Cisco Expressway および Cisco TelePresence Video Communication Server リリース ノート（X14.2）

初版：2022 年 8 月 10 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。

変更履歴

Table 1: 変更履歴

日付	変更内容	理由
2022 年 8 月	再発行済み X14.2	X14.2 リリース 置き換えられたバグ識別子
2022 年 8 月	X14.2 用の初版	X14.2 リリース

日付	変更内容	理由
2022 年 7 月	X14.0.8 用の初版	X14.0.8 リリース
2022 年 5 月	X14.0.7 用の初版	X14.0.7 リリース
2022 年 3 月	X14.0.6 用の初版	X14.0.6 リリース
2022 年 2 月	X14.0.5 用の初版	X14.0.5 リリース
2021 年 12 月	X14.0.4 用の初版	X14.0.4 リリース
2021 年 8 月	X14.0.3 用の初版。	X14.0.3 リリース
2021 年 8 月	“このリリースのその他の変更”セクションに「トラフィックサーバーが証明書の検証を強制する」に関する新しい項目を追加しました。	X14.0.2 リリース：再発行
2021 年 7 月	X14.0.2 用の初版。	X14.0.2 リリース
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 リリース
2020 年 8 月	メンテナンス リリースの更新。	X12.6.2 リリース
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 リリース
2020 年 6 月	X12.6 用の初版。	X12.6 リリース

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 *Expressway* 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
中規模 VM（OVA）	（自動生成）	X8.1 以降
大規模 VM（OVA）	（自動生成）	X8.1 以降
CE1200 Hardware Revision 2（UCS C220 M5L にプレインストール）	52E1####	X12.5.5 以降。
CE1200 Hardware Revision 1（UCS C220 M5L にプレインストール）	52E0####	X8.11.1 以降。
CE1100（UCS C220 M4L にプレインストールされた Expressway）	52D#####	メンテナンスとバグ修正のみを目的とする X12.6.x バージョンでの限定的なサポートを除き、サポートされていません（X12.5.x 以降）。脆弱性/セキュリティのサポートは、2023 年 11 月 30 日まで延長されます。
CE1000（UCS C220 M3L にプレインストールされた Expressway）	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 Expressway）	52C#####	サポート対象外（X8.10. x 以降）

スマート ライセンシングのエクスポートに関するコンプライアンス

2500 以下のエンドポイントへのシグナリング

シスコは、すべてのグローバルな輸出法および規制の厳格な遵守を維持することに全力で取り組んでいます。

すべてのソフトウェアリリースは、関連するすべての輸出管理法（特定のソフトウェアおよび技術を他の国や団体に輸出または転送する条件を管理する米国および現地の国の規制）に準拠する必要があります。

Expresswayはメディアゲートウェイであり、メディア暗号化または暗号化されたシグナリングを 2500 **以下**のエンドポイントに提供する必要があります。この制限は、*Cisco Expressway X14.2* リリースで有効になります。

（注） 2500 の安全な/暗号セッションの CAP は、Cisco TelePresence Video Communication Server（VCS）シリーズにも適用できます。

エンドポイントへの暗号化されたシグナリングとは、SIP 登録または SIP コール、H.323 登録またはコール、WebRTC コール、および XMPP 登録を指します。

重要 暗号化されたシグナリングの限られた数が、Expressway のインスタンスごとに 2500 エンドポイントを**超えない**ことを確認してください。この制限を超える必要があるお客様は、資格があれば、追加のピア/クラスタを展開して、追加のキャパシティを提供できます。

（注） Cisco Expressway の将来のリリースでは、輸出規制対象の機能を使用しない対象外のお客様には制限が適用されますが、輸出規制対象機能の使用が許可されている対象のお客様は、（適切なハードウェアで実行されている場合）この制限を超えることができる新しい SKU（利用可能な場合）を注文する必要があり、これにより、一部のお客様に必要な Expressway インスタンスの総数が削減されます。

