Campus Wireless LAN

TECHNOLOGY DESIGN GUIDE

August 2013

CISCO VALIDATED DESIGN

Table of Contents

Preface

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

CVDs include two guide types that provide tested and validated design and deployment 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 or reference existing CVDs, but also include product features and functionality across Cisco products and may 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 using their own setup and configuration.

How to Read Commands

Many CVD guides tell you how to use a command-line interface (CLI) to configure network devices. This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

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

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

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

Commands at a CLI or script prompt appear as follows:

```
Router# enable
```

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

```
police rate 10000 pps burst 10000 packets conform-action set-discard-class-
transmit 48 exceed-action transmit
```

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

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

Comments and Questions

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

For the most recent CVD guides, see the following site:

http://www.cisco.com/go/cvd

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.
- **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.

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
- Internet edge firewalls and demilitarized zone (DMZ) switching
- Campus routing, switching, and multicast
- High availability wireless using access point stateful switchover (AP SSO)
- Management of user authentication and policy
- Integration of the above with the LAN and data center switching infrastructure

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
- **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

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 following site: http://www.cisco.com/go/cvd

Introduction

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: 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

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.

Benefits:

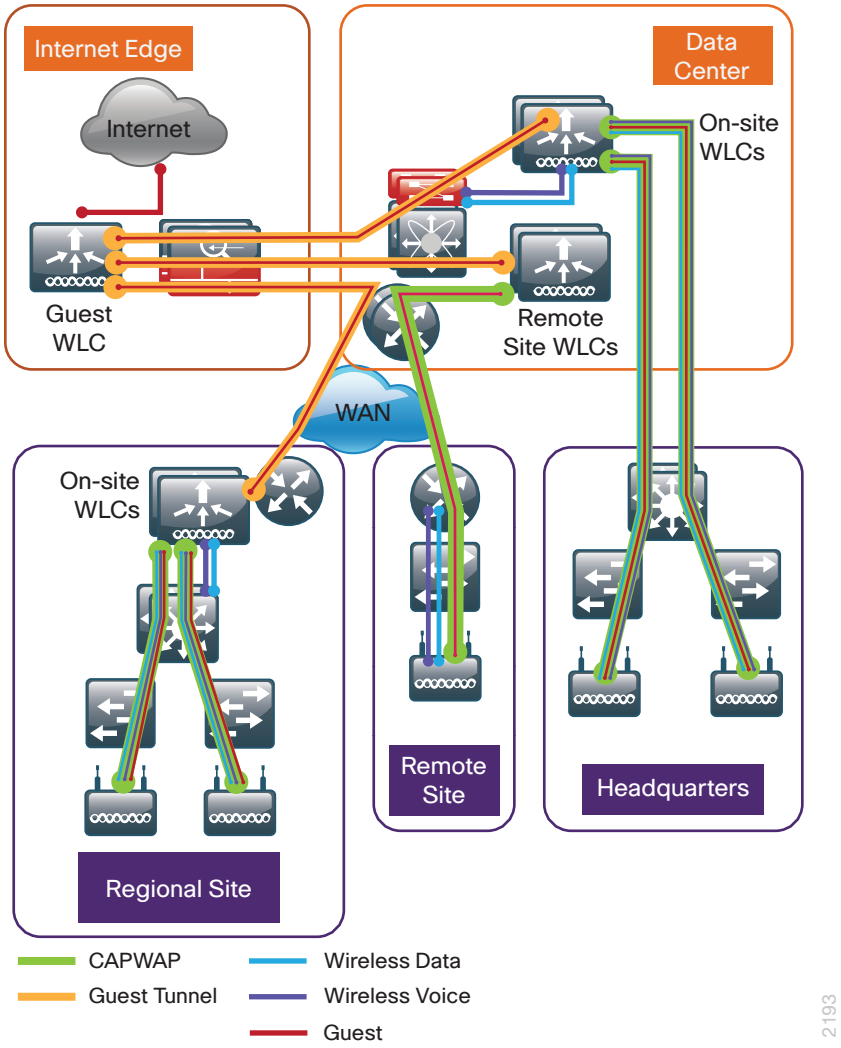
- **Productivity gains through secure, location-independent network access**—Measurable productivity improvements and communication.
- **Additional network flexibility**—Hard-to-wire locations can be reached without costly construction.
- **Cost effective deployment** – Adoption of virtualized technologies within the overall wireless architecture.
- **Easy to manage and operate**—From a single pane of glass, an organization has centralized control of a distributed wireless environment.
- **Plug-and-play deployment**—Automatic provisioning when an access point is connected to the supporting wired network.
- **Resilient, fault-tolerant design**—Reliable wireless connectivity in mission-critical environments, including complete RF-spectrum management.
- **Support for wireless users**—Bring your Own Device (BYOD) design models.
- **Efficient transmission of multicast traffic**– Support for many group communication applications, such as video and push-to-talk.

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

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

- **Lower operational expenses**—A controller-based, centralized architecture enables zero-touch configurations for lightweight access points. Similarly, it enables easy design of channel and power settings and real-time management, including identifying any RF holes in order to optimize the RF environment. The architecture offers seamless mobility across the various access points within the mobility group. A 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 release of CVD:

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

Because software license flexibility allows you to add additional access points as business requirements change, you can choose the controller that will support your needs long-term, but you purchase incremental 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 was used to map access points to their WLCs. Using Option 43 allows remote sites and each campus to define a unique mapping.

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

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

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

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

This release of the CVD 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.

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

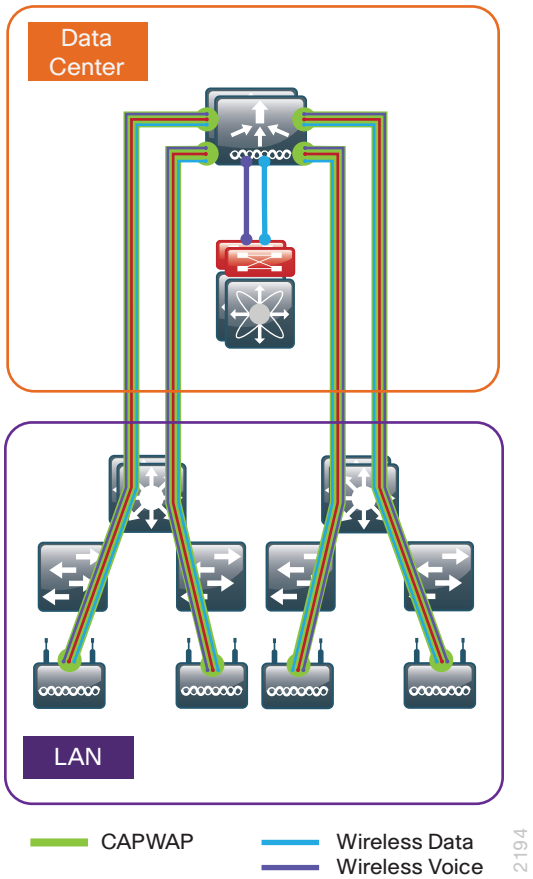
Design Models

Cisco Unified Wireless networks support two major 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 is connected to a LAN distribution layer at the site, and traffic between wireless LAN clients and the LAN is tunneled in Control and Provisioning of Wireless Access Points (CAPWAP) protocol between the controller and the access point.

Figure 2 - Local-mode design model



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

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

- Seamless mobility—In a campus environment, it is crucial that users remain connected to their session even while walking between various floors or adjacent buildings with changing subnets. The local 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 has a LAN distribution layer.
- The site has more than 50 access points.
- The site has a WAN latency greater than 100 ms round-trip to a proposed shared controller.

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

Cisco FlexConnect Design Model

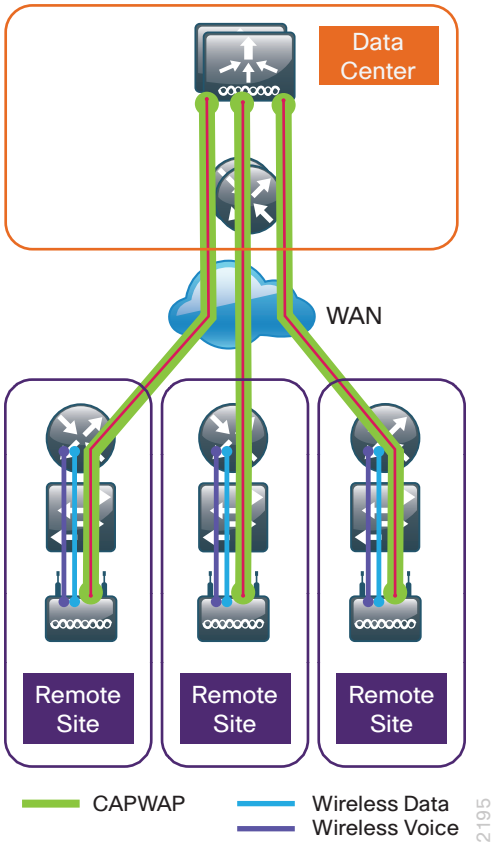
Cisco FlexConnect is a wireless solution for remote-site deployments. It enables organizations to configure and control remote-site access points from the headquarters through the WAN, without deploying a controller in each remote site.

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

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

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

Figure 3 - Cisco FlexConnect design model



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

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

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

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

High Availability

As mobility continues to increase its influence in all aspects of our personal and professional lives, availability continues to be a top concern. The Cisco 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), the resiliency of the wireless network continues to improve. By adopting the cost effective AP SSO licensing model, Cisco wireless deployments can improve the availability of the wireless network with recovery times in the sub-second range during a WLC disruption. In addition, AP SSO allows the resilient WLC to be cost-effectively licensed as a standby controller with its access point (AP) license count being automatically inherited from its paired primary WLC.

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

Multicast Support

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

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

Remote sites that utilized the Cisco Flex 7500 Series Cloud Controller or vWLC using Cisco FlexConnect in local switching mode can also benefit from the use of multicast-based applications. Multicast in 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.

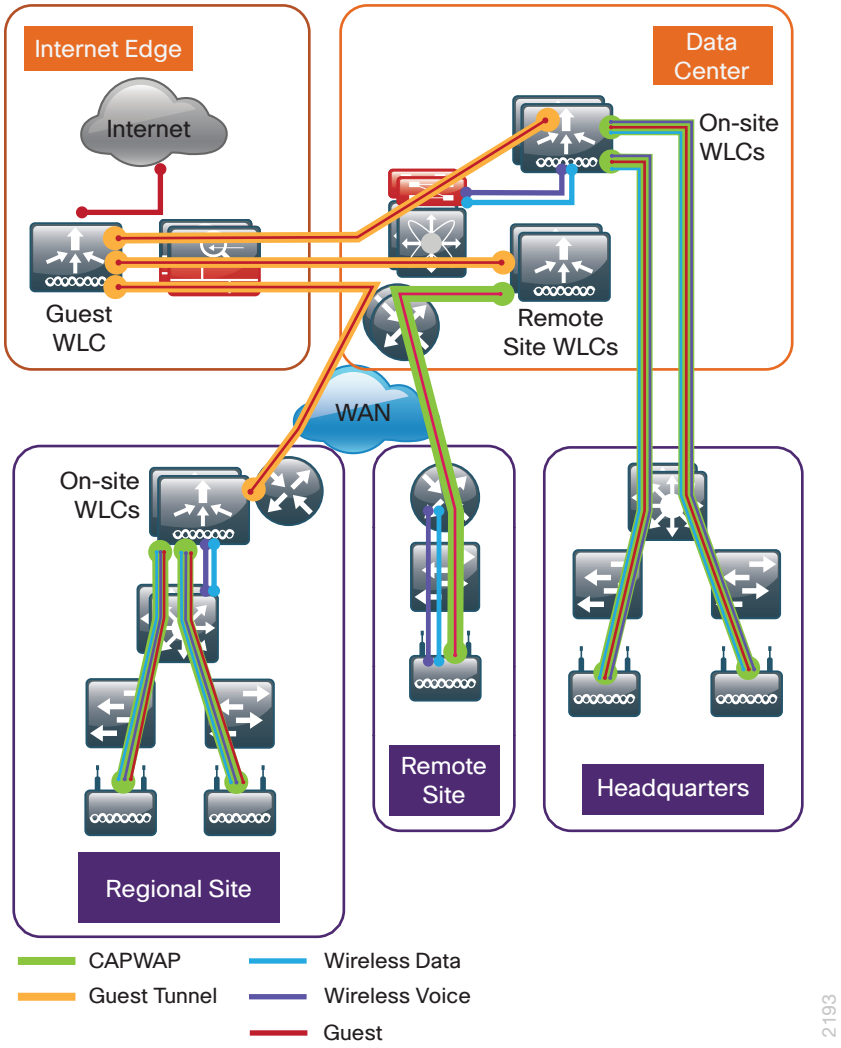
In each of the wireless design models in this CVD, the multicast support that users are accustomed to on a wired network is available wirelessly for those applications and user groups that require it.

Guest Wireless

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

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

Figure 4 - Wireless architecture overview



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

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

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

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

Deployment Details

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

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

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

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

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

PROCESS

Configuring the RADIUS Server: Cisco Secure ACS

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

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

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

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

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

Tech Tip

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

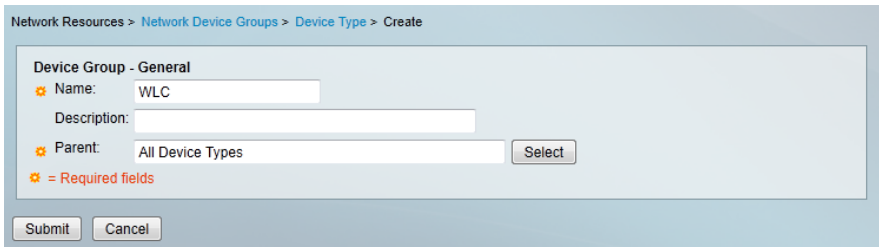
Procedure 1 Create the wireless device type group

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

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

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

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



Procedure 2 Create the TACACS+ shell profile

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

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

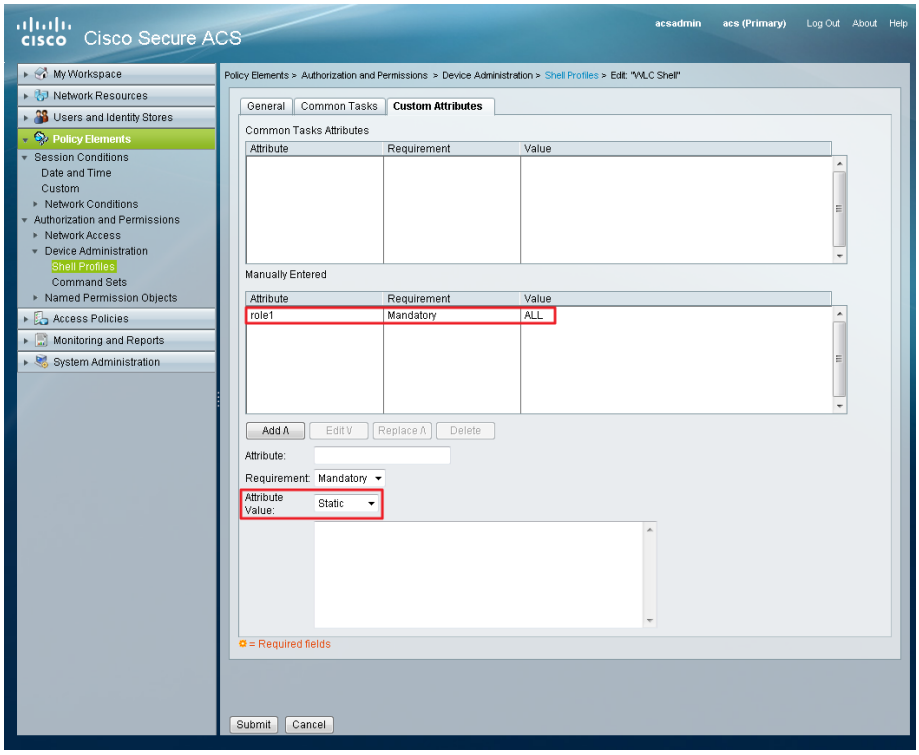
Step 2: On the General tab, In the **Name** box, enter a name for the wireless shell profile. (Example: WLC Shell)

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

Step 4: In the **Requirement** list, choose **Mandatory**.

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

Step 6: In the **Attribute Value** list, choose **Static**, and then click **Submit**.



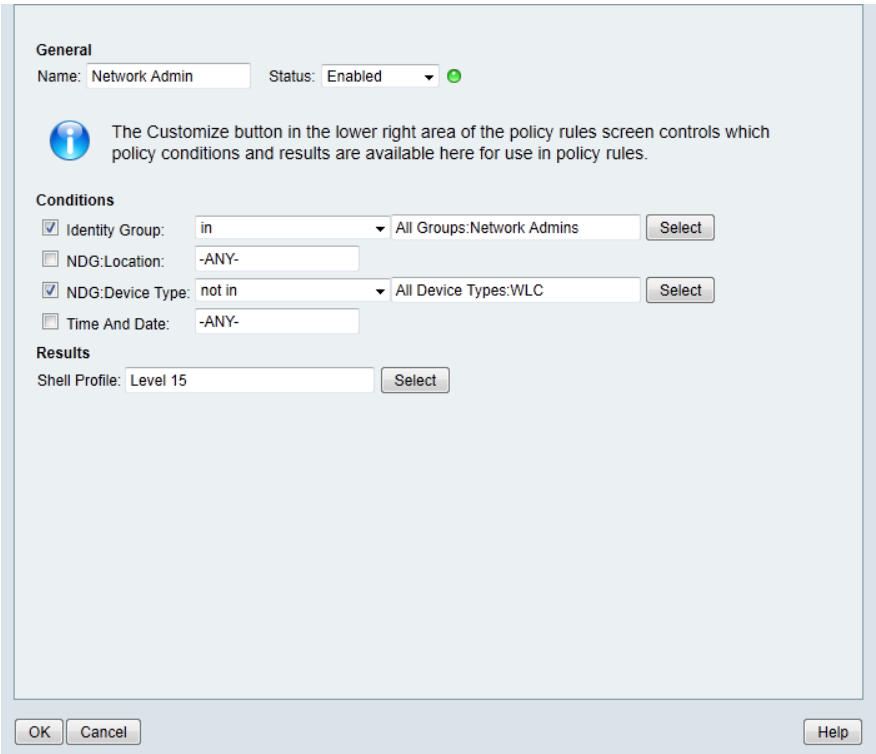
Procedure 3 Modify the device admin access policy

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

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

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

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



Next, you create a WLC authorization rule.

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

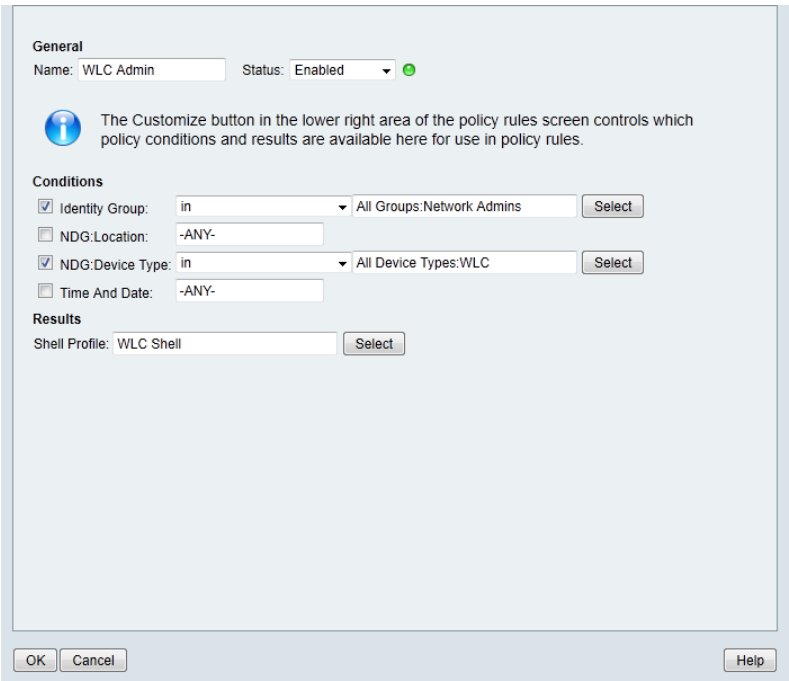
Step 5: In the **Name** box, enter a name for the WLC authorization rule. (Example: WLC Admin)

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

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

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

Step 9: Click **Save Changes**.

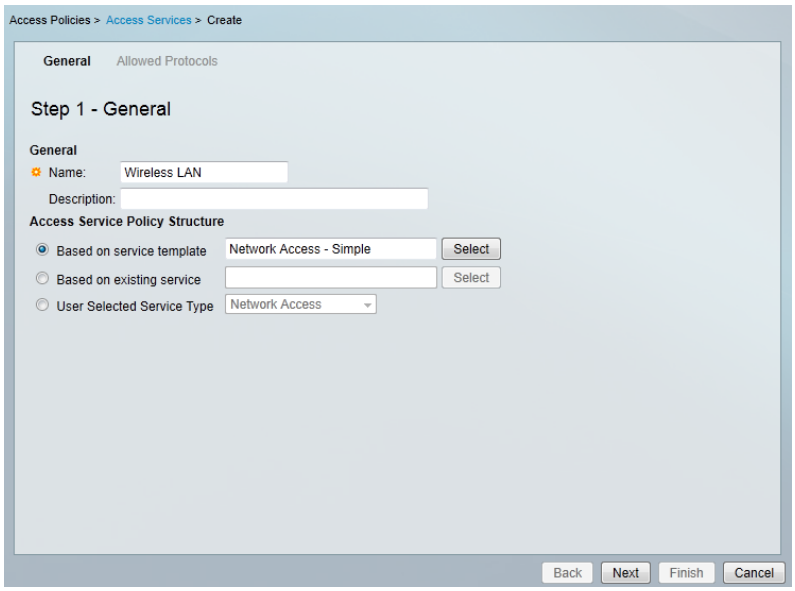


Procedure 4 Create the network access policy

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

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

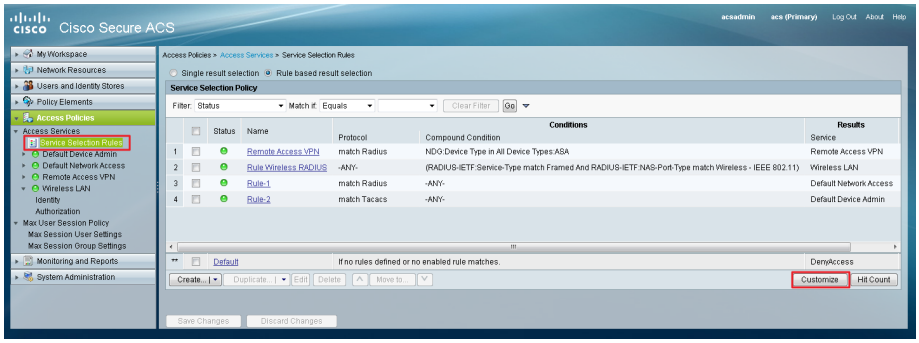
Step 3: In the **Based on Service Template** box, select **Network Access - Simple**, and then click **Next**.



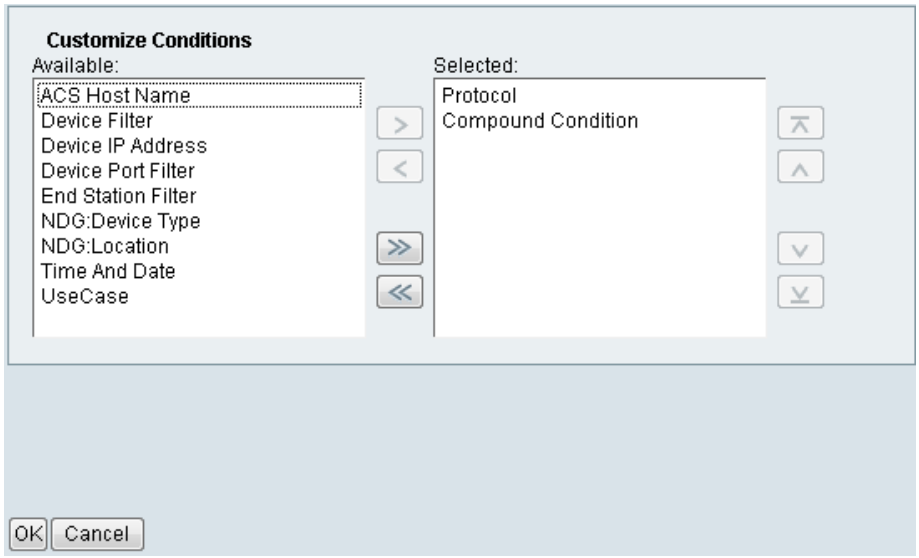
Step 4: On the Allowed Protocols pane, ensure **Allow PEAP** and **Allow EAP-Fast** are selected, and then click **Finish**.

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

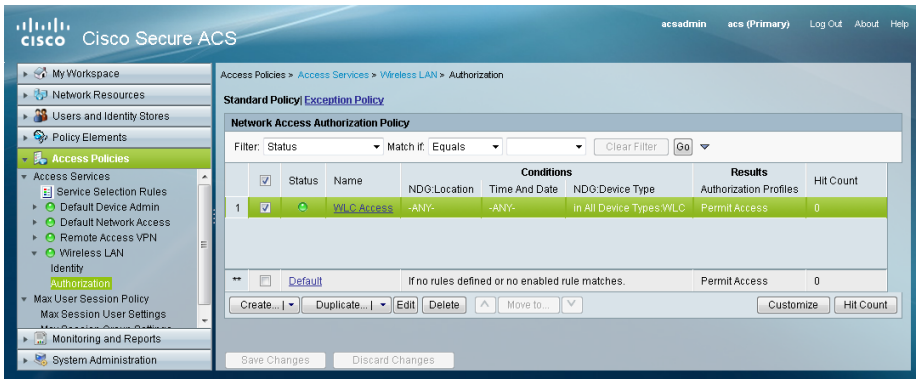
Step 6: On the Service Selection Rules pane, click **Customize**.



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



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



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

Step 9: Click **Create > Create Above**.

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

Step 11: Under Conditions, select **Compound Condition**.

Step 12: In the **Dictionary** list, choose **RADIUS-IETF**.

Step 13: In the **Attribute** box, select **Service-Type**.

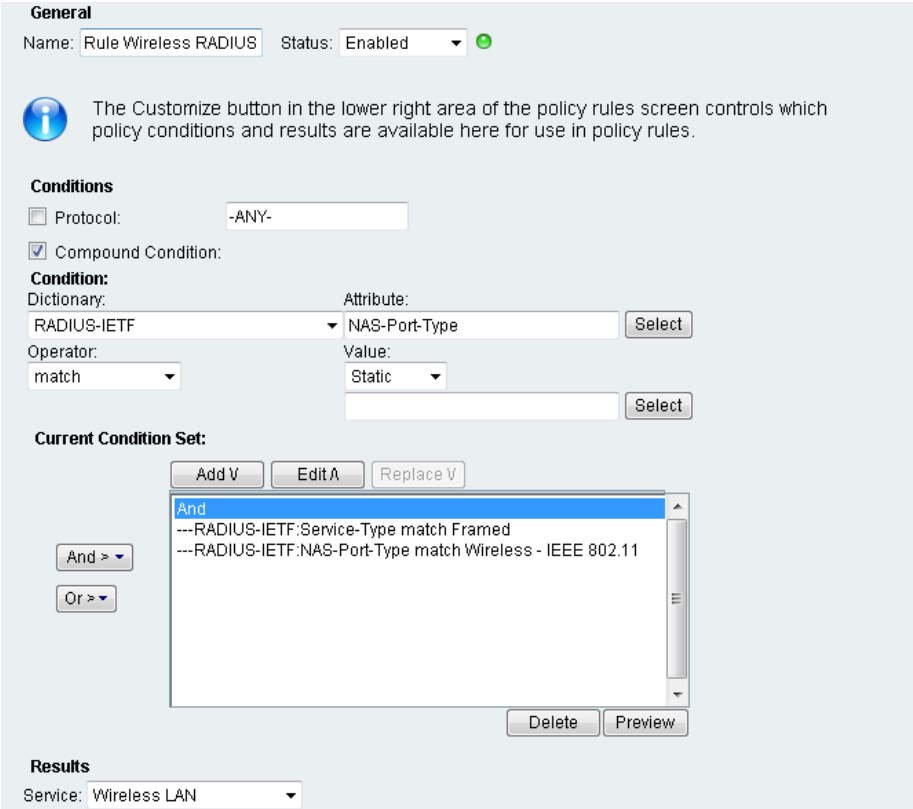
Step 14: In the **Value** box, select **Framed**, and then click **Add V**.

Step 15: Under Current Condition Set, click **And > Insert**.

Step 16: In the **Attribute** box, select **NAS-Port-Type**.

Step 17: In the **Value** box, select **Wireless - IEEE 802.11**, and then click **Add V**.

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



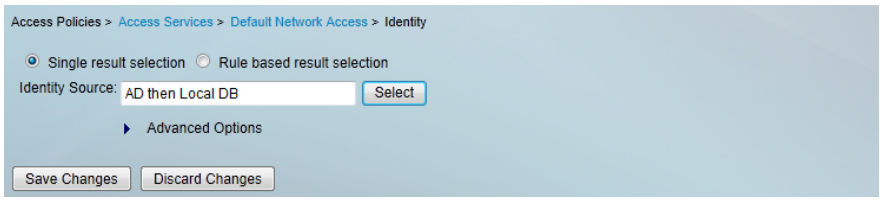
Step 19: On the Service Selection Rules pane, click **Save Changes**.

Procedure 5 Modify the network access policy

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

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

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



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

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

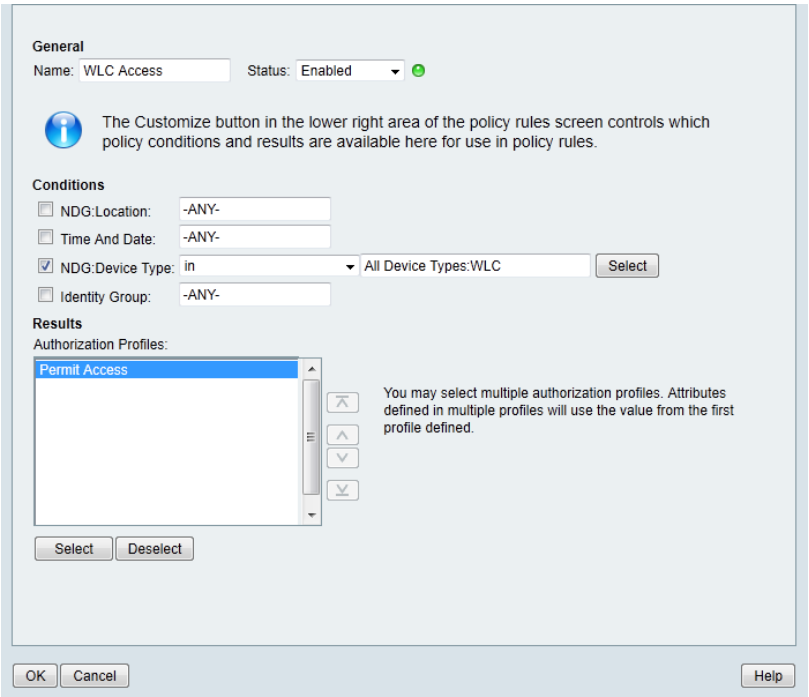
Step 5: Using the arrow buttons, move **NDG:Device Type** from the **Available** list to the **Selected** list, and then click **OK**.

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

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

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

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



Step 10: Click **Save Changes**.

Procedure 6 Create the network device

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

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

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

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

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

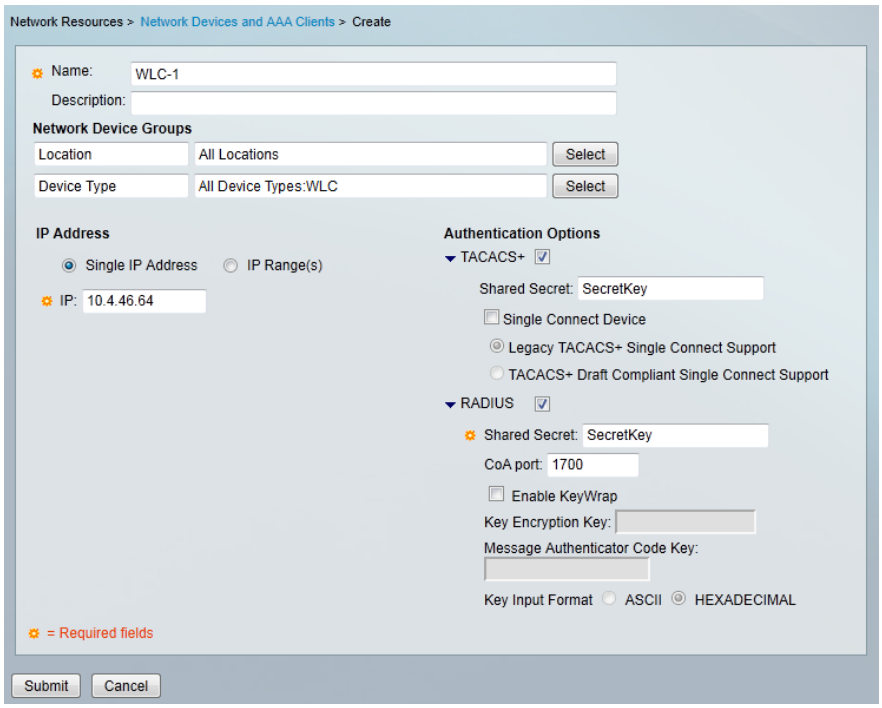
Step 4: In the **IP** box, enter the WLCs management interface IP address. (Example: 10.4.46.64)

Step 5: Select **TACACS+**.

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

Step 7: Select **RADIUS**.

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



Procedure 7 Enable the default network device

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

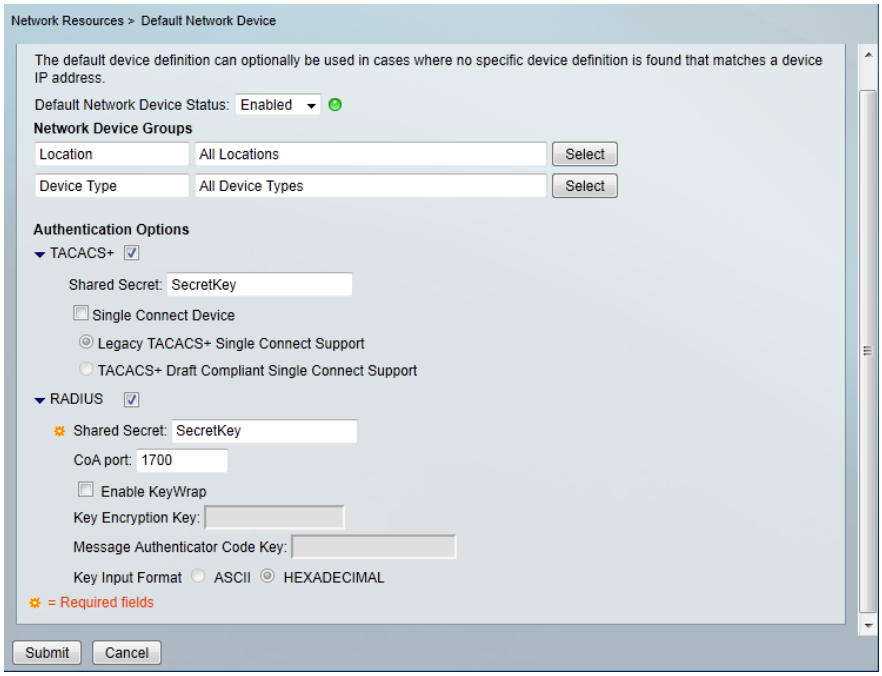
Step 1: Navigate to **Network Resources > Default Network Device**.

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

Next, you must show the RADIUS configuration.

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

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



PROCESS

Configuring the RADIUS Server: Windows Server 2008

1. Install services
2. Add the Certification Authority snap-in
3. Enroll certificates
4. Register Server in Active Directory

If you want to configure the RADIUS server on Cisco Secure ACS, use the previous process instead of this one.

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

Tech Tip

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

Procedure 1 Install services

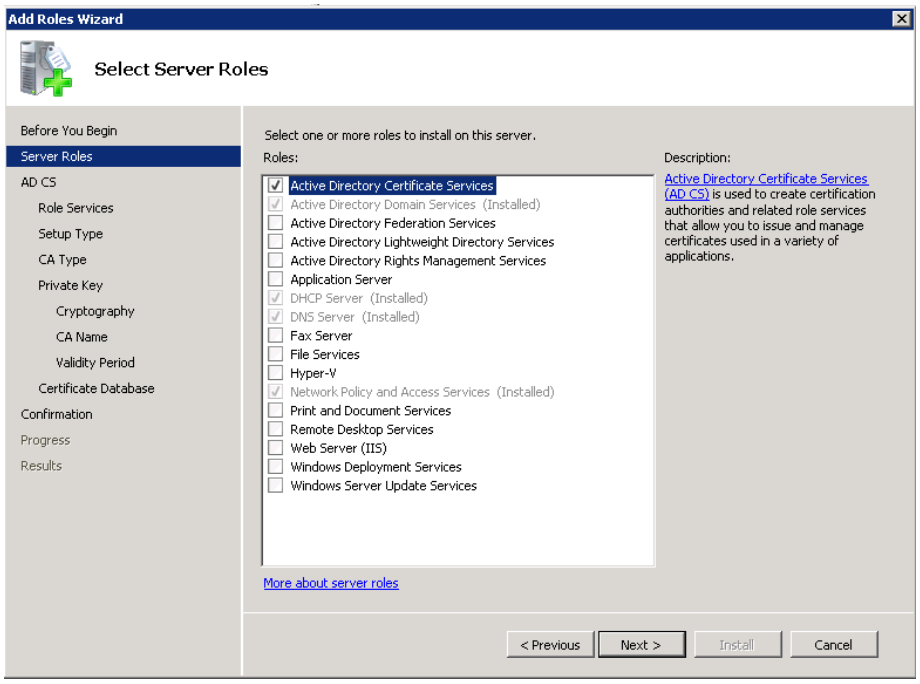
Step 1: Join the server to your existing domain (Example: cisco.local), and then restart the server.

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

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

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

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



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

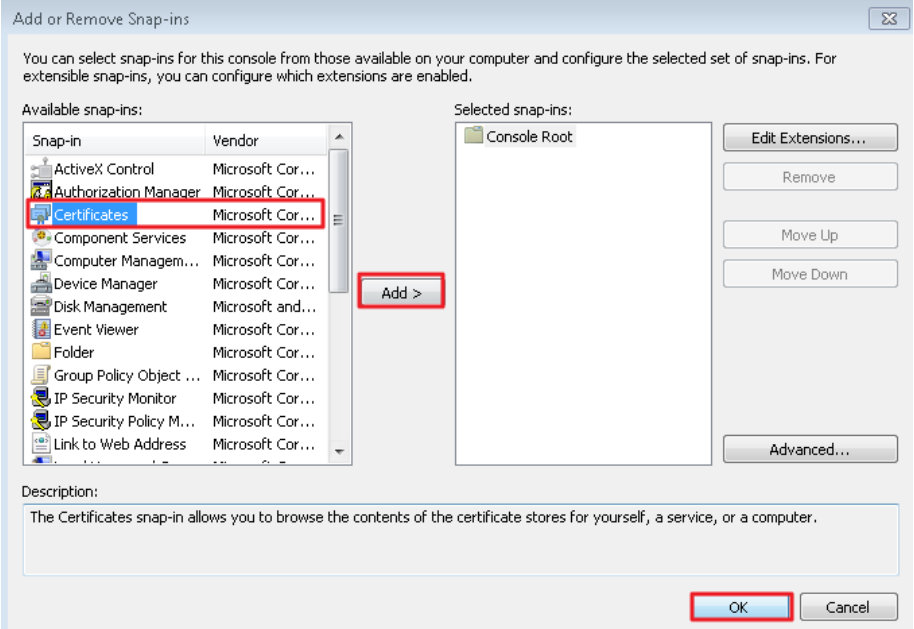
Follow the rest of the instructions in the wizard, making any changes you want or just leaving the default values as appropriate. Note that there is a warning at the end of the wizard, stating that the name of this server cannot be changed after installing the AD CS role.

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

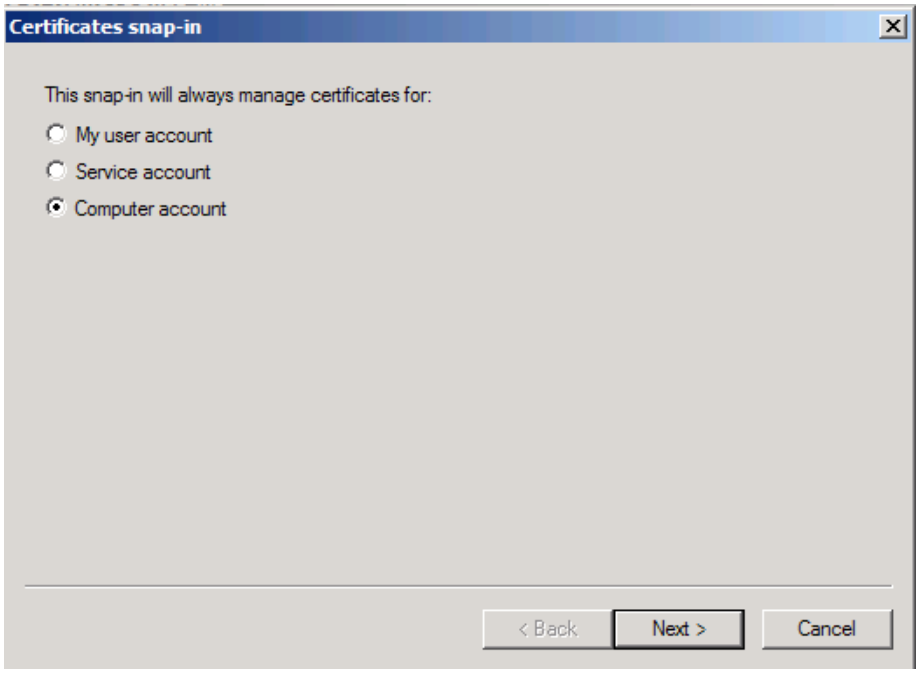
Procedure 2 Add the Certification Authority snap-in

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

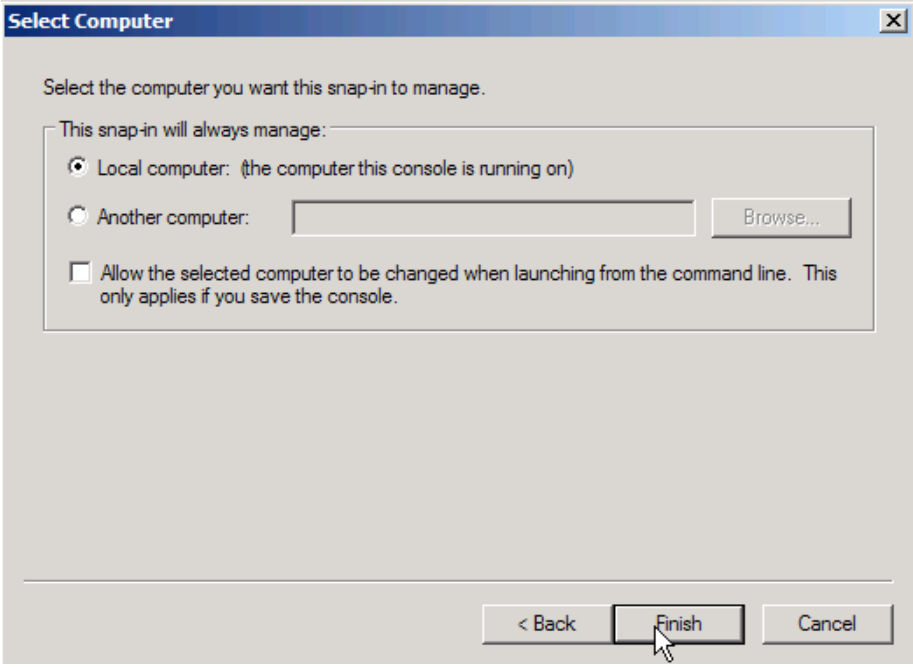
Step 2: Choose Certificates from the available snap-ins.



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

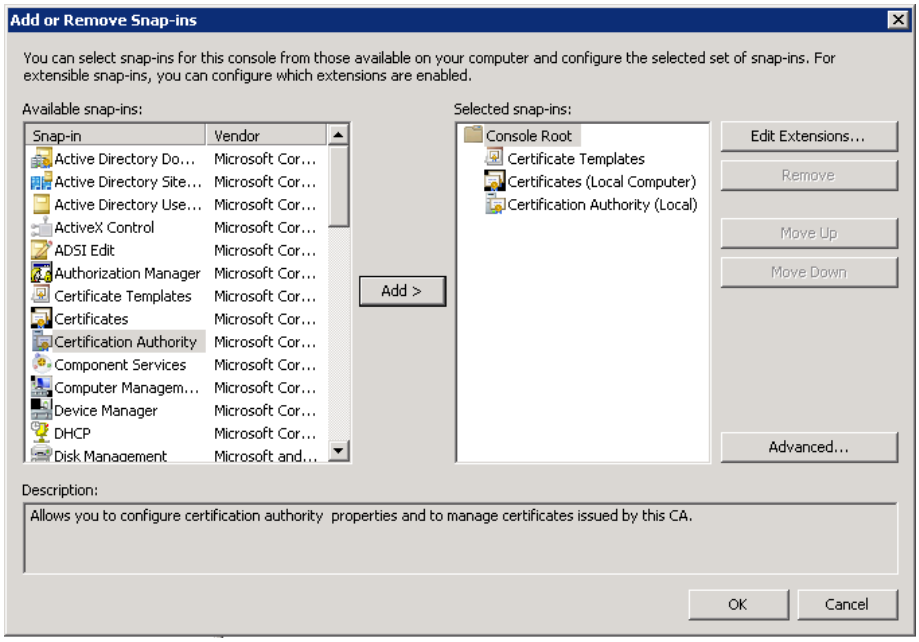


Step 4: On the Select Computer page, select **Local computer**, and then click **Finish**.



Next, add the Certification Authority snap-in.

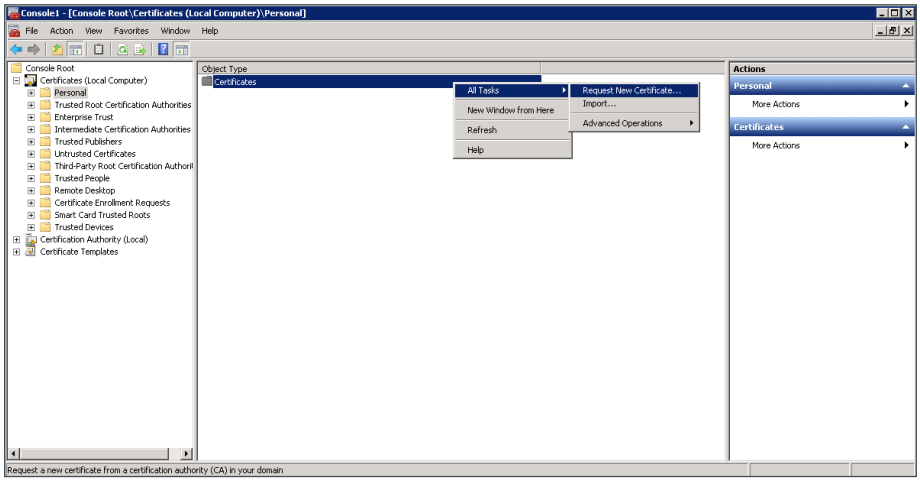
Step 5: On the Add or Remove Snap-ins dialog box, in the **Available snap-ins** list, choose **Certification Authority**, click **Add >**, choose **Local computer**, and then click **Finish**.



Step 6: On the Add or Remove Snap-ins dialog box, in the **Available snap-ins** list, choose **Certificate Templates**. The RAS/IAS template is added.

Step 7: Click **OK**. This completes the process of adding snap-ins.

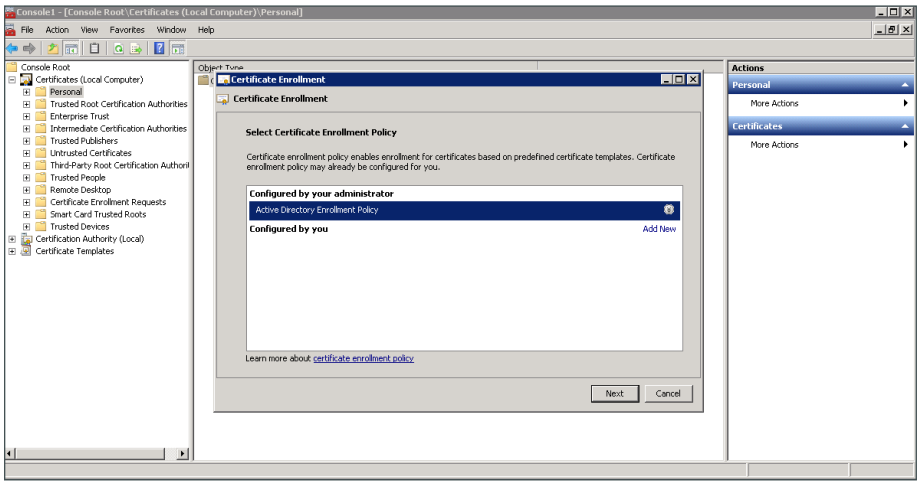
Step 8: Expand **Certificates (Local Computers) > Personal**, right-click **Certificates**, and then click **Request new certificate**.



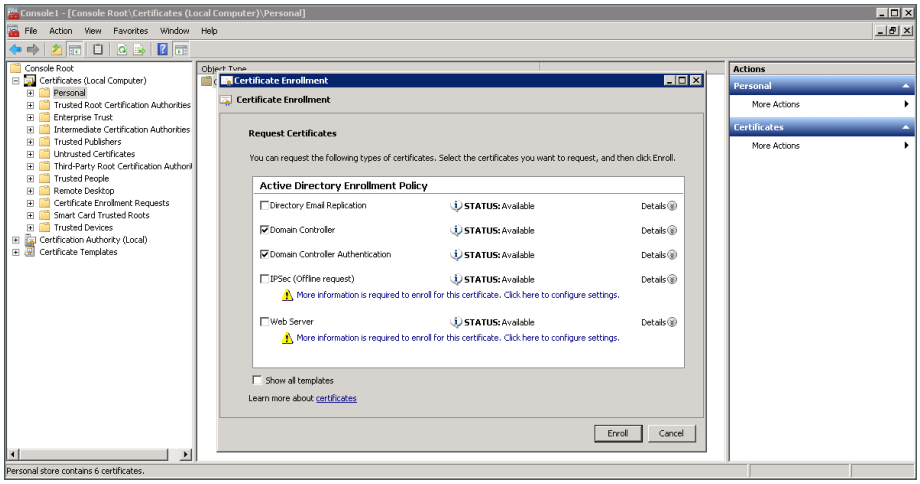
Procedure 3 Enroll certificates

Step 1: Follow the instructions in Certificate Enrollment wizard. Note the following:

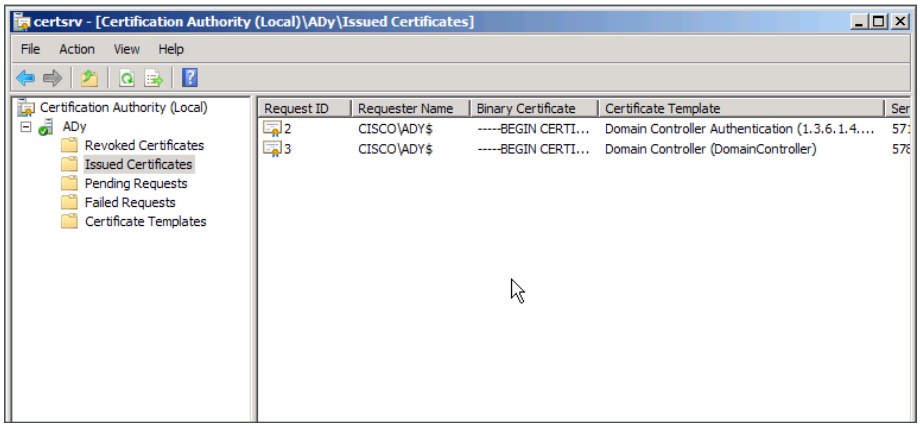
- On the Select Certificate Enrollment Policy page, select **Active Directory Enrollment Policy** as the Enrollment policy for this certificate request.



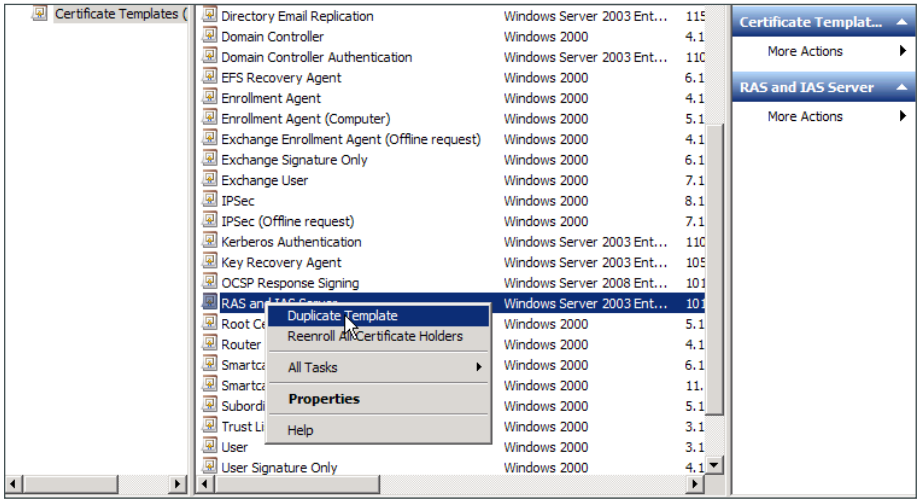
- On the Request Certificates page, select **Domain Controller** and **Domain Controller Authentication** as the type of certificates that are being requested, and then click **Enroll**.



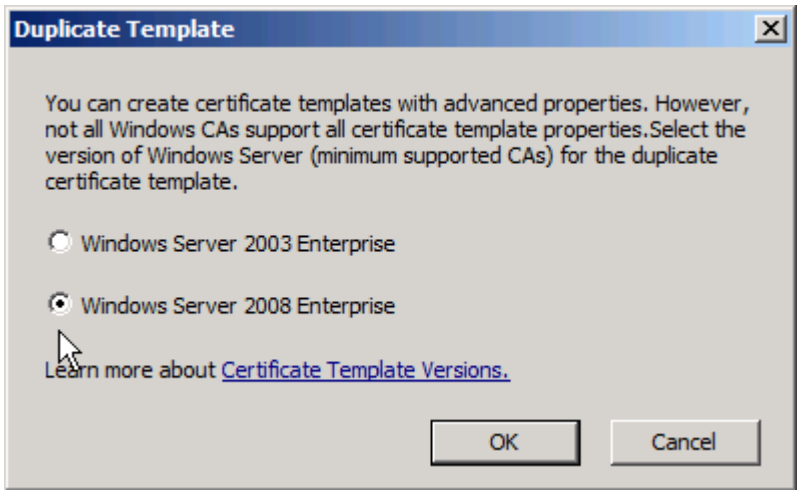
Step 2: Navigate to **Certificate Authority (Local) > Issued Certificates**, and then verify that the Certificate Templates folder appears.



