セキュリティの管理

このセクションでは、Expresswayのセキュリティの概念と設定について説明します。（ユーザアカウントの管理、デバイス認証、および登録アクセス制御に関する情報は、このガイドの後の別の章で説明します。）

セキュリティの基本

保管中のデータ

X8.11 以降、すべてのソフトウェアインストールには一意の信頼できるルートが使用されるようになっています。それぞれの Expressway システムには、そのシステムにローカルなデータを暗号化するために使用される一意のキーがあります。これにより、保管中のデータのセキュリティが次のように強化されます。

- X8.11 より前のバージョンを X8.11 以降にアップグレードすると、新しいキーが作成されます。最初の再起動時に、このキーを使用してすべてのデータが暗号化されます。

- このシステムから取得したデータを復号できるのは、このキーのみです。ほかのExpressway キーでは、このシステムのデータを復号することはできません。
- キーは UI 上で公開される事も、ローカルでもリモートでもログは記録されません。

TLS および証明書

クライアントとサーバ間の接続で TLS 暗号化を正常に機能させるためには以下が必要です。

- サーバには、アイデンティティを検証する認証局（CA）によって署名された証明書がインストールされている必要があります。
- クライアントはサーバが使用する証明書に署名した CA を信頼する必要があります。

Expressway では、TLS 接続で、クライアントまたはサーバとして Expressway を表すことができる証明書をインストールすることができます。Expressway は、HTTPS 経由のクライアント接続（通常は Web ブラウザから）を認証することもできます。また、LDAP サーバおよびHTTPS クライアント証明書の検証に使用されるCAの証明書失効リスト（CRL）をアップロードすることができます。Expresswayは、サーバ証明書署名要求（CSR）を生成することができます。そのため、これを行う外部メカニズムを使用する必要はありません。

（注） セキュアな通信（HTTPSおよびSIP/TLS）のために、Expresswayのデフォルトの証明書を、信頼できる CA が生成した証明書に置き換えることを推奨します。

表 *1*：接続タイプ別の *Expressway* の役割

接続先	Expressway の役割
エンドポイント	TLS サーバ
LDAP サーバ	クライアント
2 つの Expressway システム間	どちらかの Expressway がクライアントになる可能性があります。もう一方の Expressway は TLS サーバです。
HTTPS 経由	Webブラウザはクライアントです。Expressway はサーバです。

（注） また、TLS用にLDAPサーバが正しく設定されていることを検証するためにサードパーティのLDAP ブラウザを使用することが推奨されます。

TLS は設定が難しい場合があります。たとえば、LDAP サーバで使用する場合は、TLS との接続を保護する前に、システムがTCP上で正しく動作することを確認することをお勧めします。

注意 証明書は RFC に準拠している必要があります。CA 証明書または CRL の期限は、CA によって署名された証明書が拒否される可能性があるため許可されません。

証明書および CRL ファイルは、Web インターフェイスを介して管理され、CLI を使用してインストールすることはできません。

証明書ベースの認証の設定

「証明書ベースの認証設定（Certificate-based authentication configuration）」ページ（**[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [証明書ベースの認証設定（Certificate-based authentication configuration）]**）を使用して、クライアント ブラウザの証明書から Expressway が許可クレデンシャル（ユーザ名）を取得する方法を設定します。

この設定は、**[クライアント証明書ベースのセキュリティ（Client certificate-based security）]**（[システム（System）] ページで定義）を *[証明書ベースの認証（Certificate-based authentication）]* に設定している場合に必要です。この設定により、標準的なログイン メカニズムが使用できなくなります。また、管理者（および Expressway 経由でアクセスした場合は FindMe アカウント）は通常、スマート カード（Common Access Card（CAC）とも呼ばれる）を介して提供された有効なブラウザ証明書を提示し、その証明書に適切な認証レベルの適切なクレデンシャルが含まれている場合にのみログインできることを意味します。

証明書ベースの認証の有効化

次に、証明書ベースの認証を有効にするための推奨手順について説明します。

手順

ステップ 1 Expressway の信頼できる CA 証明書とサーバ証明書ファイルを（「**信頼された CA 証明書（Trusted CA certificate）**」ページと「**サーバ証明書（Server certificate）**」ページそれぞれに）追加します。

ステップ 2 証明書失効リストを設定します（「**CRL 管理（CRL management）**」ページ）。

ステップ 3 「**クライアント証明書テスト（Client certificate testing）**」ページを使用して、使用するクライアント証明書が有効であることを確認します。

ステップ 4 **[クライアント証明書ベースのセキュリティ（Client certificate-based security）]** を *[証明書の検証（Certificate validation）]* に設定します（「**システム管理（System Administration）**」ページ）。

ステップ 5 Expressway を再起動します。

ステップ 6 「**クライアント証明書テスト（Client certificate testing）**」ページを再度使用して、必要な正規表現と形式パターンをセットアップし、証明書からユーザ名クレデンシャルを抽出します。

ステップ 7 正しいユーザ名が証明書から取得されていることが確認された場合にのみ、**[クライアント証明書ベースのセキュリティ（Client certificate-based security）]** を *[*証明書ベースの認証（*Certificate-based authentication*）*]* に設定します。

認証と許可

Expressway が証明書ベースの認証モードで動作しているときに、ユーザ認証は Expressway 外にあるプロセスを通じて管理されます。

ユーザが Expressway にログインしようとすると、Expressway はクライアント ブラウザからの証明書を要求します。ブラウザはカード リーダと連携してスマート カードから証明書を取得します（または、証明書がすでにブラウザにロードされている場合もあります）。カードまたはブラウザから証明書をリリースするには、通常、ユーザはPINを入力して自分自身を認証するように求められます。Expresswayが受信したクライアント証明書が有効な場合（信頼できる認証局によって署名され、期限が切れておらず、CRL で失効になっていない）、ユーザは認証されていると見なされます。

ユーザの許可レベル（読み書き、読み取り専用など）を特定するには、Expresswayがユーザの許可ユーザ名を証明書から抽出し、それを関連するローカルまたはリモートの許可メカニズムに提示する必要があります。

（注） クライアント証明書が（PIN またはその他の何らかのメカニズムによって）保護されていない場合は、Expressway への認証されていないアクセスが可能になることがあります。この保護の欠如は、証明書がブラウザに保存されていない場合にも該当しますが、証明書ストアのパスワード保護を許可するブラウザもあります。

証明書からのユーザ名の取得

ユーザ名はクライアント ブラウザの証明書から **[正規表現（Regex）]** フィールドと **[ユーザ名の形式（Username format）]** フィールド（「**証明書ベースの認証設定（Certificate-based authentication configuration**）」ページ上）で定義されたパターンに従って抽出されます。

- **[正規表現（Regex）]** フィールドに（**?<name>regex**）シンタックスを使用してキャプチャ グループ用の名前を指定し、関連付けられた **[ユーザ名の形式（Username format）]** フィールドで一致サブパターンを置換できるようにします。次に例を示します。

  /(Subject:.*, CN=(?<Group1>.*))/m.

