Campus Wireless LAN

Technology Design Guide

August 2014 Series

CISCO VALIDATED DESIGN

Table of Contents

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 bandwidth-intensive 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 Design Guide

Campus Wired LAN Technology Design Guide

Device Management 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

Technology Use Cases

With the adoption of smartphones and tablets, the need to stay connected while mobile has evolved from a nice-to-have to a must-have. The use of wireless technologies 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:

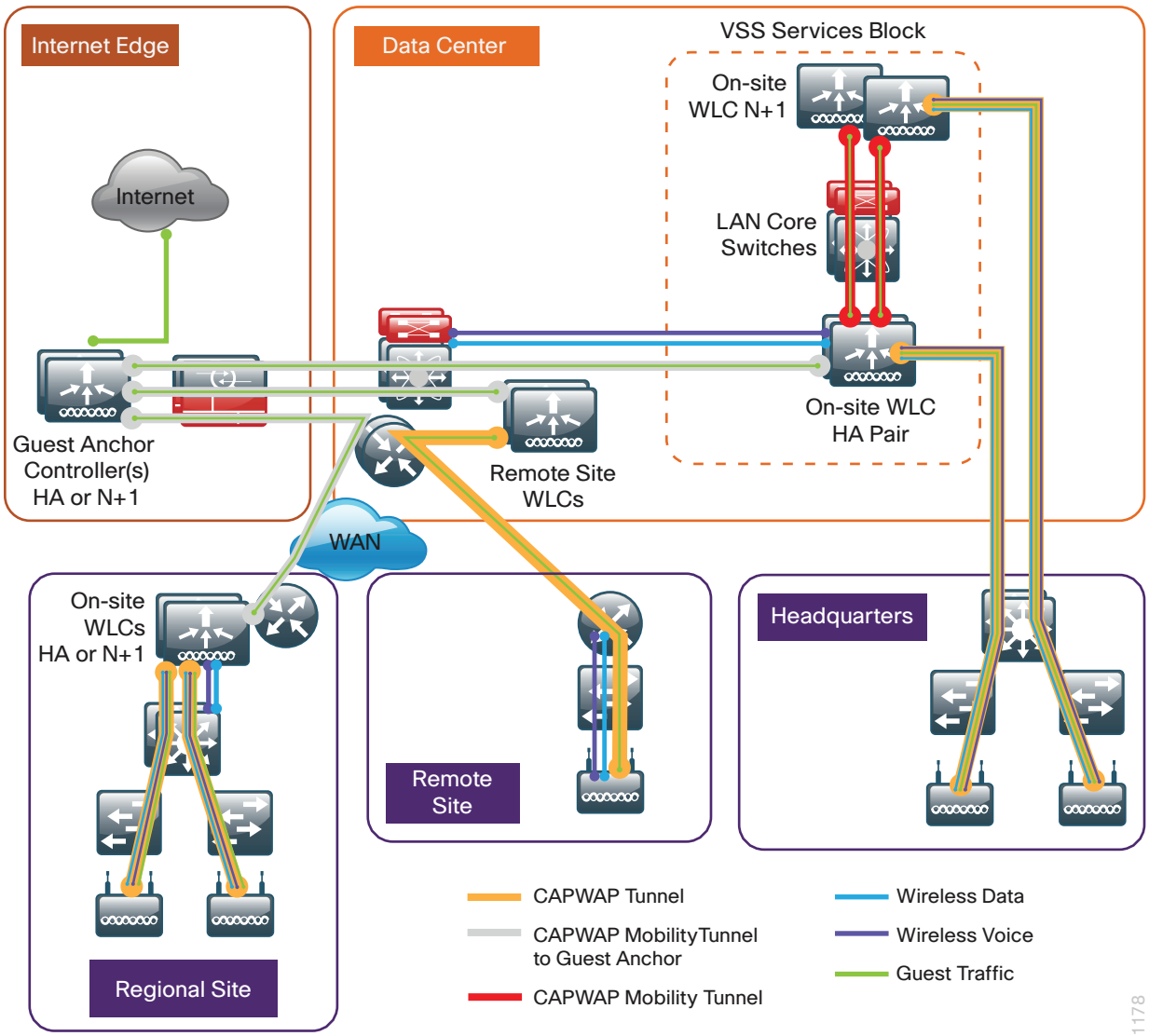
- **Productivity gains through secure, location-independent network access**—Measurable productivity improvements and communication.
- **Additional network flexibility**—Hard-to-wire locations can be reached without costly construction.
- **Cost effective deployment**—Adoption of virtualized technologies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

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



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 sub-second 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, self-optimizing wireless network. By intelligently avoiding interference, they provide the high-performance 802.11n connectivity for mission-critical mobility and performance protection for reliable application delivery.
- Cisco Aironet 3600 Series Access Points with Cisco CleanAir technology deliver more coverage for tablets, smart phones, and 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.

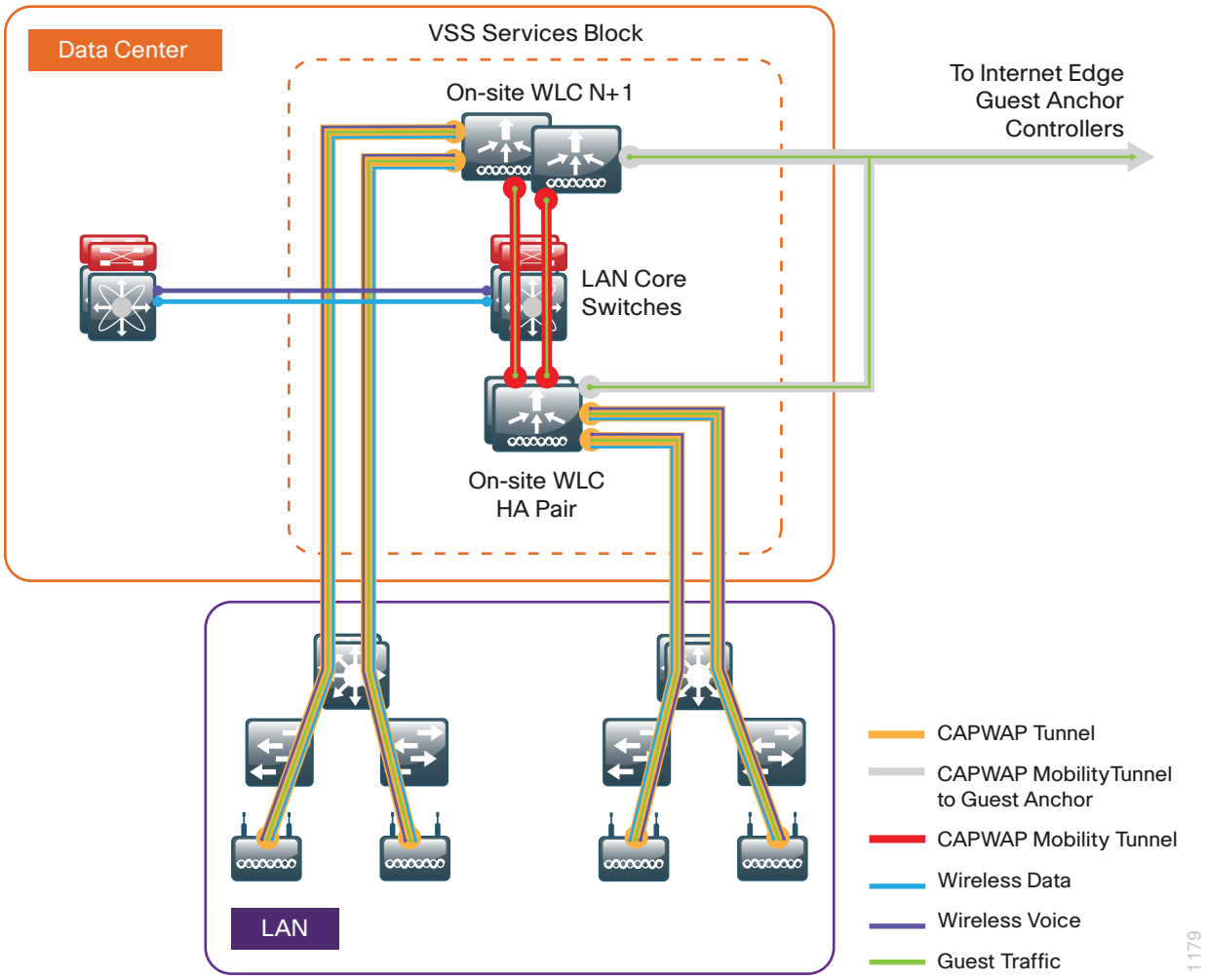
Wireless Design Models

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.

Figure 2 - Local-mode design model



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

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

- **Seamless mobility**—In a campus environment, it is crucial that users remain connected to their session even while walking between various floors or adjacent buildings with changing subnets. The local 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.

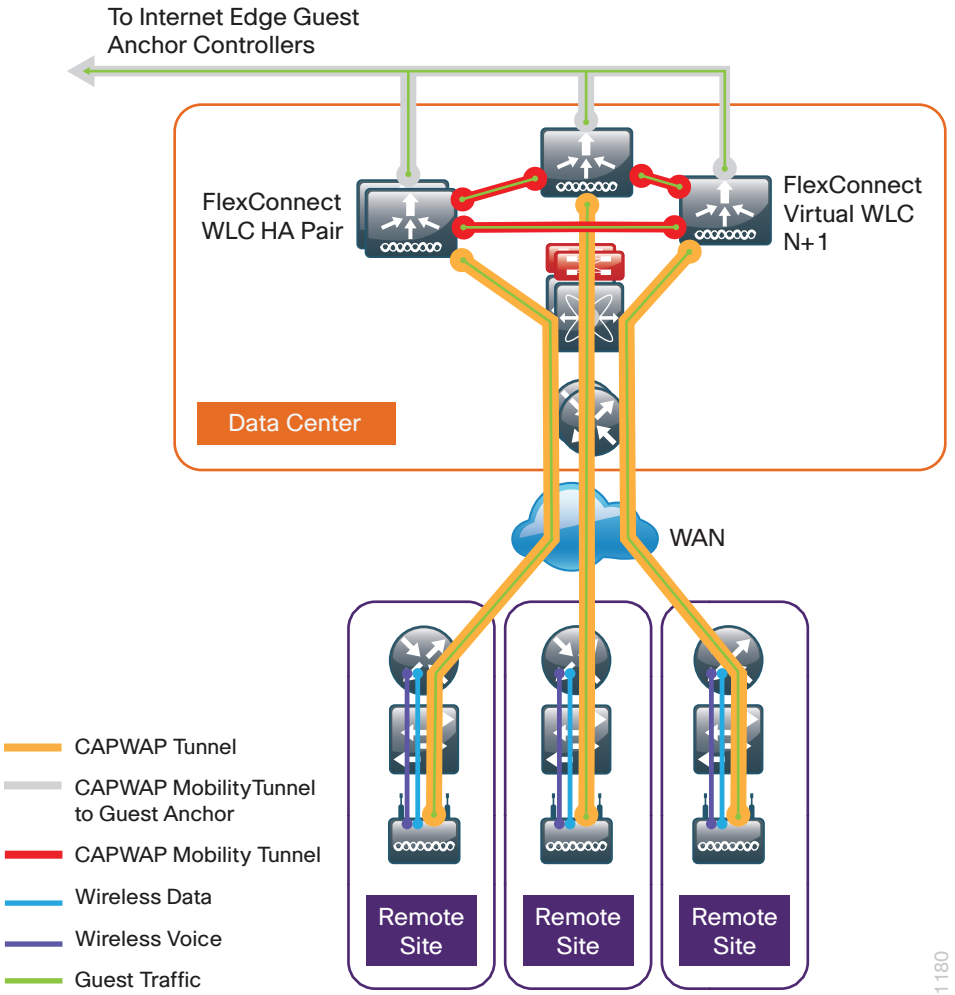
If **all** of the following are true at a site, deploy Cisco FlexConnect at the site:

- 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.

Figure 3 - Cisco FlexConnect design model



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

Table 1 - High availability feature support

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	Yes[1]	Yes	Yes
7500 Flex	Yes	Yes	Yes

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.

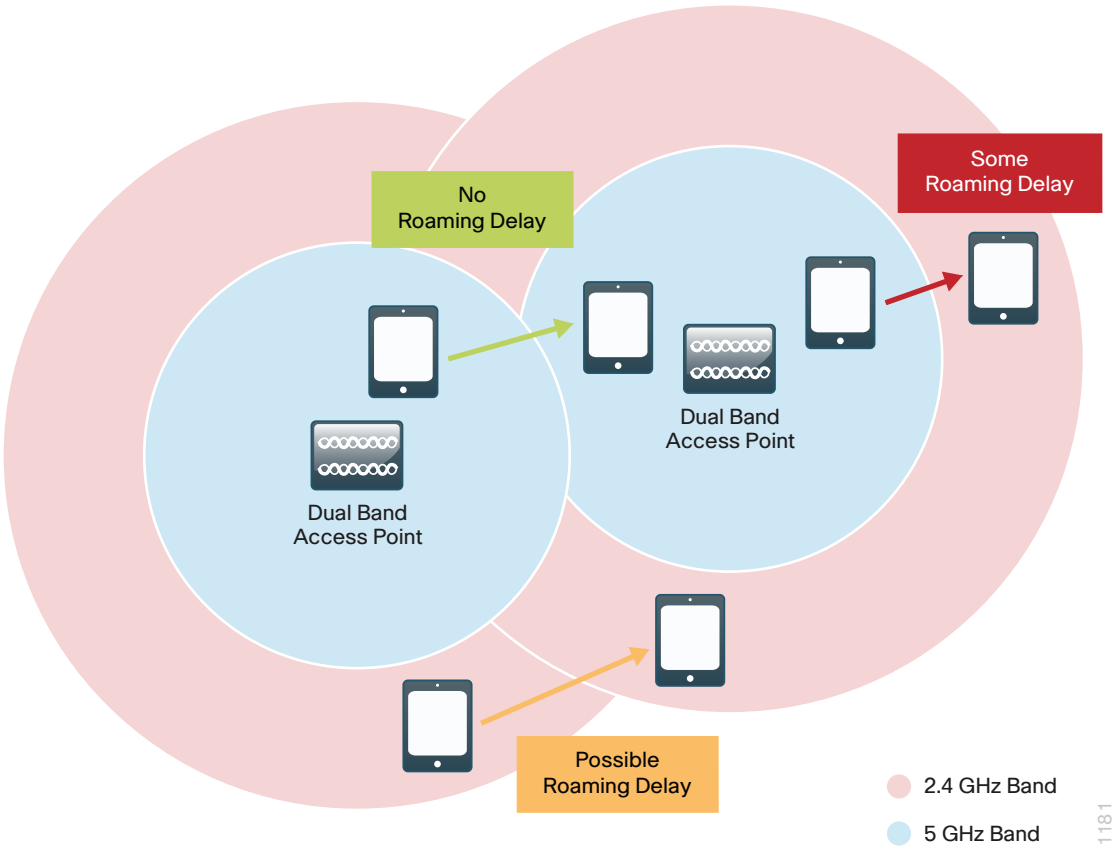
The Band Select algorithm uses a number of default values to determine if a wireless client is in fact dual-band capable. There are also times when a dual-band client will disable a particular radio based on the user deciding to disable it for any number of reasons.

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



Tech Tip

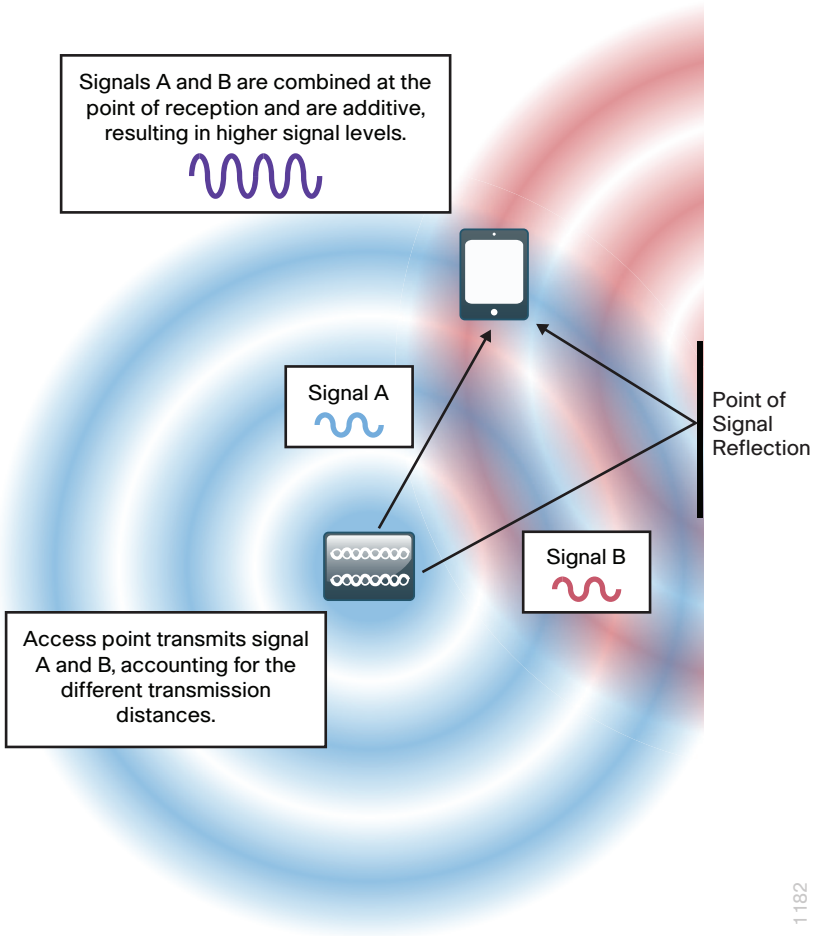
Wireless deployments that mix data, voice, and real-time services on a single SSID should not use Band Select on that WLAN. This includes voice applications such as Jabber, Facetime and Skype among other real-time applications.

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.

Table 3 - 802.11ac Bandwidth performance

Year	Technology	Theoretical PHY performance	Expected user performance[1]
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

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.

Table 4 - Worldwide 5GHz channel availability

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

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:

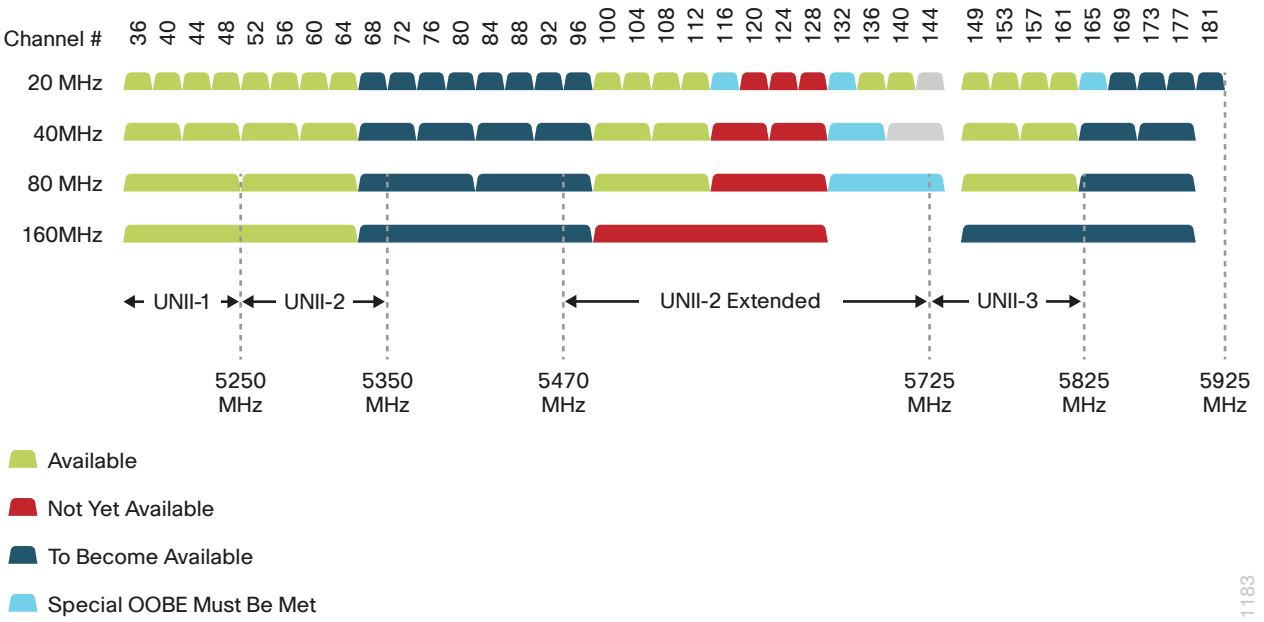
- Density of AP deployment
- Channel isolation
- Mixed cell environments
- Adjacent mixed cell and proper 802.11ac primary channel selection
- Consumer wireless device support of DFS channel set
- Increased transmit power in UNII-2 and UNII-3 bands
- Increased battery usage in UNII-2 and UNII-3 bands

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.

Figure 6 - Channel usage in the U.S.



Tech Tip

Note that some older Apple devices do not support channel 165. It is therefore recommended to restrain from using this channel as a primary or sub-channel if older Apple devices are being used. By default, channel 165 is not included in the DFS channel list and must be manually added if it is to be used.

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.

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.

40 MHz 802.11a/n Channel Naming Examples
(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

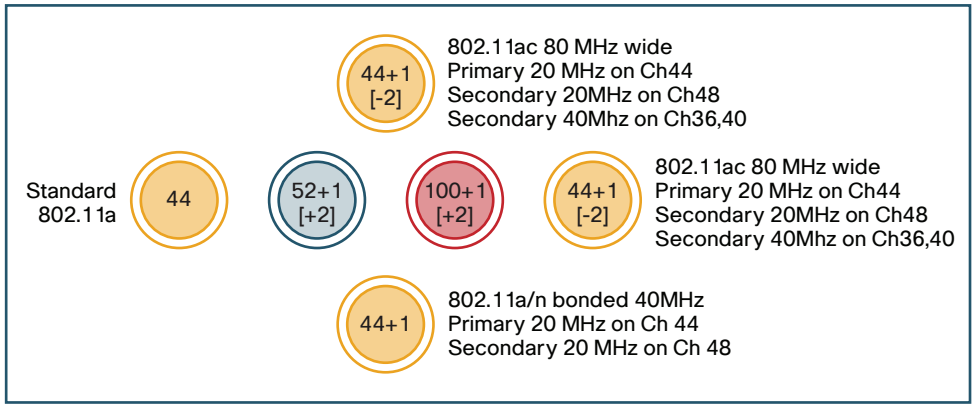
80 MHz 802.11ac Channel Naming Examples
(Primary channel)+1 [+2]
36+1[+2] = Primary 20 on 36, Secondary 20 on 40, Secondary 40 on 44 and 48

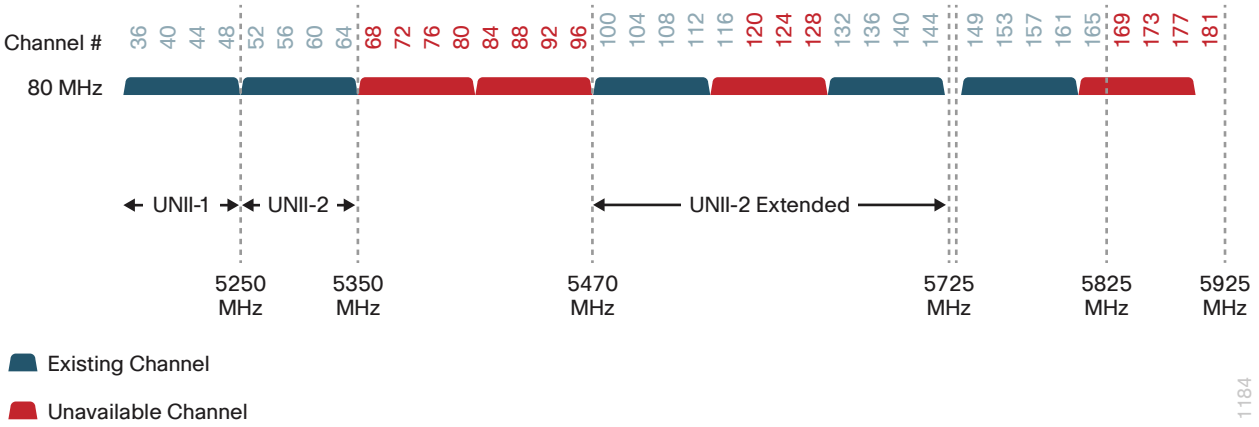
(Primary channel)-1 [+2]
40-1[+2] = Primary 20 on 40, Secondary 20 on 36, Secondary 40 on 44 and 48

(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

Figure 7 - Channel planning in mixed cell environments

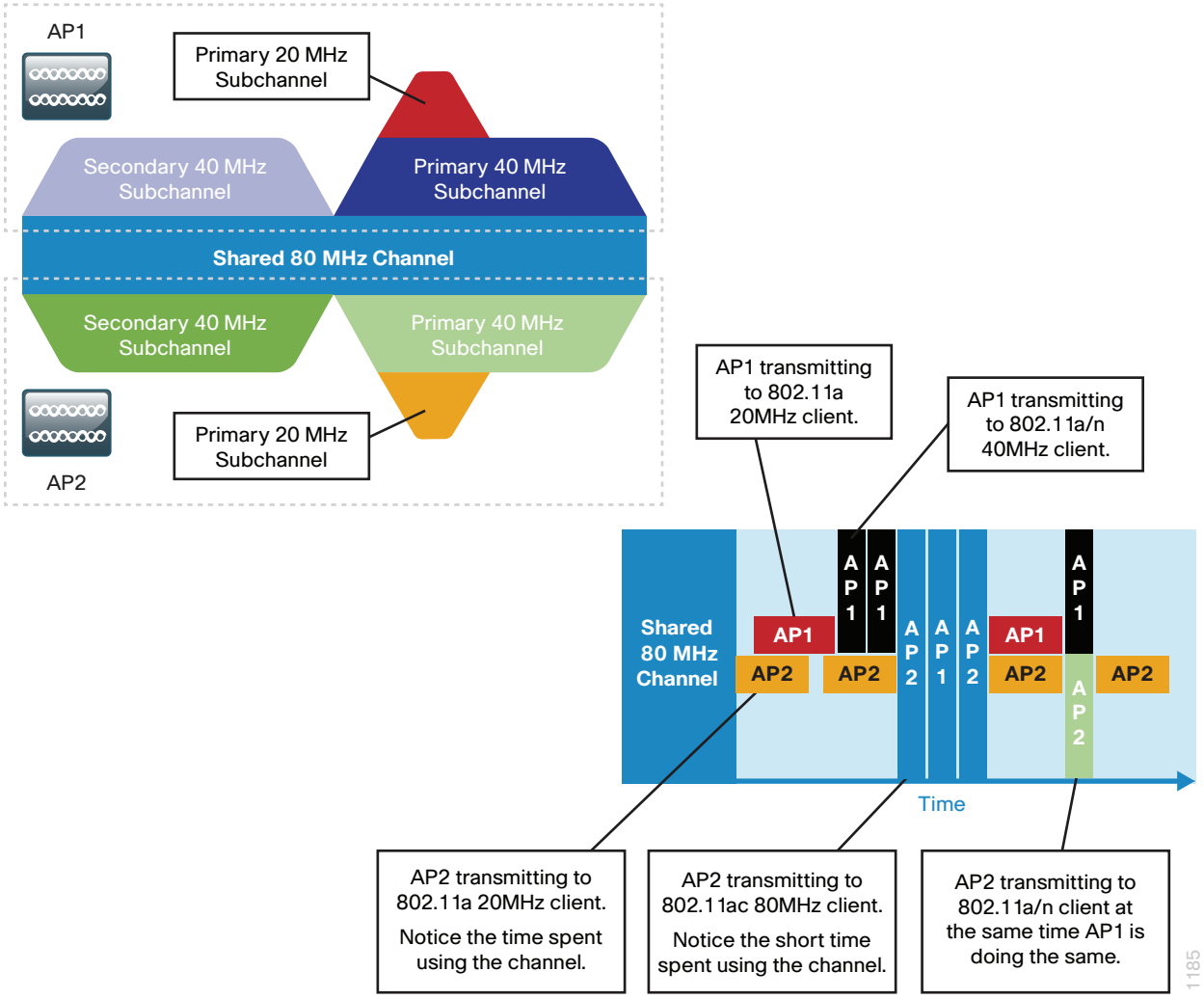




The utilization of 802.11ac channel allocation depends greatly on the wireless clients being served. For example, a deployment where most of the wireless devices are legacy 20 MHz based 802.11a or 40 MHz 802.11n. In the channel strategy describe previously, the plan is to lay out 80 MHz channels with 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.

Table 5 - 802.11ac Clear Carrier Assessment threshold values

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.

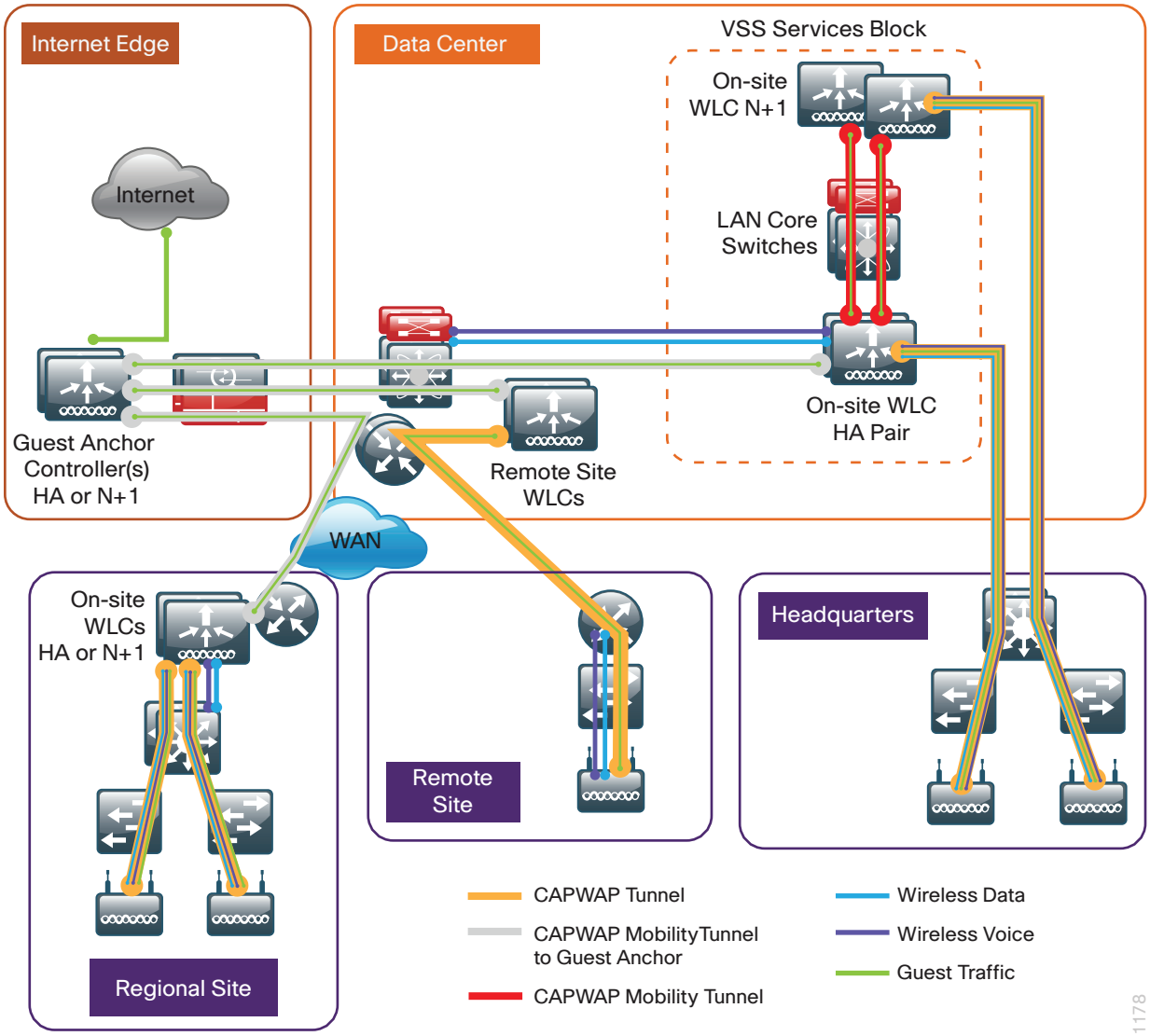
With Radio Resource Management (RRM), Transmit Power Control (TPC), and Dynamic Channel Assignment (DCA), the process of channel selection can be both automated and optimized. In the implementation section of this guide, enabling 80MHz channels using DCA for all 802.11ac access points in the network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

Figure 9 - Wireless architecture overview



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.

Tech Tip

If you are using a Cisco IOS-XE based 5760 WLC with other Cisco AireOS controllers either as a Guest Anchor in the Internet edge or as a remote anchor within your campus, you must enable the New Mobility (Converged Access) feature. You can find this global configuration **Controller > Mobility Management > Mobility Configuration**.

If you don't enable New Mobility (Converged Access), Mobility Peering cannot be established between the WLCs. This is because Cisco AireOS controllers use Ethernet over IP (EoIP) while Cisco IOS-XE controllers use CAPWAP (UDP 16666/16667). Once New Mobility (Converged Access) is enabled on the AireOS WLC, the time to detect a failure within an AireOS HA SSO configured WLC pair is increased significantly. Configuration synchronization, license inheritance, and software upgrades to the 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 conventions for commands that you enter at the command-line interface (CLI).

Commands to enter at a CLI prompt:

```
configure terminal
```

Commands that specify a value for a variable:

```
ntp server 10.10.48.17
```

Commands with variables that you must define:

```
class-map [highest class name]
```

Commands at a CLI or script prompt:

```
Router# enable
```

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

```
police rate 10000 pps burst 10000
packets conform-action
```

Noteworthy parts of system output (or of device configuration files) are highlighted:

```
interface Vlan64
  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.

Table 6 - Universal design parameters

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	

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.

Table 7 - Cisco security products used

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

PROCESS

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.

Tech Tip

Certain browsers may render the display for Cisco Secure ACS differently. In some cases, a browser may omit fields that are required for proper configuration. It is recommended that you refer to the following Cisco Secure ACS 5.5 release notes in order to obtain a list of supported browsers:
http://www.cisco.com/c/en/us/td/docs/net_mgmt/cisco_secure_access_control_system/5-5/release/notes/acs_55_rn.html

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.

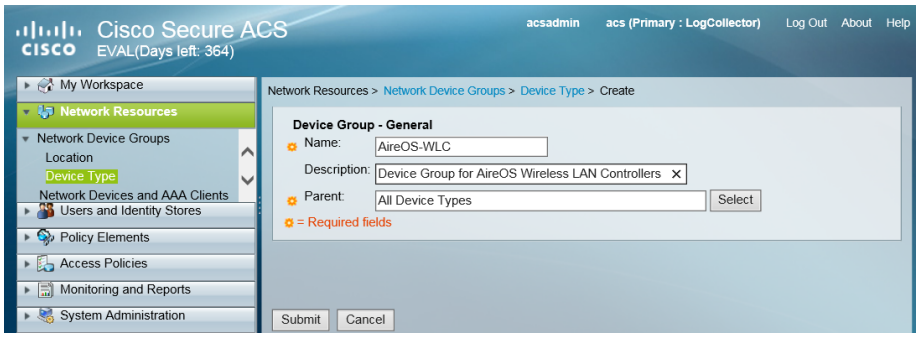
Procedure 1 Create the wireless device type group

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**.

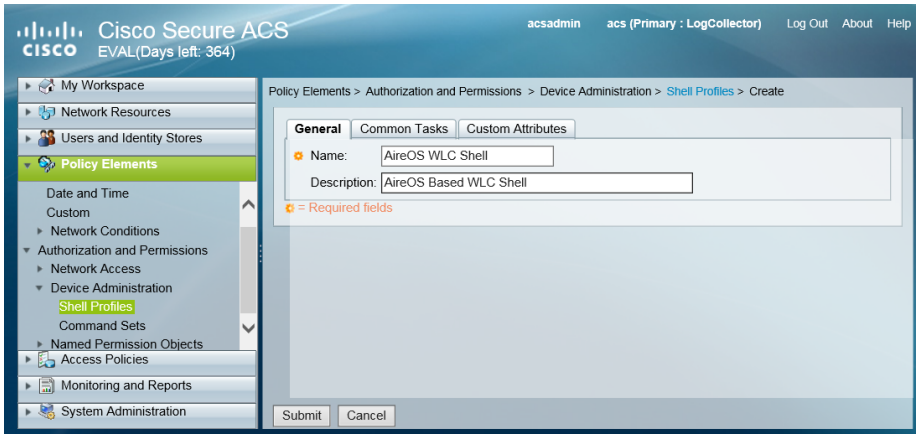


Procedure 2 Create the TACACS+ shell profile

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**.

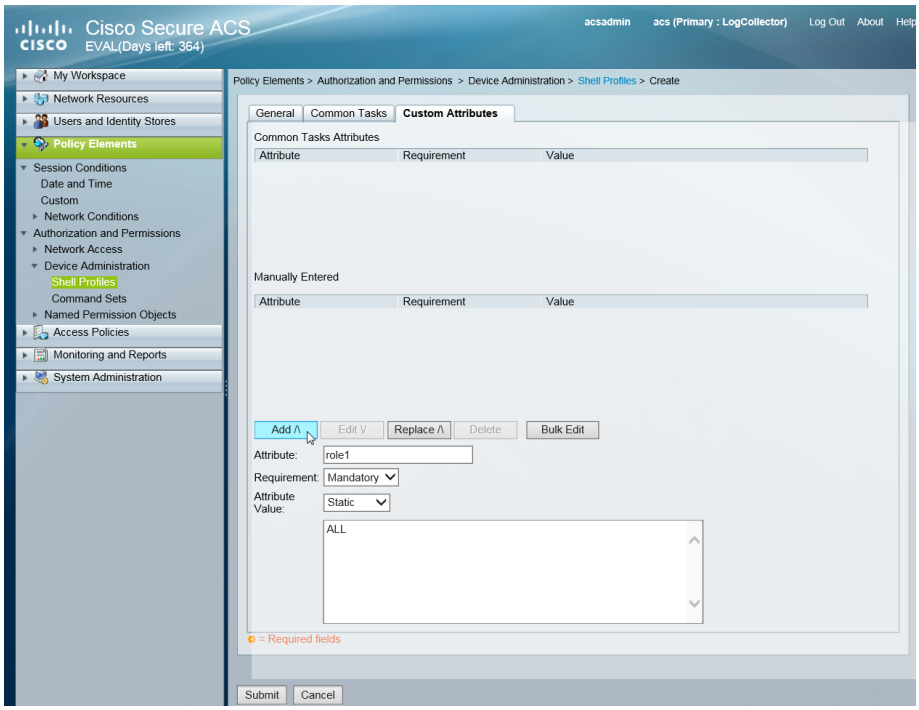
Step 2: On the General tab, In the **Name** box, enter a name for the wireless shell profile (Example: **AireOS WLC Shell**), and then in the **Description** box, enter a description.



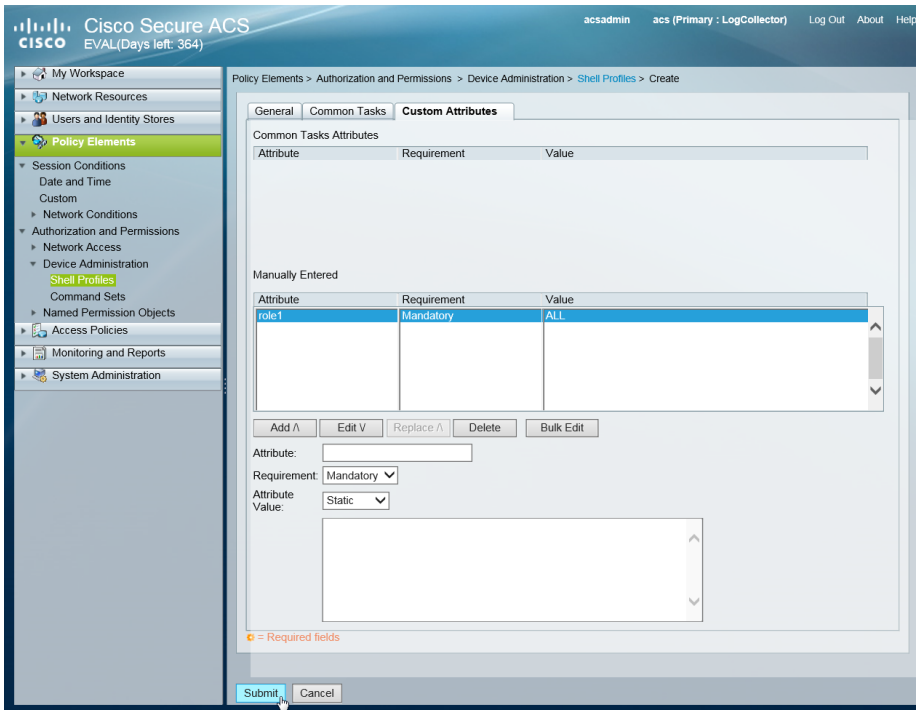
Step 3: On the Custom Attributes tab, in the **Attribute** box, enter **role1**.

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**.



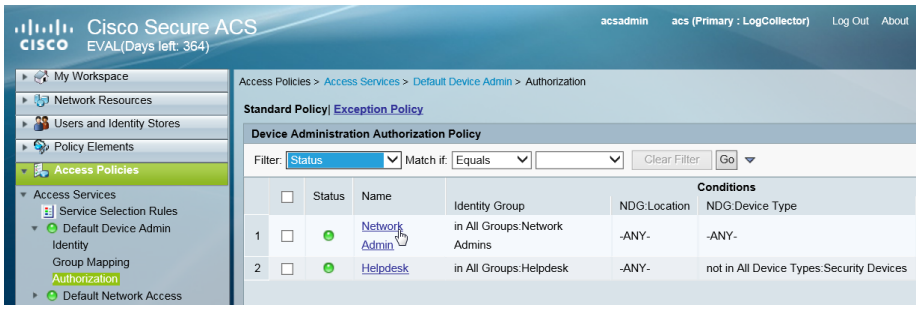
Step 6: Click **Submit**.



Procedure 3 Modify the device admin access policy

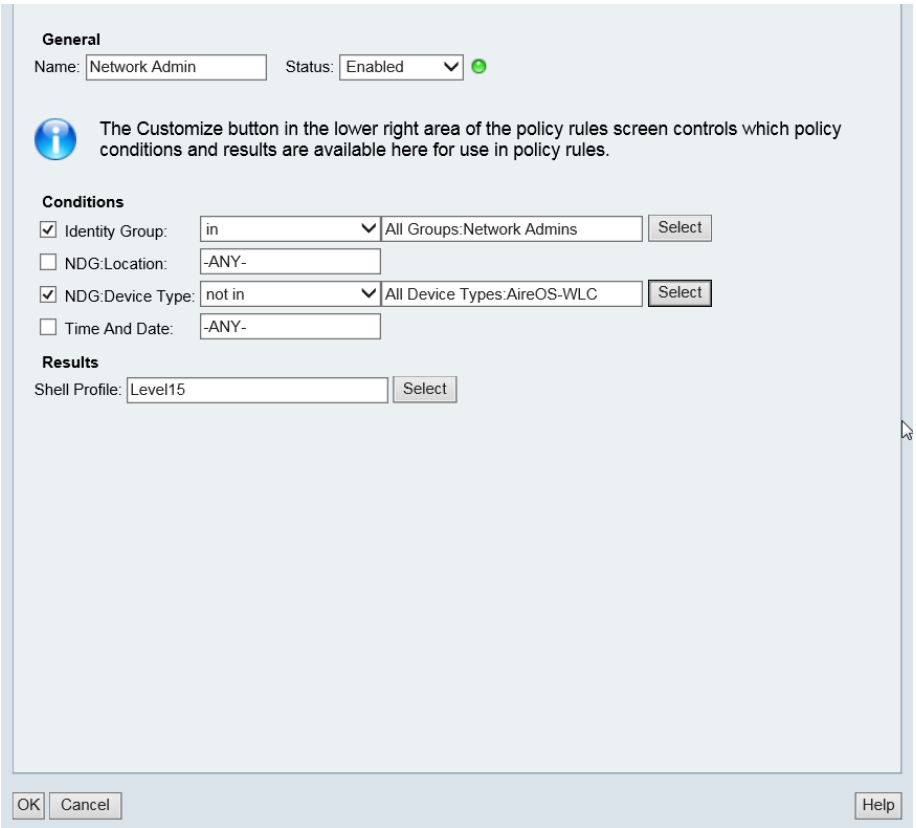
You must exclude the Cisco AireOS WLCs from the existing default authorization rule.

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



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**.



Next, create a Cisco AireOS WLC authorization rule.

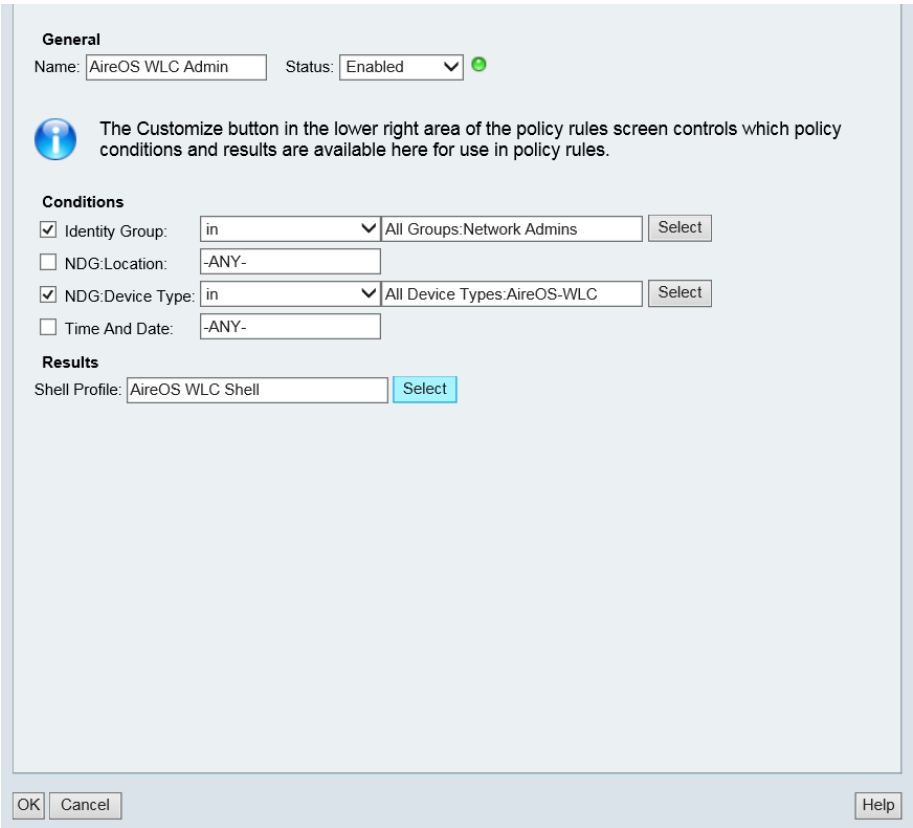
Step 4: In **Access Policies > Default Device Admin >Authorization**, click **Create**.

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**.

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**.

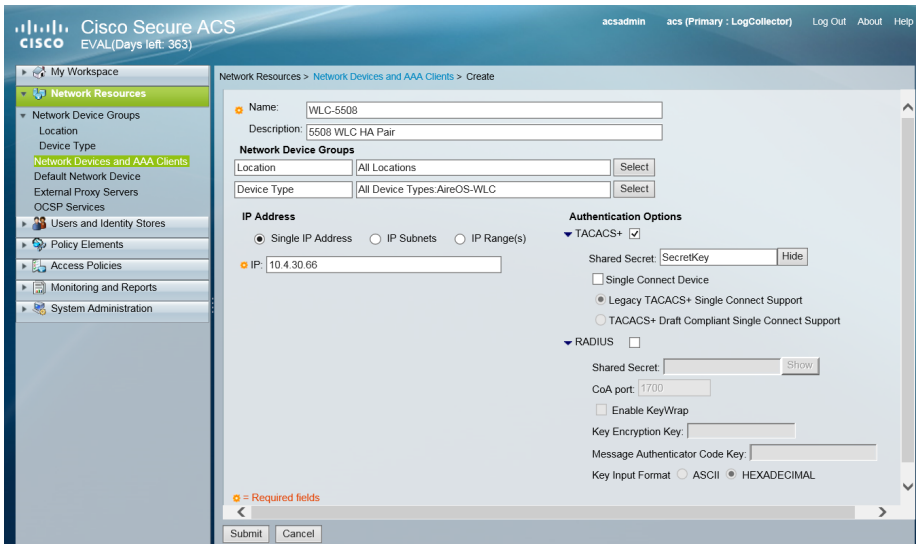
Step 2: In the **Name** box, enter the device host name (Example: WLC-5508), and then, in the **Description** box, enter a description (Example: 5508 WLC HA Pair).

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

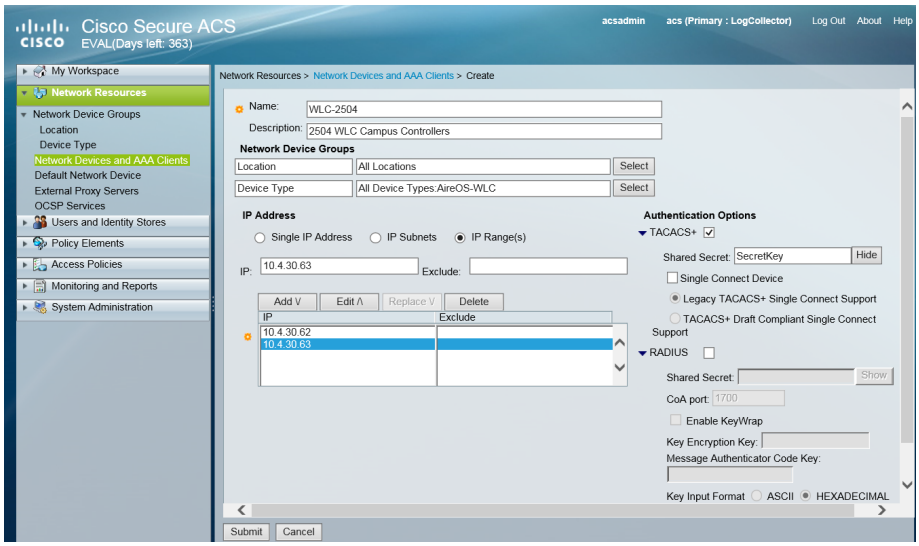
Step 4: In the **IP** box, enter the WLCs management interface IP address. (Example: 10.4.175.66)

Step 5: Select **TACACS+**.

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



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.



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-lvl = 15 when an administrator logs on. The same concept applies to AireOS devices, but instead of priv-lvl = 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-lvl = 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-lvl = 15.

PROCESS

Deploying Redundant Cisco ISE Servers

1. Perform initial setup of primary Cisco ISE server
2. Perform initial setup of redundant Cisco ISE server
3. Configure certificate trust list
4. Configure Cisco ISE deployment nodes
5. Install the Cisco ISE license
6. Configure network devices in Cisco ISE
7. Configure Cisco ISE to use Active Directory
8. Configure AD groups for Cisco ISE authentication

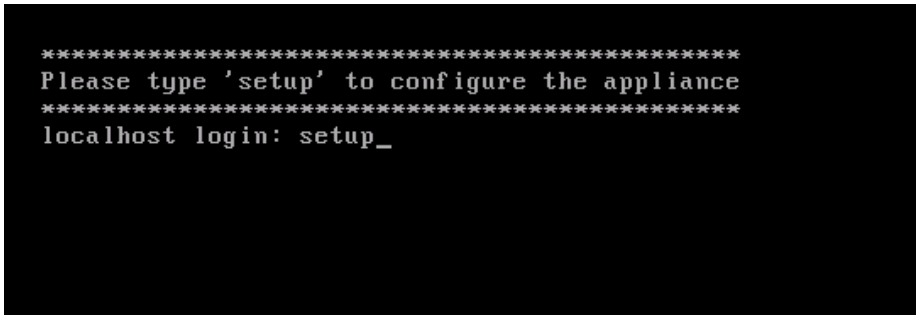
In this design, redundant Cisco ISE servers are used to provide wireless user authentication and replace Cisco Secure ACS for this purpose. Wireless user authentication uses the RADIUS protocol, and the following steps outline the installation process of the redundant ISE servers. The installation of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

Table 8 - Cisco ISE engine IP addresses and hostnames

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

Procedure 1 Perform initial setup of primary Cisco ISE server

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
```

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.

Tech Tip

The Cisco ISE administrator password expires by default every 45 days. You can reset the password from the CLI by using SSH to issue the **application reset-password ise [user account]** command.

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

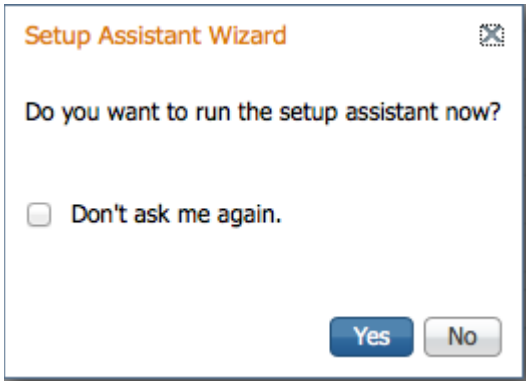
The procedure for setting up a secondary redundant Cisco ISE server is the same as for the primary, with the only difference being the IP address and host name values configured for the engine.

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

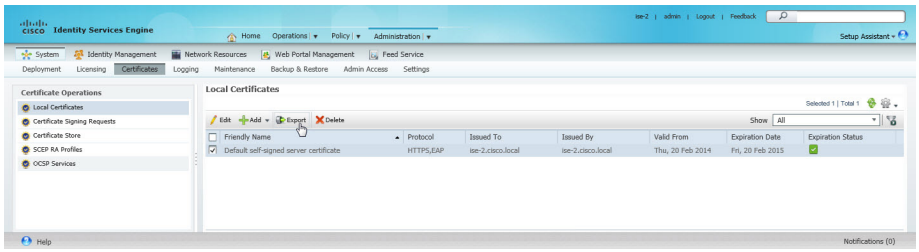
The engines use public key infrastructure (PKI) to secure communications between them. Initially in this deployment, you use local certificates, and you must configure a trust relationship between both of the engines. To do this, you need to import the local certificates from the redundant Cisco ISE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

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.

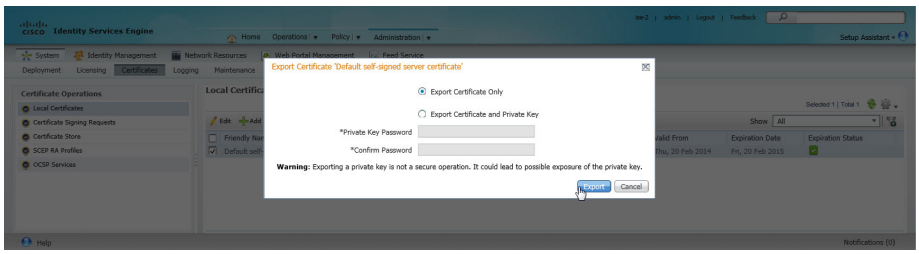


Step 2: In **Administration > System**, select **Certificates**.

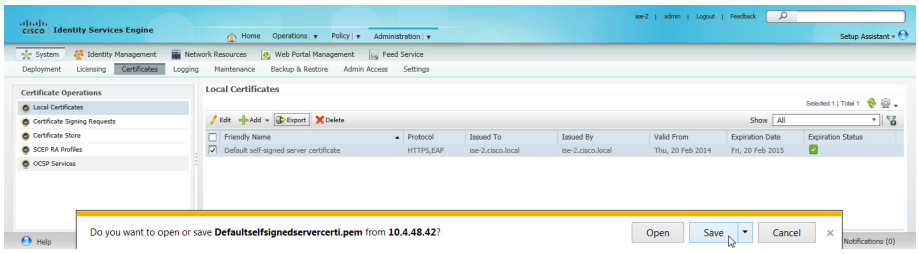
Step 3: In the Local Certificates window, select the local certificate by selecting the box next to the name of the secondary engine, **ise-2.cisco.local,** and then click **Export**.



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



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.

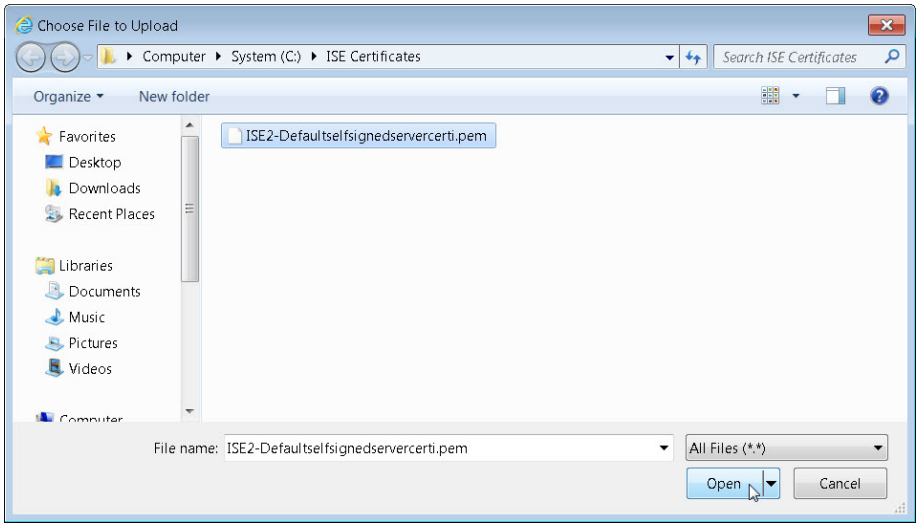


Step 6: In a browser, access the primary engine's GUI at http://**ise-1.cisco.local**.

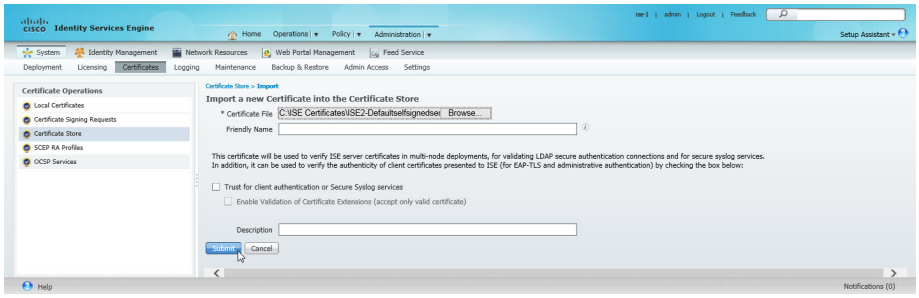
Step 7: In **Administration > System**, select **Certificates**.

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.



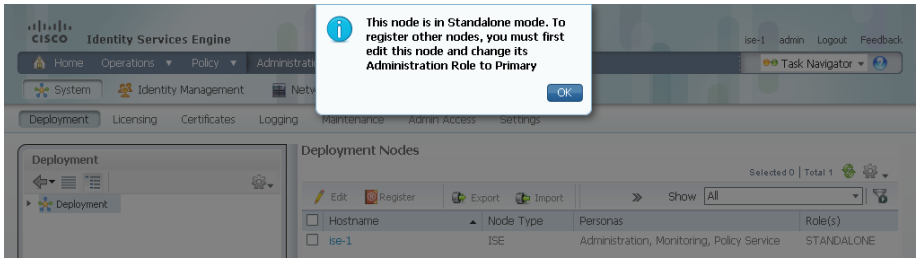
Step 10: You may enter a friendly name for the ISE2 server then click **Submit**.



Procedure 4 Configure Cisco ISE deployment nodes

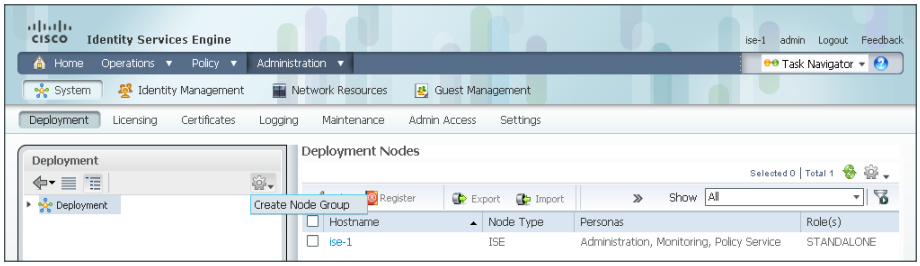
Step 1: You can configure the personas of Cisco ISE—administration, monitoring, and policy service—to run all on a single engine or to be distributed amongst several engines. This installation will run all services on the primary and redundant secondary ISE servers Connect to **http://ise-1.cisco.local**.

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**.

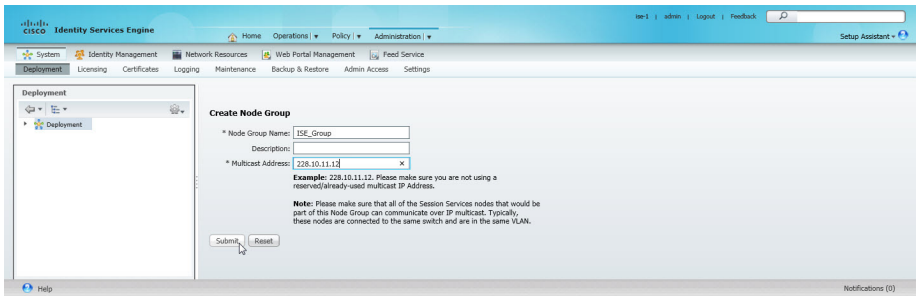


Step 3: In the Deployment pane, click the gear icon, and then select **Create Node Group**.

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.



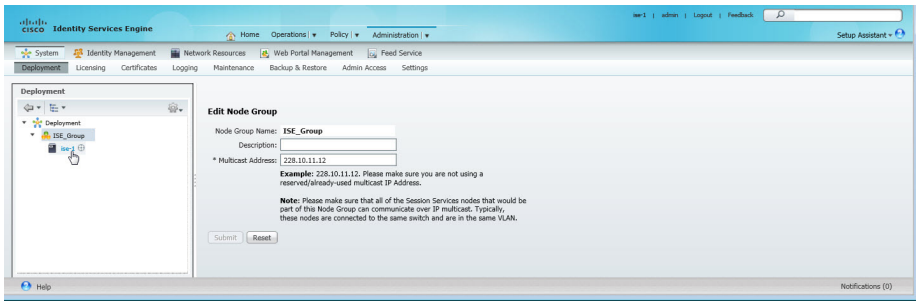
Step 4: Configure the node group with the node group name **ISE_Group** and the default multicast address of **228.10.11.12**, and then click **Submit**.



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

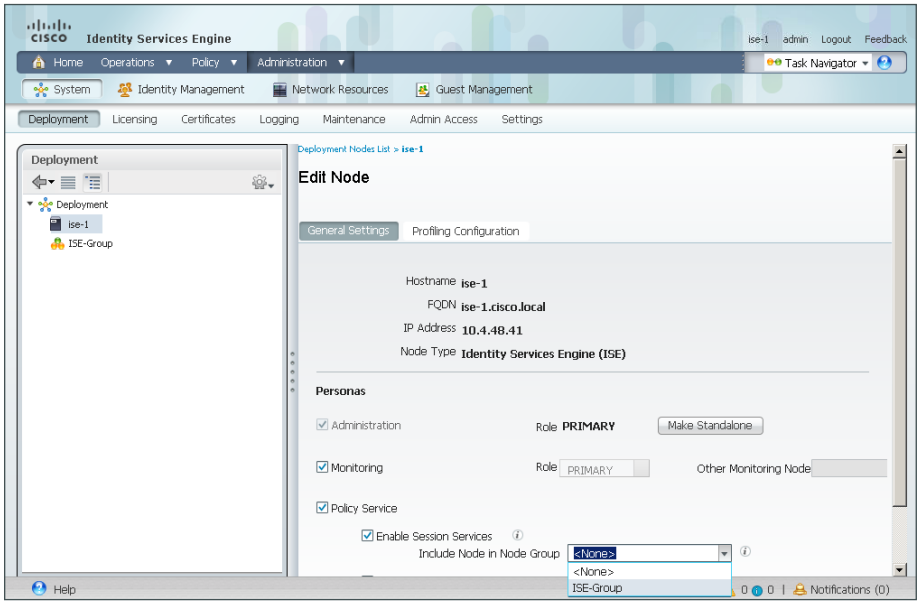
Step 6: In the Deployment pane on the left, expand **Deployment**. A list of the current deployment nodes appears.

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



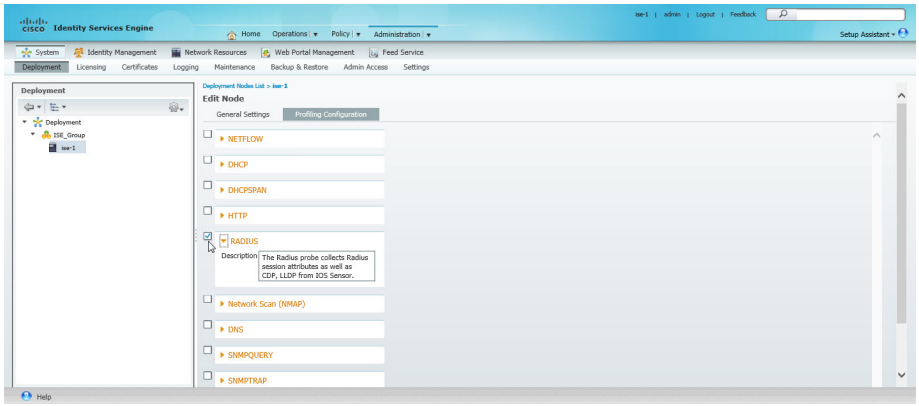
Step 8: On the General Settings tab, in the Personas section, next to the Administration Role, click **Make Primary**.

Step 9: In the **Include Node in Node Group** list, choose **ISE_Group**.

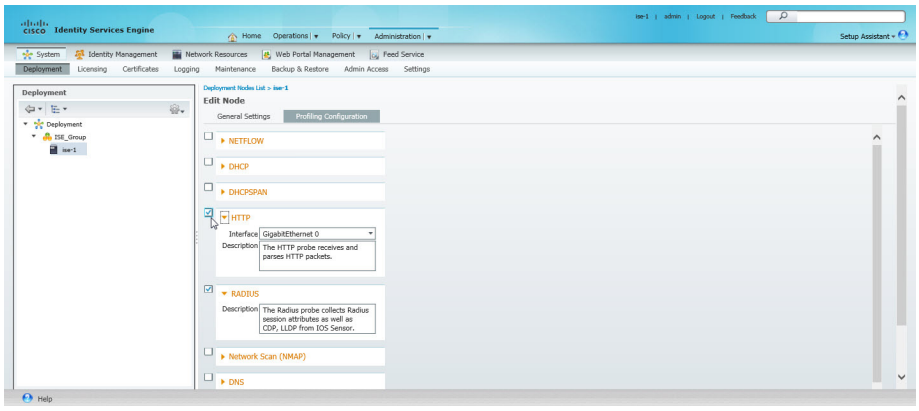


Next, you configure which methods are used to profile network endpoints.

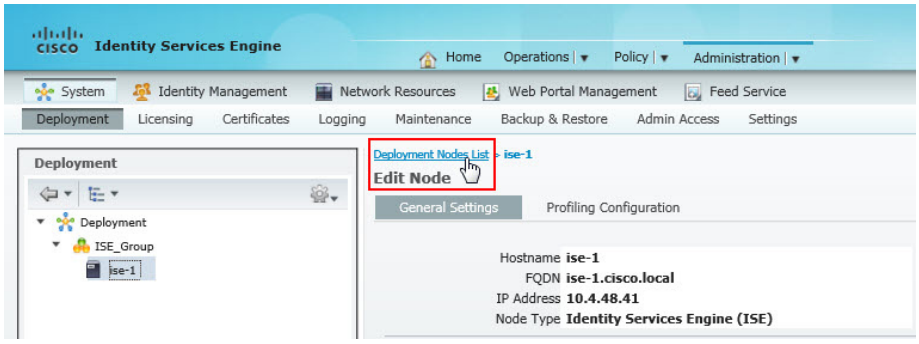
On the Profiling Configuration tab, select **RADIUS** by placing a check mark as shown and then click **Save**.



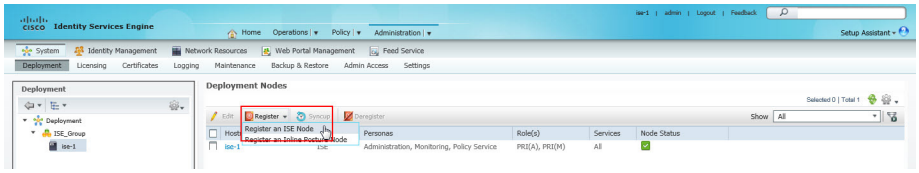
Step 10: Select **HTTP**, use the default parameters, and then click **Save**.



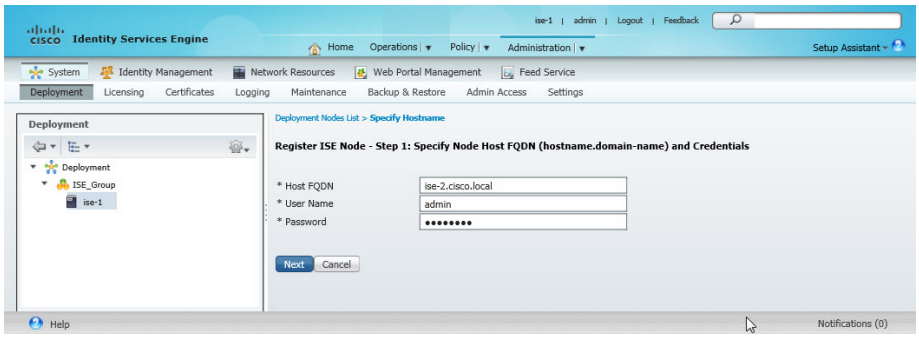
Step 11: At the top of the Edit Node window, click **Deployment Nodes List**. The Deployment Nodes window appears.



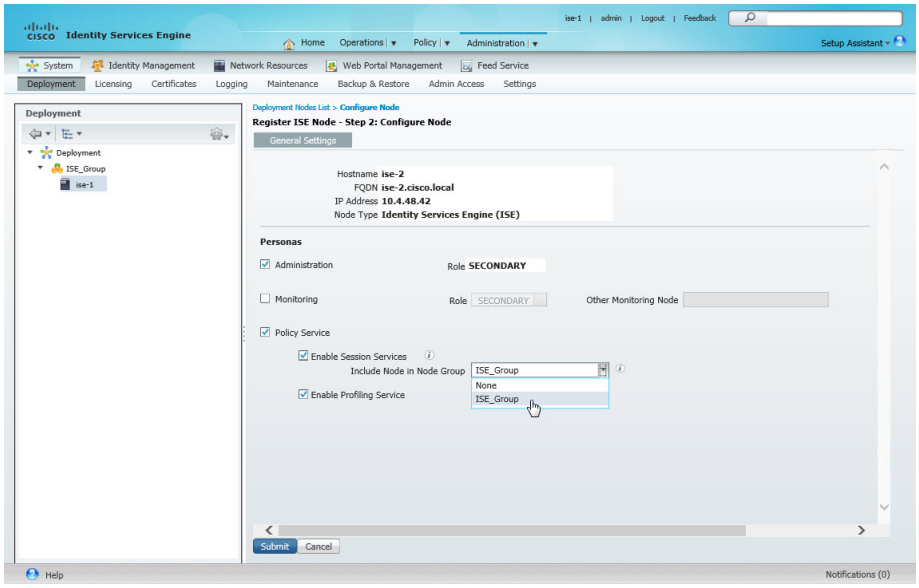
Step 12: Click **Register,** and then choose **Register an ISE Node**.



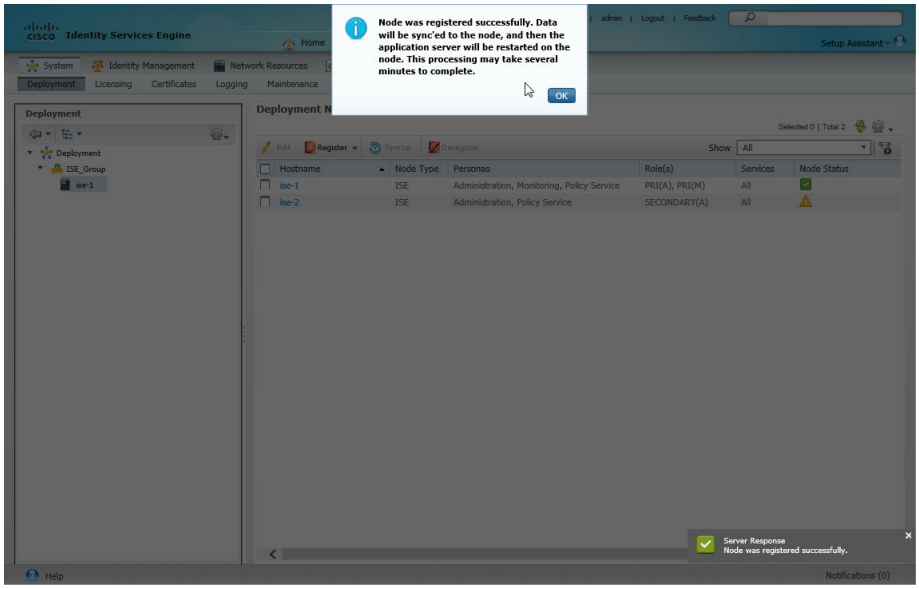
Step 13: Enter the IP address or host name of the redundant Cisco ISE engine from Table 8 (in this example, ise-2.cisco.local) and the credentials for the admin account, and then click **Next**.



