Newer Design Guide Available

Cisco Smart Business Architecture has become part of the Cisco Validated Designs program. For up-to-date guidance on the designs described in this guide, see http://cvddocs.com/fw/Aug13-350 For information about the Cisco Validated Design program, go to http://www.cisco.com/go/cvd





Wireless LAN CleanAir **Deployment Guide**

SMART BUSINESS ARCHITECTURE

February 2013 Series

BORDERLESS NETWORKS DEPLOYMENT GUIDE SBA

1 1 1 1-1-

CISCO

Preface

Who Should Read This Guide

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation
 documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

Release Series

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a 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.

The Release Notes for a series provides a summary of additions and changes made in the series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

month year Series

For example, the series of guides that we released in February 2013 is the "February Series".

You can find the most recent series of SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

How to Read Commands

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

configure terminal

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

ntp server 10.10.48.17

Commands with variables that you must define appear as follows:

class-map [highest class name]

Commands shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

Router# enable

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

wrr-queue random-detect max-threshold 1 100 100 100 100 100

100 100 100

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

interface Vlan64

ip address 10.5.204.5 255.255.2

Comments and Questions

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

If you would like to be notified when new comments are posted, an RSS feed is available from the SBA customer and partner pages.

February 2013 Series

Table of Contents

What's In This SBA Guide	1
Cisco SBA Borderless Networks	. 1
Route to Success	. 1
About This Guide	. 1
Business Overview	.2
Technology Overview	.3
Cisco CleanAir Technology	. 3
Cisco Prime Infrastructure 1.3	. 3

Deployment Details4
Installing and Configuring Cisco Prime Infrastructure 1.34
Adding Buildings and Floor Plans to Cisco Prime Infrastructure 1.317
Configuring the Wireless Network for Cisco CleanAir21
Installing the Cisco Mobility Services Engine Virtual Appliance26
Configuring Cisco Prime Infrastructure 1.3 for the Cisco MSE VA34
Troubleshooting with Cisco CleanAir
Viewing and Analyzing Cisco CleanAir42
Appendix A: Product List
Appendix B: Changes

What's In This SBA Guide

Cisco SBA Borderless Networks

Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.

Cisco SBA Borderless Networks is a comprehensive network design targeted at organizations with up to 10,000 connected users. The SBA Borderless Network architecture incorporates wired and wireless local area network (LAN) access, wide-area network (WAN) connectivity, WAN application optimization, and Internet edge security infrastructure.

Route to Success

To ensure your success when implementing the designs in this guide, you should first read any guides that this guide depends upon—shown to the left of this guide on the route below. As you read this guide, specific prerequisites are cited where they are applicable.

About This Guide

This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- Business Overview—Describes the business use case for the design. Business decision makers may find this section especially useful.
- Technology Overview—Describes the technical design for the business use case, including an introduction to the Cisco products that make up the design. Technical decision makers can use this section to understand how the design works.
- **Deployment Details**—Provides step-by-step instructions for deploying and configuring the design. Systems engineers can use this section to get the design up and running quickly and reliably.

You can find the most recent series of Cisco SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel



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. Of 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 you triple the challenges and skill set required to maintain and troubleshoot the network. Wireless networking brings a new set of unknowns that an administrator of a wired network never had to address.

Wi-Fi is no longer just a convenient technology used for casual web surfing or simple connectivity from conference rooms; it has now become a strategic part of business, education, and government. With 802.11n, wireless performance is now on par with wired networks, and businesses and organizations, such as hospitals, rely on the wireless network for mission-critical and patient-critical applications. Without running expensive site surveys with a spectrum analyzer every hour and minute of every day, the network administrator cannot tell what is happening in the user space. With limited IT resources and a lack of RF expertise, an organization requires tools to alert for potentially negative issues before a user creates a call ticket in the network call center.

Notes



Technology Overview

Cisco CleanAir Technology

Cisco CleanAir technology is the integration of Cisco Spectrum Expert Wi-Fi analysis tools with Cisco access points. Before CleanAir technology was released, operators had to walk around with an instrument to detect signals of interest and physically locate the device that generated them. CleanAir helps to automate these tasks within the system management function by adding additional intelligence over Cisco Spectrum Expert, thereby augmenting the overall experience by proactively reclaiming control over the radio spectrum. With the addition of the Cisco Mobility Services Engine virtual appliance (MSE VA), historical CleanAir information is accessible by network operators. This increased off-hours RF-based situational awareness is ideally suited for those environments that require 24x7x365 RF spectrum management, such as hospitals and manufacturing environments.

The components of a basic Cisco CleanAir solution are the Cisco wireless LAN controller and Cisco Aironet 2600 or 3600 Series access points. To take advantage of the entire set of CleanAir features, Cisco Prime Infrastructure 1.3 can display in real-time the data retrieved from CleanAir.

Cisco Prime Infrastructure 1.3 with Cisco CleanAir technology allows network administrators to visually see how well their network is performing, remotely troubleshoot client connectivity, manage wireless network resources, analyze interference devices from anywhere in the world, and more. The real power of Prime Infrastructure 1.3 with CleanAir combined with Cisco access points is the ability to visually represent the health of the RF environment to the network administrator. This allows the administrator to better manage and troubleshoot issues before they impact the end user. With Cisco MSE included in the solution, the administrator can turn back the clock and look at RF issues that occurred in the past—typically the case encountered due to the delay in reporting such issues and second-level support being engaged.

Cisco Prime Infrastructure 1.3

Cisco Prime Infrastructure enables you to configure and monitor one or more Cisco wireless LAN controllers and associated access points, monitor and troubleshoot radio technology, and visually display Cisco CleanAir data to the network administrator. Cisco Prime Infrastructure 1.3 includes the same configuration, performance monitoring, security, fault management, and accounting options used at the controller level, and it adds a graphical view of multiple controllers and managed access points.

Cisco Prime Infrastructure 1.3 is offered in both a physical and virtual appliance deployment option, providing full product functionality, scalability, ease of installation, and setup tailored to your deployment preference.

Deployment Details

To manage the Cisco Wireless LAN Controller version 7.4 with Cisco Prime Infrastructure, you must use version 1.3 of Cisco Prime Infrastructure. The procedures for properly installing and configuring Prime Infrastructure 1.3 have been provided. Please complete the following process in order to install Prime Infrastructure 1.3.

Process

Installing and Configuring Cisco Prime Infrastructure 1.3

- 1. Obtain a license
- 2. Install software
- 3. Customize the VMware environment
- 4. Configure basic settings
- 5. Configure user authentication
- 6. Configure users and user groups
- 7. Add devices and credentials

There are two ways to acquire a license. If you are using physical media, complete Option 1. If you are downloading an evaluation version of the software, complete Option 2.

Option 1. Physical media

When you purchase a product DVD, it comes with a Product Authorization Key (PAK). The PAK is normally printed on the software claim certificate included with product DVD kit.

Step 1: In a web browser, go the following site: http://cisco.com/go/license

Step 2: Select the Click here to continue to Product License Registration button and enter the PAK license key that you were given.

Procedure 1

Obtain a license

Cisco Prime Infrastructure 1.3 offers a single software installation that can manage up to 10,000 devices. Software licensing allows you to evaluate the software before deciding how you want to proceed: purchasing the license, piloting a small deployment before rolling it out organization-wide, or growing your network management system along with your network. Licensing allows you to first evaluate the software without requiring that you reinstall the software later.

Option 2. Evaluation software

Step 1: Download an evaluation copy of Prime Infrastructure from the following site:

http://cisco.com/go/nmsevals

cisco	Solutions	Products & Services	Ordering	Support	Training & Events	Partner Central	С
Cisco Store Cisco	Promotional Software	: Store					0 Items in Cart Cher
Unified Comm	unications	Networ	k Manageme	nt Trial Dov	wnloads		
All Items							
System Relea: Offering (PBO)		(P			Solution (WINDOW Release date : Oct 2	S OS) 4.2 - Updated 29 2012	
Cisco WebEx I Software Dowr	Meetings Server Tria nload					i integrated suite of man	
Unified Comm Software Partn (ELECTRONIC	er Bundle Offer Kit		simplify the con technologies. Read more	figuration, admi	nistration, monitorin	g, and troubleshooting c	of Cisco® networks and
Network Mana Downloads	gement Trial		Free Download			to Cart	
All Items		Cash I	Cisco Prime Inf	rastructure 1.3	ease date : Feb 20 2	2013	
Cisco Prime N (Windows)	letwork Registrar 8.					ted solution for complet	e lifecycle and
	letwork Registrar 8. Jal Appliance for				pplication performa	nce. Ci Read more	, along with deep visibility
Cisco Prime C Provisioning 9			Free Download	ł	Add	to Cart	
Cisco Prime C Provisioning 9		C000			Solution 4.2. Virtua - Release date : Fel		
Cisco Prime C Assurance 9.0			simplify the con			i integrated suite of man g, and troubleshooting c	
Network Mana Resale	gement Not-For-		technologies. Read more				
All Items			Free Download	ł	- Add	to Cart	

Via email, you will receive a PAK license key.

Step 2: In a web browser, go the following site: http://cisco.com/go/license

Step 3: Click Click here to continue to Product License Registration and enter the PAK license key that you were given.



Install software

You can install the Cisco Prime Infrastructure 1.3 soft appliance by using the Prime Infrastructure Open Virtualization Archive (OVA) image. Before installing, please note the following:

- Make sure that your system meets the recommended hardware and software specifications listed in the Cisco Prime Infrastructure release notes.
- It takes approximately 30 minutes (deployment in the local system) or 50 minutes (deployment in the network) to install the soft appliance on a virtualized environment.
- Soft appliance OVA software can be installed only in a VMware environment.

Tech Tip

You do not need to install any soft appliance image on the virtual machine (VM) before installing Cisco Prime Infrastructure, because the Prime Infrastructure OVA image has an embedded RedHat Enterprise soft appliance.

It is recommended you do the following before installing the Cisco Prime Infrastructure 1.3 soft appliance:

- · Configure DNS entries for each network device.
- Enable Simple Network Management Protocol (SNMP) and Secure Shell (SSH) Protocol on the devices you are going to import.
- Create an email address that Cisco Prime Infrastructure will use on your internal email server in order to send reports to subscribed users.

Step 1: In the VMware vSphere client, click File, and then choose Deploy OVF Template.



Step 2: In the Deploy OVF Template wizard, on the Source page, browse to the location of the Cisco Prime Infrastructure OVA file, and then click **Next**.

Step 3: On the OVF Template Details page, review the OVF template details, and then click **Next**.

🛃 Deploy OVF Template			- • ×
OVF Template Details Verify OVF template details.			
Source OVF Template Details Name and Location Host / Cluster Resource Pool Disk Format Ready to Complete	Product: Version: Vendor: Publisher: Download size: Size on disk: Description:	Cisco Prime Network Control System Virtual Appliance 1.3.0.20 Cisco Systems, Inc No certificate present 4.5 G8 Unknown (thin provisioned) 195.3 G8 (thick provisioned)	
Help		< Back Next	> Cancel

Step 4: On the Name and Location page, enter a unique and descriptive name for the virtual appliance that you are installing (Example: PI-1-3), choose a location to install the virtual appliance, and then click **Next**.

Step 5: On the Host /Cluster page, choose the host or cluster on which to install this virtual machine, and then click **Next**.

Step 6: On the Storage page, choose where you want to store the virtual machine files, and then click **Next**.

Step 7: On the Disk Format page, select **Thick Provision Lazy Zeroed**, and then click **Next**.

Step 8: On the Network Mapping page, in the Destination Networks column, choose the appropriate network mapping group previously defined to the VMware environment (Example: Servers_1), and then click **Next**.

Deploy OVF Template			
Network Mapping What networks should t	he deployed template use?		
Source OVF Template Details Name and Location	Map the networks used in this OVF	template to networks in your inventory	
Host / Cluster	Source Networks	Destination Networks	
Storage	Default	Servers_1	•
<u>Disk Format</u> Network Mapping			
Ready to Complete		1	g
	Description:		
	Default Network		×
Help		< Back Next >	Cancel

Step 9: On the Ready to Complete page, review the selected options, and then click **Finish**. The OVF installation of Cisco Prime Infrastructure 1.3 begins.

Procedure 3

Customize the VMware environment

(Optional)

It may be necessary to customize the VMware environment so that keystrokes are not accidently repeated when typing in the console window. If you find that key strokes are repeating when entering various settings, it may be necessary to configure a keyboard delay value. This procedure is optional but is included here in the event that it is required.

Step 1: Using the vSphere client access the VMware vCenter environment and highlight the Prime Infrastructure virtual host just installed, and then on the Getting Started tab, click **Edit virtual machine settings**.

Step 2: On the Virtual Machine Properties dialog box, click the **Options** tab, select **General**, and then click **Configuration Parameters**.

PI-1-3-20 - Virtual Machine Pro	perties	
Hardware Options Resources Pr	ofiles VServices	Virtual Machine Version: 7
Hardware Options Resources Pr Settings General Options vApp Options Properties IP Allocation Policy OVF Settings Advanced VMware Tools Power Management Advanced General CPUID Mask General CPUID Mask Memory/CPU Hotplug Boot Options Fibre Channel NPIV CPU/MMU Virtualization Swapfile Location	ofiles vServices Summary PI-1-3-20 Enabled Configured Fixed, IPv4 Enabled Configured Shut Down Standby Normal Expose Nx flag to Disabled/Disabled Normal Boot None Automatic Use default settings	Virtual Machine Version: 7 Settings Disable acceleration Renable logging Debugging and Statistics Run normally Record Debugging Information Record Statistics Record Statistics Configuration Parameters Click the Configuration Parameters button to edit the advanced configuration settings. Configuration Parameters
Help		OK Cancel

Step 3: On the Configuration Parameters dialog box, click **Add Row**, in the Name column, enter **keyboard.typematicMinDelay**, and in the Value column, enter **2000000** (2 million), and then click **OK**.

Configuration Parameters

Modify or add configuration parameters as needed for experimental features or as instructed by technical support. Entries cannot be removed.

Name 🗠	Value						
pciBridge5.vir	pcieRootPort						
pciBridge5.fu	8						
pciBridge6.pr	true						
pciBridge6.vir	pcieRootPort						
pciBridge6.fu	8						
pciBridge7.pr	true						
pciBridge7.vir	pcieRootPort						
pciBridge7.fu	8						
vmware.tools	0						11
vmware.tools	8389						H
vmware.tools	none						11
vmware.tools	unknown						
migrate.host	none						
migrate.migra	0						
keyboard.typ	2000000						
٠		.111				•	Ť
						Add Ro	w
			01	1	Garant	Liele	
			OK		Cancel	Help	

Step 4: On the Virtual Machine Properties dialog box, click OK.

Step 5: On the newly installed virtual machine, click the **Getting Started** tab, and then click **Power on the virtual machine**.

Step 6: To begin the setup wizard, access the **Console** tab and enter **setup** as the localhost login user ID. This one time login with automatically start the setup script.



Step 7: In the startup script, enter the following configuration details for the server :

· Hostname-Prime-Infra

×

- · IP address—10.4.48.35
- · IP netmask-255.255.255.0
- · Default gateway-10.4.48.1
- · DNS domain name—cisco.local
- Primary name server—10.4.48.10
- Add/Edit another name server? Y/N—N
- Primary NTP server—10.4.48.17
- Add/Edit secondary NTP server? Y/N—N
- System time zone—PST8PDT



Step 8: Create a username and password for accessing the Cisco Prime Infrastructure appliance console. This user will have the privilege to enable the shell access.

Tech Tip

The default username is **admin**. You cannot use **root** as the username because it is a reserved username. You can use only alphanumeric characters for the username. Enter and confirm the admin password. By default, this password is set as the shell password.

