CHAPTER 5

Client Matter Codes と Forced Authorization Codes

Forced Authorization Codes（FAC）と Client Matter Codes（CMC）を使用すると、コールへのアクセスとアカウンティングを管理できます。CMC は、課金可能なクライアントに対するコール アカウンティングと課金を支援し、Forced Authorization Codes は特定のユーザが発信できるコールのタイプを規定します。

Client Matter Codes を使用すると、コールが特定のクライアント マターに関連していることを示すコードを入力するように強制されます。Client Matter Code（CMC; クライアント マター コード）は、コール アカウンティングや課金を目的として、顧客や学生、またはその他の個人に対して割り当てることができます。Forced Authorization Codes 機能を使用すると、コールを完了する前に有効な認証コードを入力するように強制されます。

CMC 機能と FAC 機能を使用するには、ルート パターンを変更し、各ルート パターンに対する FAC や CMC の有効化または無効化を反映するようにダイヤル プラン ドキュメントを更新する必要があります。

この章は、次の内容で構成されています。

Client Matter Codes の概要

Client Matter Codes 機能を使用する場合、ユーザはクライアント マター コードを入力して、特定のダイヤルされた番号に接続する必要があります。ルート パターンを使用して CMC を有効または無効にし、複数のクライアント マター コードを設定できます。CMC 対応のルート パターンを使用してルーティングされる番号をダイヤルすると、ユーザはトーンによってクライアント マター コードの入力を求められます。ユーザが有効な CMC を入力すると、コールが開始されます。ユーザが無効なコードを入力すると、リオーダーが発生します。CMC は CDR に書き込みを行うため、CAR（CDR Analysis and Reporting）を使用して情報を収集できます。CAR はクライアントのアカウンティングと料金請求のレポートを生成します。

Client Matter Codes 機能は、各クライアントのコールの長さを追跡する必要がある法律事務所、会計事務所、コンサルティング会社、その他の企業や組織などで役立ちます。CMC を実装する前に、CMC を通して追跡するクライアント グループ、個人、集団などのすべてのリストを入手しておく必要があります。コードを連続して割り当てるか、任意の順番で割り当てるか、または既存のクライアント番号を CMC に使用するかなど、特定のコード構造が必要であるかどうかを決定します。追跡する各クライアント（またはグループ、個人など）には、Cisco CallManager Administration の Client Matter Code Configuration ウィンドウでクライアント マター コードを追加する必要があります。次に、Cisco CallManager Administration で、新しいルート パターンまたは既存のルート パターンに対して CMC を有効にします。CMC の設定が完了したら、CMC 対応のルート パターンを指定するようにダイヤル プランのドキュメントを更新したことを確認します。

ヒント　ほとんどのコールでユーザが CMC を入力するように設定する場合は、ダイヤル プランのほとんどまたはすべてのルート パターンで、CMC を有効にすることを考慮してください。このような場合、ユーザはクライアントに関連していないコールに関しては、CMC と コードを 1 つ（555 など）取得する必要があります。すべてのコールが自動的にユーザに対して CMC の入力を求めます。ユーザは、CMC を起動したり、特別な数字をダイヤルする必要はありません。たとえば、ユーザが電話番号をダイヤルすると、システムはユーザに対してクライアント コードの入力を求めます。クライアントの事柄に関連するコールの場合、ユーザは適切な CMC を入力します。コールがクライアントに無関係な場合、ユーザは 555 を入力します。

選択した番号のユーザだけが CMC を入力する場合は、たとえば、8.@ を使用するなど、CMC 専用のルート パターンを新しく作成することを考慮してください。このようなパターンを作成すると、ユーザが 8 で始まる電話番号を入力した場合だけ、システムはクライアント コードの入力を求めます。このような方法で CMC を実装すると、CMC を起動する手段を提供しながら、既存のダイヤル プランをそのまま残すことができます。たとえば、クライアントに関連するコールでは、ユーザは 8-214-555-1234 をダイヤルして、CMC を起動します。クライアントに関連しない一般的なコールでは、ユーザは通常通り、214-555-1234 だけをダイヤルします。

