Cisco Video Communication Server による Mobile & Remote Access

導入ガイド

初版：2014 年 4 月

最終更新日：2016 年 4 月

Cisco VCS X8.7

Cisco Unified CM 9.1(2)SU1 以降

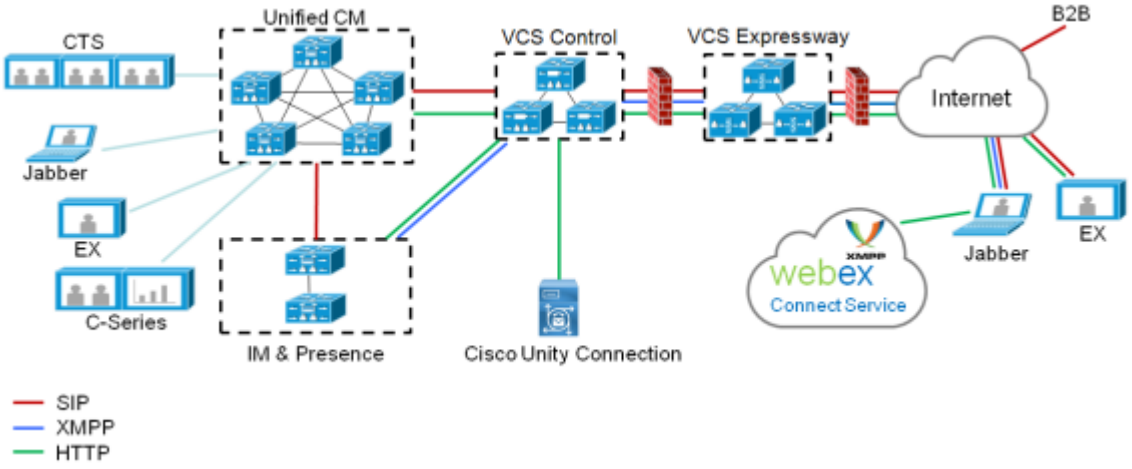
Mobile & Remote Access の概要

Cisco Unified Communications の Mobile & Remote Access は Cisco Collaboration Edge アーキテクチャの中核を成します。Cisco Jabber などのエンドポイントが企業ネットワーク外にある場合に、Cisco Unified Communications Manager（Unified CM）への登録、呼制御、プロビジョニング、メッセージング、およびプレゼンスの機能を使用することができるようになります。VCS は、Unified CM 登録にセキュアなファイアウォール トラバーサルと回線側サポートを提供します。

ソリューションによって以下が実現します。

- **オフプレミス アクセス**：企業ネットワーク外においても、Jabber および EX/MX/SX シリーズ クライアントで一貫したエクスペリエンスを提供
- **セキュリティ**：セキュアな Business-to-Business（B2B）コミュニケーション
- **クラウド サービス**：エンタープライズ クラスの柔軟性と拡張性に優れたソリューションにより、WebEx の統合とさまざまなサービス プロバイダーに対応
- **ゲートウェイと相互運用性サービス**：メディアおよびシグナリングの正規化、非標準エンドポイントのサポート

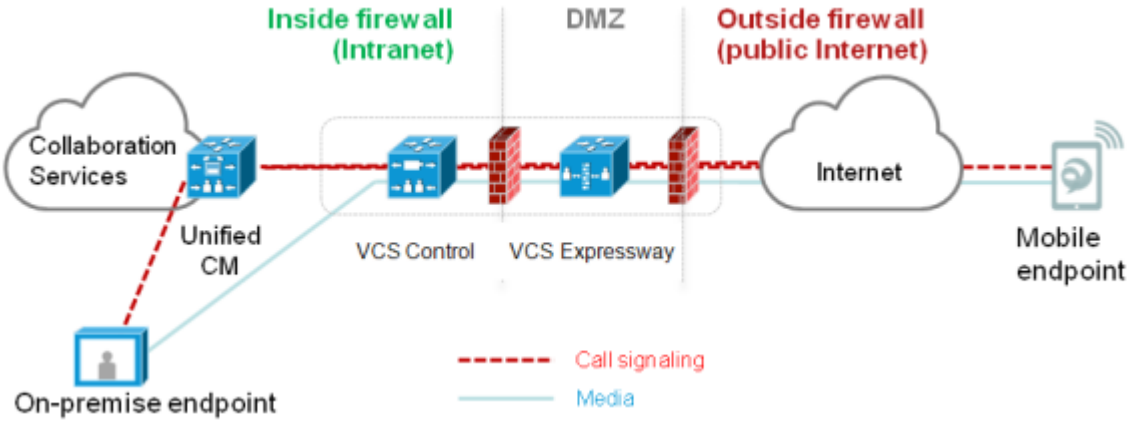
図 1　ユニファイド コミュニケーション：Mobile & Remote Access



サードパーティ製 SIP または H.323 デバイスは VCS Control に登録でき、必要に応じて SIP トランクを介して Unified CM によって登録されたデバイスと相互運用できます。

Mobile & Remote Access の概要

図 2　一般的なコール フロー：シグナリングおよびメディア パス



- Unified CM は、モバイルとオンプレミスの両方のエンドポイントにコール制御を提供します。
- シグナリングは、モバイル エンドポイントと Unified CM の間で Expressway ソリューションを横断します。
- メディアは Expressway ソリューションを横断し、エンドポイント間で直接リレーされます。すべてのメディアが VCS Control とモバイル エンドポイント間で暗号化されます。

導入の適用範囲

以下の主要な VCS ベースの導入は相互に排他的です。これらは、同一の VCS（トラバーサル ペア）上で同時に実装できません。

- モバイル & リモート アクセス
- Microsoft 相互運用性
- Jabber Guest
- ハイブリッド サービス（コネクタ ホスト）

VPN を使用しない Jabber クライアント接続

Mobile & Remote Access ソリューションがオンプレミスとクラウド ベースのハイブリッド型サービス モデルをサポートし、企業内外で一貫したエクスペリエンスを提供します。VPN で企業ネットワークに接続せずに Jabber アプリケーション トラフィックのセキュアな接続を提供します。Windows、Mac、iOS および Android プラットフォームでデバイスとオペレーティング システムに依存しない Cisco Jabber クライアントのソリューションです。

企業外の Jabber クライアントで以下を実現します。

- インスタント メッセージングおよびプレゼンス サービスの使用
- 音声/ビデオ通話
- 社内ディレクトリの検索

導入シナリオ

- コンテンツの共有
- Web 会議の開始
- ビジュアル ボイスメールへのアクセス

注：Jabber Web および Cisco Jabber Video for TelePresence（Jabber Video）はサポートしていません。

関連資料

次のマニュアルおよびサイトに含まれる情報は、ユニファイド コミュニケーション環境のセットアップに役立ちます。

- *VCS 基本設定（Control および Expressway）導入ガイド [英語]*
- *VCS クラスタの作成およびメンテナンス導入ガイド*
- *VCS を使用した証明書の作成と利用の導入ガイド [英語]*
- *VCS 管理者ガイド [英語]*
- Cisco Unified Communications Manager 設定ガイド [英語] *のCisco Unified Communications Manager での IM and Presence Service の設定および管理*（使用するバージョンに適合するもの）
- 「*Directory Integration and Identity Management*」（『Cisco Collaboration System 10.x Solution Reference Network Designs（SRND）』マニュアル）
- Cisco Unified Communications Manager のメンテナンスおよびオペレーション ガイド *のCisco Unified Communications アプリケーション用 SAML SSO 導入ガイド [英語]*（使用するバージョンに適合するもの）
- Jabber クライアントの設定方法：
  - *Cisco Jabber for Windows*
  - *Cisco Jabber for iPad*
  - *Cisco Jabber for Android*
  - *Cisco Jabber for Mac*
  - *『Cisco Jabber DNS Configuration Guide』*

導入シナリオ

ここでは、サポートしている導入環境について説明します。

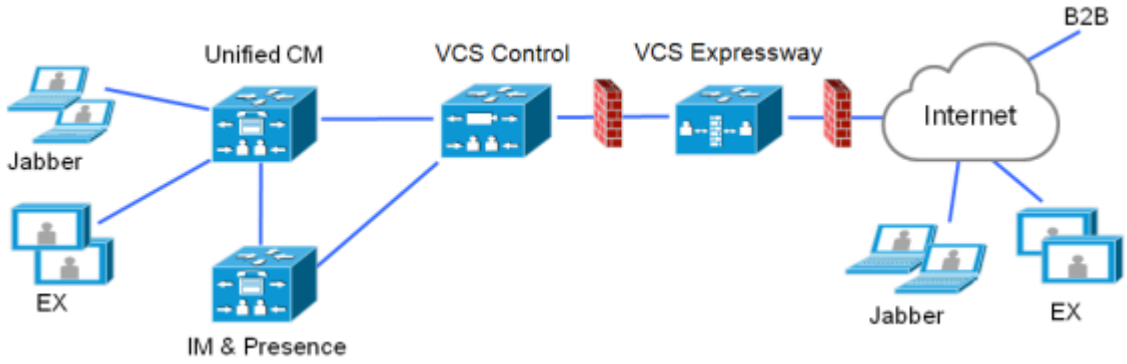
- 単一のネットワーク要素
- 単一のクラスタ化されたネットワーク要素
- 複数のクラスタ化されたネットワーク要素

導入シナリオ

- ハイブリッド展開
- サポートされていない展開

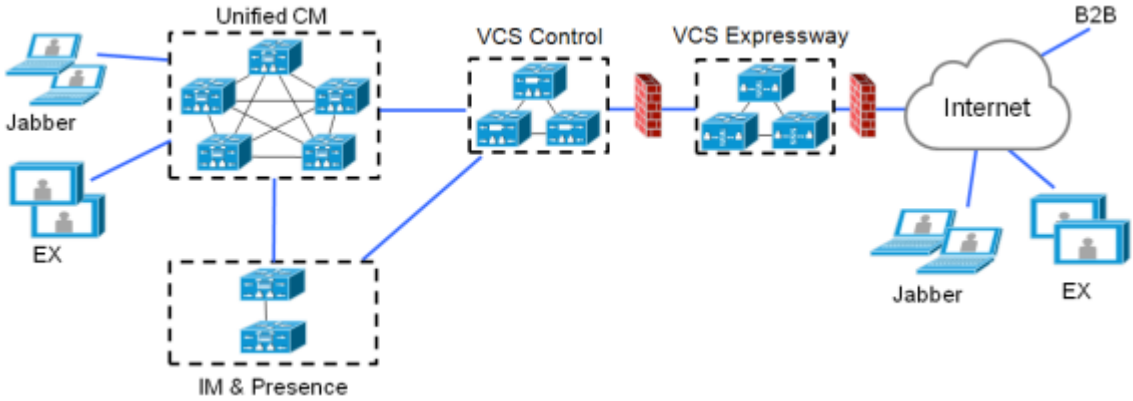
単一のネットワーク要素

このシナリオでは、単一の（クラスタ化されていない）Unified CM、IM & Presence、VCS Control、VCS Expressway サーバが存在しています。



単一のクラスタ化されたネットワーク要素

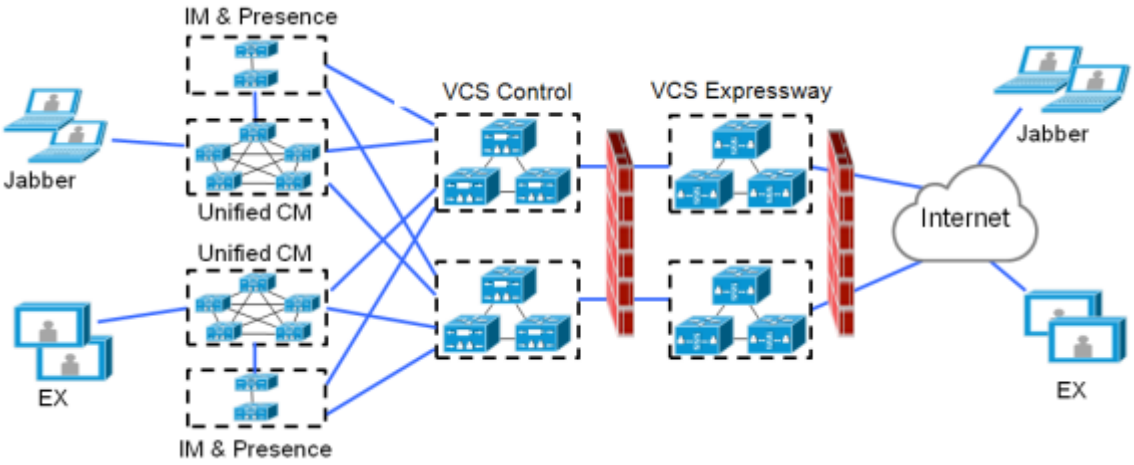
このシナリオでは、各ネットワーク要素がクラスタ化されています。



導入シナリオ

複数のクラスタ化されたネットワーク要素

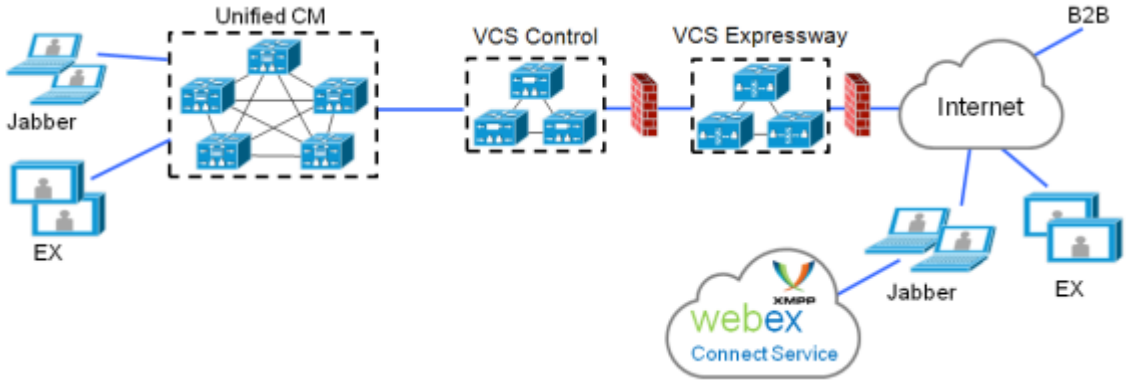
このシナリオでは、各ネットワーク要素に複数のクラスタが存在します。



- Jabber クライアントはすべてのルートで独自のクラスタにアクセスできます
- VCS Control は、ホーム クラスタ検出要求をルーティングするときに、ラウンド ロビンを使用してノード（パブリッシャまたはサブスクライバ）を選択します
- Unified CM と IM and Presence Service クラスタのそれぞれの組み合わせで、同じドメインを使用する必要があります
- クラスタ間検索サービス（ILS）は、Unified CM クラスタでアクティブである必要があります
- クラスタ間ピア リンクは IM and Presence Service クラスタ間に設定し、Intercluster Sync Agent（ICSA）がアクティブである必要があります

ハイブリッド展開

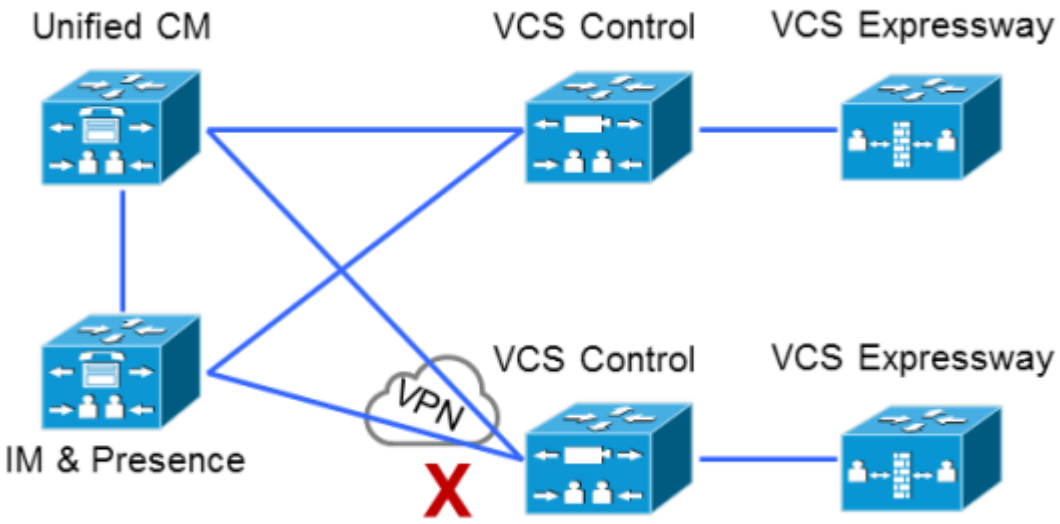
このシナリオでは、Jabber クライアントの IM and Presence サービスは WebEx クラウドを通じて提供されます。



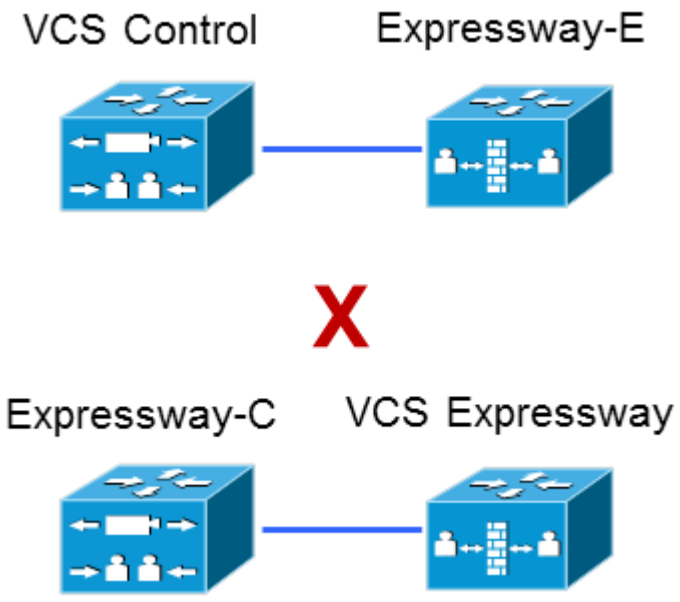
導入シナリオ

サポートされていない展開

VCS Control と Unified CM サービス/クラスタ間の VPN リンクは、サポートされません。



「混合」トラバーサル接続はサポートされません。つまり、Cisco VCS と Cisco Expressway 間のトラバーサル ゾーンまたはユニファイド コミュニケーション トラバーサル ゾーンは、*設定可能な場合でも*サポートされません。



明確にすると、Expressway-E への VCS Control トラバーサルも、VCS Expressway への Expressway-C トラバーサルもサポートされません。

設定の概要

ここでは、Mobile & Remote Access 用のユニファイド コミュニケーション システムの設定の手順の概要を示します。以下がすでに設定されていることを想定します。

- *VCS 基本設定（Control および Expressway）導入ガイド* [英語] で指定されているとおりの基本的な VCS Control、VCS Expressway の設定（このマニュアルには、DMZ に VCS Expressway を展開するさまざまなネットワーク オプションに関する情報が含まれています）。
- 次のマニュアルで指定されている Unified CM と IM and Presence Service の設定：Cisco Unified Communications Manager 設定ガイド [英語] *の Cisco Unified Communications Manager での IM and Presence Service の設定および管理*（使用するバージョンに適合するもの）。

