証明書とサーバ セキュリティの管理

この章は、次の項で構成されています。

サーバ証明書の管理

証明書署名要求（CSR）を生成して新しい証明書を取得し、新しい証明書を Cisco IMC にアップロードして現在のサーバ証明書と交換することができます。サーバ証明書は、Verisign のようなパブリック認証局（CA）、または独自に使用している認証局のいずれかによって署名されます。生成される証明書キーの長は 2048 ビットです。

（注） この章に記載されている以下のタスクを実行する前に、Cisco IMC の時刻が現在の時刻に設定されていることを確認します。

手順

ステップ 1 Cisco IMC から CSR を生成します。

ステップ 2 証明書の発行と署名を行う認証局に CSR ファイルを送信します。組織で独自の自己署名証明書を生成している場合は、CSR ファイルを使用して自己署名証明書を生成できます。

ステップ 3 新しい証明書を Cisco IMC にアップロードします。

（注） アップロードされた証明書は、Cisco IMC によって生成された CSR から作成される必要があります。この方法で作成されていない証明書はアップロードしないでください。

証明書署名要求の生成

自己署名証明書は、**generate-csr** コマンドを使用して手動で生成するか、ホスト名の変更時に自動的に生成できます。ホスト名の変更および事自己署名証明書の自動生成の詳細は、「**共通プロパティの設定**」セクションを参照してください。

証明書署名要求を手動で生成するには、次の手順を実行します。

始める前に

- 証明書を設定するには、admin 権限を持つユーザとしてログインする必要があります。
- Cisco IMC の時刻が現在の時刻に設定されてい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	Server# **scope certificate**	証明書コマンド モードを開始します。
ステップ 2	Server /certificate # **generate-csr**	証明書署名要求（CSR）の生成に関するダイアログを起動します。

証明書署名要求に関して、次の情報の入力を求めるプロンプトが表示されます。

名前	説明
[コモンネーム（Common Name）] フィールド	Cisco IMC の完全修飾名。 デフォルトでは、サーバの CN は CXXX-YYYYYY 形式で表示されます（XXX はサーバのモデル番号で YYYYYY はシリアル番号です）。 最新バージョンにアップグレードするとき、CN はそのまま保持されます。
[Organization Name] フィールド	証明書を要求している組織。
[組織単位（Organization Unit）] フィールド	組織ユニット。
[地域（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。

名前	説明
[State Name] 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。
[Country Code] ドロップダウンリスト	会社が存在する国。
[Email] フィールド	会社の電子メールの連絡先。

要求された情報を入力すると、証明書署名要求が生成され、コンソール出力に表示されます。CSR ファイルは作成されませんが、コンソール出力から CSR 情報をコピーして、テキストファイルに貼り付けることができます。

例

次に、証明書署名要求を生成する例を示します。

```
Server# scope certificate
Server /certificate # generate-csr
Common Name (CN): test.example.com
Organization Name (O): Example, Inc.
Organization Unit (OU): Test Department
Locality (L): San Jose
StateName (S): CA
Country Code (CC): US
Email: user@example.com
Continue to generate CSR?[y|N]y


-----BEGIN CERTIFICATE REQUEST-----
MIIB/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
ZgAMivyCsKgb/6CjQtsofvzxmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
-----END CERTIFICATE REQUEST-----

Copy everything from "-----BEGIN ..."  to "END CERTIFICATE REQUEST-----",
paste to a file, send to your chosen CA for signing,
and finally upload the signed certificate via upload command.
              ---OR---
Continue to self sign CSR and overwrite the current certificate?
All HTTPS and SSH sessions will be disconnected. [y|N]N
```

次のタスク

次のいずれかの作業を実行します。

- 公共の認証局から証明書を取得せず、組織も独自の認証局を運用していない場合、CSR から自己署名証明書を内部生成し、すぐにサーバにアップロードするよう、Cisco IMC を設定できます。この処理を行うには、この例では最後のプロンプトの後に **y** と入力します。
- 組織が自己署名証明書を生成するための独自の証明書サーバを運用している場合は、「-----BEGIN ...」から「END CERTIFICATE REQUEST-----」までのコマンド出力をコピーして、csr.txt というファイルに貼り付けます。CSR ファイルを証明書サーバに入力して、自己署名証明書を生成します。
- 公共の認証局から証明書を取得する場合は、「-----BEGIN ...」から「END CERTIFICATE REQUEST-----」までのコマンド出力をコピーして、csr.txt というファイルに貼り付けます。CSR ファイルを認証局に提出して、署名付き証明書を取得します。
- 証明書のタイプが [サーバ（Server）] であることを確認します。

Cisco IMC によって自己署名証明書を内部生成し、アップロードする最初のオプションを使用しない場合は、証明書コマンドモードで **upload** コマンドを使用して新しい証明書をアップロードする必要があります。

信頼できない CA 署名付き証明書の作成

パブリック認証局（CA）を使用してサーバ証明書の生成と署名を行う代わりに、独自の CA を運用して独自の証明書に署名することができます。このセクションでは、Linux で実行されている OpenSSL 証明書サーバを使用して CA を作成するコマンドおよびサーバ証明書を生成するコマンドについて説明します。OpenSSL の詳細については、http://www.openssl.org を参照してください。

