Client Matter Codes and Forced Authorization Codes

This chapter provides information about Forced Authorization Codes (FAC) and Client Matter Codes (CMC) which allow you to manage call access and accounting. CMC assists with call accounting and billing for billable clients, while Forced Authorization Codes regulate the types of calls that certain users can place.

Client matter codes force the user to enter a code to specify 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. The Forced Authorization Codes feature forces the user to enter a valid authorization code before the call completes.

The CMC and FAC features require that you make changes to route patterns and update your dial plan documents to reflect that you enabled or disabled FAC and/or CMC for each route pattern.

Configure Client Matter Codes and Forced Authorization Codes

Forced Authorization Codes (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 Forced Authorization Codes regulate the types of calls that certain users can place.

Client matter codes force the user to enter a code to specify 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. The Forced Authorization Codes feature forces the user to enter a valid authorization code before the call completes.

Perform the following steps to configure client matter codes and forced authorization codes.

Procedure

Step 1 Review feature limitations.

Step 2 Design and document the system; for example, document a list of client matters that you want to track.

Step 3 Insert the codes by using Cisco Unified Communications Manager Administration or by using Bulk Administration Tool (BAT).

Tip Consider using BAT for small or large batches of codes; the comma separated values (CSV) file in BAT can serve as a blueprint for the codes, corresponding names, corresponding levels, and so on.

Step 4 To enable FAC or CMC, add or update route patterns in Cisco Unified Communications Manager Administration.

Step 5 Update your dial plan documents or keep a printout of the BAT CSV file with your dial plan documents.

Step 6 Provide all necessary information, for example, codes, to users and explain how the features works.

Related Topics

Client Matter Codes and Forced Authorization Codes, on page 1
Interactions and Restrictions, on page 4
Client Matter Codes, on page 2
Forced Authorization Codes, on page 3
Configure Client Matter Codes, on page 6
Configure Forced Authorization Codes, on page 8
Enable Client Matter Codes, on page 7
Enable Forced Authorization Codes, on page 9
Provide Information to Users, on page 10

Client Matter Codes

To use the Client Matter Codes feature, users must enter a client matter code to reach certain dialed numbers. You enable or disable CMC through route patterns, and you can configure multiple client matter codes. When a user dials a number that is routed through a CMC-enabled route pattern, a tone prompts the user for the client matter code. When the user enters a valid CMC, the call occurs; if the user enters an invalid code, reorder occurs. The CMC writes to the CDR, so you can collect the information by using CDR Analysis and Reporting (CAR), which generates reports for client accounting and billing.

The Client Matter Codes feature benefits law offices, accounting firms, consulting firms, and other businesses or organizations where tracking the length of the call for each client is required. Before you implement CMC, obtain a a list of all clients, groups, individuals, parties, and so on that you plan to track through CMC. Determine whether you can assign the codes consecutively, arbitrarily, or whether your organization requires a special code structure; for example, using existing client account numbers for CMC. For each client (or group, individual, and so on) that you want to track, you must add a client matter code in the Client Matter Code Configuration window of Cisco Unified Communications Manager Administration. Then, in Cisco Unified Communications Manager Administration, you must enable CMC for new or existing route patterns. After you configure CMC, make sure that you update your dial plan documents to indicate the CMC-enabled route patterns.

Tip If you want users to enter a CMC for most calls, consider enabling CMC for most or all route patterns in the dial plan. In this situation, users must obtain CMCs and a code, such as 555, for calls that do not relate to clients. All calls automatically prompt the users for a CMC, and the users do not have to invoke CMC or dial special digits. For example, a user dials a phone number, and the system prompts the user for the client code; if the call relates to a client matter, the user enters the appropriate CMC; if the call does not relate to a client, the user enters 555.

Tip If only a select number of users must enter a CMC, consider creating a new route pattern specifically for CMC; for example, use 8.@, which causes the system to prompt users for the client code when the phone number that is entered starts with the number 8. Implementing CMC in this manner provides a means to invoke CMC and allows the existing dial plan to remain intact. For example, for client-related calls, a user may dial 8-214-555-1234 to invoke CMC; for general calls that are not related to clients, the users just dial 214-555-1234 as usual.

Forced Authorization Codes

When you enable FAC through route patterns in Cisco Unified Communications Manager Administration, users must enter an authorization code to reach the intended recipient of the call. When a user dials a number that is routed through a FAC-enabled route pattern, the system plays a tone that prompts for the authorization code.

