



サービス ディスカバリの設定

- [サービス ディスカバリのオプション, 1 ページ](#)
- [DNS SRV レコードの確認, 2 ページ](#)
- [カスタマイゼーション, 3 ページ](#)
- [手動接続設定, 11 ページ](#)

サービス ディスカバリのオプション

サービス ディスカバリにより、クライアントは自動的に企業のネットワークでサービスを検出することができます。次のいずれかのオプションを使用してサービス ディスカバリを設定できます。

オプション	説明
DNS SRV レコードの確認, (2 ページ)	クライアントはサービスを自動的に検出して接続します。 これは推奨オプションです。
カスタマイゼーション, (3 ページ)	インストール パラメータ、URL の設定、または企業モビリティ管理を使用してサービス検出をカスタマイズできます。
手動接続設定, (11 ページ)	手動接続設定は、サービス ディスカバリが使用されていない場合にフォールバック メカニズムを提供します。

DNS SRV レコードの確認

はじめる前に

『*Planning Guide for Cisco Jabber*』の「*Service Discovery*」の章で、SRV レコードの要件を確認してください。

手順

展開用のSRV レコードの作成：

オプション	説明
_cisco-uds	Cisco Unified Communications Manager バージョン 9.0 以降の場所を提供します。クライアントは Cisco Unified Communications Manager からサービス プロファイルを取得してオーセンティケータを特定できます。
_collab-edge	Cisco VCS Expressway または Cisco Expressway-E の場所を提供します。クライアントは Cisco Unified Communications Manager からサービス プロファイルを取得してオーセンティケータを特定できます。

SRV レコードの例

```
_cisco-uds._tcp.DOMAIN service location:
priority = 0
weight = 0
port = 8443
svr hostname=192.168.0.26
```

次の作業

[SRV レコードのテスト](#), (2 ページ)

SRV レコードのテスト

SRV レコードを作成したら、それらがアクセス可能かどうかを確認するためにテストします。

手順

-
- ステップ 1 コマンド プロンプトを開きます。
 - ステップ 2 nslookup と入力します。
デフォルトの DNS サーバおよびアドレスが表示されます。これが想定された DNS サーバであることを確認してください。
 - ステップ 3 set type=SRV と入力します。
 - ステップ 4 各 SRV レコードの名前を入力します。

例 : `_cisco-uds.exampledomain`

- サーバとアドレスが表示される : SRV レコードにアクセスできます。
- 「`_cisco-uds.exampledomain: Non-existent domain`」 と表示される : SRV レコードに関する問題が存在します。

カスタマイゼーション

Windows のカスタマイゼーション

インストーラ スイッチ : Cisco Jabber for Windows

Cisco Jabber をインストールするときに、オーセンティケータとサーバアドレスを指定できます。インストーラは、ブートストラップファイルにこれらの詳細を保存します。ユーザがクライアントを初めて起動した際に、ブートストラップファイルを読み取ります。サービスディスカバリが展開されている場合は、ブートストラップファイルが優先されます。

ブートストラップファイルは、サービスディスカバリが展開されていない場合やユーザに手動で自分の接続設定を指定させたくない場合に、サービスディスカバリのフォールバックメカニズムを提供します。

クライアントは、最初に起動したときのみ、ブートストラップファイルを読み取ります。クライアントは、最初の起動後にサーバアドレスと設定をキャッシュし、以降の起動ではキャッシュからロードします。

Cisco Unified Communications Manager リリース 9.x 以降を使用したオンプレミス展開では、ブートストラップファイルを使用せず、代わりに、サービスディスカバリを使用することをお勧めします。

