Configuring the Mobility Services Engine for CMX

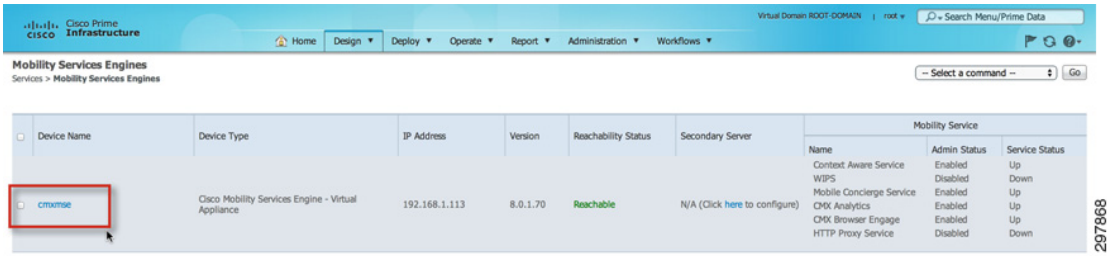
September 4, 2014

Once the Mobility Services Engine (MSE) is configured and synchronized with the WLC, different components of the CMX solution, namely CMX Analytics and CMX Visitor Connect, can be turned on from the MSE UI interface. Note that even if you enabled the services to be turned on as described in Adding Mobility Services Engine in Chapter 24, "Configuring Cisco Prime Infrastructure," the services may not be explicitly turned on.

To verify that the services are indeed turned on using the MSE web GUI:

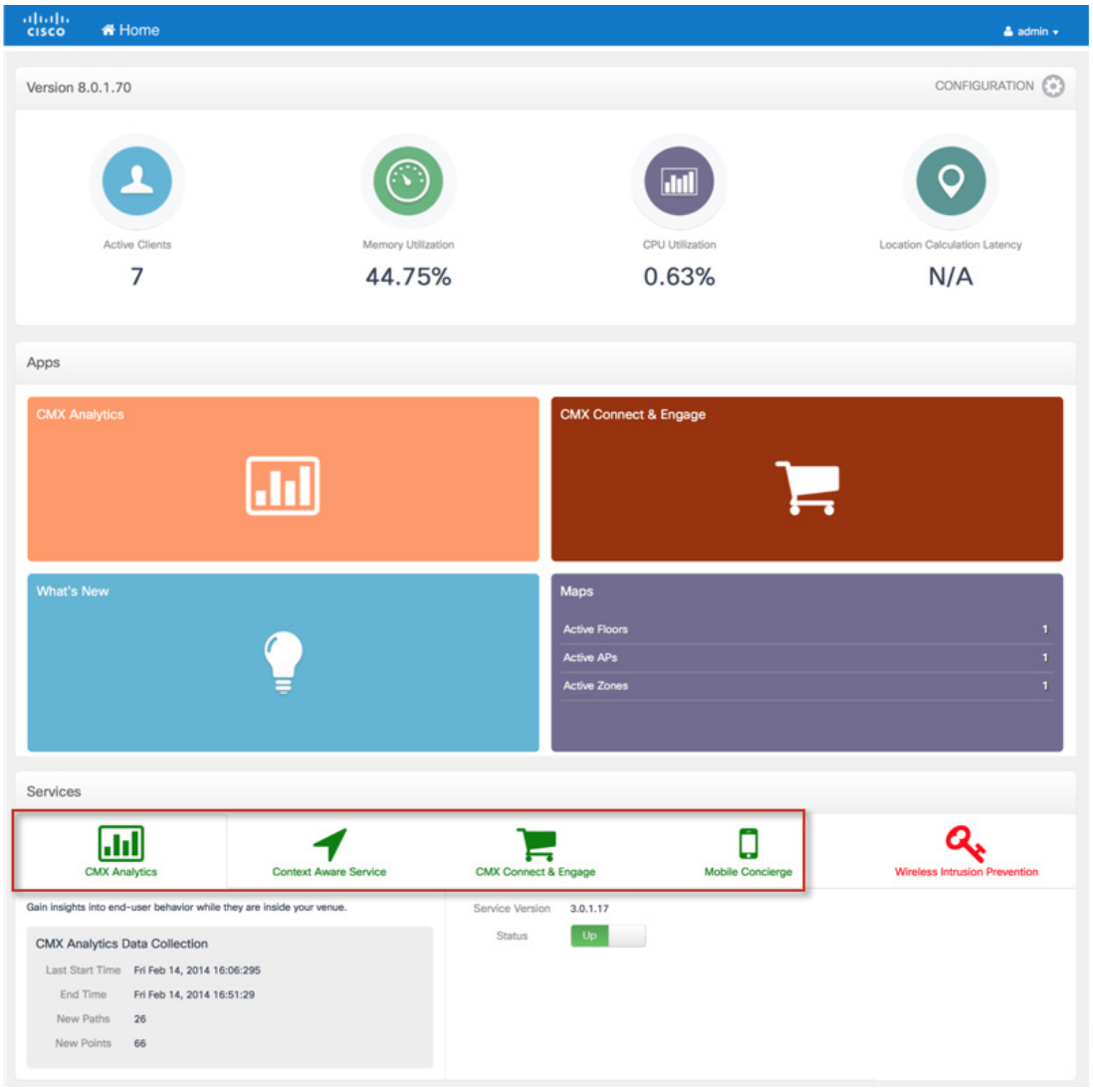
Step 1 To access the MSE web UI, go to **Design > Mobility Sync Services** within Cisco Prime Infrastructure and click the configured MSE to open the UI in a different page, as shown in Figure 25-1.

