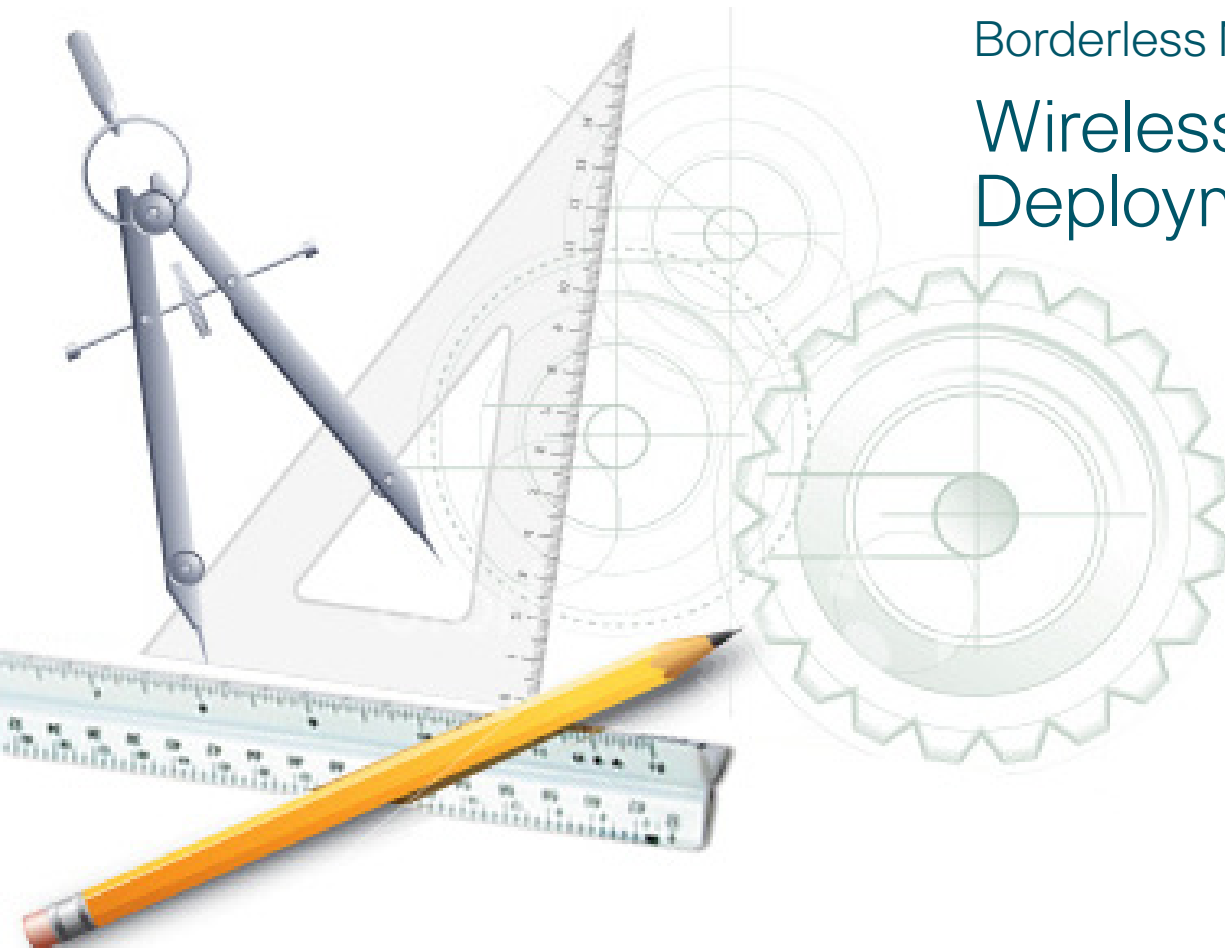




Smart Business Architecture  
Borderless Networks for Midsize Organizations

# Wireless CleanAir Deployment Guide



## Table Of Contents

▪ <b>Who Should Read This Guide</b> .....	4	▪ <b>Licensing</b> .....	11
Using This Collaboration Guide.....	4	Summary of Steps to Install the License .....	11
Additional Information.....	4	▪ <b>Add Wireless LAN Controller(s) to Cisco WCS</b> .....	13
▪ <b>Business Overview</b> .....	5	▪ <b>Building and Floor Plan</b> .....	13
The CleanAir Access Point.....	5	Adding the First Campus and Building.....	13
▪ <b>Technology Overview</b> .....	6	▪ <b>Configuring the Cisco Wireless Solution for CleanAir</b> .....	15
Cisco CleanAir Technology.....	6	Event-Driven Radio Resource Management (EDRRM).....	15
Wireless Control System.....	6	▪ <b>Troubleshooting with CleanAir</b> .....	21
Mobility Services Engine (optional component) .....	6	Accessing Remote CleanAir for Spectrum Connect.....	21
▪ <b>Configuration Details</b> .....	6	▪ <b>Appendix A: Parts List</b> .....	24
Outline List of Tasks for a Successful Deployment .....	6		
▪ <b>Installation</b> .....	7		
Run Application .....	7		

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. CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries. All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R) 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) © 2010 Cisco Systems, Inc. All rights reserved.

### This document is for the reader who:

- Wants a general understanding of Radio Resource Management.
- Understands the challenges of unlicensed Radio Spectrum
- Has already deployed the Smart Business Architecture Foundation for Midsize Networks Deployment guide and is looking for a wireless Network Management Solution
- Has an existing network and needs guidance on how to add Wireless Network Management
- Wants to better understand how to react to unforeseen Wireless Network Interference.

### Who Should Read This Guide

This guide should be of interest to anyone in a midsize organization who wants to understand the benefits of using the Wireless Network Management and Cisco 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.

### 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 (WCS) Navigator can solve within your organization and the capabilities it brings to bear to solve them.

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

The **Cisco Wireless Control System (WCS) 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 Navigator for your organization.

### Additional Information

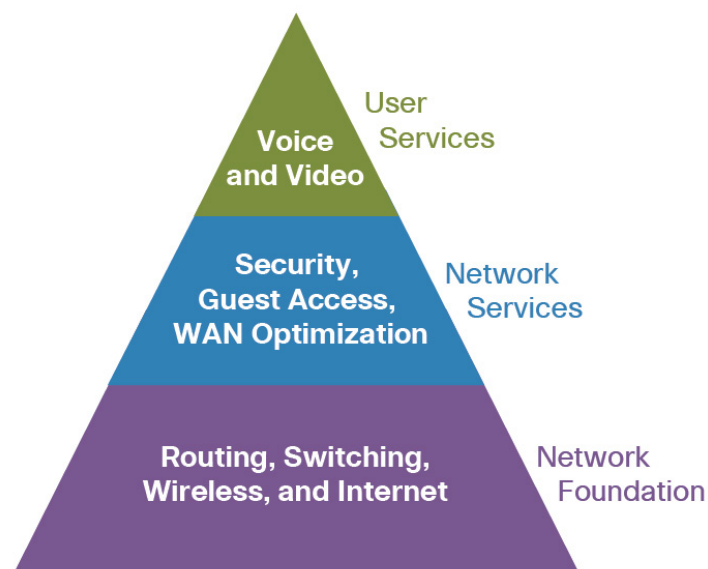
This guide is a companion document to the Borderless Network Architecture for Midsize Customers Design Guide and Deployment Guide.

The Cisco Borderless Architecture for Midsize Customers 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 Smart Business Architecture for Midsize Customers is designed to address the common requirements of organizations with 2000 to 10000 employees. Each organization 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.

Figure 1.



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 Smart Business Architecture such as the Internet connection, WAN infrastructure, and security help ensure a business can rely on applications such as web conferencing for critical collaboration.

