# Cisco TelePresence Video Communication Server リリースノート (X14.0.1)

**初版**：2021 年 6 月 2 日

## このマニュアルについて

このマニュアルの構成は、次のとおりです。



## プレビュー機能の免責事項

このリリースの一部の機能は、既知の制限や不完全なソフトウェア依存関係があるため、「プレビュー」ステータスのみで提供されます。Cisco は、通知なしでいつでもプレビュー機能を無効にする権利を有します。

実稼働環境では、プレビュー機能に依存しないでください。Cisco テクニカルサポートでは、プレビュー機能を使用するお客様に、限定的なサポート（重大度 4）を提供します。

# はじめに

## 変更履歴

表 *1:* リリースノートの変更履歴

| 日付 | 変更内容 | 理由 |
|---|---|---|
| 2021 年 6 月 | X14.0.1 初版 | X14.0.1 リリース |
| 2021 年 5 月 | MRA の制限セクションに制限を追加。 | X14.0 リリース - 再発行 |
| 2021 年 4 月 | X14.0 初版 | X14.0 リリース |
| 2020 年 12 月 | X12.7 初版 | X12.7 |
| 2020 年 8 月 | メンテナンス リリースの更新。 | X12.6.2 |
| 2020 年 7 月 | ソフトウェアのダウングレード（サポート対象外）に関する問題について誤解を招くセクションを削除しました。 | ドキュメントの訂正 |
| 2020 年 7 月 | メンテナンス リリースの更新。OAuth トークン認証のエンドポイント要件も明確化。 | X12.6.1 |
| 2020 年 6 月 | X12.6 初版 | X 12.6 |

# サポートされるプラットフォーム

表 *2:* このリリースでサポートされている ***Cisco VCS*** プラットフォーム

| プラットフォーム名 | シリアル番号 | ソフトウェア バージョンのサポート範囲 |
|---|---|---|
| 小規模 VM（OVA） | （自動生成） | X8.1 以降<br>VCS の場合、X8.11 以降のバージョンのサポートは、メンテナンスおよびバグ修正の目的のみを目的としています。新機能はサポートされていません。 |

| プラットフォーム名 | シリアル番号 | ソフトウェア バージョンのサポート範囲 |
|---|---|---|
| 中規模 VM（OVA） | （自動生成） | X8.1 以降<br>VCS の場合、X8.11 以降のバージョンのサポートは、メンテナンスおよびバグ修正の目的のみを目的としています。新機能はサポートされていません。 |
| 大規模 VM（OVA） | （自動生成） | X8.1 以降<br>VCS の場合、X8.11 以降のバージョンのサポートは、メンテナンスおよびバグ修正の目的のみを目的としています。新機能はサポートされていません。 |
| CE1100（UCS C220 M4L にプレインストールされた Cisco VCS） | 52D##### | サポートされていません（X12.5.x 以降） |
| CE1000（UCS C220 M3L にプレインストールされた VCS） | 52B##### | サポート対象外（X8.10. x 以降） |
| CE500（UCS C220 M3L にプレインストールされた Cisco VCS） | 52C##### | サポート対象外（X8.10. x 以降） |

## VCS 製品サポートに関する通知

シスコは、Cisco TelePresence Video Communication Server（VCS）**製品の販売終了日**および**サポート終了日**を発表しました。詳細については、https://www.cisco.com/c/en/us/products/collateral/unified-communications/telepresence-video-communication-server-vcs/eos-eol-notice-c51-743969.html を参照してください。

## CE1100、CE1000、および CE500 アプライアンスのハードウェア サポートに関する通知

このセクションは、**ハードウェア** サポート サービスのみに適用されます。

**CE500 および CE1000 アプライアンス - 販売終了のお知らせ**

Cisco Expressway CE500 および CE1000 アプライアンスハードウェアプラットフォームは、シスコではサポートされなくなりました。詳細については、「販売終了のお知らせ」を参照してください。

**CE1100 アプライアンス：2018 年 11 月 13 日からの販売終了および撤回するハードウェアサービスサポートの事前通知。**

2018 年 11 月 13 日以降、Cisco の CE1100 アプライアンスを注文することはできません。今後のリリースでアプライアンス用のハードウェア サポート サービスを撤回します。このプラッ

トフォームのライフサイクルにおけるその他の重要な日付については、「販売終了のお知らせ」[英語] を参照してください。

# 相互運用性および互換性

## 製品の互換性

### 詳細マトリックス

Cisco Expressway は標準規格に準拠しており、シスコとサードパーティの両方の標準規格の SIP および H.323 機器と相互運用します。特定のデバイスの相互運用性に関するご質問については、シスコの担当者にお問い合わせください。

### モバイル & リモートアクセス（MRA）

MRA と互換性のある製品についての詳細は、『Cisco Expressway 経由のモバイルおよびリモートアクセス導入ガイド』のインフラストラクチャ製品およびエンドポイントのバージョン表を参照してください。

## 並行して実行できる Cisco VCS サービスはどれか?

『Cisco Expressway 管理者ガイド』で、同じ Cisco VCS システムまたはクラスタに共存できる Cisco VCS サービスについて詳しく説明しています。「概要」セクションにある「「同時にホストできるサービス」」の表を確認してください。たとえば、MRA が CMR Cloud と共存できるかどうかを知る必要がある場合（これは可能）、表によってわかります。

# 撤回または廃止された機能とソフトウェア

Cisco VCS 製品セットは見直しが続けられており、機能が製品で取り消しまたは廃止され、機能のサポートが以降のリリースで取り消されることが示される場合があります。この表は、現在廃止済みステータスである機能または X12.5 以降で取り消された機能の一覧です。

**表 *3:* 廃止および取り消された機能**

| 機能/ソフトウェア | ステータス（Status） |
|---|---|
| VMware ESXi6.0（VM ベースの展開） | 非推奨メソッド |
| Cisco Jabber Video for TelePresence（Movi）<br>（注） Cisco Jabber Video for TelePresence（ビデオ通信に Cisco VCS と連携して動作します）に関連しており、Unified CM と連携して動作する Cisco Jabber soft クライアントではありません。 | 非推奨メソッド |

| 機能/ソフトウェア | ステータス（Status） |
|---|---|
| Findme デバイス/ロケーション プロビジョニング サービス：Cisco TelePresence FindMe/Cisco TelePresence Management Suite プロビジョニング拡張機能（Cisco TMSPE） | 非推奨メソッド |
| Cisco VCS Starter Pack Express | 非推奨メソッド |
| Smart Call Home のプレビュー機能 | X12.6.2 で取り消し済み |
| Cisco VCS 組み込み転送プロキシ | X12.6.2 で取り消し済み |
| Cisco Webex ハイブリッドサービスのコネクタとしての Cisco VCS の使用 | X12.6 で取り消し済み |
| Cisco Advanced Media Gateway | X12.6 で取り消し済み |
| VMware ESXi5.x（VM ベースの展開） | X12.5 で取り消し済み |