Figure 25-1 Click the MSE URL



Step 2 Log in to the MSE UI with the username **admin** and the password **admin**. The default username and password can be changed in the MSE UI. On the MSE UI, different services and their status are listed near the end of the page. Select each service and turn them **on** or **off**. For the CMX solution, ensure that CMX Analytics, Context Aware Services, Mobile Concierge Services, and CMX Connect & Engage are turned on. Note that this assumes all of these services are running on a single MSE.

Figure 25-2 MSE Dashboard View

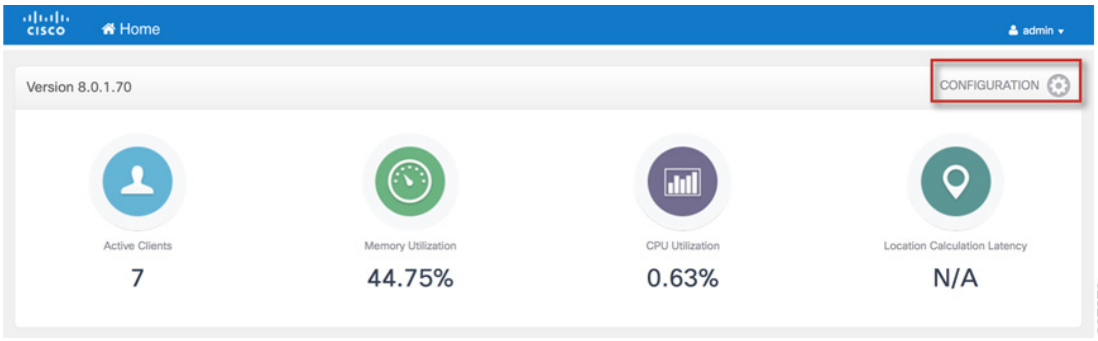


Verifying CMX Settings

Once CMX has been enabled, it is important to check and verify that the CMX solution components are up and running and that everything is set up properly.

