ユーザ アカウント

ユーザ アカウントについて

Expressway には通常運用用の 2 つのタイプのユーザアカウントがあります。

- **管理者アカウント**：Expressway を設定する際に使用します。
- **FindMe アカウント**：企業内の個人が FindMe プロファイルを設定する際に使用します。（Expressway が TMS Provisioning Extension サービスを使用して FindMe データを提供している場合、Expressway を介した FindMe アカウントの構成は適用されません。）

アカウントの認証

管理者アカウントと FindMe アカウントは、Expressway へのアクセスが許可される前に認証されている必要があります。

Expressway はアカウントをローカルに、または LDAP を使用してリモート ディレクトリ サービスと照合して（現在は Windows Active Directory のみでサポート）認証することができます。また、ローカルとリモートで管理されているアカウントも使用できます。リモート オプションを使用すると、企業内のすべての Expressway 用のディレクトリ サービスに管理者グループを設定できます。これにより、Expressway ごとに個別のアカウントを持つ必要がなくなります。

リモート認証の設定の詳細については、LDAP を使用したリモート アカウント認証の設定を参照してください。

リモートソースを管理者または FindMe アカウントのいずれかの認証に使用している場合は、Expressway を次のように設定する必要があります。

- 適切な LDAP サーバ接続の設定。
- この Expressway への管理者と FindMe のアクセスを管理するリモートディレクトリサービスにすでにセットアップ済みの対応するグループ名に一致する管理者グループまたは FindMe グループ、あるいはその両方（管理者グループの設定とユーザグループの設定を参照してください。）

また Expressway は証明書ベースの認証を使用するように設定することもできます。これは通常、Expressway を安全性の高い環境に導入する場合に必要になります。

パスワードの複雑度

複雑度の要件は、パスワード セキュリティの設定 ページ（**[ユーザ（Users）]** > **[パスワードセキュリティ（Password security）]**）から、ローカルで管理されているパスワードに対して指定できます。

すべてのパスワードとユーザ名で大文字と小文字が区別されます。

アカウント タイプ

管理者アカウント

管理者アカウントを使用して Expressway を設定します。

Expressway には、完全な読み取り/書き込みアクセス権が付与されたデフォルトの **admin** アカウントがあります。これは、Web インターフェイス、API インターフェイスまたは CLI を使用して Expressway にアクセスするために使用できます。

（注） *[リモートのみ（Remote only）]* 認証ソースが使用中の場合は、デフォルトの **admin** アカウントを使用して Expressway にアクセスすることはできません。

Web インターフェイスと API インターフェイスのみを使用して Expressway にアクセスできるようにするには、新たにローカル管理者アカウントを追加します。

リモートで管理する管理者アカウントを使用すると、Web インターフェイスと API インターフェイスまたは CLI を使用して Expressway にアクセスできます。

1 つの管理者アカウントを緊急時アカウントに設定できます。この特殊なアカウントは、リモート認証ができない場合にローカル認証が許可されないときでも Expressway にアクセスできます。

設定ログ

設定ログには、すべてのログイン試行と、Webインターフェイスを使用して行われた設定変更が記録されます。これらは監査証跡に使用できます。これは、複数の管理者アカウントがあるときに特に役立ちます。

複数の管理セッション

複数の管理者セッションを同時に実行できます。これらのセッションは、Webインターフェイス、コマンド ライン インターフェイス、またはその両方を組み合わせて使用していることがあります。これにより、各管理者セッションで同じ設定を変更しようとすると、1つのセッションに加えた変更によりもう1つのセッションに加えた変更が上書きされることにご注意ください。

セッションの制限とタイムアウト

ネットワークサービスの説明に従って、アカウントセッションの制限と非アクティブタイムアウトを設定できます。

ログイン履歴ページ（高度なアカウントセキュリティ）

システムが高度なアカウントセキュリティモードになっている場合はログインした直後に**「ログイン履歴（Login history）」**ページが表示されます。このページには、現在ログインしているアカウントの最新の履歴が示されます。

FindMe アカウント

企業内の個人が FindMe アカウントを使用して、それらの個人が FindMe ID を通じて接続できるデバイスと場所を設定します。

各 FindMe アカウントには、ユーザ名とパスワードを使用してアクセスします。

- リモート FindMe アカウント認証を選択した場合は、Expressway 管理者はリモート ディレクトリ サービスの対応するグループ名と照合するように FindMe グループをセットアップする必要があります。

（注） ユーザ名とパスワードの詳細のみリモートで管理されます。

- FindMe ID、デバイス、および場所などの FindMe アカウントのその他プロパティはローカル Expressway データベースに保存されます。

FindMe アカウントの詳細と、関連付けられた FindMe デバイスと場所の定義の詳細については、FindMe アカウントの設定セクションを参照してください。

多くの FindMe アカウントのプロビジョニングが必要な場合は、Cisco TMS を使用することを推奨します。FindMe アカウントとユーザ アカウントの設定の詳細については、『Cisco TMS プロビジョニング拡張導入ガイド』を参照してください。

root アカウント

Expressway は Expressway オペレーティング システムへのログインに使用できる root アカウントを提供します。通常の運用では **root** アカウントを使用しないでください。特に、このアカウントを使用してシステム設定を行わないでください。代わりに管理者のアカウントを使用します。

詳細については、root アカウントの使用の項を参照してください。

注意 **admin** および **root** アカウントの X8.9 より前のデフォルトのパスワードはよく知られています。これらのアカウントには強力なパスワードを使用する必要があります。新しいシステムが X8.9 以降である場合は、スタートアップ時にデフォルト以外のパスワードを指定する必要があります。

詳細情報

管理者アカウントの設定を参照してください。

パスワード セキュリティの設定

「パスワード セキュリティ（Password security）」ページ（**[ユーザ（Users）]** > **[パスワード セキュリティ（Password security）]**）は、ローカルアカウントのパスワードが承認される前に最小レベルの複雑さを満たす必要があるかどうかを制御します。

