



ネットワークとシステムの設定

ここでは、Web インターフェイスの [システム (System)]メニューに表示されるネットワークサービスと設定に関連するオプションについて説明します。これらのオプションによって、IP 設定、ファイアウォールルール、侵入からの保護、Expressway が使用する外部サービス (DNS、NTP、SNMP など) といった、Expressway が存在するネットワークに関連する設定を行うことができます。

- [ネットワーク設定 \(1 ページ\)](#)
- [侵入からの保護 \(13 ページ\)](#)
- [ネットワーク サービス \(25 ページ\)](#)
- [外部マネージャ設定値の設定 \(42 ページ\)](#)
- [専用管理インターフェイス \(DMI\) の設定 \(43 ページ\)](#)
- [TMS プロビジョニング拡張サービスの設定 \(46 ページ\)](#)

ネットワーク設定

ここでは、Web インターフェイスの [システム (System)]メニューに表示されるネットワークサービスと設定に関連するオプションについて説明します。これらのオプションによって、IP 設定、ファイアウォールルール、侵入からの保護、Expressway が使用する外部サービス (DNS、NTP、SNMP など) といった、Expressway が存在するネットワークに関連する設定を行うことができます。

イーサネット設定



- (注) このページで設定する速度は、Cisco Expressway 物理アプライアンス上で稼働するシステムにのみ適用されます。仮想マシン (VM) ベースのシステムには適用されません。VM システムに対して示される接続速度は無効であり、基礎となる物理 NIC の実際の速度とは関係なく常に 10000 Mb/s として表示されます。これは、VM では物理 NIC から実際の速度を取得できないためです。

「イーサネット (Ethernet)」ページ ([システム (System)]>[ネットワークインターフェイス (Network interfaces)]>[イーサネット (Ethernet)]) には、Expressway とその接続先イーサネットネットワークとの間の接続速度が表示されます。Expressway では自動ネゴシエーションのみがサポートされるため、[速度 (Speed)] は常に [自動 (Auto)] に設定されます。Expressway とこれに接続されているスイッチは、接続の速度とデュプレックスモードを自動的にネゴシエートします。

IP の設定

「IP」ページ ([システム (System)]>[ネットワークインターフェイス (Network interfaces)]>[IP]) を使用して、Expressway の IP プロトコルとネットワークインターフェイスの設定を行います。

IP プロトコルの設定

Expressway が IPv4 と IPv6 のどちらを使用するか、あるいは IP プロトコルスイートの両方のバージョンを使用するかを設定できます。デフォルトは [両方 (Both)] です。

- **[IPv4 のみ (IPv4 only)]** : IPv4 アドレスを使用したエンドポイントからの登録のみを許可し、IPv4 で通信する 2 つのエンドポイント間のコールのみを受け入れます。IPv4 でのみ他のシステムと通信します。
- **[IPv6 のみ (IPv6 only)]** : IPv6 アドレスを使用したエンドポイントからの登録のみを許可し、IPv6 で通信する 2 つのエンドポイント間のコールのみを受け入れます。IPv6 でのみ他のシステムと通信します。
- **[両方 (Both)]** : IPv4 または IPv6 のいずれかのアドレスを使用したエンドポイントからの登録を許可し、どちらのプロトコルを使用したコールでも受け入れます。IPv4 のみのエンドポイントと IPv6 のみのエンドポイント間のコールの場合は、Expressway が IPv4 から IPv6 へのゲートウェイとして機能します。他のシステムとはいずれかのプロトコルで通信します。

一部のエンドポイントは IPv4 と IPv6 の両方をサポートしますが、Expressway に登録するときにエンドポイントが使用できるプロトコルは 1 つのみです。エンドポイントに Expressway の IP アドレスを指定するために使用した形式によって、どちらのプロトコルを使用するかが決定します。IPv4 または IPv6 のいずれかを使用してエンドポイントを登録すると、Expressway はこのアドレッシングスキームを使用してコールのみを送信します。別のアドレッシングスキームを使用した別のデバイスからのそのエンドポイントへのコールは Expressway によって変換されます (ゲートウェイ機能)。

Expressway で設定されたすべての IPv6 アドレスは、/64 ネットワークプレフィックス長があるものとして処理されます。

IPv4 と IPv6 のインターワーキング

Expressway は IPv4 デバイスと IPv6 デバイス間のコールのゲートウェイとして機能します。この機能を有効にするには、**[IP プロトコル (IP protocol)]** に **[両方 (Both)]** を選択します。

Expressway が IPv4 から IPv6 へのゲートウェイとして機能するコールはトラバーサル コールであるため、リッチメディアセッションライセンスが必要です。

IP ゲートウェイ

Expressway が使用するデフォルトの **[IPv4 ゲートウェイ (IPv4 gateway)]** と **[IPv6 ゲートウェイ (IPv6 gateway)]** を設定できます。これらは、Expressway のローカルサブネットの範囲内にはない IP アドレスに対して IP 要求を送信するゲートウェイです。

- デフォルトの **[IPv4 ゲートウェイ (IPv4 gateway)]** は 127.0.0.1 です。デフォルトを変更する場合は、コミッションプロセス時に変更する必要があります。
- 入力されている場合、**[IPv6 ゲートウェイ (IPv6 gateway)]** はスタティック グローバル IPv6 アドレスである必要があります。リンクローカルまたはステートレス自動設定 (SLAAC) IPv6 アドレスを指定することはできません。

LAN の設定

Expressway のプライマリ ネットワーク ポートは LAN 1 です。このポートに **[IPv4 アドレス (IPv4 address)]** と **[サブネットマスク (subnet mask)]**、**[IPv6 アドレス (IPv6 address)]** と **[最大転送単位 (MTU) (Maximum transmission unit (MTU))]** を設定できます。Expressway は、両方の LAN ポートにデフォルトの IP アドレス 192.168.0.100 が設定された状態で出荷されます。これにより、Expressway をネットワークに接続し、デフォルトのアドレスを使用してアクセスすることで、リモートから設定できます。

入力されている場合、**[IPv6 アドレス (IPv6 address)]** はスタティック グローバル IPv6 アドレスである必要があります。リンクローカルまたはステートレス自動設定 (SLAAC) アドレスを指定することはできません。

デフォルトでは、**[最大転送単位 (MTU) (Maximum transmission unit (MTU))]** は 1,500 バイトに設定されます。

高度なネットワーキングが有効になっている場合は、LAN 2 ポートに対してもこれらのオプションを設定できます。

専用管理インターフェイス

Expressway の DMI を有効にする場合は、次の方法を実行します。

手順

ステップ 1 **[専用管理インターフェイスの使用 (Use Dedicated Management Interface)]** を **[はい (Yes)]** に設定します。

ステップ 2 **[LAN3 - DMI]** セクションで、次を実行します。

1. LAN3 ポートの IPv4 アドレスまたは IPv6 アドレスを指定します。
2. IPv4 では、サブネットマスクも指定します。

3. IPv6の場合は、静的なグローバルアドレスを使用します。リンクローカルまたはステータスの SLAAC は使用できません。
4. 必要に応じて、ポートの**最大伝送ユニット (MTU)** を設定することで、DMI 経由で送信できるイーサネットパケットの最大サイズを変更します。デフォルト値は 1500 バイトです。

ステップ3 システムを再起動します。これらの変更を有効にするには、再起動が必要です。

これで、DMIが管理トラフィック用のインターフェイスとしてLAN3でアクティブ化されました。DMIを管理用の唯一のインターフェイスとして使用する場合は、次のタスクに進みます。

次のタスク

DMI 単独のインターフェイス作成

DMI 単独のインターフェイス作成

(オプション) DMI を唯一のインターフェイスにする - サーバ管理トラフィック

Expressway がサーバである場合に、このタスクを使用して、管理トラフィックに DMIを使用します。

1. これは、管理サービス (Web ユーザインターフェイス、REST API、CLI) または SNMP に対して実行できます。DMI 専用を設定するサービスに応じて、次の手順のいずれかまたは両方を実行します。
 - [システム (System)] > [SNMP] ページに進み、[設定 (Configuration)] セクションで、[専用管理インターフェイスのみを使用する (Use Dedicated Management Interface)] を [はい (Yes)] に設定します。
 - [システム (System)] > [管理設定 (Administration settings)] に進み、[サービス (Services)] セクションで、[管理インターフェイスのみを使用する (管理用) (Use Dedicated Management Interface only (for administration))] を [はい (Yes)] に設定します。
2. 変更を Web ユーザインターフェイスと API に適用するにはシステムを再起動する必要があります。再起動するまで LAN1/LAN2 からアクセスできる状態が維持されます。変更は、再起動に関係なく、コマンドラインインターフェイス (SSH) および SNMP サービスに対して即時に有効になります。

指定された管理サービスに、DMI/LAN3 ポートからのみアクセスできるようになりました。



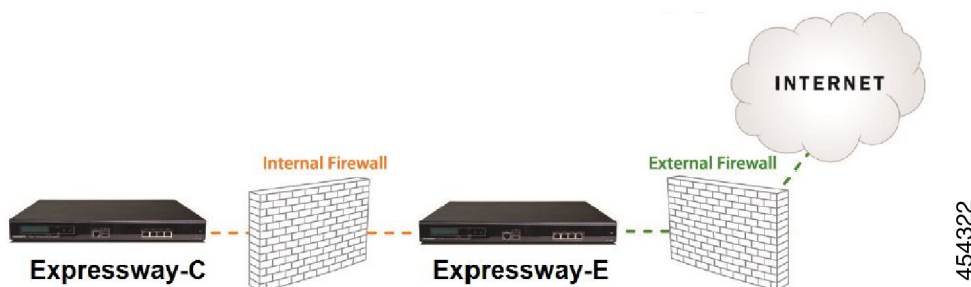
(注) Expressway では、管理サービスが DMI を唯一のインターフェイスとして使用するよう設定されている間は、この DMI を無効にすることはできません。

(オプション) DMI を唯一のインターフェイスにする - サブネット外のクライアント管理トラフィック

Expressway ソフトウェアのバージョンに応じて、Expressway がクライアントとして動作する管理トラフィックでは、ターゲットサーバが DMI/LAN3 ポートと同じサブネット内にある場合にのみ、トラフィックを DMI に送信できます。リリースノートをチェックして、この問題が適用されるのか確認してください。適用される場合、LAN3 と同じサブネットにサーバを導入できない場合は、オプションで、サービスごとに LAN3 用のスタティック IP ルートを設定することで、Expressway 管理トラフィックに DMI の使用を強制できます。

高度なネットワーキングおよびデュアルネットワークインターフェイスについて

高度なネットワーキング機能を使用すると、Expressway-E の LAN 2 イーサネットポートを有効にして、Expressway のセカンダリ IP アドレスを取得できます。この機能には Expressway-E がスタティック NAT デバイスの背後にある導入環境に対するサポートも含まれているため、個別のパブリック IP アドレスとプライベート IP アドレスを取得できます。



デュアルネットワーク インターフェイスの設定

デュアルネットワークインターフェイスは、Expressway-E システムでのみサポートされています。Expressway-C では展開できません。

デュアルネットワークインターフェイスは、Expressway-E が個別のネットワークセグメント上にある 2 つの個別ファイアウォール間の DMZ に存在する導入環境用のインターフェイスです。このような導入環境では、ルータが内部ネットワーク上のデバイスが IP トラフィックをパブリックインターネットにルーティングできないようにしますが、その代わりに、トラフィックは Expressway-E などのアプリケーションプロキシを通過する必要があります。