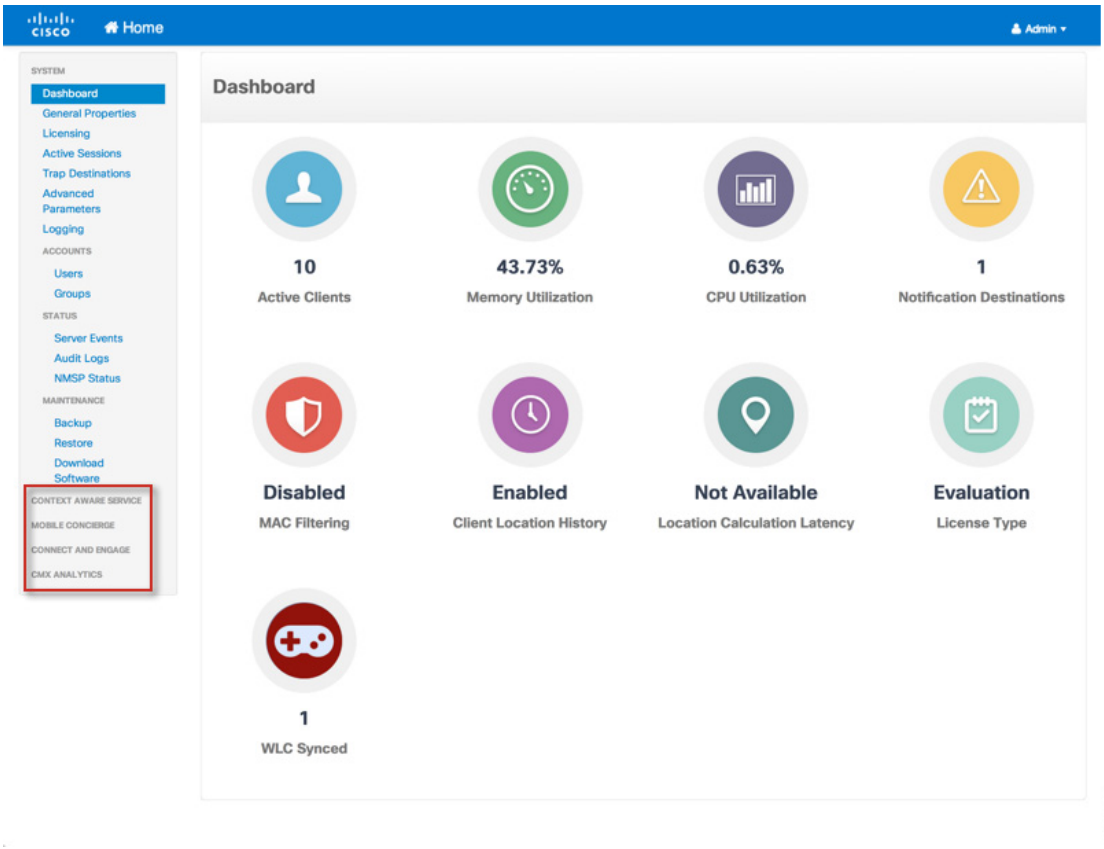
Step 1 On the MSE UI Dashboard, click the **configuration icon**.

Figure 25-3 Click the Configuration Icon on the Dashboard



Step 2 Verify under each of the tabs for Context Aware Service, CMX Analytics, and CMX Connect and Engage that the services are up and are pulling data.

Figure 25-4 Services List on the CMX Dashboard



Step 3 Verify that the Context Aware Service is turned on. Under Tracking parameters, ensure that wireless clients are being tracked. Under History parameters, ensure that client history is enabled. CMX Analytics relies on the history of clients being maintained.