詳細については、『Cisco Expressway 管理者ガイド（X14.2）』を参照してください。

VMware 7.0 U2 での OVA の展開に関する通知

Note これは、現在のリリースにおける既知の問題です。X14.2 OVA を展開すると、vCenter 7.0 U2 バージョンの VMware では“無効な証明書”が表示されますが、古いバージョンでは“信頼できる証明書”が表示されます。この問題の詳細については、ナレッジ記事を参照してください。

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、以下のリンクで確認できます。

このソフトウェア リリースで解決された問題は、Cisco Expressway および Cisco TelePresence Video Communication Server のユーザが対象となりますが、このリリースで追加された新機能は Cisco TelePresence Video Communication Server（VCS）製品ではサポートされません。

この通知は、Cisco Expressway シリーズ製品には影響しません。

CE1200、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。

CE1200 アプライアンス

重要 Expressway CE1200 で使用されるコンポーネントの供給の問題により、注文処理が遅れています。供給の問題を考慮して、脆弱性/セキュリティのサポートの終了は 2023 年 11 月 30 日まで延長されます。

ユーザーインターフェイスに表示される、「**サポートされていないハードウェア**」の警告は無視してください。

CE1100 アプライアンス：サポート終了およびハードウェア サービス サポート撤回の事前通知

新しい Expressway アプライアンスのタイムリーな供給に影響を及ぼしているコンポーネント不足に関する発生中の問題を考慮して、Cisco Expressway CE1100 アプライアンスをまだ使用しているお客様をサポートするために、シスコは脆弱性/セキュリティサポートの終了を 2021 年 11 月 14 日（当初のサポート終了のお知らせ）から、有効なサービス契約を結んでいるお客様のサポートの最終日に合わせて、2023 年 11 月 30 日に延長することを決定しました。

（注） お客様はこのリリースのソフトウェアを Expressway CE1100 で実行し、セキュリティの改善/脆弱性の修正の恩恵を受けることができますが、多くの新機能はより新しくより強力なハードウェアを必要とするため、このリリースの Expressway ソフトウェアで追加された新機能の CE1100 プラットフォームでの使用はサポートされません。

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。

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。特定のデバイスの相互運用性に関する質問については、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）

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、エンドポイントおよびインフラストラクチャ製品のバージョン表に記載しています。

MRA の場合、最新の特長と機能にアクセスするには、Expressway を最新バージョンの UCM と組み合わせて展開することをお勧めします。ただし、Expressway には、以前の UCM リリースとの下位互換性もあります。

同時に実行できる Expressway サービス

『Cisco Expressway 管理者ガイド』で、どの Expressway サービスが同じ Expressway 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**」の章にある「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。

X14.2 の機能のサマリー

Table 3: リリース番号別の機能

機能/変更	ステータス
CDB API アクセスの有効化または無効化	X14.2 から対応
TLS 検証モード	X14.2 から対応
/tmp/ パスでファイルをアップロードする	X14.2 から対応
スマートライセンスフェーズ II	X14.2 から対応
MRA over IPv6	X14.2 から対応
XCP ルーティング情報	X14.2 から対応
承認済み暗号化プリミティブとパラメータ	X14.2 から対応