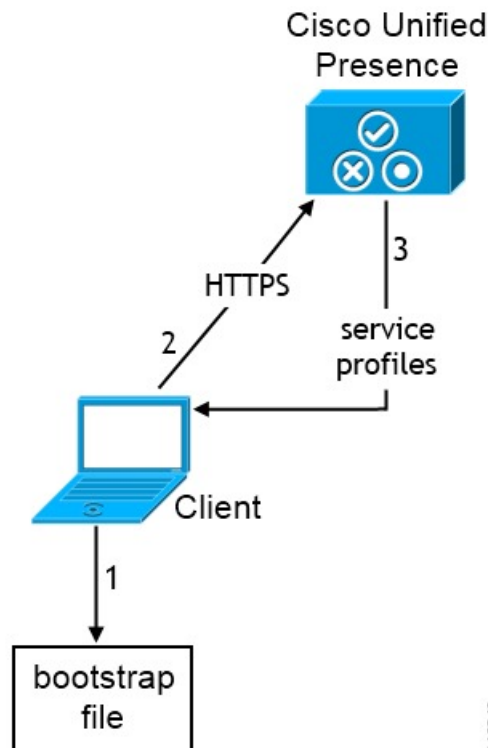
オンプレミスでの展開のブートストラップの設定

次の表は、さまざまな展開タイプの引数値を示します。

製品モード	サーバのリリース	引数値
フル UC (デフォルトモード)	リリース 9 以降 : <ul style="list-style-type: none"> • Cisco Unified Communications Manager • Cisco Unified Communications Manager IM and Presence Service 	次のインストーラ スイッチと値を使用する。 <ul style="list-style-type: none"> • AUTHENTICATOR=CUP • CUP_ADDRESS= <presence_server_address>

製品モード	サーバのリリース	引数値
IM 専用 (デフォルトモード)	リリース 9 以降 : Cisco Unified Communications Manager IM and Presence Service	次のインストーラ スイッチと値を使用する。 <ul style="list-style-type: none"> • AUTHENTICATOR=CUP • CUP_ADDRESS= <presence_server_address>

次の図は、クライアントがオンプレミスでの展開の場合、ブートストラップ設定の使用法を示しています。



348840

ユーザがクライアントを初めて起動する際に、次が実行されます。

- 1 クライアントは、ブートストラップファイルから設定を取得します。

クライアントが、デフォルトモードで起動して、Cisco Unified Communications Manager IM and Presence サービスがオーセンティケータであると判断します。クライアントは、サービスディスカバリの結果により、その他の指示がなされない限り、プレゼンスサーバのアドレスを取得します。

- 2 クライアントが Cisco Unified Communications Manager IM and Presence サービスから認証され、設定を取得します。

- 3 クライアントは、プレゼンス サーバからサービス プロファイルを取得します。

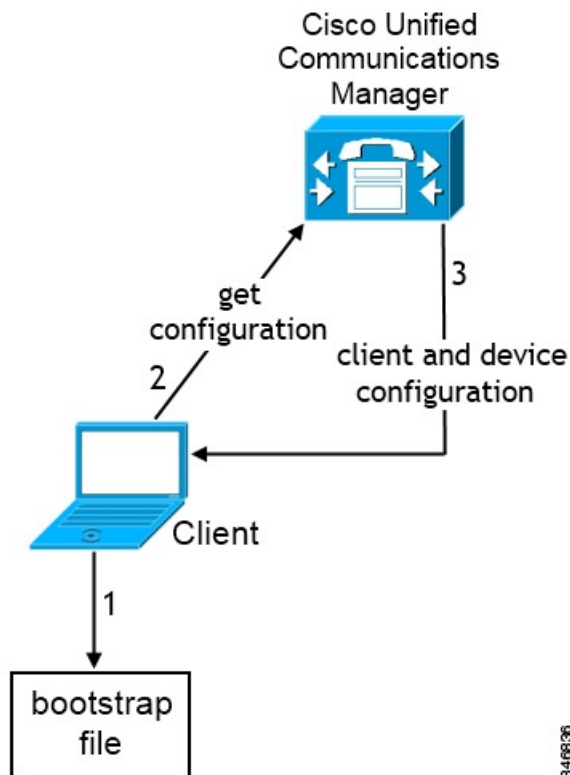
電話モードのオンプレミスの展開におけるブートストラップの設定

インストール中に、次のように引数の値を設定します。

- AUTHENTICATOR の値として CUCM を設定します。
- PRODUCT_MODE の値として phone_mode を設定します。
- TFTP の値として TFTP サーバアドレスを設定します。
- CTI の値として CTI サーバアドレスを設定します。
- CCMCIP の値として CCMCIP サーバアドレスを設定します。

Cisco Unified Communications Manager リリース 9.x 以前 : Cisco Extension Mobility を有効にする場合は、CCMCIP に使用される Cisco Unified Communications Manager ノードで Cisco Extension Mobility サービスをアクティブにする必要があります。Cisco Extension Mobility の詳細については、使用している Cisco Unified Communications Manager のリリースに応じた『Feature and Services』ガイドを参照してください。