To learn more about Cisco Borderless Network Architecture, visit:

<http://www.cisco.com/go/smartarchitecture> or  
<http://www.cisco.com/go/partner/smartarchitecture>

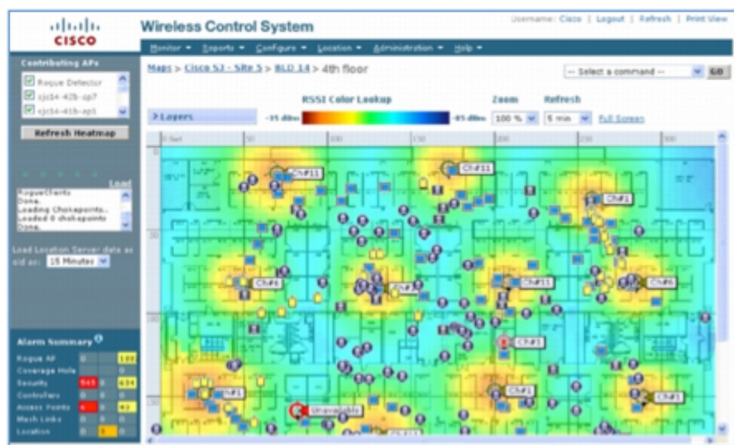
# Wireless CleanAir Deployment Guide

## Business 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



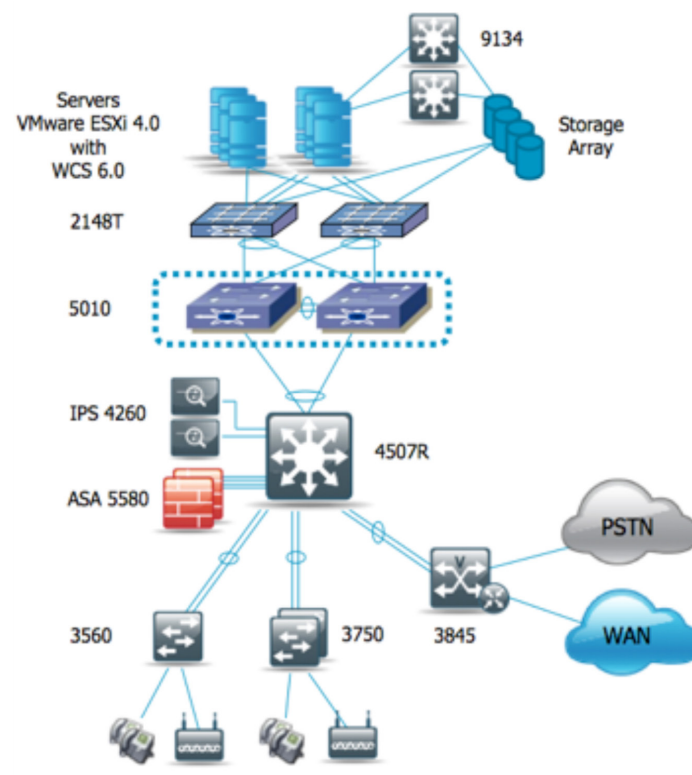
Radio is the manipulation of the magnetic field that is invisible to the naked eye. Without running expensive site surveys with a spectrum expert every hour and minute of every day, the network administrator cannot tell what is happening in the user space. The Wireless Control system collects the data 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 businesses as well 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.

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 syslog to make the network IT staff aware of the mitigated issue and alert them to watch for other issues, enforce the company radio policy, or do both.

Figure 3. Simplified Network Diagram



### Technology Overview

#### Cisco CleanAir Technology

Cisco CleanAir is the integration of Cisco Spectrum Expert technology with a Cisco Access point. Before Cisco CleanAir, 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 in proactively reclaiming control over the radio 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 CleanAir feature, the Cisco WCS can display in real time the data retrieved from 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 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 leveraging VMware ESXi 4.0 within the data center, as illustrated in Figure 4.

#### Mobility Services Engine (optional component)

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 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 endpoint (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 of an endpoint 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 organization requires, the same Cisco Wireless Control System software runs on different hardware, as described in the product Release Notes.

#### Outline List of Tasks for a Successful Deployment

This section lists the tasks that must be completed for a successful deployment.

1. Installation
  - a. Install Cisco Wireless Control System on a VMware ESXi 4.0 virtual machine
2. Licensing
  - a. Install the license to bring Cisco WCS online
3. Wireless LAN controller
  - a. Add Wireless LAN controller(s) to Cisco WCS
4. Building and Floor plan
  - a. Add the building or site to Cisco WCS
  - b. Add individual floor plans to each building
  - c. Place each Access point on the floor plan map
5. Templates
  - a. Create configuration templates for new controllers
  - b. Create configuration templates for different access points



### Installation

The installation steps outlined here 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 use the default ports, however, consult your security policy to be sure your company 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)

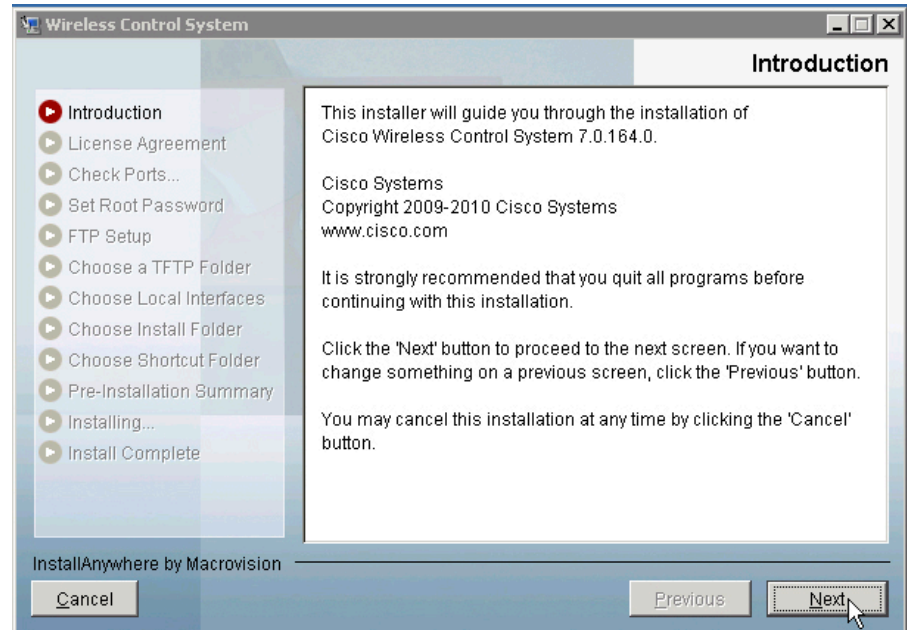
### Run Application

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

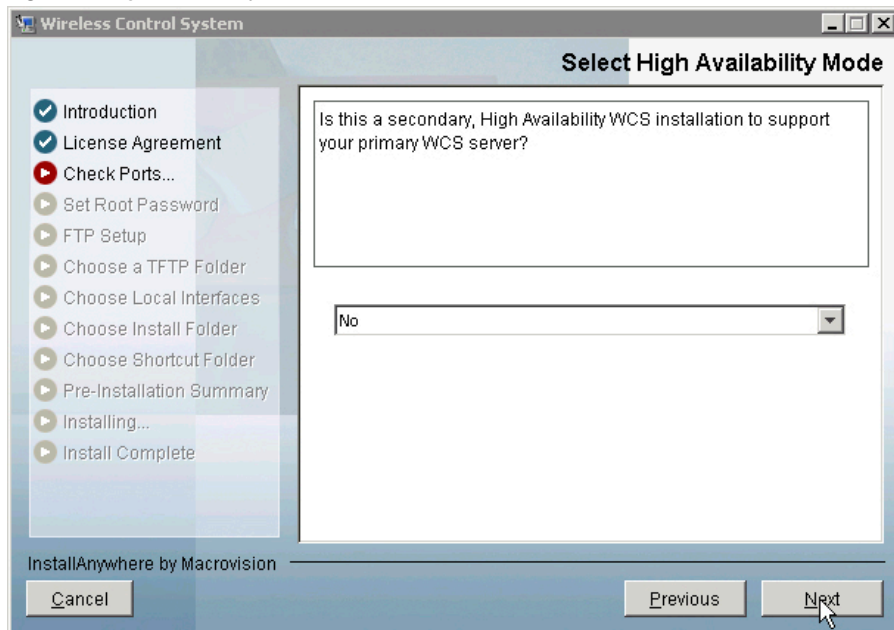


The introductory screen summarizes the application you downloaded and prompts you to move to the next screen. You must accept the license agreement and click **Next**.

