






Newer Cisco Validated Design Guides Available

This guide is part of an older series of Cisco Validated Designs.

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

-  [Open the latest version of this guide](#)
-  [Access the latest series of CVD Guides](#)
-  [Continue reading this archived version](#)





Campus CleanAir

Technology Design Guide

April 2014



Table of Contents

Preface	1
CVD Navigator	2
Use Cases	2
Scope	2
Proficiency.....	3
Introduction	4
Technology Use Cases	4
Use Case: Proactive Interference Protection by Using Cisco CleanAir.....	4
Use Case: Historical RF Management by Using Cisco CleanAir and Cisco Prime Infrastructure	5
Use Case: CleanAir Spectrum Intelligence using MetaGeek Chanalyzer.....	5
Design Overview.....	5
Cisco CleanAir Technology.....	5
Cisco Prime Infrastructure 1.4.1	6
Deployment Details	7
Adding Buildings and Floor Plans to Cisco Prime Infrastructure	7
Configuring the Wireless Network for Cisco CleanAir.....	13
Installing the Cisco Mobility Services Engine Virtual Appliance	21
Configuring Cisco Prime Infrastructure for the Cisco MSE-VA.....	31
Troubleshooting with Cisco CleanAir	45
Viewing real-time and historical CleanAir using Prime Infrastructure	45
Viewing real-time CleanAir using MetaGeek’s Chanalyzer	49
Appendix A: Product List	66
Appendix B: Changes	69

Preface

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

CVDs include two guide types that provide tested and validated design and deployment details:

- **Technology design guides** provide deployment details, information about validated products and software, and best practices for specific types of technology.
- **Solution design guides** integrate or reference existing CVDs, but also include product features and functionality across Cisco products and may include information about third-party integration.

Both CVD types provide a tested starting point for Cisco partners or customers to begin designing and deploying systems using their own setup and configuration.

How to Read Commands

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

Commands to enter at a CLI appear as follows:

```
configure terminal
```

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

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

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

Commands at a CLI or script prompt appear as follows:

```
Router# enable
```

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

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

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

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

Comments and Questions

If you would like to comment on a guide or ask questions, please use the [feedback form](#).

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

<http://www.cisco.com/go/cvd/campus>

CVD Navigator

The CVD Navigator helps you determine the applicability of this guide by summarizing its key elements: the use cases, the scope or breadth of the technology covered, the proficiency or experience recommended, and CVDs related to this guide. This section is a quick reference only. For more details, see the Introduction.

Use Cases

This guide addresses the following technology use cases:

- **Proactive Interference Protection by Using Cisco CleanAir**—Continuous Wi-Fi spectrum analysis graphically shows the source and location of interference impacting the Wi-Fi network. Advanced real-time spectrum analysis and diagnostic capabilities are available with Cisco CleanAir-enabled access points.
- **Historical RF Management by Using Cisco CleanAir and Cisco Prime Infrastructure**—Graphical floor-plan heat maps depict the location, type, and impact zone of Wi-Fi interference in a historical context.
- **Report Builder using MetaGeek Chanalyzer 5 and Cisco CleanAir**—Create custom reports using collected spectrum intelligence with Cisco CleanAir access points on 2.4GHz and 5GHz bands.
- **802.11ac 80 MHz Channel Spectrum Intelligence**—Using the Cisco Aironet 3700 Series Access Point and MetaGeek Chanalyzer 5 with Cisco CleanAir, visualize interference in 40 MHz-wide or 80 MHz-wide 802.11ac channel(s).

For more information, see the “Use Cases” section in this guide.

Scope

This guide covers the following areas of technology and products:

- Cisco CleanAir for onsite, remote-site, and guest wireless LAN controllers
- Network management using Cisco Prime Infrastructure
- Wi-Fi RF spectrum management using MetaGeek Chanalyzer and Cisco Prime Infrastructure
- Access to historical CleanAir information by using Cisco Mobility Services Engine (MSE)
- Cisco MSE and Prime Infrastructure virtual appliance

For more information, see the “Design Overview” section in this guide.

Related CVD Guides



Campus Wireless LAN
Technology Design Guide



Prime Infrastructure
Technology Design Guide

To view the related CVD guides,
click the titles or visit the following site:
<http://www.cisco.com/go/cvd/campus>

Proficiency

This guide is for people with the following technical proficiencies—or equivalent experience:

- **CCNA Wireless**—1 to 3 years installing, operating, and troubleshooting wireless LANs
- **VCP VMware**—At least 6 months installing, deploying, scaling, and managing VMware vSphere environments

Introduction

Technology Use Cases

Wireless technology impacts our lives each and every day. As a result of the explosive growth of mobile devices, detection and isolation of interference has become a top concern for Wi-Fi network administrators and managed service providers.

As a society, we continue to expect trouble-free wireless access with a performance profile similar to that of our wired network experience. When wireless performance is impacted due to interference, it is usually transitory in nature. Immediate access to IT engineers specializing in wireless technology is often not possible, and by the time the issue is reported, it usually has cleared.

With Cisco CleanAir, spectrum intelligence that was once restricted to specially built and costly troubleshooting hardware is now available in each Cisco CleanAir access point. In fact, not only can real-time spectrum analysis identify and locate the sources of interference, it is automatically recorded to the Mobility Services Engine for later analysis. Remote access to real-time spectrum analysis is now available to the Wi-Fi network administrator without regard to the administrator's physical location.

Cisco CleanAir is not only a passive action in Wi-Fi network management; it can also take action to reduce the effects of interference. As a result of interference events, Event-Driven Radio Resource Management (EDRRM) can react in real time to interference issues that are significantly impairing the wireless user experience. At such times, the Cisco CleanAir events can cause the access points affected to change channels in order to side step the interference. This is analogous to stepping off the train track when you detect an oncoming train. Reducing interference events improves the Wi-Fi experience for wireless users, while at the same time ensures that the Wi-Fi network administrator has a better day.

Use Case: Proactive Interference Protection by Using Cisco CleanAir

Without regard to the location of the Wi-Fi network administrator, advanced spectrum analysis information is available in real-time and on an historical basis. With proactive interference protection, Cisco CleanAir can trigger interference avoidance mechanisms, including channel change and transmit power adjustments.

This design guide enables the following Cisco CleanAir capabilities:

- **Advanced real-time spectrum analysis**—Wi-Fi spectrum analysis allows network administrators to visually see the source and location of interference impacting the Wi-Fi network.
- **Detection and classification**—Wi-Fi interferences are identified by type (Bluetooth, microwave ovens, video cameras, Digital Enhanced Cordless Telecommunications (DECT) phones and many more) and severity.
- **Historical Localization of interference sources**—The location of the source of interference is displayed on a scale floor plan or campus map. This is available to the network administrator in both real-time and historical modes of operation.
- **Air quality index**—Enable constant, proactive monitoring of the RF spectrum and enable the creation of an Air Quality Index for each access point.

Use Case: Historical RF Management by Using Cisco CleanAir and Cisco Prime Infrastructure

Many times interference is transient in nature, affecting us at the most inopportune times. The skilled personnel required to troubleshoot these issues are not always available. The Cisco Mobility Services Engine allows organizations and managed service providers to post event access to RF spectrum information.

This design guide enables the following network capabilities:

- Allowing Wi-Fi network administrators access to historical Cisco CleanAir information for post event troubleshooting
- Configuration and use of the Cisco Mobility Services Engine for CleanAir historical reporting
- Use of Cisco Prime Infrastructure to provide CleanAir reporting information
- Graphical map displaying the location of the interference-generating source by using Cisco Prime Infrastructure
- Display of the size and scope of the area impacted by the interference
- Classification of the interference types for each event

Use Case: CleanAir Spectrum Intelligence using MetaGeek Chanalyzer

Real-time spectrum intelligence is sometimes necessary to diagnose the type and location of interference impacting the wireless network. In many industries such as healthcare and manufacturing, effective spectrum management is an ongoing requirement to ensure proper and safe operation of the numerous devices connected via Wi-Fi.

This design guide provides two methods of extracting the most from the Cisco CleanAir enabled Wi-Fi network. With the inclusion of MetaGeek Chanalyzer software, the network administrator can obtain in depth real-time Cisco CleanAir spectrum intelligence.

This design guide enables the following Spectrum Intelligence capabilities:

- Configuration and installation of MetaGeek Chanalyzer software
- Enable Spectrum Expert Connect (SE-Connect) mode on Cisco CleanAir access points
- Guidance for the use of both products in obtaining CleanAir Spectrum Intelligence directly from CleanAir Access points
- Troubleshooting guidance using MetaGeek Chanalyzer software
- Usage of the advanced visualization and operation capabilities of MetaGeek's Chanalyzer software
- Creation of custom reports using the MetaGeek Chanalyzer software.

Design Overview

Cisco CleanAir Technology

Cisco CleanAir technology is the integration of real-time and historical RF Spectrum Intelligence obtained directly from Cisco CleanAir 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. Cisco CleanAir automates these tasks by adding additional intelligence over standalone spectrum analyzers. 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 constant 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 Series 2600, 3600 or 3700 Series access points. To take advantage of the entire set of CleanAir features, Cisco Prime Infrastructure 1.4.1 can display in real-time the data retrieved from CleanAir. The Cisco 3500 and 1550 series access points are also capable of providing CleanAir spectrum intelligence but are not covered in this guide.

Cisco Prime Infrastructure 1.4.1 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 1.4.1 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 the Cisco Mobility Services Engine Virtual Appliance (MSE-VA) included in the solution, the administrator can turn back the clock and look at RF issues that occurred in the past. This is typically the case due to end users delaying the reporting of such issues and first-level support working the problem before turning it over to second and third level support.

Cisco Prime Infrastructure 1.4.1

Cisco Prime Infrastructure enables you to configure and monitor one or more Cisco wireless LAN controllers and associated access points, monitor, troubleshoot and manage the RF spectrum, then visually display Cisco CleanAir data to the network administrator. Cisco Prime Infrastructure 1.4.1 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 1.4.1 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

In order to use Cisco Prime Infrastructure to manage the Cisco wireless LAN controller that are running Cisco AireOS version 7.6, you must use version 1.4.1 of Cisco Prime Infrastructure. The procedures for properly installing and configuring Prime Infrastructure 1.4.1 have been provided in the [Prime Infrastructure Technology Design Guide](#) available at <http://cisco.com/go/cvd/campus> .

This guide assumes that you have completed all of the steps in the [Prime Infrastructure Technology Design Guide](#) prior to completing this guide.

PROCESS

Adding Buildings and Floor Plans to Cisco Prime Infrastructure

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 1.4.1 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 1.4.1, visibility of this otherwise unknown or convoluted data that Prime Infrastructure 1.4.1 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

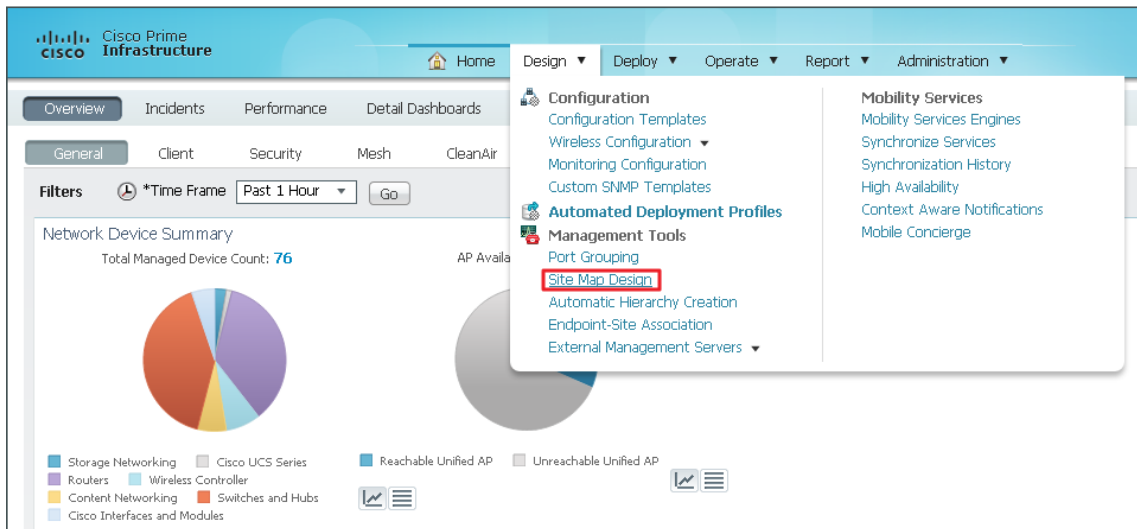
Even though your organization may have only one building today, it may end up with another building; or perhaps each campus is a single building today, but it could have more buildings in the future. The campus, building, floor approach makes it easy to understand and organize as you dig for more information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



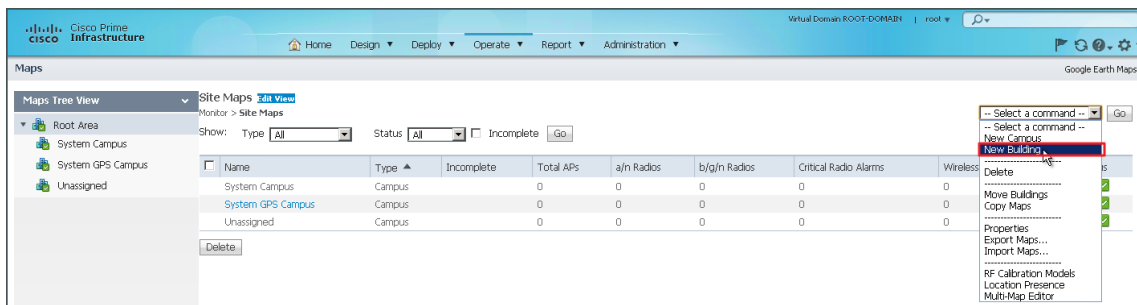
Tech Tip

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. Counting ceiling tiles or floor tiles is a good method to use if dimensions are not available via building blue prints.

Step 1: In Cisco Prime Infrastructure 1.4.1, navigate to **Design > Management Tools > Site Map Design**.



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



Step 3: Enter the following information about the building:

- Building Name—**Headquarters**
- Contact—**Networking Team**
- Number of floors—**1**
- Number of Basements—**0**
- Horizontal Span (feet)—**525**
- Vertical Span (feet)—**325**
- Address—**500 Main Street**
- 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.

Virtual Domain ROOT-DOMAIN | root

Home Design Deploy Operate Report Administration

Maps Google Earth Maps

Edit Building
Monitor > Site Maps > Headquarters

Building Name: Headquarters
 Contact: Networking Team
 Number of Floors: 1
 Number of Basements: 0
 Dimensions (feet): Horizontal Span: 525.0, Vertical Span: 325.0
 Address: 500 Main Street
 Latitude: 37.418717
 Longitude: -121.919382

OK Cancel

Step 4: Click the name of the newly created building. This selects the building.

Virtual Domain ROOT-DOMAIN | root

Home Design Deploy Operate Report Administration

Maps Google Earth Maps

Maps Tree View Site Maps Add View
Monitor > Site Maps

Show: Type All Status All Incomplete Go

Name	Type	Incomplete	Total APs	a/n Radios	b/g/n Radios	Critical Radio Alarms	Wireless Clients	Status
System Campus	Campus	0	0	0	0	0	0	✓
System GPS Campus	Campus	0	0	0	0	0	0	✓
Unassigned	Campus	0	0	0	0	0	0	✓
System Campus > Headquarters	Building	0	0	0	0	0	0	✓

Delete

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

Virtual Domain ROOT-DOMAIN

Home Design Deploy Operate Report Administration

Maps Tree View Building View
Monitor > Site Maps > System Campus > Headquarters

None detected

-- Select a command -- Go

- Select a command --
- New Floor Area
- Edit Building
- Delete Building
- Copy Building ...
- Configure Interferer Notifications

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

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

The screenshot shows the 'New Floor Area' configuration page in Cisco Prime Infrastructure. The breadcrumb trail is 'Monitor > Site Maps > System Campus > Headquarters > New Floor Area'. The form contains the following fields and values:

Floor Area Name	First Floor
Contact	Networking Team
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

Buttons: Next, Cancel, No file chosen

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

The screenshot shows the 'New Floor Area' configuration page after a file has been selected. The breadcrumb trail is 'Monitor > Site Maps > System Campus > Headquarters > New Floor Area'. The form contains the following fields and values:

Floor Area Name	First Floor
Contact	Networking Team
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 SJC23-AFP-1.png
Convert CAD File to	PNG

Buttons: Next, Cancel

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**.

The screenshot shows the Cisco Prime Infrastructure web interface. The top navigation bar includes 'Home', 'Design', 'Deploy', 'Operate', 'Report', and 'Administration'. The main content area is titled 'New Floor Area' and contains the following fields:

- Floor Area Name: First Floor
- Contact: Networking Team
- 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): Horizontal Span: 407.7, Vertical Span: 306.2
- Coordinates of top left corner (feet): Horizontal Position: 0, Vertical Position: 0

Below the form, there is a checkbox for 'Launch Map Editor after floor creation (To rescale floor and draw walls)' and two buttons: 'OK' (highlighted with a red box) and 'Cancel'. A note below the buttons reads: 'Use mouse to position the floor image by dragging it. And use CTRL key with mouse to resize the floor.'

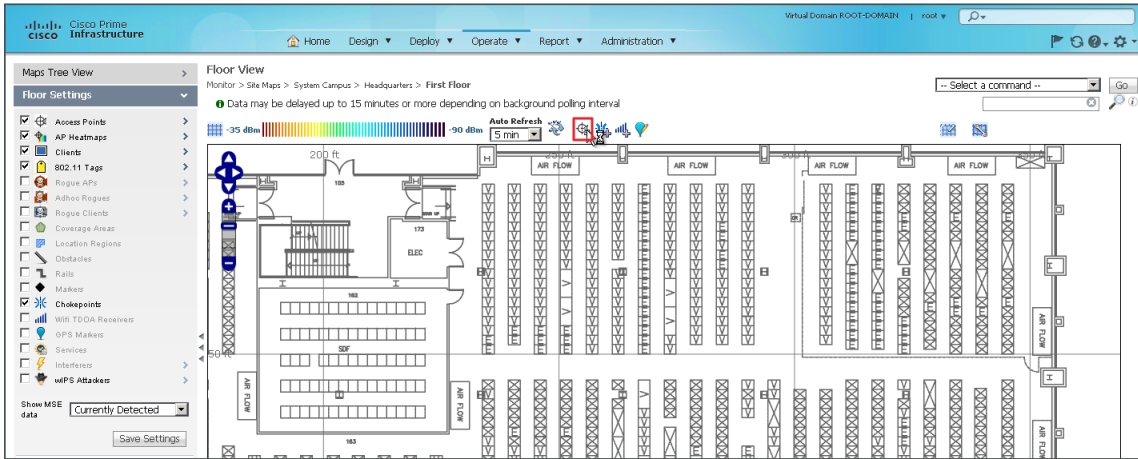
The bottom part of the screenshot shows a map with a grid. The horizontal axis is labeled '0 feet', '100', '200', '300', '400', '500'. The vertical axis is labeled '0', '100', '200'. A floor plan image is overlaid on the grid, with its top-left corner at the 0,0 coordinate.

Procedure 2 Place access points on the map

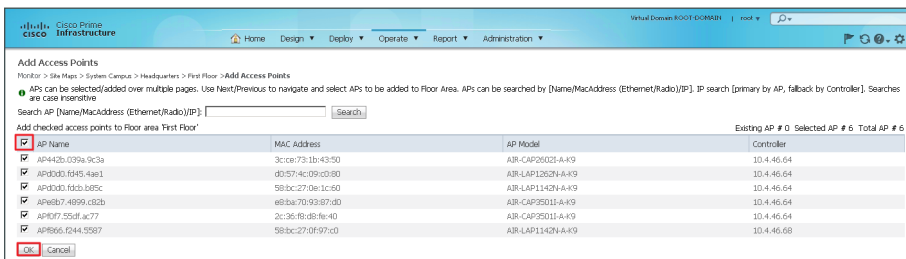
The final piece of the puzzle is to place the access points at the proper locations on your individual floor plans. If you take the time to place your access points where they are actually located, the wireless LAN controllers work in conjunction with Cisco Prime Infrastructure 1.4.1 and will give an accurate view of locations of interference.

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.