次の図は、電話モードの展開において、クライアントがブートストラップ設定をどのように使用できるかを示したものです。



3-46836

ユーザがクライアントを初めて起動する際に、次プロセスが実行されます。

- 1 クライアントは、ブートストラップ ファイルから設定を取得します。

クライアントが電話モードで起動して、Cisco Unified Communications Manager がオーセンティケータであると判断します。クライアントは、サービス ディスカバリの結果が定まらない場合に、TFTP サーバ（および Jabber for Windows と Jabber for Mac の場合の CTI サーバ）のアドレスも取得します。

- 2 クライアントが Cisco Unified Communications Manager から認証され、設定を取得します。
- 3 クライアントは、デバイスおよびクライアント設定を取得します。

Mac およびモバイルのカスタマイゼーション

構成 URL ワークフロー

手順

	コマンドまたはアクション	目的
ステップ 1	構成 URL , (6 ページ)	
ステップ 2	Web サイトからの構成 URL のユーザへの提供 , (9 ページ)	

構成 URL

ユーザが手動でサービス ディスカバリ情報を入力しなくても Cisco Jabber を起動できるようにするには、構成 URL を作成してユーザに配布します。

電子メールで直接、ユーザにリンクを送信するか、Web サイトにリンクを掲載することで、ユーザに構成 URL リンクを提供できます。

URL に次のパラメータを含めます。

- **ServicesDomain** : 必須。すべての構成 URL に Cisco Jabber でのサービス ディスカバリに必要な IM and Presence サーバのドメインを含める必要があります。
- **VoiceServiceDomain** : IM and Presence サーバのドメインが音声サーバのドメインと異なるハイブリッドクラウドベースのアーキテクチャを展開する場合にのみ必要です。Cisco Jabber が音声サービスを検出できるようにするために、このパラメータを設定します。
- **ServiceDiscoveryExcludedServices** : 任意。サービス ディスカバリ プロセスから次のサービスを除外できます。
 - WEBEX : この値を設定すると、クライアントは次のように動作します。

- CAS 検索を実行しません。

- 検索 :

- `_cisco-uds`
- `_cuplogin`
- `_collab-edge`

- CUCM : この値を設定すると、クライアントは次のように動作します。

- `_cisco-uds` を検索しません。

- 検索 :

- `_cuplogin`
- `_collab-edge`

- CUP : この値を設定すると、クライアントは次のように動作します。

- `_cuplogin` を検索しません。

- 検索 :

- `_cisco-uds`
- `_collab-edge`

カンマで区切った複数の値を指定して、複数のサービスを除外できます。

3つのサービスをすべて除外した場合、クライアントはサービス ディスカバリを実行せず、手動で接続設定を入力することをユーザに求めます。

- `ServicesDomainSsoEmailPrompt` : 任意。ユーザのホーム クラスタを決定する際に、ユーザに対して電子メール プロンプトを表示するかどうかを指定します。
 - ON
 - OFF
- `EnablePRTEncryption` : 任意。PRT ファイルの暗号化を指定します。Cisco Jabber for Mac で使用します。
 - true
 - false
- `PRTCertificateName` : 任意。証明書の名前を指定します。Cisco Jabber for Mac で使用します。
- `InvalidCertificateBehavior` : 任意。無効な証明書に対するクライアントの動作を指定します。
 - `RejectAndNotify` : 警告ダイアログが表示され、クライアントはロードされません。

- PromptPerSession : 警告ダイアログが表示され、ユーザは無効な証明書を受け入れるか、または拒否できます。
- PRTCertificateUrl : 信頼できるルート認証局の証明書ストアにある公開キーを含む証明書の名前を指定します。モバイルクライアント向け Cisco Jabber に適用されます。
- Telephony_Enabled : ユーザに対して電話機能を有効にするかどうかを指定します。デフォルトは true です。
 - はい (True)
 - いいえ (False)
- ForceLaunchBrowser : ユーザに外部ブラウザの使用を強制する場合に使用します。モバイルクライアント向け Cisco Jabber に適用されます。
 - はい (True)
 - いいえ (False)



