



Campus CleanAir

Technology Design Guide

August 2014 Series



Table of Contents

Preface	1
CVD Navigator	2
Use Cases	2
Scope	2
Introduction	3
Technology Use Cases	3
Use Case: Proactive Interference Protection by Using Cisco CleanAir.....	3
Use Case: Historical RF Management by Using Cisco CleanAir and Cisco Prime Infrastructure	4
Use Case: CleanAir Spectrum Intelligence using MetaGeek Chanalyzer.....	4
Design Overview.....	4
Cisco CleanAir Technology.....	4
Cisco Prime Infrastructure	5
Deployment Details	6
Adding Buildings and Floor Plans to Cisco Prime Infrastructure	6
Configuring the Wireless Network for Cisco CleanAir.....	12
Installing the Cisco Mobility Services Engine Virtual Appliance	33
Configuring Cisco Prime Infrastructure for the Cisco MSE-VA.....	39
Troubleshooting with Cisco CleanAir	51
Viewing real-time and historical CleanAir using Prime Infrastructure	51
Viewing real-time CleanAir using MetaGeek’s Chanalyzer	56
Appendix A: Product List	72
Appendix B: Changes	75

Preface

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

CVDs include two guide types that provide tested design 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 existing CVDs but also include product features and functionality across Cisco products and sometimes 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.

CVD Foundation Series

This CVD Foundation guide is a part of the *August 2014 Series*. As Cisco develops a CVD Foundation series, the guides themselves are tested together, in the same network lab. This approach assures that the guides in a series are fully compatible with one another. Each series describes a lab-validated, complete system.

The CVD Foundation series incorporates wired and wireless LAN, WAN, data center, security, and network management technologies. Using the CVD Foundation simplifies system integration, allowing you to select solutions that solve an organization's problems—without worrying about the technical complexity.

To ensure the compatibility of designs in the CVD Foundation, you should use guides that belong to the same release. For the most recent CVD Foundation guides, please visit [the CVD Foundation web site](#).

Comments and Questions

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

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 CVD Foundation web site](#).

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 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 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 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

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 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 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

How to Read Commands

This guide uses the following conventions for commands that you enter at the command-line interface (CLI).

Commands to enter at a CLI prompt:

```
configure terminal
```

Commands that specify a value for a variable:

```
ntp server 10.10.48.17
```

Commands with variables that you must define:

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

Commands at a CLI or script prompt:

```
Router# enable
```

Long commands that line wrap are underlined.

Enter them as one command:

```
police rate 10000 pps burst 10000  
packets conform-action
```

Noteworthy parts of system output (or of device configuration files) are highlighted:

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

In order to use Cisco Prime Infrastructure to manage the Cisco wireless LAN controllers that are running Cisco AireOS, you must use a compatible version of Cisco Prime Infrastructure. Check the release notes for compatibility information. The versions used to validate this guide are shown in Appendix A: Product List. The procedures for properly installing and configuring Prime Infrastructure 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 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, visibility of this otherwise unknown or convoluted data that Prime Infrastructure 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.

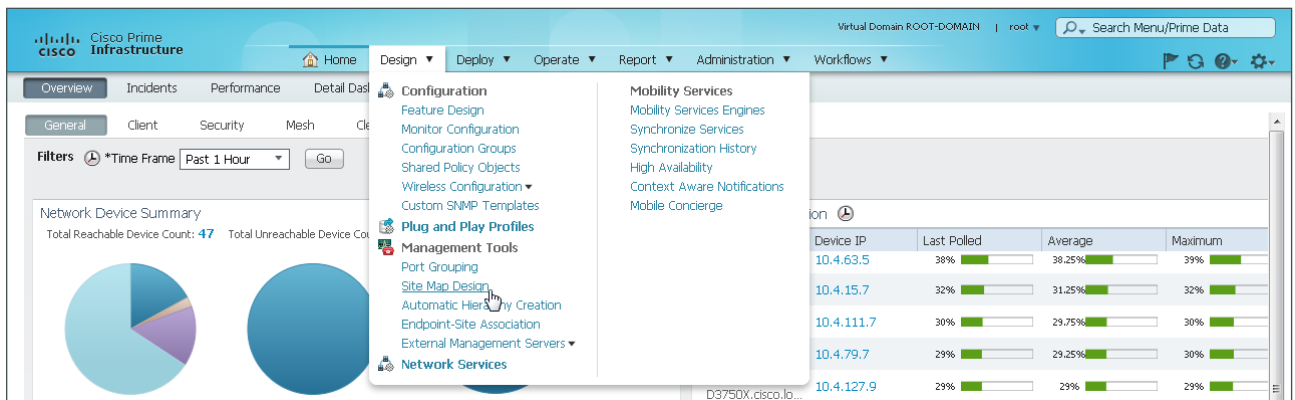
Procedure 1 Add the first campus and building

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.

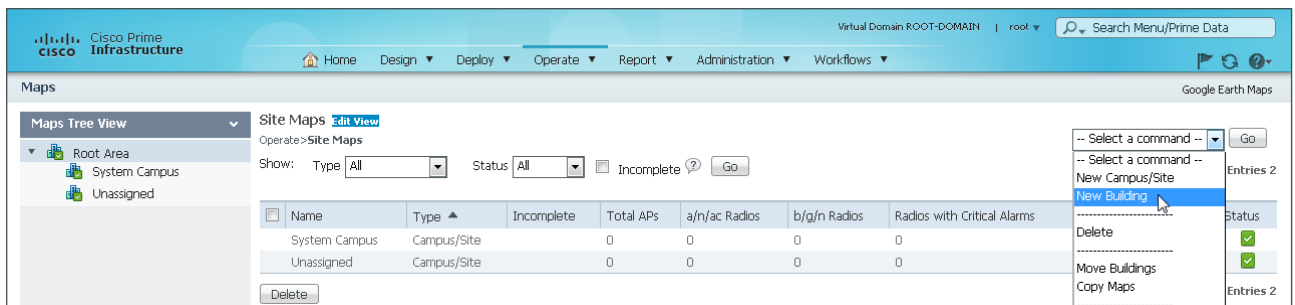
Tech Tip

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, navigate to **Design > Management Tools > Site Map Design**.



Step 2: At the top right, in the **Select a command** list, choose **New Building**, and then click **Go**.



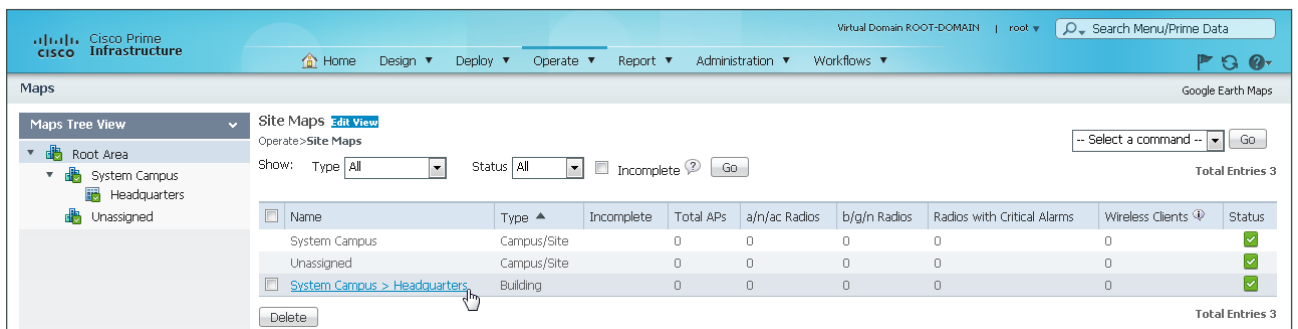
Step 3: Enter the following information about the building and then click **OK** to accept the updates:

- Building Name—**Headquarters**
- Contact—**Networking Team**
- Number of floors—**1**
- Number of Basements—**0**
- Horizontal Span (feet)—**360**
- Vertical Span (feet)—**300**
- 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.

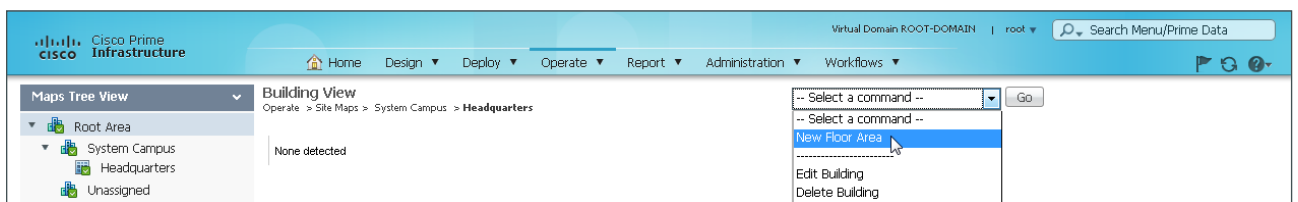
Step 4: Click the name of the newly created building. This selects the building.



The screenshot shows the Cisco Prime Infrastructure interface. The 'Maps' section is active, displaying a 'Site Maps' view. A table lists three entries: 'System Campus', 'Unassigned', and 'System Campus > Headquarters'. The 'System Campus > Headquarters' entry is selected, and a mouse cursor is hovering over it. The table columns include Name, Type, Incomplete, Total APs, a/h/ac Radios, b/g/n Radios, Radios with Critical Alarms, Wireless Clients, and Status.

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

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



The screenshot shows the Cisco Prime Infrastructure interface. The 'Building View' section is active, displaying a 'Building View' for 'System Campus > Headquarters'. A dropdown menu is open, showing a list of commands: '-- Select a command --', '-- Select a command --', 'New Floor Area', 'Edit Building', and 'Delete Building'. The 'New Floor Area' option is highlighted, and a mouse cursor is hovering over it.

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

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

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

New Floor Area
Operate > Site Maps > System Campus > Headquarters > New Floor Area First Floor

Floor Area Name:
Contact:
Floor:
Floor Type (RF Model):
Floor Height (feet):
Image File: **MyFloorPlan.png**
 Maintain Aspect Ratio

Dimensions(feet)
Horizontal Span:
Vertical Span:
Coordinates of top left corner(feet)
Horizontal Position:
Vertical Position:

Total Floor Area Size (sq. feet) : 92073.5
 Launch Map Editor after floor creation (To rescale floor and draw walls)

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

0 feet 50 100 150 200 250 300 350
0
50
100
150

The floor view appears for the new floor area you just created.

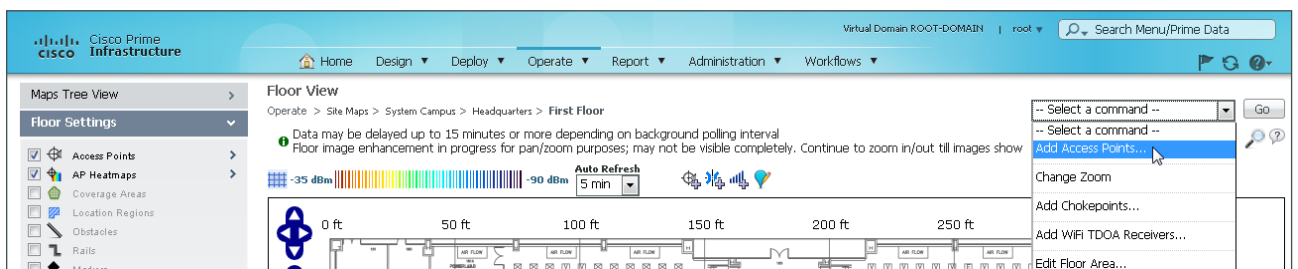


Procedure 2 Place access points on the map

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 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: At the top right, in the **Select a command** list, choose **Add Access Points**, and then click **Go**.



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

Virtual Domain ROOT-DOMAIN | root | Search Menu/Prime Data

Home Design Deploy Operate Report Administration Workflows

Add Access Points

Operate > Site Maps > System Campus > Headquarters > First Floor > Add Access Points

APs can be selected/added over multiple pages. Use Next/Previous to navigate and select APs to be added to Floor Area. APs can be searched by [Name/MacAddress (Ethernet/Radio)/IP]. IP search [primary by AP, fallback by Controller]. Searches are case insensitive

Search AP [Name/MacAddress (Ethernet/Radio)/IP]: Search

Add checked access points to Floor area 'First Floor'

AP Name	MAC Address	AP Model	Controller
<input checked="" type="checkbox"/> AP6c20.560e.3909	34:a8:4e:bb:f0:10	AIR-CAP1602I-A-K9	10.4.175.66
<input checked="" type="checkbox"/> AP6c20.560e.416d	34:a8:4e:c6:76:40	AIR-CAP1602I-A-K9	10.4.175.62
<input type="checkbox"/> APECC8.8288.2F70	ec:c8:82:c0:bd:90	AIR-OEAP602I-A-K9	192.168.19.20
<input type="checkbox"/> APECC8.8288.85B0	ec:c8:82:c2:16:a0	AIR-OEAP602I-A-K9	192.168.19.20
<input checked="" type="checkbox"/> APe4d3.f11e.a748	24:01:c7:f6:ad:30	AIR-CAP2602I-A-K9	10.4.175.66
<input checked="" type="checkbox"/> APf972.eaa7.0374	0c:f8:03:b9:3d:10	AIR-CAP2602E-A-K9	10.4.175.66
<input checked="" type="checkbox"/> APfc99.473e.1d31	20:3a:07:e5:50:10	AIR-CAP3602I-A-K9	10.4.175.66

Existing AP # 0 Selected AP # 5 Total AP # 5

OK Cancel

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**.

Virtual Domain ROOT-DOMAIN | root | Search Menu/Prime Data

Home Design Deploy Operate Report Administration Workflows

Selected AP Details

AP: APe4d3.f11e.a748
 MacAddress: 24:01:c7:f6:ad:30
 AP Model: AIR-CAP2602I-A-K9
 Protocol: 802.11a/n/ac
 Horiz: 314.177
 Vert: 11.3242
 AP Height: 10
 Antenna: Internal-2600-5GHz
 Antenna/AP Image:

Floor View

Operate > Site Maps > System Campus > Headquarters > First Floor

APe4d3.f11e.a748 (24:01:c7:f6:ad:30)

200 ft 250 ft 300 ft 350 ft

AIR FLOW

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

Virtual Domain ROOT-DOMAIN | root | Search Menu/Prime Data

Home Design Deploy Operate Report Administration Workflows

Selected AP Details

AP: AP6c20.560e.3909
 MacAddress: 34:a8:4e:bb:f0:10
 AP Model: AIR-CAP1602I-A-K9
 Protocol: 802.11a/n/ac
 Horiz: 313.8
 Vert: 11.9
 AP Height: 10
 Antenna: Internal-1602-5GHz

Floor View

Operate > Site Maps > System Campus > Headquarters > First Floor

Please wait...

RF Prediction is recomputed for newly positioned APs. This operation can take a long time depending on the number of APs and the number of walls.

Configuring the Wireless Network for Cisco CleanAir

1. Create a Cisco CleanAir access point template
2. Apply the Cisco CleanAir access point template
3. Create controller EDRRM templates
4. Deploy EDRRM
5. 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.

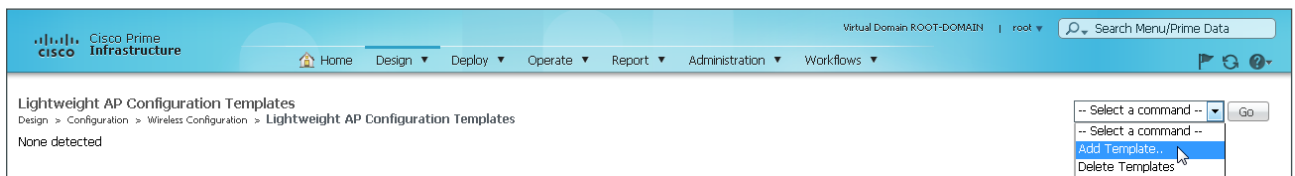
Cisco Prime Infrastructure can handle all management tasks within the network. You can still perform management tasks at each individual controller, but that approach is not recommended, as it often results in a fragmented configuration. With the Cisco CleanAir access point operating from the wireless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

Procedure 1 Create a Cisco CleanAir access point template

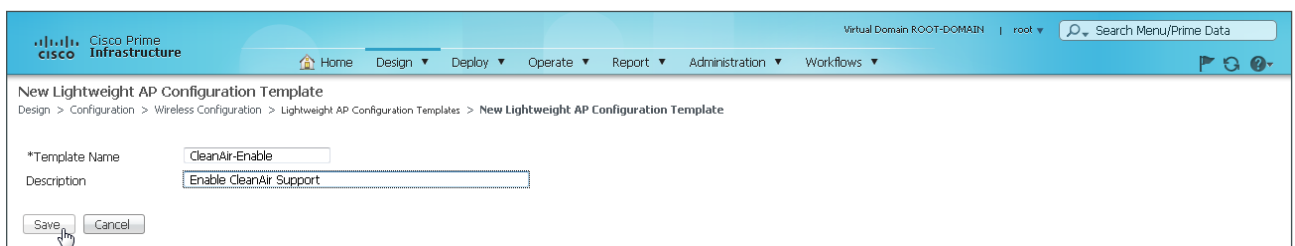
The first step in order to turn on Cisco CleanAir is to ensure that Cisco CleanAir is enabled on each of the access points (APs) for both 2.4 and 5 GHz bands. The following steps outline how to create a template within Cisco Prime Infrastructure to enable CleanAir on an access point.

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

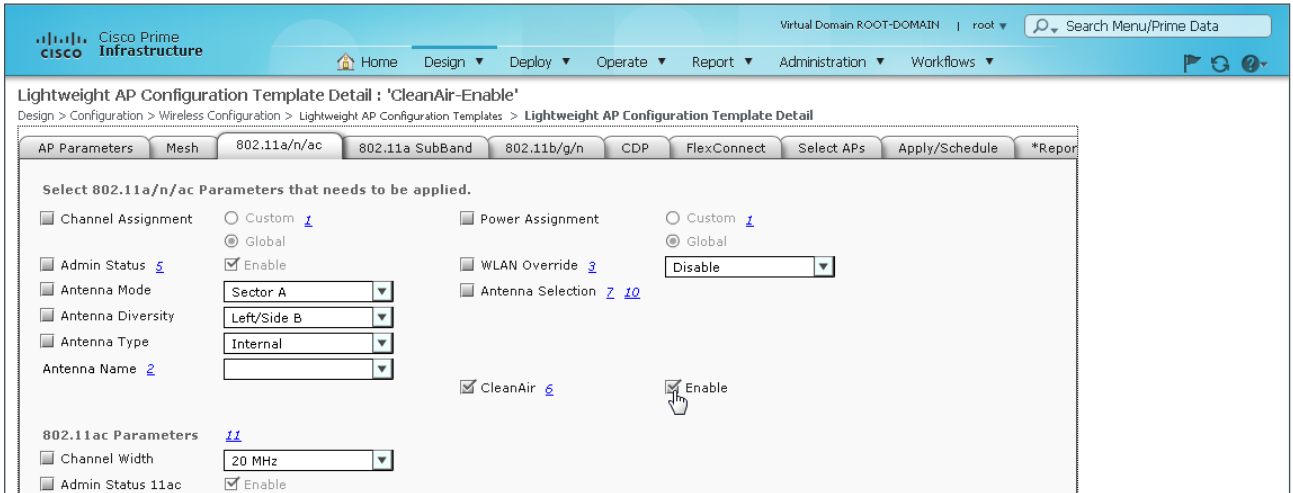
Step 2: In the **Select a command** list, choose **Add Template**, and then click **Go**.



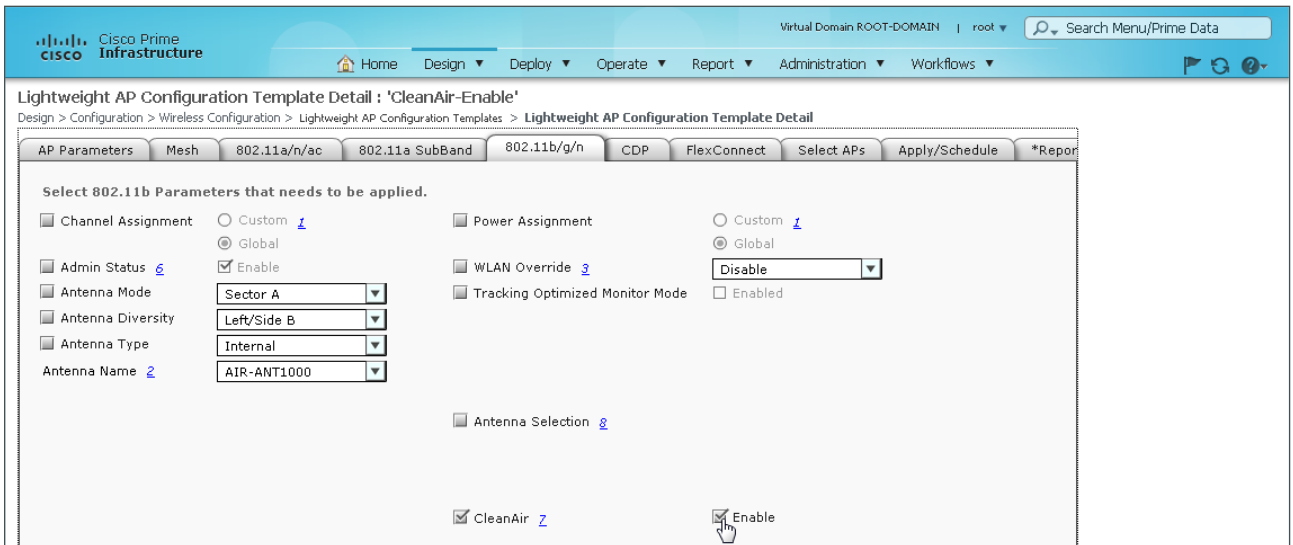
Step 3: In the **Template Name** box, enter a name, in the **Description** box, enter a description, and then click **Save**.



