



ローカル認証および許可の設定

- [ローカル認証および許可の設定方法](#) (1 ページ)
- [ローカル認証および許可のモニタリング](#) (3 ページ)
- [ローカル認証および許可の機能履歴](#) (4 ページ)

ローカル認証および許可の設定方法

スイッチのローカル認証および許可の設定

ローカルモードでAAAを実装するようにスイッチを設定すると、サーバーがなくても動作するようにAAAを設定できます。この場合、スイッチは認証および許可の処理を行います。この設定ではアカウント機能は使用できません。



(注) AAA方式を使用してHTTPアクセスに対しスイッチのセキュリティを確保するには、**ip http authentication aaa** グローバル コンフィギュレーション コマンドでスイッチを設定する必要があります。AAA認証を設定しても、AAA方式を使用したHTTPアクセスに対しスイッチのセキュリティは確保しません。

ローカルモードでAAAを実装するようにスイッチを設定して、サーバーがなくても動作するようにAAAを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login default local**
5. **aaa authorization exec default local**
6. **aaa authorization network default local**
7. **username name [privilege level] { password encryption-type password }**
8. **end**

9. `show running-config`
10. `copy running-config startup-config`

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： デバイス> <code>enable</code>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> • パスワードを入力します（要求された場合）。
ステップ 2	configure terminal 例： デバイス# <code>configure terminal</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 3	aaa new-model 例： デバイス (config)# <code>aaa new-model</code>	AAA をイネーブルにします。
ステップ 4	aaa authentication login default local 例： デバイス (config)# <code>aaa authentication login default local</code>	ローカル ユーザ名データベースを使用するログイン認証を設定します。 default キーワードにより、ローカルユーザデータベース認証がすべてのポートに適用されます。
ステップ 5	aaa authorization exec default local 例： デバイス (config)# <code>aaa authorization exec default local</code>	ユーザの AAA 許可を設定し、ローカルデータベースを確認して、そのユーザに EXEC シェルの実行を許可します。
ステップ 6	aaa authorization network default local 例： デバイス (config)# <code>aaa authorization network default local</code>	ネットワーク関連のすべてのサービス要求に対してユーザ AAA 許可を設定します。
ステップ 7	username name [privilege level] { password encryption-type password } 例：	ローカル データベースを入力し、ユーザ名ベースの認証システムを設定します。 ユーザごとにコマンドを繰り返し入力します。

	コマンドまたはアクション	目的
	デバイス (config)# username your_user_name privilege 1 password 7 secret567	<ul style="list-style-type: none"> • <i>name</i> には、ユーザー ID を 1 ワードで指定します。スペースと引用符は使用できません。 • (任意) <i>level</i> には、アクセス権を得たユーザーに設定する権限レベルを指定します。指定できる範囲は 0 ~ 15 です。レベル 15 では特権 EXEC モードでのアクセスが可能です。レベル 0 では、ユーザ EXEC モードでのアクセスとなります。 • <i>encryption-type</i> には、暗号化されていないパスワードが後ろに続く場合は 0 を、暗号化されたパスワードが後ろに続く場合は 7 を指定します。 • <i>password</i> には、ユーザーがスイッチにアクセスする場合に入力する必要があるパスワードを指定します。パスワードは 1 ~ 25 文字で、埋め込みスペースを使用でき、username コマンドの最後のオプションとして指定します。
ステップ 8	end 例： デバイス (config)# end	特権 EXEC モードに戻ります。
ステップ 9	show running-config 例： デバイス# show running-config	入力を確認します。
ステップ 10	copy running-config startup-config 例： デバイス# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ローカル認証および許可のモニタリング

ローカル認証および許可の設定を表示するには、**show running-config** 特権 EXEC コマンドを使用します。

ローカル認証および許可の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	ローカル認証および許可	ローカルモードで AAA を実装するようにデバイスを設定すると、サーバがなくても動作するように AAA を設定できます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。

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。