(注) ForceLaunchBrowser は、クライアント証明書の展開および Android OS 5.0 よりも前のデバイスに使用されます。

- IP_Mode : Jabber クライアントのネットワーク IP プロトコルを指定します。
 - IPV4 のみ : Jabber は IPv4 接続のみ試行します。
 - IPV6 のみ : Jabber は IPv6 接続のみ試行します。
 - 2つのスタック (デフォルト) : Jabber は IPv4 または IPv6 のいずれかと接続できます。

構成 URL は次の形式で作成します。

```
ciscojabber://provision?ServicesDomain=<domain_for_service_discover>
&VoiceServicesDomain=<domain_for_voice_services>
&ServiceDiscoveryExcludedServices=<services_to_exclude_from_service_discover>
&ServicesDomainSsoEmailPrompt=<ON/OFF>
```




(注) パラメータには大文字と小文字の区別があります。構成 URL を作成する際は、次の表記を使用する必要があります。

- ServicesDomain
- VoiceServicesDomain
- ServiceDiscoveryExcludedServices
- ServicesDomainSsoEmailPrompt
- EnablePRTEncryption
- PRTCertificateURL
- PRTCertificateName
- InvalidCertificateBehavior
- Telephony_Enabled
- ForceLaunchBrowser
- IP_Mode

例

- ciscojabber://provision?ServicesDomain=cisco.com
- ciscojabber://provision?ServicesDomain=cisco.com
&VoiceServicesDomain=alphauk.cisco.com
- ciscojabber://provision?ServicesDomain=service_domain
&VoiceServicesDomain=voicesservice_domain&ServiceDiscoveryExcludedServices=WEBEX
- ciscojabber://provision?ServicesDomain=cisco.com
&VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM, CUP
- ciscojabber://provision?ServicesDomain=cisco.com
&VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM, CUP
&ServicesDomainSsoEmailPrompt=OFF

Web サイトからの構成 URL のユーザへの提供

電子メールで直接、ユーザにリンクを送信するか、Web サイトにリンクを掲載することで、ユーザに構成 URL リンクを提供できます。



(注) Android オペレーティングシステムの制約により、Cisco Jabber for Android ユーザが Android アプリケーションから直接構成 URL を開くと、問題が発生することがあります。この問題を回避するために、Web サイトを使用して構成 URL リンクを配布することをお勧めします。

URL プロビジョニングのために Web サイト探索オプションを使用する場合は、Mozilla Firefox を使用することをお勧めします。

Web サイトからリンクを配布するには、次の手順を実行します。

手順

-
- ステップ 1** HTML ハイパーリンクとして構成 URL を含む内部 Web ページを作成します。
- ステップ 2** 内部 Web ページへのリンクを電子メールでユーザに送信します。
その電子メールのメッセージで、次の手順を実行するようにユーザに指示します。
- 1 クライアントをインストールします。
 - 2 電子メール メッセージ内のリンクをクリックして、内部 Web ページを開きます。
 - 3 内部 Web ページ上のリンクをクリックして、クライアントを設定します。
-

企業モビリティ管理によるモバイルの設定

企業モビリティ管理 (EMM) を使用する前に、以下を確認してください。

- EMM ベンダーが Android for Work または Apple Managed App Configuration をサポートしている。
- Android デバイスの OS が 5.0 以降、または。

EMM を使用して、Cisco Jabber for Android や Cisco Jabber for iPhone and iPad に Cisco Jabber を設定することができます。EMM の設定の詳細については、EMM プロバイダーから提供される管理者用の説明書を参照してください。

Jabber をマネージドデバイスでのみ実行する場合、証明書ベースの認証を展開し、EMM を使用してクライアント証明書を登録できます。

EMM を使用するときは、EMM アプリケーションで AllowUrlProvisioning パラメータを False に設定し、URL 設定を無効にします。パラメータの設定の詳細は、『AllowUrlProvisioning Parameter』を参照してください。

EMM ベンダーは、アプリケーションの設定で様々な型の値を設定できますが、Cisco Jabber は String 型の値しか読み取りできません。

EMM では、jabber-config.xml ファイルの設定と同じパラメータを設定できます。EMM では次のパラメータを設定します。

- ServicesDomain
- VoiceServicesDomain
- ServiceDiscoveryExcludedServices
- ServicesDomainSsoEmailPrompt
- EnablePRTEncryption
- PRTCertificateURL

