• **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1** | **1**

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.



cisco.

SBA ^{FOR} GOVT

MIDSIZE

BORDERLESS NETWORKS

Wireless CleanAir Deployment Guide

SBA FOR GOVERNMENT

Revision: H2CY10

The Purpose of this Document

This Wireless Deployment Guide introduces the Cisco Clean Air solution.

It explains the requirements that were considered when building the Cisco Smart Business Architecture (SBA) for Government design and introduces each of the products that were selected.

Who Should Read This Guide

This guide is intended for the reader with any or all of the following:

- · Wants a general understanding of radio resource management.
- · Understands the challenges of unlicensed radio spectrum
- · Is looking for a wireless network management solution
- Needs guidance on how to add wireless network management
- · Wants a network that can react to wireless network interference.

Related Documents

Before reading this guide Data Center Design Overview Data Center Deployment Guide Foundation Deployment Guide Foundation Configuration Guide



Table of Contents

Introduction	1
Guiding Principles	
Agency Overview	2
Technology Overview	3
Configuration Details	4
Installation of WCS	5
Installation of WCS License	10

Add Wireless LAN Controllers to Cisco WCS	13
Adding Buildings and Floor Plans	15
Configuring CleanAir	19
Troubleshooting with CleanAir	23
Appendix A: Parts List	26
Appendix B: SBA for Midsize Agencies Document System	27

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, THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE USE OR INABILITY OF USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE USE OR INABILITY OF USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE TECHNICAL 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)

© 2010 Cisco Systems, Inc. All rights reserved.

Table of Contents

Introduction

The Cisco® SBA for Midsize Agencies is a comprehensive design for networks with up to 1000 users. This out-of-the-box design is simple, fast, affordable, scalable, and flexible.

The Cisco SBA for Midsize Agencies incorporates LAN, WAN, wireless, security, WAN optimization, and unified communication technologies tested together as a solution. This solution-level approach simplifies the system integration normally associated with multiple technologies, allowing you to select the modules that solve your agency's problems rather than worrying about the technical details.

We have designed the Cisco SBA to be easy to configure, deploy, and manage. This architecture:

- Provides a solid network foundation
- · Makes deployment fast and easy
- · Accelerates ability to easily deploy additional services
- · Avoids the need for re-engineering of the core network

By deploying the Cisco SBA, your agency can gain:

- A standardized design, tested and supported by Cisco
- Optimized architecture for midsize agencies with up to 1000 users and up to 20 branches
- · Flexible architecture to help ensure easy migration as the agency grows
- Seamless support for quick deployment of wired and wireless network
 access for data, voice, teleworker, and wireless guest
- Security and high availability for agency information resources, servers, and Internet-facing applications
- Improved WAN performance and cost reduction through the use of WAN optimization
- Simplified deployment and operation by IT workers with CCNA[®] certification or equivalent experience
- Cisco enterprise-class reliability in products designed for midsize agencies

Guiding Principles

We divided the deployment process into modules according to the following principles:

- Ease of use: A top requirement of Cisco SBA was to develop a design that could be deployed with the minimal amount of configuration and day-two management.
- Cost-effective: Another critical requirement as we selected products was
 to meet the budget guidelines for midsize agencies.
- Flexibility and scalability: As the agency grows, so too must its infrastructure. Products selected must have the ability to grow or be repurposed within the architecture.
- Reuse: We strived, when possible, to reuse the same products throughout the various modules to minimize the number of products required for spares.

Figure 1. SBA Model



The Cisco SBA can be broken down into the

following three primary, modular yet interdependent components for the midsize agency.

- Network Foundation: A network that supports the architecture
- Network Services: Features that operate in the background to improve and enable the user experience without direct user awareness
- · User Services: Applications with which a user interacts directly

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 net-work triple. Wireless networking brings a new set of unknowns that a wired net-work never had to address.

The Cisco Wireless Control System (WCS) with CleanAir Technology allow the net-work 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 which 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 Cisco WCS 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 be-fore 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 agencies 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.

With Event Driven Radio Resource Management (RRM), 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 or enforce the agency 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 lo-cation 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 3.

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 supple-mental 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 end-point 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 WCS requires having Windows Server 2003 loaded, and within the SBA architecture, we have loaded Windows Server 2003 on a VMware ESXi 4.0 platform. This document leverages the standard server configuration that supports up to 2,000 Cisco Aironet lightweight access points, 1,000 standalone access points, and 450 Cisco wireless LAN controllers. A lowend server can support up to 500 Cisco Aironet lightweight access points, 200 standalone access points, and 125 Cisco wire-less LAN controllers. This information can help you determine your network needs and future growth. No matter what your agency requires, the same Cisco WCS software runs on different hardware, as describe in the product Release Notes.

