CHAPTER 5

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.

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.

This chapter contains information on the following topics:

Introducing 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 CallManager Administration. Then, in Cisco CallManager 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.

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.

Introducing Forced Authorization Codes

When you enable FAC through route patterns in Cisco CallManager 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 CallManager 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 CallManager 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 CMC and 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 CallManager provides redundancy, which handle the normal processes that are in place for Cisco CallManager.

The CMC and FAC features work with all Cisco IP Phone models and MGCP-controlled analog gateways.

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

- 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 a 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 CallManager Administration or the Cisco CallManager User Options Pages. You can configure call forwarding, but all calls that are forwarded to a 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 a 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 CallManager.

- The CMC and FAC features do not support overlap sending because the Cisco CallManager 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 on 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 FAC and CMC tones can only be played on SCCP phones, TAPI/JTAPI ports, and MGCP FXS ports.
- 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 "Using FAC/CMC with CTI, JTAPI, and TAPI Applications" section on page 5-4.
- Cisco WebDialer does not support FAC or CMC.
- Cisco IP SoftPhone cannot play tones; however, after a Cisco 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 a 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.

Using the Cisco Bulk Administration Tool (BAT)

You can use BAT to insert, update, and delete CMC and FAC. For more information on how to perform these tasks, refer to the *Cisco CallManager Bulk Administration Guide* that is compatible with this release of Cisco CallManager.

Using CDR Analysis and Reporting (CAR)

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, refer to the *Cisco CallManager Serviceability Administration Guide* and the *Cisco CallManager Serviceability System Guide*.

Using FAC/CMC with CTI, JTAPI, and TAPI Applications

In most cases, Cisco CallManager 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 CallManager. If Cisco CallManager receives the appropriate codes, the call connects to the intended party. If Cisco CallManager does not receive the appropriate codes, Cisco CallManager sends an error to the application that indicates which code is missing.

Cisco CallManager does not support call forwarding through FAC- or CMC-enabled route patterns. For more information, see the "Interactions and Restrictions" section on page 5-3.

System Requirements

The minimum requirements for CMC and FAC specify that every server in the cluster must have Cisco CallManager 5.0.

Installation of CMC and FAC

The CMC and FAC features install automatically when you install Cisco CallManager. To make these features work in your Cisco CallManager network, you must perform the tasks that are described in the "CMC and FAC Configuration Checklist" section on page 5-5.

CMC and FAC Configuration Checklist

Use Table 5-1 as a guide when you configure CMC and FAC.

Table 5-1 Cisco CMC and FAC Configuration Checklist

Configuration Steps		Related Procedures and Topics
Step 1	Review feature limitations.	Interactions and Restrictions, page 5-3
Step 2	Design and document the system; for example, document a list of client matters that you want to track.	Introducing Client Matter Codes, page 5-2 Introducing Forced Authorization Codes, page 5-2
Step 3	Insert the codes by using Cisco CallManager Administration or by using Cisco 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.	Client Matter Codes Configuration, page 5-6 Forced Authorization Codes Configuration, page 5-9
Step 4	To enable FAC or CMC, add or update route patterns in Cisco CallManager Administration.	Enabling Client Matter Codes For Route Patterns, page 5-8 Enabling Forced Authorization Codes for Route Patterns, page 5-12
Step 5	Update your dial plan documents or keep a printout of the BAT CSV file with your dial plan documents.	Refer to your dial plan documents.
Step 6	Provide all necessary information, for example, codes, to users and explain how the features works.	Providing Information to Users, page 5-13

Client Matter Codes Configuration

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.

This section contains the information on the following topics:

Finding Client Matter Codes

Cisco CallManager lets you locate specific CMCs on the basis of specific criteria. To locate CMCs, perform the following procedure:

Note During your work in a browser session, Cisco CallManager Administration retains your search preferences. If you navigate to other menu items and return to this menu item, Cisco CallManager Administration retains your search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Call Routing > Client Matter Codes**.

The Find and List window displays.

Tip To find all CMCs that are registered in the database, click **Find** without entering any search text.