（注） これらのコマンドは、Cisco IMC ではなく、OpenSSL パッケージを使用している Linux サーバで入力します。

始める前に

- 組織内のサーバで、証明書サーバのソフトウェア パッケージを取得してインストールします。
- Cisco IMC の時刻が現在の時刻に設定されてい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	**openssl genrsa -out** *CA_keyfilename keysize* 例： `# openssl genrsa -out ca.key 2048`	このコマンドは、CA で使用される RSA 秘密キーを生成します。 （注） ユーザ入力なしで CA がキーにアクセスできるように、このコマンドに -des3 オプションは使用しないでください。 指定されたファイル名には、指定されたサイズの RSA キーが含まれています。
ステップ 2	**openssl req -new -x509 -days** *numdays* **-key** *CA_keyfilename* **-out** *CA_certfilename* 例： `# openssl req -new -x509 -days 365 -key ca.key -out ca.crt`	このコマンドは、指定されたキーを使用して、CA の自己署名証明書を新規に作成します。証明書は指定された期間有効になります。このコマンドは、ユーザに証明書の追加情報を求めるプロンプトを表示します。 証明書サーバは、アクティブな CA です。
ステップ 3	**echo "nsCertType = server" > openssl.conf** 例： `# echo "nsCertType = server" > openssl.conf`	このコマンドは、証明書がサーバ限定の証明書であることを指定する行を OpenSSL 設定ファイルに追加します。この指定により、認証されたクライアントがサーバになりすます man-in-the-middle 攻撃を防御できます。 OpenSSL 設定ファイル openssl.conf には、"nsCertType = server" という文が含まれています。
ステップ 4	**openssl x509 -req -days** *numdays* **-in** *CSR_filename* **-CA** *CA_certfilename* **-set_serial 04 -CAkey** *CA_keyfilename* **-out** *server_certfilename* **-extfile openssl.conf** 例： `# openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 04 -CAkey ca.key -out myserver05.crt -extfile openssl.conf`	このコマンドは、CA が CSR ファイルを使用してサーバ証明書を生成するように指示します。 サーバ証明書は、出力ファイルに含まれています。

	コマンドまたはアクション	目的
ステップ 5	**openssl x509 -noout -text -purpose -in <cert file>** 例： `openssl x509 -noout -text -purpose -in <cert file>`	生成された証明書のタイプが [Server] であることを確認します。 （注） フィールド [Server SSL] および [Netscape SSL] サーバの値が [Yes] でない場合は、タイプが [Server] の証明書を生成するように openssl.conf が設定されていることを確認します。
ステップ 6	（任意） 生成された証明書に正しい使用期限が設定されていない場合は、Cisco IMC の時刻が現在の時刻に設定されていることを確認し、ステップ 1 ～ 5 を繰り返して証明書を再生成します。	正しい使用期限が設定された証明書が作成されます。

例

この例は、CA の作成方法、および新規に作成された CA が署名するサーバ証明書の生成方法を示します。これらのコマンドは、OpenSSL を実行している Linux サーバで入力します。

```
# /usr/bin/openssl genrsa -out ca.key 2048 Generating RSA private key, 2048
bit long modulus .............++++++ .....++++++ e is 65537 (0x10001) #
/usr/bin/openssl req -new -x509 -days 365 -key ca.key -out ca.crt You are about
 to be asked to enter information that will be incorporated into your certificate
 request. What you are about to enter is what is called a Distinguished Name
or a DN. There are quite a few fields but you can leave some blank For some
fields there will be a default value, If you enter '.', the field will be left
 blank. ----- Country Name (2 letter code) [GB]:US State or Province Name (full
 name) [Berkshire]:California Locality Name (eg, city) [Newbury]:San Jose
Organization Name (eg, company) [My Company Ltd]:Example Incorporated
Organizational Unit Name (eg, section) []:Unit A Common Name (eg, your name or
 your server's hostname) []:example.com Email Address []:admin@example.com #
echo "nsCertType = server" > openssl.conf # /usr/bin/openssl x509 -req -days
365 -in csr.txt -CA ca.crt -set_serial 01 -CAkey ca.key -out server.crt -extfile
 openssl.conf Signature ok subject=/C=US/ST=California/L=San Jose/O=Example
Inc./OU=Unit A/CN=example.com/emailAddress=john@example.com Getting CA Private
 Key #
```

次のタスク

新しい証明書を Cisco IMC にアップロードします。

サーバ証明書のアップロード

始める前に

- 証明書をアップロードするには、admin 権限を持つユーザとしてログインする必要があります。
- アップロードする証明書は、読み取り可能テキストとして使用できる必要があります。アップロード手順で、証明書テキストをコピーして CLI に貼り付けます。
- 生成された証明書のタイプが [サーバ（Server）] であることを確認します。
- 次の証明書形式がサポートされています。
  - .crt
  - .cer
  - .pem

（注） 最初に、Cisco IMC 証明書管理 CSR の生成手順を使用して CSR を生成し、その CSR を使用してアップロード用の証明書を取得する必要があります。この方法で取得されていない証明書はアップロードしないでください。

（注） 新しいサーバ証明書がアップロードされると、現在の HTTPS および SSH セッションはすべて切断されます。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope certificate**	証明書コマンド モードを開始します。
ステップ 2	Server /certificate # **upload**	新しいサーバ証明書を入力してアップロードするためのダイアログが起動します。

プロンプトが表示されたら、証明書テキストをコピーしてコンソールに貼り付け、CTRL を押した状態で D を押して証明書をアップロードします。

例

次に、新しい証明書をサーバにアップロードする例を示します。

```
Server# scope certificate
Server /certificate # upload
Please paste your certificate here, when finished, press CTRL+D.
-----BEGIN CERTIFICATE-----
MIIB/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
ZgAMivyCsKgb/6CjQtsofvzxmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
-----END CERTIFICATE-----
<CTRL+D>
```

キー管理相互運用性プロトコル

キー管理相互運用性プロトコル（KMIP）は、主要な管理サーバでキーまたは機密データを処理するためのメッセージ形式を定義する通信プロトコルです。KMIP はオープン スタンダードで、複数のベンダーによってサポートされています。キー管理には、複数の相互運用可能な実装が伴うため、KMIP クライアントは KMIP サーバと効率的に連動します。

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、発信データを復号するハードウェアが含まれています。ドライブまたはメディア暗号化キーは、この機能を制御します。しかし、セキュリティを維持するために、ドライブはロックされている必要があります。セキュリティ キー ID とセキュリティ キー（キー暗号キー）を使用すると、この目的を達成できます。キー ID では、ドライブに一意の ID が提供されます。

