



# CHAPTER 17

## クライアント識別コードと強制承認コード

Forced Authorization Code (FAC; 強制承認コード) と Client Matter Code (CMC; クライアント識別コード) を使用すると、コールへのアクセスとアカウントिंग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 アカウントिंगと課金を支援し、FAC 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。

クライアント識別コード機能を有効にすると、コールが特定のクライアントに関連していることを示すコードをユーザが入力する必要があります。コール アカウントिंगと課金の目的で、顧客、学生などのユーザにクライアント識別コードを割り当てることができます。強制承認コード機能を有効にすると、ユーザがコールを確立する前に有効な承認コードを入力する必要があります。

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、ダイヤル プラン ドキュメントを更新して各ルート パターンに対する FAC や CMC の有効化または無効化を反映させる必要があります。

この章は、次の内容で構成されています。

- 「クライアント識別コードおよび強制承認コードの設定チェックリスト」 (P.17-2)
- 「クライアント識別コードの概要」 (P.17-3)
- 「強制承認コードの概要」 (P.17-4)
- 「インタラクションおよび制限事項」 (P.17-4)
- 「システム要件」 (P.17-6)
- 「CMC および FAC のインストール」 (P.17-6)
- 「クライアント識別コードの設定」 (P.17-7)
- 「CMC の設定項目」 (P.17-9)
- 「ルート パターンでのクライアント識別コードの有効化」 (P.17-10)
- 「強制承認コードの設定」 (P.17-10)
- 「FAC の設定項目」 (P.17-12)
- 「ルート パターンでの強制承認コードの有効化」 (P.17-13)
- 「ユーザへの情報の提供」 (P.17-14)
- 「CDR Analysis and Reporting の使用方法」 (P.17-6)
- 「関連項目」 (P.17-15)

# クライアント識別コードおよび強制承認コードの設定チェックリスト

Forced Authorization Code (FAC; 強制承認コード) と Client Matter Code (CMC; クライアント識別コード) を使用すると、コールへのアクセスとアカウントिंग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 アカウントिंगと課金を支援し、FAC 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。

クライアント識別コード機能を有効にすると、コールが特定のクライアントに関連していることを示すコードをユーザが入力する必要があります。コール アカウントिंगと課金の目的で、顧客、学生などのユーザにクライアント識別コードを割り当てることができます。強制承認コード機能を有効にすると、ユーザがコールを確立する前に有効な承認コードを入力する必要があります。

クライアント識別コードと強制承認コードを使用する際には、表 17-1 をガイドとして使用してください。クライアント識別コードと強制承認コードの詳細については、「関連項目」(P.17-15) を参照してください。

表 17-1 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.17-4)
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。	「クライアント識別コードの概要」(P.17-3) 「強制承認コードの概要」(P.17-4)
ステップ 3	Cisco Unified Communications Manager の管理ページまたは一括管理ツール (BAT) を使用してコードを挿入します。 <b>ヒント</b> 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 内のカンマ区切り値 (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。	「クライアント識別コードの設定」(P.17-7) 「強制承認コードの設定」(P.17-10)
ステップ 4	FAC または CMC を有効にするには、Cisco Unified Communications Manager の管理ページでルート パターンを追加または更新します。	「ルート パターンでのクライアント識別コードの有効化」(P.17-10) 「ルート パターンでの強制承認コードの有効化」(P.17-13)
ステップ 5	ダイヤル プラントキュメントを更新するかダイヤル プラント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 プラントキュメントを参照してください。
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.17-14)

## クライアント識別コードの概要

クライアント識別コード機能を使用する場合、ユーザはクライアント識別コードを入力して、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識別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識別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、CDR Analysis and Reporting (CAR) 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トリングと料金請求のレポートを生成します。

