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	認証に有効化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。
local	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	認証に有効化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 サーバーに送信されたすべての **aaa authentication enable** 要求には、ユーザー名 **$enabx$** 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+ サーバー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ー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有効化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
```

enable authentication

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
local	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
```

を参照してください。

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

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

login block-for

Login Block-for

次のグローバル コンフィギュレーション モード コマンドを使用して、指定された回数のログイン試行失敗後の静音モード期間を設定します。デフォルト設定に戻すには、コマンドの no 形式を使用します。

構文

login block-for seconds **attempts** tries **within** seconds

no login block-for

パラメータ

- **Block for seconds**：静音モード期間（ログイン試行が拒否される時間）の長さ（秒単位）（範囲は 1 ～ 65535（18 時間）秒）。
- **attempts** tries：静音モード期間をトリガーするログイン試行の失敗回数（範囲は 1 ～ 100）。
- **within** seconds：静音モード期間のトリガーに必要な、その回数のログイン試行失敗が生じる時間の長さ（秒単位）（範囲 1 ～ 3600（1 時間）秒）。

デフォルト設定

デバイスで静音モードが設定されていません。

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

指定の時間（**within** seconds）内に、指定された回数の接続試行が失敗した（**attempt** tries）場合、デバイスは指定の期間（**block-for** seconds）の間、追加のログイン試行を受け入れません。

静音モード期間中、デバイスへの管理接続は、指定された接続のみを許可する静音モードアクセスクラスによって制限されます（コマンド **login quiet-mode access-class**）。コンソール接続をサポートするデバイスの場合、「console_only」管理アクセスリストがデフォルトの静音モードアクセスクラスとして使用されます。この場合、静音モード期間中は、ネットワーク（Telnet、SSH、SNMP、HTTP、または HTTPS）を介したすべてのログイン試行が拒否されます。

このコマンドは、静音モードアクセスクラス（デフォルトまたはユーザー定義）が設定されている場合にのみ設定できます。「login quiet-mode access-class」を参照してください。

login block-for コマンドがデバイスですでに設定されており、そのコマンドが「監視期間」中に新しいパラメータで再設定された場合、現在のカウントは終了し、新しいパラメータを使用

して新しいカウントが開始されます。ログイン攻撃の静音モード期間中に設定された場合、そのコマンドは拒否されます。

コマンドの **no** 形式を使用すると、この機能が無効になり、静音モード期間が終了します（アクティブな場合）。

例

例 1：次の例では、180 秒以内に 18 回を超えてログイン試行に失敗した場合に、すべてのログイン要求を 180 秒間ブロックする方法を示します。

```
switchxxxxxx(config)# login block-for 180 attempts 18 within 180
```

例 2：次の例では、デバイスの静音モード期間中にコマンドを設定しようとしています。

```
switchxxxxxx(config)# login block-for 18 attempts 8 within 50
```

デバイスが静音モードの間は、login block-for の設定はできません。

例 3：次の例では、コマンドの設定に失敗しています。失敗の理由：静音モードアクセスクラス（デフォルトまたはユーザー定義）が設定されていません。

```
switchxxxxxx(config)# login block-for 770 attempts 7 within 613
```

静音モードアクセスクラスが設定されていないため、login block-for を設定できません。

login delay

失敗したログイン試行に対するデバイス応答の遅延を設定するには、 **login delay** 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

login delay seconds

no login delay

パラメータ

- seconds：失敗したログイン試行間に課される遅延（秒単位）（範囲 1 ～ 10 秒）。

デフォルト設定

デフォルトでは、ログイン遅延は無効になっています。

コマンド モード

デフォルトでは、ログイン遅延は無効になっています。

使用上のガイドライン

login delay コマンドを使用すると、ログイン試行に失敗した後のデバイスの応答に遅延が生じます（HTTP、HTTPS、Telnet、SSH、および SNMP）。遅延により、見込まれる辞書攻撃からの保護が強化されます。