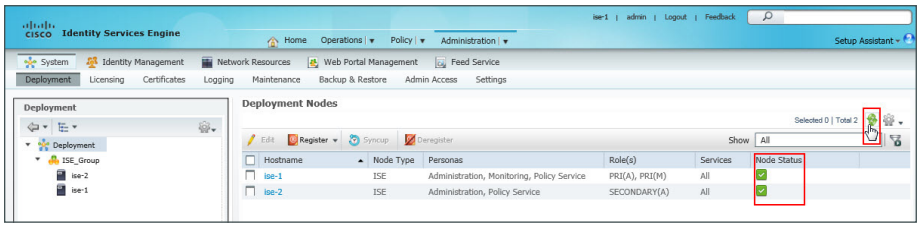
Step 14: Select only **Administration** and **Policy Service**. In the Administration section under **Role** list ensure **Secondary** is displayed. In the Policy Service section, in the **Node Group** list, Choose **ISE_Group**.



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



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.



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.

> **Tech Tip**
>
> Cisco ISE 1.2 supports the following browsers: Mozilla Firefox Versions 5.x, 8.x, 9.x, 14.x, 15.x, 18.x, 19.x, and 20.x; and Microsoft Internet Explorer 8.x, 9.x, and 10.x. Failure to use a supported browser may result in the inability to see various fields or controls.

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**.

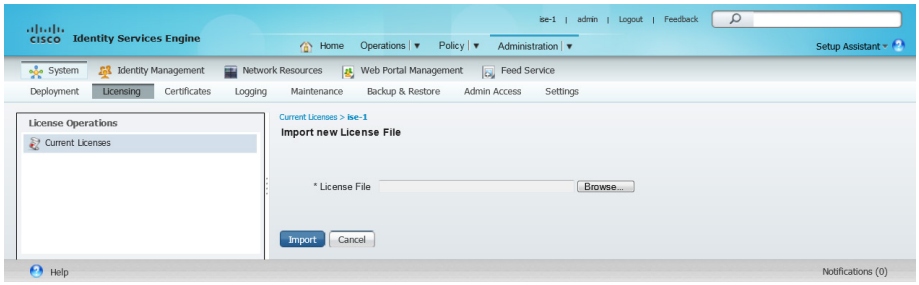
Notice that you see only one node here because the secondary node does not require licensing.

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**.

> **Tech Tip**
>
> When installing a Base license and an Advanced license, you must install the Base license first.

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



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

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**.

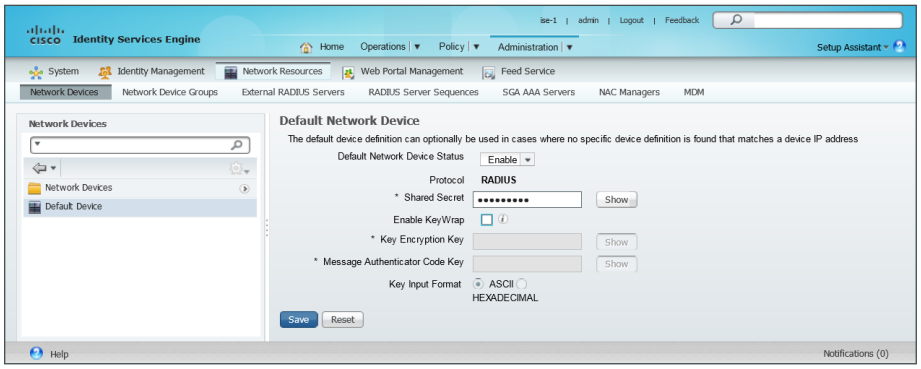
Step 2: In the left pane, click **Default Device**.

Tech Tip

Each network device can be configured individually, or devices can be grouped by location, by device type, or by using IP address ranges. The other option is to use the default device to configure the parameters for devices that aren't specifically configured. All of Cisco's network devices have to use the same key, so for simplicity, this example uses the default device.

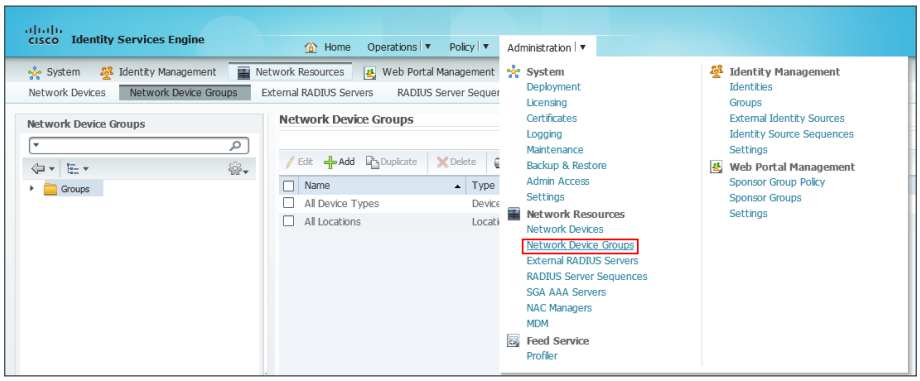
Step 3: In the **Default Network Device Status** list, choose **Enable**.

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

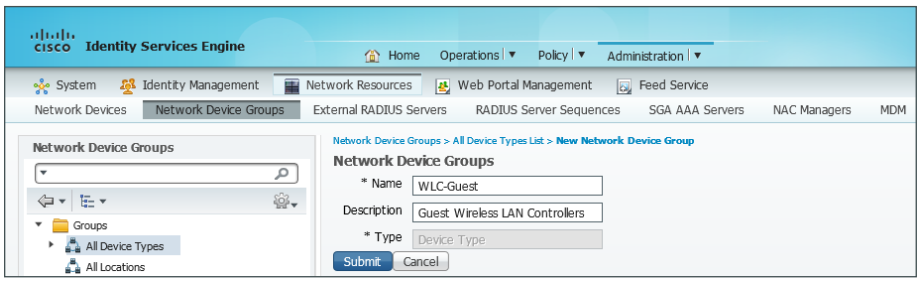


Next, create a Device group that contains the Anchor Guest wireless LAN controllers within the DMZ Internet edge. This will be used later when we define a policy that will be applied to authentication requests from guest users that will use the Sponsor Portal Identity Store, which, starting with Cisco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

Step 5: Within Cisco ISE, navigate to **Administration > Network Resources > Network Device Groups.**



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.



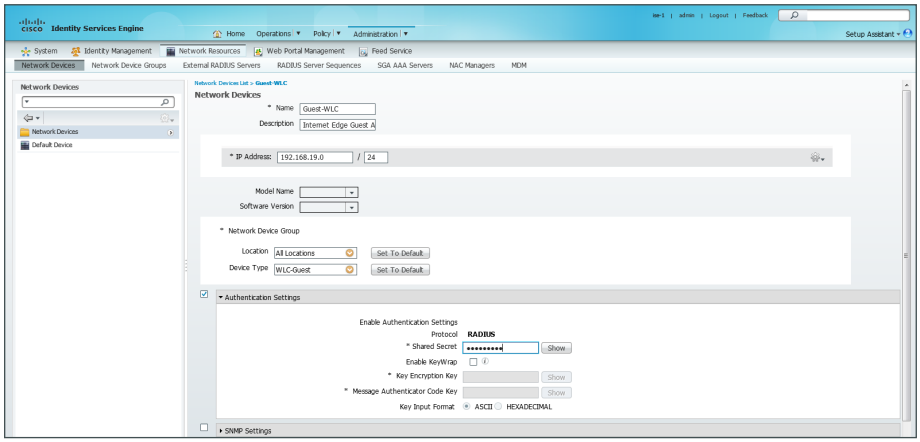
Step 7: Navigate to **Administration > Network Resources > Network Devices**, and then select **+Add**. A new network device is added.

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).



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.

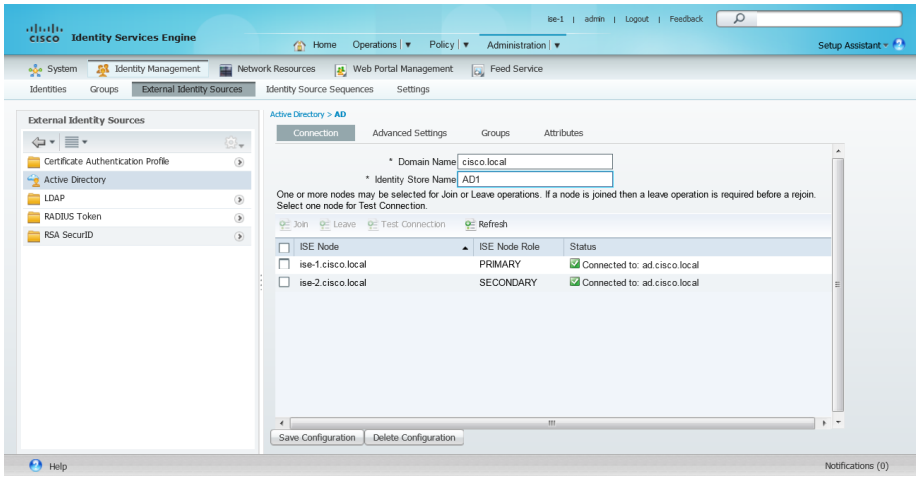
Step 1: On the menu bar, mouse over **Administration**, and then, in the Identity Management section, choose **External Identity Sources**.

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

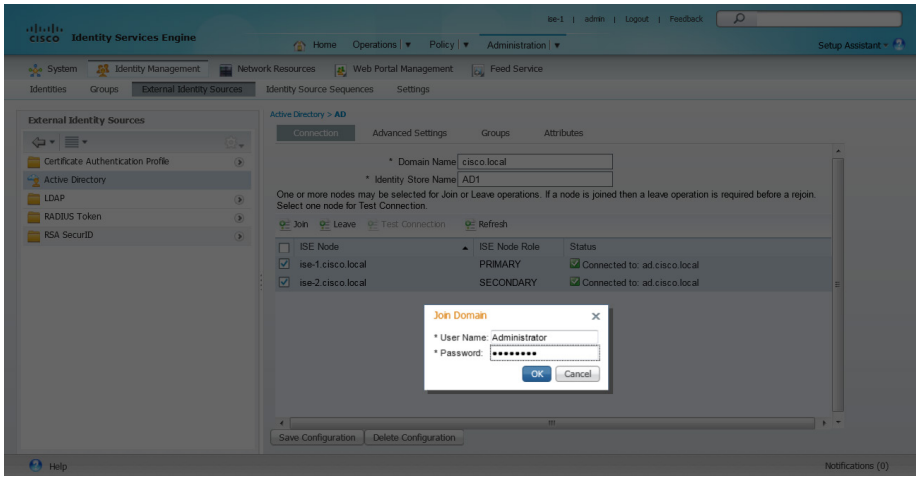
Step 3: On the Connection tab, configure the connection to the AD server by entering the AD domain (Example: cisco.local), the name of the server (Example: AD1), and then click **Save Configuration**.

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

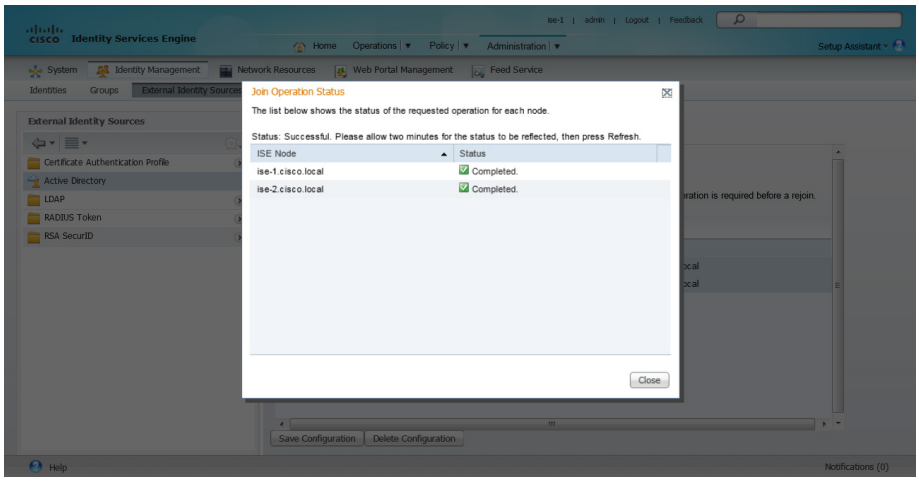
Step 5: Enter the credentials for a domain user, and then click **OK**.



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



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



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.

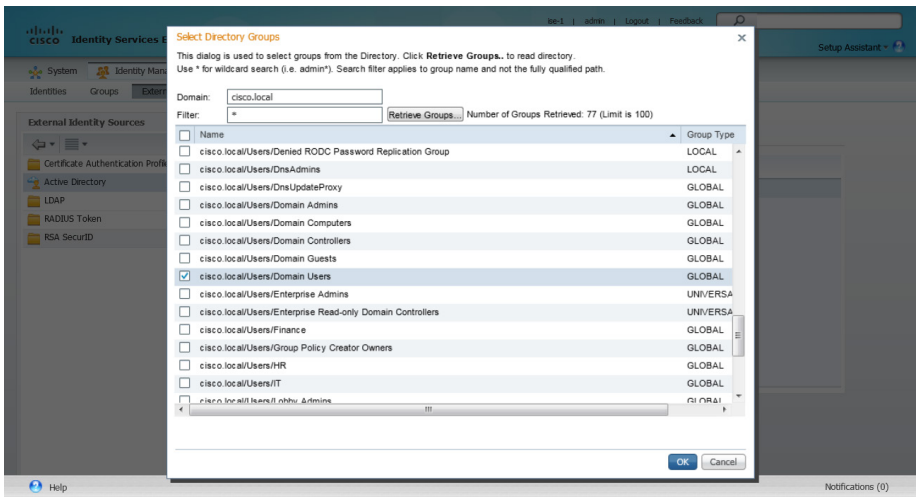
Step 1: On the menu bar, move your mouse over **Administration**, and then, in the Identity Management section, choose **External Identity Sources**.

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

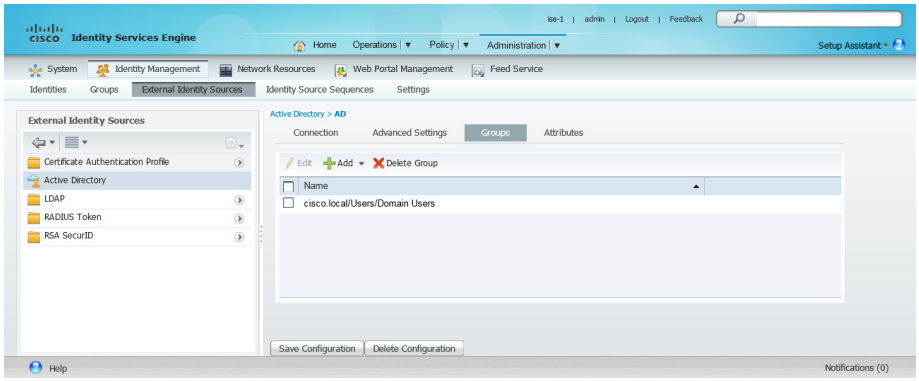
Step 3: Click the **Groups** tab, click **Add**, and then click **Select Groups from Directory**.

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.



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



PROCESS

Configuring On-Site AireOS Wireless Controllers

1. Configure services block for the Cisco 2500, WiSM2 or 5500 Series WLC
2. Connecting the redundancy port for Cisco 5500 Series WLC
3. Configure the switch for Cisco WiSM2 Series WLC
4. Configure the WLC Cisco AireOS platforms by using the Startup Wizard
5. Configure the time zone
6. Configure SNMP
7. Limit which networks can manage the WLC
8. Configure wireless user authentication using Cisco ISE
9. Configure management authentication using Cisco ACS
10. Enable multicast support
11. Create the WLAN data interface
12. Create the wireless LAN voice interface
13. Configure the data wireless LAN for multicast
14. Configure the voice wireless LAN
15. Configure the resilient Cisco 2500 Series controller
16. Enable Band Select and ClientLink on Cisco AireOS WLCs
17. Enable 802.11ac using DCA on Cisco AireOS WLCs

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.

Table 9 - Cisco on-site wireless controller parameters checklist

Parameter	CVD values primary controller	CVD values resilient controller	Site-specific values
Controller parameters			
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[3]	
Default gateway	10.4.175.1	10.4.175.1	
Redundant management IP address (HA SSO)[1]	10.4.175.164[1]	10.4.175.165[1]	
Redundancy port connectivity (HA SSO)[1]	Dedicated Ethernet cable[1] Layer 2 network[2]	Dedicated Ethernet cable[1] Layer 2 network[2]	
Hostname	WLC-1	WLC-2[3]	
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

Parameter	CVD values primary controller	CVD values resilient controller	Site-specific values
Wireless data network 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 network 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

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.

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
!
interface Vlan120
 description Wireless Voice Network
 ip address 10.4.20.1 255.255.252.0
 ip pim sparse-mode
 no shutdown
!
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.

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.

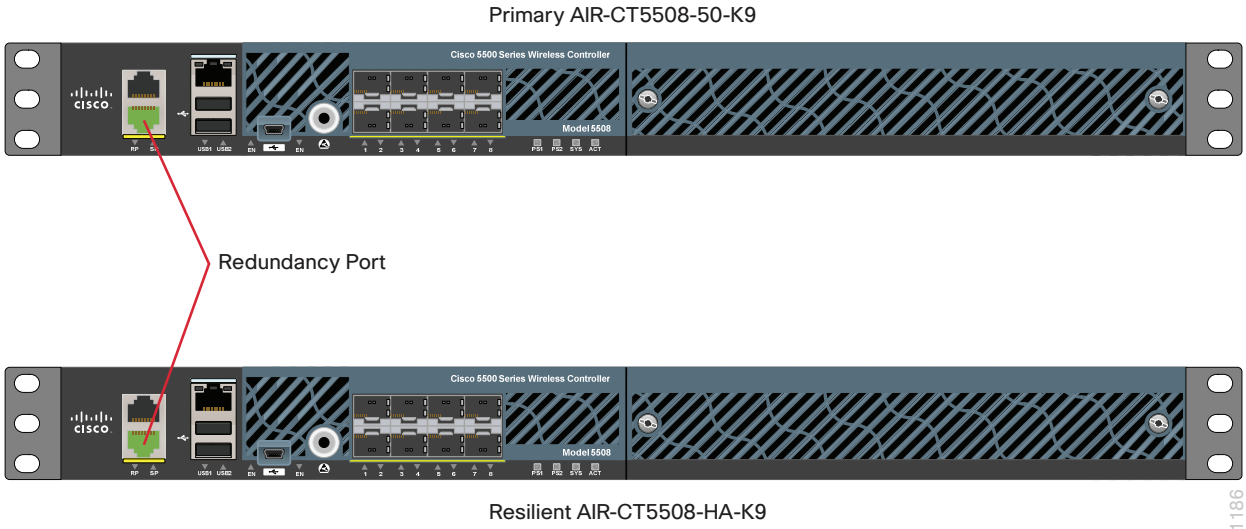
```
interface GigabitEthernet [port 1]
 description To WLC Port 1
interface GigabitEthernet [port 2]
 description To WLC Port 2
!
interface range GigabitEthernet [port 1], GigabitEthernet [port 2]
  switchport
  macro apply EgressQoS
  ! for 6500 with 1Gbps Ethernet, use:
  ! macro apply EgressQoSOneGig
  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 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

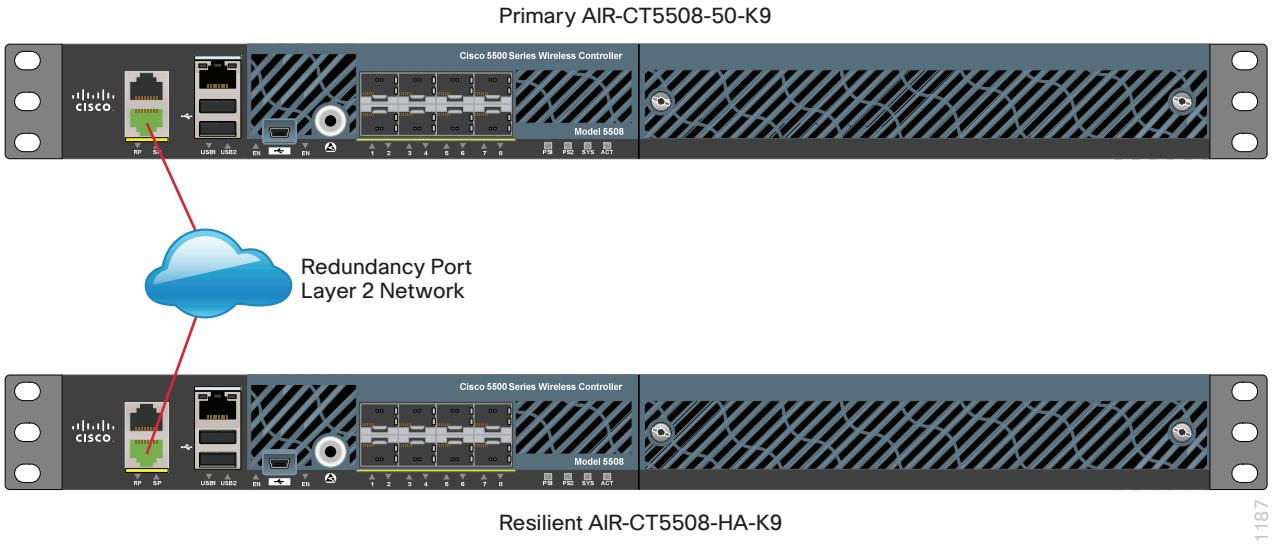
If you are using a Cisco 5500 Series WLC pair and wish to enable the HA SSO feature, continue with this procedure. When using high availability, a dedicated special-purpose port is available on the Cisco 5500 Series WLC. This port is located on the in the lower left of the front panel.

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.



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



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
```

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
```

Tech Tip

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.

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: 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
```

Tech Tip

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
```

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: 239.1.1.1)

```
Multicast IP Address: 239.1.1.1
```

Tech Tip

The multicast address must be unique for each controller or high availability controller pair in the network. The multicast address entered is used as the source multicast address, 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

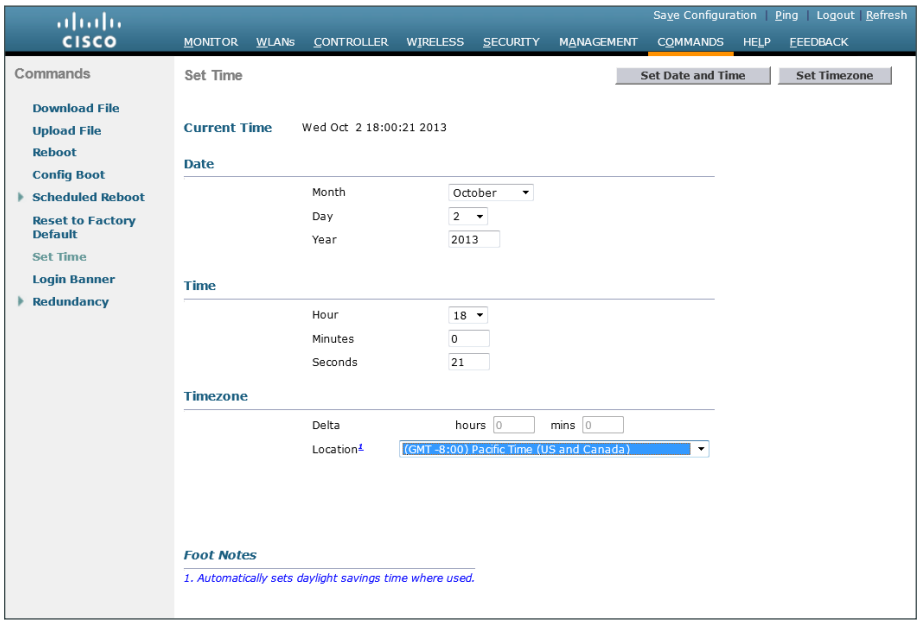
Configuring the time and date of the WLC is critical, because certificate validation is performed using the date/time as configured on the WLC. Improper date/time may prevent access points from successfully registering with the WLC. Ensure that the proper data and time has been obtained from the NTP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

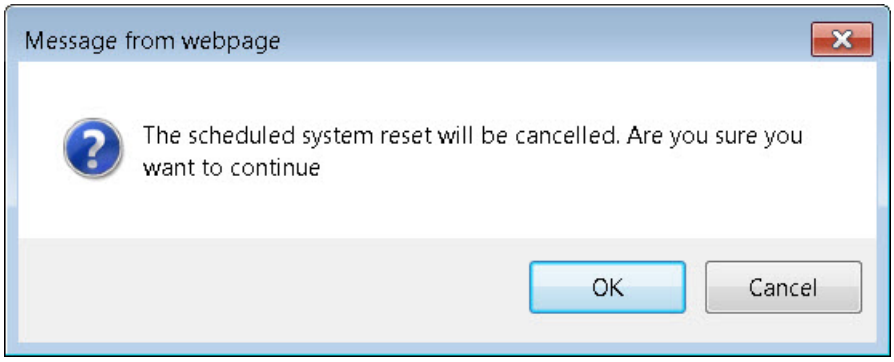
Step 2: Navigate to **Commands > Set Time**.

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

Step 4: Click **Set Time zone**.



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 6 Configure SNMP

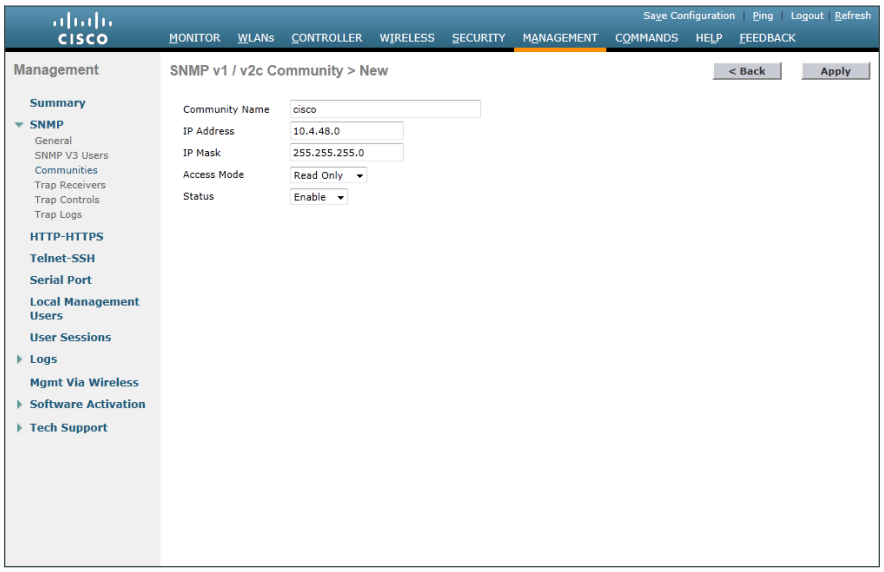
Step 1: In **Management > SNMP > Communities**, click **New**.

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)

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



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

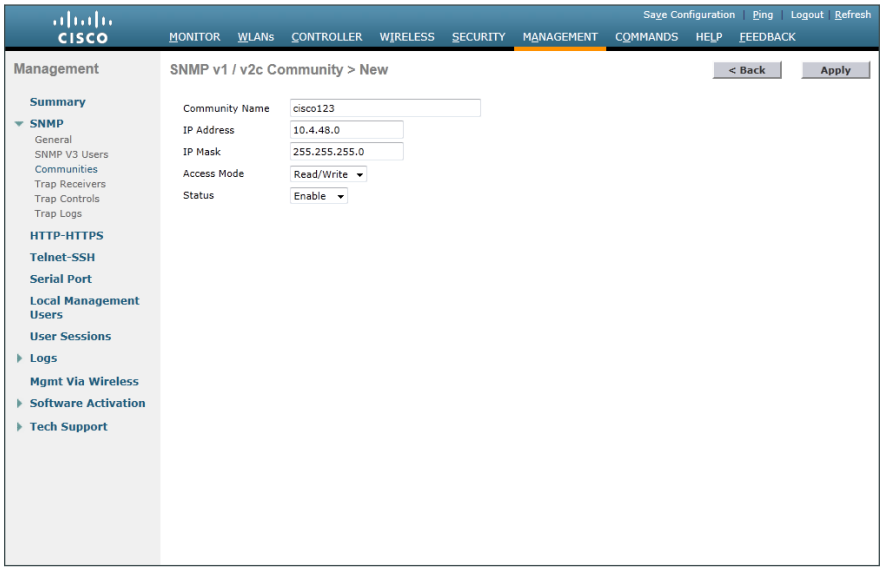
Step 7: Enter the Read/Write **Community Name**. (Example: cisco123)

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**.

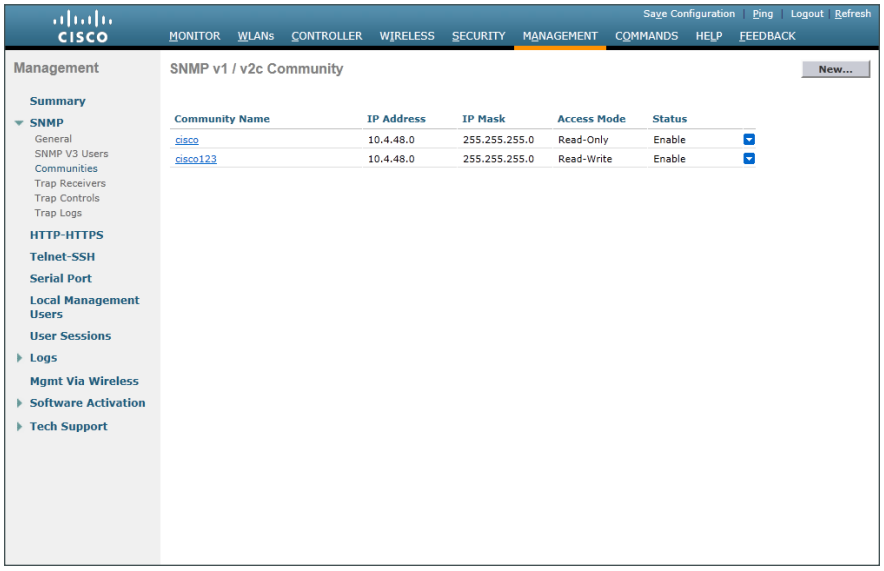


Step 12: Navigate to **Management > SNMP > Communities**.

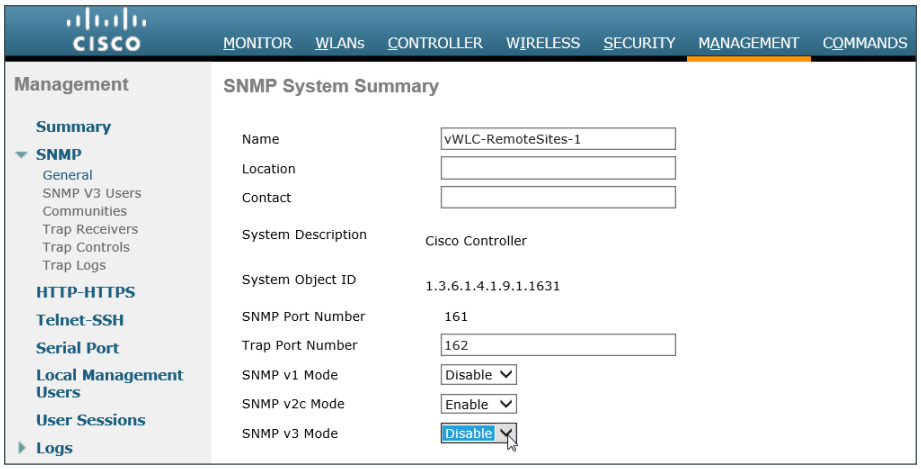
Step 13: On the right side of the **public** community, point and click the blue down arrow, and then click **Remove**.

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.

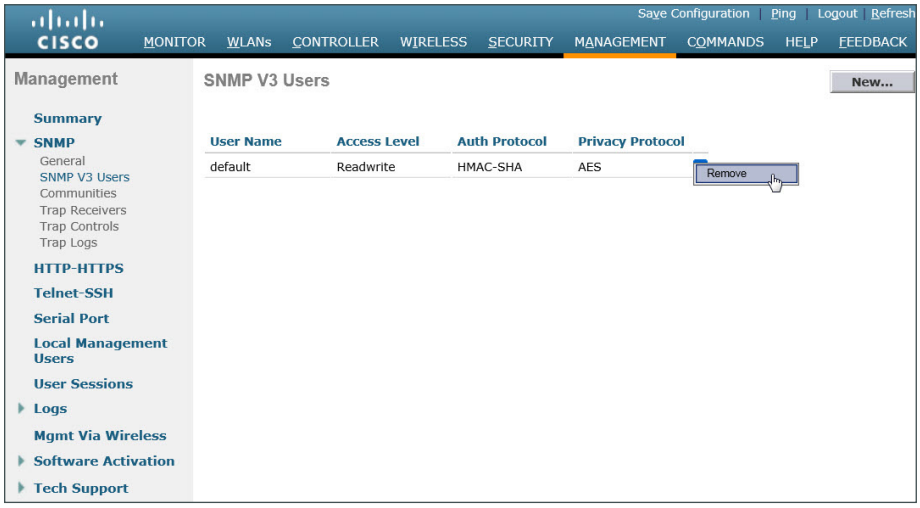


Step 16: Navigate to **Management > SNMP > General** and disable SNMP v3 Mode, then press **Apply**.

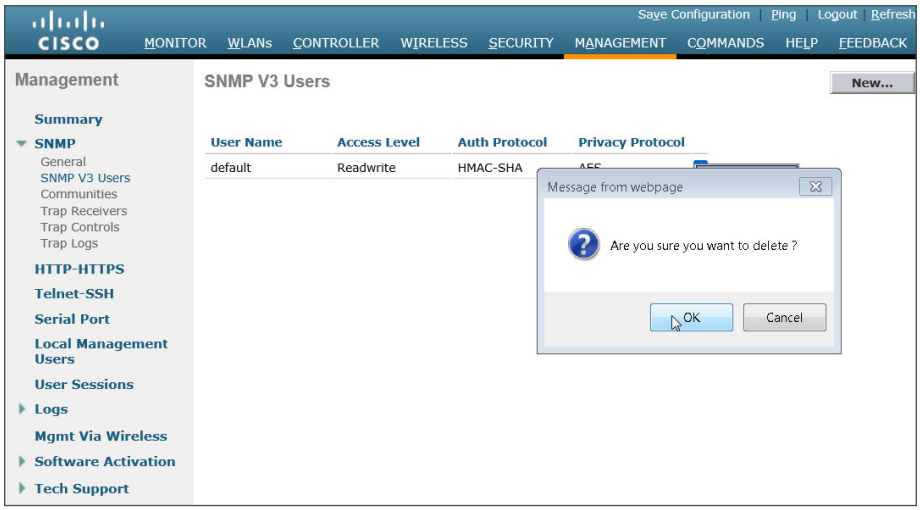


Step 17: Navigate to **Management > SNMP Communities > SNMP V3 Users**.

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



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



Tech Tip

Changes to the SNMP configuration may sometimes require you to reboot the WLC.

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.

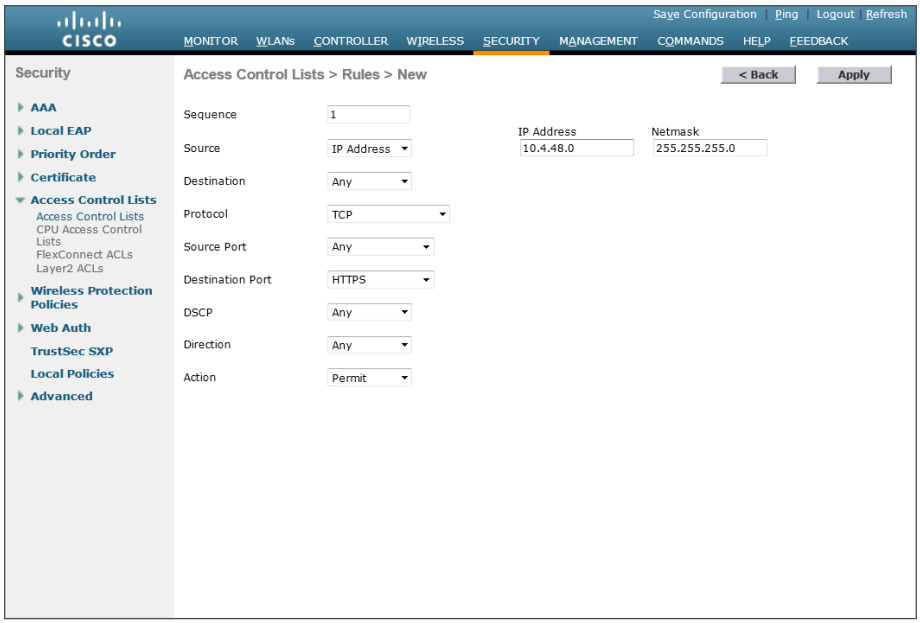
Step 1: In **Security > Access Control Lists > Access Control Lists**, click **New**.

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**

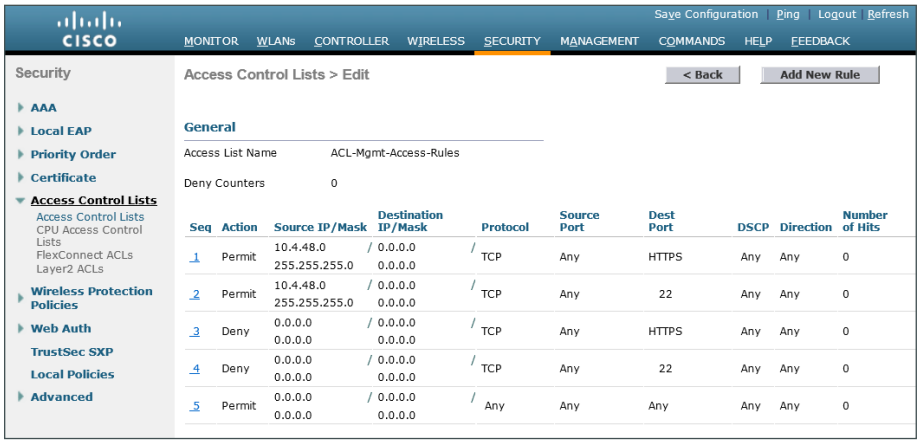


Then click **Apply**.

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

Table 10 - Access 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	TCP	Any	Other/22	Permit
3	Any	Any	TCP	Any	HTTPS	Deny
4	Any	Any	TCP	Any	Other/22	Deny
5	Any	Any	Any	Any	Any	Permit



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

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

Procedure 8 Configure wireless user authentication using Cisco ISE

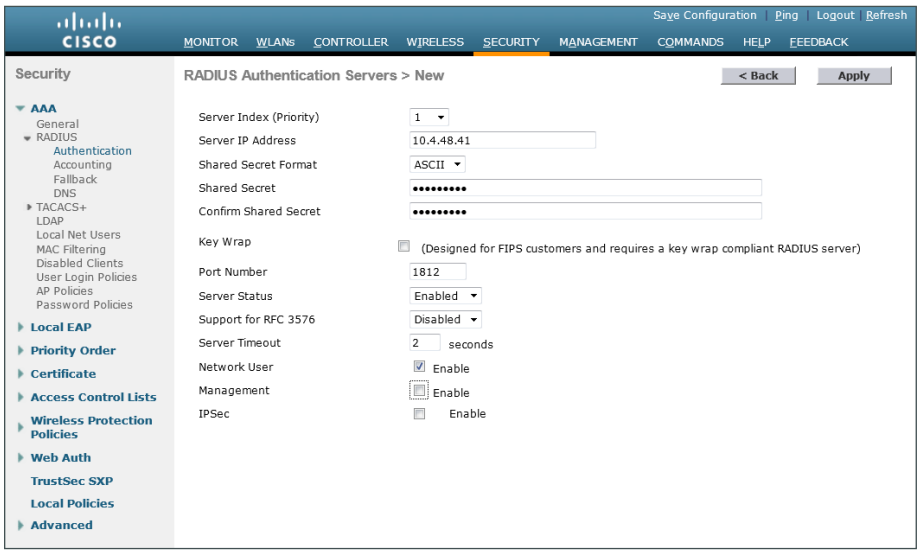
In this design, the RADIUS authentication service is provided by the Cisco Identity Services Engine (ISE). The Cisco ACS server is used solely for network administrative access to the WLC using TACACS+.

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**.

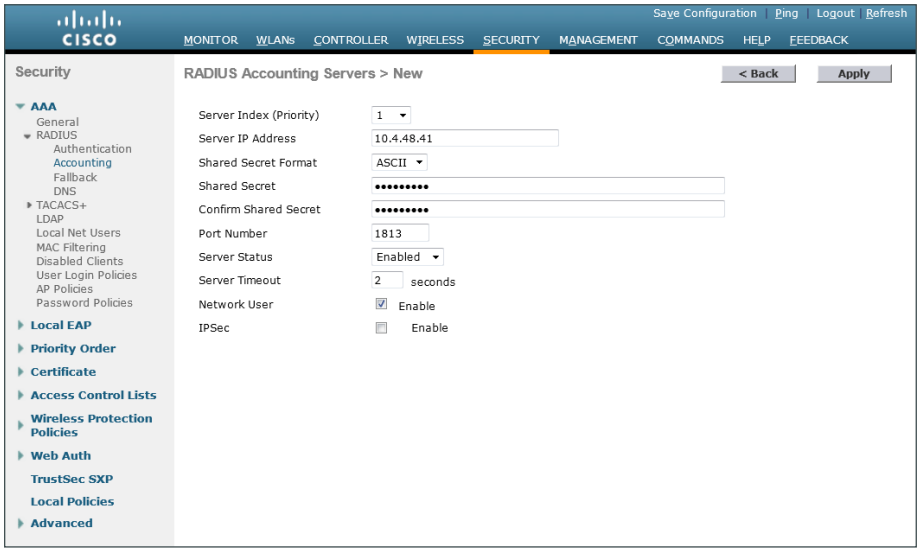


Step 5: Repeat the Step 1 through Step 4 in the above process to add the secondary Cisco ISE authentication server (Example: 10.4.48.42), then press apply followed by click Save Configuration.

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)



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 9 Configure management authentication using Cisco ACS

(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.

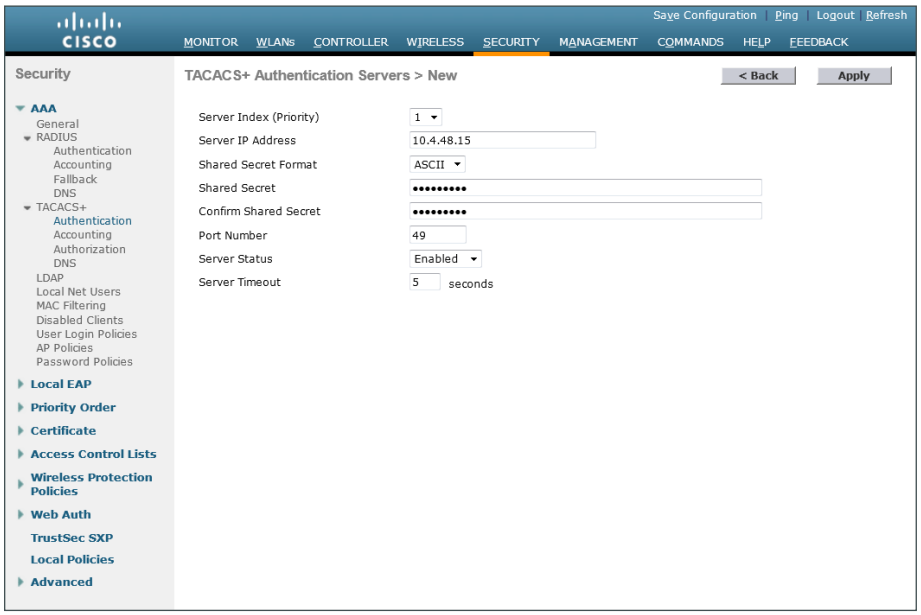
Tech Tip

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)

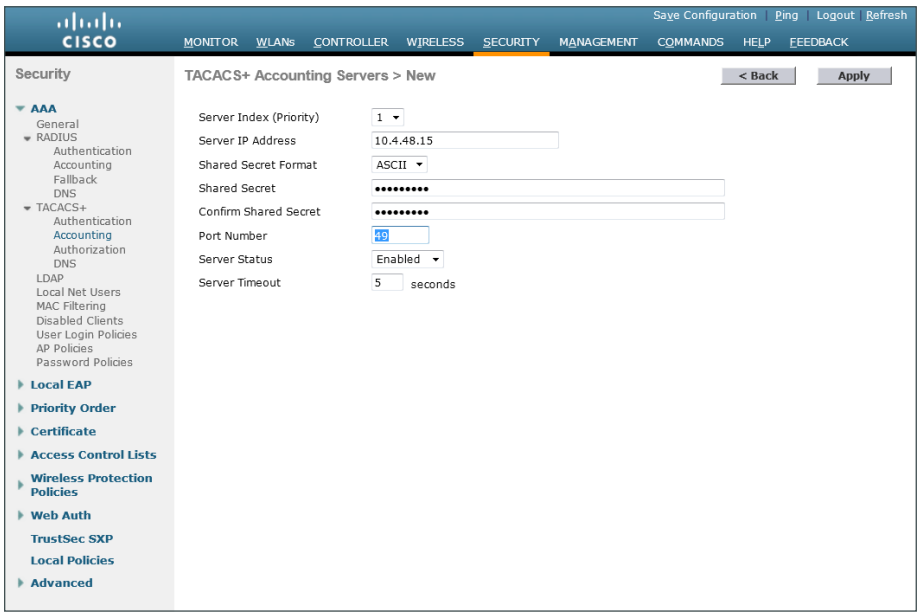
Step 3: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)



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

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

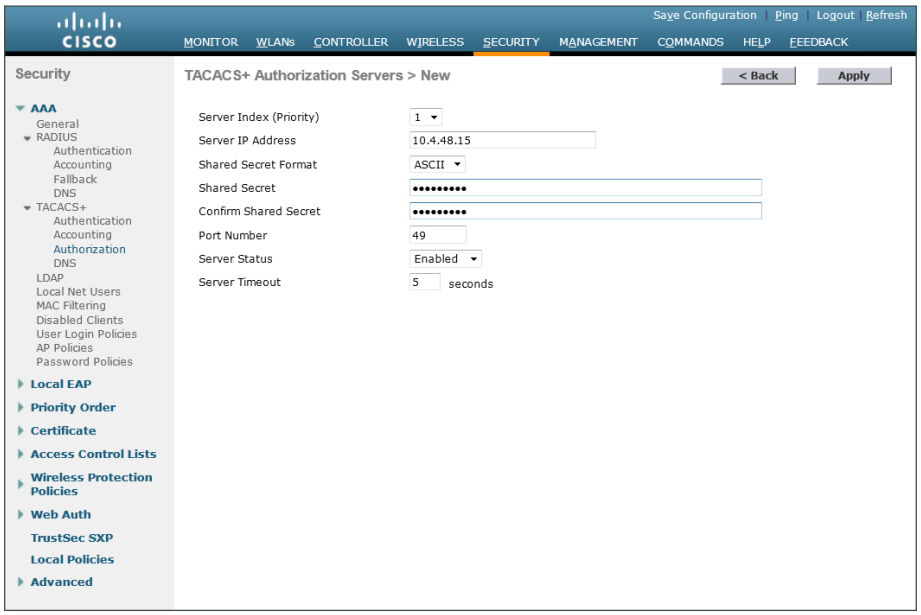
Step 6: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)



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)

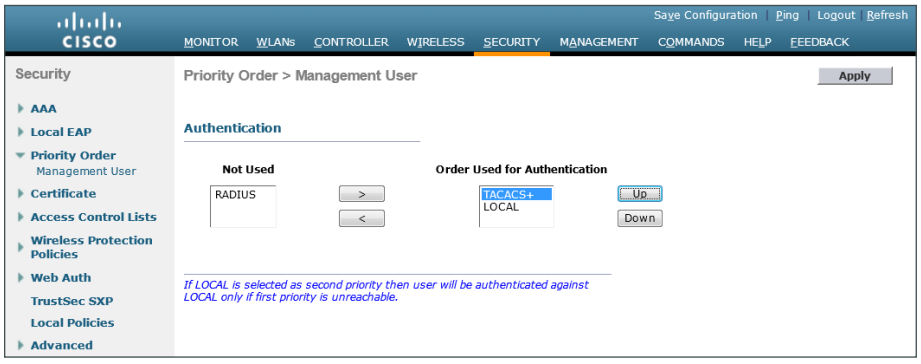


Step 10: Navigate to **Security > Priority Order > Management User**.

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.

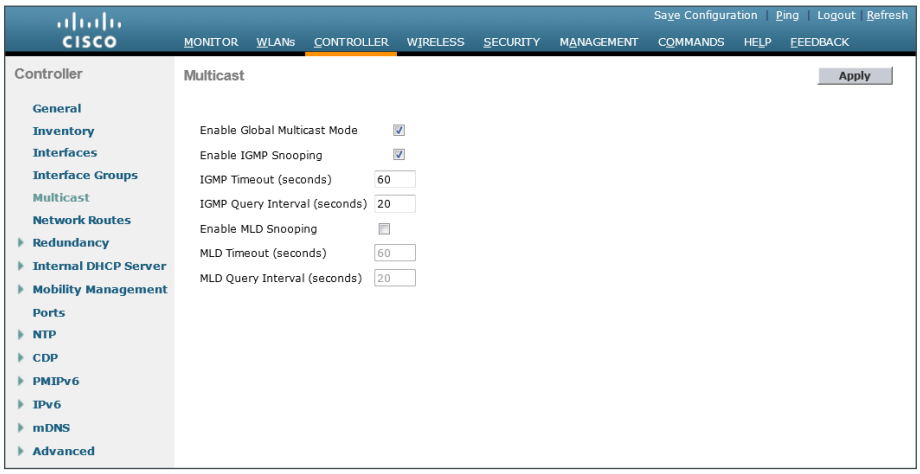
Procedure 10 Enable multicast support

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**.



Step 2: Navigate to **Controller > General**.

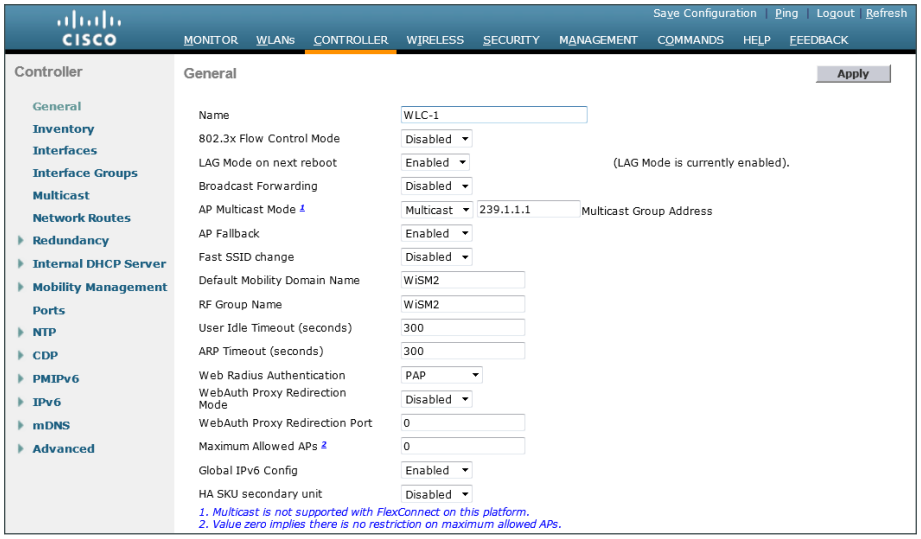
Step 3: If you are using Cisco 5500 or WiSM2 Series Wireless LAN Controllers, in the **AP Multicast Mode** list, choose **Multicast**, and then in the box, enter the multicast IP address that is to be used for multicast delivery (Example: 239.1.1.1), and then click **Apply**.

Reader Tip

Each redundant controller pair must use a unique multicast group address. It is recommended to use the IANA administratively scoped address range 239.0.0.0 - 239.255.255.255 excluding 239.0.0.X and 239.128.0.X. More information about multicast addressing can be found here:

http://www.cisco.com/en/US/tech/tk828/technologies_white_paper09186a00802d4643.shtml

Step 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**.



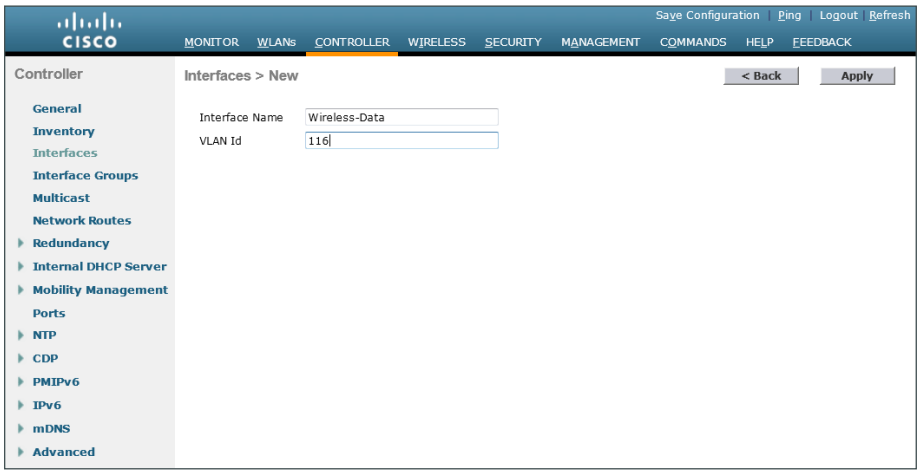
Procedure 11 Create the WLAN data interface

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)

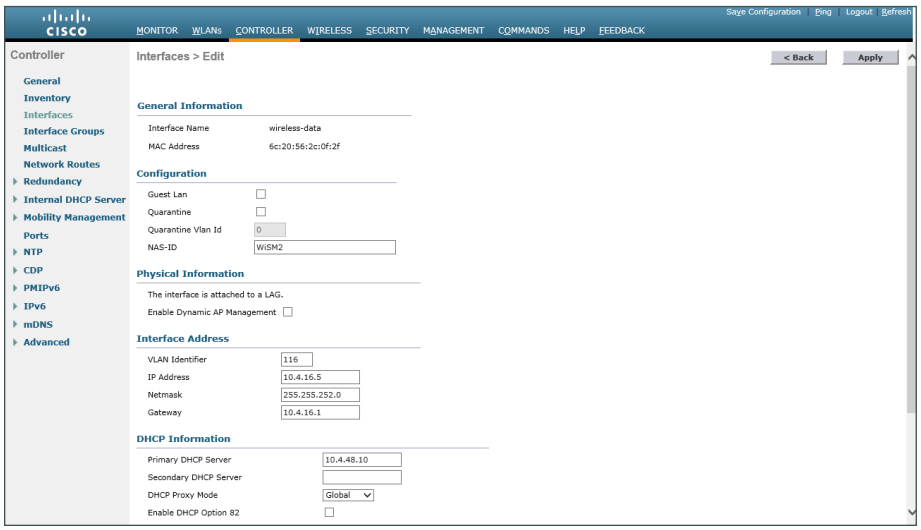


Step 4: In the **IP Address** box, enter the IP address assigned to the WLC interface. (Example: 10.4.16.5)

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**.



Tech Tip

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

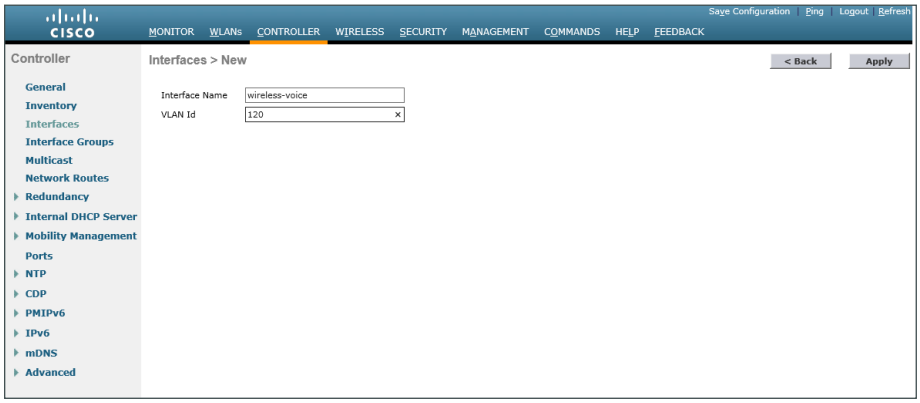
Procedure 12 Create the wireless LAN voice interface

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)

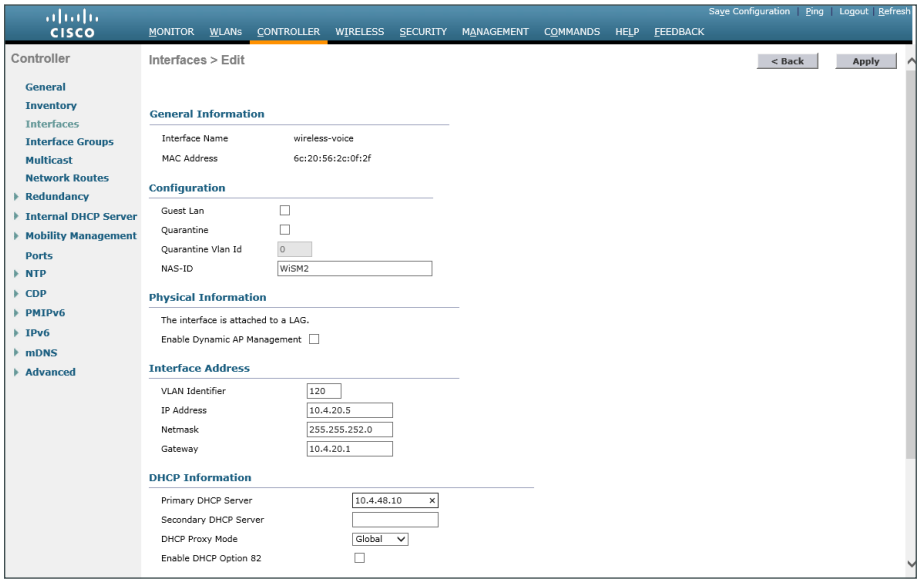


Step 4: In the **IP Address** box, enter the IP address assigned to the WLC interface. (Example: 10.4.20.5)

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**.



Tech Tip

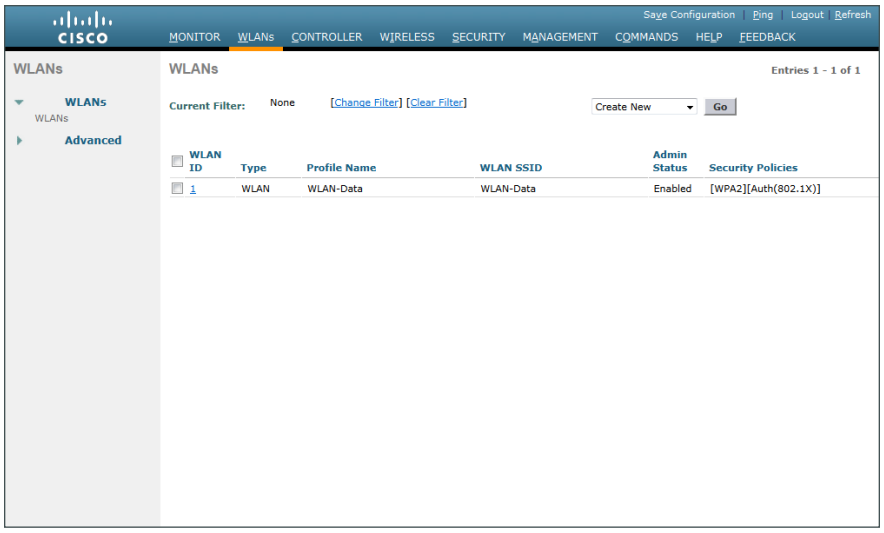
To prevent DHCP from assigning wireless clients addresses that conflict with the WLC's addresses, exclude the addresses you assign to the WLC interfaces from DHCP scopes on the DHCP server.

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.

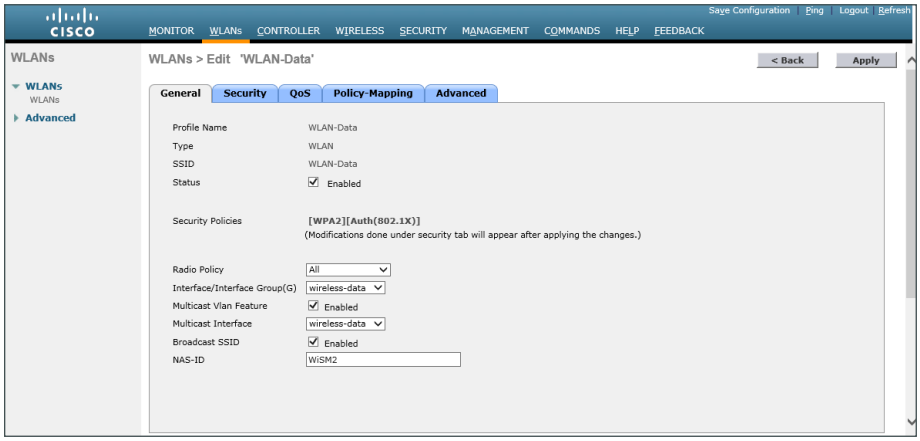
Step 1: Navigate to **WLANs**.

Step 2: Click the WLAN ID number of the SSID created in Procedure 4. (Example: WLAN-Data)



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

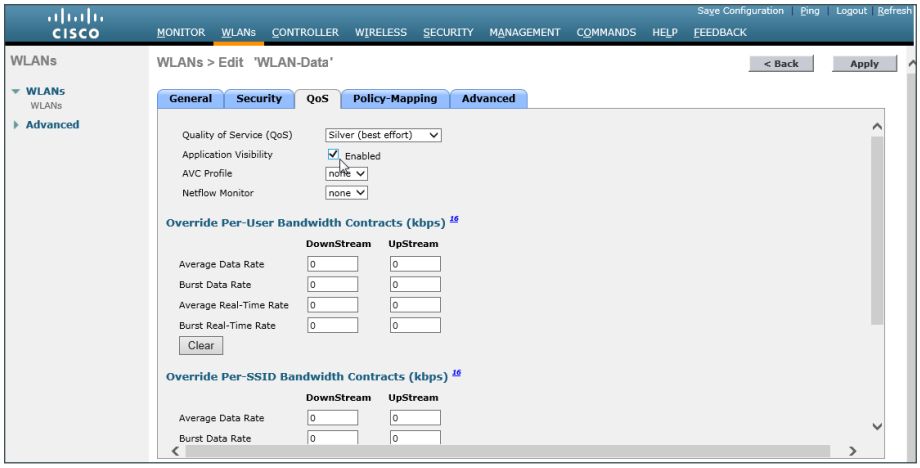
Step 4: If you want to enable multicast on the WLAN-Data wireless LAN, select **Multicast VLAN Feature**, and then in the **Multicast Interface** list, choose the WLAN data interface. (Example: wireless-data)



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.

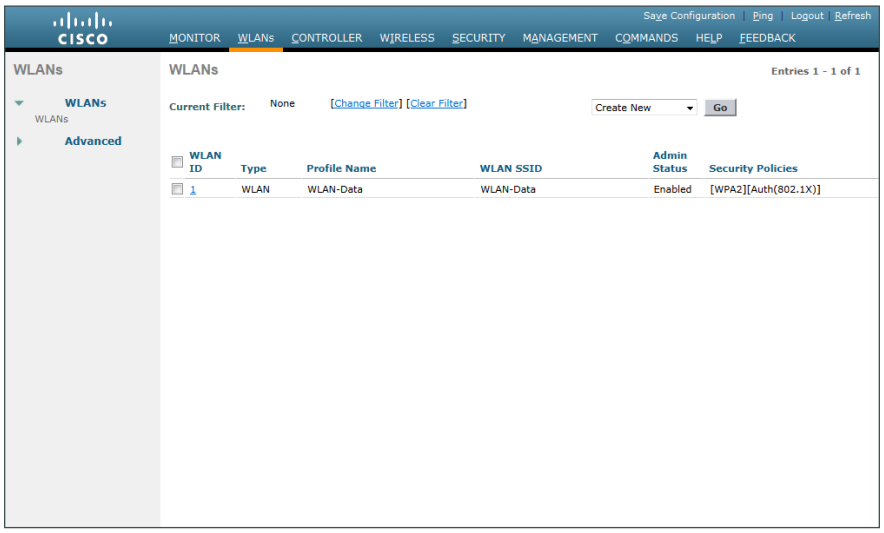


Procedure 14 Configure the voice wireless LAN

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.

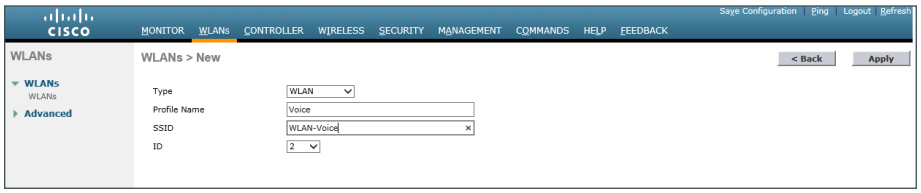
Configure the voice WLAN by changing the default QoS settings to platinum and segmenting the voice traffic onto the voice wired VLAN.

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)

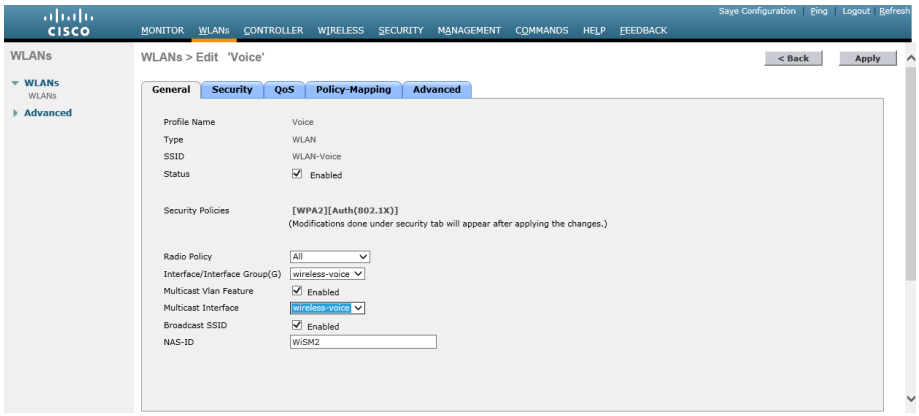


Step 4: On the General tab, next to Status, select **Enabled**.

Step 5: In the **Interface/Interface Group(G)** list, choose the interface created in Procedure 12. (Example: wireless-voice)

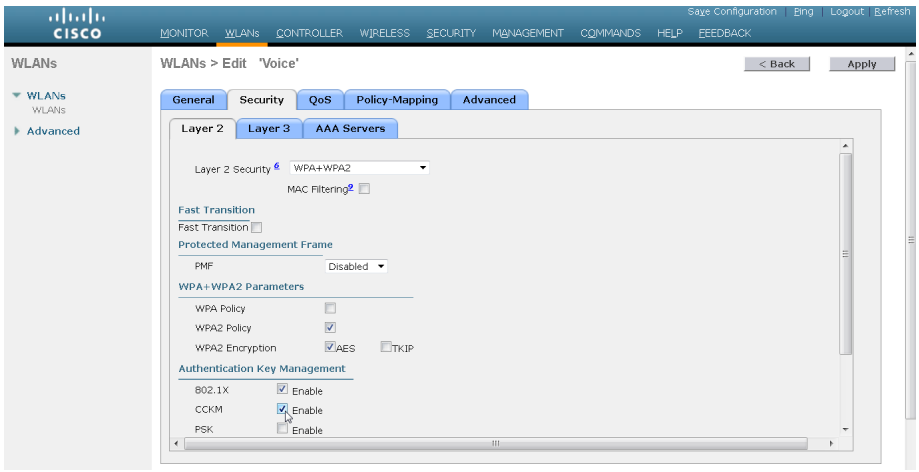
Step 6: If you want to enable multicast on the WLAN-Voice wireless LAN, select **Multicast VLAN Feature**, and then in the **Multicast Interface** list, choose the WLAN Voice interface. (Example: wireless-voice)

Step 7: Click **Apply**.

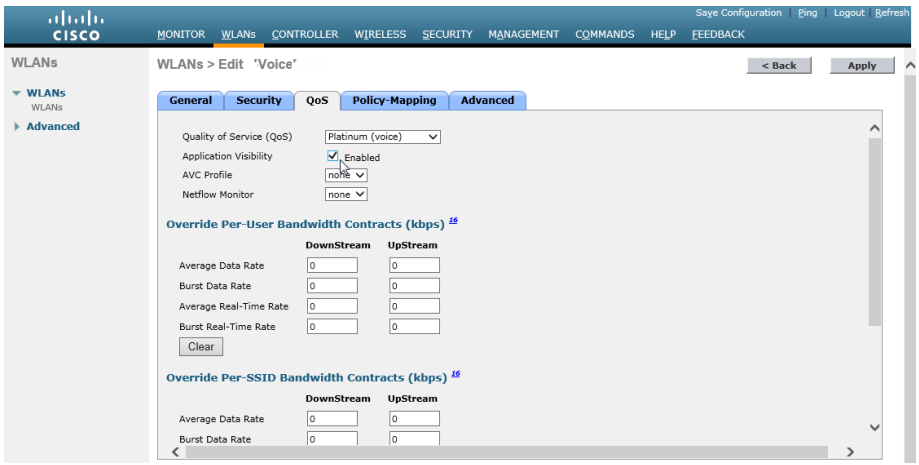


Step 8: On the **Security > Layer 2** tab, enable Cisco Centralized Key Management (CCKM) by selecting **Enable**.

> **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.



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



Procedure 15 Configure the resilient Cisco 2500 Series controller

(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.

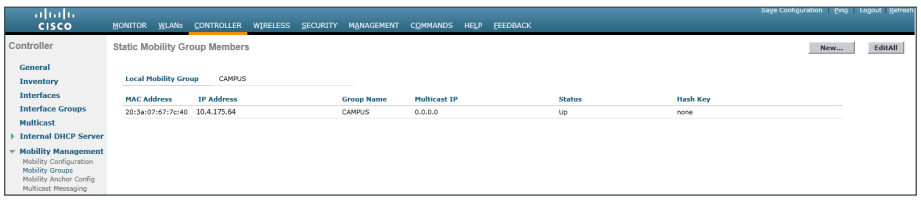
Even when configured as a pair, controllers do not share configuration information as they do when using HA SSO, so you must configure each controller separately.

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 inter-controller WLAN roaming and controller redundancy.

Step 1: Repeat Procedure 4 through Procedure 14 for the resilient controller.

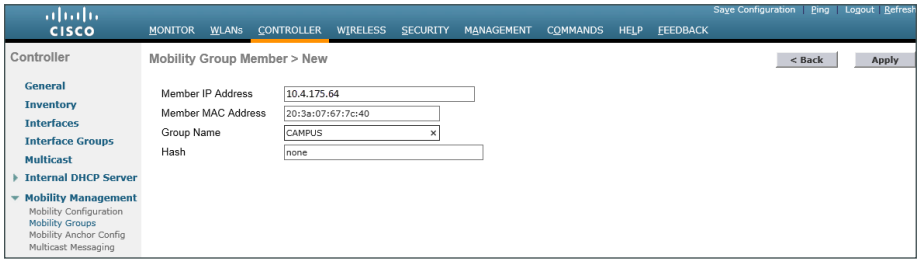
Step 2: On the primary controller, navigate to **Controller > Mobility Management > Mobility Groups**. The MAC address, IP address, and mobility group name for the local controller are shown.



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)

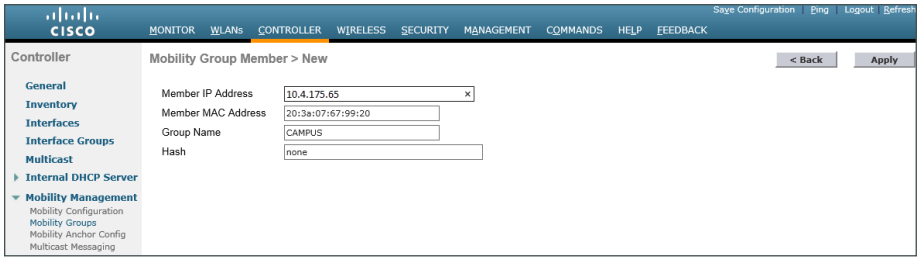
Step 5: In the **Member MAC Address** box, enter the MAC address of the primary controller, and then click **Apply**.



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

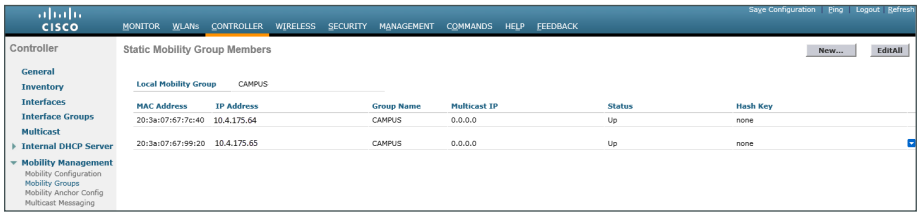
Step 7: In the **Member IP Address** box, enter the IP address of the resilient controller. (Example: 10.4.175.65)

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



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**.

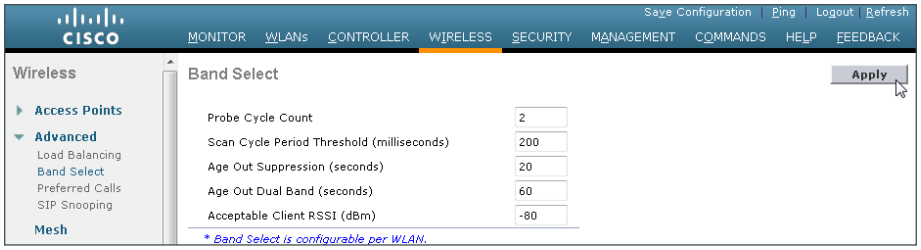


Procedure 16 Enable Band Select and ClientLink on Cisco AireOS WLCs

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.

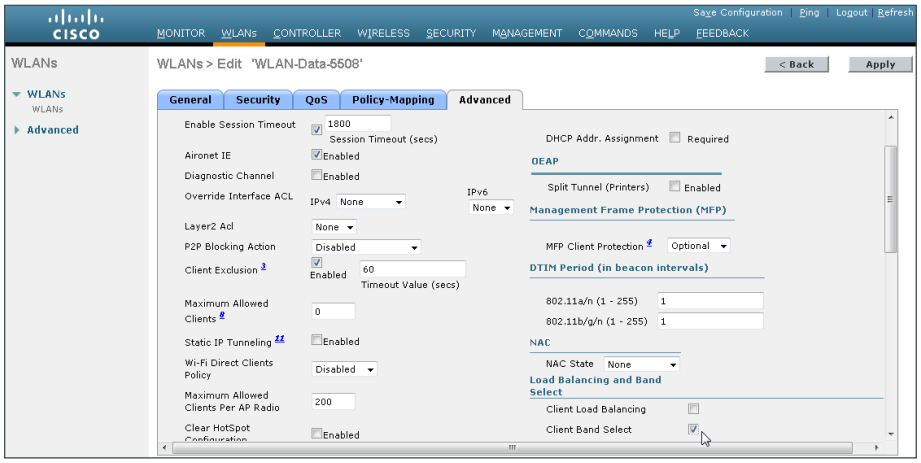
Step 1: Navigate to **Wireless > Advanced > Band Select**, verify the following values are present for Band Select, and then click **Apply**.



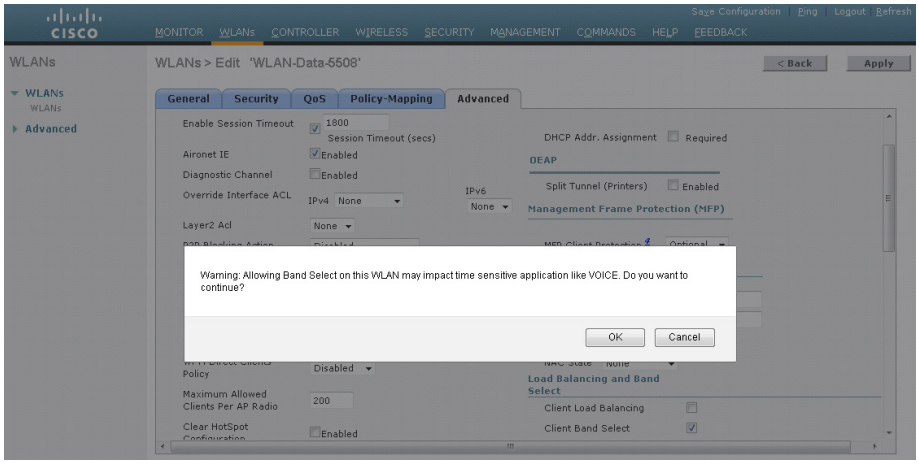
Next, enable Band Select on the WLAN-Data WLAN.

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**.

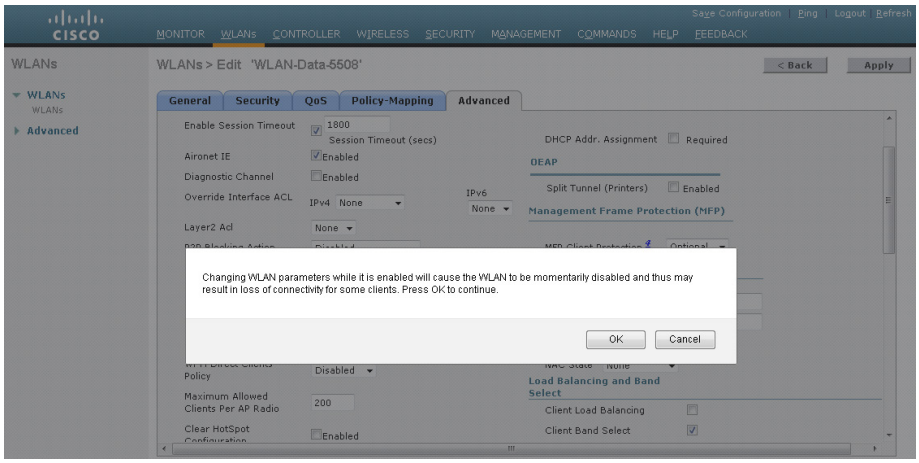


Step 4: Click **OK**. This acknowledges that enabling Band Select may impact time sensitive applications such as Voice.



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.



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.

> **Caution**
>
> 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)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.

> **Caution**
>
> Performing this action is disruptive to ALL access-points on this controller providing 802.11b (2.4 GHz) services.