デュアルネットワークインターフェイスを有効にするには

始める前に

- LAN 1 ポートを設定し、Expressway を再起動してから LAN 2 ポートを設定してください。
- LAN 1 インターフェイスと LAN 2 インターフェイスは、重複しない別のサブネット上にある必要があります。

- Expressway-E が DMZ にある場合、Expressway-E の外部 IP アドレスはパブリック IP アドレスである必要があります。また、スタティック NAT モードが有効になっている場合は、スタティック NAT アドレスにパブリック ネットワークからアクセス可能である必要があります。
- また、Expressway-E を企業内の内部ファイアウォールを通過するために使用することができます。この場合、「パブリック」 IP アドレスはパブリックネットワークからアクセスできませんが、企業内の別の部分へのアクセスが可能な IP アドレスです。
- インターフェイスの一方または両方の IP アドレスを変更する必要がある場合は、UI または CLI を使用して変更することができます。必要に応じて、両方を同時に変更できます。また、新しいアドレスは、再起動後に有効になります。

手順

ステップ 1 [デュアル ネットワーク インターフェイスを使用する (Use dual network interfaces)] を [はい (Yes)] に設定します。

ステップ 2 [外部 LAN インターフェイス (External LAN interface)] 設定では、インターフェイスとして [LAN2] を選択します。

外部インターフェイスのスタティック NAT を有効にする選択を行えるようになりました。この設定はどのポートが TURN サーバリレーを割り当てるかを決定します。

トラブルシューティングのヒント

高度なネットワーキングを有効にしても、イーサネットポートの1つのみを設定する場合は、[デュアルネットワークインターフェイスを使用する (Use dual network interfaces)] を [いいえ (No)] に切り替えます。

スタティック NAT の設定

スタティック NAT デバイスの背後に Expressway-E を導入して、パブリック IP アドレスとプライベート IP アドレスを個別に取得できるようにします。この機能は、Expressway-E が DMZ 内にあり、高度なネットワーキング機能が有効にされた展開環境で使用することを目的としています。

このような展開環境では、プライベート IPv4 アドレスとパブリック IPv4 アドレスの両方を使用するために、外向きの LAN ポートで NAT が有効にされます。内向きの LAN ポートではスタティック NAT が有効にされないため、単一の IP アドレスを使用します。このような導入環境においては、Expressway-E の内向きの IP アドレスを使用するようにトラバーサルクライアントを設定する必要があります。

静的 NAT を有効にするには

外部に面した LAN ポートに対して、次の設定を指定します。

手順

- ステップ 1 [IPv4アドレス (IPv4 address)] フィールドに、ポートのプライベート IP アドレスを入力します。
- ステップ 2 [IPv4スタティックNATモード (IPv4 static NAT mode)] を [オン (On)] に設定します。
- ステップ 3 [IPv4 スタティック NAT アドレス (IPv4 static NAT address)] フィールドに、ポートのパブリック IP アドレスを入力します。これは、(NAT 要素外部での) アドレス変換後の IP アドレスです。

IPv6 モードの機能と制限

Expressway の IP インターフェイスを [IPv6 のみ (IPv6 Only)] モードに設定すると、これらのインターフェイスは IPv6 のみを使用します。これらは他のシステムとの通信に IPv4 を使用せず、IPv4 と IPv6 の間 (デュアルスタック) でインターワーキングを行いません。

サポートされている IPv6 の明示的な機能

- Expressway 登録された IPv6 エンドポイント間のコール。
- DiffServ トラフィック クラス (TC) のタギング。
- TURN サーバ (Expressway-E 上)。
- 自動侵入防御。
- DNS ルックアップ。
- ポートの使用およびステータス ページ。

サポートされている RFC

- RFC 2460 : Internet Protocol, Version 6 (IPv6) Specification (この仕様のうち、スタティックグローバルアドレスのみを実装)。
- RFC 2464 : Transmission of IPv6 Packets over Ethernet Networks。
- RFC 3596 : DNS Extensions to Support IP Version 6。
- RFC 4213 : Basic Transition Mechanisms for IPv6 Hosts and Routers。
- RFC 4291 : IP Version 6 Addressing Architecture。
- RFC 4443 : Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification。
- RFC 4861 : Neighbor Discovery for IP version 6 (IPv6)。
- RFC 5095 : Deprecation of Type 0 Routing Headers in IPv6。

- RFC 6156 : Traversal Using Relays around NAT (TURN) Extension for IPv6。

IPv6 モードの既知の制限

- IPv6 アドレスはスタティックである必要があります。これらは、リンクローカルまたは SLAAC アドレスにはなれません。
- IP アドレスまたはそのゲートウェイの IP アドレスを変更した場合は、Expressway を再起動する必要があります。
- Mobile & Remote Access (MRA) は、IPv6 モードでテストまたはサポートされません。MRA の場合、プライマリ コール制御エージェントは IPv6 をサポートしない Unified CM です。
- 分散証明書失効リストからの失効ステータスの取得は、IPv6 モードではサポートされません。

DNS の設定

[DNS] ページ ([システム (System)]>[DNS]) を使用して、Expressway の DNS サーバと DNS を設定します。

システム ホスト名とドメイン名の設定

[システム ホスト名 (System host name)] で、この Expressway を表す DNS ホスト名を定義します。

- システム ホスト名はクラスタ内の各ピアに一意である必要があります。
- リモートログサーバ上の Expressway を識別するために使用します ([システムホスト名 (System host name)] を指定しない場合は、デフォルト名の「TANDBERG」が使用されます。)
- 名前には、英字、数字、ハイフン、下線のみを使用できます。最初の文字は英字、最後の文字は英字または数字にする必要があります。

[ドメイン名 (Domain name)] は、非修飾サーバアドレス (例 : ldapserver) の解決を試みるときに使用されます。クエリが DNS サーバに送信される前に、非修飾サーバアドレスの末尾に追加されます。サーバアドレスが完全修飾の場合 (ldapserver.mydomain.com など)、または IP アドレスの形式である場合は、DNS サーバに問い合わせるまではサーバアドレスの後ろにドメイン名は追加されません。ドメイン名は次の Expressway 設定に適用されます。

- LDAP サーバ
- NTP サーバ
- 外部マネージャ サーバ
- リモート ログイン サーバ

すべてのサーバアドレスには IP アドレスまたは FQDN（完全修飾ドメイン名）を使用することをお勧めします（Expressway の FQDN は、システムのホスト名とドメイン名をつなげた形式になります）。

SIP メッセージングへの影響

システムのホスト名とドメイン名は、SIP メッセージングでのこの Expressway への参照を識別するためにも使用されます。この場合、エンドポイントではその SIP プロキシとして、Expressway を（推奨されていない IP アドレス形式ではなく）FQDN 形式で設定しています。

この場合、たとえばエンドポイントに設定されている FQDN が Expressway に設定されているシステムホスト名とドメイン名とが一致しなければ、Expressway は INVITE 要求を拒否します。



(注) SIP プロキシ FQDN は、エンドポイントが Expressway に送信した SIP 要求のルートヘッダーに組み込まれているために、このチェックが行われます。

カスタム ドメイン検索

[ドメイン検索 (Search domains)] 設定は、外部ホストが Expressway-C とは異なる DNS ドメイン内にあり、非修飾ホスト名が設定されているエッジ展開に適しています。必要に応じて、この設定を使用して 1 つ以上の DNS ドメインを指定できます。Expressway は、指定されたドメインを 1 つずつ非修飾ホスト名に追加し、作成された FQDN を DNS でクエリします。DNS から IP アドレスが返されるまで、このプロセスが繰り返されます。つまり、ホスト間の接続を設定する際は、FQDN を入力する必要はありません。

複数のアドレスはスペースで区切ります。

DNS 要求

デフォルトでは、DNS 要求はシステムのエフェメラルポート範囲にあるランダムポートを使用します。その代わりに、必要に応じて、[DNS 要求のポート範囲 (DNS requests port range)] を [カスタムポート範囲を使用 (Use a custom port range)] に設定してから、[DNS 要求のポート範囲の開始 (DNS requests port range start)] フィールドと [DNS 要求のポート範囲の終了 (DNS requests port range end)] フィールドを定義することによって、カスタムポート範囲を指定できます。



(注) 設定したソースポート範囲が狭いと、DNS スプーフィング攻撃に対する脆弱性が高まります。

DNS サーバアドレスの設定

次の場合は、アドレス解決のために 1 つ以上の DNS サーバをクエリするように指定する必要があります。

- 外部アドレスの指定時に、IPアドレスではなく FQDN を使用する場合（LDAP および NTP サーバや、ネイバーゾーン、ピアなど）。
- [URI ダイヤリング](#)や [ENUM ダイヤリング](#)などの機能を使用する場合。

デフォルトの DNS サーバ

最大 5 つのデフォルトの DNS サーバを指定できます。Expressway は一度に 1 つのサーバをクエリします。そのサーバが利用不可の場合、Expressway はリスト内の別のサーバを試します。

サーバを指定する順序は重要ではありません。Expressway は、最後に利用可能であることが既知となったサーバを優先します。

ドメイン単位の DNS サーバ

5 つのデフォルトの DNS サーバに加え、指定したドメインに 5 つの明示的 DNS サーバを指定できます。これは、特定のドメイン階層が明示的部署にルーティングされる必要がある場合、導入で役に立ちます。

追加するドメイン別 DNS サーバの各アドレスに、最大 2 つのドメイン名を指定できます。これらのドメインでの DNS クエリは、デフォルト DNS サーバではなく、指定した DNS サーバに転送されます。

ドメインごとの冗長サーバを指定するには、ドメインごとの DNS サーバアドレスをさらに追加し、そのアドレスを同じドメイン名に関連付けます。これらのドメインに対する DNS 要求は両方の DNS サーバに同時に送信されます。

特定のホスト名の要求に、どのドメインネームサーバ（DNS サーバ）が応答しているかを確認するには、[DNS ルックアップツール](#)（[メンテナンス（Maintenance）]>[ツール（Tools）]>[ネットワークユーティリティ（Network utilities）]>[DNS ルックアップ（DNS lookup）]）を使用します。

転送プロトコル

Expressway は UDP と TCP を使用して DNS 解決を行います。DNS サーバからは、通常、UDP と TCP 応答が送られます。UDP 応答が 512 バイトの UDP メッセージサイズの制限を超えていると、Expressway は UDP 応答を処理できません。一般に、これが問題になることはありません。Expressway は代わりに TCP 応答を処理できるためです。

ただし、ポート 53 での TCP インバウンドをブロックしている場合、UDP 応答のサイズが 512 バイトを超えていると、Expressway は DNS からの応答を処理できません。この場合、DNS ルックアップツールを使用しても結果は表示されず、要求したアドレスを必要とするすべての操作は失敗します。

DNS レコードのキャッシング

DNS ルックアップをキャッシュすることでパフォーマンスを向上させることができます。DNS 設定が変更されるたびに、キャッシュが自動的に消去されます。必要に応じて、[DNS キャッシュの消去（Flush DNS cache）] をクリックして強制的に消去することもできます。

DSCP / Quality of Service の設定

DSCP マーキングについて

X8.9 から、Expressway では Mobile & Remote Access を含む、ファイアウォールを通過するトラフィックに対する、改善された DSCP (DiffServ コードポイント) パケットマーキングがサポートされます。DSCP は、パケットの QoS レベルの測定です。トラフィックの優先順位付けに対してきめ細かい制御を提供するために、DSCP 値はこれらの個々のトラフィックタイプに対して送信 (マーキング) されます。