クライアント識別コード機能は、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 Unified Communications Manager の管理ページの [CMC の設定 (Client Matter Codes Configuration)] ウィンドウでクライアント識別コードを追加する必要があります。次に、Cisco Unified Communications Manager の管理ページで、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 を設定した後、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 の入力を求めるため、ユーザは、CMC を起動したり、特別な数字をダイヤルしたり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。クライアントマター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、ユーザは通常どおり、214-555-1234 だけをダイヤルします。

## 強制承認コードの概要

Cisco Unified Communications Manager の管理ページのルート 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、承認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、システムは承認コードの入力を求めるトーンを再生します。

Cisco Unified Communications Manager の管理ページでは、さまざまなレベルの承認を設定できます。ユーザ承認コードが、ダイヤルした番号へのルーティングに指定された承認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。承認が受け入れられると、コールが開始されます。承認の名前は Call Detail Record (CDR; 呼詳細レコード) に書き込みを行うため、CDR Analysis and Reporting (CAR) 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、一意の承認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。各ユーザに承認コードを指定し、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承認レベルを指定します。Cisco Unified Communications Manager の管理ページのルート 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、承認レベルを設定します。

FAC を実装するには、承認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。承認レベルは 0 ~ 255 の範囲で指定する必要があります。シスコでは任意の承認レベルを許容しているため、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承認レベル 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承認レベル 20 を設定する。
- 国際電話に承認レベル 30 を設定する。



**ヒント** 承認レベルを 10 ずつ増加することで、より多くの承認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承認コードを入力して、次のプロンプトでクライアント識別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承認コードを、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 Unified Communications Manager が提供する冗長性は、Cisco Unified Communications Manager 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 Unified IP Phone 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。

- CMC の数は、Cisco Unified Communications Manager の起動に必要な時間に直接影響を及ぼすため、CMC の数は 60,000 に制限する必要があります。この数を超える CMC を設定すると、大幅な遅延が発生する場合があります。たとえば、400,000 の CMC を持つシステムの場合は起動に 1 時間かかり、100 万の CMC を持つシステムの場合は起動に 4 時間かかります。
- 電話番号をダイヤルした後、聴覚に障害のあるユーザは、承認コードまたはクライアント識別コードを入力する前に 1 ～ 2 秒待つ必要があります。
- FAC または CMC 対応のルート パターンに自動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 Unified Communications Manager の管理ページまたは Cisco Unified CM のユーザ オプション ページで設定された自動転送に適用されます。自動転送を設定することはできますが、FAC または CMC 対応のルート 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 [不在] 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、コールの自動転送は失敗します。

FAC または CMC が有効なルート パターンにコールが自動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、自動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、その番号への自動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 Unified Communications Manager 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 Unified Communications Manager 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。[ルート パターンの設定 (Route Pattern Configuration)] ウィンドウの [FAC が必須 (Require Forced Authorization Code)] または [CMC が必須 (Require Client Matter Code)] チェックボックスをオンにすると、[オーバーラップ送信を許可 (Allow Overlap Sending)] チェックボックスは無効になります。[オーバーラップ送信を許可 (Allow Overlap Sending)] チェックボックスをオンにすると、[FAC が必須 (Require Forced Authorization Code)] および [CMC が必須 (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 を実行する電話機、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、「[CTI、JTAPI、および TAPI アプリケーションでの FAC/CMC の使用方法](#)」(P.17-6) 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。ただし、Cisco IP SoftPhone ユーザは、電話番号をダイヤルした後、コードを入力する前に 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 対応のルート パターンを使用してルーティングされる場合、電話機の [リダイヤル] ソフトキーを押すときは、承認コードまたは 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、承認コードまたは 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 一括管理ツールの使用方法

CMC および FAC の挿入、更新、削除には、一括管理ツール (BAT) を使用します。これらの操作方法の詳細については、このリリースの **Cisco Unified Communications Manager** と互換性のある『*Cisco Unified Communications Manager Bulk Administration ガイド*』を参照してください。