Figure 25-5 Figure 36 Ensure Tracking Parameters on CMX

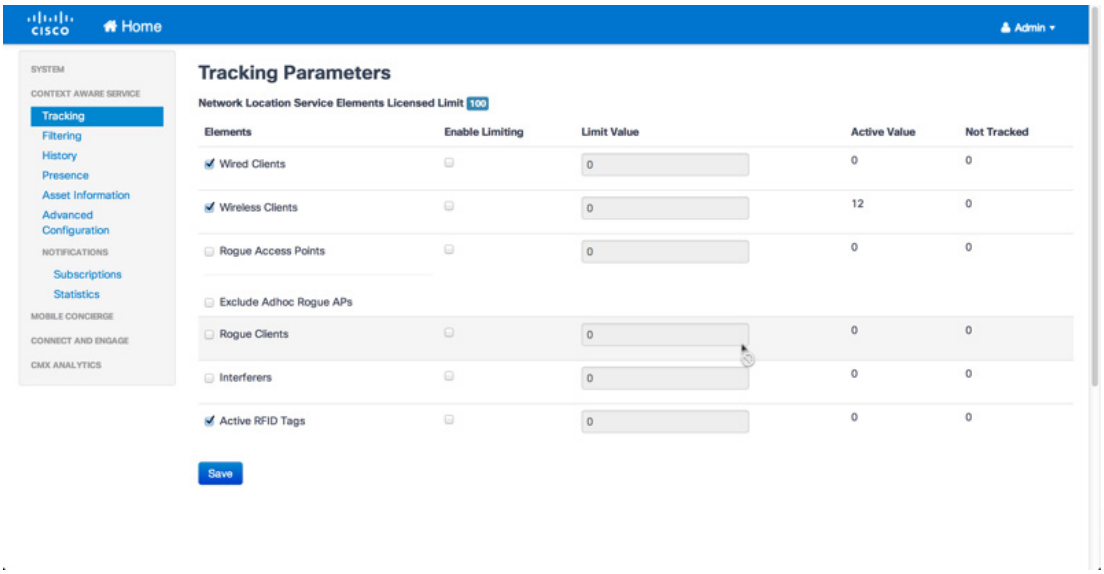
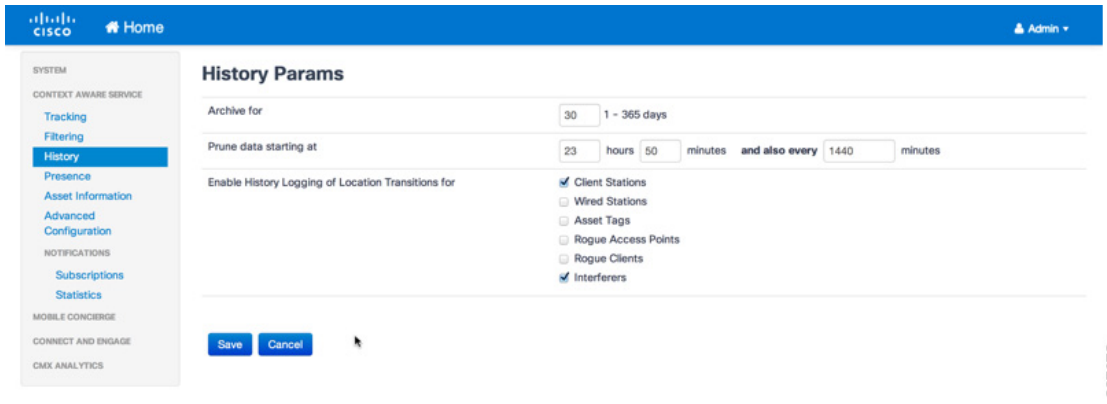


Figure 25-6 History Parameters for CMX

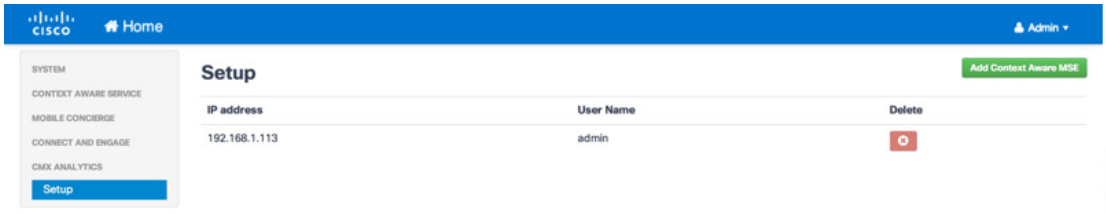


Step 4 Verify that under **Connect and Engage > Setup**, the MSE is listed as one of the CAS MSEs. If its not listed, it is important to use the **Add** button and add the MSE IP address. In most cases this should be configured automatically.

