



クライアント識別コードと強制承認コード

- [クライアント識別コードと強制承認コードの概要（1 ページ）](#)
- [クライアント識別コードと強制承認コードの前提条件（1 ページ）](#)
- [クライアント識別コードと強制承認コードの設定タスク フロー（2 ページ）](#)
- [クライアント識別コードと強制承認コードの連携動作（5 ページ）](#)
- [クライアント識別コードと強制承認コードの制約事項（6 ページ）](#)

クライアント識別コードと強制承認コードの概要

クライアント識別コード（CMC）と強制承認コード（FAC）により、コールアクセスとアカウントリングを効果的に管理できます。CMC はクライアントのコール アカウントリングおよび請求を支援し、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。

CMC を使用する場合、ユーザはコードを入力する必要があります。この操作により、コールが特定のクライアント識別に関連していることが指定されます。コール アカウントリングおよび請求を目的として、クライアント識別コードを顧客、学生、またはその他のグループに割り当てることができます。FAC を使用する場合、コールが確立する前に、特定のアクセス レベルで割り当てられた有効な認証コードをユーザが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の前提条件

- SCCP と SIP を実行する Cisco Unified IP Phone は、CMC と FAC をサポートしています。
- CMC と FAC のトーンは、SCCP または SIP を実行している Cisco Unified IP Phone、TAPI/JTAPI ポート、および MGCP FXS ポートでのみ再生されます。

クライアント識別コードと強制承認コードの設定タスクフロー

CMC と FAC は、別々または一緒に実装できます。たとえば、特定のクラスのコール（市外通話など）の発信をユーザに許可するとともに、特定のクライアントにコールのクラスを割り当てるとします。CMC トーンと FAC トーンは、ユーザには同じ音に聞こえます。そのため、両方のコードを設定する場合、この機能では、最初のトーンの後で FAC を入力し、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。

始める前に

- [クライアント識別コードと強制承認コードの前提条件（1 ページ）](#)を確認してください。

手順

	コマンドまたはアクション	目的
Step 1	クライアント識別コードの設定（2 ページ）を行うには、次のサブタスクを完了します。 <ul style="list-style-type: none"> • クライアント識別コードの追加（3 ページ） • クライアント識別コードの有効化（3 ページ） 	使用する予定の CMC リストが完成したら、そのコードをデータベースに追加して、ルートパターンで CMC 機能を有効にします。
Step 2	強制承認コードの設定（4 ページ）を行うには、次のサブタスクを完了します。 <ul style="list-style-type: none"> • 強制承認コードの追加（4 ページ） • 強制承認コードの有効化（4 ページ） 	使用する予定の FAC リストと認可レベルが決定したら、そのコードをデータベースに追加して、ルートパターンで FAC 機能を有効にします。

クライアント識別コードの設定

手順

	コマンドまたはアクション	目的
Step 1	クライアント識別コードの追加（3 ページ）	使用する一意のクライアント識別コードを決定し、システムに追加します。CMC の数は、システムの起動に要する時間の長さに直接影響するので、CMC の数を 60,000 までに制限してください。この最大数を超

	コマンドまたはアクション	目的
		える CMC を設定する場合は、遅延が非常に大きくなることに注意してください。
Step 2	クライアント識別コードの有効化 (3 ページ)	ルート パターンを介してクライアント識別コードを有効にします。

クライアント識別コードの追加

使用する一意のクライアント識別コードを決定し、システムに追加します。CMC の数は、システムの起動に要する時間の長さ直接影响到するので、CMC の数を 60,000 までに制限してください。この最大数を超える CMC を設定する場合は、遅延が非常に大きくなることに注意してください。

手順

-
- Step 1** [Cisco Unified CM 管理 (Cisco Unified CM Administration)] から、以下を選択します。 **コールルーティング > クライアントの区別コード**。
 - Step 2** [新規追加] をクリックします。
 - Step 3** [クライアント識別コード (Client Matter Code)] フィールドで、通話の発信時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。
 - Step 4** [説明 (Description)] フィールドに、クライアント識別コードを特定する場合のクライアント名を入力します。
 - Step 5** [保存] をクリックします。
-

クライアント識別コードの有効化

ルート パターンを介してクライアント識別コードを有効にします。

始める前に

[クライアント識別コードの追加 \(3 ページ\)](#)