```
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) y
```

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 .............................. -50
      Legacy Tx Beamforming Configuration .......
CUSTOMIZED
      Legacy Tx Beamforming ..................... ENABLED
      Antenna Type...............................
INTERNAL_ANTENNA
```

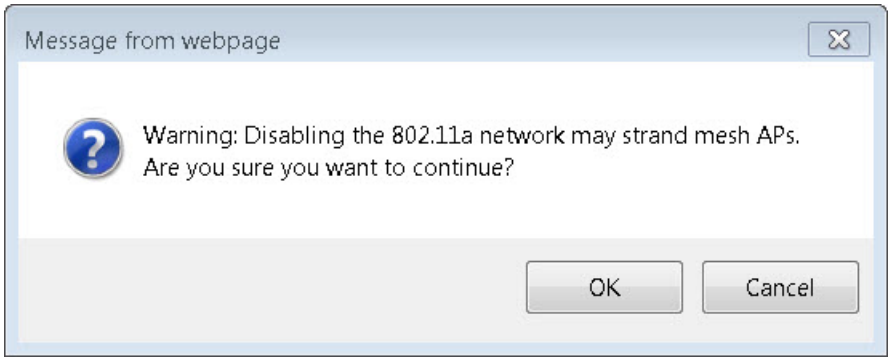
Procedure 17 Enable 802.11ac using DCA on Cisco AireOS WLCs

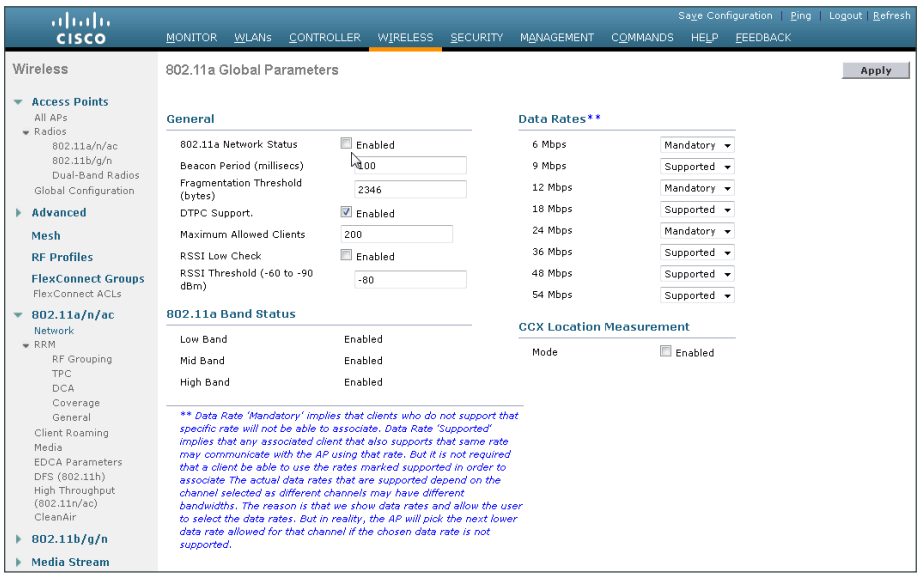
With the advent of 802.11ac Wave 1, 40 and 80 MHz wide channels can be enabled. This can be accomplished manually on an AP-by-AP basis, or globally by using Dynamic Channel Assignment (DCA). Changing the default channel width for 802.11ac capable access points requires the 802.11a network to be disabled.

Reader Tip

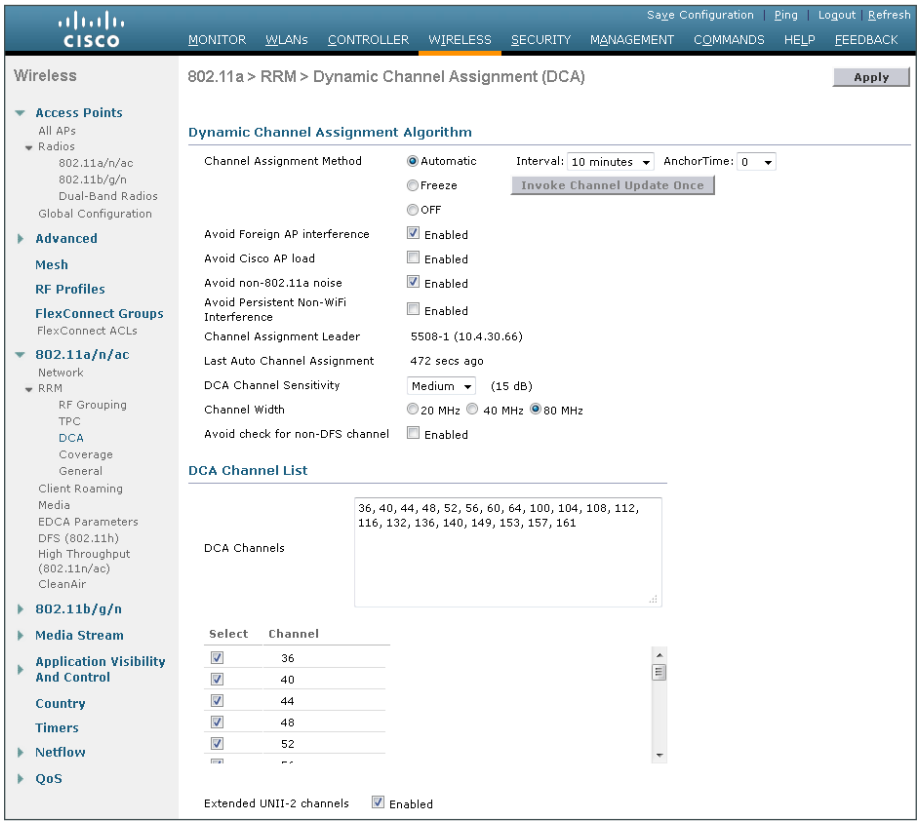
It may be helpful to review the "802.11ac Bandwidth Performance" and "802.11ac Channel Planning" sections in the introductory section of this guide before proceeding with these steps.

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**.

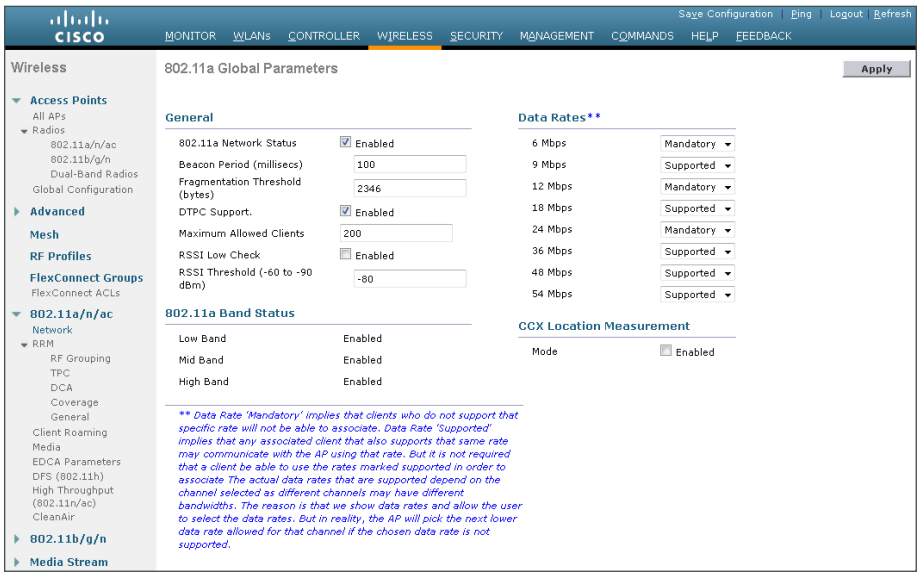




Step 2: Navigate to **Wireless > 802.11a/n/ac > RRM > DCA**, select the desired channel width to use (Example: 20 MHz, 40 MHz, 80 MHz), and then, if available in your regulatory domain, enable **Extended UNII-2 Channels**. (The window may need to be scrolled to view this option.) Click **Apply**.

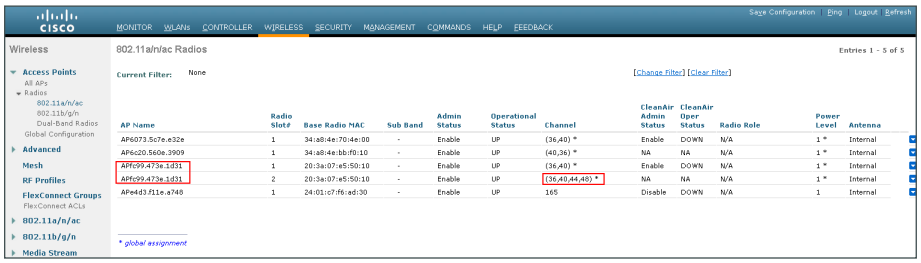


Step 3: Enable the 802.11a network by navigating to **Wireless > 802.11a/n/ac > Network**, selecting the **802.11a Network Status** Enabled box, clicking **Apply**, and then clicking **Save Configuration**. Agree to confirmation questions.



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.



Tech Tip

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.

PROCESS

Configuring On-Site 5760 (IOS-XE) Wireless Controller

1. Configure the Services Block for the Cisco 5760 Series WLC
2. Use CLI to initially configure Cisco 5760 Series WLC
3. Configure wireless user authentication on Cisco 5760 Series WLC
4. Configure management authentication on Cisco 5760 Series WLC
5. Configure wireless settings on the 5760
6. Enable multicast support on 5760 WLC
7. Configure the 5760 voice wireless LAN
8. Configure the 5760 data Wireless LAN
9. Apply QoS on the Cisco 5760 Series Wireless LAN Controller
10. Enable Band Select and ClientLink 1.0 on Cisco 5760 Series WLC
11. Enable 802.11ac on the Cisco 5760 Series WLC
12. Create the mobility peers on Cisco IOS-XE WLCs
13. Configure the guest WLAN on IOS-XE controllers

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.

Procedure 1 Configure the Services Block for the Cisco 5760 Series WLC

(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
!
interface Vlan120
 description Wireless Voice Network
 ip address 10.4.20.1 255.255.252.0
 ip pim sparse-mode
 no shutdown
!
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.

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
!
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.

Tech Tip

High availability support on Cisco 5760 using the stacking cables began in release 3.3.0SE. Ensure that both 5760 controllers are using the 3.3.2SE or later.

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

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)#
```

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.

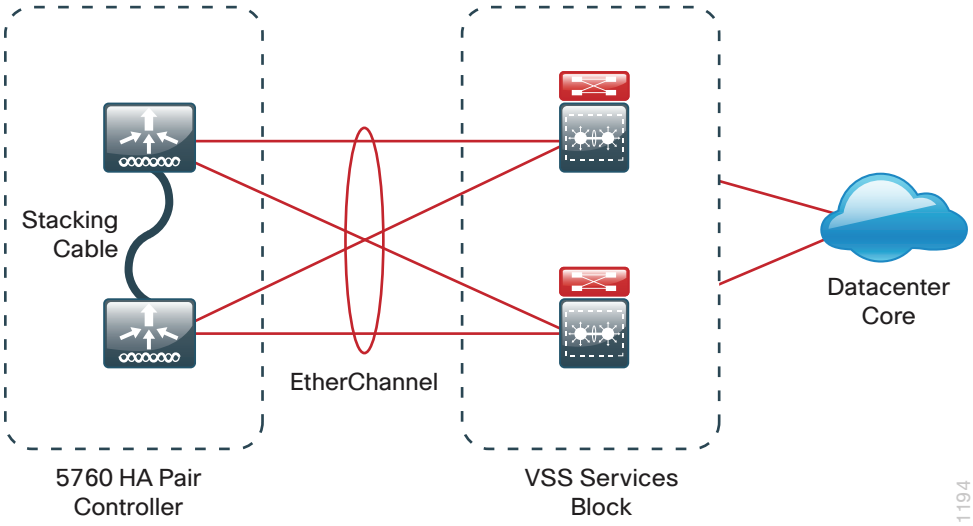
```
interface Vlan[WLAN Data vlan]
 ip address [ip address] [mask]
 ip helper-address [dhcp server ip address]
```

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
```

Tech Tip

When using a Cisco 5760 Series WLC high availability pair that is connected to a VSS-based services block, it is possible to configure all 12 ports of the 5760 pair in a single EtherChannel with 8 ports forwarding and 4 serving as backup links. When one of the 8 primary ports fail, one of the hot-standby ports automatically becomes active. The system (Services VSS switch or 5760 high availability pair) with the highest lacp system-priority determines which links are active. Configuring the 5760 high availability pair with a lacp system-priority lower than the default of 32768 and lower than its upstream VSS switch, will cause the 5760 high availability pair to determine which links are active and which are placed in hot standby mode. All port members in a LACP EtherChannel bundle have a default lacp port-priority of 32768. Assigning a higher lacp port-priority to the backup ports will make them less desirable and place them in Hot Standby status.

```
5760-WLC(config)#lacp system-priority 16384
5760-WLC(config)#interface TenGigabitEthernet [desired
backup port number]
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 c1sco123
username admin password c1sco123
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
!
aaa new-model
radius-server attribute 6 on-for-login-auth
radius-server dead-criteria time 10 tries 3
radius-server deadtime 3
!
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
!
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
!
!
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
!
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

Tech Tip

The Cisco 5760 Series WLC supported browsers as of Cisco IOS-XE version 3.3.0SE are as follows:

Google Chrome Version 26.x
Microsoft Internet Explorer Version 10.x
Mozilla Firefox Version 20.x

Procedure 3 Configure wireless user authentication on Cisco 5760 Series WLC

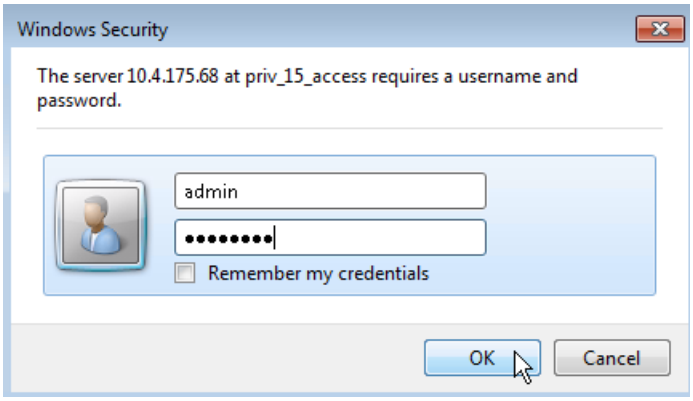
Step 1: Starting in this release of the CVD, the RADIUS authentication service is provided by the Cisco Identity Services Engine (ISE). The Cisco ACS server will solely be used for network administrative access to the WLC using TACACS+.

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

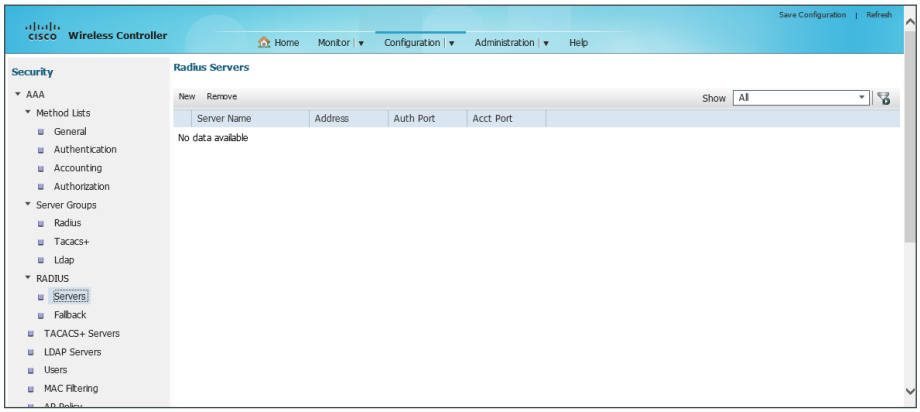
Step 2: When accessing the WLC using a web browser using SSL, accept the WLC self-signed certificate. Depending on the browser in use, select the option that allows you to continue to the website using the certificate presented to the browser.

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).



Next, define a new RADIUS server.

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

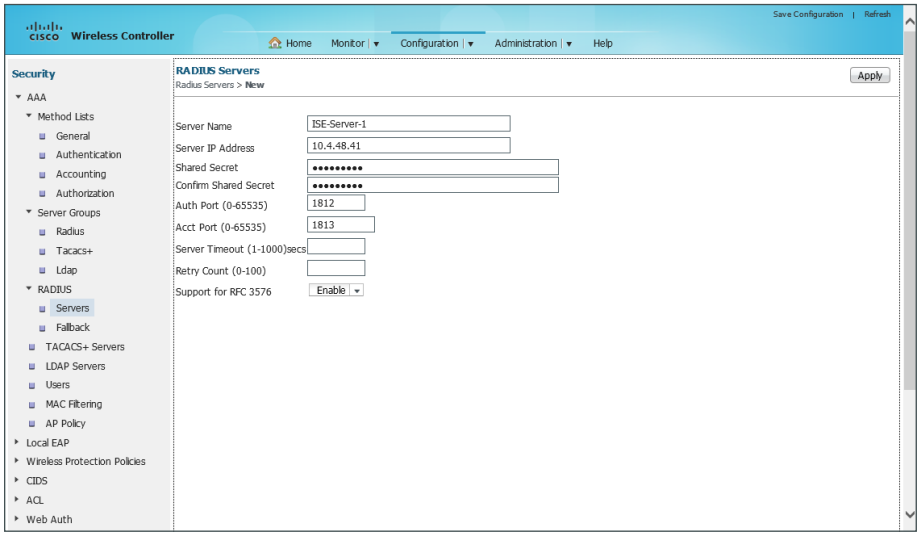


Step 5: Enter a name for the Cisco ISE server, the IP address, and the shared secret (SecretKey).

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

Tech Tip

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.



The preceding steps apply this configuration.

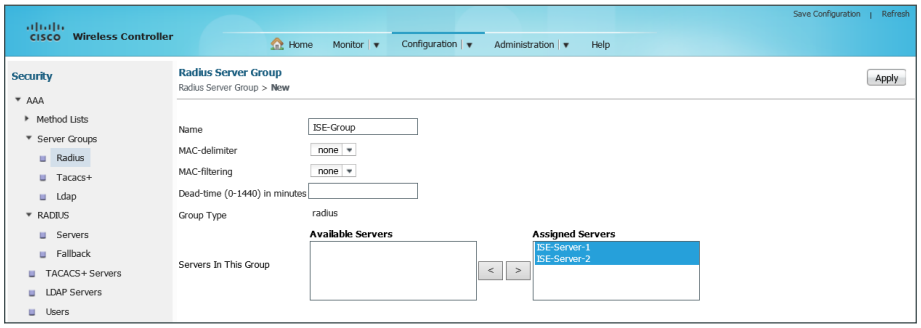
```
radius server [RADIUS Server Name]
 address ipv4 [IP address] auth-port 1812 acct-port 1813
 key [SecretKey]
```

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**.



The preceding steps apply this configuration.

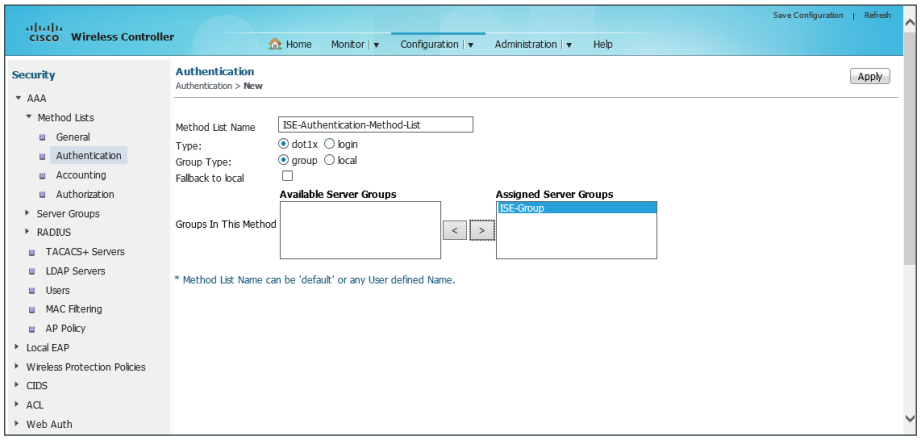
```
aaa group server radius [Group Name]
 server name [RADIUS Server Name]
!
```

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**.



The preceding steps apply this configuration.

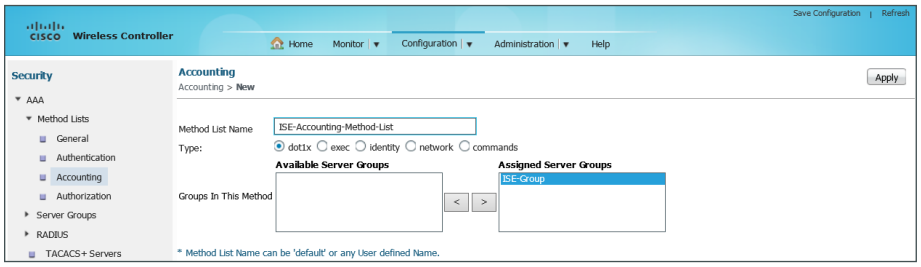
```
aaa authentication dot1x [Method List Name] group [Group Name]
```

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**.



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)

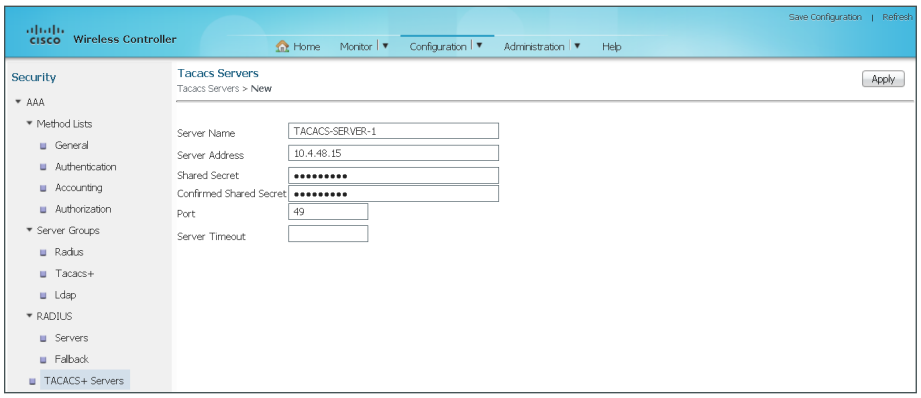
Beginning with this CVD, Cisco Secure ACS will be used solely to provide authentication, authorization and accounting (AAA) services for controlling network management access. Secure ACS will not be used to provide security services for wireless users authenticating to the wireless network.

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**.



The preceding steps apply this configuration.

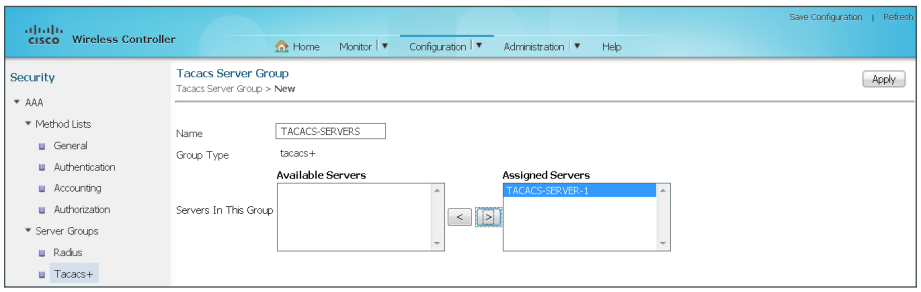
```
tacacs server [Server Name]
 address ipv4 [IP address]
 key [SecretKey]
```

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**.



The preceding steps apply this configuration.

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

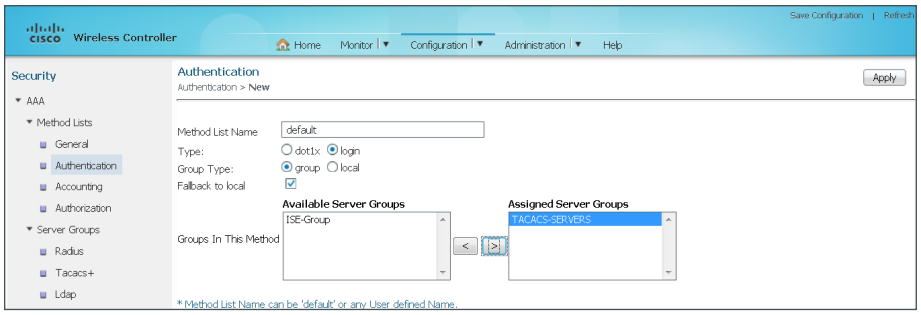
Next, create a default Method List for TACACS+ management access to the WLC.

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**.



The preceding steps apply this configuration.

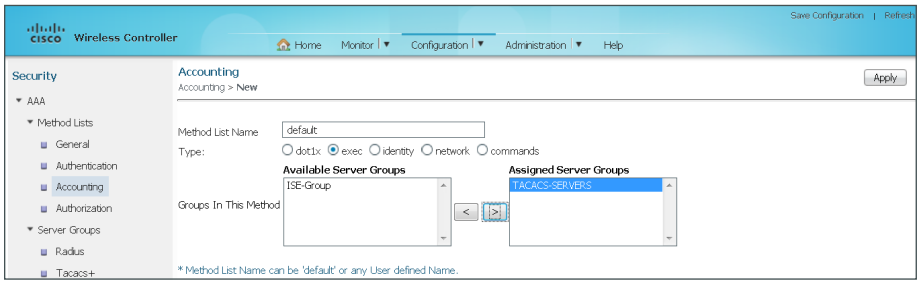
```
aaa authentication login default group [TACACS Group Name] local
```

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**.



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**.

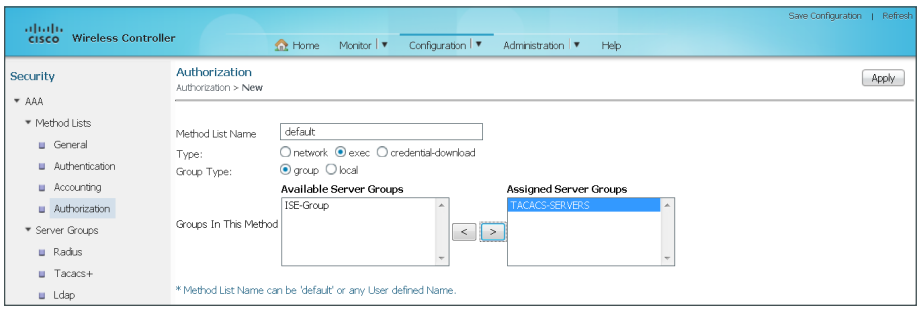
Step 14: Enter a Method List name. (Example: ACS-Authorization-Method-List)

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**.

Tech Tip

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.



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
```

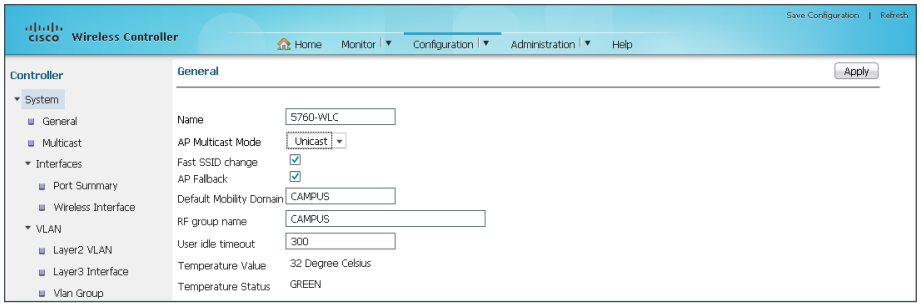
Procedure 5 Configure wireless settings on the 5760

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**.

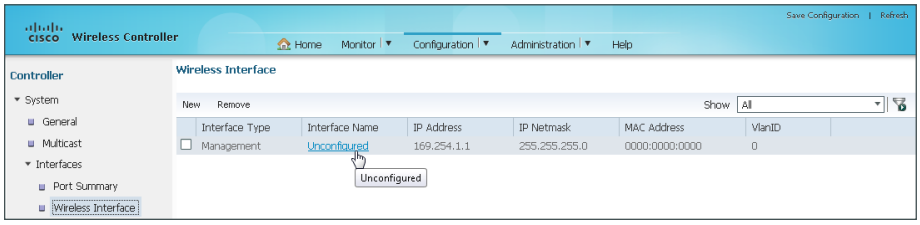
Step 2: Select **Fast SSID change**, enter a **Default Mobility Domain** name (Example: Campus) and an **RF group name** (Example: CAMPUS), and then click **Apply**.



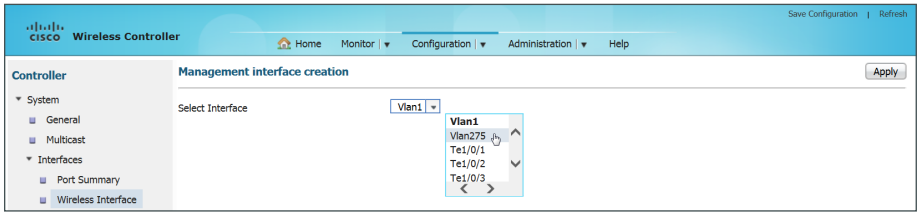
The preceding steps apply this configuration.

```
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.



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.



The preceding steps apply this configuration.

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

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.

Reader Tip

Each redundant controller pair must use a unique multicast group address. It is recommended to use the IANA administratively scoped address range 239.0.0.0239.255.255.255 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

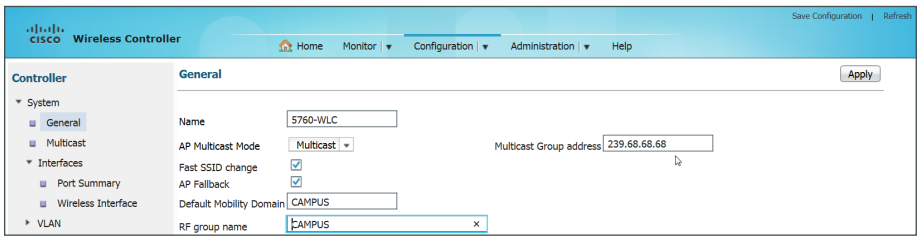
Step 1: Navigate to **Configuration > Controller > System > General**.

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)

Tech Tip

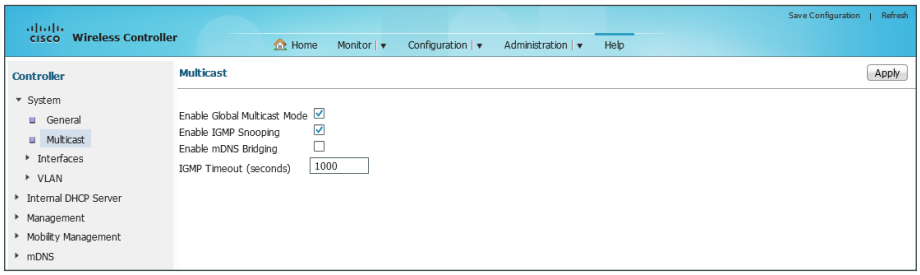
The multicast address must be unique for each controller or controller high availability pair in the network. The multicast address entered is used as the source multicast address, which the access points registered to the controller will use for receiving wireless user-based multicast streams.



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**



The preceding steps apply this configuration.

```
wireless multicast
```

Example

```
wireless multicast
ap capwap multicast 239.68.68.68
```

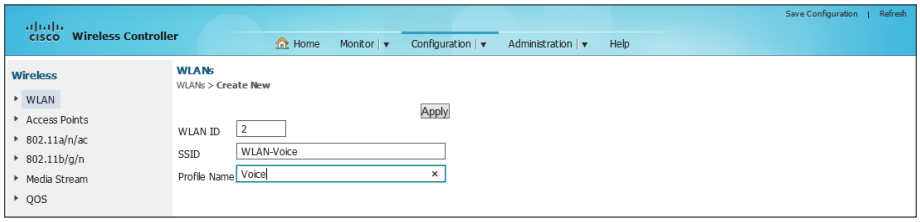
Procedure 7 Configure the 5760 voice wireless LAN

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**.

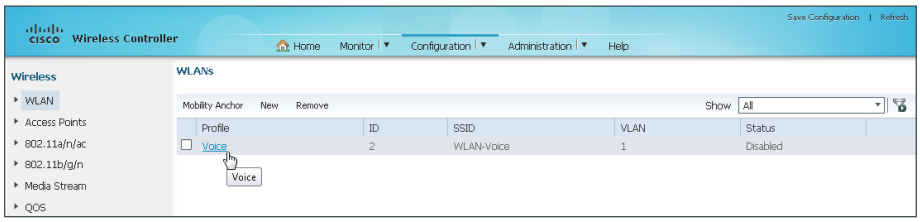


The preceding steps apply this configuration.

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

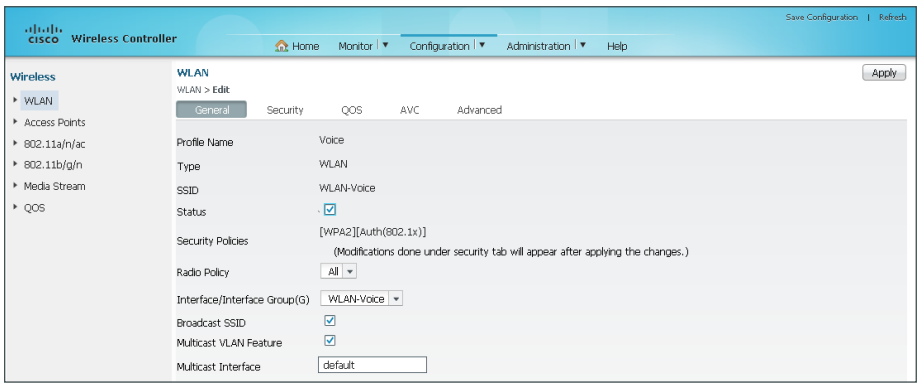
Next, configure the specific parameters of the Voice WLAN.

Step 3: Click the profile name you just created.

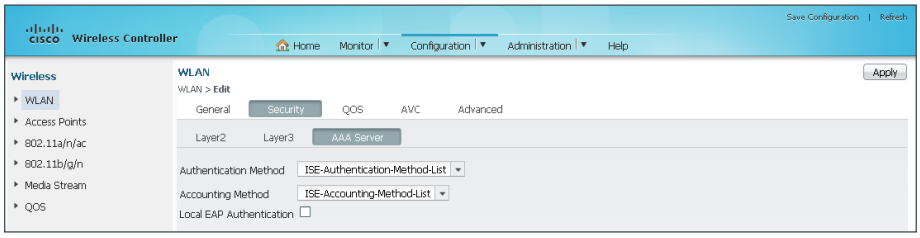


Step 4: On the General Tab for the Wireless Voice WLAN, from the menu, choose the **WLAN-Voice interface**.

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



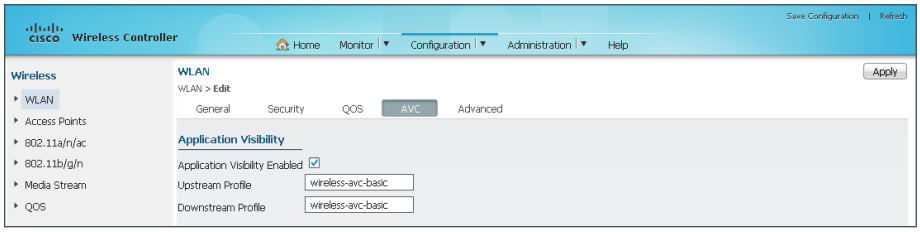
Step 6: On the Security Tab, navigate to AAA Server, and then choose the RADIUS authentication and accounting method lists that you created in Procedure 3, and then click **Apply**.



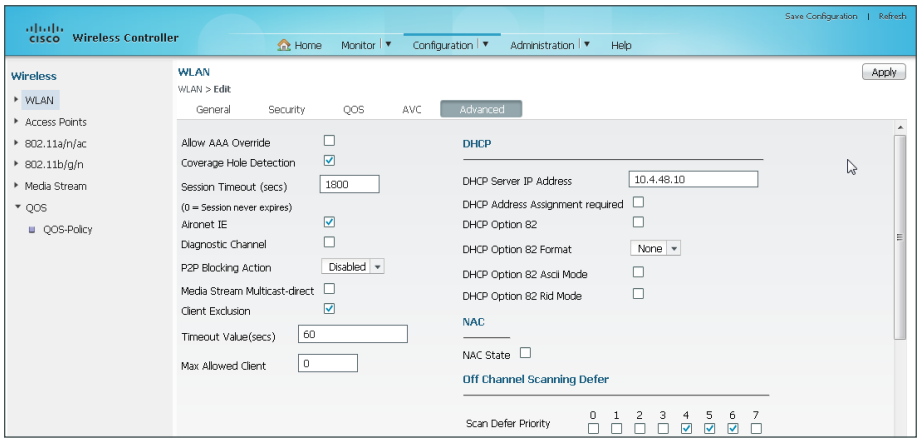
Reader Tip

Precious metal QoS policies (platinum, gold, silver and bronze) will be applied using CLI for the three SSIDs supported in this guide after each of the WLANs (Voice, Data, Guest) have been created. The use of the precious metal named QoS policies on the Cisco 5760 Series WLC aligns to those which already exist on the Cisco AireOS based controllers. The Cisco IOS-XE based controllers offer modular Quality of Service CLI (MQC) mechanisms that provide greater flexibility with regard to QoS. Depending on the requirements, MQC may provide advantages over the precious metal based QoS.

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



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**



The preceding steps apply this configuration.

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

Example

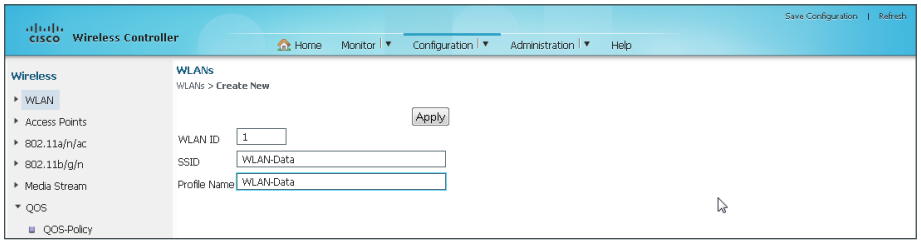
```
wlan Voice 2 WLAN-Voice
 accounting-list ISE-Accounting-Method-List
 client vlan WLAN-Voice
 ip flow monitor wireless-avc-basic input
 ip flow monitor wireless-avc-basic output
 security dot1x authentication-list ISE-Authentication-Method-List
 session-timeout 1800
 no shutdown
```

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**.

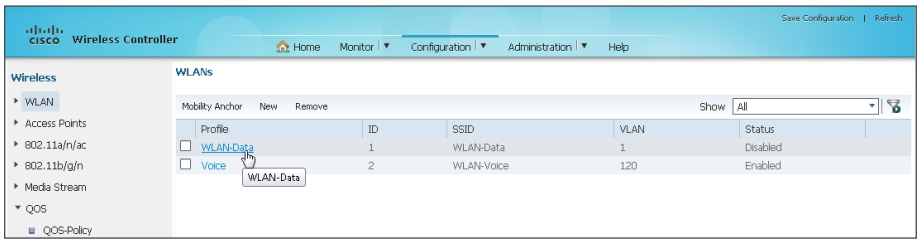


The preceding steps apply this configuration.

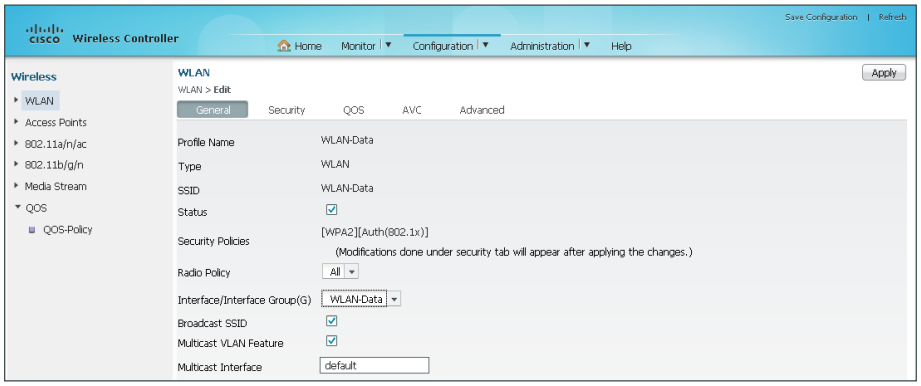
```
wlan [Profile Name] [WLAN ID] [SSID]
 shutdown
```

Next, configure the specific parameters of the Data WLAN.

Step 3: Click the profile name you just created.



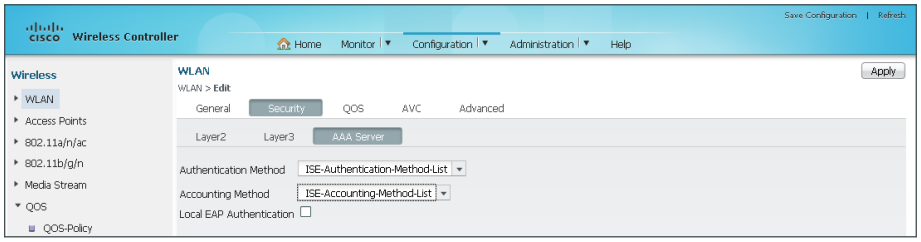
Step 4: On the General Tab for the Wireless Data WLAN, from the menu, choose the WLAN-Data interface, and then select both **Multicast VLAN Feature** and **Status**, then click **Apply**. This enables multicast and the WLAN.



The preceding steps apply this configuration.

```
wlan [Profile Name] [WLAN ID] [SSID]
 client vlan [VLAN Name]
 no shutdown
```

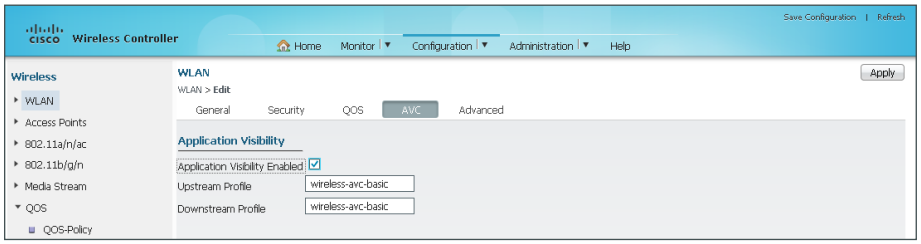
Step 5: On the Security Tab, navigate to AAA Server, select the RADIUS authentication and accounting method lists created in Procedure 3 then click **Apply**.



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]
```

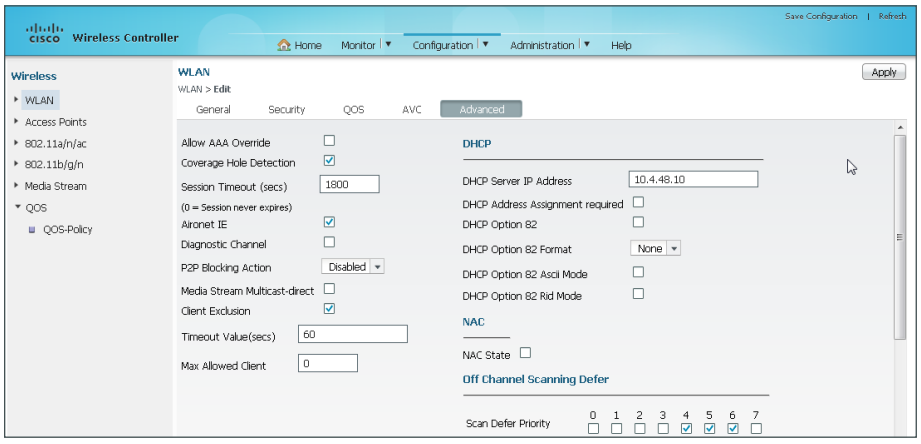
Step 6: On the AVC tab, select **Application Visibility Enabled** and then click **Apply**. This enables Application Visibility and Control.



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**.



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.

Table 12 - QoS precious metal to WLAN mapping

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

Tech Tip

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
```

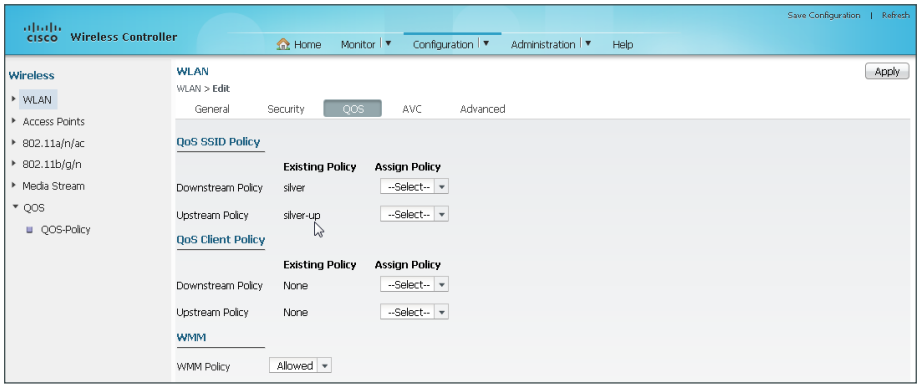
Step 6: Verify that the service policies have been applied to the WLANs by entering the following command and noting the QoS service policy.

```
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

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.

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.



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

Enabling 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-select
Band Select Probe Response    : per WLAN enabling
Cycle Count                   : 2
Cycle Threshold (millisec)    : 200
Age Out Suppression (sec)     : 20
Age Out Dual Band (sec)       : 60
Client RSSI (dBm)             : -80
5760-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#
```

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

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

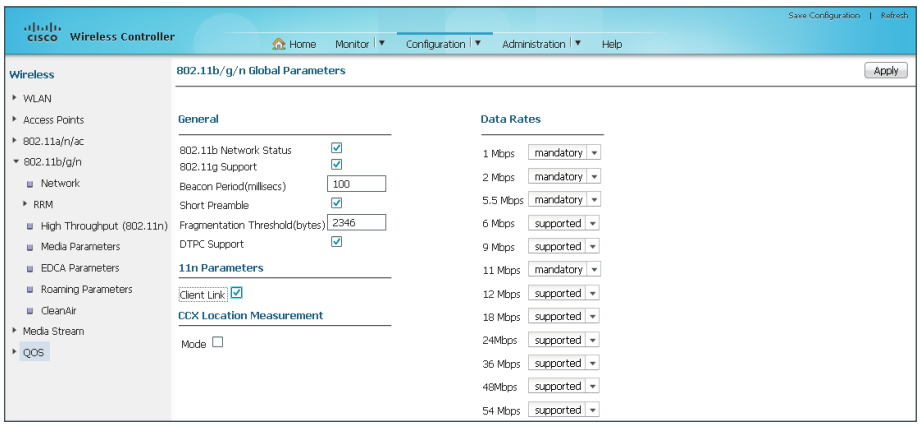
Step 5: Enable Band Select on the Data WLAN by first disabling the WLAN, and then enabling band-select and re-enabling the WLAN.

```
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.

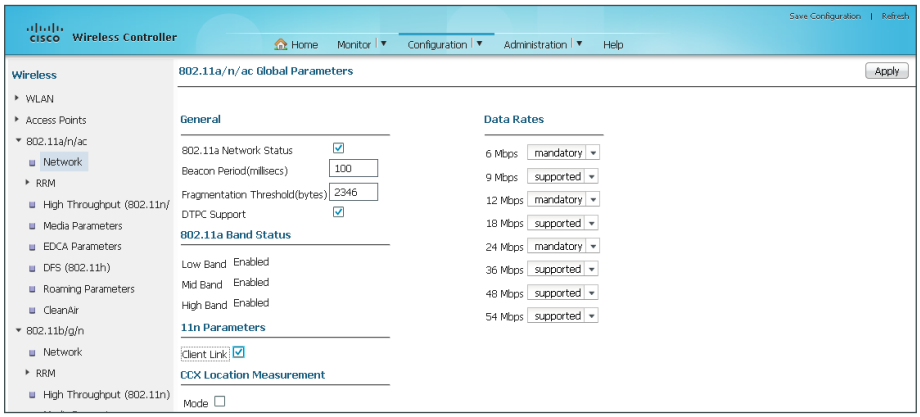
Step 6: If you are using Generation 1 access points and need to enable Cisco Client Link version 1.0., navigate to **Configuration > Wireless > 802.11b/g/n >Network >11n Parameters** and enable Client Link 1.0 by selecting the Client Link option, and then clicking **Apply**.



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**.



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
```

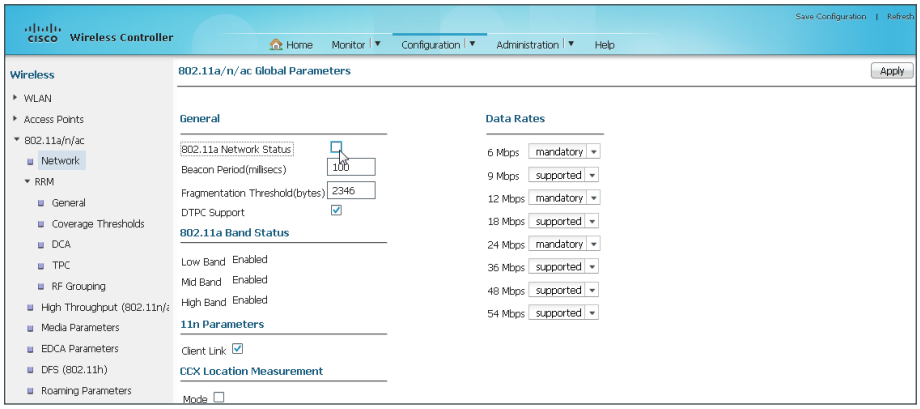
Procedure 11 Enable 802.11ac on the Cisco 5760 Series WLC

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.

Tech Tip

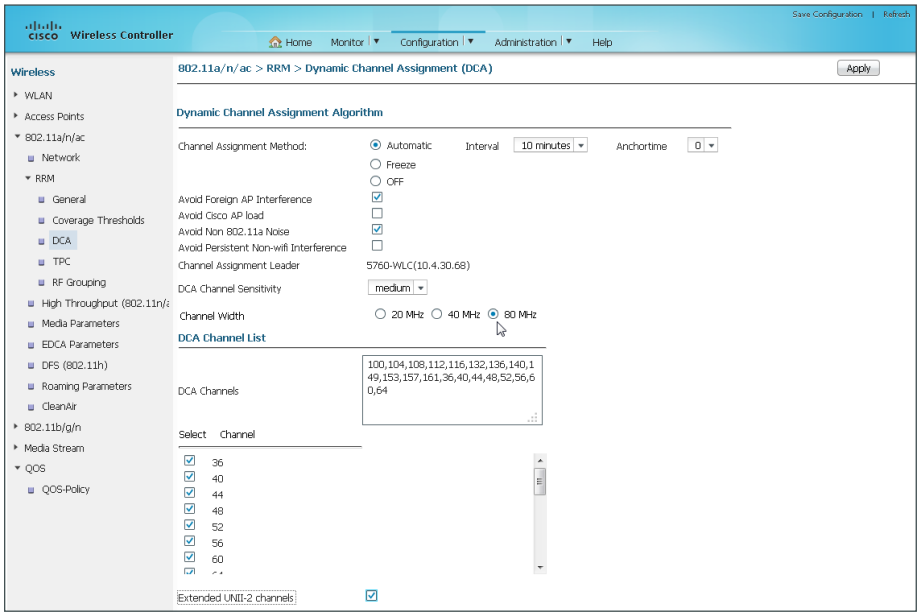
For more information on channel assignment, please read the 802.11ac section in the introductory section of this guide before completing the following procedure. Note that changing the default channel width for 802.11ac capable access points will require the 802.11a network to be disabled and is therefore disruptive.

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**.

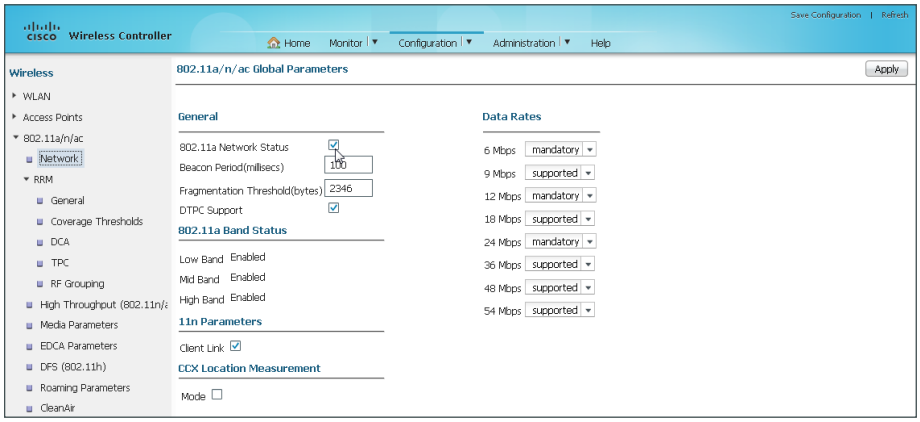


Step 2: Navigate to **Configuration > Wireless > 802.11a/n/ac > RRM > DCA** and select the desired Channel Width to use (Example: 20 MHz, 40 MHz, 80 MHz).

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



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**.



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
!
ap dot11 5 GHz shutdown
!
!add the UNII-2 Channels
!
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
!
ap dot11 5 GHz rrm channel dca chan-width 80
!
! Configure supported and mandatory data rates
!
```

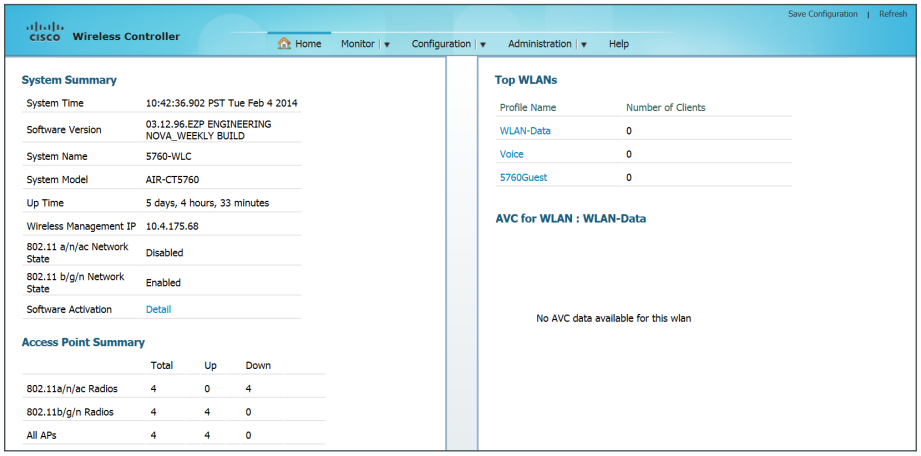
```
ap dot11 5 GHz rate RATE_6M mandatory
ap dot11 5 GHz rate RATE_9M supported
ap dot11 5 GHz rate RATE_12M mandatory
ap dot11 5 GHz rate RATE_18M supported
ap dot11 5 GHz rate RATE_24M mandatory
ap dot11 5 GHz rate RATE_36M supported
ap dot11 5 GHz rate RATE_48M supported
ap dot11 5 GHz rate RATE_54M supported
ap group default-group
!
! Enable the 5 GHz network
!
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)

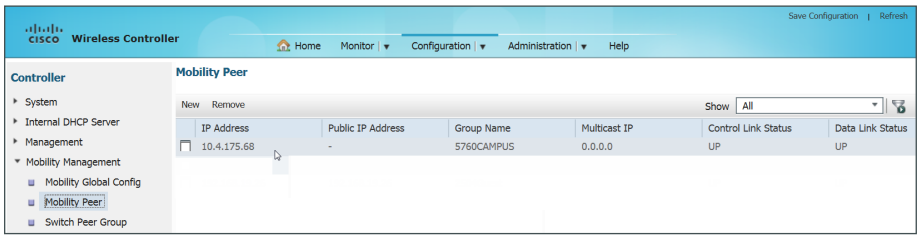
You need to complete this procedure if you have a Cisco IOS-XE 5760 based controller that is providing wireless guest services to your enterprise, and acting as a foreign anchor controller. As a foreign anchor controller, the first step is to create the mobility peers to the DMZ-based Internet edge anchor 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)



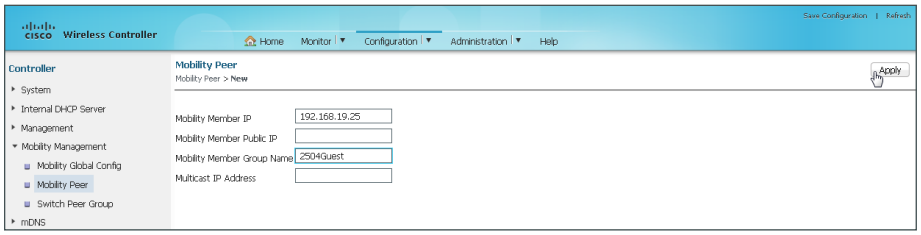
Next, create a new mobility peer to the DMZ-based Cisco 2504 Series anchor controllers.

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



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**.

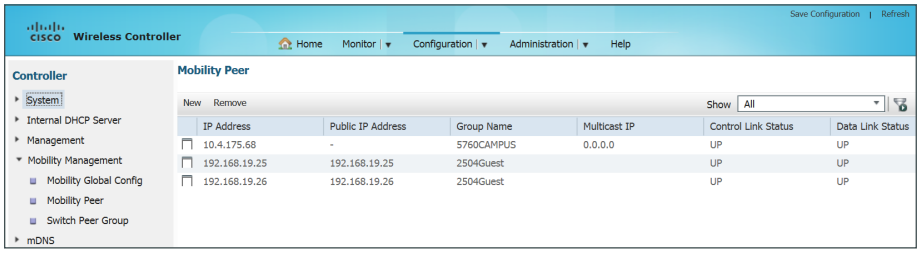


The preceding steps apply this configuration.

```
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.



Tech Tip

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

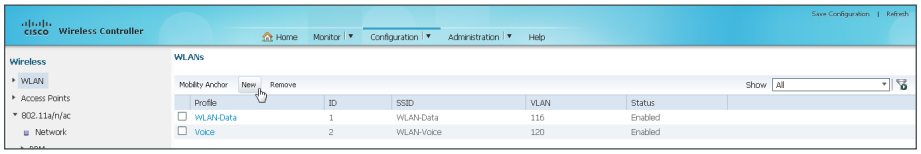
```
wireless mobility group member ip 192.168.19.25 public-ip 192.168.19.25 group 2504Guest
wireless mobility group member ip 192.168.19.26 public-ip 192.168.19.26 group 2504Guest
```

Procedure 13 Configure the guest WLAN on IOS-XE controllers

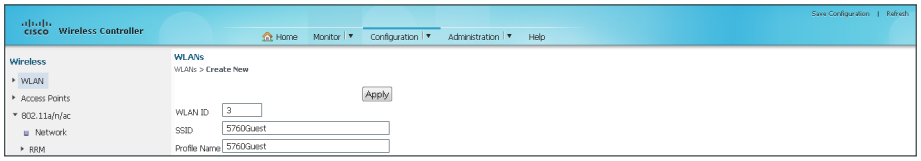
Step 1: Access the SSL-based web Interface of the Cisco 5760 Series WLC foreign anchor controller by using your browser. (Example: https://10.4.175.68/wireless)

Next, create a guest wireless LAN.

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



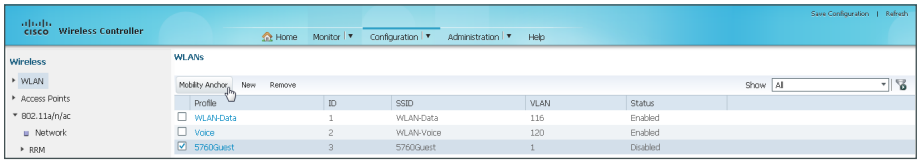
Step 3: In the **WLANs > Create New page**, enter a unique WLAN ID (Example: **3**), the **Guest Wireless SSID** (Example: **5760Guest**), and the **Profile Name** (Example: **5760Guest**), and then click **Apply**.



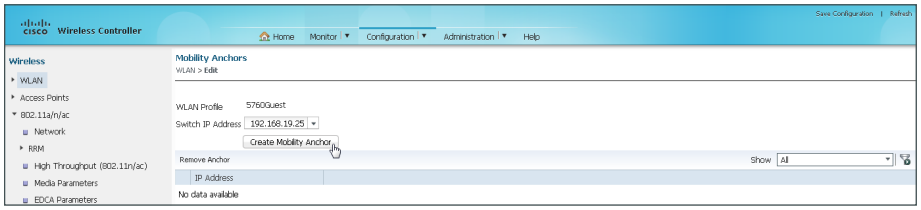
The preceding steps apply this configuration.

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

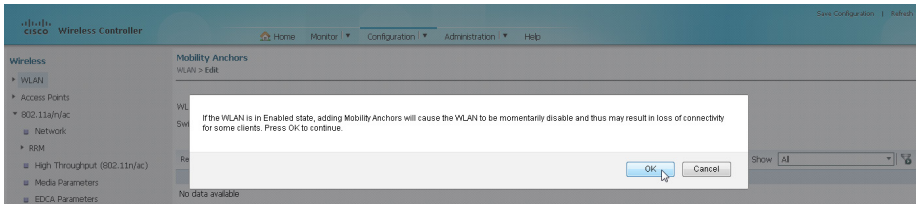
Step 4: Select the check box for the Guest WLAN, and then click **Mobility Anchor**.



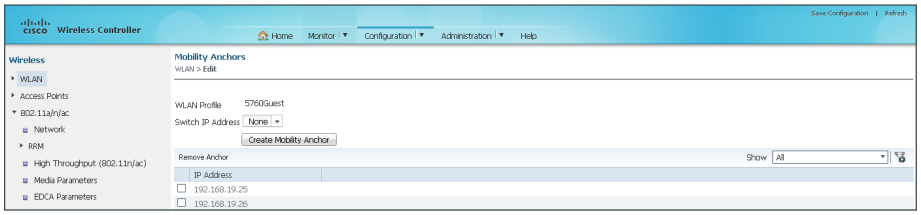
Step 5: In the **Switch IP Address** list, choose one of the Guest Anchor Controllers configured in the Internet DMZ, and then click **Create Mobility Anchor**.



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.



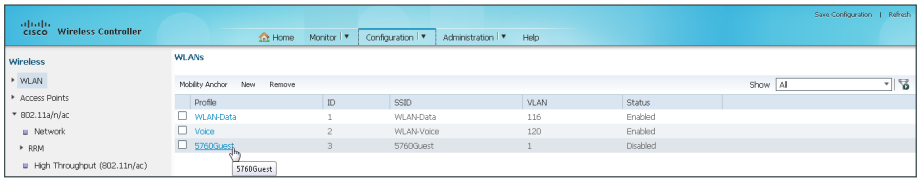
Step 7: If you have two anchor controllers in the DMZ, repeat Step 1 through Step 6 for the second guest anchor controller.



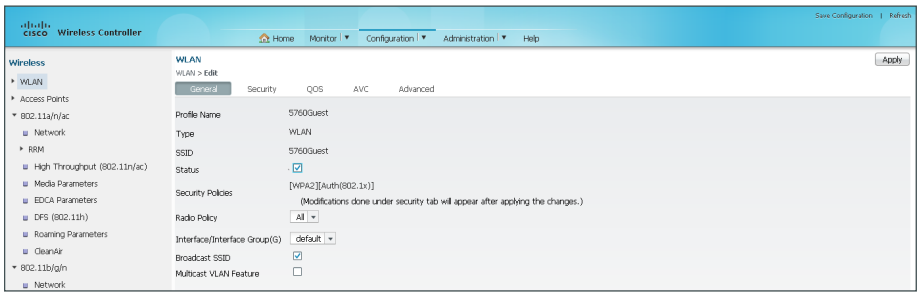
The preceding steps apply this configuration.

```
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)



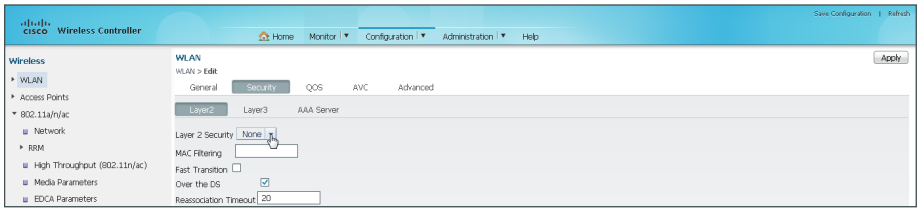
Step 9: On the General tab, select **Status**. This enables the WLAN.



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

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

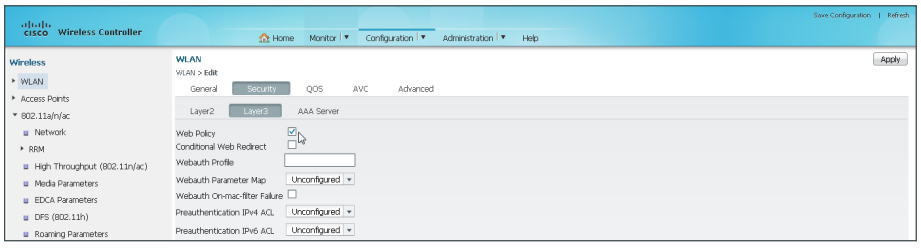
Step 10: Click the **Security** tab, and then, on the Layer 2 tab, in the **Layer 2 Security** list, choose **None**.



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.



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

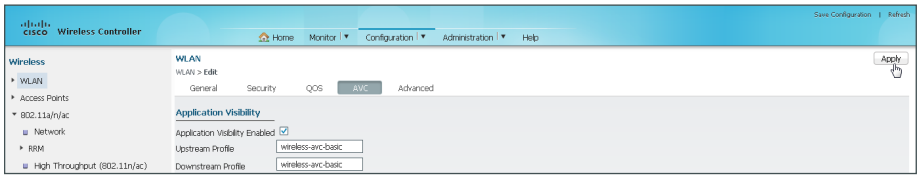
```
wlan [Profile Name] [WLAN ID] [SSID]
 security web-auth
```

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
```

PROCESS

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.

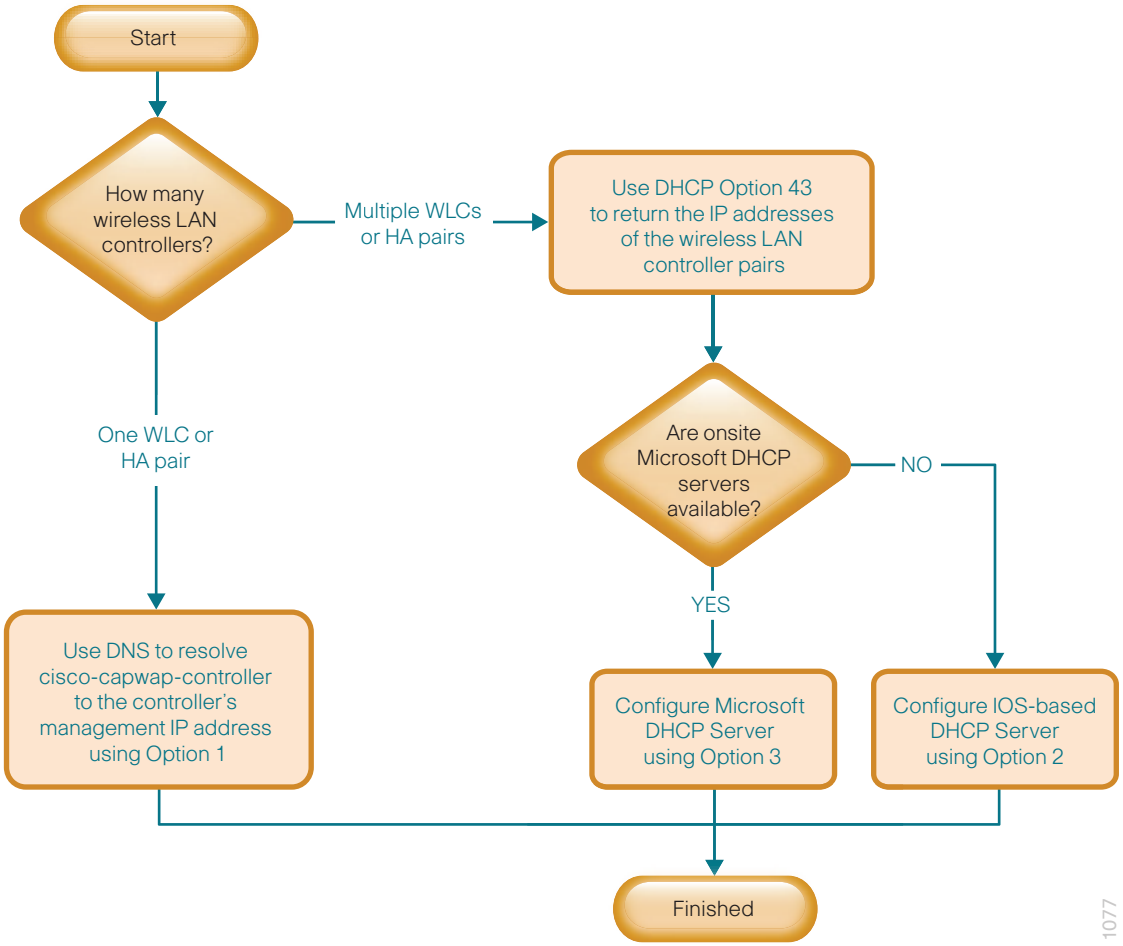
Procedure 1 Configure controller discovery

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.

