

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Conventions](#)

[Configure](#)

[Network Diagram](#)

[Configure Forced Authorization Code](#)

[Configure the Route Pattern](#)

[Restrict Only One Phone to Use FAC](#)

[Verify](#)

[Troubleshoot](#)

[Forced Authorization Codes Randomly Stop to Work](#)

Introduction

This document provides a sample configuration on how you can use Forced Authorization Codes (FAC) in conjunction with route patterns to restrict the access to long distance calls for certain groups of users.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco CallManager configuration
- [Route pattern configuration](#)
- [Cisco IP phone configuration](#)

Components Used

The information in this document is based on Cisco CallManager 11.0 and later.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

FAC and Client Matter Codes (CMC) allow you to manage call access and accounting. CMC assists with call accounting and billing for billable clients, while FACs regulate the certain types of

calls that you can place. The FAC feature forces you to enter a valid authorization code before the call connects. The FAC process is defined here:

1. You dial a number that goes to a FAC-enabled route pattern.
2. Cisco CallManager tells the phone to play a special tone.
3. Then you enter the authorization code. The system then either waits for the FAC Timer (T302/ or interdigit timer) to expire (default 15 seconds) or for the user to press the # key. **Note:** Since the FAC timer affects T302 timer, bear in mind that if you adjust this timer to permit more time for FAC input, it extends the time for normal calls as well.
4. If the code is correct, the call is extended to the exiting gateway and Cisco CallManager generates a Call Detail Record (CDR) flagged with the FAC number.

This document illustrates how a company can restrict call routing for a certain group of users using the FAC. For illustration purposes, consider an organization with these two types of IP phone users:

- Employees
- Managers

This is the requirement:

- The Employee IP phones should be granted access to long distance calls only if the caller enters a FAC with the adequate access level.
- The organization managers should be able to make long distance calls from their IP phones without the need to enter a code.

Conventions

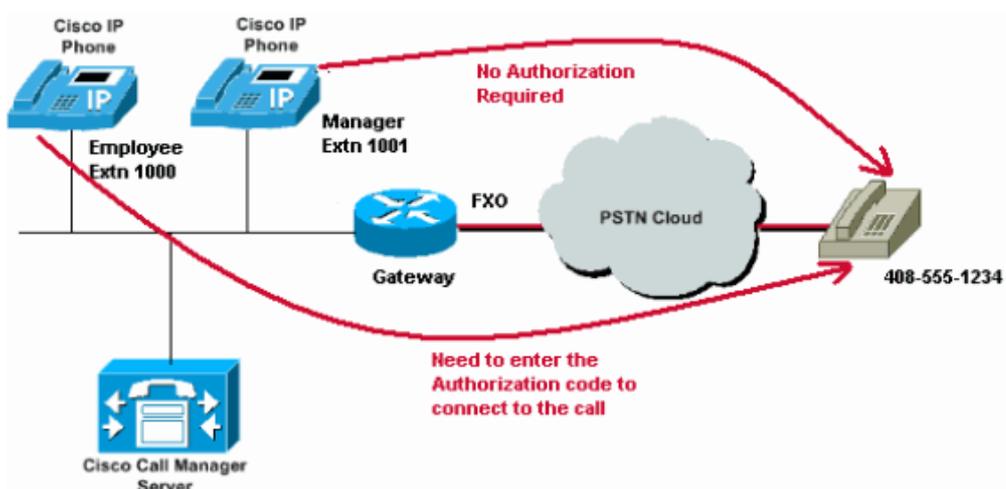
Refer to the [Cisco Technical Tips Conventions](#) for more information on document conventions.

Configure

Perform the configuration procedures in this section in order to meet the requirements mentioned under the Background Information section.

