Cisco TelePresence Video Communication Server リリース ノート（X14.0）

初版：2021 年 4 月 12 日

このマニュアルについて

このドキュメントでは、以下のトピックを扱います。

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 用の初版	X14.0.1 リリース
2021 年 5 月	「MRA に関する制限事項」セクションに制限事項を追加。	X14.0 リリース：再発行
2021 年 4 月	X14.0 用の初版	X14.0 リリース
2020 年 12 月	X12.7 用の初版	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 用の初版	X 12.6

サポートされるプラットフォーム

Table 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 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 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 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#####	サポート対象外（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。詳細は https://www.cisco.com/c/en/us/products/collateral/unified-communications/telepresence-video-communication-server-vcs/eos-eol-notice-c51-743969.html で確認できます。

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 アプライアンスのハードウェア プラットフォームは、シスコによるサポートが終了しています。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：販売終了およびハードウェア サービス サポート終了の事前通知。

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、アプライアンスのハードウェア サポート サービスを終了します。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、「販売終了の通知」[英語] を参照してください。

相互運用性および互換性

製品の互換性情報

詳細マトリックス

Cisco Expressway は標準ベースであり、シスコ製とサードパーティ製の両方の標準ベース SIP 機器およびH.323機器と相互運用できます。特定のデバイスとの相互運用性については、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）

特に MRA に関して互換性のある製品については、『Cisco Expressway 経由での Mobile and Remote Access 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に記載しています。

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、どの Cisco VCS サービスが同じ Cisco VCS システムまたはクラスタで共存できるかについて詳細に説明しています。「概要」セクションにある「同時にホストできるサービス」“”の表を参照してください。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。

削除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、機能が製品から削除されることや、以降のリリースで機能のサポートが終了することを意味する廃止となることがあります。この表は、現在廃止ステータスである機能、または X12.5 以降で削除された機能の一覧です。

Table 3: 廃止および削除された機能

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） **Note** TelePresence 版 Cisco Jabber Video（ビデオ コミュニケーションで Cisco VCS と連携して動作）に関連するものであり、Unified CM と連携して動作する Cisco Jabber ソフトウェア クライアントには該当しません。	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 で削除
Cisco VCS 組み込み転送プロキシ	X12.6.2 で削除
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 で削除
Cisco Advanced Media Gateway	X12.6 で削除
VMware ESXi 5.x（VM ベースの展開）	X12.5 で削除

レイ・バウム法に対するサポートなし

Expressway は MLTS（マルチライン電話システム）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 Communications Manager を Cisco Emergency Responder と共に使用する必要があります。

関連資料

Table 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 エンジニアが提供する、Cisco VCS の一般的な構成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 ページで利用できます（“Expressway videos” で検索）。
仮想マシンのインストール	Expressway インストール ガイド ページの『仮想マシンでの Cisco Expressway インストレーション ガイド』
物理アプライアンスのインストール	VCS インストール ガイド ページの『Cisco Video Communication Server CE1100 アプライアンス インストレーション ガイド』
シングルボックス システムの基本設定	Expressway コンフィギュレーション ガイド ページの『Cisco Expressway Registrar Deployment Guide（Cisco Expressway レジストラ導入ガイド）』
ペアリングされたボックス システムの基本設定（ファイアウォール トラバーサル）	Expressway コンフィギュレーション ガイド ページの Cisco Expressway-E および Expressway-C の『基本設定導入ガイド』

管理およびメンテナンス	VCS メンテナンスとオペレーション ガイド ページの『Cisco TelePresence VCS Administrator Guide（Cisco TelePresence VCS アドミニストレータ ガイド）』
クラスタ	Expressway コンフィギュレーション 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	Expressway コンフィギュレーション 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 コンフィギュレーション ガイド ページの『Cisco Expressway IP Port Usage Configuration Guide（Cisco Expressway IP ポートの使用コンフィギュレーション ガイド）』
ユニファイドコミュニケーション	Expressway コンフィギュレーション ガイド ページの『Cisco Expressway 経由の Mobile and Remote Access』
Cisco Meeting Server	Expressway コンフィギュレーション ガイド ページの『Cisco Meeting Server with Cisco Expressway Deployment Guide（Cisco Expressway による Cisco Meeting Server 導入ガイド）』 Cisco Meeting Server プログラミング ガイド ページの『Cisco Meeting Server API Reference Guide（Cisco Meeting Server API リファレンス ガイド）』 Cisco Meeting Server のその他のガイドは、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 コンフィギュレーション ガイド ページの『Cisco Expressway with Microsoft Infrastructure Deployment Guide（Microsoft インフラストラクチャを使用した Cisco Expressway 導入ガイド）』 Expressway コンフィギュレーション ガイド ページの Cisco Jabber およびビジネス版 Microsoft Skype のインフラストラクチャ構成チートシート
REST API	Expressway コンフィギュレーション ガイド ページの『Cisco Expressway REST API Summary Guide（Cisco Expressway REST API サマリー ガイド）』（API は自己記述されているため概要レベルの情報のみ）
MultiWay 会議	Expressway コンフィギュレーション ガイド ページの『Cisco TelePresence Multiway Deployment Guide（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 X 12.5 以降の新機能は、**Cisco VCS ではサポートされておらず**、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の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、オプション キーの変更のサポートが含まれます。