例

例 1：次の例では、ログイン試行が失敗した後に 5 秒の遅延を設定しています。

```
switchxxxxxx(config)# login delay 5
```

login quiet-mode access-class

デバイスがログイン静音モードに移行するときに適用される管理アクセス制御リスト（MACL）を指定するには、login quiet-mode access-class 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

login quiet-mode access-class name

no login quiet-mode access-class

パラメータ

- ***name***：ログイン静音モードでデバイスに適用する管理 ACL の名前。

デフォルト設定

デフォルトでは、「console-only」管理アクセスリストがデフォルトの静音モードアクセスクラスとして適用されます。コンソールをサポートしていないデバイスの場合、静音モードアクセスクラスにデフォルトはありません。

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

login quiet-mode access-class コマンドを使用して、ログイン待機期間中に選択したホストがデバイス管理にアクセスできるようにします。指定した管理 ACL に基づいてアクセスが許可されます。management access-list コマンドを使用してこのコマンドを設定する前に、管理アクセスリストを作成する必要があります。

この設定により、静音モード期間中であっても、クライアントまたはクライアントのリストへのアクセスを許可できるようになります。コンソール接続をサポートするデバイスでは、静音モード期間中はデフォルトで「console-only」管理アクセスリストが適用されます。つまり、すべてのネットワークログイン接続（telnet、SSH、SNMP、HTTP、HTTPS）が拒否されますが、コンソールからの接続は許可されます。コンソールをサポートしていないデバイスでは、デフォルトのアクセスクラスはなく、ユーザーが最初に静音モードアクセスクラスを定義していない場合は、login block-for コマンドを設定できません。

静音モード期間中に設定した場合、そのコマンドは拒否されます。

このコマンドの no 形式を使用すると、静音モードアクセスクラスがデフォルト設定に戻ります。コンソールのないデバイスでは、login block-for コマンドが設定されている場合、no コマンドを適用できません。

例

例 1 ：次の例は、quiet-acl 管理アクセスリストに基づいて、静音モード期間中に接続を受け入れるようにデバイスを設定する方法を示しています。

```
switchxxxxxx(config)# login quiet-mode access-class quiet-acl
```

show login

ログイン設定とステータスを表示するには、次の特権 EXEC モードコマンドを使用します。

構文

show login

パラメータ

該当なし

デフォルト設定

該当なし

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、コマンド **login delay**、**Login block-for and login quiet-mode access-class** に関連する設定とステータスを表示します。

例

例 1：次の例は、ログイン設定が適用または変更されていない場合の出力を示しています。

```
switchxxxxxx# show login
Login delay: disabled
Login Attacks watch: disabled
Quiet-Mode access list: console-only (the default)
```

例 2：次の例は、ユーザーがログイン遅延を 5 秒に設定し、ログインブロック期間を設定し、デバイスが静音モードではない場合の show login コマンドの出力を示しています。

```
switchxxxxxx# show login
Login delay: 5 second
Login Attacks watch: enabled
If more than 4 login failures occur in 60 seconds or less, logins will be disabled for
60 seconds.
Quiet-Mode access list: console-only (the default)
Quiet-Mode: inactive
Watch Window remaining time: 44 seconds.
Present login failure count: 3.
```

（注） ログイン失敗数は、（監視ウィンドウ内で）まだ有効である最も早い失敗ログインからカウントされます。

例 3：次の例は、ユーザーがログイン遅延を 5 秒に設定し、ログインブロック期間を設定し、デバイスが静音モードになっている場合の出力を示しています。

```
switchxxxxxx# show login
Login delay: 5 second
Login Attacks watch: enabled
If more than 4 login failures occur in 60 seconds or less, logins will be disabled for
60 seconds.
Quiet-Mode access list: console-only (the default)
Quiet-Mode: active (time remaining: 20 seconds)
```

show login failures

失敗したログイン試行に関する情報を表示するには次の特権EXECモードコマンドを使用します。

構文

Show login failures

パラメータ

該当なし

デフォルト設定

該当なし

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、最近 50 回の失敗したログイン試行に関する情報を表示します。情報には、失敗した試行で入力されたユーザー名（試行の一部として入力された場合）、失敗した試行で使用された送信元IP、失敗した試行で要求されたサービス、この接続の失敗試行回数、およびこの接続の最後の失敗試行のタイムスタンプが含まれます。エントリは、最新のタイムスタンプから最も古いものへとソートされます。

