Getting Started

This chapter provides information on prerequisites, system requirements, and enabling the Cisco CMX analytics service.

This chapter contains the following sections:

Prerequisites for Enabling CMX Analytics Service

- The CMX analytics system takes input from the Cisco Mobilily Service Engine (MSE). The CMX analytics is installed as part of the MSE installation but you must select CMX Analytics service explicitly from the list of available services in the Prime Infrastructure UI. For details on enabling the CMX analytics service, see the "Enabling CMX Analytics Service on the Mobility Services Engine" section on page 2-46.
- If you want to use data from specific parts of your network, then you must edit the `mse.properties` (`/opt/mse/analytics/intellify/tools/MSEclient/mse.properties`) file in order to select either network, building, or floor that you want to analyze.

  Follow these guidelines when editing the `mse.properties` file.

  - Network, building, or floors—By default, the analytics takes all the data that is available in the MSE. These three settings allow you to download only a subset. For example, if you have three building B1, B2, and B3 in network N and want to run analytics only on building B1 and building B2, then you need to specify as `buildings=N>B1,N>B2`.
  - max-history—By default, when the analytics becomes active for the first time, it searches for the previous three days data in the MSE history file and tries to fetch data if there is any. If there is more data available in the history file and you want to retrieve, then you must set this to a different value.

    If you set the max-history to `nnnD`, then it retrieves nnn days and if you set to `nnnW`, then it retrieves nnn weeks.
  - Control the size of the database—A new parameter `Prune db parameters` is added in the mse.properties file to help control the size of the database. Once the database reaches the threshold value of 5million points, it removes the oldest data to reset the size to 4.9 million points.

Note In order for the CMX analytics to access data from the MSE, you must set the history parameters on the MSE. For more information, see the "Configuring MSE Tracking and History Parameters" section on page 2-23.

Note Depending on your browser and the hardware, images over 2MB may not appear in the 3D environment. In the `mse.properties` file, set the value of `max-dimension`. For example, setting `max-dimension` to 2048 can reduce the resolution of the picture to at most 2048 pixels on the longest side.

  - All settings (including the above mentioned information) are documented in the properties file.
- CMX analytics requires both floor plans and coverage areas to be defined in the Prime Infrastructure UI in order for CMX analytics visualization and reporting to function. You need to provide floor numbers for each floor plan. Floors on the same level should have the same number and floors above should have a higher number. The choice of coverage areas correspond to the zones which you want to report on. If you want to know the details of location A, then an area defining that location should be made available in the Prime Infrastructure. See the "Adding Floor Areas" section on page 2-36 and "Defining Coverage Area" section on page 2-41 for more information.

- You must define at least three GPS markers for each floor in the Prime Infrastructure UI.
- You need three APs to get any location information on the device.

Prime Infrastructure Delivery Modes

Prime Infrastructure comes preinstalled on a physical appliance with various performance characteristics. Prime Infrastructure software runs on either a dedicated Prime Infrastructure appliance or on a VMware server. Prime Infrastructure software image does not support the installation of any other packages or applications on this dedicated platform. The inherent scalability of Prime Infrastructure allows you to add appliances to a deployment and increase performance and resiliency.

Prime Infrastructure is delivered in two modes, the physical appliance and the virtual appliance. This section contains the following topics:

Physical Appliance

The physical appliance is a dual Intel 2.40 GHz Xeon E5620 quad core processor, with 16 GB RAM, and four hard drives running in a RAID level 5 configuration. The physical appliance runs the latest 64-bit Red Hat Linux Operating System.

The physical appliance supports up to 15000 Cisco Aironet lightweight access points, 5000 standalone access points, 5000 switches and 1200 Cisco wireless LAN controllers.

Note To receive the expected results with the Prime Infrastructure, you need a high performance physical appliance with built-in redundancy for hard disks, power supplies and internal cooling fans.

Virtual Appliance

Prime Infrastructure is also offered as a virtual appliance to help support lower level deployments. Prime Infrastructure can be run on a workstation or a server and access points can be distributed unevenly across controllers.

Prime Infrastructure virtual appliance software is distributed as an Open Virtualization Archive (OVA) file. There are three recommended levels of Prime Infrastructure distribution with different resources and numbers of devices supported.

This section contains the following topics:

Note You can deploy the OVA file directly from the vSphere Client; you do not need to extract the archive before performing the deployment.

You can install the Prime Infrastructure virtual appliance using any of the methods for deploying an OVF supported by the VMware environment. Before starting, make sure that Prime Infrastructure virtual appliance distribution archive is in a location that is accessible to the computer on which you are running the vSphere Client.

Note For more information about setting up your VMware environment, see the VMware vSphere 4.0 documentation.

Virtual Appliance for Large Deployment

- Supports up to 15000 Cisco Aironet lightweight access points, 5000 standalone access points, 5000 switches, and 1200 Cisco wireless LAN controllers.
- 16 Processors at 2.93 GHz or better.
- 16-GB RAM.
- 300 GB minimum free disk space is required on your hard drive.

Note The free disk space listed is a minimum requirement but might be different for your system depending on the number of backups that are performed.

Virtual Appliance for Medium Deployment

- Supports up to 7500 Cisco Aironet lightweight access points, 2500 standalone access points, 2500 switches, and 600 Cisco wireless LAN controllers.
- 8 Processors at 2.93 GHz or better.
- 12-GB RAM.
- 300 GB minimum free disk space is required on your hard drive.

Virtual Appliance for Small Deployment

- Supports up to 3000 Cisco Aironet lightweight access points, 1000 standalone access points, 1000 switches, and 240 Cisco wireless LAN controllers.
- 4 Processors at 2.93 GHz or better.
- 8-GB RAM.
- 200 GB minimum free disk space is required on your hard drive.

Note The free disk space listed is a minimum requirement, but several variables (such as backups) impact the disk space.

Operating Systems Requirements

The following operating systems are supported:

- Red Hat Linux Enterprise server 5.4 64-bit operating system installations are supported.
- Red Hat Linux version support on VMware ESX version 3.0.1 and later with either local storage or SAN over fiber channel.
- The recommended deployments for a virtual appliance are UCS and ESX/ESXi.

Note Individual operating systems running Prime Infrastructure in VMware must follow the specifications for the size of Prime Infrastructure that you intend to use.

Client Requirements

Prime Infrastructure user interface requires Mozilla Firefox 11.0 or 12.0 or Internet Explorer 8 or 9 with the Chrome plug-in releases or Google Chrome 19.0.

Note We strongly advise that you do not enable third-party browser extensions. In Internet Explorer, you can disable third-party browser extensions by choosing Tools > Internet Options and unselecting the Enable third-party browser extensions check box on the Advanced tab.

The client running the browser must have a minimum of 1 GB of RAM and a 2-GHz processor. The client device should not be running any CPU or memory-intensive applications.

Note We recommend a minimum screen resolution of 1280 x 800 pixels.

Prerequisites

Before installing Prime Infrastructure, ensure that you have completed the following:

- Meet the necessary hardware and software requirements for Prime Infrastructure.
- Check the compatibility matrix for the supported controller, Cisco IOS software releases.
- Update your system with the necessary critical updates and service packs.

Note See the latest release notes for information on the service packs and patches required for correct operation of Prime Infrastructure.

- To receive the expected results, you should run no more than 3 concurrent Prime Infrastructure setups for standard server use (4 GB memory and 3 GHz CPU speed) and no more than 5 concurrent Prime Infrastructure setups for high-end server use (8 GB memory and 3 GHz CPU speed).
- Verify that the following ports are open during installation and startup:
  - HTTP: configurable during install (80 by default)
  - HTTPS: configurable during install (443 by default)

- 1315
- 1299
- 6789
- 8009
- 8456
- 8005
- 69
- 21
- 162
- 8457
- 1522 (for HA configuration between the primary and secondary Prime Infrastructure)

Note Make sure your firewall rules are not restrictive. You can check the current rules on Linux with the built-in iptables -L command.

Reinstalling Prime Infrastructure on a Physical Appliance

You must have root privileges to install Prime Infrastructure on a physical appliance.

To reinstall Prime Infrastructure on a physical appliance, follow these steps:

Step 1 Insert the provided Prime Infrastructure software Image DVD. The system boots up and the following console appears:

```
ISOLINUX 3.11 2005-09-02  Copyright (C) 1994-2005

           Welcome to Cisco Prime Infrastructure

To boot from hard disk, press <Enter>.

Available boot options:

  [1] Prime Infrastructure Installation (Keyboard/Monitor)
  [2] Prime Infrastructure Installation (Serial Console)
  [3] Recover administrator password. (Keyboard/Monitor)
  [4] Recover administrator password. (Serial Console)
  <Enter> Boot existing OS from Hard Disk.

Enter boot option and press <return>.

boot:
```

Step 2 Select option 1 to reinstall Prime Infrastructure software image. The system reboots and the configure appliance screen appears.

Step 3 Enter the initial setup parameters and the system reboots again. Remove the DVD and follow the steps to start the Prime Infrastructure server.

Deploying Prime Infrastructure Virtual Appliance

This section describes how to deploy the Prime Infrastructure virtual appliance from the VMware vSphere Client using the Deploy OVF Wizard or from the command line. (VMware vSphere Client is a Windows application for managing and configuring the vCenter Server.) This section contains the following topics:

Deploying Prime Infrastructure Virtual Appliance from the VMware vSphere Client

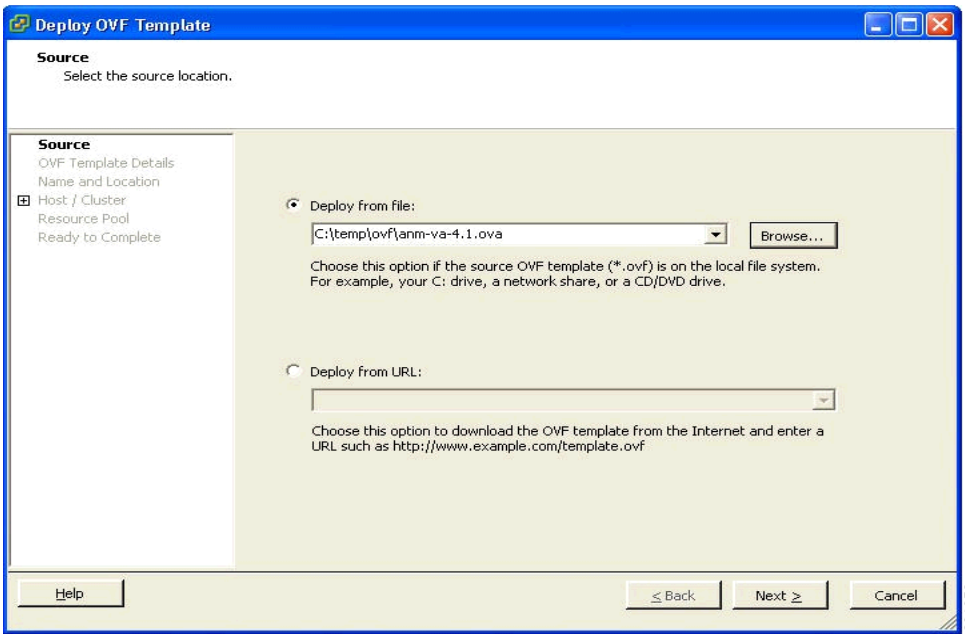
Prime Infrastructure Virtual Image is packaged as an OVA file. An OVA is a collection of items in a single archive. In the vSphere Client, you can use the Deploy OVF Wizard to create a virtual machine, running the Prime Infrastructure virtual appliance application, as described in this section.

Note While the following procedure provides a general guideline for how to deploy the Prime Infrastructure virtual appliance, the exact steps that you need to perform might vary depending on the characteristics of your VMware environment and setup.

To deploy the Prime Infrastructure virtual appliance, follow these steps:

Step 1 From the VMware vSphere Client main menu, choose **File > Deploy OVF Template**. The Deploy OVF Template Source window appears (see Figure 2-1).

