



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 \(3 ページ\)](#)
- [パスワード暗号化の設定 \(3 ページ\)](#)
- [パスワード暗号化の設定の確認 \(7 ページ\)](#)
- [パスワード暗号化の設定例 \(7 ページ\)](#)

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 (タイプ 6 暗号化ともいう) を有効にすることができます。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設定する必要があります。

AES パスワード暗号化をイネーブルにしてプライマリ キーを設定すると、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 を設定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設定は、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。
- タイプ 6 暗号化は、MACsec キーチェーンでのみサポートされます。レガシー RPM または cloudsec キーではサポートされません。
- 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。
- タイプ 6 暗号化は、AES パスワード暗号化機能が有効で、プライマリ キーが設定されている場合にのみ設定できます。
- プライマリ キーが設定され、AES パスワード暗号化機能がスイッチでイネーブルになっている場合、キーチェーン `infra` の下の各 MACsec キー ストリング設定は、タイプ 6 暗号化で自動的に暗号化されます。
- プライマリ キーの設定は、スイッチに対してローカルです。あるスイッチからタイプ 6 に設定された実行データを取得し、別のプライマリ キーが設定されている別のスイッチに適用すると、新しいスイッチでの復号化は失敗します。
- タイプ 6 暗号化の後にスタートアップ コンフィギュレーションを消去し、コンフィギュレーション置換機能を使用すると、プライマリ キーが PSS に保存されないため、コンフィギュレーションの置換は失敗します。したがって、MACsec タイプ 6 暗号化キー文字列の設定が失われます。

- タイプ 6 のキーを設定すると、SKSD が提供する復号コマンドを適用しないと、既存のタイプ 6 の暗号化キー文字列をタイプ 7 の暗号化キー文字列に変更できません。
- タイプ 6 暗号化がサポートされていない古いイメージでコールドリブートによってシステムをダウングレードする場合は、コールドリブートを続行する前に設定を削除する必要があります。これを行わないと、設定が失われます。
- システムをダウングレードすると、タイプ 6 の設定は失われます。
- ISSD によってシステムをダウングレードすると、機能確認チェックが呼び出され、ダウングレードに進む前に設定を削除するように通知されます。**encryption decrypt** コマンドを使用して、タイプ 6 暗号化キーをタイプ 7 暗号化キーに変換してから、ダウングレードを続行できます。
- ISSU のアップグレード中に、タイプ 7 暗号化キーを含む古いイメージからタイプ 6 暗号化をサポートする新しいイメージに移行する場合、再暗号化が強制されるまで、rpm は既存のキーをタイプ 6 暗号化キーに変換しません。再暗号化を適用するには、**encryption re-encrypt obfuscated** コマンドを使用します。
- タイプ 6 暗号化の後にプライマリ キーを変更すると、既存のタイプ 6 暗号化キー文字列に対する復号コマンドは失敗します。既存のタイプ 6 キースtring を削除し、新しいキースtring を設定する必要があります。

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 キー	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 キーを設定し、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 Example: <pre>switch# key config-key ascii New Master Key: Retype Master Key:</pre>	<p>プライマリ 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。</p> <p>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。</p>
ステップ 2	configure terminal Example: <pre>switch# configure terminal switch(config)#</pre>	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	[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。
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。

	Command or Action	Purpose
		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: switch# encryption re-encrypt obfuscated	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。この機能は、macsec キーチェーンではサポートされていません。

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:	タイプ6暗号化パスワードを元の状態に変換します。

	Command or Action	Purpose
	switch# encryption decrypt type6 Please enter current Master Key:	

MACsec キーでのタイプ 6 暗号化の有効化

Advanced Encryption Standard (AES) パスワード暗号化機能とも呼ばれるタイプ 6 暗号化機能を使用すると、タイプ 6 暗号化形式で MACsec キーを安全に保存できます。

Cisco NX-OS リリース 9.3(5) 以降では、MACsec 機能をサポートするすべての Cisco Nexus 9000 シリーズ スイッチに、タイプ 6 暗号化形式で MACsec キーを保存できます。

手順

	コマンドまたはアクション	目的
ステップ 1	configure terminal 例： switch# configure terminal switch(config)#	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 2	[no] key config-key ascii 例： switch(config)# key config-key ascii switch(config)# New Master Key: Switch(config)# Retype Master Key:	スイッチのマスターキーを設定します。
ステップ 3	[no] feature password encryption aes 例： switch(config)# feature password encryption aes	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	key chain name macsec 例： switch(config)# key chain 1 macsec switch(config-macseckeychain)#	MACSec キーチェーンを作成して MACSec キーのセットを保持し、MACSec キーチェーン設定モードを開始します。
ステップ 5	key key-id 例： switch(config-macseckeychain)# key 1000 switch(config-macseckeychain-macseckey)#	MAC secキーを作成し、MACsec キー設定モードを開始します。範囲は 1 ~ 32 オクテットで、最大サイズは 64 です。AES_128 は 32 ビットで使用され、AES_256 は 64 ビットで使用されます。
ステップ 6	key-octet-string octet-string cryptographic-algorithm {AES_128_CMAC AES_256_CMAC} 例：	そのキーの octet スtring を設定します。octet-string 引数には、最大 64 文字の 16 進数文字を含めることができます。オクテット キーは内部でエンコードされるため、 show running-config

	コマンドまたはアクション	目的
	<pre>switch(config-macseckeychain-macseckey) # key-octet-string abcdef0123456789abc0ef0123456789abc0ef0123456789abc0ef0123456789 cryptographic-algorithm AES_256_CMAC</pre>	<p>macsec コマンドの出力にクリア テキストのキーが現れることはありません。</p> <p>キーオクテット文字列には、次のものが含まれます。</p> <ul style="list-style-type: none"> • 0 暗号化タイプ - 暗号化なし (デフォルト) • 6 Encryption Type-Proprietary (Type-6 encrypted) • 7 暗号化タイプ - 最大 64 文字の、独自仕様 WORD キー オクテット文字列

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	<p>encryption delete type6</p> <p>Example:</p> <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

次に、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設定する例を示します。

```
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=="
```