# レイ・バウム法に対するサポートなし

Expressway は MLTS（Multiline Telephone System）ではありません。レイ・バウム法の要件を順守する必要があるお客様は、Cisco Unified Communication Manager を Cisco Emergency Responder と共に使用する必要があります。

# 関連資料

**表 *4*：関連ドキュメントとビデオへのリンク**

| | |
|---|---|
| サポート ビデオ | Cisco TAC エンジニアから提供された一般的な Cisco VCS 設定手順に関するビデオは、Expressway/VCS スクリーンキャストビデオリスト ページで入手できます（「Expressway ビデオ」を検索）。 |
| 仮想マシンのインストール | Expressway 設置ガイドページの『*Cisco Expressway* 仮想マシン設置ガイド』 |
| 物理アプライアンスのインストール | VCS 設置ガイドページの『*Cisco Video Communication Server CE1100* アプライアンス設置ガイド』 |
| 単一システムの基本設定 | Expressway 設置ガイドページの『*Cisco Expressway* レジストラ導入ガイド』。 |
| ペアボックスシステムの基本設定（ファイアウォール トラバーサル） | Expressway 構成ガイドページの『*Cisco Expressway-E* および *Expressway-C* 基本設定導入ガイド』 |

| | |
|---|---|
| 管理およびメンテナンス | VCS メンテナンスおよび操作ガイドページの『*Cisco TelePresence VCS* 管理者ガイド』 |
| クラスタ | Expressway 構成ガイドページの『*Cisco Expressway* クラスタの作成とメンテナンス導入ガイド』 |
| 証明書 | Cisco Expressway 構成ガイドページの『*Cisco Expressway* 証明書の作成と使用に関する導入ガイド』 |
| ポート | Expressway 構成ガイドページの『*Cisco Expressway IP* ポートの使用構成ガイド』 |
| ユニファイドコミュニケーション | Expressway 構成ガイドページの『*Cisco Expressway* 経由のモバイルおよびリモートアクセス』 |
| Cisco Meeting Server | Expressway 構成ガイドページの『*Cisco Expressway* による *Cisco Meeting Server* 導入ガイド』<br>Cisco Meeting Server プログラミングガイドページの『*Cisco Meeting Server API* リファレンスガイド』<br>その他の *Cisco Meeting Server* のガイドは、Cisco Meeting Server コンフィギュレーションガイドページに用意されています。 |
| Cisco Webex ハイブリッド サービス | ハイブリッド サービス ナレッジ ベース |
| Cisco Hosted Collaboration Solution（HCS） | HCS のお客様用マニュアル |
| Microsoft インフラストラクチャ | Expressway 構成ガイドページの『*Cisco Expressway with Microsoft Infrastructure* 導入ガイド』<br>Expressway 構成ガイドページの『*Cisco Jabber and Microsoft Skype for Business Infrastructure Configuration Cheatsheet*』 |
| REST API | Expressway 構成ガイドページの『*Cisco Expressway REST API* サマリーガイド』（API が自己文書化されている高レベル情報のみ） |
| MultiWay 会議 | Expressway 構成ガイドページの『*Cisco TelePresence Multiway* 導入ガイド』 |

# Cisco VCS は新機能の適用除外

ソフトウェアバージョン X12.5 以降の新機能は、**Cisco VCS ではサポートされていません**。また、Cisco Expressway シリーズのみに適用されます。Cisco VCS システムについては、このバー

ジョンは保守およびバグ修正目的でのみ提供されます。これには、セキュリティ機能の強化、アラームベースの電子メール通知、およびオプション キーの変更のサポートが含まれます。

# X14.0.1 の機能と変更点

**重要** ソフトウェアバージョン X 12.5 以降の新機能は、Cisco VCS ではサポートされていません。また、Cisco Expressway シリーズのみに適用されます。Cisco VCS システムについては、このバージョンは保守およびバグ修正目的でのみ提供されます。これには、セキュリティ機能の強化、アラームベースの電子メール通知、およびオプション キーの変更のサポートが含まれます。

## セキュリティ機能の拡張

このリリースでは、継続的なセキュリティ機能拡張の一部として、さまざまなセキュリティ関連の機能向上が適用されています。この大部分はバックグラウンドで動作しますが、次のように、ユーザインターフェイスまたは構成に影響を与える変更もあります。

- 管理者は、CLI コマンドを使用して Expressway SSH 設定を更新することなく、Web インターフェイスから設定可能な TCP ポート 22 で SSH 暗号を設定できる柔軟性を備えています。
- シスコの製品セキュリティベースラインを満たすために、次のサービスの暗号フィルタが更新されました。
  - リバースプロキシで使用される SSL 暗号
  - Apache で使用される SSL 暗号
  - UC サービスの発見で使用される SSL 暗号
  - XMPP で使用される SSL 暗号
  - LDAP の SSL 暗号
- シスコ製品セキュリティベースラインを満たすために、SSH キー設定の暗号化アルゴリズムが更新されました。許可されていないキー交換アルゴリズムが削除されました。
  - ecdh-sha2-nistp521
  - ecdh-sha2-nistp384

  次のキー交換アルゴリズムが追加されました。
  - ecdh-sha2-nistp256
  - diffie-hellman-group14-sha256
  - diffie-hellman-group14-sh1

- Expressway-E は、サイレント SIP スキャン（SIP OPTIONS を使用）およびスパムコール（SIP INVITE を使用）にさらされます。これは、DoS 攻撃に非常によく似ています。この SIP ベースの DOS 攻撃から保護するために、Fail2Ban での SIP 認証の失敗は次の場合に有効になります。
  - X14.0 以降のバージョンの Expressway 新規インストール
  - X14.0 以降のバージョンの初期設定へのリセット
- X14.0 リリースから、SIP トランザクションのレート制限を設定できます。Web UI から、1 秒あたりの接続数とバースト制限値を有効化や無効化または変更できます。デフォルトでは、1 秒あたりの接続数の値は 100 で、バースト制限は 20 です。
- X14.0リリースから、自動保護または SIP 登録障害検出システムが拡張され、次の条件に対応できるようになりました。
  - ライセンスの制限の超過
  - メンテナンス モード
  - ポリシーで不許可
  - リソース使用不能
  - 登録の再試行が不許可
- X14.0 リリース以降、Expressway VM が低速 CPU と低メモリのサブ仕様ハードウェアで実行されている場合、サポートされていない/非準拠のハードウェア警告アラームが表示されます。
- X14.0 リリースから、MRAを介したCUCM/電話セキュリティ機能サポートの拡張の一部として、ポート 6971 が OAuth 対応 MRA クライアントの HTTPS 許可リストに追加され、設定ファイルがダウンロードされます。
- X14.0.1 以降のリリースでは、複数の管理者アカウントとグループに CLI でアクセスできます。詳細については、「管理者アカウントとフィールド参照について」を参照してください。
- X14.0.1 リリースから、信頼ストアと導入準備信頼ストアに 2 つの新しいアラームが導入され、管理者に通知されます。
  - 証明書が 21 日以内に期限切れになることを示すアラーム
  - 証明書の期限が切れたことを示すアラーム