## Wireless CleanAir Deployment Guide

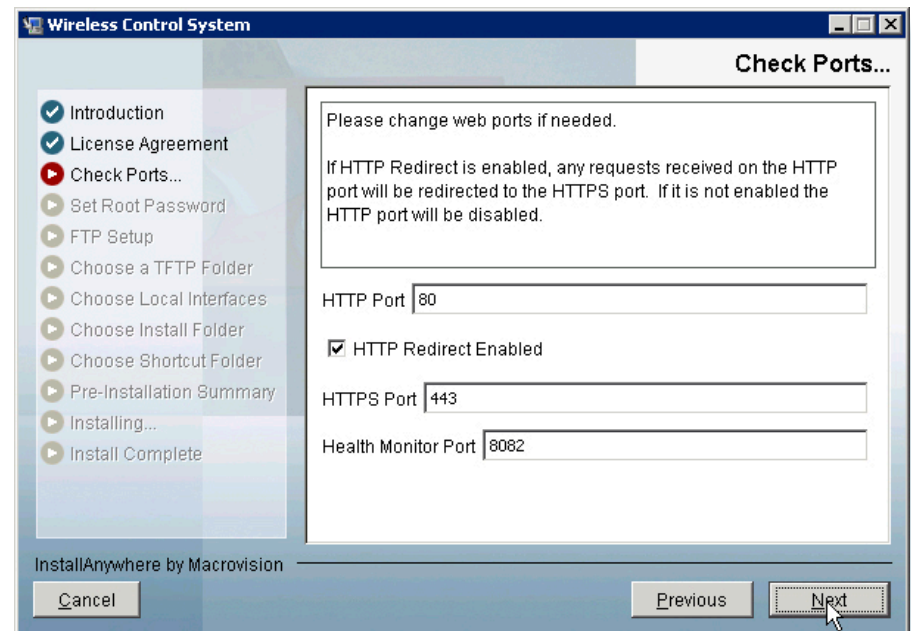
The installer checks for any previous installations. It asks if this installation is for High Availability or is being built as a secondary WCS. We do not set up a secondary or High Availability installation in this guide; however, you can do this simply by repeating this installation and selecting **Yes**. Select **No** as illustrated in Figure 5.

Figure 5. High Availability Mode Selection



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





## Wireless CleanAir Deployment Guide

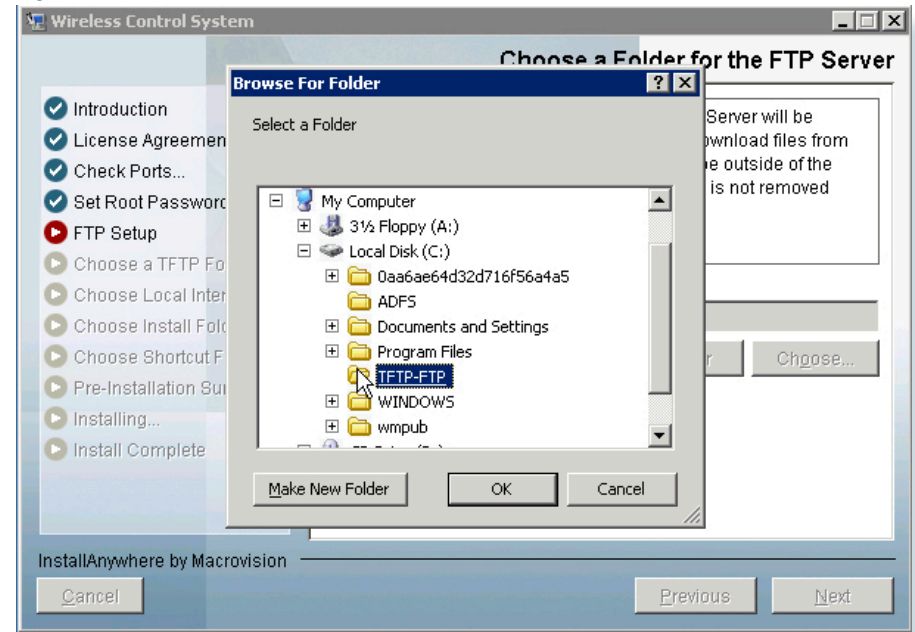
You must define the root password next. This password is the locally defined administration password. The password will be checked for strength; however, password strength should follow your security policy. The root password is only used for the local administrator.

Figure 7. Root Password



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.

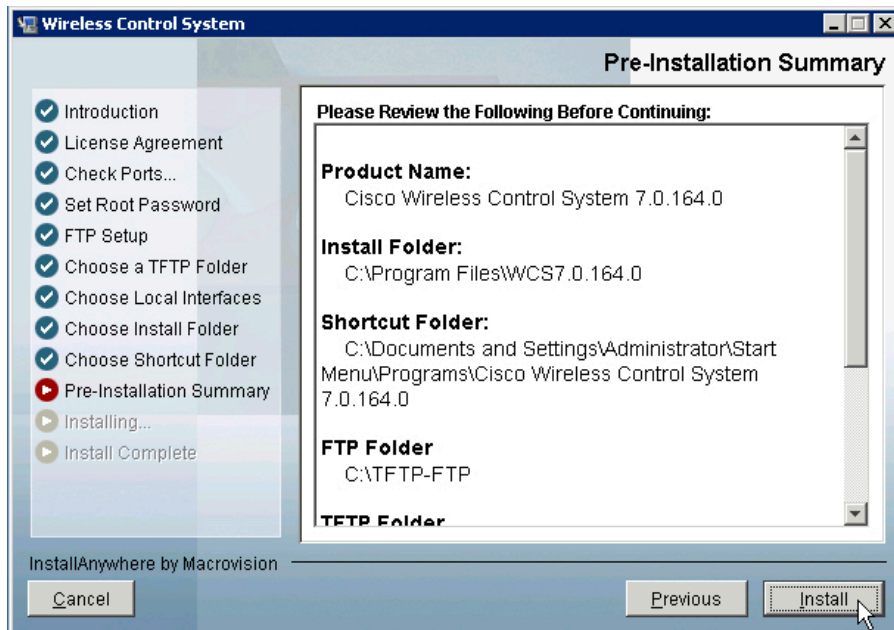
Figure 8. File Folder Selection



## Wireless CleanAir Deployment Guide

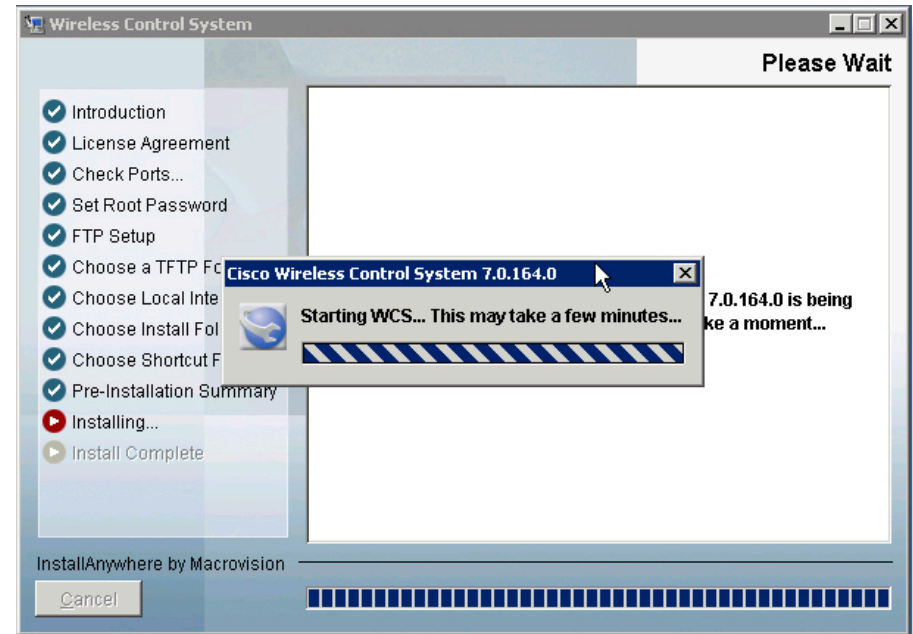
Click **Next** on the installation icon folder options to get to the installation summary. Review your choices before the installation begins.