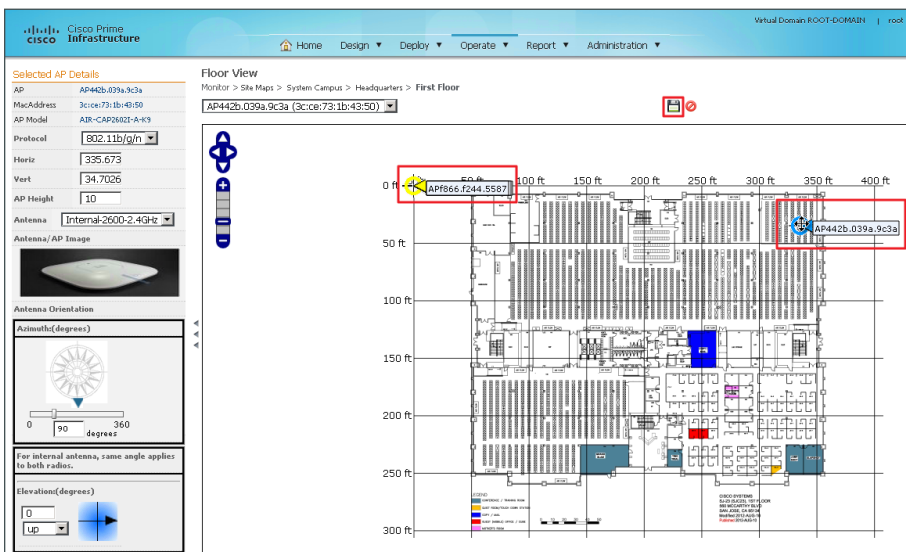
Step 2: Select the Add Access Point crosshairs button.



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



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.

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, 3600, or 3700 series access points has Cisco CleanAir capabilities. By accessing the web interface on the wireless LAN controllers, current information about your RF environment can be obtained. When using Cisco Prime Infrastructure, a complete network view across multiple wireless LAN controllers can be displayed. When viewing CleanAir information on the Wireless LAN Controller directly, only locally obtained CleanAir information from registered access points is displayed.

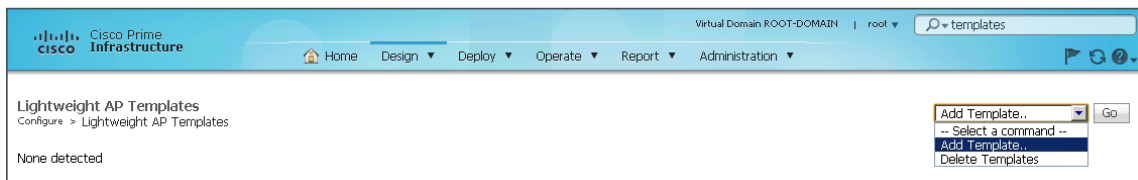
Cisco Prime Infrastructure 1.4.1 can handle all management tasks within the network. You can still perform management tasks at each individual controller, but that approach is not recommended, as it often results in a fragmented configuration. With the Cisco CleanAir access point operating from the wireless LAN controller, you can log in to Cisco Prime Infrastructure 1.4.1 and configure your controller to support CleanAir.

Procedure 1 Create a Cisco CleanAir AP template

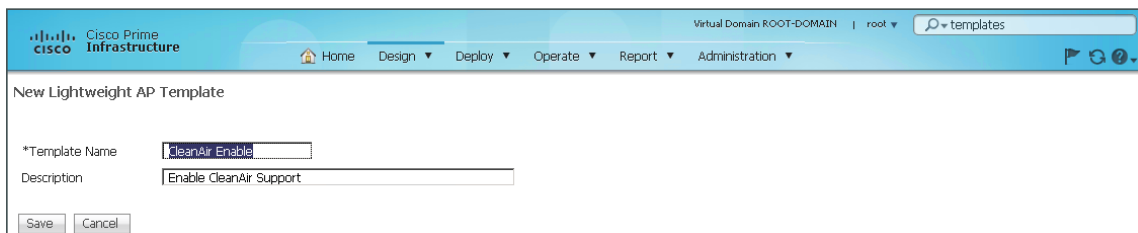
The first step in order to turn on Cisco CleanAir is to ensure that Cisco CleanAir is enabled on each of the access points (APs) for both 2.4 and 5 GHz bands. The following steps outline how to create a template within Cisco Prime Infrastructure 1.4.1 to enable CleanAir on an AP.

Step 1: In Cisco Prime Infrastructure 1.4.1, navigate to **Design > Configuration > Wireless Configuration > Lightweight AP Configuration Templates**.

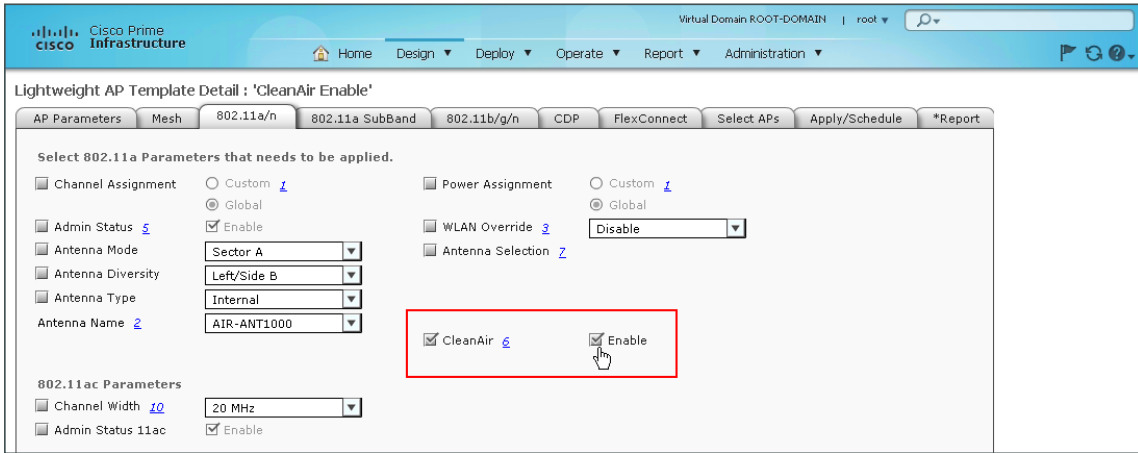
Step 2: In the **Select a command** list, choose **Add Template**, and then click **Go**.



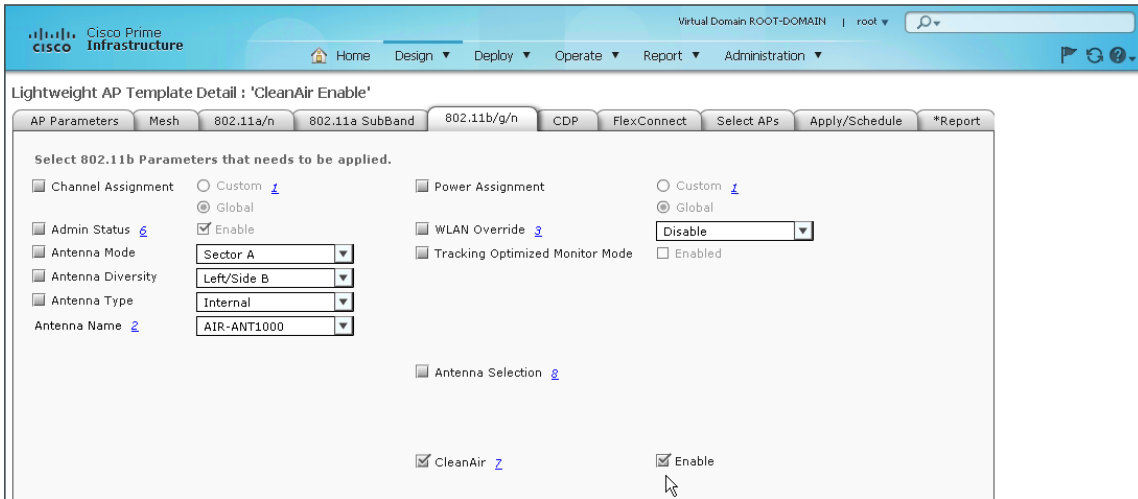
Step 3: In the **Template Name** box, enter a name, in the **Description** box, enter a description, and then click **Save**.



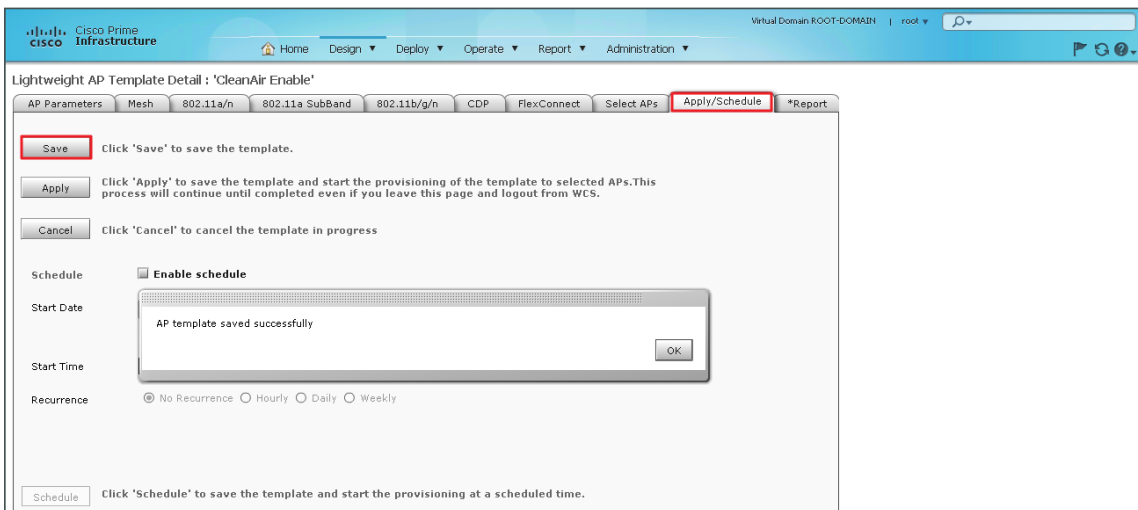
Step 4: On the 802.11a/n tab, ensure that both **CleanAir** and **Enable** are selected.



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



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



Procedure 2 Apply the Cisco CleanAir AP template

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

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.

Lightweight 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

Search APs

AP Name	Ethernet MAC	Controller	Map
<input type="checkbox"/> AP0d0.f45.4ae1	d0:d0:fd:45:4a:e1	10.4.46.64	
<input type="checkbox"/> RS201-LAP1142N	f8:66:f2:44:55:87	10.4.46.68	
<input type="checkbox"/> APe8b7.4899.c82b	e8:b7:48:99:c8:2b	10.4.46.64	
<input checked="" type="checkbox"/> AP442b.039a.9c3a	44:2b:03:9a:9c:3a	10.4.46.64	
<input type="checkbox"/> 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.

Lightweight 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

Click 'Save' to save the template.

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.

Click 'Cancel' to cancel the template in progress

Schedule **Enable schedule**

Start Date (Current server time: 11/09/2012 08:02:19)

Start Time Hr Min

Recurrence No Recurrence Hourly Daily Weekly

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

Lightweight 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**

Apply Status: **Completed**

Applied On: **11/9/12 9:14 AM**

AP Name	Status	Ethernet MAC	Controller	Map
AP442b.039a.9c3a	Success	44:2b:03:9a:9c:3a	10.4.46.64	

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

- In Cisco Prime Infrastructure 1.4.1, the SNMP Read/Write Community string for the WLC is correct.
- In Cisco Prime Infrastructure 1.4.1, 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 classified interference devices. That makes AQ a reliable metric in that you know 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 reaction time (30 seconds). If an interferer is operating on an active channel and is causing enough AQ degradation to trigger EDRRM, clients cannot use the degraded access point or channel. To recover from degraded service, the access point must select an alternative operational 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 1.4.1, 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**.

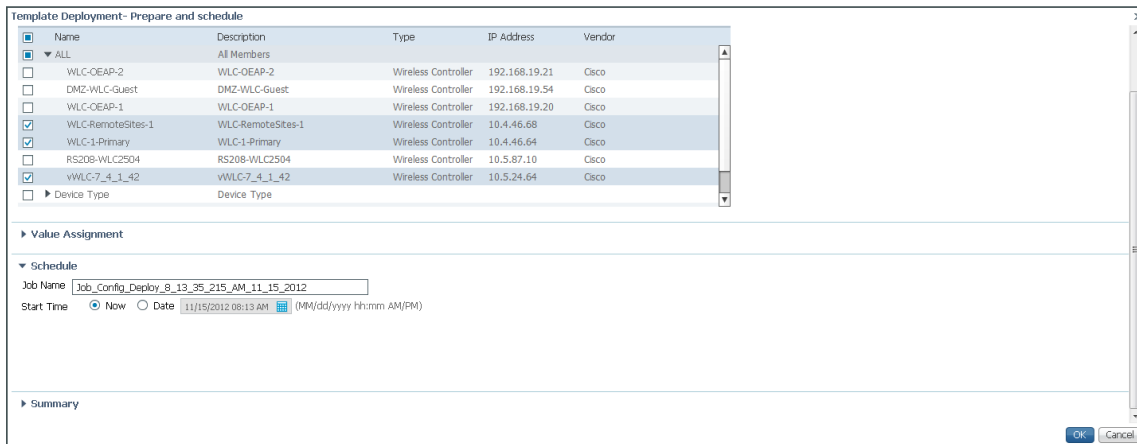
The screenshot shows the Cisco Prime Infrastructure Configuration Templates interface. The left sidebar displays a tree view of templates, with the path **802.11a or n > dot11a-RRM > DCA** selected. The main content area shows the configuration for the **DCA** template. The **Template Basic** section includes fields for ***Name** (Enable 802-11an EDRRM), **Description** (Enable 802-11an EDRRM), **Author** (root), and **Feature Category** (DCA). The **Validation Criteria** section shows ***Device Type** set to **Wireless Controller** and **OS Version** as an empty field. The **Template Detail** section is expanded to show the **New Controller Template** configuration. Under **Dynamic Channel Assignment Algorithm**, the **Assignment Mode** is set to **Automatic**. Several interference avoidance options are listed with checkboxes: **Avoid Foreign AP Interference**, **Avoid Cisco AP load**, **Avoid non 802.11 Noise**, and **Avoid Persistent Non-WiFi Interference** are all disabled, while **Signal Strength Contribution** is enabled. The **Channel Width** is set to **20 MHz**. Under **Event Driven RRM**, **Event Driven RRM** is checked and **Sensitivity Threshold** is set to **Medium**. A **Footnotes** section at the bottom contains the note: "1. Event Driven RRM fields are supported for controller version 7.0.x.x onwards." Buttons for **Save as New Template** and **Cancel** are visible at the bottom.

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.

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**.

i Tech Tip

The deployment of the template may fail if the 802.11a network is enabled on the controller. If this occurs, disable the interface and redeploy the template.



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

i Tech Tip

If the 802.11b/g/n network is enabled on the controller, the deployment of the template may fail. If this occurs, disable the interface and redeploy the template.

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 1.4.1, 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, and 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**.

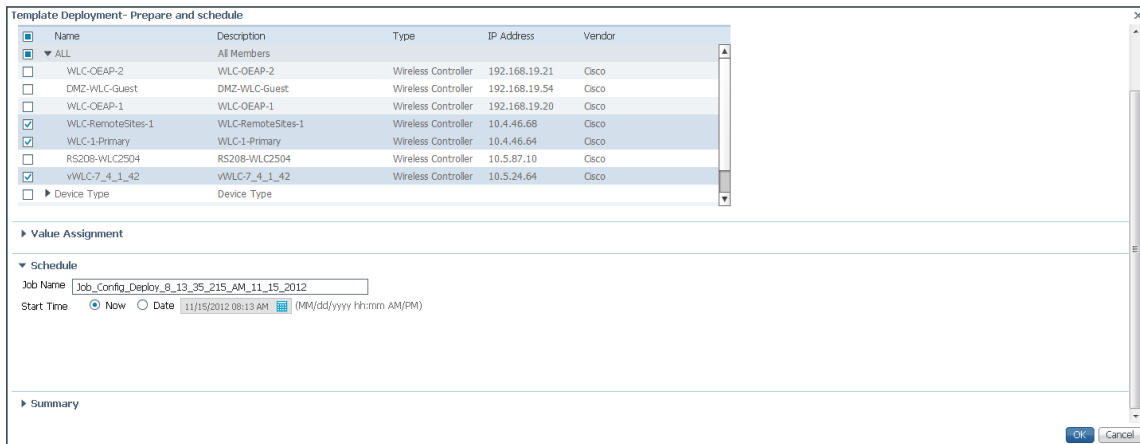
The screenshot shows the Cisco Prime Infrastructure Configuration Templates page. The left sidebar shows a tree view of templates, with 'CleanAir' selected under '802.11a or n'. The main content area is titled 'CleanAir' and shows the following configuration details:

- Template Basic:** *Name: CleanAir 802-11a, Description: CleanAir 802-11a, Author: root, Feature Category: CleanAir.
- Validation Criteria:** *Device Type: Wireless Controller, OS Version: (empty).
- Template Detail:** CleanAir Enable.
- Reporting Configuration:** Report Interferers Enable.
 - Interferers Ignored for Reporting:** Canopy, SuperAG, TDD Transmitter, WiFi Invalid Channel, WiFi Inverted, WIMAX Fixed, WIMAX Mobile.
 - Interferers Selected for Reporting:** Continuous Transmitter, DECT-Like Phone, Jammer, Video Camera.
- Alarm Configuration:** Air Quality Alarm Enable, Air Quality Unclassified category Alarm Enable, Interferers For Security Alarm Enable.
 - Interferers Ignored for Security Alarms:** Canopy, SuperAG, TDD Transmitter, WiFi Invalid Channel, WiFi Inverted, WIMAX Fixed, WIMAX Mobile.
 - Interferers Selected for Security Alarms:** Continuous Transmitter, DECT-Like Phone, Jammer, Video Camera.

At the bottom, there are buttons for 'Save as New Template' and 'Cancel'.

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

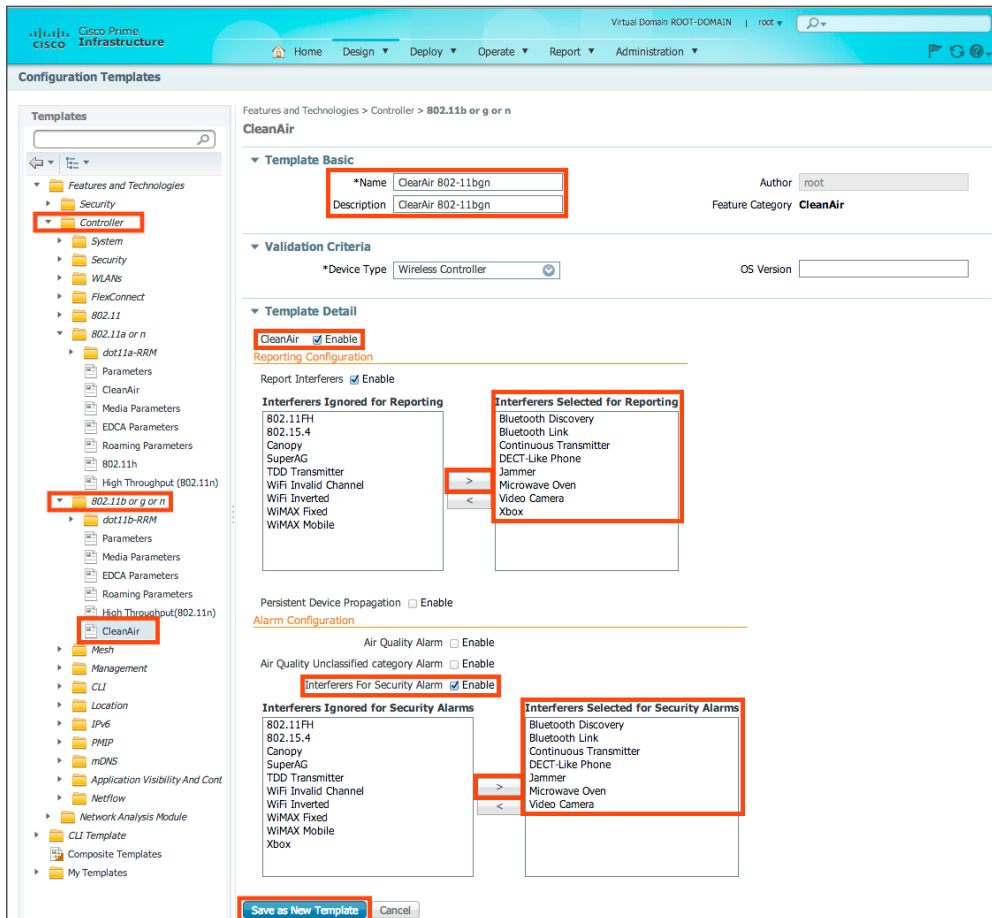
Step 4: After saving, at the bottom of the screen, click **Deploy**, select each of the wireless LAN controllers to apply the template to, and then click **OK**.



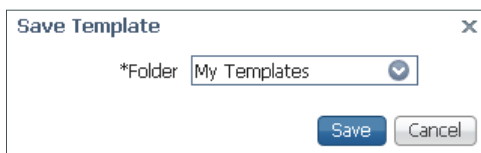
Step 5: In Cisco Prime Infrastructure 1.4.1, navigate to **Design > Configuration Template > Feature and Technology > Controller > 802.11b or g or n > CleanAir**.

