



SED セキュリティ ポリシー

- [自己暗号化ドライブのセキュリティ ポリシー, 1 ページ](#)
- [コントローラとディスクのセキュリティ フラグ, 2 ページ](#)
- [ローカルセキュリティ ポリシーの管理, 3 ページ](#)
- [KMIP クライアント証明書ポリシー, 5 ページ](#)
- [リモートセキュリティ ポリシーの管理, 7 ページ](#)
- [ディスクのセキュリティのイネーブル化とディセーブル化, 10 ページ](#)
- [コントローラのセキュリティのディセーブル化, 10 ページ](#)
- [ロックされたディスクのロックの解除, 11 ページ](#)
- [セキュア外部設定ディスクの消去, 11 ページ](#)

自己暗号化ドライブのセキュリティ ポリシー

自己暗号化ドライブ (SED) には、リアルタイムで着信データを暗号化し、送信データを復号化する特殊なハードウェアが搭載されています。ディスク上のデータは常にディスクで暗号化され、暗号化された形式で格納されます。暗号化されたデータはディスクから読み出す際に常に復号化されます。メディア暗号化キーがこの暗号化と復号化を制御します。このキーは、プロセッサやメモリに格納されることはありません。Cisco UCS Manager は、Cisco UCS C シリーズと S シリーズのサーバの SED セキュリティ ポリシーをサポートしています。

SED は、セキュリティ キーを指定してロックする必要があります。このセキュリティ キーはキー暗号化キーまたは認証パスフレーズとも呼ばれ、メディア暗号化キーの暗号化に使用されます。ディスクがロックされていない場合は、データの取得にキーは必要ありません。

Cisco UCS Manager では、セキュリティ キーをローカルでも、リモートからでも設定できます。ローカルでキーを設定した場合、そのキーを覚えておく必要があります。キーを忘れた場合はそれを取得することはできず、データが失われます。キー管理サーバ (KMIP サーバとも呼ばれる) を使用して、キーをリモートから設定できます。この方法で、ローカル管理でのキーの保管と取得に関する問題に対処します。

SED の暗号化と復号化は、ハードウェアを通じて実行されます。したがって、全体的なシステムパフォーマンスに影響しません。SED は瞬時に暗号を消去することで、ディスクの使用停止や再展開のコストを削減します。メディア暗号化キーを変更することで、暗号消去が実行されます。ディスクのメディア暗号化キーを変更すると、そのディスク上のデータは復号化できず、すぐに使用できない状態になります。Cisco UCS Manager リリース 3.1(3) では、SED は C シリーズサーバと S シリーズサーバにディスク盗難防止機能を提供します。HX サーバについては、SED はノード盗難防止機能を提供します。

コントローラとディスクのセキュリティ フラグ

セキュリティ フラグは、ストレージ コントローラとディスクの現在のセキュリティ ステータスを示します。

ストレージ コントローラとディスクには、次のセキュリティ フラグがあります。

- **Security Capable** : コントローラまたはディスクが SED 管理をサポートできることを示します。
- **Security Enable** : コントローラまたはディスクにセキュリティ キーがプログラムされており、セキュリティがデバイス上で有効であることを示します。このフラグは、セキュリティ ポリシーを設定してサーバに関連付け、コントローラとディスクを保護しているときに設定されます。HX デバイスでは、このフラグは設定されません。
- **Secured** : コントローラまたはディスクにセキュリティ キーがプログラムされており、セキュリティが HX デバイス上で有効であることを示します。

次のセキュリティ フラグは、ストレージ ディスクにのみ適用されます。

- **Locked** : ディスク キーがコントローラ上のキーと一致していないことを示します。これは、異なるキーでプログラムされたサーバ間でディスクを移動すると発生します。ロックされたディスク上のデータにはアクセスできないため、オペレーティングシステムがディスクを使用できません。このディスクを使用するには、ディスクのロックを解除するか、または外部設定を安全に消去します。
- **Foreign Secured** : セキュア ディスクは外部設定になっていることを示します。正しいキーでロックされたディスクのロックを解除しても、ディスクが外部設定状態になっており、そのディスク上のデータが暗号化されているとこのようになります。このディスクを使用するには、外部設定をインポートするか、または外部設定をクリアします。

ローカル セキュリティ ポリシーの管理

ローカル セキュリティ ポリシーの作成

はじめる前に

新しいストレージ プロファイルまたは既存のストレージ プロファイルにローカル ポリシーを作成できます。

手順

-
- ステップ 1 [Navigation] ペインで、[Storage] > [Storage Profiles] の順に展開します。
 - ステップ 2 ポリシーを作成するストレージ プロファイルを選択します。
 - ステップ 3 [Security Policy] タブをクリックし、[Create Security Policy] をクリックします。
 - ステップ 4 [Local Policy] オプションをクリックします。
 - a) [Key] に入力します。
キーには 32 個の英数字を使用する必要があります。
 - b) [OK] をクリックします。
ポリシーが正常に作成されたというメッセージが表示されます。
-

