Newer Cisco SBA for Government Guides Available

This guide is part of an older series of Cisco Smart Business Architecture for Government. To access the latest Cisco SBA for Government Guides, go to http://www.cisco.com/go/govsba

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

SBA

SBA FOR GOVT

LARGE

BORDERLESS NETWORKS

Wireless CleanAir Deployment Guide

SBA FOR GOVERNMENT

Revision: H2CY10

Using this Borderless Networks Guide

This document is for the reader who:

- Wants a general understanding of Radio Resource management.
- Understands the challenges of the unlicensed Radio Spectrum.
- Has already read the *Cisco Smart Business Architecture for Government Large Agencies—Borderless Networks LAN Deployment Guide* and is looking for a Wireless Network Management Solution.
- Has an existing network and needs guidance on how to add Wireless and Radio Spectrum Management.
- Wants to better understand how to react to unforeseen Wireless Network challenges.

Using this Collaboration Guide

This guide is a concise reference on Wireless Network Management and is organized into the following sections:

The **Introduction** outlines the issues the Cisco Wireless Control System and Navigator can solve within your agency and the capabilities it provides to solve them.

The **Technology Overview** section introduces Cisco Wireless Control System and describes how it is delivered as Software as a Service (SaaS).

The **Cisco Wireless Control System (WCS) and Navigator Solutions Overview** section discusses the various Wireless Network Management solution offerings, the differences between them, and how to decide which one is right for you.

How to Get Cisco Wireless Control System points you to the correct resource to order Cisco WCS or Navigator for your agency.

Who Should Read This Guide

This guide should be of interest to anyone in a large government agency who wants to understand the benefits of using the Wireless Network Management, Cisco's Wireless Control System (WCS), and the Wireless Control System Navigator offerings, to learn how to choose among them, and to find out how to purchase one of these products.

The audience also includes technology resellers who want to understand more about the Cisco Wireless offerings and to learn how to become a Cisco Wireless authorized partner.

This guide does not require any specific technical background other than general computer experience.

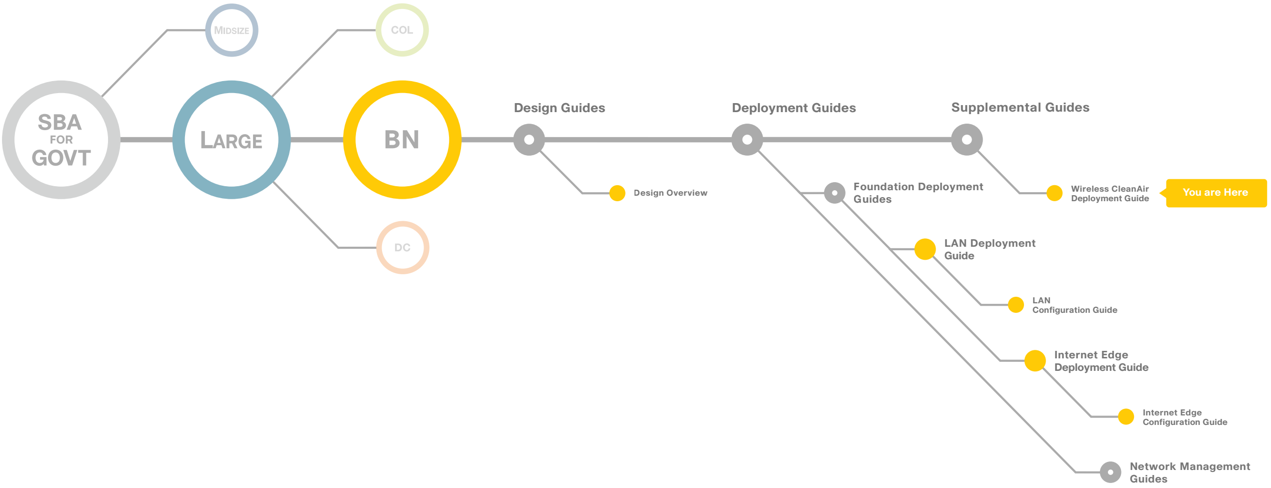

SBA FOR GOVT
MIDSIZE
LARGE
COL
DC
BN
Design Guides
Design Overview
Deployment Guides
Foundation Deployment Guides
LAN Deployment Guide
LAN Configuration Guide
Internet Edge Deployment Guide
Internet Edge Configuration Guide
Network Management Guides
Supplemental Guides
Wireless CleanAir Deployment Guide
You are Here

Table of Contents

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental. Cisco Unified Communications SRND (Based on Cisco Unified Communications Manager 7.x)

Introduction

This guide is a companion document to the Cisco SBA for Large Agencies—Borderless Network Design Overview and deployment guides.

The Cisco SBA for Large Agencies is a prescriptive architecture that delivers an easy-to-use, flexible, and scalable network with wired, wireless, security, WAN optimization, and unified communication components. The architecture eliminates the challenges of integrating the various network components by using a standardized design that is reliable and has comprehensive support offerings.

The Cisco SBA for Large Agencies is designed to address the common requirements of agencies with 2000 to 10000 employees. Each agency is unique, however, and so are its requirements. Because of that, the Cisco Borderless Network Architecture was built so that additional capabilities could be added without redesigning the network.

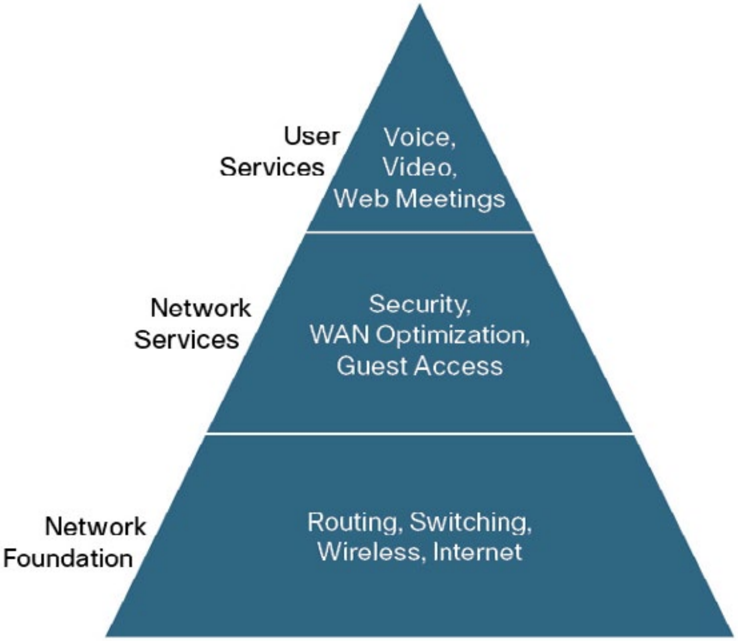
One way that the Cisco Borderless Network Architecture accomplishes this extensibility is by breaking down the architecture into three primary layers: Network Foundation, Network Services, and User Services. See Figure 1.

The Cisco Wireless Control System is a User Service. User Services are the services or applications we use everyday and interact with directly. They range from picking up the phone to use the phone service, to reading our email using the email service. How well a User Service interacts with the Network Service impacts how it performs when a user actually uses it, which makes Wireless Network management an imperative for a healthy network.

Reliable Network Services provided by the Cisco SBA such as the Internet connection, WAN infrastructure, and security help ensure an agency can rely on applications such as web conferencing for critical collaboration.

To learn more about Cisco SBA for Large Agencies—Borderless Network, visit:
http://www.cisco.com/go/smartarchitecture or
http://www.cisco.com/go/partner/smartarchitecture

Figure 1. Network Services, Services and Foundation

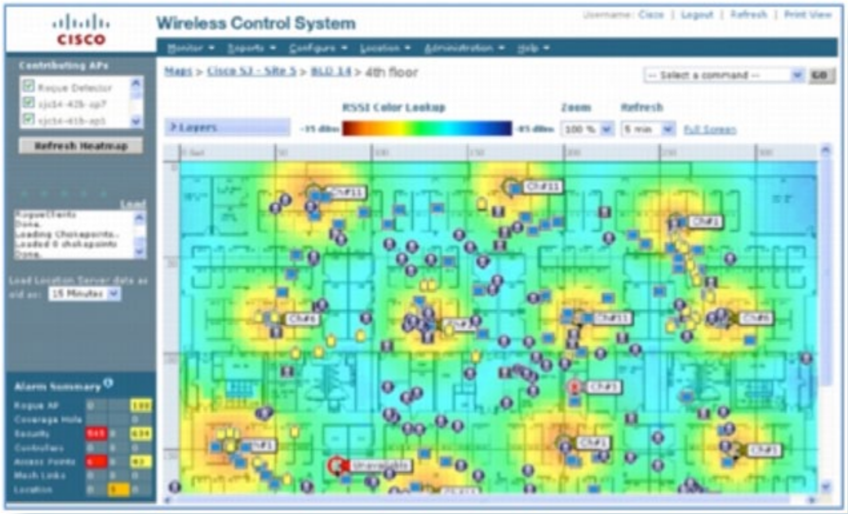

User Services
Voice, Video, Web Meetings
Network Services
Security, WAN Optimization, Guest Access
Network Foundation
Routing, Switching, Wireless, Internet

Agency Overview

The challenges of running a wired data network are beyond the expectations of most other jobs. The challenges go beyond simply adding a machine and handing it over to the desktop IT department or to the end user to leverage as they desire. With the numerous challenges that arise with any application, the network is always the easiest entity to blame for failure. Now add a wireless data network to the picture and the challenges and skill set required to maintain and troubleshoot the network triple. Wireless networking brings a new set of unknowns that a wired network never had to address.

The Cisco Wireless Control System (WCS) with CleanAir Technology allow the Network Administration IT staff to visually see how well their network is performing, troubleshoot client connectivity remotely, manage wireless network resources, and analyze interference devices from anywhere in the world and more. The real power of Cisco WCS with CleanAir combined with CleanAir access points is the ability to visually represent the radio environment to the network administrator to better manage and troubleshoot issues before they become issues.

Figure 2. WCS Heat Map

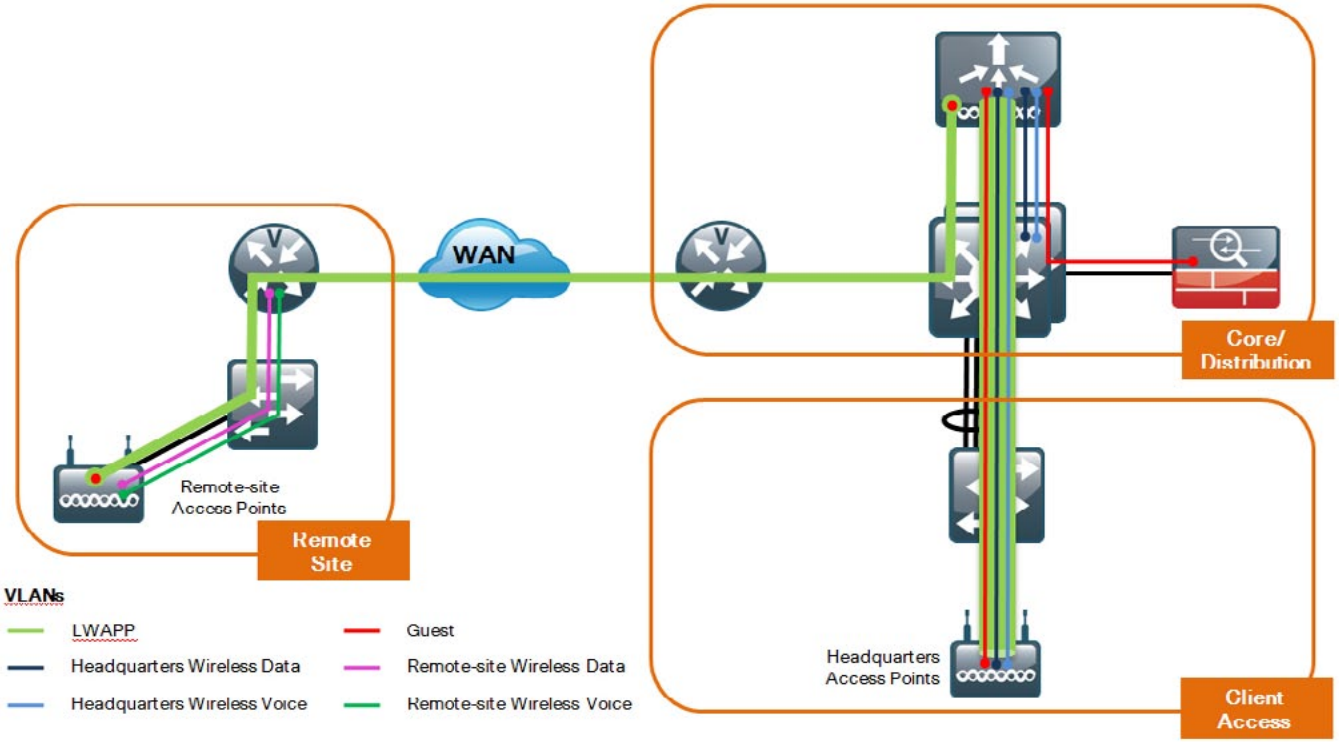


Radio is the manipulation of the magnetic field that is invisible to the naked eye. Without running expensive site surveys with a spectrum expert every hour and minute of every day, the network administrator cannot tell what is happening in the user space. The Wireless Control system collects the data from all the Wireless LAN Controllers (WLC) in the network, while each CleanAir access point does a spectrum sweep of the environment and alerts the administrator of any potentially negative issue before a user creates a call ticket in the network call center.

The CleanAir Access Point

Unlicensed bands need to be proactively managed. Wi-Fi is no longer a convenience technology used for casual web surfing or simple connectivity from conference rooms. With 802.11n, wireless performance is now on par with wired networks where organizations such as hospitals rely on the wireless network for mission-critical and patient-critical applications. With limited IT resources, lack of tools, and lack of RF expertise, the CleanAir access point with Integrated Spectrum hardware can fill the RF expertise gap and limit or eliminate network downtime.

Figure 3. Simplified Network Diagram


WAN
Remote-site Access Points
Remote Site
Core/ Distribution
Headquarters Access Points
Client Access
VLANs
LWAPP
Headquarters Wireless Data
Headquarters Wireless Voice
Guest
Remote-site Wireless Data
Remote-site Wireless Voice

With Event Driven Radio Resource Management, an issue within the wireless radio network can be identified and mitigated without any user interaction. Alerts can be sent out via email as well as through syslog to make the network IT staff aware of the mitigated issue and alert them to watch for other issues, enforce the agency radio policy, or do both.

Technology Overview

Cisco CleanAir Technology

Cisco CleanAir is the integration of Cisco Spectrum Expert technology with a Cisco access point. Before Cisco CleanAir was available, operators had to walk around with an instrument to detect chosen signals and physically locate the device. Cisco CleanAir helps to automate these tasks within the system management function by adding additional intelligence over Spectrum Expert, and thereby augmenting the overall experience by proactively reclaiming control over the spectrum.

The components of a basic Cisco CleanAir technology are the Wireless LAN Controller and the Cisco 3500 Series access points. To take advantage of the entire Cisco CleanAir feature, the Cisco WCS can display in real time the data retrieved from Cisco CleanAir. Adding the Mobility Services Engine (which is addressed in a separate guide) further enhances the available features and provides the history and location of specific interference devices.

Wireless Control System

Cisco WCS enables you to configure and monitor one or more controllers and associated access points, to monitor and troubleshoot radio technology, and to visually display Cisco CleanAir data to the network administrator. Cisco WCS includes the same configuration, performance monitoring, security, fault management, and accounting options used at the controller level and adds a graphical view of multiple controllers and managed access points.

Cisco WCS runs on Windows 2003/SP2, Windows 2003 R2/SP2 32-bit installations, and Red Hat Linux Enterprise Server 5.0 32-bit installations. On both Windows and Linux, Cisco WCS runs as a service, which runs continuously and resumes running after a reboot. The configuration in this guide runs the Windows 2003 Operating System within a virtual machine and leverages VMware ESXi 4.0 within the data center.

Mobility Services Engine

The Mobility Service Engine (MSE) can run multiple related or independent services such as location and wireless IDS/IPS services, the CleanAir database functionality, as well as future services. The MSE is an independent appliance and is leveraged by the Cisco WCS. The MSE and the services it supports are discussed in another supplemental guide.

Location or Context-Aware

The Cisco location service solution (also referred to as the context-aware service) provides the capability to determine the physical location of a tracked entity in the network and additional contextual information such as the serial number of the tracked entity. The tracked entity can be a wireless endpoint, a wired end-point (a phone or PC), a wired switch, or a wireless controller. Location information is critical for wired endpoints. For example, a phone in the lobby of an office building can have different policies from a phone in a conference room or in an employee office. Today, the policies are statically administered based on the MAC address and not based on the location of the endpoint itself. Knowing the location of a wired entity provides additional intelligence to push the right set of policies to tracked devices based not only on the user's credentials and MAC address, but also on the location of the device. This document does not cover the location service solution; this information is presented in a different supplemental guide.