Figure 9. Installation Summary



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

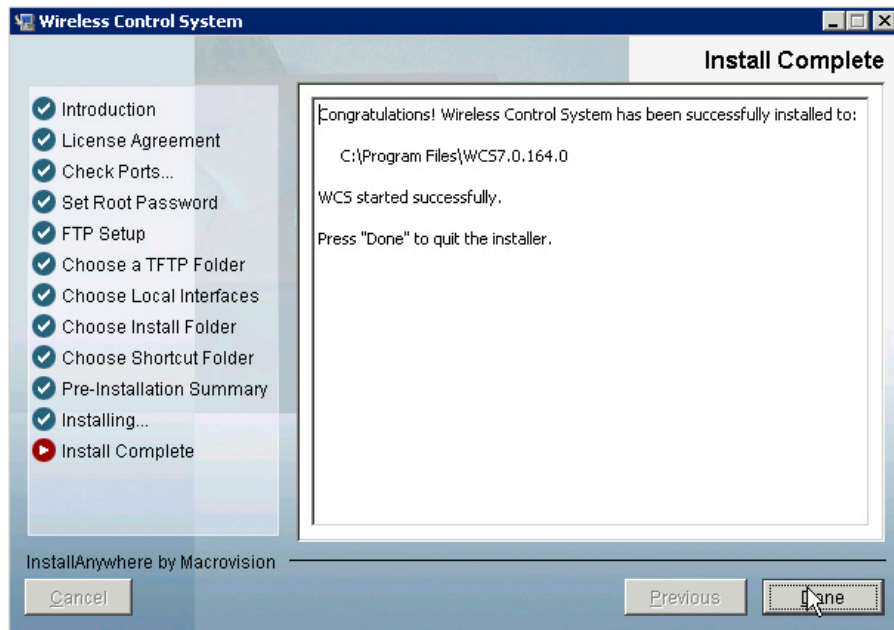
Figure 10. Starting WCS for the first time



## Wireless CleanAir Deployment Guide

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

Figure 11. Installation Complete



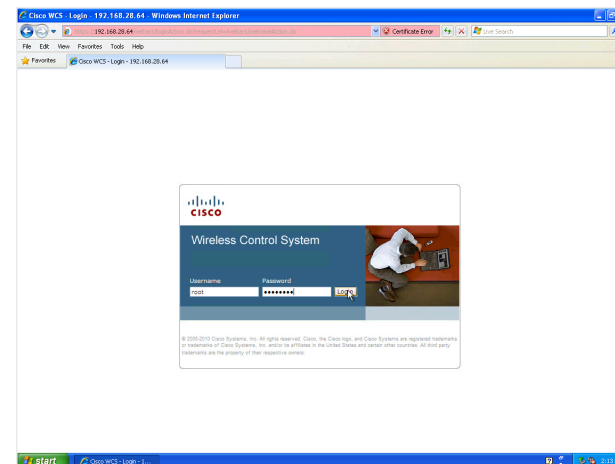
## Licensing

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 192.168.28.64  
`https:// 192.168.28.64`
3. Log in to the Cisco WCS server as the system administrator. (Be aware that usernames and passwords are case-sensitive.)

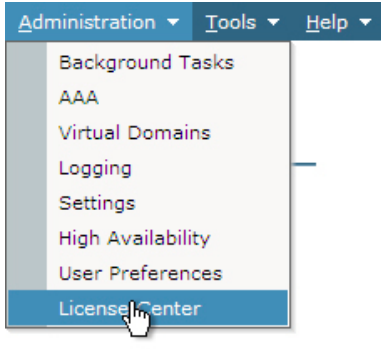
Figure 12. WCS Login Screen



## Wireless CleanAir Deployment Guide

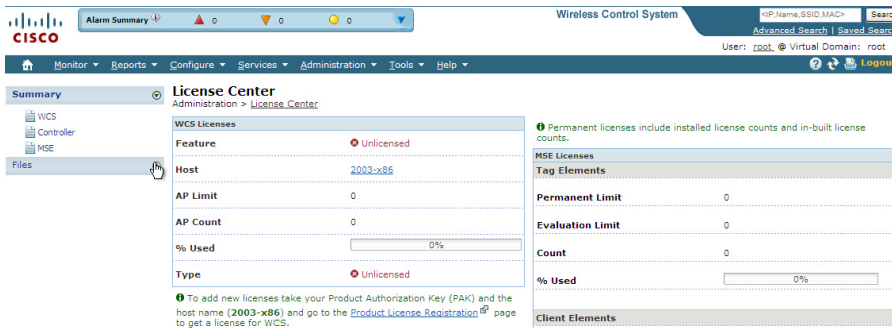
4. From the **Administration** menu select **License Center**.

Figure 13. Navigate to License Center



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

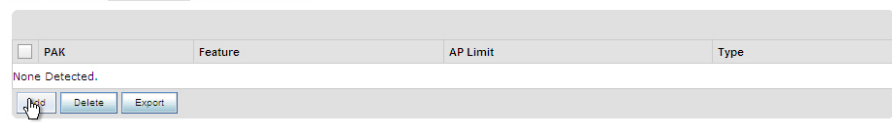
Figure 14. License Center, Add PAK



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

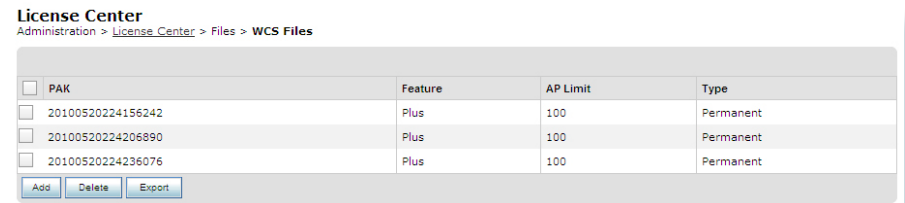
**License Center**  
Administration > License Center > Files > WCS Files



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

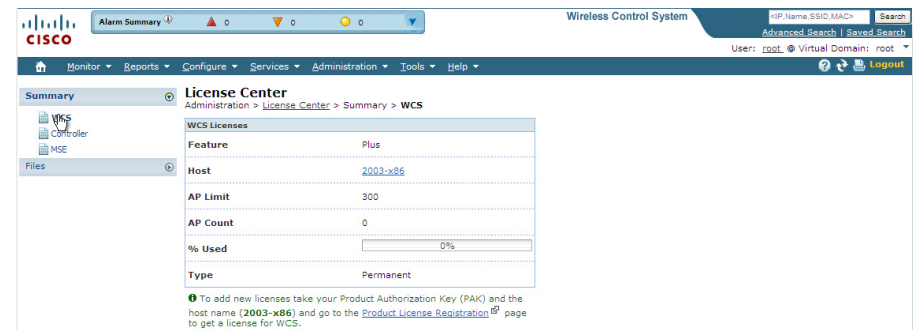
8. Repeat this step for each additional license you have received.

Figure 16. Importing License Files



Once completed, all your license files should appear as shown. 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 show in Figure 17.

Figure 17. License Summary



## Wireless CleanAir Deployment Guide

### 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 18. From the drop-down list on the right, select **Add Controllers...** and click **Go**. You are prompted to enter the Controller IP address. Use the default settings for all other parameters including the Telnet/SSH password.

Figure 18. Add Controllers

Alarm Summary 0 0 0 215

Monitor Reports Configure Services Administration Tools Help

**Add Controllers**  
Configure > Controllers > Add Controllers

**General Parameters**

Add Format Type: Device Info

IP Addresses: 192.168.31.64 (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)

OK Cancel

**NOTE:** 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 19.

Figure 19. List of Controllers

Wireless Control System

Alarm Summary 0 0 0 215

Monitor Reports Configure Services Administration Tools Help

**Controllers**  
Configure > Controllers

-- Select a command -- Go

IP Address	Controller Name	Type	Location	Software Version	Mobility Group Name	Reachability Status	Audit Status
192.168.31.64	HQ-WLC	5500		7.0.98.0	SBA	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**.

### Building and Floor Plan

The real advantage to any management system is the presentation of the information that 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 floor maps 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.

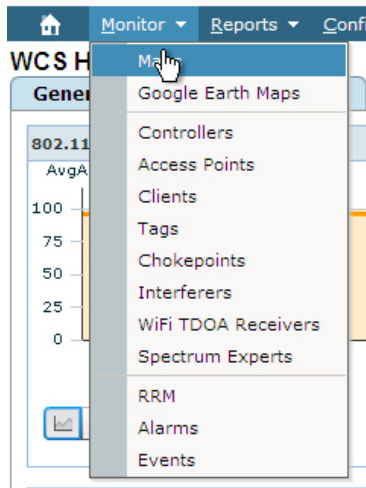
**NOTE:** You need to know the dimension of the campus picture you are bringing into the system so that you can scale the drawing appropriately as each building and floor are added.

# Wireless CleanAir Deployment Guide

Step 1: Log in to the Cisco Wireless Control System.