トラフィックのタイプ	提供されたデフォルト値	Web UI フィールド
ビデオ	34	QoS Video
音声	46	QoS Audio
XMPP	24	QoS XMPP
シグナリング	24	QoS Signaling

X8.9 以前は、すべてのシグナリングとメディアトラフィックにまとめて DSCP 値を適用する必要がありました。

必要に応じて、[システム (System)] > [QoS (Quality of Service)] の Web UI ページ (または [CLI]) から、デフォルトの DSCP 値を変更できます。

注：

- DSCP 値「0」は標準のベストエフォートサービスを指定します。
- DSCP マーキングは SIP と H.323 トラフィックに適用されます。
- TURN トラフィックが実際に Expressway により処理される場合は、DSCP マーキングは TURN メディアに適用されます。
- メディアタイプが特定できない場合、トラフィックタイプ「ビデオ」がデフォルトで割り当てられます。(たとえば、異なるメディアタイプが同じポートに多重化されている場合です)。

既存の QoS/DSCP コマンドと API の廃止



(注) X8.9 から QoS/DSCP 値を指定する、以前の方法をサポートしていません。以前の Web UI 設定の QoS モードおよび QoS 値、CLI コマンド `xConfiguration IP QoS Mode` と `xConfiguration IP QoS Value` および対応する API は廃止されました。これらのコマンドは使用しないでください。

現在これらのコマンドを使用している場合

Expressway をアップグレードするときに、定義された既存の QoS の値は新規フィールドに自動的に適用され、提供されたデフォルトを置き換えます。たとえば、値 20 を定義したら、4 つの DSCP すべての設定（QoS Audio、QoS Video、QoS XMPP、QoS Signaling）も 20 に設定されます。

ダウングレードはサポートされません。アップグレード前のソフトウェアバージョンに戻る必要があると、QoS の設定は、最初に提供されるデフォルト値にリセットされます。つまり、QoS モードは [なし (None)] に、QoS 値は [0] に設定されます。手動で、使用する値を定義し直す必要があります。

DSCP 値の設定

必要に応じて、指定された DSCP のデフォルト値を変更するには、[QoS (Quality of Service)] ページ ([システム (System)] > [QoS (Quality of Service)]) に移動し、使用する新しい値を指定します。

スタティック ルート

Expressway から IPv4 または IPv6 のアドレス範囲へのスタティック ルートを定義できます。[システム (System)] > [ネットワーク インターフェイス (Network interfaces)] > [スタティック ルート (Static routes)] に移動します。

このページでは、スタティック ルートを表示、追加、削除できます。

[高度なネットワーキング (Advanced Networking)] オプションを使用して DMZ に Expressway を導入する場合は、スタティック ルートが必要になることがあります。また、他の複雑なネットワーク導入環境でも必要になることがあります。

スタティック ルートの追加：

手順

ステップ 1 この Expressway からの新しいスタティックルートの基本宛先アドレスを入力します。

203.0.113.0 または **2001:db8::** などを入力します。

ステップ 2 範囲を定義するプレフィックス長を入力します。

この例を拡張する場合、**24** と入力して IPv4 範囲の 203.0.113.0 ~ 203.0.113.255 を定義するか、または **32** と入力して IPv6 範囲の 2001:db8:: ~ 2001:db8:ffff:ffff:ffff:ffff:ffff:ffff を定義します。

アドレス範囲フィールドに、IP アドレスとプレフィックス長から Expressway が計算した範囲が表示されます。

ステップ 3 新しいルート用にゲートウェイの IP アドレスを入力します。

ステップ 4 新しいルートのイーサネットインターフェイスを選択します。

このオプションは、2つ目のイーサネットインターフェイスが有効な場合にのみ、使用できません。[LAN 1] または [LAN 2] を選択してそのインターフェイスを介したルートを適用するか、[自動 (Auto)] を選択して Expressway がいずれのインターフェイスでもこのルートをとれるようにします。

ステップ 5 [ルートの作成 (Create route)] をクリックします。

新しいスタティックルートがテーブルに表示されます。必要に応じて、このテーブルからルートを削除できます。

- (注)
- IP ルートは CLI を使用して設定することもできます。その場合は、**xCommand RouteAdd** コマンドと **xConfiguration IP Route** コマンドを使用します。
 - 最大 50 のネットワークとホストの組み合わせを設定できます。
 - root としてログインし、ip route ステートメントを使用して IP ルートを設定しないでください。

侵入からの保護

ファイアウォール ルールの設定

ファイアウォール ルールは Expressway へのアクセスを IP レベルで制御する IP テーブル ルールを設定する機能を提供します。Expressway では、これらのルールが複数のグループに分類されており、次の順序で適用されます。

- **動的システム ルール**：これらのルールは、すべての確立された接続/属性を維持します。これらには、特定のアドレスをブロックするなど、自動検出機能によって挿入された任意のルールも含まれます。最後に、ループバックインターフェイスからのアクセスを許可するルールが含まれます。
- **設定不可のアプリケーションルール**：このルールはアプリケーション固有の必要なすべてのルール (SNMP トラフィックや H.323 ゲートキーパー検出を許可するなど) を組み込みます。
- **ユーザ設定が可能なルール**：このオプションは、手動で設定したすべてのファイアウォール ルール (この項で説明) を組み込みます。このルールは、何が Expressway にアクセス可能なのか (通常は何を制限するか) を詳細に定義します。このグループには、Expressway LAN 1 インターフェイス (および高度なネットワーキング オプション キーがインストールされている場合には LAN 2 インターフェイス) に送信されるすべてのトラフィックを許可する最終的なルールがあります。

また、以前のルールによってまだ明確に許可されていない、または拒否されていないブロードキャストやマルチキャストのトラフィックを破棄する、設定できない最終的なルールもあります。

デフォルトでは、Expressway の特定の IP アドレスに送信されるトラフィックはアクセスが許可されますが、Expressway が明示的にそのトラフィックをリッスンしていない場合はそのトラフィックが破棄されます。仕様に対してシステムをロックダウンするには、追加のルールをアクティブに設定する必要があります。



(注) 発信接続からのリターントラフィックは常に受け入れ可能です。

ユーザ設定ルール

通常、ユーザ設定のルールは、何が Expressway へアクセスできるかを制限するために使用されます。次の操作を実行できます。

- そこからのトラフィックを許可または拒否する、発信元 IP アドレスのサブネットを指定します。
- 拒否されたトラフィックをドロップするか却下するかを選択します。
シナリオによっては、ファイアウォールルールでドロップまたは拒否するように設定されているインバウンドトラフィックでも、Expressway がプロキシする場合があります。これは、ファイアウォールルールは新しいインバウンドトラフィックにのみ適用されるためです。内部ネットワーク上のデバイスがアウトバウンド接続を開始した場合、外部ネットワーク上のデバイスは同じポートを使用して応答します。IP テーブルには既存のメディアパス情報が含まれているため、ファイアウォールルールよりも優先されます。
- SSH、HTTP/HTTPS などのよく知られたサービスを設定するか、トランスポートプロトコルとポート範囲に基づいてカスタマイズされたルールを指定します。
- LAN 1 インターフェイスと LAN 2 インターフェイスには異なるルールを設定します（**高度なネットワーキング** オプション キーがインストールされている場合）。ただし、マルチキャスト アドレスなどの特定の宛先アドレスは設定できません。
- ルールを適用するプライオリティを指定します。

ファイアウォール ルールの設定およびアクティブ化

[**ファイアウォール ルールの設定 (Firewall rules configuratio)**] ページを使用して、一連の新しいファイアウォール ルールを設定し、アクティブにします。

表示されたルールセットが最初に、現在アクティブなルールのコピーになります。（ファイアウォールルールが定義されていないシステムでは、リストは空です。）ルールの数が多い場合は、[**フィルタ (Filter)**] オプションを使用して表示されるルールセットを限定できます。



(注) 組み込みルールは、このリストには表示されません。



一連のファイアウォールルールを変更するには、新しいルールを追加するか、または既存のルールを修正または削除します。現在のアクティブなルールに加えた変更は保留状態に維持されます。変更が完了したら、新しいルールをアクティブにして前のセットを置き換えます。UDP関連のルールの場合、新しいルールは次のシステムの再起動時にのみ有効になります（ただし、UDPルールを削除すると、ルールセットをアクティブにした後すぐに無効になります）。

ルールを設定しアクティブにするには、次の手順を実行します。

手順

ステップ 1 [システム (System)] > [保護 (Protection)] > [ファイアウォールルール (Firewall rules)] > [設定 (Configuration)] に移動します。

ステップ 2 必要に応じてルールを追加、変更、または削除して変更を加えます。

ルールの順序を変更するには、上下矢印キー  と  を使用して、隣接するルールのプライオリティを入れ替えます。

- 新規または変更されたルールは [保留中 (Pending)] ([状態 (State)] カラム内) として表示されます。
- 削除されたルールは、[削除保留中 (Pending delete)] として表示されます。

ステップ 3 新しい一連のファイアウォールルールの設定が終了したら、[ファイアウォールルールのアクティブ化 (Activate firewall rules)] をクリックします。

ステップ 4 新しいルールをアクティブ化することを確認します。これにより、既存のアクティブなルールセットが設定したばかりのルールセットに置き換えられます。

新しいルールをアクティブ化することを確認した後、これらは検証され、エラーがあれば報告されます。

ステップ 5 エラーがなければ、新しいルールが一時的にアクティブ化され、「ファイアウォールルールの確認 (Firewall rules confirmation)」ページが表示されます。

ここで、15 秒以内に新しいルールを保存することを確認します。

- [変更内容を受け入れる (Accept changes)] をクリックして永続的にルールを適用します。
- 15 秒の制限時間をすぎた場合、または [変更のロールバック (Rollback changes)] をクリックすると、以前のルールが復帰し、設定ページに戻ります。

15 秒の時間制限によって実行される自動ロールバック機能により、新しいルールが適用された後でも、変更がアクティブ化されたクライアントシステムは、以前と同様にシステムにアクセスできます。クライアントシステムが (Web インターフェイスにアクセスでき

なくなったために) 変更を確認できない場合、ロールバックにより、再びシステムにアクセスできるようになることが確認されます。

ステップ 6 この手順は、UDP ルールを追加する場合にのみ適用されます。つまり、**[転送 (Transport)] = [UDP]** を設定した 1 つ以上のカスタムルールです。新しい UDP ルールは、次にシステムを再起動するまで有効になりません。この特殊なケースでは、ファイアウォールルールの有効化だけでは十分ではありません。削除された UDP ルールにはこの要件はなく、ルールセットを有効にするとすぐに無効になります。

ファイアウォールルールを設定すると、**[すべての変更内容を復元 (Revert all changes)]** オプションも表示されます。これによって、保留中のすべての変更が破棄され、ルールの作業中のコピーが現在のアクティブなルールと一致するようにリセットされます。

ルール設定

各ルールの設定可能なオプションは次のとおりです。

フィールド	説明	使用方法のヒント
優先度 (Priority)	ファイアウォールルールを適用する順序。	最もプライオリティの高いルール (1、次が 2、その次が 3 など) が最初に適用されます。 ファイアウォールルールのプライオリティは一意にする必要があります。同じプライオリティを持つルールが複数あるとルールのアクティブ化が失敗します。
インターフェイス	アクセスを制御する LAN インターフェイス。	これは、 高度なネットワーキング のオプションキーがインストールされている場合にのみ適用されます。