機能/変更	ステータス
TrafficServer の DOS 保護を有効にする	X14.2 から対応
電子メール通知を削減	X14.2 から対応
xCommand FIPS を使用する別の方法	X14.2 から対応
RedSky E911 ロケーションサービス	X14.0.4 から対応
サービス選択ウィザード	X14.0.3 から対応
IP アドレスを禁止/禁止解除	X14.0.3 から対応
IP アドレスを免除	X14.0.3 から対応
コール詳細レコード（CDR）構成	X14.0.3 から対応
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。	X14.0.1 からサポート対象
新しい RAML RESTA PI で SNMP の詳細を設定する機能。	X14.0.1 からサポート対象
コマンド インターフェイスを使用してアラームを表示および確認する機能	X14.0.1 からサポート対象
SSO/OAuth サインインでの URI リダイレクトのサポート	X14.0 以降でサポート
AV1 のサポート	X14.0 以降でサポート
“Jabber のゼロ ダウンタイム”での XCP サポート	X14.0 以降でサポート
P2P からミーティングへのエスカレーション	X14.0 以降でサポート
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	X14.0 以降でサポート
Cisco Jabber の MRA SIP 登録フェールオーバー	X14.0 以降でサポート
MRA モバイル アプリケーション管理クライアント	プレビュー
IM&P 用の Android プッシュ通知パブリッシャー	プレビュー（X12.6.2 からはデフォルトで無効）
Cisco Contact Center のヘッドセット機能	プレビュー

削除または廃止された機能とソフトウェア

Expressway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 4: 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
ハードウェア セキュリティ モジュール（HSM）のサポート	X14.2 から廃止
Microsoft Internet Explorer ブラウザのサポート	X14.0.2 で非推奨にされました。
VMware ESXi 6.0（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 Expressway 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
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
Expressway Starter Pack	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
Expressway 組み込み転送プロキシ	X12.6.2 で削除
Cisco Advanced Media Gateway	X12.6 で取り消し済み
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

表 5 : 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、Expressway 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	Expressway インストール ガイド ページの『Cisco Expressway CE1200 アプライアンス インストール 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	*Expressway* メンテナンスとオペレーション ガイド ページの『Cisco Expressway 管理者ガイド』http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-maintenance-guides-list.html（有用性情報を含む）
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）』
モバイル & リモート アクセス	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 導入ガイド』

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）』

X14.2 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、ユーザー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。

/tmp/ パスでファイルをアップロードする

ファイルのアップロードプロセスを安全に保つために、**/tmp/** パスでファイルをアップロードする必要があります。

たとえば、次のコマンドについて考えてみます。パスの先頭に **/tmp/** を使用します。

```
xcommand Passworddictionarywrite /tmp/random_file
```

TrafficServer の DOS 保護を有効にする

SIP および EDGE トラフィックカテゴリの新しい接続には、デフォルトのレート制限が設定されています。管理カテゴリもモニタリングキャパシティに含まれており、構成されたレベルを超える接続イベントの可視性とロギングを可能にします。

承認済み暗号化プリミティブとパラメータ

Expressway は SIP サービスの Anonymous Diffie Hellmen（ADH）暗号をサポートしていないため、TC/CE エンドポイントは SIP の証明書を有効にする必要があります（自己署名証明書はオン モードにする必要があります）。

管理用拡張機能

スマートライセンス

シスコ スマート ソフトウェア ライセンシングは、ライセンスについて考える新しい方法です。

Note Cisco Expressway X14.2 はスマートライセンス**のみ**をサポートし、エンドポイントへの暗号化されたシグナリング セッションは 2500 に制限されます。また、MRA 障害につながる可能性のあるトラフィックサーバーの動作（バグ識別子 CSCwc69661 が参照）の変更も含まれています。こちらを参照してください。詳細については、X14.2 にアップグレードする前に、『*Cisco Expressway and Cisco TelePresence Video Communication Server* リリースノート（*x14.2*）』および『*Cisco Expressway* 管理者ガイド（*x14.2*）』を参照してください。

この方法は、通常、クラウドベースの Cisco Smart Software Manager（CSSM）を使用して管理されます。または、オンプレミスでの対応が必要な環境の場合は、Smart Software Manager オンプレミス製品（旧称 “Smart Software Manager サテライト”）を使用できます。

スマート ライセンスを使用すると、お客様が自社の Expressway ノードまたはクラスタからライセンスを使用する柔軟性が得られます。

スマート ライセンシングでは次のことを実行できます。

- ライセンスの使用状況とライセンス数の表示。
- 各ライセンス タイプのステータスの表示。
- Cisco Smart Software Manager または Smart Software Manager オンプレミスで利用可能な製品ライセンスを参照してください。
- Cisco Smart Software Manager または Smart Software Manager オンプレミスによるライセンス認証の更新。
- 登録の更新