- **[厳格なパスワードを適用（Enforce strict passwords）]** が *[オン（On）]* に設定されている場合、その後に設定される対象となるアカウントのパスワードはすべて、厳密なパスワードを構成するための以下のルールに従う必要があります。
- **[厳密なパスワードを強制する（Enforce strict passwords）]** が *[オフ（Off）]* に設定されている場合、パスワードに対して追加のチェックは行われません。デフォルトはオフです。

生成されたパスフレーズのエントロピーの最小ビット数も、このページで 0ー255 の範囲で構成できます（デフォルトは6）。

（注） この設定に関係なく、管理者アカウントに対して空のパスワードを設定することはできません。

厳格なパスワードの範囲

厳格なパスワードの適用設定は、Expressway で管理されているローカルアカウントにのみ適用されます。

- ローカル管理者アカウント

- ローカル FindMe ユーザアカウント
- ローカル認証データベース クレデンシャル（他のデバイスが Expressway での認証を求められている場合に使用する有効なユーザ名とパスワードのリスト）

Expressway で使用される他のパスワード（LDAP/リモートに保存されている管理者や FindMe のクレデンシャルなど）には影響はありません。

（注） すべてのパスワードとユーザ名で大文字と小文字が区別されます。

厳密なパスワードに関する設定不可能なルール

[厳密なパスワードを強制する（Enforce strict passwords）] が *[オン（On）]* に設定されている場合は、次のパスワード規則が常に適用され、構成できません。

- 同じ文字列の複数インスタンスを避ける（連続しないインスタンスもチェック）
- 3 文字以上の連続文字列を避ける（「「abc」」や「「123」」など）
- 辞書にある単語や辞書にある単語の反転を避ける
- 回文を避ける（「「risetovotesir」」など）

管理者アカウント、ローカル認証データベース、および FindMe ユーザのパスワードの作成または変更中に、**[厳格なパスワードを適用する (Enforce strict passwords]** がオンで、ユーザ名と同じ文字がストレートまたはリバースの順序（小文字または大文字）の場合、ページの上部にエラーメッセージが表示されます。

厳密なパスワードに関する設定可能なルール

パスワード ポリシーの以下のプロパティを設定できます。

[カスタム禁止パスワードディクショナリを有効にする（Enable custom forbidden password dictionary）] が *[オン（On）]* に設定されている場合、カスタム禁止パスワードディクショナリを使用して厳密なパスワードチェックを実行できます。

[カスタム禁止パスワードディクショナリを有効にする（Enable custom forbidden password dictionary）] が *[オフ（Off）]* に設定されている場合、厳密なパスワードチェックを実行するときにカスタムディクショナリは使用されません。デフォルトは [オフ（Off）] です。

- 長さは ASCII 文字で 6 文字以上、255 文字以下（デフォルトは 15）
- 数字 [0-9] の数は 0 ～ 255（デフォルトは 2）
- 大文字 [A-Z] の数は 0 ～ 255（デフォルトは 2）
- 小文字 [a-z] の数は 0 ～ 255（デフォルトは 2）
- 特殊文字の数 [(space), @, $ etc.) などの 7 ビット ASCII からの印刷可能な文字] は、0 ～ 255（デフォルトは 2）です。

- 許容される連続繰り返し文字の数は 1 ～ 255（デフォルトの 0 ではチェックは無効になるため、連続繰り返し文字はデフォルトで許容されます。パスワードに連続繰り返しが含まれないようにするには、1 に設定します）
- 文字クラスの最小数は0～4（デフォルトの0はチェックを無効にします）文字クラスは、数字、小文字、大文字、および特殊文字です。

  必要な文字クラスの数とクラスあたりの文字数の間で優先順位の効果が現れる場合があります。

  例：各クラス 2 文字というデフォルトの要件のままにしておくと、4 つの文字クラスが必要であるという暗黙的なルールが存在します。この場合、**[文字クラスの最小数（Minimum number of character classes）]** の設定は無意味になります。または、文字クラスの最小数を 2 に設定し、各クラスから必要な文字の最小数を 0 に設定した場合、各クラスに必要な最小文字数を0にすると、任意の 2 つのクラスの文字を含むパスワードで十分になります（その他の条件を満たしていると見なします）。

パスワードの暗号化

Expressway に設定されているすべてのパスワードが暗号化またはハッシュ形式のいずれかで安全に保存されます。これは、次の項目に適用されます。これらのすべての項目にはユーザ名とパスワードが関連付けられています。

- デフォルトの admin 管理者アカウント
- 追加の管理者アカウント
- ローカル認証データベース クレデンシャル（他のデバイスが Expressway での認証を求められている場合に使用する有効なユーザ名とパスワードのリスト）
- アウトバウンド接続クレデンシャル（別のシステムでの認証に必要な場合に Expressway が使用）
- LDAP サーバ（LDAP サーバにバインドする際に Expressway が使用）

ローカルの管理者アカウントのパスワードは、SHA512 を使用してハッシュされます。他のパスワードは暗号化された形式で保存されます。

Web インターフェイスと CLI の比較

Webインターフェイスを使用してパスワードを入力または表示する場合は、入力する文字の代わりにプレースホルダ文字が表示されます。

コマンドラインインターフェイスを使用してパスワードを入力する場合は、プレーンテキストでパスワードを入力します。ただし、コマンドを実行した後、パスワードは*{cipher}*プレフィックスを使用して暗号化された形式で表示されます。次に例を示します。

xConfiguration Authentication Password: "{cipher}xcy6k+4NgB025vYEgoEXXw=="

パスワードの最大長

次の表に、入力可能なプレーンテキスト文字の最大数をパスワードのタイプごとに示します。

パスワード タイプ	最大長
admin アカウント	1024
その他のローカル管理者アカウント	1024
ローカル データベース認証クレデンシャル	128
アウトバウンド接続クレデンシャル	128
LDAP サーバ	60
FindMe アカウント	1024