フィールド	説明	使用方法のヒント
IPアドレス (IP address) とプレフィックス長 (Prefix length)	これら2つのフィールドによって、ルールが適用されるIPアドレスの範囲が決定されます。	[アドレス範囲 (Address range)] フィールドに、[IPアドレス (IP address)] と [プレフィックス長 (Prefix length)] の設定の組み合わせに基づき、ルールが適用されるIPアドレスの範囲が表示されます。 プレフィックス長の範囲は、IPv4 アドレスの場合は 0 ~ 32、IPv6 アドレスの場合は 0 ~ 128 です。
サービス	ルールが適用されるサービスを選択するか、[カスタム (Custom)] を選択して、独自の転送タイプとポート範囲を指定します。	(注) サービスの宛先ポートをこの後で Expressway 上に再設定する場合は (80 ~ 8080 など)、以前のポート番号を含むファイアウォールルールは自動的に更新されません。
トランスポート (Transport)	ルールが適用されるトランスポートプロトコル。	サービスを [カスタム (Custom)] に指定している場合のみ適用されます。
ポート範囲の開始と終了	ルールが適用されるポート範囲。	UDP または TCP の [カスタム (Custom)] サービスを指定している場合のみ適用されます。

フィールド	説明	使用方法のヒント
アクション (Action)	<p>ルールに一致する IP トラフィックに対して実行されるアクション。</p> <p>[許可 (Allow)]: トラフィックを受け入れます。</p> <p>[ドロップ (Drop)]: 送信者に応答せずにトラフィックをドロップします。</p> <p>[拒否 (Reject)]: 「「unreachable」」という応答によりトラフィックを拒否します。</p>	<p>トラフィックをドロップすると、潜在的な攻撃者には、どのデバイスがパケットをフィルタリングするか、またその理由などの情報が提供されません。</p> <p>導入の環境をセキュアにするため、まずすべてのサービスへのアクセスを拒否するプライオリティの低いルールセット（たとえばプライオリティ 50000）を設定してから、特定の IP アドレスへのアクセスを選択的に許可するプライオリティのより高いルール（たとえばプライオリティ 20）を設定することができます。</p>
説明	(オプション) ファイアウォールルールのフリー形式の説明。	ルールの数が多い場合は、オプションの説明により [フィルタ (Filter)] を使用して、関連するルールセットを見つけることができます。

現在アクティブなファイアウォールルール

[現在アクティブなファイアウォールルール (Current active firewall rules)] ページ ([システム (System)] > [保護 (Protection)] > [ファイアウォールルール (Firewall rules)] > [現在アクティブなルール (Current active rules)]) には、システムに現在設定されているユーザ設定のファイアウォールルールが表示されます。このリストに表示されない組み込みルールセットもあります。

ルールを変更するには、「ファイアウォールのルール設定 (Firewall rules configuration) 」 ページに移動する必要があります。ここで、新しいルールセットの設定とアクティブ化ができます。

自動化された侵入からの保護の設定

自動保護サービスを使用して、悪意のあるトラフィックを検出およびブロックし、辞書ベースでの不正ログイン攻撃から Expressway を保護することができます。

これは、システム ログ ファイルを解析して、SIP、SSH、Web/HTTPS アクセスなど、特定のサービスカテゴリへの繰り返されるアクセスの失敗を検出することにより機能します。指定し

た時間ウィンドウ内の失敗の数が設定したしきい値に達すると、送信元のホストアドレス（侵入者）と宛先ポートは、指定した期間ブロックされます。この期間を過ぎると、一時的にブロックされた可能性のある悪意のないホストを締め出すことがないように、ホストアドレスは自動的にブロック解除されます。

1つまたは複数のカテゴリで例外となるアドレス範囲を設定することができます（下記の、[例外的設定](#)を参照してください）。

[ファイアウォールルール](#)の設定は、ファイアウォールルールと組み合わせて使用する必要があります。特定の脅威を動的に検出して一時的にブロックするには、自動保護を使用し、一定範囲の既知のホストアドレスを永続的にブロックするには、ファイアウォールルールを使用します。

保護カテゴリについて

Expressway で使用可能な一連の保護カテゴリは、実行中のソフトウェアのバージョンに応じて事前に設定されています。各カテゴリを有効化、無効化、および設定することはできますが、新たなカテゴリを追加することはできません。

また、特定のログ ファイル メッセージを各カテゴリに関連付けるルールは事前に設定されており、変更できません。[システム (System)] > [保護 (Protection)] > [自動検出 (Automated detection)] > [設定 (Configuration)] に移動してカテゴリの名前をクリックすることにより、特定のカテゴリへのアクセスの失敗/侵入として処理されたログファイルエントリのサンプルを確認することができます。サンプルは、ページ下部の [ステータス (Status)] セクションの上部に表示されます。

自動保護の有効化

X8.9以降、次を含むさまざまなカテゴリの自動侵入防御がデフォルトで有効になっています。

- HTTP プロキシ認証の失敗
- HTTPプロキシプロトコル違反
- SSH認証エラー
- SSHプロトコル違反
- XMPPプロトコル違反

この変更は新しいシステムに影響します。アップグレードされたシステムは既存の防御設定を維持します。

手順

ステップ 1 [システム (System)] > [管理 (Administration)] に移動します。

ステップ 2 [自動保護サービス (Automated protection service)] を [オン (On)] に設定します。

ステップ 3 [保存 (Save)] をクリックします。

これでサービスは実行されますが、環境に必要な保護カテゴリと例外を設定する必要があります。

保護カテゴリの設定

[自動検出の概要 (Automated detection overview)] ページ ([システム (System)] > [保護 (Protection)] > [自動検出 (Automated detection)] > [設定 (Configuration)]) を使用して、Expressway の保護カテゴリを有効にして設定し、現在のアクティビティを表示します。

このページには、以下に示す、すべての使用可能なカテゴリの概要が表示されます。

- **[ステータス (Status)]** : カテゴリが [オン (On)] または [オフ (Off)] のどちらに設定されているかを示します。[オン (On)] の場合、さらにカテゴリの状態が示されます。通常は [アクティブ (Active)] の状態になっていますが、カテゴリが有効化または無効化された直後は一時的に [初期化中 (Initializing)] または [シャットダウン中 (Shutting down)] と表示される場合があります。[失敗 (Failed)] と表示されている場合は、アラームを確認してください。
- **[現在ブロック中 (Currently blocked)]** : このカテゴリで現在ブロックされているアドレスの数。
- **[失敗の合計 (Total failures)]** : このカテゴリに関連付けられているサービスへの失敗したアクセス試行の合計数。
- **[ブロックの合計 (Total blocks)]** : ブロックがトリガーされた回数。



- (注)
- 通常、[ブロックの合計 (Total blocks)] の数は [失敗の合計 (Total failures)] の数よりも少なくなります ([トリガー レベル (Trigger level)] が 1 に設定されている場合を除く)。
 - 同じアドレスが複数回、カテゴリごとにブロックおよびブロック解除される場合があり、各ブロックが個別にカウントされます。

- **[除外 (Exemptions)]** : このカテゴリで例外として設定されているアドレスの数。

このページから、現在ブロックされているアドレスや特定のカテゴリに適用されている例外も確認できます。

カテゴリの有効化または無効化

手順

-
- ステップ 1 [システム (System)] > [保護 (Protection)] > [自動検出 (Automated detection)] > [設定 (Configuration)] に移動します。
 - ステップ 2 有効または無効にするカテゴリの隣にあるチェックボックスを選択します。
 - ステップ 3 必要に応じて [有効 (Enable)] または [無効 (Disable)] をクリックします。
-

カテゴリのブロッキングルールの設定

手順

-
- ステップ 1 [システム (System)] > [保護 (Protection)] > [自動検出 (Automated detection)] > [設定 (Configuration)] に移動します。
 - ステップ 2 設定するカテゴリの名前をクリックします。このカテゴリの設定ページが表示されます。
 - ステップ 3 必要に応じて、カテゴリの以下の項目を設定します。
 - [状態 (State)] : このカテゴリへの保護を有効にするか無効にするかを指定します。
 - [説明 (Description)] : フリー形式のカテゴリの説明。
 - [Trigger level] および [Detection] ウィンドウ : これらの設定の組み合わせにより、カテゴリのブロッキングしきい値を定義します。これらにより、失敗したアクセス試行が何回発生したらブロックをトリガーするか、および、これらの失敗の発生数をカウントする時間ウィンドウを指定します。
 - [ブロック期間 (Block duration)] : ブロックが維持される期間。
 - ステップ 4 [保存 (Save)] をクリックします。
-

例外の設定

[自動検出の除外 (Automated detection exemptions)] ページ ([システム (System)] > [保護 (Protection)] > [自動検出 (Automated detection)] > [除外 (Exemptions)]) を使用して、1 つまたは複数の保護カテゴリから常に除外する IP アドレスを設定できます。

手順

-
- ステップ 1 [システム (System)] > [保護 (Protection)] > [自動検出 (Automated detection)] > [例外 (Exemptions)] に移動します。

- ステップ2 設定する[アドレス (Address)]または[新規 (New)]をクリックして新しいアドレスを指定します。
- ステップ3 [アドレス (Address)]および[プレフィックス長 (Prefix length)]に値を入力して、除外する IP アドレスの範囲を定義します。
- ステップ4 このアドレスを例外とするカテゴリを選択します。
- ステップ5 [Add address] をクリックします。

(注) 現在ブロックされているアドレスを除外する場合、(「**ブロックされたアドレス (Blocked addresses)**」ページで手動でブロック解除しない限り) そのアドレスはブロック期限が切れるまでブロックされ続けることに注意してください。

ブロックされたアドレスの管理

「**ブロックされたアドレス (Blocked addresses)**」ページ ([システム (System)] > [保護 (Protection)] > [自動検出 (Automated detection)] > [ブロックされたアドレス (Blocked addresses)]) を使用して、自動保護サービスにより現在ブロックされているアドレスを管理できます。

- これにより、現在ブロックされているすべてのアドレス、それらのアドレスがどのカテゴリからブロックされているかが表示されます。
- アドレスをブロック解除するか、または、アドレスのブロック解除と同時にそれを例外リストに追加することができます。アドレスを永続的にブロックする場合は、そのアドレスを設定済みの[ファイアウォールルール](#)の設定に追加する必要があります。

「**自動検出の概要 (Automated detection overview)**」ページに記載のリンクによってこのページにアクセスした場合、選択したカテゴリによってページの内容がフィルタリングされています。また、アドレスがそのカテゴリからブロック解除されるまでの残り時間も表示されます。

アクセスの失敗および侵入の調査

特定のアクセスの失敗または侵入の試行を調査する必要がある場合、各カテゴリに関連付けられた関連トリガーのログメッセージをすべて確認することができます。目的

手順

- ステップ1 [システム (System)] > [保護 (Protection)] > [自動検出 (Automated detection)] > [設定 (Configuration)] に移動します。
- ステップ2 調査するカテゴリの名前をクリックします。
- ステップ3 [このカテゴリについて一致するすべての侵入からの保護のトリガーを表示する (View all matching intrusion protection triggers for this category)] をクリックします。

そのカテゴリのすべての関連イベントが表示されます。その後、トリガー中のイベントのリストを検索すると、ユーザ名、アドレス、またはエイリアスなど、関連イベントの詳細を確認できます。

自動保護サービスおよびクラスタ化システム

自動保護サービスがクラスタ化システムで有効の場合、以下のように動作します。

- ピアでごとにそれぞれの接続の失敗数が維持され、それぞれのピアでトリガーしきい値に達したときに初めて、侵入者のアドレスはそれぞれのピアによりブロックされます。
- アドレスは、アクセスの失敗が発生したピアに対してのみブロックされます。つまり、アドレスがあるピアでブロックされた場合でも、（やはりブロックされる可能性がある）他のピアへアクセスを試行することができます。
- ブロックされているアドレスは、現在のピアに対してのみブロック解除できます。アドレスが他のピアによりブロックされている場合は、そのピアにログインしてから解除する必要があります。
- カテゴリの設定および例外リストは、クラスタ全体に適用されます。
- 「**自動検出の概要 (Automated detection overview)**」ページには、現在のピアの統計情報のみが表示されます。

