導入シナリオ

オンプレミス展開

オンプレミス展開とは、社内ネットワークのすべてのサービスをセットアップ、管理、保守する展開です。

次のモードで Cisco Jabber を展開できます。

- **フル UC**：フル UC モードを展開するには、インスタント メッセージングとプレゼンス機能を有効にし、ボイスメールと会議機能をプロビジョニングし、音声とビデオ用のデバイスを使用してユーザをプロビジョニングします。
- **IM 専用**：IM 専用モードを展開するには、インスタント メッセージングとプレゼンス機能を有効にします。 デバイスを使用してユーザをプロビジョニングしないでください。
- **電話機モード**：電話機モードでは、ユーザのプライマリ認証が Cisco Unified Communications Manager で行われます。 電話機モードを展開するには、音声とビデオ機能用のデバイスを使用してユーザをプロビジョニングします。 また、ボイス メールなどの追加サービスを持つ個人をプロビジョニングできます。

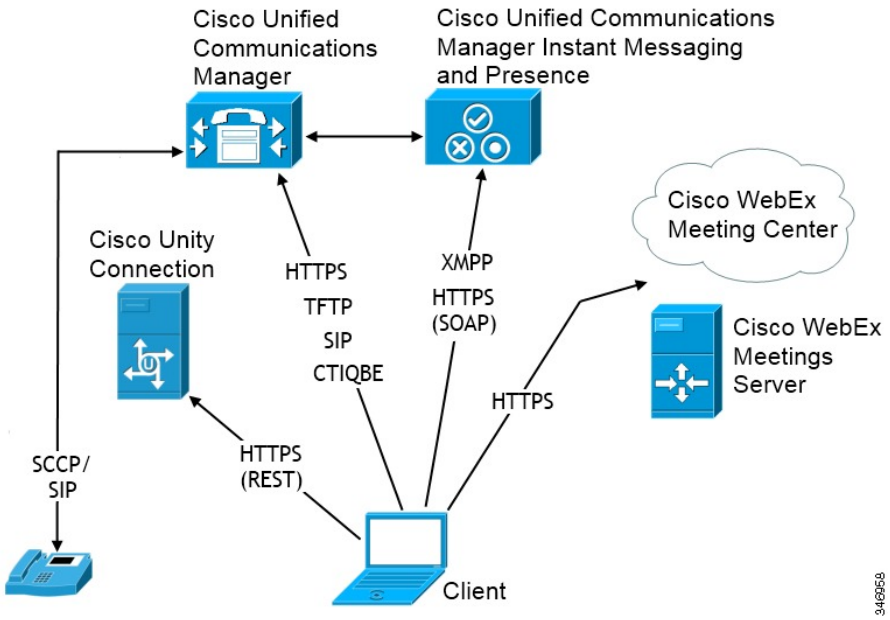
デフォルト製品モードは、ユーザのプライマリ認証が IM and Presence サーバで行われるモードです。

Cisco Unified Communications Manager を使用したオンプレミス展開

Cisco Unified Communications Manager IM and Presence サービスによるオンプレミス展開で使用可能なサービスは次のとおりです。

- **プレゼンス**：Cisco Unified Communications Manager IM and Presence Service 経由で対応可否を公開し、他のユーザの対応可否をサブスクライブします。
- **IM**：Cisco Unified Communications Manager IM and Presence Service 経由で IM を送受信します。
- **ファイル転送**：Cisco Unified Communications Manager IM and Presence Service 経由でファイルとスクリーンショットを送受信します。
- **音声コール**：卓上電話機または Cisco Unified Communications Manager 経由のコンピュータを使用して音声コールを発信します。
- **ビデオ**：Cisco Unified Communications Manager 経由でビデオ コールを発信します。
- **ボイスメール**：Cisco Unity Connection 経由でボイス メッセージを送受信します。
- **会議**：次のいずれかと統合します。
  - Cisco WebEx Meeting Center：ホスト型会議機能を提供します。
  - Cisco WebEx Meeting Server：オンプレミス会議機能を提供します。

次の図は、Cisco Unified Communications Manager IM and Presence Service によるオンプレミス展開のアーキテクチャを示しています。



