



## 暗号化の管理

- [自己暗号化ドライブの概要 \(1 ページ\)](#)
- [HyperFlex クラスタが暗号化できることの確認 \(2 ページ\)](#)
- [ローカル暗号化キーの構成 \(2 ページ\)](#)
- [ローカル暗号化キーの変更 \(3 ページ\)](#)
- [ローカルの暗号化キーの無効化 \(3 ページ\)](#)
- [暗号化されたディスクを安全に消去する \(4 ページ\)](#)
- [リモート キー管理 \(4 ページ\)](#)
- [リモート暗号化キーの構成 \(5 ページ\)](#)
- [証明書署名要求の生成 \(6 ページ\)](#)
- [CSR \(証明書署名要求\) を使用したキー管理サーバの構成 \(7 ページ\)](#)
- [自己署名証明書の生成 \(8 ページ\)](#)
- [SSC \(自己署名証明書\) を使用したキー管理サーバの構成 \(10 ページ\)](#)
- [暗号化の再起動 \(11 ページ\)](#)

## 自己暗号化ドライブの概要

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暗号化された形式で格納されます。メディアの暗号化キーは、データ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。

セキュリティキー (キー暗号化キーまたは認証パスフレーズとも呼ばれます) を使用して、メディア暗号化キーを暗号化します。SED を有効にするには、セキュリティ キーを入力する必要があります。ディスクがロックされていない場合、データをフェッチするのにキーは必要ありません。

Cisco HyperFlex Systems を使用して、ローカルまたはリモートのセキュリティ キーを構成できます。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、ドライブの電源が再投入されると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。

## HyperFlex クラスタが暗号化できることの確認

### HX Data Platform Plug-inを使用しての確認

1. HX Data Platform Plug-in から vSphere Web Clientにログインします。
2. [Global Inventory Lists (グローバル インベントリ リスト)] > [Cisco HyperFlex Systems] > [Cisco HX Data Platform] > [Cluster\_Name] > [Summary (概要)] > の順に選択します。
3. HyperFlex クラスタに SED ドライブが含まれていて暗号化可能な場合は、[Summary] タブの上部に [Data At Rest Encryption-Capable] が表示されます。

### HX Connect ユーザ インターフェイスを使用しての確認

1. HX Connect UI から、[Encryption] を選択します。
2. HX クラスタに SED ドライブが含まれていて暗号化可能な場合は、[Encryption] ページに [Data At Rest Encryption-Available] が表示されます。

## ローカル暗号化キーの構成

ステップ1 Cisco HyperFlex Connect ナビゲーション ウィンドウで、[Encryption] を選択します。

ステップ2 [Encryption] ページで、[Configure encryption] をクリックします。

ステップ3 次の Cisco UCS Manager クレデンシャルを入力します。

UI 要素	基本情報
[UCS Manager host name] フィールド	Cisco UCS Manager のクラスタ ホスト名です。 IP アドレスまたは FQDN を入力します。 <eng-fi12.eng.storvisor.com>
[User name] フィールド	<admin> ユーザ名
[Password] フィールド	<admin> password

[Next] をクリックします。

**ステップ 4** ローカルで生成され、保存された暗号化キーを使用して HyperFlex クラスタを保護するには、[Local Key] を選択します。

[Next] をクリックします。

**ステップ 5** このクラスタの暗号キー（パスフレーズ）を入力してください。

（注） ちょうど 32 文字の英数字で入力します。

**ステップ 6** [Enable Encryption] をクリックします。

## ローカル暗号化キーの変更

**ステップ 1** Cisco HyperFlex Connect ナビゲーション ウィンドウで、[Encryption] を選択します。

**ステップ 2** [Encryption] ページで、[Re-key] をクリックします。

**ステップ 3** 次の Cisco UCS Manager クレデンシャルを入力します。

UI 要素	基本情報
[UCS Manager host name] フィールド	たとえば <i>10.193.211.120</i> と入力します。
[User name] フィールド	<admin> ユーザ名。
[Password] フィールド	<admin> パスワード。