- Cisco Smart Software Manager または Smart Software Manager オンプレミスによる登録解除
- Cisco Smart Software Manager でのライセンスの再登録

Important

- 製品アクティベーションキー（PAK）ライセンス（オプションキー）は、バージョン X14.2 から削除されました。
- スマートライセンスはデフォルトであり、Expressway-C および Expressway-E の唯一のライセンスモードです。
- スマート ライセンス モードでは、この機能はデフォルトで有効になっているため、キーは必要ないか、サポートされません。また、ライセンス登録ポータル で変換できない場合があります。

スマートライセンスの予約のタイプ

Cisco スマートライセンス予約は、ライセンスを予約してデバイスにインストールすることを目的としています。このプロセスにより、シスコデバイスから一意の予約コードを生成でき、このコードは、Cisco スマートアカウントのインベントリからライセンスタイプと数量を予約するために使用されます。

ライセンスの予約タイプは次のとおりです。

- **永久ライセンス予約（PLR）**：すべてのライセンスが予約されています。
- **特定ライセンス予約（SLR）**：特定のライセンスのみが予約されます。

Cisco スマートライセンス予約とそのタイプの詳細については、『Cisco Expressway 管理者ガイド（X14.2）』の「*Cisco* スマートライセンス予約とそのタイプについて」セクションを参照してください。

コマンドライン インターフェイスの更新

この機能をサポートするために、次の新しい CLI コマンドが導入されました。

- `xconfiguration License Smart ReservationEnable: On`
- `xcommand License Smart Reservation Request`
- `xcommand License Smart Reservation Install <authorization code>`
- `xcommand License Smart Reservation Return`
- `xcommand License Smart Reservation ReturnAuthorization <auth code>`
- `xcommand License Smart Reservation Cancel`

Note 次のコマンドは、永久ライセンス予約（PLR）と特定ライセンス予約（SLR）の両方に共通です。

PLR および SLR の CLI コマンドのリストの詳細については、『Cisco Expressway 管理者ガイド（X14.2）』の「*PLR* および *SLR* の *CLI* コマンド」に関するセクションを参照してください。

パーマネント ライセンスの予約

永久ライセンス予約（PLR）は、Cisco Smart Licensing ソリューションの一部です。スマートライセンスにはスマートアカウントが必要です。製品を再アクティブ化して最新のライセンスステータスをレポートするには、Cisco Smart Software Management（CSSM）または Smart Software Manage（SSM オンプレミス）に接続する必要があります。インターネットアクセスが制限された非常に安全な内部ネットワークがある場合は、Cisco 永久ライセンス予約（PLR） ライセンスを使用します。

永久ライセンスは、評価ライセンスに適用することができ、段階的に適用することもできます（つまり、複数の永久保証ライセンスを所有する、などが可能です）。その機能は、外部環境との通信が不可能な、安全性が非常に高い環境向けに設計されています。

Cisco 永久ライセンス予約の設定方法の詳細については、『Cisco Expressway 管理者ガイド（x14.2）』の「永久ライセンス予約」のセクションを参照してください。

特定ライセンス予約

特定ライセンス予約は、Cisco Smart Software Manager または Cisco Smart Software Manager オンプレミスに常時接続できない、安全性の高いネットワークで使用される機能です。この機能により、お客様は使用状況を通信することなく、デバイス（製品インスタンス - Expressway）にソフトウェアライセンスを導入できます。

特定ライセンス予約は、Cisco Expressway 製品インスタンスに対し、永久または期限付きのライセンスを予約できます。Cisco Smart Software Manager から生成された承認コードは、Expressway 製品にインストールできます。また、指定されたライセンス消費内で製品を実行している場合、定期的な同期は必要ありません。

