID Status Security Policies
	I WEAN WEAN-Data	wEAN-Data Enabled [WPA2][Adth(602.1X)]

**Step 3:** On the General tab, in the **Interface/Interface Group(G)** list, choose the interface created in Procedure 11. (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)

սիսիս			Save Configuration Ping Logout Refresh
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECUR.	TY MANAGEMENT COMMANDS HELI	P <u>F</u> EEDBACK
WLANs	WLANs > Edit 'WLAN-Data'		< Back Apply
VLANs	General Security QoS Policy-Mapping	Advanced	
Advanced	Profile Name WLAN-Data		
	Type WLAN		
	SSID WLAN-Data		
	Status 🗹 Enabled		
	Security Policies [WPA2][Auth(802.1X)] (Modifications done under sec	rity tab will appear after applying the changes.	.)
	Radio Policy All V		
	Interface/Interface Group(G) wireless-data		
	Multicast Interface wireless-data		
	Broadcast SSID Senabled		
	NAS-ID WISM2		
			V

Step 5: Click Apply.

Next, enable Application Visibility and Control (AVC).

**Step 6:** Navigate to the QoS tab, select **Application Visibility**, click **Apply**, and then click **Save Configuration**, and agree to confirmation questions.

ahaha	Save Configuration   Ping   Logo	out   <u>R</u> efresh
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	
WLANs	WLANs > Edit 'WLAN-Data' < Back A	Apply
WLANs	General Security QoS Policy-Mapping Advanced	_
Advanced	Quality of Service (QoS)     Silver (best effort)       Application Visibility     U Enabled	^
	AVC Profile note	
	Override Per-User Bandwidth Contracts (kbps) <sup>16</sup>	
	DownStream     UpStream       Average Data Rate     0     0       Burst Data Rate     0     0       Average Real-Time Rate     0     0	
	Override Per-SSID Bandwidth Contracts (kbps) <sup>16</sup>	
	Average Data Rate 0 0	
	Burst Data Rate 0 0 >	,

## Procedure 14 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.

Configure the voice WLAN by changing the default QoS settings to platinum and segmenting the voice traffic onto the voice wired VLAN.

a ha ha		Sa <u>v</u> e Configuration <u>P</u> ing Logout <u>R</u> efresh
cisco	MONITOR WLANS CONTROLLER WIRELESS SEC	CURITY MANAGEMENT COMMANDS HELP FEEDBACK
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 1: On the WLANs page, in the list, choose Create New, and then click Go.

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)

cisco	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY MANAGEME	NT COMMANDS	HELP	<u>F</u> EEDBACK	Sage configuration   Ping   Logout   Kerresh
WLANs	WLANs > New						< Back Apply
<ul> <li>₩LANs</li> <li>WLANs</li> <li>Advanced</li> </ul>	Type Profile Name SSID ID	WLAN       Voice       WLAN-Voice       2	×				

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 12. (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.

ahaha		Save Configuration   Ping   Logout   Refresh
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK	
WLANs	WLANs > Edit 'Voice'	< Back Apply
WLANs     WLANs	General Security QoS Policy-Mapping Advanced	
Advanced	Profile Name Voice	
	Type WLAN	
	SSID WLAN-Voice	
	Status 🗹 Enabled	
	Security Policies [WPA2][Auth(002.1X)] (Hodifications done under security tab will appear after applying the changes.)	
	Radio Policy All	
	Interface/Interface Group(G) wireless-voice 🗸	
	Multicast Vian Feature 🗹 Enabled	
	Multicast Interface wireless-voice 🗸	
	Broadcast SSID 🗹 Enabled	
	NAS-ID WISM2	
		~

Step 8: On the Security > Layer 2 tab, enable Cisco Centralized Key Management (CCKM) by selecting Enable.

i Tech Tip CCKM may not be compatible with older wireless clients that do not support the CCX v4.0 or v5.0 extensions. Disabling CCKM may be necessary in environments where older wireless devices are used or where public use of wireless devices using 802.1x/ WPA2 is a requirement. cisco WLANs WLANs > Edit 'Voice' < Back Apply ▼ WLANs General Security QoS Policy-Mapping Advanced Layer 2 Layer 3 AAA Servers Advanced Layer 2 Security <sup>6</sup> WPA+WPA2 Ŧ MAC Filtering Fast Transition Fast Transition 📃 Protected Management Frame DME Disabled 💌 WPA+WPA2 Parameters WPA Policy WPA2 Policy V WPA2 Encryption Ass TKIP Authentication Key Management 802.1X Enable Enable Enable CCKM

PSK

Step 9: On the QoS tab, in the Quality of Service (QoS) list, choose Platinum (voice), enable Application Visibility, and then click Apply.

սիսիս cisco	MONITOR WLANS CONT	ROLLER WIRELESS	SECURITY MANAGEMENT	C <u>o</u> mmands he <u>l</u> p	Save Configuration Ping	Logout <u>R</u> efresh
WLANs	WLANs > Edit 'Voice'	S for the			< Back	Apply
<ul> <li>▼ WLANS WLANS</li> <li>&gt; Advanced</li> </ul>	Ceneral Security Quality of Service (QoS) Application Visibility AVC Profile Netflow Monitor Override Per-User Ban Average Data Rate Burst Data Rate Average Real-Time Rate	Qos Policy-Ma Platnum (voice) Platnum	(kbps) <sup>15</sup> ream			^
	Burst Real-Time Rate Clear Override Per-SSID Bar Average Data Rate Burst Data Rate	o     o       odwidth Contracts       DownStream     UpS       o     o       o     o       o     o	(kbps) <sup>16</sup> tream			Ŷ

# (Optional)

If you are configuring Cisco 2500 Series WLCs, HA SSO is not supported. You should complete this procedure in order to join multiple controllers to a mobility group. If you are configuring a Cisco WiSM2 or 5500 Series WLCs, HA SSO is supported and you should skip this procedure.

A *mobility group* is a group of wireless LAN controllers that share the same group name. Controllers sharing the same mobility group name exchange wireless client state information, controller load, client data (to facilitate seamless inter-controller roaming) and controller redundancy information. It is for this reason that in an N+1 redundancy model that a shared mobility group be established.

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 HA 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 HA 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, controllers servicing an area where seamless roaming is required should use the same mobility group name. In environments where seamless roaming is not required (for example, between multiple buildings), it is recommended that you use different mobility domain names between the building-dedicated controllers. This best practice prevents unneeded mobility information from being shared between controllers across buildings.

When you create a mobility group, you enable multiple controllers in a network to dynamically share information and forward data traffic when inter-controller 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 4 through Procedure 14 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.

							ogout <u>R</u> efrei
cisco	MONITOR WLANS CONTROLLER W	IRELESS SECURITY MANAGEMENT	COMMANDS HELP EEEDBACK				
Controller	Static Mobility Group Members					New	EditAll
General Inventory	Local Mobility Group CAMPUS						
Interfaces	MAC Address IP Address	Group Name	Multicast IP	Status	Hash Key		
Interface Groups	20:3a:07:67:7c:40 10.4.175.64	CAMPUS	0.0.0.0	Up	none		
Multicast							
Internal DHCP Server							
<ul> <li>Mobility Management Mobility Configuration Mobility Groups Mobility Anchor Config Multicast Messaging</li> </ul>							

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: 10.4.175.64)

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

ahaha										Save Configuration Ping	Logout <u>R</u> efrest
cisco	MONITOR WL	ANs	<u>C</u> ONTROLLER	WIRELESS	SECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK		
Controller	Mobility Grou	up Me	ember > New							< Back	Apply
General Inventory Interfaces Interface Groups	Member IP Ad Member MAC Group Name Hash	ddress Addre	10.4.175.0 ss 20:3a:07: CAMPUS	54 67:7c:40	×						
Multicast <ul> <li>Internal DHCP Server</li> </ul>											
<ul> <li>Mobility Management</li> <li>Mobility Configuration</li> <li>Mobility Groups</li> <li>Mobility Anchor Config</li> <li>Multicast Messaging</li> </ul>											

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: 10.4.175.65)

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

ահահո									Save Configuration   Ping	Logout <u>R</u> efresh
CISCO	MONITOR WLANS	<u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK		
Controller	Mobility Group I	/lember > New							< Back	Apply
General Inventory Interfaces Interface Groups Multicast F Internal DHCP Server	Member IP Addre Member MAC Add Group Name Hash	ss 10.4.175 dress 20:3a:07 CAMPUS none	65		×					
<ul> <li>Mobility Management Mobility Configuration Mobility Groups Mobility Anchor Config Multicast Messaging</li> </ul>										

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 connectivity between all the controllers by examining the mobility group information. In the Status column, all controllers should be listed as Up.

ululu cisco	MONITOR WLANS	CONTROLLER WIRE	LESS SECURITY	MANAGEMENT	COMMANDS	HELP EEEDBACK		Sage Configuration Ping Logo	ut <u>R</u> efresh
Controller	Static Mobility G	oup Members						New	EditAll
General Inventory	Local Mobility Gro	CAMPUS							
Interfaces	MAC Address	IP Address		Group Name	Multicast IP		Status	Hash Key	
Interface Groups	20:3a:07:67:7c:40	10.4.175.64		CAMPUS	0.0.0.0		Up	none	
Multicast <ul> <li>Internal DHCP Server</li> </ul>	20:3a:07:67:99:20	10.4.175.65		CAMPUS	0.0.0.0		Up	none	
<ul> <li>Mobility Management         Mobility Configuration             Mobility Groups             Mobility Anchor Config             Multicast Messaging         </li> </ul>									

Procedure 16	Enable Band Select and ClientLink on Cisco AireOS WLCs
--------------	--

**i** Tech Tip Enabling Band Select and Cisco ClientLink 1.0 is disruptive to active users on the WLAN. Enabling Band Select on WLANs that provide real-time wireless services (i.e., WLAN-Voice) is not recommended. Also note that ClientLink 1.0 only applies to generation 1 access points. ClientLink 2.0 and 3.0 are both enabled by default for generation 2 and the Cisco Aironet 3700 Series Access Point, respectively.

Step 1: Navigate to Wireless > Advanced > Band Select, verify the following values are present for Band Select, and then click Apply.

a da a d							onfiguration   ]		o <u>q</u> out <u>R</u> efresh
cisco	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK
Wireless	Band Sel	ect							Apply
Access Points	Probe Cy	cle Count			2				
<ul> <li>Advanced</li> </ul>	Scan Cy	cle Period <sup>-</sup>	Fhreshold (millised	conds)	200				
Load Balancing Band Select	Age Out	Suppressio	in (seconds)		20				
Preferred Calls	Age Out Dual Band (seconds)								
SIP Snooping	Acceptab	le Client R	SSI (dBm)		-80				
Mesh	* Band Se	elect is con	figurable per WLA	Ν.					

Next, enable Band Select on the WLAN-Data WLAN.

Step 2: Navigate to WLANs and select the WLAN-Data WLAN.

Step 3: Navigate to the Advanced tab, enable Client Band Select (scrolling the window may be required to see the option), and then click Apply.

CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK
WLANs	WLANs > Edit 'WLAN-Data-5508'
WLANs     WLANs	General Security QoS Policy-Mapping Advanced
▶ Advanced	Enable Session Timeout       I 1000         Aironet IE       Session Timeout (secs)       DHCP Addr. Assignment       Required         Diagnostic Channel       Enabled       DEAP         Override Interface ACL       IPv4       None ▼       None ▼         Layer2 Ad       None ▼       None ▼       Nanagement Frame Protection (MFP)         Layer2 Ad       None ▼       MPP Client Protection <sup>4</sup> Optional ▼         Client Exclusion <sup>3</sup> Enabled       DTIM Period (in beacon intervals)
	Maximum Allowed     0     802.11a/n (1 - 255)     1       Clients <sup>d</sup> 0     802.11a/n (1 - 255)     1       Static IP Tunneling <sup>dd</sup> Enabled     NAC       Wi-Fi Direct Clients     Disabled     NAC State     None       Policy     Disabled     Load Balancing and Band       Maximum Allowed     200     Client Load Balancing       Clear HotSpot     Enabled     Client Band Select

**Step 4:** Click **OK**. This acknowledges that enabling Band Select may impact time sensitive applications such as Voice.

uluilu cisco		ROLLER WIRELESS SEC	JRITY MANA	Saye Configuration   <u>P</u> ing   GEMENT C <u>O</u> MMANDS HELP <u>E</u> EEDBACK	Logout   <u>R</u> efresh
WLANs	WLANs > Edit 'WLAN-I	Data-5508'		< Back	Apply
₩LANs WLANs	General Security	QoS Policy-Mapping	Advanced		
▶ Advanced	Enable Session Timeout Aironet IE Diagnostic Channel Override Interface ACL Layer2 Acl Warning: Allowing Ban continue?	1000     Session Timeout (secs)     Session Timeout (secs)     Denabled     JPv4 None     None     One      destect on this WLAN may impa	IPv6 None 👻	DHCP Addr. Assignment Required DEAP Split Tunnel (Printers) Enabled Management Frame Protection (MFP) Marin Clina Resolution Control II a application like VOICE. Do you want to	E
	Policy Maximum Allowed Clients Per AP Radio	Disabled -		Load Balancing and Band Select Client Load Balancing	
	Clear HotSpot	Enabled		Client Band Select	

**Step 5:** Click **OK**. This acknowledges that enabling Band Select will be disruptive to any user currently using this WLAN.

Step 6: Click Save Configuration, and acknowledge confirmations. The configuration is saved.

cisco	MONITOR WLANS CONT	ROLLER WIRELESS SECT	JRITY MANA	Sa <u>v</u> e Configuration <u>P</u> ing Logout ! GEMENT C <u>O</u> MMANDS HELP <u>E</u> EEDBACK	<u>R</u> efresh
WLANs	WLANs > Edit 'WLAN-	Data-5508'		< Back Ap	ply
WLANs WLANs Advanced	General Security Enable Session Timeout	QoS Policy-Mapping	Advanced		*
	Aironet IE Diagnostic Channel	Session Timeout (secs) Enabled Enabled	10.16	DHCP Addr. Assignment Required OEAP Split Tunnel (Printers) Enabled	
	Override Interface ACL Layer2 Acl	IPv4 None   None   Disclored	None -	Management Frame Protection (MFP)	н
	Changing WLAN para result in loss of conne	meters while it is enabled will cau ctivity for some clients. Press OK	se the WLAN to to continue.	be momentarily disabled and thus may	
			OK Cancel		
	Policy Maximum Allowed	Disabled 👻		Load Balacing and Band Select	
	Clients Per AP Radio	200		Client Load Balancing	
	Clear HotSpot	Enabled	m	Client Band Select	*

i Tech Tip

Starting in Cisco AireOS release 7.2, Cisco ClientLink 2.0 is enabled by default and supported by generation 2 access points (Cisco Aironet 1600, 2600, and 3600 Series). ClientLink 1.0 (Legacy ClientLink) is disabled by default and applies only to generation 1 access points (Cisco Aironet 1140, 3500, 1250, 1260 Series). In release 7.6, ClientLink 3.0 along with 2.0 is enabled by default. The Command Line Interface (CLI) must be used to enable or disable ClientLink 1.0. It can be globally enabled on a radio (2.4 GHz and/or 5 GHz) basis and is not enabled on a per-WLAN instance.

**Step 7:** Before you enable Cisco ClientLink 1.0 from the CLI of the Cisco AireOS controller, the 802.11a network must first be disabled by entering the following.



Performing this action is disruptive to ALL access-points on this controller providing 802.11a (5 GHz) services.

config 802.11a disable network

**Step 8:** When prompted that disabling the 802.11a network may strand mesh APs, enter **Y** to confirm the possible disruption of service.

Disabling the 802.11a network may strand mesh APs. Are you sure you want to continue?  $(y/n)\,\textbf{Y}$ 

**Step 9:** From the CLI of the Cisco AireOS controller, enable Cisco ClientLink 1.0 (also called *Legacy Tx Beamforming*) for the all generation 1 ClientLink 1.0 capable access points operating in the 802.11a band by entering the following.

config 802.11a beamforming global enable

Step 10: From the CLI of the Cisco AireOS controller, enable the 802.11a network by entering the following. config 802.11a enable network

Step 11: From the CLI of the AireOS controller, disable the 802.11b network by entering the following.



config 802.11b disable network

**Step 12:** From the CLI of the Cisco AireOS controller, enable Cisco ClientLink for the all ClientLink capable access points operating in the 802.11b band by entering the following.

config 802.11b beamforming global enable

Step 13: From the CLI of the Cisco AireOS controller, enable the 802.11b network by entering the following.

config 802.11b enable network

**Step 14:** Save the configuration by entering the following command, and then confirm that you want to save the configuration by pressing **y**.

save config Are you sure you want to save? (y/n)  ${\boldsymbol y}$ 

1 Tech Tip
If you want to see if a particular AP has ClientLink (beamforming) enabled, enter the following CLI command on the WLC. (Example: show ap config 802.11b AP4403. a734.8a68)
show ap config [802.11b   802.11a] [AP Name]
(Cisco Controller) >show ap config 802.11b AP4403.
a734.8a68
Phy OFDM parameters
Configuration
AUTOMATIC
Current Channel 11
Channel Assigned By DCA
Extension Channel NONE
Channel Width 20 Mhz
Allowed Channel List
1,2,3,4,5,6,7,8,9,10,11
TI Threshold
Legacy Tx Beamforming Configuration
CUSTOMIZED
Legacy Tx Beamforming ENABLED
Antenna Type
INTERNAL_ANTENNA

# Procedure 17 Enable 802.11ac using DCA on Cisco AireOS WLCs

With the advent of 802.11ac Wave 1, 40 and 80 MHz wide channels can be enabled. This can be accomplished manually on an AP-by-AP basis, or globally by using Dynamic Channel Assignment (DCA). Changing the default channel width for 802.11ac capable access points requires the 802.11a network to be disabled.

### OO Reader Tip

It may be helpful to review the "802.11ac Bandwidth Performance" and "802.11ac Channel Planning" sections in the introductory section of this guide before proceeding with these steps.

August 2014 Series

Step 1: Disable the 802.11a network by navigating to Wireless > 802.11a/n/ac > Network, clearing the 802.11a Network Status check box, pressing OK on the resulting Warning message and then clicking Apply.



սիսիս								Logout   <u>R</u> efresh
cisco	MONITOR WLANS CONTR	ROLLER WIRELESS	SECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK	
Wireless	802.11a Global Paramete	ers						Apply
<ul> <li>Access Points         <ul> <li>All APs</li> <li>Dedice</li> </ul> </li> </ul>	General			Data Rates**				
Nouse 11a/n/ac     802.11a/n/ac     802.11a/n/ac     802.11b/g/n     Dual-Band Radios     Global Configuration     Advanced     Mesh     RF Profiles     FlexConnect Groups     FlexConnect ACLs	802.11a Network Status Beacon Period (millisecs) Fragmentation Threshold (bytes) DTPC Support. Maximum Allowed Clients RSSI Low Check RSSI Threshold (-60 to -90 dBm)	Enabled 2346 Enabled 200 Enabled -80		6 Mbps 9 Mbps 12 Mbps 18 Mbps 24 Mbps 36 Mbps 48 Mbps 54 Mbps	Mai Sup Mai Sup Sup Sup Sup	ndatory - oported - oported - ndatory - oported - oported - oported -	• • • •	
▼ 802.11a/n/ac	802.11a Band Status			CCX Location	Measureme	nt		
RRM RF Grouping TPC DCA	Low Band Mid Band High Band	Enabled Enabled Enabled		Mode	E 6	nabled		
Coverage General Client Roaming Media EDCA Parameters DFS (602.11h) High Throughput (802.11h/ac) CleanAir \$ 802.11b/g/n	** Data Rate 'Mandatory' implies that cleants who do not support that specific rate will not be able to associate. Data Rate 'Supported' implies that any associated client that also supports that same rate may communicate with the AV using that rate. But it is not required that a client be able to use the rates marked supported in order to associate The actual data rates that are supported dispend on the channel selected as different channels may have different bandwidths. The reason is that we show data rates and allow the user to select the data rates. But in reality, the AP will polit the next lower data rate allowed for that channel if the channel data rate is not allowed for that channel if the channel data rates is not			t er				
Media Stream								

**Step 2:** Navigate to **Wireless > 802.11a/n/ac > RRM > DCA**, select the desired channel width to use (Example: 20 MHz, 40 MHz, 80 MHz), and then, if available in your regulatory domain, enable **Extended UNII-2 Channels**. (The window may need to be scrolled to view this option.) Click **Apply**.

սիսիս						Sa <u>v</u> e	Configuration	<u>P</u> ing   I	.ogout <u>R</u> efresh
CISCO	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLE	R W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK
Wireless	802.11a>	RRM > I	Dynamic Ch	nannel Assig	nment (DCA	)			Apply
Access Points     All APs     Dedies	Dynamic	Channel .	Assignment	Algorithm					
802.11a/n/ac 802.11b/g/n Dual-Band Radios Global Configuration	Channel .	Assignment	: Method	Automatic Freeze OFF	Interval: 1 Invoke C	0 minutes 👻 And hannel Update O	horTime: 0 🗸		
Advanced	Avoid For	reign AP int	erference	🔽 Enabled					
Mesh	Avoid Cis	co AP load		Enabled					
RF Profiles	Avoid nor	n-802.11a r	noise	🔽 Enabled					
FlexConnect Groups	Avoid Pei Interfere	rsistent Nor nce	i-WiFi	🔲 Enabled					
FlexConnect ACLs	Channel	Assignment	Leader	5508-1 (10.4.3	0.66)				
<ul> <li>802.11a/n/ac</li> <li>Network</li> </ul>	Last Auto	Channel A	ssignment	472 secs ago					
▼ RRM	DCA Cha	innel Sensit	ivity	Medium 👻	(15 dB)				
TPC	Channel	Width		© 20 MHz © 4	0 MHz 🖲 80 MH	z			
DCA	Avoid che	eck for non-	DFS channel	🔲 Enabled					
Coverage General	DCA Char	nel List							
Client Roaming Media EDCA Parameters DFS (802.11h) High Throughput (802.11n/ac) CleanAir	DCA Cha	nnels	36, 40, 116, 13	44, 48, 52, 56, 6 2, 136, 140, 149	0, 64, 100, 104 , 153, 157, 161	, 108, 112,			
▶ 802.11b/g/n									
Media Stream	Select	Channe							
Application Visibility	<b>V</b>	36				*			
And Control		40				-			
Country	V.	44							
Timers	V	52							
Netflow	(Trial)					*			
▶ QoS									
	Extended	UNII-2 cha	annels 🛛 🗹 Er	nabled					

Step 3: Enable the 802.11a network by navigating to Wireless > 802.11a/n/ac > Network, selecting the 802.11a Network Status Enabled box, clicking Apply, and then clicking Save Configuration. Agree to confirmation questions.

						Sa <u>v</u> e Con	figuration   <u>P</u> ing	Lo <u>q</u> out   <u>R</u> efresh
CISCO	MONITOR WLANS CONTR	OLLER WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	
Wireless	802.11a Global Paramete	rs						Apply
Access Points     All APs     Radios     802.11a/n/ac     802.11b/g/n	General 802.11a Network Status Beacon Period (millisecs)	✓ Enabled 100		Data Rates** 6 Mbps 9 Mbps	Mai	ndatory •	-	
Global Configuration	Fragmentation Threshold	2346		12 Mbps	Mai	ndatory •	-	
Advanced	DTPC Support.	🗹 Enabled		18 Mbps	Sup	oported ·	•	
Mesh	Maximum Allowed Clients	200		24 Mbps	Mai	ndatory 🔸	•	
RF Profiles	RSSI Low Check	Enabled		36 Mbps	Sup	oported ·	•	
FlexConnect Groups FlexConnect ACLs	RSSI Threshold (-60 to -90 dBm)	-80		48 Mbps 54 Mbps	Sup	oported ·	•	
▼ 802.11a/n/ac	802.11a Band Status							
Network	Low Band	Enabled	Enabled -		Measuremei	isurement		
RF Grouping	Mid Band	Enabled		Mode	E 6	nabled		
TPC DCA Coverage	High Band	Enabled						
General Client Roaming Media EDCA Parameters DFS (802.11h) High Throughput (802.11n/ac) CleanAir 802.11b/g/n	** Data Rate 'Mendatory' implies that clients who do not support that specific rate will not be able to associate. Data Rate 'Supported' implies that any associated client that also supports that rane rate may communicate with the AP using that rate. But it is not required that a client be able to use the rates marked supported in order to associate The actual data rates that are supported depend on the channel selected as different channels may have different bandwidths. The reason is that we show data rates and allow the user to select the data rates. Data in reality, the AP will pick the next lower data rate allowed for that channel if the chosen data rate is not summorth.			er r				
Media Stream								

Once you have connected access points to the network, verify that 802.11ac is enabled on a capable AP.

Navigate to **Wireless > Access Points > Radios > 802.11a/n/ac**. Notice the dynamic channel assignment shown on the 802.11ac access point (Example: APfc99.473e.1d31). Keep in mind that the channel selection process is run by default every 10 minutes initially, so you may need to wait a few minutes for the channel selection to occur.

սիսիս					COMMINICE					Sa <u>v</u> e Configurati	on   <u>P</u> ing	
Wireless	802.11a/n/ac Radios	WINELES	is gecokin Mgi	AGEMENT 1	-Owwards	HELP EEEDS	HCK				t	intries 1 - 5 of 5
Access Points     All APs	Current Filter: None							[Change Filt	er] [Clear F	ilter]		
<ul> <li>Radios</li> <li>802.11a/n/ac</li> <li>802.11b/g/n</li> <li>Dual-Band Radios</li> </ul>	AP Name	Radio Slot#	Base Radio MAC	Sub Band	Admin Status	Operational Status	Channel	CleanAir Admin Status	CleanAir Oper Status	Radio Role	Power Level	Antenna
Global Configuration	AP6073.5c7e.e32e	1	34:a8:4e:70:4e:00		Enable	UP	(36,40) *	Enable	DOWN	N/A	1*	Internal
Advanced	AP6c20.560e.3909	1	34:a8:4e:bb:f0:10		Enable	UP	(40,36) *	NA	NA	N/A	1*	Internal
Mesh	APfc99.473e.1d31	1	20:3a:07:e5:50:10		Enable	UP	(36,40) *	Enable	DOWN	N/A	1*	Internal
RF Profiles	APfc99.473e.1d31	2	20:3a:07:e5:50:10		Enable	UP	(36,40,44,48) *	NA	NA	N/A	1 *	Internal
FlexConnect Groups	APe4d3.f11e.a748	1	24:01:c7:f6:ad:30		Enable	UP	165	Disable	DOWN	N/A	1	Internal
FlexConnect ACLs												
▶ 802.11a/n/ac												
▶ 802.11b/g/n	* alabel essianment											
▶ Media Stream												

# Tech Tip

i

The access point shown in the graphic above is Cisco 3602 Series with an 802.11ac Radio Module (AIR-RM3000AC). This access point has an internal 802.11a radio and with the addition of the 802.11ac Radio Module in the modular expansion slot, it effectively has two 5 GHz radios. Priority is given to the internal 802.11a radio if both radios need to transmit at the same point in time.



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 services block in the data center 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 points.

This section covers the Cisco 5760 Series Wireless LAN Controller operating in Cisco Unified Wireless Network (CUWN) mode. In this mode, both the Mobility Controller (MC) and Mobility Agent (MA) services are not separated and both remain on the WLC. Because the Cisco IOS-XE based 5760 controller is a different operating system from that of the Cisco AireOS controllers, the configuration of the AireOS controllers is covered separately. If you are deploying an AireOS WLC for on-site local-mode deployment, skip to Procedure 1 in the Configuring On-Site AireOS Wireless Controllers process in this guide.

If you are deploying remote access points using Cisco FlexConnect, proceed to the section called Configuring Remote-Site Wireless with Cisco FlexConnect in the guide.

This design guide supports Cisco 5760 Series WLC using the stacking cable to form a redundant WLC pair. This high availability design is similar to that of AP SSO where configuration synchronization and keep-alive monitoring occurs, but over a stacking cable as opposed to a dedicated redundancy port. Wireless LAN controller failure detection is sub-second allowing very quick access point recovery during the failure of the primary wireless LAN controller. Unlike HA SSO however, wireless client state information is not synchronized between the primary and secondary WLC. During a WLC failure, wireless clients are required to re-authenticate. Depending on the application in use and type of access being provided (guest vs EAP), this re-authentication may or may not be visible to the wireless client. For voice- and video-based applications, the disruption may be more noticeable.

August 2014 Series

## (Optional)

The shared services block is comprised of two Cisco 6500 Series Switches configured as a Virtual Switching System (VSS) supporting wireless LAN controller services for campus-based wireless access. Use this procedure to configure connectivity for Cisco 5760 series WLC within the VSS services block.

Complete this procedure if the VSS Services Block switches have not been configured as described previously in the AireOS wireless LAN controller section above.

**Step 1:** Within the Cisco Catalyst 6500 VSS services block, create the wireless VLANs for connectivity to the data, voice, and wireless LAN controller VLANs. The management VLAN can contain other Cisco appliances and does not have to be dedicated to the WLCs.

```
vlan 116
name WLAN_Data
exit
vlan 120
name WLAN_Voice
exit
vlan 275
name WLAN_Mgmt
exit
```

**Step 2:** Configure a switch 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
ip pim sparse-mode
no shutdown
T
interface Vlan120
description Wireless Voice Network
ip address 10.4.20.1 255.255.252.0
ip pim sparse-mode
no shutdown
T
interface Vlan275
description Wireless Management Network
ip address 10.4.175.1 255.255.255.0
ip pim sparse-mode
no shutdown
```

**Step 3:** Configure an 802.1Q trunk to be used for the connection to the 5760. This permits Layer 3 services for each of the networks defined on the WLC. The VLANs allowed on the trunk are limited to only the VLANs that are active on the WLC. The trunk is built using multiple Ethernet interfaces grouped into a logical PortChannel configuration for resiliency.

August 2014 Series

Tech Tip

i

If you are deploying a Cisco Catalyst 3750 Series LAN switch stack as a services block, you need to add the **switchport trunk encapsulation dot1q** command to the Port-channel configuration. Additionally, if you are using the 6500 with 1-Gigabit Ethernet ports, apply the EgressQoSOneGig macro instead of the EgressQoS macro. These macros are defined in the Campus Wired LAN Technology Design Guide.

```
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
  ! for 6500 with 1Gbps Ethernet, use:
  ! macro apply EgressQoSOneGig
  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 allowed vlan 116,120,275
 switchport mode trunk
logging event link-status
 no shutdown
```

Step 4: Repeat Step 3 for each of the 5760 series wireless LAN controllers in your environment.

#### Procedure 2 Use CLI to initially configure Cisco 5760 Series WLC

While the Cisco 5760 IOS-XE based Series Wireless LAN Controller has a startup wizard, it is easier to provide a startup configuration using the command line interface (CLI) when using LAG as configured in this CVD. Follow the procedure below to provide an initial configuration supporting high availability with LAG support.



**Step 1:** Ensure that the resilient/secondary Cisco 5760 Series WLC is powered on without a configuration and is connected to the primary 5760 by using the stacking cable.

```
Tech Tip
```

i

You can use only one console port (either RJ-45 or mini USB) for input at a time. Both are enabled for output but only one is enabled input with the USB mini-type B console taking precedence over the traditional RJ45 style console port. Note that the Cisco USB console driver must be installed on your PC if you are using the mini-USB console port.

To download the latest Cisco Windows USB Console Driver, go to the Cisco software download page at http://www.cisco.com/cisco/software/navigator.html, click Wireless > Wireless LAN Controller > Standalone Controllers > Cisco 5700 Series Wireless LAN Controllers > Cisco 5760 Wireless LAN Controller > USB Console Software, and then follow the download instructions.

**Step 2:** Erase the previous configuration by accessing either of the previously configured Cisco 5760 Series WLCs in the high availability pair. Access either of the console ports on the primary/active 5760 and enter the following commands.

```
Controller>enable

Controller#erase startup-config

Erasing the nvram filesystem will remove all configuration files! Continue?

[confirm] <ENTER>

[OK]

Erase of nvram: complete

Controller#reload

System configuration has been modified. Save? [yes/no]: no <ENTER>

Reload command is being issued on Active unit, this will reload the whole stack

Proceed with reload? [confirm] yes <ENTER>
```

**Step 3:** Once the Cisco 5760 Series WLC high availability pair has reloaded, exit from the System Configuration dialog box by entering No to the following prompt.

Would you like to enter the initial configuration dialog? [yes/no]: No

Step 4: Exit the autoinstall by entering yes at the following prompt and pressing return to get started.

Would you like to terminate autoinstall [yes]: **yes** Press RETURN to get started! Controller>

Step 5: Enter enable mode by entering enable and pressing Enter.

Controller> **enable** Controller#

Step 6: Enter configuration mode by entering configure terminal and pressing Enter.

Controller> configure terminal
Controller(config)#

August 2014 Series

**Step 7:** Set the time zone, NTP servers, and timestamps to be included in debug and logging messages by entering the following commands.

ntp server [ip address]
clock timezone [timezone] [offset] 0
service timestamps debug datetime msec
service timestamps log datetime msec

Step 8: Configure a host name for this controller pair by entering the following command.

hostname [hostname]

**Step 9**: Configure the enable secret, admin username, and the password encryption service by entering the following commands:

```
username admin password [password]
enable secret [password]
service password encryption
```

**Step 10:** Define the TACACS+ server and TACACS+ server groups. Also define the default login, exec, and accounting method lists.

```
tacacs server TACACS-SERVER-1
address ipv4 [IP Address]
key SecretKey
!
aaa group server tacacs+ TACACS-SERVERS
server name TACACS-SERVER-1
!
aaa authentication login default group TACACS-SERVERS local
aaa authorization exec default group TACACS-SERVERS local
aaa accounting exec default start-stop group TACACS-SERVERS
aaa authorization console
```

Step 11: Create the VLANs used for the data, voice, and management VLANs by entering the following.

```
vlan [data VLAN]
name WLAN-Data
vlan [voice VLAN]
name WLAN-Voice
vlan [management VLAN]
name WLAN-Mgmt
```

**Step 12:** Create the Switch Virtual Interface (SVI) for the wireless LAN management VLAN interface and configure the default gateway.

```
interface Vlan[management VLAN]
ip address [ip address] [mask]
ip helper-address [dhcp server IP address]
!
ip default-gateway [default router]
ip route 0.0.0.0 0.0.0.0 [default router]
```

Step 13: Create the SVI for the wireless LAN data VLAN interface.

interface Vlan[WLAN Data vlan]
ip address [ip address] [mask]
ip helper-address [dhcp server ip address]

Step 14: Create the SVI for the wireless LAN voice VLAN interface.

interface Vlan[WLAN Voice vlan]
ip address [ip address] [mask]
ip helper-address [dhcp server ip address]

Step 15: Configure EtherChannel member interfaces.

The following is an example of the initial Cisco 5760 configuration within the 6500 VSS-based services block.



This step describes configuring the member interfaces of the EtherChannel to redundantly connect to the two Cisco Catalyst 6500 Series VSS Switches.

```
interface range TenGigabitEthernet[port number] - [port number]
description [description for VSS Switch 1]
!
interface range TenGigabitEthernet[port number] - [port number]
description [description for VSS Switch 2]
!
interface range TenGigabitEthernet[port number] - [port number],
TenGigabitEthernet[port number] - [port number]
switchport
logging event link-status
logging event trunk-status
logging event bundle-status
channel-protocol lacp
channel-group [number] mode active
```

i	Tech Tip
Wher VSS- single of the The s syste pair w upstre are ac Ether port- Stanc	n using a Cisco 5760 Series WLC high availability pair that is connected to a based services block, it is possible to configure all 12 ports of the 5760 pair in a e EtherChannel with 8 ports forwarding and 4 serving as backup links. When one 8 primary ports fail, one of the hot-standby ports automatically becomes active. system (Services VSS switch or 5760 high availability pair) with the highest lacp m-priority determines which links are active. Configuring the 5760 high availability with a lacp system-priority lower than the default of 32768 and lower than its eam VSS switch, will cause the 5760 high availability pair to determine which links ctive and which are placed in hot standby mode. All port members in a LACP Channel bundle have a default lacp port-priority of 32768. Assigning a higher lacp priority to the backup ports will make them less desirable and place them in Hot fby status.
5	5760-WLC(config)#lacp system-priority 16384
5	5760-WLC(config)#interface TenGigabitEthernet [desired]
ł	packup port number]
5	5760-WLC(config-if)#lacp port-priority 6500

Step 16: Configure a trunk.

Configure an 802.1Q trunk that will be used to provide the voice, data, and management VLANs to the Cisco 5760 Series WLC. The following commands will be automatically applied to those physical interfaces that are members of the Port-Channel group created in the previous step.

```
interface port-channel [number]
description EtherChannel link to the Services 6500VSS pair
switchport mode trunk
switchport trunk allowed vlan [data VLAN],[voice VLAN],[management VLAN]
logging event link-status
logging event trunk-status
logging event bundle-status
no shutdown
```

**Step 17:** Create an access list. This provides added security to the management and control plane of the wireless LAN controller.

access-list [ACL number]permit [network management subnet]

**Step 18:** Enable Simple Network Management Protocol (SNMP) in order to allow the controller be managed by a Network Management System (NMS), and then configure SNMPv2c both for a read only and a read-write community string.

```
snmp-server community [read only community string] RO [access list]
snmp-server community [read write community string] RW [access list]
snmp-server location [location]
snmp-server contact [contact]
```

**Step 19:** Configure RADIUS settings that request RADIUS attribute 6 be included in authentication requests as well as miscellaneous timers.

```
aaa new-model
radius-server attribute 6 on-for-login-auth
radius-server dead-criteria time 10 tries 3
radius-server deadtime 3
```

**Step 20:** Configure device management protocols, default passwords, and access control to the vty lines used for CLI management access as defined in Step 17 above.

```
ip domain-name cisco.local
ip ssh version 2
line vty 0 15
transport input ssh
transport preferred none
access-class [access list] in
```

Step 21: Enable AAA authentication for the web GUI interface.

```
ip http authentication aaa login-authentication default
ip http authentication aaa exec-authorization default
```

Step 22: Enable dot1x authentication globally on the controller.

dot1x system-auth-control

The following is an example of the initial Cisco 5760 Series WLC configuration within the Cisco Catalyst 6500 Series VSS-based services block.

```
ntp server 10.4.48.17
clock timezone PST -8 0
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
ip domain-name cisco.local
ip ssh version 2
hostname 5760-WLC
enable secret clscol23
username admin password clscol23
vlan 116
name WLAN-Data
vlan 120
name WLAN-Voice
vlan 275
name WLAN-Mgmt
exit
interface Vlan116
 description WLAN-Data VLAN
 ip address 10.4.16.68 255.255.252.0
 ip helper-address 10.4.48.10
interface Vlan120
 description WLAN-Voice VLAN
```

```
ip address 10.4.20.68 255.255.252.0
 ip helper-address 10.4.48.10
interface Vlan275
 ip address 10.4.175.68 255.255.255.0
 ip helper-address 10.4.48.10
ip default-gateway 10.4.175.1
ip route 0.0.0.0 0.0.0.0 10.4.175.1
access-list 55 permit 10.4.48.0 0.0.0.255
snmp-server community cisco RO 55
snmp-server community cisco123 RW 55
snmp-server location My-Location
snmp-server contact My-NOC
1
aaa new-model
radius-server attribute 6 on-for-login-auth
radius-server dead-criteria time 10 tries 3
radius-server deadtime 3
T.
dot1x system-auth-control
tacacs server TACACS-SERVER-1
address ipv4 10.4.48.15
key SecretKey
aaa group server tacacs+ TACACS-SERVERS
server name TACACS-SERVER-1
T.
aaa authentication login default group TACACS-SERVERS local
aaa authorization exec default group TACACS-SERVERS local
aaa accounting exec default start-stop group TACACS-SERVERS
aaa authorization console
line vty 0 15
 transport input ssh
 transport preferred none
 access-class 55 in
L
ip http authentication aaa login-authentication default
ip http authentication aaa exec-authorization default
interface range TenGigabitEthernet1/0/1-2
description To Services 6500VSS-Switch-1
I.
interface range TenGigabitEthernet2/0/1-2
```

description To Services 6500VSS-Switch-2 interface range TenGigabitEthernet1/0/1-2, TenGigabitEthernet2/0/1-2 switchport logging event link-status logging event trunk-status logging event bundle-status channel-protocol lacp channel-group 1 mode active interface port-channel 1 description EtherChannel link to the Services 6500VSS pair switchport mode trunk switchport trunk allowed vlan 116,120,275 logging event link-status logging event trunk-status logging event bundle-status no shutdown

**Step 23:** Continue the configuration of the Cisco 5760 Series WLC by accessing the web GUI on the 5760 redundant pair via the following URL in one of the supported browsers (Example : https://**10.4.175.68**/wireless).

### https://[ip address of 5760]/wireless



## Procedure 3 Configure wireless user authentication on Cisco 5760 Series WLC

**Step 1:** Starting in this release of the CVD, the RADIUS authentication service is provided by the Cisco Identity Services Engine (ISE). The Cisco ACS server will solely be used for network administrative access to the WLC using TACACS+.

Table 11 - Cisco ISE configuration values

ISE server	IP address	Hostname	Shared secret
Primary	10.4.48.41	ISE-Server-1	SecretKey
Secondary	10.4.48.42	ISE-Server-2	SecretKey

**Step 2:** When accessing the WLC using a web browser using SSL, accept the WLC self-signed certificate. Depending on the browser in use, select the option that allows you to continue to the website using the certificate presented to the browser.

**Step 3:** Enter the Cisco Secure ACS based username and password. If Secure ACS is not available, the WLC will fall back to the locally defined userid and password that was created in Procedure 2, "Use CLI to initially configure Cisco 5760 Series WLC." (Example: admin/c1sco123).

Windows Security	×
The server 10.4.175.68 at priv_15_access requires a username and password.	
admin         •••••••         •••••••         Remember my credentials	
OK Canc	el

Next, define a new RADIUS server.

Step 4: Navigate to Configuration > Security > AAA > RADIUS > Servers, and then click New.

ahah									Save Configuration	Refresh	^
cisco Wireless Controller		🔬 Home	Monitor   🔻	Configuration   🔻	Administration	• Help					
Security	Radius Servers										
▼ AAA	New Remove						Sho	W Al		- 8	
<ul> <li>Method Lists</li> </ul>	Server Name	9	Address	Auth Port	Acct Port						
General	No data available										
Authentication											
Accounting											
Authorization											
<ul> <li>Server Groups</li> </ul>											
Radius											
Tacacs+											1
Ldap											
* RADIUS											
Servers											
Falback											
TACACS+ Servers											
LDAP Servers											
Users											
MAC Filtering											~
AB Doley											_

Step 5: Enter a name for the Cisco ISE server, the IP address, and the shared secret (SecretKey).

Step 6: In the Auth Port box, enter 1812, in the Acct Port box, enter 1813, and then click Apply.

Tech Tip

i

For consistency between this guide and other CVD guides, we have standardized on these well-known TCP ports for RADIUS authentication and accounting: 1812 and 1813. The Cisco Identity Services Engine supports both the older 1645/1646 ports and the newer standardized 1812/1813 ports by default.

cisco Wireless Controlle					Save Configuration	Refresh	^
cisco Wireless Controlle Security * AAA * Method Lists @ General @ Authentcation # Accounting @ Authentcation * Server Groups @ Radius # Tacacs+ @ Ldap * RADUS @ Servers @ Falback # TacACS+ Servers # DAP Servers	Anne     Anne     Anne     Anne     Anne     Anne     Server     Server     Name     Server     Ind.48.41     Shared Secret     Auth Port (0-65535)     IB13     Server     Timeout (1-1000)secs     Retry Count (0-100)     Support for RFC 3576     Enable •	I         I           I         I           I         I           I         I	Administration   •	Help		Apply	
Users MAC Filtering AAC Filtering AP Policy Local EAP Wreless Protection Policies CIDS ACL Web Auth							<

The preceding steps apply this configuration.

```
radius server [RADIUS Server Name]
address ipv4 [IP address] auth-port 1812 acct-port 1813
key [SecretKey]
```

**Step 7:** Repeat the steps above to define the redundant Cisco ISE RADIUS server using the values found in Table 11.

Step 8: Navigate to Configuration > Security > AAA > Server Groups > Radius, and then click New.

Step 9: Enter the Radius Group name. (Example: ISE-Group).

**Step 10:** In the **Available Servers** list, choose the Cisco ISE RADIUS servers just created, move them to the **Assigned Servers** list by clicking the right arrow, and then click **Apply**.

allalla						Save configuration   Refresh
CISCO Wireless Controller	🔂 Hom	e Monitor 🔻 Co	onfiguration   🔻	Administration   🔻	Help	
Security	Radius Server Group Radius Server Group > New					Apply
▼ AAA						
Method Lists		IEE Crown	7			
Server Groups	Name	13E-Group				
u Radius	MAC-delimiter	none 🔻				
Tacacs+	MAC-filtering	none 🔻	_			
🗉 Ldap	Dead-time (0-1440) in minutes					
▼ RADIUS	Group Type	radius				
Servers		Available Servers		Assigned 8	Servers	
Fallback				ISE-Server		
TACACS+ Servers	Servers In This Group			< >	-	
LDAP Servers						
Users						

The preceding steps apply this configuration.

```
aaa group server radius [Group Name]
server name [RADIUS Server Name]
!
```

Next, create a Method List for wireless user authentication.

Step 11: Navigate to Configuration > Security > AAA > Method Lists > Authentication, and then click New.

Step 12: Enter a Method List name. (Example: ISE-Authentication-Method-List)

**Step 13:** In the **Available Server Group** list, choose the Server Group, move it to the **Assigned Server Groups** list by clicking the right arrow, and then click **Apply**.

ahaha		Save Configuration   Refresh	~
cisco Wireless Controlle	🕫 🏠 Home Monitor   🔻 Configuration   🔻 Administration   👻 Help		
Security	Authentication Authentication > New	Apply	
AAA     Method Lists     General     Authentication     Accounting     Authentication     Server Groups     KADDUS     TADDUS	Wethod Litt Name     ISE-Authentication-Method-List       Type: <ul> <li></li></ul>		
LOAP Servers     Users     MAC Filtering     AP Policy     Local EAP     Wireless Protection Policies     CIDS	* Method List Name can be 'defaut' or any User defined Name.		
<ul> <li>ACL</li> <li>Web Auth</li> </ul>			~

The preceding steps apply this configuration.

```
aaa authentication dot1x [Method List Name] group [Group Name]
Next, create a Method List for wireless user accounting.
```

Step 14: Navigate to Configuration > Security > AAA > Method Lists > Accounting, and click New.

Step 15: Enter a Method List name. (Example: ISE-Accounting-Method-List)

**Step 16:** In the **Available Server Group** list, choose the Server Group, move it to the **Assigned Server Groups** list by clicking the right arrow, and then click **Apply**.

սիսիս		Save Configuration   Refresh
CISCO Wireless Controller	🟠 Home Monitor 🔻 Configuration 🔻 Administration 🔻 Help	
Security	Accounting Accounting > New	Apply
* AAA		
Method Lists     General	Method List Name         ISE-Accounting-Method-List           Type:              Ø dottx	
Authentication	Available Server Groups Assigned Server Groups	
Accounting	ISE-Group	
<ul> <li>Authorization</li> </ul>	Groups In This Method	
<ul> <li>Server Groups</li> </ul>		
RADIUS		
TACACS+ Servers	* Method List Name can be 'default' or any User defined Name.	

The preceding steps apply this configuration.

aaa accounting dot1x [Method List Name] start-stop group [Group Name]

#### Example

```
radius server ISE-Server-1
address ipv4 10.4.48.41 auth-port 1812 acct-port 1813
key SecretKey
!
aaa group server radius ISE-Group
server name ISE-Server-1
!
aaa authentication dot1x ISE-Authentication-Method-List group ISE-Group
aaa accounting dot1x ISE-Accounting-Method-List start-stop group ISE-Group
```

**Procedure 4** Configure management authentication on Cisco 5760 Series WLC

## (Optional)

Beginning with this CVD, Cisco Secure ACS will be used solely to provide authentication, authorization and accounting (AAA) services for controlling network management access. Secure ACS will not be used to provide security services for wireless users authenticating to the wireless network.

The following steps were completed as part of the initial CLI configuration in the preceding section. They are shown here to provide the necessary configuration guidance via the web interface.

Define a new TACACS+ server.

Step 1: Navigate to Configuration > Security > AAA > TACACS+ Servers, and then click New to define a new TACACS+ server.

**Step 2:** Enter a name for the ACS server (Example: TACACS-SERVER-1), the IP address (Example:10.4.48.15), and the shared secret (SecretKey), and then click **Apply**.

				Save Configuration   Refresh
cisco Wireless Controlle	🔝 Home Mo	nitor I 🔻 Configuration I 🔻	Administration 💌 Help	
Security	Tacacs Servers			Apply
▼ AAA				
▼ Method Lists	Server Name TACACS-SERV	/FR-1		
General	Censur Address 10.4.48.15			
<ul> <li>Authentication</li> </ul>	Shared Secret			
<ul> <li>Accounting</li> </ul>	Confirmed Shared Secret			
<ul> <li>Authorization</li> </ul>	Port 49			
▼ Server Groups	Server Timeout			
Radius				
Tacacs+				
🗉 Ldap				
▼ RADIUS				
Servers				
Falback				
TACACS+ Servers				

The preceding steps apply this configuration.