  ここで定義する正規表現は、*PHP* 正規表現のガイドラインに準拠する必要があります。

- **[ユーザ名の形式（Username format）]** フィールドには、固定テキストと **[正規表現（Regex）]** で使用したキャプチャ グループの名前を組み合わせて含めることができます。各キャプチャ グループ名を#で区切ります。例：**prefix#Group1#suffix** 各キャプチャ グループ名は正規表現の処理から取得されたテキストに置き換えられます。

「クライアント証明書のテスト」ページを使用して、**[正規表現（Regex）]** と **[ユーザ名の形式（Username format）]** のさまざまな組み合わせを証明書に適用した結果をテストできます。

緊急アカウントと証明書ベースの認証

高度なアカウント セキュリティ モードでは、リモート認証だけでなく、認証サーバが利用できない場合のために緊急アカウントも指定する必要があります。高度なアカウント セキュリティ モードの設定を参照してください。

証明書ベースの認証を使用している場合、緊急アカウントでは、クレデンシャルの一致する有効な証明書を提示することで認証できる必要があります。

緊急アカウントのクライアント証明書を作成し、CN を [ユーザ名の形式（Username format）] と一致させ、この証明書を緊急管理者の証明書ストアにロードする必要があります。

信頼された CA 証明書リストの管理

「信頼できる CA 証明書（Trusted CA certificate）」 ページ（**[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）]**）で、この Expressway が信頼する証明局（CA）の証明書のリストを管理できます。Expressway への TLS 接続が証明書検証を要求したときは、Expressway に提示された証明書が、このリストの信頼できる CA によって署名され、ルート CA に対する完全なトラスト チェーン（中間 CA）がある必要があります。

- 1 つ以上の CA 証明書を含む新しいファイルをアップロードするには、**[参照（Browse）]** をクリックして必要な PEM ファイルの場所を指定し、**[CA 証明書の追加（Append CA certificate）]** をクリックします。これにより、新しい証明書が CA 証明書の既存リストに加えられます。特定の発行者およびサブジェクトの既存の証明書を交換する場合は、手動で以前の証明書を削除する必要があります。
- 現在アップロードされたすべての CA 証明書をシステムの信頼できる CA 証明書の元のリストと交換するには、[Reset to default CA certificate] をクリックします。
- 現在アップロードされた信頼できる CA 証明書のリスト全体を表示する場合、人間可読形式で表示するには **[Show all (decoded)]** をクリック、または raw 形式でファイルを表示するには **[Show all (PEM file)]** をクリックします
- 個別の信頼できる CA 証明書を表示するには、特定の CA 証明書の行で **[View (decoded)]** をクリックします。
- 1 つ以上の CA 証明書を削除するには、該当する CA 証明書の隣にあるボックスにチェックを入れて、[Delete] をクリックします。

（注） TLS の暗号化された LDAP サーバへの接続（アカウント認証用）を確認する証明書失効リストを有効にしている場合は、信頼できる CA 証明書ファイルに PEM でエンコードされた CRL データを追加する必要があります。

デフォルトで含まれるルート CA

Expressway X12.6 以降には、次の信頼されたルート CA が含 まれます。*Cisco Intersection CA* バンドルの一部としてインストールされます 。

- O=Internet Security Research Group, CN=ISRG Root X1
- O=Digital Signature Trust Co., CN=DST Root CA X3

Expressway のサーバ証明書の管理

サーバ証明書ページ（[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [サーバ証明書（Server certificate）]）を使用して Expressway サーバ証明書を管理します。Expressway は、HTTPS 経由で TLS 暗号化および Web ブラウザを使用してクライアントシステムと通信するときに Expressway を識別します。

現在ロードされている証明書の詳細を表示して、CSR の生成、新しい証明書のアップロード、ACME サービスを設定できます。これらのタスクについては、「Expressway 設定ガイド」ページの 「*Cisco Expressway* 証明書の作成と使用導入ガイド」を参照してください。

（注） RSA キーに基づく証明書を使用することを強く推奨します。

DSA キーに基づく証明書など他のタイプの証明書はテストされておらず、あらゆるシナリオで Expressway と連携するとは限りません。

ACME サービスの使用

X12.5 以降、Cisco Expressway シリーズでは、ACME (AutomatedCertificate Management Environment) プロトコルをサポートするようになっています。このプロトコルにより、Let's Encrypt などの認証局から Expressway-E に署名済みの証明書を自動的に導入することが可能になります。

サーバ証明書とクラスタ化システム

CSR の生成時には、1 つの要求および秘密キーの組み合わせがそのピア専用に生成されます。Expressway のクラスタがある場合は、各ピアで個別の署名要求を生成する必要があります。これらの要求はその後、認証局に送信し、返されたサーバ証明書を関連する各ピアにアップロードする必要があります。

正しいサーバ証明書が適切なピアにアップロードされていることを確認する必要があります。そうでないと、各ピアに保存された秘密キーがアップロードされた証明書に対応しません。

サーバ証明書とユニファイド コミュニケーション

モバイルおよびリモートアクセスを導入する場合は、Unified Communication と Expressway の証明書要件の詳細については、「Expressway 設定ガイド」ページの「*Cisco Expressway* 証明書の作成と使用導入ガイド」を参照してください。

証明書失効リスト（CRL）の管理

証明書失効リストファイル（CRL）は、TLS/HTTPS を介して Expressway と通信するクライアントブラウザおよび外部システムにより提示される証明書を検証するために Expressway によって使用されます。CRL は、廃棄され Expressway との通信に使用できなくなった証明書を識別します。