Figure 2-1 Deploy OVF Template Window

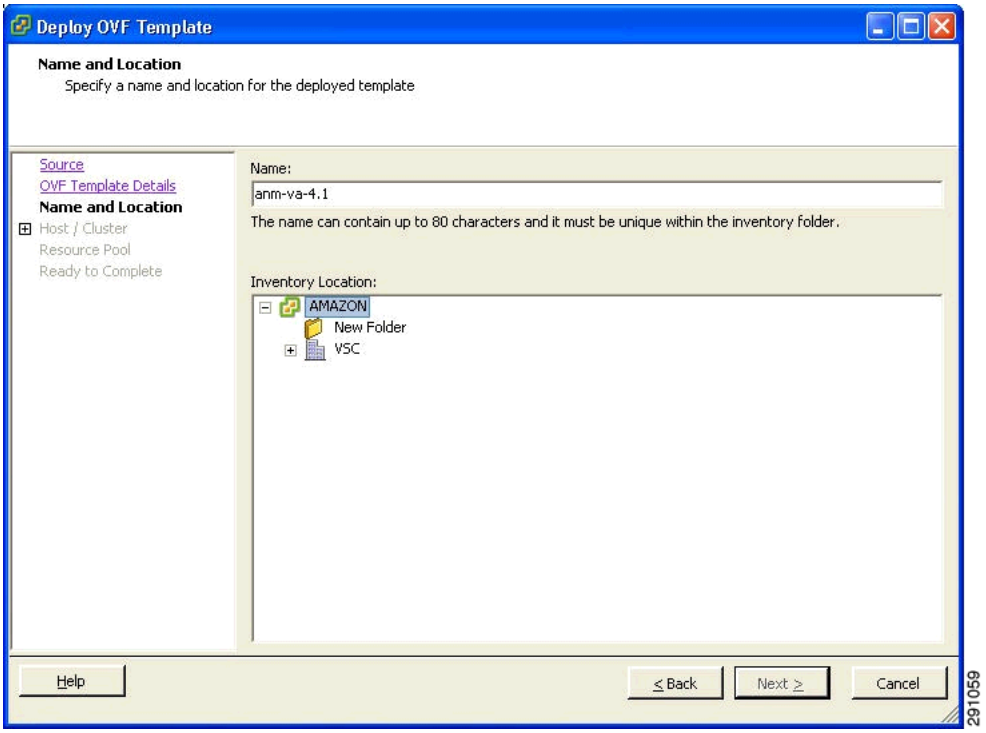


Step 2 Choose **Deploy from file** and choose the OVA file that contains the Prime Infrastructure virtual appliance distribution.

Step 3 Click **Next**. The OVF Template Details window appears. VMware ESX/ESXi reads the OVA attributes. The details include the product you are installing, the size of the OVA file (download size), and the amount of disk space that needs to be available for the virtual machine (size on disk).

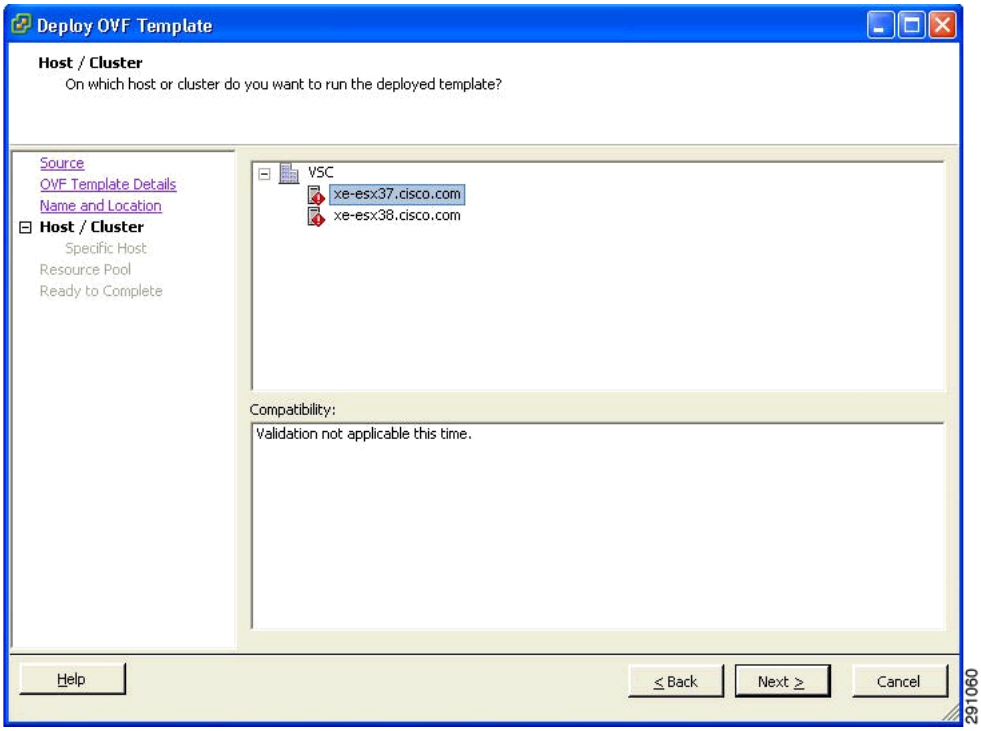
Step 4 Verify the OVF Template details and click **Next**. The Name and Location window appears (see Figure 2-2).

Figure 2-2 Name and Location Window



Step 5 Either keep the default name for the VM to be deployed in the Name text box or provide a new one and click **Next**. This name value is used to identify the new virtual machine in the VMware infrastructure; you should use any name that distinguishes this particular VM in your environment. The Host / Cluster window appears (see Figure 2-3).

Figure 2-3 Host/Cluster Window



Step 6 Choose the destination host or HA cluster on which you want to deploy the Prime Infrastructure VM, and click **Next**. The Resource Pool window appears.

Step 7 If you have more than one resource pool in your target host environment, choose the resource pool to use for the deployment, and click **Next**. The Ready to Complete window appears.

Step 8 Review the settings shown for your deployment and, if needed, click **Back** to modify any of the settings shown.

Step 9 Click **Finish** to complete the deployment. A message notifies you when the installation completes and you can see the Prime Infrastructure virtual appliance in your inventory.

Step 10 Click **Close** to dismiss the Deployment Completed Successfully dialog box.

Deploying Prime Infrastructure Virtual Appliance using the Command Line Client

This section describes how to deploy Prime Infrastructure virtual appliance from the command line. As an alternative to using the vSphere Client to deploy Prime Infrastructure OVA distribution, you can use the VMware OVF Tool, which is a command-line client.

To deploy an OVA with the VMware OVF Tool, use the **ovftool** command, which takes the name of the OVA file to be deployed and the target location as arguments, as in the following example:

```
ovftool Prime Infrastructure-VA-X.X.X-large.ova vi://my.vmware-host.example.com/
```

In this case, the OVA file to be deployed is Prime Infrastructure-VA-X.X.X-large.ova and the target ESX host is my.vmware-host.example.com. For complete documentation on the VMware OVF Tool, see the VMware vSphere 4.0 documentation.

Setting Up Prime Infrastructure

This section describes how to configure the initial settings of Prime Infrastructure virtual appliance.

Note These steps need to be performed only once, upon first installation of Prime Infrastructure virtual appliance.

To configure the basic network and login settings for Prime Infrastructure virtual appliance system, follow these steps. When the steps are completed, Prime Infrastructure virtual appliance is accessible over the network.

Note Once you put Prime Infrastructure Image DVD in the physical appliance for reinstallation, you get the same console prompt. Use the following steps to reinstall Prime Infrastructure for the physical appliance.

Step 1 At the login prompt, enter the **setup** command.

```
localhost.localdomain login: setup
```

Prime Infrastructure configuration script starts. The script takes you through the initial configuration steps for Prime Infrastructure virtual appliance. In the first sequence of steps, you configure network settings.

Step 2 When prompted, enter the following settings:

a. The hostname for the virtual appliance.

b. The IP address for the virtual appliance.

c. The IP default subnet mask for the IP address entered.

d. The IP address of the default gateway for the network environment in which you are creating the virtual machine.

e. The default DNS domain for the target environment.

f. The IP address or hostname of the primary IP nameserver in the network.

g. At the Add/Edit another nameserver prompt, you can enter **y** (yes) to add additional nameservers, if desired. Otherwise, press **Enter** to continue.

h. The NTP server location (or accept the default by pressing **Enter**). At the Add/Edit secondary NTP server prompt, you can enter **y** (yes) to add another NTP server. Otherwise, enter **n** (no) to continue.

Step 3 Enter the username for the user account used to access Prime Infrastructure system running on the virtual machine. The default username is admin, but you can change this to another username by typing it here.

Step 4 Enter the password for Prime Infrastructure. The password must be at least eight characters and must include both lowercase and uppercase letters and at least one number. It cannot include the username. After you enter the password, the script verifies the network settings you configured. For example, it attempts to reach the default gateway that you have configured.

After verifying the network settings, the script starts Prime Infrastructure installation processes. This process can take several minutes, during which there is no screen feedback. When finished, the following banner appears on the screen:

```
=== Initial Setup for Application: Prime Infrastructure ===
```

After this banner appears, the configuration starts with database scripts and reboots the server.

Note If you are installing a physical appliance, remove the ISO DVD from the DVD tray.

Step 5 Log in as admin and enter the admin password.

Step 6 Exit the console using the **exit** command.

Starting the Prime Infrastructure Server

This section provides instructions for starting Prime Infrastructure on either a physical or virtual appliance.

To start Prime Infrastructure when it is installed on a physical or virtual appliance, follow these steps:

Step 1 Log into the system as administrator.

Step 2 Using the command-line interface, enter the following command:

```
ncs start
```

Logging into Prime Infrastructure User Interface

To log into Prime Infrastructure user interface through a web browser, follow these steps:

Step 1 Launch Internet Explorer 8 or 9 or Mozilla Firefox 11.0 or 12.0 on a different computer than the one on which you installed and started Prime Infrastructure.

Note When you use Firefox to log in and access Prime Infrastructure for the first time, the Firefox web browser displays a warning stating that the site is untrustable. When Firefox displays this warning, follow the prompts to add a security exception and download the self-signed certificate from Prime Infrastructure server. After you complete this procedure, Firefox accepts Prime Infrastructure server as a trusted site both now and during all future login attempts.

Step 2 In the address line of browser, enter https://ncs-ip-address, where ncs-ip-address is the IP address of the server on which you installed and started Prime Infrastructure. Prime Infrastructure user interface displays the Login page.

Step 3 Enter your username. The default username is root.

Step 4 Enter the root password you created during setup.

Note If any licensing problems occur, a message appears in an alert box. If you have an evaluation license, the number of days until the license expires is shown. You are also alerted to any expired licenses. You have the option to go directly to the licensing page to address these problems.

Step 5 Click **Login** to log into Prime Infrastructure. Prime Infrastructure user interface is now active and available for use. Prime Infrastructure home page appears. Prime Infrastructure home page enables you to choose the information that you want to see. You can organize the information in user-defined tabs called dashboards. The default view comes with default dashboards and preselected dashlets for each, and you can arrange them as you like. You can predefine what appears on the home page by choosing the monitoring dashlets that are critical for your network. For example, you might want different monitoring dashlets for a mesh network so that you can create a customized mesh dashboard.

Note If the database or Apache web server does not start, check the launchout.txt file in Linux. You see a generic "failed to start database" or "failed to start the Apache web server" message.

Note When an upgrade occurs, the user-defined tabs arranged by the previous user in the previous version are maintained. Therefore, the latest dashlets might not show. Look at the Edit dashboard link to find what new dashlets are added.

The home page provides a summary of the Cisco Unified Network Solution, including coverage areas, the most recently detected rogue access points, access point operational data, reported coverage holes, and client distribution over time.

By default, you should see six dashboards in Prime Infrastructure home page: the General, Client, Security, Mesh, CleanAir, and ContextAware dashboards.

Note When you use Prime Infrastructure for the first time, the network summary pages show that the Controllers, Coverage Areas, Most Recent Rogue APs, Top 5 APs, and Most Recent Coverage Holes databases are empty. It also shows that no client devices are connected to the system. After you configure Prime Infrastructure database with one or more controllers, Prime Infrastructure home page provides updated information.

To exit Prime Infrastructure user interface, close the browser page or click **Log Out** in the upper-right corner of the page. Exiting an Prime Infrastructure user interface session does not shut down Prime Infrastructure on the server.

When a system administrator stops Prime Infrastructure server during your Prime Infrastructure session, your session ends, and the web browser displays the message: "The page cannot be displayed." Your session does not reassociate to Prime Infrastructure when the server restarts. You must restart Prime Infrastructure session.

Managing Licenses

This section contains the following topics:

License Center

The License Center allows you to manage Prime Infrastructure, wireless LAN controllers, and MSE licenses. The License Center is available from Prime Infrastructure Administration menu. To view the License Center page, choose **Administration > License Center**.

Note Although Prime Infrastructure and MSE licenses can be fully managed from the License Center, WLC licenses can only be viewed. You must use WLC or CLM to manage WLC licenses.