```
tacacs server [Server Name]
address ipv4 [IP address]
key [SecretKey]
```

Next, create a new TACACS+ Server Group that contains the ACS TACACS+ server defined in the preceding steps.

Step 3: Navigate to Configuration > Security > AAA > Server Groups > Tacacs+, and click New.

Step 4: Enter the Tacacs Server Group Name. (Example: TACACS-SERVERS)

**Step 5:** In the **Available Servers** list, choose the TACACS+ server that you just created, move it to the **Assigned Servers** list by clicking the right arrow, and then click **Apply**.

ahah		Save Configuration   Refresh
cisco Wireless Controlle	🖌 Home Monitor 🔍 Configuration 🔍 Administration 💌 Help	
Security	Tacacs Server Group Tacacs Server Group > New	Apply
▼ AAA		
<ul> <li>Method Lists</li> <li>General</li> </ul>	Name TACACS-SERVERS	
<ul> <li>Authentication</li> </ul>	Group Type tacads+ Available Servers Assigned Servers	
<ul> <li>Accounting</li> </ul>	▲ TACACS-SERVER-1 ▲	
Authorization	Servers In This Group	
▼ Server Groups		
Radius	ΨΨ	
Tacacs+		

The preceding steps apply this configuration.

aaa group server tacacs+ [TACACS Group Name]
server name [Server Name]

Next, create a default Method List for TACACS+ management access to the WLC.

Step 6: Navigate to Configuration > Security > AAA > Method Lists > Authentication, and then click New.

Step 7: Enter a Method List name (Example: default).

**Step 8:** Select the **login** as the Method List Type and **group** as the Group Type, and then select **Fallback to local**, which enables fallback to local authentication.

**Step 9:** In the **Available Server Groups** list, choose the ACS Server Group (Example: TACACS-SERVERS), move it to the **Assigned Server Groups** list by clicking the right arrow, and then click **Apply**.

de de			Save Configuration   Refresh
cisco Wireless Controll	er	🟡 Home Monitor 🖙 Configuration 💌 Administration 💌 Help	
Security	Authentication Authentication > New		Αρρίγ
▼ AAA			
<ul> <li>Method Lists</li> <li>General</li> </ul>	Method List Name	default	
General	Type:	O dot1x      login	
Authentication	Group Type:	● group ○ local	
<ul> <li>Accounting</li> </ul>	Fallback to local		
<ul> <li>Authorization</li> </ul>		Available Server Groups Assigned Server Groups	
▼ Server Groups	Groups In This Matho		
Radius	Groups in mismouris		
Tacacs+			
u Ldap	* Method List Name ca	an be 'default' or any User defined Name.	

The preceding steps apply this configuration.

aaa authentication login **default** group **[TACACS Group Name]** local Next, create a Method List for TACACS accounting.

Step 10: Navigate to Configuration > Security > AAA > Method Lists > Accounting, and then click New.

**Step 11:** Enter a Method List name (Example: ACS-Accounting-Method-List), and then select **exec**, which enables accounting start/stop records for exec commands issued to the controller.

**Step 12:** In the **Available Server Groups** list, choose the ACS TACACS Server Group, move it to the **Assigned Server Groups** list by clicking the right arrow, and then click **Apply**.

di di		Save Configuration   Refresh
cisco Wireless Controlle	er 🔬 Home Monitor 🛛 Configuration 🔽 Administration 💌 Help	
Security	Accounting	Apply
▼ AAA		
<ul> <li>Method Lists</li> <li>General</li> </ul>	Method List Name default Type: Odot1x: O evec O identity O network. O commands	
Authentication	Available Server Groups Assigned Server Groups	
L Accounting	ISE-Group  A TACACS-SERVERS	
Authorization	Groups In This Method	
▼ Server Groups		
Radius		
Tacacs+	* Method List Name can be 'default' or any User defined Name.	

The preceding steps apply this configuration.

aaa accounting exec default start-stop group [TACACS Group Name]

Next, create a Method List for TACACS authentication exec requests.

Step 13: Navigate to Configuration > Security > AAA > Method Lists > Authorization, and click New.

Step 14: Enter a Method List name. (Example: ACS-Authorization-Method-List)

Step 15: Select exec as the type and group as the Group Type.

**Step 16:** In the **Available Server Groups** list, choose the ACS TACACS Server Group, move it to the **Assigned Server Groups** list by clicking the right arrow, and then click **Apply**.

i Tech	л Тір							
In order for the web interface to function properly with TACACS+, the Method List Name must be called "default". Failure to define the default method list will cause authorization errors (WSMA) to occur on various screens within the web interface.								
dialia cisco Wireless Controll	er 🔗 Home Montor I y Configuration I y Administration I y Help							
Security	Authorization Authorization > New Apply							
<ul> <li>Average</li> <li>Method Lists</li> <li>General</li> <li>Authentication</li> <li>Accounting</li> <li>Authonization</li> <li>Server Groups</li> <li>Radus</li> <li>Tacas+</li> </ul>	Method List Name default Type: network @ exec O credential-download Group Type: @ group O coal Available Server Groups Assigned Server Groups Groups In This Method							
🗉 Ldap	* Method List Name can be 'default' or any User defined Name.							

In order to use the ACS/TACACS method lists just created for web GUI authentication, assign them as AAA method lists used for IP HTTP. This can only be done from the CLI.

Step 17: Access the CLI on the 5760 and enter the following commands.

ip http authentication aaa login-authorization default ip http authentication aaa exec-authorization default

#### Example

```
tacacs server TACACS-SERVER-1
address ipv4 10.4.48.15
key SecretKey
!
aaa group server tacacs+ TACACS-SERVERS
server name TACACS-SERVER-1
aaa authentication login default group TACACS-SERVERS local
aaa authorization exec default group TACACS-SERVERS local
aaa accounting exec default start-stop group TACACS-SERVERS
!
ip http authentication aaa login-authentication default
ip http authentication aaa exec-authorization default
```

#### Procedure 5 Configure wireless settings on the 5760

There are a number of wireless related management settings that need to be configured on the Cisco 5760 Series WLC in order to enable wireless support. This includes the default mobility domain, RF group name, which is used between wireless LAN controllers to share information about wireless clients and Radio Resource Management, respectively. It is recommended to use a different mobility group name when dedicated wireless LAN controllers are being used for each building. This best practice approach will eliminate un-needed client state information from being shared between controllers. Likewise, if buildings are physically separate from each other from an RF perspective, it is recommended to use different RF Group names to size of the data collected that is used during Radio Resource Management (RRM) calculations.

Fast SSID Change is recommended as it allows a wireless client to switch from one WLAN SSID to another on the same controller without delay. Finally, the wireless LAN controller needs to have a VLAN identified that will be used for wireless management.

Step 1: Navigate to Configuration > Controller > System > General.

Step 2: Select Fast SSID change, enter a Default Mobility Domain name (Example: Campus) and an RF group name (Example: CAMPUS), and then click Apply.

ahaha							Save Configuration   Refresh
cisco Wireless Controlle	er s	🏠 Home 🛛 Mon	orlv	Configuration	Administration 🛛 🔻	Help	
Controller	General						Apply
<ul> <li>System</li> </ul>							
General	Name	5760-WLC					
Multicast	AP Multicast Mode	Unicast 👻					
▼ Interfaces	Fast SSID change	$\checkmark$					
Port Summary	AP Fallback						
Wireless Interface	Default Mobility Domain	CAMPUS					
▼ VLAN	RF group name	CAMPUS					
I laver2 VI AN	User idle timeout	300					
<ul> <li>Layor2 Interface</li> </ul>	Temperature Value	32 Degree Celsi	s				
<ul> <li>Vian Group</li> </ul>	Temperature Status	GREEN					

The preceding steps apply this configuration.

wireless client fast-ssid-change
wireless mobility group name [Mobility Group Name]
wireless rf-network [RF Group Name]

Step 3: Navigate to Configuration > Controller > System > Interfaces > Wireless Interface, and then click the Unconfigured interface name.

cisco Wireless Controllo	er	☆ Home Monitor ▼	Configuration 🔻	Administration 🗐	Help	Save C	ionfiguration   Refresh
Controller	Wireless Interfa	се					
▼ System	New Remove				Sho	Al .	- 6
General	Interface Typ	e Interface Name	IP Address	IP Netmask	MAC Address	VlanID	
Multicast	Management	Unconfigured	169.254.1.1	255.255.255.0	0000:0000:0000	0	
Interfaces     Port Summary     Wireless Interface		( <sup>m</sup> ) Unconfi	gured				

**Step 4:** In the **Select Interface** list, choose the VLAN interface that will be used for wireless management (Example: VLAN 275), click **Apply**, and then click **Save Configuration**. The running configuration is saved.

ahah								Save Configuration   Refresh
cisco Wireless Controlle		er	A Home	Monitor   🔻	Configuration   •	Administration   🔻	Help	
Controlle	er	Management in	terface creation	on				Apply
* System	ı	Select Interface			Vlan1 v			
🗉 Ge	eneral	Serect Interface			Vlan1			
🔳 Mu	ulticast				Vlan275	ь <b>^</b>		
* Inter	rfaces				Te1/0/1 Te1/0/2	~		
	Port Summary				Te1/0/3	•		
•	Wireless Interface					•		

The preceding steps apply this configuration.

```
wireless management interface Vlan [VLAN Number]
```

# i Tech Tip

In order to manage the wireless LAN controller from a wireless client, enter the following using the CLI interface on the Cisco 5760 Series WLC:

```
wireless mgmt-via-wireless
```

The management over wireless feature allows you to configure and monitor the WLC using a wireless client. All management tasks, with the exception of uploading and downloading to/from the controller are supported.

## Example

```
wireless client fast-ssid-change
wireless mobility group name CAMPUS
wireless rf-network CAMPUS
!
wireless management interface Vlan275
```

## Procedure 6 Enable multicast support on 5760 WLC

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 CUWN based 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.

The various multicast streams can be delivered to the APs in one of two manners. The first is called *multicast-unicast*, and in this mode each multicast stream is converted to unicast and sent to the access points with wireless clients who have requested the multicast stream. If many users across many access points are requesting the same stream, the WLC must replicate each frame of the multicast stream, convert it into a unique unicast format and replicate it for each access point with an associated multicast subscriber. At large numbers of access points and subscribed multicast users, this becomes highly inefficient.

A more scalable method is to use Multicast-Multicast (MC-MC) mode. In MC-MC mode, the multicast stream is converted to a unique controller-to-AP multicast flow. The underlying campus infrastructure, which must be configured for multicast, will facilitate this MC-MC flow to reach each AP that has subscribed wireless users. The end result is a much more scalable and efficient method for handling multicast flows across the campus network.

OO Reader Tip	
Each redundant controller pair must use a unique multicast group address.	
239.0.0.239.255.255.255 excluding 239.0.0.X239.128.0.X. More information about multicast addressing can be found here:	
http://www.cisco.com/en/US/tech/tk828/technologies_white_ paper09186a00802d4643.shtml	

Step 1: Navigate to Configuration > Controller > System > General.

Step 2: In the AP Multicast Mode list, choose Multicast.

**Step 3:** In the **Multicast Group address** box, enter the IP multicast address that will be used to forward the multicast streams from this controller, and then click **Apply**. (Example: 239.68.68.68)

i	Tech Tip
The pair i addr wirel	multicast address must be unique for each controller or controller high availability n the network. The multicast address entered is used as the source multicast ess, which the access points registered to the controller will use for receiving ess user-based multicast streams.
սիսիս cisco W	ireless Controller 🔬 Home Monitor   🔻 Configuration   🔻 Administration   🔻 Help

cisco Wireless Controlle	er f	🏠 Home 🛛 Monitor   🔻	Configuration   🔻	Administration   🔻	Help	
Controller	General					Apply
▼ System						
General	Name	5760-WLC				
<ul> <li>Multicast</li> </ul>	AP Multicast Mode	Multicast 👻		Multicast Group address	239.68.68.68	]
<ul> <li>Interfaces</li> </ul>	Fast SSID change	✓			De .	
Port Summary	AP Fallback	✓				
Wireless Interface	Default Mobility Domain	CAMPUS				
▶ VLAN	RF group name	¢AMPUS	×			

The preceding steps apply this configuration.

ap capwap multicast [Multicast Group Address]

Step 4: Navigate to Configuration > Controller > System > Multicast, select Enable Global Multicast Mode. Click Apply, and then click Save Configuration

ahaha	Save Configuration   Refresh
cisco Wireless Controlle	🖍 Home Monitor   🔻 Configuration   👻 Administration   👻 Help
Controller	Multicast Apply
▼ System	
General	Enable Global Multicast Mode 🗹
u Multicast	Enable (SMP Snooping 🗹
<ul> <li>Interfaces</li> </ul>	
▶ VLAN	IGMP I meout (seconds)
Internal DHCP Server	
<ul> <li>Management</li> </ul>	
Mobility Management	
mDNS	

The preceding steps apply this configuration.

wireless multicast

#### Example

wireless multicast

ap capwap multicast 239.68.68.68

Procedure 7 Configure the 5760 voice wireless LAN

When compared to data traffic, voice traffic is not tolerant of delay, jitter, or packet loss. In some cases, multicast may be used in one-to-many push to talk types of applications, but mainly unicast is used as the primary method of communication.

This procedure creates a voice WLAN and applies the QoS settings necessary provide Platinum QoS service to these flows. For alignment to the Cisco AireOS controllers QoS mechanisms, this guide uses the *precious metal* based QoS policies as used within the AireOS controllers. The Cisco IOS-XE based controllers have inherited the modular QoS CLI (MQC) from Cisco IOS-routers and switches. MQC provides significantly more flexibility than precious metal based QoS. This guide uses the the precious metal QoS policies to align to the same precious metal QoS policies which are available in the AireOS based controllers.

Step 1: Navigate to Configuration > Wireless > WLANs, and then click New.

**Step 2:** Enter a WLAN ID (Example 2), the Wireless SSID (Example: WLAN-Voice), and a meaningful profile name (Example: Voice), and then click **Apply**.

սիսիս		Save Configuration   Refresh
cisco Wireless Controlle	🟠 Home Monitor 🔻 Configuration 💌 Administration 💌 Help	
Wireless	WLANs VILANs > Create New	
<ul> <li>WLAN</li> <li>Access Points</li> <li>802.11a/n/ac</li> <li>802.11b/g/n</li> <li>Media Stream</li> <li>QOS</li> </ul>	Apply           WLAN ID         2           SSID         WLAN-Voke           Profile Name         Vokel	

The preceding steps apply this configuration.

```
wlan [Profile Name] [WLAN ID] [SSID]
shutdown
```

Next, configure the specific parameters of the Voice WLAN.

Step 3: Click the profile name you just created.

ahaha						Save Configuration	Refresh
cisco Wireless Controlle	r 🏠 Home	Monitor 🛛 🔻	Configuration	▼ Help			
Wireless	WLANs						
WLAN	Mobility Anchor New Remove				Show A	I	- 76
<ul> <li>Access Points</li> </ul>	Profile	ID	SSID	VLAN	9	itatus	
▶ 802.11a/n/ac	Voice	2	WLAN-Voice	1	[	)isabled	
▶ 802.11b/g/n	< m						
Media Stream	Voice						
▶ QOS							

Step 4: On the General Tab for the Wireless Voice WLAN, from the menu, choose the WLAN-Voice interface.

Step 5: Select Multicast VLAN Feature then select Status , and then click Apply. This enables multicast and the WLAN.

ahaha		Save Configuration   Refresh
cisco Wireless Controll	er 🏠 Hom	e Monitor 🔻 Configuration 🔍 Administration 🔍 Help
Wireless WLAN	WLAN WLAN > Edit General Security	QOS AVC Advanced
<ul> <li>Access Points</li> <li>802.11a/n/ac</li> </ul>	Profile Name	Voice
▶ 802.11b/g/n	Туре	WLAN
<ul> <li>Media Stream</li> </ul>	SSID	WLAN-Voice
▶ QOS	Status	
	Security Policies	[WPA2][Auth(802.1x)] (Modifications done under security tab will appear after applying the changes.)
	Radio Policy	All
	Interface/Interface Group(G)	WLAN-Voice *
	Broadcast SSID	
	Multicast VLAN Feature	$\checkmark$
	Multicast Interface	default

**Step 6:** On the Security Tab, navigate to AAA Server, and then choose the RADIUS authentication and accounting method lists that you created in Procedure 3, and then click **Apply**.

ahah		Save Configuration   Refresh
cisco Wireless Controlle	🖍 Home Monitor 🔻 Configuration 🔻 Administration 🔻 Help	
Wireless	WLAN SERIE	Apply
<ul> <li>WLAN</li> <li>Access Delete</li> </ul>	General Security QOS AVC Advanced	
<ul> <li>B02.11a/n/ac</li> </ul>	Layer2 Layer3 AAA Server	
<ul> <li>802.11b/g/n</li> </ul>	Authentication Method ISE-Authentication-Method-List *	
<ul> <li>Media Stream</li> <li>QOS</li> </ul>	Accounting Method ISE-Accounting-Method-List  Local EAP Authentication	



**Step 7:** On the AVC tab, select **Application Visibility Enabled**, and then click **Apply**. Application Visibility and Control is enabled.

ahah	Save Configuration   Refr	esh
cisco Wireless Controll	ar 🕜 Home Monitor 🔻 Configuration 🔍 Administration 🔍 Help	
Wireless	WLAN Apply	
N 147 651	WLAN > Edit	
- WLAN	General Security QOS AVC Advanced	
<ul> <li>Access Points</li> </ul>		
<ul> <li>802.11a/n/ac</li> </ul>	Application Visibility	
▶ 802.11b/g/n	Application Visibility Enabled 🗹	
Media Stream	Upstream Profile Wireless-avc-basic	
▶ QOS	Downstream Profile Wireless-avc-basic	

**Step 8:** On the Advanced Tab, provide the IP address of the DHCP Server (Example: 10.4.48.10). Click **Apply**, and then click **Save Configuration** 

			Save Configuration   Refresh
cisco Wireless Controlle	🕫 🏠 Home Monitor 🔻 Configur	ation 🔻 Administration 🔻 Help	
Wireless WLAN Access Points	WLAN > Edit General Security QOS AVC	Advanced	Apply
<ul> <li>B02.11a/n/ac</li> <li>B02.11b/g/n</li> <li>Media Stream</li> <li>QOS</li> <li>QOS-Policy</li> </ul>	Allow AAA Override Coverage Hole Detection Session Timeout (secs) 1800 (0 = Session rever expres) Aixment IE Diagnostic Channel P2P Blocking Action Media Stream Multicast-direct Citent Exclusion Timeout Value(secs) 60 Max Allowed Client 0	DHCP           DHCP Server IP Address         10.4.48.10           DHCP Address Assignment required         □           DHCP Option 82         □           DHCP Option 82 Assignment required         □           DHCP Option 82 Assignment required         □           DHCP Option 82 Assid Mode         □           DHCP Option 82 Assid Mode         □           NAC         □           NAC State         □           DIf Channel Scanning Defer         □	
		Scan Defer Priority	

The preceding steps apply this configuration.

```
wlan [Profile Name] [WLAN ID] [SSID]
ip dhcp server [DHCP Server Address]
```

#### Example

```
wlan Voice 2 WLAN-Voice
accounting-list ISE-Accounting-Method-List
client vlan WLAN-Voice
ip flow monitor wireless-avc-basic input
ip flow monitor wireless-avc-basic output
security dot1x authentication-list ISE-Authentication-Method-List
session-timeout 1800
no shutdown
```

#### Procedure 8 Configure the 5760 data Wireless LAN

Providing separation to data and voice traffic remains a best practice and is essential in any good network design. This ensures proper treatment of the respective IP traffic regardless of the medium it is traversing. This procedure defines the data wireless LAN.

Step 1: Navigate to Configuration > Wireless > WLANs, and then click New.

**Step 2:** Enter a WLAN ID (Example: 1), the Wireless SSID (Example: WLAN-Data), and a meaningful profile name (Example: WLAN-Data), and then click **Apply**.

abab		Save Configuration   Refresh
cisco Wireless Controlle	🕫 🙆 Home Monitor 🔍 Configuration 💌 Administration 🔍 Help	
Wireless	WLANs WLANs Screate New	
WLAN		
<ul> <li>Access Points</li> </ul>	Apply	
▶ 802.11a/n/ac	WLAN ID 1	
▶ 802.11b/g/n	SSID WLAN-Data	
<ul> <li>Media Stream</li> </ul>	Profile Name WLAN-Data	
* QOS	B	
QOS-Policy		

The preceding steps apply this configuration.

wlan	[Profile	Name]	[WLAN	ID]	[SSID]
shut	down				

Next, configure the specific parameters of the Data WLAN.

Step 3: Click the profile name you just created.

ahaha					Sav	Save Configuration   Refresh	
cisco Wireless Controlle	r	🏡 Home 🛛 Monitor 🖡 🔻	Configuration 💌 Ac	Iministration 💌 Help			
Wireless	WLANs						
WLAN	Mobility Anchor New	v Remove			Show All	- 8	
<ul> <li>Access Points</li> </ul>	Profile	ID	SSID	VLAN	Status		
<ul> <li>802.11a/n/ac</li> </ul>	WLAN-Data	1	WLAN-Data	1	Disabled		
▶ 802.11b/g/n	Voice 🖄	2	WLAN-Voice	120	Enabled		
Media Stream	WEAR	I-Data					
▼ QOS							
QOS-Policy							

**Step 4:** On the General Tab for the Wireless Data WLAN, from the menu, choose the WLAN-Data interface, and then select both **Multicast VLAN Feature** and **Status**, then click **Apply**. This enables multicast and the WLAN.

ahaha			Save Configuration   Refresh
cisco Wireless Controlle	er 🏠 Horr	e Monitor 🔍 Configuration 🔍 Administration 🔍 Help	
Wireless	WLAN		Apply
WLAN	WLAN > Edit	006 AVC Advanced	
Access Points	General Goculty	200 Arc Auralian	
▶ 802.11a/n/ac	Profile Name	WLAN-Data	
▶ 802.11b/g/n	Туре	WLAN	
<ul> <li>Media Stream</li> </ul>	SSID	WLAN-Data	
▼ Q05	Status		
<ul> <li>QOS-Policy</li> </ul>	Security Policies	[WPA2][Auth(802.1x)] (Modifications done under security tab will appear after applying the changes.)	
	Radio Policy	All 💌	
	Interface/Interface Group(G)	WLAN-Data 💌	
	Broadcast SSID		
	Multicast VLAN Feature		
	Multicast Interface	default	

The preceding steps apply this configuration.

wlan	[Prof:	ile Name]	[WLAN	ID]	[SSID]
clie	ent vla	an <b>[VLAN</b>	Name]		
no s	shutdow	wn			
**Step 5:** On the Security Tab, navigate to AAA Server, select the RADIUS authentication and accounting method lists created in Procedure 3 then click **Apply**.

ahaha		Save Configuration   Refresh
cisco Wireless Controlle	🕫 🏠 Home Monitor 🔻 Configuration 🔻 Administration 🔻 Help	
Wireless	WLAN > Edit	Apply
<ul> <li>WLAN</li> <li>Amount Delimite</li> </ul>	General Security QOS AVC Advanced	
<ul> <li>B02.11a/n/ac</li> </ul>	Layer2 Layer3 AAA Server	
▶ 802.11b/g/n	Authentication Method ISE-Authentication-Method-List 💌	
<ul> <li>Media Stream</li> </ul>	Accounting Method ISE-Accounting-Method-List 💌	
<ul> <li>QOS</li> <li>QOS-Policy</li> </ul>	Local EAP Authentication	

The preceding steps apply this configuration.

```
wlan [Profile Name] [WLAN ID] [SSID]
accounting-list [RADIUS Accounting Method List Name]
security dot1x authentication-list [RADIUS Authentication Method List Name]
```

**Step 6:** On the AVC tab, select **Application Visibility Enabled** and then click **Apply**. This enables Application Visibility and Control.

ahaha	Save Configurat	ion   Refresh
cisco Wireless Controlle	er 🏠 Home Monitor 🔻 Configuration 🔻 Administration 🔻 Help	
Wireless	WLAN	Apply
WLAN	WLAN > Edit	
<ul> <li>Access Points</li> </ul>	deneral security QUS Avic Advanced	
▶ 802.11a/n/ac	Application Visibility	
▶ 802.11b/g/n	Application Visibility Enabled 🗹	
Media Stream	Upstream Profile wireless-avc-basic	
▼ QOS	Downstream Profile Wireless-avc-basic	
QOS-Policy		

The preceding steps apply this configuration.

```
wlan [Profile Name] [WLAN ID] [SSID]
ip flow monitor wireless-avc-basic input
ip flow monitor wireless-avc-basic output
```

**Step 7:** On the Advanced Tab, provide the IP address of the DHCP Server (Example: 10.4.48.10), and then click **Apply** followed by **Save Configuration**.

ale ale					Save Configuration   Refresh
cisco Wireless Controllo	er 🏠 Home Monit	orl <b>v</b> Con	figuration 💌 Administration 💌	Help	
Wireless • WLAN • Access Points • 802.11a/n/ac • 802.11b/g/n • Meda Stream • QOS	VLAN     Security     QOS       Allow AAA Overide     Ocoverage Hole Detection     Isso       Session Timeout (sacs)     18000     18000       (or – Session ever sopres)     Anonet IE     Isso       Diagnostic Channel     Disabled       Media Stream Multicast-direct     Isso       Cient Exclusion     Isso       Timeout Value(secs)     60       Max Allowed Client     0	AVC	Advanced DHCP DHCP Server IP Address DHCP Address DHCP Address DHCP Option 82 DHCP Option 82 DHCP Option 82 Rormat DHCP Option 82 Roll Mode NAC NAC NaC State	10.4.48.10 quired       None *   	La E
			Scan Defer Priority		

The preceding steps apply this configuration.

```
wlan [Profile Name] [WLAN ID] [SSID]
ip dhcp server [DHCP Server Address]
```

## Example

```
wlan WLAN-Data 1 WLAN-Data
accounting-list ISE-Accounting-Method-List
client vlan WLAN-Data
ip dhcp server 10.4.48.10
ip flow monitor wireless-avc-basic input
ip flow monitor wireless-avc-basic output
security dot1x authentication-list ISE-Authentication-Method-List
session-timeout 1800
no shutdown
```

## Procedure 9 Apply QoS on the Cisco 5760 Series Wireless LAN Controller

The Cisco IOS-XE Wireless LAN based controllers provide extremely flexible QoS policies that can be applied to the port, SSID or wireless client. This method of QoS is referred to as modular QoS CLI (MQC) and is not covered at this time in this guide. For information about using MQC on the Cisco 5760 WLC, see the *QoS Configuration Guide, Cisco IOS XE Release 3E (Catalyst 3850 Switches)*, here: http://www.cisco.com/en/US/docs/switches/lan/catalyst3850/software/release/3se/qos/configuration\_guide/b\_qos\_3se\_3850\_cg.html

To align with the QoS policies available on the Cisco AireOS based wireless LAN controllers, this guide describes implementing the precious metal QoS policies on the Cisco 5760 WLC. These policies are based on the 802.11e eight user priorities (UP), which are grouped into four distinct QoS levels:

- Platinum/Voice (User Priority 7 and 6)–Ensures a high quality of service for voice over wireless.
- Gold/Video (User Priority 5 and 4)–Supports high-quality video applications.
- Silver/Best Effort (User Priority 3 and 0)—Supports normal bandwidth for clients. This is the default setting.
- Bronze/Background (User Priority 2 and 1)-Provides the lowest bandwidth for guest services.

While the precious metal policies are available and hard coded on the Cisco IOS-XE series of Wireless LAN controllers such as the 5760, they cannot be configured from the web-based GUI. The hard coded names for each of the precious metal QoS policies are case sensitive and are shown in the following table.

WLAN usage	Downstream policy	Upstream policy
Voice	platinum	platinum-up
	gold	gold-up
Data	silver	silver-up
Guest	bronze	bronze-up

Table 12 -	QoS precious	metal to	WLAN	mapping
------------	--------------	----------	------	---------



The precious metal policies are hard coded and do not appear in any CLI show commands. Use caution when configuring them as they are all in lower case.

Step 1: On the Cisco 5760 Series WLC, enter enable mode by entering enable and pressing enter.

Controller> **enable** Controller#

Step 2: Enter configuration mode by entering configure terminal and pressing enter.

Controller> **configure terminal** Controller(config)#

Step 3: Apply the platinum QoS policy to the Voice Wireless LAN by entering the following.

wlan [Voice Profile Name] [Voice WLAN ID] [Voice SSID]
service-policy output platinum
service-policy input platinum-up

Step 4: Apply the silver QoS policy to the Data Wireless LAN by entering the following.

```
wlan [Data Profile Name] [Data WLAN ID] [Data SSID]
service-policy output silver
service-policy input silver-up
```

Step 5: Save the running configuration by entering the following.

copy running-config startup-config

**Step 6:** Verify that the service policies have been applied to the WLANs by entering the following command and noting the QoS service policy.

```
Controller(config)#show wlan all

QoS Service Policy - Input

Policy Name : silver-up

Policy State : Validation Pending

QoS Service Policy - Output

Policy Name : silver

Policy State : Validation Pending
```

## Tech Tip

i

The service policy will initially show as Validation Pending. This is because there have not yet been any wireless client associations to that WLAN and the verification is performed when the policy is implemented for the wireless client when they associate.

August 2014 Series

Step 7: Verify that the service policies have been allied to the WLANs by navigating to Configuration > Wireless > WLAN, clicking the WLAN, clicking the QoS tab, and then noting the service policy name.

alialia		Save Configuration   Refresh
cisco Wireless Controlle	ller 🙆 Home Monitor 🔻 Configuration 💌 Administration 💌 Help	
Wireless	WLAN > Edit	Apply
Access Points	General Security QOS AVC Advanced	
▶ 802.11a/n/ac	QoS SSID Policy	
802.11b/g/n	Existing Policy Assign Policy	
Media Stream	Downstream Policy silverSelect- *	
▼ QOS ■ OOS-Policy	Upstream Policy silver-upSelect *	
	QoS Client Policy	
	Existing Policy Assign Policy	
	Downstream Policy NoneSelect- *	
	Upstream Policy NoneSelect *	
	WMM	
	WMM Policy Allowed •	

#### **Example**

```
wlan WLAN-Data 1 WLAN-Data
  service-policy output silver
  service-policy input silver-up
!
wlan Voice 2 WLAN-Voice
  service-policy output platinum
  service-policy input platinum-up
```

Procedure 10 Enable Band Select and ClientLink 1.0 on Cisco 5760 Series WLC

This procedure describes how to enable Band Select and ClientLink 1.0 on the Cisco 5760 Series WLC.

		Caution
E	nabli	ng Band Select and Cisco ClientLink1.0 is disruptive to active wireless users.

**Step 1:** From the Cisco 5760 Series WLC console, verify that the default values for Band Select are in effect by entering the following command.

```
5760-WLC#sh wireless band-selectBand Select Probe Response: per WLAN enablingCycle Count: 2Cycle Threshold (millisec): 200Age Out Suppression (sec): 20Age Out Dual Band (sec): 60Client RSSI (dBm): -805760-WLC#
```

Step 2: On the Cisco 5760 Series WLC, verify the status of Band Select by entering the following command.

5760-WLC#show wlan id 1 | begin Band Band Select : Disabled Load Balancing : Disabled IP Source Guard : Disabled <SNIP> 5760-WLC#

Step 3: On the Cisco 5760 Series WLC, enter enable mode by entering enable and pressing enter.

Controller> **enable** Controller#

Ĭ

Step 4: Enter configuration mode by entering configure terminal and pressing enter.

```
Controller> configure terminal
Controller(config)#
```

**Step 5:** Enable Band Select on the Data WLAN by first disabling the WLAN, and then enabling band-select and re-enabling the WLAN.

```
wlan [Data Profile Name] [Data WLAN ID] [Data SSID]
shutdown
band-select
no shutdown
Tech Tip
```

By default, Legacy Client Link (Version 1.0) is disabled and version 2 and 3 are enabled
by default. Client Link version 2 is supported by generation 2 access points (1600,
2600, 3600) and version 3 is supported by the Cisco 3700 Series access point.

**Step 6:** If you are using Generation 1 access points and need to enable Cisco Client Link version 1.0., navigate to **Configuration > Wireless > 802.11b/g/n >Network >11n Parameters** and enable Client Link 1.0 by selecting the Client Link option, and then clicking **Apply**.

ahah			Save Configuration   Refresh
cisco Wireless Controlle	r 🏠 Home 🛛 Monitor 🗐 🔻	Configuration	
Wireless	802.11b/g/n Global Parameters		Apply
▶ WLAN			
Access Points	General	Data Rates	
B02.11a/n/ac     B02.11b/g/n     Wetwork     RRM     High Throughput (802.11n)     Media Parameters     W EDCA Parameters     W EDCA Parameters     W CleanAir	802.11b Network Status         V           802.11g Support         V           Bascon Period(millescs)         100           Short Preamble         V           Fragmentation Threshold(bytes)         2346           DTPC Support         V           11n Parameters         Cent Link           Ctx Location Measurement         C	1 Mbps mandatory + 2 Mbps mandatory + 5.5 Mbps mandatory + 6 Mbps supported + 9 Mbps supported + 11 Mbps mandatory + 12 Mbps supported + 18 Mbps supported +	
<ul> <li>Media Stream</li> <li>QOS</li> </ul>	Mode 🗆	24Mbps supported + 36Mpps supported + 48Mpps supported + 54Mpps supported +	

The preceding steps apply this configuration. ap dot11 24ghz beamforming



Step 7: If you are using Generation 1 access points and need to enable Cisco Client Link version 1.0., navigate to Configuration > Wireless > 802.11a/n/ac >Network >11n Parameters and enable Client Link (1.0) by selecting the Client Link (1.0) option, clicking Apply, and then clicking Save Configuration.

ahaha			Save Configuration   Refresh
cisco Wireless Controllei	🔂 Home 🛛 Monitor 🛛 🔻	Configuration	
Wireless	802.11a/n/ac Global Parameters		Apply
▶ WLAN			
<ul> <li>Access Points</li> </ul>	General	Data Rates	
<ul> <li>802.11a/r/ac</li> <li>Network</li> <li>RRM</li> <li>High Throughput (802.11n/ Media Parameters</li> <li>EDCA Parameters</li> <li>DFS (802.11h)</li> <li>Roaming Parameters</li> <li>CleanAr</li> <li>802.11b/g/n</li> <li>Network</li> </ul>	802.11a Network Status 2 Beacon Period(millecs) 100 Fragmentation Threshold(bytes) 2346 DTK: Support 2 802.11a Band Status Low Band Enabled High Band Enabled 11n Parameters Client Link 2	6 Mbps supported + 9 Mbps supported + 12 Mbps mandatory + 18 Mbps supported + 24 Mbps supported + 48 Mbps supported +	
<ul> <li>RRM</li> <li>High Throughput (802.11n)</li> </ul>	CCX Location Measurement		

The preceding steps apply this configuration.

```
ap dot11 5ghz beamforming
```

## Example

wlan WLAN-Data 1 WLAN-Data
shutdown
band-select
no shutdown
!
ap dot11 24ghz beamforming
ap dot11 5 GHz beamforming

# Procedure 11 Enable 802.11ac on the Cisco 5760 Series WLC

With the advent of 802.11ac, wave 1, 40 and 80MHz wide channels can be enabled. This can be accomplished manually on an AP by AP basis, or can be enabled globally by using Dynamic Channel Assignment (DCA). Due to the complexities of channel assignment, it is strongly recommended to allow the DCA process to select the best channels.



Step 1: Disable the 802.11a network by navigating to Configuration > Wireless > 802.11a/n/ac > Network, clearing the 802.11a Network Status check box, and then clicking Apply.

aludu				Save Configuration   Refresh
cisco Wireless Controller	🟡 Home 🛛 Monitor 🛛 🔻	Configuration	Administration 🛛 🔻	Help
Wireless	802.11a/n/ac Global Parameters			Apply
WLAN				
<ul> <li>Access Points</li> </ul>	General		Data Rates	
<ul> <li>Ø02.11a/n/ac</li> <li>Network</li> <li>RM</li> <li>General</li> <li>Coverage Thresholds</li> <li>DCA</li> <li>TPC</li> <li>RG Grouping</li> <li>High Throughput (802.11n/s)</li> <li>Media Parameters</li> <li>EDCA Parameters</li> <li>DCA Parameters</li> <li>DCA Parameters</li> <li>DCA Parameters</li> <li>DCA Parameters</li> </ul>	802.11a Network Status) Beacon Period(milises) Fragmentation Threshold(bytes) [2346 DTC Support © 802.11a Beats Low Band Enabled Migh Band Enabled High Band Enabled 11n Parameters Cirk Location Measurement Mode [		6 Mops mandatory 9 Mops supported # 12 Mops mandatory = 18 Mops supported # 24 Mops supported # 48 Mops supported # 48 Mops supported #	

Step 2: Navigate to Configuration > Wireless > 802.11a/n/ac > RRM > DCA and select the desired Channel Width to use (Example: 20 MHz, 40 MHz, 80 MHz).

Step 3: If it is available in your regulatory domain, select Extended UNII-2 Channels, and then click Apply.

alialia			Save Configuration   Refresh
cisco Wireless Controller	. 🏠 Home Monito	or 🔻 Configuration 💌 Administration 💌 Help	
Wireless	802.11a/n/ac > RRM > Dynamic C	hannel Assignment (DCA)	Apply
<ul> <li>WLAN</li> <li>Access Points</li> </ul>	Dynamic Channel Assignment Algo	rithm	
<ul> <li>* 802.113/n/ac</li> <li>Network</li> <li>* RRM</li> <li>General</li> <li>Coverage Thresholds</li> <li>DCA</li> <li>TPC</li> <li># RF Grouping</li> <li># Help Throughput (802.11n/s)</li> <li>Media Parameters</li> </ul>	Channel Assignment Method: Avoid Foreign AP Interference Avoid Cisco AP load Avoid Non 802. La Noise Avoid Persistent Non-will Interference Channel Assignment Leader DCA Channel Sensitivity Channel Width	Autonatic Interval 10 minutes      Anchortime 0	
<ul> <li>EDCA Parameters</li> <li>DFS (802.11h)</li> <li>Roaming Parameters</li> <li>CleanAr</li> <li>802.11b/g/n</li> <li>Moda Extramo</li> </ul>	DCA Channel List DCA Channels Select Channel	L≩ 100,104,108,112,116,132,136,140,1 49,153,157,161,36,40,44,48,52,56,6 0,64	
<ul> <li>read socialit</li> <li>▼QQS</li> <li>■ QQS-Policy</li> </ul>	Y         36           Y         40           Y         44           Y         48           Y         52           Y         56           G7         60           G7         61           Extended UNIL2 channels		

Step 4: Enable the 802.11a network by navigating to Configuration > Wireless > 802.11a/n/ac > Network, selecting 802.11a Network Status, clicking Apply, and then clicking Save Configuration.

			Save Configuration   Refresh
cisco Wireless Controller	🔝 Home Monitor 🔻	Configuration	
Wireless	802.11a/n/ac Global Parameters		Apply
▶ WLAN			
Access Points	General	Data Rates	
<ul> <li>B02.11a/n/ac</li> <li>Network</li> <li>RRM</li> <li>General</li> <li>Coverage Thresholds</li> <li>DCA</li> <li>TPC</li> <li>RF Grouping</li> <li>High Throughput (802.11n/i</li> <li>Meda Parameters</li> <li>EDCA Parameters</li> <li>EDCA Parameters</li> <li>DFS (802.11h)</li> <li>Raming Parameters</li> <li>Cleandir</li> </ul>	802.11a Network Status     Image: Constraint of the status       Beacon Period(millecs)     100       Fragmentation Threshold(bytes)     2346       DTPC Support     Image: Constraint of the status       B02.11a Band Status     Image: Constraint of the status       Low Band Enabled     Image: Constraint of the status       High Band Enabled     Image: Constraint of the status       Client Link II     Image: Constraint of the status       Mode     Image: Constraint of the status	6 Mbps mandatory = 9 Mbps supported = 12 Mps supported = 18 Mbps supported = 24 Mbps supported = 36 Mbps supported = 48 Mbps supported = 54 Mbps supported =	

i Tech Tip

The DCA process runs on a timed interval. For existing networks, forcing the DCA process to restart from a clean state is recommended. The DCA process can be manually restarted using the **ap dot11 5 GHz rrm dca restart** command. Note that shutting down the 5 GHz network does not clear the historical information that the DCA process has learned. Over time, however, the 802.11ac based channel selection process will converge, selecting channels and aligning the primary channels in mixed cell environments.

#### Example

```
! Disable the 5 GHz network
Т
ap dot11 5 GHz shutdown
!
!add the UNII-2 Channels
Т
ap dot11 5 GHz rrm channel dca add 100
ap dot11 5 GHz rrm channel dca add 104
ap dot11 5 GHz rrm channel dca add 108
ap dot11 5 GHz rrm channel dca add 112
ap dot11 5 GHz rrm channel dca add 116
ap dot11 5 GHz rrm channel dca add 132
ap dot11 5 GHz rrm channel dca add 136
ap dot11 5 GHz rrm channel dca add 140
!
! Enable channel width of 80 or optionally 40
1
ap dot11 5 GHz rrm channel dca chan-width 80
I.
! Configure supported and mandatory data rates
T
```

```
ap dot11 5 GHz rate RATE 6M mandatory
ap dot11 5 GHz rate RATE 9M supported
ap dot11 5 GHz rate RATE 12M mandatory
ap dot11 5 GHz rate RATE 18M supported
ap dot11 5 GHz rate RATE 24M mandatory
ap dot11 5 GHz rate RATE 36M supported
ap dot11 5 GHz rate RATE 48M supported
ap dot11 5 GHz rate RATE 54M supported
ap group default-group
!
! Enable the 5 GHz network
1
no ap dot11 5 GHz shutdown
end
! The following command is a global command
! and will restart the 5 GHz DCA process
ap dot11 5 GHz rrm dca restart
```

Procedure 12 Create the mobility peers on Cisco IOS-XE WLCs

# (Optional)

You need to complete this procedure if you have a Cisco IOS-XE 5760 based controller that is providing wireless guest services to your enterprise, and acting as a foreign anchor controller. As a foreign anchor controller, the first step is to create the mobility peers to the DMZ-based Internet edge anchor controllers. In this example, there are two 2504 guest anchor controllers located in the Internet edge and configured as new mobility controllers.

**Step 1:** Access the Cisco 5760 Series foreign anchor controller in the datacenter services block by using its SSL-based URL. (Example: https://10.4.175.68/wireless)

de de									Save Configuration	Refresh
cisco Wireless Co	ontroller		🔝 Home	Monitor   🔻	Configu	ration   •	Administration   🔻	Help		
System Summary							Top WLANs			
System Time	10:42:36.9	902 PST 1	Tue Feb 4 2014				Profile Name	Number of Clients		
Software Version	03.12.96.E NOVA_WE	ZP ENGI EKLY BU	NEERING				WLAN-Data	0		
System Name	5760-WLC						Voice	0		
System Model	AIR-CT576	50					5760Guest	0		
Up Time	5 days, 4 l	nours, 33	minutes							
Wireless Management IF	10.4.175.6	8					AVC for WLAN : WL	LAN-Data		
802.11 a/n/ac Network State	Disabled									
802.11 b/g/n Network State	Enabled									
Software Activation	Detail						No AVC data :	available for this wish		
Access Point Summa	ry						No Ave data t			
	Total	Up	Down							
802.11a/n/ac Radios	4	0	4							
802.11b/g/n Radios	4	4	0							
All APs	4	4	0							

Next, create a new mobility peer to the DMZ-based Cisco 2504 Series anchor controllers.

Step 2: Navigate to Configuration > Controller > Mobility Management > Mobility Peer, and then click New.

սիսիս									Save Configuration   Refresh
cisco Wireless Controll	er	🔬 Home	Monitor   🔻	Configurat	tion   🔻 🗛	dministration	▼ Help		
Controller	Mobility Peer								
<ul> <li>System</li> </ul>	New Remove							Show All	- 6
Internal DHCP Server	IP Address		Public IP Address		Group Name		Multicast IP	Control Link Stat	us Data Link Status
<ul> <li>Management</li> </ul>	10.4.175.68	N	-		5760CAMPUS		0.0.0.0	UP	UP
<ul> <li>Mobility Management</li> </ul>		4							
Mobility Global Config     Mobility Peer									
Switch Peer Group									

**Step 3:** In the **Mobility Member IP** box, enter the IP address of each of the 2504 DMZ-based anchor controllers. (Example 192.168.19.25).

**Step 4:** In the **Mobility Member Group Name** box, enter the mobility group name as defined on the DMZ based 2504 anchor controller (Example: 2504Guest), and then click **Apply**.

abab		Save Configuration   Refresh
cisco Wireless Controller	🟡 Home Monitor 🔻 Configuration 🔻 Administration 🔻 Help	
Controller	Mobility Peer Mobility Peer > New	Apply
Internal DHCP Server	Mobility Member IP 192.168.19.25	
<ul> <li>Management</li> <li>Mobility Management</li> </ul>	Mobility Member Public IP Mobility Member Public IP ZSV4Guest	
<ul> <li>Mobility Global Config</li> <li>Mobility Peer</li> </ul>	Multicast IP Address	
<ul> <li>Switch Peer Group</li> <li>mDNS</li> </ul>		

The preceding steps apply this configuration.