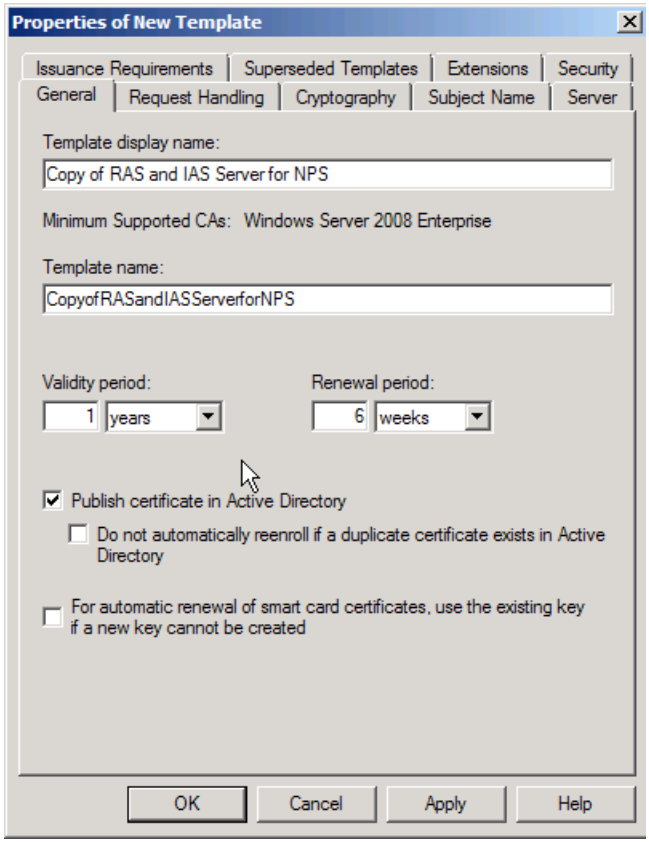
Step 3: Right-click the **Certificate Templates** folder, and in the right pane, right-click **RAS and IAS Server**, and then click **Duplicate Template**.



Step 4: Select **Windows Server 2008 Enterprise**, and then click **OK**.



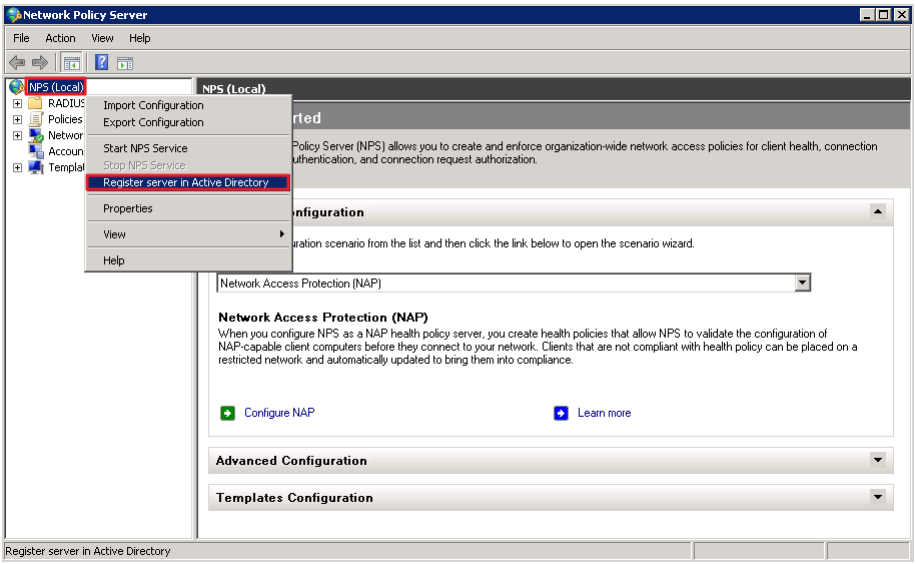
Step 5: In the **Template display name** box, enter a valid display name, select **Publish Certificate in Active Directory**, click **Apply**, and then close the MMC console.



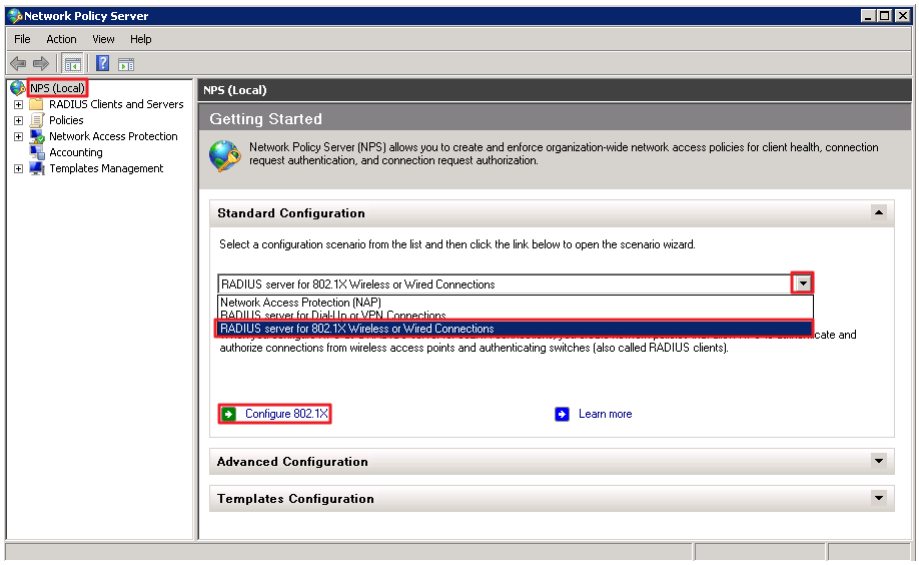
Procedure 4 Register Server in Active Directory

Step 1: Open the Network Policy Server administrative console by navigating to **Start > Administrative Tools > Network Policy Server**.

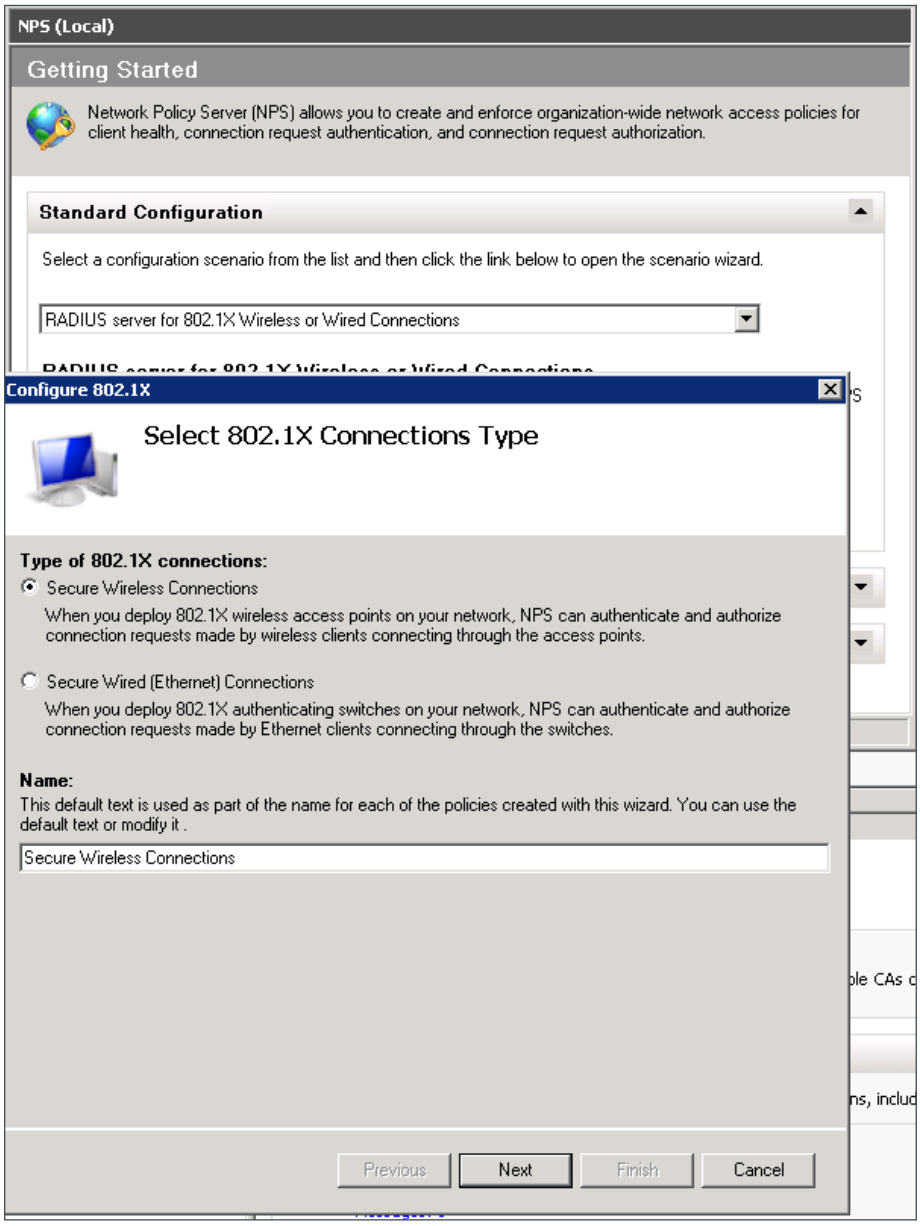
Step 2: Right-click the parent node **NPS (Local)**, click **Register server in Active Directory**, click **OK to authorize this computer to read users' dial-in properties from the domain**, and then click **OK**.



Step 3: With the NPS (Local) node still selected, select **RADIUS server for 802.1X Wireless or Wired Connections**, and then click **Configure 802.1X**.

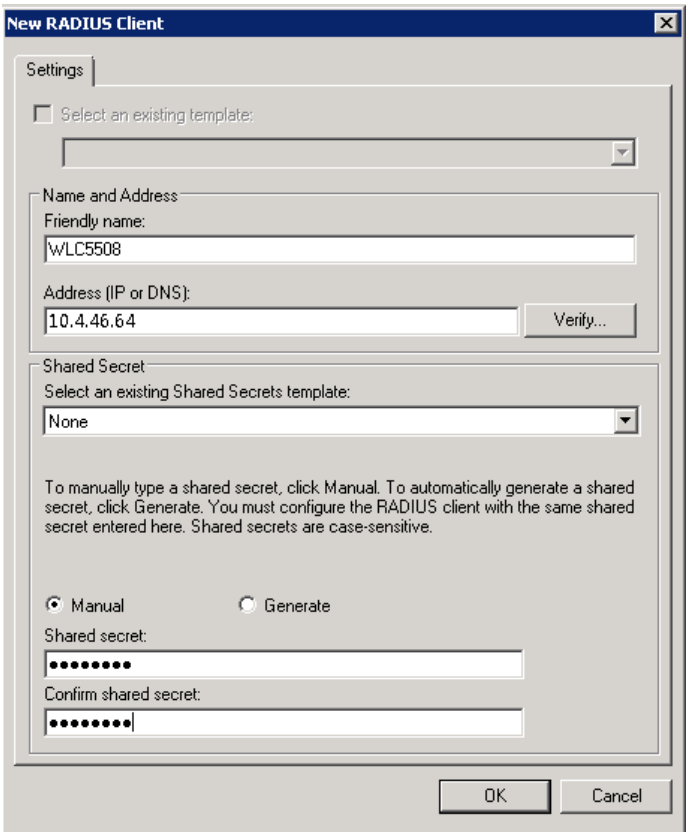


Step 4: In the Configure 802.1X wizard, under Type of 802.1X connections, select **Secure Wireless Connections**, and in the **Name** box, enter an appropriate name for the policies that you want to create, and then click **Next**.



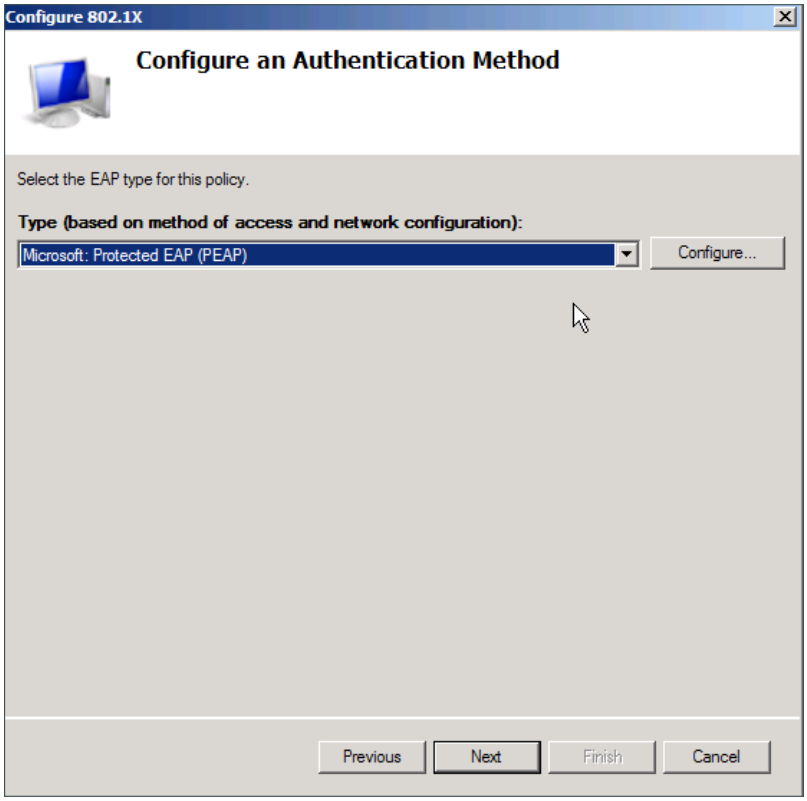
Next, add each of the wireless LAN controllers as RADIUS clients.

Step 5: In the **Friendly name** box, click **Add**, enter a name for the controller (Example: WLC5508), provide the IP address or DNS entry for the controller, provide the Shared Secret (Example: SecretKey), and then click **OK**.

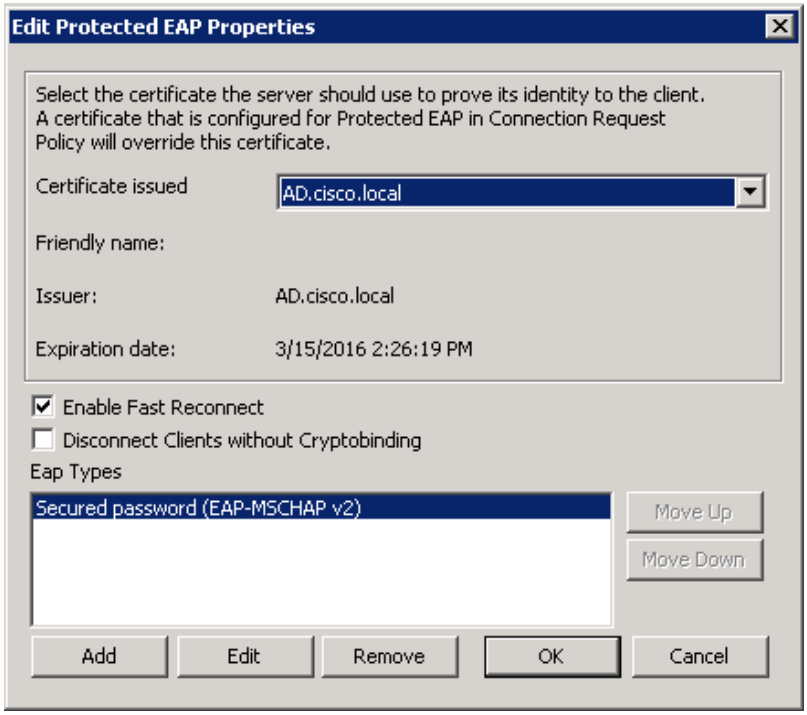


Step 6: Click **Next**.

Step 7: On the Configure an Authentication Method page, in the **Type** box, select **Microsoft: Protected EAP (PEAP)**, and then click **Configure**.



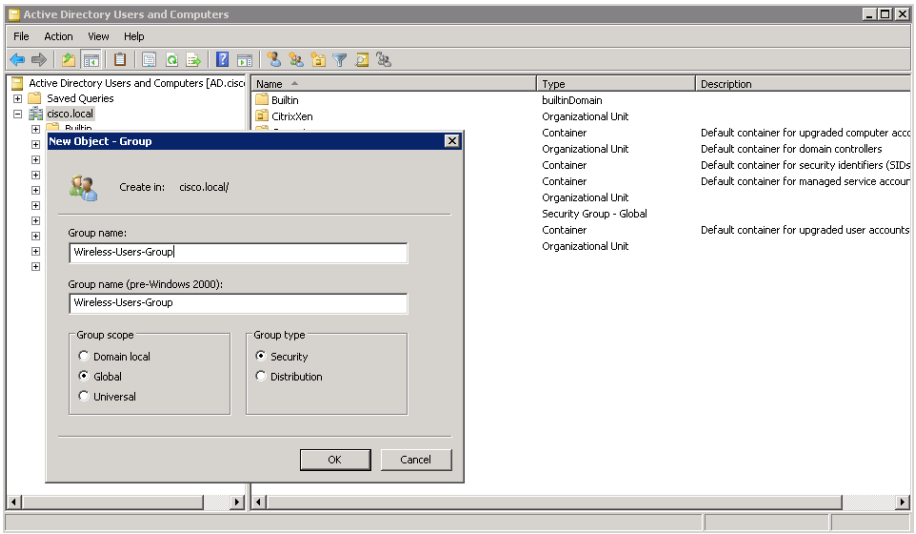
Step 8: In the **Certificate issued** list, ensure that the certificate you enrolled in Step 6 is selected, and then click **OK**.



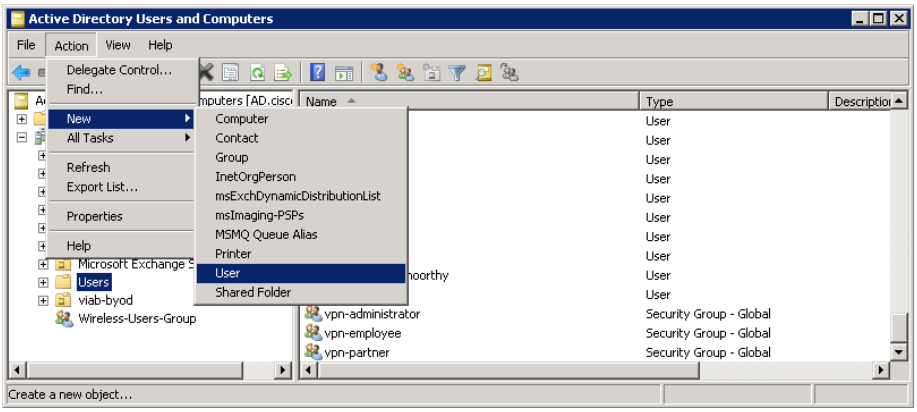
Step 9: If you would like to use a group that you have already created, in Specify User Groups, click **Add**, select the desired group, and then skip to Step 11.

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

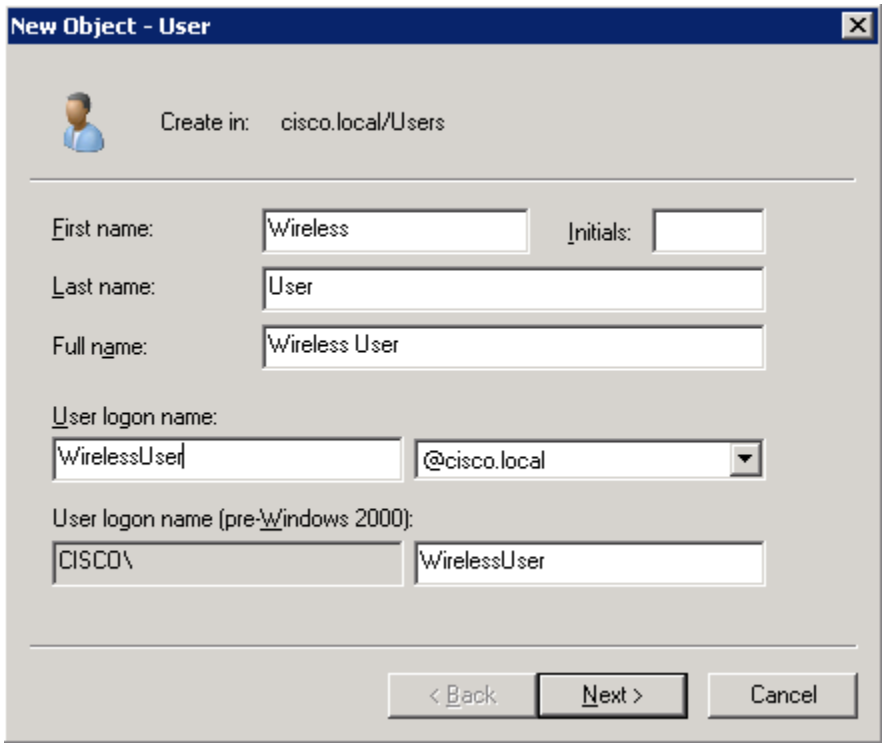
Step 10: Navigate to **Start > Administrative Tools > Active Directory Users and Computers**. In the Active Directory Users and Computers window, right-click **cisco.local**, and then navigate to **New > Group**. Create a group called **Wireless-Users-Group**.



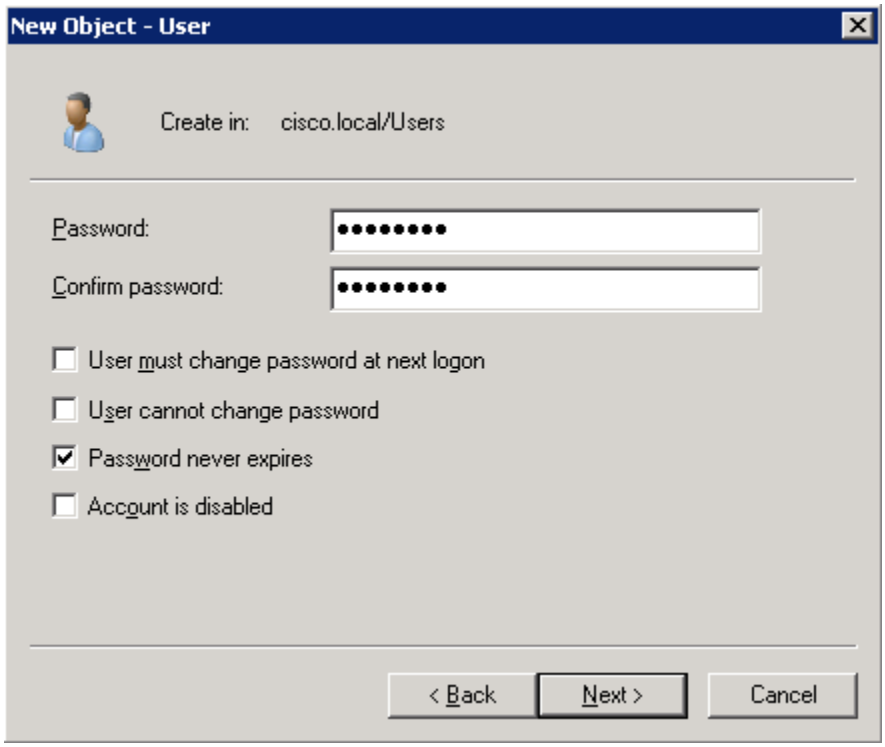
Step 11: In the Active Directory Users and Computer management console, create a wireless user (Example: Wireless User) by selecting the **Action > New > User**.



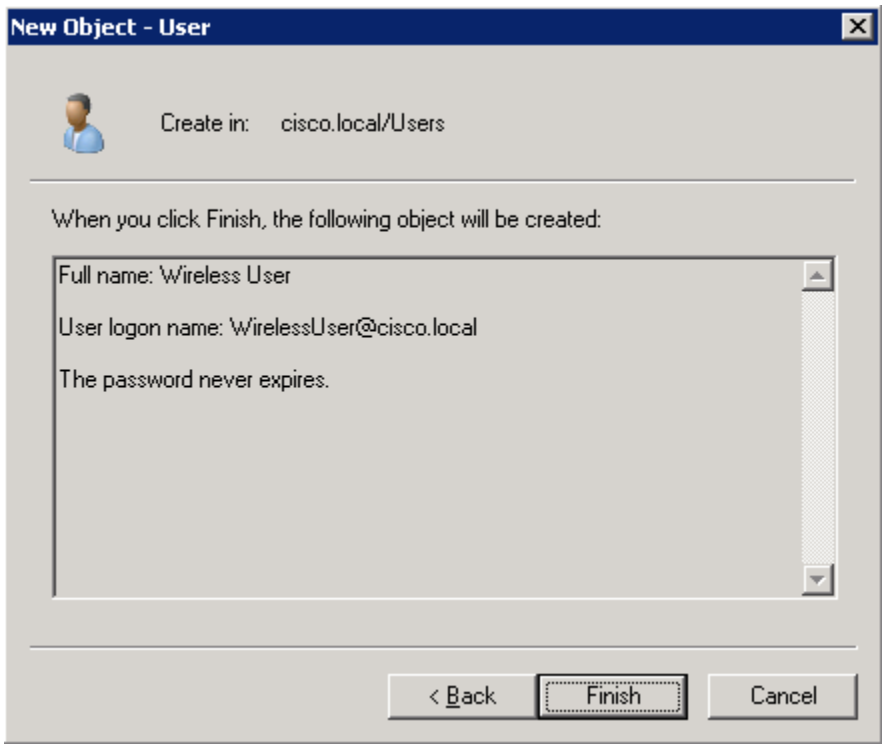
Step 12: Provide the necessary user information, and then click **Next.**.



Step 13: Enter a password, and then click **Next**.

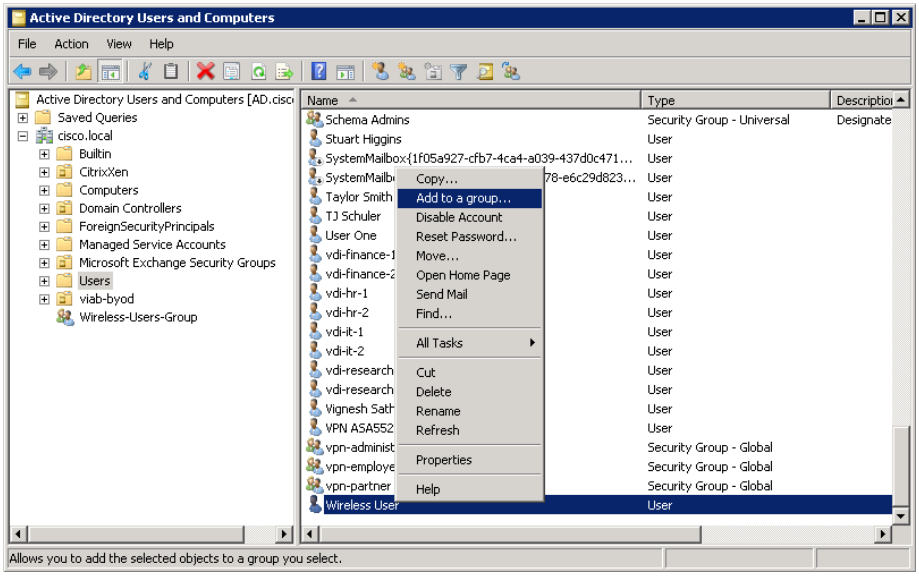


Step 14: Review the information about the new user being added, and click **Finish.**

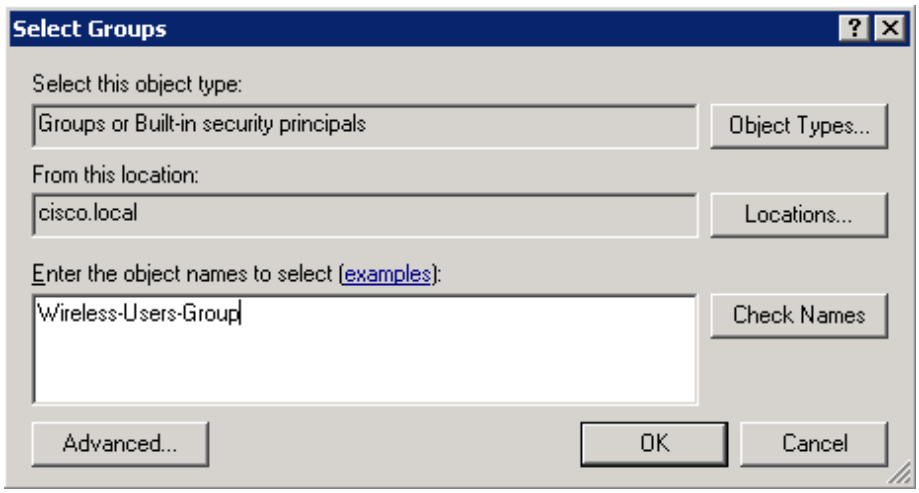


Step 15: Within the Active Directory Users and Computer management console, select the users folder.

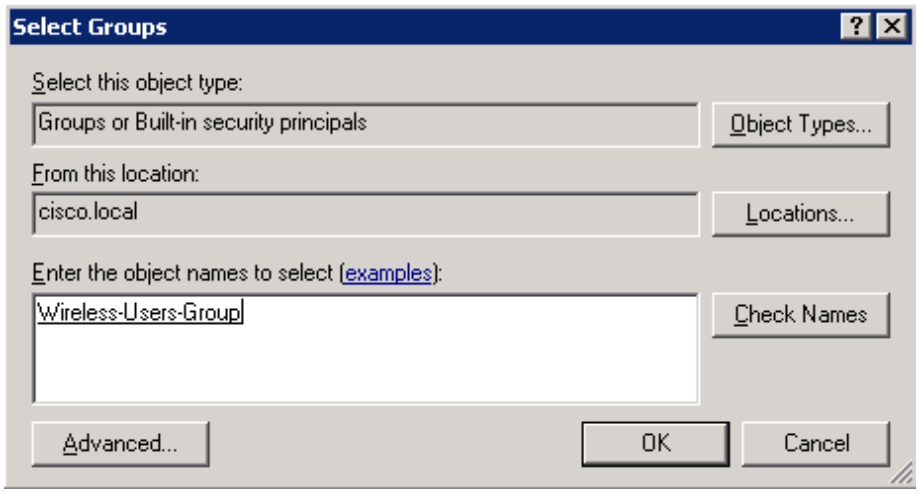
Step 16: Locate the wireless user (Example: Wireless User) that you want to add to the newly created Wireless-Users-Group, and then right click on the user and select **Add to a group...**



Step 17: Enter the name of the Wireless-Users-Group, and then click **Check Names**.



Step 18: Click **OK. This** completes the process of adding the user to the wireless group.

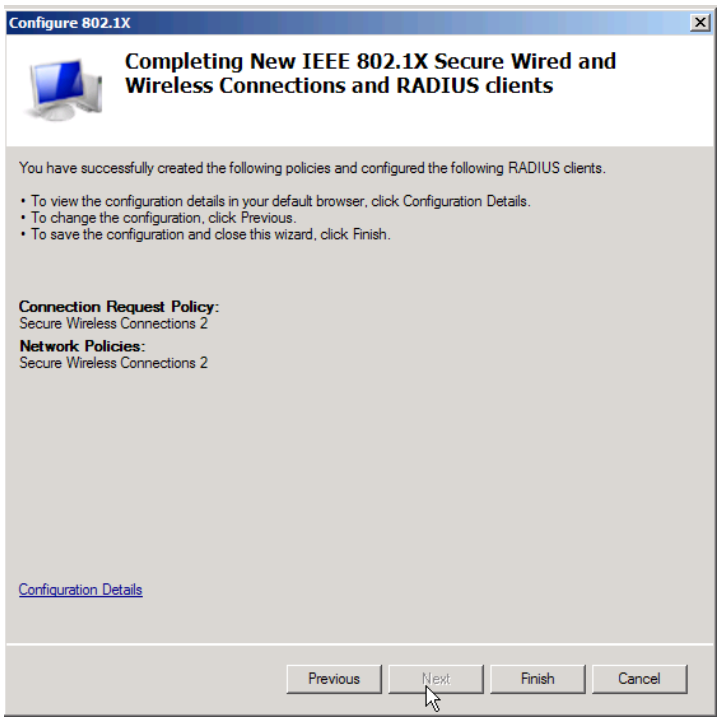


Tech Tip

It is recommended that you add both the machine accounts and user accounts to this group (Example: Wireless-Users-Group) in order to allow the machine to authenticate before the user logs in).

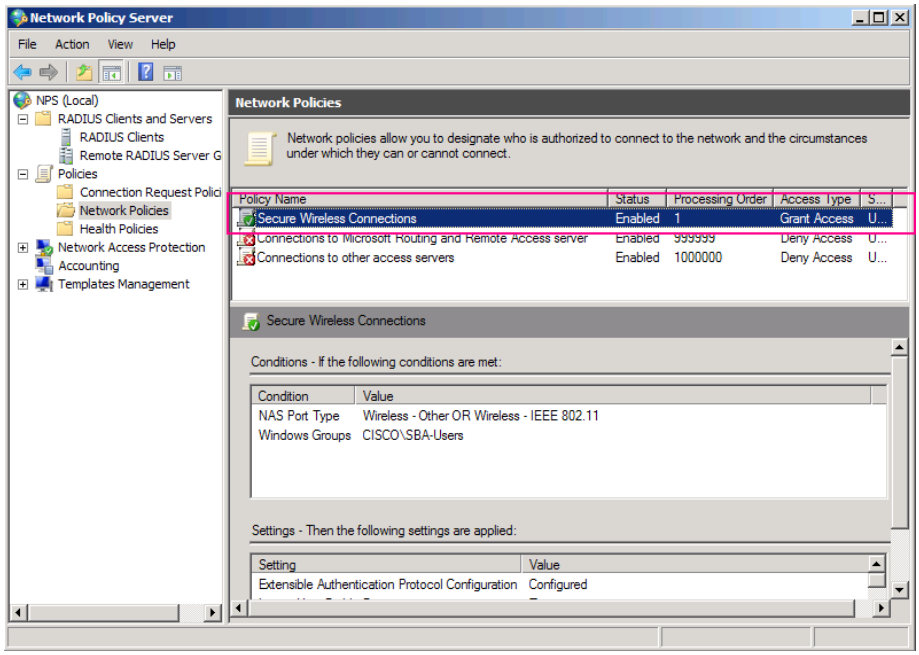
Step 19: On the next step of the Network Policy Server (NPS (Local)) wizard, configure VLAN information or accept the default settings, and then click **Next**.

Step 20: Click **Finish**. This completes the configuration of 802.1X.



Step 21: Restart the Network Policy Server service, and then navigate to **NPS (Local) > Policies**.

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

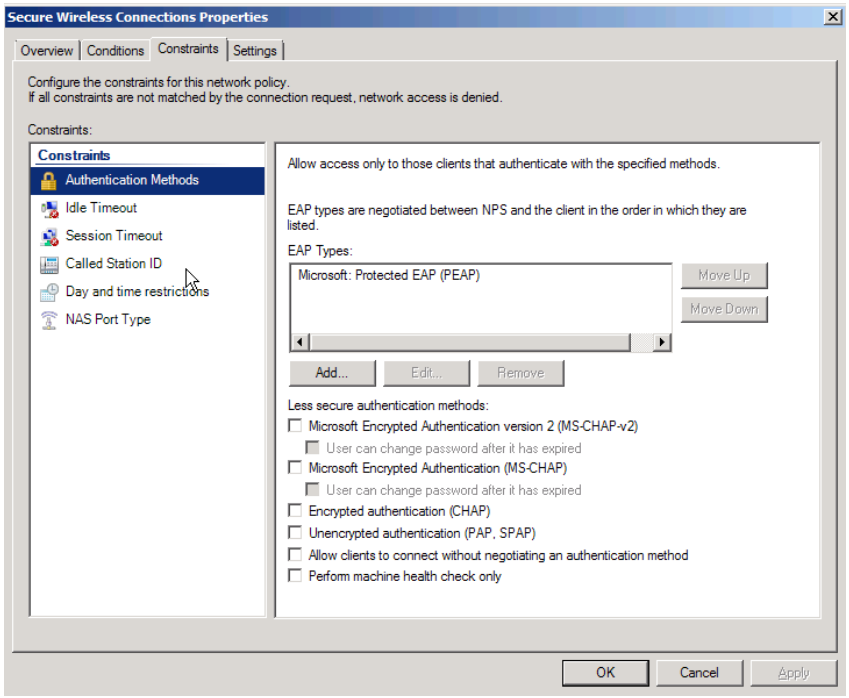


Step 22: If you want to remove the less secure authentication methods and increase the encryption methods in the network policy, continue with this procedure.

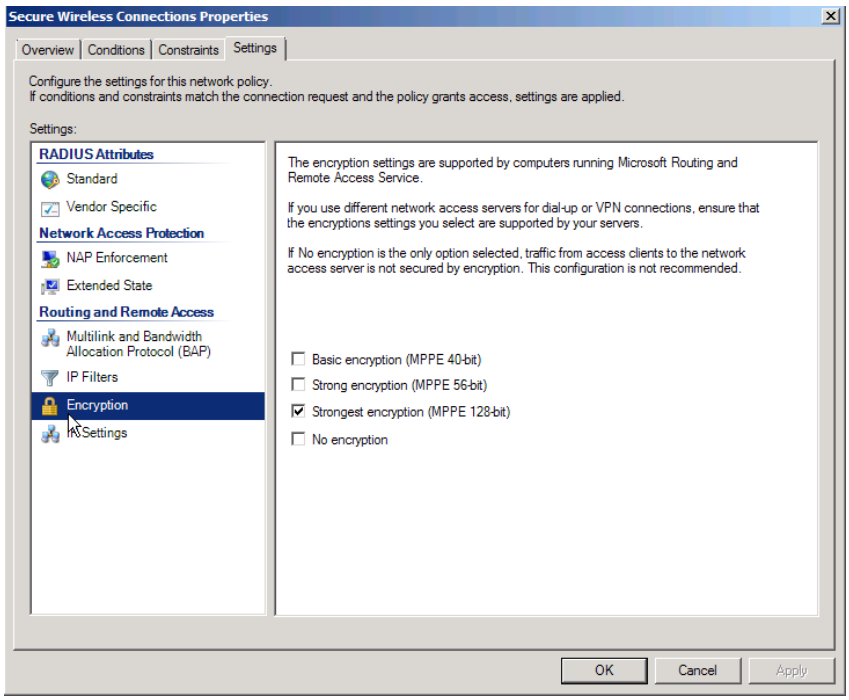
If you would like to use the default authentication and encryption methods, skip to the next process.

Step 23: Under the Network Policies node, open the properties of the newly created policy.

Step 24: On the Constraints tab, under **Less secure authentication methods**, clear all of the check boxes.



Step 25: On the Settings tab, click **Encryption**, clear all check boxes except **Strongest encryption (MPPE 128-bit)**, and then click **OK**.



Step 26: Restart the Network Policy Server service.

PROCESS

Configuring On-Site Wireless Controllers

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

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

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

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

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

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

Table 2 - Cisco on-site wireless controller parameters checklist

Parameter	CVD values primary controller	CVD values resilient controller (optional)	Site-specific values
Controller parameters			
Switch interface number	1/0/3, 2/0/3	1/0/4, 2/0/4	
VLAN number	146	146	
Time zone	PST -8 0	PST -8 0	
IP address	10.4.46.64/24	10.4.46.65/24[2]	
Default gateway	10.4.46.1	10.4.46.1	
Redundant management IP address (AP SSO)1	10.4.46.74[1]	10.4.46.75[1]	
Redundancy port connectivity (AP SSO)[1]	Dedicated Ethernet cable[1]	Dedicated Ethernet cable[1]	
Hostname	WLC-1	WLC-2[2]	
Local administrator username and password	admin/C1sco123	admin/C1sco123	
Mobility group name	CAMPUS	CAMPUS	
RADIUS server IP address	10.4.48.15	10.4.48.15	
RADIUS shared key	SecretKey	SecretKey	
Management network (optional)	10.4.48.0/24	10.4.48.0/24	
TACACS server IP address (optional)	10.4.48.15	10.4.48.15	
TACACS shared key (optional)	SecretKey	SecretKey	
Wireless data network parameters			
SSID	WLAN-Data	WLAN-Data	
VLAN number	116	116	
Default gateway	10.4.16.1	10.4.16.1	
Controller interface IP address	10.4.16.5/22	10.4.16.6/22	
Wireless voice network parameters			
SSID	WLAN-Voice	WLAN-Voice	
VLAN number	120	120	
Default gateway	10.4.20.1	10.4.20.1	
Controller interface IP address	10.4.20.5/22	10.4.20.6/22	

Notes:

1. AP SSO is only supported on the Cisco 5500 Series WLC.
2. The resilient Cisco 2500 Series WLC will require an IP address, as AP SSO is not supported on this platform.

Procedure 1 Configure the switch for the WLC

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

```
vlan 116
 name WLAN_Data
vlan 120
 name WLAN_Voice
vlan 146
 name WLAN_Mgmt
```

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

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

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

```
vlan 116
 name WLAN_Data
vlan 120
 name WLAN_Voice
vlan 146
 name WLAN_Mgmt
```

Step 4: On the server room distribution switch, configure two uplink ports and an EtherChannel trunk to the server room access switches.

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

interface range tenGigabitEthernet [port 1],tenGigabitEthernet [port 2]
 description Link to Server Room Switch
 switchport trunk allowed vlan 116,120,146
 switchport mode trunk
 channel group 12
 logging event link-status

 logging event trunk-status
 no shutdown
```

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

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

interface Port-channel1
 description EtherChannel Link to Distribution Switch
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 116,120,146
 switchport mode trunk
 logging event link-status
 no shutdown
```

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

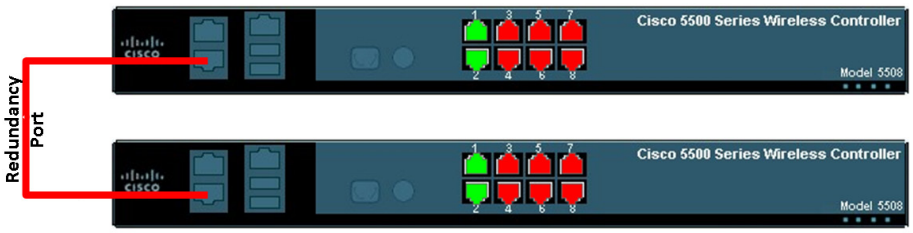
If you are deploying the Cisco Catalyst 4500 Series LAN distribution switch, you do not need to use the **switchport trunk encapsulation dot1q** command in the following configurations.

```
interface GigabitEthernet [port 1]
 description To WLC Port 1
interface GigabitEthernet [port 2]
 description To WLC Port 2
!
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 116,120,146
 switchport mode trunk
 logging event link-status
 no shutdown
```

Procedure 2 Connecting the redundancy port

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

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



Procedure 3 Configure the WLC platform

After the WLC is physically installed and powered up, you will see the following on the console. If you do not see this, press "-" a few times to force the wizard to back 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 a Cisco 5500 Series Wireless LAN Controller, use DHCP for the service port interface address.

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

Step 5: Enable the management interface.

```
Enable Link Aggregation (LAG) [yes][NO]: YES
Management Interface IP Address: 10.4.46.64
Management Interface Netmask: 255.255.255.0
Management interface Default Router: 10.4.46.1
Management Interface VLAN Identifier (0 = untagged): 146
```

> **Tech Tip**
>
> If you are configuring the Cisco 2500 Series Wireless LAN Controllers, you will need to configure both WLCs individually as they do not support AP-SSO and are therefore managed and configured separately. (Examples: 10.4.46.64 for WLC-1 and 10.4.46.65 for WLC-2)

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, enable AP SSO in order to enable high availability.

```
Enable HA [yes][NO]: YES
Configure HA Unit [PRIMARY][secondary]: PRIMARY
Redundancy Management IP Address: 10.4.46.74
Peer Redundancy Management IP Address: 10.4.46.75
```

Step 8: The virtual interface is used by the WLC for mobility DHCP relay, guest web authentication and intercontroller communication. Enter an IP address that is not used in your organization's network. (Example: 192.0.2.1)

```
Virtual Gateway IP Address: 192.0.2.1
```

Step 9: If you are configuring a Cisco 2500 Series Wireless LAN Controller, enter a multicast address for delivery of IP multicast traffic by using the multicast-multicast method. This multicast address will be used by each AP in order to listen for incoming multicast streams from the wireless LAN controller. (Example: 239.1.1.1)

```
Multicast IP Address: 239.1.1.1
```

Step 10: Enter a name for the default mobility and RF group. (Example: CAMPUS)

```
Mobility/RF Group Name: CAMPUS
```

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): WLAN-Data
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 radio resource management (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 respond with **no**, the system restarts without saving the configuration, and you have to complete this procedure again. Please wait for the "Configuration saved!" message before power-cycling the Wireless LAN Controller.

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

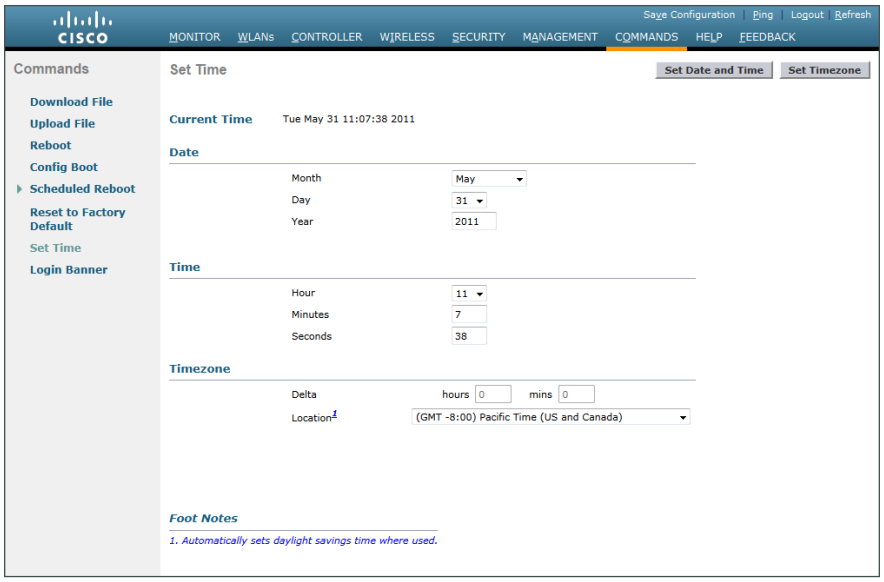
Step 19: After the WLC has reset, log in to the Cisco Wireless LAN Controller Administration page by using the credentials defined in Step 3. (Example: https://wlc-1.cisco.local/)

Procedure 4 Configure the time zone

Step 1: Navigate to **Commands > Set Time**.

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

Step 3: Click **Set Timezone**.



Procedure 5 Configure SNMP

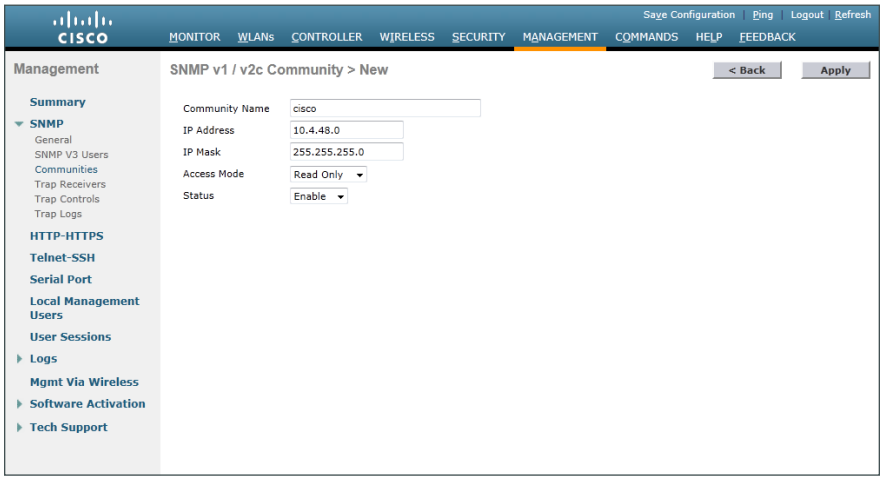
Step 1: In **Management > SNMP > Communities**, click **New**.

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

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

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

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



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

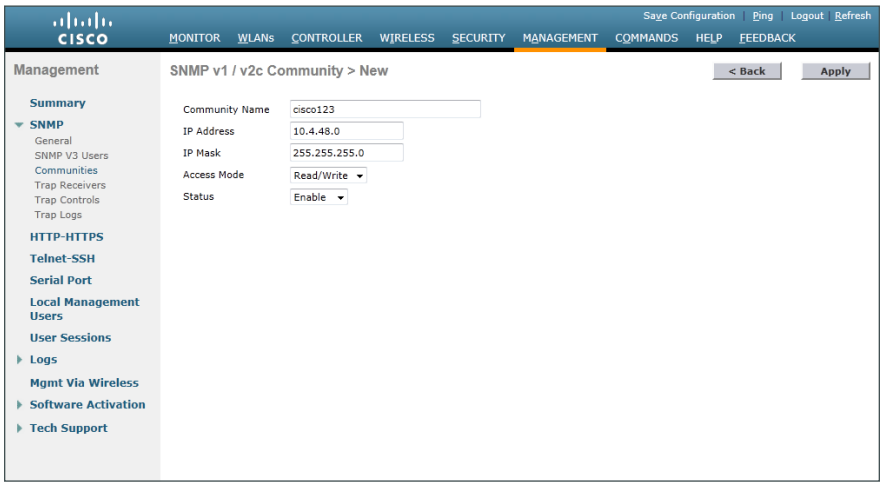
Step 7: Enter the **Community Name**. (Example: cisco123)

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**.

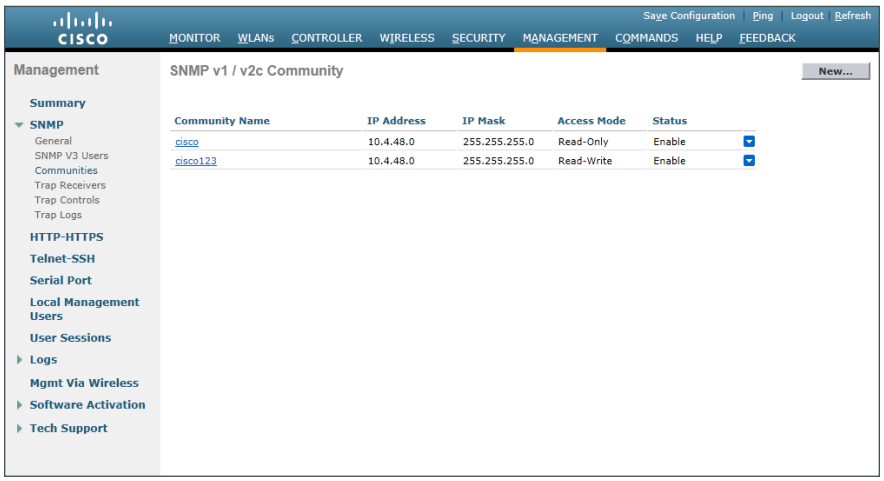


Step 12: Navigate to **Management** > **SNMP** > **Communities**.

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

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

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



Procedure 6 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 Simple Network Management Protocol (SNMP).

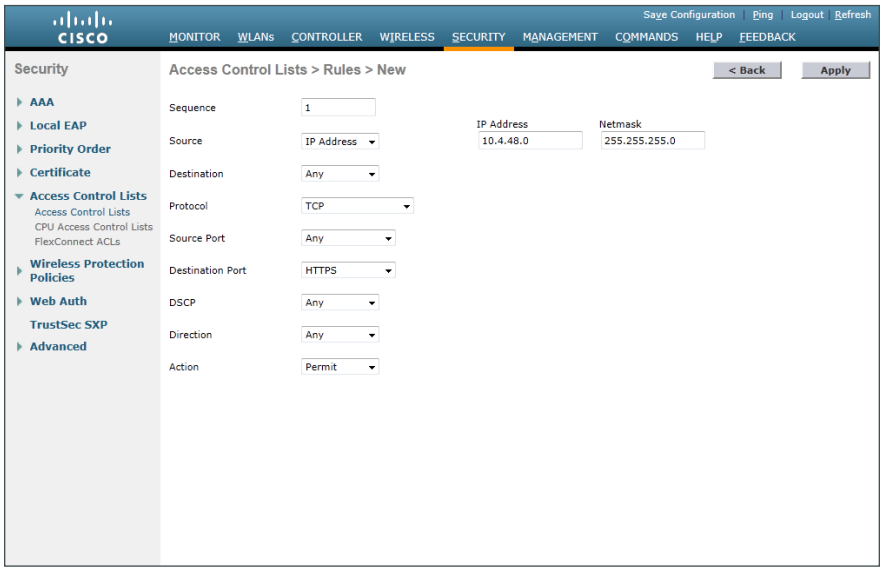
Step 1: In **Security > Access Control Lists > Access Control Lists**, click **New**.