Figure 25-7 CAS Service Setup

Step 5 Verify that under **CMX Analytics > Setup**, the MSE is listed as one of the CAS MSE. If its not listed, it is important to use the **Add** button and add the MSE IP address. In most cases this should be configured automatically.

Figure 25-8 Analytics Services Setup



Configuring Role-Based Access Control (RBAC) on the MSE

The MSE itself has its own role-based access control (RBAC) separate from the CMX Connect & Engage service. For role-based access control of the CMX Connect & Engage service, see Chapter 27, "Configuring RBAC on CMX Connect & Engage."

To configure RBAC, the MSE administrator must first log in to the MSE via the graphical user interface (GUI).

The following provides an example of the URL to access the MSE Home page.

https://<MSE_IP_Address>/mseui/apps

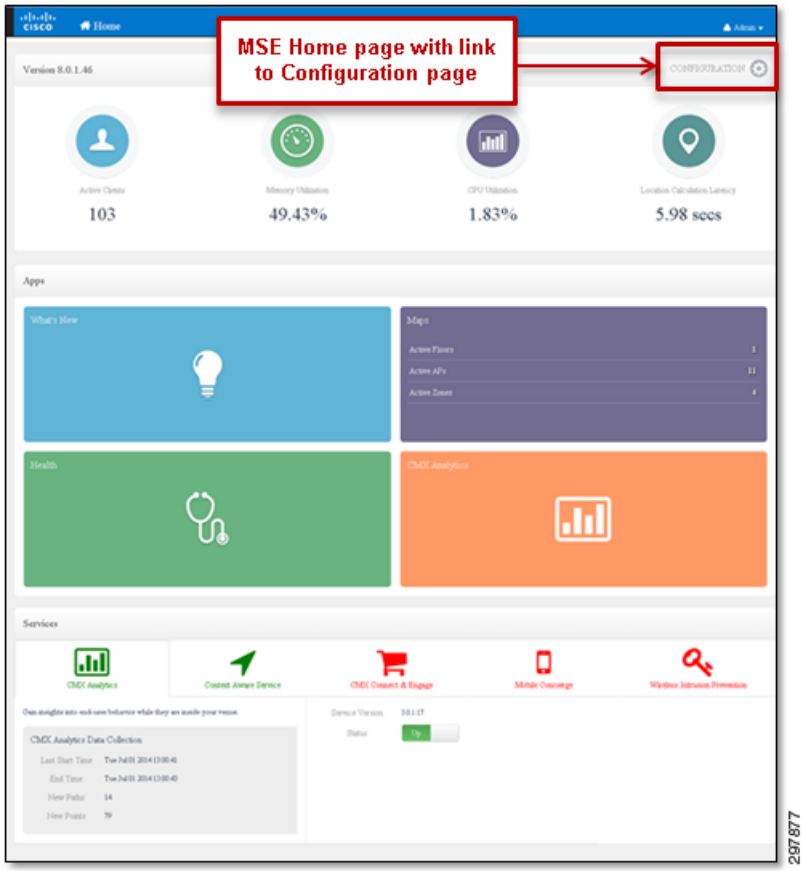
MSE_IP_Address is the IP address of the MSE server.

Figure 25-9 shows an example of the login screen which should be displayed.