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**.



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



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**.

Installing the Cisco Mobility Services Engine Virtual Appliance

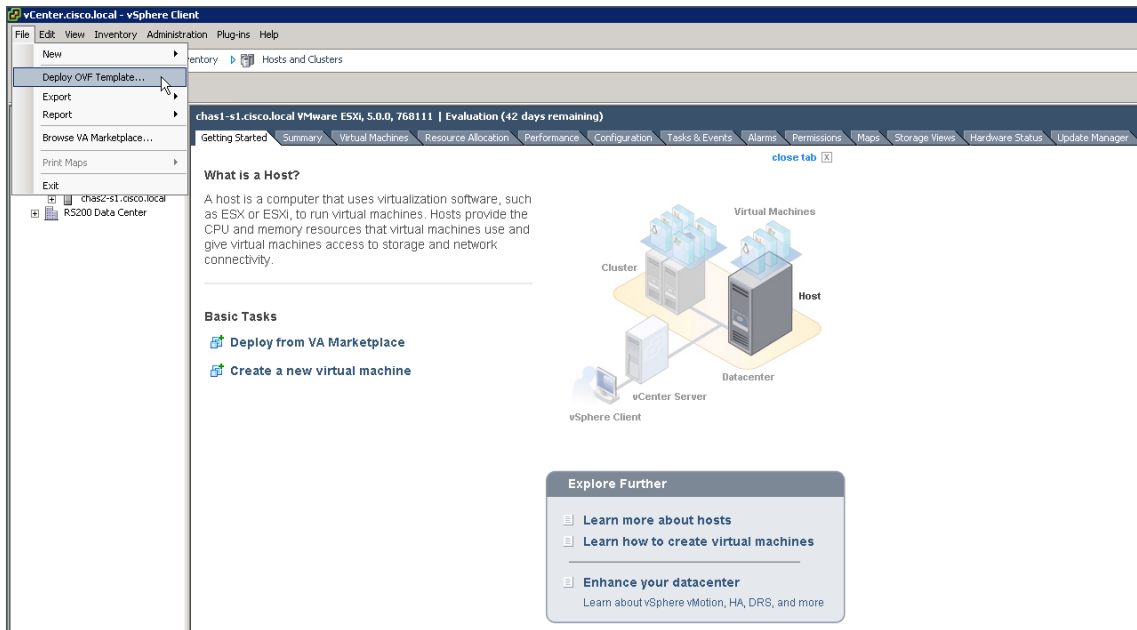
1. Install the Cisco MSE virtual appliance
2. Start the Cisco MSE virtual appliance
3. Configure the Cisco MSE virtual appliance
4. Verify installation of MSE virtual appliance

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 many more services such as the Cisco Mobile Experience (CMX), the use of the Cisco MSE-VA in this design 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.

Procedure 1 Install the Cisco MSE virtual appliance

Step 1: Using 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 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**.

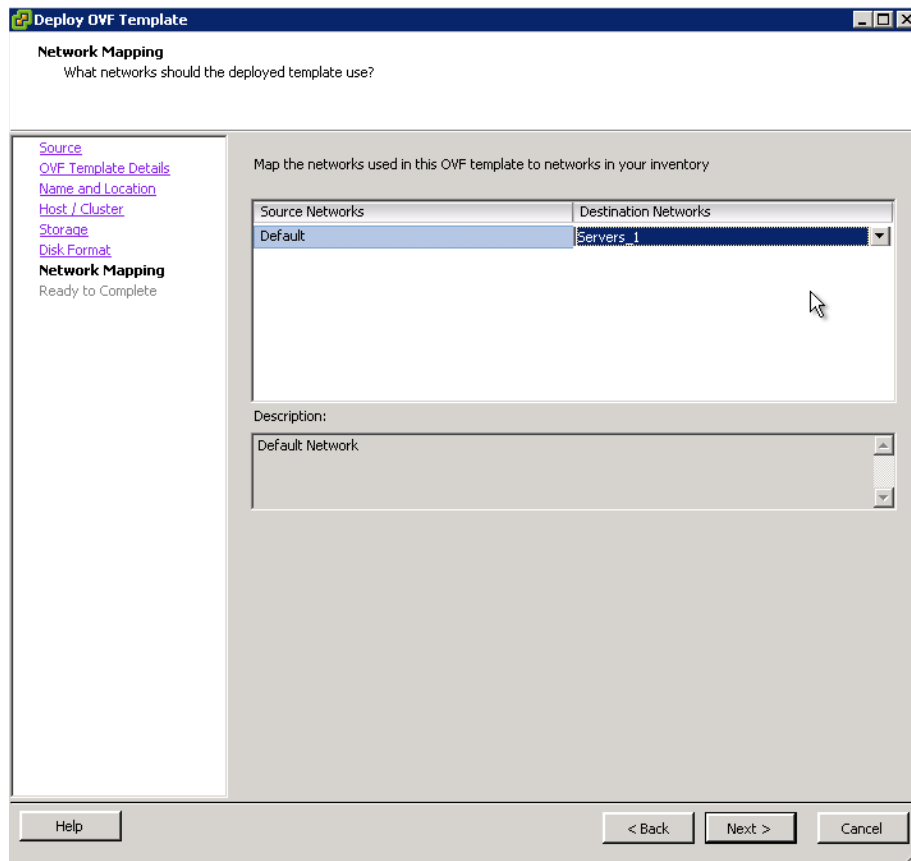
Step 4: On the Name and Location page, enter a unique and descriptive name for the virtual appliance that you are installing (Example: vMSE-VA), choose a location to install the virtual appliance, and then click **Next**.

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**.



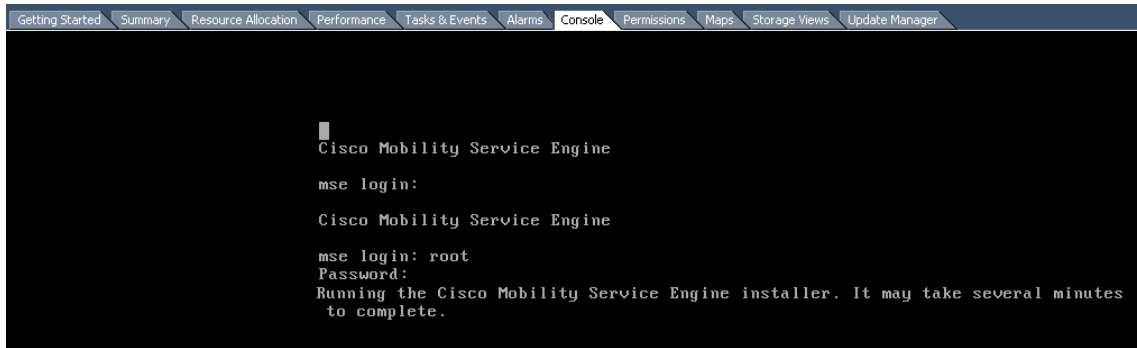
Step 9: On the Ready to Complete page, review the selected options, and then click **Finish**. The OVF installation begins.

Procedure 2 Start the Cisco MSE virtual appliance

Next, install the Cisco Mobility Services Engine Virtual Appliance software on the new virtual machine.

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

Step 2: 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.



```
Getting Started Summary Resource Allocation Performance Tasks & Events Alarms Console Permissions Maps Storage Views Update Manager

Cisco Mobility Service Engine
mse login:
Cisco Mobility Service Engine
mse login: root
Password:
Running the Cisco Mobility Service Engine installer. It may take several minutes
to complete.
```



Tech Tip

The installation process can take 45 minutes or more to complete. 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 then press **<Enter>**.

Step 3: At the prompt to setup parameters in the Setup Wizard, enter **YES**, and then press **Enter**.

```
Setup parameters via Setup Wizard (yes/no) [yes]: YES
-----
Welcome to the Cisco Mobility Services Engine appliance setup.
You may exit the setup at any time by typing <Ctrl+C>.
-----
Would you like to configure MSE using menu options (yes/no): No
```

Step 4: 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
```

Step 5: 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 6: 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 7: Type **Y** for Yes, and then configure the eth0 interface parameters.

```
Current IP address=[1.1.1.10]  
Current eth0 netmask=[255.255.255.0]  
Current gateway address=[1.1.1.1]  
Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Yes]: Yes
```

Enter an IP address for first ethernet interface of this machine.

Enter eth0 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]: **255.255.255.0**

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 8: 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 9: 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 10: 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              |
| 4) Aruba               | 30) Mexico                  |
| 5) Bahamas             | 31) Montserrat              |
| 6) Barbados            | 32) Netherlands Antilles    |
| 7) Belize              | 33) Nicaragua               |
| 8) Bolivia             | 34) Panama                  |
| 9) Brazil              | 35) Paraguay                |
| 10) Canada             | 36) Peru                    |
| 11) Cayman Islands     | 37) Puerto Rico             |
| 12) Chile              | 38) St Barthelemy           |
| 13) Colombia           | 39) St Kitts & Nevis        |
| 14) Costa Rica         | 40) St Lucia                |
| 15) Cuba               | 41) St Martin (French part) |
| 16) Dominica           | 42) St Pierre & Miquelon    |
| 17) Dominican Republic | 43) St Vincent              |
| 18) Ecuador            | 44) Suriname                |
| 19) El Salvador        | 45) Trinidad and Tobago     |
| 20) French Guiana      | 46) Turks & Caicos Is       |
| 21) Greenland          | <b>47) United States</b>    |
| 22) Grenada            | 48) Uruguay                 |
| 23) Guadeloupe         | 49) Venezuela               |
| 24) Guatemala          | 50) Virgin Islands (UK)     |
| 25) Guyana             | 51) Virgin Islands (US)     |
| 26) Haiti              |                             |
- ```
#? 47 <ENTER>
```

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

```

<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) Yes
2) No
#? 1 <ENTER>

```

Step 11: 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 12: 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.

```
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) LOCAL0 (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 13: Type **S** for Skip. This skips the next step, which is used for modifying the iptables for the 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 14: 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 15: 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/(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 16: 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 17: 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 : **99999**

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, the GRUB password must be entered. If the password is lost or forgotten, the virtual appliance cannot be booted. Configuring a GRUB password should be done with consideration and documented accordingly in your organization's operations manual.

Step 18: Select **Yes**, and configure the Cisco Prime Network Control System (NCS) communications username.

```
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: C1scO!349@
```

```
Confirm NCS communication password : C1scO!349@
```

Step 19: Confirm and approve the settings obtained through the Setup Wizard.

```
-----BEGIN-----
```

```
Host name=vMSE-VA
```

```
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>
```

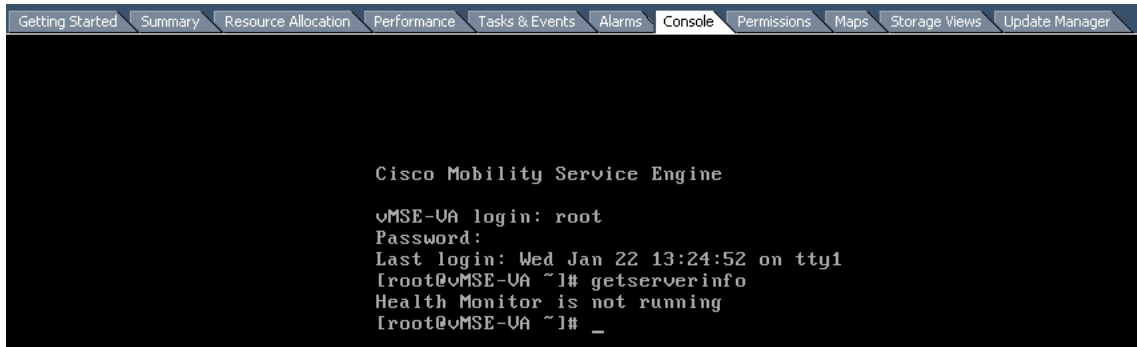

Procedure 4 Verify installation of MSE virtual appliance

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 16 (Example: Hgt50N3181.5n2B).

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



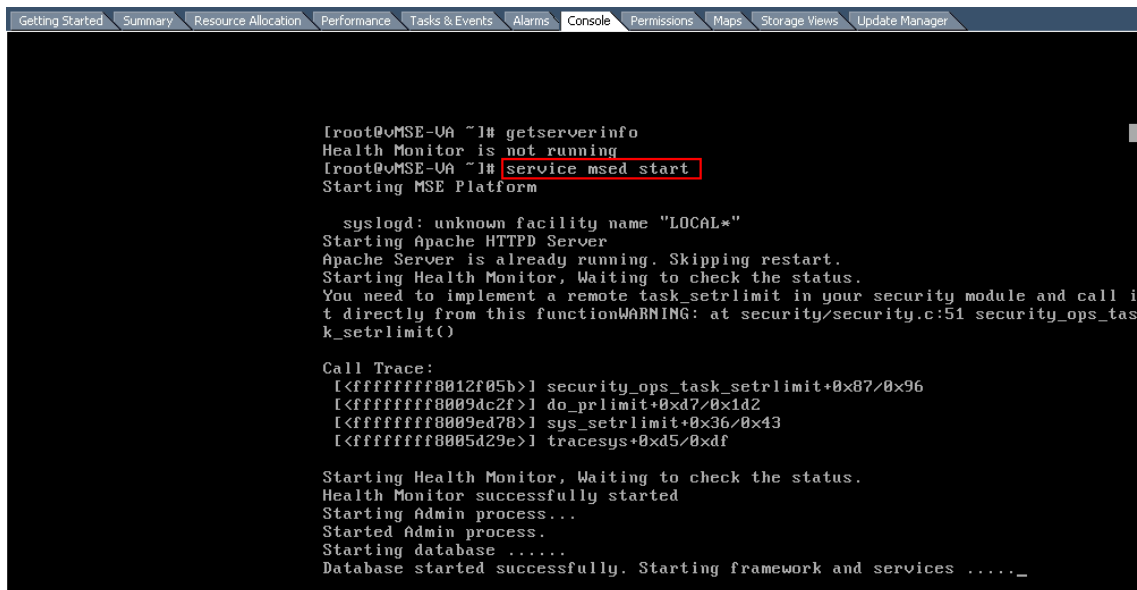
```
Getting Started Summary Resource Allocation Performance Tasks & Events Alarms Console Permissions Maps Storage Views Update Manager

Cisco Mobility Service Engine

VMSE-UA login: root
Password:
Last login: Wed Jan 22 13:24:52 on tty1
[root@VMSE-UA ~]# getserverinfo
Health Monitor is not running
[root@VMSE-UA ~]# _
```

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.



```
Getting Started Summary Resource Allocation Performance Tasks & Events Alarms Console Permissions Maps Storage Views Update Manager

[root@VMSE-UA ~]# getserverinfo
Health Monitor is not running
[root@VMSE-UA ~]# service msed start
Starting MSE Platform

syslogd: unknown facility name "LOCAL*"
Starting Apache HTTPD Server
Apache Server is already running. Skipping restart.
Starting Health Monitor, Waiting to check the status.
You need to implement a remote task_setrlimit in your security module and call it directly from this functionWARNING: at security/security.c:51 security_ops_task_setrlimit()

Call Trace:
[<ffffffff8012f05b>] security_ops_task_setrlimit+0x87/0x96
[<ffffffff8009dc2f>] do_prlimit+0xd7/0x1d2
[<ffffffff8009ed78>] sys_setrlimit+0x36/0x43
[<ffffffff8005d29e>] tracesys+0xd5/0xdf

Starting Health Monitor, Waiting to check the status.
Health Monitor successfully started
Starting Admin process...
Started Admin process...
Starting database .....
Database started successfully. Starting framework and services ....._
```

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

Configuring Cisco Prime Infrastructure for the Cisco MSE-VA

1. Log in to Cisco Prime Infrastructure
2. Add a user ID for the Cisco MSE-VA
3. Add the Cisco MSE-VA to Prime Infrastructure
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 must be configured with the relevant Cisco MSE-VA information. This configuration allows Prime Infrastructure communicate with the MSE-VA server.



Tech Tip

Cisco Prime Infrastructure 1.4.1 supports the following browsers:

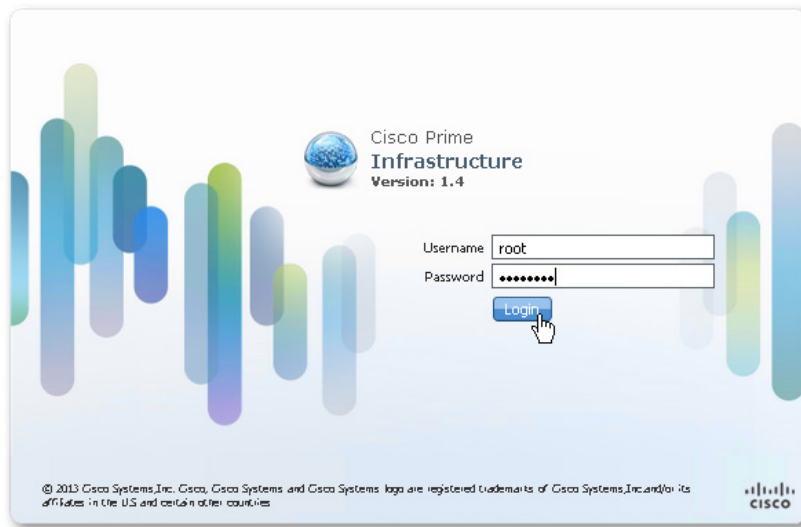
- Google Chrome—25.0, 26.0 or 27.0
- Mozilla Firefox— ESR 17.x, 17.0 or later
- Microsoft Internet Explorer 8.0 or 9.0 with Chrome plug-in.
(Native Internet Explorer is not supported.)

The recommended minimum resolution for each browser is 1280x800 pixels.

Procedure 1 Log in to Cisco Prime Infrastructure

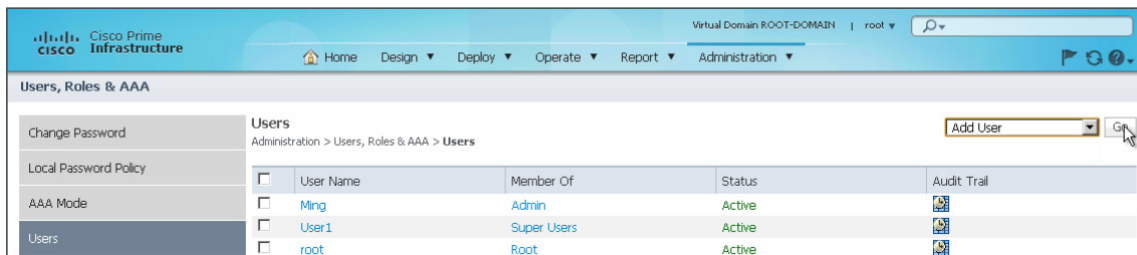
Step 1: Using a supported browser, access the Cisco Prime Infrastructure management interface (Example: <https://prime-infra.cisco.local> or 10.4.48.35).

Step 2: Log on using the configured Cisco Prime Infrastructure user ID and password (Example: root/1Qazxsw2).



Procedure 2 Add a user ID for the Cisco MSE-VA

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

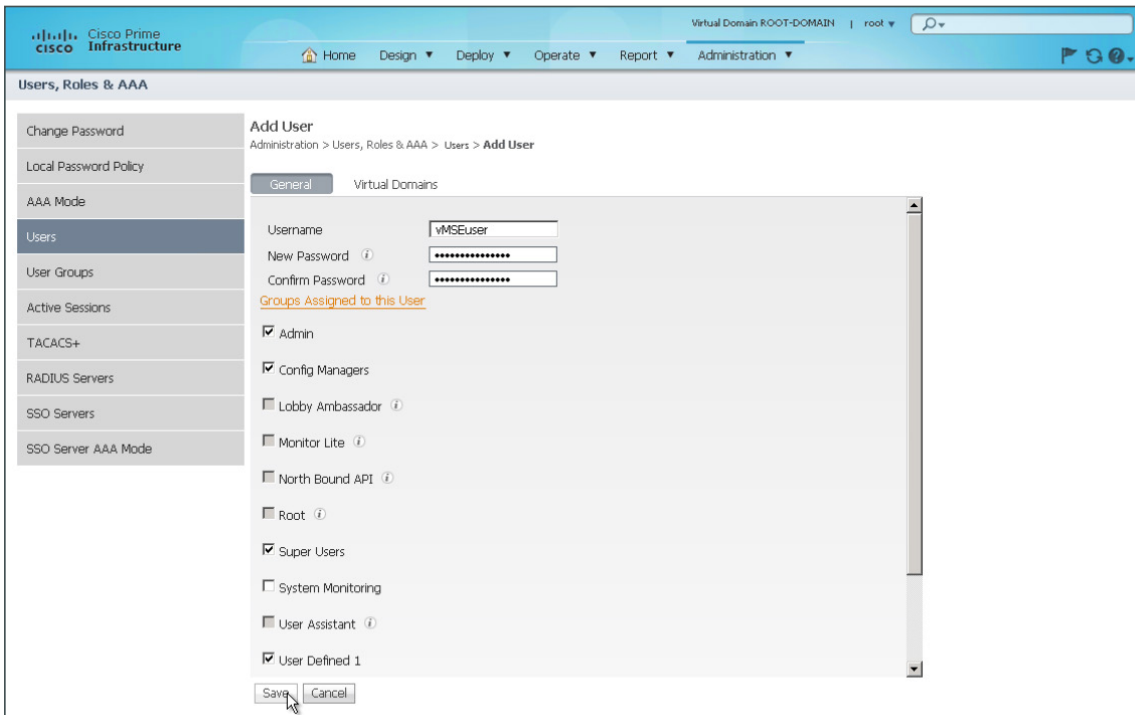


Step 2: Enter the username (Example: vMSEuser) and password (Example: C1scO!349@) that you configured in Step 18 of Procedure 3, “Configure the Cisco MSE virtual appliance.”