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

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

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

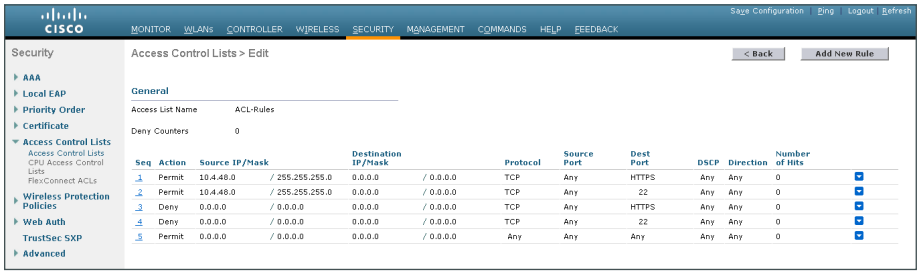
- Sequence–**1**
- Source–**10.4.48.0 / 255.255.255.0**
- Destination–**Any**
- Protocol–**TCP**
- Destination Port–**HTTPS**
- Action–**Permit**



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

Table 3 - Access rule configuration values

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



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

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

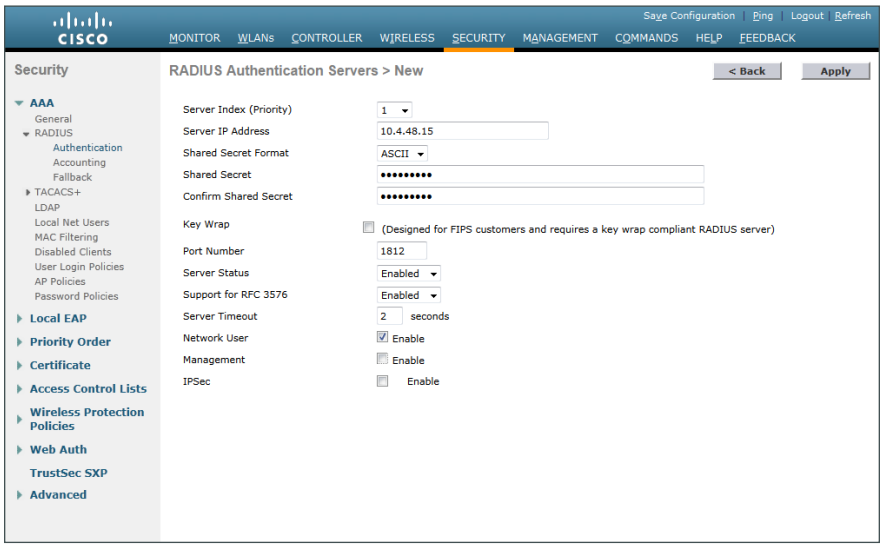
Procedure 7 Configure wireless user authentication

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

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

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

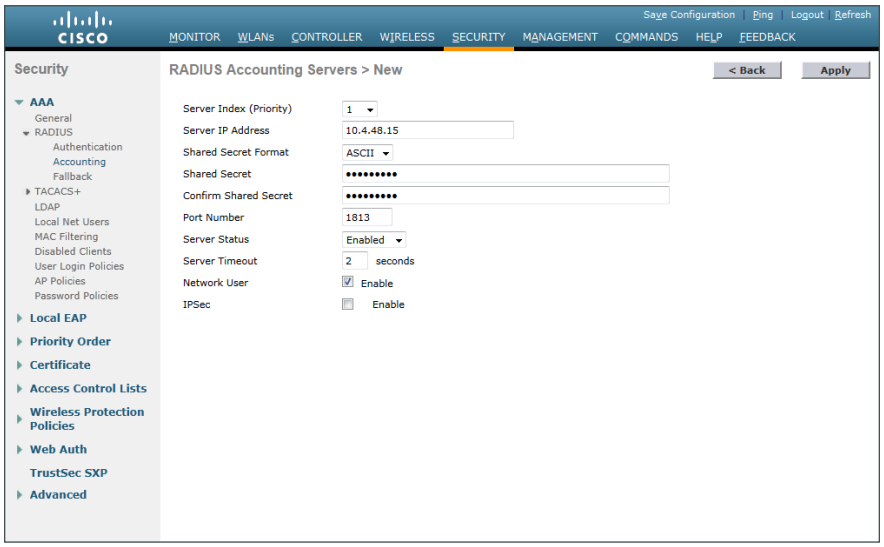
Step 4: To the right of Management, clear **Enable**, and then click **Apply**.



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

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

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



Procedure 8 Configure management authentication

(Optional)

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

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

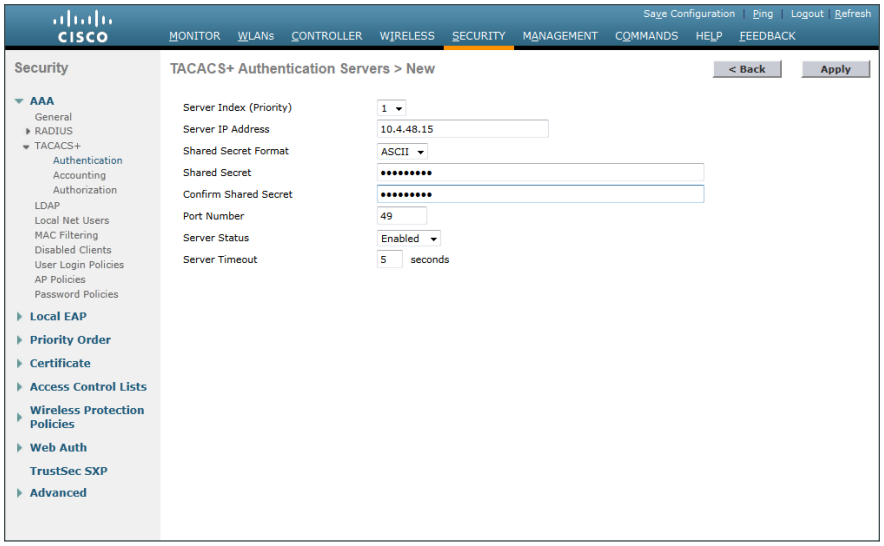
Tech Tip

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

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

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

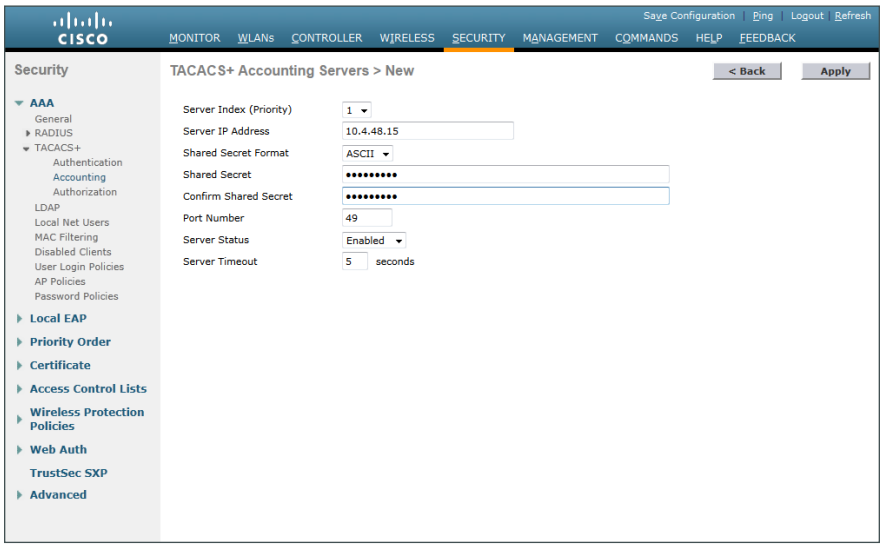
Step 3: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)



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

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

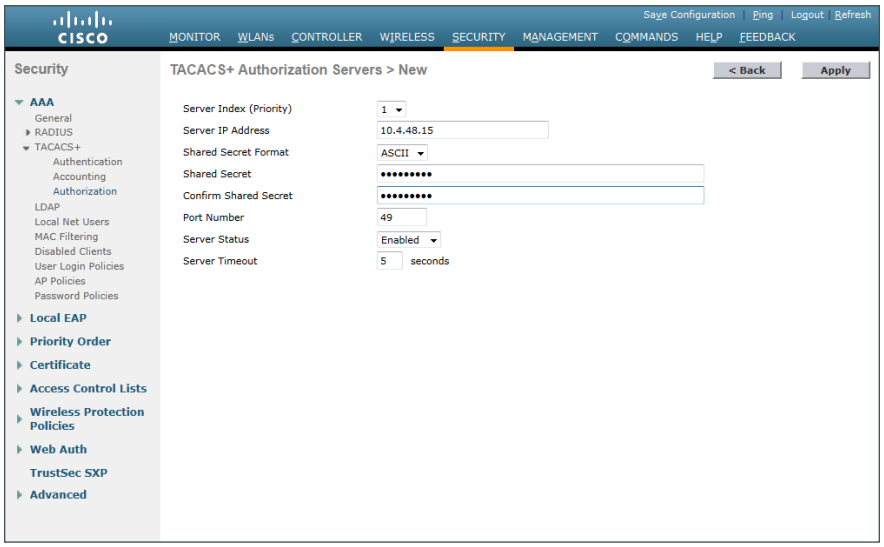
Step 6: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)



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)

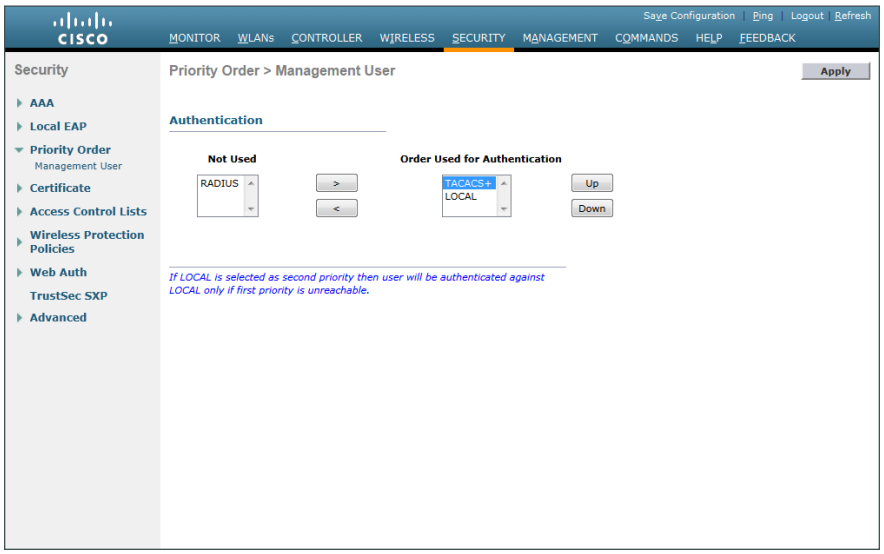


Step 10: Navigate to **Security > Priority Order > Management User**.

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.

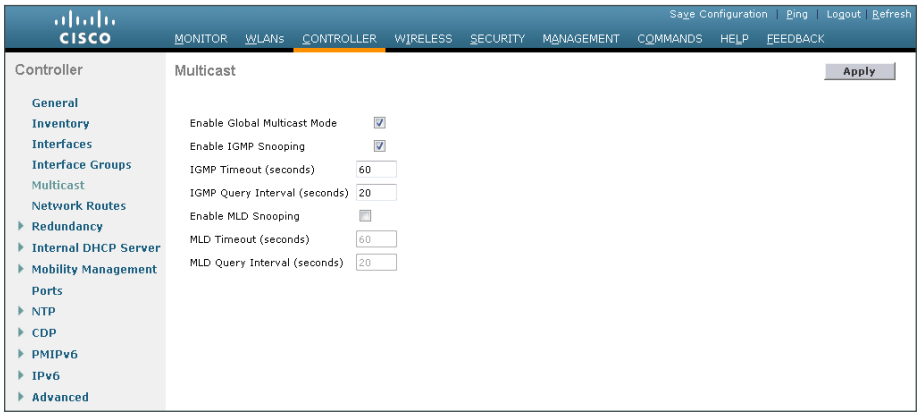
Step 13: Using the arrow buttons, move **RADIUS** to the **Not Used** list, and then click **Apply**.



Procedure 9 Enable multicast support

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

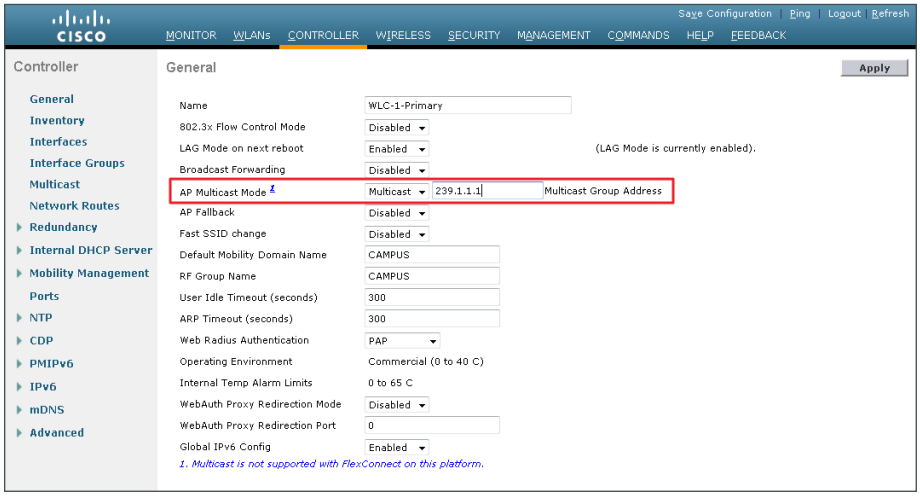
Step 1: In **Controller > Multicast**, select **Enable Global Multicast Mode** and **Enable IGMP Snooping**, and then click **Apply**.



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

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

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



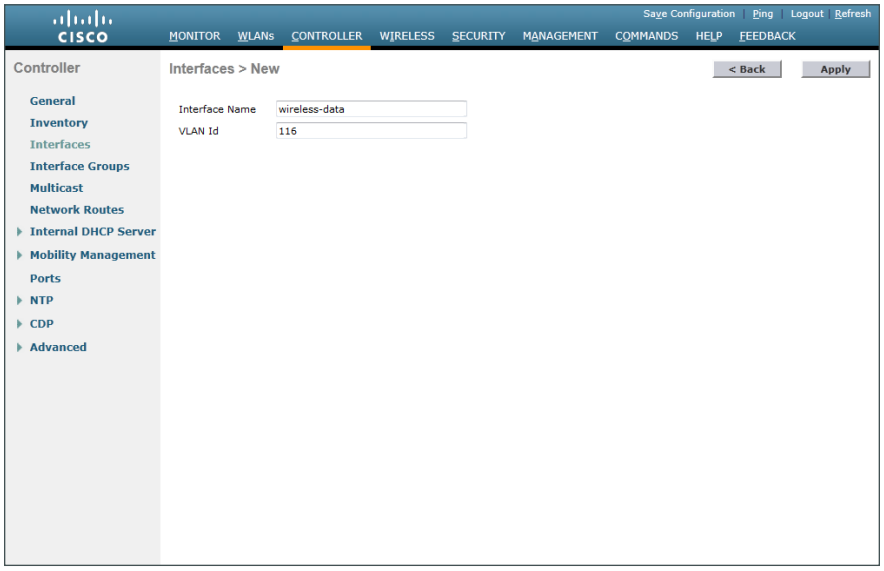
Procedure 10 Create the WLAN data interface

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

Step 1: In **Controller>Interfaces**, click **New**.

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

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



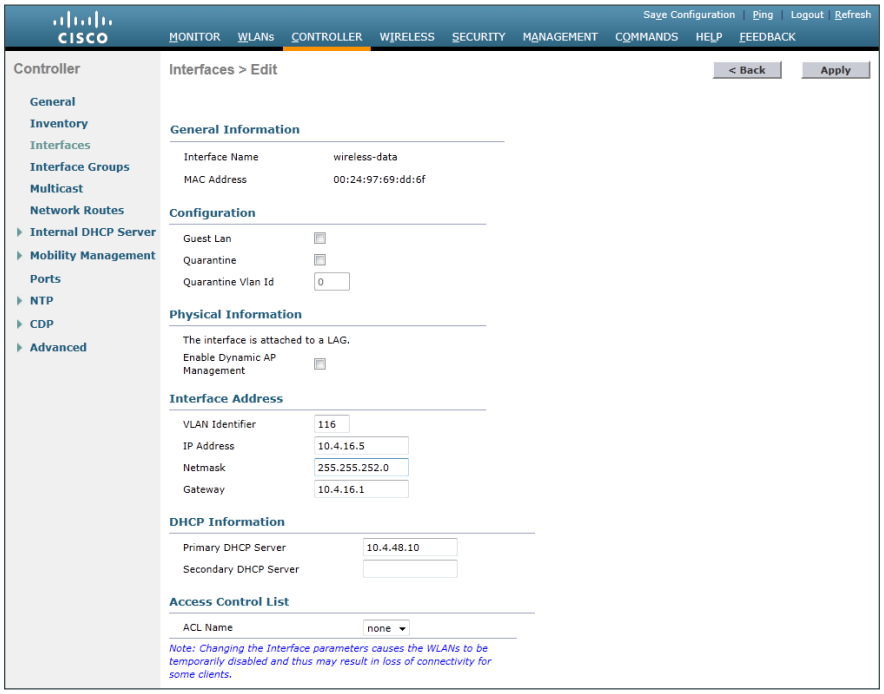
Step 4: If you are deploying a Cisco 2500 Series Wireless LAN Controller, in the **Port Number** box, enter the number of the port that is connected to the LAN distribution switch. (Example: 1)

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

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

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

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



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.

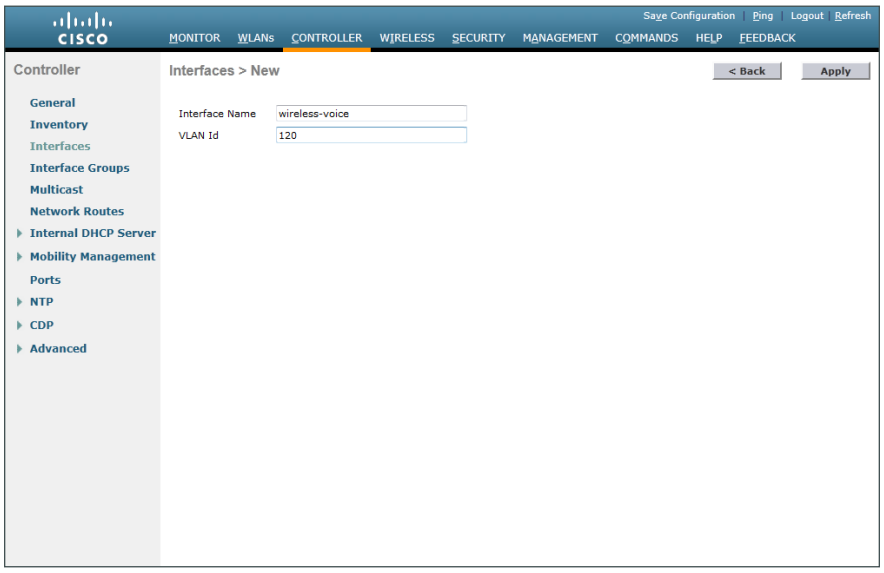
Procedure 11 Create the wireless LAN voice interface

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)



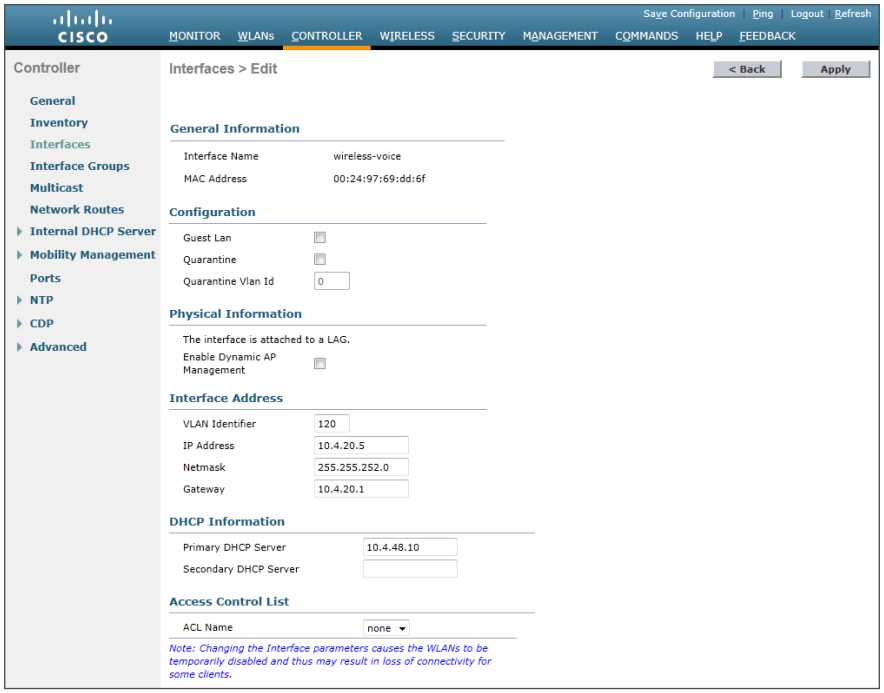
Step 4: If you are deploying a Cisco 2500 Series Wireless LAN Controller, in the **Port Number** box, enter the number of the port that is connected to the LAN distribution switch. (Example: 1)

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

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

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

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



Tech Tip

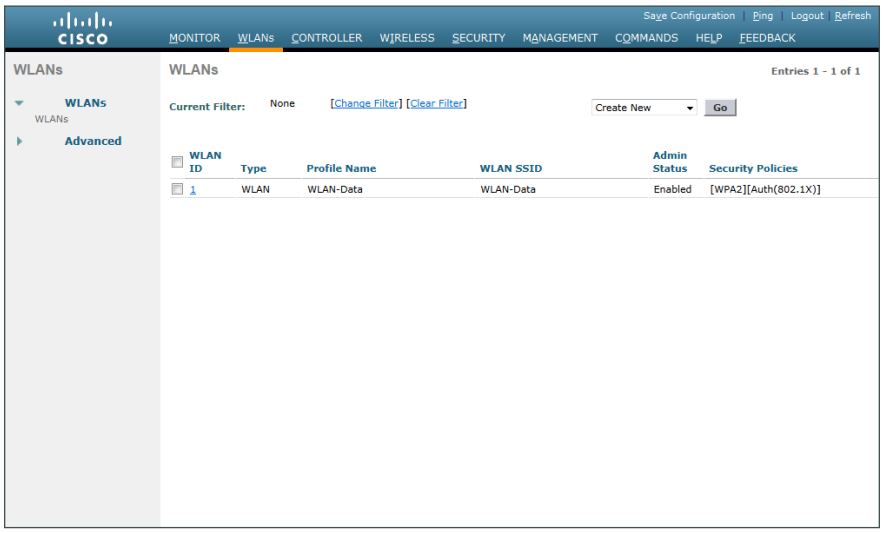
To prevent DHCP from assigning wireless clients addresses that conflict with the WLC's addresses, exclude the addresses you assign to the WLC interfaces from DHCP scopes.

Procedure 12 Configure the data wireless LAN

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

Step 1: Navigate to **WLANs**.

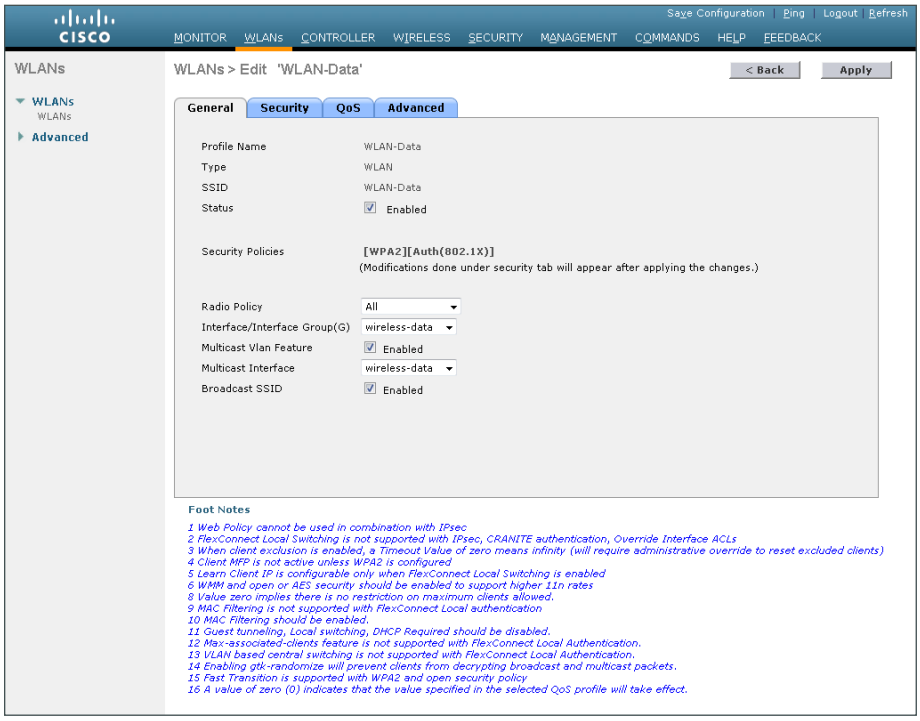
Step 2: Click the WLAN ID number of the SSID created in Procedure 3. (Example: WLAN-Data)



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

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

Step 5: Click **Apply**.

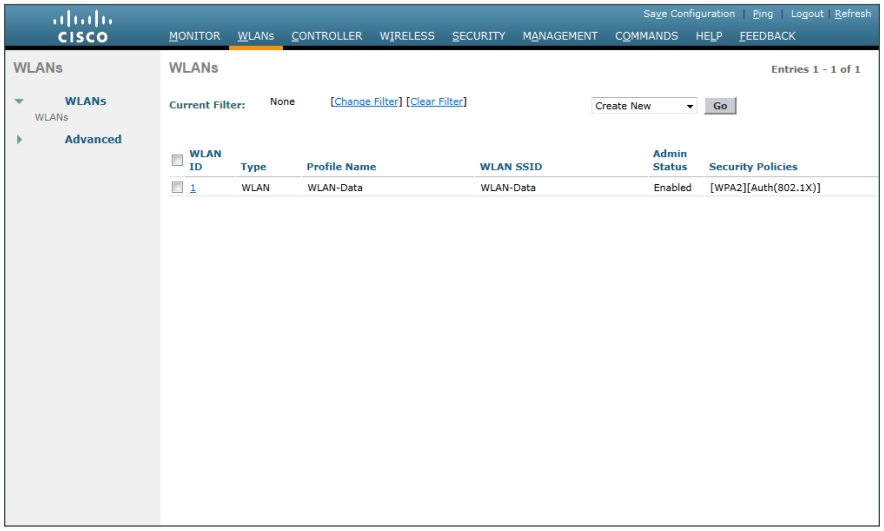


Procedure 13 Configure the voice wireless LAN

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

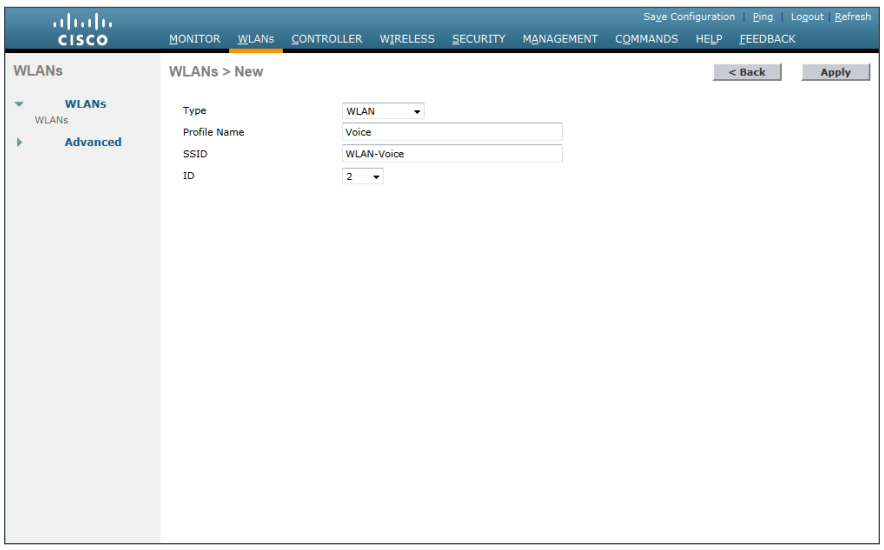
To configure the voice WLAN, change the default QoS settings to Platinum and segment the voice traffic onto the voice wired VLAN.

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



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

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

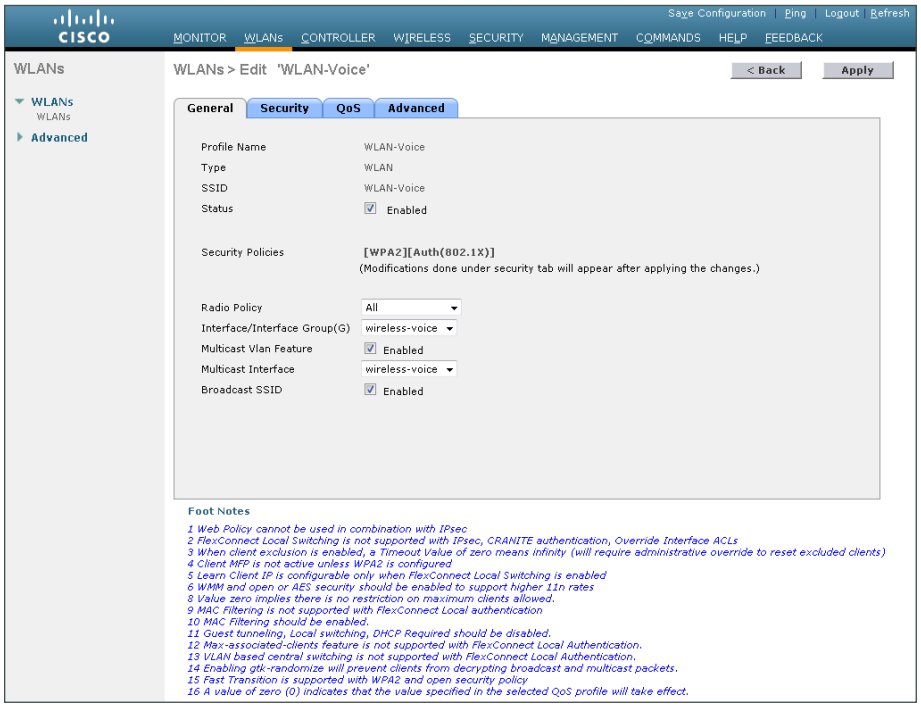


Step 4: On the General tab, next to Status, select **Enabled**.

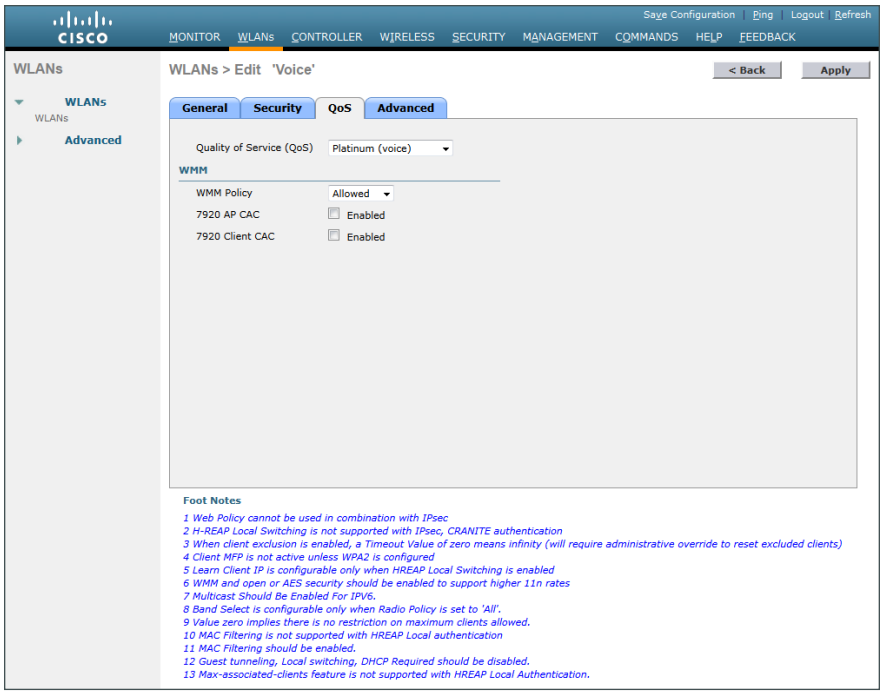
Step 5: In the **Interface/Interface Group(G)** list, choose the interface created in Procedure 11. (Example: wireless-voice)

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

Step 7: Click **Apply**.



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



Procedure 14 Configure the resilient controller

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

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

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

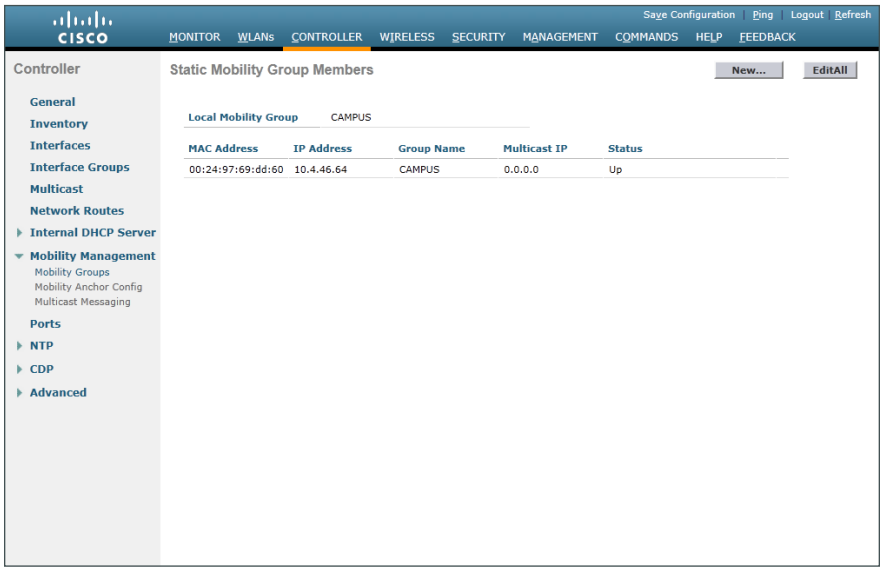
Even when configured as a pair, controllers do not share configuration information as they do when using AP SSO, so you must configure each controller separately.

Because it is possible for a wireless client in your network to roam from an access point joined to one controller to an access point joined to another controller, both controllers should be deployed in the same mobility group.

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

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

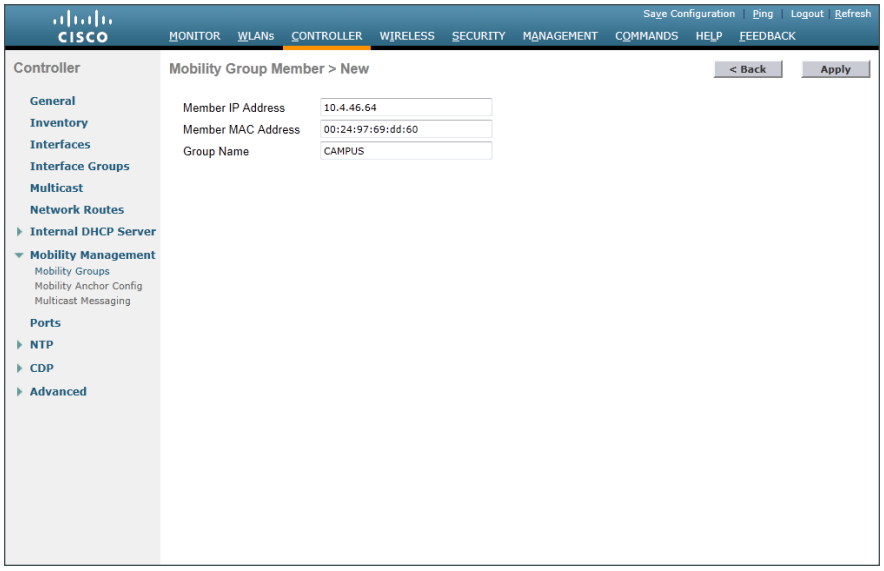
Step 2: On the primary controller, navigate to **Controller > Mobility Management > Mobility Groups**. The MAC address, IP address, and mobility group name for the local controller are shown.



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

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

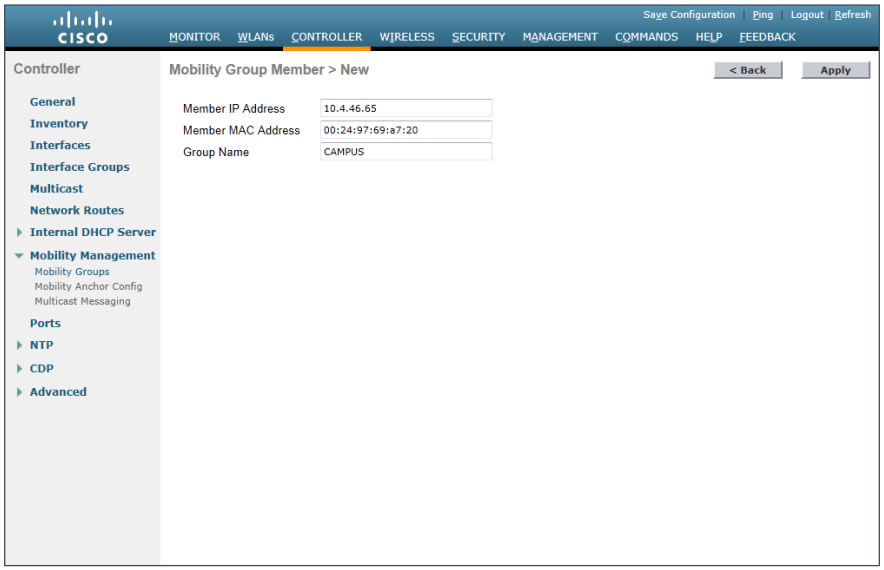
Step 5: In the **Member MAC Address** box, enter the MAC address of the primary controller, and then click **Apply**.



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

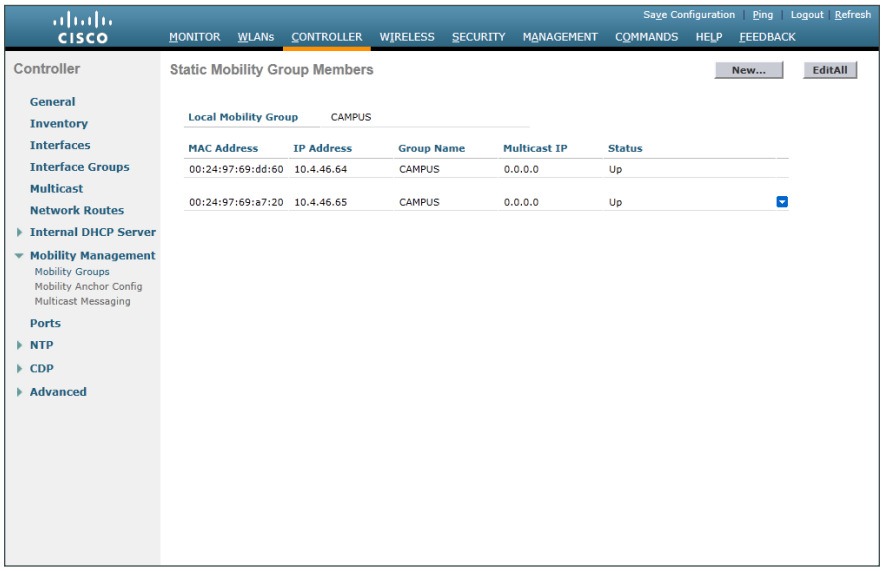
Step 7: In the **Member IP Address** box, enter the IP address of the resilient controller. (Example: 10.4.46.65)

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



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

Step 10: Navigate to **Controller > Mobility Management > Mobility Groups** on each controller, and then verify that connectivity is up between all the controllers by examining the mobility group information. In the Status column, all controllers should be listed as **Up**.



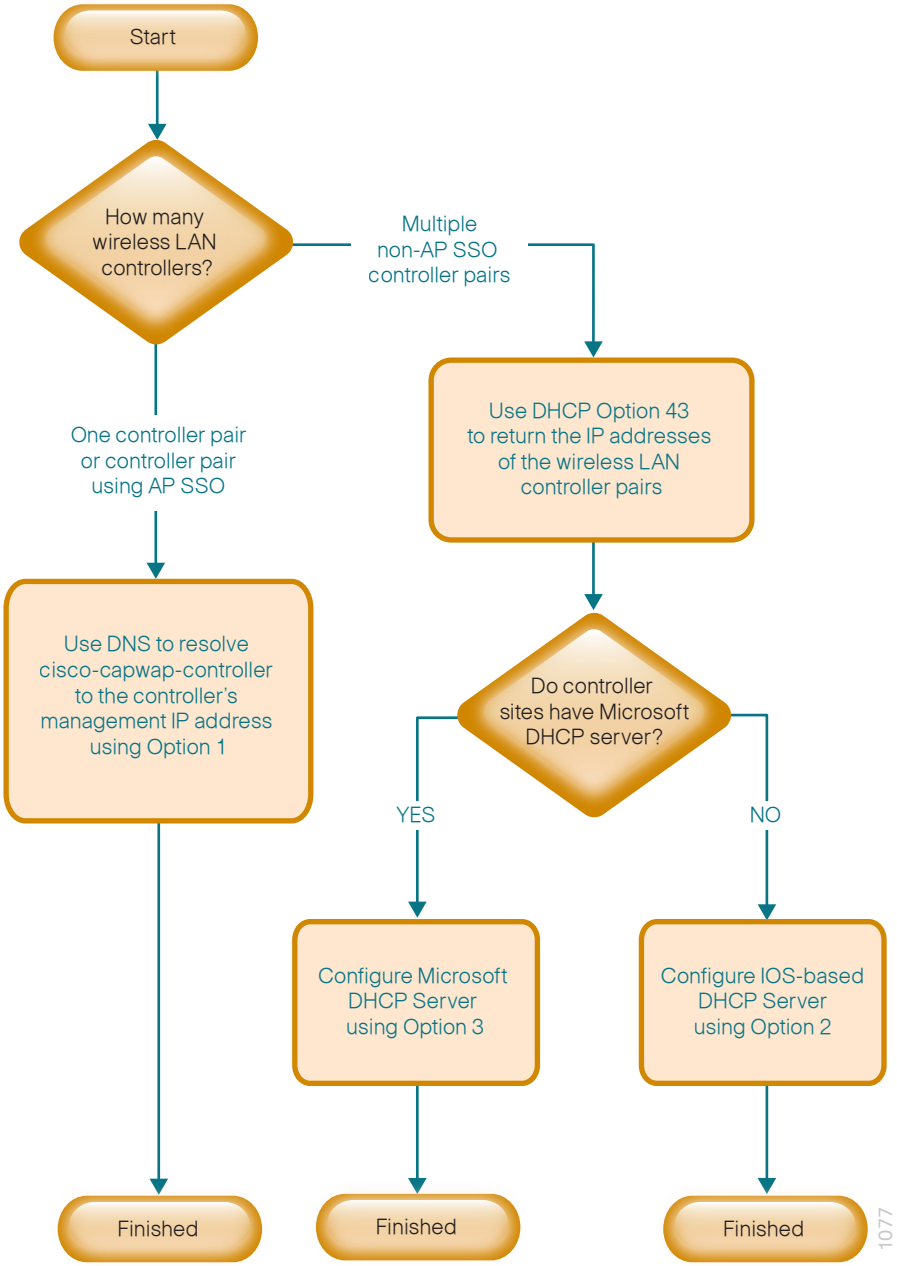
Procedure 15 Configure controller discovery

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

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

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

Figure 5 - Flow chart of WLC discovery configuration options



Option 1: Only one WLC pair in the organization

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

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

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

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

Step 1: Assemble the DHCP Option 43 value.

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

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

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

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

```
ip dhcp pool [pool name]
 option 43 hex f1080a042e400a042e41
```

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

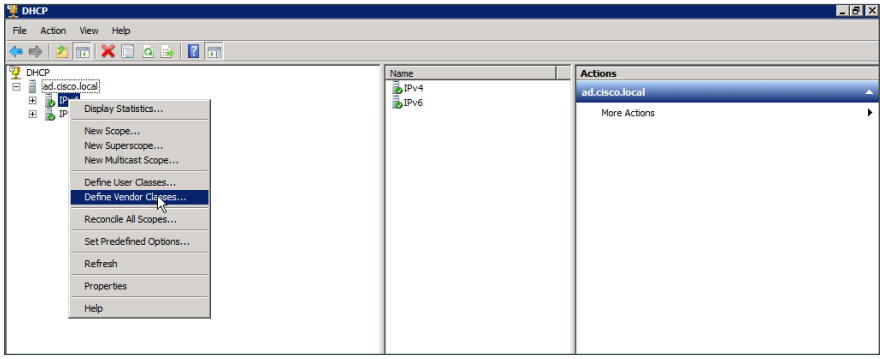
This procedure shows how the Microsoft DHCP server is configured in order to return vendor-specific information to the lightweight Cisco Aironet 1600, 2600, and 3600 Series Access Points used in this design guide. The vendor class identifier for a lightweight Cisco Aironet access point is specific to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

Table 4 - Vendor class identifiers

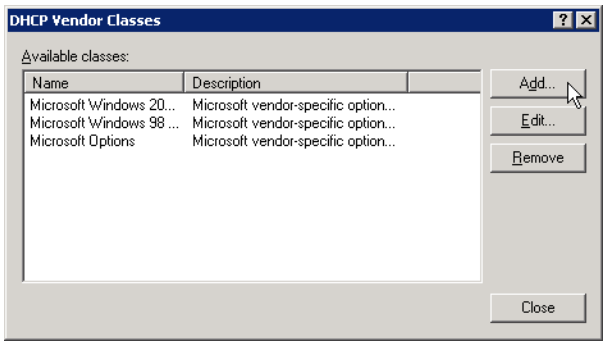
Access point	Vendor class identifier
Cisco Aironet 1600 Series	Cisco AP c1600
Cisco Aironet 2600 Series	Cisco AP c2600
Cisco Aironet 3600 Series	Cisco AP c3600

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

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



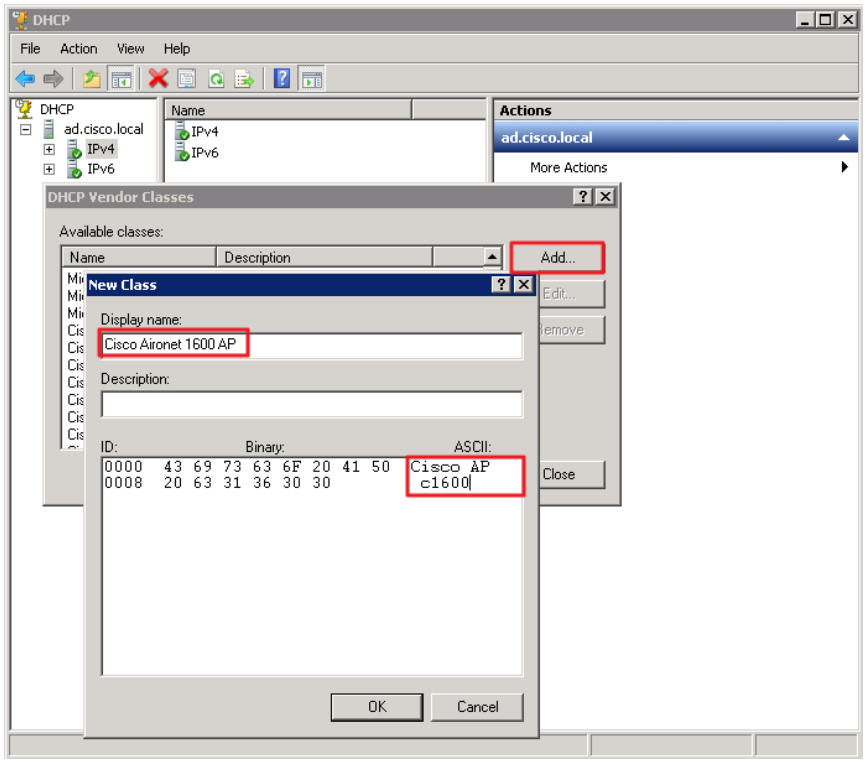
Step 3: In the DHCP Vendor Classes dialog box, click **Add**.



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

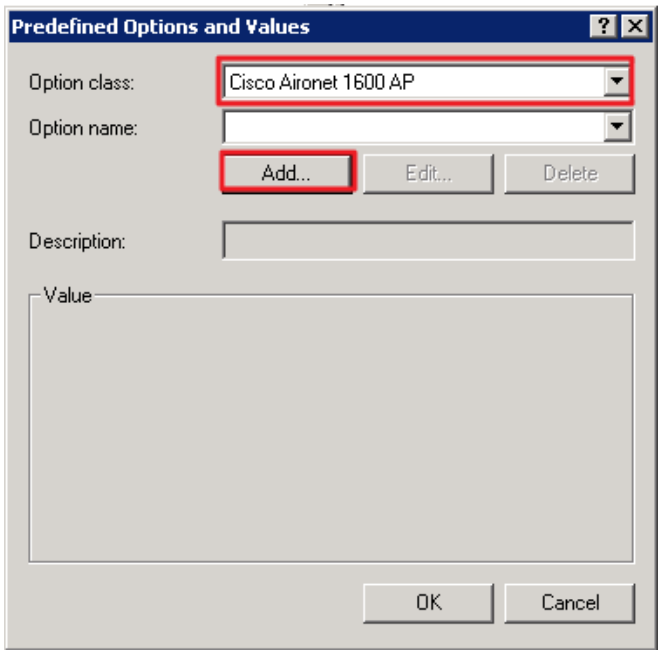
Step 5: In the ASCII section, enter the vendor class identifier for the appropriate access point series from Table 4, and then click **OK**. (Example: Cisco AP c1600)

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



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

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

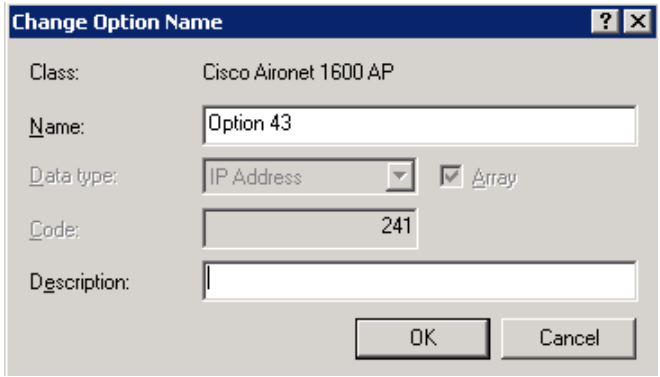


Step 9: In the Option Type dialog box, enter a **Name**. (Example: Option 43)

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**.



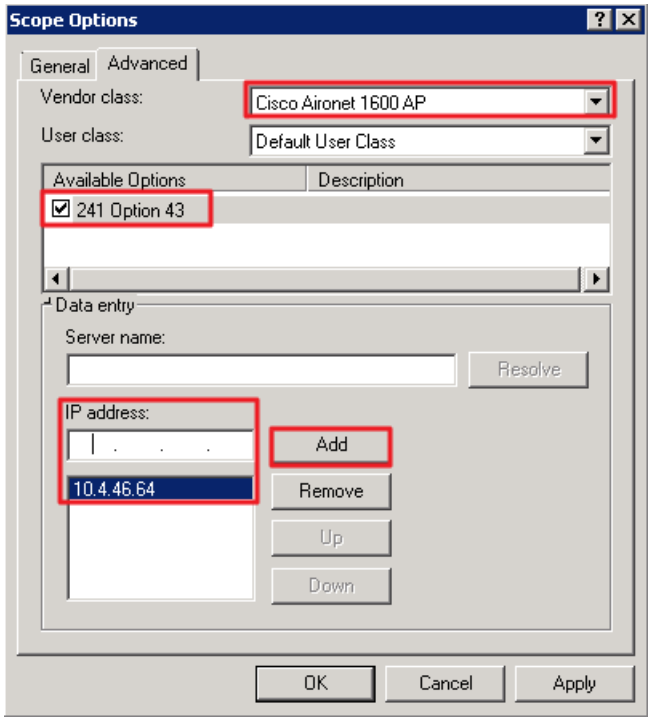
The vendor class and suboption are now programmed into the DHCP server. Now, you need to define the vendor-specific information for the DHCP scope.

Step 13: Choose the DHCP scope that you will 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** list, choose the class created in Step 4.

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

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



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

Procedure 16 Connect the access points

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

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

```
interface GigabitEthernet [port]
  description Access Point Connection
  switchport access vlan 100
  switchport voice vlan 101
  switchport host
  macro apply EgressQoS
  switchport port-security maximum 11
  switchport port-security
  switchport port-security aging time 2
  switchport port-security aging type inactivity
  switchport port-security violation restrict
  ip arp inspection limit rate 100
  ip dhcp snooping limit rate 100
  ip verify source
```

Procedure 17 Configure access points for resiliency

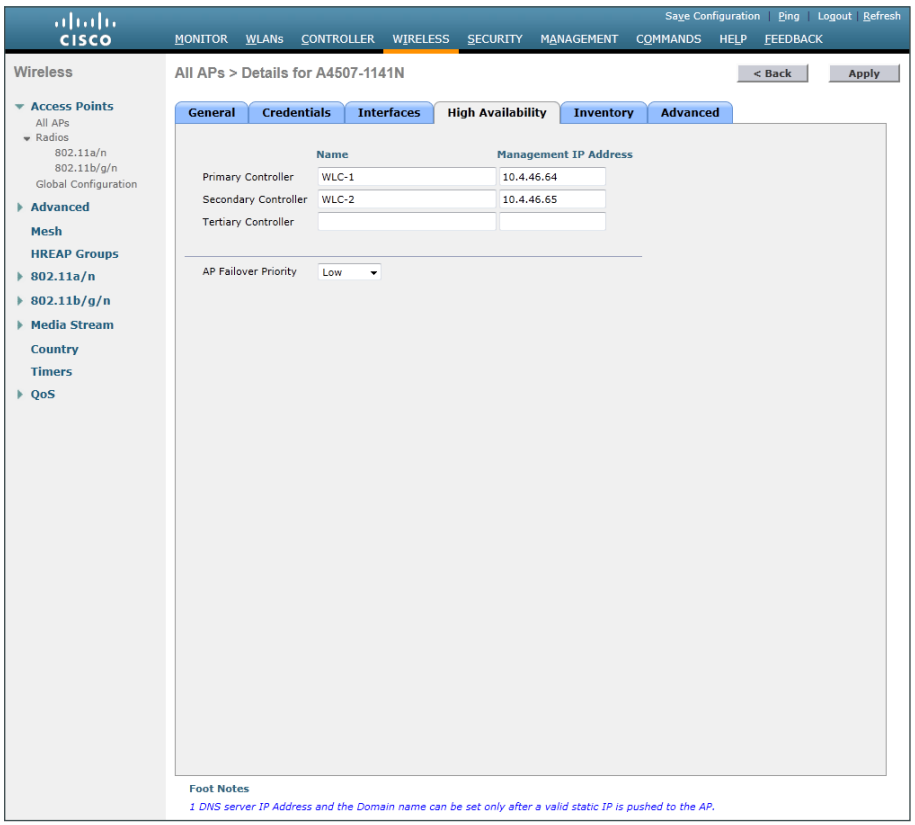
Step 1: For access points that are connecting to a WLC that is not using AP-SSO, it is necessary to configure these access points with the IP addresses of each of the non AP-SSO controllers. If you are installing access points that will connect to a pair of WLC's using AP-SSO, please skip this procedure.

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

Step 3: Click the **High Availability** tab.

