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

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は保存されません。Cisco UCS Manager は、Cisco UCS C シリーズと B-シリーズ M5 サーバ、および 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しなければなりません。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、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) を使用すると、リモートでキーを設定できます。この方法により、ローカル管理でのキーの保管と取得に伴なう問題に対処することができます。

SEDの暗号化と復号化はハードウェアを介して行われます。したがって、システムの全体的なパフォーマンスには影響がありません。SEDは、瞬間的な暗号化消去によってディスクの廃止コストや再配置コストを削減します。暗号化消去は、メディア暗号キーを変更することによって実行されます。ディスクのメディア暗号キーが変更されると、そのディスク上のデータは復号不能になるので、ただちにデータが使用不可になります。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。Cisco UCS Managerリリース 4.0(2) では、UCS B シリーズ M5 サーバに SED セキュリティ ポリシーを拡張します。

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。

データを安全に削除する

委員会規制 (EU) 2019/424 は、データを安全に処分することを要求しています。

データの安全な廃棄は、Cisco UCS サーバのさまざまなドライブ、メモリ、およびストレージからデータを消去し、工場出荷時の設定にリセットするための、一般的なツールを使用することによって可能になります。

委員会規制 (EU) 2019/424 に準拠するためのデータの安全な削除は、次の Cisco UCS サーバでサポートされています。

- Cisco UCS B200
- Cisco UCS B480
- Cisco UCS C125
- Cisco UCS C220
- Cisco UCS C240
- Cisco UCS C480
- Cisco UCS S3260

安全にデータを削除するため、UCS サーバに取り付けられているデバイスについて十分に理解し、適切なツールを実行する必要があります。場合によっては、複数のツールを実行する必要がある場合があります。

データを安全に消去する方法の詳細については、https://www.cisco.com/web/dofc/18794277.pdf を参照してください。

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

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope org**	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **create storage-profile** *storage-profile-name*	指定された名前を持つストレージ プロファイルを組織レベルで作成し、ストレージ プロファイル設定モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	UCS-A /org/storage-profile* # **create security**	指定されたストレージ プロファイルのセキュリティポリシーを作成し、セキュリティ ポリシー モードを開始します。
ステップ 4	UCS-A /org/storage-profile/security* # **create drive-security**	指定されたストレージ プロファイルのセキュリティのドライブ セキュリティ ポリシーを作成し、ドライブ セキュリティ ポリシー モードを開始します。
ステップ 5	UCS A/org/storage-profile/security/drive-セキュリティ * # **create local**	指定されたストレージ プロファイルのローカル セキュリティ ポリシーを作成し、ローカル ポリシー モードを開始します。
ステップ 6	UCS-A /org/storage-profile/security/drive-security/local* # **set security-key** *security-key*	ローカル ポリシーの指定されたセキュリティ キーを設定します。セキュリティ キーには、32 文字がなければなりません。
ステップ 7	UCS-A /org/storage-profile/security/drive-security/local* # **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

この例では、セキュリティ キーをもつローカル セキュリティ ポリシーの作成方法を示します。

```
UCS-A# scope org
UCS-A /org # create storage-profile stp-demo
UCS-A /org/storage-profile* # create security
UCS-A /org/storage-profile/security* # create drive-security
UCS-A /org/storage-profile/security/drive-security* # create local
UCS-A /org/storage-profile/security/drive-security/local* # set security-key
thereare32charactersinthisseckey
UCS-A /org/storage-profile/security/drive-security/local* # commit-buffer
UCS-A /org/storage-profile/security/drive-security/local #
```

ローカル セキュリティ ポリシーのセキュリティ キーの変更

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope org**	ルート組織モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	UCS-A /org # **scope storage-profile** *storage-profile-name*	指定されたストレージ プロファイルのストレージ プロファイル設定モードを開始します。
ステップ 3	UCS-A /org/storage-profile # **scope security**	指定されたストレージ プロファイルのセキュリティ ポリシー モードを開始します。
ステップ 4	UCS A/org/storage-profile/security # **scope drive-security**	指定されたストレージ プロファイル セキュリティのドライブ セキュリティ ポリシー モードを開始します。
ステップ 5	UCS A/org/storage-profile/security/drive-security # **scope local**	指定されたストレージ プロファイルのローカル ポリシー モードを開始します。
ステップ 6	UCS A/org/storage-profile/security/drive-security/local # **set deployed-security-key** *existing-security-key*	新しいキーを設定するために、サーバで展開される既存のキーを指定します。
ステップ 7	UCS-A /org/storage-profile/security/drive-security/local* # **set security-key** *new-security-key*	ローカルポリシーの新しいセキュリティ キーを設定します。
ステップ 8	UCS-A /org/storage-profile/security/drive-security/local* # **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

この例では、ローカル セキュリティ ポリシーのセキュリティ キーを変更する方法を示します。

```
UCS-A# scope org
UCS-A /org # scope storage-profile stp-demo
UCS-A /org/storage-profile # scope security
UCS-A /org/storage-profile/security # scope drive-security
UCS-A /org/storage-profile/security/drive-security # scope local
UCS-A /org/storage-profile/security/drive-security/local # set deployed-security-key
thereare32charactersinthisseckey
UCS-A /org/storage-profile/security/drive-security/local* # set security-key
thereare32charactersinthisnewkey
UCS-A /org/storage-profile/security/drive-security/local* # commit-buffer
UCS-A /org/storage-profile/security/drive-security/local #
```

ローカルからリモートへのセキュリティ ポリシーの変更

始める前に

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope org**	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **scope storage-profile** *storage-profile-name*	選択したストレージプロファイルのストレージ プロファイル 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	UCS-A /org/storage-profile # **scope security**	指定されたストレージプロファイルのセキュリティポリシーモードを開始します。
ステップ 4	UCS A/org/storage-profile/security # **scope drive-security**	指定されたストレージプロファイルセキュリティのドライブセキュリティポリシー モードを開始します。
ステップ 5	UCS A/org/storage-profile/security/drive-security # **create remote**	リモートポリシーモードを作成し、開始します。
ステップ 6	UCS-A /org/storage-profile/security/drive-security/remote* # **set deployed-security-key** *existing-security-key*	サーバで展開された既存のキーを指定します。
ステップ 7	UCS-A /org/storage-profile/security/drive-security/remote* # **set primary-server** *primary-server-name*	プライマリ サーバ ホスト名または IP サーバを設定します。
ステップ 8	（任意） UCS-A /org/storage-profile/security/drive-security/remote* # **set secondary-server** *secondary-server-name*	セカンダリ サーバ ホスト名または IP サーバを設定します。
ステップ 9	（任意） UCS-A /org/storage-profile/security/drive-security/remote* # **set port** *kmip-server-port-number*	KMIP サーバのポート番号を設定します。KMIP サーバ ポート番号は、1024 から 65535 の範囲を設定できます。
ステップ 10	UCS-A /org/storage-profile/security/drive-security/remote* # **set server-certificate**	リモート セキュリティ ポリシーに KMIP 証明書を設定します。