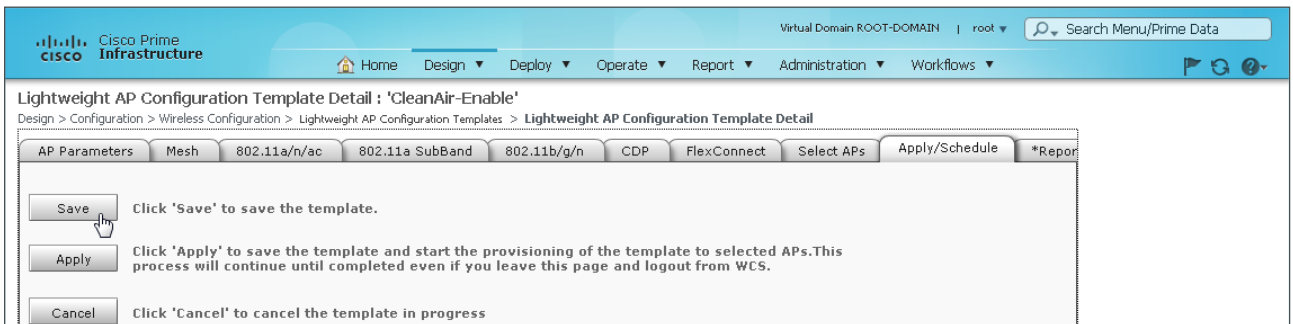
Step 4: On the 802.11a/n/ac tab, ensure that both **CleanAir** and **Enable** are selected.



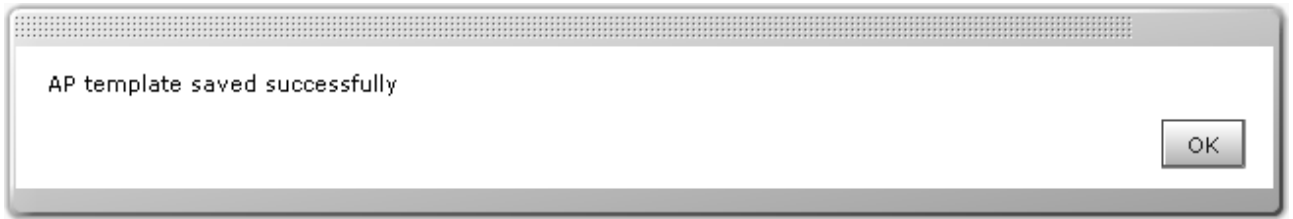
Step 5: On the 802.11b/g/n tab, ensure that both **CleanAir** and **Enable** are selected.



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



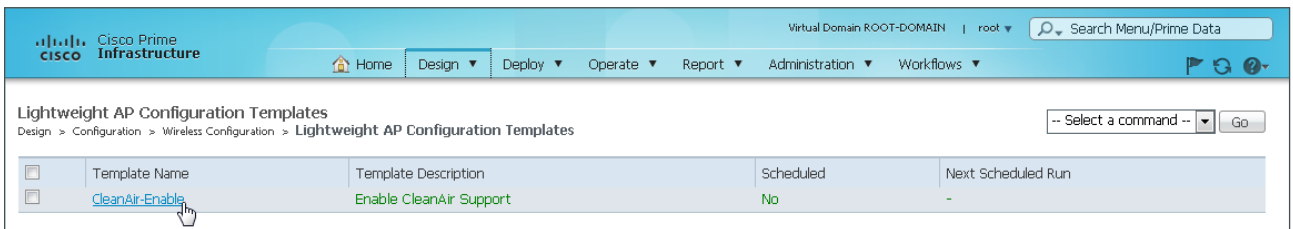
The created access point configuration template for CleanAir is saved.



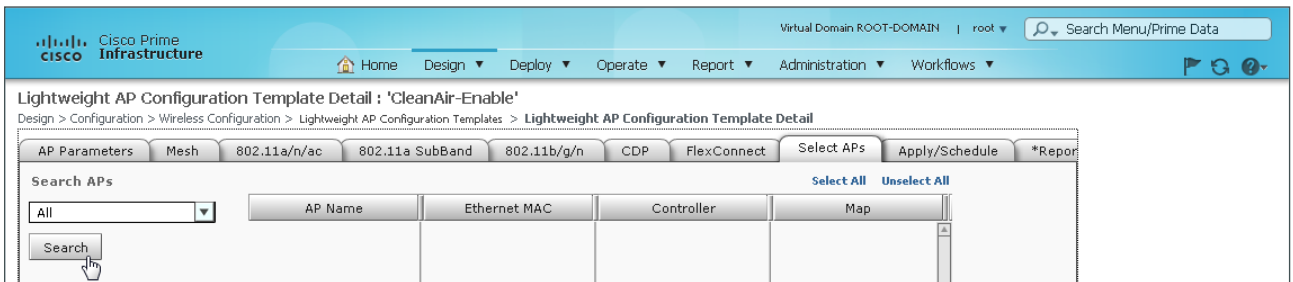
Procedure 2 Apply the Cisco CleanAir access point template

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

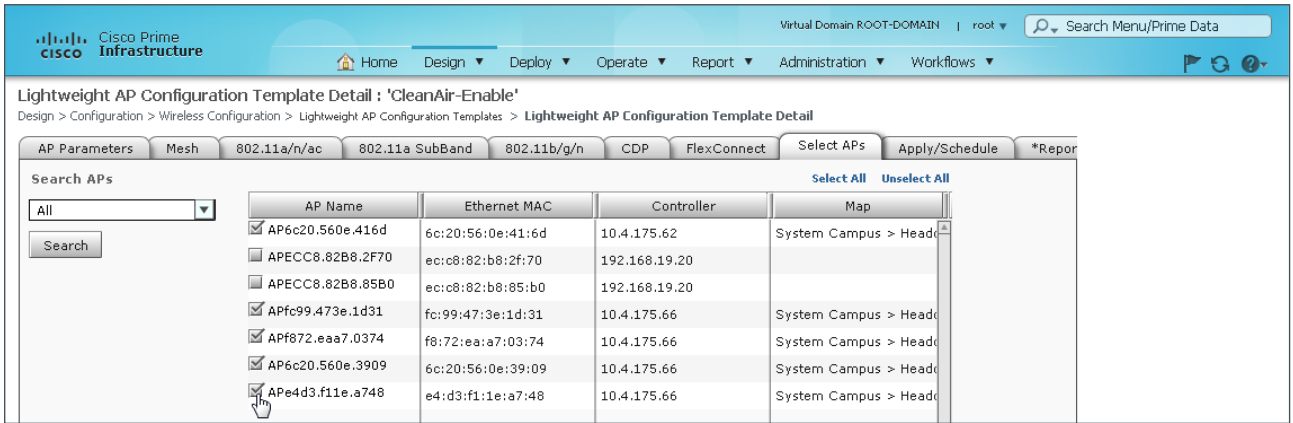
Step 2: From the list of defined templates, choose the template that you created in Step 3 of the previous procedure (Example: CleanAir-Enable).



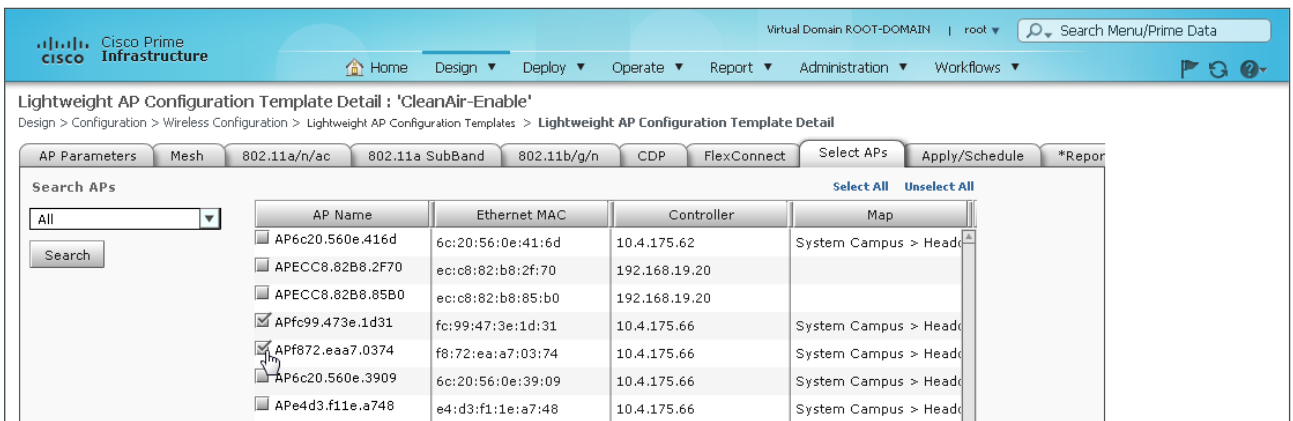
Step 3: On the **Select APs** tab, in the **Search APs** list, choose **All**, and then click **Search**. By default, all access points are selected.



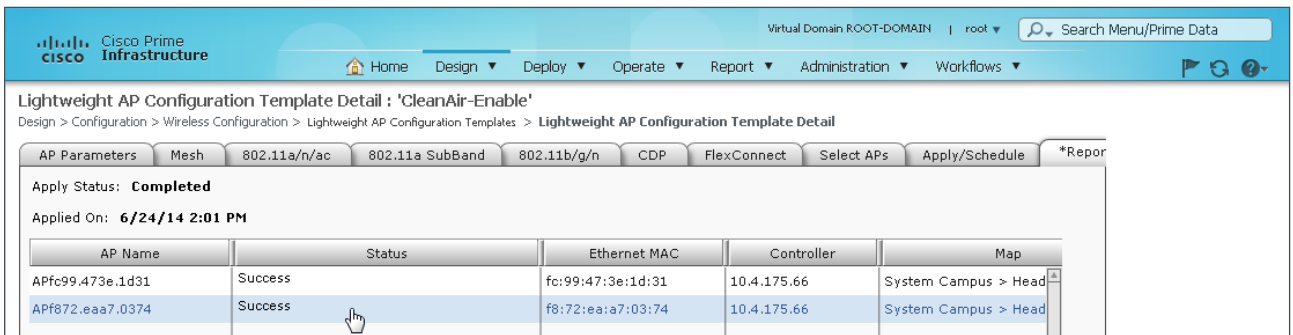
If you want to enable only certain access points, click **Unselect All**, and then individually select the access points you want to enable.



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



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



If the CleanAir Enable template is not successfully applied, ensure that in Cisco Prime Infrastructure:

- The SNMP Read/Write Community string for the WLC is correct.
- Under **Operate > Device Work Center**, and then on the left **Device Type > Wireless Controller**, the WLC Audit Status listed for the controller associated with the access point is **Identical**. If the status is **Mismatched**, running a new sync for the wireless controller device can help.

Procedure 3 Create controller EDRRM templates

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, and first you must enable Cisco CleanAir, as described in the previous procedures.

In this procedure, you create templates that are used to enable EDRRM for both the 2.4 and 5Ghz bands, which changes the behavior of Dynamic Channel Assignment (DCA). When you make changes to DCA, you must disable the radio resources before applying the changes. You also create the templates to disable and enable the radio resources to allow the EDRRM change, for a total of six templates to cover both bands.

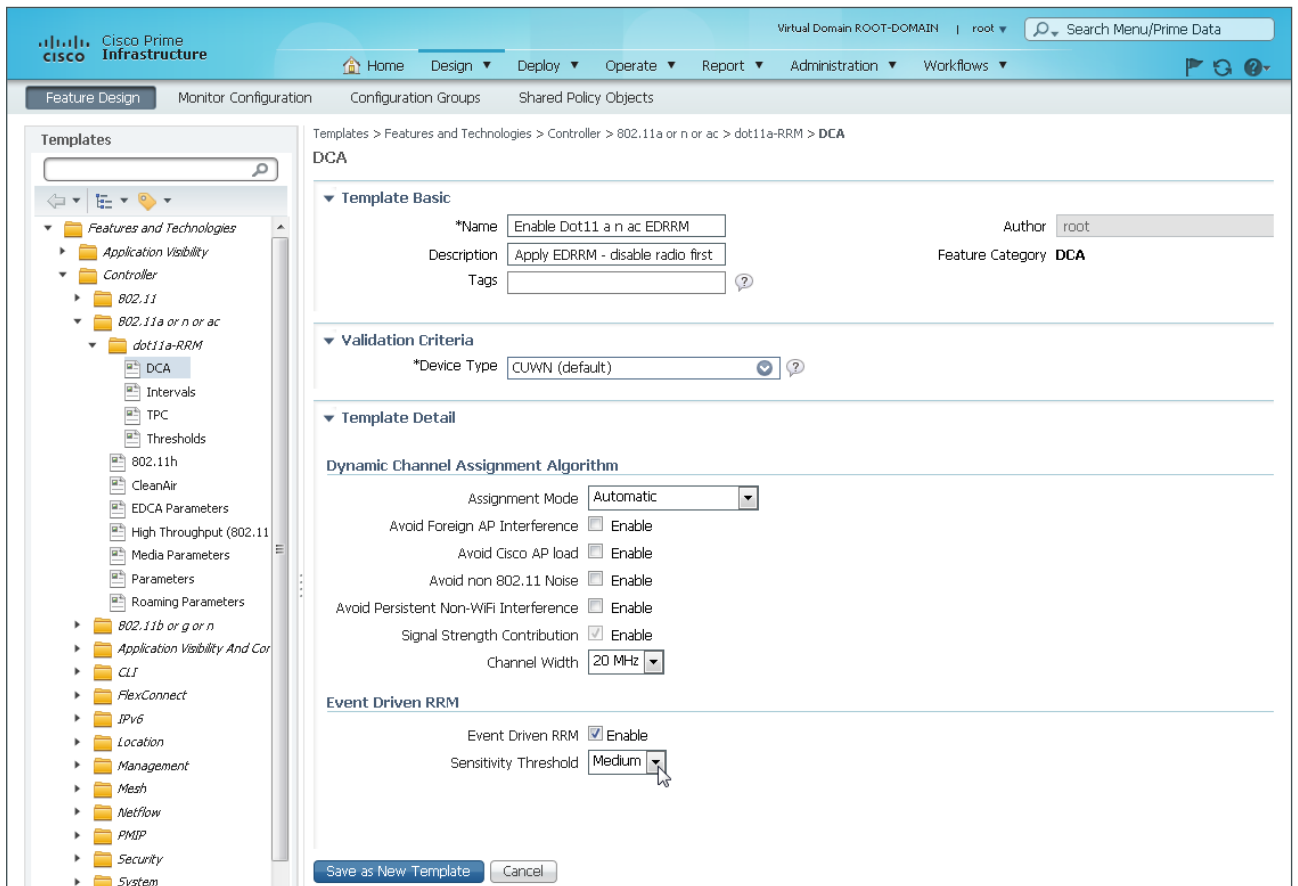


Tech Tip

In the next procedure, you use the templates you are creating here to disable the radio resources, apply the EDRRM change for DCA, and then enable the radio resources again.

Step 1: In Cisco Prime Infrastructure, navigate to **Design > Configuration > Feature Design**, and then, in the tree on the left, navigate to **Features and Technologies > Controller > 802.11a or n or ac > dot11a-RRM**, and then select the **DCA** feature template.

Step 2: Without using illegal characters such as “/” or “.”, provide a meaningful name for the template (Example: Enable Dot11 a n ac EDRRM). In the **Assignment Mode** list, choose **Automatic**, for Event Driven RRM, select **Enable**, and then in the **Sensitivity Threshold** list, choose **Medium**.

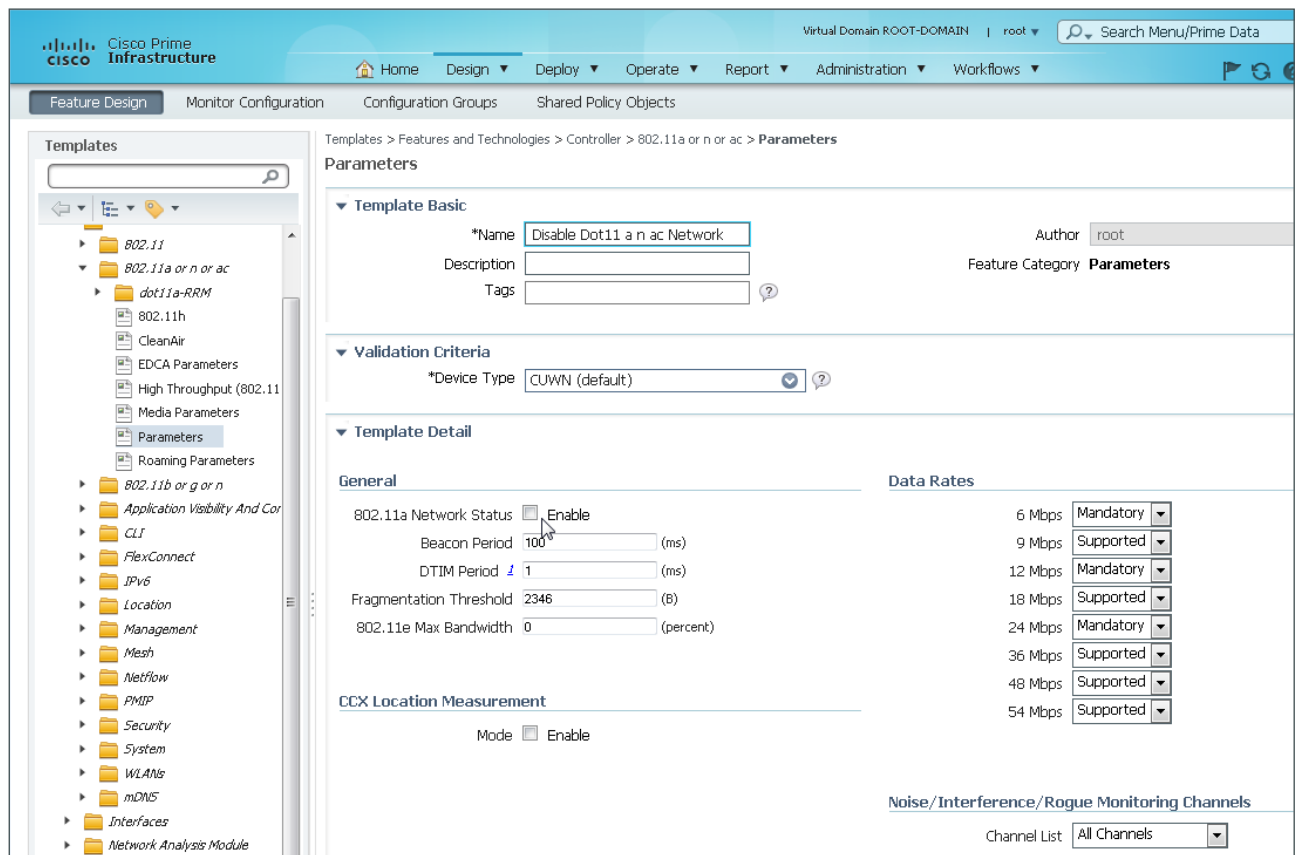


Step 3: Click **Save as New Template**, and then, on the Save Template dialog box, click **Save**. This saves the template in the default My Templates folder.

Step 4: In the tree on the left, navigate to **Features and Technologies > Controller > 802.11a or n or ac**, and then select the **Parameters** feature template, used to enable and disable Network Status.

Step 5: Provide a meaningful name for the template (Example: Disable Dot11 a n ac Network).

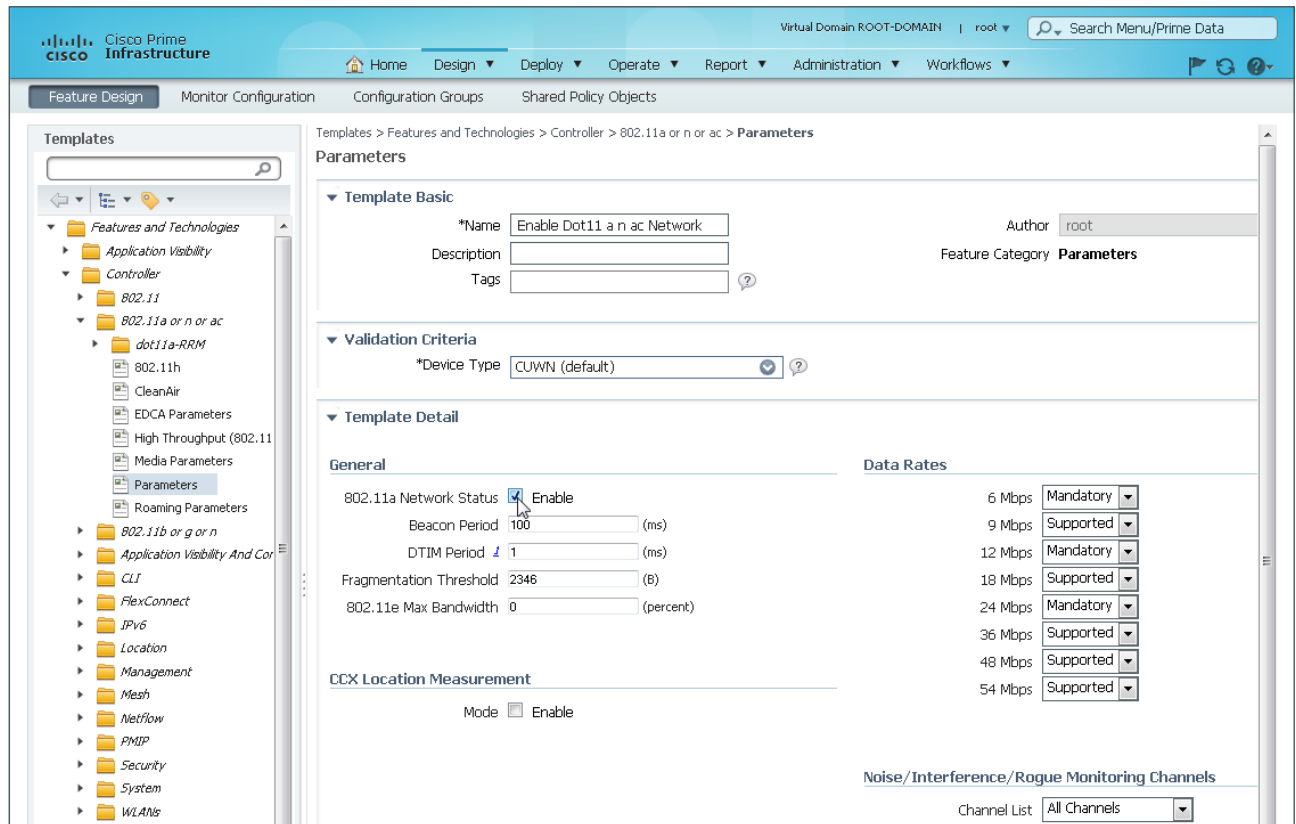
Step 6: In the **General** section, make sure **Enable** is cleared.