PI-1-3-20

Getting Started Summary Resource Allocation Performance Tasks & Events Alarms, Console Permissions Maps Storage Views

Press 'Ctrl-C' to abort setup Enter hostname[]: Prime-Infra Enter IP address[]: 10.4.48.35 Enter IP default netmask[]: 255.255.255.0 Enter IP default gateway[]: 10.4.48.1 Enter default DNS domain[]: cisco.local Enter primary nameserver[]: 10.4.48.10 Add/Edit another nameserver? Y/N : N Enter primary NTP server[time.nist.gov]: 10.4.48.17 Add/Edit secondary NTP server? Y/N : N Enter system timezone[UTC]: PST8PDT Enter username[admin]: Enter password Enter password again: Bringing up network interface... Pinging the gateway... Pinging the primary nameserver... Do not use 'Ctrl-C' from this point on... Appliance is configured Installing applications... Installing NCS ...

Step 9: If you are planning to use this server as a standalone server or if this is the first or primary server, at the Will this server be used as a Secondary for HA? prompt, enter no.

_	
	PI-1-3-20
	Getting Started Summary Resource Allocation Performance Tasks & Events Alarms Console Permissions Maps Storage Views
	Enter password again:
	Bringing up network interface
	Pinging the gateway
	Pinging the primary nameserver
	Do not use ' $Ctrl-C'$ from this point on
	Appliance is configured
	Installing applications
	Installing NCS Prime Infrastructure Application installation completed
	Install Completed Successfully
	find: /storeddata/Installed: No such file or directory
	Application Install Completed.
	Post-install Process Started
	Post-install Version Validation Process Started
	* Cisco Prime Infrastructure Setup *

	Enter "^" to return to previous question.

	* High Availability Role Selection *

	Will this server be used as a Secondary for HA? (yes/no):no_

Step 10: Enter and confirm the password for the root account that will be used to access the GUI through a browser. This password must contain a minimum of five characters and is also used for the System Identity account.

Step 11: Enter and confirm an FTP password, review the settings, and then at the **Apply these settings?** prompt, enter **Y**.

-1-3-20	
etting Started Summary Resource Allocation Performance Tasks & Events Alarms Console Permissions	Maps Storage Views
Enter root password:	
Enter root password again:	
Enter root password again.	
* FTP Password Selection	
7	
Enter ftp password:	
Enter ftp password again:	
* Summary *	

Server will not be a Secondary	
Root Password is set.	
Ftp Password is set.	
Apply these settings? (y/n)y	
Settings Applied.	
Application bundle (NCS) installed successfully	
=== Initial Setup for Application: NCS ===	
Running database cloning script	

It takes 15 to 20 minutes to process the database engine, and then the server automatically reboots.

PI G

I-1-3-20	
-1-3-20	
Setting Started Summary Resource Allocation Performance Tasks & Events Alarms Console Permissions Maps Storage	Views
Enter root password:	
Enter root password again:	

FTP Password Selection	
* * * * * * * * * * * * * * * * * * * *	
Enter ftp password:	
Enter ftp password again:	

* Summary *	

Server will not be a Secondary	
Root Password is set.	
Ftp Password is set.	
Apply these settings? (y/n)y	
Settings Applied.	
Application bundle (NCS) installed successfully	
approaction balance theory instantion endocourting	
=== Initial Setup for Application: NCS ===	
Running database cloning script	
Running database creation script	

Procedure 4

Configure basic settings

Tech Tip

Prime Infrastructure supports the following browsers.

- Google Chrome—19.0 build
- Mozilla Firefox— ESR 10.x, 13.0 and 14.0
- Microsoft Internet Explorer 8.0 or 9.0 with Chrome plug-in.

Native Internet Explorer is not supported. The recommended minimum resolution for each browser is 1280 x 800 pixels

Step 1: On the client machine, in a web browser, disable any pop-up blockers.

Next, you enable JavaScript.

Step 2: If you are using Internet Explorer 8 or later, navigate to Tools > Internet Options > Security > Custom level > Settings, and then under Scripting of Java applets, select Enable.

If you are using Mozilla Firefox 9.x, navigate to **Tools > Option > Content**, and then select **Enable JavaScript**.

If you are using Chrome 19 or later, navigate to Chrome > Preferences > Privacy, click Content Settings, and then under JavaScript, select Allow all sites to run JavaScript.

Step 3: In the web browser, open the Cisco Prime Infrastructure portal (Example: https://prime-infra.cisco.local).

Step 4: Log in by using the username **root** and the password that you provided during installation.



Step 5: Navigate to Administration > System Settings > Mail Server Configuration, and then in the Primary SMTP Server section, in the Hostname/IP box, enter the host name of the SMTP server (Example: smtp. cisco.local).

Step 6: In the Sender and Receiver section, in the **From** box, enter the email address from which you want to send notifications, and then in the **To** box, enter the email address to which you want notifications sent.

Step 7: Select Apply recipient list to all existing alarm email notifications,

and then click **Save**. This enables you to receive email alerts about network issues, job status, report generation, etc.

Mail Server Configurati	on			
Administration > System Setting				
Primary SMTP Server				
Hostname/IP	smtp.cisco.local	Port	25	
Username (Optional)				
Password				
Confirm Password				
Secondary SMTP Server (Op	tional)			
Hostname/IP		Port	25	
Username (Optional)				
Password				
Confirm Password				
Sender And Receivers				
From	PI@Prime-Infra.cisco.local			
То	johnsmith@thiscompany.com			
10	comma-separated email addresses			
Apply recipient list to all examples of the second seco	kisting alarm email notifications.			
Subject	This text will be appended to the email	subject		
Configure email notification f	or individual alarm categories.	500,000		
Save Cancel Test	Delete			

Procedure 5

Configure user authentication

(Optional)

Cisco Prime Infrastructure can use its local database, RADIUS or TACACS+ in order to authenticate user logins. To enable a common authentication experience for network administrators across network devices and the network management system, this guide describes how to configure Cisco Prime Infrastructure to use TACACS+ authentication.

Step 1: Navigate to Administration > Users, Roles & AAA, and then in the left column, select AAA Mode.

Step 2: Select TACACS+ and Enable fallback to Local, and in the list, choose ONLY on no server response, and then click Save.

cisco Prime cisco Infrastructure	Virtual Domain ROOT-DOMAIN root v
cisco Infrastructure	🏠 Home Design 🔻 Deploy 🔻 Operate 🔻 Report 🔻 Administration 👻 📂 🕄 🚱 🗸
Users, Roles & AAA	
Change Password	AAA Mode Settings Administration > Users, Roles & AAA > AAA Mode Settings
Local Password Policy	
AAA Mode Users	AAA Mode ⑦ ● Local ● RADIUS ● TACACS+ ● SSO ☑ Brable falbadk to Local ONLY on no server response ▼
User Groups	Save
Active Sessions	
TACACS+	
RADIUS Servers	
SSO Servers	

Step 3: In the left column, click TACACS+. In the upper right drop down list, choose Add TACACS+ Server, and then click Go.

uluulu, Cisco Prime	Virtual Domain ROOT-DOMAIN root v	ρ.
cisco Prime cisco Infrastructure	🏠 Home Design 🔻 Deploy 🔻 Operate 🔻 Report 🔻 Administration 🔻	P 3 0-
Users, Roles & AAA		
Change Password	TACACS + Administration > Users, Roles & AAA > TACACS + Servers	Add TACACS+ Server Go
Local Password Policy	None detected	Add TACACS+ Server Delete TACACS+ Server(s)
AAA Mode		
Users		
User Groups		
Active Sessions		
TACACS+		
RADIUS Servers		
SSO Servers		

Step 4: In the Server IP Address box, enter the IP address of the TACACS+ server (Example: 10.4.48.15), and in the Shared Secret and Confirm Shared Secret boxes, enter the secret key (Example: SecretKey), and then click Save.

داده Cisco Prime cisco Infrastructure					Virtual Domain ROOT-DOMAIN roo	ν Dγ	
cisco Infrastructure	🟠 Home De	esign 🔻 Deploy 🔻	Operate 🔻	Report 🔻	Administration 🔻		P 30.
Users, Roles & AAA							
Change Password	Add TACACS + Server Administration > Users, Roles		TACACS+ Serv	er			
Local Password Policy							
AAA Mode	*Server Address	10.4.48.15					
Users	*Port	49					
User Groups	Shared Secret Format	ASCII					
A strange of the strange	*Shared Secret 🕸	•••••					
Active Sessions	*Confirm Shared Secret						
TACACS+	*Retransmit Timeout	5 (secs)					
RADIUS Servers	*Retries	1					
SSO Servers	Authentication Type	PAP 💌					
330 36(16)5	Local Interface IP	10.4.48.35 💌					
	Save Cancel						

Procedure 6

Configure users and user groups

User groups (or *roles*) are collections of privileges that dictate the type of system access the user has. Some predefined roles are:

- System Monitoring—These users can access network status information only. They cannot perform any action on a device or schedule a job on a network.
- Config Managers—Users can perform all system monitoring tasks and tasks related to network data collection. They cannot perform any task that requires write access on the network.
- Admin—Users can monitor and configure operations and perform all system administration tasks.
- Super Users—Users can perform all Cisco Prime Infrastructure operations, including administration and approval tasks.

When using an authentication module other than the Cisco Prime Infrastructure local database, Prime Infrastructure authenticates the user against the external module. After the user is successfully authenticated, Prime Infrastructure assigns the configured role to this user.

Step 1: Navigate to Administration > Users, Roles & AAA> Users.

Step 2: In the Select a command list, choose Add User, and then click Go.

Users, Roles & AAA					
Change Password	Users Admini	S stration > Users, Roles & AAA > Users			Select a command Add User Delete User(s) Lock User(s)
Local Password Policy		User Name	Member Of	Status	Unlock User(s)
AAA Mode		root	Root	Active	
Users					
User Groups					

Step 3: Enter the username and password, under Groups Assigned to this User, select the role for the user, and then click **Save**.

Users, Roles & AAA	
Change Password Local Password Policy	Add User Administration > Users, Roles & AAA > Users > Add User General Virtual Domains
AAA Mode	
Users	Username ExampleAdministrator
User Groups	New Password ② •••••••
Active Sessions	Groups Assigned to this User
TACACS+	🗆 Admin
RADIUS Servers	Config Managers
SSO Servers	🗆 Lobby Ambassador 🦻
SSO Server AAA Mode	\Box Monitor Lite $\sqrt{2}$
	\Box North Bound API $?$
	□ Root 🤅
	☑ Super Users
	System Monitoring
	🗆 User Assistant 🦻
	Save Cancel

For any users who require different permissions than those included in Super Users, create user accounts and assign Cisco Prime Infrastructure user groups to each of the user accounts you create.

Change Password	User Groups Administration > Users, Roles & AAA > Us	er Groups		
Local Password Policy	Group Name	Members	Audit Trail	Export
AAA Mode	Admin		S	Task Li
	Config Managers			Task Li
Users	Lobby Ambassador			Task Li
User Groups	Monitor Lite			Task Li
	North Bound API		<u></u>	Task Li
Active Sessions	Root	root	٩	Task Li
TACACS+	Super Users			Task Li
	System Monitoring		<u>_</u>	Task Li
RADIUS Servers	User Assistant		()	Task Li
SSO Servers	User Defined 1		(s)	Task Li
SOU Servers	User Defined 2		<u></u>	Task L
SSO Server AAA Mode	User Defined 3		<u>.</u>	Task Li
	User Defined 4		6	Task Li

Procedure 7

Add devices and credentials

Before Cisco Prime Infrastructure 1.3 can manage a device, the device must be in the database. You can add devices to the database in three ways:

- Discover the devices by using a discovery protocol
- Add devices manually
- · Import devices in bulk

Cisco Prime Infrastructure supports Layer 2 and Layer 3 protocols for device discovery. Device discovery using Cisco Discovery Protocol is the preferred protocol used by Prime Infrastructure in order to discover network devices in the LAN.

Both Cisco Discovery Protocol and SNMP must be enabled on devices before using this procedure. If you did not deploy your network by using the Cisco SBA Borderless Networks Deployment Guides, which enable both of these protocols, see the Cisco Prime Infrastructure guidance found on the link below. This is found on the Cisco Prime product page within the Cisco the Prime for IT tab. The Cisco Prime product page can be located at www.cisco.com/go/prime.

http://www.cisco.com/en/US/products/ps12239/index.html

This procedure uses a number of Cisco Prime Infrastructure Discovery features including Layer 2 based Cisco Discover Protocol (CDP), SNMP v2 and SSH.

Step 1: Navigate to Operate > Discovery.

Step 2: In the upper right corner, click **Discovery Settings**, and then click **New**. The values that you enter are the default credentials that Prime Infrastructure uses in order to manage the device inventory, configuration, and software.

Oevice Work Center Discovery				🙀 Quick Discovery 👪 Discovery Sett	ngs
	Discovery Settings			×	
Discovery Jobs	🕞 Run Now 🧮 Schedule 🚦	🗞 New 🔓 Copy 💥 Delete 🥖 Edit		😔 🎡 🗸	
	Name	Date Created	Date Modified	All	
Name		No data available		Credentia	

Step 3: In the Name box, enter SBA_Default, expand Layer 2, and then next to CDP Module, click the + icon.

Step 4: In CDP Module, select **Enable Cisco Discovery Protocol**, click **Add Row**, in the **Seed Device** box, enter the cored switch IP address (Example: 10.4.40.49), and then below the Seed Device box, click **Save**.

Tech Tip

If you leave the Hop Count column blank, the discovery process continues until the end neighbor is reached. Depending on the network size, this could be a large number of network devices. In large networks, it is recommend to add a Hop count value to restrict the size of the discovery.

Discovery Settings	×
*Name SBA_Default Current Discov Settings	very
Protocol Settings CDP Module ①	
PingSweep Module	
▼ Layer 2 Protocols	
CDP Module 👄	
Enable Cisco Discovery Protocol Enable Cross Router Boundry	
🖉 Edit 🗙 Delete 👰 Add Row Import CSV File 🔶	
Seed Device Hop Count	
II O 10.4.40.49	
0 10.4.40.53	
Save Cancel	
Son creaentian	
SnmpV3 Credential	
Preferred Management IP	
Use Loopback 👻	
Save Run N	low Cancel

Step 5: Under Credential Settings, next to SnmpV2 Credential, click the **+** icon.

Step 6: Select **Enable SnmpV2 Credential**, click **Add Row**, enter the IP address (Example: *.*.*) and read community string (Example: cisco123), and then below the IP box, click **Save**.

Discovery Settings			×
*Name SBA_Default		Current Discovery Settings	
Protocol Settings		CDP Module	
PingSweep Module	÷	SnmpV2 Credential 🕀	
▼ Layer 2 Protocols			
CDP Module	¢		
LLDP Module	÷		
Advanced Protocols			
Filters			
IP Filter	÷		
Advanced Filters			
Credential Settings			
SnmpV2 Credential	0		_
Enable SnmpV2 Credential			
🖊 Edit 🗙 Delete 👷 Add Row			
IP		Read Community String	
• *.*.*		•••••	
	Save Cancel		

Step 7: Under Credential Settings, next to SSH Credential, click the **+** icon.

Step 8: Select **Enable ssh Credential**, enter the IP address (Example: 0.0.0.0), username, password, and enable password, select **SSHv2**, and then below the User Name box, click **Save**.

Discovery Settings			x		Virt
*Name SBA_Default	Current Disc Settings	covery		Operate 🔻	Report 🔻
Protocol Settings	CDP Module⊕				
PingSweep Module	SnmpV2 Creden	itial 🕀			
▼ Layer 2 Protocols	SSH Credential	\oplus			
CDP Module					
LLDP Module 🔶				_	Discovery Sett
Advanced Protocols				data available	Discovery Set
Filters					
IP Filter 🔶					
Advanced Filters					
Credential Settings					
SnmpV2 Credential				Cotting	-
Telnet Credential				scovery Setting data available	S
SSH Credential					
Enable ssh Credential					
🖉 Edit 🔀 Delete 📄 Add Row					
	User Name	Password	1	Enable Passw	SSH Vers
IP	obdi Hama				

Step 9: On the Discovery Settings dialog box, click **Run Now**. This saves the configuration and begins device discovery.