Network Diagram

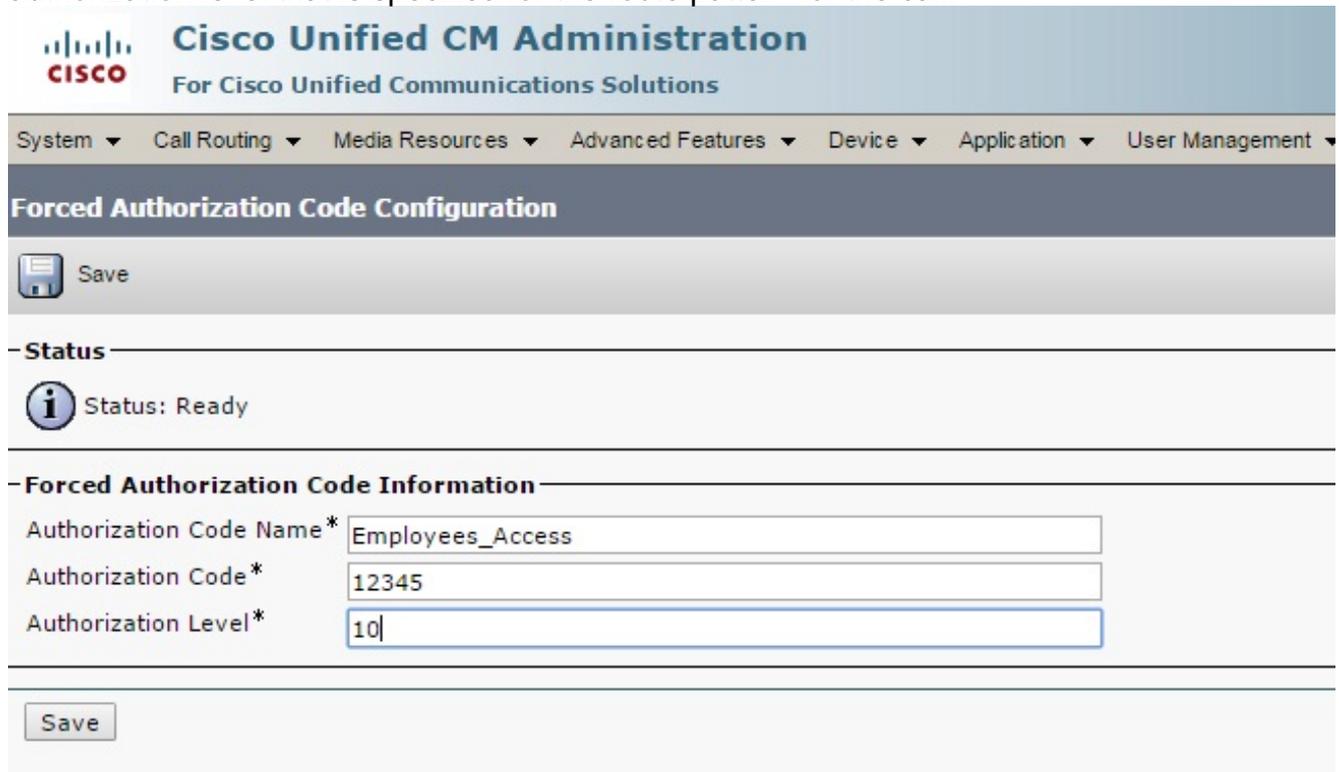
This document uses this network setup, as shown in the image:



Configure Forced Authorization Code

Before you enable the FAC through the route patterns, you need to define the FACs in Cisco CallManager Administration. Complete these steps in order to accomplish this.

1. In Cisco CallManager Administration, navigate to **Call Routing > For**.
2. In the window that opens up, click on **Add New**.
3. Configure these parameters in the FAC Configuration window and click **Save**.
Authorization Code Name—Enter a unique name that is no more than 50 characters. This name ties the authorization code to a specific user or group of users.
Authorization Code—Enter a unique authorization code that is no more than 16 digits. In our example, this code is configured as **12345**. The user enters this code when the user places a call through a FAC-enabled route pattern.
Authorization Level—Enter a three-digit authorization level that exists in the range of 0 to 255; the default equals 0. The level that you assign to the authorization code determines whether the user can route calls through FAC-enabled route patterns. In order to successfully route a call, the user authorization level must equal or be greater than the authorization level that is specified for the route pattern for the call.



The screenshot displays the Cisco Unified CM Administration web interface. At the top, the Cisco logo and the text "Cisco Unified CM Administration For Cisco Unified Communications Solutions" are visible. Below this is a navigation menu with options: System, Call Routing, Media Resources, Advanced Features, Device, Application, and User Management. The main heading is "Forced Authorization Code Configuration". There is a "Save" button with a floppy disk icon. Below that, the "Status" section shows "Status: Ready" with an information icon. The "Forced Authorization Code Information" section contains three input fields: "Authorization Code Name*" with the value "Employees_Access", "Authorization Code*" with the value "12345", and "Authorization Level*" with the value "10". A "Save" button is located at the bottom of the form.

Configure the Route Pattern

Complete these steps in order to enable FAC for the long distance route pattern:

1. In the Cisco CallManager Administration window, create two different partitions. For example, **LongDistanceEmployees** and **LongDistanceManager**.
Note: Refer to [Understanding and Using Partitions and Calling Search Spaces with Cisco CallManager](#) for information on how to create partitions.
2. Create two different Calling Search Spaces (CSSs) named **Employees** and **Manager**. Include the partition **LongDistanceEmployees** in the Employees CSS and **LongDistanceManager** in the the Manager CSS.
Note: Refer to [Calling Search Space](#)

[Configuration](#) for more information on how to configure a CSS.