Figure 25-9 MSE Login Page

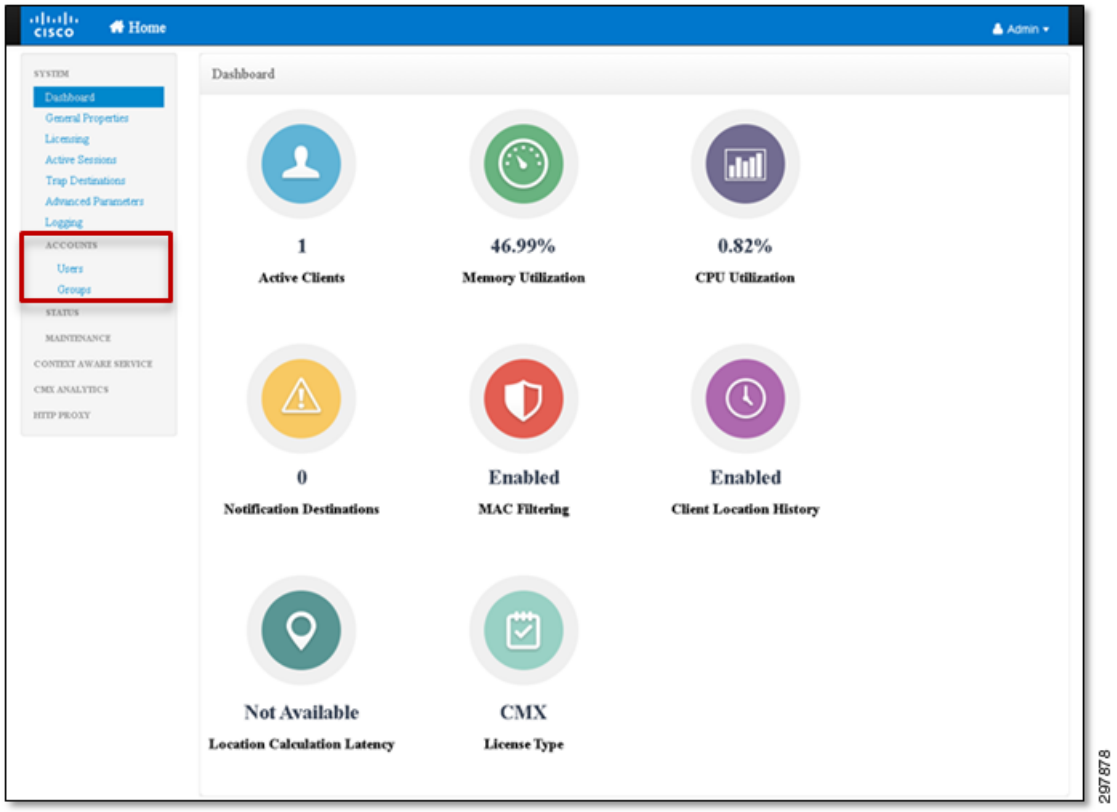
Upon logging in, the MSE administrator is automatically taken to the MSE Home page, as shown in Figure 25-10.

Figure 25-10 Example of MSE Home Page with Link to Configuration



To configure role-based access control, the MSE administrator needs to click the **Settings icon** in the upper right corner of the page to display the MSE Dashboard page, as shown in Figure 25-11.

Figure 25-11 Example of MSE Dashboard

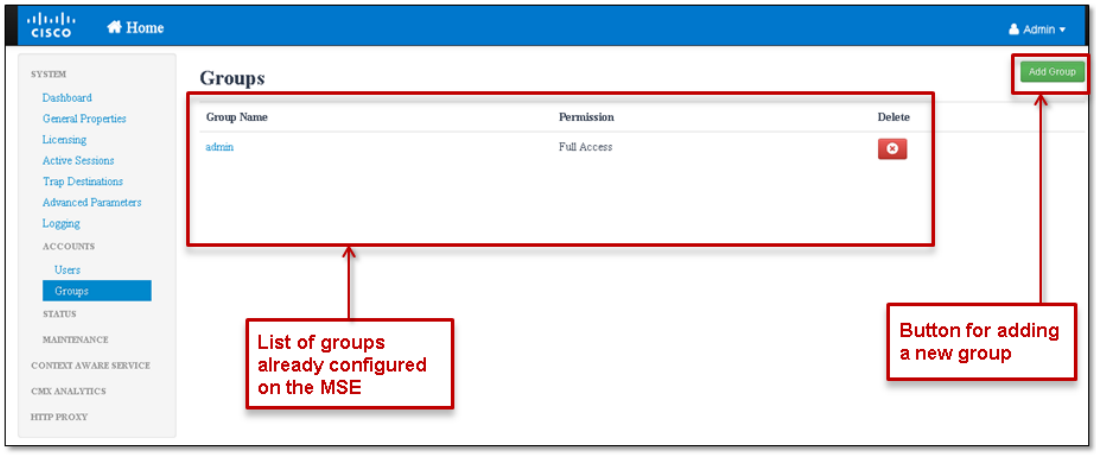


The panel on the left side of the page has four main topics (with sub-topics under several of the main topics) for configuration of the MSE:

