



## CHAPTER 10

# Provisioning Other Hosted Unified Communications Services Features

---

This chapter describes how to use VisionOSS Unified Services Manager (USM) application to provision the components of the Cisco Hosted Unified Communications Services (UCS), Release 7.1(a) platform.

It details how to use the application to manage the various Hosted UCS features of a Cisco Multi-tenant Hosted Unified Communications Services (UCS) 7.1(a) deployment.

This chapter includes the following sections:

- [Provider Specific Features, page 10-2](#)
- [Customer Specific Features, page 10-6](#)
- [Customer Specific Features, page 10-6](#)
- [Phone Specific Features, page 10-8](#)

# Provider Specific Features

Cisco Hosted Unified Communications Services, Release 7.1(a) introduces support for provider specific features.

This section describes the required steps to provision a provider or per-country provider specific features in a Cisco Hosted UCS 7.1(a) environment.

This section contains:

- [Forced Central PSTN Breakout, page 10-2](#)
- [Forced OffNet, page 10-3](#)
- [Forced Authorisation Codes \(FAC\), page 10-4](#)

## Forced Central PSTN Breakout

The Cisco Hosted UCS 5.1(b) platform extends support to the Forced Central PSTN Breakout functionality.

You can configure the Cisco PGW using USM to analyze the outgoing PSTN calls and to “force” the use of the central gateways for some PSTN destinations. Additionally, the Administrator can provision a subset of these numbers to be “allowed” to use the local gateway.

The following section explains how to configure the Forced Central PSTN Breakout in two ways:

- [Forced To Use, page 10-2](#)
- [Allowed To Use, page 10-3](#)

## Forced To Use

To provision a range of numbers to be “Forced” to use Central Gateways, perform the following steps:

### Procedure

- 
- Step 1** Go to **Provider Administration > Providers**.
  - Step 2** Select the provider you want to configure, from the Search Results area.
  - Step 3** Click **Advanced Mgt.**
  - Step 4** Click **International Gateway Usage**.
  - Step 5** Select the Cisco PGW that you want to configure, from the Search Results area.
  - Step 6** Click **Add**.
  - Step 7** Enter the following:
    - Country: <country>, for example, *United States*
    - National Code: Although it says National Code, you can enter any part of a E.164 number (even the full E.164 number if you want to “Force” only one number to go out through the Central PSTN Breakout), for example *212211*
  - Step 8** Select Force Central.

**Note**

---

Country and Gateway Usage are mandatory fields.

---

**Step 9** Click **Add**.

This generates the configuration details of the Forced Central PSTN Breakout.

---

## Allowed To Use

To provision a range of numbers to be “Allowed” to use Local Gateways, perform the following steps:

### Procedure

---

**Step 1** Go to **Provider Administration > Providers**.

**Step 2** Select the provider you want to configure, from the Search Results area.

**Step 3** Click **Advanced Mgt.**

**Step 4** Click **International Gateway Usage**.

**Step 5** Select the Cisco PGW that you want to configure, from the Search Results area.

**Step 6** Click **Add**.

**Step 7** Enter the following:

- Country: <country>, for example, `United States`
- National Code: Although it says National Code, you can enter any part of a E.164 number (even the full E.164 number if you want to “Force” only one number to go out through the Central PSTN Breakout), for example `2122112`

**Tip**

---

The example numbers mentioned will force all numbers in the ranges from 212-211-0000 to 212-211-1999 and from 212-211-3000 to 212-211-9999 to use the Central PSTN Breakout.

---

**Step 8** Select Allow Local.

**Step 9** Click **Add**.

This generates the configuration details of the Forced Central PSTN Breakout.

---

Repeat this procedure for all providers.

## Forced OffNet

Cisco Hosted UCS 7.1(a) extends support to the Forced OffNet facility.