Step 7: Click **Save as New Template**, and then, on the Save Template dialog box, click **Save**. This saves the template in the default My Templates folder.

Step 8: For a second time, in the tree on the left, navigate to **Features and Technologies > Controller > 802.11a or n or ac**, and then select the **Parameters** feature template.

Step 9: Provide a meaningful name for the template (Example: Enable Dot11 a n ac Network). In the **General** section, select **Enable**.



Step 10: Click **Save as New Template**, and then, on the Save Template dialog box, click **Save**. This saves the template in the default My Templates folder.

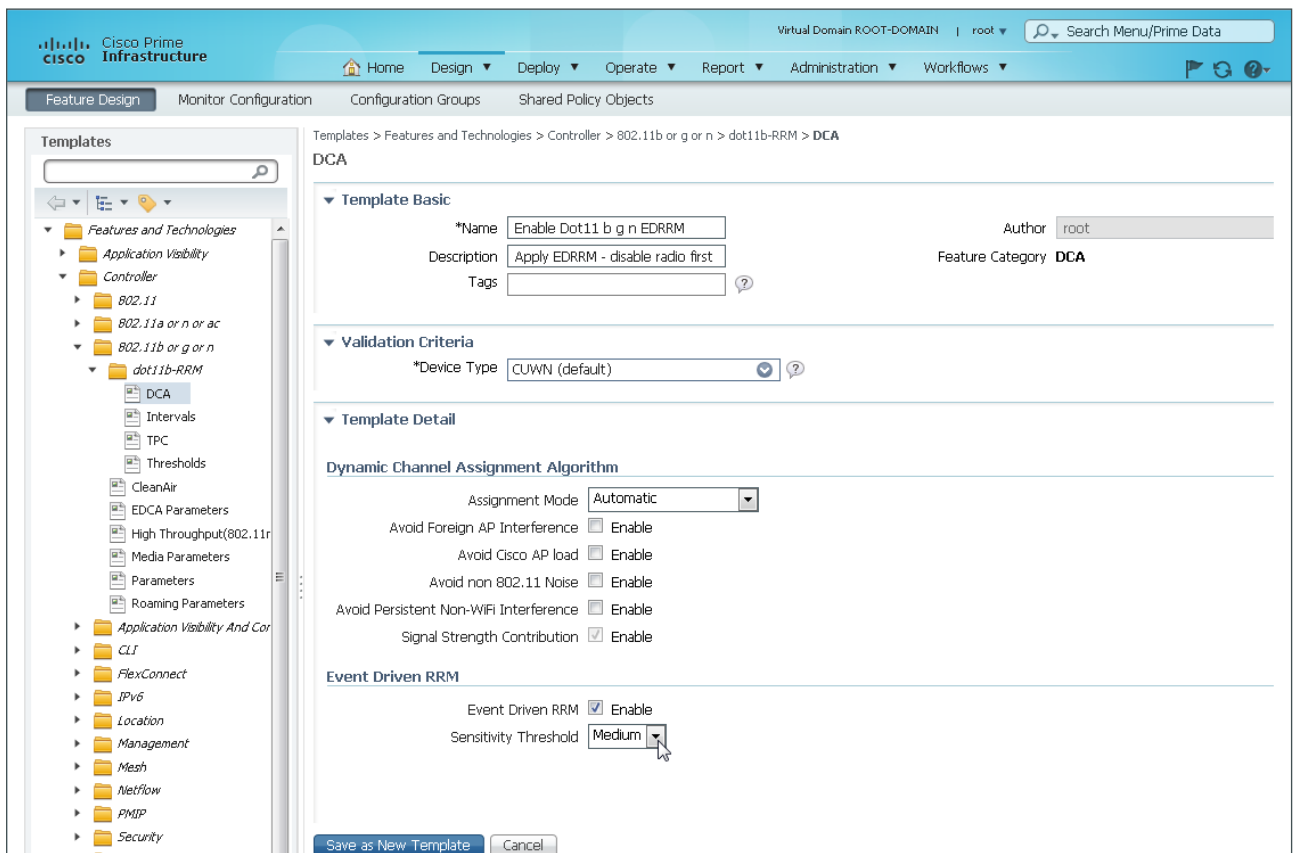
Step 11: In the tree on the left, navigate to **Features and Technologies > Controller > 802.11b or g or n > dot11b-RRM**, and then select the **DCA** feature template.

Step 12: Provide a meaningful name for the template (Example: Enable Dot11 b g n EDRRM).

Step 13: In the **Assignment Mode** list, choose **Automatic**.

Step 14: For Event Driven RRM, select **Enable**.

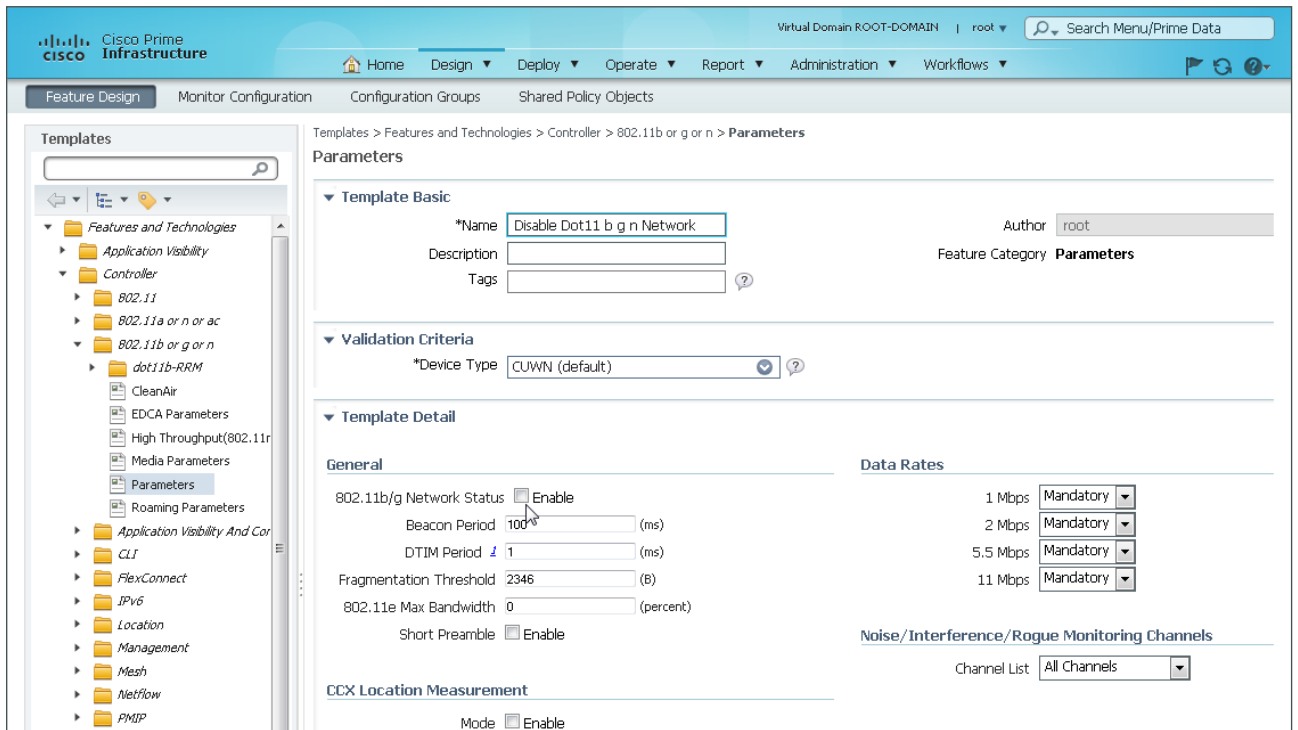
Step 15: In the **Sensitivity Threshold** list, choose **Medium**.



Step 16: Click **Save as New Template**, and then, on the Save Template dialog box, click **Save**. This saves the template in the default My Templates folder.

Step 17: In the tree on the left, navigate to **Features and Technologies > Controller > 802.11b or g or n**, and then select the **Parameters** feature template.

Step 18: Provide a meaningful name for the template (Example: Disable Dot11 b g n Network). In the General section, next to 802.11b/g Network Status, make sure **Enable** is cleared.



Step 19: Click **Save as New Template**, and then, on the Save Template dialog box, click **Save**. This saves the template in the default My Templates folder.

Step 20: For a second time, in the tree on the left, navigate to **Features and Technologies > Controller > 802.11b or g or n**, and then select the **Parameters** feature template.

Step 21: Provide a meaningful name for the template (Example: Enable Dot11 b g n Network). In the General section, next to 802.11b/g Network Status, select **Enable**.

The screenshot displays the Cisco Prime Infrastructure configuration interface. The breadcrumb path is: Templates > Features and Technologies > Controller > 802.11b or g or n > Parameters. The left sidebar shows a tree view of templates, with 'Parameters' selected under '802.11b or g or n'. The main content area is titled 'Parameters' and is divided into several sections:

- Template Basic:** *Name: Enable Dot11 b g n Network; Author: root; Feature Category: Parameters.
- Validation Criteria:** *Device Type: CUWN (default).
- Template Detail:**
 - General:** 802.11b/g Network Status: Enable; 802.11g Support: Enable; Beacon Period: 100 (ms); DTIM Period: 1 (ms); Fragmentation Threshold: 2346 (B); 802.11e Max Bandwidth: 0 (percent); Short Preamble: Enable.
 - Data Rates:** 1 Mbps: Mandatory; 2 Mbps: Mandatory; 5.5 Mbps: Mandatory; 11 Mbps: Mandatory.
 - Noise/Interference/Rogue Monitoring Channels:** Channel List: All Channels.
 - CCX Location Measurement:** Mode: Enable.

Step 22: Click **Save as New Template**, and then, on the Save Template dialog box, click **Save**. This saves the template in the default My Templates folder.

Procedure 4 Deploy EDRRM

You use the templates you created in the previous procedure to disable the radio resources, apply the EDRRM change for DCA, and then enable the radio resources again.

Caution

Disabling the radio resources causes a loss of network service for clients that were using the devices during the change.

Step 1: Navigate to **Design > Configuration > Feature Design**, and then in the tree on the left, navigate to **My Templates**, select the template you created to disable the 5GHz network (Example: Disable Dot11 a n ac Network), and click **Deploy**.

The screenshot displays the Cisco Prime Infrastructure web interface. The top navigation bar includes 'Home', 'Design', 'Deploy', 'Operate', 'Report', 'Administration', and 'Workflows'. The current page is 'Feature Design' under 'Configuration Groups'.

The left sidebar shows a tree view of templates under 'My Templates' > 'Discovered Templates'. The selected template is 'Disable Dot11 a n ac Network'.

The main content area shows the configuration for the 'Disable Dot11 a n ac Network' template. The breadcrumb is 'Templates > My Templates > Disable Dot11 a n ac Network'.

Template Basic

- *Name: Disable Dot11 a n ac Network
- Description: [Empty field]
- Tags: [Empty field]
- Author: root
- Feature Category: Parameters

Validation Criteria

- *Device Type: CUWN (default)

Template Detail

General

- Applied To Controllers: 0
- 802.11a Network Status: Enable
- Beacon Period: 100 (ms)
- DTIM Period: 1 (ms)
- Fragmentation Threshold: 2346 (B)
- 802.11e Max Bandwidth: 0 (percent)

Data Rates

- 6 Mbps: Mandatory
- 9 Mbps: Supported
- 12 Mbps: Mandatory
- 18 Mbps: Supported
- 24 Mbps: Mandatory
- 36 Mbps: Supported
- 48 Mbps: Supported
- 54 Mbps: Supported

CCX Location Measurement

- Mode: Enable

Noise/Interference/Rogue Monitoring Channels

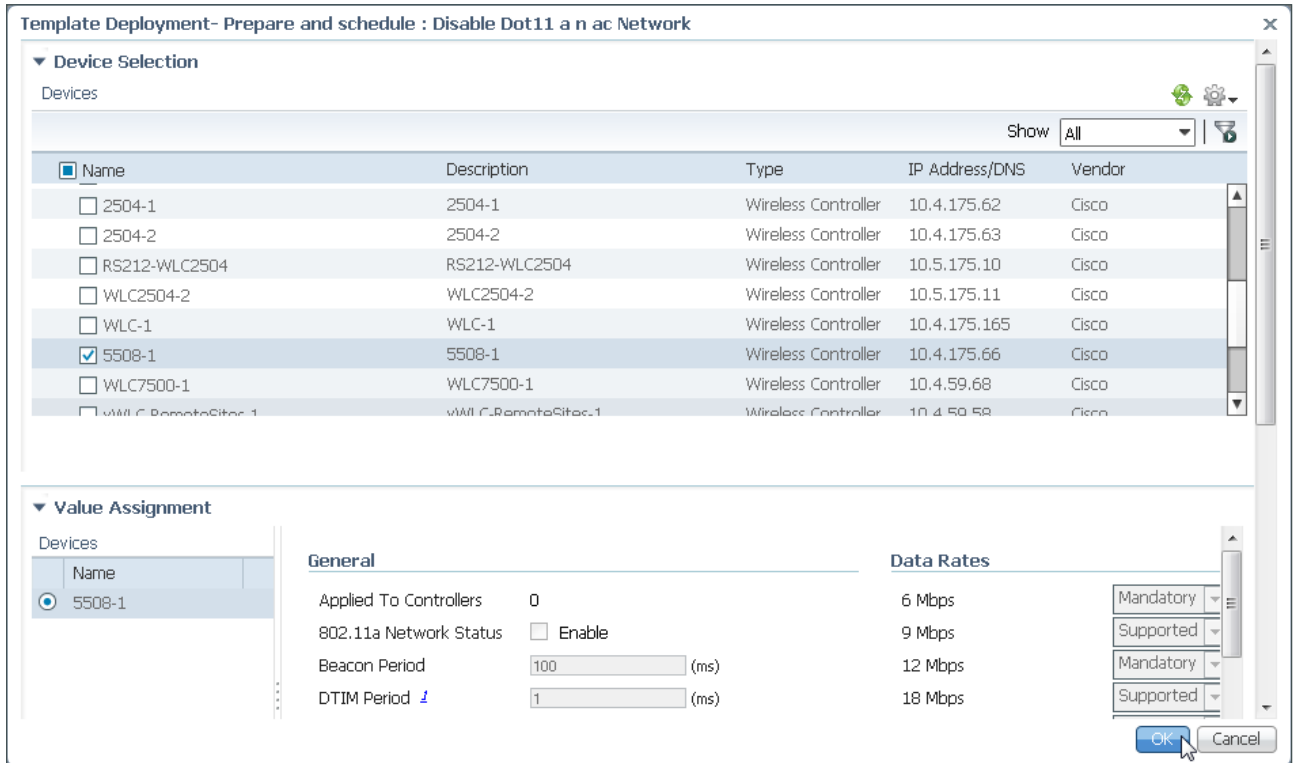
- Channel List: All Channels

Footnotes:

- DTIM period is not applicable from 5.0.0.0 version of controller.
- CCX Location Measurement Interval can be changed only when measurement mode is enabled.

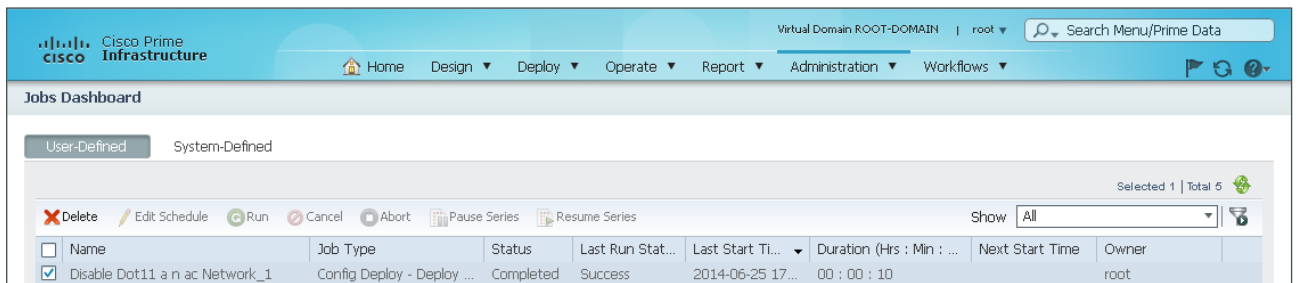
At the bottom, there are buttons for 'Save', 'Save as New Template', 'Cancel', 'Publish', and 'Deploy'.

Step 2: In the **Template Deployment** box, in the **Device Selection** section, select the controllers for EDRRM deployment, and click **OK**.

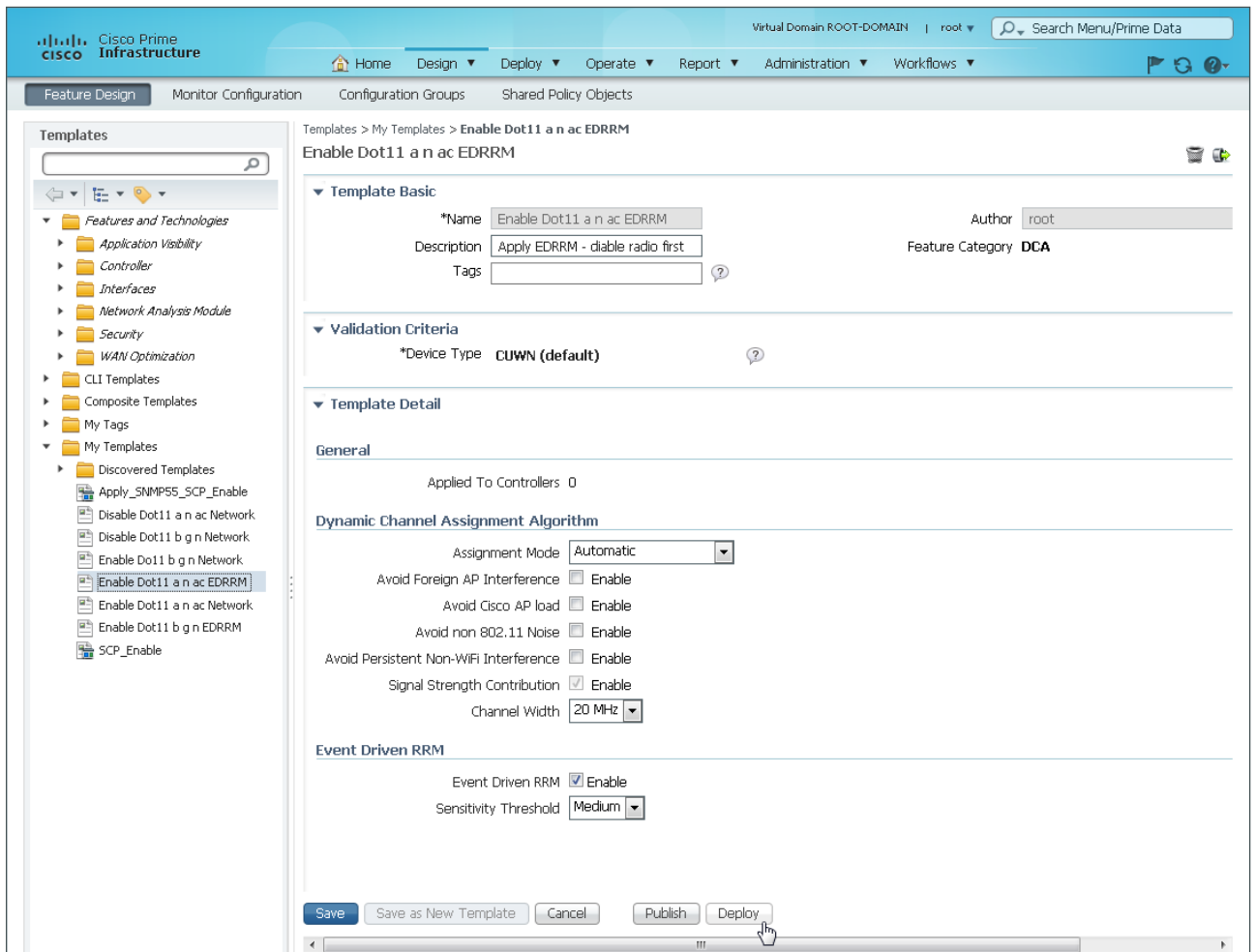


The Schedule parameters default to **Now**, so the template deployment starts immediately.

Step 3: If you want to check the job status, you can navigate to **Administration > Jobs Dashboard**.