TLS/HTTPS クライアントおよびサーバ証明書に署名する CA の CRL データをアップロードすることを推奨します。イネーブルの場合、CRL のチェックはトラストチェーンのすべての CA に適用されます。

証明書失効ソース

Expressway は複数のソースから証明書失効情報を取得できます。

- CRL 分散ポイントからの CRL データの自動ダウンロード
- 証明書内のチェック対象 OCSP（Online Certificate Status Protocol）レスポンダ URI 経由（SIP TLS のみ）
- CRL データの手動アップロード
- Expressway の**信頼できる CA 証明書**ファイル内に組み込まれた CRL データ

制限事項と使用上のガイドライン

次の制約事項および使用上のガイドラインが適用されます。

- SIP TLS 接続を確立するときに、設定ページの **[証明書失効確認（Certificate revocation checking）][SIP]**の設定が CRL データ ソースに適用されます。
- 自動的にダウンロードされた CRL ファイルが、手動でロードされた CRL ファイルを上書きする場合（SIP TLS 接続を確認する場合、手動でアップロードされた CRL データと自動でダウンロードされた CRL データの両方を使用する可能性がある場合は除く）
- 外部ポリシーサーバによって提示された証明書を検証する際に、Expressway は手動でロードされた CRL のみを使用します。

- リモート ログイン アカウントを認証するために LDAP サーバの TLS 接続を確認する場合、Expressway は**信頼できる CA 証明書（[ツール（Tools）]> [セキュリティ（Security）]> [信頼できる CA 証明書（Trusted CA certificate）]**）に組み込まれた CRL データのみを使用します。

  LDAP 接続の場合、Expressway はサーバの証明書配布ポイントの URL または発行する CA 証明書から CRL をダウンロードしません。また、[CRL 管理（CRL management）] ページの手動または自動更新設定も使用しません。

自動 CRL 更新

（注） 自動 CRL 更新を実行するように Expressway を設定することを推奨します。これにより、最新の CRL が証明書の検証に使用できるようになります。

手順

ステップ 1 **[メンテナンス（Maintenance）]>[セキュリティ（Security）]>[CRL 管理（CRL management）]** に移動します。

ステップ 2 **[自動 CRL 更新（Automatic CRL updates）]** を *[有効（Enabled）]* に設定します。

ステップ 3 Expressway が CRL ファイルを取得できる **HTTP/HTTPS 分散ポイント**のセットを入力します。

（注）
- 新しい行にそれぞれ分散ポイントを指定する必要があります。
- HTTP/HTTPS 分散ポイントのみがサポートされます。HTTPS を使用する場合、分散ポイントのサーバ自体に有効な証明書が必要です。
- PEM および DER エンコード CRL ファイルがサポートされています。
- 分散ポイントは、CRL ファイルまたは複数の CRL ファイルを含む ZIP および GZIP アーカイブを直接示す場合があります。
- URL またはダウンロードしたアーカイブから解凍されたファイルのファイル拡張子は、Expressway がその基盤となるファイル タイプを決定するため、重要ではありませんが、代表的な URL は次の形式となります。
  - http://example.com/crl.pem
  - http://example.com/crl.der
  - http://example.com/ca.crl
  - https://example.com/allcrls.zip
  - https://example.com/allcrls.gz

ステップ 4 **[Daily update time]** を入力します（UTC 単位で）。これは、Expressway が分散ポイントからその CRL の更新を試行するおおよその時刻です。

ステップ 5 [保存（Save）] をクリックします。

手動 CRL 更新

CRL ファイルは Expressway に手動でアップロードできます。外部ポリシー サーバによって提示された証明書は、手動でロードされた CRL に対してのみ検証できます。

手順

ステップ 1 **[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[CRL 管理（CRL management）]** に移動します。

ステップ 2 **[参照（Browse）]** をクリックして、ファイル システムから必要なファイルを選択します。また、PEM エンコード形式である必要があります。

ステップ 3 [CRL ファイルのアップロード（Upload CRL file）] をクリックします。

これによって、選択したファイルがアップロードされ、以前にアップロードした CRL ファイルが置換されます。

Expressway から手動でアップロードされたファイルを削除する場合は、**[失効リストの削除（Remove revocation list）]** をクリックします。

注：認証局の CRL が期限切れの場合、その CA から発行されたすべての証明書が無効として扱われます。

オンライン証明書ステータス プロトコル（OCSP）

Expressway は OCSP レスポンダとの接続を確立して特定の証明書のステータスを照会することができます。Expressway は使用する OCSP レスポンダを、確認する証明書に示されているレスポンダ URI から決定します。OCSP レスポンダは「良好（good）」、「失効（revoked）」、または「不明（unknown）」で証明書のステータスを送信します。

OCSP の利点は、失効リスト全体をダウンロードする必要がないことです。OCSP は SIP TLS 接続のみでサポートされます。OCSP を有効にする方法については、以下を参照してください。

OCSP レスポンダへ接続するには、Expressway-E からのアウトバウンド通信が必要です。使用している OCSP レスポンダのポート番号（通常はポート 80 または 443）をチェックし、Expressway-E からそのポートへのアウトバウンド通信が可能であることを確認します。

SIP TLS 接続を確認する失効の設定

また、証明書失効確認が SIP TLS 接続でどのように管理されるかを設定する必要があります。

1. **[Configuration]** > **[SIP]** を選択します。
2. **[証明書失効確認（Certificate revocation checking）]** セクションまでスクロールし、適宜設定を行います。

フィールド	説明	使用方法のヒント
Certificate revocation checking mode	失効確認が SIP TLS 接続の確立時に交換された証明書に対し実行されるかどうかを制御します。	失効確認をイネーブルにすることを推奨します。
Use OCSP	Online Certificate Status Protocol（OCSP）を証明書失効確認を実行するために使用するかどうかを制御します。	OCSP を使用するには、以下の条件が必要です。 • チェック対象の X.509 証明書に OCSP レスポンダの URI が含まれている必要があります。 • OCSP レスポンダーは、SHA-256 ハッシュアルゴリズムをサポートしている必要があります。サポートされていない場合、OCSP 失効チェックと証明書検証は失敗します。
Use CRLs	証明書失効リスト（CRL）を証明書失効確認を実行するために使用するかどうかを制御します。	CRL は、証明書が OCSP をサポートしていない場合に使用できます。 CRL は手動で Expressway にロードしたり、事前に設定された URI から自動的にダウンロードしたりできます（証明書失効リスト（CRL）の管理を参照）あるいは、X.509 証明書に含まれている CRL 配布ポイント（CDP）URI からも自動的にダウンロードすることもできます。
Allow CRL downloads from CDPs	X.509 証明書に含まれる CDP URI からの CRL のダウンロードを許可するかどうかを制御します。	