Notes

Installation of WCS

Process

1. Create Windows 2003 Virtual Machine

2. Install Cisco Wireless Control System

Procedure 1

Create Windows 2003 Virtual Machine

The owner of the VMware server should create a virtual machine and install Windows Server 2003 on the newly created virtual machine.

Procedure 2

Install Cisco Wireless Control System

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 WCS 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 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)

Step 1: 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 in Figure 4.

Figure 4. WCS Initial Configuration

🐙 Wireless Control System		_ 🗆 🗙
A CONTRACT		Introduction
 Introduction License Agreement Check Ports Set Root Password FTP Setup Choose a TFTP Folder Choose Local Interfaces Choose Install Folder Choose Shortcut Folder Pre-Installation Summary Installing Install Complete 	This installer will guide you through the Cisco Wireless Control System 7.0.164 Cisco Systems Copyright 2009-2010 Cisco Systems www.cisco.com It is strongly recommended that you qui continuing with this installation. Click the 'Next' button to proceed to the change something on a previous scree You may cancel this installation at any t button.	i.O. it all programs before next screen. If you want to on, click the 'Previous' button.
InstallAnywhere by Macrovision — <u>C</u> ancel		Previous Next

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**.

Step 2: Select High Availability Mode

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

🐙 Wireless Control System	
	Select High Availability Mode
 Introduction License Agreement Check Ports Set Root Password FTP Setup Choose a TFTP Folder Choose Local Interfaces Choose Install Folder Choose Shortcut Folder Pre-Installation Summary Installing Install Complete 	Is this a secondary, High Availability WCS installation to support your primary WCS server?
InstallAnywhere by Macrovision — <u>C</u> ancel	Previous Next

Step 3: Define Management Ports

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

Figure 6. Port Configuration

🖫 Wireless Control System		
		Check Ports
 Introduction License Agreement Check Ports Set Root Password FTP Setup Choose a TFTP Folder Choose Local Interfaces Choose Install Folder Choose Shortcut Folder Pre-Installation Summary Installing Install Complete 	Please change web ports if needed. If HTTP Redirect is enabled, any reque port will be redirected to the HTTPS po HTTP port will be disabled. HTTP Port 80 ✓ HTTP Redirect Enabled HTTPS Port 443 Health Monitor Port 8082	
InstallAnywhere by Macrovision — <u>Cancel</u>		Previous Next

Step 4: Create Root password

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

堰 Wireless Control System	
	Enter Root Password
 Introduction License Agreement Check Ports Set Root Password FTP Setup Choose a TFTP Folder Choose Local Interfaces Choose Install Folder Choose Shortcut Folder Pre-Installation Summary Installing Install Complete 	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: ****
InstallAnywhere by Macrovision – <u>C</u> ancel	Previous Next

Step 5: Choose TFTP and FTP folders

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. Select folder and click **Next** through each screen.

Figure 8. File Folder Selection

🐙 Wireless Control Syst	em	
	Choose	e a Folder for the FTP Server
-	Browse For Folder	? ×
Introduction	Select a Folder	Server will be
🕑 License Agreemen		ownload files from
🕑 Check Ports		e outside of the
📀 Set Root Password	🖃 😼 My Computer	is not removed
🖸 FTP Setup	🕀 🖑 31⁄2 Floppy (A:)	
Choose a TFTP Fo	□	
Choose Local Inter	⊕ 0aa6ae64d32d716f56a4a5 ☐ ADF5	
Choose Install Fold	E Cocuments and Settings	
Choose Shortcut F	🕀 🔂 Program Files	r Choose
Pre-Installation Sur		
D Installing		
Install Complete		<u> </u>
	Make New Folder OK	Cancel
		///
InstallAnywhere by Macr	ovision	
<u>C</u> ancel		Previous Next

Step 6: Verify Configuration Settings

The Pre-Installation Summary will review all your decision without any password information. Review this summary and select **Install** to begin installation.

Figure 9. Installation Summary

Introduction	Please Review the Following Before Continuing:
License Agreement	A A A A A A A A A A A A A A A A A A A
 Check Ports Set Root Password 	Product Name: Cisco Wireless Control System 7.0.164.0
 FTP Setup Choose a TFTP Folder 	Install Folder: C:\Program Files\WCS7.0.164.0
 Choose Local Interfaces Choose Install Folder 	Shortcut Folder: C:\Documents and Settings\Administrator\Start
 Choose Shortcut Folder Pre-Installation Summary 	Menu\Programs\Cisco Wireless Control System 7.0.164.0
Installing Install Complete	FTP Folder C:\TFTP-FTP
	TETP Folder

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

Figure 10. Starting WCS for the first time

🐙 Wireless Control System		
		Please Wait
🗸 🗸 Choose Local Inte	reless Control System 7.0.164.0 Starting WCS This may take a few mint	7.0.164.0 is being ke a moment
InstallAnywhere by Macrovision	,	

Step 7: Finish Installation

Click **Done** to close the installation application and startup WCS for the first time. You are now running Cisco WCS.