Figure 10 - Flow chart of WLC discovery configuration options



Option 1: Only one WLC pair in the organization

Step 1: Configure the organization's DNS servers (Example: 10.4.48.10) to resolve the **cisco-capwap-controller** host name to the management IP address of the controller (Example: 10.4.175.64). 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.

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

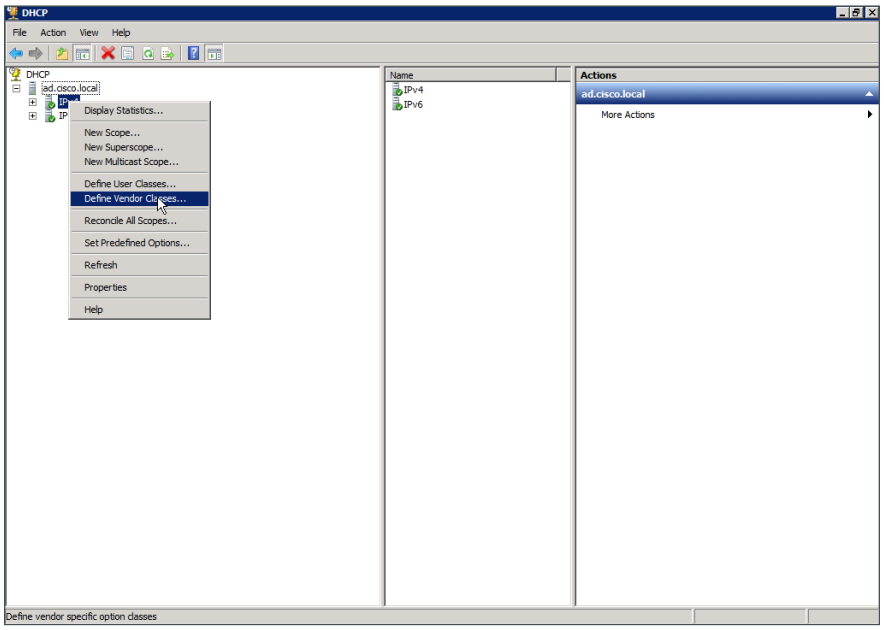
This procedure shows how the Microsoft DHCP server is configured in order to return vendor-specific information to the lightweight Cisco Aironet 1600, 2600, 3600 and 3700 Series Access Points used in this design guide. The vendor class identifier for a lightweight Cisco Aironet access point is specific to each model type. To support more than one access point model, you must create a vendor class for each model type.

Table 13 - Vendor class identifiers

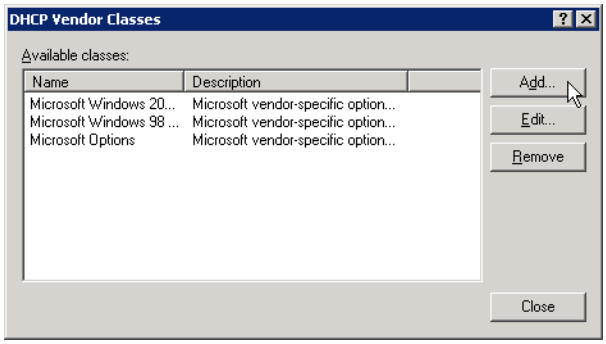
Access point	Vendor class identifier
Cisco Aironet 1600 Series	Cisco AP c1600
Cisco Aironet 2600 Series	Cisco AP c2600
Cisco Aironet 3600 Series	Cisco AP c3600
Cisco Aironet 3700 Series	Cisco AP c3700

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

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



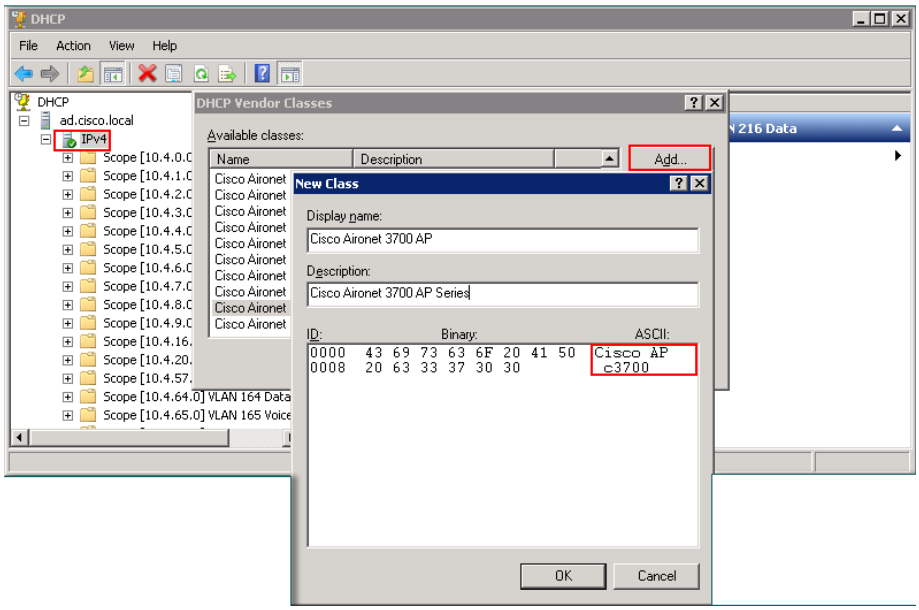
Step 3: In the DHCP Vendor Classes dialog box, click **Add**.



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

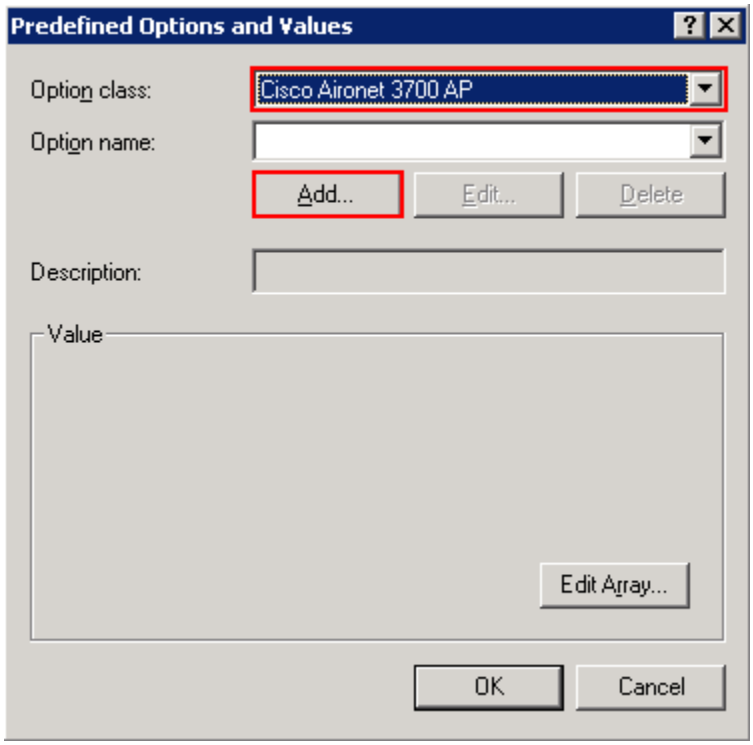
Step 5: In the ASCII section, enter the vendor class identifier for the appropriate access point series from Table 13, and then click **OK**. (Example: Cisco AP c3700)

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



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**.

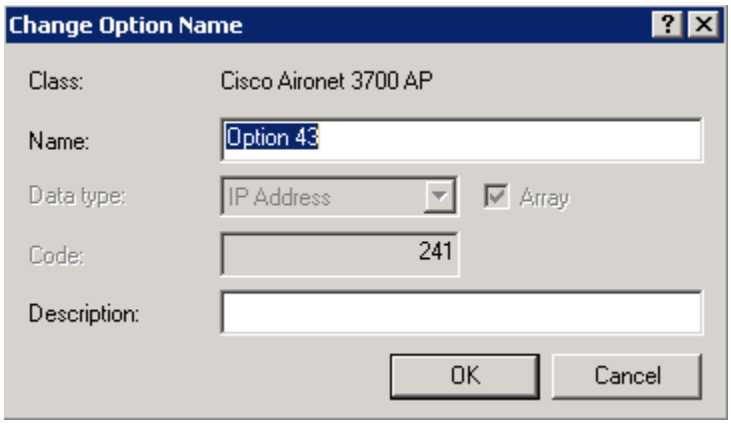


Step 9: In the Option Type dialog box, enter a **Name**. (Example: Option 43)

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**.



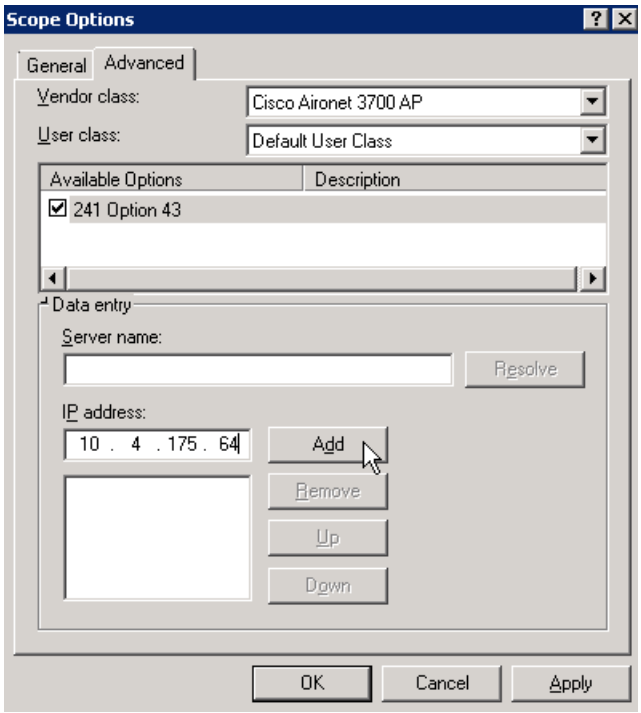
The vendor class and suboption are now programmed into the DHCP server. Now, you need to define the vendor-specific information for the DHCP scope.

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)



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)

Step 4: Click **Save Configuration**.

PROCESS

Configuring Remote-Site Wireless with Cisco FlexConnect

1. Install the Cisco vWLC for FlexConnect designs
2. Configure the console port on the vWLC
3. Configure the vWLC network adapters
4. Configure the data center switches for the Cisco Flex 7500 Series WLC
5. Configure the LAN distribution switch
6. Connect the redundancy port
7. Configure the WLC platform
8. Configure the time zone
9. Configure SNMP
10. Limit which networks can manage the WLC
11. Configure wireless user authentication using Cisco ISE
12. Configure management authentication using Cisco ACS
13. Configure the resilient WLC
14. Configure mobility groups
15. Configure the data wireless LAN
16. Configure the voice wireless LAN
17. Configure controller discovery
18. Configure the remote-site router
19. Configure the remote-site switch for APs
20. Enable licensing on the vWLC
21. Configure the AP for Cisco FlexConnect
22. Configure access points for resiliency
23. Configure Cisco FlexConnect groups
24. Enable 802.11ac using DCA on Cisco AireOS Flex Controllers

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.

Table 14 - Cisco remote-site wireless controller parameters checklist

Parameter	CVD values primary controller	CVD values resilient controller if not using HA SSO	Site-specific values
Controller parameters			
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)[1]	10.4.59.168	10.4.59.169	
Redundancy port connectivity (HA SSO)[1]	Dedicated Ethernet cable[1] Layer 2 network[2]	Dedicated Ethernet cable[1] Layer 2 network[2]	
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	

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			
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.

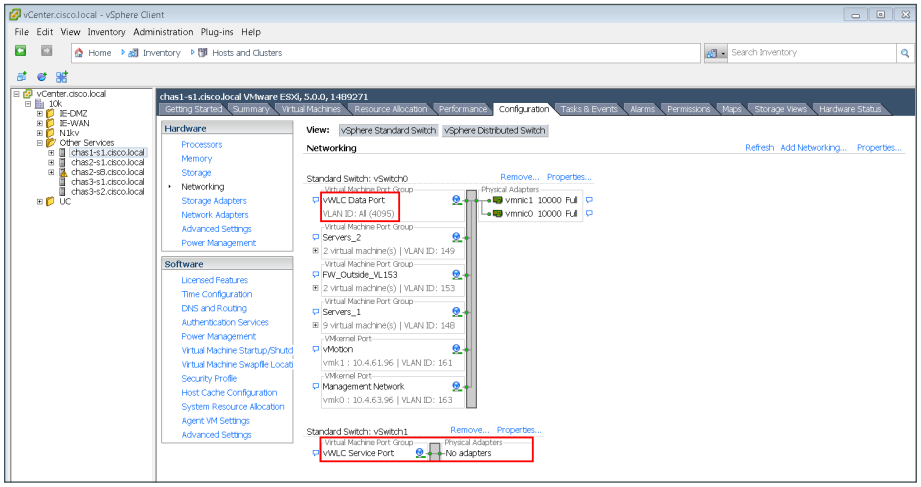
Tech Tip

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

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

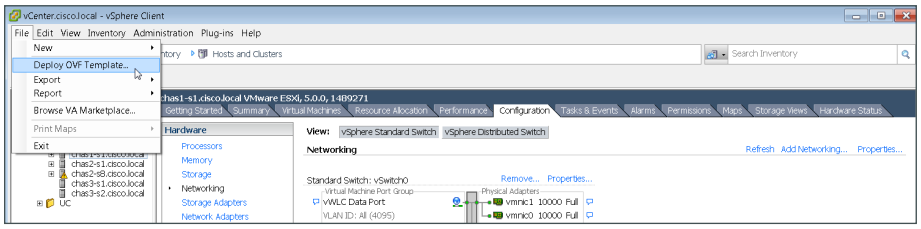
Step 1: Begin by preparing the VMware host machine networking environment. On the physical host machine, in vCenter, create two virtual switches (vSwitch0, and vSwitch1), as follows:

- 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.



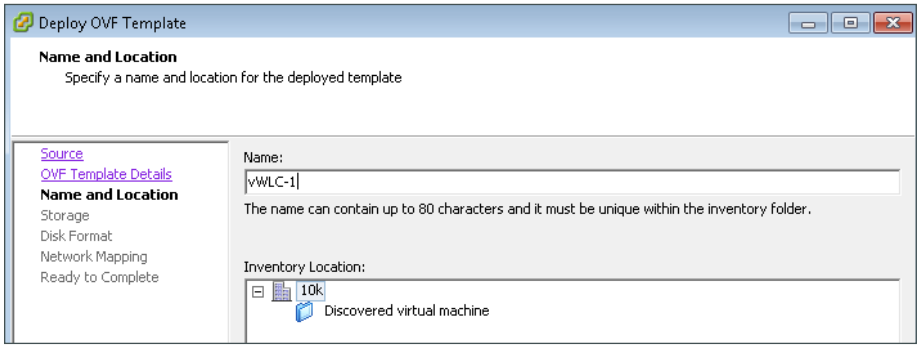
Next, install the Cisco vWLC OVA file obtained from Cisco.

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

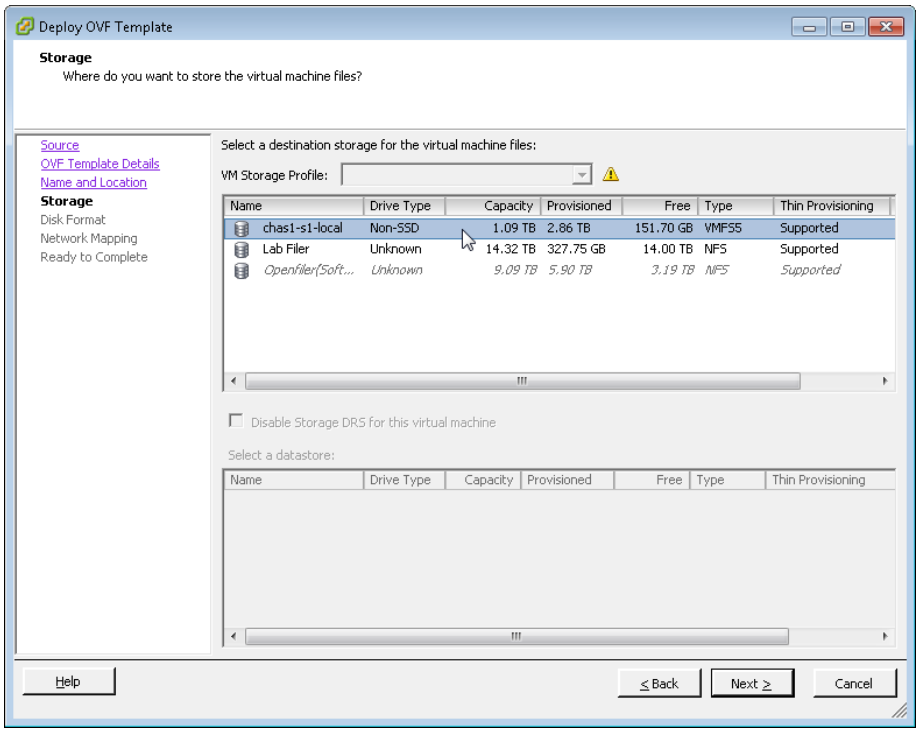


Step 3: Complete the Deploy OVF Template wizard. Note the following:

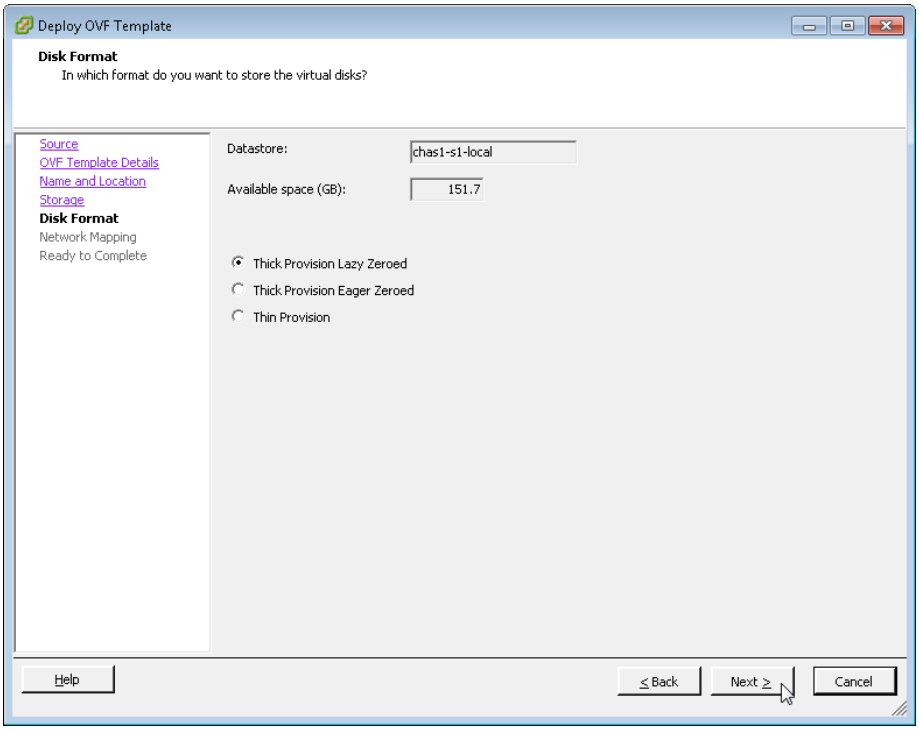
- On the Source page, select the downloaded Cisco vWLC OVA file that you obtained from Cisco.
- On the Name and Location page, provide a unique name for the virtual Wireless LAN controller. (Example: vWLC-1)



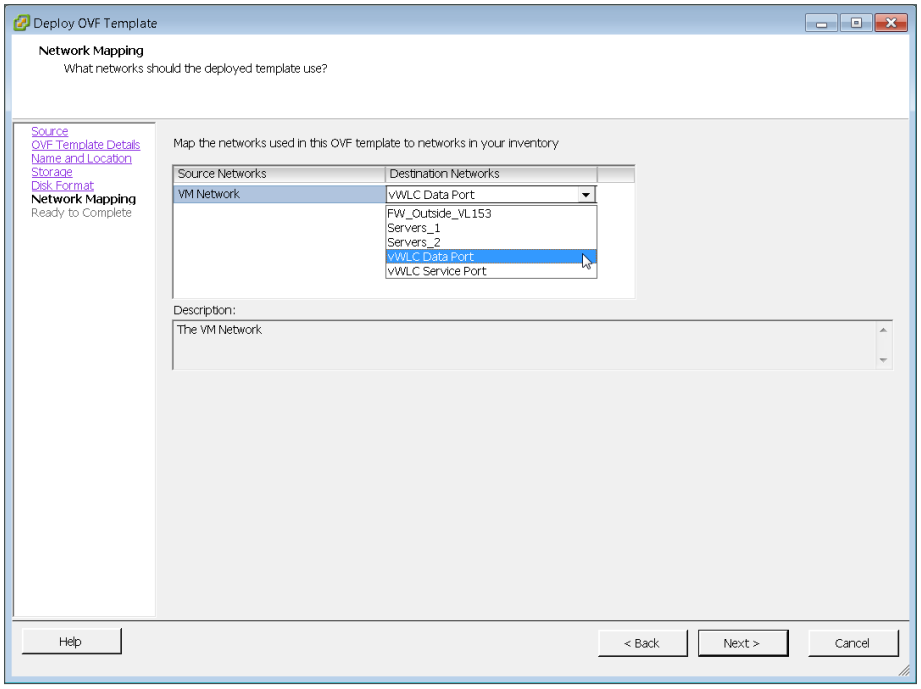
Step 4: On the Storage page, select the storage destination of the virtual machine.

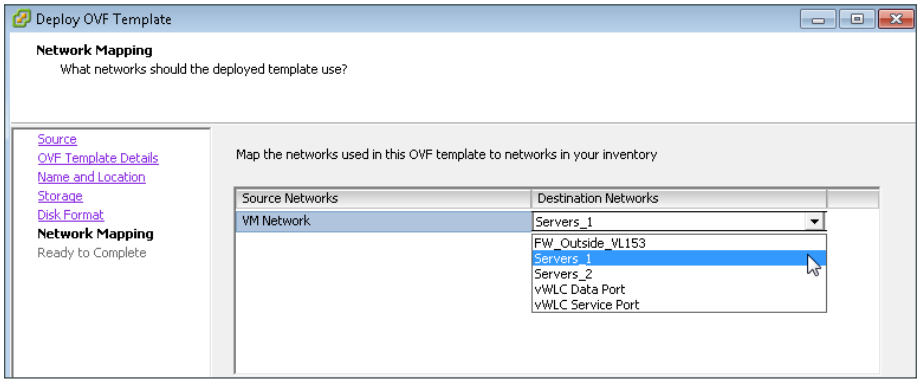


Step 5: On the Disk Format page, select **Thick Provision Lazy Zeroed**.

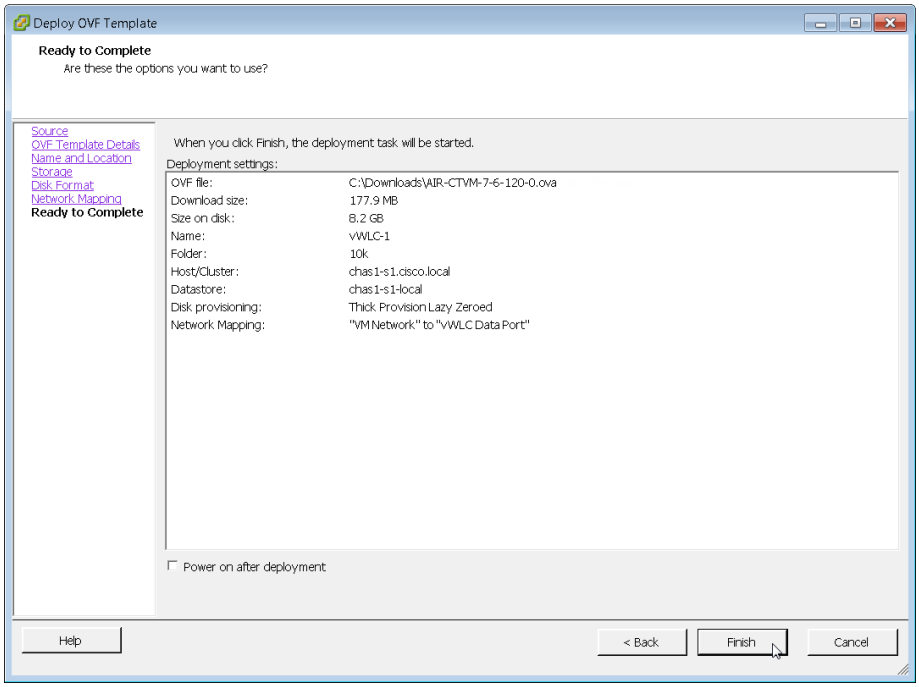


Step 6: On the Network Mapping page, in the **Destination Networks** list, choose the network defined on the VM host machine that will be used on the vWLC management interface. (Example: vWLC Data Port)





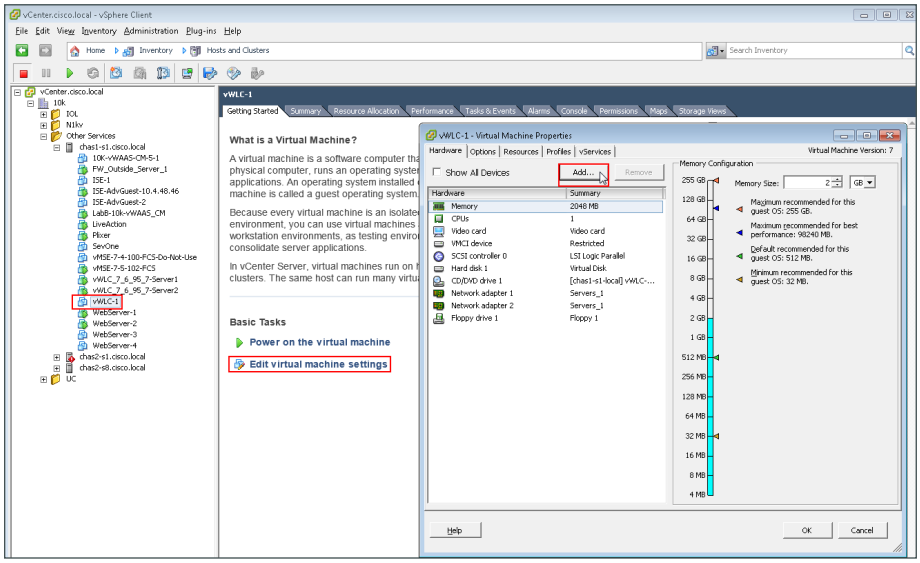
Step 7: On the Ready to Complete page, review the settings, and then click **Finish**. Deployment of the OVA file begins, and it may take a few minutes to complete.



Procedure 2 Configure the console port on the vWLC

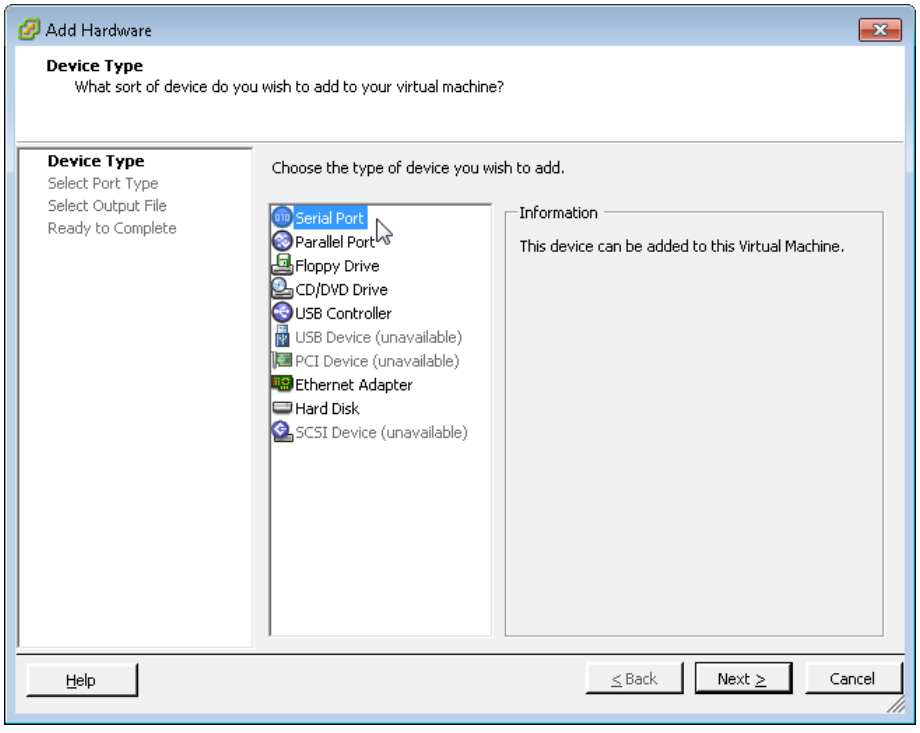
When the Cisco vWLC starts, the console tab within vSphere will display a repetitive message stating to press any key in order to make the Console tab the default terminal for console messages from the vWLC. If a key is not pressed during the vWLC startup, console communication to the vWLC through the 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**.

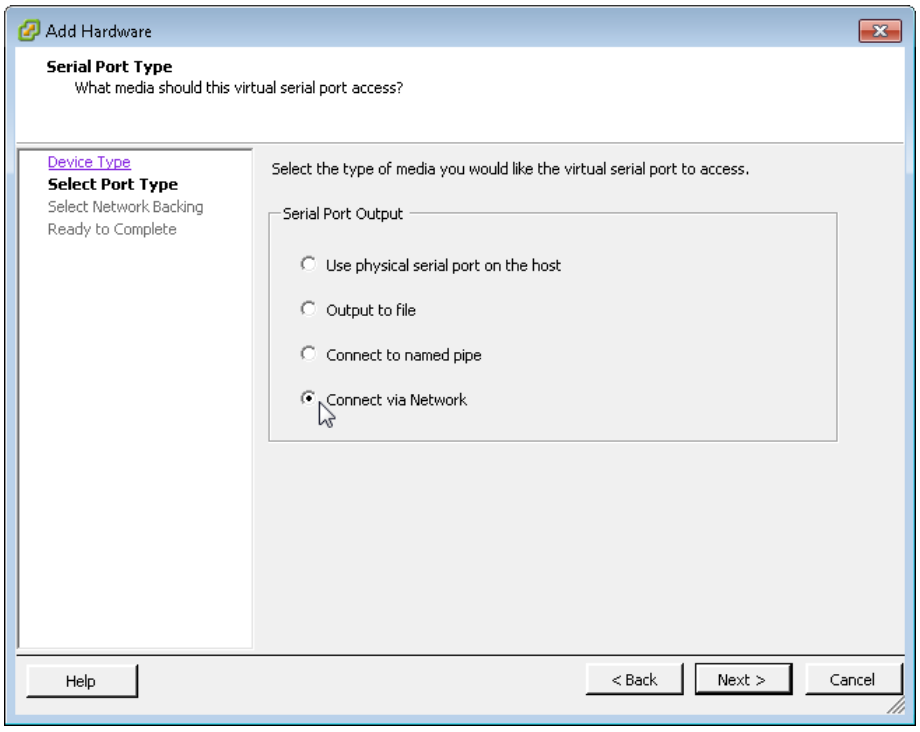


Step 2: Complete the Add Hardware wizard. Note the following:

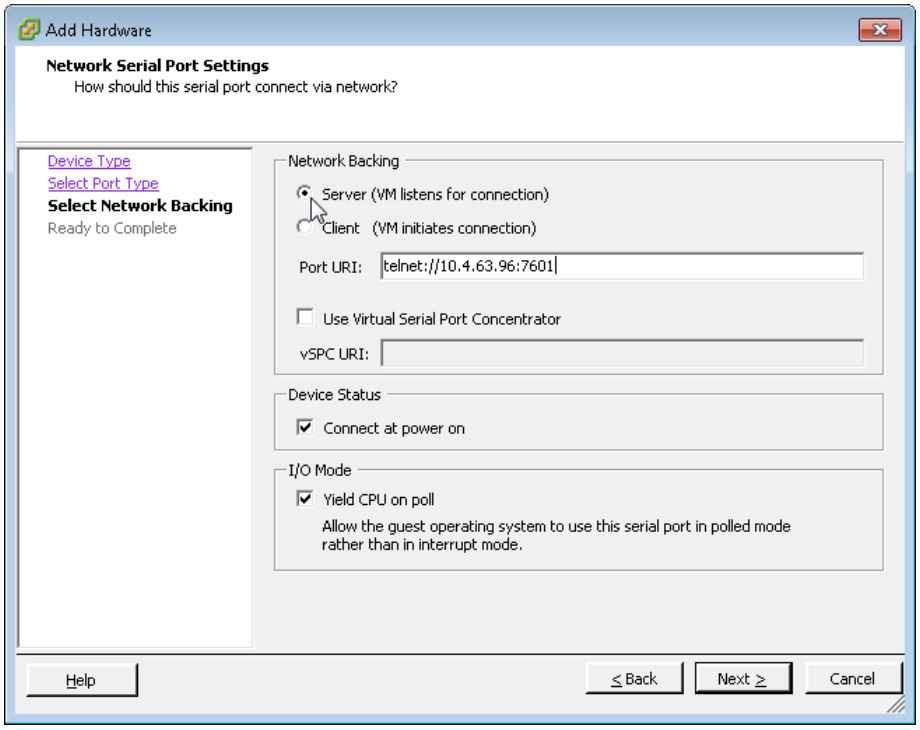
- On the Device Type page, select **Serial Port**.



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

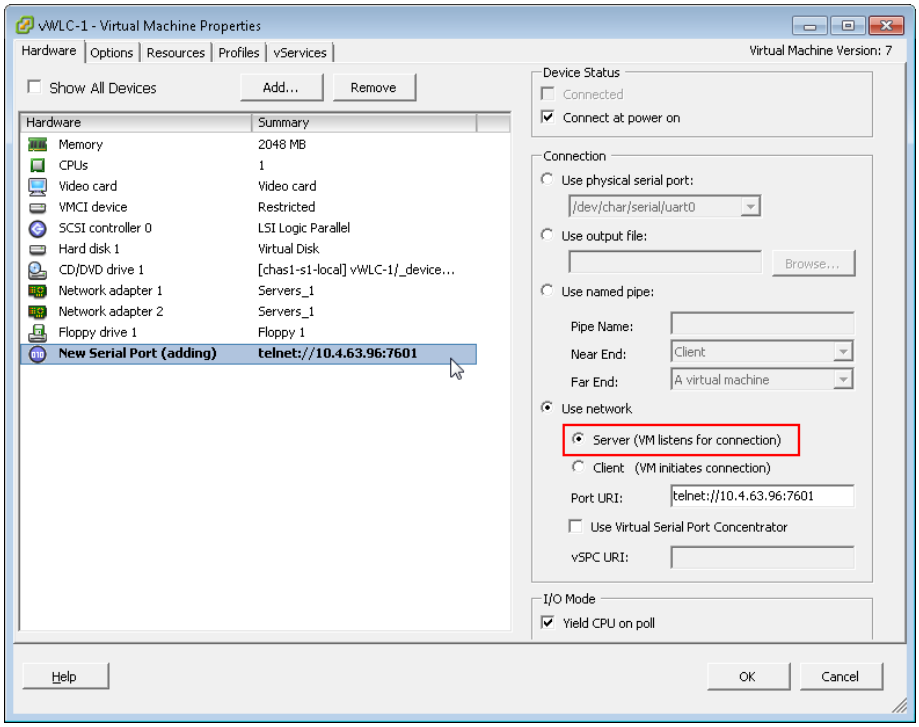


- On the Network Backing page, select **Server (VM listens for connection)**, and then in the **Port URI** box, enter **telnet://[Host Machine IP Address]:[Unique TCP Port]**. (Example: telnet://10.4.63.96:7601) This configures IP address and TCP port number that are used access the console port via Telnet.



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

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

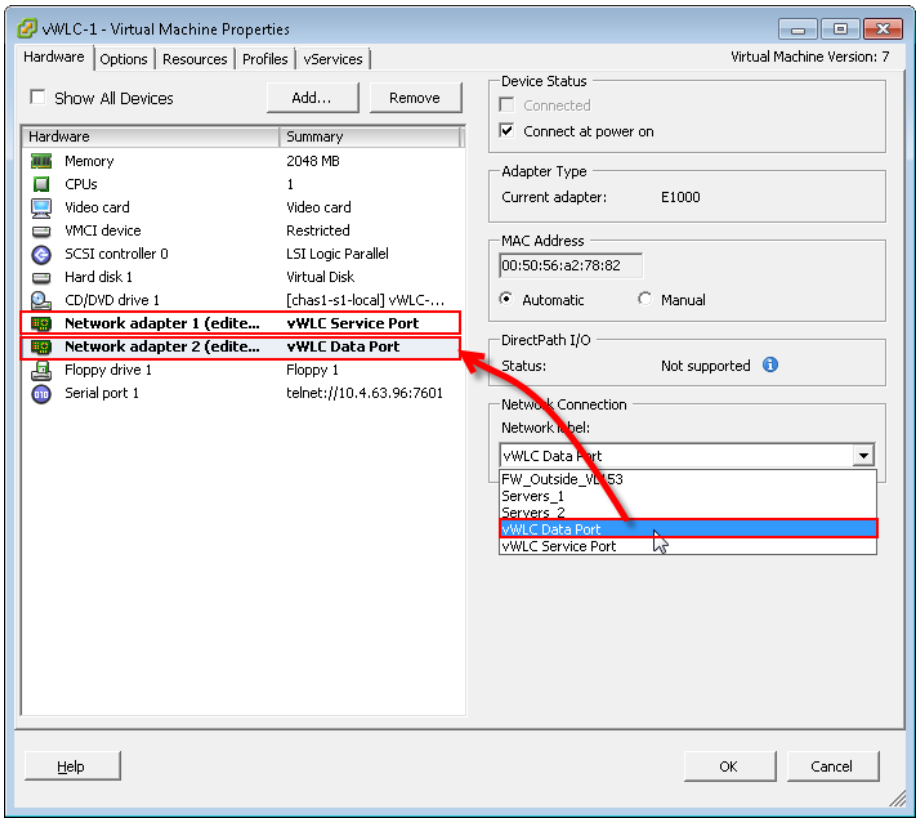


Procedure 3 Configure the vWLC network adapters

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

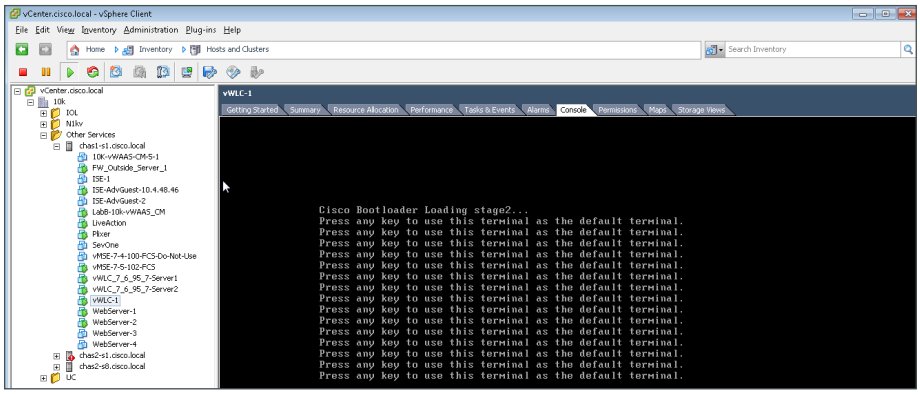
Step 1: In the Virtual Machine Properties dialog box, select **Network adapter 1**, and then in the **Network label** list, choose **vWLC Service Port**.

Step 2: Select **Network adapter 2**, and in the **Network label** list, choose **vWLC Data Port**, and then click **OK**.



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.

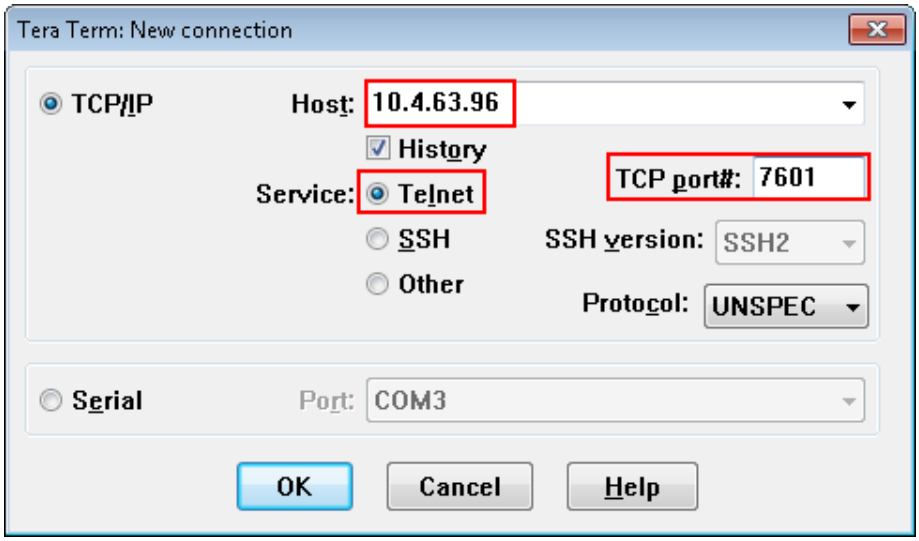
Within the Console tab you are prompted to "Press any key to use this terminal as the default terminal." However, you do not need to press any key because access via the serial port that was created in Procedure 2 will be used.



Tech Tip

In the event that you are unable to use Telnet to connect to the serial port defined for the vWLC, you can restart the 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.



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.

Procedure 5 Configure the LAN distribution switch

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

```
vlan 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
```