前提条件

次のソフトウェア バージョンを実行していることを確認します。

- VCS X8.1.1 以降
- Unified CM 9.1(2)SU1 以降および IM and Presence Service 9.1(1) 以降

Mobile & Remote Access でサポートしているクライアント

VCS X8.1.1 以降：

- Cisco Jabber for Windows 9.7 以降
- Cisco Jabber for iPhone and iPad 9.6.1 以降
- Cisco Jabber for Android 9.6 以降
- Cisco Jabber for Mac 9.6 以降
- TC7.0.1 以降のファームウェアを実行する Cisco TelePresence エンドポイント/コーデック

VCS X8.6 以降：

ファームウェア バージョン11.0(1)以降を実行す電話機の場合、Mobile and Remote Access は現在 Cisco IP Phone 78/8800 シリーズで公式にサポートされています。これらの電話機と使用するには、VCS X8.7以降を推奨します。

- Cisco IP Phone 8800 シリーズ
- Cisco IP Phone 7800 シリーズ

設定の概要

MRA は、ファームウェア バージョン10.2.4(99) 以降を実行する Cisco DX シリーズのエンドポイントで公式にサポートされます。このサポートは VCS バージョンX8.6 で発表されました。

- Cisco DX650
- Cisco DX80
- Cisco DX70

Mobile & Remote Access 経由で Cisco Unified Communications Manager に登録するために DX シリーズまたは IP Phone 78/8800 シリーズのエンドポイントを展開する場合、次の点に注意する必要があります。

- **電話セキュリティ プロファイル：**いずれかの電話機の電話セキュリティ プロファイルで **TFTP 暗号化設定**にチェックマークが付いている場合、Mobile & Remote Access でその電話機を使用することはできません。これは、MRA ソリューションが CAPF（Certificate Authority Proxy Function）とインタラクティブに機能するデバイスをサポートしないためです。
- **信頼リスト：**これらのエンドポイントのルート CA の信頼リストは変更できません。この VCS Expressway サーバ証明書が、エンドポイントが信頼する CA のいずれかにより署名され、その CA が VCS Control および VCS Expressway により信頼されていることを確認してください。
- **帯域幅制限：**Cisco Unified Communications Manager のデフォルト リージョンの**ビデオ コールの最大セッション ビット レート**は、デフォルトで 384 kbps です。VCS Control の**デフォルトのコール帯域幅**も、デフォルトで 384 kbps です。これらの設定は、DX シリーズで予想されるビデオ品質を実現するには低すぎる場合があります。

設定の概要

EX/MX/SX シリーズのエンドポイント（TC ソフトウェアを実行）

プロビジョニング モードが [Expressway 経由の Cisco UCM（Cisco UCM via Expressway）] に設定されていることを確認します。

Unified CM で、これらのエンドポイントの **[IP アドレッシング モード（IP Addressing Mode）]** が *[IPV4_ONLY]* に設定されていることを確認する必要があります。

これらのエンドポイントでは、サーバ証明書の検証で接続している VCS Expressway のアイデンティティを確認する必要があります。これを行うには、信頼できる CA のリストで VCS Expressway のサーバ証明書の署名に使用された認証局が必要です。

これらのエンドポイントには、最も一般的なプロバイダー（Thawte、Verisign など）に対応するデフォルトの CA リストが付属しています。適切な CA が含まれていない場合は追加する必要があります。詳細については、エンドポイントの管理者ガイドの「Managing the list of trusted certificate authorities」を参照してください。

相互認証は任意です。これらのエンドポイントで、クライアント認証を提供する必要はありません。相互 TLS を設定する場合は、クライアント証明書のプロビジョニングに CAPF 登録を使用できません。エンドポイントに手動で証明書を適用する必要があります。クライアント証明書は VCS Expressway で信頼される認証局によって署名される必要があります。

設定の概要

Jabber クライアント

Jabber クライアントでは、サーバ証明書の検証で接続している VCS Expressway のアイデンティティを確認する必要があります。これを行うには、信頼できる CA のリストで VCS Expressway のサーバ証明書の署名に使用された認証局が必要です。

Jabber は、基盤となるオペレーティング システムの証明書メカニズムを使用します。

- Windows：証明書マネージャ
- MAC OS X：キー チェーン アクセス
- IOS：信頼ストア
- Android：場所とセキュリティ設定

Mobile & Remote Access 用の Jabber クライアントの設定方法は、各クライアントに該当するインストレーション ガイドを参照してください。

- *Cisco Jabber for Windows*
- *Cisco Jabber for iPad*
- *Cisco Jabber for Android*
- *Cisco Jabber for Mac*（X8.2 以降が必要）

DNS レコード

ここでは、パブリック（外部）とローカル（内部）DNS の要件について説明します。詳細については、Jabber のインストールとアップグレード ガイド ページの *Cisco Jabber プランニング ガイド [英語]*（使用するバージョンに適合するもの）を参照してください。

パブリック DNS

エンドポイントが Mobile & Remote Access に使用する VCS Expressway を検出できるように、パブリック（外部）DNS は `_collab-edge._tls.<domain>` SRV レコードで設定する必要があります。SIP サービス レコードも必要です（Mobile & Remote Access だけではなく一般的な導入にも必要です）。たとえば、2 つの VCS Expressway システムのクラスタの場合は、次のようになります。

ドメイン	サービス	プロトコル	プライオリティ（Priority）	Weight	ポート（Port）	ターゲット ホスト（Target host）
example.com	collab-edge	tls	10	10	8443	vcse1.example.com
example.com	collab-edge	tls	10	10	8443	vcse2.example.com
example.com	sips	tcp	10	10	5061	vcse1.example.com
example.com	sips	tcp	10	10	5061	vcse2.example.com

設定の概要

ローカル DNS

ローカル（内部）DNS には `_cisco-uds._tcp.<domain>` SRV レコードが必要です。次に例を示します。

ドメイン	サービス	プロトコル	プライオリティ（Priority）	Weight	ポート（Port）	ターゲット ホスト（Target host）
example.com	cisco-uds	tcp	10	10	8443	cucmserver1.example.com
example.com	cisco-uds	tcp	10	10	8443	cucmserver2.example.com

（注）

- `cisco-uds` SRV レコードが内部ネットワークの外部で解決されないことを確認します。外部で解決されると、Jabber クライアントは VCS Expressway を介してモバイルおよびリモート アクセスのネゴシエーションを開始しません。
- Mobile and Remote Access で使用する ユニファイド コミュニケーションのノードでは、前方参照と逆引き参照の両方に内部 DNS レコードを作成する必要があります。これにより、FQDN ではなく、IP アドレスまたはホスト名が使用されている場合に VCS Control がノードを検索できるようになります。

ファイアウォール

- 関連するポートが内部ネットワーク（VCS Control が配置されている）と DMZ（VCS Expressway が配置されている）間、および DMZ とパブリック インターネット間のファイアウォールで設定されていることを確認します。詳細については、「Mobile and Remote Access ポートのリファレンス」（p.42）を参照してください。
- VCS Expressway で 1 つの NIC が有効になっていて、スタティック NAT モードを使用する場合は、次の点に注意してください。

  ネットワークの外側から見えるとおりに、VCS Expressway の FQDN を、VCS Control のセキュア トラバーサル ゾーン上のピア アドレスとして入力する必要があります。スタティック NAT モードでは、着信シグナリングとメディア トラフィックを、プライベート名ではなく外部 FQDN に送信するように VCS Expressway が要求するためです。

  また、これは外部ファイアウォールが VCS Control から VCS Expressway の外部 FQDN へのトラフィックを許可する必要があることも意味します。これは、NAT リフレクションと呼ばれ、すべてのタイプのファイアウォールでサポートされているわけではありません。

  詳細については、*VCS 基本設定（Control および Expressway）導入ガイド [英語] の付録、「高度なネットワーク展開」*を参照してください。

Unified CM

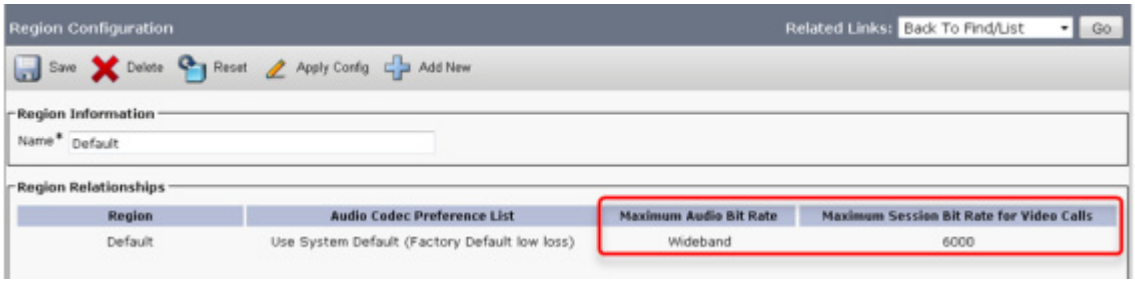
1. 複数の Unified CM クラスタで構成される場合、ILS（クラスタ間検索サービス）をすべてのクラスタで設定する必要があります。

   これは、VCS がそれぞれのユーザのホーム Unified CM クラスタと通信し、Unified CM ノードのいずれかに、UDS（ユーザ データ サービス）クエリーを送信するホーム クラスタを検出する必要があるからです。

   Unified CM ドキュメント [英語] の使用するバージョンの「クラスタ間の検索サービス」を検索してください。

設定の概要

2. 地域間と地域内（[システム（System）] > [リージョン情報（Region Information）] > [リージョン（Region）]）で、[ビデオ コールの最大セッション ビット レート（Maximum Session Bit Rate for Video Calls）] が 6000 kbps などのシステムの適切な上限に設定されていることを確認します。

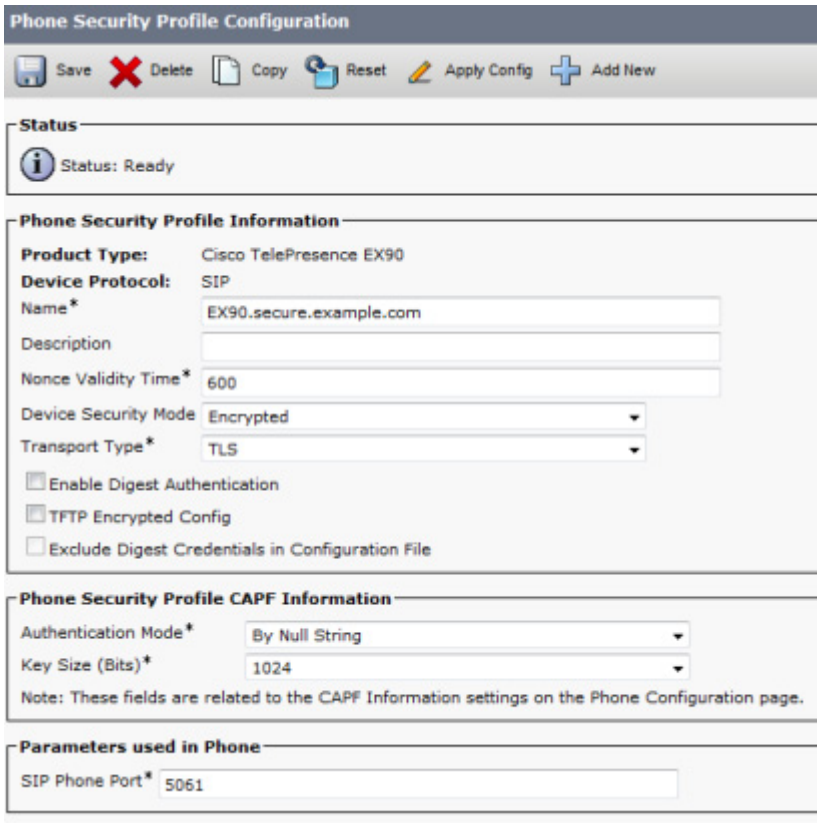


詳細については、「*Region setup*」を参照してください。

3. TLS に設定され、リモート アクセスを必要とするデバイスに使用される Unified CM（**[システム（System）] > [セキュリティ（Security）] > [電話セキュリティ プロファイル（Phone Security Profile）]**）の **[電話セキュリティ プロファイル（Phone Security Profile）]** には、エンタープライズ ドメイン（jabber.secure.example.com など）を含む FQDN 形式の**名前**が必要です。（これは、これらの名前が VCS Control サーバ証明書のサブジェクト代替名のリストに含まれている必要があるためです）。

   注：セキュアなプロファイルでは、**[デバイス セキュリティ モード（Device Security Mode）]**に *[暗号化（Encrypted）]* を設定する必要があります。理由は、VCS が暗号化されていない TLS 接続を許可しないためです。**[デバイスのセキュリティ モード（Device Security Mode）]** に *[認証済み（Authenticated）]* を設定した場合、Unified CM は VCS が拒否する NULL-SHA 暗号スイートのみを提供します。

設定の概要



4. Unified CM サーバ（**[システム（System）] > [サーバ（Server）]**）が（IP アドレスではなく）**ホスト名**で設定されている場合、これらのホスト名が VCS Control で解決可能であることを確認します。
5. セキュア プロファイルを使用している場合、VCS Control の証明書に署名した認証局のルート CA が *CallManager の信頼*証明書（**Cisco Unified OS Administration** アプリケーションの **[セキュリティ（Security）] > [証明書の管理（Certificate Management）]**）としてインストールされていることを確認します。
6. **Cisco AXL Web Service** が、リモート アクセスで使用される Unified CM サーバを検出するために使用する Unified CM パブリッシャでアクティブであることを確認します。これは、**Cisco Unified Serviceability** アプリケーションを選択し、[ツール（Tools）] > [サービスのアクティブ化（Service Activation）] で確認できます。
7. リモートおよびモバイル デバイスを（直接またはデバイス モビリティによって）パブリック アクセス可能な NTP サーバを使用するように設定することを推奨します。
   1. パブリック NTP サーバ [システム（System）] > [電話用 NTP（Phone NTP Reference）] を設定します。
   2. 日付/時刻グループ（[システム（System）] > [日時グループ（Date/Time Group）]）に電話用 NTP を追加します。
   3. エンドポイント（[システム（System）] > [デバイス プール（Device Pool）]）のデバイス プールに日時グループを割り当てます。

設定の概要

IM and Presence Service

Cisco AXL Web Service が、リモート アクセス用の他の IM and Presence Service ノードを検出する IM and Presence Service パブリッシャでアクティブになっていることを確認します。これは、**Cisco Unified Serviceability** アプリケーションを選択し、[ツール（Tools）] > [サービスのアクティブ化（Service Activation）] で確認できます。

複数の IM and Presence Service クラスタで Mobile & Remote Access を導入する場合は、クラスタ間にクラスタ間ピア リンクを設定し、すべてのクラスタで Intercluster Sync Agent（ICSA）をアクティブにする必要があります。これにより、ユーザ データベースがクラスタ間で確実に複製され、VCS Control で正しく XMPP トラフィックをルーティングできます。

正しい設定の詳細については、*Cisco Unified Communications Manager での IM and Presence Service の設定および管理*の「Intercluster Peer の設定」の章を参照してください。使用するバージョンの正しいマニュアルは、次の URL を参照してください。http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html

VCS

次の手順は、VCS Expressway、VCS Control で必要な設定の概要を示します。詳細については、「VCS の Mobile & Remote Access の設定」（p.21）を参照してください。

1. **[システムのホスト名（System host name）]** と **[ドメイン名（Domain name）]** が、すべての VCS に指定されていること、およびすべての VCS のシステムが信頼できる NTP サービスに同期されていることを確認します。
2. [ユニファイド コミュニケーション モード（Unified Communications mode）] を [モバイル アンド リモート アクセス（Mobile and remote access）] に設定します。
3. VCS Control 上で、Unified CM、IM and Presence Service および Cisco Unity Connection サーバを設定します。
4. サービスが Unified CM にルーティングされる VCS Control のドメインを設定します。
5. （任意）追加の展開を作成して、ドメインと UC サービスをその展開に関連付けます。
6. 適切なサーバ証明書および信頼できる CA 証明書をインストールします。
7. VCS Expressway と VCS Control 間のユニファイド コミュニケーション トラバーサル ゾーン接続を設定します。
8. 必要に応じて、リモート Jabber クライアントからアクセスする必要がある企業内の Web サービスの HTTP サーバ許可リストを設定します。
9. （任意）コラボレーション エッジ経由の SSO を設定して、外部 Jabber クライアントとユーザの Unified CM プロファイル間の共通アイデンティティを有効にします。

注：VCS の設定変更は通常即座に適用されます。システムの再起動または他のアクションが必要な場合は、バナー メッセージまたはアラームで通知されます。

ユニファイド コミュニケーションの前提条件

ユニファイド コミュニケーションのためのセキュアなトラバーサル ゾーン接続の設定

ユニファイド コミュニケーション機能（Mobile & Remote Access、または Jabber Guest など）をサポートするには、VCS Control と VCS Expressway 間にユニファイド コミュニケーション トラバーサル ゾーン接続が必要です。次の内容を取り上げます。

- VCS Control と VCS Expressway に適切なセキュリティ証明書をインストールします。
- VCS Control と VCS Expressway 間のユニファイド コミュニケーション トラバーサル ゾーン接続を設定します。

注：VCS あたり 1 つの*ユニファイド コミュニケーション トラバーサル* ゾーンのみ設定する必要があります。

VCS のセキュリティ証明書のインストール

VCS Control と VCS Expressway 間の信頼を設定する必要があります。

1. VCS Control と VCS Expressway に適切なサーバ証明書をインストールします。
   - 証明書には、**Client Authentication** 拡張子を含める必要があります。システムは、ユニファイド コミュニケーション機能が有効になっている場合、この拡張子を指定せずにサーバ証明書をアップロードすることはできません。
   - VCS には、証明書署名要求（CSR）を生成する機能が組み込まれており、CSR を生成する場合に推奨される方法です。
     - 要求に署名する CA がクライアント認証拡張子を除外していないことを確認します。
     - 生成した CSR には、クライアント認証要求と有効化されたユニファイド コミュニケーション機能に関連するサブジェクト代替名が含まれます（必要に応じて、「ユニファイド コミュニケーションのサーバ証明書要件」（p.18）を参照してください）。
   - CSR を生成または VCS にサーバ証明書をアップロードするには、**[メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [サーバ証明書（Server certificate）]** を選択します。新しいサーバ証明書を有効にするには、VCS を再起動する必要があります。
2. 両方の VCS に、VCS のサーバ証明書に署名した CA の信頼できる認証局（CA）証明書をインストールします。

   展開されるユニファイド コミュニケーション機能に基づいて、次のように信頼要件が追加されます。

   Mobile & Remote Access を導入する場合：
   - VCS Control は Unified CM と IM&P の Tomcat 証明書を信頼する必要があります。
   - 状況に応じて、VCS Control と VCS Expressway の両方で、エンドポイントの証明書に署名した認証局を信頼する必要があります。

ユニファイド コミュニケーションの前提条件

Jabber Guest を導入する場合：

- Jabber Guest サーバがインストールされると、自己署名証明書がデフォルトで使用されます。ただし、信頼できる認証局によって署名された証明書をインストールできます。VCS Control に Jabber Guest サーバの自己署名証明書、または Jabber Guest サーバの証明書に署名した CA の信頼できる CA 証明書をインストールする必要があります。