Forced Authorization Codes の概要

Cisco CallManager Administration のルート パターンを使用して FAC を有効にする場合は、意図したコールの受信者に接続するために、認証コードを入力する必要があります。ユーザが FAC 対応のルート パターンを使用してルーティングされる番号をダイヤルすると、システムは認証コードの入力を求めるトーンを再生します。

Cisco CallManager Administration では、様々なレベルの認証を設定できます。ユーザ認証コードが、ダイヤルした番号へのルーティングに指定された認証のレベルに一致していないか、または超えている場合、ユーザにはリオーダー音が聞こえます。認証が受け入れられると、コールが開始されます。認証の名前は CDR（Call Detail Record）に書き込みを行うため、CAR（CDR Analysis and Reporting）を使用して情報を編成できます。CAR はアカウンティングと料金請求のレポートを生成します。

FAC は、単科大学や総合大学など、特定のクラスのコールへのアクセスを制限することで利点を得られるさまざまな組織で使用できます。同様に、一意の認証コードを割り当てることによって、どのユーザがコールを発信したかを判別できます。各ユーザに認証コードを指定し、適切な チェックボックスをオンにして、関連するルート パターンの FAC を有効にし、そのルート パターンを使用したコールに最小限の認証レベルを指定します。Cisco CallManager Administration のルート パターンを更新した後、ダイヤル プランのドキュメントを更新して、FAC 対応のルート パターンを定義し、認証レベルを設定します。

FAC を実装するには、認証レベルのリストと対応する説明を作成して、レベルを定義する必要があります。認証レベルは 0 ～ 255 の範囲で指定する必要があります。シスコでは、任意の認証レベルを使用することができるため、組織にとって意味のある番号を定義できます。レベルを定義する前に、システムに対して設定できる例またはレベルを示した次の事項を検討してください。

- 北米での州間の長距離電話に認証レベル 10 を設定する。
- 州内のコールは州間のコールよりもコストがかかることがあるため、北米での州内の長距離電話に認証レベル 20 を設定する。
- 国際電話に認証レベル 30 を設定する。

ヒント　認証レベルを 10 ずつ増加することで、より多くの認証コードを追加する必要がある場合に備えたスケーラビリティのある構造を確立できます。

インタラクションおよび制限事項

CMC と FAC は同時に実装することも、別々に実装することもできます。たとえば、ユーザに対し、長距離電話などの特定のクラスのコールをかけることを許可するとともに、特定のクライアントへのコールのクラスを割り当てるとします。前の例で示したように CMC と FAC を同時に実装した場合、ユーザは番号をダイヤルし、プロンプトが示されたらユーザ固有の認証コードを入力して、次のプロンプトでクライアント マター コードを入力します。CMC と FAC のトーンはユーザには同じ音に聞こえるため、これらの機能では、最初のトーンの後で認証コードを、2 番目のトーンの後で CMC を入力するようユーザに指示します。

Cisco CallManager が提供する冗長性は、Cisco CallManager で実行される通常のプロセスを処理します。

CMC 機能と FAC 機能は、すべての Cisco IP Phone モデルと MGCP 制御によるアナログ ゲートウェイで動作します。

CMC および FAC を実装する前に、次の制限事項を確認してください。

- 電話番号をダイヤルした後、聴覚に障害のあるユーザは、認証コードまたはクライアント マター コードを入力する前に 1 ～ 2 秒待つ必要があります。
- FAC 対応ルート パターンまたは CMC 対応ルート パターンに転送されるコールは、コードを入力するユーザがいないため失敗します。この制限事項は、Cisco CallManager Administration または Cisco CallManager User Options ページで設定されたコールの転送に適用されます。コールの転送を設定することはできますが、FAC 対応ルート パターンまたは CMC 対応ルート パターンに転送されたすべてのコールはリオーダーになります。ユーザが CFwdALL ソフトキーを押し、FAC または CMC が有効になっているルート パターンの番号を入力すると、ユーザはリオーダーを受信し、コールの転送は失敗します。

FAC または CMC が有効なルート パターンにコールが転送されるような設定を防止することはできません。コードが入力されないため、これらのルート パターンを使用して転送されたコールは切断されます。コール処理割り込みを最小限にするには、コールの転送を設定する前に番号をテストします。これを行うには、転送先の番号をダイヤルします。コードを入力するように求められても、その番号へのコール転送は設定しないでください。この方法をユーザにアドバイスし、転送コールが目的の宛先に到達しないことによって発生する苦情の件数を削減します。