Cisco Unified Presence によるオンプレミス展開

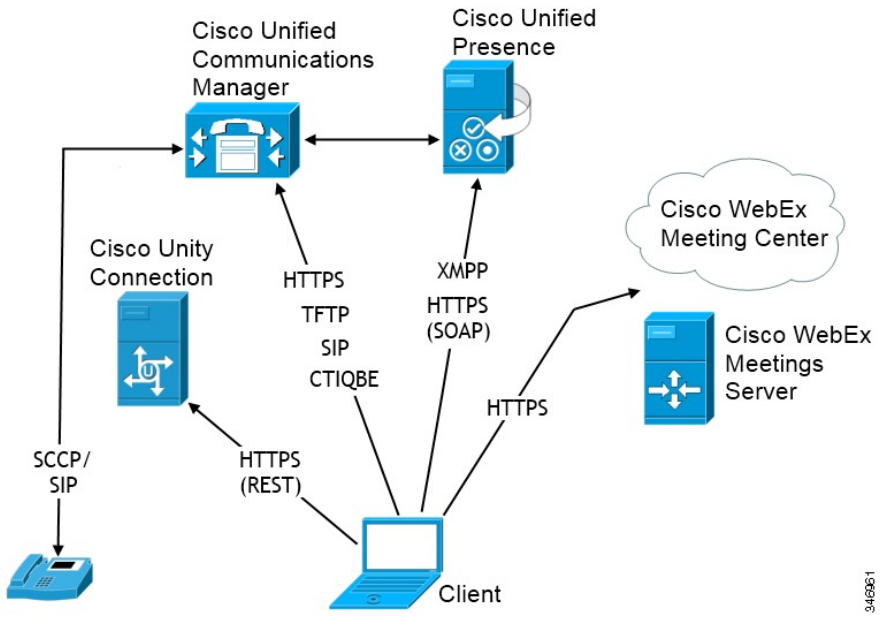
Cisco Unified Presence によるオンプレミスで使用可能なサービスは次のとおりです。

- **プレゼンス**：Cisco Unified Presence 経由で対応可否を公開し、他のユーザの対応可否をサブスクライブします。

- **IM**：Cisco Unified Presence 経由で IM を送受信します。
- **音声コール**：卓上電話機または Cisco Unified Communications Manager 経由のコンピュータを使用して音声コールを発信します。
- **ビデオ**：Cisco Unified Communications Manager 経由でビデオ コールを発信します。
- **ボイスメール**：Cisco Unity Connection 経由でボイス メッセージを送受信します。
- **会議**：次のいずれかと統合します。
  - **Cisco WebEx Meeting Center**：ホスト型会議機能を提供します。
  - **Cisco WebEx Meeting Server**：オンプレミス会議機能を提供します。

（注） モバイル クライアント用の Cisco Jabber は電話機モード中の会議をサポートしません。

次の図は、Cisco Unified Presence によるオンプレミス展開のアーキテクチャを示しています。



電話機モードでのオンプレミス展開

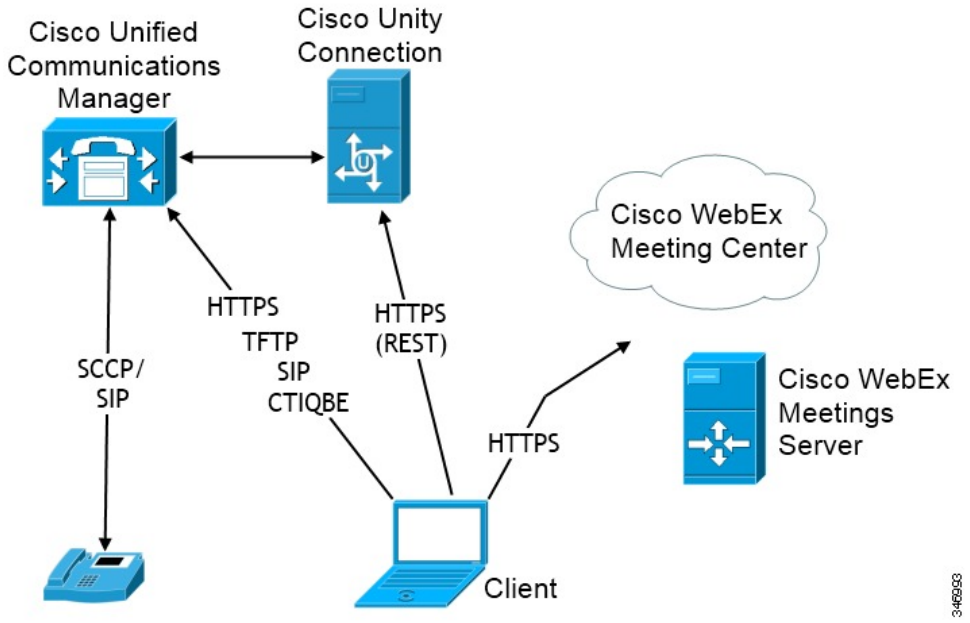
電話機モード展開で使用可能なサービスは次のとおりです。

- **音声コール**：卓上電話機または Cisco Unified Communications Manager 経由のコンピュータを使用して音声コールを発信します。
- **ビデオ**：Cisco Unified Communications Manager 経由でビデオ コールを発信します。