- PRTCertificateName
- InvalidCertificateBehavior
- Telephony_Enabled
- ForceLaunchBrowser
- FIPS_MODE
- AllowUrlProvisioning
- IP_Mode

FIPS_MODE パラメータ

EMMを使用してCisco Jabber モバイルクライアントのFIPS モードを有効または無効にするには、このパラメータを使用します。

- true : Cisco Jabber は FIPS モードです。
- false : Cisco Jabber は FIPS モードではありません。

例:<FIPS_MODE> false </FIPS_MODE>

AllowUrlProvisioning パラメータ

URL による設定から EMM に移行する場合、このパラメータを使用します。

このパラメータには次の値が適合します。

- true (デフォルト) : ブートストラップ設定は URL による設定により行われます。
- false : ブートストラップ設定は URL による設定では行われません。

例 : <AllowURLProvisioning>false</AllowURLProvisioning>

手動接続設定

手動接続設定は、サービス ディスカバリが使用されていない場合にフォールバック メカニズムを提供します。

Cisco Jabber を起動すると、[詳細設定 (Advanced settings)] ウィンドウでオーセンティケータとサーバアドレスを指定できます。クライアントは、その後の起動時にロードするローカルアプリケーション設定にサーバアドレスをキャッシュします。

Cisco Jabber は、次のような場合に、最初の起動時にこれらの詳細設定を入力するようにユーザに要求します。

- Cisco Unified Communications Manager リリース 9.x 以降を使用したオンプレミス : クライアントがサービス プロファイルからオーセンティケータとサーバアドレスを取得できない場合。

ユーザが [詳細設定 (Advanced settings)] ウィンドウで入力した設定は、SRV レコードやブートストラップの設定を含め、その他のソースよりも優先されます。

[Cisco IM & Presence] を選択すると、クライアントは Cisco Unified Communications Manager IM and Presence サービスから UC サービスを取得します。クライアントはサービス プロファイルまたは SSO 検出を使用しません。



(注) Cisco Jabber for Windows の場合、SRV レコードが解決されるサーバ数に関わらず、サービス検出は 20 秒後に停止します。サービス検出中に Cisco Jabber が `_cisco-uds` を検出すると、20 秒以内に最初の 2 つのサーバへの接続が試みられます。優先順位が高い 2 つのサーバに対するサービス検出の試行後は、Cisco Jabber はサーバへの接続を試みません。

ユーザは、稼働中のサーバを手動で指定するか、サービス検出の対象となる 2 つの優先順位の高いサーバのうち少なくとも 1 つのサーバを指定するように、SRV の優先順位を並べ替えることができます。

サービス ディスカバリの自動接続設定

[詳細設定 (Advanced settings)] ウィンドウで [自動 (Automatic)] オプションを選択することによって、サーバを自動で検出できます。

この自動オプションにより、ユーザがサービス接続の詳細を手動で設定する方法から、サービス ディスカバリを使用する方法に変更することができます。たとえば、最初の起動時に、[詳細設定 (Advanced settings)] ウィンドウで、手動でオーセンティケータを設定し、サーバアドレスを指定します。

クライアントは、手動設定のキャッシュを常にチェックします。手動設定は、SRV レコードより優先され、Cisco Jabber for Windows ではブートストラップ ファイルより優先されます。したがって SRV レコードを配置し、サービス ディスカバリを使用する場合は、最初の電源投入から手動設定を上書きする必要があります。