Step 4: After the job has completed, navigate to **Design > Configuration > Feature Design**, and then in the tree on the left, navigate to **My Templates**, select the template you created to enable EDRRM for the 5GHz band (Example: Enable Dot11 a n ac EDRRM), and click **Deploy**.



Step 5: In the **Template Deployment** box, in the **Device Selection** section, select the controllers for EDRRM deployment, and click **OK**.

Template Deployment- Prepare and schedule : Enable Dot11 a n ac EDRRM

<input type="checkbox"/>	DMZ-WLC5508-Guest-1	DMZ-WLC5508-Guest-1	Wireless Controller	192.168.19.54	Cisco
<input checked="" type="checkbox"/>	5508-1	5508-1	Wireless Controller	10.4.175.66	Cisco
<input type="checkbox"/>	Cisco Wireless Services Module 2 (WIS...	Cisco Wireless Services Module 2 (Wi			

▼ Value Assignment

Devices

Name	
5508-1	

Avoid Cisco AP load Enable

Avoid non 802.11 Noise Enable

Avoid Persistent Non-WiFi Interference Enable

Signal Strength Contribution Enable

Channel Width 20 MHz

Event Driven RRM

Event Driven RRM Enable

Sensitivity Threshold Medium

▼ Schedule

Job Name Enable Dot11 a n ac EDRRM_1

Start Time Now Date 06/25/2014 05:42 PM (MM/dd/yyyy hh:mm AM/PM)

OK Cancel

The Schedule parameters default to **Now**, so the template deployment starts immediately.

Step 6: If you want to check the job status, you can navigate to **Administration > Jobs Dashboard**.

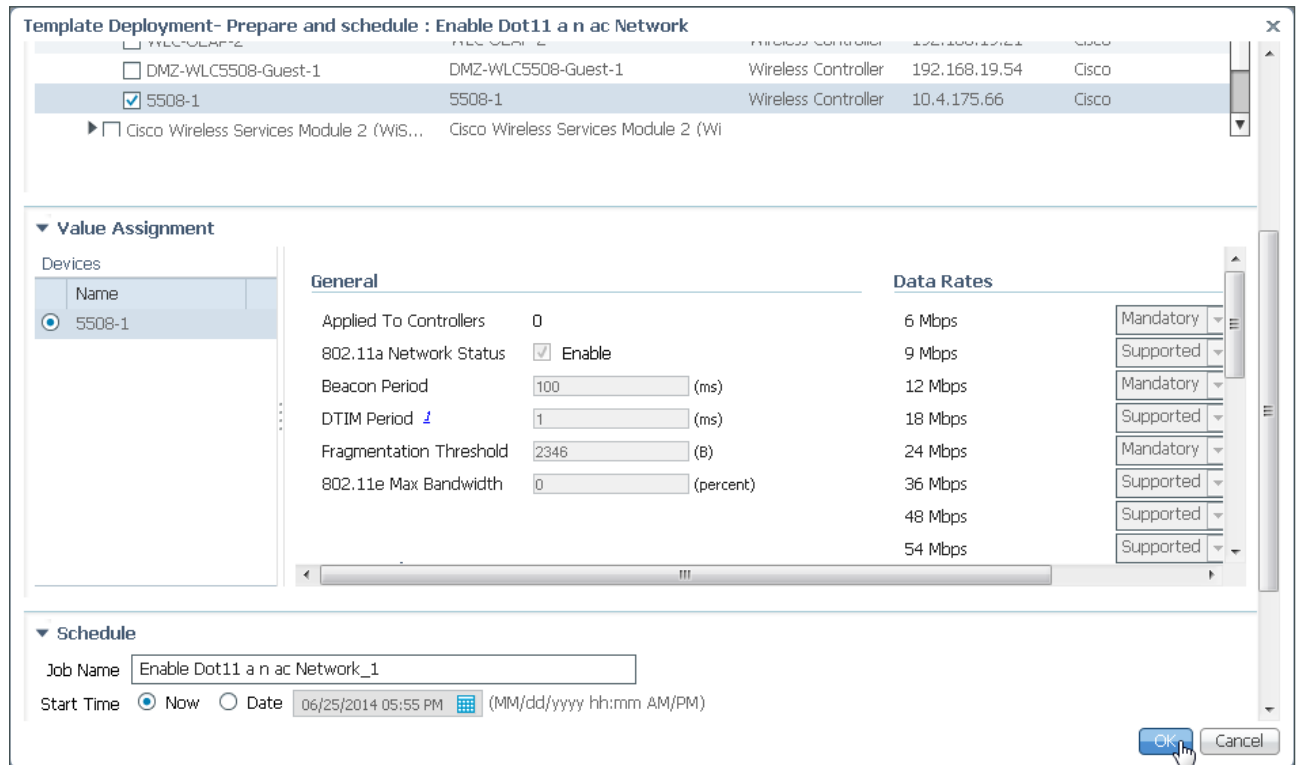
Step 7: After the job has completed, in the top menu, navigate to **Design > Feature Design**, and then in the tree on the left, navigate to **My Templates**, and select the template you created to enable the 5GHz network (Example: Enable Dot11 a n ac Network), and click **Deploy**.

The screenshot displays the Cisco Prime Infrastructure web interface for configuring a template. The breadcrumb trail is **Templates > My Templates > Enable Dot11 a n ac Network**. The main content area is titled **Enable Dot11 a n ac Network** and contains the following sections:

- Template Basic:**
 - *Name: Enable Dot11 a n ac Network
 - Description: (empty field)
 - Tags: (empty field)
 - Author: root
 - Feature Category: Parameters
- Validation Criteria:**
 - *Device Type: CUWN (default)
- Template Detail:**
 - General:**
 - Applied To Controllers: 0
 - 802.11a Network Status: Enable
 - Beacon Period: 100 (ms)
 - DTIM Period: 1 (ms)
 - Fragmentation Threshold: 2346 (B)
 - 802.11e Max Bandwidth: 0 (percent)
 - Data Rates:**
 - 6 Mbps: Mandatory
 - 9 Mbps: Supported
 - 12 Mbps: Mandatory
 - 18 Mbps: Supported
 - 24 Mbps: Mandatory
 - 36 Mbps: Supported
 - 48 Mbps: Supported
 - 54 Mbps: Supported
 - CCX Location Measurement:**
 - Mode: Enable
 - Noise/Interference/Rogue Monitoring Channels:**
 - Channel List: All Channels
- Footnotes:**
 - DTIM period is not applicable from 5.0.0.0 version of controller.
 - CCX Location Measurement Interval can be changed only when measurement mode is enabled.

At the bottom of the page, there are buttons for **Save**, **Save as New Template**, **Cancel**, **Publish**, and **Deploy**. A mouse cursor is pointing at the **Deploy** button.

Step 8: In the **Template Deployment** box, in the **Device Selection** section, select the controllers for EDRRM deployment, and click **OK**.



The Schedule parameters default to **Now**, so the template deployment starts immediately.

Step 9: If you want to check the job status, you can navigate to **Administration > Jobs Dashboard**.

Once the job is complete, you have enabled EDRRM for the 5GHz band. You now repeat the steps for the 2.4GHz band.

Step 10: Navigate to **Design > Configuration > Feature Design**, and then in the tree on the left, navigate to **My Templates**, select the template you created to disable the 2.4GHz network (Example: Disable Dot11 b g n Network), and click **Deploy**.

Step 11: In the **Template Deployment** box, in the **Device Selection** section, select the controllers for EDRRM deployment, and click **OK**.

The Schedule parameters default to **Now**, so the template deployment starts immediately.

Step 12: If you want to check the job status, you can navigate to **Administration > Jobs Dashboard**.

Step 13: After the job has completed, navigate to **Design > Configuration > Feature Design**, and then in the tree on the left, navigate to **My Templates**, select the template you created to enable EDRRM for the 2.4GHz band (Example: Enable Dot11 b g n EDRRM), and click **Deploy**.

Step 14: In the **Template Deployment** box, in the **Device Selection** section, select the controllers for EDRRM deployment, and click **OK**.

The Schedule parameters default to **Now**, so the template deployment starts immediately.

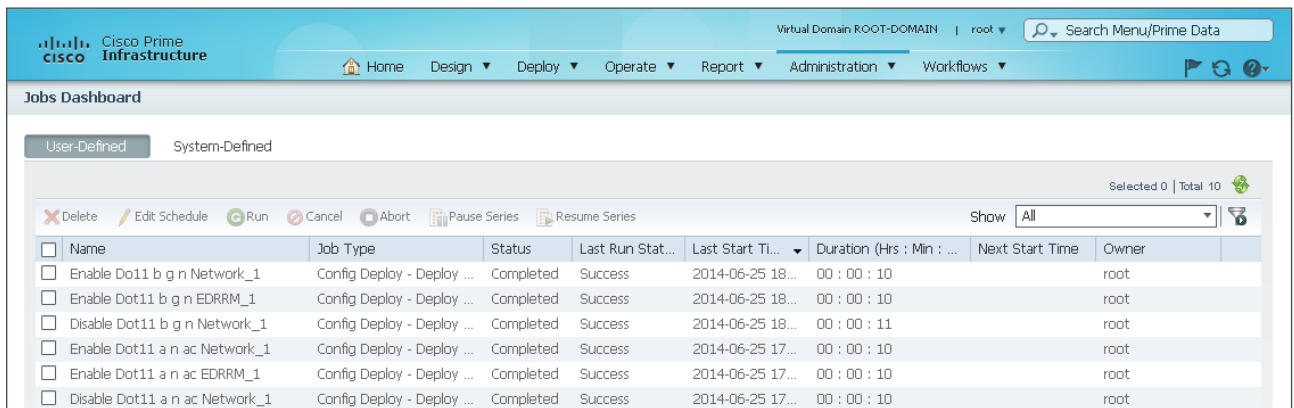
Step 15: If you want to check the job status, you can navigate to **Administration > Jobs Dashboard**.

Step 16: After the job has completed, in the top menu, navigate to **Design > Feature Design**, and then on the left navigate to **My Templates**, and select the template you created to enable the 2.4GHz network (Example: Enable Dot11 b g n Network), and click **Deploy**.

Step 17: In the **Template Deployment** box, in the **Device Selection** section, select the controllers for EDRRM deployment, and click **OK**.

The Schedule parameters default to Now, so the template deployment starts immediately.

Step 18: Navigate to **Administration > Jobs Dashboard**. All of the jobs should now show status as **Completed** and **Success**.



The screenshot shows the Cisco Prime Infrastructure Jobs Dashboard. The interface includes a top navigation bar with the Cisco Prime Infrastructure logo, a search bar, and a menu with options like Home, Design, Deploy, Operate, Report, Administration, and Workflows. Below the navigation bar, there are tabs for 'User-Defined' and 'System-Defined'. A toolbar contains actions like Delete, Edit Schedule, Run, Cancel, Abort, Pause Series, and Resume Series. A table lists jobs with columns for Name, Job Type, Status, Last Run Status, Last Start Time, Duration, Next Start Time, and Owner. All listed jobs are in a 'Completed' status with a 'Success' last run status.

<input type="checkbox"/>	Name	Job Type	Status	Last Run Stat...	Last Start Ti...	Duration (Hrs : Min : ...	Next Start Time	Owner
<input type="checkbox"/>	Enable Do11 b g n Network_1	Config Deploy - Deploy ...	Completed	Success	2014-06-25 18...	00 : 00 : 10		root
<input type="checkbox"/>	Enable Dot11 b g n EDRRM_1	Config Deploy - Deploy ...	Completed	Success	2014-06-25 18...	00 : 00 : 10		root
<input type="checkbox"/>	Disable Dot11 b g n Network_1	Config Deploy - Deploy ...	Completed	Success	2014-06-25 18...	00 : 00 : 11		root
<input type="checkbox"/>	Enable Dot11 a n ac Network_1	Config Deploy - Deploy ...	Completed	Success	2014-06-25 17...	00 : 00 : 10		root
<input type="checkbox"/>	Enable Dot11 a n ac EDRRM_1	Config Deploy - Deploy ...	Completed	Success	2014-06-25 17...	00 : 00 : 10		root
<input type="checkbox"/>	Disable Dot11 a n ac Network_1	Config Deploy - Deploy ...	Completed	Success	2014-06-25 17...	00 : 00 : 10		root

You have now enabled EDRRM for 2.4GHz band, in addition to the 5GHz band previously enabled.

Procedure 5 Create a Cisco CleanAir controller template

Next, you 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, navigate to **Design > Feature Design**, on the left navigate to **Features and Technologies > Controller > 802.11a or n or ac**, and then select the **CleanAir** template.

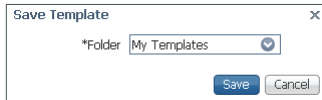
Step 2: On the CleanAir template, do the following:

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

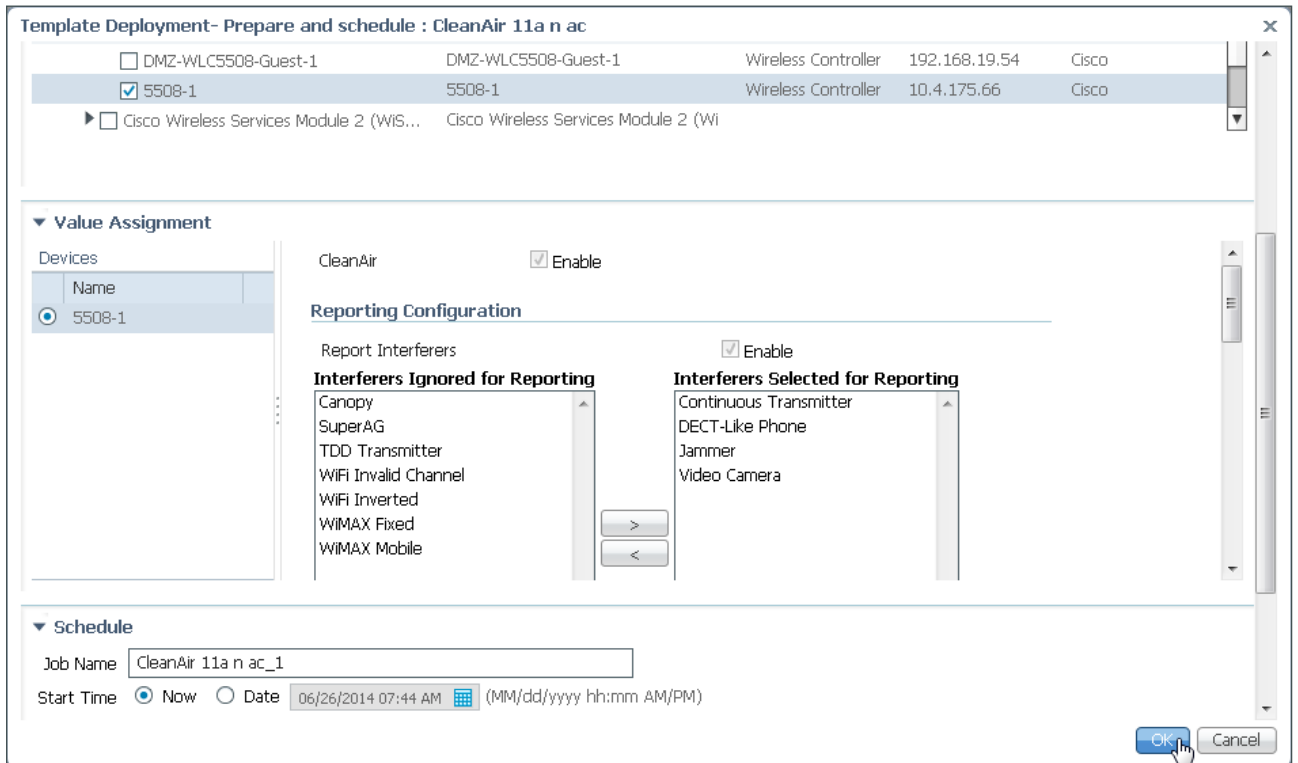
The screenshot displays the Cisco Prime Infrastructure configuration page for the CleanAir template. The breadcrumb trail indicates the path: Templates > Features and Technologies > Controller > 802.11a or n or ac > CleanAir. The left-hand navigation pane shows the tree structure under 'Features and Technologies' > 'Controller' > '802.11' > '802.11a or n or ac' > 'CleanAir'. The main configuration area is divided into several sections:

- Template Basic:** *Name: CleanAir 11a n ac; Author: root; Feature Category: CleanAir.
- Validation Criteria:** *Device Type: CUWN (default).
- 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 Alarm Threshold: 1 (1-100).
 - Air Quality Unclassified category Alarm Enable; Air Quality Unclassified Category Severity Threshold: 1 (1-99).
 - Interferers For Security Alarm Enable.
 - Interferers Ignored for Security Alarms:** Canopy, SuperAG, TDD Transmitter, WIFI Invalid Channel, WIFI Inverted, WIMAX Fixed, WIMAX Mobile.
 - Interferers Selected for Security Alarms:** Continuous Transmitter, DECT-Like Phone, Jammer, Video Camera.

Step 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, navigate to **Design > Feature Design**, on the left navigate to **Features and Technology > Controller > 802.11b or g or n**, and then select the **CleanAir** template.

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

- Provide a meaningful name and 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 Discovery, 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 is activated.
- Move the following interferer types to the Interferers Selected for Security Alarms box: **Bluetooth Discovery, Bluetooth Link, Continuous Transmitter, DECT-Like Phone, Jammer, Microwave Oven, Video Camera, Xbox**.

The screenshot shows the Cisco Prime Infrastructure configuration interface for the CleanAir template. The breadcrumb path is: Templates > Features and Technologies > Controller > 802.11b or g or n > CleanAir.

Template Basic

- *Name: CleanAir 11b or g or n
- Description: CleanAir 11b or g or n
- Tags: (empty)
- Author: root
- Feature Category: CleanAir

Validation Criteria

- *Device Type: CUWN (default)

Template Detail

- CleanAir Enable

Reporting Configuration

- Report Interferers Enable

Interferers Ignored for Reporting	Interferers Selected for Reporting
802.11FH	Bluetooth Discovery
802.15.4	Bluetooth Link
Canopy	Continuous Transmitter
SuperAG	DECT-Like Phone
TDD Transmitter	Jammer
WiFi Invalid Channel	Microwave Oven
WiFi Inverted	Video Camera
WIMAX Fixed	Xbox
WIMAX Mobile	

Persistent Device Propagation Enable

Alarm Configuration

- Air Quality Alarm Enable
- Air Quality Alarm Threshold: 1 (1-100) (Air Quality value 100 is best and 1 is worst)
- Air Quality Unclassified category Alarm Enable
- Air Quality Unclassified Category Severity Threshold: 1 (1-99)
- Interferers For Security Alarm Enable

Interferers Ignored for Security Alarms	Interferers Selected for Security Alarms
802.11FH	Bluetooth Discovery
802.15.4	Bluetooth Link
Canopy	Continuous Transmitter
SuperAG	DECT-Like Phone
TDD Transmitter	Jammer
WiFi Invalid Channel	Microwave Oven
WiFi Inverted	Video Camera
WIMAX Fixed	Xbox

Step 7: Click **Save as New Template**, 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**.

PROCESS

Installing the Cisco Mobility Services Engine Virtual Appliance

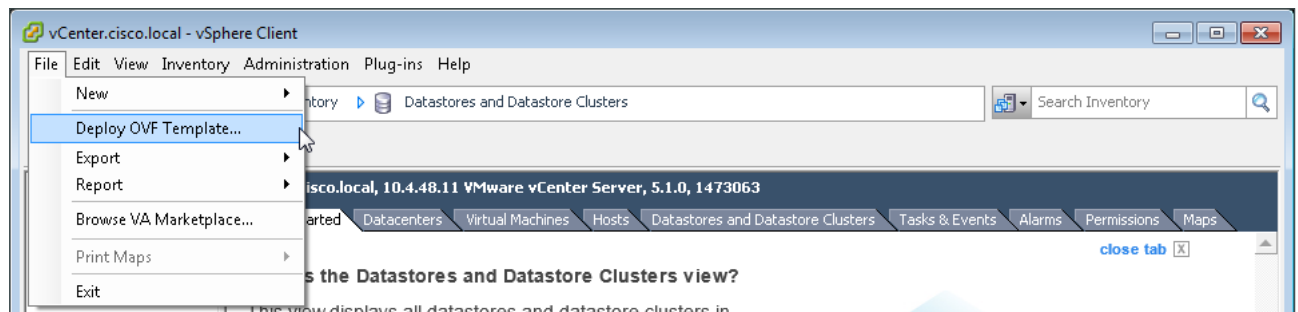
1. Install the Cisco MSE virtual appliance
2. Start the Cisco MSE virtual appliance
3. Configure the Cisco MSE virtual appliance
4. Verify installation of MSE virtual appliance

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

Although capable of 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**.

