Managing Certificates and Server Security

This chapter includes the following sections:

Managing Server Certificates

The examples in this section show how to use the Cisco IMC XML API to manage server certificates. Each example shows the XML API request followed by the response from Cisco IMC.

This section includes the following examples:

Retrieving Certificate Details

Request:

```
<configResolveClass cookie="1448761796/eb8a8234-25a4-15a4-8002-9a6ae7925a88"
classId="currentCertificate" inHierarchical="false"></configResolveClass>
```

Response:

```
<configResolveClass cookie="1448761796/eb8a8234-25a4-15a4-8002-9a6ae7925a88"
response="yes" classId="currentCertificate">
 <outConfigs>
  <currentCertificate dn="sys/cert-mgmt/curr-cert" serialNumber="C764DC592E154539"
   countryCode="US" state="California" locality="San Jose" organization="cisco"
   organizationalUnit="cisco" commonName="cisco" issuerCountryCode="US"
   issuerState="California" issuerLocality="San Jose" issuerOrganization="cisco"
   issuerOrganizationalUnit="cisco" issuerCommonName="cisco"
   validFrom="Nov 20 05:11:22 2015 GMT" validTo="Nov 17 05:11:22 2025 GMT"/>
```

```
  </outConfigs>
</configResolveClass>
```

Generating Certificate Signing Request

Request:

```
<configConfMo cookie='1448761796/eb8a8234-25a4-15a4-8002-9a6ae7925a88'
dn="sys/cert-mgmt/gen-csr-req" inHierarchical="false">
 <inConfig>
  <generateCertificateSigningRequest commonName="cisco" organization="cisco"
   organizationalUnit="cisco" locality="San Jose" state="California" countryCode="United
States"
   protocol="ftp" remoteServer="10.10.10.10" user="user" pwd="cisco123"
   remoteFile="/tmp/host.csr" dn="sys/cert-mgmt/gen-csr-req"/>
 </inConfig>
</configConfMo>
```

Response:

```
<configResolveClass cookie="1448761796/eb8a8234-25a4-15a4-8002-9a6ae7925a88"
response="yes" classId="currentCertificate">
 <outConfigs>
  <currentCertificate dn="sys/cert-mgmt/curr-cert" serialNumber="C764DC592E154539"
   countryCode="US" state="California" locality="San Jose" organization="cisco"
   organizationalUnit="cisco" commonName="cisco" issuerCountryCode="US"
   issuerState="California" issuerLocality="San Jose" issuerOrganization="cisco"
   issuerOrganizationalUnit="cisco" issuerCommonName="cisco"
   validFrom="Nov 20 05:11:22 2015 GMT" validTo="Nov 17 05:11:22 2025 GMT"/>
 </outConfigs>
</configResolveClass>
```

Retrieving the Status of a Certificate Signing Request

Request:

```
<configResolveClass cookie="1448761796/eb8a8234-25a4-15a4-8002-9a6ae7925a88"
 classId="generateCertificateSigningRequest" inHierarchical="false">
</configResolveClass>
```

Response:

```
<configResolveClass cookie="1448761796/eb8a8234-25a4-15a4-8002-9a6ae7925a88"
response="yes" classId="generateCertificateSigningRequest">
 <outConfigs>
  <generateCertificateSigningRequest dn="sys/cert-mgmt/gen-csr-req"
   commonName="Common Name" organization="Organization" organizationalUnit="Organizational

   Unit" locality="Locality" state="State" countryCode="Country Code" email="Email Address"

   selfSigned="no" protocol="none" remoteServer="" remoteFile="" user="" pwd=""
   csrStatus="Completed CSR"/>
 </outConfigs>
</configResolveClass>
```

Generating Self-Signed Certificate

Request:

```
<configConfMo cookie='1448761796/eb8a8234-25a4-15a4-8002-9a6ae7925a88'
dn="sys/cert-mgmt/gen-csr-req" inHierarchical="false">
 <inConfig>
 <generateCertificateSigningRequest commonName="cisco" organization="cisco"
  organizationalUnit="cisco" locality="Banglore" state="KARNATAKA"
  countryCode="India" dn="sys/cert-mgmt/gen-csr-req" selfSigned="yes"/>
 </inConfig>
```

```
</configConfMo>
```