In Cisco Unified Communications Manager Administration, you can configure various levels of authorization. If the user authorization code does not meet or exceed the level of authorization that is specified to route the dialed number, the user receives a reorder tone. If the authorization is accepted, the call occurs. The name of the authorization writes to call detail records (CDRs), so you can organize the information by using CDR Analysis and Reporting (CAR), which generates reports for accounting and billing.

You can use FAC for colleges, universities, or any business or organization when limiting access to specific classes of calls proves beneficial. Likewise, when you assign unique authorization codes, you can determine which users placed calls. For each user, you specify an authorization code, then enable FAC for relevant route patterns by selecting the appropriate check box and specifying the minimum authorization level for calls through that route pattern. After you update the route patterns in Cisco Unified Communications Manager Administration, update your dial plan documents to define the FAC-enabled route patterns and configured authorization level.

To implement FAC, you must devise a list of authorization levels and corresponding descriptions to define the levels. You must specify authorization levels in the range of 0 to 255. Cisco allows authorization levels to be arbitrary, so you define what the numbers mean for your organization. Before you define the levels, review the following considerations, which represent examples or levels that you can configure for your system:

- Configure an authorization level of 10 for interstate long-distance calls in North America.
- Because intrastate calls often cost more than interstate calls, configure an authorization level of 20 for intrastate long-distance calls in North America.
- Configure an authorization level of 30 for international calls.

Tip Incrementing authorization levels by 10 establishes a structure that provides scalability when you need to add more authorization codes.

Interactions and Restrictions

You can implement client matter codes (CMC) and forced authorization codes (FAC) 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. If you implement CMC and FAC together as described in the previous example, the user dials a number, enters the user-specific authorization code when prompted to do so, and then enters the client matter code at the next prompt. CMC and FAC tones sound the same to the user, so the feature tells the user to enter the authorization code after the first tone and enter the CMC after the second tone.

Cisco Unified Communications Manager provides redundancy, which handles the normal processes that are in place for Cisco Unified Communications Manager.

The CMC and FAC features work with all Cisco Unified IP Phones running SCCP and SIP, Cisco Mobility, and gateways.

Before you implement CMC and FAC, review the following restrictions:

- Because the number of CMCs directly impacts the time that is required for Cisco Unified Communications Manager to start up, you should limit the number of CMCs to 60,000. If you configure more CMCs than that, expect significant delays. For example, a system with 400,000 CMCs requires 1 hour to start up; a system with 1 million CMCs requires 4 hours to start up.
- After dialing the phone number, hearing-impaired users should wait 1 or 2 seconds before entering the authorization or client matter code.
- Calls that are forwarded to an FAC- or CMC-enabled route pattern fail because no user is present to enter the code. This limitation applies to call forwarding that is configured in Cisco Unified Communications Manager Administration or the Cisco Unified Communications Self Care Portal. You can configure call forwarding, but all calls that are forwarded to an FAC- or CMC-enabled route pattern results in reorder. When a user presses the CFwdALL softkey and enters a number that has FAC or CMC enabled on the route pattern, the user receives reorder, and call forwarding fails.

  You cannot prevent the configuration of call forwarding to an FAC- or CMC-enabled route pattern; forwarded calls that use these route patterns drop because no code is entered. 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 does not localize FAC or CMC. 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, FAC and CMC are localized.

- The CMC and FAC features do not support overlap sending because the 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 becomes disabled. If you check the Allow Overlap Sending check box, the Require Forced Authorization Code and the Require Client Matter Code check boxes become disabled.

- The CMC and FAC feature on Cisco Mobility does not support an alternative number as its DVO callback number. The DVO callback number has to be the number registered in the MI (Mobility Identity) page.

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

- Calls that originate from a SIP trunk, H.323, or MGCP gateway fail if they encounter a route pattern that requires FAC or CMC and the caller is not configured as Cisco Unified Mobility.

- H.323 analog gateways do not support FAC or CMC because these gateways cannot play tones.

- Restrictions apply to CTI devices that support FAC and CMC. For more information, see the Use FAC/CMC with CTI JTAPI and TAPI Applications, on page 5.

- Cisco Web Dialer does not support FAC or CMC.

- Cisco IP softphone cannot play tones; however, after a Cisco IP softphone user dials a directory number, the user can use CMC and FAC by waiting 1 or 2 seconds before entering the code.

