MRA デバイスの導入準備

アクティベーションコードによるMRAデバイスの導入準備

アクティベーションコードは、モバイルおよびリモートアクセス（MRA）用のリモートエンドポイントの導入準備をするためのシンプルで安全な方法を提供します。この機能により、MRAユーザーが初めて電話を使用するときにオンプレミスにいる必要がなくなります。リモートユーザーは、電話を接続し、アクティベーションコードを入力すると、通話を開始できます。

この機能は、導入準備に対応するため、Cisco Cloud を活用します。管理者は Cisco Unified Communications Manager をクラウドに導入し、デバイスアクティベーション中にすべてのリモート MRA ユーザーが接続する Expressway クラスタでクラスタ全体の MRA アクティベーションドメインを指定します。

複数の Expressway クラスタがある場合、MRA サービスドメインを使用すると、電話機が登録する Expressway を指定できます。電話機がアクティブ化されると、電話機は構成ファイルをダウンロードします。このファイルには、その電話機に割り当てられている Expressway クラスタを持つ MRA サービスドメインへのリダイレクトが含まれています。

アクティベーションコードとは何ですか。

アクティベーションコードは、1 回だけ使用できる 16 桁の値であり、電話機を登録する前にユーザーが電話機に入力する必要があります。ユーザーは正しいコードを入力する必要があります。入力しないと、電話が登録されません。アクティベーションコードは、電話機を安全に導入するメソッドであり、管理者が手動で個々の電話機の MAC アドレスを収集して入力する必要がありません。

カスタム証明書（オプション）

独自の証明書を使用する場合は、クラウドを使用して証明書をMRA電話機に配布し、Expresswayとの信頼を確立できるようにします。このオプションでは、証明書を最初にExpresswayにアップロードしてから、Cisco Unified Communications Manager の **PhoneEdge-trust** ストアにアップロードする必要があります。証明書は Cisco Cloud にアップロードされるため、デバイスのアクティベーションプロセス中に電話機が証明書をダウンロードできます。

MRA 導入準備プロセスフロー

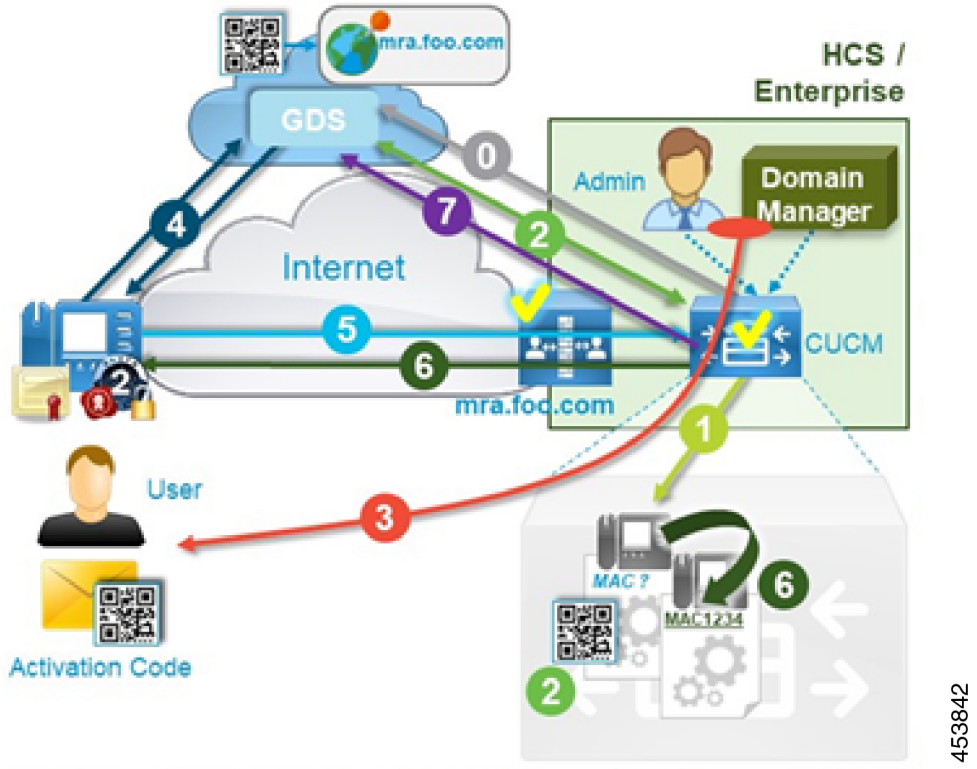
次の表には、MRAモードでのデバイスアクティベーションコード導入準備による新しいMRA電話の導入準備のプロセスフローが含まれています。プロセスの図については、番号の付いた各手順を後続の図と一致させてください。