フィールド	説明	使用方法のヒント
Fallback behavior	たとえば、失効の送信元に連絡を取れないなど、失効ステータスを確立できない場合に、失効確認の動作を制御します。 *[失効として処理（Treat as revoked）]*：証明書を失効したとして処理します（そのため、TLS 接続を許可しません）。 *[失効していないものとして処理（Treat as not revoked）]*：失効していないものとして証明書を処理します。 デフォルト：*[Treat as not revoked]*	*[失効していないものとして処理（Treat as not revoked）]*では、失効の送信元に連絡をとれない場合、システムは通常の方法で稼働し続けますが、失効した証明書が承認される可能性があることを意味します。

MRA オンボーディングの mTLS クライアント証明書検証の管理

mTLS の CA 証明書ページには、**「信頼できる CA 証明書リストの管理（Managing the Trusted CA Certificate List）」**ページ（**[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）]**）からアクセスできます。このページが適用されるのは、Cisco Unified Communications 製品でモバイルおよびリモート アクセス（MRA）用に Expressway を使用していて、アクティベーション コードによるオンボーディングが MRA に対して有効にされている場合のみです。

クライアント証明書のテスト

ここでは、**「クライアント証明書テスト（Client certificate testing）」**ページ（**[メンテナンス（Maintenance）]**>**[セキュリティ（Security）]**> **[クライアント証明書テスト（Client certificate testing）]**）を使用して、クライアント証明書を確認してから、[クライアント証明書の検証（client certificate validation）] を有効にします。方法は以下のとおりです。

- Expressway の現在の信頼できる CA リストおよびロードされている場合は失効リスト（証明書失効リスト（CRL）の管理）を参照）と照合して確認し、クライアント証明書が有効であるかどうかをテストします。
- 証明書の許可クレデンシャル（ユーザ名）を取得する正規表現とテンプレート パターンを適用した結果をテストします。

ローカルファイルシステムまたはブラウザで現在ロードされている証明書について、証明書とテストできます。

証明書が有効かどうかをテストするには

手順

ステップ 1 [証明書の送信元（Certificate source）] を選択します。次のいずれかを選択できます。

- PEM またはプレーン テキストのいずれかの形式のファイル システムからテスト ファイルをアップロードする（この場合は、**[参照（Browse）]** をクリックしてテストする証明書ファイルを選択します）。
- 現在ブラウザにロードされている証明書と照合してテストする（システムが *[*証明書の検証（*Certificate validation*）*]* を使用するようにすでに設定されていて、現在、証明書がロードされている場合にのみ使用できます）。

ステップ 2 **[証明書ベースの認証パターン（Certificate-based authentication pattern）]** セクションを無視します。このセクションは許可クレデンシャルを証明書から抽出する場合にのみ使用します。

ステップ 3 [証明書の確認（Check certificate）] をクリックします。
テストの結果が **[証明書のテスト結果（Certificate test results）]** セクションに表示されます。

証明書から許可クレデンシャル（ユーザ名）を取得するには

手順

ステップ 1 **[証明書の送信元（Certificate source）]** を上記で説明したように選択します。

ステップ 2 **[正規表現（Regex）]** フィールドと [ユーザ名の形式（Username format）] フィールドを必要に応じて設定します。これは、証明書内で該当する文字列パターンを検索する正規表現を指定することで、指定した証明書からユーザ名を抽出することを目的としています。現在、これらのフィールドはデフォルトで「**証明書ベースの認証設定（Certificate-based authentication configuration）**」ページの設定になるように設定されていますが、必要に応じて変更できます。

- **[正規表現（Regex）]** フィールドに（**?<name>regex**）シンタックスを使用してキャプチャグループ用の名前を指定し、関連付けられた **[ユーザ名の形式（Username format）]** フィールドで一致サブパターンを置換できるようにします。次に例を示します。

  /(Subject:.*, CN=(?<Group1>.*))/m.

  ここで定義する正規表現は、PHP 正規表現のガイドラインに準拠する必要があります。

- **[ユーザ名の形式（Username format）]** フィールドには、固定テキストと **[正規表現（Regex）]** で使用したキャプチャ グループの名前を組み合わせて含めることができます。各キャプチャ グループ名を#で区切ります。例：**prefix#Group1#suffix** 各キャプチャ グループ名は正規表現の処理から取得されたテキストに置き換えられます。

ステップ 3 [証明書の確認（Check certificate）] をクリックします。
テストの結果が **[証明書のテスト結果（Certificate test results）]** セクションに表示されます。**[結果の文字列（Resulting string）]** の項目はユーザ名クレデンシャルであり、関連する許可メカニズムと照合して確認され、ユーザの許可（アカウント アクセス）レベルが決定します。

ステップ 4 必要に応じて **[正規表現（Regex）]** フィールドと **[ユーザ名の形式（Username format）]** フィールドを変更し、正しい結果が得られるまでテストを繰り返すことができます。

（注） **[証明書の送信元（Certificate source）]** がアップロードされた PEM またはプレーン テキスト ファイルの場合は、テストを初めて実行したときに選択したファイルが一時的に Expressway へアップロードされます。

- 同じファイルに対して **[正規表現（Regex）]** と **[ユーザ名の形式（Username format）]** をさまざまに組み合わせてテストを続ける場合は、テストごとにファイルを再選択する必要はありません。
- ファイルシステムのテストファイルの内容を変更する、または別のファイルを選択する場合は、**[参照（Browse）]** を再度選択して、新しいファイルまたは変更したファイルを選択してアップロードします。