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

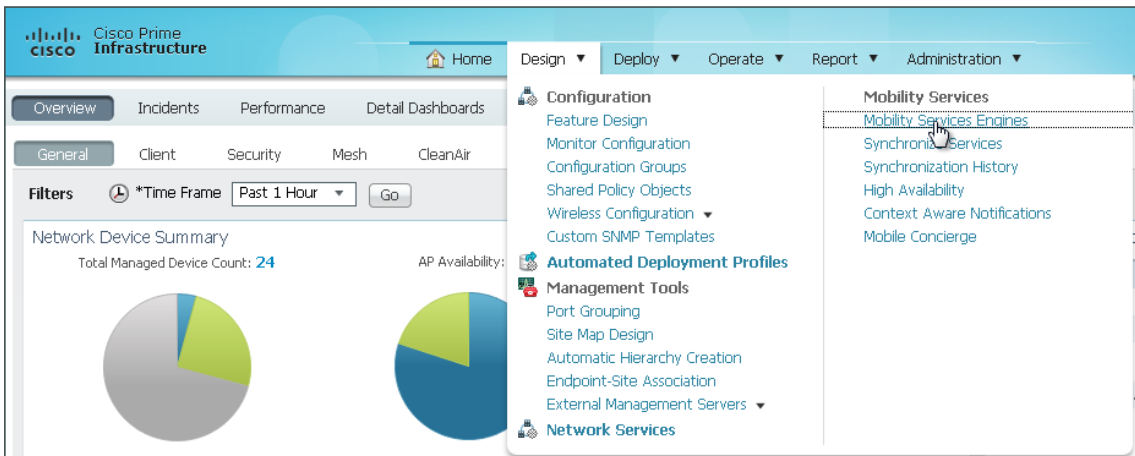
i Tech Tip

It may be necessary to modify the password policy in Cisco Prime Infrastructure 1.4.1 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.

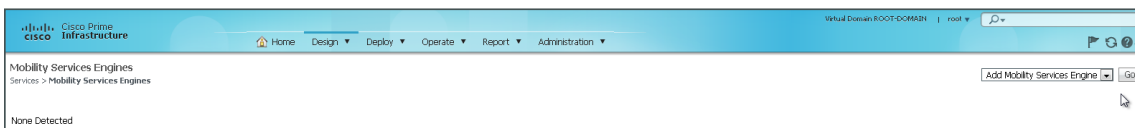


Procedure 3 Add the Cisco MSE-VA to Prime Infrastructure

Step 1: Navigate to Design > Mobility Services Engines.



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



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

- Device Name—**vMSE-VA**
- IP Address—**10.4.48.40**
- Contact Name—**Networking Team**
- Username—**admin** (do not change this)
- Password—(do not change the auto-filled value)

Add Mobility Services Engine

Device Name:

IP Address:

Contact Name:

Username:

Password:

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

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

! Starting version 7.2.x of the MSE, Virtual IP (VIP) address support has been added for High Availability. If you wish to use High Availability and have configured a VIP, add the MSE using the VIP and not the health monitor 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**.

MSE License Summary

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

Service	Platform Limit by AP	Type	Installed Limit by AP	License Type
vMSE-VA Not Activated (AIR-MSE-VA-K9:V01:vMSE-VA.cisco.local_4682359c-83ac-11e3-aaad-005056a27888)				
CAS	200	CAS Elements	100	Evaluation (120 days left)
wIPS	2000	wIPS Monitor Mode APs	10	Evaluation (120 days left)
		wIPS Local Mode APs	10	Evaluation (120 days left)
MC	200	Mobile Concierge	10	Evaluation (120 days left)
ANA	200	Location Analytics	10	Evaluation (120 days left)

[Add License](#) [Remove License](#)

[Back](#) [Next](#)

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**.

The screenshot shows the 'MSE License Summary' page in Cisco Prime Infrastructure. A modal dialog titled 'Add A License File' is open, displaying the MSE Name: **vmse-va(AIR-MSE-VA-K9:V01:vmse-va.cisco.local_4682359c-83ac-11e3-aaad-005056a27888)** and the License File: **Choose File** No file chosen. The dialog has 'OK' and 'Cancel' buttons. In the background, a table lists license details:

Service	Platform Limit by AP	Type	Installed Limit by AP	License Type
vmse-va Not Activated (AIR-MSE-VA-K9:V01:vmse-va.cisco.local_4682359c-83ac-11e3-aaad-005056a27888)				
CAS	200	CAS Elements	100	Evaluation (120 days left)
wIPS	2000	wIPS Monitor Mode APs	10	Evaluation (120 days left)
		wIPS Local Mode APs	10	Evaluation (120 days left)
MC	200	Mobile Concierge	10	Evaluation (120 days left)
ANA	200	Location Analytics	10	Evaluation (120 days left)

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

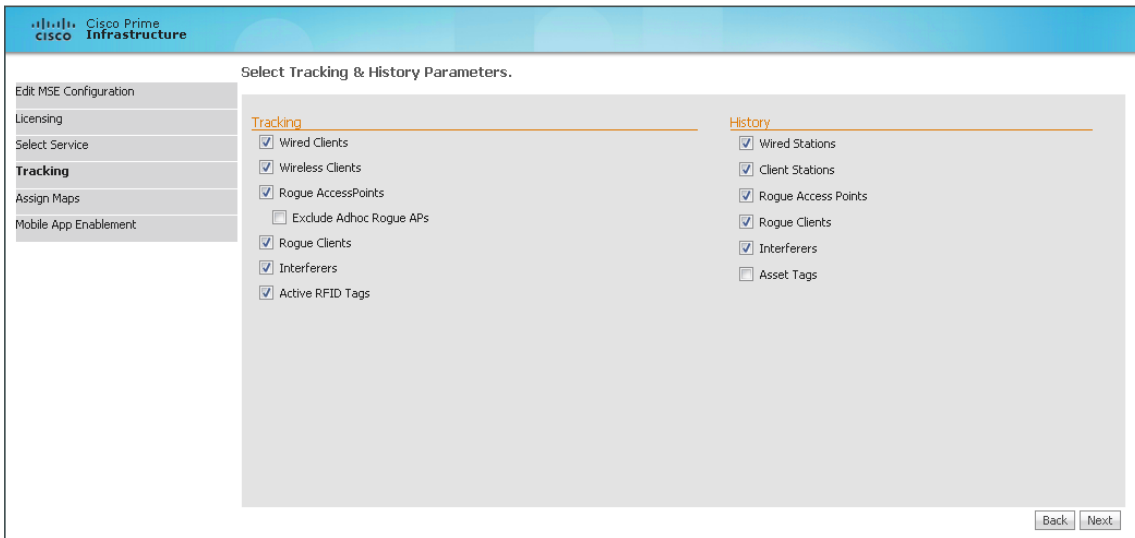
The screenshot shows the 'Select Mobility Service' page in Cisco Prime Infrastructure. The page lists several services with checkboxes:

- Context Aware Service
- WIPS
- Mobile Concierge Service
- CMX Analytics
- CMX Browser Engage
- HTTP Proxy Service

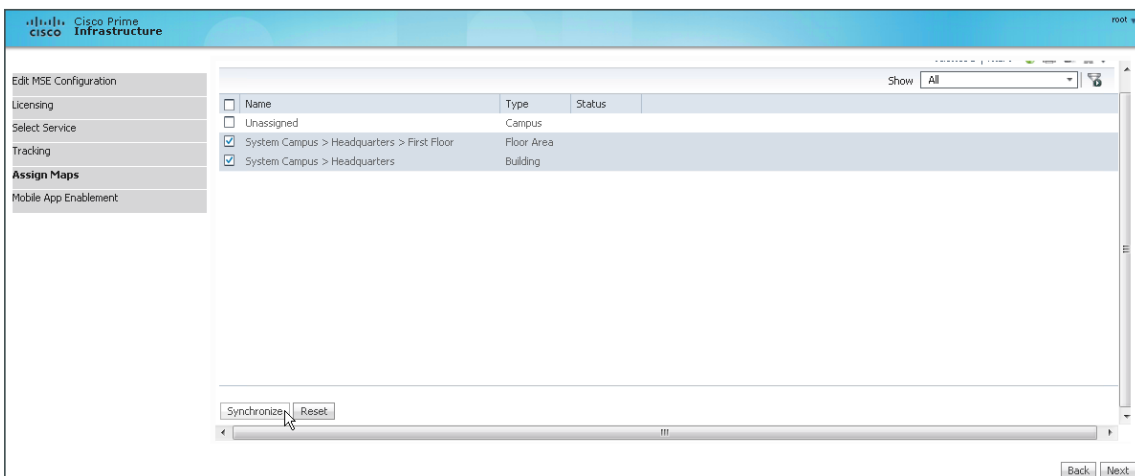
Step 6: On the Tracking page, enable the following real-time and historical tracking services as shown in the following table, and then click **Next**.

Table 1 - Tracking and history parameters

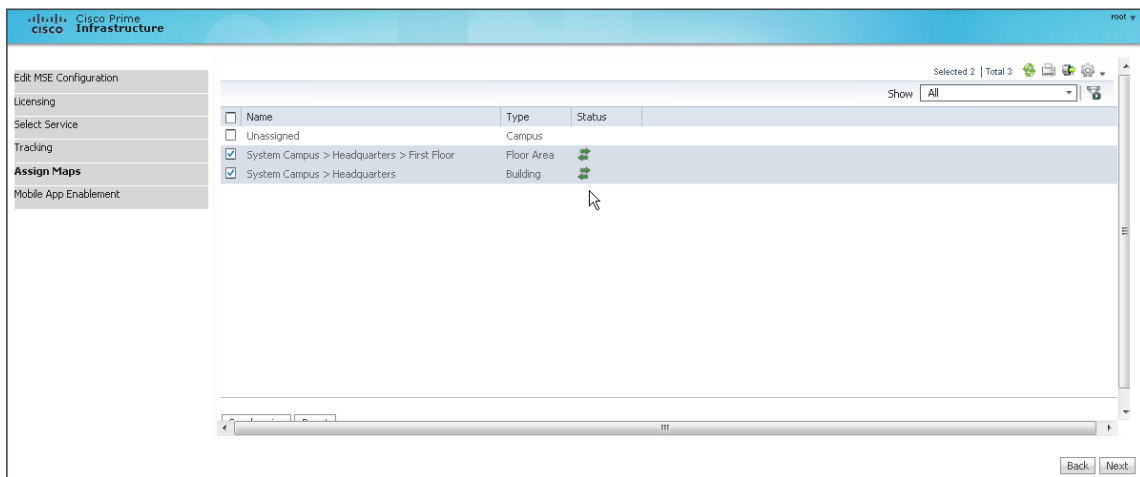
Tracking	History
Wired Client	Wired Stations
Wireless Clients	Client Stations
Rogue Access Points	Rogue Access Points
Rogue Clients	Interferers
Interferers	Rogue Clients
Active RFID Tags	—



Step 7: On the Assign Maps page, select the building and floor plan created and click **Synchronize**.

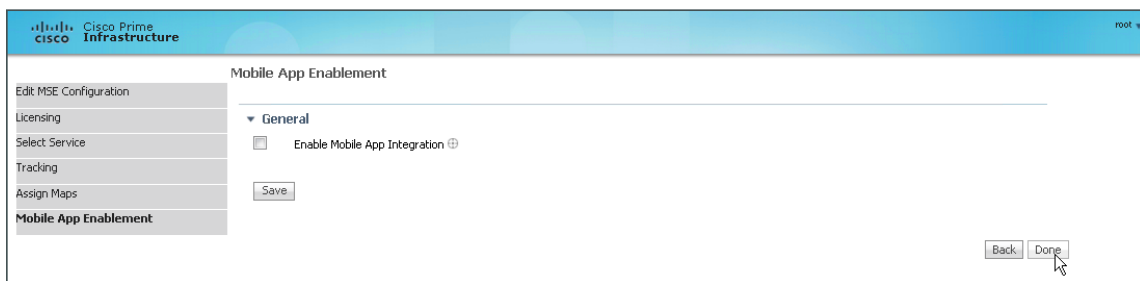


The Status changes to bi-directional as shown by the green arrows in the status column.



Step 8: Click **Next** to continue.

Step 9: 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**.



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 the configured IP address of the Cisco MSE-VA is reachable and that each of the mobility services are available.

Device Name	Device Type	IP Address	Version	Reachability Status	Secondary Server	Mobility Service		
						Name	Admin Status	Service Status
vMSE-VA [Admin View]	Cisco Mobility Services Engine - Virtual Appliance	10.4.48.40	7.6.100.0	Reachable	N/A (Click here to configure)	Context Aware Service	Enabled	Up
						WIPS	Enabled	Up
						Mobile Concierge Service	Disabled	Down
						CMX Analytics	Disabled	Down
						CMX Browser Engage	Disabled	Down
						HTTP Proxy Service	Disabled	Down

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 license tracking, navigate to **Design > Mobility Services Engines**, and then select the Cisco MSE-VA installed.

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**.

Tracking Parameters: vMSE-VA
 Services > Mobility Services Engines > vMSE-VA > Context Aware Service > Administration > Tracking Parameters

When Cisco Tag Engine is enabled, the Licensed Limit for Network Location Service elements also includes Asset Tracking elements.

Tracking Parameters

Network Location Service Elements:		Licensed Limit = 100			
Enable	Tracking Parameters	Enable Limiting	Limit Value	Active Value	Not Tracked
<input checked="" type="checkbox"/>	Wired Clients	<input checked="" type="checkbox"/>	15	0	0
<input checked="" type="checkbox"/>	Wireless Clients	<input type="checkbox"/>	0	0	0
<input checked="" type="checkbox"/>	Rogue AccessPoints	<input checked="" type="checkbox"/>	45	0	0
<input type="checkbox"/> Exclude Adhoc Rogue APs					
<input checked="" type="checkbox"/>	Rogue Clients	<input checked="" type="checkbox"/>	10	0	0
<input checked="" type="checkbox"/>	Interferers	<input checked="" type="checkbox"/>	30	0	0
<input checked="" type="checkbox"/>	Active RFID Tags	<input type="checkbox"/>	0	0	0

Save Cancel



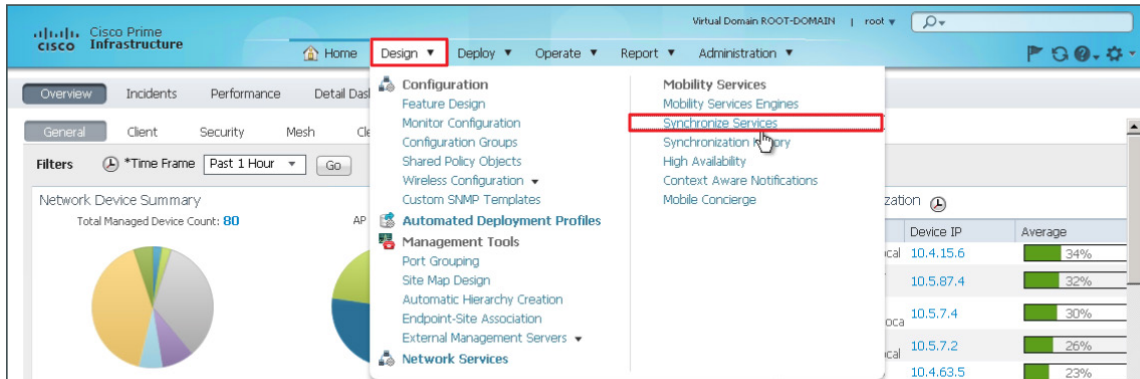
Tech Tip

The reason we are limiting the number of licenses used for each type of tracking parameter is to prevent 100% of the licenses from being used by a single tracking parameter.

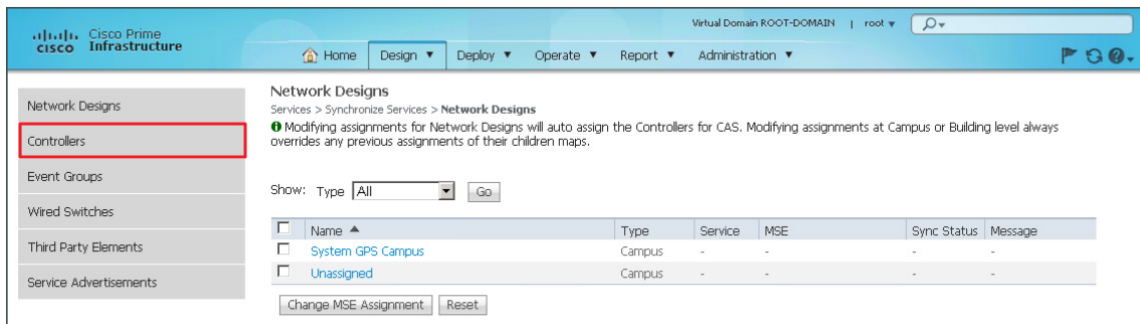
Procedure 5 Synchronize the WLCs to use Cisco MSE

In order to establish and assign the Cisco MSE-VA 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.

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



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



Step 3: Select each of the wireless LAN controllers that you want to assign to the Cisco MSE, and then click **Change MSE Assignment**. It does not make sense to select dedicated guest anchor controllers as these WLCs will typically not have access points registered directly to them.

Virtual Domain ROOT-DOMAIN | root

Home Design Deploy Operate Report Administration

Controllers
Services > Synchronise Services > Controllers
For MSE versions prior to 7.0.x, modifying the assignment for one service will also modify the assignment for the other service(s).

Name	IP Address	Version	Service	MSE	Sync Status	Message
<input type="checkbox"/> 2504-1	10.4.30.62	7.6.100.0	-	-	-	-
<input type="checkbox"/> 2504-2	10.4.30.63	7.6.100.0	-	-	-	-
<input checked="" type="checkbox"/> 5508-1	10.4.30.66	7.6.100.0	CAS	vMSE-VA [NMSP Status]	↕	-
			wIPS	vMSE-VA [NMSP Status]	↕	-
<input type="checkbox"/> DMZ-WLC2504-Guest-1	192.168.19.25	7.6.100.0	-	-	-	-
<input type="checkbox"/> DMZ-WLC2504-Guest-2	192.168.19.26	7.6.100.0	-	-	-	-
<input type="checkbox"/> DMZ-WLC5508-Guest-1	192.168.19.54	7.6.100.0	-	-	-	-
<input checked="" type="checkbox"/> WISM2	10.4.30.64	7.6.100.0	CAS	vMSE-VA [NMSP Status]	↕	-
			wIPS	vMSE-VA [NMSP Status]	↕	-
<input checked="" type="checkbox"/> WLC7500-1	10.4.59.68	7.6.100.0	CAS	vMSE-VA [NMSP Status]	↕	-
			wIPS	vMSE-VA [NMSP Status]	↕	-
<input checked="" type="checkbox"/> vWLC_7_6_95_7-Server1	10.4.59.58	7.6.95.7	CAS	vMSE-VA [NMSP Status]	↕	-
			wIPS	vMSE-VA [NMSP Status]	↕	-
<input checked="" type="checkbox"/> vWLC_7_6_95_7-Server2	10.4.59.59	7.6.95.7	CAS	vMSE-VA [NMSP Status]	↕	-
			wIPS	vMSE-VA [NMSP Status]	↕	-

Change MSE Assignment Reset

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

Choose MSEs

Name	IP Address	CAS	wIPS	MSAP
vMSE-VA	10.4.48.40	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Synchronize Cancel

Procedure 6 Enable NMSP between MSE and WLCs

(Optional)

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 wIPS 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 recommended that all infrastructure components utilize NTP for consistent clock synchronization. In addition, the WLC must have the MAC address and Key Hash of the MSE-VA configured. The key is normally added automatically by Cisco Prime if the WLC was initially discovered using the Read/Write SNMP community string. The manual process of configuring the MSE credentials into the WLCs is shown below.