Configuration Details

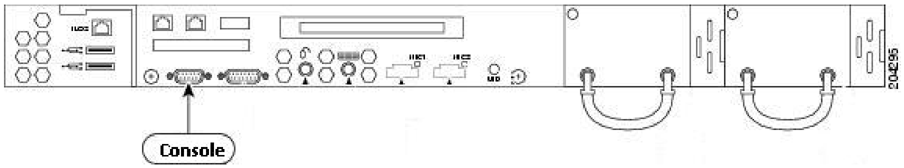
This Cisco Wireless Control System requires having Windows 2003 Server loaded, and within the SBA architecture, we have loaded Windows 2003 Server on a VMware ESXi 4.0 platform. This document leverages the standard server configuration that supports up to 2000 Cisco Aironet lightweight access points, 1000 standalone access points, and 450 Cisco wireless LAN controllers. A low-end server can support up to 500 Cisco Aironet lightweight access points, 200 standalone access points, and 125 Cisco wireless LAN controllers. This information can help you determine your network needs and future growth. No matter what your agency requires, it is the same Cisco Wireless Control System software that runs on different hardware, as described in the product Release Notes.

Install the Mobility Service Engine

The Mobility Solutions Engine (MSE) can be leveraged within the CleanAir solution to create an Interference History. Many issues that occur in the day-to-day operations of a Wireless Network are intermittent and often hard to track down. Leveraging the power of the MSE, you can track an issue by the time of day and build upon the historical data that can help mitigate these difficult, if not impossible, network interference devices.

Initial Configuration of the MSE

Step 1: Connect your console cable to the console port of the MSE.



Step 2: Power on the Mobility Services Engine.

Step 3: Follow the on-screen prompts and provide the following required information in this order:

1. Hostname
2. IP address
3. Network mask
4. Default gateway
5. DNS server IP address
6. Login banner
7. SSH password (WCS Username and Password is used by the WCS for secure communication)
8. WCS communication username
9. WCS communication password (which must have two uppercase and two lowercase characters, two digits, and two special characters to be accepted)

Provide the following optional information:

1. NTP server IP address
2. Second Ethernet IP address

Process

1. Installation
2. Licensing
3. Wireless LAN controller
4. Add Mobility Service Engine to Wireless Control System
5. Building and Floorplan
6. Configuring the Cisco Wireless Solution for CleanAir

Procedure 1 Installation

The installation steps outlined in this section are typical for most applications and perhaps intuitive to most users. With every installation, knowing up front what you need to have ready is essential for a quick and easy installation experience. With the Cisco Wireless Control System, planning the hostname ahead of time when building the machine makes for a logical and easy-to-troubleshoot network. For the actual installation of the Cisco Wireless Control System service, keep the following information handy for a smooth installation process.

1. HTTP, HTTPS, and health monitor port information
   a. We will use the default ports, however, consult your security policy to be sure your agency policy is to use default ports
2. Root password
3. FTP file folder on local machine
4. TFTP file folder on local machine
5. Installation folder (a default folder will be chosen under Program Files)

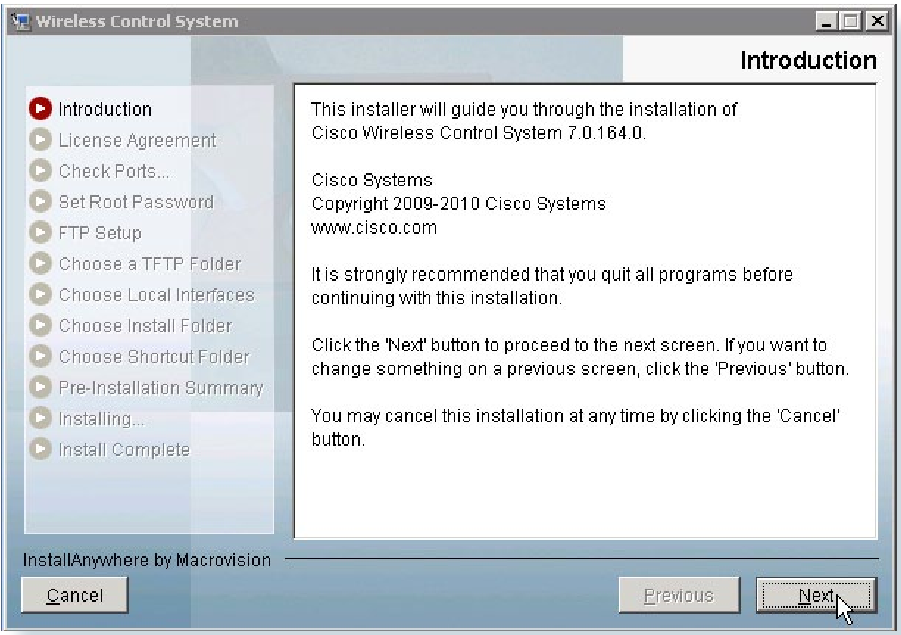
Run Application

Double-click the Cisco WCS application that you downloaded from Cisco.com. It should have a name similar to the following:

```
WCS-STANDARD-K9-7.0.164.0.exe
```

You see the introductory screen as shown here.

Figure 4. WCS Initial Configuration



This installer will guide you through the installation of Cisco Wireless Control System 7.0.164.0.

Cisco Systems
Copyright 2009-2010 Cisco Systems
www.cisco.com

It is strongly recommended that you quit all programs before continuing with this installation.

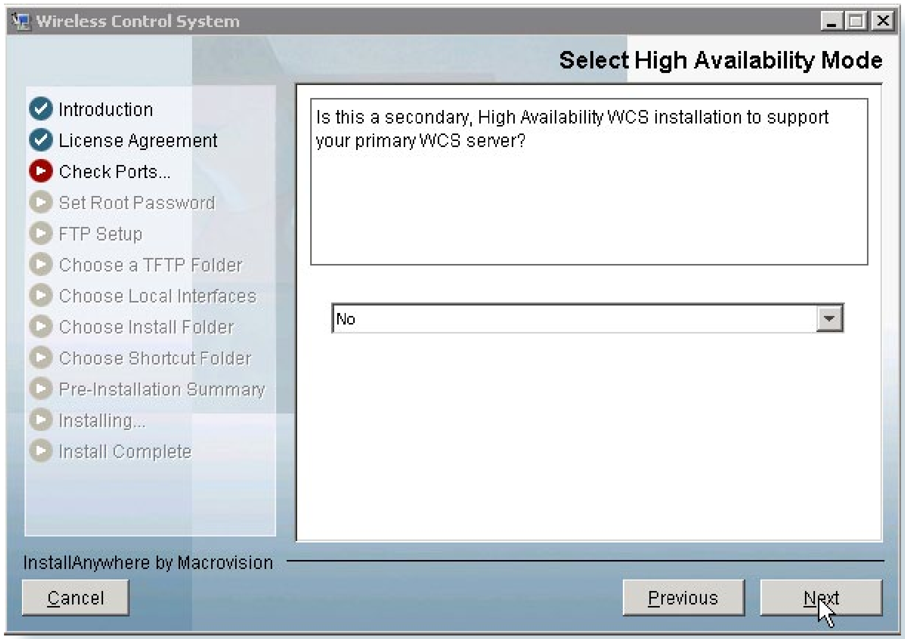
Click the 'Next' button to proceed to the next screen. If you want to change something on a previous screen, click the 'Previous' button.

You may cancel this installation at any time by clicking the 'Cancel' button.

The introduction summarizes the application you downloaded and prompts you to move to the next screen. You must accept the license agreement and click **Next**.

The installer checks for any previous installations. It asks if this installation is for High Availability or is being built as a secondary WCS. We do not set up a secondary or High Availability installation in this guide; however, you can do this simply by repeating this installation and selecting **Yes**.

Figure 5. High Availability Mode Selection



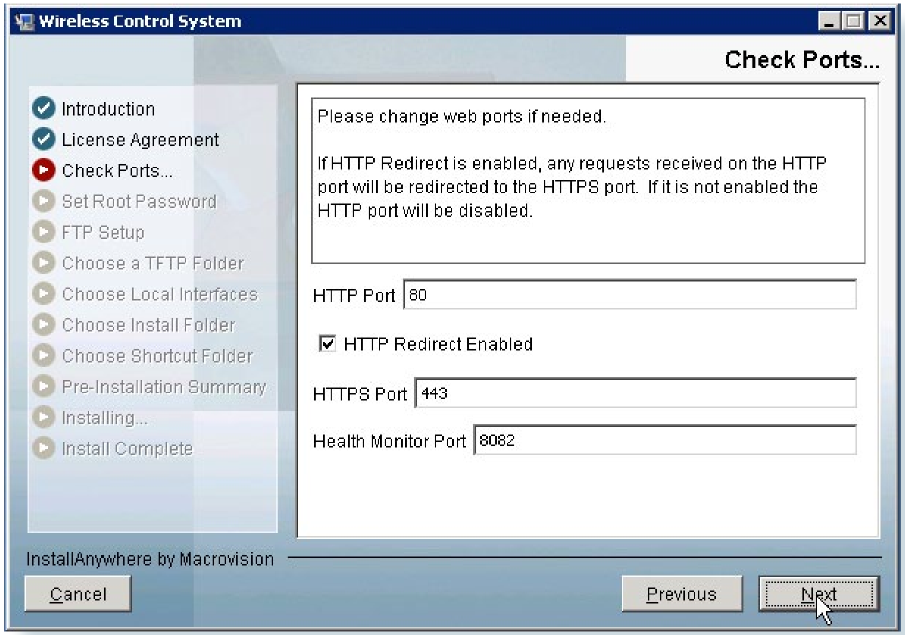
Select High Availability Mode

Is this a secondary, High Availability WCS installation to support your primary WCS server?

No

The next two screens prompt you to either accept the default ports or assign alternative ports for access services on your Cisco WCS. Unless your security policy specifies something different, click **Next**.

Figure 6. Port Configuration



Check Ports...

Please change web ports if needed.

If HTTP Redirect is enabled, any requests received on the HTTP port will be redirected to the HTTPS port. If it is not enabled the HTTP port will be disabled.

HTTP Port 80

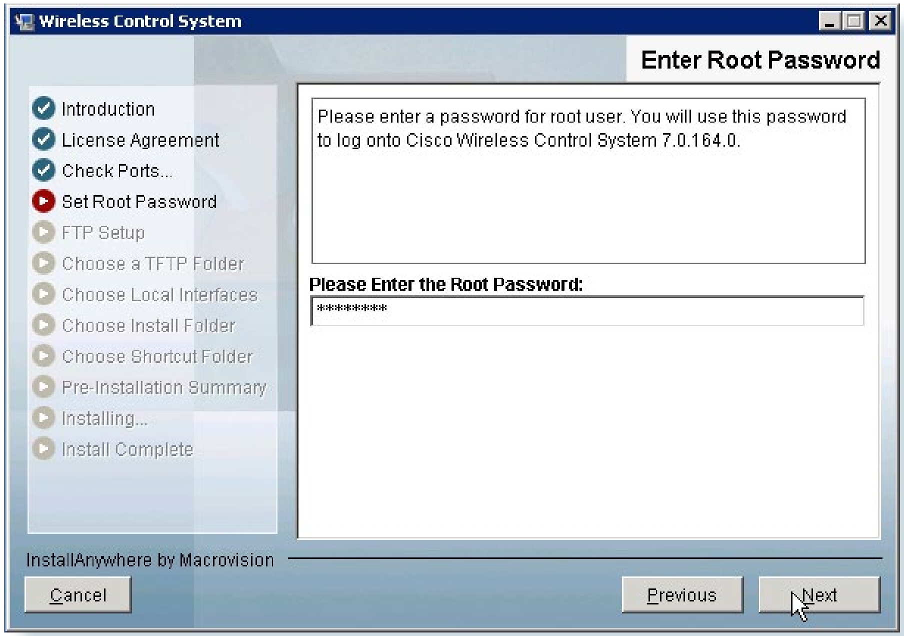
☑ HTTP Redirect Enabled

HTTPS Port 443

Health Monitor Port 8082

You must define the root password next. This password is the locally defined administration password. The password will be checked for strength; however, password strength should follow your security policy. The root password is only used for the local administrator.

Figure 7. Root Password

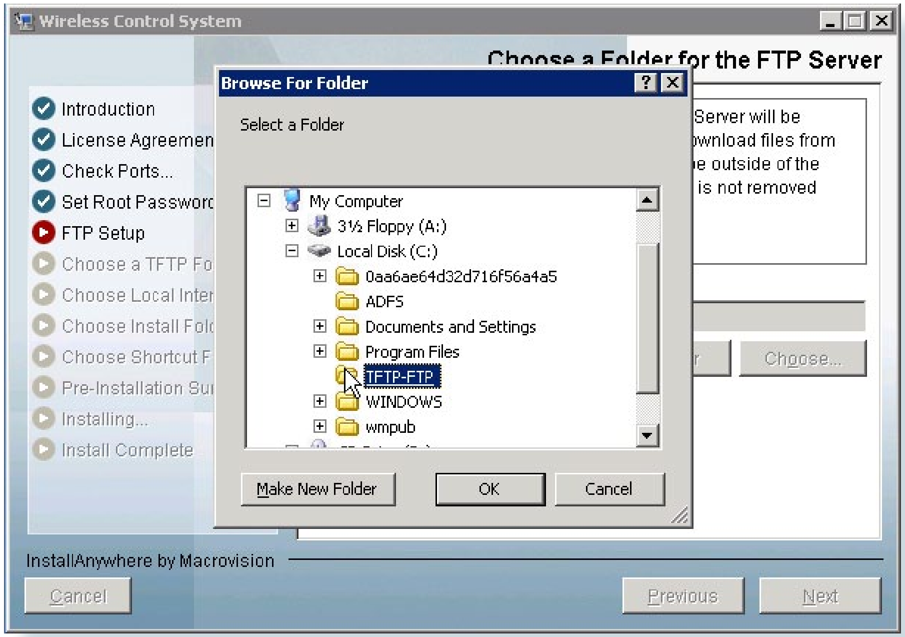


Please enter a password for root user. You will use this password to log onto Cisco Wireless Control System 7.0.164.0.

Please Enter the Root Password: *********

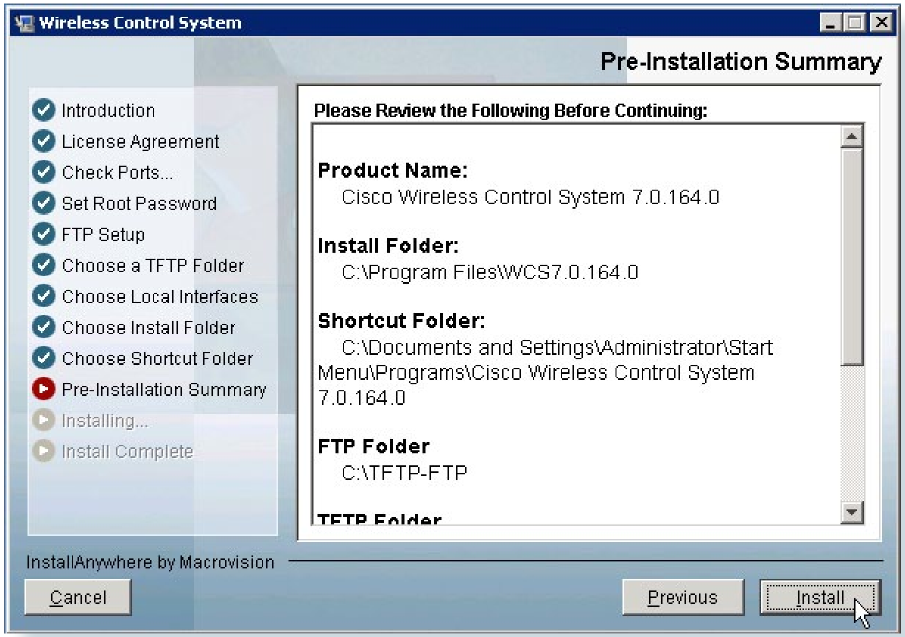
Choose your FTP folder, TFTP folder, and the installation folder on the local machine for WCS. As a pre-check, we created an FTP folder and a separate TFTP folder for this function and allowed the default folder for the Cisco WCS installation.

Figure 8. File Folder Selection



Click **Next** on the installation icon folder options to get to the installation summary. Review your choices before the installation begins.