Discovery Settings	x
*Name SBA_Default	Current Discovery
	Settings
Protocol Settings	CDP Module
PingSweep Module 4	SnmpV2 Credential ⊕
▼ Layer 2 Protocols	SSH Credential
CDP Module	
LLDP Module	
Advanced Protocols	
Filters	
IP Filter 4	>
Advanced Filters	
Credential Settings	
SnmpV2 Credential	è
Telnet Credential 4	>
SSH Credential	>
SnmpV3 Credential	>
Preferred Management IP	
Use Loopback	•
	Save Run Now Cancel

me	 Copy 🗙 Delete 🥖 Date Created		Date Modified	_
A_Default	2012-Nov-17 22:1	4:12	2012-Nov-17 22:25:13	
7				
			Success	

Prime Infrastructure starts discovering the devices on the network. The amount of time this discovery process takes depends on the number of devices on the network.

Step 10: If you want to view the discovery progress, click Operate > Discovery. If you want to instantly update the in-progress results, click the green refresh icon in the upper right corner.

Name								
Name						Show	All	- 5
	Status	Start Time	End Time	Discovery Settings	Reacha	Filtered	Credentia	
Job_Discovery_18_28_0	_0_18 RUNNING	2012-Nov-18 18:2		SBA_Default	22	0	1	
Name	Start Time	End Time	Discovery Sett			Filtered	Credential Errors	
Name				ings Reacha		Filtered D	Credential Errors	
Name Job_Discovery_18_28_0_0_1	8 2012-Nov-18 1	8:2	Discovery Sett				Credential Errors	
Name Job_Discovery_18_28_0_0_1 Reachable Filtered	8 2012-Nov-18 1 Credential Error	8:2	Discovery Sett SBA_Default	22		D	1	
Name Job_Discovery_18_28_0_0_1 Reachable Filtered IP Address	8 2012-Nov-18 1	8:2	Discovery Sett			D	Credential Errors 1 1 New Device	
Name Job_Discovery_18_28_0_0_1 Reachable Filtered JP Address 192.168.18.10	8 2012-Nov-18 1 Credential Error SysObjectId	8:2 rs	Discovery Sett SBA_Default SysName	22 SysLocation		D	1 New Device	0
Job_Discovery_18_28_0_0_1 Reachable Filtered IP Address	8 2012-Nov-18 1 Credential Error	8:2 rs .9.1.907	Discovery Sett SBA_Default	22 SysLocation			1	0

After the process is completed, the status changes from running to completed.

								Show	All		
		Name	Status	Start Time	End Time	Discovery Setti	ings	Reacha	Filtered	Credentia	
•	8	Job_Discovery_18_28_0_0_18_	COMPLETED	2012-Nov-18 18:2	2012-Nov-18 18:4	SBA_Default		38	0	28	
Dise	ove	ry Jobs Instances									
-			Start Time	End Time	Discovery Settings	1	Reachable	Filtered	0	redential Errors	
	Nam										
			2012-Nov-18 18:2				38	0	28		
		_Discovery_18_28_0_0_18	2012-Nov-18 18:2								
	Job_	_Discovery_18_28_0_0_18	2012-Nov-18 18:2	2012-Nov-18 18:4.			38		28		
	Job_	Discovery_18_28_0_0_18 Reachable Filtered	2012-Nov-18 18:2 Credential Errors	2012-Nov-18 18:4.	SBA_Default	2	38		28	8 Device	
	Job_	Discovery_18_28_0_0_18 Reschable Filtered IP Address	2012-Nov-18 18:2 Credential Errors SysObjectId	2012-Nov-18 18:4. Sys 907 WA	SBA_Default	2	38		28 New	8 Device	
	Job_	Discovery_18_28_0_0_18 Reschable Filtered IP Address 10.4.32.162	2012-Nov-18 18:2 Credential Errors SysObjectId .1.3.6.1.4.1.9.1.5	2012-Nov-18 18:4. Sys 907 WP 907 WP	SBA_Default Name AS-7341-2.cisco.local	2	38		28 New false	8 Device	
	Job_	Discovery_18_28_0_0_18 Reschable Filtered IP Address 10.4.32.162 10.4.32.161	2012-Nov-18 18:2 Credential Errors SysObjectId .1.3.6.1.4.1.9.1.9 .1.3.6.1.4.1.9.1.9	2012-Nov-18 18:4 Sys 907 WA 907 WA	SBA_Default Name AS-7341-2.cisco.local AS-7341-1.cisco.local	2	38		28 New false false	8 Device	

Devices on the network have now been discovered and are ready for other management tasks such as asset, configuration, and software-image management.

Process Adding Buildings and Floor Plans to Cisco Prime Infrastructure 1.3 1. Add the first campus and building

2. Place access points on the map

The real advantage of any management system is that it can present information in a way that helps you make intelligent decisions. Cisco Prime Infrastructure 1.3 brings visibility to the radio spectrum, which allows the administrator to see the coverage that is being provided to users. By including the building and floor maps in Cisco Prime Infrastructure 1.3, visibility of this otherwise unknown or convoluted data that Prime Infrastructure 1.3 derives from the wireless network is enabled. You need to have an image of your floor plan before you begin this procedure. The file can be in JPEG, PNG, or GIF format; and it can also be in CAD DXF or DWG format.

Procedure 1

Add the first campus and building

Even though your organization may have only one building today, it may end up with another building; or perhaps each campus is a single building today, but it could have more buildings in the future. The campus, building, floor approach makes it easy to understand and organize as you dig for more information and peel away the layers to find what you are looking for.



Tech Tip

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

Step 1: In Cisco Prime Infrastructure 1.3, navigate to Design > Management Tools > Site Map Design.



Step 2: In the Select a command list, choose New Building, and then click Go.

alualu. Cisco Prime							Artual Domain ROOT-DOMAIN roo	ب ا	D+	
cisco Infrastructure	🟠 Home De	sign 🔹 Deploy	V Operate 🔻	Report •	Administration 🔻				P 61	0.0
Maps									Google 8	Earth Maps
Maps Tree View Maps Tree View Maps Tree Vi	Site Maps <u>Edit View</u> Monitor > Site Maps Show: Type Al	Status All	💽 🗆 Incomplete	GO					Select a command Select a command New Campus New Building .	Go
🍓 System GPS Campus	Name	Туре 🔺	Incomplete	Total APs	a/n Radios	b/g/n Radios	Critical Radio Alarms	Wireless	Delete	б
💩 Unassigned	System Campus	Campus		0	0	0	0	0	Move Buildings	2
	System GPS Campus	Campus		0	0	0	0	0	Copy Maps	2
	Unassigned	Campus		0	0	0	0	0	Properties	2
	Delete								Export Maps Import Maps	
									RF Calibration Models Location Presence Multi-Map Editor	

Step 3: Enter the following information about the building:

- Building Name—Headquarters
- Contact—SBA
- Number of floors—1
- Number of Basements-0
- Horizontal Span (feet)—525
- · Vertical Span (feet)-325
- · Address—560 McCarthy Blvd
- · Latitude and Longitude—As appropriate

Tech Tip

It may be helpful to specify accurate latitude and longitude values for sites that have multiple buildings across a diverse geographic area, such as within a city or in multiple cities. These values can be determined by using Google Maps (http://maps.google.com). Enter the address of the location, right-click the pushpin icon, and then click **What's here?** The coordinates are shown in the search bar.

cisco Prime cisco Infrastructure	🟠 Home	Design 🔻 Deploy 🔻	Operate 🔻	Report 🔻	Administration 🔻
Maps					
Maps Tree View 🗸 🗸	New Building Monitor > Site Maps > System Cam	pus > New Building			
Bystem Campus	Building Name Contact	Headquarters SBA			
Unassigned	Number of Floors Number of Basements	1			
	Dimensions (feet)	Horizontal Span Vertical Span	525 325		
	Address Latitude	560 McCarthy Blvd 37.418717			
	Longitude	-121.919382			

Step 4: Select your newly created building by clicking on its name.

cisco Prime						Vieto	al Domain ROOT-DOMAIN	×πΩ+	
cisco Infrastructure	🟠 Home Design	 Deploy < Opt 	erate 🔻 Report	 Administ 	ration 💌			ł	P 0 0 . 4
1aps									Google Earth Ma
Maps Tree View Maps Tree View Maps Root Area Maps System Campus	Site Maps Fat View Montor > Site Maps Show: Type All St	atus 🗚 💌 🗆	Incomplete Go					Select a comm	and 💌 🛛 Go
🍓 System GPS Campus	Name	Type 🔺	Incomplete	Total APs	a/n Radios	b/g/n Radios	Critical Radio Alarms	Wireless Clients 🕀	Status
💩 Unassigned	System Campus	Campus		0	0	0	0	0	
	System GPS Campus	Campus		0	0	0	0	0	S
	Unassigned	Campus		0	0	0	0	0	~
	System Campus > Headquarters	Building		0	0	0	0	0	
	Delete								

Step 5: In the Select a command list, choose New Floor Area, and then click Go.

uluulu Cisco Prime		Virtual Domain ROOT-DOMAIN
cisco Infrastructure	🏠 Home Design ▼ Deploy ▼ Operate ▼ Report ▼ Administration ▼	
🔹 🍓 Root Area	Building View Monitor > Site Maps > System Compute > Headquarters	GO
Interpretation of the system Campus is system GPS Campus interpretation of the system GPS Campus interpretation of the system	None detected Est Building Debte Building Copy Building	

Step 6: Enter the following information about the floor area:

- Floor Area Name—First Floor
- · Contact—SBA
- Floor—1
- Floor Type (RF Model)—Cubes And Walled Offices
- Floor Height (feet)—10.0
- Convert CAD File to—PNG

cisco Prime cisco Infrastructure	Home Design ▼ Deploy ▼ Operate ▼ Report ▼ Administration ▼
New Floor Area Monitor > Site Maps > System Campus > Headquarters > New Floor Area	
Floor Area Name	First Floor
Contact	SBA
Floor	1
Floor Type (RF Model)	Cubes And Walled Offices 💌
Floor Height (feet)	10.0
Image or CAD File or Qualcomm(R) Map Extraction Tool Output	Choose File No file chosen Convert CAD File to PNG
Next Cancel	Att No file chosen

Step 7: Click **Choose File**, and select the floor plan image filename stored locally on your machine. Once selected, click **Next**.



Step 8: Position the building such that its upper left corner is oriented at the 0/0 feet position on the grid. Some floor plans may have additional whitespace that does not represent the dimensions of your building. Verify proper placement of your new floor area details and image, and then click **OK**.

cisco Infrastructure	▲ Home Design ▼ Deploy ▼ Operate ▼ Report ▼ Administration ▼									
New Floor Area Monitor > Site Maps > System Campus >	Headquarters > New Floor Area First Floor									
Floor Area Name	First Floor									
Contact	SBA									
Floor	1 💌									
Floor Type (RF Model)	Cubes And Walled Offices									
Floor Height (feet)	10.0									
Image File	SJC23-AFP-1.png									
	🗹 Maintain Aspect Ratio									
	Dimensions(feet) Coordinates of top left corner(feet)									
	Horizontal Span 407.7 Horizontal Position 0									
	laub.2									
Total Floor Area Size (sq. feet) :	1248/3.4 Bation (To rescale floor and draw walls)									
QK Cancel										
Lise mouse to position the floor ima	ge by dragging it. And use CTRL key with mouse to resize the floor.									
	0 400 500									

Procedure 2

Place access points on the map

The final piece of the puzzle is to place the access points at the proper locations on your individual floor plans. If you take the time to place your access points where they are actually located, the wireless LAN controllers that work in conjunction with Cisco Prime Infrastructure 1.3 give an accurate view of your network and the devices located in it.

Step 1: Position the floor space so that the zoom and position make it easy to locate the exact position of the access points being added.

Step 2: Select the Add Access Point crosshairs button.

cijuaju Cisco Prime cisco Infrastructure	Winuil Domain RCOT-DOMAIN	rost v Dv
cisco Infrastructure	🏠 Home Design 🖲 Deploy 🔻 Operate 🔻 Report 👻 Administration 👻	P 80.4
Maps Tree View > Floor Settings >	Floor View floors' Jew Key S sylem Carpo > Hedganing > Rint Floor O Dear may be delayed up to 15 minutes or more depending on background poling interval	Select a command Co
Image: Weight access Points > Image: Weight access Points > Image: Weight access Points >	-90 dBm Safrah	112 153
✓ Clients > ✓ 1 802.11 Tags >		AR FLOW
Generation Generation		
Show MSE Currently Detected Save Settings		

Step 3: Select access points that are registered with the system but not yet placed for the headquarters building.

Controller]. Search
Controller]. Search
Controller]. Search
AP # 6 Total AP

Step 4: Carefully place each access point as close to its real position in the building as possible by dragging each one to its proper location, and then click **Save**.



Wait while the system calculates the heat maps from the placement and floor plan area.

Process

Configuring the Wireless Network for Cisco CleanAir

- 1. Create a Cisco CleanAir AP template
- 2. Apply the Cisco CleanAir AP template
- 3. Create a controller EDRRM template
- 4. Create a Cisco CleanAir controller template

A Cisco wireless LAN controller with connected Cisco Aironet 2600 or 3600 Series access points is immediately Cisco CleanAir-capable. The wireless LAN controllers can give you immediate information about your environment. Where Cisco Prime Infrastructure 1.3 can present a complete network view, the wireless LAN controller displays only data retrieved from the locally connected CleanAir access points.

Cisco Prime Infrastructure 1.3 can handle all management tasks within the network. You can still perform management tasks at each individual controller, but that approach it is not recommended, as it often results in a fragmented configuration. With the Cisco CleanAir access point operating from the wireless LAN controller, you can log in to Cisco Prime Infrastructure 1.3 and configure your controller to support CleanAir.

Procedure 1

Create a Cisco CleanAir AP template

The first step in order to turn on Cisco CleanAir is to ensure that Cisco CleanAir is enabled on each of the access points (APs) for both 2.4 and 5 GHz bands. The following steps outline how to create a template within Cisco Prime Infrastructure 1.3 to enable CleanAir on an AP.

Step 1: In Cisco Prime Infrastructure 1.3, navigate to Design > Configuration > Wireless Configuration > Lightweight AP Configuration Templates.

cisco Infrastructure	🟠 Home	Design 🔻 Deploy 🔻 🔿	Operate 🔻 🛛 Rep	port 🔻 Administration 💌
ightweight AP Templates onføære > Lightweight AP Templates Ione detected		Management Tools	Lightweight AP Co Autonomous AP Co Switch Location Co Autonomous AP M Controller Configur WIPS Profiles n	onfiguration Templates onfiguration Templates ligration Templates

Step 2: In the Select a command list, choose Add Template, and then click Go.



Step 3: In the Template Name box, enter a name, in the Description box, enter a description, and then click Save.