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

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



PROCESS

Configuring Remote-Site Wireless with Cisco FlexConnect

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

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

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

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

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

Table 5 - Cisco remote-site wireless controller parameters checklist

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

Procedure 1 Install the vWLC for FlexConnect designs

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

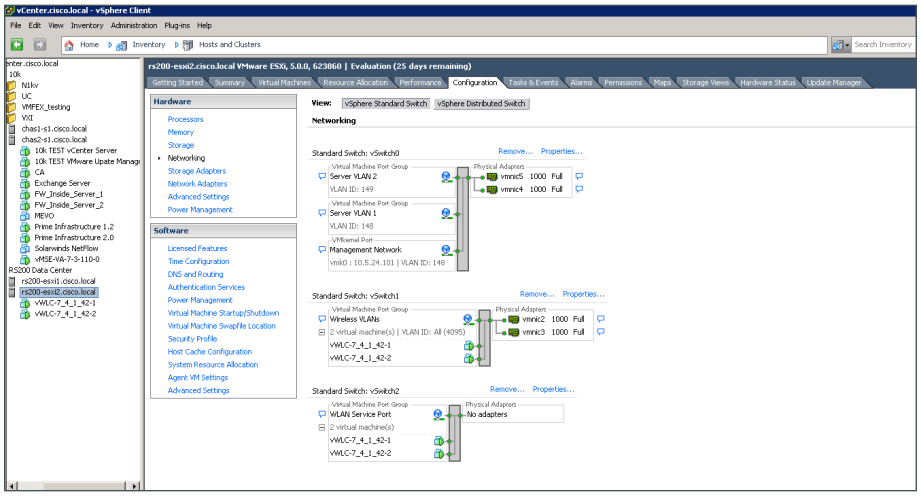
Tech Tip

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

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

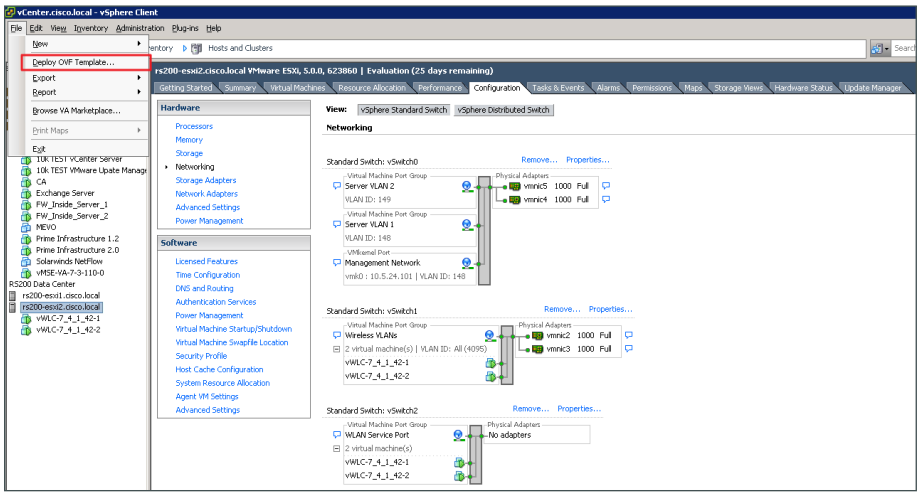
Step 1: Begin by preparing the VMware host machine networking environment. On the physical host machine, in vCenter, create three virtual switches (vSwitch0, vSwitch1, and vSwitch2), as follows:

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



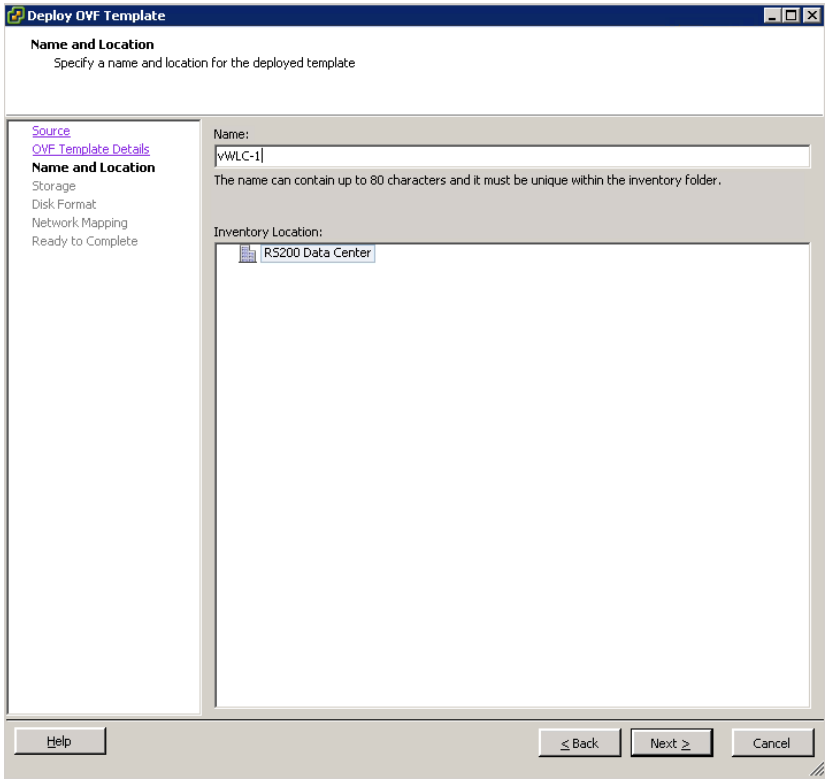
Next, you install the vWLC OVA file obtained from Cisco.

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

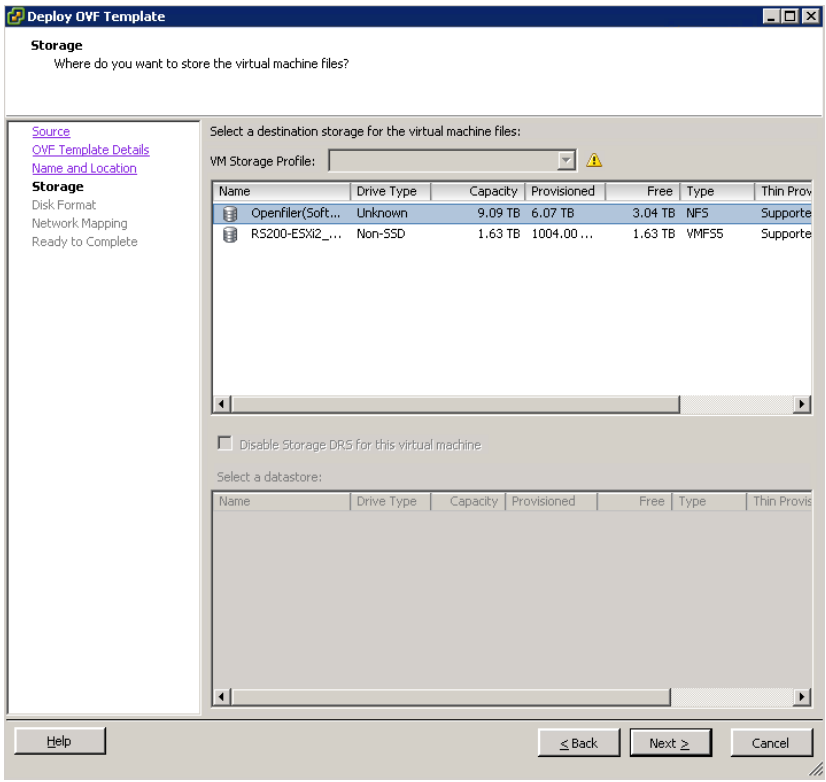


Step 3: Complete the Deploy OVF Template wizard. Note the following:

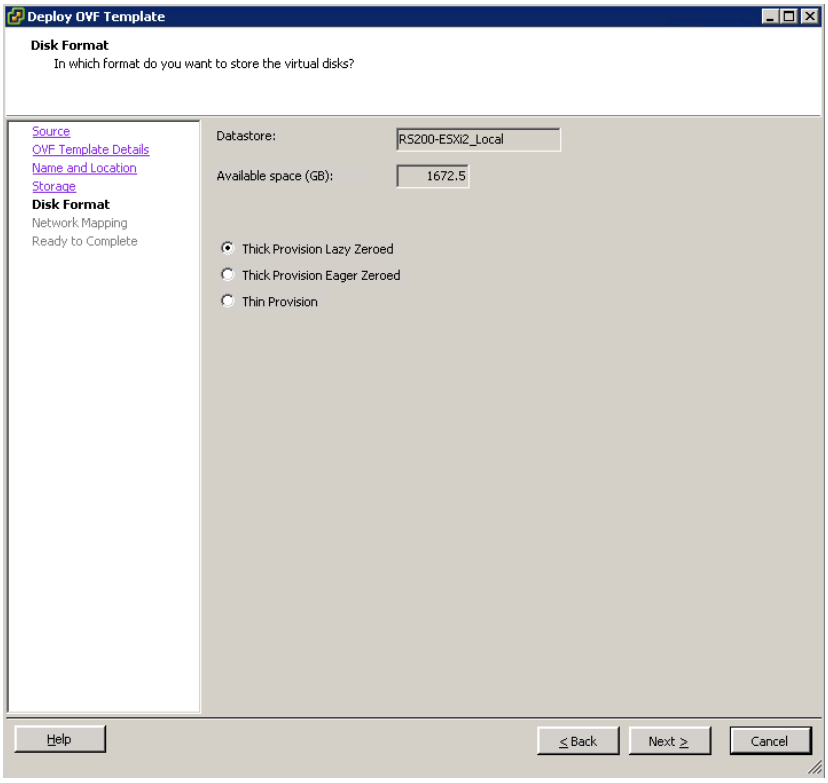
- On the Source page, select the downloaded vWLC OVA file that you obtained from Cisco.
- On the Name and Location page, provide a unique name for the virtual Wireless LAN controller. (Example: vWLC-1)



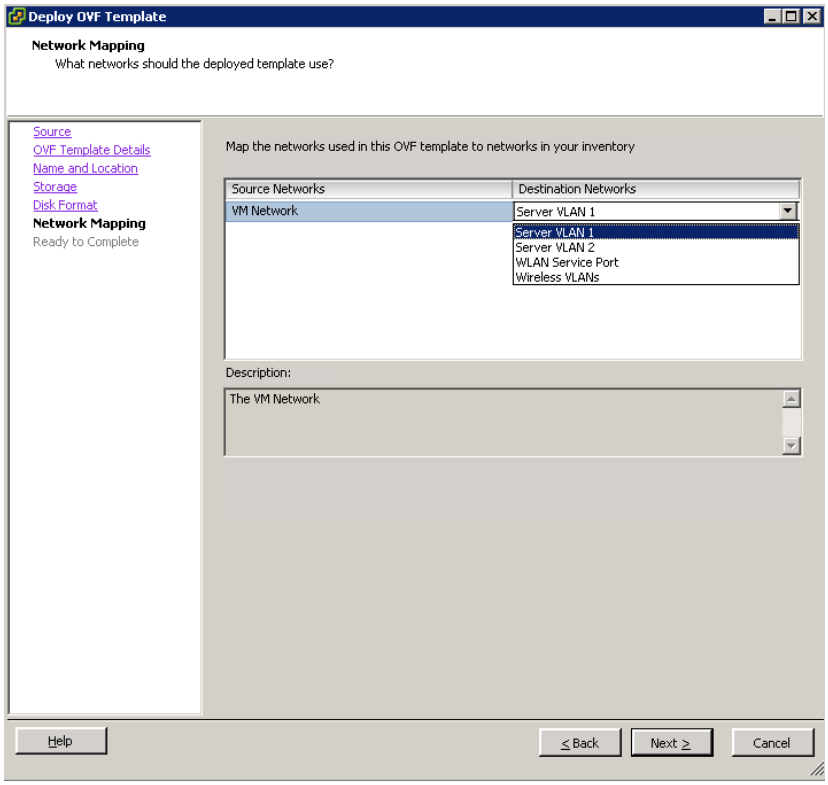
Step 4: On the Storage page, select the storage destination of the virtual machine.



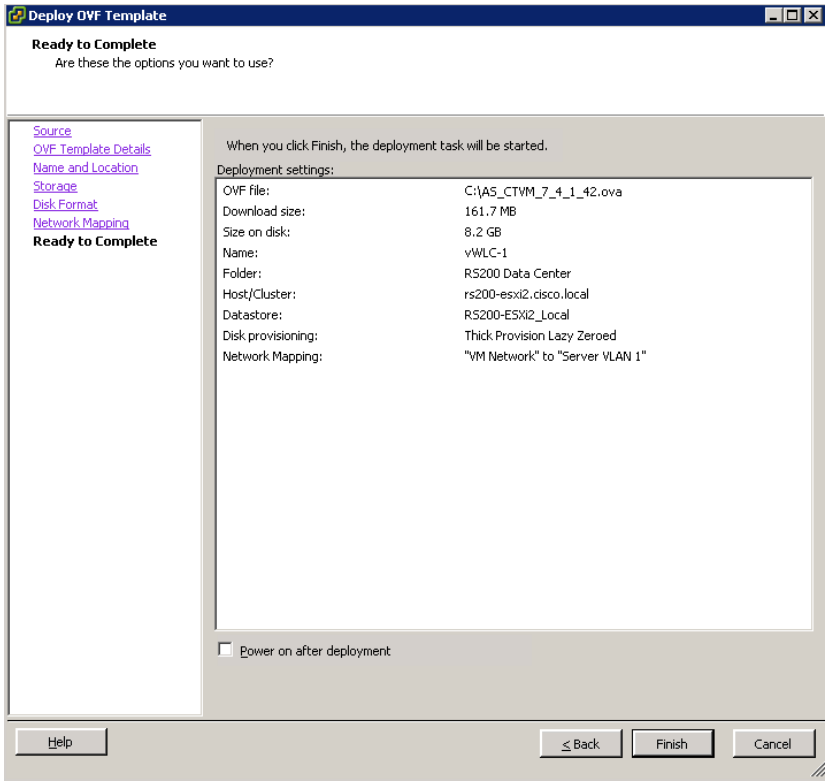
Step 5: On the Disk Format page, select **Thick Provision Lazy Zeroed**.



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: Server VLAN 1)



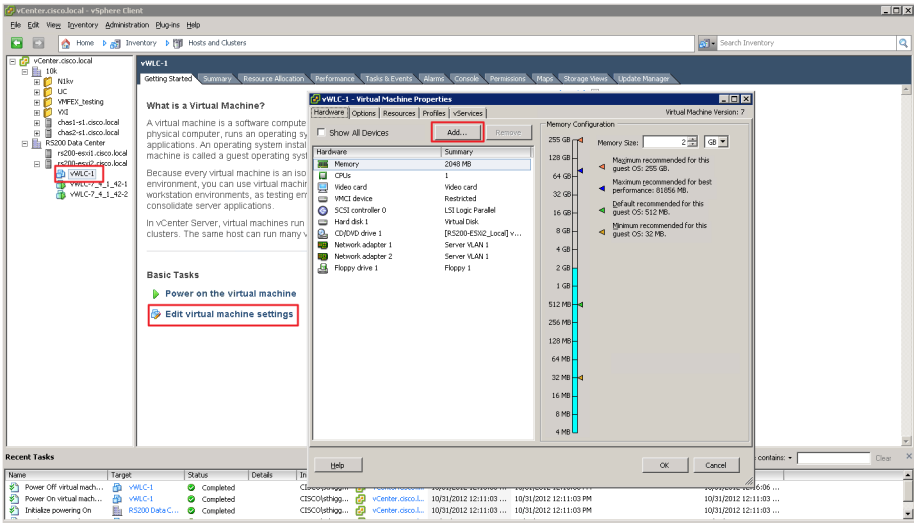
Step 7: On the Ready to Complete page, review the settings, and then press **Finish**. Deployment of the OVA file begins, and it may take a few minutes to complete.



Procedure 2 Configure the console port on the vWLC

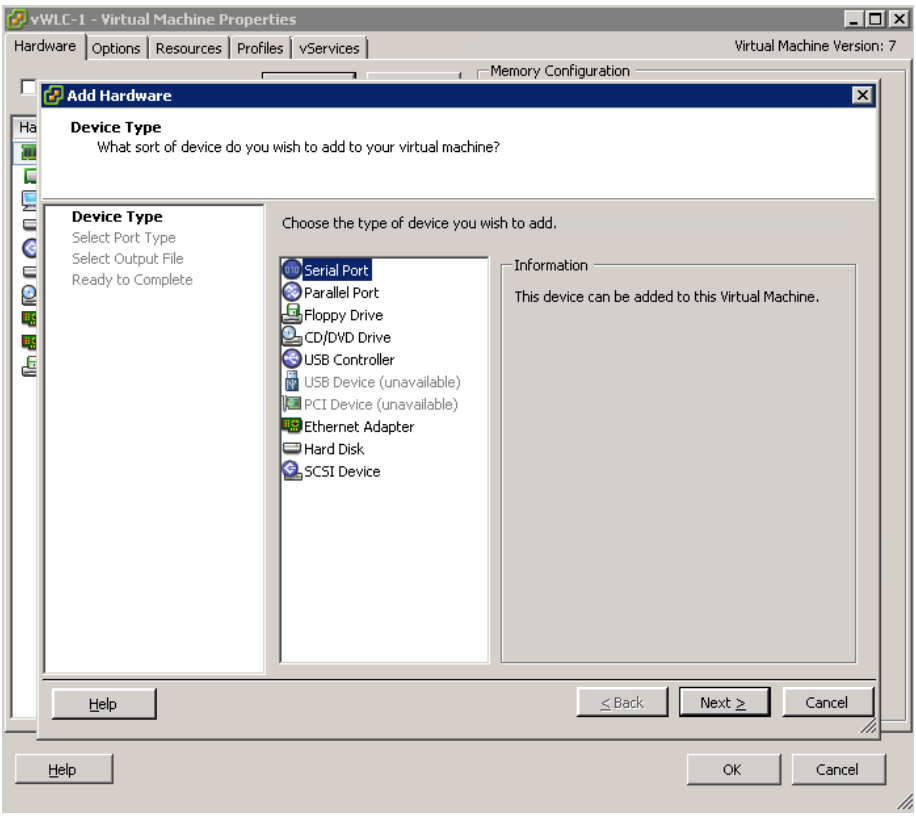
When the vWLC starts, the Console tab within vSphere will display a repetitive message stating to press any key in order to make the Console tab the default terminal for console messages from the vWLC. If a key is not pressed during the vWLC startup, console communication to the vWLC through the vSphere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

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

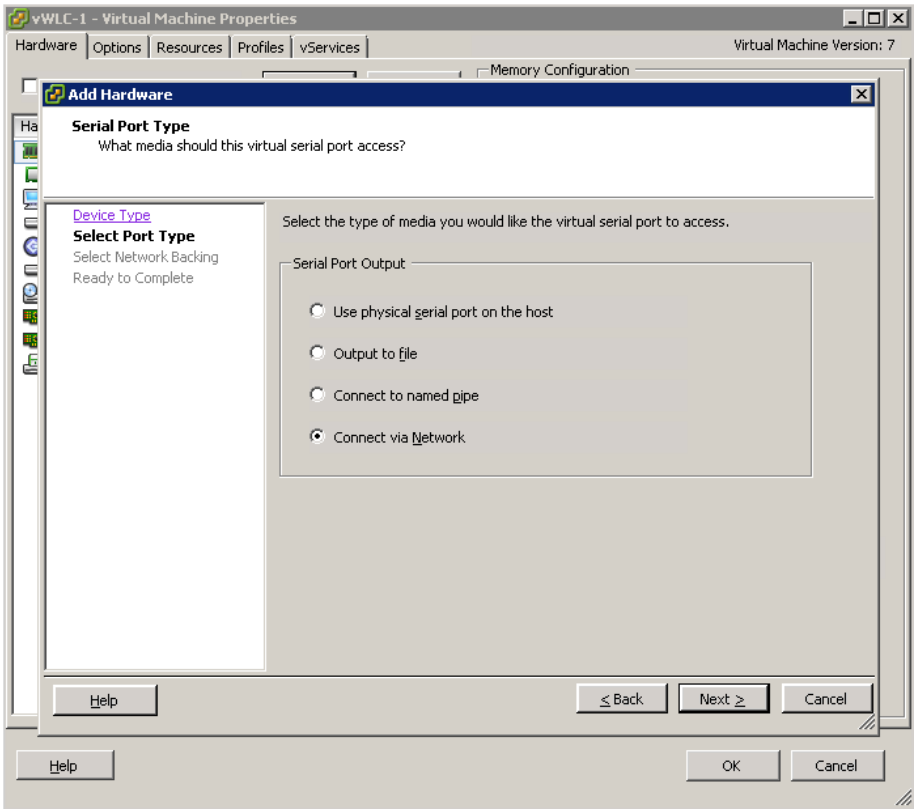


Step 2: Complete the Add Hardware wizard. Note the following:

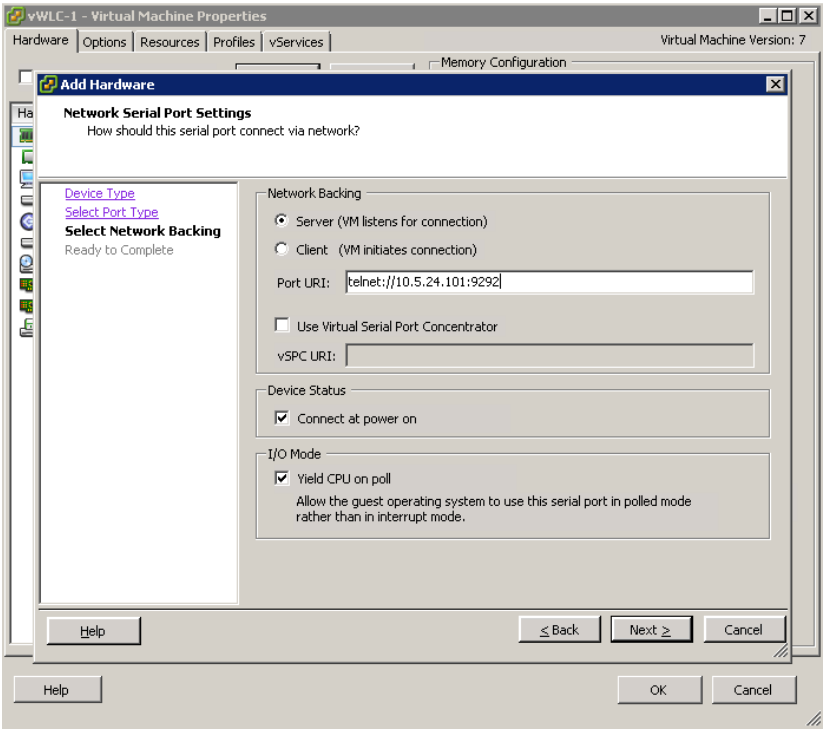
- On the Device Type page, select **Serial Port**.



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

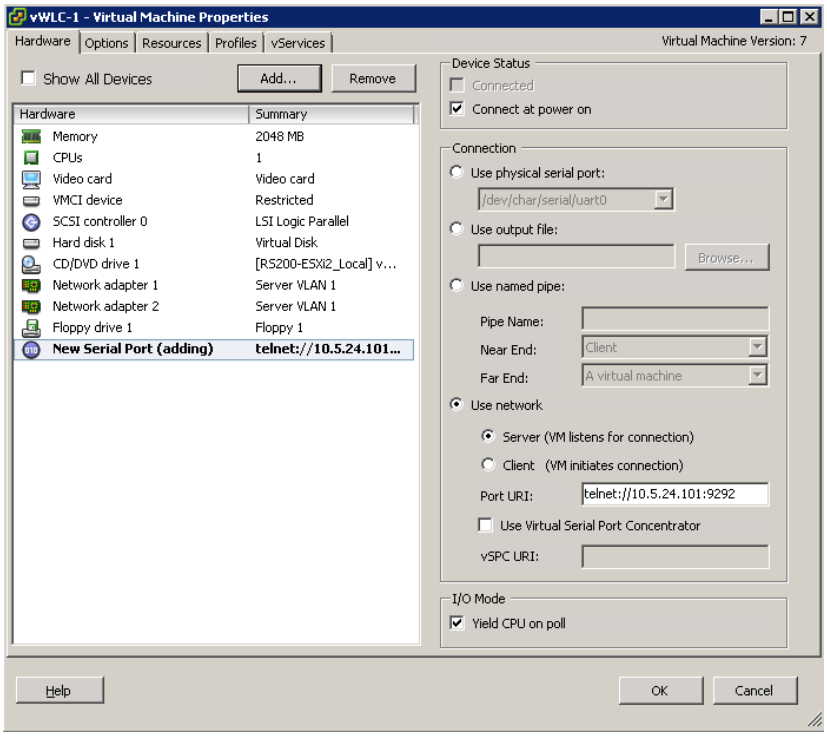


- On the Network Backing page, select **Server (VM listens for connection)**, and then in the **Port URI** box, enter **telnet://[Host Machine IP Address]:[Unique TCP Port]**. (Example: telnet://10.5.24.101:9292) This configures IP address and TCP port number that are used access the console port via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



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

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

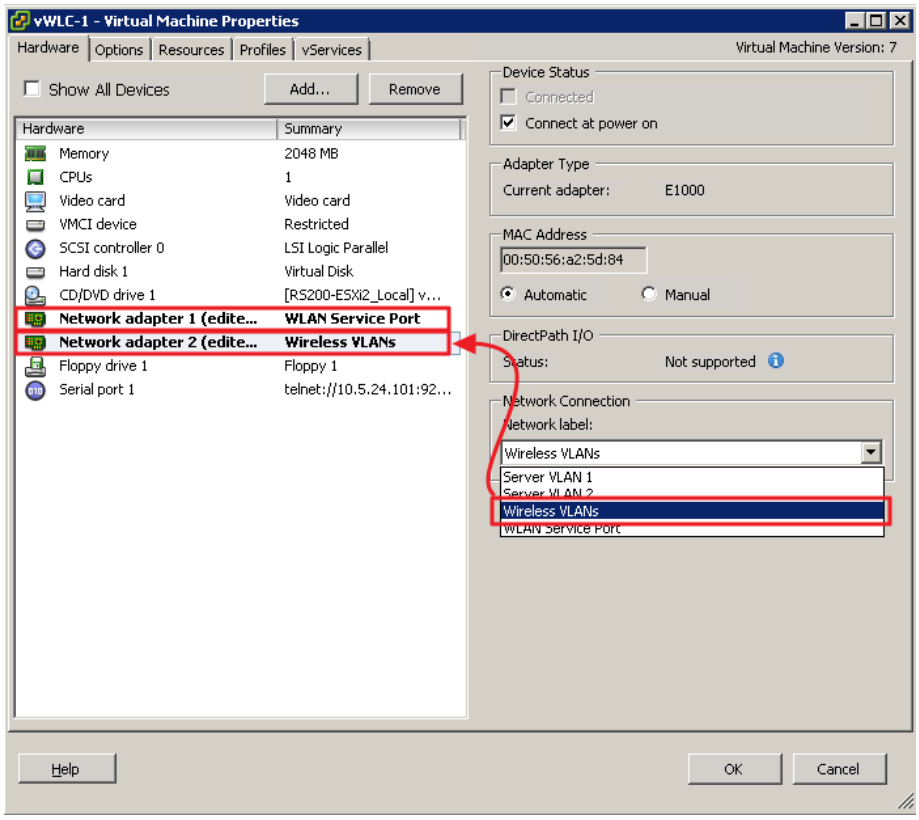


Procedure 3 Configure the vWLC network adapters

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

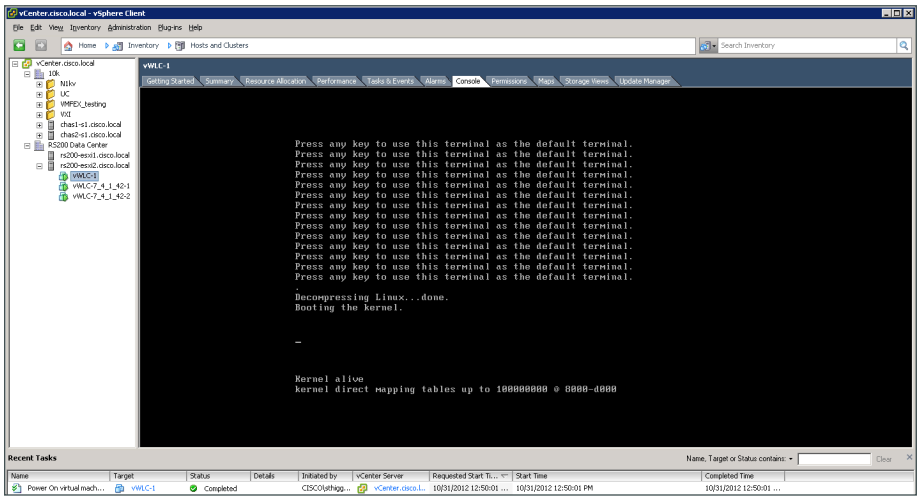
Step 1: In the Virtual Machine Properties dialog box, select **Network adapter 1**, and then in the **Network label** list, choose **WLAN Service Port**.

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



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.

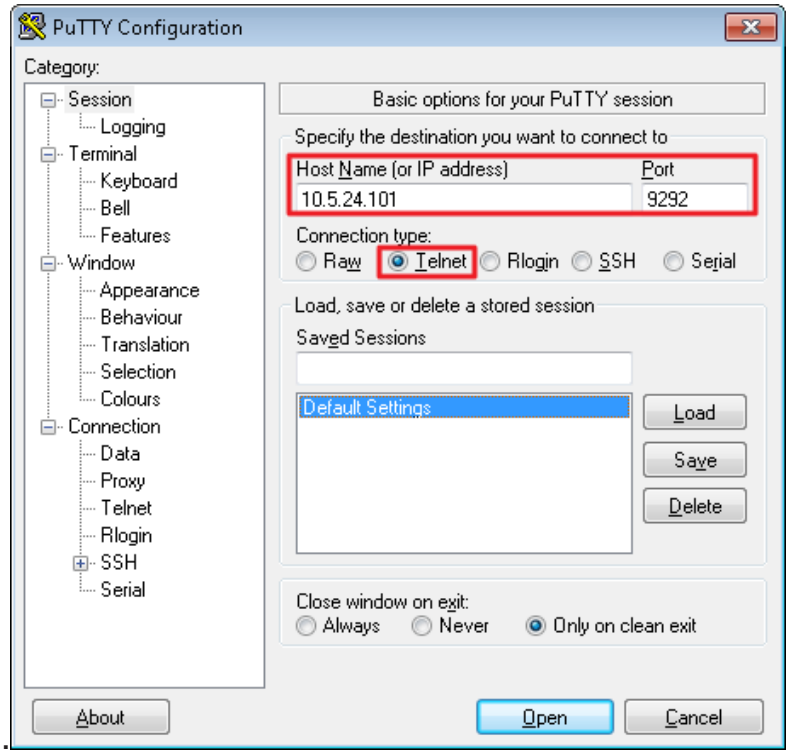
Within the Console tab you are prompted to "Press any key to use this terminal as the default terminal." However, you do not need to press any key because access via the serial port that was created in Procedure 2 will be used.



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 vWLC and press any key during the initial boot up in order to use the VMware console port as the access method.

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



Procedure 4 Configure the data center switches

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

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

```
Vlan 146
  name WLAN_Mgmt
```

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

```
interface port-channel65
  description Link to WLC7500-1
  switchport mode trunk
  switchport trunk allowed vlan 146
  no shutdown
interface port-channel66
  description Link to WLC7500-2
  switchport mode trunk
  switchport trunk allowed vlan 146
  no shutdown
```

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

```
interface Vlan146
  no shutdown
  description Wireless Management Network
  no ip redirects
  ip address 10.4.46.2/24
  ip router eigrp 100
  ip passive-interface eigrp 100
  ip pim sparse-mode
  hsrp 146
    priority 110
    ip 10.4.46.1
```

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

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

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

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

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

Procedure 5 Configure the LAN distribution switch

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

```
vlan 146
 name WLAN_Mgmt
```

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

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

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

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

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

```
interface TenGigabitEthernet [number]
 description To WLC port 1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 146
 switchport mode trunk
 macro apply EgressQoS
 logging event link-status
 logging event trunk-status
 no shutdown
```

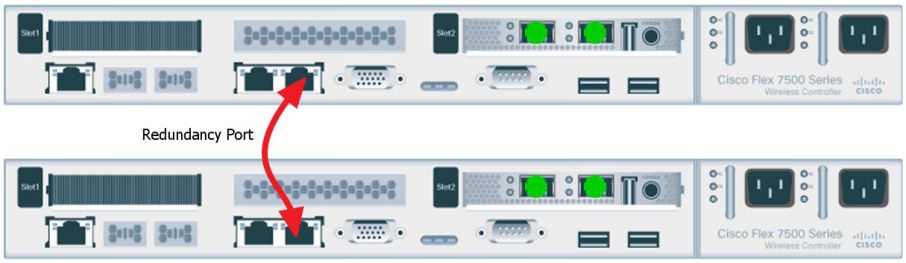
If you are deploying a Cisco 5500 Series Wireless LAN Controller, configure at least two distribution switch interfaces as an EtherChannel trunk.

```
interface GigabitEthernet [port 1]
 description To WLC Port 1
interface GigabitEthernet [port 2]
 description To WLC Port 2
!
interface range GigabitEthernet [port 1], GigabitEthernet [port 2]
  switchport
  macro apply EgressQoS
  channel-group [number] mode on
  logging event link-status
  logging event trunk-status
  logging event bundle-status
!
interface Port-channel [number]
 description To WLC
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 146
 switchport mode trunk
 logging event link-status
 no shutdown
```

Procedure 6 Connecting the redundancy port

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

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



Procedure 7 Configure the WLC platform

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

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

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

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

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

```
Enable Link Aggregation (LAG) [yes][NO]: YES
Management Interface IP Address: 10.4.46.68
Management Interface Netmask: 255.255.255.0
Management interface Default Router: 10.4.46.1
Management Interface VLAN Identifier (0 = untagged): 146
```

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

```
Management Interface Port Num [1 to 1]: 1
```

Step 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 7500 Series Wireless LAN Controller as a primary WLC in an AP-SSO redundant pair, complete the following steps. This enables AP SSO on the primary.

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

Step 8: If you are deploying a Cisco 7500 Series Wireless LAN Controller as a secondary WLC in an AP-SSO redundant pair, complete the following steps. This enables AP SSO on the secondary

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

Step 9: The virtual interface is used by the WLC for mobility DHCP relay and intercontroller communication. Enter an IP address that is not used in your organization's network. (Example: 192.0.2.1)

```
Virtual Gateway IP Address: 192.0.2.1
```

Step 10: Enter a name for the default mobility and RF group. (Example: REMOTES)

```
Mobility/RF Group Name: REMOTES
```

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): WLAN-Data
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 respond with **no**, the system will restart without saving the configuration, and you will have to complete this procedure again.

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

Step 19: After the WLC has restarted, access the console port on the WLC and configure it to automatically convert the APs to Cisco FlexConnect mode as they register.

```
config ap autoconvert flexconnect
```

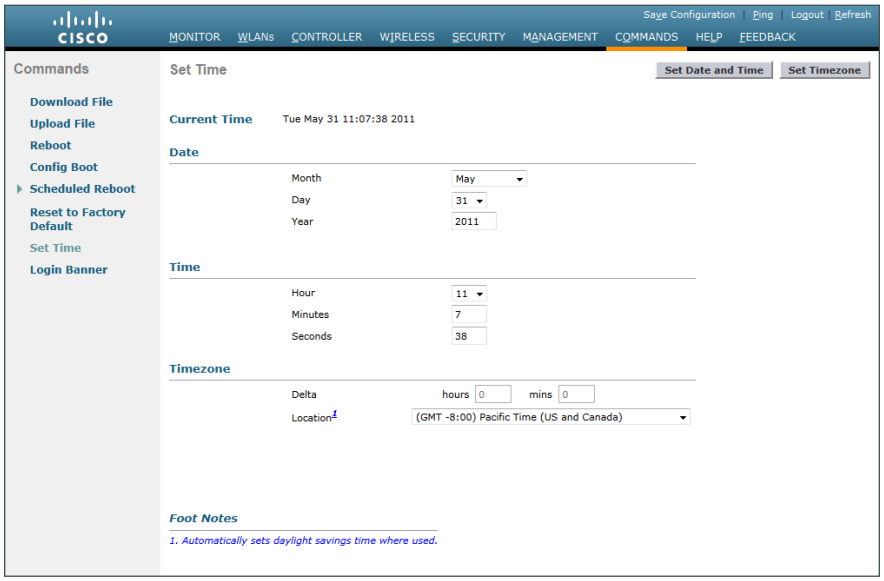
Step 20: Log in to the Cisco Wireless LAN Controller Administration page by using the credentials defined in Step 2. (Example: https://WLC-RemoteSites-1.cisco.local/)

Procedure 8 Configure the time zone

Step 1: Navigate to **Commands > Set Time**.

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

Step 3: Click **Set Timezone**.



Procedure 9 Configure SNMP

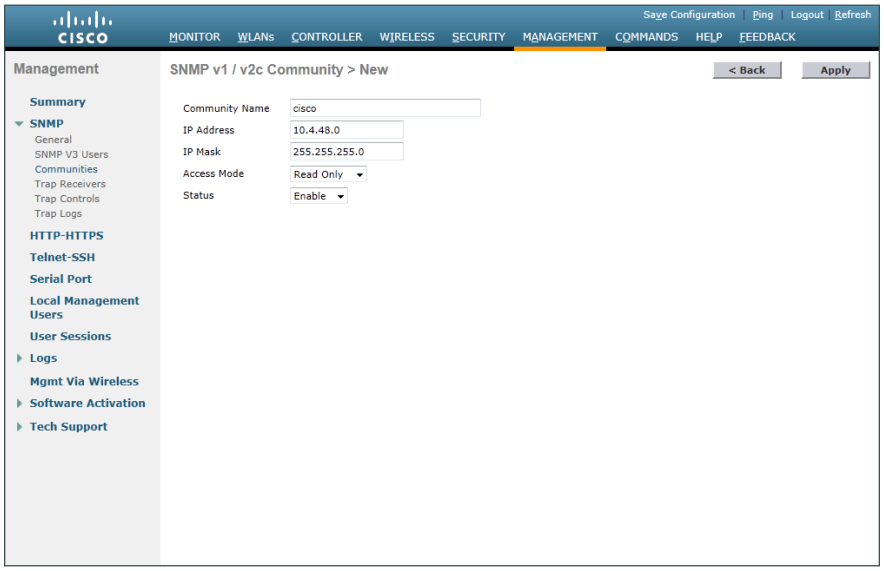
Step 1: In **Management > SNMP > Communities**, click **New**.

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

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

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

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



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

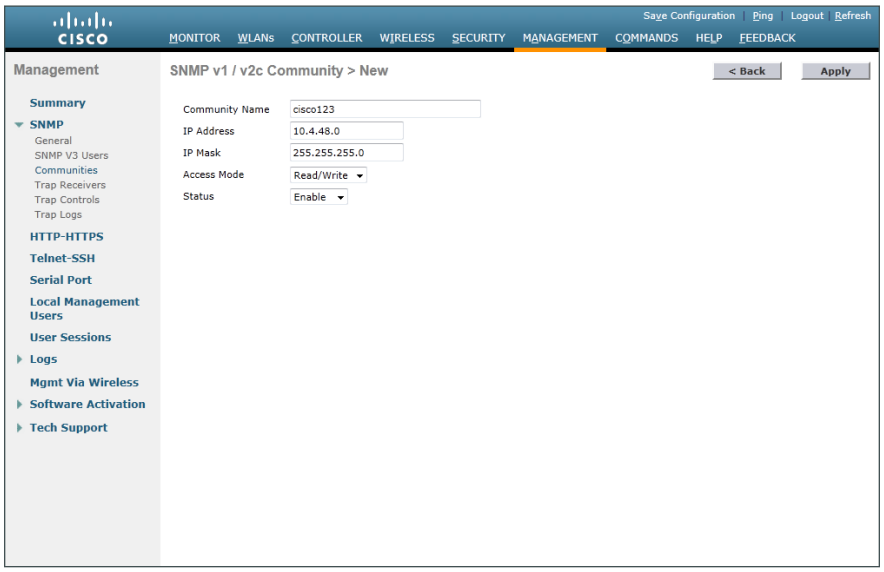
Step 7: Enter the **Community Name**. (Example: cisco123)

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.**

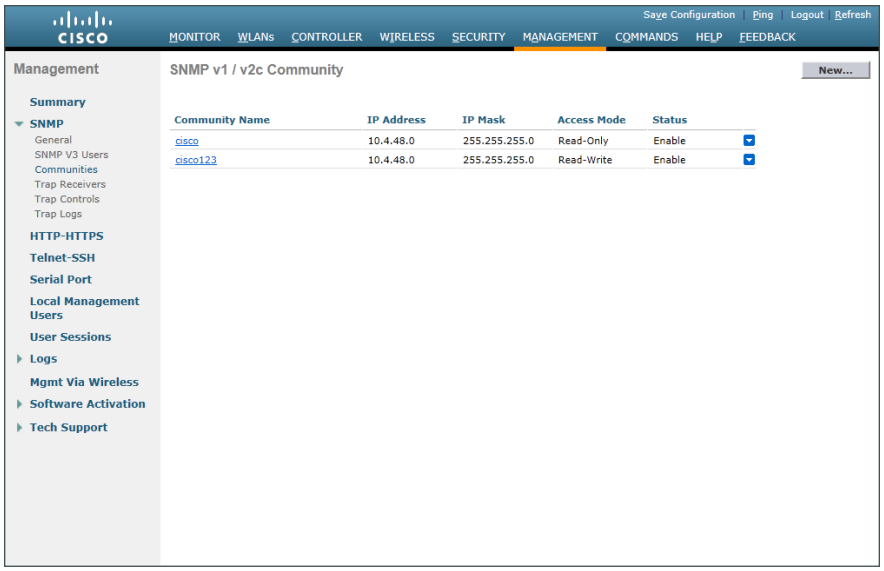


Step 12: Navigate to **Management** > **SNMP** > **Communities**.

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

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

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



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 SNMP.

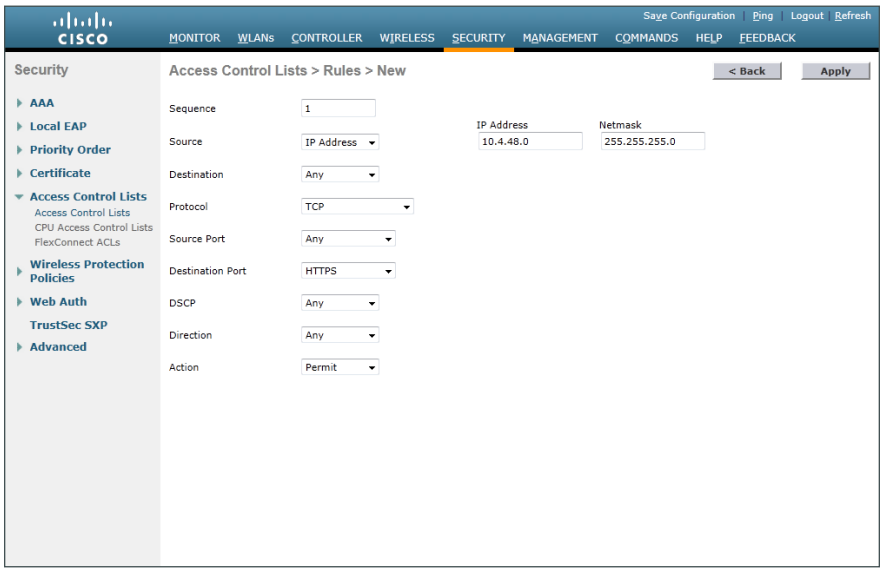
Step 1: In **Security > Access Control Lists > Access Control Lists**, click **New**.

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**.

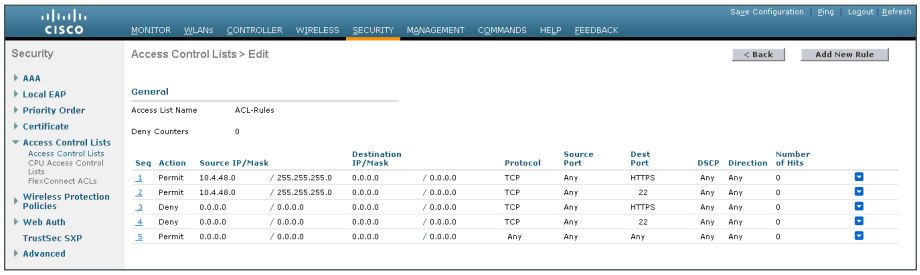
Step 4: In the window, enter the following configuration details, and then click **Apply**.

- 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 four more times, using the configuration details in the following table.

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



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

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

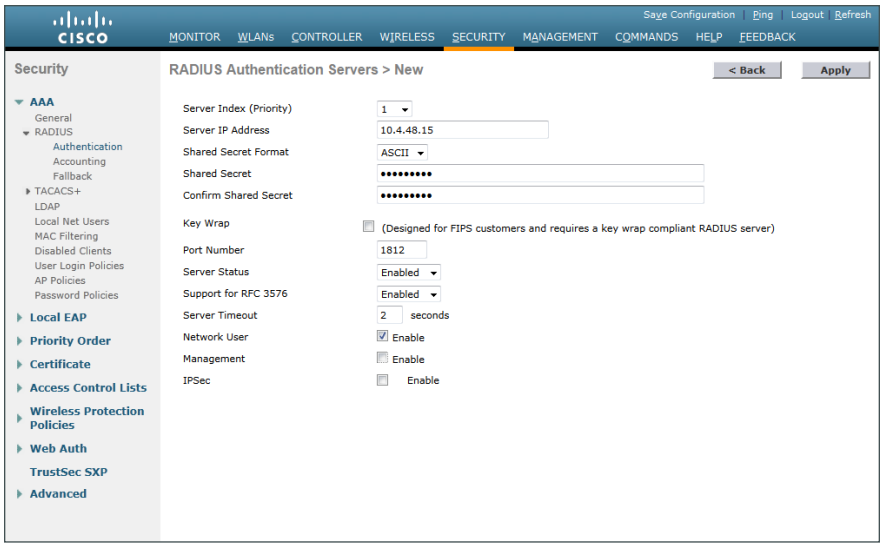
Procedure 11 Configure wireless user authentication

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

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

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

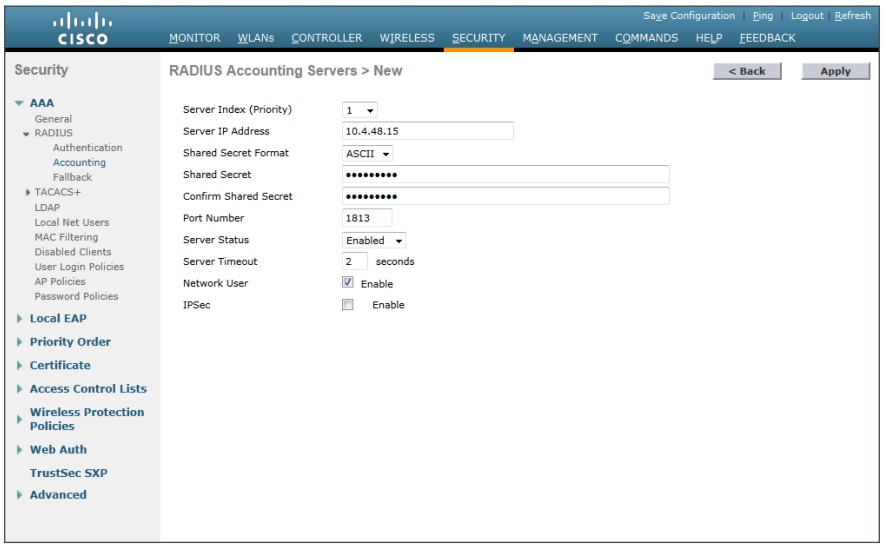
Step 4: To the right of Management, clear **Enable**, and then click **Apply**.



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

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

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



Procedure 12 Configure management authentication

(Optional)

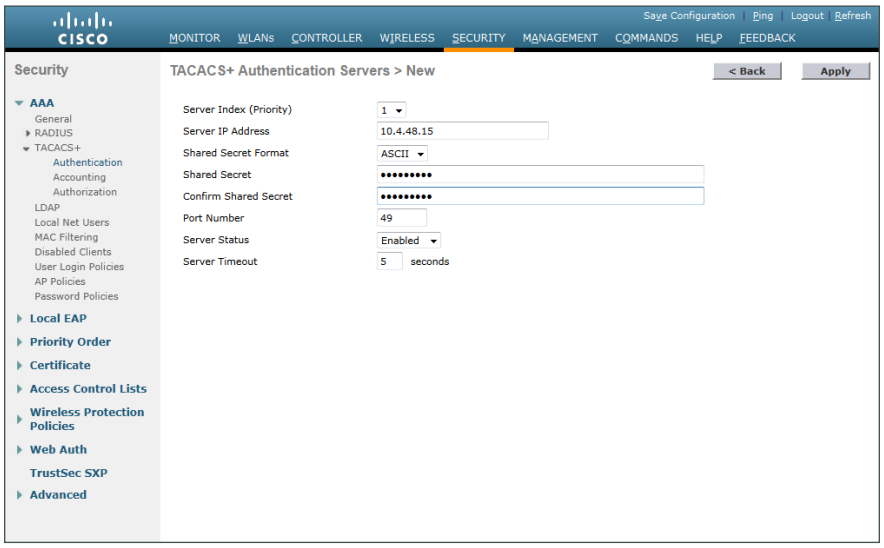
You can use this procedure to deploy centralized management authentication by configuring an authentication, authorization and accounting (AAA) service. If you prefer to use local management authentication, skip to Procedure 13.

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

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

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

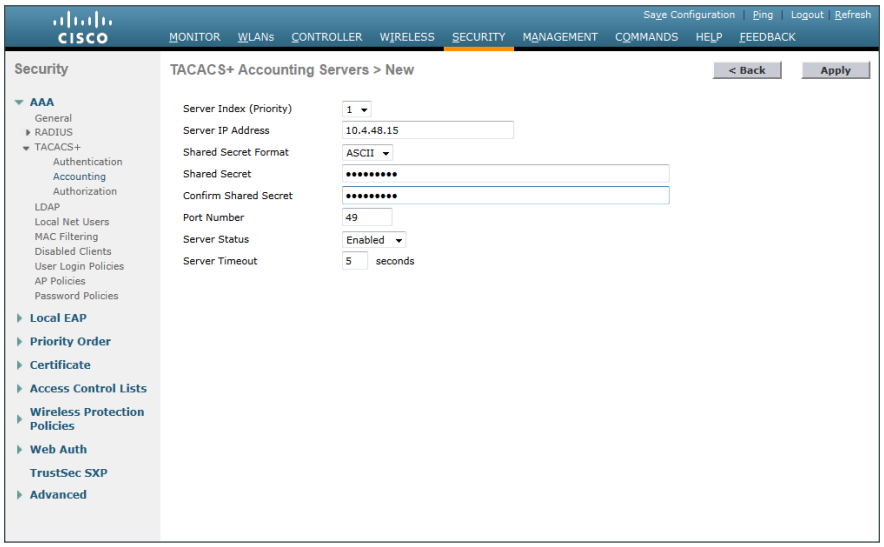
Step 3: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)



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

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

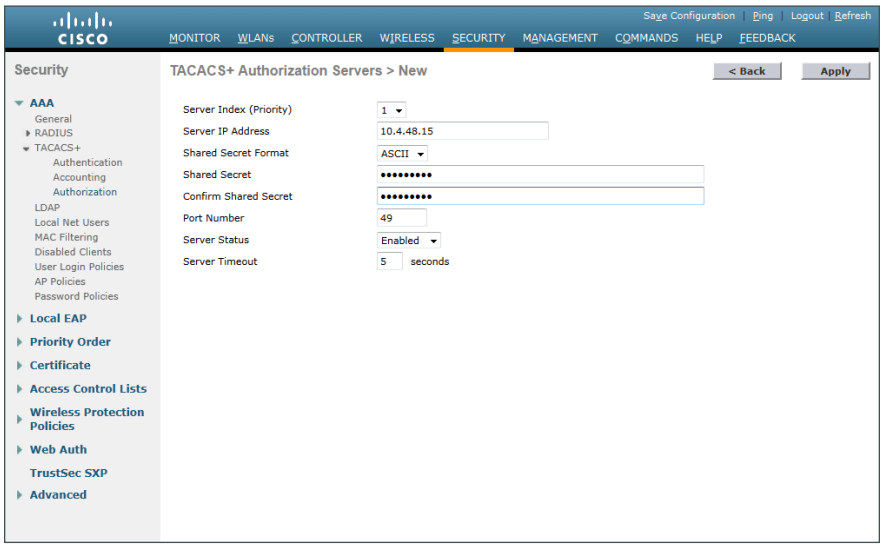
Step 6: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)



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)

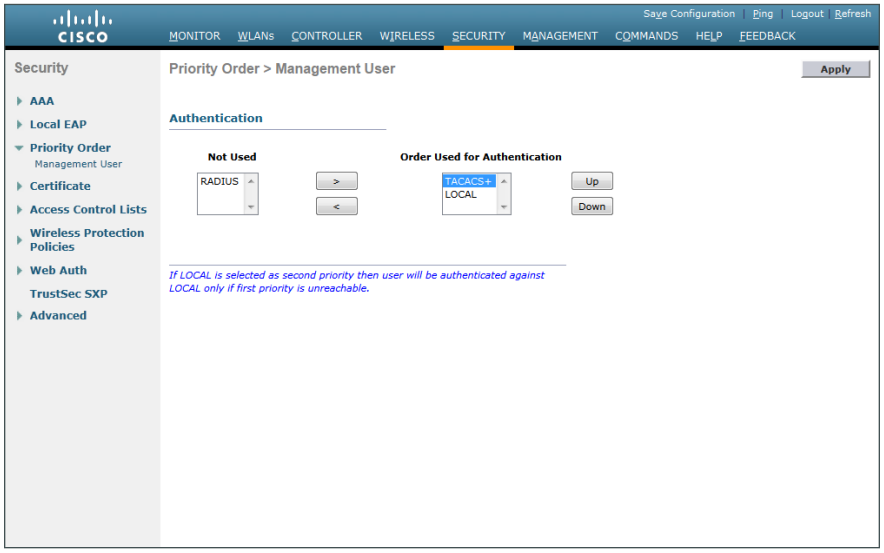


Step 10: Navigate to **Security > Priority Order > Management User**.

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**.