```
wireless mobility group member ip [IP Address of DMZ Anchor] public-ip [IP
Address of DMZ Anchor] group [DMZ Anchor Mobility Group Name]
```

Step 5: Repeat the previous steps for the second anchor controller. (Example:192.168.19.26)

Step 6: Navigate to Configuration > Controller > Mobility Management > Mobility Peer, 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. The negotiation process may take 30-90 seconds to complete, so press **Refresh** to see the current status.

ahah					Si	ve Configuration   Refresh
cisco Wireless Controlle	er	🟡 Home 🛛 Monitor   🗸	Configuration   +	dministration   👻 Help		
Controller	Mobility Peer					
<ul> <li>System</li> </ul>	New Remove				Show All	- 5
Internal DHCP Server	IP Address	Public IP Addres	ss Group Name	Multicast IP	Control Link Status	Data Link Status
Management	10.4.175.68		5760CAMPUS	0.0.0.0	UP	UP
<ul> <li>Mobility Management</li> </ul>	192.168.19.2	5 192.168.19.25	2504Guest		UP	UP
Mobility Global Config	192.168.19.2	6 192.168.19.26	2504Guest		UP	UP
Mobility Peer						
Switch Peer Group						
mDNS						



Make sure that the mobility group names match exactly between the controllers. If the Cisco 5760 Series WLC, for example, uses a Mobility Group name of 5760CAMPUS, make sure that the anchor controller has a peer pointing to the 5760 high availability pair using its exact Default Mobility Domain name. Conversely, the 5760 must also specify the Mobility Domain names of the anchor controllers located in the DMZ/ Internet edge.

## Example

wireless mobility group member ip 192.168.19.25 public-ip 192.168.19.25 group 2504Guest wireless mobility group member ip 192.168.19.26 public-ip 192.168.19.26 group 2504Guest

**Procedure 13** Configure the guest WLAN on IOS-XE controllers

**Step 1:** Access the SSL-based web Interface of the Cisco 5760 Series WLC foreign anchor controller by using your browser. (Example: https://10.4.175.68/wireless)

Next, create a guest wireless LAN.

Step 2: Navigate to Configuration > Wireless > WLAN, and then select New.

alada								Save Configuration   Refresh
cisco Wireless Controller	🏠 н	ome Monitor 🕅	Configuration	Administration 🛛 🔻	Help			
Wireless	WLANS							
WLAN	Mobility Anchor New Rem	nove					Show All	- 8
<ul> <li>Access Points</li> </ul>	Profile 🖤	ID	SSID		VLAN	Status		
* 802.11a/n/ac	WLAN-Data	1	WLAN-Data		116	Enabled		
Network	Voice	2	WLAN-Voice	2	120	Enabled		

Step 3: In the WLANs > Create New page, enter a unique WLAN ID (Example: 3), the Guest Wireless SSID (Example: 5760Guest), and the Profile Name (Example: 5760Guest), and then click Apply.

ahaha		Save Configuration   Refresh
cisco Wireless Controller	🟡 Home Monitor 🗵 Configuration 🔍 Administration 🔍 Help	
Wireless	WLANs WLANs Create New	
WLAN		
<ul> <li>Access Points</li> </ul>	[Apply]	
* 802.11a/n/ac	WLAN ID	
<ul> <li>Network</li> </ul>	SSID 5760Guilst	
► RRM	Profile Name 5760Guest	

The preceding steps apply this configuration.

wlan [Profile Name] [WLAN ID] [SSID]
shutdown

Step 4: Select the check box for the Guest WLAN, and then click Mobility Anchor.

aludu							Save Configuration   Refresh
cisco Wireless Controller		🏡 Home 🛛 Monitor 🔍	Configuration	Administration 🔻 Help			
Wireless	WLANs						
WLAN	Mobility Anchor	w Remove				Show Al	- 6
<ul> <li>Access Points</li> </ul>	Profile	ID	SSID	VLAN	Status		
* 802.11a/n/ac	WLAN-Data	1	WLAN-Data	116	Enabled		
Network	Voice	2	WLAN-Voice	120	Enabled		
► RRM	5760Guest	3	5760Guest	1	Disabled		



**Step 5:** In the **Switch IP Address** list, choose one of the Guest Anchor Controllers configured in the Internet DMZ, and then click **Create Mobility Anchor**.

alialia		Save Configuration   Refresh
cisco Wireless Controller	🛆 Home Monitor 🔻 Configuration 💌 Administration 💌 Help	
Wireless	Mobility Anchors wLAN > Edit	
Access Points	WLAN Profile 5760Guest	
* 8D2.11a/n/ac w Network	Switch IP Address 192.168.19.25 •	
<ul> <li>▶ RRM</li> <li>■ High Throughput (802.11n/ac)</li> </ul>	Remove Andrar Show Al	• 8
Media Parameters     EDCA Parameters	1P Address No data available	

**Step 6:** Click **OK**. This acknowledges that the action of creating an Anchor will temporarily disable the WLAN and may therefore be disruptive for wireless clients using this WLAN.

alialia		Save Configuration   Refresh
cisco Wireless Controller	🛆 Home Monitor 💌 Configuration 💌 Administration 💌 Help	
Wireless	Mobility Anchors WUNI > Edit	
<ul> <li>Access Points</li> <li>802.11a/n/ac</li> </ul>	WL If the WLAN is in Enabled state, adding Mobility Anchors will cause the WLAN to be momentarily disable and thus may result in loss of connectivity	
<ul> <li>Network</li> <li>RRM</li> </ul>	BW for some clients. Press OK to continue.	Channe [11
<ul> <li>High Throughput (802.11n/ac)</li> <li>Media Parameters</li> </ul>	Ke Cancel	on in the second se
EDCA Parameters	NO GALE ATRIBUE	

**Step 7:** If you have two anchor controllers in the DMZ, repeat Step 1 through Step 6 for the second guest anchor controller.

adaada		lave Configuration   Refresh
cisco Wireless Controller	🟡 Home Monitor 🔻 Configuration 💌 Administration 💌 Help	
Wireless	Mobility Anchors	
VLAN	17/2012 COIC	
Access Points		
* 802.11a/n/ac	WLAN Profile S760dulist	
Network	Switch IP Address None •	
► RRM	Create Mobility Anchor	
<ul> <li>High Throughput (802.11n/ac)</li> </ul>	Remove Andror Show All	- 6
Media Parameters	IP Address	
- FDCA December	192.168.19.25	
EUCA Parameters	92.166.19.26	

The preceding steps apply this configuration.

```
wlan [Profile Name] [WLAN ID] [SSID]
mobility anchor [IP Address of Guest Anchor 1]
mobility anchor [IP Address of Guest Anchor 2]
shutdown
```

**Step 8:** Navigate to **Configuration > Wireless > WLAN**, and click the Guest WLAN you created previously. (Example: 5760Guest)

ahaha									Save Configuration   Refresh
cisco Wireless Controller		🟡 Home	Monitor 🛛 💌	Configuration	Administration 🛛 🔻	Help			
Wireless	WLANS								
WLAN	Mobility Anchor N	ew Remove						Show AI	- 8
Access Points	Profile		ID	SSID		VLAN	Status		
* 802.11a/n/ac	WLAN-Data		1	WLAN-Data	1	116	Enabled		
<ul> <li>Network</li> </ul>	Voice		2	WLAN-Voic	0	120	Enabled		
► RRM	5760Guest		з	5760Guest		1	Disabled		
<ul> <li>High Throughput (802.11n/ac)</li> </ul>	576	OGuest							

Step 9: On the General tab, select Status. This enables the WLAN.

de de			Save Configuration   Refresh
cisco Wireless Controller	🏠 Ho	ne Monitor 🔻 Configuration 🔍 Administration 👻 Help	
Wireless	WLAN		Apply
VILAN	WLAN > Edit		
Access Points	General Security	UUS AVC Advanced	
* 802.11a/n/ac	Profile Name	5760Guest	
<ul> <li>Network</li> </ul>	Туре	WLAN	
► RRM	SSID	5760Guest	
<ul> <li>High Throughput (802.11n/ac)</li> </ul>	Status	. 🗹	
Media Parameters	Son with Daktion	[WPA2][Auth(802.1x)]	
EDCA Parameters	Secondy Policies	(Modifications done under security tab will appear after applying the changes.)	
DFS (802.11h)	Radio Policy	Al 💌	
Roaming Parameters	Interface/Interface Group(G)	default *	
u GeanAir	Broadcast SSID		
▼ 802.11b/g/n	Multicast VLAN Feature		
Network			

If using CLI access, the following CLI will enable the WLAN.

wlan [Profile Name] [WLAN ID] [SSID]
no shutdown

Step 10: Click the Security tab, and then, on the Layer 2 tab, in the Layer 2 Security list, choose None.



If using CLI access, the following CLI will disable the default Layer 2 security.

```
wlan [Profile Name] [WLAN ID] [SSID]
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
```

Step 11: On the Layer 3 tab, select Web Policy. This enables Web Authentication.

ababa	Sw	ve Configuration   Refresh
cisco Wireless Controller	🟡 Home Monitor 🔻 Configuration 🔻 Administration 🔻 Help	
Wireless	WLAN	Apply
WLAN	VILAN > Edit	
Access Points	deneral security QUS AVC Autranceu	
* 802.11a/n/ac	Layer2 Layer3 AAA Server	
Network	Web Policy	
▶ RRM	Conditional Web Redirect	
<ul> <li>High Throughput (802.11n/ac)</li> </ul>	Websuth Profile	
Media Parameters	Webauth Parameter Map Unconfigured *	
EDCA Parameters	Websuth On-mac-filter Falure	
DFS (802.11h)	Preauthentication IPv4 ACL Unconfigured *	
Roaming Parameters	Preauthentication IPv6 ACL Unconfigured +	

If using CLI access, the following CLI will enable Layer 3 Web authentication, also known as Web-Auth.

wlan [Profile Name] [WLAN ID] [SSID]
security web-auth

**Step 12:** Enable the built-in bronze precious metal QoS policies (as are currently used in AireOS controllers) for this WLAN by accessing the Cisco 5760 Series WLC SSO pair via CLI and entering the following in configuration mode.

```
wlan [Guest Profile Name] [Guest WLAN ID] [Guest SSID]
service-policy output bronze
service-policy input bronze-up
```

**Step 13:** Using the web interface for the Cisco 5760 Series foreign anchor controller, click the **AVC** tab (Application Visibility and Control), and then enable AVC by selecting **Application Visibility Enabled**.

Step 14: Click Apply, and then click Save Configuration.



If using CLI access, the following CLI will enable AVC

```
wlan [Profile Name] [WLAN ID] [SSID]
```

ip flow monitor wireless-avc-basic input

ip flow monitor wireless-avc-basic output

#### Example

```
wlan 5760Guest 3 5760Guest
ip flow monitor wireless-avc-basic input
ip flow monitor wireless-avc-basic output
mobility anchor 192.168.19.25
mobility anchor 192.168.19.26
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2
ciphers aes
security web-auth
service-policy output bronze
service-policy input bronze-up
session-timeout 1800
no shutdown
```



# Configuring Controller Discovery and Access Point Connectivity

- 1. Configure controller discovery
- 2. Connect the access points
- 3. Configure access points for resiliency using the Cisco 2500 Series WLC

For controllers operating in Cisco Unified Wireless Network (CUWN) mode, the discovery process is the same as described previously. This is true for both Cisco AireOS controllers and the Cisco 5760 Series WLC when it is not operating in Unified Access / New Mobility mode. This section describes the steps necessary to allow the access points to discover the wireless LAN controller.

# Procedure 1 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.



# 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: 10.4.175.64). 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.

August 2014 Series

# 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 sub option, as follows:

- *Type* is always the sub option 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 10.4.175.64 and 10.4.175.65. The type is 0xf1. The length is 2 \* 4 = 8 = 0x08. The IP addresses translate to 0a04af40 (10.4.175.64) and 0a04af41(10.4.175.65). When the string is assembled, it yields **f1080a04af400a04af41**.

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 f1080a04af400a04af41

# 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, 3600 and 3700 Series Access Points used in this design 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.

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
Cisco Aironet 3700 Series	Cisco AP c3700

Table 13 - Vendor class identifiers

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

August 2014 Series

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

9 DHCP			_ 8 ×
File Action View Help			
(= -> 2 📰 💥 🗈 0 🖻 🛛 📅			
2 DHCP	Name	Actions	
ad.cisco.local	IPv4	ad.cisco.local	A
Display Statistics	IPv6	More Actions	+
New Scope			
New Superscope			
New Malacast Scope			
Define User Classes Define Vendor Classes			
Reconcile All Scopes			
Cat Dardsford October			
Set Predenned Options			
Refresh			
Properties			
Help			
	1		
	1		
Define vendor specific option classes	1		

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

DI	HCP Vendor Classes		? ×
-	<u>A</u> vailable classes:		 
	Name	Description	Add
	Microsoft Windows 20 Microsoft Windows 98 Microsoft Options	Microsoft vendor-specific option Microsoft vendor-specific option Microsoft vendor-specific option	Edit
			Close

Step 4: In the New Class dialog box, enter a Display Name. (Example: Cisco Aironet 3700 AP)

**Step 5:** In the ASCII section, enter the vendor class identifier for the appropriate access point series from Table 13, and then click **OK**. (Example: Cisco AP c3700)

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

😲 DHCP			. 🗆 🗙
File Action View Help			
🗢 🔿 🖄 🛅 🗙 🗎	a 🗟 🚺		
2 DHCP	DHCP ¥endor C	lasses ?X	
ad.cisco.local	Available classe	1216 Data	-
E Scope [10.4.0			•
	C Cisco Aircrah	Description Aga	
	C Cisco Aironet	New Class ? X	
⊞ ≦ Scope [10.4.3	C Cisco Aironet	Disnlau name:	
🕀 🧮 Scope [10.4.4	c Cisco Aironet	Cisco Aironet 2700 AP	
🕀 🧮 Scope [10.4.5	C Lisco Aironet	CISCO Allohiet 3780 Al	
🕀 🗎 Scope [10.4.6	C Cisco Aironet	Description:	
⊞ 🚞 Scope [10.4.7	C Cisco Aironet	Cisco Aironet 3700 AP Series	
⊕ Scope [10.4.8	C Cisco Aironet		
⊞ Scope [10.4.9     □	C Cisco Aironet	ID: Binary: ASCII:	
E Scope [10.4.2]	р. 1	0000 43 69 73 63 6F 20 41 50 Cisco AP	
	7	0008 20 63 33 37 30 30	
	LOT VLAN 164 Data		
⊞	5.0] VLAN 165 Voice		
	-		
J			
		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 created in Step 4, and then click Add.

Predefined Options and Values					
Optio <u>n</u> class: Opti <u>o</u> n name:	Cisco Aironet 3700 AP				
Description:	Add Edit Delete				
- Value	Edit A <u>r</u> ray				
	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 3700 AP					
Name:	Option 43					
Data type:	IP Address 🔽 🔽 Array					
Code:	241					
Description:		ſ				
	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 be installing Access Points on, right-click **Scope Options**, and then click **Configure Options**.

Step 14: Click the Advanced tab, and in the Vendor class dropdown 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: 10.4.175.64)

Scope Options	? ×
General Advanced	
⊻endor class:	Cisco Aironet 3700 AP
<u>U</u> ser class:	Default User Class
Available Options	Description
✓ 241 Option 43	
d Data entry	<b>_</b>
<u>S</u> erver name:	
	R <u>e</u> solve
I <u>P</u> address:	
10 . 4 . 175 . 64	Add
	Remove
	Down
	OK Cancel Apply

**Step 17:** If you are using the Cisco 2500 Series WLC, repeat Step 16 for the non HA SSO capable resilient controller, and then click **Apply**. (Example: 10.4.175.65)

## Procedure 2 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 216
  switchport voice vlan 217
  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 3 Configure access points for resiliency using the Cisco 2500 Series WLC

When access points connecting to a WLC not using SSO, it is necessary to configure the access points with the IP addresses of each of the non SSO controllers. This is because they appear as two separate wireless LAN controllers and do not appear as a single HA controller pair. If you are installing access points that will connect to a pair of WLC's using HA SSO, please skip this procedure. On the primary controller, navigate to **Wireless**, and then select the desired access point.

Step 1: Click the High Availability tab.

**Step 2:** In the **Primary Controller** box, enter the name and management IP address of the primary controller. (Example: WLC-1 / 10.4.175.64)

**Step 3:** In the **Secondary Controller** box, enter the name and management IP address of the resilient controller, and then click **Apply**. (Example: WLC-2 / 10.4.175.65)

uluilu cisco	MONITOR WLANS CO	NTROLLER WIRELESS	SECURITY MANAGEMENT	COMMANDS HELP	Sa <u>v</u> e Configuration   Ping <u>F</u> EEDBACK	Logout <u>R</u> efresh
Wireless	All APs > Details for A	AP4403.a7a2.fe2c			< Back	Apply
Access Points     All APs     Radios	General Credentia	Is Interfaces H	ligh Availability Inventor	y Advanced		
802.11a/n/ac 802.11b/g/n Dual-Band Radios Global Configuration	Primary Controller [ Secondary Controller [	Name WLC-2504-1 WLC-2504-2	Management IP Addres 10.4.175.64 10.4.175.65	ss		
<ul> <li>Advanced</li> <li>Mesh</li> <li>RF Profiles</li> </ul>	Tertiary Controller					
FlexConnect Groups FlexConnect ACLs	AP Failover Priority	Low				

Step 4: Click Save Configuration.



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 HA SSO, when you have a large number of access points or remote sites. Alternately, for smaller deployments, the use of a Cisco 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 head-end don't have the necessary capacity or the WAN head-end is not co-located with a campus.

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

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

Parameter	CVD values primary controller	CVD values resilient controller if not using HA SSO	Site-specific values
Controller parameters	1		·
Switch interface number	1/0/3, 2/0/3	1/0/4, 2/0/4	
VLAN number	159	159	
Time zone	PST -8 0	PST -8 0	
IP address Flex 7500	10.4.59.68/24	10.4.59.69/24	
Default gateway Flex 7500 & vWLC	10.4.59.1	10.4.59.1	
Redundant management IP address (HA SSO) <sup>1</sup>	10.4.59.168	10.4.59.169	
Redundancy port connec- tivity (HA SSO) <sup>1</sup>	Dedicated Ethernet cable <sup>1</sup> Layer 2 network <sup>2</sup>	Dedicated Ethernet cable <sup>1</sup> Layer 2 network <sup>2</sup>	
Hostname Flex 7500	WLC-RemoteSites-1	WLC-RemoteSites-2	
IP address vWLC	10.4.59.58	10.4.59.59	
Hostname vWLC	vWLC_7_6_110_0- Server1	vWLC_7_6_110_0- Server2	
vWLC Virtual Console Port Telnet Port	7601	7602	
Local administrator username and password	admin/C1sco123	admin/C1sco123	
Mobility group name Flex 7500	REMOTES	REMOTES	
Mobility group name vWLC	REMOTES-vWLC	REMOTES-vWLC	
Primary Cisco ISE RADIUS server IP address	10.4.48.41	10.4.48.41	
Secondary Cisco ISE RADIUS server IP address	10.4.48.42	10.4.48.42	
Network RADIUS shared key	SecretKey	SecretKey	
Management network	10.4.48.0/24	10.4.48.0/24	
ACS TACACS server IP address	10.4.48.15	10.4.48.15	
TACACS shared key	SecretKey	SecretKey	
Voice VLAN default gateway	10.5.43.1	10.5.43.1	

<u> </u>	~ .					
Table $11 -$	Cisco	remote-site	wireless	controller	narameters	checklist
	01000		vn cicoo	Controller	parameters	CIICCRIDE

Table 14 (continued) - Cisco remote-site wireless controller parameters checklist

Parameter	CVD values primary controller	CVD values resilient controller if not using HA SSO	Site-specific values
Remote site parameters	6		
Wireless data SSID	WLAN-Data	WLAN-Data	
Wireless data VLAN number	65	65	
Data VLAN default gateway	10.5.42.1	10.5.42.1	
Wireless voice SSID	WLAN-Voice	WLAN-Voice	
Wireless voice VLAN number	70	70	
Voice VLAN default gateway	10.5.43.1	10.5.43.1	

Notes:

- 1. HA SSO is only supported on the Cisco 5500, WiSM2, 7500 Series WLC.
- 2. HA SSO over Layer 2 network support is supported on Cisco 5500, WiSM2, and 7500 Series WLC provided the redundancy port round-trip time is less than 80 milliseconds

# Procedure 1 Install the Cisco vWLC for FlexConnect designs

The Cisco 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.



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."

August 2014 Series

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

- On vSwitch0 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 vSwitch1, 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.

🕢 vCenter.cisco.local - vSphere Clier	nt				83
File Edit View Inventory Admin	nistration Plug-ins Help				
🖸 🔯 🟠 Home 🕨 🛃 Inve	entory 🕨 🕅 Hosts and Clusters	eg - Sea	rch Inventory		٩
File Edit View Inventory Adms	Hardwork Help Internet P ● ● Host and Custers duals at a kickoload Weiward EdX instruction and Common A the Hardware Heroware Stronge Adapters Advanced Settings Advanced Settings Herowith Adapters Advanced Settings Time Configuration CMS and Routing Advanced Settings Time Configuration CMS and Routing Routing Settings From Management With Michael Settings Power Management Settings Time Configuration CMS and Routing Seting Sett	Solo, 1499271 Statistics Resource Mocation Reformance Confuration Traits is Events Aurent Removar Reformance Confuration Reformation Reformatio Reformation Reformation Reformation Refor	ch inventory (Storage www.), Hardware Refech: Add Helworking	*Status	<b>Q</b>
	Virtual Machine Swapfle Locati Security Profile Host Cache Configuration System Resource Alocation Agent: VM Settings Advanced Settings	Vitiani 1004.6136 (VLMID: 151 Vitiani Romanni Vetwork vitiko : 104.6336 (VLMID: 153 Standard Swicht vSwicht 1 Remove Properties Vitiani Remini Voi Capp Presci Adapter			

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

Step 2: In vCenter, select the physical machine, click File, and then click Deploy OVF Template.

🕢 vCenter.cisco.local - vSphere (	lient		- D 🔀
File Edit View Inventory Ac	ministration Plug-ins Help		
New	• htory • [1] Hosts and Clusters		All - Search Inventory Q
Deploy OVF Template			
Export	•		
Report	has1-s1.cisco.local VMware E	SXi, 5.0.0, 1489271	
Browse VA Marketplace	Getting Started Summary V	intual Machines Resource Alocation Performance Configuration Tasks & Events Alarms	Permissions Maps Storage Views Hardware Status
Print Maps	Hardware	View: vSphere Standard Switch vSphere Distributed Switch	
Exit	Processors	Networking	Refresh Add Networking Properties
I chas2-s1.cisco.loca	Memory		
Chas2-s8.cisco.loca	Storage	Standard Switch: vSwitch0 Remove Properties	
chas3-s2.cisco.loca	Networking	Virtual Machine Port Group Physical Adapters	
⊞ 📁 UC	Storage Adapters	VWLC Data Port	
	Network Adapters	VLAN ID: All (4095)	

Step 3: Complete the Deploy OVF Template wizard. Note the following:

- On the Source page, select the downloaded Cisco 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)

💋 Deploy OVF Template	
Name and Location Specify a name and loca	ition 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:         Image: State

Step 4: On the Storage page, select the storage destination of the virtual machine.

🕝 Deploy OVF Template					
<b>Storage</b> Where do you want to stor	e the virtual machine files	7			
Source OVF Template Details Name and Location	Select a destination stor- VM Storage Profile:	age for the virtu	ual machine files:		
Storage	Name	Drive Type	Capacity Provisioned	Free Type	Thin Provisioning
Disk Format	👔 chas1-s1-local	Non-SSD	1.09 TB 2.86 TB	151.70 GB VMFS5	Supported
Ready to Complete	👔 Lab Filer	Unknown	14.32 TB 327.75 GB	14.00 TB NFS	Supported
rioddy to complete	Openfiler(Soft	Unknown	9.09 TB 5.90 TB	3.19 TB NF5	Supported
	Disable Storage DR     Select a datastore:	S for this virtual	III I machine		•
	Name	Drive Type	Capacity Provisioned	Free Type	Thin Provisioning
			m	and I wa	,
ūsib				<u>SBack</u> Next	≥ <u>Cancel</u>

Step 5: On the Disk Format page, select Thick Provision Lazy Zeroed.

🕝 Deploy OVF Template				
<b>Disk Format</b> In which format do you wa	ant to store the virtual disks?			
Source OVF Template Details Name and Location Storage Disk Format Network Mapping Ready to Complete	Datastore: Available space (GB): Thick Provision Lazy Zer Thick Provision Eager Ze Thin Provision	chas1-s1-local 151.7 roed eroed		
Help			≤Back Next ≥	Cancel

**Step 6:** 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: vWLC Data Port)

🕝 Deploy OVF Template			- • •
Network Mapping What networks sh	ould the deployed template use?		
Source OVE-Template Details Name and Location Bisk Format Network Mapping Ready to Complete	Map the networks used in this Source Networks VM Network Description: The VM Network	OVF template to networks in your inventory           Destination Networks           WWLC Data Port           FW_OUtside VL153           Servers_1           Servers_2           WWLC Data Port	
Help		< Back	vext > Cancel

letwork Mapping What networks should	the deployed template use?		
ource WF Template Details ame and Location	Map the networks used in this OVF	template to networks in your inventory	
torage	Source Networks	Destination Networks	
<u>isk Format</u>	VM Network	Servers_1	•
etwork Mapping		FW_Outside_VL153	
eady to Complete		Servers_1	
		Servers_2	10
		WILC Data Fort	
		IVWLS Service Port	

**Step 7:** On the Ready to Complete page, review the settings, and then click **Finish**. Deployment of the OVA file begins, and it may take a few minutes to complete.

🖉 Deploy OVF Template	:			- • •
Ready to Complete				
Are these the opti	ions you want to use?			
Source OVF Template Details	When you click Finish, the depk	oyment task will be started.		
Name and Location Storage	Deployment settings:			
Disk Format	OVF file:	C:\Downloads\AIR-CTVM-7-6-120-0.ova		
Network Mapping	Download size:	177.9 MB		
Ready to complete	Size on disk:	8.2 GB		
	Name:	VWLC-1		
	Folder:	10k		
	Host/Cluster:	chasi-si.cisco.iocai		
	Datastore:	Chast-strocal Thick Provision Latv Zaroad		
	Network Manoing	"VM Network" to "v/M/ C Data Port"		
	network mapping.	Windowork to Wate Data For		
	Power on after deployment			
			1	1
Help			< Back Finish	Cancel
				1.

# Procedure 2 Configure the console port on the vWLC

When the Cisco 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 Cisco vWLC (Example: vWLC-1), click **Edit virtual machine settings**, and then in the Virtual Machine Properties dialog box, click **Add**.

🖉 vCenter.cisco.local - vSphere Client		
Eile Edit View Inventory Administration Plug-in	s <u>H</u> elp	
🖸 🔯 🔥 Home 🕨 🏭 Inventory 🕨 🎁 Ha	osts and Clusters	🛃 - Search Inventory 🔍
🔳 II 🕨 🕲 🖄 🕼 📴 😽	• 🏇 🦫	
Control cock.bcal     Control cock.bcal	Witcl     Geting Stand     Sumps)     Resource Addation     Re       Geting Stand     Sumps)     Resource Addation     Re       What is a Virtual Machine ?     A virtual machine is a software compare this projection in galaction and the software compared the soft	Vital Radrie Verson 7

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

• On the Device Type page, select Serial Port.

🕜 Add Hardware		<b>—</b> ×
<b>Device Type</b> What sort of device do yo	ou wish to add to your virtual machine?	
Device Type Select Port Type Select Output File Ready to Complete	Choose the type of device you wish to add.	ine.
Help	_≤Back Next ≥	Cancel //

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

🖉 Add Hardware		×
Serial Port Type What media should this vi	rtual serial port access?	
Device Type Select Port Type Select Network Backing Ready to Complete	Select the type of media you would like the virtual serial port to access.  Serial Port Output  Use physical serial port on the host  Output to file  Connect to named pipe  Connect via Network	
Help	< Back Next >	Cancel

 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://10.4.63.96:7601) This configures IP address and TCP port number that are used access the console port via Telnet.

🕝 Add Hardware		×
Network Serial Port Setting How should this serial port	gs connect via network?	
Device Type Select Port Type Select Network Backing Ready to Complete	Network Backing         Server (VM listens for connection)         Client (VM initiates connection)         Port URI:         telnet://10.4.63.96:7601         Use Virtual Serial Port Concentrator         vSPC URI:         Device Status         Image: Connect at power on         I/O Mode         Image: Yield CPU on poll         Allow the guest operating system to use this serial port in polled mode rather than in interrupt mode.	
Help	<u>≤</u> 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.

🕜 vWLC-1 - Virtual Machine Proper	ties	
Hardware Options Resources Pro	files VServices	Virtual Machine Version: 7
	Add Remove	Device Status
Hardware	Summary	Connect at power on
Memory	2048 MB	Connection
🔲 CPUs	1	Connection
📃 📃 Video card	Video card	Use physical serial port:
🔲 📟 VMCI device	Restricted	/dev/char/serial/uart0 📃
SCSI controller 0	LSI Logic Parallel	C Use output file:
😑 Hard disk 1	Virtual Disk	Parmar 1
CD/DVD drive 1	[chas1-s1-local] vWLC-1/_device	Browse,
Network adapter 1	Servers_1	O Use named pipe:
Network adapter 2	Servers_1	Dine Name
Floppy drive 1	Floppy 1	Pipe Name:
New Serial Port (adding)	telnet://10.4.63.96:7601	Near End:
	43	Far End: A virtual machine
		<ul> <li>Use network</li> </ul>
		<ul> <li>Server (VM listens for connection)</li> </ul>
		C Client (VM initiates connection)
		Port URI: telnet://10.4.63.96:7601
		Use Virtual Serial Port Concentrator
		vSPC URI:
		I/O Mode
		Vield CPU on poll
Help		OK Cancel
		//

# **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 vWLC Service Port.

Step 2: Select Network adapter 2, and in the Network label list, choose vWLC Data Port, and then click OK.

🖉 vWLC-1 - Virtual Machine Properti	es	
Hardware Options Resources Profil	es VServices	Virtual Machine Version: 7
	Add Remove	Device Status
Hardware Memory CPUs Wideo card WMCI device SCSI controller 0 Hard disk 1 CD/DVD drive 1 Network adapter 1 (edite Rioppy drive 1 Serial port 1	Add     Reinitive       Summary     2048 MB       1     Video card       Restricted     LSI Logic Parallel       Virtual Disk     [chas1-s1-loca] vWLC       vWLC Service Port     vWLC Data Port       Floppy 1     telnet://10.4.63.96:7601	Connected  Connect at power on  Adapter Type Current adapter: E1000  MAC Address 00:50:56:a2:78:82  Automatic  Automatic  DirectPath I/O Status: Not supported  Network Connection Network Ubel:  VULC Data Nort  FW_Outside_V0153 Servers_1 Servers_1 Servers_2 VULC Data Port VWLC Service Port
		OK Cancel

**Step 3:** In the left column, start the virtual wireless LAN controller for the first time by selecting the virtual machine you just installed, and then clicking 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." However, you do not need to press any key because access via the serial port that was created in Procedure 2 will be used.

Ø vCenter.cisco.local - vSphere Client	
Elle Edit View Igventory Administration Plug-ins Help	
💽 🔯 Atome D 🚓 Inventory D 👹 Hosts and Clusters	🛃 - Search Inventory
Center.disco.local vWLC-1	
10k     Getting Started Summary Resource Allocation Performance Tasks & Events Alarms Console Permissione Ma	os Storate Views
Cher Services	
chast-st.cisco.local	
10K-vwaas-cm-s-1	
FW_Outside_Server_1	
A ISE-1	
15E-AdvGuest-10.4.48.46	
BE-MAVGUES-2	
Blade Doctored in Section 2017 Press and key to use this terminal as the default termi	nal.
Press any key to use this terminal as the default termi	nal.
Sevone Press any key to use this terminal as the default termi	nal.
MMSE-7-4-100-FCS-Do-Not-Use Press any key to use this terminal as the default termi	nal.
MSE-7-5-102-FCS Press any key to use this terminal as the default termi	nal.
wulc_7_6_95_7-Server1 Press any key to use this terminal as the default termi	nal.
www.c_7.6.95,7.5erver2 Press any key to use this terminal as the default termi	nal.
wulc-1 Press any key to use this terminal as the default termi	nal.
WebServer-1 Press any key to use this terminal as the default termi	nal.
Webserver-2 Press any key to use this terminal as the default terminal	nal.
Press any key to use this terminal as the default termi	nal
Press any key to use this terminal as the default termi	nal
Press any key to use this terminal as the default termi	nal.
Press any key to use this terminal as the default termi	nal.



In the event that you are unable to use Telnet to connect to the serial port defined for the vWLC, you can restart the Cisco 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, access the Cisco vWLC console port by connecting via Telnet to the IP address and TCP port defined in the Add Hardware wizard in the previous procedure.

Tera Term: New co	nnection	×
	Hos <u>t</u> : 10.4.63.96 Hist <u>o</u> ry Service: Telnet SSH Other	TCP port#: 7601 SSH version: SSH2 version: VNSPEC version: VNSPEC version:
© S <u>e</u> rial	Po <u>r</u> t: COM3	•
	OK Cancel	<u>H</u> elp

The deployment of the vWLC is now complete.

# Procedure 4 Configure the data center switches for the Cisco Flex 7500 Series WLC

When using a dedicated design controller model with the Cisco Flex 7500 Series 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 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 159 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-channel65
  description Link to WLC7500-1
  switchport mode trunk
  switchport trunk allowed vlan 159
  no shutdown
interface port-channel66
  description Link to WLC7500-2
  switchport mode trunk
  switchport trunk allowed vlan 159
  no shutdown
```

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

```
interface Vlan159
no shutdown
description Remote Site Wireless Management Network
no ip redirects
ip address 10.4.59.2/24
ip router eigrp 100
ip passive-interface eigrp 100
ip pim sparse-mode
hsrp 159
priority 110
ip 10.4.59.1
```

**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 159
  channel-group 65
  no shutdown
interface Ethernet104/1/1
  description link to 7500-1
  switchport mode trunk
  switchport trunk allowed vlan 159
  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 Controller.

```
interface Ethernet103/1/2
  description link to 7500-2
  switchport mode trunk
  switchport trunk allowed vlan 159
  channel-group 66
  no shutdown
interface Ethernet104/1/2
  description link to 7500-2
  switchport mode trunk
  switchport trunk allowed vlan 159
  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.



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

```
vlan 159
name WLAN_Mgmt
```

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

```
interface Vlan159
description Remote Site Wireless Management Network
ip address 10.4.59.1 255.255.255.0
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 Controller, configure a 10-Gigabit distribution switch interface as a trunk. Note that when deploying a Cisco Flex 7500 Series 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 dot1q
switchport trunk allowed vlan 159
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
Т
interface Port-channel [number]
description To WLC
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 159
 switchport mode trunk
logging event link-status
no shutdown
```

## Procedure 6 Connect the redundancy port

If you are using a Cisco vWLC, skip this procedure. If you are using a Cisco Flex 7500 Series WLC and you wish to enable the HA SSO feature, continue with this procedure. When using the high availability feature known as Stateful Switchover (HA 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 Ethernet cable between the primary and standby WLC, as shown in the following.

Redundancy Port

The 7500 Redundancy Port (RP) may be extended across a Layer 2 network provided that it meets the following requirements:

- Two 7500 models connected via back-to-back route processor (RP) port in the same data center or
- Two 7500 models connected via the RP port over Layer 2 VLAN in the same or different data centers or
- Two 7500 models connected to a virtual switching system (VSS) pair and
  - Round-trip time (RTT) latency between each WLC RP is 80ms or less and
  - Preferred MTU on the redundancy port link of 1500 or more and
  - Bandwidth between the redundancy ports is 60 Mbps or more



Procedure 7 Configure the WLC platform

If you are installing a vWLC, the virtual 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 Cisco vWLC if the vSphere console was selected as the default terminal when the vWLC was started.

Once connected, upon initial boot up of the WLC, you should see the following on the console. If you do not see this, press – a few times to force the startup wizard to back up to the previous step.

Welcome to the Cisco Wizard Configuration Tool Use the '-' character to backup

Step 1: Terminate the autoinstall process.

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

Step 2: Enter a system name. (Example: WLC-RemoteSites-1)

System Name [Cisco d9:3d:66] (31 characters max): WLC-RemoteSites-1

Step 3: 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 4: Use DHCP for the service port interface address.

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

**Step 5:** If you are deploying a shared Cisco 5500 or Cisco Flex 7500 Series Wireless LAN Controller, enable Link Aggregation (LAG).

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

**Step 6:** Enable the management interface. If configuring the secondary resilient controller in an HA controller pair, this IP address will only be in use during the first boot up of the WLC. Once the secondary resilient WLC downloads the configuration from the primary WLC and becomes a member of the HA controller pair, this IP address will no longer be used. In an N+1 configuration however, the secondary resilient controller is not part of the HA controller pair and will have its own unique IP address as configured.

```
Management Interface IP Address: 10.4.59.68
Management Interface Netmask: 255.255.255.0
Management interface Default Router: 10.4.59.1
Management Interface VLAN Identifier (0 = untagged): 159
```

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

Management Interface Port Num [1 to 1]: 1

**Step 7:** Enter the DHCP server for clients. (Example: 10.4.48.10)

Management Interface DHCP Server IP Address: 10.4.48.10

**Step 8:** If you are deploying a shared Cisco 5500 or Cisco Flex 7500 Series Wireless LAN Controller, enable HA SSO. The virtual Wireless LAN Controller does not support HA SSO.

Step 9: If you are configuring the primary controller in an HA controller pair using the following values.

Enable HA (Dedicated Redundancy Port is used by Default) [yes][NO]: YES

If you are configuring the primary controller in an HA controller pair use the following values.

Configure HA Unit [PRIMARY][secondary]: **PRIMARY** 

Redundancy Management IP Address: 10.4.59.168

Peer Redundancy Management IP Address: 10.4.59.169

If you are configuring the secondary controller in an HA controller pair use the following values.

Configure HA Unit [PRIMARY][secondary]: **SECONDARY** Redundancy Management IP Address: **10.4.59.169** Peer Redundancy Management IP Address: **10.4.59.168** 

**Step 10:** The virtual interface is used by the WLC for mobility DHCP relay and inter-controller 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 11: Enter a name for the default mobility and RF group. (Example: REMOTES) Mobility/RF Group Name: **REMOTES** 

Step 12: Enter an SSID for the WLAN that supports data traffic. This is used later in the deployment process. Network Name (SSID): WLAN-Data Configure DHCP Bridging Mode [yes][NO]: NO

Step 13: Enable DHCP snooping.
 Allow Static IP Addresses {YES][no]: NO

- Step 14: 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 Warning! The default WLAN security policy requires a RADIUS server. Please see documentation for more details.
- Step 15: 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 16: 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 17: Enable the RRM auto-RF feature. This helps you keep your network up and operational. Enable Auto-RF [YES] [no]: YES Step 18: 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 19:** Save the configuration. If you respond with **no**, the system will restart 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
```

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.

The WLC resets and displays a User: login prompt.

```
(Cisco Controller)
Enter User Name (or 'Recover-Config' this one-time only to reset configuration to
factory defaults)
User:
```

If you have been configuring the secondary Shared Cisco 5500 or Cisco Flex 7500 controller as a high availability controller pair, then at this point the configuration for the secondary controller is now complete. After the system reset finishes, the secondary controller downloads its configuration from the primary. Web access to the HA pair is now obtained by using the IP address assigned to the management interfaces of the primary controller. Because no further steps in this procedure or process are used when configuring the secondary controller in an HA pair, you must use the following steps and procedures only for initial configuration of the primary controller.

**Step 20:** If you are configuring a Cisco Flex 7500 or virtual Wireless LAN Controller (vWLC), after the WLC has restarted, logon to the console using local userid and password. To configure the WLC to automatically convert the APs to Cisco FlexConnect mode as they register enter the following command.

config ap autoconvert flexconnect

Procedure 8 Configure the time zone

Configuring the time and date of the WLC is critical, because certificate validation is performed using the date/ time as configured on the WLC. Improper date/time may prevent access points from successfully registering with the WLC. Verify the proper data and time is obtained from the NTP server as configured in the Startup Wizard

**Step 1:** Use a web browser to log in to the Cisco Wireless LAN Controller administration web page by using the credentials defined in Step 3. (Example: https://WLC-RemoteSites-1.cisco.local/)

Step 2: Navigate to Commands > Set Time.

Step 3: In the Location list, choose the time zone that corresponds to the location of the WLC.

Step 4: Click Set Time zone.

	Saye Configuration Bing Logout Befresh MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Commands	Set Time Set Timezone
Download File Upload File Reboot	Current Time Tue May 31 11:07:38 2011 Date
Config Boot Scheduled Reboot	Month May -
Reset to Factory Default	Year Z011
Set Time	Time
	Hour 11 - Minutes 7 Seconds 38
	Timezone
	Delta hours 0 mins 0 Location <sup>4</sup> (GMT -8:00) Pacific Time (US and Canada) •
	Foot Notes I. Automatically sets daylight savings time where used.

**Step 5:** Press **OK** when prompted that continuing will cancel any scheduled system resets. Any scheduled system resets will be canceled as changing the time zone may cause a system reset at an undesirable time.



Procedure 9 Configure SNMP

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

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

Step 3: Enter the IP Address of your network management network. (Example: 10.4.48.0)

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

ahaha							Sa <u>v</u> e Cor	figuration   <u>P</u> ing   Logout   <u>R</u> ef	
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBACK	
CISCO Management Summary SNMP General SNMP V3 Users Communities Trap Receivers Trap Controls Trap Logs HTTP-HTTPS Telnet-SSH Serial Port Local Management Users User Sessions Logs	MONITOR SNMP v1 Communi IP Addres IP Mask Access Mc Status	WLANS / v2c Cc ty Name s	CONTROLLER pmmunity > N cisco 10.4.48.0 255.255.255.0 Read Only • Enable •	WIRELESS	SECURITY	MANAGEMENT	Saye Cor	ifiguration Ping Logout <u>P</u> et HELP FEEDBACK <back apply<="" td=""><td>resh</td></back>	resh
Software Activation     Tech Support									

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

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

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

Step 8: Enter the IP Address of your network management network. (Example: 10.4.48.0)

Step 9: Enter the IP Mask of your network management network. (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.

CISCO     MONITOR     WLANS     CONTROLLER     WIRELESS     SECURITY     MANAGEMENT     COMMANDS     HELP     FEEDBACK       Management     SNMP v1 / v2c     Community > New     < Back     Apply       Summary     Community Name     cisco123          * SNMP     IP Address     10.4.48.0          General     IP Mask     255.255.255.0          Communities     Access Mode     Read/Write •          Trap Receivers     Status     Enable •          HTIP-HITIPS     Telnet-SSH     Serial Port          Logs     User Sessions
Management     SNMP v1 / v2c Community > New     < Back
Summary     Community Name     discol23       ▼ SMMP     IP Address     10.4.48.0       General     IP Mask     255.255.00       Communities     Access Mode     Read/Write ▼       Trap Receivers     Status     Enable ▼       HTTP-HTTPS     Telnet-SSH       Serial Port     Local Management       Users     Users
Software Activation     Fach Support

Step 12: Navigate to Management > SNMP > Communities.

**Deployment Details** 

**Step 13:** On the right side of the **public** community, point and click the blue down arrow, and then click **Remove**. On the "Are you sure you want to delete?" message, click **OK**.

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

սիսիս							Sa <u>v</u> e Co	nfiguratio	n   <u>P</u> ing   L	.ogout   <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMEN	COMMANDS	HELP	<u>F</u> EEDBACK	
Management	SNMP v1	/ v2c Co	ommunity							New
Summary										
▼ SNMP	Communit	y Name		IP Address	IP Mask	Access	Mode Status			
General SNMP V3 Lisers	cisco			10.4.48.0	255.255.25	55.0 Read-O	nly Enable			
Communities	cisco123			10.4.48.0	255.255.25	55.0 Read-W	rite Enable			
Trap Receivers										
Trap Logs										
HTTP-HTTPS										
Telnet-SSH										
Serial Port										
Local Management Users										
User Sessions										
Logs										
Mgmt Via Wireless										
Software Activation										
Tech Support										

Step 15: Navigate to Management > SNMP > General and disable SNMP v3 Mode, then press Apply.

cisco	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>s</u> ecurity	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS
Management	SNMP Sys	stem Su	immary				
Summary SNMP General	Name Location		vWLC-F	emoteSites-1			
SNMP V3 Users Communities Trap Receivers Trap Controls	Contact System De	escription	Cisco Cont	roller			
HTTP-HTTPS	System Ob	oject ID	1.3.6.1.4.	1.9.1.1631			
Telnet-SSH	SNMP Port	Number	161				
Serial Port	Trap Port M	Number	162				
Local Management Users	SNMP v1 N	1ode Mode	Disable	<ul><li>✓</li><li>✓</li></ul>			
User Sessions Logs	SNMP v3 N	Iode	Disable	Y Y			

Step 16: Navigate to Management > SNMP Communities > SNMP V3 Users

Step 17: On the right side of the default User Name, point and click the blue down arrow, and then click Remove

ahaha						Sa <u>v</u> e C	Configuration   [	2ing   L	ogout   <u>R</u> efresh
cisco	<u>M</u> ONITOR	<u>W</u> LANs	<u>CONTROLLER</u>	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK
Management	s	SNMP V3	Users						New
Summary									
▼ SNMP		User Name	Access	Level Au	th Protocol	Privacy Protoco	bl		
General		default	Readwrit	e HM	AC-SHA	AES	Remove		
Communities							4		
Trap Receivers									
Trap Logs									
HTTP-HTTPS									
Telnet-SSH									
Serial Port									
Local Manager Users	ment								
User Sessions									
▶ Logs									
Mgmt Via Wire	eless								
Software Activ	vation								
Frech Support									

Step 18: Press OK to confirm that you are sure you want to delete, then press Save Configuration

- altala							Save Co	onfiguration   ]	Ping   L	ogout   <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs	<u>CONTROLLER</u>	WIRELESS	<u>S</u> ECURIT	Y M <u>A</u> NAC	GEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK
Management	~	SNMP V3	Users							New
Summary										
▼ SNMP		User Name	Access I	Level Au	th Protoco	l Privac	y Protoco	I.		
General		default	Readwrit	e HM	AC-SHA	AEC		_		
Communities						Message fro	m webpage	1	23	
Trap Receivers Trap Controls Trap Logs						? ▲	kre you sure	you want to dele	ete ?	
HTTP-HTTPS						•				
Telnet-SSH										
Serial Port								ок с	ancel	
Local Manager Users	nent									
User Sessions										
Logs										
Mgmt Via Wire	less									
Software Activ	ation									
Frech 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 SSH or HTTPS.

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

Step 2: Enter an access control list name and select ACL Type IPv4, 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

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

սիսիս							Sa <u>v</u> e Co	nfiguratio	n   <u>P</u> ing   Logout   <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK
Security	Access C	control L	ists > Rules >	New					< Back Apply
<ul> <li>AAA</li> <li>Local EAP</li> <li>Priority Order</li> </ul>	Sequence Source		1 IP Address	-	IP Addr 10.4.4	ess 18.0	Netmask 255.255.255.0		
Certificate	Destination		Any	•					
<ul> <li>Access Control Lists Access Control Lists CPU Access Control Lists</li> </ul>	Protocol		TCP	-					
FlexConnect ACLs	Source Port		Any	-					
Wireless Protection     Policies	Destination I	Port	HTTPS	•					
Web Auth	DSCP		Any	•					
TrustSec SXP Advanced	Direction		Any	•					
	Action		Permit	•					

Then click Apply.

Sequence	Source	Destination	Protocol	Source port	Destination port	Action
1	10.4.48.0/ 255.255.255.0	Any	ТСР	Any	HTTPS	Permit
2	10.4.48.0/ 255.255.255.0	Any	ТСР	Any	Other/22	Permit
3	Any	Any	ТСР	Any	HTTPS	Deny
4	Any	Any	ТСР	Any	Other/22	Deny
5	Any	Any	Any	Any	Any	Permit

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

cisco	<u>M</u> ON:	ITOR		s <u>c</u> ontr	OLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK			Sa <u>v</u> e Cont	iguration	<u>P</u> ing   Logout   <u>R</u> efresh
Security	Acc	ess C	ontrol	Lists > E	dit									< Bac	<	Add New Rule
AAA     Local EAP     Priority Order     Certificate     Access Control Lists     Access Control Lists     CPU Access Control	Geni Acces Deny Seq	eral Is List N Counte Actio	ame irs n So	ACL- 0 urce IP/M	Rules		Destination IP/Mask	1	Protoc	ol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
Lists FlexConnect ACLs	1	Permi	t 10.	4.48.0	/ 255.	255.255.0	0.0.0	/ 0.0.0.0	TCP		Anγ	HTTPS	Any	Any	0	
Wireless Protection	2	Permi	t 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	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	TCP		Any	22	Any	Any	0	
TrustSec SXP Advanced	<u>.5</u>	Permi	t 0.0	.0.0	/ 0.0.	0.0	0.0.0	/ 0.0.0.0	Any		Anγ	Any	Any	Any	0	

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 then Save Configuration.

**Procedure 11** Configure wireless user authentication using Cisco ISE

In this design, the RADIUS authentication service is provided by the Cisco Identity Services Engine (ISE). The Cisco ACS server is used solely for network administrative access to the WLC using TACACS+.