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.

Name	IP Address	Version	Service	MSE	Sync Status	Message
2504-1	10.4.30.62	7.6.100.0	-	-	-	-
2504-2	10.4.30.63	7.6.100.0	-	-	-	-
5508-1	10.4.30.66	7.6.100.0	CAS	vMSE-VA [NMSP Status]	+	-
			wIPS	vMSE-VA [NMSP Status]	+	-
DMZ-WLC2504-Guest-1	192.168.19.25	7.6.100.0	-	-	-	-
DMZ-WLC2504-Guest-2	192.168.19.26	7.6.100.0	-	-	-	-
DMZ-WLC5508-Guest-1	192.168.19.54	7.6.100.0	-	-	-	-
WISM2	10.4.30.64	7.6.100.0	CAS	vMSE-VA [NMSP Status]	+	-
			wIPS	vMSE-VA [NMSP Status]	+	-
WLC7500-1	10.4.59.68	7.6.100.0	CAS	vMSE-VA [NMSP Status]	+	-
			wIPS	vMSE-VA [NMSP Status]	+	-

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.

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

Property	Value
Summary	
IP Address	10.4.59.68
Version	7.6.100.0
Target Type	Controller
NMSP Status	Inactive
Echo Request Count	0
Echo Response Count	0
Last Activity Time	-
Last Echo Request Message Received At	-
Last Echo Response Message Received At	-
Model	7500
MAC Address	70:81:05:ce:ca:a9
Capable NMSP Services	N/A
Subscribed Services	
Service	None Detected
Subservices	
Messages	
Message Type	IN / OUT
Count	
Last Activity Time	
Bytes	

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: Record 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 login: root
Password:
Last login: Wed Jan 22 13:27:43 on tty1
[root@VMSE-VA ~]# cmd
-bash: cmd: command not found
[root@VMSE-VA ~]# 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:a2:78:88
Key Hash: 1f80d6662f2e42f9bf53f16671838193c3d751f1
Certificate Type: SSC