ステップ 5 [正規表現（Regex）] フィールドと [ユーザ名の形式（Username format）] フィールドをデフォルト値から変更して Expressway の実際の設定の値（[証明書ベースの認証設定（Certificate-based authentication configuration）] ページで指定）を使用した場合、[これらの設定を永続的にする（Make these settings permanent）] をクリックします。

（注）
- アップロードしたテスト ファイルは、ログイン セッションの終了時点で Expressway から自動的に削除されます。
- 正規表現は符号化された証明書のプレーンテキストバージョンに適用されます。システムは **openssl x509 -text -nameopt RFC2253 -noout** コマンドを使用して、符号化された形式からプレーン テキストの証明書を抽出します。

セキュア トラバーサルのテスト

このユーティリティは、Expressway-C と Expressway-E の間でセキュアな接続を確立できるかどうかをテストします。セキュアな接続は、ユニファイドコミュニケーションのトラバーサル ゾーンでは必須ですが、通常のトラバーサル ゾーンでは任意（推奨）です。

セキュア トラバーサルのテストが失敗した場合、可能な場合はこのユーティリティによって適切な解決策を示した警告が発行されます。

手順

ステップ 1 **Expressway-C で [メンテナンス（Maintenance）] > [セキュリティ（Security）] > [セキュア トラバーサルのテスト（Secure traversal test）]** に移動します。

ステップ 2 この Expressway-C とペアにする Expressway-E の FQDN を入力します。

ステップ 3 ペアの Expressway-E に表示されるとおりに、この Expressway-C の TLS 確認名を入力します。

この設定は、Expressway-E のトラバーサルゾーンの設定ページの SIP セクションにあります。

ステップ 4 [テスト接続（Test connection）] をクリックします。

セキュア トラバーサルのテスト ユーティリティは、トラバーサル ゾーンの両側のホストが互いに認識し合い、もう一方の証明書チェーンを信頼しているかどうかを確認します。

（注） Expressway でサポートされている最小 TLS バージョンを有効にするセキュアな接続の適切性をテストするには、**HTTPS 最小 TLS バージョン**を選択する必要があります。また 、**HTTPS 暗号**を同じ目的で選択します。この *HTTPTLSversion* の選択は 、VCSE、CUCM、CUP、UCXN などの Unified Communication サーバとの接続確立に必要です。これらの設定は、**[暗号（Ciphers）]**ページ（**[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[暗号（Ciphers）]** で設定されます。

HSM を使用した Expressway のサーバ証明書の管理

重要 ExpresswayでのHSM機能のサポートは、Expressway ソフトウェアのバージョンによっては、**プレビュー機能のみ**になる場合があります。たとえば、バージョン X12.6 のプレビュー機能です。HSM を使用する前に Expressway バージョンのリリースノートを確認し、そのステータスがソフトウェアバージョンのプレビューである場合は、**プレビュー機能として実装する意思があり、Expressway リリースノートに含まれるプレビューの免責事項に従う場合にのみ、HSM を有効にしてください。**現時点で、この機能を構成および有効にする手順は、Expressway リリースノートに記載されています。

これらの手順は、HSM が Expressway ですでに有効になっていることを前提としています（**[メインテナンス（Maintenance）] > [セキュリティ（security）] > [HSM 設定（HSM configuration）]**）。

手順

ステップ 1 **[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[サーバ証明書（Server certificate）]** に移動します。

ステップ 2 [CSR の作成（Generate CSR）] をクリックします。**[CSR の生成（Generate CSR）]** ページに移動します。

[サーバ証明書の種類（Server certificate type）] の項は **[CSR 生成（Generate CSR）]** ページの上部に表示されます。HSM の使用法が構成されていない場合、この項は表示されません。

Expressway クラスタがある場合は、CSR フィールドが誤って完了した場合に問題が発生する可能性があります。これらのフィールドを入力する方法の詳細については、「*Cisco Expressway* シリーズ設定ガイド」ページの「Cisco Expressway クラスタの作成とメンテナンスの導入ガイド」を参照 してください。

ステップ 3 HSM 秘密キーと CSR として生成した後、**サーバ証明書**ページに戻ります。

ステップ 4 **証明書署名要求（CSR）**の項から、生成された HSM CSR を表示およびダウンロードできます。

ステップ 5 **[ダウンロード（Download）]** をクリックして、証明書をダウンロードします。

ステップ 6 証明書署名機関を使用して証明書に署名します。

プライベートキーと証明書のインストール

（注） ハードウェアセキュリティモジュール（HSM）機能を使用する場合にのみ、次の手順を使用します。

手順

ステップ 1 署名付き証明書をアップロードするには、**[ファイルの選択（Choose File）]** をクリックして場所に移動し、証明書を選択します。

ステップ 2 証明書ファイルと対応する証明書タイプを選択し、**[サーバ証明書データのアップロード（Upload server certificate）]** をクリック して証明書をアップロードします。

詳細については、Expressway のサーバ証明書の管理に関するセクションを参照してください。

クラスター全体で HSM キー ハンドルをダウンロードする

HSM 証明書と秘密きーを Expressway に展開した後、HSM 証明書と秘密キーをクラスタ内の他の Expressway に展開できます。手順は、次のとおりです。

手順

ステップ 1 プライマリピア。1 つ目の Expressway から、この 2 つのキーをダウンロードします。**[サーバ証明書データ（Server certificate data）]** セクションに、オプションの証明書とプライベートキーを導入した後、**[HSM キーハンドルのダウンロード（Download HSM key handle）]** ボタンが表示されます。

ステップ 2 クラスタピア上。**[新しい証明書のアップロード（Upload new certificate）]** セクションから、HSM 証明書を含む HSM 秘密キーをクラスター内の他のピアにアップロードします。署名付き HSM 証明書とプライベートキーを参照して選択します。

Expressway を再起動

HSM 証明書が Expressway にインストールされた後、**サーバー証明書**ページのバナーにより、Expressway を再起動するように求められます。アラームも発生して再起動します。証明書がインストールされているが、Expressway が証明書を使用し始めるには再起動が必要です。

再起動後、アラームは消え、Expressway上のすべてのサービスが新しい HSM 証明書を使用します。

ハードウェアセキュリティモジュールの機能設定

HSM 設定ページ（**[メンテナンス（Maintenance）]** > **[セキュリティ（Security）]** > **[HSM 設定（HSM configuration）]**）は、Expressway を使用する場合に、そのデバイスを管理するために使用します。