- **ボイスメール**：Cisco Unity Connection 経由でボイス メッセージを送受信します。
- **会議**：次のいずれかと統合します。
  - **Cisco WebEx Meeting Center**：ホスト型会議機能を提供します。
  - **Cisco WebEx Meeting Server**：オンプレミス会議機能を提供します。

（注） Cisco Jabber for Android は電話機モードの会議をサポートしません。

次の図は、電話機モードでのオンプレミス展開のアーキテクチャを示しています。



クラウドベース展開

クラウドベース展開は、Cisco WebEx がサービスをホストする展開の 1 つです。 Cisco WebEx 管理ツールでクラウドベース展開を管理および監視します。

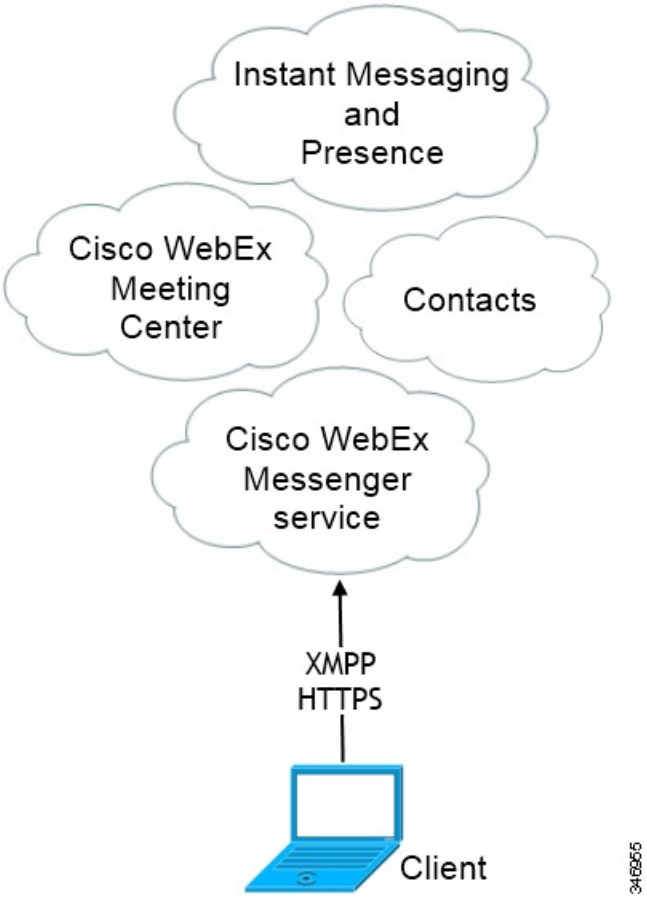
クラウドベース展開

クラウドベース展開で使用可能なサービスは次のとおりです。

- **連絡先ソース**：Cisco WebEx Messenger サービスが連絡先を解決します。
- **プレゼンス**：Cisco WebEx Messenger サービスを使用すれば、ユーザは自分の対応可否を公開し、他のユーザの対応可否にサブスクライブできます。

- **インスタント メッセージング**：Cisco WebEx Messenger サービスを使用すれば、インスタント メッセージを送受信することができます。
- **会議**：Cisco WebEx Meeting Center がホスト型ミーティング機能を提供します。