Figure 11. Installation Complete

堰 Wireless Control System		
		Install Complete
 Introduction License Agreement Check Ports Set Root Password FTP Setup Choose a TFTP Folder Choose Local Interfaces Choose Install Folder Choose Shortcut Folder Pre-Installation Summary Installing Install Complete 	Congratulations! Wireless Control System ha C:\Program Files\WCS7.0.164.0 WCS started successfully. Press "Done" to quit the installer.	as been successfully installed to:
InstallAnywhere by Macrovision — <u>C</u> ancel		Previous

Notes		

Installation of WCS

Process

License

- 1. Request Wireless Control System License
- 2. Log Into WCS as Administrator and Install License

Procedure 1

Request Wireless Control System License

Cisco 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.

If you have not already received the licensing files, you must perform this procedure.

Step 1: Determine the WCS hostname and number of access points.

Step 2: Email <u>licensing@cisco.com</u> with the WCS hostname and number of access points.

You will receive the license files in an email from Cisco.

Procedure 2

Log Into WCS and Install License File

Step 1: Save License File

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.)

Step 2: Connect to Wireless Control System

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

Step 3: Log into WCS as Administrator

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



Step 4: Go to the License Center

From the Administration menu select License Center.

Figure 13. Navigate to License Center



Step 6: Add License

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

Figure 15. A	Add New PAK		
License Center Administration > License	<u>e Center</u> > Files > WCS Files		
РАК	Feature	AP Limit	Туре
None Detected.			
Child Delete Ex	port		

Click **Upload**. The Cisco WCS server then imports the license. Repeat this step for each additional license you have received.

Step 5: Go to WCS Files

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

Figure 14. License Center, Add PAK

	ummary 🛈	🋦 o 🔻 o	• • • • • • • • • •	Wireless Control System	<ip,name,ssid,mac> Searce Advanced Search Saved Searce</ip,name,ssid,mac>
lisco					User: root @ Virtual Domain: root
Monitor ▼ R	eports 👻	<u>C</u> onfigure • <u>S</u> ervices •	<u>A</u> dministration ▼ <u>T</u> ools ▼ <u>H</u> elp ▼		🔞 🤣 📇 Logou
ummary	۲	License Center Administration > License	Center		
iii wcs		WCS Licenses		Permanent licenses include i	nstalled license counts and in-built license
Controller		Feature	O Unlicensed	counts.	
iles	(F)			MSE Licenses	
		Host	<u>2003-x86</u>	Tag Elements	
		AP Limit	0	Permanent Limit	0
		AP Count	0	Evaluation Limit	0
		% Used	0%	Count	0
		Туре	O Unlicensed	% Used	0%
			ke your Product Authorization Key (PAK) and and go to the <u>Product License Registration</u> ^{gar} p		

Figure 16. Importing License Files

License Center Administration > License Center > Files > WCS Files

PAK	Feature	AP Limit	Туре
20100520224156242	Plus	100	Permanent
20100520224206890	Plus	100	Permanent
20100520224236076	Plus	100	Permanent
Add Delete Export			

When you have completed importing licenses, all your license files should appear as shown in Figure 16. 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

Alarm Su CISCO	immary 🕀	▲ 0 ▼ 0		Wireless Control System <u>Advanced Search</u> <u>Seved Search</u> User: <u>root</u> © Virtual Domain: root
Monitor ▼ Re	sports 🔻	Configure - Services	★ Administration ★ Tools ★ Help ★	💡 🤯 🦉 Logoul
Summary	۲	License Center Administration > License	Center > Summary > WCS	
Controller		WCS Licenses		
MSE		Feature	Plus	
iles	۲	Host	<u>2003-x86</u>	
		AP Limit	300	
		AP Count	0	
		% Used	0%	
		Туре	Permanent	
		0 To add new licenses	take your Product Authorization Key (PAK) and the	
		host name (2003-x86 to get a license for WC) and go to the <u>Product License Registration</u> ^{ga} page S.	

Notes

Add Wireless LAN

Controllers 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.