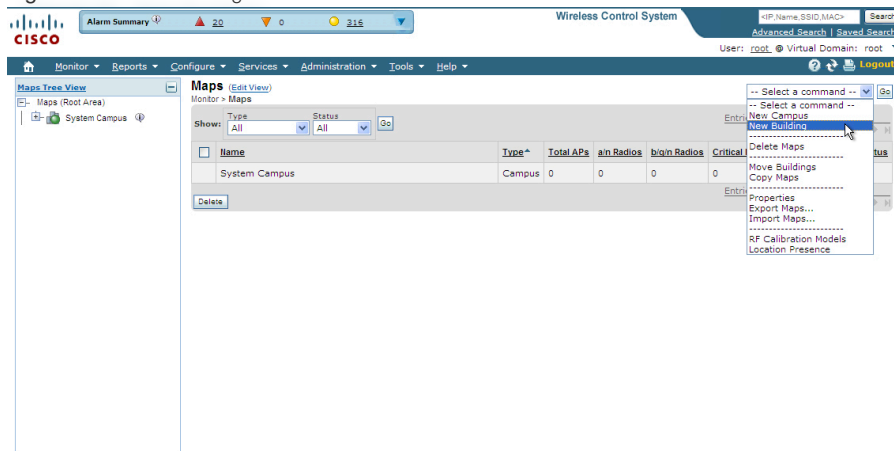
Step 2: Navigate to Monitor > Maps.

Figure 20. Finding Building Maps



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

Figure 21. New Building



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

Building Name: SBA-Headquarters

Contact: Albert Gudgin

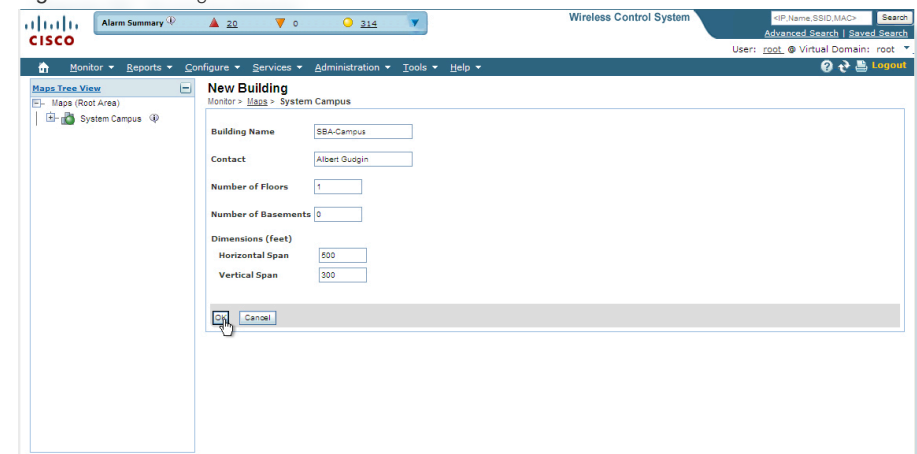
Number of floors: 1

Number of Basements: 0

Horizontal Span (feet): 500

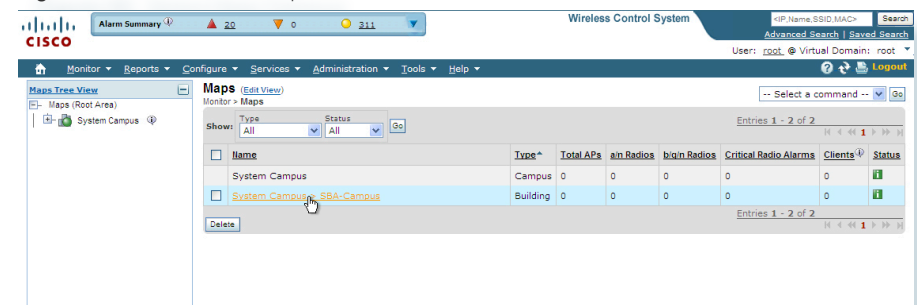
Vertical Span (feet): 300

Figure 22. Building Details



Step 5: Select your generated campus.

Figure 23. Select New Campus

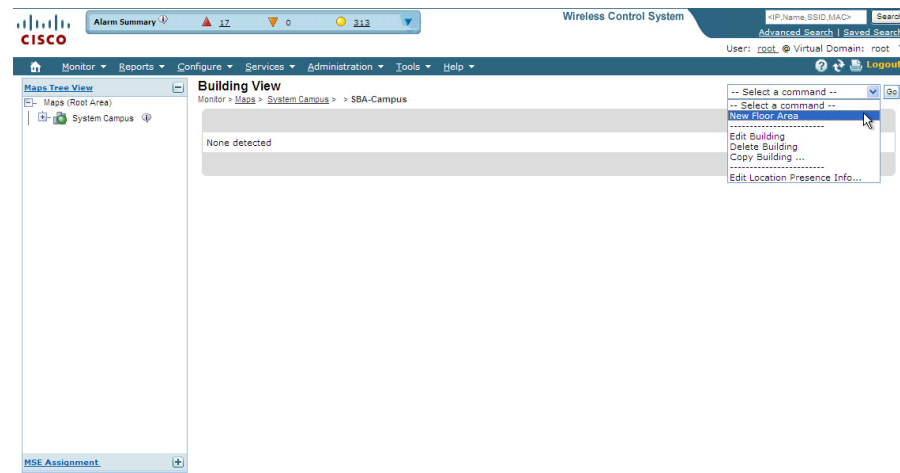




## Wireless CleanAir Deployment Guide

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

Figure 24. New Floor Area



**Step 7:** Create a floor name, contact name, floor number, description of the area, and the floorplan image, and click **Next**:

**Floor Area Name:** SBA-Headquarters

**Contact:** Albert Gudgin

**Floor:** 1 (selected from drop-down list)

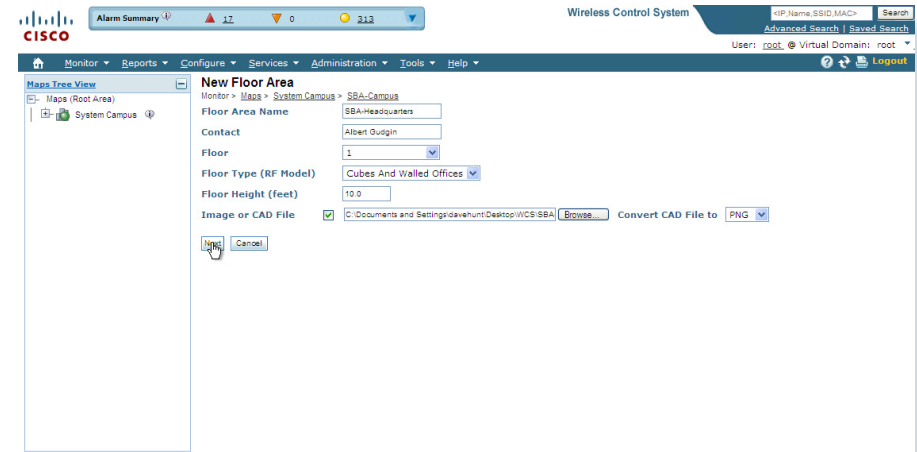
**Floor Type (RF Model):** Cubes And Walled Offices  
(selected from drop-down)

**Floor Height (feet):** 10.0

**Image or CAD File:** C:\Documents and Settings\SBA-Headquarters.png

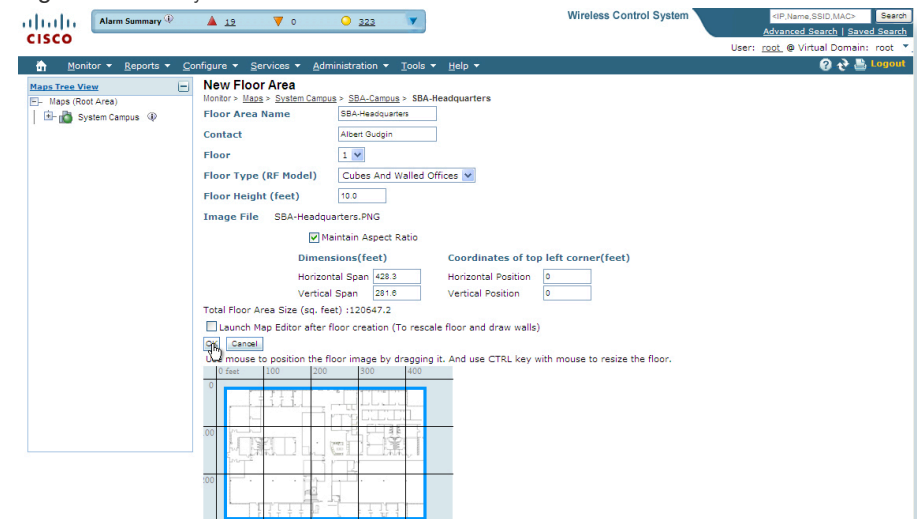
**Convert CAD File to:** PNG (Leave the default drop-down selection)