cmd> [root@VMSE-VA ~]# _
```

Next, 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:a2:78:88 f80d6662f2e42f9bf53
f16671838193c3d751f1
(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 Addr          Cert Type      Key Hash
-----
00:50:56:a2:78:88 SSC           1f80d6662f2e42f9bf53f16671838193c3d751f1
(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 1.4.1, navigate to **Design > Mobility Services > Synchronize Services > Controllers**, and then for every WLC connected to Cisco MSE and used for CAS or wIPS, click the **[NMSP Status]** link.

Network Design		Controllers								
Controllers		Service: Synchronize Services > Controllers ● For MSE versions prior to 7.0.x, modifying the assignment for one service will also modify the assignment for the other service(s).								
Event Groups	Wired Switches	Third Party Elements	Service Advertisements	Name	IP Address	Version	Service	MSE	Sync Status	Message
				2504-1	10.4.30.62	7.6.100.0	CAS	vMSE-VA	[NMSP Status]	-
				2504-2	10.4.30.63	7.6.100.0	CAS	vMSE-VA	[NMSP Status]	-
				5508-1	10.4.30.66	7.6.100.0	CAS	vMSE-VA	[NMSP Status]	-
				DMG-WLCC504-Guest-1	192.168.19.25	7.6.100.0	-	-	-	-
				DMG-WLCC504-Guest-2	192.168.19.26	7.6.100.0	-	-	-	-
				DMG-WLCC508-Guest-1	192.168.19.54	7.6.100.0	-	-	-	-
				WISM2	10.4.30.64	7.6.100.0	CAS	vMSE-VA	[NMSP Status]	-
				WLC7500-1	10.4.59.68	7.6.100.0	CAS	vMSE-VA	[NMSP Status]	-
				vWLC_7_6_95_7-Server1	10.4.59.58	7.6.95.7	wIPS	vMSE-VA	[NMSP Status]	-
				vWLC_7_6_95_7-Server2	10.4.59.59	7.6.95.7	wIPS	vMSE-VA	[NMSP Status]	-

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.

The screenshot displays the Cisco Prime Infrastructure web interface. The main content area shows the 'NMSP Connection Status Details' for the IP address 10.4.59.68. The interface includes a navigation menu on the left and a main panel with a summary table and a subscribed services table.

Summary	
IP Address	10.4.59.68
Version	7.6.100.0
Target Type	Controller
NMSP Status	Active
Echo Request Count	6
Echo Response Count	8
Last Activity Time	2014-Jan-23, 07:06:15 PST
Last Echo Request Message Received At	2014-Jan-23, 07:06:14 PST
Last Echo Response Message Received At	2014-Jan-23, 07:06:14 PST
Model	7500
MAC Address	70:81:05:ice:ca:a9
Capable NMSP Services	IPv6_CLIENTS_SUPPORT, RSSI, INFORMATION, STATISTICS, IDS, HANDOVER, AP MONITOR, SPECTRUM

Subscribed Services	
Service	Subservices
AP MONITOR	SUBSCRIPTION
IDS	WIRELESS IDS
INFORMATION	MOBILE_STATION, ROGUE
RSSI	MOBILE_STATION, TAG, ROGUE
SPECTRUM	AGGREGATED_INTERFERER_DEVICE_REPORT
STATISTICS	MOBILE_STATION, TAG

Troubleshooting with Cisco CleanAir

With the addition of the Cisco Mobility Services Engine virtual appliance (MSE-VA), historical Cisco CleanAir information is readably accessible through Cisco Prime Infrastructure. The ability to determine the quality of the RF spectrum combined with the ability to retrieve baseline historical information is key information needed in RF spectrum troubleshooting.

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

The Cisco Aironet 2600, 3600, and 3700 Series access points can be put in Spectrum Expert-Connect (SE-Connect) mode and used as a virtual remote interface to the MetaGeek Chanalyzer 3rd party application. When an access point is placed in Spectrum Expert Connect mode, it no longer provides wireless services to users but instead has complete visibility of the entire licensed band. When connecting to an access point that is in local mode, the MetaGeek Chanalyzer software has visibility to the channels active on the access point, and wireless services are not interrupted. In both cases, the physical location of those with advanced RF skill sets is no longer relevant as remote access to the network is all that is required.

By changing the role of your CleanAir access point to either local or SE-Connect mode and connecting to it using the MetaGeek Chanalyzer software, the Wi-Fi network administrator can view the environment directly and in detail. Your organization no longer needs to fly expensive personnel onsite in order to troubleshoot challenging physical-layer issues that are too often intermittent in nature.

PROCESS

Viewing real-time and historical CleanAir using Prime Infrastructure

1. View historical Cisco CleanAir information

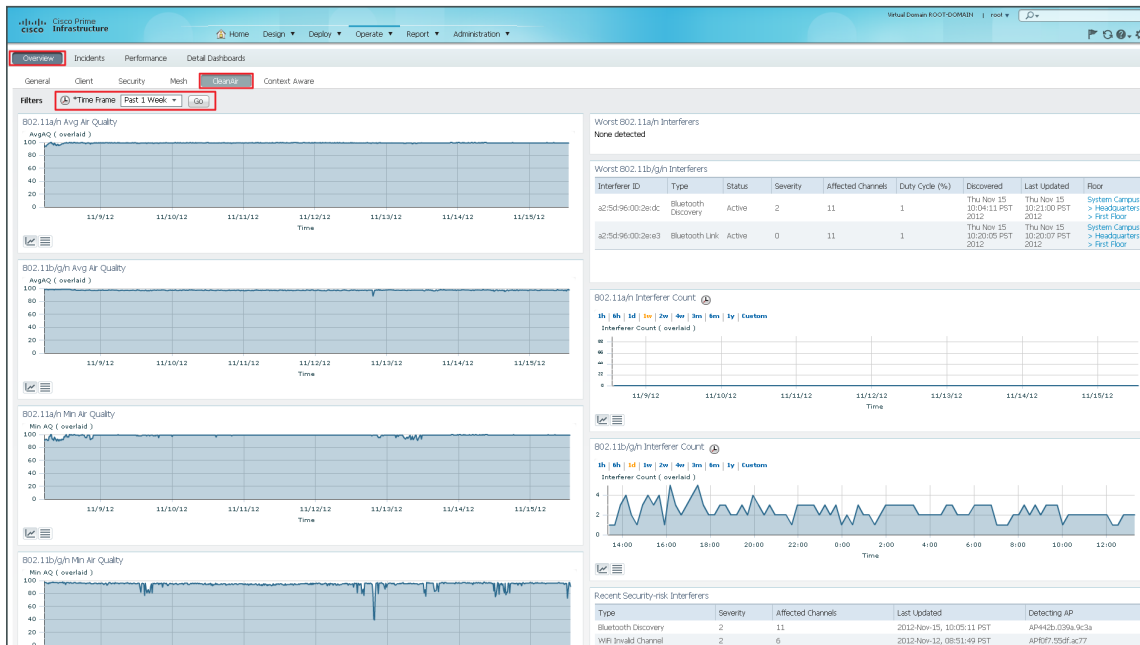
When the call for assistance arrives, it almost certainly will originate from a location that does not have knowledgeable human resources to troubleshoot, identify, and fix the issue. Wi-Fi devices are designed to send and receive Wi-Fi signals, but they do not have the capability to identify non-Wi-Fi radio interferers, such as microwave ovens, Digital Enhanced Cordless Telecommunications (DECT) phones, analog wireless cameras, or even radio jammers. The specialized Spectrum Analysis Engine (SAgE) ASIC in the Cisco CleanAir access points can identify these devices and with triangulation from the MSE, can locate their position on a map.

When the call comes in, identifying the facts about the issue to make informed decisions regarding the next steps for effective mitigation is critical to effective problem resolution. Examples of some of the information used in the decision process are the location of the problem, type of interference (if known), impacted areas and time of day (for example, if the issue occurs most of the time during lunch hours). Armed with as much information from the end user as possible, combined with the fact that Cisco Prime Infrastructure indicates a drop in Air Quality (AQ), the Wi-Fi engineer can begin to examine the RF environment in depth using Cisco Prime Infrastructure, Cisco Mobility Services Engine and Cisco CleanAir access points.

Procedure 1 View historical Cisco CleanAir information

Oftentimes it's imperative that a historical baseline for RF spectrum management is available. As is the case with many network engineers and integration partners responsible for a wireless network, problems invariably occur when support personnel are not onsite. When using Cisco Prime Infrastructure combined with the Cisco Mobility Services Engine Virtual Appliance (MSE-VA), you can easily view historical RF based CleanAir information. This provides the ability for those responsible for the operation of the wireless network to examine the state of the RF environment after the RF based interference event has cleared.

Step 1: In Cisco Prime Infrastructure 1.4.1, navigate to **Home > Overview > CleanAir**, in the **Filters** list, choose the desired time frame, and then click **Go**.



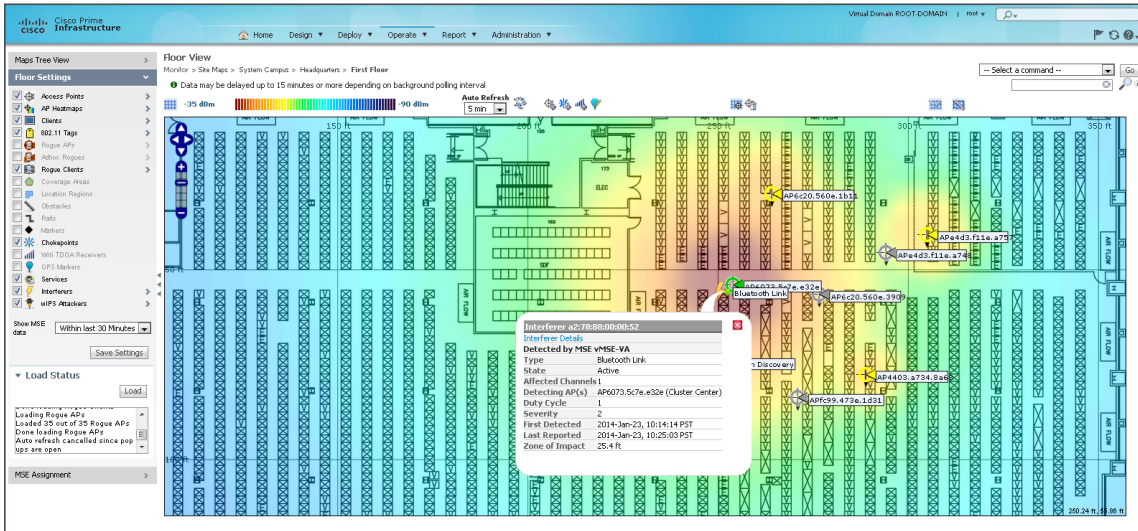
Tech Tip

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:

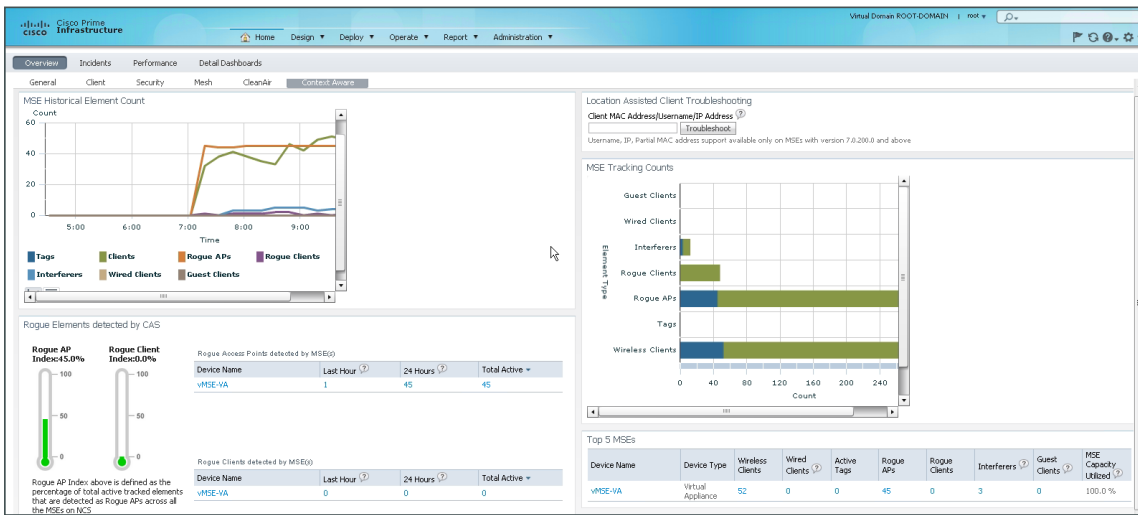
1. Ensure that CleanAir-capable APs have been configured on the floor plan or map and that their radios are enabled.
2. Ensure that all CleanAir settings have been successfully applied to the APs and wireless LAN controller via the templates described in this document.
3. Repeat Step 4 in Procedure 5 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.

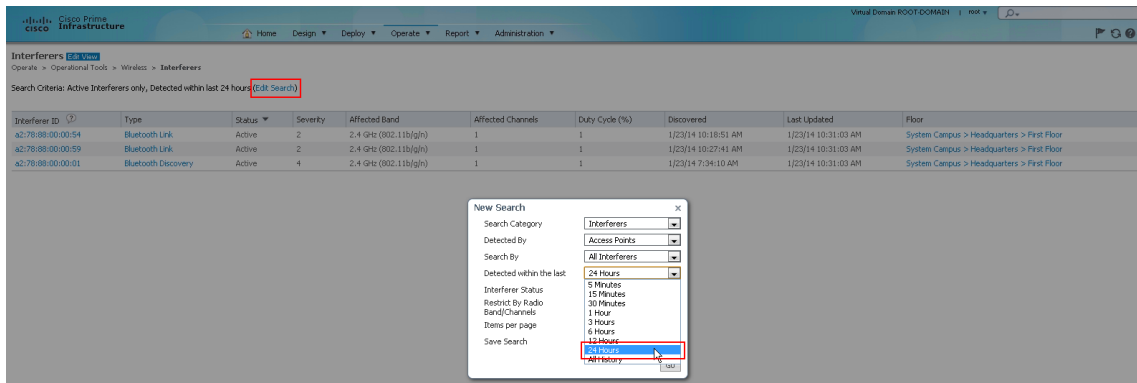
Step 3: In the left pane, under Floor Settings, select **Interferers**. The list of interferers is graphically displayed.



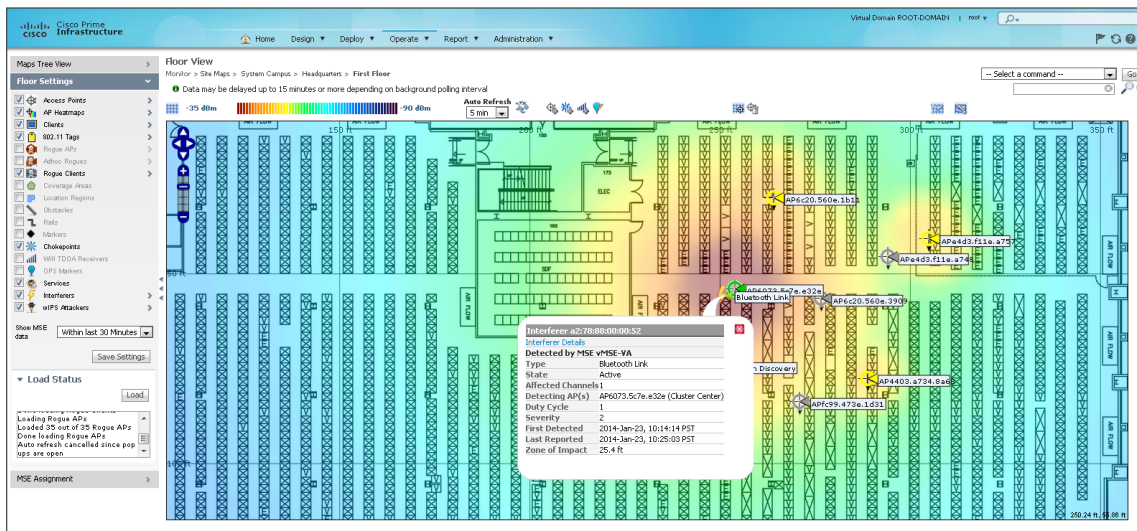
Step 4: Navigate to **Overview > Context Aware**. This displays the historical information on the number of rogues, wireless clients, and other context-aware information obtained from the Cisco MSE-VA.



Step 5: Within Cisco Prime Infrastructure 1.4.1, 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.



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.



Viewing real-time CleanAir using MetaGeek's Chanalyzer

PROCESS

1. Install MetaGeek Chanalyzer
2. Analyzing RF environment using MetaGeek Chanalyzer & Cisco CleanAir
3. Remote Spectrum Analysis using MetaGeek Chanalyzer
4. Using MetaGeek Chanalyzer to produce RF impact reports

Cisco has partnered with MetaGeek and now provides real-time Cisco CleanAir spectrum intelligence to the MetaGeek Chanalyzer product. The Chanalyzer product from MetaGeek provides the network administrator with the same capabilities found in the Cisco Spectrum Expert software but with advanced visualizations and many more features. The MetaGeek Chanalyzer product allows you to get the most from Cisco CleanAir access points with and without the WSSI module.

When using the MetaGeek Chanalyzer product with a Cisco CleanAir access point, the network administrator can view both the 2.4GHz and 5GHz bands simultaneously while zooming into specific time periods using a Digital Video Recorder (DVR) like capability. The advanced graphics visualizations produced clearly show the type of interference (Bluetooth, DECT among a few) and its location within the RF band. Information captured can be saved to a file to serve as a baseline, or transmitted to 2nd or 3rd level engineers for analysis.

The outstanding and informative graphic visualizations that the Chanalyzer product produces can be coupled with advanced reporting capabilities. This allows wireless network engineers and/or integration partners to produce professional reports that graphically show the impact of the interference in a way that can be easily understood and visualized.

The following procedures outline the installation and use of the MetaGeek Chanalyzer product with Cisco CleanAir.



