ユーザーアクセスと認証の設定

vManage NMS のユーザーおよびユーザーグループを追加、編集、表示、または削除するには、[Manage Users] 画面を使用します。

[admin] ユーザーとしてログインしているユーザー、または [Manage Users] 書き込み権限を持つユーザーだけが、vManage NMS のユーザーおよびユーザーグループを追加、編集、または削除できます。

強化されたパスワードの設定

表 *1:* 機能の履歴

機能名	リリース情報	説明
強化されたパスワード	Cisco IOS XE リリース 17.3.1a Cisco vManage リリース 20.3.1	この機能により、Cisco vManage でパスワードポリシールールが有効になります。パスワードポリシールールが有効になると、Cisco vManage では強力なパスワードの使用が強制されます。
	Cisco IOS XE リリース 17.9.1a Cisco vManage リリース 20.9.1	この機能を使用すると、事前定義された中程度のセキュリティまたは高セキュリティのパスワード条件を適用するように Cisco vManage を設定できます。

強力なパスワードの強制

強力なパスワードの使用を推奨します。強力なパスワードの使用を強制するには、Cisco vManage でパスワードポリシールールを有効にする必要があります。

パスワードポリシールールを有効にした後は、新しいユーザー用に作成されるパスワードはルールで定義されている要件を満たす必要があります。さらに、Cisco vManage リリース 20.9.1 以降のリリースでは、既存のパスワードがルールで定義されている要件を満たしていない場合、次回のログイン時にパスワードを変更するように求められます。

1. Cisco vManage のメニューで、**[Administration]** > **[Settings]** を選択します。
2. [Password Policy] で、[Edit] を選択します。
3. Cisco vManage リリースに基づいて、次のいずれかのアクションを実行します。
   - Cisco vManage リリース 20.9.1 より前のリリースの場合は、[Enabled] をクリックします。
   - Cisco vManage リリース 20.9.1 以降のリリースの場合は、[Medium Security] または [High Security] をクリックしてパスワード条件を選択します。

   デフォルトでは、[Password Policy] は [Disabled] に設定されています。
4. [Password Expiration Time (Days)] フィールドで、パスワードが期限切れになるまでの日数を指定できます。

デフォルトでは、パスワードの有効期限は 90 日です。

パスワードの有効期限が切れる前に、パスワードの変更を求めるバナーが表示されます。パスワードの有効期限が 60 日以上の場合、このバナーはパスワードの有効期限が切れる 30 日前に最初に表示されます。パスワードの有効期限が 60 日未満の場合、このバナーは、有効期限に設定されている日数の半分の時点で最初に表示されます。有効期限が切れる前にパスワードを変更しないと、ログインがブロックされます。このようなシナリオでは、管理者ユーザーがパスワードを変更してアクセスを復元できます。

（注） パスワード有効期限ポリシーは、admin ユーザーには適用されません。

5. [Save] をクリックします。

パスワード要件

Cisco vManage では、パスワードポリシールールを有効にすると、次のパスワード要件が適用されます。

- 次のパスワード要件は、Cisco vManage リリース 20.9.1 より前のリリースに適用されます。
  - 8 文字以上、32 文字以下。
  - 少なくとも 1 つの大文字を含む。
  - 少なくとも 1 つの小文字を含む。
  - 少なくとも 1 つの数字を含む。
  - 次の特殊文字のうち少なくとも 1 つを含む必要があります。# ? ! @ $ % ^ & * -。
  - ユーザーのフルネームまたはユーザー名を含まない。
  - 以前に使用したパスワードを再利用しない。
  - パスワード内の少なくとも 4 つの位置に異なる文字を含む。
- 最小リリース：Cisco IOS XE リリース 17.9.1a、Cisco vManage リリース 20.9.1：

パスワード条件	要件
中レベルセキュリティ	• 最低 8 文字を含む • 32 文字以下にする • 少なくとも 1 つの小文字を含む • 少なくとも 1 つの大文字を含む • 少なくとも 1 つの数字を含む • 次の特殊文字を少なくとも 1 つ含む：# ? ! @ $ % ^ & * - • 最近使用した 5 つのパスワードのいずれかと同じではない • ユーザーのフルネームまたはユーザー名を含まない
高レベルセキュリティ	• 最低 15 文字を含む • 32 文字以下にする • 少なくとも 1 つの小文字を含む • 少なくとも 1 つの大文字を含む • 少なくとも 1 つの数字を含む • 次の特殊文字を少なくとも 1 つ含む：# ? ! @ $ % ^ & * - • 最近使用した 5 つのパスワードのいずれかと同じではない • ユーザーのフルネームまたはユーザー名を含まない • 少なくとも 8 文字が古いパスワードと同じ位置にない

許可されるパスワード試行回数

アカウントがロックされるまでに、パスワード入力を連続して 5 回まで試行できます。パスワード試行に 6 回失敗すると、15 分間ロックアウトされます。7 回目の試行で正しくないパスワードを入力すると、ログインが許可されず、15 分のロックタイマーが再び開始されます。

アカウントがロックされたら、アカウントが自動的にロック解除されるまで 15 分間待ってください。または、管理者に連絡してパスワードをリセットするか、管理者にアカウントのロック解除を依頼してください。

（注） パスワードを複数回入力しなかった場合も、アカウントはロックされます。パスワードフィールドに何も入力しない場合、パスワードは無効または正しくないと見なされます。

パスワード変更ポリシー

（注） 強力なパスワードを有効にするには、パスワードポリシールールが有効になっている必要があります。詳細については、強力なパスワードの強制 （2 ページ）を参照してください。

パスワードをリセットするときは、新しいパスワードを設定する必要があります。古いパスワードを使用してパスワードをリセットすることはできません。

（注） Cisco vManage リリース 20.6.4、および Cisco vManage リリース 20.9.1 以降のリリースでは、ログアウトしたユーザー、またはローカルまたはリモート TACACS サーバーでパスワードが変更されたユーザーは、古いパスワードを使用してログインすることはできません。ユーザーは、新しいパスワードを使用してのみ、ログインできます。

ロックされたユーザーのリセット

ユーザーがパスワードを複数回試行した後にロックされた場合、必要な権限を持つ管理者は、このユーザーのパスワードを更新できます。

ユーザーアカウントのロック解除には、パスワードの変更とユーザーアカウントのロック解除の 2 つの方法があります。

（注） この操作を実行できるのは、**netadmin** ユーザーまたは User Management Write ロールを持つユーザーだけです。

ロックされたユーザーのパスワードをリセットするには、次の手順に従います。

1. [Users]（**[Administration]** > **[Manage Users]**）で、ロックを解除するアカウントを持つユーザーをリストから選択します。
2. **[. . .]** をクリックし、[Reset Locked User] を選択します。
3. [OK] をクリックして、ロックされたユーザーのパスワードをリセットすることを確認します。この操作は取り消すことができないので、注意が必要です。

   または、[Cancel] をクリックして操作をキャンセルできます。

CLI を使用したロックされたユーザーのリセット

次のように CLI を使用して、ロックされたユーザーをリセットできます。

1. admin ユーザーとしてデバイスにログインします。
2. 次のコマンドを実行します。

   ```
   デバイス# request aaa unlock-user username
   ```
3. プロンプトが表示されたら、ユーザーの新しいパスワードを入力します。

ユーザの管理

Cisco vManage のメニューで、**[Administration]** > **[Manage Users]** を選択し、ユーザーおよびユーザーグループを追加、編集、表示、または削除します。

次の点に注意してください。

- **admin** ユーザーとしてログインしているユーザー、または [Manage Users] 書き込み権限を持つユーザーだけが、Cisco vManage のユーザーおよびユーザーグループを追加、編集、または削除できます。
- 各ユーザーグループには、このセクションに示されている機能の読み取りまたは書き込み権限を付与できます。書き込み権限には読み取り権限が含まれます。
- すべてのユーザーグループが、選択された読み取りまたは書き込み権限に関係なく、Cisco vManage ダッシュボードに表示される情報を確認できます。

表 *2:* ユーザーグループ権限：*Cisco IOS XE SD-WAN* デバイス

機能	読み取り権限	書き込み権限
アラーム	**[Monitor]** > **[Logs]** > **[Alarms]** ページで、アラームフィルタを設定し、デバイスで生成されたアラームを表示します。 Cisco vManage リリース 20.6.x 以前のリリース：**[Monitor]** > **[Alarms]** ページで、アラームフィルタを設定し、デバイスで生成されたアラームを表示します。	追加の権限はありません。

機能	読み取り権限	書き込み権限
監査ログ	**[Monitor]** > **[Logs]** > **[Alarms]** ページと **[Monitor]** > **[Logs]** > **[Audit Log]** ページで、監査ログフィルタを設定し、デバイスのすべてのアクティビティに関するログを表示します。 Cisco vManage リリース 20.6.x 以前のリリース：**[Monitor]** > **[Alarms]** ページと **[Monitor]** > **[Audit Log]** ページで、監査ログフィルタを設定し、デバイスのすべてのアクティビティに関するログを表示します。	追加の権限はありません。
証明書	**[Configuration]** > **[Certificates]** > **[WAN Edge List]** で、オーバーレイネットワーク内のデバイスのリストを表示します。 **[Configuration]** > **[Certificates]** > **[Controllers]** ウィンドウで、証明書署名要求（CSR）と証明書を表示します。	**[Configuration]** > **[Certificates]** > **[WAN Edge List]** ウィンドウで、デバイスを検証および無効化し、デバイスをステージングし、有効なコントローラデバイスのシリアル番号を Cisco vBond オーケストレーション に送信します。 **[Configuration]** > **[Certificates]** > **[Controllers]** ウィンドウで、CSR を生成し、署名付き証明書をインストールし、RSA キーペアをリセットし、コントローラデバイスを無効化します。

機能	読み取り権限	書き込み権限
CLI アドオンテンプレート （サポート対象の最小リリース：Cisco vManage リリース 20.7.1）	**[Configuration]** > **[Templates]** ウィンドウで CLI アドオン機能テンプレートを表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** ウィンドウで、CLI アドオン機能テンプレートを作成、編集、削除、およびコピーします。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。 （注） このオプションの詳細については、機能テンプレートの詳細な RBAC に関する情報を参照してください。
Cloud OnRamp	**[Configuration]** > **[Cloud OnRamp for SaaS]** および **[Configuration]** > **[Cloud OnRamp for IaaS]** ウィンドウでクラウドアプリケーションを表示します。	追加の権限はありません。
[Cluster]	**[Administration]** > **[Cluster Management]** ウィンドウで、Cisco vManage で動作中のサービス、Cisco vManage サーバーに接続されているデバイスのリスト、およびクラスタ内のすべての Cisco vManage サーバーで使用可能なサービスと動作中のサービスに関する情報を表示します。	**[Administration]** > **[Cluster Management]** ウィンドウで、現在の Cisco vManage の IP アドレスを変更し、Cisco vManage サーバーをクラスタに追加し、統計データベースを設定し、クラスタの Cisco vManage サーバーを編集および削除します。
コロケーション	**[Configuration]** > **[Cloud OnRamp for Colocation]** ウィンドウでクラウドアプリケーションを表示します。	追加の権限はありません。

機能	読み取り権限	書き込み権限
[Config Group] > **[Device]** > **[Deploy]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	この権限では、機能は提供されません。	設定を Cisco IOS XE SD-WAN デバイス に展開します。 （注） 既存の機能設定を編集するには、[Template Configuration] の書き込み権限が必要です。
デバイス CLI テンプレート （サポート対象の最小リリース：Cisco vManage リリース 20.7.1）	**[Configuration]** > **[Templates]** ウィンドウでデバイス CLI テンプレートを表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** ウィンドウで、デバイス CLI テンプレートを作成、編集、削除、およびコピーします。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。 （注） このオプションの詳細については、機能テンプレートの詳細な RBAC に関する情報を参照してください。

機能	読み取り権限	書き込み権限
デバイス インベントリ	**[Configuration]** > **[Devices]** > **[WAN Edge List]** ウィンドウで、デバイスの実行中の設定とローカル設定、テンプレートアクティビティのログ、およびデバイスへの設定テンプレート適用のステータスを表示します。 **[Configuration]** > **[Devices]** > **[Controllers]** ウィンドウで、デバイスの実行中の設定とローカル設定や、コントローラデバイスへの設定テンプレート適用のステータスを表示します。	**[Configuration]** > **[Devices]** > **[WAN Edge List]** ウィンドウで、デバイスの許可済みシリアル番号ファイルを Cisco vManage にアップロードし、デバイスを Cisco vManage 設定モードから CLI モードに切り替え、デバイス設定をコピーし、ネットワークからデバイスを削除します。 **[Configuration]** > **[Devices]** > **[Controllers]** ウィンドウで、オーバーレイネットワークのコントローラデバイスを追加および削除し、コントローラデバイスの IP アドレスとログイン情報を編集します。

機能	読み取り権限	書き込み権限
デバイスのモニタリング	**[Monitor]** > **[Geography]** ウィンドウで、デバイスの地理的な位置を表示します。 **[Monitor]** > **[Logs]** > **[Events]** ページで、デバイスで発生したイベントを表示します。 Cisco vManage リリース 20.6.x 以前のリリース：**[Monitor]** > **[Events]** ページで、デバイスで発生したイベントを表示します。 **[Monitor]** > **[Devices]** ページで（デバイスが選択されている場合のみ）、ネットワーク内のデバイスのリストを、デバイスステータスの概要、SD-WAN Application Intelligence Engine（SAIE）および Cflowd フロー情報、トランスポートロケーション（TLOC）ロス、遅延、およびジッター情報、制御およびトンネル接続、システムステータス、ならびにイベントとともに表示します。 （注） Cisco vManage リリース 20.7.x 以前では、SAIE フローはディープパケットインスペクション（DPI）フローと呼ばれていました。 Cisco vManage リリース 20.6.x 以前のリリース：デバイス情報は **[Monitor]** > **[Network]** ページに表示されます。	**[Monitor]** > **[Devices]** ページで（デバイスが選択されている場合のみ）、デバイスを ping し、トレースルートを実行し、IP パケットのトラフィックパスを分析します。