داند المعالم Cisco Prime دادده Infrastructure				Virtual Domain ROOT-DOMAIN root 🔻	Ø + templates						
cisco Infrastructure	🟠 Home	Design 🔻	Deploy 🔻	Operate 🔻	Report 🔻	Administration 🔻	P G Ø.				
New Lightweight AP Template											
*Template Name	Air Enable										
Description Ena	le CleanAir Support										
Save Cancel											

Step 4: On the 802.11a/n tab, ensure that both **CleanAir** and **Enable** are selected.

	uluulu, Cisco Prime								Virt	tual E	omain ROOT-D	OMAIN roo	•	ρ ,		
	cisco Infrastructure			🏠 Home	Design	 Deploy 	 Opera 	te 🔻	Report 🔻	,	Administratio	n 🔻				P 80.
Ľ	ightweight AP Template	Detail :	'CleanAi	ir Enable'												
	AP Parameters Mesh	802.1	1a/n	802.11a S	ubBand	802.11b/g/r	n CDP	FI	exConnect	Υ	Select APs	Apply/Sch	edule	*Report		
	Select 802.11a Parame	ters tha	t needs t	o be appli	ied.											
	🔲 Channel Assignment	O Cust	im 🗶			Power Assign	iment	🔿 Cus	tom 🗶						ĺ –	
		Glob	al					🖲 Glol	al						i i	
	🔲 Admin Status 🧕	🗹 Enab	е			WLAN Overri	de <u>3</u>	Disab	e		v				1	
	🔲 Antenna Mode	Sector	A	•		Antenna Sele	action Z								i i	
	🔲 Antenna Diversity	Left/Sid	le B	•											ĺ –	
	🔲 Antenna Type	Interna		•											ĺ –	
	Antenna Name 🔒			•					_						ĺ –	
					1	CleanAir <u>6</u>	[🗹 Ena	ole						i i	
									_							

Step 5: On the 802.11b/g/n tab, ensure that both **CleanAir** and **Enable** are selected.

uluulu Cisco Prime		Virtual Domain ROOT-DOMAIN root v 🔎 🗸	
cisco Infrastructure	🟠 Home E	esign 🔻 Deploy 🔻 Operate 🔻 Report 🗶 Administration 🔻	P 80.
Lightweight AP Templat	e Detail : 'CleanAir Enable'		
AP Parameters Mesh	802.11a/n 802.11a SubB	and 802.11b/g/n CDP FlexConnect Select APs Apply/Schedule *Report	
Select 802.11b Parame	eters that needs to be applied.		
🗐 Channel Assignment	O Custom 1	Power Assignment O Custom <u>1</u> O Custom <u>1</u> O	
🔲 Admin Status 🙍		Global WLAN Override 2 Disable	
Antenna Mode	Sector A	Tracking Optimized Monitor Mode	
Antenna Diversity Antenna Type	Left/Side B 🔻		
Antenna Name 🚊	AIR-ANT1000		
		Antenna Selection 8	
		-	
		🗹 CleanAir д 🗹 Enable	

Step 6: On the Apply/Schedule tab, click Save.

allada Cisco Prime				irtual Domain ROOT-DOMAIN root 🔻	ρ.
cisco Infrastructure	▲ Home Design ▼ Deploy ▼	Operate 🔻 Report 🔻	Administration 🔻		P 3 0.
Lightweight AP Template Detail : 'Cle	anAir Enable'				
AP Parameters Mesh 802.11a/n	802.11a SubBand 802.11b/g/n	CDP FlexConnect	Select APs Apply/Schedu	e *Report	
Save Click 'Save' to save the	template.				
Apply Click 'Apply' to save the	e template and start the provisioning ntil completed even if you leave this	of the template to select	ed APs.This		
Cancel Click 'Cancel' to cancel	the template in progress				
Schedule 🔤 Enable schedu	le				
Start Date AP template sa	ved successfully				
			ок		
Start Time					
Recurrence No Recurrence	O Hourly O Daily O Weekly				
alist to be detailed as seen					
Schedule Click 'Schedule' to save	the template and start the provision	ing at a scheduled time.			

Procedure 2

Step 1: Navigate to Design > Configuration > Wireless Configuration > Lightweight AP Configuration Templates.

cisco Infrastructure	🟠 Home	Design 🔻 Deploy 🔻 Operate 💌	Report v Administration v
Lightweight AP Templates Configure > Lightweight AP Templates Vone detected		Autonated Deployn Management Tools Port Grouping	Mobility Services Mobility Services Engines Synchronize Services Synchronization History High Availability Configuration Templates In Configuration Templates In Configuration Templates In Gundguration Templates Iguration Groups

Step 2: From the list of defined templates, choose the template that you created in Step 3 of the previous procedure (Example: CleanAir Enable).

Step 3: On the Select APs tab, in the Search APs list, choose All, and then click Search. By default, all APs are selected.

If you want to enable only certain APs, click **Unselect All**, and then individually select the APs you want to enable.

alualu, Cisco Prime				Virtual Domain ROOT-DOMAIN root 👻 💭 🛩	
cisco Infrastructure	🟠 Home	Design 🔻 Deploy 🔻	Operate 🔻 Report 🔻	Administration 🔻	P 30.
Lightweight AP Template D	etail : 'CleanAir Enable'				
AP Parameters Mesh	802.11a/n 802.11a Sub	Band 802.11b/g/n	CDP FlexConnect	Select APs Apply/Schedule *Report	
Search APs				Select All Unselect All	
All	AP Name	Ethernet MAC	Controller	Map	
Search	APd0d0.fd45.4ae1	d0:d0:fd:45:4a:e1	10.4.46.64	A	
Search	RS201-LAP1142N	f8:66:f2:44:55:87	10.4.46.68		
	APe8b7.4899.c82b	e8:b7:48:99:c8:2b	10.4.46.64		
	AP442b.039a.9c3a	44:2b:03:9a:9c:3a	10.4.46.64		
	APf0f7.55df.ac77	f0:f7:55:df:ac:77	10.4.46.64		

Step 4: On the Apply/Schedule tab, click **Apply**. The CleanAir Enable template is applied to the selected APs.

albala Cisco Prime Vebulloman ROOT-DOMARE + root + Dr-	
	.00.
ightweight AP Template Detail : 'CleanAir Enable'	
AP Parameters Mesh 802.11a/n 802.11a SubBand 802.11b/g/n CDP FlexConnect Select APs Apply/Schedule *Report	
Save Click 'Save' to save the template.	
Apply Click 'Apply' to save the template and start the provisioning of the template to selected APs.This process will continue until completed even if you leave this page and logout from WCS.	
Cancel Click 'Cancel' to cancel the template in progress	
Schedule 🔲 Enable schedule	
Start Date	
(Current server time: 11/09/2012 08:02:19)	
Start Time 00 W Hr 00 W Min	
Recurrence O No Recurrence O Hourly O Daily O Weekly	

Step 5: On the Report tab, verify that the Template was successfully applied.

Juliulu, Cisco Prime			Virtual Domain ROOT-DOMAIN root	• (D•
cisco Infrastructure	🟦 Home 🛛 Design 🔻 Des	oloy 🔻 Operate 🔻 Report '	 Administration 	P 30.
Lightweight AP Template Detail	: 'CleanAir Enable'			
AP Parameters Mesh 802.	11a/n 802.11a SubBand 802.11	b/g/n CDP FlexConnect	Select APs Apply/Schedule	*Report
Apply Status: Completed				
Applied On: 11/9/12 9:14 AM				
AP Name	Status	Ethernet MAC	Controller Ma	2
AP442b.039a.9c3a Succe	ess	44:2b:03:9a:9c:3a 10.4.4	46.64	<u>A</u>

If the CleanAir Enable template is not successfully applied, ensure that:

- 1. In Cisco Prime Infrastructure 1.3, the SNMP Read/Write Community string for the WLC is correct.
- In Cisco Prime Infrastructure 1.3, under Operate> Device Work Center > Device Type > Wireless Controller, the WLC Audit Status is Identical and not Mismatched.

Procedure 3

Create a controller EDRRM template

Event-driven radio resource management (EDRRM) is a feature that allows an access point that is in distress to bypass normal RRM intervals and immediately change channels. A Cisco CleanAir access point always monitors Air Quality (AQ) and reports on AQ in 15-second intervals. AQ is a better metric than normal Wi-Fi chip noise measurements because AQ only reports on classified interference devices. That makes AQ a reliable metric in that you know that what is reported is not caused by Wi-Fi energy (and hence is not a transient, normal spike). The key benefit of EDRRM is very fast action time (30 seconds). If an interferer is operating on an active channel and is causing enough AQ degradation that it triggers EDRRM, clients cannot 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. You must enable it in two steps: enable Cisco CleanAir and then enable EDRRM.

In this procedure, you create a template that is used to enable EDRRM for both the 2.4 and 5Ghz bands.

Step 1: In Cisco Prime Infrastructure 1.3, navigate to Design > Configuration Templates > Controller, and then in the tree, navigate to 802.11a or n > dot11a-RRM > DCA.

Step 2: Without using illegal characters such as "/" or ".", provide a meaningful name for the template. In the **Assignment Mode** list, choose **Automatic**, for Event Drive RRM, select **Enable**, and then in the **Sensitivity Threshold** list, choose **Medium**.

Feature Design Monitor Configurati	on Configuration Groups Shared Policy Objects
Templates	
٩	
(= + E + % +	Peatures and Technologies > Controller > 802.11a or n > dot11a-RRM
	reactes and real-modules > construer > eaching and reacted and reacted by the second sec
Features and Technologies	
 Interfaces 	▼ Template Basic
🔻 🚞 Controller	*Name Enable 802 an EDRRM Author root
System	Description Enable 802 an EDRRM Feature Category DCA
 Security WLANS 	
 Munar FlexConnect 	Tagi
► B02.11	
▼ = 802.11a or n	▼ Validation Criteria
▼	*Device Type CUWN (default) OS Version
Thresholds	
Thtervals	▼ Template Detail
TPC	General
E DCA	Dynamic Channel Assignment Algorithm
Parameters	Asignment Mode Automatic
🖹 CleanAir 🖉	Avoid Foreign AP Interference
Media Parameters	
EDCA Parameters	Avoid Cisco AP load Enable
Roaming Parameters	Avoid non 802.11 Noise 🔲 Enable
🖹 802.11h	Avoid Persistent Non-WiFi Interference 🔲 Enable
High Throughput (802.11	Signal Strength Contribution 🗹 Enable
 B02.11b or g or n 	Channel Width 20 MHz 💌
Mash	Event Driven RRM
Management	Event Driven RRM 📝 Enable
• 😑 ar	Sensitivity Threshold Medum
Location	
▶ □ JPv6	
PMIP	
 mONS Application Visibility And Cor 	
Appleation Visibility And Lor Netflow	Footnotes:
 memow Security 	1. Event Driven RRM fields are supported for controller version 7.0.x.x onwards.
 Security WAN Optimization 	
Application Visibility	
Aleback Analysis Mackde	Save as New Template
< III +	

Step 3: Click **Save as New Template**, and then, on the Save Template dialog box, click **Save**. This saves the template in the My Templates folder.

Save Template			×
*Folder	My Templates	٢	
		Save	ancel

Step 4: After saving the new template into the My Templates folder, at the bottom of the screen, click **Deploy**, select each of the wireless LAN controllers to apply the template to, and then click **OK**.

	Name	Description	Type	IP Address	Vendor	
	ALL	All Members				A
]	WLC-OEAP-2	WLC-OEAP-2	Wireless Controller	192.168.19.21	Cisco	
	DMZ-WLC-Guest	DMZ-WLC-Guest	Wireless Controller	192.168.19.54	Cisco	
	WLC-OEAP-1	WLC-OEAP-1	Wireless Controller	192.168.19.20	Cisco	
2	WLC-RemoteSites-1	WLC-RemoteSites-1	Wireless Controller	10.4.46.68	Cisco	
	WLC-1-Primary	WLC-1-Primary	Wireless Controller	10.4.46.64	Cisco	
	RS208-WLC2504	RS208-WLC2504	Wireless Controller	10.5.87.10	Cisco	
	vWLC-7_4_1_42	vWLC-7_4_1_42	Wireless Controller	10.5.24.64	Cisco	
] ▶	Device Type	Device Type				T
Sche	e Assignment dule					
Sche	dule ne]ob_Config_Deploy_8_13	3_35_215_AM_11_15_2012 11/15[2012 08:13 AM 📄 (M4M/dd/yyy	y Fh:mm AM(PM)			

Step 5: Repeat Step 2 through Step 4 for 802.11b/g/n.

Procedure 4

Create a Cisco CleanAir controller template

The next step is to configure the controller for Cisco CleanAir, and then for each band, you identify which types of interferers are important to report and alarm on.

Step 1: In Cisco Prime Infrastructure 1.3, navigate to Design > Configuration Templates > Controller > 802.11a or n > CleanAir.

Step 2: On the CleanAir template, do the following:

- Provide a meaningful name and description (Example: CleanAir 11a or n).
- · Next to CleanAir, select Enable.
- Next to Report Interferers, select **Enable**. The interferers selection box for reporting appears.
- Move the following interferer types to the Interferers Selected for Reporting box: Continuous Transmitter, DECT-Like Phone, Jammer, Video Camera.
- Next to Interferers For Security Alarm, select **Enable**. The interferers selection box for security alarms appears.
- Move the following interferer types to the Interferers Selected for Security Alarms box: Continuous Transmitter, DECT-Like Phone, Jammer, Video Camera.

cisco Prime cisco Infrastructure	Home Design Depky Operate Report Administration
Feature Design Monitor Configurati	on Configuration Groups Shared Policy Objects
Templates	Features and Technologies > Controller > 802.11a or n CleanAlr
 FlexConnect B02.11 B02.13 or n 	Validation Criteria *Device Type (CUMN (default)) OS Version
Add Sector	• Tenglate Detail Canado @ Endo Percent ing Configuration Interference Solucitad for Reporting Separation for Solucitad Formation Interference Solucitad for Reporting View Invested View Invested View Invested View Invested View Invested View Invested View Invested View Invested View Invested Invested
۰ III ا	Save as New Template Cancel

Step 3: Click Save as New Template, on the Save Template dialog box, choose My Templates, and then click Save.

Save Template			×
*Folder	My Templates	0	
		Save	ancel

Step 4: After saving, at the bottom of the screen, click **Deploy**, select each of the wireless LAN controllers to apply the template to, and then click **OK**.

	Name	Description	Type	IP Address	Vendor	
	▼ ALL	All Members				
)	WLC-OEAP-2	WLC-OEAP-2	Wireless Controller	192.168.19.21	Cisco	
]	DMZ-WILC-Guest	DMZ-WLC-Guest	Wireless Controller	192.168.19.54	Cisco	
]	WLC-OEAP-1	WLC-OEAP-1	Wireless Controller	192.168.19.20	Cisco	
1	WLC-RemoteSites-1	WLC-RemoteSites-1	Wireless Controller	10.4.46.68	Cisco	
•	WLC-1-Primary	WLC-1-Primary	Wireless Controller	10.4.46.64	Cisco	
]	RS208-WLC2504	RS208-WLC2504	Wireless Controller	10.5.87.10	Cisco	
•	vWLC-7_4_1_42	vWLC-7_4_1_42	Wireless Controller	10.5.24.64	Cisco	
))	 Device Type 	Device Type				v
	ue Assignment					
Sch ib N	edule arreConfig_Deploy_8_1	3_35_215_AM_11_15_2012 11/152012 08:13 AM 💼 (44M/dd/yyy	y hh:mm AM/PM)			

Step 5: In Cisco Prime Infrastructure 1.3, navigate to Design > Feature Design > Controller > 802.11b or g or n > CleanAir.

Step 6: On the CleanAir template, do the following:

- Provide a meaningful name (Example: CleanAir 11b or g or n).
- Provide a meaningful description (Example: CleanAir 11b or g or n).
- Next to CleanAir, select Enable.
- Next to Report Interferers, select **Enable**. The interferers selection box for reporting appears.
- Move the following interferer types to the Interferers Selected for Reporting box: Bluetooth Discover, Bluetooth Link, Continuous Transmitter, DECT-Like Phone, Jammer, Microwave Oven, Video Camera, Xbox.
- Next to Interferers For Security Alarm, select **Enable**. The interferers selection box for security alarms appears.
- Move the following interferer types to the Interferers Selected for Security Alarms box: Bluetooth Discover, Bluetooth Link, Continuous Transmitter, DECT-Like Phone, Jammer, Microwave Oven, Video Camera, Xbox.

cisco Prime	Home Design Deploy Operate Report Administration
Feature Design Monitor Configurat	ion Configuration Groups Shared Policy Objects
Templates	Features and Technologies > Controller > 802.11b or g or n CleanAir
	Template Basic Name Gennér 11b or g or n Description Gennér 11b or g or n Feature Category CleanAir Tags
WLANS MECOnnect On 2 X	Validation Criteria *Devce Type (CUWN (default) Of Verson
 B22.11 B22.11 or g or B22.11 b or g or B22.11 b or g or C22.11 b or g or CAGA or anneters CAGA or anneters CAN anneters CAN	Template Detail Detail
Security Generation MARU Optimization Application Heading Application Heading CLI Translate My Tags Composite Templates	802.13-4 Buttooth Discovery 802.15-4 Carooy Carooy Carooy TOD Traventter Caronow With Invald Charnel 2 WMAX. Fixed Microwate Oven VMAX. Rubbe Viola Carena Save at New Template Caronal

Step 7: Click Save as New Template, on the Save Template dialog box, choose My Templates, and then click Save.