異なるキーには異なる使用要件があります。現在、ローカル キーの管理および追跡の責任は主にユーザにあるため、人的ミスが生じる可能性があります。ユーザはさまざまなキーとそれらの機能を覚えている必要があり、それが困難な場合があります。KMIP は、この懸念領域に対処し、人的関与なしでキーを効率的に管理します。

KMIP の有効化または無効化

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope kmip**	KMIP コマンド 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	Server/kmip# **set enabled {yes | no}**	KMIP をイネーブルまたはディセーブルにします。
ステップ 3	Server/kmip*# **commit**	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 4	（任意） Server/kmip # **show detail**	KMIP ステータスを表示します。

例

次に KMIP を有効にする例を示します。

```
Server # scope kmip
Server /kmip # set enabled yes
Server /kmip *# commit
Server /kmip # show detail
  Enabled: yes
Server /kmip #
```

KMIP 設定のクライアント秘密キーおよびクライアント証明書の作成

パブリック認証局（CA）を使用してサーバ証明書の生成と署名を行う代わりに、独自の CA を運用して独自の証明書に署名することができます。このセクションでは、Linux で実行されている OpenSSL 証明書サーバを使用して CA を作成するコマンドおよびサーバ証明書を生成するコマンドについて説明します。OpenSSL の詳細については、http://www.openssl.org を参照してください。

（注） これらのコマンドは、Cisco IMC ではなく、OpenSSL パッケージを使用している Linux サーバで入力します。

始める前に

- 組織内のサーバで、証明書サーバのソフトウェアパッケージを取得してインストールします。
- Cisco IMC の時刻が現在の時刻に設定されてい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	**openssl genrsa -out** *Client_Privatekeyfilename keysize* 例：	このコマンドは、クライアント証明書の生成に使用されるクライアント秘密キーを生成します。

	コマンドまたはアクション	目的
	`# openssl genrsa -out client_private.pem 2048`	指定されたファイル名には、指定されたサイズの RSA キーが含まれています。
ステップ 2	**openssl req -new -x509 -days** *numdays* **-key** *Client_Privatekeyfilename* **-out** *Client_certfilename* 例： `# openssl req -new -x509 -key client_private.pem -out client.pem -days 365`	このコマンドは、前の手順で入手したクライアント秘密キーを使用して、新しい自己署名クライアント証明書を生成します。証明書は指定された期間有効になります。このコマンドは、ユーザに証明書の追加情報を求めるプロンプトを表示します。 新しい自己署名クライアント証明書が作成されます。
ステップ 3	KMIP サーバから KMIP ルート CA 証明書を取得します。	ルート CA 証明書の取得については、KMIP のベンダー マニュアルを参照してください。

次のタスク

新しい証明書を Cisco IMC にアップロードします。

KMIP クライアント証明書のダウンロード

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope kmip**	KMIP コマンド モードを開始します。
ステップ 2	Server/kmip # **set enabled yes**	KMIP を有効にします。
ステップ 3	Server/kmip*# **commit**	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 4	Server/kmip # **scope kmip-client-certificate**	KMIP クライアント証明書コマンド モードを開始します。
ステップ 5	Server /kmip/kmip-client-certificate # **download-client-certificate** *remote-protocol IP アドレス KMIP クライアント証明書ファイル*	リモート サーバに接続するためのプロトコルを指定します。次のいずれかのタイプを指定できます。 • TFTP

	コマンドまたはアクション	目的
		• FTP • SFTP • SCP • HTTP （注） Cisco UCS C シリーズ サーバでは、リモート サーバからファームウェアを更新したときの、サーバのフィンガープリントの確認をサポートするようになりました。このオプションは、リモート サーバ タイプとして SCP または SFTP を選択した場合にのみ使用できます。 このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue?」というメッセージが表示されます。サーバ フィンガープリントの信頼性に応じて、[y] または [n] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。
ステップ 6	確認プロンプトで、**y** と入力します。	これにより KMIP クライアント証明書のダウンロードが開始されます。
ステップ 7	（任意） Server /kmip/kmip-client-certificate # **paste-client-certificate**	プロンプトで、署名付き証明書の内容を貼り付け、**Ctrl+D** を押します。 （注） 前の手順のリモート サーバ メソッドを使用するか、貼り付けオプションを使用して、クライアント証明書をダウンロードできます。