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

Step 2: Enter the ISE Server IP Address. (Example: 10.4.48.41)

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

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

11111						Sa <u>v</u> e Co	nfiguration <u>P</u> ir	ng T Log	lout <u>R</u> efresh
CISCO	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>E</u> EEDBACK
Security	RADIUS	Authenti	cation Servers	s > Edit			< Bac	k	Apply
- AAA	Server In	dav		1					
General	Server III	uex		1					
- RADIUS	Server Ad	ldress		10.4.48.41					
Authentication	Shared Se	ecret Form	at	ASCII 🔻					
Accounting	Channel Ca								
Fallback	Silareu Se	ecrei							
DNS I	Confirm S	Shared Sec	ret	•••••					
IDAD	Kau Wasa		_						
Local Net Users	Key wrap			(Designed for	FIPS custome	ers and requires a	key wrap compli	ant RADI	IUS server)
MAC Filtering	Port Numb	ber		1812					
Disabled Clients	Server St	atus		Enabled 👻					
User Login Policies				Endbled					
AP Policies	Support fo	or RFC 357	6	Enabled 👻					
Password Policies	Server Tir	meout		2 second	s				
Local EAP	Network L	Jser		🔽 Enable					
Priority Order	Managem	ent		Enable					
Certificate	IPSec			Enable					
Access Control Lists									

**Step 5:** Repeat the Step 1 through Step 4 in the above process to add the secondary Cisco ISE authentication server (Example 10.4.48.42), then press apply followed by click Save Configuration.

Step 6: In Security > AAA > RADIUS > Accounting, click New.

Step 7: Enter the ISE Server IP Address. (Example: 10.4.48.41)

Step 8: Enter and confirm the Shared Secret (Example: SecretKey), and then click Apply.

ահահո							nfiguration <u>P</u> ir	ng   Log	iout <u>R</u> efresh
CISCO	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	SECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	EEEDBACK
CISCO  Security      AAA     General      RADIUS     Authentication     Accounting     Fallback     DNS     TACACS+     LDAP     Local Net Users     MAC Filtering     Disabled Clients     Instain Poliagion	MONITOR RADIUS Server Server Shared Shared Confirm Port Nui Server Server	WLANS Account Index Address Secret Form Secret o Shared Sec mber Status Timeout	CONTROLLER ing Servers > 1 10.4.4 at ASCI eve 1813 Enabl 2 	WIRELESS Edit 48.41 I • ed • seconds	SECURITY	Sa⊻e Con	nfiguration <u>P</u> ir C <u>O</u> MMANDS C <b>Bacl</b>	ng   Log HEL₽ ★	out <u>R</u> efresh <u>EEEDBACK</u> Apply
AP Policies Password Policies > Local EAP > Priority Order > Certificate > Access Control Lists	IPSec			Enable					

**Step 9:** Repeat Step 6 through Step 8 to add the secondary Cisco ISE accounting server (Example 10.4.48.42), click **Apply**, and then click **Save Configuration**.

### Procedure 12 Configure management authentication using Cisco ACS

You can use this procedure to deploy centralized management authentication by configuring an authentication, authorization and accounting (AAA) service.

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)

սիսիս				of cup TD/		Sa <u>v</u> e Co	nfiguration   <u>P</u> ing	Lo <u>q</u> out   <u>R</u> efresh
CISCO Security  AAA General RADIUS TACACS+ Authentication Accounting Authorization LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies Password Policies Password Policies Password Policies Password Policies Password Policies Password Policies	MONITOR WLANS TACACS+ Account Server Index (Priority) Server IP Address Shared Secret Shared Secret Confirm Shared Secret Port Number Server Status Server Timeout	CONTROLLER 1 ▼ 10.4.4 ASCII 49 Enabl 5	WIRELESS > New 48.15 ••• ••• ed •	SECURITY	MANAGEMENT	Saye Cc	nfiguration <u>Bing</u> HELP <u>FEEDBAC</u> <b>&lt; Back</b>	Logout   <u>R</u> efresh K Apply
Local EAP     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)

ahaha									n <u>P</u> ing Lo <u>q</u> out <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Security • AAA General • RADIUS • TACACS+ Authentication Accounting	Server In Server IP Shared Se Shared Se	► Author dex (Priorit Address ecret Forma	ization Serve y) ıt	1 • 10.4.48.15 ASCII •					< Back Apply
Authorization LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies	Confirm S Port Num Server St Server Tir	ihared Secr ber atus meout	et	49 Enabled ▼ 5 secon	ds				
Local EAP									
Priority Order									
Certificate									
Access Control Lists									
<ul> <li>Wireless Protection</li> <li>Policies</li> </ul>									
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.

**Step 14:** Verify that TACACS+ authentication is functioning properly by logging off the wireless LAN controller and logging back on. If you are unable to logon, verify that the WLC has been added to the ACS server properly by reviewing the ACS Section called Configuring Cisco Secure ACS for Wireless Infrastructure Access above.

#### Procedure 13 Configure the resilient WLC

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 with HA SSO, there will not be any access points registered to the resilient WLC.

Step 1: Configure the resilient HA SSO secondary WLC by repeating Procedure 5 through Procedure 10.

### Procedure 14 Configure mobility groups

In the event that you are using two WLCs using HA SSO mode of operation (Shared Cisco 5500 Series WLCs or Cisco Flex 7500 Series Cloud Controllers), you should skip this procedure as two WLCs in a high availability pair share the same configuration and operate as one appliance. If you are using two or more WLCs without HA SSO (2504 or vWLCs), then complete this procedure in order to place both controllers into a common mobility group.

This form of redundancy is often referred to as N+1, and in this mode the two or more controllers operate concurrently. For naming, we have assigned roles such as Primary and Secondary. For clarity, please note that all controllers in an N+1 configuration are active and from an access-point of view have equal capabilities. In addition, unlike HA SSO, controllers in an N+1 configuration may be comprised of different models (Cisco 5500, 2504, 7500, 8500, and vWLC Series).

### i Tech Tip

At this time the Cisco 5760 Series WLC does not support FlexConnect and therefore cannot provide FlexConnect services to remote site access points.

The common mobility group name and mobility configuration outlined in this procedure merely allows controllers to share mobility information regarding the wireless clients being serviced. This information sharing greatly improves inter-controller roaming performance.

**Step 1:** On each of the non-high availability controllers that shall be in the mobility group, navigate to **Controller > Mobility Management > Mobility Groups**. Record the MAC address, IP address, and mobility group name for the local controller are shown on the Static Mobility Group Members page. Record them in the following table.

	CVD values primary controller	CVD values secondary controller	Site-specific values primary controller	Site-specific values secondary controller
Controller name	vWLC-RemoteSites-1	vWLC-RemoteSites-2		
IP address	10.4.59.58	10.4.59.59		
MAC address	00:50:56:a2:18:19	00:50:56:a2:47:64		
Mobility group name	REMOTES	REMOTES		

Table 15 - FlexConnect mobility group values

Figure 11 - FlexConnect Mobility Group WLC-1 (Primary)

սիսիս									Save Configuration Ping	Logout   <u>R</u> efrest
cisco	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	FEEDBACK		
Controller	Static Mobility G	roup Members	6						New	EditAll
General										
Inventory	Local Mobility Gr	oup REMOTE	s							
Interfaces	MAC Address	IP Address	Group	Name	Multicast IP	Status			Hash Key	
Interface Groups	00:50:56:a2:18:1	9 10.4.59.58	REMOT	ES	0.0.0.0	Up			4670056ef1853c7c2739db3f3fd58fi	c7ce0394b
Multicast										
Network Routes										
<ul> <li>Mobility Management</li> <li>Mobility Configuration</li> <li>Mobility Groups</li> <li>Mobility Anchor Config</li> <li>Multicast Messaging</li> </ul>										

Figure 12 - FlexConnect Mobility Group WLC-2 (Secondary)

uludu cisco	MONITOR WLANS CO	NTROLLER WIRELE	SS SECURITY MANA	GEMENT C <u>O</u> MMANDS	HELP EEEDBACK	Sage Configuration   Eing   Logout	Refrest
Controller	Static Mobility Group	Members				New	EditAll
General Inventory	Local Mobility Group	REMOTES					
Interfaces	MAC Address	IP Address	Group Name	Multicast IP	Status	Hash Key	
Interface Groups	00150156182147164	10.4.59.59	REMOTES	0.0.0.0	Up	916115964D5088d390088670813187268B606D9	
Multicast							
Network Routes							
<ul> <li>Mobility Management         Mobility Configuration             Mobility Groups             Mobility Anchor Config             Multicast Messaging         </li> </ul>							

Step 2: On the resilient controller (Example: vWLC-RemoteSites-2), 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 controller designated as the primary controller, vWLC-RemoteSites-1 in this case. (Example: 10.4.59.58)

Step 4: In the Member MAC Address box, enter the MAC address of the primary controller, and then click Apply. (Example: 00:50:56:a2:18:19)

،،ا،،،ا،، cısco	<u>M</u> ONITOR <u>W</u> LANs	CONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Controller	Mobility Group M	ember > New						
General Inventory Interfaces Interface Groups Multicast Network Routes Mobility Management Mobility Configuration Mobility Anchor Config Multicast Messaging	Member IP Address Member MAC Addre Group Name Hash	10.4.59.5 00:50:56: REMOTES none	8 a2:18:19					
بابراب					Sa <u>v</u> e Co	nfiguration <u>P</u>	ing Lo	gout <u>R</u> efresh
. cısco	<u>M</u> ONITOR <u>W</u> LANS	CONTROLLER	WIRELESS	SECURITY	Sa <u>v</u> e Co M <u>A</u> NAGEMENT	nfiguration <u>P</u> C <u>O</u> MMANDS	ing Lo : HE <u>L</u> P	<u>g</u> out <u>R</u> efresh <u>F</u> EEDBACK
cisco Controller	Monitor wLans Mobility Group Men	<u>controller</u> nber > New	WIRELESS	<u>s</u> ecurity	Sa <u>v</u> e Co M <u>A</u> NAGEMENT	infiguration   <u>P</u> C <u>O</u> MMANDS <b>&lt; B</b>	ing   Lo : HELP <b>ack</b>	gout   <u>R</u> efresh <u>F</u> EEDBACK <b>Apply</b>
cisco Controller General	Monitor WLANs Mobility Group Men Member IP Address	<u>c</u> ontroller nber > New 10.4.59.59	WIRELESS	SECURITY	Sa <u>v</u> e Co M <u>a</u> nagement	nfiguration <u>P</u> C <u>O</u> MMANDS <b>&lt; B</b>	ing   Lo : HE <u>L</u> P :ack	gout <u>R</u> efresh <u>F</u> EEDBACK <b>Apply</b>
cisco Controller General Inventory	MONITOR WLANS Mobility Group Men Member IP Address Member MAC Address	<u>Controller</u> nber > New 10.4.59.59 00:50:56:a	W <u>I</u> RELESS 2:09:90	SECURITY	Sa <u>v</u> e Co M <u>a</u> nagement	infiguration <u>P</u> C <u>O</u> MMANDS <b>K</b> B	ing   Lo : HE <u>L</u> P :ack	gout   <u>R</u> efresh <u>F</u> EEDBACK <b>Apply</b>
Controller General Inventory Interfaces	MONITOR WLANS Mobility Group Men Member IP Address Member MAC Address Group Name	<u>CONTROLLER</u> nber > New 10.4.59.59 00:50:56:a REMOTES-	WIRELESS 2:09:90 WLC	SECURITY	Sa <u>v</u> e Co M <u>A</u> NAGEMENT	nfiguration <u>P</u> C <u>O</u> MMANDS <b>&lt; B</b>	ing   Lo : HELP ack	gout <u>R</u> efresh <u>F</u> EEDBACK <b>Apply</b>
Controller General Inventory Interfaces Interface Groups	MONITOR WLANS Mobility Group Men Member IP Address Member MAC Address Group Name Hash	<u>Controller</u> nber > New 10.4.59.59 00:50:56:a REMOTES none	WIRELESS 2:09:90 WLC	SECURITY	Save Co M <u>a</u> nagement	nfiguration   <u>P</u> C <u>O</u> MMANDS <b>&lt; B</b>	ing   Lo : HELP ack	gout <u>R</u> efresh <u>F</u> EEDBACK <b>Apply</b>
Controller General Inventory Interfaces Multicast	MONITOR WLANS Mobility Group Men Member IP Address Member MAC Address Group Name Hash	CONTROLLER nber > New 10.4.59.59 00:50:56:a REMOTES- none	WIRELESS 2:09:90 WLC	SECURITY	Saye Co M <u>A</u> NAGEMENT	nfiguration   <u>P</u> C <u>O</u> MMANDS < B	ing   Lo : HELP :ack	gout <u>R</u> efresh <u>F</u> EEDBACK <b>Apply</b>

Step 5: On the controller designated as the primary controller (vWLC-RemoteSites-1), 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: 10.4.59.59)

Step 7: In the Member MAC Address box, enter the MAC address of the resilient controller, and then click Apply. (Example: 00:50:56:a2:47:64)

ىرايىرايى cısco	<u>M</u> onitor	<u>W</u> LANs	<u>C</u> ontroller	W <u>I</u> RELESS	<u>s</u> ecurity	M <u>a</u> nagement	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK
Controller	Mobility (	Group M	ember > New						
General Inventory Interfaces Interface Groups Multicast Network Routes	Member Member Group Na Hash	IP Address MAC Addr ame	10.4.59.5           ess         00:50:56           REMOTES           none	9 :a2:47:64					
<ul> <li>Mobility Management</li> <li>Mobility Configuration</li> <li>Mobility Groups</li> <li>Mobility Anchor Config</li> <li>Multicast Messaging</li> </ul>									

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

**Step 9:** Navigate to **Controller > Mobility Management > Mobility Groups** on each of the controllers, 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** as shown below (Primary/Secondary).

cisco	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY MANAGEMENT	COMMANDS HELP	FEEDBACK	sage consignation   End   codour   Kenesi
Controller	Static Mobility Gro	oup Members				New EditAll
General Inventory	Local Mobility Grou	up REMOTES				
Interfaces	MAC Address	IP Address	Group Name	Multicast IP	Status	Hash Key
Interface Groups	00:50:56:a2:18:19	10.4.59.58	REMOTES	0.0.0.0	Up	4670056ef1853c7c2739db3f3fd58f0c7ce0394b
Multicast						
Network Routes	00:50:56:a2:47:64	10.4.59.59	REMOTES	0.0.0.0	Up	none 🔤
<ul> <li>Mobility Management Mobility Configuration Mobility Groups Mobility Anchor Config Multicast Messaging</li> </ul>						

،،۱،،۱،، cısco	MONITOR WLANS OF	ONTROLLER WIRELESS SECURITY	MANAGEMENT COMMANDS H	ELP BEEDBACK	Sa <u>v</u> e Configu	ration Bing Logout Befresh
Controller	Static Mobility Group	p Members				
General Inventory	Local Mobility Group	REMOTES				
Interfaces	MAC Address	IP Address	Group Name	Multicast IP	Status	Hash Key
Interface Groups	00:50:56:a2:47:64	10.4.59.59	REMOTES	0.0.0.0	Up	916115f64b50f8ad39b
Multicast Network Routes	00:50:56:a2:18:19	10.4.59.58	REMOTES	0.0.0.0	Up	none
<ul> <li>Mobility Management Mobility Configuration Mobility Groups Mobility Andhor Config Multicast Messacing</li> </ul>						

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, ensure that it is enabled by selecting **Enabled**, and then click **Apply**.

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	
WLANs	WLANs > Edit 'WLAN-Data'	
VLANS	General Security QoS Policy-Mapping Advanced	
Advanced	Profile Name WLAN-Data Type WLAN SED WLAN Data WLC	
	Status Renabled	
	Security Policies [WPA2][Auth(802.1X + CCKM)] (Modifications done under security tab will appear after applying the changes.)	
	Radio Policy All  Interface/Interface Group(G) management	
	Multicast Vlan Feature	
	Broadcast SSID 🗹 Enabled NAS-ID vvuLC-RemoteSites-1	

Step 4: On the Security > Layer 2 tab, enable CCKM. This enables fast roaming.

Tech Tip

i

CCKM may not be compatible with older wireless clients that do not support the CCX v4.0 or v5.0 extensions. Disabling CCKM may be necessary in environments where older wireless devices are used or where public use of wireless devices using 802.1x/ WPA2 is a requirement.

ululu cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK
WLANs	WLANs > Edit 'WLAN-Data'
WLANS	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2       Layer 3       AAA Servers         Layer 2 Security #       WPA+WPA2          MAC Filtering?          Fast Transition          Protected Management Frame          PMF       Disabled          WPA+WPA2 Parameters          WPA Policy          WPA2 Policy          WPA2 Policy          WPA2 Policy          WPA2 Encryption          Ø2.1X       Enable         CCKM       Enable         PSK       Enable

**Step 5:** On the Advanced tab, specify that DHCP Address Assignment is required, disable mDNS Snooping, enable FlexConnect Local Switching, and then click **Apply**.

cisco	Monitor <u>wi</u> lans <u>controller</u> wireless security management commands help <u>feedback</u>		
WLANs	WLANs > Edit 'WLAN-Data'	< Back	Apply
VLANS	General Security QoS Policy-Mapping Advanced		
VILANS  Advanced	Deficition     Deficit Margine       Annext I:          Detabled         Decomposition         Decomposition		
	mows snooping L 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.

ahaha		Save Configuration   Ping   Logout   Refresh
cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEM	IENT C <u>O</u> MMANDS HELP <u>F</u> EEDBACK
WLANs	WLANs	Entries 1 - 1 of 1
WLANS	Current Filter: None [Change Filter] [Clear Filter]	Create 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 1: On the WLANs page, in the list, choose Create New, and then click Go.

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)

CISCO     MONITOR     WLANS     CONTROLLER     WIRELESS     SECURITY     MANAGEMENT     COMMANDS     HELP     FEEDBACK       WLANS     WLANS     WLANS     VULANS       Apply       WLANS     Type     WLAN        Apply       Y MLANS     Type     WLAN            Y MLANS     Type     WLAN            Y Advanced     Type     WLAN-voice            JD     2	1111111				nfiguration <u>P</u> ing Logout <u>R</u> efresh
WLANS     WLANS     WLANS     WLAN        WLANS     Type     WLAN     Profile Name       Voice     SID     WLAN-Voice       ID     I	CISCO	MONITOR WLANS CONTRO	LLER WIRELESS SECURITY	MANAGEMENT COMMANDS	HELP FEEDBACK
WLANS     Type     WLAN       Profile Name     Voice       SSID     WLAN-Voice       ID     2	WLANs	WLANs > New			< Back Apply
	VLANS VLANS Advanced	Type Profile Name SSID ID	WLAN  Voice VULAN-Voice 2 V		<u>νυμη</u>

**Step 4:** On the Advanced tab, disable mDNS Snooping, because this is not supported with FlexConnect Local Switching. For voice WLANs, DHCP-required is not a recommended configuration, because roaming between WLCs that use different DHCP servers may result in frame loss. Additionally, some voice deployments require static IP address assignment for voice endpoints.

սիսիս		Sa <u>v</u> e Configuration   <u>P</u> ing   Logout   <u>R</u> efresh
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT	COMMANDS HELP EEEDBACK
WLANs	WLANs > Edit 'Voice'	< Back Apply
WLANS WLANS	General Security QoS Advanced	
Advanced	100000) Seconds	Passive Lilent
	Client user idle threshold (0- 10000000) 0 Bytes	Passive Client
	Off Channel Scanning Defer	Voice
	Case Defer Briefer 0 1 2 3 4 5 6 7	Media Session Snooping 📃 Enabled
		Re-anchor Roamed Voice Clients 📃 Enabled
		KTS based CAC Policy Enabled
	Scan Defer Time 100	Client Profiling
	(msecs)	DHCP Profiling
	FlexConnect	HTTP Profiling
	FlexConnect Local Switching 2 Enabled	mDNS
	FlexConnect Local Auth 12 Enabled	mDNS Snooping Enabled
	Learn Client IP Address S	
	Vlan based Central Enabled Switching 42 Enabled	я. 
	Central DHCP Processing Enabled	
	Override DNS Enabled	
	NAT-PAT Enabled	
		-
		•

Step 5: Enable FlexConnect Local Switching by selecting Enabled, and then click Apply.

Step 6: On the QoS tab, in the Quality of Service (QoS) list, choose Platinum (voice), and then click Apply.



Step 7: On the Security > Layer 2 tab, enable CCKM. This enables fast roaming.

Tech Tip

i

CCKM may not be compatible with older wireless clients that do not support the CCX v4.0 or v5.0 extensions. Disabling CCKM may be necessary in environments where older wireless devices are used or where public use of wireless devices using 802.1x/ WPA2 is a requirement.

cisco	Sage configuration len MONITOR WI ANS CONTROLLER WIRFLESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	.ogout <u>R</u> efresh
WLANs	WLANs > Edit 'Voice'	Apply
WLANS	General Security QoS Policy-Mapping Advanced	
▶ Advanced	Layer 2 Layer 3 AAA Servers Layer 2 Security @ WPA+WPA2  MAC Filtering@  Fast Transition Fast Transition Protected Management Frame Protected Management Frame WPA+WPA2 Parameters	
	WPA Policy       WPA2 Policy       WPA2 Policy       WPA2 Encryption       Øaes       TKIP       Authentication Key Management       B02.1X       CKM       Fenable       PSK	*

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

CISCO	MONITOR WLANS CONTROL	LLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	
WLANs	WLANs > Edit 'Voice'	< Back Ap	pply
WLANS WLANS	General Security Qo	IS Advanced	_
Advanced	a. (1. n.		
	Profile Name	Voice	
	Туре	WLAN	
	SSID	WLAN-Voice	
	Status	C 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)	management 👻	
	Multicast Vlan Feature	Enabled	
	Broadcast SSID	V Enabled	
	NAS-ID	WLC-RemoteSites-1	
Í			
Í			

### 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.



## **Option 1: Only one WLC pair in the organization**

If HA 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: 10.4.59.58) 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 (10.4.59.58) and 0a042e45(10.4.59.59). When the string is assembled, it yields **f1080a043b3a0a043b3b**.

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 f1080a043b3a0a043b3b

# 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, 3600 and 3700 Series Access Points used in this design 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.

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
Cisco Aironet 3700 Series	Cisco AP c3700

Table 16 - Vendor class identifiers

**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.
---------	--------------------	-----------------	-------------------	-----------------------	-----------------

🍹 DHCP			_ 8 ×
File Action View Help			
(= =) 🖄 📰 🗙 🚍 💁 📓 🖬			
2 DHCP	Name	Actions	
E iad.dsco.local	IPv4	ad.cisco.local	<b>▲</b>
<ul> <li>Display Statistics</li> </ul>	IPv6	More Actions	•
New Scope			
New Superscope			
New Multicast Scope			
Define User Classes Define Vendor Classes			
Descrite All Servers			
Records An Scopes			
Set Predefined Options			
Refresh			
Properties			
Help			
	1		
Define vendor specific option classes			

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

DI	HCP Vendor Classes		? ×
-	<u>A</u> vailable classes:		 
	Name	Description	Add
	Microsoft Windows 20 Microsoft Windows 98 Microsoft Options	Microsoft vendor-specific option Microsoft vendor-specific option Microsoft vendor-specific option	Edit
			Close

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 13, and then click **OK**. (Example: Cisco AP c1600)

the second secon	IX
File Action View Help	
Property         Name         Actions	
ad.cisco.local	-
IPv6     More Actions	•
DHCP Vendor Classes	
Available classes:	
Name Description Add	
Mi New Class	
Cis Cisco Aligned 1000 AD	
Cis Description:	
D: Binary: ASCII:	
0008 20 63 31 36 30 30 c1600	
OK Cancel	

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

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

Predefined Options	and ¥alues	? ×
Option class:	Cisco Aironet 1600 AP	•
Option name:		•
	Add Edit Del	ete
Description:		
_ Value		
L	OK Car	ncel

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

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
Description:	
	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, 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: 10.4.59.58)

cope Options			?
General Advanced			
Vendor class:	Cisco Aironet 1600	AP	<b>v</b>
User class:	Default User Class		•
Available Options 241 Option 43	Description	I	
▲ Data entry			•
Server name:			
		F	Resolve
IP address:			
	Add		
10.4.59.58	Remove		
	Up		
	Down		
	OK	Cancel	Apply

**Step 17:** If you are not using HA SSO (as is the case with the vWLC), it is necessary to repeat Step 16 for the resilient controller, and then click **Apply**. (Example: 10.4.59.69)

ope options		?
General Advanced		
Vendor class:	Cisco Aironet 1600 AP	•
User class:	Default User Class	-
Available Options	Description	
☑ 241 Option 43		
•		
<sup>-1</sup> Data entry		
Server name:		_
	Resolve	
IP address:		_
IP address:	Add	
IP address:	Add	
IP address:	Add Remove Up	
IP address:	Add Remove Up Down	
IP address:	Add Remove Up Down	

**Procedure 18** 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 Application Optimization Using Cisco WAAS Technology Design 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
!
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 dot1Q 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
!
interface GigabitEthernet0/2.70
description Wireless Voice
encapsulation dot1Q 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 Application Optimization Using Cisco WAAS Technology Design 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.

# i Tech Tip

You do not need to specify the trunk encapsulation type on Catalyst 2960X and 4500 Series switches, but you do need to specify it on Catalyst 3750X 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 nonegotiate
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. You can activate the demo license included with the Cisco vWLC deployment by completing the following steps. After you acquire a permanent license from licensing@cisco.com, you must install and activate it, using the same steps below.



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

Step 2: Change the Priority to High by using the Set Priority button, and then click Apply.

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

Step 4: Reboot the Cisco 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 20 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.

ahaha					age Configuration   Ping	Logout Befresh
CISCO	MONITOR WLANS CONTR	OLLER WIRELESS SECURITY	MANAGEMENT COMMANDS HI	LP FEEDBACK		1
Wireless	All APs > Details for AP6c	:20.560e.1b11			< Back	Apply
<ul> <li>Access Points         <ul> <li>All APs</li> <li>Radios</li> <li>802.11a/n/ac</li> </ul> </li> </ul>	General Credentials	Interfaces High Availability	Inventory FlexConnect	Advanced		
802.11b/g/n Dual-Band Radios	General		versions			
Global Configuration	AP Name	AP6c20.560e.1611	Primary Software Version	7.6.100.0		
Advanced	Location	default location	Backup Software Version	0.0.0.0		
Mesh	AP MAC Address	60120156106110111	Predownload Status	None		
RF Profiles	Adapta Chabia	341481461041010	Predownloaded Version	None		
FlexConnect	Admin Status	Enable •	Predownload Next Ketry Time	NA		
FlexConnect ACLs	AP Note	None	Boot Version	15.7.7.4		
▶ 802.11a/n/ac	Operational Status	REG	IOS Version	15.2(4)1936		
▶ 802.11b/g/n	Port Number	LAG	Mini IOS Version	0.0.0.0		
Media Stream	Venue Group	Unspecified T	IP Confin			
Application	Venue Type	Unspecified *	10 address			
Visibility And Control	Venue Name		Electro ID			
Country	Language		5680C 1P			
Timers			Time Statistics			
Netflow			UP Time	27 d, 21 h 57 m 26 s		
▶ 00S			Controller Associated Time	7 d, 16 h 13 m 19 s		
			Controller Association Latency	0 d, 06 h 00 m 31 s		
	Hardware Reset	Set to Fa	ctory Defaults			
	Perform a hardware reset o	on this AP Clear	configuration on this AP and reset it to	factory		
	Reset AP Now	Ueraul				
		C	lear All Config			
			Clear Config Except Static IP			

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)

սիսիս				050110777/		Sa <u>v</u> e Configu	uration Ping	Logout   <u>R</u> efresh
CISCO	MONITOR WL	ANS <u>C</u> UNTRULL	ER VV <u>I</u> RELESS	SECORITY	MANAGEMENT	C <u>O</u> MMANDS H	ELP <u>F</u> EEDBAC	ĸ
Wireless	All APs > Det	ails for AP6c20	560e.1b11				< Back	Apply
<ul> <li>Access Points         All APs         Radios         802.114/n/ac         802.11b/g/n         Dual-Band Radios         Global Configuration         Advanced         Mesh         RF Profiles         FlexConnect Groups         FlexConnect ACLs         802.11a/n/ac         802.11b/g/n         Media Stream         Application Visibility         And Control         Country         Timers         Netflow         QoS     </li> </ul>	General VLAN Support Netive VLAN FlexConnect Group Name PreAuthentice External Wei Local Split A Central DHC Laver2 ACLs OfficeExtend OfficeExtend AP Enable Leas Latency Controller Join	Credentials     I       I     ID       64     64       bauthentication AGL       cLis       P       Coccessing       AP       d       t	vlan Mappi	gh Availability	Inventory	FlexConnect	Advanced	E

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 19 and then click **Apply**. (Example: 70)

սիսիս								Configuration   <u>P</u> i	ng   Loj	<u>q</u> out   <u>R</u> efresh
CISCO	MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>s</u> ecur		MANAGEMEN	T C <u>O</u> MMANDS	HE <u>L</u> P	EEEDBACK
Wireless	All APs >	AP6c20	.560e.1b11 > '	VLAN Mappi	ngs			< Back		Apply
Access Points     All APs	AP Name	AP6	c20.560e.1b11							
<ul> <li>Radios</li> <li>802.11a/n/ac</li> <li>802.11b/g/n</li> </ul>	Base Radi MAC	<b>0</b> 34:a	a8:4e:ba:10:f0							
Dual-Band Radios Global Configuration	WLAN VLA	N Mappi	ng							
Advanced	Make AF	9 Specific	▼ Go							
Mesh	WLAN					VLAN				
RF Profiles	Id	SSID				ID	NAT-PAT	Inheritance		
FlexConnect Groups	1	WLAN-Dat	a-7500			65	no	Wlan-specific		
FlexConnect ACLs	2 WLAN-Voice-7500					70	no	Wlan-specific		
▶ 802.11a/n/ac										
▶ 802.11b/g/n	Centrally s	switched	Wlans							
Media Stream	WLAN Id SS	ID			VI IC	AN				
Application Visibility And Control	3 75	00Guest			N,	/A				
Country	AP level V		Manning							
Timers	All level v	LAN AGE		Eaross Al	9					
Netflow	Vian Iu	Ing	ICSS ALL	Lyress Au	.L.					
b 0.05	Group lev	el VLAN	ACL Mapping							
F Q05	Vlan Id	Ing	ress ACL	Egress A(	L					
	East Not									
	1. Vlan do	oes not tak	e effect for NAT-I	PAT enabled WL	INS.					

#### **Procedure 22** Configure access points for resiliency

If you are using the HA SSO feature on a Cisco 5500 Series WLC or Cisco Flex 7500 Series Cloud Controller, skip this procedure, as the resilient controller automatically tracks the primary controller and assumes its IP address in the event of a failure. The HA SSO feature is not available on the virtual wireless LAN controller (vWLC) or 2500 series WLC.

**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: vWLC-RemoteSites-1/ 10.4.59.58)

**Step 4:** In the **Secondary Controller** box, enter the name and management IP address of the resilient WLC, and then click **Apply**. (Example: vWLC-RemoteSites-2/ 10.4.59.59)

cisco	<u>M</u> onitor	<u>W</u> LANs	<u>C</u> ontro	LLER WIRELE	ss <u>s</u> eci	JRITY M	<u>a</u> nagement	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Wireless	All APs > [	Details f	or AP3	602-RS201						
Access Points     All APs     Radios	General	Crede	ntials	Interfaces	High Av	ailability	Inventory	FlexCon	nect	Advanced
802.11a/n/ac 802.11b/g/n		Name				Management IP Address				
Global Configuration	Primary Controller VWLC-Rem			-RemoteSites-1	teSites-2 10.4.59.59					
Advanced	Controller									
Mesh										
FlexConnect Groups	AP Failov	er Priority	Low	~						

**Procedure 23** 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: Click Add AP, and then select Select APs from current controller.

August 2014 Series

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

alialia cisco	MONITOR WLANS CONTROLLE	R WIRELESS SECURITY	/ MANAGEMENT	COMMANDS	HELP FEED	Sa <u>v</u> e Configuration IBACK	<u>P</u> ing   I	Logout   <u>R</u> efresh
All APs     Access Points     All APs     Access Points     All APs     Cadios     B02.11s/n/ac     802.11s/n/ac     B02.11s/n/ac     Advanced     Mesh     RF Profiles     FlexConnect Groups     FlexConnect Groups     FlexConnect ACLs     802.11b/a/n     Media Stream     Application Visibility     And Control     Country     Timers     Netflow     Qos	YONITOR         YULANS         CONTROLLE           FlexConnect Groups > Edit         General         Local Authentication           Group Name         Enable AP Local Authentication <sup>2</sup> FlexConnect APs           Add AP         Select APs from current controll         AP Name           AP Name         APedd3 f110 a757 +         Ethernet MAC           AP NAC         AP NAC         AP APAC	VIRELESS     SECURITY       "Remote Site 1"     """"""""""""""""""""""""""""""""""""	ACL Mapping ACL Mapping Status Associated Associated	Central DHCP	WLAN VI. WLAN VI. Sever ype ddress erver ype bardd confirm hared confirm dd dd ver Type Configured Configured	An mapping An mapping An mapping An mapping Address Unconfigured Unconfigured	F F C C C	Apply Apply Fort D D D D D D D D D D D D D D D D D D D
	٠	111						-

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

**Step 7:** Under AAA, enter the **Server IP Address** for the Primary ISE server (Example: 10.4.48.41) and the **Shared Secret** (Example: Secret Key), and then click **Add**.

**Step 8:** Repeat the process for the secondary ISE Server (Example: 10.4.48.42) and **Shared Secret** (Example: SecretKey), click **Apply**, and then click **Save Configuration**.

արտիս										Eing Logout Refres
CISCO	MONITOR WLANS CO	ONTROLLER V	VIRELESS SECUR	ITY MANAGEMENT	COMMANDS	HELP EEED	BACK			
Wireless	FlexConnect Groups	>Edit 'Rer	mote Site 1'							Apply
▼ Access Points										
All APs	General Local Aut	thentication	Image Upgrade	ACL Mapping	Central DHC	P WLAN VLA	N mapping			
<ul> <li>Radios</li> <li>802.11a/n/ac</li> <li>802.11b/g/n</li> <li>Dual-Band Radios</li> <li>Global Configuration</li> </ul>	Group Name Enable AP Local Auther	Remo	ote Site 1							
Advanced	FlexConnect APs				[	AAA				
Mesh	Add AP					Server IP	10.4.48.42			
RF Profiles	AP MAC Address	AP Name		Status		Address Server Type	Secondary -			
FlexConnect ACLs	44:03:a7:34:8a:68	AP4403.a73	34.8a68	Associated		Shared				
▶ 802.11a/n/ac	6c:20:56:0e:1b:11	AP6c20.560	le.1b11	Associated		Confirm				
▶ 802.11b/g/n						Shared Secret				
Media Stream						Port Number	1812			
Application Visibility     And Control						Add				
Country										
Timers						Server Type	Address	Port		
Netflow						Primary	10.4.48.41	1812		
▶ QoS								-	-	

Step 9: Repeat Procedure 23 for each remote site.
# **Procedure 24** Enable 802.11ac using DCA on Cisco AireOS Flex Controllers

With the advent of 802.11a wave 1, 40 and 80MHz wide channels can be enabled. This can be accomplished manually on an AP by AP basis, or can be enabled globally using Dynamic Channel Assignment (DCA). Note that changing the default channel width for 802.11ac capable access points will require the 802.11a network to be disabled.



Step 1: Disable the 802.11a network by navigating to Wireless > 802.11a/n/ac > Network, clearing 802.11a Network Status, and then clicking Apply.

սիսիս							Ga <u>v</u> e Cont	iguration <u>P</u> ing	Logout <u>R</u> efresh
cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u>	ONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	EEEDBACK	
Wireless	802.11a Global Parar	meters							Apply
Access Points     All APs     Radios     Rodios     B02.11a/n/ac     802.11a/n/ac     802.11a/n/ac     Global Configuration     Global Configuration     Advanced     Mesh     RF Profiles     FlexConnect Groups     FlexConnect ACLs	General 802.11a Network Status Beacon Period (millisecs Fragmentation Thresholi (bytes) DTPC Support. Maximum Allowed Client RSSI Low Check RSSI Threshold (-60 to dBm)	: End ;) to d 23 v End ts 200 -90 -8(	ibled ) 46 ibled ibled		Data Rates** 6 Mbps 9 Mbps 12 Mbps 18 Mbps 24 Mbps 36 Mbps 48 Mbps 54 Mbps	Mar Sup Mar Sup Sup Sup Sup	idatory • ported • idatory • idatory • ported • ported •		
▼ 802.11a/n/ac	802.11a Band Status								
Network R RG Grouping TPC DCA Coverage General Client Roaming Media EDCA Parameters DFS (802.11h) High Throughput (802.11n/ac) Cleanair 802.11b/g/n	Low Band Mid Band High Band ** Date Rate 'Mandatory specific rate will not be a implies that any associate may communicate with i that a client be able to u associate The actual dat channel selected as diffe bandwidths. The reason to select the data rates, data rate allowed for the supported.	Enabl Enabl Enabl v' implies that of able to associate dealer that et dealer that et the AP using th ta rates that are rent channels is that we shou But in reality, i at channel if the	ed ed ed lients who do , e. Data Rate ' lso supports t arked supports supported de v data rates ar he AP will pick e chosen data .	not support tha Supported <sup>2</sup> hat same rate is not required all or often pend on the rent d allow the use the next lower rate is not	CCX Location Mode	Measuremer	nabled	_	
Media Stream									

Step 2: Navigate to Wireless > 802.11a/n/ac > RRM > DCA and select the desired Channel Width to use (Example: 20 MHz, 40 MHz, 80 MHz). If they are available in your regulatory domain, enable Extended UNII-2 Channels, and then click Apply.

# Tech Tip

i

Depending on your environment, it may make sense to take a phased approach to implementing 80 MHz wide channels. Due to the number of variables discussed in the 802.11ac section in the introduction, enabling UNII channels first, enabling 40 MHz using DCA second and so forth may be less disruptive to your overall environment.

uluilii cisco	MONITOR	WLANs	CONTROLLE	R WIRELESS	SECURITY	Sa <u>v</u> e MANAGEMENT	Configuration	Ping   L HELP	.o <u>q</u> out   <u>R</u> efresh FEEDBACK
Wireless	802.11a>	RRM > D	Dynamic Ch	annel Assigr	iment (DCA	J)			Apply
<ul> <li>Access Points</li> <li>All APs</li> <li>Radios</li> </ul>	Dynamic	Channel /	Assignment	Algorithm					
802.11a/n/ac 802.11b/g/n Dual-Band Radios Global Configuration	Channel .	Assignment	Method	<ul> <li>Automatic</li> <li>Freeze</li> <li>OFF</li> </ul>	Interval: 1 Invoke C	0 minutes 👻 And hannel Update O	nce		
Advanced	Avoid For	eign AP inte	erference	🔽 Enabled					
Mach	Avoid Cis	co AP load		🔲 Enabled					
PE Brofiles	Avoid nor	n-802.11a n	ioise	🔽 Enabled					
ElexConnect Grouns	Avoid Per	rsistent Non	-WiFi	Enabled					
FlexConnect ACLs	Channel	nce Assignment	Leader	WLC7500-1 (10	.4.59.68)				
▼ 802.11a/n/ac	Last Auto	- Channel A:	ssignment	327 secs ago					
Network RRM	DCA Cha	nnel Sensiti	ivity	Medium 🔻 (	15 dB)				
RF Grouping	Channel	Width		© 20 MHz © 40	MHz 🖲 80 МН	z			
TPC	Avoid che	eck for non-	DFS channel	Enabled					
Coverage									
General	DCA Char	inel List							
Client Roaming Media EDCA Parameters DFS (802.11h) High Throughput (802.11n/ac) CleanAir	DCA Cha	nnels	36, 40, 4 116, 132	44, 48, 52, 56, 6( 2, 136, 140, 149,	), 64, 100, 104 153, 157, 161	, 108, 112,			
▶ 802.11b/g/n									
Media Stream	Select	Channel							
Application Visibility	$\checkmark$	36				×			
<sup>r</sup> And Control		40							
Country		44							
Timers	V	48							
Netflow		52				-			
▶ QoS									
	Extended	UNII-2 cha	innels <table-cell> En</table-cell>	abled					
	Current Dut		45						

Step 3: Enable the 802.11a network by navigating to Wireless > 802.11a/n/ac > Network, selecting 802.11a Network Status, clicking Apply, and then clicking Save Configuration.

սիսիս						Sa <u>v</u> e Con	figuration <u>P</u> ing	Lo <u>q</u> out <u>R</u> efresh
CISCO	MONITOR WLANS CONT	ROLLER WIRELESS	5 <u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	EEEDBACK	
Wireless	802.11a Global Paramet	ers						Apply
<ul> <li>Access Points         <ul> <li>All APs</li> <li>Radios</li> <li>802.11a/rt/ac</li> </ul> </li> </ul>	General 802.11a Network Status	🖉 Enabled		Data Rates**	Mai	ndatory •	-	
802.11b/g/n Dual-Band Radios Global Configuration	Ardios     Radios     Iradios     Iragmentation Threshold     (bytes)     DTPC Support.     Maximum Allowed Clients     RSSI Low Check     Groups     RSSI Threshold (-60 to -90     dm)	2346		9 Mbps 12 Mbps	Support	oported ·	•	
Advanced Mesh		Enabled		18 Mbps 24 Mbps	Sup Mai	oported ·	•	
RF Profiles FlexConnect Groups		Enabled	Enabled		Supported	oported ·	-	
<ul> <li>FlexConnect ACLs</li> <li>802.11a/n/ac</li> </ul>	802.11a Band Status			54 Mbps	Sup	oported ·	•	
Network RRM RF Grouping TPC	Low Band Mid Band	Enabled Enabled		Mode	measuremei E	nt inabled		
DCA Coverage General Client Roaming Media EDCA Parameters DTS (802.11h) High Throughput (802.11h/ge/n 9 802.11b/g/n Media Stream	High Band ** Date Anter (Mendetony' Im specific rate will not be able implies that any associated mary communicate with the a that a client be able to use it associate The excluid data rate channel selected as different bandwiths. The reason is different bandwiths. The reason is data rate allowed for that chi supported.	Enabled olies that clients who d to associate. Data Rate lient that also supports P using that rate. But e rates marked suppo es that are supported channel: may have d at we show data rates in reality, the AP will p annel if the chosen dat	o not support th "Supported" s that same rate it is not required tide in order to depend on the ifferent and allow the u. ick the next low a rate is not	at ier ir				

Next, verify that 802.11ac is enabled on a capable AP.

Step 4: Navigate to Wireless > Access Points > Radios > 802.11a/n/ac and notice the dynamic channel assignment shown on the 802.11ac access point (Example: APfc99.473e.1d31). Keep in mind that the channel selection process is run by default every 10 minutes, so you may need to wait a few minutes for the channel selection to occur.

iliilii cisco	MONITOR WLANS CONTROLLER	WIRELES	S SECURITY MA	NAGEMENT (	OMMANDS	HELP EEEDB	ACK			Sa <u>v</u> e Configur	ation   <u>P</u> ing	Logout   <u>R</u> efresh
Wireless	802.11a/n/ac Radios										E	ntries 1 - 5 of 5
Access Points     All APs	Current Filter: None							[Change Filt	er) [Clear F	itter)		
Radios     802.11a/n/ac     802.11b/g/n     Dual-Band Radios	AP Name	Radio Slot≠	Base Radio MAC	Sub Band	Admin Status	Operational Status	Channel	CleanAir Admin Status	CleanAir Oper Status	Radio Role	Power Level	Antenna
Global Configuration	AP6073.5c7e.e32e	1	34:a8:4e:70:4e:00		Enable	UP	(36,40) *	Enable	DOWN	N/A	1 *	Internal 💽
Advanced	AP6c20.560e.3909	1	34:a8:4e:bb:f0:10		Enable	UP	(40,36) *	NA	NA	N/A	1 *	Internal 🗧
Mesh	APfc99.473e.1d31	1	20:3a:07:e5:50:10		Enable	UP	(36,40) *	Enable	DOWN	N/A	1 *	Internal
RF Profiles	APfc99.473e.1d31	2	20:3a:07:e5:50:10		Enable	UP	(36,40,44,48) *	NA	NA	N/A	1*	Internal 🗧
FlexConnect Groups FlexConnect ACLs	APe4d3.f11e.a748	1	24:01:c7:f6:ad:30		Enable	UP	165	Disable	DOWN	N/A	1	Internal 🗧
▶ 802.11a/n/ac												
▶ 802.11b/g/n	* global assignment											
Media Stream												

# Tech Tip

The AP shown in the graphic above is a Cisco 3602 wireless access point with an 802.11ac radio module (AIR-RM3000AC). This AP has an internal 802.11a radio and with the addition of the 802.11ac radio module in the modular expansion slot, it effectively has two 5 GHz radios. Priority is given to the internal 802.11a radio if both radios need to transmit at the same point in time.



There are a number of best practices that, depending on the network requirements, can improve both performance and security. This process provides optional best practices in a number of areas.

Procedure 1 Globally enable Fast SSID change

# (Optional)

Step 1: Navigating to Controller > General and select Enabled.

cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	COMMANDS	HELP	<u>F</u> EEDBACK
Controller	General								
General Inventory Interfaces Interface Groups Multicast Network Routes Mobility Management Ports	Name 802.3x Fl Broadcasl AP Multic: AP Fallba Fast SSIE Default M	ow Control t Forwardin ast Mode <sup>1</sup> ck o change obility Dom	Mode g nain Name	VWLC-Remot	eSites-1				
► NTP	RF Group	Name		REMOTES					

Step 2: Click Apply and Save Configuration.

Procedure 2 Reduce the number of detected rogue APs

# (Optional)

Step 1: You can globally change the minimum Receive Signal Strength Indicator (RSSI) for rogue AP detection.

Step 2: Navigate to Security > Wireless Protection Policies > Rogue Policies > General and change the value from -128dBm to -70dBm.

cisco	MONITOR <u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	
Security	Rogue Policies								
AAA     General     RADIUS     Authentication     Accounting     Fallback     DNS     TACACS+     LDAP     Local Net Users     MAC Filtering     Disabled Clients     User Login Policies     AP Policies     Password Policies	Rogue Detection S Rogue Location Disc Expiration Timeout I Validate rogue clien Validate rogue clien Detect and report A Rogue Detection Re Rogue Detection Mili	ecurity Level overy Protocol for Rogue AP and R Is against AAA is against MSE d-Hoc Networks port Interval (10 to imum RSSI (-70 to	ogue Client en 300 Sec) 1-128)	C L D L T L L L L L L L L L L L L L	ow sable v 200 Secon Enabled Enabled D 0	⊖ High ds	0	Critical	Custom
Local EAP	Rogue Detection Tra	nsient Interval (0,	120 to 1800 S	ec) 0	18				
Priority Order	Rogue Client Thresh	old (0 to disable, 1	to 256)	0					
Certificate	Rogue containment	automatic rate sele	ction		Enabled				

Step 3: Press Apply and Save Configuration.

Procedure 3 Enable CCKM to enable fast roaming

# (Optional)

This procedure is for data and voice WLANs that use 802.1x/WPA2 and provide wireless services to CCX v4.0 or CCX v5.0 clients.

Step 1: On the Security > Layer 2 tab, enable CCKM.

WPA+WPA2 Parameters WPA Policy

WPA2 Encryption Authentication Key Management 802.1X Enable Enable

WPA2 Policy

CCKM PSK 4

**[**] V

ZAES TKIP





A shared guest controller is one that is simply provides services for both guest wireless users as well as enterprise wireless users. In this example, the WLC is connected to a LAN distribution switch which provides Layer 2 connectivity to the Cisco Adaptive Security Appliance (ASA)-based VLAN 1128. Management of the shared WLC is provided by the management interface already configured on the WLC.

In a shared guest controller design, the shared anchor controller is on the inside of the ASA firewall. It **does not** require explicit access rules in the DMZ-based ASA to:

- Manage the shared guest controller (https, SNMP, etc.)
- · Allow CAPWAP to allow APs register
- Allow DHCP requests to pass through the ASA on behalf of the wireless guest user.

In a dedicated guest controller design, a dedicated guest controller physically resides within the DMZ Internet edge and has an explicit wireless management interface that is used to manage the dedicated WLC. This is discussed starting in the section called Configuring Guest Wireless: Dedicated Guest Controller below.

The following procedure outlines the steps necessary to configure a shared guest controller. It assumes that the initial setup procedure of the Campus controller has been fully completed, and that controller is operational. If you are placing a dedicated guest anchor controller in the Internet Edge DMZ, skip this section and proceed to the Configuring Guest Wireless: Dedicated Guest Controller section below.

