



パスワード暗号化の設定

この章では、Cisco NX-OS デバイスにパスワード暗号化を設定する手順について説明します。
この章は、次の項で構成されています。

- [AES パスワード暗号化およびプライマリ暗号キーについて \(1 ページ\)](#)
- [パスワード暗号化の注意事項と制約事項 \(2 ページ\)](#)
- [パスワード暗号化のデフォルト設定 \(2 ページ\)](#)
- [パスワード暗号化の設定 \(2 ページ\)](#)
- [パスワード暗号化の設定の確認 \(5 ページ\)](#)
- [パスワード暗号化の設定例 \(5 ページ\)](#)

AES パスワード暗号化およびプライマリ暗号キーについて

強力で、反転可能な 128 ビットの高度暗号化規格 (AES) パスワード暗号化を有効にすることができます。タイプ 6 暗号化とも言います。タイプ 6 暗号化の使用を開始するには、AES パスワード暗号化機能を有効にし、パスワード暗号化および復号化に使用されるプライマリ暗号キーを構成する必要があります。

AES パスワード暗号化を有効にしてプライマリ キーを構成すると、タイプ 6 パスワード暗号化を無効にしない限り、サポートされているアプリケーション (現在は RADIUS と TACACS+) の既存および新規作成されたクリア テキスト パスワードがすべて、タイプ 6 暗号化の形式で保存されます。また、既存の弱いすべての暗号化パスワードをタイプ 6 暗号化パスワードに変換するように Cisco NX-OS を構成することもできます。

関連トピック

- [プライマリ キーの設定および AES パスワード暗号化機能の有効化 \(3 ページ\)](#)
- [グローバル RADIUS キーの設定](#)
- [特定の RADIUS サーバ用のキーの設定](#)
- [グローバル TACACS+ キーの設定](#)
- [特定の TACACS+ サーバ用のキーの設定](#)

プライマリ キーの設定および AES パスワード暗号化機能の有効化 (3 ページ)

パスワード暗号化の注意事項と制約事項

パスワード暗号化設定時の注意事項と制約事項は次のとおりです。

- AES パスワード暗号化機能、関連付けられた暗号化と復号化のコマンド、およびプライマリ キーを設定できるのは、管理者権限 (network-admin) を持つユーザだけです。
- AES パスワード暗号化機能を使用できるアプリケーションは RADIUS と TACACS+ だけです。
- タイプ 6 暗号化パスワードを含む構成は、ロールバックに準拠していません。
- プライマリ キーがなくても AES パスワード暗号化機能を有効にできますが、プライマリ キーがシステムに存在する場合だけ暗号化が開始されます。
- TACACS+ の場合、AES パスワード暗号化機能をイネーブルにし、プライマリキーを設定した後、**encryption re-encrypt obfuscated** コマンドを実行して、パスワードをタイプ 6 暗号化パスワードに変換する必要があります。
- プライマリ キーを削除するとタイプ 6 暗号化が停止され、同じプライマリ キーが再構成されない限り、既存のすべてのタイプ 6 暗号化パスワードが使用できなくなります。
- デバイス設定を別のデバイスに移行するには、他のデバイスに移植する前に設定を復号化するか、または設定が適用されるデバイス上に同じプライマリ キーを設定します。
- Cisco NX-OS リリース 9.3(6) 以降、タイプ 6 暗号化パスワードを元の状態に戻すことは、MACsec キーチェーンではサポートされていません。