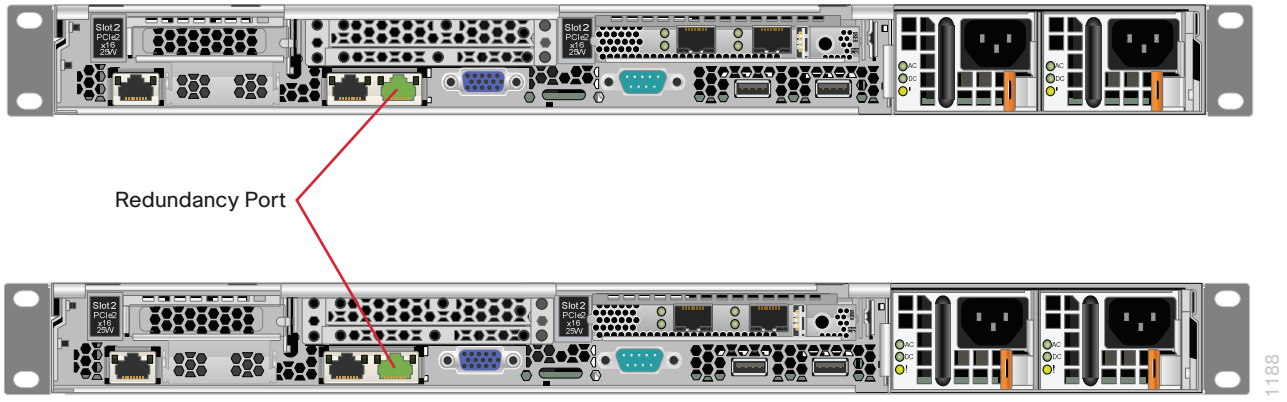
If you are deploying a Cisco 5500 Series Wireless LAN Controller, configure at least two distribution switch interfaces as an EtherChannel trunk.

```
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
!
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

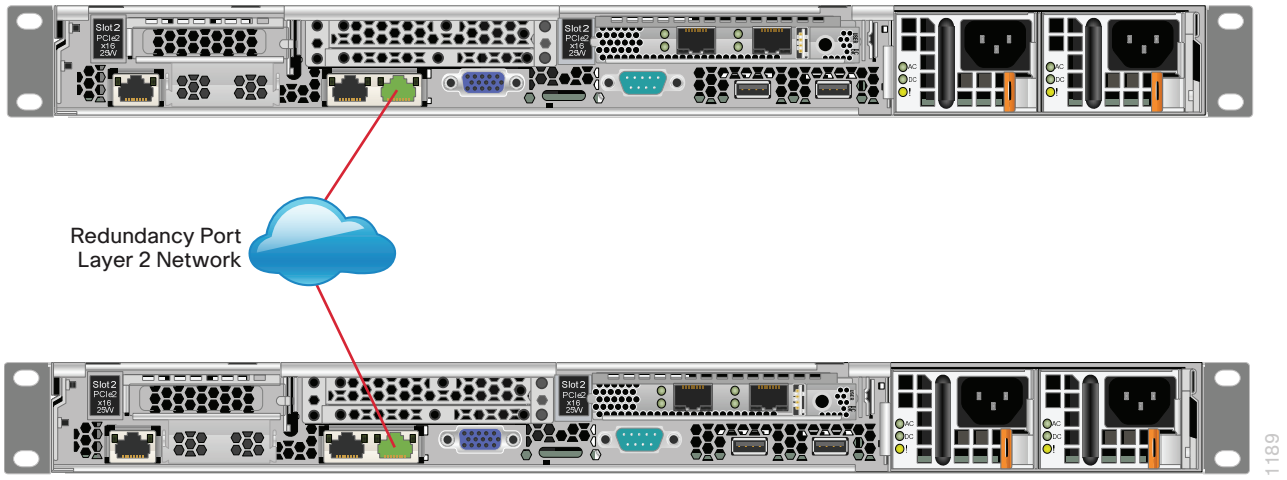
If you are using a Cisco vWLC, skip this procedure. If you are using a Cisco Flex 7500 Series WLC and you wish to enable the HA SSO feature, continue with this procedure. When using the high availability feature known as Stateful Switchover (HA SSO), a dedicated special-purpose port is available on the 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.



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

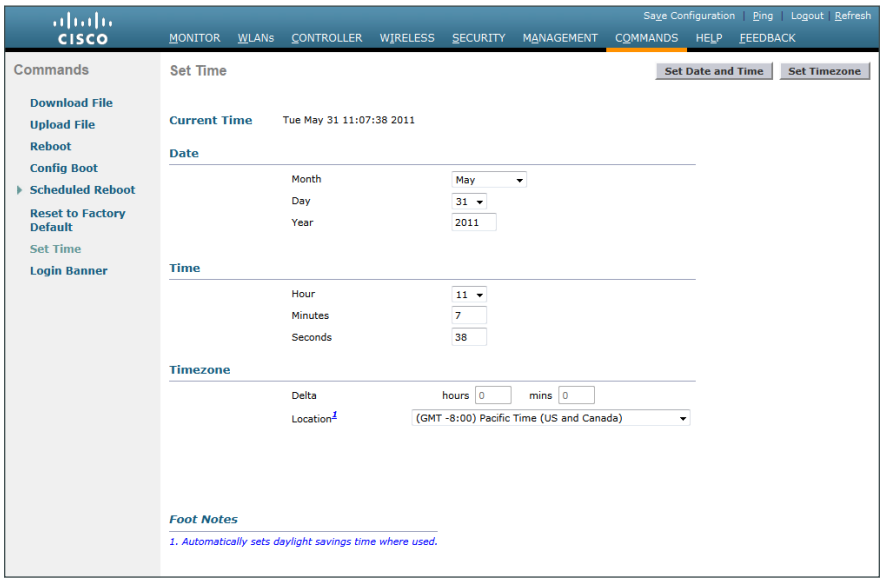
Configuring the time and date of the WLC is critical, because certificate validation is performed using the date/time as configured on the WLC. Improper date/time may prevent access points from successfully registering with the WLC. Verify the proper data and time is obtained from the NTP server as configured 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/)

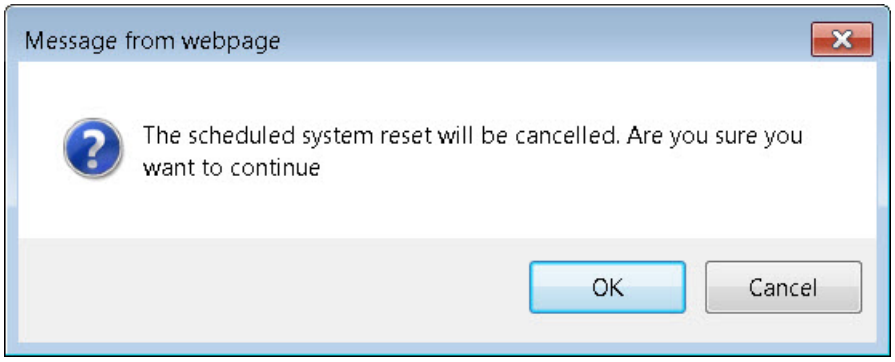
Step 2: Navigate to **Commands > Set Time**.

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

Step 4: Click **Set Time zone**.



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

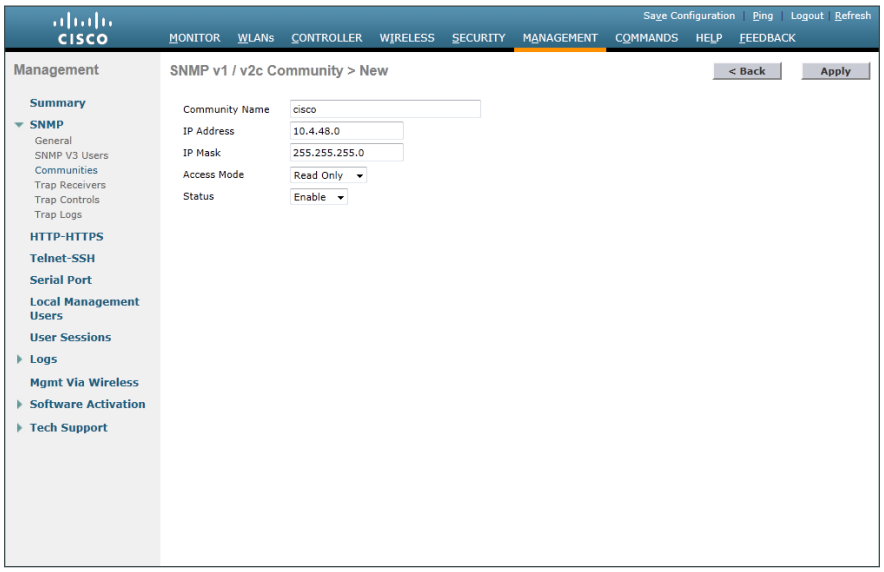
Step 1: In **Management > SNMP > Communities**, click **New**.

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)

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



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

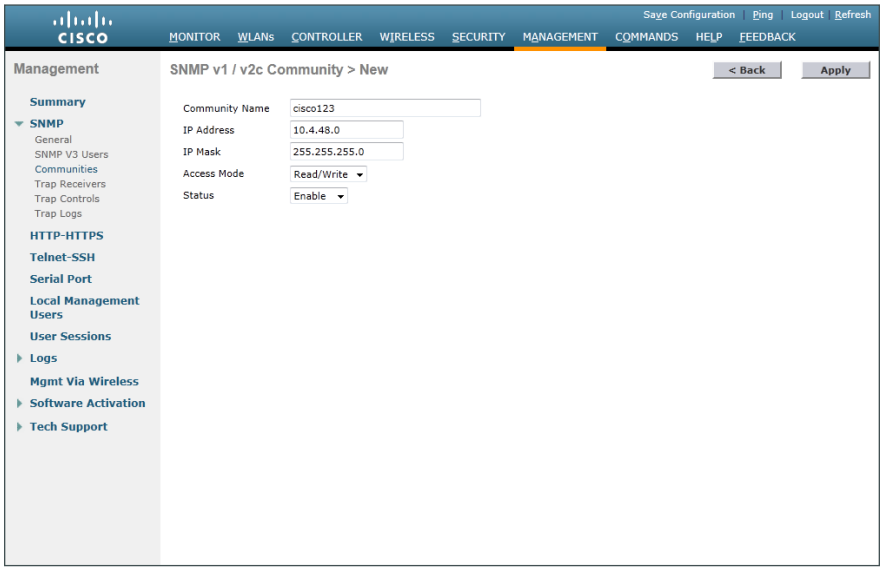
Step 7: Enter the Read/Write **Community Name**. (Example: cisco123)

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**.

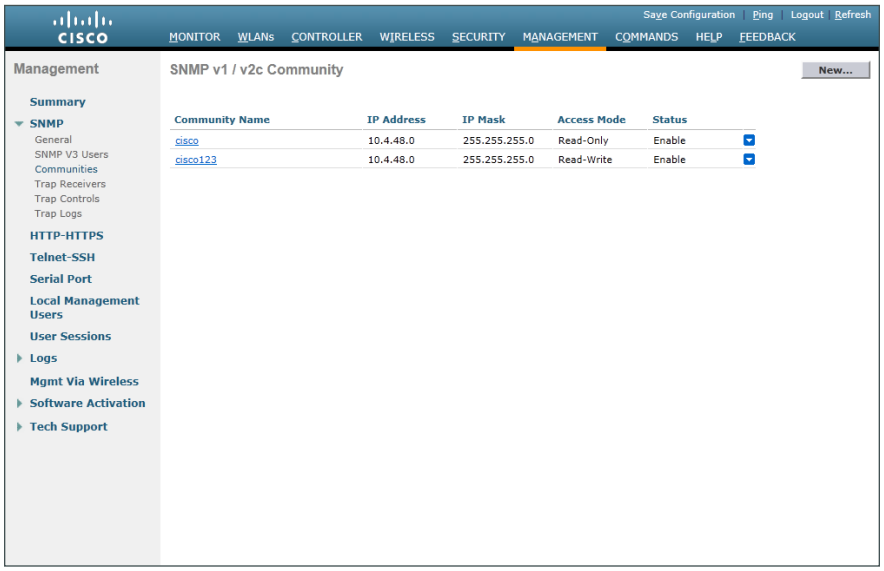
Step 11: In the **Status** list, choose **Enable**, and then click **Apply.**



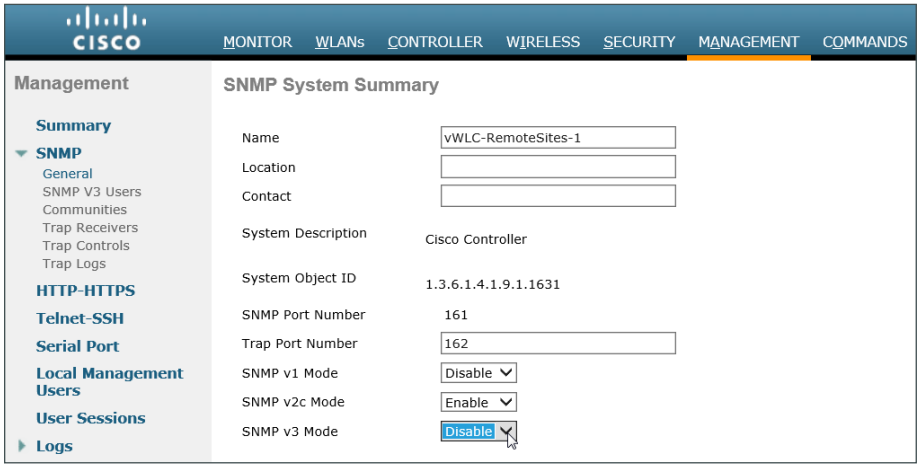
Step 12: Navigate to **Management > SNMP > Communities**.

Step 13: On the right side of the **public** community, point and click the blue down arrow, and then click **Remove**. 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.

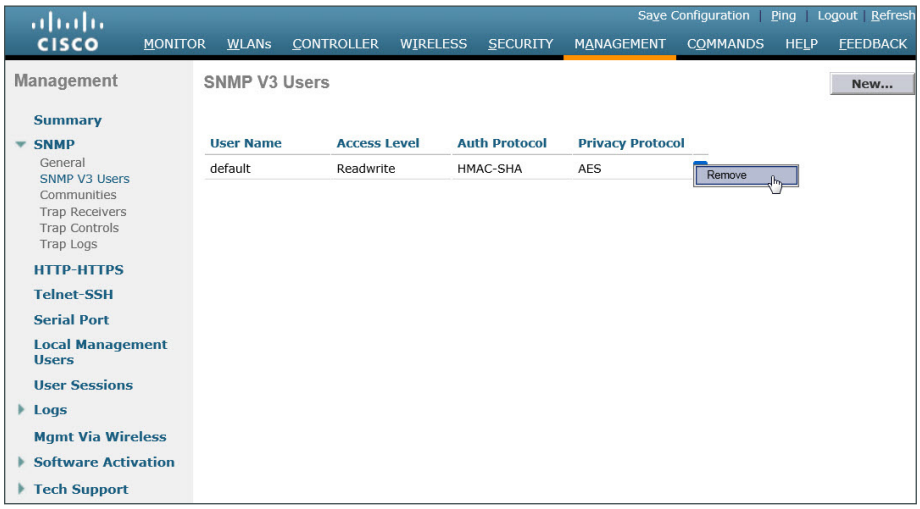


Step 15: Navigate to **Management > SNMP > General** and disable SNMP v3 Mode, then press **Apply**.

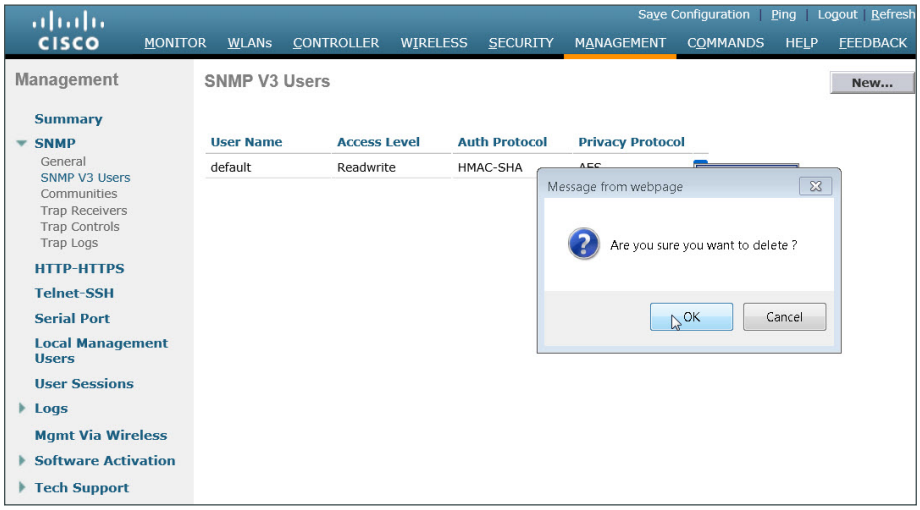


Step 16: Navigate to **Management > SNMP Communities > SNMP V3 Users**

Step 17: On the right side of the **default** User Name, point and click the blue down arrow, and then click **Remove**



Step 18: Press **OK** to confirm that you are sure you want to delete, then press **Save Configuration**



Tech Tip

Changes to the SNMP configuration may sometimes require that the WLC be rebooted.

Procedure 10 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 SSH or HTTPS.

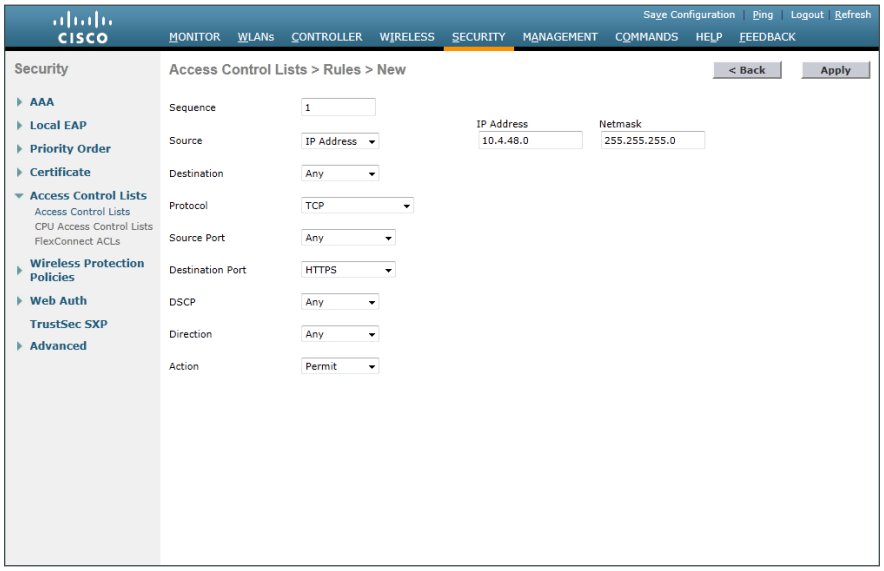
Step 1: In **Security > Access Control Lists > Access Control Lists**, click **New**.

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

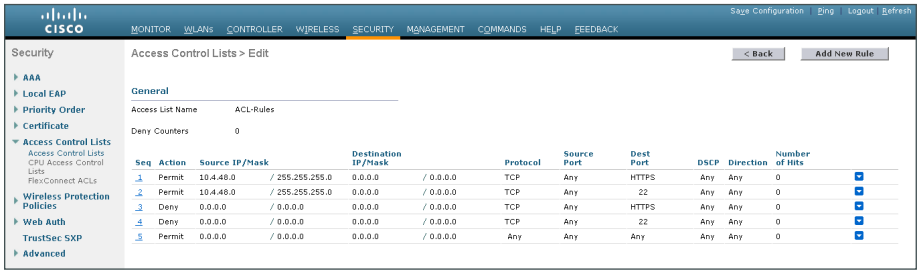
- Sequence—1
- Source—IP Address—**10.4.48.0 / 255.255.255.0**
- Destination—**Any**
- Protocol—**TCP**
- Destination Port—**HTTPS**
- Action—**Permit**



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	TCP	Any	HTTPS	Permit
2	10.4.48.0/ 255.255.255.0	Any	TCP	Any	Other/22	Permit
3	Any	Any	TCP	Any	HTTPS	Deny
4	Any	Any	TCP	Any	Other/22	Deny
5	Any	Any	Any	Any	Any	Permit



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

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

Procedure 11 Configure wireless user authentication using Cisco ISE

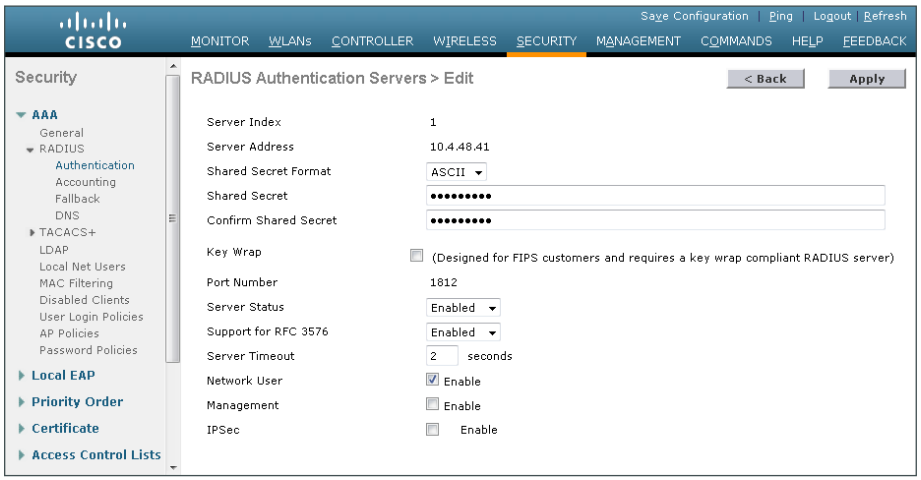
In this design, the RADIUS authentication service is provided by the Cisco Identity Services Engine (ISE). The Cisco ACS server is used solely for network administrative access to the WLC using TACACS+.

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**.

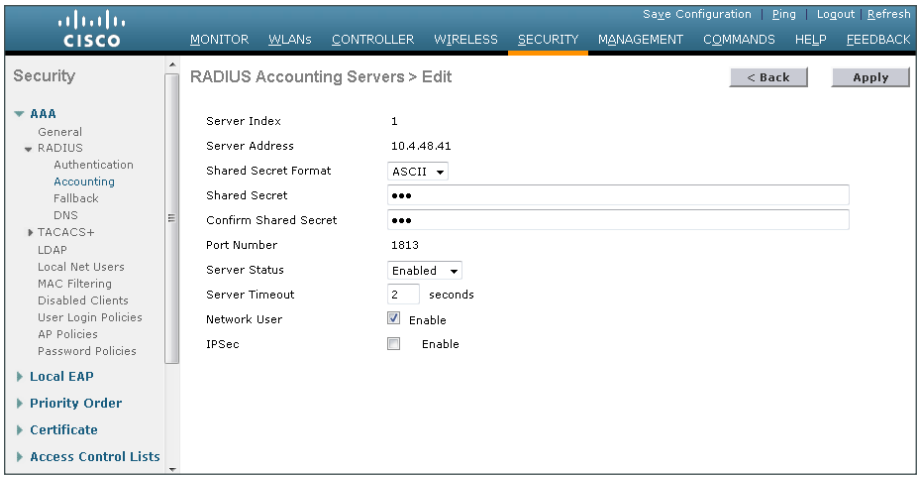


Step 5: Repeat the Step 1 through Step 4 in the above process to add the secondary Cisco ISE authentication server (Example 10.4.48.42), then press apply followed by click Save Configuration.

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**.



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

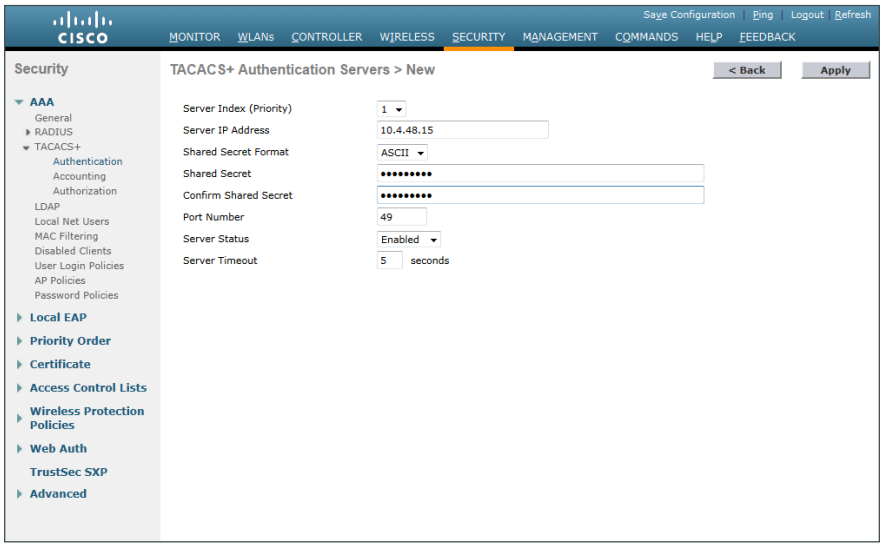
You can use this procedure to deploy centralized management authentication by configuring an authentication, authorization and accounting (AAA) service.

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)

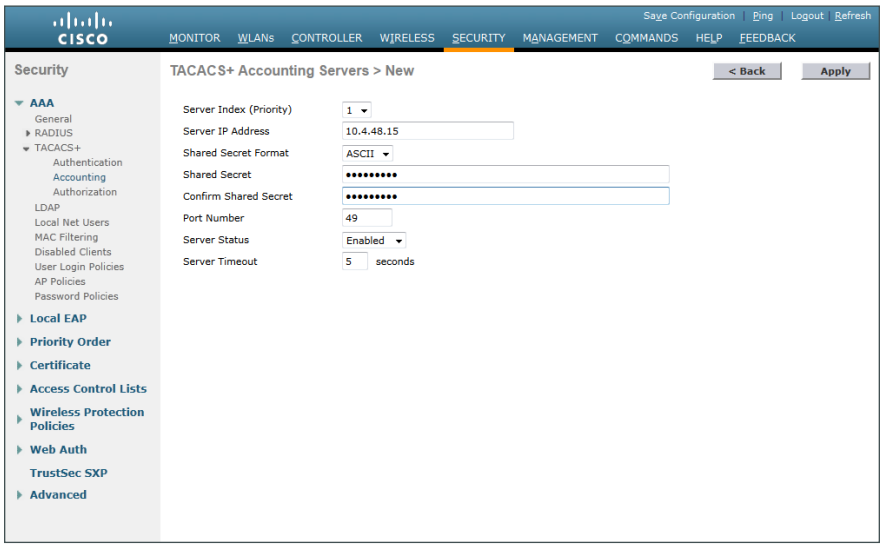
Step 3: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)



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

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

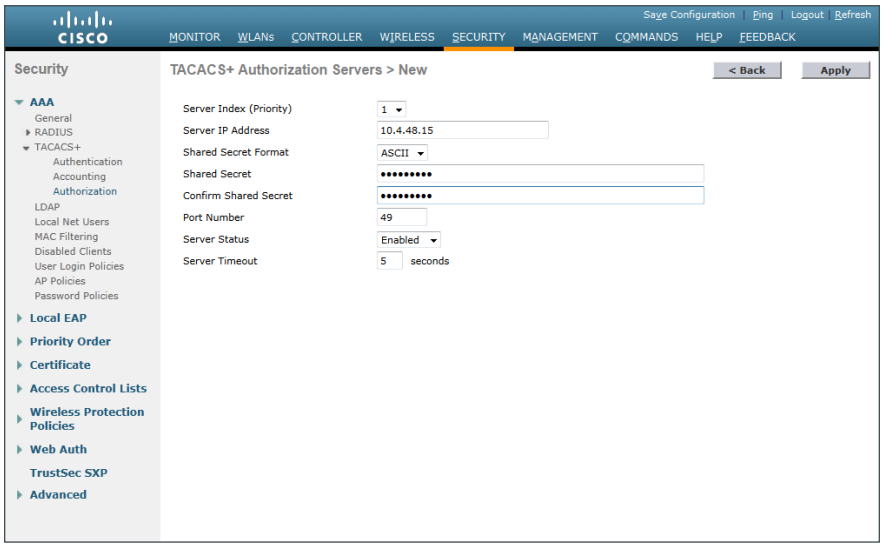
Step 6: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)



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)

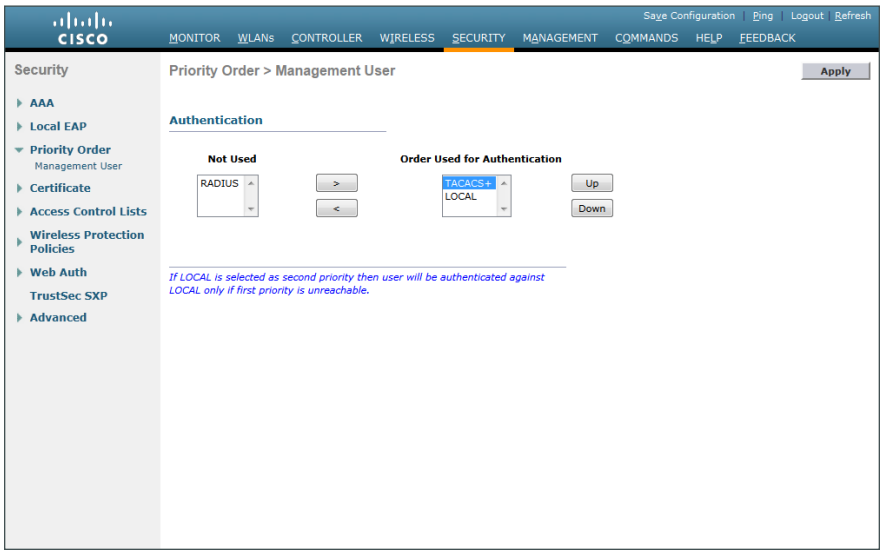


Step 10: Navigate to **Security > Priority Order > Management User**.

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).

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.

Table 15 - FlexConnect mobility group values

	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		

Figure 11 - FlexConnect Mobility Group WLC-1 (Primary)

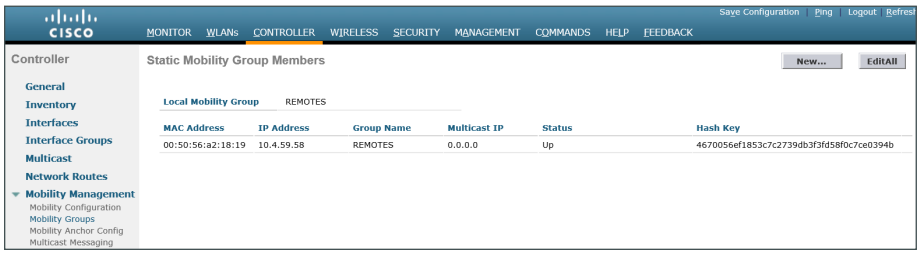
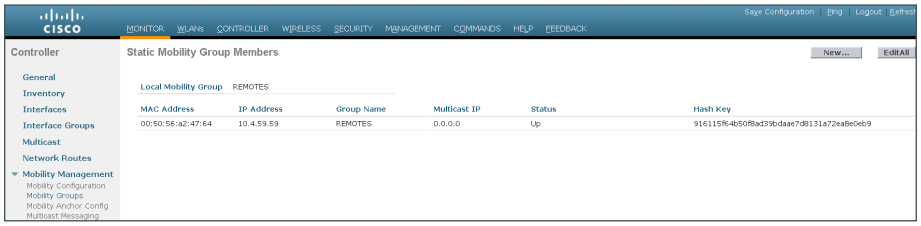


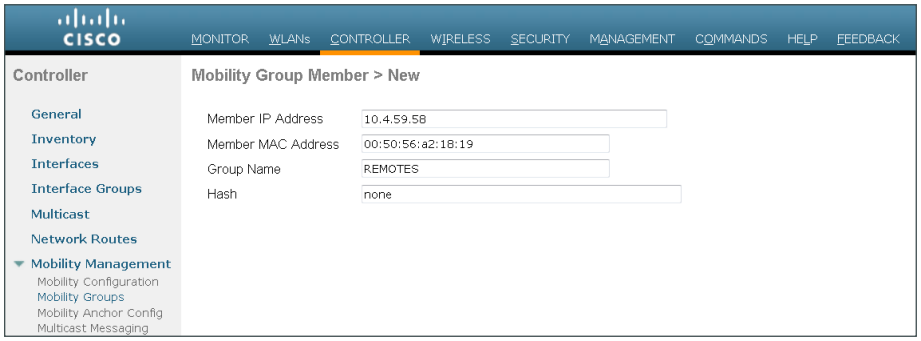
Figure 12 - FlexConnect Mobility Group WLC-2 (Secondary)

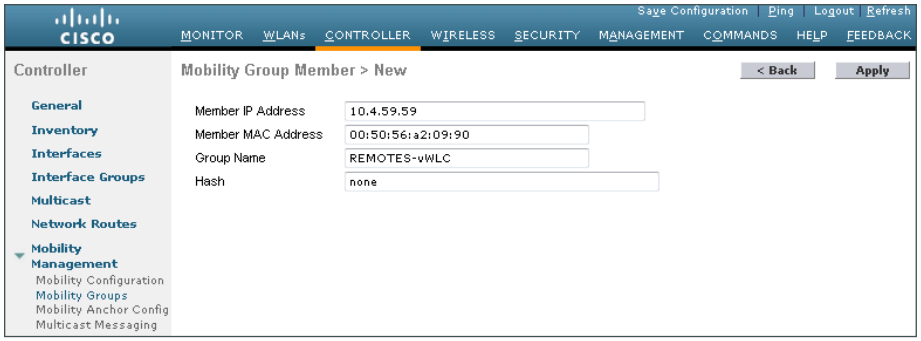


Step 2: On the resilient controller (Example: vWLC-RemoteSites-2), navigate to **Controller > Mobility Management > Mobility Groups**, and then click **New**.

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)

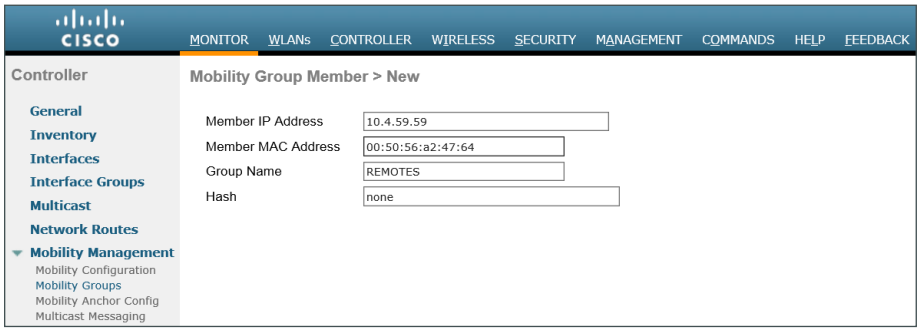




Step 5: On the controller designated as the primary controller (vWLC-RemoteSites-1), navigate to **Controller > Mobility Management > Mobility Groups**, and then click **New**.

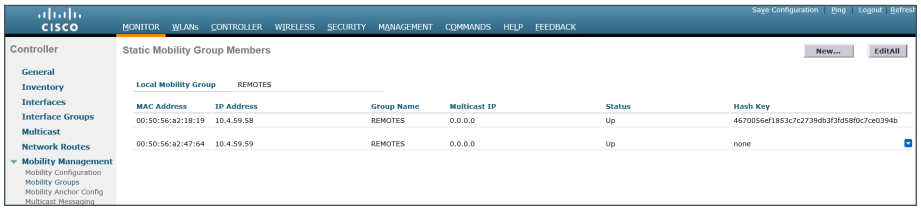
Step 6: In the **Member IP Address** box, enter the IP address of the resilient controller. (Example: 10.4.59.59)

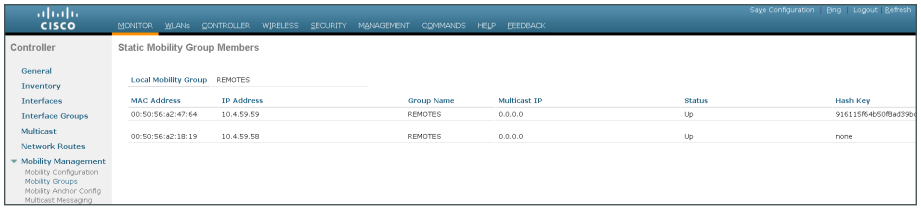
Step 7: In the **Member MAC Address** box, enter the MAC address of the resilient controller, and then click **Apply**. (Example: 00:50:56:a2:47:64)



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).





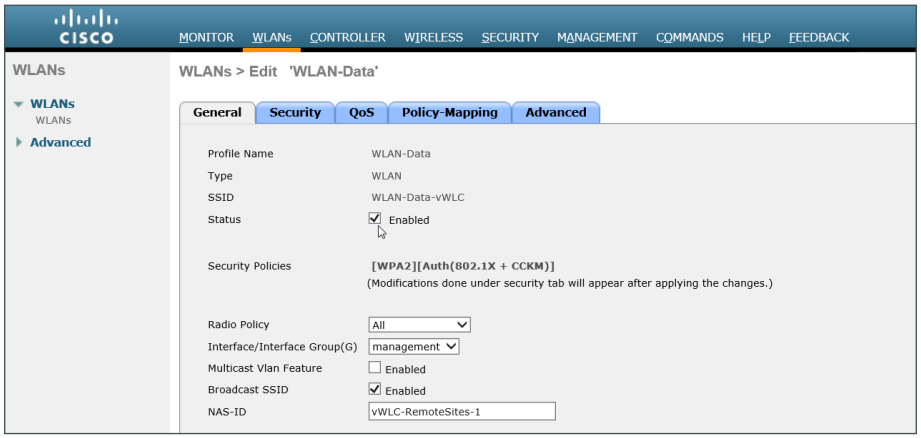
Procedure 15 Configure the data wireless LAN

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.

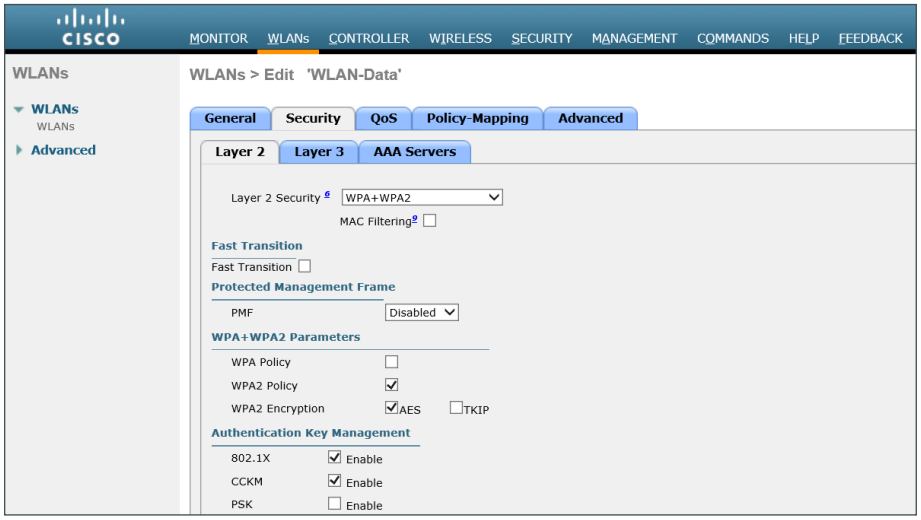
Step 3: On the General Tab, to the right of Status, ensure that it is enabled by selecting **Enabled**, and then click **Apply**.



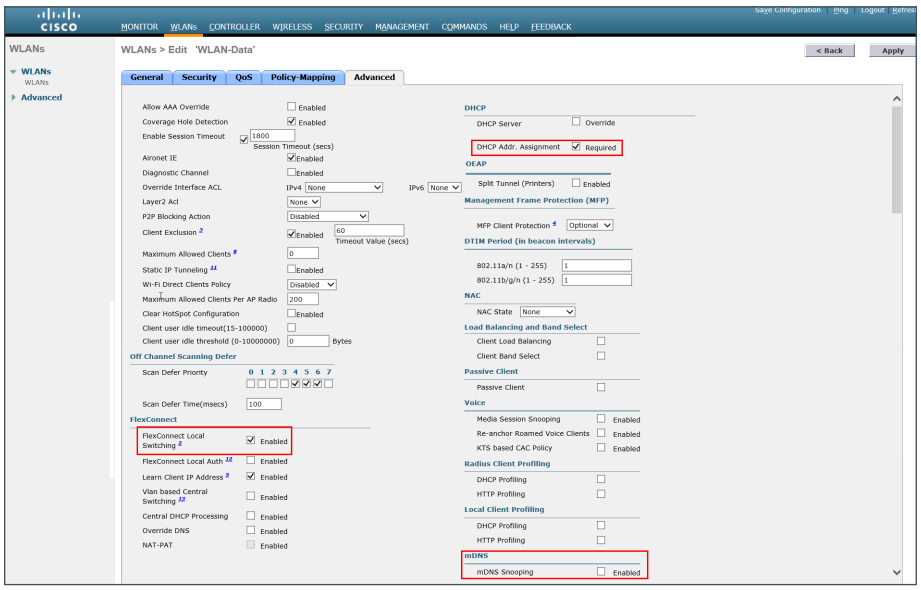
Step 4: On the **Security > Layer 2** tab, enable **CCKM**. This enables fast roaming.

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.



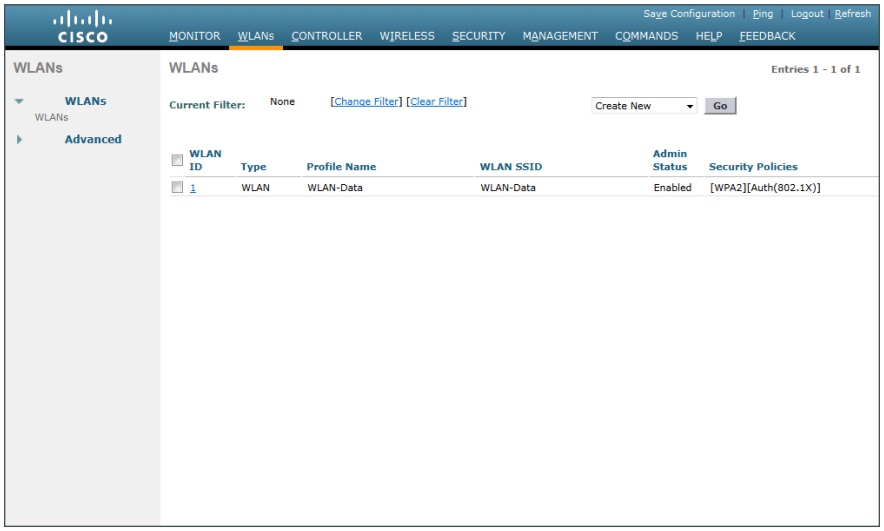
Step 5: On the Advanced tab, specify that DHCP Address Assignment is required, disable mDNS Snooping, enable FlexConnect Local Switching, and then click **Apply**.



Procedure 16 Configure the voice wireless LAN

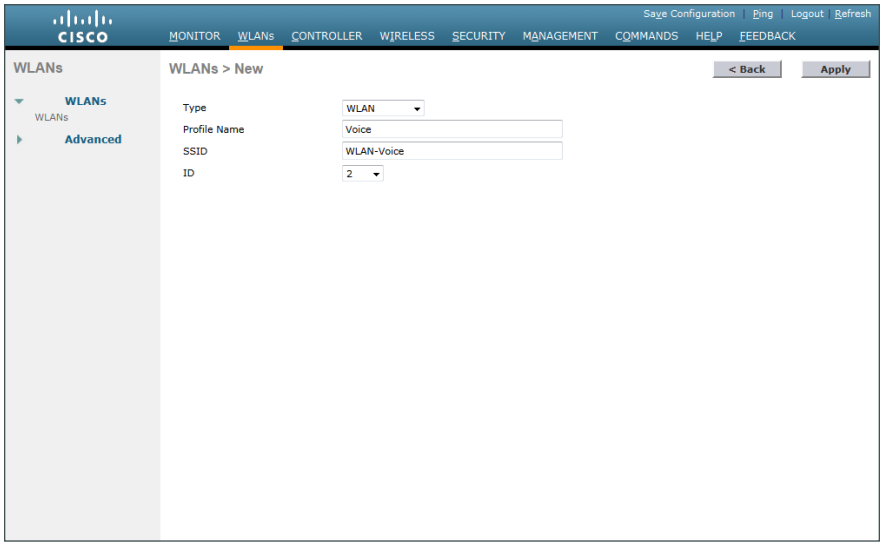
Wireless voice traffic is unique among other types of data traffic in that it cannot effectively handle delay and jitter or packet loss. To configure the voice WLAN, change the default QoS settings to Platinum and segment the voice traffic onto the voice wired VLAN.

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



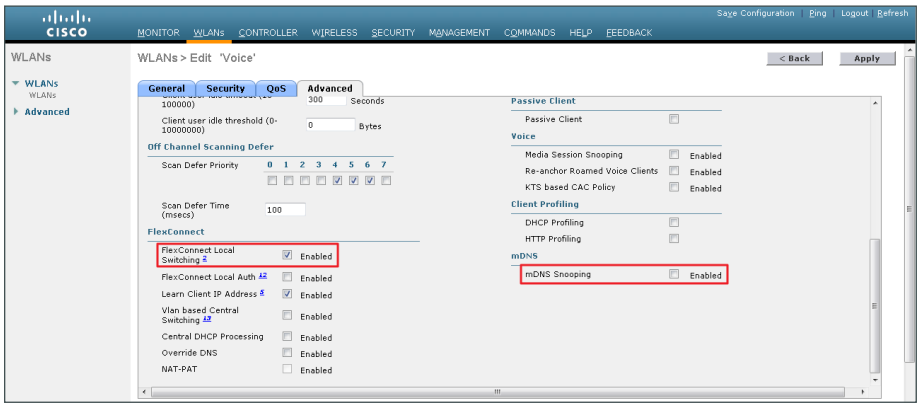
Step 2: Enter the **Profile Name**. (Example: Voice)

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

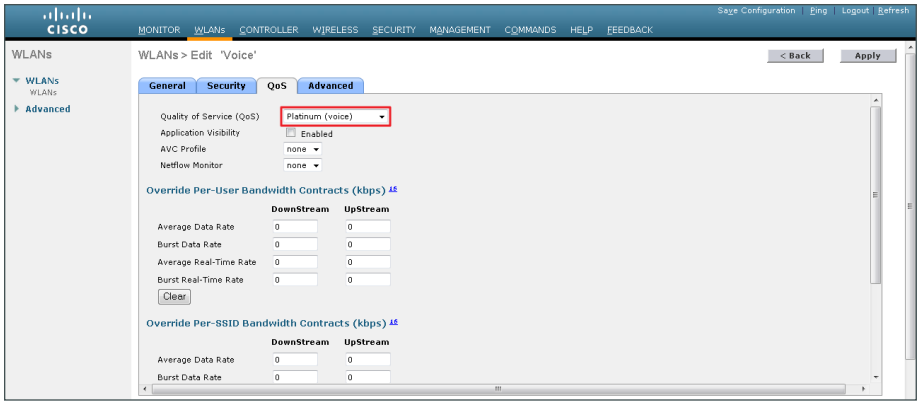


Step 4: On the Advanced tab, disable mDNS Snooping, because this is not supported with FlexConnect Local Switching. For voice WLANs, DHCP-required is not a recommended configuration, because roaming between WLCs that use different DHCP servers may result in frame loss. Additionally, some voice deployments require static IP address assignment for voice endpoints.

Step 5: Enable FlexConnect Local Switching by selecting **Enabled**, and then click **Apply**.



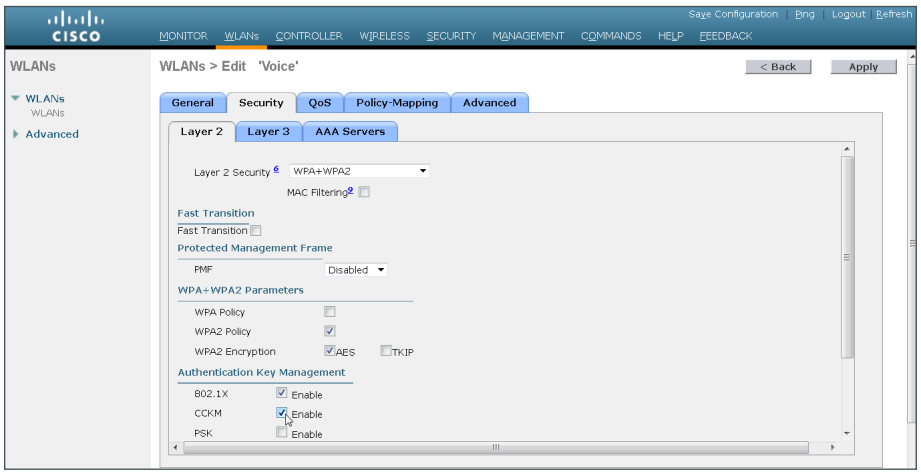
Step 6: On the QoS tab, in the **Quality of Service (QoS)** list, choose **Platinum (voice)**, and then click **Apply**.



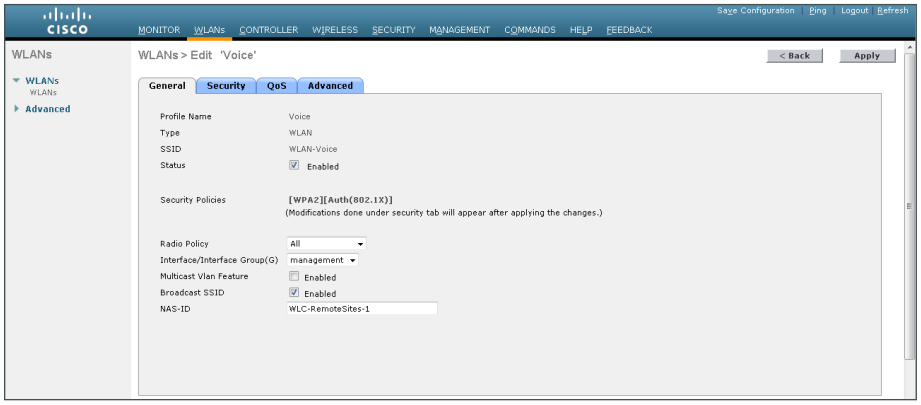
Step 7: On the **Security > Layer 2** tab, enable **CCKM. This** enables fast roaming.

Tech Tip

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.



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



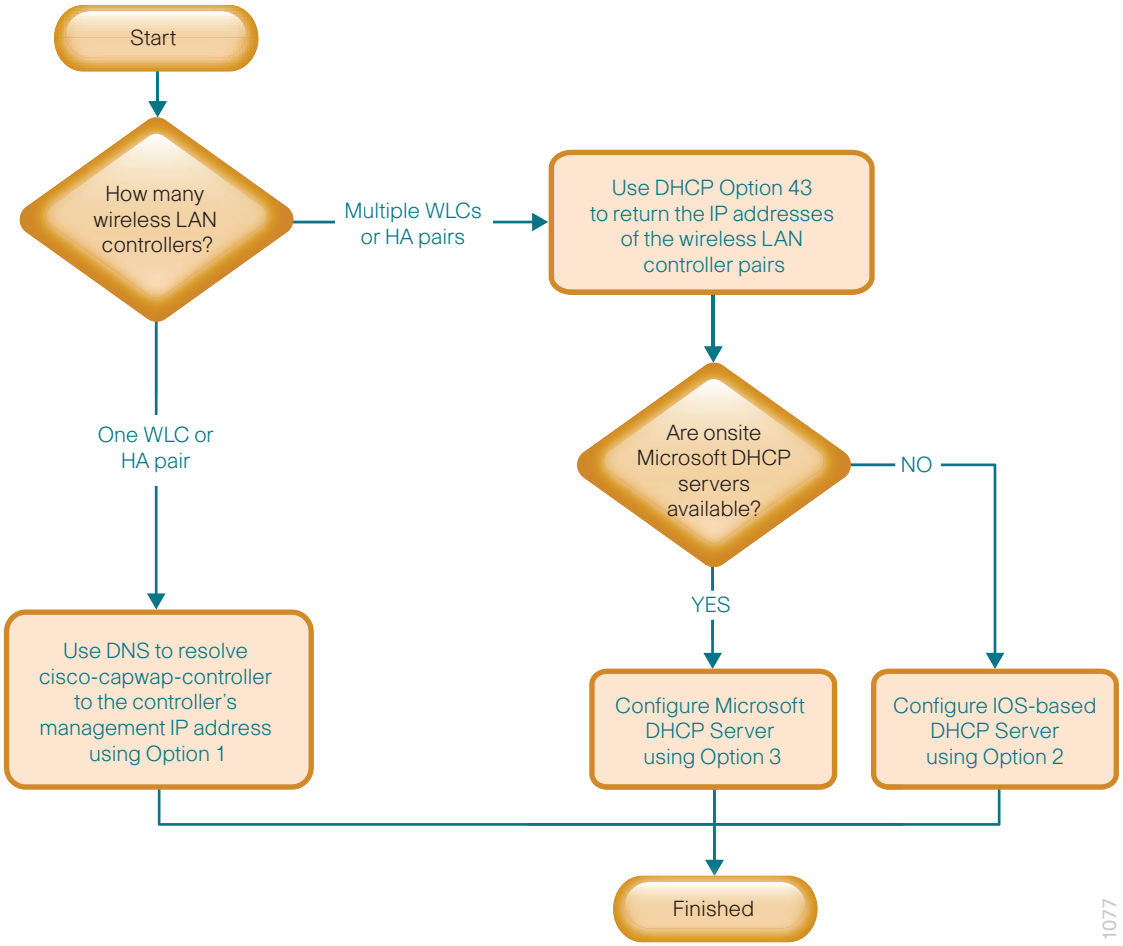
Procedure 17 Configure controller discovery

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

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

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

Figure 13 - Flow chart of WLC discovery configuration options



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

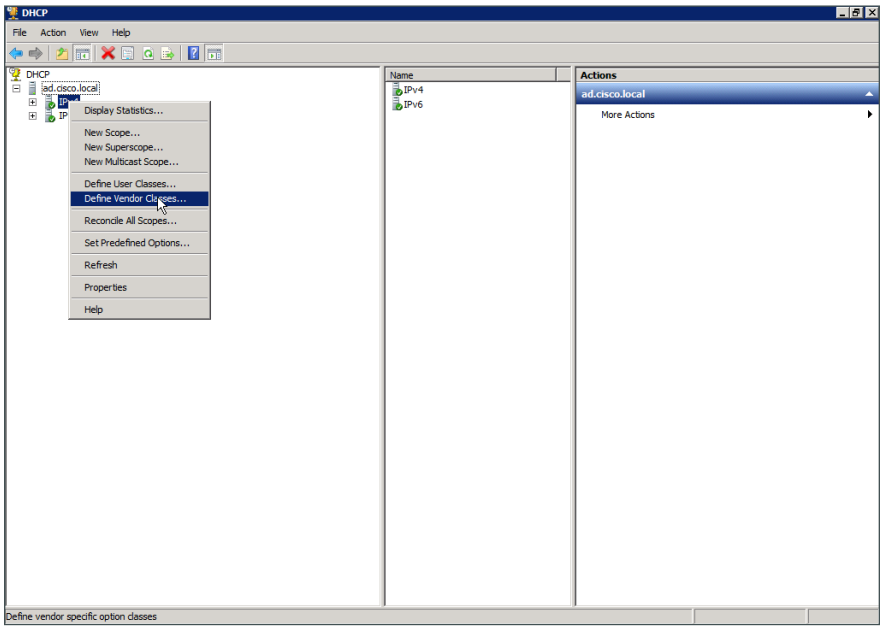
This procedure shows how the Microsoft DHCP server is configured to return vendor-specific information to the lightweight Cisco Aironet 1600, 2600, 3600 and 3700 Series Access Points used in this design guide. The vendor class identifier for a lightweight Cisco Aironet access point is specific to each model type. To support more than one access point model, you must create a vendor class for each model type.

Table 16 - Vendor class identifiers

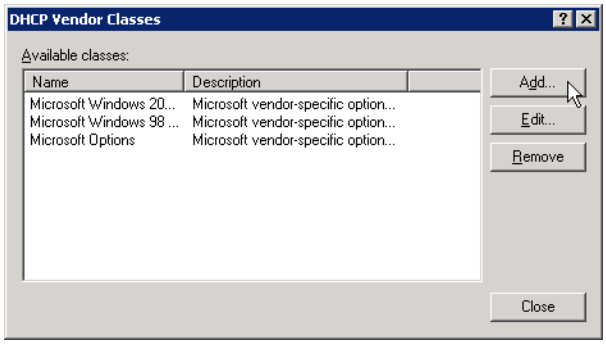
Access point	Vendor class identifier
Cisco Aironet 1600 Series	Cisco AP c1600
Cisco Aironet 2600 Series	Cisco AP c2600
Cisco Aironet 3600 Series	Cisco AP c3600
Cisco Aironet 3700 Series	Cisco AP c3700

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

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



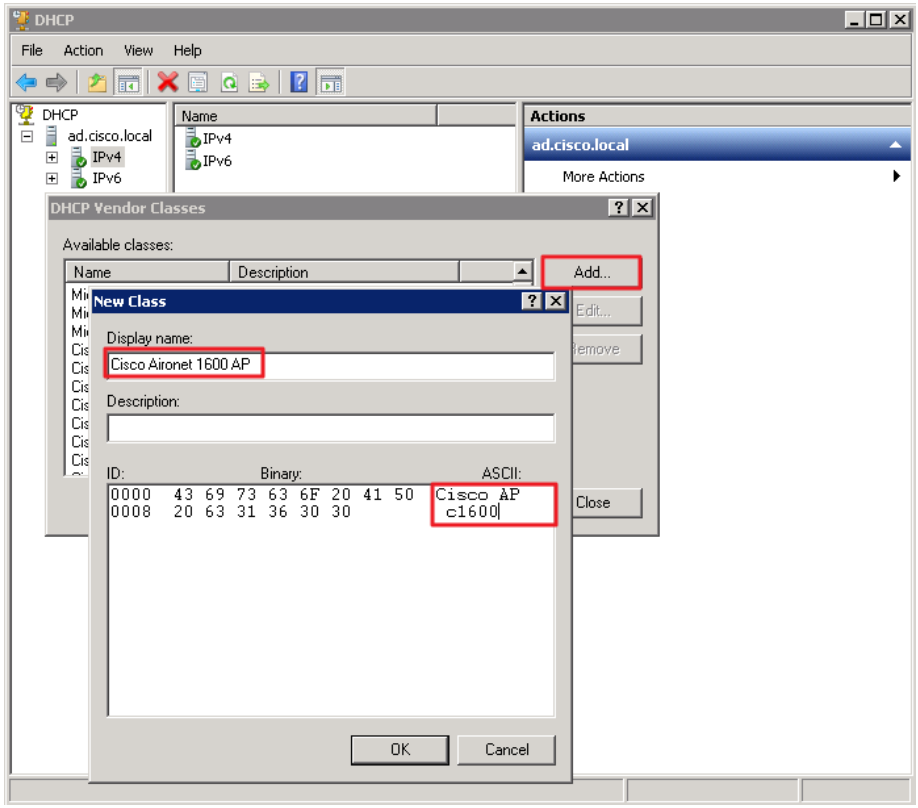
Step 3: In the DHCP Vendor Classes dialog box, click **Add**.



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

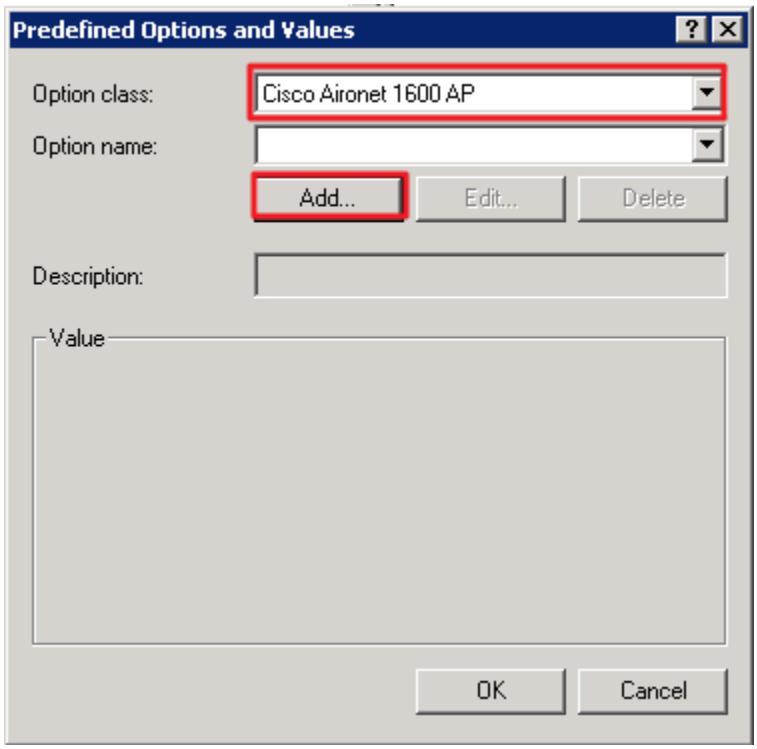
Step 5: In the ASCII section, enter the vendor class identifier for the appropriate access point series from Table 13, and then click **OK**. (Example: Cisco AP c1600)

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**.

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

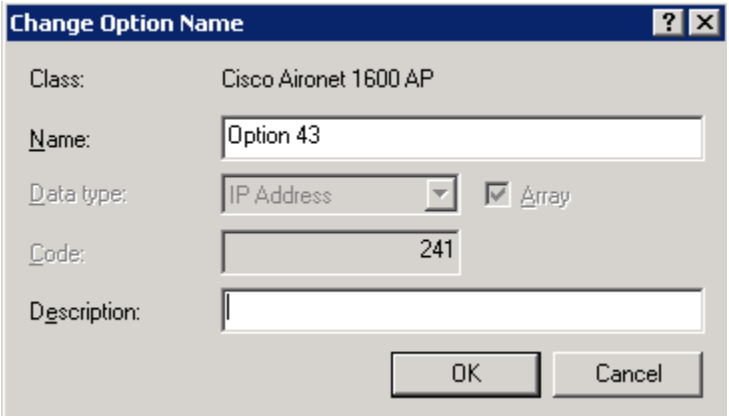


Step 9: In the **Option Type** dialog box, enter a **Name**. (Example: Option 43)

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**.



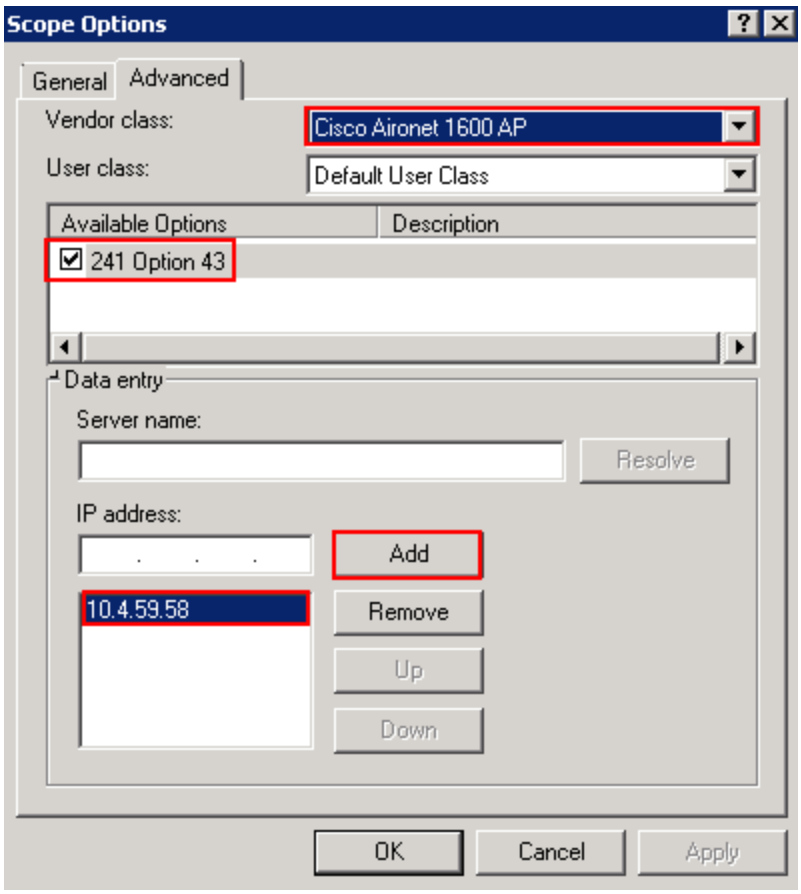
The vendor class and suboption are now programmed into the DHCP server. Now, you need to define the vendor-specific information for the DHCP scope.

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

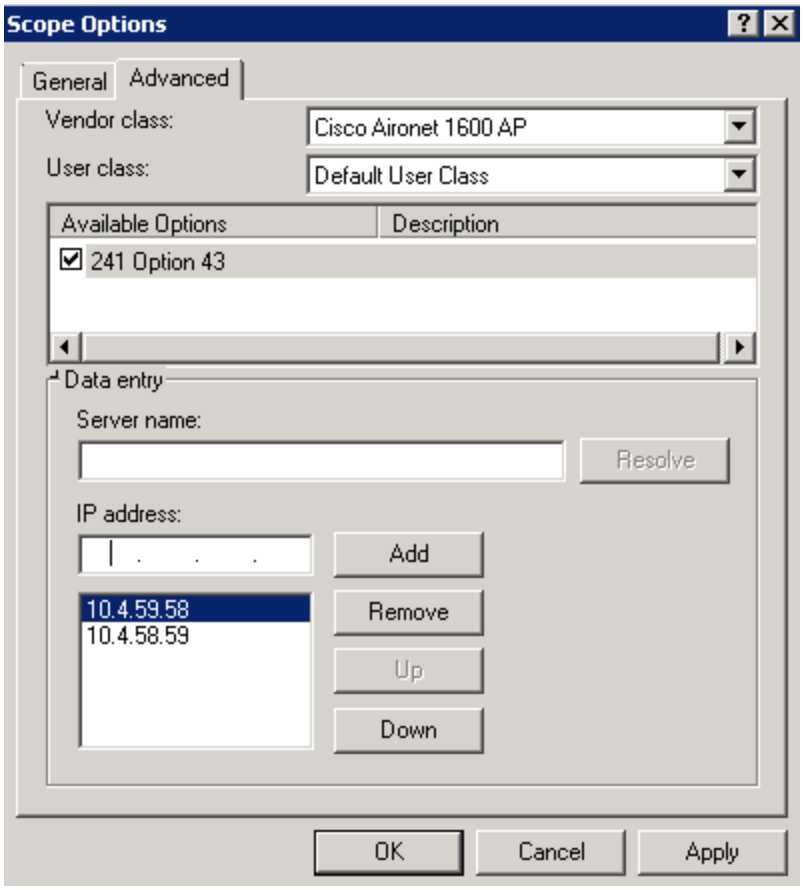
Step 14: Click the **Advanced** tab, and then in the **Vendor class** list, choose the class you created in this procedure. (Example: Cisco Aironet 1600 AP)

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)



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)



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.

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.

Caution

If you do not activate the demo licenses, you will be unable to register the access point with the vWLC.

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

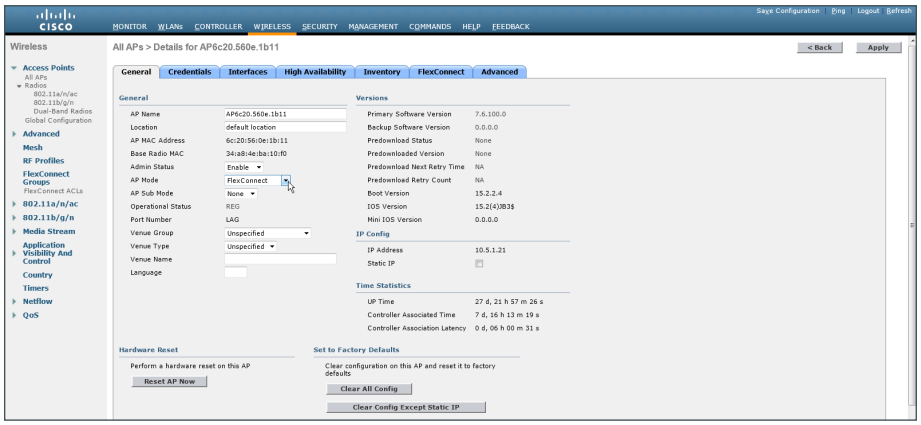
Step 1: Connect the access point to the remote-site switch, and then wait for the light on the access point to turn a solid color.

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.

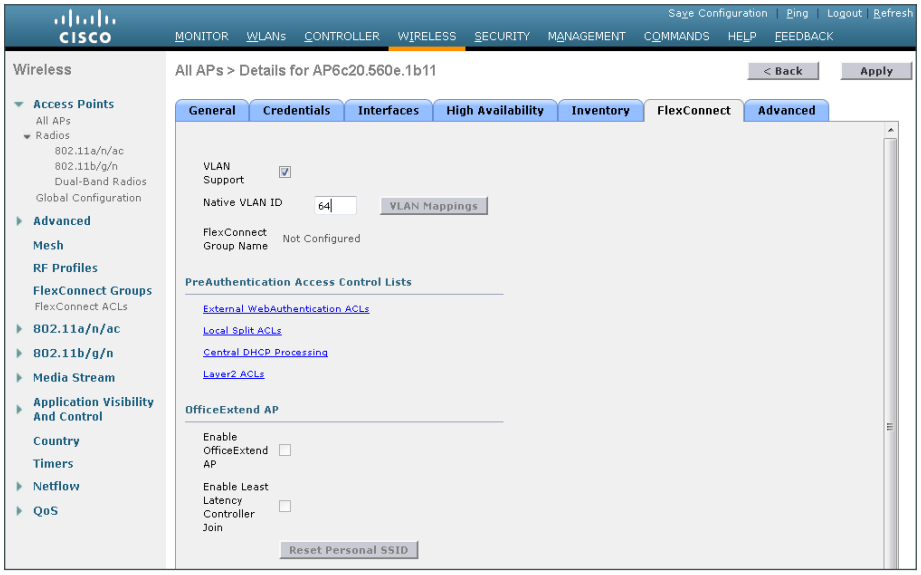
If the access points were registered to the WLC prior to issuing the **autoconvert** command, on the General tab, in the **AP Mode** list, choose **FlexConnect**, and then click **Apply**. Wait for the access point to reboot and reconnect to the controller. This should take approximately three minutes.



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

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

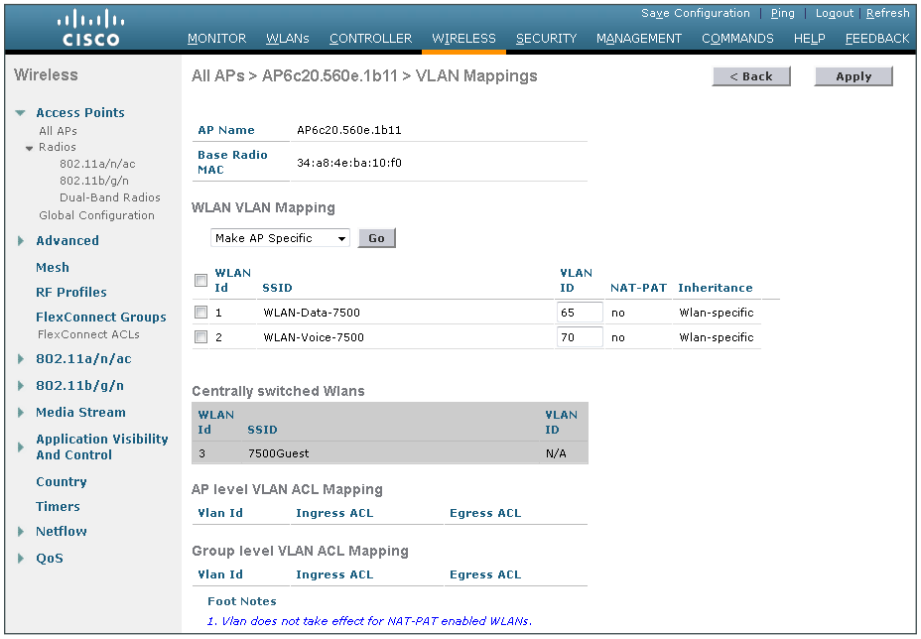
Step 7: In the **Native VLAN ID** box, enter the trunk's native VLAN number as configured in Procedure 17, and then click **Apply**. (Example: 64)



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)



Procedure 22 Configure access points for resiliency

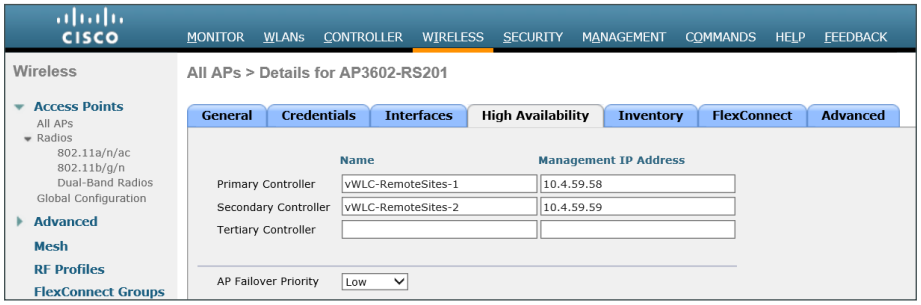
If you are using the HA SSO feature on a Cisco 5500 Series WLC or Cisco Flex 7500 Series Cloud Controller, skip this procedure, as the resilient controller automatically tracks the primary controller and assumes its IP address in the event of a failure. The HA SSO feature is not available on the virtual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



Procedure 23 Configure Cisco FlexConnect groups

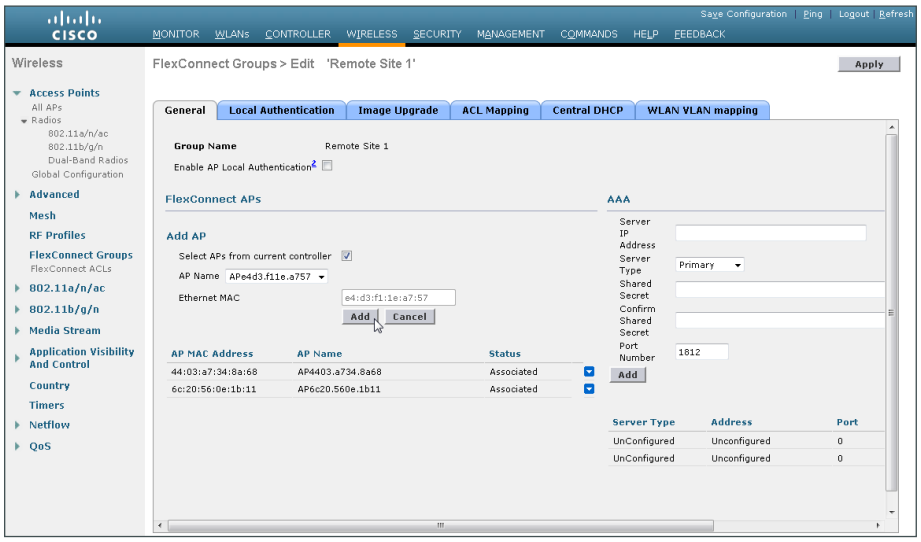
Step 1: On the WLC, navigate to **Wireless > FlexConnect Groups**, and then click **New**.

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**.

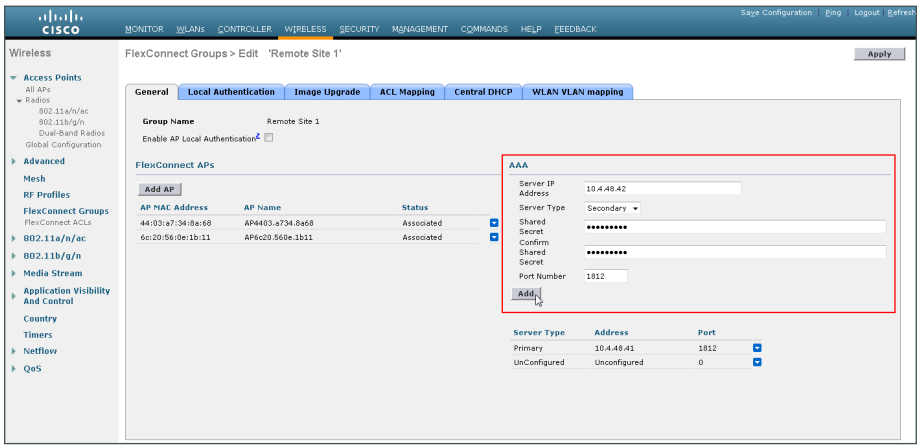
Step 5: In the **AP Name** list, choose an access point that is located at the site, and then click **Add**.



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

Step 7: Under AAA, enter the **Server IP Address** 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**.



Step 9: Repeat Procedure 23 for each remote site.

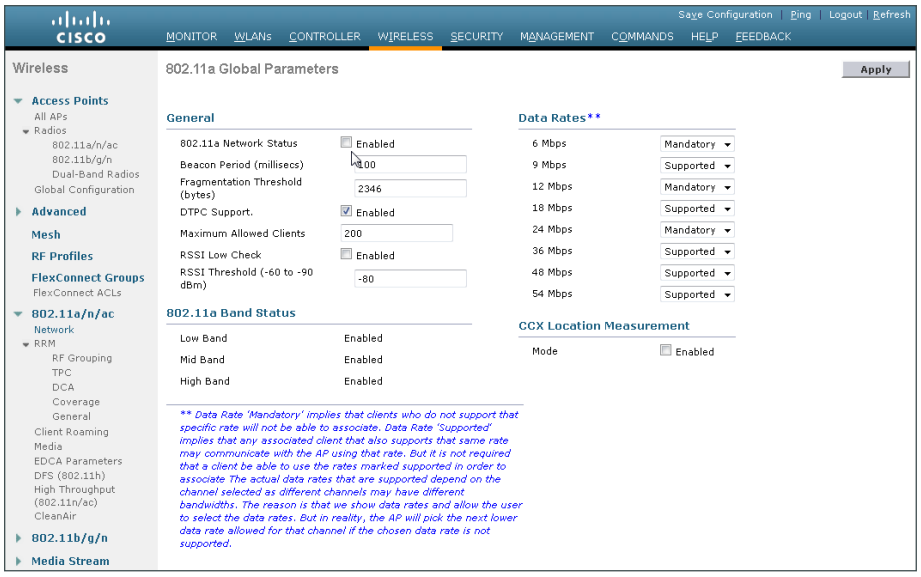
Procedure 24 Enable 802.11ac using DCA on Cisco AireOS Flex Controllers

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.

Tech Tip

Before enabling 802.11ac bonded channels, please review the 802.11ac section in the introduction of this document.

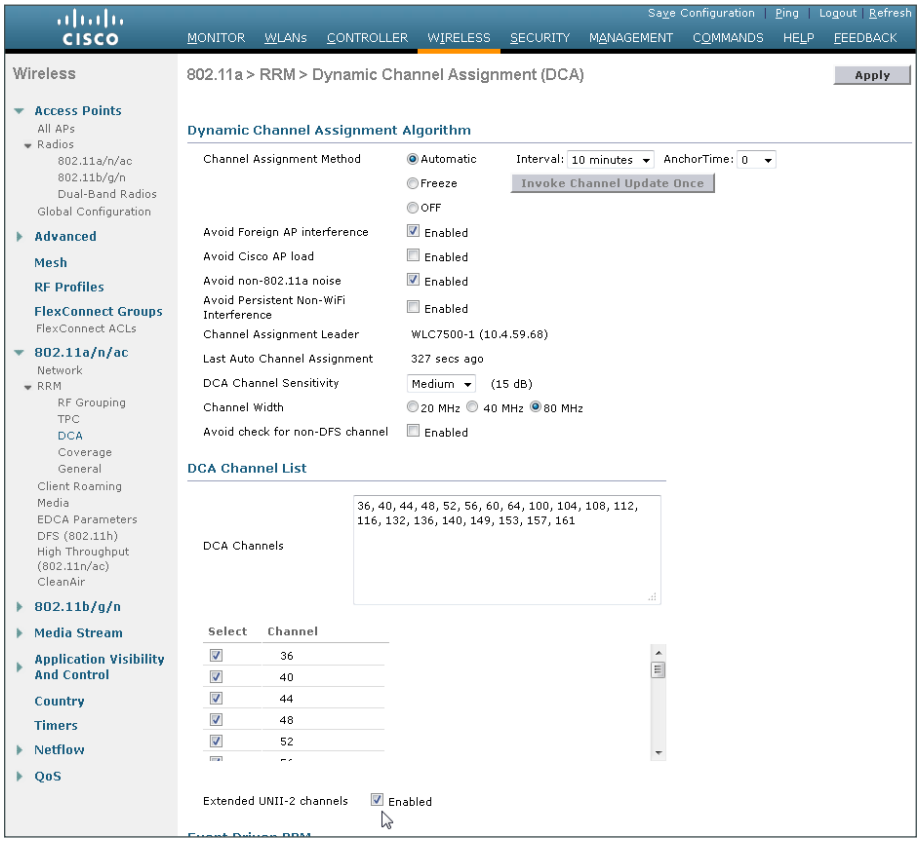
Step 1: Disable the 802.11a network by navigating to **Wireless > 802.11a/n/ac > Network**, clearing **802.11a Network Status**, and then clicking **Apply**.



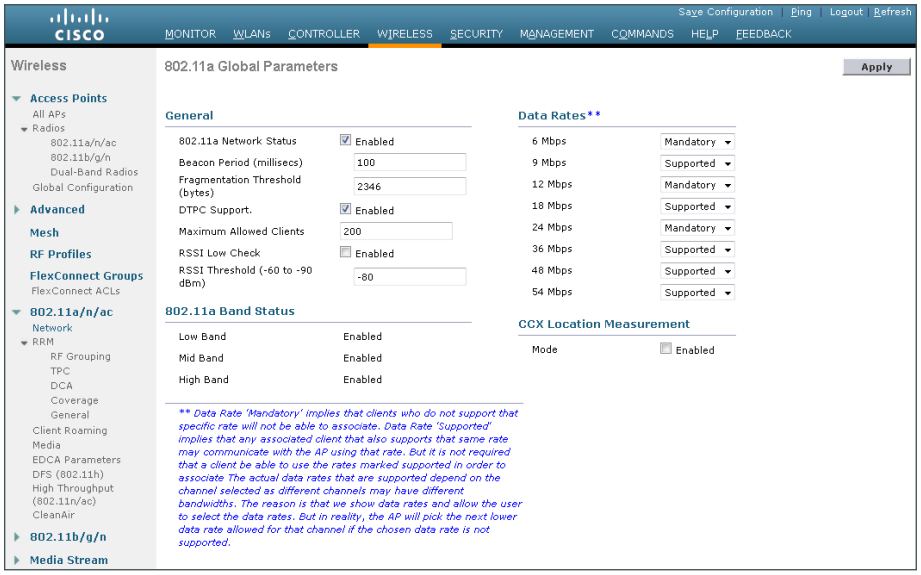
Step 2: Navigate to **Wireless > 802.11a/n/ac > RRM > DCA** and select the desired Channel Width to use (Example: 20 MHz, 40 MHz, 80 MHz). If they are available in your regulatory domain, enable **Extended UNII-2 Channels**, and then click **Apply**.

Tech Tip

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.

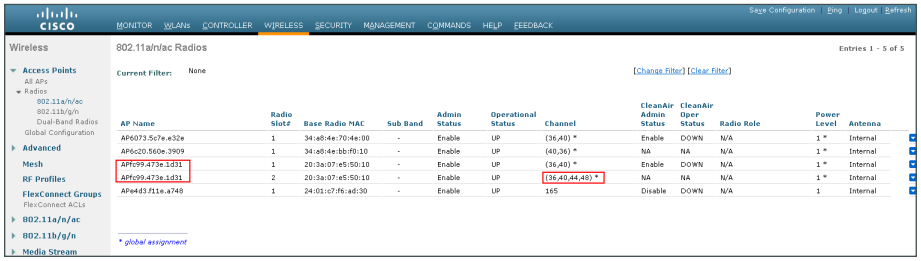


Step 3: Enable the 802.11a network by navigating to **Wireless > 802.11a/n/ac > Network**, selecting **802.11a Network Status**, clicking **Apply**, and then clicking **Save Configuration**.



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.



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.

PROCESS

Follow Additional Best Practices

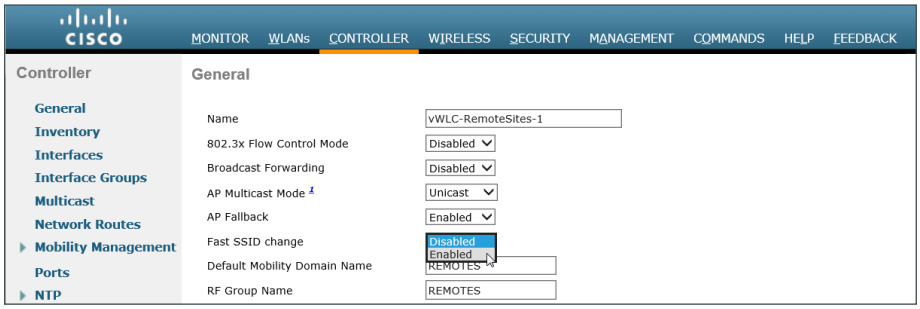
1. Globally enable Fast SSID change
2. Reduce the number of detected rogue APs
3. Enable CCKM to enable fast roaming

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**.



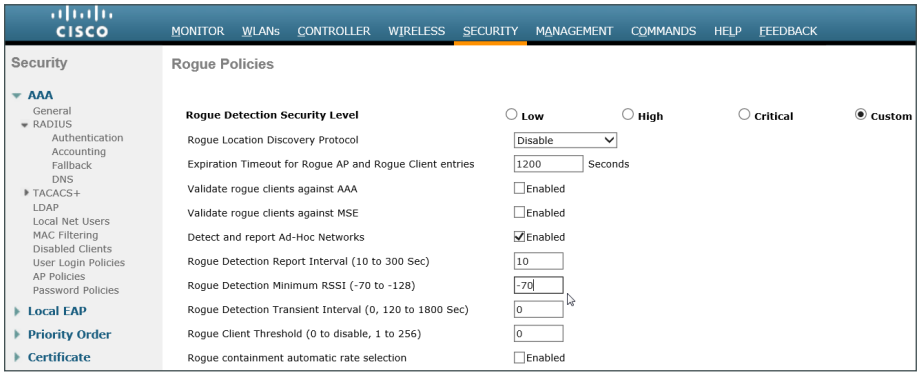
Step 2: Click **Apply** and **Save Configuration**.

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**.



Step 3: Press **Apply** and **Save Configuration**.

Procedure 3 Enable CCKM to enable fast roaming

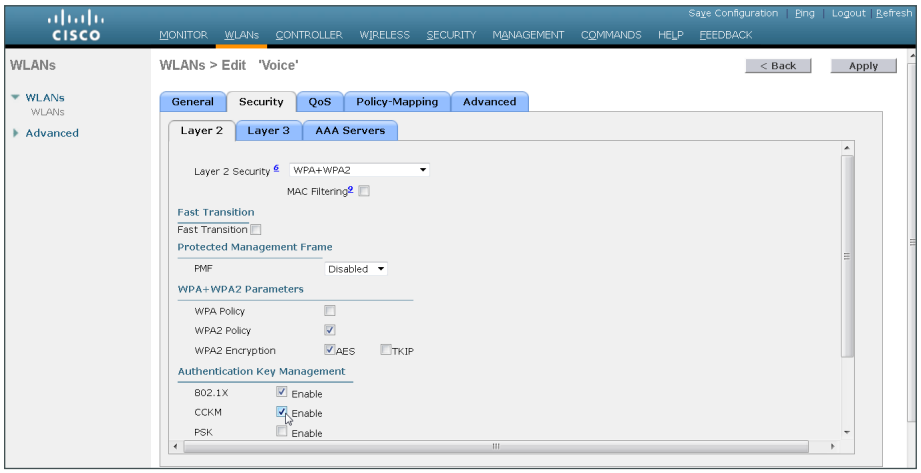
(Optional)

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.

Tech Tip

Note that 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.



PROCESS

Configuring Guest Wireless: Shared Guest Controller