## CDR Analysis and Reporting の使用方法

CDR Analysis and Reporting (CAR) を使用すると、承認コード名、承認レベル、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 Unified Communications Manager CDR Analysis and Reporting Administration Guide*』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 Unified Communications Manager 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。ユーザは、コールを発信したり、アドホック会議を作成したり、FAC または CMC 対応のルート パターンを使用して打診転送を実行したりする場合、トーンの受信後にコードを入力する必要があります。ユーザは、FAC または CMC 対応のルート 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、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 Unified Communications Manager に送信する必要があります。Cisco Unified Communications Manager 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 Unified Communications Manager が適切なコードを受信しない場合、Cisco Unified Communications Manager 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 Unified Communications Manager は、FAC または CMC 対応のルート パターンを使用した自動転送をサポートしていません。詳細については、「[インタラクティブおよび制限事項](#)」(P.17-4) を参照してください。

## システム要件

CMC と FAC の最小要件として、クラスタ内のすべてのサーバに Cisco Unified Communications Manager 5.0 以降がインストールされている必要があります。

## CMC および FAC のインストール

CMC 機能と FAC 機能は、Cisco Unified Communications Manager 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 Unified Communications Manager ネットワークで使用できるようにするには、「[クライアント識別コードの設定](#)」(P.17-7) で説明されている作業を実行する必要があります。

## クライアント識別コードの設定

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。

- 「クライアント識別コードの検索」(P.17-7)
- 「クライアント識別コードの設定」(P.17-8)
- 「クライアント識別コードの削除」(P.17-9)
- 「CMC の設定項目」(P.17-9)
- 「ルート パターンでのクライアント識別コードの有効化」(P.17-10)
- 「ユーザへの情報の提供」(P.17-14)



### ヒント

クライアント識別コードを設定する前に、「クライアント識別コードおよび強制承認コードの設定チェックリスト」(P.17-2) を参照してください。

## クライアント識別コードの検索

Cisco Unified Communications Manager では、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は、Cisco Unified Communications Manager の管理ページで検索プリファレンスが保持されます。他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でも、検索を変更するかブラウザを閉じない限り、検索プリファレンスは Cisco Unified Communications Manager の管理ページで保持されています。

### 手順

**ステップ 1** [コールルーティング (Call Routing)] > [CMC] を選択します。

検索と一覧表示のウィンドウが表示されます。

**ステップ 2** データベース内のすべてのレコードを検索するには、ダイアログボックスが空になっていることを確認し、「ステップ 3」に進みます。

特定のレコードをフィルタリングまたは検索するには、次の操作を実行します。

- 最初のドロップダウン リスト ボックスで、検索パラメータを選択します。
- 2 番目のドロップダウン リスト ボックスで、検索パターンを選択します。
- 必要に応じて、適切な検索文字を入力します。



### (注)

別の検索条件を追加するには、[+] ボタンをクリックします。条件を追加した場合は、指定したすべての条件に一致するレコードが検索されます。条件を削除するには、[-] ボタンをクリックして、最後に追加された条件を削除するか、または [フィルタのクリア (Clear Filter)] ボタンをクリックして、追加されたすべての検索条件を削除します。

**ステップ 3** [検索 (Find)] をクリックします。

すべてのレコードまたは条件に一致するレコードが表示されます。[ ページあたりの行数 (Rows per Page)] ドロップダウンリストボックスで別の値を選択すると、各ページに表示される項目数を変更できます。



**(注)** 適切なレコードの横にあるチェックボックスをオンにして、[ 選択項目の削除 (Delete Selected)] をクリックすると、データベースから複数のレコードを削除できます。[ すべてを選択 (Select All)] をクリックして [ 選択項目の削除 (Delete Selected)] をクリックすると、この選択対象として設定可能なすべてのレコードを削除できます。