機能	読み取り権限	書き込み権限
デバイス リブート	**[Maintenance]** > **[Device Reboot]** ウィンドウで、再起動操作を実行できるデバイスのリストを表示します。	**[Maintenance]** > **[Device Reboot]** ウィンドウで、1 つまたは複数のデバイスを再起動します。
ディザスタ リカバリ	**[Administration]** > **[Disaster Recovery]** ウィンドウで、Cisco vManage 上で実行されているアクティブクラスタとスタンバイクラスタに関する情報を表示します。	追加の権限はありません。
[Event]	**[Monitor]** > **[Logs]** > **[Events]** ページで、デバイスの地理的な位置を表示します。 **[Monitor]** > **[Events]** ページで、デバイスの地理的な位置を表示します。	**[Monitor]** > **[Logs]** > **[Events]** ページで（デバイスが選択されている場合のみ）、デバイスを ping し、トレースルートを実行し、IP パケットのトラフィックパスを分析します。
[Feature Profile] > **[Other]** > **[Thousandeyes]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Other Profile] セクションで [ThousandEyes] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Other Profile] セクションで [ThousandEyes] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Service]** > **[Dhcp]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Service Profile] セクションで [DHCP] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Service Profile] セクションで [DHCP] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[Service]** > **[Lan/Vpn]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Service Profile] セクションで [LAN/VPN] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Service Profile] セクションで [LAN/VPN] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Service]** > **[Lan/Vpn/Interface/Ethernet]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Service Profile] セクションで [Ethernet Interface] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Service Profile] セクションで [Ethernet Interface] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Service]** > **[Lan/Vpn/Interface/Svi]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Service Profile] セクションで [SVI Interface] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Service Profile] セクションで [SVI Interface] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[Service]** > **[Routing/Bgp]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Service Profile] セクションで [Routing/BGP] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Service Profile] セクションで [Routing/BGP] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Service]** > **[Routing/Ospf]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Service Profile] セクションで [Routing/OSPF] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Service Profile] セクションで [Routing/OSPF] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Service]** > **[Switchport]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Service Profile] セクションで [Switchport] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Service Profile] セクションで [Switchport] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[Service]** > **[Wirelesslan]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Service Profile] セクションで [Wireless LAN] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Service Profile] セクションで [Wireless LAN] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[System]** > **[Interface/Ethernet]** > **[Aaa]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [AAA] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [AAA] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[System]** > **[Interface/Ethernet]** > **[Banner]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [Banner] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [Banner] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[System]** > **[Basic]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [Basic] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [Basic] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[System]** > **[Bfd]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [BFD] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [BFD] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[System]** > **[Global]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [Global] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [Global] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[System]** > **[Logging]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [Logging] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [Logging] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[System]** > **[Ntp]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [NTP] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [NTP] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[System]** > **[Omp]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [OMP] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [OMP] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[System]** > **[Snmp]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [System Profile] セクションで [SNMP] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [System Profile] セクションで [SNMP] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Transport]** > **[Cellular Controller]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Transport & Management Profile] セクションで [Cellular Controller] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Transport & Management Profile] セクションで [Cellular Controller] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Transport]** > **[Cellular Profile]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > **（設定グループを表示する）** ページの [Transport & Management Profile] セクションで [Cellular Profile] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > **（設定グループを追加または編集する）** ページの [Transport & Management Profile] セクションで [Cellular Profile] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[Transport]** > **[Management/Vpn]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > （設定グループを表示する）ページの [Transport & Management Profile] セクションで [Management VPN] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > （設定グループを追加または編集する）ページの [Transport & Management Profile] セクションで [Management VPN] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Transport]** > **[Management/Vpn/Interface/Ethernet]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > （設定グループを表示する）ページの [Transport & Management Profile] セクションで [Management Ethernet Interface] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > （設定グループを追加または編集する）ページの [Transport & Management Profile] セクションで [Management VPN and Management Internet Interface] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Transport]** > **[Routing/Bgp]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > （設定グループを表示する）ページの [Transport & Management Profile] セクションで [BGP Routing] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > （設定グループを追加または編集する）ページの [Transport & Management Profile] セクションで [BGP Routing] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[Transport]** > **[Tracker]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > （**設定グループを表示する**）ページの [Transport & Management Profile] セクションで [Tracker] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > （**設定グループを追加または編集する**）ページの [Transport & Management Profile] セクションで [Tracker] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Transport]** > **[Wan/Vpn]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > （**設定グループを表示する**）ページの [Transport & Management Profile] セクションで [Wan/Vpn] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > （**設定グループを追加または編集する**）ページの [Transport & Management Profile] セクションで [Wan/Vpn] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
[Feature Profile] > **[Transport]** > **[Wan/Vpn/Interface/Cellular]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** > （**設定グループを表示する**）ページの [Transport & Management Profile] セクションで [Wan/Vpn/Interface/Cellular] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** > （**設定グループを追加または編集する**）ページの [Transport & Management Profile] セクションで [Wan/Vpn/Interface/Cellular] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。

機能	読み取り権限	書き込み権限
[Feature Profile] > **[Transport]** > **[Wan/Vpn/Interface/Ethernet]** （サポート対象の最小リリース：Cisco vManage リリース 20.9.1）	**[Configuration]** > **[Templates]** >（設定グループを表示する）ページの [Transport & Management Profile] セクションで [Wan/Vpn/Interface/Ethernet] 設定を表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** >（設定グループを追加または編集する）ページの [Transport & Management Profile] セクションで [Wan/Vpn/Interface/Ethernet] 設定を作成、編集および削除します。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。
統合管理	**[Administration]** > **[Integration Management]** ウィンドウで、Cisco vManage で実行中のコントローラに関する情報を表示します。	追加の権限はありません。
ライセンス管理	**[Administration]** > **[License Management]** ウィンドウで、Cisco vManage で実行中のデバイスのライセンス情報を表示します。	**[Administration]** > **[License Management]** ページで、Cisco スマートアカウントの使用を設定し、管理するライセンスを選択して、Cisco vManage とライセンスサーバー間でライセンス情報を同期します。
インターフェイス（**Interface**）	**[Monitor]** > **[Network]** > **[Interface]** ページで、デバイスのインターフェイスに関する情報を表示します。 Cisco vManage リリース 20.6.x 以前のリリース：デバイスのインターフェイスに関する情報は **[Monitor]** > **[Network]** > **[Interface]** ページに表示されます。	**[Monitor]** > **[Devices]** > **[Interface]** ページで、[Chart Options] を編集して、表示するデータのタイプを選択し、データを表示する期間を編集します。

機能	読み取り権限	書き込み権限
ユーザーの管理	**[Administration]** > **[Manage Users]** ウィンドウで、ユーザーとユーザーグループを表示します。	**[Administration]** > **[Manage Users]** ウィンドウで、Cisco vManage のユーザーとユーザーグループを追加、編集、および削除し、ユーザーグループの権限を編集します。
その他の機能テンプレート （サポート対象の最小リリース：Cisco vManage リリース 20.7.1）	**[Configuration]** > **[Templates]** ウィンドウで、SIG 機能テンプレート、SIG ログイン情報テンプレート、および CLI アドオン機能テンプレートを除くすべての機能テンプレートを表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** ウィンドウで、SIG 機能テンプレート、SIG ログイン情報テンプレート、および CLI アドオン機能テンプレートを除くすべての機能テンプレートを作成、編集、削除、およびコピーします。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。 （注） このオプションの詳細については、機能テンプレートの詳細な RBAC に関する情報を参照してください。
ポリシー	**[Configuration]** > **[Policies]** ウィンドウで、ネットワーク内のすべての Cisco vSmart コントローラ またはデバイスの共通ポリシーを表示します。	**[Configuration]** > **[Policies]** ウィンドウで、ネットワーク内のすべての Cisco vSmart コントローラ またはデバイスの共通ポリシーを作成、編集、および削除します。
ポリシーの設定	**[Configuration]** > **[Policies]** ウィンドウで、作成されたポリシーのリストとその詳細を表示します。	**[Configuration]** > **[Policies]** ウィンドウで、ネットワーク内のすべての Cisco vSmart コントローラ およびデバイスの共通ポリシーを作成、編集、および削除します。

機能	読み取り権限	書き込み権限
ポリシーの展開	**[Configuration]** > **[Policies]** ウィンドウで、ポリシーが適用されている Cisco vSmart コントローラ の現在のステータスを表示します。	**[Configuration]** > **[Policies]** ウィンドウで、ネットワーク内のすべての Cisco vManage サーバーの共通ポリシーをアクティブ化および非アクティブ化します。
RBAC VPN	**[Monitor]** > **[VPN]** ページで、ロールに基づいて VPN グループとセグメントを表示します。 Cisco vManage リリース 20.6.x 以前のリリース：**[Dashboard]** > **[VPN Dashboard]** ページで、ロールに基づいて VPN グループとセグメントを表示します。	**[Administration]** > **[VPN Groups]** ウィンドウで、Cisco vManage の VPN と VPN グループを追加、編集、および削除し、VPN グループの権限を編集します。
ルーティング	**[Monitor]** > **[Devices]** > **[Real-Time]** ページで、デバイスのリアルタイムルーティング情報を表示します。 Cisco vManage リリース 20.6.x 以前のリリース：デバイスのリアルタイムルーティングに関する情報は **[Monitor]** > **[Network]** > **[Real-Time]** ページに表示されます。	**[Monitor]** > **[Devices]** > **[Real-Time]** ページで、コマンドフィルタを追加して情報表示を迅速化させます。
セキュリティ	**[Configuration]** > **[Security]** ウィンドウで、セキュリティポリシーが適用されている Cisco vSmart コントローラ の現在のステータスを表示します。	**[Configuration]** > **[Security]** ウィンドウで、ネットワーク内のすべての Cisco vManage サーバーのセキュリティポリシーをアクティブ化および非アクティブ化します。
セキュリティポリシー設定	**[Configuration]** > **[Security]** > **[Add Security Policy]** ウィンドウで、ネットワーク内のすべての Cisco vManage サーバーの共通ポリシーをアクティブ化および非アクティブ化します。	**[Configuration]** > **[Security]** > **[Add Security Policy]** ウィンドウで、ネットワーク内のすべての Cisco vManage サーバーのセキュリティポリシーをアクティブ化および非アクティブ化します。

機能	読み取り権限	書き込み権限
セッション管理	**[Administration]** > **[Manage Users]** > **[User Sessions]** ウィンドウで、ユーザーセッションを表示します。	**[Administration]** > **[Manage Users]** > **[User Sessions]** ウィンドウで、Cisco vManage のユーザーとユーザーグループを追加、編集、および削除し、ユーザーセッションを編集します。
Settings	**[Administration]** > **[Settings]** ウィンドウで、組織名、Cisco vBond オーケストレーションの DNS または IP アドレス、証明書認証設定、デバイスに適用されているソフトウェアのバージョン、Cisco vManage のログインページのカスタムバナー、および統計情報を収集するための現在の設定を表示します。	**[Administration]** > **[Settings]** ウィンドウで、組織名、Cisco vBond オーケストレーションの DNS または IP アドレス、証明書認証設定、デバイスに適用されているソフトウェアのバージョン、Cisco vManage のログインページのカスタムバナー、および統計情報を収集するための現在の設定を編集し、Web サーバー証明書の証明書署名要求（CSR）を生成し、証明書をインストールします。
SIG テンプレート （サポート対象の最小リリース：Cisco vManage リリース 20.7.1）	**[Configuration]** > **[Templates]** ウィンドウで、SIG 機能テンプレートおよび SIG ログイン情報テンプレートを表示します。 （注） この操作には、[Template Configuration] の読み取り権限が必要です。	**[Configuration]** > **[Templates]** ウィンドウで、SIG 機能テンプレートおよび SIG ログイン情報テンプレートを作成、編集、削除、およびコピーします。 （注） この操作には、[Template Configuration] の書き込み権限が必要です。 （注） このオプションの詳細については、機能テンプレートの詳細な RBAC に関する情報を参照してください。

機能	読み取り権限	書き込み権限
ソフトウェアアップグレード	**[Maintenance]** > **[Software Upgrade]** ウィンドウで、デバイスのリスト、ソフトウェアアップグレードを実行できるCisco vManage のカスタムバナー、およびデバイスで実行されているソフトウェアの現在のバージョンを表示します。	**[Maintenance]** > **[Software Upgrade]** ウィンドウで、デバイスに新しいソフトウェアイメージをアップロードし、デバイスのソフトウェアイメージをアップグレード、アクティブ化、および削除し、ソフトウェアイメージをデバイスのデフォルトイメージに設定します。
システム	**[Configuration]** > **[Templates]** > **[Device Template]** ウィンドウで、Cisco vManage テンプレートを使用して設定されたシステム全体のパラメータを表示します。 （注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] は [Device] と呼ばれます。	**[Configuration]** > **[Templates]** > **[Device Template]** ウィンドウで、Cisco vManage テンプレートを使用して設定されたシステム全体のパラメータを設定します。 （注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] は [Device] と呼ばれます。
テンプレートの設定	**[Configuration]** > **[Templates]** ウィンドウで、機能テンプレートとデバイステンプレートを表示します。	**[Configuration]** > **[Templates]** ウィンドウで、機能テンプレートまたはデバイステンプレートを作成、編集、削除、およびコピーします。 （注） Cisco vManage リリース 20.7.1 以降、デバイスにすでにアタッチされているテンプレートを作成、編集、または削除するには、ユーザーに [Template Deploy] オプションに対する書き込み権限が必要です。