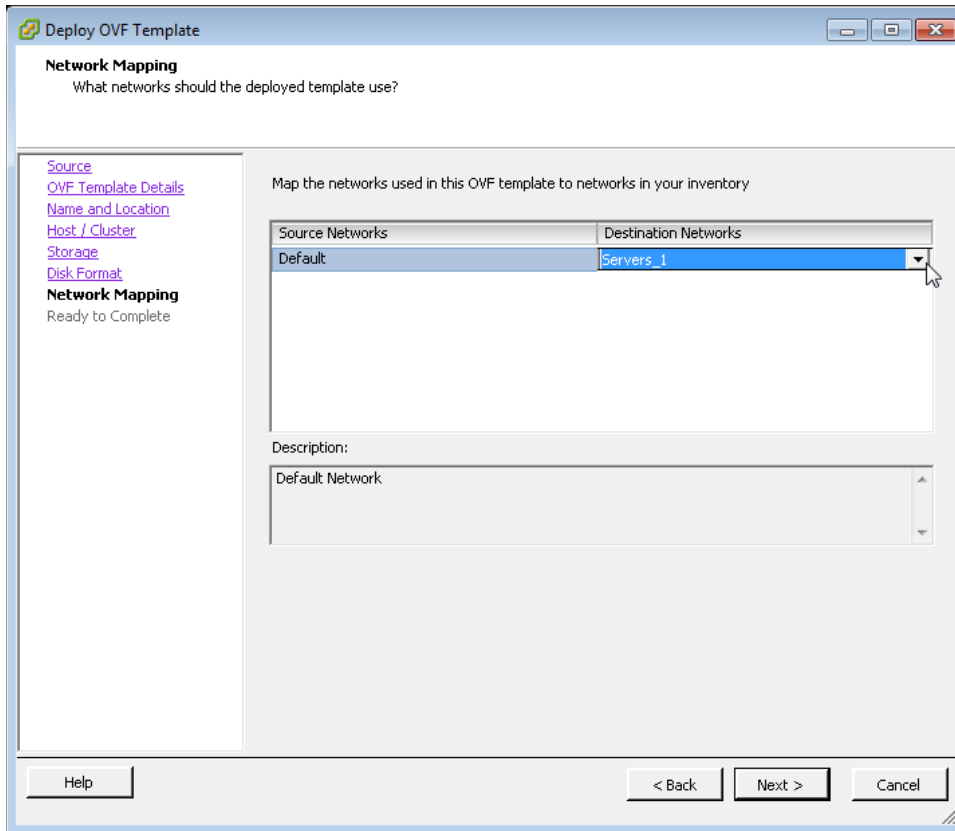
Step 4: On the Name and Location page, enter a unique and descriptive name for the virtual appliance that you are installing (Example: MSE-VA), choose a location to install the virtual appliance, and then click **Next**.

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: MSE-VA), and then in the **Getting Started** tab select **Power on the virtual machine**.

Step 2: Using a console view of the VM, wait for the **mse login** prompt to appear, enter the default username and password: **root/password**.

```
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 half an hour 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.

The installation completes and the virtual machine automatically restarts.

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>**.

```
Cisco Mobility Service Engine
```

```
mse login: root
```

```
Password:
```

Step 3: At the prompt to setup parameters in the Setup Wizard, enter **yes**, and at the prompt to configure MSE using menu options, enter **no**, and then press **Enter**.

```
Enter whether you would like to set up the initial parameters manually or via the  
setup wizard.
```

```
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: Follow the Startup Wizard prompts and update the following parameters:

- Configure hostname? (Y)es/(S)kip/(U)se default [Yes]: **Yes**
 - Enter a host name [mse]: **mse-va**
- Configure domain name? (Y)es/(S)kip/(U)se default [Yes]: **Yes**
 - Enter a domain name: **cisco.local**
- Configure high availability? (Y)es/(S)kip/(U)se default [Yes]: **Skip**
- Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Yes]: **Yes**
 - Enter eth0 IP address [1.1.1.10]: **10.4.48.40**
 - Enter network mask [255.255.255.0]: **255.255.255.0**
 - Enter default gateway address [1.1.1.1]: **10.4.48.1**
- Configure eth1 interface parameters? (Y)es/(S)kip/(U)se default [Yes]: **Skip**
- 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] : **none**
- Configure timezone? (Y)es/(S)kip/(U)se default [Yes]: **Yes**
 - Please select a continent or ocean... #?: **2** (Americas)
 - Please select a country... #?: **47** (United States)
 - Please select a time zone... #?: **21** (Pacific Time)
 - Is the above information OK?... #?: **1** (Yes)
- Configure future MSE restart day and time? (Y)es/(S)kip [Skip]: **Skip**
- Configure Remote Syslog Server Configuration parameters? (Y)es/(S)kip/(U)se default [Yes]: **Yes**
 - Enter Remote Syslog Server Server IP address: **10.4.48.15**
 - Enter a priority level (1-3) : **2** (WARNING level)
 - Enter a facility (0-7) : **4** (LOCAL4 (20))

i 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 Host access control settings? (Y)es/(S)kip [Skip]: **Skip**
- Configure NTP related parameters? (Y)es/(S)kip/(U)se default [Yes]: **Yes**
 - 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]: **none**
- Configure NTP Authentication? (Y)es/(S)kip/(U)se default [Yes]: **Skip**
- Configure audit rules and enable Audit daemon? (Y)es/(S)kip/(U)se default [Yes]: **Skip**

- Configure login banner? (Y)es/(S)kip/(U)se Default [Yes]: **Skip**
- Configure system console restrictions? (Y)es/(S)kip/(U)se default [Yes]: **Skip**
- Configure ssh access for root (Y)es/(S)kip/(U)se default [Yes]: **Yes**
 - Enable ssh root access (yes/no) [no]: **yes**
- Configure single user mode password check (Y)es/(S)kip/(U)se default [Yes]: **Skip**
- Configure root password? (Y)es/(S)kip/(U)se default [Yes]: **Yes**
 - Enter new password: **[strong root password]**

i Tech Tip

Cisco MSE requires the use of strong passwords, which must be up to 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.

- Configure login/password related parameters? (Y)es/(S)kip/(U)se default [Yes]: **Skip**
- Configure GRUB password (Y)es/(D)isable/(S)kip/(U)se default [Yes]: **Skip**

i 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 requirements.

- Configure NCS communications username? (Y)es/(S)kip/(U)se default [Yes]: **Yes**
 - Enter a username: **MSEuser**
- Configure NCS communications password? (Y)es/(S)kip/(U)se default [Yes]: **Yes**
 - Enter NCS communication password: **[NCS password]**
 - Confirm NCS communication password: **[NCS password]**

Step 5: Confirm and approve the settings obtained through the Setup Wizard, by entering **yes <ENTER>**.

```
-----BEGIN-----
Host name=mse-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/Anchorage
Enable NTP=yes, NTP servers=10.4.48.17
Enable SSH root access = yes
Enable Single User Mode Password Check = no
Root password is changed
NCS username is changed.
NCS password is changed.
Remote Syslog Server IPAddress=10.4.48.15, Remote Syslog Server
Facility=LOCAL4
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 step.

Configuration Changed
Is the above information correct (yes, no, or A): yes
```

The configuration is applied and you are returned to a login prompt.

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, select the Cisco MSE-VA virtual machine and do a Restart Guest operation.

Step 2: On the Console tab, log in to the Cisco MSE by entering **root** for the user ID your **[strong root password]** configured with the Startup Wizard.

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

```
Cisco Mobility Service Engine

mse-va login: root
Password:
Last login: Fri Jun 27 10:20:26 on tty1
[root@mse-va ~]# getserverinfo
Health Monitor is not running
[root@mse-va ~]#
```


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.

```
[root@mse-va ~]# service msed start
Starting MSE Platform

    syslogd: unknown facility name "LOCAL*"
Flushing any pending data from Admin Process read and write pipe.
Starting Apache HTTPD Server
Apache Server is already running. Skipping restart.
Starting Health Monitor, Waiting to check the status.
Health Monitor successfully started
Starting Admin process...
Stared 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.

PROCESS

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.

Cisco Prime Infrastructure supports specific web browser client configurations and versions. Management functionality can be impaired when you deviate from the supported clients. As an example, the supported versions of Internet Explorer require the Google Chrome Frame plugin. For the latest information about supported web browser clients, see the System Requirements references in the [Cisco Prime Infrastructure release notes](#).

Procedure 1 Log in to Cisco Prime Infrastructure

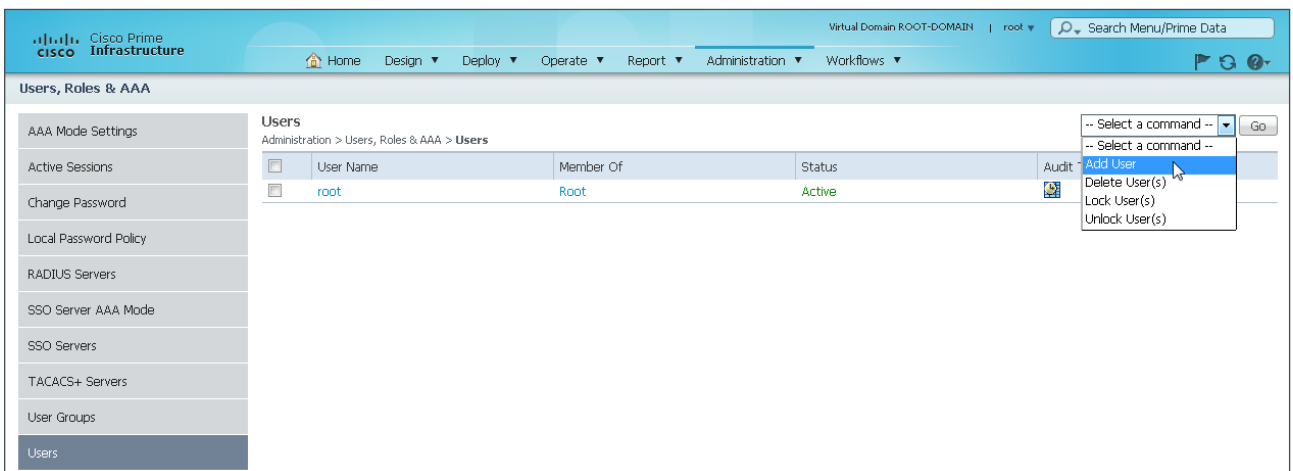
Step 1: Using a supported browser, access the Cisco Prime Infrastructure management interface (Examples: <https://prime-infra.cisco.local> or <https://10.4.48.35>).

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, Roles & AAA**, in the tree on the left, click **Users**, in the **Select a command** list, choose **Add User**, and then click **Go**.

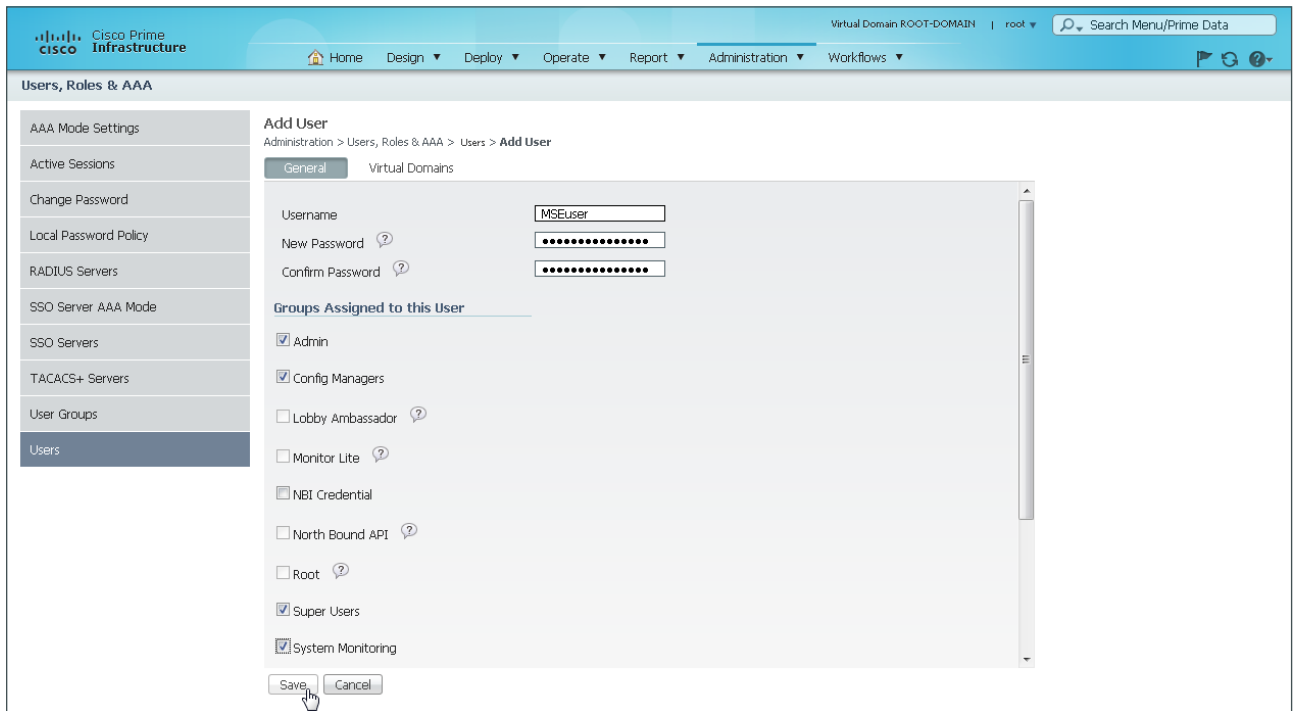


Step 2: Enter the username (Example: MSEuser) and the **[MCS password]** that you configured for the MSE Virtual Appliance.

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

Tech Tip

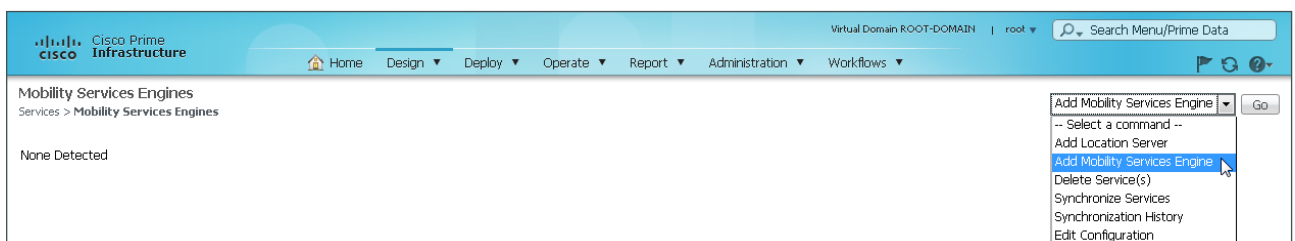
It may be necessary to modify the password policy in Cisco Prime Infrastructure in order to accept passwords that deviate from the policy. To do this, navigate to **Administration > Users, Roles & AAA > Local Password Policy**, and modify the necessary policy settings in order to match your security policy.



Procedure 3 Add the Cisco MSE-VA to Prime Infrastructure

Step 1: From the top menu, navigate to **Design > Mobility Services > Mobility Services Engines**.

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



Step 3: On the Add Mobility Services Engine page, enter the following parameters and then click **Next**:

- Device Name—**MSE-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)
- HTTP—Clear Enable selection

Add Mobility Services Engine

Device Name:

IP Address:

Contact Name:

Username:

Password:

HTTP: Enable

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

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

! 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
MSE-VA Not Activated (AIR-MSE-VA-K9-V01:mse-va.cisco.local_6)				
CAS	2500	CAS Elements	100	Evaluation (120 days left)
wIPS	6000	wIPS Monitor Mode APs	10	Evaluation (120 days left)
		wIPS Local Mode APs	10	Evaluation (120 days left)
MC	2500	Mobile Concierge	10	Evaluation (120 days left)
ANA	2500	Location Analytics	10	Evaluation (120 days left)

Add License **Remove License**

Back **Next**

Step 5: 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**.

Add A License File

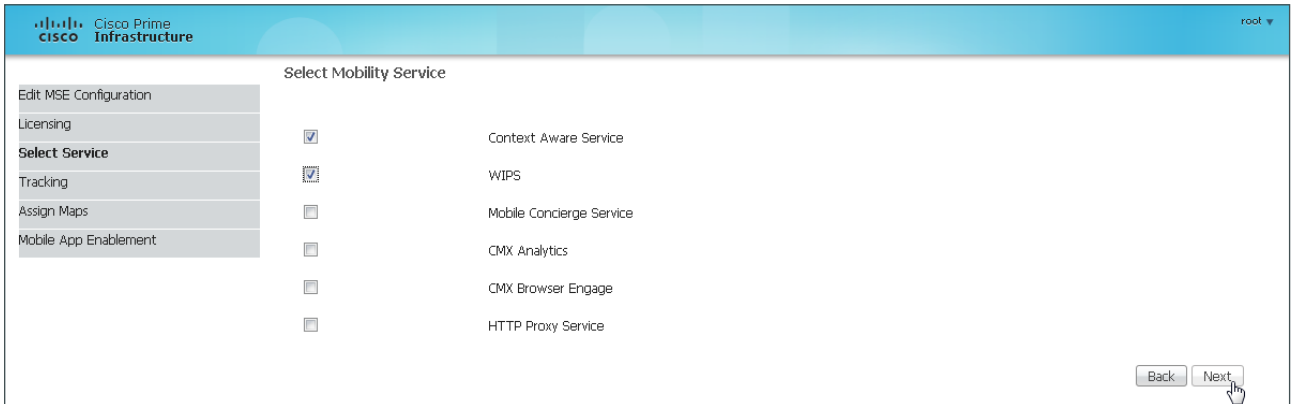
MSE Name: **vMSE-VA(AIR-MSE-VA-K9-V01:vMSE-VA.cisco.local_4682359c-83ac-11e3-aaad-005056a27888)**

License File: No file chosen

OK **Cancel**

Step 6: On the MSE License Summary page, click **Next**.

Step 7: On the Select Mobility Service page, select **Context Aware Service**, Wireless Intrusion Protection Service (**WIPS**) and then click **Next**.



Step 8: 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	Rogue Clients
Interferers	Interferers
Active RFID Tags	—

Step 9: On the Assign Maps page, select the building and floor plan created and click **Synchronize**.

The screenshot shows the Cisco Prime Infrastructure interface. On the left is a navigation menu with options: Edit MSE Configuration, Licensing, Select Service, Tracking, Assign Maps (highlighted), and Mobile App Enablement. The main area displays a table with the following data:

<input type="checkbox"/>	Name	Type	Status
<input checked="" type="checkbox"/>	System Campus > Headquarters > First Floor	Floor Area	
<input checked="" type="checkbox"/>	System Campus > Headquarters	Building	
<input type="checkbox"/>	Unassigned	Campus	

Below the table are buttons for 'Synchronize' and 'Reset'. The 'Synchronize' button is being clicked. At the top right, it says 'Selected 2 | Total 3' and 'Show All'. At the bottom right, there are 'Back' and 'Next' buttons.

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

This screenshot is similar to the previous one, but the 'Status' column now contains green double-headed arrows for the two selected items, indicating a bi-directional relationship.

<input type="checkbox"/>	Name	Type	Status
<input checked="" type="checkbox"/>	System Campus > Headquarters > First Floor	Floor Area	↔
<input checked="" type="checkbox"/>	System Campus > Headquarters	Building	↔
<input type="checkbox"/>	Unassigned	Campus	

Step 10: Click **Next** to continue.

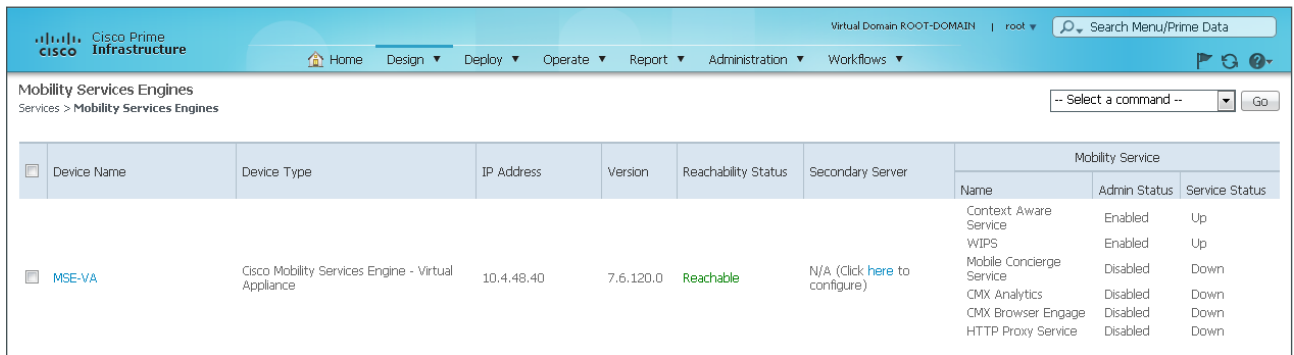
Step 11: On the Mobile App Enablement page, do not enable Mobile App Integration, click **Done**, and then on the “Your MSE Settings have been saved” message, click **OK**.

The screenshot shows the 'Mobile App Enablement' page. Under the 'General' section, there is an unchecked checkbox for 'Enable Mobile App Integration'. Below it is a 'Save' button. At the bottom right, there are 'Back' and 'Done' buttons. The 'Done' button is being clicked.

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.



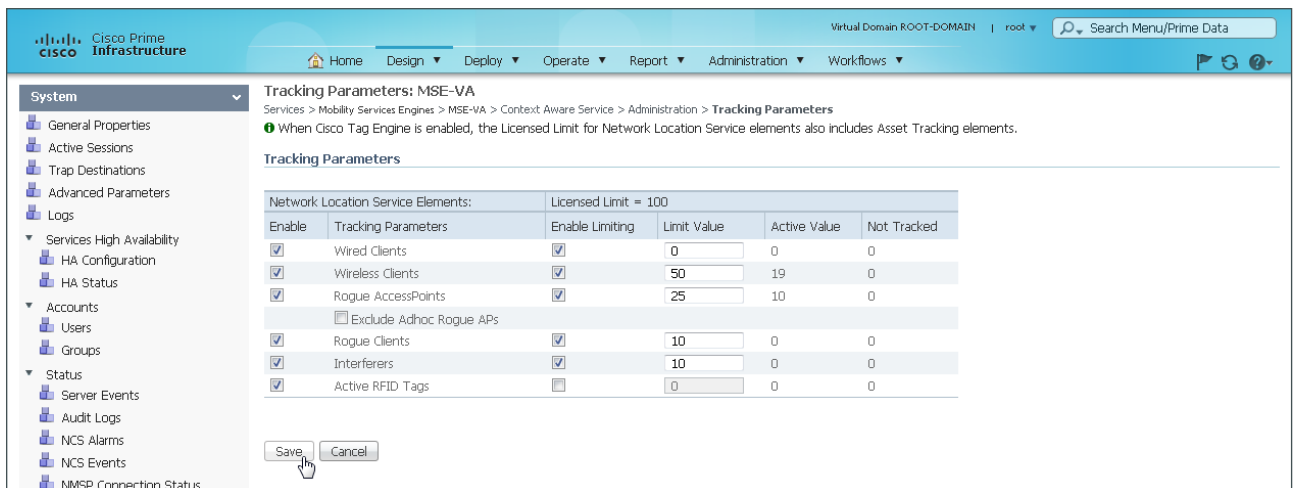
Device Name	Device Type	IP Address	Version	Reachability Status	Secondary Server	Mobility Service		
						Name	Admin Status	Service Status
MSE-VA	Cisco Mobility Services Engine - Virtual Appliance	10.4.48.40	7.6.120.0	Reachable	N/A (Click here to configure)	Context Aware Service	Enabled	Up
						WIPS	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 Device Name of 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: **0** Wired Clients + **50** Wireless Clients + **25** Rogue Access Points + **10** Rogue Clients + **15** Interferers = 100 Licensed Elements). When appropriately valued, click **Save**.



Tracking Parameters: MSE-VA
 Services > Mobility Services Engines > MSE-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.

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"/>	0	0	0
<input checked="" type="checkbox"/>	Wireless Clients	<input checked="" type="checkbox"/>	50	19	0
<input checked="" type="checkbox"/>	Rogue AccessPoints	<input checked="" type="checkbox"/>	25	10	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"/>	10	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.

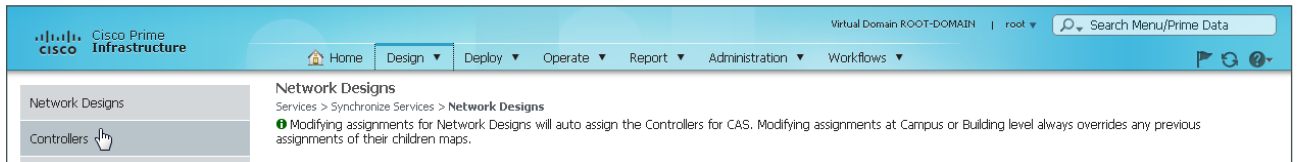
Procedure 5 Synchronize the WLCs to use Cisco MSE

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**.



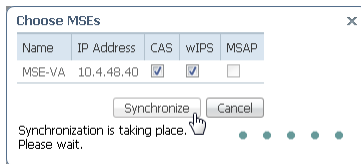
Step 2: On the left side of the page, in the list, click **Controllers**.



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

Name	IP Address	Version	Service	MSE	Sync Status	Message
<input type="checkbox"/> A3850-D6500.cisco.local	10.4.15.6	03.03.03SE	-	-	-	-
<input checked="" type="checkbox"/> vWLC-Server1	10.4.59.58	7.6.120.0	CAS	MSE-VA [NMSP Status]	↔	-
<input checked="" type="checkbox"/> WLC7500-1	10.4.59.68	7.6.120.0	CAS	MSE-VA [NMSP Status]	↔	-
<input type="checkbox"/> A3650-D6880.cisco.local	10.4.79.6	03.03.01SE	-	-	-	-
<input type="checkbox"/> A3850-D4507.cisco.local	10.4.95.6	03.03.03SE	-	-	-	-
<input type="checkbox"/> A3650-D4500X.cisco.local	10.4.111.6	03.03.03SE	-	-	-	-
<input type="checkbox"/> A3850-D3750X.cisco.local	10.4.127.5	03.03.01SE	-	-	-	-
<input type="checkbox"/> A3650-D3750X.cisco.local	10.4.127.6	03.03.03SE	-	-	-	-
<input type="checkbox"/> 2504-1	10.4.175.62	7.6.120.0	-	-	-	-
<input type="checkbox"/> 2504-2	10.4.175.63	7.6.120.0	-	-	-	-
<input checked="" type="checkbox"/> WLC-1	10.4.175.64	7.6.120.0	CAS	MSE-VA [NMSP Status]	↔	-
<input checked="" type="checkbox"/> 5508-1	10.4.175.66	7.6.120.0	CAS	MSE-VA [NMSP Status]	↔	-
<input checked="" type="checkbox"/> 5760-WLC.cisco.local	10.4.175.68	03.03.03SE	CAS	MSE-VA [NMSP Status]	↔	-
<input type="checkbox"/> WLC-1	10.4.175.165	7.6.120.0	-	-	-	-

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



The synchronization process completes, and you are returned to the Controllers selection screen.

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 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 > Mobility Services Engine** and then select your Mobility Services Engine.

Step 2: In the tree on the left, navigate to **Status**, and then click **NMSP Connection Status**.

The screenshot shows the Cisco Prime Infrastructure web interface. The navigation tree on the left is expanded to 'Status' > 'NMSP Connection Status'. The main content area displays the 'NMSP Connection Status: MSE-VA' page. It includes a 'Summary' table and a detailed 'NMSP Connection Status' table.

Device	Total	Not Active
Controllers	5	3
Switches	0	0

IP Address	Target Type	Version	NMSP Status	Echo Request Count	Echo Response Count	Last Message Received
10.4.59.58	Controller	7.6.120.0	Inactive	0	0	-
10.4.59.68	Controller	7.6.120.0	Inactive	0	0	-
10.4.175.64	Controller	7.6.120.0	Inactive	0	0	-
10.4.175.66	Controller	7.6.120.0	Active	211	211	2014-Jun-30, 11:08:09 PDT
10.4.175.68	NGWC Switch	N/A	Active	210	210	2014-Jun-30, 11:08:09 PDT

Step 3: If all of the WLCs have an NMSP status of **Active**, skip to the next procedure.

Step 4: If any of the WLCs has an NMSP status of **Inactive**, perform the steps below for each inactive WLC. On the console of the Cisco MSE-VA, login as **root**, use the **[strong root password]** you previously configured, and then in the CLI issue the **cmdshell** command.

The response is the **cmd>** prompt.