信頼できる認証局（CA）証明書を VCS にアップロードするには、**[メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [信頼できる CA 証明書（Trusted CA certificate）]** を選択します。新しい信頼できる CA 証明書を有効にするには、VCS を再起動する必要があります。

VCS のサーバ証明書を作成してアップロードする方法および信頼できる認証局のリストをアップロードする方法の詳細については、*VCS を使用した証明書の作成と利用の導入ガイド* [英語] を参照してください。

暗号化された VCS トラバーサル ゾーンの設定

VCS Control と VCS Expressway 間のセキュアなトラバーサル ゾーン接続によってユニファイド コミュニケーション機能をサポートするには、次の手順を実行します。

- VCS Control および VCS Expressway は*ユニファイド コミュニケーション トラバーサル*タイプのゾーンに設定する必要があります。これは自動的に適切なトラバーサル ゾーン（VCS Control 上で選択されたときは、トラバーサル クライアント ゾーン、VCS-E 上で選択されたときは、トラバーサル サーバ ゾーン）を設定します。そのゾーンは、**[TLS 検証モード（TLS verify mode）]** が *[オン（On）]* かつ **[メディア暗号化モード（Media encryption mode）]** が *[強制暗号化（Force encrypted）]* の状態で SIP TLS を使用します。
- 両方の VCS が相互のサーバ証明書を信頼する必要があります。各 VCS がクライアントとサーバの両方として機能する際、各 VCS の証明書がクライアントとしてもサーバとしても有効であることを確認する必要があります。
- H.323 または暗号化されていない接続も必要な場合、トラバーサル ゾーンの個別のペアを設定する必要があります。

セキュアなトラバーサル ゾーンを設定するには、VCS Control と VCS Expressway を次のように設定します。

1. [設定（Configuration）] > [ゾーン（Zones）] > [ゾーン（Zones）] へ移動します。
2. [新規（New）] をクリックします。
3. 次のようにフィールドを設定します（他のすべてのフィールドはデフォルト値のままにします）。

	VCS Control	VCS Expressway
[名前（Name）]	「Traversal zone」など	「Traversal zone」など
タイプ（Type）	*Unified Communications traversal*	*Unified Communications traversal*
[接続クレデンシャル（Connection credentials）] セクション		
[ユーザ名（Username）]	「exampleauth」など	「exampleauth」など
[パスワード（Password）]	「ex4mpl3.c0m」など	[ローカル認証データベースの追加/編集（Add/Edit local authentication database）] をクリックし、ポップアップ ダイアロ

ユニファイド コミュニケーションの前提条件

	VCS Control	VCS Expressway
		グで [新規（New）] をクリックして、[名前（Name）] に（例：「exampleauth」）と [パスワード（Password）] に（例：「ex4mpl3.c0m」）を入力して、[クレデンシャルの作成（Create credential）] をクリックします。
[SIP] セクション		
ポート（Port）	7001	7001
TLS サブジェクト名の確認（TLS verify subject name）	N/A	トラバーサル クライアントの証明書で検索する名前を入力します（Subject Common Name または Subject Alternative Name 属性である必要があります）。トラバーサル クライアントのクラスタがある場合は、ここでクラスタ名を指定し、各クライアントの証明書に含まれることを確認します。
[認証（Authentication）] セクション		
認証ポリシー（Authentication policy）	*クレデンシャルを確認しない*	*クレデンシャルを確認しない*
[ロケーション（Location）] セクション		
ピア 1 アドレス（Peer 1 address）	VCS Expressway の FQDN を入力します。 注：IP アドレスを使用する場合（推奨していません）、そのアドレスが VCS Expressway サーバ証明書に含まれている必要があります。	N/A
ピア 2 ～ 6 アドレス（Peer 2...6 address）	VCS Expressway のクラスタである場合は、追加ピアの FQDN を入力します。	N/A

4. [ゾーンの作成（Create zone）] をクリックします。

ユニファイド コミュニケーションのサーバ証明書要件

Cisco Unified CM の証明書

Mobile & Remote Access で重要な 2 つの Cisco Unified Communications Manager 証明書は、*CallManager* 証明書と *tomcat* 証明書です。これらは Cisco Unified Communications Manager に自動的にインストールされ、デフォルトで自己署名されて同じ一般名（CN）を持ちます。

外部エンドポイントと内部エンドポイント間で最適なエンドツーエンドのセキュリティを達成するため、CA 署名付き証明書の使用を推奨します。ただし、自己署名証明書を使用する場合、この 2 つの証明書には、異なる一般名が必要です。これは、VCS が同じ CN を持つ二つの自己署名証明書を許可しないためです。*CallManager* と *tomcat* の自己署名証明書に VCN の信頼できる CA リストと同じ CN がある場合、そのうちの 1 つのみを信頼できます。その場合、VCS Control と Cisco Unified Communications Manager 間のセキュア HTTP またはセキュア SIP は失敗します。

また、Cisco Collaboration システム リリース 10.5.2 の製品に対する *tomcat* 証明書署名要求を作成する場合、CSCus47235 に注意する必要があります。ノードの FQDN がサブジェクト代替名として証明書にあることを保証するため、この問題を回避する必要があります。*VCS X8.5.2 リリース ノート*に回避策の詳細があります。

VCS 証明書

VCS の証明書署名要求（CSR）ツールでは、VCS でサポートされるユニファイド コミュニケーション機能に適した関連するサブジェクト代替名（SAN）について確認が求められ、組み込まれます。

次の表は、どのユニファイド コミュニケーションの機能にどの CSR 代替名の要素が適用されるかを示します。

サブジェクト代替名として↓次の項目を追加します	←これらの目的で CSR を生成する場合→			
	モバイル & リモート アクセス	Jabber Guest	XMPP フェデレーション	ビジネス ツー ビジネス コール
Unified CM 登録ドメイン	VCS Expressway でのみ必要	–	–	–
XMPP フェデレーション ドメイン	–	–	VCS Expressway でのみ必要	–
IM and Presence のチャット ノード エイリアス（フェデレーテッド グループ チャット）	–	–	必須	–
Unified CM 電話セキュリティ プロファイル名	VCS Control でのみ必要	–	–	–

ユニファイド コミュニケーションの前提条件

（注）

- IM and Presence ノードの追加または名前変更、新しい TLS 電話セキュリティ プロファイルの追加などにより、チャット ノード エイリアスが追加または名前変更された場合は、VCS Control 用に新しいサーバ証明書を作成することが必要になる場合があります。
- 新しいチャット ノード エイリアスがシステムに追加される場合、または Unified CM か XMPP フェデレーション ドメインが変更される場合は、新しい VCS Expressway の証明書を作成する必要があります。
- 新しくアップロードされたサーバ証明書を有効にするには、VCS を再起動する必要があります。

VCS Control / VCS Expressway の各機能要件についての詳細は、次のとおりです。

VCS Control サーバ証明書の要件

VCS Control サーバ証明書ではサブジェクト代替名のリストに、次の要素を含める必要があります。

- **Unified CM 電話セキュリティ プロファイル名**：暗号化された TLS 用に設定され、リモート アクセスを必要とするデバイスに使用される Unified CM のすべての**電話セキュリティ プロファイル**の FQDN 形式での名前。FQDN 形式を使用し、複数のエントリをカンマで区切ります。

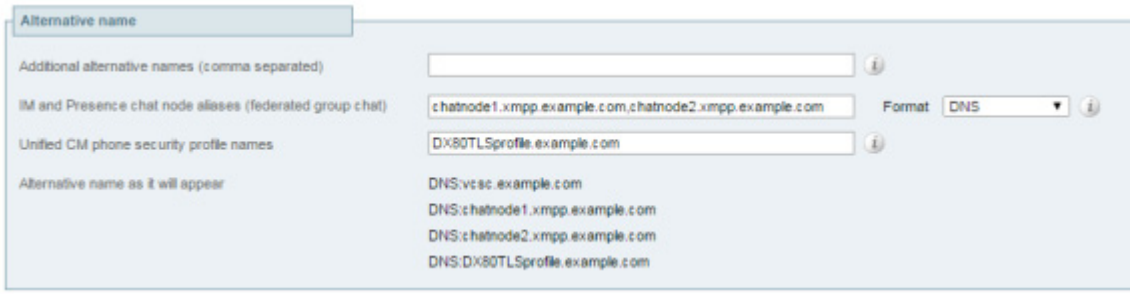
  代替名としてセキュア電話プロファイルを持つことで、これらのプロファイルを使用するデバイスからのメッセージ転送の場合、Unified CM は VCS Control と TLS 経由で通信できます。

- **IM and Presence チャット ノード エイリアス（フェデレーテッド グループ チャット）**：IM and Presence サーバで設定される**チャット ノード エイリアス**（たとえば chatroom1.example.com）。これらは、フェデレーテッド連絡先との TLS を介したグループ チャットをサポートするユニファイド コミュニケーション XMPP フェデレーション導入にのみ必要です。

  VCS Control は一連の IM&P サーバを検出すると、CSR にチャット ノード エイリアスを自動的に含めます。

  CSR を生成するときは、チャット ノード エイリアスに DNS 形式を使用することを推奨します。VCS Expressway サーバ証明書の代替名には、同一のチャット ノード エイリアスを含める必要があります。

図 3　VCS Control の CSR ジェネレータでのセキュリティ プロファイルおよびチャット ノード エイリアスに対するサブジェクト代替名の入力



ユニファイド コミュニケーションの前提条件

VCS Expressway サーバ証明書の要件

VCS Expressway サーバ証明書ではサブジェクト代替名のリストに、次の要素を含める必要があります。

- **[Unified CM 登録ドメイン（Unified CM registrations domains）]**：Unified CM の登録用に VCS Control で設定されているすべてのドメイン。これらはエンドポイント デバイスと VCS Expressway 間のセキュアな通信に必要です。

  DNS 形式を選択し、必要な FQDN を手動で指定します。複数のドメインが必要な場合は FQDN をカンマで区切ります。代わりに *CollabEdgeDNS* 形式を選択すると、入力したドメインにプリフィックス `collab-edge.` が追加されます。この形式は、トップ レベル ドメインを SAN として含めたくない場合に推奨されます（次のスクリーンショットの例を参照してください）。

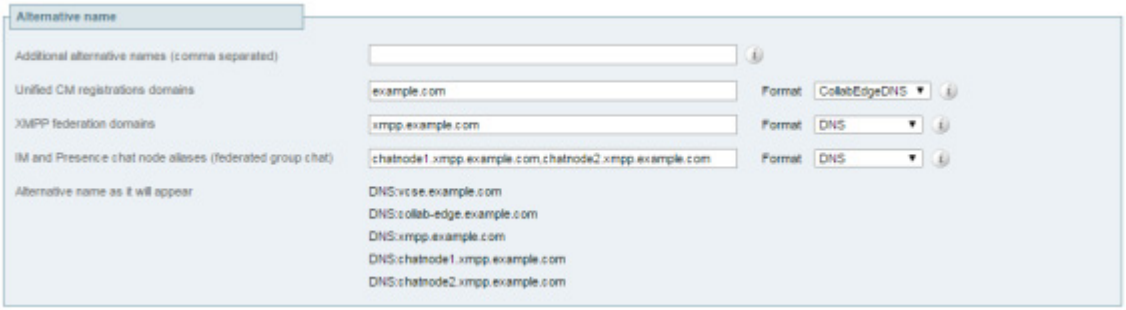
- **XMPP フェデレーション ドメイン**：ポイントツーポイント XMPP フェデレーションに使用するドメイン。これらは、IM&P サーバで設定され、XMPP フェデレーション用のドメインとして VCS Control でも設定する必要があります。

  DNS 形式を選択し、必要な FQDN を手動で指定します。複数のドメインが必要な場合は FQDN をカンマで区切ります。*XMPPAddress* 形式を使用しないでください。この形式は CA によってサポートされない可能性があり、VCS ソフトウェアの将来のバージョンでは廃止される可能性があります。

- **[IM and Presence チャット ノード エイリアス（フェデレーテッド グループ チャット）（IM and Presence chat node aliases (federated group chat)）**：VCS Control の証明書で入力されたものと同じ**チャット ノード エイリアス**のセット。フェデレーテッド連絡先との TLS を介したグループ チャットをサポートする音声とプレゼンスの導入にのみ必要です。

  VCS コントロールの同等の**[CSR の作成（Generate CSR）]** ページから、チャット ノード エイリアスのリストをコピーできます。

図 4　VCS Expressway の CSR ジェネレータでの Unified CM 登録ドメイン、XMPP フェデレーション ドメイン、およびチャット ノード エイリアスに対するサブジェクト代替名の入力



VCS の Mobile & Remote Access の設定

VCS の Mobile & Remote Access の設定

ここでは、VCS Control、VCS Expressway の Mobile & Remote Access 機能を有効にして設定するために必要な手順と、サービスに使用される Unified CM サーバと IM&P サーバを検出する方法について説明します。

VCS のセキュリティ証明書のインストールとセキュアなトラバーサル ゾーンの設定

ユニファイド コミュニケーション機能（Mobile & Remote Access、または Jabber Guest など）をサポートするには、VCS Control と VCS Expressway 間にユニファイド コミュニケーション トラバーサル ゾーン接続が必要です。次の内容を取り上げます。

- VCS Control と VCS Expressway に適切なセキュリティ証明書をインストールします。
- VCS Control と VCS Expressway 間のユニファイド コミュニケーション トラバーサル ゾーン接続を設定します。

この方法については、以下を参照してください。

- 「ユニファイド コミュニケーションのためのセキュアなトラバーサル ゾーン接続の設定」（p.15）（システムにセキュアなトラバーサル ゾーンが設定されていない場合）
- 「ユニファイド コミュニケーションのサーバ証明書要件」（p.18）

注：XMPP フェデレーションを使用する場合、証明書署名要求を生成する際に必要なすべての情報を使用できるように、VCS Control で IM&P サーバが検出できる必要があります。

VCS Control の設定

ここでは、VCS Control で必要な設定手順について説明します。

DNS および NTP 設定

VCS での基本的なシステム設定の確認および設定を行います。

1. **システムのホスト名**と**ドメイン名** が指定されていることを確認します（[システム（System）] > [DNS]）。
2. ローカル DNS サーバが指定されていることを確認します（[システム（System）] > [DNS]）。
3. すべての VCS システムが信頼できる NTP サービス（**[システム（System）] > [時間（Time）]**）に同期されていることを確認します。ローカル ポリシーに従って**認証**方式を使用します。

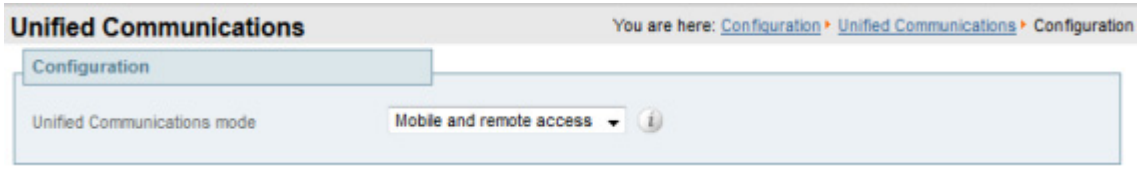
VCS のクラスタがある場合、すべてのピアに対してこの作業を実行します。

VCS の Mobile & Remote Access の設定

Mobile & Remote Access 用の VCS Control の有効化

Mobile & Remote Access 機能を有効にするには、次の手順を実行します。

1. [設定（Configuration）] > [ユニファイド コミュニケーション（Unified Communications）] > [設定（Configuration）] を選択します。
2. [ユニファイド コミュニケーション モード（Unified Communications mode）] を [モバイル アンド リモート アクセス（Mobile and remote access）] に設定します。
3. [保存（Save）] をクリックします。



注：関連するドメインとトラバーサル ゾーンを設定する前に、[モバイル アンド リモート アクセス（Mobile and remote access）] を選択する必要があります。

Unified CM にルーティングされるようにドメインを設定

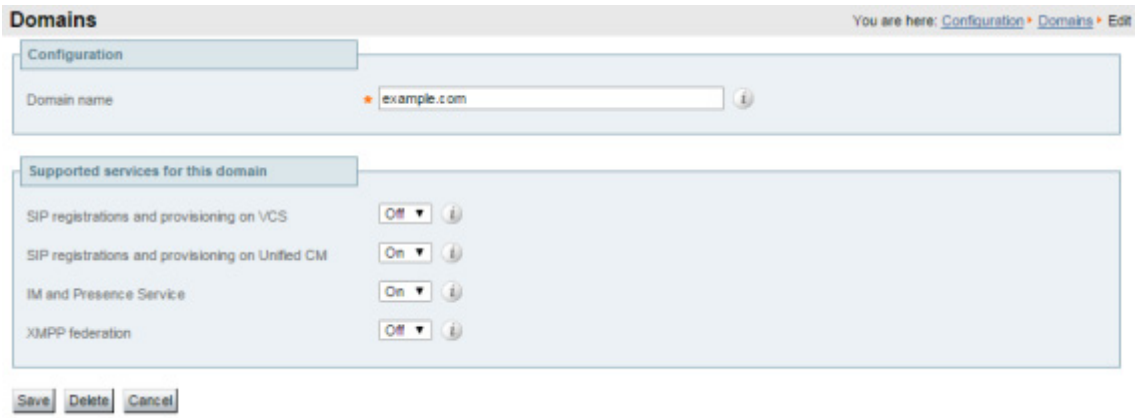
登録、コール制御、プロビジョニング、メッセージングおよびプレゼンス サービスが Unified CM にルーティングされるようにドメインを設定する必要があります。

1. VCS Control で、**[設定（Configuration）] > [ドメイン（Domains）]** を選択します。
2. サービスが Unified CM にルーティングされるドメインを選択します（まだドメインがない場合は、新しいドメインを作成します）。
3. ドメインごとに、そのドメインで VCS がサポートするサービスを *[オン（On）]* にします。使用可能なサービスは次のとおりです。
   - **VCS での SIP 登録とプロビジョニング**：VCS は、この SIP ドメインに対する権限があります。VCS はこのドメインの SIP レジストラおよびプレゼンス サーバとして機能し、このドメインを含むエイリアスの登録を試みるすべての SIP エンドポイントの登録要求を受け入れます。
   - **Unified CM での SIP 登録およびプロビジョニング**：この SIP ドメインのエンドポイントの登録、コール制御およびプロビジョニングのサービスが Unified CM によって提供されます。VCS はユニファイド コミュニケーション ゲートウェイとして機能し、Unified CM 登録にセキュアなファイアウォール トラバーサルおよび回線側のサポートを提供します。
   - **IM and Presence Service**：この SIP ドメインのインスタント メッセージングおよびプレゼンス サービスは、Unified CM IM and Presence サービスによって提供されます。
   - **XMPP フェデレーション**：このドメインとパートナー ドメイン間で XMPP フェデレーションを有効化します。

VCS の Mobile & Remote Access の設定

- **展開**：複数の展開がある場合は、ドメインと、選択された展開を関連付けます。1 つの展開のみが存在する場合（常に少なくとも 1 つの展開が存在する）、この設定はありません。