Tip To learn more about Prime Infrastructure License Center, go to Cisco.com to watch a multimedia presentation. Here you can also find the learning modules for a variety of Prime Infrastructure topics. Over future releases, we will add more overview and technical presentations to enhance your learning.

This section contains the following topics:

Prime Infrastructure License Information

Prime Infrastructure Licenses portion of the License Center page displays the following:

- Feature—The type of license. It can be Prime Infrastructure or DEMO.
- Device Limit—The total number of licensed access points and switches.
- Device Count—The current number of access points and switches using licenses.

  Note AP count includes both associated and unassociated access points. When you are near the AP limit, you can delete any unassociated access points to increase available license capacity. For a demo license, you can click the "If you do not have a Product Authorization Key (PAK), please click here for available licenses" link and choose **Wireless Control System Trial License**.

  Note Autonomous access points are not counted towards the total device count for your license.

- % Used—The percentage of access points and switches licensed across Prime Infrastructure. If the percentage drops to 75%, the value appears in red. At this level, a message also appears indicating that both associated and unassociated access points are part of the AP count.
- Type—Permanent if all licenses are permanent. If any licenses are evaluations (or demos), it shows the number of days remaining on the license that has the fewest number of days until expiration.

Note To obtain a new license for Prime Infrastructure, go to the Product License Registration link

(https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet)

and provide your Product Authorization Key (PAK) and hostname.

Note If you choose **Summary > Prime Infrastructure** from the left sidebar menu, only Prime Infrastructure license information is displayed.

See the *Cisco Wireless Control System Licensing and Ordering Guide* at this URL: http://www.cisco.com/en/US/prod/collateral/wireless/ps5755/ps6301/ps6305/product_data_sheet0900aecd804b4646.html#wp9000156.

It covers selecting the correct SKU, ordering the SKU, installing the software, registering the PAK certificate, and installing the license file on the server.

WLC Controller License Information

The Controller Licensing portion of the License Center page provides the following information for both WPLUS and Base licenses:

- Controller Count—The current number of licensed controllers.

  Note Only 5500 series controllers are included in the count. Prime Infrastructure provides only an inventory view and issues warnings if a license is expiring.

  Note Clicking the number in this column is the same as choosing **Summary > Controller** from the left sidebar menu, except that it is sorted by the feature you select. This page provides a summary of active controllers.

- AP Limit—The total number of licensed access points.
- Type—The four different types of licenses are as follows:

  Note For any controllers with a type other than Permanent, the least number of days left to expiration is shown.

  - Permanent—Licenses are node-locked and have no usage period associated with them. They are issued by the licensing portal of Cisco and must be installed using management interfaces on the device. Upon installation of these licenses, you have the necessary permissions across different versions.
  - Evaluation—Licenses are non-node-locked and are valid only for a limited period. They are used only when no permanent, extension, or grace period licenses exist. Before using an evaluation license, you must accept an End User License Agreement (EULA). Even though they are non-node-locked, their usage is recorded on the device. The number of days remaining on the evaluation license that has the fewest number of days until expiration is shown.

- Extension—Licenses are node-locked and metered. They are issued by licensing portal of Cisco and must be installed using management interfaces on the device. Before using an extension license, you must accept a EULA during installation.
- Grace Period—Licenses are node-locked and metered. These licenses are issued by the licensing portal of Cisco as part of the permission ticket to rehost a license. They are installed on the device as part of the rehost operation, and you must accept a EULA as part of the rehost operation.

If you need to revoke a license from one controller and install it on another, it is called *rehosting*. You might want to rehost a license to change the purpose of a controller.

Note The licensing status is updated periodically. To initiate an immediate update, choose **Administration > Background Tasks** and run the Controller License Status task.

If your network contains various Cisco licensed devices, you might want to consider using the Cisco License Manager (CLM) to manage all of the licenses using a single application. CLM is a secure client/server application that manages Cisco software licenses network wide. You can download the CLM software and access user documentation at this URL: http://www.cisco.com/go/clm. You can either register a PAK certificate with CLM or with the licensing portal found at the following URL: https://tools.cisco.com/SWIFT/Licensing/PrivateRegistrationServlet.

WLC Controller License Summary

If you want to see more details about controller licensing, from the left sidebar menu, choose the **Summary > Controller**. The License Center page appears. All currently active licenses on the controller are summarized.

All licensed controllers and their information in the bulleted list below are displayed. If you want to change how the controller results are displayed, click **Edit View**. In the Edit View page, highlight License Status, and click **Hide** to remove the column from the display.

Above the Controller Summary list is a series of filters that allow you to filter the list by Controller Name, Feature, Type, or Greater Than Percent Used. For example, if you enter 50, the list shows any WLCs that have more than 50% of its licenses used.

Note You can also use the **Advanced Search** link to sort the list of controllers.

- Controller Name—Provides a link to the Files > Controller Files page.
- Controller IP—The IP address of the controller.
- Model—The controller model type.
- Feature—The type of license, either Base or WPLUS. The Base license supports the standard software set, and the WPLUS license supports the premium Wireless Plus (WPLUS) software set. The WPLUS software set provides the standard feature set as well as added functionality for OfficeExtend access points, CAPWAP data encryptions, and enterprise wireless mesh.
- AP Limit—The maximum capacity of access points allowed to join this controller.
- AP Count—The current number of access points using licenses.
- % Used—The percentage of licensed access points that are being used. If the percentage is greater than 75%, the bar appears red to indicate that the limit is being approached.
- Type—The three different types of licenses are as follows:

Note For any controllers with a type other than Permanent, the least number of days left to expiration is shown.

  - Permanent—Licenses are node-locked and have no usage period associated with them. They are issued by licensing portal of Cisco and must be installed using management interfaces on the device. Upon installation of these licenses, you have the necessary permissions across different versions.
  - Evaluation—Licenses are non-node-locked and are valid only for a limited time period. They are used only when no permanent, extension, or grace period licenses exist. Before using an evaluation license, you must accept an End User License Agreement (EULA). Even though they are non-node-locked, their usage is recorded on the device. The number of days remaining on the evaluation license which has the fewest number of days until expiration is shown.
  - Extension—Licenses are node-locked and metered. They are issued by licensing portal of Cisco and must be installed using management interfaces on the device. Before using an extension license, you must accept a EULA during installation.

Note If a license shows as expired, the controller does not stop functioning. Only upon a reboot, the controller with the expired license become inactive.

- Status—In Use, Not in Use, Inactive, or EULA Not Accepted.
  - Inactive—The license level is being used, but this license is not being used.
  - Not In Use—The license level is not being used and this license is not currently recognized.
  - Expired In Use—The license is being used, but is expired and will not be used upon next reboot.
  - Expired Not In Use—The license has expired and can no longer be used.
  - Count Consumed—The ap-count license is In Use.

Mobility Services Engine (MSE) License Information

There are three types of licenses:

- Permanent—Licenses are node-locked and have no usage period associated with them. They are issued by licensing portal of Cisco and must be installed using management interfaces on the device. Upon installation of these licenses, you have the necessary permissions across different versions.
- Evaluation—Licenses are non-node-locked and are valid only for a limited time period. They are used only when no permanent, extension, or grace period licenses exist. Before using an evaluation license, you must accept an End User License Agreement (EULA). Even though they are non-node-locked, their usage is recorded on the device. The number of days remaining on the evaluation license which has the fewest number of days until expiration is shown.
- Extension—Licenses are node-locked and metered. They are issued by licensing portal of Cisco and must be installed using management interfaces on the device. Before using an extension license, you must accept a EULA during installation.

The MSE Licenses portion of the License Center page provides information for each service. See (Table 2-1).

Note

- When a license is deleted, the mobility services engine automatically restarts to load the new license limits.
- If Partner tag engine is up, then the MSE license information consists of information on tag licenses as well.
- For more information on MSE licenses, see the *Cisco Connected Mobile Experiences Configuration Guide, Release 7.5*.

Mobility Services Engine (MSE) License Summary

If you want to see more details about MSE licensing, choose **Summary > MSE** from the left sidebar menu. The License Center page appears.

All licensed MSEs are listed in the following columns:

- MSE Name—Provides a link to the MSE license file list page.

Note The icon to the left of the MSE Name/UDI indicates whether the mobility services engine is low-end or high-end.
A high-end mobility services engine (3350) has a higher memory capacity and can track up to 18,000 clients and tags. A low-end mobility services engine (3310) can track up to 2000 clients and tags.

- Type—Specifies the type of MSE.

Note Under wIPS Monitor Mode APs or wIPS Local Mode APs, an active link takes you to a list of licensed access points. You cannot access a list of licensed clients or tags.

- Limit—Displays the total number of client elements licensed across MSEs.
- Count—Displays the number of client elements that are currently licensed across MSEs.
- Unlicensed Count—Displays the number of client elements that are not licensed.

Note wIPS service does not process the alarms generated from these unlicensed access points.

- % Used—Displays the percentage of clients used across all MSEs.
- License Type—The three different types of licenses are as follows:
  - Permanent—Licenses are node-locked and have no usage period associated with them. They are issued by licensing portal of Cisco and must be installed using management interfaces on the device. Upon installation of these licenses, you have the necessary permissions across different versions.
  - Evaluation—Licenses are non-node-locked and are valid only for a limited time period. They are used only when no permanent, extension, or grace period licenses exist. Before using an evaluation license, you must accept an End User License Agreement (EULA). Even though they are non-node-locked, their usage is recorded on the device. The number of days remaining on the evaluation license which has the fewest number of days until expiration is shown.
  - Extension—Licenses are node-locked and metered. They are issued by licensing portal of Cisco and must be installed using management interfaces on the device. Before using an extension license, you must accept a EULA during installation.
- Status
  - Active—License is installed and being used by a feature.
  - Inactive—License is installed but not being used by a feature.
  - Expired—License has expired.
  - Corrupted—License is corrupted.

- For more information on MSE licenses, see the *Cisco Connected Mobile Experiences Configuration Guide, Release 7.5*.

Managing Prime Infrastructure Licenses

If you choose Files > Prime Infrastructure Files from the left sidebar menu, you can manage Prime Infrastructure licenses. This page displays the following information:

- Product Activation Key (PAK)
- Feature
- Access point limit
- Type

This section contains the following topics:

- Adding a New Prime Infrastructure License File, page 2-19
- Deleting a Prime Infrastructure License File, page 2-19

Adding a New Prime Infrastructure License File

To add a new Prime Infrastructure license file, follow these steps:

Step 1 In the License Center > Files > Prime Infrastructure Files page, click **Add**.

Step 2 In the Add a License File dialog box, enter or browse to the applicable license file.

Step 3 Once displayed in the License File text box, click **Upload**.

Deleting a Prime Infrastructure License File

To delete a Prime Infrastructure license file, follow these steps:

Step 1 In the License Center > Files > Prime Infrastructure Files page, select the check box of Prime Infrastructure license file that you want to delete.

Step 2 Click **Delete**.

Step 3 Click **OK** to confirm the deletion.

Monitoring Controller Licenses

If you choose Files > Controller Files from the left sidebar menu, you can monitor the controller licenses.

Note Prime Infrastructure does not directly manage controller licenses, rather it simply monitors the licenses. To manage the licenses you can use command-line interface, Web UI, or Cisco License Manager (CLM).

This page displays the following parameters:

- Controller Name
- Controller IP—The IP address of the controller.
- Feature—License features include wplus-ap-count, wplus, base-ap-count, and base.

  For every physical license installed, two license files display in the controller: a feature level license and an ap-count license. For example if you install a “WPlus 500” license on the controller, “wplus” and “wplus-ap-count” features display. There are always two of these features active at any one time that combine to enable the feature level (WPlus or Base) and the AP count.

  Note You can have both a WPlus and Base license, but only one can be active at any given time.

- AP Limit—The maximum capacity of access points allowed to join this controller.
- EULA status—Displays the status of the End User License Agreement and is either Accepted or Not Accepted.
- Comments—User entered comments when the license is installed.
- Type—The four different types of licenses are as follows:
  - Permanent—Licenses are node locked and have no usage period associated with them. They are issued by Cisco licensing portal and must be installed using management interfaces on the device. Upon installation of these licenses, you have the necessary permissions across different versions.
  - Evaluation—Licenses are non-node locked and are valid only for a limited time period. They are used only when no permanent, extension, or grace period licenses exist. Before using an evaluation license, you must accept an End User License Agreement (EULA). Even though they are non-node locked, their usage is recorded on the device. The number of days left displays for the evaluation license with the fewest number of remaining active license days.
  - Extension—Licenses are node locked and metered. They are issued by Cisco licensing portal and must be installed using management interfaces on the device. Before using an extension license, you must accept a EULA during installation.
  - Grace Period—Licenses are node locked and metered. These licenses are issued by Cisco licensing portal as part of the permission ticket to rehost a license. They are installed on the device as part of the rehost operation, and you must accept a EULA as part of the rehost operation.