```
Cisco Mobility Service Engine

mse-va login: root
Password:
Last login: Fri Jun 27 11:40:19 on ttyl
[root@mse-va ~]# cmdshell

cmd>_
```

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

```
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:a2:29:c3
Key Hash: f72a2850e64fe2a3ff990ebe56276328d80d8fff
Certificate Type: SSC

cmd>
```

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. Type `exit` to exit from the `cmd>` environment.

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

Step 7: Choose a wireless LAN controller that is displayed as Inactive, and use either the physical console port or SSH to connect to the controller CLI, log in, 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: Use the information obtained from the MSE-VA in Step 6 with the `config auth-list` command to authorize the Cisco MSE to connect to the wireless LAN controller.

```
(Cisco Controller) >config auth-list add ssc 00:50:56:a2:29:c3
f72a2850e64fe2a3ff990ebe56276328d80d8fff
(Cisco Controller) >
```

Step 9: Type **show auth-list** to verify that the Cisco MSE has been authorized on the wireless LAN controller, enter **save config**, confirm, and then **exit**.

```
(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:a2:29:c3                      SSC                                     f72a2850e64fe2a3ff990ebe56276328d80d8fff
```

```
(Cisco Controller) >save config
Are you sure you want to save? (y/n) y
Configuration Saved!
(Cisco Controller) >exit
```

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 should verify that the NMSP status is now active.

Step 11: Navigate to **Design > Mobility Services > Mobility Services Engine**, select your Mobility Services Engine, on the left navigate to **Status**, and then click **NMSP Connection Status**.

The NMSP status should now be **Active** for each of the WLCs with the updated auth-list.

The screenshot shows the Cisco Prime Infrastructure web interface. The breadcrumb navigation is: Services > Mobility Services Engines > MSE-VA > System > Status > NMSP Connection Status. The main content area displays the NMSP Connection Status for MSE-VA. It includes a summary table and a detailed table of connection status.

Device	Total	Not Active
Controllers	5	0
Switches	0	0

IP Address	Target Type	Version	NMSP Status	Echo Request Count	Echo Response Count	Last Message Received
10.4.59.58	Controller	7.6.120.0	Active	109	109	2014-Jun-30, 12:48:41 PDT
10.4.59.68	Controller	7.6.120.0	Active	60	60	2014-Jun-30, 12:48:41 PDT
10.4.175.64	Controller	7.6.120.0	Active	11	11	2014-Jun-30, 12:48:40 PDT
10.4.175.66	Controller	7.6.120.0	Active	613	613	2014-Jun-30, 12:48:40 PDT
10.4.175.68	NGWC Switch	N/A	Active	612	612	2014-Jun-30, 12:48:40 PDT

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.

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 personal 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, navigate to **Home > Overview > CleanAir**, in the **Filters** list, choose the desired time frame, and then click **Go**.

The screenshot displays the Cisco Prime Infrastructure CleanAir dashboard. The interface includes a navigation bar with tabs for Overview, Incidents, Performance, and Detail Dashboards. The CleanAir section is active, showing a filters section with a time frame set to 'Past 1 Week' and a 'Go' button. The dashboard contains several charts and tables:

- 802.11a/n/ac Avg Air Quality:** A line chart showing average air quality (AvgAQ) over time from 6/26/14 to 6/30/14. The y-axis ranges from 0 to 100.
- 802.11b/g/n Avg Air Quality:** A line chart showing average air quality (AvgAQ) over time from 6/26/14 to 6/30/14. The y-axis ranges from 0 to 100.
- 802.11a/n/ac Min Air Quality:** A line chart showing minimum air quality (Min AQ) over time from 6/26/14 to 6/30/14. The y-axis ranges from 0 to 100.
- Worst 802.11a/n/ac Interferers:** A table listing the top interferers. The table has columns for Interferer ID, Type, Status, Severity, Affected Channels, Duty Cycle (%), and Discovered. One interferer is listed: a2:29:c3:00:00:01, Continuous Transmitter, Active, 0, 108, 100, discovered on Mon Jun 30 13:53:21 PDT 2014.
- Worst 802.11b/g/n Interferers:** A section indicating 'None detected'.
- 802.11a/n/ac Interferer Count:** A line chart showing the interferer count over time from 6/24/14 to 6/29/14. The y-axis ranges from 0 to 32.
- 802.11b/g/n Interferer Count:** A line chart showing the interferer count over time from 6/24/14 to 6/29/14. The y-axis ranges from 0 to 32.
- Recent Security-risk Interferers:** A section at the bottom of the dashboard.

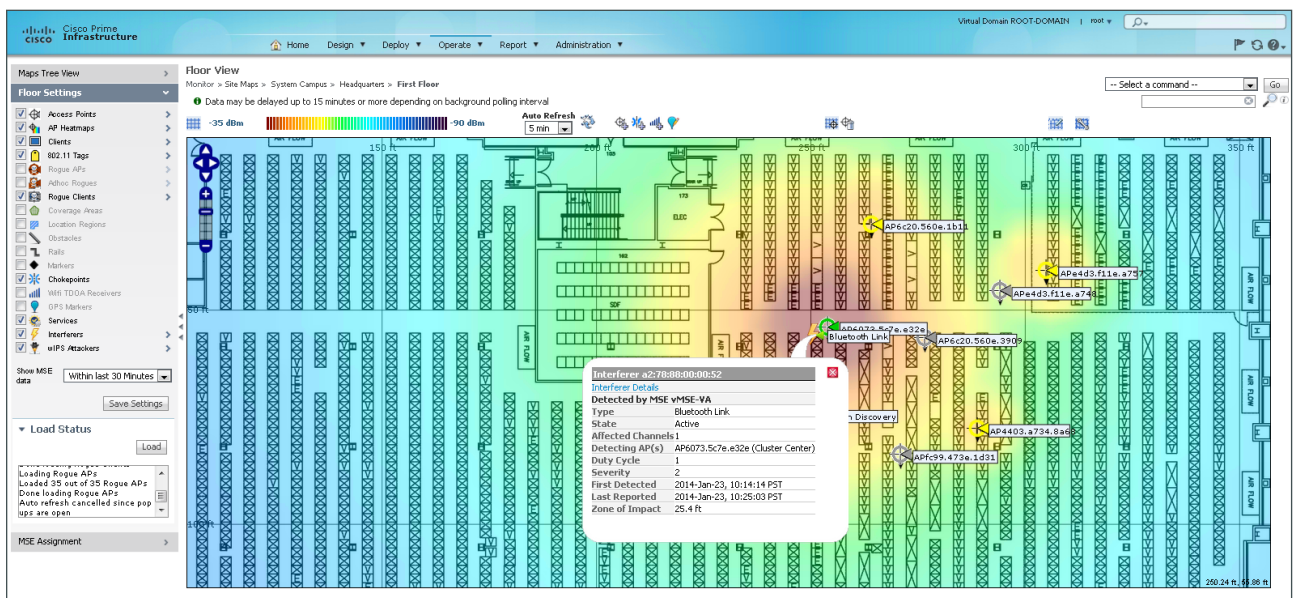
Tech Tip

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 access points 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 access points and wireless LAN controller via the templates described in this document.
3. Repeat Step 4 in Procedure 5, “Synchronize the WLCs to use Cisco MSE”, 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: If you want to look at a specific location, you can navigate to **Operate > Maps** and select a location to view.

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

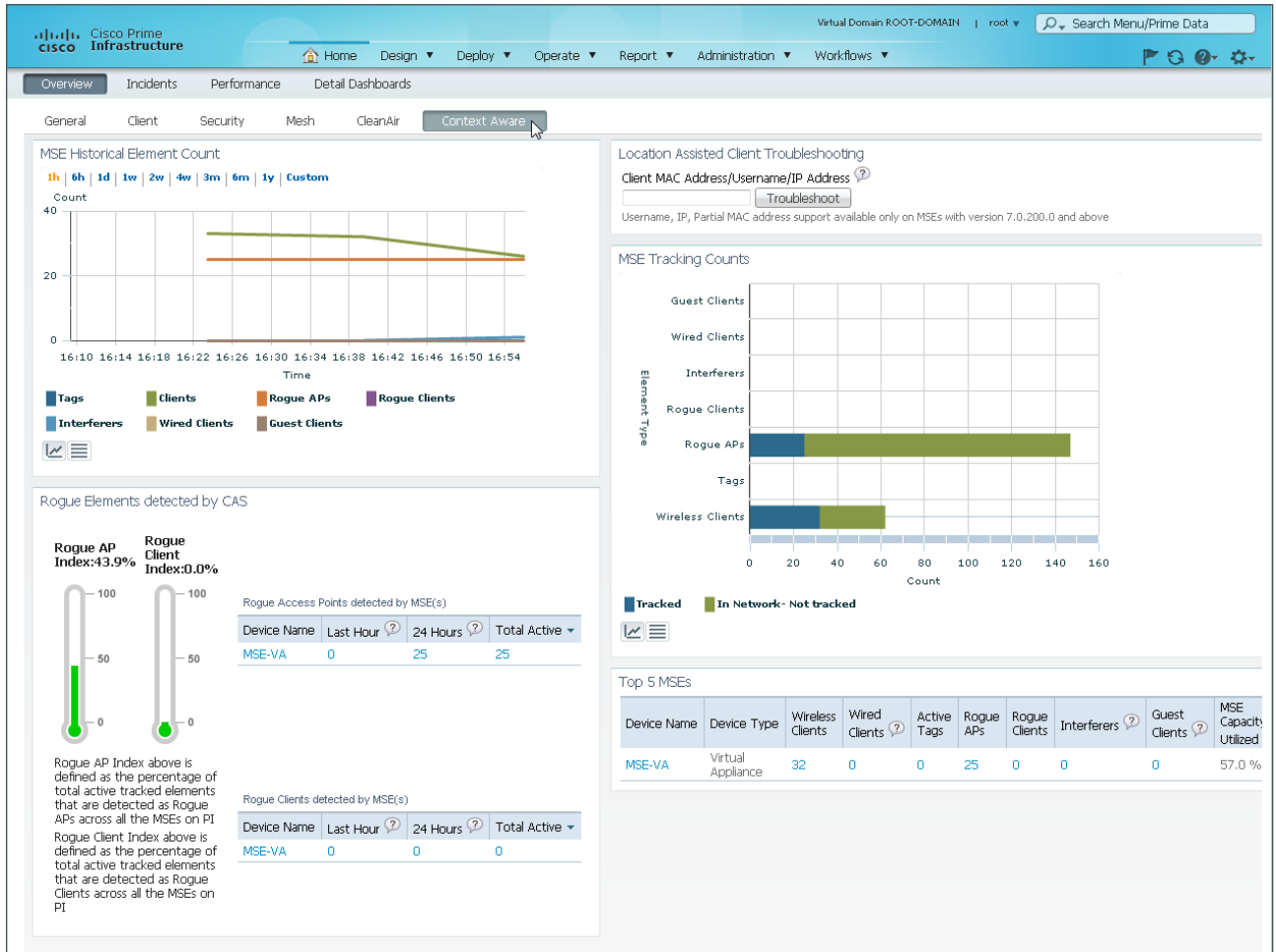


The screenshot displays the Cisco Prime Infrastructure interface. The main area shows a floor plan with a heatmap overlay representing signal strength, ranging from -35 dBm (blue) to -90 dBm (red). A pop-up window titled "Interferer a2:7b:88:00:00:52" is visible, providing details about the detected interferer:

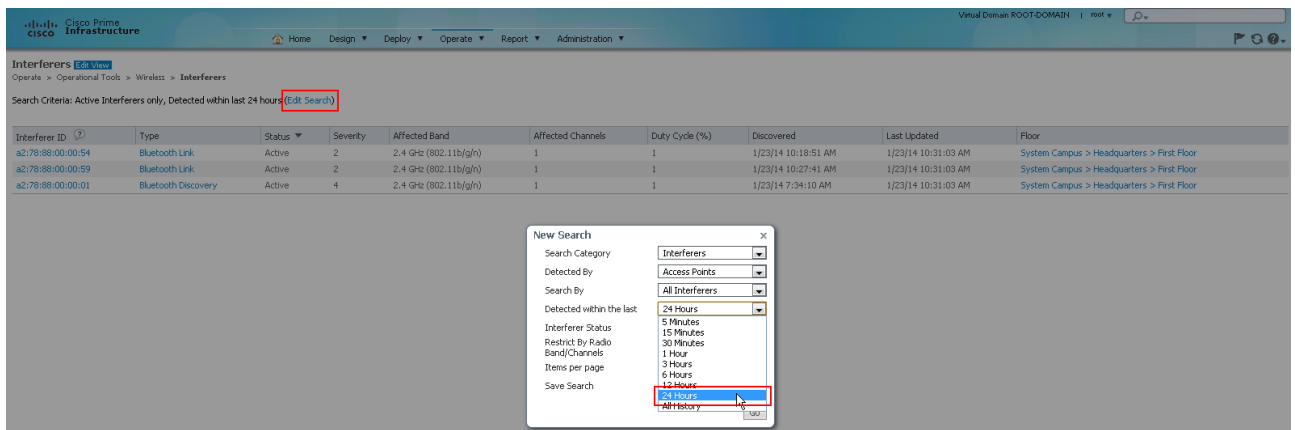
Interferer Details	
Detected by	MSE vMSE-VA
Type	Bluetooth Link
State	Active
Affected Channels	1
Detecting AP(s)	AP6073.5c7e.e32e (Cluster Center)
Duty Cycle	1
Severity	2
First Detected	2014-Jan-23, 10:14:14 PST