次の作業

こうして作成されたキーは、そのサーバのストレージプロファイルに関連付けられ、ストレージコントローラの下に展開されます。これを確認するには、[Equipment] > [Server] > [Server ID] > [Inventory] > [Storage] > [Controller] の順に移動して SAS ストレージ コントローラを選択します。[General] タブに移動し、[Security] フィールドが [drive security enable] として表示されているかどうかを確認します。

ローカル セキュリティ ポリシーの変更

手順

-
- ステップ 1 [Navigation] ペインで、[Storage] > [Storage Profiles] の順に展開します。
 - ステップ 2 ポリシーを作成したストレージ プロファイルを選択します。
 - ステップ 3 [Security Policy] タブをクリックします。
 - ステップ 4 (任意) ローカルポリシーのキーを変更するには、[Local Policy] 領域で次の手順を実行します。
 - a) [Key] フィールドにデータベースの新しいセキュリティ キーを入力します。

b) [Deployed Key] フィールドにデータベースの現在のセキュリティ キーを入力します。

ステップ 5 (任意) セキュリティ ポリシーを ローカル ポリシーからリモート ポリシーに変更するには、次の手順を実行します。

a) [Remote Policy] オプションをクリックします。

b) [IP Address/Hostname] フィールドにプライマリ サーバの詳細情報を入力します。

c) (任意) [IP Address/Hostname] フィールドにセカンダリ サーバの詳細情報を入力します。

d) (任意) [Deployed Key] フィールドにデータベースの現在のセキュリティ キーを入力します。

e) (任意) [Port] フィールドに、サーバのポート番号を入力します。

f) [KMIP Server Public Certificate] フィールドに KMIP 証明書の内容を入力します。

g) (任意) [Add Login Details] をクリックしてユーザ クレデンシャルを入力します。

ステップ 6 [Save Changes] をクリックします。

ローカル セキュリティ ポリシーを使用しているサーバへのセキュアなディスクの挿入

サーバにセキュアなディスクを挿入すると、次のいずれかが行われます。

- ドライブ上のセキュリティキーが、サーバのセキュリティキーと一致し、自動的にロックが解除されます。
- ディスク上のセキュリティキーとサーバ上のセキュリティキーが異なります。ディスクはロックされたディスクとして表示されます。ロックされたディスク上で次のいずれかを実行できます。
 - セキュアな外部設定を消去してディスク上のすべてのデータを削除します。
 - ディスクの正しいキーを提供してディスクのロックを解除します。ディスクのロックを解除すると、ディスクは **Foreign Secured** の状態になります。これらのディスクの外部設定は、すぐにインポートするか、またはクリアする必要があります。



(注) 現在の一連のディスクの外部設定をインポートする前に別の一連のディスクのロックを解除すると、現在の一連のディスクは再度ロックされ、**Locked** の状態になります。

KMIP クライアント証明書ポリシー

KMIP サーバとも呼ばれているキー管理サーバを使用して、キーをリモートから設定できます。リモート ポリシーを作成する前に、KMIP クライアント証明書ポリシーを作成する必要があります。証明書の生成に使用するホスト名は KMIP サーバのシリアル番号です。

証明書ポリシーは、2つの独立した範囲から作成できます。

- グローバルスコープ：最初にこの範囲でグローバル証明書ポリシーを作成できます。この範囲で証明書を変更しても、証明書は再生成されません。
- サーバスコープ：この範囲で証明書ポリシーを作成または変更できます。作成または変更すると、証明書が再生成されます。このような証明書はそのサーバに固有であり、そのサーバについてグローバル証明書がオーバーライドされます。

KMIP クライアント証明書ポリシーを作成したら、次のいずれかを実行します。

- KMIP サーバに生成された証明書をコピーします。
- 生成された証明書署名要求を使用して CA 署名付き証明書を取得します。この CA 署名付き証明書を CIMC にコピーします。

グローバル KMIP クライアント証明書ポリシーの作成

グローバル KMIP クライアント証明書ポリシーを作成することができます。

このポリシーを使用しているときに証明書の作成に使用するホスト名はサーバのシリアル番号です。

手順

- ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
- ステップ 2 [Work] ペインの [Policies] タブをクリックします。
- ステップ 3 [Security] サブタブをクリックします。
- ステップ 4 [Create KMIP Client Cert Policy] をクリックします。
- ステップ 5 表示された [Create KMIP Client Cert Policy] ダイアログボックスで、次の情報を入力します。

名前	説明
Country Code	会社所在国の国コード。 アルファベット 2 文字を大文字で入力します。
状態	証明書を要求している会社の本社が存在する州または行政区分。 32 文字まで入力します。