	コマンドまたはアクション	目的
ステップ 11	（任意） UCS-A /org/storage-profile/security/drive-security/remote* # **set timeout** *timeout-seconds*	ストレージと KMIP サーバの間の通信がタイム アウトする秒数を設定します。タイムアウトは 5 秒 ～ 20 秒の範囲となる場合があります。
ステップ 12	UCS-A /org/storage-profile/security/drive-security/remote* # **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。
ステップ 13	UCS A/org/storage-profile/security/drive-security/remote #**exit**	ドライブ セキュリティ ポリシー モードを開始します。
ステップ 14	UCS-A /org/storage-profile/security/drive-security # **delete local**	既存のローカルセキュリティ ポリシーを削除します。
ステップ 15	UCS-A /org/storage-profile/security/drive-security* # **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

この例では、ローカルからリモートへのセキュリティ ポリシーを変更する方法を示します。

```
UCS-A # scope org
UCS-A /org # scope storage-profile stp-demo
UCS-A /org/storage-profile # scope security
UCS-A /org/storage-profile/security # scope drive-security
UCS-A /org/storage-profile/security/drive-security # create remote
UCS-A /org/storage-profile/security/drive-security/remote* # set deployed-security-key
thereare32charactersinthisseckey
UCS-A /org/storage-profile/security/drive-security/remote* # set primary-server 10.10.10.1
UCS-A /org/storage-profile/security/drive-security/remote* # set secondary-server
10.10.10.2
UCS-A /org/storage-profile/security/drive-security/remote* # set port 5696
UCS-A /org/storage-profile/security/drive-security/remote* # set server-certificate
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Prompt Certificate:
>-----BEGIN CERTIFICATE-----
    MIIEEDCCAvigAwIBAgIGALOfZVDsMA0GCSqGSIb3DQEBCwUAMIGQMSowKAYDVQQD
    EyFDRyBDQSBTIG9uIHZvcm1ldHJpY2RzbS5jaXNjby5jb20xFTATBgNVBAsTDFNh
    dmJ1U3RvcmRldjEWMBQGA1UEChMNQ2lzY28gU3lzdGVtczERMA8GA1UEBxMIU2Fu
    IEpvc2UxEzARBgNVBAgTCkNhbGlmb3JuaWExCzAJBgNVBAYTAlVTMB4XDTE2MDkw
    NzE5MzMwMVoXDTI2MDkwOTE5MzMwMVowgZAxKjAoBgNVBAMTIUNHIENBIFMgb24g
    dm9ybWV0cmljZHNtLmNpc2NvLmNvbTEVMBMGA1UECxMMU2F2YnVTdG9yZGV2MRYw
    FAYDVQQKEw1DaXNjbyBTeXN0ZW1zMREwDwYDVQQHEwhTYW4gSm9zZTETMB>EGA1UE
    CBMKQ2FsaWZvcm5pYTELMAkGA1UEBhMCVVMwggEiMA0GCSqGSIb3DQEBAQUAA4IB
    DwAwggEKAoIBAQDhX2UdIV>TQTchGo1FjAc5u1W9zAo/YkjD22ANpbEPiAmgWL97c
    Xwj7yzArflrZ2kWvQCm4f6AdLOFUWzbuo+Fxd3rurd>w6BhJXdLj8Piq8094PqCLp
    qdUF83SsRVVbCXHxOqdk9jsSQrvTcV4PloNrelMLq/mOqsaODs+us4ng7sMDtGXv
    LeKFC8DUEm0GlGQACwiJ3s9O4+P2CI/d4P/>EyWwqABf3YJmAI1EQyUnoTwrg6EgY
    ZvcpHsmjXnbBZrL+ON7FBcbrTanvjyJxE6tFf5cRPGhymfna7Fd3lfVwZCcGIoR+
```

```
    EOIAwgetzIRM6FzMiV2/tDT8STo/oo5Tg3dDAgMBAAGjbj>BsMBIGA1UdEwEB/wQI
    MAYBAf8CAQAwDgYDVR0PAQH/>>>>>>>>>BAQDAgEGMB0GA1UdDgQWBBRnYyFiAK2lEDZJNC0Y
    VlIqMgiUJDAnBgNVHSMEIDAegBRnYyFiAK2lEDZJNC0YVlIqMgiUJIIGALOfZVDs
    MA0GCSqGSIb3DQEBCwUAA4IBAQAfhB2+Ft8V2ELAFa7PcG/rU09ux7LYcCjt3STa
    mzKdZ7Rn5COvknKrJX+EefT7xl03CQXT9aeSAddQUOCy8fhiPoaMFrlTgs1hdS0p
    NJvfxV6QCun2UMRSuxWfG>0QFfofnXeIGkAmEYOpUdArSOTbtt4v6Lja1A+KEsvWW
    5KaVemo2nsd+iD0IPCOhpShAgaAwpnYUq9mLfVgvV07Z+hmkuOIQTZ2+h+pJQtE0
    +U5qaTts4pMXpqQPjlid0NMuaPug1SpSD7KBsjwR1SzehzPdns16uprmvWa3VBk3
    OK6y55FoIu+Wg9i/8kmfkghyGwTfo6weEKbleuVwupvpriMF>
    -----END CERTIFICATE-----

UCS-A /org/storage-profile/security/drive-security/remote* # commit-buffer
UCS-A /org/storage-profile/security/drive-security/remote # exit
UCS-A /org/storage-profile/security/drive-security # delete local
UCS-A /org/storage-profile/security/drive-security* # commit-buffer
UCS-A /org/storage-profile/security/drive-security #
```

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っています。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

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 # **create kmip-client-cert-policy**	KMIP証明書ポリシーを作成し、KMIP クライアント証明書ポリシーモードを開始します。
ステップ 3	UCS-A /security/kmip-client-cert-policy* # **set country** *country-code*	KMIP 証明書ポリシーの国コードを指定します。国コードは大文字で 2 文字を含まなければなりません。
ステップ 4	UCS-A /security/kmip-client-cert-policy* # **set locality** *locality-code*	ローカリティの名前またはKMIP 証明書ポリシーの都市を指定します。ローカリティの名前として最大32 文字までを入力します。
ステップ 5	UCS-A /security/kmip-client-cert-policy* # **set org-name** *org-name*	KMIP 証明書ポリシーを要求する組織名を指定します。組織名として最大32 文字を入力します。
ステップ 6	UCS-A /security/kmip-client-cert-policy* # **set org-unit-name** *unit-name*	KMIP 証明書ポリシーを要求する組織ユニット名を指定します。組織ユニット名として最大64 文字を入力します。
ステップ 7	UCS-A /security/kmip-client-cert-policy* # **set state** *state-code*	KMIP 証明書ポリシーの州、地域、または郡の名前を指定します。州の名前として最大で 32 文字を入力します。