Figure 25. New Floor Details and Image Upload



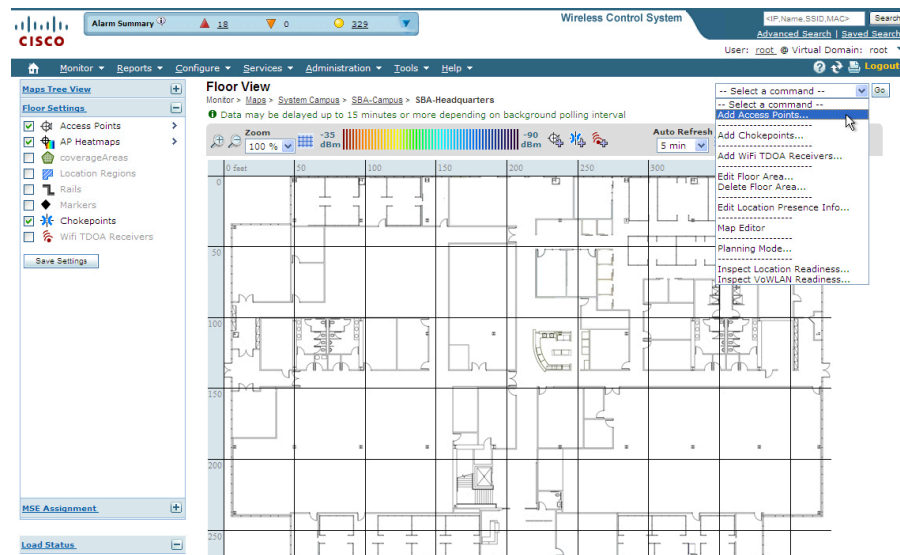
**Step 8:** Verify your new floor area details and image and click **OK**.

Figure 26. Verify New Floor Details



# Wireless CleanAir Deployment Guide

Figure 27. Floor View



## Place Access Points

The final piece of the puzzle is to place the access points at the proper location on your individual floor plans. 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 in to Cisco WCS.

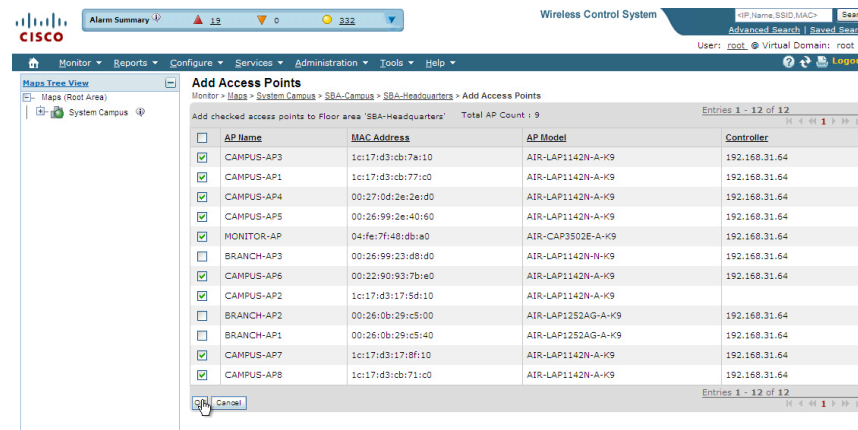
**Step 2:** Navigate to **Monitor > Maps**.

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

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

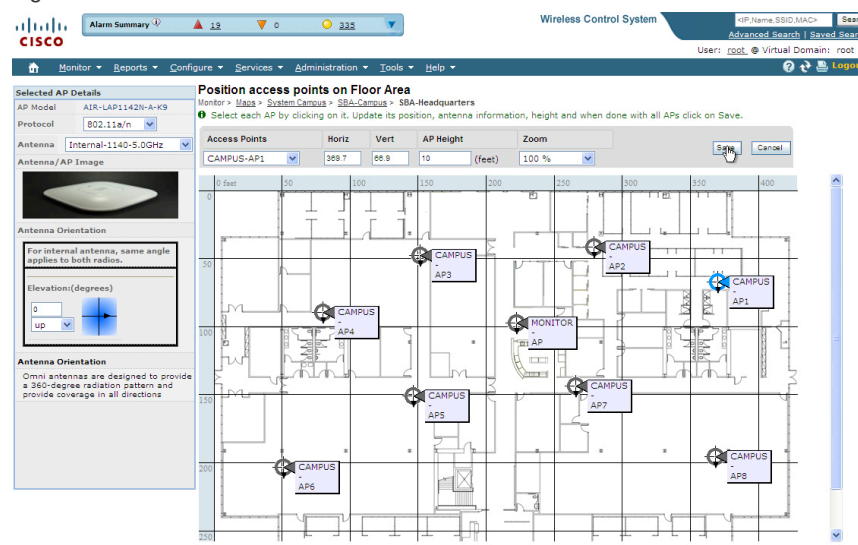
**Step 5:** Select access points that are registered with the system and not yet placed for the headquarters building.

Figure 28. Select APs to Place on a New Floor



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

Figure 29. AP Placement



**NOTE:** You must now wait while the system calculates the heatmaps from the placement and floor plan area.

### Configuring the Cisco Wireless Solution for CleanAir

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

With the Cisco Wireless Control System in the network, all management can be handled at the Cisco 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 log into the Cisco Wireless Control System and configure our controller to support CleanAir.

### Event-Driven Radio Resource Management (EDRRM)

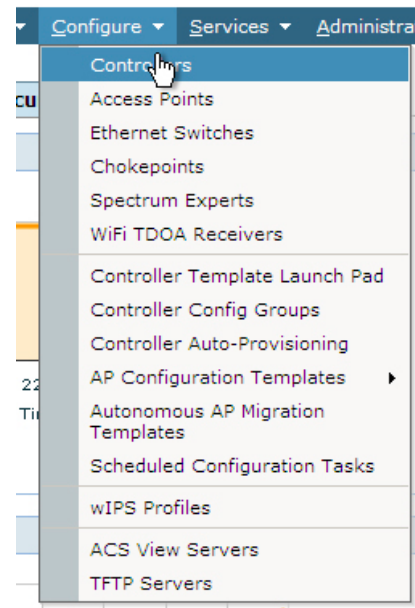
Event-Driven RRM is a feature that allows an access point that is in distress to bypass normal RRM intervals and immediately change channels. A CleanAir access point always monitors AirQuality (AQ), and reports on AQ in 15 second intervals. AirQuality is a better metric than relying on normal Wi-Fi chip 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 feature 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 in to Cisco WCS.

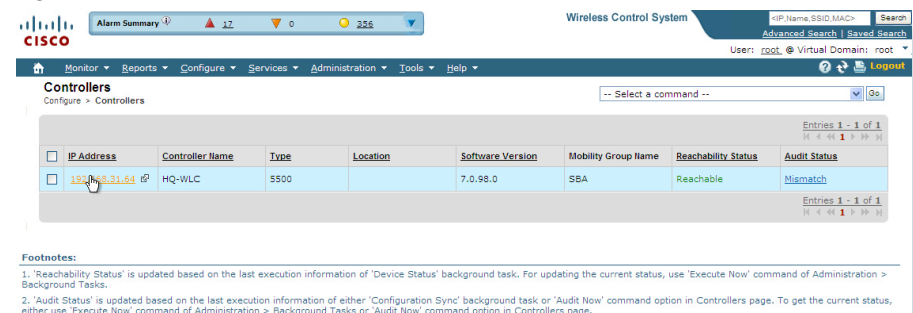
**Step 2:** Navigate to **Configure > Controllers**.