例

この例は、KMIP クライアント証明書をダウンロードします。

```
Server # scope kmip
Server /kmip # set enabled yes
Server /kmip *# commit
Server /kmip # scope kmip-client-certificate
Server /kmip/kmip-client-certificate # show detail
    KMIP client certificate Available: 1
    Download client certificate Status: COMPLETED
    Export client certificate Status: NONE
Server /kmip/kmip-client-certificate #  download-client-certificate tftp 10.10.10.10
KmipCertificates/
svbu-xx-blr-dn1-13_ClientCert.pem
  You are going to overwrite the KMIP client certificate.
  Are you sure you want to proceed and overwrite the KMIP client certificate? [y|N]y
KMIP client certificate downloaded successfully

You can  either use the remote server method from the previous steps or use the paste
option to download the client certificate.

Server /kmip/kmip-client-certificate # paste-client-certificate
Please paste your certificate here, when finished, press CTRL+D.
----BEGIN CERTIFICATE-----
MIIDTzCCAjegAwIBAgIQXuWPdBbyTb5M7/FT8aAjZTANBgkqhkiG9w0BAQUFADA6
MRMwEQYKCZImiZPyLGQBGRYDY29tMRMwEQYKCZImiZPyLGQBGRYDbmV3MQ4wDAYD
VQQDEwVuZXdDQTAeFw0xNTAzMTIxMTM5MTZaFw0yMDAzMTIxMTQ5MTVaMDoxEzAR
BgoJkiaJk/IsZAEZFgNjb20xEzARBgoJkiaJk/IsZAEZFgNuZXcxDjAMBgNVBAMT
BW5ld0NBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuPSAwHtk0IbM
Cd5tYdCa498bfX5Nfdgnq5zE+cGIOqv0dAkucofC/Y0+m7hne9H12aQ9SqTOK1+L
5IT3PVCczhasI7L7jAa+Oe5AOYw7Nsugw5Bd23n42BTVMMp7xsgr1mVfFoHXbBkQ
wiT9DieyImSyGiq5n0/8Iooc0iN5WPMVcHO2ysz76jR8p07xRqgYNCl6cbKAhWfZ
oYIwjhpZv0+SXEs8sEJZKDUhWIfOIpnDL7MoZYgl/kymgs/0hsW4L338jy303c7T
TwnG2/7BOMK0YFkEhqcjlkamGP7MKB2T9e/Cug6VkvFSkkim8M1eHx1gEnQxRtAG
YGp1n55iHQIDAQABo1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAd
BgNVHQ4EFgQUl2F3U7cggzCuvRWliZWg91n5lccwEAYJKwYBBAGCNxUBBAMCAQAw
DQYJKoZIhvcNAQEFBQADggEBAJXoJJDDB3QH0q8VY8G/oC1SkAwyOE1dH0NdxFES
tNqQMTaRB2Sb2L/ZzAtfIaZ0Xab9Ig4MqNIMBbHDCwlzhD5gX42GPYWhA/GjRj3O
Q5KcRaEFomxp+twRrJ25ScVSczKJaRonWqKDVL9TwoSuDar3ObiS9ZC0KuBBf0vu
dzrJEYY/1zz7WVPZVyevhba3VSt4LW75URTqOKBSuKO+fvGyyNHWvMPFEIEnJAKt
7QmhO2fiWhD8CxaPFIByqkvrJ96no6oBxdEcjm9n1MttF/UJcpypSPH+46mRn5Az
SzgCBftYNjBPLcwbZGJkF/GpPwjd0TclMM08UOdqiTxR7Ts=
-----END CERTIFICATE-----
  You are going to overwrite the KMIP Client Certificate.
  Are you sure you want to proceed and overwrite the KMIP Client Certificate? [y|N]
y
Server /kmip/kmip-client-certificate #
```

KMIP クライアント証明書のエクスポート

始める前に

- このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

- KMIP クライアント証明書をエクスポートするには、証明書がダウンロードされ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	Server# **scope kmip**	KMIP コマンド モードを開始します。
ステップ 2	Server /kmip # **scope kmip-client-certificate**	KMIP クライアント証明書コマンドモードを開始します。
ステップ 3	Server /kmip/kmip-client-certificate # **export-client-certificate** *remote-protocol IP アドレス KMIP ルート CA 証明書ファイル*	リモート サーバに接続するためのプロトコルを指定します。次のいずれかのタイプを指定できます。 • TFTP • FTP • SFTP • SCP • HTTP

	コマンドまたはアクション	目的
		（注） Cisco UCS C シリーズ サーバでは、リモート サーバからファームウェアを更新したときの、サーバのフィンガープリントの確認をサポートするようになりました。このオプションは、リモートサーバタイプとして SCP または SFTP を選択した場合にのみ使用できます。 このアクションを実行しながら、リモートサーバタイプとして SCP または SFTP を選択した場合、「Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue?」というメッセージが表示されます。サーバ フィンガープリントの信頼性に応じて、[y] または [n] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。 証明書のエクスポートを開始します。
ステップ 4	（任意） Server /kmip/kmip-client-certificate # **show detail**	証明書のエクスポートのステータスを表示します。

例

この例は、KMIP クライアント証明書をエクスポートします。

```
Server # scope kmip
Server /kmip # scope kmip-client-certificate
Server /kmip/kmip-client-certificate #  export-client-certificate ftp 10.10.10.10
/TFTP_DIR/KmipCertificates
/svbu-xx-blr-dn1-13_ClientCert.pem_exported_ftp
Username: username
Password:
KMIP Client Certificate exported successfully
Server /kmip/kmip-client-certificate # show detail
    KMIP Client Certificate Available: 1
    Download KMIP Client Certificate Status: COMPLETED
    Export KMIP Client Certificate Status: COMPLETED
Server /kmip/kmip-client-certificate #
```

KMIP クライアント証明書の削除

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope kmip**	KMIP コマンド モードを開始します。
ステップ 2	Server# /kmip **scope kmip-client-certificate**	KMIP クライアント証明書バインド コマンド モードを開始します。
ステップ 3	Server /kmip/kmip-client-certificate # **delete-client-certificate**	確認のプロンプトが表示されます。
ステップ 4	確認プロンプトで、**y** と入力します。	これで KMIP クライアント証明書が削除されます。

例

この例は、KMIP クライアント証明書を削除します。

```
Server # scope kmip
Server /kmip # scope kmip-client-certificate
Server /kmip/kmip-client-certificate # delete-client-certificate
  You are going to delete the KMIP Client Certificate.
  Are you sure you want to proceed and delete the KMIP Client Certificate? [y|N]y
 KMIP Client Certificate deleted successfully.
```

KMIP ルート CA 証明書のダウンロード

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope kmip**	KMIP コマンド モードを開始します。
ステップ 2	Server/kmip # **set enabled yes**	KMIP を有効にします。
ステップ 3	Server/kmip * # **commit**	トランザクションをシステムの設定にコミットします。

	コマンドまたはアクション	目的
ステップ 4	Server /kmip # **scope kmip-root-ca-certificate**	KMIP ルート CA 証明書のコマンド モードを開始します。
ステップ 5	Server /kmip/kmip-root-ca-certificate # **download-root-ca-certificate** *remote-protocol IP* アドレス *KMIP CA* 証明書ファイル	リモート サーバに接続するためのプロトコルを指定します。次のいずれかのタイプを指定できます。 • TFTP • FTP • SFTP • SCP • HTTP （注） Cisco UCS C シリーズ サーバでは、リモート サーバからファームウェアを更新したときの、サーバのフィンガープリントの確認をサポートするようになりました。このオプションは、リモート サーバ タイプとして SCP または SFTP を選択した場合にのみ使用できます。 このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」というメッセージが表示されます。サーバ フィンガープリントの信頼性に応じて、[y] または [n] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。
ステップ 6	確認プロンプトで、**y** と入力します。	これにより KMIP ルート CA 証明書のダウンロードが開始されます。