Save Template			×
*Folder	My Templates	٢	
		Save	ancel

Step 8: After saving, at the bottom of the screen, click **Deploy**, select each of the wireless LAN controllers to apply the template to, and then click **OK**.

Process Installing the Cisco Mobility Services Engine Virtual Appliance

- 1. Install the Cisco MSE virtual appliance
- 2. Start the Cisco MSE virtual appliance
- 3. Configure the Cisco MSE virtual appliance
- 4. Verify installation of MSE virtual appliance

The Cisco MSE VA is deployed within a VMware environment hosted within the data center or server room. This document assumes that a fully functional VMware environment has been deployed and is operational.

Although capable of much more, the use of the Cisco MSE VA in this deployment guide is to provide historical Cisco CleanAir reporting. Through the use of the MSE, historical information regarding the location and types of interferers is visible through Cisco Prime Infrastructure 1.3. **Procedure 1**

Install the Cisco MSE virtual appliance

Step 1: Using the VMware vSphere client, click File, and then choose Deploy OVF Template.

New +	entory 🕨 🎁 Hosts and Clusters	
Deploy OVF Template Export Report	chas1-s1.cisco.local VMware ESXi, 5.0.0, 768111 Evaluation (42 days	r remaining)
Browse VA Marketplace Print Maps		ormance Configuration Tasks & Events Alarms Permissions Maps Storage Views Hardware Status Update Mana close tab
E 00 11 0486-911.0500.00.03 21 FS200 Data Center	What is a Host? A host is a computer that uses virtualization software, such as EGX or ESO, to run virtual machines hosts provide the CPU and memory resources that virtual machines use and give withual machines access to storage and network connectivity. Basic Tasks Boploy from VA Marketplace If Create a new virtual machine If Create a new virtual machine	Urtual Machines Cluster Under Granter Server Ucarter Server
		Explore Further Learn more about hosts Learn how to create virtual machines Enhance your datacenter Learn about signifiere Widdon, FA, DRS, and more

Step 2: In the Deploy OVF Template wizard, on the Source page, browse to the location of the Cisco MSE Open Virtual Appliance (OVA) file, and then click **Next**.

Step 3: On the OVF Template Details page, review the OVF template details, and then click **Next**.

Step 4: On the Name and Location page, enter a unique and descriptive name for the virtual appliance that you are installing (Example: vMSE-VA-7-4-0-31), choose a location to install the virtual appliance, and then click **Next**.

Step 5: On the Host /Cluster page, choose the host or cluster on which to install this virtual machine, and then click **Next**.

Step 6: On the Storage page, choose where you want to store the virtual machine files, and then click **Next**.

Step 7: On the Disk Format page, select **Thick Provision Lazy Zeroed**, and then click **Next**.

Step 8: On the Network Mapping page, in the Destination Networks column, choose the appropriate network mapping group previously defined to the VMware environment (Example: Servers_1), and then click **Next**.

🚱 Deploy OVF Template			_ 🗆 ×
Network Mapping			
What networks should t	he deployed template use?		
r	_		
<u>Source</u> OVF Template Details	Map the networks used in this OVF	template to networks in your inventory	
Name and Location			
Host / Cluster	Source Networks	Destination Networks	
<u>Storage</u> Disk Format	Default	Servers_1	-
Network Mapping			
Ready to Complete		Ν	
		13	
	Description:		
	Default Network		<u> </u>
			-
Help		< Back Next > C	ancel

Step 9: On the **Ready to Complete** page, review the selected options, and then click **Finish**. The OVF installation begins.

Deploy O¥F Template		_ 🗆
Ready to Complete		
Are these the options y	ou want to use?	
	_	
Source	When you click Finish, the deploy	mont task will be started
OVF Template Details Name and Location		nienciask will be started.
Storage	Deployment settings: OVF file:	C:\Downloads\MSE-VA-7-4-0-31-Generic.ova
Disk Format	Download size:	
Network Mapping	Size on disk:	488.3 GB
Ready to Complete		488.3 GB
	Name:	Cisco Mobility Services Engine Virtual Appliance
	Folder:	10k
	Host/Cluster:	chas1-s1.cisco.local
	Datastore:	chas1-s1-local
	Disk provisioning:	Thick Provision Lazy Zeroed
	Network Mapping:	"Default" to "Servers_1"
	1	
	Power on after deployment	
Help		a Daula I Thata Council
holp		< Back Finish Cancel

Procedure 2

Start the Cisco MSE virtual appliance

Next, install the Cisco MSE software on the new virtual machine.

Step 1: In the VMware vSphere client, select the virtual machine just installed (Example: vMSE-7-4-0-31), and then select **Power on the virtual machine**.

Step 2: On the Console tab, after you receive the "Cisco Mobility Services Engine" banner, press **Enter**. The "ImportError: No module named gamin" error appears.

Step 3: At the **mse login** prompt, enter the default username and password: **root/password**. The installation begins and can take up to 45 minutes to complete, depending on the performance of the VM host machine.



Tech Tip

The installation process can take 45-60 minutes or more to complete. At times during the automated installation process, there may be times where no indication of progress is displayed. Your installation time may vary depending on CPU resources available.

Procedure 3

Configure the Cisco MSE virtual appliance

Step 1: After the virtual machine restarts, in VMware vSphere, navigate to the Console tab.

Step 2: At the mse login prompt, enter root for the user ID and password for the password and press <Enter>. The Setup Wizard will ask you if it should be stared, enter YES and press Enter.

Setup parameters via Setup Wizard (yes/no) [yes]: YES

Step 3: Type **Y** for Yes, and then enter the host name of the Cisco MSE virtual appliance.

Current hostname=[mse] Configure hostname? (Y)es/(S)kip/(U)se default [Yes]: Enter a host name [mse]: **vMSE-VA-7-4-0-31**

Step 4: Type **Y** for Yes, and then configure the domain name. (Example: cisco.local)

Current domain=[] Configure domain name? (Y)es/(S)kip/(U)se default [Yes]:<ENTER>

Enter a domain name for the network domain to which this device belongs. It must contain only letters, digits, hyphens [LDH rule] and dots. It cannot begin and end with a hyphen.

Enter a domain name : cisco.local

Step 5: Type S for Skip. This skips the high availability configuration.

Current role=[Primary] Configure High Availability? (Y)es/(S)kip/(U)se default [Yes]: Skip <ENTER>

Step 6: Type Y for Yes, and then configure the ethO interface parameters. Current IP address=[1.1.1.10] Current ethO netmask=[255.255.255.0] Current gateway address=[1.1.1.1] Configure ethO interface parameters? (Y)es/(S)kip/(U)se default [Yes]: Yes Enter an IP address for first ethernet interface of this machine. Enter ethO IP address [1.1.1.10] : 10.4.48.40 Enter the network mask for IP address 10.4.48.40. Enter network mask [255.255.255.0]: 255.255.0 Enter a default gateway address for this machine. Note that the default gateway must be reachable from the first ethernet interface. Enter the default gateway address [1.1.1.1]: 10.4.48.1 **Step 7:** Type **S** for Skip. This skips the configuration of a second Ethernet interface.

The second ethernet interface is currently disabled for this machine.

Configure eth1 interface parameters? (Y)es/(S)kip/(U)se default [Yes]: Skip <ENTER>

Step 8: Type Y for Yes, and then configure the DNS (Example: 10.4.48.10).
Domain Name Service (DNS) Setup
DNS is currently enabled.
No DNS servers currently defined
Configure DNS related parameters? (Y)es/(S)kip/(U)se default
[Yes]: Yes
Enable DNS (yes/no) [yes]: Yes
Enter primary DNS server IP address: 10.4.48.10
Enter backup DNS server IP address (or none) [none] : <ENTER>

Step 9: Configure the current time zone (Example: America/Los Angeles).

Current timezone=[America/New_York] Configure timezone? (Y)es/(S)kip/(U)se default [Yes]: Yes

<ENTER>

Please identify a location so that time zone rules can be set correctly.

Please select a continent or ocean.

- 1) Africa
- 2) Americas
- 3) Antarctica
- 4) Arctic Ocean
- 5) Asia
- 6) Atlantic Ocean
- 7) Australia
- 8) Europe
- 9) Indian Ocean
- 10) Pacific Ocean
- 11) UTC I want to use Coordinated Universal Time.
- 12) Return to previous setup step (^).
- #? **2 <ENTER>**

- 3) Argentina 29) Martinique 30) Mexico 31) Montserrat 32) Netherlands Antilles 33) Nicaraqua 34) Panama 35) Paraguay 36) Peru 37) Puerto Rico 38) St Barthelemy 39) St Kitts & Nevis 40) St Lucia 41) St Martin (French part) 42) St Pierre & Miguelon 43) St Vincent 44) Suriname 45) Trinidad and Tobago 46) Turks & Caicos Is 47) United States 48) Uruquay 49) Venezuela 50) Virgin Islands (UK)
- 26) Haiti
- #? 47 <ENTER>

Select your time zone from the country specific time zone menu.

51) Virgin Islands (US)

<SNIP>

20) Mountain Standard Time - Arizona

21) Pacific Time

22) Alaska Time

#? 21 <ENTER>

The following information has been given: United States Pacific Time

Therefore TZ='America/Los Angeles' will be used. Local time is now: Fri Oct 5 07:54:52 PDT 2012. Universal Time is now: Fri Oct. 5 14:54:52 UTC 2012. Is the above information OK?

#? 1 **<ENTER>**

Step 10: Choose the default option as to when Cisco MSE automatically restarts.

Enter whether you would like to specify the day and time when you want the MSE to be restarted. If you don't specify anything, then Saturday 1 AM will be taken as the default. Configure future restart day and time ? (Y)es/(S)kip [Skip]: <ENTER>

Step 11: Specify the remote syslog server used to publish the Cisco MSE logs (Example: 10.4.48.15).

Tech Tip

Selecting a priority level of 2 generates both warning and information-level messages. The facility value is a way of determining which process created the message. LOCAL0 through LOCAL7 are typically used for networking equipment.

1) Yes 2) No

- 4) Aruba
- 5) Bahamas
- 6) Barbados
- 7) Belize
- 8) Bolivia
- 9) Brazil
- 10 Canada
- 11) Cayman Islands
- 12) Chile
- 13) Colombia
- 14) Costa Rica
- 15) Cuba
- 16) Dominica
- 17) Dominican Republic
- 18) Ecuador
- 19) El Salvador
- 20) French Guiana
- 21) Greenland
- 22) Grenada
- 23) Guadeloupe
- 24) Guatemala
- 25) Guyana

Configure Remote Syslog Server to publish/MSE logs MSE logs. A Remote Syslog Server has not been configured for this machine. Configure Remote Syslog Server Configuration parameters? (Y) es/(S)kip/(U)se default [Yes]: Yes Configure Remote Syslog Server IP address : 10.4.48.15 Configure Remote Syslog Server Priority parameter. select a priority level 1) ERROR (ERR) 2) WARNING 3) INFO Enter a priority level (1-3) : 2 <ENTER> Configure Remote Syslog Server's Facility parameter. Select a logging facility 0) LOCALO (16) 1) LOCAL1 (17) 2) LOCAL2 (18) 3) LOCAL3 (19) 4) LOCAL4 (20) 5) LOCAL5 (21) 6) LOCAL6 (22) 7) LOCAL7 (23) Enter a facility(0-7) :4 <ENTER> Step 12: Type S for Skip. This skips the next step, which is used for modify-

Step 12: Type S for Skip. This skips the next step, which is used for modifying the iptables for Cisco MSE.

Enter whether or not you would like to change the iptables for this machine (giving access to certain host).

Configure Host access control settings ?(Y)es/(S)kip [Skip]:
<ENTER>

Step 13: Configure Network Time Protocol (NTP), as shown below. Network Time Protocol (NTP) Setup. If you choose to enable NTP, the system time will be configured from NTP servers that you select. Otherwise, you will be prompted to enter the current date and time. NTP is currently disabled. Configure NTP related parameters? (Y)es/(S)kip/(U)se default [Yes] Yes Enter whether or not you would like to set up the Network Time Protocol (NTP) for this machine. If you choose to enable NTP, the system time will be configured from NTP servers that you select. Otherwise, you will be prompted to enter the correct date and time. Enable NTP (yes/no) [no]: Yes Enter NTP server name or address: 10.4.48.17 Enter another NTP server IP address (or none) [none]: <ENTER> Configure NTP Authentication ? (Y)es/(S)kip/(U)se default [Yes]: Skip

Step 14: Type **S** for Skip. This skips the configuration of the Cisco MSE audit rules, login banner, and console access.

Audit rules Setup.

Configure audit rules and enable Audit daemon? (Y)es/(S)kip/ $% \left(X\right) =\left(X\right) \left(X\right)$

(U) se default [Yes]: Skip <ENTER>

Current Login Banner = [Cisco Mobility Service Engine]
Configure login banner (Y)es/(S)kip/(U)se default [yes]: Skip
<ENTER>

System console is not restricted. Configure system console restrictions (Y)es/(S)kip(U)se default value [Yes] : **Skip <ENTER>**

Step 15: Type Yes. This enables SSH root access.

SSH root access is currently enabled.

Configure ssh access for root (Y)es/(S)kip(U)se default [Yes]:

<ENTER>

Enter whether or not you would like to enable ssh root login. If you disable this option, only console root login will be possible.

Enable ssh root access (yes/no): Yes <ENTER>

Single user mode password check is currently disabled.

Configure single user mode password check (Y)es/(S)kip/(U)se

default [Yes]: Skip <ENTER>

Configure root password (Y)es/(S)kip/(U)se default [Yes]:

<ENTER>

You can now choose the new password.

A valid password should be a mix of upper and lower case letters,

digits, and other characters. You can use a 14 character long password with characters from all of these classes. An upper case letter that begins the password and a digit that ends it do

not count towards the number of character classes used. Enter new password: Hgt50N3181.5n2B <ENTER>

Tech Tip

Cisco MSE requires the use of strong passwords, which must be a minimum of 14 characters long with rigid requirements on the use of various character classes. Choose a strong password and document it according to your internal InfoSec policies. **Step 16:** Accept the default log-in parameters and GRand Unified Bootloader (GRUB) settings.

Login and password strength related parameter setup Maximum number of days a password may be used : 999999 Minimum number of days allowed between password changes : 0 Minimum acceptable password length : disabled Login delay after failed login : 5 Checking for strong passwords is currently enabled Configure login/password related parameters? (Y)es/(S)kip/(U) se default [Yes]: Skip <ENTER> GRUB password is not currently configured. Configure GRUB password (Y)es/(S)kip/(U)se default [Yes]: Skip <ENTER>

Tech Tip

GRUB is used to password-protect the boot loader in Linux systems. If you specify a GRUB password, each time the virtual appliance is booted up, the GRUB password must be entered. If the password is lost or forgotten, the virtual appliance cannot be booted up. Configuring a GRUB password should be done with consideration and documented accordingly in your organization's operations manual.
Step 17: Configure the Cisco Prime Network Control System (NCS) communications username by selecting Yes to configure it.

Configure NCS communications username? (Y)es/(S)kip/(U)se default [Yes]: Yes <ENTER> Enter an admin username. This user is used by the NCS and other northbound systems to authenticate their SOAP/XML session with the server. Enter a username : vMSEuser Configure NCS communication password? (Y)es/(S)kip/(U)se default [Yes]: Yes <ENTER> Enter a password for the admin user. The admin user is used by the NCS and other northbound systems to authenticate their SOAP/XML session with the server. Once the password is updates, it must correspondingly be updated on the NCS page for MSE General Parameters so that the NCS can communicate with the MSE. Enter NCS communication password: Clsc0!349@ Confirm NCS communication password : Clsc0!349@

Step 18: Confirm and approve the settings obtained through the Setup Wizard.