Figure 14 - Shared Guest wireless anchor controller architecture



### 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

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

Vlan 1128 name dmz-guest-wlan Step 2: Configure the interfaces that connect to the Internet edge firewalls by adding the wireless VLAN.

```
Interface GigabitEthernet1/0/24
description IE-ASA5545Xa Gig0/1
!
interface GigabitEthernet2/0/24
description IE-ASA5545Xb Gig0/1
!
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
switchport trunk allowed vlan add 1128
```

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.

Interface label	IP address & netmask	VLAN	Security level	Name
GigabitEthernet0/1.1128	192.168.28.1/22	1128	10	dmz-guest-wlan

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: GigabitEthernet0/1)

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-guest-wlan)

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:       SigabitEthernet0/1         VLAN ID:       1128         Subinterface ID:       1128         Interface Name:       dmz-guest-wlan         Security Level:       10         Dedicate this interface to management only
Channel Group:
Enable Interface      IP Address      Obtain Address via DHCP      Use PPPoE
IP Address:       192.168.28.1         Subnet Mask:       255.255.252.0
Description: WLC DMZ Guest WLAN trunk to DMZ Switch
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	Prefix Length	Standby IP Address	Monitored
igabitEthernet0/0.300	inside	🖳 10.4.24.30	255.255.255.224	🖳 10.4.24.29	<b>v</b>
igabitEthernet0/1.1116	dmz-web	🖳 192.168.16.1	255.255.255.0	🖳 192.168.16.2	<b>v</b>
L		🖳 2001:db8:a:1::1	64	🖳 2001:db8:a:1::2	
igabitunernet0/1.1117	dmz-email	🖳 192.168.17.1	255.255.255.0	🖳 192.168.17.2	<b>v</b>
igabitEthernet0/1.1118	dmz-dmvpn	🖳 192.168.18.1	255.255.255.0	🖳 192.168.18.2	<b>v</b>
igabitEthernet0/1.1119	dmz-mgmt-wlan	🖳 192.168.19.1	255.255.255.0	🖳 192.168.19.2	<b>V</b>
igabitEthernet0/1.1123	dmz-management	💐 192.168.23.1	255.255.255.0	💐 192.168.23.2	<b>V</b>
igabitEthernet0/1.1128	dmz-guest-wlan	💐 192.168.28.1	255.255.252.0	💐 192.168.28.2	<b>V</b>
SigabitEthernet0/3.16	outside-16	💐 172.16.130.124	255.255.255.0	🖳 172.16.130.123	<b>v</b>
		💐 2001:db8:a::1	64	🖳 2001:db8:a::2	
SigabitEthernet0/3.17	outside-17	🖳 172.17.130.124	255.255.255.0	🖳 172.17.130.123	<b>v</b>

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. In this design, the outside-16 address would normally be a globally unique and Internet-routable address provided by the Internet service provider (ISP). In these examples, the outside-16 and outside-17 address space is non-routable RFC 1918 space. Two ISPs are represented with distinct address space, as shown in Table 18.





Table 18 - Wireless guest address mapping

Wireless LAN guest users	ISP-provided globally unique IP address space	ISP name
192.168.28.0/22	172.16.130.124 (outside-16)	ISP A
	172.17.130.124 (outside-17)	ISP B

NAT configuration varies depending on whether a single or dual ISP configuration is used. Most of the configuration is common to both designs, although there are some additional steps for configuring both outside interfaces in the dual ISP design.

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

Step 2: Click Add > Network Object.

**Step 3:** In the **Name box**, enter a description for the address translation. (Example: dmz-guests-network-ISPa, dmz-guests-network-ISPb)

Step 4: In the Type list, select Network.

**Step 5:** In the **IP Address** box, enter the address that summarizes all DMZ Guest networks. (Example: 192.168.28.0)

Step 6: In the Netmask box, enter the internal summary 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, select Dynamic PAT (Hide).

Step 10: In the Translated Addr box, enter the name of the primary Internet connection interface, and then click OK. (Example: outside-16, outside-17)

📴 Edit Network	: Object					
Name:	dmz-guests-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 Automa	atic Address Translation Rules					
Type:	Dynamic PAT (Hide) 🔻					
Translated A	Translated Addr: outside-16					
Use one-1	to-one address translation					
PAT Pool	Translated Address:					
Round	Robin					
Extend	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 throu	iqh to interface PAT(dest intf): dmz-dmvpn					
Use IPv6						
	Advanced					
	OK Cancel Help					

Step 11: On the Network Objects/Groups pane, click Apply.

Step 12: If you are using a single ISP design, continue to Procedure 5 "Create network objects".

If you are using the dual ISP design, repeat Step 1-Step 11 for the resilient Internet connection, using the correct input for the alternate Internet connection. (Example: dmz-guests-network-ISPa, outside-17)

🔄 Add Network	c Object					
Name:	dmz-guests-network-ISPb					
Type:	Network					
IP Version:	● IPv4					
IP Address:	192.168.28.0					
Netmask:	255.255.252.0					
Description:	DMZ outside PAT address for ISPb					
NAT	*					
🔽 Add Automa	atic Address Translation Rules					
Type:	Dynamic PAT (Hide) 🔻					
Translated A	ddr: outside-17					
Use one-1	to-one address translation					
PAT Pool	Translated Address:					
Round	Robin					
Extend	PAT uniqueness to per destination instead of per interface					
Transla	Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023					
Fall throu	igh to interface PAT(dest intf): dmz-dmvpn 🔹					
Use IPv6	for interface PAT					
	Advanced					
	OK Cancel Help					

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

Procedure 4	Configure shared quest anchor WLC security policy
	boiningare shared guest anonor web security policy

In a shared guest anchor controller configuration, the WLC is providing two services, the first of which is providing CAPWAP services directly to the access points. In addition to this, the WLC is providing guest services to the wireless users. As such, the shared guest WLC has an interface that connects directly to the DMZ network.

In this procedure, the access policy for the guest wireless hosts are applied to allow outbound traffic to the Internet. The policy will also restrict all internal access, with a few exceptions such as DNS, DHCP, and HTTP/ HTTPS for DMZ web services such as walled gardens.

Step 1: On the Internet edge ASA appliance, navigate to Configuration > Firewall > Access Rules.

Interface	Action	Source	Destination	Service	Description	Logging Enable / Level
Any	permit	dmz-guest-wlan-network	internal-dns	tcp/domain, udp/domain	Allow guest wireless users to resolve DNS names.	Yes / Default
Any	permit	dmz-guest-wlan-network	internal-dhcp	udp/bootps	Allow wireless guest users to obtain/renew an IP address from the internal DHCP server	Yes / Default
Any	permit	dmz-guest-wlan-network	dmz-web-network	tcp/http, tcp/ https	Allow wireless guest users access to DMZ based webservers, possibly for walled garden access	Yes / Default
Any	deny	dmz-guest-wlan-network	dmz-networks, internal-network	ip	Deny traffic from the wireless guest network to the internal and DMZ resources	Yes / Default
Any	permit	dmz-guest-wlan-network/22	Any	ip	Allow wireless DMZ users access to the Internet	Yes / Default

Table 19 - Guest network policy rules (shared guest controller)

Step 2: Repeat Step 3 through Step 11 for all rules listed in Table 19.

i Tech Tip

24 🔽 🛃 dmz-networks

Step 3 is important for keeping the rules in the correct order.

Step 3: Click the rule that denies traffic from the DMZ toward other networks.



(2)

IP ip

😫 Deny

Step 4: Click Add > Insert.

Step 5: For Interface, select the interface listed in Table 19. (For example: Any)

Step 6: For Action, select the action listed in Table 19. (For example: permit)

Step 7: For Source, select the source listed in Table 19. (For example: dmz-guest-wlan-network)

Step 8: For Destination, select the destination listed in Table 19. (For example: internal-dns)

Step 9: For Service, enter the service listed in Table 19. (For example: tcp/domain, udp/domain)

Step 10: Enter a description. (The table text is a sample.)

Step 11: Configure Logging according to the settings in Table 19, and then click OK.

Step 12: After adding all of the rules in Table 19, in the order listed, click Apply on the Access Rules pane.

27	$\checkmark$	ng dmz-guest-wlan-network/22	🚇 internal-dns	🕸 domain 🝺 domain	🖌 Permit	0	Allow Guest Wireless users to resolve DNS names.
28	<b>V</b>	🖷 dmz-guest-wlan-network/22	📇 internal-dhcp	🐲 bootps	🖌 Permit	0	Allow wireless guest users to obtain/renew an IP address from the internal DHCP server
29	$\checkmark$	🚔 dmz-guest-wlan-network/22	🚔 dmz-web-netw	ໝ⊳ http ⊯⊳ https	🖌 Permit	0	Allow wireless guest users access to DMZ based webservers, possibly for walled garden access
30	$\checkmark$	룖 dmz-guest-wlan-network/22	dmz-networks ∰ internal-network	<b>⊥e&gt;</b> ip	🕴 Deny	0	Deny traffic from the wireless guest network to the internal and dmz resources
31	<b>V</b>	🖷 dmz-guest-wlan-network/22	🧇 any		🖌 Permit	0	Allow Wireless DMZ users access to the Internet
32	1	dmz-networks	anv4	IP in	😣 Denv	107 3	Deny IP traffic from DMZ to any other network.

Procedure 5

Configure the dynamic routing protocol

Perform this procedure if your installation uses EIGRP as the campus-based IGP.

You can use a dynamic routing protocol in order to easily configure reachability between networks connected to the appliance and those that are internal to the organization. The steps below allow the advertisement of the dmz-guests-network to the rest of the campus network using EIGRP.

Step 1: Navigate to Configuration > Device Setup > Routing > EIGRP > Setup.

Step 2: On the Networks tab, click Add.

**Step 3:** In the Add EIGRP Network dialog box, in the **IP Address** box, enter the network address for the dmzguests-network created above. (Example: 192.168.28.0)

**Step 4:** In the **Netmask** box, enter the /22 netmask for the dmz-guests-network created previously, and then click **OK**. (Example: 255.255.252.0)

🝯 Edit EIGR	RP Network
EIGRP AS:	100 🔻
IP address:	192.168.28.0
Netmask:	255.255.252.0 👻
ОК	Cancel Help

Step 5: In the Setup pane, click Apply.

### **Procedure 6** Create the guest wireless LAN interface on the AireOS Anchor WLCs

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 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:** On the Anchor Controller (Cisco ASA 5500 or Cisco 2504 Series Wireless Controller) located in the Internet edge DMZ, navigate to **Controller>Interfaces**, and then click **New**.

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

1 1						Save C	onfiguration   Pi	nallo	nout Refresh
	MONITOR				CECUDITY				
CISCO	MONITOR	<u>W</u> LANS	CONTROLLER	WIRELESS	SECORITY	MANAGEMENT	C <u>O</u> MMANDS	nc <u>u</u> p	<u>F</u> EEDDACK
Controller	r	Inter	faces > New				< Back		Apply
General		Int	erface Name	Nireless-Guest					
Invento	ry	Inc		melebb edebe					
Interfac	es	VL	AN Id	1128					
Tatasfaa	- C								
Interiac	e Groups								
Multicas	t								
Network	Routes								
Mobility	Managemer	it							
Ports									
► NTP									
► CDP									
▶ IPv6									
▶ mDNS									
Advance	ed								

Step 3: Enter the VLAN Id, and then click Apply. (Example: 1128)

**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)

սիսի						Sa <u>v</u> e (	Configuration	<u>P</u> ing   L	.ogout <u>R</u> efresh
CISCO	MONITOR	WLANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Controller	Interfaces	s > Edit					< Back		Apply
General									
Inventory	General I	nformatio	on						
Interfaces	Interface	Name	wineless	augat					
Interface Groups	Interrace	Name	Wireless	-guest					
Multicast	MAC Add	ress	88:43:e	1:/e:11:cr					
Internal DHCP Server	Configura	tion							
Mobility Management	Guest Lar	n							
Ports	Quarantir	e							
▶ NTP	Quarantin	e Vlan Id	0						
► CDP	Dhusieal I								
▶ IPv6	Physical 1	niormau	on						
Advanced	The interf	ace is attac	ched to a LAG.						
	Enable Dy	namic AP I	Management 📃						
	Interface	Address				_			
	VLAN Ide	ntifier	112	8					
	IP Addres	s	192	.168.28.5					
	Netmask		255	.255.252.0					
	Gateway		192	.168.28.1					
	DHCP Info	ormation							
	Primary D	HCP Serve	er 1	0.4.48.10					
	Secondar	y DHCP Se	rver						
	Access Co	ontrol Lis	t						
	ACL Nam	e	r	ione 🔻					
	Note: Chang temporarily some clients	ing the Inte disabled ar	erface parameters ad thus may result	s causes the Wi t in loss of conr	ANs to be ectivity for				
6									

# Tech Tip

i

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 7 Configure the guest wireless LAN on Cisco AireOS WLCs

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

uluili. cisco	MONITOR WLANS CONTROLLER WIRELESS	Saye Configuration Ping Logout <u>R</u> efres <u>S</u> ECURITY MANAGEMENT COMMANDS HELP <u>F</u> EEDBACK
WLANs	WLANs	Entries 1 - 2 of 2
WLANS	Current Filter: None [Change Filter] [Clear	Filter] Create New - Go
Advanced	ULAN ID Type Profile Name	Admin WLAN SSID Status Security Policies
	2 WLAN WLAN-Data	WLAN-Data Enabled [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)

			Sa <u>v</u> e Co	nfiguration <u>P</u> ing Lo <u>g</u> out <u>R</u> efresh
cisco	MONITOR WLANS CONTROL	LER WIRELESS SECURITY	MANAGEMENT COMMANDS	HELP FEEDBACK
WLANs	WLANs > New			< Back Apply
wLANs     WLANs     Advanced	Type Profile Name SSID ID	WLAN  Guest Guest 3		

**Step 4:** On the General tab, in the **Interface/Interface Group(G)** list, choose the interface created in Procedure 6. (Example: wireless-guest)

				Sa <u>v</u> e Configuration   <u>P</u> ing   Logou	ıt   <u>R</u> efresh
CISCO	MONITOR WLANS CON	TROLLER WIRELESS	SECURITY MANAGEMENT	COMMANDS HELP FEEDBACK	
WLANs	WLANs > Edit 'Guest	ť		< Back	Apply
<ul> <li>WLANs</li> </ul>	General Security	QoS Advanced			
WLANs					
Advanced	Profile Name	Guest			
	Turne	WI AN			
	Type	WEAK			
	SSID	Guest			
	Status	Enabled			
	Security Policies	[WPA2][Auth(802.1X)]			
		(Modifications done under se	ecurity tab will appear after ap	olving the changes.)	
	De die Delieu				
	Radio Policy	All			
	Interface/Interface Group(G)	wireless-guest 👻			
	Multicast vian Feature	Enabled			
	Broadcast SSID	Enabled			
	Foot Notes				
	1 Web Policy cannot be use	ed in combination with IPsec			
	2 H-REAP Local Switching i	s not supported with IPsec, Cl	RANITE authentication	administrativa avarrida ta racat avaludad all	opto)
	4 Client MFP is not active u	nless WPA2 is configured	ero means immity (will require	aurimistrative override to reset excluded clie	ens)
	5 Learn Client IP is configu	rable only when HREAP Local	Switching is enabled		
	b WMM and open or AES se 7 Multicast Should Be Enable	ecurity snouid be enabled to si iled For IPV6.	upport nigner 11n rates		
	8 Band Select is configurab	le only when Radio Policy is s	et to 'All'.		
	9 Value zero implies there	is no restriction on maximum	clients allowed.		
	11 MAC Filtering should be	enabled.	encouon		
	12 Guest tunneling, Local s	witching, DHCP Required show	uld be disabled.		
	13 Max-associated-clients I	reature is not supported with i	HREAP Local Authentication.		

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

CISCO	Sage comiguitation _migugout_genesi Monitor _wlans _controller wireless _ecurity management commands Help _eedback
WLANs	WLANs > Edit 'Guest' Apply
WLANS	General Security QoS Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Layer 2 Security <sup>®</sup> None
	Foot Notes 1 Web Policy cannot be used in combination with IPsec 2 H-R2AF 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 NPE is not active unless WRA2 is configured 5 Learn Client IP is configureable only when HREAP Local Switching is enabled 6 WMM and open or AES security should be enabled to support higher 11n rates 7 Multicest Should be Enabled For IPV6. 8 Band Select is configurable only when Radio Policy is set to 'AII' 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 turneling, Local switching, DHCP Required should be disabled. 13 Mar-associated-clients feature is no supported with HREAP Local Authentication.



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.

iliulu cisco	Save Configuration Ping Logout <u>R</u> efresh MONITOR <u>W</u> LANS <u>C</u> ONTROLLER WIRELESS <u>S</u> ECURITY M <u>A</u> NAGEMENT C <u>O</u> MMANDS HELP <u>F</u> EEDBACK
WLANs	WLANs > Edit 'Guest' <back apply<="" th=""></back>
WLANS	General Security QoS Advanced
Advanced	Quality of Service (QoS)     Bronze (background) •       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, CARNITE authentication 3 When clear texclusion 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 HRAP 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 IPr6. 8 Band Select is configurable only when HRAP Local Switching is support higher 11n rates 7 Multicast Should be Enabled for IPr6. 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 tunnelling, Local switching, DHCP Required should be disabled. 13 Marcsolated-clients fature is not supported with HREAP Local Authentication.

Sa<u>ve</u> Configuration | <u>P</u>ing | Logout | <u>R</u>efr uluulu cisco MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK WLANs < Back Apply WLANs > Edit 'Guest' WLANS WLANs General Security QoS Advanced Advanced Profile Name Guest Туре WIAN 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) management -Multicast Vlan Feature 🔲 Enabled Broadcast SSID Enabled Foot Notes
9 H-REAP Local Switching is not supported with IPsec, CRANITE authentication
3 When cleart exclusion is enabled, a Timeout Value of zero means infinity (will req
4 Cleart MPP is not active unless WPA, accordigued
b Witching to a category sound with the subscription of the support higher 11n rates
9 Witching and a category sound with the support higher 11n rates
9 Walk zero implies there is no restriction on maximum clients allowed.
10 MAC Filtering should be enabled.
11 MAC Filtering should be enabled.
12 Guest timeling. Local Switching, DHCP Required should be disabled.
13 Max-associated-clients feature is no supported with HREAP Local Authentication. Foot Notes strative override to reset excluded cl

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

# Procedure 8 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.

ahaha		CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	Save Co	nfiguration <u>P</u> ing	Logout   <u>R</u> efresh
CISCO Management Summary SNMP HTTP-HTTPS Telnet-SSH Serial Port Local Management Users User Sessions Logs Mgmt Via Wireless Software Activation Tech Support	Local Manageme User Name Password Confirm Password User Access Mode	Controller ent Users > Ne Gues Lobb	WRELESS W t-Admin yAdmin V		<b>NGNAGEMEN</b>		< Back	Appły

# Procedure 9 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 (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.

 cisco	Lobby Ambassador Guest Management	Logout   Refresh   Help
Guest Management	Guest Users List	New
	Items 0 User Name WLAN SSID Account Remaining Time Description	to 0 of 0

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

cisco	Lobby Ambassador Gues	t Management	Logout	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 BNx54yY		
	WLAN SSID	Any WLAN		
	Description	ht.		

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.



In a dedicated wireless guest controller design, the guest anchor controller (for instance, a Cisco 2504 or 5508 Series Wireless Controller) physically resides within the DMZ in the Internet edge. Unlike the shared design discussed previously, the DMZ-based switch has both a Guest Wireless and Wireless Management VLAN that is configured on the DMZ switch and Cisco ASA firewall.

In a dedicated guest controller design, the dedicated anchor controller is connected to the DMZ interface of the Cisco ASA firewall. It therefore **requires** explicit access rules in the DMZ-based ASA appliance to do the following:

- Manage the shared guest controller (https, SNMP, etc.)
- Enable CAPWAP in order to allow reachability between anchor and foreign anchor controllers when new
  mobility is configured
- Enable EoIP (Ethernet over IP) in order to allow reachability between Cisco AireOS-based anchor and foreign anchor controllers
- · Allow DHCP requests to pass through the Cisco ASA appliance on behalf of the wireless guest user



In this design, the dedicated anchor controller is either a Cisco AireOS-based 2504 or 5508 Series WLC. For an AireOS controller to provide anchor guest services to a Cisco IOS-XE controller (Cisco 5760 Series Wireless LAN Controller) as described in this guide, the AireOS controller must have the Enable New Mobility (Converged Access) feature enabled. Once enabled, the WLC will use CAPWAP to communicate with other controllers configured within a common mobility group. This mandates that the other AireOS controllers also have the Enable New Mobility (Converged Access) enabled.

When the New Mobility feature is enabled on a Cisco AireOS HA SSO Pair, the HA SSO convergence time is negatively affected. For this reason, this guide deploys a dedicated pair of Cisco 2504 WLC using N+1 with New Mobility (Converged Access) enabled. These WLCs provide anchor guest services with the Cisco 5760 Series WLC foreign anchor controllers within the data center-based VSS Services block. The following illustration describes the guest anchor peering being used in this guide.



Figure 16 - Dedicated Guest wireless anchor controller architecture

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 dmz-mgmt-wlan
vlan 1128
name dmz-guest-wlan
```

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
switchport nonegotiate
macro apply EgressQoS
logging event link-status
logging event trunk-status
no shutdown
```

**Step 3:** Connect the WLC EtherChannel uplinks to separate devices in the DMZ stack, and then configure two or more physical interfaces to be members of the EtherChannel. It is best if they are added in multiples of two.

This deployment uses Layer 2 EtherChannels in order to connect the WLCs to the DMZ switch. 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.

```
Interface range GigabitEthernet1/0/13, GigabitEthernet2/0/13
description DMZ-WLC-Guest-1
!
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
logging event bundle-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 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
switchport nonegotiate
logging event link-status
no shutdown
```

```
interface Port-channel13
description DMZ-WLC-Guest-2
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1119,1128
switchport mode trunk
switchport nonegotiate
logging event link-status
no shutdown
```

# **Procedure 2** Configure the firewall's DMZ interfaces for the Guest Anchor controller

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.

Interface label	IP address/netmask	VLAN	Security level	Name
GigabitEthernet0/1.1119	192.168.19.1/24	1119	50	dmz-mgmt-wlan
GigabitEthernet0/1.1128	192.168.28.1/22	1128	10	dmz-guest-wlan



**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,	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
Use Static IP      Obtain Address via DHCP      Use PPPoE
IP Address:
Subnet Mask: 255.0.0.0 -
Description:
OK Cancel Help

Step 4: On the Interface pane, click Add > Interface.

**Step 5:** In the Add Interface dialog box, in the **Hardware Port** list, choose the interface configured in Step 2. (Example: GigabitEthernet0/1)

Step 6: In the VLAN ID box, enter the VLAN number for the DMZ VLAN. (Example: 1119)

Step 7: In the Subinterface ID box, enter the VLAN number for the DMZ VLAN. (Example: 1119)

Step 8: Enter an Interface Name. (Example: dmz-mgmt-wlan)

Step 9: In the Security Level box, enter a value of 50.

Step 10: In the IP Address box, enter an interface IP address. (Example: 192.168.19.1)

Step 11: In the Subnet Mask box, enter the interface subnet mask (Example: 255.255.255.0) and then click OK.

🖬 Add Interface 🛛 🕅
General Advanced IPv6
Hardware Port:       GigabitEthernet0/1 ▼         VLAN ID:       1119         Subinterface ID:       1119         Interface Name:       dmz-mgmt-wlan         Security Level:       50         □       Dedicate this interface to management only         Channel Group:
O Use Static IP     O Obtain Address via DHCP     Use PPPoE
IP Address:       192.168.19.1         Subnet Mask:       255.255.255.0
Description: WLC DMZ Managment Interface to DMZ Switch
OK Cancel Help

Step 12: On the Interface pane, click Apply.

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	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	🖳 192.168.16.2	<b>v</b>
L		🖳 2001:db8:a:1::1	64	💐 2001:db8:a:1::2	
Gigabitunernet0/1.1117	dmz-email	🖳 192.168.17.1	255.255.255.0	🖳 192.168.17.2	$\checkmark$
GigabitEthernet0/1.1118	dmz-dmvpn	🖳 192.168.18.1	255.255.255.0	🖳 192.168.18.2	$\checkmark$
GigabitEthernet0/1.1119	dmz-mgmt-wlan	목, 192.168.19.1	255.255.255.0	🖳 192.168.19.2	<b>V</b>
SigabitEthernet0/1.1123	dmz-management	🖳 192.168.23.1	255.255.255.0	🖳 192.168.23.2	$\checkmark$
GigabitEthernetO/1.1128	dmz-guest-wlan	🚚 192.168.28.1	255.255.252.0	💐 192.168.28.2	$\checkmark$
GigabitEthernet0/3.16	outside-16	🖳 172.16.130.124	255.255.255.0	💐 172.16.130.123	$\checkmark$
		🚚 2001:db8:a::1	64	💐 2001:db8:a::2	
GigabitEthernet0/3.17	outside-17	🖳 172.17.130.124	255.255.255.0	🖳 172.17.130.123	<b>v</b>

Step 16: Repeat Step 4 through Step 15 for the dmz-guest-wlan interface.

Step 17: At the bottom of the window, click the Save to Flash icon. This saves the active configuration.

# Procedure 3 Configure NAT

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. In this example, the outside-16 address would normally be a globally unique and Internet-routable address provided by the ISP. In these examples, the outside-16 and outside-17 address space is non-routable RFC 1918 space. Two ISPs are represented with distinct address space, as shown in Table 21.

Figure 17 - Dual ISP topology



Table 21 - Wireless guest address mapping

Wireless LAN guest users	ISP-provided globally unique IP address space	Service provider name
192.168.28.0/22	172.16.130.124 (outside-16)	ISP A
	172.17.130.124 (outside-17)	ISP B

NAT configuration varies depending on whether a single- or dual-ISP configuration is used. Most of the configuration is common to both designs, although there are some additional steps for configuring both outside interfaces in the dual ISP design.

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

# Step 2: Click Add > Network Object.

The Add Network Object dialog box appears.

**Step 3:** In the **Name box**, enter a description for the address translation. (Example: dmz-guests-network-ISPa, dmz-guests-network-ISPb)

Step 4: In the Type list, select Network.

**Step 5:** In the **IP Address** box, enter the address that summarizes all DMZ Guest networks. (Example: 192.168.28.0)

Step 6: In the Netmask box, enter the internal summary 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, select Dynamic PAT (Hide).

Step 10: In the Translated Addr box, enter the name of the primary Internet connection interface, and then click OK. (Example: outside-16, outside-17)

📮 Edit Network	: Object			
Name:	dmz-guests-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	۲			
📝 Add Automa	atic Address Translation Rules			
Type:	Dynamic PAT (Hide) 🔻			
Translated A	ddr: outside-16			
Use one-1	Use one-to-one address translation			
PAT Pool	Translated Address:			
Round Robin				
Extend	Extend PAT uniqueness to per destination instead of per interface			
Transla	Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023			
🗌 Fall throu	igh to interface PAT(dest intf): dmz-dmvpn			
Use IPv6 for interface PAT				
Advanced				
	OK Cancel Help			

Step 11: On the Network Objects/Groups pane, click Apply.

Step 12: If you are using a single ISP design, continue to Procedure 5, "Create network objects".

If you are using the dual ISP design, repeat Step 1 through Step 11 for the resilient Internet connection, using the correct input for the alternate Internet connection. (Example: dmz-guests-network-ISPa, outside-17)

🔄 Add Network	c Object			
Name:	dmz-guests-network-ISPb			
Туре:	Network			
IP Version:	● IPv4			
IP Address:	192.168.28.0			
Netmask:	255.255.252.0			
Description:	DMZ outside PAT address for ISPb			
NAT	*			
🔽 Add Automa	atic Address Translation Rules			
Type:	Dynamic PAT (Hide) 🔻			
Translated A	ddr: outside-17			
Use one-	Use one-to-one address translation			
PAT Pool	Translated Address:			
Round Robin				
Extend	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 throu	☐ Fall through to interface PAT(dest intf): dmz-dmvpn			
Use IPv6	Use IPv6 for interface PAT			
	Advanced			
	OK Cancel Help			

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

### **Procedure 4** Configure Cisco ASA routing for dual-ISP environments

If you have two ISPs that have each provided a NetBlock of routable address space to your organization, complete the following steps. However, if you have a single Internet connection, skip this step and proceed to Procedure 5, "Create network objects".

This procedure implements a static route for the resilient Internet connection that becomes active when reachability to an IP host within the primary (ISP-b) is lost. Next, you edit the default route to the primary Internet CPE's address.

Step 1: Navigate to Configuration > Device Setup > Routing > Static Routes.

Step 2: Select the default route, and then click Edit.

Step 3: Verify that the Metric box remains set to 1.



Step 4: In the Edit Static Route dialog box, in the Options pane, select Tracked.

Step 5: In the Track ID box, enter 1.

Step 6: In the Track IP Address box, enter an IP address for the ISP's cloud. (Example: 172.18.1.1)

Step 7: In the SLA ID box, enter 16.

**Step 8:** In the **Target Interface** list, select the primary Internet connection interface, and then click **OK**. (Example: outside-16)

付 Edit Static Route	2			
IP Address Type:	IPv4  IPv6			
Interface:	outside-16 👻			
Network:	any4			
Gateway IP:	172.16.130.126 Metric: 1			
Options				
🔘 None				
Tunneled (Default tunnel gateway for VPN traffic)				
Tracked				
Track ID: 1	Track IP Address: 172.18.1.1			
SLA ID: 16	Target Interface: outside-16 🗸			
Monitoring C	ptions			
Enabling the tracked option starts a job for monitoring the state of the route, by pinging the track address provided.				
ОК	Cancel Help			

Step 9: On the Information dialog box, click OK.

Next, you create the secondary default route to the resilient Internet CPE's address.

Step 10: In Configuration > Device Setup > Routing > Static Routes, click Add.

**Step 11:** In the Add Static Route dialog box, in the **Interface** list, select the resilient Internet connection interface created in Step 15. (Example: outside-17)

Step 12: In the Network box, select any4.

Step 13: In the Gateway IP box, enter the primary Internet CPE's IP address. (Example: 172.17.130.126)



Step 14: In the Metric box, enter 50, and then click OK.

Edit Static Route	X			
IP Address Type:				
Interface:	outside-17 👻			
Network:	any4			
Gateway IP:	172.17.130.126 Metric: 50			
Options				
None				
Tunneled (Default tunnel gateway for VPN traffic)				
🔘 Tracked				
Track ID:	Track IP Address:			
SLA ID:	Target Interface: IPS-mgmt 👻			
Monitoring O	ptions			
Enabling the tra state of the rou	cked option starts a job for monitoring the te, by pinging the track address provided.			
ОК	Cancel Help			

Step 15: On the Static Routes pane, click Apply.

Next, you add a host route for the tracked object via the Internet-CPE-1 address. This assures that probes to the tracked object will always use the primary ISP connection.

Step 16: In Configuration > Device Setup > Routing > Static Routes, click Add.

**Step 17:** In the Add Static Route dialog box, in the **Interface** list, select the primary Internet connection interface. (Example: outside-16)

**Step 18:** In the **Network** box, enter the IP address used for tracking in the primary default route. (Example: 172.18.1.1/32)

August 2014 Series



**Step 19:** In the **Gateway IP** box, enter the primary Internet CPE's IP address, and then click **OK**. (Example: 172.16.130.126)

💁 Add Static Route				
IP Address Type:	IPv4 O IPv6			
Interface:	outside-16 🗸			
Network:	172.18.1.1/32			
Gateway IP:	172.16.130.126 Metric: 1			
Options				
None				
<ul> <li>Tunneled (Default tunnel gateway for VPN traffic)</li> </ul>				
© Tracked				
Track ID:	Track IP Address:			
SLA ID:	Target Interface: inside 🚽			
Monitoring Options				
Enabling the tracked option starts a job for monitoring the state of the route, by pinging the track address provided.				
OK Cancel Help				

Step 20: On the Static Routes pane, click Apply.

Step 21: In Cisco ASDM, refresh the configuration.

Step 22: If you want to monitor the reachability of the object, navigate to Monitoring > Interfaces > Connection outside-16 > Track Status for id-1.

### Procedure 5 Create network objects

The use of objects and group objects in the ASA appliance make its configuration more easily understood. The following steps create a series of objects that represent the WLCs in your environment.



Table 22 - Wireless LAN Controller network objects

Network object name	Object type	IP address
internal-wlc2504-1	Host	10.4.175.62
internal-wlc2504-2	Host	10.4.175.63
internal-wlcWiSM2-HA-SSO	Host	10.4.174.64
internal-wlc-5508-HA-SSO	Host	10.4.175.66
internal-wlc5760-SSO-Pair	Host	10.4.175.68
internal-wlc_vWLC-1	Host	10.4.59.58
internal-wlc_vWLC-2	Host	10.4.59.59
internal-wlc7510-Flex-HA-SSO	Host	10.4.59.68
dmz-wlc2504-1	Host	192.169.19.25
dmz-wlc2504-2	Host	192.168.19.26
dmz-wlc5508-HA-SSO	Host	192.168.19.54

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

**Step 2:** Repeat Step 3 through Step 6 for all objects listed in Table 22. If the object already exists, then skip to the next object in the table.

### Step 3: Click Add > Network Object.

The Add Network Object dialog box appears.

**Step 4:** In the **Name** box, enter a description of the WLC. (Examples: internal-wlc-5508-HA-SSO, internal-wlc7510-Flex-HA-SSO, internal-wlc5760-SSO-Pair)

Step 5: In the Type list, choose Host.

**Step 6:** In the **IP Address** box, enter the WLC's management interface IP address, and then click **OK**. (Example: 10.4.175.66)

🖆 Edit Network	Object	×
Name:	internal-wlc5508-HA-SSO	
Туре:	Host	-
IP Version:	● IPv4	
IP Address:	10.4.175.66	
Description:	HA SSO Redundant Pair WLC5508 in Services Block	
NAT		*
	OK Cancel Help	
Next, to simplify the security policy configuration for similar network objects, you create network object groups that will contain the individual WLCs specific to their places in the network (PIN).

Table 23 -	Wireless LAN controller object groups	

Network object group name	Network objects	Description
internal-wlc-group	internal-wlc2504-1	Internal Wireless LAN Controllers
	internal-wlc2504-2	
	internal-wlcWiSM2-HA-SSO	
	internal-wlc-5508-HA-SSO	
	internal-wlc5760-SSO-Pair	
	internal-wlc_vWLC-1	
	internal-wlc_vWLC-2	
	internal-wlc7510-Flex-HA-SSO	
dmz-wlc-group	dmz-wlc2504-1	DMZ Wireless LAN Controllers
	dmz-wlc2504-2	
	dmz-wlc5508-HA-SSO	

#### Step 7: Click Add > Network Object Group.

**Step 8:** Repeat 0 and Step 10 for each WLC Place in the Network from Table 23 (Example: internal-wlc-group) The Add Network Object Group dialog box appears.

Step 9: In the Group Name box, enter a name for the group.

**Step 10:** In the Existing Network Objects/Groups pane, select every WLC specific to its location in the network and then click **Add** to move each Network Object into the Network Object Group.

Group Name: interna	l-wlc-group						
Description: Interna	al Wireless LAN Contro	ollers					
Existing Network	Objects/Groups:				Members in Group:		
Ceate new Network	DipletSynops: IP Address IP Address IP 24.103.19.35 IP 21.08.19.55 IP 21.08.19.75 IP 21.08.19.75 IP 21.08.19.75 IP 21.08.19.75 IP 21.08.19.75 IP 21.08.19.75 IP 21.08.49.75 IP 21.08.48.10 IP 448.10 IP 448.11 IP 448.17 IP 448.42 IP 448.42	Netmask 255,255,252,0 255,254,0,0 255,254,0,0	Description GLESS WLC3506-2 HA SSO Redundar Guest WLC5760-1 Guest WLC5760-1 Internal T/510 Flex Internal T/510 Flex Internal T/510 Flex Internal INTP serve Internal INTP serve Internal ISE Server Wireless LAN Com DMZ Wireless LAN	Add >> << Remove	Members in Group: Name Internal-WUC-1 Internal-S04-1 Internal-S04-2 Internal-S04-2 Internal-S04-3 Internal-S04-4 Internal-S04-3 Internal-Wic5760-S00-Pair	P Address 10.4.59.58 10.4.59.59 10.4.175.62 10.4.175.62 10.4.175.68 10.4.175.68 10.4.175.68 10.4.175.68	NetmackPrefix Length
Name: (optional)							
Type:	Host			•			
IP Version:	🧿 IPv4   🔘 IPv6						
IP Address:							
					<		, the second sec
			ОК	Cancel	нею		

Step 11: Review the configured Network Object Groups for completeness, and then click OK.

Configuration > Firewall > Objects > Network Objects/Groups						
💠 Add 🔹 🗹 Edit 👔 Delete   🔍 Where Used 🔍 Not (	Jsed					
Filter:				Filter Clear		
Name	IP Address	Netmask	Description	Object NAT A		
Network Objects						
Network Object Groups						
😑 🚅 dmz-wic-group						
- 🖪 dmz-wlc2504-1	192.168.19.25		DMZ WLC Anchor Controller 2504-1			
- 📇 dmz-wlc2504-2	192.168.19.26		DMZ WLC Anchor Controller 2504-2			
dmz-wic5508-HA-SSO	192.168.19.54		DMZ WLC Anchor Controller 5508 HA SSO Pair			
🖶 🚟 dmz-wlc-redundancy-group						
🕀 🎆 internal-ISE-Servers						
🗄 🎆 internal-wic-group			Internal Wireless LAN Controllers			
- 📇 internal-wlc2504-1	10.4.175.62		Internal 2504-1 WLC			
Internal-wlc2504-2	10.4.175.63		Internal 2504-2 WLC			
- 📇 internal-wlc5508-HA-SSO	10.4.175.66		HA SSO Redundant Pair WLC5508 in Services B.			
Internal-wlc5760-HA-SSO	10.4.175.68		HA Redundant Pair WLC 5760 in Services Block			
- 📇 internal-wic7510-Flex-HA-SSO	10.4.59.68		HA SSO Redundant Pair WLC7510 Flex Controlle			
Internal-wic_wWLC-1	10.4.59.58		Internal vWLC-1 WLC			
📇 internal-wic_vWLC-2	10.4.59.59		Internal vWLC-1 WLC			
Internal-wicWiSM2-HA-SSO	10.4.175.64		HA SSO Redundant Pair WLC WISM2 in Service			

When a HA SSO WLC is in HOT STANDBY mode, the redundancy port is used to communicate with the internal NTP server for time synchronization. Since either of the WLCs in HA SSO mode could be in the HOT STANDBY, you need to create network objects that identify each of the redundancy ports for both controllers in the high availability pair.

Table 24 - DMZ HA Wireless LAN Controller RP Network Objects

Network object name	Object type	IP address
dmz-wlc-primary-5508-RP	Host	192.168.19.154
dmz-wlc-secondary-5508-RP	Host	192.168.19.155

**Step 12:** Repeat steps Step 13 through Step 15 for each of the DMZ based HA SSO Redundancy Ports shown in Table 24.

The Add Network Object dialog box appears.

Step 13: In the Name box, enter a description of the WLC. (Example: dmz-wlc-primary-5508-RP)

Step 14: In the Type list, choose Host.

Step 15: In the IP Address box, enter the primary WLC's redundancy-port interface IP address, and then click OK. (Example: 192.168.19.154)

靖 Add Network	k Object	×
Name:	Hmz-wlc-primary-5508-RP	
Туре:	Host	•
IP Version:	IPv4 O IPv6	
IP Address:	192.168.19.154	
Description:	Primary WLC Redundancy Port	
NAT		×
001		Ť
	OK Cancel Help	

Next, to simplify the security policy configuration for each HA SSO based controller in the DMZ, you create a network object group that will contain each of the individual HA SSO WLCs within the DMZ.

Table 25 - DMZ wireless LAN controller HA SSO redundancy port object group

Network object Group name	Network Objects	Description
dmz-wlc-redundancy-group	dmz-wlc-5508-primary-RP dmz-wlc-5508-secondary-RP	DMZ wireless LAN controllers redundancy port group

**Step 16:** Create a network object group that groups each of the redundancy ports on any HA SSO controller within the DMZ, as shown in Table 25. (Example: dmz-wlc-redundancy-group).