It allows you to configure the Cisco PGW using USM to analyze outgoing PSTN calls and to “Force” all OffNet calls to go out of the Hosted UCS environment, even if the destination is a user in the Hosted UCS environment.

The following section explains how to configure the Forced OffNet option.

To provision a range of numbers to be “Forced” out of the Hosted UCS environment, perform the following steps:

#### Procedure

**Step 1** Go to **Provider Administration > Countries**.

**Step 2** Select the Country you want to configure, from the Search Results area.



#### Caution

Ensure to add a reseller for the correct provider. It displays the name of the provider.

**Step 3** Click **Force OffNet**.

**Step 4** In the Add Prefix area, enter the following:

- Prefix <Prefix>, enter the E.164 number prefix which will define the range of E.164 numbers to be “Forced” Offnet, for example: 441630212
- Country Code



#### Tip

The example prefix mentioned will force all numbers in the range from 441630212000 to 441630212999 out of the Hosted UCS environment.

**Step 5** Click **Add**.

This generates the configuration details of the Forced Central PSTN Breakout.

Repeat this procedure for all providers.

If you were to upgrade to Cisco Hosted UCS 7.1(a), the Administrator deletes existing “Forced” OffNet configurations.

This occurs when you provision “Forced” OffNet in Cisco Hosted UCS 5.1(b) by replacing the PGW transaction (used for the “Forced” Central PSTN Breakout feature in the PGW model) with the PGW transaction required for the “Forced” OffNet feature, and then utilize the USM interface to provision “Forced” Central PSTN Breakout.

After upgrading to Cisco Hosted UCS 7.1(a), the Administrator must re-provision the previously configured numbers using the provisioning procedure as described in [Forced Central PSTN Breakout](#).

## Forced Authorisation Codes (FAC)

Forced Authorization Codes (FACs) allow administrators to manage call access and accounting. This feature regulates the types of calls that certain users can place by forcing the user to enter a valid authorization code before the call completes. Each FAC has three items of data associated with it, and is associated to a route pattern. Following sections describes how to provision FAC on HUCS 7.1a deployment.

- [FAC Static Configuration, page 10-5](#)
- [Add Forced Authorization Codes, page 10-5](#)
- [Move FAC to a Location, page 10-5](#)

## FAC Static Configuration

FAC on CUCM is associated with Route Patterns. Hence, route patterns which require FAC need to be updated on CUCM.

- 
- Step 1** Find the Route Pattern on CUCM which require FAC. If you want outgoing central break-out PSTN calls on a location to use FACs, search for the PSTN route pattern for that location in CUCM, for example, search for **9.01[2-9][02-9]XXXXXXXX** route pattern which require FAC. You can use CUCM Digit Analyzer, in case you are not sure of which route pattern is chosen for the dialed number.
- Step 2** Check **Require Forced Authorization Code** check box
- Step 3** Set Authorization Level, default **0**.
- 



**Note**

Authorization Level for a route pattern should be lesser than the FAC code authorization level for call completion using FAC. Otherwise, call routing to dialed number through that Route Pattern would fail.

---

## Add Forced Authorization Codes

To add provision FACs on CUCM via USM, follow the steps below:

- 
- Step 1** Navigate to **Resources > Authorisation Codes** at provider level.
- Step 2** Click **Add Range**.
- Step 3** Under Details section, enter the following:
- Range Start—<FACRangeStart>; for example, **1234**
  - Name—<FACname>; for example, **FACTOPSTN**
  - Level—<AuthorisationLevel>; for example, **2**
  - Range Size—<CodeRangeSize>; for example, **1**
- Step 4** Click **Add Range**.
- 



**Note**

Authorization Level for a route pattern should be lesser than the FAC code authorization level for call completion using FAC. Otherwise, call routing to dialed number through that Route Pattern would fail.

---

## Move FAC to a Location

After adding a FAC, it should be moved to location to which FAC is required.