## （プレビュー）ハードウェア セキュリティ モジュール（HSM）のサポート

X12.6 リリース以降、Expressway は、プレビュー ベースでのみ、X12.6 から HSM をサポートしています。HSMは、強力な認証のためにデジタルキーを保護および管理し、アプリケーション、ID、およびデータベースで使用する暗号化、暗号解読、および認証などの重要な機能に対して crypto プロセスを提供します。HSM デバイスは、コンピュータまたはネットワークサー

バに直接接続するプラグインカードまたは外部デバイスとして提供されます。これにより、アラームを出したりHSMを動作不能にしたりすることによって、ハードウェアおよびソフトウェアの改ざんを防ぐことができます。

新しい**[保守（Maintenance）]**>**[セキュリティ（Security）]**>**[HSM構成（HSM configuration）]**ページが、Expressway の Web ユーザインターフェイスに追加されました。

Expresswayは、現在、(プレビューベースで)、HSMプロバイダーとして、Entrust nShield Connect XC のみをサポートしています。

**重要** Gemaltoの「「SafeNet Luna」」ネットワークデバイスは、ユーザインターフェイスでも参照されていますが、**このデバイスは、現在 Expressway ではサポートされていません**。

## （プレビュー）Cisco Contact Center のヘッドセット機能 - MRA 展開

この機能は、Mobile & Remote Access を使用して Expressway を導入する場合に該当します。これは現在プレビュー ステータスで提供されています。

新しいデモンストレーション ソフトウェアにより、互換性のあるシスコ ヘッドセットに一部の Cisco Contact Center 機能が提供されるようになりました。X12.6 からは、関連するエンドポイント、ヘッドセット、または Unified CM で必要なソフトウェア バージョンが実行されている場合は、Expressway が自動でこれらのヘッドセットの新機能をサポートします。この機能はUnified CMインターフェイスから有効になっており、Expressway でのユーザによる設定は必要ありません。

詳細については、https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cucm/whitePaper/CUCM_Headsets_for_ContactCenter_WP.pdfのホワイトペーパー『*Cisco Headset and Finesse Integration for Contact Center*』を参照してください。

## （プレビュー）モバイルアプリケーション管理クライアントによるプッシュ構成 - MRA 展開

この機能は、Mobile & Remote Access を使用して Expressway を導入する場合に該当します。これは現在プレビュー ステータスで提供されています。

この機能により、 Mobile and Remote Access を介したプッシュ構成サポートには、JabberintuneやJabberblackberry のようなモバイルアプリケーション管理（MAM）クライアントのサポートが含まれるようになりました。そのため、プッシュ構成サービスは、Jabberintuneおよび Jabberblackberryクライアントを実行しているすべてのデバイスで使用できます。

## （プレビュー）Android デバイスでのプッシュ構成 - MRA 展開

この機能は、MRA を使用する Expressway を導入する場合に適用されます。X12.6 では、外部の製品バージョンの依存関係によって、プレビューステータスのみで導入されました。

X12.6.2 では、この機能は既知の問題（バグID CSCvv12541 を参照）が原因でデフォルトでオフになっています。

X12.7 で、バグ ID CSCvv12541 は修正されました。ただし、この機能はソフトウェアの依存関係が保留中のため、プレビューステータスのままです。

### Android デバイスのプッシュ構成を有効にする方法

この機能は、 Expressway コマンド ライン インターフェイスを介して有効化されます。これは、**Android ユーザにサービスを提供するすべての IM および Presence サービスノードがサポートされているリリースを実行している場合**にのみ実行します。

CLI コマンドは、*xConfiguration XCP Config FcmService: On* です。

（注） このコマンドを使用すると、現在 MRA 経由でサインインしているユーザの IM および Presence サービスが中断されます。そのため、これらのユーザは再度サインインする必要があります。

## （プレビュー）互換性のある電話機の KEM サポート - MRA 展開

Cisco IP 電話 8800 シリーズのデバイス用のキー拡張モジュール（KEM）アクセサリ向けに、MRA を正式にはテストおよび検証していません。ただし、私たちは実験条件の下で、複数の DN を持つ KEM が MRA で満足できる程度に動作していることを確認しています。これらは公式なテストでは**ありません**が、COVID-19 危機管理の観点では、この情報は、サポートされていないプレビュー機能を使用することを希望するお客様にとって有用となっています。

SIP パスヘッダーは、Expressway で有効にする必要があります。また、パスヘッダーをサポートする Unified CM ソフトウェアバージョンが必要です（リリース 11.5（1）SU4 またはそれ以降を推奨）。

## UI からのサポートされていない機能の継続的な削除

使いやすさと一貫性を向上させるために、廃止された機能をユーザインターフェイスから削除しています。リリースごとの詳細は、撤回または廃止された機能とソフトウェアを参照してください。

X14.0リリースでは、この点に関する変更はありません。

## 今回のリリースでのその他の変更点

- X14.0.1 リリースで、スプリット VPN の状況下で SSO ログインを使用する MRA が、ログインに使用される UCM ノードを追跡するように Expressway C で修正され、ログインフローのメッセージに同じ UCM ノードが使用されていることを確認します。これにより、送信元 IP が変更された場合でも、ログインを成功させるには一意の CUCM が必要になります。
- X14.0.1リリースでは、誤ったトラバーサルゾーンを使用したMRA登録に関する次の問題が修正されています。
  1. PRRH「登録」が有効な場合の適応型ルーティングのサポート。

2. PRRA「登録」が有効になっている同じ Expressway で MRA と B2B の両方に 2 つのゾーンが設定されている場合の適切なゾーンルックアップおよび選択。

## REST API への変更点

リモート設定を容易にするために、Expressway 用の REST API を利用できます。たとえば、Cisco Prime Collaboration Provisioning などのサードパーティのシステムがあります。新機能の追加にあたって、REST API から構成、コマンド、およびステータス情報にアクセスする手段を追加していますが、同時に、以前の Expressway のバージョンで導入された一部の機能に REST API を選択的に改良しています。