Surption:         Livitz Wireless Law Controller's Redundancy Port Group           Existing Network Objects/Groups:         Members in Group:           Name         IP Address         Netring           Bit dotts         Netring         IP Address         IP Address           Bit dotts         Netring         IP Address         Netring           Bit dotts         Netring         IP Address         IP Address           Bit dotts         Netring         IP Address         IP Address           Bit dotts         Netring         IP Address         IP Address           Bit dotts         IP Address         IP Address         IP Address           Bit dotts         IP Address         IP Address         IP Address           Bit memal-Network         IP Address         IP Address         IP Address           Bit memal-Network         IP Address	Members in Group:         Members in Group: <sup>A1</sup> <sup>IP</sup> <sup>Address</sup> Netroit Sole-perimary-RP <sup>A1</sup> <sup>IP</sup> <sup>Address</sup> Netroit Sole-perimary-RP <sup>A22, Address</sup> Netroit <sup>A22, Address</sup> 104, 175, 68 <sup>IP</sup> Address          Idm2-wilc <sup>IP</sup> Address          Netroit <sup>IP</sup> Address          Netroit <sup>IP</sup> Address          Netroit <sup>IP</sup> Address          Idm2-wilc              <	minting .	This cash and group	na Dadardana D							
Bit once         IP Address         Netro         IP Address         Netro           Image: Once Web/Yob 2         122.000137/0         Name         IP Address         IP Address           Image: Once Web/Yob 2         122.000137/0         255.2         Image: Once Web/Yob 2         Image: Once Web/Yob	Objects/Groups:         Members in Group:           Name         IP Address         Netmasking           VetWork         192,168,28,0         255,2           Ve5004         104,175,62         Intervise           VetWork         104,175,62         Intervise           VetWork         104,475,62         Intervise           VetWork         104,475,62         Intervise           VetWork         104,475,62         Intervise           VetWork         104,475,62         Intervise           VetWork         104,475,63         Intervise           VetWork         104,48,10         Intervise           VetWork         104,475,63         Intervise           VetWork         104,48,10         Intervise           Vetwork         104,48,17         Intervise           Vetwork         104,175,64         Intervise           Vetwork         104,175,64         Intervise           Vetwork         104,48,41         Intervise	cription: DIVI2	Wireless LAN Controlle	ers Redundancy Por	t Group						
Lexiting Network Ubjects/groups:         Mame         All         IP Address           Name         IP Address         Netm           Bit Nutz, Web/Work         192.166.28.0         255.2           Bit Internal-2504-1         104.175.62           Bit Internal-7510-4         104.475.63           Bit Internal-7510-1         104.475.63           Bit Internal-7510-1         104.475.63           Bit Internal-7510-1         104.48.10           Bit Internal-7510-1         104.48.10           Bit Internal-Network         104.40.0           Bit Internal-Network         104.40.0           Bit Internal-Network-10.0.4.0.0         255.2           Bit Internal-WitS090-HA-SSO         104.175.66           Bit Internal-WitS090-HA-SSO         104.4275.66           Bit Inte	Collect/products:         Image: Mathematical Statute         Image: Mathematical Statute         Image: Mathematical Statute         Native           And Image: Mathematical Statute         192.168.28.00         255.2         Image: Mathematical Statute         <							Mandaana in Cusum			
Name         IP Address         Netn           Image: Internal-Reserved 2         422.000.157/0         102.166.20.0           Image: Internal-2504-1         104.175.62         255.2           Image: Internal-2504-2         104.175.63         255.2           Image: Internal-2504-2         104.175.63         255.2           Image: Internal-2504-2         104.475.63         255.2           Image: Internal-7510-2         104.490.66         255.2           Image: Internal-retwork-ISPa         10.4.48.10         255.2           Image: Internal-retwork-ISPa         10.4.48.10         255.2           Image: Internal-retwork-ISPa         10.4.48.17         255.2           Image: Internal-retwork-ISPa         10.4.48.17         255.2           Image: Internal-retwork-ISPa         10.4.475.66         255.2           Image: Internal-retwork-ISPa         10.4.39.59         255.2           Image: Internal-retwork-ISPa         10.4.48.17         255.2           Image: Internal-retwork-ISPa         10.4.175.66         255.2           Image: Internal-retwork-ISPa         10.4.175.66         255.2           Image: Internal-retwork-ISPa         10.4.175.66         255.2           Image: Internal-retwork-ISPa         10.4.175.66         255.2 <td>Name         IP Address         Netmas           Network         192.168.28.0         255.2           1-2504-1         10.4.175.63         1           1+7510-2         10.4.175.63         1           1+7510-2         10.4.175.63         1           1+7510-2         10.4.175.63         1           1+7510-1         10.4.48.10         1           1+7510-2         10.4.49.58         1           1+7510-1         10.4.48.10         1           1+7510-1         10.4.48.10         1           1+7510-2         10.4.175.63         1           1+7510-1         10.4.59.59         1           1+retwork-1SPa         10.4.00         255.2           I+retwork-1SPa         10.4.175.64         1           1+webc250-520-320-1         10.4.175.64         1           1+webc250-5500-320         10.4.175.66         1           1-wist508+HA-SS0         10.4.175.66         1           1SE=1         10.4.48.41         T</td> <td>Existing Networ</td> <td>rk Objects/Groups:</td> <td></td> <td></td> <td></td> <td></td> <td>members in a oup.</td> <td></td> <td></td> <td></td>	Name         IP Address         Netmas           Network         192.168.28.0         255.2           1-2504-1         10.4.175.63         1           1+7510-2         10.4.175.63         1           1+7510-2         10.4.175.63         1           1+7510-2         10.4.175.63         1           1+7510-1         10.4.48.10         1           1+7510-2         10.4.49.58         1           1+7510-1         10.4.48.10         1           1+7510-1         10.4.48.10         1           1+7510-2         10.4.175.63         1           1+7510-1         10.4.59.59         1           1+retwork-1SPa         10.4.00         255.2           I+retwork-1SPa         10.4.175.64         1           1+webc250-520-320-1         10.4.175.64         1           1+webc250-5500-320         10.4.175.66         1           1-wist508+HA-SS0         10.4.175.66         1           1SE=1         10.4.48.41         T	Existing Networ	rk Objects/Groups:					members in a oup.			
at Unite Web/Yob 2         192:100:15/10           -all Once Web/Yob 2         192:168:28:0         255:2           -all Once Web/Yob 2         104:175:62         255:2           -all Internal-2500+1         104:175:63         2           -all Internal-7510-2         104:39:69         2           -all Internal-7510-2         104:39:69         2           -all Internal-7510-2         104:39:69         2           -all Internal-7510-2         104:49:10         2           -all Internal-frame-frame         104:48:10         2           -all Internal-retwork         10:44:80         2           -all Internal-retwork         10:44:80         2           -all Internal-retwork         10:44:89:58         4           -all Internal-work         10:44:89:58         4           -all Internal-work         10:45:95:59         4           -all Internal-work         10:45:95:59         4           -all Internal-work         10:41:75:66         4           -all Internal-work         10:41:75:66         4           -all Internal-work         10:41:75:66         4           -all Internal-Web/Sto0-Sto-Pair         10:41:75:66         4           -all Internal-Web/Sto0-Sto-Pair         10	Kurrov 2     122.100.157/0       Network     102.168.28.0       125.168.28.0     255.2       1-2504-1     10.4.175.62       1-7510-1     10.4.59.69       1-7510-1     10.4.59.68       1-6hs     10.4.48.10       1-hots     10.4.175.64       1-wwxC-2     10.4.175.64       1-wwxDc-2     10.4.175.64       1-wwxDc760-SSO-Pair     10.4.175.64       1-wwxDc760-SSO-Pair     10.4.175.66       1-wwxDc760-SSO-Pair     10.4.175.66       1-wwxDc760-SSO-Pair     10.4.175.68       1055-1     10.4.175.64	Name	~ 1	IP Address	Netrr			Name		IP Address	Netmas
■ Guest-Network       192.166.28.0       255.2         ■ Internal-2504-1       10.4.175.62       10.4.175.63         ■ Internal-7510-4       10.4.175.63       10.4.59.68         ■ Internal-7510-10-4       10.4.89.68       10.4.89.68         ■ Internal-retwork       10.4.0.0       255.2         ■ Internal-network       10.4.0.0       255.2         ■ Internal-network       10.4.0.0       255.2         ■ Internal-network-15Pa       10.4.0.0       255.2         ■ Internal-web/x0-C-1       10.4.59.59       10.4.175.66         ■ Internal-wit/S500-HA-SSO       10.4.175.66       10.4.175.66         ■ Internal-wit/S50-SSO-Pair       10.4.175.66          ■ Internal-wit/S50-SSO-Pair       10.4.495.66          ■ Internal-wit/S500-HA-SSO       10.4.175.66          ■ Internal-wit/S50-SSO-Pair       10.4.175.66          ■ Internal-wit/S50-SSO-Pair       10.4.492.10	Network 192.168.28.0 255.2 +2504-1 104.175.62 +2504-2 10.4.175.63 +7510-2 10.4.59.68 +7510-4 10.4.48.10 +6dns 10.4.48.10 +6dns 10.4.48.10 +6dns 10.4.48.10 +1retwork-ISPa 10.4.00 255.2 +1retwork-ISPa 10.4.00 255.2 +1retwork-ISPa 10.4.00 255.2 +1retwork-ISPa 10.4.00 255.2 +1retwork-ISPa 10.4.175.64 +wic5760-SSO-Pair 10.4.175.66 +wic5760-SSO-Pair 10.4.175.66 +wic5760-SSO-Pair 10.4.175.66 +wic5760-SSO-Pair 10.4.175.66 +wic5760-SSO-Pair 10.4.175.66 +wic5760-SSO-Pair 10.4.175.66	a unz	WIL3/00 Z	172.100.17.70				💬 🖪 dmz-wlc-5508-primary	/-RP	192.168.19.154	
	Add >> Add >> Add >> Add >> Add >> Add >> Add >>	- 🛃 Gues	t-Network	192.168.28.0	255.2			🛄 🖳 dmz-wlc-5508-second	ary-RP	192.168.19.155	
→ Sinternal+2504-2       10.4.175.63         → Sinternal+7510-2       10.4.595.69         → Sinternal+7510-2       10.4.595.69         → Sinternal+6trop       10.4.48.10         → Sinternal+6trop       10.4.48.10         → Sinternal+6trop       10.4.48.10         → Sinternal+6trop       10.4.48.10         → Sinternal+6trop       10.4.48.17         → Sinternal+6trop       10.4.48.17         → Sinternal+6trop       10.4.48.17         → Sinternal+6trop       10.4.59.59         → Internal+WLC-2       10.4.59.59         → Internal+WLC-2       10.4.175.64         → Sinternal+WC550-FAsc       10.4.175.66         → Sinternal-WC550-FAsc       10.4.175.66         → Sinternal-WC550-Fasc       10.4.175.66	h-250-2 10.4.175.63 h-7510-4A-SSO 10.4.59.69 h-7510-HA-SSO 10.4.59.68 h-dhcp 10.4.48.10 h-dhc 10.4.48.10 h-network 10.4.0.0 255.2 h-retwork-1SPa 10.4.0.0 255.2 h-retwork-1SPa 10.4.0.0 255.2 h-retwork-1SPa 10.4.0.0 255.2 h-retwork-1SPa 10.4.175.64 h-wic5509-HA-SSO 10.4.175.64 h-wic5509-SBO-Pair 10.4.175.66 h-wic5560-SBO-Pair 10.4.175.66 h-wic5560-SBO-Pair 10.4.175.66 h-wic5560-SBO-Pair 10.4.175.66 h-wic5560-SBO-Pair 10.4.175.66 h-wic5560-SBO-Pair 10.4.175.66 h-wic5560-SBO-Pair 10.4.175.66	- 📇 interi	nal-2504-1	10.4.175.62							
■ Internal-7510-12       10.4.59.69         ■ Bit Internal-7510-14A-SSO       10.4.89.68         ■ Internal-drop       10.4.48.10         ■ Bit Internal-Intervork       10.4.00         ■ Internal-Intervork       10.4.0.0         ■ Internal-Intervork       10.4.99.58         ■ Bit Internal-WUC-1       10.4.99.59         ■ Internal-WitSSO       10.4.175.64         ■ Internal-WitSSO       10.4.175.66         ■ Internal-WISSO       10.4.175.66         ■ Internal-WISSO       10.4.175.66	H-7510-2 10.4.59.69 H-7510-HA-SSO 10.4.59.68 H-dhcp 10.4.48.10 H-dhs 10.4.48.10 H-dhs 10.4.48.10 H-dhs 10.4.48.10 H-wwork-ISPa 10.4.00 255.2 H-metwork-ISPa 10.4.059.59 H-wwLC-2 10.4.59.59 H-wwLC-2 10.4.59.59 H-wwS508-HA-SSO 10.4.175.66 H-wlC5500-SSO-Pair 10.4.175.66 H-MLC5500-SSO-Pair 10.4.175.66 H-MLC5	- 📇 interi	nal-2504-2	10.4.175.63							
■ Internal-75:10+HA-SSO       10.4.59:68         ■ Sinternal-drop       10.4.84:10         ■ Internal-retwork       10.4.48:10         ■ Internal-network       10.4.0.0         ■ Internal-network       10.4.0.0         ■ Internal-retwork       10.4.99:58         ■ Internal-WULC-1       10.4.59:59         ■ Internal-WULC-2       10.4.59:59         ■ Internal-WULC-2       10.4.75:64         ■ Internal-WUS500-HA-SSO       10.4.175:66         ■ Internal-WUS500-Fair       10.4.475:68	Ir751014A-SSO 10.4.59.68 Ir4dnp 10.4.48.10 Ir4ns 10.4.0.0 255.2 Ir4np 10.4.48.10 Ir4nstvork 10.4.0.0 255.2 Ir4np 10.4.48.17 Ir4WLC-2 10.4.59.58 Ir4WLC-2 10.4.59.59 Ir4WSm2+HA-SSO 10.4.175.64 Ir4WIC5500-SSO-Pair 10.4.175.68 Ir4NS5760-SSO-Pair 10.4.175.68 Ir5E-1 10.4.48.41 WI ► ►	- 🖪 interi	nal-7510-2	10.4.59.69							
	H-dhcp 10.4.48.10 H-dhc 10.4.48.10 H-network 10.4.0.0 255.2 H-network:EPa 10.4.0.0 255.2 H-mby 10.4.48.17 H-why T-1 10.4.59.58 H-WLC-2 10.4.59.59 H-WLC-2 10.4.59.59 H-WLC5500-HA-SSO 10.4.175.64 H-wLC5760-SSO-Par 10.4.175.66 H-WLC5760-SSO-Par 10.4.175.66 H-WLC5760-SSO-Par 10.4.175.68 HT ►	- 📇 interi	nal-7510-HA-SSO	10.4.59.68							
- Bi Internal-dros         10.4.48.10           - Bi Internal-network         10.4.0.0         255.2           - Bi Internal-network-ISPa         10.4.0.0         255.2           - Bi Internal-NWLC-1         10.4.99.59         E           - Bi Internal-WUC-2         10.4.99.59         E           - Bi Internal-WicS00 FIA-SS0         10.4.175.66         E           - Bi Internal-WicS00-FAA-SS0         10.4.175.66         <	H-dns 10.4.48.10 H-retwork-ISPa 10.4.0.0 255.2 H-retwork-ISPa 10.4.48.17 H-WMLC-1 10.4.59.58 H-WMLC-2 10.4.59.59 H-WMC5508-HA-SSO 10.4.175.66 H-WC5508-HA-SSO 10.4.175.66 H-WC5508-HA-SSO 10.4.175.66 H-WC5508-HA-SSO 10.4.175.66 H-WC5508-HA-SSO 10.4.175.66 H-WC5508-HA-SSO 10.4.175.66	- 🖪 interi	nal-dhcp	10.4.48.10							
→ memainetwork         10.4.0.0         255.2           → memainetwork         10.4.0.0         255.2           → memainetwork         10.4.0.0         255.2           → memainetwork         10.4.48.17         Ξ           → memainetwork         10.4.59.59         Ξ           → memainetwork         10.4.59.59         Add >>           → memainetwork         10.4.175.64         Add >>           → memainetwork500-50-Par         10.4.175.66         <	linetwork 10.4.0.0 255.2 linetwork 10.4.0.0 255.2 linetwork 10.4.0.0 255.2 linetwork 10.4.48.17 linetwork 20.4.48.17 linetwork 20.4.475.68 lise 10.4.175.68 lise 10.4.175.68 lise 10.4.175.68 lise 10.4.185.68 lise 10.4.	Binternal-ndtwork     Binternal-network     Binternal-network     Binternal-network     Binternal-wtp     Binternal		10.4.48.10							
→ Bit memal-http       10.4.0.0       255.2         → Bit memal-http       10.4.48.17       Image: State	linetwork:ISPa 10.4.0.0 255.2 http://dx.17 10.4.59.58 http://dx.17 10.4.59.58 http://dx.17 10.4.59.59 http://dx.17 10.4.175.64 http://dx.17 10			10.4.0.0	255.2						
→ Binternal-wup         10.4.49.1/           → Binternal-WUC-1         10.4.59.59           → Binternal-WUC-2         10.4.59.59           → Binternal-Wic500+Na/SSO         10.4.175.66           → Binternal-Wic550+Na/SSO         10.4.175.66           → Binternal-Wic550+Na/SSO         10.4.175.66           → Binternal-Wic550+Na/SSO         10.4.175.66	H-rhp 10.4.48.17 ■ H-WALC-1 10.4.59.58 ■ H-WALC-2 10.4.59.59 ■ H-WISS508-HA-SSO 10.4.175.66 ■ H-WISS509-HA-SSO 10.4.175.66 ■ H-WISS500-SD-Pair 10.4.175.68 ■ USE-1 10.4.48.41 ▼			10.4.0.0	255.2						
	l+vwLC-1 10.4.59.59 l+vwLSSO 10.4.175.64 l+vwLSSO 10.4.175.64 l=vsLSSO +SO-Pair 10.4.175.66 l_SE-1 10.4.48.41 ▼ III ▶			10.4.48.17		=					
	Add >> Add Add Add Add Add Add Add Add Add Add			10.4.59.58							
	I-WISTRG+HA-SSO 10.4.175.64 I-WIC5508-HA-SSO 10.4.175.66 I_JISE-1 10.4.48.41 ▼ III ▶			10.4.59.59			Add >>				
nema+wic5308-Ha-SSU 10.4.1/5.66     internal-wic5760-SSO-Pair 10.4.1/5.66     internal-wic5760-SSO-Pair 10.4.48.41	III 0.4.175.66 IJSE-1 10.4.48.41 ~			10.4.1/5.64		-13					
- 3 internal Wic5/00-550-Yarr 10.4.1/5.08	III + 10.4.48.41 +			10.4.175.66			<< Remove				
				10.4.1/5.68		_ [ ]					
	► THE SECOND SECONDO SECOND SECOND SECONDO SECON	- as nen	nal_15E-1	10.4.48.41		Ť					
		•	111		•						
Create new Network Object member:		Name: (option	al)								
Name: (optional)		Type:	Host			-					
Name: (optional) Type: Host	Host	IP Version:	IPv4								
Name: (optional) Type: Host  Version: 0 Prv4  Prv6	 Host ● IPv4	IP Address									
Version:     IP Version:       IP Version:     IP Version:	Host Prv4  Prv6	1 Mului 855.				_		1			



Step 17: On the Add Network Object Group dialog box, click OK.

Procedure 6 Configure dedicated guest anchor WLC security policy

The anchor controllers located in the DMZ need to communicate to the internal network for a number of services such as RADIUS, TACACS+, NTP, FTP and CAPWAP. This procedure provides connectivity from the dmz-mgmt-wlan (VLAN 1119) to the internal network.

Step 1: On the Internet edge ASA appliance, navigate to Configuration > Firewall > Access Rules.

Step 2: Repeat Step 3 through Step 11 for all rules listed in Table 26.

i	Tech Tip
Step :	3 is important for keeping the rules in the correct order.

Table 26 - Firewall policy rules for DMZ WLC Management Interface

Interface	Action	Source	Destination	Service	Description	Logging Enable / Level
Any	Permit	dmz-wlc-group	internal-aaa	tcp/tacacs, udp/1812, udp/1813	Allow DMZ based WLC's to com- municate with the AAA/ACS Server on the internal network.	Selected / Default
Any	Permit	dmz-wlc-group	internal-ntp	udp/ntp	Allow WLC's to communicate with the NTP server located in the data center.	Selected / Default
Any	Permit	dmz-wlc-group	any	tcp/ftp, tcp/ ftp-data	Allow the WLC's to communicate with any FTP server.	Selected / Default
Any	Permit	dmz-wlc-group	internal-wlc- group	97, udp/16666, udp/5246, udp/5247	Allow DMZ based WLC's to com- municate with the internal WLC's	Selected / Default
Any	Permit	dmz-wlc-group	internal-dhcp	udp/bootps	Allow DMZ WLC's to obtain IP address via internal DHCP server	Selected / Default
Any	Permit	dmz-wlc- redundancy- group	internal-ntp	udp/ntp	Allow Standby HA SSO WLC's to communicate to internal NTP server using RP port	Selected / Default

Step 3: Click the rule that denies traffic from the dmz-networks towards the internal network.

🔽 📲 dmz-networks

🌍 any

😣 Deny

IP ip

#### Caution

Be sure to perform this step for *every* rule listed in Table 26. Inserting the rules above the DMZ-to-any rule keeps the added rules in the same order as listed, which is essential for the proper execution of the security policy.

Step 4: Click Add > Insert.

Step 5: In the Interface list, choose the interface. (Example: Any)

Step 6: For the Action option, select the action. (Example: Permit)

Step 7: In the Source box, choose the source. (Example: dmz-wlc-group)

Step 8: In the Destination box, choose the destination. (Example: internal-aaa)

Step 9: In the Service box, enter the service. (Example: tcp/tacacs, udp/1812, udp/1813)

Step 10: In the Description box, enter a useful description.

Step 11: Select or clear Enable Logging. (Example: Selected)

Step 12: In the Logging Level list, choose the logging level value, and then click OK. (Example: Default)

Add Access	Rule					
Interface:	Any 👻					
Action: 💿 Perr	nit 💿 Deny					
Source Criteria						
Source:	dmz-wlc-group					
User:						
Security Group:	· · · · · · · · · · · · · · · · · · ·					
Destination Crite	eria					
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 Logging						
Logging Leve	el: Default 🗸					
More Options	¥					
	OK Cancel Help					

Step 13: After adding all of the rules and in the order listed in Table 26, click Apply on the Access Rules pane.

19	$\checkmark$	🏽 dmz-wlc-group	🚇 internal-aaa	100 tacacs 1812 100 1813	🖌 Permit	450	Allow DMZ based WLC's to communicate with the AAA/ACS Server on the internal network.
20	-	😹 dmz-wlc-group	📇 internal-ntp	🚥 ntp	🖌 Permit	0	Allow WLC's to communicate with the NTP server located in the data center.
21	<b>v</b>	👷 dmz-wlc-group	any	ໝ⊳ ftp ໝ> ftp-data	🖌 Permit	0	Allow the WLC's to communicate with any FTP server.
22	<b>V</b>	😹 dmz-wlc-group	🗰 internal-wic-group	→ 97 16666 5246 5247	🖌 Permit	0	Allow DMZ based WLC's to communicate with the internal WLC's
23	-	🐖 dmz-wlc-group	📇 internal-dhcp	🐲 bootps	🖌 Permit	0	Allow DMZ WLC's to obtain IP address via internal DHCP server
24	1	🕷 dmz-wic-redundancy-group	📇 internal-ntp	💵 ntp	🖌 Permit	0	Allow Standby HA SSO WLC's to communicate to internal NTP server using RP port
25	177	- dmz-potworke	Average 1	TR in	Dopy	102 ->	Denv IP traffic from DM7 to any other network

### Procedure 7 Configure guest network security policy

In this procedure, the access policy for the guest wireless hosts will be applied to allow outbound traffic to the Internet. It will also restrict all internal access, with a few exceptions such as DNS, DHCP, and HTTP/HTTPS for DMZ web services such as walled gardens.

Interface	Action	Source	Destination	Service	Description	Logging enable/level
Any	Permit	dmz-guest-wlan-network	internal-dns	tcp/domain, udp/domain	Allow Guest Wireless users to resolve DNS names	Selected / Default
Any	Permit	dmz-guest-wlan-network	internal-dhcp	udp/bootps	Allow wireless guest users to obtain/renew an IP address from the internal DHCP server	Selected / Default
Any	Permit	dmz-guest-wlan-network	dmz-web-network	tcp/http, tcp/ https	Allow wireless guest users access to DMZ based web servers, possibly for walled garden access	Selected / Default
Any	Deny	dmz-guest-wlan-network	dmz-networks, internal-network	ip	Deny traffic from the wireless guest network to the internal and DMZ resources	Selected / Default
Any	Permit	dmz-guest-wlan- network/22	Any	ip	Allow wireless DMZ users access to the Internet	Selected / Default

Table 27 - Gues	network policy r	ules
-----------------	------------------	------

Step 1: On the Internet edge ASA appliance, navigate to Configuration > Firewall > Access Rules.

Step 2: Repeat Step 3 through Step 12 for all rules listed in Table 27.



Step 3: Click the rule that denies traffic from the DMZ toward other networks.

24	🛃 dmz-networks	1	🅎 any	IP ip	😣 Deny



Be sure to perform this step for *every* rule listed in Table 27. Inserting the rules above the DMZ-to-any rule keeps the added rules in the same order as listed, which is essential for the proper execution of the security policy.

Step 4: Click Add > Insert.

- Step 5: In the Interface list, choose the interface. (Example: Any)
- Step 6: For the Action option, select the action. (Example: permit)
- Step 7: In the Source box, choose the source. (Example: dmz-guest-wlan-network)
- Step 8: In the Destination box, choose the destination. (Example: internal-dns)
- Step 9: In the Service box, enter the service. (Example: tcp/domain, udp/domain)
- Step 10: In the Description box, enter a useful description.
- Step 11: Select or clear Enable Logging. (Example: Selected)

Step 12: In the Logging Level list, choose the logging level value, and then click OK. (Example: Default)

Step 13: After adding all of the rules in Table 27 in the order listed, on the Access Rules pane, click Apply.

27	1	n dmz-guest-wlan-network/22	📇 internal-dns	🚥 domain 🚥 domain	🖌 Permit	0	Allow Guest Wireless users to resolve DNS names.
28	1	🚔 dmz-guest-wlan-network/22	📇 internal-dhcp	🚥 bootps	🖌 Permit	0	Allow wireless guest users to obtain/renew an IP address from the internal DHCP server
29	1	🚮 dmz-guest-wlan-network/22	🚔 dmz-web-netw	ໝ∾http ™ohttps	🖌 Permit	0	Allow wireless guest users access to DMZ based webservers, possibly for walled garden access
30	<b>v</b>	룖 dmz-guest-wlan-network/22	dmz-networks 感 internal-network	up ⊴∎	😮 Deny	0	Deny traffic from the wireless guest network to the internal and dmz resources
31	1	🖷 dmz-guest-wlan-network/22	any	📧 ip	🖌 Permit	0	Allow Wireless DMZ users access to the Internet
32	<b>V</b>	🚅 dmz-networks	🚳 any4	IP ip	😣 Deny	10F 3	Deny IP traffic from DMZ to any other network.

Configure the HA SSO based DMZ wireless LAN guest anchor controller by using the following values.

Parameter	CVD values primary controller	CVD values resilient controller	Site-specific values					
Controller parameter	rs							
Switch interface number	1/0/13, 2/0/13	1/0/14, 2/0/14						
VLAN number	1119	N/A						
Time zone	PST -8 0	N/A						
IP address	192.168.19.54/24	N/A						
Default gateway	192.168.19.1	N/A						
Redundant manage- ment IP address (AP SSO)	192.168.19.154	192.168.19.155						
Redundancy port connectivity HA SSO)	Dedicated Ethernet cable	Dedicated Ethernet cable						
Hostname	DMZ-WLC5508-Guest-1	N/A						
Local administra- tor username and password	admin/C1sco123	N/A						
Mobility group name	5508Guest	N/A						
Primary ISE RADIUS server IP address	10.4.48.41	N/A						
Secondary ISE RADIUS server IP address	10.4.48.42	N/A						
RADIUS shared key	SecretKey	N/A						
Management network (optional)	10.4.48.0/24	N/A						
ACS TACACS server IP address	10.4.48.15	N/A						
TACACS shared key (optional)	SecretKey	N/A						
Wireless data network parameters								
SSID	Guest or 5508Guest, WiSM2Guest, vWLC- Guest, 7510Guest	N/A						
VLAN number	1128	N/A						
Default gateway	192.168.28.1	N/A						
Controller wireless data interface IP address	192.168.28.54	N/A						

Table 28 - Cisco DMZ wireles	s controller parameters checklist
------------------------------	-----------------------------------

OO Reader Tip

This section of the guide uses the Cisco 5508 Series Wireless Controller guest as the SSID to provide clarity as to which DMZ-based wireless anchor controller is being configured.

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

Step 1: Terminate the autoinstall process.

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

Step 2: Enter a system name. (Example: DMZ-WLC5508-Guest-1)
System Name [Cisco\_7e:8e:43] (31 characters max): DMZ-WLC5508-Guest-1

Step 3: Enter an administrator username and password.

Tech Tip

i

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 4: Use DHCP for the service port interface address.

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

**Step 5:** 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: 255.255.0 Management interface Default Router: 192.168.19.1 Management Interface VLAN Identifier (0 = untagged): 1119

Step 6: Enter the default DHCP server for clients. (Example: 10.4.48.10)

Management Interface DHCP Server IP Address: 10.4.48.10

**Step 7:** If you are deploying a Cisco 5500 Series Wireless LAN Controller and you want to enable HA SSO, enable high availability.

```
Enable HA [yes][NO]: YES
Configure HA Unit [Primary][secondary]: [Primary or Secondary]
Redundancy Management IP Address: 192.168.19.154
Peer Redundancy Management IP Address: 192.168.19.155
```