- シスコは、FAC または CMC をローカライズしていません。CMC 機能と FAC 機能は、Cisco CallManager がサポートしているどのロケールに対しても、同じデフォルト トーンを使用しています。
- Cisco CallManager　ではユーザに対してコードの入力を求めるタイミングを判別できないため、CMC 機能と FAC 機能は、オーバーラップ送信をサポートしていません。Route Pattern Configuration ウィンドウの Require Forced Authorization Code または Require Client Matter Code チェックボックスをオンにすると、Allow Overlap Sending チェックボックスは無効になります。Allow Overlap Sending チェックボックスをオンにすると、Require Forced Authorization Code および Require Client Matter Code チェックボックスは無効になります。
- FAC と CMC のトーンを再生できるのは、SCCP Phone、TAPI/JTAPI ポート、および MGCP FXS ポートの上だけです。
- H.323 アナログ ゲートウェイはトーンを再生できないため、FAC または CMC をサポートしていません。
- FAC と CMC をサポートする CTI デバイスには、制限事項があります。詳細については、P.5-8 の「CTI、JTAPI、および TAPI アプリケーションでの FAC/CMC の使用方法」を参照してください。
- Cisco WebDialer は FAC または CMC をサポートしていません。
- Cisco IP SoftPhone はトーンを再生できませんが、Cisco SoftPhone ユーザが電話番号をダイヤルした後、コードを入力する前にユーザが 1 ～ 2 秒待つことで、CMC および FAC を使用できます。
- FAC または CMC に # を追加しない場合、システムは T302 タイマーを待ち、コールを延長します。
- ダイヤルした番号が FAC または CMC を有効にしたルート パターンを使用してルーティングされる場合、電話機の Redial ソフトキーを押すときは、認証コードまたは CMC を入力する必要があります。シスコは、以前のコールで入力されたコードを保存しません。
- 短縮ダイヤル ボタンには、認証コードまたは CMC を設定できません。システムがコードの入力を求めたら、コードを入力する必要があります。

Cisco Bulk Administration Tool（BAT）の使用方法

CMC および FAC の挿入、更新、削除には、BAT を使用します。これらの作業を行うための詳細については、このリリースの Cisco CallManager と互換性のある『*Bulk Administration Tool ユーザ ガイド*』を参照してください。

CAR（CDR Analysis and Reporting）の使用方法

CAR（CDR Analysis and Reporting）を使用すると、認証コード名、認証レベル、および CMC の詳細などのコール詳細を提供するレポートを実行できます。CAR でレポートを生成する方法の詳細については、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』と『*Cisco CallManager Serviceability システム ガイド*』を参照してください。

CTI、JTAPI、および TAPI アプリケーションでの FAC/CMC の使用方法

多くの場合、Cisco CallManager は CTI、JTAPI、または TAPI アプリケーションに対して、ユーザがコール中にコードを入力する必要があることをアラートできます。ユーザがコールを発信する場合、Ad Hoc 会議を作成するか、FAC または CMC を有効にしたルート パターンを使用して打診転送を実行しますが、ユーザはトーンを受信したら、コードを入力する必要があります。ユーザが FAC または CMC を有効にしたルート パターンを使用してコールを転送またはブラインド転送する場合、ユーザはトーンを受信しないため、アプリケーションがコードを Cisco CallManager に送信する必要があります。Cisco CallManager が適切なコードを受信すると、コールは目的の宛先に接続されます。Cisco CallManager が適切なコードを受信しない場合、Cisco CallManager はどのコードが欠落しているかを示すエラーをアプリケーションに送信します。

Cisco CallManager は、FAC または CMC を有効にしたルート パターンを使用したコール転送をサポートしていません。詳細については、P.5-6 の「インタラクションおよび制限事項」を参照してください。

システム要件

次の情報は、CMC および FAC を使用する場合の最小限の要件です。

- Cisco CallManager 4.1：クラスタ内のすべてのサーバ
- 最新のサポート パックをインストールした Microsoft Windows 2000：クラスタ内のすべてのサーバ

