AAA コマンド

この章は、次の項で構成されています。

aaa authentication login

ログイン時に適用される 1 つ以上の認証方式を設定するには、**aaa authentication login** グローバル コンフィギュレーション モード コマンドを使用します。デフォルトの認証方式に戻すには、このコマンドの **no** 形式を使用します。

構文

aaa authentication login [**authorization**] {**default** | *list-name*} *method1* [*method2...*]

no aaa authentication login {**default** | *list-name*}

パラメータ

- **authorization**：特定のリストに認証と許可の適用を指定します。キーワードを設定しない場合は、特定のリストにのみ認証が適用されます。
- **default**：この引数の後に続く認証方式を、ユーザがログインするときのデフォルト方式リストとして使用します（このリストに名前はありません）。
- ***list-name***：ユーザがログインするときに有効にされる、認証方式のリストの名前を指定します（長さ：1 ～ 12 文字）。
- ***method1*** [*method2...*]：認証アルゴリズムが（指定された順序で）試行する方式のリストを指定します。他の認証方式が使用されるのは、前の方式が失敗した場合ではなく、エラーが返された場合に限られます。すべての方式でエラーが返された場合でも認証を成功させるには、コマンド ラインに最後の方式として **none** を指定します。次のリストから 1 つ以上の方式を選択します。

キーワード	説明
enable	認証にイネーブル パスワードを使用します。
line	認証にライン パスワードを使用します。
ローカル	ローカルに定義されたユーザ名を認証に使用します。
none	認証を使用しません。
radius	認証にすべてのRADIUSサーバのリストを使用します。
tacacs	認証にすべての TACACS+ サーバのリストを使用します。

デフォルト設定

方式を指定しない場合、デフォルトではローカルで定義されたユーザとパスワードが使用されます。これは、**aaa authentication login local** コマンドを入力した場合と同じです。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

list-name パラメータとともにこのコマンドを入力して、認証方式のリストを作成します。*list-name* は、任意の文字列です。method 引数は、認証アルゴリズムが指定された順番で試行する方式のリストを指定します。

注。ログインに対して認証が有効になっており、スイッチが TACACS+ サーバからユーザレベル 15 を受信する場合は enable コマンドは必要なく、レベル 1 を受信する場合は enable コマンドが必要です。

no aaa authentication login *list-name* コマンドは、別のコマンドで参照されていない場合にのみ、リスト名を削除します。

例

次の例では、コンソールの認証ログイン方式を設定しています。

```
switchxxxxxx(config)# aaa authentication login authen-list radius local none
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# login authentication authen-list
```

aaa authentication enable

aaa authentication enable グローバル コンフィギュレーション モード コマンドは、より高い特権レベルにアクセスするための 1 つ以上の認証方式を設定します。デフォルトの認証方法に戻すには、このコマンドの **no** 形式を使用します。

構文

aaa authentication enable [**authorization**] {**default** | *list-name*} *method* [*method2...*]}

no aaa authentication enable {**default** | *list-name*}

パラメータ

- **authorization**：特定のリストに認証と許可の適用を指定します。キーワードを設定しない場合は、特定のリストにのみ認証が適用されます。
- **default**：この引数の後にリストされた認証方式を、より高い特権レベルにアクセスするときのデフォルト方式リストとして使用します。
- ***list-name***：ユーザがより高い権限レベルにアクセスするときに有効にする認証方式のリストの名前を指定します。（長さ：1 ～ 12 文字）
- ***method*** [*method2...*]：特定の順序で認証アルゴリズムが試行する方式のリストを指定します。追加の認証方式が使用されるのは、前の方式が失敗した場合ではなく、エラーが戻った場合に限られます。すべての方式でエラーが返された場合でも認証を成功させるには、コマンド ラインに最後の方式として **none** を指定します。次のリストから 1 つ以上の方式を選択します。