	コマンドまたはアクション	目的
ステップ 8	（任意） UCS-A /security/kmip-client-cert-policy* # **set email** *email-address*	リクエストに関連付けられた電子メール アドレスを指定します。
ステップ 9	（任意） UCS-A /security/kmip-client-cert-policy* # **set validity** *days*	証明書の有効期間を日数で指定します。有効期間は 365 日から 3650 日間です。
ステップ 10	UCS-A /security/kmip-client-cert-policy* # **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。
ステップ 11	UCS A/security/kmip-client-cert-policy # **show**	KMIP 証明書ポリシーの詳細を表示します。

例

この例では、KMIP 証明書のポリシーを作成する方法を示します。

```
UCS-A# scope security
UCS-A /security # create kmip-client-cert-policy
UCS-A /security/kmip-client-cert-policy* # set country IN
UCS-A /security/kmip-client-cert-policy* # set locality BLR
UCS-A /security/kmip-client-cert-policy* # set org-name XYZ
UCS-A /security/kmip-client-cert-policy* # set org-unit-name Ops
UCS-A /security/kmip-client-cert-policy* # set state KA
UCS-A /security/kmip-client-cert-policy* # commit-buffer
UCS-A /security/kmip-client-cert-policy # show

KMIP Client certificate policy:
Certificate request country name: IN
State, province or county (full name): KA
Locality name (eg, city): BLR
Organisation name (eg, company): XYZ
Organisational Unit Name (eg, section): Ops
Certificate request e-mail name:
Validity of certificate in number of days: 1095
UCS-A /security/kmip-client-cert-policy #
```

サーバ用の KMIP クライアント証明書の作成

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope server** *server-number*	指定したサーバのサーバ設定モードを開始します。
ステップ 2	UCS-A /server # **create kmip-client-cert-policy**	KMIP 証明書ポリシーを作成し、KMIP クライアント証明書ポリシーモードを開始します。
ステップ 3	UCS A/server/kmip-client-cert-ポリシー * # **set country** *country-code*	KMIP 証明書ポリシーの国コードを指定します。国コードは大文字で 2 文字を含まなければなりません。
ステップ 4	UCS A/server/kmip-client-cert-ポリシー * # **set locality** *locality-code*	ローカリティの名前またはKMIP 証明書ポリシーの都市を指定します。ローカリティの名前として最大 32 文字までを入力します。
ステップ 5	UCS-A /server/kmip-client-cert-policy* # **set org-name** *org-name*	KMIP 証明書ポリシーを要求する組織名を指定します。組織名として最大 32 文字を入力します。
ステップ 6	UCS-A /server/kmip-client-cert-policy* # **set org-unit-name** *unit-name*	KMIP 証明書ポリシーを要求する組織ユニット名を指定します。組織ユニット名として最大 64 文字を入力します。
ステップ 7	UCS-A /server/kmip-client-cert-policy* # **set state** *state-code*	KMIP 証明書ポリシーの州、地域、または郡の名前を指定します。州の名前として最大で 32 文字を入力します。
ステップ 8	（任意） UCS A/server/kmip-client-cert-ポリシー * # **set email** *email-address*	リクエストに関連付けられた電子メール アドレスを指定します。
ステップ 9	（任意） UCS-A /server/kmip-client-cert-policy* # **set validity** *days*	証明書の有効期間を日数で指定します。有効期間は 365 日から 3650 日間です。
ステップ 10	UCS-A /server/kmip-client-cert-policy* # **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。
ステップ 11	UCS A/server/kmip-client-cert-policy # **show**	KMIP 証明書の詳細を表示します。

例

この例では、rack-mount サーバで KMIP 証明書を作成する方法を示します。

```
UCS-A# scope server 5
UCS-A /server # create kmip-client-cert-policy
UCS-A /server/kmip-client-cert-policy* # set country IN
UCS-A /server/kmip-client-cert-policy* # set locality BLR
UCS-A /server/kmip-client-cert-policy* # set org-name XYZ
UCS-A /server/kmip-client-cert-policy* # set org-unit-name Ops
UCS-A /server/kmip-client-cert-policy* # set state KA
UCS-A /server/kmip-client-cert-policy* # commit-buffer
UCS-A /server/kmip-client-cert-policy* # show

KMIP Client certificate policy:
Certificate request country name: IN
State, province or county (full name): KA
Locality name (eg, city): BLR
Organisation name (eg, company): XYZ
Organisational Unit Name (eg, section): Ops
Certificate request e-mail name:
Validity of certificate in number of days: 1095
UCS-A /server/kmip-client-cert-policy #
```

この例では、ブレード サーバで KMIP 証明書を作成する方法を示します。

```
UCS-A# scope server 1/5
UCS-A chassis/server # create kmip-client-cert-policy
UCS-A chassis/server/kmip-client-cert-policy* # set country IN
UCS-A chassis/server/kmip-client-cert-policy* # set locality BLR
UCS-A chassis/server/kmip-client-cert-policy* # set org-name XYZ
UCS-A chassis/server/kmip-client-cert-policy* # set org-unit-name Ops
UCS-A chassis/server/kmip-client-cert-policy* # set state KA
UCS-A chassis/server/kmip-client-cert-policy* # commit-buffer
UCS-A chassis/server/kmip-client-cert-policy* # show

KMIP Client certificate policy:
Certificate request country name: IN
State, province or county (full name): KA
Locality name (eg, city): BLR
Organisation name (eg, company): XYZ
Organisational Unit Name (eg, section): Ops
Certificate request e-mail name:
Validity of certificate in number of days: 1095
UCS-A /server/kmip-client-cert-policy #
```