Tech Tip

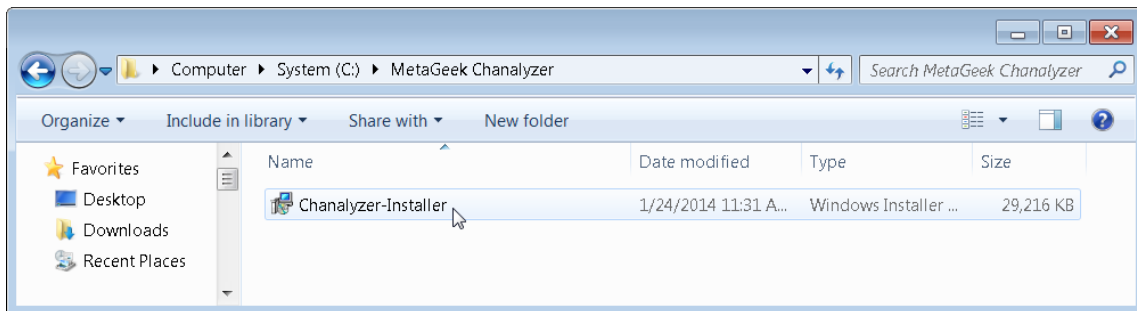
A free 7 day trial of the MetaGeek Chanalyzer product can be downloaded from MetaGeek at the following URL: <http://www.metageek.net/support/downloads/>

Procedure 1 Install MetaGeek Chanalyzer

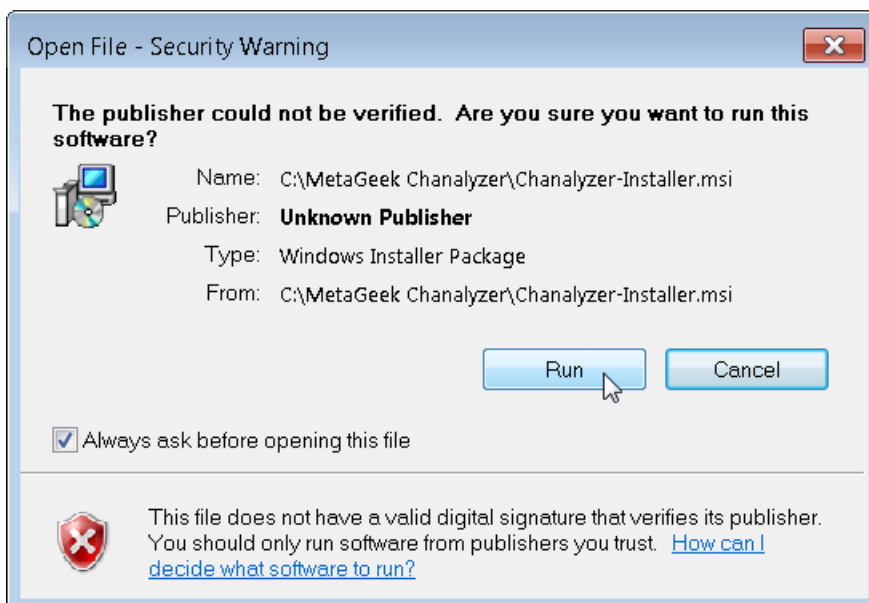
The MetaGeek Chanalyzer is supported on Microsoft Windows 8, 7, Vista and XP (SP3) with .NET 4.0 installed. The minimum hardware requirements are 4GB of RAM and a display resolution of 1024x600 or greater. Apple Mac laptops are supported via OSX virtualization using VMware Fusion and Parallels. If using a virtual machine, a USB based Wi-Fi adapter will be required to provide local spectrum intelligence. More information can be found on the MetaGeek website at the following URL:

<http://www.metageek.net/products/chanalyzer-cleanair>

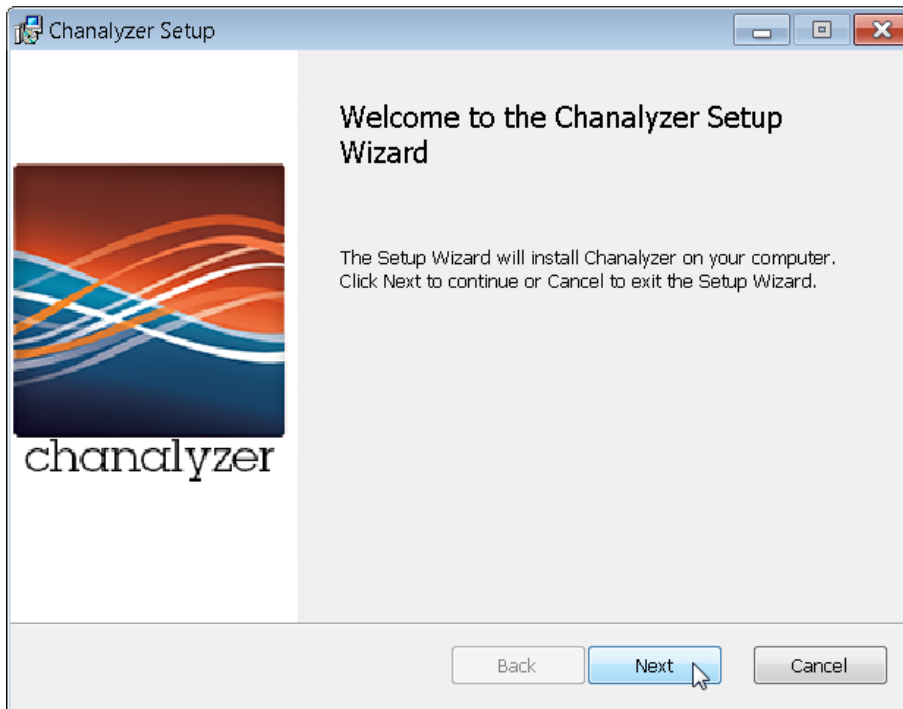
Step 1: Launch the MetaGeek Chanalyzer software.



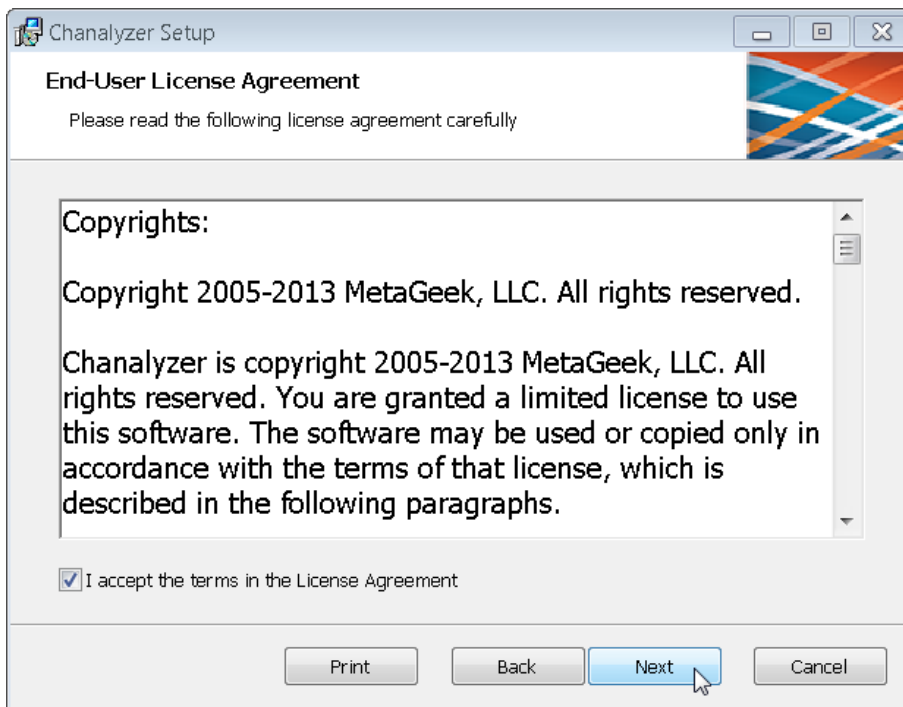
Step 2: If prompted with a Security Warning to run the file, select **Run**



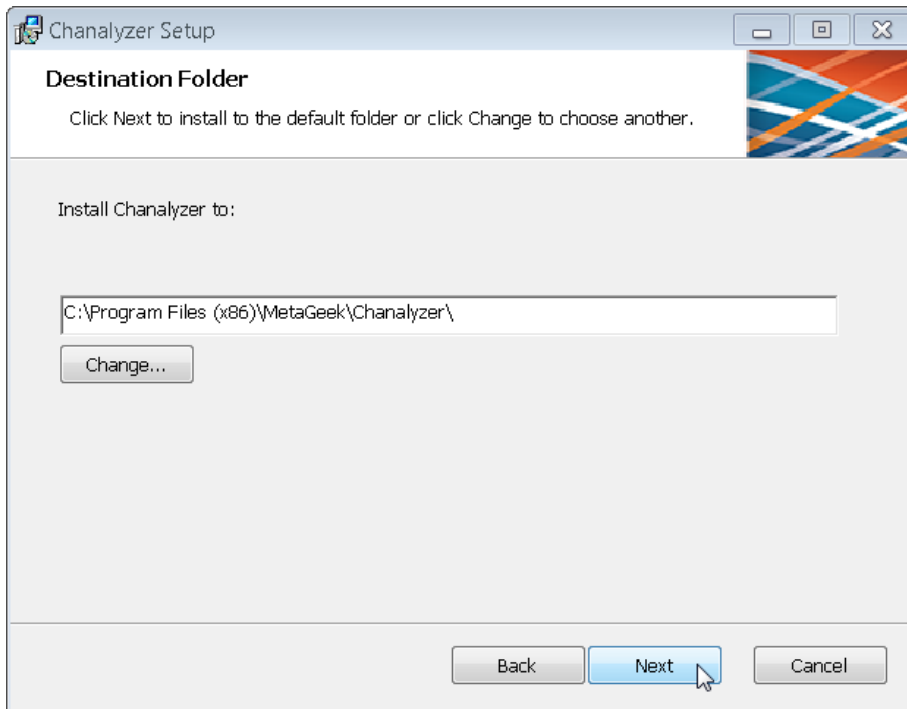
Step 3: Press **Next** to begin the installation of the Chanalyzer Setup Wizard.



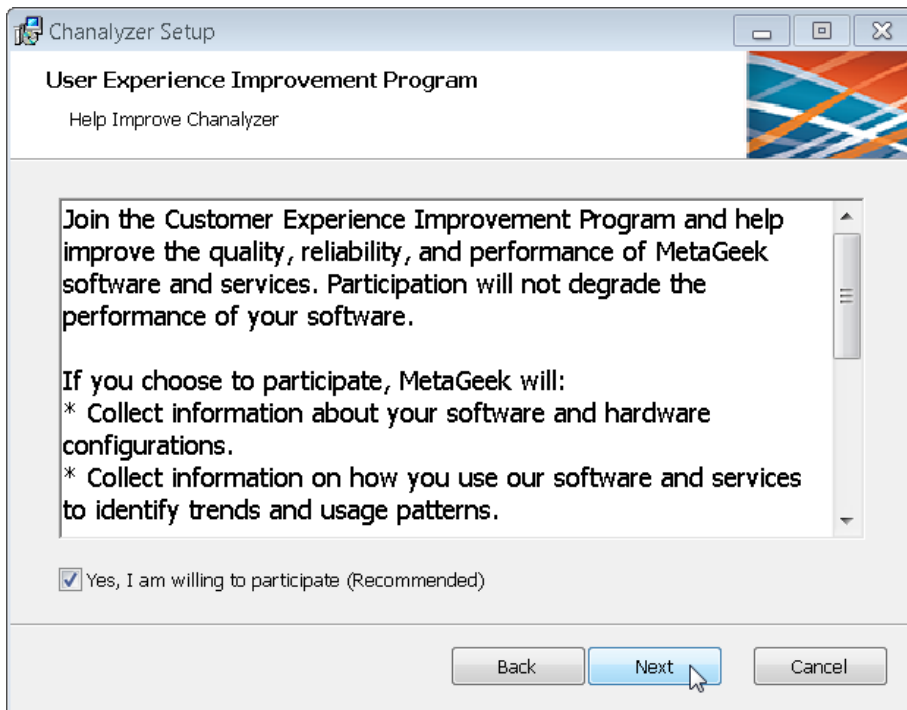
Step 4: If you agree with the License Agreement, select **I accept the terms in the license agreement** and press **Next**.



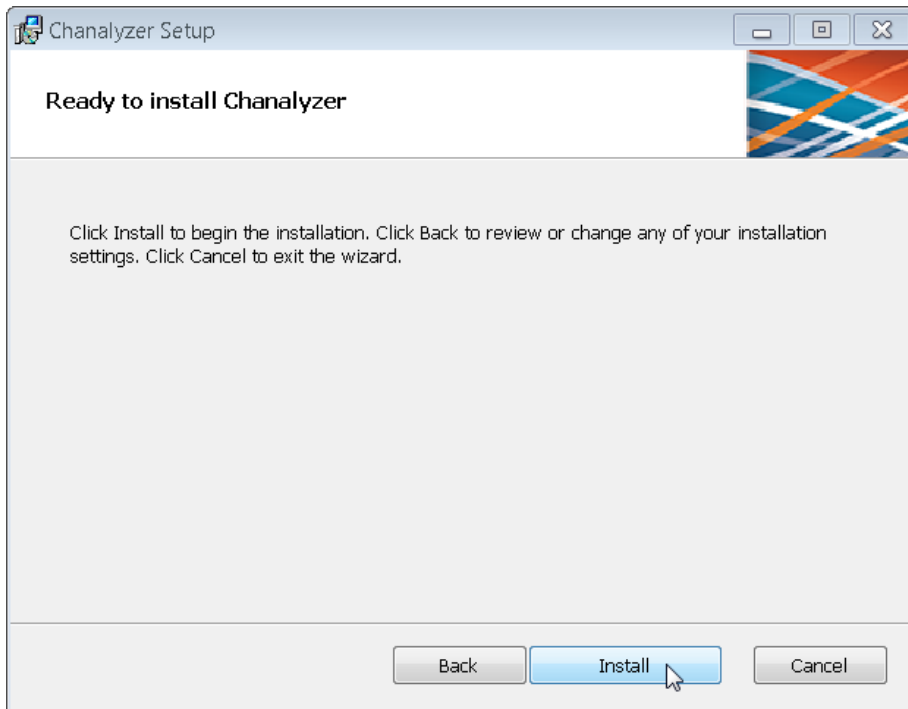
Step 5: Verify that the default installation location is correct and press **Next**.



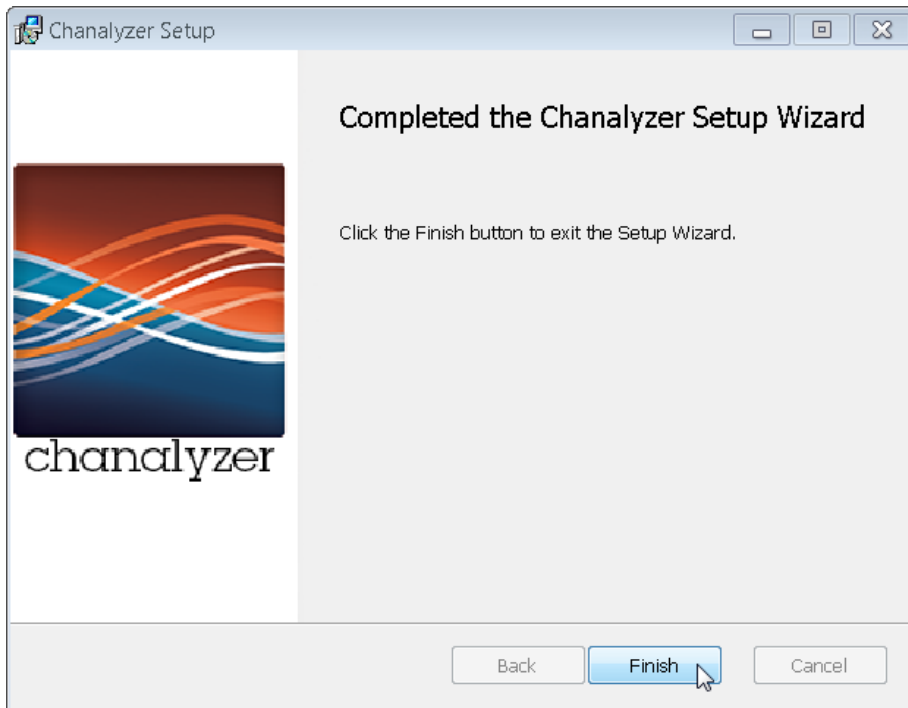
Step 6: Select **Next** to grant permission to participate in the Customer Experience Improvement Program. If you do not wish to participate remove the check mark from the Yes, I am willing to participate (Recommended) prompt and press **Next**.



Step 7: Press **Install** to begin the installation of the MetaGeek Chanalyzer software.



Step 8: Once the installation completes, press **Finish** to complete the installation.



Procedure 2 Analyzing RF environment using MetaGeek Chanalyzer & Cisco CleanAir

The Cisco CleanAir capable access point must be changed to Spectrum Expert Connect (SE-Connect) mode to view then entire 2.4GHz and 5GHz bands. This change is disruptive to the wireless users that are associated to the access point, and caution should be exercised before enabling SE-Connect mode on the access point.

If visibility to the channels that are currently being used by the access point is all that is required, it is not necessary to place the access point into SE-Connect mode. Cisco CleanAir access points which are operating in local mode have the ability to provide Cisco CleanAir spectrum intelligence to the MetaGeek Chanalyzer software for the channel currently in operation.

Once the access point has rebooted and is operating in SE-Connect mode, collect the Key Hash and IP address of the access point as outlined in the following procedure.



Tech Tip

An access point operating in SE-Connect mode is passive and will not provide wireless services to end users. It does however provide complete visibility to the 2.4GHz and 5GHz licensed bands. If visibility to the entire licensed bands is not required, an access point operating in local mode will provide wireless user services and visibility to the currently assigned channels in both 2.4GHz and 5GHz bands. This is inclusive of 80MHz wide bonded channels found in 802.11ac when using the Cisco 3700 access point.

Step 1: Log in to the wireless LAN controller and navigate to **WIRELESS**.

Step 2: Select the Cisco CleanAir access point that is closest to the suspected source of interference, and would have the least impact to the wireless network users.

Step 3: If the access point is operating in local mode and visibility to the entire 2.4GHz and 5GHz band is not required, skip to Step 5. Otherwise, in the **AP Mode** drop-down list, choose **SE-Connect**, and then click **Apply**.

Step 4: Wait for the access point to reboot and reconnect to the wireless LAN controller.

The screenshot shows the configuration page for AP6073.5c7e.e32e. The 'AP Mode' dropdown menu is open, and 'SE-Connect' is selected. The 'Network Spectrum Interface Key' is 9301E11063322DA1BA8FB532894DB4D. The IP address is 10.4.90.13.

General		Versions	
AP Name	AP6073.5c7e.e32e	Primary Software Version	7.6.100.0
Location	default location	Backup Software Version	0.0.0.0
AP MAC Address	60:73:5c:7e:e3:2e	Predownload Status	None
Base Radio MAC	34:a8:4e:70:4e:00	Predownload Version	None
Admin Status	Enable	Predownload Next Retry Time	NA
AP Mode	SE-Connect	Predownload Retry Count	NA
AP Sub Mode	local	Boot Version	12.4.25.1
Operational Status	monitor	IOS Version	15.2(4)JB3
Port Number		Mini IOS Version	7.3.1.73
Venue Group	SE-Connect	IP Config	
Venue Type	Unspecified	IP Address	10.4.90.13
Venue Name		Static IP	<input type="checkbox"/>
Language		Time Statistics	
Network Spectrum Interface Key	9301E11063322DA1BA8FB532894DB4D	UP Time	0 d, 19 h 11 m 23 s
		Controller Associated Time	0 d, 19 h 09 m 53 s
		Controller Association Latency	0 d, 00 h 01 m 29 s

Step 5: Copy the Network Spectrum Interface Key and the IP address.

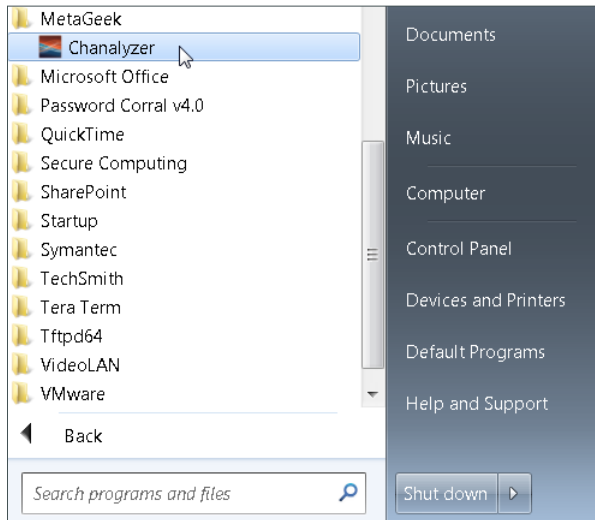
The screenshot shows the configuration page for AP6073.5c7e.e32e. The 'AP Mode' dropdown menu is open, and 'SE-Connect' is selected. The 'Network Spectrum Interface Key' is 9301E11063322DA1BA8FB532894DB4D. The IP address is 10.4.90.13.

General		Versions	
AP Name	AP6073.5c7e.e32e	Primary Software Version	7.6.100.0
Location	default location	Backup Software Version	0.0.0.0
AP MAC Address	60:73:5c:7e:e3:2e	Predownload Status	None
Base Radio MAC	34:a8:4e:70:4e:00	Predownload Version	None
Admin Status	Enable	Predownload Next Retry Time	NA
AP Mode	SE-Connect	Predownload Retry Count	NA
AP Sub Mode	local	Boot Version	12.4.25.1
Operational Status	monitor	IOS Version	15.2(4)JB3
Port Number		Mini IOS Version	7.3.1.73
Venue Group	SE-Connect	IP Config	
Venue Type	Unspecified	IP Address	10.4.90.13
Venue Name		Static IP	<input type="checkbox"/>
Language		Time Statistics	
Network Spectrum Interface Key	9301E11063322DA1BA8FB532894DB4D	UP Time	0 d, 19 h 11 m 23 s
		Controller Associated Time	0 d, 19 h 09 m 53 s
		Controller Association Latency	0 d, 00 h 01 m 29 s

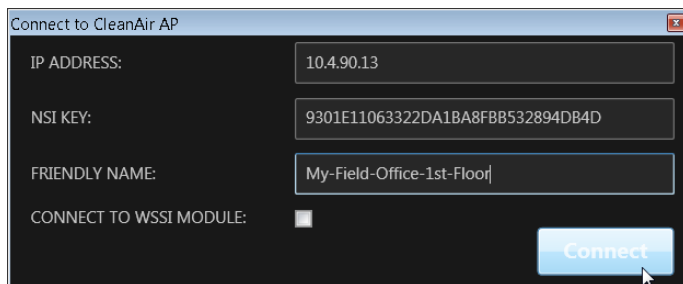
Table 2 - SE-Connect Access Point Information

Value	Example	Site Specific Values
Network Spectrum Interface Key	9301E11063322DA1BA8FBB532894DB4D	
IP Address	10.4.90.13	

Step 6: On a Supported Windows platform with MetaGeek Chanalyzer installed, launch the Chanalyzer application.



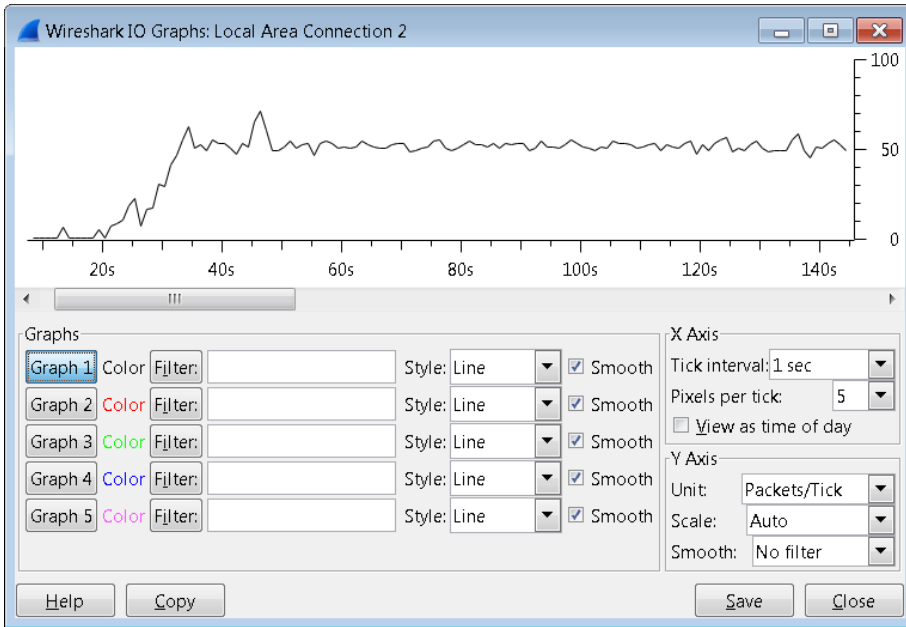
Step 7: Once MetaGeek's Chanalyzer navigate to **CleanAir > Connect to CleanAir AP** and enter a useful name for the AP in SE-Connect mode followed by its IP address and the Network Spectrum Interface Key (NSI Key) that you copied in Step 5 then press **Connect**.



When using MetaGeek Chanalyzer software, a connection is made from the Chanalyzer application directly to the CleanAir access point on TCP port 37540 for 802.11b/g/n and 37550 for 802.11a/n. If connection problems occur, verify the following:

- IP address of the Cisco CleanAir access point is correct
- The CleanAir access point's NSI key is correct
- Network reachability exists between the CleanAir access point and the workstation where the MetaGeek Chanalyzer is installed
- No network devices are blocking the necessary TCP connections
- The Cisco CleanAir access point has CleanAir administratively enabled and the operational status is UP
- The Cisco CleanAir access point is either in local or SE-Connect mode. Access points operating Other modes such as FlexConnect will not display

During normal operation, the bandwidth requirements between the MetaGeek Chanalyzer workstation and the CleanAir access point should not exceed 100kbps. The following bandwidth utilization of ~50-60kbps was observed using MetaGeek Chanalyzer software version 5.0.3.36 to a Cisco Aironet 3600 Series Access Point operating in SE-Connect mode on a fairly active Wi-Fi lab environment.

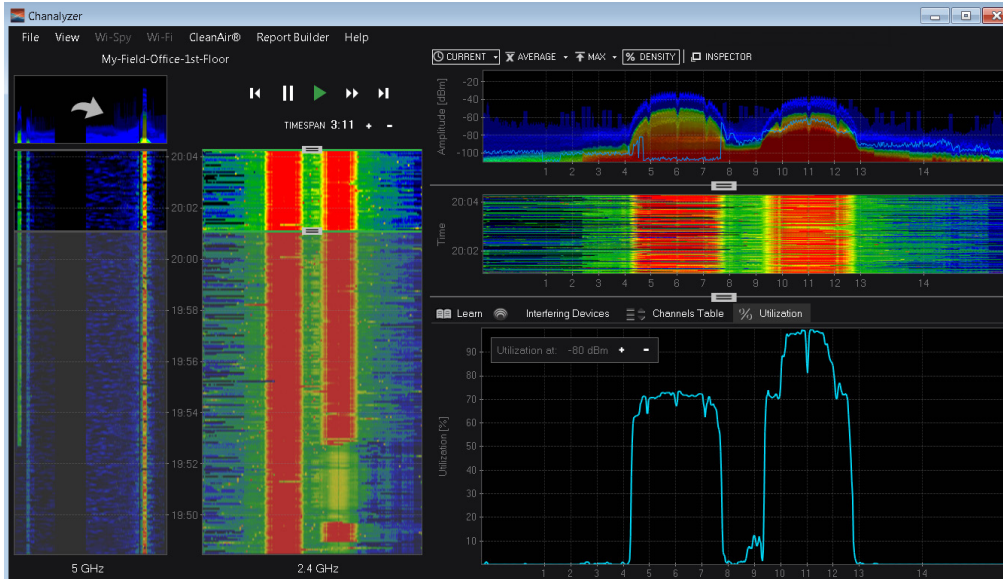


Reader Tip

Notice in the graphic above that channels 1-14 in the 2.4GHz band are visible. The complete licensed band is shown when the access point is placed in SE-Connect mode.

Procedure 3 Remote Spectrum Analysis using MetaGeek Chanalyzer

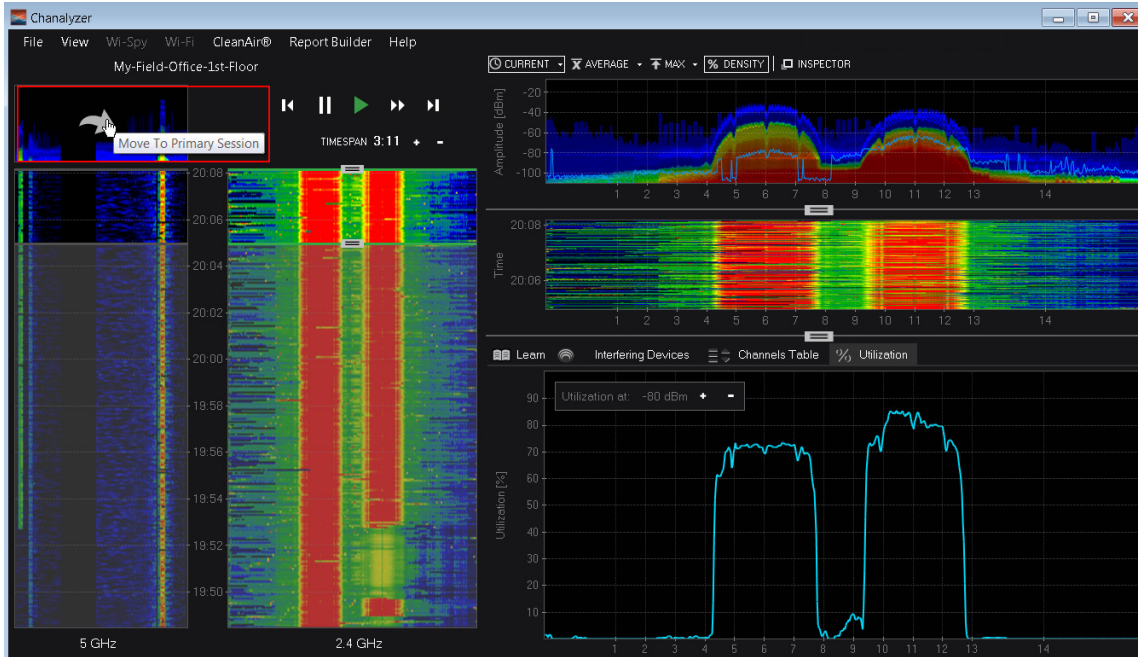
By using the Cisco CleanAir capability of the MetaGeek Chanalyzer product, the network administrator has real-time, physical-layer RF spectrum intelligence without having to drive or fly onsite. The following figure illustrates this capability in a Wi-Fi-only environment and gives you an understanding of how MetaGeek Chanalyzer shows what is happening in both the 2.4GHz and 5GHz bands simultaneously.



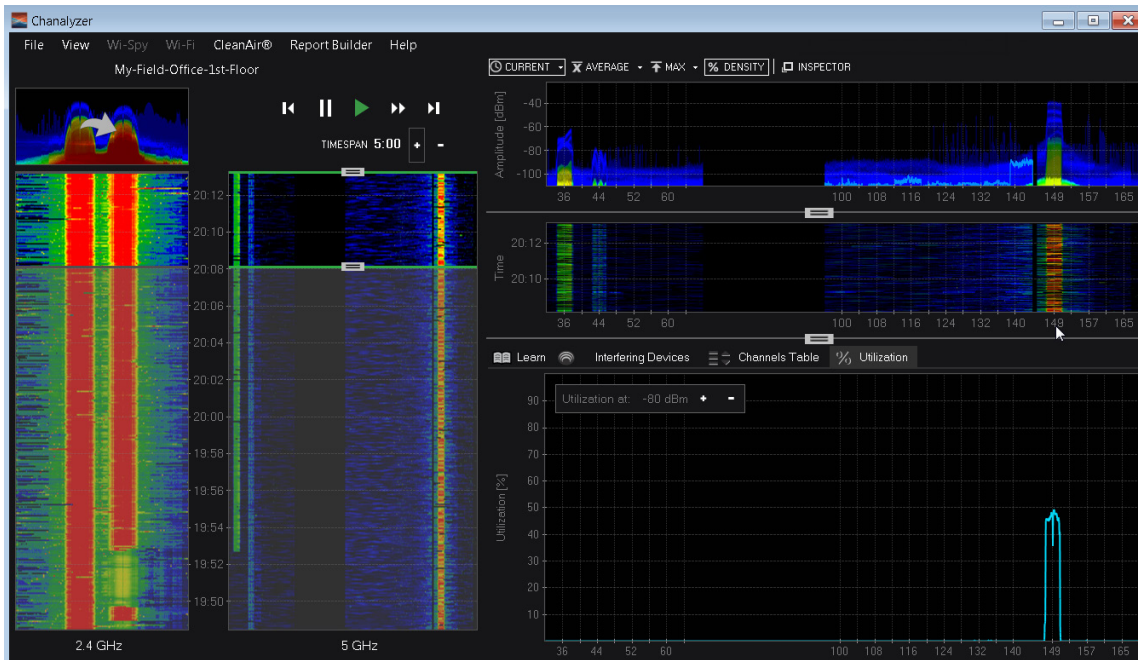
In the graphic shown above, the network administrator can easily determine that the utilization on Channel 6 and channel 11 (in the 2.4GHz band) are relatively heavily utilized. This is evident in the following:

- The Red “lines” shown on the left most 2.4Ghz Waterfall graphic
- The channel utilization (6 and 11) shown in the lower right quadrant of the graphic (~70% & 99% respectively)
- The Density Amplitude portion in the upper right quadrant

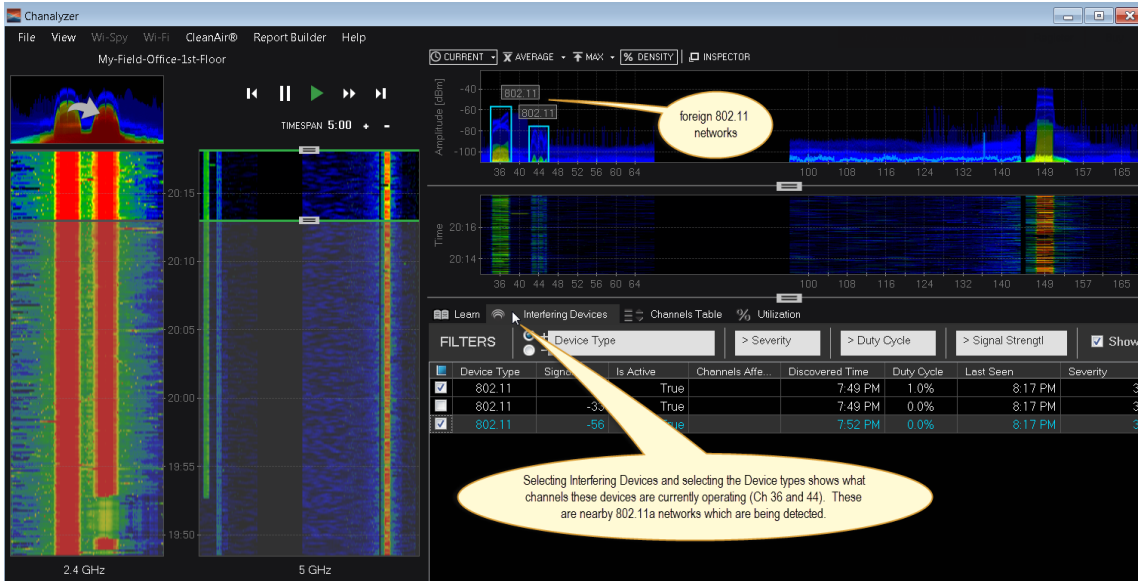