重要 HSM 機能は、Expressway ソフトウェアバージョンに応じて、**プレビュー機能のみ**使用できます。たとえば、バージョン X12.6 のプレビュー機能です。HSM を使用する前に、Expressway バージョンのリリースノートを確認してください。ソフトウェアバージョンのステータスがプレビューである場合は、プレビュー機能として実装する場合にのみ HSM を有効にしてください。現時点で、このセクションでは、Expressway リリースノートに記載されているのではなく、その方法について説明しています。

最小限 TLS バージョンと暗号スイートの設定

[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [暗号（Ciphers）] ページは、Expressway 上のサービスの最小 TLS バージョンと、関連する暗号スイートを管理するために使用されます。

（注） セキュリティを強化するため、すべての暗号化セッションに TLS のバージョン 1.2 以降を推奨します。

以下のセキュアな接続を確立する場合、Expressway はデフォルトで TLS 1.2 に設定されます。

- HTTPS
- 証明書のチェック機能
- Cisco Meeting Server の検出
- SIP
- XMPP
- UC サーバ ディスカバリ
- リバース プロキシ
- LDAP
- [SMTP メールサーバ]
- TMS プロビジョニングサービス

場合によっては、再起動が必要です。

暗号スイートの設定または TLS プロトコルのバージョンを次のバージョンに変更した後、再起動する必要があります。

- SIP
- XCP

最小TLSバージョン

既存のシステムのアップグレードでは、以前の動作とデフォルトが維持され、デフォルトは TLS 1.2 に設定されません。

新しいインストールの場合は、Expressway に接続する必要があるすべてのブラウザおよび他の機器が TLS 1.2 をサポートしています。

必要に応じて（通常は旧式の機器との互換性のため）、サービスごとに最小 TLS バージョンはバージョン 1.0 または 1.1 を使用するように構成できます。

暗号スイート

Expressway のサービスに暗号スイートとサポートされる最小 TLS バージョンを設定できます。暗号スイートを表に示します（暗号文字列は OpenSSL 形式です）。

Expressway がクライアント（HTTPS など）として動作できるサービスの場合、同じ最小 TLS バージョンと暗号スイートがネゴシエートされます。

サービス	暗号スイートの値（デフォルト）
HTTPS 暗号方式	EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL
リバース プロキシの TLS 暗号方式	EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL
SIP TLS 暗号方式	EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:+ADH
UC サーバ ディスカバリの TLS 暗号方式	EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL
XMPP TLS 暗号方式	EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL
LDAP TLS 暗号方式	EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL
TMS TLS 暗号方式	EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL
SMTP 暗号	EECDH:EDH:HIGH:- AES256+SHA:!MEDIUM:!LOW:!3DES:!MD5:!PSK:!eNULL:!aNULL

SIP 動作 - ADH 勧告を無効にする

E20 など、一部のエンドポイントは、接続するときに匿名 Diffie-Hellman（ADH）のみをサポートし、ADH はデフォルトの暗号スイートで有効になっています。ただし、インバウンド接続の場合は、セキュリティ上の理由から、`!ADH` を追加して常に無効にする必要があります

SIP から ADH を削除すると、一部のレガシーエンドポイントへの発信接続が失敗することに注意してください。

SSH の設定

トンネルの設定

Expressway ペアでは SSH トンネルを使用して Expressway-E から Expressway-C にセキュアにデータを転送します。Expressway-E が接続を開く必要はありません。Expressway-C は、固定 TCP ポートでリッスンしている Expressway-E との TCP セッションを開始します。セッション開始後、Expresswayペアは選択済みの暗号方式とアルゴリズムを使用して、データをセキュアに共有するために暗号化されたトンネルを確立します。

ペアが SSH トンネルの暗号化に使用する暗号とアルゴリズムは次のように構成されています。

1. **[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [SSH 接続（SSH configuration）]** に移動します。
2. 必要に応じて、次の設定を変更します。

設定	説明
暗号	*aes256 ctr*：CTR（カウンタ）モードを使用して 256 ビットのブロックを暗号化する Advanced Encryption Standard。（デフォルト）
公開キー アルゴリズム	*X509v3-sign-rsa*（デフォルト） *X509v3*、*ssh*、*rsa*
キー交換アルゴリズム	*ecdh-sha2-nistp256* *nistp384 sha2 ecdh*（デフォルト)

3. [保存（Save）] をクリックします。

Remote Access Configuration

ペアが SSH クライアントとサーバー間のリモートアクセスを暗号化するために使用する暗号とアルゴリズムは、次のように構成されています。

1. **[メンテナンス（Maintenance）] > [セキュリティ（Security）] > [SSH 接続（SSH configuration）]** に移動します。
2. 必要に応じて、次の設定を変更します。

設定	説明
暗号	*“aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr”*
キー交換アルゴリズム	*“ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group14-sha1”*
MAC アルゴリズム	*“hmac-sha2-512,hmac-sha2-256,hmac-sha1”*

3. [保存（Save）] をクリックします。

高度なセキュリティ

「高度なセキュリティ（Advanced Security）」ページ（**[メンテナンス（Maintenance）] > [高度なセキュリティ（Advanced security）]**）を使用して、極めてセキュアな環境で使用するように Expressway を設定します。このページを表示するには、**[高度のアカウント セキュリティ（Advanced Account Security）]** オプション キーをインストールする必要があります。

システムを次のように設定できます。

- 高度なアカウント セキュリティ モードの設定
- FIPS140-2 暗号化モードの設定

高度なアカウント セキュリティ モードの設定

高度なアカウント セキュリティを有効にすると、Web インターフェイスを使用してリモートから認証されたユーザのみにログインアクセスが限定され、一部のシステム機能へのアクセスも制限されます。Expressway が高度なアカウント セキュリティ モードになっていることを示すために、**[分類バナー（Classification banner）]** メッセージとして指定したテキストがすべての Web ページに表示されます。

高度なアカウント セキュリティ モードへの変更を有効にするには、システムをリブートする必要があります。

HTTP メソッド

Expressway の Web サーバでは、次の HTTP メソッドが許可されています。

方法	Web UI での使用	API での使用	用途
GET	はい	はい	指定したリソースからデータを取得します。たとえば、Expressway の Web インターフェイスの特定のページを返します。
POST	はい	はい	Web リソースにデータを適用します。たとえば、管理者が Expressway の Web インターフェイスを使用して、設定の変更を保存する場合などです。