キーワード	説明
enable	認証にイネーブル パスワードを使用します。
line	認証にライン パスワードを使用します。
none	認証を使用しません。
radius	認証にすべての RADIUS サーバのリストを使用します。
tacacs	認証にすべての TACACS+ サーバのリストを使用します。

デフォルト設定

デフォルトでは、認証リストはありません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

aaa authentication enable *list-name method1 [method2...]* コマンドを入力してリストを作成します。ここで、*list-name* はこのリストに名前を付けるのに使用する文字列です。method 引数は、認証アルゴリズムが指定された順番で試行する方式のリストを指定します。

デバイスから RADIUS サーバに送信されたすべての **aaa authentication enable** 要求には、ユーザ名 **$enabx$** が含まれています。ここで、**x** は要求された特権レベルです。

デバイスから TACACS+ サーバに送信されたすべての **aaa authentication enable** 要求には、ログイン認証用に入力されたユーザ名が含まれています。

追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。すべての方式でエラーが返された場合でも認証を成功させるために、コマンド ラインに最後の方式として **none** を指定します。

no aaa authentication enable *list-name* は、参照されていない場合にのみ、リスト名を削除します。

例

次の例では、より高い特権レベルにアクセスするための認証用のイネーブルパスワードを設定しています。

```
switchxxxxxx(config)# aaa authentication enable enable-list radius none
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# enable authentication enable-list
```

login authentication

login authentication ライン コンフィギュレーション モード コマンドは、リモート Telnet またはコンソールセッションのログイン認証方式リストを指定します。デフォルトの認証方式に戻すには、このコマンドの **no** 形式を使用します。

構文

login authentication {**default** | *list-name*}

no login authentication

パラメータ

- **default**：**aaa authentication login** コマンドで作成された、デフォルト リストを使用します。
- ***list-name***：**aaa authentication login** コマンドで作成された、指定されたリストを使用します。

デフォルト設定

default

コマンド モード

ライン コンフィギュレーション モード

例 1：次の例では、ログイン認証方式をコンソール セッションのデフォルト方式として指定しています。

```
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# login authentication default
```

例 2：次の例では、コンソールの認証ログイン方式を方式のリストとして設定しています。

```
switchxxxxxx(config)# aaa authentication login authen-list radius local none
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# login authentication authen-list
```

認証のイネーブル化

enable authentication ライン コンフィギュレーション モード コマンドは、リモート Telnet またはコンソールから、より高い特権レベルにアクセスするための認証方式を指定します。デフォルトの認証方式に戻すには、このコマンドの **no** 形式を使用します。

構文

enable authentication {**default** | *list-name}*

no enable authentication

パラメータ

- **default**：**aaa authentication enable** コマンドで作成された、デフォルト リストを使用します。
- ***list-name***：**aaa authentication enable** コマンドで作成された、指定されたリストを使用します。

デフォルト設定

default です。

コマンド モード

ライン コンフィギュレーション モード

例 1：次の例では、コンソールからより高い特権レベルにアクセスするときの認証方式を、デフォルト方式として指定しています。

```
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# enable authentication default
```

例 2：次の例では、より高い特権レベルにアクセスするための認証方式のリストを設定しています。

```
switchxxxxxx(config)# aaa authentication enable enable-list radius none
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# enable authentication enable-list
```

ip http authentication

ip http authentication グローバル コンフィギュレーション モード コマンドは、HTTP サーバ アクセス用の認証方式を指定します。デフォルトの認証方式に戻すには、このコマンドの **no** 形式を使用します。

構文

ip http authentication aaa login-authentication [**login-**authorization] *method1* [*method2...*]

no ip http authentication aaa login-authentication

パラメータ

- **login-**authorization：認証と許可の適用を指定します。キーワードを設定しない場合は、認証のみが適用されます。
- ***method*** [*method2...*]：特定の順序で認証アルゴリズムが試行する方式のリストを指定します。追加の認証方式が使用されるのは、前の方式が失敗した場合ではなく、エラーが戻った場合に限られます。すべての方式でエラーが返された場合でも認証を成功させるには、コマンド ラインに最後の方式として **none** を指定します。次のリストから 1 つ以上の方式を選択します。

