管理者のユーザ名とパスワードの設定

- 機能情報の確認，1 ページ
- 管理者のユーザ名とパスワードの設定について，1 ページ
- 管理者のユーザ名とパスワードの設定，3 ページ
- 例：管理者のユーザ名とパスワードの設定，5 ページ
- 管理者のユーザ名とパスワードに関する追加情報，5 ページ
- 管理者のユーザ名とパスワードの設定の機能履歴と情報，6 ページ

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。 Cisco.com のアカウントは必要ありません。

管理者のユーザ名とパスワードの設定について

管理者のユーザ名とパスワードを設定しておくと、権限のないユーザによるスイッチの設定変更や設定情報の表示を防ぐことができます。この項では、初期設定とパスワード リカバリの手順を説明します。

スイッチに関連付けられた一つ以上のアクセス ポイントを管理および設定する管理者のユーザ名とパスワードを設定することもできます。

強力なパスワード

管理者ユーザがアクセス ポイントを管理するため、ASCII キーによる暗号化パスワードなどの強力な管理者パスワードを設定できます。

強力なパスワードを作成する場合は、次のガイドラインに従ってください。

- 次のカテゴリ（小文字、大文字、数字、特殊文字）のうち、少なくとも 3 つが必要です。

（注） GUI のログインでは、ユーザ名とパスワードでの特殊文字の使用はサポートされません。

- 新しいパスワードは、関連付けられているユーザ名と同じにしたり、ユーザ名を反転させたりすることはできません。
- パスワードの文字を 4 回以上連続して繰り返すことはできません。
- パスワードに **cisco**、**ocsic**、**admin**、**nimda** を使用することはできません。また、これらの文字のいくつかを大文字にしたり、i を「1」、「|」、または「!」に、「o」を「0」に、または「s」を「$」に置き換たりすることもできません。
- ユーザ名およびパスワードで許容される最大文字数は 32 文字です。

暗号化パスワード

パスワードには 3 種類のキーを設定できます。

- ランダムに生成されたキー：このキーはランダムに生成され、最も安全なオプションです。1 台のシステムから別のシステムへコンフィギュレーション ファイルをエクスポートするには、キーもエクスポートする必要があります。
- 静的キー：最も単純なオプションは固定（静的）暗号キーを使用することです。固定キーを使用すれば、キー管理は必要ありませんが、キーが何らかの方法で検出されると、データはそのキーの知識を持つ任意のユーザによって復号化できます。これは、セキュアなオプションではなく、CLI では難読化と呼ばれます。
- ユーザによって定義されたキー：ユーザ自身がキーを定義できます。1 台のシステムから別のシステムへコンフィギュレーション ファイルをエクスポートするには、双方のシステムで同じキー設定する必要があります。

管理者のユーザ名とパスワードの設定

手順の概要

1. **configure terminal**
2. **wireless security strong-password**
3. **username** *admin-username***password {0** *unencrypted_password* **| 7** *hidden_password***|** *unencrypted_text***}**
4. **username** *admin-username***secret {0** *unencrypted_secret_text* **| 4** *SHA256 encrypted_secret_text***| 5** *MD5 encrypted_secret_text***| LINE}**
5. **ap mgmtuser username** *username***password{0** *unencrypted password* **| 8** *AES encrypted password***}secret{0** *unencrypted password* **| 8** *AES encrypted password***}**
6. **ap dot1x username** *username***password{0** *unencrypted password* **| 8** *AES encrypted password***}**
7. **end**
8. **ap nameapnamemgmtuser username** *username***password** *password***secret** *secret _text*
9. **apnameapnamedot1x-user** *username***password** *password*

手順の詳細

	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`	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	**wireless security strong-password** 例： `Switch(config)# wireless security strong-password`	管理者ユーザのための強力なパスワード ポリシーをイネーブルにします。
ステップ 3	**username** *admin-username***password {0** *unencrypted_password* **| 7** *hidden_password***|** *unencrypted_text***}** 例： `Switch(config)# username adminuser1 password 0 QZsek239@`	管理者のユーザ名とパスワードを指定します。 管理者は、スイッチを設定し、設定情報を表示できます。
ステップ 4	**username** *admin-username***secret {0** *unencrypted_secret_text* **| 4** *SHA256 encrypted_secret_text***| 5** *MD5 encrypted_secret_text***| LINE}** 例： `Switch(config)# username adminuser1 secret 0 QZsek239@`	管理者のシークレットを指定します。

	コマンドまたはアクション	目的
ステップ 5	**ap mgmtuser username** *username***password{0** *unencrypted password* **| 8** *AES encrypted password***}secret{0** *unencrypted password* **| 8** *AES encrypted password***}** 例： `Switch(config)# ap mgmtuser username cisco password 0 Qwci12@ secret 0 Qwci14@!`	スイッチへ設定されたすべてのアクセス ポイントを管理するため、システムの管理者のユーザ名とパスワードを指定します。 特権アクセス ポイント管理のためのシークレット テキストを含めることもできます。 （注） パスワードが強力なパスワードポリシーを満たしていない場合、パスワードは有効なエラーメッセージとともに拒否されます。たとえば、次のパスワードは、強力なパスワードでないため、拒否されます。 `Switch# ap mgmtuser username cisco password 0 abcd secret 0 1234`
ステップ 6	**ap dot1x username** *username***password{0** *unencrypted password* **| 8** *AES encrypted password***}** 例： `Switch(config)# ap dot1x username cisco password 0 Qwci12@`	スイッチへ設定されたすべてのアクセス ポイントを管理するため、802.1X のユーザ名とパスワードを指定します。
ステップ 7	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 8	**ap nameapnamemgmtuser username** *username***password** *password***secret** *secret _text* 例： `Switch# ap name APf0f7.55c7.7b23 mgmtuser username cisco password Qne35! secret Nzep592$`	スイッチに設定された特定のアクセス ポイントを管理するための管理者のユーザ名、パスワード、およびシークレット テキストを設定します。
ステップ 9	**apnameapnamedot1x-user** *username***password** *password* 例： `Switch# ap name APf0f7.55c7.7b23 dot1x-user username cisco password Qne35!`	特定のアクセス ポイントの 802.1X ユーザ名とパスワードを設定します。

例：管理者のユーザ名とパスワードの設定

次に、コンフィギュレーション モードで、管理者のユーザ名と、厳格なパスワード ポリシーに則ったパスワードを設定する例を示します。

```
Switch# configure terminal
Switch(config)# wireless security strong-password
Switch(config)# username adminuser1 password 0 QZsek239@
Switch(config)# ap mgmtuser username cisco password 0 Qwci12@ secret 0 Qwci14@!
Switch(config)# ap dot1x username cisco password 0 Qwci12@
Switch# end
```

次に、グローバル EXEC モードで、管理者のユーザ名およびパスワードをアクセス ポイントに設定する例を示します。

```
Switch# wireless security strong-password
Switch# ap name APf0f7.55c7.7b23 mgmtuser username cisco password Qwci12@ secret Qwci14@
Switch# ap name APf0f7.55c7.7b23 dot1x-user username cisco password Qwci12@
Switch# end
```

管理者のユーザ名とパスワードに関する追加情報

関連資料

関連項目	マニュアル タイトル
システム管理コマンド	『*System Management Command Reference Guide (Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)*』

標準および RFC

標準/RFC	Title
なし	—

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

管理者のユーザ名とパスワードの設定の機能履歴と情報

リリース	機能情報
Cisco IOS XE 3.2SECisco IOS XE 3.2SECisco IOS XE 3.3SE	この機能が導入されました。