  Note Types other than Permanent display the number of days left until the license expires. Licenses not currently in use do not have their counts reduced until they become “In Use”.

- Status
  - In Use—The license level and the license are in use.
  - Inactive—The license level is being used, but this license is not being used.
  - Not In Use—The license level is not being used and this license is not currently recognized.
  - Expired In Use—The license is being used, but is expired and will not be used upon next reboot.
  - Expired Not In Use—The license has expired and can no longer be used.
  - Count Consumed—The ap-count license is In Use.

Note If you need to filter the list of license files, you can enter a controller name, feature, or type and click **Go**.

Managing Mobility Services Engine (MSE) Licenses

If you choose Files > MSE Files from the left sidebar menu, you can manage the mobility services engine licenses.

This section contains the following topics:

- Deleting a Mobility Services Engine License File, page 2-21

Deleting a Mobility Services Engine License File

To delete a mobility services engine license file, follow these steps:

Step 1 In the License Center > Files > MSE Files page, select the check box of the mobility services engine license file that you want to delete.

Step 2 Click **Delete**.

Step 3 Click **OK** to confirm the deletion.

Adding a Mobility Services Engine to the Prime Infrastructure

You can add MSE using the Add Mobility Services Engine dialog box in the Mobility Service page. In this dialog box, you can add licensing files, tracking parameters, and assign maps to MSE. If you launch the wizard with an existing MSE for configuration, then the Add MSE option appears as Edit MSE Details. This section contains the following topics:

- Enabling Services on the Mobility Services Engine, page 2-22
- Configuring MSE Tracking and History Parameters, page 2-23
- Assigning Maps to the MSE, page 2-24

Note The Prime Infrastructure Release 1.0 recognizes and supports MSE 3355 appropriately.

To add a mobility services engine to the Prime Infrastructure, log into the Prime Infrastructure and follow these steps:

Step 1 Verify that you can ping the mobility services engine.

Step 2 Choose **Services > Mobility Services** to display the Mobility Services page.

Step 3 From the Select a command drop-down list, choose **Add Mobility Services Engine**. Click **Go**.

Step 4 In the Device Name text box, enter a name for the mobility services engine.

Step 5 In the IP Address text box, enter the IP address of the mobility services engine.

Step 6 (Optional) In the Contact Name text box, enter the name of the mobility services engine administrator.

Step 7 In the User Name and Password text boxes, enter the username and password for the mobility services engine.

This refers to the Prime Infrastructure communication username and password created during the setup process.

If you have not specified the username and password during the setup process, use the defaults.

The default username and password are both *admin*.

Note If you changed the username and password during the automatic installation script, enter those values here. If you did not change the default passwords, we recommend that you rerun the automatic installation script and change the username and password.

Step 8 Select the **HTTP** check box to allow communication between the mobility services engine and third-party applications. By default, the Prime Infrastructure uses HTTPs to communicate with MSE.

Step 9 Select the **Delete synchronized service assignments** check box if you want to permanently remove all service assignments from the mobility services engine.

This option is applicable for network designs, wired switches, controllers and event definitions. The existing location history data is retained, however, you must use manual service assignments to perform any future location calculations.

Step 10 Click **Next**. The Prime Infrastructure automatically synchronizes the selected elements with the MSE.

After the synchronization, the MSE License Summary page appears. You can use the MSE License Summary page to install a license, add a license, remove a license, install an activation license, and install service license.The Select Mobility Service page appears.

Note After adding a new mobility services engine, you can synchronize network designs (campus, building, and outdoor maps), controllers, switches (Catalyst Series 3000 only), and event groups on the local mobility services engine using the Prime Infrastructure. You can perform this synchronization immediately after adding a new mobility services engine or at a later time. To synchronize the local and the Prime Infrastructure databases, see the Information About Synchronizing the Prime Infrastructure and Mobility Services Engines, page 2-24.

Enabling Services on the Mobility Services Engine

To enable services on the mobility services engine, follow these steps:

Step 1 After adding the license file, the Select Mobility Service page appears.

Step 2 To enable a service on the mobility services engine, select the check box next to the service. The different type of services are as follows:

- Context Aware Service—If you select the Context Aware Service check box, then you must select a location engine to perform location calculation. You can choose **CAS to track clients**, **rogues**, **interferers**, and **tags**. You can choose either of the following engines to track tags:
  - Cisco Context-Aware Engine for Clients and Tags
  - Partner Tag Engine

Note By default, the Context Aware Service check box and Cisco Context-Aware Engine for Clients and Tags radio button are enabled.

- Wireless Intrusion Prevention System—If you select the Wireless Intrusion Prevention System check box, it detects wireless and performance threats.
- MSAP Service—If you select the MSAP Service check box, it provides service advertisements that describe the available services for the mobile devices.

Note With MSE 6.0 and later, you can enable multiple services (CAS and wIPS) simultaneously. Before Version 6.0, mobility services engines only supported one active service at a time.

Step 3 Click **Next** to configure the tracking and history parameters.

Configuring MSE Tracking and History Parameters

Step 1 After you enable services on the mobility services engine, the Select Tracking & History Parameters page appears.

Note If you skip configuring the tracking parameters, the default values are selected.

Step 2 You can select the clients that you want to keep track of by selecting the corresponding Tracking check box(es). The various tracking parameters are as follows:

- Wired Clients
- Wireless Clients
- Rogue Access Points
  - Exclude Adhoc Rogue APs
- Rogue Clients
- Interferers
- Active RFID Tags

Note You must select Wireless Clients for CMX analytics.

Step 3 You can enable the history tracking of devices by selecting the corresponding devices check box(es). The different history parameters are as follows:

- Wired Stations
- Client Stations
- Rogue Access Points
- Rogue Clients
- Interferers

- Asset Tags

Step 4 Click Next to Assign Maps to the MSE.

Assigning Maps to the MSE

Note The Assigning Maps page is available only if you select CAS as one of the services to be enabled on the MSE.

Step 1 Once you configure MSE tracking and history parameters, the Assigning Maps page appears.

The Assign Maps page shows the following information:

- Map Name
- Type (building, floor, campus)
- Status

Step 2 You can see the required map type by selecting All, Campus, Building, Floor Area, or Outdoor Area from the Filter option available on the page.

Step 3 To synchronize a map, select the **Name** check box and click **Synchronize**.

Upon synchronization of the network designs, the appropriate controllers that have APs assigned on a particular network design are synchronized with the MSE automatically. Click **Done** to save the MSE settings.

Information About Synchronizing the Prime Infrastructure and Mobility Services Engines

This section describes how to synchronize the Prime Infrastructure and mobility services engines manually and automatically.

Note The **Services > Synchronize Services** page is available only in the virtual domain in Release 7.3.101.0.

After adding a mobility services engine to the Prime Infrastructure, you can synchronize network designs (campus, building, floor, and outdoor maps), controllers (name and IP address), specific Catalyst 3000 series and 4000 series switches, and event groups with the mobility services engine.

- Network Design—A logical mapping of the physical placement of access points throughout facilities. A hierarchy of a single campus, the buildings that comprise that campus, and the floors of each building constitute a single network design.
- Controller—A selected controller that is associated and regularly exchanges location information with a mobility services engine. Regular synchronization ensures location accuracy.
- Wired Switches—Wired Catalyst switches that provide an interface to wired clients on the network. Regular synchronization ensures that location tracking of wired clients in the network is accurate.

  - The mobility services engine can be synchronized with Catalyst stackable switches (3750, 3750-E, 3560, 2960, IE-3000 switches), switch blades (3110, 3120, 3130, 3040, 3030, 3020), and switch ports.
  - The mobility services engine can also be synchronized with the following Catalyst 4000 series switches: WS-C4948, WS-C4948-10GE, ME-4924-10GE, WS-4928-10GE, WS-C4900M, WS-X4515, WS-X4516, WS-X4013+, WS-X4013+TS, WS-X4516-10GE, WS-X4013+10GE, WS-X45-SUP6-E, and WS-X45-SUP6-LE.

- Event Groups—A group of predefined events that define triggers that generate an event. Regular synchronization ensures that the latest defined events are tracked. Event groups can also be created by third-party applications. For more information on third-party application created event groups, see the "Configuring Automatic Database Synchronization and Out-of-Sync Alerts" section on page 2-28.
- Third Party Elements—When you synchronize elements with MSE, there might be event groups on the MSE that have been created by third-party applications. You can either delete the unused elements or mark them as third-party elements.
- Service Advertisements—MSAP provides service advertisements on mobile devices. This shows the service advertisement that is synchronized with the MSE.

Prerequisites for Synchronizing the Mobility Services Engine

- Be sure to verify software compatibility between the controller, Prime Infrastructure, and the mobility services engine before synchronizing. See the latest mobility services engine release notes at the following URL:

  http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html
- Communication between the mobility services engine, Prime Infrastructure, and the controller is in Coordinated Universal Time (UTC). Configuring NTP on each system provides devices with UTC time. The mobility services engine and its associated controllers must be mapped to the same NTP server and the same Prime Infrastructure server. An NTP server is required to automatically synchronize time between the controller, Prime Infrastructure, and the mobility services engine. However, the timezone for MSE should still be set to UTC. This is because wIPS alarms require that the MSE time be set to UTC.

Working with Third-Party Elements

When you synchronize elements with MSE, there might be event groups on the MSE that have been created by third-party applications. You can either delete the unused elements or mark them as third-party elements.

This section contains the following topic:

Deleting Elements or Marking Them as Third-Party Elements, page 2-25

Deleting Elements or Marking Them as Third-Party Elements

To delete elements or mark them as third-party elements, follow these steps:

Step 1 Choose **Services** > **Synchronize Services**.

The Network Designs page appears.

Step 2 In the Network Designs page, choose **Third Party Elements** from the left sidebar menu.

The Third Party Elements page appears.

Step 3 Select one or more elements.

Step 4 Click one of the following buttons:

- **Delete Event Groups**—Deletes the selected event groups.
- **Mark as 3rd Party Event Group(s)**—Marks the selected event groups as third-party event groups.

Synchronizing Controllers with a Mobility Services Engine

This section describes how to synchronize a controller, assign an MSE to any wireless controller and also to unassign a network design, controller, wired switch, or event group from a mobility services engine. This section contains the following topics:

Synchronizing a Controller, Catalyst Switch, or Event Group

To synchronize network designs, a controller, a Catalyst switch, or event group with the mobility services engine, follow these steps:

Step 1 Choose **Services > Synchronize Services**.

The left sidebar menu contains the following options: **Network Designs**, **Controllers**, **Event Groups**, **Wired Switches**, **Third Party Elements**, and **Service Advertisements**.

Step 2 From the left sidebar menu, choose the appropriate menu options.

Step 3 To assign a network design to a mobility services engine, in the Synchronize Services page, choose **Network Designs** from the left sidebar menu.

The Network Designs page appears.

Step 4 Select all the maps to be synchronized with the mobility services engine by selecting the corresponding **Name** check box.

Note Through Release 6.0, you can assign only up to a campus level to a mobility services engine. Starting with Release 7.0 this option is granular to a floor level. For example, you can choose to assign floor1 to MSE 1, floor2 to MSE 2, and floor3 to MSE 3.

Step 5 Click **Change MSE Assignment**.

Step 6 Select the mobility services engine to which the maps are to be synchronized.

Step 7 Click either of the following in the MSE Assignment dialog box:

- **Save**—Saves the mobility services engine assignment. The following message appears in the Messages column of the Network Designs page with a yellow arrow icon:

  "To be assigned - Please synchronize."

- **Cancel**—Discards the changes to the mobility services engine assignment and returns to the Network Designs page.

You can also click **Reset** to undo the mobility services engine assignments.

Note A network design may include a floor in a campus or a large campus with several buildings, each monitored by a different mobility services engine. Because of this, you may need to assign a single network design to multiple mobility services engines.

Note Network design assignments also automatically picks up the corresponding controller for synchronization.

Step 8 Click **Synchronize** to update the mobility services engine(s) database(s).

When items are synchronized, a green two-arrow icon appears in the Sync. Status column for each synchronized entry.

You can use the same procedure to assign wired switches or event groups to a mobility services engine. To assign a controller to a mobility services engine, see "Synchronizing Controllers with a Mobility Services Engine" section on page 2-26 for more information.

Assigning an MSE to the Controller

To assign a mobility services engine with any wireless controller on a per-service basis (CAS or wIPS), follow these steps:

Step 1 Choose **Services > Synchronize Services**.