（注） パスワードが暗号化されて保存される場合は、プレーンテキストバージョンよりも多くの文字が使用されます。

禁止パスワード辞書

（注） 使用禁止パスワードディクショナリを構成していない場合は、それをクリックすると警告メッセージが表示されます。

```
この Expressway は現在、カスタム禁止パスワード辞書を使用するよう設定されていません。
```

禁止パスワードディクショナリのダウンロード

ステップ 1 **[ユーザ（Users）]** > **[禁止されているパスワード（Forbidden password）]**に移動します。

ステップ 2 **[ディクショナリのダウンロード（Download dictionary）]** をクリックして、現在のバージョンのディクショナリをローカルドライブにダウンロードします。

禁止パスワードディクショナリのアップロード

（注）
- **.txt** ファイルのみサポートされています。
- 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してください。

  たとえば、次のコマンドを考えてみます。

  ```
  xcommand Passworddictionarywrite
  ```

  パスの先頭に **/tmp/** を使用します。

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

  /tmp/ が指定されていない場合、次のエラーメッセージが表示されます。

  ```
  PasswordDictionaryWriteCommandError: Forbidden password dictionary file
  path must start with /tmp/
  ```

ステップ 1 **[ユーザ（Users）]** > **[禁止されているパスワード（Forbidden password）]**に移動します。

ステップ 2 [Choose File] をクリックします。

ステップ 3 ローカルドライブからアップロードするディクショナリファイルを選択し、**[ディクショナリのアップロード（Upload dictionary）]** をクリックします。
結果：新しいディクショナリがアップロードされ、アプリケーションに統合されます。

禁止パスワードディクショナリの更新

ステップ 1 **[ユーザ（Users）]** > **[禁止されているパスワード（Forbidden password）]**に移動します。

ステップ 2 **[ディクショナリのダウンロード（Download dictionary）]** をクリック します。

現在のバージョンのディクショナリをダウンロードし、必要な変更を行います。

ステップ 3 **[ファイルの選択（Choose File）]** をクリックして更新ファイルを選択します。

ステップ 4 **[ディクショナリのアップロード（Upload dictionary）]** をクリックします。

更新されたディクショナリがアップロードされ、アプリケーションに統合されます。

パスフレーズの生成

パスフレーズを生成すると、パスワードよりも長く、単語間にスペースが含まれるランダムなセキュアパスフレーズが提供されます。これにより、文字、数字、記号の不可解なシリーズがなく、セキュリティが向上し、使いやすさが向上します。許可されていないユーザーがそれらを復号化するのを防ぎます。生成されるパスフレーズのデフォルト長は 64 です。

ステップ 1 **[メンテナンス（Maintenance）]** > **[ツール（Tools）]** > **[パスフレーズの生成（Generate Passphrase）]**に移動します。

ステップ 2 新しく**[生成されたパスフレーズ（Generated passphrase）]**が表示されます。

管理者アカウントの設定

「管理者アカウント（Administrator accounts）」ページ（**[ユーザ（Users）]** > **[管理者アカウント（Administrator accounts）]** > ）ページには、Expressway 上のすべてのローカル管理者アカウントのリストが表示されます。

一般に、ローカル管理者アカウントは、WebインターフェイスまたはAPIインターフェイスの Expressway にアクセスするために使用されますが、CLI にアクセスすることはできません。

このページでは、次の操作を実行できます。

- 新しい管理者アカウントの作成
- 管理者パスワードの変更
- アカウントのアクセス レベルの変更：[読み取り/書き込み（Read-write）]、[読み取り専用（Read-only）]、または [オーディタ（Auditor）]
- アカウントのアクセス範囲の変更：[Web アクセス（Web access）]、[API アクセス（API access）]、またはこの両方
- 個別または複数の管理者アカウントの削除、有効化、または無効化
- 緊急時アカウントの指定

管理者アカウントの詳細情報の編集

デフォルトの管理者アカウントと追加したローカル管理者アカウントの詳細情報は編集できます。

ステップ 1 **[ユーザ（Users）]** > **[管理者アカウント（Administrator accounts）]**に移動します。

ステップ 2 関連する管理者アカウントの **[アクション（Actions）]** で、**[ユーザの編集（Edit user）]** をクリックします。

新しいページが表示され、選択した管理者アカウントのパスワードを除くすべてのフィールドを編集できます。

パスワードの変更

ステップ 1 **[ユーザ（Users）]** > **[管理者アカウント（Administrator accounts）]**に移動します。

ステップ 2 関連する管理者アカウントの **[アクション（Actions）]** で、**[パスワードの変更（Change password）]** をクリックします。

新しいページが表示され、選択した管理者アカウントのパスワードを変更できます。

ステップ 3 **[関連タスク（Related tasks）]** セクションに移動し、**[パスフレーズの生成（Related tasks）]** をクリックします。

[生成されたパスフレーズ（Generated passphrase）] ページに新しいパスフレーズが表示されます。

ステップ 4 **[新しいパスワード（New password）]** フィールドと **[新しいパスワードの確認（Confirm new password）]** フィールドのテキストボックスに、新しく生成されたパスフレーズを入力するかコピーして貼り付けます。

ステップ 5 **現在のパスワード**を入力 して、パスワード変更プロセスを承認します。

ステップ 6 [保存（Save）] をクリックします。

パスワードの変更が正常に表示されるメッセージ。

管理者アカウントとフィールド参照について

このデフォルトのローカル管理者 「admin」 アカウントには完全な読み取り/書き込みのアクセス権があり、Web UI、API インターフェイス、または CLI を使用して Expressway にアクセスできます。

このアカウントのユーザ名は **admin** です（すべて小文字）。

（注） 現在、組み込みの**管理者**ユーザーのみが CLI にアクセスできます。X14.0.1 以降のリリースでは、複数の管理者アカウントとグループがCLIにアクセスできます。管理者ユーザーは、ユーザーインターフェイスを介してこのアクセスを提供できます。同様に、管理者ユーザーはCLIと REST API の間でアクセスを切り替えることもできます。