この API は、RAML を使用して自己記述されており、`https://<ipaddress>/api/raml` で RAML の定義にアクセスできます。

| 構成 API | API が導入されたバージョン |
|---|---|
| SNMP の設定 | X14.0.1 |
| アラーム - 表示と確認 | X14.0.1 |
| 専用管理インターフェイス（DMI） | X12.7 |
| Diagnostic Logging | X12.6.3 |
| スマートライセンシング | X 12.6 |
| クラスタ | X8.11 |
| Smart Call Home | X8.11 |
| Microsoft 製品との相互運用性 | X8.11 |
| B2BUA TURN サーバ | X8.10 |
| admin アカウント | X8.10 |
| ファイアウォールルール | X8.10 |
| SIP 設定 | X8.10 |
| サーバ名の識別用のドメイン証明書 | X8.10 |
| MRA 拡張機能 | X8.9 |
| ビジネスツービジネス コール | X8.9 |
| MRA | X8.8 |

# 未解決および解決済みの問題

## バグ検索ツール

以下のリンクに従って、このリリースで未解決および解決済みの問題に関する最新情報をお読みください。

- 変更された日付順に並べられたすべての未解決の問題（最新のものが最初）
- X14.0.1 で解決済みの問題
- X14.0 で解決済みの問題

## このバージョンで特に重要な問題

**リッチメディアセッションライセンスは、1 つの NIC Cisco VCS サーバが Jabber Guest サービスをホスティングしているため、消費されません。**

CSCva36208

X8.8 のライセンスモデルを変更すると、Cisco VCS Expressway サーバの Jabber Guest サービスのライセンスに関する問題が明らかになります。Cisco VCS ペアが「「単一の NIC」」Jabber Guest 導入の一部である場合、Cisco VCS Expressway は Jabber Guest コールごとに 1 つの RMS ライセンスをカウントする必要がありますが、そうではありません。この問題により、サーバが複数のコールを処理している場合でも使用率が低くなるため、サーバの負荷について混乱が生じる可能性があります。

（注） デュアル NIC Jabber Guest の導入を推奨します。単一の NIC 導入を使用している場合は、今後のアップグレードでサービスの継続性を確保するために、Cisco VCS のサーバが正しくライセンスされていることを確認してください。

# 制限事項

## 一部の Cisco VCS 機能はプレビューであるか、外部の依存関係がある

シスコでは、Cisco VCS の新機能をできるだけ迅速に提供することを目指しています。まだ利用できない他のシスコ製品の更新が必要な場合や、既知の問題や制限が一部の機能の展開に影響するため、新機能が公式にサポートされない場合があります。ユーザがこの機能を使用してなおメリットを享受できる場合は、リリースノートで「「プレビュー」」としてマークしています。レビュー機能は使用できますが、**実稼働環境では使用を控えることを推奨します**。場合によっては、この機能を使用しないことを推奨します。これは、それ以降の更新が、その他の

製品に対して行われるまでです。このリリースでプレビューステータスでのみ提供されるCisco VCS の機能は、このノートの「機能の履歴表」に記載されています。

## サポートされていない機能

現時点では、クラスタ展開の 1 つの Cisco VCS ノードで障害が発生した場合や、何らかの理由でネットワーク接続が失われた場合、Unified CM が再起動した場合は、影響を受けるノードを通過するすべてのアクティブなコールが失敗します。コールは別のクラスタ ピアに渡されません。これは X12.5x の新しい動作ではありませんが、見過ごされていたために、以前のリリースでは文書化されていませんでした。Bug ID CSCtr39974 を参照してください。

DTLS は Cisco VCS によって終了されません。メディアを保護するための DTLS はサポートされていません。 SRTP は、コールを保護するために使用されます。Cisco VCS を介して DTLS コールを発信しようとすると失敗します。DTLS プロトコルは SDP に挿入されますが、暗号化された iX プロトコルを通過する場合に限ります。

X12.5 から、Expresswayは、RFC 4028で指定されているように、セッションの更新のみを目的として、MRA 接続を介した SIP UPDATE のサポートを限定的に提供します。ただし、この機能を使用するための特別な要件がない場合は、この設定をオンにしないでください。SIP UPDATE のその他の使用はサポートされておらず、このメソッドに依存する機能は期待どおりに機能しません。

Cisco VCS は SIP UPDATE メソッド（RFC 3311）をサポートしていないため、このメソッドに依存する機能は期待どおりには動作しません。

音声コールは、状況によってはビデオコールとしてライセンスされる場合があります。厳密な音声のみのコールは、ビデオ通話よりも少ないライセンスを消費します。ただし、音声通話には、ActiveControl を有効にする iX チャネルなどの非オーディオチャネルが含まれている場合、ライセンスのためにビデオ通話として扱われます。

## Cisco VCS TURN は STUN サーバとして動作しない

X12.6.1 以降では、セキュリティ強化により、 Cisco VCS Expressway TURN サーバは汎用 STUN サーバとして動作しなくなり、認証されていない STUN バインディング要求を受け入れません。

その結果、以下のシナリオが考えられます。

- **シナリオ A**：（『*Cisco Expressway* および *Microsoft* インフラストラクチャ導入ガイド』*[英語]* で説明されているように）Microsoft との相互運用性の目的で TURN クライアントとして B2BUA を使用する場合、B2BUA は、サーバが動作しているかどうかを確認するために STUN バインドリクエストを TURN サーバに送信することはありません。つまり、Cisco VCS X12.6.1 以降では、到達可能でない TURN サーバの使用を B2BUA が試みた結果、**コールが失敗する可能性があります**。
- **シナリオ B**：Cisco VCS X12.6.1 以降をインストールする前に Expressway と Meeting Server WebRTC を使用する（さらに Expressway-E が TURN サーバとして構成されている）場合、最初に Meeting Server ソフトウェアをバージョン 3.0 またはバージョン 2.9.x または 2.8.x の互換性のあるメンテナンスリリースにアップグレードします。バグ ID CSCvv01243 を参

照してください。この要件は、他の Meeting Server のバージョンが Cisco VCS Expressway 上の TURN サーバに向けて STUN バインドリクエストを使用することによるものです（Cisco VCS Expressway TURN サーバの構成の詳細については、『*Cisco Meeting Server* 版 *Cisco Expressway Web* プロキシ導入ガイド』を参照してください）。

## Cisco Webex ハイブリッド コール サービス

Expressway X12.6 以降は、ハイブリッドコールサービスの導入に必要なコールコネクタソフトウェアのホストには機能しません。また、Expressway コネクタホストに以前のサポートされているバージョンを使用する必要があります。詳細については、https://help.webex.com/ でハイブリッドコールサービスの既知の問題のドキュメントをご覧ください。

## プロダクト ライセンスの登録 - スマート ライセンスへの変換に関する問題

この項目は、既存の Expressway ライセンス（RMS、デスクトップ、またはルーム）をスマート ライセンスの利用資格に変換する場合に適用されます。この場合は、Cisco Product License Registration ポータルのオプションを使用して一部のライセンスだけを部分的に変換することはしないでください。既知の問題により、一部のライセンスのみを変換する場合、システムは残りのライセンスも自動的に失効または削除します。そのため、変換されていないライセンスも削除され、それらを取得するにはライセンスケースが必要になります。