（注） UCM パブリッシャでデバイス アクティベーション サービスを開始して、モバイルおよびリモートアクセス経由でクライアントの導入準備をする場合は、UDS および CCM サービスも開始する必要があります。サーバーが更新されない場合は、Expressway-C の Unified Communications 構成の UCM クラスタを削除または再検出します。

プロセス手順	プロセスの流れ
0	管理者は Cloud 導入準備を構成し、MRA アクティベーションドメインと MRA サービスドメインを指定します。
1	管理者は、MAC アドレスを指定せずに完全なデバイス構成をプロビジョニングします。デバイス名は、ランダムな BAT MAC アドレスになります。
2	管理者が、このデバイスのアクティベーション コードを要求します。デバイスアクティベーションサービスは、クラウドベースのデバイスアクティベーション サービスからコードを要求します。
3	アクティベーションコードがユーザーに送信されます（E メールまたはセルフケア ポータル経由）。
4	ユーザーがアクティベーションコードを入力します。電話機はクラウドからMRAターゲットを取得します。
5	電話機はExpresswayの場所を学習し、SRPハンドシェイクでMIC+アクティベーションコードを使用して認証します。
6	デバイス アクティベーション サービスが電話機の MAC を使用してデータベース内のデバイス構成を更新し、成功したことを電話機に送信します。

プロセス手順	プロセスの流れ
7	電話機が登録され、その電話機の TFTP からの固有構成ファイルを取得し、Unified CM に登録されます。電話機が別の MRA サービスドメインに割り当てられている場合、構成ファイルにリダイレクトされます。その後、電話機は MRA サービスドメインを使用して登録できます。
8	デバイスアクティベーションサービスは、クラウドからアクティベーションコードをリリースします。コードは今後再利用できます。

図 *1:* アクティベーションコードによる *MRA* デバイス導入準備プロセス



デバイスの導入準備の前提条件

次の表に、MRA エンドポイントのアクティベーションコード導入準備のサポート情報を示します。

表 *1: MRA* アクティベーションコード導入準備サポート情報

サポート	詳細
最小リリース	Expressway X12.5.1 Cisco Unified Communications Manager 12.5(1)SU1 Cisco IP Phone ファームウェア 12.5(1)SR3
サポートされるエンドポイント	Cisco IP Phones 7811、7821、7832、7841、7861、8811、8832、8832NR、8841、8845、8851、8851NR、8861、8865、8865NR

（注） リリース X14.0 の時点で、モバイルおよびリモートアクセス用にサポートされている Cisco IP Phone 78xx シリーズおよび 88xx シリーズを導入準備している場合、 電話は、**Cisco Unified Communications Manager** の **[電話構成（Phone Configuration）]** ウィンドウで **[MRAを介したアクティベーションコードを許可（Allow Activation Code via MRA）]** チェックボックスがオンになっている場合のみ、MRA モードに切り替えられます。

このアプローチを使用して、MRA 電話のアクティベーションコード導入準備を設定する必要があります。さらに、MRA 電話のユーザーは、電話機をアクティブにして使用するために正しいアクティベーションコードを入力する必要があります。

アクティベーションコードの導入準備についての詳細は、『*Cisco Unified Communications Manager* 向け機能構成ガイド』の「アクティベーションコードを介したデバイスの導入準備」章を参照してください。