Figure 30. Configure Controllers



**Step 3:** Select your Wireless LAN Controller.

Figure 31. Select HQ-WLC

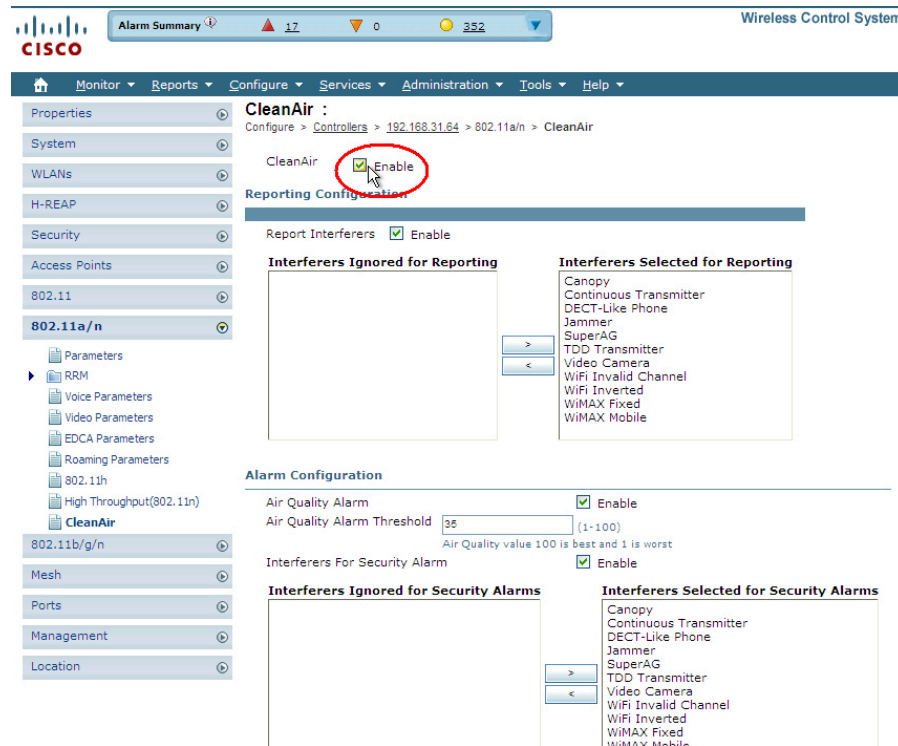


## Wireless CleanAir Deployment Guide

**Step 4:** From the left-side menu, navigate to 802.11a/n > CleanAir.

**Step 5:** Check the **CleanAir Enable** checkbox and then select Interferers that you want the system to react to. Click **Save**.

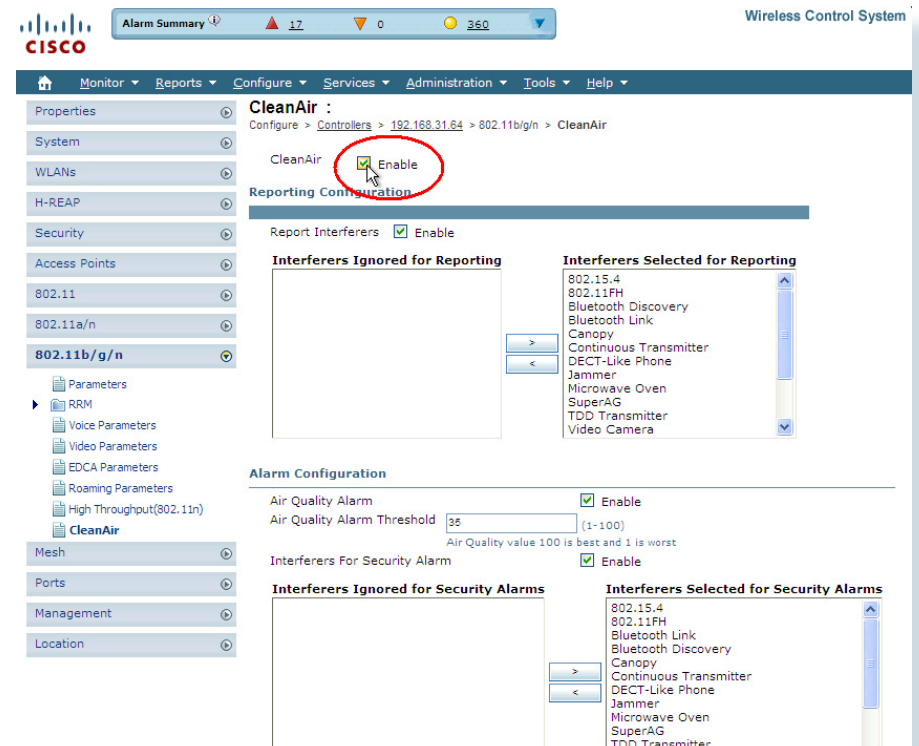
Figure 32. Enable CleanAir and Configure Interferers for 802.11a/n.



**Step 6:** From the left-side menu, navigate to 802.11b/g/n > CleanAir.

**Step 7:** Check the **CleanAir Enable** checkbox and select the Interferers that you want the system to react to. Click **Save**.

Figure 33. Enable CleanAir and Configure Interferers for 802.11b/g/n



## Wireless CleanAir Deployment Guide

Step 8: From the left-side menu, navigate to 802.11a/n > RRM > DCA.

Figure 34. DCA Parameters for 802.11a/n

4.9Ghz channels will be shown and can be configured only if Public Safety option is enabled.

**Dynamic Channel Assignment Algorithm**

Template Applied: Automatic

Assignment Mode: Automatic

Update Interval: 600 (secs)

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

Outdoor AP DCA: ☐ Enable

Channel Width: 20 MHz

**DCA List Channels**

Selected DCA channels: 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161

Select	Channel
<input checked="" type="checkbox"/>	36
<input checked="" type="checkbox"/>	40
<input checked="" type="checkbox"/>	44
<input checked="" type="checkbox"/>	48
<input checked="" type="checkbox"/>	52
<input checked="" type="checkbox"/>	56

**Event Driven RRM**

Event Driven RRM: ☒ Enable

Sensitivity Threshold: Medium

Save Audit

Step 9: Check the checkbox for Event Driven RRM and click Save.

Figure 35. Enable Event-Driven RRM for 802.11a/n

4.9Ghz channels will be shown and can be configured only if Public Safety option is enabled.

**Dynamic Channel Assignment Algorithm**

Template Applied: Automatic

Assignment Mode: Automatic

Update Interval: 600 (secs)

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

Outdoor AP DCA: ☐ Enable

Channel Width: 20 MHz

**DCA List Channels**

Selected DCA channels: 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161

Select	Channel
<input checked="" type="checkbox"/>	36
<input checked="" type="checkbox"/>	40
<input checked="" type="checkbox"/>	44
<input checked="" type="checkbox"/>	48
<input checked="" type="checkbox"/>	52
<input checked="" type="checkbox"/>	56