MRA 導入での自動保護

Expressway-C を Mobile & Remote Access に使用すると、Unified CM と Expressway-E から多くのインバウンドトラフィックを受信します。

Expressway-C の自動保護を使用するには、自動的に作成されたネイバーゾーンとユニファイドコミュニケーションのセキュアなトラバーサルゾーンを使用するすべてのホストについて免除を追加する必要があります。Expressway は、検出された Unified CM または関連ノードの免除を自動では作成しません。

その他の情報

- ブロックされているホストアドレスがシステムにアクセスしようとする時、要求はドロップされます（ホストは応答を受信しません）。
- 複数のカテゴリでホストアドレスを同時にブロックすることは可能ですが、すべてのカテゴリでブロックされるとは限りません。それぞれのブロックが異なるタイミングで期限切れになる可能性があります。
- （手動で、またはブロック期限が終了して）アドレスがブロック解除された場合は、カテゴリのトリガーレベルで指定した数の失敗が消化されて初めて、そのカテゴリによる2回目のブロックを設定できます。

- カテゴリは、有効になるたびにリセットされます。システムが再起動した場合、または自動保護サービスがシステム レベルで有効になると、すべてのカテゴリがリセットされます。カテゴリがリセットされると、以下のように動作します。
 - 現在ブロックされているアドレスがあれば、ブロック解除されます。
 - 失敗およびブロックの現在の合計はゼロにリセットされます。
- 「自動検出の概要 (Automated detection overview)」 ページで [すべての侵入からの保護 イベントを表示 (View all intrusion protection events)] をクリックすると、自動保護サービスに関連付けられているすべてのイベント ログが表示されます。
- アップグレード元 X14.0 リリース：
 - SIP 登録の失敗は、新しいインストールと工場出荷時のリセットケースでデフォルトで有効になっています。アップグレードのシナリオでは、前の値が保持されます。
 - SIP 認証の失敗は、新しいインストールと工場出荷時のリセットケースでデフォルトで有効になっています。アップグレードのシナリオでは、前の値が保持されます。
 - Expressway-C がサービスに影響を与えている場合は、SIP 認証失敗ジェイルルールを無効にします。

レート制限の設定

レート制限の概要ページ ([システム (System)] > [保護 (Protection)] > [レートの制限 (Rate limits)] > [設定 (Configuration)]) は、クラッシュ、CPU 使用率が高い、メモリ使用量が多いなどの問題なく Expressway が実行できる SIP トラフィックレートを制限するために使用されます。

X14.0 リリースから、SIP トラフィックのレート制限はデフォルトで有効になっています。

1. デフォルトでは、1 秒あたり 100 の接続が許可され、SIP ポート 5060、5061、& 5062 に設定されている場合は 20 の制限があります。
2. 1 秒あたりの接続数および制限速度を有効または無効にするか、変更できます。
3. 秒の範囲の値あたりの接続数は 1 ~ 150 で、デフォルト値は 100 です。
4. 限界範囲の値は 15 ~ 30 で、デフォルト値は 20 です。
5. バーグラフには、確立された接続数とドロップされた接続数が表示されます。

**重要**

- TCP プロトコルの場合にのみ「新規」の状態が新しい接続と見なされます。関連した接続および確立された接続はすべて同じ接続として扱われるため、パケットが既存の接続からドロップされません。
- UDP プロトコルの場合は、関連した接続および確立された接続すべてが「新規」接続として実行されます。

レート制限ルールの設定

レート制限ルールを設定するには、次の手順を実行します。

1. [システム (System)] > [保護 (Protection)] > [レートの制限 (Rate limits)] > [設定 (Configuration)] へ移動します。
2. 設定するカテゴリの名前をクリックします。
このカテゴリの設定ページが表示されます。
3. 必要に応じて、カテゴリの以下の項目を設定します。
 1. [ステータス (Status)] : レート制限モードが有効か無効かを示します。
 2. 接続 (1 秒毎) : 1 秒あたりの接続数を変更します。
 3. [限界値 (Burst limit)] : 一致する接続/パケットの最大初期数で、この数値は、上記の制限に達するたびに、この数値まで 1 ずつ再充電されます。
4. [保存 (Save)] をクリックします。

ネットワーク サービス

システム名とアクセス設定値の設定

「システム管理 (System administration)」ページ ([システム (System)] > [管理 (Administration)]) は、次の設定に使用します。

- Cisco Expressway システムの名前。
- 管理者が使用できるシステムへのアクセス方法。シリアルケーブルでユニットに直接接続された PC を使用して Expressway を管理できますが、IP を使用してリモートからシステムにアクセスしなければならない場合もあります。それには、HTTPS を介して Web インターフェイスを使用するか、SSH を介してコマンドラインインターフェイスを使用します。
- FindMe または Cisco Telepresence Management Suite Provisioning Extension に含まれる他のプロビジョニング サービスを使用するかどうか。

- 管理サービス（Web ユーザーインターフェイス、REST API、CLI）が LAN3 上で Expressway の専用管理インターフェイス（DMI）を使用するために、オプションで管理サービスの直接管理トラフィック。

表 1:[システム管理 (System Administration)] ページの設定

フィールド	説明	使用方法のヒント
システム名 (System name)	Expressway を識別するために使用します。システム名は、Web インターフェイスのさまざまな場所、および（ラック内の他のシステムと識別できるように）ユニットの前面パネルに表示されます。	容易に、かつ一意的にシステムを識別できる名前を付けることを推奨します。
エフェメラルポート範囲 (Ephemeral port range)	Expressway コール処理によって制限されている場合を除き、開始値と終了値によって、エフェメラルアウトバウンド接続に使用するポート範囲が定義されます。	
Services		
シリアルポート/コンソール (Serial port/console)	VMware コンソール経由でシステムにローカルでアクセスできるかどうか。 デフォルトは [On] です。	シリアルポート/コンソールアクセスは、通常は無効になっていますが、再起動後の 1 分間は常に有効になります。
SSH サービス (SSH service)	SSH と SCP を使用して Expressway にアクセスできるかどうか。 デフォルトは [On] です。	
Web インターフェイス (HTTPS を使用) (Web interface (over HTTPS))	Web インターフェイス経由で Expressway にアクセスできるかどうか。 デフォルトは [On] です。	

フィールド	説明	使用方法のヒント
プロビジョニングサービス (Provisioning services)	[システム (System)] > [TMS プロビジョニング拡張サービス (TMS Provisioning Extension services)] のページに、Expressway Web ユーザーインターフェイスでアクセスさせるかどうかを指定します。アクセス可能な場合、このページから、Cisco TelePresence Management Suite Provisioning Extension (Cisco TMSPE) とユーザ、デバイス、FindMe、電話帳のプロビジョニングサービスに接続できます。 デフォルトは [オフ (Off)] です。	FindMe は、Expressway X12.5 で非推奨となり、以降のリリースではサポートが終了します。
専用管理インターフェイス (DMI) のみを使用	管理サービス (Web ユーザーインターフェイス、REST API、CLI) が LAN3 上で Expressway の専用管理インターフェイス (DMI) を使用するために、オプションで管理サービスの管理トラフィックが必要です。 デフォルトは [いいえ (No)] です。	SNMP 管理トラフィックでは、[システム > SNMP] ページから同じ機能を使用できます。
セッション制限 (Session Limit)		
セッションタイムアウト (Session timeout)	セッションがタイムアウトするまでに管理セッション (シリアルポート、HTTPS、または SSH) または FindMe セッションが非アクティブになる可能性がある分数。デフォルトは 30 分です。	
アカウント単位のセッションの制限 (Per-account session limit)	個々の管理者アカウントが各 Expressway で許可される同時セッション数。	これには、Web セッション、SSH セッション、およびシリアルセッションが含まれます。セッション制限は、root アカウントには適用されません。 値を 0 にすると、セッション制限はオフになります。

フィールド	説明	使用方法のヒント
システムセッションの制限 (System session limit)	各 Expressway で許可される同時管理者セッションの最大数。	これには、Webセッション、SSHセッション、およびシリアルセッションが含まれます。セッション制限は、rootアカウントには適用されません。ただし、アクティブなルートアカウントセッションは、現在の管理者セッションの総数にカウントされます。 値を0にすると、セッション制限はオフになります。
システム保護 (System protection)		
自動保護サービス (Automated protection service)	自動化された侵入からの保護の設定 をアクティブにするかどうかを指定します。 デフォルトは [On] です。	サービスを有効にした後は、特定の 保護カテゴリについて を設定する必要があります。
自動検出保護 (Automatic discovery protection)	Cisco TMS などの管理システムがこの Expressway をどのように検出するかを制御します。 [オフ (Off)] : 自動検出が許可されません。 [オン (On)] : この Expressway を検出するように Cisco TMS を手動で設定する必要があります。また、Cisco TMS が管理者アカウントのクレデンシャルを提供する必要があります。 デフォルトは [オフ (Off)] です。	システムを再起動して変更はすべて有効にします。
Web サーバの設定 (Web server configuration)		
HTTP リクエストを HTTPS にリダイレクト (Redirect HTTP requests to HTTPS)	HTTP 要求を HTTPS ポートにリダイレクトするかどうかを指定します。 デフォルトは [オフ (Off)] です。	HTTP を使用したアクセスを機能させるには、HTTPS も有効にする必要があります。 プロトコルを前に付加しないでアドレスを入力すると、ブラウザでは HTTP (ポート 80) と想定します。この設定が [オン (On)] の場合、Expressway は Web ブラウザを Web 管理者ポート にリダイレクトします。

フィールド	説明	使用方法のヒント
HTTP Strict Transport Security (HSTS)	<p>Web ブラウザがこのサーバへのアクセスにセキュアな接続のみを使用するように指示するかどうかを決定します。この機能を有効にすると、中間者 (MITM) 攻撃に対する保護が強化されます。</p> <p>[オン (On)] : Web サーバからのすべての応答は、有効期限が 1 年の Strict Transport Security ヘッダーが追加されて送信されます。</p> <p>[オフ (Off)] : : Strict Transport Security ヘッダーは送信されず、ブラウザは通常どおりに動作します。</p> <p>デフォルトは [オン (On)] です。</p>	<p>HSTS の詳細については、以下を参照してください。</p>
Web 管理者ポート (Web administrator port)	<p>管理者が Expressway Web インターフェイスにアクセスするための https リスニングポートを設定します。</p> <p>Meeting Server Web プロキシなどで TCP 443 を必要とする機能を有効にする場合は、Expressway-E で Web 管理にデフォルト以外のポートを使用することを強くお勧めします。</p> <p>変更を有効にするために Expressway を再起動します。</p>	<p>デフォルト以外のポートを使用し、アドレスの前に https:// プロトコルを付加する場合は、ポートを付加する必要があります。たとえば、ブラウザにアドレス <code>https://vcse.example.com:7443</code> を入力します。 <code>https://vcse.example.com</code> を使用すると、ブラウザはポート 443 を想定し、Expressway はアクセスを拒否します。</p> <p>ネットワーク要素が Web 管理ポートへのトラフィックをブロックすると、Expressway への Web アクセスが失われることがあります。この状態が発生した場合は、SSH またはコンソールを使用してポートを変更できます。</p>