CMC および FAC のインストール

CMC および FAC 機能は、Cisco CallManager のインストール時に自動的にインストールされます。これらの機能を Cisco CallManager ネットワークで使用できるようにするには、P.5-10 の「CMC および FAC の設定チェックリスト」で説明されている作業を実行する必要があります。

CMC および FAC の設定チェックリスト

CMC および FAC を設定する際は、表 5-1 をガイドとして使用します。

表 5-1　Cisco CMC および FAC の設定チェックリスト

設定手順		関連手順と関連項目
ステップ 1	機能の制限を確認します。	インタラクションおよび制限事項（P.5-6）
ステップ 2	システムを設計し文書化します。たとえば、追跡するクライアント マターのリストを作成します。	Client Matter Codes の概要（P.5-3） Forced Authorization Codes の概要（P.5-5）
ステップ 3	Cisco CallManager Administration または BAT（Cisco Bulk Administration Tool）を使用してコードを挿入します。 **ヒント**　小規模または大規模なコードのバッチとして BAT を使用することを検討します。BAT 内のコンマ区切り値（CSV）ファイルは、コード、対応する名前、対応するレベルなどを計画するために役立ちます。	Client Matter Codes の設定（P.5-11） Forced Authorization Codes の設定（P.5-19）
ステップ 4	FAC または CMC を有効にするには、Cisco CallManager Administration のルート パターンを追加または更新します。	ルート パターンでの Client Matter Codes の有効化（P.5-18） ルート パターンでの Forced Authorization Codes の有効化（P.5-26）
ステップ 5	ダイヤル プラン ドキュメントを更新するかダイヤル プラン ドキュメントとともに BAT CSV ファイルを印刷して保管します。	ダイヤル プラン ドキュメントを参照します。
ステップ 6	たとえば、コードなどの必要なすべての情報をユーザに提供し、機能の動作を説明します。	ユーザへの情報の提供（P.5-28）

Client Matter Codes の設定

使用する CMC のリストを取得したら、これらのコードをデータベースに追加して、ルート パターンの CMC 機能を有効にします。

この項では、次のトピックについて取り上げます。

クライアント マター コードの検索

Cisco CallManager を使用すると、特定の条件に基づいて、特定の CMC を検索できます。CMC を検索するには、次の手順を実行します。

（注）　ブラウザ セッションでの作業中、Cisco CallManager Administration は、検索プリファレンスを保持します。ほかのメニュー項目に移動してこのメニュー項目に戻った場合、検索を変更するかブラウザを閉じない限り、Cisco CallManager Administration によって検索プリファレンスが保持されます。

手順

ステップ 1　**Feature >Client Matter Code** を選択します。

Find and List ウィンドウが表示されます。

ヒント　データベースに登録されているすべての CMC を検索するには、検索文字を入力せずに **Find** をクリックします。

ステップ 2　最初の Find Client Matter Codes where ドロップダウン リスト ボックスから、Client Matter Code または Description などのオプションを 1 つ選択します。

（注）　最初のドロップダウン リスト ボックスで選択した基準によって、検索で生成されるリストのソート方法が決まります。たとえば、Client Matter Code を選択すると、結果リストの左のカラムに Client Matter Code カラムが表示されます。

ステップ 3　2 番目の Find Client Matter Codes where ドロップダウン リスト ボックスから、begins with、contains、ends with、is exactly などのオプションを 1 つ選択します。

ステップ 4　必要に応じて適切な検索文字を入力して、**Find** をクリックします。また、ページごとに表示する項目の件数を指定できます。

（注）　適切な CMC の横にあるチェックボックスをオンにして、**Delete Selected** をクリックすると、Find and List ウィンドウから複数の認証コードを削除できます。ウィンドウに表示されたすべての CMC を削除するには、Matching records タイトルバーのチェックボックスをオンにして、**Delete Selected** をクリックします。

ステップ 5　レコードのリストで、表示する CMC をクリックします。

選択した CMC がウィンドウに表示されます。

関連項目

- Client Matter Codes の概要（P.5-3）
- インタラクションおよび制限事項（P.5-6）
- システム要件（P.5-9）
- CMC および FAC の設定チェックリスト（P.5-10）
- クライアント マター コードの追加（P.5-14）
- クライアント マター コードの更新（P.5-15）
- クライアント マター コードの削除（P.5-16）
- CMC の設定項目（P.5-17）
- ルート パターンでの Client Matter Codes の有効化（P.5-18）