Process 1. Login to the Wireless Control System 2. Add each controller to WCS

Procedure 1

Login to the Wireless Control System

Step 1: Connect to Wireless Control System

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

Step 2: Log into WCS as Administrator

Log in to the Cisco WCS server as the system administrator. (Be aware that usernames and passwords are case-sensitive.)

Procedure 2

Add Each Controller to WCS

Step 1: Go to Controllers

Navigate to Configure and then to Controllers, which should bring you to an empty list of controllers as shown in Figure 16 - Add Controllers.

Figure 18. Add Controllers

Alarm Sumn	nary 🔍 💧 🔺 0		
CISCO			
<u>M</u> onitor ▼ <u>R</u> epo	orts 🔻 <u>C</u> onfigure 🔻	Services - Administration - Tools -	<u>H</u> elp 🔻
Add Controllers			
Configure > <u>Controllers</u> > 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 C	apabilities 🔍		
SNMP Parameters 🔍			
Version	v2c	~	
Retries	2]	
Timeout	10	(secs)	
Committee (- d and a	7	
Community	private]	
Telnet/SSH Parameters			
User Name	admin		
Password	•••••	-	
Confirm Password	•••••		
Retries	3]	
Timeout	80	(secs)	
QK Cancel			
U .			

Step 2: Add All Controllers

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.

Tech Tip

You may enter each controller IP address separated by a comma, or you can select a comma-delimited (CSV) spreadsheet with the IP Addresses of all controllers. In the 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



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

Notes

Adding Buildings and Floor Plans

The real advantage to any management system is the presentation of the information which you can then use to make informed decisions. The Cisco WCS 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.

Process

- 1. Adding the First Campus and Building
- 2. Placing Access Points

Procedure 1

Adding the First Campus and Building

Every organizational method starts by categorizing the approach; with the Cisco WCS, 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 in-formation 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 in to the Cisco WCS.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



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 floor plan 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



Procedure 2

Placing 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 WCS 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.

Figure 27. Floor View

Alarm Summary (1)	▲ <u>18</u> ▼ 0 ○ <u>329</u> ▼	Wireless Control System	<ip,name,ssid,mac> Search Advanced Search Saved Search</ip,name,ssid,mac>
Monitor Y Reports Y Con	figure 🕶 Services 👻 Administration 👻 Tools	▼ Halo ▼	User: root @ Virtual Domain: root <
Maps Tree View ⊥ Floor Settings — ♥ ✿ Access Points > ♥ ♦ AP Heatmaps > ● • ●	Floor View Nontor > Mags > System Campus > SBA-Campus > S O Data may be delayed up to 15 minutes or m D Data may be delayed up to 15 minutes or m D Data may be delayed up to 15 minutes or m D Data may be delayed up to 15 minutes or m D Data may be delayed up to 15 minutes or m D Data may be delayed up to 15 minutes or m D Data may be delayed up to 15 minutes or m D Data may be delayed up to 15 minutes or m D Data may be delayed up to 15 minutes or m D Data may be delayed up to 15 minutes or m D Data may be delayed up to 15 minutes or m D Data may be delayed up to 15 minutes or m D Data may be delayed up to 15 minutes or m D Data may be delayed up to 15 minutes or m D Data may be delayed up to 15 minutes or m D Data may be delayed up to 15 minutes or m D Data may be delayed up to 15 minutes or m D Data may be delayed up to 15 minutes or m D D Data may be delayed up to 15 minutes or m D D D D D D D D D D D D D D D D D D D	BA-Headquarters tore depending on background polling interval	Select a command V Go Select a command Add Access Points
Cocation Regions Arails Arails Arakers Xtherefore Chokepoints			Edit Floor Area Delete Floor Area Edit Location Presence Info Map Editor
Save Settings	50 F		Planning Mode Inspect Location Readiness Inspect VoWLAN Readiness
MSE Assignment (+)			
Load Status –			

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



Tech Tip

You must now wait while the system calculates the heat maps from the placement and floor plan area.

Configuring CleanAir

With the Cisco WCS 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 WCS and configure our controller to support CleanAir.

Event Driven Radio Resource Management

Event Driven RRM (EDRRM) 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.

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.

Process



Procedure 1 Enable CleanAir

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

Monitor 🔻 R	eports 🔻 Configure 👻 S	ervices 🔻 Adminis	stration 🔻 Tools 👻 H	elp 👻		User: ros	ot @ Virtual Domain: ro 😰 📌 🕒 Lo
Controllers Configure > Control		ervices 👻 <u>A</u> dminis	aration	eip *	Select a con	nmand	v 60
							Entries 1 - 1 of 1
IP Address	Controller Name	Туре	Location	Software Version	Mobility Group Name	Reachability Status	Audit Status
192 (K68.31.6	4 명 HQ-WLC	5500		7.0.98.0	SBA	Reachable	Mismatch
							Entries 1 - 1 of 1
otnotes:							
	is updated based on the last	execution informati	on of 'Device Status' ba	ckground task. For upda	ting the current status,	use 'Execute Now' com	mand of Administration :

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.