----BEGIN-----Host name=vMSE-VA-7-4-0-31 Domain=cisco.local Eth0 IP address=10.4.48.40, Eth0 network mask=255.255.255.0 Default gateway=10.4.48.1 Enable DNS=yes, DNS servers=10.4.48.10 Time zone=America/Los Angeles Enable NTP=yes, NTP Servers=10.4.48.17 Enable SSH root access=yes Root password is changed. NCS username is changed. NCS password is changed. Remote Systemlog Server IPAddress=10.4.48.15, Remote Syslog Server Facility=Local0 Remote Syslog Server Priority=WARNING -----END-----

You may enter "yes" to proceed with configuration, "no" to make more changes, or "^" to go back to the previous setup. Configuration Changed

Is the above information correct (yes, no, or ^): Yes <ENTER>

Procedure 4

• Verify installation of MSE virtual appliance

Manually restart the Cisco MSE server and using the following steps, confirm that the MSE processes have indeed started.

Step 1: In VMware vSphere, shutdown and restart the Cisco MSE VA host.

Step 2: On the Console tab, log in to the Cisco MSE by entering **root** for the user ID and the password configured in Step 15 (Example: Hgt50N3181.5n2B).

Step 3: When logged in, enter the getserverinfo command, and then note the status of the Health Monitor.



Step 4: If the Cisco MSE Health Monitor is running, skip to the next procedure.

If the Cisco MSE Health Monitor is not running, enter the service msed start command. The MSE platform processes start.

vMSE-7-4-0-31
Getting Started Summary Resource Allocation Performance Tasks & Events Alarms Console Permissions Maps Storage Views Update Manager
vMSE-VA-7-4-8-31 login: root
Password:
Last login: Wed Nov 7 89:33:85 on tty1
[rootQ∨MSE-VA-7-4-8-31 ~]# getserverinfo Health Monitor is not running
Iroot@vMSE-UA-7-4-8-31 ~]# service msed start
Starting MSE Platform
no crontab for root
syslogd: unknown facility name "LOCAL*"
ip_tables: (C) 2000-2006 Netfilter Core Team
Netfilter messages via NETLINK v0.30. ip_conntrack version 2.4 (8192 buckets, 65536 max) - 304 bytes per conntrack
Starting Health Monitor, Waiting to check the status.
Starting Health Monitor, Waiting to check the status.
Health Monitor successfully started Starting Admin process
Starting namin process.
Starting database
Database started successfully. Starting framework and services Framework and services successfully started
rancours and services successfully started
[root0vMSE-VA-7-4-0-31 ~]#

Step 5: Repeat Step 3 and verify that the MSE Health Monitor is running.

Process



Configuring Cisco Prime Infrastructure 1.3 for the Cisco MSE VA

- 1. Log in to Cisco Prime Infrastructure 1.3
- 2. Add a user ID for the Cisco MSE VA
- 3. Add the Cisco MSE VA
- 4. Confirm Cisco MSE VA addition and license
- 5. Synchronize the WLCs to use Cisco MSE
- 6. Enable NMSP between MSE and WLCs

Cisco Prime Infrastructure 1.3 must be configured with the relevant Cisco MSE VA information. This configuration allows Prime Infrastructure 1.3 to communicate with the MSE VA server.



Tech Tip

Prime Infrastructure supports the following browsers.

- Google Chrome—19.0 build
- Mozilla Firefox— ESR 10.x. 13.0 and 14.0
- Microsoft Internet Explorer 8.0 or 9.0 with Chrome plug-in.

Native Internet Explorer is not supported. The recommended minimum resolution for each browser is 1280 x 800 pixels.

Tech Tip

Prime Infrastructure supports the following browsers.

- Google Chrome—19.0 build
- Mozilla Firefox— ESR 10.x, 13.0 and 14.0
- Microsoft Internet Explorer 8.0 or 9.0 with Chrome plug-in.

Native Internet Explorer is not supported. The recommended minimum resolution for each browser is 1280 x 800 pixels

Step 1: Using a supported browser, access the Cisco Prime Infrastructure 1.3 management interface (Example: https://10.4.48.38).

Step 2: Log on using the configured Cisco Prime Infrastructure 1.3 user ID and password (Example: root/Prime13).

 ★ → C https://1 	14.48.38/webacs/pages/common/login.jsp;sessionid=41C12B80896802EFC8B4C99B33F13ECB	
	© 2013 Cisco Systems,Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco System,Inc.and/or its affiliates in the U.S and certain other countries cisco	

Procedure 2

Add a user ID for the Cisco MSE VA

Step 1: In Cisco Prime Infrastructure 1.3, navigate to Administration > Users, in the list, choose Add User, and then click Go.

uluulu Cisco Prime						Virtual Domain ROOT-DOMAIN	root v	. ₽ +	
cisco Infrastructure	🟠 Hor	ne Design 🔻	Deploy 🔻	Operate 🔻	Report 🔻	Administration 🔻			P 80.
Users, Roles & AAA									
Change Password	Users Administration > Us	ers, Roles & AAA > U:	sers					Add User	G
Local Password Policy	User Na	ne	Ν	lember Of		Status		Audit Trail	
AAA Mode	Ming		A	dmin		Active			
Users	User1		S	uper Users		Active		۹	
oses	🗖 root		R	oot		Active			

Step 2: Enter the username (Example: vMSEuser) and password (Example: C1scO!349@) that you configured in Step 17 of Procedure 3, "Configure the Cisco MSE virtual appliance."

Step 3: Select Admin, Config Managers, Super Users, and System Monitoring, and then click Save.



It may be necessary to modify the password policy in Cisco Prime Infrastructure 1.3 in order to accept passwords that contain variations of the word Cisco as used above. To do this, navigate to Administration > Users, Roles & AAA > Local Password Policy, and modify the necessary policy settings in order to match your security policy.

cisco Prime	Virtual Domain ROOT-DOMAIN root ¥ 🔎 V	
cisco Infrastructure	🟠 Home Design 🔻 Deploy 🔻 Operate 🗶 Report 👻 Administration 👻	P 00.
Users, Roles & AAA		
Change Password	Add User Administration > Users, Roles & AAA > Users > Add User	
Local Password Policy		
AAA Mode	General Virtual Domains	
Users	Username VMSEuser	
User Groups	New Password ①	
Active Sessions	Groups Assigned to this User	
TACACS+	₩ Admin	
RADIUS Servers	✓ Config Managers	
SSO Servers	ELobby Ambassador 🕖	
SSO Server AAA Mode	Monitor Lite (1)	
	North Bound API	
	E Root @	
	₩ Super Users	
	System Monitoring	
	■ User Assistant ①	
	Vuser Defined 1	
	Save Cancel	



Add the Cisco MSE VA

Step 1: Navigate to Design > Mobility Services Engines.



Step 2: In the list, choose Add Mobility Services Engine, and then click Go.

uluulu. Cisco Prime		Virtual Domain K001:DOMAIN root y Dy
cisco Infrastructure	Home Design ▼ Deploy ▼ Operate ▼ Report ▼ Administration ▼	P 00.
Mobility Services Engines Services > Mobility Services Engines		Add Mobility Services Engine Ga
		la l
None Detected		

Step 3: On the Add Mobility Services Engine page, enter the following parameters:

- · Device Name-vMSE-VA-7-4-0-31
- IP Address—10.4.48.40
- Contact Name—SBA
- · Username—admin (do not change this)
- · Password—(do not change the auto filled value)
- HTTP Enable—No



Tech Tip

Note that enabling HTTP changes the default from HTTPS. It is recommended that you leave HTTP disabled for added security. It is not necessary to change the password.

cisco Prime Cisco Infrastructure			root
	Add Mobility Services Engine		
Add MSE Configuration			
Licensing	Device Name	VMSE-VA-7-4-0-31	
Select Service	IP Address	10.4.48.40	
Tracking	IP Address	1 10.4.48.40	
Assign Maps	Contact Name	SBA Admin	
Mobile App Enablement	Username 🖓	admin	
	Password ②		
	HTTP D	Enable	
	O Selecting Delete synchronized set Existing location history data is retained	ments IP (Network designs, controllers, whed wetches and event definitions) vice assignments permanently removes all service assignments from the MSE. Thomewer you must use manual service assignments to do any future location calculations. au IP (VIP) address support has been added for High Availability. If you with to use High Availability and have configured a VIP, add the MSE IP.	
		Next	

Step 4: On the MSE License Summary page, review the Cisco Prime licensing for the Cisco MSE VA. If you do not have additional licenses to add, click **Next**.

dit MSE Configuration	MSE License Su	immary							
-	B Darmanant lican	ene includ	o installed licens	e counts and in-built lic	opro countr				
icensing									
elect Service						License Type		Unlicensed Count	
racking	vMSE-VA-7-4-0-31	Not Acti	ivated (AIR-M	SE-VA-K9:V01:vMSE	-VA-7-4-0-31	cisco.local_6687b736	i-2903-:	L1e2-9dfc-005056	ia25d96)
ssign Maps		CAS	18000	CAS Elements	100	Evaluation (60 days left)	0	0	0%
lobile App Enablement		wIPS	5000	wIPS Monitor Mode APs	10	Evaluation (60 days left)	0	0	0%
		WIP5	5000	wIPS Local Mode APs	10	Evaluation (60 days left)	0	0	0%
	Add License F	temove Li	cense						

If you have additional licenses for the MSE, click **Add License**. On the Add A License File dialog box, click **Choose File**, select the Cisco MSE license file that you received as part of the fulfillment process, and then click **OK**. On the MSE License Summary page, click **Next**.

cisco Prime cisco Infrastructure									root v
	MSE Lice	ense Summary							
Edit MSE Configuration									
Licensing				and in-built license cour ted based on AP count	nts. (using 50 elements per AP)				
Select Service		Platform Limit by AP		Installed Limit by AP		Count	Unlicensed Count	% Liked	
Tracking	Service	(by elements)	Туре	(by elements)	License Type		s by elements		
Assign Maps	VMSE-VA-	7-4-0-42 Not Activa	ted (AIR-MSE-VA-K	9:V01:vMSE-VA-7-4-	0-42.cisco.local_da311c7	4-747e-11e	2-9d1b-005056a2	21c77)	
Mobile App Enablement	CAS	360 (18000)	CAS Elements	10 (100)	Evaluation (118 days left)	54	50	54%	
	License File:	Choose File MSE2	012120223800.lic			[-o	K Cancel	0%	
								Back Next	

Step 5: On the Select Mobility Service page, select **Context Aware Service**, Wireless Intrusion Protection Service (WIPS), and Mobile **Concierge Service**, and then click **Next**.

cisco Prime cisco Infrastructure	
	Select Mobility Service
Edit MSE Configuration	
Licensing	Context Aware Service
Select Service	
Tracking	Oisco Context-Aware Engine for Clients and Tags
Assign Maps	\odot Partner Tag Engine (2)
Mobile App Enablement	V WIPS
	Mobile Concierge Service
	Location Analytics Service

Step 6: On the Tracking page, enable the following real-time and historical tracking services as shown in the following table, and then click **Next**.

Table 1 - Tracking and history parameters

Tracking	History
Wired Client	Wired Stations
Wireless Clients	Client Stations
Rogue Access Points	Rogue Access Points
Rogue Clients	Interferers
Active RFID Tags	

dt MBE Configuration Centring elect Service acking ssign Maps Icoble App Enablement	Select Tracking & History Parameters.	History Viewed Stations Calent Stations Rogue Access Points Rogue Clients Interferers Asset Tags	

Step 7: On the Assign Maps page, click Next.

Step 8: On the Mobile App Enablement page, do not enable Mobile App Integration, click **Done**, and then on the "Your MSE Settings have been saved" message, click **OK**.

cisco Infrastructure		root w
Cisco Infrastructure	Mobile App Enablement	
	Create location-based notifications and offers. Powered by meridian	ne

Procedure 4

Confirm Cisco MSE VA addition and license

It may be necessary to limit the number of elements that are being tracked, according to the license. If you are using the evaluation license, which allows 100 items to be tracked and expires in 180 days, you may have to limit what those license elements are being used for. This procedure provides guidance for manually configuring which items to track.

Step 1: Navigate to **Design > Mobility Services Engines**, and then verify that configured IP address of the Cisco MSE VA is reachable and that each of the mobility services are available.

	Lulu, Cisco Prime				Virtu	al Domain ROOT-DOMAIN	root ▼ 🔎 Ψ		
		🟠 Home Desi	gn 🔻 Deploy 🔻	Operate 🔻	Report 🔻 Ad	ministration 🔻		P	.00.
		5					Select	a command	GO
_							Mo	bility Service	
CISCO Finite Cisco Prime Cisco Prime Cisco Prime Cisco Finitestructure Cisco Finitestruc									
	vMSE-VA-7-4-0-31	Cisco Mobility Services Engine - Virtual Appliance	10.4.48.40	7.4.0.31	Reachable		Service Wireless Intrusion Protection Service Mobile Concierge	Enabled	Up

Step 2: If you do not want to manually configure which devices are tracked, skip to the next procedure.

If you want to manually configure tracking, navigate to **Design > Mobility Services Engines**, and then select the Cisco MSE.

Step 3: In the tree, navigate to Context Aware Services > Administration > Tracking Parameters.

Step 4: Enable only the Network Location Service elements necessary, and then enter a limit value that conforms to your Licensed Limit (Example: 15 Wireless Clients + 45 Rogue Access Points + 10 Rogue Clients + 30 Interferers = 100 Licensed Elements). When appropriately valued, click Save.

		🏠 Home Design ▼ Deploy	▼ Operate ▼ I	Report 🔻 Adm	inistration 🔻		P G Ø.
System		Parameters: vMSE-VA-7-4					
Context Aware Service	~	Mobility Services Engines > vMSE-VA-7-4-			,		
🖁 General		lisco Tag Engine is enabled, the Lic Parameters	ensed Limit for Network	Location Service	elements also inclu	ides Asset Tracking	elements.
Administration							
	Network	Location Service Elements:	Licensed Limit =	100			
Tracking Parameters	Enable	Tracking Parameters	Enable Limiting	Limit Value	Active Value	Not Tracked	
ᡖ Filtering Parameters		Wired Clients		0	0	0	
🏪 History Parameters		Wireless Clients		15	15	1	
ᡖ Presence Parameters	v	Rogue AccessPoints		45	45	50	
ᡖ Import Asset Information		Exclude Adhoc Rogue APs					
Export Asset Information	1	Rogue Clients	V	10	0	0	
	v	Interferers		30	0	0	
Hava iccu							
ᡖ Northbound Notifications	Asset Tra	acking Elements:					
ᡖ Location Parameters	Enable	Tracking Parameters	Enable Limiting	Limit Value	Active Value	Not Tracked	
ᡖ Notification Parameters	10	Active RFID Tags		0	0	0	
 Partner Engine 		Active to the toge		0	0	0	
ᡖ Partner Engine Status	Save	Cancel					
Notification Statistics							
wIPS Service							

Procedure 5

Synchronize the WLCs to use Cisco MSE

In order to establish and assign Cisco MSE to each of the wireless LAN controllers, it is first necessary to synchronize them. In the following steps, you assign the MSE VA to each of the wireless LAN controllers in Cisco Prime Infrastructure 1.3.

Step 1: Navigate to Design > Mobility Services > Synchronize Services.



Step 2: On the left side of the page, in the list, click Controllers.

ululu Cisco Prime			Virtual Domain R	tOOT-DOMAIN root	• (P+	
cisco Infrastructure		Operate 🔻 Report 🔻	Administratio	on 🔻		P 9
Network Designs Controllers	Network Designs Services > Synchronize Services > Network Design Modifying assignments for Network Designs overrides any previous assignments of their cl	s will auto assign the Controlle	ers for CAS. Mot	difying assignments at	Campus or Buildin	ng level always
	Show: Type All Go					
	Show: Type All Go	Type	Service	MSE	Sync Status	Message
Event Groups Wired Switches Third Party Elements		Type Campus		MSE	Sync Status	Message
Wired Switches	Name A		-			-

Step 3: Select each of the wireless LAN controllers that you want to assign to the Cisco MSE, and then click **Change MSE Assignment**.

cisco Infrastructure		☆ Home Design ▼ E	Deploy 🔻 Operate 🔻	Report 🔻	Administra	tion 🔻		P 8 0
Network Designs Controllers	Servio	trollers res > Synchronize Services > Con r MSE versions prior to 7.0.x,		for one service	will also mo	dify the assignment	t for the other service('s).
Event Groups	V	Name 🔺	IP Address	Version	Service	MSE	Sync Status	Message
	1	DMZ-WLC-Guest	192.168.19.54	7.4.1.42	-	-		
Wired Switches		RS208-WLC2504	10.5.87.10	7.4.1.42	-	-	-	-
Third Party Elements	1	WLC-1-Primary	10.4.46.64	7.4.1.42		-		-
Third Party Clements	1	WLC-OEAP-1	192.168.19.20	7.3.101.0				-
Service Advertisements	1	WLC-OEAP-2	192.168.19.21	7.3.101.0				
	1	WLC-RemoteSites-1	10.4.46.68	7.4.1.42	-	-		-
	1	WLC-7_4_1_42	10.5.24.64	7.4.1.42				

Step 4: On the Choose MSEs dialog box, select **CAS** (Context Aware Service) and **wIPS**, and then click **Synchronize**.