さらに、次の前提条件があります。

- X12.5 より前のリリースから Expressway をアップグレードした場合は、この機能を設定する前に Expressway-C の Unified CM サーバーを更新してください。Expressway-C で、**[構成（Configuration）]** > **[Unified Communications]** > **[Unified CMサーバー（Unified CM servers）]** の順に選択し、**[サーバーを更新（Refresh servers）]** をクリックします。
- **Cisco デバイス アクティベーション サービス**—このサービスは、Cisco Unified Communications Manager で実行する必要があります（サービスはデフォルトで実行されます）。Cisco Unified Serviceability のサービスのリストをチェックして、サービスが実行されていることを確認します。
- **OAuth リフレッシュ ログイン**—この機能は、**OAuth Refresh Login Flow** 企業パラメータを **[有効（Enabled）]** に設定し、Cisco Unified Communications Manager で有効にします。
- **セルフケアポータル**—ユーザーがセルフケアポータルを使用して、電話をアクティブ化させる場合に使用します。
  - **Show Phones Ready to Activate** 企業パラメータは、Cisco Unified Communications Manager で **[True]** に設定します。

- エンドユーザーはポータルへのログインアクセスが必要です。セルフケア構成詳細の「*Cisco Unified Communications Manager* 用機能構成ガイド」の「セルフケアポータル」章を参照してください。
- セルフケアポータルは、MRA ではサポートされていないので、リモートユーザーは、VPN を使用してポータルにアクセスする必要があります。

- **ドメインネームシステム（DNS）SRV レコード**—MRA アクティベーション ドメインと MRA サービスドメインの場合、適切な Expressway クラスタを指す *_collab_edge* SRV を構成する必要があります。
- **シスコクラウドオンボーディングの TCP ポート 443 ネットワーク要件**：シスコクラウドへの次の URL/接続を行うために、Cisco Unified Communications Manager と IM and Presence Service/パブリッシャからポート 443 を介して接続を有効にする必要があります。
  - fos-a.wbx2.com
  - idbroker.webex.com
  - push.webexconnect.com
  - btpush.webexconnect.com

（注） TCP ポート 443 は、アウトバウンド HTTPS リクエストの場合は Cisco Unified CM のパブリッシャノードから開いている必要があります（シスコクラウドオンボーディング）。

MRA デバイス導入準備の構成フロー

以下の手順に従って、MRA モードでアクティベーションコードを使用して MRA デバイスの導入準備を構成します。

手順	手順
ステップ 1	Cisco Unified Communication Manager および Expressway で OAuth 認証を有効にします。 **1.** Cisco Unified CM で OAuth を有効にする方法 **1.** Cisco Unified CM Administrationで、**[システム（System）]** > **[企業パラメータ（Enterprise Parameters）]**の順に選択します。 **2.** **OAuth Refresh Login Flow**パラメータを **[有効（Enabled）]** に設定します。 **3.** [保存（Save）] をクリックします。 **2.** Expressway で OAuth 更新認証を有効にする方法 **1.** **[構成（Configuration）]** > **[Unified Communications]** > **[構成（Configuration）]** > **[MRAアクセス制御（MRA Access Control）]**の順に選択します。 **2.** **[OAuth トークンによる承認（更新あり）（Authorize by OAuth token with refresh）]** を **オン**にします。 **3.** **[保存（Save）]** をクリックします。
ステップ 2	MRA アクティベーションコードの導入準備のために、Cisco Unified Communication Manager をクラウドに導入準備します。 **1.** Cisco Unified CM の管理から、**[詳細機能（Advanced Features）]** > **[Cisco Cloud 導入準備（Cisco Cloud Onboarding）]** を選択します。 **2.** **[バウチャーを生成（Generate Voucher）]** ボタンをクリックします。 **3.** **[Cisco Cloudでアクティベーションコードの導入準備を有効化（Enable Activation Code Onboarding with Cisco Cloud）]** チェックボックスをオンにします。 **4.** **MRA アクティベーションドメイン** を指定します。 **5.** [保存（Save）] をクリックします。 （注） • MRA アクティベーションドメインの Collab-edge ドメインネームシステム（DNS）レコードが存在する必要があります。 • クラスタごとに 1 つの MRA アクティベーションドメインの制限があります。MRA アクティベーションは、MRA サービスドメインのリストに自動的に追加されます。