Procedure 13 Configure the resilient WLC

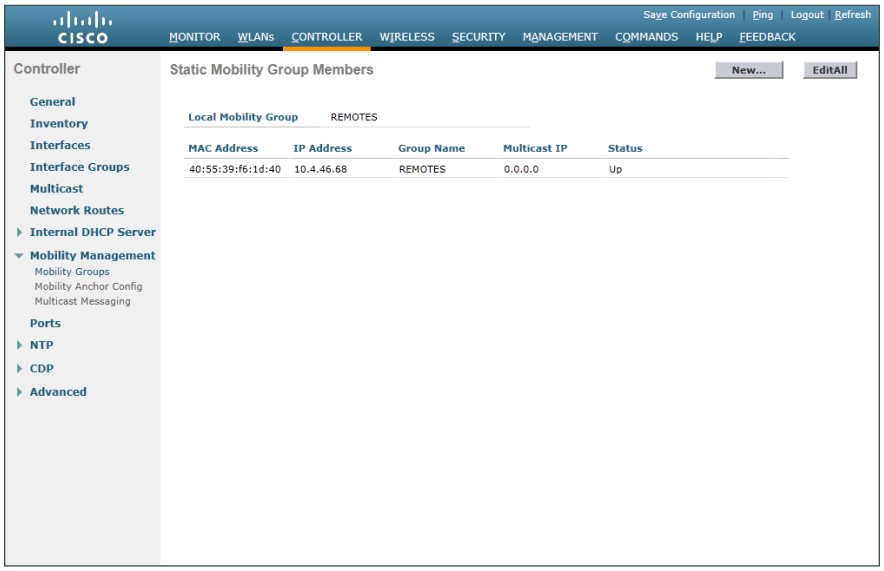
This design uses two WLCs. The first is the primary WLC, and the access points register to it. The second WLC provides resiliency in case the primary WLC fails. Under normal operation, there will not be any access points registered to this WLC.

Step 1: Configure the resilient AP-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 AP SSO mode of operation (Cisco 5500 Series WLCs or Cisco Flex 7500 Series Cloud Controllers), you should skip this procedure. If you are using two or more WLCs without AP SSO (vWLCs), then complete this procedure in order to create a mobility group.

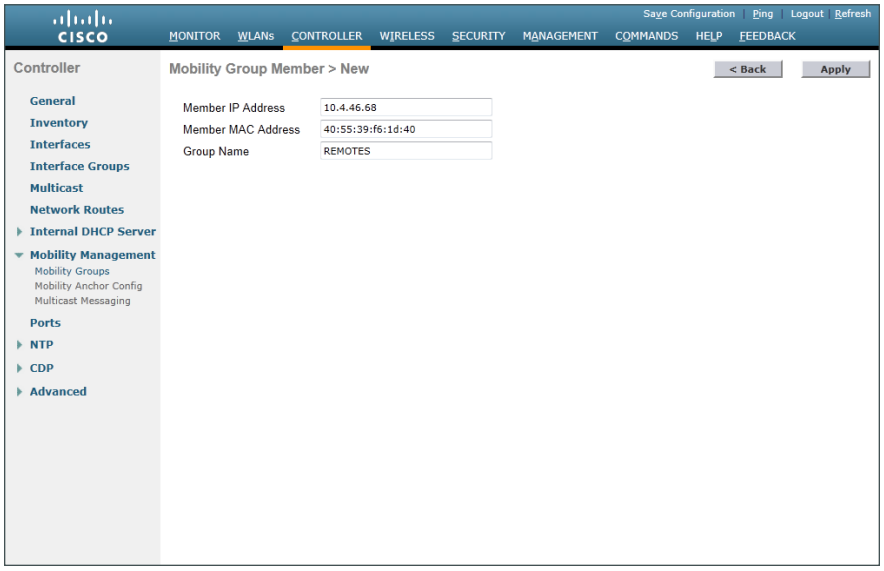
Step 1: On the primary controller, navigate to **Controller > Mobility Management > Mobility Groups**. The MAC address, IP address, and mobility group name for the local controller are shown on the Static Mobility Group Members page.



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

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

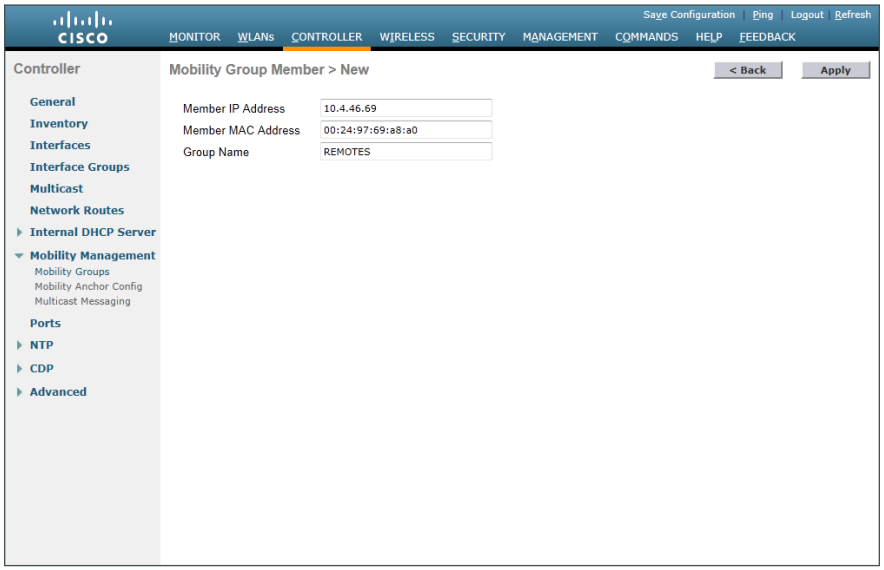
Step 4: In the **Member MAC Address** box, enter the MAC address of the primary controller, and then click **Apply**.



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

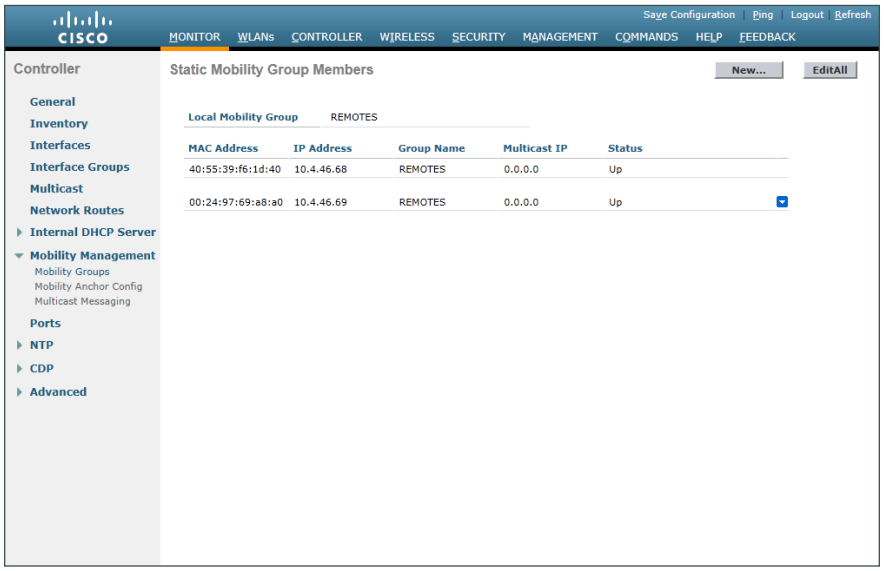
Step 6: In the **Member IP Address** box, enter the IP address of the resilient controller. (Example: 10.4.46.69)

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



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

Step 9: Navigate to **Controller > Mobility Management > Mobility Groups**, and then verify that connectivity is up between all the controllers by examining the mobility group information. In the Status column, all controllers should be listed as **Up**.



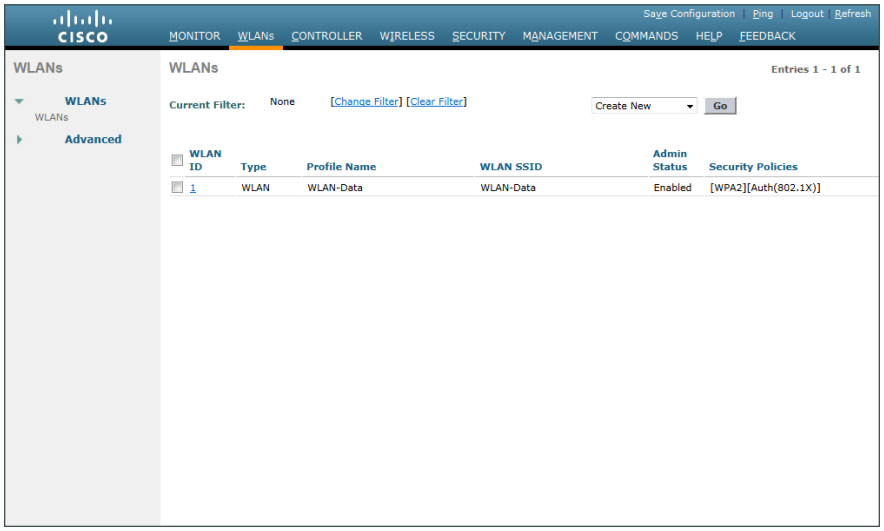
Procedure 15 Configure the data wireless LAN

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

Step 1: Navigate to **WLANs**.

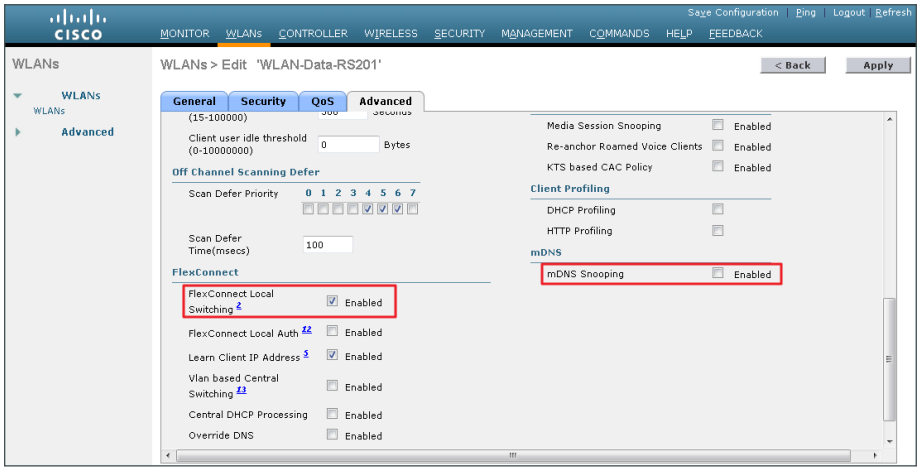
Step 2: Click the WLAN ID number of the data SSID.

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



Step 4: On the Advanced tab, disable mDNS Snooping as this is not supported with FlexConnect Local Switching.

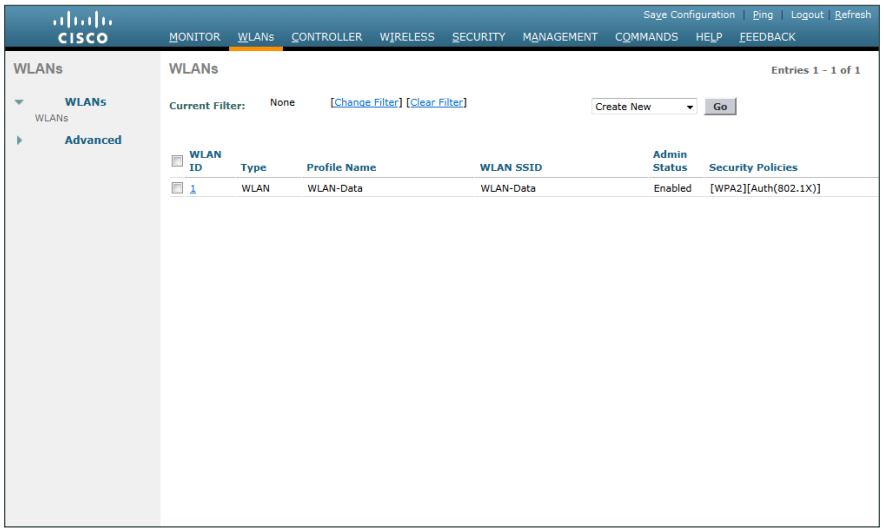
Step 5: Enable FlexConnect Local Switching by selecting **Enabled**, and then click **Apply**.



Procedure 16 Configure the voice wireless LAN

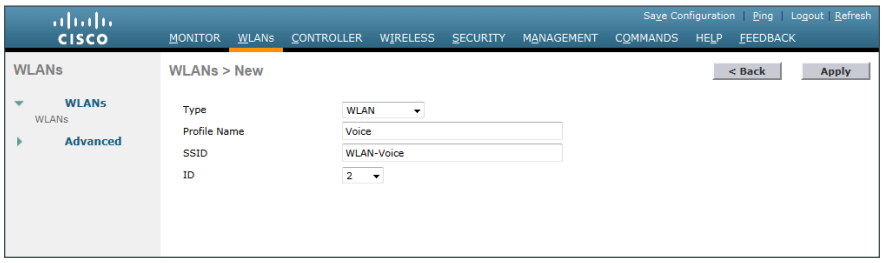
Wireless voice traffic is unique among other types of data traffic in that it cannot effectively handle delay and jitter or packet loss. To configure the voice WLAN, change the default QoS settings to Platinum and segment the voice traffic onto the voice wired VLAN.

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



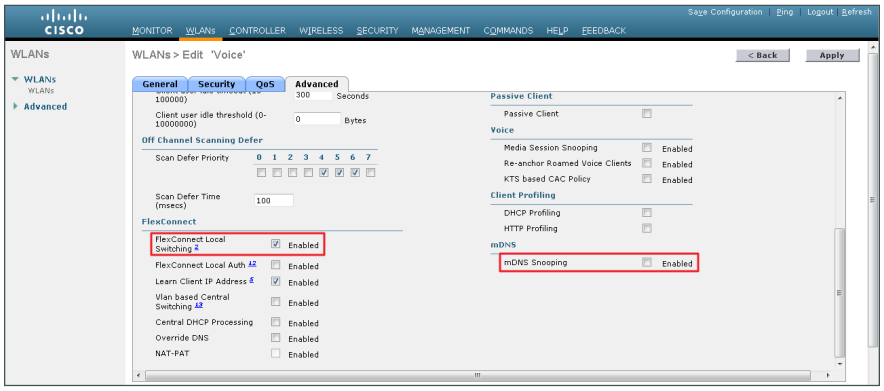
Step 2: Enter the **Profile Name**. (Example: Voice)

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

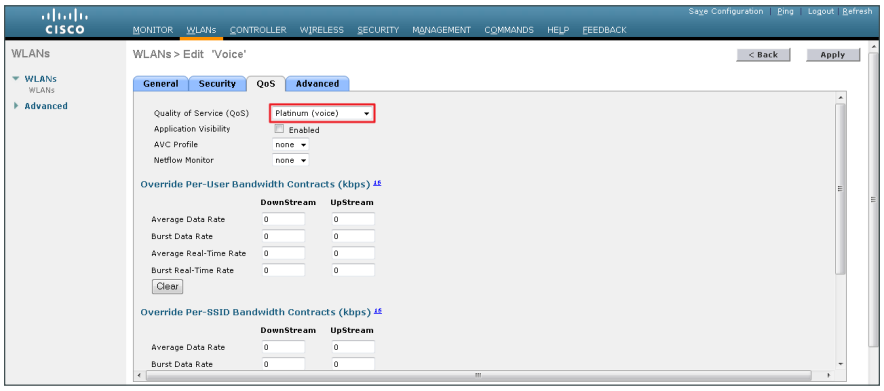


Step 4: On the Advanced tab, disable mDNS Snooping as this is not supported with FlexConnect Local Switching.

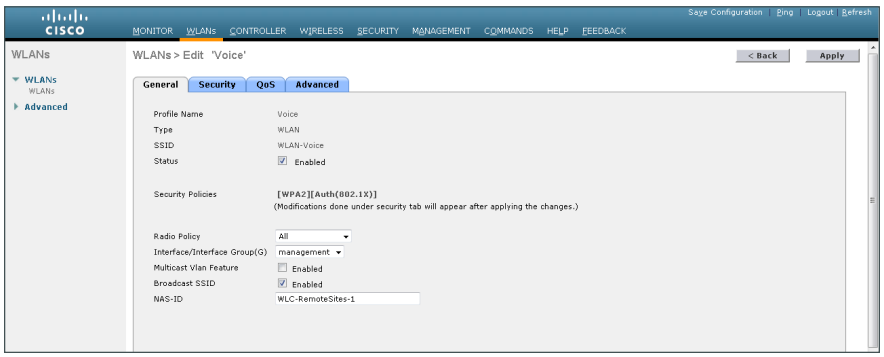
Step 5: Enable FlexConnect Local Switching by selecting **Enabled**, and then click **Apply**.



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



Step 7: On the General tab, to the right of Status, select **Enabled**, and then click **Apply**.



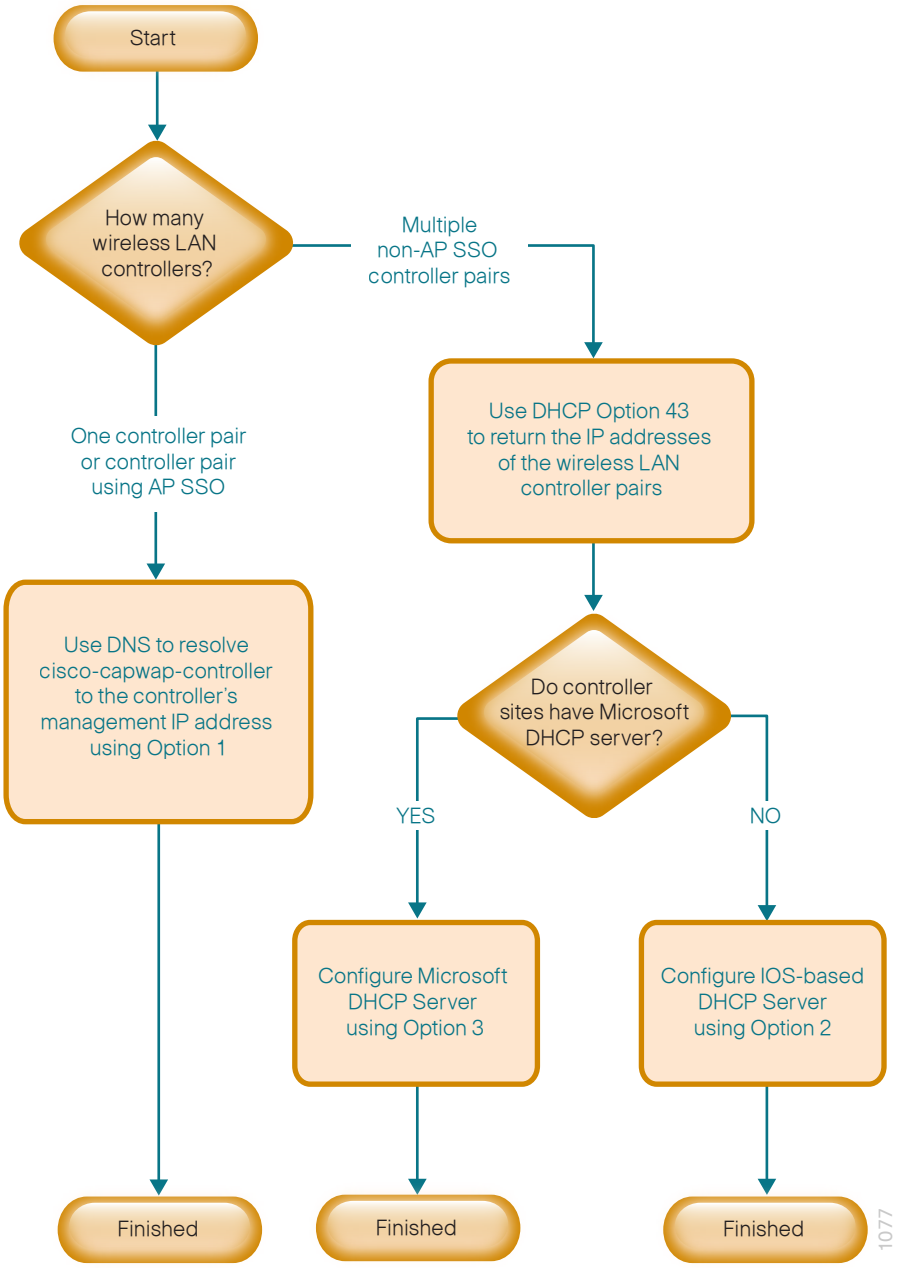
Procedure 17 Configure controller discovery

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 6 - Flow chart of WLC discovery configuration options



Option 1: Only one WLC pair in the organization

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

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

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

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

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

Step 1: Assemble the DHCP Option 43 value.

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

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

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

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

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

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

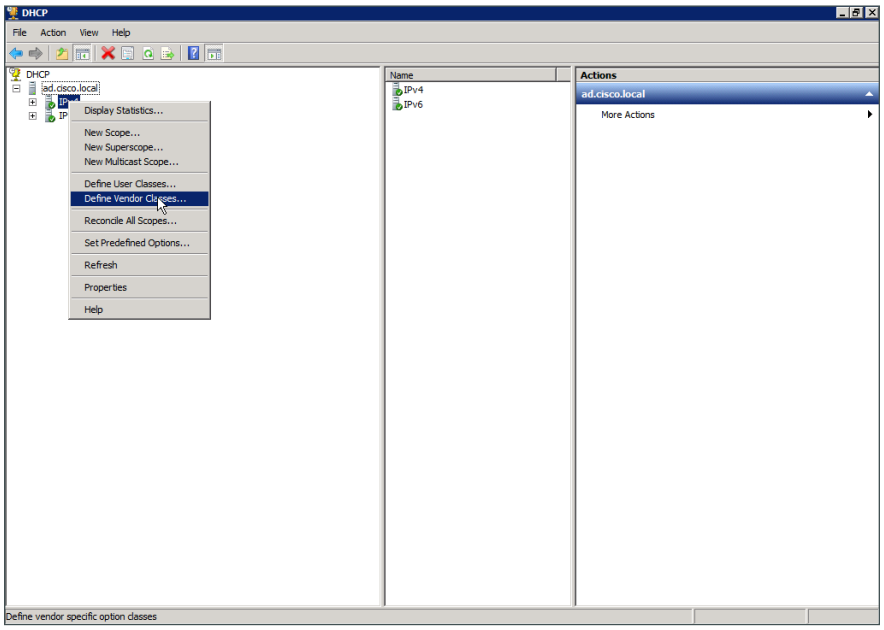
This procedure shows how the Microsoft DHCP server is configured to return vendor-specific information to the lightweight Cisco Aironet 1600, 2600, and 3600 Series Access Points used in this design guide. The vendor class identifier for a lightweight Cisco Aironet access point is specific to each model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

Table 6 - Vendor class identifiers

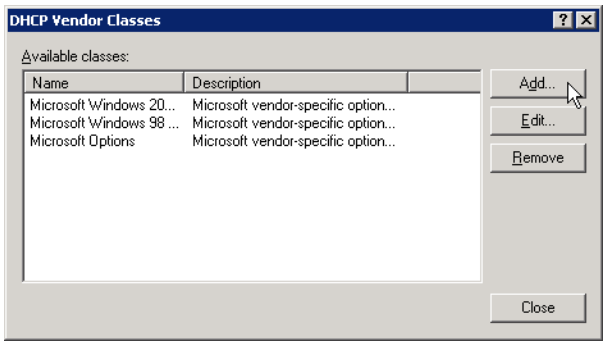
Access point	Vendor class identifier
Cisco Aironet 1600 Series	Cisco AP c1600
Cisco Aironet 2600 Series	Cisco AP c2600
Cisco Aironet 3600 Series	Cisco AP c3600

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

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



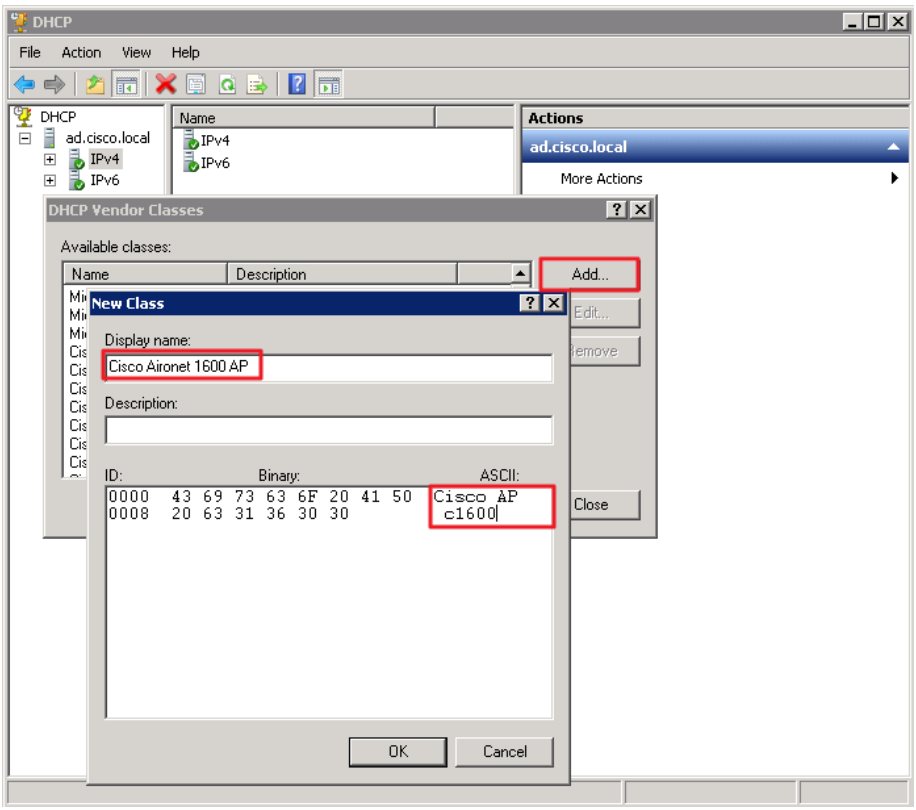
Step 3: In the DHCP Vendor Classes dialog box, click **Add**.



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

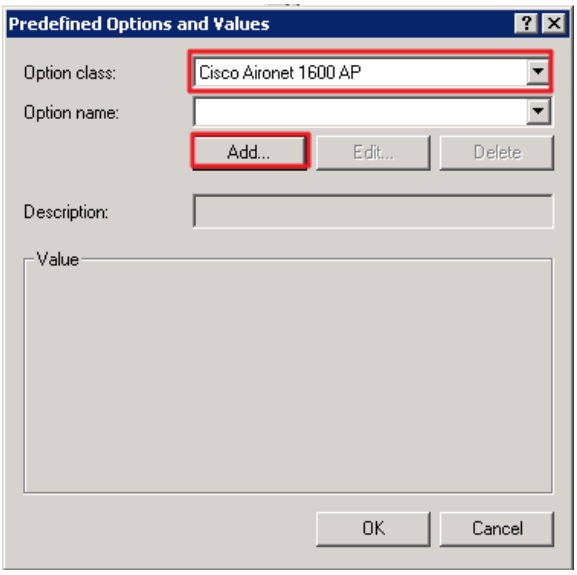
Step 5: In the ASCII section, enter the vendor class identifier for the appropriate access point series from Table 6, and then click **OK**. (Example: Cisco AP c1600)

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**.

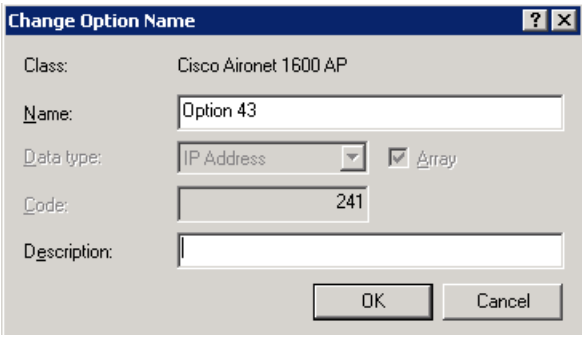


Step 9: In the **Option Type** dialog box, enter a **Name**. (Example: Option 43)

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**.



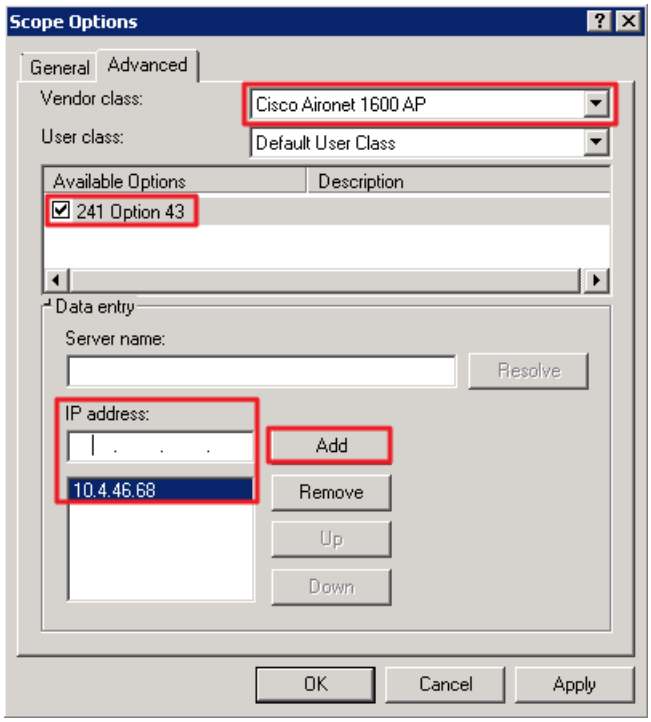
The vendor class and suboption are now programmed into the DHCP server. Now, you need to define the vendor-specific information for the DHCP scope.

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: 10.4.46.68)



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

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

```
interface GigabitEthernet 1/0/23
  description FlexConnect Access Point Connection
  switchport trunk encapsulation dot1q
  switchport trunk native vlan 64
  switchport trunk allowed vlan 64,65,70
  switchport mode trunk
  switchport port-security maximum 255
  spanning-tree portfast trunk
  macro apply EgressQoS
```

Procedure 20 Enable licensing on the vWLC

The Wireless LAN Controller virtual Appliance OVA includes a temporary 60-day license that includes 200 access points. You can activate the demo license included with the 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 > Licensing**.

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 vWLC by navigating to **Commands > Reboot > Save and Reboot**.

Procedure 21 Configure the AP for Cisco FlexConnect

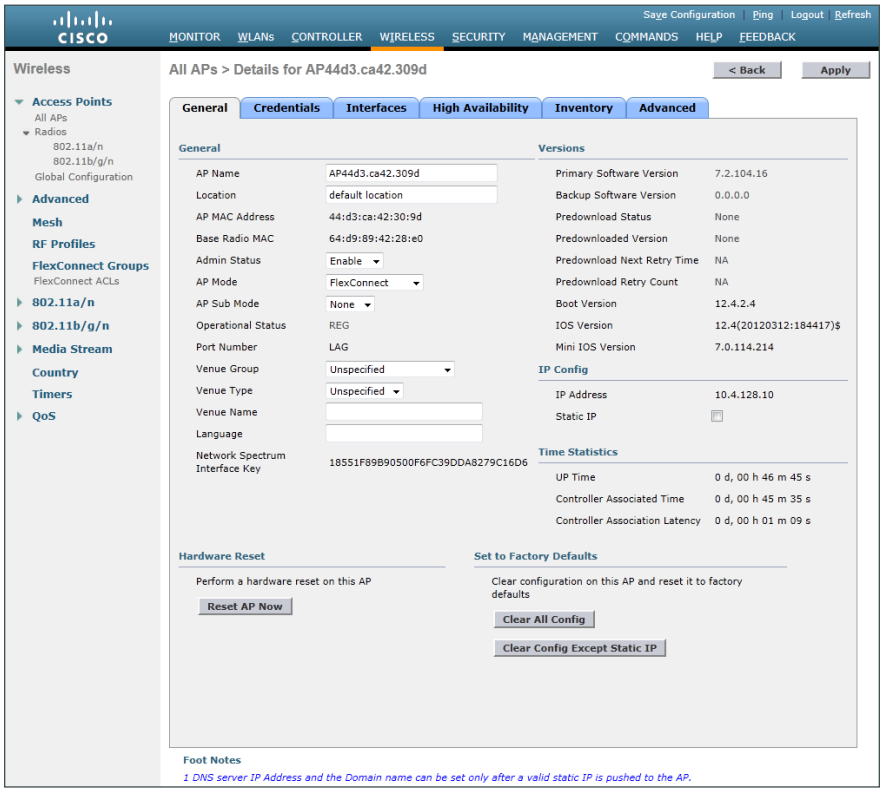
Step 1: Connect the access point to the remote-site switch, and then wait for the light on the access point to turn a solid color.

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

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

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

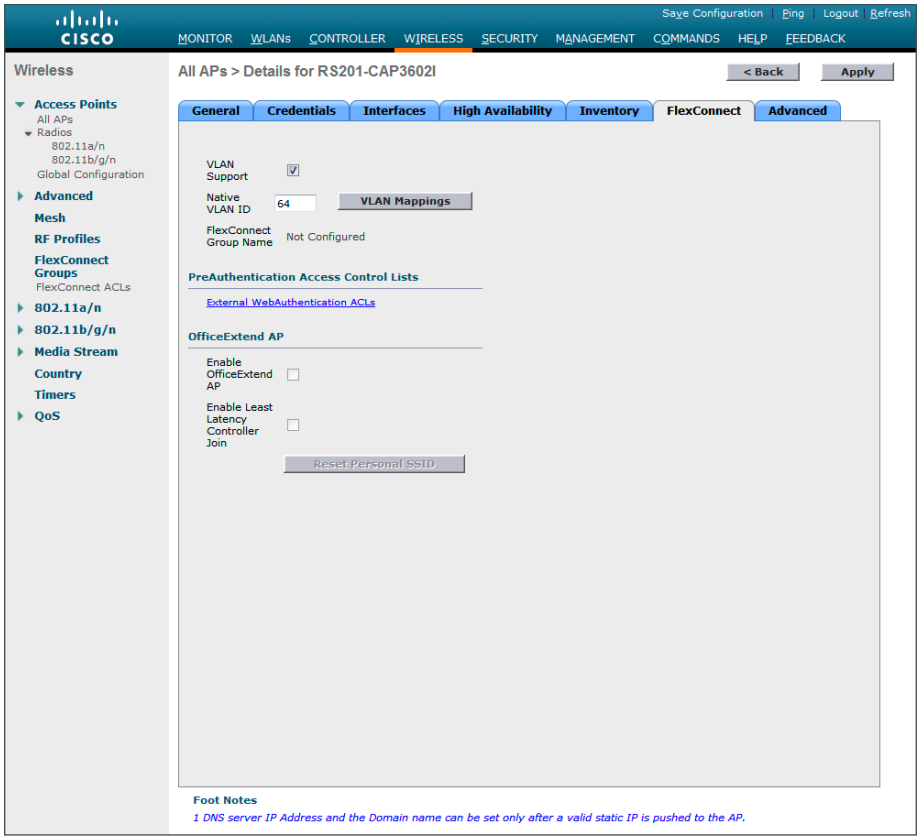
If the access points were registered to the WLC prior to issuing the **autoconvert** command, on the General tab, in the **AP Mode** list, choose **FlexConnect**, and then click **Apply**. Wait for the access point to reboot and reconnect to the controller. This should take approximately three minutes.



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

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

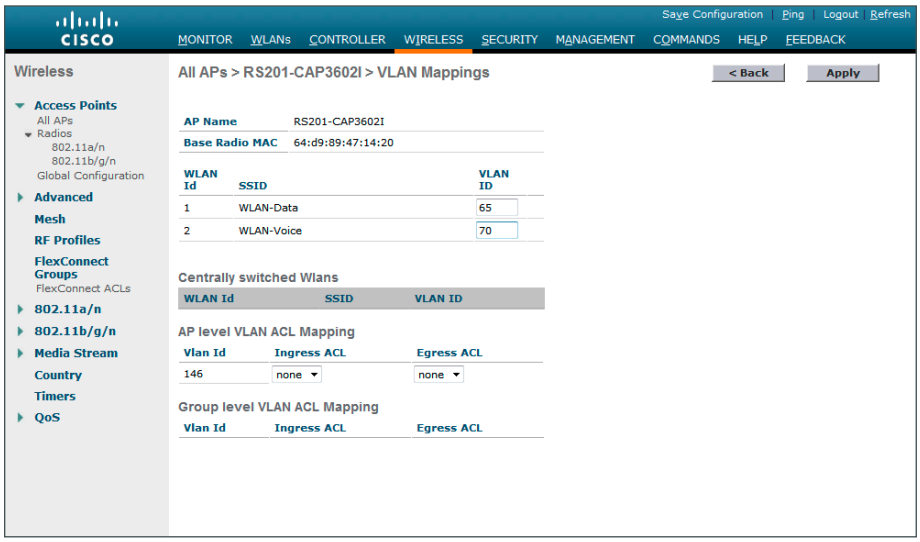
Step 7: In the **Native VLAN ID** box, enter the trunk's native VLAN number as configured in Procedure 17, and then click **Apply**. (Example: 64)



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 17, and then click **Apply**. (Example: 70)



Procedure 22 Configure access points for resiliency

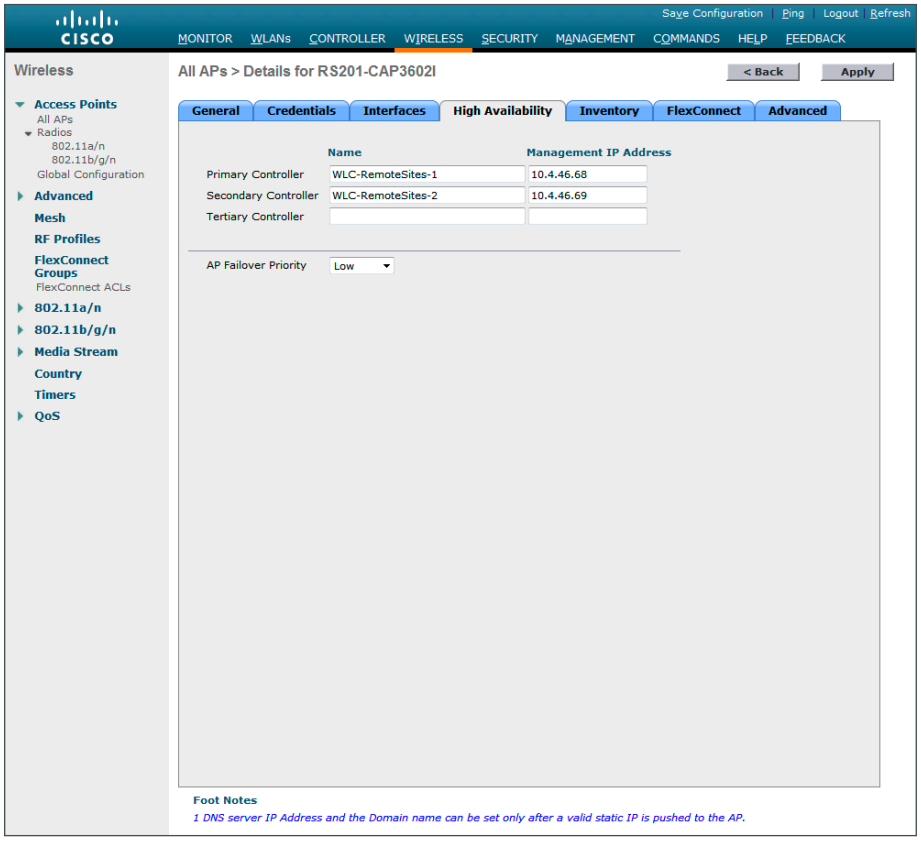
If you are using the AP SSO high availability feature on a Cisco 5500 Series WLC or Cisco Flex 7500 Series Cloud Controller, skip this procedure, as the resilient controller automatically tracks the primary controller and assumes its IP address in the event of a failure. The AP SSO feature is not available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

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

Step 2: Click the **High Availability** tab.

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

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



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

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

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

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

Step 8: Repeat Procedure 23 for each remote site.

PROCESS

Configuring Guest Wireless: Shared Guest Controller

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

Procedure 1 Configure the distribution switch

The VLAN used in the following configuration examples is:

Guest Wireless–**VLAN 1128, IP: 192.168.28.0/22**

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

```
vlan 1128
 name Guest_Wireless
```