方法	Web UI での使用	API での使用	用途
オプション	いいえ	はい	指定した URL に対し、サーバでサポートされている HTTP メソッドを返します。たとえば、Expressway は OPTIONS を使用して HTTP/1.1 コンプライアンス用にプロキシ サーバをテストできます。
PUT	いいえ	はい	指定した URI に保存するリソースを送信します。REST API コマンドはこのメソッドを使用して、Expressway 設定を変更します。
DELETE	いいえ	はい	指定したリソースを削除します。たとえば、REST API はレコードの削除に DELETE を使用します。

API へのユーザ アクセスを無効にする方法

管理者はデフォルトで API にアクセスできます。これは、次の 2 つの方法で無効化できます。

- Expressway が高度なアカウント セキュリティ モードで動作している場合、API アクセスはすべてのユーザで自動的に無効になります。
- 個別の管理者の API アクセスは、ユーザ設定オプションを使用して無効にできます。

前提条件

高度なアカウント セキュリティ モードを有効にするには、次の項目が必須です。

- 管理者アカウントにリモート アカウント認証を使用するようにシステムを設定する必要があります。
- **高度なアカウント セキュリティ**のオプション キーをインストールする必要があります。
- リモート認証が利用できない場合にアクセスできるように、ローカル管理者アカウントを作成し、緊急アカウントとして指定する必要があります。この目的にリモート アカウントを使用することはできません。

  組み込み *admin* アカウントを使用しないでください。

⚠

注意 Expressway は、緊急アカウントを除いたすべてのアカウントでローカル認証を許可していません。モードを有効にする前に、リモート ディレクトリ サービスが正常に機能していることを確認します。

また、以下のようにシステムを設定することを推奨します。

- SNMP を無効にする。

- セッション タイムアウト期間をゼロ以外の値に設定する。
- HTTPS クライアント証明書の検証を有効にする。
- ユーザ アカウントの LDAP サーバの設定では TLS 暗号化を使用し、証明書失効リスト（CRL）を [すべて（All）] に設定する。
- リモート ロギングを無効にする。
- インシデント レポートを無効にする。
- 接続を外部マネージャに対して行う場合は、HTTPS を使用し、証明書の確認を有効にする。

推奨されていない設定にはアラームが発行されます。

高度なアカウント セキュリティの有効化

高度なアカウント セキュリティを有効にするには、次の手順を実行します。

手順

ステップ 1 **[メンテナンス（Maintenance）]** > **[高度なセキュリティ（Advanced security）]** に移動します。

ステップ 2 [分類バナー（Classification banner）] に入力します。

ここで入力したテキストがすべての Web ページに表示されます。

ステップ 3 **[高度なアカウント セキュリティ モード（Advanced Account Security）]** を *[オン（On）]* に設定します。

ステップ 4 **[保存（Save）]** をクリックします。

ステップ 5 Expressway 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）]**）。

Expressway 機能：変更と制限

セキュア モードのとき、標準的な Expressway 機能に対して次の変更と制限が適用されます。

- SSH を使用したシリアル ポートを通じたアクセスが無効になり、オンにできない（pwrec パスワード リカバリ機能も使用できなくなる）。
- HTTPS を使用したアクセスが有効になり、オフにできない。
- コマンドライン インターフェイス（CLI）と API アクセスが使用できない。
- 管理者アカウントの認証ソースが [リモートのみ（Remote Only）] に設定され、変更できない。
- ローカル認証が無効になる。緊急アカウントを除いて、root アカウントまたはローカル管理者アカウントではアクセスできない。

- 緊急アカウントのみが緊急アカウントを変更できる。
- 証明書ベースの認証を使用している場合は、緊急アカウントをクライアントの証明書のクレデンシャルで認証する必要がある。緊急アカウントと証明書ベースの認証を参照してください。
- 同じユーザまたは異なるユーザによるログイン試行が3回連続で失敗した場合にExpresswayのログイン アクセスを 60 秒間ブロックする。
- ログイン直後に現在のユーザに以前ログインした日時とそのアカウントを使用してログインに失敗した試行の詳細を表示します。
- 読み取り専用または読み取り/書き込みのアクセス レベルを持つ管理者アカウントは、[イベント ログ（Event Log）]、[設定ログ（Configuration Log）]、[ネットワーク ログ（Network Log）] ページを表示できない。これらのページを表示できるのは、監査役のアクセス レベルを持つアカウントのみである。
- 「**アップグレード（Upgrade）**」ページに**システム プラットフォーム**コンポーネントのみが表示される。

Expressway が高度なアカウント セキュリティ モードから実行されるたびに、イベント ログ、設定ログ、ネットワーク ログ、通話履歴、検索履歴、登録履歴がクリアされます。

（注） 侵入からの保護を有効にすると、ブロックされている既存のアドレスのブロックが解除された状態になります。

高度なアカウント セキュリティの無効化

（注） この操作によりすべての設定が消去されます。このモードを終了した場合、設定または履歴を維持することはできません。システムは出荷時の状態に戻ります。

手順

ステップ 1 緊急アカウントでログインします。

ステップ 2 高度なアカウント セキュリティ モードを無効にします（**[メンテナンス（Maintenance）]** > **[高度なセキュリティ（Advanced security）]**）。

ステップ 3 サインアウトします。

ステップ 4 コンソールに接続します。

ステップ 5 **root** としてサインインし、**factory-reset** を実行します。

詳細については、「デフォルト設定の復元（工場出荷時にリセットされた状態」を参照してください。

FIPS140-2 暗号化モードの設定

FIPS140 は暗号モジュールのセキュリティ要件を指定する米国およびカナダ政府の標準規格です。FIPS140-1 は 1994 年に機密データ保護のための必須の標準規格になり、2001 年に FIPS140-2 に取って代わられました。Expressway X8.8 以降には、FIPS140-2 対応機能が実装されています。

