# E

# enable password

さまざまな権限レベルへのアクセスを制御するローカル パスワードを設定するには、グローバル コンフィギュレーション モードで **enable password** コマンドを使用します。 パスワードの要件を削除するには、このコマンドの **no** 形式を使用します。

**enable password** [**level** *level*] {*password*| [ *encryption-type* ] *encrypted-password*}

**no enable password** [**level** *level*]

## 構文の説明

| | |
|---|---|
| **level** *level* | （任意）パスワードが適用されるレベル。 0 ～ 15 の数字を使用して最大 16 個の権限レベルを指定できます。 レベル 1 が通常の EXEC モード ユーザ権限です。 この引数が、コマンドまたはコマンドの **no** 形式で指定されていない場合、権限レベルはデフォルトの 15 になります（従来のイネーブル権限）。 |
| *password* | イネーブル モードを開始するパスワードのユーザ タイプ。 |
| *encryption-type* | （任意）パスワードの暗号化に使用されるシスコ独自のアルゴリズム。 現在使用可能な暗号化タイプは 5 だけです。 *encryption-type* を指定する場合は、入力する次の引数は暗号化されたパスワード（すでに Cisco ルータにより暗号化されたパスワード）である必要があります。 |
| *encrypted-password* | ユーザが入力する暗号化パスワード。別のルータ設定からコピーされます。 |

## コマンド デフォルト

パスワードは定義されていません。 デフォルトはレベル 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

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 10.0 | このコマンドが導入されました。 |

| リリース | 変更内容 |
|---|---|
| 12.2(33)SRA | このコマンドが、Cisco IOS Release 12.(33)SRA に統合されました。 |
| 12.2SX | このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。 |

## 使用上のガイドライン

**注意** enable password コマンドまたは enable secret コマンドのいずれも設定されていない場合に、コンソールに設定されている回線パスワードがある場合、コンソール回線パスワードはすべての VTY（Telnet および Secure Shell（SSH））セッションのイネーブル パスワードとして機能します。

このコマンドを **level** オプションとともに使用して、特定の権限レベルのパスワードを定義します。 レベルおよびパスワードを設定した後、このレベルにアクセスする必要のあるユーザにパスワードを提供してください。 各レベルでアクセスできるコマンドを指定するには、**privilege level** コンフィギュレーション コマンドを使用します。

通常、暗号化タイプを入力しません。 通常、このコマンドに Cisco ルータによりすでに暗号化されたパスワードをコピー アンド ペーストする場合に限り、暗号化タイプを入力します。

**注意** 暗号化タイプを指定し、クリア テキスト パスワードを入力した場合は、イネーブル モードを再開できません。 どのような方法で暗号化されたパスワードでも、失われた場合、回復することはできません。

**service password-encryption** コマンドが設定されている場合、**more nvram:startup-config** コマンドを入力すると、**enable password** コマンドで作成するパスワードの暗号化された形式が表示されます。

**service password-encryption** コマンドを使用して、パスワード暗号化をイネーブルまたはディセーブルにできます。

イネーブル パスワードの定義は、次のとおりです。

- 1 ～ 25 文字の大文字と小文字の英数字を含める必要があります。
- 先頭にスペースを指定できますが、無視されます。 ただし、中間および末尾のスペースは認識されます。
- パスワードを作成するときに、Ctrl+v キーの組み合わせを押してから疑問符（?）を入力すると、パスワードに疑問符を含めることができます。たとえば、*abc?123* というパスワードを作成するには、次の手順を実行します。
  - **abc** を入力します。

- **Ctrl+v** を押します。
- **?123** を入力します。

システムからイネーブル パスワードを入力するように求められた場合、疑問符の前に Ctrl+v を入力する必要はなく、パスワードのプロンプトにそのまま abc?123 と入力できます。