Alarm Summary	Ð	▲ <u>17</u> ▼ 0 O <u>352</u> ▼ Wireless Control System
CISCO		
<u> <u> M</u>onitor ▼ <u>R</u>eports </u>	• <u>c</u>	Configure ▼ Services ▼ Administration ▼ Tools ▼ Help ▼
Properties	€	CleanAir : Configure > Controllers > 192.168.31.64 > 802.11a/n > CleanAir
System	۲	
WLANs	۲	
H-REAP	۲	Reporting Configuration
Security	⊳	Report Interferers 🗹 Enable
Access Points	⊛	Interferers Ignored for Reporting Interferers Selected for Reporting
802.11	⊛	Canopy Continuous Transmitter
802.11a/n		DECT-Like Phone Jammer SuperAG
 Parameters RRM Voice Parameters Video Parameters EDCA Parameters EDCA Parameters Roming Parameters 802.11h 		TDD Transmitter Video Camera WiFi Invalid Channel WiFi Inverted WiMAX Fixed WiMAX Mobile
High Throughput(802.11n)		Air Quality Alarm
CleanAir 802.11b/g/n	€	Air Quality Alarm Threshold 25 (1-100) Air Quality value 100 is best and 1 is worst
Mesh	•	Interferers For Security Alarm
Ports	•	Interferers Ignored for Security Alarms Interferers Selected for Security Alarms
Management	•	Canopy Continuous Transmitter DECT- Like Phone
Location	•	Jammer SuperAG
Location	۲	 TDD Transmitter Video Camera WiFi Invalid Channel WiFi Inverted WiM4X Kixed WiM4X Mobile

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

Alarm Summary	Ф.	▲ 17 Vireless Control Sys
sco		
<u>M</u> onitor - <u>R</u> eports	<u>-</u> ⊆	_onfigure ▼ _ Services ▼ _ Administration ▼ _ Tools ▼ _ Help ▼
Properties	۲	CleanAir : Configure > <u>Controllers</u> > 1 <u>92.168.31.64</u> > 802.11b/g/n > CleanAir
System	⊛	
WLANs	۲	CleanAir C Enable
H-REAP	۲	Reporting Configuration
Security	۲	Report Interferers 🗹 Enable
Access Points	۲	Interferers Ignored for Reporting 802.15.4
802.11	۲	802.11FH Bluetooth Discovery
802.11a/n	۲	Bluetooth Link
802.11b/g/n	•	Continuous Transmitter COLLike Phone
Parameters		Jammer Microwave Oven
RRM Voice Parameters		SuperAG TDD Transmitter
Video Parameters		Video Camera
EDCA Parameters		Alarm Configuration
Roaming Parameters High Throughput(802.11n)		Air Quality Alarm
CleanAir		Air Quality Alarm Threshold 35 (1-100) Air Quality value 100 is best and 1 is worst
Mesh	۲	Interferers For Security Alarm
Ports	۲	Interferers Ignored for Security Alarms Interferers Selected for Security Alarms
Management	۲	802.15.4 802.11FH
Location	۲	Bluetooth Link Bluetooth Discovery
		Canopy Continuous Transmitter
		< DECT-Like Phone
		Jammer Microwave Oven
		SuperAG TDD Transmitter

Procedure 2

Enable Event Driven RRM

Step 1: Continuing in Cisco WCS, from the left-side menu, navigate to 802.11a/n > RRM > DCA.