Figure 9. Installation Summary



Pre-Installation Summary

Please Review the Following Before Continuing:

Product Name:
Cisco Wireless Control System 7.0.164.0

Install Folder:
C:\Program Files\WCS7.0.164.0

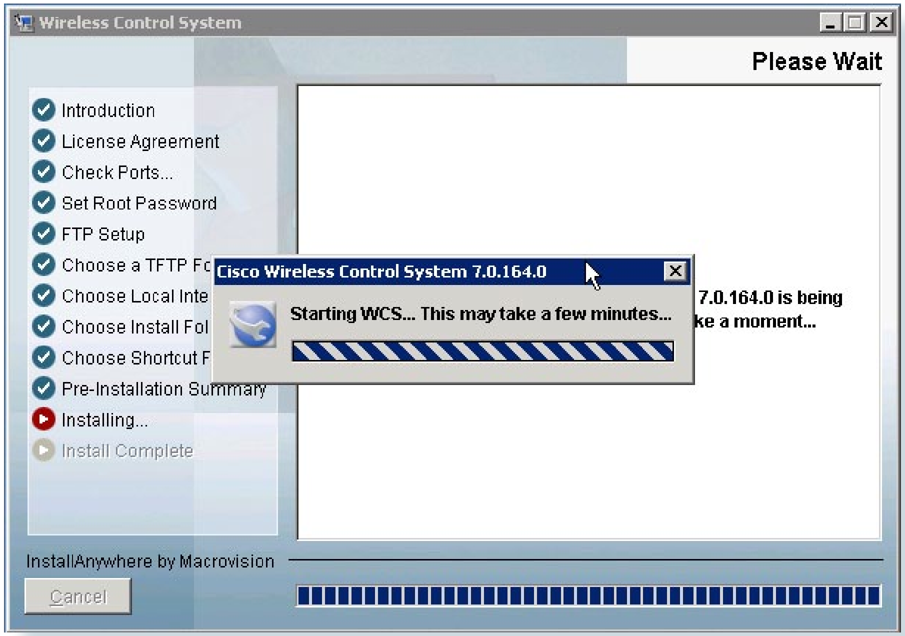
Shortcut Folder:
C:\Documents and Settings\Administrator\Start Menu\Programs\Cisco Wireless Control System 7.0.164.0

FTP Folder
C:\TFTP-FTP

TFTP Folder

Once the installation completes, you can start Cisco WCS services.

Figure 10. Starting WCS for the First Time



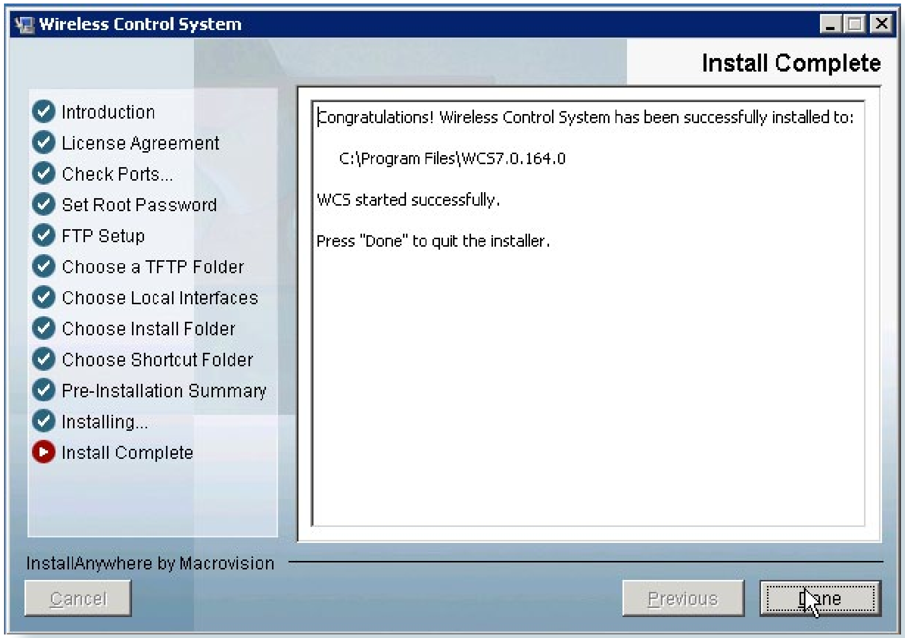
Cisco Wireless Control System 7.0.164.0

Starting WCS... This may take a few minutes...

7.0.164.0 is being
ke a moment...

Click **Done** to close the installation application. You are now running Cisco WCS.

Figure 11. Installation Complete



Congratulations! Wireless Control System has been successfully installed to:

C:\Program Files\WCS7.0.164.0

WCS started successfully.

Press "Done" to quit the installer.

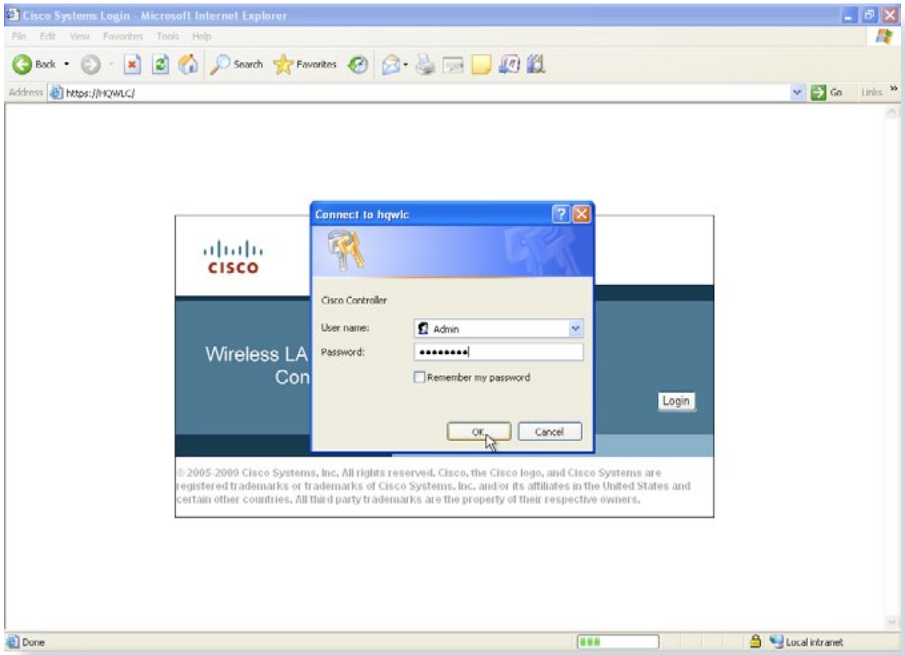
Procedure 2 Licensing

Cisco Wireless Control System (WCS) is licensed by the number of access points and services you desire. For this guide, we upload a license that includes Spectrum Intelligence as a service and 250 access points

Summary of Steps to Install the License

1. Save the license file (.lic) to a temporary directory on your hard drive. (You will receive an email from Cisco with an attached license file.)
2. Open a browser and in the location or address field, enter the following URL and replace the IP address with the IP address or host name of the Cisco WCS server: https: // <IP address>. In our example, we have Cisco WCS installed at 10.4.200.19
   https:// 10.4.200.19
3. Log into the Cisco WCS server as system administrator. (Be aware that usernames and passwords are case-sensitive.)

Figure 12. WCS Login Screen



Cisco Controller

User name: Admin

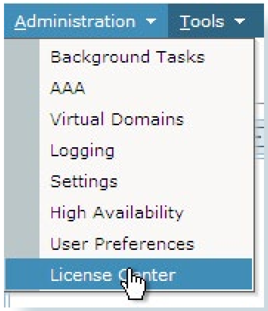
Password: ••••••••

□ Remember my password

© 2005-2009 Cisco Systems, Inc. All rights reserved. Cisco, the Cisco logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All third party trademarks are the property of their respective owners.

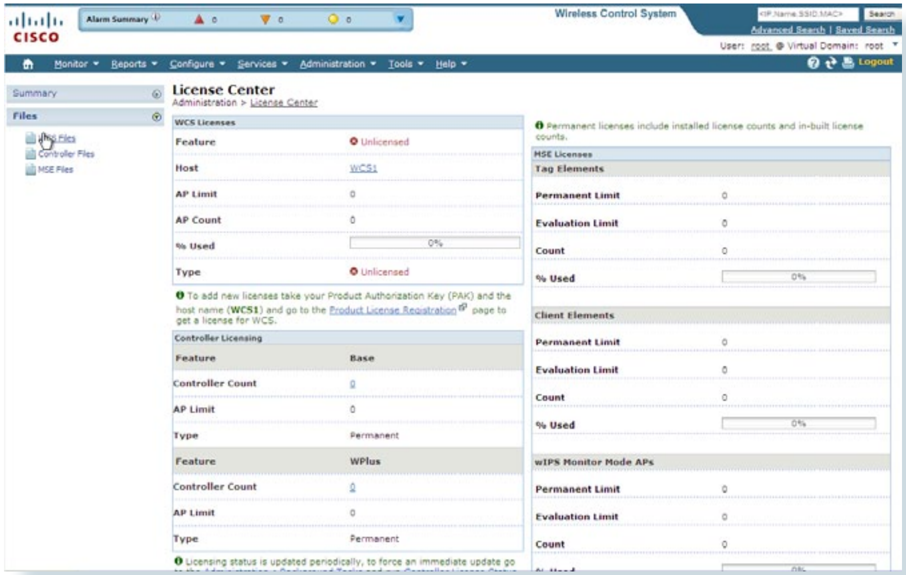
4. From the **Administration** menu, select **License Center**.

Figure 13. Navigate to License Center



5. On the right, select **Files** and then select **WCS Files**.

Figure 14. License Center, Add PAK



License Center
Administration > License Center

WCS Licenses	
Feature	Unlicensed
Host	WCS1
AP Limit	0
AP Count	0
% Used	0%
Type	Unlicensed

To add new licenses take your Product Authorization Key (PAK) and the host name (**WCS1**) and go to the Product License Registration page to get a license for WCS.

Controller Licensing	
Feature	Base
Controller Count	0
AP Limit	0
Type	Permanent
Feature	WPlus
Controller Count	0
AP Limit	0
Type	Permanent

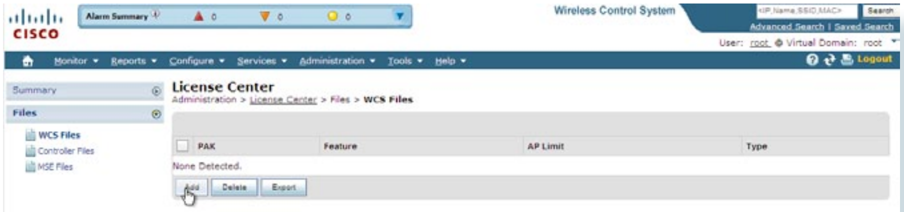
Licensing status is updated periodically, to force an immediate update go

Permanent licenses include installed license counts and in-built license counts.

MSE Licenses	
Tag Elements	
Permanent Limit	0
Evaluation Limit	0
Count	0
% Used	0%
Client Elements	
Permanent Limit	0
Evaluation Limit	0
Count	0
% Used	0%
wIPS Monitor Mode APs	
Permanent Limit	0
Evaluation Limit	0
Count	0

6. Under **PAK**, select **Add**, and click **Choose File** to navigate to the location where you saved the .lic file.

Figure 15. Add New PAK



License Center
Administration > License Center > Files > **WCS Files**

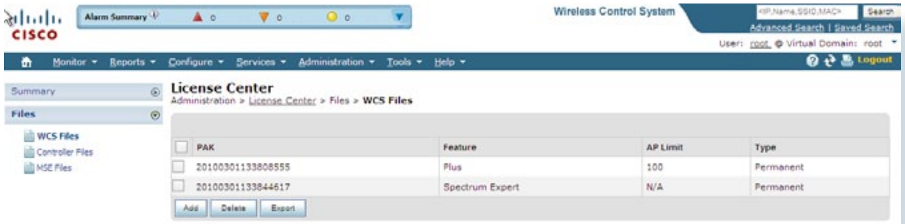
☐	PAK	Feature	AP Limit	Type

None Detected.

7. Click **Upload**. The Cisco WCS server then imports the license.

8. Repeat this step for each additional license you have received.

Figure 16. Importing License Files



License Center
Administration > License Center > Files > **WCS Files**

☐	PAK	Feature	AP Limit	Type
☐	20100301133808555	Plus	100	Permanent
☐	20100301133844617	Spectrum Expert	N/A	Permanent

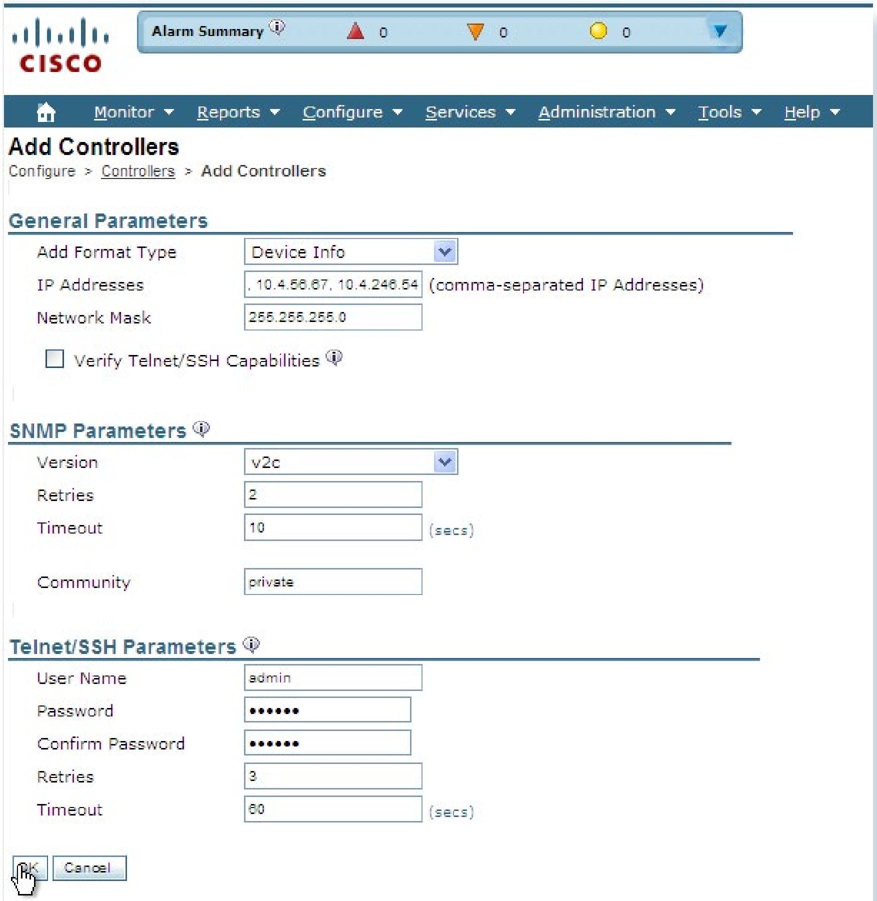
Once completed, all your license files should appear as shown in Figure 15. To verify that your license files do indeed provide the access point count and the services you ordered, return to the **Administration** menu and select **License Center**. We uploaded both Spectrum Intelligence as a service and as a single 100AP license as shown in Figure 16.

Procedure 3 Add Wireless LAN Controller(s) to Cisco WCS

Each controller must be added to Cisco WCS so the network can be monitored and centrally managed. This process is very simple, but necessary.

Navigate to **Configure** and then to **Controllers**, which should bring you to an empty list of controllers as shown in Figure 17. From the drop-down list on the right, select **Add Controllers...** and click **Go**. You are prompted to enter the Controller(s) IP address(es). (Enter all your controller IP addresses separated by a comma as shown in this example: 10.4.56.64, 10.4.56.65, 10.4.56,66, 10.4.246.54.) Use the default settings for all other parameters including the Telnet/SSH password.