名前	説明
地名	証明書を要求している会社の本社が存在する市または町。 32 文字まで入力します。
組織名	証明書を要求している組織。 32 文字まで入力します。
部署名	組織ユニット 最大 64 文字まで入力できます。
Email	要求に関連付けられている電子メールアドレス。
Validity	証明書の有効期間。

ステップ 6 [OK] をクリックします。

サーバ用の KMIP クライアント証明書ポリシーの作成

サーバ用の KMIP クライアント証明書ポリシーを作成できます。この証明書は、特定のサーバにのみ適用され、グローバル KMIP クライアント証明書をオーバーライドします。

このポリシーを使用しているときに証明書の作成に使用するホスト名はサーバのシリアル番号です。

手順

- ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
- ステップ 2 [Equipment] > [Rack Mounts] > [Servers] > [Server Number] の順に展開します。
- ステップ 3 [Work] ペインで、[Inventory] タブをクリックし、[Storage] サブタブをクリックします。
- ステップ 4 [Security] サブタブをクリックします。
- ステップ 5 [Create KMIP Client Cert Policy] をクリックします。
- ステップ 6 表示された [Create KMIP Client Cert Policy] ダイアログボックスで、次の情報を入力します。

名前	説明
Country Code	会社所在国の国コード。 アルファベット 2 文字を大文字で入力します。
状態	証明書を要求している会社の本社が存在する州 または行政区分。 32 文字まで入力します。
地名	証明書を要求している会社の本社が存在する市 または町。 32 文字まで入力します。
組織名	証明書を要求している組織。 32 文字まで入力します。
部署名	組織ユニット 最大 64 文字まで入力できます。
Email	要求に関連付けられている電子メール アドレ ス。
Validity	証明書の有効期間。

ステップ 7 [OK] をクリックします。

リモートセキュリティポリシーの管理

リモートセキュリティポリシーの作成

新規ストレージプロファイルまたは既存のストレージプロファイルにリモートポリシーを作成できます。

はじめる前に

KMIP クライアント証明書ポリシーを作成したことを確認します。

手順

-
- ステップ 1** [Navigation] ペインで、[Storage] > [Storage Profiles] の順に展開します。
- ステップ 2** ポリシーを作成するストレージプロファイルを選択します。
- ステップ 3** [Security Policy] タブをクリックし、[Create Security Policy] をクリックします。
- ステップ 4** [Remote Policy] オプションをクリックします。
- [IP Address/Hostname] フィールドにプライマリ サーバの詳細情報を入力します。
 - (任意) [IP Address/Hostname] フィールドにセカンダリ サーバの詳細情報を入力します。
 - (任意) [Port] フィールドに、サーバのポート番号を入力します。
 - [KMIP Server Public Certificate] フィールドに KMIP 証明書の内容を入力します。
 - (任意) [Add Login Details] をクリックしてユーザ クレデンシャルを入力します。
 - [OK] をクリックします。
ポリシーが正常に作成されたというメッセージが表示されます。
-

次の作業

こうして作成されたキーは、そのサーバのストレージプロファイルに関連付けられ、ストレージコントローラの下に展開されます。これを確認するには、[Equipment] > [Server] > [Server ID] > [Inventory] > [Storage] > [Controller] の順に移動して SAS ストレージコントローラを選択します。[General] タブに移動し、[Security] フィールドが [drive security enable] として表示されているかどうかを確認します。

リモート セキュリティ ポリシーの変更

手順

-
- ステップ 1** [Navigation] ペインで、[Storage] > [Storage Profiles] の順に展開します。
- ステップ 2** ポリシーを作成したストレージプロファイルを選択します。
- ステップ 3** [Security Policy] タブをクリックします。
- ステップ 4** リモート ポリシーを変更するには、[Remote Policy] 領域で次の手順を実行します。
- [IP Address/Hostname] フィールドにプライマリ サーバの詳細情報を入力します。
 - (任意) [IP Address/Hostname] フィールドにセカンダリ サーバの詳細情報を入力します。
 - (任意) [Port] フィールドに、サーバのポート番号を入力します。
 - [KMIP Server Public Certificate] フィールドに KMIP 証明書の内容を入力します。
この証明書をブラウザから Base 64 形式で保存します。

- e) (任意) [Add Login Details] をクリックしてユーザ クレデンシャルを入力します。
- ステップ 5** セキュリティ ポリシーを リモート ポリシーからローカル ポリシーに変更するには、次の手順を実行します。
- a) [Local Policy] オプションをクリックします。
 - b) [Key] フィールドにコントローラの新しいセキュリティ キーを入力します。
- ステップ 6** [Save Changes] をクリックします。
-