機能	読み取り権限	書き込み権限
テンプレートの展開	**[Configuration]** > **[Templates]** ウィンドウで、デバイステンプレートにアタッチされているデバイスを表示します。	**[Configuration]** > **[Templates]** ウィンドウで、デバイステンプレートにデバイスをアタッチします。
ツール	**[Tools]** > **[Operational Commands]** ウィンドウで、**admin tech** コマンドを使用してデバイスのシステムステータス情報を収集します。	**[Tools]** > **[Operational Commands]** ウィンドウで、**admin tech** コマンドを使用してデバイスのシステムステータス情報を収集し、**interface reset** コマンドを使用して 1 回の操作でデバイスのインターフェイスをシャットダウンして再起動します。 **[Tools]** > **[Operational Commands]** ウィンドウで、ネットワークを再検索して新しいデバイスを検出し、Cisco vManage と同期させます。 **[Tools]** > **[Operational Commands]** ウィンドウで、デバイスへの SSH セッションを確立し、CLI コマンドを発行します。
vAnalytics	**[Cisco vManage]** > **[vAnalytics]** ウィンドウで vAnalytics を起動します。	追加の権限はありません。
Workflows	**[Cisco vManage]** > **[Workflows]** ウィンドウからワークフローライブラリを起動します。	追加の権限はありません。

マルチテナント環境の RBAC ユーザーグループ

次の表に、マルチテナント環境でのロールベースアクセスコントロール（RBAC）のユーザーグループ権限のリストを示します。

- R は読み取り権限を表します。
- W は書き込み権限を表します。

表 *3:* マルチテナント環境の *RBAC* ユーザーグループ

機能	Provider Admin	Provider Operator	Tenant Admin	テナントのオペレータ
Cloud OnRamp	RW	R	RW	R
コロケーション	RW	R	RW	R
RBAC VPN	RW	R	RW	R
セキュリティ	RW	R	RW	R
セキュリティポリシー設定	RW	R	RW	R
vAnalytics	RW	R	RW	R

Add User

1. Cisco vManage メニューから **[Administration]** > **[Manage Users]** を選択します。
2. デフォルトでは、[Users] が選択されています。テーブルに、デバイスで設定されているユーザーのリストが表示されます。
3. 既存のユーザーのパスワードを編集、削除、または変更するには、[...] をクリックして、[Edit]、[Delete]、または [Change Password] をそれぞれクリックします。
4. 新規ユーザを追加するには、[Add User] をクリックします。
5. [Full Name]、[Username]、[Password]、および [Confirm Password] の各詳細情報を追加します
6. [User Groups] ドロップダウンリストで、ユーザーを追加するユーザーグループを選択します。
7. [Resource Group] ドロップダウンリストで、リソースグループを選択します。

（注） このフィールドは Cisco IOS XE リリース 17.5.1a 以降で利用できます。

8. [Add] をクリックします。

ユーザーの削除

ユーザーがデバイスにアクセスする必要がなくなった場合は、そのユーザーを削除できます。ユーザーがログインしている場合、そのユーザーを削除してもログアウトされません。

ユーザーを削除するには、次の手順を実行します。

1. Cisco vManage メニューから **[Administration]** > **[Manage Users]** を選択します。

2. 削除するユーザーの [...] をクリックし、[Delete] をクリックします。
3. ユーザーの削除を確認するには、[OK] をクリックします。

ユーザーの詳細の編集

ユーザーのログイン情報を更新したり、ユーザーグループのユーザーを追加または削除することができます。ログインしているユーザーの詳細情報を編集した場合、変更はそのユーザーがログアウトした後に有効になります。

ユーザーの詳細情報を編集するには、次のようにします。

1. Cisco vManage メニューから **[Administration]** > **[Manage Users]** を選択します。
2. 編集するユーザーの [...] をクリックし、[Edit] をクリックします。
3. ユーザーの詳細を編集します。

   ユーザーグループのユーザーを追加または削除することもできます。
4. [Update] をクリックします。

ユーザー パスワードの変更

必要に応じて、ユーザーのパスワードを更新できます。強力なパスワードの使用を推奨します。

はじめる前に

管理者ユーザーのパスワードを変更する場合は、この手順を実行する前に、クラスタ内のすべての Cisco vManage インスタンスからデバイステンプレートをアタッチ解除してください。この手順を完了した後、デバイステンプレートを再アタッチできます。

ユーザーのパスワードを変更するには、次の手順に従います。

1. Cisco vManage メニューから **[Administration]** > **[Manage Users]** を選択します。
2. パスワードを変更するユーザーの [...] をクリックし、[Change Password] をクリックします。
3. 新しいパスワードを入力し、それを確認します。

（注） 対象のユーザーがログインしている場合はログアウトされます。

4. [Done] をクリックします。

SSH セッションを使用してデバイスにログインしているユーザーの確認

1. Cisco vManage メニューから**[Monitor]** > **[Devices]**の順に選択します。

Cisco vManage リリース 20.6.x 以前：Cisco vManage メニューから**[Monitor]** > **[Network]**の順に選択します。

2. [Hostname] 列で、使用するデバイスを選択します。
3. [Real Time] をクリックします。
4. [Device Options] で、[AAA users]（Cisco IOS XE SD-WAN デバイス の場合）を選択します。

   このデバイスにログインしているユーザーのリストが表示されます。

HTTP セッションを使用してデバイスにログインしているユーザーの確認

1. Cisco vManage メニューから **[Administration]** > **[Manage Users]** を選択します。
2. [User Sessions] をクリックします。

   Cisco vManage 内のすべてのアクティブな HTTP セッションのリスト（ユーザー名、ドメイン、送信元 IP アドレスなどを含む）が表示されます。

CLI を使用したユーザーの設定

各デバイスでCLIを使用してユーザーログイン情報を設定できます。この方法により、追加のユーザーを作成し、それらのユーザーに特定のデバイスへのアクセス権を付与することが可能です。CLIを使用してユーザーのための作成するログイン情報は、そのユーザーのCisco vManageログイン情報とは異なるものにすることができます。また、デバイスごとに同じユーザーの異なるログイン情報を作成できます。**netadmin** 権限を持つすべての Cisco IOS XE SD-WAN デバイス ユーザーが、新しいユーザーを作成できます。

ユーザーアカウントを作成するには、ユーザー名とパスワードを設定し、ユーザーをグループに追加します。

次の例は、既存のグループへのユーザー Bob の追加を示しています。

```
デバイス(config)# system aaa user bob group basic
```

次の例は、新しいグループ `test-group` へのユーザー Alice の追加を示しています。

```
デバイス(config)# system aaa user test-group
デバイス(config)# system aaa user alice group test-group
```

ユーザー名の長さは 1 ー 128 文字で、先頭は英字にする必要があります。名前に使用できるのは、英小文字、0 ー 9 の数字、ハイフン（-）、下線（_）、ピリオド（.）のみです。英大文字は使用できません。一部のユーザー名は、予約されているために設定できません。予約済みユーザー名のリストについては、『Cisco SD-WAN Command Reference Guide』で **aaa** コンフィギュレーション コマンドを参照してください。

パスワードは、ユーザーのパスワードです。各ユーザー名にはパスワードが必要であり、ユーザーは自分のパスワードを変更できます。CLI では、文字列がすぐに暗号化され、パスワードは読み取り可能な形で表示されません。ユーザーには、 Cisco IOS XE SD-WAN デバイスにログインする際に、正しいパスワードの入力を 5 回試みることができます。5 回の試行で正しく

入力できなかった場合、そのユーザーはデバイスからロックアウトされ、再度ログインを試みるまでに 15 分間待つ必要があります。

（注） 特殊文字 ! を含むユーザーパスワードは二重引用符（" "）で囲みます。パスワード全体を二重引用符で囲まない場合、構成データベース（?）はこの特殊文字をスペースとして扱い、パスワードの残りの部分を無視します。

たとえば、パスワードが C!sc0 の場合は、"C!sc0" を使用します。

グループ名は、Cisco SD-WAN の標準グループの名前（**basic**、**netadmin**、または **operator**）か、 **usergroup** コマンド（後述）で設定されたグループの名前です。管理者ユーザーがグループを変更することによってユーザーの権限を変更する場合、そのユーザーは、そのときにデバイスにログインしているとログアウトされ、再度ログインする必要があります。

admin ユーザー名の工場出荷時のデフォルトパスワードは、admin です。 Cisco IOS XE SD-WAN デバイスを最初に設定するときに、このパスワードを変更することを強く推奨します。

```
デバイス(config)# username admin password
$9$3/IL3/UF2F2F3E$J9NKBeKlWrq9ExmHk6F5VAiDMOFQfD.QPAmMxDdxz.c
```

パスワードは、ASCII 文字列で設定します。次の例のように、CLI では、文字列がすぐに暗号化され、パスワードは読み取り可能な形で表示されません。

```
デバイス(config)# show run
...
aaa authentication login default local
aaa authentication login user1 group basic
aaa authentication login user2 group operator
aaa authentication login user3 group netadmin
aaa authorization exec default local
```

RADIUS を使用して AAA 認証を実行している場合は、パスワードを確認するように特定の RADIUS サーバーを設定できます。

```
デバイス(config)#  radius server tag
```

タグは、**radius server tag** コマンドで定義した文字列です（『Cisco SD-WAN Command Reference Guide』を参照）。

ユーザーグループの管理

ユーザーはグループに配置されます。グループは、ユーザーが表示および変更を許可されている特定の構成および操作コマンドを定義します。1 人のユーザーが 1 つ以上のグループに属することができます。Cisco SD-WAN ソフトウェアには標準ユーザーグループが用意されており、必要に応じてカスタムユーザーグループを作成できます。

- [basic]：インターフェイスおよびシステム情報を表示する権限を持つユーザーが含まれます。
- [netadmin]：Cisco vManage ですべての操作を実行できる管理者ユーザーがデフォルトで含まれます。このグループに他のユーザーを追加できます。

- [operator]：情報を表示する権限のみを持つユーザーを含みます。
- サポート対象の最小リリース：Cisco vManage リリース 20.9.1

  [network_operations]：非セキュリティポリシーの表示と変更、デバイステンプレートのアタッチとデタッチ、非セキュリティデータの監視など、セキュリティ以外の操作を Cisco vManage で実行できるユーザーが含まれます。
- サポート対象の最小リリース：Cisco vManage リリース 20.9.1

  [security_operations]：セキュリティポリシーの表示と変更、セキュリティデータの監視など、セキュリティ操作を Cisco vManage で実行できるユーザーが含まれます。

注：すべてのユーザーグループが、選択された読み取りまたは書き込み権限に関係なく、Cisco vManage ダッシュボードに表示される情報を確認できます。

ユーザーグループの削除

不要になったユーザーグループは削除できます。たとえば、特定のプロジェクト用に作成したユーザーグループを、そのプロジェクトの終了時に削除する場合があります。

1. Cisco vManage メニューから **[Administration]** > **[Manage Users]** を選択します。
2. **[User Groups]**をクリックします。
3. 削除するユーザーグループの名前をクリックします。

（注） デフォルトのユーザーグループ（basic、netadmin、operator、network_operations、security_operations）は削除できません。

4. [Trash] アイコンをクリックします。
5. ユーザーグループの削除を確認するには、[OK] をクリックします。

ユーザーグループ権限の編集

既存のユーザーグループのグループ権限を編集できます。この手順では、必要なユーザーグループの構成済み機能の読み取りおよび書き込みアクセス許可を変更できます。

1. Cisco vManage メニューから **[Administration]** > **[Manage Users]** を選択します。
2. **[User Groups]**をクリックします。
3. 権限を編集するユーザーグループの名前を選択します。

（注） デフォルトのユーザーグループ（basic、netadmin、operator、network_operations、security_operations）の権限は編集できません。

4. [Edit] をクリックし、必要に応じて権限を編集します。
5. **[Save]** をクリックします。

adminユーザーがグループを変更することによってユーザーの権限を変更する場合、そのユーザーは、そのときにデバイスにログインしているとログアウトされ、再度ログインする必要があります。

CLI を使用したグループの作成

Cisco SD-WAN ソフトウェアには、デフォルトのユーザーグループ（**basic**、**netadmin**、**operator**、**network_operations**、**security_operations**）が用意されています。ユーザー名 **admin** は自動的に **netadmin** ユーザーグループに配置されます。

必要に応じて、追加のカスタムグループを作成し、グループメンバーが持つ権限ロールを設定できます。特定の権限を持つカスタムグループを作成するには、グループ名と権限を設定します。

```
デバイス(config)# aaa authentication login user1 group radius enable
デバイス(config)# aaa authentication login user2 group radius enable
デバイス(config)# aaa authentication login user3 group radius enable
デバイス(config)#
```

group-name の長さは 1 ー 128 文字で、先頭は英字にする必要があります。名前に使用できるのは、英小文字、0 ー 9 の数字、ハイフン（-）、下線（_）、ピリオド（.）のみです。名前に大文字は使用できません。一部のグループ名は予約されているため、設定できません。それらのリストについては、aaa 設定コマンドを参照してください。

リモート RADIUS または TACACS+ サーバーが認証を検証しても、ユーザーグループを指定しない場合、ユーザーはユーザーグループ **basic** に配置されます。リモートサーバーが認証を検証し、VSA Cisco SD-WAN-Group-Name を使用してユーザーグループ（X とします）を指定する場合、ユーザーはそのユーザーグループのみに配置されます。ただし、そのユーザーがローカルにも設定され、ユーザーグループ（Y とします）に属している場合、ユーザーは両方のグループ（X と Y）に配置されます。

task オプションでは、グループメンバーが持つ権限ロールを一覧表示します。ロールは、**インターフェイス**、**ポリシー**、**ルーティング**、**セキュリティ**、および**システム**の 1 つ以上にすることができます。

Cisco vManage でのセッションの設定

表 *4 :* 機能の履歴

機能の履歴	リリース情報	説明
Cisco vManage でのセッションの設定	Cisco IOS XE リリース 17.3.1a Cisco vManage リリース 20.3.1	この機能を使用すると、Cisco vManage の内部で開いているすべての HTTP セッションを確認できます。ユーザー名、送信元 IP アドレス、ユーザーのドメイン、およびその他の情報の詳細が表示されます。ユーザー管理書き込みアクセス権を持つユーザー（netadmin ユーザー）は、疑わしいユーザーのセッションのログアウトをトリガーできます。