  ドメインごとに、該当するすべてのサービスを *[オン（On）]* にします。たとえば、同じドメインは、Jabber または EX シリーズ デバイスなど回線側のユニファイド コミュニケーション サポートを必要とするエンドポイント、およびサードパーティ SIP または H.323 デバイスなど VCS サポートを必要とするその他のエンドユーザにより使用されます、（このシナリオでは、このエンドポイントから送信されたシグナリング メッセージは、回線側のユニファイド コミュニケーションまたは VCS サポートが必要かどうかを表します）。



ユニファイド コミュニケーション サーバとサービスの検出

VCS Control は、MRA ユーザに登録、コール制御、プロビジョニング、ボイス メール、メッセージングおよびプレゼンス サービスを提供するユニファイド コミュニケーション サービス/ノードのアドレス詳細で設定する必要があります。

これらのサービスは WebEx クラウドで提供されるため、ハイブリッド モデルを展開する場合、IM and Presence Service の設定は必須ではありません。

注：この手順で設定された接続はスタティックです。検出されたユニファイド コミュニケーション ノードを再設定またはアップグレードした後は、VCS Control 上の設定を更新する必要があります。詳細については、「検出したノードを更新する必要がある理由」（27 ページ）を参照してください。

[設定（Configuration）] > [ユニファイド コミュニケーション（Unified Communications）] > [<UC サーバ タイプ>（<UC server type>）] に移動し、[サーバの更新（Refresh servers）]をクリックします。

VCS Control に提示する証明書の信頼

ユニファイド コミュニケーション サービスの検出時に **[TLS 検証モード（TLS verify mode）]** が *[オン（On）]* になっている場合は、IM and Presence Service ノードおよび Unified CM サーバによって提示される証明書を信頼するように VCS Control を設定する必要があります。

VCS の Mobile & Remote Access の設定

1. アップロードする適切な CA 証明書を特定します。
   - サーバの Tomcat および CallManager 証明書が CA 署名付きの場合は、VCS Control の信頼できる CA リストに証明書発行者のルート CA が含まれている必要があります。
   - サーバで自己署名証明書を使用する場合は、VCS Control の信頼できる CA のリストに、検出されたすべての IM and Presence Service ノード、Cisco Unity Connection サーバ、Unified CM サーバからの自己署名証明書が含まれている必要があります。
2. VCS Control に、必要な証明書をアップロードします（**[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 certificate）]**）。
3. VCS Control を再起動します（**[メンテナンス（Maintenance）] > [オプションの再起動（Restart options）]**）。

Unified CM サーバの検出

1. VCS Control で、**[設定（Configuration）] > [ユニファイド コミュニケーション（Unified Communications）] > [Unified CM サーバ（Unified CM servers）]** を選択します。

   このページには、すでに検出されている Unified CM ノードがリストされます。
2. Unified CM パブリッシャ ノードの詳細を追加します。

   1.[新規（New）] をクリックします。

   2.**Unified CM パブリッシャのアドレス**を入力します。

   [TLS 検証モード（TLS verify mode）] が [オン（On）] の場合は、FQDN を入力する必要があります。

   3. このサーバにアクセスできるアカウントの **[ユーザ名（Username）]** と **[パスワード（Password）]** を入力します。

   注：これらのクレデンシャルは VCS のデータベースに恒久的に保存されます。対応する Unified CM ユーザには、*Standard AXL API Access* ロールが必要です。

   4.（推奨）**[TLS 検証モード（TLS verify mode）]** を *[オン（On）]* に切り替えたままにし、VCS でノードの証明書を確実に確認できるようにします。

   Unified CM ノードは、AXL および UDS クエリー用の Tomcat 証明書と後続の SIP トラフィック用の CallManager 証明書を表します。Unified CM サーバで自己署名証明書を使用する場合は、VCS Control の信頼できる CA のリストに、すべての Unified CM サーバからの Tomcat 証明書と CallManager 証明書のコピーを含める必要があります。

   5.（任意）このノード/クラスタが属する展開を選択します。

   複数の展開を作成していない場合、[展開（Deployment）] フィールドは表示されません。複数の展開を使用しないように選択した場合、すべてのノードはデフォルトの展開に属します。

   6.[アドレスの追加（Add address）] をクリックします。

   TLS 検証モードを有効にすると、VCS は、セキュアな接続を確立できるかどうかをテストします。したがって、検出プロセスを進める前に、TLS 設定エラーを見つけることができます。

セキュア接続テストが成功した場合、または TLS 検証モードを有効にしていない場合は、パブリッシャへのアクセスと、関連付けられたノードの詳細の取得が試行されます。

3. 必要に応じて、他の Unified CM ノード/クラスタで検出手順を繰り返します。
4. 複数のパブリッシャ アドレスを設定した後、すべてのノードの詳細情報を更新するために、[サーバの更新（Refresh servers）] をクリックします。

IM および Presence サービス ノードの検出

1. VCS Control で、**[設定（Configuration）] > [ユニファイド コミュニケーション（Unified Communications）] > [IM and Presence Service ノード（IM and Presence Service nodes）]** を選択します。

   このページには、すでに検出されている IM and Presence Service ノードがリストされます。

2. 次のように、IM and Presence Service データベース パブリッシャ ノードの詳細を追加します。

   1.[新規（New）] をクリックします。

   2.**IM and Presence Service データベース パブリッシャ ノード**のアドレスを入力します。

   [TLS 検証モード（TLS verify mode）] が [オン（On）] の場合は、FQDN を入力する必要があります。

   3. このサーバにアクセスできるアカウントの **[ユーザ名（Username）]** と **[パスワード（Password）]** を入力します。

   注：これらのクレデンシャルは VCS のデータベースに恒久的に保存されます。対応する IM and Presence Service ユーザには、*Standard AXL API Access* ロールがある必要があります。

   4.（推奨）**[TLS 検証モード（TLS verify mode）]** を *[オン（On）]* に切り替えたままにし、VCS でノードの Tomcat 証明書を確実に確認できるようにします（XMPP 関連の通信の場合）。

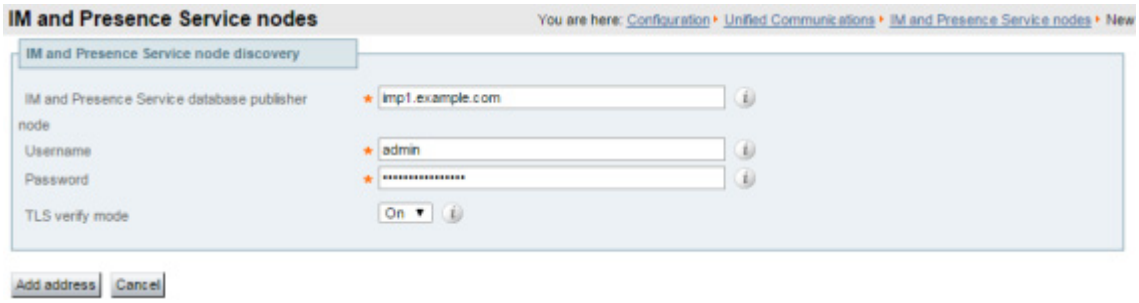
   5.（任意）このノード/クラスタが属する展開を選択します。

   複数の展開を作成していない場合、[展開（Deployment）] フィールドは表示されません。複数の展開を使用しないように選択した場合、すべてのノードはデフォルトの展開に属します。

6.[アドレスの追加（Add address）] をクリックします。

TLS 検証モードを有効にすると、VCS は、セキュアな接続を確立できるかどうかをテストします。したがって、検出プロセスを進める前に、TLS 設定エラーを見つけることができます。

セキュア接続テストが成功した場合、または TLS 検証モードを有効にしていない場合は、パブリッシャへのアクセスと、関連付けられたノードの詳細の取得が試行されます。



注：検出されたノードのステータスは、VCS Control と VCS Expressway 間に有効なトラバーサル ゾーン接続が存在しない限り（設定されていない可能性がある）、**[非アクティブ（Inactive）]** になります。

3. 必要に応じて、他の IM and Presence Service ノード/クラスタで検出手順を繰り返します。
4. 複数のパブリッシャ アドレスを設定した後、すべてのノードの詳細情報を更新するために、[サーバの更新（Refresh servers）] をクリックします。

Cisco Unity Connection サーバの検出

1. VCS Control で、**[設定（Configuration）] > [ユニファイド コミュニケーション（Unified Communications）] > [Unity Connection サーバ（Unity Connection servers）]** を選択します。

   このページには、すでに検出されている Cisco Unity Connection ノードがリストされます。

2. Cisco Unity Connection パブリッシャ ノードの詳細を追加します。

   1.[新規（New）] をクリックします。

   2.**Unity Connection のアドレス**を入力します。

   [TLS 検証モード（TLS verify mode）] が [オン（On）] の場合は、FQDN を入力する必要があります。

   3. このサーバにアクセスできるアカウントの **[ユーザ名（Username）]** と **[パスワード（Password）]** を入力します。

   注：これらのクレデンシャルは VCS のデータベースに恒久的に保存されます。

   4.（推奨）**[TLS 検証モード（TLS verify mode）]** を *[オン（On）]* に切り替えたままにし、VCS で Tomcat 証明書を確実に確認できるようにします。

   5.（任意）このノード/クラスタが属する展開を選択します。

   複数の展開を作成していない場合、[展開（Deployment）] フィールドは表示されません。複数の展開を使用しないように選択した場合、すべてのノードはデフォルトの展開に属します。

6.[アドレスの追加（Add address）] をクリックします。

TLS 検証モードを有効にすると、VCS は、セキュアな接続を確立できるかどうかをテストします。したがって、検出プロセスを進める前に、TLS 設定エラーを見つけることができます。

セキュア接続テストが成功した場合、または TLS 検証モードを有効にしていない場合は、パブリッシャへのアクセスと、関連付けられたノードの詳細の取得が試行されます。

3. 必要に応じて、他の Cisco Unity Connection ノード/クラスタで検出手順を繰り返します。
4. 複数のパブリッシャ アドレスを設定した後、すべてのノードの詳細情報を更新するために、[サーバの更新（Refresh servers）] をクリックします。

自動的に生成されたゾーンと検索ルール

VCS Control は、それ自体と検出された各 Unified CM ノード間に設定できないネイバー ゾーンを自動的に生成します。TCP のゾーンは必ず作成されます。また、Unified CM ノードの **[クラスタ セキュリティ モード（Cluster Security Mode）]**（**[システム（System）] > [エンタープライズ パラメータ（Enterprise Parameters）] > [セキュリティ パラメータ（Security Parameters）]**）が *[1（Mixed）]* に設定されている場合、TLS ゾーンも作成されます（セキュア プロファイルでプロビジョニングされたデバイスをサポートできるようにするため）。TLS ゾーンは、Unified CM 検出で **[TLS 検証モード（TLS verify mode）]** が有効になっている場合、**[TLS 検証モード（TLS verify mode）]** は *[オン（On）]* で設定されます。これは、VCS Control が後続の SIP 通信用の CallManager 証明書を確認することを意味します。各ゾーンは「CEtcp-<node name>」または「CEtls-<node name>」の形式で作成されます。

また、同じ命名規則に従って、設定不可能な検索ルールが各ゾーンに自動的に作成されます。ルールはプライオリティ 45 で作成されます。検索ルールの対象となる Unified CM ノード名が長い場合、検索ルールは正規表現を使ってアドレスのパターンマッチを行います。

注：登録エンドポイントにルーティング情報を戻す際、ロード バランシングは Unified CM で管理されます。

検出されたノードを更新する理由

VCS Control は、ユニファイド コミュニケーション ノードを検出すると、ゾーン、およびそのノードに向けてネットワークの外部から発信されるプロキシ要求の検索ルールを作成する上で必要な情報を読むための接続を確立します。

この情報は、静的なものです。つまり、手動で新しいノードの検出を開始するか、以前検出されたノードの設定を更新する場合にのみ、VCS はその情報を読みます。検出後、関連する設定がノードで変更された場合、新しい設定と VCS Control がそのノードについて認識している内容の不一致によって、障害が発生する場合があります。

VCS Control がユニファイド コミュニケーション ノードから読む情報は、各ノード タイプおよびロールによって異なります。次のリストには、VCS からの更新を必要とすると予想される UC 設定の例が含まれています。リストはすべてを網羅するものではありません。ノード上の設定変更が MRA サービスに影響を与えていると思われる場合は、潜在的な問題となる既知のソースを削除するため、これらのノードを更新する必要があります。

VCS の Mobile & Remote Access の設定

- クラスタの変更（たとえばノードの追加または削除）
- セキュリティパラメータの変更（たとえば混合モードの有効化）
- 接続ソケットの変更（たとえばSIPポートの設定）
- TFTP サーバの設定変更
- ノードのソフトウェア アップグレード

VCS Control での HTTP サーバ許可リストの設定

Jabber クライアント エンドポイントは、企業内のその他の Web サービスへのアクセスが必要になる場合があります。これには、企業外から取得する HTTP トラフィックに対するアクセス権を VCS が付与するようにサーバの許可リストを設定する必要があります。

次に、許可リストに追加する必要がある機能とサービスの例を示します。

- 表示によるボイスメール
- Jabber 更新サーバ
- カスタム HTML タブ/アイコン
- Photo Host ディレクトリ
- 高度なファイル転送（AFT）
- 問題レポート ツール サーバ

注：AFT 機能が VCS で機能するようにするには、すべての Unified CM IM および Presence Service のクラスタで Unified CM IM ノードと Presence Service ノードが手動または自動で許可リストに追加されていることを確認します。

HTTP アクセスを許可するアドレスを設定するには、次の手順を実行します。

1. VCS Control で、**[設定（Configuration）] > [ユニファイド コミュニケーション（Unified Communications）] > [設定（Configuration）]** を選択します。
2. [HTTP サーバ許可リスト（HTTP server allow list）] をクリックします。
3. 外部 Jabber クライアントがアクセスできる HTTP サーバのホスト名または IP アドレスを設定します。

   クライアントが提供する URI のサーバ部分がここに入力した名前のいずれかに一致する場合、または DNS ルックアップで、指定した IP アドレスに解決される場合にアクセスが許可されます。

VCS Control は検出した（CallManager および TFTP サービスを実行中の） Unified CM のノード、IM および Presence Service のノード、ならびに Cisco Unity Connection のノードをすべて許可リストに追加します。これらのエントリは削除できません。これらのエントリが [HTTP サーバ許可リスト（HTTP server allow list）] ページの [自動設定許可リスト（Auto-configured allow list）] セクションに表示されます。

VCS の Mobile & Remote Access の設定

VCS Expressway の設定

ここでは、VCS Expressway で必要な設定手順について説明します。

DNS および NTP 設定

VCS での基本的なシステム設定の確認および設定を行います。

1. **システムのホスト名**と**ドメイン名** が指定されていることを確認します（[システム（System）] > [DNS]）。
2. パブリック DNS サーバが指定されていることを確認します（[システム（System）] > [DNS]）。
3. すべての VCS システムが信頼できる NTP サービス（**[システム（System）] > [時間（Time）]**）に同期されていることを確認します。ローカル ポリシーに従って**認証**方式を使用します。

VCS のクラスタがある場合、すべてのピアに対してこの作業を実行します。

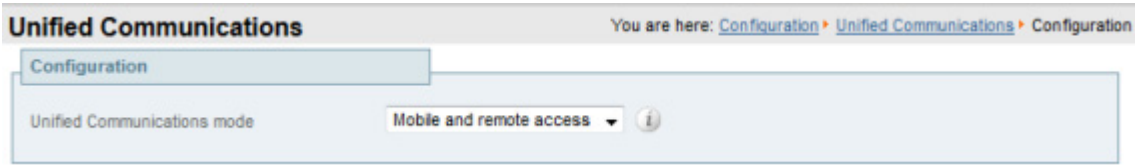
注：**<System host name>.<Domain name>** の組み合わせが、この VCS Expressway の FQDN です。この FQDN がパブリック DNS で解決可能であることを確認します。

VCS Expressway のクラスタがある場合、各ピアの**[ドメイン名（Domain name）]**が同じであり、*大文字と小文字が区別されること*を確認してください。

Mobile & Remote Access 用の VCS Expressway の有効化

Mobile & Remote Access 機能を有効にするには、次の手順を実行します。

1. [設定（Configuration）] > [ユニファイド コミュニケーション（Unified Communications）] > [設定（Configuration）] を選択します。
2. [ユニファイド コミュニケーション モード（Unified Communications mode）] を [モバイル アンド リモート アクセス（Mobile and remote access）] に設定します。
3. [保存（Save）] をクリックします。



TURN サービスが VCS Expressway で無効になっていることの確認

TURN サービスが Mobile & Remote Access に使用する VCS Expressway で無効にされていることを確認します。

1. [設定（Configuration）] > [トラバーサル（Traversal）] > [TURN] を選択します。
2. [TURN サービス（TURN services）] が [オフ（Off）] になっていることを確認します。

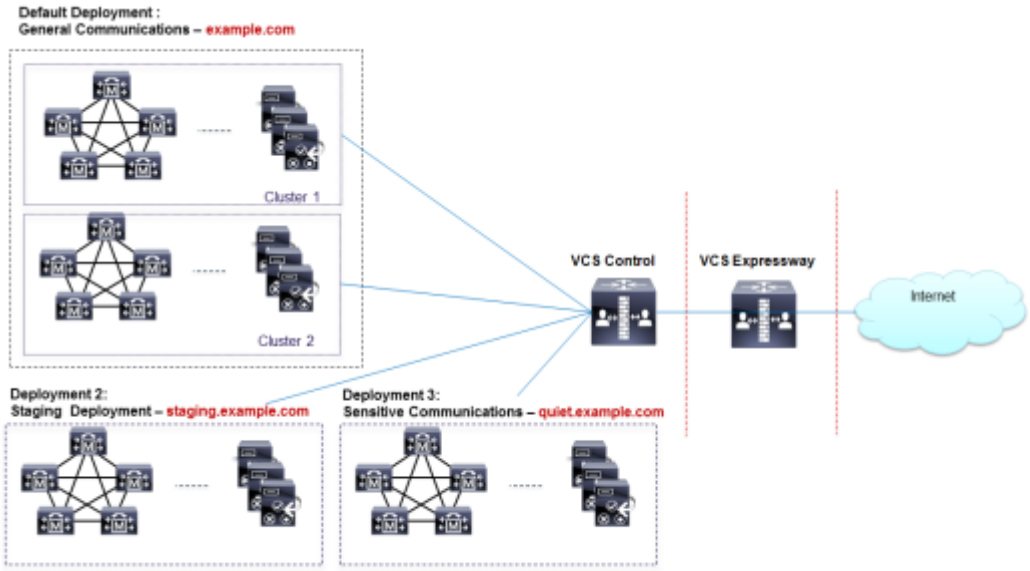
ユニファイド コミュニケーション サービスをパーティション化するための配置の使用

配置とは、Unified CM、Cisco Unity Connection、および IM and Presence Service ノードなどのドメインまたは 1 つ以上のユニファイド コミュニケーション サービス プロバイダーを包含するために使用される抽象的な境界です。

配置を複数にする目的は、Mobile & Remote Access（MRA）ユーザが使用できるユニファイド コミュニケーション サービスをパーティション化することです。これにより、異なる MRA ユーザのサブセットが、同じ VCS のペアを介して異なるセットのサービスにアクセスできます。配置を 10 より多くしないようお勧めします。