1. Configure the distribution switch
2. Configure the firewall DMZ interface
3. Configure network address translation
4. Configure shared guest anchor WLC security policy
5. Configure the dynamic routing protocol
6. Create the guest wireless LAN interface on the AireOS Anchor WLCs
7. Configure the guest wireless LAN on Cisco AireOS WLCs
8. Create the lobby admin user account
9. Create guest accounts

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.

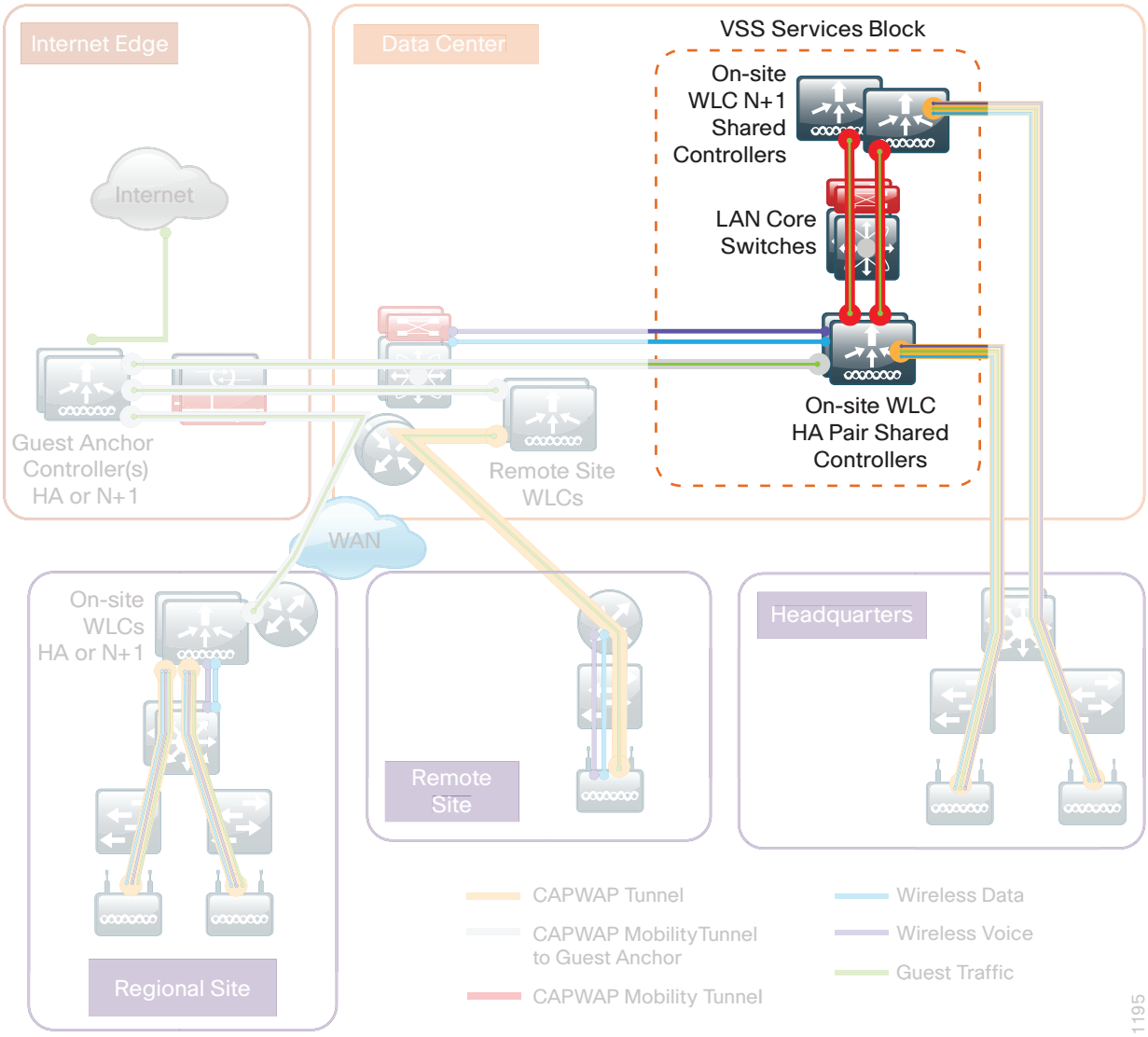
In a shared guest controller design, the shared anchor controller is on the inside of the ASA firewall. It **does not** require explicit access rules in the DMZ-based ASA to:

- 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.

Table 17 - Cisco ASA DMZ interface information

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)

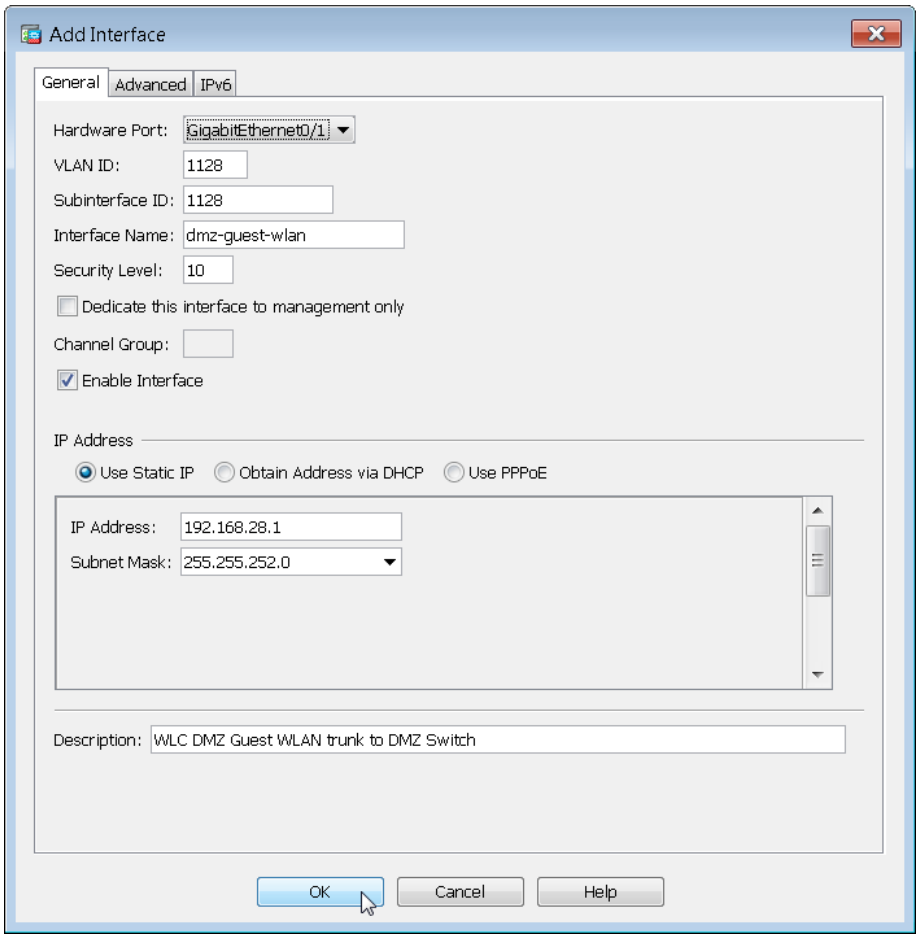
Step 6: In the **Subinterface ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1128)

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)

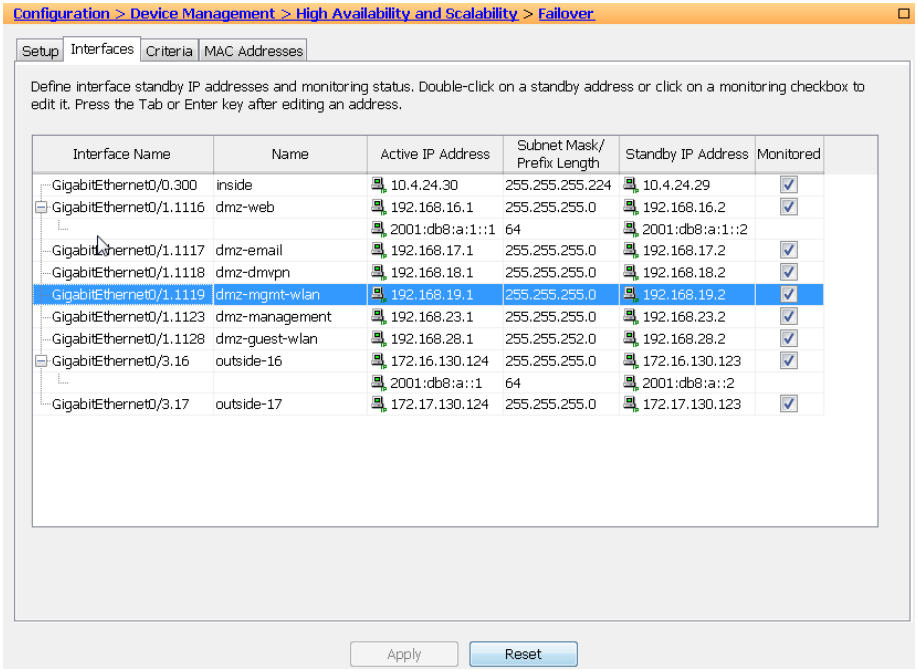
Step 10: Enter the interface **Subnet Mask**, and then click **OK**. (Example: 255.255.252.0)



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**.



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.

Figure 15 - Dual ISP topology

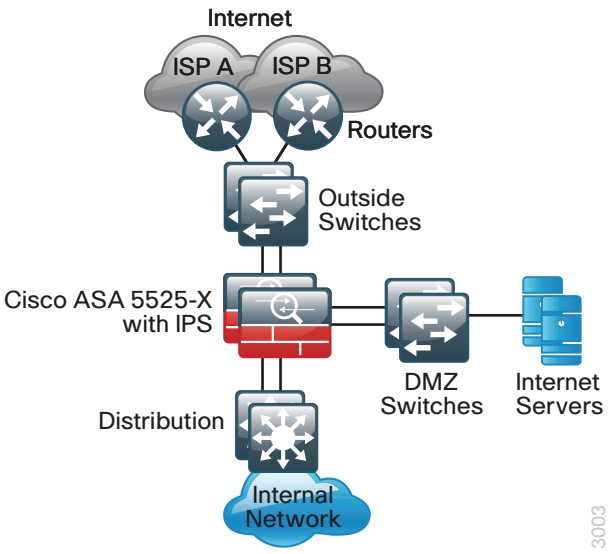


Table 18 - Wireless guest address mapping

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)

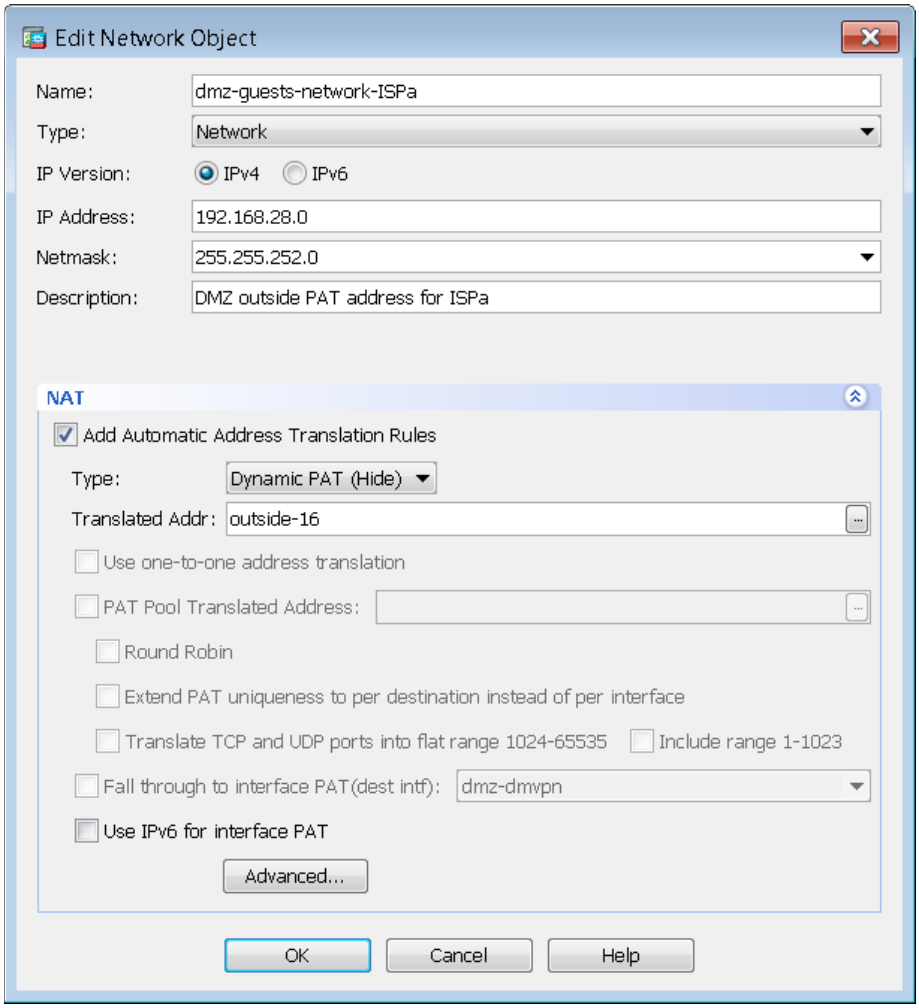
Step 6: In the **Netmask** box, enter the internal summary netmask. (Example: 255.255.252.0)

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)**.

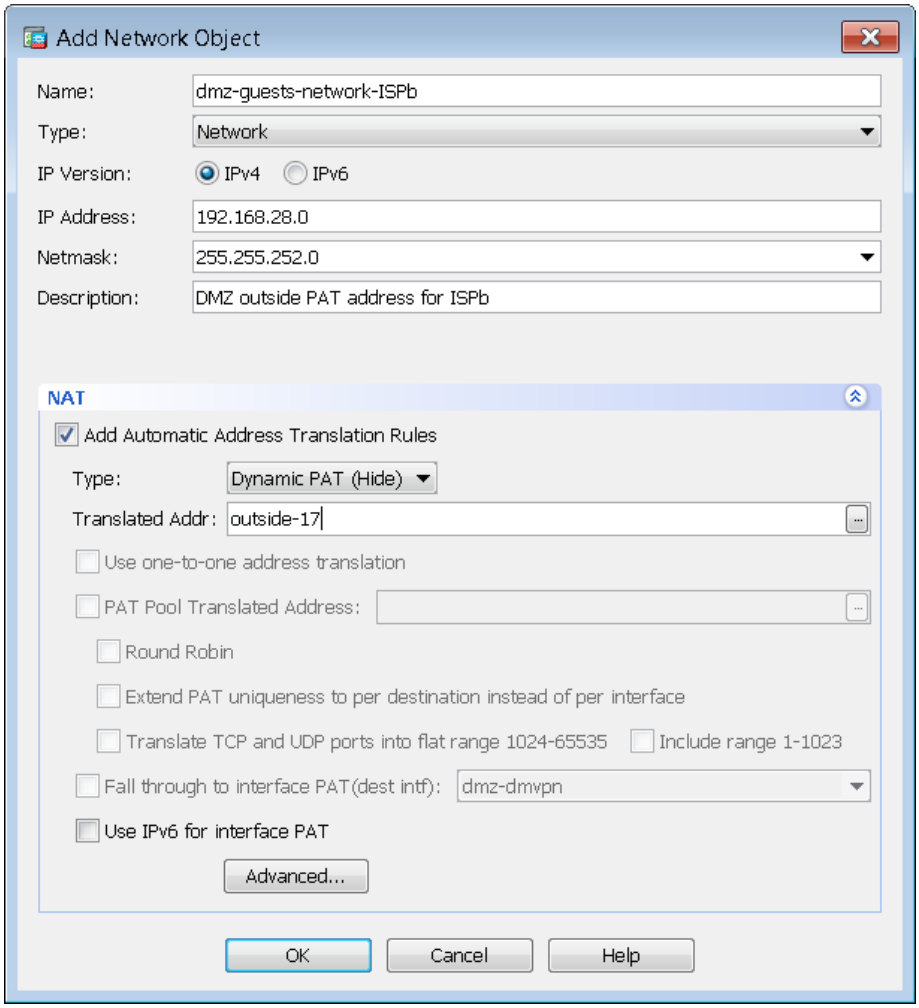
Step 10: In the **Translated Addr** box, enter the name of the primary Internet connection interface, and then click **OK**. (Example: outside-16, outside-17)



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)



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

Procedure 4 Configure shared guest anchor WLC 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**.

Table 19 - Guest network policy rules (shared guest controller)

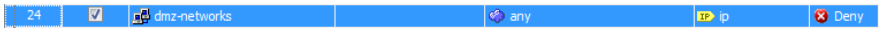
Interface	Action	Source	Destination	Service	Description	Logging Enable / Level
Any	permit	dmz-guest-wlan-network	internal-dns	tcp/domain, udp/domain	Allow guest wireless users to resolve DNS names.	Yes / Default
Any	permit	dmz-guest-wlan-network	internal-dhcp	udp/bootps	Allow wireless guest users to 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

Step 2: Repeat Step 3 through Step 11 for all rules listed in Table 19.

Tech Tip

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.



Caution

Be sure to perform this step for *every* rule listed in Table 19. 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: 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	☑	dmz-guest-wlan-network/22	internal-dns	domain domain	Permit	0	Allow Guest Wireless users to resolve DNS names.
28	☑	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	☑	dmz-guest-wlan-network/22	dmz-web-netw...	http https	Permit	0	Allow wireless guest users access to DMZ based webservers, possibly for walled garden access
30	☑	dmz-guest-wlan-network/22	dmz-networks internal-network	ip	Deny	0	Deny traffic from the wireless guest network to the internal and dmz resources
31	☑	dmz-guest-wlan-network/22	any	ip	Permit	0	Allow Wireless DMZ users access to the Internet
32	☑	dmz-networks	any4	ip	Deny	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.

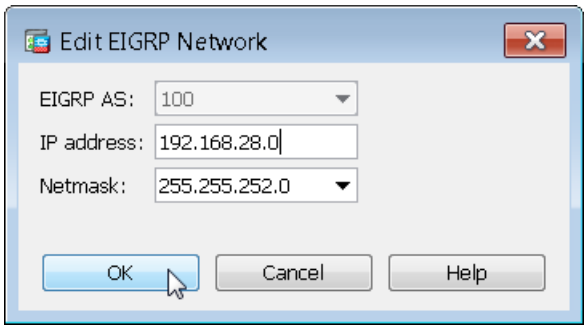
You can use a dynamic routing protocol in order to easily configure reachability between networks connected to the appliance and those that are internal to the organization. The steps below allow the advertisement of the dmz-guests-network to the rest of the campus network using EIGRP.

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 dmz-guests-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)



Step 5: In the Setup pane, click **Apply**.

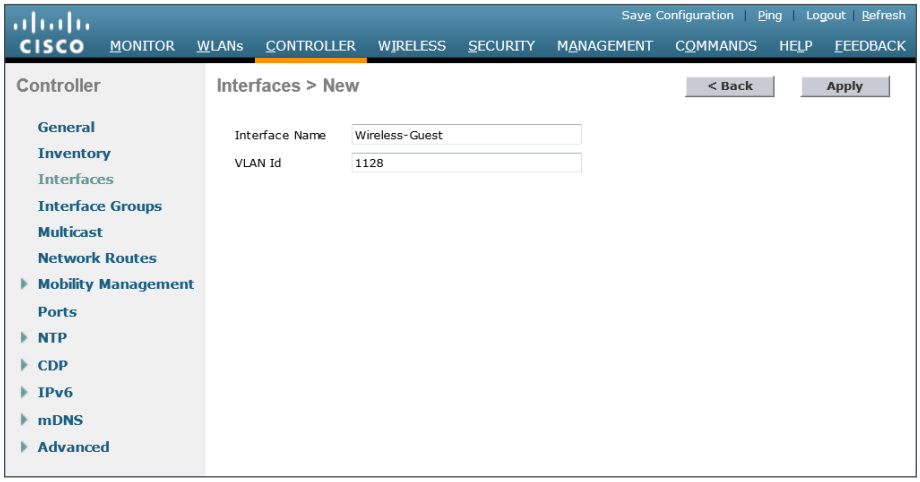
Procedure 6 Create the guest wireless LAN interface on the AireOS Anchor WLCs

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)

Step 3: Enter the **VLAN Id**, and then click **Apply**. (Example: 1128)

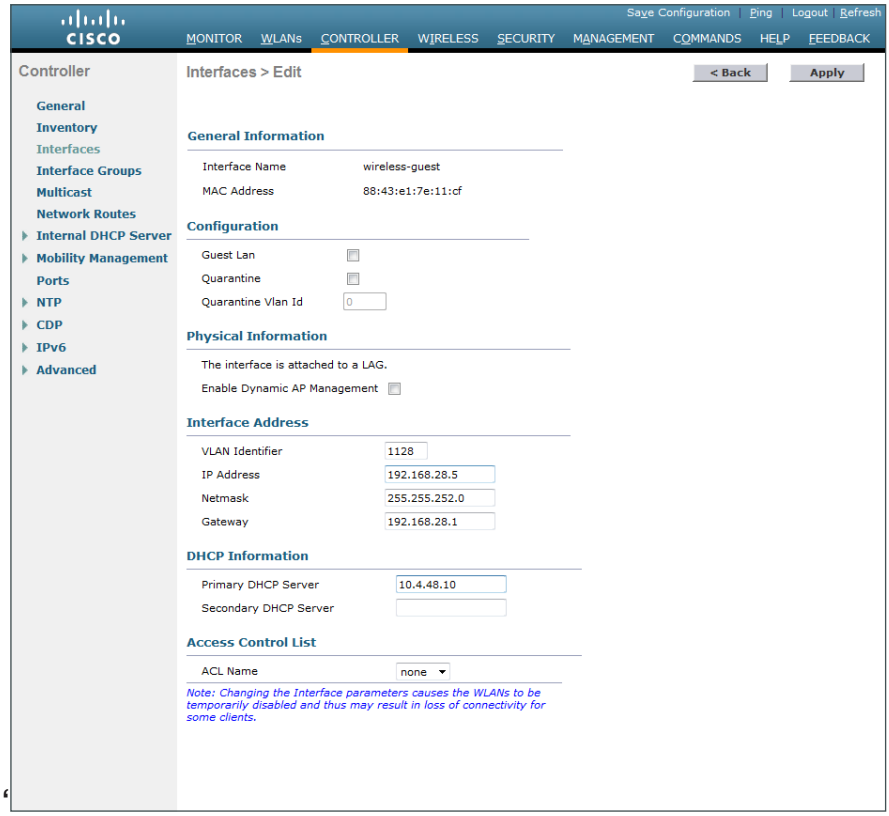


Step 4: In the **IP Address** box, enter the IP address you want to assign to the WLC interface. (Example: 192.168.28.5)

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)

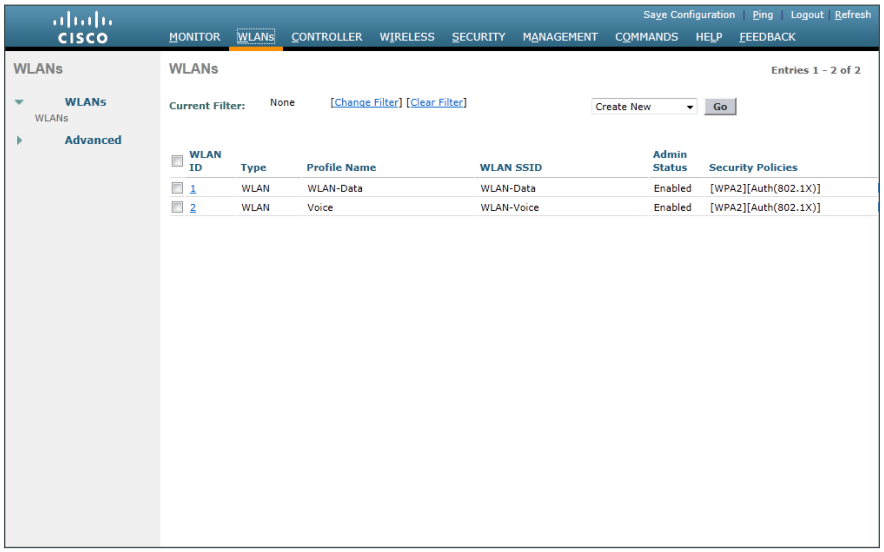


Tech Tip

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.

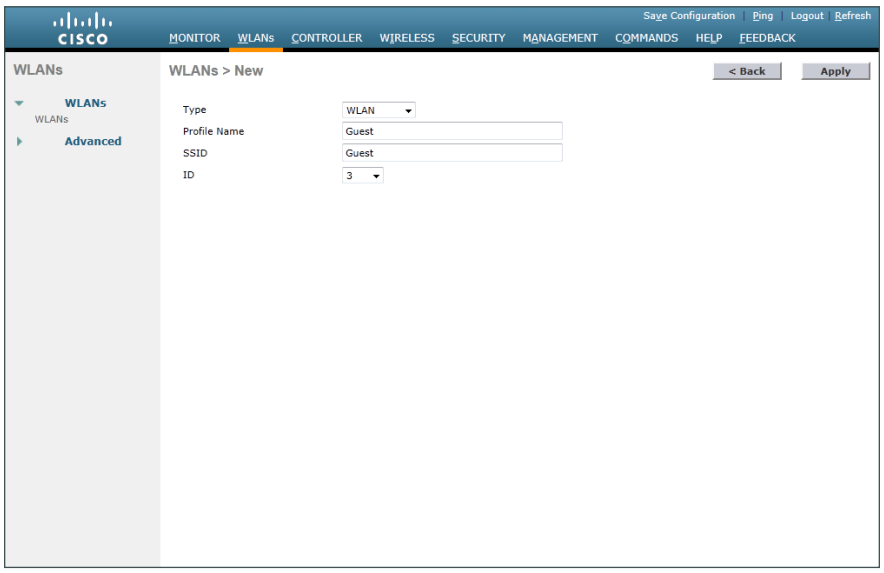
Procedure 7 Configure the guest wireless LAN on Cisco AireOS WLCs

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

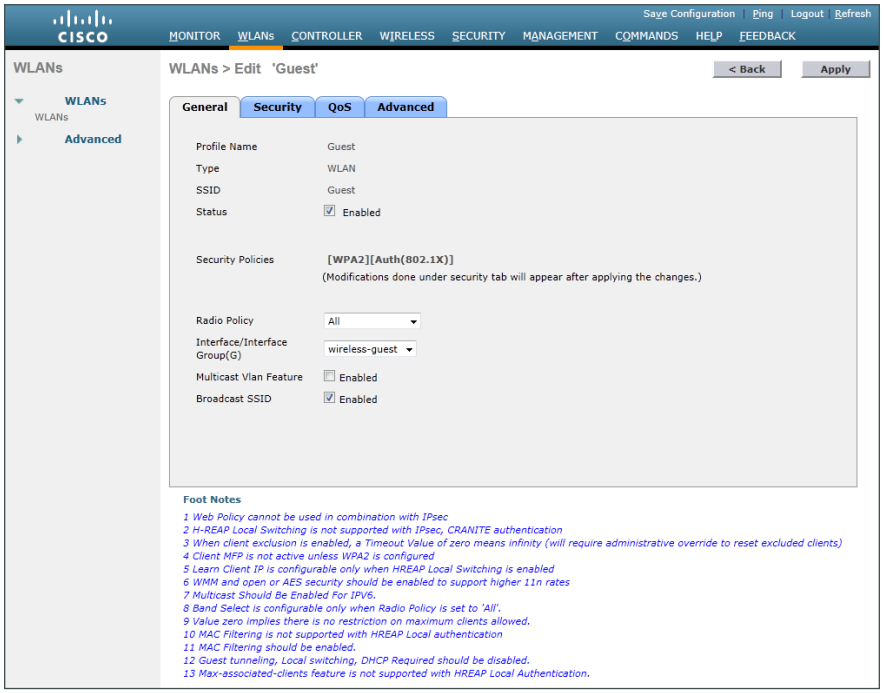


Step 2: Enter the **Profile Name**. (Example: Guest)

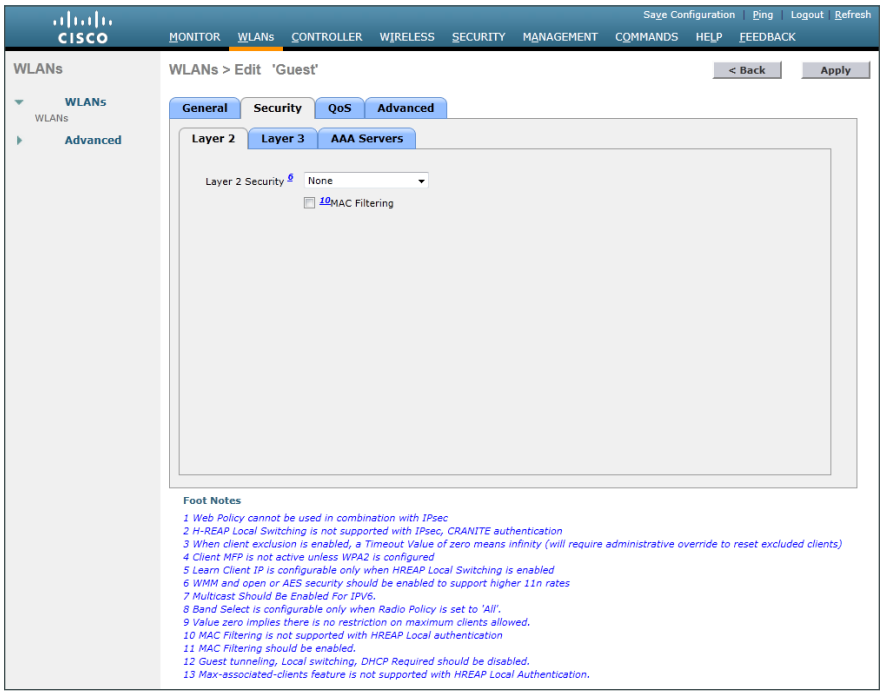
Step 3: In the **SSID** box, enter the guest WLAN name, and then click **Apply**. (Example: Guest)



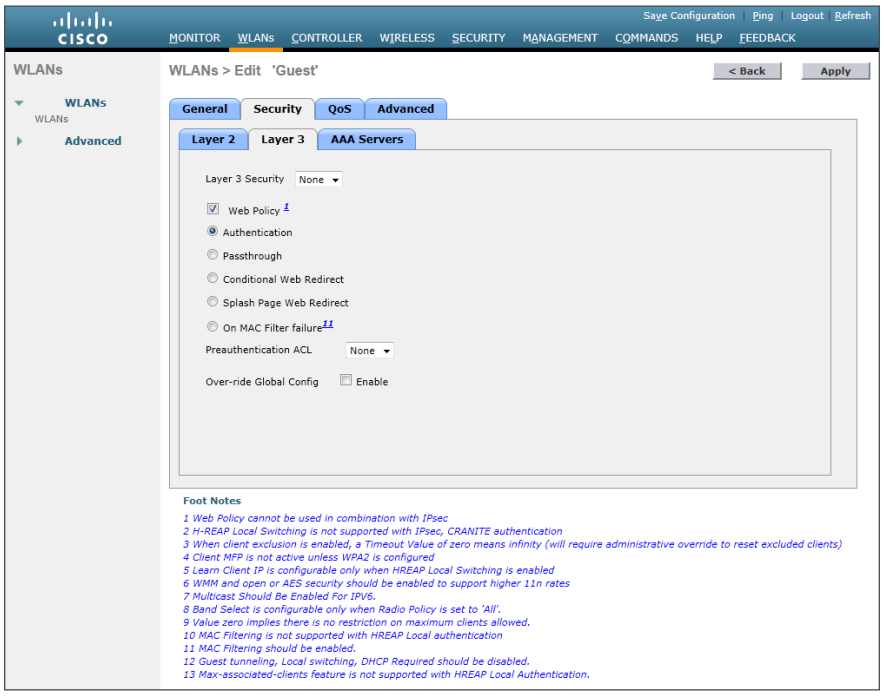
Step 4: On the General tab, in the **Interface/Interface Group(G)** list, choose the interface created in Procedure 6. (Example: wireless-guest)



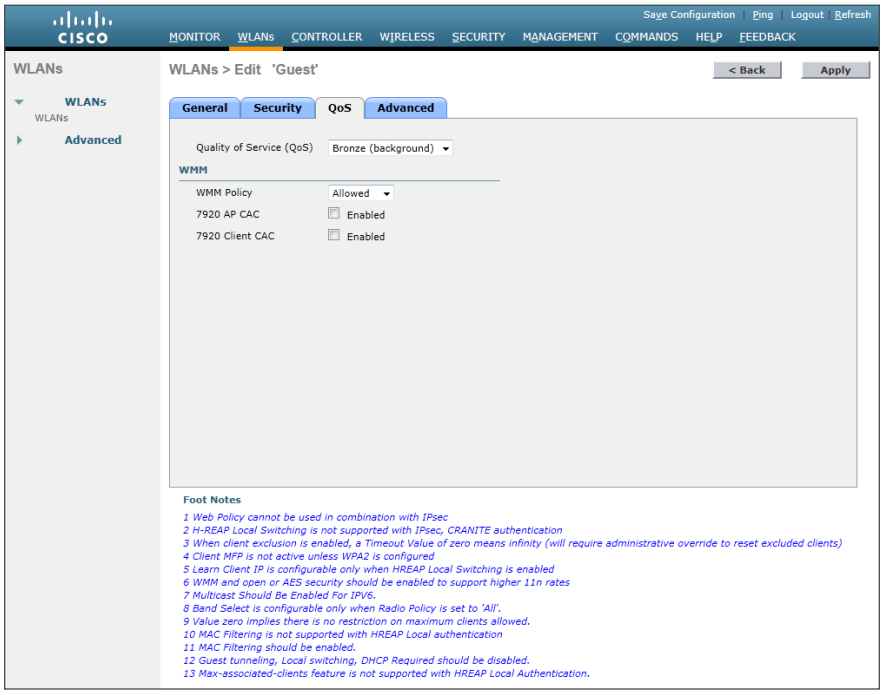
Step 5: Click the **Security** tab, and then on the Layer 2 tab, in the **Layer 2 Security** list, choose **None**.



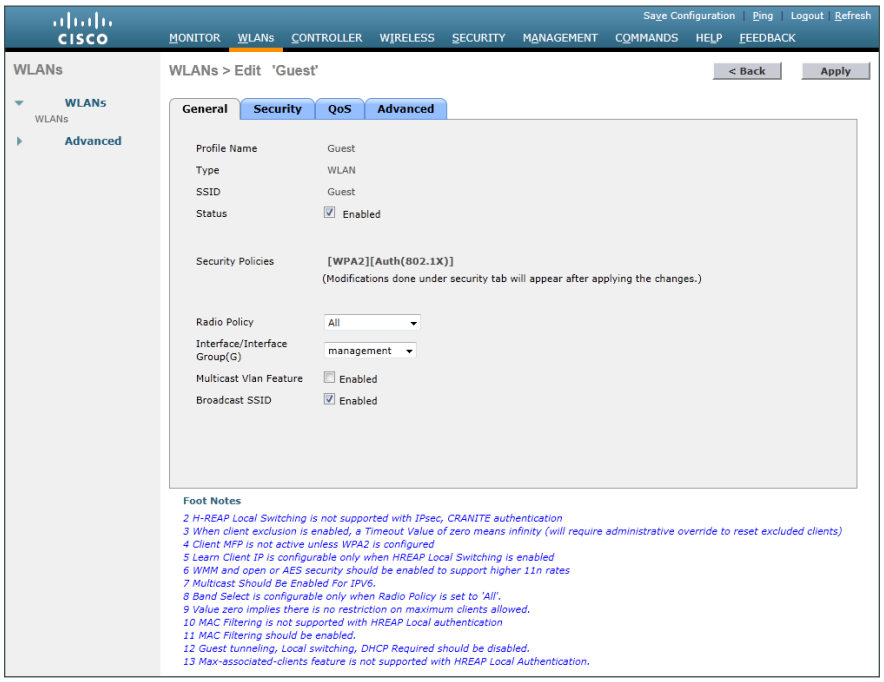
Step 6: On the **Layer 3** tab, select **Web Policy**, and then click **OK**.



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



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

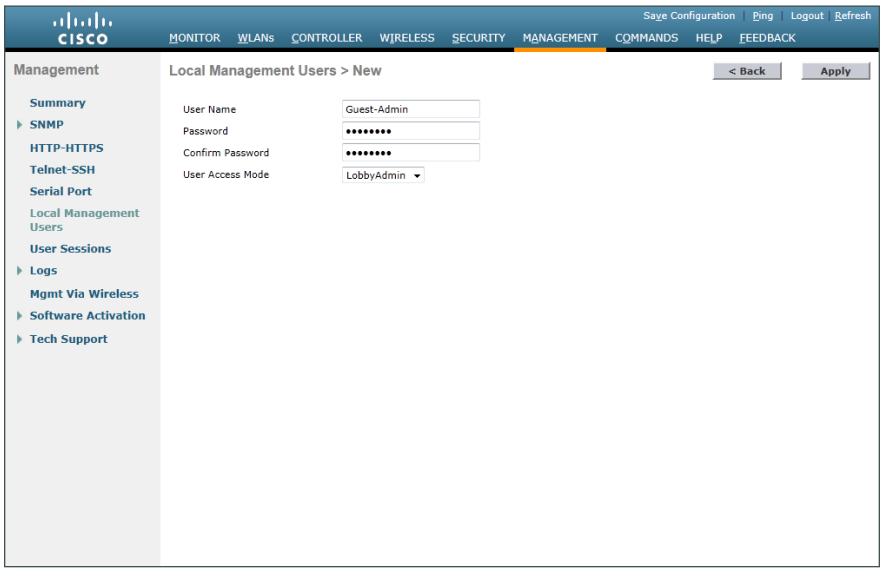
Typically, the lobby administrator is the first person to interact with your corporate guests. The lobby administrator can create individual guest user accounts and passwords that last from one to several days, depending upon the length of stay for each guest.

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**.

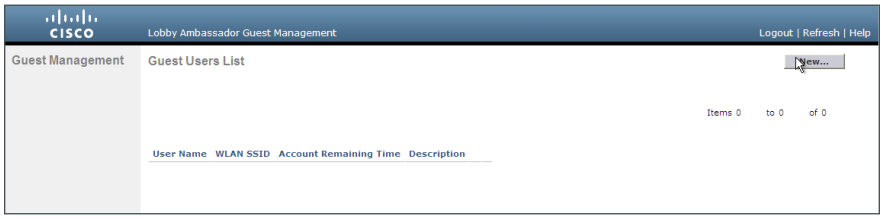


Procedure 9 Create guest accounts

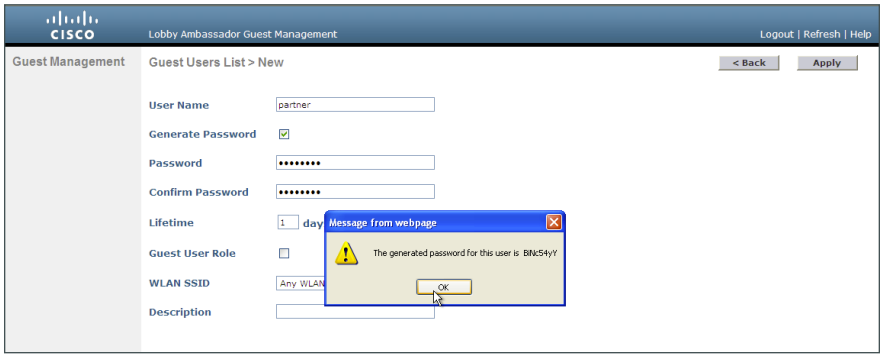
Now you can use the lobby administrator account to create usernames and passwords for partners, customers, and anyone else who is not normally granted access to your network.

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**.



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



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

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

PROCESS

Configuring Guest Wireless: Dedicated Guest Controller

1. Configure the DMZ switch connection to the Guest Anchor controller
2. Configure the firewall's DMZ interfaces for the Guest Anchor controller
3. Configure NAT
4. Configure Cisco ASA routing for dual-ISP environments
5. Create network objects
6. Configure dedicated guest anchor WLC security policy
7. Configure guest network security policy
8. Configure the DMZ WLC
9. Configure the time zone
10. Configure SNMP
11. Limit which networks can manage the WLC
12. Configure management authentication
13. Create the guest wireless LAN interface
14. Configure the guest WLAN on the AireOS Anchor Controllers
15. Configure anchor controller mobility group peers
16. Configure Cisco IOS-XE mobility groups
17. Create the lobby admin user account
18. Configure the internal WLCs for a guest
19. Create guest accounts

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.

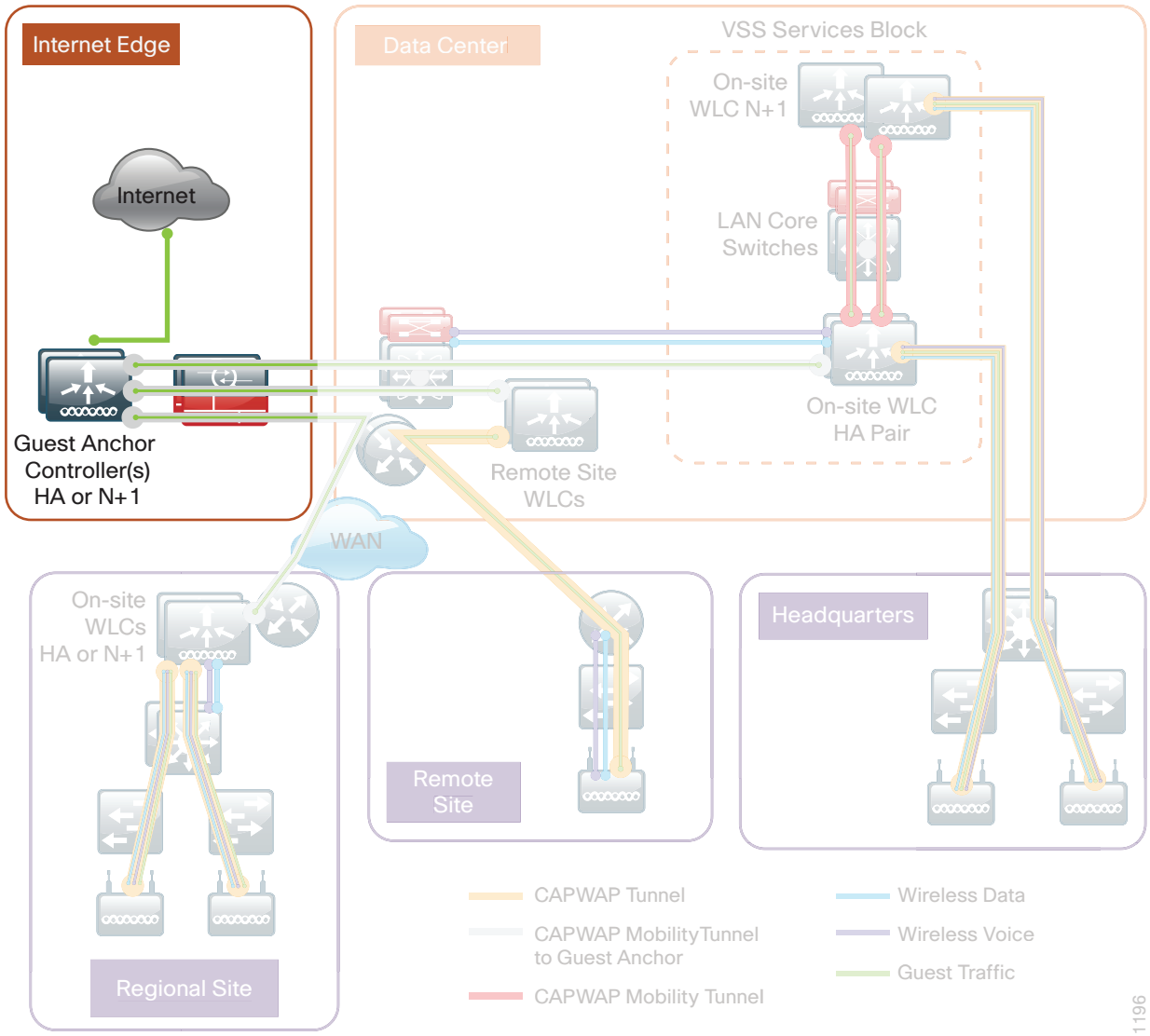
In a dedicated guest controller design, the dedicated anchor controller is connected to the DMZ interface of the Cisco ASA firewall. It therefore **requires** explicit access rules in the DMZ-based ASA appliance to do the following:

- 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



Procedure 1 Configure the DMZ switch connection to the Guest Anchor controller

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.

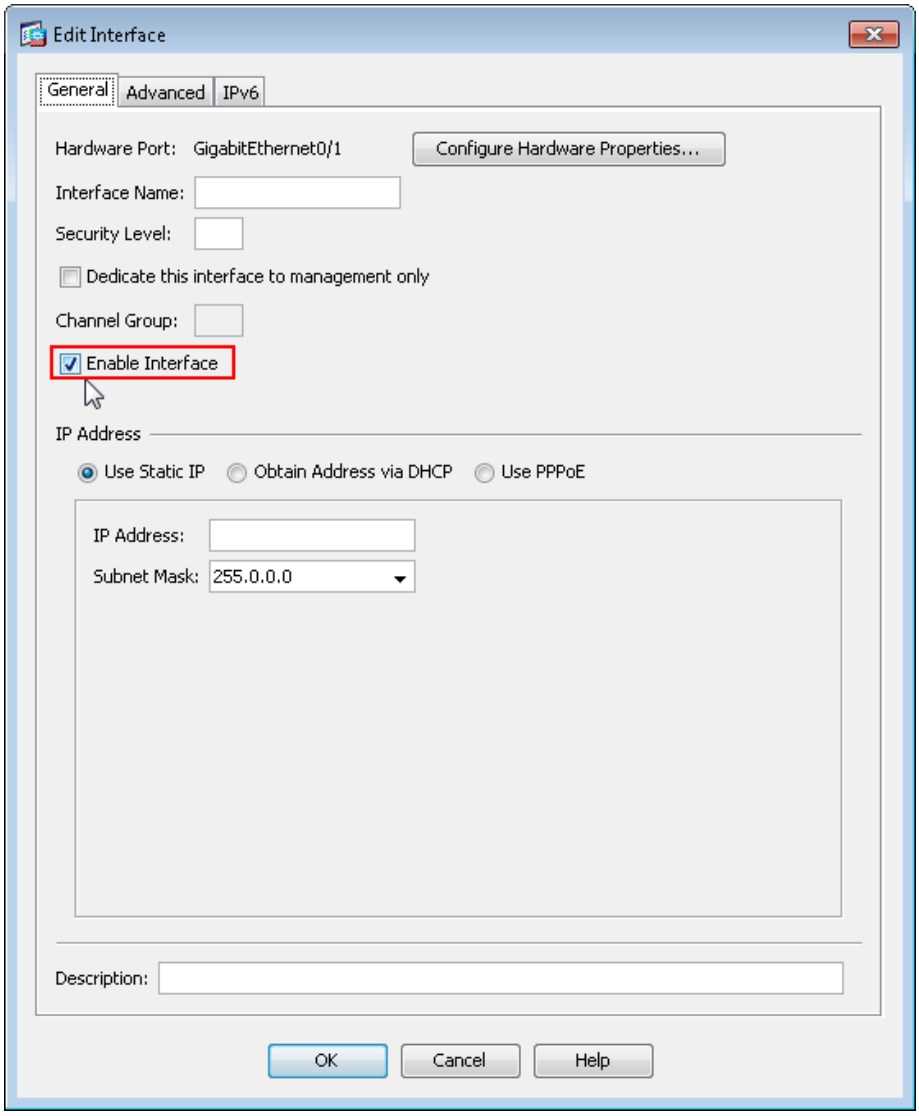
Table 20 - Cisco ASA DMZ interface information

Interface label	IP address/netmask	VLAN	Security level	Name
GigabitEthernet0/1.1119	192.168.19.1/24	1119	50	dmz-mgmt-wlan
GigabitEthernet0/1.1128	192.168.28.1/22	1128	10	dmz-guest-wlan

Step 1: Using a browser, access the Cisco ASA GUI. (Example: https://10.4.24.30)

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**.



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)

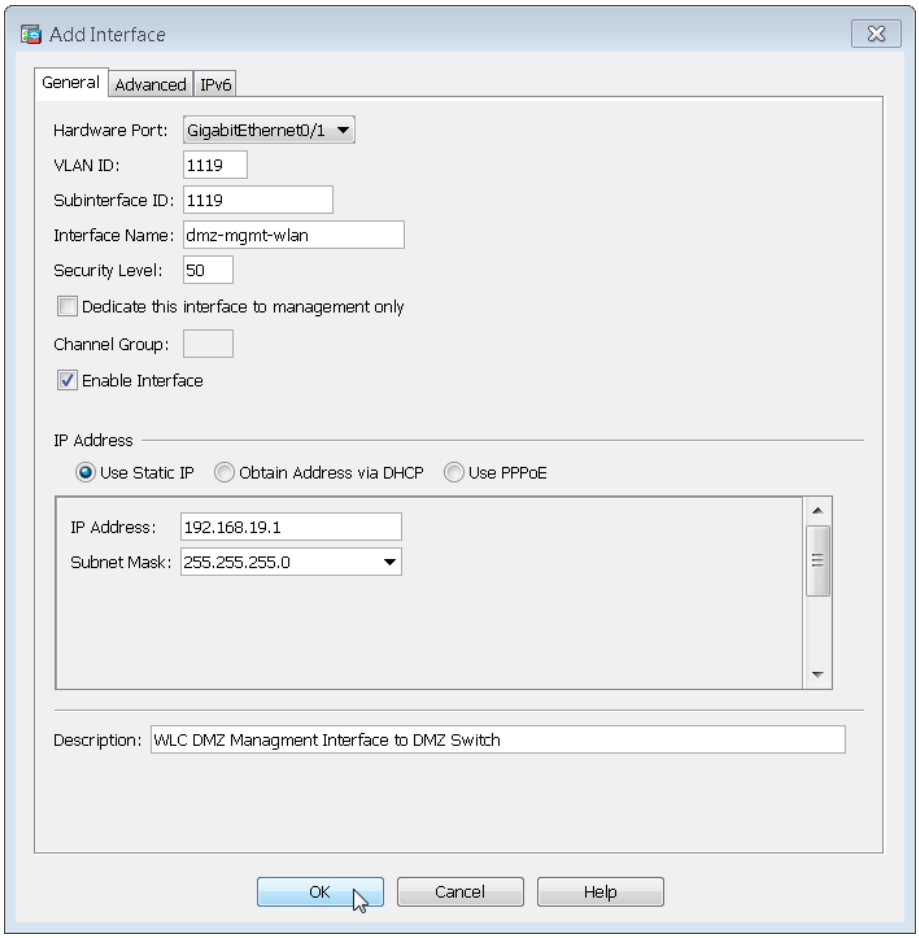
Step 7: In the **Subinterface ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1119)

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**.

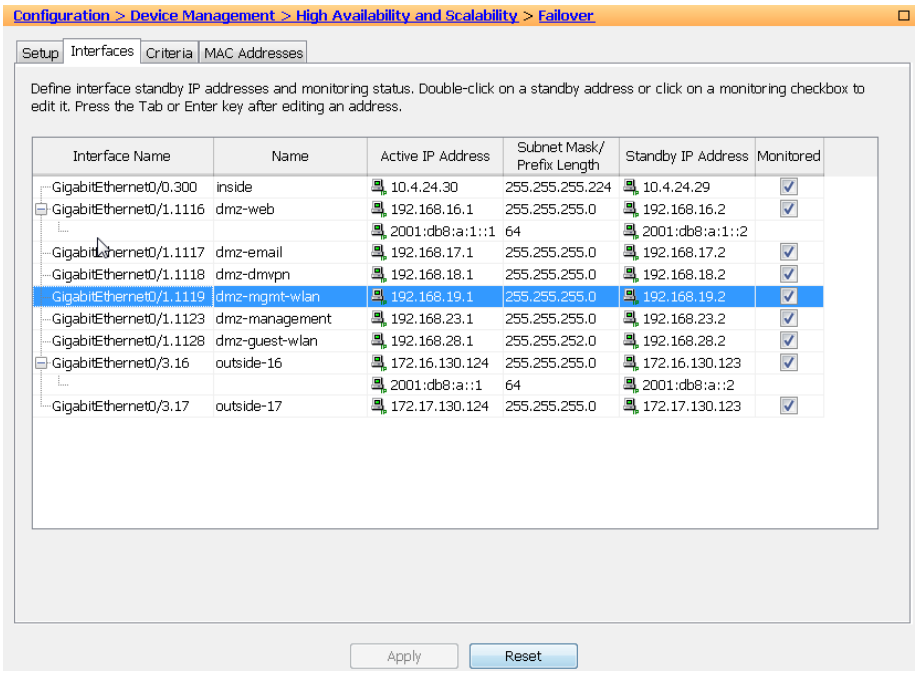


Step 12: On the Interface pane, click **Apply**.

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**.



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

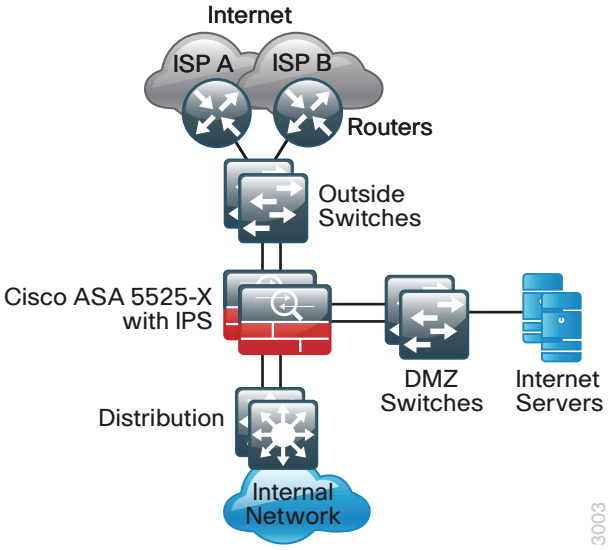


Table 21 - Wireless guest address mapping

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)

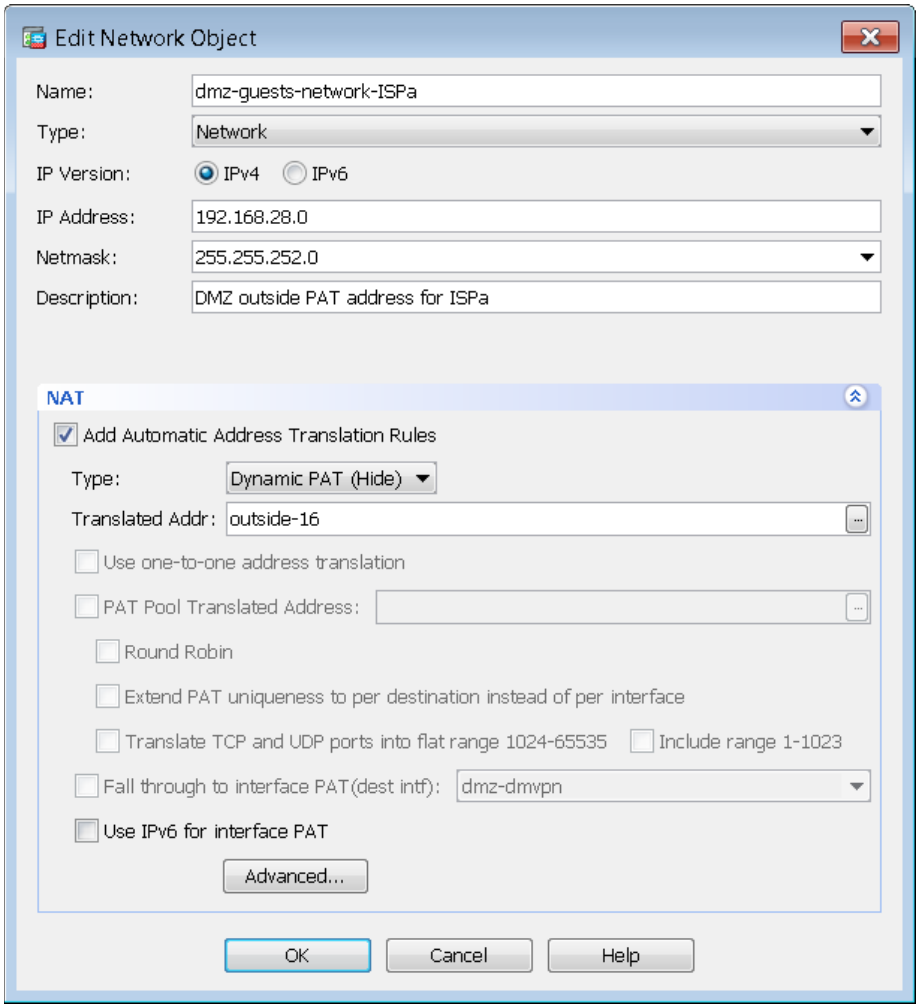
Step 6: In the **Netmask** box, enter the internal summary netmask. (Example: 255.255.252.0)

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)**.

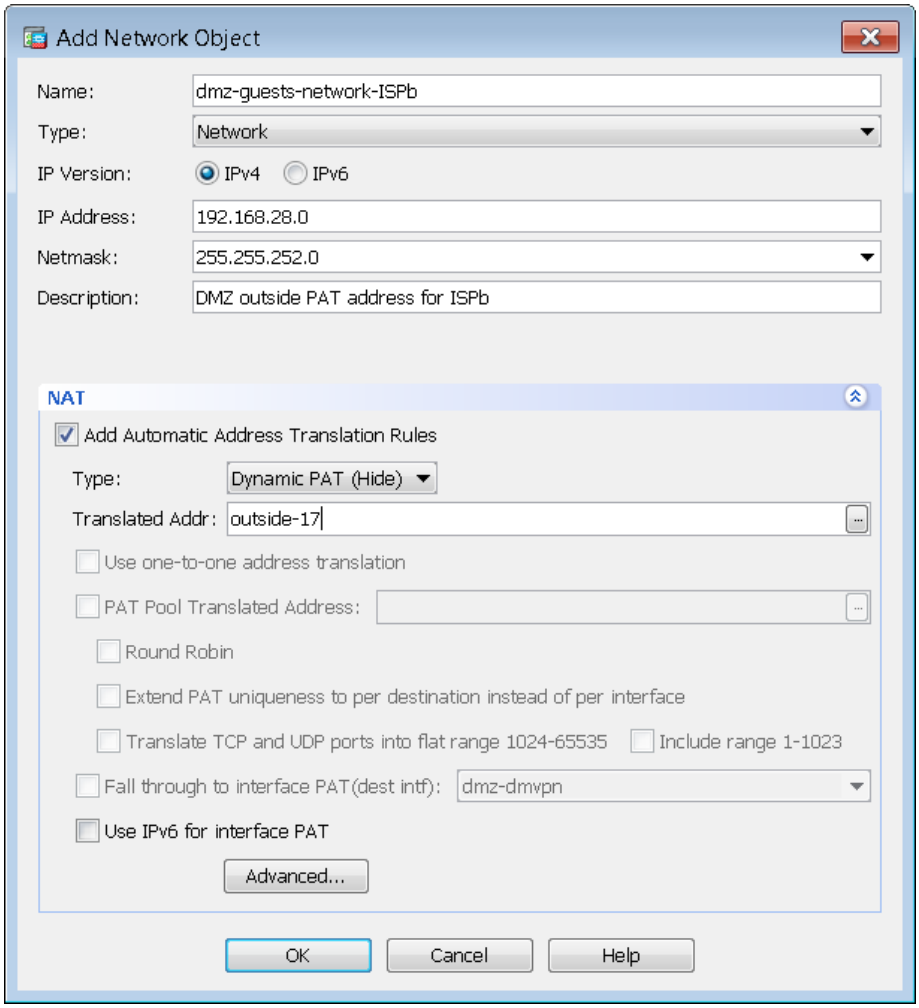
Step 10: In the **Translated Addr** box, enter the name of the primary Internet connection interface, and then click **OK**. (Example: outside-16, outside-17)



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)



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**.

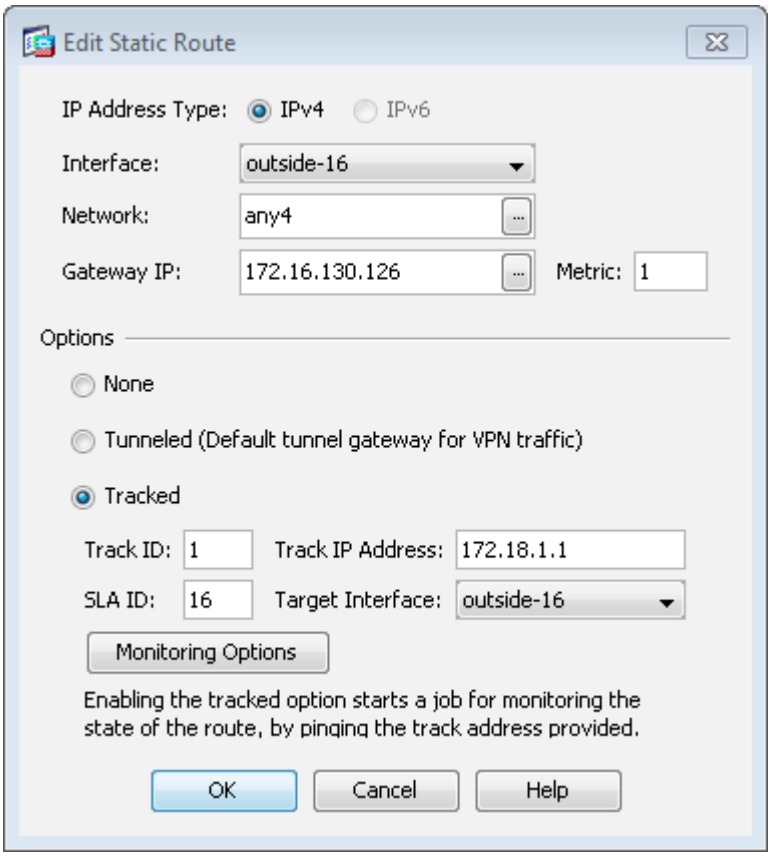
Step 4: In the Edit Static Route dialog box, in the **Options** pane, select **Tracked**.

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)



Step 9: On the Information dialog box, click **OK**.

Next, you create the secondary default route to the resilient Internet CPE's address.

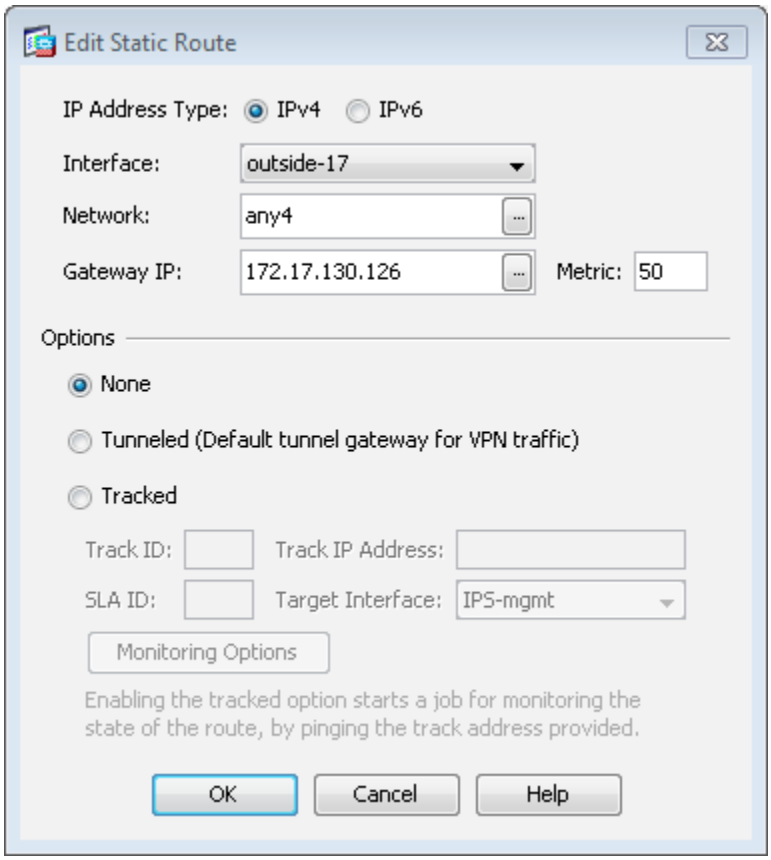
Step 10: In **Configuration > Device Setup > Routing > Static Routes**, click **Add**.

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**.



Step 15: On the Static Routes pane, click **Apply**.

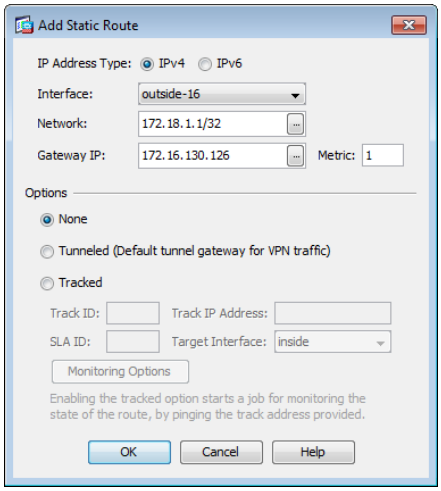
Next, you add a host route for the tracked object via the Internet-CPE-1 address. This assures that probes to the tracked object will always use the primary ISP connection.

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)

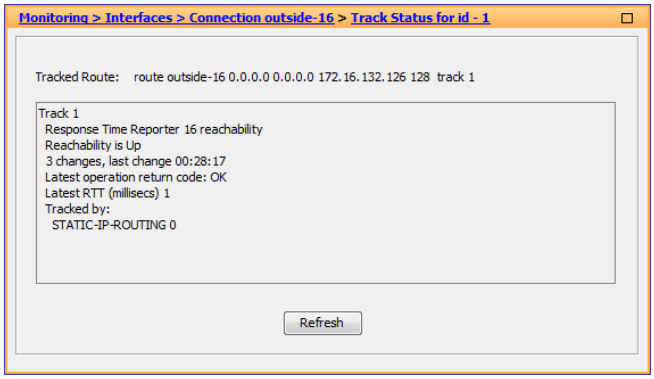
Step 19: In the **Gateway IP** box, enter the primary Internet CPE's IP address, and then click **OK**. (Example: 172.16.130.126)



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.

Reader Tip

The numbers and type of Wireless LAN Controllers in your environment will vary. The list below is inclusive of the WLCs in the test environment used to produce this CVD.

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.

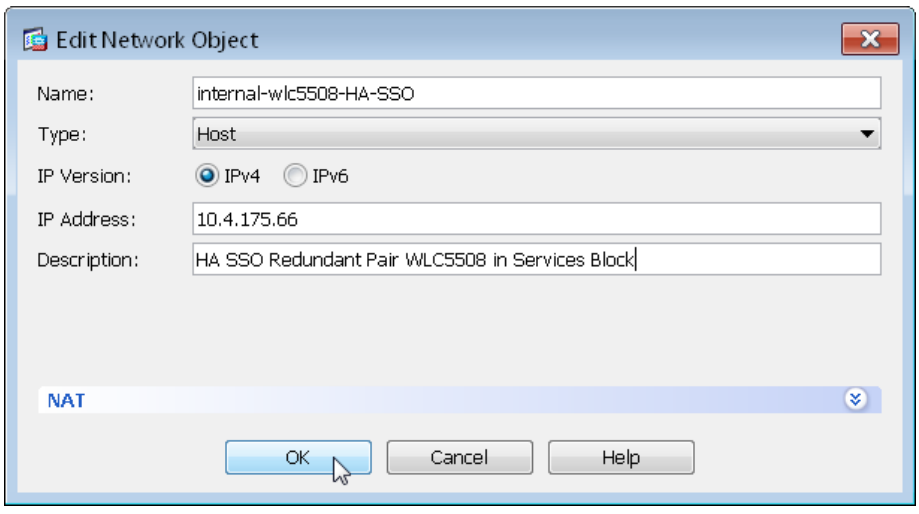
Step 3: Click **Add > Network Object**.

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)



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	

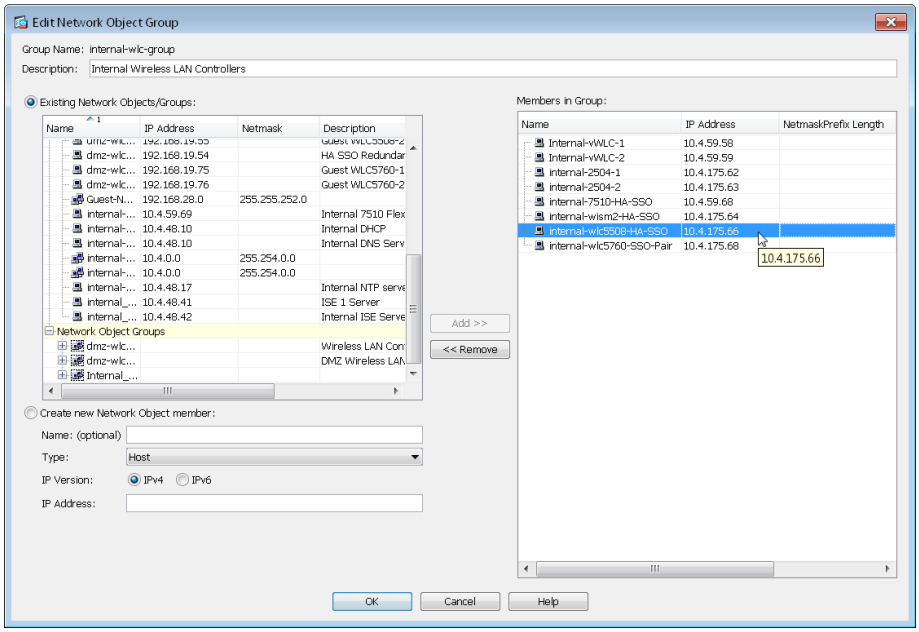
Step 7: Click **Add > Network Object Group**.

Step 8: Repeat 0 and Step 10 for each WLC Place in the Network from Table 23 (Example: internal-wlc-group)

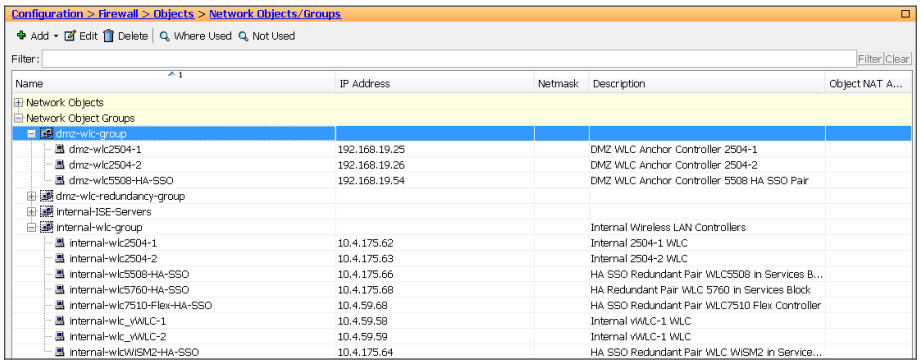
The Add Network Object Group dialog box appears.

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.



Step 11: Review the configured Network Object Groups for completeness, and then click **OK**.



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

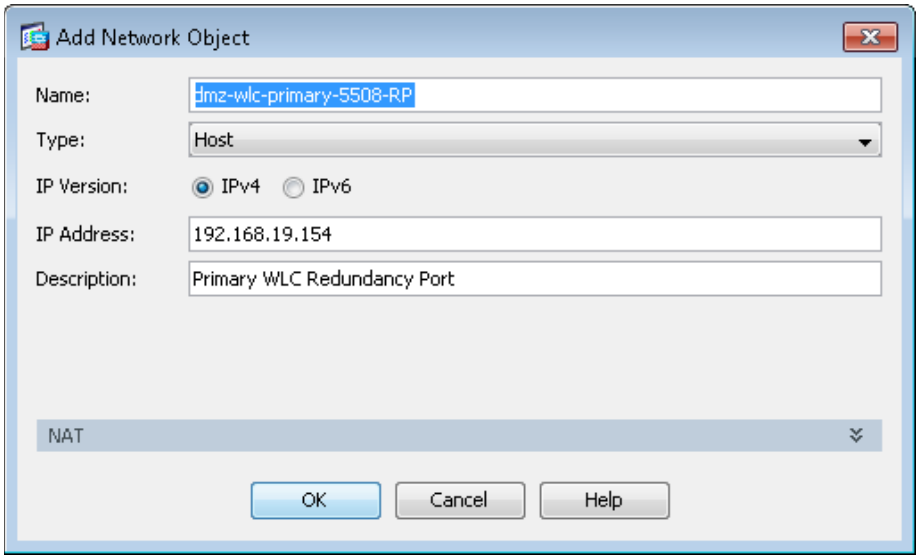
Step 12: Repeat steps Step 13 through Step 15 for each of the DMZ based HA SSO Redundancy Ports shown in Table 24.

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)

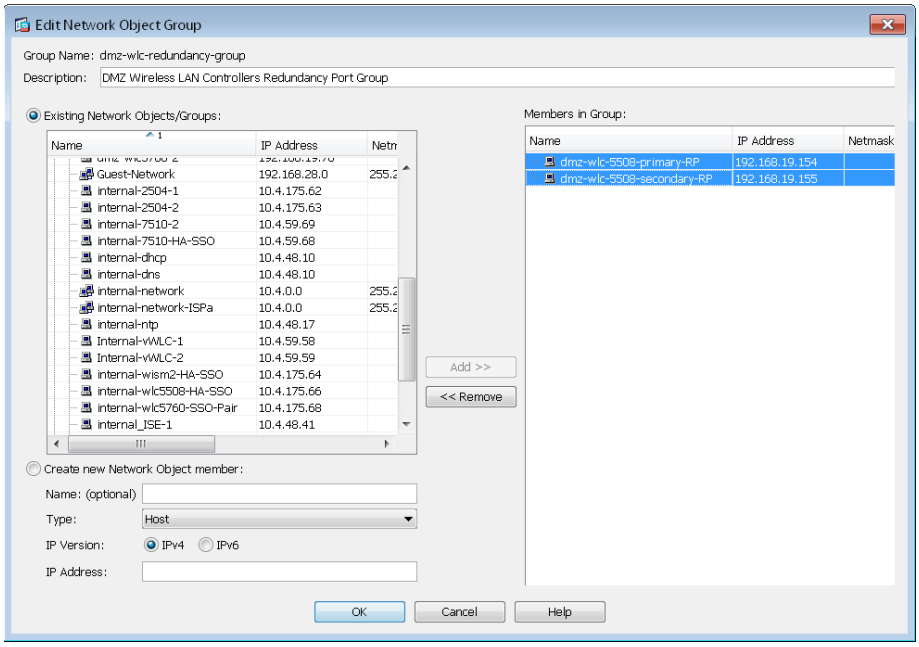


Next, to simplify the security policy configuration for each HA SSO based controller in the DMZ, you create a network object group that will contain each of the individual HA SSO WLCs within the DMZ.

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).



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.

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 communicate 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 communicate 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.

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)

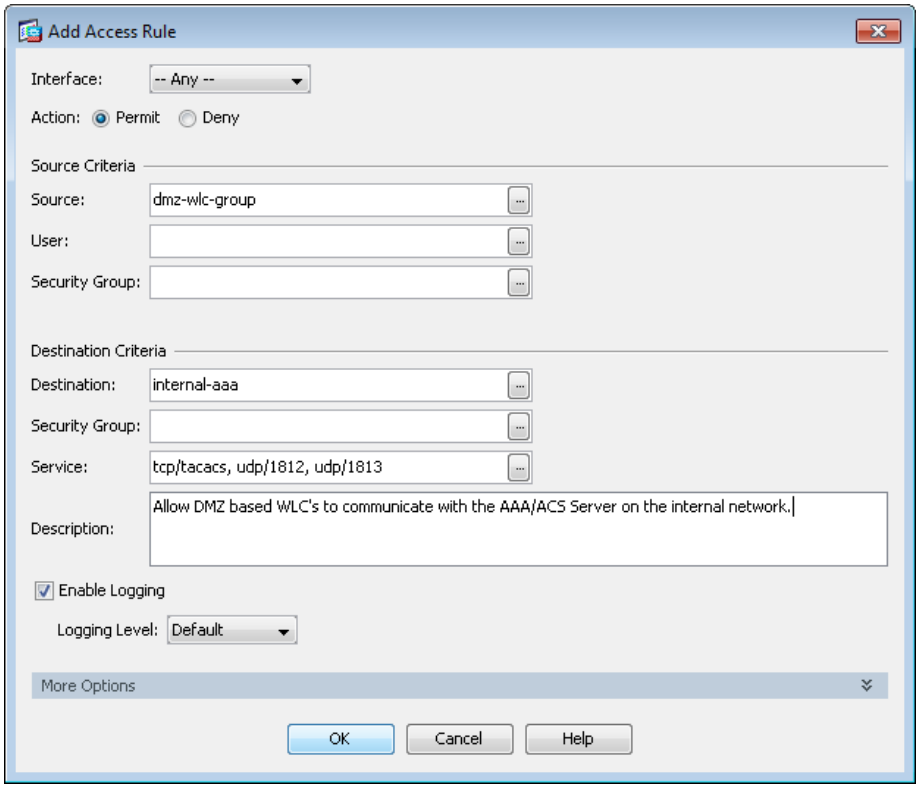
Step 8: In the **Destination** box, choose the destination. (Example: internal-aaa)

Step 9: In the **Service** box, enter the service. (Example: tcp/tacacs, udp/1812, udp/1813)

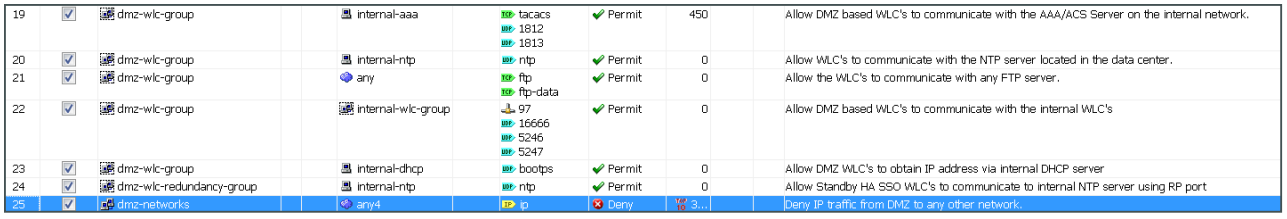
Step 10: In the **Description** box, enter a useful description.

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)



Step 13: After adding all of the rules and in the order listed in Table 26, click **Apply** on the Access Rules pane.



19	✓	dmz-wlc-group	internal-aaa	tacacs 1812 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	✓	dmz-wlc-group	any	ftp ftp-data	Permit	0		Allow the WLC's to communicate with any FTP server.
22	✓	dmz-wlc-group	internal-wlc-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	✓	dmz-wlc-redundancy-group	internal-ntp	ntp	Permit	0		Allow Standby HA SSO WLC's to communicate to internal NTP server using RP port
25	✓	dmz-networks	any4	ip	Deny	3...		Deny IP traffic from DMZ 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.

Table 27 - Guest network policy 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	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

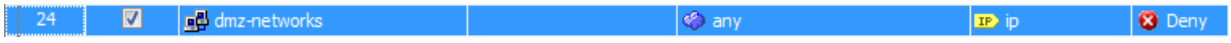
Step 1: On the Internet edge ASA appliance, navigate to **Configuration > Firewall > Access Rules**.

Step 2: Repeat Step 3 through Step 12 for all rules listed in Table 27.

Tech Tip

Step 3 is important for keeping keep the rules in the correct order

Step 3: Click the rule that denies traffic from the DMZ toward other networks.



> **Caution**
>
> 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)

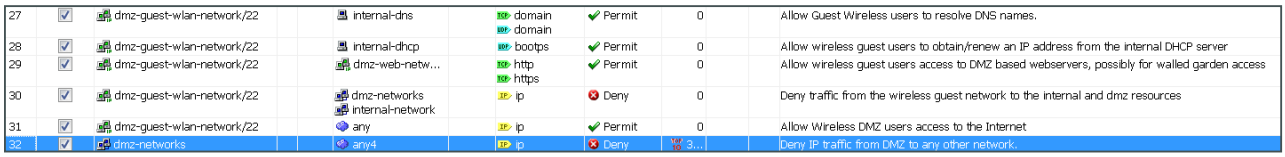
Step 9: In the **Service** box, enter the service. (Example: tcp/domain, udp/domain)

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	☑	dmz-guest-wlan-network/22	internal-dns	domain domain	Permit	0	Allow Guest Wireless users to resolve DNS names.
28	☑	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	☑	dmz-guest-wlan-network/22	dmz-web-netw...	http https	Permit	0	Allow wireless guest users access to DMZ based webservers, possibly for walled garden access
30	☑	dmz-guest-wlan-network/22	dmz-networks internal-network	ip	Deny	0	Deny traffic from the wireless guest network to the internal and dmz resources
31	☑	dmz-guest-wlan-network/22	any	ip	Permit	0	Allow Wireless DMZ users access to the Internet
32	☑	dmz-networks	any4	ip	Deny	3...	Deny IP traffic from DMZ to any other network.

Procedure 8 Configure the DMZ WLC

Configure the HA SSO based DMZ wireless LAN guest anchor controller by using the following values.

Table 28 - Cisco DMZ wireless controller parameters checklist

Parameter	CVD values primary controller	CVD values resilient controller	Site-specific values
Controller parameters			
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 management 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 administrator 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	

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

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: 255.255.255.0
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
```