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

```
interface GigabitEthernet1/0/24
 description IE-ASA5540a Gig0/1
!
interface GigabitEthernet2/0/24
 description IE-ASA5540b Gig0/1
!
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
 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 7 - Cisco ASA DMZ interface information

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

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

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

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

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

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

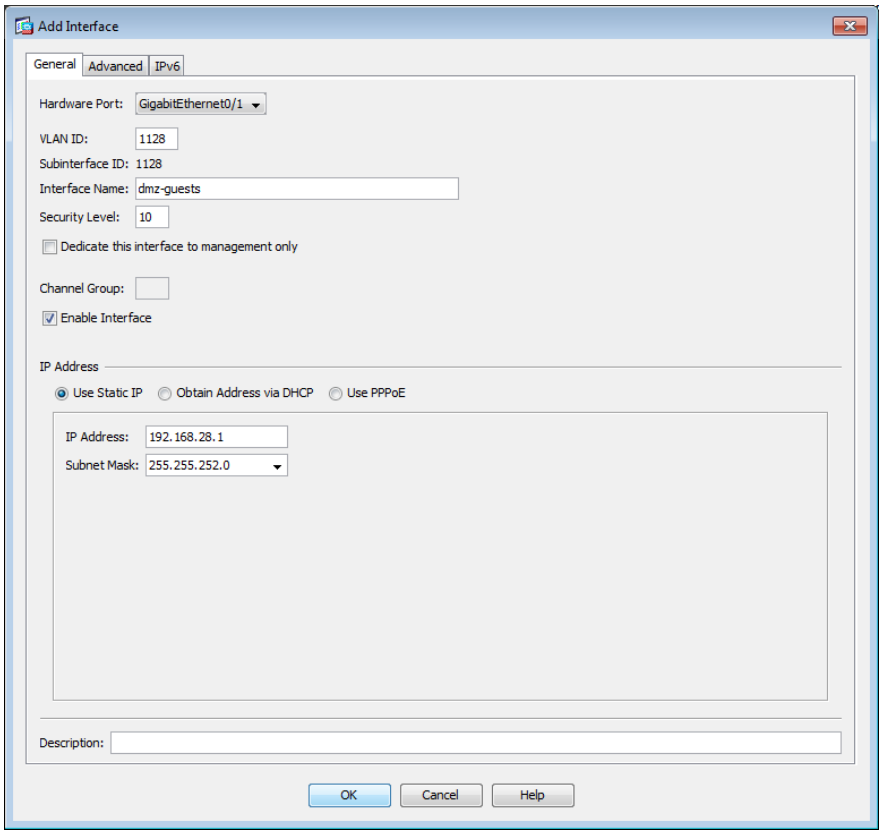
Step 6: In the **Subinterface ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1128)

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

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

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

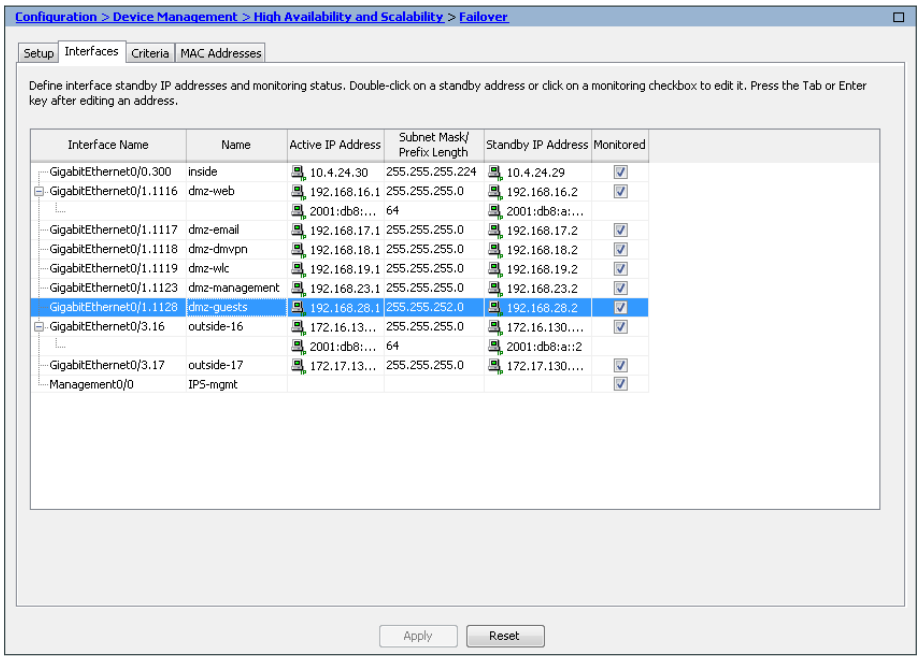
Step 10: Enter the interface **Subnet Mask**, and then click **OK**. (Example: 255.255.252.0)



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.

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

Step 2: Click **Add > Network Object**.

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

Step 4: In the **Type** list, choose **Network**.

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

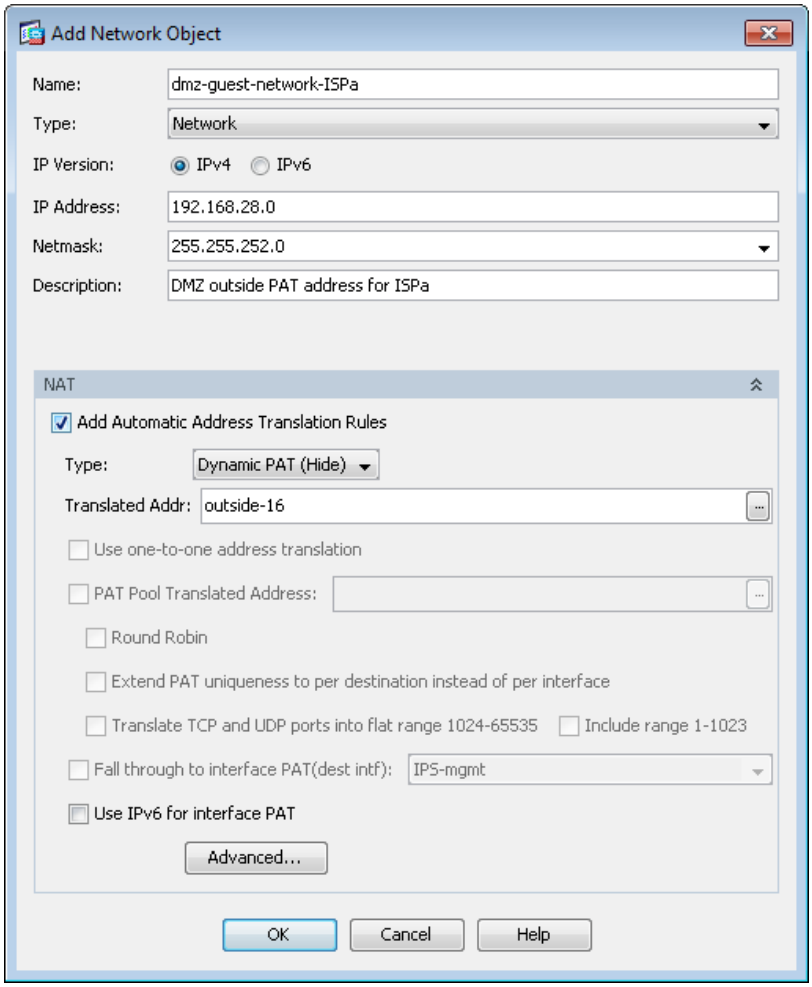
Step 6: Enter the guest DMZ netmask. (Example: 255.255.252.0)

Step 7: Click the two down arrows. The NAT pane expands.

Step 8: Select **Add Automatic Address Translation Rules**.

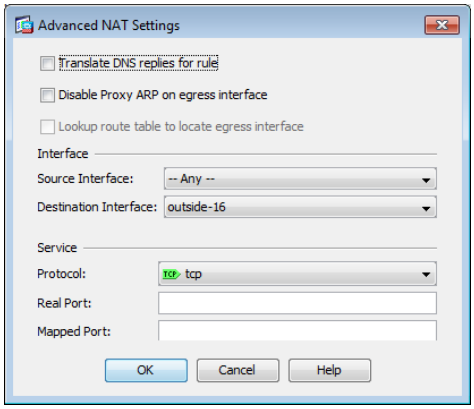
Step 9: In the **Type** list, choose **Dynamic PAT (Hide)**.

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



Step 11: Click **Advanced**.

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

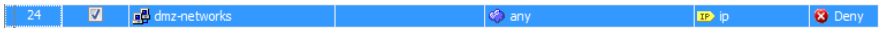


Step 13: In the Add Network Object dialog box, click **OK**.

Procedure 4 Configure guest network security policy

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

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



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

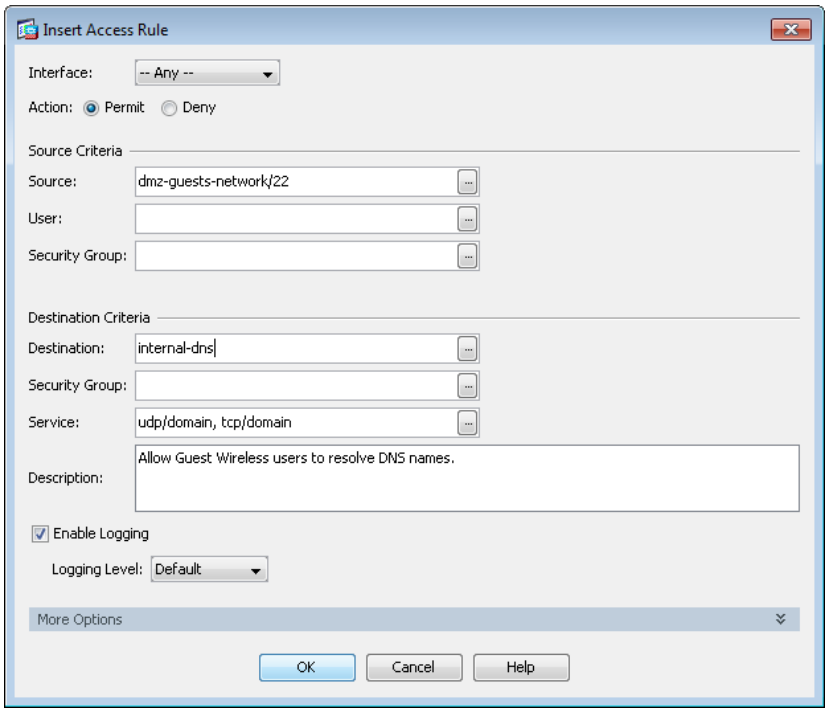
Step 3: Click **Add > Insert**.

Step 4: In the **Interface** list, choose **Any**.

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

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

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



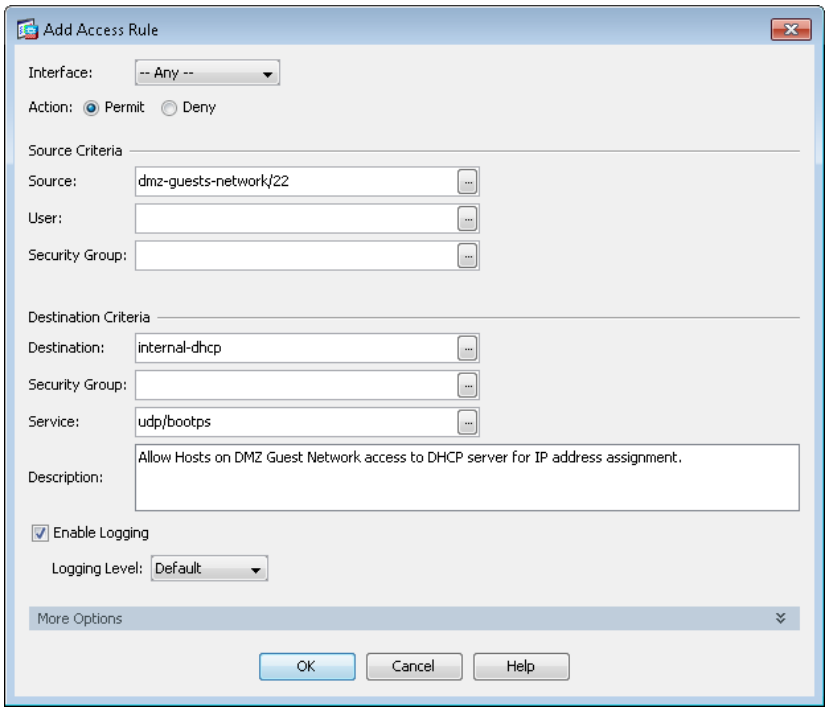
Step 8: Click **Add > Insert**.

Step 9: In the **Interface** list, choose **Any**.

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

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

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



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

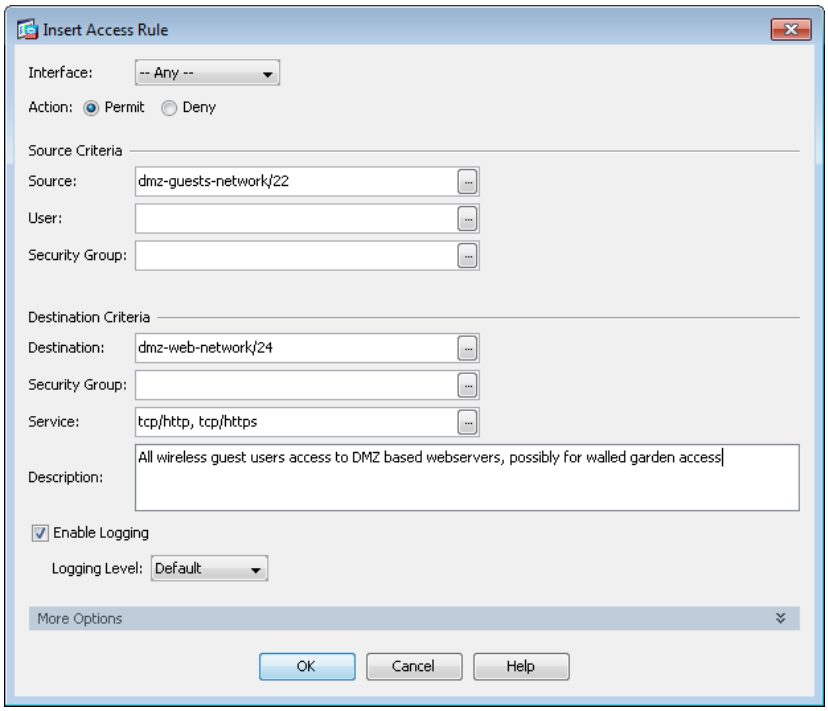
Step 13: Click **Add > Insert**.

Step 14: In the **Interface** list, choose **Any**.

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

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

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



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

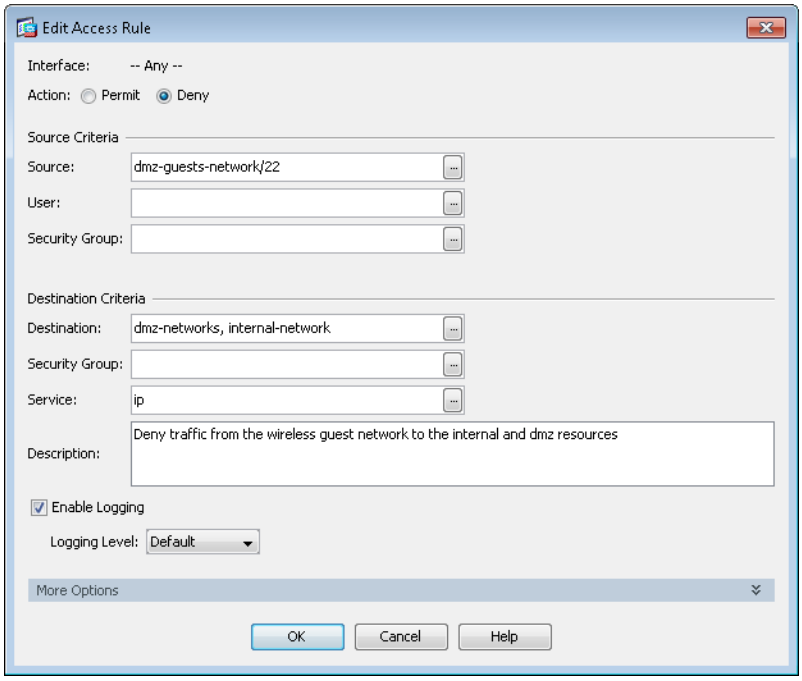
Step 18: Click **Add > Insert**.

Step 19: In the **Interface** list, choose **Any**.

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

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

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

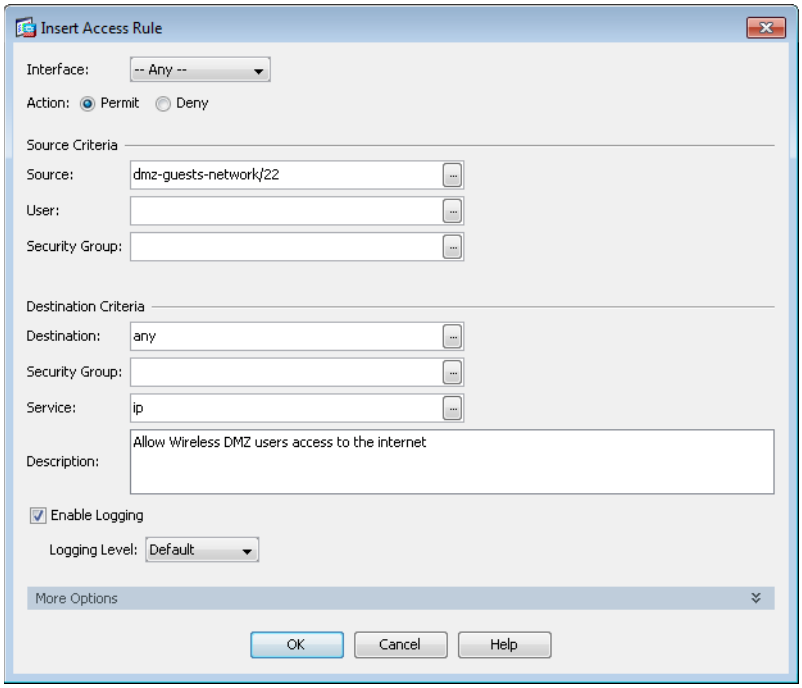


Next, you enable the guests to communicate with the Internet.

Step 23: Click **Add > Insert**.

Step 24: In the **Interface** list, choose **Any**.

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



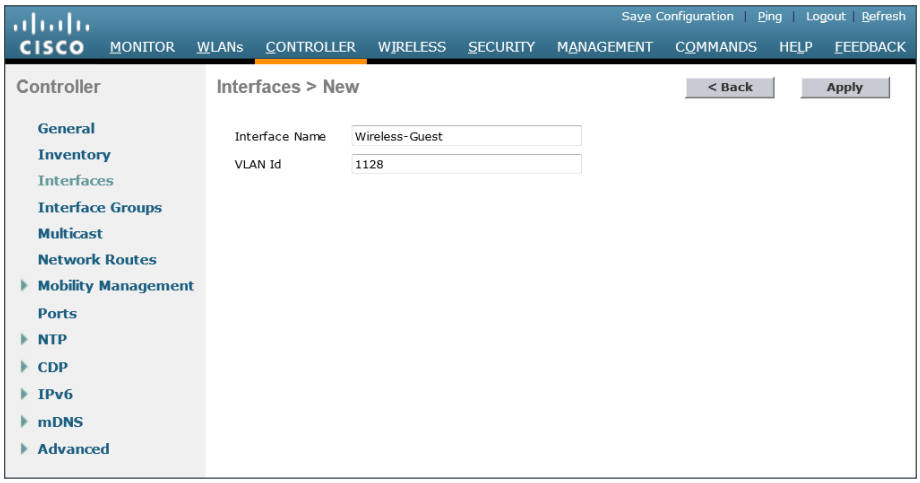
Procedure 5 Create the guest wireless LAN interface

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

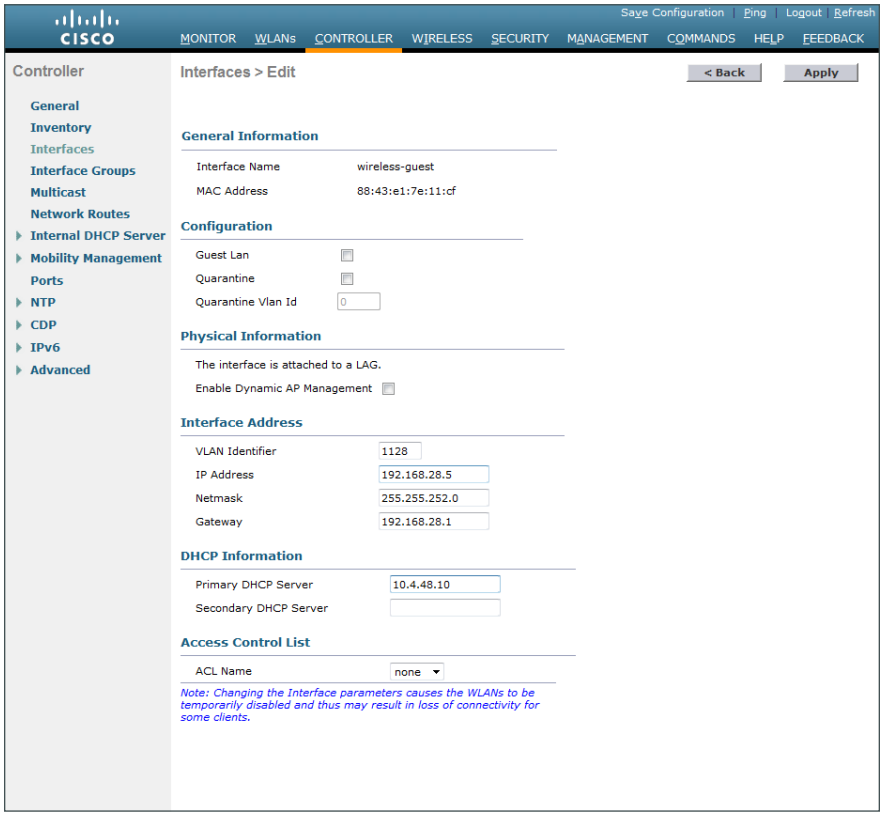


Step 4: In the **IP Address** box, enter the IP address you want to assign to the WLC interface. (Example: 192.168.28.5)

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)

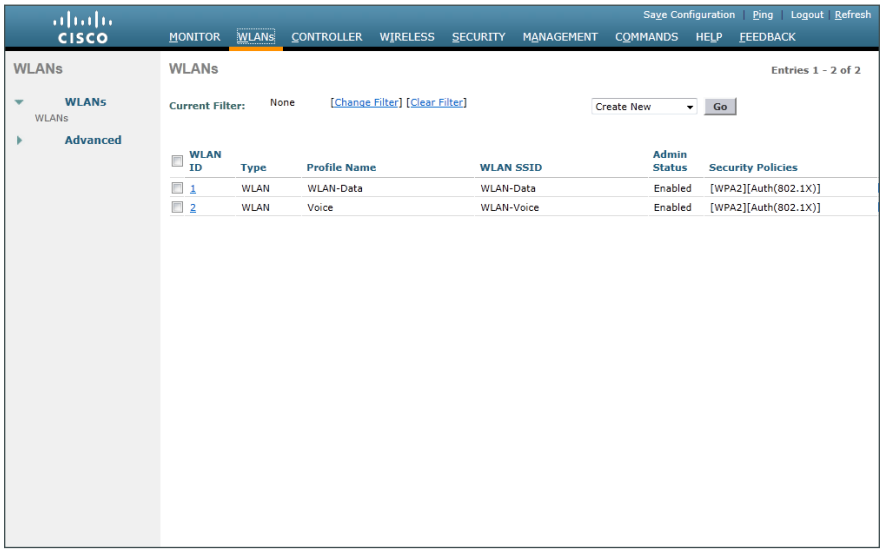


Tech Tip

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.

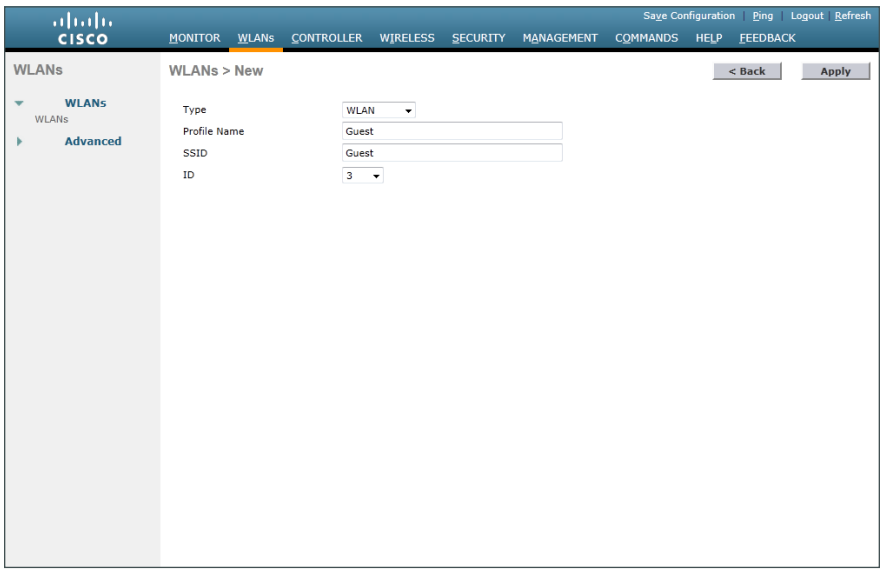
Procedure 6 Configure the guest wireless LAN

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

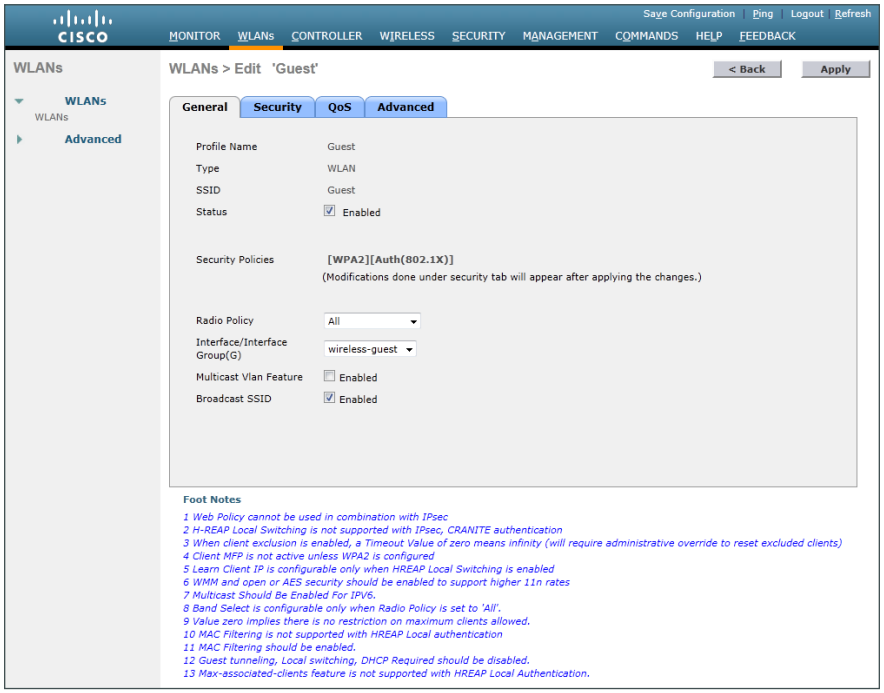


Step 2: Enter the **Profile Name**. (Example: Guest)

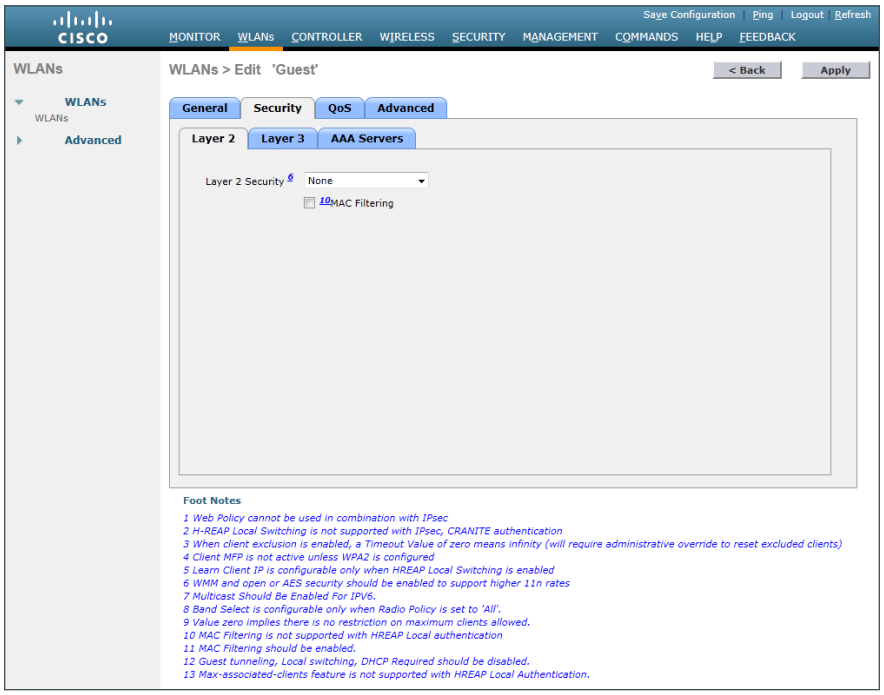
Step 3: In the **SSID** box, enter the guest WLAN name, and then click **Apply**. (Example: Guest)



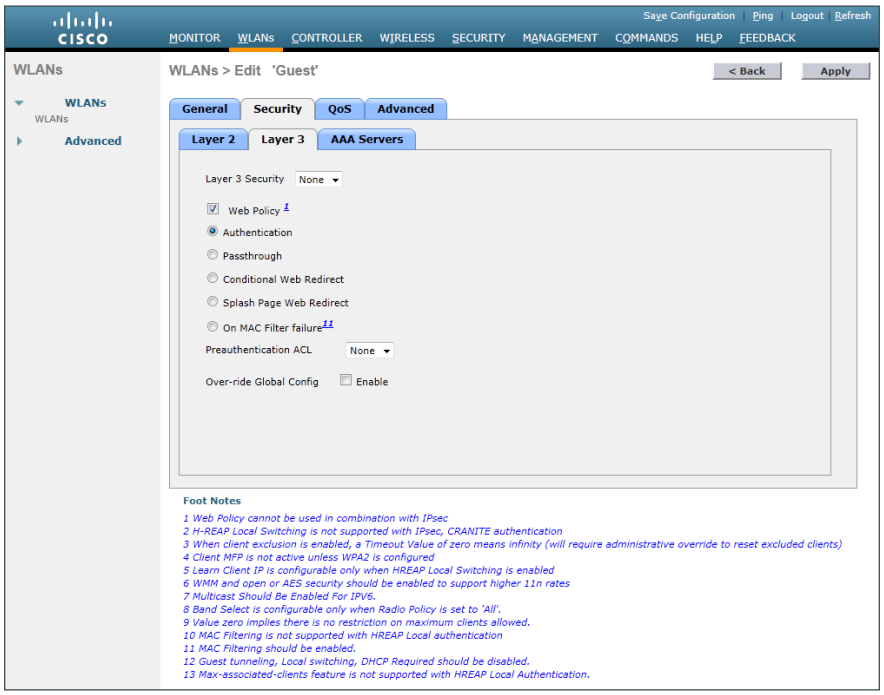
Step 4: On the General tab, in the **Interface/Interface Group(G)** list, choose the interface created in Procedure 5. (Example: wireless-guest)



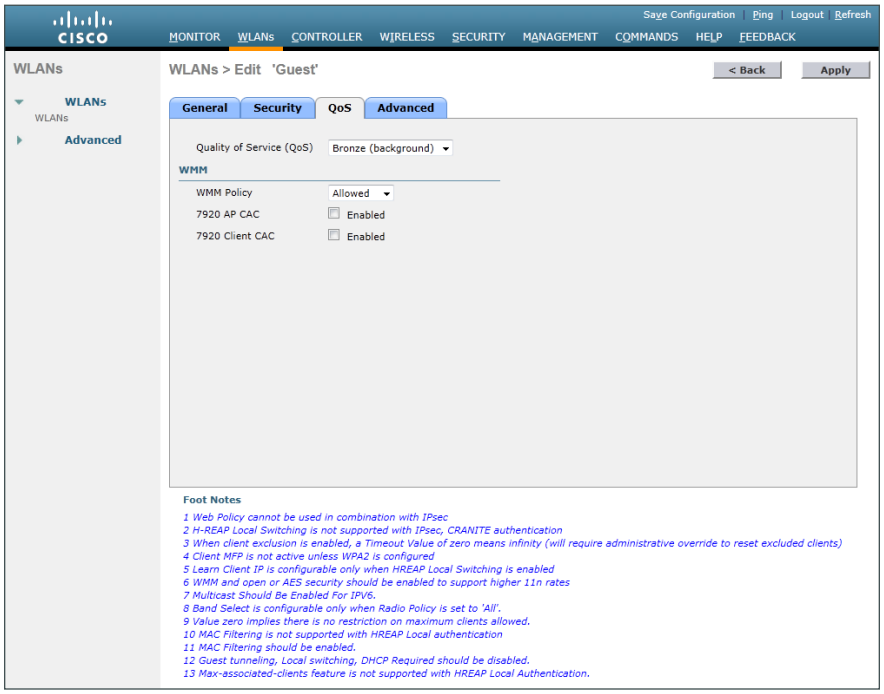
Step 5: Click the **Security** tab, and then on the Layer 2 tab, in the **Layer 2 Security** list, choose **None**.



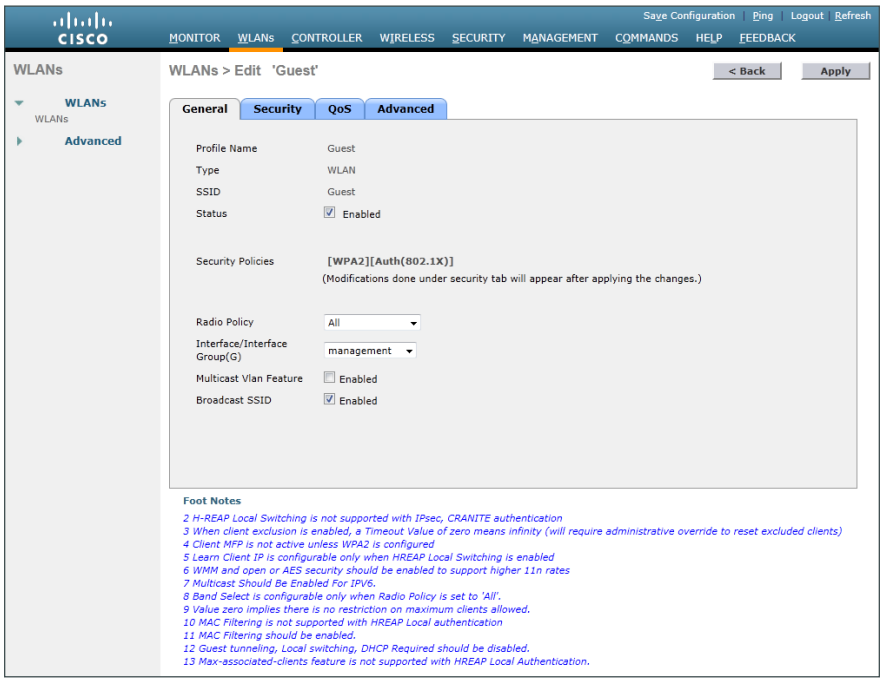
Step 6: On the **Layer 3** tab, select **Web Policy**, and then click **OK**.



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 7 Create the lobby admin user account

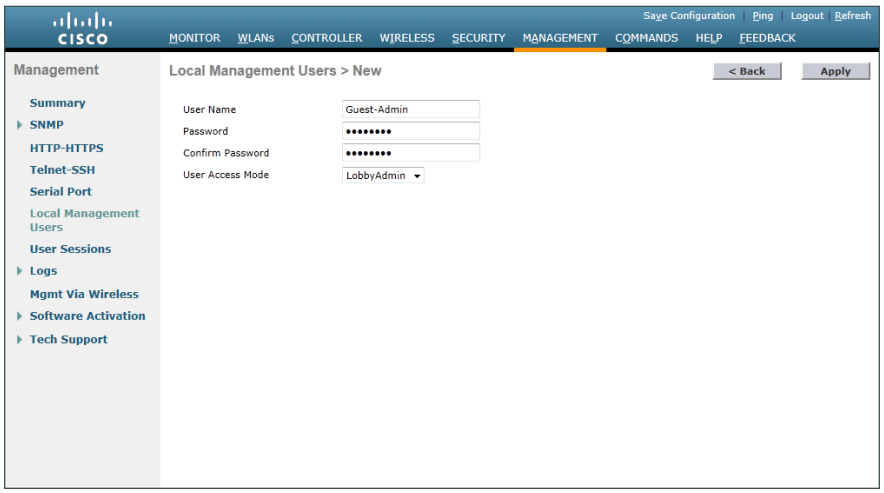
Typically, the lobby administrator is the first person to interact with your corporate guests. The lobby administrator can create individual guest user accounts and passwords that last from one to several days, depending upon the length of stay for each guest.

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

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

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

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

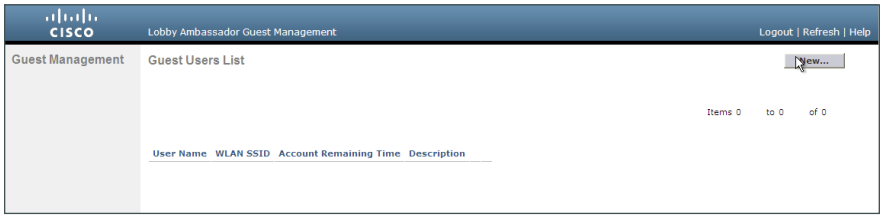


Procedure 8 Create guest accounts

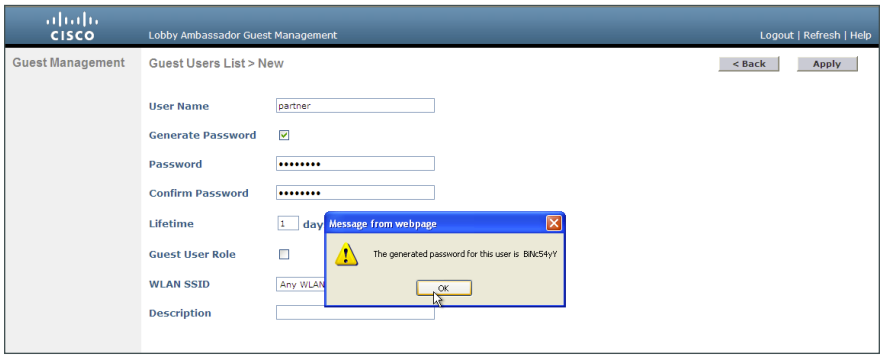
Now you can use the lobby administrator account to create usernames and passwords for partners, customers, and anyone else who is not normally granted access to your network.

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

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



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

Procedure 1 Configure the DMZ switch

The VLANs used in the following configuration examples are:

- Guest Wireless–**VLAN 1128, IP: 192.168.28.0/22**
- Wireless management–**VLAN 1119, IP 192.168.19.0/24**

Step 1: On the DMZ switch, create the wireless VLANs.

```
vlan 1119
 name WLAN_Mgmt
vlan 1128
 name Guest_Wireless
```

Step 2: Configure the interfaces that connect to the Internet firewalls as trunk ports and add the wireless VLANs.

```
interface GigabitEthernet1/0/24
 description IE-ASA5545a Gig0/1
!
interface GigabitEthernet2/0/24
 description IE-ASA5545b Gig0/1
!
interface range GigabitEthernet1/0/24, GigabitEthernet2/0/24
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan add 1119, 1128
 switchport mode trunk
 macro apply EgressQoS
 logging event link-status
 logging event trunk-status
 no shutdown
```

Step 3: This deployment uses Layer 2 EtherChannels in order to connect the WLCs to the DMZ switch. Connect the WLC EtherChannel uplinks to separate devices in the DMZ stack.

On the DMZ switch, the physical interfaces that are members of a Layer 2 EtherChannel are configured prior to configuring the logical port-channel interface. Doing the configuration in this order allows for minimal configuration because most of the commands entered to a port-channel interface are copied to its members' interfaces and do not require manual replication.

Configure two or more physical interfaces to be members of the EtherChannel. It is best if they are added in multiples of two.

