パスワード管理

Cisco UCS パスワードに関するガイドライン

ローカル認証された各ユーザ アカウントには、パスワードが必要です。admin または aaa の権限を持つユーザは、Cisco UCS Managerを設定して、ユーザのパスワードの強度チェックを実行できます。表 1 : UCS パスワードに使用可能な ASCII 文字の表 （1 ページ） に、UCS パスワードに使用可能な ASCII 文字のリストを示します。

表 *1 : UCS* パスワードに使用可能な *ASCII* 文字の表

出力可能な ASCII 文字	説明
A ～ Z	大文字の A ～ Z
a ～ z	小文字の a ～ z
0 ～ 9	数字の 0 ～ 9
!	感嘆符
"	引用符
%	パーセント記号
&	アンパサンド
'	アポストロフィ

出力可能な ASCII 文字	説明
(	左カッコ
)	右カッコ
*	アスタリスク
+	プラス記号
,	カンマ
-	ハイフン
.	ピリオド
/	スラッシュ
:	コロン
;	セミコロン
<	小なり
>	大なり
@	アット マーク
[	開き大カッコ
\	バックスラッシュ
]	閉じ大カッコ
^	キャレット
_	アンダースコア
`	アクサングラーブ
{	開き中カッコ
|	縦棒
}	閉じ中カッコ
~	チルダ

シスコでは強力なパスワードを使用することを推奨しています。そうしなかった場合、ローカル認証されたユーザに対するパスワードの強度チェックで、Cisco UCS Manager によって次の要件を満たさないパスワードが拒否されます。

- 8 ～ 80 文字を含む。
- パスワードの強度の確認が有効になっている場合はパスワード長は可変で、6 ～ 80 文字の間で設定できます。

（注） デフォルトは 8 文字です。

- 次の少なくとも 3 種類を含む。
  - 小文字
  - 大文字
  - 数字
  - 特殊文字
- aaabbb など連続して 3 回を超えて繰り返す文字を含まない。
- ユーザ名と同一、またはユーザ名を逆にしたものではない。
- パスワード ディクショナリ チェックに合格する。たとえば、パスワードには辞書に記載されている標準的な単語に基づいたものを指定することはできません。
- 次の記号を含まない。$（ドル記号）、?（疑問符）、=（等号）。
- ローカル ユーザ アカウントおよび admin アカウントのパスワードは空白にしない。

Cisco UCS ユーザ名に関するガイドライン

ユーザ名は、Cisco UCS Manager のログイン ID としても使用されます。Cisco UCS ユーザ アカウントにログイン ID を割り当てるときは、次のガイドラインおよび制約事項を考慮してください。

- ログイン ID には、次を含む 1 ～ 32 の文字を含めることができます。
  - 任意の英字
  - 任意の数字
  - _（アンダースコア）
  - -（ダッシュ）
  - .（ドット）
- ログイン ID は、Cisco UCS Manager 内で一意である必要があります。
- ログイン ID は、英文字から始まる必要があります。アンダースコアなどの特殊文字や数字から始めることはできません。

- ログイン ID では、大文字と小文字が区別されます。
- すべてが数字のログイン ID は作成できません。
- ユーザ アカウントの作成後は、ログイン ID を変更できません。ユーザ アカウントを削除し、新しいユーザ アカウントを作成する必要があります。

変更間隔のパスワード変更の最大回数の設定

パスワード プロファイル プロパティを変更するには、admin または aaa 権限を持っている必要があります。パスワード履歴を除き、これらのプロパティは、admin または aaa 権限を持つユーザに適用されません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope password-profile**	パスワード プロファイル セキュリティ モードを開始します。
ステップ 3	UCS-A /security/password-profile # **set change-during-interval enable**	ローカル認証されたユーザが実行できる、指定時間内のパスワード変更回数を制限します。
ステップ 4	UCS-A /security/password-profile # **set change-count** *pass-change-num*	ローカル認証されたユーザが、[Change Interval] の間に自分のパスワードを変更できる最大回数 を指定します。 この値は、0 ～ 10 から自由に設定できます。
ステップ 5	UCS-A /security/password-profile # **set change-interval** *num-of-hours*	[Change Count] フィールドで指定したパスワード変更回数が有効になる時間の最大数 を指定します。 この値は、1 ～ 745 時間から自由に設定できます。 たとえば、このフィールドが 48 に設定され、[Change Count] フィールドが 2 に設定されている場合、ローカル認証されたユーザは 48 時間以内に 2 回を超えるパスワード変更を実行することはできません。

	コマンドまたはアクション	目的
ステップ 6	UCS-A /security/password-profile # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、change during interval オプションを有効にし、変更回数を 5 回、変更間隔を 72 時間に設定し、トランザクションをコミットします。

```
UCS-A # scope security
UCS-A /security # scope password-profile
UCS-A /security/password-profile # set change-during-interval enable
UCS-A /security/password-profile* # set change-count 5
UCS-A /security/password-profile* # set change-interval 72
UCS-A /security/password-profile* # commit-buffer
UCS-A /security/password-profile #
```