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

始める前に

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope org**	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **scope storage-profile** *storage-profile-name*	選択したストレージプロファイルのストレージ プロファイル 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	UCS-A /org/storage-profile # **create security**	セキュリティ モードを作成し、開始します。
ステップ 4	UCS-A /org/storage-profile/security* # **create drive-security**	ドライブ セキュリティ モードを作成し、開始します。
ステップ 5	UCS A/org/storage-profile/security/drive-セキュリティ * # **create remote**	リモート ポリシー モードを作成し、開始します。
ステップ 6	UCS-A /org/storage-profile/security/drive-security/remote* # **set primary-server** *primary-server-name*	プライマリ サーバ ホスト名または IP サーバを設定します。
ステップ 7	（任意） UCS-A /org/storage-profile/security/drive-security/remote* # **set secondary-server** *secondary-server-name*	セカンダリ サーバ ホスト名または IP サーバを設定します。
ステップ 8	（任意） UCS-A /org/storage-profile/security/drive-security/remote* # **set port** *kmip-server-port-number*	KMIP サーバのポート番号を設定します。KMIP サーバ ポート番号は、1024 から 65535 の範囲を設定できます。
ステップ 9	UCS-A /org/storage-profile/security/drive-security/remote* # **set server-certificate**	リモート セキュリティ ポリシーに KMIP 証明書を設定します。
ステップ 10	（任意） UCS-A /org/storage-profile/security/drive-security/remote* # **set timeout** *timeout-seconds*	ストレージと KMIP サーバの間の通信がタイム アウトする秒数を設定します。タイムアウトは 5 秒 ～ 20 秒の範囲となる場合があります。
ステップ 11	（任意） UCS-A /org/storage-profile/security/drive-security/remote* # **create login**	KMIP サーバのログインの詳細を作成し、ログイン モードを開始します。
ステップ 12	（任意） UCS-A /org/storage-profile/security/drive-security/remote/login* # **set username** *username*	KMIPサーバにログインするためのユーザ名を設定します。
ステップ 13	（任意） UCS-A /org/storage-profile/security/drive-security/remote/login* # **set password** *password*	KMIP サーバにログインするためのパスワードを設定します。

	コマンドまたはアクション	目的
ステップ 14	UCS-A /org/storage-profile/security/drive-security/remote/login* # **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

```
UCS-A # scope org
UCS-A /org # scope storage-profile stp-demo
UCS-A /org/storage-profile # create security
UCS-A /org/storage-profile/security* # create drive-security
UCS-A /org/storage-profile/security/drive-security* # create remote
UCS-A /org/storage-profile/security/drive-security/remote* # set primary-server 10.10.10.1
UCS-A /org/storage-profile/security/drive-security/remote* # set secondary-server
10.10.10.2
UCS-A /org/storage-profile/security/drive-security/remote* # set port 5696
UCS-A /org/storage-profile/security/drive-security/remote* # set server-certificate
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Prompt Certificate:
>-----BEGIN CERTIFICATE-----
    MIIEEDCCAvigAwIBAgIGALOfZVDsMA0GCSqGSIb3DQEBCwUAMIGQMSowKAYDVQQD
    EyFDRyBDQSBTIG9uIHZvcm1ldHJpY2RzbS5jaXNjby5jb20xFTATBgNVBAsTDFNh
    dmJ1U3RvcmRldjEWMBQGA1UEChMNQ2lzY28gU3lzdGVtczERMA8GA1UEBxMIU2Fu
    IEpvc2UxEzARBgNVBAgTCkNhbGlmb3JuaWExCzAJBgNVBAYTAlVTMB4XDTE2MDkw
    NzE5MzMwMVoXDTI2MDkwOTE5MzMwMVowgZAxKjAoBgNVBAMTIUNHIENBIFMgb24g
    dm9ybWV0cmljZHNtLmNpc2NvLmNvbTEVMBMGA1UECxMMU2F2YnVTdG9yZGV2MRYw
    FAYDVQQKEw1DaXNjbyBTeXN0ZW1zMREwDwYDVQQHEwhTYW4gSm9zZTETMB>EGA1UE
    CBMKQ2FsaWZvcm5pYTELMAkGA1UEBhMCVVMwggEiMA0GCSqGSIb3DQEBAQUAA4IB
    DwAwggEKAoIBAQDhX2UdIV>TQTchGo1FjAc5u1W9zAo/YkjD22ANpbEPiAmgWL97c
    Xwj7yzArflrZ2kWvQCm4f6AdLOFUWzbuo+Fxd3rurd>w6BhJXdLj8Piq8094PqCLp
    qdUF83SsRVVbCXHxOqdk9jsSQrvTcV4PloNrelMLq/mOqsaODs+us4ng7sMDtGXv
    LeKFC8DUEm0GlGQACwiJ3s9O4+P2CI/d4P/>EyWwqABf3YJmAI1EQyUnoTwrg6EgY
    ZvcpHsmjXnbBZrL+ON7FBcbrTanvjyJxE6tFf5cRPGhymfna7Fd3lfVwZCcGIoR+
>   EOIAwgetzIRM6FzMiV2/tDT8STo/oo5Tg3dDAgMBAAGjbj>BsMBIGA1UdEwEB/wQI
    MAYBAf8CAQAwDgYDVR0PAQH/>>>>>>>>>BAQDAgEGMB0GA1UdDgQWBBRnYyFiAK2lEDZJNC0Y
    VlIqMgiUJDAnBgNVHSMEIDAegBRnYyFiAK2lEDZJNC0YVlIqMgiUJIIGALOfZVDs
    MA0GCSqGSIb3DQEBCwUAA4IBAQAfhB2+Ft8V2ELAFa7PcG/rU09ux7LYcCjt3STa
    mzKdZ7Rn5COvknKrJX+EefT7xl03CQXT9aeSAddQUOCy8fhiPoaMFrlTgs1hdS0p
    NJvfxV6QCun2UMRSuxWfG>0QFfofnXeIGkAmEYOpUdArSOTbtt4v6Lja1A+KEsvWW
    5KaVemo2nsd+iD0IPCOhpShAgaAwpnYUq9mLfVgvV07Z+hmkuOIQTZ2+h+pJQtE0
    +U5qaTts4pMXpqQPjlid0NMuaPug1SpSD7KBsjwR1SzehzPdns16uprmvWa3VBk3
    OK6y55FoIu+Wg9i/8kmfkghyGwTfo6weEKbleuVwupvpriMF>
    -----END CERTIFICATE-----

UCS-A /org/storage-profile/security/drive-security/remote* # create login
UCS-A /org/storage-profile/security/drive-security/remote/login* # set username user1
UCS-A /org/storage-profile/security/drive-security/remote/login* # set password Password
UCS-A /org/storage-profile/security/drive-security/remote/login* # exit
UCS-A /org/storage-profile/security/drive-security/remote # exit
UCS-A /org/storage-profile/security/drive-security # show detail expand

Drive Security:
    Remote:
        Primary Server Name: 10.10.10.1
        Secondary Server Name:10.10.10.2
        KMIP Server Port: 5696
        Deployed Security Key:
        KMIP Server Certificate: -----BEGIN CERTIFICATE-----
```

```
MIIEEDCCAvigAwIBAgIGALOfZVDsMA0GCSqGSIb3DQEBCwUAMIGQMSowKAYDVQQD
EyFDRyBDQSBTIG9uIHZvcm1ldHJpY2RzbS5jaXNjby5jb20xFTATBgNVBAsTDFNh
dmJ1U3RvcmRldjEWMBQGA1UEChMNQ2lzY28gU3lzdGVtczERMA8GA1UEBxMIU2Fu
IEpvc2UxEzARBgNVBAgTCkNhbGlmb3JuaWExCzAJBgNVBAYTAlVTMB4XDTE2MDkw
NzE5MzMwMVoXDTI2MDkwOTE5MzMwMVowgZAxKjAoBgNVBAMTIUNHIENBIFMgb24g
dm9ybWV0cmljZHNtLmNpc2NvLmNvbTEVMBMGA1UECxMMU2F2YnVTdG9yZGV2MRYw
FAYDVQQKEw1DaXNjbyBTeXN0ZW1zMREwDwYDVQQHEwhTYW4gSm9zZTETMBEGA1UE
CBMKQ2FsaWZvcm5pYTELMAkGA1UEBhMCVVMwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQDhX2UdIVTQTchGo1FjAc5u1W9zAo/YkjD22ANpbEPiAmgWL97c
Xwj7yzArflrZ2kWvQCm4f6AdLOFUWzbuo+Fxd3rurdw6BhJXdLj8Piq8094PqCLp
qdUF83SsRVVbCXHxOqdk9jsSQrvTcV4PloNrelMLq/mOqsaODs+us4ng7sMDtGXv
LeKFC8DUEm0GlGQACwiJ3s9O4+P2CI/d4P/EyWwqABf3YJmAI1EQyUnoTwrg6EgY
ZvcpHsmjXnbBZrL+ON7FBcbrTanvjyJxE6tFf5cRPGhymfna7Fd3lfVwZCcGIoR+
EOIAwgetzIRM6FzMiV2/tDT8STo/oo5Tg3dDAgMBAAGjbjBsMBIGA1UdEwEB/wQI
MAYBAf8CAQAwDgYDVR0PAQH/BAQDAgEGMB0GA1UdDgQWBBRnYyFiAK2lEDZJNC0Y
VlIqMgiUJDAnBgNVHSMEIDAegBRnYyFiAK2lEDZJNC0YVlIqMgiUJIIGALOfZVDs
MA0GCSqGSIb3DQEBCwUAA4IBAQAfhB2+Ft8V2ELAFa7PcG/rU09ux7LYcCjt3STa
mzKdZ7Rn5COvknKrJX+EefT7xl03CQXT9aeSAddQUOCy8fhiPoaMFrlTgs1hdS0p
NJvfxV6QCun2UMRSuxWfG0QFfofnXeIGkAmEYOpUdArSOTbtt4v6Lja1A+KEsvWW
5KaVemo2nsd+iD0IPCOhpShAgaAwpnYUq9mLfVgvV07Z+hmkuOIQTZ2+h+pJQtE0
+U5qaTts4pMXpqQPjlid0NMuaPug1SpSD7KBsjwR1SzehzPdns16uprmvWa3VBk3
OK6y55FoIu+Wg9i/8kmfkghyGwTfo6weEKbleuVwupvpriMF
-----END CERTIFICATE-----
```