[Next] をクリックします。

**ステップ 4** クラスタの [Existing Encryption Key] と [New Encryption Key] を入力します。

（注） ちょうど 32 文字の英数字で入力します。

**ステップ 5** [Re-key] をクリックします。

## ローカルの暗号化キーの無効化

**ステップ 1** Cisco HyperFlex Connect ナビゲーション ウィンドウで、[Encryption] を選択します。

**ステップ 2** [Encryption] ページの [Edit configuration] ドロップダウンメニューから、[Disable encryption] を選択します。

**ステップ 3** 次の Cisco UCS Manager クレデンシャルを入力します。

UI 要素	基本情報
[UCS Manager host name] フィールド	Cisco UCS Manager のクラスタ ホスト名です。 IP アドレスまたは FQDN を入力します。 <eng-fi12.eng.storvisor.com>
[User name] フィールド	<admin> ユーザ名
[Password] フィールド	<admin> password

[Next] をクリックします。

**ステップ 4** クラスタで暗号化キーを無効にするには、クラスタで使用中の暗号化キーを入力します。

**ステップ 5** [Disable encryption] をクリックします。

**ステップ 6** クラスタで暗号化キーを無効にするを確認するために [Disable encryption?] ダイアログボックスで、[Yes, disable encryption] をクリックします。

## 暗号化されたディスクを安全に消去する

**ステップ 1** Cisco HyperFlex Connect ナビゲーション ウィンドウで、[System Information] を選択します。

**ステップ 2** [Disks] タブで、ローカル キーを安全に消去するディスクを選択します。

**ステップ 3** [Secure Erase] ボタンをクリックします。

**ステップ 4** クラスタ上の暗号化されたディスクを安全に消去するには、クラスタで使用中の暗号化キーを入力します。

**ステップ 5** [Secure erase] をクリックします。

**ステップ 6** [Erase this disk?] ダイアログボックスで、[Yes, erase this disk] をクリックして暗号化されたディスクを安全に消去します。

## リモート キー管理

リモート KMIP 証明書 の処理の一般的な手順は次のとおりです。

- 自己署名する場合は、設定でローカルの認証局を指定し、ルート証明書を取得します。
- 信頼されたサードパーティの CA を使用する場合は、設定でそれを指定し、そのルート証明書を使用します。
- クラスタ キーを尋ねる HX 暗号化フィールドにルート証明書を入力します。
- SSL サーバ証明書を作成し、証明書署名要求 (CSR) を生成します。

- 使用しているルート証明書で CSR に署名します。
- クライアント証明書を使用する KMIP サーバ設定を更新します。
- SSL 証明書とルート CA が利用可能な状態で、選択したベンダーに固有の KMIP サービス設定で続行します。

### SafeNet キー管理

SafeNet キー管理サーバを使用した暗号化キーの管理に関する詳細については、『[HyperFlex Encryption and SafeNet Key Management TechNote](#)』および『[SafeNet Admin Guide](#)』を参照してください。

### Vormetric キー管理

Vormetric キー管理サーバを使用した暗号化キーの管理に関する詳細は、[Vormetric サポートポータル](#)のマニュアルダウンロードセクションを参照してください。

## リモート暗号化キーの構成

**ステップ 1** Cisco HyperFlex Connect ナビゲーション ウィンドウで、[Encryption] を選択します。

**ステップ 2** [Encryption] ページで、[Configure encryption] をクリックします。

**ステップ 3** 次の Cisco UCS Manager クレデンシアルを入力します。

UI 要素	基本情報
[UCS Manager host name] フィールド	Cisco UCS Manager のクラスタ ホスト名です。 IP アドレスまたは FQDN を入力します。 <eng-fi12.eng.storvisor.com>
[User name] フィールド	<admin> ユーザ名
[Password] フィールド	<root> パスワード

[Next] をクリックします。

**ステップ 4** キー管理 (KMIP) サーバによって生成されたリモートセキュリティ キーを使用して HyperFlex クラスタを保護するには、[Key Management Server] を選択します。

次の証明書の 1 つを使用するようにクラスタ内の自己暗号化ドライブを持つサーバを構成できます。

- [Use certificate authority signed certificates] : 外部認証局によって署名された証明書署名要求 (CSR) を生成します。
- [Use self-signed certificates] : 自己署名の証明書を生成します。