**ステップ 4** 表示されたレコードリストから、目的のレコードのリンクをクリックします。

**(注)** ソート順を逆にするには、リストのヘッダーにある上矢印または下矢印をクリックします (使用可能な場合)。

選択した項目がウィンドウに表示されます。

**追加情報**

「[関連項目](#)」(P.17-15) を参照してください。

## クライアント識別コードの設定

Cisco Unified Communications Manager の管理ページで CMC を入力するか、Cisco 一括管理ツール (BAT) を使用して CMC を入力します。BAT を使用する場合、BAT のカンマ区切り値 (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、ダイヤルブランドキュメントを更新するか、またはダイヤルブ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 Unified Communications Manager の管理ページで CMC を追加または更新するには、次の手順を実行します。

**手順****ステップ 1** 次のいずれかの手順を実行します。

- CMC を追加するには、[ コールルーティング (Call Routing)] > [CMC] を選択し、[ 新規追加 (Add New)] をクリックします。「[ステップ 2](#)」に進みます。
- CMC を更新するには、「[クライアント識別コードの検索](#)」(P.17-7) の説明に従って更新する CMC を検索し、「[ステップ 2](#)」に進みます。

**ステップ 2** 適切な設定値を入力します (表 17-2 を参照)。**ステップ 3** [保存 (Save)] をクリックします。**ステップ 4** すべての CMC を追加したら、「[ルートパターンでのクライアント識別コードの有効化](#)」(P.17-10) を参照してください。**追加情報**

「[関連項目](#)」(P.17-15) を参照してください。



## CMC の設定項目

Client Matter Code (CMC; クライアント識別コード) を使用すると、コールへのアクセスとアカウントリングを管理できます。CMC は、ユーザに対して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することで、課金可能なクライアントに対するコールアカウントリングと課金を支援します。クライアント識別コードは、コール アカウントリ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。

クライアント識別コードを設定する際には、表 17-1 をガイドとして使用してください。クライアント識別コードと強制承認コードの詳細については、「関連項目」(P.17-15) を参照してください。

「表 17-2」と「クライアント識別コードの設定」(P.17-8) を併せて参照してください。

表 17-2 CMC を追加する場合の設定項目

設定項目	説明
[CMC]	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。
[説明 (Description)]	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。説明には、任意の言語で最大 50 文字を指定できますが、二重引用符 (")、パーセント記号 (%)、アンパサンド (&)、バックslash (\)、山カッコ (<>)、または角カッコ ([ ] および { }) は使用できません。

### 追加情報

「関連項目」(P.17-15) を参照してください。

## クライアント識別コードの削除

Cisco Unified Communications Manager の管理ページで 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、「クライアント識別コードの検索」(P.17-7) を参照してください。
- ステップ 2 [CMC の設定 (Client Matter Codes Configuration)] ウィンドウが表示されたら、[削除 (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。

### 追加情報

「関連項目」(P.17-15) を参照してください。

## ルート パターンでのクライアント識別コードの有効化

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 Unified Communications Manager の管理ページで、[コールルーティング (Call Routing)] > [ルート/ハント (Route/Hunt)] > [ルートパターン (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 Unified Communications Manager 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、[ルートパターンの検索と一覧表示 (Find and List Route Patterns)] ウィンドウに検索条件を入力します。
  - 新しいルート パターンを追加するには、『Cisco Unified Communications Manager 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** [ルートパターンの設定 (Route Pattern Configuration)] ウィンドウで、[CMC が必須 (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 パターンを更新した場合は、[保存 (Save)] をクリックします。
  - 新しいルート パターンを追加した場合は、[保存 (Save)] をクリックします。
- ステップ 5** クライアント識別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、「[ユーザへの情報の提供](#)」(P.17-14) を参照してください。
- 

### 追加情報

「[関連項目](#)」(P.17-15) を参照してください。

## 強制承認コードの設定

この項は、次の内容で構成されています。

- 「[強制承認コードの検索](#)」(P.17-11)
- 「[強制承認コードの設定](#)」(P.17-12)
- 「[強制承認コードの削除](#)」(P.17-13)
- 「[FAC の設定項目](#)」(P.17-12)
- 「[ユーザへの情報の提供](#)」(P.17-14)
- 「[ルート パターンでの強制承認コードの有効化](#)」(P.17-13)