## 例

次に、権限レベル 2 のパスワード「pswd2」をイネーブルにする例を示します。

```
enable password level 2 pswd2
```

次に、暗号化タイプ 7 を使用して、ルータのコンフィギュレーション ファイルからコピーされた権限レベル 2 の暗号化パスワード「$1$i5Rkls3LoyxzS8t9」を設定する例を示します。

```
enable password level 2 5 $1$i5Rkls3LoyxzS8t9
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **disable** | 特権 EXEC モードを終了し、ユーザ EXEC モードに戻ります。 |
| **enable** | 特権 EXEC モードを開始します。 |
| **enable secret** | **enable password** コマンドよりも強化したセキュリティ レイヤを指定します。 |
| **privilege** | ユーザの新しい権限レベルを設定し、コマンドをその権限レベルに関連付けます。 |
| **service password-encryption** | パスワードを暗号化します。 |
| **show privilege** | 現在の権限レベルを表示します。 |

# enable secret

**enable password** コマンドよりも強化したセキュリティ レイヤを指定するには、グローバル コンフィギュレーション モードで **enable secret** コマンドを使用します。 **enable secret** 機能をオフにするには、このコマンドの **no** 形式を使用します。

**enable secret** [**level** *level*] {**[0]** *unencrypted-password*| *encryption-type encrypted-password*}

**no enable secret** [**level** *level*] [*encryption-type encrypted-password*]

## 構文の説明

| | |
|---|---|
| **level** *level* | （任意）パスワードが適用されるレベルを指定します。 1 ～ 15 の数字を使用して最大 15 個の権限レベルを指定できます。 レベル 1 が通常の EXEC モード ユーザ権限です。 *level* 引数が、コマンドまたはコマンドの **no** 形式で指定されていない場合、権限レベルはデフォルトの 15 になります（従来のイネーブル権限）。 |
| **0** | （任意）暗号化されていないクリアテキスト パスワードを指定します。 パスワードは Secure Hash Algorithm（SHA）256 シークレットに変換されて、ルータに保存されます。 |
| *unencrypted-password* | イネーブル モードを開始するユーザのパスワード。 このパスワードは、**enable password** コマンドで作成されたパスワードとは異なっている必要があります。 |
| *encryption-type* | パスワードの暗号化に使用されるシスコ独自のアルゴリズム。 このコマンドで使用可能な暗号化タイプは 4 および 5. です。<br>• **4**：SHA-256 で暗号化されたシークレット ストリングを指定します。 SHA256 シークレット ストリングはルータ コンフィギュレーションからコピーされます。<br>• **5**：メッセージ ダイジェスト アルゴリズム 5（MD5）により暗号化されたシークレットを指定します。 |
| *encrypted-password* | 別のルータ コンフィギュレーションからコピーされる暗号化パスワード。 |

## コマンド デフォルト

グローバルは定義されていません。コンフィグ(config)トのレベルは 15 です。

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 11.0 | このコマンドが導入されました。 |
| 12.2(33)SRA | このコマンドが、Cisco IOS Release 12.2(33)SRA に統合されました。 |
| 12.2SX | このコマンドは、Cisco IOS Release 12.2SX トレインでサポートされます。このトレインの特定の 12.2SX リリースにおけるサポートは、フィーチャ セット、プラットフォーム、およびプラットフォーム ハードウェアによって異なります。 |
| 15.0(1)S | このコマンドが Cisco IOS Release 15.0(1)S に統合されました。 暗号化タイプ **4** のサポートが追加されました。 |