キーワード	説明
ローカル	認証にローカルなユーザ名データベースを使用します。
none	認証を使用しません。
radius	認証にすべての RADIUS サーバのリストを使用します。
tacacs	認証にすべての TACACS+ サーバのリストを使用します。

デフォルト設定

ローカル ユーザ データベースがデフォルトの認証ログイン方式です。これは、**ip http authentication local** コマンドを入力した場合と同じです。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

このコマンドは、HTTP および HTTPS サーバ ユーザに関係します。

例

次の例では、HTTP アクセス認証方式を指定しています。

```
switchxxxxxx(config)# ip http authentication aaa login-authentication radius local none
```

show authentication methods

show authentication methods 特権 EXEC モード コマンドは、認証方式に関する情報を表示します。

構文

show authentication methods

コマンド モード

特権 EXEC モード

例

次の例では、認証の設定を表示しています。

switchxxxxxx# **show**

```
authentication methods
Login Authentication Method Lists
---------------------------------
Default: Radius, Local, Line
Consl_Login(with authorization): Line, None
Enable Authentication Method Lists
---------------------------------
Default: Radius, Enable
Consl_Enable(with authorization): Enable, None
```

.

Line	Login Method List	Enable Method List
Console	Consl_Login	Consl_Enable
Telnet	Default	Default
SSH	Default	Default

```
HTTP, HHTPS: Radius, local
Dot1x: Radius
```

パスワード

ライン（アクセス方式とも呼ばれ、コンソールやTelnetなどがあります）のパスワードを指定するには、**password** ライン コンフィギュレーション モード コマンドを使用します。デフォルトのパスワードに戻すには、このコマンドの **no** 形式を使用します。

構文

password {*unencrypted-password* [**method** *hash-method***]** | *encrypted-password* **encrypted**}

no password

パラメータ

- ***unencrypted-password***：ユーザの認証パスワード。（範囲：1 ～ 64）
- [**method** *hash-method***]** ：（任意）クリアテキストパスワードの暗号化に使用する方式を指定します。サポートされる値：

  sha512：基盤のハッシュアルゴリズムとして SHA512 を使用した HMAC による PBKDF2 暗号化。**method** パラメータを指定しない場合は、これがデフォルトの方式になります。
- **encrypted encrypted-password**：パスワードが暗号化され、ソルトを使用してハッシュされることを指定します。すでに暗号化されているパスワード（たとえば、別のデバイスのコンフィギュレーション ファイルからコピーしたパスワード）を入力するには、このキーワードを使用します。*encrypted-password* は *$<type>$<salt>$<encrypted-password>* 形式で指定します。ここで、

  <*type*>：ハッシュの生成に使用するハッシュアルゴリズムのタイプを示す整数値です。

  <salt>：ソルトに使用する 96 ビットの Base64 エンコーディング（長さ：16 バイト）

  - **<*encrypted-password*>**：暗号化されたハッシュ出力の Base64 エンコーディング（長さ：86 バイト）

デフォルト設定

パスワードは定義されていません。

コマンド モード

ライン コンフィギュレーション モード

使用上のガイドライン

unencrypted-password は、パスワードの複雑さの要件を順守する必要があります。

例

次に、コンソール行にパスワード「secreT123!」を指定する例を示します。

```
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# password secreT123!
```

enable password

通常レベルおよび特権レベルへのアクセスを制御するためのローカルパスワードを設定するには、**enable password** グローバル コンフィギュレーション モード コマンドを使用します。デフォルトのパスワードに戻すには、このコマンドの **no** 形式を使用します。