Figure 17. Add Controllers



Add Controllers

Configure > Controllers > Add Controllers

General Parameters

Add Format Type	Device Info
IP Addresses	, 10.4.56.67, 10.4.246.54 (comma-separated IP Addresses)
Network Mask	255.255.255.0

□ Verify Telnet/SSH Capabilities

SNMP Parameters

Version	v2c
Retries	2
Timeout	10 (secs)
Community	private

Telnet/SSH Parameters

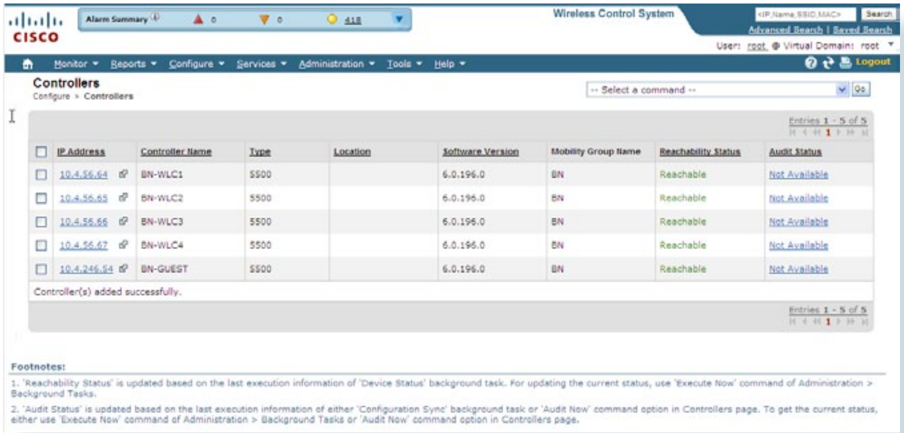
User Name	admin
Password	••••••
Confirm Password	••••••
Retries	3
Timeout	60 (secs)

Tech Tip

You may enter every controller IP address separated by a comma, or you can select a comma-delimited (CSV) spreadsheet with the IP addresses of your controllers. In our example, we selected a single controller by IP address to allow for clarification.

Click **OK**, which tests for connectivity to each controller you have specified and provides you with a list of your controllers, their hostname, and an indication if they are reachable as shown in Figure 18.

Figure 18. List of Controllers



Controllers

Configure > Controllers

□	IP Address	Controller Name	Type	Location	Software Version	Mobility Group Name	Reachability Status	Audit Status
□	10.4.56.64	BN-WLC1	5500		6.0.196.0	BN	Reachable	Not Available
□	10.4.56.65	BN-WLC2	5500		6.0.196.0	BN	Reachable	Not Available
□	10.4.56.66	BN-WLC3	5500		6.0.196.0	BN	Reachable	Not Available
□	10.4.56.67	BN-WLC4	5500		6.0.196.0	BN	Reachable	Not Available
□	10.4.246.54	BN-GUEST	5500		6.0.196.0	BN	Reachable	Not Available

Controller(s) added successfully.

Footnotes:

1. 'Reachability Status' is updated based on the last execution information of 'Device Status' background task. For updating the current status, use 'Execute Now' command of Administration > Background Tasks.
2. 'Audit Status' is updated based on the last execution information of either 'Configuration Sync' background task or 'Audit Now' command option in Controllers page. To get the current status, either use 'Execute Now' command of Administration > Background Tasks or 'Audit Now' command option in Controllers page.

To Audit the Controller immediately, select the hyperlink next to your controller initially labeled **Not Available** and then click **Audit Now**.

Upgrade Controllers for CleanAir Support

CleanAir software support for the 3502 access points and the integrated Spectrum Expert hardware begins with 7.0.98.0 or later. Managing multiple controllers with Cisco WCS is important and the ability to upgrade all five controllers simultaneously shows the true power of the Cisco Wireless Control System, this upgrade process can be then scheduled and streamlined to maximize network uptime.

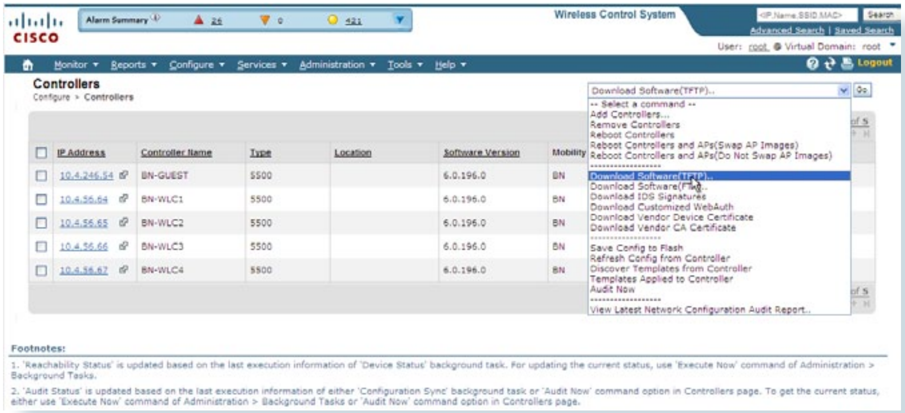
Step 1: Log into Cisco WCS

Step 2: Navigate to **Configure > Controllers**.

Step 3: Select **All Controllers**.

Step 4: From the drop-down list at the right, select **Download Software (TFTP)** and **Go**.

Figure 19. Download Software via TFTP


cisco
Alarm Summary
26
0
421
Wireless Control System
<IP,Name,SSID,MAC>
Search
Advanced Search | Saved Search
User: root Virtual Domain: root
Monitor
Reports
Configure
Services
Administration
Tools
Help
Logout
Download Software(TFTP)..
Go
-- Select a command --
Add Controllers...
Remove Controllers
Reboot Controllers
Reboot Controllers and APs(Swap AP Images)
Reboot Controllers and APs(Do Not Swap AP Images)
Download Software(TFTP)..
Download Software(FTP)..
Download IDS Signatures
Download Customized WebAuth
Download Vendor Device Certificate
Download Vendor CA Certificate
Save Config to Flash
Refresh Config from Controller
Discover Templates from Controller
Templates Applied to Controller
Audit Now
View Latest Network Configuration Audit Report..
of 5

Controllers

Configure > Controllers

□	IP Address	Controller Name	Type	Location	Software Version	Mobility
□	10.4.246.54	BN-GUEST	5500		6.0.196.0	BN
□	10.4.56.64	BN-WLC1	5500		6.0.196.0	BN
□	10.4.56.65	BN-WLC2	5500		6.0.196.0	BN
□	10.4.56.66	BN-WLC3	5500		6.0.196.0	BN
□	10.4.56.67	BN-WLC4	5500		6.0.196.0	BN

Footnotes:

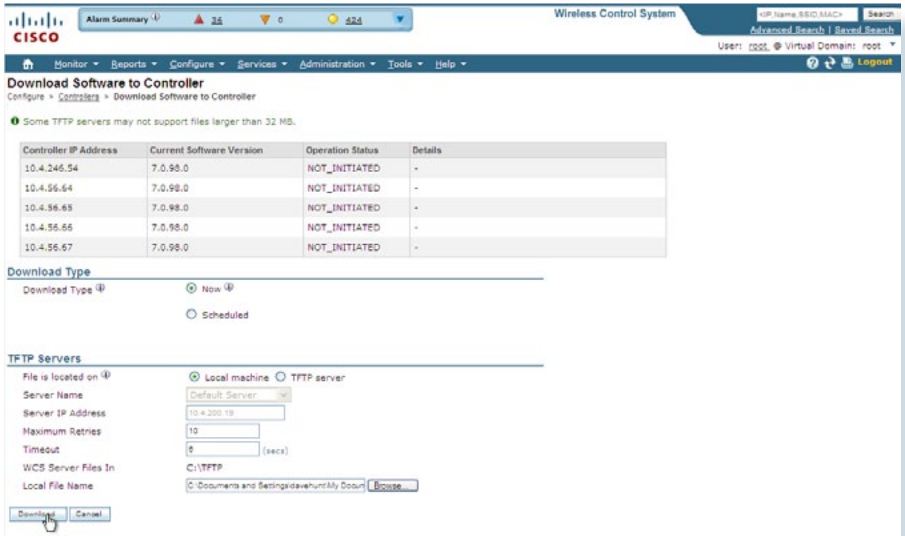
1. 'Reachability Status' is updated based on the last execution information of 'Device Status' background task. For updating the current status, use 'Execute Now' command of Administration > Background Tasks.

2. 'Audit Status' is updated based on the last execution information of either 'Configuration Sync' background task or 'Audit Now' command option in Controllers page. To get the current status, either use 'Execute Now' command of Administration > Background Tasks or 'Audit Now' command option in Controllers page.

Step 5: Answer the software controller prompts:

1. Keep **Download Type Now** Selected.
2. Keep **File is located on … Local Machine** Selected.
3. Leave **Maximum Retries** and **Timeout** at their default values.
4. From **Browse**, select the file **AIR-CT5500-K9-7-0-98-0.aes** and click **OK**.
5. Click **Download**.

Figure 20. Download Software to All Machines



Download Software to Controller

Configure > Controllers > Download Software to Controller

Some TFTP servers may not support files larger than 32 MB.

Controller IP Address	Current Software Version	Operation Status	Details
10.4.246.54	7.0.98.0	NOT_INITIATED	-
10.4.56.64	7.0.98.0	NOT_INITIATED	-
10.4.56.65	7.0.98.0	NOT_INITIATED	-
10.4.56.66	7.0.98.0	NOT_INITIATED	-
10.4.56.67	7.0.98.0	NOT_INITIATED	-

Download Type

Download Type: ● Now ○ Scheduled

TFTP Servers

File is located on: ● Local machine ○ TFTP server

Server Name: Default Server

Server IP Address: 10.4.200.19

Maximum Retries: 10

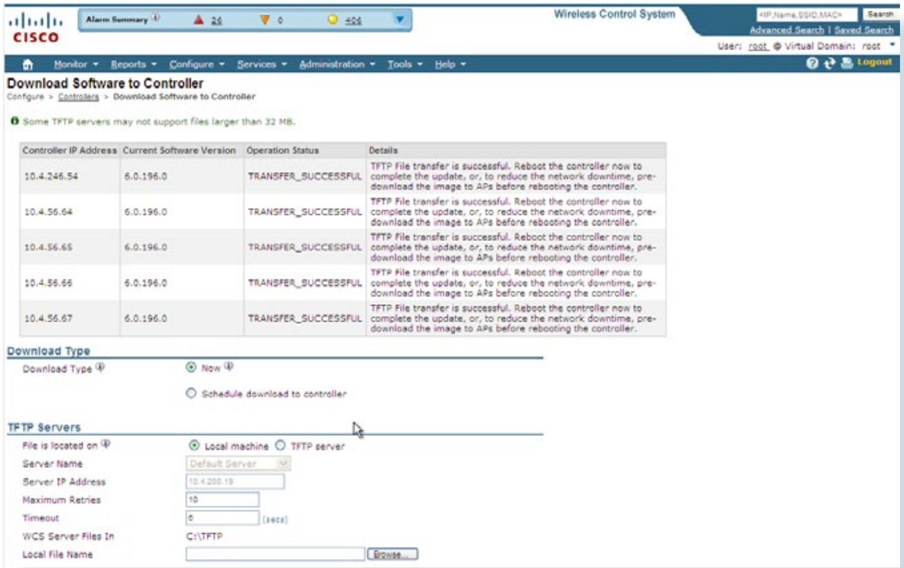
Timeout: 6 (secs)

WCS Server Files In: C:\TFTP

Local File Name: C:\Documents and Settings\davehunt\My Docum

Once the file is uploaded to every controller, you must reboot these controllers. You can do the reboot process all at once, which does not allow traffic during the upgrade, or you can schedule your controllers to reboot in a logical fashion to keep wireless connectivity available during this change opportunity.

Figure 21. Transfer Complete, Reboot Controller to Continue



Download Software to Controller

Configure > Controllers > Download Software to Controller

Some TFTP servers may not support files larger than 32 MB.

Controller IP Address	Current Software Version	Operation Status	Details
10.4.246.54	6.0.196.0	TRANSFER_SUCCESSFUL	TFTP File transfer is successful. Reboot the controller now to complete the update, or, to reduce the network downtime, pre-download the image to APs before rebooting the controller.
10.4.56.64	6.0.196.0	TRANSFER_SUCCESSFUL	TFTP File transfer is successful. Reboot the controller now to complete the update, or, to reduce the network downtime, pre-download the image to APs before rebooting the controller.
10.4.56.65	6.0.196.0	TRANSFER_SUCCESSFUL	TFTP File transfer is successful. Reboot the controller now to complete the update, or, to reduce the network downtime, pre-download the image to APs before rebooting the controller.
10.4.56.66	6.0.196.0	TRANSFER_SUCCESSFUL	TFTP File transfer is successful. Reboot the controller now to complete the update, or, to reduce the network downtime, pre-download the image to APs before rebooting the controller.
10.4.56.67	6.0.196.0	TRANSFER_SUCCESSFUL	TFTP File transfer is successful. Reboot the controller now to complete the update, or, to reduce the network downtime, pre-download the image to APs before rebooting the controller.

Download Type

Download Type ● Now

○ Schedule download to controller

TFTP Servers

File is located on ● Local machine ○ TFTP server

Server Name Default Server

Server IP Address 10.4.200.19

Maximum Retries 10

Timeout 6 (secs)

WCS Server Files In C:\TFTP

Local File Name Browse...

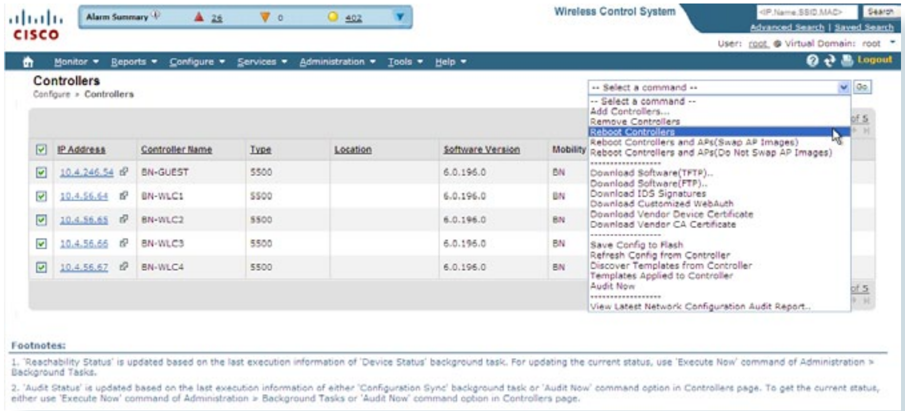
Step 1: Log into Cisco WCS.

Step 2: Navigate to **Configure > Controllers**.

Step 3: Select **All Controllers**.

Step 4: From the right drop-down list, select **Reboot Controllers**.

Figure 22. Reboot Controller


Alarm Summary
26
0
402
Wireless Control System
Search
Advanced Search | Saved Search
User: root Virtual Domain: root
Monitor
Reports
Configure
Services
Administration
Tools
Help
Logout
-- Select a command --
Go
-- Select a command --
Add Controllers...
Remove Controllers
Reboot Controllers
Reboot Controllers and APs(Swap AP Images)
Reboot Controllers and APs(Do Not Swap AP Images)
Download Software(TFTP)..
Download Software(FTP)..
Download IDS Signatures
Download Customized WebAuth
Download Vendor Device Certificate
Download Vendor CA Certificate
Save Config to Flash
Refresh Config from Controller
Discover Templates from Controller
Templates Applied to Controller
Audit Now
View Latest Network Configuration Audit Report..
of 5
of 5

Controllers

Configure > Controllers

☑	IP Address	Controller Name	Type	Location	Software Version	Mobility
☑	10.4.246.54	BN-GUEST	5500		6.0.196.0	BN
☑	10.4.56.64	BN-WLC1	5500		6.0.196.0	BN
☑	10.4.56.65	BN-WLC2	5500		6.0.196.0	BN
☑	10.4.56.66	BN-WLC3	5500		6.0.196.0	BN
☑	10.4.56.67	BN-WLC4	5500		6.0.196.0	BN

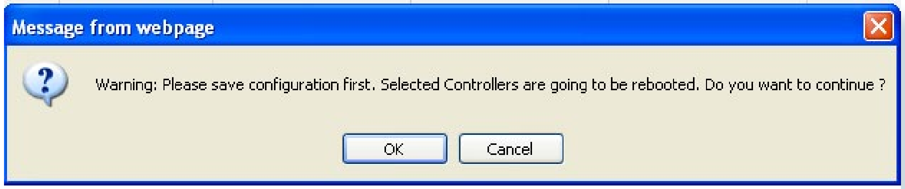
Footnotes:

1. 'Reachability Status' is updated based on the last execution information of 'Device Status' background task. For updating the current status, use 'Execute Now' command of Administration > Background Tasks.

2. 'Audit Status' is updated based on the last execution information of either 'Configuration Sync' background task or 'Audit Now' command option in Controllers page. To get the current status, either use 'Execute Now' command of Administration > Background Tasks or 'Audit Now' command option in Controllers page.

Step 5: Click **OK** to the Warning “**Warning: Please save configuration first. Selected Controllers are going to be rebooted. Do you want to continue?**”

Figure 23. Warning: You Are About to Reload Your Controller!



Message from webpage

Warning: Please save configuration first. Selected Controllers are going to be rebooted. Do you want to continue ?