リモート セキュリティ キーの変更

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope server** *server-id*	指定されたサーバのサーバ モードを開始します。
ステップ 2	UCS-A /server # **scope raid-controller** *raid-controller-id {SAS | SAT}*	RAID コントローラ モードを開始します。現在、Cisco UCS Manager は SAS コントローラでのみ SED をサポートします。
ステップ 3	UCS-A /server/raid-controller # **set admin-state modify-remote-key**	リモートのセキュリティ ポリシーのセキュリティ キーを変更します。
ステップ 4	UCS-A /server/raid-controller # **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

この例では、ラックマウント サーバ用のコントローラのリモートのセキュリティ キーを変更する方法を示します。

```
UCS-A# scope server 3
UCS-A /server # scope raid-controller 1 sas
UCS-A /server/raid-controller # set admin-state modify-remote-key
```

```
UCS-A /server/raid-controller* # commit-buffer
UCS-A /server/raid-controller #
```

この例では、ブレードサーバ用のコントローラのリモートのセキュリティ キーを変更する方法を示します。

```
UCS-A# scope server 1/3
UCS-A chassis/server # scope raid-controller 1 sas
UCS-A chassis/server/raid-controller # set admin-state modify-remote-key
UCS-A chassis/server/raid-controller* # commit-buffer
UCS-A chassis/server/raid-controller #
```

リモートからローカルへのセキュリティ ポリシーの変更

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope org**	ルート組織モードを開始します。
ステップ 2	UCS-A /org # **scope storage-profile** *storage-profile-name*	指定されたストレージプロファイルのストレージプロファイル設定モードを開始します。
ステップ 3	UCS-A /org/storage-profile # **scope security**	指定されたストレージプロファイルのセキュリティポリシーモードを開始します。
ステップ 4	UCS A/org/storage-profile/security # **scope drive-security**	指定されたストレージプロファイルセキュリティのドライブセキュリティポリシー モードを開始します。
ステップ 5	UCS-A /org/storage-profile/security/drive-security # **delete remote**	既存のリモートのセキュリティ ポリシーを削除します。
ステップ 6	UCS-A /org/storage-profile/security/drive-security* # **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。
ステップ 7	UCS A/org/storage-profile/security/drive-security # **create local**	ローカルポリシーモードを作成し、開始します。
ステップ 8	UCS-A /org/storage-profile/security/drive-security/local* # **set security-key** *security-key*	ローカルポリシーのセキュリティ キーを設定します。

	コマンドまたはアクション	目的
ステップ 9	UCS-A /org/storage-profile/security/drive-security/local* # **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。
ステップ 10		

例

この例では、ローカルにリモートからセキュリティ ポリシーを変更する方法を示します。

```
UCS-A# scope org
UCS-A /org # scope storage-profile stp-demo
UCS-A /org/storage-profile # scope security
UCS-A /org/storage-profile/security # scope drive-security
UCS-A /org/storage-profile/security/drive-security # delete remote
UCS-A /org/storage-profile/security/drive-security* # commit-buffer
UCS-A /org/storage-profile/security/drive-security # create local
UCS-A /org/storage-profile/security/drive-security/local* # set security-key
thereare32charactersinthisseckey
UCS-A /org/storage-profile/security/drive-security/local* # commit-buffer
UCS-A /org/storage-profile/security/drive-security/local #
```