これを回避するには、**[変換数量 (Quantity to Convert)]**フィールドが **[利用可能数量 (Quantity Available)]**フィールドと同じ値であることを確認してください。これはページを開いたときのデフォルトになっています。

## クラスタ化されたシステムのスタティック NAT

X 12.5.5 から、スタティック NAT 機能のサポートはクラスタ化されたシステムに拡張されます (スタンドアロンシステムのサポートは X 12.5.3 で導入されました)。ただし、TURN サーバとして設定されているピアは、対応するパブリック インターフェイスのプライベート アドレスを使用して到達可能である必要があります。

## MRA に関する制限事項

Cisco VCS for Mobile & Remote Access（MRA）を使用する場合、現状では、サポートされない機能と制限がいくつか存在します。MRA と連動しないことがわかっている主要なサポートされていない機能のリストについては、『*Cisco Expressway* 経由の *Mobile & Remote Access*』ガイドの「Mobile & Remote Access を使用する場合にサポートされる機能とサポートされない機能」で詳しく説明されています。

7800/8800 シリーズのどの電話機とその他のエンドポイントが MRA をサポートしているかの詳細については、『*Cisco Expressway* 経由のモバイルおよびリモートアクセス』の「*MRA* 要件」のセクションを参照してください。

MRA を介したセッション更新サポートの SIP UPDATEにはいくつかの制限があります。たとえば、SIP UPDATE メソッド（RFC 3311）に依存する次の機能ではエラーが生じます。

- エンドツーエンドのセキュアコールのために、MRA エンドポイントのセキュリティアイコンを表示するように要求します。
- MRA エンドポイントの名前または番号を表示するための発信者 ID を変更するように要求します。

## MRA IM&P デュアル接続 (MRA HA) - 使用しない

Expressway X12.7 は、IM&P デュアル接続モードをサポートできます。ただし、この機能は広範囲にわたるソリューション全体にまだ実装されていないため、使用しないでください。

## エンドポイント/クライアントとの MRA OAuth トークン認証

標準の MRA モード（ICE なし）では、Unified CM で設定されている MRA アクセス ポリシー設定に関係なく、Cisco Jabber のユーザは、次の場合に、ユーザ名とパスワードを使用するか、従来のシングル サインオンを使用して認証することができます。

- Jabber ユーザが（更新トークンがサポートされない）11.9 より前のバージョンを実行しており、非トークン認証方式を許可するように Cisco VCS が設定されている場合。

ICE パススルー モードでは、ICE MRA コール パスがエンドツーエンドで暗号化されている必要があります（『Expressway MRA Deployment Guide（Expressway MRA 導入ガイド）』 https://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-installation-and-configuration-guides-list.htmlの「Expressway-C と Unified CM の間のシグナリング パスの暗号化」を参照してください）。エンドツーエンドの暗号化では通常、物理エンドポイント向けに Unified CM を混合モードにする必要があります。ただし Jabber クライアントについては、混合モードではない Unified CM クラスタで SIP OAuth を活用することによって、エンドツーエンドの暗号化の要件を満たすことができます。

（注） Unified CM が混合モードでない場合は SIP OAuth を有効にする必要がありますが、標準のセキュア プロファイルを使用して登録できる場合は、Jabber には SIP OAuth は必要ありません。

詳細については、『Expressway MRA Deployment Guide（Expressway MRA 導入ガイド）』の「MRA アクセス制御の設定」セクション、および『Deploying OAuth with Cisco Collaboration Solution（Cisco Collaboration Solution リリース 12.0 での OAuth の導入）』ホワイト ペーパー [英語] を参照してください。

## クラスタ内のピアを追加または削除するときの偽アラーム

新しいピアがクラスタに追加されたときに、クラスタが実際に正しく構成されている場合でも、複数の 20021 アラーム（「クラスタ通信の失敗：... を確立できません（Cluster communication failure: Unable to establish...）」）が発生する可能性があります。アラームは、クラスタ内の既存のピアに表示されます。通常、不要なアラームは、新しいピアが正常に追加された時点から 5 分以上経過した後に引き下げられます。

これらのアラームは、ピアがクラスタから削除された場合にも発生します。これは一般に、ピアを削除する場合に有効なアラーム動作です。ただし、ピアを追加する場合と同様に、アラームが 5 分以上低下することはありません。

## 仮想システム

- この問題は、Cisco VCSs が VMWare vCenter 7.0.x を使用して特定の ESXi バージョンを備えた仮想化システムとして実行されている場合に適用されます。これは、ESXi 6.7.0 で VMWare vCenter 7.0.1 を使用して VCS OVA を導入するテスト中に検出されました。*[OVF テンプレートの導入（Deploy OVF Template）]* ウィザードの *[準備完了（Ready to complete）]* 最終ページには、前のウィザードページで入力された実際の値ではなく、テンプレートの値が表示されます。問題は表面的であり、「[完了（FINISH）]」 をクリックすると、OVA は入力された値を使用して期待どおりに展開されます。バグ ID CSCvw64883 を参照してください。
- ESXi 側の チャンネル対応スケジューラが有効化されていて、CPU の負荷が 70% を超える場合、ビデオ コールのキャパシティが制限される場合があります。
- 物理的な Cisco VCS アプライアンスの場合、**高度なネットワーキング**機能を使用すると、設定したイーサネットポートごとに速度とデュプレックスモードを設定できます。ただし、仮想マシンベースの Cisco VCS システムに対して、イーサネットポートごとに速度を設定することはできません。

  また、仮想マシンベースのシステムでは、実際の物理的 NIC 速度に関係なく、Cisco VCS とイーサネットネットワーク間の接続速度が常に 10000 Mb/s と表示されます。これは、物理 NIC から実際の速度を取得できないという仮想マシンの制限が原因です。

## Gbps の NIC 逆多重化ポートを搭載した中規模アプライアンス

1 Gbps の NIC を使用する中規模システムを X8.10 以降にアップグレードすると、Cisco VCS は自動的にアプライアンスを大規模システムに変換します。これは、 Cisco VCS Expressway が、大規模システム（36000 ～ 36011）のデフォルトの逆多重化ポートで多重化 RTP/RTCP トラフィックをリッスンし、中規模システム用に設定された逆多重化ポートではないことを意味します。この場合、これらのポートはファイアウォールで開かれないため、Cisco VCS Expressway はコールをドロップします。

### 回避策

X8.11.4 から、**[System（システム）]**> **[Administration settings（管理設定）]**ページ（**[Deployment Configuration（展開構成）]** リストから *[Medium（中）]* を選択）を使用して、システム サイズを手動で [Medium（中）] に戻すことができます。