	コマンドまたはアクション	目的
ステップ 7	（任意） Server /kmip/kmip-root-ca-certificate # **paste-root-ca-certificate**	プロンプトで、ルートCA証明書の内容を貼り付け、**Ctrl+D** を押します。 （注） 前の手順のリモートサーバメソッドを使用するか、貼り付けオプションを使用して、ルートCA証明書をダウンロードできます。

例

この例は、KMIP ルート CA 証明書をダウンロードします。

```
Server # scope kmip
Server /kmip # set enabled yes
Server /kmip *# commit
Server /kmip # scope kmip-root-ca-certificate
Server /kmip/kmip-root-ca-certificate # show detail
    KMIP Root CA Certificate Available: 1
    Download Root CA Certificate Status: COMPLETED
    Export Root CA Certificate Status: NONE
Server /kmip/kmip-root-ca-certificate # download-root-ca-certificate tftp 10.10.10.10
KmipCertificates/
svbu-xx-blr-dn1-13_ServerCert.pem
  You are going to overwrite the KMIP Root CA Certificate.
  Are you sure you want to proceed and overwrite the KMIP Root CA Certificate? [y|N]y
KMIP Root CA Certificate downloaded successfully

You can  either use the remote server method from the previous steps or use the paste
option to download the client certificate.

Server /kmip/kmip-root-ca-certificate # paste-root-ca-certificate
Please paste your certificate here, when finished, press CTRL+D.
----BEGIN CERTIFICATE-----
MIIDTzCCAjegAwIBAgIQXuWPdBbyTb5M7/FT8aAjZTANBgkqhkiG9w0BAQUFADA6
MRMwEQYKCZImiZPyLGQBGRYDY29tMRMwEQYKCZImiZPyLGQBGRYDbmV3MQ4wDAYD
VQQDEwVuZXdDQTAeFw0xNTAzMTIxMTM5MTZaFw0yMDAzMTIxMTQ5MTVaMDoxEzAR
BgoJkiaJk/IsZAEZFgNjb20xEzARBgoJkiaJk/IsZAEZFgNuZXcxDjAMBgNVBAMT
BW5ld0NBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuPSAwHtk0IbM
Cd5tYdCa498bfX5Nfdgnq5zE+cGIOqv0dAkucofC/Y0+m7hne9H12aQ9SqTOK1+L
5IT3PVCczhasI7L7jAa+Oe5AOYw7Nsugw5Bd23n42BTVMMp7xsgr1mVfFoHXbBkQ
wiT9DieyImSyGiq5n0/8Iooc0iN5WPMVcHO2ysz76jR8p07xRqgYNCl6cbKAhWfZ
oYIwjhpZv0+SXEs8sEJZKDUhWIfOIpnDL7MoZYgl/kymgs/0hsW4L338jy303c7T
TwnG2/7BOMK0YFkEhqcjlkamGP7MKB2T9e/Cug6VkvFSkkim8M1eHx1gEnQxRtAG
YGp1n55iHQIDAQABo1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAd
BgNVHQ4EFgQUl2F3U7cggzCuvRWliZWg91n5lccwEAYJKwYBBAGCNxUBBAMCAQAw
DQYJKoZIhvcNAQEFBQADggEBAJXoJJDDB3QH0q8VY8G/oC1SkAwyOE1dH0NdxFES
tNqQMTaRB2Sb2L/ZzAtfIaZ0Xab9Ig4MqNIMBbHDCwlzhD5gX42GPYWhA/GjRj3O
Q5KcRaEFomxp+twRrJ25ScVSczKJaRonWqKDVL9TwoSuDar3ObiS9ZC0KuBBf0vu
dzrJEYY/1zz7WVPZVyevhba3VSt4LW75URTqOKBSuKO+fvGyyNHWvMPFEIEnJAKt
7QmhO2fiWhD8CxaPFIByqkvrJ96no6oBxdEcjm9n1MttF/UJcpypSPH+46mRn5Az
SzgCBftYNjBPLcwbZGJkF/GpPwjd0TclMM08UOdqiTxR7Ts=
-----END CERTIFICATE-----
  You are going to overwrite the KMIP Root CA Certificate.
  Are you sure you want to proceed and overwrite the KMIP Root CA Certificate? [y|N]
```

```
y
Server /kmip/kmip-root-ca-certificate #
```

KMIP ルート CA 証明書のエクスポート

始める前に

- このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。
- KMIP ルート CA 証明書をエクスポートするには、証明書がダウンロードされ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	Server # **scope kmip**	KMIP コマンド モードを開始します。
ステップ 2	Server /kmip # **scope kmip-root-ca-certificate**	KMIP ルート CA 証明書のコマンド モードを開始します。
ステップ 3	Server /kmip/kmip-root-ca-certificate # **export-root-ca-certificate** *remote-protocol IP アドレス KMIP ルート CA 証明書ファイル*	リモート サーバに接続するためのプロトコルを指定します。次のいずれかのタイプを指定できます。 • TFTP • FTP • SFTP • SCP • HTTP

	コマンドまたはアクション	目的
		（注） Cisco UCS C シリーズ サーバでは、リモート サーバからファームウェアを更新したときの、サーバのフィンガープリントの確認をサポートするようになりました。このオプションは、リモートサーバタイプとして SCP または SFTP を選択した場合にのみ使用できます。 このアクションを実行しながら、リモートサーバタイプとして SCP または SFTP を選択した場合、「Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue?」というメッセージが表示されます。サーバ フィンガープリントの信頼性に応じて、[y] または [n] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。 証明書のエクスポートを開始します。
ステップ 4	（任意） Server /kmip/kmip-root-ca-certificate # **show detail**	証明書のエクスポートのステータスを表示します。