Last Reported	2014-Jan-23, 10:25:03 PST
Zone of Impact	25.4 ft

The interface also shows a "Load Status" section on the left, indicating that 35 Rogue APs have been loaded and that auto-refresh is cancelled since pop-ups are open.

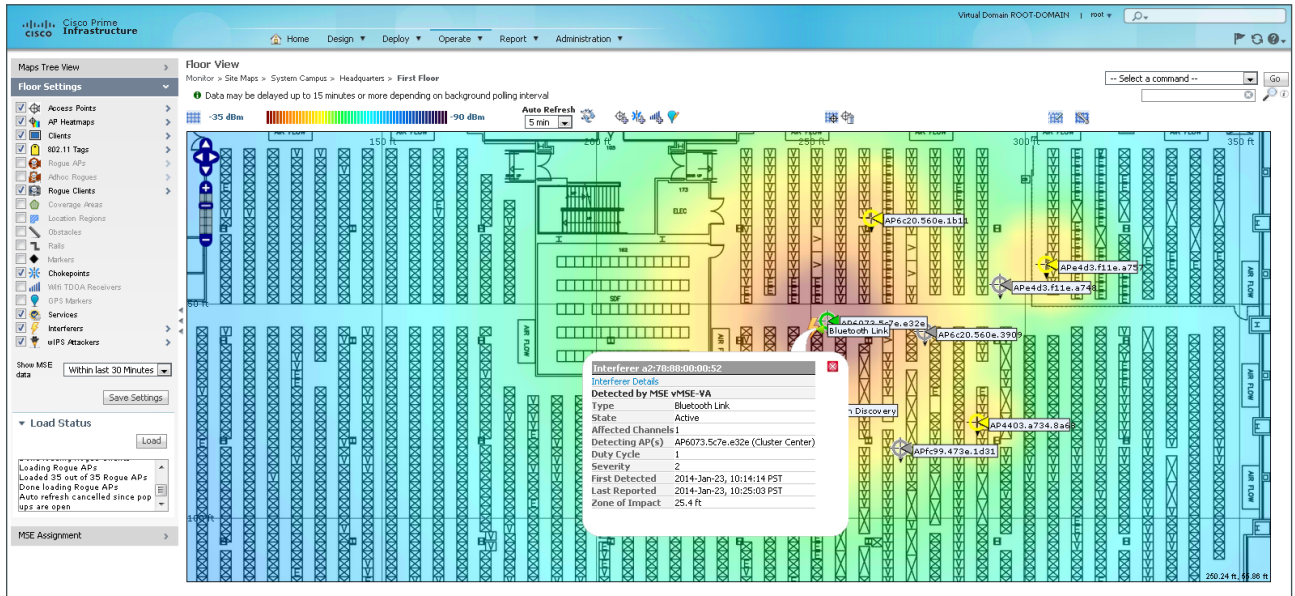
Step 4: Navigate to **Home > Overview > Context Aware**. This displays the historical information on the number of rogues, wireless clients, and other context-aware information obtained from the Cisco MSE-VA.



Step 5: Within Cisco Prime Infrastructure, 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

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

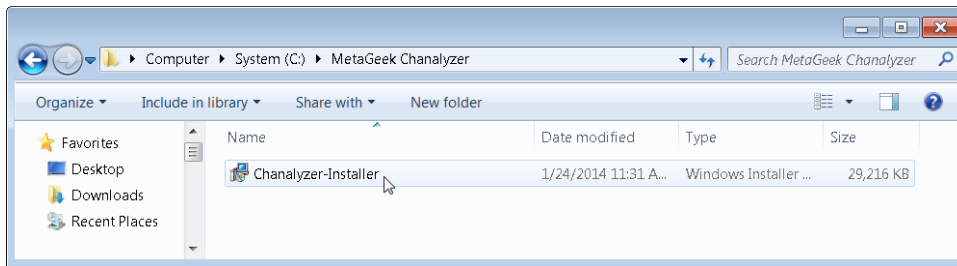
A free 7 day trial of the MetaGeek Chanalyzer product can be downloaded from MetaGeek at the following URL: <http://www.metageek.net/support/downloads/>

Procedure 1 Install MetaGeek Chanalyzer

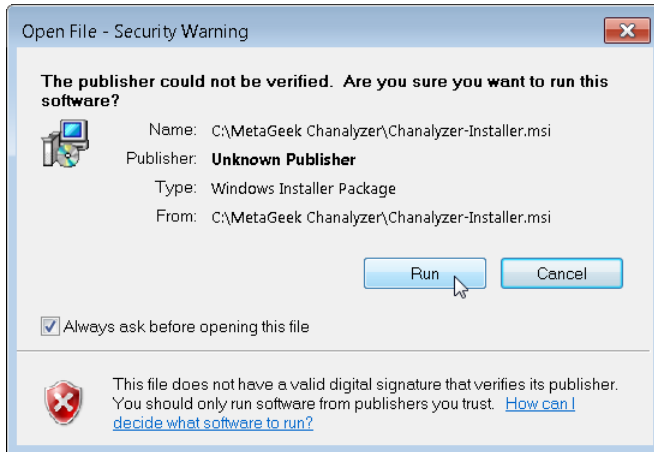
The MetaGeek Chanalyzer is supported on Microsoft Windows platforms. Apple Mac OSX is supported using VMware Fusion and Parallels virtualization. If you are using a virtual machine, a USB-based Wi-Fi adapter is required to provide local spectrum intelligence. More information can be found on the MetaGeek website at the following URL:

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

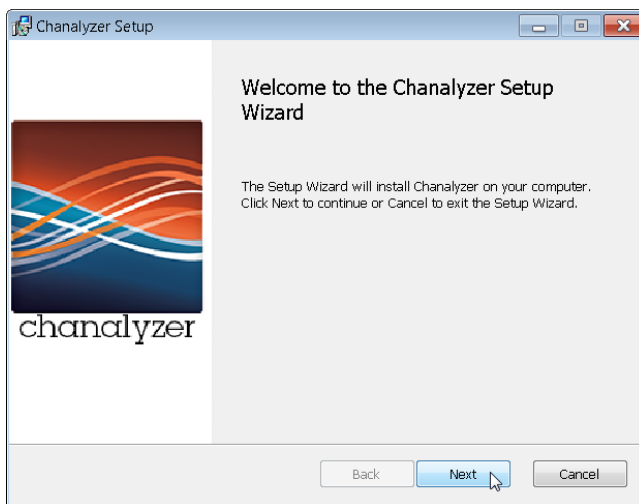
Step 1: Launch the MetaGeek Chanalyzer software.



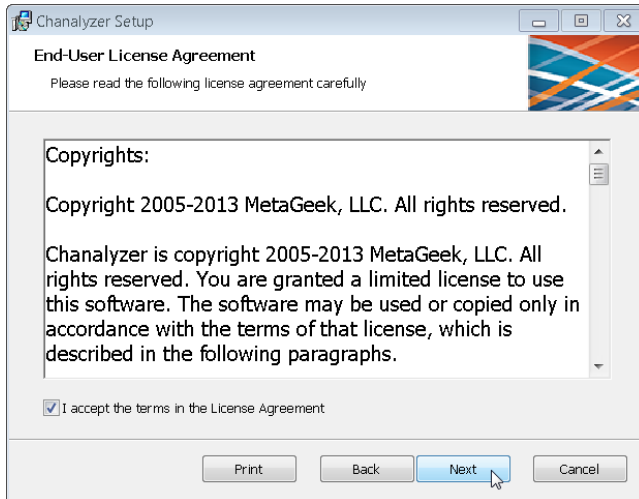
Step 2: If prompted with a Security Warning to run the file, select **Run**



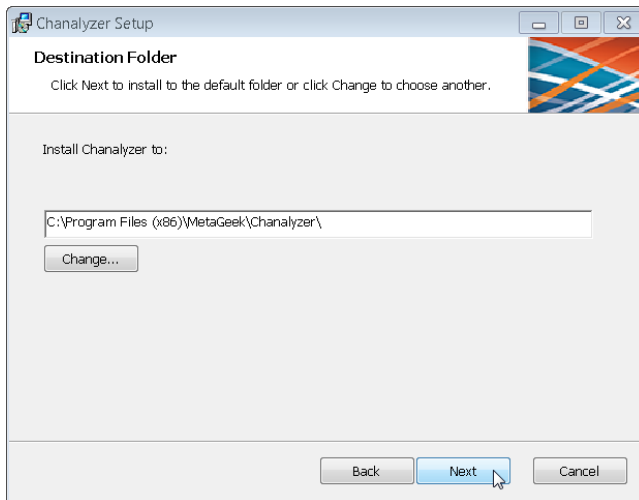
Step 3: Press **Next** to begin the installation of the Chanalyzer Setup Wizard.



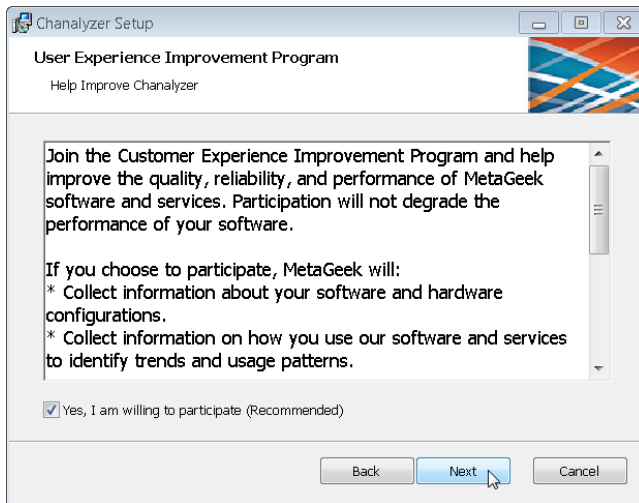
Step 4: If you agree with the License Agreement, select **I accept the terms in the license agreement** and press **Next**.



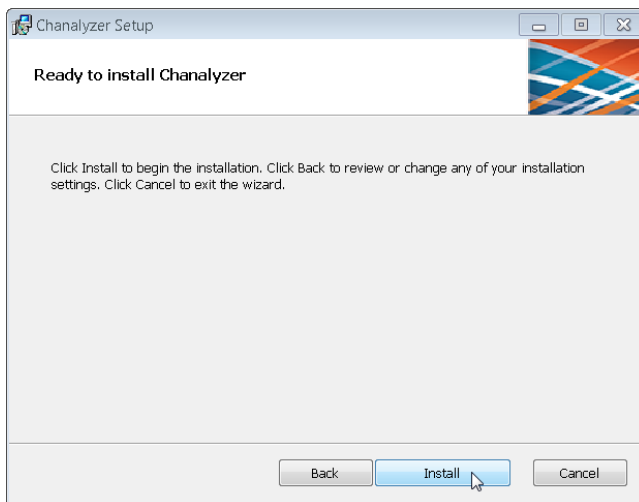
Step 5: Verify that the default installation location is correct and press **Next**.



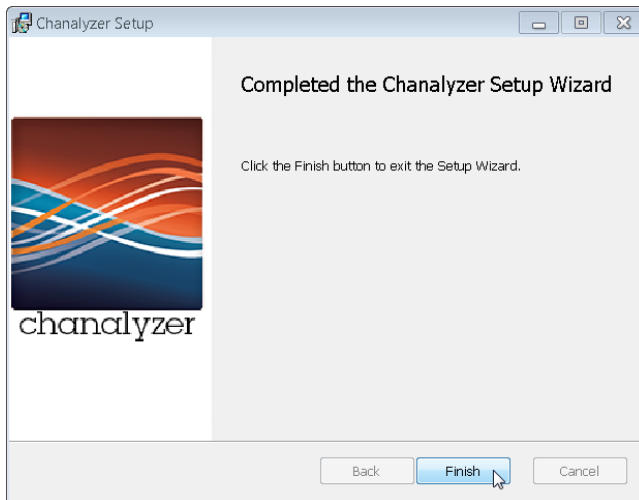
Step 6: Select **Next** to grant permission to participate in the Customer Experience Improvement Program. If you do not wish to participate remove the check mark from the Yes, I am willing to participate (Recommended) prompt and press **Next**.



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

A Cisco CleanAir-capable access point can view the entire 2.4GHz and 5GHz bands, but to do so, you must configure the access point to use Spectrum Expert Connect (SE-Connect) mode. The change to SE-Connect mode is disruptive to the wireless users who are associated to the access point. If all that is required is visibility to the channels that are currently being used by the Cisco CleanAir access point operating in local mode, it is not necessary to place the access point into SE-Connect mode.

The Cisco CleanAir spectrum intelligence is provided to the MetaGeek Chanalyzer software using 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.

Because MetaGeek Chanalyzer can be used independently of Cisco Prime Infrastructure, the configuration of the access point is shown using the native controller management interface.

Step 1: Using a web browser, log in to the wireless LAN controller for the access point to be used for spectrum visibility 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.

AP Name	IP Address	AP Model	AP MAC	AP Up Time	Admin Status	Operational Status
AP7cad.74ff.7b5e	10.4.8.21	AIR-CAP37021-A-K9	7c:ad:74:ff:7b:5e	28 d, 06 h 33 m 36 s	Enabled	REG
APe02f.6da3.52d4	10.4.8.22	AIR-CAP26021-A-K9	e0:2f:6d:a3:52:d4	28 d, 05 h 51 m 29 s	Enabled	REG
AP4403.a7a2.fe2c	10.4.8.20	AIR-CAP36021-A-K9	44:03:a7:a2:fe:2c	28 d, 06 h 00 m 25 s	Enabled	REG

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 at the top of the screen click **Apply**.

General		Versions	
AP Name	AP7cad.74ff.7b5e	Primary Software Version	7.6.120.0
Location	default location	Backup Software Version	0.0.0.0
AP MAC Address	7c:ad:74:ff:7b:5e	Predownload Status	None
Base Radio MAC	08:cc:68:b5:43:90	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	15.2.4.0
Operational Status	monitor	IOS Version	15.2(4)1B5\$
Port Number	Unspecified	Mini IOS Version	7.6.1.118
Venue Group	Unspecified	IP Config	
Venue Type	Unspecified	IP Address	10.4.8.21
Venue Name		Static IP	<input type="checkbox"/>
Language			

Step 4: At the prompt, select OK.

Warning: Changing AP Mode will reboot the AP and will rejoin the controller after a few minutes. Are you sure you want to continue?

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

Step 5: When the access point is available again from the **Wireless** tab, select the access point, use a text editor to copy the Network Spectrum Interface Key and the IP address for later use when configuring the MetaGeek Chanalyzer application.

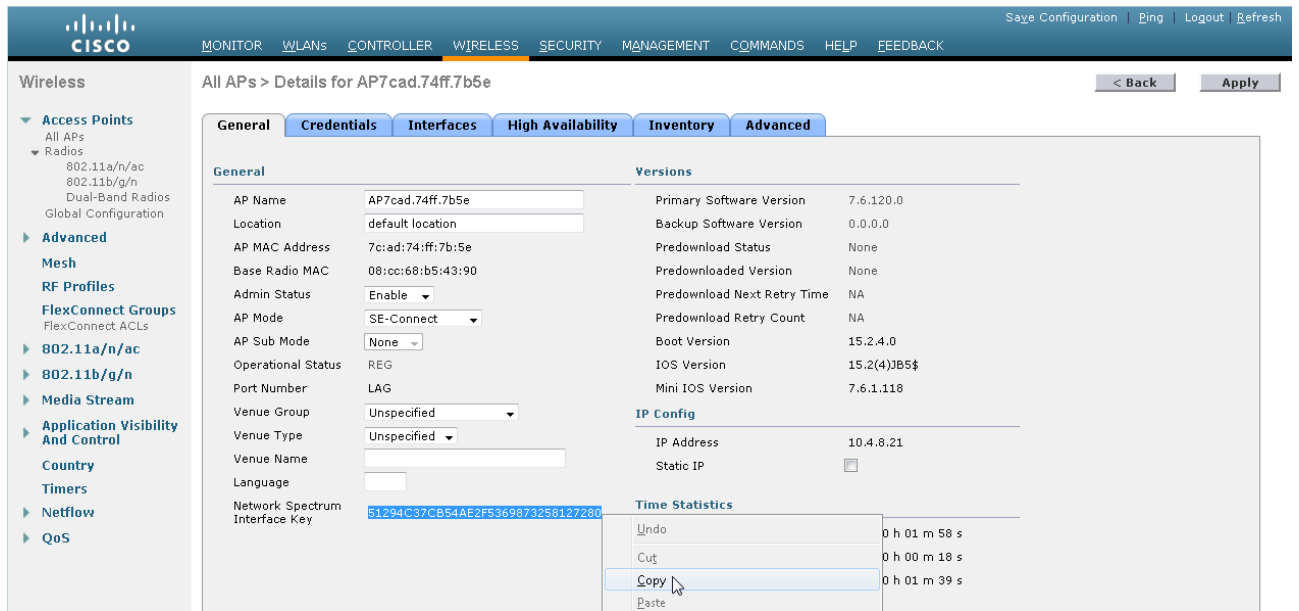
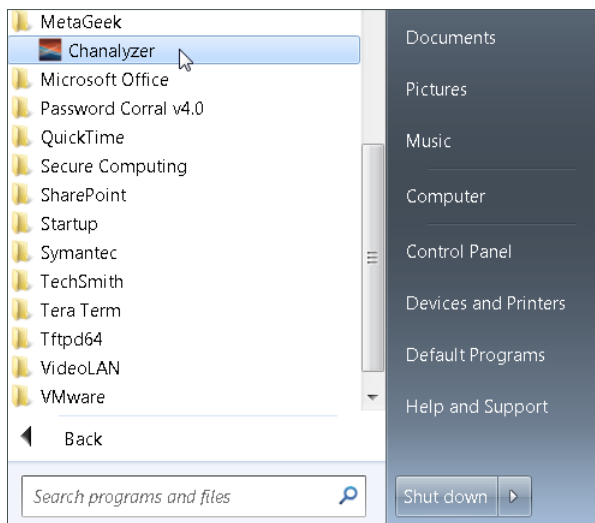


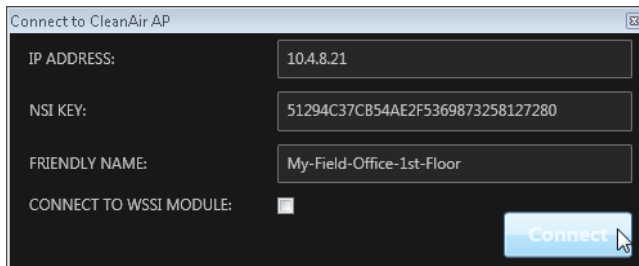
Table 2 - SE-Connect Access Point Information

Value	Example	Site Specific Values
Network Spectrum Interface Key	51294C37CB54AE2F5369873258127280	
AP-IP Address	10.4.8.21	

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 access point 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**.



Connect to CleanAir AP

IP ADDRESS: 10.4.8.21

NSI KEY: 51294C37CB54AE2F5369873258127280

FRIENDLY NAME: My-Field-Office-1st-Floor

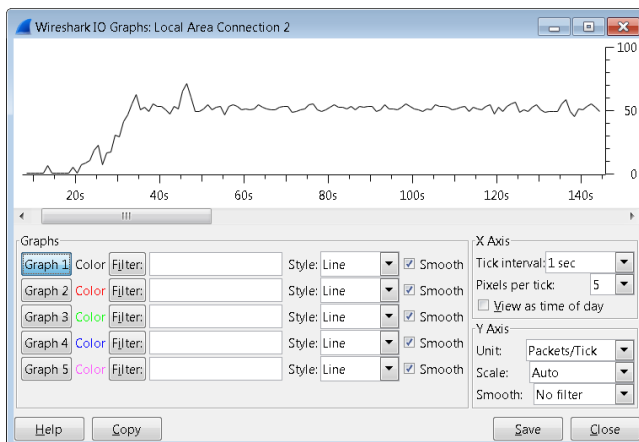
CONNECT TO WSSI MODULE:

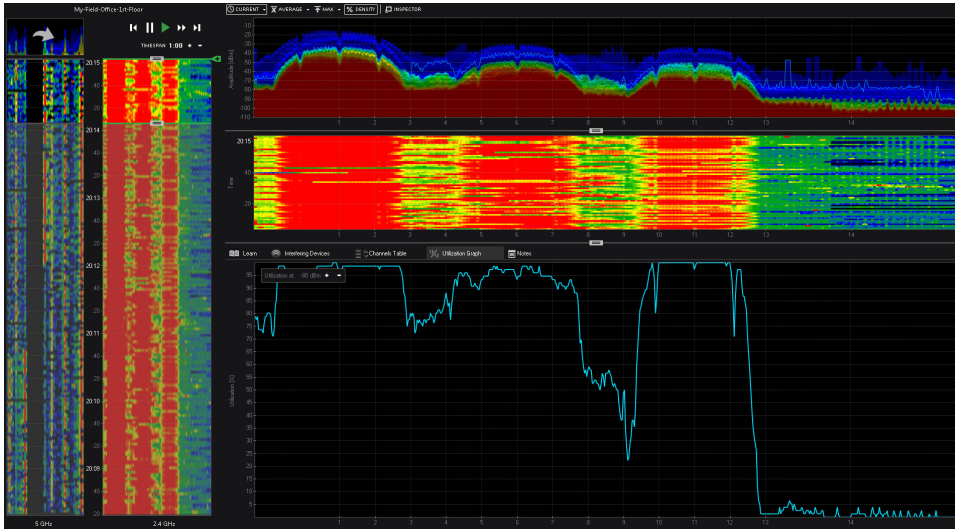
Connect

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.





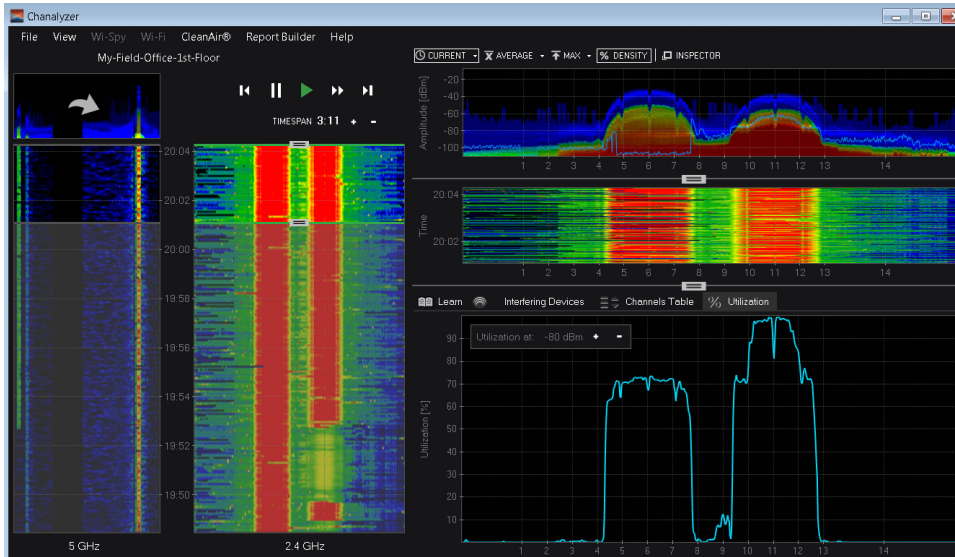
Reader Tip

In the graphic above, because the access point is placed in SE-Connect mode, the complete licensed band is visible (channels 1-14 in the 2.4GHz band for the United States).

Procedure 3