**Event Driven RRM**

Event Driven RRM: ☒ Enable

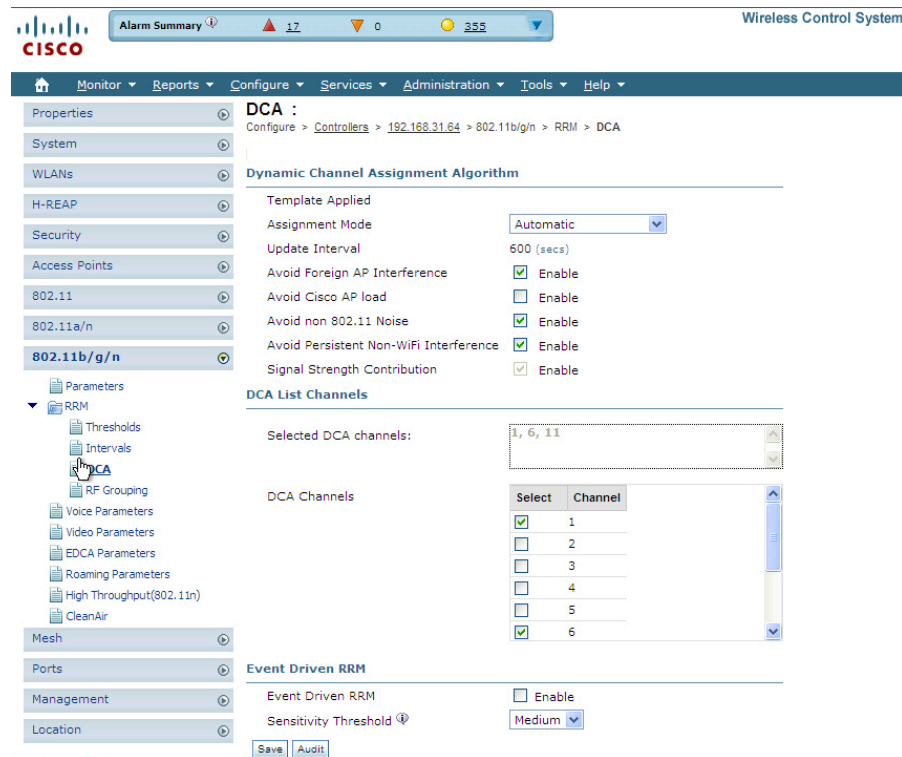
Sensitivity Threshold: Medium

Save Audit

## Wireless CleanAir Deployment Guide

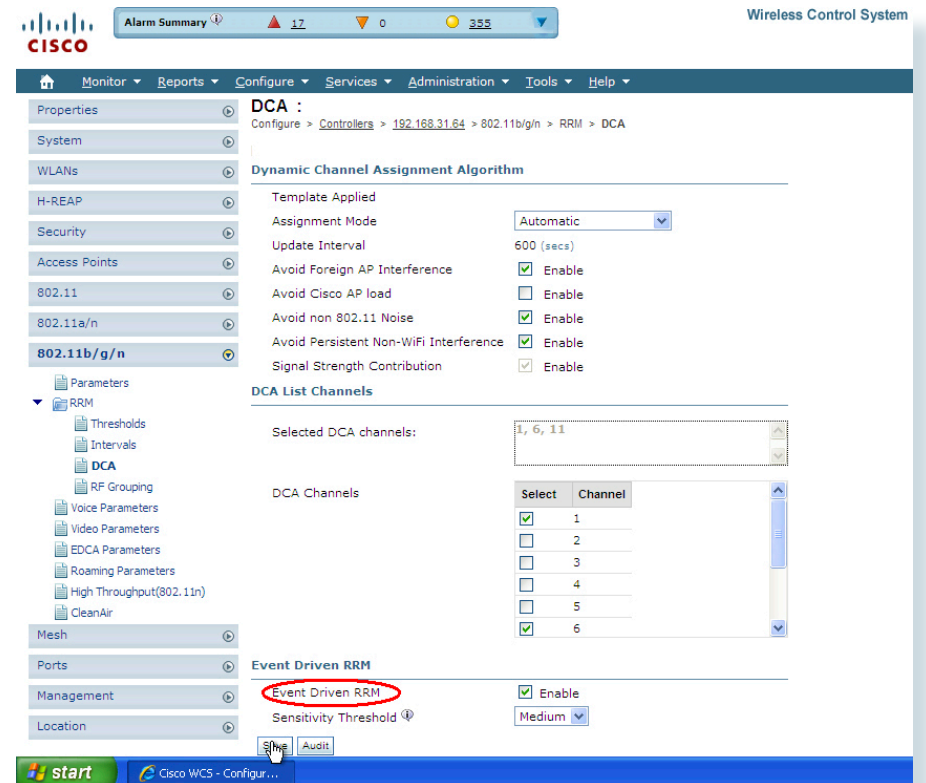
Step 10: From the left-side menu, navigate to 802.11b/g/n > RRM > DCA.

Figure 36. DCA Parameters for 802.11b/g/n



Step 11: Check the checkbox for Event Driven RRM and click Save.

Figure 37. Enabled Event-Driven RRM for 802.11b/g/n





## Wireless CleanAir Deployment Guide

### 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 as possible from the end user, look at the radio environment because the system shows that clients are connecting and Cisco 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 CleanAir access point that is closest to the suspected issue.

**Step 4:** From the drop-down menu 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 38. Change Mode

The screenshot shows the Cisco Wireless LAN Controller configuration page for the access point named 'MONITOR-AP'. The 'General' tab is selected. In the 'AP Mode' dropdown menu, 'SE-Connect' is chosen. Other visible fields include 'Location' set to 'Zest AP', 'AP MAC Address' as 'c4:7d:4f:3a:e5:44', and 'Base Radio MAC' as '04:fe:7f:48:db:a0'. The 'Admin Status' is 'Enable'. The 'Versions' section on the right lists software and boot versions. At the bottom, there are buttons for 'Reset AP Now', 'Set to Factory Defaults', and 'Clear All Config'.

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

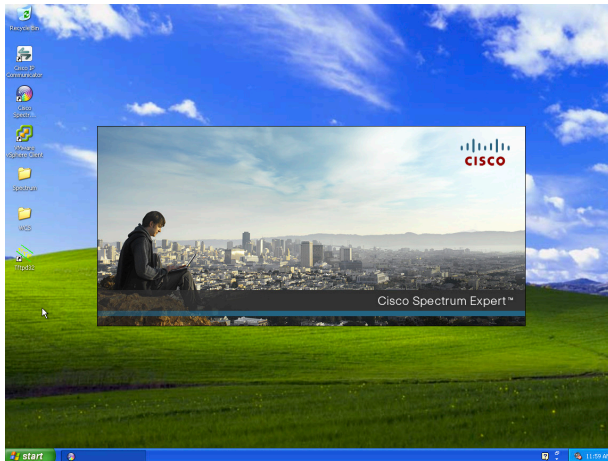
Figure 39. Capture Network Key and IP Address

This screenshot shows the same configuration page as Figure 38, but with 'SE-Connect' selected in the 'AP Mode' dropdown. Two fields are highlighted with red circles: the 'Network Spectrum Interface Key' with the value '649DAFD8192BAB4144EB130F02B9D991' and the 'IP Address' with the value '192.168.8.237'. The 'Static IP' checkbox is unchecked. The 'Time Statistics' section at the bottom shows 'UP Time' as '0 d, 16 h 50 m 23 s'.

## Wireless CleanAir Deployment Guide

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

Figure 40. Launch Spectrum Expert



**Step 8:** Select the **Radial Button Remote Sensor**:

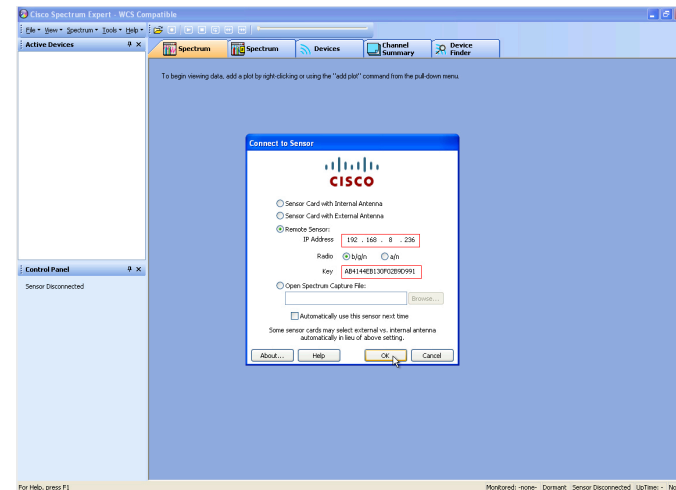
**Step 8A:** Enter the IP address of the CleanAir access point

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

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

**Step 8D:** Click OK.

Figure 41. Enter Remote CleanAir Details



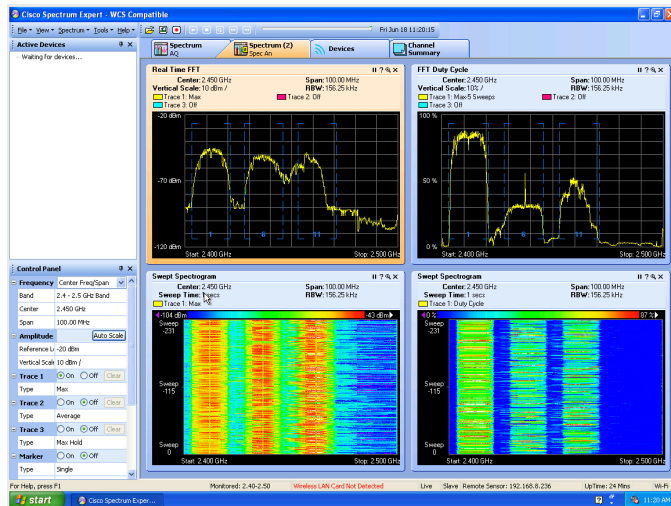
The connected Windows machine now connects to the remote CleanAir access point on UDP port 37540 if you selected b/g or on UDP port 37550 if you selected a/n during preceding setup. If connection problems occur, verify that you can ping the CleanAir access point and that there are no port blocking network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

## Wireless CleanAir Deployment Guide

### 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 42 shows this capability in a Wi-Fi-only environment, and gives you an understanding of what is really happening in your remote environment.

Figure 42. 2.4Ghz Spectrum Using the CleanAir Access Point as the Remote Sensor



**NOTE:** Observe in Figure 42 that the Windows XP Spectrum Expert device does not detect a Wireless LAN card and that the remote sensor is at 192.168.8.236.

### 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)	70.164.0
	Cisco Wireless LAN Controller	AIR-CT5508-100-K9	70.98.0
	Cisco Access Point	AIR-CAP3502E-A-K9	70.98.0
	Cisco Access Point	AIR-CAP3502I-A-K9	70.98.0
	Cisco Access Point	AIR-LAP1142-A-K9	70.98.0
	Cisco Spectrum Expert	AIR-CSCO-SE-WIFI-C	4.0.60



**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](http://www.cisco.com/go/offices).

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

C07-611640-00 07/10