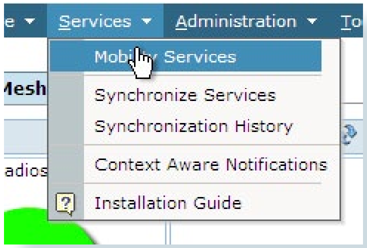
Procedure 4 Add the Mobility Service Engine

You must add the Mobility Service Engine to the Wireless Control System. Using the WCS Comunication username and password that you used earlier will allow Cisco WCS to poll the MSE database for historical context information. At a later time, Wireless Intrusion Prevention System services can be added if needed.

Step 1: Log into WCS.

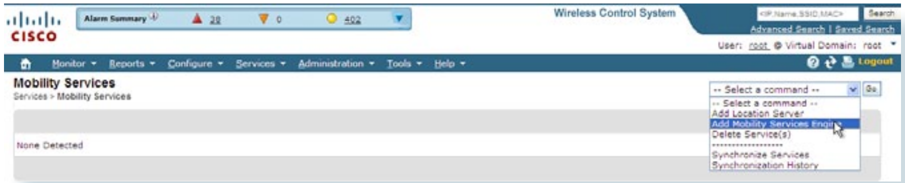
Step 2: Navigate to **Services > Mobility Services**.

Figure 24. New Mobility Service



Step 3: From the drop-down list, select Add Mobility Services Engine and click Go.

Figure 25. Add Mobility Service Engine



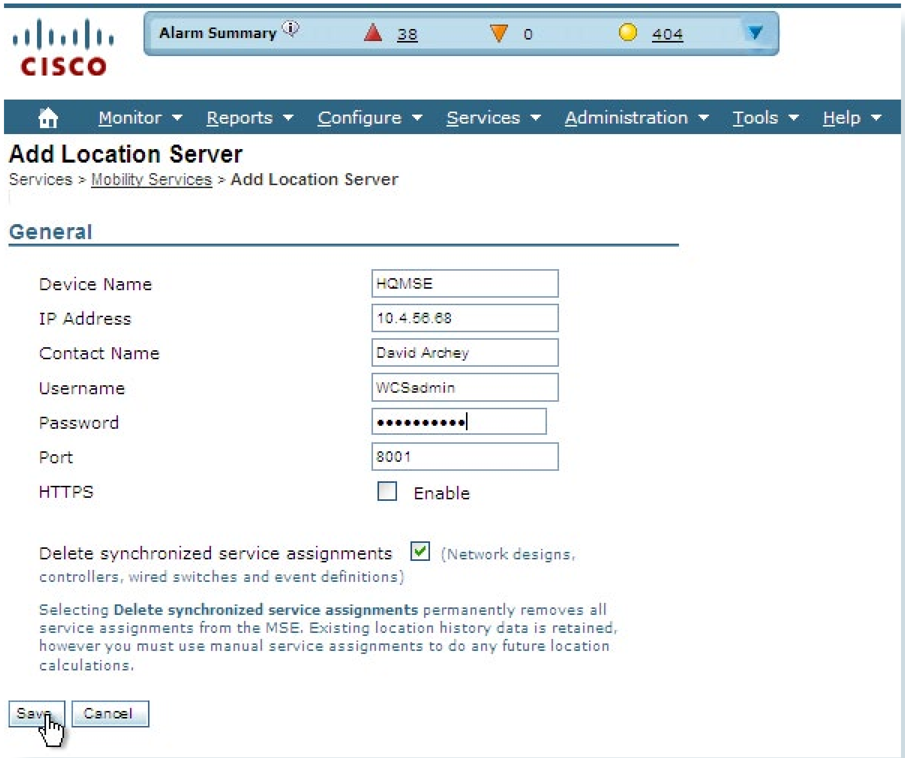
Mobility Services
Services > Mobility Services

None Detected

Step 4: Enter the following information and click **Save**:

1. Device name
2. IP address
3. Contact name
4. Username (WCS communication username)
5. Password (WCS communication password)
6. Port (accept the default)

Figure 26. Define New MSE and Communication Credentials



Add Location Server
Services > Mobility Services > Add Location Server

General

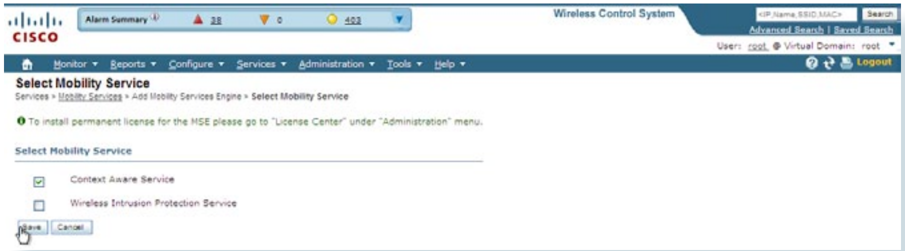
Device Name HQMSE
IP Address 10.4.56.68
Contact Name David Archey
Username WCSadmin
Password ••••••••••
Port 8001
HTTPS □ Enable

Delete synchronized service assignments ☑ (Network designs, controllers, wired switches and event definitions)

Selecting **Delete synchronized service assignments** permanently removes all service assignments from the MSE. Existing location history data is retained, however you must use manual service assignments to do any future location calculations.

Step 5: Check the **Context Aware Service** check box and click **Save**.

Figure 27. Select Mobility Engine Services



Select Mobility Service
Services > Mobility Services > Add Mobility Services Engine > Select Mobility Service

To install permanent license for the MSE please go to "License Center" under "Administration" menu.

Select Mobility Service

☑ Context Aware Service
□ Wireless Intrusion Protection Service

Procedure 5 Building and Floor Plan

The real advantage to any management system is the presentation of the information, which you can then use to make informed decisions. The Cisco Wireless Control System brings visibility to the radio spectrum, which allows the administrator to see the coverage that is provided to the users. Including the building and floorplans in Cisco WCS creates the visibility to this otherwise unknown or convoluted data that the network provides.

Adding the First Campus and Building

Every organizational method starts by categorizing the approach; with the Cisco Wireless Control System, the approach is familiar. Even though you may only have one building today, you may end up with another building, or perhaps each Campus is a single building today, but could have more buildings tomorrow. The campus, building, floor approach makes it easy to understand as you dig for more information and peel away the layers to find what you are looking for.

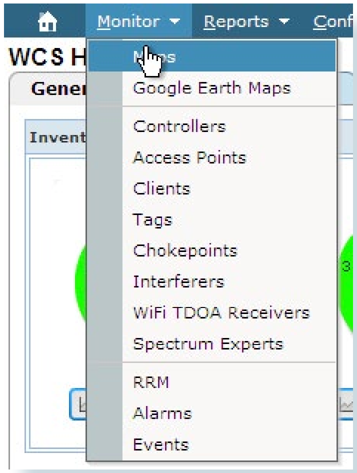
Tech Tip

You need to know the dimension of the campus picture you are bringing into the system so that you can scale the drawing appropriately as each building and floor are added.

Step 1: Log into the Wireless Control System.

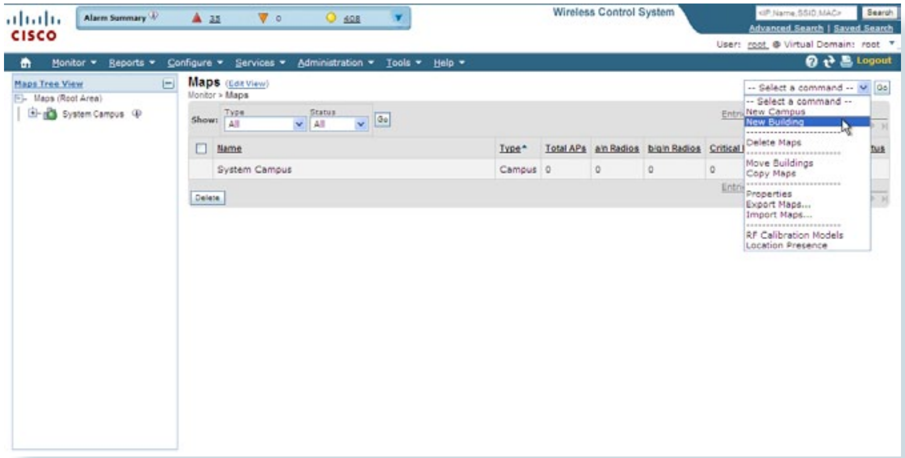
Step 2: Navigate to **Monitor** > **Maps**.

Figure 28. Finding Building Maps



Step 3: From the drop-down list, select **New Building** and click **Go**.

Figure 29. New Building

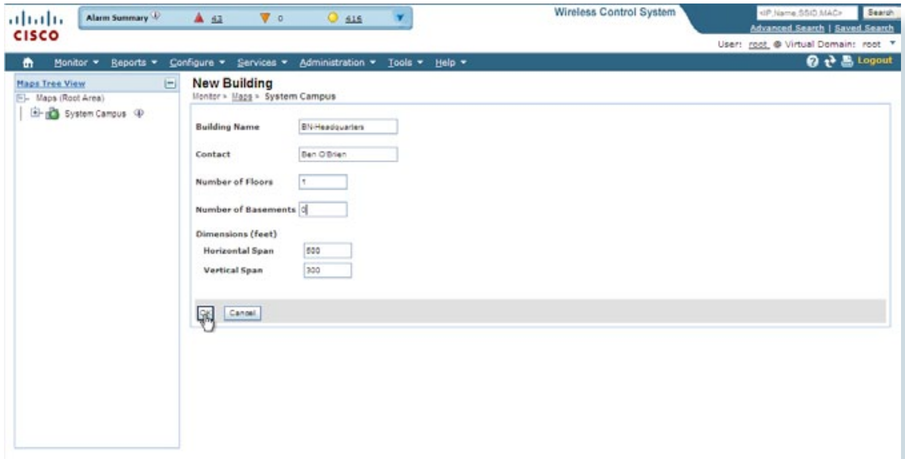


Name	Type	Total APs	a/n Radios	b/g/n Radios	Critical
System Campus	Campus	0	0	0	0

Step 4: Create name, contact name, and characteristics of the building:

- **Building Name:** BN-Headquarters
- **Contact:** Ben O'Brien
- **Number of floors:** 1
- **Number of Basements:** 0
- **Horizontal Span (feet):** 500
- **Vertical Span (feet):** 300

Figure 30. Building Details



New Building

Monitor » Maps » System Campus

Building Name: BN-Headquarters

Contact: Ben O'Brien

Number of Floors: 1

Number of Basements: 0

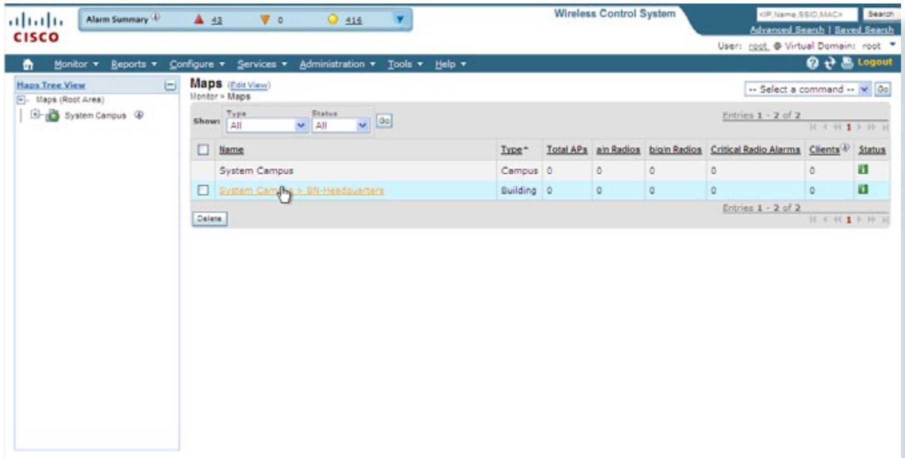
Dimensions (feet)

Horizontal Span: 500

Vertical Span: 300

Step 5: Select your newly created building.

Figure 31. Select New Campus



Maps (Edit View)

Monitor » Maps

Show: Type All, Status All

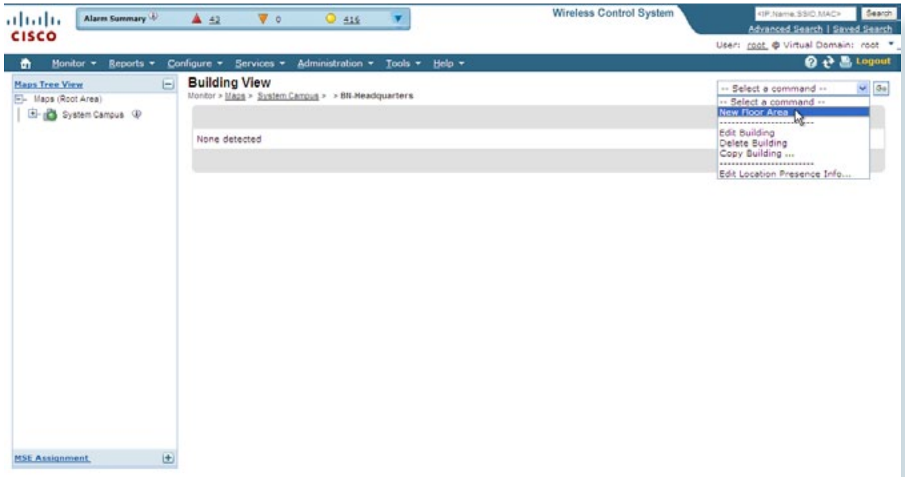
Entries 1 - 2 of 2

	Name	Type	Total APs	a/n Radios	b/g/n Radios	Critical Radio Alarms	Clients	Status
	System Campus	Campus	0	0	0	0	0	🟩
□	System Campus > BN-Headquarters	Building	0	0	0	0	0	🟩

Entries 1 - 2 of 2

Step 6: Select **New Floor Area** from the drop-down menu and click **Go**.

Figure 32. New Floor Area



Building View

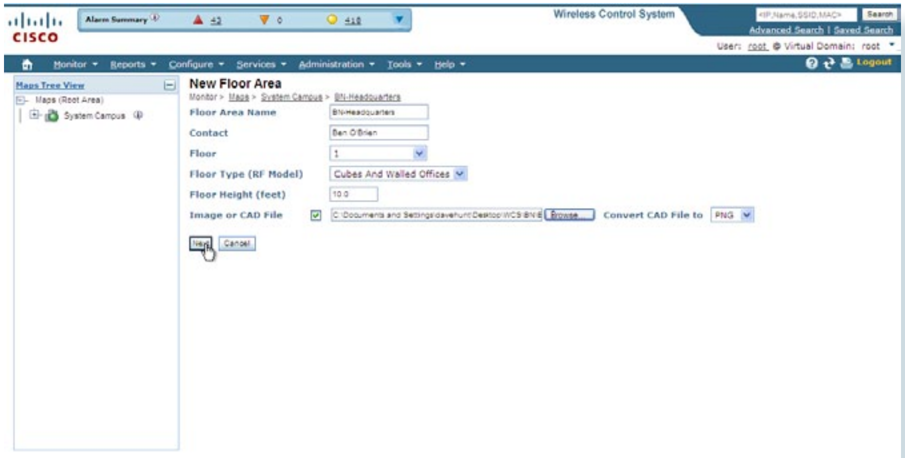
Monitor > Maps > System Campus > > BN-Headquarters

None detected

Step 7: Create a floor name, contact name, floor number, and a description of the area. Select the floor plan image. Click **Next**:

- **Floor Area Name:** BN-Headqaurters
- **Contact:** Ben O'Brien
- **Floor:** 1 (selected from drop-down list)
- **Floor Type (RF Model):** Cubes And Walled Offices (select from the drop-down list)
- **Floor Height (feet):** 10.0
- **Image or CAD File:** C:\Documents and Settings\BN-Headquarters.png
- **Convert CAD File to:** PNG (Accept the default drop-down selection)

Figure 33. New Floor Details and Image Upload



New Floor Area

Monitor > Maps > System Campus > BN-Headquarters

Floor Area Name: BN-Headquarters

Contact: Ben O'Brien

Floor: 1

Floor Type (RF Model): Cubes And Walled Offices

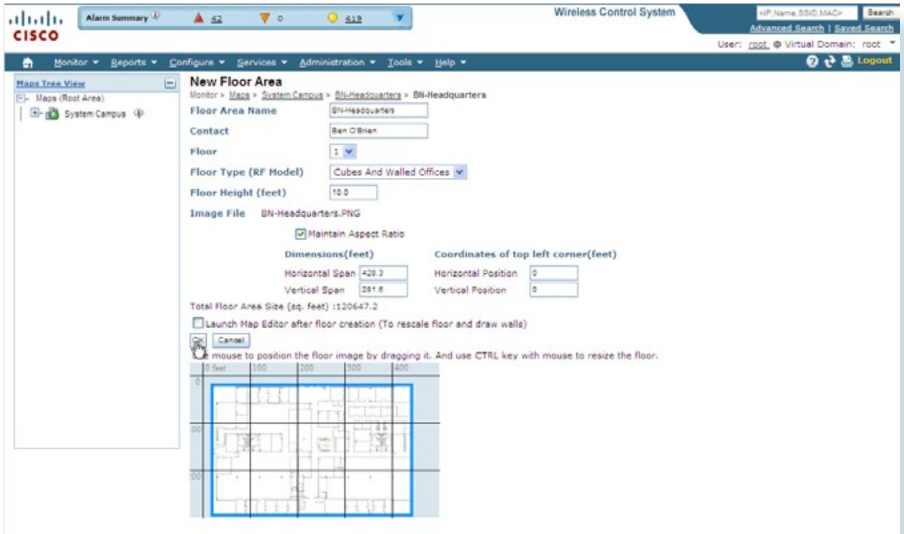
Floor Height (feet): 10.0

Image or CAD File: ☑ C:\Documents and Settings\davehunt\Desktop\WCS\BN\E

Convert CAD File to: PNG

Step 8: Verify your new floor area details and image and click **OK**.