例

```
switchxxxxxx#  show login failures
```

このデバイスでの最近 50 回のログイン失敗に関する情報。

ユーザ名	Source IP	サービス	Count	Timestamp
————————	————————	————————	————————	————————
ffff	10.5.44.25	Telnet	3	2021 年 7 月 7 日（水）00:01:23 edt
fff	10.5.44.25	Telnet	4	2021 年 7 月 8 日（木）08:37:08 edt
bb	10.5.44.25	ssh	2	2021 年 7 月 7 日（水）00:17:59 edt
fff	10.5.44.25	ssh	2	2021 年 7 月 7 日（水）00:20:37 edt

ユーザ名	Source IP	サービス	Count	Timestamp
ffff	10.5.44.25	ssh	2	2021 年 7 月 7 日（水）00:21:12 edt
aaaa	fe80::1111	ssh	2	2021 年 7 月 7 日（水）00:21:26 edt
	10.5.44.25	Telnet	3	2021 年 7 月 7 日（水）00:38:14 edt
aaa	10.5.44.22	Telnet	1	2021 年 7 月 8 日（木）08:37:16 edt
555	10.5.44.23	Telnet	1	2021 年 7 月 8 日（木）08:37:26 edt

clear login failures

ログイン失敗データベースをクリアするには、次の特権EXECモードコマンドを使用します。

構文

clear login failures

パラメータ

該当なし

デフォルト設定

該当なし

コマンド モード

特権 EXEC モード

使用上のガイドライン

ログイン失敗データベース内のすべてのエントリをクリアするには、このコマンドを使用します（コマンド **show login failures**）。

例

```
switchxxxxxx#  clear login failures
```

clear login quiet-mode

アクティブな静音モード期間をただちに終了するには、次の特権EXECモードコマンドを使用します。

構文

clear login quiet-mode

パラメータ

該当なし

デフォルト設定

該当なし

コマンド モード

特権 EXEC モード

使用上のガイドライン

機能を無効にせずにアクティブな静音期間を終了するには、このコマンドを使用します（コマンド **login block-for**）。静音モード期間タイマーがタイムアップにならなくても、静音モード期間が終了します。

例

```
switchxxxxxx#  clear login quiet-mode
11-Aug-2021 10:33:12 :%ABC-I-XXX: Quiet-Mode is OFF, terminated by user
```

password

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**}

password generate-password [**method** hash-method]

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***]** ：（オプション）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。

generate-password オプションが選択されている場合、ユーザーがパスワードを入力する必要はありません。代わりに、デバイスがランダムベースのパスワード提案を自動的に生成します。この提案はユーザーに示され、提案されたパスワードを受け入れるか拒否するかを選択するオプションが表示されます。ユーザーが提示されたパスワードを受け入れることを選択した場合、指定したユーザー名とこのパスワード（暗号化形式）がデバイス設定ファイルに追加されます。提示されたパスワードをユーザが拒否した場合は、ユーザーが新しいコマンドを入力する必要があります。

例

例 1：次の例では、コンソール行にパスワード「secreT123!」を指定しています。

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

例 2：この例のコマンドには、generate-password キーワードが含まれています。この場合、デバイスはランダムに生成されたパスワードの使用を提案します。次の例では、ユーザーは提示されたパスワードを受け入れることを選択しています。

```
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# password generate-password
Generated password: aBgrT9!59Hq$
Accept generated password (y/n) [Y] y
"Configuration and password are added to device configuration. Please Note
password for future use."
```

例 3：この例のコマンドには、generate-password キーワードが含まれています。この場合、デバイスはランダムに生成されたパスワードの使用を提案します。次の例では、ユーザーは提示されたパスワードを拒否することを選択しています。

```
switchxxxxxx(config)# line console
switchxxxxxx(config-line)# password generate-password
Generated password: aBgrT9!59Hq$
Accept generated password (y/n) [Y] n
"Auto generated password rejected by user. Password configuration is not added to
device configuration"
```