Figure 34. DCA Parameters for 802.11a/n

Alarm Summary	Ф.	🔺 <u>17</u>	0	<u> </u>	Y	Wireless Control Syster
CISCO						
Monitor	<u>▼ ⊆</u>	Configure - <u>S</u> er	vices 👻	Administration	▼ <u>T</u> ools ▼ <u>H</u> elp ▼	
Properties	۲	DCA :			14-1 DDM - DOA	
System	۲	Configure > <u>Contr</u>	rollers > 15	<u>92.168.31.64</u> > 802.1	1a/n > RRM > DCA	
WLANs	€	0 4.9Ghz chanr	nels will b	e shown and can	be configured only if Public	Safety option is enabled.
H-REAP	⊛	Dynamic Chan	nel Assi	gnment Algoritl	ım	
Security	•	Template Ap	olied			
Access Points	•	Assignment			Automatic 🗸	
	-	Update Inter			600 (secs)	
802.11	۲	Avoid Foreig	in AP Inte	rference	Enable	
802.11a/n	€	Avoid Cisco	AP load		Enable	
Parameters		Avoid non 8	02.11 Nois	se	Enable	
 RRM Thresholds 		Avoid Persis	tent Non-	WiFi Interference	Enable	
Intervals		Signal Stren	gth Contr	ibution	Enable	
Diffe vais		Outdoor AP	DCA		Enable	
RF Grouping		Channel Wid	ith		20 MHz 💌	
Voice Parameters		DCA List Chan	nels			
Video Parameters EDCA Parameters Roaming Parameters 802.11h High Throughput(802.11n)		Selected DC	A channe	Is	36, 40, 44, 48, 52, 50 153, 157, 161	5, 60, 64, 149,
802.11b/g/n	۲	Select C	hannel			^
Mesh	۲	36				
Ports	⊛	 ✓ 40 ✓ 44 				
Management	•	✓ 44 ✓ 48				
-	-	52				
Location	۲					

Step 2: Check the checkbox for Event Driven RRM and click Save.

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

WLANs	€	0 4.9Ghz c	nannels wil	l be shown and can be	configured only if Pub	lic Safety option is e	enabled.
H-REAP	€	Dynamic C	hannel As	signment Algorithn	1		
Security	€	Template	e Applied				
Access Points	⊛	Assignm	ent Mode		Automatic 💌		
802.11	•	Update I	nterval		600 (secs)		
802.11a/n	•		-	terference	Enable		
	U		sco AP load		Enable		
Parameters RRM			n 802.11 N		Enable		
Thresholds				n-WiFi Interference	Enable		
Intervals		-	trength Co	ntribution	Enable		
DCA		Outdoor			Enable		
RF Grouping		Channel			20 MHz 💙		
Voice Parameters		DCA List C	nannels				
Video Parameters EDCA Parameters		Selected	DCA chan	nels	36, 40, 44, 48, 52,	56, 60, 64, 149,	~
Roaming Parameters					153, 157, 161		
🖹 802.11h							
High Throughput(802.11n)							~
📄 CleanAir							
802.11b/g/n	⊛	Select	Channel				^
Mesh	⊛		36				
Ports	⊳		40 44				
Management	€		48				
Location	⊳	 Image: A start of the start of	52				
Location	U	~	56				~
		Event Driv	on DDM				
		Event Driv	en KKPI				
		Event Dr	iven RRM)	Enable		
		Sensitivi	ty Thresho	ld 🔍	Medium 💌		
		Since Audi	t				
🛃 start 💦 🧷 Cisco WCS	- Con						

Step 3: From the left-side menu, navigate to 802.11b/g/n > RRM > DCA.