> **Tech Tip**
>
> The DMZ-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. Generally, each WLC providing multicast services using the multicast-multicast method 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
```

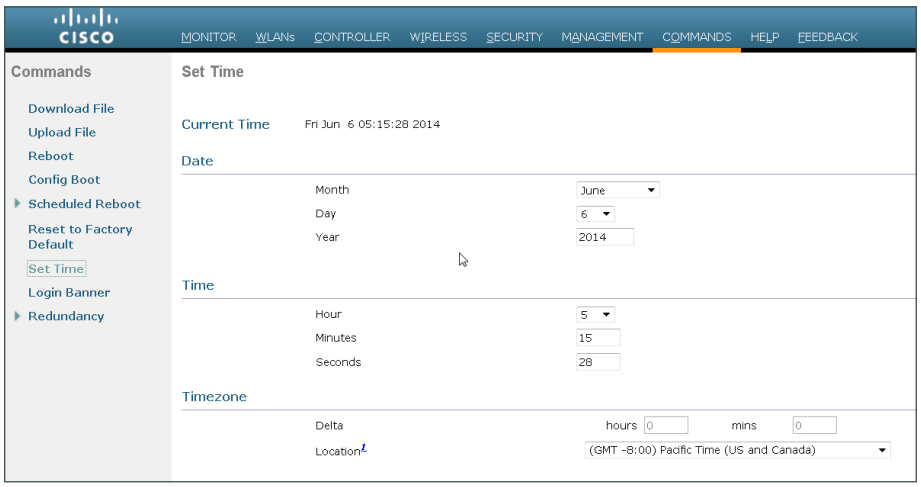
Step 19: After the WLC has reset, log in to the Cisco Wireless LAN Controller Administration page by using the credentials defined in Step 3. (Example: https://**dmz-wlc-guest.cisco.local**/)

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**.



Procedure 10 Configure SNMP

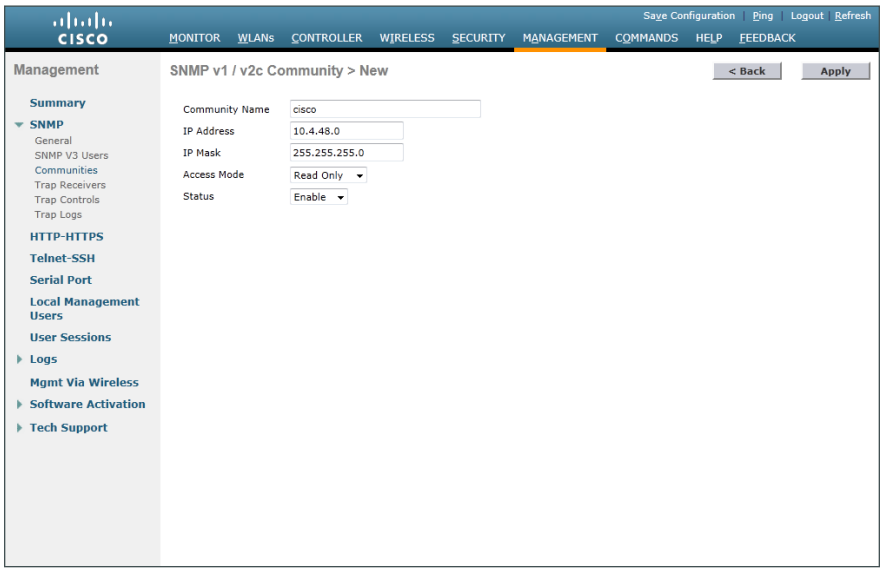
Step 1: In **Management > SNMP > Communities**, click **New**.

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)

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



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

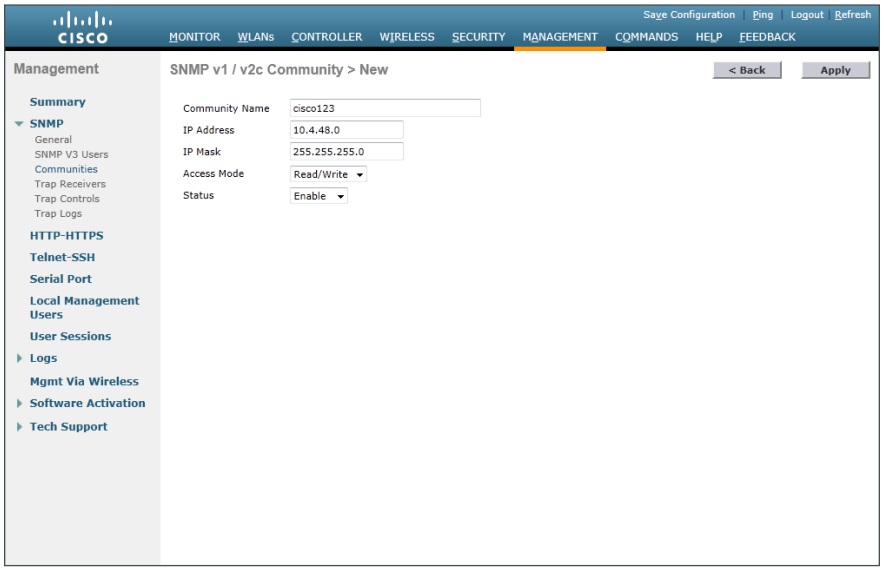
Step 7: Enter the **Community Name**. (Example: cisco123)

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**.

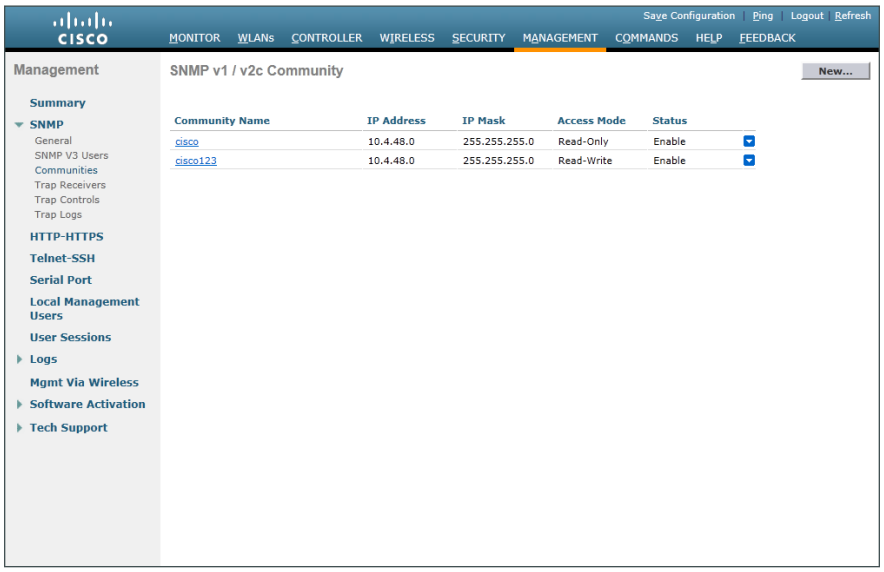


Step 12: Navigate to **Management > SNMP > Communities**.

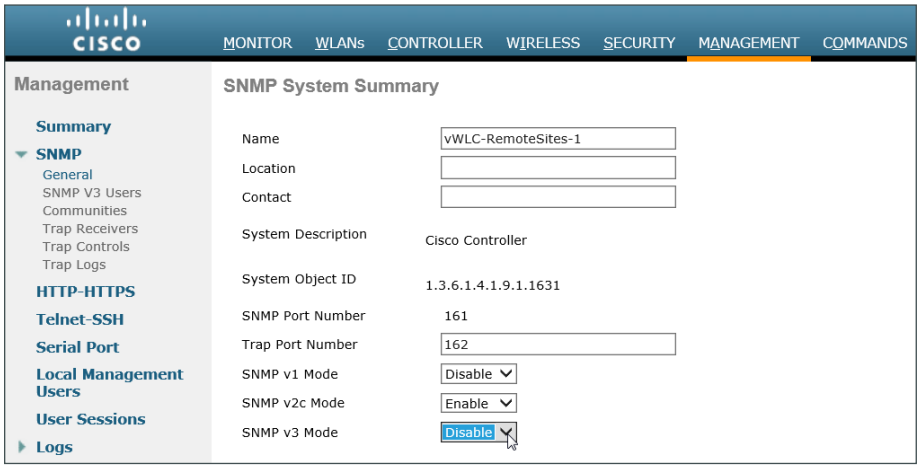
Point to the blue box for the **public** community, and then click **Remove**.

Step 13: On the "Are you sure you want to delete?" message, click **OK**.

Step 14: Repeat Step 12 and Step 13 for the **private** community.

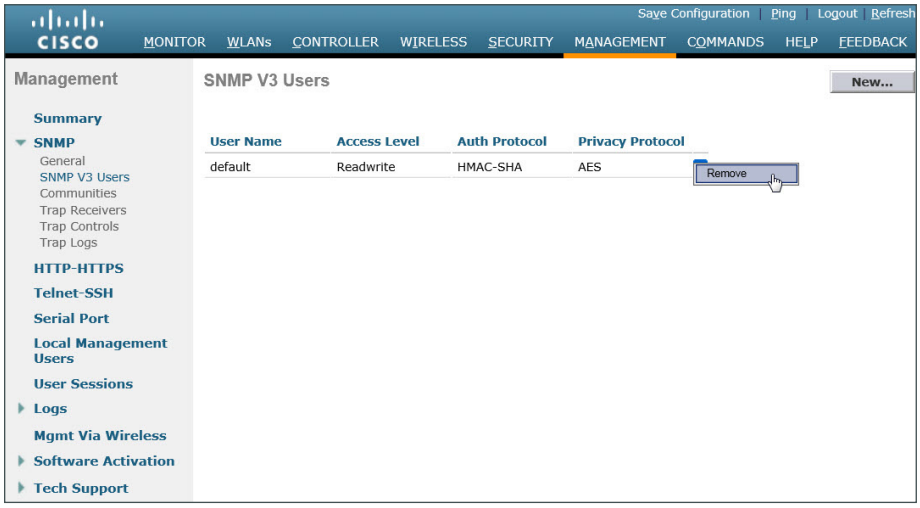


Step 15: Navigate to **Management > SNMP > General** and disable SNMP v3 Mode, and then press **Apply**.

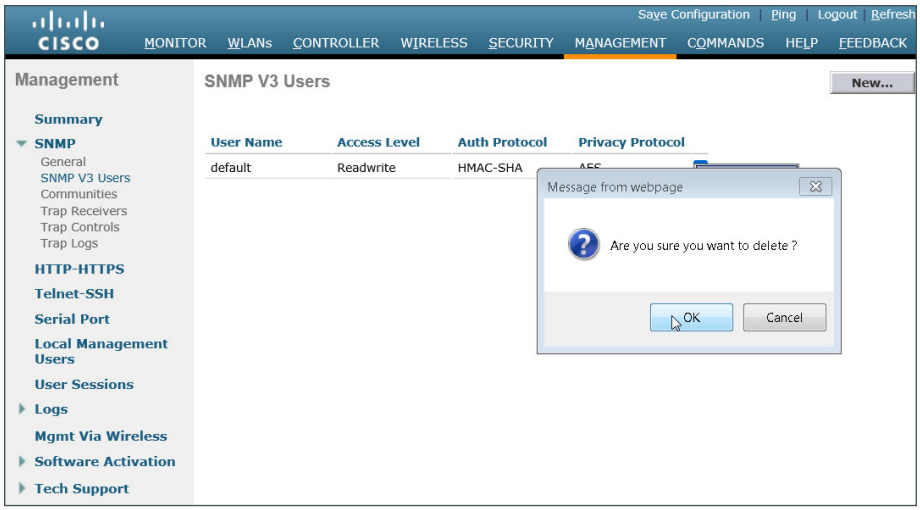


Step 16: Navigate to **Management > SNMP Communities > SNMP V3 Users**.

Step 17: On the right side of the **default** User Name, point and click the blue down arrow, and then click **Remove**.



Step 18: Press **OK** to confirm that you are sure you want to delete, then press **Save Configuration**.



Tech Tip

Changes 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.

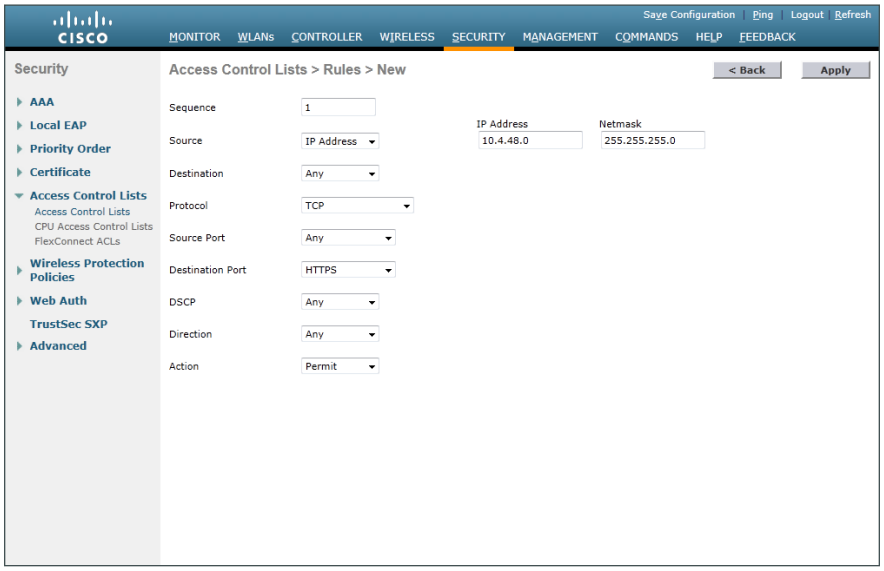
Step 1: In **Security > Access Control Lists > Access Control Lists**, click **New**.

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**.

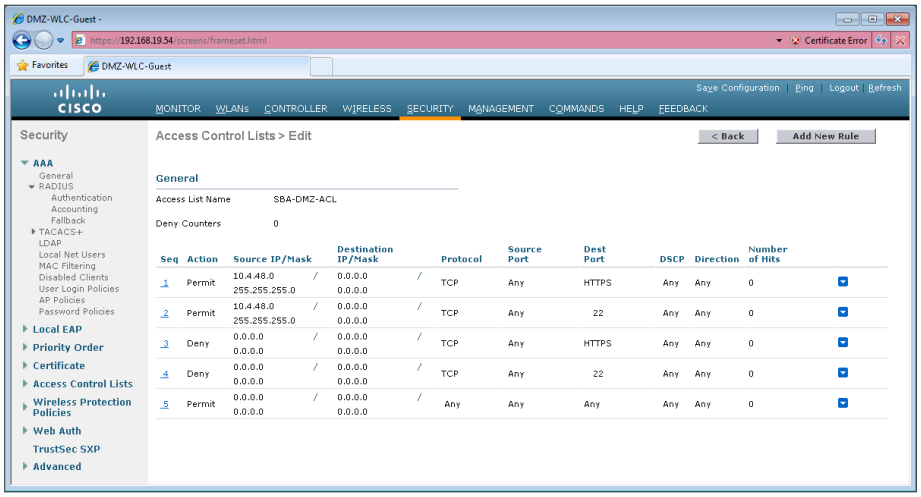
- Sequence–**1**
- Source–**10.4.48.0 / 255.255.255.0**
- Destination–**Any**
- Protocol–**TCP**
- Destination Port–**HTTPS**
- Action–**Permit**



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	TCP	Any	Other/22	Permit
3	Any	Any	TCP	Any	HTTPS	Deny
4	Any	Any	TCP	Any	Other/22	Deny
5	Any	Any	Any	Any	Any	Permit



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

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

Procedure 12 Configure management authentication

(Optional)

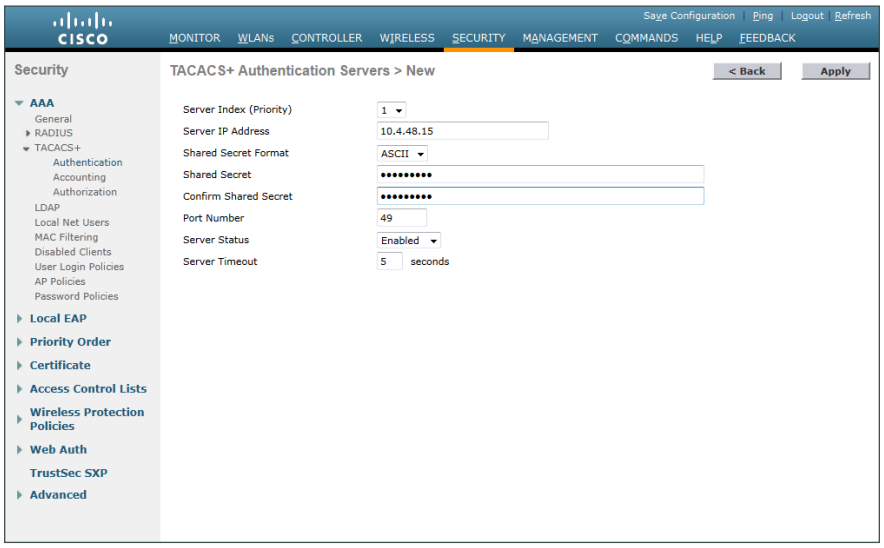
You can use this procedure to deploy centralized management authentication by configuring an authentication, authorization and accounting (AAA) service using Cisco Secure ACS. If you prefer to use local management authentication, skip to Procedure 13.

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)

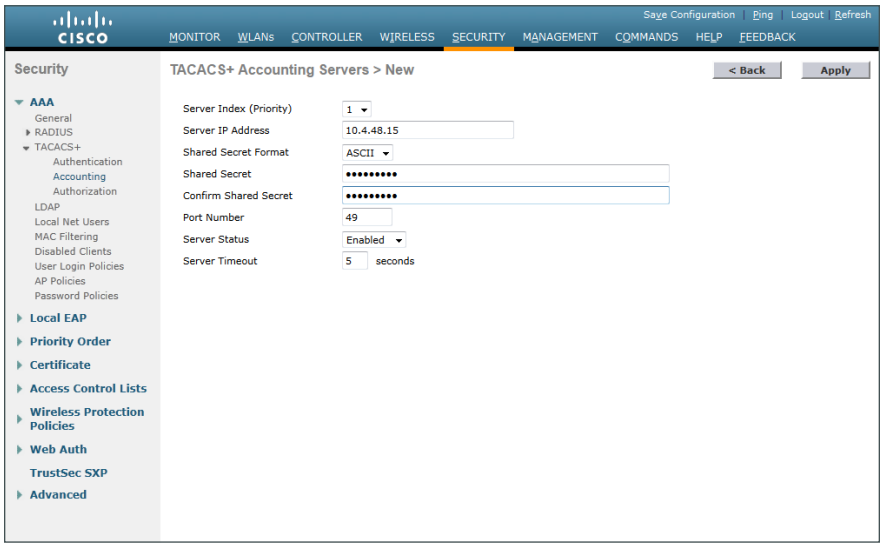
Step 3: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)



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

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

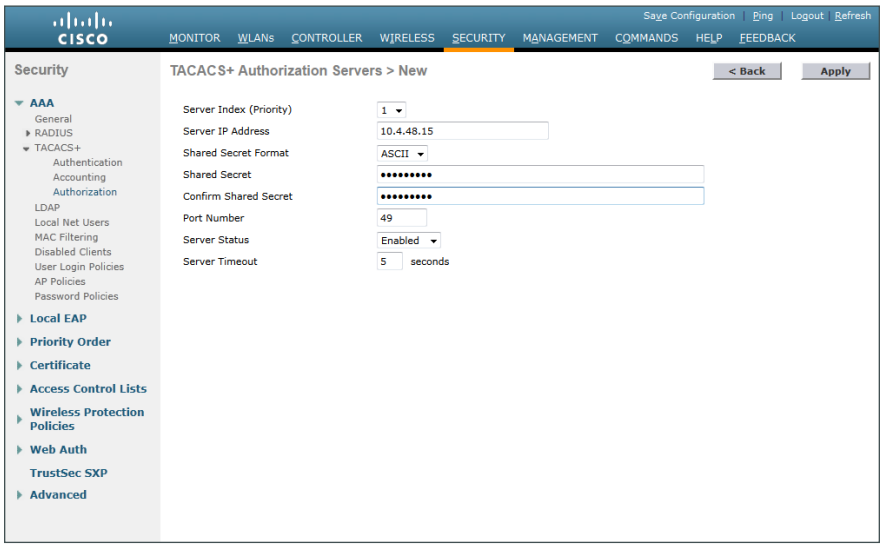
Step 6: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)



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)

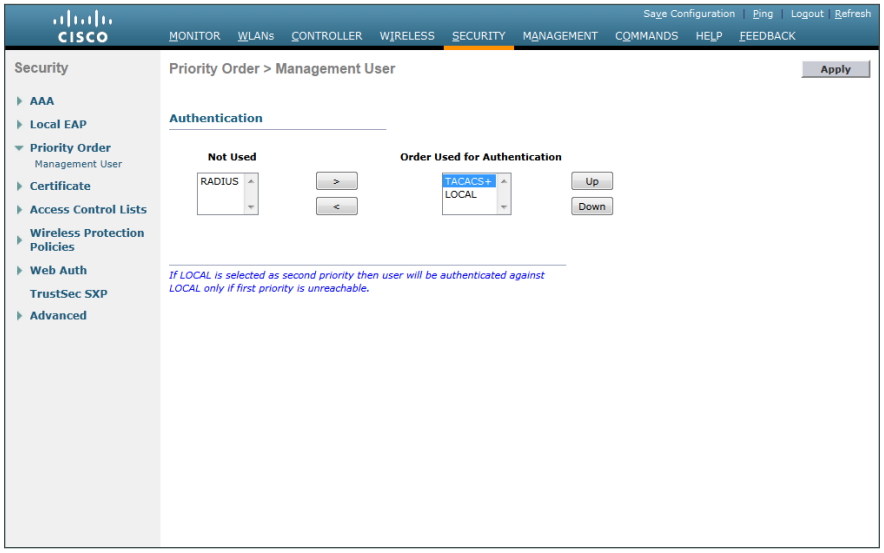


Step 10: Navigate to **Security > Priority Order > Management User**.

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

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

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



Tech Tip

If 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

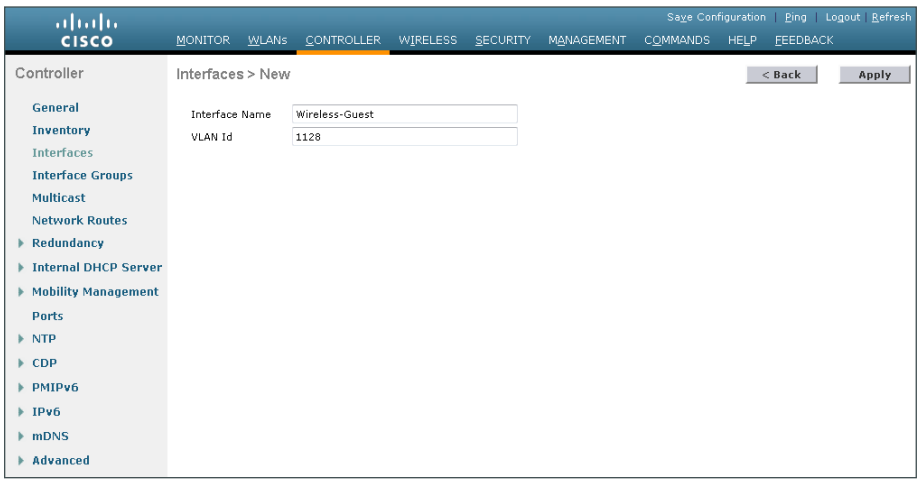
The guest wireless interface is connected to the DMZ of the Cisco ASA 5545X security appliance. This allows guest wireless traffic only to and from the Internet. All guest traffic, regardless of the controller to which the guest initially connects, is tunneled to the guest WLC and leaves the controller 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)

Step 3: Enter the **VLAN Id**, and then click **Apply**. (Example: 1128)

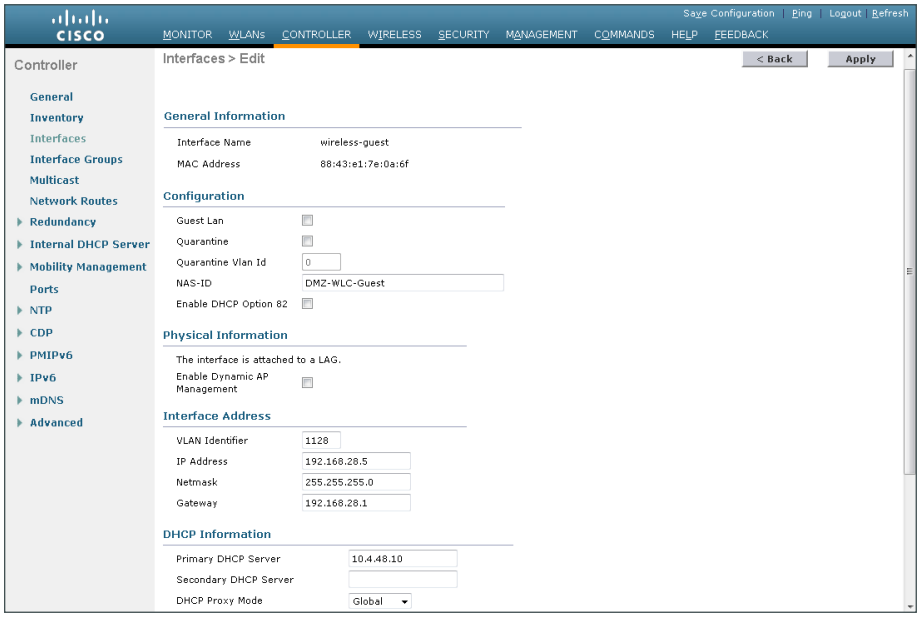


Step 4: In the **IP Address** box, enter the IP address to assign to the WLC interface. (Example: 192.168.28.5)

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)



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.

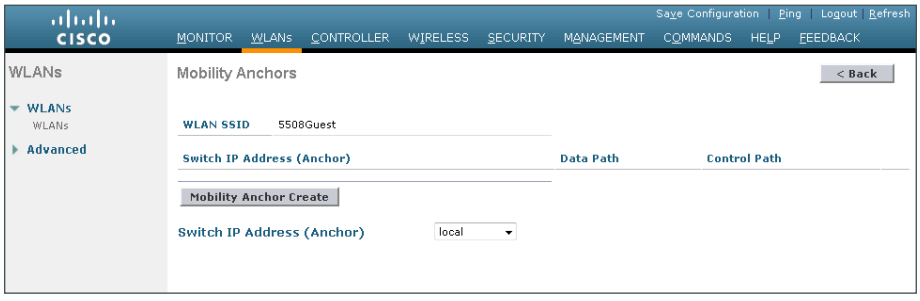
Procedure 14 Configure the guest WLAN on the AireOS Anchor Controllers

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)**.

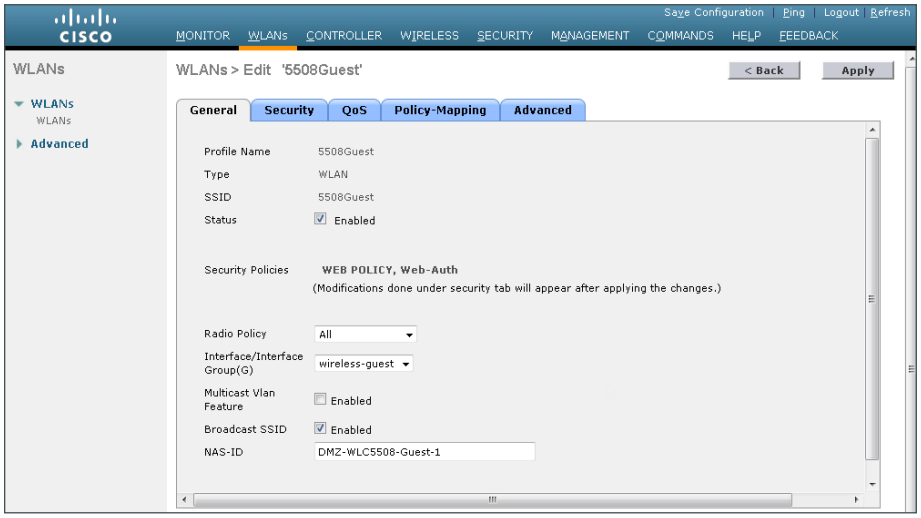
Step 4: Click **Mobility Anchor Create**, and then click **OK**.



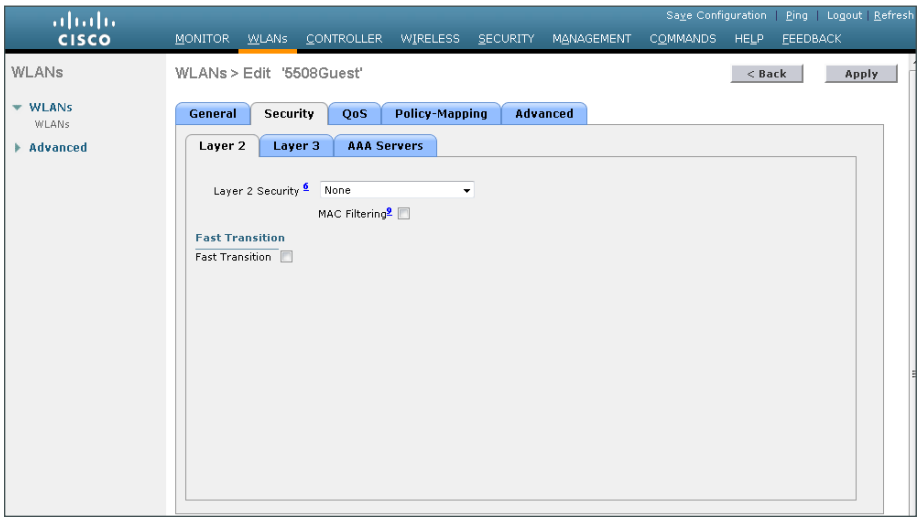
Step 5: Click **Back**.

Step 6: Click the **WLAN ID** of the SSID created in Procedure 8. (Example: 5508Guest)

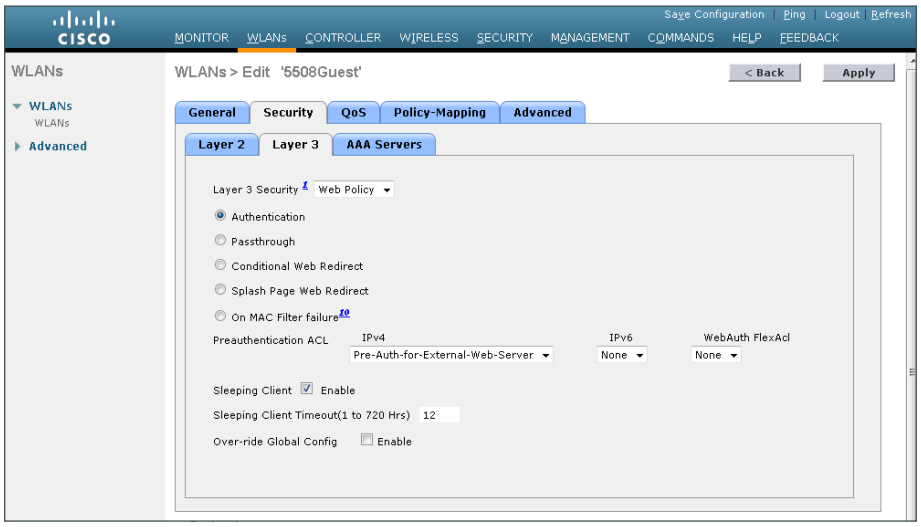
Step 7: On the General tab, in the **Interface/Interface Group(G)** list, choose the interface created in Procedure 13. (Example: wireless-guest)



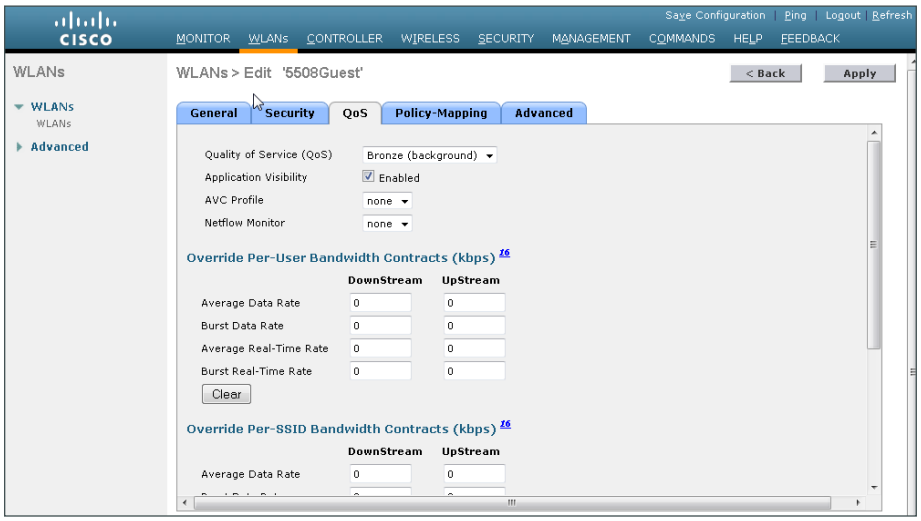
Step 8: Click the **Security** tab, and then on the Layer 2 tab, in the **Layer 2 Security** list, choose **None**.



Step 9: On the Layer 3 tab, select **Web Policy**, and then click **OK**.



Step 10: On the QoS tab, in the **Quality of Service (QoS)** list, choose **Bronze (background)**, select **Enable** next to Application Visibility, click **Apply**, and then click **OK**.



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.

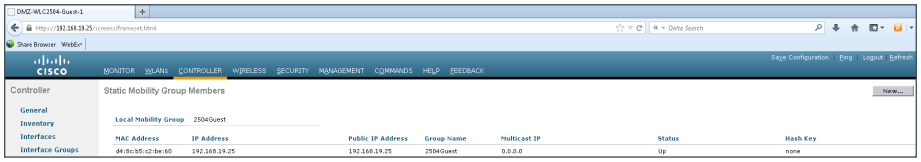
If you are using a pair of Cisco 5508 Series Wireless Controllers in an N+1 configuration instead of HA SSO, or if you are using a pair of Cisco 2504 Series Wireless Controllers, you need to add each of the WLCs to a common mobility group.

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.



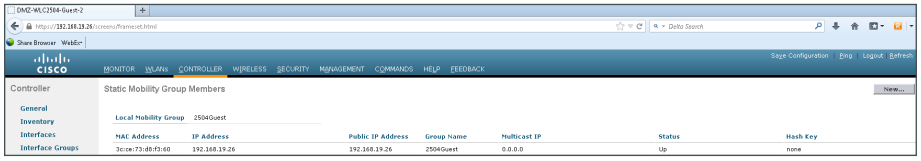


Table 30 - Internet edge anchor controller values

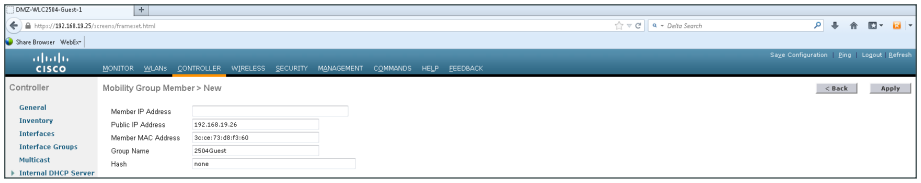
WLC name & Location	WLC and HA Type	MAC address	IP address	Mobility group name
DMZ-WLC2504-Guest-1 / DMZ	2504 N+1	d4:8c:b5:c2:be:60	192.168.19.25	2504Guest
DMZ-WLC2504-Guest-2 / DMZ	2504 N+1	3c:ce:73:d8:f3:60	192.168.19.26	2504Guest

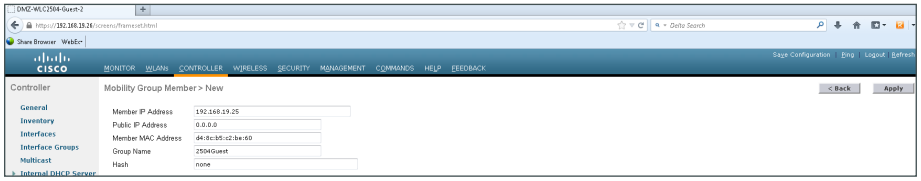
Step 3: On each DMZ-based anchor controller that is using an N+1 redundancy model, navigate to **Controller > Mobility Management > Mobility Groups**, and then click **New**.

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)

Step 6: In the **Group Name** box, enter the mobility group name configured on the guest controller, and then click **Apply**. (Example: 2504Guest)





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**.

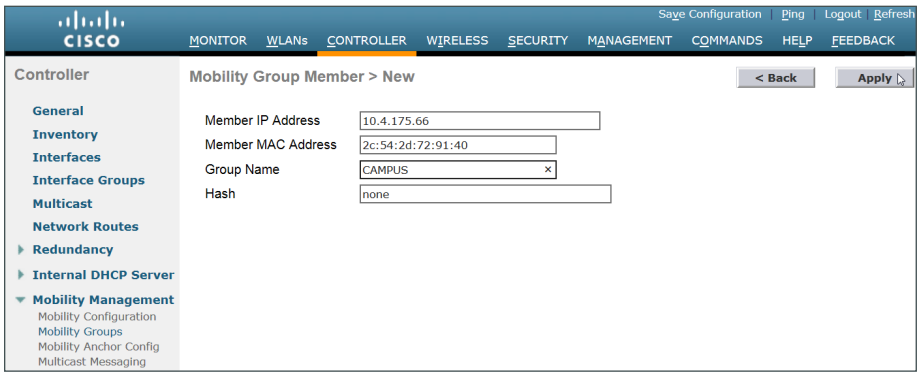
Step 8: In the **Member IP Address** box, enter the IP address of a campus or remote-site foreign anchor controller. (Example: 10.4.175.66)

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)

Tech Tip

There are a number of ways to find the MAC address on a Cisco AireOS controller. One method is to navigate to **Controller > Inventory**. There you will see the burned-in MAC Address. Alternately you can obtain the MAC address by navigating to **Controller > Mobility Management > Mobility Groups** and locating the local peer entry.



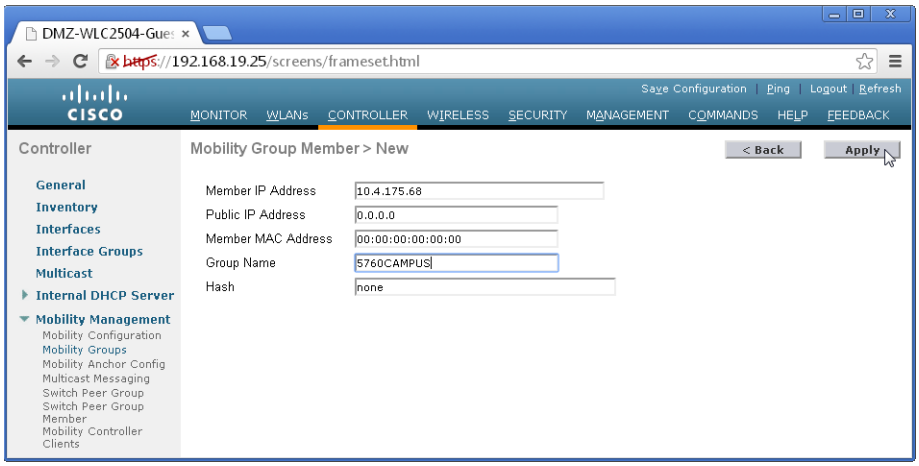
Step 11: On each controller, click **Save Configuration**, and then click **OK**.

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).

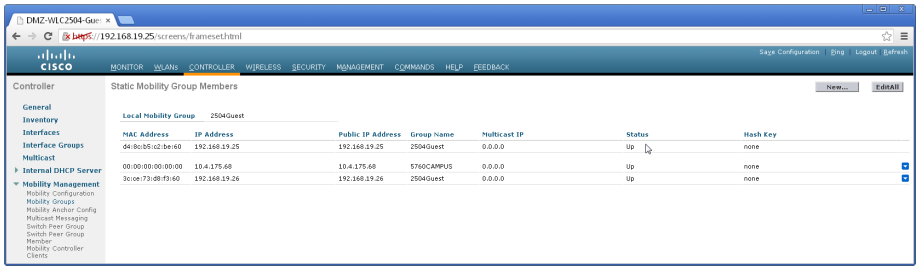
Step 15: In the **Group Name** box, enter the mobility group configured on the Cisco 5760 Series foreign anchor controller (Example: 5760CAMPUS), click **Apply**, and then click **Save Configuration**.

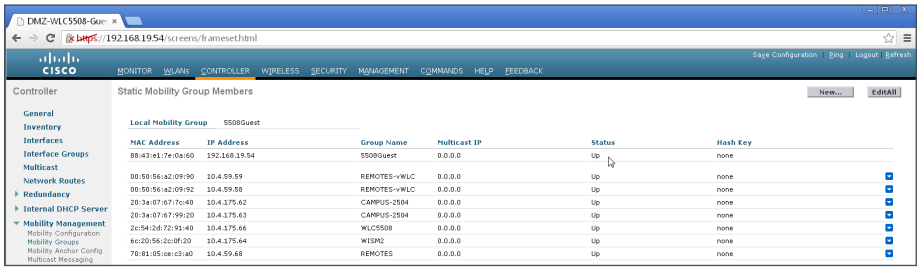


Tech Tip

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**.





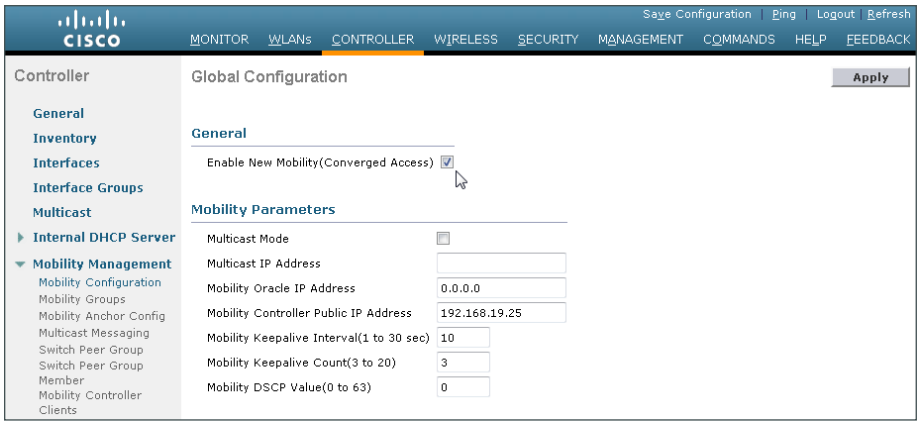
Procedure 16 Configure Cisco IOS-XE mobility groups

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.

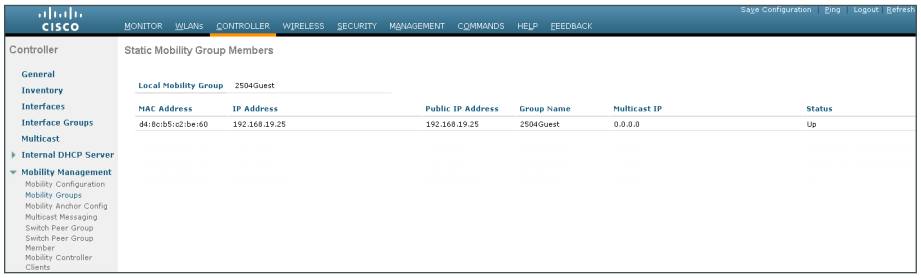
On each of the Cisco 2504 Series DMZ anchor controller(s), enable New Mobility (Converged Access).

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).



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.



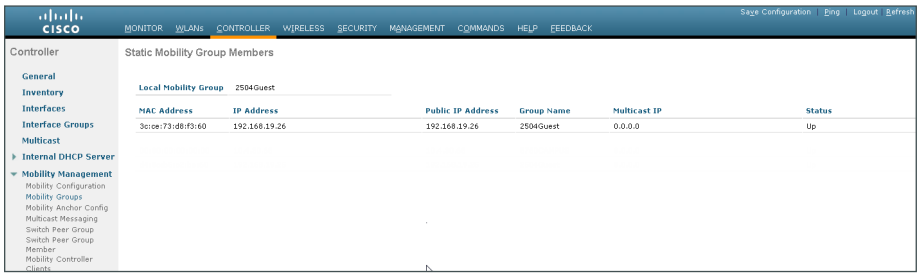


Table 31 - Internet edge anchor controller values

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

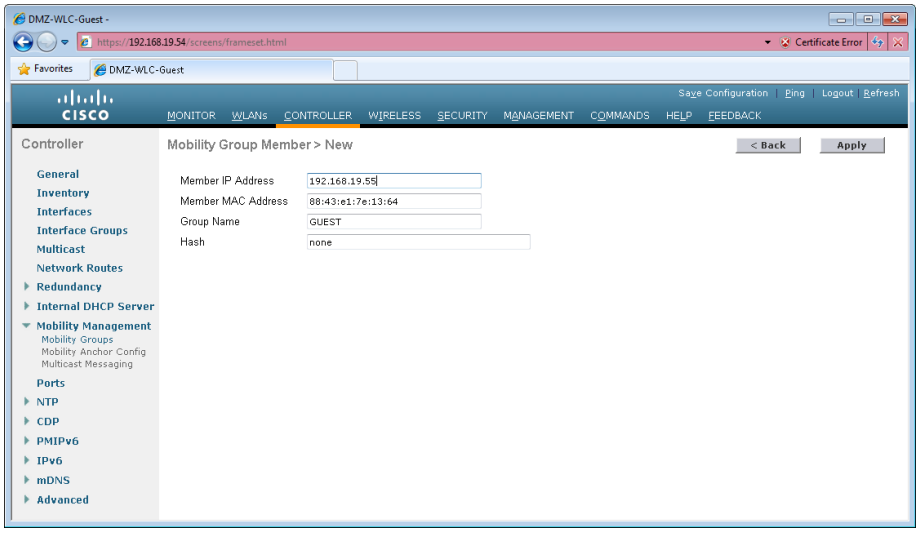
Next, allow the DMZ-based 2504 N+1 anchor controller pair to share mobility information by creating a common mobility group. Perform the following steps on each anchor controller.

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)

Step 7: In the **Group Name** box, enter the mobility group name configured on the guest controller, and then click **Apply**. (Example: Guest)

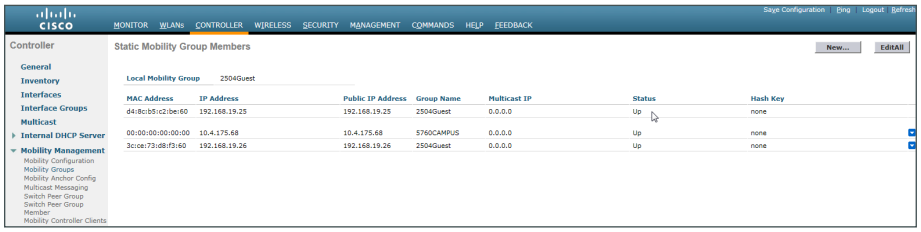


Step 8: On both of the DMZ guest anchor controllers, navigate to **Controller > Mobility Management > Mobility Groups**, and then click **New**.

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)

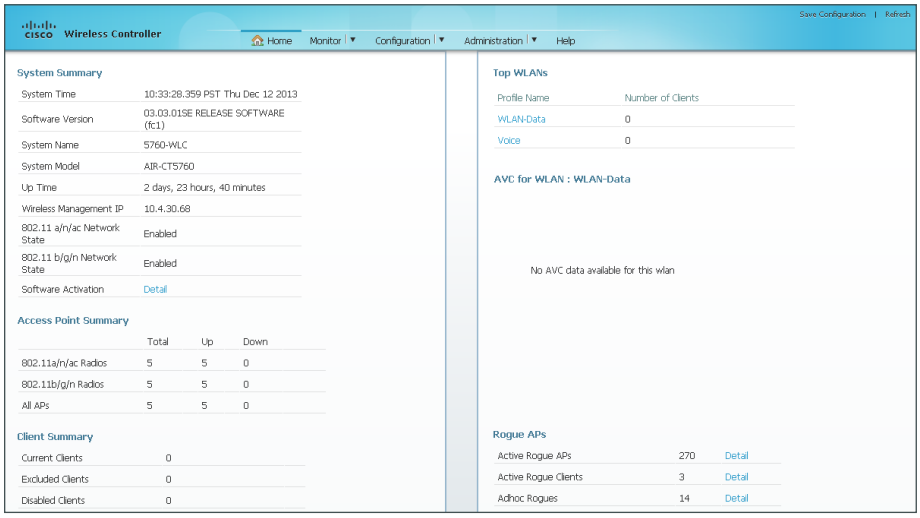


Tech Tip

The controller 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 communication to utilize CAPWAP as opposed to Ethernet over IP (EoIP).

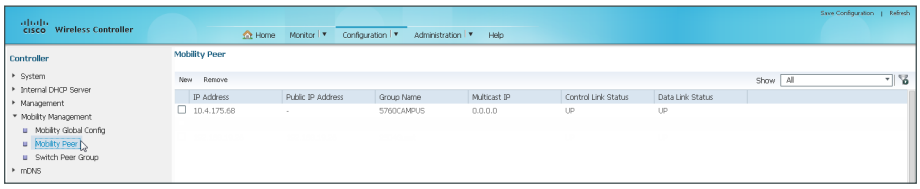
Step 12: On each controller, click **Save Configuration**, and then click **OK**.

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)



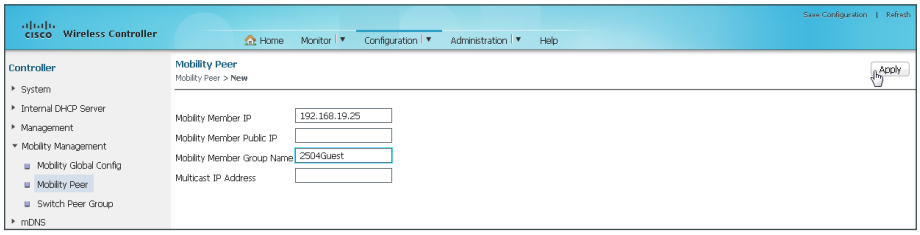
Next, create a new mobility peer to the DMZ-based Cisco 2504 Series anchor controller.

Step 14: Navigate to **Configuration > Controller > Mobility Management > Mobility Peer**, and then click **New**.



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).

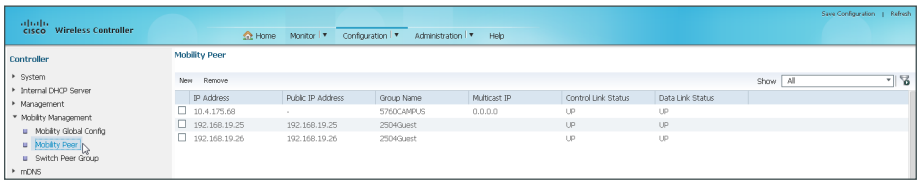
Step 16: In the **Mobility Member Group Name** box, enter the mobility group name as defined on the DMZ-based Cisco 2504 Series anchor controller (Example: 2504Guest), and then click **Apply**.



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.



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."

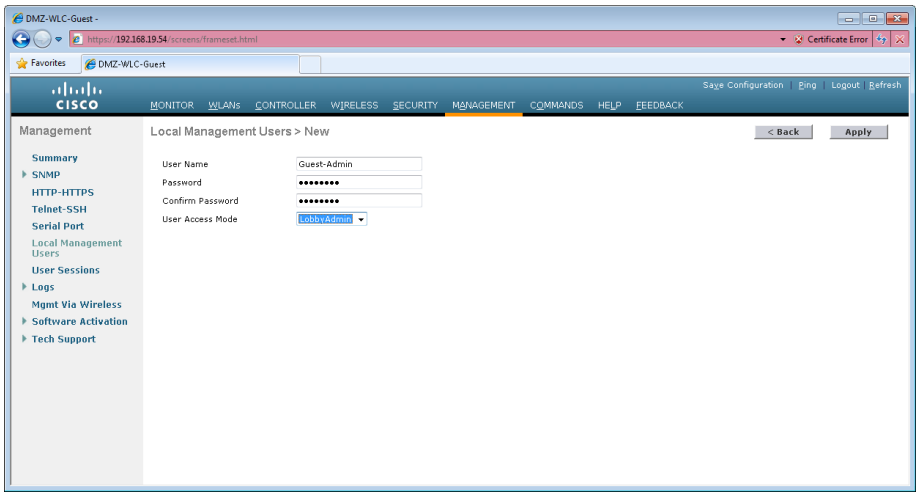
Option 1: Local WLC-based lobby admin user account

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)

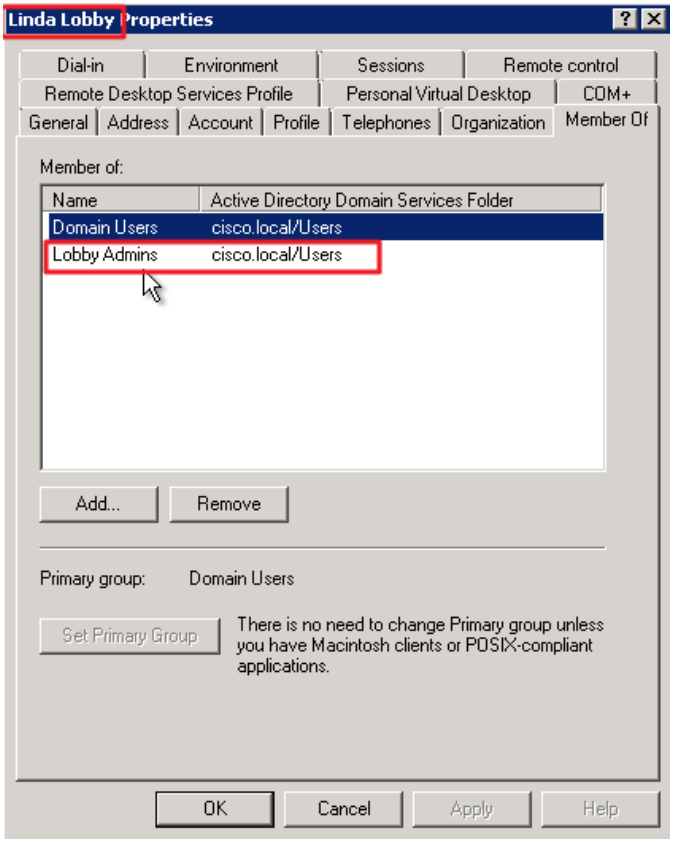
Step 4: In the **User Access Mode** list, choose **LobbyAdmin**, and then click **Apply**.



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.

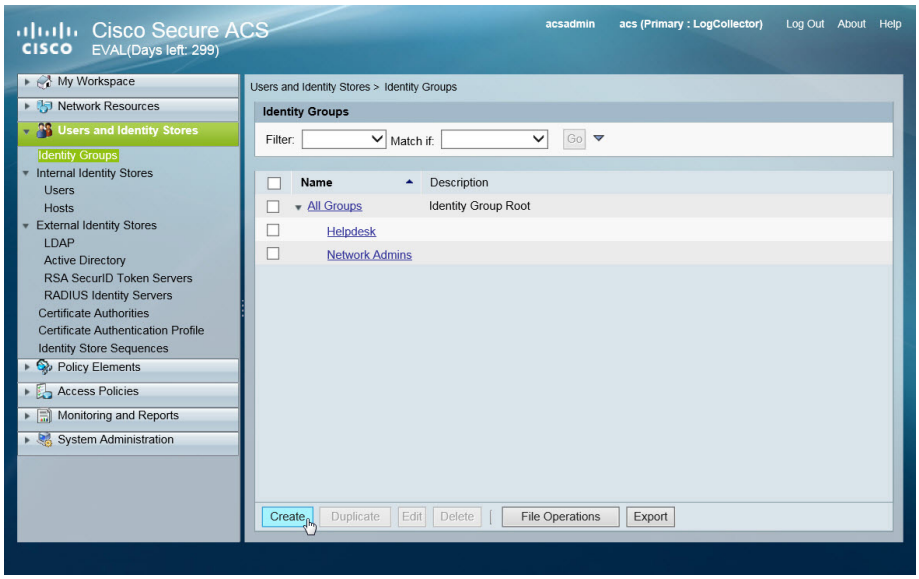
Step 1: Within Microsoft Active Directory, it is assumed that a lobby ambassador group (Example: Lobby Admins) has been created. Contained within this group are each of the lobby ambassador employees within the organization. (Example: Linda Lobby)



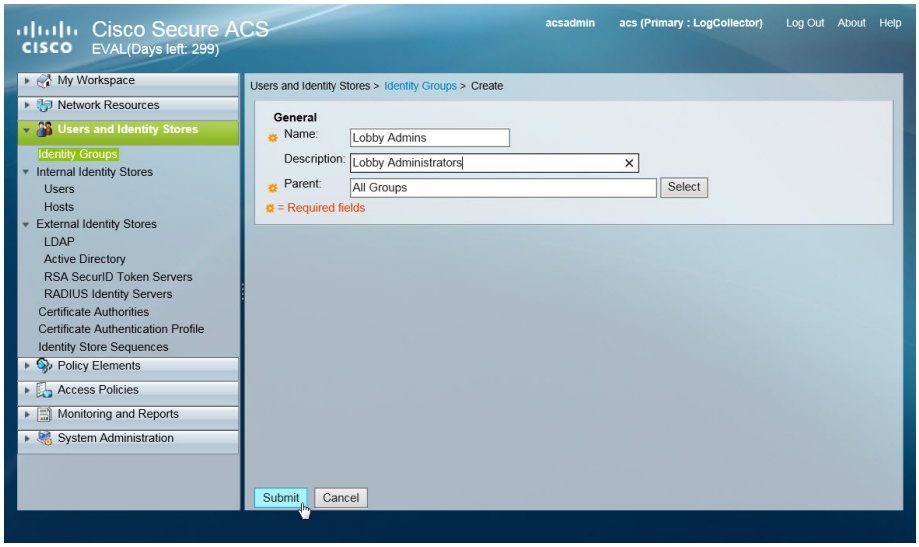
Step 2: Log in to Cisco Secure ACS via the GUI (https://acs.cisco.local).

Step 3: Navigate to **Users and Identity Stores > Identity Groups**.

Step 4: Click **Create**.



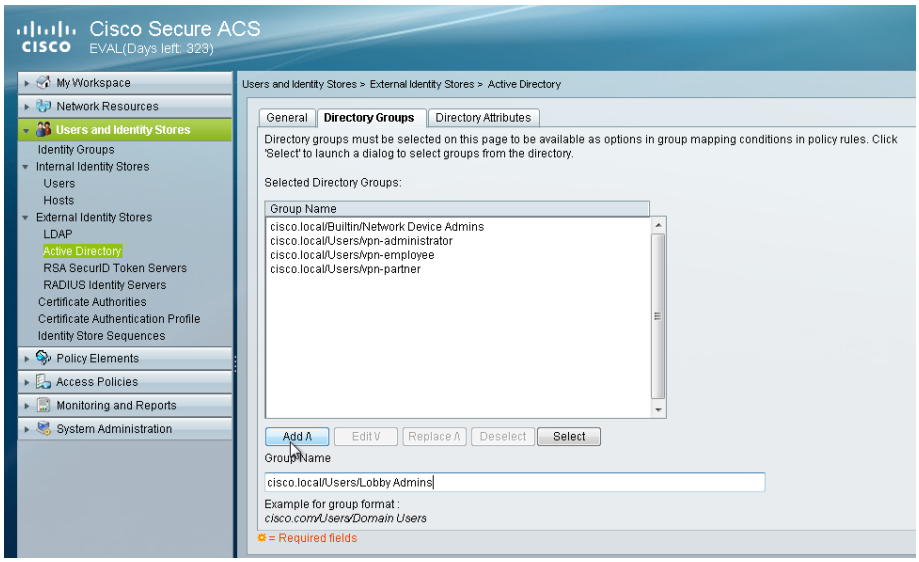
Step 5: In the Name box, enter **Lobby Admins,** and then enter a description for the group then click **Submit**.



Step 6: In Cisco Secure ACS, navigate to **Users and Identity Stores > External Identity Stores > Active Directory**.

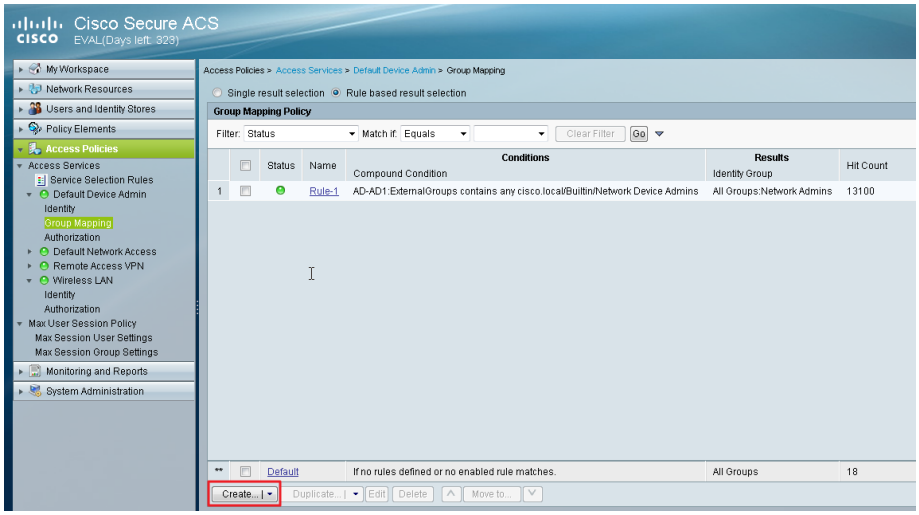
Step 7: Click the **Directory Groups** tab, and in the **Group Name** box, enter the lobby admin group (Example: cisco.local/Users/Lobby Admins), and then click **Add**.

The lobby admin group appears in the Selected Directory Groups list.

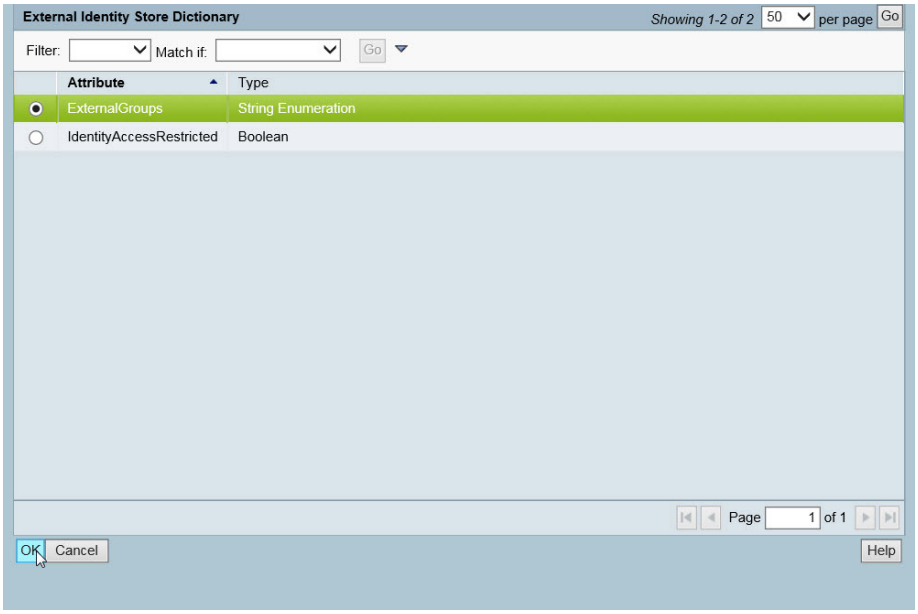


Next, the Active Directory group that was just added to Cisco Secure ACS needs to be mapped to a Secure ACS policy.

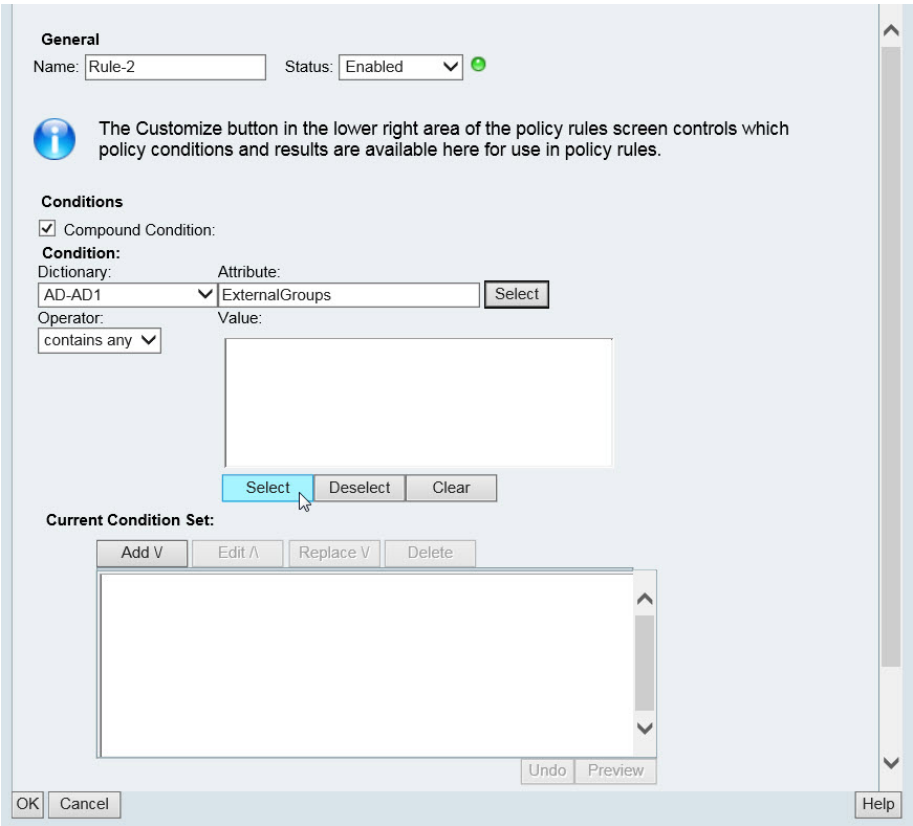
Step 8: In Cisco Secure ACS, navigate to **Access Policies > Access Services > Default Device Admin > Group Mapping**, and then at the bottom of the screen, click **Create**.



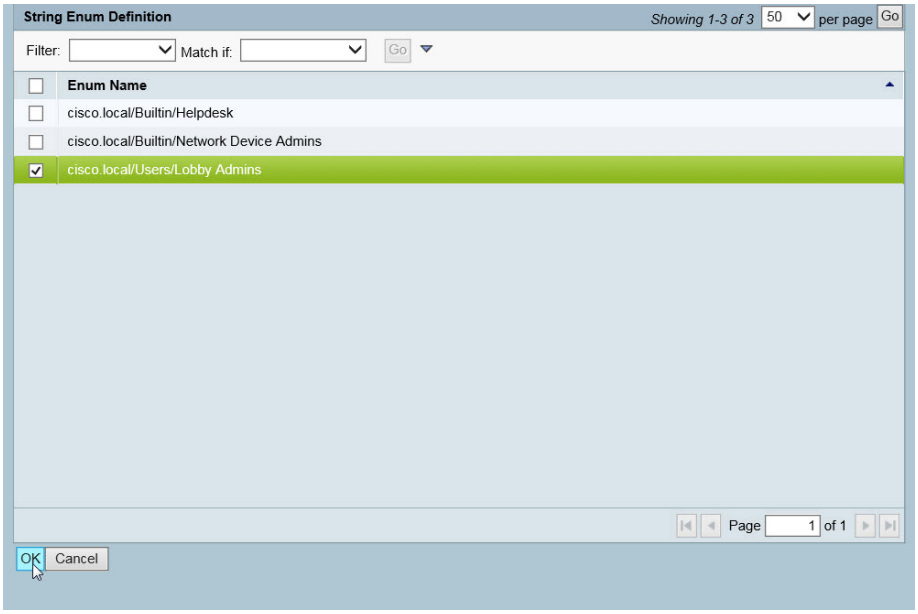
Step 9: Under Conditions, select **Compound Condition**, in the **Dictionary** list, choose **AD-AD1**, and then in the **Attribute** box, click **Select** and select **External Groups** and press **OK**. This selects External Groups.



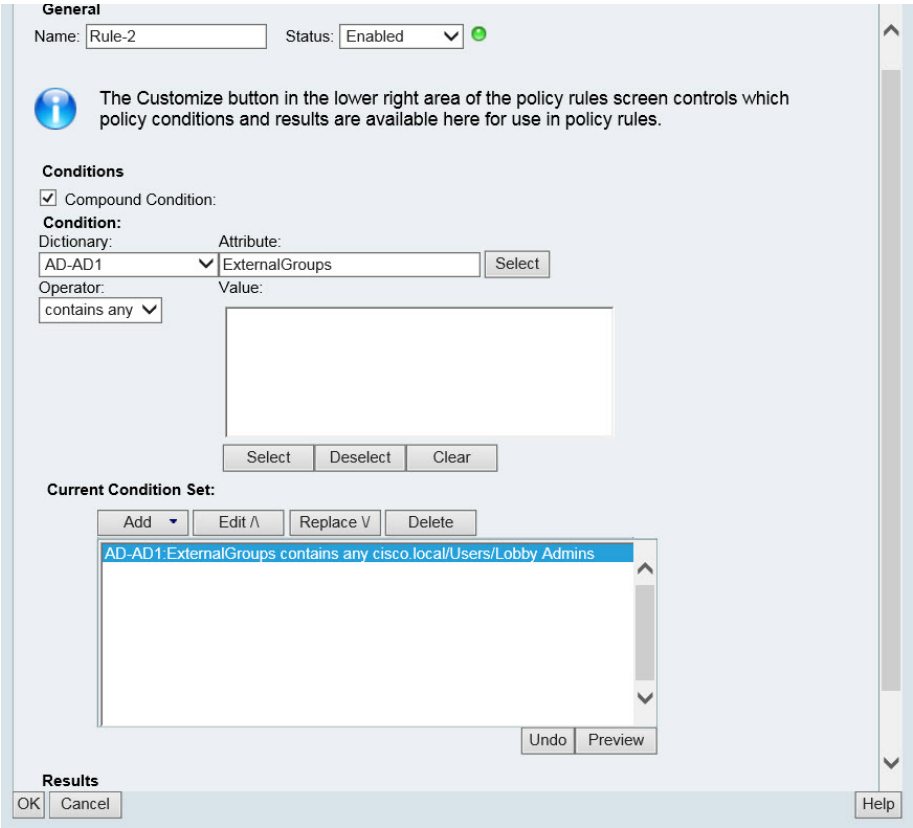
Step 10: Under the Value box, click **Select**.



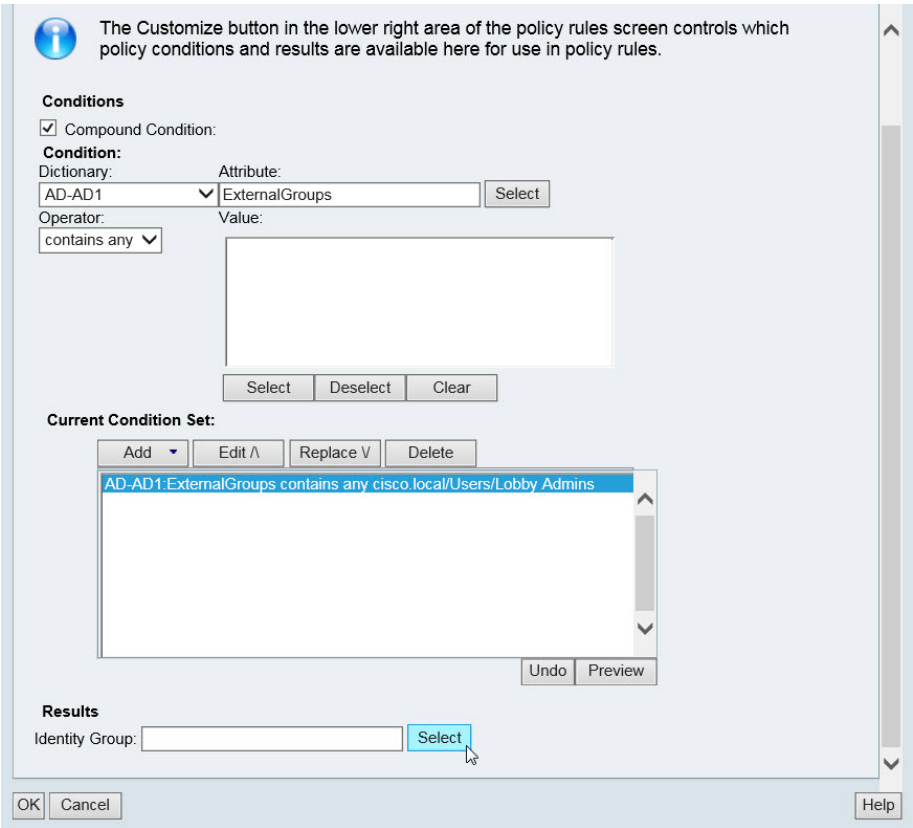
Step 11: In the **String Enum Definition** dialog box, select the lobby admin Active Directory group (Example: cisco.local/Users/Lobby Admins), and then click **OK**.



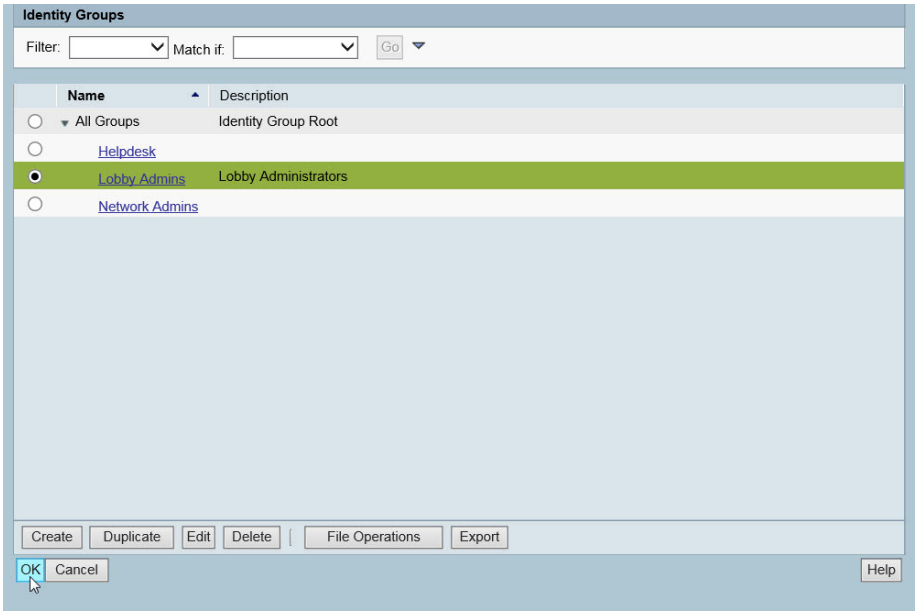
Step 12: Under Current Condition Set, click **Add**. The new condition appears in the Current Condition Set box.



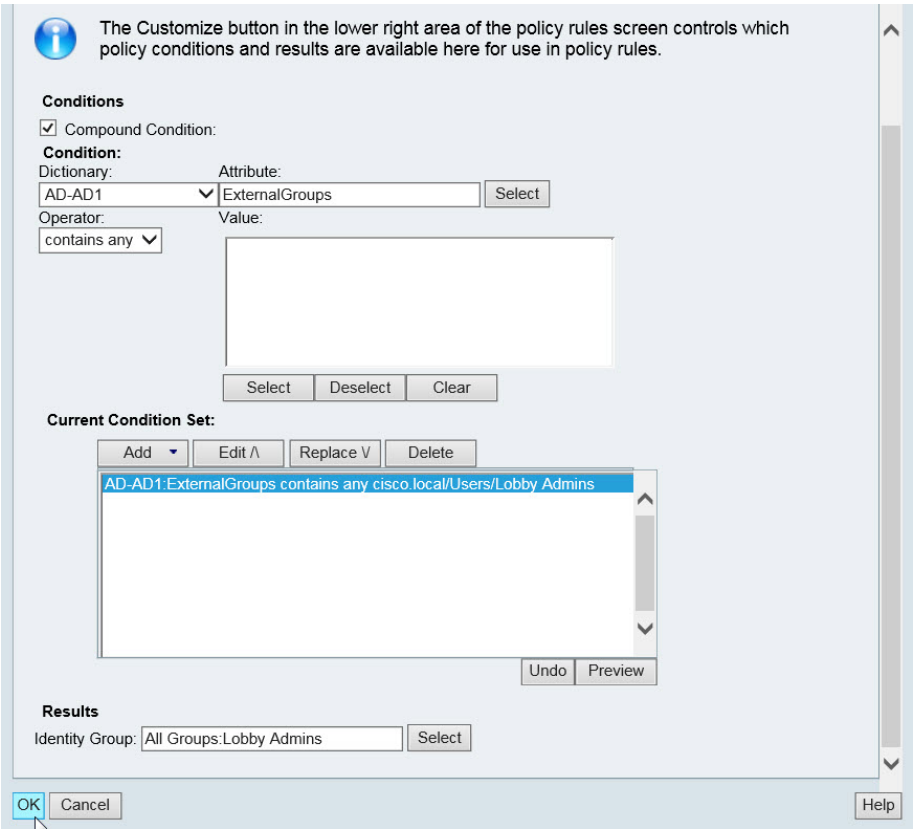
Step 13: Scroll down and under Results, click **Select**



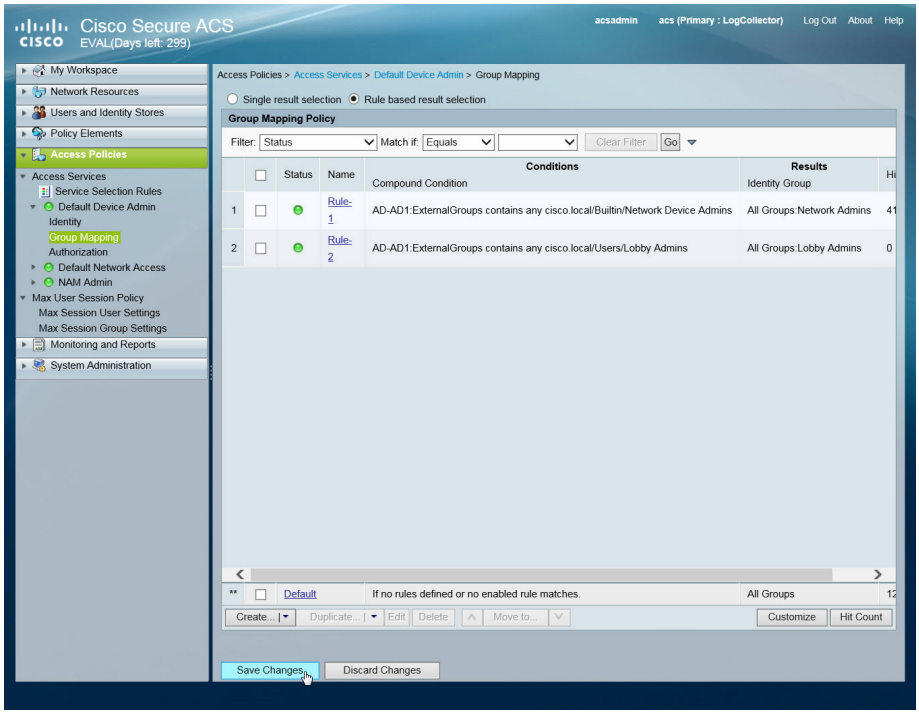
Step 14: Select the Cisco Secure ACS identity group (Example: Lobby Admins) that will be mapped to the Active Directory group specified in the Current Condition Set, and then click **OK**.



Step 15: Press **OK** to complete the group mapping.



Step 16: Save the changes by selecting **Save Changes**.



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.

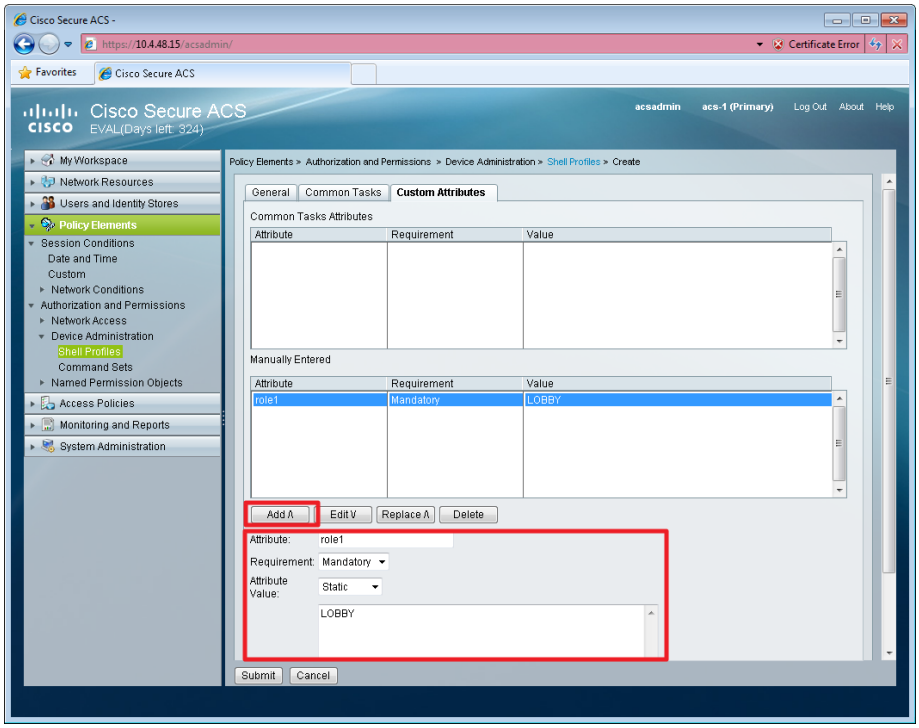
Step 17: In **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles**, click **Create**.

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**.



Step 22: Click **Submit**.

Next, you create a WLC authorization rule.

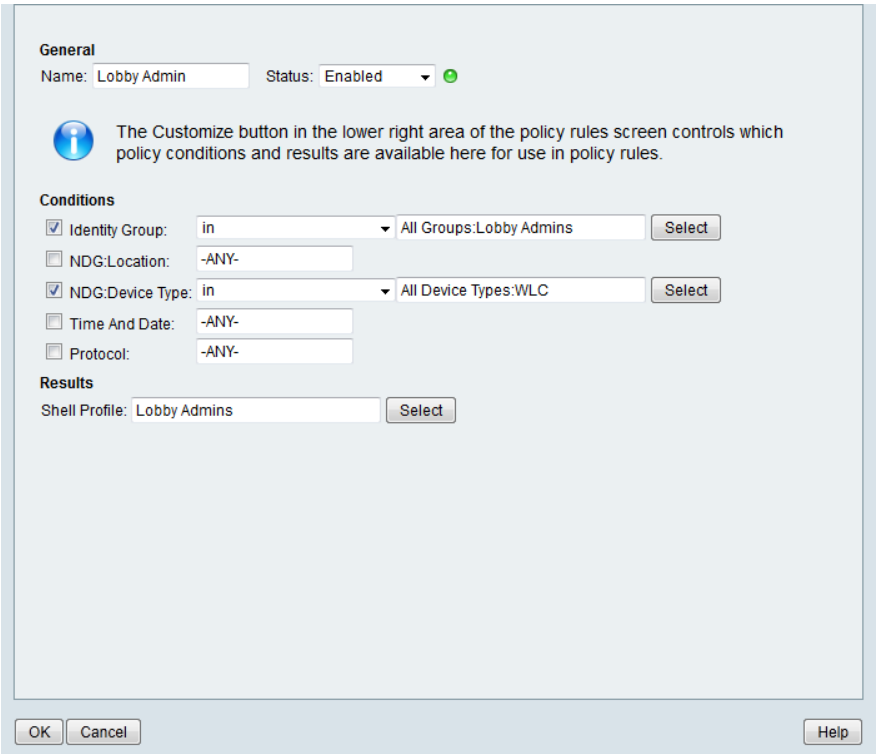
Step 23: In **Access Policies > Default Device Admin > Authorization**, click **Create**.

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**.

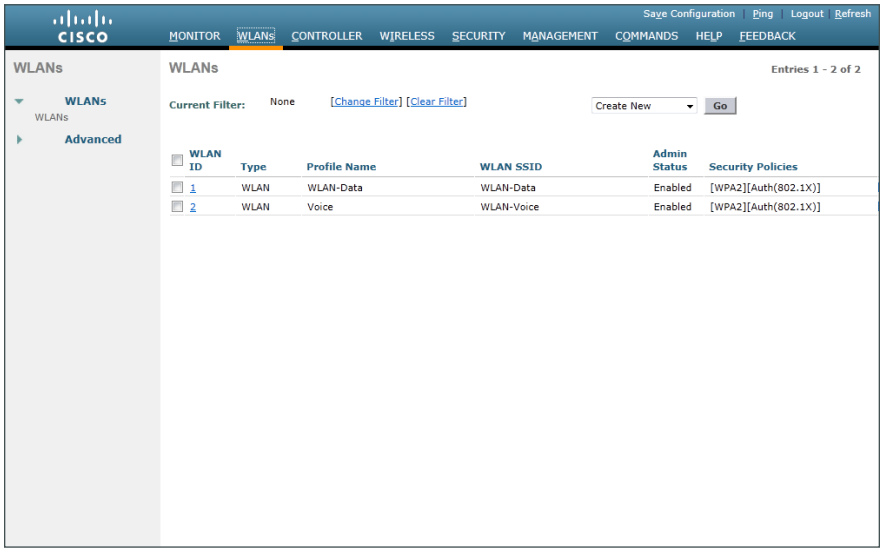


Step 28: Click **Save Changes**.

Procedure 18 Configure the internal WLCs for a guest

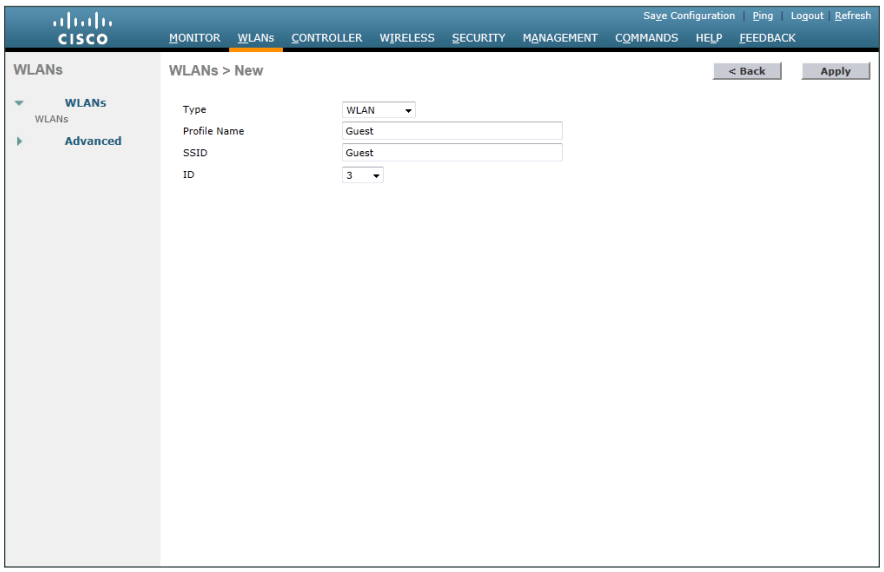
When a client connects to the guest SSID, the client must be anchored to the controller in the DMZ. The guest clients' traffic is tunneled from the wireless controller where the access point (the foreign anchor controller) is registered to the guest controller in the DMZ (the anchor controller). The 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**.