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*}

enable [**level** *privilege-level*] [**method** *hash-method*] **generate-password**

enable masked-secret [**level** *privilege-level*] [**method** *hash-method*]

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***]**：（オプション）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。

generate-password オプションを使用すると、パスワードを入力する代わりに、ランダムに生成されたパスワードの提案がユーザーに示されます。この提案は、現在のすべてのパスワード強度設定に準拠します

ユーザーは、提示されたパスワードを受け入れるか拒否するかを選択できます。ユーザーがパスワードを受け入れることを選択した場合、このパスワードは、構成ファイルで設定したイネーブルレベルに対して（暗号化された形式で）追加されます。

ユーザーがパスワードの提案を拒否した場合は、このイネーブルレベルを設定するためにコマンドを再度入力する必要があります。

例

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
$15$TqKC13RgV/QJb2Ma$4JmeD7wgRGH2iwGKMM+g4M53uQxpOMlhkUN56UMAEUuMqhw0bsRH27zakc7
2hLxt/YhEknPA6LX7fTgqwZn6Vw==
```

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
```

例 3：この例のコマンドには、**generate-password** キーワードが含まれています。この場合、デバイスはランダムに生成されたパスワードの使用を提案します。次の例では、ユーザーは提示されたパスワードを**受け入れる**ことを選択しています。

```
switchxxxxxx(config)# enable password generate-password
Generated password: aBgrT9!59Hq$
Accept generated password (y/n) [Y] y
“Configuration and password are added to device configuration. Please Note
password for future use”
```

例 4：この例のコマンドには、generate-password キーワードが含まれています。この場合、デバイスはランダムに生成されたパスワードの使用を提案します。次の例では、ユーザーは提示されたパスワードを拒否することを選択しています。

```
switchxxxxxx(config)# enable password generate-password
Generated password: aBgrT9!59Hq$
Accept generated password (y/n) [Y] n
“Auto generated password rejected by user. Password configuration is not added to
device configuration”
```

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}}}}

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

username *name* {[**method** hash-method] **masked-secret** | {**privilege** privilege-level {[**method** hash-method] **masked-secret**}

no username name

パラメータ

- ***name***：ユーザの名前。（範囲：1 ～ 20 文字）
- [**method** *hash-method*]：（オプション）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）
- **generate-password**：デバイスは、ランダムベースのパスワード提案を自動的に生成します。ユーザーは、提示されたパスワードを受け入れるか拒否するかを選択できます。

- **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。

generate-password オプションを使用すると、パスワードを入力する代わりに、ランダムに生成されたパスワードの提案がユーザーに示されます。この提案は、現在のすべてのパスワード強度設定に準拠します。ユーザーは、提示されたパスワードを受け入れるか拒否するかを選択できます。ユーザーがパスワードを受け入れることを選択した場合、このパスワードは、構成ファイルで設定したユーザー名に対して（暗号化された形式で）追加されます。

ユーザーがパスワードの提案を拒否した場合は、このユーザーを設定するためにコマンドを再度入力する必要があります。

ユーザーは、（現在のユーザー名を維持しつつ）現在のセッションへのログインに使用するアカウントのパスワードの変更を要求する場合、現在のパスワードを知っている必要があります。ユーザーは、現在のパスワードをクリアテキスト形式で入力するように求められます。パスワードの変更は、ユーザーが現在のパスワードを正しく入力した場合にのみ成功します。

最後のレベル 15 のユーザーは削除できず、リモートユーザーになることもできません。

例

例 1：ユーザー tom（レベル 15）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+g4M53uQxpOM1hkUN56UMAEUuMqhw0bsRH27zakc72hLxt/YhEknPA6LX7fTgqwZn6Vw==
```

例 3：この例のコマンドには、generate-password キーワードが含まれています。この場合、デバイスはランダムに生成されたパスワードの使用を提案します。次の例では、ユーザーは提示されたパスワードを受け入れることを選択しています。