X8.11.4 より前の回避策は、ファイアウォール上の大規模システムのデフォルトの逆多重化ポートを開くことです。

## 言語パック

Cisco VCS Web ユーザインターフェイスを変換すると、新しい Cisco VCS 言語パックを X8.10.3 から入手できます。古い言語パックは、x8.10 では動作しません。ソフトウェア（または x8.9.）。パックをインストールまたは更新する手順については、『*Cisco VCS* 管理者ガイド』を参照してください。

## Xmpp フェデレーション - IM&P ノード障害の動作

XMPP 外部フェデレーションを使用する場合、停止後に IM および Presence サービスノードが別のノードにフェールオーバーしても、影響を受けるユーザーは他のノードに動的に移動されないことに注意してください。Cisco VCS はこの機能をサポートしておらず、テストされていません。

## Cisco Webex Calling が Dual-NIC Cisco VCS で失敗する場合

この問題は、デュアル NIC Cisco VCS Expressway を使用して Cisco VCS を展開する場合に適用されます。Cisco Webex Calling 要求が、外部インターフェイスと Cisco VCS Control を使用するインターフェイスの両方に適用される場合は、失敗する可能性があります。これは、Webex INVITE を非 NAT として扱うため、SIP Via ヘッダーから送信元アドレスを直接抽出する、現在の Cisco VCS Control のルーティング動作に起因します。

（注） ルートが重複するリスクとこの問題が発生するリスクを最小限に抑えるため、スタティックルートをできるだけ具体的にすることをお勧めします。

## デュアルホーム会議-SIP メッセージサイズ

Microsoft 側で AVMCU を起動した Cisco VCS および Meeting Server を介してデュアルホーム会議を活用する場合は、最大 SIP メッセージサイズを 32768 バイト（デフォルト）以上に設定する必要があります。大規模な会議（つまり、約 9 人以上の参加者から）に対して、より大きな値が必要になる可能性があります。**[設定（Configuration）] > [プロトコル（Protocols）] > [SIP]**で、**SIP の最大サイズ**を介して定義します。

## Expressway および Cisco Meeting Server を使用したドメイン内 Microsoft Interop

Microsoft の相互運用性のために Meeting Server を使用する場合、現時点では次のドメイン内または企業内のシナリオに制限が適用されます。

「**シングル ドメイン**」の場合、および（サブネットワーク間で内部ファイアウォールを使用するなどの理由で） *Cisco VCS Expressway* が *Microsoft* フロント エンド サーバに「**直接接続**」している構成の場合は、*Microsoft* ベースの *SIP* ネットワークと標準ベースの *SIP* ネットワークを別々に展開します。たとえば、*1* つの *(*サブ*)* ネットワーク内の *Cisco Unified Call Manager* と、同じドメイン内の *2* 番目 *(*サブ*)* ネットワーク内の *Microsoft*。

この場合、通常、2 つのネットワーク間の Microsoft の相互運用性はサポートされません。また、Meeting Server と Microsoft 間のコールは拒否されます。

### 回避策

VCS Expressway を介在させずにドメイン内ネットワークを展開できない場合（Meeting Server <> VCS Control <> Microsoft を構成することはできません）、回避策は VCS-C を各サブネットに展開し、VCS-E がそれらの間を移動することです。つまり、以下のようになります。

Meeting Server <> VCS Control <> ファイアウォール <> VCS Expressway <> ファイアウォール <> VCS Control <> Microsoft

## オプションキーは 65 キー以下のみに対して有効

65 を超えるオプションキー（ライセンス）を追加しようとすると、それらは Cisco VCS Web インターフェイスに通常どおり表示されます（**[メンテナンス（Maintenance）]** > **[オプションキー（Option keys）]**）。適用されるオプション キーは最初の 65 個のみです。66 個目以降のオプションキーは追加されているように見えても実際には Cisco VCS によって処理されません。Bug ID CSCvf78728 を参照してください。

# コラボレーション ソリューション アナライザの使用

コラボレーションソリューションアナライザは、Cisco Technical Assistance Center（TAC）が導入の検証（および Cisco VCS ログファイル解析）を支援するために作成したものです。たとえば、ビジネス ツー ビジネス コール テスターを使用して、コールの検証とテストを行うことができます。これには、Microsoft インターワーキングコールが含まれます。

コラボレーション ソリューション アナライザを使用するには、カスタマー アカウントまたはパートナー アカウントが必要です。

## はじめに

### 手順

**ステップ 1** ログ分析ツールを使用する予定であれば、まず、 Cisco VCS のログを収集します。

**ステップ 2** https://cway.cisco.com/tools/CollaborationSolutionsAnalyzer/ にサインインします。

X12.6 からは、**[診断ロギング（Diagnostic logging）]** ページの **[ログの分析（Analyze log）]** ボタン（**[メンテナンス（Maintenance）]**> **[診断（Diagnostics）]**）を使用し、コラボレーション ソリューションアナライザのトラブルシューティングツールへのリンクを開けます。

**ステップ 3** 使用するツールをクリックします。たとえば、ログを使用するには、次のようにします。

1. [ログ分析（Log analysis）] をクリックします。
2. ログファイルをアップロードします。

3. 分析するファイルを選択します。
4. [分析の実行（Run Analysis）] をクリックします。

   ツールはログファイルを分析し、生のログよりも理解しやすい形式で情報を表示します。たとえば、ラダー図を生成して SIP コールを表示することができます。

# バグ検索ツールの使用

バグ検索ツールには、問題の説明と利用可能な解決策など、このリリースおよび以前のリリースの未解決の問題と解決済みの問題に関する情報があります。これらのリリース ノートに示されている ID によって、それぞれの問題の説明に直接移動できます。

**このマニュアルに記載された問題に関する情報を検索するには、次の手順を実行します。**

1. Web ブラウザを使用して、バグ検索ツールに移動します。https://tools.cisco.com/bugsearch/
2. cisco.com のユーザ名とパスワードでログインします。
3. **検索**フィールドにバグ ID を入力して、**検索**をクリックします。

**ID がわからない場合に情報を検索するには、次の手順を実行します。**

1. [検索（Search）] フィールドに製品名を入力し、[検索（Search）] をクリックします。
2. 表示されるバグのリストで[フィルタ（Filter）] ドロップダウン リストを使用し、[キーワード（Keyword）]、[変更日（Modified Date）]、[重大度（Severity）]、[ステータス（Status）]、[テクノロジー（Technology）] のいずれかでフィルタリングを行います。