構文

enable password [**level** *privilege-level*] {[**method** *hash-method***]** *unencrypted-password* | **encrypted** encrypted-password}

no enable password [**level** *privilege-level*]

パラメータ

- **level** privilege-level：パスワードが適用されるレベル。指定しない場合、レベルは 15 になります。（範囲：1 ～ 15）
- [**method** *hash-method***]** ：（任意）クリアテキストパスワードの暗号化に使用する方式を指定します。サポートされる値：

  sha512：基盤のハッシュアルゴリズムとして SHA512 を使用した HMAC による PBKDF2 暗号化。**method** パラメータを指定しない場合は、これがデフォルトの方式になります。
- ***unencrypted-password***：このレベルのパスワード。（範囲：0 ～ 159 文字）
- **encrypted encrypted-password**：パスワードが暗号化され、ソルトを使用してハッシュされることを指定します。すでに暗号化されているパスワード（たとえば、別のデバイスのコンフィギュレーション ファイルからコピーしたパスワード）を入力するには、このキーワードを使用します。*encrypted-password* は *$<type>$<salt>$<encrypted-password* > 形式で指定します。ここで、

  <*type*>：ハッシュの生成に使用するハッシュアルゴリズムのタイプを示す整数値です。

  <salt>：ソルトに使用する 96 ビットの base64 エンコーディング（長さ：16 バイト）

  - **<*encrypted-password*>**：暗号化されたハッシュ出力の Base64 エンコーディング（長さ：86 バイト）

デフォルト設定

level のデフォルトは 15 です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

unencrypted-password は、パスワードの複雑さの要件を順守する必要があります。

管理者が新しい **enable** パスワードを設定すると、そのパスワードは自動的に暗号化され、コンフィギュレーションファイルに保存されます。どのようにパスワードを入力した場合でも、コンフィギュレーション ファイルにはキーワード **encrypted** と暗号化された値で表示されます。暗号化されたキーワードを実際に入力する場合にのみ、管理者は **encrypted** キーワードを使用する必要があります。

あるスイッチ（たとえば、スイッチB）で設定されたパスワードを別のスイッチ（たとえば、スイッチ A）に手動でコピーする場合、管理者はスイッチ A で **enable** コマンドを入力するときに、この暗号化されたパスワードの前に **encrypted** を追加する必要があります。この方法では、2 つのスイッチのパスワードが同じになります。

暗号化されたキーワードを実際に入力する場合にのみ、管理者は **encrypted** キーワードを使用する必要があります。

例 1：このコマンドは、すでに暗号化されているパスワードを設定します。パスワードは、入力されたとおりにコンフィギュレーション ファイルにコピーされます。このパスワードを使用してデバイスにログインするには、ユーザは暗号化されていない形式を知っている必要があります。

```
switchxxxxxx(config)# enable password encrypted
```

例 2：次に、レベル 1 の暗号化されていないパスワードを設定する例を示します（コンフィギュレーション ファイルで暗号化されます）。

```
switchxxxxxx(config)# enable password level 1 let-me-In
```

service password-recovery

パスワード回復メカニズムを有効にするには、**service password-recovery** グローバル コンフィギュレーション モード コマンドを使用します。このメカニズムにより、デバイスのコンソール ポートに物理的にアクセスしているエンドユーザは、ブート メニューを表示して、パスワードの回復プロセスを起動することができます。パスワード回復メカニズムを無効にするには、**no service password-recovery** コマンドを使用します。パスワード回復メカニズムが無効になっている場合でも、ブート メニューへのアクセスは許可され、ユーザはパスワード回復プロセスを起動できます。この場合の異なる点は、すべてのコンフィギュレーション ファイルとすべてのユーザ ファイルが削除されることです。「All the configuration and user files were removed」というログ メッセージが端末に生成されます。

構文

service password-recovery

no service password-recovery

デフォルト設定

サービス パスワードの回復はデフォルトで有効になっています。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