次の図は、クラウドベース展開のアーキテクチャを図示したものです。



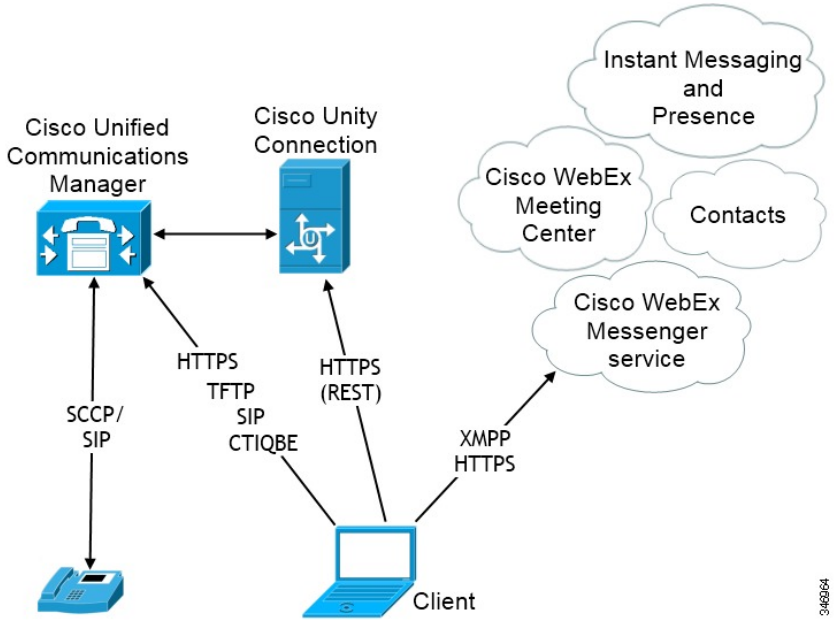
ハイブリッド クラウドベース展開

ハイブリッド クラウドベース展開で使用可能なサービスは次のとおりです。

- **連絡先ソース**：Cisco WebEx Messenger サービスが連絡先を解決します。
- **プレゼンス**：Cisco WebEx Messenger サービスを使用すれば、ユーザは自分の対応可否を公開して、他のユーザの対応可否にサブスクライブできます。
- **インスタント メッセージング**：Cisco WebEx Messenger サービスを使用すれば、インスタント メッセージを送受信することができます。
- **音声**：卓上電話機または Cisco Unified Communications Manager 経由のコンピュータを使用して音声コールを発信します。

- **ビデオ**：Cisco Unified Communications Manager 経由でビデオ コールを発信します。
- **会議**：Cisco WebEx Meeting Center がホスト型ミーティング機能を提供します。
- **ボイスメール**：Cisco Unity Connection 経由でボイス メッセージを送受信します。

次の図は、ハイブリッド クラウドベース展開のアーキテクチャを図示したものです。



シングル サインオンを使用した展開

Security Assertion Markup Language（SAML）シングル サインオン（SSO）を使用したサービスを有効にすることができます。 SAML SSO は、オンプレミス、クラウド、ハイブリッド展開で使用できます。

次の手順では、ユーザが Cisco Jabber クライアントを起動したあとの SAML SSO のサインイン フローについて説明します。

1. ユーザが Jabber クライアントを起動します。 ユーザに Web フォームを使用したサインインを要求するようにアイデンティティ プロバイダー（略して *IdP*）を設定した場合は、その形式がクライアントに表示されます。
2. Cisco Jabber クライアントが、Cisco WebEx Messenger サービス、Cisco Unified Communications Manager、Cisco Unity Connection などの接続先のサービスに認証要求を送信します。
3. サービスが IdP に認証を要求するためにクライアントをリダイレクトします。
4. IdP がクレデンシャルを要求します。 クレデンシャルは、次のいずれかの方法で指定できます。

- ユーザ名とパスワードのフィールドを含むページをユーザに表示する、フォーム ベースの認証。
- 統合 Windows 認証（IWA）用 Kerberos（Windows のみ）
- スマート カード認証（Windows のみ）

5 IdP がブラウザまたはその他の認証方式に Cookie を提供します。 IdP が SAML を使用して ID を認証すると、サービスはクライアントにトークンを提供できます。
6 クライアントがトークンを使用してサービスにログインします。

認証方式

認証メカニズムは SSO のユーザ エクスペリエンスに影響します。 たとえば、Kerberos を使用する場合は、クライアントがユーザにクレデンシャルを要求しません。これは、ユーザがすでに認証され、デスクトップへのアクセス権を取得しているからです。

ユーザ セッション

ユーザがセッションにサインインします。セッションからユーザに Cisco Jabber サービスを使用する事前定義の時間が提示されます。 セッションの継続時間を制御するには、Cookie とトークンのタイムアウト パラメータを設定します。 セッションの期限が切れて、Jabber がそれを自動的に更新できなかった場合は、ユーザ入力が必要なため、再認証を要求するプロンプトが表示されます。この現象は、認証 Cookie が有効でなくなった時点で発生する可能性があります。 Kerberos またはスマート カードが使用されている場合は、スマート カードから PIN が要求されなければ、再認証の操作をする必要はありません。ボイスメール、着信コール、インスタント メッセージングなどのサービスが中断するリスクはありません。