X8.9より前のデフォルトパスワードは**TANDBERG**（すべて大文字）です。X8.9以降では、新しいシステムはスタートアップ時にセキュアなインストールウィザードを実行するため、システムがネットワークに接続される前に新しいパスワードを提供できます。

admin は、削除も名前の変更も、無効化も行えず、アカウント レベルを *[*読み取り/書き込み（*Read-write*）*]* から変更できませんが、Web アクセスと API アクセスを無効にすることはできます。

X8.9 より前のバージョンからシステムをアップグレードした場合、パスワードを変更する必要があることがあります。特に IP による管理が有効になっている場合は、強力なパスワードを選択してください。

admin アカウントのパスワードを忘れた場合は、読み取り/書き込みアクセス権を持つ別の管理者アカウントとしてログインして、**admin** アカウントのパスワードを変更することができます。ほかの管理者アカウントがない場合、またはそれらのパスワードも忘れた場合でも、Expressway への物理的なアクセスがあれば **admin** アカウントのパスワードをリセットできます。詳細については、忘れた場合のパスワードのリセットを参照してください。

管理者アカウントのフィールド リファレンス

フィールド	説明（**Description**）	使用方法のヒント
名前（**Name**）	管理者アカウントのユーザ名。	「「root」」などの一部の名前は予約されています。ローカル管理者アカウントのユーザ名では、大文字と小文字が区別されます。
アクセス レベル（Access level）	管理者アカウントのアクセス レベル： *[Read-write]*：すべての設定情報の表示と変更を許可します。これにより、デフォルトの **admin** アカウントと同じ権限が与えられます。 *[Read-only]*：ステータスおよび設定情報の表示のみを許可し、変更は許可しません。「**アップグレード（Upgrade）**」ページなどのいくつかのページは、読み取り専用アカウントに対してはブロックされています。 *[*オーディタ（*Auditor*）*]*：**[イベント ログ（Event Log）]** ページ、**[設定ログ（Configuration Log）]** ページ、**[ネットワーク ログ（Network Log）]** ページ、**[アラーム（Alarms）]** ページ、および **[概要（Overview）]** ページのみにアクセスできます。 デフォルト：[Read-write]	現在ログインしているユーザのアクセス権限は、各 Web ページの下部にあるシステム情報バーに表示されます。 デフォルトの **admin** アカウントのアクセス レベルは *[*読み取り/書き込み（*Read-write*）*]* から変更できません。

フィールド	説明（**Description**）	使用方法のヒント
パスワード（Password）	この管理者が Expressway へのログインに使用するパスワード。	Expressway のすべてのパスワードは暗号化されます。そのため、ここにはプレースホルダのみが表示されます。 パスワードを入力すると、**[パスワード（Password）]** フィールドの横にあるバーの色が変わり、パスワードの複雑さが示されます。パスワード セキュリティの設定ページ（**[ユーザ（Users）]** > **[パスワード セキュリティ（Password security）]**）で、ローカル管理者パスワードの複雑さ要件を設定できます。 ブランク パスワードは設定できません。 （注） 管理者アカウント、ローカル認証データベース、およびFindMeユーザのパスワードの作成または変更中に、「**[厳格なパスワードを適用する（Enforce strict passwords）]**」がオンで、ユーザ名と同じ文字がストレートまたはリバースの順序（小文字または大文字）の場合、ページの上部にエラーメッセージが表示されます。
New password	アカウントの新しいパスワードを入力します。	このフィールドは、パスワードを変更するときにのみ表示されます。
パスワードの確認（Confirm Password）	アカウントのパスワードを再入力します。	このフィールドは、アカウントを作成するとき、またはそのパスワードを変更するときにのみ表示されます。

フィールド	説明（**Description**）	使用方法のヒント
緊急時アカウント（Emergency account）	*[*はい（*Yes*）*]* を選択すると、このアカウントを緊急時アカウントとして使用します。 読み取り/書き込みアクセスと Web アクセスが可能な有効になっているローカル管理者アカウントを使用する必要があります。	1 つの緊急時アカウントを許可でき、このアカウントを使用すると、ローカル認証が許可されない場合でも Expressway にアクセスできます。 このアカウントの目的は、リモート認証が使用できないときにシステムからロックアウトされるのを回避できるようにするためです。
Web アクセス（Web Access）	このアカウントが Web インターフェイスを使用してシステムにログインできるかどうかを選択します。 デフォルト：[Yes]	
パスワードの強制的なリセット（Force password reset）	[はい（Yes）]を選択する場合、新しいユーザする必要があります新しいパスワードを作成ログインするときにします。 デフォルト：[いいえ（No）]	
API アクセス（API access）	このアカウントがアプリケーション プログラミングインターフェイス（API）を使用してシステムのステータスおよび設定にアクセスできるかどうかを選択します。 デフォルト：[Yes]	Cisco TMS などのシステムによる XML および REST API へのアクセスを制御します。
状態（State）	アカウントが *[*有効（*Enabled*）*]* か *[*無効（*Disabled*）*]* かを選択します。無効なアカウントはシステムにアクセスできません。	
現在のパスワード（Your current password）	変更を承認する必要がある場合、ここに自身の現在のパスワードを入力します。	セキュリティを強化するため、システムはアカウントを作成したりパスワードを変更すると、管理者に自分自身のパスワードを入力するように求めます。

アクティブな管理者セッションの表示

「アクティブな管理者セッション（Active administrator sessions）」ページ（**[ユーザ（Users）]**> **[アクティブな管理者セッション（Active administrator sessions）]**）には、この Expressway に現在ログインしているすべての管理者アカウントのリストが表示されます。

これには、ログイン時刻、セッション タイプ、IP アドレスとポート、および最後にこの Expressway へアクセスした日時などのセッションの詳細が示されます。

必要なセッションを選択して [セッションの終了（Terminate session）] をクリックすることで、アクティブな Web セッションを終了できます。

[セッション タイム アウト（Session time out）] 値をゼロに設定している場合は、このページに多くのセッションが一覧表示されます。これは通常、管理者が Expressway からログアウトせずにブラウザを閉じてセッションを終了した場合に発生します。