例

この例は、KMIP ルート CA 証明書をエクスポートします。

```
Server # scope kmip
Server /kmip # scope kmip-root-ca-certificate
Server /kmip/kmip-root-ca-certificate #  export-root-ca-certificate tftp 10.10.10.10
KmipCertificates/
svbu-xx-blr-dn1-13_ServerCert.pem_exported_tftp
KMIP Root CA Certificate exported successfully
Server /kmip/kmip-root-ca-certificate # show detail
    KMIP Root CA Certificate Available: 1
    Download Root CA Certificate Status: COMPLETED
    Export Root CA Certificate Status: COMPLETED
Server /kmip/kmip-root-ca-certificate #
```

KMIP ルート CA 証明書の削除

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope kmip**	KMIP コマンド モードを開始します。
ステップ 2	Server# /kmip **scope kmip-root-ca-certificate**	KMIP ルート CA 証明書バインド コマンド モードを開始します。
ステップ 3	Server /kmip/kmip-root-ca-certificate # **delete-root-ca-certificate**	確認のプロンプトが表示されます。
ステップ 4	確認プロンプトで、**y** と入力します。	これで KMIP ルート CA 証明書が削除されます。

例

この例は、KMIP ルート CA 証明書を削除します。

```
Server # scope kmip
Server /kmip # scope kmip-root-ca-certificate
Server /kmip/kmip-root-ca-certificate # delete-root-ca-certificate
  You are going to delete the KMIP root CA certificate.
  Are you sure you want to proceed and delete the KMIP root CA certificate? [y|N]y
 KMIP root CA certificate deleted successfully.
```

KMIP クライアント秘密キーのダウンロード

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope kmip**	KMIP コマンド モードを開始します。
ステップ 2	Server/kmip# **set enabled yes**	KMIP を有効にします。
ステップ 3	Server/kmip*# **commit**	トランザクションをシステムの設定にコミットします。

	コマンドまたはアクション	目的
ステップ 4	Server/kmip # **scope kmip-client-private-key**	KMIP クライアント秘密キー コマンド モードを開始します。
ステップ 5	Server /kmip/kmip-client-private-key # **download-client-pvt-key** *remote-protocol IP アドレス KMIP クライアント秘密キー ファイル*	リモート サーバに接続するためのプロトコルを指定します。次のいずれかのタイプを指定できます。 • TFTP • FTP • SFTP • SCP • HTTP （注） Cisco UCS C シリーズ サーバでは、リモート サーバからファームウェアを更新したときの、サーバのフィンガープリントの確認をサポートするようになりました。このオプションは、リモート サーバ タイプとして SCP または SFTP を選択した場合にのみ使用できます。 このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」というメッセージが表示されます。サーバ フィンガープリントの信頼性に応じて、[y] または [n] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。
ステップ 6	確認プロンプトで、**y** と入力します。	これにより KMIP クライアント秘密キーのダウンロードが開始されます。

	コマンドまたはアクション	目的
ステップ 7	（任意） Server /kmip/kmip-client-private-key # **paste-client-pvt-key**	プロンプトで、秘密キーの内容を貼り付け、**Ctrl+D** を押します。 （注） 前の手順のリモート サーバ メソッドを使用するか、貼り付けオプションを使用して、クライアント秘密キーをダウンロードできます。

例

この例は、KMIP クライアント秘密キーをダウンロードします。

```
Server # scope kmip
Server /kmip # set enabled yes
Server /kmip *# commit
Server /kmip # scope kmip-client-private-key
Server /kmip/kmip-client-private-key # show detail
    KMIP Client Private Key Available: 1
    Download Client Private Key Status: COMPLETED
    Export Client Private Key Status: NONE
Server /kmip/kmip-client-private-key #  download-client-pvt-key tftp 10.10.10.10
KmipCertificates/
svbu-xx-blr-dn1-13_ClientPvtKey.pem
  You are going to overwrite the KMIP Client Private Key.
  Are you sure you want to proceed and overwrite the KMIP Client Private Key? [y|N]y
KMIP Client Private Key downloaded successfully

You can  either use the remote server method from the previous steps or use the paste
option to download the client certificate.

Server /kmip/kmip-client-private-key # paste-client-pvt-key
Please paste your client private here, when finished, press CTRL+D.
----BEGIN CERTIFICATE-----
MIIDTzCCAjegAwIBAgIQXuWPdBbyTb5M7/FT8aAjZTANBgkqhkiG9w0BAQUFADA6
MRMwEQYKCZImiZPyLGQBGRYDY29tMRMwEQYKCZImiZPyLGQBGRYDbmV3MQ4wDAYD
VQQDEwVuZXdDQTAeFw0xNTAzMTIxMTM5MTZaFw0yMDAzMTIxMTQ5MTVaMDoxEzAR
BgoJkiaJk/IsZAEZFgNjb20xEzARBgoJkiaJk/IsZAEZFgNuZXcxDjAMBgNVBAMT
BW5ld0NBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAuPSAwHtk0IbM
Cd5tYdCa498bfX5Nfdgnq5zE+cGIOqv0dAkucofC/Y0+m7hne9H12aQ9SqTOK1+L
5IT3PVCczhasI7L7jAa+Oe5AOYw7Nsugw5Bd23n42BTVMMp7xsgr1mVfFoHXbBkQ
wiT9DieyImSyGiq5n0/8Iooc0iN5WPMVcHO2ysz76jR8p07xRqgYNCl6cbKAhWfZ
oYIwjhpZv0+SXEs8sEJZKDUhWIfOIpnDL7MoZYgl/kymgs/0hsW4L338jy303c7T
TwnG2/7BOMK0YFkEhqcjlkamGP7MKB2T9e/Cug6VkvFSkkim8M1eHx1gEnQxRtAG
YGp1n55iHQIDAQABo1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAd
BgNVHQ4EFgQUl2F3U7cggzCuvRWliZWg91n5lccwEAYJKwYBBAGCNxUBBAMCAQAw
DQYJKoZIhvcNAQEFBQADggEBAJXoJJDDB3QH0q8VY8G/oC1SkAwyOE1dH0NdxFES
tNqQMTaRB2Sb2L/ZzAtfIaZ0Xab9Ig4MqNIMBbHDCwlzhD5gX42GPYWhA/GjRj3O
Q5KcRaEFomxp+twRrJ25ScVSczKJaRonWqKDVL9TwoSuDar3ObiS9ZC0KuBBf0vu
dzrJEYY/1zz7WVPZVyevhba3VSt4LW75URTqOKBSuKO+fvGyyNHWvMPFEIEnJAKt
7QmhO2fiWhD8CxaPFIByqkvrJ96no6oBxdEcjm9n1MttF/UJcpypSPH+46mRn5Az
SzgCBftYNjBPLcwbZGJkF/GpPwjd0TclMM08UOdqiTxR7Ts=
-----END CERTIFICATE-----
  You are going to overwrite the KMIP client private key.
  Are you sure you want to proceed and overwrite the KMIP Client Private Key? [y|N]
```

```
y
Server /kmip/kmip-client-private-key #
```