シングル サインオンの要件

サポートされるアイデンティティ プロバイダー

IdP は、Security Assertion Markup Language（SAML）に準拠している必要があります。 クライアントは次のアイデンティティ プロバイダーをサポートします。

- Ping Federate 6.10.0.4
- Microsoft Active Directory Federation Services (ADFS) 2.0
- Open Access Manager (OpenAM) 10.1

（注） OpenAM で使用する Globally Persistent Cookie が設定されていることを確認します。

IdP を設定すると、その設定がクライアントへのサインイン方法に影響します。 Cookie のタイプ（永続的またはセッション）や認証メカニズム（Kerberos または Web フォーム）などの一部のパラメータによって、ユーザの認証頻度が決定されます。

クッキー

ブラウザでの Cookie 共有を有効にするには、セッション Cookie ではなく、永続的な Cookie を使用する必要があります。 永続的な Cookie は、ユーザに Internet Explorer を使用しているクライアントまたはその他のデスクトップ アプリケーションで 1 回クレデンシャルを入力するように要求します。 セッションCookieの場合は、ユーザがクライアントを起動するたびにクレデンシャルを入力する必要があります。 IdP 上の設定として永続的な Cookie を設定します。 Open Acess Manager を IdP として使用している場合は、（Realm Specific Persistent Cookie ではなく）Globally Persistent Cookie を設定する必要があります。

必要なブラウザ

ブラウザとクライアント間で認証 Cookie（IdP から発行された）を共有するには、次のブラウザのいずれかをデフォルト ブラウザに指定する必要があります。

製品	必要なブラウザ
Cisco Jabber for Windows	Internet Explorer
Cisco Jabber for Mac	Safari
Cisco Jabber for iPhone and iPad	Safari
Cisco Jabber for Android	Chrome

（注） Android で SSO を使用している場合は、組み込みブラウザが外部ブラウザと Cookie を共有できません。

シングル サインオンとリモート アクセス

Expressway Mobile and Remote Access を使用して企業ファイアウォールの外側からクレデンシャルを入力するユーザの場合は、シングル サインオンに次の制限があります。

- シングル サインオン（SSO）は、Cisco Expressway 8.5 と Cisco Unified Communications Manager リリース 10.5.2 以降で使用できます。
- セキュアな電話機の Expressway for Mobile and Remote Access を介して SSO を使用することはできません。
- 使用するアイデンティティ プロバイダーは内部 URL と外部 URL を同じにする必要があります。 URL が異なる場合は、ユーザが企業ファイアウォールの内側から外側にまたはその逆に移動するときに再度サインインするように要求されることがあります。

クライアント内の SAML SSO の有効化

はじめる前に

- WebEx Messenger を使用しない場合は、Cisco Unified Communications Applications 10.5.1 Service Update 1 で SSO を有効にします。このサービス上での SAML SSO の有効化方法については、『*SAML SSO Deployment Guide for Cisco Unified Communications Applications, Release 10.5*』を参照してください。
- Cisco Unity Connection バージョン 10.5 で SSO を有効にします。このサービス上での SAML SSO の有効化方法については、『*Managing SAML SSO in Cisco Unity Connection*』を参照してください。
- WebEx Messenger を使用する場合は、WebEx Messenger サービスで SSO を有効にして Cisco Unified Communications アプリケーションと Cisco Unity Connection をサポートします。このサービス上での SAML SSO の有効化方法については、『*Cisco WebEx Messenger Administrator's Guide*』の「*Single Sign-On*」を参照してください。

  このサービス上での SAML SSO の有効化方法については、『*Cisco WebEx Messenger Administrator's Guide*』の「`Single Sign-On`」を参照してください。

手順

ステップ 1 Web ブラウザで証明書を検証できるように、すべてのサーバに証明書を配布してください。これを行わない場合、無効な証明書に関する警告メッセージが表示されます。 証明書の検証に関する詳細については、「証明書の検証」を参照してください。

ステップ 2 クライアントの SAML SSO のサービス検出を確認します。 クライアントは、標準サービス検出を使用してクライアントの SAML SSO を有効化します。 次の設定パラメータを使用してサービス検出を有効にします。ServicesDomain、VoiceServicesDomain、および ServiceDiscoveryExcludedServices。サービス検出の有効化方法については、「クライアントがサービスを検出する方法」を参照してください。