3. You need to create two separate long distance route patterns, one that uses the partition **LongDistanceEmployees** and another that uses the partition **LongDistanceManager**. Then configure the route pattern that uses the **LongDistanceEmployees** partition to use FAC. Complete these steps:

In the CallManager Administration window, navigate to **Call Routing > Route/Hunt > Route Pattern** and click on **Add New**. In the Route Pattern Configuration window, enter the long distance route pattern and select the **LongDistanceEmployees** partition for this route pattern.

Also select the correct Gateway or Route List along with any other desired configuration. Check **Require Forced Authorization Code** and enter the Authorization Level. The number that you specify in this field determines the minimum authorization level that is needed to successfully route a call through this route pattern. Now click **Save**.

Cisco Unified CM Administration
For Cisco Unified Communications Solutions

System ▾ Call Routing ▾ Media Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administ

Route Pattern Configuration

Save

Status
Status: Ready

Pattern Definition

Route Pattern* 408XXXXXXX

Route Partition LongDistanceEmployees

Description Long Distance Route Pattern for Employees

Numbering Plan -- Not Selected --

Route Filter < None >

MLPP Precedence* Default

Apply Call Blocking Percentage

Resource Priority Namespace Network Domain < None >

Route Class* Default

Gateway/Route List* 10.127.238.20 (Edit)

Route Option
 Route this pattern
 Block this pattern No Error

Call Classification* OffNet

External Call Control Profile < None >

Allow Device Override Provide Outside Dial Tone Allow Overlap Sending Urgent Priority

Require Forced Authorization Code
Authorization Level* 10

Require Client Matter Code

Click **Add New** in order to add the long distance route pattern that uses the **LongDistanceManager** partition.

In the Route Pattern Configuration window, enter the same long distance route pattern (as in step 2) and select the **LongDistanceManager** partition for this route pattern, as shown in the

image. Ensure that the correct Gateway or Route List is selected for this configuration. Also, this route pattern should not be configured to use FAC.

The screenshot displays the Cisco Unified CM Administration interface for Route Pattern Configuration. The breadcrumb navigation shows: System > Call Routing > Media Resources > Advanced Features > Device > Application > User Management > Bulk Ad. The main title is "Route Pattern Configuration". Below the title are icons for Save, Delete, Copy, and Add New. The "Pattern Definition" section contains the following fields:

- Route Pattern*: 408XXXXXXX
- Route Partition: LongDistanceManager
- Description: Long Distance Route Pattern for Manager
- Numbering Plan: -- Not Selected --
- Route Filter: < None >
- MLPP Precedence*: Default
- Apply Call Blocking Percentage
- Resource Priority Namespace Network Domain: < None >
- Route Class*: Default
- Gateway/Route List*: 10.127.238.20 (with an [Edit](#) link)
- Route Option:
 - Route this pattern
 - Block this pattern (No Error)
- Call Classification*: OffNet
- External Call Control Profile: < None >
- Allow Device Override
- Provide Outside Dial Tone
- Allow Overlap Sending
- Urgent Priority
- Require Forced Authorization Code
- Authorization Level*: 0
- Require Client Matter Code

- Under the IP Phone Configuration window, include the Employee IP Phone Directory Number to the **LongDistanceEmployees** partition and to the Employees CSS. Also, include the Manager IP Phone Directory Number to the **LongDistanceManager** partition and to the Manager CSS. **Note:** The CSS used by the Employee IP phones must not include the **LongDistanceManager** partition and the CSS used by the manager's IP phone must not include the **LongDistanceEmployees** partition.

Restrict Only One Phone to Use FAC

Complete these steps in order to restrict only one phone to use FAC to make long distance calls.

- Copy the route pattern configuration for that Long Distance pattern and put it in a new partition that can be only accessed by that phone.
- Create a separate Calling Search Space specific for that phone, this also includes the LD partition.
- Enable FAC for that route pattern so only the phone in question is required to enter the code.

Verify

Complete these steps in order to verify if your configurations work properly:

1. From Employee Extension 1000, call the long distance number **4085551234**. The system should play a tone that prompts for the authorization code. Once the authorization code is entered, the call is connected. **Note:** In order to immediately route the call after the user enters the code, the users can press **#** on the phone. Otherwise the call occurs after the interdigit timer expires, which equals 15 seconds by default.
2. From the Manager's Extension 1001, call the long distance number **4085551234**. The call should be connected without prompting for any authorization code.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Forced Authorization Codes Randomly Stop to Work

When you dial the number that matches a route pattern with FAC configured, you hear the tone to enter the FAC. However, when you enter the FAC, you receive a reorder tone and the call is released.

As a temporary workaround for this issue, go to the FAC Configuration page and click **Save**.