Step 2 In the Network Designs page, choose **Controller** from the left sidebar menu.

Step 3 Select the controllers to be assigned to the mobility services engine by selecting the corresponding **Name** check box.

Step 4 Click **Change MSE Assignment**.

Step 5 Choose the mobility services engine to which the controllers must be synchronized.

Step 6 Click either of the following in the Choose MSEs dialog box:

- **Save**—Saves the mobility services engine assignment. The following message appears in the Messages column of the Controllers page with a yellow arrow icon:

  "To be assigned - Please synchronize."

- **Cancel**—Discards the changes to mobility services engine assignment and returns to the Controllers page.

You can also click **Reset** to undo the mobility services engine assignments.

Step 7 Click **Synchronize** to complete the synchronization process.

Step 8 Verify that the mobility services engine is communicating with each of the controllers for only the chosen service. This can be done by clicking the NMSP status link in the status page.

Note After Synchronizing a controller, verify that the timezone is set on the associated controller.

Note Controller names must be unique for synchronizing with a mobility services engine. If you have two controllers with the same name, only one is synchronized.

You can use the same procedure to assign Catalyst switches or event groups to a mobility services engine.

Note A switch can only be synchronized with one mobility services engine. However, a mobility services engine can have many switches attached to it.

Unassigning a Network Design, Controller, Wired Switch, or Event Group from the MSE

To unassign a network design, controller, wired switch, or event group from a mobility services engine, follow these steps:

Step 1 Choose **Services > Synchronize Services**.

Step 2 From the left sidebar menu, choose the appropriate menu options.

Step 3 Select one or more elements by selecting the **Name** check box, and click **Change MSE Assignment**. The Choose MSEs dialog box appears.

Step 4 Unselect the mobility services engine if you do not want the elements to be associated with that mobility services engine by selecting either the **CAS** or **wIPS** check box.

Step 5 Click **Save** to save the assignment changes.

Step 6 Click **Synchronize**.

The Sync Status column appears blank.

Configuring Automatic Database Synchronization and Out-of-Sync Alerts

Manual synchronization of the Prime Infrastructure and mobility services engine databases is immediate. However, future deployment changes (such as changes to maps and access point positions) can yield incorrect location calculations and asset tracking until resynchronization.

To prevent out-of-sync conditions, use the Prime Infrastructure to carry out synchronization. This policy ensures that synchronization between the Prime Infrastructure and mobility services engine databases is triggered periodically and any related alarms are cleared.

Any change to one or more of any synchronized component is automatically synchronized with the mobility services engine. For example, if a floor with access points is synchronized with a particular mobility services engine and then one access point is moved to a new location on the same floor or another floor that is also synchronized with the mobility services engine, then the changed location of the access point is automatically communicated.

To further ensure that the Prime Infrastructure and MSE are in sync, smart synchronization happens in the background.

This section contains the following topics:

Configuring Automatic Database Synchronization

To configure smart synchronization, follow these steps:

Step 1 Choose **Administration >Background Tasks**.

Step 2 Select the **Mobility Service Synchronization** check box.

The Mobility Services Synchronization page appears.

Step 3 To set the mobility services engine to send out-of-sync alerts, select the Out of Sync Alerts **Enabled** check box.

Step 4 To enable smart synchronization, select the Smart Synchronization **Enabled** check box.

Note Smart synchronization does not apply to elements (network designs, controllers, or event groups) that have not yet been assigned to a mobility services engine. However, out-of-sync alarms are still generated for these unassigned elements. For smart synchronization to apply to these elements, you must manually assign them to a mobility services engine.

Note When a mobility services engine is added to an Prime Infrastructure, the data in the Prime Infrastructure is always treated as the primary copy that is synchronized with the mobility services engine. All synchronized network designs, controllers, event groups and wired switches that are present in the mobility services engine and not in the Prime Infrastructure are removed automatically from mobility services engine.

Step 5 Enter the time interval, in minutes, that the smart synchronization is to be performed.

By default, the smart-sync is enabled.

Step 6 Click **Submit**.

For Smart controller assignment and selection scenarios, see the "Smart Controller Assignment and Selection Scenarios" section on page 2-30.

Smart Controller Assignment and Selection Scenarios

Scenario 1

If a floor having at least one access point from a controller is chosen to be synchronized with the mobility services engine in the Network Designs menu of the Synchronize Services page, then the controller to which that access point is connected is automatically selected to be assigned to the mobility services engine for CAS service.

Scenario 2

When at least one access point from a controller is placed on a floor that is synchronized with the mobility services engine, the controller to which the access point is connected is automatically assigned to the same mobility services engine for the CAS service.

Scenario 3

An access point is added to a floor and assigned to a mobility services engine. If that access point is moved from controller A to controller B, then controller B is automatically synchronized to the mobility services engine.

Scenario 4

If all access points placed on a floor that is synchronized to the MSE are deleted, then that controller is automatically removed from the mobility services engine assignment or unsynchronized.

Out-of-Sync Alarms

Out-of-sync alarms are of the minor severity (yellow), and are raised in response to the following conditions:

- Elements are modified in the Prime Infrastructure (the auto-sync policy pushes these elements)
- Elements other than controllers exist in the mobility services engine database but not in the Prime Infrastructure
- Elements are not assigned to any mobility services engine (the auto-sync policy does not apply)

Out-of-sync alarms are cleared when the following occurs:

- The mobility services engine is deleted

Note When you delete a mobility services engine, the out-of-sync alarms for that system are also deleted. In addition, if you delete the last available mobility services engine, the alarm for the following event: "elements not assigned to any server" is deleted.

- Elements are synchronized manually or automatically
- User manually clears the alarms (although the alarms may reappear in the future when the scheduled task is next executed)

Viewing Mobility Services Engine Synchronization Status

You can use the Synchronize Services feature in the Prime Infrastructure to view the status of network design, controller, switch, and event group synchronization with a mobility services engine.

This section contains the following topics:

Viewing Mobility Services Engine Synchronization Status

To view the synchronization status, follow these steps:

Step 1 Choose **Services > Synchronize Services**.

Step 2 From the left sidebar menu, choose **Network Designs**, **Controllers**, **Event Groups**, **Wired Switches**, **Third Party Elements**, or **Service Advertisements**.

For each of the elements, the Sync. Status column shows the synchronization status. A green two-arrow icon indicates that its corresponding element is synchronized with the specified server such as a mobility services engine. A gray two-arrow icon with a red circle indicates that its corresponding item is not synchronized with a provided server.

The Message column shows the reason for failure if the elements are out of sync.

You can also view the synchronization status at **Monitor > Site Maps > System Campus >** *Building* **>** *Floor*.

where *Building* is the building within the campus and *Floor* is a specific floor in that campus building.

The MSE Assignment option on the left sidebar menu shows which mobility services engine the floor is currently assigned to. You can also change the mobility services engine assignment in this page.

Viewing Synchronization History

You can view the synchronization history for the last 30 days for a mobility services engine. This is especially useful when automatic synchronization is enabled as alarms are automatically cleared. Synchronization history provides a summary of those cleared alarms.

To view synchronization history choose **Services > Synchronization History**. The Synchronization History page appears. Click the column headings to sort the entries.

Table 2-2 describes the table column headings that appear in the Synchronization History page.

Deleting an MSE License File

To delete an MSE license file, follow these steps:

Step 1 Choose **Services > Mobility Service Engine**.

The Mobility Services page appears.

Step 2 Click **Device Name** to delete a license file for a particular service.

Step 3 From the Select a command drop-down list, choose **Edit Configuration**.

The Edit Mobility Services Engine dialog box appears.

Step 4 Click **Next** in the Edit Mobility Services Engine dialog box.

The MSE License Summary page appears.

Step 5 Choose the MSE license file that you want to delete in the MSE License Summary page.

Step 6 Click **Remove License**.

Step 7 Click **OK** to confirm the deletion or **Cancel** to close this page without deleting the license.

Step 8 Click **Next** to enable services on the mobility services engine.

Deleting a Mobility Services Engine from the Prime Infrastructure

To delete one or more mobility services engines from the Prime Infrastructure database, follow these steps:

Note The **Services > Mobility Services Engine** page is available only in the virtual domain in Release 7.3.

Step 1 Choose **Services > Mobility Services**.

The Mobility Services page appears.

Step 2 Select the mobility services engine to be deleted by selecting the corresponding **Device Name** check box(es).

Step 3 From the Select a command drop-down list, choose **Delete Service(s)**. Click **Go**.

Step 4 Click **OK** to confirm that you want to delete the selected mobility services engine from the Prime Infrastructure database.

Step 5 Click **Cancel** to stop deletion.

Viewing Clients and Users

To view clients and users in the Prime Infrastructure UI, follow these steps:

Step 1 Choose **Monitor > Clients and Users** to view both wired and wireless clients information. The Clients and Users page appears.

The Clients and Users table displays a few columns by default. If you want display the additional columns that are available, click  , and then click **Columns**. The available columns appear. Select the columns that you want to show in the Clients and Users table. When you click anywhere in a row, the row is selected and the client details are shown.

The following columns are available in the Clients and Users table:

- MAC Address—Client MAC address.
- IP Address—Client IP address.

  The IP address that appears in the IP Address column is determined by a predefined priority order. The first IP address available in the following order appears in the IP address field:

  - IPv4 address.
  - IPv6 unique global address. If there are multiple addresses of this type, most recent IPv6 address the client received are shown, because a user can have two global IPv6 addresses but one might be from an older router advertisement that is being aged out.
  - IPv6 unique local address. If there are multiple IPv6 unique local addresses, the most recent one is used.
  - IPv6 link-local address. The IPv6 clients always have at least one link-local address.

  The following are the different IPv6 address types:

  - Link-local Unicast—The link-local addresses are designed to be used for addressing on a single link for purposes such as auto-address configuration, neighbor discovery, or when no routers are present.
  - Site-local Unicast—The site-local addresses are designed to be used for addressing inside of a site without the need for a global prefix.
  - Global Unicast—The global unicast address uniquely identifies the client in the global network and is equivalent to a public IPv4 address. A client can have multiple global unicast addresses.

Note When there is more than one IP address of the same type, only the most recent IP address of that type appears, and the rest appear in the QuickView page when you hover your mouse cursor over the QuickView (+) icon.

- IP Address Type—The IP address type such as IPv4 and IPv6.
- PMIP Client—Specifies if the client is a PMIP client.
- PMIP State—State of the PMIP client. The available states are as follows:
  - Unknown—Indicates that the state of the client cannot be determined.
  - Activated—Indicates that the client is ready to establish a tunnel.
  - Tunneled—Indicates that a bidirectional tunnel is established.
- Global Unique—The aggregate global unicast address of an IPv6 address. This field is populated only if a client is assigned a global unique IPv6 address.
- Unique Local—The local unicast address of an IPv6 address. This field is populated only if a client is assigned a local unique IPv6 address.
- Link Local—The link-local unicast address of an IPv6 address. This field is populated only if a client is assigned a link-local IPv6 address.
- User Name—Username based on 802.1x authentication or Web authentication. Unknown is displayed for a client connected without a username.
- Type—Indicates the client type.
  -  Indicates a lightweight client
  -  indicates a wired client
  -  Indicates an autonomous client
- Vendor—Device vendor derived from OUI.
- AP Name—Wireless only
- Device Name—Network authentication device name, for example, WLC, switch.
- Location—Map location of connected device.
- ISE—Yes/No. This column represents whether the client is authenticated using the ISE, which is added to Prime Infrastructure.
- Endpoint Type—Endpoint type as reported by the ISE, available only when the ISE is added (for example, iPhone, iPad, Windows workstation).
- Posture—Latest client posture status
- SSID—Wireless only
- Profile Name—Wireless only
- VLAN——Indicates the access VLAN ID for this client.
- Status—Current client status
  - Idle—Normal operation; no rejections of client association requests.
  - Auth Pending—Completing a AAA transaction.
  - Authenticated—802.11 authentication complete.
  - Associated—802.11 association complete. This is also used by wired clients to represent that a client is currently connected to the network.