フィールド	説明	使用方法のヒント
クライアント証明書ベースのセキュリティ (Client certificate-based security)	<p>クライアントシステム（通常は Web ブラウザ）が HTTPS を使用して Expressway と通信するために必要なセキュリティ レベルを制御します。</p> <p>[不要 (Not required)] : クライアントシステムはどのような形式の証明書も提示する必要はありません。</p> <p>[証明書の検証 (Certificate validation)] : クライアントシステムは、信頼できる認証局 (CA) が署名した有効な証明書を提示する必要があります。</p> <p>(注) [不要 (Not required)] から [証明書の検証 (Certificate validation)]に変更する場合は、再起動が必要です。</p> <p>[証明書ベースの認証 (Certificate-based authentication)] : クライアントシステムは、信頼できる CA が署名した有効な証明書を提示する必要があり、その証明書にはクライアントの認証クレデンシャルが含まれている必要があります。</p> <p>デフォルト : [不要 (Not required)]</p>	

フィールド	説明	使用方法のヒント
		<p>重要</p> <ul style="list-style-type: none"> <p>• [証明書の検証 (Certificate validation)] を有効にすると、ブラウザ (クライアントシステム) は、Expressway の信頼できる CA 証明書リストの CA が署名した有効な (日付において有効であり、CRL により失効されていない) クライアント証明書がある場合にのみ、Expressway の Web インターフェイスを使用できます。</p> <p>• この機能を有効にする前に、ブラウザに有効なクライアント証明書があることを確認してください。証明書をブラウザにアップロードする手順はブラウザのタイプによって異なります。また、証明書を有効にするにはブラウザの再起動が必要になる場合もあります。</p> <p>• CA 証明書をアップロードするには「信頼できる CA 証明書リストの管理 (Managing the Trusted CA Certificate List)」 (ページ) ページを、クライアント証明書をテストするには「クライアント証明書のテスト (Testing Client Certificates)」 ページを使用します。</p> <p>• [証明書ベースの認証 (Certificate-based authentication)] を有効</p>

フィールド	説明	使用方法のヒント
		<p>にすると、標準のログインメカニズムが使用できなくなります。ブラウザ証明書が有効で、提供されたクレデンシャルに適切な許可レベルがある場合のみ、ログインできます。ブラウザ証明書から Expressway がクレデンシャルを取得する方法は、「証明書ベースの認証設定 (Certificate-based authentication configuration)」 ページで設定できます。</p> <ul style="list-style-type: none"> この設定は、Expressway のサーバ証明書のクライアント検証に影響しません。
証明書失効リスト (CRL) の確認中 (Certificate revocation list (CRL) checking)	<p>HTTPS クライアント証明書を証明書失効リスト (CRL) と照合して確認するかどうかを指定します。</p> <p>[なし (None)] : CRL チェックは実行されません。</p> <p>[ピア (Peer)] : クライアントの証明書を発行した CA に関連付けられた CRL のみを確認します。</p> <p>[すべて (All)] : クライアントの証明書を発行した CA の信頼できる証明書チェーン内のすべての CRL を確認します。</p> <p>デフォルト : [すべて (All)]</p>	<p>[クライアント証明書ベースのセキュリティ (Client certificate-based security)] が有効になっている場合のみ適用されます。</p>

フィールド	説明	使用方法のヒント
CRLのアクセス不可のフォールバック動作 (CRL inaccessibility fallback behavior)	<p>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。</p> <ul style="list-style-type: none"> • [失効として処理 (<i>Treat as revoked</i>)] : 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 (<i>Treat as not revoked</i>)] : 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] 	[クライアント証明書ベースのセキュリティ (Client certificate-based security)] が有効になっている場合のみ適用されます。
展開設定 (Deployment Configuration)		

フィールド	説明	使用方法のヒント
Configuration	<p>システムのサイズを決定します。オプションは次のいずれかです。</p> <p>[大 (<i>Large</i>)] : 8 個の CPU コア、6 GB のメモリ、1 Gbps または 10 Gbps の NIC。</p> <p>[中 (<i>Medium</i>)] : 2 個の CPU コア、4 GB のメモリ、1 Gbps の NIC。</p>	<p>1 Gbps の NIC を使用する中規模システムをアップグレードすると、Expressway 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。その結果、Expressway-E は大規模システム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、Expressway はコールをドロップします。</p> <p>この問題が発生した場合は、次のいずれかの操作を行います。</p> <ul style="list-style-type: none"> • システムのデフォルトサイズを [中 (<i>Medium</i>)] に変更し、多重化 RTP/RTCP トラフィック用に設定されているポートを使用するには、[中 (<i>Medium</i>)] を選択します。 • 大規模システムとして使用する場合は、大規模システムのデフォルトの逆多重化ポートをファイアウォールで開きます。 <p>このオプションは、Expressway-Es として導入され、次の最小仕様で CE1200 以降のアプライアンスでのみ使用できます。</p> <ul style="list-style-type: none"> • サポートされる Expressway ソフトウェアバージョン (詳細については、アプライアンスの <i>Cisco Expressway CExxxx</i> インストールガイドを参照) • CPU : 8 コア • メモリ : 6 GB • NIC : 1 Gbps

デフォルトでは、HTTPS と SSH を使用したアクセスが有効になっています。セキュリティを最適化するには、HTTPS と SSH を無効にし、シリアルポートを使用してシステムを管理しま

す。シリアルポートへのアクセスではパスワードのリセットが許可されるため、Expressway は物理的にセキュアな環境にインストールすることを推奨します。

HTTP 厳重トランスポートセキュリティ

HTTP Strict Transport Security (HSTS) は、Web サーバがセキュアな接続のみを使用して通信するように Web ブラウザに強制するメカニズムです。バージョンによっては、一部のブラウザでサポートされていない場合があります。HSTS を有効にすると、HSTS をサポートするブラウザは以下のように動作します。

- Web サイトへのセキュアでないリンクは、サーバにアクセスする前に、自動的にセキュアなリンクに置き替えられます (たとえば、`http://example.com/page/` は、`https://example.com/page/` に変更されます)。
- 接続がセキュアである (たとえば、サーバの TLS 証明書が有効かつ信頼でき、期限切れでない) 場合のみアクセスを許可します。

HSTS をサポートしないブラウザは、Strict-Transport-Security ヘッダーを無視し、以前と同じように動作します。サーバには以前と同様にアクセスできます。

対応ブラウザは、完全修飾名で IP アドレスではなくサーバにアクセスする場合に、Strict-Transport-Security ヘッダーのみを尊重します。

SNMP 設定値の設定

[SNMP] ページ ([システム (System)] > [SNMP]) を使用して、Expressway の SNMP を設定します。

Cisco Telepresence Management Suite (Cisco TMS) や HP OpenView などのツールは SNMP ネットワーク管理システム (NMS) として機能することができます。これらのツールでは、Expressway などのネットワーク デバイスの管理上の注意が必要な状態をモニタできます。Expressway は RFC 1213 で定義されているように、最も基本的な MIB-II ツリー (.1.3.6.1.2.1) をサポートします。

Expressway によって次のような情報が使用可能になります。

- システムの動作期間
- システム名
- ロケーション
- 連絡先
- インターフェイス
- ディスク領域、メモリ、その他の機器固有の統計情報

SNMP は、デフォルトでディセーブルになっています。そのため、Expressway を SNMP NMS (Cisco TMS を含む) でモニタするには、代替の **SNMP モード** を選択する必要があります。設定可能なオプションは次のとおりです。

フィールド	説明	使用方法のヒント
SNMP モード (SNMP mode)	SNMP サポートのレベルを制御します。 [無効 (Disabled)] : SNMP サポートなし。 [v3 セキュア SNMP (v3 secure SNMP)] : 認証および暗号化をサポート。 [v3 および TMS サポート (v3 plus TMS support)] : セキュア SNMPv3 および、OID 1.3.6.1.2.1.1.2.0 にのみ非セキュアアクセス。 [v2c] : 非セキュアなコミュニティベースの SNMP。	セキュア SNMPv3 を使用する際に外部マネージャとして Cisco TMS も使用する場合は、[v3 および TMS サポート (v3 plus TMS support)] を選択する必要があります。
説明	SNMP で表示したときのシステムのカスタム説明。デフォルトは、カスタムの説明なし (空のフィールド) です。	このフィールドを空にしておくと、デフォルトの SNMP の説明が使用されます。
コミュニティ名 (Community name)	Expressway の SNMP コミュニティ名。 デフォルトは <i>public</i> です。	[v2c] や [v3 および TMS サポート (v3 plus TMS support)] を使用している場合にのみ適用されます。
システム管理者 (System contact)	Expressway の問題についての問い合わせが可能な担当者の名前。 デフォルトは [管理者 (Administrator)] です。	[システム管理者 (System contact)] および [ロケーション (Location)] は、クエリのフォローアップ時に管理者により参照用に使用されます。
[所在地 (Location)]	Expressway の物理的な場所を指定します。	
ユーザ名 (Username)	Expressway の SNMP ユーザ名。SNMP マネージャに対してこの SNMP エージェントを識別するために使用します。	[v3 セキュア SNMP (v3 secure SNMP)] または [v3 および TMS サポート (v3 plus TMS support)] を使用している場合にのみ適用されます。

フィールド	説明	使用方法のヒント
専用管理インターフェイス (DMI) のみを使用	必要に応じて、SNMPがLAN3で Expressway の専用管理インターフェイス (DMI) を使用するために、管理トラフィックが必要です。 デフォルトは [いいえ (No)] です。	管理サービス (Web ユーザーインターフェイス、REST API、CLI) に関連する管理トラフィックでは、[システム (System)] > [管理の設定 (Administration settings)] ページからでも同じ機能を使用できます。
[v3 認証 (v3 Authentication)] の設定 (SNMPv3 にのみ適用可能)		
認証モード (Authentication Mode)	SNMPv3 認証を有効または無効にします。	
タイプ (Type)	認証クレデンシアルをハッシュするために使用されるアルゴリズム。X12.5.7 から、SHA (セキュアハッシュアルゴリズム) がサポートされている唯一のオプションです。MD5 (メッセージダイジェストアルゴリズム5) のパスワードはサポートされていません。	
[パスワード (Password)]	認証クレデンシアルの暗号化に使用するパスワード。	8文字以上でなければなりません。
[v3 プライバシー (v3 Privacy)] の設定 (SNMPv3 にのみ適用可能)		
プライバシーモード (Privacy Mode)	SNMPv3 暗号化を有効または無効にします。	
タイプ (Type)	メッセージの暗号化に使用されるセキュリティ モデル。 [AES] : Advanced Encryption Standard、128 ビット暗号化。 デフォルトかつ推奨される設定は [AES] です。	
[パスワード (Password)]	メッセージの暗号化に使用するパスワード。	8文字以上でなければなりません。

Expressway は SNMP トラップや SNMP セットをサポートしません。したがって、SNMP を使用して Expressway を管理することはできません。



- (注) SNMP は、関連する情報が潜在的に機密情報であるため、デフォルトでは無効になっています。パブリックインターネットまたは内部システム情報を公開したくないその他の環境では、Expressway で SNMP を有効にしないでください。

時刻の設定

[時間 (Time)] ページ ([システム (System)] > [時間 (Time)]) を使用して、Expressway の NTP サーバを設定し、ローカルタイムゾーンを指定します。

NTP サーバは、時刻の正確性を確保するために Expressway が同期するリモートサーバです。NTP サーバは Expressway に UTC 時刻を提供します。