Figure 34. Verify New Floor Details



New Floor Area

Monitor > Maps > System Campus > BN-Headquarters > BN-Headquarters

Floor Area Name: BN-Headquarters

Contact: Ben O'Brien

Floor: 1

Floor Type (RF Model): Cubes And Walled Offices

Floor Height (feet): 10.0

Image File: BN-Headquarters.PNG

☑ Maintain Aspect Ratio

Dimensions(feet)

Horizontal Span: 428.3

Vertical Span: 281.6

Coordinates of top left corner(feet)

Horizontal Position: 0

Vertical Position: 0

Total Floor Area Size (sq. feet) :120647.2

□ Launch Map Editor after floor creation (To rescale floor and draw walls)

mouse to position the floor image by dragging it. And use CTRL key with mouse to resize the floor.

Place Access Points

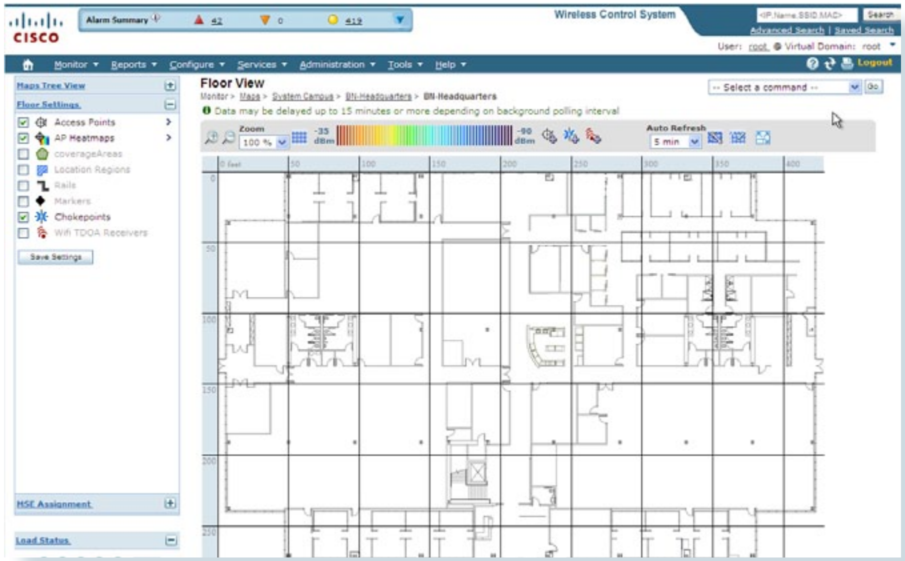
The final piece of the puzzle is to place the access points at the proper location on your individual floorplans. The Wireless LAN Controllers that work in conjunction with the Cisco Wireless Control System give an accurate view and device location, if you take the time to place your access points where they actually are located.

Step 1: Log into Cisco WCS.

Step 2: Navigate to **Monitor > Maps**.

Step 3: Select your new Floor plan, **BN-Headquarters**.

Figure 35. Floor View



Floor View

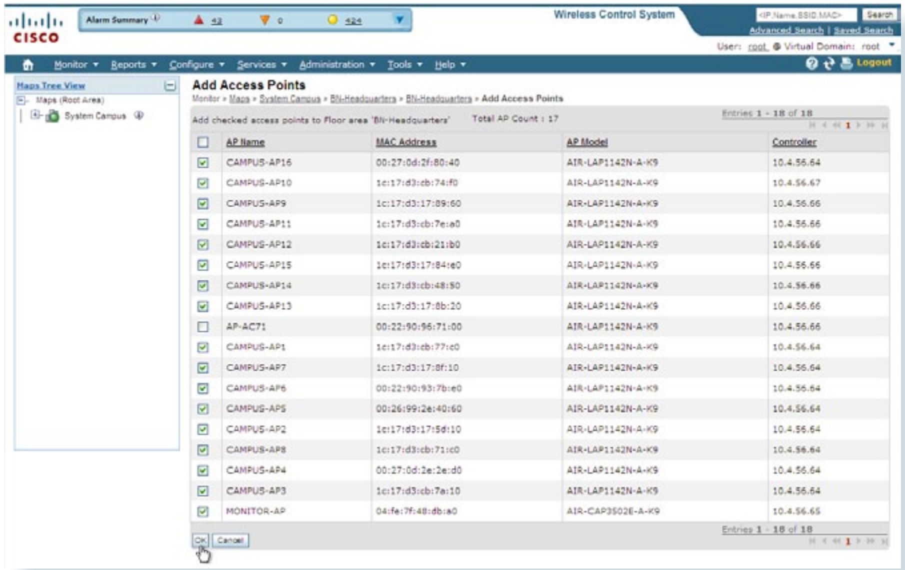
Monitor > Maps > System Campus > BN-Headquarters > BN-Headquarters

Data may be delayed up to 15 minutes or more depending on background polling interval

Step 4: From the right drop-down list, select **Add Access Points** and click **Go**.

Step 5: Select access points that are registered with the system but not yet placed for the headquarters building.

Figure 36. Select APs to Place on New Floor



Add Access Points

Monitor » Maps » System Campus » BN-Headquarters » BN-Headquarters » Add Access Points

Add checked access points to Floor area 'BN-Headquarters' Total AP Count : 17

Entries 1 - 18 of 18

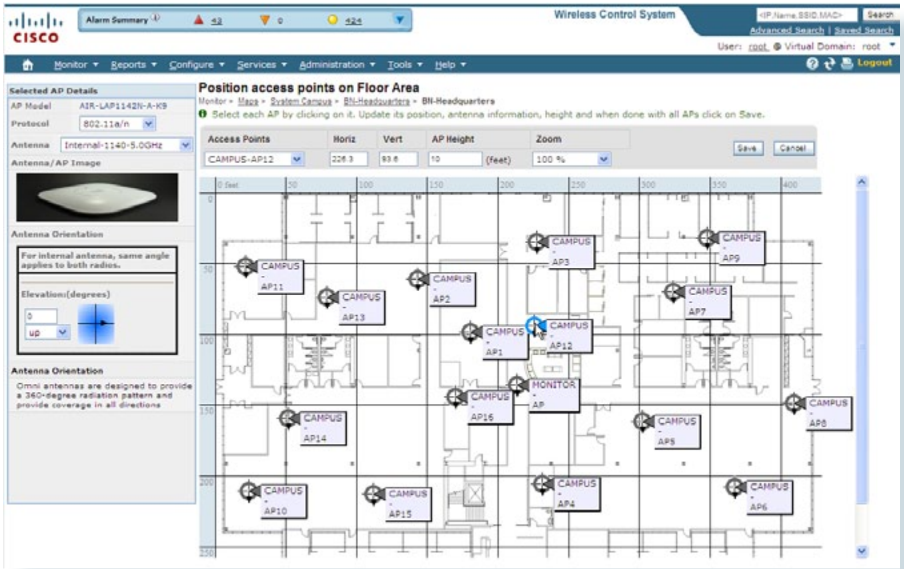
□	AP Name	MAC Address	AP Model	Controller
☑	CAMPUS-AP16	00:27:0d:2f:80:40	AIR-LAP1142N-A-K9	10.4.56.64
☑	CAMPUS-AP10	1c:17:d3:cb:74:f0	AIR-LAP1142N-A-K9	10.4.56.67
☑	CAMPUS-AP9	1c:17:d3:17:89:60	AIR-LAP1142N-A-K9	10.4.56.66
☑	CAMPUS-AP11	1c:17:d3:cb:7e:a0	AIR-LAP1142N-A-K9	10.4.56.66
☑	CAMPUS-AP12	1c:17:d3:cb:21:b0	AIR-LAP1142N-A-K9	10.4.56.66
☑	CAMPUS-AP15	1c:17:d3:17:84:e0	AIR-LAP1142N-A-K9	10.4.56.66
☑	CAMPUS-AP14	1c:17:d3:cb:48:50	AIR-LAP1142N-A-K9	10.4.56.66
☑	CAMPUS-AP13	1c:17:d3:17:8b:20	AIR-LAP1142N-A-K9	10.4.56.66
□	AP-AC71	00:22:90:96:71:00	AIR-LAP1142N-A-K9	10.4.56.66
☑	CAMPUS-AP1	1c:17:d3:cb:77:c0	AIR-LAP1142N-A-K9	10.4.56.64
☑	CAMPUS-AP7	1c:17:d3:17:8f:10	AIR-LAP1142N-A-K9	10.4.56.64
☑	CAMPUS-AP6	00:22:90:93:7b:e0	AIR-LAP1142N-A-K9	10.4.56.64
☑	CAMPUS-AP5	00:26:99:2e:40:60	AIR-LAP1142N-A-K9	10.4.56.64
☑	CAMPUS-AP2	1c:17:d3:17:5d:10	AIR-LAP1142N-A-K9	10.4.56.64
☑	CAMPUS-AP8	1c:17:d3:cb:71:c0	AIR-LAP1142N-A-K9	10.4.56.64
☑	CAMPUS-AP4	00:27:0d:2e:2e:d0	AIR-LAP1142N-A-K9	10.4.56.64
☑	CAMPUS-AP3	1c:17:d3:cb:7a:10	AIR-LAP1142N-A-K9	10.4.56.64
☑	MONITOR-AP	04:fe:7f:48:db:a0	AIR-CAP3502E-A-K9	10.4.56.65

Entries 1 - 18 of 18

OK Cancel

Step 6: Carefully place each access point as close to its real position in the building as possible and click **Save**.

Figure 37. AP Placement



User: root Virtual Domain: root

Selected AP Details

AP Model: AIR-LAP1142N-A-K9

Protocol: 802.11a/n

Antenna: Internal-1140-5.0GHz

Antenna/AP Image

Antenna Orientation

For internal antenna, same angle applies to both radios.

Elevation:(degrees) 0 up

Antenna Orientation

Omni antennas are designed to provide a 360-degree radiation pattern and provide coverage in all directions

Position access points on Floor Area

Monitor > Maps > System Campus > BN-Headquarters > BN-Headquarters

Select each AP by clicking on it. Update its position, antenna information, height and when done with all APs click on Save.

Access Points	Horiz	Vert	AP Height	Zoom
CAMPUS-AP12	226.3	93.6	10 (feet)	100 %

Tech Tip

You must now wait while the system calculates the heatmaps from the placement and floorplan area.

Notes

Configuring the Cisco Wireless Solution for CleanAir

The Wireless LAN controller with the connected Cisco AIR-CAP3500 access points is immediately CleanAir capable. The Wireless LAN controllers can give you immediate information about your environment. Where the WCS can take a network view, the WLC only displays data retrieved from the locally connected CleanAir access points.

With the Cisco Wireless Control System in the network, all management will be handled at the WCS. Management can be done at each controller, but we do not recommend this. With the CleanAir access point operating from the wireless LAN Controller, we can log into the Cisco Wireless Control System and configure our controller to support CleanAir.

Event-Driven Radio Resource Management (EDRRM)

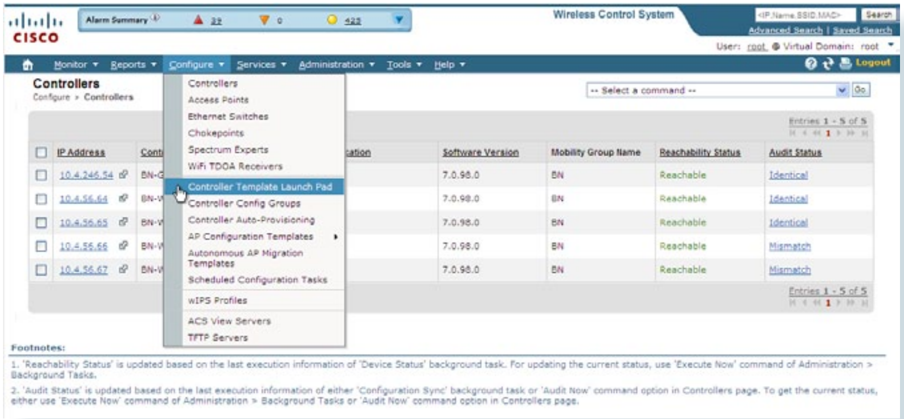
Event-Driven RRM is a feature that allows an access point that is in distress to bypass normal RRM intervals and immediately change channels. A CleanAir access point always monitors AirQuality (AQ), and reports on AQ in 15 second intervals. AirQuality is a better metric than relying on normal Wi-Fi chip noise measurements because AQ only reports on classified interference devices. That makes AQ a reliable metric in that we know what is reported is not because of Wi-Fi energy (and hence is not a transient normal spike).

The key benefit of the EDRRM is very fast action time (30 seconds). If an interferer is operating on an active channel and is causing enough AQ degradation that it triggers EDRRM, then no clients will be able to use that access point or channel. The only thing to do is get the access point off that channel. The EDRRM feature is not enabled by default and must be enabled. This process has two steps: enable CleanAir and then enable Event-Driven RRM.

Step 1: Log into Cisco WCS.

Step 2: Navigate to **Configure > Controller Template Launch Pad**.

Figure 38. Controller Templates



Controllers

Configure > Controllers

□	IP Address	Conti	ation	Software Version	Mobility Group Name	Reachability Status	Audit Status
□	10.4.246.54	BN-G		7.0.98.0	BN	Reachable	Identical
□	10.4.56.64	BN-W		7.0.98.0	BN	Reachable	Identical
□	10.4.56.65	BN-W		7.0.98.0	BN	Reachable	Identical
□	10.4.56.66	BN-W		7.0.98.0	BN	Reachable	Mismatch
□	10.4.56.67	BN-W		7.0.98.0	BN	Reachable	Mismatch

Footnotes:

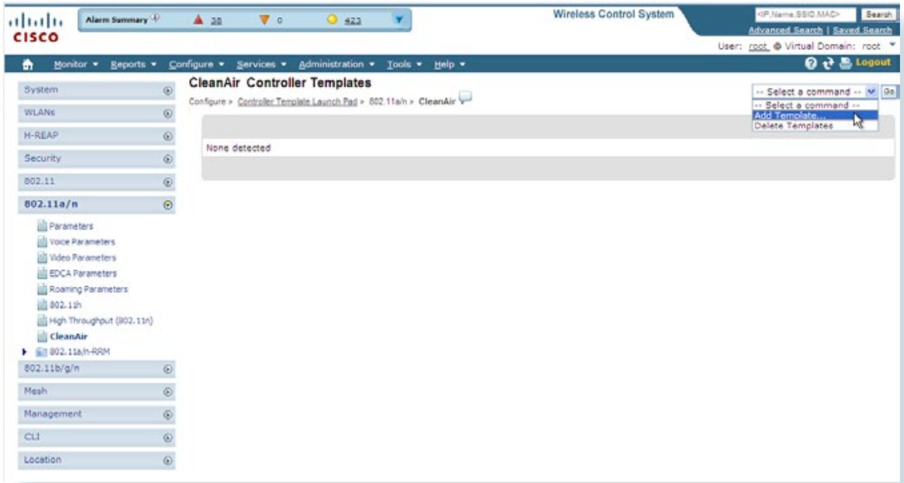
1. 'Reachability Status' is updated based on the last execution information of 'Device Status' background task. For updating the current status, use 'Execute Now' command of Administration > Background Tasks.

2. 'Audit Status' is updated based on the last execution information of either 'Configuration Sync' background task or 'Audit Now' command option in Controllers page. To get the current status, either use 'Execute Now' command of Administration > Background Tasks or 'Audit Now' command option in Controllers page.

Step 3: Navigate to **802.11a/n > CleanAir**.