Cisco Smart Software Manager でライセンスを予約する機能は、スマートアカウントプロファイルを介して実行されます。

Cisco 固有のライセンスの予約を設定する方法の詳細については、Cisco Expressway 管理者ガイド（X14.2）の特定のライセンス予約に関するセクションを参照してください。

その他の情報と制限事項

特定のライセンス予約モードの Expressway は、次を導入します。

- ライセンスは、クラスタ内の Expressway ノード全体で共有されます。
- ライセンスの使用状況は、Expressway のローカル スマート エージェントに報告されます。

Cisco Smart Licensing の設定方法の詳細については、『Cisco Expressway 管理者ガイド（X14.2）』の *Smart Licensing* に関する章、「その他の情報」セクション、「制限事項」を参照してください。

設定の詳細

Cisco Smart Licensing の設定方法の詳細については、『Cisco Expressway 管理者ガイド（X14.2）』の *Smart Licensing* に関する章を参照してください。

プレビュー機能

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。

（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：X14.2 リリース以降廃止

Expressway X12.6 リリースでは、**プレビュー**機能として HSM 機能が追加されています（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）。

メンテナンス > **セキュリティ** > **HSM 構成**ページは、このバージョンの Expressway ソフトウェアの Expressway ユーザーインターフェイスに引き続き表示されますが、この機能は廃止され、将来のソフトウェアリリースでユーザーインターフェイスから削除されます。

（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 and Remote Access を使用して Expressway を展開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。

詳細は、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。

（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、Mobile and Remote Access を使用して Expressway を展開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。

この機能を使用すると、Jabber Intune や Jabber BlackBerry 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、Mobile and Remote Access を介したプッシュ通知のサポート対象

になります。その結果、Jabber Intune クライアントや Jabber BlackBerry 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、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）。

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。

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。

表 *6 : REST API* のリスト

構成 API	API が導入されたバージョン
CDB REST API アクセス：CDB REST API アクセスの有効化/無効化	X14.2
サービス選択ウィザード	X14.0.3
アクティブアラームを確認する機能	X14.0.3
IP アドレスを禁止/禁止解除	X14.0.3
IP アドレスを免除	X14.0.3
コール詳細レコード（CDR）構成	X14.0.3
ステータス：fail2banbannedaddress	X14.0.2
SNMP 構成	X14.0.1
アラーム：表示および確認	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

今回のリリースでのその他の変更点

TLS 検証モード

VCS（ATS）と CUCM/CUP/JabberGuest/UNITY/CMS の間で通信が発生した場合、デフォルトでサーバー証明書の検証が有効になっています。お客様がリリース 14.2 にアップグレードする場合、CUCM/CUP/JabberGuest/UNITY/CMS サーバー証明書の CA が VCS CA 信頼ストアに存在する必要があります。お客様がサーバー証明書の検証を無効/有効にする場合、次のコマンドを使用します。

```
xConfiguration EdgeConfigServer VerifyOriginServer: OFF/ON
```

スマート ライセンシングのエクスポートに関するコンプライアンス

2500 以下のエンドポイントへのシグナリング

Note

- 2500 件の登録/通話/セッションのエクスポート制限は、すべてのお客様に対してデフォルトでオンになっています。これは、すべてのお客様が 2500 を超える暗号化接続を**作成できない**ことを意味します。
- エンドポイントへの暗号化されたシグナリングセッションの上限は 2500 です。
- 製品アクティベーションキー（PAK）ライセンス（オプションキー）は、Cisco Expressway X14.2 リリースから削除されました。
- スマートライセンスはデフォルトであり、Expressway-C および Expressway-E の**唯一のライセンスモードです。**

Important

2 つの暗号化されたシグナリングセッションが同じエンドポイントからのものであるかどうかを判断するのに十分な情報が Expressway にない場合があります。たとえば、Expressway が個別の SIP および XMPP 登録（個別の暗号化されたシグナリングセッション）を認識する Jabber では、それらが単一のエンドポイントからのものかどうかを判断できません。これは二重にカウントされます。