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

Monitor ▼ Reports ▼ Configure ▼ Services ▼ Administration ▼ Tools ▼ Help ▼ Properties DCA System DCA WLANs DCA WLANs DCA H-REAP Domanic Channel Assignment Algorithm Access Points Automatic ▼ B02.111 Deameters Controllers Solution (Sec.s) Avoid Foreign AP Interference Enable Avoid Oreign AP Interference Enable Avoid Persistent Non-WiFi Interference Enable Signal Strength Contribution ✓ Enable Parameters Selected DCA channels: 1, 6, 11 Wideo Parameters DCA Channels Select Channel Wideo Parameters 2 3 Wideo Parameters 2 3 Wideo Parameters 2 3 Wideo Parameters 2 3 Wideo Parameters 3 4	ss Control System
Configure > Controllers > 192.168.31.64 > 802.11b/g/n > RRM > DCA System Dynamic Channel Assignment Algorithm H-REAP Template Applied Access Points Avoid Foreign AP Interference 802.11 Avoid Foreign AP Interference 802.11a/n Avoid Foreign AP Interference Boz.11a/n Avoid Porsistent Non-WiFi Interference Boz.11b/g/n Selected DCA channels: Improved Thresholds Improved Selected DCA channels: Improved CA Channels Select Channel Select Channel	
System Dynamic Channel Assignment Algorithm WLANs Dynamic Channel Assignment Algorithm H-REAP O Security O Access Points O B02.111 O B02.111 O B02.111 O B02.111 O B02.112/n O B02.11b/g/n O B1 Thresholds Selected DCA channels: I, 6, 11 Intervals Selected DCA channels: I, 6, 11 Intervals Select Channels I Intervals I I I Intervals I I I Intervals I I I Intervals I I I Intervals I <thi< th=""> I <thi< th=""></thi<></thi<>	
H-REAP Image: Constraint of the second s	
Security Assignment Mode Automatic Security Update Interval 600 (secs) Access Points Avoid Foreign AP Interference Enable 802.11 Avoid Gisco AP load Enable 802.11a/n Avoid Hore 802.11 Noise Enable 802.11b/g/n Avoid Persistent Non-WiFi Interference Enable Parameters Select Channels Enable Parameters DCA List Channels: 1, 6, 11 Web Parameters DCA Channels 1 Wideo Parameters 2 3 Wideo Parameters 3 3	
Security Image: Constraint of the security Access Points Update Interval 500 (secs) Access Points Avoid Foreign AP Interference Enable 802.11 Avoid Cisco AP load Enable 802.11a/n Avoid Cisco AP load Enable 802.11b/g/n Avoid Persistent Non-WiFi Interference Enable 802.11b/g/n Signal Strength Contribution Enable Parameters DCA List Channels Enable Intervals Selected DCA channels: 1, 6, 11 Intervals Select Channel Image: Channel Video Parameters DCA Channels Image: Channel Wideo Parameters Image: Channel Image: Channel Image: Roaming Parameters Image: Channel Image: Channel Roaming Parameters Image: Channel Image: Channel Roaming Parameters Image: Channel Image: Channel	
Access Points Update Interval 500 (soce) Access Points Avoid Foreign AP Interference Enable 802.11 Avoid Foreign AP Interference Enable 802.11a/n Avoid Foreign AP Interference Enable 802.11b/g/n Avoid Persistent Non-WiFi Interference Enable 802.11b/g/n Signal Strength Contribution Enable Parameters DCA List Channels: 1, 6, 11 Intervals Intervals Video Parameters Voice Parameters DCA Channels Intervals Video Parameters 1 2 Roaming Parameters 3	
Avoid Foreign AP Interference ✓ Enable 802.11 Avoid Foreign AP Interference ✓ Enable 802.11a/n Avoid Cisco AP load Enable 802.11b/g/n Avoid Persistent Non-WiFi Interference ✓ Enable 802.11b/g/n Avoid Persistent Non-WiFi Interference ✓ Enable Image: Signal Strength Contribution ✓ Enable Image: Select d DCA channels ✓ Image: Network ✓ Image: Select d DCA channels ✓ Image: Network	
802.11a/n Avoid non 802.11 Noise Enable Avoid non 802.11 Noise Enable Avoid Persistent Non-WiFi Interference Enable Signal Strength Contribution Enable DCA List Channels: If A control CA channels: If A control CA channels Select Channel CA channels CA channels CA channels CA channels If CA channels Select Channel If CA channels If CA channels	
Avoid Persistent Non-WiFi Interference B02.11b/g/n Brameters RRM Thresholds Thresholds Thresholds Thresholds Parameters DCA List Channels: 1, 6, 11 Parameters DCA Channels Voice Parameters Voice Parameters Voice Parameters CA Roaming Parameters Roaming Parameters	
B02.11b/g/n Signal Strength Contribution Image: Contribution Parameters DCA List Channels Image: Thresholds Selected DCA channels: Image: Thresholds Selected DCA parameters Image: Thresholds Selected DCA parameters Image: Thresholds Thresholds Image: Thresholds Selected DCA parameters Image: Threshol	
image: Parameters DCA List Channels image: RRM DCA List Channels image: RRM DCA List Channels image: Rred manage: Registration of the second seco	
□ High Info@put(002.11h) □ CleanAir Mesh ⓒ ⓒ 6 ♥ 6	
Ports Event Driven RRM	
Management Event Driven RRM Enable Location Save Audit	

Step 4: Check the checkbox for Event Drive RRM and click Save.

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

Alarm Summary	Ф.	····▲ <u>17</u> ······▼ 0 ······ ● <u>355</u> ··			Wireless Control Sy
sco					
<u>M</u> onitor - <u>R</u> eports	• <u>c</u>	Configure 🔻 Services 👻 Administration 👻	<u>T</u> ools	▼ <u>H</u> elp ▼	
operties	۲	DCA : Configure > <u>Controllers</u> > <u>192.168.31.64</u> > 802.1	1b/a/n > R	RM > DCA	
/stem	۲				
LANs	⊛	Dynamic Channel Assignment Algorith	ım		
REAP	۲	Template Applied			
ecurity	۲	Assignment Mode	Automa		*
ccess Points	€	Update Interval	600 (sec:		
		Avoid Foreign AP Interference	🗹 Ena		
02.11	۲	Avoid Cisco AP load	Ena		
)2.11a/n	۲	Avoid non 802.11 Noise Avoid Persistent Non-WiFi Interference	Ena		
)2.11b/g/n	•	Signal Strength Contribution	Ena		
Parameters		DCA List Channels	C Llia	bie	
RRM					
Thresholds		Selected DCA channels:	1, 6, 11		
DCA					<u>~</u>
RF Grouping		DCA Channels	Select	Channel	^
Voice Parameters				1	
Video Parameters				2	
Roaming Parameters				3	
High Throughput(802.11n)				4	
📄 CleanAir				5	
esh	۲		V	6	<u>×</u>
orts	۲	Event Driven RRM			
anagement	⊳	Event Driven RRM	🗹 Enat	le	
cation	€	Sensitivity Threshold 🕸	Medium	*	
	0	Silwe Audit			

