Manuals+ — User Manuals Simplified.

cisco Client Matter Codes and Forced Authorization Codes User Guide

Contents

cisco Client Matter Codes and Forced Authorization Codes

Forced Authorization Code Configuration

Save

Status

Status: Ready

Forced Authorization Code Information

Authorization Code Name* : Employees_Access

Authorization Code* : 12345

Authorization Level* : 10

Save

Client Matter Codes and Forced Authorization Codes Overview

With client matter codes (CMCs) and forced authorization codes (FACs), you can effectively manage call access and accounting. CMCs assist with call accounting and billing for clients, and FACs regulate the types of calls that certain users can place. CMCs force the user to enter a code; this action specifies that the call relates to a specific client matter. You can assign client matter codes to customers, students, or other populations for call accounting and billing purposes. FACs force the user to enter a valid authorization code that is assigned at a certain access level before the call is completed.

Client Matter Codes and Forced Authorization Codes Prerequisites

- Cisco Unified IP Phones that are running SCCP and SIP support CMC and FAC.
- The CMC and FAC tones play only on Cisco Unified IP Phones that are running SCCP or SIP; TAPI/JTAPI ports; and MGCP FXS ports.

Client Matter Codes and Forced Authorization Codes Configuration Task Flow

You can implement CMCs and FACs separately or together. For example, you may authorize users to place certain classes of calls, such as long distance calls, and also assign the class of calls to a specific client. CMC and FAC tones sound the same to the user; if you configure both codes, the feature prompts the user to enter the FAC after the first tone and enter the CMC after the second tone.

Before you begin

- Review Client Matter Codes and Forced Authorization Codes Prerequisites.

Procedure

	Command or Action	Purpose
Step 1	To Configure Client Matter Codes, complete the following subtasks: • Add Client Matter Codes, • Enable Client Matter Codes,	After you finalize the list of CMCs that you plan to use, add those codes to the database and enable the CMC feature in route patterns.
Step 2	To Configure Forced Authorization Codes, complete the following subtasks: • Add Forced Authorization Codes, • Enable Forced Authorization Codes,	After you finalize the list of FACs and authorization levels that you plan to use, add those codes to the database and enable the FAC feature in route patterns.

Configure Client Matter Codes

Procedure

	Command or Action	Purpose
Step 1	Add Client Matter Codes	Determine unique client matter codes that you want to use and add them to your system. Because the number of CMCs directly affects the time that is required for your system to start up, limit the number of CMCs to a maximum of 60,000. If you configure more CMCs than the maximum number, expect significant delays.
Step 2	Enable Client Matter Codes,	Enable client matter codes through a route pattern.

Add Client Matter Codes

Determine unique client matter codes that you want to use and add them to your system. Because the number of CMCs directly affects the time that is required for your system to start up, limit the number of CMCs to a maximum of 60,000. If you configure more CMCs than the maximum number, expect significant delays.

Procedure

- **Step 1:** From Cisco Unified CM Administration, choose Call Routing > Client Matter Codes.
- **Step 2:** Click Add New.
- **Step 3:** In the Client Matter Code field, enter a unique code of no more than 16 digits that the user will enter when placing a call.
- **Step 4:** In the Description field, enter a client name if you want to identify the client matter code.
- **Step 5:** Click Save.

Enable Client Matter Codes

Enable client matter codes through a route pattern.

Before you begin

- Add Client Matter Codes.

Procedure

- **Step 1:** From Cisco Unified CM Administration, choose Call Routing > Route/Hunt > Route Pattern.
- **Step 2:** Perform one of the following tasks:
  - To update an existing route pattern, enter search criteria, click Find, and choose a route pattern from the resulting list.
  - To create a new route pattern, click Add New.
- **Step 3:** In the Route Pattern Configuration window, check the Require Client Matter Code check box.
- **Step 4:** Click Save.

Configure Forced Authorization Codes

Procedure

	Command or Action	Purpose
Step 1	Add Forced Authorization Codes,	Determine unique forced authorization codes that you want to use and add them to your system.

	Command or Action	Purpose
Step 2	Enable Forced Authorization Codes,	Enable forced authorization codes through a route pattern.

Add Forced Authorization Codes

Use this procedure to determine unique forced authorization codes that you want to use and add them to your system. To successfully route a call, the user authorization level must be equal to or greater than the authorization level that is specified for the route pattern for the call.

- **Step 1:** From Cisco Unified CM Administration, choose Call Routing > Forced Authorization Codes.
- **Step 2:** In the Authorization Code Name field, 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.
- **Step 3:** In the Authorization Code field, enter a unique authorization code that is no more than 16 digits. Users enter this code when they place a call through a FAC-enabled route pattern.
- **Step 4:** In the Authorization Level field, enter a three-digit authorization level in the range of 0 to 255.
- **Step 5:** Click Save.

Enable Forced Authorization Codes

Use this procedure to enable forced authorization codes through a route pattern.