したがって、2200 人の Jabber ユーザがいるお客様は、アップグレードしても問題ないと考えるかもしれません。しかし、X14.2 にアップグレードすると、これは 4400 シグナリングセッションと見なされ、登録とコールが拒否されます。

Table 7: 製品でサポートされているスマートライセンス機能の比較

	Cisco Expressway	Cisco TelePresence Video Communication Server（VCS）	備考
2500 の安全な/暗号化セッションの CAP	はい	はい	両方のプラットフォームで、ライセンスモデル（Smart Licensing または PAK）に関係なく、X14.2 リリースにアップグレードすると、2500 の安全な/暗号化セッションの CAP が適用されます。
高度なアカウントセキュリティ（AAS）および FIPS140-2 暗号化モードをサポート	いいえ	○ 適切なオプションキーを追加/インストールすることにより、AAS および FIPS140-2 機能を**有効にする**オプションが利用できます。	
スマート ライセンス	はい	いいえ	Cisco VCS の場合、オプションキー/PAK ライセンスモードのみ

詳細については、『Cisco Expressway 管理者ガイド（X14.2）』を参照してください。

CDB API アクセスの有効化または無効化

Expressway 製品のセキュリティを考慮して、CDB API へのアクセスはデフォルトで無効にされています。これらは、Web ユーザーインターフェイスまたは REST API を使用して有効または無効にすることができます。REST API（https://%3CIP%20address%3E/api/provisioning/common/cdbrestapiaccess）を使用して、CDB REST API へのアクセスを有効または無効にすることができます。

詳細については、『Cisco Expressway 管理者ガイド（X14.2）』を参照してください。

4+1 および 5+1 冗長モデルのサポート

Expressway は、4+1 および 5+1 冗長モデルをサポートします。クラスタごとに最大 4 つまたは 5 つの Expressway ノードと最大 N+1 の物理冗長性を設定できます。

XCP ルーティングテーブル

この改善により、Extensible Communications Platform（XCP）ルーティングテーブルの内容が表示されます。この内容は、Cisco Jabber に含まれる XCP ルーティング情報の完全なデータダンプです。この情報は、XCP の視点からのデバッグに役立ちます。これは、VCS デバイスの **routing.xml** ファイルと **developer.xcp.jabber ログ**の両方で使用できます。

さらに、ConnectionManager の情報は、デベロッパーログを通じてデータダンプとして利用することもできます。この情報には、ConnectedSockets および FailedRequests カウンタの状態が表示されます。

このすべての情報は、管理者が、各 Jabber クライアント接続のルーティング情報、接続数、および詳細を確認するのに役立ちます。

電子メール通知の削減

この改善の目的は、何らかの理由で短期間に複数のアラームが発生した場合に、管理者を電子メールでスパミングしないようにすることです。

1 時間以内に同じアラームが 2 回以上発生した場合、電子メールは 1 回だけ送信されます。同じアラームが止み、再び発生した場合は、経過時間に関係なく電子メールが送信されます。当然、これは、管理者がデバイスで電子メール通知を受信するように構成している場合にのみ適用されます。

xCommand FIPS を使用する別の方法

- **Expressway シリーズ**：**エクスポート制御**を有効にして（*[True]* に設定）FIPS をアクティブ化します。これを有効にすると、すべてのコマンド（<*leave/enter/status*>）が使用可能になります。
- **Cisco VCS**：[**オプションキーの追加**] フィールドで（または CLI コマンドを使用して）、**[メンテナンス]**>**[オプションキー]** に J00 オプションキーを追加する必要があります。FIPS（<*leave/enter/status*>）は、JOO オプションキーを追加する前にのみ表示されます。JOO オプションキーは、追加後にのみ使用できます。