**Step 8:** The virtual interface is used by the WLC for mobility DHCP relay and inter-controller 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:** 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: 239.54.54.54
```

i	Tech Tip						
The D	MZ-based guest anchor controller does not provide multicast services to guest						
users, but the Cisco 2500 Series WLC startup wizard requires an entry be made here.							
in the	campus must have a unique multicast IP address.						

Step 10: Enter a name for the default mobility and RF group. (Example: GUEST)

Mobility/RF Group Name: 5508Guest

**Step 11:** 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 12: Enable DHCP snooping.

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

Step 13: 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 14: 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 15: 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 16: Enable the RRM auto-RF feature. This helps you keep your network up and operational. Enable Auto-RF [YES][no]: YES

Step 17: 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 18:** 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 19:** After the WLC has reset, log in to the Cisco Wireless LAN Controller Administration page by using the credentials defined in Step 3. (Example: https://dmz-wlc-guest.cisco.local/)

#### Procedure 9 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 Time zone.

cisco		<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Commands Download File Upload File Reboot Config Boot Scheduled Reboot Reset to Factory Default Set Time Login Banner	Set Time Current T Date	ime	Fri Jun 6 05:15:2 Month Day Year	28 2014		June • • • • • • • • • • • • • • • • • • •			
▶ Redundancy	Timezone	2	Hour Minutes Seconds Delta Location <sup>4</sup>			5 • 15 28 hours ( (GMT -8:00	) Pacific Time (US	lins 5 and Car	0 nada)

Procedure 10 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)

սիսիս							Sa <u>v</u> e Co	nfiguration <u>P</u> ing I	.ogout   <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBACK	
Anagement Summary SNMP General SNNP V3 Users Communities Trap Receivers Trap Logs HTTP-HTTPS Telnet-SSH Serial Port Local Management Users User Sessions	MONITOR SNMP v1 Communi IP Addres IP Mask Access M Status	WLANS / v2c Cc ty Name is	CONTROLLER DOMINITY > N cisco 10.4.48.0 255.255.255.0 Read Only • Enable •	WIRELESS ew	SECURITY	MANAGEMENT	Saye Co	nfiguration <u>Ping</u> I HELP FEEDBACK	Apply
<ul> <li>Logs</li> <li>Mgmt Via Wireless</li> <li>Software Activation</li> <li>Tech Support</li> </ul>									

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

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.

CISCO       MONTROR       WLANS       CONTROLLER       WIRELESS       SECURITY       MANAGEMENT       COMMANDS       HELP       FEEDBACK         Management       SNMP v1 / v2c Community > New         Apply         Summary       Community Name       ciscol23         Apply         General       DAdress       10.4.45.0           Apply         StNF V3 Users       Community Name       ciscol23            Apply         Trap Receivers       Trap Controls       Read/Write $ array        Status       Enable  array $	CISCO     MONITOR     WILANS     CONTROLLER     WIRELESS     SECURITY     MANAGEMENT     COMMANDS     HELP     FEEDBACK       Management     SNMP v1 / v2c Community > New     < Back     Apply       Summary     Community Name     cisco123       © General     IP Address     10.4.48.0       SINP V3 Users     IP Mask     255.255.0       Communities     Access Mode     Read/Write •       Trap Receivers     Status     Enable •       HTTP-HTTPS     Telnet-SSH       Serial Port     Local Management       Users     Joan       Magn Via Wireless     > Software Activation       > Tech Support     Fech Support	CISCO MONIT Management SNMF Summary Com SNMP IP A General IP A General SNNP V3 Users IP M Communities Acce Trap Receivers Acce Trap Controls State	OR WLANS V1 / V2C Co munity Name Idress ask ss Mode	CONTROLLER CONTRO	wireless	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP <u>F</u> EEDBACK	Apply
Management     SNMP v1 / v2c Community > New     < Back	Management     SNMP v1 / v2c Community > New     < Back	Management         SNMF           Summary         Com           SNMP         IP At           General         IP M           Communities         Accee           Trap Controls         Statu           Trap Cogs         Statu	v1 / v2c Co munity Name Idress ask ss Mode	cisco123 10.4.48.0 255.255.255.0	ew				< Back	Apply
Summary     Community Name     ciaco123       SMMP     IP Address     10.4.48.0       SRNP V3 Users     IP Mark     255.255.0       Communities     Access Mode     Read/Write •       Trap Controls     Status     Enable •       HTTP-HTTPS     Telnet-SSH       Serial Port     Local Management       Users     Juser Sessions       > Logs     Mamt Via Wireless       > Software Activation       > Tech Support	Summary     Community Name     cisco123       SNNP     IP Address     10.4.48.0       General     IP Mask     255.255.0       Communities     Access Mode     Read/Write •       Trap Receivers     Status     Enable •       HTTP-HTTPS     Telnet-SSH       Serial Port     Local Management       Users     Users       J Local Management       Users       Software Activation       > Tech Support	Summary Com SNMP IP Ar General SNMP V3 Users IP M Communities Acce Trap Receivers Trap Controls State Trap Logs	munity Name Idress ask ss Mode	cisco123 10.4.48.0 255.255.255.0						
		HTTP-HTTPS Telnet-SSH Serial Port Local Management Users User Sessions Logs Mgmt Via Wireless Software Activation Tech Support		Enable -						

Step 12: Navigate to Management > SNMP > Communities.

**Deployment Details** 

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.

սիսիս								nfiguration	n   <u>P</u> ing	Logout <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMEN	COMMANDS	HELP	<u>F</u> EEDBA	CK
Management	SNMP v1	/ v2c Cc	ommunity							New
Summary										
▼ SNMP	Communit	y Name		IP Address	IP Mask	Access	Mode Status			
General SNMP V3 Users	cisco			10.4.48.0	255.255.25	55.0 Read-C	nly Enable			
Communities Trap Receivers Trap Controls Trap Logs	cisco123			10.4.48.0	255.255.2	55.0 Read-V	rite Enable			
HTTP-HTTPS										
Telnet-SSH										
Serial Port										
Local Management Users										
User Sessions										
Logs										
Mgmt Via Wireless										
Software Activation										
Tech Support										

Step 15: Navigate to Management > SNMP > General and disable SNMP v3 Mode, and then press Apply.

cisco	<u>M</u> onitor <u>w</u> l	ans <u>c</u> on	TROLLER	W <u>I</u> RELESS	<u>s</u> ecurity	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS		
Management	SNMP System	n Summa	iry						
Summary SNMP General SNMP V3 Users Communities	Name Location Contact		vWLC-F	RemoteSites-1					
Trap Receivers Trap Controls Trap Logs	System Descrip	otion							
HTTP-HTTPS	System Object	ID	1.3.6.1.4.	1.9.1.1631					
Telnet-SSH	SNMP Port Num	nber	161						
Serial Port	Trap Port Numb	ber	162						
Local Management Users	SNMP v1 Mode	e	Disable	<ul><li>✓</li><li>✓</li></ul>					
User Sessions <ul> <li>Logs</li> </ul>	SNMP v3 Mode		Disable V						

Step 16: Navigate to Management > SNMP Communities > SNMP V3 Users.

. . .

**Step 17:** On the right side of the **default** User Name, point and click the blue down arrow, and then click **Remove**.

ahaha						Sa <u>v</u> e C	onfiguration	<u>P</u> ing   L	ogout   <u>R</u> efresł
cisco	MONITOR	<u>W</u> LANs	<u>CONTROLLER</u>	WIRELESS	SECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK
Management	S	SNMP V3	Users						New
Summary									
▼ SNMP		User Name	Access I	Level Au	th Protocol	Privacy Protoco	d.		
General		default	Readwrit	e HM	AC-SHA	AES	Remove		
Communities							<u>ι         </u> γ		
Trap Receivers									
Trap Logs									
HTTP-HTTPS									
Telnet-SSH									
Serial Port									
Local Managen Users	nent								
User Sessions									
▶ Logs									
Mgmt Via Wire	less								
Software Activ	ation								
Frech Support									

Step 18: Press OK to confirm that you are sure you want to delete, then press Save Configuration.

ahaha						Sa	ve Configuration	Ping   L	ogout   <u>R</u> efresh
cisco	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURI	TY M <u>A</u> NAGEMEN	NT C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Management	ş	SNMP V3	Users						New
Summary									
▼ SNMP		User Name	Access	evel Au	th Protoco	Privacy Pro	tocol		
General		default	Readwrit	е нм	AC-SHA	AEC	-		
Communities						Message from web	page	83	
Trap Receivers Trap Controls Trap Logs						Are you	sure you want to de	lete ?	
HTTP-HTTPS									
Telnet-SSH						ſ			
Serial Port							Сок	Cancel	
Local Manager Users	nent								
User Sessions									
Logs									
Mgmt Via Wire	eless								
Software Activ	vation								
Fech Support									
	- I. T	-							

Changes to the SNMP configuration may sometimes require that the WLC be rebooted.	i	Tech Tip
	Chan	ges to the SNMP configuration may sometimes require that the WLC be rebooted.

## **Procedure 11** Limit which networks can manage the WLC

# (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

ահահո							Sa <u>v</u> e Co	nfiguratio	n   <u>P</u> ing   Lo <u>g</u> out   <u>R</u> efresl
cisco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMEN	T C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Security	Access C	control L	ists > Rules >	New					< Back Apply
AAA     Local EAP     Priority Order     Certificate     Access Control Lists     Access Control Lists     FlexConnet ACLs     Wireless Protection     Policies	Sequence Source Destination Protocol Source Port Destination	Port	1 IP Address Any TCP Any HTTPS	•	IP Addr 10.4.4	ess 18.0	Netmask 255.255.255.0		
Web Auth     TrustSec SXP     Advanced	DSCP Direction Action		Any Any Permit						

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

Table 29 -	Rule	configuration	values
------------	------	---------------	--------

Sequence	Source	Destination	Protocol	Source port	Destination port	Action
1	10.4.48.0/ 255.255.255.0	Any	TCP	Any	HTTPS	Permit
2	10.4.48.0/ 255.255.255.0	Any	ТСР	Any	Other/22	Permit
3	Any	Any	ТСР	Any	HTTPS	Deny
4	Any	Any	ТСР	Any	Other/22	Deny
5	Any	Any	Any	Any	Any	Permit

Ø DMZ-WLC-Guest -	DMZ-WLC-Guest-														
🚱 🕗 🗢 🙋 https://192.16	8.19.54/s	creens/fran	neset.html										- 6	Certificate Erro	n 😽 🗙
🚖 Favorites 🛛 🏀 DMZ-WLC-	Guest														
սիսիս cisco	MONI	tor <u>w</u>	LANS <u>C</u> ONTRO	LLER	WIRELESS	SECU	rity M <u>a</u> n	AGEMENT	COMMAND	S HELP	EEEDE	Sa⊻e Conf MACK	iguration	<u>P</u> ing   Logout	<u>R</u> efresh
Security	Acce	ess Con	trol Lists > Ec	lit								< Bac	< 1	Add New Rule	
AAA     General     RADIUS     Authentication     Accounting     Fallback     TACACS+     LDAP	Gene Acces Deny	e <b>ral</b> s List Nam Counters	e SBA-D 0	MZ-AC	L										
Local Net Users MAC Filtering	Seq	Action	Source IP/Ma	sk	Destination IP/Mask		Protocol	Source Port	Por	st rt	DSCP	Direction	Number of Hits		
Disabled Clients User Login Policies	1	Permit	10.4.48.0 255.255.255.0	/	0.0.0.0	/	TCP	Any	нт	TP S	Any	Any	0		
AP Policies Password Policies	_2	Permit	10.4.48.0 255.255.255.0	/	0.0.0.0	/	тср	Any	2	2	Any	Any	0		
Priority Order	_3	Deny	0.0.0.0	/	0.0.0.0	/	TCP	Any	нт	TPS .	Any	Any	0		
<ul> <li>Certificate</li> <li>Access Control Lists</li> </ul>	4	Deny	0.0.0.0	1	0.0.0.0 0.0.0.0	/	тср	Any	2	2	Any	Any	0		
Wireless Protection Policies	_5	Permit	0.0.0.0	/	0.0.0.0 0.0.0.0	/	Any	Any	Any		Any	Any	0		
<ul> <li>Web Auth</li> <li>TrustSec SXP</li> <li>Advanced</li> </ul>															

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 12** Configure management authentication

## (Optional)

You can use this procedure to deploy centralized management authentication by configuring an authentication, authorization and accounting (AAA) service using Cisco Secure ACS. 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 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)

	MONITOR WLANS	CONTROLLER WIR	ELESS <u>S</u> ECURITY	MANAGEMENT	Sa <u>v</u> e Config C <u>O</u> MMANDS	guration   <u>P</u> ing   HELP <u>F</u> EEDBAC	Lo <u>q</u> out   <u>R</u> efresh CK
CISCO      Security      AA     General     RADIUS     TACACS+     Authentication     Accounting     Authorization     LDAP     Local Ret Users     MAC Filtering     Disabled Clients     User Login Policies     AP Policies     Password Policies	MONITOR WLANS TACACS+ Authenti Server Index (Priority) Server IP Address Shared Secret Format Shared Secret Confirm Shared Secret Port Number Server Status Server Timeout	CONTROLLER WIR cation Servers > 1 • 10.4 ASCI 49 Enab 5	All Security	MANAGEMENT	Sa <u>ve</u> Confi C <u>Q</u> MMANDS	guration <u>Ping</u> HELP <u>FEEDBAC</u> <b>&lt; Back</b>	Logout <u>R</u> efresh :K Apply
<ul> <li>Local EAP</li> <li>Priority Order</li> <li>Certificate</li> <li>Access Control Lists</li> <li>Wirreless Protection Policies</li> <li>Web Auth TrustSec SXP</li> <li>Advanced</li> </ul>							

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)

								Logout <u>R</u> efresh
cisco	MONITOR WLANS		WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBA	ск
Security AAA General > RADIUS < TACACS+ Authentication Accounting Authorization	TACACS+ Accou Server Index (Priorit Server IP Address Shared Secret Form Shared Secret	y) 1 • 10.4 at ASC	3 > New .48.15 II ▼		]		< Back	Apply
LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Password Policies	Confirm Shared Sec Port Number Server Status Server Timeout	et •••• 49 Enat 5	oled 💌					
Local EAP								
Priority Order								
Certificate Certi								

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   <u>P</u> ing	Logout <u>R</u> efresh
CISCO	MONITOR WLANS	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP FEEDB	ACK
Security	TACACS+ Author	ization Serve	rs > New				< Back	Apply
<ul> <li>AAA</li> <li>General</li> <li>RADIUS</li> <li>TACACS+</li> <li>Authentation</li> <li>Accounting</li> <li>Authorization</li> <li>LDAP</li> <li>Local Net Users</li> <li>MAC Filtering</li> <li>Disabled Clients</li> <li>User Logn Policies</li> <li>Local EAP</li> <li>Priority Order</li> <li>Ccertificate</li> <li>Access Control Lists</li> <li>Wireless Protection</li> <li>Policies</li> <li>Web Auth</li> <li>TrustSec SXP</li> <li>Advanced</li> </ul>	Server Index (Priorit Server IP Address Shared Secret Confirm Shared Secr Port Number Server Status Server Timeout	y) it et	1 • 10.4.48.15 ASCII • • • • 49 5 second	is .				

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.

										ogout   Kenes
cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK	
Security	Priority 0	Order > I	/lanagement l	Jser						Apply
▶ AAA										
Local EAP	Authentio	cation								
<ul> <li>Priority Order</li> <li>Management User</li> </ul>	Not	Used		Order U	sed for Authe	entication				
Certificate	RADI	US 🔺	>		TACACS+ *	Up				
Access Control Lists		~	<		Ŧ	Dowr				
Wireless Protection Policies										
Web Auth	If LOCAL is	selected as	second priority the	en user will be	authenticated	against				
TrustSec SXP	LOCAL only	if first prior	ity is unreachable.							
Advanced										



i

If you are 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 Cisco Secure ACS server.

**Procedure 13** Create the guest wireless LAN interface

The guest wireless interface is connected to the DMZ of the Cisco ASA 5545X 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 are 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)

սիսիս									<u>P</u> ing   I	.ogout   <u>R</u> efresh
cisco	MONITOR	<u>W</u> LANs		W <u>I</u> RELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACI	к
Controller	Interface	s > New							Back	Apply
General Inventory Interfaces Interface Groups Multicast Network Routes Redundancy Internal DHCP Server Mobility Management Ports NTP CDP PMIPv6 InPv6 mDNS	Interface VLAN Id	Name	Wireless-Guest 1128							
Advanced										

Step 3: Enter the VLAN Id, and then click Apply. (Example: 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						Saye		Logout   <u>R</u> efresh
cisco	<u>M</u> ONITOR <u>W</u> LANS <u>C</u> C	NTROLLER WIRELES	IS <u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	EEEDBACK	
Controller	Interfaces > Edit						< Back	Apply
General								
Inventory	General Information							
Interfaces	Interface Name	wireless-guest						
Interface Groups	MAC Address	88:43:e1:7e:0a:6f						
Multicast								
Network Routes	Configuration							
Redundancy	Guest Lan							
▶ Internal DHCP Server	Quarantine							
Mobility Management	Quarantine Vlan Id	0						E
Ports	NAS-ID	DMZ-WLC-Guest						
▶ NTP	Enable DHCP Option 82							
► CDP	Physical Information							
▶ PMIPv6	The interface is attached	to a LAG.						
▶ IPv6	Enable Dynamic AP							
▶ mDNS	management							
▶ Advanced	Interface Address							
	VLAN Identifier	1128						
	IP Address	192.168.28.5						
	Netmask	255.255.255.0						
	Gateway	192.168.28.1						
	DHCP Information							
	Primary DHCP Server	10.4.48.10						
	Secondary DHCP Server							
	DHCP Proxy Mode	Global 👻						*

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 14** Configure the guest WLAN on the AireOS Anchor Controllers

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									ng   Lo <u>q</u> out   <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
WLANs	Mobility /	Anchors							< Back
✓ WLANS WLANS	WLAN SSI	D 550	3Guest						
Advanced	Switch IP	Address (	Anchor)		Data Path	Control Path			
	Mobility	Anchor Cr	eate						
	Switch IP	Address	(Anchor)	local	•				

Step 5: Click Back.

Step 6: Click the WLAN ID of the SSID created in Procedure 8. (Example: 5508Guest)

**Step 7:** On the General tab, in the **Interface/Interface Group(G)** list, choose the interface created in Procedure 13. (Example: wireless-guest)

		ogout <u>R</u> efresh
cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACH	к
WLANs	WLANs > Edit '5508Guest' <back< th=""><th>Apply</th></back<>	Apply
✓ WLANS WLANS	General Security QoS Policy-Mapping Advanced	
Advanced	Profile Name 5508Guest	Â
	Type WLAN	
	SSID 5508Guest	
	Status 🗹 Enabled	
	Security Policies WEB POLICY, Web-Auth (Modifications done under security tab will appear after applying the changes.)	E
	Radio Policy All -	
	Interface/Interface Group(G) wireless-guest 👻	E
	Multicast Vlan 🔲 Enabled Feature	
	Broadcast SSID 🛛 🗹 Enabled	
	NAS-ID DMZ-WLC5508-Guest-1	
		-
	< [	Þ

Step 8: Click the Security tab, and then on the Layer 2 tab, in the Layer 2 Security list, choose None.

cisco		<u>N</u> LANS <u>C</u> ON	TROLLER WIRELE	S <u>S</u> ECURITY	MANAGEMENT	Sa <u>v</u> e Conti C <u>O</u> MMANDS	HELP EEED	BACK			
WLANs	WLANs > E	VLANs > Edit '5508Guest' Apply									
WLANs     WLANs	General	Security	QoS Policy-M	apping Adv	anced						
Advanced	Layer 2	Layer 3	AAA Servers								
	Layer 2	: Security <sup>6</sup> N	one	•							
	Fast Trans	MA sition	C Filtering <sup>®</sup>								

Step 9: On the Layer 3 tab, select Web Policy, and then click OK.

	Sage Configuration   Bing   Logout   Befresh MONITOR WEAM- CONTROLLER WIRELESS SECTIONY MANAGEMENT COMMANDS LET SEEDAACY
WLANS WLANS WLANS WLANS Advanced	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK WLANS > Edit '5508Guest' General Security QoS Policy-Mapping Advanced Layer 3 AAA Servers Layer 3 Security Web Policy -
	Authentication  Passthrough  Conditional Web Redirect  Splash Page Web Redirect  On MAC Filter failure <sup>RR</sup> Preauthentication ACL IPV4 IPV6 WebAuth FlexAcl  Preauthentication ACL IPv4
	Sleeping Client II Enable Sleeping Client Timeout(1 to 720 Hrs) 12 Over-ride Global Config II Enable

Step 10: On the QoS tab, in the Quality of Service (QoS) list, choose Bronze (background), select Enable next to Application Visibility, click Apply, and then click OK.

					<u>P</u> ing   Logout   <u>R</u> efresh				
cisco	MONITOR WLANS CONTR	OLLER WIRELESS	SECURITY MANAGEMENT	C <u>O</u> MMANDS HELP	EEEDBACK				
WLANs	WLANs > Edit '5508Gue	sť		< Ba	ck Apply				
✓ WLANS WLANS	General Security C	20S Policy-Mappin	g Advanced						
Advanced	Quality of Service (QoS) Application Visibility	Bronze (background)	•						
	AVC Profile	none -							
	Override Per-User Bandy		E						
		DownStream UpStre	am						
	Average Data Rate	0 0							
	Burst Data Rate	0 0							
	Average Real-Time Rate	0 0							
	Burst Real-Time Rate	0 0			Ξ				
	Override Per-SSID Bandwidth Contracts (kbps) 🌆								
		DownStream UpStre	am						
	Average Data Rate	0 0			-				
	< <u> </u>				•				

### **Procedure 15** Configure anchor controller mobility group peers

The DMZ-based WLC controller(s) providing guest anchor services are called anchor controllers. They communicate with the wireless LAN controllers in your data center VSS services block, and manage the wireless APs and wireless users in your enterprise. In the context of guest wireless, the data center VSS services block based wireless LAN controllers are referred to as foreign anchor controllers because they are foreign to the actual anchor controllers located in the DMZ.

To establish this communication, a mobility peer needs to be created between the anchor and foreign anchor controllers. In the case of two 2504 N+1 anchor controllers, both must be peered with each other using a common mobility group name. In this example, both the anchor and foreign anchor controllers are Cisco AireOS controllers with the New Mobility (Converged Access) feature disabled.

In order to communicate with a Cisco IOS-XE based 5760 Series foreign anchor controller in your data center services block, the AireOS controllers must have the New Mobility (Converged Access) feature enabled. In doing so, the rapid convergence found within the 5508 based HA pair is negatively impacted.

This design uses a DMZ-based Cisco 2504 Series WLC pair with N+1 redundancy and the New Mobility (Converged Access) feature enabled.

If you are using a pair of Cisco 5508 Series Wireless Controllers in an N+1 configuration instead of HA SSO, or if you are using a pair of Cisco 2504 Series Wireless Controllers, you need to add each of the WLCs to a common mobility group.

If you are using an HA SSO pair of anchor controllers (Cisco 5508 Series Wireless Controllers), you can skip to Step 7 0in this procedure, because they do not need to be peered together since they are a high availability pair and therefore act as a single controller.

The first step is to create a mobility peer between the two non-HA SSO anchor controllers in the DMZ.

Step 1: On the guest anchor controller(s), navigate to Controller > Mobility Management > Mobility Groups.

**Step 2:** On the Static Mobility Group Member page on each anchor WLC, note the MAC address, IP address, and mobility group name for the local controller. You will need this information in the following steps.

DMZ-WLC2584-Guest-1	+							
(←)	creens/frameset.html					☆ ♥ C A = Deta Search	P 🖡 f	E 🖬 🖌 🖬 🗄
Share Browser WebExt								
ာျားပျား cisco	MONITOR WLANS CONT	ROLLER WIRELESS SECUR	UTY MANAGEMENT COMMANDS	HELP BEEDBACK			Sage Configuration   Ping	Logout   <u>R</u> efres
Controller	Static Mobility Group M	embers						New
General Inventory	Local Mobility Group	504Guest						
Interfaces	MAC Address II	P Address	Public IP Address	Group Name	Multicast IP	Status	Hash Key	
Interface Groups	d4:8c:b5:c2:be:60 1	92.168.19.25	192.168.19.25	2504Guest	0.0.0.0	Up	none	
1 DM7-W1 C)504-Gu+#-2	+							
A 1000/111100 11 20/0	comerce African and Interio					Ch = C	0	
Share Browser WebEr	a construction in					11 + C		
cisco	MONITOR WLANS CONT	ROLLER WIRELESS SECUR	RITY MANAGEMENT COMMANDS	HELP EEEOBACK			Sage Configuration   Eing	Logout   <u>R</u> efres
Controller	Static Mobility Group M	embers						New
General								

Table 30 - Internet edge anchor controller values

WLC name & Location	WLC and HA Type	MAC address	IP address	Mobility group name
DMZ-WLC2504- Guest-1 / DMZ	2504 N+1	d4:8c:b5:c2:be:60	192.168.19.25	2504Guest
DMZ-WLC2504- Guest-2 / DMZ	2504 N+1	3c:ce:73:d8:f3:60	192.168.19.26	2504Guest

**Step 3:** On each DMZ-based anchor controller that is using an N+1 redundancy model, 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 other N+1 guest controller. (Example: On DMZ-WLC2504-Guest-1 add 192.168.19.26 and on DMZ-WLC2504-Guest-2 add 192.168.19.25)

**Step 5:** In the **Member MAC Address** box, enter the MAC address of the guest controller. (Example: On DMZ-WLC2504-Guest-1 add 3c:ce:73:d8:f3:60 and on DMZ-WLC2504-Guest-2 d4:8c:b5:c2:be:60)

August 2014 Series



Step 6: In the Group Name box, enter the mobility group name configured on the guest controller, and then click Apply. (Example: 2504Guest)

DMZ-WLC2584-Guest-1	+										
← ▲ https://102.568.59.25/st	reens/frameset.html						습 또 면 의 - Delta Search	. م	÷ +	<b>1</b>	-
Share Browser WebExt											
uluulu cisco	MONITOR WLANS COM	ITROLLER WIRELESS SECURITY	MONAGEMENT	COMMANDS	HELP	FEEDBACK		Sage Configuration	Eine	Logout	Befresh
Controller	Mobility Group Membe	r > New						<	Back	A	pply
General Inventory Interfaces Interface Groups Multicost Internal DHCP Server	Member IP Address Public IP Address Member MAC Address Group Name Hash	192.168.19.26 3ctcet73id8if3i60 2504Guest none									
DMZ-WLC2504-Guest-2	+										
🗲 🚔 https://192.168.19.26/s	creens/frameset.html						合 후 C 🖉 🔍 🔹 Deito Search	٩	+ +	E -	- 🔝 -
Share Browser WebEc*											
uhuhu cisco	MONITOR WLANS CON	NTROLLER WIRELESS SECURITY	MONAGEMENT	COMMANDS	HELP	EEEOBACK		Sage Configuration	Bing	Logout	<u>B</u> efresh
Controller	Mobility Group Membe	er>New						<	8-ack		Apply
General Inventory Interfaces Interface Groups	Member IP Address Public IP Address Member MAC Address Group Name	192.168.19.25 0.0.0.0 d4:8c:b5:c2:be:60 2504Guest									
Internal DHCP Server	Hash	none									

Next, add a mobility peer on the foreign anchor controller that points to a Cisco AireOS high availability foreign controller pair.

Step 7: On the DMZ-based anchor controller(s), 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 foreign anchor controller. (Example: 10.4.175.66)

Step 9: In the Member MAC Address box, enter the MAC address of the campus or remote-site foreign anchor 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)

i Tech	Тір	
There are a nu method is to r Address. Alter Mobility Mana	umber of ways to find the MAC address on a Cisco AireOS controller. On havigate to <b>Controller &gt; Inventory</b> . There you will see the burned-in MAC mately you can obtain the MAC address by navigating to <b>Controller &gt;</b> agement > Mobility Groups and locating the local peer entry.	ie ;
uludu cisco	Save Configuration Ping Logout Refresh MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK	
Controller	Mobility Group Member > New 	
General Inventory Interfaces Interface Groups Multicast Network Routes P Redundancy	Member IP Address     10.4.175.66       Member MAC Address     2c:54:2d:72:91:40       Group Name     CAMPUS ×       Hash     none	
Internal DHCP Server		
<ul> <li>Mobility Management</li> <li>Mobility Configuration</li> <li>Mobility Groups</li> <li>Mobility Anchor Config</li> <li>Multicast Messaging</li> </ul>		

Step 11: On each controller, click Save Configuration, and then click OK.

Step 12: Repeat this process on the DMZ anchor controllers for each foreign controller in your organization.

**Step 13:** If you are peering to a Cisco IOS-XE 5760 Series high availability foreign controller pair in your data center services block, on the DMZ-based anchor controller(s), navigate to **Controller > Mobility Management > Mobility Groups**, and then click **New**.

**Step 14:** In the **Member IP Address** box, enter the IP address of the Cisco 5760 Series foreign anchor controller (Example 10.4.175.68).

**Step 15:** In the **Group Name** box, enter the mobility group configured on the Cisco 5760 Series foreign anchor controller (Example: 5760CAMPUS), click **Apply**, and then click **Save Configuration**.

DMZ-WLC2504-Gues	×						- • ×
← → C 🔒 bttps://1	92.168.19.25/screens	/frameset.htm	I				☆ 〓
սիսիս					Sa <u>v</u> e	Configuration   <u>P</u> ing	Lo <u>q</u> out   <u>R</u> efresh
CISCO	<u>M</u> ONITOR <u>W</u> LANS	<u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS HE <u>I</u>	_P <u>F</u> EEDBACK
Controller	Mobility Group Me	mber > New				< Back	Apply
General Inventory Interfaces Interface Groups Multicast Internal DHCP Server Mobility Configuration Mobility Anchor Config Multicast Messaging Switch Peer Group Switch Peer Group Switch Peer Group Switch Peer Group	Member IP Address Public IP Address Member MAC Addres Group Name Hash	10.4.175.6 0.0.0 00:00:00:00:0 5760CAMP none	8 10:00:00 US				

### Tech Tip

The mobility group used on the Cisco 5760 Series Wireless Controller can be found by navigating to **Configuration > Controller**. It is listed in the **Default Mobility Domain** box.

**Step 16:** Navigate to **Controller > Mobility Management > Mobility Groups**, and then verify that connectivity is working between all the controllers by examining the mobility group information. In the Status column, all controllers should be listed as **Up**.

DMZ-WLC2504-Gue:	× 🚬						L	
← → C <a>B</a> betps://19	92.168.19.25/screens/	frameset.html						☆ =
uluilu cisco	MONITOR WLANS	CONTROLLER WIRELESS SECURITY	MANAGEMENT CO	MMANDS HELP	EEEDBACK	_	Sage Configuration   jing   Log	out <u>R</u> efresh
Controller General Inventory	Static Mobility Grou	up Members up 2504Guest					New	EditAll
Interfaces	MAC Address	IP Address	Public IP Address	Group Name	Multicast IP	Status	Hash Key	
Interface Groups	d4:8c:b5:c2:be:60	192.168.19.25	192.168.19.25	2504Guest	0.0.0.0	Up ⊳	none	
Multicast Internal DHCP Server	00:00:00:00:00:00:00	10.4.175.68	10.4.175.60	5760CAMPUS	0.0.0.0	Up	none	
<ul> <li>Mobility Management Mobility Configuration Mobility Groups</li> <li>Mobility Groups</li> <li>Multicast Messaging Switch Peer Group</li> <li>Switch Peer Group</li> <li>Member</li> <li>Mobility Controller</li> <li>Clients</li> </ul>								

DMZ-WLC5508-Gue:	×						
← → C' 😰 beeps://1	92.168.19.54/screens/	/frameset.html					52 =
uludu cisco	MONITOR WLANS	CONTROLLER WIRELESS SECURITY	MANAGEMENT (	COMMANDS HELP EEEDBACK		Sage Configuration   Ping   D	ogout   <u>R</u> efresi
Controller	Static Mobility Grou	up Members				New	EditAll
General Inventory	Local Mobility Grou	up 5508Guest					
Interfaces	MAC Address	IP Address	Group Name	Multicast IP	Status	Hash Key	
Interface Groups	88:43:e1:7e:0a:60	192.168.19.54	5508Guest	0.0.0.0	Up N	none	
Multicast Network Routes	00:50:56:a2:09:90	10.4.59.59	REMOTES-VWLC	0.0.0.0	Up Up	none	
Redundancy	00:50:56:a2:09:92	10.4.59.58	REMOTES-YWLC	0.0.0.0	Up	none	
Internal DHCP Server	20:3a:07:67:7c:40	10.4.175.62	CAMPUS-2504	0.0.0.0	Up	none	
	20:3a:07:67:99:20	10.4.175.63	CAMPUS-2504	0.0.0.0	Up	none	
<ul> <li>Mobility Management</li> <li>Mobility Configuration</li> </ul>	2c:54:2d:72:91:40	10.4.175.66	WLC5508	0.0.0.0	Up	none	
Nobility Groups	6c:20:56:2c:0f:20	10.4.175.64	WISM2	0.0.0.0	Up	none	
Nobility Anchor Config Nulticast Nessaging	70:81:05:ce:c3:a0	10.4.59.68	REMOTES	0.0.0.0	Up	none	

## Procedure 16 Configure Cisco IOS-XE mobility groups

To communicate with a Cisco IOS-XE based foreign controller, the Cisco AireOS anchor controllers must have the New Mobility (Converged Access) feature enabled. This guide uses a pair of DMZ-based Cisco 2504 Series WLC anchor controllers using N+1 redundancy with the New Mobility (Converged Access) feature enabled.

On each of the Cisco 2504 Series DMZ anchor controller(s), enable New Mobility (Converged Access).

Step 1: Navigate to Controller > Mobility Management > Mobility Configuration, and then select Enable New Mobility (Converged Access).

Step 2: In the Mobility Controller Public IP Address box, enter the IP address of this wireless LAN controller (Example: 192.168.19.25 or 192.168.19.26).

ahaha						Sa <u>v</u> e Co	nfiguration   <u>P</u> ii	ng   Log	iout   <u>R</u> efresh
cisco	<u>M</u> ONITOR	<u>W</u> LANs		WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK
Controller	Global Co	nfigurat	ion					]	Apply
General Inventory Interfaces Interface Groups	General Enable Net	w Mobility(	Converged Access	;) 🔽					
Multicast	Mobility Pa	aramete	rs						
▶ Internal DHCP Server	Multicast M	1ode							
💌 Mobility Management	Multicast I	P Address							
Mobility Configuration	Mobility Or	racle IP Ad	ldress	0.0.0.0					
Mobility Anchor Config	Mobility Co	ontroller P	ublic IP Address	192.168.19	.25				
Multicast Messaging	Mobility Ke	eepalive Ir	terval(1 to 30 sec	) 10					
Switch Peer Group Switch Peer Group	Mobility Ke	eepalive C	ount(3 to 20)	3					
Member Mobility Controller Clients	Mobility D	SCP Value	(0 to 63)	0					

**Step 3:** On each of the Cisco 2504 Series DMZ anchor controller(s), navigate to **Controller > Mobility Management > Mobility Groups**, and then, 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.

սիսիս						Save Configuration   Ping   Logout   Refresh
Controller	Static Mobility Group	p Members	MBRAGEMENT COMMANDS	HED- FEEDBACK		
General Inventory	Local Mobility Group	2504Guest				
Interfaces	MAC Address	IP Address	Public IP Address	Group Name	Multicast IP	Status
Interrace Groups	d4:8c:b5:c2:be:60	192.168.19.25	192.168.19.25	2504Guest	0.0.0.0	Up
Multicast						Central and Data Ach Down
F Internal DHCP Server						Canand and Date Path Depen
Mobility Management Mobility Configuration Mobility Groups Mobility Affore Config Multicast Messaging Switch Peer Group Switch Peer Group Member Mobility Controller Clients						

cisco	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY MAN	AGEMENT COMMANDS	HELP EEEDBACK		Sa <u>v</u> e Configuration   <u>P</u> ing   Logout	t   <u>R</u> efresh
Controller	Static Mobility Grou	ip Members						
General Inventory	Local Mobility Grou	p 2504Guest						
Interfaces	MAC Address	IP Address		Public IP Address	Group Name	Multicast IP	Status	
Interface Groups	3c:ce:73:d8:f3:60	192.168.19.26		192.168.19.26	2504Guest	0.0.0.0	Up	
Multicast								
▶ Internal DHCP Server								
Mobility Management     Mobility Configuration     Mobility Groups     Mobility Anchor Config     Multicast Messaging     Switch Peer Group     Switch Peer Group     Member     Mobility Controller     Clente								

#### Table 31 - Internet edge anchor controller values

WLC name & Location	WLC and HA Type	MAC address	IP address	Mobility group name
DMZ-WLC2504- Guest-1 / DMZ	2504 N+1	d4:8c:b5:c2:be:60	192.168.19.25	2504Guest
DMZ-WLC2504- Guest-2 / DMZ	2504 N+1	3c:ce:73:d8:f3:60	192.168.19.26	2504Guest

Next, allow the DMZ-based 2504 N+1 anchor controller pair to share mobility information by creating a common mobility group. Perform the following steps on each anchor controller.

Step 4: Navigate to Controller > Mobility Management > Mobility Groups, and then click New.

**Step 5:** In the **Member IP Address** box, enter the IP address of the guest controller. (Example: on the 192.168.19.26 controller enter 192.168.19.25 and on the 192.168.19.25 controller enter 192.168.19.26)

**Step 6:** In the **Member MAC Address** box, enter the MAC address of the guest controller. (Example: d4:8c:b5:c2:be:60 and/or 3c:ce:73:d8:f3:60)

August 2014 Series

**Step 7:** In the **Group Name** box, enter the mobility group name configured on the guest controller, and then click **Apply**. (Example: Guest)

🟉 DMZ-WLC-Guest -								- • •
🕞 🕞 🗢 🙋 https://192.16	3.19.54/screens/frameset.html						👻 😵 Cer	tificate Error 🏼 😽 🔀
🚖 Favorites 🏾 🏉 DMZ-WLC-	Guest							
սևսև						Sa <u>v</u> e	e Configuration   <u>P</u> ing	Logout   <u>R</u> efresh
cisco	MONITOR WLANS CO	NTROLLER WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	EEEDBACK	
Controller	Mobility Group Memb	er > New					< Back	Apply
General Inventory Interfaces Multicast Network Routes P Redundancy Internal DHCP Server Mobility Management Mobility Anchor Config Multicast Messaging	Member IP Address Member MAC Address Group Name Hash	192.168.19.55 80:43:e1:7e:13:64 GUEST none						
Ports  NTP								
► CDP								
▶ PMIPv6								
▶ IPv6								
▶ mDNS								
Advanced								

Step 8: On both of the DMZ guest anchor controllers, navigate to Controller > Mobility Management > Mobility Groups, and then click New.

Step 9: In the Member IP Address box, enter the IP address of the Cisco 5760 Series foreign anchor controller pair. (Example: 10.4.175.68)

**Step 10:** In the **Member MAC Address** box, leave the default MAC address of 00:00:00:00:00:00. This is normal for mobility peers using New Mobility, which is the protocol the Cisco 5760 Series Wireless Controller uses.

**Step 11:** In the **Group Name** box, enter the mobility group name configured on the campus or remote-site controller, and then click **Apply**. (Example: 5760-CAMPUS)

iliilii cisco	MONITOR WLANS	CONTROLLER	WIRELESS S	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK		Sage Configuration	Eing Logout Berresh
Controller	Static Mobility Gro	oup Members								N	ew EditAll
General Inventory Interfaces	Local Mobility Gro	up 2504Gue	st			Cours North			Chalum	line March	
Interface Groups Multicast	d4:8c:b5:c2:be:60	192.168.19.25			192.168.19.25	2504Guest		0.0.0.0	Up De	none	
<ul> <li>Internal DHCP Server</li> <li>Mobility Management</li> </ul>	00:00:00:00:00:00 3c:ce:73:d8:f3:60	10.4.175.68 192.168.19.26			10.4.175.68 192.168.19.26	5760CAMPUS 2504Guest		0.0.0.0	Up Up	none	
Mobility Configuration Mobility Groups Mobility Anchor Config Multicast: Messaging Switch Peer Group Switch Peer Group Member Mobility Controller Clients											

<b>i</b>	Tech Tip
The c	ontroller status will be in a Control and Data Path Down state for the Cisco
5760	Series Wireless Controller until you configure a mobility group peer on the
5760	Wireless Controller that points back to each of the DMZ-based Cisco 2504
Series	anchor controllers. Note that New Mobility (Converged Access) was enabled
on the	2504 Wireless Controllers in the DMZ in order to allow the mobility group
comm	nunication to utilize CAPWAP as opposed to Ethernet over IP (EoIP).

Step 12: On each controller, click Save Configuration, and then click OK.

**Step 13:** Access the Cisco 5760 Series foreign anchor controller in the data center services block by using its SSL-based URL. (Example: https://10.4.175.68/wireless)

abab											Save Configuration   Refresh
cisco Wireless Cont	roller		☆ Home	Monitor 🛛 💌	Configuration	Adi	ministration 💌 Help				
System Summary							Top WLANs				
System Time	10:33:28	.359 PST 1	Thu Dec 12 2013				Profile Name	Number of	Clients		
Software Version	03.03.01 (fc1)	SE RELEAS	E SOFTWARE				WLAN-Data	0			
System Name	5760-WL	C					Voice	0			
System Model	AIR-CT57	'60									
Up Time	2 days, 2	3 hours, 4f	0 minutes				AVC for WLAN : WLAN-D	lata			
Wireless Management IP	10.4.30.6	58									
802.11 a/n/ac Network State	Enabled										
802.11 b/g/n Network State	Enabled						No AVC data availab	le for this wla	n		
Software Activation	Detail										
Access Point Summary	Total	Up	Down								
802.11a/n/ac Radios	5	5	0								
802.11b/g/n Radios	5	5	0								
All APs	5	5	0								
Client Summary							Rogue APs				
Current Clients	0						Active Rogue APs		270	Detail	
Excluded Clients	0						Active Rogue Clients		3	Detail	
Disabled Clients	0						Adhoc Rogues		14	Detail	

Next, create a new mobility peer to the DMZ-based Cisco 2504 Series anchor controller.

Step 14: Navigate to Configuration > Controller > Mobility Management > Mobility Peer, and then click New.

ahaha							Sive	Contiguration   Refresh
cisco Wireless Controller	🛆 Home	e Monitor 💌 Configu	ation 💌 Administrat	ion 💌 Help				
Controller	Mobility Peer							
System     Internal Data     Security	New Remove						Show All	- 8
<ul> <li>Management</li> </ul>	IP Address	Public IP Address	Group Name	Multicast IP	Control Link Status	Data Link Status		
* Mobility Management	10.4.175.68		5760CAMPUS	0.0.0.0	UP	UP		
Mobility Global Config     Mobility Peer								
Switch Peer Group								
▶ mONS								

**Step 15:** In the **Mobility Member IP** box, enter the IP address of each of the Cisco 2504 Series DMZ-based anchor controllers. (Example 192.168.19.25 and 192.168.19.26).

**Step 16:** In the **Mobility Member Group Name** box, enter the mobility group name as defined on the DMZ-based Cisco 2504 Series anchor controller (Example: 2504Guest), and then click **Apply**.

ahaha	Sa	e Configuration   Refresh
cisco Wireless Controller	🏡 Home Monitor 💌 Configuration 💌 Administration 🔍 Help	
Controller	Mobility Peer Mobility Peer > New	(Lapply)
<ul> <li>System</li> <li>Internal DHCP Server</li> <li>Management</li> <li>Mobility Management</li> <li>Mobility Global Config</li> <li>Mobility Global Config</li> </ul>	Mobility Member (P 192.168.19.25 Mobility Member Public (P 2004) Mobility Member Group, Name 2004Quest Multicast (P Address	
<ul> <li>Switch Peer Group</li> <li>mDNS</li> </ul>		

The preceding steps apply this configuration.

wireless mobility group member ip [IP Address of DMZ Anchor] public-ip [IP Address of DMZ Anchor] group [DMZ Anchor Mobility Group Name] Step 17: Navigate to Configuration > Controller > Mobility Management > Mobility Peer, and then verify that connectivity is working between all the controllers by examining the mobility group information. In the Status column, all controllers should be listed as Up. The negotiation process may take 30-90 seconds to complete, so click **Refresh** to see the current status.

cisco Wireless Controller	A Hor	ne Monitor 🔻 Confi	juration 💌 Administra	ation I <b>v</b> Help				Save Configuration   Refresh
Controller	Mobility Peer							
<ul> <li>System</li> </ul>	New Remove						Show Al	× 8
Internal DHCP Server	TO existence	public to address	Concer Manual	the design of the	Control Link Chatra	Data Link Cash of		
Management	IP AUURESS	PUDIC IP AUURESS	croch valle	MUTOPOPPI IN	CONTROL DRIK Status	Data LITIK Status		
<ul> <li>Mobility Management</li> </ul>	10.4.175.68		5760CAMPUS	0.0.00	UP	UP		
- Malatha Clabel Cardia	192.168.19.25	192.168.19.25	2504Guest		UP	UP		
Mobility Good Coring     Mobility Peer     Switch Peer Group	192.168.19.26	192.168.19.26	2504Guest		UP	UP		
▶ mDNS								

#### Example

wireless mobility group member ip 192.168.19.25 public-ip 192.168.19.25 group 2504Guest wireless mobility group member ip 192.168.19.26 public-ip 192.168.19.26 group 2504Guest

#### Procedure 17 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.

If you have deployed ISE for end user authentication services, skip the steps below and perform the steps in the process "Configuring Cisco ISE Sponsor Portal Services."

### **Option 1: Local WLC-based lobby admin user account**

**Step 1:** On the AireOS Anchor Controller in the DMZ, navigate to **Management > Local Management Users**, and then click **New**.

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

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

August 2014 Series

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

C DMZ-WLC-Guest -						
	68.19.54/screens/frameset.html				👻 🥸 Certificate Error	*7 ×
······································	MONITOR WLANS CONTR	DILLER WIRELESS SECURITY	M <u>a</u> nagement C <u>o</u>	MMANDS HELP EEEDBACK	Sa <u>v</u> e Configuration   <u>P</u> ing   Logout   ,	<u>R</u> efresh
Management Summary SMMP HTTP-HTTP5 Teinet-SSH Serial Port User Sessions Logs Management User Sessions Logs Manu Via Wireless Software Activation Fach Support	Local Management Users User Name Password Confirm Password User Access Mode	S > New Guest-Admin Colleyadmin •			< Back Apply	

# **Option 2: Centralized ACS based 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 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. Contained within this group are each of the lobby ambassador employees within the organization. (Example: Linda Lobby)



Step 2: Log in to Cisco Secure ACS via the GUI (https://acs.cisco.local).

Step 3: Navigate to Users and Identity Stores > Identity Groups.

#### Step 4: Click Create.

Cisco Secure ACS EVAL(Days left: 299)		acsadmin	acs (Primary : LogCollector)	Log Out	About	Help
► 🔂 My Workspace Users	and Identity Stores > Identity Groups					
► 🎲 Network Resources Ide	ntity Groups					
▼ 🎒 Users and Identity Stores	er: Match if:	▼ Go ▼				
Identity Groups						
Users	Name   Description					
Hosts	All Groups     Identity Group Root					
External Identity Stores	Helpdesk					_
Active Directory	Network Admins					_
RSA SecurID Token Servers						
Certificate Authorities						
Certificate Authentication Profile						
Policy Elements						
Access Policies						
Monitoring and Reports						
System Administration						
	reaten Duplicate Edit Delete Fi	le Operations	Export			
	0					

Step 5: In the Name box, enter Lobby Admins, and then enter a description for the group then click Submit.

Cisco Secure A EVAL(Days left: 299)	CS	acsadmin	acs (Primary : LogCollector)	Log Out	About	Help
My Workspace     My Workspace     My Workspace     Solution     More and Identity Stores     Identity Groups     Internal Identity Stores     Users     Hosts     External Identity Stores	Users and identity Stores > Identity Groups > Create General o Name: Lobby Admins Description: Lobby Administrators o Parent: All Groups o = Required fields		× Select			
LDAP Active Directory RSA SecurID Token Servers RADIUS Identity Servers Certificate Authonitication Profile Identity Store Sequences Policy Elements Certificate Authonitication Profile Identity Store Sequences Certificate Authonitication Profile Identity Store Sequences Certificate Authonitication Profile Identity Store Sequences Certificate Authonitication Profile Identity Store Sequences Certificate Authonitication Profile Certificate Authoni						
System Administration	Submit Cancel					

Step 6: In Cisco Secure ACS, navigate to Users and Identity Stores > External Identity Stores > Active Directory.

**Step 7:** Click 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
Network Resources     Sers and Identity Stores     Identity Groups     Internal Identity Stores     Users     Hosts     External Identity Stores     LDAP     Active Directory     RGA SecuriD Token Servers     RADIUS Identity Servers     Certificate Authentication Profile     Identity Store Sequences     Policy Elements	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 to launch a dialog to select groups from the directory."         Selected Directory Groups:         Group Name         Disco local/Users/wn-employee         cisco.local/Users/wn-partner
En Access Policies     Monitoring and Reports     System Administration	Add A Edit V Replace A Deselect Select  OroughName  cisco.local/Users/Lobby Admins  Example for group format: cisco.com/Users/Domain Users  o = Required fields

Next, the Active Directory group that was just added to Cisco Secure ACS needs to be mapped to a Secure ACS policy.

Step 8: 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 AC									
CISCO EVAL(Days leit 525)	_	/							
▶ 🔗 MyWorkspace	Acce	ss Policie	s > Acces	s Services	> Default Device Admin > Group I	Mapping			
Network Resources		O Single result selection      Rule based result selection							
B Users and Identity Stores	Gr	Group Mapping Policy							
Policy Elements	Fi	ilter: Status 🔹 Match if: Equals 🔹 🔍 Clear Filter 🛛 <b>Go</b> 💌							
🔹 🛼 Access Policies						Conditions		Results	
Access Services     Service Selection Rules			Status	Name	Compound Condition			Identity Group	Hit Count
	1	1	0	Rule-1	AD-AD1:ExternalGroups con	tains any cisco.loc	al/Builtin/Network Device Adm	ns All Groups:Network Admins	13100
Authorization Authorization O Default Network Access → O Remide Access VPN → O Vereiess LAN Identity Authorization + Max User Session Policy Max Gession Noers Settings Max Gession Noers Settings Max Gession Oroup Settings Max Gession Oroup Settings Monitoring and Reports Monitoring and Reports System Administration				I					
			Default	_	If no rules defined or no ena	bled rule matches		All Groups	18
		Create	. <b> •</b> ] D	uplicate	Edit Delete	Nove to 💟			

Step 9: Under Conditions, select Compound Condition, in the Dictionary list, choose AD-AD1, and then in the Attribute box, click Select and select External Groups and press OK. This selects External Groups.

Exter	nal Identity Store Dictiona	ry	Showing 1-2 of 2	50 🗸	per page	e Go
Filter	Match if:	V Go V				
	Attribute 🔺	Туре				
•	ExternalGroups	String Enumeration				
0	IdentityAccessRestricted	Boolean				
						_
_			Page	-	of 1	151
	-		Fage	L		
ok	Cancel					Help

Step 10: Under the Value box, click Select.

General		^
Name: Rule-2	Status: Enabled V 9	
The Custo policy cond	mize button in the lower right area of the policy rules screen controls which ditions and results are available here for use in policy rules.	
Conditions		
Compound Cond	ition:	
Condition:		
Dictionary:	Attribute:	
AD-AD1	Value:	
Contains any V	value.	
Current Condition	Select Clear	
Add V	Edit A Replace V Delete	
	Undo Preview	~
K Cancel		Help

**Step 11:** 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 1-3 of 3	50 🗸 per page Go
Filter: V Match if: Go V		
Enum Name		•
cisco.local/Builtin/Helpdesk		
cisco.local/Builtin/Network Device Admins		
✓ cisco.local/Users/Lobby Admins		
	Reference Page	1 of 1 🕨 🔰
OK Cancel		
hs		

Step 12: Under Current Condition Set, click Add. The new condition appears in the Current Condition Set box.

General		
Name: Rule-2	Status: Enabled V 9	1
The Cust	omize button in the lower right area of the policy rules screen controls which	
	futions and results are available field for use in policy futes.	
Conditions		
Compound Con	dition:	
Condition:		
Dictionary:	Attribute:	
AD-AD1	▼ ExternalGroups Select	
Operator:	Value:	
contains any V		
	Select Deselect Clear	
Current Condition	1 Set:	
Add •	· Edit ∧ Replace V Delete	
AD-AD1'E	xternalGroups contains any cisco local/Users/Lobby Admins	
	Undo Preview	
Deculte		
Cancel		Heli
		Tici

Compound Condition:	Condition	
Condition:	o on an one of the other o	
1		
Dictionary.	Attribute:	
AD-AD1	ExternalGroups     Select	
Operator:	Value:	
contains any		
	Salast Decelerat Clear	
	Jelett Deselect Olean	
Current Cond	ition Set:	
Ad		
Au	Edit / Replace V Delete	
AD-AI	01:ExternalGroups contains any cisco.local/Users/Lobby Admins	
	$\checkmark$	
	~	
	Undo Preview	
	Undo Preview	
Results	Undo Preview	

Step 13: Scroll down and under Results, click Select

**Step 14:** Select the Cisco Secure ACS identity group (Example: Lobby Admins) that will be mapped to the Active Directory group specified in the Current Condition Set, and then click **OK**.

Identity Groups
Filter: Match if. V Go V
Name Description
O All Groups Identity Group Root
O <u>Helpdesk</u>
Lobby Admins     Lobby Administrators
O <u>Network Admins</u>
Create Duplicate Edit Delete File Operations Export
CK Cancel Help
Step 15: Press OK to complete the group mapping.

Conditions		
Compound Con	dition:	
Condition: Dictionary	Attribute	
AD-AD1	✓ ExternalGroups Select	
Operator:	Value:	
contains any 🗸		
	Colort Developt Olars	
	Select Deselect Clear	
Current Condition	n Set:	
Add		
Auu	Luit A Replace V Delete	
AD-AD1:E	xternalGroups contains any cisco.local/Users/Lobby Admins	
11	Undo Preview	
Results		
lentity Group: All G	Groups: Lobby Admins Select	

Step 16: Save the changes by selecting Save Changes.

cisco EVAL(Days left: 299)	CS				acsadmin acs (Primary : Log	(Collector) Log Out About	t Help	
My Workspace	Access	s Policie	es > Acces	s Services	> Default Device Admin > Group Mapping			
Network Resources	0	O Single result selection   Rule based result selection						
Users and Identity Stores	Gro	Sroup Mapping Policy						
Policy Elements	Filt	er: Sta	atus		✓ Match if: Equals ✓ ✓ Clear Filter Go ▼			
Access Policies					Conditions	Results		
* Access Services			Status	Name	Compound Condition	Identity Group	Hi	
<ul> <li>Service Selection Rules</li> <li>O Default Device Admin Identity</li> </ul>	1		Θ	Rule- 1	AD-AD1:ExternalGroups contains any cisco local/Builtin/Network Device Admins	All Groups:Network Admins	41	
Group Mapping Authorization	2		Θ	Rule- 2	AD-AD1:ExternalGroups contains any cisco local/Users/Lobby Admins	All Groups:Lobby Admins	0	
<ul> <li>Max User Session Policy Max Session Group Settings Max Session Group Settings</li> <li>              Monitoring and Reports      </li> <li>             System Administration         </li> </ul>	×	reateave Ch	Default	uplicate	If no rules defined or no enabled rule matches.	All Groups Customize Hit Cou	> 12 It	

Next, 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 17: In Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles, click Create.

**Step 18:** Under the General tab, in the **Name** box, enter a name for the wireless shell profile. (Example: Lobby Admins)

Step 19: On the Custom Attributes tab, in the Attribute box, enter role1.

Step 20: In the Requirement list, choose Mandatory.

Step 21: In the Value box, enter LOBBY, and then click Add.

🔗 Cisco Secure ACS -		
📀 🕞 🗢 🙋 https://10.4.48.15/acsadmi	👻 🥸 Certificate Error	47 ×
🚖 Favorites 🏾 🌈 Cisco Secure ACS		
۱۱۱۱۱۱۰ Cisco Secure A cisco EVAL(Days left 324)	S aceadmin ace-1 (Primary) Log Out About	Help
Network Resources	oucy crements * Authorization and Permissions * Device Auministration * Shell Promes * Create	
Section and Identity Stores	General Common Tasks Custom Attributes	
Policy Elements	Common Tasks Attributes	
Session Conditions     Date and Time     Custom     Network Conditions     Authorization and Permissions     Network Access     Device Administration     Shell Profiles     Command Sets     Named Permission Objects     Monitoring and Reports     System Administration	Attribute     Requirement     Value       Manually Entered     -       Attribute     Requirement     Value       [Del]     Manually Entered	E
	Add A       Edit V       Replace A       Delete         Attribute:       role1         Requirement:       Mandatory •         Attribute       Static •         Value:       Static •         LO9BY       •	

Step 22: Click Submit.

Next, you create a WLC authorization rule.

Step 23: In Access Policies > Default Device Admin > Authorization, click Create.

Step 24: In the Name box, enter a name for the WLC authorization rule. (Example: Lobby Admin)

Step 25: Under Conditions, select Identity Group, and then in the box, enter All Groups:Lobby Admins.

Step 26: Select NDG:Device Type, and then in the box, enter All Device Types:WLC.

Step 27: In the Shell Profile box, enter Lobby Admins, and then click OK.

The Custo policy cond	mize button in the lo ditions and results a	wer r re av	ight area of the policy rules scre ailable here for use in policy rule	en controls s.	which
Conditions					
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-				
Results					
Shell Profile: Lobby Ad	Imins		Select		

Step 28: Click Save Changes.

#### **Procedure 18** 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 wireless controller where the access point (the foreign anchor controller) is registered to the guest controller in the DMZ (the anchor controller). The wireless client is then able to obtain an IP address from the DMZ, and in essence appears as a host on the DMZ network. 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:** Access the internal WLCs that are providing foreign anchor controller services to the anchor controller in the DMZ. On the WLANs page, in the list, choose **Create New**, and then click **Go**.

ahaha			Sa <u>v</u> e Configuration   <u>P</u> ing   Lo <u>g</u> out   <u>R</u> efresh
cisco	MONITOR WLANS CONTROLLER W	RELESS SECURITY MANAGEMENT	COMMANDS HELP FEEDBACK
WLANs	WLANs		Entries 1 - 2 of 2
WLANS	Current Filter: None [Change Filt	er] [ <u>Clear Filter</u> ] C	reate New 🔻 Go
Advanced			
	ULAN 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	Enabled [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 Cor	figuration   <u>P</u> ing   Logout   <u>R</u> efresh
cisco	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY MANAG	GEMENT C <u>O</u> MMANDS	HELP FEEDBACK
WLANs	WLANs > New				< Back Apply
WLANS WLANS Advanced	Type Profie Name SSID ID	WLAN • Guest Guest 3 •			

راریان cısco	Saye Configuration Ping Logout Refresh MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs > Edit 'Guest' < Back Apply
WLANS	General Security QoS Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Layer 2 Security 9 None -
	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 MFE is not active unites WRA2 is configured 5 Learn Client IP is configurable only when HRGAP 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 'AI'. 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 tunnelina, Local switching, DHCP Required should be disabled.
	13 Max-associated-clients feature is not supported with HREAP Local Authentication.

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** and enable sleeping client support. Sleeping client support prevents wireless clients that enter sleep mode from having to re-authenticate when they are awakened.

cisco	Save contiguration Engl Logout Refresh MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	WLANs > Edit 'Guest' Apply
WLANS	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Layer 3 Security <sup>4</sup> Web Policy ▼ © Authentication Passthrugh Conditional Web Redirect Splash Page Web Redirect On MAC Filter failure <sup>44</sup> Preauthentication ACL IPv4 <u>Pre-Auth-for-External-Web-Server</u> IPv6 <u>None</u> ✓ WebAuth FlexAcl <u>None</u> ▼ Sleeping Client Timeout(1 to 720 Hrs) 12 Over-ride Global Config Enable

Step 6: On the QoS tab, in the Quality of Service (QoS) list, choose Bronze (background).



Step 7: Enable application visibility by selecting Enabled and then click Apply.

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



Step 9: Click Back.

Step 10: Hover over the blue list next to your guest WLAN, and then click Mobility Anchors.

**Step 11:** In the **Switch IP Address (Anchor)** list, choose the IP address of the guest controller. (Example: 192.168.19.54)

Step 12: Click Mobility Anchor Create, and then click OK.

սիսիս		Say	e Configuration   Ping   Logout   <u>R</u> efresh
cisco	MONITOR WLANS CONTROLLER WIRELESS	ECURITY MANAGEMENT COMMAND	S HELP <u>F</u> EEDBACK
WLANs	Mobility Anchors		< Back
WLANS WLANS	WLAN SSID Guest-10k		
Advanced	Switch IP Address (Anchor)	Data Path	Control Path
	192.168.19.54	up	up 🔽
	Mobility Anchor Create           Switch IP Address (Anchor)	al) •	

Step 13: Repeat Step 1 through Step 11 for every internal controller in your organization.

Drocedure 10	Create quest accounts