### ヒント

強制承認コードを設定する前に、「[クライアント識別コードおよび強制承認コードの設定チェックリスト](#)」(P.17-2) を参照してください。

---

## 強制承認コードの検索

Cisco Unified Communications Manager 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は、Cisco Unified Communications Manager の管理ページで検索プリファレンスが保持されます。他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でも、検索を変更するかブラウザを閉じない限り、検索プリファレンスは Cisco Unified Communications Manager の管理ページで保持されています。

### 手順

**ステップ 1** [コールルーティング (Call Routing)] > [FAC] を選択します。

検索と一覧表示のウィンドウが表示されます。

**ステップ 2** データベース内のすべてのレコードを検索するには、ダイアログボックスが空になっていることを確認し、「[ステップ 3](#)」に進みます。

特定のレコードをフィルタリングまたは検索するには、次の操作を実行します。

- 最初のドロップダウン リスト ボックスで、検索パラメータを選択します。
- 2 番目のドロップダウン リスト ボックスで、検索パターンを選択します。
- 必要に応じて、適切な検索文字を入力します。



(注) 別の検索条件を追加するには、[+] ボタンをクリックします。条件を追加した場合は、指定したすべての条件に一致するレコードが検索されます。条件を削除するには、[-] ボタンをクリックして、最後に追加された条件を削除するか、または [フィルタのクリア (Clear Filter)] ボタンをクリックして、追加されたすべての検索条件を削除します。

**ステップ 3** [検索 (Find)] をクリックします。

すべてのレコードまたは条件に一致するレコードが表示されます。[ページあたりの行数 (Rows per Page)] ドロップダウン リスト ボックスで別の値を選択すると、各ページに表示される項目数を変更できます。



(注) 適切なレコードの横にあるチェックボックスをオンにして、[選択項目の削除 (Delete Selected)] をクリックすると、データベースから複数のレコードを削除できます。[すべてを選択 (Select All)] をクリックして [選択項目の削除 (Delete Selected)] をクリックすると、この選択対象として設定可能なすべてのレコードを削除できます。

**ステップ 4** 表示されたレコード リストから、目的のレコードのリンクをクリックします。



(注) ソート順を逆にするには、リストのヘッダーにある上矢印または下矢印をクリックします (使用可能な場合)。

選択した項目がウィンドウに表示されます。

### 追加情報

「[関連項目](#)」(P.17-15) を参照してください。

## 強制承認コードの設定

FAC 実装の設計が完了したら、Cisco Unified Communications Manager の管理ページまたは Cisco 一括管理ツール (BAT) を使用して承認コードを入力します。承認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 内のカンマ区切り値 (CSV) ファイルは、承認コード、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。



(注) 後で参照するために、ダイヤルブランドキュメントを更新するか、またはダイヤルブ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 Unified Communications Manager の管理ページで少数の承認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 Unified Communications Manager の管理ページで、[ コールルーティング (Call Routing) ] > [FAC] 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。
  - 新しい FAC を追加するには、[ 新規追加 (Add New) ] をクリックします。
  - FAC を更新するには、更新する承認コードを検索します。検索の手順は、「強制承認コードの検索」(P.17-11) を参照してください。
- ステップ 3 表 17-3 の設定方法に従って、承認コードを設定します。
- ステップ 4 [ 保存 (Save) ] をクリックします。



(注) すべての承認コードを追加したら、「ルートパターンでの強制承認コードの有効化」(P.17-13) を参照してください。

### 追加情報

「関連項目」(P.17-15) を参照してください。

## FAC の設定項目

Forced Authorization Code (FAC; 強制承認コード) を使用すると、特定のユーザが発信できるコールのタイプを規定することで、コールへのアクセスとアカウントリングを管理できます。強制承認コード機能を使用すると、コールを完了する前に有効な承認コードを入力するように強制されます。