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 Cisco 3500 Series 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 trouble-shoot 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 has indicates AirQuality has dropped.

Process

1. Configure Spectrum Connect

Procedure 1

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 in to 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

راریان cisco	MONITOR	WLANS CONTR	OLLER WIREL	ESS SECURITY	MANAGEMENT	COMMANDS	HELP FEEDBACK		Lo <u>d</u> out <u>R</u> efre
Vireless	All APs > D	All APs > Details for MONITOR-AP						< Back	Apply
All APs	General	Credentials	Interfaces	High Availability	Inventory	Advanced			
 Radios 802.11a/n 802.11b/g/n 	General				Versions				
Global Configuration					Primary Software Version Backup Software Version Predownload Status Predownloaded Version		7.0.98.0		
Advanced							0.0.0.0		
Mesh							None		
HREAP Groups							None		
802.11a/n				Predownload	Next Retry Time	e NA			
802.11b/g/n	AP Mode local AP Sub Mode H-REAP Operational Status monitor Rogue Detector Port Number Sniffer			*	Predownload	Retry Count	NA		
Media Stream					IOS Version 12.		12.4.2.4		
Country							12.4(23c)JA		
Timers							0.0.0.0		
∳ Q₀S			SE-Connect	3	IP Config				
					IP Address		192.168.8.237		
					Static IP				
					Time Statistics				
					UP Time		0 d, 00 h 01 m 16	s	
					Controller A	ssociated Time	0 d, 00 h 00 m 20	s	
					Controller A	ssociation Latenc	y 0 d, 00 h 00 m 55	s	
	Hardware Reset Set to			Set to Fa	ctory Defaults				
	Perform a hardware reset on this AP Reset AP Now			Clear default	configuration on thi	s AP and reset it	to factory		
				C	Clear All Config				
					Clear Config Ex	cept Static IP			

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

Figure 39. Capture Network Key and IP Address

General	Credentials	Interfaces	High Availability	Inventory	Advanced		
General				Versions			
AP Name		IONITOR-AP		Primary Soft	ware Version	7.0.98.0	
Location		Zest AP		Backup Software Version		0.0.0	
AP MAC	Address c	4:7d:4f:3a:e5:44		Predownload	Status	None	
Base Rad	dio MAC 0)4:fe:7f:48:db:a0		Predownload	led Version	None	
Admin St	tatus I	Enable 🔽		Predownload	Next Retry Time	NA	
AP Mode SE-Connect 🗸			Predownload Retry Count		NA		
AP Sub N	P Sub Mode None 🐱			Boot Version		12.4.2.4	
Operatio	nal Status 🛛 🛛	EG		IOS Version		12.4(23c)JA	
Port Num	nber 1	.3		Mini IOS Ver	sion	0.0.0	
Network Interface	Spectrum	49DAFD8192BAB41	44EB130F02B9D991	IP Config			
				IP Address		192.168.8.236	
				Static IP			
			Time Statistics	5			
				UP Time		0 d, 16 h 50 m 23 s	
				Controller As	ssociated Time	0 d, 16 h 49 m 27 s	
				Controller As	ssociation 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 40. Launch Spectrum Expert



Step 9: Select the Remote Sensor radio button.

Step 10: Enter the IP address of the CleanAir access point

Step 11: Enter the Network Spectrum Interface Key of the CleanAir access point.

Step 12: Select either 2.4Ghz by selecting the **b/g/n** radio button or the 5Ghz by selecting the a/n radio button.

Step 13: 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.

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. 2.4 GHz 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 Number	Software Version	
Headquarters	Cisco WCS	WCS-STANDARD-K9	7.0.164.0	
		WCS-APBASE-100		
		WCS-ADV-SI-SE-10= (optional)		
	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	

Appendix B: SBA for Midsize Agencies Document System







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.

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. 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)

C07-641135-00 12/10