クライアント マター コードの追加

Cisco CallManager Administration で CMC を入力するか、Cisco Bulk Administration Tool（BAT）を使用して CMC を入力します。BAT を使用する場合、BAT のコンマ区切り値（CSV）ファイルには、CMC とクライアント名のレコードが記載されています。CMC の設定が完了したら、ダイヤル プラン ドキュメントを更新するか、またはダイヤル プラン ドキュメントとともに BAT CSV ファイルを印刷して保管します。

Cisco CallManager Administration で CMC を追加するには、次の手順を実行します。

手順

ステップ 1　Cisco CallManager Administration で、**Feature > Client Matter Code** を選択します。

ステップ 2　ウィンドウの右上隅にある **Add a New Client Matter Code** リンクをクリックします。

ステップ 3　表 5-2 の設定項目を使用して、CMC を設定します。

ステップ 4　**Insert** をクリックします。

ステップ 5　ステップ 2 ～ステップ 4 を繰り返して、すべての CMC を追加します。

ステップ 6　すべての CMC を追加したら、P.5-18 の「ルート パターンでの Client Matter Codes の有効化」を参照してください。

関連項目

- Client Matter Codes の概要（P.5-3）
- インタラクションおよび制限事項（P.5-6）
- システム要件（P.5-9）
- CMC および FAC の設定チェックリスト（P.5-10）
- クライアント マター コードの検索（P.5-12）

クライアント マター コードの更新

Cisco CallManager Administration で CMC を更新するには、次の手順を実行します。

手順

ステップ 1　まず更新する CMC を検索します。検索の手順は、P.5-12 の「クライアント マター コードの検索」を参照してください。

ステップ 2　表 5-2 をガイドとして使用して、表示するフィールドを更新します。

ステップ 3　**Update** をクリックします。

関連項目

- Client Matter Codes の概要（P.5-3）
- インタラクションおよび制限事項（P.5-6）
- システム要件（P.5-9）
- CMC および FAC の設定チェックリスト（P.5-10）
- クライアント マター コードの検索（P.5-12）
- クライアント マター コードの追加（P.5-14）
- クライアント マター コードの削除（P.5-16）
- CMC の設定項目（P.5-17）
- ルート パターンでの Client Matter Codes の有効化（P.5-18）

クライアント マター コードの削除

Cisco CallManager Administration で CMC を削除するには、次の手順を実行します。

手順

ステップ 1　まず削除する CMC を検索します。検索の手順は、P.5-12 の「クライアント マター コードの検索」を参照してください。

ステップ 2　Client Matter Code Configuration ウィンドウが表示されたら、**Delete** をクリックします。

ステップ 3　削除を続けるには、**OK** をクリックします。

関連項目

- Client Matter Codes の概要（P.5-3）
- インタラクションおよび制限事項（P.5-6）
- システム要件（P.5-9）
- CMC および FAC の設定チェックリスト（P.5-10）
- クライアント マター コードの検索（P.5-12）
- クライアント マター コードの追加（P.5-14）
- クライアント マター コードの更新（P.5-15）
- CMC の設定項目（P.5-17）
- ルート パターンでの Client Matter Codes の有効化（P.5-18）

CMC の設定項目

表 5-2 と次の項を併せて使用します。

- クライアント マター コードの追加（P.5-14）
- クライアント マター コードの更新（P.5-15）

表 5-2　CMC を追加する場合の設定項目

設定項目	説明
Client Matter Code	コールを開始するときにユーザが入力する一意のコードを 16 桁以内で入力します。このコードを使用したコールは、CDR に表示されます。
Description	50 文字以内の名前を入力します。このオプション フィールドはクライアント コードをクライアントに関連付けます。

ルート パターンでの Client Matter Codes の有効化

ルート パターンで CMC を有効にするには、次の手順を実行します。

手順

ステップ 1　Cisco CallManager Administration で、**Route Plan > Route/Hunt > Route Pattern** を選択します。