- パスワードの回復が有効になっている場合、ユーザはブート メニューにアクセスし、ブート メニューでパスワードの回復を起動することができます。すべてのコンフィギュレーション ファイルとユーザ ファイルが保持されます。
- パスワードの回復が無効になっている場合、ユーザはブート メニューにアクセスし、ブート メニューでパスワードの回復を起動することができます。コンフィギュレーション ファイルとユーザ ファイルが削除されます。
- デバイスでセンシティブ データをユーザ定義パスフレーズで保護するように設定している場合（Secure Sensitive Data の場合）、パスワードの回復が有効になっていても、[Boot] メニューからパスワードの回復をトリガーできません。

例

次のコマンドはパスワードの回復を無効にします。

```
switchxxxxxx(config)# no service password recovery
Note that choosing to use Password recovery option in the Boot Menu during the boot
process will remove the configuration files and the user files. Would you like to continue
 ? Y/N.
```

username

ユーザ名ベースのユーザ認証アカウントを作成または編集するには、**username** グローバル コンフィギュレーション モード コマンドを使用します。ユーザアカウントを削除するには **no** 形式を使用します。

構文

username name {[**method** *hash-method*] **password** {*unencrypted-password* | {**encrypted** encrypted-password}} | {**privilege** privilege-level {[**method** *hash-method*] *unencrypted-password* | {**encrypted** encrypted-password}}}}

no username name

パラメータ

- ***name***：ユーザの名前。（範囲：1 ～ 20 文字）
- [**method** *hash-method*]：（任意）クリアテキストパスワードの暗号化に使用する方式を指定します。サポートされる値：

  sha512：基盤のハッシュアルゴリズムとして SHA512 を使用した HMAC による PBKDF2 暗号化。**method** パラメータを指定しない場合は、これがデフォルトの方式になります。
- **password**：このユーザ名のパスワードを指定します。
- ***unencrypted-password***：ユーザの認証パスワード。（範囲：1 ～ 64）
- **encrypted encrypted-password**：パスワードが暗号化され、ソルトを使用してハッシュされることを指定します。すでに暗号化されているパスワード（たとえば、別のデバイスのコンフィギュレーション ファイルからコピーしたパスワード）を入力するには、このキーワードを使用します。*encrypted-password* は *$<type>$<salt>$<encrypted-password>* 形式で指定します。ここで、

  <*type*>：ハッシュの生成に使用するハッシュアルゴリズムのタイプを示す整数値です。

  <salt>：ソルトに使用する 96 ビットの Base64 エンコーディング（長さ：16 バイト）

  - **<*encrypted-password*>**：暗号化されたハッシュ出力の Base64 エンコーディング（長さ：86 バイト）
- **privilege** privilege-level：ユーザアカウントの権限レベル。指定しない場合、レベルは 1 になります。（範囲：1 ～ 15）。

デフォルト設定

ユーザは定義されていません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

unencrypted-password は、パスワードの複雑さの要件を順守する必要があります。

最後のレベル 15 のユーザは削除できず、リモートユーザにすることもできません。

例 1：ユーザ tom（レベル 15）用の暗号化されていないパスワードを設定します。パスワードは、コンフィギュレーション ファイルで暗号化されます。

```
switchxxxxxx(config)# username tom password 1234Ab$5678
```

例 2：すでに暗号化されているユーザ jerry（レベル 15）用のパスワードを設定します。パスワードは、入力されたとおりにコンフィギュレーション ファイルにコピーされます。使用するには、ユーザが暗号化前の形式を知っている必要があります。

```
switchxxxxxx(config)# username jerry privilege 15 encrypted
$15$TqKC13RgV/QJb2Ma$4JmeD7wgRGH2iwGKMM+g4M53uQxpOMlhkUN56UMAEUuMqhw0bsRH27zakc72hLxt/YhEknPA6LX7fTgqwZn6Vw==
```

show users accounts

show users accounts 特権 EXEC モード コマンドは、ユーザのローカル データベースに関する情報を表示します。

構文

show users accounts

コマンド モード

特権 EXEC モード

例

次の例では、ユーザ ローカル データベースに関する情報を表示します。

```
switchxxxxxx# show users accounts

Username        Privilege   Password
                            Expiry date
--------        ---------   ----------
Bob             15          Jan 18 2005
Robert          15          Jan 19 2005
Smith           15          Jan 19 2005
```