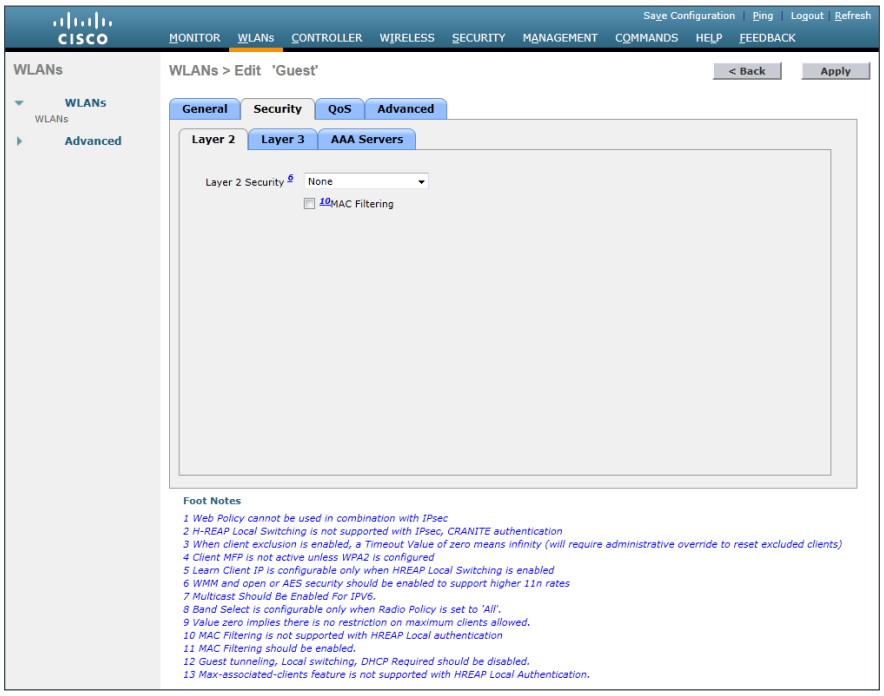


Step 2: Enter the **Profile Name**. (Example: Guest)

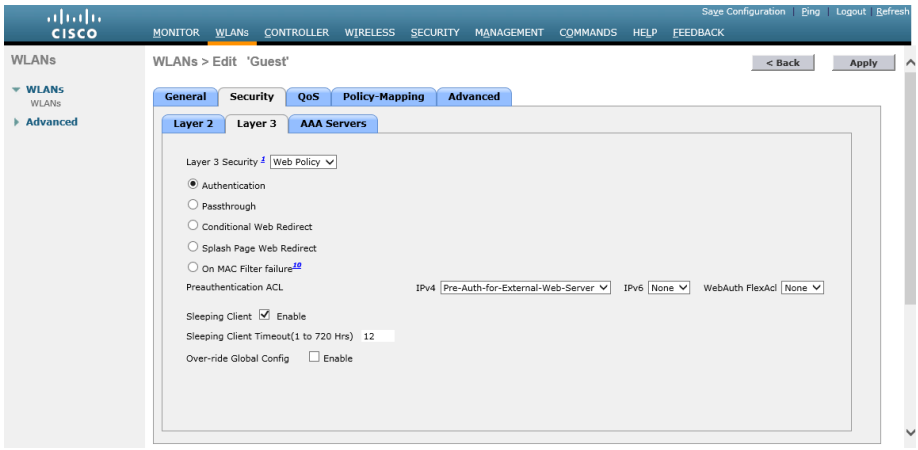
Step 3: In the **SSID** box, enter the guest WLAN name, and then click **Apply**. (Example: Guest)



Step 4: Click the **Security** tab, and then on the Layer 2 tab, in the **Layer 2 Security** list, choose **None**.

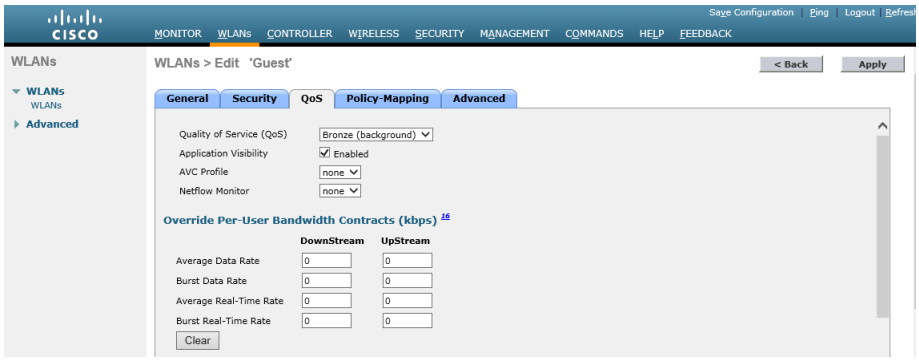


Step 5: On the Layer 3 tab, select **Web Policy** and enable sleeping client support. Sleeping client support prevents wireless clients that enter sleep mode from having to re-authenticate when they are awakened.

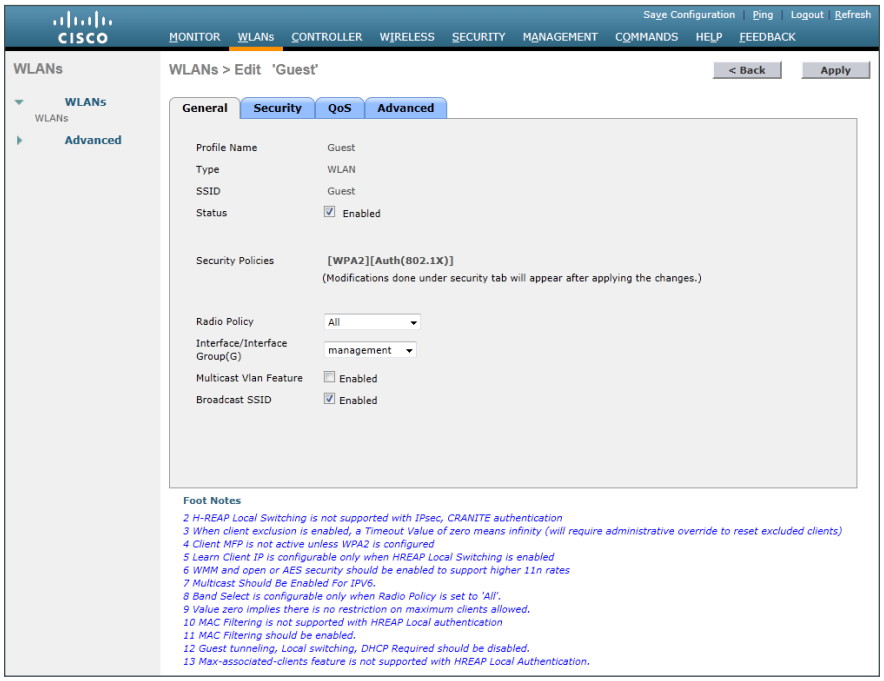


Step 6: On the QoS tab, in the **Quality of Service (QoS)** list, choose **Bronze (background)**.

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**.

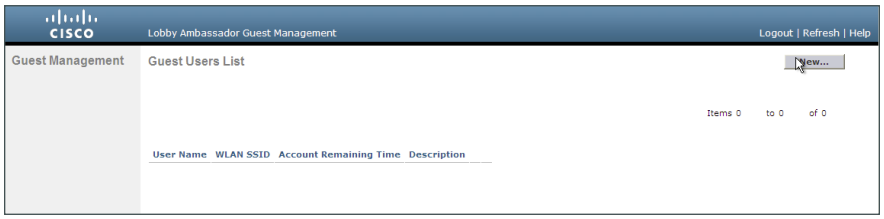
Step 13: Repeat Step 1 through Step 11 for every internal controller in your organization.

Procedure 19 Create guest accounts

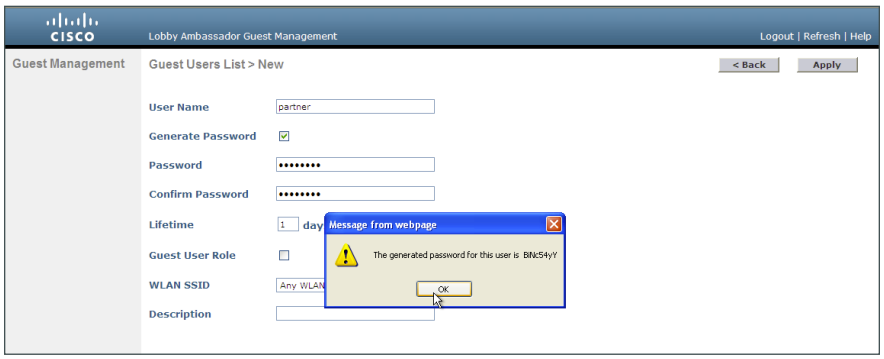
Now you can use the lobby administrator account to create usernames and passwords for partners, customers, and anyone else who is not normally granted access to your network.

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**.



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



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.

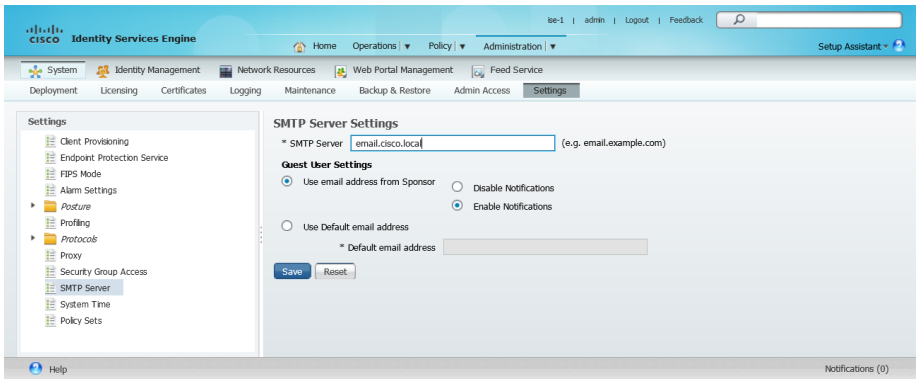
Procedure 1 Configure Cisco ISE Sponsor settings

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.

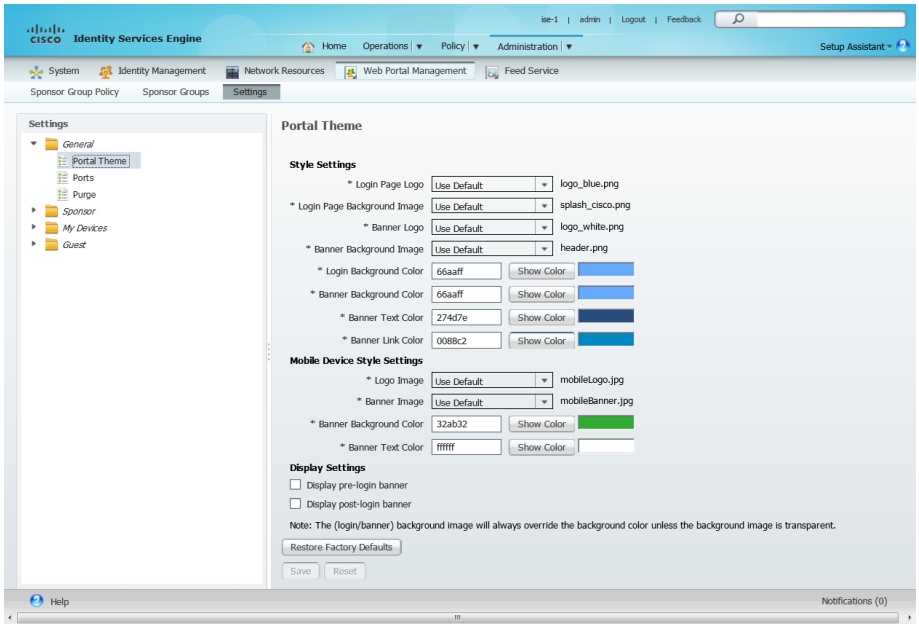
Step 1: In the Cisco ISE admin management web interface, navigate to **Administration > System > Settings > SMTP Server**, and then enter the location of the SMTP server that should be used to send guest wireless account notifications after creation. Emails can be sourced from either the sponsor's email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

Step 2: Click **Save**.



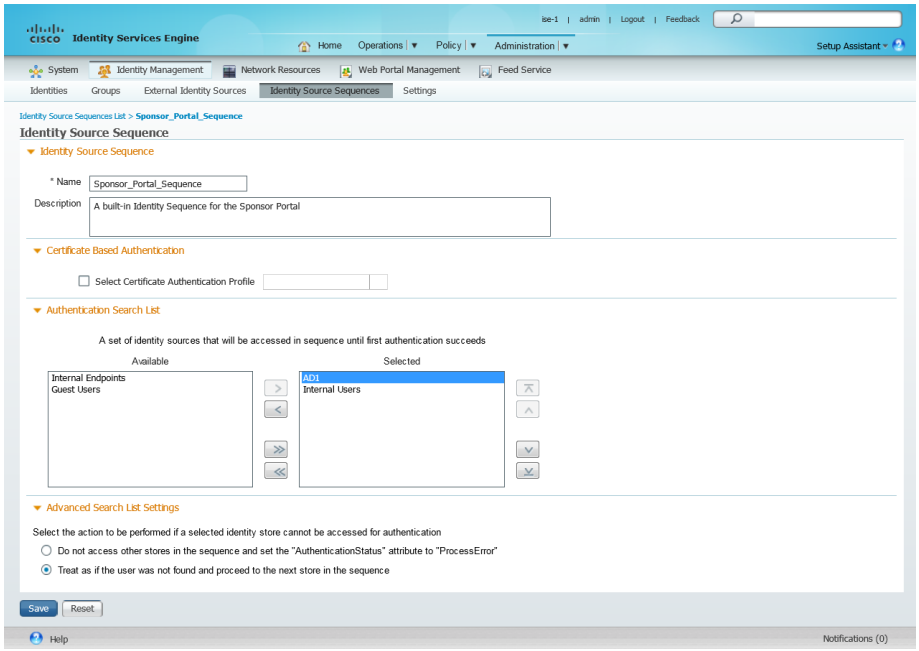
Step 3: Navigate to **Administration > Web Portal Management > Settings**, double-click **General**, and then, in the list, choose **Portal Theme**.

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.



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.

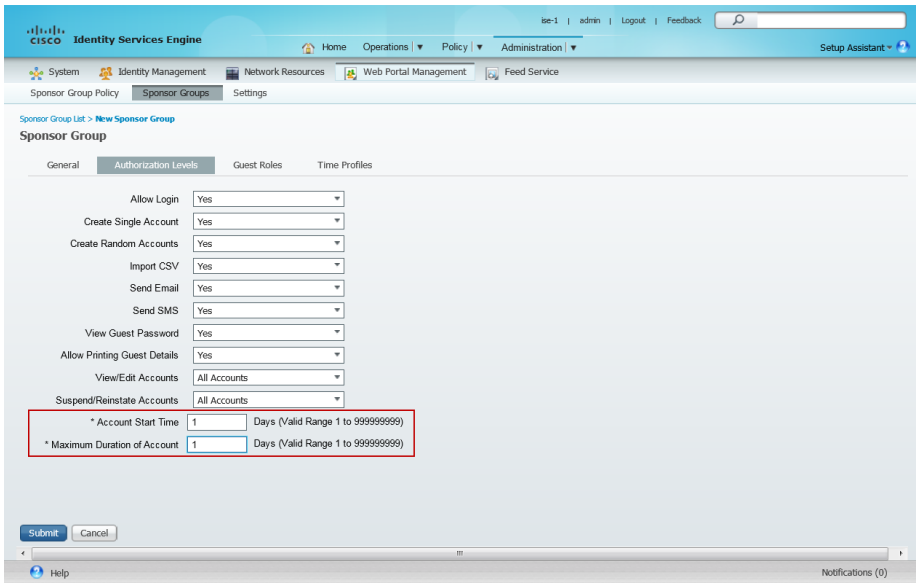


Step 6: Click **Save**.

Step 7: Navigate to **Administration > Web Portal Management > Sponsor Groups**, and then click **Add**.

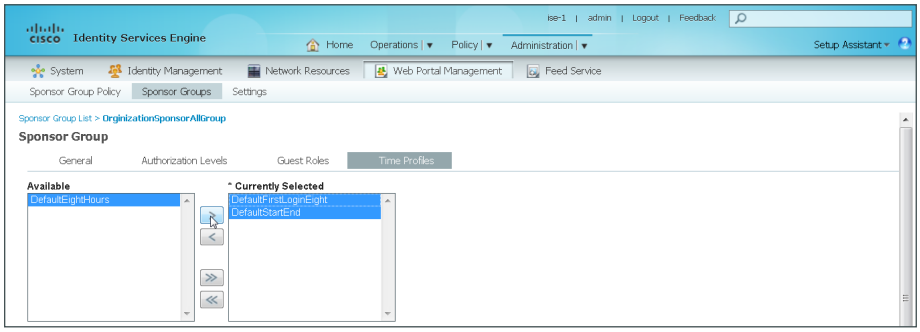
Step 8: Give the new group a name. (Example: OrganizationSponsorAllGroup)

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)



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.

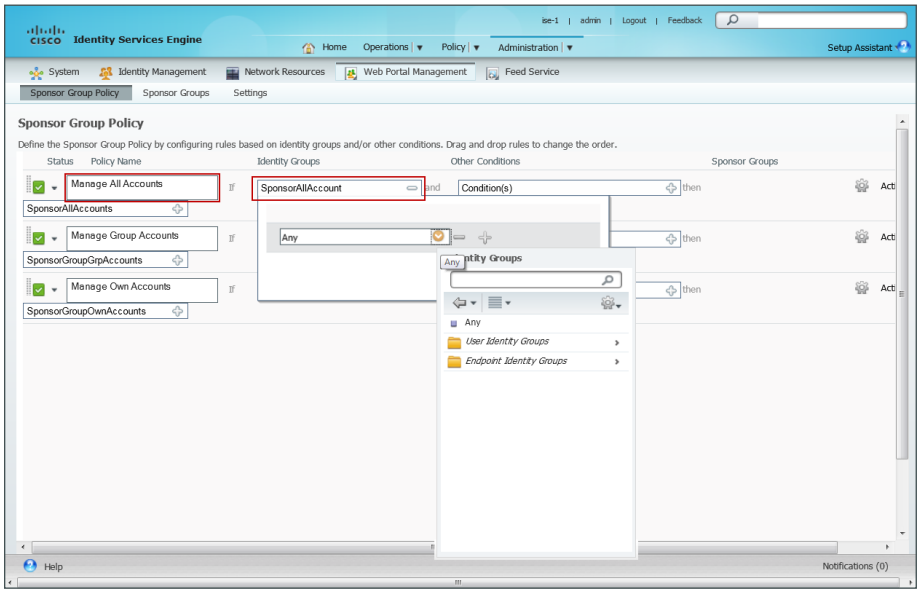


Step 12: Click **Submit.**

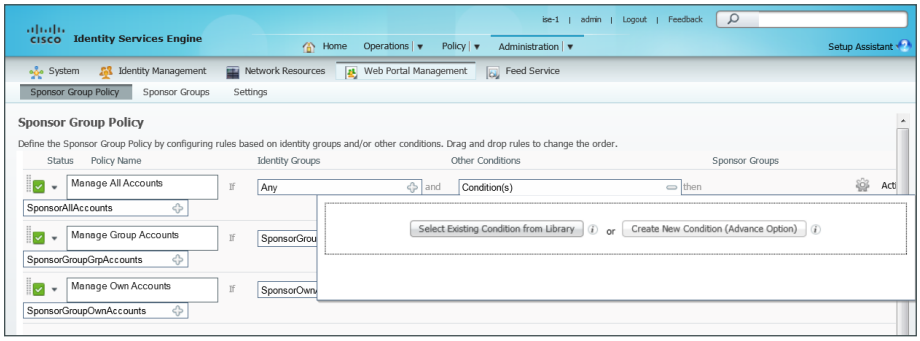
Next, you configure policies that define the sponsor group that is assigned to a sponsor, based on login credentials and other conditions.

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.

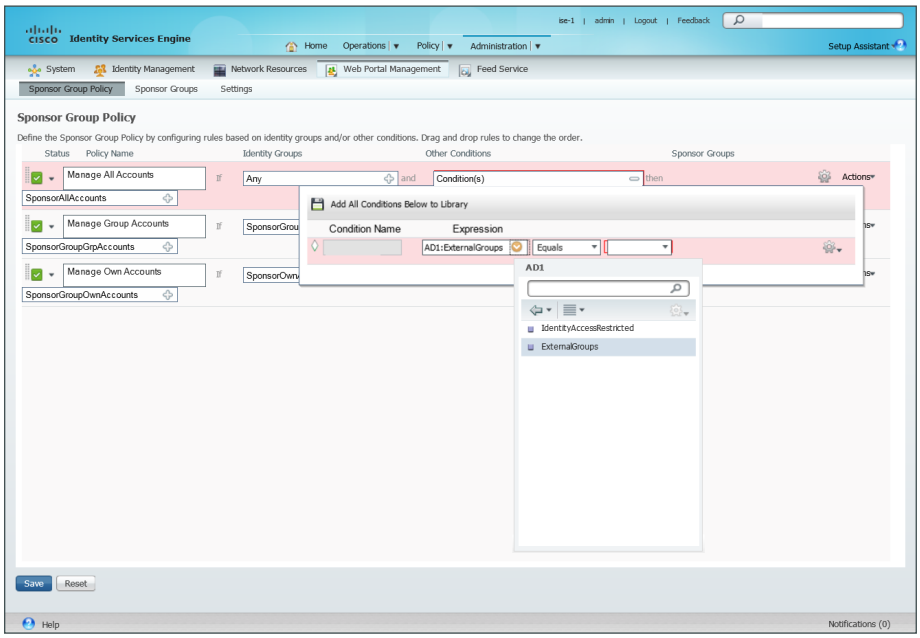


Step 15: Under the Other Conditions column for **Manage All Accounts**, click the **+** symbol, and then select **Create New Condition**.

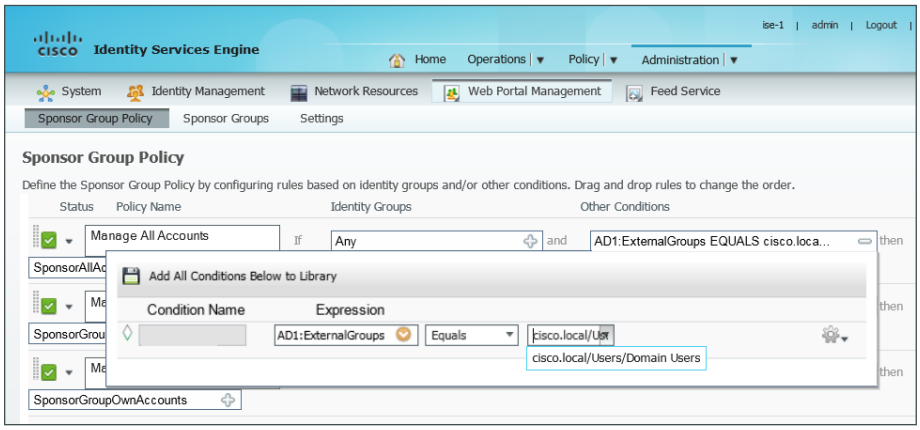


Step 16: Under Expression, next to Select Attribute, click the down arrow. The menu opens.

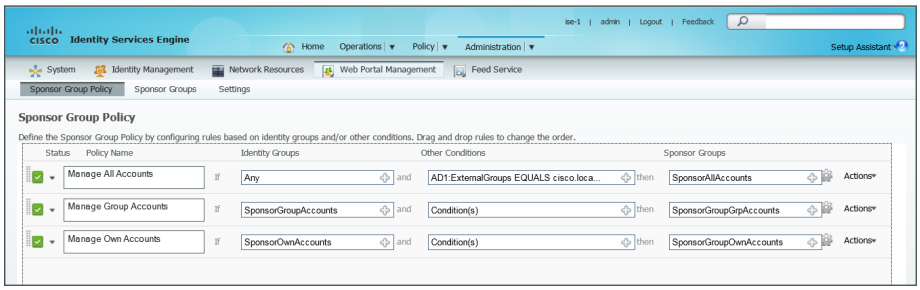
Step 17: Next to AD1, click the **>** symbol, and then choose **ExternalGroups**.



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".



Step 19: In the **Sponsor Groups** list, ensure the default, **SponsorAllAccounts**, is selected, and then click **Save**.

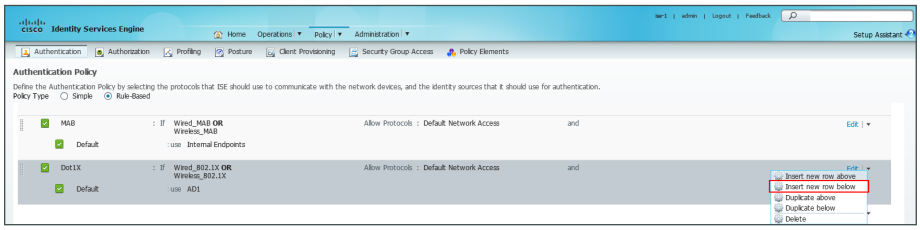


Procedure 2 Configure Cisco ISE guest authentication policy

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.

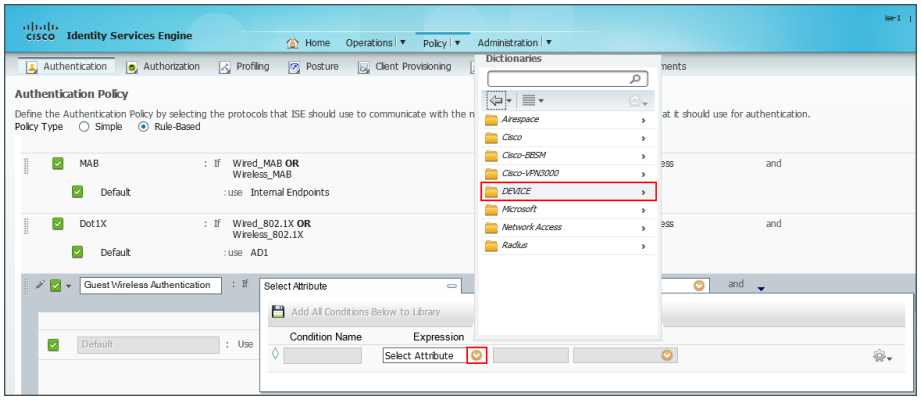
As a result, guest user authentication requests may fail since the local identity store is used by default. In order to use the guest user identity store as opposed to the internal identity store, you need to create a policy that is triggered when a RADIUS authentication request comes from a guest anchor 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.



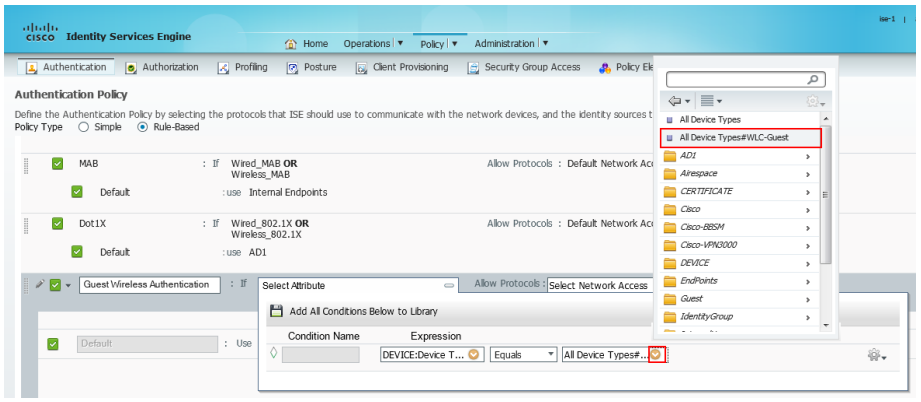
Step 2: In the Rule Name box, remove the "**Standard Rule 1**" name and replace it with a meaningful name such as **Wireless Guest Authentication**. In the **If Condition(s)** box, click the **+**, and then choose **Create New Condition (Advanced Option)**.

Step 3: Under Expression, click the down arrow to the right of Select Attribute, and then click the arrow to the right of DEVICE.

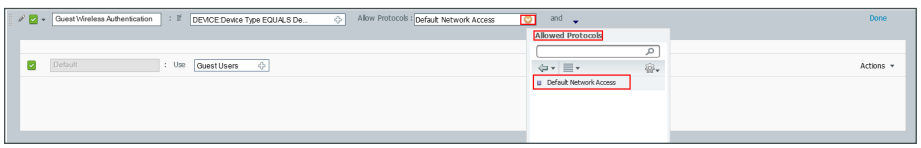


Next, ensure the policy triggers when a guest wireless LAN controller device type is responsible for the authentication request.

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.

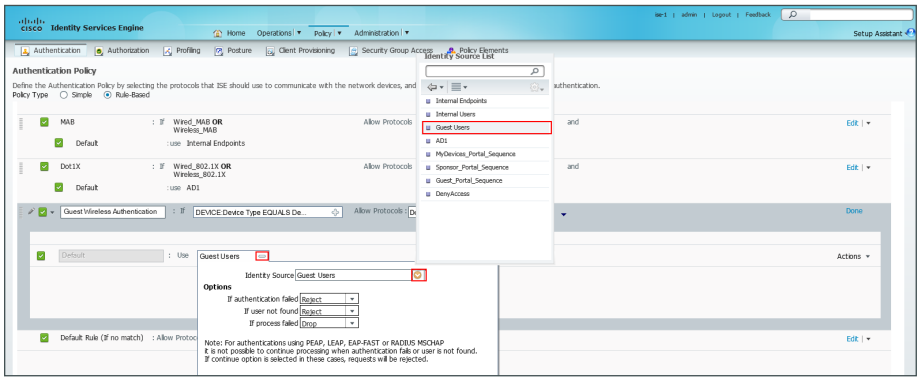


Step 5: In the **Allow Protocols: Select Network Access** box, click the down arrow, and then, under Allowed Protocols, select **Default Network Access**.

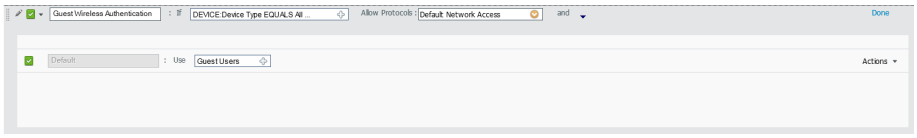


Step 6: Click the **+** for the **Use.**

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.



Step 8: In the upper right corner, click **Done**, and then click **Save**. The Authentication Policy is saved.



PROCESS

Configuring Cisco ASA Firewall and Cisco ISE for Guest Wireless

1. Create network objects
2. Create Cisco ASA security policy for Cisco ISE
3. Configure firewall policy for web portal
4. Configure the WLC for ISE Server
5. Modify guest WLAN on Cisco AireOS WLC to use Cisco ISE
6. Enable the guest wireless LAN
7. Enable captive portal bypass

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.

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.

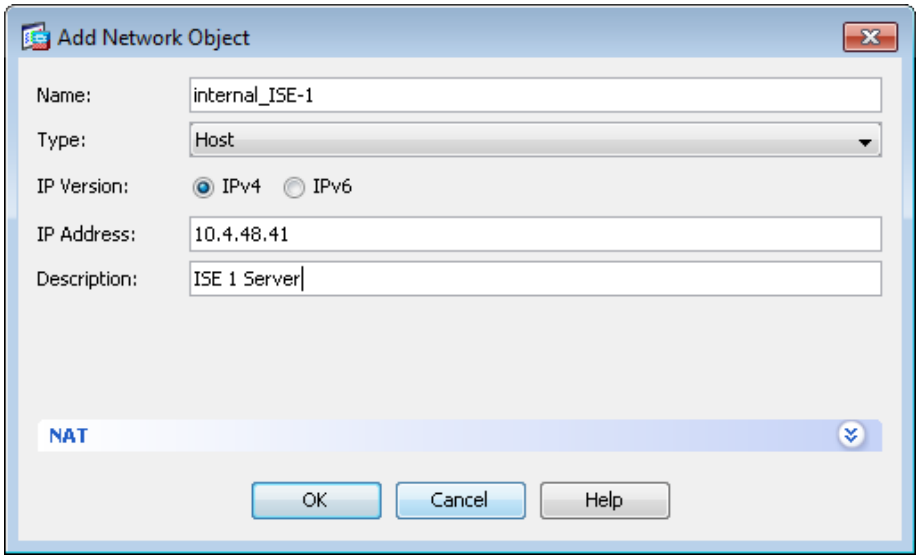
Step 3: Click **Add > Network Object**.

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)



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

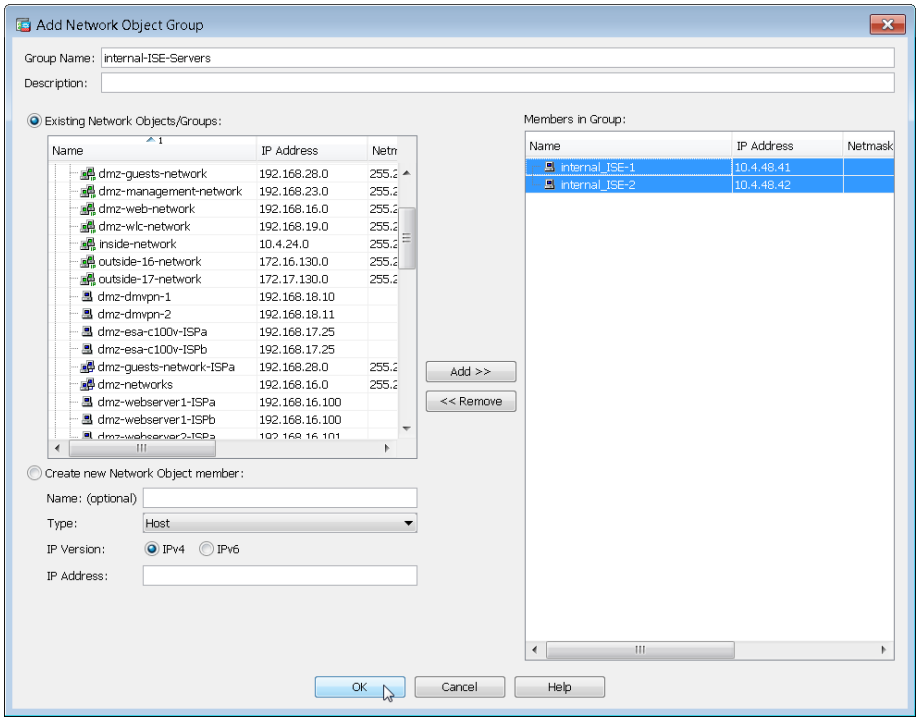
Network object group	Network objects	Group description
internal-ISE-Servers	internal_ISE-1 Internal_ISE-2	Internal ISE Servers

Step 7: Click **Add > Network Object Group**.

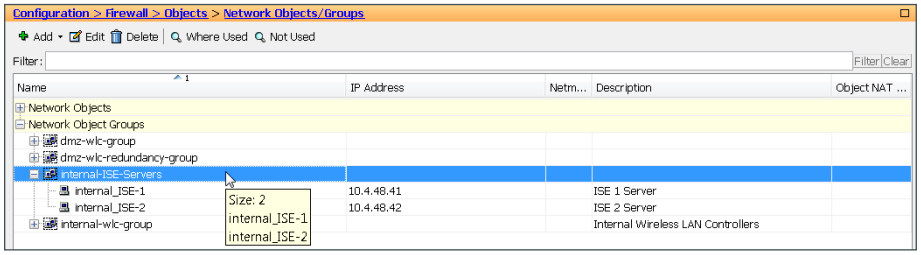
The Add Network Object Group dialog box appears.

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.



Step 10: Review the configured network object groups for completeness, and then click **OK**.



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)

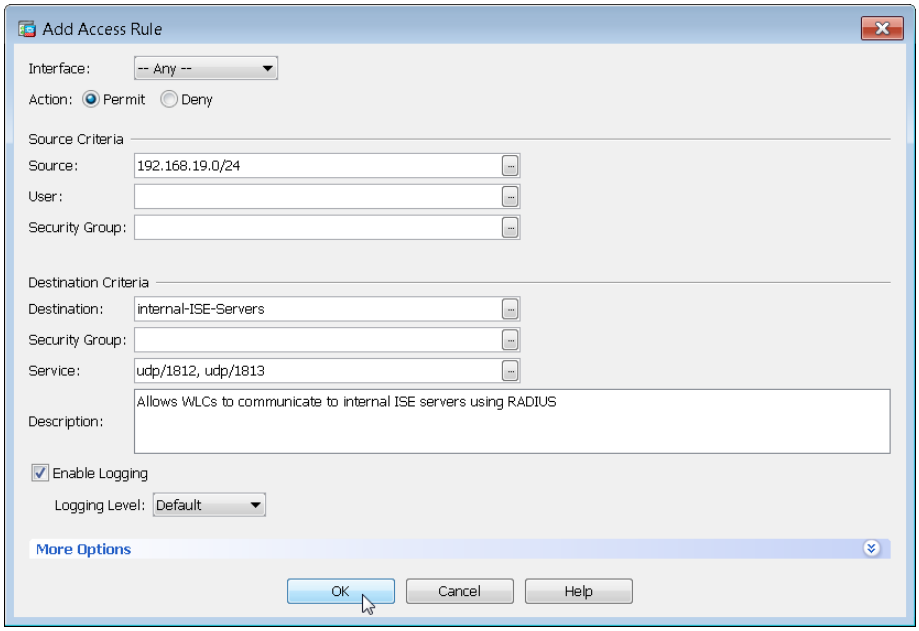
Step 7: In the **Destination** box, choose the destination. (Example: internal-ISE-Servers)

Step 8: In the **Service** box, enter the service. (Example: udp/1812, udp/1813)

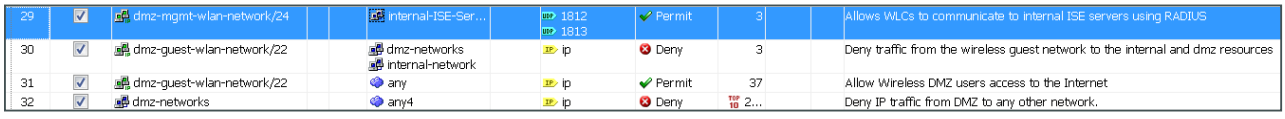
Step 9: In the **Description** box, enter a useful description

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)



Step 12: After adding the rule in Table 34, click **Apply** on the Access Rules pane.



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**.

Table 35 - Firewall policy rule for ISE Web Portal

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)

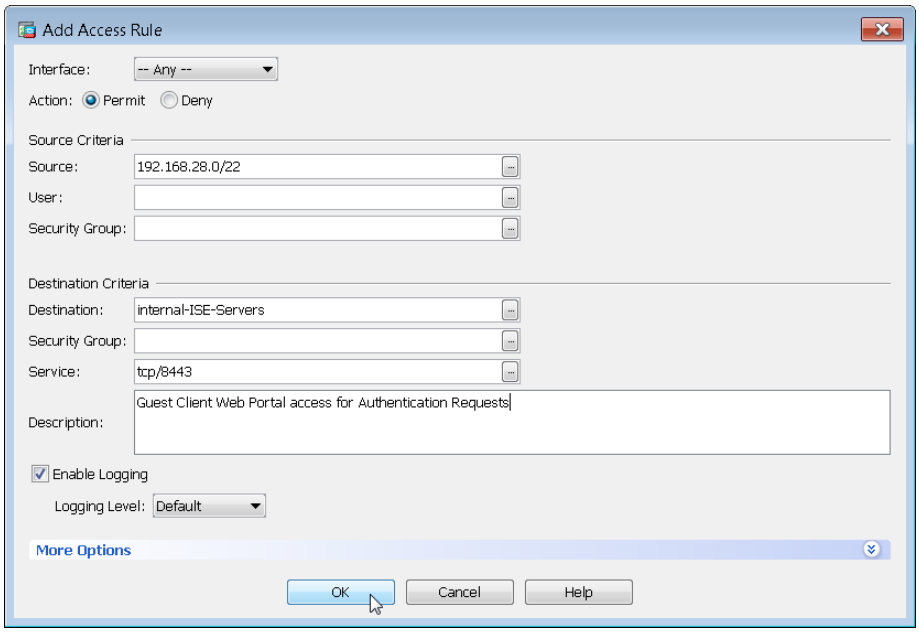
Step 7: In the **Destination** box, choose the destination. (Example: internal-ISE-Servers)

Step 8: In the **Service** box, enter the service. (Example: tcp/8433)

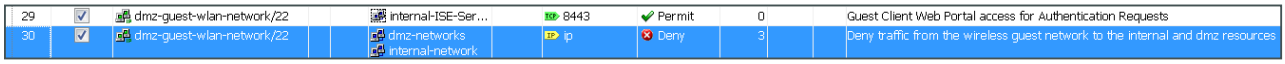
Step 9: In the **Description** box, enter a useful description.

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)



Step 12: After adding the rule in Table 35, click **Apply** on the Access Rules pane.



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.

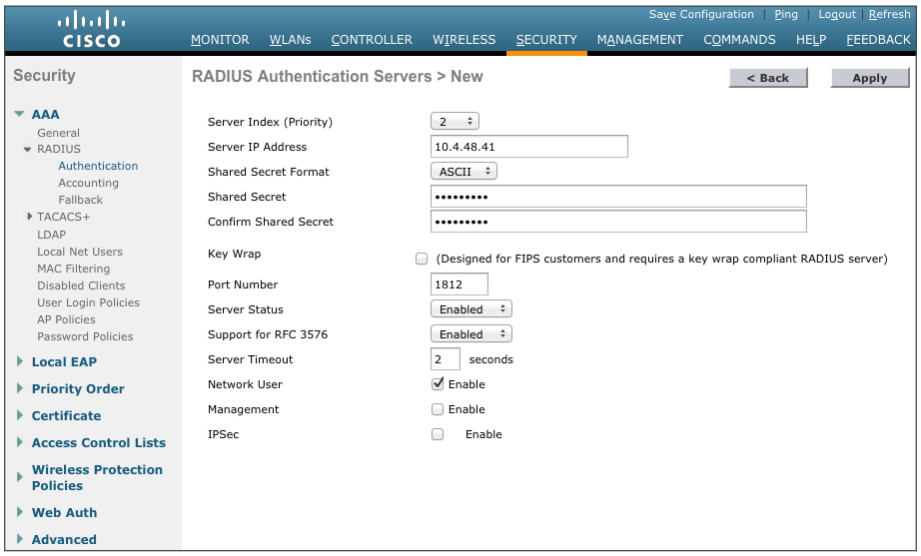
Step 4: Click **New**.

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)

Step 8: Next to Management, clear the **Enable** check box, and then click **Apply**.



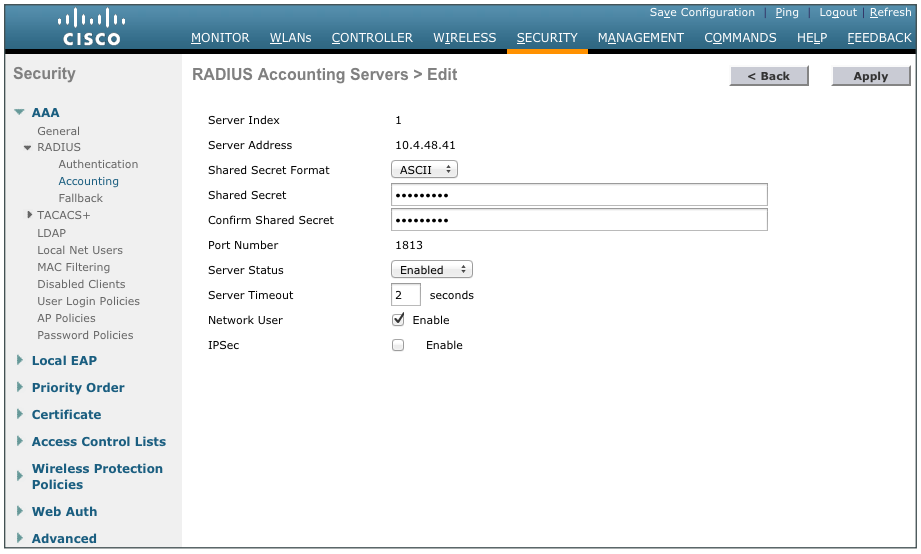
Step 9: Navigate to **Security > AAA > RADIUS > Accounting**. From here, you can add the guest server as an accounting server in the WLC.

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)

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



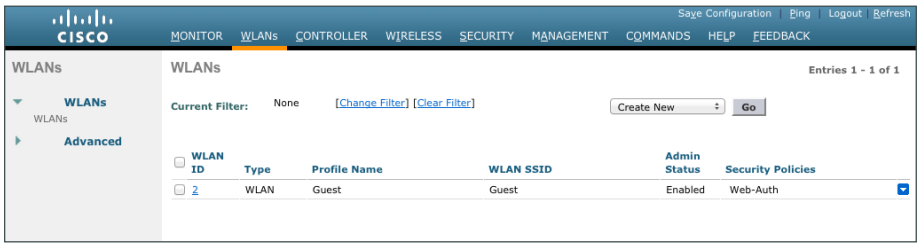
Step 14: Click **Apply**, and then repeat the process for the redundant secondary Cisco ISE server. (Example: 10.4.48.42)

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.



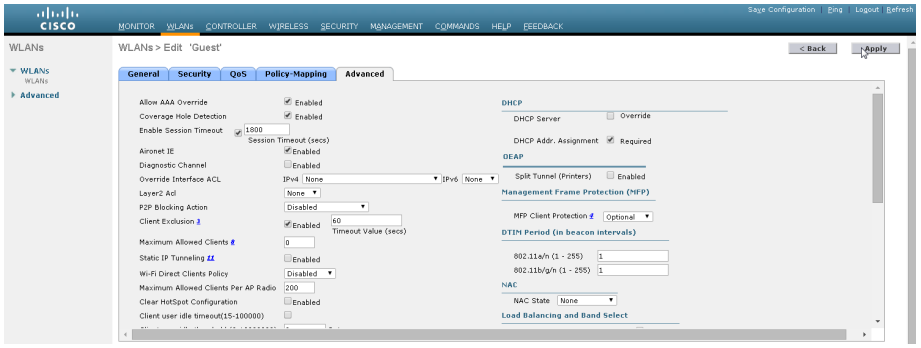
Step 3: Click the down arrow next to Create New, in the list, choose **Disable Selected**, and then click **Go**.

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.



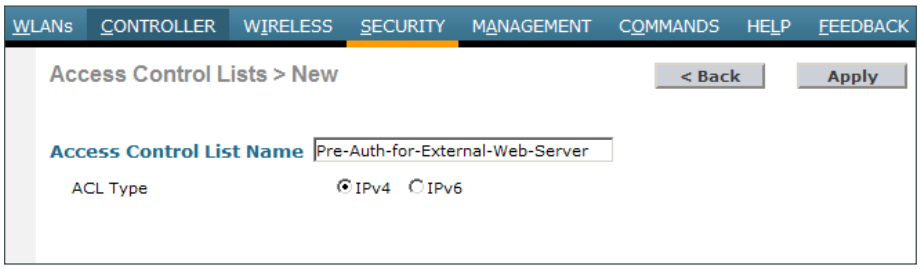
Step 8: For security purposes, next to **DHCP Addr. Assignment**, select **Required** .

Step 9: Click **Apply**.

In order for the wireless guest to have access to resources that they need before they authenticate, a pre-authentication 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.

Step 11: In the **Access Control List Name** box, enter a name for the ACL, and then click **Apply**.



Tech Tip

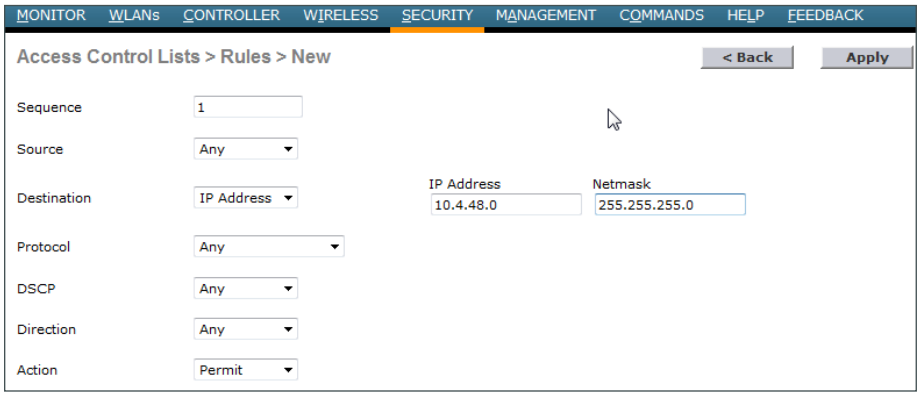
You need to apply the access control list to the DMZ based anchor controllers (but this is not needed on any of the foreign anchor controllers). This is because the raw guest user traffic originates from the DMZ anchor controller. Prior to this, the guest traffic was encapsulated in CAPWAP between the 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.

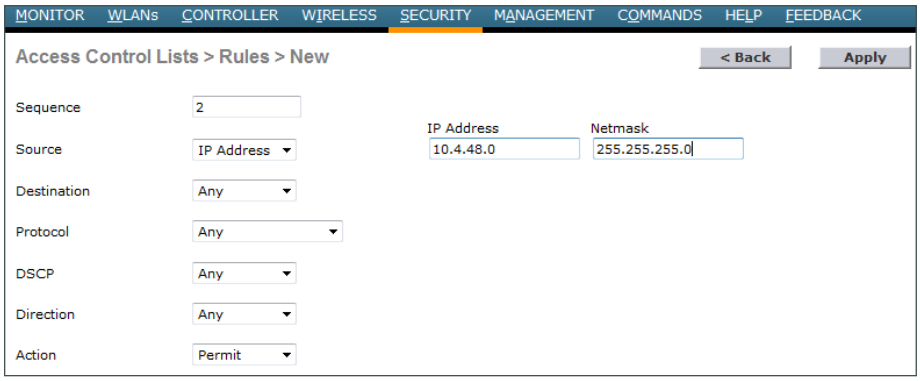
- Sequence—1
- Destination—**IP Address**
- IP Address—**10.4.48.0**
- Netmask—**255.255.255.0**
- Action—**Permit**



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**



Step 17: Navigate to **WLANs**.

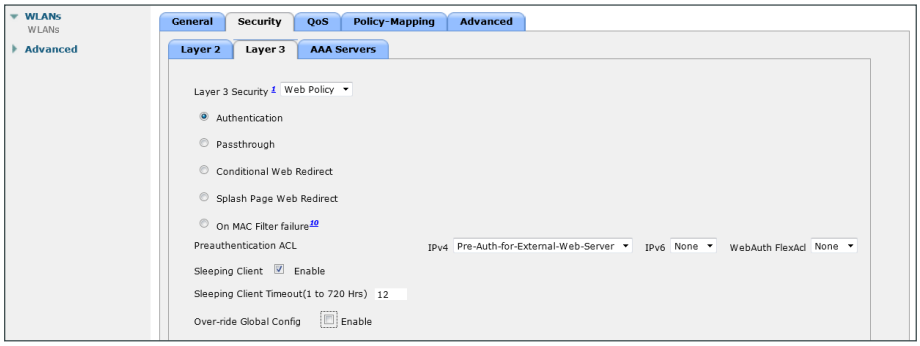
Step 18: Click the WLAN ID for the specific guest WLAN (Example 2)

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**.



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.

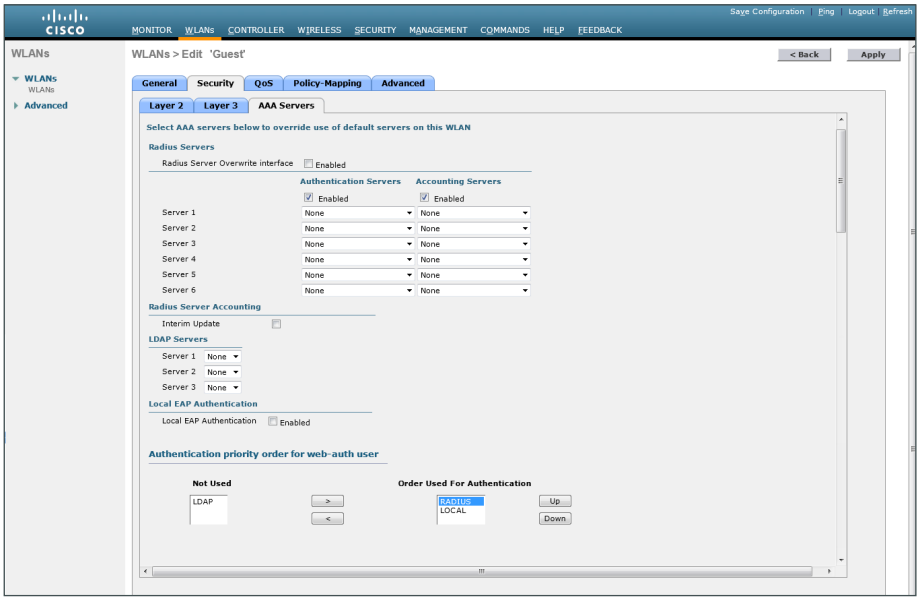
Step 22: On WLC controller, navigate to **WLANs**, and edit the WLAN by selecting the Guest Wireless LAN number. (Example 2)

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**.

Tech Tip

It is not necessary to select the server from the list because the enabled RADIUS server(s) defined under the Security > RADIUS > Authentication will be used.



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.

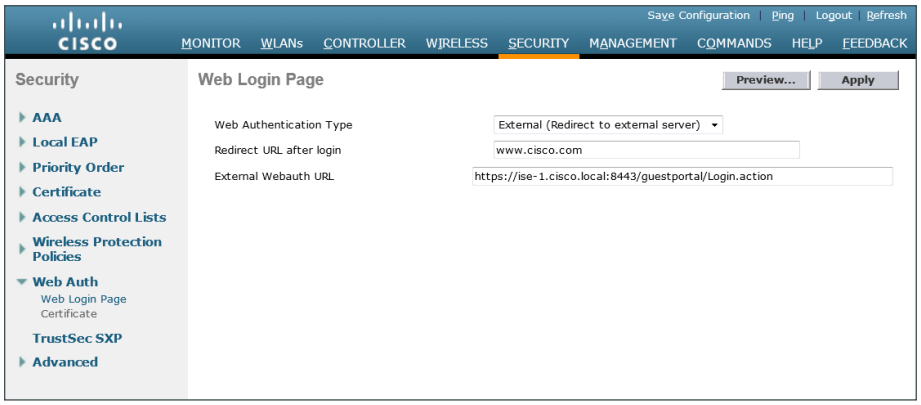
Step 25: Navigate to **Security > Web Auth > Web Login Page**.

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.



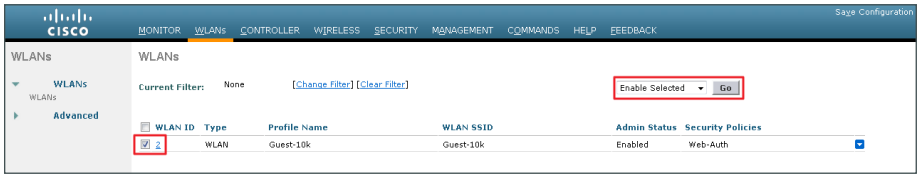
Procedure 6 Enable the guest wireless LAN

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**.



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)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.

PROCESS

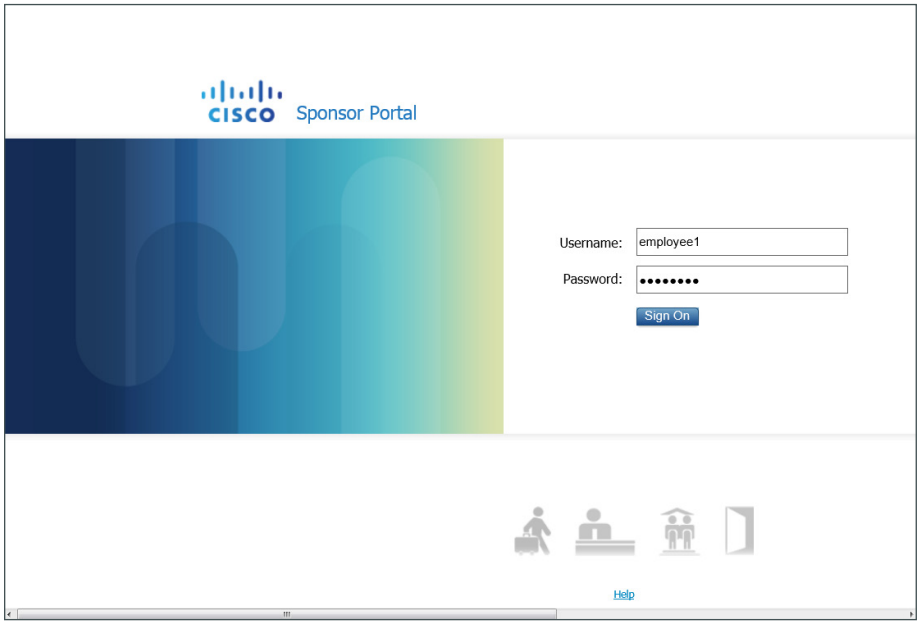
Creating and Using Guest Accounts

1. Use the Sponsor Portal
2. Testing the wireless user guest accounts

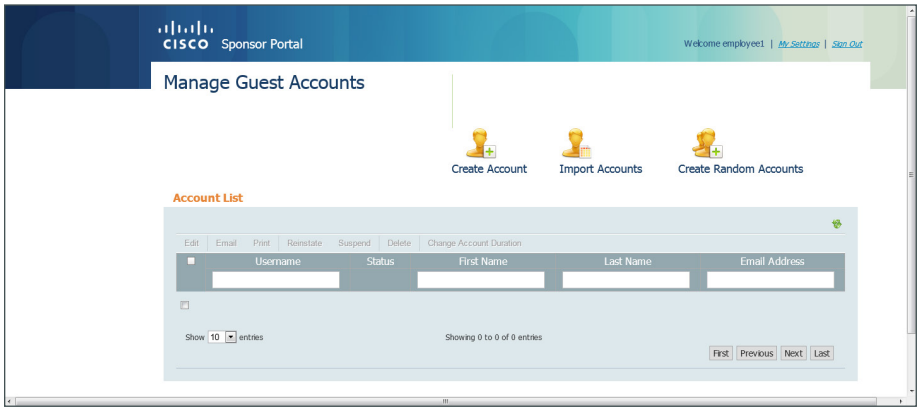
Procedure 1 Use the Sponsor Portal

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

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

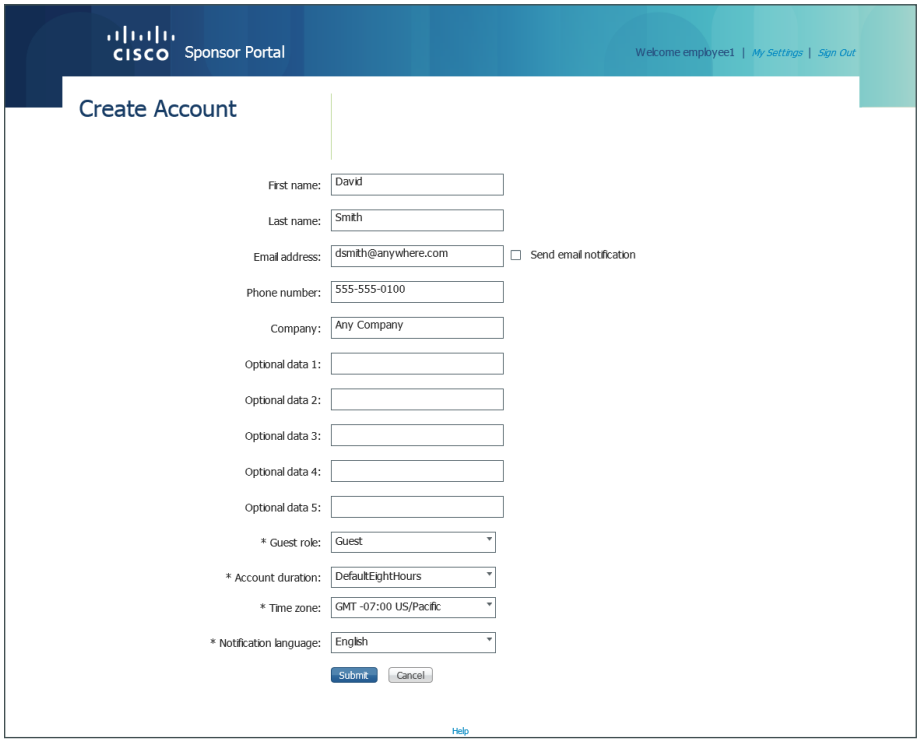


Step 2: Click **Create Account**.



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**.

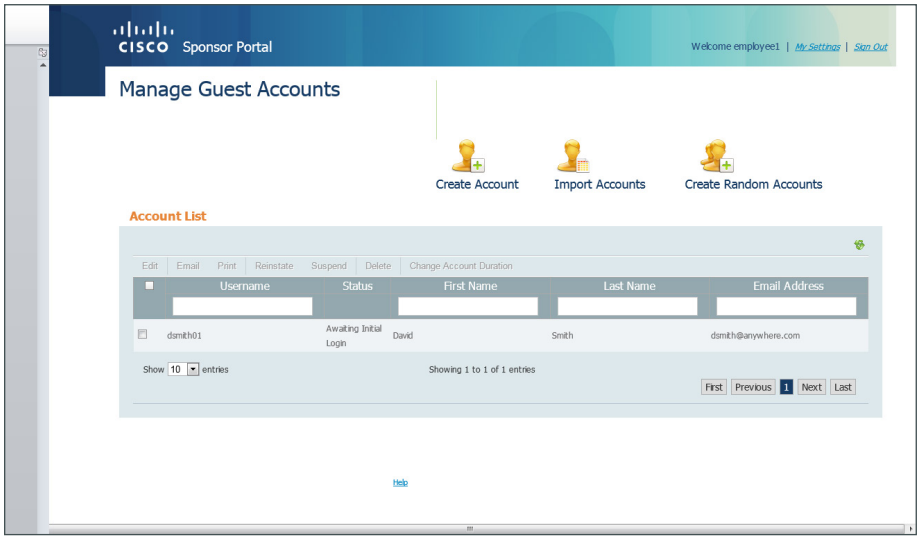
Step 4: If you have configured an SMTP server in Cisco ISE, you can optionally send an email notification to the user by selecting the **Send email notification**. In this particular example, the sponsor enters the first and last name, email address, and company name.



When the account is successfully created, Cisco ISE displays the guest account and credentials.

Step 5: For testing purposes, write down the username that was automatically created. (Example: dsmith01/36_7M2tiY)

The guest user account is now created and is shown as Awaiting Initial Login.

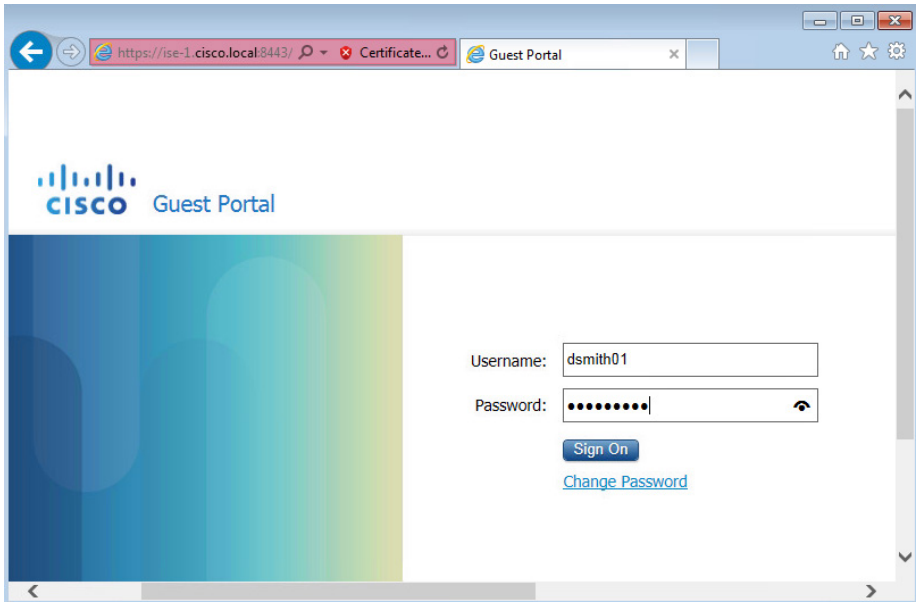


Procedure 2 Testing the wireless user guest accounts

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.

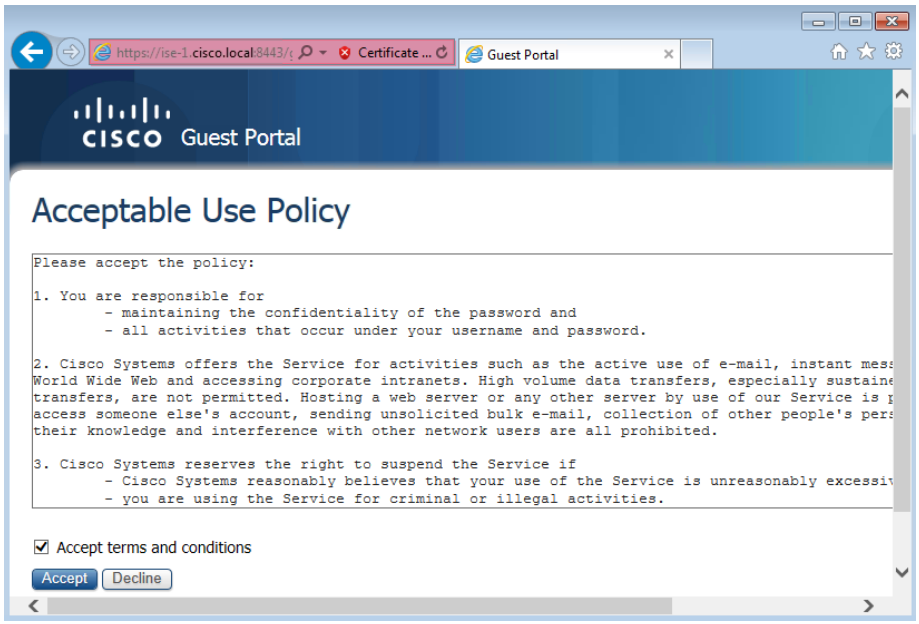
Step 1: From a wireless device, connect to the wireless guest network created. (Example: Guest)

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.

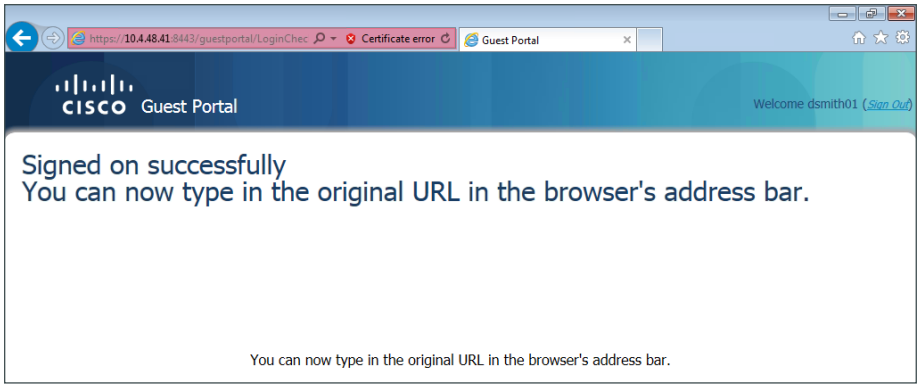


Step 3: Enter guest credentials. The Acceptable Use Policy opens.

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.



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 Controller	Cisco 7500 Series Wireless Controller for up to 6000 Cisco access points	AIR-CT7510-6K-K9	7.6.120.0
	Cisco 7500 Series Wireless Controller for up to 3000 Cisco access points	AIR-CT7510-3K-K9	
	Cisco 7500 Series Wireless Controller for up to 2000 Cisco access points	AIR-CT7510-2K-K9	
	Cisco 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 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	
	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, Guest Controller	Cisco 2500 Series Wireless Controller for up to 50 Cisco access points	AIR-CT2504-50-K9	7.6.120.0
	Cisco 2500 Series Wireless Controller for up to 25 Cisco access points	AIR-CT2504-25-K9	
	Cisco 2500 Series Wireless Controller for up to 15 Cisco access points	AIR-CT2504-15-K9	
	Cisco 2500 Series Wireless Controller for up to 5 Cisco access points	AIR-CT2504-5-K9	

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 Virtual Switch Pair	Cisco Catalyst 6800 Series 6880-X Extensible Fixed Aggregation Switch (Standard Tables)	C6880-X-LE	15.1(2)SY3 IP Services license
	Cisco Catalyst 6800 Series 6880-X Multi Rate Port Card (Standard Tables)	C6880-X-LE-16P10G	
Modular Distribution Layer Virtual Switch Pair	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
	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 Distribution Layer Switch	Cisco Catalyst 3850 Series Stackable Switch with 12 SFP Ethernet	WS-C3850-12S	3.3.3SE(15.0.1EZ3) IP Services license
	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.

B-0000355-1 09/14