Step 2 From the first Find Client Matter Codes where drop-down list box, choose one option; for example, Client Matter Code or Description.

Note The criterion that you choose in the first drop-down list box specifies how the list that your search generates will be sorted. For example, if you choose Client Matter Code, the Client Matter Code column displays as the left column of the results list.

Step 3 From the second Client Matter Codes where drop-down list box, choose one option; for example, begins with, contains, ends with, is exactly, and so on.

Step 4 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.

Note You can delete multiple client matter codes from the Find and List window by checking the check boxes next to the appropriate CMC and clicking **Delete Selected**. You can delete all CMC in the window by checking the check box in the Matching records title bar and clicking **Delete Selected**.

Step 5 From the list of records, click the CMC that you want to display.

The window displays the CMC that you choose.

Additional Information

See the "Related Topics" section on page 5-13.

Configuring Client Matter Codes

You enter CMCs in Cisco CallManager 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.

To add or update CMCs in Cisco CallManager Administration, perform the following procedure:

Procedure

Step 1 Perform one of the following tasks:

- To add CMCs, choose **Call Routing > Client Matter Codes** and click **Add New**. Continue with Step 2.
- To update CMCs, locate the CMC that you want to update, as described in the "Finding Client Matter Codes" section on page 5-6 and continue with Step 2.

Step 2 Enter the appropriate settings as described in Table 5-2.

Step 3 Click **Save**.

Step 4 After you add all CMCs, see the "Enabling Client Matter Codes For Route Patterns" section on page 5-8.

Additional Information

See the "Related Topics" section on page 5-13.

Deleting Client Matter Codes

To delete a CMC in Cisco CallManager Administration, perform the following procedure:

Procedure

Step 1 Locate the CMC that you want to delete, as described in the "Finding Client Matter Codes" section on page 5-6.

Step 2 After the Client Code Matter Configuration window displays, click **Delete**.

Step 3 To continue with the deletion, click **OK**.

Additional Information

See the "Related Topics" section on page 5-13.

CMC Configuration Settings

Use Table 5-2 in conjunction with the "Configuring Client Matter Codes" section on page 5-7.

Table 5-2 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	Enter a name of no more than 50 characters. This optional field associates a client code with a client.

Additional Information

See the "Related Topics" section on page 5-13.

Enabling Client Matter Codes For Route Patterns

Perform the following steps to enable CMCs on route patterns:

Procedure

Step 1 In Cisco CallManager 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 in the Find and List Route Pattern window, as described in "Route Pattern Configuration" in the *Cisco CallManager Administration Guide*.
- To add a new route pattern, refer to "Route Pattern Configuration" in the *Cisco CallManager 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:

- If you updated the route pattern, click **Save**.
- If you added a new route pattern, click **Save**.

Step 5 Repeat Step 2 through Step 4 for all route patterns that require a client matter code.

Step 6 After you complete the route pattern configuration, see the "Providing Information to Users" section on page 5-13.

Additional Information

See the "Related Topics" section on page 5-13.

Forced Authorization Codes Configuration

To configure FACs, see the following sections:

Finding Forced Authorization Codes

Cisco CallManager allows you to locate specific FACs on the basis of specific criteria. To locate FACs, perform the following procedure:

Note During your work in a browser session, Cisco CallManager Administration retains your search preferences. If you navigate to other menu items and return to this menu item, Cisco CallManager Administration retains your search preferences until you modify your search or close the browser.

Procedure

Step 1 Choose **Call Routing > Forced Authorization Codes**.

The Find and List window displays.

Tip To find all authorization codes that are registered in the database, click **Find** without entering any search text.

Step 2 From the first Find Authorization Codes where drop-down list box, choose one option; for example, Authorization Code Name, Authorization Code, or Authorization Code Level.

Note The criterion that you choose in the first drop-down list box specifies how the list that your search generates will be sorted. For example, if you choose Authorization Code Name, the Authorization Code Name column displays as the left column of the results list.

Step 3 From the second Find Authorization Codes where drop-down list box, choose one option; for example, begins with, contains, ends with, is exactly, and so on.