X14.0 の機能と変更点

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。その大半については目に見える変化はありませんが、ユーザ インターフェイスや構成に影響を与える変更もあります。

- 管理者は、TCP ポート 22 で SSH 暗号を構成できるようになりました。これは、Web インターフェイスから構成可能であり、Expressway SSH 構成を更新するのに CLI コマンドを使用する必要はありません。
- シスコ製品セキュリティ ベースラインを満たすために、以下のサービスの暗号フィルタが更新されています。
  - 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 サービス検出で使用される SSL 暗号
  - XMPP で使用される SSL 暗号
  - LDAP 用の 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 キー構成の暗号アルゴリズムが更新されています。許可されない一部のキー交換アルゴリズムは削除されています。
  - ecdh-sha2-nistp521
  - ecdh-sha2-nistp384

  以下のキー交換アルゴリズムが追加されています。
  - 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）の対象になります。これは DoS 攻撃と似ています。この SIP ベー

スの DOS 攻撃から保護するために、次の条件で Fail2Ban での SIP 認証の失敗が有効になります。

- X14.0 以降のバージョンからの Expressway の新規インストール
- X14.0 以降のバージョンで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構成できます。Web UI から、1 秒あたりの接続数および限界値を、有効化/無効化するか、変更することができます。デフォルトでは、1 秒あたりの接続数は 100 で、限界値は 20 です。
- X14.0 リリースから、自動保護、または SIP 登録の失敗の検出システムが拡張され、以下の状況に対応しました。
  - ライセンス制限の超過
  - メンテナンス モード
  - ポリシーによる禁止
  - リソース不足
  - 登録の禁止
- X14.0 リリースから、CPU が低速でメモリ容量も少ないサブスペックのハードウェアで Expressway VM が実行されている場合、サポートされていないか非準拠のハードウェアに関する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/電話機のセキュリティ機能のサポートの一部として、OAuth 対応の MRA クライアントが構成ファイルをダウンロードするための HTTPS 許可リストにポート 6971 が追加されています。
- 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 アクセス権を設定できます。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、信頼ストアとオンボーディング信頼ストアに、管理者に通知するための 2 つの新しいアラームが導入されます。
  - 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
  - 証明書の有効期限が切れたことを示すアラーム

リダイレクト URI のサポート

Webex クライアントの埋め込みブラウザのサポート

Expressway X14.0 リリースから、Webex 機能の SSO リダイレクト URI を有効化または無効化する切り替えが提供されます。この機能により、Cisco Jabber/Webex クライアントの埋め込みブラウザのサポートにおけるセキュリティが向上し、次のような利点が得られます。

- RFC7636 を使用して「認可コードの横取り攻撃」から保護します。
- iOS 以外のオペレーティング システムで実行されているクライアントで Android などの埋め込みブラウザを使用できます。
- Jabber クライアントと Webex クライアントで、Unified Communications Manager（および MRA）の OAuth フローに埋め込みブラウザを使用できます。
- Webex クライアントおよび Unified Communications Manager Calling を使用する際のユーザ エクスペリエンスが向上します。

詳細については、『Cisco Expressway 経由での Mobile and Remote Access 導入ガイド』を参照してください。

AV1 のサポート

Expressway X14.0 リリースから、メディアを確立するための AV1 コーデックのネゴシエーションとパススルーがサポートされます。コーデックは、SIP トラバーサル コール（Expressway がメディア ストリームを処理しているコール）でサポートされます。

P2P からミーティングへのエスカレーション

Webex ユーザは、1:1 の SIP コール中に Webex ミーティングをコールし、次のようなミーティング機能を呼び出すことができるようになりました。

- ビデオ参加者の追加
- Webex Assistant の使用
- ホワイトボードの使用

エスカレーション プロセス中に、追加の参加者を招待するのか、単に 1:1 のコールを 1:1 のミーティングに移行するのかオプションを選択できます。既存のオーディオチャンネル（モバイルまたはデスクフォン）を維持しながら、別のデータ チャンネルを介してビデオを強化したり共有したりするオプションも選択できます。