Procedure 6

Enable NMSP between MSE and WLCs

The Cisco Network Mobility Service Protocol (NMSP) is a Transport Layer Security (TLS) based protocol that manages the communication between the Cisco MSE and the wireless infrastructure inclusive of controllers and Cisco Catalyst switches. Information collected at chokepoints, along with various telemetry and emergency information, is communicated by using this protocol.

If the wireless LAN controller was discovered in Cisco Prime Infrastructure by using the Read/Write SNMP community string, then Cisco NMSP should be established automatically between the Cisco MSE and the WLC. If however the WLC was discovered using the Read Only community string, NMSP is likely in the inactive state, as shown in Step 3 below.



Tech Tip

In order for Cisco MSE to communicate with the wireless infrastructure by using NMSP, the clocks of all devices must be synchronized. It is therefore recommend that all infrastructure components utilize NTP for consistent clock synchronization.

Step 1: Navigate to Design > Mobility Services > Synchronize Services, and then in the left column, click Controllers.

Step 2: On the Controllers page, for each of the wireless LAN controllers that provide Cisco CleanAir information, click the **[NMSP status]** link.

uluulu, Cisco Prime					Virtual Domain ROOT-DOMA	IN root y 🔎	v
cisco Infrastructure		Deploy 🔻 Operate 🔻 Repo	rt 🔻 Administratio	n •			P 80
Network Designs	Controllers Services > Synchronize Services > Controllers						
Controllers	O For MSE versions prior to 7.0.x, modifying		also modify the assig	nment for the at	ner service(s).		
Event Groups	Name A	IP Address	Version	Service	MSE	Sync Status	Message
	DMZ-WLC-Guest	192,168,19,54	7.4.1.42	CAS	VMSE-VA-7-4- [NMSP	sync status	Message
Wired Switches	 DM2+WDC+GDESC 	192,108,19,04	7.4.1.42	CAS	0-31 Status]	*	
Third Party Elements				WIPS	vMSE-VA-7-4- [NMSP 0-31 Status]	#	
ervice Advertisements	R\$208-WLC2504	10.5.87.10	7.4.1.42	CAS	vMSE-VA-7-4- [NMSP 0-31 Status]	#	
				wIPS	vMSE-VA-7-4- [NMSP 0-31 Status]	#	
	WLC-1-Primary	10.4.46.64	7.4.1.42	CAS	vMSE-VA-7-4- 0-31	#	

Step 3: If any of the WLCs has an NMSP status of **Inactive**, note which WLCs are not in an active state. Perform the steps below for each of the inactive WLCs as noted.

If all of the WLCs have an NMSP status of Active, skip to the next procedure.

alialia Cisco Prime	What Domain ROOT-DOMAIN root + D+
cisco infostractare	🟠 Home Design * Deploy * Operate * Report * Administration * 🛛 🏲 🖸 🚱 -
System 🗸	NMSP Connection Status Details: 10.4.46.64
🐇 General Properties	Services > Nobility Services Engines > vMSE-VA-9-49-31> System > Subus > IMEP Connection Status > NMSP Connection Status Details
🐇 Active Sessions	Summary
ᡖ Trap Destinations	IP Address 10.4.46.64
🐇 Advanced Parameters	Version 7.4.1.42
👗 Logs	Target Type Controler
 Services High Availability 	MMSP Status Inactive 😚
HA Configuration	Echo Request Count 0 k
🕌 HA Status	Echo Response Count 0
 Accounts 	Last Activity Time -
ᡖ Users	Last Echo Request Message Received At
droups	Last Echo Response Message Received At - Model 5500
 Status 	MAC Addess
ᡖ Server Events	Capible IMSP Services N/A

Step 4: On the Cisco MSE VA, in the CLI, issue the **cmdshell** command. The response is the **cmd**> prompt.

Step 5: At the cmd> prompt, issue the show server-auth-info command.

Step 6: Copy down the key hash value and MAC address as shown on the Cisco MSE VA. Be careful not to transpose any digits in the hash string or MAC address obtained.

Cisco Mobility Service Engine
vMSE-VA-7-4-0-31 login: root Password: Last login: Wed Nov 7 09:46:27 on tty1 [root@vMSE-VA-7-4-0-31 ~]# cmdshell
cmd> show server-auth-info invoke command: com.aes.server.cli.CmdGetServerAuthInfo AesLog queue high mark: 50000 AesLog queue low mark: 500
Server Auth Info
MAC Address: 00:50:56:a2:5d:96
Key Hash: b62741ab695f6ef95e5a3fc7b84496ee8972cd8f
Certificate Type: SSC
cmd> exit
[root@vMSE-VA-7-4-0-31 ~]# _

Next, you determine if the Cisco MSE is authorized in the WLC.

Step 7: From the console port, navigate to the CLI interface of a wireless LAN controller that displayed as Inactive in Step 3, and then enter the **show auth-list** command. In the example below, there are no MSEs currently authorized to establish an NMSP session with the wireless LAN controller.

(Cisco Controller) >show auth-list Authorize MIC APs against AAA disabled Authorize LSC APs against Auth-List disabled APs Allowed to Join AP with Manufacturing Installed Certificate.... yes AP with Self-Signed Certificate.... no

AP with Locally Significant Certificate..... no

Step 8: Authorize the Cisco MSE on the wireless LAN controller by using the information obtained from the MSE VA in Step 6.

(Cisco Controller) >**conf**

(Cisco Controller) config>auth-list add ssc 00:50:56:a2:5d:96 b62741ab695f6ef95e5a3fc7b84496ee8972cd8f

5027414505510215525451275044502205720

(Cisco Controller) config>

Step 9: Verify that the Cisco MSE has been authorized on the wireless LAN controller.

(Cisco Controller) >show auth-list

Authorize MIC APs against Auth-list or AAA disabled Authorize LSC APs against Auth-List disabled APs Allowed to Join AP with Manufacturing Installed Certificate.... yes AP with Self-Signed Certificate..... no AP with Locally Significant Certificate..... no

Mac Add Cert Type Key Hash

00:50:56:a2:5d:96 SSC b62741ab695f6ef95e5a3fc7b84496ee8972cd8f (Cisco Controller) > **Step 10:** Repeat Step 7 through Step 9 for each of the wireless LAN controllers that do not have an established NMSP connection.

After manually adding the Cisco MSE key hash value and MAC address to the WLCs, you must verify that the NMSP status is now active.

Step 11: Within Cisco Prime Infrastructure 1.3, navigate to Design > Mobility Services > Synchronize Services > Controllers, and then for every WLC connected to Cisco MSE and used for CAS or wIPS, click on the [NMSP Status] link.

Julualu, Cisco Prime					Virtual Domai	ROOT-DOMAIN root w	[ρ *	
cisco Infrastructure	🙆 Home Design 🔻	Deploy Operate Report	Administration	•				P 00.
Network Designs	Controllers Services > Synchronize Services > Controllers							
Controllers	O For MSE versions prior to 7.0.x, modifyin	g the assignment for one service will a	lso modify the assignm	ent for the othe	ar service(s).			
Event Groups	□ Name ▲	IP Address	Version	Service	MSE	Sync St	tatus Message	
Wired Switches	DMZ-WLC-Guest	192.168.19.54	7.4.1.42	CAS	VMSE-VA-7-4- 0-31	[NMSP #		
Third Party Elements				wIPS	vMSE-VA-7-4- 0-31	[NMSP #		
Service Advertisements	R5208-WLC2504	10.5.87.10	7.4.1.42	CAS	vMSE-VA-7-4- 0-31	[NMSP #		
				WIPS		[NMSP #		
	WLC-1-Primary	10.4.46.64	7.4.1.42	CAS	vMSE-VA-7-4- 0-31	[NMSP #		
				wIPS	vMSE-VA-7-4- 0-31	[NMSP #		

The NMSP status should now be **Active** for each of the WLCs as shown below.

Step 12: If the status does not change to an active state, verify that the authorization list on the WLC has the proper MAC address and SSC key hash of the Cisco MSE VA. Also, ensure IP connectivity exists between the WLC, MSE, and Cisco Prime Infrastructure 1.3.

de de Cicco Drimo							Vetual Domain F	ROOT-DOMAIN root v	<i>Ω</i> +
cisco Infrastructure	۵	Home Design 🔻	Deploy 🔻	Operate 🔻	Report •	Administration •			P 80.
System	 NMSP Connection 								
🏭 General Properties	Services > Mobility Services	i Engines > vMSE-VA-7-4-0-3	11> System > S	catus > NMSP o	Connection Status	x > NMSP Connection Stat	tus Details		
🗄 Active Sessions	Summary								
ᡖ Trap Destinations	IP Address		10.4.46.64						
Advanced Parameters	Version		7.4.1.42						
Logs	Target Type		Controller						
 Services High Availability 	NMSP Status		Active						
 Services High Availability HA Configuration 	Echo Request Count		61						
	Echo Response Count		61						
ᡖ HA Status	Last Activity Time		2012-Nov-6	09, 06:12:41	PST				
 Accounts 	Last Echo Request Me	issage Received At	2012-Nov-6	09, 06:12:34	PST				
ᡖ Users	Last Echo Response M	lessage Received At	2012-Nov-6	09, 06:12:35	PST				
ᡖ Groups	Model		5500						
▼ Status	MAC Address		d0:d0:fd:9	2:67:cf					
ᡖ Server Events	Capable NMSP Service	6	IPV6_CLIEF	NTS_SUPPOR	T, RSSI, INFO	RMATION, STATISTICS, I	IDS, HANDOVER, AP MONITOR, SPEC	CTRUM	
ᡖ Audit Logs									
NCS Alarms	Subscribed Services								
NCS Events	Service	Subservices							
-	AP MONITOR	SUBSCRIPTION							
👗 NMSP Connection Status	IDG	WIRELESS IDS							
 Maintenance 	INFORMATION	MOBILE_STAT							
🚠 Backup	SPECTRUM	MOBILE_STAT AGGREGATED			DOBT				
ᡖ Restore	STATISTICS	MOBILE_STAT		_DEVICE_RE	PURI				
ᡖ Download Software	51ATISTICS	MUBILE_STAT	ton, rAG						

Troubleshooting with Cisco CleanAir

With the addition of the Cisco MSE VA, historical Cisco CleanAir information is readably accessible through Cisco Prime Infrastructure 1.3. The ability to determine the quality of the RF spectrum combined with the ability to retrieve baseline historical information is key in most RF spectrum troubleshooting.

The real power of Cisco CleanAir is that a network administrator, without leaving their own desk, can analyze the Wi-Fi spectrum in any location which they have connectivity to.

The Cisco Aironet 2600 and 3600 Series access points can be put in Spectrum Expert-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 Cisco Spectrum Expert Wi-Fi 4.0 (or later) software, the Wi-Fi network administrator can view the environment directly. Your organization no longer needs to fly expensive personnel onsite in order to troubleshoot physical-layer issues that are challenging and, too often, intermittent.

Process

Viewing and Analyzing Cisco CleanAir

- 1. View historical Cisco CleanAir information
- 2. Accessing CleanAir APs using Spectrum Expert

Procedure 1

View historical Cisco CleanAir information

Oftentimes it's imperative that a historical baseline for RF spectrum management is available. Using Cisco Prime Infrastructure 1.3 combined with the Cisco MSE VA, you can easily view historical information.

Step 1: In Cisco Prime Infrastructure 1.3, navigate to Home > Overview > CleanAir, in the Filters list, choose the desired time frame, and then click Go.

						Vetual Domain ROOT DO	w toon (I reading	[ρ+	
seo Infrastructure 🖉 Home Design * Deploy * Operate * Report * Administration *									POP
Incidents Performance Detail Dazhboards									
eneral Client Security Meth Counter Context Aware									
ters 🛞 *Tme Frame Past 1 Week * Go									
302 I La(n Avg Ar Quality Angla (unwind)	Worst 802.11a/h 1 None detected	nterferers							
10	Worst B02.11b/g/	1 Interferers							
40	Interferer ID	Type	Status	Severity	Affected Channels	Duty Cycle (%)	Discovered	Last Updated	Floor
0 30/0/12 10/10/12 10/12/12 10/12/12 10/12/12 10/12/12 10/14/12 10/14/12	42:5d:96:00:2exk	Bluetooth Discovery	Active	2	11	1	Thu Nov 15 10:04:11 PST 2012	Thu Nov 15 10:21:00 PST 2012	System C > Heador > First Pic
Z Time	42:50:96:00:20:03	Bluetooth Link	Activo	0	11	1	Thu Nov 15 10:20:05 PST 2012	Thu Nov 15 10:20:07 PST 2012	System 0 > Headq > First B
31/1/13 13/1/13 13/1/13 13/1/13 13/1/13 13/14/14/14/14/14/14/14/14/14/14/14/14/14/		11/	10/52	13/13/12	11/12/12 Time	13/13/3	12 11	/14/12	11/19/12
10/012 10/012 10/012 10/012 10/012 2 Time 2	# # 31/₩12			13/51/32		13/13/3	12 31.	aa	11/11/12
NUNUX KUNIYA NUNUYA NUNUYA NUNUYA NUNUYA NUNUYA NUNUYA Tima 2 LILATIYA Qulity a calana	# 31/W32	ierer Count @				53/33/3	12 11	/14/12	11/19/12
INTERS INTERS<	# # 31/₩12	ierer Count @				53/33/3	12 11.	/14/12	11/11/12
202 LIGHT NO CAMPY 202 LI	* * * * * * * * * * * * * * * * * * *	ierer Count @				53/33/3	12 11		11/19/12
XUMUS XUMUS <th< td=""><td>a July12</td><td>ierer Count @</td><td> Iy Custor</td><td>^^</td><td>Time</td><td></td><td><u> </u></td><td>/14/12</td><td></td></th<>	a July12	ierer Count @	Iy Custor	^^	Time		<u> </u>	/14/12	
NUMBER NUMBER NUMBER NUMBER NUMBER NUMBER NUMBER Image: Number of calls NUMBER	a July12	erer Count @ e 4e 3es 6er overleid)	Iy Custor	^^	Time		<u> </u>	~~~~	
	a a b b b b b b b b b b b b b b b b b b c c d <t< td=""><td>erer Count @ a (4a 3m 6m overlaid) rob 18+00</td><td> Iy Custor</td><td>^^</td><td>Time</td><td></td><td><u> </u></td><td>~~~~</td><td></td></t<>	erer Count @ a (4a 3m 6m overlaid) rob 18+00	Iy Custor	^^	Time		<u> </u>	~~~~	
XXV812 XXX812 XXX812<	#	erer Count a da 3m fer overleid) +00 36:00 k Interferers	Iy Custor	^^	Time		<u> </u>	~~~~	11/18/12
NUMES NUMES <th< td=""><td># JJJW32 Image: State Stat</td><td>erer Count. @ n 4e 3m fer overlaid) 100 28:00 k Interferers</td><td>1 by Custor</td><td>22:00</td><td>Time</td><td>20 4:09</td><td>6-00 D</td><td></td><td>12:00</td></th<>	# JJJW32 Image: State Stat	erer Count. @ n 4e 3m fer overlaid) 100 28:00 k Interferers	1 by Custor	22:00	Time	20 4:09	6-00 D		12:00

Tech Tip

If you find that Cisco CleanAir Air Quality graphs are not being displayed as shown above, you may need to perform one or more of the following troubleshooting steps:

- 1. Ensure that CleanAir-capable APs have been configured on the floor plan or map and that their radios are enabled.
- 2. Ensure that all CleanAir settings have been successfully applied to the APs and wireless LAN controller via the templates described in this document.
- 3. Repeat Step 4 in Procedure 5 above by first clearing CAS (Context Aware Services) and wIPS and then synchronizing. Then go back again, select CAS and wIPS, and re-synchronize.
- 4. Ensure that NMSP between the Cisco MSE and WLCs is established within Prime Infrastructure as defined in Procedure 6, "Enable NMSP between MSE and WLCs."
- 5. Ensure that the Cisco MSE services are running as described in Procedure 4, "Confirm Cisco MSE VA addition and license."