強制承認コードを設定する際には、表 17-1 をガイドとして使用してください。強制承認コードの詳細については、「関連項目」(P.17-15) を参照してください。

「表 17-3」と「強制承認コードの設定」(P.17-12) を併せて参照してください。

表 17-3 FAC の設定項目

設定項目	説明
[承認コード名 (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、承認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。
[承認コード (Authorization Code)]	一意の承認コードを 16 文字以内で入力します。ユーザは、FAC 対応のルート 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。
[承認レベル (Authorization Level)]	0 ~ 255 の範囲の 3 桁の承認レベルを入力します。デフォルトは 0 です。承認コードに割り当てるレベルによって、ユーザが FAC 対応のルート 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まります。コールを正しくルーティングするには、ユーザ承認レベルが、コールのルート パターンに指定されている承認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。

**追加情報**

「関連項目」(P.17-15) を参照してください。

## 強制承認コードの削除

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** まず削除する承認コードを検索します。検索の手順は、「強制承認コードの検索」(P.17-11) を参照してください。
- ステップ 2** [FAC の設定 (Forced Authorization Code Configuration)] ウィンドウが表示されたら、[削除 (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。

**追加情報**

「関連項目」(P.17-15) を参照してください。

## ルート パターンでの強制承認コードの有効化

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 Unified Communications Manager の管理ページで、[コールルーティング (Call Routing)] > [ルート / ハント (Route/Hunt)] > [ルートパターン (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 Unified Communications Manager 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、[ルートパターンの検索と一覧表示 (Find and List Route Patterns)] ウィンドウに検索条件を入力します。
- 新しいルート パターンを追加するには、『Cisco Unified Communications Manager 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** [ルートパターンの設定 (Route Pattern Configuration)] ウィンドウで、[FACが必須 (Require Forced Authorization Code)] チェックボックスをオンにします。

**ステップ 4** [保存 (Save)] をクリックします。



**ヒント** [FACが必須 (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、承認レベルを指定できます。

**ステップ 5** 承認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、「ユーザへの情報の提供」(P.17-14) を参照してください。

#### 追加情報

「関連項目」(P.17-15) を参照してください。

## 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。

- 「インタラクションおよび制限事項」(P.17-4) に説明されている制限事項をユーザに通知します。
- たとえば承認コード、承認レベル、クライアント識別コードなど、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、ユーザ承認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。承認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タイプを通知します。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、電話機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。

#### 追加情報

「関連項目」(P.17-15) を参照してください。

## 関連項目

- 『Cisco Unified Communications Manager 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 Unified Communications Manager システムガイド』の「ルートプランの概要」
- 「インタラクションおよび制限事項」(P.17-4)
- 「システム要件」(P.17-6)

### クライアント識別コード

- 「クライアント識別コードおよび強制承認コードの設定チェックリスト」(P.17-2)
- 「クライアント識別コードの概要」(P.17-3)
- 「クライアント識別コードの検索」(P.17-7)
- 「クライアント識別コードの設定」(P.17-8)
- 「クライアント識別コードの削除」(P.17-9)
- 「CMC の設定項目」(P.17-9)
- 「ルートパターンでのクライアント識別コードの有効化」(P.17-10)

### 強制承認コード

- 「クライアント識別コードおよび強制承認コードの設定チェックリスト」(P.17-2)
- 「強制承認コードの概要」(P.17-4)
- 「強制承認コードの検索」(P.17-11)
- 「強制承認コードの設定」(P.17-12)
- 「強制承認コードの削除」(P.17-13)
- 「FAC の設定項目」(P.17-12)
- 「ルートパターンでの強制承認コードの有効化」(P.17-13)

### 参考資料

- 『Cisco Unified Communications Manager Bulk Administration ガイド』
- 『Cisco Unified Communications Manager アドミニストレーションガイド』
- 『Cisco Unified Communications Manager CDR Analysis and Reporting Administration Guide』