ステップ 2　次のいずれかの手順を実行します。

- 既存のルート パターンを更新するには、『*Cisco CallManager アドミニストレーション ガイド*』の「ルート パターンの設定」の説明に従って、Find and List Route Pattern ウィンドウに検索基準を入力します。
- 新しいルート パターンを追加する場合は、『*Cisco CallManager アドミニストレーション ガイド*』の「ルート パターンの設定」を参照してください。

ステップ 3　Route Pattern Configuration ウィンドウで、**Require Client Matter Code** チェックボックスをオンにします。

ステップ 4　次のいずれかの手順を実行します。

- ルート パターンを更新する場合は、**Update** をクリックします。
- 新しいルート パターンを追加する場合は、**Insert** をクリックします。

ステップ 5　認証コードが必要なすべてのルート パターンについて、ステップ 2 ～ステップ 4 を繰り返します。

ステップ 6　ルート パターンの設定が完了したら、P.5-28 の「ユーザへの情報の提供」を参照してください。

関連項目

- Client Matter Codes の概要（P.5-3）
- インタラクションおよび制限事項（P.5-6）
- システム要件（P.5-9）
- CMC および FAC の設定チェックリスト（P.5-10）
- クライアント マター コードの検索（P.5-12）
- クライアント マター コードの追加（P.5-14）
- クライアント マター コードの更新（P.5-15）
- クライアント マター コードの削除（P.5-16）
- CMC の設定項目（P.5-17）

Forced Authorization Codes の設定

FAC の設定については、次の項を参照してください。

- CMC および FAC の設定チェックリスト（P.5-10）
- Forced Authorization Code の検索（P.5-20）
- Forced Authorization Code の追加（P.5-22）
- Forced Authorization Code の更新（P.5-23）
- Forced Authorization Code の削除（P.5-24）
- FAC の設定項目（P.5-25）
- ユーザへの情報の提供（P.5-28）
- ルート パターンでの Forced Authorization Codes の有効化（P.5-26）

Forced Authorization Code の検索

Cisco CallManager を使用すると、特定の条件に基づいて、特定の FAC を検索できます。FAC を検索するには、次の手順を実行します。

（注） ブラウザ セッションでの作業中、Cisco CallManager Administration は、検索プリファレンスを保持します。ほかのメニュー項目に移動してこのメニュー項目に戻った場合、検索を変更するかブラウザを閉じない限り、Cisco CallManager Administration によって検索プリファレンスが保持されます。

手順

ステップ 1　**Feature > Forced Authorization Code** を選択します。

Find and List ウィンドウが表示されます。

ヒント　データベースに登録されているすべての認証コードを検索するには、検索文字を入力せずに **Find** をクリックします。

ステップ 2　最初の Find Authorization Codes where ドロップダウン リスト ボックスから、Authorization Code Name、Authorization Code、または Authorization Code Level などのオプションを 1 つ選択します。

（注） 最初のドロップダウン リスト ボックスで選択した基準によって、検索で生成されるリストのソート方法が決まります。たとえば、Authorization Code Name を選択すると、結果リストの左のカラムに Authorization Code Name カラムが表示されます。

ステップ 3　2 番目の Find Authorization Codes where ドロップダウン リスト ボックスから、begins with、contains、ends with、is exactly などのオプションを 1 つ選択します。

ステップ 4　必要に応じて適切な検索文字を入力して、**Find** をクリックします。また、ページごとに表示する項目の件数を指定できます。

（注）　適切な FAC の横にあるチェックボックスをオンにして、**Delete Selected** をクリックすると、Find and List ウィンドウから複数の認証コードを削除できます。ウィンドウに表示されたすべての FAC を削除するには、Matching records タイトルバーのチェックボックスをオンにして、**Delete Selected** をクリックします。

ステップ 5　レコードのリストで、表示する認証コードをクリックします。

選択した FAC がウィンドウに表示されます。

関連項目

- Forced Authorization Codes の概要（P.5-5）
- インタラクションおよび制限事項（P.5-6）
- システム要件（P.5-9）
- CMC および FAC の設定チェックリスト（P.5-10）
- Forced Authorization Code の追加（P.5-22）
- Forced Authorization Code の更新（P.5-23）
- Forced Authorization Code の削除（P.5-24）
- FAC の設定項目（P.5-25）
- ルート パターンでの Forced Authorization Codes の有効化（P.5-26）