KMIP クライアント秘密キーのエクスポート

始める前に

- このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。
- KMIP クライアントの秘密キーをエクスポートするには、秘密キーがダウンロードされ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	Server# **scope kmip**	KMIP コマンド モードを開始します。
ステップ 2	Server /kmip # **scope kmip-client-private-key**	KMIP クライアント秘密キー コマンド モードを開始します。
ステップ 3	Server /kmip/kmip-client-private-key # **export-client-pvt-key** *remote-protocol IP アドレス KMIP ルート CA 証明書ファイル*	リモート サーバに接続するためのプロトコルを指定します。次のいずれかのタイプを指定できます。 • TFTP • FTP • SFTP • SCP • HTTP

	コマンドまたはアクション	目的
		（注） Cisco UCS C シリーズ サーバでは、リモート サーバからファームウェアを更新したときの、サーバのフィンガープリントの確認をサポートするようになりました。このオプションは、リモート サーバ タイプとして SCP または SFTP を選択した場合にのみ使用できます。 このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「Server (RSA) key fingerprint is <server_finger_print_ID> Do you wish to continue?」というメッセージが表示されます。サーバ フィンガープリントの信頼性に応じて、[y] または [n] をクリックします。 フィンガープリントはホストの公開キーに基づいており、接続先のホストを識別または確認できます。 証明書のエクスポートを開始します。
ステップ 4	（任意） Server /kmip/kmip-client-private-key # **show detail**	証明書のエクスポートのステータスを表示します。

例

この例は、KMIP クライアントの秘密キーをエクスポートします。

```
Server # scope kmip
Server /kmip # scope kmip-client-private-key
Server /kmip/kmip-client-private-key #  export-client-pvt-key tftp 10.10.10.10
KmipCertificates
/svbu-xx-blr-dn1-13_ClientPvtKey.pem_exported_tftp
KMIP Client Private Key exported successfully
Server /kmip/kmip-client-private-key # show detail
    KMIP Client Private Key Available: 1
    Download Client Private Key Status: COMPLETED
    Export Client Private Key Status: COMPLETED
Server /kmip/kmip-client-private-key #
```

KMIP クライアント秘密キーの削除

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope kmip**	KMIP コマンド モードを開始します。
ステップ 2	Server# /kmip **scope kmip-client-private-key**	KMIP クライアント秘密キー バインド コマンド モードを開始します。
ステップ 3	Server /kmip/kmip-client-private-key # **delete-client-pvt-key**	確認のプロンプトが表示されます。
ステップ 4	確認プロンプトで、**y** と入力します。	これでKMIPクライアントの秘密キーが削除されます。

例

この例は、KMIP クライアントの秘密キーを削除します。

```
Server # scope kmip
Server /kmip # scope kmip-client-private-key
Server /kmip/kmip-client-private-key # delete-client-pvt-key
  You are going to delete the KMIP client private key.
  Are you sure you want to proceed and delete the KMIP client private key? [y|N]y
 KMIP client private key deleted successfully.
```

KMIP サーバ ログインの資格情報の構成

この手順では、KMIP サーバのログイン資格情報を設定し、KMIP サーバのログイン資格情報をメッセージ認証に必須にする方法を示しています。

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope kmip**	KMIP コマンド モードを開始します。
ステップ 2	Server /kmip # **scope kmip-login**	KMIP ログイン コマンド 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	Server/kmip/kmip-login # **set login** *username*	KMIP サーバのユーザ名を設定します。
ステップ 4	Server/kmip/kmip-login * # **set password**	プロンプトでパスワードを入力し、パスワードの確認プロンプトで再度同じパスワードを入力します。これでKMIP サーバのパスワードが設定されます。
ステップ 5	Server/kmip/kmip-login * # **set use-kmip-cred** {**yes** | **no**}	KMIP サーバのログイン資格情報をメッセージ認証に必須にするかどうかを決定します。
ステップ 6	Server/kmip/kmip-login * # **commit**	トランザクションをシステム設定にコミットします。
ステップ 7	（任意） Server/kmip/kmip-login # **restore**	KMIP の設定をデフォルトに戻します。

例

次に、KMIP サーバの資格情報を設定する例を示します。

```
Server /kmip # scope kmip-login
Server /kmip/kmip-login # set login username
Server /kmip/kmip-login *# set password
Please enter password:
Please confirm password:
Server /kmip/kmip-login *# set use-kmip-cred yes
Server /kmip/kmip-login *# commit
Server /kmip/kmip-login # show detail
    Use KMIP Login: yes
    Login name to KMIP server: username
    Password to KMIP server: ******

You can restore the KMIP server credentials to default settings by preforming the following
 step:

Server /kmip/kmip-login # restore
Are you sure you want to restore KMIP settings to defaults?
Please enter 'yes' to confirm: yes
Restored factory-default configuration.
Server /kmip/kmip-login # show detail
    Use KMIP Login: no
    Login name to KMIP server:
    Password to KMIP server: ******
Server /kmip/kmip-login #
```