Step 4 Specify the appropriate search text, if applicable, and click **Find**. You can also specify how many items per page to display.

Note You can delete multiple authorization codes from the Find and List window by checking the check boxes next to the appropriate FAC and clicking **Delete Selected**. You can delete all FAC in the window by checking the check box in the Matching records title bar and clicking **Delete Selected**.

Step 5 From the list of records, click the authorization code that you want to display.

The window displays the FAC that you choose.

Additional Information

See the "Related Topics" section on page 5-13.

Configuring Forced Authorization Codes

After you design your FAC implementation, you enter authorization codes either in Cisco CallManager 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.

To add a small number of authorization codes in Cisco CallManager Administration, perform the steps in the following procedure.

Procedure

Step 1 In Cisco CallManager Administration, choose **Call Routing > Forced Authorization Codes**.

Step 2 Perform one of the following tasks:

- To add a new FAC, click **Add New**.
- To update an FAC, locate the authorization code that you want to update as described in the "Finding Forced Authorization Codes" section on page 5-9.

Step 3 Using the configuration settings in Table 5-3, configure the authorization codes.

Step 4 Click **Save**.

Note After you add all authorization codes, see the "Enabling Forced Authorization Codes for Route Patterns" section on page 5-12.

Additional Information

See the "Related Topics" section on page 5-13.

Deleting Forced Authorization Codes

To delete a FAC, perform the following procedure:

Procedure

Step 1 Locate the authorization code that you want to delete, as described in the "Finding Forced Authorization Codes" section on page 5-9.

Step 2 After the Forced Authorization Code Configuration window displays, click **Delete**.

Step 3 To continue with the deletion, click **OK**.

Additional Information

See the "Related Topics" section on page 5-13.

FAC Configuration Settings

Use Table 5-3 in conjunction with the "Configuring Forced Authorization Codes" section on page 5-10.

For more information, see the "Related Topics" section on page 5-13.

Table 5-3 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.

Table 5-3 Configuration Settings for FAC (continued)

Setting	Description
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.

Additional Information

See the "Related Topics" section on page 5-13.

Enabling Forced Authorization Codes for Route Patterns

Perform the following steps to enable FACs for route patterns:

Procedure

Step 1 In Cisco CallManager 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 in the Find and List Route Pattern window, as described in "Route Pattern Configuration" in the *Cisco CallManager Administration Guide*.
- To add a new route pattern, refer to "Route Pattern Configuration" in the *Cisco CallManager 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 Step 2 through Step 4 for all route patterns that require an authorization code.

Step 6 After you complete the route pattern configuration, see the "Providing Information to Users" section on page 5-13.

Additional Information

See the "Related Topics" section on page 5-13.

Providing 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" section on page 5-3.
- 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.

Additional Information

See the "Related Topics" section on page 5-13.

Related Topics

- Route Pattern Configuration, *Cisco CallManager Administration Guide*
- Understanding Route Plans, *Cisco CallManager System Guide*
- Interactions and Restrictions, page 5-3
- System Requirements, page 5-5

Forced Authorization Codes

- Introducing Forced Authorization Codes, page 5-2
- CMC and FAC Configuration Checklist, page 5-5
- Finding Forced Authorization Codes, page 5-9
- Configuring Forced Authorization Codes, page 5-10
- Deleting Forced Authorization Codes, page 5-11
- FAC Configuration Settings, page 5-11
- Enabling Forced Authorization Codes for Route Patterns, page 5-12

Client Matter Codes

- Introducing Client Matter Codes, page 5-2
- CMC and FAC Configuration Checklist, page 5-5

- Finding Client Matter Codes, page 5-6
- Configuring Client Matter Codes, page 5-7
- Deleting Client Matter Codes, page 5-8
- CMC Configuration Settings, page 5-8
- Enabling Client Matter Codes For Route Patterns, page 5-8

Additional Cisco Documentation

- *Cisco CallManager Bulk Administration Guide*
- *Cisco CallManager Administration Guide*
- *Cisco CallManager Serviceability System Guide*
- *Cisco CallManager Serviceability Administration Guide*