Step 2: Click Worst Interferers. The corresponding floor plan is displayed.

Step 3: In the left pane, under Floor Settings, select **Interferers**. The list of interferers is graphically displayed.



Step 4: Navigate to **Overview > Context Aware**. This displays the historical information on the number of rogues, wireless clients, and other context-aware information obtained from the Cisco MSE VA.



Step 5: Within Cisco Prime Infrastructure 1.3, navigate to Operate > Operational Tools > Wireless > Interferers. A list of active interferers discovered within the last 5 minutes is shown. If you click Edit Search, you can alter the timeframe.

altada Cisco Prime cisco Infrastructure		1 Home	Design 🔻	Deploy • Operate • Repo	rt • Administration •				What Danain ROOT-DOMMIN real + D+	P 6 0-0
nterferers <mark>Lanves</mark> antor > Interferers sarch Oiteris: Active Interferer	s only, Detected within	i last 5 minutes (Ed	It Search)							
Interferer ID	Type	Status 🔻	Severity	Affected Band	Affected Channels	Duty Cycle (%)	Discovered	Last Updated	Roor	
22:56.96:00:28:49	Bluetooth Link	Active	3	2.4 GHz (802.11b/g/h)	11	1	11/15/12 10:41:57 AM	11/15/12 10:45:00 AM	System Campus > Headquarters > First Floor	
s2:5d:95:00:2erea	Eluetooth Link	Active	2	2.4 GHz (802.11b/g/n)	11	1	11/15/12 10:42:34 AM	11/15/12 10:44:35 AM	System Campus > Headquarters > First Floor	
			-							

Step 6: Click the floor for any of the alarm conditions shown above. The floor plan is displayed for the affected area.



Step 7: In the Show MSE data list, choose Within the last 24 hours, and then to the right of Interferers, click the arrow.

Step 8: In the Interferer Filter pane, in the Interference Type list, choose All Interferers, select Show Zone of Impact, and then click OK. Note the zone of impact caused by all sources of interference.



Procedure 2

Accessing CleanAir APs using Spectrum Expert

When the call for assistance arrives, it almost certainly will originate from a location that does not have the knowledgeable human resources to troubleshoot, identify, and fix the issue. Wi-Fi devices 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, Digital Enhanced Cordless Telecommunications (DECT) phones, analog wireless cameras, or even radio jammers. The specialized radios in the Cisco CleanAir radio environment can identify these devices and, with triangulation, can find where these devices are located.

When the call comes in, you need to identify as many facts about the issue as possible in order to make informed decisions. The information can include the location of the problem (for example, the street side of the building does not have connectivity) and time of day (for example, the issue is pronounced at lunch time). With as much information from the end user as possible, you can now look at the radio environment because the system shows that clients are connecting and Cisco Prime Infrastructure 1.3 indicates that AQ has dropped.

The Cisco CleanAir-capable access point must be changed from either Monitor Mode or Local Mode of operation to Spectrum Expert Connect Mode (SE-Connect). This change is disruptive to the wireless users that are associated to the access point.

Step 1: Log in to the wireless LAN controller.

Step 2: Navigate to WIRELESS.

Step 3: Select the Cisco CleanAir access point that is closest to the suspected source of interference.

Step 4: In the AP Mode list, choose SE-Connect, and then click Apply.

Step 5: Wait for the access point to reboot and reconnect to the wireless LAN controller.

ireless	All APs > [Details for RS	207-CAP3602I				< Back	Ар
Access Points All APs Radios	General	Credentials	Interfaces	High Availability	Inventory	FlexConnec	t Advanced	
802.11a/n 802.11b/g/n	General				Versions			
Global Configuration	AP Name		RS207-CAP3602I		Primary Softw		7.2.110.0	
Advanced	Location		RS207		Backup Softwa		0.0.0.0	
Mesh	AP MAC A		70:ca:9b:86:30:b0		Predownload S		None	
RF Profiles	Base Rad		64:d9:89:47:60:10		Predownloader	d Version	None	
FlexConnect Groups	Admin St	atus	Enable 👻		Predownload N	lext Retry Time	NA	
FlexConnect ACLs	AP Mode		FlexConnect 💌		Predownload R	letry Count	NA	
▶ 802.11a/n	AP Sub N	lode	local FlexConnect		Boot Version		12.4.23.0	
▶ 802.11b/g/n	Operation	nal Status	monitor Rogue Detector		IOS Version		12.4(25e)JA1\$	
Media Stream	Port Num	iber	Sniffer		Mini IOS Versi	on	0.0.0.0	
Country	Venue G	roup	Bridge SE-Connect	•	IP Config			
Timers	Venue Ty	pe	Unspecified 👻		IP Address		10.5.20.21	
Qo5	Venue Na	ame			Static IP			
	Language							
		Spectrum	21E8BB3E88093C31	IOD2B258195493731	Time Statistics			
	Interface	Key			UP Time		0 d, 04 h 36 m 42 s	
					Controller Ass	ociated Time	0 d, 02 h 46 m 01 s	
					Controller Asso	ociation Latency	0 d, 00 h 00 m 10 s	
	Hardware F	leset		Set to Fact	ory Defaults			
		a hardware reset o	on this AP	Clear cor defaults	nfiguration on this A	AP and reset it to	factory	
	Reset	AP Now		Clear	All Config			
				Clear	Config Except Sta	atic IP		

Step 6: Copy the Network Spectrum Interface Key and the IP address.

Wireless	All APs > Details for R	S207-CAP3602I		< Back Apply
Access Points All APs Radios	General Credentials	Interfaces High Availabilit	y Inventory Advanced	
802.11a/n 802.11b/g/n Global Configuration	General AP Name	RS207-CAP3602I	Primary Software Version	7.2.110.0
Advanced	Location	RS207	Backup Software Version	0.0.0.0
Mesh	AP MAC Address	70:ca:9b:86:30:b0	Predownload Status	None
RF Profiles	Base Radio MAC	64:d9:89:47:60:10	Predownloaded Version	None
FlexConnect Groups	Admin Status	Enable 👻	Predownload Next Retry Time	NA
FlexConnect ACLs	AP Mode	SE-Connect 👻	Predownload Retry Count	NA
▶ 802.11a/n	AP Sub Mode	None 👻	Boot Version	12.4.23.0
▶ 802.11b/g/n	Operational Status	REG	IOS Version	12.4(25e)JA1\$
Media Stream	Port Number	1	Mini IOS Version	0.0.0.0
Country	Venue Group	Unspecified -	IP Config	
Timers	Venue Type	Unspecified 👻	IP Address	10.5.20.21
▶ QoS	Venue Name		Static IP	
	Language			
	Network Spectrum Interface Key	821B3CC03E76085FE0B4DF7BB386C73	3 Time Statistics	0 d, 00 h 06 m 33 s
			Controller Associated Time	0 d, 00 h 05 m 30 s
			Controller Association Latency	0 d, 00 h 01 m 02 s

Step 7: On a Supported Windows platform with Cisco Spectrum Expert Wi-Fi (4.0 or later) installed, launch Cisco Spectrum Expert.

Step 8: Select Remote Sensor.

Step 9: Enter the IP address and the Network Spectrum Interface Key of the Cisco CleanAir access point that you copied in Step 6.

Step 10: If the access point is on the 2.4 GHz band, select **b/g/n**, and then click **OK**.

If the access point is on the 5 GHz band, select a/n, and then click OK.

🧑 Cisco Spectrum Expert - WCS Compa	stible 🗖 🖗
<u>File • View • Spectrum • Tools • Hel</u>	p+ 📴 o 3 🗉 G 🖶 🕀 /
Active Devices 7 ×	Spectrum Spectrum Devices Channel Summary Reinder
Control Panel	To begin viewing data, add a plot by right-ficking or using the "add plot" command from the pull-down meru. Connect to Sensor Connect to Sensor Sensor Card with Internal Antenna Sensor Card with
For Help, press F1	Monitored: - none- Dormant Sensor Disconnected: 10.5.20.21 UpTime: - No

The connected Windows machine now connects to the remote Cisco CleanAir access point on UDP port 37540 (if you selected **b/g/n** in Step 10) or on UDP port 37550 (if you selected **a/n** in Step 10). If connection problems occur, verify that you can ping the Cisco CleanAir access point and that no network devices are blocking the necessary UDP port information.

Remote Spectrum Analysis

The remote sensor capability in Cisco Spectrum Expert gives you the ability to get real-time, physical-layer spectrum data without having to drive or fly onsite. The following figure illustrates this capability in a Wi-Fi-only environment and gives you an understanding of how it can show you what is really happening in your remote environment.

Figure 1 - Cisco Spectrum Expert spectrum analysis



Tech Tip

Note that in the figure above, Cisco Spectrum Expert does not detect a wireless LAN card and that the remote sensor is at 10.5.20.21.

Appendix A: Product List

Wireless LAN Controllers

Functional Area	Product Description	Part Numbers	Software
Remote Site Controller	Cisco 7500 Series Wireless Controller for up to 6000 Cisco access points	AIR-CT7510-6K-K9	7.4.100.0
	Cisco 7500 Series Wireless Controller for up to 3000 Cisco access points	AIR-CT7510-3K-K9	
	Cisco 7500 Series Wireless Controller for up to 2000 Cisco access points	AIR-CT7510-2K-K9	
	Cisco Flex 7500 Series Wireless Controller for up to 1000 access points	AIR-CT7510-1K-K9	
	Cisco 7500 Series Wireless Controller for up to 500 Cisco access points	AIR-CT7510-500-K9	
	Cisco 7500 Series Wireless Controller for up to 300 Cisco access points	AIR-CT7510-300-K9	
	Cisco 7500 Series High Availability Wireless Controller	AIR-CT7510-HA-K9	
	Cisco Virtual Wireless Controller for up to 5 Cisco access points	L-AIR-CTVM-5-K9	
	Cisco Virutal Wireless Controller 25 Access Point Adder License	L-LIC-CTVM-25A	
	Cisco Virtual Wireless Controller 5 Access Point Adder License	L-LIC-CTVM-5A	
	Cisco Virtual Wireless Controller 1 Access Point Adder License	L-LIC-CTVM-1A	
On Site, Remote Site, or	Cisco 5500 Series Wireless Controller for up to 500 Cisco access points	AIR-CT5508-500-K9	7.4.100.0
Guest Controller	Cisco 5500 Series Wireless Controller for up to 250 Cisco access points	AIR-CT5508-250-K9	
	Cisco 5500 Series Wireless Controller for up to 100 Cisco access points	AIR-CT5508-100-K9	
	Cisco 5500 Series Wireless Controller for up to 50 Cisco access points	AIR-CT5508-50-K9	
	Cisco 5500 Series Wireless Controller for up to 25 Cisco access points	AIR-CT5508-25-K9	
	Cisco 5500 Series Wireless Controller for up to 12 Cisco access points	AIR-CT5508-12-K9	
	Cisco 5500 Series Wireless Controller for High Availability	AIR-CT5508-HA-K9	
On Site Controller, Guest Controller	Cisco 2500 Series Wireless Controller for up to 50 Cisco access points	AIR-CT2504-50-K9	7.4.100.0
	Cisco 2500 Series Wireless Controller for up to 25 Cisco access points	AIR-CT2504-25-K9	
	Cisco 2500 Series Wireless Controller for up to 15 Cisco access points	AIR-CT2504-15-K9	
	Cisco 2500 Series Wireless Controller for up to 5 Cisco access points	AIR-CT2504-5-K9	

Wireless LAN Access Points

Functional Area	Product Description	Part Numbers	Software
Wireless Access Points	Cisco 3600 Series Access Point Dual Band 802.11a/g/n and CleanAir with Internal Antennas	AIR-CAP3602I-x-K9	7.4.100.0
	Cisco 3600 Series Access Point Dual Band 802.11a/g/n and CleanAir with External Antennas	AIR-CAP3602E-x-K9	
	Cisco 2600 Series Access Point Dual Band 802.11a/g/n and CleanAir with Internal Antennas	AIR-CAP2602I-x-K9	
	Cisco 2600 Series Access Point Dual Band 802.11a/g/n and CleanAir with External Antennas	AIR-CAP2602E-x-K9	

Wireless LAN

Functional Area	Product Description	Part Numbers	Software
Wireless LAN	Cisco Mobility Services Engine (Virtual Appliance)	L-MSE-7.0-K9	7.4.100.0
	MSE License PAK (E Delivery)	L-MSE-PAK	
	1000 AP WIPS Monitor Mode licenses	L-WIPS-MM-1000AP	
	100 AP WIPS Monitor Mode licenses	L-WIPS-MM-100AP	
	1 AP WIPS Monitor Mode license	L-WIPS-MM-1AP	

Network Management

Functional Area	Product Description	Part Numbers	Software
Network Management	Cisco Prime Infrastructure 1.2	R-PI12-K91	1.3.0.20 ¹
	Cisco Prime Infrastructure 1.2 Base License and Software	R-PI12-BASE-K91	
	Cisco Prime Infrastructure 1.2 - Lifecycle - 10,000 Device License	L-PI12-LF-10K1	
	Cisco Prime Infrastructure 1.2 - Lifecycle - 5000 Device License	L-PI12-LF-5K1	
	Cisco Prime Infrastructure 1.2 - Lifecycle - 2500 Device License	L-PI12-LF-2.5K1	
	Cisco Prime Infrastructure 1.2 - Lifecycle - 1000 Device License	L-PI12-LF-1K1	
	Cisco Prime Infrastructure 1.2 - Lifecycle - 500 Device License	L-PI12-LF-5001	
	Cisco Prime Infrastructure 1.2 - Lifecycle - 100 Device License	L-PI12-LF-1001	
	Cisco Prime Infrastructure 1.2 - Lifecycle - 50 Device License	L-PI12-LF-501	
	Cisco Prime Infrastructure 1.2 - Lifecycle - 25 Device License	L-PI12-LF-251	
	Cisco Spectrum Expert Wi-Fi (CardBus)	AIR-CSCO-SE-WIFI-C	4.1.11

Notes:

¹ To obtain Cisco Prime Infrastructure 1.3, order Prime Infrastructure 1.2 with a service contract and download Prime Infrastructure 1.3 from Cisco.com. Existing customers with a valid service contract can also download Cisco Prime Infrastructure 1.3. Customers without a valid service contract must purchase a service contract to gain access to the Prime Infrastructure 1.3 download on Cisco.com.

Appendix B: Changes

This appendix summarizes the changes to this guide since the previous Cisco SBA series.

- We added Cisco Prime Infrastructure to support wireless LAN controller version 7.4.
- We revised the configuration of Cisco CleanAir for APs and WLC to use Cisco Prime Infrastructure 1.3.
- We added deployment details for the installation of a Cisco Mobility Services Engine virtual appliance (MSE VA) version 7.4.
- Historical Cisco CleanAir information is now available through the addition of the Cisco Mobility Services Engine virtual appliance (MSE VA).
- Historical Cisco CleanAir information is now presented through Cisco Prime Infrastructure 1.3.



Feedback

Please use the feedback form to send comments and suggestions about this guide.



cisco.

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.

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, WITH-OUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARSING 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 UT 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 ON OT 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.

© 2013 Cisco Systems, Inc. All rights reserved.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: 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. (1110R)

B-0000350-1 3/13