Expressway クラスタのロード バランシングは SIP フェデレーションには適用されない

SIP フェデレーションに使用される Expressway 展開では、Expressway に対する SIP ボリュームの負荷が常に高くなり、SIP ボリュームを処理するために複数のピアが必要になります。Expressway では、このトラフィックを Expressway Edge トラバーサル サーバに均等に分散することができませんでした。

Expressway X14.0 リリースから、トラバーサル ゾーン接続全体でトラフィックを適切に負荷分散できます。

Jabber のゼロ ダウンタイムでの XCP サポート

Expressway X14.0 リリースから、Jabber クライアントとのデュアル接続がサポートされます。このタイプの接続をクライアント側で有効にすると、高可用性フェールオーバーイベント中のサービス ダウンタイムがゼロになります。

これは、次の場合に役立ちます。

- アップグレード中に Jabber クライアントのサービスの中断を最小限に抑えます。
- プライマリ ノードとセカンダリ ノードの間でユーザ セッションのシームレスな移行を実現します。

Cisco Jabber の SIP 登録フェールオーバー：MRA 展開

この機能は、Mobile & Remote Access（MRA）を使用して Expressway を導入する場合に該当します。

Expressway X14.0 は、クラスタ構成の Expressway 向けの既存のフェールオーバー機能を基に構築されており、MRA を介して接続する Cisco Jabber クライアントのフェールオーバー時間を大幅に改善する MRA フェールオーバーの更新が多数適用されています。更新には、適応型ルーティング、STUN キープアライブのサポート、改善されたエラー レポートが含まれます。

これらの新しい機能により、Jabber クライアントで音声とビデオの MRA 高可用性（フェールオーバー）をサポートできます。

詳細については、『Cisco Expressway 経由での Mobile and Remote Access 導入ガイド』を参照してください。

（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

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、アイデンティティ、データベースで使用する暗号化、復号化、認証などの重要な機能向けに暗号処理を提供します。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、ハードウェアとソフトウェアの改ざんを防ぎます。

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

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 をサポートします。

Important

Gemalto の “SafeNet Luna” ネットワーク デバイスは、Expressway のユーザ インターフェイスでも参照されますが、**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、MRA を使用して Expressway を展開する場合に適用されます。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。

詳細は、次の場所にあるホワイト ペーパー『Cisco Headset and Finesse Integration for Contact Center（Contact Center 向けの Cisco ヘッドセットと Finesse の統合）』に記載されています。https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cucm/whitePaper/CUCM_Headsets_for_ContactCenter_WP.pdf

（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を使用したプッシュ通知：MRA 展開

この機能は、MRA を使用して Expressway を展開する場合に適用されます。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、MRA を介したプッシュ通知サポートで、Jabberintune や Jabberblackberry などのモバイル アプリケーション管理（MAM）クライアントがサポート対象になります。その結果、Jabberintune クライアントや Jabberblackberry クライアントを実行しているすべてのデバイスでプッシュ通知サービスを利用できます。

（プレビュー）Android デバイスでのプッシュ通知：MRA 展開

この機能は、MRA を使用して Expressway を展開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り、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、既知の問題（バグ ID CSCvv12541 参照）により、この機能はデフォルトでオフに切り替えられました。

X12.7 では、バグ ID CSCvv12541 は修正済みです。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通知を有効にする方法

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。この操作は、**Android ユーザにサービスを提供する IM and Presence Service のすべてのノードでサポート対象の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：***xConfiguration XCP Config FcmService: On***

（注） このコマンドを使用すると、MRA を介して現在サインインしているユーザの IM and Presence サービスが中断されます。このため、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）。

サポートされていない機能の UI からの削除（継続中）

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、「削除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変更はありません。

今回のリリースでのその他の変更点

接続マネージャーのログが改善されました。

REST API への変更点

リモート構成を効率化するために、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などがあります。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://<ip address>/api/raml` で RAML の定義にアクセスできます。API へのアクセス方法と使用方法の概要については、Expressway インストール ガイド ページの『Cisco Expressway REST API Summary Guide（Cisco Expressway REST API サマリー ガイド）』を参照してください。

構成 API	API が導入されたバージョン
専用管理インターフェイス（DMI）	X12.7
Diagnostic Logging	X12.6.3

構成 API	API が導入されたバージョン
スマート ライセンス	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 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 NIC” Jabber Guest 展開の一部である場合、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はずですが、そうなっていません。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。