**Procedure:**

- 
- Step 1** Navigate to **Resources > Authorisation Codes** at provider level.
- Step 2** Click **Assign** on the FAC which you want to move to a location, under the column Assign/Release.

- Step 3** Enter the Range Size; for example, **1**
  - Step 4** Select the Location.
  - Step 5** Click **Assign Range**.
- 

## Customer Specific Features

This section describes the steps required to configure customer specific features in a Cisco Hosted UCS 7.1(a) environment.



### Note

The steps mentioned in this section are optional. If the HUCS7.1a deployment requires the customer specific features mentioned in this section, then following steps are to be performed based on features requirement

---

Cisco Hosted UCS 7.1(a) supports the Block OffNet To OffNet Transfer (BO2OT) customer specific feature.

It is possible to configure a customer using USM, to block a user in a Hosted UCS IP location from transferring an incoming call from the PSTN back to the PSTN.

This section contains the following:

- [Enable BO2OT on Unified CM, page 10-6](#)
- [Configure BO2OT for Customers, page 10-6](#)

## Enable BO2OT on Unified CM

To provision Unified CM to enable the Block OffNet To OffNet Transfer (BO2OT) parameter, perform the following steps:

### Procedure


---

- Step 1** Login to CUCM cluster.
  - Step 2** Navigate to System > Service Parameters.
  - Step 3** Select the CUCM server.
  - Step 4** Select the Cisco CallManager service.
  - Step 5** Under Clusterwide Parameters (Feature - General), set Block OffNet To OffNet Transfer to **True**.
  - Step 6** Click **Save**.
- 

## Configure BO2OT for Customers

To provision a specific customer to Block OffNet To OffNet Transfers, perform the following steps:

### Procedure

- 
- Step 1** Choose **General Administration > Customers**.
- Step 2** Select the customer you want to configure, from the Search Results area.
-  **Caution** Ensure that you are configuring customers for the correct reseller.
- 
- Step 3** Navigate to Customer for which BO2OT is required.
- Step 4** Click **Advanced Mgt.**
- Step 5** Click **Advanced Telephony Settings**.
- Step 6** Click **Enable** next to Block Offnet to Offnet Transfer.
- 

## Location Specific Features

This section describes the steps required to configure location specific features in a Cisco Hosted UCS 7.1(a) environment.



### Note

The steps mentioned in this section are optional. If the HUCS 7.1a deployment requires the location specific features mentioned in this section, then following steps are to be performed based on features requirement.

The following section lays emphasis to the support for overlay area codes that was initially introduced in the Cisco Hosted UCS 5.1(b).

Two principle methods are used to provide numbering relief to NPAs nearing exhaustion:

- [NPA Overlay, page 10-7](#)
- [NPA Geographic Split, page 10-8](#)

## NPA Overlay

An overlay is an alternative way of adding an area. As the name suggests, the new area code "overlays" the pre-existing area code, most often serving the identical geographic area. Numbers from this new NPA are assigned for new growth to all service providers and customers.

In the United States, according to the FCC ruling in the Second Report and Order (R&O) in CC Docket 96-98, the implementation of an NPA overlay for code relief will require a 10-digit dialing within and between NPAs for local calls to ensure dialing parity among all service providers.

The benefit of an NPA overlay is that customers retain their existing area codes. Only new lines get the new area code.

An overlay requires all customers, including those with telephone numbers in the pre-existing area code, to dial area codes for local calls.

## NPA Geographic Split

Most area codes are added by way of a geographic split. The geographic area covered by an existing area code is split in two (or three). One of the sections retains the existing area code (usually the area with the highest customer density to minimize number changes), while others receive new area codes.

The benefit of a geographic split is that an area code remains defined as a geographic area which gives the customers a fairly good idea about the location of the people they are calling.

The down-side of a geographic split is that many customers must cope with the inconvenience of changing their area code.