Step 1: To make the 5GHz band the primary band for the current session, select the arrow at the top of the 5GHz waterfall on the far left.



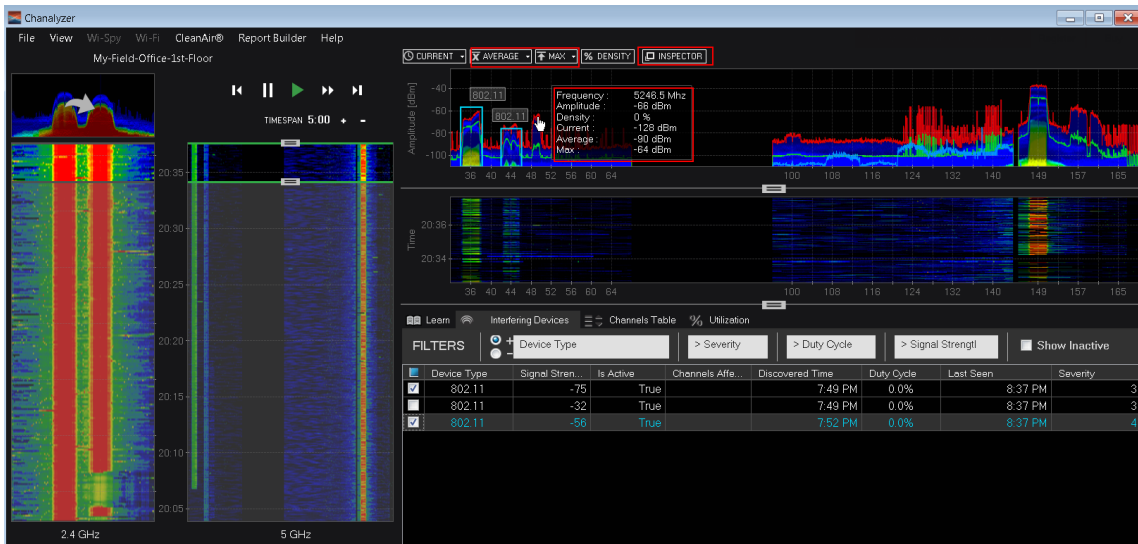
Step 2: When looking at the 5GHz band more closely, it is apparent that channel 149 is the only channel in use, with a utilization level of approximately 50%.



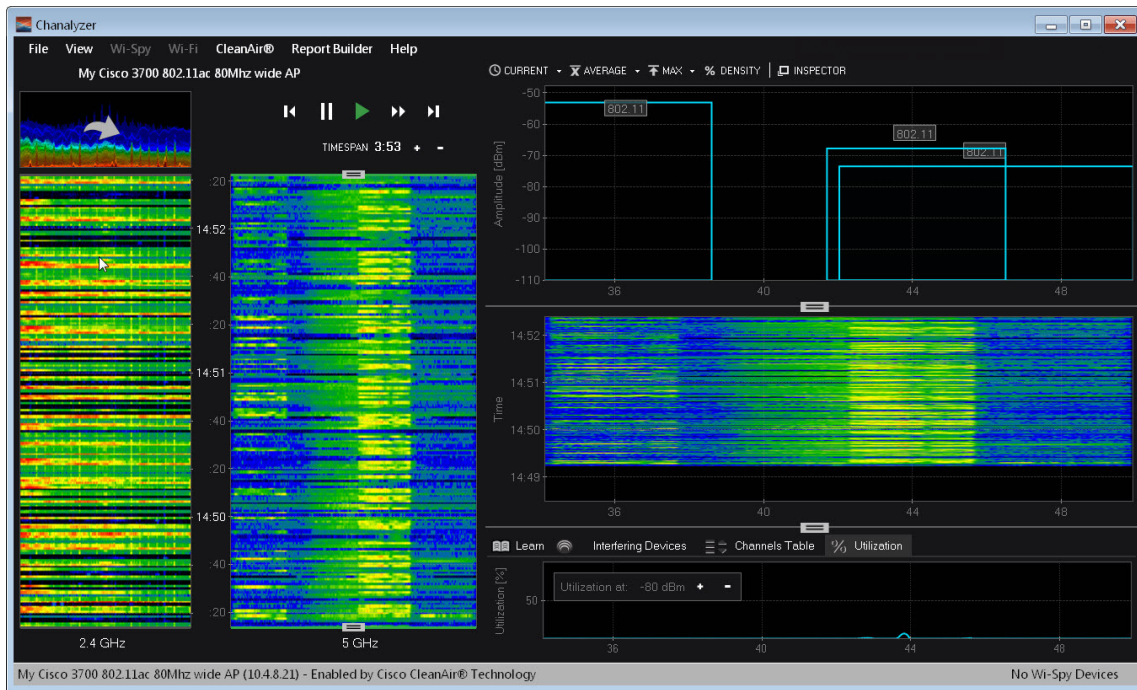
Step 3: To determine the type of interference affecting the 5GHz band, select the Interfering Devices from the Utilization graph in the lower right quadrant. In the example shown, foreign 802.11 networks are operating on channel 36 and 44.



Step 4: To view Average, Maximum and Inspection details on the Amplitude Density graph in the upper right, select Average, Max and Inspector by selecting each of them. As you mouse over the respective portions of the Amplitude graph, the inspector tool gives you details of the area being pointed to by the mouse as shown.



Step 5: When using a Cisco 3700 Series access point operating in local mode with 80MHz bonded channels, the entire 80MHz channel is visible in real time. Notice in the graphic that channels 36, 40, 44 and 48 are displayed for the 5GHz band. It also appears that there is an access point operating on a 40MHz bonded channel (44-48) and two access points each using a 20MHz channel (36 & 44).

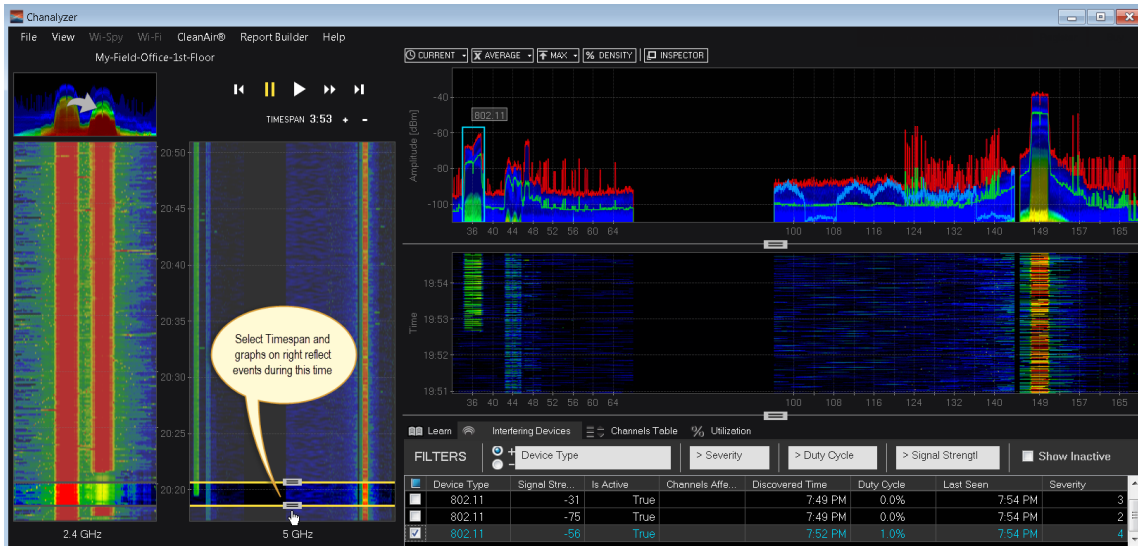


Procedure 4 Using MetaGeek Chanalyzer to produce RF impact reports

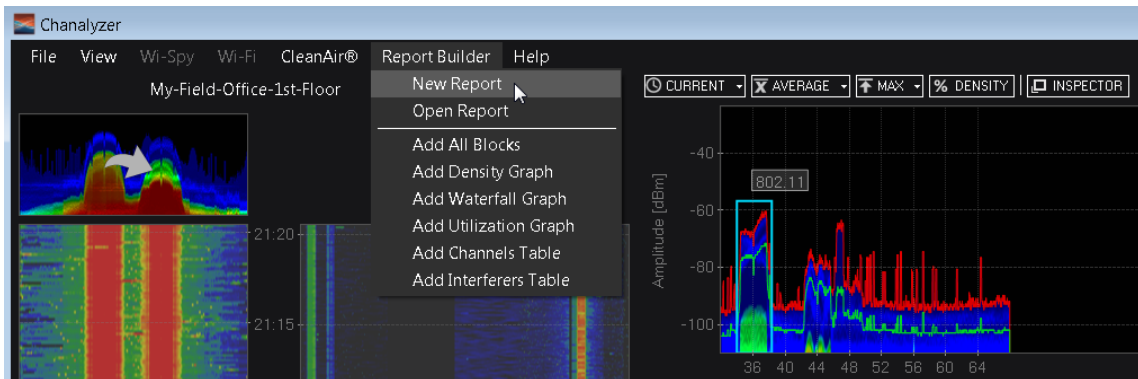
One of the powerful capabilities of the Chanalyzer product is the ability to create custom on-demand reports. By selecting a timespan during which an interesting event has occurred, it is possible to add any of the resulting graphs to the report. This DVR like capability allows you to select timespans that contain multiple events that may be impacting the performance and availability of the wireless network.

Multiple timespans can be selected allowing you to add multiple graphs to the same report, each with customized text explaining each event. These reports are especially useful to provide to customers as part of a managed wireless service, or to network operations director during weekly outage meetings.

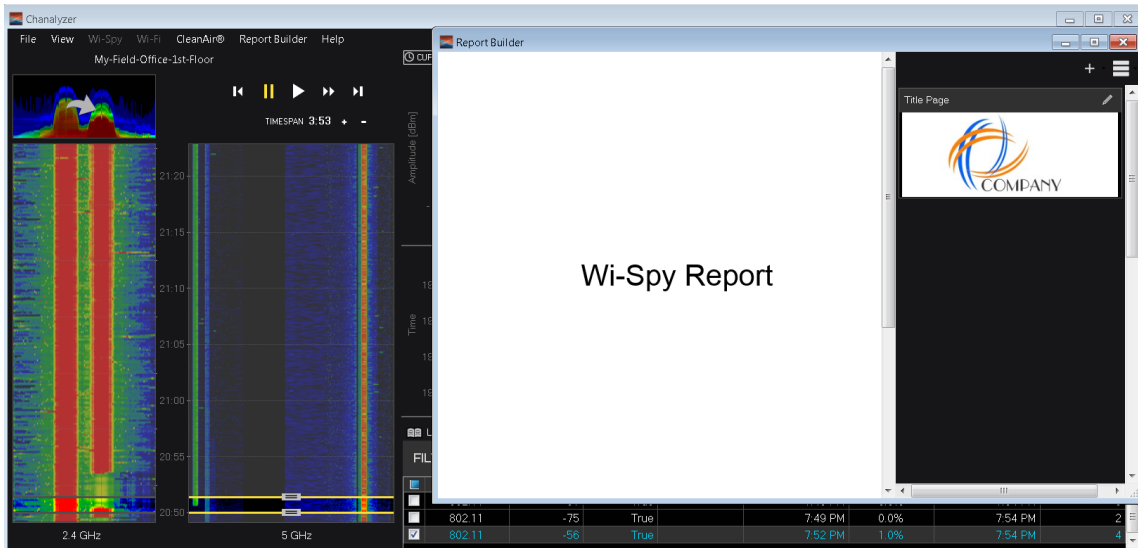
Step 1: Select the timespan when an event has occurred that needs to be included in the report. This can be done by using the controls on the 2.4GHz or 5GHz band. Notice how the information displayed in the graphs on the right only displays the data within the timespan selected.



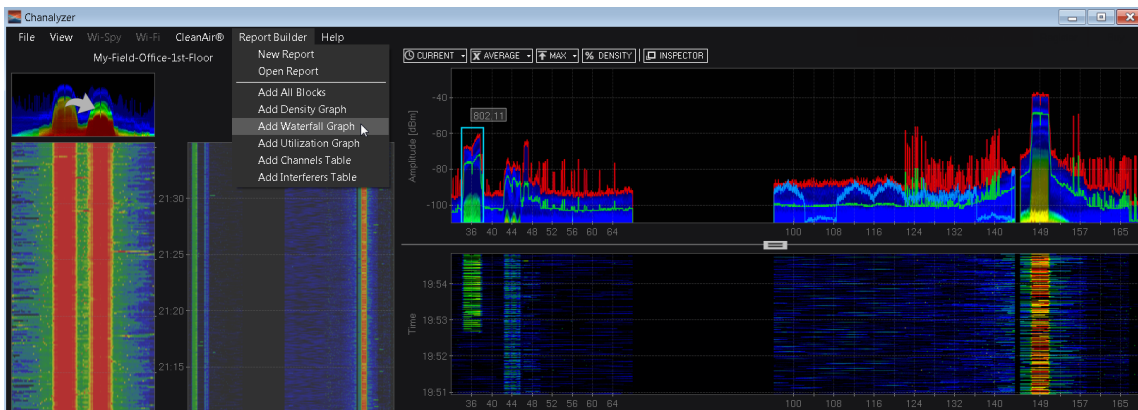
Step 2: Create a new report by navigating to Report Builder > New Report.



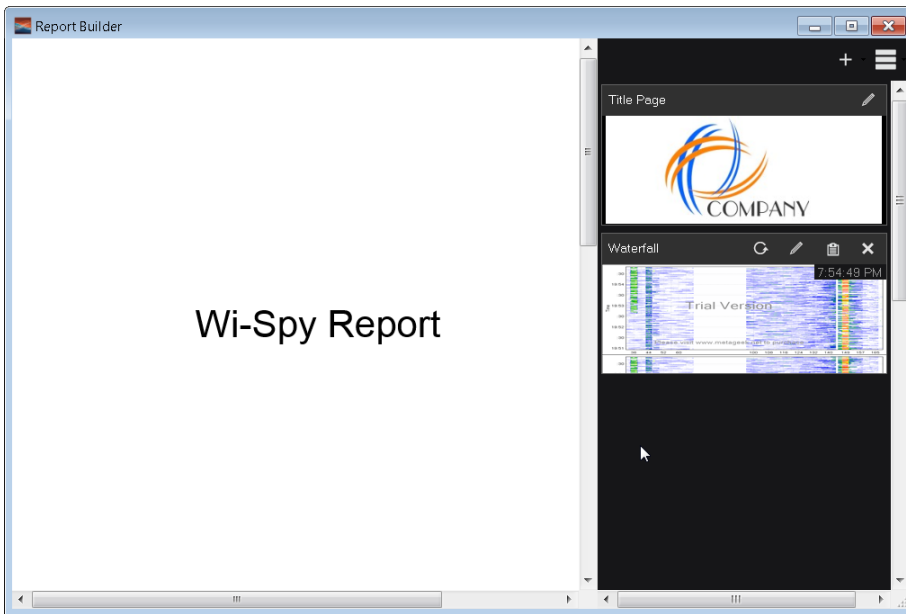
Step 3: A new report window will appear which will contain each of the graphs inserted and described in the following steps. It is possible to customize the title page by selecting edit pencil on the title screen shown on the right.



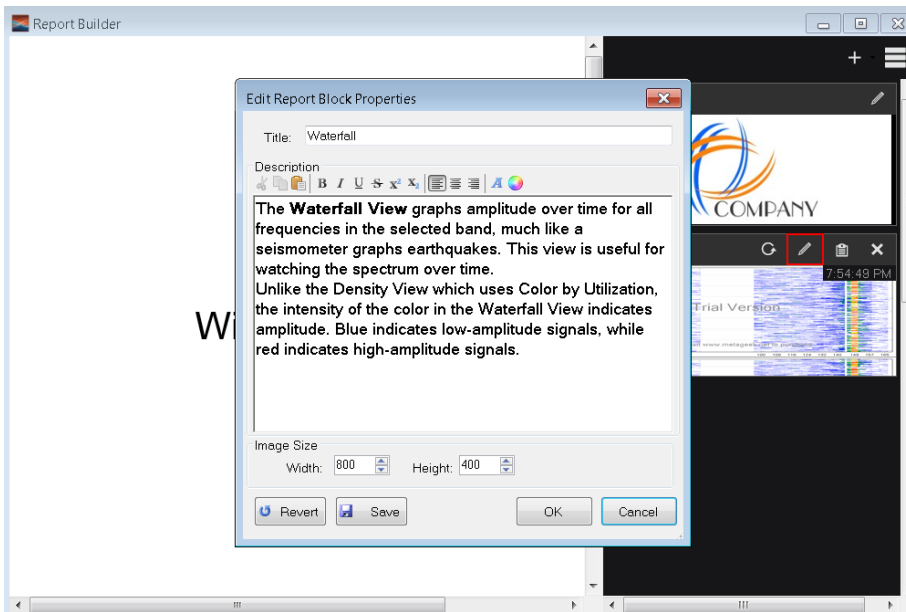
Step 4: In the example above, we see interference beginning on channel 36 as indicated by the start of a green line. To add the waterfall graph to the report select **Report Builder > Add Waterfall Graph**.



Step 5: In the report window, the waterfall graphic for the timespan selected has now been inserted as shown.

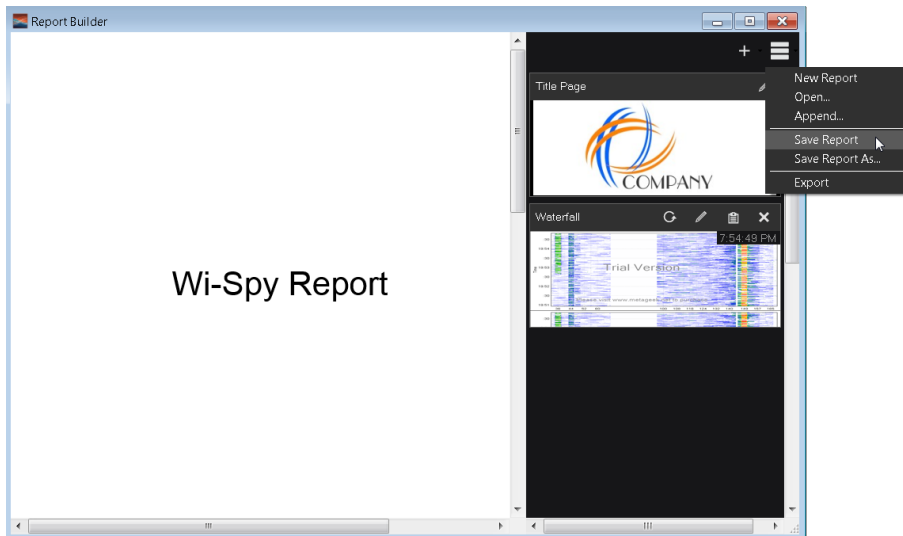


Step 6: To modify the text that appears with the Waterfall graphic in the report, select the edit pencil on the Waterfall graph. An example explanation of this event might be “The Waterfall graph shows the beginning of the interference from the adjacent retail operation (ABC Company) when they begin to scan arriving inventory using their Wi-Fi Direct enabled bar code scanners.”

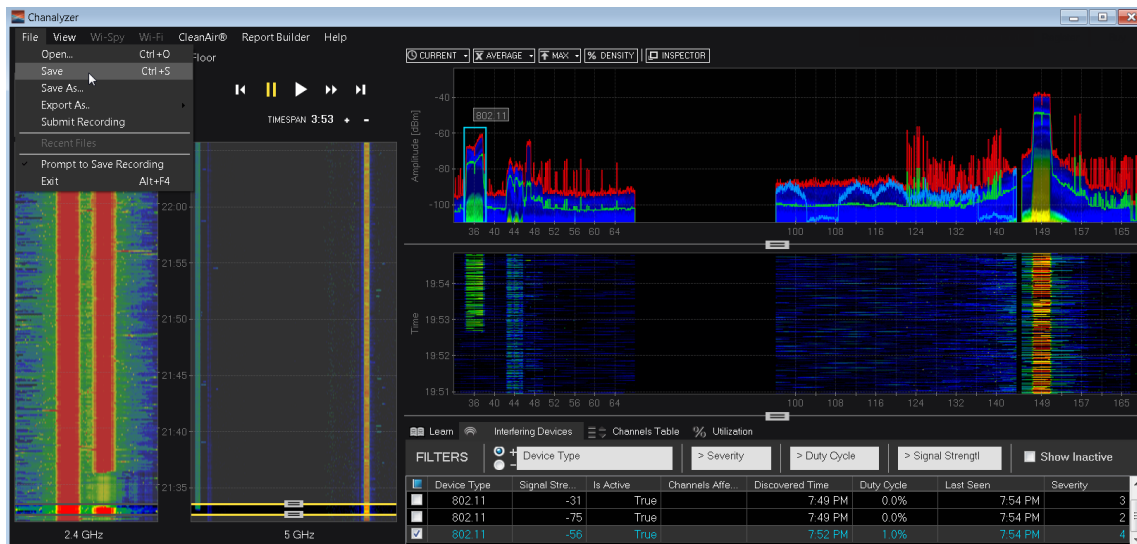


Additional graphs and timespans can be added to the report as necessary.

Step 7: Save the report by selecting the settings button and **Save Report**.



Step 8: Save the data collected for entire CleanAir session by navigating to **File > Save**.



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	7.6.110.0
	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 7500 Series Wireless Controller for up to 1000 Cisco 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 Virtual Wireless Controller 25 Access Point Adder License	L-LIC-CTVM-25A	
	Cisco Virtual Wireless Controller 5 Access Point Adder License	L-LIC-CTVM-5A	
	Cisco Virtual Wireless Controller 1 Access Point Adder License	L-LIC-CTVM-1A	
On Site, Remote Site, or Guest Controller	Cisco 5500 Series Wireless Controller for up to 500 Cisco access points	AIR-CT5508-500-K9	7.6.110.0
	Cisco 5500 Series Wireless Controller for up to 250 Cisco access points	AIR-CT5508-250-K9	
	Cisco 5500 Series Wireless Controller for up to 100 Cisco access points	AIR-CT5508-100-K9	
	Cisco 5500 Series Wireless Controller for up to 50 Cisco access points	AIR-CT5508-50-K9	
	Cisco 5500 Series Wireless Controller for up to 25 Cisco access points	AIR-CT5508-25-K9	
	Cisco 5500 Series Wireless Controller for up to 12 Cisco access points	AIR-CT5508-12-K9	
	Cisco 5500 Series Wireless Controller for High Availability	AIR-CT5508-HA-K9	
On Site Controller, Guest Controller	Cisco 2500 Series Wireless Controller for up to 50 Cisco access points	AIR-CT2504-50-K9	7.6.110.0
	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 3700 Series Access Point 802.11ac and CleanAir with Internal Antennas	AIR-CAP3702I-x-K9	7.6.110.0
	Cisco 3700 Series Access Point 802.11ac and CleanAir with External Antenna	AIR-CAP3702E-x-K9	
	Cisco 3600 Series Access Point Dual Band 802.11a/g/n and CleanAir with Internal Antennas	AIR-CAP3602I-x-K9	
	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	Cisco 802.11ac Wave 1 Module for 3600 Series Access Point	AIR-RM3000AC-x-K9=	–
	Cisco 802.11ac Wave 1 Module for 3600 Series Access Point 10 Pack	AIR-RM3000ACxK910=	–

Wireless LAN

Functional Area	Product Description	Part Numbers	Software
Wireless LAN	Cisco Mobility Services Engine (Virtual Appliance)	L-MSE-7.0-K9	7.6.110.0
	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-K9 [†]	1.4.1 [†]
	Cisco Prime Infrastructure 1.2 Base License and Software	R-PI12-BASE-K9 [†]	
	Cisco Prime Infrastructure 1.2 - Lifecycle - 10,000 Device License	L-PI12-LF-10K [†]	
	Cisco Prime Infrastructure 1.2 - Lifecycle - 5000 Device License	L-PI12-LF-5K [†]	
	Cisco Prime Infrastructure 1.2 - Lifecycle - 2500 Device License	L-PI12-LF-2.5K [†]	
	Cisco Prime Infrastructure 1.2 - Lifecycle - 1000 Device License	L-PI12-LF-1K [†]	
	Cisco Prime Infrastructure 1.2 - Lifecycle - 500 Device License	L-PI12-LF-500 [†]	
	Cisco Prime Infrastructure 1.2 - Lifecycle - 100 Device License	L-PI12-LF-100 [†]	
	Cisco Prime Infrastructure 1.2 - Lifecycle - 50 Device License	L-PI12-LF-50 [†]	
	Cisco Prime Infrastructure 1.2 - Lifecycle - 25 Device License	L-PI12-LF-25 [†]	
	MetaGeek Chanalyzer 5 with Report Builder and Cisco CleanAir	SFW-CHAN-RC	5.0.3.36
MetaGeek Chanalyzer 5	SFW-CHAN-500		
MetaGeek Cisco CleanAir Accessory for Chanalyzer 5	ACC-CHAN-CCA		

[†]To obtain Cisco Prime Infrastructure 1.4.1, order Cisco Prime Infrastructure 1.2 with a service contract and download Cisco Prime Infrastructure 1.4 and service pack 1 from Cisco.com. Existing customers with a valid service contract can also download Cisco Prime 1.4 and service pack 1. Customers without a valid service contract must purchase a service contract to gain access to the Prime Infrastructure 1.4 download on Cisco.com

Data Center Virtualization

Functional Area	Product Description	Part Numbers	Software
VMWare	ESXi	ESXi	5.0.0 Build 804277
	VMware vSphere	ESXi	

Appendix B: Changes

This appendix summarizes the changes Cisco made to this guide since its last edition.

- We added Cisco Prime Infrastructure 1.4.1 to support Cisco Wireless LAN Controller version 7.6110.0
- We added the Cisco Aironet 3700 Series Access Point, which supports IEEE 802.11ac, as a CleanAir access point (AIR-CAP3702I-x-K9 and AIR-CAP3702E-x-K9)
- We added the Cisco Aironet 3600 Series Access Point with the AIR-RM3000AC-x-K9 802.11ac radio module as a CleanAir access point
- We revised the configuration of Cisco CleanAir for access points and wireless LAN controllers to use Cisco Prime Infrastructure 1.4.1
- We refreshed the version of the Cisco Mobility Services Engine Virtual Appliance (MSE-VA) version 7.6.110.0
- Historical Cisco CleanAir spectrum intelligence data is presented using Cisco Prime Infrastructure 1.4.1
- We removed the Cisco Spectrum Expert software from the guide
- We added MetaGeek Chanalyzer software for use with Cisco CleanAir access points
- We provided troubleshooting guidance using MetaGeek Chanalyzer software
- We provided guidance for producing custom reports using MetaGeek Chanalyzer software
- We provided bandwidth utilization and connectivity using the MetaGeek Chanalyzer software
- We provided guidance on SE-Connect and local mode operation
- We included 802.11ac visibility using 80MHz bonded channels with the Cisco Aironet 3700 Series Access Point

Feedback

Please use the [feedback form](#) to send comments and suggestions about this guide.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

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

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

© 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)