Note デュアル NIC Jabber Guest 展開を推奨します。単一 NIC 展開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 のサーバにライセンスが適切に適用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。それでもこの機能を使用することでユーザがメリットが得られる場合は、リリースノートで“プレビュー”としてマークしています。プレビュー機能は使用できますが、**実稼働環境で業務に使用するのは推奨しません。**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、ノートの“機能履歴”の表に記載されています。

サポートされていない機能

現在、クラスタ展開内の Cisco VCS のノードの 1 つ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、以前のリリースでは見落としによりドキュメント化されていませんでした。バグ ID CSCtr39974 を参照してください。

Cisco VCS が DTLS を終了することはありません。メディアを保護する目的では DTLS はサポートされておらず、コールを保護するのには SRTP が使用されます。Cisco VCS を介した DTLS コールの試行は失敗します。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 から、セキュリティ強化により、Cisco VCS Expressway の 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 バインド リクエストを受け付けません。

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 with Microsoft Infrastructure Deployment Guide（Microsoft インフラストラクチャによる Cisco Expressway 導入ガイド）』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、到達不能な 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 を使用している（かつ Expressway-E が TURN サーバとして構成されている）場合は、先に Meeting Server ソフトウェアをバージョン 3.0 にアップグレードするか、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。これは、他の Meeting Server バージョンでは、Cisco VCS Expressway の TURN サーバに対して STUN バインド リクエストを使用することが理由です（Cisco VCS Expressway の TURN サーバ構成の詳細については、『*Cisco Expressway Web Proxy for Cisco Meeting Server Deployment Guide*（*Cisco Meeting Server* 用 *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 サービスの展開で必要となるコール コネクタ ソフトウェアをホスティングする目的では機能せず、Expressway コネクタ ホスト用にサポートされている旧バージョンを使用する必要があります。詳細については、ハイブリッド コール サービスの既知の問題と Expressway バージョンのサポートに関するドキュメント（https://help.webex.com/）を参照してください。

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しないでください。既知の問題により、一部のライセンスだけ変換することを選択すると、残りのライセンスも自動的に無効になるか削除されます。そのため、変換しないライセンスも削除され、回復するためにはライセンス 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）] フィールドと [利用可能数量（Quantity Available）] フィールドの値が同じ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の状態です。

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

Mobile & Remote Access（MRA）用に Cisco VCS 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、サポートされない主な機能のリストについては、『Cisco Expressway 経由の Mobile and Remote Access』ガイドで、Mobile and 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が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 Mobile and Remote Access』ガイドの MRA 要件に関するセクションを参照してください 。

1. 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リクエストします。
- 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 を変更するようにリクエストします。

2. Mobile and Remote Access（MRA）を介した Unity ボイスメールは、X14.0 リリースでは機能しません。この問題は今後のリリースで修正される予定です（バグ ID CSCvy29217 を参照）。

（注） Unity ボイスメール機能が重要である場合は、アップグレードしないでください。

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、この機能はより広範なソリューション全体には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 VCS が、VMware vCenter 7.0.x を使用して特定の ESXi バージョンを導入し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、VMware vCenter 7.0.1 と ESXi 6.7.0 を使用して VCS OVA を展開するテスト中に特定されました。[OVFテンプレートの展開（Deploy OVF Template）] ウィザードの最終ページである [準備完了（Ready to complete）] に、その前のウィザード 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。この問題は表面的なものであり、[完了（FINISH）]「

」をクリックすると、入力された値を使用して想定どおりに OVA が展開されます。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 アプライアンスでは、[高度なネットワーク（Advanced Networking）] 機能を使用することで、構成したイーサネット 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。仮想マシンベースの Cisco VCS システムでは、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 ネットワークの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 を使用する中規模アプライアンスを X8.10 以降にアップグレードする場合、Cisco VCS が、システムを自動的に大規模システムに変換します。これは、Cisco VCS Expressway は、中規模システム用に構成された逆多重化ポートではなく、大規模システム用のデフォルトの逆多重化ポート（36000 ～ 36011）で多重化 RTP/RTCP トラフィックをリッスンすることを意味します。この場合、ポート 36000 ～ 36011 はファイアウォールで開かれていないため、Cisco VCS Expressway はコールをドロップします。

回避策

X8.11.4 から、[システム（System）] > [管理設定（Administration settings）] ページ（[展開構成（Deployment Configuration）] リストから [中（Medium）] を選択）を使用して、システム サイズを手動で [中（Medium）] 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 の Web ユーザ インターフェイスを翻訳する場合、X8.10.3 以降で、新しい Cisco VCS 言語パックが提供されます。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.）。パックのインストールまたは更新の手順については、*Cisco VCS* の管理者ガイドを参照してください。