パスワード暗号化のデフォルト設定

次の表に、パスワード暗号化パラメータのデフォルト設定を示します。

表 1: パスワード暗号化パラメータのデフォルト設定

パラメータ	デフォルト
AES パスワード暗号化機能	無効
プライマリ 鍵	未設定

パスワード暗号化の設定

ここでは、Cisco NX-OS デバイスでパスワード暗号化を設定する手順について説明します。

プライマリ キーの設定および AES パスワード暗号化機能の有効化

タイプ6暗号化用のプライマリ キーを構成し、高度暗号化規格（AES）パスワード暗号化機能を有効にすることができます。

Procedure

	Command or Action	Purpose
ステップ 1	[no] key config-key ascii[<new_key> old <old_master_key>] Example: <pre>switch# key config-key ascii New Master Key: Retype Master Key:</pre>	プライマリ キー（マスター キー）を、AES パスワード暗号化機能で使用するよう設定します。プライマリ キーは、16 ～ 32 文字の英数字を使用できます。このコマンドの no 形式を使用すると、いつでもプライマリ キーを削除できます。 プライマリ キーを設定する前に AES パスワード暗号化機能を有効にすると、プライマリ キーが設定されていない限りパスワード暗号化が実行されないことを示すメッセージが表示されます。プライマリ キーがすでに設定されている場合は、新しいプライマリ キーを入力する前に現在のプライマリ キーを入力するように求められます。 Note Cisco NX-OS リリース 10.3(2)F 以降、DME ペイロードおよび非インタラクティブ モードを使用して、プライマリ キーを構成できます。
ステップ 2	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	グローバル設定モードを開始します。
ステップ 3	[no] feature password encryption aes Example: <pre>switch(config)# feature password encryption aes</pre>	AES パスワード暗号化機能を有効化または無効化します。
ステップ 4	encryption re-encrypt obfuscated Example: <pre>switch(config)# encryption re-encrypt obfuscated</pre>	既存の単純で脆弱な暗号化パスワードをタイプ 6 暗号化パスワードに変換します。

	Command or Action	Purpose
ステップ 5	(Optional) show encryption service stat Example: <pre>switch(config)# show encryption service stat</pre>	AES パスワード暗号化機能とプライマリ キーの設定ステータスを表示します。
ステップ 6	copy running-config startup-config Example: <pre>switch(config)# copy running-config startup-config</pre>	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。 Note このコマンドは、実行コンフィギュレーションとスタートアップ コンフィギュレーションのプライマリ キーを同期するために必要です。

Related Topics

[AES パスワード暗号化およびプライマリ暗号キーについて \(1 ページ\)](#)

[AES パスワード暗号化およびプライマリ暗号キーについて \(1 ページ\)](#)

[キーのテキストの設定](#)

[キーの受け入れライフタイムおよび送信ライフタイムの設定](#)

既存のパスワードのタイプ 6 暗号化パスワードへの変換

既存の単純で脆弱な暗号化パスワードをタイプ 6 暗号化パスワードに変換できます。

Before you begin

AES パスワード暗号化機能を有効にし、プライマリ キーを設定したことを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	encryption re-encrypt obfuscated Example: <pre>switch# encryption re-encrypt obfuscated</pre>	既存の単純で脆弱な暗号化パスワードをタイプ 6 暗号化パスワードに変換します。

タイプ 6 暗号化パスワードの元の状態への変換

タイプ 6 暗号化パスワードを元の状態に変換できます。

Before you begin

プライマリ キーを設定したことを確認します。

Procedure

	Command or Action	Purpose
ステップ 1	encryption decrypt type6 Example: <pre>switch# encryption decrypt type6 Please enter current Master Key:</pre>	タイプ 6 暗号化パスワードを元の状態に変換します。

タイプ 6 暗号化パスワードの削除

Cisco NX-OS デバイスからすべてのタイプ 6 暗号化パスワードを削除できます。

Procedure

	Command or Action	Purpose
ステップ 1	encryption delete type6 Example: <pre>switch# encryption delete type6</pre>	すべてのタイプ 6 暗号化パスワードを削除します。

パスワード暗号化の設定の確認

パスワード暗号化の設定情報を表示するには、次の作業を行います。

コマンド	目的
show encryption service stat	AES パスワード暗号化機能とプライマリ キーの設定ステータスを表示します。

パスワード暗号化の設定例

次の例は、プライマリ キーを作成し、AES パスワード暗号化機能を有効にして、TACACS+ アプリケーションのためのタイプ 6 暗号化パスワードを構成する方法を示しています。

```
key config-key ascii
  New Master Key:
  Retype Master Key:
configure terminal
feature password encryption aes
show encryption service stat
Encryption service is enabled.
```

```
Master Encryption Key is configured.  
Type-6 encryption is being used.  
feature tacacs+  
tacacs-server key Cisco123  
show running-config tacacs+  
feature tacacs+  
logging level tacacs 5  
tacacs-server key 6  
"JDYkqyIFWeBvzpljSfWmRZrmRSRE8syxKlOSjP9RCckFinZbJI3GD5c6rckJR/Qju2PKLmOewbheAA=="
```

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。