たとえば、ライブ MRA 環境と準備中の環境をそれぞれ構築するには、2 セットのユニファイド コミュニケーション インフラストラクチャの実装を検討します。またこの実装では、機密通信用に独立した環境も必要になる可能性があります。

図 5　ネットワーク外からアクセスされるユニファイド コミュニケーション サービスをパーティション化するための複数の配置



配置と関連のドメインおよびサービスは VCS Control で設定されます。

変更しなければ「デフォルト配置（Default deployment）」という名前のプライマリ配置が 1 つ存在します。追加の配置を作成して設定するまで、すべてのドメインとサービスがプライマリ配置に自動的に包含されます。このプライマリ配置は、名前が変更されても、メンバーが存在しなくても削除できません。

Mobile & Remote Access を介して提供するサービスをパーティション化するには、必要な数の配置を作成し、それぞれの配置に異なるドメインを関連付けます。それから、必要なユニファイド コミュニケーション リソースをそれぞれの配置に関連付けます。

ユニファイド コミュニケーション サービスをパーティション化するための配置の使用

1 つのドメインを複数の配置に関連付けることはできません。同様に、それぞれのユニファイド コミュニケーション ノードは、1 つの配置のみに関連付けることができます。

新しい配置を作成するには、次の手順を実行します。

1. VCS Control にログインします。
2. [設定（Configuration）] > [ユニファイド コミュニケーション（Unified Communications）] > [配置（Deployments）] を選択して、[新規（New）] をクリックします。
3. 配置に名前を付けて、[配置の作成（Create deployment）] をクリックします。

   新しい配置は、[配置（Deployments）] ページに表示され、ドメインまたは UC サービスを編集するときに選択可能です。

ドメインを配置に関連付けるには、次の手順を実行します。

1. [設定（Configuration）] > [ドメイン（Domains）] を選択します。

   ドメインと関連のサービスがここにリストされます。[配置（Deployments）] 列に、リストされたドメインを関連付ける場所が表示されます。
2. ドメイン名をクリックするか、新しいドメインを作成します。
3. [配置（Deployment）] フィールドで、このドメインを包含する配置を選択します。
4. [保存（Save）] をクリックします。

Unified CM またはその他のサーバ/サービスを配置に関連付けるには、次の手順を実行します。

1. [設定（Configuration）] > [ユニファイド コミュニケーション（Unified Communications）] に移動して、[Unified CM サーバ（Unified CM servers）] か [IM and Presence サービス ノード（IM and Presence Service nodes）] または [Unity Connection サーバ（Unity Connection servers）] を選択します。

   以前に検出された、選択したタイプのサービス ノードがここに表示されます。[配置（Deployments）] 列に、リストされたノードを関連付ける場所が表示されます。

   リストに情報が適切に挿入されていない場合は、「ユニファイド コミュニケーション サーバおよびサービス」（23 ページ）を参照してください。
2. サーバ/サービス ノード名をクリックします。
3. [配置（Deployment）] フィールドで、このサーバ/サービス ノードを包含する配置を選択します。
4. [保存（Save）] をクリックします。

   注：この変更を保存すると、VCS Control によってノードへの接続が更新され、接続されたユーザ向けのサービスが一時的に中断される場合があります。
5. 配置に属するその他のユニファイド コミュニケーション サービスで手順を繰り返してください。

コラボレーション エッジ経由のシングル サインオン（SSO）

ネットワークの外側からユニファイド コミュニケーション サービスにアクセスするエンドポイント用のシングル サインオンを有効にするには、この機能を使用します。エッジ経由のシングル サインオンは、エッジでの VCS ペアのセキュアなトラバーサル機能に依存し、内部のサービス プロバイダーと外部で解決可能なアイデンティティ プロバイダー（IdP）間の関係を信頼します。

エンドポイントは、VPN を介して接続する必要はありません。1 つの ID と 1 つの認証メカニズムを使用して、複数のユニファイド コミュニケーション サービスにアクセスします。認証は IdP が行います。VCS または内部 Unified CM サービスでは認証されません。

サポートされるエンドポイント

- Cisco Jabber 10.6 以降

サポートされるユニファイド コミュニケーション サービス

- Cisco Unified Communications Manager 10.5(2) 以降
- Cisco Unity Connection 10.5(2) 以降
- Cisco Unified Communications Manager IM and Presence Service 10.5(2) 以降
- 他の内部 Web サーバ（たとえば、イントラネット）

仕組み

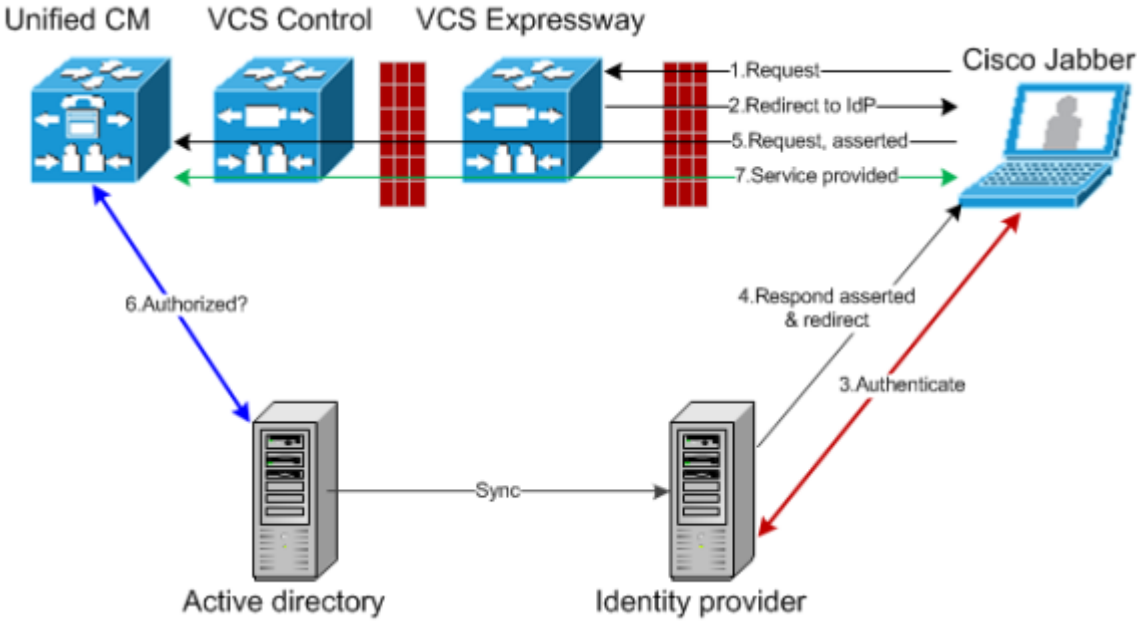
Cisco Jabber は、ユニファイド コミュニケーション サービスを要求する前に、組織のネットワーク内にいるかどうかを判定します。ネットワークの外側にいる場合は、ネットワークのエッジ上の VCS Expressway からのサービスを要求します。シングル サインオンがエッジで有効な場合、VCS Expressway は、ユーザを認証するよう署名要求を付けて IdP に Jabber をリダイレクトします。

IdP は、クライアント自体を識別するためにクライアントにチャレンジを行います。この ID が認証されると、IdP は、ID が本物であるという署名アサーションを付けて Jabber のサービス要求を VCS Expressway にリダイレクトして戻します。

VCS Expressway は IdP を信頼し、ネットワーク内の該当するサービスに要求を渡します。ユニファイド コミュニケーション サービスは、IdP と VCS Expressway を信頼するので、Jabber クライアントにサービスを提供します。

コラボレーション エッジ経由のシングル サインオン（SSO）

図 6　オンプレミス UC サービスのシングル サインオン



シングル サインオンの前提条件

VCS ペアについて

- VCS-E と VCS-C は、ネットワーク エッジで連携するように設定されている。
- VCS Control と VCS Expressway 間のユニファイド コミュニケーション トラバーサル ゾーン接続が設定されている。
- SSO を介してアクセスされる SIP ドメインは VCS Control 上で設定されている。
- VCS Control は Mobile & Remote Access モードであり、必要な Unified CM リソースが検出されている。
- 必要な Unified CM リソースのホスト名は、VCS Control 上の HTTP サーバ許可リストに追加されている。
- 複数の配置を使用する場合、SSO でアクセスされる Unified CM リソースは、Jabber クライアントからコールされるドメインと同じ展開内にある。

Cisco Jabber クライアントについて

- クライアントは、正しいドメイン名/SIP URI/チャット エイリアスを使用して内部サービスを要求するように設定されている。
- デフォルト ブラウザは VCS Expressway および IdP を解決できる。

アイデンティティ プロバイダーについて

IdP 証明書に含まれるドメインは、クライアントが IdP を解決できるように、DNS で公開されなければならない。

コラボレーション エッジ経由のシングル サインオン（SSO）

アイデンティティ プロバイダー（IdP）の選択

シスコ コラボレーション ソリューションは、SAML 2.0（セキュリティ アサーション マークアップ言語）を使用して、ユニファイド コミュニケーション サービスを利用するクライアント用の SSO（シングル サインオン）を有効にします。

SAML ベースの SSO は、企業ネットワーク内からの UC サービス要求を認証するためのオプションです。現在は、Mobile & Remote Access（MRA）経由で外部から UC サービスを要求するクライアントにまで拡張されました。

使用する環境に SAML ベース SSO を選択した場合は、次の点に注意してください。

- SAML 2.0 は、SAML 1.1 との互換性がないため、SAML 2.0 標準を使用する IdP を選択する必要があります。
- SAML ベースのアイデンティティ管理は、コンピューティングとネットワーキング業界のベンダーによって異なる方法で実装されています。したがって、SAML 標準に準拠するための幅広く受け入れられている規制はありません。
- 選択した IdP の設定や管理ポリシーは、Cisco TAC（テクニカル アシスタンス センター）のサポート対象外です。IdP ベンダーとの関係とサポート契約を利用して、IDP を正しく設定する上での支援を得られるようにしてください。シスコは IdP に関するエラー、制限、または特定の設定に関する責任を負いません。

シスコ コラボレーション インフラストラクチャは、SAML 2.0 への準拠を主張する他の IdP と互換性がある可能性もありますが、シスコ コラボレーション ソリューションでテストされているのは次の IdP だけです。

- OpenAM 10.0.1
- Active Directory Federation Services 2.0（AD FS 2.0）
- PingFederate® 6.10.0.4

ハイレベル タスク リスト

1. IdP で安全に認証できるように、アイデンティティ プロバイダーとオンプレミスのディレクトリ間の同期可能な関係を設定します。「*Directory Integration and Identity Management*」（『Cisco Collaboration System 10.x Solution Reference Network Designs (SRND)』マニュアル）を参照してください。
2. IdP から SAML メタデータ ファイルをエクスポートします。手順については、アイデンティティ プロバイダーに関するマニュアルを確認してください。たとえば、『*SAML SSO Deployment Guide for Cisco Unified Communications Applications*』の「*Enable SAML SSO through the OpenAM IdP（OpenAM IdP を通じて SAML SSO を有効にする*」を参照してください。
3. IdP からエクスポートした SAML メタデータ ファイルを、シングル サインオンでアクセスされる Unified CM サーバと Cisco Unity Connection サーバにインポートします。詳細については、ユニファイド コミュニケーションのマニュアルまたはヘルプを参照してください。
4. Unified CM サーバと Cisco Unity Connection サーバから SAML メタデータ ファイルをエクスポートします。たとえば、『*SAML SSO Deployment Guide for Cisco Unified Communications Applications*』の「*High-Level Circle of Trust Setup*」を参照してください。

コラボレーション エッジ経由のシングル サインオン（SSO）

5. IdP から SAML メタデータ ファイルをインポートして、VCS Control 上でアイデンティティ プロバイダーを作成します。
6. VCS Control 上の SIP ドメインに IdP を関連付けます。
7. SAML メタデータ ファイルを（プライマリ）VCS Control からエクスポートします。このファイルに（プライマリ）VCS Expressway の外部的に解決可能なアドレスが含まれていることを確認してください。

   VCS Control からの SAML メタデータ ファイルには、エッジと IdP 間の SAML 交換の署名と暗号化用の X.509 証明書、および IdP が VCS Expressway（ピア）にクライアントをリダイレクトするときに必要なバインディングが含まれます。
8. Unified CM サーバと Cisco Unity Connection サーバから SAML メタデータ ファイルを IdP にインポートします。OpenAM の使用例は、『*SAML SSO Deployment Guide for Cisco Unified Communications Applications*』に記載されています。
9. 同様に、VCS Control から IdP に SAML メタデータ ファイルをインポートします。詳細については IdP のマニュアルを参照してください。
10. エッジ（VCS Control および VCS Expressway 上）で SSO をオンにします。

IdP からの SAML メタデータのインポート

1. VCS Control で、**[設定（Configuration）] > [ユニファイド コミュニケーション（Unified Communications）] > [アイデンティティ プロバイダー（IdP）（Identity providers （IdP））]** を選択します。

   これを実行する必要があるのは、クラスタのプライマリ ピアのみです。
2. [SAML から新しい IdP をインポート（Import new IdP from SAML）] をクリックします。
3. [SAML ファイルをインポート（Import SAML file）] コントロールを使用して、IdP から SAML メタデータ ファイルを検索します。
4. [ダイジェスト（Digest）] を必須 SHA ハッシュ アルゴリズムに設定します。

   VCS はクライアントが IdP に提示する SAML 認証要求の署名にこのダイジェストを使用します。署名アルゴリズムは、SAML 認証要求の署名を検証するために IdP で想定されているものと一致している必要があります。
5. [アップロード（Upload] をクリックします。

   これで、VCS Control は、IdP の通信を認証し、IdP に対する SAML 通信を暗号化できます。

   注：メタデータをインポートした後は、**[設定（Configuration）] > [ユニファイド コミュニケーション（Unified Communications）] > [アイデンティティ プロバイダー（Idp）（Identity Provider （IdP））]** に移動して、IdP 行を検索し、**[アクション（Actions）]** 列で **[ダイジェストの設定（Configure Digest）]** をクリックして、署名アルゴリズムを変更できます。

コラボレーション エッジ経由のシングル サインオン（SSO）

IdP とドメインの関連付け

そのドメインの MRA ユーザによって IdP 経由で認証されるようにするには、IdP とドメインを関連付ける必要があります。IdP は少なくとも 1 つのドメインが関連付けられるまで値を追加しません。

ドメインと IdP 間には多対 1 の関係があります。1 つの IdP を複数のドメインに使用できますが、各ドメインに関連付けられる IdP は 1 つだけです。

VCS Control で、次の手順を実行します。

1. IdP リストを開き（[設定（Configuration）] > [ユニファイド コミュニケーション（Unified Communications）] > [アイデンティティ プロバイダー（IdP）（Identity providers (IdP)）]）、IdP がリストにあることを確認します。

   IdP はそのエンティティ ID 別に表示されます。それぞれ関連付けられたドメインが ID の横に表示されます。

2. IdP の行で [ドメインの関連付け（Associate domains）] をクリックします。

   この VCS Control 上のすべてのドメインリストが表示されます。この IdP にすでに関連付けられたドメインの横にはチェック マークが表示されます。また、リスト内の他のドメインに関連付けられている別の IdP がある場合は、IdP エンティティ ID も表示されます。

3. この IdP に関連付けるドメインの横にあるチェックボックスをオンにします。

   チェックボックスの横に [付け替え（Transfer）] が表示されている場合は、それをオンにすると、ドメインの既存の関連付けが解除されて、この IdP に関連付けられます。

4. [保存（Save）] をクリックします。

   選択したドメインがこの IdP に関連付けられます。

VCS Control からの SAML メタデータのエクスポート

注：VCS Control の SAML メタデータをエクスポートするには、その前に VCS Control で、VCS Expressway との有効な接続を確立する必要があります。

1. [設定（Configuration）] > [ユニファイド コミュニケーション（Unified Communications）] > [SAML データのエクスポート（Export SAML data）] を選択します。

   このページには、接続された VCS Expressway、またはクラスタの場合はすべての VCS Expressway ピアが表示されます。そのようにリストされるのは、それらに関するデータが VCS Control の SAML メタデータに含まれるためです。

2. （条件付き）複数の展開を設定する場合、SAML メタデータをエクスポートする前に展開を選択する必要があります。

3. [ダウンロード（Download）] または [すべてをダウンロード（Download all）] をクリックします。

   このページには、すべての VCS Control ピアもリストされます。それぞれに SAML メタデータをダウンロードするか、.zip ファイルですべてをエクスポートできます。

コラボレーション エッジ経由のシングル サインオン（SSO）

4. 生成されたファイルは、SAML メタデータを IdP にインポートする必要があるときにアクセスできる安全な場所にコピーします。

IDP の設定

このトピックでは、MRA 経由の SSO 用に特定の IDP を使用するときに必要な既知の追加設定を取り上げます。

次に示す設定手順は、すでに説明した前提条件およびハイレベル タスクに加えて必要で、その一部はこのマニュアルの範囲外です。

Active Directory Federation Services 2.0

VCS Expressway 用に Relying Party Trust を作成したら、それぞれのエンティティのプロパティをいくつか設定し、VCS Expressway の想定どおりに、AD FS で SAML 応答が確実に生成されるようにします。

また要求規則をそれぞれの Relying Party Trust に追加する必要があります。これは、ユーザが認証する AD 属性値に SAML 応答 uid 属性を設定します。

これらの手順は、AD FS 2.0 で検証されています。ただし、AD FS 3.0 を使用する場合も、同じ設定が必要です。

それには、次のようなことが必要となります。

- 応答全体に署名します（メッセージおよびアサーション）
- アイデンティティを **uid** 属性として送信する要求規則を追加します。

全応答に署名するには、次の手順を実行します。

Windows PowerShell® で、それぞれの VCS Expressway の *<EntityName>* に対して、次のコマンドを繰り返します。

```
Set-ADFSRelyingPartyTrust -TargetName "<EntityName>" -SAMLResponseSignature MessageAndAssertion
```

それぞれの証明書利用者信頼に対してクレーム ルールを追加するには：

1. [クレーム ルールの編集（Edit Claims Rule）] ダイアログを開き、AD 属性をクレームとして送信する新しいクレーム ルールを作成します。
2. 内部システムに対して SSO ユーザを識別するもの（通常は電子メールまたは SAMAccountName）に一致する AD 属性を選択します。
3. Outgoing Claim Type として **uid** と入力します。

コラボレーション エッジ経由のシングル サインオン（SSO）

エッジでのシングル サインオンの有効化

VCS Control で、次の手順を実行します。

1. [設定（Configuration）] > [ユニファイド コミュニケーション（Unified Communications）] > [設定（Configuration）] を選択します。
2. [シングル サインオン サポート（Single Sign-on support）] を検索し、[オン（On）] を選択します。
3. [保存（Save）] をクリックします。

（任意）SIP 認証トークンの存続可能時間を延長するには、[SIP トークン追加存続可能時間（秒）（SIP token extra time-to-live (in seconds)）] に秒数を入力します。この設定によりユーザは、クレデンシャルの期限が切れた後もコールを受け入れることができる時間が少し得られます。ただし、この便利さと、セキュリティが危険にさらされる時間が増えることとのバランスをとる必要があります。