Forced Authorization Code の追加

FAC 実装の設計が完了したら、Cisco CallManager Administration または Cisco Bulk Administration Tool（BAT）を使用して認証コードを入力します。認証コードの大きなバッチとして BAT を使用することを検討します。BAT 内のコンマ区切り値（CSV）ファイルは、認証コード、対応する名前、対応するレベルなどを計画するために役立ちます。後で参照するために、ダイヤル プラン ドキュメントを更新するか、またはダイヤル プラン ドキュメントとともに CSV ファイルを印刷して保管します。

Cisco CallManager Administration で少数の認証コードを追加する場合は、次の手順を実行します。

手順

ステップ 1　Cisco CallManager Administration で、**Feature > Forced Authorization Code** を選択します。

ステップ 2　ウィンドウの右上隅にある **Add a New Forced Authorization Code** リンクをクリックします。

ステップ 3　表 5-3 の設定項目を使用して、認証コードを設定します。

ステップ 4　**Insert** をクリックします。

ステップ 5　ステップ 2 ～ステップ 4 を繰り返して、すべての認証コードを追加します。

ステップ 6　すべての認証コードを追加したら、P.5-26 の「ルート パターンでの Forced Authorization Codes の有効化」を参照してください。

関連項目

- Forced Authorization Codes の概要（P.5-5）
- インタラクションおよび制限事項（P.5-6）
- システム要件（P.5-9）

- CMC および FAC の設定チェックリスト（P.5-10）
- Forced Authorization Code の検索（P.5-20）
- Forced Authorization Code の更新（P.5-23）
- Forced Authorization Code の削除（P.5-24）
- FAC の設定項目（P.5-25）
- ルート パターンでの Forced Authorization Codes の有効化（P.5-26）

Forced Authorization Code の更新

Cisco CallManager Administration で FAC を更新するには、次の手順を実行します。

手順

ステップ 1　まず更新する認証コードを検索します。検索の手順は、P.5-20 の「Forced Authorization Code の検索」を参照してください。

ステップ 2　表 5-3 をガイドとして使用して、表示するフィールドを更新します。

ステップ 3　**Update** をクリックします。

関連項目

- Forced Authorization Codes の概要（P.5-5）
- インタラクションおよび制限事項（P.5-6）
- システム要件（P.5-9）
- CMC および FAC の設定チェックリスト（P.5-10）
- Forced Authorization Code の検索（P.5-20）
- Forced Authorization Code の追加（P.5-22）
- Forced Authorization Code の削除（P.5-24）
- FAC の設定項目（P.5-25）
- ルート パターンでの Forced Authorization Codes の有効化（P.5-26）

Forced Authorization Code の削除

FAC を削除するには、次の手順を実行します。

手順

ステップ 1　まず削除する認証コードを検索します。検索の手順は、P.5-20 の「Forced Authorization Code の検索」を参照してください。

ステップ 2　Forced Authorization Code Configuration ウィンドウが表示されたら、**Delete** をクリックします。

ステップ 3　削除を続けるには、**OK** をクリックします。

関連項目

- Forced Authorization Codes の概要（P.5-5）
- インタラクションおよび制限事項（P.5-6）
- システム要件（P.5-9）
- CMC および FAC の設定チェックリスト（P.5-10）
- Forced Authorization Code の検索（P.5-20）
- Forced Authorization Code の追加（P.5-22）
- Forced Authorization Code の更新（P.5-23）
- FAC の設定項目（P.5-25）
- ルート パターンでの Forced Authorization Codes の有効化（P.5-26）

FAC の設定項目

表 5-3 と次の項を併せて使用します。

- Forced Authorization Code の追加（P.5-22）
- Forced Authorization Code の更新（P.5-23）

表 5-3　FAC の設定項目

設定項目	説明
Authorization Code Name	一意の名前を 50 文字以内で入力します。この名前は、認証コードと特定のユーザまたはユーザのグループを関連付けます。このコードを使用するコールについては、この名前が CDR に表示されます。
Authorization Code	一意の認証コードを 16 文字以内で入力します。ユーザは、FAC 対応ルート パターンを使用してコールを発信するときに、このコードを入力します。
Authorization Level	0 ～ 255 の範囲の 3 桁の認証レベルを入力します。デフォルトは 0 です。認証コードに割り当てるレベルによって、ユーザが FAC 対応ルート パターンを使用してコールをルーティングできるかどうかが決定されます。コールを正しくルーティングするには、ユーザ認証レベルが、コールのルート パターンに指定されている認証レベルと比較して同等または上位である必要があります。