Remote Spectrum Analysis using MetaGeek Chanalyzer

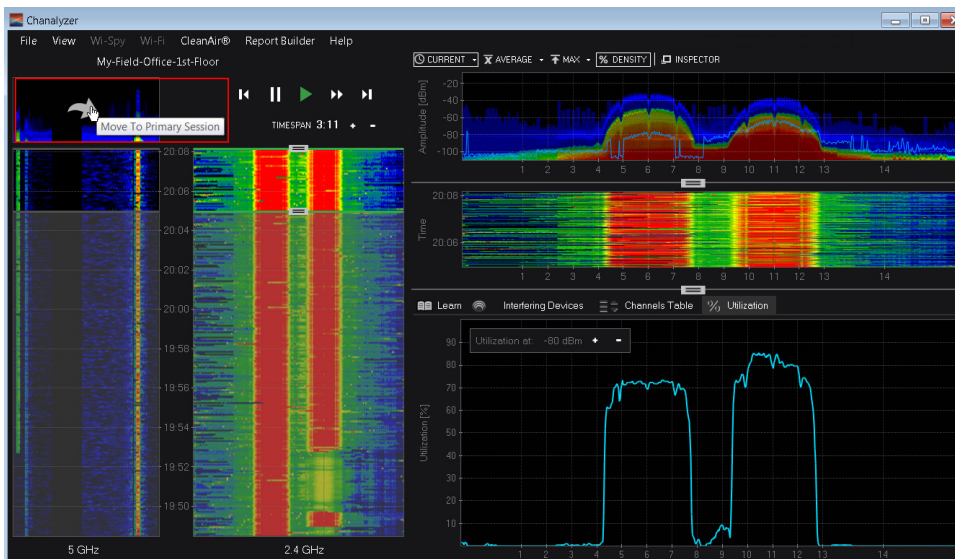
By using the Cisco CleanAir capability of the MetaGeek Chanalyzer product, the network administrator has real-time, physical-layer RF spectrum intelligence without having to drive or fly onsite. The following figure illustrates this capability in a Wi-Fi-only environment and gives you an understanding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



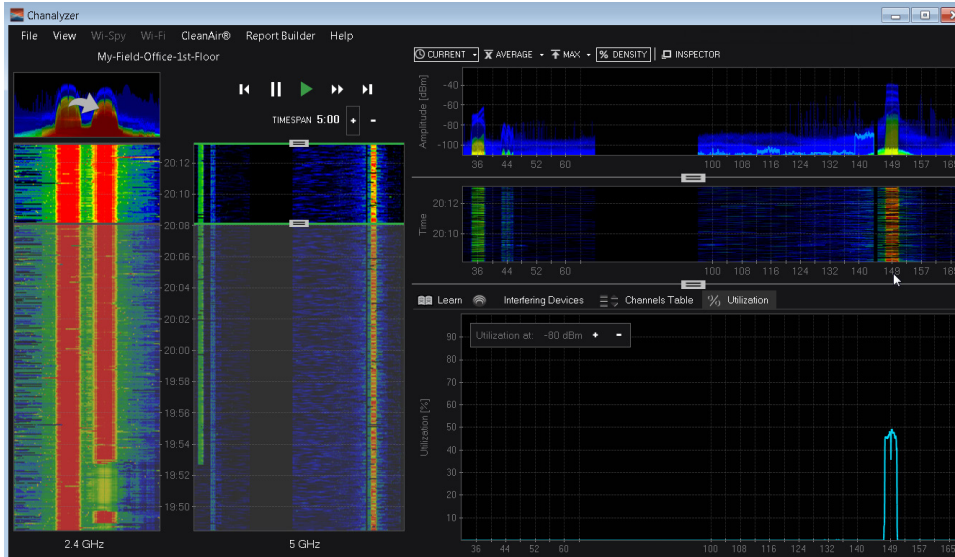
In the graphic shown above, the network administrator can easily determine that the utilization on Channel 6 and channel 11 (in the 2.4GHz band) are relatively heavily utilized. This is evident in the following:

- 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

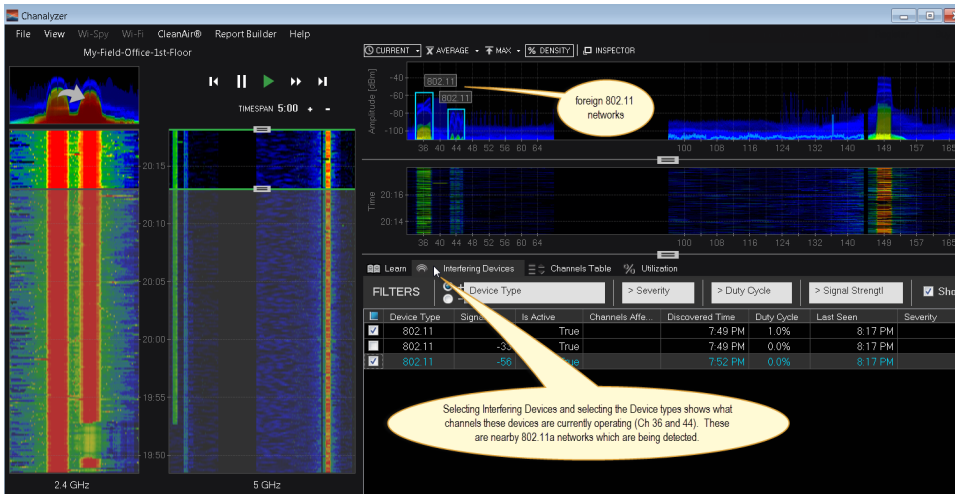
Step 1: To make the 5GHz band the primary band for the current session, select the arrow at the top of the 5GHz waterfall on the far left.



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%.



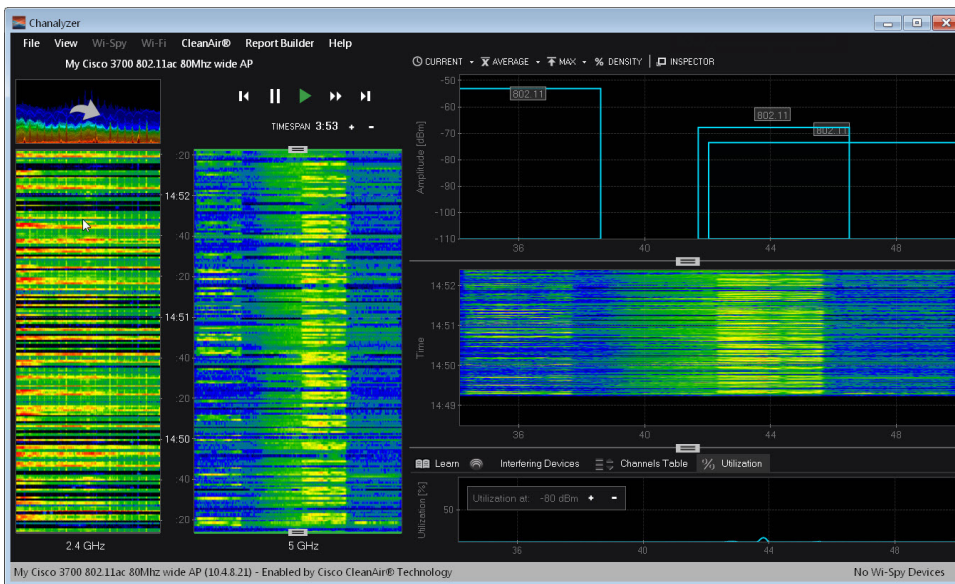
Step 3: To determine the type of interference affecting the 5GHz band, select the Interfering Devices from the Utilization graph in the lower right quadrant. In the example shown, foreign 802.11 networks are operating on channel 36 and 44.



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, it 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

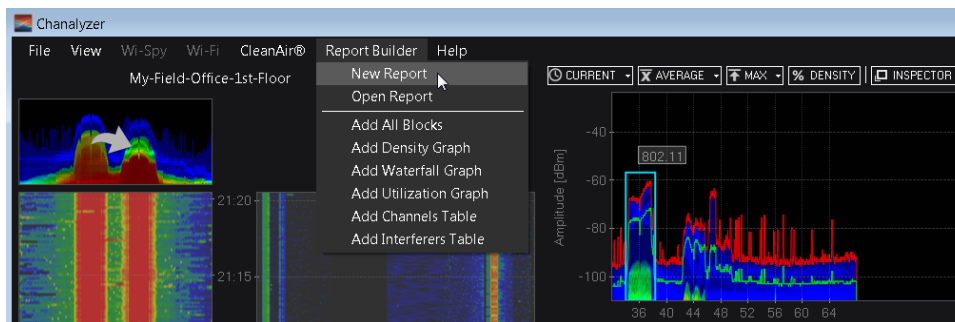
One of the powerful capabilities of the Chanalyzer product is the ability to create custom on-demand reports. By selecting a timespan during which an interesting event has occurred, it is possible to add any of the resulting graphs to the report. This DVR like capability allows you to select timespans 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.

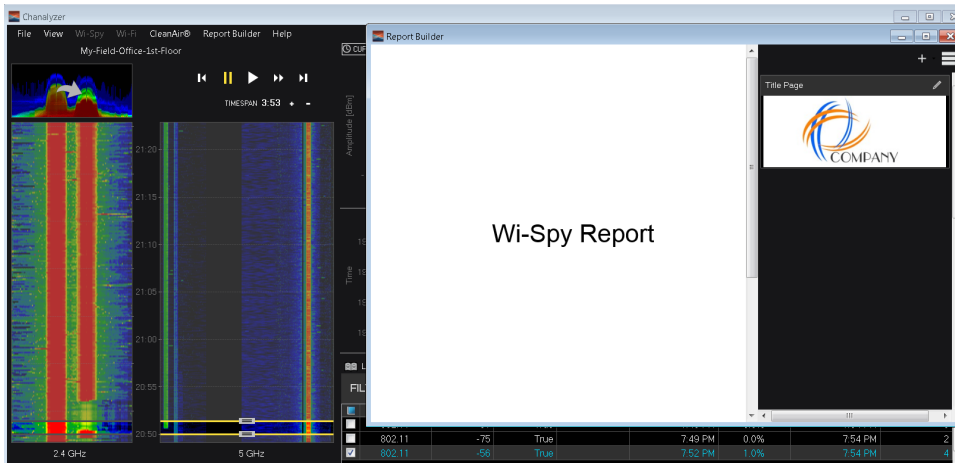
Step 1: Select the timespan when an event has occurred that needs to be included in the report. This can be done by using the controls on the 2.4GHz or 5GHz band. Notice how the information displayed in the graphs on the right only displays the data within the timespan selected.



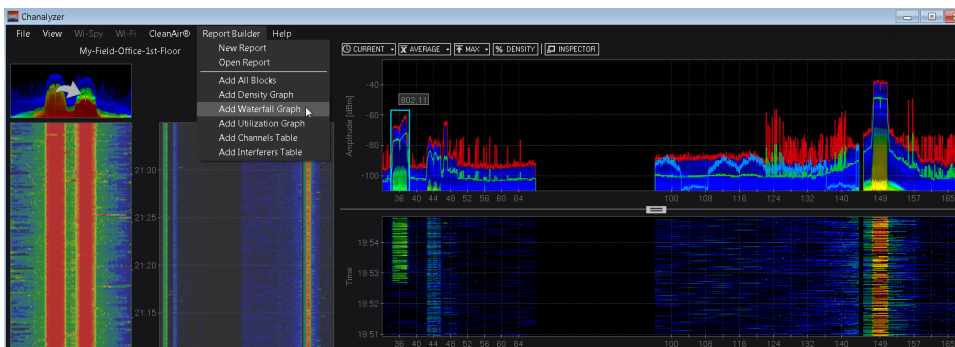
Step 2: Create a new report by navigating to Report Builder > New Report.



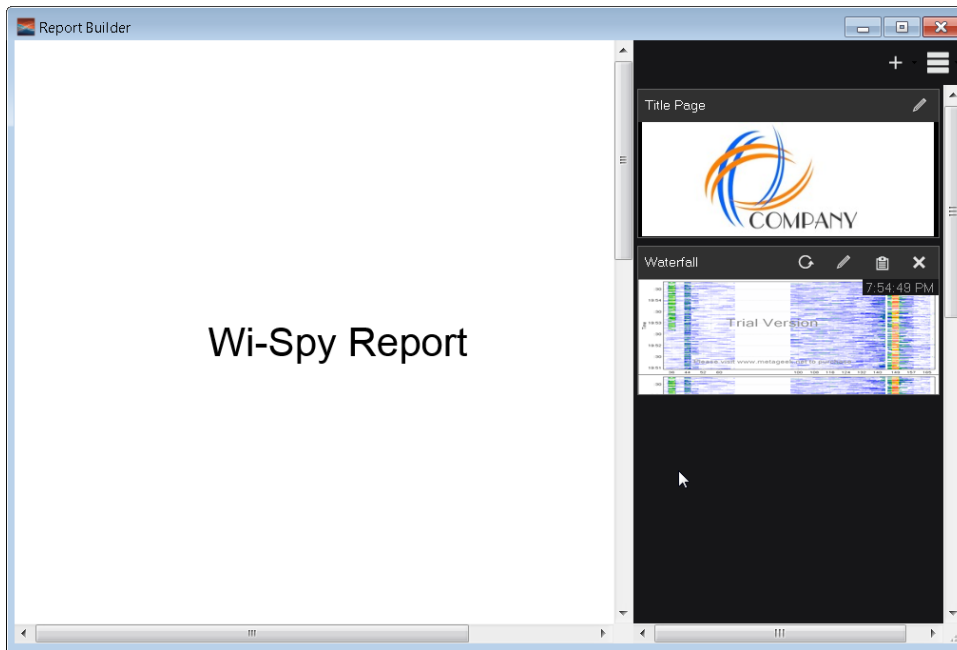
Step 3: A new report window will appear which will contain each of the graphs inserted and described in the following steps. It is possible to customize the title page by selecting edit pencil on the title screen shown on the right.



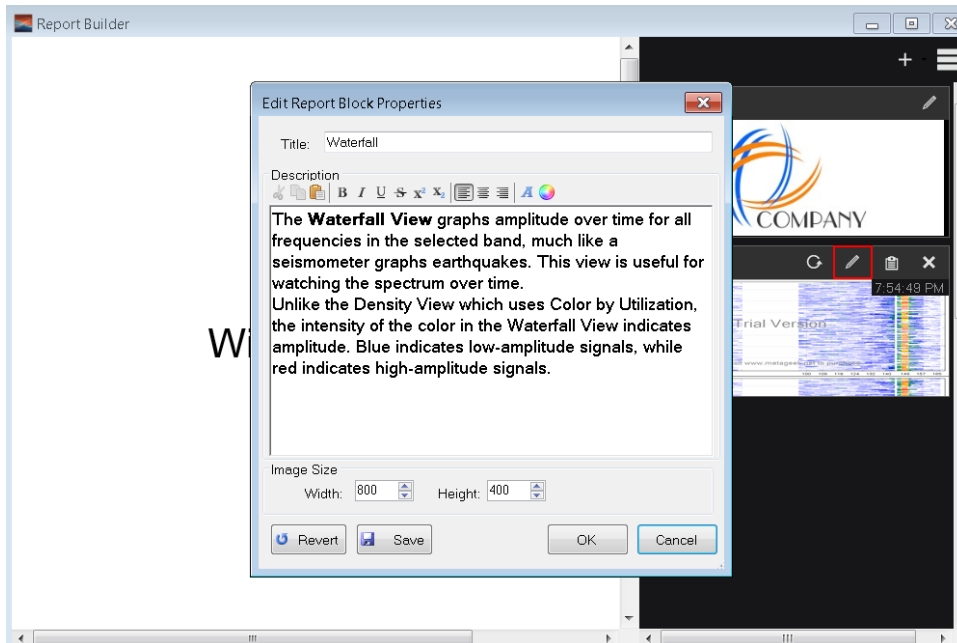
Step 4: In the example above, we see interference beginning on channel 36 as indicated by the start of a green line. To add the waterfall graph to the report select **Report Builder > Add Waterfall Graph**.



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

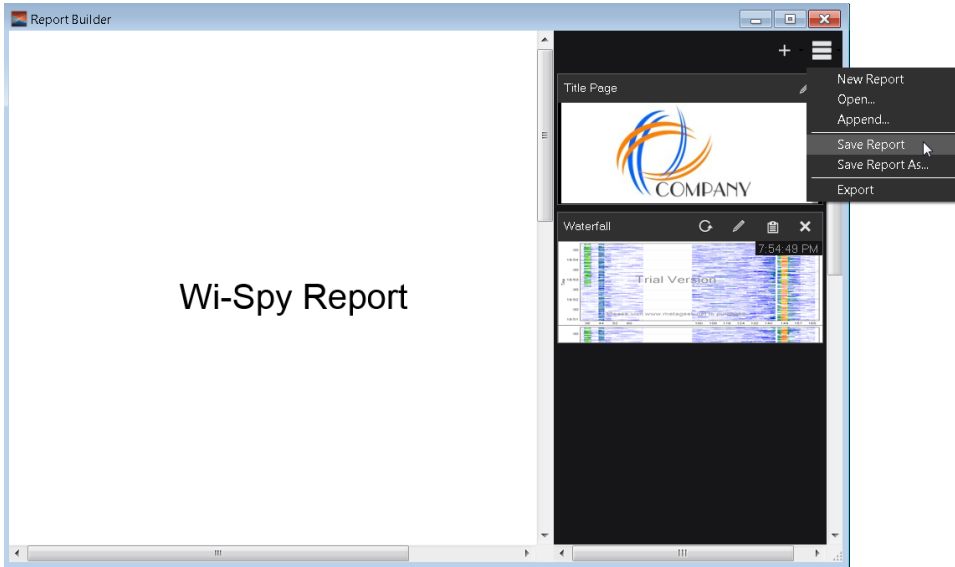


Step 6: To modify the text that appears with the Waterfall graphic in the report, select the edit pencil on the Waterfall graph. An example explanation of this event might be “The Waterfall graph shows the beginning of the interference from the adjacent retail operation (ABC Company) when they begin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

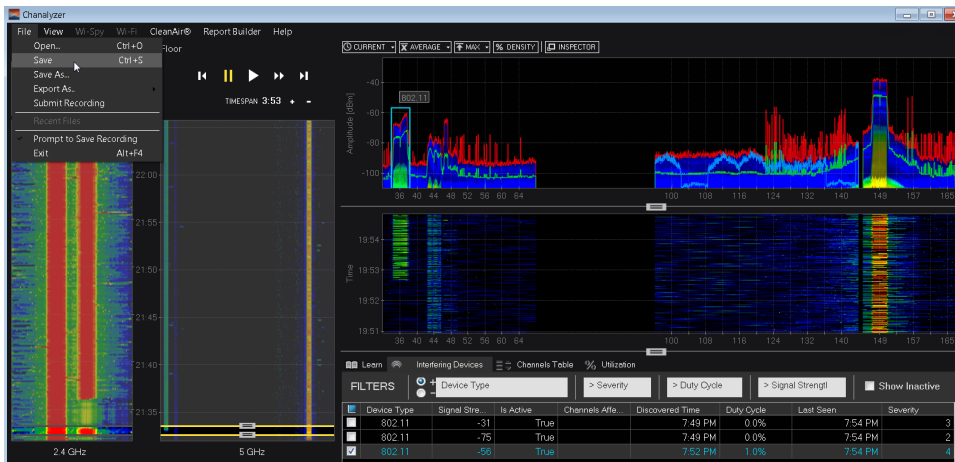


Additional graphs and timespans can be added to the report as necessary.

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	7.6.120.0
	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 Primary SKU for Adder Licenses	L-LIC-CTVM-UPG	
	Cisco Virtual Wireless Controller 1 Access Point Adder License	L-LIC-CTVM-1A	
	Cisco Virtual Wireless Controller 5 Access Point Adder License	L-LIC-CTVM-5A	
	Cisco Virtual Wireless Controller 25 Access Point Adder License	L-LIC-CTVM-25A	
On Site, Remote Site, or Guest Controller	Cisco 5500 Series Wireless Controller for up to 500 Cisco access points	AIR-CT5508-500-K9	7.6.120.0
	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	7.6.120.0
	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	7.6.120.0
	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=	7.6.120.0
	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	7.6.120.0
	MSE License PAK (E Delivery)	L-MSE-PAK	
	1 AP WIPS Monitor Mode license	L-WIPS-MM-1AP	
	100 AP WIPS Monitor Mode licenses	L-WIPS-MM-100AP	
	1000 AP WIPS Monitor Mode licenses	L-WIPS-MM-1000AP	

Network Management

Functional Area	Product Description	Part Numbers	Software
Network Management	Cisco Prime Infrastructure 2.x	R-PI2X-K9	2.x
	Prime Infrastructure 2.1 Software	R-PI21-SW-K9	2.1
	Prime Infrastructure 2.x Base License	L-PI2X-BASE	2.x
	Prime Infrastructure 2.x - Lifecycle - 25 Device License	L-PI2X-LF-25	
	Prime Infrastructure 2.x - Lifecycle - 50 Device License	L-PI2X-LF-50	
	Prime Infrastructure 2.x - Lifecycle - 100 Device License	L-PI2X-LF-100	
	Prime Infrastructure 2.x - Lifecycle - 500 Device License	L-PI2X-LF-500	
	Prime Infrastructure 2.x - Lifecycle - 1K Device Lic	L-PI2X-LF-1K	
	Prime Infrastructure 2.x - Lifecycle - 2.5K Device Lic	L-PI2X-LF-2.5K	
	Prime Infrastructure 2.x - Lifecycle - 5K Device License	L-PI2X-LF-5K	
	Prime Infrastructure 2.x - Lifecycle - 10K Device License	L-PI2X-LF-10K	
	Prime Infrastructure 2.x - Lifecycle - 15K Device License	L-PI2X-LF-15K	
	MetaGeek Chanalyzer 5 with Report Builder and Cisco CleanAir	SFW-CHAN-RC	5.0

Data Center Virtualization

Functional Area	Product Description	Part Numbers	Software
VMWare	ESXi	ESXi	5.0.0

Appendix B: Changes

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

- We refreshed this guide to reflect the changes in the operation of the Cisco Prime Infrastructure GUI, based on the version listed in Appendix A: Product List.

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.

© 2014 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)