```
Interface range GigabitEthernet1/0/13, GigabitEthernet2/0/13
description DMZ-WLC-Guest-1
!
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
 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
 logging event link-status
 no shutdown
```

Procedure 2 Configure the firewall DMZ interface

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

The various DMZ networks are connected to Cisco ASA on the appliances' Gigabit Ethernet interface via a VLAN trunk. The IP address assigned to the VLAN interface on the appliance is the default gateway for that DMZ subnet. The DMZ switch's VLAN interface does not have an IP address assigned for the DMZ VLAN.

Table 8 - Cisco ASA DMZ interface information

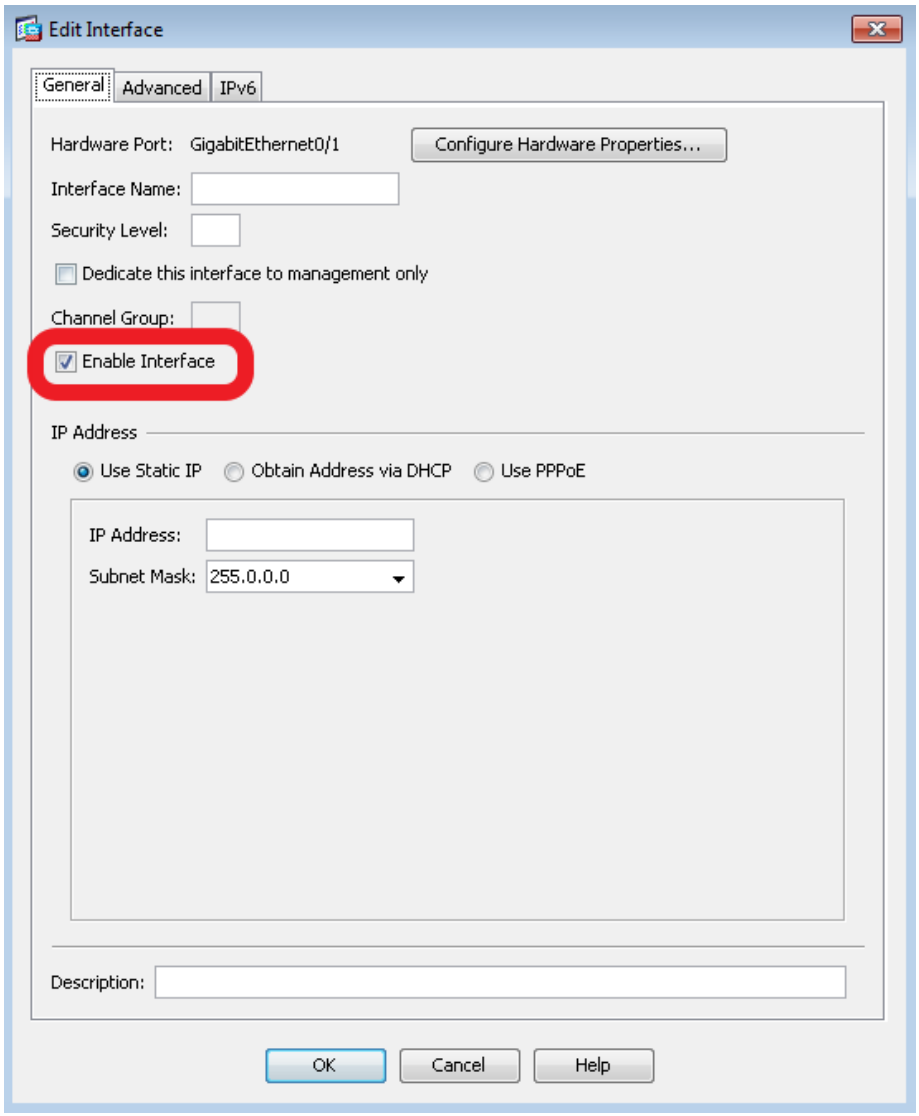
Interface Label	IP Address & Netmask	VLAN	Security Level	Name
GigabitEthernet0/1.1119	192.168.19.1/24	1119	50	dmz-wlc
GigabitEthernet0/1.1128	192.168.28.1/22	1128	10	dmz-guests

Step 1: Login to the Internet Edge firewall using Cisco ASDM.

Step 2: Navigate to **Configuration > Device Setup > Interfaces**, and then click the interface that is connected to the DMZ switch. (Example: GigabitEthernet0/1)

Step 3: Click **Edit**.

Step 4: Select **Enable Interface**, and then click **OK**.



Step 5: On the Interface pane, click **Add > Interface**.

Step 6: In the **Hardware Port** list, choose the interface configured in Step 2. (Example: GigabitEthernet0/1)

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

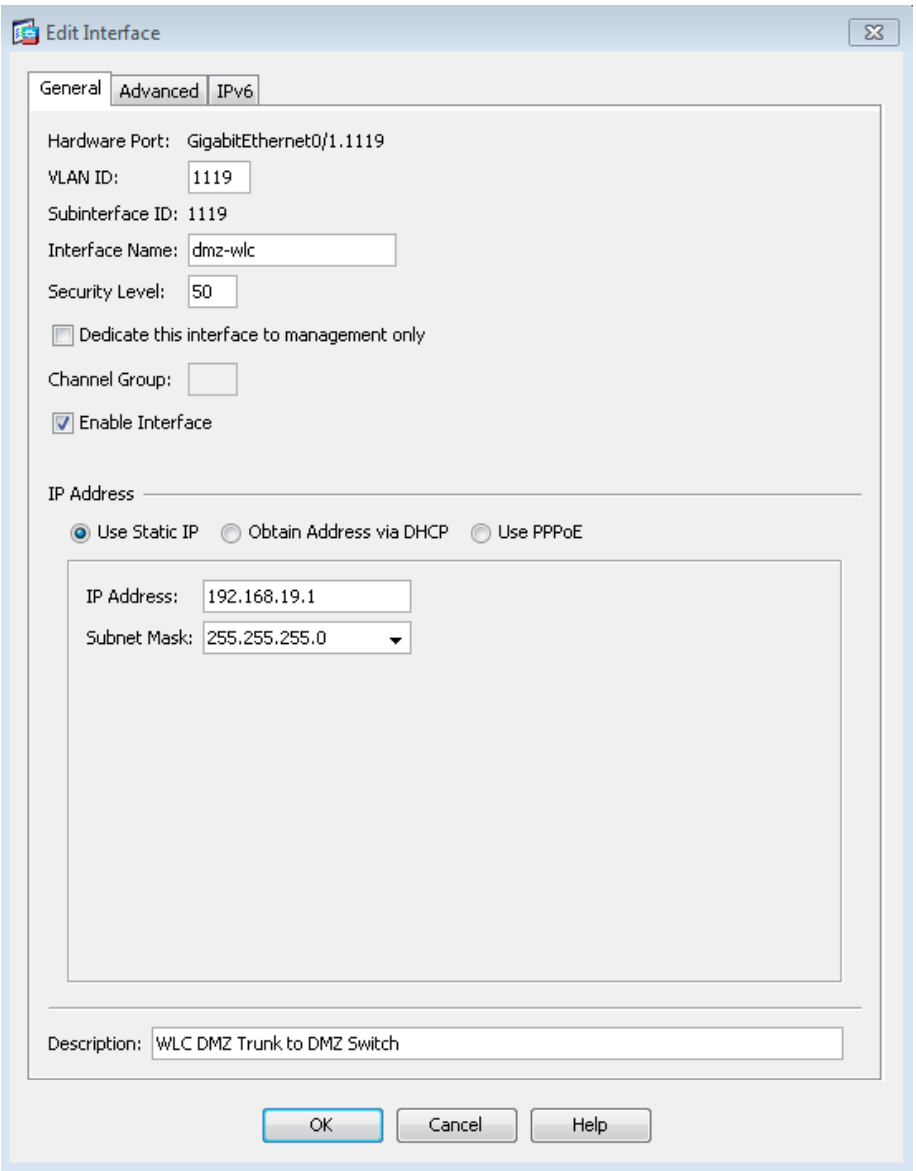
Step 8: In the **Subinterface ID** box, enter the VLAN number for the DMZ VLAN. (Example: 1119)

Step 9: Enter an **Interface Name**. (Example: dmz-wlc)

Step 10: In the **Security Level** box, enter a value of **50**.

Step 11: Enter the interface **IP Address**. (Example: 192.168.19.1)

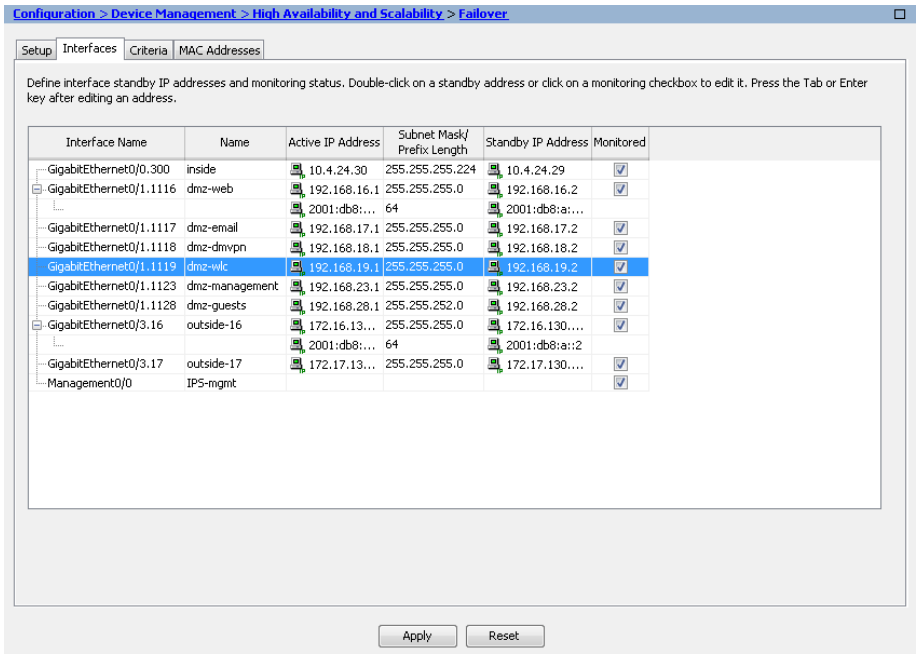
Step 12: Enter the interface **Subnet Mask**, and then click **OK**. (Example: 255.255.255.0)



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

Step 17: Repeat Step 5 through Step 12 for the dmz-guests interface.

Procedure 3 Configure Network Address Translation

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

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

Step 2: Click **Add > Network Object**.

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

Step 4: In the **Type** list, choose **Network**.

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

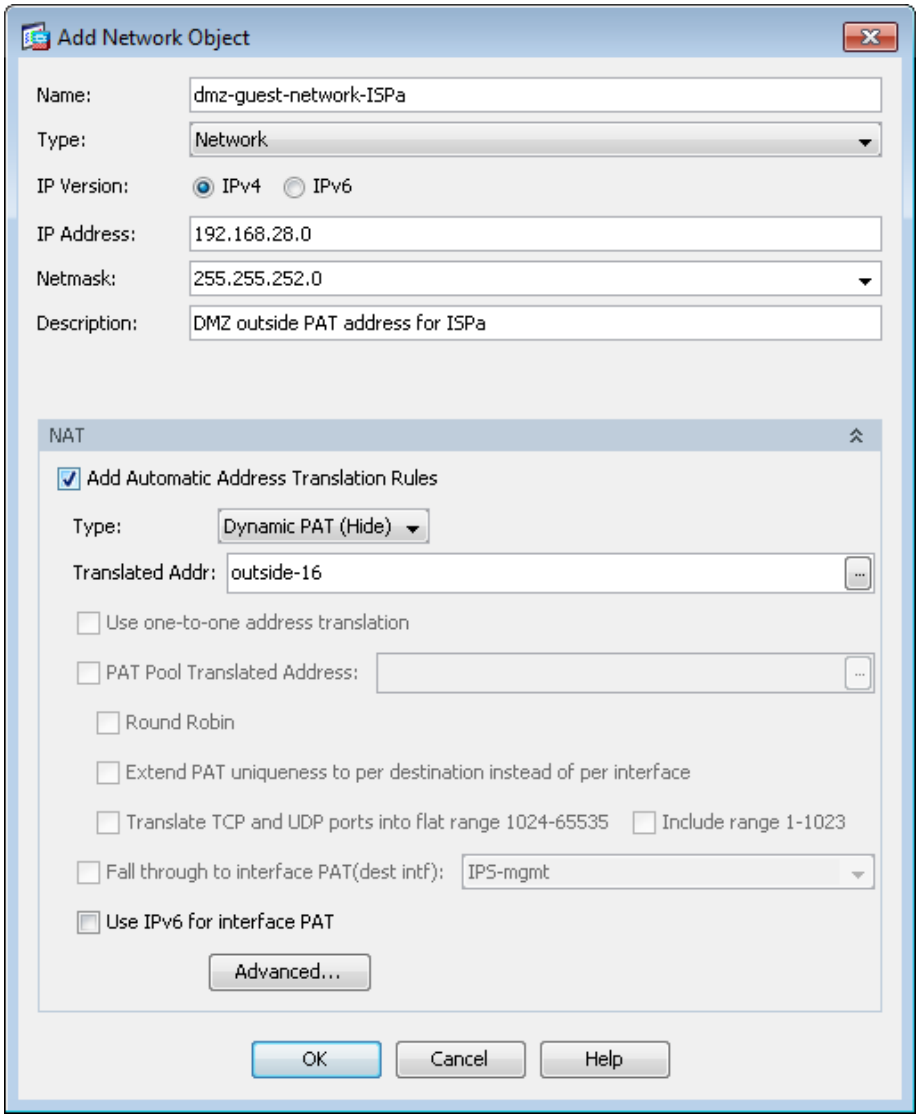
Step 6: Enter the guest DMZ netmask. (Example: 255.255.252.0)

Step 7: Click the two down arrows. The NAT pane expands.

Step 8: Select **Add Automatic Address Translation Rules**.

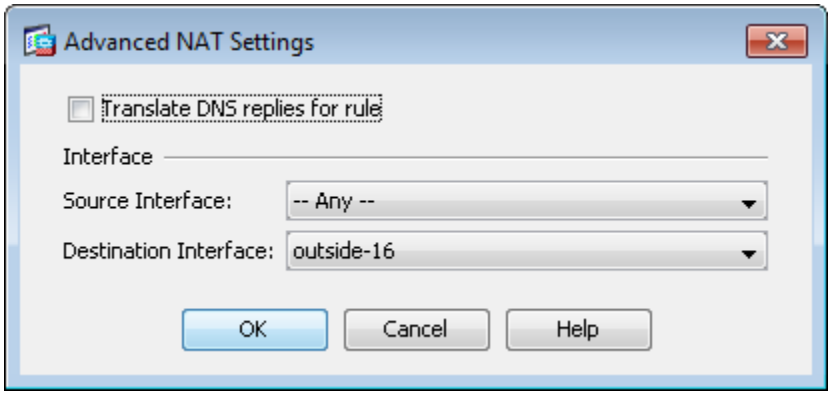
Step 9: In the **Type** list, choose **Dynamic PAT (Hide)**.

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



Step 11: Click **Advanced**.

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



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

Procedure 4 Create network objects

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

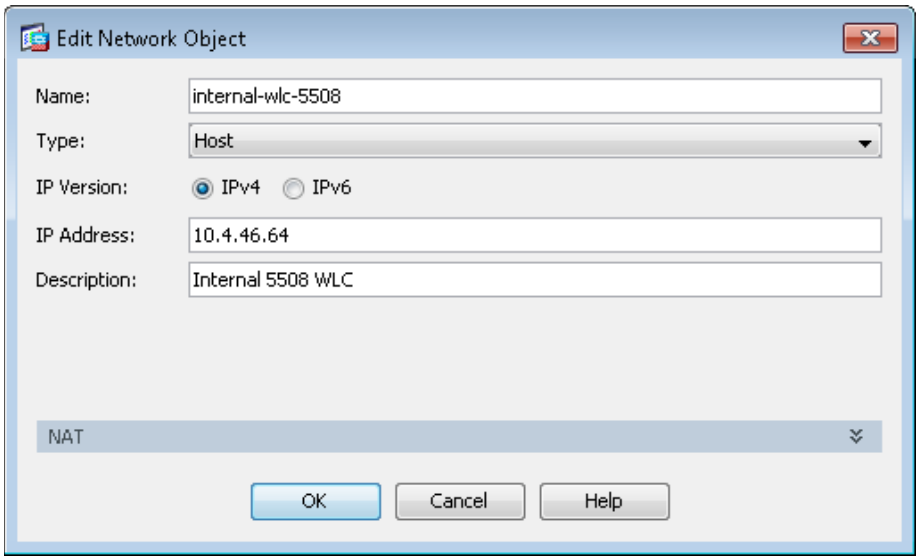
First, add a network object for the every internal WLC in your organization.

Step 2: Click **Add > Network Object**.

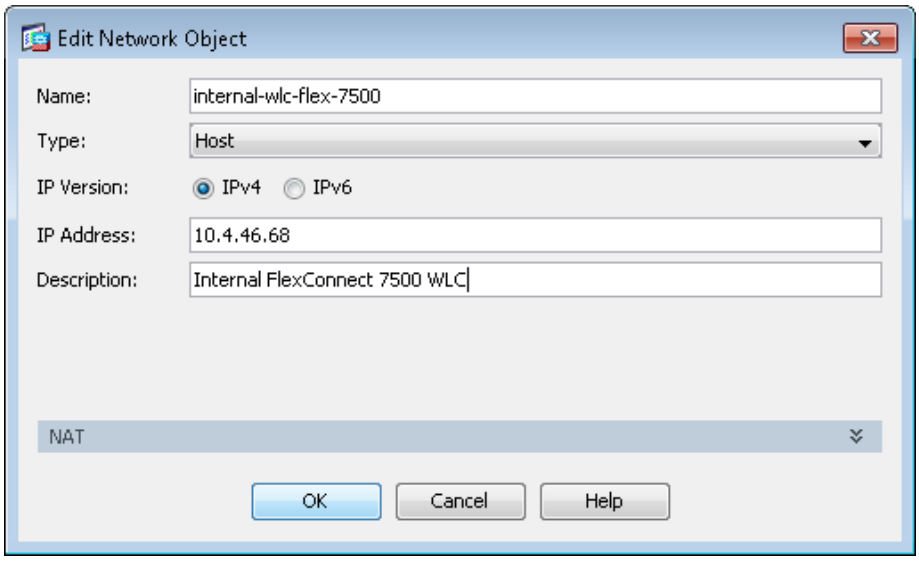
Step 3: On the Add Network Object dialog box, in the **Name** box, enter a description of the WLC. (Examples: internal-wlc-5508, internal-wlc-flex-7500)

Step 4: In the **Type** list, choose **Host**.

Step 5: In the **IP Address** box, enter the WLC's management interface IP address, and then click **OK**. (Example: 10.4.46.64, 10.4.46.68)



Step 6: Repeat Step 2 through Step 5 for every WLC inside your organization.

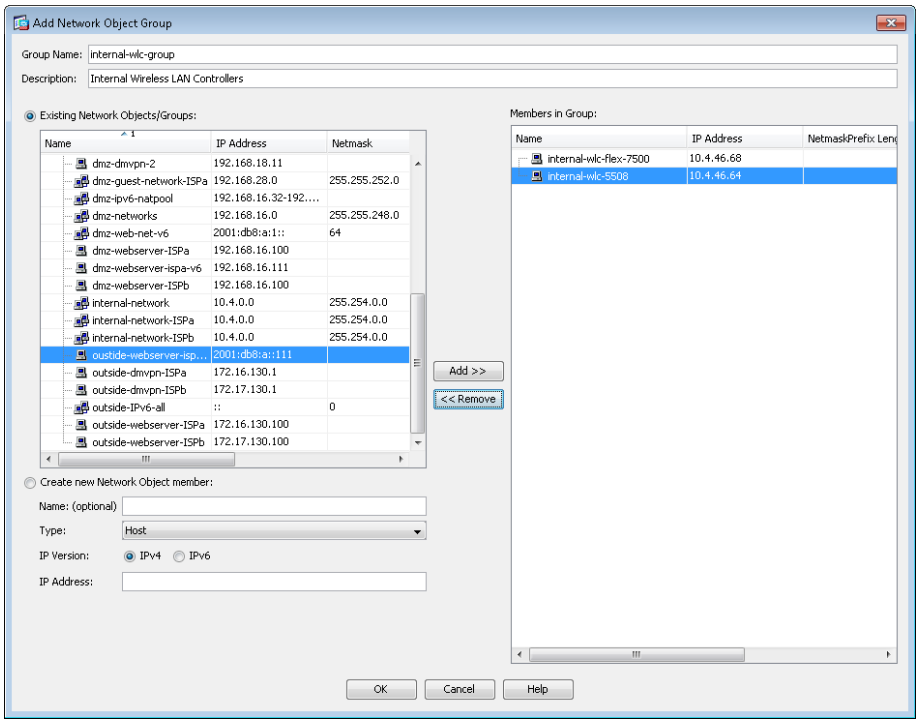


Next, to simplify security policy configuration, you create a network object group that contains every WLC inside your organization.

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

Step 8: In the Add Network Object Group dialog box, in the **Group Name** box, enter a name for the group. (Example: internal-wlc-group)

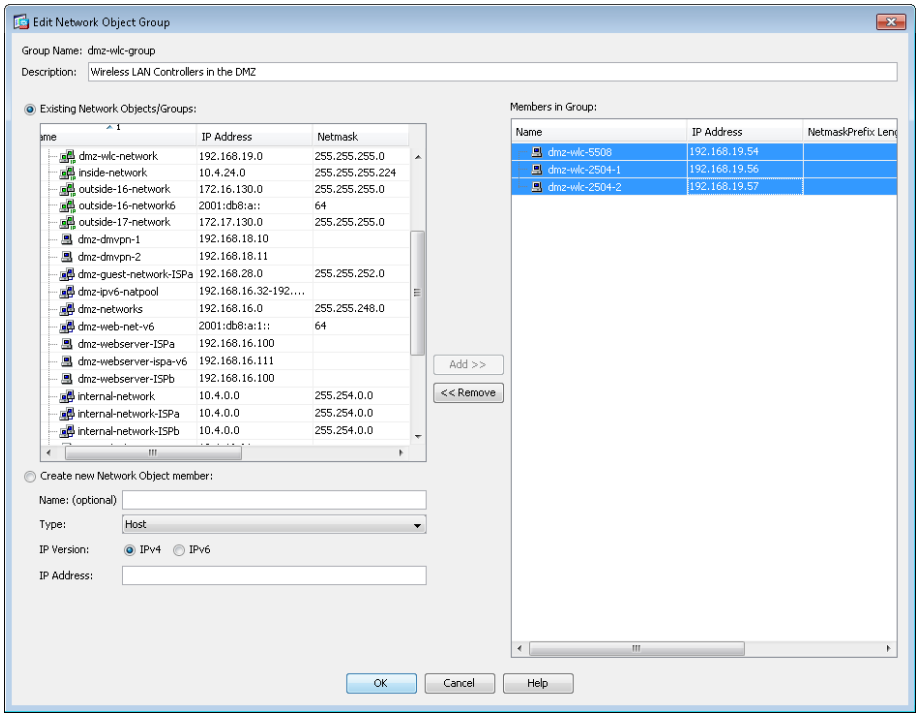
Step 9: In the Existing Network Objects/Groups pane, select every internal WLC, click **Add**, and then click **OK**.



Next, you create a network object group that contains the private DMZ address of every WLC in the DMZ. (Example: 192.168.19.54)

Step 10: Click **Add > Network Object Group**.

Step 11: In the Add Network Object Group dialog box, in the **Group Name** box, enter a name for the group. (Example: dmz-wlc-group)



Step 12: In the Existing Network Objects/Groups pane, choose the primary WLC, and then click **Add**. (Example: 192.168.19.54). If you are using the 5508 as the anchor controller, only the IP address of the primary WLC needs to be configured because this WLC model supports AP-SSO and the redundant pair uses a single IP address.

Step 13: If using a 2504 as a guest anchor controller, both the primary and resilient WLC IP addresses are necessary because this WLC does not support AP-SSO. In the Existing Network Objects/Groups pane, choose the resilient WLC, click **Add**, and then click **OK**. (Example: 192.168.19.56). You will also add the IP address of the secondary WLC's (Example: 192.168.19.57)

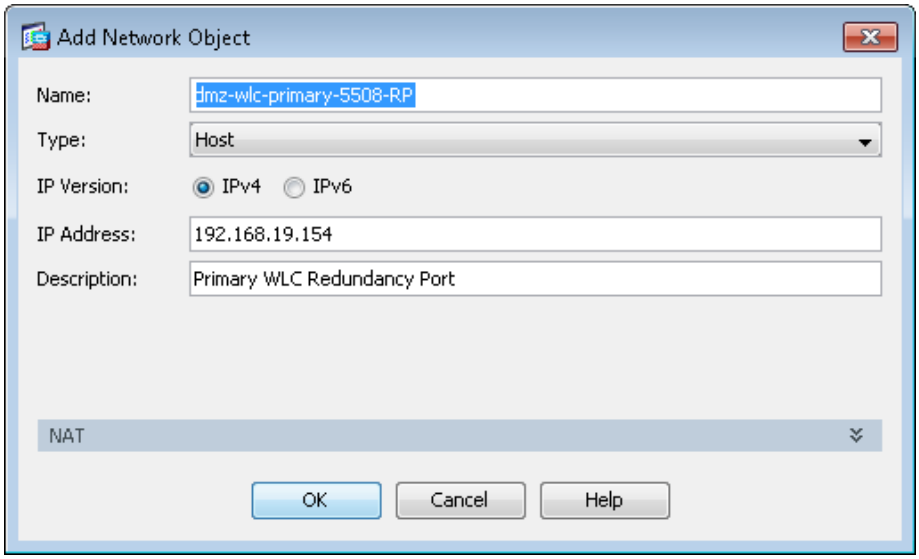
When in standby mode and using AP-SSO, the resilient Wireless LAN Controller uses the redundancy port to communicate with the NTP server. Since either of the WLCs in AP-SSO mode could be in standby, we need to create a network object that is used to identify each of the redundancy ports.

Step 14: Create a Network Object for each of the WLCs in the DMZ (Example: 192.168.19.54) by clicking **Add > Network Object**.

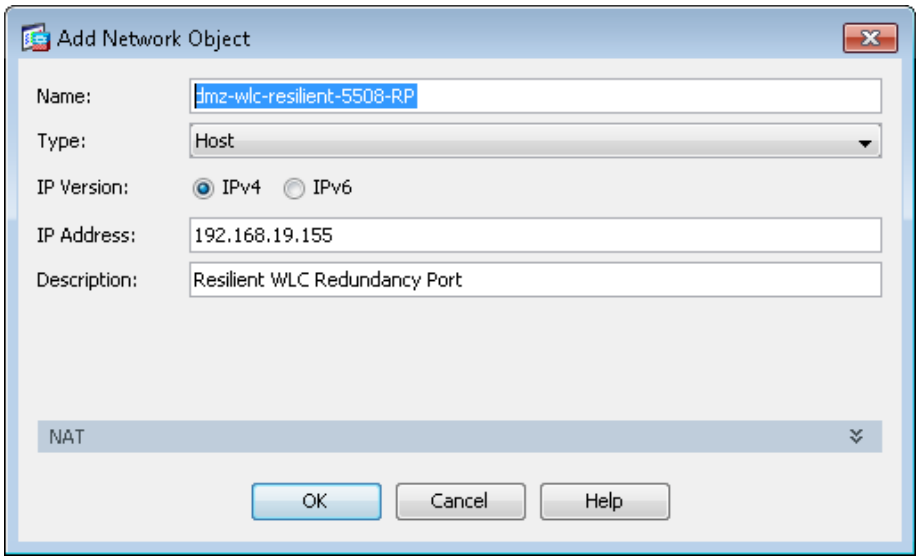
Step 15: In the Add Network Object dialog box, in the **Name** box, enter a description of the WLC. (Example: dmz-wlc-primary-5508-RP)

Step 16: In the Type list, choose **Host**.

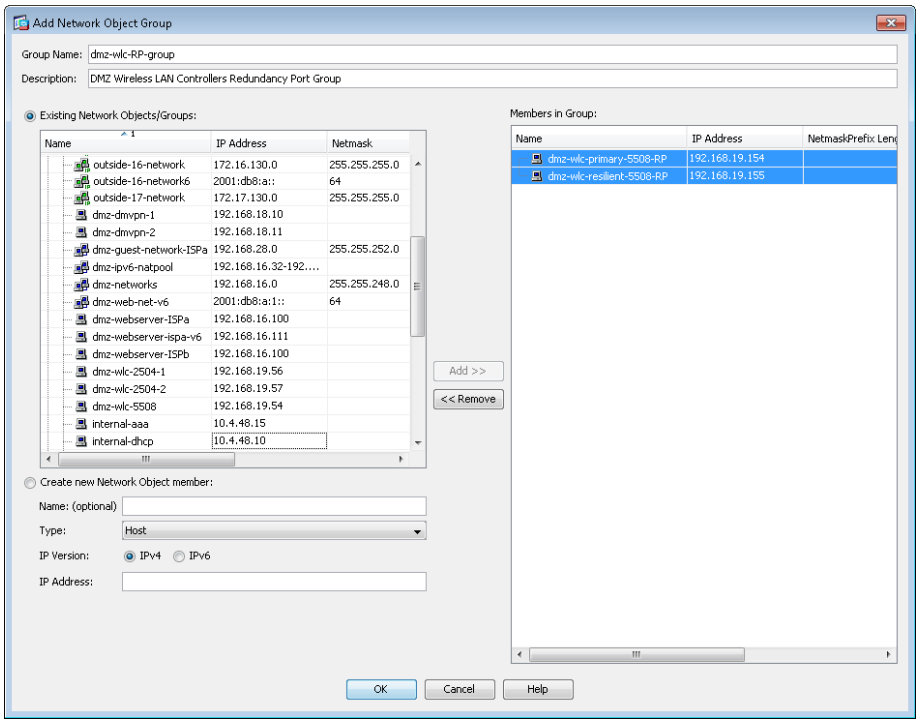
Step 17: In the **IP Address** box, enter the primary WLC's redundancy-port interface IP address, and then click **OK**. (Example: 192.168.19.154)



Step 18: Repeat the steps in Procedure 4for the resilient controller's redundancy port. (Example 192.168.19.155)



Step 19: Create a Network Object Group to group the two redundancy ports on the WLCs.

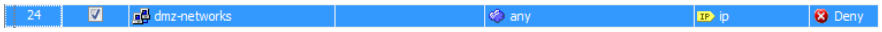


Step 20: In the Add Network Object Group dialog box, click **OK**.

Procedure 5 Configure WLC security policy

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

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



Next, you insert a new rule above the rule you selected that enables the WLCs in the DMZ to communicate with the AAA server in the data center for management and user authentication.

Step 3: Click **Add > Insert**.

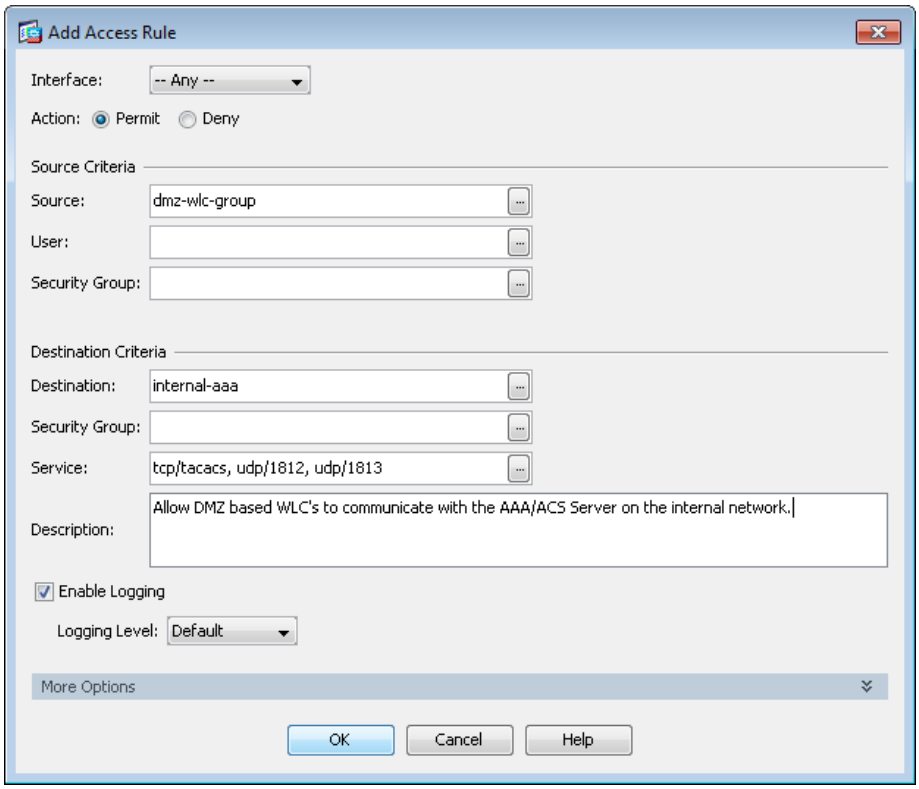
Step 4: In the Insert Access Rule dialog box, in the **Interface** list, choose **Any**.

Step 5: To the right of Action, select **Permit**.

Step 6: In the **Source** list, choose the network object group created in Step 8, "Create network objects." (Example: wlc-group)

Step 7: In the **Destination** list, choose the network object for the Cisco Secure ACS server with AAA services. (Example: internal-aaa)

Step 8: In the **Service** list, enter **tcp/tacacs, udp/1812, udp/1813**, and then click **OK**.



Next, you must allow the WLCs in the DMZ to synchronize their time with the NTP server in the data center.

Step 9: Click **Add > Insert**.

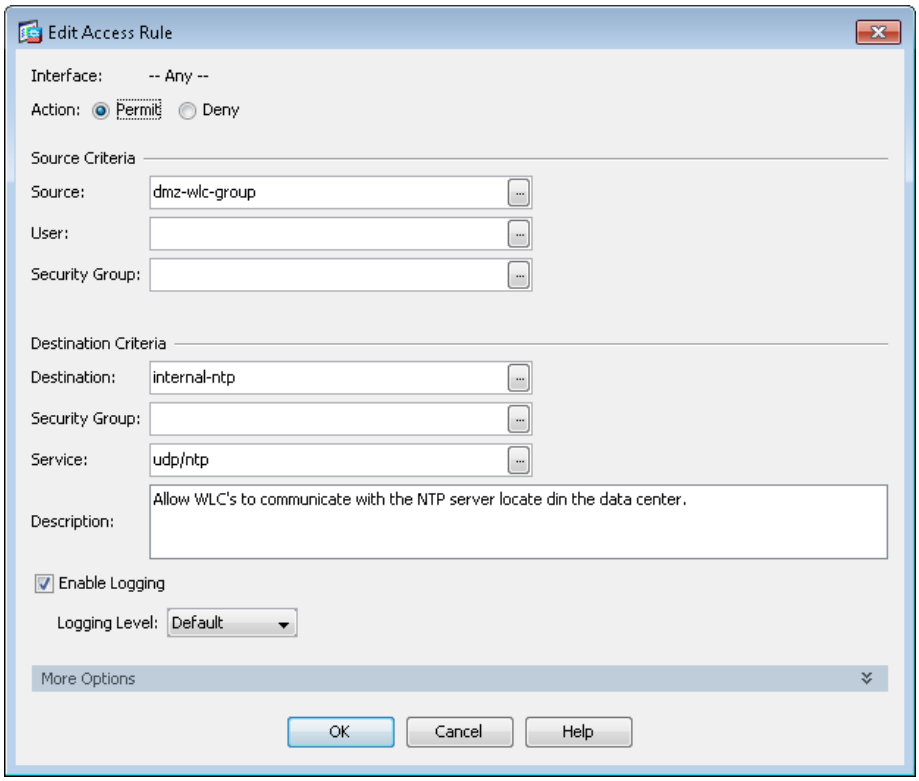
Step 10: In the Internet Access Rule dialog box, in the **Interface** list, choose **Any**.

Step 11: To the right of Action, select **Permit**.

Step 12: In the **Source** list, choose the network object group created in Step 11 of Step 13, "Create network objects." (Example: dmz-wlc-group)

Step 13: In the **Destination** list, choose the network object for the NTP server. (Example: internal-ntp)

Step 14: In the **Service** list, enter **udp/ntp**, and then click **OK**.



Next, you allow the WLCs in the DMZ to be able to download new software via FTP.

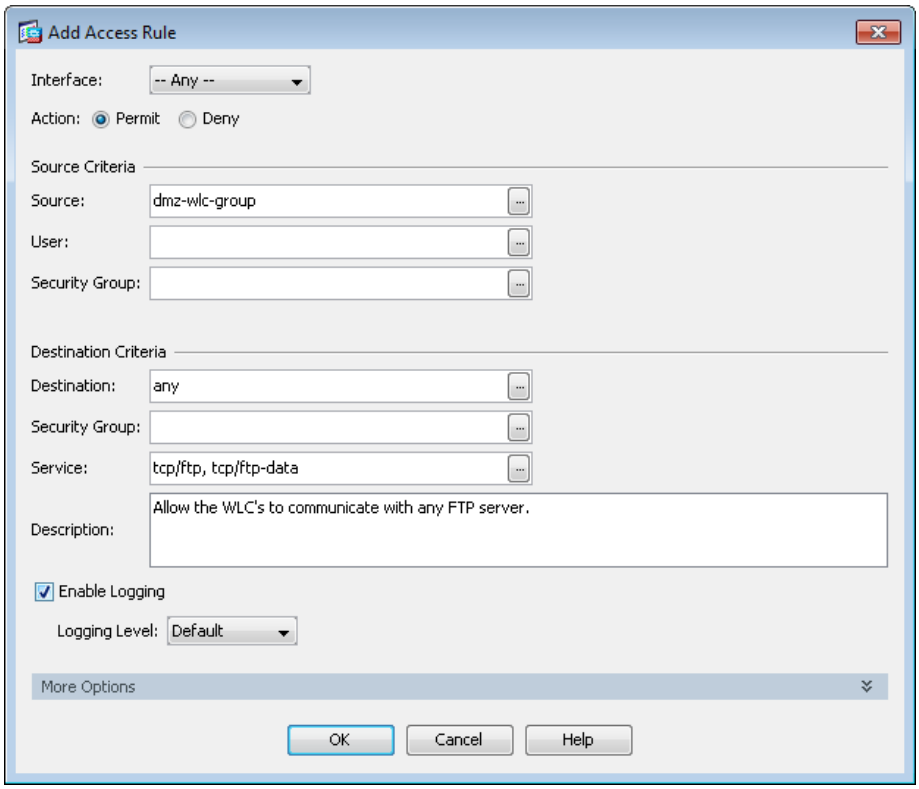
Step 15: Click **Add > Insert**.

Step 16: In the Internet Access Rule dialog box, in the **Interface** list, choose **Any**.

Step 17: To the right of Action, select **Permit**.

Step 18: In the **Source** list, choose the network object group created in Step 11 of Step 13, "Create network objects." (Example: dmz-wlc-group)

Step 19: In the **Service** list, enter **tcp/ftp, tcp/ftp-data**, and then click **OK**.



Next, you enable the DMZ guest WLC to communicate with the WLCs inside the organization.

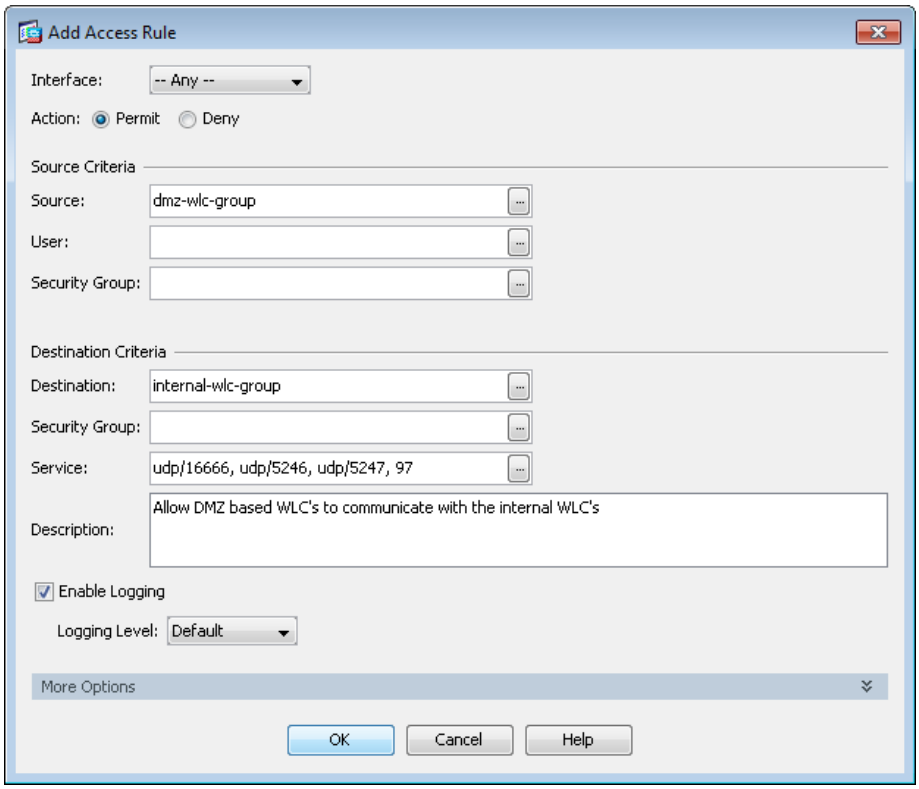
Step 20: Click **Add > Insert**.

Step 21: In the **Interface** list, choose **Any**.

Step 22: In the **Source** list, choose the network object group created in Step 11 of Step 13, "Create network objects." (Example: dmz-wlc-group)

Step 23: In the **Destination** list, choose the network object group created in Step 8 of Step 13, "Create network objects." (Example: internal-wlc-group)

Step 24: In the **Service** list, enter **udp/16666, udp/5246, udp/5247, 97**, and then click **OK**.



Next, you enable the guest WLC to communicate with the DHCP server inside your organization.

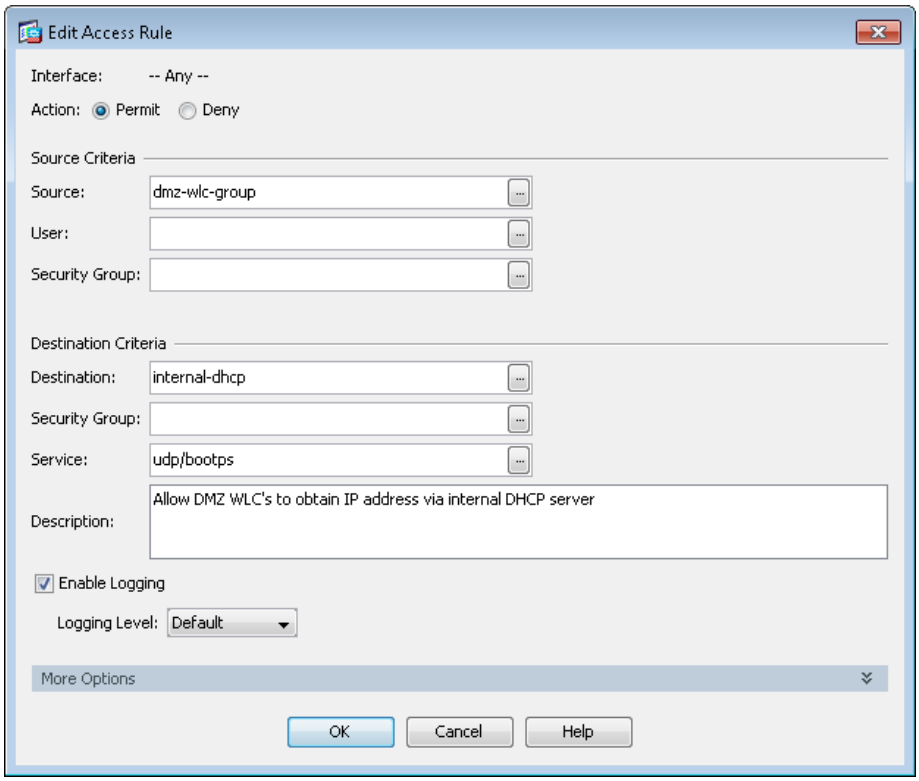
Step 25: Click **Add > Insert**.

Step 26: In the **Interface** list, choose **Any**.

Step 27: In the **Source** list, choose the network object group created in Step 11 of Step 13, "Create network objects." (Example: dmz-wlc-group)

Step 28: In the **Destination** list, choose the network object group for the internal DHCP server. (Example: internal-dhcp)

Step 29: In the **Service** list, enter **udp/bootps**, click **OK**, and then click **Apply**.



Finally, enable the guest WLC configured for AP-SSO (5500 series) in order to communicate with the internal NTP server using its redundancy port.

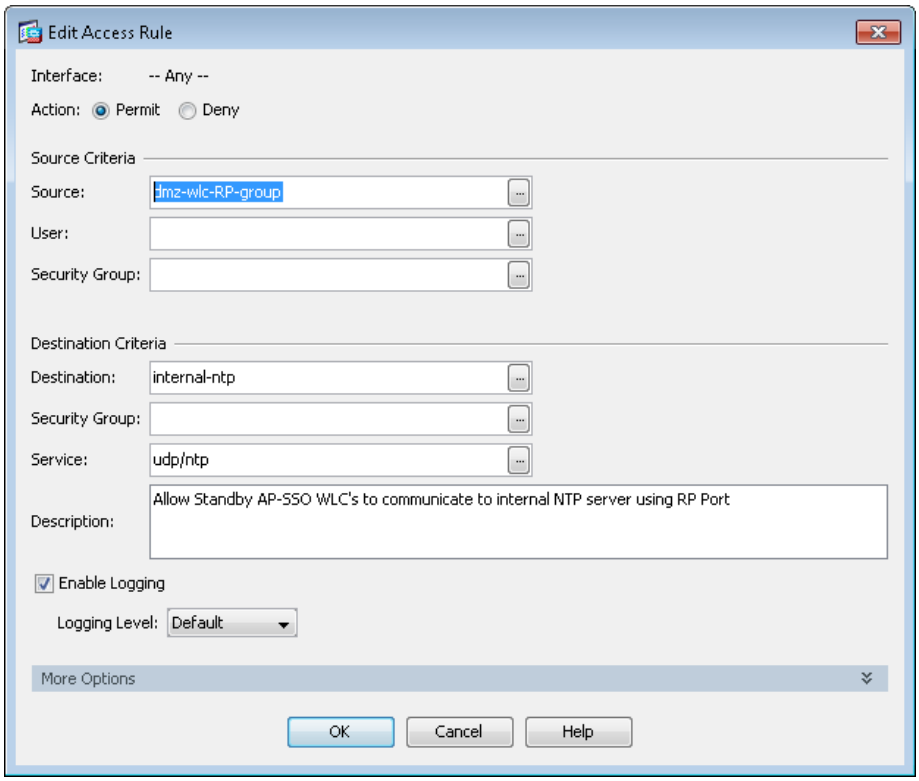
Step 30: Click **Add > Insert**.

Step 31: In the Interface list, choose **Any.**

Step 32: In the Source list, choose network group that was created for the WLC RP ports (Example: dmz-wlc-RP-group)

Step 33: In the Destination list, choose the network object group for the internal NTP server. (Example: internal-ntp)

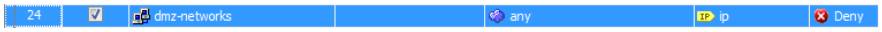
Step 34: In the Service list, enter **udp/ntp**, click **OK**, and then click **Apply**.



Procedure 6 Configure guest network security policy

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

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



First, you configure an access rule in the firewall in order to enable the guest wireless users to communicate with the internal DNS and DHCP servers in the data center.

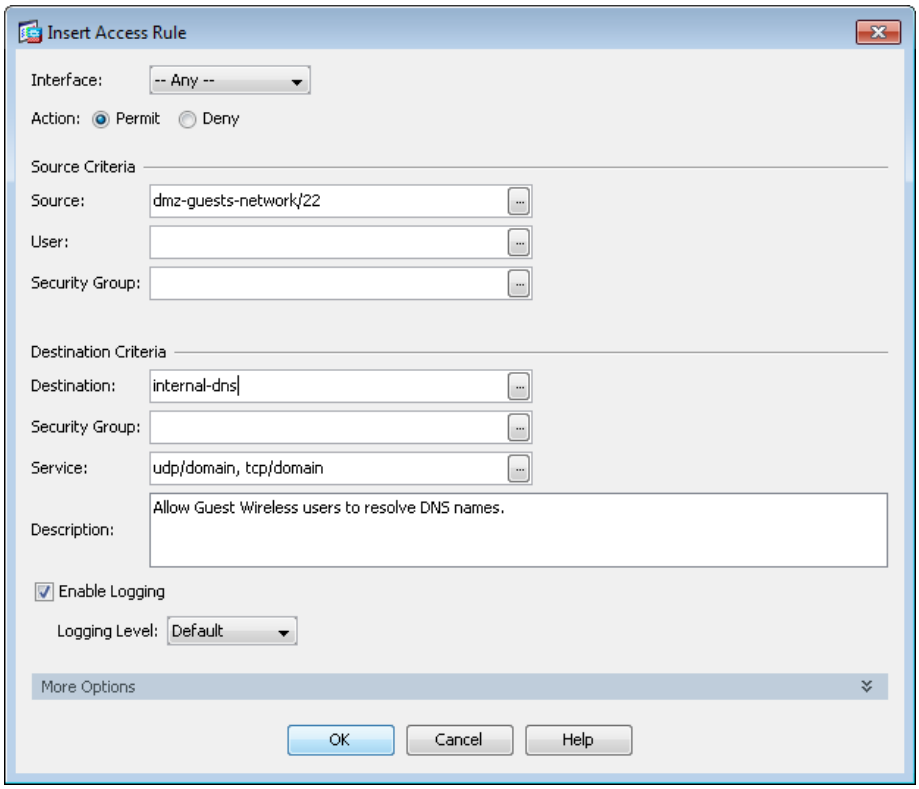
Step 3: Click **Add > Insert**.

Step 4: In the **Interface** list, choose **Any**.

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

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

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



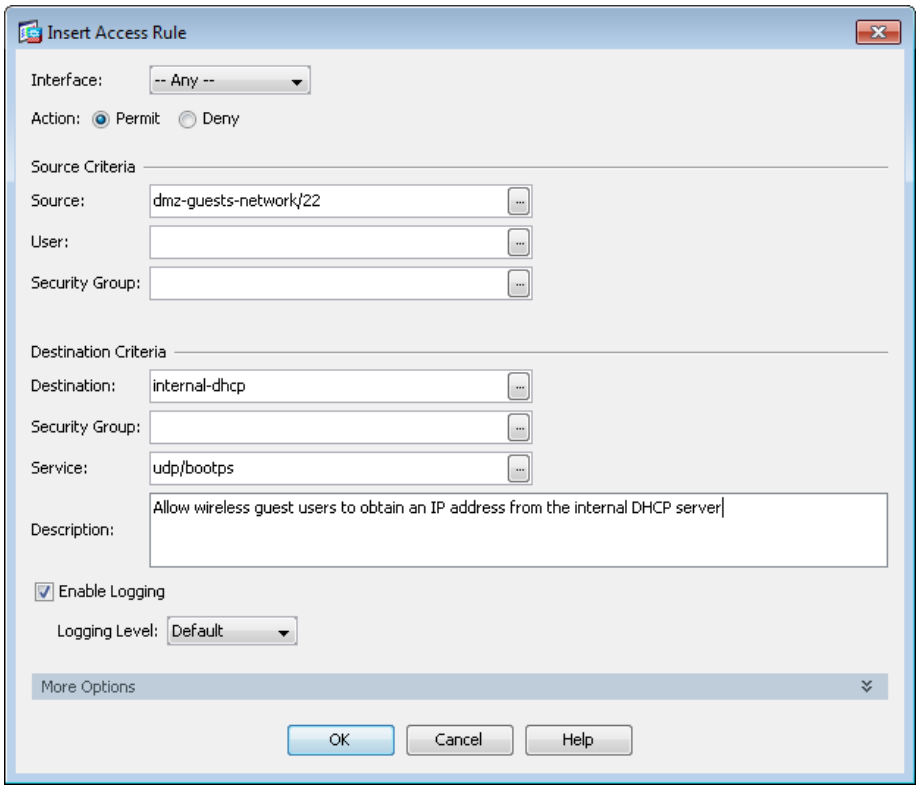
Step 8: Click **Add > Insert**.

Step 9: In the **Interface** list, choose **Any**.

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

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

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



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

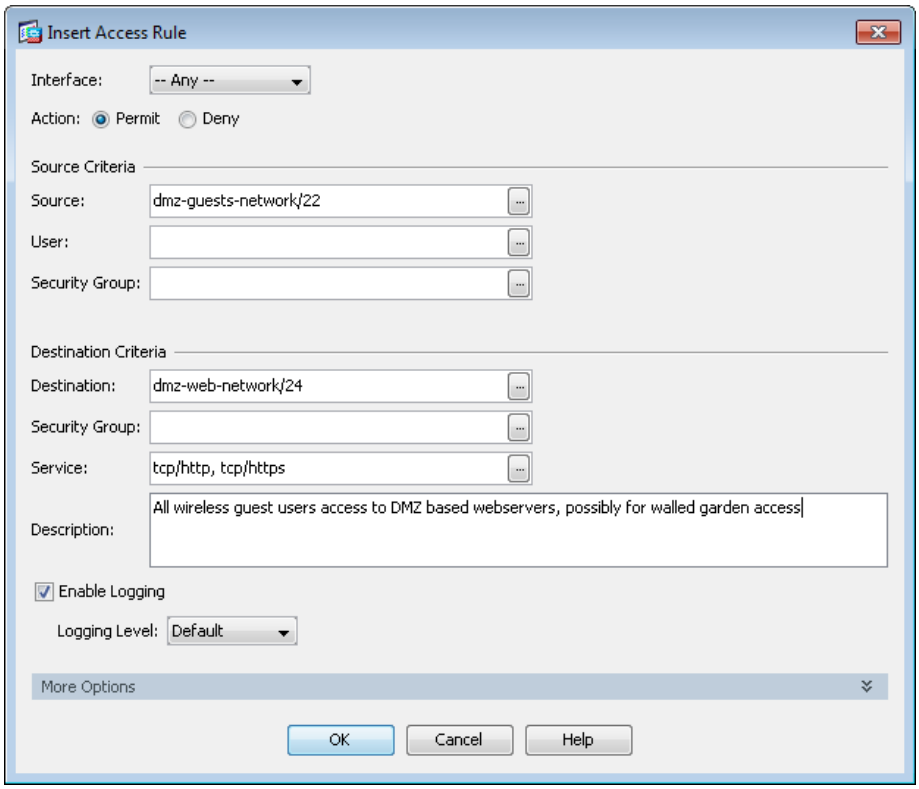
Step 13: Click **Add > Insert**.

Step 14: In the **Interface** list, choose **Any**.

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

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

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



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

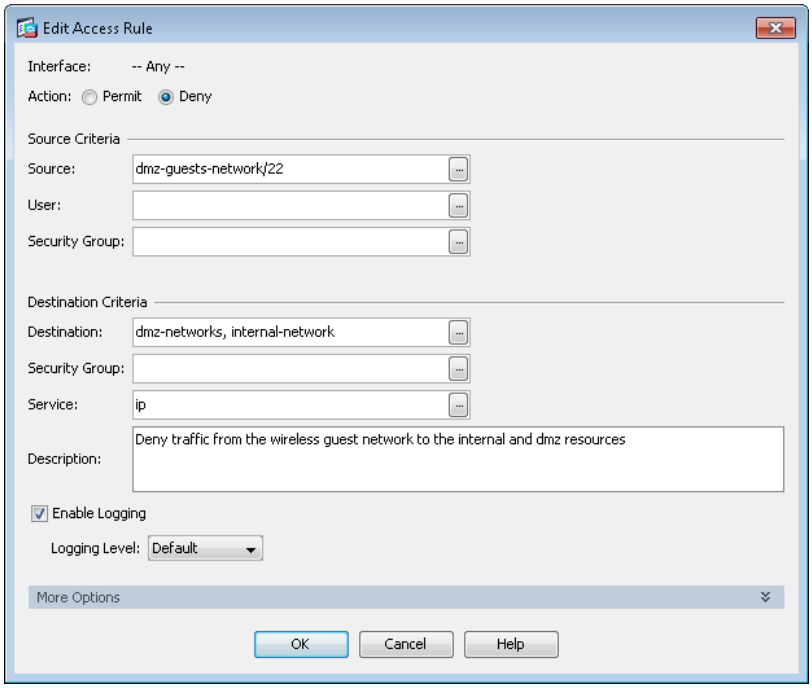
Step 18: Click **Add > Insert**.

Step 19: In the **Interface** list, choose **Any**.

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

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

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

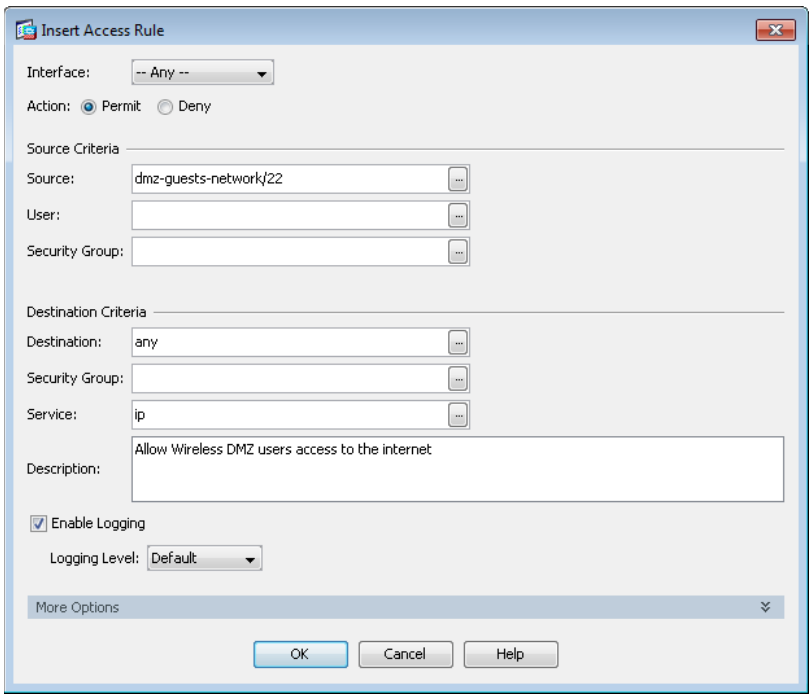


Next, you enable the guests to communicate with the Internet.

Step 23: Click **Add > Insert**.

Step 24: In the **Interface** list, choose **Any**.

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



Procedure 7 Configure the DMZ WLC

Configure the DMZ wireless LAN controller by using the following values.

Table 9 - Cisco DMZ wireless controller parameters checklist

Parameter	CVD values primary controller	CVD values resilient controller not using AP SSO	Site-specific values
Controller parameters			
Switch interface number	1/0/13, 2/0/13	1/0/14, 2/0/14	
VLAN number	1119	1119	
Time zone	PST -8 0	PST -8 0	
IP address	192.168.19.54/24	192.168.19.55/24[1]	
Default gateway	192.168.19.1	192.168.19.1	
Redundant management IP address (AP SSO)	192.168.19.154	192.168.19.155	
Redundancy port connectivity (AP SSO)	Dedicated Ethernet cable	Dedicated Ethernet cable	
Hostname	DMZ-WLC-Guest-1	DMZ-WLC-Guest-2[2]	
Local administra-tor username and password	admin/C1sco123	admin/C1sco123	
Mobility group name	GUEST	GUEST	
RADIUS server IP address	10.4.48.15	10.4.48.15	
RADIUS shared key	SecretKey	SecretKey	
Management network (optional)	10.4.48.0/24	10.4.48.0/24	
TACACS server IP address (optional)	10.4.48.15	10.4.48.15	
TACACS shared key (optional)	SecretKey	SecretKey	
Wireless data network parameters			
SSID	Wireless-Guest	Wireless-Guest	
VLAN number	1128	1128	
Default gateway	192.168.28.1	192.168.28.1	
Controller interface IP address	192.168.28.5	192.168.28.6[1]	

Notes:

1. If you're using AP SSO high availability, the IP address of the resilient WLC not required, as the secondary controller's management interface is offline until the primary fails. During this time, the IP address of the RP (Example: 192.168.19.155) is used for outbound communication to the NTP server and to monitor the status of its default gateway.
2. If using AP SSO, the resilient standby controller does not have a unique hostname, as it inherits the continuation of its paired primary WLC.

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

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

Step 1: Terminate the autoinstall process.

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

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

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

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 AP 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 intercontroller communication. Enter an IP address that is not used in your organization's network. (Example: 192.0.2.1)

```
Virtual Gateway IP Address: 192.0.2.1
```

Step 9: If configuring a Cisco 2500 Series WLC, enter the multicast IP address for communication of multicast traffic by using the multicast-multicast method. This WLC does not support multicast using the multicast-unicast method.

```
Multicast IP Address: 239.40.40.40
```

Step 10: Enter a name for the default mobility and RF group. (Example: GUEST)

```
Mobility/RF Group Name: GUEST
```

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
```

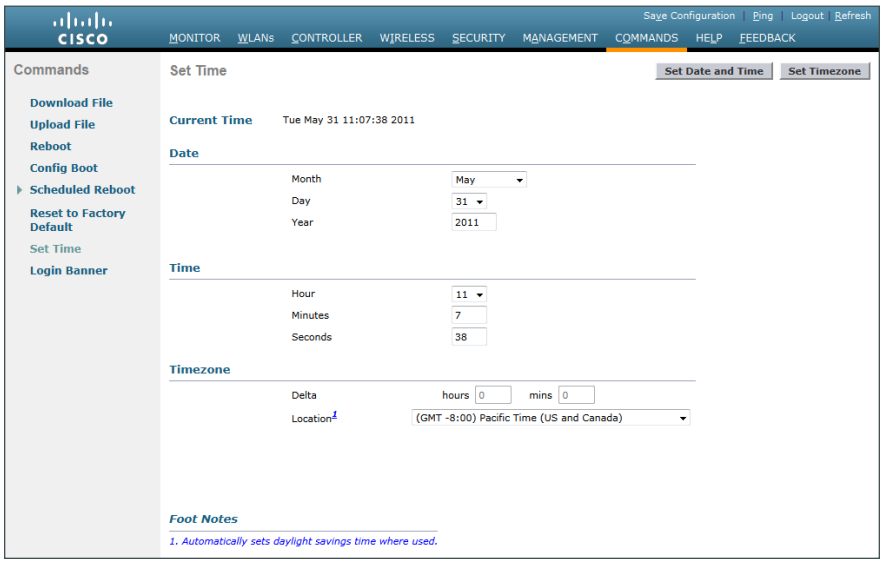
Step 19: After the WLC has reset, log in to the Cisco Wireless LAN Controller Administration page by using the credentials defined in Step 3. (Example: https://dmz-wlc-guest.cisco.local/)

Procedure 8 Configure the time zone

Step 1: Navigate to **Commands > Set Time**.

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

Step 3: Click **Set Timezone**.



Procedure 9 Configure SNMP

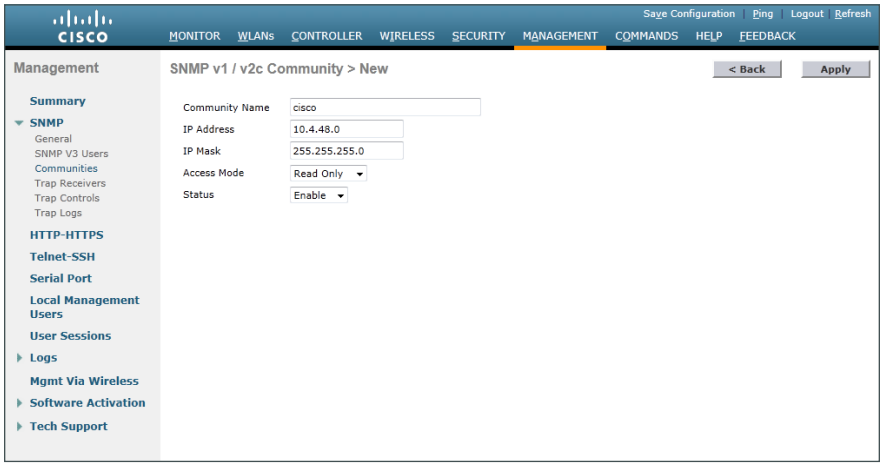
Step 1: In **Management > SNMP > Communities**, click **New**.

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

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

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

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



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

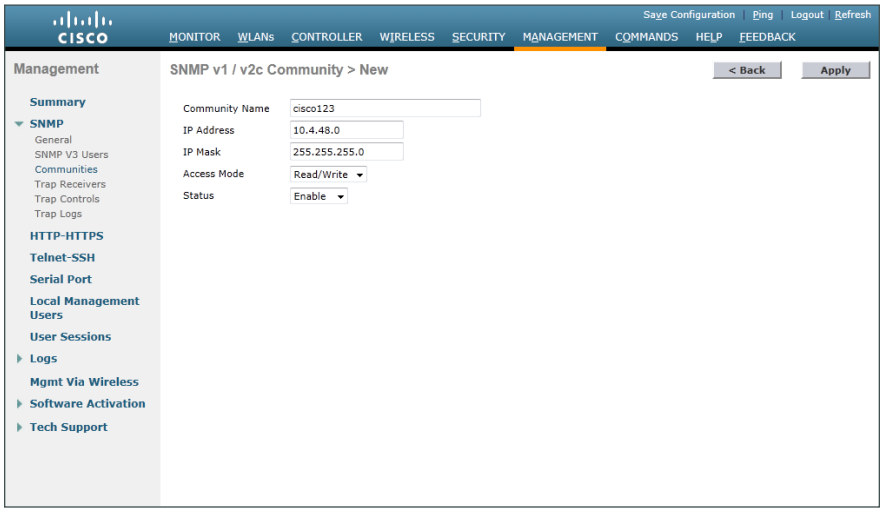
Step 7: Enter the **Community Name**. (Example: cisco123)

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**.

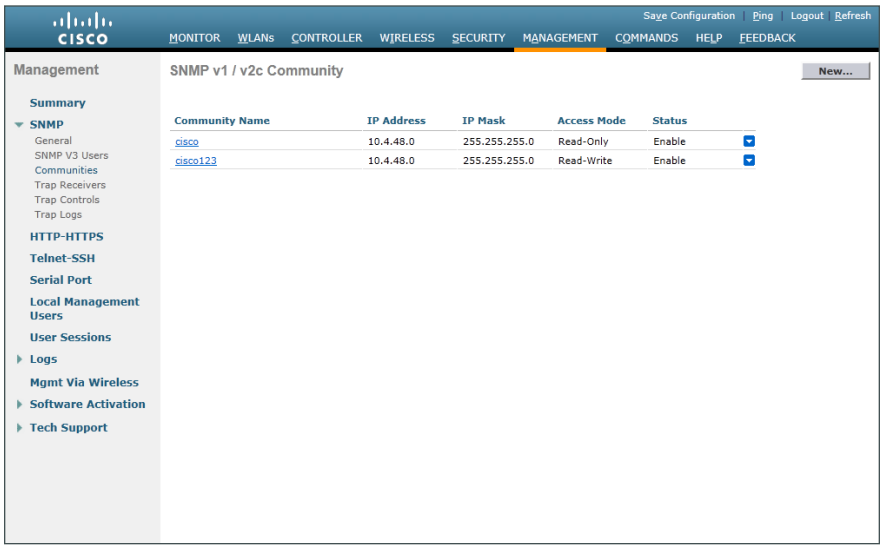


Step 12: Navigate to **Management > SNMP > Communities**.

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.



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 device via SSH or SNMP.

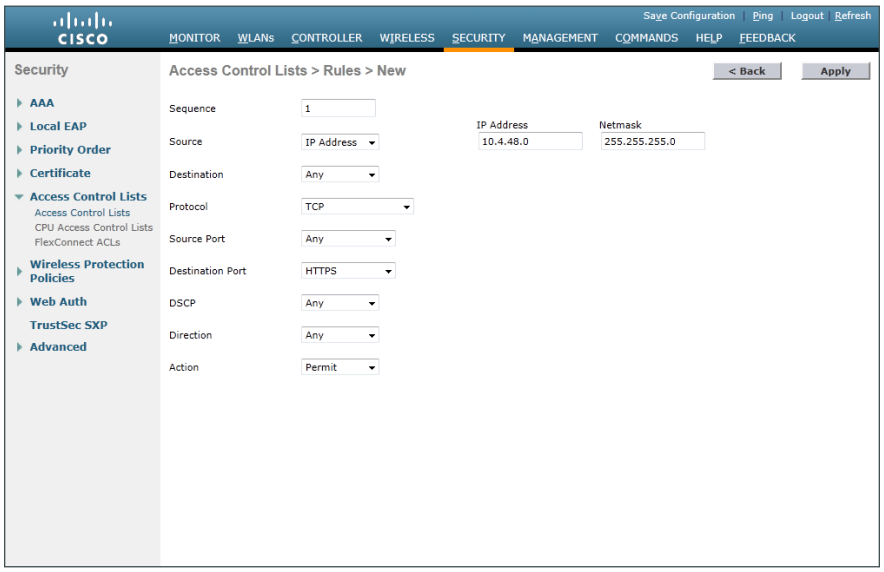
Step 1: In **Security > Access Control Lists > Access Control Lists**, click **New**.

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

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

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

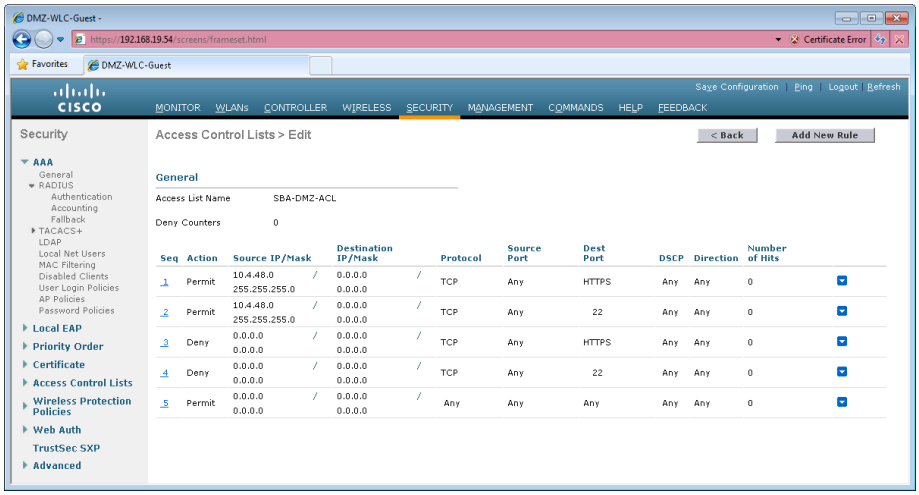
- Sequence–**1**
- Source–**10.4.48.0 / 255.255.255.0**
- Destination–**Any**
- Protocol–**TCP**
- Destination Port–**HTTPS**
- Action–**Permit**



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

Table 10 - Rule configuration values

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



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

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

Procedure 11 Configure management authentication

(Optional)

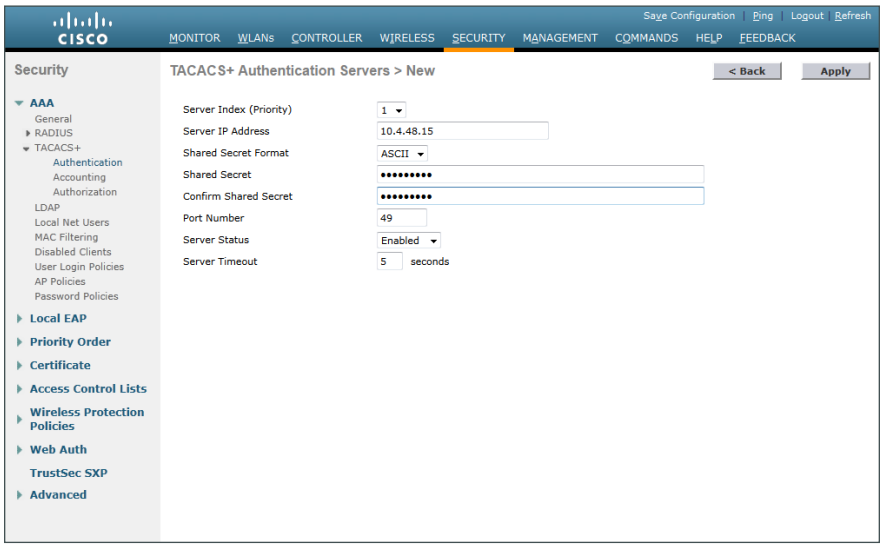
You can use this procedure to deploy centralized management authentication by configuring an authentication, authorization and accounting (AAA) service. If you prefer to use local management authentication, skip to Procedure 12.

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

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

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

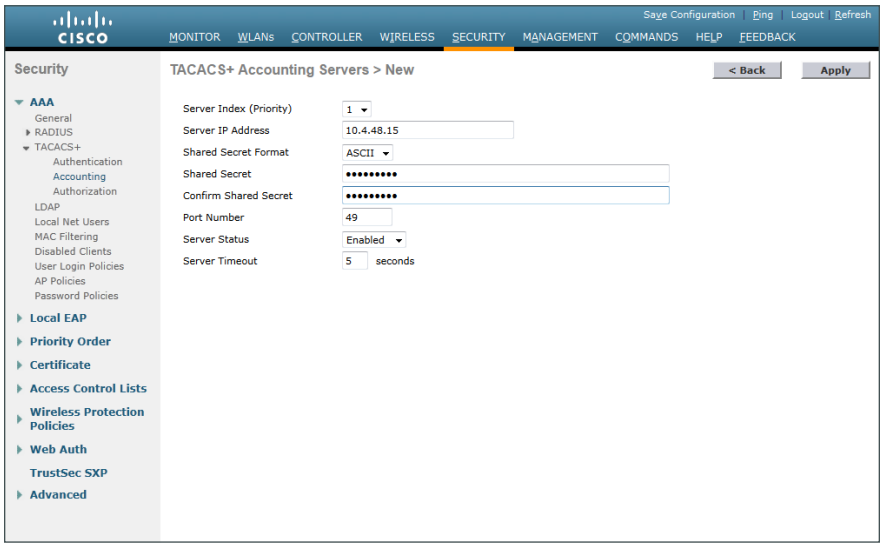
Step 3: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)



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

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

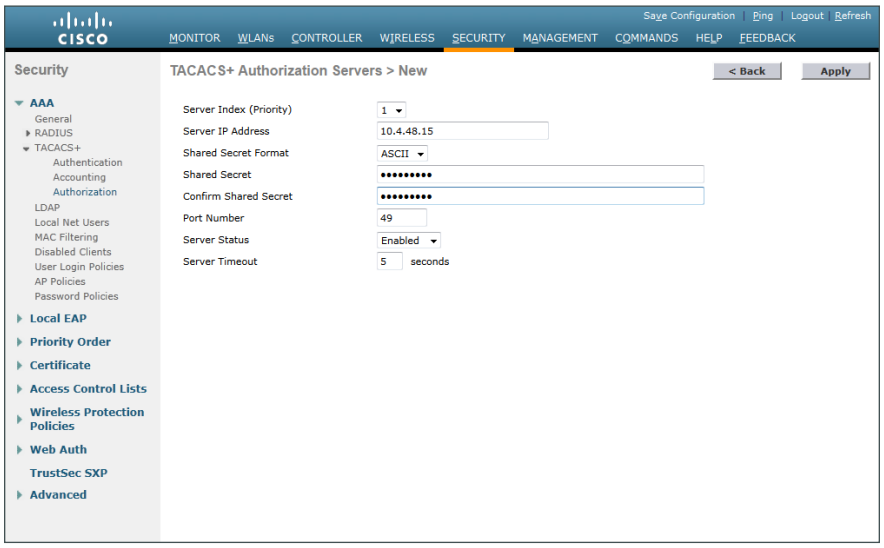
Step 6: Enter and confirm the **Shared Secret**, and then click **Apply**. (Example: SecretKey)



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)

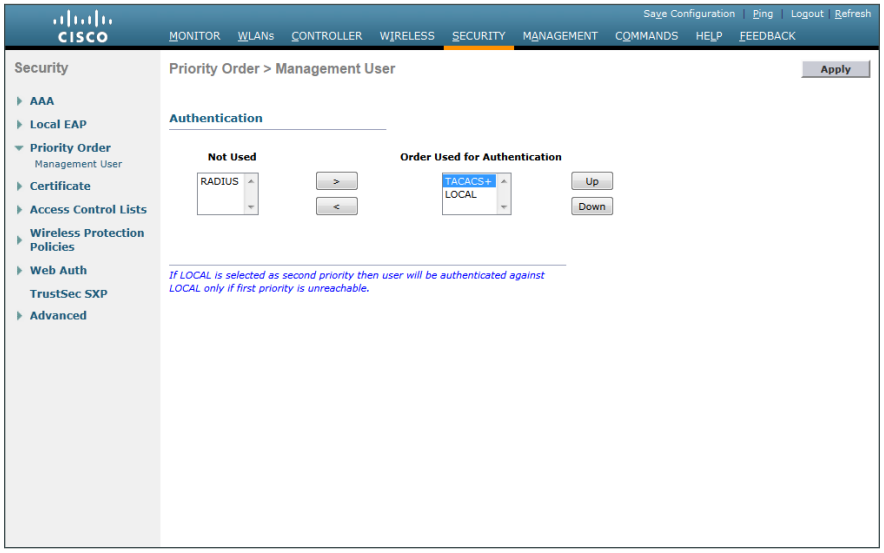


Step 10: Navigate to **Security > Priority Order > Management User**.

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 using Cisco Secure ACS in order to authenticate TACACS management access to the WLC, you must add the WLC as an authorized network access device. Failure to do so will prevent administrative access to the WLC by using the Secure ACS server.

Procedure 12 Create the guest wireless LAN interface

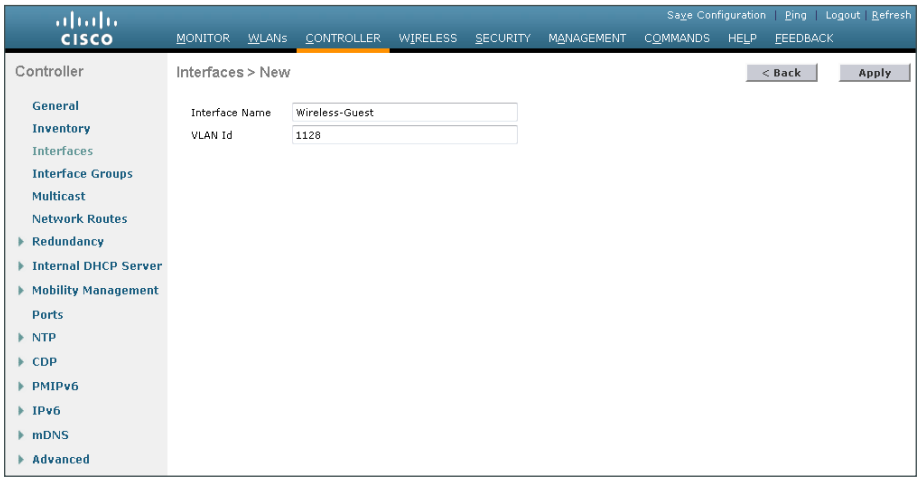
The guest wireless interface is connected to the DMZ of the Cisco ASA 5540 security appliance. This allows guest wireless traffic only to and from the Internet. All guest traffic, regardless of the controller to which the guest initially connects, is tunneled to the guest WLC and leaves the controller on this interface.

To easily identify the guest wireless devices on the network, use an IP address range for these clients that is not part of your organization's regular network. This procedure adds an interface that allows devices on the guest wireless network to communicate with the Internet.

Step 1: In **Controller>Interfaces,** click **New**.

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

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

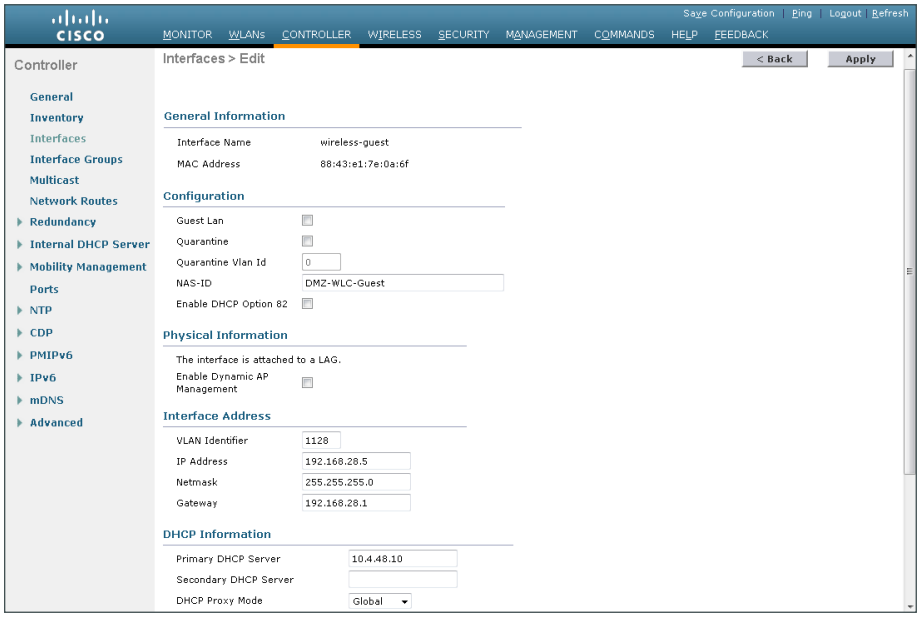


Step 4: In the **IP Address** box, enter the IP address to assign to the WLC interface. (Example: 192.168.28.5)

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.

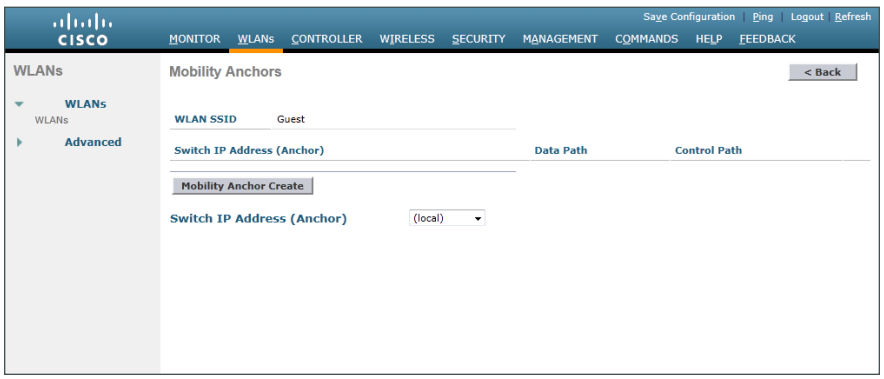
Procedure 13 Configure the guest wireless LAN

Step 1: Navigate to **WLANs**.

Step 2: Hover over the blue list next to your guest WLAN, and then click **Mobility Anchors**.

Step 3: In the **Switch IP Address (Anchor)** list, choose **(local)**.