- If you do not append the FAC or CMC with #, the system waits for the T302 timer to extend the call.

- When you press the Redial softkey on the phone, you must enter the authorization code or CMC when the number that you dialed is routed through an FAC- or CMC-enabled route pattern. Cisco does not save the code that you entered for the previous call.

- You cannot configure authorization code or CMC for speed-dial buttons. You must enter the code when the system prompts you to do so.

- FAC and CMC do not work with failover calls.

Use the Cisco Bulk Administration Tool

You can use Bulk Administration Tool (BAT) to insert, update, and delete CMC and FAC. For more information on how to perform these tasks, see the Cisco Unified Communications Manager Bulk Administration Guide that is compatible with this release of Cisco Unified Communications Manager.

Use CDR Analysis and Reporting

CDR Analysis and Reporting (CAR) allows you to run reports that provide call details for authorization code names, authorization levels, and CMCs. For information on how to generate reports in CAR, see the Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide.

Use FAC/CMC with CTI JTAPI and TAPI Applications

In most cases, Cisco Unified Communications Manager 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 FAC- or CMC-enabled route pattern, the user must enter a code after receiving the tone. When a user redirects or blind transfers a call through a FAC- or CMC-enabled route pattern, the user receives no tone, so the application must send the codes to Cisco Unified Communications Manager. If Cisco Unified Communications Manager receives the appropriate codes, the call connects to the intended party. If Cisco Unified Communications Manager does not receive the appropriate codes, Cisco Unified Communications Manager sends an error to the application that indicates which code is missing.

Cisco Unified Communications Manager does not support call forwarding through FAC- or CMC-enabled route patterns. For more information, see the Interactions and Restrictions, on page 4.

System Requirements

The minimum requirements for CMC and FAC specify that every server in the cluster must have Cisco Unified Communications Manager Release 5.0 or a later version.

Cisco Unified IP Phones that are running SCCP and SIP support CMC and FAC. The following Cisco Unified IP Phones (SCCP) support CMC and FAC:

- Cisco Unified IP Phones 6900 Series
- Cisco Unified IP Phones 7900 Series

Installation of CMC and FAC

The CMC and FAC features install automatically when you install Cisco Unified Communications Manager. To make these features work in your Cisco Unified Communications Manager network, you must perform the tasks that are described in the Configure Client Matter Codes, on page 6.

Configure Client Matter Codes

This section provides information to configure and enable client matter codes. After you obtain the list of CMCs that you plan to use, you add those codes to the database and enable the CMC feature for route patterns.

Tip Before you configure client matter codes, review the configuration summary task for client matter and forced authorization codes.

Related Topics

Configure Client Matter Codes and Forced Authorization Codes, on page 1

CMC Configuration

In Cisco Unified Communications Manager Administration, use the **Call Routing** > **Client Matter Codes** menu path to configure client matter codes.

Client matter codes (CMC) allow you to manage call access and accounting. CMC assists with call accounting and billing for billable clients by forcing the user to enter a code to specify 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.

Tips About Configuring Client Matter Codes

You enter CMCs in Cisco Unified Communications Manager Administration or through the Cisco Bulk Administration Tool (BAT). If you use BAT, the BAT comma separated values (CSV) file provides a record of CMCs and client names. After you configure CMC, make sure that you update your dial plan documents or keep a printout of the BAT CSV file with your dial plan documents.

After you add all CMCs, see the Enable Client Matter Codes, on page 7.

Using the GUI

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the Enable Client Matter Codes, on page 7 section in the Cisco Unified Communications Manager Administration Guide and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Configuration Settings Table

Use the following table as a guide when you configure client matter codes. For more information on client matter codes and forced authorization codes, see the Client Matter Codes and Forced Authorization Codes, on page 1.

This table describes the client matter codes configuration settings. Use this table in conjunction with the Configure Client Matter Codes, on page 6.

Table 1: Configuration Settings for Adding a CMC

Setting	Description
Client Matter Code	Enter a unique code of no more than 16 digits that the user will enter when placing a call. The CMC displays in the CDRs for calls that use this code.
Description	This optional field associates a client code with a client. The description can include up to 50 characters in any language, but it cannot include double-quotes ("), percentage sign (%), ampersand (&), back-slash (\), angle brackets (<>), or either type of brackets ([ ] { }).

Enable Client Matter Codes

Perform the following steps to enable CMCs on route patterns:

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Call Routing** > **Route/Hunt** > **Route Pattern**.