正確なシステム動作を実現するには正確な時刻が必要です。

NTP サーバの設定

システム時刻を同期するときに使用する 1 台以上の NTP サーバで Expressway を設定するには、システムの DNS の設定に応じて ([DNS] ページ ([システム (System)] > [DNS]) でこれらの設定を確認できます)、次の形式のいずれかで最大 5 台のサーバの [アドレス (Address)] を入力します。

- DNS サーバが設定されていない場合は、NTP サーバに IP アドレスを使用します。
- 1 つまたは複数の DNS サーバが設定されている場合、NTP サーバに FQDN または IP アドレスを使用できます。
- 1 台以上の DNS サーバに加えて DNS ドメイン名が設定されている場合、そのサーバ名、FQDN、または IP アドレスを NTP サーバに使用できます。

デフォルトでは、3 つの [アドレス (Address)] フィールドが、シスコが提供する NTP サーバに設定されます。

NTP サーバへの接続時に Expressway が使用する認証方式を設定できます。NTP サーバの接続に、次のオプションのいずれかを使用します。

認証方式	説明
<i>Disabled</i>	認証は使用されません。

認証方式	説明
対称キー (<i>Symmetric Key</i>)	対称キー認証。この方式を使用する場合は、 [キーID (Key ID)] 、 [ハッシュ (Hash)] 方式、 [パスフレーズ (Pass phrase)] を指定する必要があります。ここで入力した値は、NTP サーバ上での同等の設定値と完全に一致する必要があります。複数の NTP サーバに同じ対称キーの設定を使用できます。ただし、各サーバに異なるパスフレーズを使用して設定する場合は、各サーバに一意のキーIDがあることを確認する必要があります。
秘密キー (<i>Private key</i>)	秘密キー認証。この方式では、NTP サーバに送信されるメッセージの認証に、自動生成された秘密キーを使用します。

NTP ステータス情報の表示

[ステータス (Status)] エリアには、NTP サーバと Expressway 間の同期ステータスが次のように表示されます。

- **[起動中 (Starting)]** : NTP サービスは起動中です。
- **[同期済み (Synchronized)]** : Expressway は NTP サーバから正確なシステム時刻を正常に取得しています。
- **[非同期 (Unsynchronized)]** : Expressway が NTP サーバから正確なシステム時刻を取得できません。
- **[ダウン (Down)]** : Expressway の NTP クライアントは稼働していません。
- **[拒否 (Reject)]** : NTP サービスが NTP 応答を受け入れていません。



(注) 更新内容がステータス テーブルに表示されるまで数分かかります。

入手可能なその他の情報は次のとおりです。

フィールド	説明
NTP サーバ	要求に応答した実際の NTP サーバ。これは、NTP サーバのアドレス フィールド内の NTP サーバと異なる場合があります。

フィールド	説明
条件	各 NTP サーバの相対的なランク付けが表示されます。正確な時刻を提供しているすべてのサーバには [候補 (Candidate)] というステータスが付与されます。これらのサーバのうち、Expressway が最も正確な時刻を提供しているため、使用しているサーバには、[sys.peer] というステータスが表示されます。
フラッシュ (Flash)	サーバのステータスに関する情報を示すコード。[00 ok] は、問題がないことを意味します。コードの詳細なリストについては、「 フラッシュ ステータス用語の参照テーブル 」を参照してください。
認証	現在の認証方式のステータスを示します。[正常 (ok)]、[異常 (bad)]、[なし (none)] のいずれか。[なし (none)] 方式が [無効 (Disabled)] [認証 (Authentication)] に設定されている場合は [切斷 (Disabled)] に指定されます。
イベント	NTP が特定した最後のイベントを表示します (たとえば、[reachable] や [sys.peer] など)。
到達可能性 (Reachability)	Expressway と NTP サーバ間の最新 8 件の接続試行の結果を示します。成功の場合はティック、失敗の場合は十字形が表示されます。最新の試行の結果は右端に表示されます。 NTP の設定が変更されるたびに NTP クライアントは再起動し、[到達可能性 (Reachability)] フィールドはすべてバツに戻ります。ただし、右側のインジケータには、再起動後の最初の接続の試みの結果が示されます。ただし、再起動プロセス中に NTP サーバがコンタクト可能なままである場合もあります。
オフセット (Offset)	NTP サーバの時刻と Expressway の時刻との差。
遅延 (Delay)	NTP サーバと Expressway とのネットワーク遅延。
ストラタム (Stratum)	Expressway とリファレンスクロック間の分離度。1 は、NTP サーバが基準クロックであることを示します。
リファレンス ID (Ref ID)	基準クロックを識別するコード。
リファレンス時刻 (Ref time)	NTP サーバが基準クロックと最後に通信した時刻。

このページの残りのフィールドの定義と NTP の詳細については、[Network Time Protocol Web サイト](#)を参照してください。

Expressway の時刻表示とタイムゾーン

Web インターフェイス全体で現地時間が使用されます。時刻は画面の下部のシステム情報バーに表示され、イベントログの各行の先頭に表示されるタイムスタンプの設定に使用されます。



(注) UTC タイムスタンプは、イベントログの各イベントの末尾に組み込まれています。

Expressway は内部的にシステム時刻を UTC で維持します。システム時刻は Expressway のオペレーティングシステムの時刻に基づいており、NTP サーバを設定する場合は、その NTP を使用して同期されます。NTP サーバが設定されていない場合は、Expressway は独自のオペレーティングシステム時刻を使用して日時を決定します。

ローカルの [タイムゾーン (Time zone)] を指定すると、システムが存在するローカル時刻を Expressway が決定します。選択したタイムゾーンに関連付けられた時間数 (または分数) で UTC 時刻を補正します。また、該当する場合は夏時間を考慮するようにローカルタイムを調整します。

ログインページの設定

「ログインページの設定 (Login page configuration)」ページ ([システム (System)] > > [ログインページ (Login page)]) を使用して、ログインページに表示されるメッセージや画像を指定できます。管理者が CLI または Web インターフェイスを使用してログインすると、**ウェルカム メッセージのタイトルとテキスト**が表示されます。

Web インターフェイスを使用すると、ログインページのウェルカム メッセージの上に表示される画像をアップロードできます。

- サポートされている画像形式は、JPG、GIF、および PNG です。
- 200 x 200 ピクセルよりも大きな画像は縮小されます。

オプションで、ログインしている人が続行を許可される前にウェルカムメッセージを確認する必要があることを指定できます。この場合、システムは受諾ボタンを表示し、ユーザはこれをクリックしないと続行できません。

Expressway が [TMS プロビジョニング拡張サービス](#) を使用して FindMe アカウントのデータを提供する場合は、ユーザは Expressway ではなく、Cisco TMS から FindMe アカウントにログインします。



(注) この機能は CLI を使用して設定できません。

外部マネージャ設定値の設定

「外部マネージャ (External manager)」ページ ([システム (System)] > [外部マネージャ (External manager)]) を使用して、外部管理システムへの Expressway の接続を設定します。

外部マネージャは Cisco TelePresence Management Suite (Cisco TMS) などのリモートシステムであり、たとえば、コール試行、接続および切断など Expressway で発生するイベントをモニタするために、また、Expressway がアラーム情報を送信できる場所として使用されます。外部マネージャの使用は任意です。



(注) Cisco TMS は「TANDBERG VCS」として Expressway を識別します。

Expressway は、Cisco TMS への接続が失敗した場合もサービスを失うことなく動作し続けます。これは、Expressway がクラスタ化されている場合にも適用されます。特定のアクションは必要ありません。接続が再確立されると、Expressway と Cisco TMS は互いへの通信を自動的に再開します。

フィールド	説明	使用方法のヒント
アドレス (Address) およびパス (path)	外部マネージャを使用するには、IP アドレスまたはホスト名と、使用する外部マネージャのパスで Expressway を設定する必要があります。	Cisco TMS を外部マネージャとして使用する場合は、デフォルトパスの <code>tms/public/external/management/SystemManagementService.asmx</code> を使用します。
[Protocol]	外部マネージャとの通信に [HTTP] または [HTTPS] のどちらを使用するかを指定します。 デフォルトは <i>HTTPS</i> です。	
証明書検証モード (Certificate verification mode)	外部マネージャによって提供される証明書を確認するかどうかを制御します。	確認を有効にした場合は、外部マネージャの証明書の発行者の証明書を、Expressway の信頼できる CA 証明書を含むファイルに追加する必要があります。これは、「 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)]) から行います。

専用管理インターフェイス (DMI) の設定

X12.7 から、Expressway は専用管理インターフェイス (DMI) をサポートします。これは、管理関連のアクティビティのために Expressway にアクセスするために 3 番目の LAN ポート (LAN3) を使用する新しいネットワークインターフェイスです。ルーティングインターフェイスを他のトラフィックと共有する代わりに、管理トラフィックは LAN3 経由で送信および受信され、他のトラフィックはこのポートを使用しません。

DMI はデフォルトで無効です。



- (注) 物理 CE1200 アプライアンスを使用している場合は、物理アプライアンスに提供されているポート 3a (「図 2 : Cisco Expressway の背面図を参照」) を接続し、「背面パネルのレイアウト」の章で説明されているように DMI アドレスを設定します。具体的な手順については、「『Cisco Expressway CE1200 アプライアンス設置ガイド (Cisco Expressway CE1200 Appliance Installation Guide) 』」を参照してください。

DMI の概要

DMI の有効化には、次の 2 つの側面があります。

1. DMI 機能の有効化：管理トラフィックの LAN3 ポートをオンにします。ただし、専用ではなく、LAN1 (および、設定している場合は LAN2) も使用できます。Expressway は、LAN3 ポートだけでなく、LAN1/LAN2 上の管理トラフィックも引き続きリッスンします。
2. 管理トラフィック用のインターフェイスを LAN3 のみにする場合は、Expressway で DMI 専用に個々の管理サービスを設定する必要があります。



- (注) LAN3 サブネット外に管理サーバがある場合は、現在、これらのトラフィックを LAN3 に送信するにはスタティック IP ルートを設定する必要があります。

Expressway 管理トラフィックは、サーバベースまたはクライアントベースとして分類できません。

Expressway がサーバである管理トラフィックは、次のとおりです。

- HTTP(S) : Web UI 管理および REST API 用
- ssh : (MRA トンネル用ではなく) CLI 用
- SNMP

Expressway がクライアントである管理トラフィックの例には、次のものがあります。

- Cisco TMS などの外部マネージャへのフィードバックイベント用の HTTP(S)

- NTP
- ディレクトリ (LDAP、Active Directory)
- リモート syslog
- 収集されたシステムメトリック

DMI の設定方法

SSOをの有効化手順

始める前に

DMI インターフェイスの新しい DNS 名は、Expressway サーバ証明書にサブジェクト代替名 (SAN) として入力する必要があります。IP アドレスを使用してインターフェイス (または証明書の SAN エントリではない DNS) にアクセスする場合、証明書検証警告が発行され、アクセスがブロックされる場合があります。



注意 DMI は Expressway 設定へのアクセスを提供するので、適切に保護することが重要です。

手順

ステップ 1 Go to [システム (System)] > [ネットワークインターフェイス (Network Interfaces)] > [IP] に進み、[専用の管理インターフェイスを使用する (Use Dedicated Management Interface)] を [はい (Yes)] に設定します。に設定します。

ステップ 2 [LAN3 - DMI] セクションで、次を実行します。

1. LAN3 ポートの IPv4 アドレスまたは IPv6 アドレスを指定します。
2. IPv4 では、サブネットマスクも指定します。
3. IPv6 の場合は、静的なグローバルアドレスを使用します。リンクローカルまたはステートの SLAAC は使用できません。
4. 必要に応じて、ポートの**最大伝送ユニット (MTU)** を設定することで、DMI 経由で送信できるイーサネットパケットの最大サイズを変更します。デフォルト値は 1500 バイトです。