```
switchxxxxxx(config)# username tom generate-password privilege 15
Generated password: aBgrT9!59Hq$
Accept generated password (y/n) [Y] y
"Configuration and password are added to device configuration. Please Note
password for future use."
```

例 4：この例のコマンドには、generate-password キーワードが含まれています。この場合、デバイスはランダムに生成されたパスワードの使用を提案します。次の例では、ユーザーは提示されたパスワードを拒否することを選択しています。

```
switchxxxxxx(config)# username tom generate-password privilege 15
Generated password: aBgrT9!59Hq$
Accept generated password (y/n) [Y] n
“Auto generated password rejected by user. Password configuration is not added to
device configuration.”
```

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              ----------
Robert          15              Jan 18 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。
Privilege	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 keyboard-pattern

パスワードの複雑さの設定の一部として QWERTY キーボードパターン関連の制限を有効にするには、passwords complexity keyboard-pattern 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。

QWERTY キーボードパターン関連の制限を無効にするには、このコマンドの no 形式を使用します。

構文

passwords complexity keyboard-pattern

no passwords complexity keyboard-pattern

パラメータ

該当なし

デフォルト設定

キーボードパターンのパスワードの複雑さの設定は、デフォルトでは無効になっています。

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

QWERTY キーボードでパスワードに使用できる連続した文字は 3 文字までと定義するには、**passwords complexity keyboard-pattern** コマンドを使用します。この制限は、キーボードの文字と数字にのみ適用され、記号には適用されません。順方向と逆方向の両方の文字シーケンスは禁止されています。

この制限は、次のいずれかのコマンドを使用して定義されたパスワードに適用されます。

- username
- enable password
- password

例

次に、キーボードパターンベースのパスワード制限を有効にする例を示します。

```
switchxxxxxx(config)# passwords complexity keyboard-pattern
```

aaa accounting login start-stop

デバイス管理セッションのアカウンティングを有効にするには、グローバル コンフィギュレーション モードで **aaa accounting login start-stop** コマンドを使用します。アカウンティングを無効にするには、このコマンドの **no** 形式を使用します。

構文

aaa accounting login start-stop group {**radius** | **tacacs+**}

no aaa accounting login start-stop

パラメータ

- **group radius**：アカウンティングに RADIUS サーバを使用します。
- **group tacacs+**：アカウンティングに TACACS+ サーバを使用します。

デフォルト設定

無効

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、デバイス管理セッション（SNMP ではなく、Telnet、シリアル、およびWEB）の記録を有効にします。

ユーザ名で識別されたユーザのみが記録されます（たとえば、ラインパスワードでログインしたユーザは記録されません）。

アカウンティングが有効になっている場合、ユーザがログインまたはログアウトするたびに、デバイスが RADIUS サーバに「開始」メッセージまたは「停止」メッセージを送信します。

デバイスは、利用可能な RADIUS/TACACS+ サーバーの設定された優先順位を使用して、RADIUS/TACACS+ サーバーを選択します。

次の表では、サポートされている RADIUS アカウンティング属性値と、その属性値がスイッチによりどのメッセージで送信されるかについて説明します。

名前	Start メッセージ	Stop メッセージ	説明
User-Name (1)	対応	対応	ユーザの ID。
NAS-IP-Address (4)	対応	対応	RADIUS サーバとのセッションで使用されるスイッチの IP アドレス。

名前	Start メッセージ	Stop メッセージ	説明
Class (25)	対応	対応	指定したセッションのすべてのアカウンティング パケットに任意の値が含まれています。
Called-Station-ID (30)	対応	対応	管理セッションで使用されるスイッチの IP アドレス。
Calling-Station-ID (31)	対応	対応	ユーザの IP アドレス。
Acct-Session-ID (44)	対応	対応	一意のアカウンティング ID。
Acct-Authentic (45)	対応	対応	サプリカントの認証方法を示します。
Acct-Session-Time（46）	非対応	対応	ユーザがログインしていた期間を示します。
Acct-Terminate-Cause（49）	非対応	対応	セッションが終了した理由。

次の表では、サポートされている TACACS+ アカウンティング引数と、その引数がスイッチによりどのメッセージで送信されるかについて説明します。

名前	説明	Start メッセージ	Stop メッセージ
task_id	一意のアカウンティング セッション ID。	対応	対応
user	ログイン認証用に入力されたユーザ名。	対応	対応
rem addr	ユーザの IP アドレス	対応	対応
elapsed-time	ユーザがログインしていた期間を示します。	非対応	対応
reason	セッションが終了した理由。	非対応	対応

例