手順	手順
ステップ 3	MRA サービスドメインを設定します。 **1.** Cisco Unified CM Administrationで、**[高度な機能（Advanced Features）]** > **[MRA サービスドメイン（MRA Service Domains）]**の順に選択します。 **2.** 複数の Expressway クラスタがある場合は、MRA エンドポイントが動作する各ドメインを追加します。 **3.** ドメインをクラスタ全体のデフォルト MRA サービスドメインとして適用する場合は、**[IsDefault]** チェックボックスをオンにします。 **4.** [保存（Save）] をクリックします。
ステップ 4	オプション。MRA サービスドメインを既存のデバイスプールに割り当てます。これにより、デバイスプールを使用するすべての MRA デバイスに特定の Expressway クラスタを割り当てることができます。 **1.** Cisco Unified CM Administration で、**[システム（System）]** > **[デバイスプール（Device Pool）]**の順に選択します。 **2.** **[検索（Search）]** をクリックして、適切なデバイスプールを選択します。 **3.** **[MRAサービスドメイン（MRA Service Domain）]**ドロップダウンから、このデバイスプールを使用するデバイスに割り当てるドメインを選択します。 **4.** [保存（Save）] をクリックします。
ステップ 5	アクティベーションコードの導入準備を許可するように MRA アクセス制御を構成します。 **1.** Expressway-C で、**[構成（Configuration）]** > **[Unified Communications]** > **[構成（Configuration）]**の順に選択します。 **2.** **[OAuth トークンによる承認（更新あり）（Authorize by OAuth token with refresh）]** を **オン**にします。 **3.** **[アクティベーションコードの導入準備を許可する（Allow activation code onboarding）]** を **[はい（Yes）]** に設定します。

手順	手順
ステップ 6	インストールされている信頼できる Cisco Manufacturing Installed Certificates（MIC）を確認します。これは、アクティベーションコードの導入準備機能にアクセスするために必要です。 （注） オンボードアクティビティを実行するには、シスコの製造ルート証明書が *CallManager-trust* ストアに存在している必要があります。 **1.** Expressway-E で、**[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [信頼できるCA証明書（Trusted CA certificates）]**の順に選択します。 **2.** **[信頼できるCA証明書を導入準備するアクティベーションコード（Activation code onboarding trusted CA certificates）]** をクリックします。
ステップ 7	オプション。独自のカスタム証明書を使用する場合、 **1.** Expressway に証明書をアップロードします。 **2.** Unified Communications Manager の PhoneEdge-trust に証明書をアップロードします。 Unified Communications Manager がクラウドに証明書をアップロードします。アクティベーションプロセス中に、電話機はクラウドから証明書をダウンロードするため、電話機が Expressway と通信できるようになります。
ステップ 8	許可されているプロビジョニング方法を使用して、Cisco Unified Communications Manager データベースで電話機をプロビジョニングします。どちらのオプションを選択する場合でも、次のチェックボックスが両方ともオンになっていることを確認してください。 • **アクティベーションコードの導入準備が必要（Requires Activation Code Onboarding ）** • **MRA 経由のアクティベーションコードを許可（Allow Activation Code via MRA）** （注） 電話機にダミーの MAC アドレスをプロビジョニングできます。導入準備プロセスでは、電話機の実際の MAC アドレスを使用して**デバイス名**を更新します。 GUI または バルク管理者のどちらかを使用したサンプルプロビジョニング手順については、 *Cisco Unified Communications Manager* システム構成ガイド、リリース *12.5(1)SU1* 以降の「アクティベーションコードによるデバイス導入準備」章を参照してください。
ステップ 9	電話を MRA ユーザーに発送します。

電話機のアクティブ化

管理者には、電話機ユーザーにアクティベーションコードを送信するための2つのオプションがあります。

- セルフケアポータル — 電話機ユーザーはポータルにログインして、電話のアクティベーションコードと付随するバーコードを表示できます。アクティベーションコードを電話機に入力するか、電話機のビデオカメラを使用してバーコードをスキャンします。どちらの方法でも機能します。セルフケアの要件については、デバイス導入準備の前提条件を確認してください。
- CSV ファイルのエクスポート — 管理者は、Cisco Unified Communications Manager で、未処理のアクティベーションコードと関連するユーザの csv ファイルをエクスポートできます。このファイルの内容を使用して、MRA ユーザーにアクティベーションコードを通知できます。csv ファイルをエクスポートする方法