| Cisco IOS XE Release 3.1S | このコマンドが Cisco IOS XE Release 3.1S に統合されました。 暗号化タイプ **4** のサポートが追加されました。 |
| 15.1(4)M | このコマンドが変更されました。 暗号化タイプ **4** のサポートが追加されました。 |
| Cisco IOS Release 3.3.0SG | このコマンドが変更されました。 暗号化タイプ **5** はサポートされなくなりました。 |
| 15.1(1)SY | このコマンドが、Cisco IOS Release 15.1(1)SY に統合されました。 |
| Cisco IOS XE Release 3.2SE | このコマンドが変更されました。 暗号化タイプ **5** のサポート廃止の警告メッセージが変更されました。 |

## 使用上のガイドライン

**注意** **enable password** コマンドまたは **enable secret** コマンドのいずれも設定されていない場合に、コンソールに回線パスワードが設定されている場合、コンソール回線パスワードはすべての vty（Telnet および Secure Shell（SSH））セッションのイネーブル パスワードとして機能します。

イネーブル パスワードよりも強化したセキュリティ レイヤを追加するには、**enable secret** コマンドを使用します。 **enable secret** コマンドでは、不可逆的な暗号化機能を使用してイネーブル シークレットパスワードが保存されるため、セキュリティが向上します。追加されたセキュリティ暗号化のレイヤは、パスワードがネットワークを通過する、または TFTP サーバに保存される環境において役立ちます。

通常、ルータのコンフィギュレーション ファイルからコピーした暗号化パスワードをこのコマンドにペーストする場合にのみ、暗号化タイプを入力します。

注意 暗号化タイプを指定し、クリアテキスト パスワードを入力した場合は、イネーブル モードを再開できません。 どのような方法で暗号化されたパスワードでも、失われた場合、回復することはできません。

**enable password** コマンドと **enable secret** コマンドに同じパスワードを使用した場合は、その方法が推奨されないことを示すエラー メッセージの警告が表示されますが、パスワードは受け入れられます。 ただし、同じパスワードを使用することにより、**enable secret** コマンドによって提供される追加のセキュリティが損なわれます。

（注） **enable secret** コマンドを使用してパスワードを設定した後には、**enable password** コマンドを使用して設定されたパスワードは、**enable secret** がディセーブルになっている場合、またはCisco IOS ソフトウェアの古いバージョンが使用されている場合（古い rxboot イメージを実行している場合など）にのみ動作します。 また、どのような方法で暗号化されたパスワードでも、失われた場合、回復することはできません。

**service password-encryption** コマンドが設定されている場合、**more nvram:startup-config** コマンドを入力すると、作成するパスワードの暗号化された形式が表示されます。

**service password-encryption** コマンドを使用して、パスワード暗号化をイネーブルまたはディセーブルにできます。

イネーブル パスワードの定義は、次のとおりです。

- 大文字と小文字両方の 1 ～ 25 文字の英数字を含める必要があります。
- 先頭にスペースを指定できますが、無視されます。 ただし、中間および末尾のスペースは認識されます。
- パスワードを作成するときに、Ctrl+v キーの組み合わせを押してから疑問符（?）を入力すると、パスワードに疑問符を含めることができます。たとえば、*abc?123* というパスワードを作成するには、次の手順を実行します。
  - **abc** を入力します。
  - **Ctrl+v** を押します。
  - **?123** を入力します。

システムからイネーブル パスワードを入力するように求められた場合、疑問符の前に Ctrl+v を入力する必要はなく、パスワードのプロンプトに **abc?123** と入力できます。

（注） 3.3.0SG から 3.2.0SG へのダウングレード中に、SHA256 により暗号化されたパスワードが設定されていて、SHA256 により暗号化されたパスワードが警告なしで失われた場合は、シークレット パスワードを再設定する必要があります。

## 例

次に、**enable secret** コマンドを使用してパスワードを指定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# enable secret password
```