VCS Expressway で、次の手順を実行します。

1. [設定（Configuration）] > [ユニファイド コミュニケーション（Unified Communications）] > [設定（Configuration）] を選択します。
2. [シングル サインオン サポート（Single Sign-on support）] を検索し、[オン（On）] を選択します。
3. [保存（Save）] をクリックします。

（任意）VCS Control でホーム ノードを確認するかどうかを選択して、VCS Expressway による **`/get_edge_sso`** 要求への応答方法を選択します。

クライアントからの **`/get_edge_sso`** 要求では、クライアントが SSO によってユーザの認証を試行するかどうかを尋ねます。この要求で、クライアントは、VCS Control が、ユーザのホーム クラスタの検索に使用できるユーザのアイデンティティを提供します。

- [内部 SSO のアベイラビリティの確認（Check for internal SSO availability）] のデフォルト オプションは [はい（Yes）] です。

  VCS Expressway は VCS Control に要求を渡します。VCS Control は、Unified CM ノードの選択にラウンド ロビン アルゴリズムを使用し、そのノードに対して提供されたアイデンティティに対する UDS クエリーを実行します。Unified CM は、どのノードがユーザのホーム ノードか、そのノードはユーザ用に SSO を実行できるかどうかを判定し、VCS Control に結果を通知します。次に、VCS Control は、**`true`** または **`false`** の応答をクライアントに対して行う VCS Expressway に通知します。

- [内部 SSO のアベイラビリティの確認（Check for internal SSO availability）] に [いいえ（No）] を選択すると、次のようになります。

  VCS Expressway は、**`/get_edge_sso`** に対して常に **`true`** で応答します。ユーザのホーム Unified CM に対して内部要求を行わないため、SSO がそこで実際に使用できるかどうかを認識できません。

MRA 経由での Dial via Office-Reverse

クライアントは VCS Expressway から **true** 応答を受信すると、SSO 経由で **/get_edge_config** を試行します。**false** を受信した場合は、提供されているクレデンシャルを使用して **/get_edge_config** を試行します。エンタープライズ内の UDS によって管理されるアイデンティティから独立したクレデンシャルが対象になります。**true** を受信しても、実際はユーザのホーム ノードで SSO が有効になっていない場合は、**/get_edge_config** に失敗し、クライアントは他の認証オプションを試行しません。

選択するオプションは、実装によって完全に異なります。すべての Unified CM ノードが SSO に対応している同種の環境がある場合、[いいえ（No）] を選択して、応答時間と全体的なネットワーク トラフィックを軽減できます。一方、ロールアウト中、またはすべてのノードで SSO が使用可能であると保証できない場合、クライアントが使用する、エッジ設定の取得モードは、[はい（Yes）] を選択する必要があります。

MRA 経由での Dial via Office-Reverse

モバイル ワーカーには、オフィスで電話するときに体験するものと同じ高い品質、セキュリティと信頼性が必要です。これは、Dial via Office-Reverse （DVO-R）機能を有効にして、デュアルモード モバイル デバイスで Cisco Jabber を使用するだけで保証できます。DVO-R は会社からの Cisco Jabber 通話を自動的にルーティングします。

DVO-R はコール シグナリングと音声メディアを別々に処理します。モバイルのシグナリング、VCS でのリモート アクセスを含め、すべてのコール シグナリングは、クライアントと Cisco Unified Communications Manager 間の IP接続を経由します。音声メディアは、企業の公衆電話交換網（PSTN）ゲートウェイでセルラー インターフェイスおよびヘアピンを通過します。

音声をセルラー インターフェイスに移動させることで、IP 接続が失われた場合でも高品質のコールと安全に維持された音声を確保できます。

ユーザがコールを発信したときに、Cisco Unified Communications Manager からの折り返し電話が次のいずれかに向かうように DVO-R を設定することができます。

- ユーザのモバイル ID（携帯電話番号）。
- ユーザの代替番号（ホテルの部屋など）。

この機能は、関連システムの次のバージョンに依存します。

- Cisco Unified Communications Manager 11.0(1) 以降
- Cisco Jabber 11.1 以降

MRA 経由での Dial via Office-Reverse

図7 DVO-R のコール

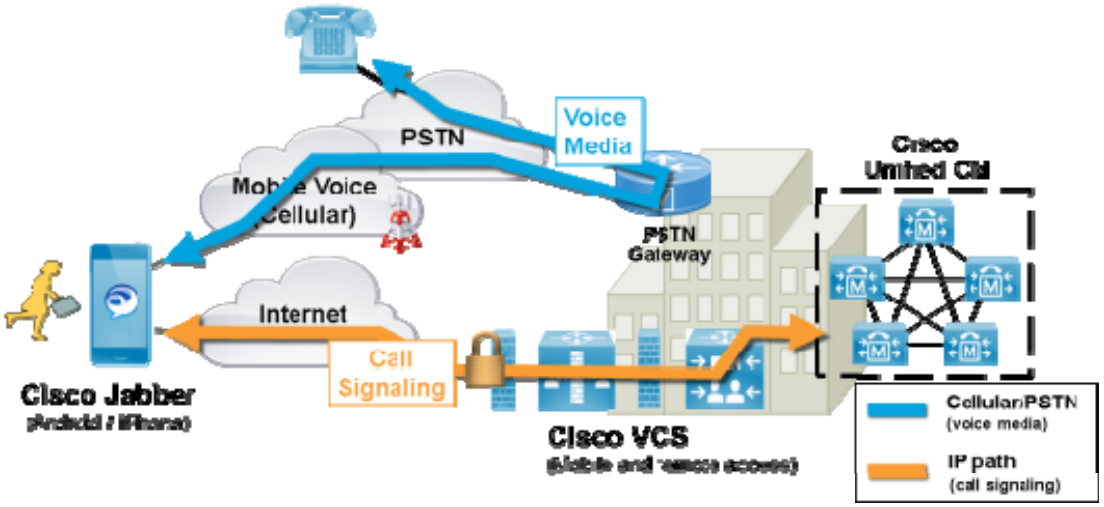
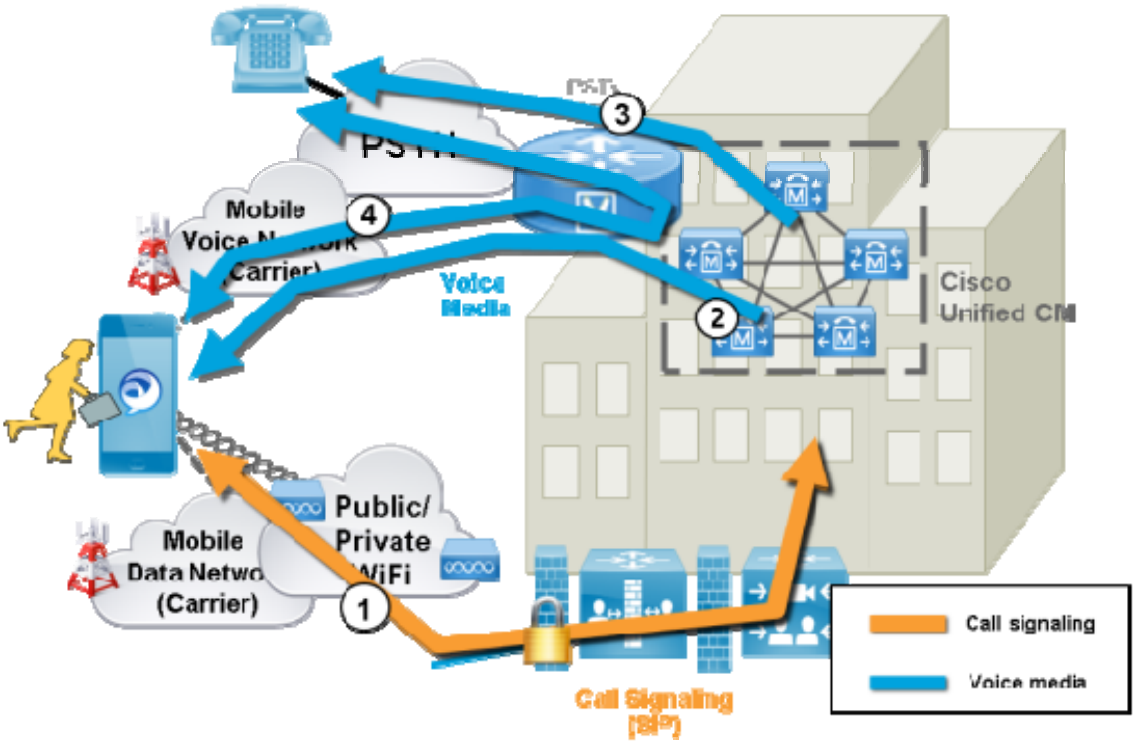
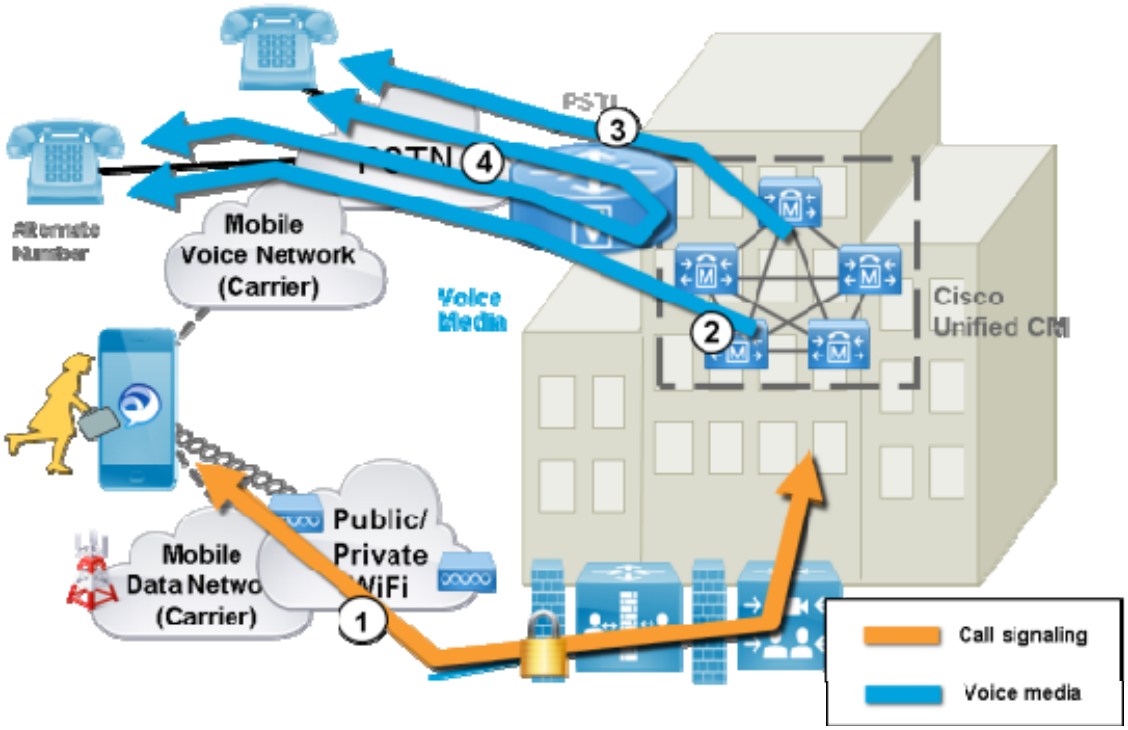


図8 モビリティ ID を使用する DVO-R



MRA 経由での Dial via Office-Reverse

図9　代替番号を使用した DVO-R



DVO-R を VCS Mobile & Remote Access で使用する方法

1. 番号をダイヤルすると、信号は IP パス（WLANまたはモバイル ネットワーク）上の Cisco Unified Communications Manager に送信されます。図 2 または 図 3 のステージ 1 を参照してください。
2. Cisco Unified Communications Manager がユーザの携帯電話番号または設定した代替番号にコールします（図 2 または 図 3 のステージ 2 を参照してください）。
3. ユーザが応答すると、Cisco Unified Communications Manager はユーザがダイヤルした番号にコールを延長し、ユーザには呼び出し音が聞こえます（図 2 または 図 3 のステージ 3 を参照してください）。
4. 相手が応答すると、進行中のコールが会社の PSTN ゲートウェイでヘアピンされます。

- モバイル ID を使用してコールを行うと、コールが会社のゲートウェイに固定されます。コールは携帯電話とデスクフォンの両方でアクティブであるため、この 2 つを切り替えることができます（図 2のステージ 4 を参照してください）。
- 代替番号を指定した場合、進行中のコールは固定されず、デスクフォンで電話を受けることはできません（図 3 のステージ 4 を参照してください）。

次の点に注意してください。

- PSTN ゲートウェイと Cisco Unified Communications Manager の間にアウトオブバンド デュアル トーン多重周波数ベース（DTMF） リレーが存在する場合、固定されたコールで DTMF 通話切替機能（たとえば *81 で保留）を使用できます。代替番号を使用している場合は通話切替機能を使用できません。

ユニファイド コミュニケーション サービスのステータスの確認

- ボイスメールにルーティングする Cisco Unified Communications Manager からのコールバックのレッグを防ぎ、それによりユーザがダイヤルする相手へのボイスメールのコールを停止するため、DVO-R のボイス メール ポリシーをユーザ制御に設定することを推奨します。これにより、コールを開始する前に、必ずキーパッド上のいずれかのキーを押して、DTMF トーンを生成する必要があります。

注：この機能は、現在モバイルおよびリモート アクセスでコールするユーザにおいて機能しますが、VCS 上に設定はありません。Unified CM ノードと Cisco Jabber クライアントで必要な設定があります。

DVO-R の設定チェックリスト

1. DVO-R をサポートするための Cisco Unified Communications Manager の設定
2. 各デバイスに対する DVO-R の設定
3. ユーザ制御のボイスメールの無効化のセットアップ
4. リモート接続先の追加（オプション）
5. Cisco Jabber クライアントの設定。

詳細については、http://www.cisco.com/c/en/us/support/unified-communications/telepresence-video-communication-server-vcs/products-configuration-examples-list.html の *Dial via Office リバース（DVO-R）を Mobile & Remote Access で動作するよう設定する [英語]* を参照してください。

ユニファイド コミュニケーション サービスのステータスの確認

VCS Control と VCS Expressway の両方で、ユニファイド コミュニケーション サービスのステータスを確認できます。

1. [ステータス（Status）] > [ユニファイド コミュニケーション（Unified Communications）] を選択します。
2. ドメイン、ゾーン、（VCS Control のみ）Unified CM および IM&P サーバの状態を確認します。

   設定エラーが存在する場合、その設定ページを表示するリンクが表示されます。

Mobile & Remote Access ポートのリファレンス

ここでは、内部ネットワーク（VCS Control が配置されている）と DMZ（VCS Expressway が配置されている）間、および DMZ とパブリック インターネット間のファイアウォールで使用する可能性があるポートの概要を示します。

VCS Control（プライベート）から VCS Expressway（DMZ）へのアウトバウンド

目的	プロトコル	VCS Control（送信元）	VCS Expressway（リスニング）
XMPP（IM and Presence）	TCP	一時ポート	7400
SSH（HTTP/S トンネル）	TCP	一時ポート	2222

Mobile & Remote Access ポートのリファレンス

目的	プロトコル	VCS Control（送信元）	VCS Expressway（リスニング）
トラバーサル ゾーン SIP シグナリング	TLS	25000 ～ 29999	7001
トラバーサル ゾーン SIP メディア（X8.1 以降での小規模/中規模システム用）	UDP	36000 ～ 59999 *	36000（RTP）、36001（RTCP）（デフォルト） 2776（RTP）、2777（RTCP）（旧デフォルト*）
トラバーサル ゾーン SIP メディア（大規模システム用）	UDP	36000 ～ 59999 *	36000 ～ 36011（6 ペアの多重化メディア トラバーサル用 RTP および RTCP ポート）

VCS Expressway（DMZ）からパブリック インターネットへのアウトバウンド

目的	プロトコル	VCS Expressway（送信元）	インターネットのエンドポイント（リスニング）
SIP メディア	UDP	36002 ～ 59999 または 36012 ～ 59999	1024 以上
SIP シグナリング	TLS	25000 ～ 29999	1024 以上

パブリック インターネットから VCS Expressway（DMZ）へのインバウンド

目的	プロトコル	インターネットのエンドポイント（送信元）	VCS Expressway（リスニング）
XMPP（IM and Presence）	TCP	1024 以上	5222
HTTP プロキシ（UDS）	TCP	1024 以上	8443
メディア	UDP	1024 以上	36002 ～ 59999 または 36012 ～ 59999 *
SIP シグナリング	TLS	1024 以上	5061
HTTPS（外部管理アクセスにのみ必要、非推奨）	TCP	1024 以上	443

VCS Control から内部インフラストラクチャとエンドポイントへ

目的	プロトコル	VCS Control（送信元）	内部デバイスのポート/範囲
XMPP（IM and Presence）	TCP	一時ポート	7400（IM and Presence）
HTTP プロキシ（UDS）	TCP	一時ポート	8443（Unified CM）
HTTP プロキシ（SOAP）	TCP	一時ポート	8443（IM and Presence）

Mobile & Remote Access ポートのリファレンス

目的	プロトコル	VCS Control（送信元）	内部デバイスのポート/範囲
HTTP（コンフィギュレーション ファイル取得）	TCP	一時ポート	6970（Unified CM）
CUC（ボイス メール）	TCP	一時ポート	443（Unity Connection）
Unity Connection からのメッセージ待機インジケータ（MWI）	TCP	一時ポート	7080（Unity Connection）
メディア	UDP	36000 ～ 59999 *	>= 1024（メディア受信者、エンドポイントなど）
SIP シグナリング	TCP	25000 ～ 29999	5060（Unified CM）
セキュア SIP シグナリング	TLS	25000 ～ 29999	5061（Unified CM）

* X8.1 以降の新規インストールでは、デフォルトのメディア トラバーサル ポートの範囲は 36000 ～ 59999 です。VCS Control では、**[設定（Configuration）] > [ローカル ゾーン（Local Zones）] > [トラバーサル サブゾーン（Traversal Subzone）]** で設定できます。大規模 VCS Expressway システムでは、その範囲の最初の 12 ポート（デフォルトでは、36000 ～ 36011）は多重化トラフィック用に常に予約されています。VCS Expressway はそれらのポートでリッスンします。大規模システムでは逆多重化リスニング ポートの範囲を明示的に設定することはできません。常にメディア ポート範囲内の最初の 6 ペアが使用されます。小規模/中規模のシステムでは、VCS Expressway で多重化 RTP/RTCP トラフィックをリッスンする 2 つのポートを明示的に指定できます（**[設定（Configuration）] > [トラバーサル（Traversal）] > [ポート（Ports）]**）。X8.2 以降にアップグレードすると、VCS Control は以前のバージョンのメディア トラバーサル ポートの範囲を保持します（50000 ～ 54999、または 36000 ～ 59999、送信元のバージョンにより異なります）。VCS Expressway は以前設定された逆多重化ペア（デフォルトでは 2776 と 2777、または 50000 と 50001、アップグレード パスにより異なります）を保持し、スイッチ **[設定された逆多重化ポートを使用する（Use configured demultiplexing ports）]** に *[はい（Yes）]* が設定されます。特定のペアのポートを設定しない場合、スイッチ **[設定された逆多重化ポートを使用する（Use configured demultiplexing ports）]** に *[いいえ（No）]* を設定すると、VCS Expressway はメディア トラバーサル ポート範囲内にあるポートの最初のペアでリッスンします（デフォルトでは 36000 と 36001）。この場合、新しいポートのファイアウォールを設定した後に、以前設定したポートを閉じることを推奨します。