手順

-
- Step 1** Cisco Unified CM Administration から、[**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。
 - Step 2** 次のいずれかの操作を実行します。
 - 既存のルートパターンを更新するには、検索条件を入力し、[**検索 (Find)**] をクリックして、結果リストからルートパターンを選択します。
 - 新規ルートパターンを作成するには、[**新規追加**] をクリックします。

- Step 3** [ルート パターンの設定 (Route Pattern Configuration)] ウィンドウで、[クライアント識別コードの要求 (Require Client Matter Code)] チェックボックスをオンにします。
- Step 4** [保存] をクリックします。

強制承認コードの設定

手順

	コマンドまたはアクション	目的
Step 1	強制承認コードの追加 (4 ページ)	使用する一意の強制承認コードを定義し、システムに追加します。
Step 2	強制承認コードの有効化 (4 ページ)	ルートパターンを介して強制承認コードを有効にします。

強制承認コードの追加

この手順を使用して、使用する一意の強制承認コードを定義し、システムに追加します。通話を正常にルーティングするためには、ユーザ認可レベルが通話のルートパターンに指定されている認可レベル以上である必要があります。

手順

- Step 1** [Cisco Unified CM の管理 (Cisco Unified CM Administration)] から、[コール ルーティング (Call Routing)] > [強制承認コード (Forced Authorization Codes)] を選択します。
- Step 2** [承認コード名 (Authorization Code Name)] フィールドに、一意の名前を 50 文字以内で入力します。
この名前は、認証コードを特定のユーザまたはユーザ グループに結び付けます。
- Step 3** [承認コード (Authorization Code)] フィールドに、一意の承認コードを 16 桁以内で入力します。
ユーザは、FAC 有効ルートパターンを介してコールを発信するときに、このコードを入力します。
- Step 4** [承認レベル (Authorization Level)] フィールドに、3 桁の承認レベルを 0 ~ 255 の範囲で入力します。
- Step 5** [保存] をクリックします。

強制承認コードの有効化

この手順を使用して、ルートパターンを介して強制承認コードを有効にします。

手順

- Step 1** Cisco Unified CM Administration から、[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。
- Step 2** 次のいずれかの操作を実行します。
 - [検索（Find）] をクリックし、結果のリストからルートパターンを選択して、既存のルートパターンを更新します。
 - [新規追加（Add New）] をクリックして、新しいルートパターンを作成します。
- Step 3** [ルートパターンの設定（Route Pattern Configuration）] ウィンドウで、[強制承認コードが必要（Require Forced Authorization Code）] チェックボックスをオンにします。
- Step 4** [認可レベル（Authorization Level）] フィールドに、0～255の間で認可レベルの値を入力します。
ルーティングを成功させるには、ユーザの FAC レベルをコールの設定レベルと等しいか、またはそれよりも大きくする必要があります。
- Step 5** [保存] をクリックします。

クライアント識別コードと強制承認コードの連携動作

表 1: クライアント識別コードと強制承認コードの連携動作

機能	データのやり取り
CDR 分析とレポート (CAR)	CDR Analysis and Reporting (CAR) を使用すれば、クライアント識別コード (CMC)、強制承認コード (FAC)、承認レベルに関するコール詳細を提示するレポートを実行できます。
CTI、JTAPI、および TAPI アプリケーション	ほとんどの場合、システムは、ユーザがコール中にコードを入力する必要がある CTI、JTAPI、TAPI アプリケーションに警告できます。ユーザがコールを発信したり、アドホック会議を作成したり、CMC 対応または FAC 対応ルートパターン経由で打診転送を実行したりする場合は、トーンの受信後にコードを入力する必要があります。 ユーザが CMC 対応または FAC 対応ルートパターン経由でコールをリダイレクトまたはブラインド転送した場合は、トーンが流れないため、アプリケーションでコードを Cisco Unified Communications Manager に送信する必要があります。システムが適切なコードを受信すると、コールが意図した通話相手に接続されます。システムが適切なコードを受信しなかった場合、Cisco Unified Communications Manager は、コードが見つからないことを示すエラーをアプリケーションに送信します。