ステップ 3 セッションの継続時間を定義します。
セッションは、Cookie およびトークン値で構成されます。 通常、Cookie はトークンより長く残ります。 cookie の寿命はアイデンティティ プロバイダーで定義され、トークンの期間はサービスで定義されます。

ステップ 4 SSO を有効にすると、デフォルトで、すべての Jabber ユーザが SSO を使用してサインインします。 管理者は、特定のユーザが SSO を使用する代わりに、Jabber ユーザ名とパスワードを使用してサインインするようにユーザ単位でこの設定を変更できます。 Jabber ユーザの SSO を無効にするには、SSO_Enabled パラメータの値を FALSE に設定します。
ユーザに電子メール アドレスを尋ねないように Jabber を設定した場合は、ユーザの Jabber への最初のサインインが非 SSO になることがあります。 展開によっては、パラメータの ServicesDomainSsoEmailPrompt を ON に設定する必要があります。 これにより、最初の SSO によるサインインの実行に必要な情報が Jabber に渡されることが保証されます。 ユーザが一度でも

Jabber にサインインしたことがある場合は、必要な情報が入手できるため、このプロンプトは必要ありません。

仮想環境での展開

仮想環境に Cisco Jabber for Windows を展開できます。

仮想環境でサポートされる機能は次のとおりです。

- 他の Cisco Jabber クライアントとのインスタント メッセージングおよびプレゼンス
- デスクフォン制御
- ボイスメール
- Microsoft Outlook 2007、2010、2013 とのプレゼンスの統合

仮想環境の要件

ソフトウェア要件

仮想環境で Cisco Jabber for Windows を展開するには、次のサポートされるソフトウェア バージョンの中から選択します。

ソフトウェア	サポートされるバージョン
Citrix XenDesktop	7.6、7.5、7.1
Citrix XenApp	7.6、公開されたデスクトップ 7.5、公開されたデスクトップ
VMware Horizon View	6.0、5.3、および 5.2

ソフトフォン要件

ソフトフォン コールに対して、Cisco Virtualization Experience Media Engine（VXME）を使用します。

仮想環境とローミング プロファイル

仮想環境では、ユーザが常に同じ仮想デスクトップにアクセスするわけではありません。 一貫したユーザ エクスペリエンスを保証するには、クライアントが起動されるたびにこれらのファイルにアクセスできる必要があります。 Cisco Jabber はユーザ データを次の場所に保存します。

- `C:\Users\username\AppData\Local\Cisco\Unified Communications\Jabber\CSF`
  - **連絡先**：連絡先キャッシュ ファイル
  - **履歴**：コールおよびチャット履歴
  - **写真キャッシュ**：ディレクトリ写真をローカルにキャッシュする
- `C:\Users\username\AppData\Roaming\Cisco\Unified Communications\Jabber\CSF`
  - **コンフィギュレーション**：ユーザ コンフィギュレーション ファイルを維持し、コンフィギュレーション ストア キャッシュを保存する
  - **クレデンシャル**：暗号化されたユーザ名およびパスワード ファイルを保存する

必要に応じて、ファイルとフォルダを除外リストに追加することによって、それらを同期から除外できます。 除外されたフォルダ内のサブフォルダを同期するには、そのサブフォルダを包含リストに追加します。

個人ユーザ設定を保存するには

- 次のディレクトリを除外しないでください。
  - `AppData\Local\Cisco`
  - `AppData\Local\JabberWerxCPP`
  - `AppData\Roaming\Cisco`
  - `AppData\Roaming\JabberWerxCPP`
- 次の専用のプロファイル管理ソリューションを使用してください。
  - **Citrix Profile Management**：これは Citrix 環境向けのプロファイル ソリューションです。 ランダム ホスト型仮想デスクトップ割り当てを使用した展開では、Citrix Profile Management がインストールされているシステムとユーザ ストア 間で各ユーザのプロファイル全体を同期させます。
  - **VMware View Persona Management**：これは、ユーザ プロファイルを保存し、それらをリモート プロファイル リポジトリと動的に同期させます。 VMware View Persona Management は Windows ローミング プロファイルを必要としないので、View ユーザ プロファイルの管理では Windows Active Directory をバイパスできます。 Persona Management は、既存のローミング プロファイルの機能を強化します。