Step 4: From the drop-down list, select **Add Template**.

Figure 39. Add 802.11a/n CleanAir Template



CleanAir Controller Templates

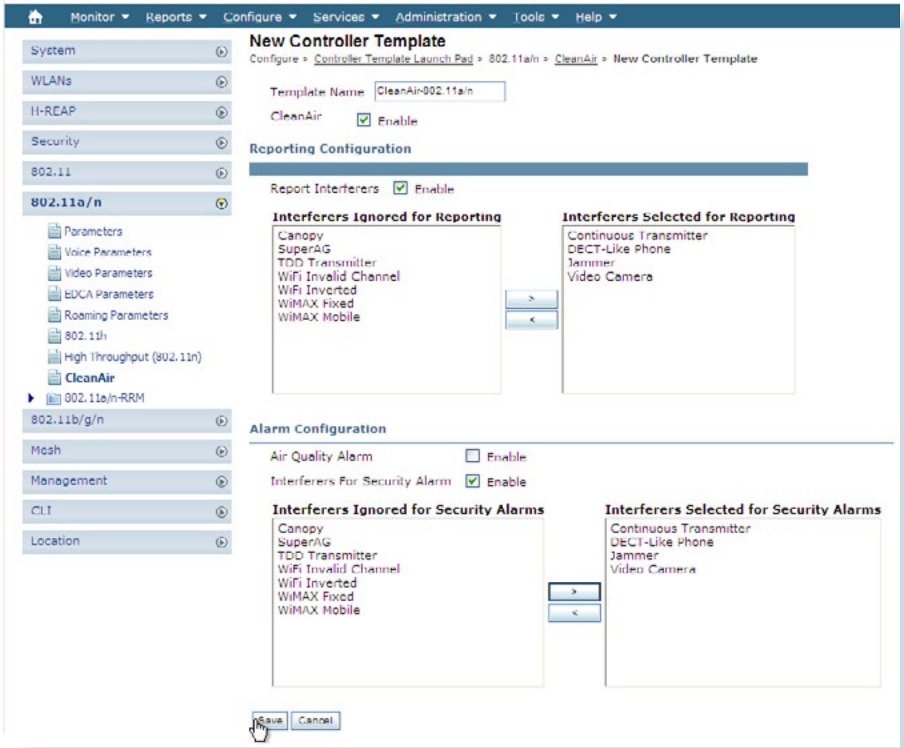
Configure > Controller Template Launch Pad > 802.11a/n > CleanAir

None detected

Step 5: Create a template name (for example, CleanAir-802.11a/n) and provide the following information:

1. Check the **CleanAir Enable** check box.
2. Check the **Report Interferers Enable** check box.
3. Add Continuous Transmitter, DECT-Like Phone, Jammer and Video Camera to **Interferers Selected for Reporting**.
4. Check the **Interferers For Security Alarm Enable** check box.
5. Add Continuous Transmitter, DECT-Like Phone, Jammer and Video Camera to **Interferers Selected for Security Alarms**
6. Select **Save**.

Figure 40. 802.11a/n CleanAir Parameters



New Controller Template

Configure > Controller Template Launch Pad > 802.11a/n > CleanAir > New Controller Template

Template Name: CleanAir-802.11a/n

CleanAir ☑ Enable

Reporting Configuration

Report Interferers ☑ Enable

Interferers Ignored for Reporting: Canopy, SuperAG, TDD Transmitter, WiFi Invalid Channel, WiFi Inverted, WiMAX Fixed, WiMAX Mobile

Interferers Selected for Reporting: Continuous Transmitter, DECT-Like Phone, Jammer, Video Camera

Alarm Configuration

Air Quality Alarm ☐ Enable

Interferers For Security Alarm ☑ Enable

Interferers Ignored for Security Alarms: Canopy, SuperAG, TDD Transmitter, WiFi Invalid Channel, WiFi Inverted, WiMAX Fixed, WiMAX Mobile

Interferers Selected for Security Alarms: Continuous Transmitter, DECT-Like Phone, Jammer, Video Camera

Step 6: Select **Apply to Controllers...**.

Step 7: Select **ALL Controllers** and click **OK**.

Step 8: Navigate to **Configure > Controller Template Launch Pad**.

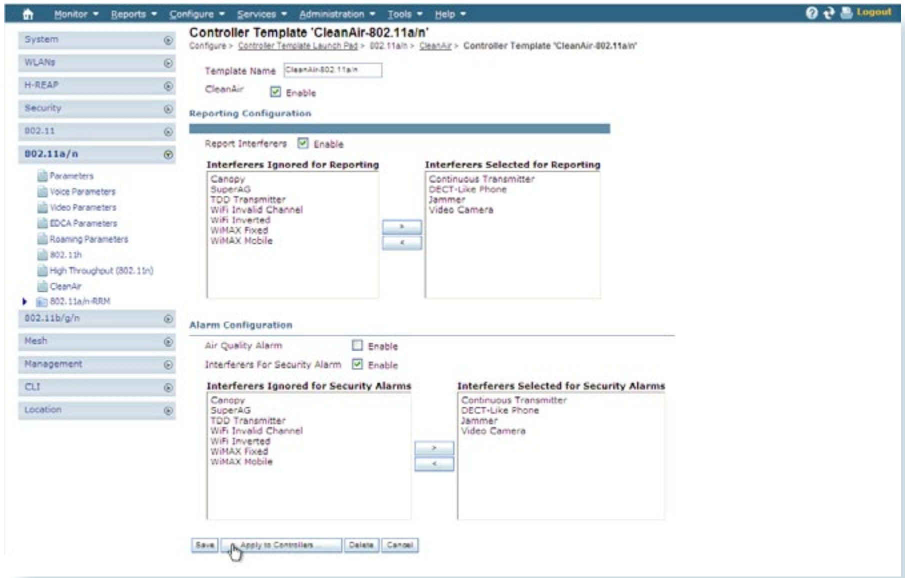
Step 9: Navigate to **802.11b/g/n > CleanAir**.

Step 10: From the drop-down list, select **Add Template**.

Step 11: Create a template name (for example, CleanAir-802.11b/g/n) and provide the following information:

1. Check the **CleanAir Enable** check box.
2. Check the **Report Interferers Enable** check box.
3. Add Continuous Transmitter, DECT-Like Phone, Jammer, Microwave Oven and Video Camera to **Interferers Selected for Reporting**.
4. Check the **Interferers For Security Alarm Enable** check box.
5. Add Continuous Transmitter, DECT-Like Phone, Jammer, Microwave Oven and Video Camera to **Interferers Selected for Security Alarms**.
6. Click **Save**.

Figure 41. 802.11b/g/n CleanAir Parameters



Controller Template 'CleanAir-802.11a/n'

Configure > Controller Template Launch Pad > 802.11a/n > CleanAir > Controller Template 'CleanAir-802.11a/n'

Template Name: CleanAir-802.11a/n

CleanAir ☑ Enable

Reporting Configuration

Report Interferers ☑ Enable

Interferers Ignored for Reporting: Canopy, SuperAG, TDD Transmitter, WiFi Invalid Channel, WiFi Inverted, WiMAX Fixed, WiMAX Mobile

Interferers Selected for Reporting: Continuous Transmitter, DECT-Like Phone, Jammer, Video Camera

Alarm Configuration

Air Quality Alarm ☐ Enable

Interferers For Security Alarm ☑ Enable

Interferers Ignored for Security Alarms: Canopy, SuperAG, TDD Transmitter, WiFi Invalid Channel, WiFi Inverted, WiMAX Fixed, WiMAX Mobile

Interferers Selected for Security Alarms: Continuous Transmitter, DECT-Like Phone, Jammer, Video Camera

Step 12: Select **Apply to Controllers...**.

Step 13: Select **ALL Controllers** and click **OK**.

Enable Event Driven Radio Resource Management

Step 1: Navigate to **Configure > Controller Template Launch Pad**.

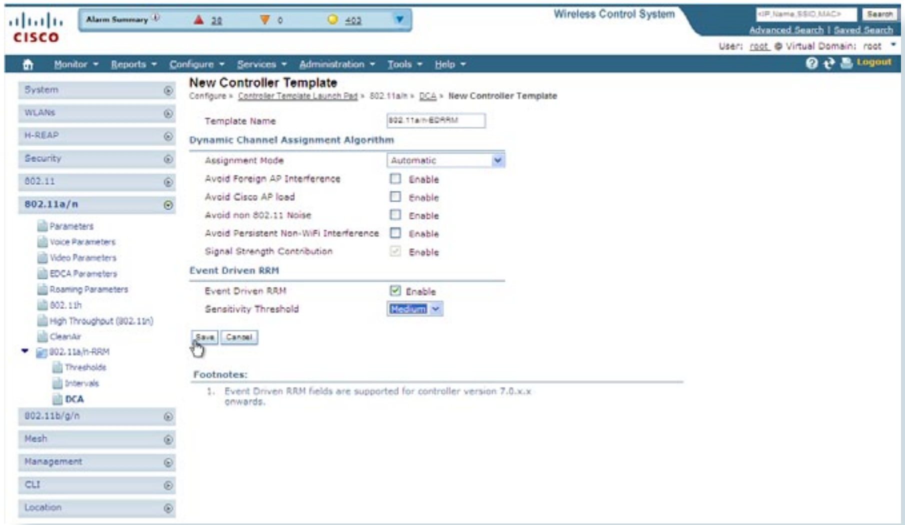
Step 2: From the left menu, navigate to **802.11a/n > 802.11a/n-RRM > DCA**.

Step 3: Select **Add Template**.

Step 4: Create a template name as follows:

1. Check the **Event Driven RRM Enable** check box.
2. Change the **Sensitivity Threshold** to **Medium**.
3. Click **Save**.

Figure 42. 802.11a/n Event Driven Enable



New Controller Template

Configure > Controller Template Launch Pad > 802.11a/n > DCA > New Controller Template

Template Name: 802.11a/n-EDRRM

Dynamic Channel Assignment Algorithm

Assignment Mode: Automatic

Avoid Foreign AP Interference: □ Enable

Avoid Cisco AP load: □ Enable

Avoid non 802.11 Noise: □ Enable

Avoid Persistent Non-WiFi Interference: □ Enable

Signal Strength Contribution: ☑ Enable

Event Driven RRM

Event Driven RRM: ☑ Enable

Sensitivity Threshold: Medium

Footnotes:

1. Event Driven RRM fields are supported for controller version 7.0.x.x onwards.

Step 5: Select **Apply to Controllers....**

Step 6: Leave **Apply to controllers selected directly** and check **All Controllers** and click **OK**.

Step 7: Navigate to **Configure > Controller Template Launch Pad**.

Step 8: From the left menu, navigate to **802.11b/g/n > 802.11b/g/n-RRM > DCA**.

Step 9: Select **Add Template**.

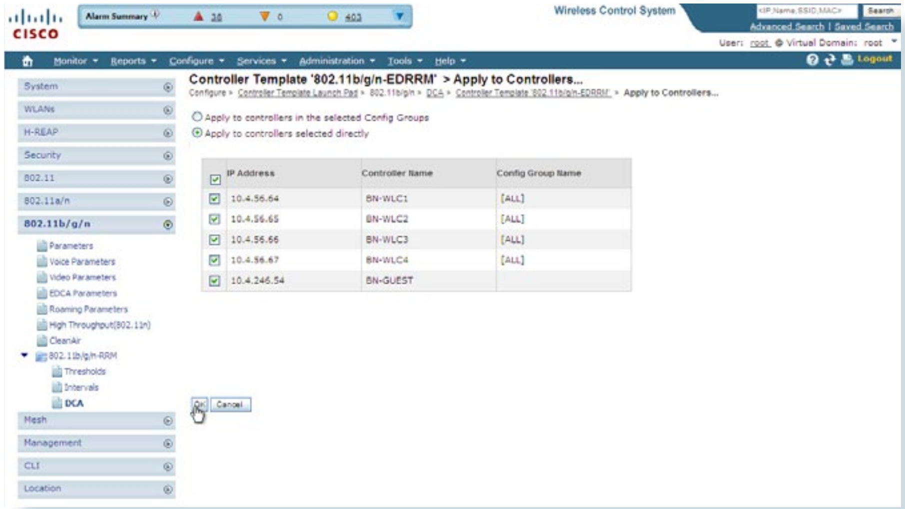
Step 10: Create a template name as follows:

1. Check the **Event Driven RRM Enable** check box.
2. Change the **Sensitivity Threshold** to **Medium**.
3. Click **Save**.

Step 11: Select **Apply to Controllers....**

Step 12: Leave **Apply to controllers selected directly** and check **All Controllers** and click **OK**.

Figure 43. Apply to All Controllers



Controller Template '802.11b/g/n-EDRRM' > Apply to Controllers...

Configure > Controller Template Launch Pad > 802.11b/g/n > DCA > Controller Template '802.11b/g/n-EDRRM' > Apply to Controllers...

○ Apply to controllers in the selected Config Groups

● Apply to controllers selected directly

☑	IP Address	Controller Name	Config Group Name
☑	10.4.56.64	BN-WLC1	[ALL]
☑	10.4.56.65	BN-WLC2	[ALL]
☑	10.4.56.66	BN-WLC3	[ALL]
☑	10.4.56.67	BN-WLC4	[ALL]
☑	10.4.246.54	BN-GUEST	

Troubleshooting with CleanAir

The real power of CleanAir is that a network administrator can be on one continent while the Wi-Fi spectrum in another office on the other side of the planet can be analyzed directly. The 3500 access points can be put in SE-Connect mode and used as a virtual remote interface for the knowledgeable engineer no matter where this valuable human resource is located. By changing the role of your CleanAir access point and connecting the Spectrum Expert 4.0 software, the Wi-Fi network administrator can now view the environment directly. There is no longer a need to fly expensive personnel onsite to troubleshoot physical layer issues that are unknown and challenging and, too often, intermittent issues.

Accessing Remote CleanAir for Spectrum Connect

When the call for assistance arrives, it is almost certainly to be in a location that does not have the knowledgeable human resources to troubleshoot, identify, and fix the issue. Wi-Fi radios are designed to send and receive Wi-Fi signals, but they do not have the capability to identify non-Wi-Fi radio interferers such as microwave ovens, DECT phones, analog wireless cameras, or even radio jammers. The specialized radios in the CleanAir radio can identify and, with triangulation, can locate where these devices are located.

When the call comes in, it is always important to identify as many facts about the issue to make informed decisions. The information can be the location of the problem (for example, “the street side of the building does not have connectivity”) and time of day (for example, “the issue is pronounced at lunch time”). With as much information from the end user as possible, it is now time to look at the radio environment because the system shows that clients are connecting and WCS indicates AirQuality has dropped.

Configure Spectrum Connect

The CleanAir-capable access point must be changed from either Monitor Mode or Local Mode of operation to Spectrum Connect Mode.

Step 1: Log into the Wireless LAN Controller

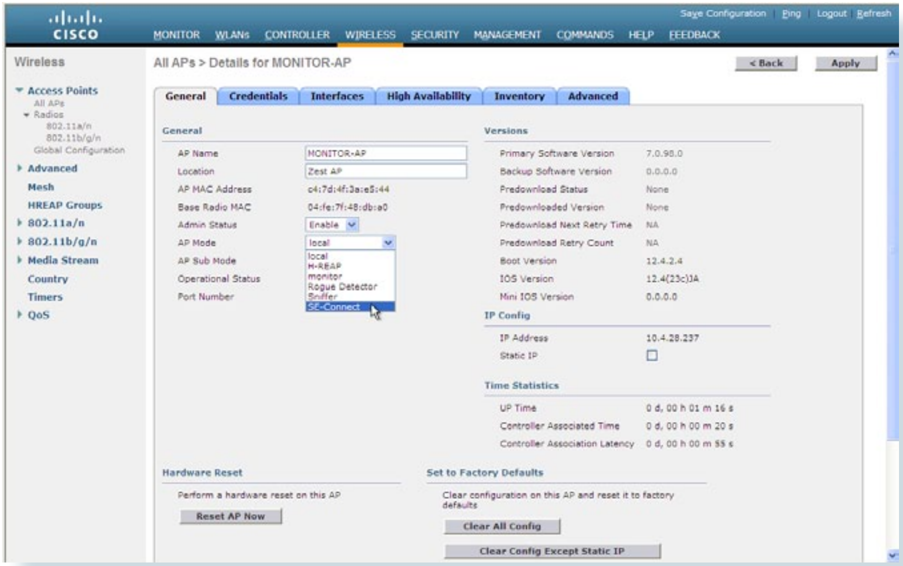
Step 2: Navigate to **WIRELESS**.

Step 3: Select the closest CleanAir AP to the suspected issue.

Step 4: From the drop-down list next to **AP Mode**, change to **SE-Connect**.