Cisco vManage でのクライアント セッション タイムアウトの設定

Cisco vManage でクライアント セッション タイムアウトを設定できます。タイムアウトが設定されている場合（キーボードまたはキーストロークアクティビティがないときのタイムアウトなど）、クライアントはシステムから自動的にログアウトされます。

（注） プロバイダーアクセスがある場合にのみ、マルチテナント環境でクライアント セッション タイムアウトを編集できます。

1. Cisco vManage のメニューから、**[Administration]** > **[Settings]** を選択します。
2. [Client Session Timeout] をクリックします。
3. [Edit] をクリックします。
4. [Enabled] をクリックします。
5. タイムアウト値を分単位で指定します。
6. [Save] をクリックします。

Cisco vManage でのセッションライフタイムの設定

セッションライフタイムを分単位で設定することにより、セッションをアクティブにしておく時間を指定できます。セッションライフタイムは、セッションをアクティブにしておくことができる時間を示します。セッションを期限切れにせずにアクティブなままにすると、デフォルトのセッションタイムアウト値である 24 時間後にセッションからログアウトされます。

デフォルトのセッションライフタイムは 1440 分間（24 時間）です。

（注） プロバイダーアクセスがある場合にのみ、マルチテナント環境でセッションライフタイムを編集できます。

1. Cisco vManage のメニューから、**[Administration]** > **[Settings]** を選択します。
2. [Session Life Time] をクリックします。
3. [Edit] をクリックします。
4. [SessionLifeTime] フィールドで、セッションタイムアウト値（分単位）をドロップダウンリストから指定します。
5. [Save] をクリックします。

Cisco vManage でのサーバー セッション タイムアウトの設定

Cisco vManage でサーバー セッション タイムアウトを設定できます。サーバー セッション タイムアウトは、非アクティブが原因で期限切れになるまでにサーバーがセッションの動作を維持する必要がある時間を示します。デフォルトのサーバー セッション タイムアウトは 30 分です。

（注） サーバー セッション タイムアウトは、プロバイダーアクセス権またはテナントアクセス権がある場合でも、マルチテナント環境では使用できません。

1. Cisco vManage のメニューから、**[Administration]** > **[Settings]** を選択します。
2. [Server Session Timeout] をクリックします。
3. [Edit] をクリックします。
4. [Timeout(minutes)] フィールドで、タイムアウト値を分単位で指定します。
5. [Save] をクリックします。

ユーザーあたりの最大セッション数の有効化

ユーザー名ごとに許可される同時HTTPセッションの最大数を有効にすることができます。値として 2 を入力する場合、2 つの同時 HTTP セッションのみを開くことができます。同じユーザー名で 3 つ目の HTTP セッションを開こうとすると、3 つ目のセッションにアクセス権が付与され、最も古いセッションがログアウトされます。

（注） ユーザーあたりの最大セッション数は、プロバイダーアクセス権またはテナントアクセス権がある場合でも、マルチテナント環境では使用できません。

1. Cisco vManage のメニューから、**[Administration]** > **[Settings]** を選択します。
2. [Max Sessions Per User] をクリックします。
3. [Edit] をクリックします。
4. [Enabled] をクリックします。

   デフォルトでは、[Max Sessions Per User] は [Disabled] に設定されています。
5. [Max Sessions Per User] フィールドで、ユーザーセッションの最大数の値を指定します。
6. [Save] をクリックします。

CLI を使用した RADIUS 認証の設定

Remote Authentication Dial-In User Service（RADIUS）は、無許可のアクセスに対してネットワークを保護する分散型クライアント/サーバーシステムです。RADIUS クライアントは RADIUS をサポートするシスコデバイス上で動作し、中央RADIUSサーバーに認証要求を送信します。RADIUS サーバーには、ユーザー認証情報とネットワーク サービス アクセス情報がすべて格納されます。

Cisco IOS XE SD-WAN デバイス でユーザー認証に RADIUS サーバーを使用するには、1 つまたは最大 8 つのサーバーを設定します。

```
デバイスconfig-transaction
デバイス(config)# radius server test address ipv4 10.1.1.55 acct-port 110
デバイス(config-radius-server)# key 33
デバイス(config-radius-server)# exit
デバイス(config)# radius server test address ipv4 10.1.1.55 auth-port 330
デバイス(config-radius-server)# key 55
デバイス(config-radius-server)#
```

RADIUS サーバーごとに、少なくともその IP アドレスとパスワードまたはキーを設定する必要があります。キーには、最大 31 文字のクリアテキスト文字列、または AES 128 ビット暗号化キーを指定できます。ローカルデバイスはキーをRADIUSサーバーに渡します。パスワードは、サーバーで使用されているものと一致する必要があります。複数のRADIUSサーバーを設定するには、サーバーごとに **server** コマンドと **secret-key** コマンドを使用します。

残りの RADIUS 設定パラメータはオプションです。

RADIUS サーバーの優先順位を設定する場合、複数の RADIUS サーバー間での選択または負荷分散の手段として、サーバーのプライオリティ値を設定します。優先順位には、0 から 7 までの値を指定できます。優先順位番号が小さいサーバーは、番号が大きいサーバーよりも優先されます。

デフォルトでは、 Cisco IOS XE SD-WAN デバイス は RADIUS サーバーへの認証接続にポート 1812 を使用し、アカウンティング接続にポート 1813 を使用します。これらのポート番号を変更するには、**auth-port** および **acct-port** コマンドを使用します。

特定のインターフェイスを介して RADIUS サーバーに到達できる場合は、**source-interface** コマンドを使用してそのインターフェイスを設定します。

特定のサーバーを AAA、IEEE 802.1X、および IEEE 802.11i の認証とアカウンティングに使用できるように、RADIUS サーバーにタグを付けることができます。ここで、4 ～ 16 文字の文字列でタグを定義します。次に、AAA を設定するとき、および 802.1X および 802.11i のインターフェイスを設定するときに、タグを **radius-servers** コマンドに関連付けます。

RADIUS サーバーが Cisco IOS XE SD-WAN デバイス とは異なる VPN にある場合は、サーバーの VPN 番号を設定して、 Cisco IOS XE SD-WAN デバイス が検出できるようにします。複数の RADIUS サーバーを設定する場合は、すべてが同じ VPN 内にある必要があります。

RADIUS サーバーからの応答を待機する場合、 Cisco IOS XE SD-WAN デバイス は 3 秒間待機してから要求を再送信します。この時間間隔を変更するには、**timeout** コマンドを使用して、1 ～ 1000 秒の値を設定します。

```
デバイス# config-transaction
 デバイス(config)# aaa group server radius server-10.99.144.201
 デバイス(config-sg-radius)# server-private 10.99.144.201 auth-port 1812 timeout 5
retransmit 3
```

SSH 認証の設定

表 *5:* 機能の履歴

機能名	リリース情報	説明
RSA キーを使用したセキュアシェル認証	Cisco IOS XE SD-WAN リリース 16.12.1b	この機能は、クライアントと Cisco SD-WAN サーバー間の通信を保護することにより、RSA キーを設定するのに役立ちます。

セキュアシェル（SSH）プロトコルは、ネットワークデバイスへの安全なリモートアクセス接続を提供します。

SSHは、公開鍵と秘密鍵を使用したユーザー認証をサポートしています。SSH認証を有効にするために、ユーザーの公開鍵は、次の場所にある認証ユーザーのホームディレクトリに保存されます。

```
~<user>/.ssh/authorized_keys
```

秘密鍵を所有するクライアントマシンで新しい鍵が生成されます。SSHサーバーの公開鍵を使用して暗号化されたメッセージは、クライアントの秘密鍵を使用して復号化されます。

Cisco SD-WAN での SSH 認証の制約事項

- Cisco IOS XE SD-WAN デバイス でサポートされる SSH RSA キーサイズの範囲は 2048 ～ 4096 です。1024 および 8192 の SSH RSA キーサイズはサポートされていません。
- Cisco IOS XE SD-WAN デバイス では、ユーザーごとに最大 2 つのキーを使用できます。

Cisco IOS XE SD-WAN デバイス での vManage を使用した SSH 認証

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [機能テンプレート] をクリックし、[テンプレートの追加] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前では、[Feature Templates] のタイトルは [Feature] です。

3. [Select Devices] で、テンプレートを作成するデバイスのタイプを選択します。
4. [Basic Information] から、[CISCO AAA] テンプレートを選択します。
5. [Local] から、[New User] をクリックし、詳細を入力します。
6. [SSH RSA Key] を入力します。

（注） [SSH RSA Key] の id_rsa.pub ファイルから完全な公開キーを入力する必要があります。

Cisco IOS XE SD-WAN デバイスで CLI を使用して SSH 認証を設定する

SSH キーベースのログインは、IOS でサポートされています。ユーザーごとに最大 2 つのキーをサポートできます。また、IOS は RSA ベースのキーのみをサポートします。

従来の IOS CLI では、次のサポートが可能です。

•キー文字列

• キーハッシュ：キー文字列は base64 でデコードされ、MD5 ハッシュが実行されます。

ただし、トランザクションヤンモデルには、（キー文字列全体ではなく）キーハッシュのみをコピーする規定があります。vManageはこの変換を行い、構成をデバイスにプッシュします。

Cisco IOS XE SD-WAN デバイス でサポートされる公開鍵

- SSH-RSA

認証順序の設定

認証順序では、SSH セッションまたはコンソールポートを介して Cisco IOS XE SD-WAN デバイスに対するユーザーアクセスを確認するときに認証方式が試行される順序を指示します。デフォルトの認証順序は、**local**、**radius**、**tacacs** の順です。デフォルトの認証順序では、認証プロセスは次の順序で実行されます。

- 認証プロセスでは、まず、ローカルデバイスの実行コンフィギュレーションにユーザー名と一致するパスワードが存在するかどうかがチェックされます。
- ローカル認証が失敗し、認証フォールバックを（**auth-fallback** コマンドで）設定していない場合、認証プロセスは停止します。しかし、認証フォールバックを設定している場合、認証プロセスは次に RADIUS サーバーをチェックします。この方法を機能させるには、**system radius server** コマンドを使用して 1 つ以上の RADIUS サーバーを設定する必要があります。RADIUS サーバーに到達できる場合、ユーザーはそのサーバーの RADIUS データベースに基づいて認証またはアクセス拒否されます。RADIUS サーバーに到達できず、複数の RADIUS サーバーを設定している場合、認証プロセスは各サーバーを順番にチェックし、そのうちの 1 つに到達できると停止します。その後、ユーザーは、そのサーバーの RADIUS データベースに基づいて認証またはアクセス拒否されます。
- RADIUS サーバーに到達できない（つまり、すべてのサーバーに到達できない）場合、認証プロセスは TACACS+ サーバーをチェックします。この方法を機能させるには、**system tacacs server** コマンドを使用して 1 つ以上の TACACS+ サーバーを設定する必要があります。TACACS+ サーバーに到達できる場合、ユーザーはそのサーバーの TACACS+ データベースに基づいて認証またはアクセス拒否されます。TACACS+ サーバーに到達できず、複数の TACACS+ サーバーを設定している場合、認証プロセスは各サーバーを順番にチェックし、そのうちの 1 つに到達できると停止します。その後、ユーザーは、そのサーバーの TACACS+ データベースに基づいて認証またはアクセス拒否されます。
- TACACS+ サーバーに到達できない場合（つまり、すべての TACACS+ サーバーに到達できない場合）、ローカル Cisco IOS XE SD-WAN デバイスへのユーザーアクセスは拒否されます。

最初に試行するものから優先順で、1 つ、2 つ、または 3 つの認証方法を指定します。認証方法を 1 つだけ設定する場合は、**ローカル**である必要があります。

このコマンドを含めない場合、「admin」ユーザーは常にローカルで認証されます。

第2または第3の認証メカニズムへのフォールバックは、ユーザーによって提供されたログイン情報が無効であるためか、サーバーに到達できないために、より優先度の高い認証サーバーがユーザーの認証に失敗したときに発生します。

次に、デフォルトの認証動作と、認証フォールバックが有効になっている場合の動作の例を示します。

- 認証順序が **radius local** として設定されている場合：
  - デフォルトの認証では、ローカル認証は、すべてのRADIUSサーバーに到達できない場合にのみ使用されます。RADIUS サーバーを介した認証の試行が失敗した場合、ユーザーは、ローカル認証に正しいログイン情報を提供した場合でも、ログインを許可されません。
  - 認証フォールバックを有効にすると、すべての RADIUS サーバーに到達できない場合、またはRADIUSサーバーがユーザーに対してアクセスを拒否した場合に、ローカル認証が使用されます。
- 認証順序が **local radius** として設定されている場合：
  - デフォルトの認証では、ローカルデバイスの実行コンフィギュレーションにユーザー名と一致するパスワードが存在しない場合、RADIUS 認証が試行されます。
  - 認証フォールバックを有効にすると、ローカルデバイスの実行コンフィギュレーションにユーザー名と一致するパスワードが存在しない場合に、RADIUS認証が試行されます。この場合、2 つの認証方式の動作は同じです。
- 認証順序が **radius tacacs local** として設定されている場合：
  - デフォルトの認証では、すべての RADIUS サーバーに到達できない場合にのみ TACACS+ が試行され、すべてのTACACS+サーバーに到達できない場合にのみ、ローカル認証が試行されます。RADIUS サーバーを介した認証の試行が失敗した場合、ユーザーは、TACACS+ サーバーに正しいログイン情報を提供した場合でも、ログインを許可されません。同様に、TACACS+ サーバーがアクセスを拒否した場合、ユーザーはローカル認証を介してログインできません。
  - 認証フォールバックを有効にすると、すべての RADIUS サーバーに到達できない場合、またはRADIUSサーバーがユーザーのアクセスを拒否した場合に、TACACS+ 認証が使用されます。続いて、すべてのTACACS+サーバーに到達できない場合、またはTACACS+サーバーがユーザーに対してアクセスを拒否した場合に、ローカル認証が使用されます。