バグ検索ツールのホーム ページの [詳細検索（Advanced Search）] を使用して、特定のソフトウェア バージョンで検索します。

Bug Search Tool のヘルプ ページには、Bug Search Tool の使用に関する詳細情報があります。

# マニュアルの入手方法およびテクニカル サポート

電子メールまたは RSS フィードで送信される柔軟な通知アラートをカスタマイズするには、シスコ通知サービスをご利用ください。

マニュアルの入手、Cisco バグ検索ツール（BST）の使用、サービス リクエストの送信、追加情報の収集の詳細については、更新情報を参照してください。

新しく作成された、または改訂されたシスコのテクニカル コンテンツをお手元で直接受信するには、更新情報の RSS フィード [英語] をご購読ください。RSS フィードは無料のサービスです。

# 付録 ：MRA 展開のアップグレード後のタスク

このセクションは、Cisco VCS for Mobile and Remote Access を使用していて、X8.9.x またはそれ以前から X8.10 以降にアップグレードする場合にのみ適用されます。

## MRA アクセス制御設定を再構成するには

重要

- アップグレード後は、[内部認証の可用性の確認（Check for internal authentication availability）] 設定がオフになります。Unified CM の認証設定によっては、一部の Cisco Jabber ユーザによるリモートログインが妨げられる場合があります。
- X8.9 の [排他（Exclusive）] オプションの設定は、[認証パス（Authentication path）] で [SAML SSO 認証（SAML SSO authentication）] を指定することで設定します。これには、ユーザ名とパスワードによる認証禁止が適用されます。

### 始める前に

システムを再起動した後、MRA アクセス制御の設定を再設定する必要があります。

### 手順

**ステップ 1** Cisco VCS Control で、**[設定（Configuration）]** > **[Unified Communications]** > **[設定（Configuration）]** > **[MRAアクセス制御（MRA Access Control）]**を選択します。

**ステップ 2** 次のいずれかを実行します。

- 新しい MRA アクセス制御方式を X8.10 から利用するには、このページで選択した方法で適切な値を設定します。どの値を適用するかについては、次の最初の表を参照してください。
- または、アップグレード前の認証アプローチを保持するには、このページの適切な値を Cisco VCS Expressway の設定に合わせて設定します。古い Cisco VCS Expressway の設定を Cisco VCS Control の新しい同等物にマッピングする方法については、次の 2 番目の表を参照してください。

**ステップ 3** 自己記述トークン（**更新を伴う OAuth トークンによる承認**）を設定する場合は、Unified CM ノードを更新します。**[設定（Configuration）]** > **[Unified Communications]** > ***[<UCサーバタイプ>]*** に移動し、**[サーバの更新（Refresh servers）]** をクリックします。

# MRA アクセス制御の設定

Web UI で実際に表示されるフィールドは、MRA が有効かどうか（[Unified Communications モード（Unified Communications mode）] が [モバイルおよびリモート アクセス（Mobile and remote access）] に設定されているかどうか）、および選択された認証パスによって異なります。テーブル内のすべてのフィールドが必ずしも表示されるわけではありません。

**表 *5 : MRA* アクセス制御の設定**

| フィールド | 説明 | デフォルト |
|---|---|---|
| **認証パス（Authentication path）** | MRA が有効になるまで非表示のフィールド。MRA 認証の制御方法を定義します。<br>*[SAML SSO* 認証（*SAML SSO authentication*）*]*：クライアントは外部 IdP によって認証されます。<br>*[UCM/LDAP* 基本認証（*UCM/LDAP basic authentication*）*]*：クライアントは、LDAP クレデンシャルに対して Unified CM によってローカルに認証されます。<br>*[SAML SSO* および *UCM/LDAP*（*SAML SSO and UCM/LDAP*）*]*：どちらの方法も許可します。<br>*[*なし（*None*）*]*：認証は適用されません。これは、MRA が最初に有効になるまでのデフォルトです。一部の展開では実際には MRA ではない機能を許可するために MRA をオンにする必要があるため、（MRA をただオフにするのではなく）「[なし（None）]」 オプションが必要です。（Meeting Server の Web プロキシ、XMPP フェデレーションなど）。これらの顧客のみが 「[なし（None）]」 を使用する必要があります。<br>（注） 他のケースでは使用しないでください。 | MRA をオンにするまでは [なし（None）]<br>MRA をオンにした後は [UCM/LDAP] |

| フィールド | 説明 | デフォルト |
| --- | --- | --- |
| **OAuth トークンによる承認（更新あり）（Authorize by OAuth token with refresh）** | このオプションでは、承認のための自己記述トークンが必要です。サポート用のインフラストラクチャを持つすべての展開で推奨される承認オプションです。<br>現在、この承認方法を使用できるのは Jabber クライアントだけです。他の MRA エンドポイントは現在サポートしていません。また、クライアントは、更新を伴う OAuth トークン承認モードにある必要があります。 | [オン（On）] |
| **OAuth トークンによる承認（Authorize by OAuth token）（以前は SSO モード）** | [認証パス（Authentication path）] が [SAML SSO] または [SAML SSO および UCM/LDAP（SAML SSO and UCM/LDAP）] の場合に利用可能。<br>このオプションには、IdP を使用した認証が必要です。現在、Jabber クライアントのみがこの承認方法を使用できますが、他の MRA エンドポイントではサポートされていません。 | [オフ（Off）] |
| **ユーザ クレデンシャルによる承認（Authorize by user credentials）** | [認証パス（Authentication path）] が [UCM/LDAP] または [SAML SSO および UCM/LDAP（SAML SSO and UCM/LDAP）] の場合に利用可能。<br>ユーザクレデンシャルによる認証を実行しようとするクライアントは、MRA によって許可されます。これには、Jabber、およびサポートされている IP フォンと TelePresence デバイスが含まれます。 | オフ（Off） |

| フィールド | 説明 | デフォルト |
| --- | --- | --- |
| 内部認証の可用性の確認（**Check for internal authentication availability**） | | [いいえ（No）] |

| フィールド | 説明 | デフォルト |
| --- | --- | --- |
| | [OAuth トークンによる承認（更新あり）（Authorize by OAuth token with refresh）] または [OAuth トークンによる承認（Authorize by OAuth token）] が有効になっている場合に利用可能。<br><br>最適なセキュリティとネットワーク トラフィックの削減のため、デフォルトは[いいえ（No）]です。<br><br>Cisco VCS Control がホーム ノードをチェックするかどうかを選択することにより、Cisco VCS Expressway がリモート クライアント認証要求にどのように反応するかを制御します。<br><br>要求は、クライアントがOAuth トークンによってユーザを認証しようとする可能性があるかどうかを尋ね、その要求にはCisco VCS Control がユーザのホーム クラスタを見つけるためのユーザ ID が含まれています。<br><br>*[*はい（*Yes*）*]*：*get_ Edge _sso* 要求は、OAuth トークンがサポートされているかどうかをユーザのホーム Unified CM に尋ねます。ホーム Unified CM は、Jabber クライアントの *get_edge_sso* 要求によって送信された ID から決定されます。<br><br>*[*いいえ（*No*）*]*：VCS が内部的に見えないように設定されている場合、 Edge の認証設定に応じて、すべてのクライアントに同じ応答が送信されます。<br><br>選択するオプションは、実装およびセキュリティ ポリシーによって異なります。すべての Unified CM ノードで OAuth トークンがサポートされている場合は、[いいえ（No）] を選択して応答時間とネットワーク全体のトラフィックを減らすことができます。または、ロールアウト中にクライアントがエッジ構成を取得するモードを使用するようにする場合や、すべてのノードでOAuth を保証できない場合は、[はい（Yes）] を選択します。<br><br>**注意**　注意：これを *[*はい（*Yes*）*]* に設定すると、認証されていないリモート クライアントからの不正な着信要求 | |