[Next] をクリックします。

## ステップ 5

## 次のタスク

証明書署名要求または自己署名の証明書を生成できます。

## 証明書署名要求の生成

ステップ 1 Cisco HyperFlex Connect ナビゲーション ウィンドウで、[Encryption] を選択します。

ステップ 2 [Encryption] ページで、[Configure encryption] をクリックします。

ステップ 3 次の Cisco UCS Manager クレデンシヤルを入力します。

UI 要素	基本情報
[UCS Manager host name] フィールド	Cisco UCS Manager のクラスタ ホスト名です。 IP アドレスまたは FQDN を入力します。 <eng-fi12.eng.storvisor.com>
[User name] フィールド	<admin> ユーザ名
[Password] フィールド	<admin> password

[Next] をクリックします。

ステップ 4 [Key Management Server] > [Use certificate authority signed certificates] を選択します。

[Next] をクリックします。

ステップ 5 キー管理 (KMIP) サーバを構成するためのリモート暗号化キーを生成するには、次の情報を入力します。

UI 要素	基本情報
[Email address] フィールド	<admin> 電子メール アドレス
[Organization name] フィールド	証明書を要求している組織。 32 文字まで入力します。
[Organization unit name] フィールド	組織ユニット 最大 64 文字まで入力できます。
[Locality] フィールド	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。

UI 要素	基本情報
[State] フィールド	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。
[Country] フィールド	会社が存在する国。 2 つの英字を大文字で入力します。
[Valid for (days)] フィールド	証明書の有効期間。

**ステップ 6** HyperFlex のすべてのノードのための証明書署名要求（CSR）を生成してそれらをダウンロードするには、[Generate certificates] をクリックします。

**ステップ 7** 証明書をダウンロードし、認証局による署名を受けます。[Close] をクリックします。

#### 次のタスク

1. 署名付き証明書をアップロードします。
2. KMIP サーバ（キー管理サーバ）を設定します。

## CSR（証明書署名要求）を使用したキー管理サーバの構成

#### 始める前に

KMIP（キーマネージメント）サーバを構成するために、ローカルマシン上で生成された CSR をダウンロードし、それが認証局によって署名され、Cisco HX Data Platform UI 経由でアップロードされていることを確認してください。

**ステップ 1** Cisco HyperFlex Connect ナビゲーション ウィンドウで、[Encryption] を選択します。

**ステップ 2** [Encryption] ページで、[Continue configuration] をクリックします。

**ステップ 3** [Continue configuration] ドロップダウンリストから、[Manage certificates] を選択して CSR をアップロードします。

**ステップ 4** 次の Cisco UCS Manager クレデンシャルを入力します。

UI 要素	基本情報
[UCS Manager host name] フィールド	Cisco UCS Manager のクラスタ ホスト名です。 IP アドレスまたは FQDN を入力します。 <eng-fi12.eng.storvisor.com>

UI 要素	基本情報
[User name] フィールド	<admin> ユーザ名
[Password] フィールド	<root> パスワード

[Next] をクリックします。

**ステップ 5** [Upload certificate authority signed certificates] を選択します。[Next] をクリックします。

**ステップ 6** [Upload new certificate] で CA 署名証明書をアップロードします。[Upload] をクリックします。

**ステップ 7** [Continue configuration] ドロップダウンリストから [Configure key management server] を選択して KMIP サーバを構成します。

**ステップ 8** Cisco UCS Manager のクレデンシャルを入力して、プライマリ キー管理 (KMIP) サーバと必要に応じてセカンダリ KMIP サーバを設定します。

UI 要素	基本情報
[Primary key management server] フィールド	プライマリ キー管理サーバの IP アドレスを入力します。
(省略可能) [Secondary key management server] フィールド	冗長化のためのセカンダリ キー管理サーバを設定した場合は、ここで詳細情報を入力します。
[Port number] フィールド	キー管理サーバに使用するポート番号を入力します。
[Public key] フィールド	KMIP サーバ構成中に生成された認証局の公開ルート証明書を入力します。