FIPS140-2 の暗号化モードの場合、暗号化のワークロードの増加によりシステム パフォーマンスが影響を受ける可能性があります。

FIPS140-2 モードが有効化された Expressway をクラスタ化できます。

前提条件

FIPS140-2 モードを有効にする前に、次のことを実行します。

- デバイスの認証にシステムが NTLM プロトコル チャレンジと Active Directory サービスの直接接続を使用していないことを確認する。NTLM は FIPS140-2 モードのときは使用できません。
- リモート LDAP サーバを経由したログイン認証が設定されている場合、SASL バインドを使用しているときは TLS 暗号化を使用することを確認する。
- **高度なアカウント セキュリティ**のオプション キーをインストールする必要があります。

FIPS140-2 のコンプライアンスには次の制限事項も必要です。

- システム全体の SIP トランスポート モードの設定で、[TLS] は *[オン（On）]*、[TCP] は *[オフ（Off）]*、[UDP] は *[オフ（Off）]* に設定する必要があります。
- すべての SIP ゾーンが TLS を使用する必要があります。
- SNMP と NTP のサーバ接続には、強力なハッシュと暗号化を使用する必要があります。次の設定を使用します。

  System > SNMP > v3 Authentication > Type = *SHA*

  System > SNMP > v3 Privacy > Type = *AES*

  System > Time > NTP server *n* > Authentication= 対称 キーです。

  System > Time > NTP server *n* > Hash= *SHA-1*

システムが仮想化アプリケーションとして実行され、アップグレードプロセスを実行しきったことない場合は、続行する前にシステムアップグレードを実行します。現在実行しているものと同じソフトウェア リリースのバージョンにシステムをアップグレードできます。この手順を実行しないと、以下で説明するアクティベーション プロセスが失敗します。

FIPS 140-2 暗号化モードの有効化

注意 FIPS 140-2 暗号モードへの移行には、システムのリセットを実行する必要があります。これにより、既存のすべての設定データが削除されます。データを保持するには、リセットを実行する直前にバックアップを実行し、リセットが完了した時点でバックアップ ファイルを復元します。

リセットによりすべての管理者アカウント情報が削除され、デフォルトのセキュリティ証明書が元の状態に戻ります。リセット完了後にログインするには、最初にインストール ウィザードを完了する必要があります。

システムを FIPS 140-2 暗号対応システムに変えるには、次の手順を実行します。

手順

ステップ 1 FIPS 140-2 暗号化モードの有効化

1. **[メンテナンス（Maintenance）] > [高度なセキュリティ（Advanced security）]** に移動します。
2. **[FIPS-2 暗号化モード（FIPS140-2 cryptographic mode）]**を *[オン（On）]* に設定します。
3. **[保存（Save）]** をクリックします。

ステップ 2 準拠していない設定を報告するために発生したアラームを修正します。

（注） モバイルおよびリモートアクセスのシナリオで FIPS を有効にすると、アラームが #40042 場合（一部の SIP 設定は TLS トランスポートを使用しません。FIPS 140-2 コンプライアンスではTLSが要求されます）、この機能を無効にして有効にしてアラームをクリアできます。

ステップ 3 現在の設定データを維持する場合は、システム バックアップを実行します。

（注） すべてのバックアップをパスワードで保護する必要があることに注意してください。

ステップ 4 システムをリセットし、FIPS140-2 モードのアクティベーションを実行します。

1. **root** として Expressway にログインします。
2. **`fips-activate`** と入力します。

このリセットは、完了するまでに最大 30 分かかります。

ステップ 5 指示に従ってインストール ウィザードを完了します。

ステップ 6 設定が適用されてシステムが再起動したら、設定したパスワードを使用して **`admin`** としてログインします。

FIPS 140-2 のコンプライアンス違反に関連するアラームが表示される場合があります。リセット前に実行したバックアップを復元する場合は、これらのアラームは無視します。バックアップを復元してもアラームが続く場合は対処する必要があります。

ステップ 7 必要に応じて、以前のデータを復元します。

（注） FIPS 140-2 モードでは 、**FIPS 140-2 暗号モード**が *[*オン（*On*）*]* に設定されている場合に撮影されたバックアップファイルのみ復元できます。以前の管理者アカウント情報とパスワードは復元されますが、以前の **root** アカウントのパスワードは復元されません。復元するデータに信頼できないセキュリティ証明書が含まれている場合は、復元プロセスの一環として行われるリスタートが完了するまでに最大6分かかる場合があります。

ステップ 8 X12.6 から、SIP TLS Diffie-Hellman キーサイズをデフォルトの 1024 ビットから少なくとも 2048 に手動で変更する必要があります。この操作を行うには、Expressway コマンドラインインターフェイスで次のコマンドを入力します（キー サイズが 2048 を超える場合は、最終的な要素の値を変更します）：*xconfiguration SIP Advanced SipTlsDhKeySize: "2048"*

FIPS140-2 対応機能

次の Expressway 機能は FIPS140-2 に対応しているか、または FIPS140-2 対応アルゴリズムを使用します。

- Web インターフェイスを使用した管理
- クラスタリング
- XML と REST API
- SSH アクセス（AES または 3DES 暗号のみの使用に限定）
- リモート LDAP サーバを介してのログイン認証（SASL バインドを使用している場合は TLS を使用すること）
- クライアント証明書の確認
- SIP 証明書の失効機能
- SNMP（SNMPv3 認証は SHA1 のみに、SNMPv3 プライバシーは AES のみに限定）
- NTP（対称キーを使用した NTP サーバ認証は SHA1 のみに限定）
- ローカル データベースと照合してのデバイス認証
- TLS を使用している場合の Expressway への、または Expressway からの SIP 接続
- Expressway への、または Expressway からの H.323 接続
- 委任クレデンシャル チェック
- SRTP メディア暗号化

- SIP/H.323 インターワーキング
- ユニファイド コミュニケーションの Mobile & Remote Access（MRA）
- TURN サーバ認証
- バックアップ/復元操作
- 外部マネージャへの接続
- 外部ポリシー サービスへの接続
- リモート ロギング
- インシデント レポート
- CSR の生成

その他の Expressway 機能は次を含めて FIPS140-2 に対応していません。

- NTLM/Active Directory による SIP 認証
- H.350 ディレクトリ サービスと照合する SIP/H.323 デバイス認証
- Microsoft 相互運用性サービス
- Cisco TMSPE の使用