Procedure

- **Step 1:** From Cisco Unified CM Administration, choose Call Routing > Route/Hunt > Route Pattern.
- **Step 2:** Perform one of the following tasks:
  - Click Find, and then choose a route pattern from the resulting list to update an existing route pattern.
  - Click Add New to create a new route pattern.
- **Step 3:** In the Route Pattern Configuration window, check the Require Forced Authorization Code check box.
- **Step 4:** In the Authorization Level field, enter the authorization level value between 0 and 255. The FAC level for the user must be greater than or equal to the configured level for the call to route successfully.
- **Step 5:** Click Save.

Client Matter Codes and Forced Authorization Codes Interactions

Table 1: Client Matter Codes and Forced Authorization Codes Interactions

Feature	Interaction

CDR Analysis and Reporting (CAR)	CDR Analysis and Reporting (CAR) allows you to run reports that provide call details for client matter codes (CMCs), forced authorization codes (FACs), and authorization levels.
CTI, JTAPI, and TAPI applications	In most cases, your system can alert a CTI, JTAPI, or TAPI application that the user must enter a code during a call. When a user places a call, creates an ad hoc conference, or performs a consult transfer through a CMC- or FAC-enabled route pattern, the user must enter a code after receiving the tone.
	When a user redirects or blind transfers a call through a CMC- or FAC-enabled route pattern, the user receives no tone, so the application must send the codes to Cisco
	Unified Communications Manager. If your system receives the appropriate codes, the call connects to the intended party. If your system does not receive the appropriate codes, Cisco Unified Communications Manager sends an error to the application that indicates which code is missing.

Cisco Web Dialer	Web Dialer supports CMCs and FACs in the following ways: • A user can enter the destination number in the dial text box of the WD HTML page or SOAP request, and then manually enter the CMC or FAC on the phone. • A user can enter the destination number followed by the FAC or CMC in the dial text box of the WD HTML page or SOAP request. For example, if the destination number is 5555, the FAC is 111, and the CMC is 222, a user can make a call by dialing 5555111# (FAC), 5555222# (CMC), or 5555111222# (CMC and FAC). **Note:** WebDialer does not handle any validation for the destination number. The phone handles the required validation. • If a user does not provide a code or provides the wrong code, the call will fail. • If a user makes a call from the WebApp with a DN that contains special characters, the call goes successfully after stripping the special characters. The same rules do not work in SOAP UI.
Speed Dial and Abbreviated Speed Dial	You can use speed dial to reach destinations that require a FAC, CMC, dialing pauses, or additional digits (such as a user extension, a meeting access code, or a voicemail password). When the user presses the configured speed dial, the phone establishes the call to the destination number and sends the specified FAC, CMC, and additional digits with dialing pauses inserted.

Client Matter Codes and Forced Authorization Codes Restrictions

Table 2: Client Matter Codes and Forced Authorization Codes Restrictions

Restriction	Description
Analog gateways	H.323 analog gateways do not support CMCs or FACs because these gateways cannot play tones.
Call forwarding	Calls that are forwarded to a CMC- or FAC-enabled route pattern fail because no user is present to enter the code. When a user presses the CFwdALL softkey and enters a number that has CMC or FAC enabled on the route pattern, call forwarding fails. To minimize call-processing interruptions, test the number before you configure call forwarding. To do this, dial the intended forwarding number; if you are prompted for a code, do not configure call forwarding for that number. Advise users of this practice to reduce the number of complaints that result from forwarded calls that do not reach the intended destination.
Cisco Unified Mobility	Calls that originate from a SIP trunk, H.323 gateway, or MGCP gateway fail if they encounter a route pattern that requires CMCs or FACs and the caller is not configured with Cisco Unified Mobility.
Dial via Office callback number	The CMC and FAC feature on Cisco Mobility does not support an alternative number as its dial via office (DVO) callback number. The DVO callback number must be the number that is registered on the **Mobility Identity** window.
Failover calls	CMCs and FACs do not work with failover calls.
Hearing-impaired users	After dialing the phone number, hearing-impaired users should wait one or two seconds before entering the authorization or client matter code.
Localization	Cisco does not localize CMCs or FACs. The CMC and FAC features use the same default tone for any locale that is supported with Cisco Unified Communications Manager. **Note** For Cisco Mobility, CMCs and FACs are localized.
Overlap sending	The CMC and FAC features do not support overlap sending because Cisco Unified Communications Manager cannot determine when to prompt the user for the code. If you check the **Require Forced Authorization Code** or the **Require Client Matter Code** check box in the **Route Pattern Configuration** window, the **Allow Overlap Sending** check box is automatically unchecked and vice-versa.
Speed-dial buttons	You cannot configure CMCs or FACs for speed-dial buttons. You must enter the code when the system prompts you to do so.

Documents / Resources

cisco Client Matter Codes and Forced Authorization Codes [pdf] User Guide
Client Matter Codes and Forced Authorization Codes, Client Matter Codes, Forced Authorization Codes, Authorization Codes

cisco Client Matter Codes and Forced Authorization Codes [pdf] User Guide
Client Matter Codes and Forced Authorization Codes, Client Matter Codes, Forced Authorization Codes, Authorization Codes, Codes

Manuals+,