- System
- Context Aware Service
- Connect & Engage
- CMX Analytics

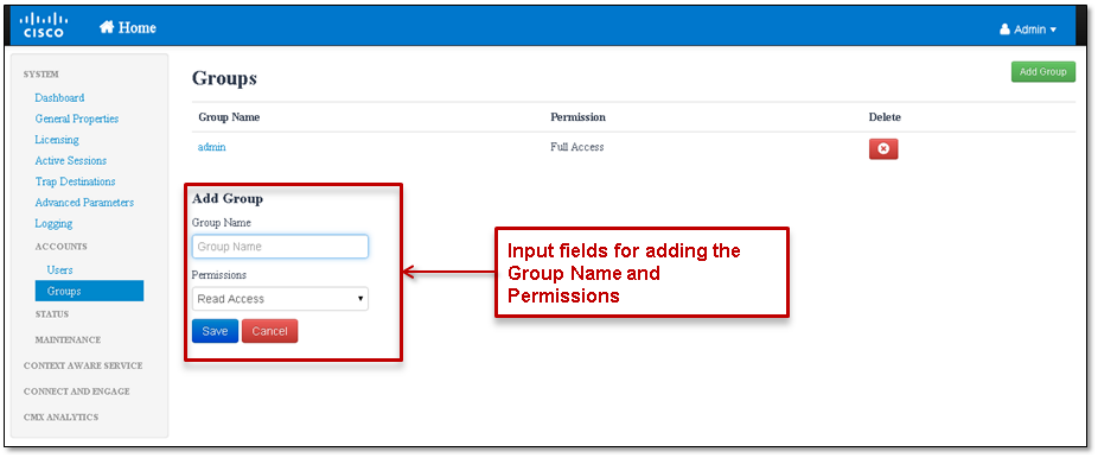
Role-based access control is configured through the Accounts sub-topic under the System topic, as shown in Figure 25-11. The MSE administrator must first configure one or more Groups by clicking the **Groups** link under the Accounts sub-topic located in the panel on the left side of the page, which displays the Groups page, as shown in Figure 25-12.

Figure 25-12 Example of Groups Page



When the MSE administrator clicks the **Add Group** button, the Groups page is modified to include input fields for the Group Name and Permissions, as shown in Figure 25-13.

Figure 25-13 Example of the Groups Page Showing the Add Group Fields



Once the MSE administrator has added the Group Name, they can select the Permissions from the drop down menu:

- Read Access—Provides only the ability to view information on the MSE.
- Write Access—Provides the ability to make modifications to the configuration of the MSE.
- Full Access—Provides complete administrative access, including the ability to enable and disable services, shutdown or reload the MSE, and upgrade MSE code versions.

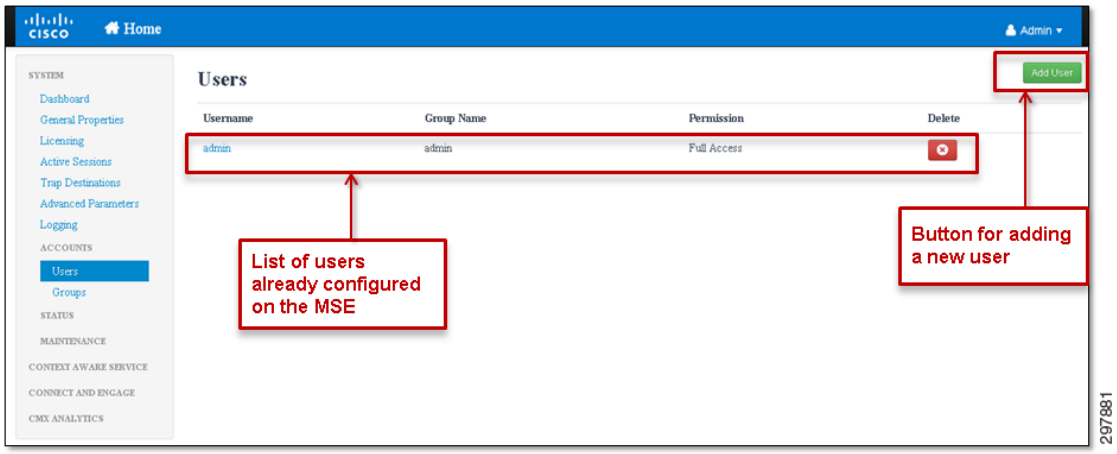
Clicking the **Save** button adds the new group with desired permissions. Clicking **Cancel** cancels the addition of the new group.