機能	データのやり取り
Cisco Web Dialer	<p>Web Dialer は、次の方法で CMC と FAC をサポートします。</p> <ul style="list-style-type: none"> • ユーザは、WD HTML ページまたは SOAP 要求のダイヤル テキストボックスに接続先番号を入力してから、電話機に手動で CMC または FAC を入力できます。 • ユーザは、WD HTML ページまたは SOAP 要求のダイヤル テキストボックスに、接続先番号に続けて、FAC または CMC を入力できます。 <p>たとえば、接続先番号が 5555、FAC が 111、CMC が 222 の場合は、5555111# (FAC)、5555222# (CMC)、または 5555111222# (CMC と FAC) をダイヤルすることにより、コールを発信できます。</p> <p>(注)</p> <ul style="list-style-type: none"> • WebDialer は、接続先番号の検証を行いません。電話機が必要な検証を処理します。 • ユーザがコードを入力しない場合、または誤ったコードを入力した場合、コールは失敗します。 • ユーザが特殊文字を含む DN を使って WebApp からコールを発信した場合は、特殊文字を削除するとコールが正常に動作します。SOAP UI にはこのルールは該当しません。
スピードダイヤルと短縮スピードダイヤル	<p>スピードダイヤルを使用して、FAC、CMC、ダイヤル中のポーズ、追加の桁（ユーザの内線番号、会議へのアクセスコード、ボイスメールのパスワードなど）が必要な接続先に到達できます。ユーザが設定されたスピードダイヤルを押すと、電話機が接続先番号へのコールを確立して、指定された FAC、CMC、ダイヤル中のポーズが挿入された追加の桁を送信します。</p>

クライアント識別コードと強制承認コードの制約事項

表 2: クライアント識別コードと強制承認コードの制約事項

制約事項	説明
アナログ ゲートウェイ	H.323 アナログ ゲートウェイではトーンを再生できないため、この種類のゲートウェイでは CMC や FAC はサポートされていません。

制約事項	説明
通話転送	<p>コードを入力するユーザがないため、CMC や FAC が有効になっているルートパターンに転送されるコールは失敗します。ユーザが [不在 (CFwdALL)] ソフトキーを押して CMC や FAC がルートパターン上で有効になっている番号を入力すると、コール転送は失敗します。</p> <p>呼処理の中断を最小限に抑えるには、コール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、転送したい番号をダイヤルしてみます。コードの入力を求められたら、その番号ではコール転送は設定できません。転送されたコールが意図した接続先に届かないことから生じる苦情の数を削減するために、ユーザにこの方法を勧めてください。</p>
Cisco Unified Mobility	SIP トランク、H.323 ゲートウェイ、MGCP ゲートウェイから発信されているコールが、CMC または FAC が必須のルートパターンに遭遇し、発信者に Cisco Unified Mobility が設定されていない場合、コールは失敗します。
Dial via Office コールバック番号	Cisco Mobility の CMC および FAC 機能では、Dial via Office (DVO) コールバック番号としての代替番号はサポートされていません。DVO コールバック番号は、[モビリティID (Mobility Identity)] ウィンドウで登録されている番号である必要があります。
フェールオーバーコール	CMC および FAC は、フェールオーバー コールとは連動しません。
聴覚障がいのあるユーザ	電話番号をダイヤル後、聴覚障がいのあるユーザが認証コードやクライアント識別コードを入力するまでに 1 ～ 2 秒間待機する必要があります。
ローカリゼーション	シスコでは、CMC や FAC をローカライズしていません。CMC および FAC 機能は、Cisco Unified Communications Manager でサポートされているすべてのロケールで同じデフォルトのトーンを使用します。 (注) Cisco Mobility では、CMC と FAC はローカライズされています。
オーバーラップ送信	Cisco Unified Communications Manager ではユーザにいつコードの入力を求めればよいかを判断できないため、CMC および FAC 機能はオーバーラップ送信をサポートしません。[ルートパターン設定 (Route Pattern Configuration)] ウィンドウで [強制承認コードが必須 (Require Forced Authorization Code)] や [クライアント識別コードが必須 (Require Client Matter Code)] のチェックボックスをオンにすると、自動的に [オーバーラップ送信を許可 (Allow Overlap Sending)] のチェックボックスはオフになり、逆もまた同様です。
スピードダイヤルボタン	CMC や FAC で短縮ダイヤルボタンの設定をすることはできません。システムに入力を求められた場合、コードを入力する必要があります。