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。

既存の仮想ドライバの保護

始める前に

- コントローラは、セキュアでなければなりません。

- 仮想ドライブは、**孤立**状態である必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *server-id*	指定されたサーバのサーバ モードを開始します。
ステップ 2	UCS-A /server# **scope raid-controller** *raid-controller-id {SAS | SAT}*	RAID コントローラ モードを開始します。 現在、 Cisco UCS Manager は SAS コントローラでのみ SED をサポートしています。
ステップ 3	UCS-A /server/raid-controller# **scope virtual-drive** *virtual-drive-id*	指定された孤立仮想ドライブの仮想ドライブ モードを開始します。
ステップ 4	UCS-A /server/raid-controller/virtual-drive# **set admin-state secure-drive-group**	既存の仮想ドライブを保護します。
ステップ 5	UCS-A /server/raid-controller/virtual-drive*# **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

この例では、ラックマウント サーバ の既存の仮想ドライブ を保護する方法を示します。

```
UCS-A# scope server 1
UCS-A /server# scope raid-controller 3 sas
UCS-A /server/raid-controller# scope virtual-drive 1000
UCS-A /server/raid-controller/virtual-drive # set admin-state secure-drive-group
UCS-A /server/raid-controller/virtual-drive*# commit-buffer
UCS-A /server/raid-controller/virtual-drive#
```

この例は、ブレード サーバの既存の仮想ドライブを保護する方法を示します。

```
UCS-A# scope server 1/4
UCS-A chassis/server# scope raid-controller 3 sas
UCS-A chassis/server/raid-controller# scope virtual-drive 1000
UCS-A chassis/server/raid-controller/virtual-drive # set admin-state secure-drive-group

UCS-A chassis/server/raid-controller/virtual-drive*# commit-buffer
UCS-A chassis/server/raid-controller/virtual-drive#
```

ディスクのセキュリティの有効化

始める前に

ディスクが JBOD であることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A# **scope server** *server-id*	指定されたサーバのサーバ モードを開始します。
ステップ 2	UCS-A /server # **scope raid-controller** *raid-controller-id {SAS | SAT}*	RAID コントローラ モードを開始します。 現在、 Cisco UCS Manager は SAS コントローラでのみ SED をサポートしています。
ステップ 3	UCS-A /server/raid-controller # **scope local-disk** *local-disk-id*	ローカル ディスク設定モードを開始します
ステップ 4	UCS A/server/raid-controller/local-disk # **set admin-state enable-security**	JBOD でセキュリティを有効にします。
ステップ 5	UCS A/server/raid-controller/local-ディスク * # **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

この例では、ラックマウント サーバの JBOD のセキュリティを有効にする方法を示します。

```
UCS-A# scope server 1
UCS-A /server # scope raid-controller 3 sas
UCS-A /server/raid-controller # scope local-disk 2
UCS-A /server/raid-controller/local-disk # set admin-state enable-security
UCS-A /server/raid-controller/local-disk* # commit-buffer
UCS-A /server/raid-controller/local-disk #
```

この例では、ブレード サーバの JBOD のセキュリティを有効にする方法を示します。

```
UCS-A# scope server 1/3
UCS-A chassis/server # scope raid-controller 3 sas
UCS-A chassis/server/raid-controller # scope local-disk 2
UCS-A chassis/server/raid-controller/local-disk # set admin-state enable-security
```

```
UCS-A chassis/server/raid-controller/local-disk* # commit-buffer
UCS-A chassis/server/raid-controller/local-disk #
```

セキュア ディスクの消去

始める前に

ディスクが **Unconfigured Good** 状態であることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope server** *server-id*	指定されたサーバのサーバ モードを開始します。
ステップ 2	UCS-A /server # **scope raid-controller** *raid-controller-id {SAS | SAT}*	RAID コントローラ モードを開始します。 現在、 Cisco UCS Manager は SAS コントローラでのみ SED をサポートしています。
ステップ 3	UCS-A /server/raid-controller # **scope local-disk** *local-disk-id*	ローカル ディスク設定モードを開始します
ステップ 4	UCS-A /server/raid-controller/local-disk # **set admin-state clear secure-drive**	セキュアなディスクを消去し、ディスクのセキュリティをクリアします。
ステップ 5	UCS A/server/raid-controller/local-ディスク * # **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

この例は、ラック マウント サーバのセキュア ディスクを消去する方法を示します。

```
UCS-A # scope server 1
UCS-A /server # scope raid-controller 3 sas
UCS-A /server/raid-controller # scope local-disk 2
UCS-A /server/raid-controller/local-disk # set admin-state clear secure-drive
UCS-A /server/raid-controller/local-disk* # commit-buffer
UCS-A /server/raid-controller/local-disk #
```

この例は、ブレード サーバのセキュア ディスクを消去する方法を示します。

```
UCS-A # scope server 1/3
UCS-A chassis/server # scope raid-controller 3 sas
```

```
UCS-A chassis/server/raid-controller # scope local-disk 2
UCS-A chassis/server/raid-controller/local-disk # set admin-state clear secure-drive
UCS-A chassis/server/raid-controller/local-disk* # commit-buffer
UCS-A chassis/server/raid-controller/local-disk #
```

コントローラのセキュリティのディセーブル化

始める前に

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope server** *server-id*	指定されたサーバのサーバ モードを開始します。
ステップ 2	UCS-A /server # **scope raid-controller** *raid-controller-id {SAS | SAT}*	RAID コントローラ モードを開始します。現在、 Cisco UCS Manager は SAS コントローラでのみ SED をサポートしています。
ステップ 3	UCS-A /server/raid-controller # **set admin-state disable-security**	コントローラのセキュリティ キーを無効にします。
ステップ 4	UCS-A /server/raid-controller # **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

この例では、ラックマウント サーバの コントローラ のセキュリティを無効にする方法を示します。

```
UCS-A# scope server 1
UCS-A /server # scope raid-controller 3 sas
UCS-A /server/raid-controller # set admin-state disable-security
UCS-A /server/raid-controller* # commit-buffer
UCS-A /server/raid-controller #
```

この例では、ブレードサーバのコントローラのセキュリティを無効にする方法を示します。

```
UCS-A# scope server 1/3
```

```
UCS-A chassis/server # scope raid-controller 3 sas
UCS-A chassis/server/raid-controller # set admin-state disable-security
UCS-A chassis/server/raid-controller* # commit-buffer
UCS-A chassis/server/raid-controller #
```