| フィールド | 説明 | デフォルト |
| --- | --- | --- |
| | が許可される可能性があります。この設定に *[*いいえ（*No*）*]* を指定すると、Cisco VCS は不正な要求を回避します。 | |

| フィールド | 説明 | デフォルト |
| --- | --- | --- |
| **ID プロバイダー：IdP の作成または変更（Identity providers: Create or modify IdPs）** | | - |

| フィールド | 説明 | デフォルト |
| --- | --- | --- |
| | [認証パス（Authentication path）] が [SAML SSO] または [SAML SSO および UCM/LDAP（SAML SSO and UCM/LDAP）] の場合に利用可能。<br>**ID プロバイダーの選択**<br>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。<br>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。<br>• 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。<br>• 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。<br>• 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。Cisco 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。<br>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。<br>• OpenAM 10.0.1<br>• Active Directory Federation Services 2.0（AD FS 2.0） | |

| フィールド | 説明 | デフォルト |
|---|---|---|
| | • PingFederate®6.10.0.4 | |
| **ID プロバイダー：SAML データのエクスポート（Identity providers: Export SAML data）** | **[認証パス（Authentication path）]** が *[SAML SSO]* または *[SAML SSO* および *UCM/LDAP*（*SAML SSO and UCM/LDAP*）*]* の場合に利用可能。<br>SAML データの操作の詳細については、「*Edge* 経由の *SAML SSO* 認証」を参照してください。 | - |
| **Jabber iOS クライアントによる組み込みの Safari の使用の許可（Allow Jabber iOS clients to use embedded Safari）** | デフォルトでは、IdP または Unified CM の認証ページは、iOS デバイスの組み込み Web ブラウザ（Safari ブラウザではない）に表示されます。このデフォルトのブラウザは iOS の信頼ストアにアクセスできないので、デバイスに導入された証明書を使用することはできません。<br>この設定では、オプションで、iOS デバイス上の Jabber がネイティブの Safari ブラウザを使用することができます。Safari ブラウザでは、デバイスの信頼ストアにアクセスできるため、OAuth 導入時にパスワードレス認証または二要素認証を有効化できるようになりました。<br>このオプションには潜在的なセキュリティの問題が存在します。認証が完了した後で、Safari から Jabber にブラウザ制御を返す機能は、カスタムプロトコルハンドラを呼び出すカスタム URL 方式を使用します。Jabber 以外の別のアプリケーションがこの方式を妨害し、iOS から制御を取得できます。この場合、アプリケーションは URL の OAuth トークンへアクセスできます。<br>すべてのモバイル デバイスが管理されているなどの理由で、iOS デバイスに Jabber のカスタム URL 形式を登録する他のアプリケーションがないと確信する場合、オプションを有効にしても安全です。別のアプリケーションがカスタム Jabber URL を妨害する可能性が心配な場合、組み込み Safari ブラウザを有効にしないでください。 | [いいえ（No）] |

| フィールド | 説明 | デフォルト |
|---|---|---|
| **SIP トークンの余分なパケット存続時間（SIP token extra time to live）** | [OAuth トークンによる承認（Authorize by OAuth token）] が [オン（On）] の場合に利用可能。<br>必要に応じて、簡単な OAuth トークンの存続可能時間（秒）を延長します。クレデンシャルの有効期限が切れた後、コールを受け入れるための短い時間枠をユーザに提供します。ただし、潜在的なセキュリティ リスクが増加します。 | 0 秒 |

# アップグレードによって適用される MRA アクセス制御値

表 *6 :* アップグレードによって適用される *MRA* アクセス制御値

| オプション | アップグレード後の値 | 従来 | 現在 |
|---|---|---|---|
| 認証パス（Authentication path） | アップグレード前の設定が適用されます<br>（注） [SSOモード（SSO mode）] : X8.9 の [オフ（Off）] は、X8.10 の 2 つの設定になります。<br>• **認証パス**=*UCM/LDAP*<br>• **ユーザ ログイン情報による承認（Authorize by user credentials）**=オン<br>[SSOモード（SSO mode）] : X8.9 の [排他（Exclusive）] は、X8.10 では 2 つの設定になっています。<br>• **認証パス**=*SAML SSO*<br>• **OAuth トークンによる承認**=オン<br>[SSOモード（SSO mode）] : X8.9 の [オン（On）] は、X8.10 では 2 つの設定になっています。<br>• **認証パス**=*SAML SSO/and UCM/LDAP*<br>• **OAuth トークンによる承認**=オン<br>• **ユーザ ログイン情報による承認（Authorize by user credentials）**=オン | 両方 | Cisco VCS Control |

| オプション | アップグレード後の値 | 従来 | 現在 |
|---|---|---|---|
| OAuth トークンによる承認（更新あり）（Authorize by OAuth token with refresh） | [オン（On）] | - | Cisco VCS Control |
| OAuth トークンによる承認（Authorize by OAuth token）（以前は SSO モード） | アップグレード前の設定が適用されます | 両方 | Cisco VCS Control |
| ユーザ クレデンシャルによる承認（Authorize by user credentials） | アップグレード前の設定が適用されます | 両方 | Cisco VCS Control |
| 内部認証の可用性の確認（Check for internal authentication availability） | [いいえ（No）] | Cisco VCS Expressway | Cisco VCS Control |
| ID プロバイダー：IdP の作成または変更（Identity providers: Create or modify IdPs） | アップグレード前の設定が適用されます | Cisco VCS Control | Cisco VCS Control（変更できません） |
| ID プロバイダー：SAML データのエクスポート（Identity providers: Export SAML data） | アップグレード前の設定が適用されます | Cisco VCS Control | Cisco VCS Control（変更できません） |

| オプション | アップグレード後の値 | 従来 | 現在 |
|---|---|---|---|
| Jabber iOS クライアントによる組み込みの Safari の使用の許可（Allow Jabber iOS clients to use embedded Safari） | [いいえ（No）] | Cisco VCS Expressway | Cisco VCS Control |
| SIP トークンの余分なパケット存続時間（SIP token extra time to live） | アップグレード前の設定が適用されます | Cisco VCS Control | Cisco VCS Control（変更できません） |