KMIP サーバ プロパティの構成

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope kmip**	KMIP コマンド モードを開始します。
ステップ 2	Server /kmip # **scope kmip-server** サーバ *ID*	選択した KMIP サーバのコマンド モードを開始します。
ステップ 3	Server /kmip/kmip-server # **set** *kmip-port*	KMIP ポートを設定します。
ステップ 4	Server /kmip/kmip-server *# **set** *kmip-server*	KMIP サーバ ID を設定します。
ステップ 5	Server /kmip/kmip-server # **set** *kmip-timeout*	KMIP サーバのタイムアウトを設定します。
ステップ 6	Server /kmip/kmip-server # **commit**	トランザクションをシステム設定にコミットします。
ステップ 7	（任意） Server /kmip/kmip-server # **show detail**	KMIP サーバの詳細を表示します。

例

次に、KMIP サーバの接続をテストする例を示します。

```
Server # scope kmip
Server /kmip # scope kmip-server 1
Server /kmip/kmip-server # set kmip-port  5696
Server /kmip/kmip-server * # set kmip-server  kmipserver.com
Server /kmip/kmip-server * # set kmip-timeout  10
Server /kmip/kmip-server * # commit
Server /kmip/kmip-server # show detail
Server number 1:
    Server domain name or IP address: kmipserver.com
    Port: 5696
    Timeout: 10
Server /kmip/kmip-server #
```

Cisco IMC での FIPS 140-2 の準拠

Federal Information Processing Standard（FIPS）パブリケーション 140-2 は、暗号モジュールの認定に使用される米国政府のコンピュータ セキュリティ標準です3.1(3) リリースでは、ラック Cisco IMC は NIST ガイドラインに従った FIPS 対応ではありません。これは FIPS 140-2 で承認された暗号化アルゴリズムとモジュールに従っていません。このリリースで、すべての CIMC サービスは、Cisco FIPS オブジェクト モジュール（FOM）を使用します。これにより、FIPS 140-2 に準拠した暗号化モジュールが提供されます。

Cisco FIPS オブジェクト モジュールは、Cisco の広範なネットワー キング製品およびコラボレーション製品に暗号化サービスを提供するソフトウェア ライブラリです。モジュールは、IPSec（IKE）、SRTP、SSH、TLS、SNMP などのサービスに対して、FIPS 140 の検証済みの暗号化アルゴリズムと KDF 機能を提供します。

セキュリティ設定の有効化

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server # **scope cimc**	Cisco IMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope security-configuration**	セキュリティの設定コマンド モードを開始します。
ステップ 3	Server /chassis/security-configuration # **set fips enabled**または**disabled**	有効になっている場合は、FIPS を有効にします。
ステップ 4	Server /chassis/security-configuration* # **commit**	FIPS を有効にして、システムにトランザクションをコミットする警告プロンプトで **y** を入力します。 （注） FIPS モードを切り替えると、SSH、KVM、SNMP、web サーバ、XMLAPI、および redfish サービスが再起動されます。

	コマンドまたはアクション	目的
		（注） FIPS、または FIPS と CC の両方を有効にすると、次の SNMP 設定の変更が発生します。 • **noAuthNoPriv** または **authNoPriv** セキュリティ レベル オプションに設定されている SNMPv2 プロトコルおよび SNMPv3 ユーザーのコミュニティ ストリング設定が無効になります。 • [NoAuthNoPriv] のセキュリティ レベル オプションが指定された SNMPv2 または SNMPv3 ユーザ向けに設定されたトラップが無効になります。 • [MD5] および [DES] 認証タイプおよびプライバシー タイプが無効になります。 • また、SSH、Webサーバ、KVM 接続で FIPS 準拠の暗号方式のみが使用されるようになります。
ステップ 5	Server /chassis/security-configuration # **set cc enabled**または**disabled**	（注） FIPS は、CC を有効にする有効な状態である必要があります。 有効にすることを選択すると、CC が有効になります。
ステップ 6	Server /chassis/security-configuration* # **commit**	FIPS を有効にして、システムにトランザクションをコミットする警告プロンプトで **y** を入力します。 （注） FIPS モードを切り替えると、SSH、KVM、SNMP、web サーバ、XMLAPI、および redfish サービスが再起動されます。

	コマンドまたはアクション	目的
		（注） FIPS、または FIPS と CC の両方を有効にすると、次の SNMP 設定の変更が発生します。 • **noAuthNoPriv** または **authNoPriv** セキュリティ レベル オプションに設定されている SNMPv2 プロトコルおよび SNMPv3 ユーザーのコミュニティ ストリング設定が無効になります。 • [NoAuthNoPriv] のセキュリティ レベル オプションが指定された SNMPv2 または SNMPv3 ユーザ向けに設定されたトラップが無効になります。 • [MD5] および [DES] 認証タイプおよびプライバシー タイプが無効になります。 • また、SSH、Webサーバ、KVM 接続で FIPS 準拠の暗号方式のみが使用されるようになります。

例

この例は、コントローラ情報を表示する方法を示します。

```
Server# scope cimc
Server /cimc # scope security-configuration
Server /cimc/security-configuration # set fips enabled
Enabling FIPS would
1. Disables support for SNMP V2 and V3 with No 'Auth/Priv' security level.
2. Disables support for 'MD5/DES' crypto algorithms in SNMP 'Auth/Priv' keys.
3. Ensures use of only FIPS-compliant ciphers in SSH, webserver and KVM connections.
Server /cimc/security-configuration* # commit
Server/cimc/security-configuration # set cc enabled
Enabling Common Criteria
Server /cimc/security-configuration* # commit
Warning: changing "fips" or "CC" will restart SSH, KVM, SNMP, webserver, XMLAPI and
redfish services.
```

```
Do you wish to continue? [y/N] y
Server /cimc/security-configuration #
```