リモートサーバーが認証を検証しても、ユーザーグループを指定しない場合、ユーザーはユーザーグループ **basic** に配置されます。

リモートサーバーが認証を検証し、ユーザーグループ（X とします）を指定する場合、ユーザーはそのユーザーグループのみに配置されます。ただし、そのユーザーがローカルにも設定され、ユーザーグループ（Y とします）に属している場合、ユーザーは両方のグループ（X と Y）に配置されます。

リモートサーバーが認証を検証し、そのユーザーがローカルに設定されていない場合、ユーザーは、**basic** ユーザーとして vshell にログインし、ホームディレクトリは /home/basic になります。

リモートサーバーが認証を検証し、そのユーザーがローカルに設定されている場合、ユーザーはローカルユーザー名（たとえば、eve）で vshell にログインし、ホームディレクトリは /home/*username*（つまり、/home/eve）になります。

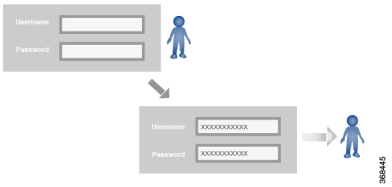
AAA を使用したロールベースアクセス

Cisco SD-WAN AAA ソフトウェアは、ロールベースのアクセスを実装して、Cisco IOS XE SD-WAN デバイス のユーザーの認可権限を制御します。ロールベースのアクセスは、次の 3 つのコンポーネントで構成されます。

- ユーザーは、Cisco IOS XE SD-WAN デバイス へのログインが許可されているユーザーです。
- ユーザーグループは、ユーザーのコレクションです。
- 権限は各グループに関連付けられています。これらは、グループのユーザーが発行を許可されているコマンドを定義します。

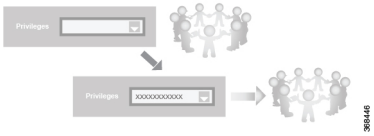
ユーザーとユーザーグループ

Cisco IOS XE SD-WAN デバイス での操作の実行が許可されているすべてのユーザーは、ログインアカウントを持っている必要があります。ログインアカウントについては、デバイス自体でユーザー名とパスワードを設定します。これらにより、ユーザーはそのデバイスにログインできます。ユーザーがアクセスを許可されている各デバイスで、ユーザー名とパスワードを設定する必要があります。



Cisco SD-WAN ソフトウェアは、UNIX スーパーユーザーと同様な、完全な管理者権限を持つユーザーである **admin** という 1 つの標準ユーザー名を提供します。デフォルトでは、**admin** ユーザー名のパスワードは**admin** です。このユーザー名を削除または変更することはできませんが、デフォルトのパスワードは変更できますし、変更する必要があります。

ユーザーグループは、Cisco IOS XE SD-WAN デバイス で共通のロールまたは権限を持つユーザーをプールします。ログインアカウント情報の構成の一環として、ユーザーがメンバーであるユーザーグループを指定します。**admin**ユーザーのグループを指定する必要はありません。このユーザーは自動的にユーザーグループ **netadmin** に属し、Cisco IOS XE SD-WAN デバイス でのすべての操作の実行が許可されるためです。



ユーザーグループ自体は、そのグループに関連付けられた権限を設定する場所です。これらの権限は、ユーザーが実行を許可されている特定のコマンドに対応し、Cisco SD-WAN ソフトウェア要素への役割ベースのアクセスを効果的に定義します。

Cisco SD-WAN ソフトウェアは、次の標準ユーザーグループを提供します。

- [basic]：[basic] グループは設定可能なグループであり、任意のユーザーおよび権限レベルに使用できます。このグループは、デバイス上の情報を表示および変更する権限を持つユーザーを含むように設計されています。
- [operator]：[operator] グループも設定可能なグループであり、任意のユーザーおよび権限レベルに使用できます。このグループは、情報を表示する権限のみを持つユーザーを含むように設計されています。
- [netadmin]：[netadmin] グループは設定不可能なグループです。デフォルトでは、このグループには**admin**ユーザーが含まれます。このグループに他のユーザーを追加できます。このグループのユーザーは、デバイスですべての操作を実行できます。
- サポート対象の最小リリース：Cisco vManage リリース 20.9.1

  [network_operations]：[network_operations] グループは設定不可能なグループです。このグループのユーザーは、デバイス上でセキュリティポリシー以外のすべての操作を実行でき、セキュリティポリシー情報は表示のみが可能です。たとえば、ユーザーはテンプレート設定を作成または変更し、災害復旧を管理し、アプリケーション対応ルーティングポリシーや CFlowD ポリシーなどの非セキュリティポリシーを作成できます。
- サポート対象の最小リリース：Cisco vManage リリース 20.9.1

  [security_operations]：[security_operations] グループは設定不可能なグループです。このグループのユーザーは、デバイス上ですべてのセキュリティ操作を実行でき、セキュリティポリシー以外の情報は表示のみが可能です。たとえば、ユーザーはUmbrellaキー、ライセンス、IPS 署名の自動更新、TLS/SSL プロキシ設定などを管理できます。

[network_operations] グループのユーザーは、デバイスへのポリシーの適用、適用されたポリシーの取り消し、およびデバイステンプレートの編集を許可されています。[security_operations] グループのユーザーは、デバイスにセキュリティポリシーを展開するために、[network_operations] ユーザーによる 0 日目の介入と、展開されたセキュリティポリシーを削除するために、N 日目の介入が必要です。ただし、セキュリティポリシーがデバイスに展開された後は、[security_operations] ユーザーは、[network_operations] ユーザーの介入を必要とせずにセキュリティポリシーを変更できます。

（注） 実行中の設定およびローカル設定を表示できるのは管理ユーザーのみです。事前定義された [operator] ユーザーグループに関連付けられたユーザーは、実行中の設定およびローカル設定にアクセスできません。事前定義されたユーザーグループ [operator] には、テンプレート設定の読み取りアクセスのみがあります。管理者ユーザー権限のサブセットのみが必要な場合は、機能リストから選択した機能を使用して、読み取りと書き込みの両方のアクセス権を持つ新しいユーザーグループを作成し、そのグループをカスタムユーザーに関連付ける必要があります。

ロールベースのアクセス権限

ロールベースのアクセス権限は、タスクと呼ばれる 5 つのカテゴリに分類されます。

- インターフェイス：Cisco IOS XE SD-WAN デバイス 上のインターフェイスを制御するための権限。
- ポリシー：コントロール プレーン ポリシー、OMP、およびデータプレーンポリシーを制御するための権限。
- ルーティング：BFD、BGP、OMP、OSPF などのルーティングプロトコルを制御するための権限。
- セキュリティ：ソフトウェアや証明書のインストールなど、デバイスのセキュリティを制御するための権限。[netadmin] グループに属するユーザーのみがシステムにソフトウェアをインストールできます。
- システム：一般的なシステム全体の権限。

次のセクションの表は、ユーザーおよびユーザーグループの AAA 認証ルールの詳細を示しています。これらの認証ルールは、CLI から発行されたコマンドと Netconf から発行されたコマンドに適用されます。

操作コマンドのユーザー認証ルール

操作コマンドのユーザー認証ルールは、ユーザー名のみに基づいています。Cisco IOS XE SD-WAN デバイス にログインできるユーザーは、ほとんどの操作コマンドを実行できます。ただし、ソフトウェアのインストールとアップグレード、デバイスのシャットダウンなど、デバイスの基本的な操作に影響を与えるコマンドを発行できるのは **admin** ユーザーだけです。

どのユーザーも **config** コマンドを発行して設定モードに入ることができ、設定モードに入ると、一般的な設定コマンドを発行できることに注意してください。また、すべてのユーザーは、**system aaa user** *self* **password** *password* コマンドを発行して、その設定変更をコミットすることにより、自分のパスワードを設定することができます。デバイスの動作を設定する実際のコマンドでは、ユーザーグループのメンバーシップに従って承認が定義されます。「設定コマンドのユーザーグループの認証ルール」を参照してください。

次の表に、一般的な CLI コマンドの AAA 認証ルールを示します。注記があるものを除き、すべてのコマンドは操作コマンドです。また、「admin」ユーザーが使用できる一部のコマンドは、そのユーザーが「netadmin」ユーザーグループに属している場合にのみ使用できます。

CLI コマンド	すべてのユーザー	管理者ユーザ
clear history	X	X
commit confirm	X	X
complete-on-space	X	X
config	X	X
exit	X	X
file	X	X
help	X	X
[no] history	X	X
idle-timeout	X	X
job	X	X
logout	—	X（netadmin グループのユーザーのみ）
monitor	X	X
nslookup	X	X
paginate	X	X
ping	X	X
poweroff	—	X（netadmin グループのユーザーのみ）
prompt1	X	X
prompt2	X	X
quit	X	X
reboot	—	X（netadmin グループのユーザーのみ）
request aaa request admin-tech request firmware request interface-reset request nms request reset request software	—	X（netadmin グループのユーザーのみ）
request execute request download request upload	X	X
request（その他すべて）	—	×

CLI コマンド	すべてのユーザー	管理者ユーザ
rollback（設定モードコマンド）	—	X（netadmin グループのユーザーのみ）
screen-length	X	X
screen-width	X	X
show cli	X	X
show configuration commit list	X	X
show history	X	X
show jobs	X	X
show parser dump	X	X
show running-config	X	X
show users	X	X
system aaa user self password password（設定モードコマンド）（注：ユーザーは自分自身を削除できません）		
tcpdump	X	X
timestamp	X	X
tools ip-route	X	X
tools netstat	X	X
tools nping	X	X
traceroute	X	X
vshell	X	X（netadmin グループのユーザーのみ）

操作コマンドのユーザーグループの認証ルール

操作コマンドのユーザーグループの認証ロールを次の表に示します。

操作コマンド	インターフェイス	ポリシー	ルーティング	セキュリティ	システム
clear app		X			
clear app-route		X			

操作コマンド	インターフェイス	ポリシー	ルーティング	セキュリティ	システム
clear arp	X				
clear bfd			X		X
clear bgp			X		X
clear bridge	X				
clear cellular	X				
clear control				X	
clear crash					X
clear dhcp					X
clear dns					X
clear igmp			X		
clear installed-certificates				X	
clear interface	X				
clear ip			X		
clear notification					X
clear omp			X		
clear orchestrator				X	
clear ospf			X		
clear pim			X		
clear policy		X			
clear pppoe	X				
clear system					X
clear tunnel				X	
clear wlan	X				
clear ztp				X	X
clock					X
debug bgp			X		

操作コマンド	インターフェイス	ポリシー	ルーティング	セキュリティ	システム
debug cellular	X				
debug cflowd		X			
debug chmgr					X
debug config-mgr					X
debug dhcp-client					X
debug dhcp-helper					X
debug dhcp-server					X
debug fpm		X			
debug ftm					X
debug igmp			X		
debug netconf					X
debug omp			X		
debug ospf			X		
debug pim			X		
debug resolver			X		
debug snmp					X
debug sysmgr					X
debug transport					X
debug ttm					X
debug vdaemon				X	X
debug vrrp				X	
debug wlan	X				
request certificate				X	
request control-tunnel				X	
request controller				X	
request controller-upload				X	

操作コマンド	インターフェイス	ポリシー	ルーティング	セキュリティ	システム
request csr				X	
request device				X	
request device-upload				X	
request on-vbond-controller				X	
request port-hop				X	
request root-cert-chain				X	
request security				X	
request vedge				X	
request vedge-upload				X	
request vsmart-upload				X	
show aaa					X
show app		X			
show app-route		X			
show arp	X				
show bfd			X		X
show bgp			X		
show boot-partition					X
show bridge	X				
show cellular	X				
show certificate				X	
show clock					X
show control				X	X
show crash					X
show debugs：debug コマンドと同じ					
show dhcp					X

操作コマンド	インターフェイス	ポリシー	ルーティング	セキュリティ	システム
show external-nat				X	X
show hardware					X
show igmp			X		
show interface	X				
show ip			X		X
show ipsec				X	
show licenses					X
show logging					X
show multicast			X		
show nms-server					X
show notification					X
show ntp					X
show omp		X	X		X
show orchestrator				X	
show ospf			X		
show pim			X		
show policer		X			
show policy		X			
show ppp	X				
show pppoe	X				
show reboot					X
show security-info				X	
show software					X
show system					X
show transport					X
show tunnel				X	
show uptime					X

操作コマンド	インターフェイス	ポリシー	ルーティング	セキュリティ	システム
show users					X
show version					X
show vrrp	X				
show wlan	X				
show ztp				X	

設定コマンドのユーザーグループの認証ルール

次の表に、設定コマンドのユーザーグループの認証ルールを示します。

コンフィギュレーション コマンド	インターフェイス	ポリシー	ルーティング	セキュリティ	システム
apply-policy		X			
banner					X
bfd			X		X
bridge	X				
[omp]		X	X		X
ポリシー		X			
security				X	X
snmp					X
system					X
vpn interface	X				
vpn ip			X		
vpn router			X		
vpn service			X		
vpn（作成、削除、命名を含むその他すべて）					X
wlan	X				

Cisco vManage テンプレートを使用した AAA の設定

表 *6:* 機能の履歴

機能名	リリース情報	説明
許可とアカウンティング	Cisco IOS XE リリース 17.5.1a Cisco vManage リリース 20.5.1	この機能では、許可（コマンドが実行される前に、ユーザーがデバイスに入力するコマンドを許可する）とアカウンティング（ユーザーがデバイスで実行するコマンドのレコードを生成する）を設定します。

Cisco vManage テンプレートを使用して AAA を設定すると、Cisco vManage で設定を行った後に、同じタイプの選択したデバイスにこの設定をプッシュできます。この手順は、同じタイプの複数のデバイスを一度に設定するのに便利な方法です。

Cisco vBond オーケストレーション、Cisco vManage インスタンス、Cisco vSmart コントローラ、および Cisco IOS XE SD-WAN デバイス には AAA テンプレートを使用します。

Cisco IOS XE SD-WAN デバイス では、RADIUS および TACACS+ と組み合わせた認証、許可、およびアカウンティング（AAA）の設定がサポートされます。