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。

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。

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope server** *server-id*	指定したサーバのサーバ モードを開始します。
ステップ 2	UCS-A /server # **scope raid-controller** *raid-controller-id {SAS | SAT}*	RAID コントローラ モードを開始します。現在、Cisco UCS Manager は SAS コントローラでのみ SED をサポートします。
ステップ 3	UCS-A /server/raid-controller # **set admin-state unlock-disk** [*security-key*]	ロックされたディスクのロックを解除します。 セキュリティキーが設定される場合、このキーは、ロックされた状態にあるディスクをロック解除するために使用されます。 セキュリティキーが設定されない場合、Cisco UCS Manager は KMIP サーバを使用してディスクをロック解除しようとします。リモート セキュリティがサーバに設定される場合のみ、セキュリティキーの設定はオプションです。
ステップ 4	UCS-A/server/raid-controller * # **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

この例では、ローカル セキュリティ ポリシーが設定されたラックマウント サーバでロックされたディスクのロックをセキュリティキーを使用して解除する方法を説明します。

```
UCS-A # scope server 1
UCS-A /server # scope raid-controller 3 sas
UCS-A /server/raid-controller # set admin-state unlock-disk thisisastring
UCS-A /server/raid-controller* # commit-buffer
UCS-A /server/raid-controller #
```

この例では、リモート セキュリティ ポリシーが設定されたラックマウント サーバでロックされたディスクのロックをKMIPサーバを使用して解除する方法を説明します。

```
UCS-A # scope server 1
UCS-A /server # scope raid-controller 3 sas
UCS-A /server/raid-controller # set admin-state unlock-disk
UCS-A /server/raid-controller* # commit-buffer
UCS-A /server/raid-controller #
```

この例では、ローカル セキュリティ ポリシーが設定されたブレード サーバでロックされたディスクをセキュリティ キーを使用して解除する方法を説明します。

```
UCS-A # scope server 1/2
UCS-A chassis/server # scope raid-controller 3 sas
UCS-A chassis/server/raid-controller # set admin-state unlock-disk thisisastring
UCS-A chassis/server/raid-controller* # commit-buffer
UCS-A chassis/server/raid-controller #
```

この例では、リモート セキュリティ ポリシーが設定されたブレード サーバでロックされたディスクのロックを KMIP サーバを使用して解除する方法を説明します。

```
UCS-A # scope server 1/2
UCS-A chassis/server # scope raid-controller 3 sas
UCS-A chassis/server/raid-controller # set admin-state unlock-disk
UCS-A chassis/server/raid-controller* # commit-buffer
UCS-A chassis/server/raid-controller #
```

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

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope server** *server-id*	指定されたサーバのサーバ モードを開始します。
ステップ 2	UCS-A /server # **scope raid-controller** *raid-controller-id {SAS | SAT}*	RAID コントローラ モードを開始します。 現在、 Cisco UCS Manager は SAS コントローラでのみ SED をサポートしています。
ステップ 3	UCS-A /server/raid-controller # **scope local-disk** *local-disk-id*	ローカル ディスク設定モードを開始します
ステップ 4	UCS-A /server/raid-controller/local-disk # **set admin-state clear secure-foreign-config-drive**	セキュアな外部設定ドライブをクリアします。
ステップ 5	UCS A/server/raid-controller/local-ディスク * # **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

この例は、ラック マウント サーバの外部設定ディスクをクリアする方法を示します。

```
UCS-A# scope server 1
UCS-A /server # scope raid-controller 3 sas
UCS-A /server/raid-controller # scope local-disk 2
UCS-A /server/raid-controller/local-disk # set admin-state clear
secure-foreign-config-drive
UCS-A /server/raid-controller/local-disk* # commit-buffer
UCS-A /server/raid-controller/local-disk #
```

この例は、ブレード サーバの外部設定ディスクをクリアする方法を示します。

```
UCS-A# scope server 1/3
UCS-A chassis/server # scope raid-controller 3 sas
UCS-A chassis/server/raid-controller # scope local-disk 2
UCS-A chassis/server/raid-controller/local-disk # set admin-state clear
secure-foreign-config-drive
UCS-A chassis/server/raid-controller/local-disk* # commit-buffer
UCS-A chassis/server/raid-controller/local-disk #
```

コントローラのセキュリティ フラグの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope server** *server-id*	指定されたサーバのサーバ モードを開始します。
ステップ 2	UCS-A /server # **scope raid-controller** *raid-controller-id {SAS | SAT}*	RAID コントローラ モードを開始します。 現在、 Cisco UCS Manager は SAS コントローラでのみ SED をサポートしています。
ステップ 3	UCS-A /server/raid-controller # **show detail**	RAID コントローラの詳細を表示します。

例

この例では、ラックマウント サーバの コントローラ のセキュリティ フラグが有効になっているか、チェックする方法を示します。

```
UCS-A # scope server 1
UCS-A /server # scope raid-controller 3 sas
UCS-A /server/raid-controller # show detail

RAID Controller:
    ID: 3
    Type: SAS
    PCI Addr: 03:00.0
    Vendor: LSI Corp.
    Model: LSI MegaRAID SAS 3108
    Serial: SV55346948
    HW Rev: C0
    Raid Support: RAID0, RAID1, RAID5, RAID6, RAID10, RAID50, RAID60
    OOB Interface Supported: Yes
    Mode: RAID
    Rebuild Rate: 30
    Controller Status: Optimal
    Config State: Applied
    Pinned Cache Status: Disabled
    Sub OEM ID: 0
    Supported Strip Sizes: 1MB,64KB,256KB,512KB,128KB
    Default Strip Size: 64KB
    PCI Slot: HBA
    Controller Flags: Drive Security Capable
```

この例では、ブレード サーバの コントローラ のセキュリティ フラグが有効になっているか、チェックする方法を示します。

```
UCS-A # scope server 1/2
UCS-A chassis/server # scope raid-controller 3 sas
UCS-A chassis/server/raid-controller # show detail

RAID Controller:
    ID: 3
    Type: SAS
    PCI Addr: 03:00.0
    Vendor: LSI Corp.
    Model: LSI MegaRAID SAS 3108
    Serial: SV55346948
    HW Rev: C0
    Raid Support: RAID0, RAID1, RAID5, RAID6, RAID10, RAID50, RAID60
    OOB Interface Supported: Yes
    Mode: RAID
    Rebuild Rate: 30
    Controller Status: Optimal
    Config State: Applied
    Pinned Cache Status: Disabled
    Sub OEM ID: 0
    Supported Strip Sizes: 1MB,64KB,256KB,512KB,128KB
    Default Strip Size: 64KB
    PCI Slot: HBA
    Controller Flags: Drive Security Capable
```

ローカル ディスクのセキュリティ フラグの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope server** *server-id*	指定されたサーバのサーバ モードを開始します。
ステップ 2	UCS-A /server # **scope raid-controller** *raid-controller-id {SAS | SAT}*	RAID コントローラ モードを開始します。 現在、 Cisco UCS Manager は SAS コントローラでのみ SED をサポートしています。
ステップ 3	UCS-A /server/raid-controller # **scope local-disk** *local-disk-id*	ローカル ディスク設定モードを開始します
ステップ 4	UCS-A /server/raid-controller/local-disk # **show detail**	ローカルディスクの詳細を表示します。