Note Smart Licensing は FIPS に準拠しています。

ECDSA 暗号を RSA より優先

ECDSA 証明書は RSA よりも優先されます。

14.2 以前のバージョンから 14.2 以降のバージョンにアップグレードする場合は、ECDSA よりも RSA 証明書を優先するために、“ECDHE-RSA-AES256-GCM-SHA384:” がデフォルトの暗号リストに追加されていることに注意してください。RSA よりも ECDSA 証明書を優先する場合は、Web UI（**[メンテナンス]** > **[セキュリティ]** > **[暗号方式]**）または CLI コマンド（**xConfiguration Ciphers**）を使用して、暗号文字列から “ECDHE-RSA-AES256-GCM-SHA384:” を削除します。

TLS 1.3 対応

X14.2 リリース以降、Expressway は SIP およびリバースプロキシ機能のために TLS 1.3 をサポートしています。

自動作成された CE ゾーンステータス

X14.0.2 以前の Expressway バージョンでは、ゾーンプロファイルで [ピア ステータスのモニタ]/[ネイバーモニタ] が [**いいえ**] に設定されている CE ゾーンのステータスが**アクティブ**であると表示されます。Expressway は CE ゾーンのピアステータスをモニタリングしていないため、より正確なステータス [**アドレス解決可能**] が示されるためです。

自動作成された UC ゾーンと関連付けられたユニファイドコミュニケーション ゾーン プロファイルはカスタマイズできず、ネイバーモニタを [**いいえ**] に設定するのは設計によるものです。

Expressway X14.0.2 以降、UC ノード宛ての自動作成された CE（tcp/tls/OAuth）ゾーンは、CSCup29823 の修正に従って、ステータスを **[アドレス解決可能]** と表示します。

トラフィックサーバーが証明書の検証を強制する

Important X14.0.2 より前のリリースから X14.2 にアップグレードする前に、次の証明書の要件が満たされていることを確認してください。

X14.0.2 以降の Expressway のトラフィック サーバー サービスの改善により、MRA に対して以下を設定する必要があります。

要件：Expressway-C 証明書に署名した認証局（CA）は、UCM が**非セキュア**モードの場合でも、Cisco Unified Communications Manager（UCM）の *Tomcat*-trust および *CallManager*-trust リストに追加する必要があります。その後で、CUCM 側で次のサービスを再起動します。

- Tomcat サービス
- CallManager サービス
- HA プロキシサービス（Tomcat で TLS を使用している場合）

理由：Expressway のトラフィック サーバー サービスは、サーバー（UCM）が要求するたびに証明書を送信します。これらの要求は、8443 以外のポート（たとえば、ポート 6971、6972 など）で実行されているサービスに対するものです。これにより、UCM が非セキュアモードの場合でも、証明書の検証が強制されます。

詳細については、『Expressway 経由のモバイルおよびリモートアクセス導入ガイド』を参照してください。

制限事項

スマート ライセンシングのエクスポートに関するコンプライアンス

制限付き機能のエクスポート：2500 を超えるエンドポイントへのシグナリング

（注） 次の面は、Cisco Expressway X14.2 リリースに関連しています。

1. Cisco Expressway X14.2 リリースは、2500 の安全なセッションの CAP を備えた**無制限**および**上限付き**バージョンです。

   注：2500 の安全なセッションの CAP は、Cisco TelePresence Video Communication Server（VCS）シリーズにも適用できます。

2. Cisco Expressway X14.2.1 の次のリリースでシステムを更新して、安全なセッションに**無制限にアクセス**できるようにします。

X14.2.1 のリリース日は未定です。

一部の Expressway 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、Expressway 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。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**（「**プレビュー機能の免責事項**」を参照してください）。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。

未解決および解決済みの問題

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）
- X14.2 で解決済みの問題

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. 表示されたバグのリストで [フィルタ（Filter）] ドロップダウンリストを使用して、[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。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。