  - Power Save—Client is in power save mode.
  - Disassociated—802.11 disassociation complete. This is also used by wired clients to represent that a client is currently not on the network.
  - To Be Deleted—The client that is deleted after disassociation.
  - Excluded—Automatically disabled by the system due to perceived security threat.
- Interface—Controller interface (wireless) or switch interface (wired) that the client is connected to.
- Protocol
  - 802.11—wireless
  - 802.3—wired
- Speed—Ethernet port speed (wired only). Displays “N/A” for wireless.
- Association Time—Last association start time (for wireless client). For a wired client, this is the time when the client is connected to a switch port. This column is blank for a client that is associated but has problems being on the network.
- Session Length—Session length.
- First Seen—Indicates the date and time when the client was first detected.
- Authentication Type—WPA, WPA2, 802.1x, MAC Auth Bypass, or Web Auth.
- Authorization Profile Names—Authorization profiles applied to this client by the ISE. This contains data only when the ISE is added and the client is authenticated by the ISE.
- Traffic (MB)—Traffic (transmitted/received) in this session in MB.
- Average Session Throughput (kbps)—Average session throughput in kbps.
- Automated Test Run—Indicates whether the client is in auto test mode. This is applicable for wireless clients only.
- AP MAC Address—Wireless only.
- AP IP Address—Wireless only.
- Anchor Controller—Lightweight wireless only.
- On Network—Shows Yes for the clients that are associated and have successfully finished authentication, if required.
- CCX—Lightweight wireless only.
- Client Host Name—Wired and wireless. Result of DNS reverse lookup.
- Device IP Address—IP address of the connected device (WLC, switch. or autonomous AP).
- Port—Switch port on WLC.
- E2E—Lightweight wireless only.
- Encryption Cipher—Wireless only.
- MSE—MSE server managing this client.
- RSSI—Wireless only.
- SNR—Wireless only.
- Router Advertisements Dropped—The router advertisements that are dropped for each client for a particular session.
- Session ID—Audit-session-ID used in the ISE and on the switch.

- FlexConnect Local Authentication—Indicates if the FlexConnect Local Authentication is enabled for this client.
- WGB Status—Indicates the status of the work group bridge mode.
- Mobility Status—Indicates the mobility status of the wireless client.
- SNMP NAC State—Indicates the state of the NAC appliance in out-of-band mode.

Step 2 Select a client or user. The following information appears:

- Client Attributes
- Client Statistics
- Client Association History
- Client Event Information
- Client Location Information
- Client CCXv5 Information

Note Client Statistics shows statistical information after the client details are shown.

Adding Floor Areas

This section describes how to add floor plans to either a campus building or a standalone building in the Prime Infrastructure database.

This section contains the following topics:

Adding Floor Areas to a Campus Building

After you add a building to a campus map, you can add individual floor plan and basement maps to the building.

Note Use the zoom controls at the top of the campus image to enlarge or decrease the size of the map view and to hide or show the map grid (which shows the map size in feet or meters).

To add a floor area to a campus building, follow these steps:

Step 1 Save your floor plan maps in .PNG, .JPG, ,JPEG, or .GIF format.

Note For CMX analytics, it is recommended that the size of image file is maximum of 500k. Loading large images into the 3D version of CMX analytics causes certain browsers to show black images. The mse.properties file can also be configured to automatically compress the image.

Note If there are problems converting the auto-cad file, an error message is displayed. The Prime Infrastructure uses a native image conversion library to convert auto-cad files into raster formats like .png. If the native library cannot be loaded, the Prime Infrastructure shows an "unable to convert the auto-cad file" message. If you receive this error, make sure all the required dependencies are met for the native library. To find any dependency problems, use ldd on Linux platforms. The following DLLs must be present under the /webnms/rfdlls Prime Infrastructure installation directory: LIBGFL254.DLL, MFC71.DLL, MSVCR71.DLL, and MSVCP71.DLL. If dependency problems occurs, you have to install the required libraries and restart Prime Infrastructure.

Note The floor map image is enhanced for zooming and panning. The floor image is not visible completely until this operation is complete. You can zoom in and out to view the complete map image. For example, if you have a high resolution image (near 181 megapixels) whose size is approximately 60 megabytes, it may take two minutes to appear on the map.

Step 2 Choose **Monitor > Site Maps**.

Step 3 From the Maps Tree View or the Monitor > Site Maps list, choose the applicable campus building to open the Building View page.

Step 4 Hover your mouse cursor over the name within an existing building rectangle to highlight it.

Note You can also access the building from the Campus View page. In the Campus View page, click the building name to open the Building View page.

Step 5 From the Select a command drop-down list, choose **New Floor Area**.

Step 6 Click **Go**. The New Floor Area page appears.

Step 7 In the New Floor Area page, follow these steps to add floors to a building in which to organize related floor plan maps:

a. Enter the floor area and contact names.

b. Choose the floor or basement number from the Floor drop-down list.

c. Choose the floor or basement type (RF Model).

d. Enter the floor-to-floor height in feet.

Note To change the unit of measurement (feet or meters), choose **Monitor > Site Maps**, and choose **Properties** from the Select a command drop-down list.

e. Select the **Image or CAD File** check box.

f. Browse to and choose the desired floor or basement image or CAD filename, and click **Open**.

Note If you are importing a CAD file, use the Convert CAD File drop-down list to determine the image file for conversion.

Tip It is not recommended to use a .JPEG (.JPG) format for an auto-cad conversion. Unless a JPEG is specifically required, use .PNG or .GIF format for higher quality images.

g. Click **Next**. At this point, if a CAD file was specified, a default image preview is generated and loaded.

Note The Prime Infrastructure uses a native image conversion library to convert auto-cad files into raster formats like .PNG. When there are issues loading the native library, Prime Infrastructure shows the following error: "Unable to convert the auto-cad file. Reason: Error while loading the auto-cad image conversion library." For more information see Prime Infrastructure online help or Prime Infrastructure documentation.

The names of the CAD file layers are listed with check boxes to the right side of the image indicating which are enabled.

Note When you choose the floor or basement image filename, the Prime Infrastructure shows the image in the building-sized grid.

Note The maps can be of any size because the Prime Infrastructure automatically resizes the maps to fit the workspace.

Note The map must be saved in .PNG, .JPG, .JPEG, or .GIF format.

h. If you have CAD file layers, you can select or deselect as many as you want and click **Preview** to view an updated image. Click **Next** when you are ready to proceed with the selected layers.

Enter the remaining parameters for the floor area.

i. Either leave the **Maintain Aspect Ratio** check box selected to preserve the original image aspect ratio or unselect the check box to change the image aspect ratio.

j. Enter an approximate floor or basement horizontal and vertical span (width and depth on the map) in feet.

Note The horizontal and vertical spans should be smaller than or the same size as the building horizontal and vertical spans in the Prime Infrastructure database.

k. If applicable, enter the horizontal position (distance from the corner of the outdoor area rectangle to the left edge of the campus map) and vertical position (distance from the corner of the outdoor area rectangle to the top edge of the campus map) in feet or meters.

Tip Use **Ctrl-click** to resize the image within the building-sized grid.

l. If desired, select the **Launch Map Editor after floor creation** check box to rescale the floor and draw walls.

m. Click **OK** to save this floor plan to the database. The floor is added to the Maps Tree View and the Design > Site Maps list.

Note Use different floor names in each building. If you are adding more than one building to the campus map, do not use a floor name that exists in another building. This overlap causes incorrect mapping information between a floor and a building.

Step 8 Click any of the floor or basement images to view the floor plan or basement map.

Note You can zoom in or out to view the map at different sizes and you can add access points.

Adding Floor Plans to a Standalone Building

After you have added a standalone building to the Prime Infrastructure database, you can add individual floor plan maps to the building.

To add floor plans to a standalone building, follow these steps:

Step 1 Save your floor plan maps in .PNG, .JPG, or .GIF format.

Note The maps can be of any size because the Prime Infrastructure automatically resizes the maps to fit the workspace.

Step 2 Browse to and import the floor plan maps from anywhere in your file system. You can import CAD files in DXF or DWG formats or any of the formats you created in Step 1.

Note If there are problems converting the auto-cad file, an error message is displayed. the Prime Infrastructure uses a native image conversion library to convert auto-cad files into raster formats like .PNG. If the native library cannot be loaded, the Prime Infrastructure shows an “unable to convert the auto-cad file” message. If you receive this error, make sure all the required dependencies are met for the native library. To find any dependency problems, use ldd on Linux platforms. The following DLLs must be present under the /webnms/rfdlls the Prime Infrastructure installation directory: LIBGFL254.DLL, MFC71.DLL, MSVCR71.DLL, and MSVCP71.DLL. If dependency problems occurs, you must install the required libraries and restart the Prime Infrastructure.

Step 3 Choose **Monitor > Site Maps**.

Step 4 From the Maps Tree View or the Design > Site Maps left sidebar menu, choose the desired building to display the Building View page.

Step 5 From the Select a command drop-down list, choose **New Floor Area**.

Step 6 Click **Go**.

Step 7 In the New Floor Area page, add the following information:

- Enter the floor area and contact names.

- Choose the floor or basement number from the Floor drop-down list.
- Choose the floor or basement type (RF Model).
- Enter the floor-to-floor height in feet.
- Select the **Image or CAD File** check box.
- Browse to and choose the desired floor or basement Image or CAD file, and click **Open**.

Note If you are importing a CAD file, use the Convert CAD File drop-down list to determine the image file for conversion.

Tip A .JPEG (.JPG) format is not recommended for an auto-cad conversion. Unless a .JPEG is specifically required, use a .PNG or .GIF format for higher quality images.

Step 8 Click **Next**. At this point, if a CAD file was specified, a default image preview is generated and loaded.

Note The Prime Infrastructure uses a native image conversion library to convert auto-cad files into raster formats like .PNG. When there are issues loading the native library, the Prime Infrastructure shows the following error: “Unable to convert the auto-cad file. Reason: Error while loading the auto-cad image conversion library. For more information, see the Prime Infrastructure online help or the Prime Infrastructure documentation”.

The names of the CAD file layers are listed with check boxes to the right side of the image indicating which are enabled.

Note When you choose the floor or basement image filename, the Prime Infrastructure shows the image in the building-sized grid.

Note The maps can be any size because the Prime Infrastructure automatically resizes the maps to fit the workspace.

Note The map must be saved in .PNG, .JPG, .JPEG, or .GIF format.

If you have CAD file layers, you can select or deselect as many as you want and click **Preview** to view an updated image. Click **Next** when you are ready to proceed with the selected layers.

Step 9 Enter the remaining parameters for the floor area.

- Either leave the **Maintain Aspect Ratio** check box selected to preserve the original image aspect ratio or unselect the check box to change the image aspect ratio.
- Enter an approximate floor or basement horizontal and vertical span (width and depth on the map) in feet.

Note The horizontal and vertical spans should be smaller than or the same size as the building horizontal and vertical spans in the Prime Infrastructure Prime Infrastructure database.

- If applicable, enter the horizontal position (distance from the corner of the outdoor area rectangle to the left edge of the campus map) and vertical position (distance from the corner of the outdoor area rectangle to the top edge of the campus map) in feet or meters.

Tip Use **Ctrl-click** to resize the image within the building-sized grid.

- Adjust the floor characteristics with the Prime Infrastructure map editor by selecting the check box next to Launch Map Editor.

Step 10 Click **OK** to save this floor plan to the database. The floor is added to the Maps Tree View and the Design > Site Maps list.

Step 11 Click any of the floor or basement images to view the floor plan or basement map.

You can zoom in or out to view the map at different sizes and you can add access points.

Defining Coverage Area

To draw a coverage area using the Prime Infrastructure UI, follow these steps:

Note You must add floor plan before drawing a coverage area.

Step 1 Add the floor plan if it is not already represented in the Prime Infrastructure.

Step 2 Choose **Monitor > Site Maps**.

Step 3 Click the Map Name that corresponds to the outdoor area, campus, building, or floor you want to edit.

Step 4 From the Select a command drop-down list, choose **Map Editor**, and click **Go**.

Step 5 It the Map Editor page, click the **Draw Coverage Area** icon on the toolbar.

A pop-up appears.

Step 6 Enter the name of the area that you are defining. Click **OK**.

A drawing tool appears.

Step 7 Move the drawing tool to the area you want to outline.

- Click the left mouse button to begin and end drawing a line.
- When you have completely outlined the area, double-click the left mouse button and the area is highlighted in the page.

The outlined area must be a closed object to appear highlighted on the map.

Step 8 Click the disk icon on the toolbar to save the newly drawn area.

Monitoring Geo-Location

The MSE provides physical location of wired clients, wired endpoints, switches, controllers, and access points present in a wireless network deployment. Currently, MSE provides location information in geo-location format to the external entities through northbound and southbound entities.

To improve the accuracy of the geo-location information provided by MSE, this feature aims to transform the geometric location co-ordinates of a device to geo-location coordinates (latitude and longitude) and provides it to the external entities through northbound and southbound interfaces.

Note At least three GPS markers are required for geo-location calculation. The maximum number of GPS markers that you can add is 20.