次の点に注意してください。

- ポート 8191/8192 TCP および 8883/8884 TCP は、VCS Control、VCS Expressway アプリケーションで内部的に使用されます。このため、これらのポートは、他の目的で割り当てることはできません。VCS Expressway はポート 8883 で外部的にリッスンするため、そのポートに TCP トラフィックをドロップする外部 LAN インターフェイスにカスタム ファイアウォール ルールを作成することを推奨します。
- VCS Expressway は SSH トンネル トラフィックをポート 2222 でリッスンします。このようなトラフィックの唯一の正当な送信者は VCS Control（クラスタ）です。このため、SSH トンネル サービスの次のファイアウォール ルールを作成することを推奨します。

その他の情報

- VCS Control のピア アドレスすべてを許可する 1 つ以上のルール（必要に応じて、内部 LAN インターフェイス経由）
- 次に、SSH トンネル サービスのすべてのトラフィックをドロップするプライオリティの低い（数値が高い）ルール（必要に応じて、内部 LAN インターフェイス上、またその場合に、外部インターフェイスですべてのトラフィックをドロップする別のルール）

その他の情報

Unified CM ダイヤル プラン

Unified CM ダイヤル プランは、VCS で登録するデバイスの影響を受けません。リモートおよびモバイル デバイスは、Unified CM でも直接登録されますが、ダイヤル プランはローカルで登録された場合と同じです。

VCS のコール タイプとライセンス

VCS は次の 2 種類のコールを区別します。

- **Unified CM リモート セッション**：これらは、「Mobile & Remote Access」コール、つまり企業外にあり、Unified CM に登録されたエンドポイントに Expressway ファイアウォール トラバーサル ソリューション経由でルーティングされるデバイスからのビデオまたは音声コールです。これらのコールは、トラバーサルの負荷に影響しますが、いかなるタイプのコール ライセンスも必要ありません。
- **VCS トラバーサル コール**：これらは、Business-to-Business（B2B）、B2BUA コール（メディア暗号化または ICE 用）、および VCS がコール シグナリングとコール メディアの両方を行うサードパーティ ソリューションにインターワークされたコール、またはゲートウェイされたコールを含む、標準的な VCS ビデオまたは音声コールです。各コールがトラバーサル コール ライセンスを使用します。

  音声専用の SIP トラバーサル コールはビデオ SIP トラバーサル コールとは別に処理されます。それぞれのトラバーサル コール ライセンスで 1 つのビデオ コールまたは 2 つの音声のみの SIP コールが許可されます。したがって、100 のトラバーサル コール ライセンスでは、90 のビデオ コールと 20 の SIP 音声専用コールが同時に許可されます。他の音声専用コール（非トラバーサル、H.323 またはインターワーキング）が標準ビデオ コールのライセンス（状況に応じてトラバーサルまたは非トラバーサル）を使用します。
- **VCS 非トラバーサル コール**：これらは、シグナリングは VCS を経由して送信されますが、メディアはエンドポイント間、またはエンドポイントとコール ルートの他システム間を直接送信される、標準的な VCS ビデオまたは音声コールです。各コールが非トラバーサル コール ライセンスを使用します。Microsoft 相互運用コールは、（メディアが VCS を通過するとしても）非トラバーサル コールとして分類されます。

また各 VCS は最大 750 の同時発生非トラバーサル コールを許可します。

その他の情報

次の点に注意してください。

- VCS は「音声専用」SIP コールを、SDP で単一の「m=」行でネゴシエートされたコールと定義します。したがって、たとえば「電話」コールを作成する場合、SIP UA が SDP に追加の m= 行を含めると、そのコールはビデオ コール ライセンスを使用します。
- 「音声専用」SIP コールが確立されている間は、（ライセンス供与された）ビデオ コールとして扱われます。「音声専用」としてライセンスされるのは、コール設定が完了してからです。これは同時に行われた場合、システムがライセンスの最大数の制限に近づいていると、一部の「音声専用」コールに接続できない可能性があることを意味します。
- VCS はコール中のライセンス最適化はサポートしていません。

異なるドメインでの Unified CM と VCS の展開

Unified CM ノードと VCS のピアは異なるドメインに配置することができます。たとえば、Unified CM ノードを **enterprise.com** ドメインに置き、VCS システムを **edge.com** ドメインに置くことができます。

この場合、Unified CM ノードでは、**サーバのホスト名または IP アドレス**に IP アドレスまたは FQDN を使用して、VCS が該当する Unified CM ノードにトラフィックをルーティングできるようにする必要があります。

Unified CM サーバと IM&P サーバが同じドメインを共有する必要があります。

Unified CM と VCS Control 間の SIP トランク

Mobile & Remote Access 用の VCS 展開では、Unified CM と VCS Control 間の SIP トランク接続は必要ではありません。注：VCS Control と検出された各 Unified CM ノード間に自動的に生成されたネイバー ゾーンは SIP トランクではありません。

ただし、SIP トランクを必要に応じて設定できます （たとえば、VCS に登録された B2B 発信者またはエンドポイントを Unified CM に登録されたエンドポイントに対して有効にできます）。

SIP トランクが設定されている場合、Unified CM への SIP 回線登録に使用されるポートとは別のリスニング ポートを Unified CM で使用する必要があります。アラームは、競合が検出されると VCS Control で発生します。

Unified CM の回線登録リスニング ポートの設定

Unified CM への回線の登録に使用されるリスニング ポートは [システム（System）] > [Cisco Unified CM] で設定されます。

[SIP 電話ポート（SIP Phone Port）] フィールドと [SIP 電話セキュア ポート（SIP Phone Secure Port）] フィールドは、それぞれ TCP、TLS 接続に使用するポートを定義し、通常 5060/5061 に設定されます。

SIP トランク リスニング ポートの設定

SIP トランクに使用されるポートが Unified CM と VCS の両方で設定されます。

その他の情報

Unified CM で、次の手順を実行します。

1. [システム（System）] > [セキュリティ（Security）] > [SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）] を選択し、SIP トランクに使用するプロファイルを選択します。

   このプロファイルが他のデバイスからの接続に使用される場合、VCS への SIP トランク接続に異なるセキュリティ プロファイルを作成することもできます。
2. 回線の登録に使用されるものと異なる [着信ポート（Incoming Port）] を設定します。
3. [保存（Save）] をクリックして、[設定を適用（Apply Config）] をクリックします。

VCS で次の手順を実行します。

1. [設定（Configuration）] > [ゾーン（Zones）] > [ゾーン（Zones）] を選択し、SIP トランクを使用する Unified CM ネイバー ゾーンを選択します。

   （注：回線側の通信で VCS Control と検出された各 Unified CM ノード間に自動的に生成されたネイバー ゾーンは設定できません）。
2. SIP **ポート**を、Unified CM で設定された**着信ポート**と同じ値に設定します。
3. [保存（Save）] をクリックします。

SIP トランクの設定の詳細については、*Cisco TelePresence Cisco Unified Communications Manager と VCS（SIP トランク）導入ガイド*を参照してください。

セキュアな通信の設定

この展開には、VCS Control と VCS Expressway、および VCS Expressway と企業外にあるエンドポイント間のセキュアな通信が必要です。これには、HTTP、SIP および XMPP 向けの暗号化された TLS 通信、および該当する場合、証明書の交換と検査の要求が含まれます。Jabber エンドポイントでは、Unified CM に保持されたクレデンシャルに対して検証される有効なユーザ名とパスワードの組み合わせを指定する必要があります。すべてのメディアが SRTP で保護されます。

VCS Control は、それ自体と検出された各 Unified CM ノード間に設定できないネイバー ゾーンを自動的に生成します。TCP のゾーンは必ず作成されます。また、Unified CM ノードの **[クラスタ セキュリティ モード（Cluster Security Mode）]**（**[システム（System）] > [エンタープライズ パラメータ（Enterprise Parameters）] > [セキュリティ パラメータ（Security Parameters）]**）が *[1（Mixed）]* に設定されている場合、TLS ゾーンも作成されます（セキュア プロファイルでプロビジョニングされたデバイスをサポートできるようにするため）。TLS ゾーンは、Unified CM 検出で **[TLS 検証モード（TLS verify mode）]** が有効になっている場合、**[TLS 検証モード（TLS verify mode）]** は *[オン（On）]* で設定されます。これは、VCS Control が後続の SIP 通信用の CallManager 証明書を確認することを意味します。

注：Unified CM が混合モードでない場合は TCP を使用するためにセキュア プロファイルがダウングレードされます。

その他の情報

Unified CM に対する VCS のネイバー ゾーンは、Unified CM パブリッシャが VCS に追加（または更新）されたときに Unified CM から返された Unified CM ノードの名前を使用します。VCS は Unified CM ノードに接続するためにその返された名前を使用します。この名前がホスト名だけの場合：

- その名前を使用してルーティング可能である必要があります
- これは、VCS が Unified CM サーバ証明書に表示されることを想定する名前です

セキュア プロファイルを使用している場合、VCS Control の証明書に署名した認証局のルート CA が *CallManager の信頼*証明書（**Cisco Unified OS Administration** アプリケーションの **[セキュリティ（Security）] > [証明書の管理（Certificate Management）]**）としてインストールされていることを確認します。

メディア暗号化

メディア暗号化は VCS Control と VCS Expressway 間、および企業外にある VCS Expressway とエンドポイント間のコールレッグに実行されます。

暗号化は、メディアが VCS Control の B2BUA にパススルーするときに物理的に適用されます。

制限事項

- IPV4 プロトコルだけが Mobile & Remote Access ユーザに対してサポートされています
- デュアル ネットワーク インターフェイスを使用する VCS Expressway システムでは、XCP 接続（IM&P XMPP トラフィック用）は、常に外部でない（つまり内部）インターフェイスを使用します。これは VCS Expressway の内部インターフェイスが、別のネットワークセグメント上にあり、システム管理の目的でのみ使用され、VCS Control のトラバーサル ゾーンが VCS Expressway の外部インターフェイスに接続する展開の場合に、XCP 接続が失敗する可能性があることを意味します。

Mobile & Remote Access を使用する場合にサポートされないエンドポイント機能

- 複数回線をサポートする IP 電話とエンドポイント上の追加回線のコール。プライマリ回線だけが Mobile & Remote Access を介してサポートされます。
- UDS の以外のディレクトリ アクセス機能
- CAPF などのリモート エンドポイントに対する証明書のプロビジョニング
- SIP UPDATEメソッド（RFC 3311）に依存する機能は、VCS がこのメソッドをサポートしないため、期待どおりには動作しません。たとえば、CUCM とエンドポイントはブラインド転送を実装するために UPDATE を使用しますが、これは MRA 経由で正常に動作しません。
- IM and Presence Service および Jabber 使用時のピアツーピア ファイル転送は、MRA ではサポートされません
  - IM and Presence Service 10.5.2 以降および Jabber 10.6 以降のクライアントでのマネージドファイル転送（MFT）は、MRA 経由でサポートされます

その他の情報

  - WebEx Messenger Service および Cisco Jabber でのファイル転送は MRA 経由でサポートされます
- デスクフォン制御（QBE/CTI）
- GSM のハンドオフとセッションの永続性などの追加のモビリティ機能
- ハント グループ/ハント パイロット/ハント リスト
- セルフケア ポータル
- Jabber SDK のサポート
- 共有回線が限定的にサポートされます。複数のエンドポイントは、回線を共有できますが、（保留/再開のような）インコール機能は応答する最初のエンドポイントだけで機能します。回線を共有しているエンドポイントが正しくコールの状態を認識しない可能性があります。

Mobile and Remote Access を使用する場合の VCS の制限およびサポートされない機能

- VCS は、MRA に使用する場合に Jabber ゲスト用に使用できません。
- Mobile & Remote Access に使用する VCS Control は、Lync 2013 のゲートウェイとして使用できません（必要に応じて、これをスタンドアロン VCS Control に設定する必要があります）。
- VCS Control と IM&P サーバ間のセキュアな XMPP トラフィック（XMPP トラフィックは VCS Control と VCS Expressway、および VCS Expressway とリモート エンドポイント間でセキュア）。
- エンドポイント管理機能（SNMP、SSH/HTTP アクセス）。
- マルチドメインおよびマルチカスタマー サポートは次のように制限されています。
  - X8.5 より前では、それぞれの VCS 導入環境で、1 つの IM&P ドメインのみがサポートされていました（IM and Presence Service 10.0 以降で複数のプレゼンス ドメインがサポートされる場合でも）。
  - X8.5 では、VCS Control で複数の配置を作成できますが、この機能も配置あたり 1 つのドメインに制限されます。
  - X8.5.1 では、1 つの配置に複数のプレゼンス ドメインを含めることができます。この機能はプレビュー中ですが、現時点ではドメインを 50 より多くしないようお勧めします。
- Mobile & Remote Access 機能は FIPS 境界内にはありません。
- HTTP プロキシを介した NTLM 認証。
- メンテナンス モード：VCS Control または VCS Expressway がメンテナンス モードになっている場合、その VCS を通過する既存のコールがドロップされます。
- VCS Expressway では TURN サービスを有効化できません。
- 大規模 VM サーバへの配置では、Unified CM への登録は 2500 のプロキシ登録に制限されます（VCS アプライアンスまたは同等の VM と同じ制限）。

その他の情報

プロトコルの概要

次の表に、ユニファイド コミュニケーション ソリューションで使用されるプロトコルと関連するサービスを示します。

プロトコル	セキュリティ	サービス
SIP	TLS	セッション確立：登録、招待など
HTTPS	TLS	ログオン、プロビジョニング/構成、ディレクトリ、ボイスメール
RTP	SRTP	メディア：音声、ビデオ、コンテンツ共有
XMPP	TLS	インスタント メッセージ、プレゼンス、フェデレーション

クラスタ化された VCS システムとフェイルオーバーの考慮事項

VCS Control のクラスタと VCS Expressway のクラスタで、フェイルオーバー（冗長性）のサポートと拡張性の向上を提供するように設定できます。

VCS クラスタを設定する方法の詳細は、*VCS クラスタの作成およびメンテナンス導入ガイド*に記載されており、Jabber エンドポイントと DNS の設定方法に関する情報は、*「Cisco Jabber の DNS の設定」*に記載されています。

Unified CM および IM&P サーバを VCS Control で検出する場合は、プライマリ ピアで実行する必要があります。

認証のレート コントロール

VCSは、指定された設定可能な期間内に、ユーザのコラボレーション サービスを認証するためにユーザのクレデンシャルを使用できる回数を制限できます。この機能は、同じユーザを認証する複数のクライアント デバイスから、または必要以上に再認証されるクライアントからの、不注意による攻撃、または実際の DoS 攻撃を阻止するために設計されました。

ユーザを認証するためにクライアントがクレデンシャルを提供するたびに、VCS は、この試行が**レート コントロール期間**で指定された以前の秒数以内に**期間あたりの最大認証数**を超えているかどうかを確認します。

試行が選択された最大値を超えた場合、VCS は試行を拒否し、HTTP エラー429「Too Many Requests」を送信します。

承認レート コントロール設定は、**[設定（Configuration）] > [ユニファイド コミュニケーション（Unified Communications）] > [設定（Configuration）]** ページの **[詳細（Advanced）]** セクションで設定できます。

クレデンシャルのキャッシング

注：これらの設定は、MRA による認証に SSO（共通アイデンティティ）を使用するクライアントには適用されません。

VCS は Unified CM によって認証されたエンドポイントのクレデンシャルをキャッシュします。VCS が認証のために Unified CM にエンドポイント クレデンシャルを必ずしも送信する必要がないため、このキャッシュにより全体的なパフォーマンスが向上します。

その他の情報

このキャッシング設定は、**[設定（Configuration）] > [ユニファイド コミュニケーション（Unified Communications）] > [設定（Configuration）]** ページの **[詳細（Advanced）]** セクションで設定できます。

[クレデンシャル更新間隔（Credentials refresh interval）] は、VCS がクライアントの認証に成功するために送信する認証トークンのライフタイムを指定します。認証に成功したクライアントは、このトークンが期限切れになる前に更新をリクエストする必要があります。そうでない場合、再認証が必要になります。デフォルトは 480 分（8 時間）です。

[クレデンシャル クリーンアップ間隔（Credentials cleanup interval）] は、VCS がキャッシュ クリアの動作の間に待つ時間を指定します。キャッシュがクリアされると期限切れのトークンのみが削除されるため、この設定は期限切れのトークンがキャッシュに保持される最大の期間です。デフォルトは 720 分（12 時間）です。

Unified CM サービス拒否のしきい値

大量の Mobile & Remote Access コールで Unified CM のサービス拒否のしきい値に達することがあります。これは、すべてのコールが同じ VCS Control（クラスタ）から Unified CM に着信するためです。

必要に応じて、**[SIP ステーション TCP ポート スロットルしきい値（SIP Station TCP Port Throttle Threshold）]** のレベルを 750 KB/秒に上げることを推奨します（**[システム（System）] > [サービス パラメータ（Service Parameters）]** から *[Cisco CallManager]* サービスを選択）。

VCS の自動侵入防御

まだ実行されていない場合は、**[自動保護サービス（Automated protection service）]**（**[システム（System）] > [システム管理（System administration）]**）を有効化する必要があります。

HTTP プロキシに対する悪意のある試行から保護するには、VCS Expressway の自動侵入防御を設定できます（**[システム（System）] > [保護（Protection）] > [自動検出（Automated detection）] > [設定（Configuration）]**）。

VCS Expressway で、次のカテゴリを有効にすることを推奨します。

- **HTTP プロキシの認証の失敗（HTTP proxy authorization failure）** と **HTTP プロキシ プロトコル違反（HTTP proxy protocol violation）**. 注：**HTTP プロキシのリソース アクセスの失敗**カテゴリを有効にしないでください。
- **XMPP プロトコル違反**

注：**自動保護サービス**では Fail2ban ソフトウェアを使用します。また、単一の発信元 IP アドレスから発信された総当たり攻撃から保護します。

その他の情報

付録 1： トラブルシューティング

一般技術 53
アラームとステータスのチェック 53
診断ログの取得 53
DNS レコードの確認 54
VCS Expressway の到達可能性の確認 55
コール ステータスの確認 55
VCS 経由で Unified CM に登録されたデバイスのチェック 56
VCS Control が Unified CM に同期していることの確認 56
SSO のステータスとトークンの確認 57
VCS 証明書/TLS 接続の問題 57
Cisco Jabber サインイン問題 57
XMPP のバインド障害が原因で Jabber がサインインできない 57
SSH のトンネル障害が原因で Jabber がサインインできない 57
VCS Expressway クラスタ内の異なるピアに接続するときに Jabber がログインできない 58
VCS が「401 unauthorized」エラー メッセージを返す 58
「407 proxy authentication required」または「500 Internal Server Error」エラーによる通話障害 58
コールのビット レートが 384 kbps に制限される/BFCP（プレゼンテーション共有）使用時の
ビデオ問題 58
エンドポイントが Unified CM に登録できない 59
IM and Presence Service レルムの変更 59
ボイスメール サービスなし（「403 Forbidden」応答） 59
サービス要求の「403 Forbidden」応答 59
クライアント HTTPS 要求が VCS によってドロップされる 60