ルート パターンでの Forced Authorization Codes の有効化

ルート パターンで FAC を有効にするには、次の手順を実行します。

手順

ステップ 1　Cisco CallManager Administration で、**Route Plan > Route/Hunt > Route Pattern** を選択します。

ステップ 2　次のいずれかの手順を実行します。

- 既存のルート パターンを更新するには、『*Cisco CallManager アドミニストレーション ガイド*』の「ルート パターンの設定」の説明に従って、Find and List Route Pattern ウィンドウに検索基準を入力します。
- 新しいルート パターンを追加する場合は、『*Cisco CallManager アドミニストレーション ガイド*』の「ルート パターンの設定」を参照してください。

ステップ 3　Route Pattern Configuration ウィンドウで、**Require Forced Authorization Code** チェックボックスをオンにします。

ステップ 4　Authorization Level フィールドに、ルート パターンに指定する認証レベルを入力します。このフィールドで指定した数値は、このルート パターンを使用したコールを正しくルーティングするために必要な最小限の認証レベルを決定します。

ヒント　Require Forced Authorization Code チェックボックスをオンにしない場合でも、指定した数値はデータベースに保存されているため、認証レベルを指定できます。

ステップ 5　次のいずれかの手順を実行します。

- ルート パターンを更新する場合は、**Update** をクリックします。
- 新しいルート パターンを追加する場合は、**Insert** をクリックします。

ステップ 6　認証コードが必要なすべてのルート パターンについて、ステップ 2 ～ステップ 5 を繰り返します。

ステップ 7　ルート　パターンの設定が完了したら、P.5-28 の「ユーザへの情報の提供」を参照してください。

関連項目

- Forced Authorization Codes の概要（P.5-5）
- インタラクションおよび制限事項（P.5-6）
- システム要件（P.5-9）
- CMC および FAC の設定チェックリスト（P.5-10）
- Forced Authorization Code の検索（P.5-20）
- Forced Authorization Code の追加（P.5-22）
- Forced Authorization Code の更新（P.5-23）
- Forced Authorization Code の削除（P.5-24）
- FAC の設定項目（P.5-25）

ユーザへの情報の提供

機能の設定が完了したら、次の情報をユーザに通知します。

- P.5-6 の「インタラクションおよび制限事項」に説明されている制限事項をユーザに通知します。
- たとえば認証コード、認証レベル、クライアント マター コードなど、これらの機能を使用するために必要なすべての情報をユーザに提供します。番号をダイヤルするとコードの入力を求めるトーンが聞こえることを、ユーザに通知します。
- FAC の場合、ユーザ認証コードを入力して発信されたコールは、ユーザまたはユーザの部署に属すると見なされます。認証コードを覚えておくか、安全な場所に記録しておくようユーザに勧めます。
- ユーザが使用できるコールの種類を通知します。たとえば、電話機の管理者に問題を知らせる前に、ユーザは電話を切り、ダイヤルした番号とコードをリトライする必要があります。
- トーンが完了する前にコードを入力できることをユーザに通知します。
- ユーザがコードを入力した後、コールをすぐにルーティングするには、電話機の # を押します。押さない場合、コールはディジット間タイマー（T302）が満了した後に接続されます。このタイマーは、デフォルトで 15 秒です。
- ユーザが無効なコードを入力すると、電話はリオーダー音を再生します。コードの入力を間違えた場合は、電話を切り、もう一度コールを開始する必要があります。リオーダー音が続く場合は、ユーザは電話またはシステムの管理者に、コードに問題がある可能性があることを知らせる必要があります。

その他の情報

関連項目

- 『*Cisco CallManager アドミニストレーション ガイド*』の「ルート パターンの設定」
- 『*Cisco CallManager システム ガイド*』の「ルート プランの概要」

その他のシスコ マニュアル

- *Bulk Administration Tool ユーザ ガイド*
- *Cisco CallManager Serviceability システム ガイド*
- *Cisco CallManager Serviceability アドミニストレーション ガイド*