（注） PPP を使用している場合、または CHAP で MLPPP を使用している場合は、テンプレートを介して秘密鍵を使用してローカルユーザーを設定する必要があります。

[Template] 画面に移動しテンプレートを命名

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Device Templates] をクリックし、[Create Template] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] のタイトルは [Device] です。

3. [Create Template] ドロップダウンリストから、[From Feature Template] を選択します。
4. [Device Model] ドロップダウンリストから、テンプレートを作成するデバイスのタイプを選択します。
5. [Basic Information] を選択します。

6. AAA のカスタムテンプレートを作成するには、[Factory_Default_AAA_CISCO_Template] を選択し、[Create Template] をクリックします。AAA テンプレートフォームが表示されます。フォームの上部にはテンプレートに名前を付けるためのフィールドがあり、下部には AAA パラメータを定義するためのフィールドがあります。
7. [テンプレート名（Template Name）] フィールドに、テンプレートの名前を入力します。名前の最大長は 128 文字で、英数字のみを使用できます。
8. [Template Description] フィールドに、テンプレートの説明を入力します。説明の最大長は 2048 文字で、英数字のみを使用できます。

初めて機能テンプレートを開くと、デフォルト値を持つパラメータごとに、その範囲が [Default] に設定され（チェックマークで示される）、デフォルト設定またはデフォルト値が表示されます。デフォルト値を変更するか、値を入力するには、パラメータフィールドの左側にある [Scope] ドロップダウンリストをクリックし、次のいずれかを選択します。

表 *7:*

パラメータの範囲	範囲の説明
デバイス固有（ホストのアイコンで示される）	デバイス固有の値がパラメータに使用されます。デバイス固有のパラメータの場合、機能テンプレートに値を入力できません。Cisco IOS XE SD-WAN デバイス をデバイステンプレートにアタッチするときに、値を入力します。 [Device Specific] をクリックすると、[Enter Key] ボックスが表示されます。このボックスには、作成する CSV ファイル内のパラメータを識別する一意の文字列であるキーが表示されます。このファイルは、キーごとに 1 つの列を含む Excel スプレッドシートです。ヘッダー行にはキー名（行ごとに1つのキー）が含まれます。その後の各行は、デバイスに対応し、そのデバイスのキーの値を定義します。Cisco IOS XE SD-WAN デバイスをデバイステンプレートにアタッチするときに、この CSV ファイルをアップロードします。詳細については、「Create a Template Variables Spreadsheet」を参照してください。 デフォルトのキーを変更するには、新しい文字列を入力し、[Enter Key] ボックスの外にカーソルを移動します。 デバイス固有のパラメータの例としては、システム IP アドレス、ホスト名、GPS ロケーション、サイト ID などがあります。
グローバル（地球のアイコンで示される）	パラメータの値を入力し、その値をすべてのデバイスに適用します。 デバイスのグループにグローバルに適用できるパラメータの例としては、DNS サーバー、Syslog サーバー、インターフェイス MTU などがあります。

ユーザーとユーザーグループのローカルアクセスの設定

ユーザーおよびユーザーグループのデバイスへのローカルアクセスを設定できます。ローカルアクセスは、RADIUS または TACACS+ 認証が失敗した場合にデバイスへのアクセスを提供します。

個々のユーザーのローカルアクセスを構成するには、[Local] を選択します。

新しいユーザーを追加するには、[Local] から [+ New User] をクリックし、次のパラメータを設定します。

表 *8:*

パラメータ名	説明
Name	ユーザの名前を入力します。ユーザー名の長さは 1 ー 128 文字で、先頭は英字にする必要があります。名前に使用できるのは、英小文字、0 ー 9 の数字、ハイフン（-）、下線（_）、ピリオド（.）のみです。英大文字は使用できません。 次のユーザー名は予約されているため、設定できません。backup、basic、bin、daemon、games、gnats、irc、list、lp、mail、man、news、nobody、proxy、quagga、root、sshd、sync、sys、uucp、および www-data。また、viptela-reserved で始まる名前は予約されています。
パスワード	ユーザーのパスワードを入力します。 各ユーザー名にはパスワードが必要です。ユーザーは自分のパスワードを変更できます。 管理ユーザーのデフォルトパスワードは admin です。このパスワードから変更することを強く推奨します。 （注） Cisco vManage AAA テンプレートを使用してローカルユーザーを設定する場合、Cisco vManage は Cisco タイプ 9 パスワードタイプを使用します。Cisco タイプ 9 パスワードタイプは、ローカルユーザーのパスワードをハッシュするために scrypt アルゴリズムを使用します。Cisco vManage AAA テンプレートは、ローカルユーザーのパスワードのハッシュに Cisco タイプ 9 パスワードタイプだけを使用します。 デバイス CLI テンプレートまたは CLI アドオンテンプレートを使用してローカルユーザーを設定する場合、ローカルユーザーのパスワードのハッシュに他の Cisco パスワードタイプを選択できます。詳細については、「CLI アドオンテンプレートを使用したタイプ 6 パスワードの設定」を参照してください。

パラメータ名	説明
Privilege Level 1 OR 15	特権レベル 1 または 15 から選択します。 • [Level 1]：ユーザー EXEC モード。読み取り専用です。アクセスできるコマンドは `ping` などに限定されています。 • [Level 15]：特権 EXEC モード。`reload` コマンドなど、すべてのコマンドにアクセスできます。また設定の変更も可能です。デフォルトで、特権レベル 15 の EXEC コマンドは、特権レベル 1 で使用できるコマンドのスーパーセットです
SSH RSA キー	[+ Add] ボタンをクリックして、SSH RSA キーを追加します。SSH RSA キーを貼り付けるための新しいフィールドが表示されます。キーを削除するには、[-] ボタンをクリックします。 デバイスは、最大 2 の SSH RSA キーをサポートします。

[Add] をクリックして、新しいユーザーを追加します。[+ New User] をもう一度クリックして、さらにユーザーを追加します。

ユーザーグループのローカルアクセスを設定するには、最初にユーザーを基本グループまたはオペレータグループのいずれかに配置します。admin は自動的に netadmin グループに配置されます。次に、ユーザーグループを設定します。この設定を行うには、[Local] から [User Group] を選択します。

[+ New User Group] をクリックし、次のパラメータを設定します。

表 *9*:

パラメータ名	説明
Name	認証グループの名前。ユーザー名の長さは 1 ー 128 文字で、先頭は英字にする必要があります。名前に使用できるのは、英小文字、0 ー 9 の数字、ハイフン（-）、下線（_）、ピリオド（.）のみです。英大文字は使用できません。Cisco SD-WAN ソフトウェアには、basic、netadmin、および operator の 3 つの標準ユーザーグループが用意されています。ユーザー admin は自動的にグループ netadmin に配置され、このグループの唯一のユーザーです。RADIUS または TACACS+ サーバーから学習したすべてのユーザーは、グループ basic に配置されます。basic グループのすべてのユーザーは、operator グループのすべてのユーザーと同様の、タスクを実行するための同じ権限を持っています。次のグループ名は予約されているため、設定できません。adm、audio、backup、bin、cdrom、dialout、dip、disk、fax、floppy、games、gnats、input、irc、kmem、list、lp、mail、man、news、nogroup、plugdev、proxy、quagga、quaggavty、root、sasl、shadow、src、sshd、staff、sudo、sync、sys、tape、tty、uucp、users、utmp、video、voice、および www-data。また、文字列 viptela-reserved で始まるグループ名は予約されています。

パラメータ名	説明
機能タイプ	[Preset] をクリックして、ユーザーグループのプリセットロールのリストを表示します。[Custom] をクリックして、構成されている承認タスクのリストを表示します。
機能	機能テーブルには、ユーザーグループのロールが一覧表示されます。これらのロールは、インターフェイス、ポリシー、ルーティング、セキュリティ、およびシステムです。各ロールにより、ユーザーグループはデバイス構成の特定の部分の読み取りまたは書き込み、および特定のタイプの操作コマンドを実行できます。[Read]、[Write]、および [None] の適切なボックスをクリックして、各ロールのグループに権限を割り当てます。

[Add] をクリックして、新しいユーザーグループを追加します。

別のユーザーグループを追加するには、[+ New User Group] を再度クリックします。

ユーザーグループを削除するには、エントリの右側にあるごみ箱アイコンをクリックします。basic、netadmin、operator の 3 つの標準ユーザーグループは削除できません。

RADIUS 認証の設定

展開で RADIUS を使用している場合は、RADIUS 認証を設定します。

RADIUS サーバーへの接続を設定するには、[RADIUS] から [+ New Radius Server] をクリックし、次のパラメータを設定します。

表 *10*:

パラメータ名	説明
Address	RADIUS サーバーホストの IP アドレスを入力します。
Authentication Port	RADIUS サーバーへの認証要求に使用する UDP 宛先ポートを入力します。認証にサーバーを使用しない場合、ポート番号を 0 に設定します。デフォルト：ポート 1812
Accounting Port	802.1X および 802.11i アカウンティング情報を RADIUS サーバーに送信するために使用する UDP ポートを入力します。 範囲：0 ～ 65535。デフォルト：1813。
タイムアウト	要求を再送信する前に、デバイスが RADIUS 要求への応答を待機する秒数を入力します。 デフォルト：5 秒。 範囲：1 ～ 1000

パラメータ名	説明
Retransmit Count	デバイスがRADIUS要求をサーバーに再送信する回数を入力します。デフォルト：5 秒。
[Key]（廃止）	認証および暗号化のために Cisco IOS XE SD-WAN デバイス が RADIUS サーバーに渡すキーを入力します。キーを長さ 1 ～ 31 文字のテキスト文字列として入力すると、すぐに暗号化されます。または、AES 128 ビット暗号化キーを入力することもできます。キーは、RADIUS サーバーで使用する AES 暗号化キーと一致させる必要があります。

[Add] をクリックして、新しい RADIUS サーバーを追加します。

別の RADIUS サーバーを追加するには、[+ New RADIUS Server] を再度クリックします。

サーバーを削除するには、ごみ箱アイコンをクリックします。

CLI の同等の設定：

```
Device(config)# radius server 10.99.144.201
Device1(config-radius-server)# retransmit 5
Device(config-radius-server)# timeout 10
```

TACACS+ 認証の設定

展開で TACACS+ を使用している場合は、TACACS+ 認証を設定します。

TACACS+ サーバーへの接続を設定するには、[TACACS] から [+ New TACACS Server] をクリックし、次のパラメータを設定します。

表 *11* :

パラメータ名	説明
Address	TACACS+ サーバーホストの IP アドレスを入力します。
Port	TACACS+ サーバーへの認証要求に使用する UDP 宛先ポートを入力します。認証にサーバーを使用しない場合、ポート番号を 0 に設定します。 デフォルト：ポート 49
タイムアウト	要求を再送信する前に、デバイスが TACACS+ 要求への応答を待機する秒数を入力します。デフォルト：5 秒。範囲：1 ～ 1000
Key	認証と暗号化のために Cisco IOS XE SD-WAN デバイス が TACACS+ サーバーに渡すキーを入力します。キーを長さ 1 ～ 31 文字のテキスト文字列として入力すると、すぐに暗号化されます。または、AES 128 ビット暗号化キーを入力することもできます。キーは、TACACS+ サーバーで使用する AES 暗号化キーと一致させる必要があります。

[Add] をクリックして、新しい TACACS サーバーを追加します。

別の TACACS サーバーを追加するには、[+ New TACACS Server] を再度クリックします。

サーバーを削除するには、ごみ箱アイコンをクリックします。

8021X の設定

802.1X の設定については、IEEE 802.1X 認証の設定 （59 ページ）を参照してください。

認証順序の設定

デバイスの認証順序と認証フォールバックを設定できます。認証順序では、システムがユーザーの認証を試みる順序を指定し、現在の認証方法が使用できない場合に認証を続行する方法を提供します。フォールバックでは、ユーザーを認証できない場合、またはRADUSやTACACS+サーバーに到達できない場合に、認証のメカニズムを提供します。

Cisco IOS XE SD-WAN デバイス で AAA 認証順序および認証フォールバックを設定するには、[Authentication] タブを選択し、次のパラメータを設定します。

表 12：

パラメータ名	説明
サーバーグループの順序	AAA サーバーグループを使用するようにデバイスを設定すると、既存のサーバーホストをグループ化できます。既存のサーバーホストをグループ化すると、設定したサーバーホストのサブセットを選択し、それを特定のサービスに使用できます Cisco IOS XE SD-WAN デバイス へのユーザーアクセスを検証するときに、ソフトウェアが試行する認証方法のデフォルトの順序を変更するには、次の手順を実行します。 **1.** ServerGroups 優先順位フィールドをクリックして、サーバーグループのドロップダウンリストを表示します。リストには、ローカル、RADIUS、および TACACS 認証方式のグループが表示されます。 **2.** リストから、Cisco IOS XE SD-WAN デバイス へのアクセスを試みるユーザーをソフトウェアで検証する順序でグループを選択します。 リストから少なくとも 1 つのグループを選択する必要があります。

認可およびアカウンティングの設定

表 *13 :* 機能の履歴

機能名	リリース情報	説明
許可とアカウンティング	Cisco IOS XE リリース 17.5.1a Cisco vManage リリース 20.5.1	この機能では、許可（コマンドが実行される前に、ユーザーがデバイスに入力するコマンドを許可する）とアカウンティング（ユーザーがデバイスで実行するコマンドのレコードを生成する）を設定します。

認可の設定

許可を設定できます。これにより、TACACS+サーバーは、コマンドを実行する前に、ユーザーがデバイスに入力するコマンドを許可します。許可は、TACACS+ サーバーで設定されたポリシーと、[Authorization] タブで設定したパラメータに基づいています。

前提条件

- [Authentication] タブで、TACACS+ サーバーとローカルサーバーを認証順序の最初に設定する必要があります。

許可を設定するには、[Authorization] タブを選択し、[+ New Authorization Rule] をクリックして、次のパラメータを設定します。