IM&P ノード障害での XMPP フェデレーションの動作

XMPP 外部フェデレーションを使用する場合、停止後に IM and Presence Service 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 を展開する場合に該当します。Cisco VCS Control を使用するインターフェイスと外部インターフェイスの両方に同じ（重複する）静的ルートが適用される場合に、Cisco Webex Calling リクエストが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という現在の Cisco VCS Expressway のルーティング動作に起因します。

Note 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 と Meeting Server を介してデュアルホーム会議を使用する場合は、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。[構成（Configuration）] > [プロトコル（Protocols）] > [SIP] を選択し、[SIP最大サイズ（SIP max size）] で定義します。

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。

単一のドメイン内、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により）*Cisco VCS Expressway* を *Microsoft* のフロントエンド サーバに**直接接続**する構成では、個別の *Microsoft* 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、同じドメイン内で、*1* つの（サブ）ネットワークに *Cisco Unified Call Manager*、*2* つ目の（サブ）ネットワークに *Microsoft* を展開します。

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することができない場合（Meeting Server <> VCS Control <> Microsoft を構成できない場合）の回避策としては、各サブネットに VCS-C を展開し、サブネット間を通過させるために VCS-E を配置します。つまり、以下のようになります。

Meeting Server <> VCS Control <> Firewall <> 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）を追加しようとした場合、それらのキーは Cisco VCS の Web インターフェイス（[メンテナンス（Maintenance）] > [オプションキー（Option keys）]）では正常に見えます。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、展開の検証を支援するため、また、Cisco VCS のログ ファイル解析することでトラブルシューティングを支援するために、Cisco Technical Assistance Center （TAC）が作成したものです。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、[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）]）を使用して、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くことができます。

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。

バグ検索ツールのヘルプ ページには、バグ検索ツール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 2：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設定するには

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、[構成（Configuration）] > [Unified Communications] > [構成（Configuration）] > [MRAアクセス制御（MRA Access Control）] に移動します。

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方法を保持するには、このページで、Cisco VCS Expressway の以前の設定に合わせて適切な値を設定します。従来の Cisco VCS Expressway の設定と同等の Cisco VCS Control の新しい設定を調べるには、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（[OAuth トークンによる承認（更新あり）（Authorize by OAuth token with refresh）]）を構成する場合は、Unified CM ノードを更新します。[構成（Configuration）] > **[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。

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。

Table 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。 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。 UCM/LDAP Basic 認証（UCM/LDAP basic authentication）：クライアントは、Unified CM によって LDAP 資格情報に対してローカルに認証されます。 SAML SSO および UCM/LDAP（SAML SSO and UCM/LDAP）：どちらの方法も許可します。 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。単に MRA をオフにするのではなく [なし（None）]“ ”オプションが用意されているのは、展開によっては、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です。（Meeting Server の Web プロキシ、XMPP フェデレーションなど）。[なし（None）]“ ”は、そのような場合にのみ使用してください。 **Note** 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）] MRA をオンにした後は [UCM/LDAP]
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。 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）]

フィールド	説明	デフォルト
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。 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。 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。 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。 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 クライアント認証リクエストにどのように反応するかを制御します。 リクエストは、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、そのリクエストには 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。 はい（Yes）：*get_edge_sso* リクエストで、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 に確認します。ホーム Unified CM は、Jabber クライアントの *get_edge_sso* リクエストによって送信されたアイデンティティから判別されます。 いいえ（No）：Cisco VCS が内部を参照しないように構成されている場合に、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。 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。 **Caution** これを[はい（Yes）]に設定すると、	

フィールド	説明	デフォルト
	認証されていないリモートクライアントからの不正なインバウンドリクエス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 は不正なリクエストを防止します。	

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。 **ID プロバイダーの選択** 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。 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。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。 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）	

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。 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。 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。 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。 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。 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

Table 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 **Note** [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。 • **認証パス（Authentication path）** = *UCM/LDAP* • **ユーザ ログイン情報による承認（Authorize by user credentials）** = オン（*On*） [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。 • **認証パス（Authentication path）** = *SAML SSO* • **OAuth トークンによる承認（Authorize by OAuth token）** = オン（*On*） [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。 • **認証パス（Authentication path）** = *SAML SSO* および *UCM/LDAP* • **OAuth トークンによる承認（Authorize by OAuth token）** = オン（*On*） • **ユーザ ログイン情報による承認（Authorize by user credentials）** = オン（*On*）	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）