Note For CMX Analytics, the 2D OpenStreetMaps requires all points to be geo-located as latitude/longitude in order for the results to be displayed in the correct location.

This section contains the following topics:

Adding a GPS Marker to a Floor Map

To add a GPS marker to a floor map, follow these steps:

Step 1 Choose **Monitor > Site Maps** to display the Maps page.

Step 2 Choose **Campus Name > Building Name > Floor Name**.

Step 3 Choose the **Add/Edit GPS Markers Information** menu option on the top left menu to open the Add/Edit GPS page.

A GPS Marker icon appears on the top left corner of the map (X=0 Y=0).

Step 4 You can drag the GPS Marker icon and place it in the desired location on the map or enter the X and Y position values in the GPS Marker Details table on the left sidebar menu to move the marker to the desired position.

Note If the markers added are too close, then the accuracy of geo-location information is less.

Step 5 Enter the Latitude and Longitude degrees for the selected GPS Marker icon in the left sidebar menu.

Step 6 Click **Save.**

The GPS Marker information is saved to the database.

Step 7 Click **Apply to other Floors of Building** to copy GPS markers on one floor of a building to all the remaining floors of that building.

Note The GPS marker information is required by the CMX analytics to show results for the building in the 2D Open Street Maps view. A warning message is displayed if these GPS markers are not set.

Editing a GPS Marker

To edit a GPS marker present on the floor, follow these steps:

Step 1 Choose **Monitor > Site Maps** to display the Maps page.

Step 2 Choose the **Campus Name > Building Name > Floor Name**.

Step 3 Choose the **Add/Edit GPS Markers Information** menu option on the top left menu to open the Add/Edit GPS page.

Step 4 Select an existing GPS marker present on the floor.

Step 5 From the left sidebar menu, you can change the Latitude, Longitude, X Position, and Y Position which is associated with the GPS marker.

Step 6 Click **Save**.

The modified GPS marker information is now saved to the database.

Deleting a GPS Marker Present on a Floor

To delete a GPS marker present on a floor, follow these steps:

Step 1 Choose **Monitor > Site Maps** to display the Maps page.

Step 2 Choose **Campus Name > Building Name > Floor Name**.

Step 3 Choose the **Add/Edit GPS Markers Information** menu option to open the Add/Edit GPS page.

Step 4 Select an existing GPS Marker which is present on the floor from the left sidebar menu.

Note You can delete multiple GPS markers present on a floor by selecting the **Multiple GPS Markers** check box.

Step 5 Click **Delete GPS Marker**.

Step 6 The selected GPS marker is deleted from the database.

Inclusion and Exclusion Areas on a Floor

- Inclusion and exclusion areas can be any polygon shape and must have at least three points. Points can sometime be located outside the building. If this is where the devices are, then a coverage area should be created. At other times, the points are actually inside and should be moved to the nearest inside location (same applies for unlikely areas inside). Defining inclusion and exclusion areas does this and therefore the analytic results are more consistent.
- You can only define one inclusion region on a floor. By default, an inclusion region is defined for each floor when it is added to Prime Infrastructure. The inclusion region is indicated by a solid aqua line, and generally outlines the region.
- You can define multiple exclusion regions on a floor.
- Newly defined inclusion and exclusion regions appear on heatmaps only after the mobility services engine recalculates location.

This section contains the following topics:

Defining an Inclusion Region on a Floor

To define an inclusion area, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 Click the name of the appropriate floor area.

Step 3 From the Select a command drop-down list, choose **Map Editor**.

Step 4 Click **Go**.

Step 5 At the map, click the aqua box on the toolbar.

Note A message box appears reminding you that only one inclusion area can be defined at a time. Defining a new inclusion region automatically removes the previously defined inclusion region. By default, an inclusion region is defined for each floor when it is added to Prime Infrastructure. The inclusion region is indicated by a solid aqua line and generally outlines the region.

Step 6 Click **OK** in the message box that appears. A drawing icon appears to outline the inclusion area.

Step 7 To begin defining the inclusion area, move the drawing icon to a starting point on the map and click once.

Step 8 Move the cursor along the boundary of the area you want to include and click to end a border line. Click again to define the next boundary line.

Step 9 Repeat Step 8 until the area is outlined and then double-click the drawing icon. A solid aqua line defines the inclusion area.

Step 10 Choose **Save** from the Command menu or click the **disk** icon on the toolbar to save the inclusion region.

Note If you made an error in defining the inclusion area, click the area. The selected area is outlined by a dashed aqua line. Next, click the **X** icon on the toolbar. The area is removed from the floor map.

Step 11 Select the **Location Regions** check box if it is not already selected. If you want it to apply to all floor maps, click **Save settings**. Close the Layers configuration page.

Step 12 To resynchronize Prime Infrastructure and MSE databases, choose **Services > Synchronize Services**.

Note If the two DBs are already synchronized then a resynchronization happens automatically every time there is a change. There is no need for an explicit resynch.

Step 13 In the Synchronize page, choose **Network Designs** from the Synchronize drop-down list and then click **Synchronize**.

You can confirm that the synchronization is successful by viewing two green arrows in the Sync. Status column.

Note Newly defined inclusion and exclusion regions appear on heatmaps only after the mobility services engine recalculates location.

Defining an Exclusion Region on a Floor

To further refine location calculations on a floor, you can define areas that are excluded (exclusion areas) in the calculations. For example, you might want to exclude areas such as an atrium or stairwell within a building. As a rule, exclusion areas are generally defined within the borders of an inclusion area.

To define an exclusion area, follow these steps:

Step 1 Choose **Monitor > Site Maps**.

Step 2 Click the name of the appropriate floor area.

Step 3 From the Select a command drop-down list, choose **Map Editor**.

Step 4 Click **Go**.

Step 5 At the map, click the purple box on the toolbar.

Step 6 Click **OK** in the message box that appears. A drawing icon appears to outline the exclusion area.

Step 7 To begin defining the exclusion area, move the drawing icon to the starting point on the map, and click once.

Step 8 Move the drawing icon along the boundary of the area you want to exclude. Click once to start a boundary line, and click again to end the boundary line.

Step 9 Repeat Step 8until the area is outlined and then double-click the drawing icon. The defined exclusion area is shaded in purple when the area is completely defined. The excluded area is shaded in purple.

Step 10 To define additional exclusion regions, repeat Step 5 to Step 9.

Step 11 When all exclusion areas are defined, choose **Save** from the Command menu or click the **disk** icon on the toolbar to save the exclusion region.

Note To delete an exclusion area, click the area to be deleted. The selected area is outlined by a dashed purple line. Next, click the **X** icon on the toolbar. The area is removed from the floor map.

Step 12 Select the **Location Regions** check box if it is not already selected, click **Save setting**s, and close the Layers configuration page when complete.

Step 13 To resynchronize Prime Infrastructure and location databases, choose **Services > Synchronize Services**.

Step 14 In the Synchronize page, choose **Network Designs** from the Synchronize drop-down list and then click **Synchronize**.

You can confirm that the synchronization is successful by viewing two green arrows in the Sync. Status column.

Enabling CMX Analytics Service on the Mobility Services Engine

To enable CMX analytics service on the mobility services engine within the Prime Infrastructure UI, follow these steps:

Step 1 Choose **Services > Mobility Services Engine**.

The Mobility Services Engines page appears.

Step 2 In the Mobility Services page, click the **Device Name** to configure its properties.

Step 3 To enable CMX analytics service on the mobility services engine, select the check box next to the CMX analytics Service.

Step 4 Click **Save**.

Step 5 Click **Done** to save the settings.

Managing User Accounts

The Cisco Prime Infrastructure Administration enables you to schedule tasks, administer accounts, and configure local and external authentication and authorization. Also, set logging options, configure mail servers, and data management related to configuring the data retain periods. Information is available about the types of Prime Infrastructure licenses and how to install a license.

Organizations need an easy and cost-effective method to manage and control wireless network segments using a single management platform. They need a solution that supports limiting an individual administrator to manage or control the wireless LAN.

This section contains the following topics:

Configuring Prime Infrastructure User Accounts

This section describes how to configure a Prime Infrastructure user. The accounting portion of the AAA framework is not implemented at this time. Besides complete access, you can give administrative access with differentiated privileges to certain user groups. Prime Infrastructure supports external user authentication using these access restrictions and authenticates the users against the TACACS+ and RADIUS servers.

The username and password supplied by you at install time are always authenticated, but the steps you take here create additional superusers. If the password is lost or forgotten, you must run a utility to reset the password to another user-defined password.

To configure a new user account to Prime Infrastructure, follow these steps:

Step 1 Start Prime Infrastructure server by following the instructions in the "Starting the Prime Infrastructure Server" section on page 2-11.

Step 2 Log into Prime Infrastructure user interface as *root*.

Note We recommend that you create a new superuser assigned to the SuperUsers group.

Step 3 Choose **Administration > AAA**. The Change Password page appears.

Step 4 In the Old Password text box, enter the current password that you want to change.

Step 5 Enter the username and password for the new Prime Infrastructure user account. You must enter the password twice.

Note These entries are case sensitive.

Step 6 Choose **User Groups** from the left sidebar menu. The All Groups page displays the following group names.

Note Some usergroups cannot be combined with other usergroups. For instance, you cannot choose both lobby ambassador and monitor lite.

- System Monitoring—Allows users to monitor Prime Infrastructure operations.
- ConfigManagers—Allows users to monitor and configure Prime Infrastructure operations.
- Admin—Allows users to monitor and configure Prime Infrastructure operations and perform all system administration tasks.

Note If you choose admin account and log in as such on the controller, you can also see the guest users under Local Net Admin.

- SuperUsers—Allows users to monitor and configure Prime Infrastructure operations and perform all system administration tasks including administering Prime Infrastructure user accounts and passwords. Superusers tasks can be changed.
- Users Assistant—Allows only local net user administration. User assistants cannot configure or monitor controllers. They must access the Configure > Controller page to configure these local net features.

Note If you create a user assistant user, log in as that user, and choose **Monitor > Controller**, you receive a "permission denied" message, which is an expected behavior.

- Lobby Ambassador—Allows access for configuration and management of only Guest User user accounts.
- Monitor lite—Allows monitoring of assets location.
- Root—Allows users to monitor and configure Prime Infrastructure operations and perform all system administration tasks including changing any passwords. Only one user can be assigned to this group and is determined upon installation. It cannot be removed from the system, and no task changes can be made for this user.

Step 7 Click the name of the user group to which you assigned the new user account. The Group Detail > *User Group* page shows a list of this permitted operations of the group.

From this page you can also show an audit trail of login and logout patterns or export a task list.

Step 8 Make any desired changes by selecting or unselecting the appropriate check boxes for task permissions and members.

Note Any changes you make affect all members of this user group.

Note To view complete details in the Monitor > Client details page and to perform operations such as Radio Measurement, users in User Defined groups need permission for Monitor Clients, View Alerts & Events, Configure Controllers, and Client Location.

Step 9 Click **Submit** to save your changes or **Cancel** to leave the settings unchanged.

Deleting Prime Infrastructure User Accounts

To delete a Prime Infrastructure user account, follow these steps:

Step 1 Start Prime Infrastructure server by following the instructions in the "Starting the Prime Infrastructure Server" section on page 2-11.

Step 2 Log into Prime Infrastructure user interface as a user assigned to the SuperUsers group.

Step 3 Choose **Administration > AAA**.

Step 4 Choose **Users** from the left sidebar menu to display the Users page.

Step 5 Select the check box to the left of the user account(s) to be deleted.

Step 6 From the Select a command drop-down list, choose **Delete User(s)**, and click **Go**.

When prompted, click **OK** to confirm your decision. The user account is deleted and can no longer be used.

Changing Passwords

To change the password for a Prime Infrastructure user account, follow these steps:

Step 1 Start Prime Infrastructure server by following the instructions in the "Starting the Prime Infrastructure Server" section on page 2-11.

Step 2 Log into Prime Infrastructure user interface as a user assigned to the SuperUsers group.

Step 3 Choose **Administration > AAA** to display the Change Password page.

Step 4 Enter your old password.

Step 5 Enter the new password in both the New Password and Confirm New Password text boxes.

Step 6 Click **Save** to save your changes. The password for this user account has been changed and can be used immediately.

Viewing or Editing User Account Information

To see the group the user is assigned to or to adjust a password or group assignment for that user, follow these steps:

Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **Users**.

Step 3 Click a user in the User Name column. The User Detail : *User Group* page appears.

You can see which group is assigned to this user or change a password or group assignment.