Step 5: Click **Apply** and wait for the access point to reboot and reconnect to the Wireless LAN Controller.

Figure 44. Change Mode



All APs > Details for MONITOR-AP

General

AP Name	MONITOR-AP
Location	Zest AP
AP MAC Address	c4:7d:4f:3a:e5:44
Base Radio MAC	04:fe:7f:48:db:a0
Admin Status	Enable
AP Mode	local
AP Sub Mode	
Operational Status	
Port Number	

Versions

Primary Software Version	7.0.98.0
Backup Software Version	0.0.0.0
Predownload Status	None
Predownloaded Version	None
Predownload Next Retry Time	NA
Predownload Retry Count	NA
Boot Version	12.4.2.4
IOS Version	12.4(23c)JA
Mini IOS Version	0.0.0.0

IP Config

IP Address	10.4.28.237
Static IP	□

Time Statistics

UP Time	0 d, 00 h 01 m 16 s
Controller Associated Time	0 d, 00 h 00 m 20 s
Controller Association Latency	0 d, 00 h 00 m 55 s

Hardware Reset

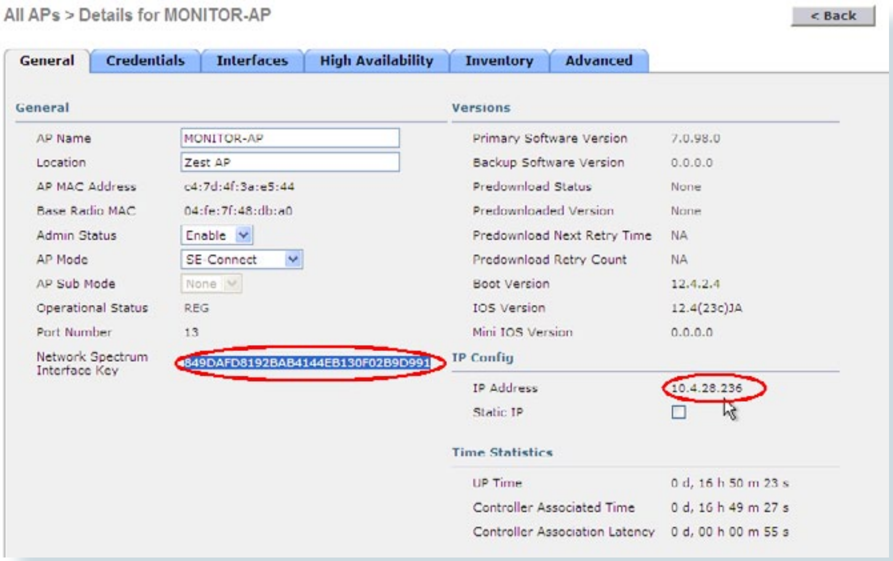
Perform a hardware reset on this AP

Set to Factory Defaults

Clear configuration on this AP and reset it to factory defaults

Step 6: Copy the **Network Spectrum Interface Key** and the CleanAir access point IP address.

Figure 45. Capture Network Key and IP Address



All APs > Details for MONITOR-AP

General

AP Name	MONITOR-AP
Location	Zest AP
AP MAC Address	c4:7d:4f:3a:e5:44
Base Radio MAC	04:fe:7f:48:db:a0
Admin Status	Enable
AP Mode	SE Connect
AP Sub Mode	None
Operational Status	REG
Port Number	13
Network Spectrum Interface Key	849DAFD8192BAB4144EB130F02B9D991

Versions

Primary Software Version	7.0.98.0
Backup Software Version	0.0.0.0
Predownload Status	None
Predownloaded Version	None
Predownload Next Retry Time	NA
Predownload Retry Count	NA
Boot Version	12.4.2.4
IOS Version	12.4(23c)JA
Mini IOS Version	0.0.0.0

IP Config

IP Address	10.4.28.236
Static IP	□

Time Statistics

UP Time	0 d, 16 h 50 m 23 s
Controller Associated Time	0 d, 16 h 49 m 27 s
Controller Association Latency	0 d, 00 h 00 m 55 s

Step 7: On a Supported Windows platform with Cisco Spectrum Expert Connect (4.0 or greater) installed, launch Spectrum Expert.

Figure 46. Launch Spectrum Expert

Step 8: Select the **Remote Sensor** radio button:

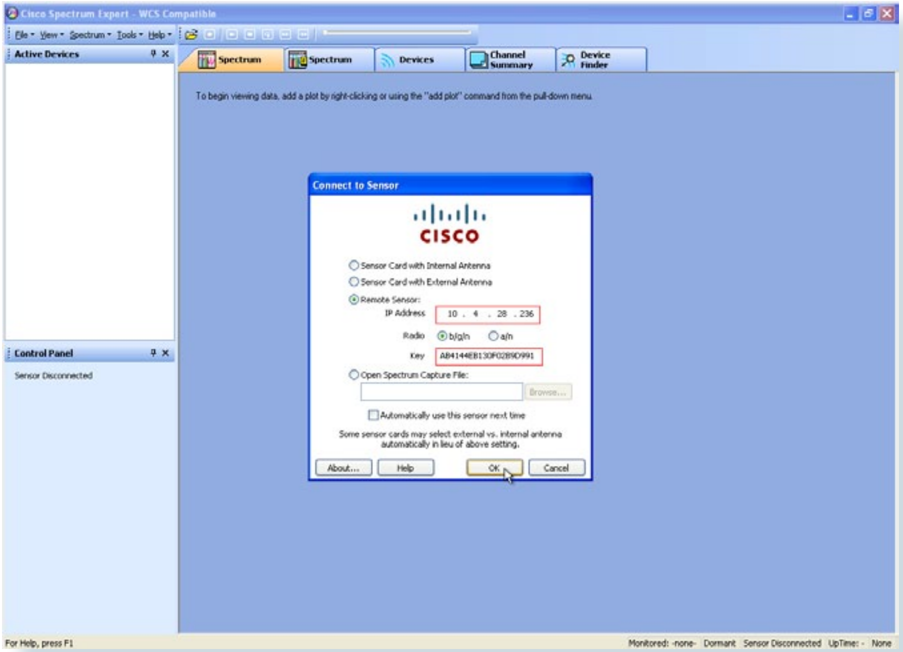
Step 8A: Enter the IP address of the CleanAir access point

Step 8B: Enter the Network Spectrum Interface Key of the CleanAir access point.

Step 8C: Select either 2.4 GHz by selecting the **b/g/n** radio button or the 5 GHz by selecting the **a/n** radio button.

Step 8D: Click **OK**.

Figure 47. Enter Remote CleanAir Details



Sensor Disconnected

To begin viewing data, add a plot by right-clicking or using the "add plot" command from the pull-down menu

Connect to Sensor

○ Sensor Card with Internal Antenna
○ Sensor Card with External Antenna
● Remote Sensor:
IP Address 10 . 4 . 28 . 236
Radio ● b/g/n ○ a/n
Key AB4144EB130F02B9D991
○ Open Spectrum Capture File:
□ Automatically use this sensor next time

Some sensor cards may select external vs. internal antenna automatically in lieu of above setting.

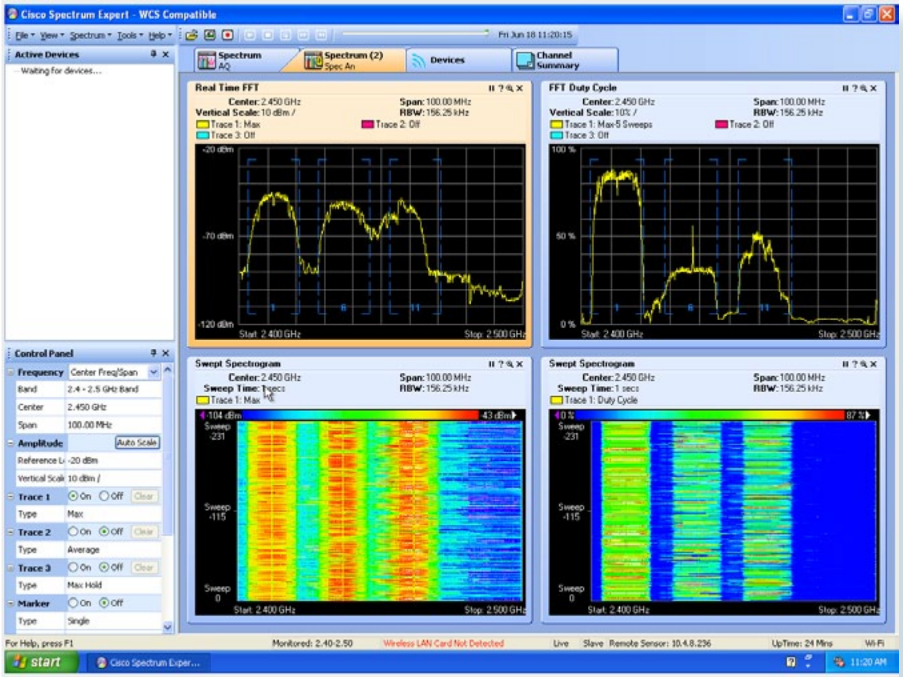
For Help, press F1 Monitored: -none- Dormant Sensor Disconnected UpTime: - None

The connected Windows machine now connects to the remote CleanAir access point on UDP port 37540 if you selected b/g or on UDP port 37550 if you selected a/n during preceding setup steps. If connection problems occur, verify that you can ping the CleanAir access point and that there are no port-blocking network devices that may be blocking the necessary UDP port information.

Remote Spectrum

The remote sensor capability is the ability to get real-time, physical layer spectrum data without having to drive or fly onsite. Figure 48 illustrates this capability in a Wi-Fi-only environment, and gives you an understanding of what is really happening in your remote environment.

Figure 48. 2.4 GHz Spectrum Using the CleanAir Access Point as the Remote Sensor



Cisco Spectrum Expert - WCS Compatible

Fri Jun 18 11:20:15

Active Devices

Waiting for devices...

Control Panel

Frequency	Center Freq/Span
Band	2.4 - 2.5 GHz Band
Center	2.450 GHz
Span	100.00 MHz
Amplitude	Auto Scale
Reference L	-20 dBm
Vertical Scale	10 dBm /
Trace 1	● On ○ Off Clear
Type	Max
Trace 2	○ On ● Off Clear
Type	Average
Trace 3	○ On ● Off Clear
Type	Max Hold
Marker	○ On ● Off
Type	Single

Real Time FFT

Center: 2.450 GHz Span: 100.00 MHz
Vertical Scale: 10 dBm / RBW: 156.25 kHz
🟨 Trace 1: Max 🟥 Trace 2: Off
🟦 Trace 3: Off

FFT Duty Cycle

Center: 2.450 GHz Span: 100.00 MHz
Vertical Scale: 10% / RBW: 156.25 kHz
🟨 Trace 1: Max-5 Sweeps 🟥 Trace 2: Off
🟦 Trace 3: Off

Swept Spectrogram

Center: 2.450 GHz Span: 100.00 MHz
Sweep Time: 1 secs RBW: 156.25 kHz
🟨 Trace 1: Max

Swept Spectrogram

Center: 2.450 GHz Span: 100.00 MHz
Sweep Time: 1 secs RBW: 156.25 kHz
🟨 Trace 1: Duty Cycle

For Help, press F1 Monitored: 2.40-2.50 Wireless LAN Card Not Detected Live Slave Remote Sensor: 10.4.8.236 UpTime: 24 Mins Wi-Fi

Notes

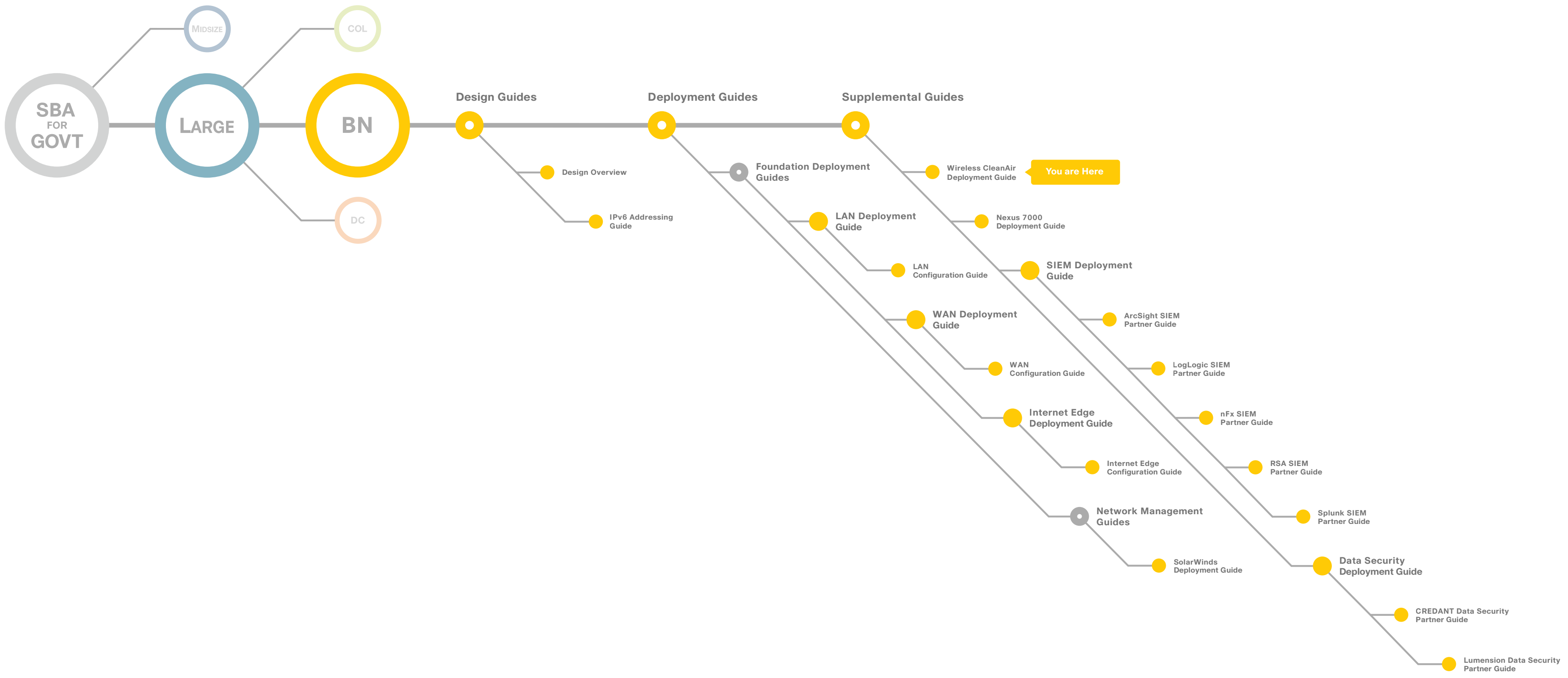
Tech Tip

Observe in Figure 48 that the Windows XP Spectrum Expert device does not detect a Wireless LAN card and that the remote sensor is at 10.4.28.236.

Appendix A: Parts List

Functional Area	Product	Part Numbers	Software Version
Headquarters	Cisco WCS	WCS-STANDARD-K9 WCS-APBASE-100 WCS-ADV-SI-SE-10= (optional)	7.0.164.0
	Cisco Wireless LAN Controller	AIR-CT5508-100-K9	7.0.98.0
	Cisco Access Point	AIR-CAP3502E-A-K9	7.0.98.0
	Cisco Access Point	AIR-CAP3502I-A-K9	7.0.98.0
	Cisco Access Point	AIR-LAP1142-A-K9	7.0.98.0
	Cisco Spectrum Expert	AIR-CSCO-SE-WIFI-C	4.0.60
	Cisco Mobility Service Engine	AIR-MSE-3350-K9	7.0.105.0

Appendix B: SBA for Large Agencies Document System



SBA FOR GOVT

MIDSIZE

LARGE

COL

BN

DC

Design Guides

- Design Overview
- IPv6 Addressing Guide

Deployment Guides

- Foundation Deployment Guides
  - LAN Deployment Guide
    - LAN Configuration Guide
  - WAN Deployment Guide
    - WAN Configuration Guide
  - Internet Edge Deployment Guide
    - Internet Edge Configuration Guide
- Network Management Guides
  - SolarWinds Deployment Guide

Supplemental Guides

- Wireless CleanAir Deployment Guide — You are Here
- Nexus 7000 Deployment Guide
- SIEM Deployment Guide
  - ArcSight SIEM Partner Guide
  - LogLogic SIEM Partner Guide
  - nFx SIEM Partner Guide
  - RSA SIEM Partner Guide
  - Splunk SIEM Partner Guide
- Data Security Deployment Guide
  - CREDANT Data Security Partner Guide
  - Lumension Data Security Partner 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.**