次の表に、この出力で表示される重要なフィールドについて説明します。

フィールド	説明
Username	ユーザ名。
特権	ユーザの特権レベル。
Password Expiry date	ユーザのパスワードの有効期限。

passwords complexity

パスワードの複雑さが有効になっている場合のパスワードの最小要件を制御するには、**passwords complexity** グローバル コンフィギュレーション モード コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

構文

passwords complexity {**min-length** number} | {**min-classes** number} | {**no-repeat** number} | **not-current** | **not-username** | **not-manufacturer-name**

no passwords complexity min-length | **min-classes** | **no-repeat** | **not-current** | **not-username** | **not-manufacturer-name**

パラメータ

- **min-length** number：パスワードの最小長を設定します。（範囲：8 ー 64）
- **min-classes** number：最小限の文字クラス（標準のキーボードで利用可能な大文字、小文字、数字、および特殊文字など）を設定します。（範囲：1 ～ 4）
- **no-repeat** number：新しいパスワードで連続して繰り返すことができる最大文字数を指定します。（範囲：1 ー 16）
- **not-current**：新しいパスワードを現在のパスワードと同じにできないことを指定します。
- **not-username**：パスワードでユーザ名またはユーザ名の大文字と小文字を変更した類似の名前を繰り返したり、逆にして使用することができないことを指定します。
- **not-manufacturer-name**：パスワードで製造者名または製造者名の大文字と小文字を変更した類似の名前を繰り返したり、逆にして使用することができないことを指定します。

デフォルト設定

最小長は 8 です。

クラスの数は 3 です。

no-repeat のデフォルトは 3 です。

その他のすべての制御はデフォルトで有効になっています。

コマンド モード

グローバル コンフィギュレーション モード

例

次の例では、最小限必要なパスワードの長さを 10 文字に設定しています。

```
switchxxxxxx(config)# passwords complexity min-length 10
```

passwords aging

パスワード エージングを適用するには、**passwords aging** グローバル コンフィギュレーション モード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

構文

passwords aging *days*

no passwords aging

パラメータ

- ***days***：パスワード変更が強制されるまでの日数を指定します。0 を使用すると、エージングを無効にできます。（範囲：0 ～ 365）。

デフォルト設定

180

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

エージングは、特権レベル 15 のローカル データベースのユーザにのみ、特権レベル 15 のパスワードを有効にするために関係します。

パスワード エージングを無効にするには、**passwords aging 0** を使用します。

no passwords aging を使用すると、エージング タイムがデフォルトに設定されます。

例

次の例では、エージング タイムを 24 日に設定しています。

```
witchxxxxxx(config)# passwords aging 24
```

show passwords configuration

show passwords configuration 特権 EXEC モード コマンドは、パスワードの管理設定に関する情報を表示します。

構文

show passwords configuration

コマンド モード

特権 EXEC モード

例

```
switchxxxxxx# show passwords configuration
Passwords aging is enabled with aging time 180 days.
Passwords complexity is enabled with the following attributes:
 Minimal length: 3 characters
 Minimal classes: 3
 New password must be different than the current: Enabled
 Maximum consecutive same characters: 3
 New password must be different than the user name: Enabled
New password must be different than the manufacturer name: Enabled
Following set to internal since it is not supported
Enable Passwords
Level
-----
1
15
Line Passwords
Line
-----
Console
Telnet
SSH
```

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。