This section describes the required procedure to define an Overlay Area Code in US Locations with a 10-digit local dialing support. Once the code is configured, a user in these locations can make local calls to a phone in the Overlay Area Code by dialing the “External Prefix” followed by NPA-NXX-XXXX (where NPA is the configured Overlay Area Code).

## Add Overlay Area Codes

Overlay Area Codes are defined in USM as Adjacent Area Codes.




### Note

Overlay Area Code in Hosted UCS7.1a is supported only for location with central PSTN breakout. Location with local PSTN breakout does not support this feature

To add an Overlay Area Code, perform the following steps:

### Procedure

- 
- Step 1** Choose **General Administration > Locations**.
  - Step 2** Select a location for which you want to assign an Overlay Area Code.
- 
-  **Caution** Ensure that you are adding the Overlay Area Code for the correct location.
- 
- Step 3** Click **Advanced Mgt.**
  - Step 4** Click **Adjacent Area Codes**.
  - Step 5** Click **Add**.
  - Step 6** For Enter Adjacent Area Code, enter <OverlayAreaCode>, for example **646**
  - Step 7** Click **Add**.
- 

Repeat this procedure for all required Overlay Area Codes and for all locations.

## Phone Specific Features

This section helps you configure phone specific features in a Cisco Hosted UCS 7.1(a) environment.



Support for XML Phone Application was tested for the first time on Hosted UCS 7.1 (a).

It is possible to configure the Unified CM IP phones to access different XML applications. The Services button on the Cisco Unified CM IP phone helps you select the Phone Services option to access these XML applications.

This section describes three functions you can perform for the XML application:

- [Create Service Type for the XML Phone Service, page 10-9](#)
- [Add XML Phone Service to a Feature Group, page 10-9](#)
- [Personalize phone with XML Application, page 10-10](#)

## Create Service Type for the XML Phone Service

To configure a new phone service, perform the following steps:

### Procedure

---

- Step 1** Go to **Setup Tools > Service Types**.
  - Step 2** Click **Add**.
  - Step 3** Provide a Service Name. For example, `Calendar`
  - Step 4** Provide a description. For example, `Calendar Phone Service`
  - Step 5** Provide a tag. For example, `Calendar`
  - Step 6** Select the Service Category. For example, `phoneapplication`
  - Step 7** Provide the URL of the service. For example,  
`http://10.100.92.33/bvsmweb/bvsmroaming.cgi?device=#DEVICENAME#`
  - Step 8** Click **Add** to create the Phone Service.
- 

## Add XML Phone Service to a Feature Group

To use the already created phone service, you need to add the service to a customer feature group.

To do this, perform the following steps:

### Procedure

---

- Step 1** Go to **General Administration > Feature Groups**.  
If you are not at customer level, you must select the customer of the feature group you want to create or modify.
  - Step 2** Select the feature group where you want to incorporate the phone service or create a new feature group.
  - Step 3** Select the phone service tag that you previously created. For example, `Calendar`
  - Step 4** Click **Add**.
-

## Personalize phone with XML Application

You can personalize a phone application, which is not available in the feature groups, to other phones and user mobility profiles. You can do this when you do not want to make available a phone service for all the phones using the same feature group, but need to only add the service to a specific phone of a location.

To do this, perform the following steps:

### Procedure

---

- Step 1** Go to **General Administration > Locations**.
  - Step 2** Select the location where the phones you want to personalize are located.
  - Step 3** Click **Preferences**.
  - Step 4** Click **PersonalizePhoneApplications** from the list.
  - Step 5** Check the checkbox to enable the setting and click **Modify**.  
Once you enable this preference, you can personalize any phone in that location.
  - Step 6** Go to **Location Administration > Phone Management**.
  - Step 7** Click the MAC address of the phone you want to personalize.
  - Step 8** Scroll down to Phone Applications area and click **Personalize**.
  - Step 9** Click **Subscribe**.
  - Step 10** From the drop down menu, select the Phone service that you created and click **Submit**.
-