LDAP を使用したリモート アカウント認証の設定

管理者アカウント認証のためのリモートディレクトリサービスへの LDAP 接続を設定するには、**「LDAP 設定（LDAP configuration）」**ページ（**[ユーザ（Users）]** > **[LDAP 設定（LDAP configuration）]**）を使用します。

（注） Expressway は、リモート認証用に Microsoft Active Directory の LDAP インターフェイスをサポートします。Okta などの他の LDAP インターフェイスは、現在サポートされていない構成です。

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（Description）	使用方法のヒント
[リモートアカウント認証（Remote account authentication）]：このセクションでは、リモートアカウント認証用の LDAP の使用を有効または無効にできます。		

フィールド	説明（**Description**）	使用方法のヒント
管理者認証ソース（**Administrator authentication source**）	管理者のログイン クレデンシャルを認証する場所を定義します。 *[*ローカルのみ（*Local only*）*]*：システムに保存されているローカルデータベースと照合してクレデンシャルを確認します。 *[*リモートのみ（*Remote only*）*]*：外部クレデンシャルディレクトリと照合してクレデンシャルを確認します。 *[*両方（*Both*）*]*：最初にシステムに保存されているローカルデータベースと照合して確認し、一致するアカウントが見つからなかった場合は外部クレデンシャルディレクトリが代わりに使用されます。 デフォルトは [Local only] です。	*[Both]* を選択すると、ローカルで定義したアカウントを引き続き使用できます。これは、LDAP サーバとの接続や認証の問題をトラブルシューティングするときに役立ちます。 *[*リモートのみ（*Remote only*）*]* の認証が使用されている場合は、デフォルトの **admin** アカウントを含め、ローカルで設定した管理者アカウントを使用してログインできません。 （注） Expressway が Cisco TMS によって管理されている場合、*[*リモートのみ（*Remote only*）*]* は使用しないでください。

[LDAP サーバ設定（LDAP server configuration）]：このセクションでは、LDAP サーバへの接続の詳細を指定します。

Expressway は、LDAP サーバーでユーザーを検索するために、**distinguishedName** という名前の属性を検索します。

（注） LDAP サーバーのユーザーレコードに、**distinguishedName** という名前の有効な属性があることを確認します。

フィールド	説明（**Description**）	使用方法のヒント
FQDNアドレス解決（FQDN address resolution）	LDAPサーバアドレスを解決する方法を定義します。 *[SRV* レコード（*SRV record*）*]*：DNS SRV レコード ルックアップ。 *[*アドレス レコード（*Address record*）*]*：DNS A レコードまたは AAAA レコード ルックアップ。 *[IP* アドレス（*IP address*）*]*：IP アドレスとして直接入力。 デフォルトは *[Address record]* です。 SRV レコードを使用する場合は、*ldap._tcp.<domain> records* を標準 LDAP ポート 389 で使用していることを確認してください。Expressway は LDAP 用に他のポート番号をサポートしていません。 SRV として LDAPS を使用するには、AD サーバが STARTTLS 拡張機能をサポートしている必要があります。（ポート 636 を使用して LDAPS を実行する場合は、アドレスレコードを使用してFQDNを解決し、ポート 636 に直接接続する必要があります。）	SRV ルックアップは _ldap._tcp レコードです。複数のサーバが返された場合、各 SRV レコードの優先度とウェイトによって、サーバが使用される順序が決まります。
[ホスト名（Host name）] と **[ドメイン（Domain）]** または **サーバ アドレス（Server address）**	サーバ アドレスの指定方法は、**FQDN アドレス解決**の設定によって異なります。 *[SRV* レコード（*SRV record*）*]*：サーバ アドレスの**ドメイン**部分だけが必要です。 *[*アドレス レコード（*Address record*）*]*：**ホスト名**と**ドメイン**を入力します。これらは組み合わされて、DNS アドレス レコードを検索するための完全なサーバ アドレスになります。 *[IP* アドレス（*IP address*）*]*：**サーバ アドレス**をIPアドレスとして直接入力します。	TLS を使用する場合、ここに入力するアドレスは、LDAPサーバから提示される証明書に含まれる CN（コモン ネーム）と一致している必要があります。
ポート（Port）	LDAP サーバで使用する IP ポート。	Expresswayは、LDAP暗号化接続に対してポート 636 または 3269 のみをサポートします。

フィールド	説明（Description）	使用方法のヒント
暗号化	LDAP サーバへの接続を Transport Layer Security（TLS）を使用して暗号化するかどうかを決定します。 • *[TLS]*：LDAP サーバへの接続に TLS 暗号化を使用します。 • *Off*：暗号化は使用されません。 デフォルトは、[TLS] です。 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。	TLS が有効になっている場合は、Expressway の信頼済み CA 証明書ファイル内の認証局が LDAP サーバ証明書に署名する必要があります。 **[TLS 用の CA 証明書ファイルをアップロード（Upload a CA certificate file forTLS）]（[関連タスク（Related tasks）]** セクション内）をクリックし、「信頼できる CA 証明書リストの管理」ページに移動します。
証明書失効リスト（CRL）の確認中（Certificate revocation list (CRL) checking）	LDAP サーバとの TLS 接続を確立するときに証明書失効リスト（CRL）を確認するかどうかを指定します。 *None*：CRL チェックは実行されません。 *Peer*：LDAP サーバ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。 *All*：LDAP サーバ証明書を発行した 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。 デフォルトは [なし（None）] です。	失効リストを使用している場合は、必要な CRL データも CA 証明書ファイル内に含める必要があります。
[認証設定（Authentication configuration）]：このセクションでは、LDAP サーバにバインドするときに使用する Expressway の認証クレデンシャルを指定します。		
バインド DN（Bind DN）	LDAP サーバにバインドするときに Expressway で使用される識別名（大文字と小文字の区別なし）。 cn=、ou=、dc= の順に DN を指定する必要があります。 （注） LDAP ユーザに最小の権限を与える必要があります。	名前の中に含まれる特殊文字は、LDAP 標準（*RFC 4514*）に従ってバックスラッシュでエスケープする必要があります。名前と名前の間の区切り文字はエスケープしないでください。 通常、バインド アカウントは特別な権限を持たない読み取り専用のアカウントです。
バインド パスワード（Bind Password）	LDAP サーバにバインドするときに Expressway で使用されるパスワード（大文字と小文字の区別あり）。	プレーン テキストの最大長は 60 文字で、暗号化されます。