Procedure 19	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 DMZ wireless LAN controller's web interface (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.

cisco	Lobby Ambassador Guest Management	Logout   Refresh   Help
Guest Management	Guest Users List	New
	Items 0 User Name WLAN SSID Account Remaining Time Description	to 0 of 0

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

cisco	Lobby Ambassador Gues	t Management	Logout   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 Cisco ISE Sponsor Portal Services**

- 1. Configure Cisco ISE Sponsor settings
- 2. Configure Cisco ISE guest authentication policy

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

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

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

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

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

#### Procedure 1 Configure Cisco ISE Sponsor settings

Centralized Web Authentication (CWA) using Cisco ISE allows for email and SMS text messages to be sent to guests with their account credentials. In addition, ISE also uses SMTP to send email notifications to administrators for various alarm conditions that may arise over time. Both of these functions are accomplished through the configuration of an SMTP email server which must be able to use ISE in order to enable this functionality. Before you begin, ensure that the following conditions are met:

- A functional SMTP server is available to Cisco ISE and has the capabilities to forward emails to other email servers and and/or users.
- A third-party SMS gateway account that allows notifications to be sent in email format as SMS text messages.

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

#### Step 2: Click Save.

ululu CISCO Identity Services Engine	ise-1   admin   Lopout   Feedback	Setup Assistant 🕶 🕗
🔆 System 🥂 Identity Management 🕋 Networ	k Resources 🙀 Web Portal Management 🛛 🙀 Feed Service	
Deployment Licensing Certificates Logging	Maintenance Backup & Restore Admin Access Settings	
Settings Clent Provisioning Endpoint Protection Service ERPS Mode Atom Settings Posture Proting Protecols Protecols SMTP Server System Time Policy Sets	SMTP Server Settings  * SMTP Server email.exemple.com)  Gest User Settings  • Use email address from Sporsor  • Use Default email address  * Orfault email address  Sover Reset.	
🕑 Help		Notifications (0)

Step 3: Navigate to Administration > Web Portal Management > Settings, double-click General, and then, in the list, choose Portal Theme.

This page defines the sponsor portal layout and is where you configure customizations for the portal page. Notice that there are both general portal style settings as well as mobile device style settings. Make any necessary adjustments as necessary if a customized sponsor portal is required.

alada	ise-1   admin   Logout   Feedback	
CISCO Identity Services Engine	The Administration V Policy Setup Assista	nt 🕶 🕐
🔆 System 🙀 Identity Management	Network Resources 🛛 🙀 Web Portal Management 🛛 👦 Feed Service	
Sponsor Group Policy Sponsor Groups	attings	
Settings Ports	Portal Theme     Subsetting: <ul> <li>Supple Logi</li> <li>Logi Dagia</li> <li>Logi Dagia</li> <li>Logi Dagia</li> <li>Supple Logi</li> <li>Supple Logi<!--</th--><th></th></li></ul>	
🙆 Help	Notifications	(0)
()	m	-

Step 4: Navigate to Administration > Identity Management > Identity Source Sequences, and then click Sponsor\_Portal\_Sequences.

**Step 5:** In the **Available** list, choose the AD identity store, **AD1**, and then move it to the top of the **Selected** list. This forces Sponsor authentication to use the AD database first and the Internal Users database second.

ahah	ise-1   admin   Logout   Feedback	
CISCO Identity Services Engine	Home Operations        Policy        Administration	Setup Assistant 👻 🕗 .
💑 System 🏼 👰 Identity Management 🛛 🕋 Ne	twork Resources 🛛 🛃 Web Portal Management 🛛 🖓 Feed Service	
Identities Groups External Identity Sources	Identity Source Sequences Settings	
Identity Source Sequences List > Sponsor_Portal_Sequence Identity Source Sequence		
✓ Identity Source Sequence		
* Name Sponsor_Portal_Sequence		
Description A built-in Identity Sequence for the Sp	onsor Portal	
▼ Certificate Based Authentication		
Select Certificate Authentication Profile	P	
<ul> <li>Authentication Search List</li> </ul>		
A set of identity sources that will be	accessed in sequence until first authentication succeeds	
Available	Selected	
Internal Endpoints Guest Users	Internal Users	
✓ Advanced Search List Settings		
Select the action to be performed if a selected identit	y store cannot be accessed for authentication	
O Do not access other stores in the sequence and	id set the "AuthenticationStatus" attribute to "ProcessError"	
<ul> <li>Treat as if the user was not found and proceed</li> </ul>	to the next store in the sequence	
Save		

Step 6: Click Save.

Step 7: Navigate to Administration > Web Portal Management > Sponsor Groups, and then click Add.

**Step 8:** Give the new group a name. (Example: OrganizationSponsorAllGroup)

Step 9: On the Authorization Levels tab, set the Account Start Time and Maximum Duration of Account in accordance with your InfoSec policy. (Example: 1 Day each)

alada	ise-1   admin   Logout   Feedback	
cisco Identity Services Eng	ine	Setup Assistant 🕶 🕗
💑 System 🛛 👰 Identity Manager	ment 📲 Network Resources 🛛 🙀 Web Portal Management 🛛 🖓 Feed Service	
Sponsor Group Policy Sponsor G	roups Settings	
Sponsor Group List > New Sponsor Group		
Sponsor Group		
General Authorization Lew	els Guest Roles Time Profiles	
Allow Login	Yes *	
Create Single Account	Yes *	
Create Random Accounts	Yes •	
Import CSV	Yes	
Send Email	Yes *	
Send SMS	Yes •	
View Guest Password	Yes	
Allow Printing Guest Details	Yes *	
View/Edit Accounts	All Accounts	
Suspend/Reinstate Accounts	All Accounts	
* Account Start Time	1 Days (Valid Range 1 to 999999999)	
* Maximum Duration of Account	1 Days (Valid Range 1 to 999999999)	
Submit Cancel		
4	Π	- F
🕗 Help		Notifications (0)

Step 10: In the Guest Roles section, select SponsorAllAccount.

Step 11: On the Time Profiles tab, in the Available list, select DefaultFirstLoginEight and DefaultStartEnd and move it to the Currently Selected list. Remove DefaultEightHours from the Currently Selected list.

ahah				ise-1   admi	n   Logout   Feedback	ρ
cisco Identity S	ervices Engine	🛕 Home	Operations    Polic	cy   🔻 Administration   🔻		Setup Assistant 👻 🕙
🔆 System 🏼 🖗	Identity Management	🔛 Network Resources	🛃 Web Portal Manaç	gement 🛛 🔯 Feed Service		
Sponsor Group Policy	Sponsor Groups	Settings				
Sponsor Group List > Orgini	zationSponsorAllGroup					
Sponsor Group						
General	Authorization Levels	Guest Roles	Time Profiles			
Available DefaultEightHours		* Currently Selected DefaultFirstLognEight DefaultStartEnd				

#### Step 12: Click Submit.

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

#### Step 13: Navigate to Administration > Web Portal Management > Sponsor Group Policy.

Step 14: Next to Manage All Accounts, under Identity Groups, click the + symbol, and then choose Any.

alah		ise-1   admin   I	Logout   Feedback	
cisco Identity Services Engine	🟠 Home Operations 🔻	Policy V Administration V		Setup Assistant 🕙
💑 System 🛛 🎇 Identity Management	Network Resources 🛛 🛃 Web Portal Mar	nagement 🕞 Feed Service		
Sponsor Group Policy Sponsor Groups	Settings			
Sponsor Group Policy				•
Define the Sponsor Group Policy by configuring rule	s based on identity groups and/or other condition	ons. Drag and drop rules to change the order.		
Status Policy Name	Identity Groups	Other Conditions	Sponsor Groups	
Manage All Accounts	SponsorAllAccount -	and Condition(s)	🛟 then	🚔 Acti
SponsorAllAccounts				
Manage Group Accounts	d Any	○ - +	🛟 then	🚔 Acti
SponsorGroupGrpAccounts 🔶		Any ntity Groups		
Manage Own Accounts	rF	٩	A then	Si Act
SponsorGroupOwnAccounts		- ⇔ • ■ •		ME
		🔲 Any		
		User Identity Groups >>		
		Endpoint Identity Groups >>		
				-
🕗 Help				Notifications (0)
•		m		

Step 15: Under the Other Conditions column for Manage All Accounts, click the + symbol, and then select Create New Condition.

alada				ise-1   admin	Logout   Feedback	Q		
CISCO Identity Services Engine		🙆 Но	ome Operations   ¥ Polic	cy 🛛 🔻 Administration 🛛 🔻			Setup Assist	ant 🕙
💑 System 🛛 🧸 Identity Management		Network Resources	🛃 Web Portal Manageme	ent 👦 Feed Service				
Sponsor Group Policy Sponsor Groups	Se	ttings						
Sponsor Group Policy Define the Sponsor Group Policy by configuring	rules b	ased on identity grou	ps and/or other conditions. Dra	aq and drop rules to change the orde	r.			-
Status Policy Name		Identity Groups	0	ther Conditions		Sponsor Groups		
Manage All Accounts	If	Any	🛟 and	Condition(s)	👄 then		÷	Acti
SponsorAllAccounts		Г						
Manage Group Accounts	If	SponsorGrou	Select Exi	isting Condition from Library () o	Create New Condit	ion (Advance Option)		
SponsorGroupGrpAccounts								
Manage Own Accounts	If	SponsorOwn						
SponsorGroupOwnAccounts								

Step 16: Under Expression, next to Select Attribute, click the down arrow. The menu opens.

**Step 17:** Next to AD1, click the > symbol, and then choose **ExternalGroups**.

ke-1   admin   Logout   Feedback D				
cisco Identity Services Engine		۲	me Operations   V Policy   V Administration   V	Setup Assistant 🕗
🔆 System 🥂 Identity Management		etwork Resource	Web Portal Management 🔂 Feed Service	
Sponsor Group Policy Sponsor Groups	Set	tings		
Sponsor Group Policy				
Define the Sponsor Group Policy by configuring	rules ba	sed on identity a	ps and/or other conditions. Drag and drop rules to change the order.	
Status Policy Name		Identity Groups	Other Conditions	Sponsor Groups
Manage All Accounts	If	Any		then 🙀 Actions*
SponsorAllAccounts	1		Add All Conditions Below to Library	
Manage Group Accounts	If	SponsorGrou	Condition Name Expression	)5 <del>v</del>
SponsorGroupGrpAccounts	1		AD1:ExternalGroups 📀 🛛 Equals 🔻 🛛	▼ @ <sub>*</sub>
Manage Own Accounts	If	SponsorOwn	ADI	15*
SponsorGroupOwnAccounts 🔶	1			
			↓ ■ .	<b>资</b> •
			IdentityAccessivestracted      ExternalCourse	
			Extensioops	
Save Reset				
O Help				Notifications (0)

**Step 18:** In first drop-down list, choose **Equals**, and then, in the second drop-down list, choose the AD group **yourdomain.local/Domain Users**, which was added earlier in Step 3 of Procedure 7, "Configure Cisco ISE to use Active Directory".

CISCO Identity Services Engine	í ho	me Operations   🔻 Policy   🕯	Administration   🔻	ise-1   admin   Logout
💑 System 🧏 Identity Management	Network Resources	🛃 Web Portal Management	Feed Service	
Sponsor Group Policy Sponsor Groups	Settings			
Sponsor Group Policy Define the Sponsor Group Policy by configuring Status Policy Name	rules based on identity group Identity Groups	os and/or other conditions. Drag ar Other	nd drop rules to change th Conditions	e order.
SponsorAllAc	If Any	4 and AD	1:ExternalGroups EQUAL	S cisco.loca 🗢 then
SponsorGrou	Expression AD1:ExternalGroups	Equals 🔻 cisco.local/Ust		then
SponsorGroupOwnAccounts	-	cisco.local/Use	s/Domain Users	then

Step 19: In the Sponsor Groups list, ensure the default, SponsorAllAccounts, is selected, and then click Save.

սիսիս				ise-1 (	admin   Logou	t   Feedback		
cisco Identity Services Engine		Home Operations	Po	licy 🔻 Administration 🛛			Se	itup Assistant 🕙
💑 System 🛛 🎉 Identity Management	The Net	twork Resources 🛛 🙀 Web Portal M	anagem	ent 🕞 Feed Service				
Sponsor Group Policy Sponsor Groups	Setti	igs						
Sponsor Group Policy								
Define the Sponsor Group Policy by configuring	rules bas	ed on identity groups and/or other cond	itions. D	rag and drop rules to change the order.				
Status Policy Name		Identity Groups	(	Other Conditions		Sponsor Groups		
Manage All Accounts	If	Any 💠	and	AD1:ExternalGroups EQUALS cisco.loca.	cþ then	SponsorAllAccounts	¢ ĝ	Actions*
Manage Group Accounts	] If	SponsorGroupAccounts	and	Condition(s)	then	SponsorGroupGrpAccounts	4 <sup>22</sup>	Actions*
Manage Own Accounts	] If	SponsorOwnAccounts	and	Condition(s)	🗘 then	SponsorGroupOwnAccounts	¢Ê	Actions*

**Procedure 2** Configure Cisco ISE guest authentication policy

In versions of Cisco ISE prior to ISE 1.2, ISE allowed each portal defined to support either guest, Central Web Authentication (CWA), or both. Starting in ISE 1.2, the guest users created by the sponsor are no longer displayed in the local identity store. Instead they are stored within the Guest Sponsor identity store and visible within the sponsor portal provided that the sponsor has the proper rights to view the guests accounts created.

As a result, guest user authentication requests may fail since the local identity store is used by default. In order to use the guest user identity store as opposed to the internal identity store, you need to create a policy that is triggered when a RADIUS authentication request comes from a guest anchor controller within the Internet edge DMZ.

**Step 1:** Within Cisco ISE, navigate to **Policy > Authentication**, select the down arrow to the right of Edit for the Dot1X policy, which came as part of the default ISE installation, and then click **Insert new row below** as shown.

ahaha			iser1   admin   Logout   Feedb	eck (D
cisco Identity Services Engine	Home Operations  Policy  Administ	ration 🔻		Setup Assistant 🕗
Authentication S Authorization	🔣 Profiling 👩 Posture 👸 Client Provisioning 🚊 Secu	ty Group Access 🛛 🔒 Policy Elements		
Authentication Policy				
Define the Authentication Policy by selectin Policy Type O Simple   Rule-Based	g the protocols that ISE should use to communicate with the network of	evices, and the identity sources that it should use for a	uthentication.	
MAB	: If Wired_MAB OR Allow Wireless_MAB	Protocols : Default Network Access	and	Edit   •
Default	: use Internal Endpoints			
Dot 1X	: If Wired_802.1X OR Allow Wireless. 802.1X	Protocols : Default Network Access	and	Fdt   +
🗹 Default	:use AD1			Insert new row below
				Duplicate below

Step 2: In the Rule Name box, remove the "Standard Rule 1" name and replace it with a meaningful name such as Wireless Guest Authentication. In the If Condition(s) box, click the +, and then choose Create New Condition (Advanced Option).

r 🗹 🔹	Guest Wireless Authentication	: 1f	Condition(s) Condition(s) Select Network Access O and	Done
	Default :	Use	Select Dating Gridten from Library. 0 or [Create New Condition (Advance Option)] 0	Actions +

**Step 3:** Under Expression, click the down arrow to the right of Select Attribute, and then click the arrow to the right of DEVICE.

alado a construction of the second	Bel (
CISCO Identity Services Engine	Policy V Administration V
Authentication Authentication Policy Define the Authentication Policy by selecting the protocols that ISE should use to communic Policy Type Simple Rule-Based MAB If Wried_MAB_OR	Provisioning Dictionaries Provisioning Arespace Cisco
Wickss_MAB Default ::use Internal Endpoints Dot1X :: If Wirkd_802.1X OR Wirkss_602.1X	Class And DetWood  DetWood  Access  Set  Set  Set  Set  Set  Set  Set
Default : use AD1     Select Attribute	Radus ,
Default     : Use     Condition Name     Select	Expression et Attribute 📀 📀 🖓 🖓

Next, ensure the policy triggers when a guest wireless LAN controller device type is responsible for the authentication request.

**Step 4:** Select **Device Type** for the Selection Attribute, leave **Equals** as the default condition, click the down arrow to the right of the Device Type, and then choose **All Device Types#WLC-Guest**. The WLC-Guest Device type was created previously in Step 6 of Procedure 6 above.

abala za da contra contra		ise-1 (
CISCO Identity Services Engine		
📃 Authentication 👩 Authorization 🔀 Profiling 💽 Posture 👸 Client Provisioning 📑 Security Group Access 🞄 Policy	Ek	
Authentication Policy		
Define the Authentication Bolicy by selection the protocols that ISE should use to communicate with the network devices and the identity enurge		
Policy Type Simple Rule-Based	All Device Types	
	All Device Types#WLC-Guest	
MAB : If Wired_MAB OR Allow Protocols : Default Network /	Aci ADI >	
" Wireless_MAB	Airespace >	
Default : use Internal Endpoints	CERTIFICATE > E	
	Cisco >	
Dot1X : If Wired_802.1X OR Allow Protocols : Default Network A Wireless 802.1X	Aci Cisco-BBSM >	
Default : use AD1	Cisco-VPN3000 >	
	DEVICE >	
🖉 🗸 Guest Wireless Authentication : If Select Attribute 👝 Allow Protocols : Select Network Acces	as EndPoints >	
	Guest >	
Add All Conditions Below to Library	IdentityGroup >	
Condition Name Expression		
DEVICE:Device T 📀 Equals 🔻 All Device Types#.		- iii

Step 5: In the Allow Protocols: Select Network Access box, click the down arrow, and then, under Allowed Protocols, select Default Network Access.

🛛 🖉 🗸 Guest Wireless Authentication : If DENCE Device Type EQUIALS De 💠 Allow Protocols : [Default Network Access 💽 and 🖕	Done
Allowed Protocols	
🛂 Detault : Uzer Guest Users 💠	Actions +
U Default Network Access	

Step 6: Click the + for the Use.

**Step 7:** Next to the **Identity Source** box, click the down arrow, and then choose **Guest Users** as the Identity Source that will be used for authentication requests matching the If condition–namely RADUIS requests from the Internet edge guest anchor controllers.

altada		ise-1   admi	Lopost   Feedback
cisco Identity Services Engine  ( ) Home Operations   Policy  Administrati	ni <b>v</b>		Setup Assistant
🔒 Authentication 🧑 Authorization 📝 Profiling 👰 Posture 👼 Client Provisioning 😭 Security C	roup Access . Policy Elements Identity Source List		
Authentication Policy	٩		
Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devic	es, and 🖕 🖌 📃 🔹 🛞 🖕	authentication.	
Policy Type O Simple O Rule-Based	Internal Endpoints		
MAB : If Wired_MAB OR Allow Pro	u Internal Users	and	Edit   👻
Wireless_MAB	a Guest users	-	
Deraut : use interna Endpoints	MyDevices_Portal_Sequence		
Dot1X : If Wired_802.1X OR Allow Pro	tocols B Sponsor_Portel_Sequence	and	Edit   👻
Default :use AD1	Guest_Portal_Sequence		
	U DenyAccess		
Guest Wireless Authentication : If DEVICE Device Type EQUALS De 💠 Allow Proton	ols : Dr	•	Done
Default : Use Guest Users			Actions *
Identity Source Guest Users	0		
Options	_		
If authentication failed Reject *			
If process failed Drop *			
Default Rule (If no match) : Allow Protoc Note: For authentications using PEAP_IEAP_EAP_EAP_OT or J	ADD IS MSCHAR		Edit   •
t is not possible to continue processing when authenticatio	n fails or user is not found.		
a containe option is selected in these cases, requests with			

Step 8: In the upper right corner, click Done, and then click Save. The Authentication Policy is saved.





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

#### Procedure 1 Create network objects

The use of objects and group objects in Cisco ASA make the configuration of the ASA appliance more easily understood. The following steps create a series of objects that represent the WLCs in your environment.

OO Reader Tip

The number of ISEs in your environment may vary. The list below is based on two ISE servers providing authentication services.

#### Table 32 - Identity Server Engine network objects

Network object name	Object type	IP address
internal_ISE-1	Host	10.4.48.41
internal_ISE-2	Host	10.4.48.42

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

**Step 2:** Repeat Step 3 through Step 6 for all objects listed in Table 32. If the object already exists, skip to the next object in the table.

#### Step 3: Click Add > Network Object.

The Add Network Object dialog box appears.

**Step 4:** In the **Name** box, enter a description of the WLC. (Example: internal\_ISE-1)

Step 5: In the Type list, choose Host.

**Step 6:** In the **IP Address** box, enter the WLC's management interface IP address, and then click **OK**. (Example: 10.4.48.41)

🔂 Add Network	: Object
Name:	internal_ISE-1
Туре:	Host 🗸
IP Version:	IPv4
IP Address:	10.4.48.41
Description:	ISE 1 Server
NAT	*
	OK Cancel Help

After adding the network objects listed in Table 32, you create network object groups that contain each of the ISE servers in your environment. Creating network object groups simplifies the security policy configuration for similar network objects.

#### Table 33 - Wireless LAN controller object groups

Network object group	Network objects	Group description
internal-ISE-Servers	internal_ISE-1 Internal_ISE-2	Internal ISE Servers

#### Step 7: Click Add > Network Object Group.

The Add Network Object Group dialog box appears.

Step 8: In the Group Name box, enter a name for the group. (Example: internal-ISE-Servers)

Step 9: For each network object listed in Table 33, select the network object in the Existing Network Objects/ Groups list, and then click Add to move each network object into the Members in Group list.

up Name	: internal-ISE-Servers						
cription:							
Existing M	Network Objects/Groups:				Members in Group:		
Name	<b>▲</b> 1	IP address	Netrr		Name	IP Address	Netmas
	l deux cucata entrunel:	100.160.00.0	OFF C A		👝 🖪 internal_ISE-1	10.4.48.41	
	g umz-guesis-network	192.108.28.0	200.2		- 🖪 internal_ISE-2	10.4.48.42	
	g umz-management-network L dess web setwerk	192.168.23.0	200.2				
	g umz-web-network	192.108.10.0	200.2				
	s unz vie netvork	10.4.24.0	255 1 =				
	nutside-16-network	172 16 130 0	255.2				
	outside-17-network	172 17 130.0	255.2				
	dmz-dmynn-1	192 168 18 10	20012				
	dmz-dmvnn-2	192,168,18,11					
	dmz-esa-c100v-ISPa	192.168.17.25					
	dmz-esa-c100v-ISPb	192.168.17.25					
	dmz-quests-network-ISPa	192.168.28.0	255.2	Add			
	dmz-networks	192.168.16.0	255.2	Auu //			
🔳	dmz-webserver1-ISPa	192.168.16.100		<< Remove			
	dmz-webserver1-ISPb	192.168.16.100					
	dmz-wahearvar2-IGPa	102 168 16 101	*				
•	111		•				
Create n	ew Network Object member:						
Name: (	optional)						
Type:	Host		•				
IP Versio	on: 💿 IPv4 🔘 IPv6						
IP Addro							
I Addre							
					4		
					× [		

Step 10: Review the configured network object groups for completeness, and then click OK.

Configuration > Firewall > Obje	<u>cts</u> > <u>Network Objects/G</u> i	<u>oups</u>			
🗣 Add 🔹 🗹 Edit 📋 Delete   🔍 N	Where Used 🔍 Not Used				
Filter:					Filter Clear
Name		IP Address	Netm	Description	Object NAT
Network Objects					
🖻 Network Object Groups					
🕀 🎯 dmz-wlc-group					
🗄 🐨 dmz-wic-redundancy-grou	μ				
🖬 🌌 internal-ISE-Servers	Ν				
- 📇 internal_ISE-1	Cinc. 2	10.4.48.41		ISE 1 Server	
🛄 internal_ISE-2	Size: Z	10.4.48.42		ISE 2 Server	
🗄 😹 internal-wic-group	Internal_ISE-1			Internal Wireless LAN Controllers	
	internal_ISE-2				

Procedure 2 Create Cisco ASA security policy for Cisco ISE

If you are using the shared guest WLC deployment model, in which the WLC resides on the internal network, skip to Procedure 3. If you are using the dedicated deployment model, in which the WLC resides on the Internet DMZ, continue to the next step.

Step 1: On the Internet edge ASA appliance, navigate to Configuration > Firewall > Access Rules.

Table 34 -	Firewall policy rules	for Identity Services	Engine
------------	-----------------------	-----------------------	--------

Interface	Action	Source	Destination	Service	Description	Logging Enable / Level
Any	Permit	dmz-mgmt- wlan-network	internal-ISE- Servers	udp/1812, udp/1813	Allows WLCs to communicate to internal ISE servers using RADIUS	Selected / Default

Step 2: Click the rule that denies traffic from the dmz-networks toward the internal network.

Step 3: Click Add > Insert.

Step 4: In the Interface list, choose the interface. (Example: Any)

Step 5: For the Action option, select the action. (Example: Permit)

Step 6: In the Source box, choose the source. (Example: dmz-mgmt-wlan-network)

Step 7: In the Destination box, choose the destination. (Example: internal-ISE-Servers)

Step 8: In the Service box, enter the service. (Example: udp/1812, udp/1813)

Step 9: In the Description box, enter a useful description

Step 10: Select or clear Enable Logging. (Example: Selected)

Step 11: In the Logging Level list, choose the logging level value, and then click OK. (Example: Default)

🔁 Add Access	Rule
Interface:	Any 🔻
Action: 🧿 Pern	nit 🔘 Deny
Source Criteria	
Source:	192.168.19.0/24
User:	
Security Group:	
Destination Cuits	
Destination of the	
Cosuritu Crourou	
Security Group:	
Service:	udp/1812, udp/1813
Description:	Allows WLCs to communicate to internal ISE servers using RADIUS
🔽 Enable Loggi	ng
Logging Levi	el: Default 👻
More Options	*
	OK Cancel Help

Step 12: After adding the rule in Table 34, click Apply on the Access Rules pane.

29	<b>V</b>	dmz-mgmt-wlan-network/24	internal-ISE-Ser	₩⊅ 1812 ₩> 1813	🖌 Permit		
30	<b>v</b>	뤍 dmz-guest-wlan-network/22	를 dmz-networks 를 internal-network	ıı⊅ ip	😮 Deny	3	Deny traffic from the wireless guest network to the internal and dmz resources
31	1	🚔 dmz-guest-wlan-network/22	<li>any</li>	팓 ip	🖌 Permit	37	Allow Wireless DMZ users access to the Internet
32	<b>v</b>	👼 dmz-networks	any4	팓 ip	🕴 Deny	10 2	Deny IP traffic from DMZ to any other network.

#### Procedure 3 Configure firewall policy for web portal

Wireless guest clients need access through the firewall to the Cisco ISE server in order to access the web portal for their authentication requests.

Step 1: On the Internet edge ASA appliance, navigate to Configuration > Firewall > Access Rules.

T-I-I-OF	<b>—</b> !			6- 10	F 14/-1-	Dentel
1 able 35 -	Firewall	policy	ruie	tor IS	E VVED	Portai

 $\checkmark$ 

Interface	Action	Source	Destination	Service	Description	Logging Enable / Level
Any	Permit	dmz-guest- wlan-network	internal-ISE- Servers	tcp/8433	Guest Client Web Portal access for Authentication Requests	Selected / Default

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

Step 3: Click Add > Insert and then, using the information listed in Table 35, continue with this procedure.

- Step 4: In the Interface list, choose the interface. (Example: Any)
- Step 5: For the Action option, select the action. (Example: Permit)
- **Step 6:** In the **Source** box, choose the source. (Example: dmz-guest-wlan-network)
- Step 7: In the Destination box, choose the destination. (Example: internal-ISE-Servers)
- Step 8: In the Service box, enter the service. (Example: tcp/8433)
- Step 9: In the Description box, enter a useful description.
- Step 10: Select or clear Enable Logging. (Example: Selected)

Step 11: In the Logging Level list, choose the logging level value, and then click OK. (Example: Default)

🔤 Add Access	Rule
Interface:	Any 💌
Action: 🧿 Perm	nit 🔘 Deny
Source Criteria	
Source:	192.168.28.0/22
User:	
Security Group:	
Destination Crite	ria
Destination:	internal-ISE-Servers 🔤
Security Group:	
Service:	trp/8443
Description:	Guest Client Web Portal access for Authentication Requests
🔽 Enable Loggi	ng
Logging Leve	al: Default 🔹
More Options	*
	OK Cancel Help

Step 12: After adding the rule in Table 35, click Apply on the Access Rules pane.

 29
 ✓
 J dnz-guest-wlan-network/22
 J fittemal-ISE-Ser...
 100
 843
 ✓ Permit
 0
 Guest Client Web Portal access for Authentication Requests

 30
 ✓
 J dnz-guest-wlan-network/22
 J dnz-networks
 IP
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P
 P</

Procedure 4 Configure the WLC for ISE Server

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

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

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

Step 4: Click New.

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

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

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

August 2014 Series



					Sa <u>v</u> e C	onfiguration   <u>P</u> i	ing   Lo	gout   <u>R</u> efresh
CISCO	MONITOR WLANS	<u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK
Security	ecurity RADIUS Authentication Servers					< Bac	k	Apply
AAA     General     RADIUS     Authentication     Accounting     Enthance	Server Index (Prior Server IP Address Shared Secret Forr Shared Secret	ity) nat	2 ‡ 10.4.48.41 ASCII ‡					
► TACACS+ LDAP Local Net Users	Confirm Shared Se Key Wrap	cret	••••••••••••••••••••••••••••••••••••••	r FIPS custome	ers and requires a	key wrap complia	Int RADIU	JS server)
Disabled Clients User Login Policies AP Policies Password Policies	Port Number Server Status Support for RFC 35	76	1812 Enabled					
Local EAP	Server Timeout		2 second	is				
<ul><li>Priority Order</li><li>Certificate</li></ul>	Network User Management	☑ Enable						
Access Control Lists	IPSec		Enable					
Wireless Protection     Policies								
Web Auth								
Advanced								

Step 8: Next to Management, clear the Enable check box, and then click Apply.

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

Step 10: Click New.

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

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

									10ut   <u>R</u> efresh
cisco	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK
Security	RADIUS A	Account	ing Servers >	• Edit			< Bac	k	Apply
	Server Ad Shared Se Shared Se	dress ecret Forma ecret	10.4 at ASC	.48.41					
▶ TACACS+ LDAP Local Net Users MAC Filtering	Confirm S Port Numl Server Sta	hared Secr per atus	et •••• 181	bled \$					
Disabled Clients User Login Policies AP Policies Password Policies	Server Tin Network L	neout Jser	2 2 E	seconds nable Enable					
Local EAP	1.000			Lindbic					
Priority Order									
Certificate									
Access Control Lists									
Wireless Protection     Policies									
Web Auth									
Advanced									

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

**Step 14:** Click **Apply**, and then repeat the process for the redundant secondary Cisco ISE server. (Example: 10.4.48.42)

#### Procedure 5 Modify guest WLAN on Cisco AireOS WLC to use Cisco ISE

Step 1: On the guest anchor wireless LAN controller's main menu bar, click WLANs.

In order to modify the Web Authentication Type later in the procedure, you must disable the WLANs using Web-Auth as an authentication method. The following steps disable, modify, and re-enable the Guest WLAN.

Step 2: Next to the Guest Wireless LAN (WLAN), select the check box.

،،ا،،،ا،، cısco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	Sa <u>v</u> e C <u>O</u> MMANDS	Configur	ration <u>P</u> ing <u>F</u> EEDBACK	Logout   <u>R</u> e	fresh
WLANs	WLANs								En	tries 1 - 1 o	of 1
WLANs	Current Filt	er: No	ne [ <u>Change</u>	e Filter] [Clear F	Create New 🗧 Go						
Advanced		Туре	Profile Nam	ie	WLAN :	SSID	Admin Status	Sec	urity Policies		
	2 WLAN Guest		Guest	Guest			Enabled Web-Auth		b-Auth		

Step 3: Click the down arrow next to Create New, in the list, choose Disable Selected, and then click Go.

Step 4: Click OK. This confirms that you want to disable the selected WLANs.

Step 5: Repeat this process for each Guest WLAN that you may have created.

Step 6: Click the WLAN ID for the Guest WLAN that you want to edit (Example: 2).

**Step 7:** On the Advanced tab, next to Allow AAA Override, select **Enabled**. This allows the per-client session timeout to be set from the Cisco ISE server.

			Logout   Kerresh
CISCO	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK		
WLANs	WLANs > Edit 'Guest'	< Back	Apply
VLANS WLANS	General Security QoS Policy-Mapping Advanced		
▶ Advanced	Allow AAA Override 🖉 Enabled DHCP Coverage Nole Detection 🖉 Enabled DHCP Server 🔲 Override		Î
	Enable Session Timeout (seco) DHCP Addr. Assignment 🖉 Required Aronet JE Transled DEAP Dispositor Channel Chanled		
	Override Interface ACL         IPv4         INne         IPv6         None         IEnabled           Layer2 Ad         None          Management Frame Protection (http://innet.i		
	P2P Blocking Action Disabled • MP9 Client Protection # Optional • Client Evolution # @Enabled Timeout Value (seco) DTIM Period (in beacon intervals)		
	Maximum Adoved Clents #         0           Static ID Turnwing #1         @Enabled         002.11a/n (1 - 255)         1           Wri-F Direct Clents Policy         Disabled ▼         002.11b/m (1 - 255)         1		
	NAC         NAC           Clew HMSpkt Camfiguration         Enabled           NAC State         NAC State           Clew HMSpkt Camfiguration         Enabled           Clew Local Biancing and Band Select         Enabled		
			+

Step 8: For security purposes, next to DHCP Addr. Assignment, select Required .

#### Step 9: Click Apply.

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

Step 10: Navigate to Security > Access Control Lists > Access Control Lists, and then click New. This allows you to create a new access control list.

August 2014 Series

Step 11: In the Access Control List Name box, enter a name for the ACL, and then click Apply.

<u>W</u> LANs		WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK
Acc	cess Control L	ists > New			< Bac	k	Apply
Acc	<b>eess Control Lis</b> CL Type	t Name Pre-	Auth-for-Exte	rnal-Web-Server			

i	Tech Tip							
You n	eed to apply the access control list to the DMZ based anchor controllers (but this							
is not	needed on any of the foreign anchor controllers). This is because the raw guest							
user traffic originates from the DMZ anchor controller. Prior to this, the guest traffic was								
encap	sulated in CAPWAP between the anchor and foreign anchor controllers.							

Step 12: Click the name of the ACL.

Step 13: Click Add New Rule

**Step 14:** Enter the following information, and then click **Apply**. This defines an ACL that allows access to the management network. In this example, access is allowed to the 10.4.48.0 network, and access to specific resources is controlled on the Cisco ASA itself. This approach reduces the locations in which changes need to be made as the network evolves.

- · Sequence-1
- Destination-IP Address
- · IP Address-10.4.48.0
- Netmask-255.255.255.0
- Action-Permit

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	<u>F</u> EEDBACK
Access C	ontrol L	ists > Rules >	New			1	< Back	Apply
Sequence		1						
Source		Any -	•			20		
			-	IP Addre	ss N	letmask		
Destination		IP Address 🔻		10.4.48	.0	255.255.255.0		
Protocol		Any	•					
DSCP		Any 🔻	·					
Direction		Any 🔻						
Action		Permit 🔻	·					

Step 15: Click Add New Rule.

**Step 16:** Enter the following information, and then click **Apply**. This defines another ACL entry in order to allow the return traffic from the 10.4.48.0 network to the guest clients.

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

MONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	COMMANDS	HE <u>L</u> P	<u>F</u> EEDBACK
Access C	ontrol L	ists > Rules >	New			1	< Back	Apply
Sequence		2		ID Addre		Netmask		
Source		IP Address	·	10.4.48	.0	255.255.255.0		
Destination		Any 🗸	•					
Protocol		Any	•					
DSCP		Any 🔻						
Direction		Any -						
Action		Permit 👻	•					

Step 17: Navigate to WLANs.

Step 18: Click the WLAN ID for the specific guest WLAN (Example 2)

Step 19: Click Security, and then click Layer 3.

**Step 20:** On the Layer 3 tab, make sure **Web Policy** is selected, and then in the **IPv4** list, choose the ACL that was created in Step 10 (Example Pre-Auth-For-External-Web-Server).

Sleeping wireless clients are clients with guest access that have successfully completed web authentication. For battery conservation, these devices may go to sleep and wake up over the period of time that they are connected to the Guest Wireless network. To prevent these devices from having to repeat the web authentication, enable the sleeping client function.

Step 21: Next to Sleeping Client, select Enable, and then click Apply.

WLANS     WLANS	General Security QoS Policy-Mapping Advanced
Advanced	Layer 2 Layer 3 AAA Servers
	Layer 3 Security 4 Web Policy •
	Authentication
	Passthrough
	Conditional Web Redirect
	Splash Page Web Redirect
	On MAC Filter failure <sup>10</sup>
	Preauthentication ACL IPv4 Pre-Auth-for-External-Web-Server V IPv6 None V WebAuth FlexAd None V
	Sleeping Client 🗹 Enable
	Sleeping Client Timeout(1 to 720 Hrs) 12
	Over-ride Global Config Enable

If you are using a shared deployment model, in which the WLC lives on the *inside* of the Internet edge firewall, it will typically provide authentication services to both wireless guest users as well as internal enterprise wireless users. If this is the case, continue to the next steps. If however, you are using a dedicated deployment model, in which the WLC resides on the Internet edge DMZ and handles only guest wireless, skip to Step 25.

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

**Step 22:** On WLC controller, navigate to **WLANs**, and edit the WLAN by selecting the Guest Wireless LAN number. (Example 2)

Step 23: Under the Guest WLAN selected, navigate to Security > AAA Servers. Ensure that both Authentication Servers and Accounting Servers are enabled by selecting the Enabled check box under each column respectively.

Step 24: Scroll down to the bottom of the screen and under Authentication Priority order for web-auth user, move RADIUS to the top of the list followed by LOCAL, ensure that LDAP is under Not Used, and then click Apply.

i	Tech Tip
lt is no serve	ot necessary to select the server from the list because the enabled RADIUS r(s) defined under the Security > RADIUS > Authentication will be used.

ANs	WLANs > Edit 'Guest'	< Back Apply
VLANs WLANs	General Security QoS Policy-Mapping Advanced	
Advanced	Layer 2 Layer 3 AAA Servers	
	Select AAA servers below to override use of default servers on this WLAN	×
	Padius Servers	1
	Radius Server Overwrite interface	
	Authentication Servers Accounting Servers	=
	V Enabled V Enabled	
	Server 1 None  Vone	
	Server 2 None   None	
	Server 3 None   None	
	Server 4 None  Vone  Vone	
	Server 5 None   None	
	Server 6 None Vone Vone	
	Radius Server Accounting	
	Interim Update	
	LDAP Servers	
	Server 1 None •	
	Server 2 None *	
	Local EAD Authentication	
	Local EXP Authentication Enabled	
	Authentication priority order for web-auth user	
	Not Used Order Used For Authentication	
	LDAP > RADIUS Up	
	< LOCAL Down	
		•

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

Step 25: Navigate to Security > Web Auth > Web Login Page.

Step 26: In the Web Authentication Type list, choose External (Redirect to external server).

**Step 27:** If desired, in the **Redirect URL after login** box, enter a URL for the webpage that the user will be redirect to after they log in. (Example www.cisco.com)

**Step 28:** In the **External Webauth URL** box, enter the following URL which is the Cisco ISE server's guest portal login page:

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

**Step 29:** Click **Apply**, and then click **OK**. This confirms that you have been reminded to configure the external pre-authentication ACL.

սիսիս						Sa <u>v</u> e (	Configuration   P	ing   Lo	gout <u>R</u> efresh
CISCO	<u>M</u> ONITOR	<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	MANAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Security	Web L	ogin Pag	le				Preview	v	Apply
	Web A	uthenticatio	on Type		External (Redir	ect to external serv	er) 🔻		
Local EAP	Redired	t URL after	login		www.cisco.com	n			
Priority Order	Extern	al Webauth	URL	htt	:ps://ise-1.cisco	.local:8443/guestpc	rtal/Login.action		
Certificate									
Access Control Lists									
Wireless Protection Policies									
<ul> <li>Web Auth</li> <li>Web Login Page</li> <li>Certificate</li> </ul>									
TrustSec SXP									
Advanced									



The next step is to enable the guest WLANs that had to be disabled in the previous procedure in order to change the authentication method.

Step 1: On the menu bar, navigate to WLANs.

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

Step 3: Next to Create New, click the arrow, and then choose Enable Selected.

uluilu cisco	Monitor what controller wireless security management commands help eeedback	Saye Configuration
WLANs	WLANs	
WLANs     WLANs	Current Filter: None [Change Filter] [Clear Filter] Enable Selected  Go	
Advanced	E WLAN ID Type Profile Name WLAN SSID Admin Status Security Policies	
	Image: WLAN         Guest-10k         Enabled         Web-Auth	

Step 4: Click Go, and then click OK.



#### Procedure 7 Enable captive portal bypass

Because of a change made in Apple iOS device behavior when connecting to a guest wireless network that uses web authentication, you may need to enable captive portal bypass via the CLI of the WLC. Using Wireless Internet Service Provider roaming (iWISPr) protocol, Apple devices attempt to determine if they have an active connection to the Internet by repeatedly trying to access a designated and hidden Apple website (http://www. apple.com/library/test/success.html). When the wireless devices gets re-directed to the Web Authentication page and does not receive a response for the designated website, the Apple device will launch a pseudo web browser to allow the user to authenticate. This pseudo browser may not work properly when being redirected to Cisco ISE. The captive-bypass enable command will prevent this pseudo browser from being launched and instead allow the user to authenticate when opening a standard browser.

Step 1: Using SSH, navigate to the IP address of the guest WLC, and then log in with an administrator account.

**Step 2:** Enable captive bypass, save the configuration, and then restart the controller by entering the following commands.

(Cisco Controller) config network web-auth captive-bypass enable Web-auth support for Captive-Bypass will be enabled. You must reset system for this setting to take effect. (Cisco Controller) >save config Are you sure you want to save? (y/n) y Configuration Saved! (Cisco Controller) >reset system

Are you sure you would like to reset the system? (y/N) ${\bf Y}$ 

**Step 3:** If you are using a Cisco 2500 series WLC, repeat Procedure 4 for the resilient 2500 series WLC. This is necessary because the 2500 WLC does not support HA SSO and the two controllers must be individually configured.



Procedure 1 Use the Sponsor Portal

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

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

cisco Sponsor Portal	
	Username: employee1 Password: •••••• Sign On
7 1 m	



CISCO Sponsor Portal			Welcome employee1   <u>Mr Settinas</u>   <u>Sign Out</u>
Manage Guest Accounts	Create Account	Import Accounts	Create Random Accounts
Account List			
Frlit Fmail Drint Dainetata Suenard Dalata			*
Username Status	First Name	Last Name	Email Address
Show 10 • entries	Showing 0 to 0 of 0 entries		First Previous Next Last
	m		

**Step 3:** Enter the information for the guest account as required by corporate policy (and the settings implemented in Procedure 1, "Configure Cisco ISE Sponsor settings", in the "Configuring Cisco ISE Sponsor Portal Services" process, and then click **Submit**.

**Step 4:** If you have configured an SMTP server in Cisco ISE, you can optionally send an email notification to the user by selecting the **Send email notification**. In this particular example, the sponsor enters the first and last name, email address, and company name.

CISCO Sponsor Portal	Wekome employee1   My Settings   Spn Out
Create Account	
First name:	David
Last name:	Smith
Email address:	dsmith@anywhere.com
Phone number:	555-555-0100
Company:	Any Company
Optional data 1:	
Optional data 2:	
Optional data 3:	
Optional data 4:	
Optional data 5:	
* Guest role:	Guest
* Account duration:	DefaultEightHours
* Time zone:	GMT -07:00 US/Pacific *
* Notification language:	English
	Submt Cancel
	Heb
	heip

When the account is successfully created, Cisco ISE displays the guest account and credentials.

August 2014 Series

**Step 5:** For testing purposes, write down the username that was automatically created. (Example: dsmith01/36\_7M2tiY)

CISCO Sponsor Portal	Welcome employee1   My Settings   Sign Out
Successfully Created Guest Account:	
Username:	dsmith01
Password:	36_7M2tiY
First name:	David
Last name:	Smith
Email address:	dsmith@anywhere.com
Phone number:	555-555-0100
Company:	Any Company
Status:	Awaiting Initial Login
Suspended:	false
Optional data 1:	
Optional data 2:	
Optional data 3:	
Optional data 4:	
Optional data 5:	
Guest role:	Guest
Time zone:	GMT -07:00 US/Pacific
Notification language:	English
Account duration:	DefaultEightHours
Account start date:	2013-09-13 13:32:48
Account expiration date:	2013-09-13 21:32:48
	Print View Guest Accounts
Hain	

The guest user account is now created and is shown as Awaiting Initial Login.

ili. cis	co Spon:	sor Portal				Welcome employee1   <u>Mr Settinas</u>   <u>San C</u>
Ma	inage Gi	uest Accou	ints			
				Create Account	Import Accounts	2+ Create Random Accounts
Ac	count List					
						\$
	Edit Email	Print Reinstate Username	Suspend Delete Status	Change Account Duration First Name	Last Name	Email Address
8	dsmith01		Awaiting Initial Login	rid	Smith	dsmith@anywhere.com
s	Show 10 • ent	tries		Showing 1 to 1 of 1 entri	25	First Previous 1 Next Last
			Hel	2		

#### Procedure 2 Testing the wireless user guest accounts

For guests to be authenticated, they need to connect to the guest SSID and get an IP address from the 1128 VLAN that will be in the 192.168.28.0/22 range.

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

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

C Certificate C C Guest Portal X	6 🛧 🛱
	~
alulu -	
CISCO Guest Portal	
Username: dsmith01	
Password:	~
Sign On	
Change Password	
	~
	>

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

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



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



#### i Tech Tip

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

config network web-auth secureweb disable

## Appendix A: Product List

## **Wireless LAN Controllers**

Functional Area	Product Description	Part Numbers	Software	
Remote Site	Cisco 7500 Series Wireless Controller for up to 6000 Cisco access points	AIR-CT7510-6K-K9	7.6.120.0	
Controller	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 7500 Series Wireless Controller for up to 1000 Cisco access points	AIR-CT7510-1K-K9		
	Cisco 7500 Series Wireless Controller for up to 500 Cisco access points	AIR-CT7510-500-K9		
	Cisco 7500 Series Wireless Controller for up to 300 Cisco access points	AIR-CT7510-300-K9	]	
	Cisco 7500 Series High Availability Wireless Controller	AIR-CT7510-HA-K9		
	Cisco Virtual Wireless Controller for up to 5 Cisco access points	L-AIR-CTVM-5-K9		
	Cisco Virtual Wireless Controller 25 Access Point Adder License	L-LIC-CTVM-25A		
	Cisco Virtual Wireless Controller 5 Access Point Adder License	L-LIC-CTVM-5A		
	Cisco Virtual Wireless Controller 1 Access Point Adder License	L-LIC-CTVM-1A		
On Site Controller	Cisco 5760 Series Wireless Controller for up to 1000 Cisco access points	AIR-CT5760-1K-K9	3.3.3SE(15.0.1EZ3)	
	Cisco 5760 Series Wireless Controller for up to 500 Cisco access points	AIR-CT5760-500-K9		
	Cisco 5760 Series Wireless Controller for up to 250 Cisco access points	AIR-CT5760-250-K9		
	Cisco 5760 Series Wireless Controller for up to 100 Cisco access points	AIR-CT5760-100-K9		
	Cisco 5760 Series Wireless Controller for up to 50 Cisco access points	AIR-CT5760-50-K9		
	Cisco 5760 Series Wireless Controller for up to 25 Cisco access points	AIR-CT5760-25-K9		
	Cisco 5760 Wireless Controller for High Availability	AIR-CT5760-HA-K9		
On Site, Remote Site, or Guest	Cisco WiSM2 Series Wireless Controller for up to 1000 Cisco access points	WS-SVC-WISM2-K-K9	7.6.120.0	
Controller	Cisco WiSM2 Series Wireless Controller for up to 500 Cisco access points	WS-SVC-WISM2-5-K9	]	
	Cisco WiSM2 Series Wireless Controller for up to 300 Cisco access points	WS-SVC-WISM2-3-K9		
	Cisco WiSM2 Series Wireless Controller for up to 100 Cisco access points	WS-SVC-WISM2-1-K9		
	Cisco WiSM2 Series Wireless Controller for High Availability	WS-SVC-WISM2-HA-K9		
	Cisco 5500 Series Wireless Controller for up to 500 Cisco access points	AIR-CT5508-500-K9		
	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,	Cisco 2500 Series Wireless Controller for up to 50 Cisco access points	AIR-CT2504-50-K9	7.6.120.0	
Guest 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 3700 Series Access Point 802.11ac and CleanAir with Internal Antennas	AIR-CAP3702I-x-K9	7.6.120.0
	Cisco 3700 Series Access Point 802.11ac and CleanAir with External Antenna	AIR-CAP3702E-x-K9	
	Cisco 3600 Series Access Point Dual Band 802.11a/g/n and CleanAir with Internal Antennas	AIR-CAP3602I-x-K9	
	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	

## Wireless LAN

Functional Area	Product Description	Part Numbers	Software
Wireless LAN	Cisco 802.11ac Wave 1 Module for 3600 Series Access Point	AIR-RM3000AC-x-K9=	7.6.120.0
	Cisco 802.11ac Wave 1 Module for 3600 Series Access Point 10 Pack	AIR-RM3000ACxK910=	
Cisco ISE Server	Cisco Identity Services Engine Virtual Appliance	ISE-VM-K9=	1.2.0.899– Cumulative Patch 8
	Cisco ISE Wireless 5-year License for 500 Endpoints	LS-ISE-AD5Y-W-500=	
	Cisco ISE Wireless 5-year License for 250 Endpoints	LS-ISE-AD5Y-W-250=	
	Cisco ISE Wireless 5-year License for 100 Endpoints	LS-ISE-AD5Y-W-100=	

## **Access Control**

Functional Area	Product Description	Part Numbers	Software
Authentication Services	ACS 5.5 VMware Software And Base License	CSACS-5.5-VM-K9	5.5.0.46.2 Cumulative Patch

## Internet Edge

Functional Area	Product Description	Part Numbers	Software
Firewall	Cisco ASA 5545-X IPS Edition - security appliance	ASA5545-IPS-K9	ASA 9.1(5) IPS 7.1(8p2)E4
	Cisco ASA 5525-X IPS Edition - security appliance	ASA5525-IPS-K9	
	Cisco ASA 5515-X IPS Edition - security appliance	ASA5515-IPS-K9	
	Cisco ASA 5512-X IPS Edition - security appliance	ASA5512-IPS-K9	
	Cisco ASA 5512-X Security Plus license	ASA5512-SEC-PL	
	Firewall Management	ASDM	7.1(6)

## Internet Edge LAN

Functional Area	Product Description	Part Numbers	Software
DMZ Switch	Cisco Catalyst 2960-X Series 24 10/100/1000 PoE and 2 SFP+ Uplink	WS-C2960X-24PS	15.0(2)EX5 LAN Base license
	Cisco Catalyst 2960-X FlexStack-Plus Hot-Swappable Stacking Module	C2960X-STACK	

## **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(3) Layer 3 License
	Cisco Nexus 5596 Layer 3 Switching Module	N55-M160L30V2	
	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	
	Cisco Nexus 5500 Layer 3 Enterprise Software License	N55-LAN1K9	
	Cisco Nexus 5500 Storage Protocols Services License, 8 ports	N55-8P-SSK9	
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 4500E Series 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.3.1XO(15.1.1XO1) IP Base license
	Cisco Catalyst 4500E Supervisor Engine 8-E, Unified Access, 928Gbps	WS-X45-SUP8-E	
	Cisco Catalyst 4500E 12-port 10GbE SFP+ Fiber Module	WS-X4712-SFP+E	
	Cisco Catalyst 4500E 48-Port 802.3at PoE+ 10/100/1000 (RJ-45)	WS-X4748-RJ45V+E	
	Cisco Catalyst 4500E Series 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.5.3E(15.2.1E3) IP Base license
	Cisco Catalyst 4500E Supervisor Engine 7L-E, 520Gbps	WS-X45-SUP7L-E	
	Cisco Catalyst 4500E 48 Ethernet 10/100/1000 (RJ45) PoE+,UPoE ports	WS-X4748-UPOE+E	
	Cisco Catalyst 4500E 48 Ethernet 10/100/1000 (RJ45) PoE+ ports	WS-X4648-RJ45V+E	
Stackable Access Layer Switch	Cisco Catalyst 3850 Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3850-48F	3.3.3SE(15.0.1EZ3) IP Base license
	Cisco Catalyst 3850 Series Stackable 24 Ethernet 10/100/1000 PoE+ Ports	WS-C3850-24P	
	Cisco Catalyst 3850 Series 2 x 10GE Network Module	C3850-NM-2-10G	
	Cisco Catalyst 3850 Series 4 x 1GE Network Module	C3850-NM-4-1G	
	Cisco Catalyst 3650 Series 24 Ethernet 10/100/1000 PoE+ and 2x10GE or 4x1GE Uplink	WS-C3650-24PD	3.3.3SE(15.0.1EZ3) IP Base license
	Cisco Catalyst 3650 Series 24 Ethernet 10/100/1000 PoE+ and 4x1GE Uplink	WS-C3650-24PS	
	Cisco Catalyst 3650 Series Stack Module	C3650-STACK	
	Cisco Catalyst 3750-X Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-48PF-S	15.2(1)E3 IP Base license
	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-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	
	Cisco Catalyst 2960-X Series 24 10/100/1000 Ethernet and 2 SFP+ Uplink	WS-C2960X-24PD	15.0(2)EX5 LAN Base license
	Cisco Catalyst 2960-X FlexStack-Plus Hot-Swappable Stacking Module	C2960X-STACK	
Standalone Access Layer Switch	Cisco Catalyst 3650 Series 24 Ethernet 10/100/1000 PoE+ and 4x1GE Uplink	WS-C3650-24PS	3.3.3SE(15.01EZ3) IP Base license

### LAN Distribution Layer

Functional Area	Product Description	Part Numbers	Software
Modular Distribution Layer Virtual Switch Pair	Cisco Catalyst 6800 Series 6807-XL 7-Slot Modular Chassis	C6807-XL	15.1(2)SY3 IP Services license
	Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4	VS-S2T-10G	
	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	
	Cisco Catalyst 6500 CEF720 48 port 10/100/1000mb Ethernet	WS-X6748-GE-TX	
	Cisco Catalyst 6500 Distributed Forwarding Card 4	WS-F6K-DFC4-A	
	Cisco Catalyst 6500 Series 6506-E 6-Slot Chassis	WS-C6506-E	
	Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4	VS-S2T-10G	
	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	
	Cisco Catalyst 6500 48-port GigE Mod (SFP)	WS-X6748-SFP	
	Cisco Catalyst 6500 Distributed Forwarding Card 4	WS-F6K-DFC4-A	
	Cisco Catalyst 6500 24-port GigE Mod (SFP)	WS-X6724-SFP	
	Cisco Catalyst 6500 Distributed Forwarding Card 4	WS-F6K-DFC4-A	
Extensible Fixed Distribution Layer	Cisco Catalyst 6800 Series 6880-X Extensible Fixed Aggregation Switch (Standard Tables)	C6880-X-LE	15.1(2)SY3 IP Services license
Virtual Switch Pair	Cisco Catalyst 6800 Series 6880-X Multi Rate Port Card (Standard Tables)	C6880-X-LE-16P10G	
Modular Distribution	Cisco Catalyst 4500E Series 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.5.3E(15.2.1E3) Enterprise Services license
Layer Virtual Switch	Cisco Catalyst 4500E Supervisor Engine 7-E, 848Gbps	WS-X45-SUP7-E	
	Cisco Catalyst 4500E 12-port 10GbE SFP+ Fiber Module	WS-X4712-SFP+E	
	Cisco Catalyst 4500E 48-Port 802.3at PoE+ 10/100/1000 (RJ-45)	WS-X4748-RJ45V+E	
Fixed Distribution Layer Virtual Switch Pair	Cisco Catalyst 4500-X Series 32 Port 10GbE IP Base Front-to-Back Cooling	WS-C4500X-32SFP+	3.5.3E(15.2.1E3) Enterprise Services license
Stackable	Cisco Catalyst 3850 Series Stackable Switch with 12 SFP Ethernet	WS-C3850-12S	3.3.3SE(15.0.1EZ3) IP Services license
Distribution Layer Switch	Cisco Catalyst 3850 Series 4 x 1GE Network Module	C3850-NM-4-1G	
	Cisco Catalyst 3850 Series 2 x 10GE Network Module	C3850-NM-2-10G	
	Cisco Catalyst 3750-X Series Stackable 12 GbE SFP ports	WS-C3750X-12S-E	15.2(1)E3 IP Services 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	

#### LAN Core Layer

Functional Area	Product Description	Part Numbers	Software
Modular Core Layer Virtual Switch Pair	Cisco Catalyst 6800 Series 6807-XL 7-Slot Modular Chassis	C6807-XL	15.1(2)SY3 IP Services license
	Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4	VS-S2T-10G	
	Cisco Catalyst 6500 4-port 40GbE/16-port 10GbE Fiber Module w/DFC4	WS-X6904-40G-2T	
	Cisco Catalyst 6500 16-port 10GbE Fiber Module w/DFC4	WS-X6816-10G-2T	
	Cisco Catalyst 6500 48-port GbE SFP Fiber Module w/DFC4	WS-X6848-SFP-2T	
	Cisco Catalyst 6500 Series 6506-E 6-Slot Chassis	WS-C6506-E	
	Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4	VS-S2T-10G	
	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	
	Cisco Catalyst 6500 24-port GigE Mod (SFP)	WS-X6724-SFP	
	Cisco Catalyst 6500 Distributed Forwarding Card 4	WS-F6K-DFC4-A	

#### LAN Distribution – Services Block

Functional Area	Product Description	Part Numbers	Software
Modular Distribution Layer Virtual Switch Pair	Cisco Catalyst 6800 Series 6807-XL 7-Slot Modular Chassis	C6807-XL	15.1(2)SY3 IP Services license
	Cisco Catalyst 6500 VSS Supervisor 2T with 2 ports 10GbE and PFC4	VS-S2T-10G	
	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	
	Cisco Catalyst 6500 CEF720 48 port 10/100/1000mb Ethernet	WS-X6748-GE-TX	
	Cisco Catalyst 6500 Distributed Forwarding Card 4	WS-F6K-DFC4-A	
Wireless LAN Controller	Cisco WiSM2 Series Wireless Controller for up to 1000 Cisco access points	WS-SVC-WISM2-K-K9	7.6.120.0
	Cisco WiSM2 Series Wireless Controller for up to 500 Cisco access points	WS-SVC-WISM2-5-K9	
	Cisco WiSM2 Series Wireless Controller for up to 300 Cisco access points	WS-SVC-WISM2-3-K9	
	Cisco WiSM2 Series Wireless Controller for up to 100 Cisco access points	WS-SVC-WISM2-1-K9	
	Cisco WiSM2 Series Wireless Controller for High Availability	WS-SVC-WISM2-HA-K9	

#### **Data Center Virtualization**

Functional Area	Product Description	Part Numbers	Software
VMWare	ESXi	ESXi	5.1
	VMware vSphere	ESXi	

# Appendix B: Changes

This appendix summarizes the changes to this guide since its last edition.

- We added the 7.6.120.0 release of firmware to all Cisco AireOS WLCs.
- We upgraded the 5760 IOS-XE to release 3.3.3SE.
- We upgraded the redundant Cisco ISE servers to 1.2 Service Patch 8.
- We upgraded the VSS Services distribution block from a pair of 6509s to a 6807 in a Virtual Switching System Quad-Supervisor Stateful Switchover configuration using VS-SUP2T-10G.
- We validated the HA SSO WiSM2 in the upgraded 6807 VSS Quad-Supervisor Stateful Switchover (VS4O) pair using SUP2T.
- · We incorporated and validated numerous wireless best practices, including:
  - Enabled Fast Secure Roaming by enabling CCKM support on AireOS Controllers
  - Incorporated design recommendations for improved roaming and WLC performance based on size and design of mobility domain
  - Incorporated design recommendations for improving WLC RRM performance by providing guidance on RF Domain design
  - Enabled Sleeping Client Support
  - Eliminated Dynamic Trunking Protocol (DTP) overhead for WLCs and APs using trunk ports through switchport nonegotiate
  - Disabled SNMP v3
  - Altered RSSI value for rogue detection from -128dBm to -70dBm to reduce size of rogue detection area - helping to reduce false positive rogue detection
  - Enabled Fast SSID change support
  - Required DHCP address assignment for added security to Data and Guest WLANs
  - Enabled Allow AAA Override to allow ISE/RADIUS to override local WLC policy if necessary (BYOD, QoS, VLAN, Bonjour, etc.)
- We enabled Dual ISP High Availability using object tracking for guest access outbound PAT.
- We improved overall readability of the Cisco ASA firewall configuration sections throughout the guide.

#### Feedback

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

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

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

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

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

© 2014 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 09/14