```
switchxxxxxx(config)# aaa accounting login start-stop group radius
```

aaa accounting dot1x

802.1x セッションのアカウンティングを有効にするには、**aaa accounting dot1x** 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。アカウンティングを無効にするには、このコマンドの **no** 形式を使用します。

構文

aaa accounting dot1x start-stop group radius

no aaa accounting dot1x start-stop group radius

デフォルト設定

無効

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、802.1x セッションの記録を有効にします。

アカウンティングが有効になっている場合、ネットワークに対してユーザがログインまたはログアウトするたびに、デバイスがRADIUSサーバに開始メッセージまたは停止メッセージを送信します。デバイスは、利用可能なRADIUSサーバの設定された優先順位を使用して、RADIUSサーバを選択します。

新しいサプリカントにより古いサプリカントが置き換えられた場合（ポートステートが許可のままでも）、ソフトウェアは古いサプリカントの停止メッセージと、新しいサプリカントの開始メッセージを送信します。

マルチセッション モード（dot1x 複数ホスト認証）では、ソフトウェアは認証されたサプリカントごとに開始メッセージまたは停止メッセージを送信します。

複数ホスト モード（dot1x 複数ホスト）では、ソフトウェアは認証されたサプリカントにのみ開始メッセージまたは停止メッセージを送信します。ポートがforce-authorizedの場合、ソフトウェアは開始メッセージまたは停止メッセージを送信しません。

ソフトウェアは、ゲスト VLAN または認証されていない VLAN 上でトラフィックを送信しているホストの開始メッセージまたは停止メッセージを送信しません。

次の表では、サポートされているRADIUSアカウンティング属性値と、その属性値がスイッチによりいつ送信されるかについて説明します。

名前	Start	停止	説明
User-Name (1)	対応	対応	サプリカントの ID。

名前	Start	停止	説明
NAS-IP-Address (4)	対応	対応	RADIUS サーバとのセッションで使用されるスイッチの IP アドレス。
NAS-Port (5)	対応	対応	サプリカントがログインしているスイッチ ポート。
Class (25)	対応	対応	特定のセッションのすべてのアカウンティング パケットに含まれる任意の値。
Called-Station-ID (30)	対応	対応	スイッチの MAC アドレス。
Calling-Station-ID (31)	対応	対応	サプリカントの MAC アドレス。
Acct-Session-ID (44)	対応	対応	一意のアカウンティング ID。
Acct-Authentic (45)	対応	対応	サプリカントの認証方法を示します。
Acct-Session-Time（46）	非対応	対応	サプリカントがログインしていた時間を示します。
Acct-Terminate-Cause（49）	非対応	対応	セッションが終了した理由。
Nas-Port-Type (61)	対応	対応	サプリカントの物理ポートタイプを示します。

例

```
switchxxxxxx(config)# aaa accounting dot1x start-stop group radius
```

show accounting

show accounting EXEC モード コマンドは、スイッチでどのタイプのアカウンティングが有効になっているかに関する情報を表示します。

構文

show accounting

コマンド モード

ユーザ EXEC モード

例

次の例では、アカウンティング ステータスに関する情報を表示しています。