**ステップ 9** [Save] をクリックしてクラスタをリモート管理キーで暗号化します。

例

## 自己署名証明書の生成

**ステップ 1** Cisco HyperFlex Connect ナビゲーション ウィンドウで、[Encryption] を選択します。

**ステップ 2** [Encryption] ページで、[Configure encryption] をクリックします。

**ステップ 3** 次の Cisco UCS Manager クレデンシャルを入力します。

UI 要素	基本情報
[UCS Manager host name] フィールド	Cisco UCS Manager のクラスタ ホスト名です。 IP アドレスまたは FQDN を入力します。 <eng-f12.eng.storvisor.com>
[User name] フィールド	<admin> ユーザ名
[Password] フィールド	<root> パスワード

[Next] をクリックします。

**ステップ 4** [Key Management Server] > [Use self-signed certificates] を選択します。

[Next] をクリックします。

**ステップ 5** キー管理 (KMIP) サーバを構成するためのリモート暗号化キーを生成するには、次の情報を入力します。

UI 要素	基本情報
[Email address] フィールド	<admin> 電子メールアドレス
[Organization name] フィールド	証明書を要求している組織。 32 文字まで入力します。
[Organization unit name] フィールド	組織ユニット 最大 64 文字まで入力できます。
[Locality] フィールド	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。
[State] フィールド	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。
[Country] フィールド	会社が存在する国。 2 つの英字を大文字で入力します。
[Valid for (days)] フィールド	証明書の有効期間。

**ステップ 6** すべての HyperFlex ノードのために自己署名証明書を生成してそれらをダウンロードするには、[Generate certificates] をクリックします。

**ステップ 7** 証明書をダウンロードし、認証局による署名を受けます。[Close] をクリックします。

### 次のタスク

- 署名付き証明書をアップロードします。

2. KMIP サーバ（キー管理サーバ）を設定します。

## SSC（自己署名証明書）を使用したキー管理サーバの構成

### 始める前に

KMIP（キー マネージメント）サーバを構成するためにローカル マシン上で生成された SSC がダウンロードされていることを確認してください。

- ステップ 1 Cisco HyperFlex Connect ナビゲーション ウィンドウで、[Encryption] を選択します。
- ステップ 2 [Encryption] ページで、[Edit configuration] をクリックします。
- ステップ 3 [Edit configuration] ドロップダウンリストから、[Manage certificates] を選択します。
- ステップ 4 次の Cisco UCS Manager のクレデンシャルを入力して、プライマリ キー管理（KMIP）サーバと必要に応じてセカンダリ KMIP サーバを設定します。

UI 要素	基本情報
[UCS Manager host name] フィールド	Cisco UCS Manager のクラスタ ホスト名です。 IP アドレスまたは FQDN を入力します。 <eng-fi12.eng.storvisor.com>
[User name] フィールド	<admin> ユーザ名
[Password] フィールド	<admin> password

[Next] をクリックします。

- ステップ 5 プライマリおよびセカンダリ キー管理（KMIP）サーバのクレデンシャルを入力します。

UI 要素	基本情報
[Primary key management server] フィールド	プライマリ キー管理サーバの IP アドレスを入力します。
（省略可能）[Secondary key management server] フィールド	冗長化のためのセカンダリ キー管理サーバを設定した場合は、ここで詳細情報を入力します。
[Port number] フィールド	キー管理サーバに使用するポート番号を入力します。
[Public key] フィールド	KMIP サーバ構成中に生成された認証局の公開ルート証明書をを入力します。

ステップ 6 [Save] をクリックしてクラスタをリモート管理キーで暗号化します。

## 暗号化の再起動

HyperFlex クラスタを安全に暗号化するには、Cisco UCS Manager のクレデンシャルを入力して、キー管理サーバまたは ローカル キーの構成を再度開始します。

UI 要素	基本情報
[UCS Manager host name] フィールド	Cisco UCS Manager のクラスタ ホスト名です。 IP アドレスまたは FQDN を入力します。 <eng-fi12.eng.storvisor.com>
[User name] フィールド	<admin> ユーザ名
[Password] フィールド	<admin> password