**enable secret** コマンドでパスワードを指定した後には、ユーザはアクセスするために、このパスワードを入力する必要があります。 **enable password** コマンドで設定されたパスワードは、動作しなくなります。

```
Password: password
```

次に、暗号化タイプ 4 を使用して、ルータのコンフィギュレーション ファイルからコピーされた権限レベル 2 の暗号化パスワード「$1$FaD0$Xyti5Rkls3LoyxzS8」をイネーブルにする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# enable password level 2 4 $1$FaD0$Xyti5Rkls3LoyxzS8
```

次に、ユーザが **enable secret 5** *encrypted-password* コマンドを入力したときに表示される警告メッセージの例を示します。

```
Device(config)# enable secret 5 $1$FaD0$Xyti5Rkls3LoyxzS8

Warning: The CLI will be deprecated soon
'enable secret 5 <password>'
Please move to 'enable secret <password>' CLI
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **enable** | 特権 EXEC モードを開始します。 |
| **enable password** | さまざまな権限レベルへのアクセスを制御するローカル パスワードを設定します。 |
| **service password-encryption** | パスワードを暗号化します。 |

# enrollment http-proxy

プロキシ サーバを介して HTTP により認証局（CA）にアクセスするには、ca-trustpoint コンフィギュレーション モードで**enrollment http-proxy** コマンドを使用します。

**enrollment http-proxy** *host-name port-num*

## 構文の説明

| | |
|---|---|
| *host-name* | CA を取得するために使用するプロキシ サーバを定義します。 |
| *port-num* | CA へのアクセスに使用するポート番号を指定します。 |

## コマンド デフォルト

このコマンドをイネーブルにしない場合、CA は HTTP 経由でアクセスされません。

## コマンド モード

ca-trustpoint コンフィギュレーション

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 12.2(8)T | このコマンドが導入されました。 |
| 12.2(18)SXD | このコマンドが、Cisco IOS Release 12.2(18)SXD に統合されました。 |

## 使用上のガイドライン

**enrollment http-proxy** コマンドは、**enrollment** コマンドとともに使用する必要があります。このコマンドにより、CA の登録パラメータを指定します。

## 例

次に、bomborra プロキシ サーバを介して HTTP により「ka」という名前の CA にアクセスする例を示します。

```
crypto ca trustpoint ka
 enrollment url http://kahului
 enrollment http-proxy bomborra 8080
 crl optional
```

関連コマンド

| コマンド | 説明 |
|---|---|
| **crypto ca trustpoint** | ルータが使用する CA を宣言します。 |
| **enrollment** | CA の登録パラメータを指定します。 |

# enrollment url（ca-profile-enroll）

登録要求を送信する認証局（CA）サーバの URL を指定するには、ca-profile-enroll コンフィギュレーション モードで **enrollment url** コマンドを使用します。 登録プロファイルから登録 URL を削除するには、このコマンドの **no** 形式を使用します。

**enrollment url** *url*

**no enrollment url** *url*

## 構文の説明

| | |
|---|---|
| *url* | ルータが証明書要求を送信する CA サーバの URL。<br>登録に Simple Certificate Enrollment Protocol（SCEP）を使用している場合、*url* 引数は、http://CA_name（CA_name は、CA のホスト ドメイン ネーム システム（DNS）名、または IP アドレス）の形式で指定する必要があります。<br>登録に TFTP を使用している場合は、*url* 引数を tftp://certserver/file_specification の形式で指定する必要があります。 （URL にファイル指定が含まれない場合、ルータの完全修飾ドメイン名（FQDN）が使用されます）。 |

## コマンド デフォルト

このコマンドを使用して指定するまで、ルータは CA URL を認識しません。

## コマンド モード

Ca-profile-enroll コンフィギュレーション

## コマンド履歴

| リリース | 変更内容 |
|---|---|
| 12.2(13)ZH | このコマンドが導入されました。 |
| 12.3(4)T | このコマンドが Cisco IOS Release 12.3(4)T に統合されました。 |

## 使用上のガイドライン

このコマンドにより、証明書を認証し、証明書を登録するための異なる URL または異なる方法（たとえば、手動認証、TFTP 登録など）を指定することができます。

## 例

次に、プロファイル名「E」の HTTP 経由での証明書登録をイネーブルにする例を示します。

```
crypto pki trustpoint Entrust
  enrollment profile E
  serial
crypto pki profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **crypto pki profile enrollment** | 登録プロファイルを定義します。 |