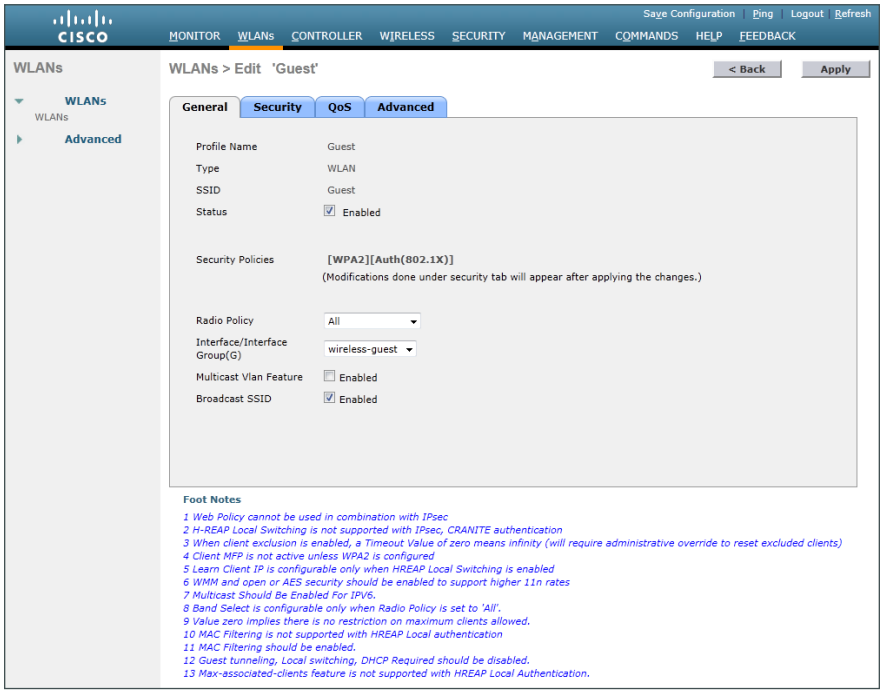
Step 4: Click **Mobility Anchor Create**, and then click **OK**.



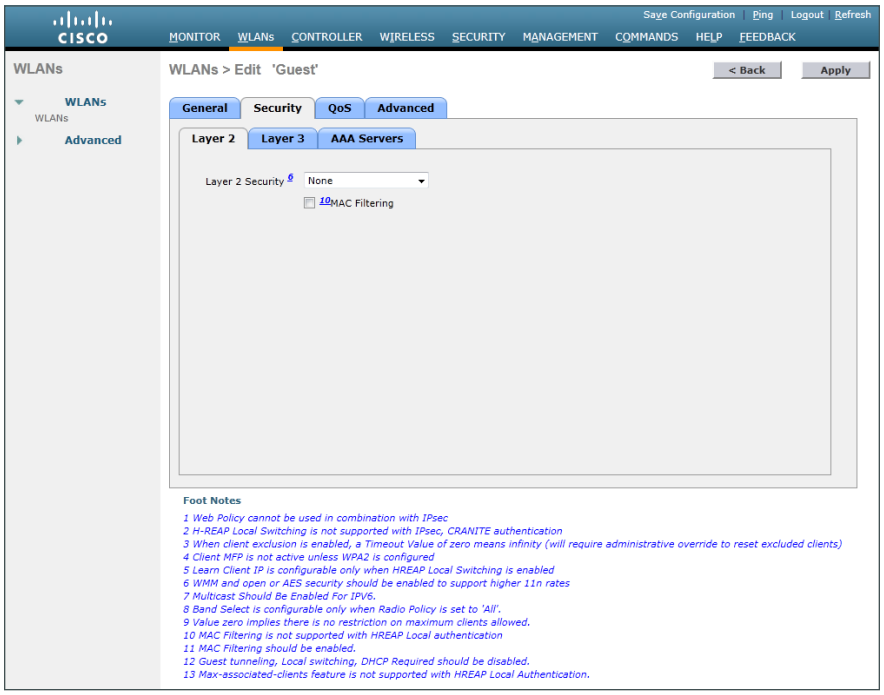
Step 5: Click **Back**.

Step 6: Click the **WLAN ID** of the SSID created in Procedure 7. (Example: Guest)

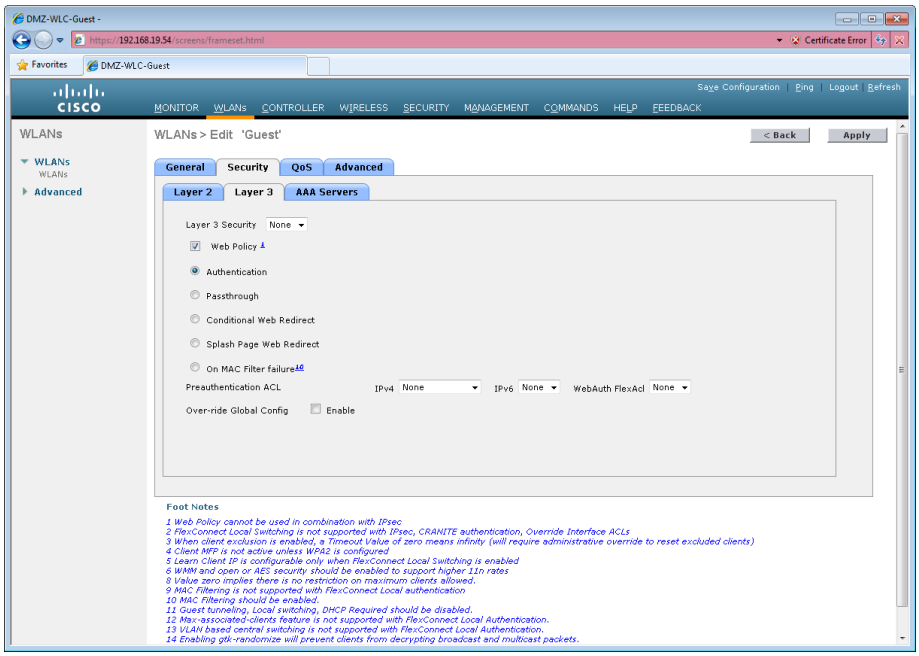
Step 7: On the General tab, in the **Interface/Interface Group(G)** list, choose the interface created in Procedure 12. (Example: wireless-guest)



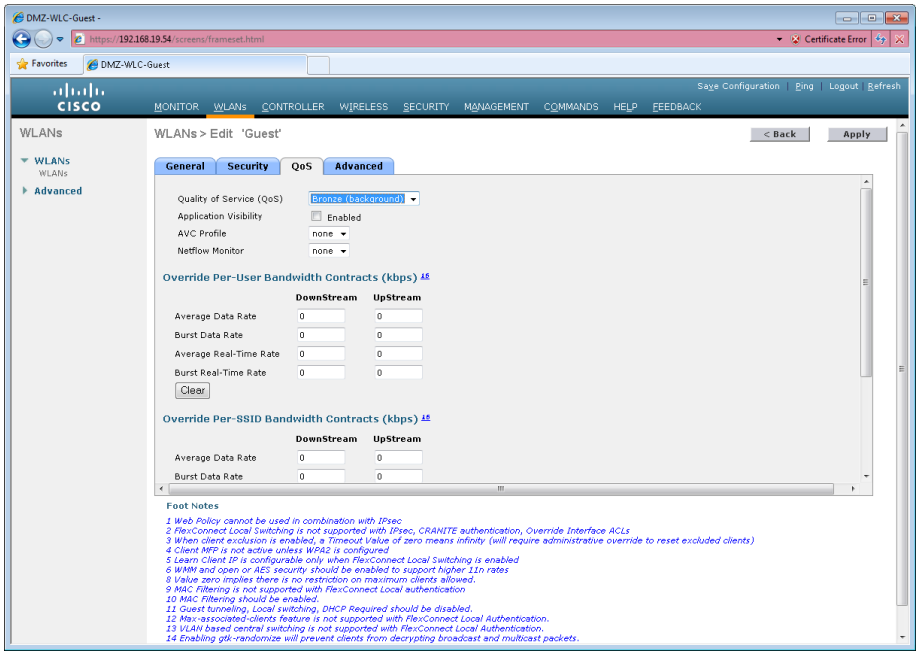
Step 8: Click the **Security** tab, and then on the Layer 2 tab, in the **Layer 2 Security** list, choose **None**.



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



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

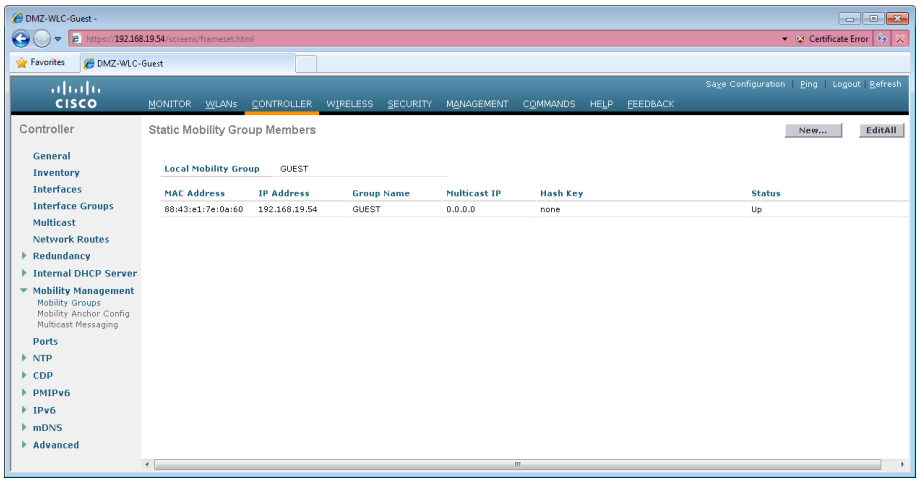


Procedure 14 Configure mobility groups

If you are not using AP-SSO, then you need to add each of the WLCs to the mobility group.

Step 1: On the guest controller, navigate to **Controller > Mobility Management > Mobility Groups**.

Step 2: On the Static Mobility Group Member page, note the MAC address, IP address, and mobility group name for the local controller. You need this information for the following steps.

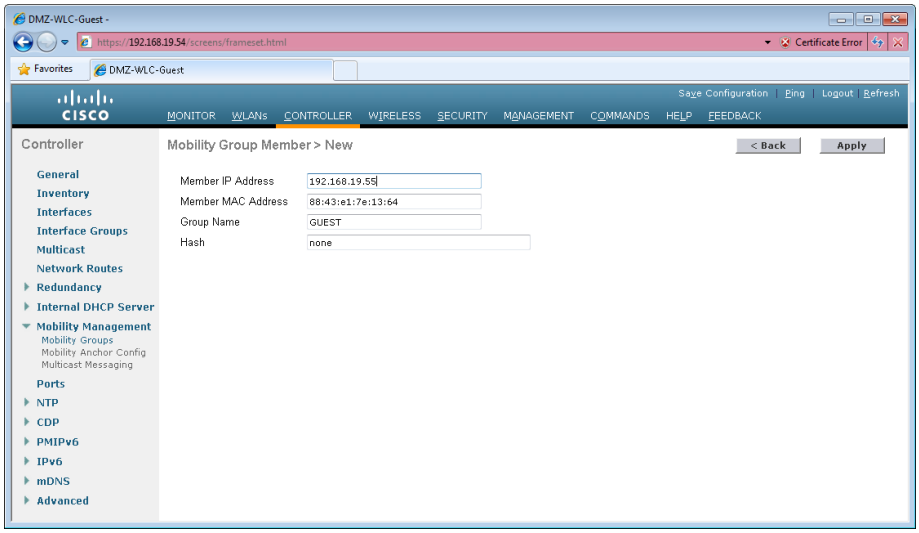


Step 3: On every controller in your organization that is not a resilient WLC and is providing DMZ guest access services, navigate to **Controller > Mobility Management > Mobility Groups**, and then click **New**.

Step 4: In the **Member IP Address** box, enter the IP address of the guest controller. (Example: 192.168.19.54 and/or 192.168.19.55 if not using AP-SSO)

Step 5: In the **Member MAC Address** box, enter the MAC address of the guest controller.

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

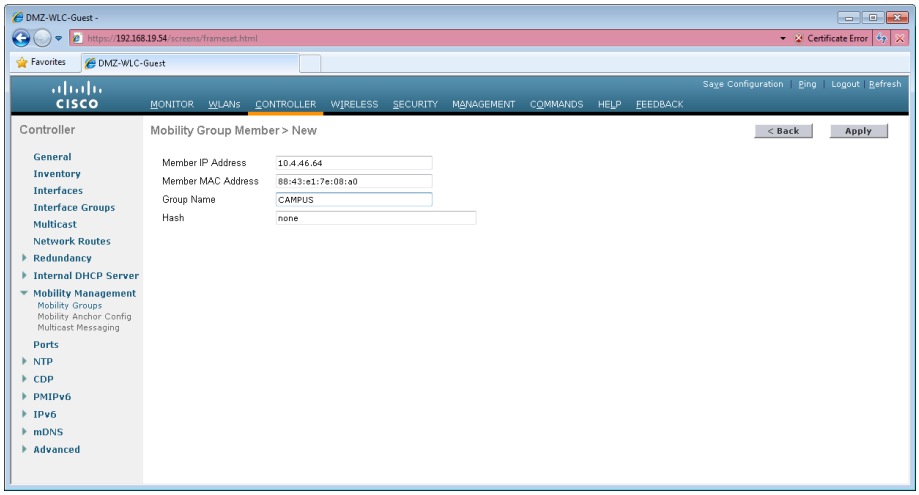


Step 7: On the guest controller, navigate to **Controller > Mobility Management > Mobility Groups**, and then click **New**.

Step 8: In the **Member IP Address** box, enter the IP address of a campus or remote-site controller. (Example: 10.4.46.64)

Step 9: In the **Member MAC Address** box, enter the MAC address of the campus or remote-site controller.

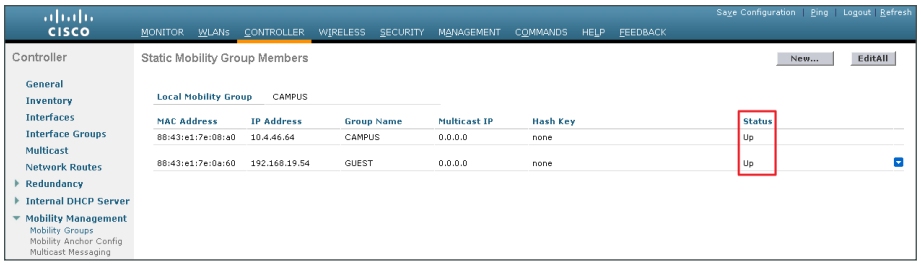
Step 10: In the **Group Name** box, enter the mobility group name configured on the campus or remote-site controller, and then click **Apply**. (Example: CAMPUS)



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

Step 12: Repeat Step 7 through Step 11 on every controller in your organization.

Step 13: Navigate to **Controller > Mobility Management > Mobility Groups**, and then verify that connectivity is up between all the controllers by examining the mobility group information. In the Status column, all controllers should be listed as **Up**.



Procedure 15 Create the lobby admin user account

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

You have two options to configure the lobby admin user account.

If you have not deployed Cisco Secure ACS and TACACS+ for management access control to the controller, perform the steps in Option 1.

If you have deployed Cisco Secure ACS and TACACS+ for management access control to the controller, perform the steps in Option 2.

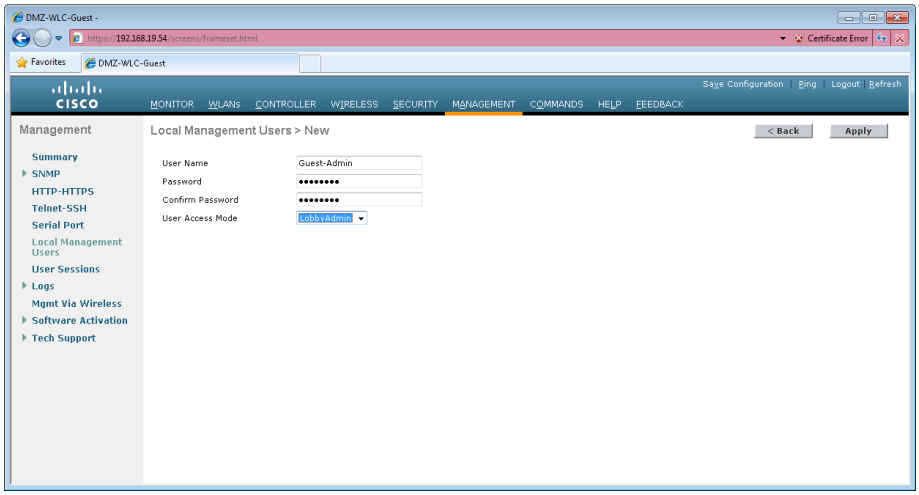
Option 1: Local lobby admin user account

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

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

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

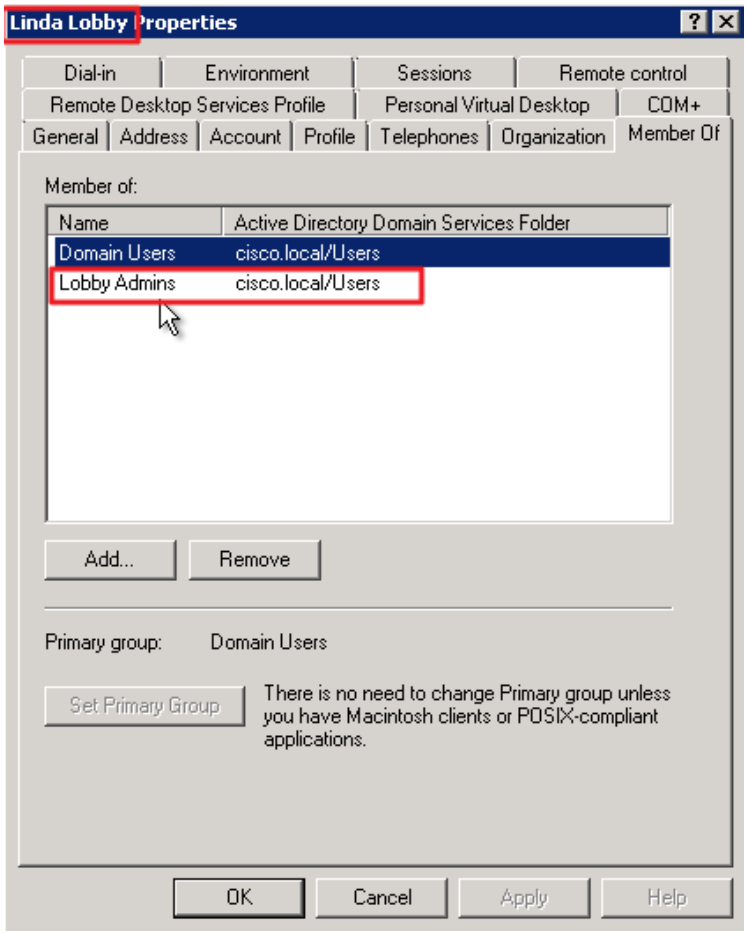
Step 4: In the **User Access Mode** list, choose **LobbyAdmin**, and then click **Apply**.



Option 2: Centralized lobby admin user account

Create groups in the Cisco Secure ACS internal identity store for network device administrators and helpdesk users. Users in the network device administrator group have enable-level EXEC access to the network devices when they log in, while helpdesk users must type in the enable password on the device in order to get enable-level access.

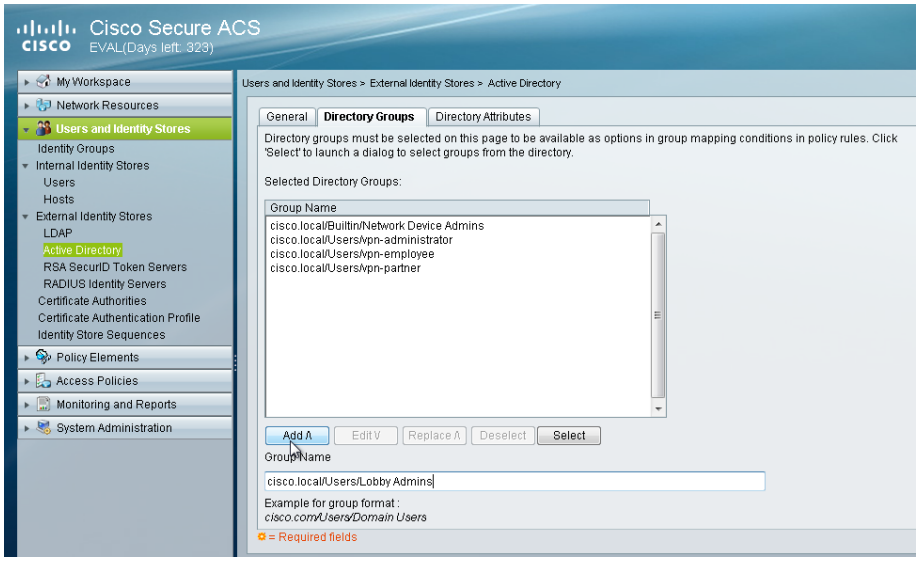
Step 1: Within Microsoft Active Directory, it is assumed that a lobby ambassador group (Example: Lobby Admins) has been created. Within this group is each of the lobby ambassadors employees within the organization. (Example: Linda Lobby)



Step 2: In Cisco Secure ACS, navigate to **Users and Identity Stores > External Identity Stores > Active Directory**.

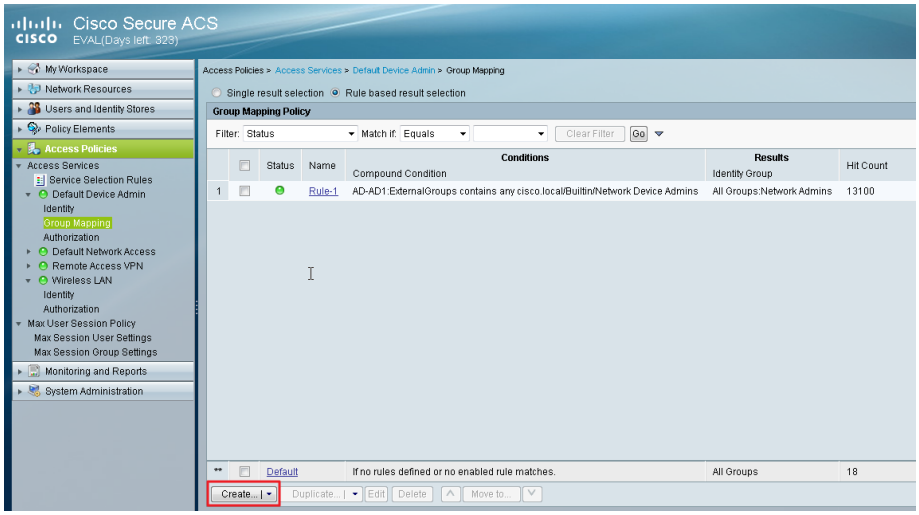
Step 3: Click the **Directory Groups** tab, and in the **Group Name** box, enter the lobby admin group (Example: cisco.local/Users/Lobby Admins), and then click **Add**.

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.

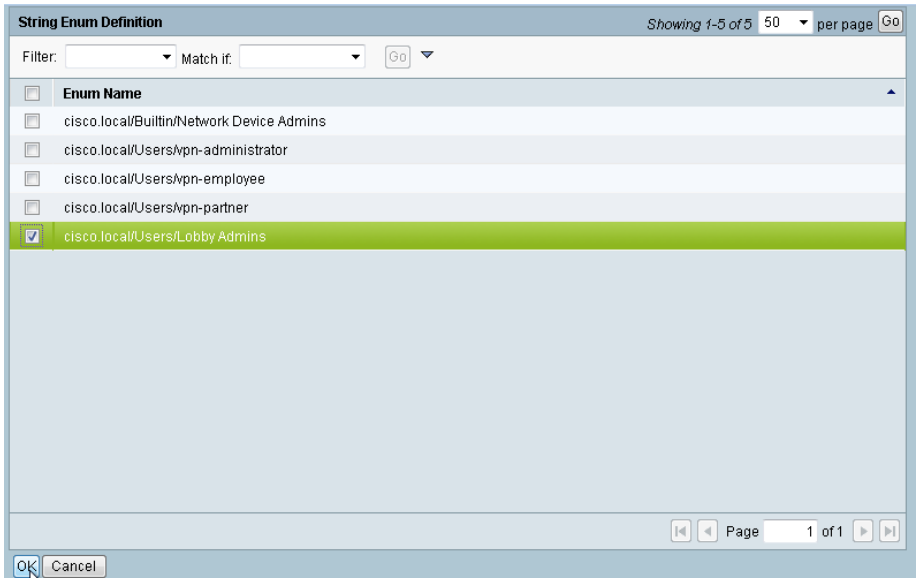
Step 4: In Cisco Secure ACS, navigate to **Access Policies > Access Services > Default Device Admin > Group Mapping**, and then at the bottom of the screen, click **Create**.



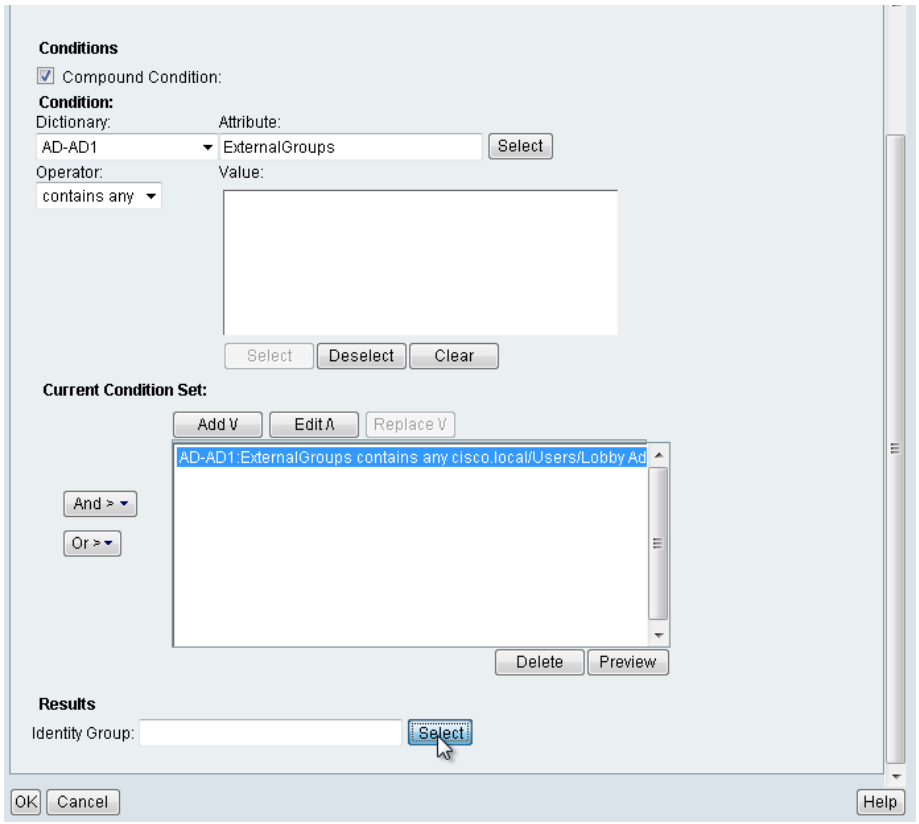
Step 5: Under Conditions, select **Compound Condition**, in the **Dictionary** list, choose **AD-AD1**, and then in the **Attribute** box, click **Select**. This selects External Groups.

Step 6: Under the Value box, click **Select**.

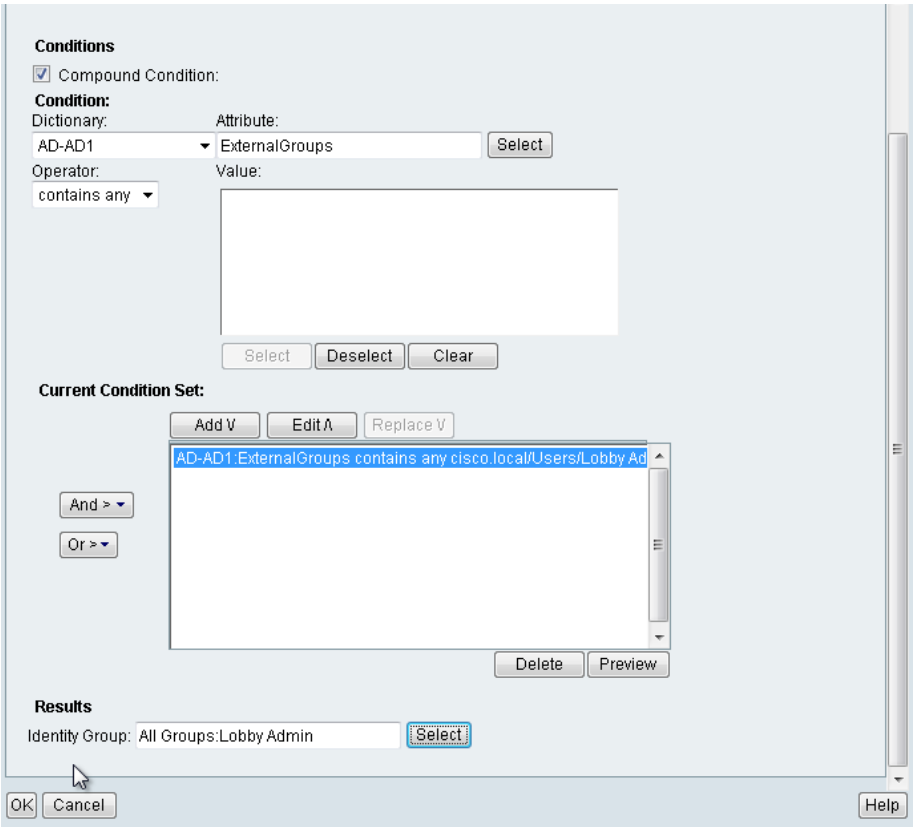
Step 7: In the String Enum Definition dialog box, select the lobby admin Active Directory group (Example: cisco.local/Users/Lobby Admins), and then click **OK**.



Step 8: Under Current Condition Set, click **Add**. The new condition appears in the **Current Condition Set** box.



Step 9: Under Results, click **Select**, select the Cisco Secure ACS identity group that will mapped to the Active Directory group specified in the Current Condition Set, and then click **OK**.



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

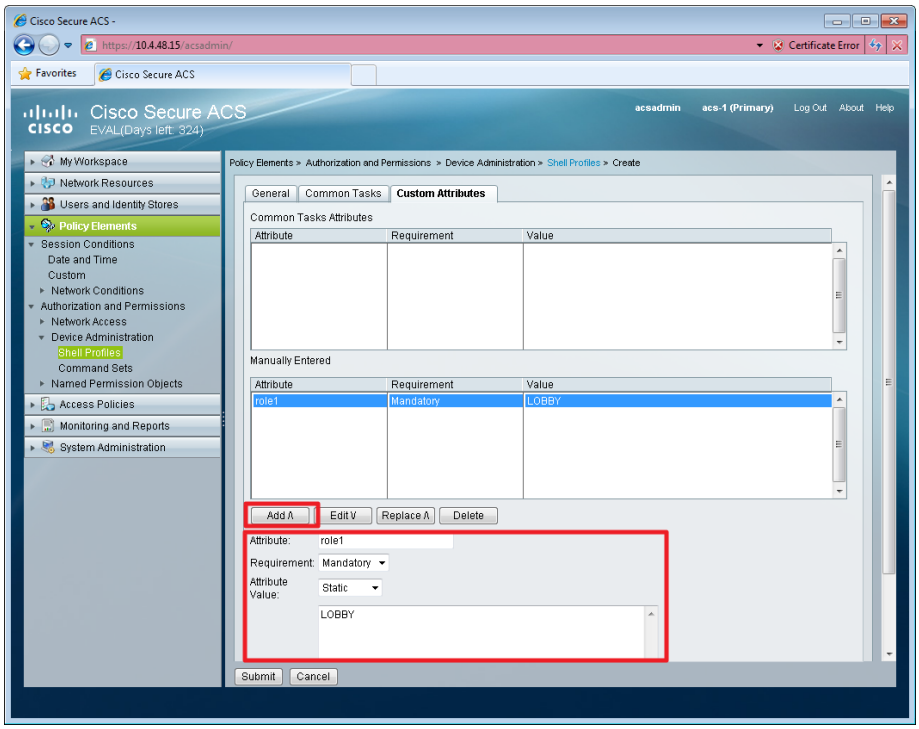
Step 10: In **Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles**, click **Create**.

Step 11: Under the General tab, in the **Name** box, enter a name for the wireless shell profile. (Example: Lobby Admins)

Step 12: On the Custom Attributes tab, in the **Attribute** box, enter **role1**.

Step 13: In the **Requirement** list, choose **Mandatory**.

Step 14: In the **Value** box, enter **LOBBY**, and then click **Add**.



Step 15: Click **Submit**.

Next, you create a WLC authorization rule.

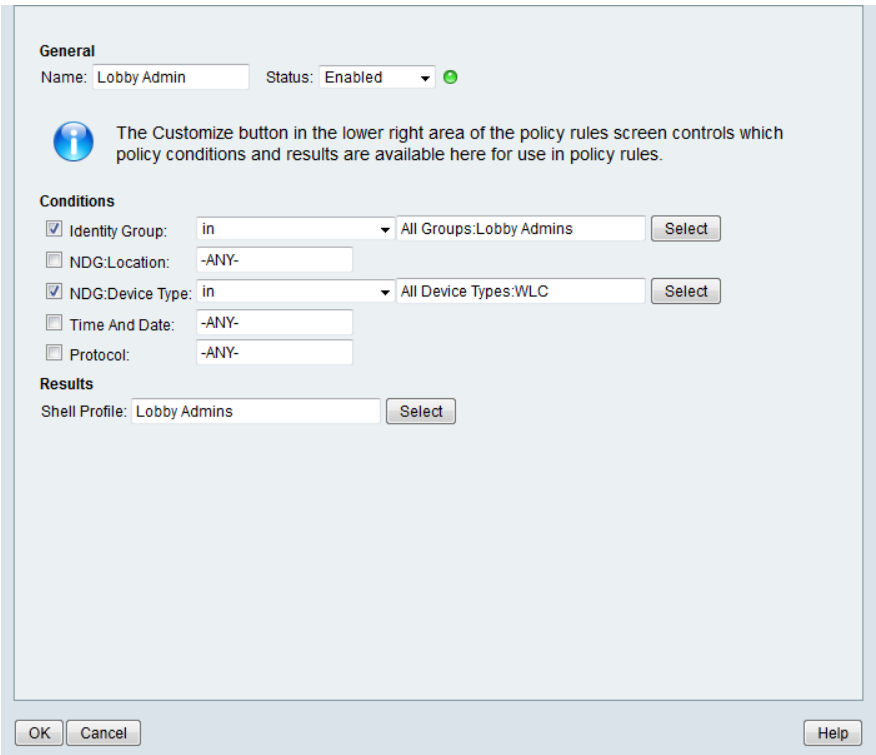
Step 16: In **Access Policies > Default Device Admin > Authorization**, click **Create**.

Step 17: In the **Name** box, enter a name for the WLC authorization rule. (Example: Lobby Admin)

Step 18: Under Conditions, select **Identity Group**, and then in the box, enter **All Groups:Lobby Admins**.

Step 19: Select **NDG:Device Type**, and then in the box, enter **All Device Types:WLC**.

Step 20: In the **Shell Profile** box, enter **Lobby Admins**, and then click **OK**.

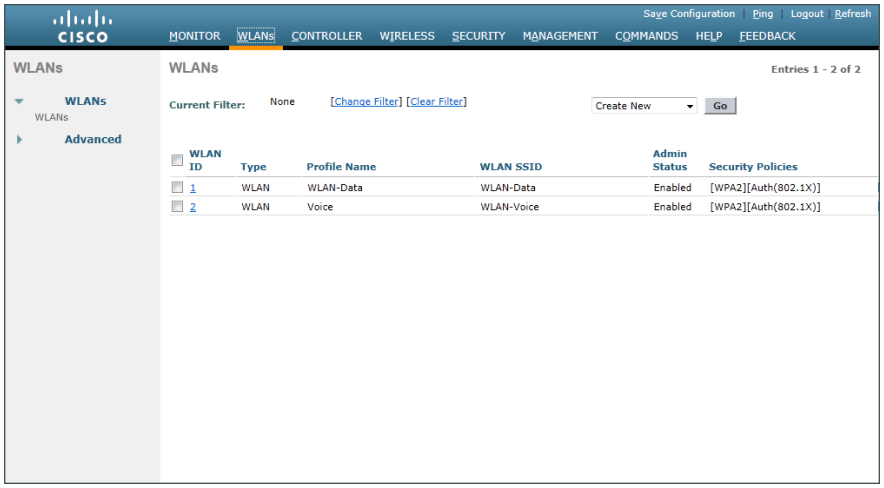


Step 21: Click **Save Changes**.

Procedure 16 Configure the internal WLCs for a guest

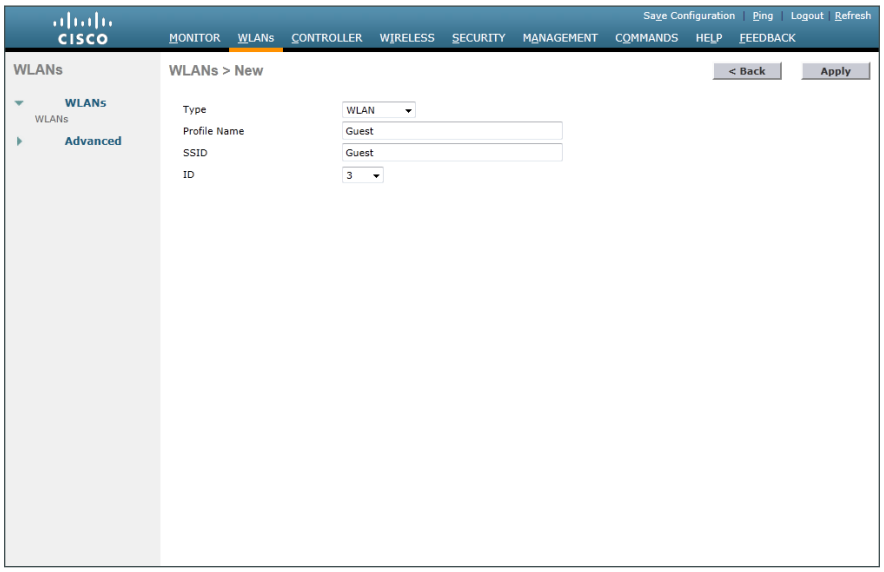
When a client connects to the guest SSID, the client must be anchored to the controller in the DMZ. The guest clients' traffic is tunneled from the controller to which the access point is connected to the guest controller, where the access point is given an IP address for the DMZ. The clients' traffic is then redirected to the web authentication page located on the guest controller. The client will not be authorized to connect with any IP protocol until it presents credentials to this authentication page.

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

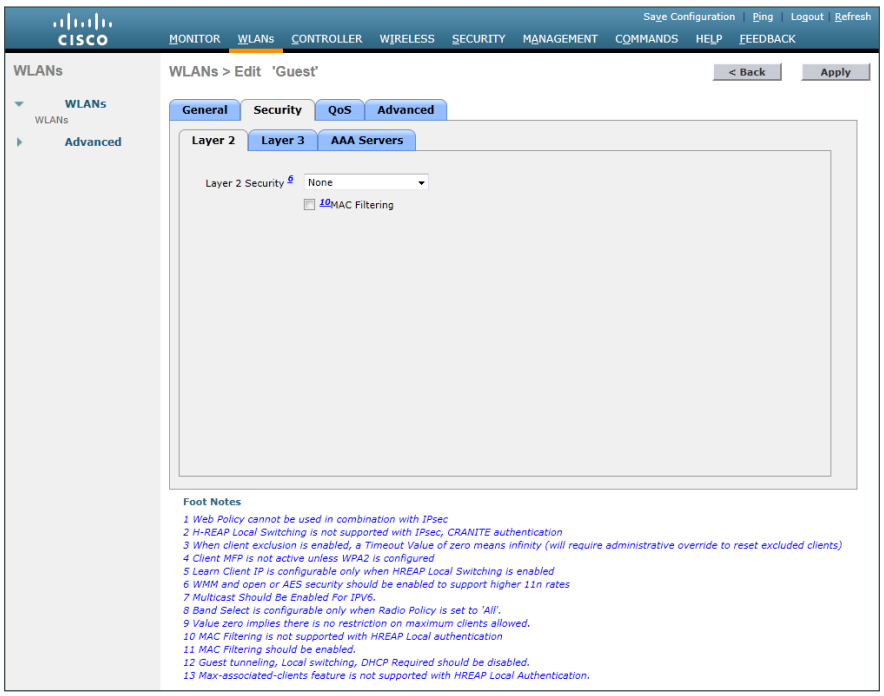


Step 2: Enter the **Profile Name**. (Example: Guest)

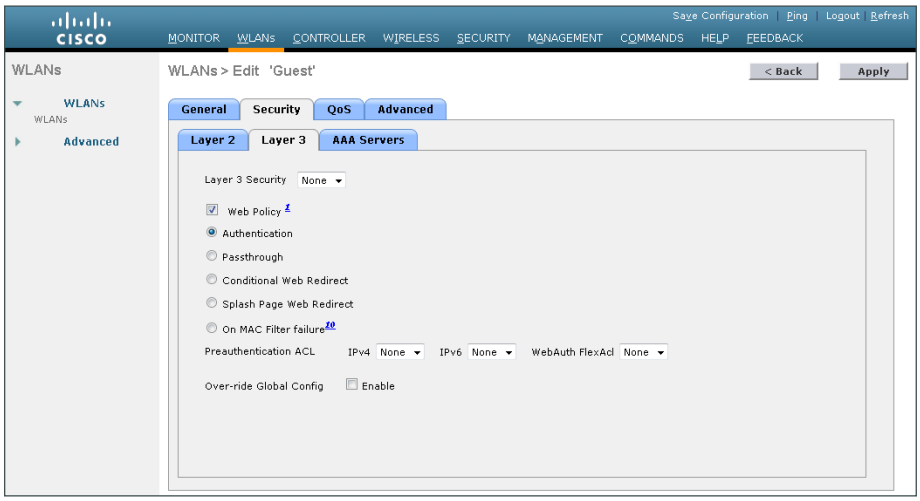
Step 3: In the **SSID** box, enter the guest WLAN name, and then click **Apply**. (Example: Guest)



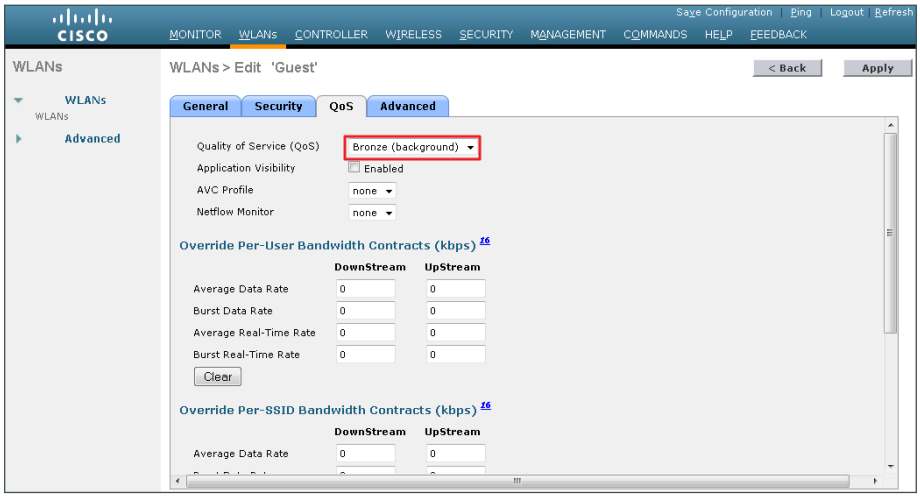
Step 4: Click the **Security** tab, and then on the Layer 2 tab, in the **Layer 2 Security** list, choose **None**.



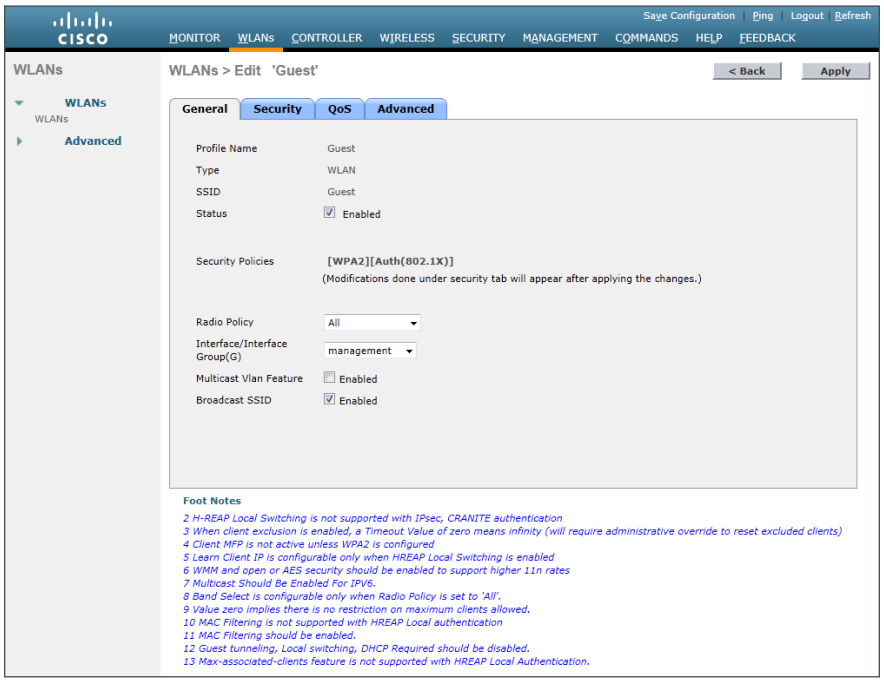
Step 5: On the Layer 3 tab, select **Web Policy**.



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



Step 7: On the General tab, to the right of Status, select **Enabled**, and then click **Apply**.



Step 8: Click **Back**.

Step 9: Hover over the blue list next to your guest WLAN, and then click **Mobility Anchors**.

Step 10: In the **Switch IP Address (Anchor)** list, choose the IP address of the guest controller. (Example: 192.168.19.54)

Step 11: Click **Mobility Anchor Create**, and then click **OK**.

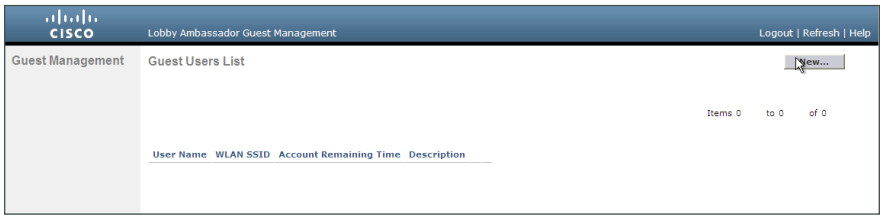
Step 12: Repeat Step 1through Step 10 for every internal controller in your organization.

Procedure 17 Create guest accounts

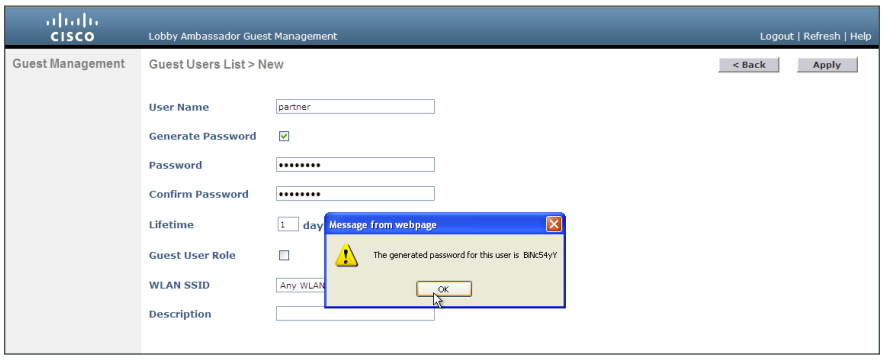
Now you can use the lobby administrator account to create usernames and passwords for partners, customers, and anyone else who is not normally granted access to your network.

Step 1: Using a web browser, open the DMZ wireless LAN controller's web interface (for example, https://guest-1.cisco.local/), and then log in using your LobbyAdmin account with the username and password created in Active Directory. (Example: LindaLobby/c1sco123)

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



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



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

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

Appendix A: Product List

Wireless LAN Controllers

Functional Area	Product Description	Part Numbers	Software
Remote Site Controller	Cisco 7500 Series Wireless Controller for up to 6000 Cisco access points	AIR-CT7510-6K-K9	7.4.100.0
	Cisco 7500 Series Wireless Controller for up to 3000 Cisco access points	AIR-CT7510-3K-K9	
	Cisco 7500 Series Wireless Controller for up to 2000 Cisco access points	AIR-CT7510-2K-K9	
	Cisco Flex 7500 Series Wireless Controller for up to 1000 access points	AIR-CT7510-1K-K9	
	Cisco 7500 Series Wireless Controller for up to 500 Cisco access points	AIR-CT7510-500-K9	
	Cisco 7500 Series Wireless Controller for up to 300 Cisco access points	AIR-CT7510-300-K9	
	Cisco 7500 Series High Availability Wireless Controller	AIR-CT7510-HA-K9	
	Cisco Virtual Wireless Controller for up to 5 Cisco access points	L-AIR-CTVM-5-K9	
	Cisco Virutal Wireless Controller 25 Access Point Adder License	L-LIC-CTVM-25A	
	Cisco Virtual Wireless Controller 5 Access Point Adder License	L-LIC-CTVM-5A	
	Cisco Virtual Wireless Controller 1 Access Point Adder License	L-LIC-CTVM-1A	
On Site, Remote Site, or Guest Controller	Cisco 5500 Series Wireless Controller for up to 500 Cisco access points	AIR-CT5508-500-K9	7.4.100.0
	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	7.4.100.0
	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 3600 Series Access Point Dual Band 802.11a/g/n and CleanAir with Internal Antennas	AIR-CAP3602I-x-K9	7.4.100.0
	Cisco 3600 Series Access Point Dual Band 802.11a/g/n and CleanAir with External Antennas	AIR-CAP3602E-x-K9	
	Cisco 2600 Series Access Point Dual Band 802.11a/g/n and CleanAir with Internal Antennas	AIR-CAP2602I-x-K9	
	Cisco 2600 Series Access Point Dual Band 802.11a/g/n and CleanAir with External Antennas	AIR-CAP2602E-x-K9	
	Cisco 1600 Series Access Point Dual-band controller-based 802.11a/g/n with Internal Antennas	AIR-CAP1602I-x-K9	
	Cisco 1600 Series Access Point Dual-band controller-based 802.11a/g/n with External Antennas	AIR-CAP1602E-x-K9	

Access Control

Functional Area	Product Description	Part Numbers	Software
Authentication Services	ACS 5.3 VMware Software and Base License	CSACS-5.3-VM-K9	5.3

Data Center Core

Functional Area	Product Description	Part Numbers	Software
Core Switch	Cisco Nexus 5596 up to 96-port 10GbE, FCoE, and Fibre Channel SFP+	N5K-C5596UP-FA	NX-OS 5.2(1)N1(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 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.4.0.SG(15.1-2SG) IP Base license
	Cisco Catalyst 4500 E-Series Supervisor Engine 7L-E	WS-X45-SUP7L-E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+ ports	WS-X4648-RJ45V+E	
	Cisco Catalyst 4500 E-Series 48 Ethernet 10/100/1000 (RJ45) PoE+,UPoE ports	WS-X4748-UPOE+E	
Stackable Access Layer Switch	Cisco Catalyst 3850 Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3850-48F	3.2.1SE(15.0-1EX1) 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 3750-X Series Stackable 48 Ethernet 10/100/1000 PoE+ ports	WS-C3750X-48PF-S	15.0(2)SE2 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	
Standalone Access Layer Switch	Cisco Catalyst 3560-X Series Standalone 48 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-48PF-S	15.0(2)SE2 IP Base license
	Cisco Catalyst 3560-X Series Standalone 24 Ethernet 10/100/1000 PoE+ ports	WS-C3560X-24P-S	
	Cisco Catalyst 3750-X Series Two 10GbE SFP+ and Two GbE SFP ports network module	C3KX-NM-10G	
	Cisco Catalyst 3750-X Series Four GbE SFP ports network module	C3KX-NM-1G	
Stackable Access Layer Switch	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-48FPD-L	15.0(2)SE2 LAN Base license
	Cisco Catalyst 2960-S Series 48 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-48FPS-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Two 10GbE SFP+ Uplink ports	WS-C2960S-24PD-L	
	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 PoE+ ports and Four GbE SFP Uplink ports	WS-C2960S-24PS-L	
	Cisco Catalyst 2960-S Series Flexstack Stack Module	C2960S-STACK	

LAN Distribution Layer

Functional Area	Product Description	Part Numbers	Software
Modular Distribution Layer Virtual Switch Pair	Cisco Catalyst 6500 E-Series 6-Slot Chassis	WS-C6506-E	15.1(1)SY 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 24-port GbE SFP Fiber Module w/DFC4	WS-X6824-SFP-2T	
Modular Distribution Layer Switch	Cisco Catalyst 4507R+E 7-slot Chassis with 48Gbps per slot	WS-C4507R+E	3.4.0.SG(15.1-2SG) Enterprise Services license
	Cisco Catalyst 4500 E-Series Supervisor Engine 7-E, 848Gbps	WS-X45-SUP7-E	
	Cisco Catalyst 4500 E-Series 24-port GbE SFP Fiber Module	WS-X4624-SFP-E	
	Cisco Catalyst 4500 E-Series 12-port 10GbE SFP+ Fiber Module	WS-X4712-SFP+E	
Stackable Distribution Layer Switch	Cisco Catalyst 3750-X Series Stackable 12 GbE SFP ports	WS-C3750X-12S-E	15.0(2)SE2 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 Switch	Cisco Catalyst 6500 E-Series 6-Slot Chassis	WS-C6506-E	15.1(1)SY 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 24-port GbE SFP Fiber Module w/DFC4	WS-X6824-SFP-2T	

WAN Remote Site

Functional Area	Product Description	Part Numbers	Software
Modular WAN Remote-site Router	Cisco 3945 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3945-VSEC/K9	15.2(4)M3 securityk9 license datak9 license
	Cisco 3925 Voice Sec. Bundle, PVDM3-64, UC and SEC License PAK	C3925-VSEC/K9	
	Data Paper PAK for Cisco 3900 series	SL-39-DATA-K9	
	Cisco 2951 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2951-VSEC/K9	
	Cisco 2921 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2921-VSEC/K9	
	Cisco 2911 Voice Sec. Bundle, PVDM3-32, UC and SEC License PAK	C2911-VSEC/K9	
	Data Paper PAK for Cisco 2900 series	SL-29-DATA-K9	
	1941 WAAS Express only Bundle	C1941-WAASX-SEC/K9	
	Data Paper PAK for Cisco 1900 series	SL-19-DATA-K9	
Fixed WAN Remote-site Router	Cisco 881 SRST Ethernet Security Router with FXS FXO 802.11n FCC Compliant	C881SRST-K9	15.2(4)M3 securityk9 license datak9 license

Internet Edge

Functional Area	Product Description	Part Numbers	Software
Firewall	Cisco ASA 5545-X IPS Edition - security appliance	ASA5545-IPS-K9	ASA 9.0(1) IPS 7.1(7) 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 ASA5512-X Security Plus license	ASA5512-SEC-PL	
	Firewall Management	ASDM	7.0(2)

Internet Edge LAN

Functional Area	Product Description	Part Numbers	Software
DMZ Switch	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 ports	WS-C3750X-24T-S	15.0(2)SE2 IP Base license

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 08/13