パラメータ名	説明
コンソール	コンソールアクセスコマンドの認証を実行するには、このオプションを有効にします。
コンフィギュレーション コマンド	コンフィギュレーション コマンドの認証を実行するには、このオプションを有効にします。
メソッド	[Command] を選択します。これにより、ユーザーが入力するコマンドが許可されます。
Privilege Level 1 or 15	許可するコマンドの権限レベル（1または15）を選択します。この権限レベルを持つユーザーが入力したコマンドが許可されます。
Groups	以前に設定した TACACS グループを選択します。この認証ルールが定義するパラメータは、このグループに関連付けられている TACACS サーバーによって使用されます。

パラメータ名	説明
認証	このオプションを有効にすると、認証されたユーザーにのみ、この承認ルールが定義するパラメータが適用されます。このオプションを有効にしない場合、ルールはすべてのユーザーに適用されます。

[add] をクリックして、新しい認証ルールを追加します。

別の認証ルールを追加するには、[+ New Accounting Rule] を再度クリックします。

認証ルールを削除するには、行の右側にあるごみ箱アイコンをクリックします。

CLI の同等の設定：

```
system
   aaa
     aaa authorization console
     aaa authorization config-commands
     aaa authorization exec default list-name method
     aaa authorization commands level default list-name method
```

アカウンティングの設定

アカウンティングを設定できます。これにより、TACACS+ サーバーは、ユーザーがデバイスで実行するコマンドのレコードを生成します。

前提条件

- TACACS+ サーバーとローカルサーバーは、[Authentication] タブの認証順序で、それぞれ 1 番目と 2 番目に設定する必要があります。「認証順序の設定」を参照してください。

アカウンティングを設定するには、[Accounting] タブを選択し、[+ New Accounting Rule] をクリックして、次のパラメータを構成します。

表 *14*：

パラメータ名	説明
[Method]	[Command] を選択すると、ユーザーが実行したコマンドがログに記録されます。
Privilege Level 1 or 15	特権レベル（1 または 15）を選択します。アカウンティングレコードは、この特権レベルのユーザーが入力したコマンドに対してのみ生成されます。
Enable Start-Stop	イベントの開始時に開始アカウンティング通知、イベントの終了時に停止レコード通知を送信する場合は、[On] をクリックします。
Groups	Choose a previously configured TACACS group. このアカウンティングルールが定義するパラメータは、このグループに関連付けられている TACACS サーバーによって使用されます。

[Add] をクリックして新しいアカウンティングルールを追加します。

別のアカウンティングルールを追加するには、[+New Accounting Rule] を再度クリックします。

アカウンティングルールを削除するには、行の右側にあるごみ箱アイコンをクリックします。

CLI の同等の設定：

```
system
  aaa
    aaa accounting exec default start-stop group group-name
    aaa accounting commands level default start-stop group group-name
    aaa accounting network default start-stop group group-name
    aaa accounting system default start-stop group group-name
```

IEEE 802.1X 認証の設定

表 *15 :* 機能の履歴

機能名	リリース情報	説明
SD-WAN の 802.1X サポート	Cisco IOS XE リリース 17.2.1r	この機能により、Cisco IOS XE SD-WAN デバイス で IEEE 802.1X 認証を有効にできます。Cisco vManage を使用してこの機能を設定できるようにするには、Cisco vManage で Cisco SD-WAN リリース 20.1.1 が実行されていることを確認してください。

Cisco IOS XE リリース 17.2.1r 以降、IEEE 802.1X は Identity-Based Networking Services（IBNS）1.0 IOS-XE CLI に基づいてサポートされます。この機能は、LAN インターフェイスと WAN インターフェイスの両方でサポートされています。

IEEE 802.1X オープン認証とホストモード

4 つのホストモード（単一ホストモード、複数ホストモード、複数ドメイン認証モード、および複数認証モード）のいずれかを設定して、認証前にデバイスがネットワークアクセスを取得できるようにすることができます。

オープン認証は、ホストモードの設定後に **authentication open** コマンドを入力することで有効になり、設定済みのホストモードの拡張として機能します。たとえば、シングルホストモードでオープン認証を有効にした場合、ポートでは 1 つの MAC アドレスだけが許可されます。認証前オープンアクセスが有効の場合、ポートの初期トラフィックは制限され、ポートに設定されている 802.1X とは無関係です。ポートに 802.1X 以外のアクセス制限が設定されていない場合、クライアントデバイスは設定されている VLAN 上でフルアクセスが可能です。オープン認証は、CLI テンプレートのみを使用して設定できます。Cisco vManage で dot1x 機能テンプレートを使用してオープン認証を設定することはできません。

前提条件

- IEEE 802.1x サービスを認証するように RADIUS 認証サーバーを有効にします。
- スイッチ ポート インターフェイスで IEEE 802.1X 構成を有効にします。
- 認証済みクライアントと非認証クライアントに対して、次の VLAN 設定を有効にします。
  - 制限 VLAN（または認証拒否 VLAN）
  - ゲスト VLAN
  - クリティカル VLAN（または認証失敗 VLAN）
  - クリティカル音声 VLAN
- 次のいずれかのホストモード認証を有効にします。
  - シングルホストモード
  - マルチホストモード
  - 複数認証モード
  - マルチドメインモード
- RADIUS アカウンティング属性の設定
- 必要に応じて、アドオンテンプレートで VLAN ID を使用した IEEE 802.1X 認証イベントを有効にする必要があります。

制約事項

- IEEE 802.1X 認証、許可、およびアカウンティング（AAA）は、複数のグループではサポートされていません。
- Cisco vManage によって認証順序 IEEE 802.1X MAB CLI を無効にすることはできません。この認証順序 CLI が存在すると、MAB クライアントがオンラインの場合、MAB 認証で 60 秒の遅延が発生します。
- 認証オープンは機能テンプレートではサポートされていませんが、CLI アドオンテンプレートで展開できます。

vManage を使用した IEEE 802.1X 認証の設定

IEEE 802.1X は、ポートベースのネットワーク アクセス コントロール（PNAC）プロトコルであり、有線ネットワークに接続するデバイスに認証を提供することにより、許可されていないネットワークデバイスが有線ネットワークにアクセスするのを防ぎます。

RADIUS 認証サーバーは、ネットワークが提供するサービスにクライアントがアクセスする前に、ポートに接続されている各クライアントを認証する必要があります。

インターフェイスで IEEE 802.1X 認証を設定するには、最初に [Cisco AAA] 機能テンプレートを作成します。

1. Cisco vManage で、**[Configuration]** > **[Templates]** を選択します
2. [Feature Templates] をクリックしてから、[Add Template] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前では、[Feature Templates] のタイトルは [Feature] です。

3. 左側のパネルのリストからデバイスを選択します。
4. [Cisco AAA] テンプレートを選択します。
5. [Template Name] と [Description] に入力します。
6. [RADIUS] タブを選択し、[RADIUS SERVER] で [New RADIUS Server] をクリックします。
7. 次のパラメータを設定します。

パラメータ名	説明
[Mark as Optional Row]	設定をデバイス固有としてマークするには、[Mark as Optional Row] チェックボックスをオンにします。
アドレス	RADIUS サーバーの IP アドレスを入力します。
Authentication Port	[Authentication] をクリックし、[Add New Authentication Entry] をクリックして、IEEE 802.1X セッション中に RADIUS サーバーに送信する RADIUS 認証の属性と値（AV）のペアを構成します。 エントリを保存するには、[Add] をクリックします。
Accounting Port	[Accounting] をクリックし、[Add New Accounting Entry] をクリックして、IEEE 802.1X セッション中に RADIUS サーバーに送信する RADIUS アカウンティングの属性と値（AV）のペアを構成します。 エントリを保存するには、[Add] をクリックします。
タイムアウト	RADIUS サーバーからの応答を待機する時間を設定します
Retransmit Count	この RADIUS サーバーに接続する回数を設定します。
キー	RADIUS サーバーの共有キーを入力します。

8. [Add] をクリックします。
9. [RADIUS GROUP] を選択し、[New RADIUS Group] をクリックして、次のパラメータを設定します。

パラメータ名	説明
VPN-ID	RADIUS または他の認証サーバーに到達できる VPN を入力します。
Source Interface	RADIUS サーバーに到達するために使用されるインターフェイスを入力します。
RADIUS サーバ	RADIUS サーバーを設定します。

10. [Add] をクリックします。
11. [802.1X] タブを選択し、次のパラメータを入力します。

パラメータ名	説明
Authentication Param	認証パラメータを有効にするには、[On] をクリックします。
Accounting Param	アカウンティングパラメータを有効にするには、[On] をクリックします。

12. この機能テンプレートを保存するには、[Save] をクリックします。
13. デバイスでこの機能を有効にするには、これらの機能テンプレートをデバイステンプレートに追加してください。

（注） Cisco vManage リリース 20.5 より前に作成されたテンプレートはデバイスに接続すると失敗するため、AAA 機能テンプレートを再作成する必要があります。

次に、スイッチポートデバイスに使用できる [Switch Port] テンプレートを作成します。

1. [Switch Port] テンプレートを作成するには、上記の手順 1 ～ 3 を繰り返します。
2. [Switch Port] テンプレートを選択します。
3. [Template Name] と [Description] に入力します。
4. [Interface] タブを選択し、[New Interface] をクリックします。
5. 次のパラメータを設定します。

パラメータ名	説明
インターフェイス名	インターフェイス名を入力します。
速度	インターフェイス速度を入力します。
VLAN 名	VLAN 名を入力します。

パラメータ名	説明
VLAN ID	ブリッジングドメインに関連付けられた VLAN 識別子を入力します。
802.1X	このインターフェイスで IEEE 802.1X 認証を有効にします。[On] を選択します。 これにより、以下にリストされている追加のパラメータセットが提供されます。
Interface PAE Type	IEEE 802.1x インターフェイス PAE タイプを入力します。
Control Direction	単方向または双方向の認証モードを入力します。
Host Mode	IEEE 802.1X インターフェイスが単一のホスト（クライアント）または複数のホスト（クライアント）へのアクセスを許可するかどうかを選択します。 • [Multi Auth]：音声 VLAN 上の 1 つのホストとデータ VLAN 上の複数のホストへのアクセスを許可します。 • [Multi Host]：複数のホストへのアクセスを許可します • [Single Host]：最初に認証されたホストにのみアクセスを許可します。これがデフォルトです。 • [Multi-Domain]：ホストと音声デバイス（同じスイッチポート上の IP 電話など）の両方にアクセスを許可します。 （注） これらのオプションは、「Global」ホストモード設定でのみ使用できます。
定期再認証	IEEE 802.1X クライアントを再認証する頻度を入力します。デフォルトでは、最初の LAN アクセス要求の後、再認証は試行されません。 範囲：0 ～ 1440 分

6. [Advanced Options] をクリックし、次のように入力します。

パラメータ名	説明
Authentication Order	IEEE 802.1X インターフェイスに接続するデバイスを認証するときに使用する認証方法の順序を入力します。デフォルトの認証順序は RADIUS、次に MAC 認証バイパス（MAB）です。
MAC 認証バイパス	RADIUS サーバーで MAC 認証バイパス（MAB）を有効にし、RADIUS サーバーを使用して非 IEEE 802.1X 準拠のクライアントを認証する場合に選択します。

パラメータ名	説明
Port Control Mode	インターフェイスで IEEE 802.1X ポートベースの認証を有効にするには、ポート制御モードを入力します。 自動：IEEE 802.1X 認証を有効にし、ポートを未承認状態で起動するには、これを設定します。これにより、ポート経由で送受信できるのは EAPOL フレームのみです。
音声VLAN ID	音声 VLAN ID を設定します。
Critical VLAN	IEEE 802.1x 準拠クライアントのクリティカル VLAN（または認証失敗VLAN）を入力します。RADIUS認証またはRADIUSサーバーが失敗した場合のネットワークアクセスを構成します。
Critical Voice VLAN	クリティカル音声 VLAN を有効にします。
ゲスト VLAN	クライアントが MAB リストにない場合、ゲスト VLAN を設定して、IEEE 802.1X 対応でないクライアントをドロップします。
制限付き VLAN	IEEE 802.1x 準拠クライアントの制限付き VLAN（または認証失敗 VLAN）を入力します。RADIUS 認証に失敗した IEEE 802.1X 準拠クライアントへの限定サービスを設定します。

7. [Add] をクリックします。
8. この機能テンプレートを保存するには、[Save] をクリックします。
9. デバイスでこの機能を有効にするには、これらの機能テンプレートをデバイステンプレートに追加してください。

IEEE 802.1X オープン認証の設定

IEEE 802.1X オープン認証は、CLI アドオンテンプレートを使用して設定できます。

```
Device# config-transaction
Device(config)# interface GigabitEthernet2
Device(config-if)# authentication open
```

CLI を使用した IEEE 802.1X 認証の設定

設定

この機能には、次の 2 セットの設定が必要です。

1. **グローバル AAA コマンドを設定します。**
    1. IEEE 802.1X をグローバルに有効または無効にします

```
Device(config)# aaa authentication dot1x default group radius-0
Device(config)# aaa authorization network default group radius-0
Device(config)# dot1x system-auth-control
Device(config)# radius-server dead-criteria time 10 tries 3
Device(config)# radius-server deadtime 15
```

2. アカウンティングを有効にします

```
Device(config)# aaa accounting dot1x default start-stop group radius-0
```

2. インターフェイスレベルのコマンドを設定します。

1. ポート単位で IEEE 802.1X を有効または無効にします

```
Device(config-if)# dot1x pae authenticator
Device(config-if)# authentication port-control auto
```

2. ポート単位で MAB を有効または無効にします

```
Device(config-if)# mab
```

3. ホストモードを選択します

```
Device(config-if)# authentication host-mode  <multi-auth | multi-domain |
multi-host | single-host>
```