リモート セキュリティ キーの変更

手順

- ステップ 1** [Navigation] ペインで [Equipment] をクリックします。
- ステップ 2** [Equipment] > [Rack-Mounts] > [Servers] > [Server Number] の順に展開します。
- ステップ 3** [Work] 領域の [Inventory] タブをクリックします。
- ステップ 4** [Storage] サブタブをクリックします。
- ステップ 5** [Controllers] タブで、SAS コントローラを選択します。
- ステップ 6** [General] タブで、[Modify Remote Key] をクリックします。
-

リモート セキュリティ ポリシーを使用しているサーバへのセキュアなディスクの挿入

リモートセキュリティポリシーを使用しているサーバにセキュアなディスクを挿入すると、ストレージディスクはロックされたディスクとして表示されます。次のいずれかを実行します。

- 以前にローカル キーを使用してディスクがロックされていた場合は、そのローカル キーを使用してディスクのロックを手動で解除します。
- リモート KMIP サーバを使用してロックを解除します。

セキュアなディスクをローカルセキュリティポリシーを使用しているサーバからリモートセキュリティポリシーを使用しているサーバに移動すると、ディスクはロックされた状態として表示されます。ローカル キーを使用してディスクのロックを手動で解除します。

ディスクのセキュリティのイネーブル化とディセーブル化

はじめる前に

- ディスクのセキュリティを有効にするには、ディスクが JBOD であることを確認します。
- ディスクをセキュアに消去するには、そのディスクが未設定で良好な状態になっている必要があります。

手順

-
- ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
 - ステップ 2 [Equipment] > [Rack-Mounts] > [Servers] > [Server Number] の順に展開します。
 - ステップ 3 [Work] 領域の [Inventory] タブをクリックします。
 - ステップ 4 [Storage] サブタブをクリックします。
 - ステップ 5 [Disks] タブで、ディスクを選択します。
 - ステップ 6 [Details] 領域で、[Enable Encryption] をクリックします。
 - ステップ 7 セキュア ディスクを無効にするには、[Secure Erase] をクリックします。
-

コントローラのセキュリティのディセーブル化

はじめる前に

SAS コントローラ上でのみ、セキュリティを無効にすることができます。コントローラ上のセキュリティを無効にするには、まずすべてのセキュア ディスク上のセキュリティを無効にしてから、コントローラのすべてのセキュア仮想ドライブを削除します。

手順

-
- ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
 - ステップ 2 [Equipment] > [Rack-Mounts] > [Servers] > [Server Number] の順に展開します。
 - ステップ 3 [Work] 領域の [Inventory] タブをクリックします。
 - ステップ 4 [Storage] サブタブをクリックします。
 - ステップ 5 [Controllers] タブで、SAS コントローラを選択します。
 - ステップ 6 [General] タブで、[Disable Security] をクリックします。
-

ロックされたディスクのロックの解除

SEDのキーがコントローラ上のキーと一致していない場合、そのディスクは[Locked, Foreign Secure]と表示されます。そのディスクのセキュリティキーを提供するか、またはリモート KMIP サーバを使用して、ディスクのロックを解除します。ディスクのロックを解除した後、外部設定をインポートするか、またはクリアします。

手順

-
- ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
 - ステップ 2 [Equipment] > [Rack-Mounts] > [Servers] > [Server Number] の順に展開します。
 - ステップ 3 [Work] 領域の [Inventory] タブをクリックします。
 - ステップ 4 [Storage] サブタブをクリックします。
 - ステップ 5 [Controller] タブで、SAS コントローラを選択します。
 - ステップ 6 ローカルセキュリティポリシーで保護されているディスクのロックを解除するには、次の手順を実行します。
 - a) [General] タブで、[Unlock Disk] をクリックします。
 - b) [Key] テキスト ボックスに、そのディスクをロックするのに使用したキーを入力します。
 - c) [OK] をクリックします。
 - ステップ 7 リモート KMIP サーバで保護されているディスクのロックを解除するには、[General] タブで [Unlock For Remote] をクリックします。
-

ロックされたディスクのロックを解除すると、そのディスクのセキュリティステータスは[Foreign Secure]と表示されます。

次の作業

外部設定をインポートするか、またはクリアします。

セキュア外部設定ディスクの消去

ロックされた状態のディスクがあり、そのディスクを既存のデータにアクセスせずに使用する場合は、セキュアな外部設定ディスクを消去できます。

手順

- ステップ 1 [Navigation] ペインで [Equipment] をクリックします。
 - ステップ 2 [Equipment] > [Rack-Mounts] > [Servers] > [Server Number] の順に展開します。
 - ステップ 3 [Work] 領域の [Inventory] タブをクリックします。
 - ステップ 4 [Storage] サブタブをクリックします。
 - ステップ 5 [Disks] タブで、ディスクを選択します。
 - ステップ 6 [General] タブで、[Secure Erase Foreign Configuration] をクリックします。
-