その他の情報

リモート アクセス用の IM&P サーバが設定できない 60

「Failed: <address> is not a IM and Presence Server」 60

無効な SAML アサーション 60

一般技術

アラームとステータスのチェック

問題のトラブルシューティングでは、まず、アラームが発生したかどうかを確認することを推奨します（[ステータス（Status）] > [アラーム（Alarms）]）。アラームが存在する場合は、**[アクション（Action）]** 列にある手順に従ってください。VCS Control と VCS Expressway の両方で、アラームを確認する必要があります。

次に、ステータスのサマリーおよび設定情報の範囲を確認するには、**[ステータス（Status）] > [ユニファイド コミュニケーション（Unified Communications）]** を選択します。VCS Control と VCS Expressway の両方で、このステータス ページを確認する必要があります。

必要な設定がない、または無効なエラー メッセージが表示された場合は、関連する設定ページへのリンクが提供されます。

VCS で次の項目を変更した場合は、無効なサービスまたはエラーが示される可能性があります。

- サーバまたは CA 証明書
- DNS の設定
- ドメインの設定

このような場合、これらの設定の変更を反映するにはシステムの再起動が必要です。

診断ログの取得

Jabber for Windows

Jabber for Windows のログ ファイルは **csf-unified.log** として **C:\Users\<UserID>\AppData\Local\Cisco\Unified Communications\Jabber\CSF\Logs** の下に保存されます。

コンフィギュレーション ファイルは **C:\Users\<UserID>\AppData\Roaming\Cisco\Unified Communications\Jabber\CSF\Config** の下にあります。

VCS の診断ログの実行

システムの問題のトラブルシューティングに VCS の診断ログ ツールを使用できます。また、長時間に渡ってシステム アクティビティの診断ログを生成し、ログをダウンロードすることができます。

その他の情報

診断ログを実行する前に、適切なロギング モジュールのログ レベルを設定する必要があります。

1. [メンテナンス（Maintenance）] > [診断（Diagnostics）] > [詳細設定（Advanced）] > [サポート ログの設定（Support Log configuration）] を選択します。
2. 次のログを選択します。
   - developer.edgeconfigprovisioning
   - developer.trafficserver
   - developer.xcp
3. [デバッグに設定（Set to debug）] をクリックします。

これで、診断ログの取得を開始できます。

1. [メンテナンス（Maintenance）] > [診断（Diagnostics）] > [診断ログ（Diagnostics logging）] に移動します。
2. オプションで、[ロギング中に tcpdump を採取（Take tcpdump while logging）] を選択します。
3. [新規ログを開始（Start new log）] をクリックします。
4. （任意）**マーカー** テキストを入力して、[マーカーを追加（Add marker）] をクリックします。
   - 特定のアクティビティが実行される前に、マーカー機能を使用して、ログ ファイルにコメント テキストを追加できます。これは、ダウンロードされた診断ログ ファイルで関連するセクションを後で識別するのに役立ちます。
   - 診断ログの進行中に、必要なだけマーカーを追加できます。
   - マーカー テキストは「`DEBUG_MARKER`」タグと一緒にログに追加されます。
5. 診断ログでトレースするシステムの問題を再現します。
6. [ログの停止（Stop Logging）] をクリックします。
7. [ログのダウンロード（Download log）] をクリックして、ローカル ファイル システムに診断ログ アーカイブを保存します。アーカイブを保存するように要求されます（実際の表現は、ブラウザによって異なります）。

診断ログを完了した後、[サポート ログの設定（Support Log configuration）] ページに戻り、*INFO*レベルに変更されたロギング モジュールをリセットします。

DNS レコードの確認

システムの問題のトラブルシューティングには VCS の DNS ルックアップ ツールを使用できます（**[メンテナンス（Maintenance）] > [ツール（Tools）] > [ネットワーク ユーティリティ（Network utilities）] > [DNS ルックアップ（DNS lookup）]**）。SRV レコードのルックアップには、H.323、SIP、ユニファイド コミュニケーション、および TURN サービスに固有のものが含まれます。

注：VCS Control から DNS ルックアップを実行すると、企業内からのビューが返され、VCS Expressway で実行すると、DMZ 内から表示できる内容が返されます。これは、必ずしもパブリック インターネットでエンドポイントに使用可能なレコードと同じセットとは限りません。

その他の情報

DNS ルックアップには、ユニファイド コミュニケーションに使用される次の SRV サービスが含まれています。

- _collab-edge._tls
- _cisco-uds._tcp

注：次の SRV レコードは、ルックアップ ツールまたはクライアントからクエリーできますが、必須ではありません。これらに関連する名前エラーは無視できます。

- _cisco-phone-tftp._tcp
- _cisco-phone-http._tcp
- _cuplogin._tcp

VCS Expressway の到達可能性の確認

VCS Expressway の FQDN がパブリック DNS で解決可能であることを確認します。

FQDN は **[システム（System）] > [DNS]** で設定され、**<System host name>.<Domain name>** として組み込まれています。

コール ステータスの確認

コール ステータス情報は現在のコールと完了したコールの両方に対して表示できます。

- **現在のコール**：**[コール ステータス（Call status）]** ページ（**[ステータス（Status）] > [コール（Calls）] > [コール（Calls）]**）は、VCS に登録されたデバイスとの送受信が現在行われているコール、または VCS を通過しているすべてのコールをリストします。
- **完了したコール**：[コール履歴（Call history）] ページ（[ステータス（Status）] > [コール（Calls）] > [履歴（History）]）はアクティブでなくなったすべてのコールをリストします。リストは、最新の 500 コールに制限され、VCS が最後に再起動してから発生したコールのみが含まれます。

コール ステータス情報の同じセットは、**[登録ごとのコール（Calls by registration）]** ページ（**[登録の詳細（Registration details）]** 経由でアクセス可能）でも表示できます。

VCS がクラスタに含まれている場合、クラスタ内のピアに適用されるすべてのコールが表示されますが、リストはピア 1 つあたりで最新の 500 コールに限定されます。

Mobile & Remote Access コールの識別

コール ステータスおよびコール履歴ページにはすべてのコール タイプが表示されます。これには、Unified CM リモート セッション（Mobile & Remote Access が有効な場合）だけでなく、VCS トラバーサル コールおよび非トラバーサル コールが含まれます。

コール タイプを区別するにはコール コンポーネントをドリルダウンする必要があります。Mobile & Remote Access コールには、コールが VCS Control で表示されるか VCS Expressway で表示されるかによって、さまざまなコンポーネントの特性があります。

その他の情報

- VCS-C では、Unified CM のリモート セッションに 3 つのコンポーネントがあります（メディア暗号化の実行に B2BUA を使用するため）。コンポーネントの 1 つが、VCS と Unified CM 間に自動的に生成されるネイバー ゾーンの 1 つを経由してコールの経路を指定します（名前の前に **CEtcp** または **CEtls** が付きます）。
- VCS-E には、**CollaborationEdgeZone** を経由してコールの経路を指定するコンポーネントが 1 つあります。

注：両方のエンドポイントが企業外（つまりオフプレミス）にある場合は、2 つの独立したコールとして扱われます。

VCS 経由で Unified CM に登録されたデバイスのチェック

Unified CM のデバイスの識別

VCS で Unified CM に登録したデバイスを識別するには、次の手順を実行します。

1. Unified CM で、[デバイス（Device）] > [電話（Phone）] を選択し、[検索（Find）] をクリックします。
2. [IP Address] 列をチェックします。VCS で登録されたデバイスが登録時に経由した VCS Control の **IP アドレス**を表示します。

VCS Control でプロビジョニングされたセッションの識別

VCS でプロビジョニングされたセッションを識別するには、次の手順を実行します。

1. VCS Control で、**[ステータス（Status）] > [ユニファイド コミュニケーション（Unified Communications）]** を選択します。
2. [詳細ステータス情報（Advanced status information）] セクションで、[プロビジョニング セッションの表示（View provisioning sessions）] をクリックします。

   これは、現在および最近の（赤色で表示）すべてのプロビジョニング セッションの一覧を表示します。

VCS Control が Unified CM に同期していることの確認

Unified CM クラスタまたはノード構成への変更は、Unified CM と VCS Control 間の通信の問題の原因になる可能性があります。これには、以下への変更が含まれます。

- Unified CM クラスタ内のノード数
- 既存のノードのホスト名または IP アドレス
- リスニング ポート番号
- セキュリティ パラメータ
- 電話セキュリティ プロファイル

そのような変更が VCS Control に反映されることを確認する必要があります。そのためには、すべての Unified CM と IM and Presence Service のノードを再検出する必要があります（VCS で **[設定（Configuration）] > [ユニファイド コミュニケーション（Unified Communications）]** を選択します）。

その他の情報

SSO のステータスとトークンの確認

ユーザの SSO トークンは、[ユーザ（Users）] > [SSOトークン所有者（SSO token holders）] で確認してクリアできます。これにより、特定のユーザの SSO アクセスの問題を特定できます。

[ステータス（Status）] > [ユニファイド コミュニケーション（Unified Communications）] > [SSO 統計情報の詳細を表示（View detailed SSO statistics）] で SSO 統計情報を確認できます。このページの予期しない要求または応答により、設定または認証の問題を識別できる可能性があります。

VCS 証明書/TLS 接続の問題

VCS サーバ証明書または信頼できる CA 証明書が変更された場合、その変更が有効になる前に VCS を再起動する必要があります。

セキュア プロファイルを使用している場合、VCS Control の証明書に署名した認証局のルート CA が *CallManager の信頼*証明書（**Cisco Unified OS Administration** アプリケーションの **[セキュリティ（Security）] > [証明書の管理（Certificate Management）]**）としてインストールされていることを確認します。

Cisco Jabber サインイン問題

XMPP のバインド障害が原因で Jabber がサインインできない

XMPP のバインド障害（「Cannot communicate with the server」エラー メッセージ）が原因で Jabber クライアントがサインインできない可能性があります。

これは、Jabber クライアント ログのリソースのバインド エラーによって示されます。次に例を示します。

```
                    XmppSDK.dll #0, 201, Recv:<iq id='uid:527a7fe7:00000cfe:00000000' type='error'><bind
xmlns='urn:ietf:params:xml:ns:xmpp-bind'/><error code='409' type='cancel'><conflict
xmlns='urn:ietf:params:xml:ns:xmpp-stanzas'/></error></iq>                XmppSDK.dll #0,
CXmppClient::onResourceBindError            XmppSDK.dll #0, 39, CTriClient::HandleDisconnect, reason:16
```

これは通常、IM and Presence Intercluster Sync Agent が正しく実行されない場合に発生します。詳細については、「IM and Presence intercluster deployment configuration」を参照してください。

SSH のトンネル障害が原因で Jabber がサインインできない

SSH トンネルが確立できないことが原因で、Jabber がサインインできない場合があります。VCS Control と VCS Expressway 間のトラバーサル ゾーンは、他のあらゆる点で正常に動作します。VCS は「アプリケーションが失敗しました - 予期せぬソフトウェア エラーが portforwarding.pyc で検出されました」と報告します。

これは、VCS Expressway DNS ホスト名にアンダースコア文字を含めると発生する可能性があります。**[システム（System）] > [DNS]** を選択し、**[システム ホスト名（System host name）]** に文字、数字、ハイフンしか含まれていないことを確認します。

その他の情報

VCS Expressway クラスタ内の異なるピアに接続するときに Jabber がログインできない

VCS Expressway ピア間の DNS ドメイン名が一致しない場合、Jabber ログイン障害が発生します。ドメイン名は、クラスタ内のすべてのピアにおいて、大文字小文字も含めて同じである必要があります。

各ピアの **[システム（System）] > [DNS]** を選択し、すべてのピアの**[ドメイン名（Domain name）]** が同じであることを確認します。

VCS が「401 unauthorized」エラー メッセージを返す

「401 unauthorized」エラー メッセージは、VCS がエンドポイント クライアントによって提示されたクレデンシャルを認証しようとした場合に発生することがあります。この原因は次のとおりです。

- クライアントが不明なユーザ名、または間違ったパスワードを提供しています。
- ILS（クラスタ間の検索サービス）が、すべての Unified CM クラスタに設定されていません。これは UDS のクエリーがクライアントのホーム クラスタを検出するために、VCS で使用する Unified CM ノードによっては、断続的な障害の原因となる可能性があります。

「407 proxy authentication required」または「500 Internal Server Error」エラーによる通話障害

通話障害は VCS のトラバーサル ゾーンが *[クレデンシャルの確認（Check credentials）]* の **[認証ポリシー（Authentication policy）]** で設定されていると発生する場合があります。Mobile & Remote Access に使用するトラバーサル ゾーンの **[認証ポリシー（Authentication policy）]** が、*[クレデンシャルを確認しない（Do not check credentials）]* に設定されていることを確認します。

コールのビット レートが 384 kbps に制限される/BFCP（プレゼンテーション共有）使用時のビデオ問題

これは、Unified CM で設定された地域内のビデオ ビット レート制限によって生じる可能性があります。

地域間と地域内（[システム（System）] > [リージョン情報（Region Information）] > [リージョン（Region）]）で、[ビデオ コールの最大セッション ビット レート（Maximum Session Bit Rate for Video Calls）] が 6000 kbps などのシステムの適切な上限に設定されていることを確認します。

その他の情報

エンドポイントが Unified CM に登録できない

エンドポイントはさまざまな理由で登録できない場合があります。

- エンドポイントは、Unified CM と VCS Control 間に設定された SIP トランクも存在する場合は、Unified CM に登録できない可能性があります。SIP トランクが設定されている場合、Unified CM への SIP 回線登録に使用されるポートとは別のリスニング ポートを Unified CM で使用する必要があります。詳細については、「Unified CM と VCS Control 間の SIP トランク」（p.46）を参照してください。
- VCS Control のサーバ証明書に、暗号化された TLS に設定され、リモート アクセスを必要とするデバイスに使用される Unified CM の電話セキュリティ プロファイルのすべての名前であるサブジェクト名の代替名リストが含まれていない場合、セキュアな登録は失敗する場合があります（「Failed to establish SSL connection」メッセージ）。注：これらの名前は、Unified CM と VCS の証明書の両方で FQDN 形式にする必要があります。

IM and Presence Service レルムの変更

プロビジョニングの障害は、IM and Presence Service レルムが変更されて、VCS Control 上のレルム データが更新されていない場合に発生する可能性があります。

たとえば、IM and Presence Service ノードのアドレスが変更された場合、または新しいピアが IM and Presence Service クラスタに追加された場合にこの障害が発生する可能性があります。

診断ログには、VCS Control でレルムが見つからないため、「`Failed to query auth component for SASL mechanisms`」のような INFO メッセージが含まれる場合があります。

[設定（Configuration）] > [ユニファイド コミュニケーション（Unified Communications）] > [IM and Presence Service ノード（IM and Presence Service nodes）] に移動し、**[サーバの更新（Refresh servers）]** をクリックして、更新した設定を保存します。プロビジョニングの障害が解決されない場合は、IM and Presence Service ノード設定を確認して、再度更新します。

ボイスメール サービスなし（「403 Forbidden」応答）

Cisco Unity Connection（CUC）のホスト名が VCS Control の HTTP サーバの許可リストに含まれていることを確認します。

サービス要求の「403 Forbidden」応答

サービスは、VCS Control、VCS Expressway が信頼できる NTP サーバに同期されていない場合、失敗する可能性があります（「403 Forbidden」応答）。すべての VCS システムが信頼できる NTP サービスに同期されていることを確認します。

その他の情報

クライアント HTTPS 要求が VCS によってドロップされる

VCS Expressway の自動侵入防御機能によって、HTTP プロキシ経由でリソースにアクセスするクライアント IP アドレスから、不正な試行（404 エラー）が繰り返し検出された場合に発生することがあります。

クライアント アドレスがブロックされないようにするには、**[HTTP プロキシのリソース アクセスの失敗（HTTP proxy resource access failure）]** カテゴリ（**[システム（System）] > [保護（Protection）] > [自動検出（Automated detection）] > [設定（Configuration）]**）が無効にされていることを確認します。

リモート アクセス用の IM&P サーバが設定できない

「Failed: <address> is not a IM and Presence Server」

このエラーは、リモート アクセスに使用する IM&P サーバを設定しようとした場合に発生する可能性があります（[設定（Configuration）] > [ユニファイド コミュニケーション（Unified Communications）] > [IM and Presence サーバ（IM and Presence servers）]）。

これは IM&P サーバの CA 証明書が欠落していることが原因で、9.1.1 を実行するシステムに適用されます。詳細情報および推奨ソリューションは「bug CSCul05131」で説明されています。

無効な SAML アサーション

クライアントが SSO 経由で認証に失敗した場合、1 つの潜在的な原因は、IDP からの無効なアサーションが VCS Control により拒否されたことです。

「無効な SAML 応答」のログを確認します。

一つの例は、ユーザ ID を VCS Control に送信する要求規則が ADFS にない場合です。この場合、ログに「No uid Attribute in Assertion from IdP」が表示されます。

VCSは、`uid` という属性のアイデンティティがある ADFS からの要求によりユーザ ID がアサートされることを想定しています。ADFS に移動し、ユーザの AD 電子メール アドレス（または展開により異なる sAMAccountName）を各 Relying Party に対する「uid」として送信するための要求規則を各 Relying Party Trust で作成する必要があります。

マニュアルの変更履歴

次の表に、このマニュアルの変更履歴の要約を示します。

日付	説明
2016 年 4 月	DNS 設定に関するアドバイスを CSCuz08798 に対応するように改訂。
2015 年 11 月	X8.7 に関する内容を更新。
2015 年 7 月	X8.6 に関する内容を更新。
2015 年 6 月	X8.5.3 に関する内容を更新、UC ノードの DNS ルックアップに関する注意事項を追加。
2015 年 4 月	X8.5.2 に関する内容を更新、認証レート制御に関する情報を追加し、マニュアルの不備を修正。
2015 年 2 月	SSO の機能変更に伴い X8.5.1 用に更新：デフォルトで SAML 要求の SHA-256 署名、IdP 前提条件の表現の変更。
2014 年 12 月	X8.5 用の新機能と X8.2 バージョンからの修正により更新。
2014 年 8 月	X8.2 バージョンによる共有回線の制限を追加してこのドキュメントの X8.1.1 バージョンを再発行。
2014 年 7 月	クライアント サポートの詳細および削除されたメディアの暗号化の制限を更新して再発行。
2014 年 7 月	ファイアウォールのアドバイス、サポートされていない展開を更新して再発行。
2014 年 7 月	ドメインのスクリーンショットを更新して再発行。
2014 年 6 月	X8.2 用に再発行。
2014 年 4 月	初版。

シスコの法的情報

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

ハード コピーおよびソフト コピーの複製は公式版とみなされません。最新版はオンライン版を参照してください。

シスコは世界各国 200 箇所にオフィスを開設しています。各オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/go/offices [英語]）をご覧ください。

シスコの商標または登録商標

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. シスコの商標の一覧は www.cisco.com/web/JP/trademark_statement.htm に掲載されています。Third-party trademarks mentioned are the property of their respective owners.The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1110R)