Step 2 Perform one of the following tasks:

a) To update an existing route pattern, enter search criteria in the Find and List Route Pattern window, as described in the Cisco Unified Communications Manager Administration Guide.

b) To add a new route pattern, see the Cisco Unified Communications Manager Administration Guide.

Step 3 In the Route Pattern Configuration window, check the Require Client Matter Code check box.

Step 4 Perform one of the following tasks:

a) If you updated the route pattern, click Save.

b) If you added a new route pattern, click Save.

Step 5 Update an existing route pattern, or add a new route pattern for all route patterns that require a client matter code.

Step 6 After you complete the route pattern configuration, see the Provide Information to Users, on page 10.

Configure Forced Authorization Codes

This section provides information to configure and enable forced authorization codes.

Tip Before you configure forced authorization codes, review the configuration summary task for client matter and forced authorization codes..

After you design your FAC implementation, you enter authorization codes either in Cisco Unified Communications Manager Administration or through the Cisco Bulk Administration Tool (BAT). Consider using BAT for large batches of authorization codes; the comma separated values (CSV) file in BAT serves as a blueprint for authorization codes, corresponding names, and corresponding levels.

Note For future reference, make sure that you update your dial plan documents or keep a printout of the CSV file with your dial plan documents.

Related Topics

Configure Client Matter Codes and Forced Authorization Codes, on page 1

FAC Configuration

In Cisco Unified Communications Manager Administration, use the **Routing** > **Forced Authorization Codes** menu path to configure forced authorization codes.

Forced Authorization Codes (FAC) allow you to manage call access and accounting by regulating the types of calls that certain users can place. The Forced Authorization Codes feature forces the user to enter a valid authorization code before the call completes.

For instructions on how to use the Cisco Unified Communications Manager Administration Graphical User Interface (GUI) to find, delete, configure, or copy records, see the *Cisco Unified Communications Manager Administration Guide* and its subsections, which explain how to use the GUI and detail the functions of the buttons and icons.

Tip After you add all authorization codes, see the topic to enable forced authorization codes.

Related Topics

Enable Forced Authorization Codes, on page 9
FAC Configuration Settings, on page 9

FAC Configuration Settings

The following table describes the FAC configuration settings.

Table 2: Configuration Settings for FAC

Setting	Description
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; this name displays in the CDRs for calls that use this code.
Authorization Code	Enter a unique authorization code that is no more than 16 digits. 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. 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.

Related Topics

Client Matter Codes and Forced Authorization Codes, on page 1
Configure Forced Authorization Codes, on page 8

Enable Forced Authorization Codes

Perform the following steps to enable FACs for route patterns:

Procedure

Step 1 In Cisco Unified Communications Manager Administration, choose **Call Routing** > **Route/Hunt** > **Route Pattern**.

Step 2 Perform one of the following tasks:

a) To update an existing route pattern, enter search criteria in the Find and List Route Pattern window, as described in the Cisco Unified Communications Manager Administration Guide.

b) To add a new route pattern, see the Cisco Unified Communications Manager Administration Guide.

Step 3 In the Route Pattern Configuration window, check the Require Forced Authorization Code check box.

Step 4 Click **Save.**

Tip Even if you do not check the Require Forced Authorization Code check box, you can specify the authorization level because the database stores the number that you specify.

Step 5 Repeat for all route patterns that require an authorization code.

Step 6 After you complete the route pattern configuration, see the Provide Information to Users, on page 10.

Provide Information to Users

After you configure the feature(s), communicate the following information to your users:

- Inform users about restrictions that are described in Interactions and Restrictions, on page 4.
- Provide users with all necessary information to use the features; for example, authorization code, authorization level, client matter code, and so on. Inform users that dialing a number produces a tone that prompts for the codes.
- For FAC, the system attributes calls that are placed with the user authorization code to the user or the user department. Advise users to memorize the authorization code or to keep a record of it in a secure location.
- Advise users of the types of calls that users can place; before a user notifies a phone administrator about a problem, users should hang up and retry the dialed number and code.
- Inform users that they can start entering the code before the tone completes.
- 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 (T302) expires; that is, after 15 seconds by default.
- The phone plays a reorder tone when the user enters an invalid code. If users misdial the code, the user must hang up and try the call again. If the reorder tone persists, users should notify the phone or system administrator that a problem may exist with the code.