例

この例では、ラックマウント サーバの ローカルディスク のセキュリティ フラグを表示する方法を示します。

```
UCS-A # scope server 1
UCS-A /server # scope raid-controller 3 sas
UCS-A /server/raid-controller #scope local-disk 2
UCS-A /server/raid-controller/local-disk # show detail

Local Disk:
    ID: 4
    Block Size: 512
    Physical Block Size: 4096
    Blocks: 1560545280
    Raw Size: 763097
    Size: 761985
    Technology: SSD
    Operability: Operable
    Oper Qualifier Reason: N/A
    Presence: Equipped
    Connection Protocol: SAS
    Product Variant: default
    Product Name: 800GB Enterprise performance SAS SED SSD (10 FWPD) - MTFDJAK800MBS
    PID: UCS-SD800GBEK9
    VID: V01
    Vendor: MICRON
    Model: S650DC-800FIPS
    Vendor Description: Micron
    Serial: ZAZ090VD000822150Z3
    HW Rev: 0
    Running-Vers: MB13
    Average Seek Time (R/W): N/A
    Track to Track Seek Time (R/W): 115ms
    Part Number: 16-100911-01
    SKU: UCS-SD800GBEK9
    Drive State: Online
    Power State: Active
    Link Speed: 12 Gbps
    Enclosure Association Type: Direct Attached
    Device Version: MB13
    Drive Security Flags: Secured,Security Enabled,Security Capable
```

この例では、ブレード サーバの ローカル ディスク のセキュリティ フラグを表示する方法を示します。

```
UCS-A # scope server 1/2
UCS-A chassis/server # scope raid-controller 3 sas
UCS-A chassis/server/raid-controller #scope local-disk 2
UCS-A chassis/server/raid-controller/local-disk # show detail

Local Disk:
    ID: 4
    Block Size: 512
    Physical Block Size: 4096
    Blocks: 1560545280
    Raw Size: 763097
```

```
Size: 761985
Technology: SSD
Operability: Operable
Oper Qualifier Reason: N/A
Presence: Equipped
Connection Protocol: SAS
Product Variant: default
Product Name: 800GB Enterprise performance SAS SED SSD (10 FWPD) - MTFDJAK800MBS
PID: UCS-SD800GBEK9
VID: V01
Vendor: MICRON
Model: S650DC-800FIPS
Vendor Description: Micron
Serial: ZAZ090VD000822150Z3
HW Rev: 0
Running-Vers: MB13
Average Seek Time (R/W): N/A
Track to Track Seek Time (R/W): 115ms
Part Number: 16-100911-01
SKU: UCS-SD800GBEK9
Drive State: Online
Power State: Active
Link Speed: 12 Gbps
Enclosure Association Type: Direct Attached
Device Version: MB13
Drive Security Flags: Secured,Security Enabled,Security Capable
```

仮想ドライブのセキュリティ フラグの表示

手順

	コマンドまたはアクション	目的
ステップ 1	UCS-A # **scope server** *server-id*	指定されたサーバのサーバ モードを開始します。
ステップ 2	UCS-A /server # **scope raid-controller** *raid-controller-id {SAS | SAT}*	RAID コントローラ モードを開始します。 現在、 Cisco UCS Manager は SAS コントローラでのみ SED をサポートしています。
ステップ 3	UCS-A /server/raid-controller # **scope virtual-drive** *virtual-drive-id*	仮想ドライブ モードを開始します。
ステップ 4	UCS-A /server/raid-controller/virtual-drive # **show detail**	仮想デバイスの詳細を表示します。

例

この例では、ラックマウント サーバの仮想ディスク のセキュリティ フラグを表示する方法を示します。

```
UCS-A # scope server 1
UCS-A /server # scope raid-controller 3 sas
UCS-A /server/raid-controller # scope virtual-drive 1000
UCS-A /server/raid-controller/virtual-drive # show detail

Virtual Drive:
    ID: 1000
    Name: luna
    Block Size: 512
    Blocks: 20971520
    Size: 10240
    Operability: Operable
    Presence: Equipped
    Lifecycle: Allocated
    Drive State: Optimal
    Type: RAID 0 Striped
    Strip Size (KB): 64
    Access Policy: Read Write
    Read Policy: Normal
    Configured Write Cache Policy: Write Through
    Actual Write Cache Policy: Write Through
    IO Policy: Direct
    Drive Cache: No Change
    Bootable: False
    Oper Device ID: 0
    Change Qualifier: No Change
    Config State: Applied
    Deploy Action: No Action
    Service Profile Lun Reference: org-root/ls-sp1/vdrive-ref-lun-1
    Assigned To Server: sys/rack-unit-1
    Available Size on Disk Group (MB): 751745
    Unique Identifier: 90ae6ea0-6a39-49e1-9c0d-0f3e2e9ecfce
    Vendor Unique Identifier: 678da6e7-15b2-9c20-2011-c4f60c40e57a
    Security Flags: Drive Security Enable,Drive Security Capable
```

この例は、ブレードサーバの仮想ディスクのセキュリティ フラグを表示する方法を示しています。

```
UCS-A # scope server 1/2
UCS-A chassis/server # scope raid-controller 3 sas
UCS-A chassis/server/raid-controller # scope virtual-drive 1000
UCS-A chassis/server/raid-controller/virtual-drive # show detail

Virtual Drive:
    ID: 1000
    Name: luna
    Block Size: 512
    Blocks: 20971520
    Size: 10240
    Operability: Operable
    Presence: Equipped
    Lifecycle: Allocated
    Drive State: Optimal
    Type: RAID 0 Striped
    Strip Size (KB): 64
    Access Policy: Read Write
    Read Policy: Normal
    Configured Write Cache Policy: Write Through
    Actual Write Cache Policy: Write Through
```

```
IO Policy: Direct
Drive Cache: No Change
Bootable: False
Oper Device ID: 0
Change Qualifier: No Change
Config State: Applied
Deploy Action: No Action
Service Profile Lun Reference: org-root/ls-sp1/vdrive-ref-lun-1
Assigned To Server: sys/rack-unit-1
Available Size on Disk Group (MB): 751745
Unique Identifier: 90ae6ea0-6a39-49e1-9c0d-0f3e2e9ecfce
Vendor Unique Identifier: 678da6e7-15b2-9c20-2011-c4f60c40e57a
Security Flags: Drive Security Enable,Drive Security Capable
```

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。