```
switchxxxxxx# show accounting
Login: Radius
802.1x: Disabled
```

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

パスワードエージングは、デフォルトで無効になっています。

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

パスワードエージング設定は、ローカルデータベースのユーザー、イネーブルパスワード、および回線パスワードに関連します。

パスワードエージングが有効になっている場合、パスワードの有効期限日まで 10 日以内の期間にユーザーがデバイスにログインすると、パスワードがまもなく期限切れになることを通知する警告が表示されます。ユーザーは、パスワードを変更しなくてもデバイスへのアクセスが許可されます。この段階で、期限日までにパスワードを変更するのはユーザーの責任です。

パスワードの有効期限が切れた後にユーザーがデバイスにログインすると、新しいパスワードを入力するように求められ、新しいパスワードが設定されるまでデバイス管理へのアクセスが許可されません。

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。

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
```

password complexity history

passwords complex history グローバル コンフィギュレーション モード コマンドは、パスワードを再利用できるようになるまでに必要なパスワード変更の回数を設定します。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 complexity history *number*

no passwords complexity history

パラメータ

number：パスワードの再利用が可能になるまでに必要なパスワード変更の回数を指定します。（範囲：3 ～ 12）。

デフォルト設定

デフォルトでは、パスワードの再利用までに必要なパスワード変更の回数は 12 回です。

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

この設定は、ローカルユーザーのパスワード、回線パスワード、およびイネーブルパスワードに関連します。

ローカルユーザーの履歴は、デバイスでサポートされているローカルユーザー数までのユーザーについて保持されます。

設定のダウンロード中は、パスワード履歴はチェックされません。

パスワード履歴チェックが無効になっている場合でも、パスワード履歴は保持されます。

例

次の例では、パスワードの再利用が可能になるまでに必要なパスワード変更の回数を 10 に設定しています。

```
switchxxxxxx(config)# passwords complexity history 10
```

aaa login-history file

aaa login-history file グローバル コンフィギュレーション モード コマンドは、ログイン履歴ファイルへの書き込みを有効にします。ログイン履歴ファイルへの書き込みを無効にするには、このコマンドの no 形式を使用します。

構文

aaa login-history file

no aaa login-history file

デフォルト設定

ログイン履歴ファイルへの書き込みが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

ログイン履歴は、デバイスの内部バッファに保存されます。

例

次の例では、ログイン履歴ファイルへの書き込みを有効にしています。

```
switchxxxxxx(config)# aaa login-history file
```

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

パラメータ

該当なし

デフォルト設定

該当なし

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 history is enabled, the number of previous passwords to check is 12
Passwords complexity is enabled with the following attributes:
 Minimal length: 8 characters
 Minimal classes: 3
 Maximum consecutive same characters: 3
 Password cannot include more than 2 sequential numbers or characters
Password cannot contain the username, manufacturer name or product name
Password must be different from current password
Password cannot contain commonly used passwords or known breached passwords
```

show users login-history

show users **login-history** 特権 EXEC モードコマンドは、ユーザーのログイン履歴に関する情報を表示します。

構文

show users login-history [**username** name]

パラメータ

- name：ユーザーの名前。（範囲：1 ～ 20 文字）。

デフォルト設定

該当なし

コマンド モード

特権 EXEC モード。

使用上のガイドライン

このコマンドは、Radius や TACACS などのリモート AAA サーバーを使用して認証されたユーザーではなく、ローカル AAA データベースを使用して認証されたユーザーに関する情報を表示します。

例

次に、ユーザーのログイン履歴に関する情報を表示する例を示します。

例 1：次の例では、180 秒以内に 18 回を超えてログイン試行に失敗した場合に、すべてのログイン要求を 180 秒間ブロックする方法を示します。

```
switchxxxxxx# show users login-history
File save: Enabled.
Login Time              Username  Protocol    Location
--------------------
Jan 18 2004 23:58:17    Robert    HTTP        172.16.1.8
Jan 19 2004 07:59:23    Robert    HTTP        172.16.1.8
Jan 19 2004 08:23:48    Bob       Serieal
Jan 19 2004 08:29:29    Robert    HTTP        172.16.1.8
Jan 19 2004 08:42:31    John      SSH         172.16.0.1
Jan 19 2004 08:49:52    Betty     Telnet      172.16.1.7
```

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。