Adding a New User

The Add User page allows the administrator to set up a new user login including username, password, groups assigned to the user, and virtual domains for the user.

Note You can only assign virtual domains to a newly created user which you own. By assigning virtual domains to a user, the user is restricted to information applicable to those virtual domains.

This section contains the following topics:

Adding User Names, Passwords, and Groups

To add a new user, follow these steps:

Step 1 Choose **Administration > AAA**.

Step 2 From the left sidebar menu, choose **Users**.

Step 3 From the Select a command drop-down list, choose **Add User**.

Step 4 Click **Go**. The Users page appears.

Step 5 Enter a new **Username**.

Step 6 Enter and confirm a password for this account.

Step 7 Select the check box(es) of the groups to which this user is assigned.

Note If the user belongs to Lobby Ambassador, Monitor Lite, Northbound API, or Users Assistant group, the user cannot belong to any other group.

- Admin—Allows users to monitor and configure Prime Infrastructure operations and perform all system administration tasks.
- ConfigManagers—Allows users to monitor and configure Prime Infrastructure operations.
- System Monitoring—Allows users to monitor Prime Infrastructure operations.
- Users Assistant—Allows local net user administration only.
- Lobby Ambassador—Allows guest access for configuration and management only of user accounts. If Lobby Ambassador is selected, a Lobby Ambassador Defaults tab appears.
- Monitor Lite—Allows monitoring of assets location.
- North Bound API User—A user group used by Prime Infrastructure Web Service consumers. That is, any North Bound APIs.

Note If you are creating a North Bound API user from TACACS or RADIUS, the default user domain should be *root*.

Note North Bound API Users cannot be assigned a Virtual Domain. When a North Bound API group is selected, the Virtual Domains tab is not available.

- SuperUsers—Allows users to monitor and configure Prime Infrastructure operations and perform all system administration tasks including administering Prime Infrastructure user accounts and passwords. Superuser tasks can be changed.
- Root—This group is only assignable to 'root' user and that assignment cannot be changed.
- User Defined.

Assigning a Virtual Domain

To assign a virtual domain to this user, follow these steps:

Step 1 Click the **Virtual Domains** tab. This tab displays all virtual domains available and assigned to this user.

Note The Virtual Domains tab enables the administrator to assign virtual domains for each user. By assigning virtual domains to a user, the user is restricted to information applicable to those virtual domains.

Note North Bound API Users cannot be assigned a Virtual Domain. When a North Bound API group is selected, the Virtual Domains tab is not available.

Step 2 Click to highlight the virtual domain in the Available Virtual Domains list that you want to assign to this user.

Note You can select more than one virtual domain by holding down the Shift or Control key.

Step 3 Click **Add >**. The virtual domain moves from the Available Virtual Domains to the Selected Virtual Domains list.

To remove a virtual domain from the Selected Virtual Domains list, click to highlight the domain in the Selected Virtual Domains list, and click **Remove**. The virtual domain moves from the Selected Virtual Domains to the Available Virtual Domains list.

Step 4 Click **Submit** to save the changes or **Cancel** to close the page without adding or editing the current user.

Logging into CMX Analytics User Interface

To log into CMX analytics user interface through a web browser, follow these steps:

Step 1 In the address line of browser, enter **https://mse-ip-address/ui/**, where mse-ip-address is the IP address of the CMX analytics server. CMX analytics user interface displays the User Login page.

Step 2 Enter your username.

Step 3 Enter your password.

Step 4 Click **Login** to log into CMX analytics.

The CMX analytics home page appears.

WebGL Requirements

The CMX analytics in Release 7.4 and 7.5 provides ability to view the analytic results in both 2D (Open Street Maps) and 3D (WebGL) environments. This provides improved understanding of results on multiple floor paths, or when dwell times are calculated throughout a multi-storey building. The 3D environment presents the same information as the 2D environment.

WebGL is an advanced feature that provides graphic capabilities. All browsers do not support WebGL on a particular hardware. Verify your browser compatibility at the following URL: http://get.webgl.org/. If your browser supports WebGL, then you must see a spinning cube.

If your browser does not support WebGL, you must do the following:

- Update your latest drivers for video card.
- For Google Chrome, follow the instructions given in the Google Chrome support website.
- For Firefox, follow these steps to enable WebGL:
  - In the browser address line, enter about:config
  - In the Search text box, enter webgl to filter the settings.
  - Double click webgl.forceenabled.
  - Make sure that webgl.disables is disabled.
- For Safari, follow these steps to enable WebGL:
  - Download the latest building of Safari browser.
  - You must enable the Develop menu and enable the WebGL.
  - To enable Develop menu, choose **Safari** > **Preferences**.
  - Click the **Advanced** tab.
  - Select the **Show Develop menu in menu bar** check box.
  - Choose **Enable WebGL** from the Develop menu.

Note If your system does not support 3D, then the analytic results are displayed only in 2D Open Street Maps view.

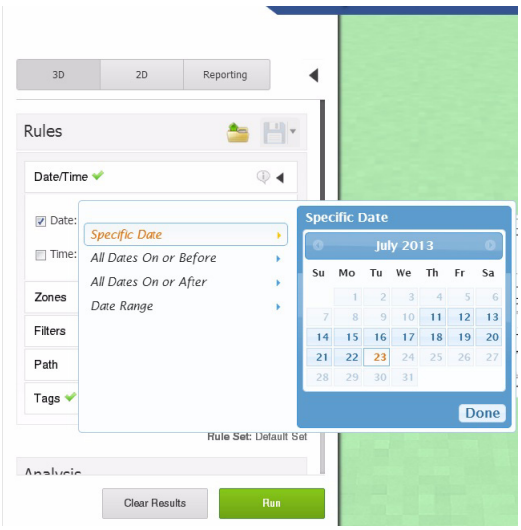
- Internet Explorer 10 does not have the built-in support for WebGL and Microsoft has not announced any plans for implementing it in the future. WebGL support can be manually added to Internet Explorer using third-party plugins such as Chrome-frame.

Validating Analytics

After installing the analytics, you need to validate the results and ensure that the correct data is coming.

Step 1 Look at the date to see how much data is in the Analytics database. When the analytics starts for the first time, it downloads the previous three days data by default if it is available. This may take several hours if there is a lot of data stored in the MSE. Therefore, you should see the current data appearing after an hour or so.

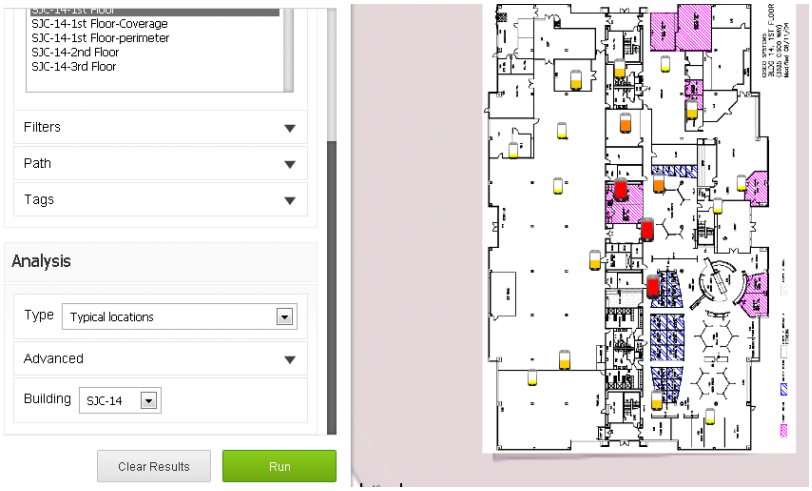
Figure 2-4



Step 2 Next check that the point data coming in is reflecting where in the building it is expected. Using the Heatmap option this show areas of high and low density of points. First, these points should be in locations where you can expect visitors and secondly they should reflect areas where high and low traffic is expected.

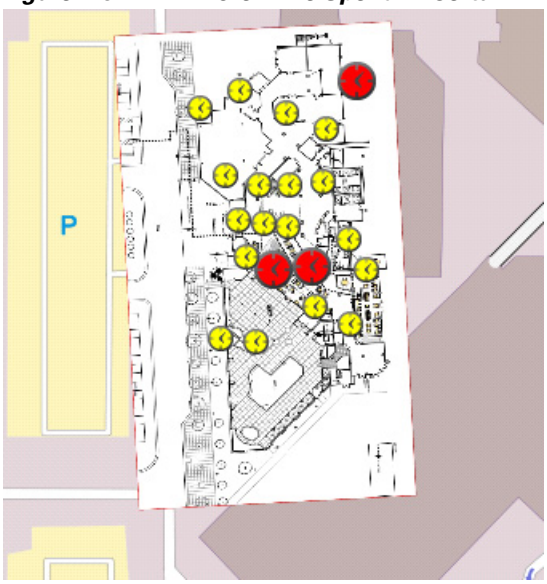
Step 3 Press the run button and this should carry out a typical location analysis for today across the whole building. Here we check that the distribution of device icons show areas where it is expected most/least people visited for the whole day. This check can be further refined by limiting the zones or time window.

Figure 2-5 Distribution of Devices across the Floor



Equally, we can validate areas where people spend more time than others, such as reception, restaurants, etc.

Figure 2-6 More Time Spend in Certain Areas



Step 4 Running the Snapshot report is a way to validate that the distribution of devices across the building at any one time is consistent and for any one zone how it changes during the day.

Figure 2-7 Numbers of Devices Across one Building

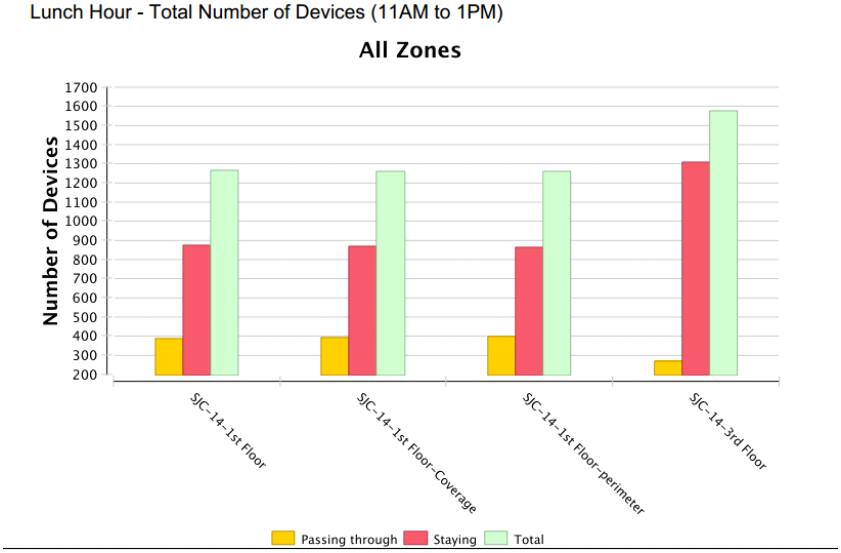
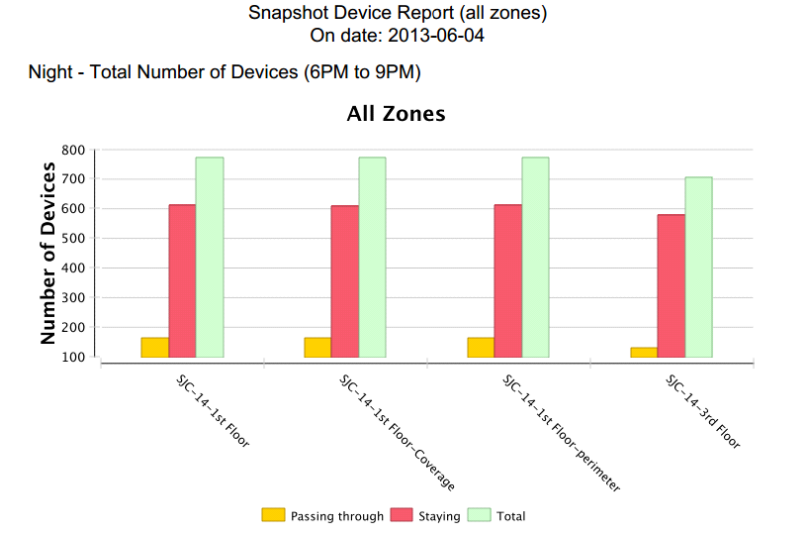


Figure 2-8 Numbers of Devices Across one Building at a Different Time Window



Step 5 These initial first validation steps will ensure that the data is making sense. Use the Rules at the left hand side to further focus in on certain time periods or zones where you know the number and type of visitors. Remember through that we are dealing with devices rather than actual people and so a conversion will need to be made.