フィールド	説明（**Description**）	使用方法のヒント
SASL	LDAP サーバにバインドするときに使用する SASL（Simple Authentication and Security Layer）のメカニズム。 *None*：メカニズムを使用しません。 *DIGEST-MD5*：DIGEST-MD5 メカニズムを使用します。 デフォルトは *[DIGEST-MD5]* です。	企業のポリシーに応じて、Simple Authentication and Security Layer を有効にします。
バインド ユーザ名（Bind username）	Expressway が LDAP サーバにログインするときに使用するアカウントのユーザ名（大文字と小文字の区別あり）。 SASL が有効になっている場合にのみ必要です。	これは、sAMAccountName（セキュリティ アクセス マネージャ アカウント名）になるように設定します（AD では、これはアカウントのユーザ ログオン名です）。
[ディレクトリ設定（Directory configuration）]：このセクションでは、アカウントとグループ名を検索するときに使用する基本識別名を指定します。		
アカウントのベース DN（Base DN for accounts）	データベース構造においてユーザ アカウント検索の開始点となる識別名の ou= および dc= 定義（大文字と小文字の区別なし）。 ou=、dc= の順に DN を指定する必要があります。	アカウントとグループのベース DN は、dc レベル以下にする必要があります（必要に応じてすべての dc= 値と ou= 値を含めてください）。LDAP 認証では、サブ dc アカウントを確認しません。下のレベルの ou= および cn= レベルのみを確認します。
グループのベース DN（Base DN for groups）	データベース構造においてグループ検索の開始点となる識別名の ou= および dc= 定義（大文字と小文字の区別なし）。 ou=、dc= の順に DN を指定する必要があります。	**グループのベース DN** を指定しない場合は、アカウントのベース DN がグループおよびアカウントの両方に使用されます。
ネストされたサブグループの検索深度	LDAP 検索のグループの深さを制限するために使用されます。	最適な検索パフォーマンスのために、リモート管理者の上位レベルのグループを Expressway の（管理者）グループとして定義し、検索深さを 「「1」」 に設定します。

フィールド	説明（**Description**）	使用方法のヒント
すべてのメンバーの検索をスキップ	認証検索プロセス中に管理者グループのメンバールックアップを無効または有効にするために使用されます。デフォルトは「*[*はい（*Yes*）*]*」で、メンバールックアップをスキップします。	設定されているグループのメンバー数が相対的に多い場合は、この設定を「*[*はい（*Yes*）*]*」のままにしておくことをお勧めします。ただし、設定されているグループのメンバーが相対的に少ない導入では、「*[*いいえ（*No*）*]*」（メンバールックアップを行う）に設定すると、認証の遅延が減少する 場合があります。

LDAP サーバの接続ステータスの確認

LDAP サーバへの接続のステータスはページの下部に表示されます。

状態 = 使用可能

エラー メッセージは表示されません。

[State] = [Failed]

次のエラー メッセージが表示されることがあります。

エラー メッセージ	理由/解決方法
DNSはリバース検索を実行できません（DNS unable to do reverse lookup）	SASL 認証にはリバース DNS 検索が必要です。 （注） 逆引きルックアップを容易にするために、152.50.10.in-addr.arpa（アドレスのサブネットは 10.50.152.0/24）とアドレス内のターゲット DNS サーバの形式にします。これにより、サブネット内のすべての要求がデフォルトサーバではなく、ターゲット DNS サーバに送信されます。
DNS で LDAP サーバアドレスを解決できません（DNS unable to resolve LDAP server address）	有効な DNS サーバが設定されていることと、LDAP サーバのアドレスのスペルを確認します。

エラー メッセージ	理由/解決方法
LDAP サーバへの接続に失敗しました。サーバのアドレスとポートを確認してください（Failed to connect to LDAP server. Check server address and port）	LDAP サーバの詳細が正しいことを確認します。
TLS 接続の設定に失敗しました。CA 証明書を確認してください（Failed to setup TLS connection. Check your CA certificate）	TLS には、CA 証明書、秘密キー、およびサーバ証明書が必要です。
サーバへの接続に失敗しました。コードが返されました <戻りコード>（Failure connecting to server. Returned code<return code>）	その他の一般的な問題。
無効なアカウントのベース DN です（Invalid Base DN for accounts）	**アカウントのベース DN** を確認してください。現在の値は、LDAP ディレクトリの有効な部分を記述したものではありません。
無効なサーバ名または DNS 障害（Invalid server name or DNS failure）	LDAP サーバ名の DNS 解決に失敗しました。
無効なバインドクレデンシャル（Invalid bind credentials）	**[バインド DN（Bind DN）]** および **[バインド パスワード（Bind password）]** を確認してください。このエラーは、SASL を *[*なし（*None*）*]* に設定する必要があるときに、*[DIGEST-MD5]* に設定した場合にも表示されることがあります。

エラー メッセージ	理由/解決方法
無効なバインド DN（Invalid bind DN）	[Bind DN] を確認してください。現在の値は LDAP ディレクトリ内の有効なアカウントを記述したものではありません。 **バインド DN** の長さが 74 文字以上ある場合に、この失敗した状態が誤って報告されることがあります。実際に失敗したかどうかを確認するには、有効なグループ名を使用して Expressway 上で管理者グループを設定します。Expressway から「「保存されました（saved）」」と報告された場合は問題ありません（Expressway は指定されたグループが見つかるかどうかを確認します）。グループが見つからないと報告された場合は、**バインド DN** が誤っているか、グループが誤っているか、あるいはそのほかの設定項目が誤っている可能性があります。
インストールされた CA 証明書がありません（There is no CA certificate installed）	TLS には、CA 証明書、秘密キー、およびサーバ証明書が必要です。
設定を取得できません（Unable to get configuration）	LDAP サーバ情報がないか、誤っています。