パスワードの変更禁止間隔の設定

パスワード プロファイル プロパティを変更するには、admin または aaa 権限を持っている必要があります。パスワード履歴を除き、これらのプロパティは、admin または aaa 権限を持つユーザに適用されません。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope password-profile**	パスワード プロファイル セキュリティ モードを開始します。
ステップ 3	UCS-A /security/password-profile # **set change-during-interval disable**	間隔中の変更機能を無効にします。
ステップ 4	UCS-A /security/password-profile # **set no-change-interval** *min-num-hours*	ローカル認証されたユーザが、新しく作成されたパスワードを変更する前に待機する時間の最小数。 を指定します。 この値は、1 ～ 745 時間から自由に設定できます。 この間隔は、[Change During Interval] プロパティが [Disable] に設定されている場合、無視されます。
ステップ 5	UCS-A /security/password-profile # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次に、間隔中の変更オプションを無効にし、変更禁止間隔を72時間に設定し、トランザクションをコミットする例を示します。

```
UCS-A # scope security
UCS-A /security # scope password-profile
UCS-A /security/password-profile # set change-during-interval disable
UCS-A /security/password-profile* # set no-change-interval 72
UCS-A /security/password-profile* # commit-buffer
UCS-A /security/password-profile #
```

パスワード履歴カウントの設定

パスワードプロファイルプロパティを変更するには、adminまたはaaa権限を持っている必要があります。

手順

	コマンドまたはアクション	目的
ステップ1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ2	UCS-A /security # **scope password-profile**	パスワード プロファイル セキュリティ モードを開始します。
ステップ3	UCS-A /security/password-profile # **set history-count** *num-of-passwords*	ローカル認証されたユーザが、以前に使用されたパスワードを再利用できるまでに、作成する必要がある一意のパスワードの数を指定します。 この値は、0 ～ 15 から自由に設定できます。 デフォルトでは、[History Count] フィールドは0に設定されます。これにより、履歴カウントが無効になるため、ユーザはいつでも以前に使用していたパスワードを再利用できます。
ステップ4	UCS-A /security/password-profile # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、パスワード履歴カウントを設定し、トランザクションをコミットします。

```
UCS-A # scope security
UCS-A /security # scope password-profile
UCS-A /security/password-profile # set history-count 5
UCS-A /security/password-profile* # commit-buffer
UCS-A /security/password-profile #
```

ローカル認証されたユーザのパスワード プロファイル

パスワード プロファイルには、Cisco UCS Manager のローカル認証されたすべてのユーザのパスワード履歴やパスワード変更間隔プロパティが含まれます。ローカル認証されたユーザに異なるパスワード プロファイルを指定することはできません。

（注） パスワード プロファイル プロパティを変更するには、admin または aaa 権限を持っている必要があります。パスワード履歴を除き、これらのプロパティは、admin または aaa 権限を持つユーザに適用されません。

パスワード履歴カウント

パスワード履歴のカウントにより、ローカル認証されたユーザが同じパスワードを再使用しないようにすることができます。パスワード履歴カウントを設定すると、Cisco UCS Manager は過去に使用されたパスワードを最大 15 個まで保存します。パスワード履歴カウントには最新のパスワードを先頭に、パスワードが新しい順に保存されます。そのため、履歴カウントがしきい値に達したときには、最も古いパスワードを再使用できます。

パスワード履歴カウントで設定された数のパスワードを作成して使用すると、ユーザはパスワードを再使用できます。たとえば、パスワード履歴カウントを 8 に設定した場合、ユーザは 9 番目のパスワードが期限切れになるまで最初のパスワードを再使用できません。

デフォルトでは、パスワード履歴は 0 に設定されます。この値は、履歴のカウントを無効にし、ユーザはいつでも前のパスワードを使用できます。

ローカル認証されたユーザのパスワード履歴カウントをクリアして、以前のパスワードを再使用可能にすることができます。

パスワード変更間隔

パスワード変更間隔は、ローカル認証されたユーザが特定の時間内に行えるパスワード変更の回数を制限します。次の表で、パスワード変更間隔の 2 つの間隔設定オプションについて説明します。

間隔の設定	説明	例
[No password change allowed]	パスワードの変更後、指定された時間の間は、ローカル認証されたユーザのパスワードを変更することはできません。 1 ～ 745 時間の変更禁止間隔を指定できます。デフォルトでは、変更禁止間隔は 24 時間です。	パスワード変更後 48 時間以内にユーザがパスワードを変更するのを防ぐため： • [Change During Interval] を無効に設定 • [No Change Interval] を 48 に設定
[Password changes allowed within change interval]	ローカル認証されたユーザのパスワードを事前に定義された時間内に変更できる最大回数を指定します。 変更間隔を 1 ～ 745 時間で、パスワード変更の最大回数を 0 ～ 10 で指定できます。デフォルトでは、ローカル認証されたユーザに対して、48 時間間隔内で最大 2 回のパスワード変更が許可されます。	パスワード変更後 24 時間以内に最大 1 回のパスワード変更を許可するには、次のような設定を行います。 • [Change during interval] を有効に設定 • [Change count] を 1 に設定 • [Change interval] を 24 に設定

ローカル認証されたユーザのパスワード履歴のクリア

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope security**	セキュリティ モードを開始します。
ステップ 2	UCS-A /security # **scope local-user** *user-name*	指定されたユーザ アカウントに対するローカル ユーザ セキュリティ モードを開始します。
ステップ 3	UCS-A /security/local-user # **set clear password-history yes**	指定されたユーザアカウントのパスワード履歴をクリアします。
ステップ 4	UCS-A /security/local-user # **commit-buffer**	トランザクションをシステムの設定にコミットします。

例

次の例は、パスワード履歴カウントを設定し、トランザクションをコミットします。

```
UCS-A # scope security
UCS-A /security # scope local-user admin
UCS-A /security/local-user # set clear password-history yes
UCS-A /security/local-user* # commit-buffer
UCS-A /security/local-user #
```