ステップ 3 システムを再起動します。これらの変更を有効にするには、再起動が必要です。

これで、DMI が管理トラフィック用のインターフェイスとして LAN3 でアクティブ化されました。DMI を管理用の唯一のインターフェイスとして使用する場合は、次のタスクに進みます。

(注) Expressway VM の場合、OVF テンプレートに、DMI IP アドレスを定義するカスタマイズオプションがあります。

(オプション) DMI 単独のインターフェイス作成

(オプション) DMI を唯一のインターフェイスにする - サーバ管理トラフィック

Expressway がサーバである場合に、このタスクを使用して、管理トラフィックに DMI を使用します。



注意

これを行う前に、LAN3 で必要なサービスがアクセス可能であることを確認してください。そうしないと、DMI のみへの変更後にこれらのサービスがアクセスできなくなります。回復する唯一の方法は、コンソール (シリアル/VMWare) を使用して DMI をオフにすることであるため、これは管理サービスにとって特に重要です。

1. これは、管理サービス (Web ユーザインターフェイス、REST API、CLI) または SNMP に対して実行できます。DMI 専用を設定するサービスに応じて、次の手順のいずれかまたは両方を実行します。
 - [システム (System)] > [SNMP] に進み、[設定 (Configuration)] セクションで、[専用管理インターフェイスのみを使用する (Use Dedicated Management Interface)] を [はい (Yes)] に設定します。
 - [システム (System)] > [管理設定 (Administration settings)] に進み、[サービス (Services)] セクションで、[管理インターフェイスのみを使用する (管理用) (Use Dedicated Management Interface only (for administration))] を [はい (Yes)] に設定します。
2. 変更を Web ユーザインターフェイスと API に適用するにはシステムを再起動する必要があります。再起動するまで LAN1/LAN2 からアクセスできる状態が維持されます。変更は、再起動に関係なく、コマンドラインインターフェイス (SSH) および SNMP サービスに対して即時に有効になります。

指定された管理サービスに、DMI/LAN3 ポートからのみアクセスできるようになりました。



(注) Expressway では、管理サービスが DMI を唯一のインターフェイスとして使用するよう設定されている間は、この DMI を無効にすることはできません。

(オプション) DMI を唯一のインターフェイスにする - サブネット外のクライアント管理トラフィック

Expressway ソフトウェアのバージョンに応じて、Expressway がクライアントとして動作する管理トラフィックでは、ターゲットサーバが DMI/LAN3 ポートと同じサブネット内にある場合のみ、トラフィックを DMI に送信できます。LAN3 と同じサブネットにサーバを導入できない場合は、オプションで、サービスごとに LAN3 用のスタティック IP ルートを設定することで、Expressway 管理トラフィックに DMI の使用を強制できます。

例

この例では、次のサブネットを含む Expressway を想定しています。

- LAN3 サブネット範囲 : a.b.128.0 ~ a.b.191.255
- LAN1 サブネット範囲 : x.y.156.0 ~ x.y.159.255

Expressway で NTP を設定するとします。NTP サーバが LAN1 サブネット内にあります。Expressway からの発信 NTP トラフィックと NTP からの着信応答で DMI/LAN3 を使用します。これは、LAN3 用のスタティックルートを次の設定で作成することで実現できます ([システム (System)] > [ネットワーク インターフェイス (Network interfaces)] > [スタティックルート (Static routes)])。

- IP アドレス : x.y.151.0
- プレフィックス長 : 24
- ゲートウェイ : 172.22.128.1 (LAN3 サブネットのゲートウェイ)
- インターフェイス : LAN3

詳細については、[スタティック ルート](#)を参照してください。

TMS プロビジョニング拡張サービスの設定

Cisco TMSPE サービスは Cisco TMS でホストされます。これらのサービスは、Expressway の [プロビジョニングサーバ](#) がエンドポイント デバイスからのプロビジョニング要求に対応するために使用するユーザ、デバイス、および電話帳のデータを提供します。また、FindMe サービスの FindMe アカウントの設定データも Expressway に提供します。

X8.11 以降、Cisco TMS でホストされるプロビジョニング サービスを有効にするには、Web ユーザインターフェイスで [システム (System)] > [管理設定 (Administration settings)] ページを使用するか、デバイス プロビジョニング CLI コマンド (*xconfiguration Administration DeviceProvisioning*) を使用します。これらのサービスは、特別なオプションキーやライセンスがなくても有効にできます。次のデバイスのプロビジョニング サービスを使用できます。

- ユーザ
- FindMe
- 電話帳

- デバイス

新規インストールでは、すべてのサービスがデフォルトで無効になっています。既存のシステムでは、アップグレード後も現在のサービス設定が維持されたままになります。

はじめる前に

プロビジョニングサービスをまだ有効にしていない場合は、[システム (System)] > [管理 (Administration)] に移動して [プロビジョニングサービス (Provisioning services)] を [オン (ON)] に設定します。[システム (System)] > [TMS プロビジョニング拡張サービス (TMS Provisioning Extension services)] ページを使用して、Expressway が Cisco TMSPE サービスに接続する方法と使用するサービスを設定します。(サービス自体を設定するには、TMS を使用することをお勧めします。Expressway を使用して Cisco TMSPE サービス設定を変更した場合、それらの変更は TMS に適用されません)。

FindMe は、特殊なケースです。プロビジョニングサービスを有効にすると、次の設定警告アラームが表示されます。FindMe のみを使用し、他のプロビジョニングサービスは使用しない予定である場合、これらのアラームは無視できます。

- 電話帳を正しく動作させるには、デフォルトサブゾーンとその他の関連サブゾーンで認証ポリシーを有効にする必要があります。また、エンドポイントが登録されていない場合は、デフォルトゾーンで認証を有効にする必要もあります (*For phone book requests to work correctly, authentication policy must be enabled on the Default Subzone and any other relevant subzone; authentication must also be enabled on the Default Zone if the endpoints are not registered*) 。
- プロビジョニングを正しく動作させるには、デフォルトゾーンと、プロビジョニング要求を受信する関連ゾーンで認証ポリシーを有効にする必要があります (*For provisioning to work correctly, authentication policy must be enabled on the Default Zone and any other relevant zone that receives provisioning requests*) 。

設定

次の表に、プロビジョニング サービスに設定可能なオプションを記載します。

表 2: プロビジョニングサービスに設定可能なオプション

フィールド	説明	使用方法のヒント
デフォルトの接続設定		
このセクションでは、Cisco TMSPE サービスにアクセスするためのデフォルトの接続設定値を指定します。各サービスでこれらの設定値を使用することも、サービスごとに固有の設定値を使用することもできます (たとえば、サービスごとに異なる Cisco TMSPE サーバを使用するなど)。		

フィールド	説明	使用方法のヒント
サーバアドレス (Server address)	IP アドレスまたはサービスの完全修飾ドメイン名 (FQDN)。	
接続先ポート (Destination port)	Cisco TMSPE サービスのリスニングポート。	
暗号化	<p>Cisco TMSPE サービスを接続するための暗号化。詳細については、「最小 TLS バージョンと暗号スイートの設定」を参照してください。</p> <p>[オフ (<i>Off</i>)] : 暗号化なし。</p> <p><i>TLS</i> : TLS 暗号化を提供します。</p> <p>デフォルトは [<i>TLS</i>] です。</p>	TLS 接続を推奨します。
証明書の確認 (Verify Certificate)	<p>Cisco TMSPE サービスによって提示される証明書を Expressway の現在の信頼できる CA リスト、および (存在する場合は) 失効リストと照合して確認するかどうかを制御します。</p> <p>デフォルトは [はい (<i>Yes</i>)] です。</p>	<p>検証が有効にされていない場合 :</p> <ul style="list-style-type: none"> • IIS (Cisco TMSPE サーバ上) が署名付きの証明書とともにインストールされており、SSL 接続を適用するように設定されている必要があります。 • Cisco TMSPE サーバの証明書の発行者の証明書を、Expressway の信頼できる CA 証明書を含むファイルに追加する必要があります。これは、「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 (<i>Maintenance</i>)] > [セキュリティ (<i>Security</i>)] > [信頼できる CA 証明書 (<i>Trusted CA certificate</i>)] から行います。

フィールド	説明	使用方法のヒント
証明書のホスト名の確認 (Check certificate hostname)	Cisco TMSPE サービスによって提供される証明書に記載されているホスト名を Expressway で検証するかどうかを制御します。 デフォルトは [はい (Yes)] です。	これは、 [証明書の確認 (Verify certificate)] が [はい (Yes)] に設定されている場合に適用されます。 有効な場合、証明書のホスト名 (共通名) と指定した サーバアドレス が一致する必要があります。サーバアドレスが IP アドレスの場合、必要なホスト名は DNS ルックアップによって取得されます。
基本グループ (Base Group)	この Expressway (または Expressway クラスター) を Cisco TMSPE サービスで識別するために使用する ID。	TMS 管理者がこの値を提供します。 通常、 デバイス サービスが使用する 基本グループ ID は他のサービスが使用する ID とは違うため、明示的に指定する必要があります。
認証ユーザ名 (Authentication username) とパスワード (password)	Cisco TMSPE サービスを使用して Expressway がそれ自体を認証するために使用するユーザ名と対応するパスワード。	TLS 暗号化が有効になっていない場合、認証パスワードはクリアテキストで送信されます。
<p>サービス固有の設定</p> <p>Cisco TMSPE サービスのそれぞれ (ユーザ、FindMe、電話帳、および デバイス) の接続の詳細を指定できます。</p>		
このサービスに接続 (Connect to this service)	Expressway を Cisco TMSPE サービスに接続するかどうかを制御します。 デフォルトは [いいえ (No)] です。	[はい (Yes)] の場合、接続のステータスがフィールドの横に表示されます。表示されるステータスは [チェック中 (Checking)]、[アクティブ (Active)]、または [失敗 (Failed)] です。(完全なステータス情報を表示するには、 [詳細 (details)] をクリックします)。

フィールド	説明	使用方法のヒント
ポーリング間隔 (Polling interval)	Expressway が Cisco TMSPE サービスのアップデートを確認する頻度。デフォルトは次のとおりです。 [FindMe] : 2分 [ユーザ (Users)] : 2分 [電話帳 (Phone books)] : 1日 [デバイス (Device)]サービスのポーリング間隔は 30 秒に設定されています。これは変更できません。	ページの下部にある [更新の確認 (Check for updates)] をクリックすると、すべてのサービスの即時更新を要求できます。
デフォルトの接続設定を使用する (Use the default connection configuration)	サービスに Cisco TMSPE サービスのデフォルトの接続設定を使用するかどうかを制御します。 デフォルトは [はい (Yes)] です。	[いいえ (No)] を選択すると、追加の接続設定パラメーター式が表示されます。別の接続詳細を指定して、サービスのデフォルトの接続設定をオーバーライドできます。

Expressway と Cisco TMS 間のデータの即時再同期は、いつでも行うことができます。それには、「TMS プロビジョニング拡張サービス (TMS Provisioning Extension services) 」ページで [完全同期の実行 (Perform full synchronization)] をクリックします。これにより、データが削除されて完全に更新されるまでの数秒間、Expressway 上でサービスが停止します。Cisco TMS 内での最近の更新のみを Expressway に適用する場合は、別の方法として、[更新の確認 (Check for updates)] をクリックしてください。