管理者グループの設定

「管理者グループ（Administrator groups）」ページ（**[ユーザ（Users）]** > **[管理者グループ（Administrator groups）]**）には、Expressway で設定したすべての管理者グループのリストが表示されます。このページでは、グループを作成、編集、削除できます。

管理者グループは、LDAP を使用したリモート アカウント認証の設定が有効になっている場合にのみ適用されます。

Expressway の Web インターフェイスにログインすると、リモート ディレクトリ サービスと照合してクレデンシャルが認証され、所属するグループに関連付けられたアクセス権が割り当てられます。管理者アカウントが複数のグループに属している場合は、最も高いレベルの権限が割り当てられます。

（注） LDAP ユーザーは、グループに CLI アクセスを構成している場合、CLI を使用して Expressway にログインできるようになりました。

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（**Description**）	使用方法のヒント
名前（Name）	管理者グループの名前。 次の文字はすべて使用できません。 / \ [ ] : ; | = , + * ? > < @ "	Expressway で定義されるグループ名は、この Expressway への管理者アクセス権を管理するリモート ディレクトリ サービスでセットアップされているグループ名と一致する必要があります。
アクセス レベル（Access level）	管理者グループのメンバーに付与されるアクセス レベル： *[Read-write]*：すべての設定情報の表示と変更を許可します。これにより、デフォルトの **admin** アカウントと同じ権限が与えられます。 *[Read-only]*：ステータスおよび設定情報の表示のみを許可し、変更は許可しません。「**アップグレード（Upgrade）**」ページなどのいくつかのページは、読み取り専用アカウントに対してはブロックされています。 *[オーディタ（Auditor）]*：**[イベントログ（Event Log）]** ページ、[設定ログ（Configuration Log）] ページ、**[ネットワークログ（Network Log）]** ページ、**[アラーム（Alarms）]** ページ、および **[概要（Overview）]** ページのみにアクセスできます。 *[なし（None）]*：すべてのアクセスが拒否されます。 デフォルト：[Read-write]	管理者が複数のグループに属している場合は、管理者が属するすべてのグループ（無効状態のグループは無視）の各アクセス設定で最も高いレベルの権限が割り当てられます。詳細については、下記の複数のグループに属するアカウントのアクセス レベルの決定を参照してください。
Web アクセス（Web Access）	このグループのメンバーが Web インターフェイスを使用してシステムにログインできるかどうかを決定します。 デフォルト：[Yes]	
API アクセス（API Access）	このグループのメンバーがアプリケーション プログラミング インターフェイス（API）を使用してシステムのステータスおよび設定にアクセスできるかどうかを決定します。 デフォルト：[Yes]	Cisco TMS などのシステムによる XML および REST API へのアクセスを制御します。

フィールド	説明（**Description**）	使用方法のヒント
状態（**State**）	グループが有効になっているか、無効になっているかを示します。無効になっているグループのメンバーへのアクセスは拒否されます。	管理者アカウントが有効状態と無効状態の両方が混在する複数の管理者グループに属する場合、アクセスは有効になります。

複数のグループに属するアカウントのアクセス レベルの決定

管理者がさまざまなアクセス レベルの複数のグループに属する場合、最も高いアクセス レベルが付与されます。無効状態のグループは無視されます。

たとえば、以下のグループが設定されているとします。

グループ名	アクセス レベル	**Web** アクセス	**API** アクセス
管理者	読み取りと書き込み	-	-
リージョン **A**	読み取り専用	はい	-
リージョン **B**	読み取り専用	-	はい
リージョン **C**	読み取り専用	はい	はい

次の表は、これらのグループの1つ以上に属するアカウントに付与されるアクセス権限の例を示しています。

属するグループ	付与されるアクセス権限
管理者とリージョン **A**	Web インターフェイスへの読み取り/書き込みアクセス、API アクセスなし
管理者とリージョン **B**	API インターフェイスへの読み取り/書き込みアクセス、Web インターフェイス アクセスなし
管理者とリージョン **C**	Web インターフェイスと API インターフェイスへの読み取り/書き込みアクセス
リージョン **A** のみ	Web インターフェイスへの読み取り専用アクセスで、API アクセスなし

忘れた場合のパスワードのリセット

どのアカウント パスワードもリセットすることができます。これを行うには、デフォルトの **admin** アカウントか、または読み取り/書き込みアクセス権があるほかの管理者アカウントとし

て Expressway にログインします。これができない場合は、コンソールを使用して **admin** パスワードまたは **root** パスワードをリセットします。

（注） パスワードをリセットしても保存済みの設定とデータは影響を受けません。

Web インターフェイスによる管理者アカウントのパスワードの変更

デフォルトの管理者アカウントと追加したローカル管理者アカウントのパスワードは変更できます。

ステップ 1 **[ユーザ（Users）]** > **[管理者アカウント（Administrator accounts）]**に移動します。

ステップ 2 関連する管理者アカウントの **[アクション（Actions）]** で、**[パスワードの変更（Change password）]** をクリックします。

新しいページが表示され、選択した管理者のパスワードを変更できます。

ステップ 3 新しいパスワードを入力し、確認のために再度入力します。

（注） また、現在ログインしている管理者アカウントのパスワードも入力し、パスワードの変更を許可します。

シリアル接続によるルートまたは管理者パスワードのリセット

ハードウェア Expressway で **admin** パスワード、または **root** パスワードを次のようにリセットします。

ステップ 1 シリアル ケーブルを使用して Expressway に PC を接続します。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。

ステップ 2 Expressway を再起動します。

ステップ 3 ユーザ名 **pwrec** を使用して PC からログインします。パスワードは不要です。

ステップ 4 管理者アカウント認証ソースが[リモート（Remote）]に設定されている場合は、その設定を[両方（Both）]に変更するオプションが表示されます。これにより、ローカル管理者アカウントがシステムにアクセスできるようになります。

