Other system menu options

This chapter provides brief descriptions of selected System menu options. A pointer to documents that contain a more detailed description for each of these System menu options is provided.

BLF presence group setup

In Cisco Unified Communications Manager Administration, use the **System** > **BLF Presence Group** menu path to configure BLF presence groups.

When you configure BLF Presence in Cisco Unified Communications Manager Administration, an interested party, known as a watcher, can monitor the real-time status of a directory number or SIP URI, a presence entity, from the device of the watcher.

Cisco Unified Communications Manager controls which destinations a watcher can monitor with BLF presence groups. A BLF presence group contains watchers and the destinations that can be monitored by the watchers in the group. To allow watchers in one group to monitor directory numbers in other groups, you specify permission settings to allow or block (disallow) the BLF presence request. Presence authorization works with the BLF presence groups that are configured to ensure that a watcher has permission to monitor the status of a destination.

After you configure the BLF presence groups, you apply a BLF presence group to the following items in Cisco Unified Communications Manager Administration:

- Directory number—Presence entity for which you want status
- SIP trunk—Watcher
- Phone that is running SIP—Watcher
- Phone that is running SCCP—Watcher
- Application user—Watcher
- End user—Watcher

For information about configuring BLF presence groups, see the *Cisco Unified Communications Manager Features and Services Guide*.

Device mobility group setup

In Cisco Unified Communications Manager Administration, use the **System** > **Device Mobility** > **Device Mobility Group** menu path to configure device mobility groups.

Device mobility groups support the device mobility feature. Device mobility groups represent the highest level geographic entities in your network. Depending upon the network size and scope, your device mobility groups could represent countries, regions, states or provinces, cities, or other entities. For example, an enterprise with a worldwide network might choose device mobility groups that represent individual countries, whereas an enterprise with a national or regional network might define device mobility groups that represent states, provinces, or cities.

See topics related to device mobility group configuration in the *Cisco Unified Communications Manager Features and Services Guide* for more information on the Device Mobility feature.

Device mobility info setup

In Cisco Unified Communications Manager Administration, use the **System** > **Device Mobility** > **Device Mobility Info** menu path to configure device mobility info.

The Device Mobility Info window specifies the subnets and device pools that are used for device mobility. When a phone registers with Cisco Unified Communications Manager, the system compares the IP address of the device to device mobility subnets that are specified in the Device Mobility Info window and associated with one of the device pools.

The matching subnet becomes the device home subnet for the purpose of device mobility.

See the *Cisco Unified Communications Manager Features and Services Guide* for more information on the Device Mobility feature.

Physical location setup

In Cisco Unified Communications Manager Administration, use the **System** > **Physical Location** menu path to configure physical locations.

Physical locations support the Device Mobility feature. Physical locations provide a means of distinguishing the parameters that relate to a specific geographical location from other parameters. For example, a media resources server may serve a specific office or campus within the enterprise. When a device roams to another office or campus and reregisters with Cisco Unified Communications Manager, you want to have the media resources server at the roaming location serve the device. By defining the physical location according to availability of media services, you can assure efficient and cost-effective reassignment of services as devices move from one physical location to another. Depending upon the network structure and allocation of services, you may define physical locations based upon a city, enterprise campus, or building.

See topics related to physical location configuration in the *Cisco Unified Communications Manager Features and Services Guide* for more information on the device mobility feature.

Certificate setup

In Cisco Unified Communications Manager Administration, use the **System** > **Security** > **Certificate** menu path to configure certificates.

Phone security profile setup

In Cisco Unified Communications Manager Administration, use the **System** > **Security** > **Phone Security Profile** menu path to configure phone security profiles.

The Phone Security Profile window includes security-related settings such as device security mode, CAPF settings, digest authentication settings (only for phones that are running SIP), and encrypted configuration file settings. You must apply a security profile to all phones that are configured in Cisco Unified Communications Manager Administration.

For information on configuring and applying a phone security profile, see the *Cisco Unified Communications Manager Security Guide*.

SIP trunk security profile setup

In Cisco Unified Communications Manager Administration, use the **System** > **Security** > **SIP Trunk Security Profile** menu path to configure SIP trunk security profiles.

The SIP Trunk Security Profile window includes security-related settings such as transport type, device security mode, digest authentication settings, and authorization settings for incoming SIP messages. You must apply a security profile to all SIP trunks that are configured in Cisco Unified Communications Manager Administration.

For information on configuring and applying a SIP trunk security profile, see the *Cisco Unified Communications Manager Security Guide*.

CUMA server security profile setup

In Cisco Unified Communications Manager Administration, use the **System** > **Security** > **CUMA Server Security Profile** menu path to configure CUMA server security profiles.

The CUMA Server Security Profile window includes security-related settings such as device security mode, incoming transport type, and X.509 subject name. This security profile automatically gets applied to all Cisco Unified Mobile Communicator clients that you configure in the device configuration window of Cisco Unified Communications Manager Administration.

For information on configuring a Cisco Unity Mobility Advantage (CUMA) server security profile, see the *Cisco Unified Communications Manager Security Guide*. For information on setting up a security profile for a CUMA server, see your Cisco Unified Mobility Advantage documentation. Make sure that the CUMA Security Profile you configure on Cisco Unified Communications Manager matches the security profile on the CUMA servers.

License Usage Report setup

In Cisco Unified Communications Manager Administration, use the **System** > **Licensing** > **License Usage Report** menu path to configure the license usage report.

Geolocation setup

In Cisco Unified Communications Manager Administration, use the **System** > **Geolocation Configuration** menu path to configure geographic locations for use with geographic location filters and logical partition policies to provision logical partitioning and other features.

Tip Do not confuse locations with geolocations. Locations, which you configure by using the **System** > **Location** menu option, allow you to define entities that a centralized call-processing system uses to provide call admission control (CAC). Geolocations, which you configure by using the **System** > **Geolocation Configuration**menu option, allow you to specify geographic locations that you use to associate Cisco Unified Communications Manager devices for features such as logical partitioning.

For an explanation of geolocations, location conveyance, and configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*.

For more information on how the logical partitioning feature uses geolocations, see the *Cisco Unified Communications Manager Features and Services Guide*.

Geolocation filter setup

In Cisco Unified Communications Manager Administration, use the **System** > **Geolocation Filter** menu path geographic location filters for use with geographic locations and logical partition policies to provision logical partitioning.

For an explanation of geolocations filters, including configuration details, see the *Cisco Unified Communications Manager Features and Services Guide*.

For more information on how the logical partitioning feature uses geolocation filters, see the *Cisco Unified Communications Manager Features and Services Guide*.