4. 音声 VLAN を設定します

```
Device(config-if)# switchport voice vlan <vlan-id>
```

5. IEEE 802.1X 制御方向を選択します

```
Device(config-if)# authentication control-direction <both | in>
```

6. 定期的な再認証と、対応する再認証間隔および非アクティブタイムアウト時間を有効にします

```
Device(config-if)# authentication periodic
Device(config-if)# authentication timer reauthenticate <internal-in-sec>
Device(config-if)# authentication timer inactivity <timeout-in-sec>
```

7. ポート単位で認証順序を設定します

```
Device(config-if)# authentication order dot1x mab
```

8. 制限 VLAN を指定します

```
Device(config-if)#  authentication event fail action authorize vlan <vlan-id>
```

9. ゲスト VLAN を指定します

```
Device(config-if)# authentication event no-response action authorize vlan
<vlan-id>
```

10. クリティカル VLAN を指定します

```
Device(config-if)# authentication event server dead action authorize vlan
<vlan-id>
```

11. クリティカル音声 VLAN 機能を有効にします

```
Device(config-if)# authentication event server dead action authorize voice
```

ポスチャアセスメントのサポート

表 *16 :* 機能の履歴

機能名	リリース情報	説明
ポスチャアセスメントのサポート	Cisco IOS XE リリース 17.3.1a Cisco vManage リリース 20.3.1	この機能により、ポスチャアセスメント機能を利用して、企業のセキュリティポリシーに従ってエンドポイントのコンプライアンスを検証できます。Identity Services Engine（ISE）のポスチャ機能は、Cisco 1100 サービス統合型ルータに統合されています。この機能は、Cisco vManage のアドオン機能テンプレートを使用してのみ設定できます。

ネットワークでは、企業のセキュリティポリシーへの準拠を保証するためにエンドポイントの検証が必要であり、ポスチャ評価によってこれを検証できます。ポスチャモジュールは、ネットワークに接続されているエンドポイントにセキュリティポリシーを適用します。Cisco 1100 サービス統合型ルータと ISE（アイデンティティ サービス エンジン）のエンドポイント間の接続では、それらの間の認証相互作用が必要です。IEEE 802.1X は、ポスチャアセスメントに推奨される標準認証プロセスです。MAC 認証バイパス（MAB）も使用できます。

これに使用されるポスチャ エージェント ソフトウェアは、Cisco AnyConnect ポスチャアセスメントです。Cisco AnyConnect ソフトウェアはエンドポイントにインストールされ、ポスチャと呼ばれるモジュールがあります。Cisco AnyConnect は、ISE サーバーからセキュリティポリシーをダウンロードし、エンドポイントの条件（マルウェア対策の条件、スパイウェア対策の条件、ウイルス対策の条件、アプリケーションの条件、USB の条件）をチェックします。すべての条件が満たされている場合、Cisco AnyConnect は ISE サーバーに「準拠」という結果を返します。そうでない場合、Cisco AnyConnect は「非準拠」という結果を返します。認証およびリダイレクト アクセス コントロール リスト（ACL）によるエンドポイントの認可と認証の後、クライアントエンドの Cisco AnyConnect ポスチャモジュールは、ポスチャポリシーサーバーでポスチャ評価を開始します。

ポスチャ評価が完了して認証されると、新しいポリシーを再認証または再許可するために、RADIUS サーバーから ISE で設定されたポリシーによって RADIUS CoA（許可変更）プロセスが開始されます。ポスチャ評価が成功すると、ネットワーク全体へのアクセスは、CoA 再認証コマンドによって Cisco ISR 1100 ルータおよびクライアントにプッシュされます。

ポスチャアセスメントの前提条件

- 基本的な IEEE 802.1x 認証プロセスが機能している必要があります。

- 認可変更（CoA）がサポートされている必要があります。
- リダイレクト ACL、ダウンロード可能な ACL（dACL）、およびクリティカル ACL が利用可能である必要があります。
- デバイス トラッキング ポリシー（アイデンティティ用）がサポートされている必要があります。
- URL リダイレクトがサポートされている必要があります。

ポスチャアセスメントの制約事項

- 8 ポートの Cisco 1100 サービス統合型ルータのみが、dACL やリダイレクト ACL などの ACL 機能をサポートします。
- ACL およびアクセス制御エントリ（ACE）ルールは、>、<、>=、<= などの比較操作をサポートしていません。
- 最大 120 の dACL ACE がサポートされ、64 のリダイレクト ACL ACE がサポートされます。
- ポート ACL および IPv6 ACL はサポートされていません。
- IP オプションと IP フラグメント ACL はサポートされていません。
- VLAN 単位のデバイストラッキングはサポートされていません。
- 収集やアドレストラッキングなど、制限されたポート単位のデバイストラッキング ポリシー オプションのみが許可されます。

Cisco SD-WAN でのポスチャ評価の設定

1. Cisco vManage の CLI アドオンテンプレートを使用して、AAA、IEEE 802.1x、ポスチャ評価を設定し、ACL とデバイストラッキングをリダイレクトします。

   設定例を以下に示します。

（注） `aaa new-model` はデフォルトで Cisco SD-WAN で有効になっており、ユーザーが設定することはできません。ただし、非 SD-WAN イメージ上に設定される必要があります。

1. AAA の設定

```
aaa new-model
radius server ISE1

address ipv4 198.51.100.255 auth-port 1812 acct-port 1813
key cisco

aaa group server radius ISE
 server name ISE1
!
aaa authentication dot1x default group ISE
aaa authorization network default group ISE
aaa accounting dot1x default start-stop group ISE

interface vlan 15
 ip address 198.51.100.1 198.51.100.254
```

```
interface GigabitEthernet0/1/0
 switchport mode access
 switchport access vlan 15

ip radius source-interface vlan 15
```

2. **IEEE 802.1x 認証および許可の設定**

```
policy-map type control subscriber simple_dot1x
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x
!
interface GigabitEthernet0/1/7
 switchport access vlan 22
 switchport mode access
 access-session closed
 access-session port-control auto
 dot1x pae authenticaton
 service-policy type control subscriber simple_dot1x
!
interface Vlan22
 ip address 198.51.100.1 198.51.100.254
```

（注） IEEE 802.1x エンドポイントは GigabitEthernet0/1/7 に接続されています。

3. **ポスチャ評価の設定および ACL のリダイレクト**

```
ip http server
ip http secure-server

ip access-list extended ACL-POSTAUTH-REDIRECT
10 deny tcp any host 192.0.2.255
20 deny tcp any any eq domain
30 deny udp any any eq domain
40 deny udp any any eq bootpc
50 deny udp any any eq bootps
60 permit tcp any any eq www
70 permit tcp any any eq 443
```

4. **デバイストラッキングの設定**

```
!
device-tracking policy tracking_test
 security-level glean
 no protocol ndp
 no protocol dhcp6
 tracking enable
!
interface GigabitEthernet0/1/7
 device-tracking attach-policy tracking_test
```

（注） 上記の IP アドレスは ISE に属しています。

この設定を Cisco vManage の CLI アドオンテンプレートに追加するために実行する必要がある手順は、ここに記載されています。

2. ISE で CoA 再認証と dACL を設定するには、次の手順を実行します。
   1. ダウンロード可能な ACL を作成し、その中に ACE を定義します。

      ACL 名：TEST_IP_PERMIT_ALL

      ACE：permit ip any any
   2. 認証結果を作成し、ダウンロード可能な ACL を dACL として選択します。
   3. **[Administration]** > **[System]** > **[Settings]** > **[Policy Settings]** に移動し、[Policy Sets] 設定で、認証結果を認証ポリシーとして選択します。
3. CLI アドオンテンプレートを作成したら、それをデバイステンプレートにアタッチしてから、Cisco vManage はデバイステンプレートのすべての設定をデバイスにプッシュします。

Cisco IOS XE SD-WAN ルータのタイプ 6 パスワード

表 *17* : 機能の履歴

機能名	リリース情報	説明
Cisco IOS XE SD-WAN ルータのタイプ 6 パスワード	Cisco IOS XE リリース 17.4.1a Cisco vManage リリース 20.4.1	この機能により、安全な可逆暗号化を使用するタイプ 6 パスワードを使用できます。この暗号化は、より安全なアルゴリズムを使用してパスワードを暗号化することにより、セキュリティを強化します。これらのパスワードは、サポートされるテンプレート（70 ページ）で詳しく説明されているテンプレートでサポートされています。

タイプ 6 パスワードの概要

タイプ 6 パスワード機能により、Advanced Encryption Scheme（AES）アルゴリズムに基づく認証、許可、およびアカウンティング（AAA）および Simple Network Management Protocol（SNMP）設定の安全な可逆暗号化が可能になります。

可逆暗号化は、可逆的な対称暗号化アルゴリズムを使用してパスワードを暗号化するプロセスです。ユーザーが入力したパスワードが有効かどうかを確認するために、パスワードが復号され、ユーザーが入力したパスワードと比較されます。この暗号化を実行するには、対称暗号化アルゴリズムにキーを指定する必要があります。使用する暗号化アルゴリズムは、PKCS#5 パ

ディングを使用した暗号ブロック連鎖（CBC）モードの Advanced Encryption Scheme（AES）アルゴリズムです。このアルゴリズムは、RADIUS、TACACS+、SNMP、TrustSec などの AAA 機能に使用されます。

Cisco vManage リリース 20.4.1 およびそれ以降のリリースでサポートされているテンプレートを作成すると、デフォルトでタイプ 6 パスワードが使用されます。Cisco vManage ではパスワードを暗号化し、そのパスワードを安全なトンネル経由でルータに送信します。次に、ルータはパスワードをタイプ 6 形式に暗号化し、それをデバイスに保存します。

（注） Cisco IOS XE SD-WAN デバイスでは、デバイスの 0 日目の起動時に、特権レベル 15 を持つ管理者ユーザーがデフォルトで作成されます。ユーザーがこの管理者ユーザーを削除しないことをお勧めします。

（注） パスワードの完全性に対する悪意のある攻撃の脆弱性を減らすために、タイプ 6 パスワードを使用することをお勧めします。デバイスを Cisco IOS XE リリース 17.4.1a にアップグレードすると、すべての AAA、RADIUS キー、および TACACS+ キーがタイプ 6 に暗号化されます。

サポートされるプラットフォーム

Cisco IOS XE SD-WAN デバイス。

サポートされるテンプレート

次のテンプレートは、タイプ 6 パスワードをサポートしています。

- Cisco AAA テンプレートを使用した RADIUS および TACACS 認証。
- SNMP テンプレート。
- CLI アドオンテンプレート。

機能制限

- SNMP テンプレートの場合、コミュニティ名はデフォルトで暗号化されます。したがって、既存の SNMP テンプレートをタイプ 6 のパスワードにアップグレードするには、コミュニティとトラップターゲットを削除して再作成します。
- **keychain key-string** コマンドでタイプ 6 パスワードを使用する場合、クリアテキストのパスワードの最大長は 38 文字です。

Cisco vManage を使用したタイプ 6 パスワードの設定

タイプ 6 パスワードへの既存のテンプレートのアップグレード

Cisco vManage で既存のテンプレートのパスワードをタイプ 6 のパスワードにアップグレードするには、次の手順を実行します。

（注） ルータを Cisco IOS XE リリース 17.4.1a にアップグレードすると、サポートされているすべてのパスワードがタイプ 6 のパスワードに自動的にアップグレードされます。

1. **[Configuration]** > **[Templates]** に移動します
2. [Feature Templates] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

3. タイプ 6 のパスワードにアップグレードするテンプレートに対し、[…] ボタンをクリックします。
4. [Edit] をクリックします。
5. **[Save]** をクリックします。

（注） パスワードを更新するために、テンプレートに他の変更を加える必要はありません。[Save] をクリックすると、Cisco vManage ではパスワードがタイプ 6 のパスワードに自動的にアップグレードされます。

CLI アドオンテンプレートを使用したタイプ 6 パスワードの設定

次の手順を実行して、CLI アドオン機能テンプレートを使用するときにタイプ 6 のパスワードを設定できます。

1. **[Configuration]** > **[Templates]** に移動します。
2. [Feature Templates] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

3. [Add template] をクリックします。

4. [Select Devices] ペインで、テンプレートを作成するデバイスを選択します。
5. [Select Template] ペインで、[Other Templates] セクションまで下にスクロールします。
6. [CLI Add-On Template] をクリックします。CLI アドオン機能テンプレートの詳細については、「CLI Add-on Feature Templates」を参照してください。
7. テンプレート名と説明を入力します。
8. デバイスで実行する CLI を入力するか貼り付けます。
9. CLI で平文パスワードを選択し、[Encrypt Type 6] ボタンをクリックします。
10. [Save] をクリックします。

タイプ6パスワードの確認

パスワードがタイプ6のパスワードにアップグレードされたことを確認するには、次のいずれかを実行します。

- Cisco vManage では、タイプ 6 パスワードをサポートする構成をデバイスにアタッチすると、構成プレビューに暗号化されたパスワードが表示されます。次に例を示します。

  ```
  snmp-server community 0
  $CRYPT_CLUSTER$ptqX7nQr6QvC8YZuoMGOkw==$6cVCeSpOfoVFe5iqhJqvQQ== ro
  ```

  コマンドでタイプが `0` と表示されているにもかかわらず、文字列 `$CRYPT_CLUSTER$ptqX7nQr6QvC8YZuoMGOkw==$6cVCeSpOfoVFe5iqhJqvQQ==` は暗号化されたパスワードを表しています。パスワードが暗号化されている場合は、`$CRYPT_CLUSTER$` で始まります。

- デバイスで次のコマンドを実行して、暗号化されたパスワードを表示できます。

  ```
  デバイス#show run | sec aaa
  aaa new-model
  aaa group server tacacs+ tacacs-0
  server-private 10.0.0.1 key 6 BibgKcVeWF]^aK[XfEIICXMCbdScBYAAB
  aaa group server radius radius-0
  server-private 10.0.0.2 timeout 5 retransmit 3 key 6 CHd_VK[]NHEdcVCWGCaENGINQHLBEhDBe
  ```

  出力には、パスワードがタイプ6であることが表示され、暗号化されたパスワードも表示されます。

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。