ステップ 5 変更するアカウント（**ルート**または**管理者**）を選択します。

ステップ 6 新しいパスワードを入力するように求められます。

次のタスク

pwrec のアカウントは、再起動後に 1 分間だけアクティブになります。その後はパスワードをリセットするためにシステムを再起動する必要があります。

vSphere での root パスワードまたは admin パスワードのリセット

管理者アカウントまたは **root** アカウントのパスワードを忘れた場合、VM（仮想マシン）Expressway を使用している場合は、次の手順を使用してパスワードをリセットできます。

ステップ 1 [vSphere クライアント（vSphere Client）] を開きます。

ステップ 2 リンク [コンソールの起動（Launch Console）] をクリックします。

ステップ 3 Expressway をリブートします。

ステップ 4 vSphere コンソールで、ユーザー名 **pwrec** を使用してログインします。パスワードは必要ありません。

ステップ 5 プロンプトが表示されたら、パスワードを変更するアカウント（*root* または管理者アカウントのユーザ名）を選択します。

ステップ 6 新しいパスワードを入力するように求められます。

次のタスク

pwrec のアカウントは、再起動後に 1 分間だけアクティブになります。その後はパスワードをリセットするためにシステムを再度リブートする必要があります。

root アカウントの使用

Expressway は Expressway オペレーティング システムへのログインに使用できる root アカウントを提供します。このアカウントのユーザー名は **root**（すべて小文字）で、プロンプトが表示されたら任意のパスワードを設定します。**root** アカウントにデフォルトのパスワードが設定されている場合は、Web インターフェイスと CLI にアラームが表示されます。

（注） **root** アカウントは機密情報にアクセスできる場合があるため、通常運用では使用しないでください。また、このアカウントを使用して特定のシステム設定を実行しないでください。代わりに **admin** アカウントを使用します。

root アカウントのパスワードの変更

ステップ 1 既存のパスワードを使用し、**root** として Expressway にログインします。デフォルトでは、これを実行できるのはシリアル接続または SSH の場合のみです。

ステップ 2 コマンド **passwd** を入力します。

新しいパスワードの入力を求められます。

ステップ 3 新しいパスワードを入力し、プロンプトが表示されたらパスワードを再入力します。

ステップ 4 **exit** と入力して root アカウントからログアウトします。

SSH を使用した root アカウントへのアクセス

（注）
- root アカウントへは、シリアル接続または SSH でのみアクセスできます。
- SSH を使用してログインしているときに SSH アクセスを無効にした場合、現在のセッションはログアウトするまではアクティブですが、その後の SSH アクセスは拒否されます。

SSH を使用して root アカウントへのアクセスを有効または無効にすることができます。

ステップ 1 **root** としてシステムにログインします。

ステップ 2 次のいずれかのコマンドを入力します。

- rootaccess --ssh on**rootaccess --ssh on**：SSH を使用したアクセスを有効にします。
- **rootaccess --ssh off**：SSH を使用したアクセスを無効にします。

ステップ 3 **exit** と入力して root アカウントからログアウトします。

Pwrec アカウントのパスワード設定

X14.0 リリース時点では、コマンドライン インターフェイスからのみ pwrec アカウントのパスワードを設定できます。

重要 パスワードを設定すると、アカウントには常にパスワードが必要になります。現在、パスワードをリセットする方法はありません。

パスワードを設定するには、次の手順を実行します。

- SSH または物理アプライアンスを介して root としてログインします。
- 「pwrec のパスワード」を使用してパスワードを設定します。
- 新しいパスワードを入力したら確認用パスワードを入力するよう求められます。

- 両方のパスワードがメッセージに一致する場合は、「「passwd: password updated successfully」」と表示されます。
  - パスワードがメッセージと一致しない場合は、「Sorry 「, passwords don't match」」というメッセージが表示されます。

SSO トークンの管理

（注） このページは、**[OAuth トークンによる承認（Authorize by OAuth token）]** で設定された標準 OAuth トークンに適用されます。自己記述 OAuth トークン（[OAuth トークンによる承認（更新あり）（Authorize by OAuth token with refresh）] で設定）には適用されません。

1. **現在 SSO トークンを保持しているユーザのリストを表示**：SSO トークンを保持しているユーザのリストを表示するには、**[ユーザ（Users）]** > **[SSO トークンを保持しているユーザ（SSO token holders）]**のリストを表示します。このページは、特定のユーザのシングルサイオンに関連するトラブルシューティングに役立ちます。
2. **すべての所有者からのトークンの削除**：このページを使用して、**すべての所有者からトークンを削除**することもできます。このオプションはユーザへ中断を余儀なくする可能性があるため、続行する前にその必要性を確認してください。たとえば、セキュリティの侵害を認識している、または内部インフラストラクチャやエッジインフラストラクチャをアップグレードする場合は必要である可能性があります。

特定のユーザのトークン管理

ステップ 1 [任意] 小型のリストを返すようにユーザ名のサブストリングをフィルタリングします。

リスト内に多くのリストがあり、その長いリストが複数ページに及び、それぞれのページに最大 200 のユーザ名がある場合にこれが必要なことがあります。

ステップ 2 ユーザ名をクリックすると、そのユーザが所有するトークンの詳細を表示できます。

[ユーザ **<Username>** の ***SSO* トークン（*SSO tokens for user*）**] ページが表示されます。このページにはそのユーザに発行されたトークンの詳細のリストが表示されます。詳細には、トークンの発行者と有効期限が含まれています。

ステップ 3 （任意）UC サービスへのアクセスを続行する前にユーザの ID を確認する場合は、**[これらのトークンの削除（Delete these tokens）]** をクリックします。

ユーザのクライアントがこの Expressway-C を介して UC サービスに次回アクセスすると、クライアントは新しい署名付き要求を使用して IdP にリダイレクトされます。ユーザは Expressway-C に ID をアサートで

きるように IdP で再認証する必要があることがあります。ユーザは、承認された新しいトークンを使用して発行することができます。

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。