Note As of MSE version 8.0, it is not recommended to utilize Read Access groups on the MSE. CMX Presence Analytics currently does not participate in Role-Based Access Control (RBAC) on the MSE. Hence any userid which is part of a Read Access group is also able to add/modify/delete CMX Presence Analytics configuration. Note that the use of only Write Access and Full Access groups means that any non-IT

personnel who require access to the CMX Analytics dashboard, analytics tab, or reports may also have access to add/modify/delete CMX Analytics (location and presence) configuration. One way to mitigate some of this risk is for IT personnel to download CMX Analytics Reports and email them to non-IT personnel at regular intervals. Alternatively, the list of non-IT personnel—such as store operations managers, marketing executives, etc.—who have direct access to the MSE for CMX Analytics should be kept tightly controlled.

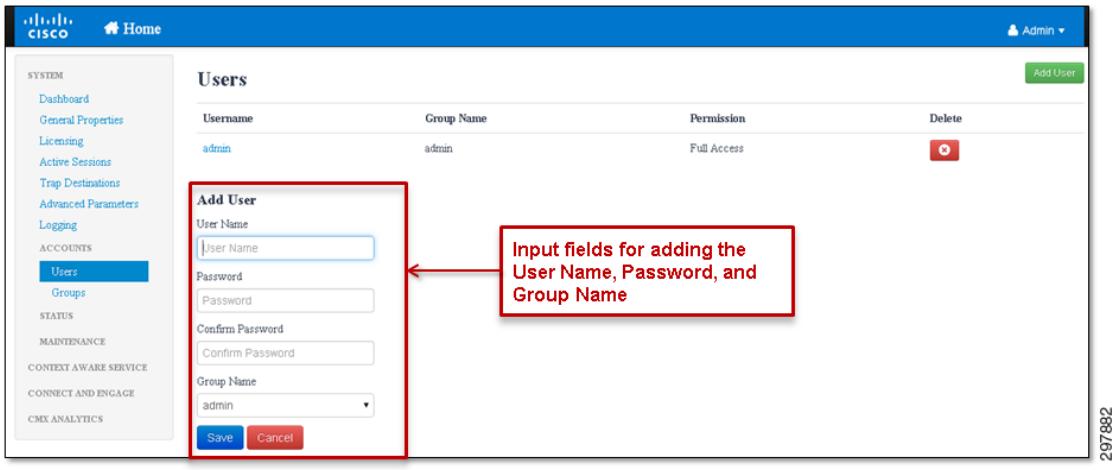
Once the MSE administrator has added the new group, they can add individual user accounts to the group by clicking the **Users** link under the Accounts topic located in the panel on the left side of the page. This displays the Users page, as shown in Figure 25-14.

Figure 25-14 Example of the Users Page



When the MSE administrator clicks the **Add User** button, the Users page is modified to include input fields for the User Name, Password, and Group Name, as shown in Figure 25-15.

Figure 25-15 Example of the Users Page Showing the Add User Fields



Once the MSE administrator has added the User Name and Password, they can select the **Group Name** from the drop-down menu. Only groups which were previously configured appear in the drop-down menu.

Clicking the **Save** button adds the new user with desired permissions. Clicking **Cancel** cancels the addition of the new user.