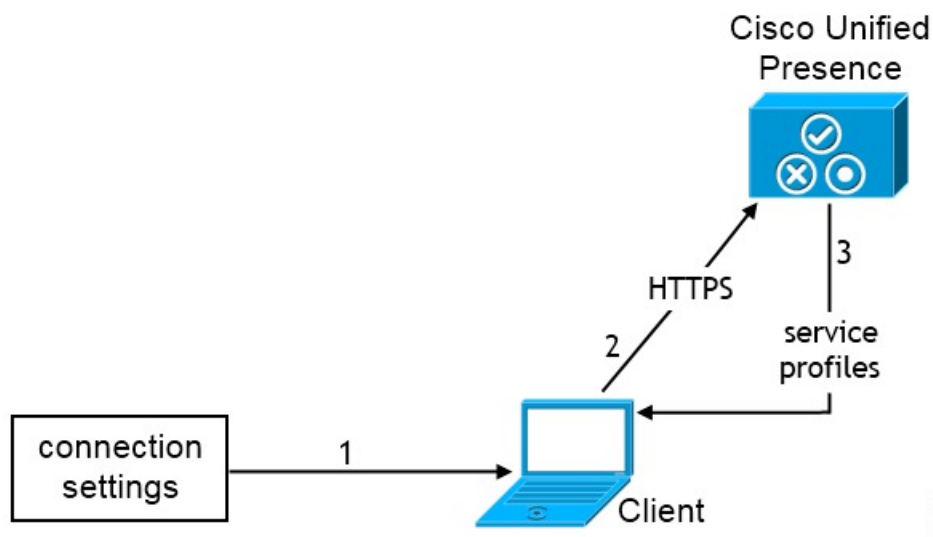
オンプレミスでの展開における手動接続設定

ユーザは、[詳細設定 (Advanced settings)] ウィンドウで、Cisco Unified Presence または Cisco Unified Communications Manager IM and Presence サービスをオーセンティケータとして設定し、サーバアドレスを指定できます。



メモ `_cuplogin` SRV レコードを使用して、デフォルトのサーバアドレスを自動的に設定することもできます。

次の図は、オンプレミスの展開において、クライアントが手動接続設定をどのように使用できるかを示したものです。



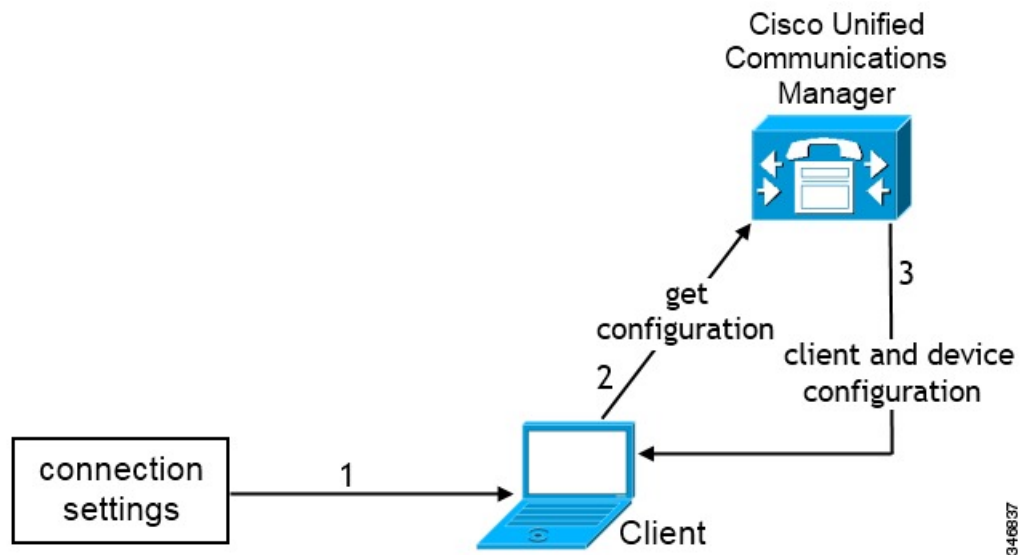
- 1 ユーザが [詳細設定 (Advanced settings)] ウィンドウで手動で接続設定を入力します。
- 2 クライアントが Cisco Unified Presence または Cisco Unified Communications Manager IM and Presence サービスの認証を受けます。
- 3 クライアントは、プレゼンス サーバからサービス プロファイルを取得します。

電話モードのオンプレミスの展開における手動接続設定

ユーザは、[詳細設定 (Advanced settings)] ウィンドウで、Cisco Unified Communications Manager をオーセンティケータに設定し、次のサーバアドレスを指定できます。

- TFTP サーバ (TFTP server)
- CCMCIP サーバ
- CTI サーバ (Cisco Jabber for Windows と Cisco Jabber for Mac)

次の図は、電話モードの展開において、クライアントが手動接続設定をどのように使用できるかを示したものです。



346837

- 1 ユーザが [詳細設定 (Advanced settings)] ウィンドウで手動で接続設定を入力します。
- 2 クライアントが Cisco Unified Communications Manager から認証され、設定を取得します。
- 3 クライアントは、デバイスおよびクライアント設定を取得します。