  1. Cisco Unified CM Administration から、**[デバイス（Device）]** > **[電話（Phone）]** を選択します。
  2. [関連リンク（Related Links）] から [アクティベーションコードのエクスポート（Export Activation Codes）] を選択し、[移動（Go）] をクリックします。

（注） アクティベーションコードのデフォルトの有効期間は 168 時間（7 日間） です。この値は、Cisco Unified Communications Manager の **Activation Time to Live (Hours)** サービスパラメータを使用して再構成できます。アクティベーションコードの有効期限が切れた場合、管理者は **[アクティベーションコードの解放（Release Activation Code）]** をクリックし、**[電話機の構成（Phone Configuration）]** ウィンドウの **[新しいアクティベーションコードを生成（Generate New Activation Code）]** をクリックすると、アクティベーションコードをリセットできます。

アクティベーションコードの入力

MRA ユーザーが電話機を接続すると、アクティベーションコードを入力するように求められます。アクティベーションコードを入力するか、セルフケアポータルに表示されるバーコードをスキャンすると、電話機が起動するので、構成ファイルをダウンロードして登録します。

これで、電話機を使用できる状態になりました。

安全な導入準備のための追加オプション

次のオプションは、セキュリティを強化するために構成プロセスをわずかに変更します。

オプション 1：管理者が実際の MAC アドレスを使用して電話をプロビジョニングする

管理者は、ダミーの MAC アドレスを使用するのではなく、実際の MAC アドレスを使用して電話機を Cisco Unified Communications Manager に追加します。この方法では、アクティベーションコードが実際の電話機の MAC アドレスに関連付けられ、アクティベーションコードがその電話機でのみ機能するため、セキュリティが強化されます。ただし、この方法では、管理者が各電話機の MAC アドレスを個別に収集して入力する必要があります。

オプション 2：管理者は、MRA モードでの再導入準備のためにリモートユーザーに送信する前に、オンプレミスの電話をアクティブ化します。

この方法では、管理者は、アクティベーションコード要件をリセットして MRA ユーザーに出荷する前に、オンプレミスモードで電話をアクティブ化します。MRA ユーザーは、電話を MRA モードでアクティブ化します。

- 管理者はアクティベーションコード導入準備（オンプレミスモード）を設定し、電話機にダミーの MAC アドレスをプロビジョニングします。
- 管理者は、オンプレミス環境で電話の導入準備をして登録します。このプロセスにより、Cisco Unified Communications Manager の**デバイス名**が実際の電話機の MAC アドレスで更新され、電話機がファームウェアロードを更新できるようになります。
- 管理者は MRA モードのアクティベーションコード導入準備を設定し、アクティベーションコード要件をリセットして、新しいコードが入力されるまで電話をロックします。

（注） **[電話機の構成（Phone Configuration）]** ウィンドウで、アクティベーションコードをリセットして電話をロックするため、次の両方のチェックボックスをオンにする必要があります。

- **アクティベーションコードの導入準備が必要（Requires Activation Code Onboarding ）**
- **MRA 経由のアクティベーションコードを許可（Allow Activation Code via MRA）**

- 管理者は電話機を MRA ユーザーに発送し、ユーザーに新しいアクティベーションコードを通知します。
- リモート MRA ユーザーは、電話機を使用するために新しいアクティベーションコードを入力する必要があります。

このオプションには次の利点があります。

- アクティベーションコードは MAC アドレスに関連付けられ、その電話でのみ機能するため、セキュリティが向上します。
- ユーザーが電話機を受け取ったときに、電話機のファームウェアがすでに最新であることを確認します。

- 管理者が個別の MAC アドレスを収集して入力する必要はありません。

オンプレミスモードでのアクティベーションコード導入準備の構成方法については、『*Cisco Unified Communications Manager* 向けシステム構成ガイド』「アクティベーションコード」章の「オンプレミスタスク」を参照してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。