Response:

```
<configConfMocookie="1448761796/eb8a8234-25a4-15a4-8002-9a6ae7925a88" response="yes"
dn="sys/cert-mgmt/gen-csr-req">
 <outConfig>
  <generateCertificateSigningRequest dn="sys/cert-mgmt/gen-csr-req" commonName="Common Name"

   organization="Organization" organizationalUnit="Organizational Unit" locality="Locality"

   state="State" countryCode="Country Code" email="Email Address" selfSigned="no"
   protocol="none" remoteServer="" remoteFile="" user="" pwd=""
   csrStatus="Completed CSR" status="modified"/>
 </outConfig>
</configConfMo>
```

Uploading a Signed Certificate

Request:

```
<configConfMo cookie='1448762867/b32d6bdd-25a4-15a4-8002-9a6ae7925a88'
dn="sys/cert-mgmt/upload-cert" inHierarchical="false">
<inConfig>
 <uploadCertificate adminAction="remote-cert-upload" protocol="sftp" user="user"
  remoteServer="10.10.10.10" remoteFile="/tmp/xmlTest.crt" pwd="cisco123"
  dn="sys/cert-mgmt/upload-cert"/>
 </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/cert-mgmt/upload-cert"
cookie="1448762867/b32d6bdd-25a4-15a4-8002-9a6ae7925a88"
response="yes">
 <outConfig>
  <uploadCertificate dn="sys/cert-mgmt/upload-cert" adminAction="no-op" protocol="none"
   remoteServer="" remoteFile="" user="" pwd="" certificateContent="Certificate Content"
   status="modified"/>
  </outConfig>
</configConfMo>
```

Managing LDAP Certificates

The examples in this section show how to use the Cisco IMC XML API to retrieve and perform LDAP certificate management tasks. Each example shows the XML API request followed by the response from Cisco IMC.

This section includes the following examples:

Enabling Binding of an LDAP CA Certificate

Request:

```
<configConfMo cookie='1457742601/2dd5f334-2dcf-1dcf-8005-515545067ff0'
dn='sys/ldap-ext/ldap-ca-cert-mgmt'>
<inConfig>
 <ldapCACertificateManagement dn='sys/ldap-ext/ldap-ca-cert-mgmt'
  bindingCertificate='enabled'/>
 </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/ldap-ext/ldap-ca-cert-mgmt"
cookie="1470032930/13a3ed5e-38fd-18fd-800f-ad7c7d74a254" response="yes">
 <outConfig>
  <ldapCACertificateManagement dn="sys/ldap-ext/ldap-ca-cert-mgmt"
  description="LDAP CA Certificate Management"
  bindingCertificate="enabled" status="modified"  >
  </ldapCACertificateManagement>
 </outConfig>
</configConfMo>
```

Disabling Binding of CA Certificate

Request:

```
<configConfMo cookie='1457742601/2dd5f334-2dcf-1dcf-8005-515545067ff0'
dn='sys/ldap-ext/ldap-ca-cert-mgmt'>
 <inConfig>
  <ldapCACertificateManagement
  dn='sys/ldap-ext/ldap-ca-cert-mgmt' bindingCertificate='disabled'/>
 </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/ldap-ext/ldap-ca-cert-mgmt"
cookie="1470032930/13a3ed5e-38fd-18fd-800f-ad7c7d74a254" response="yes">
 <outConfig>
  <ldapCACertificateManagement dn="sys/ldap-ext/ldap-ca-cert-mgmt"
  description="LDAP CA Certificate Management"
  bindingCertificate="disabled" status="modified" >
  </ldapCACertificateManagement>
 </outConfig>
</configConfMo>
```

Downloading LDAP CA Certificate using TFTP Protocol

Request:

```
<configConfMo cookie='1470032930/13a3ed5e-38fd-18fd-800f-ad7c7d74a254'
dn='sys/ldap-ext/ldap-ca-cert-mgmt/ldap-ca-cert-download' inHierarchical='false'>
 <inConfig>
  <downloadLdapCACertificate protocol='tftp' remoteServer='10.10.10.10'
   remoteFile='new_com_chain.cer' dn='sys/ldap-ext/ldap-ca-cert-mgmt/ldap-ca-cert-download'/>

 </inConfig>
</configConfMo>
```

TFTP used in the preceding example is the default protocol. You can also download the LDAP CA certificate using the other available protocols such as the FTP, SFTP, SCP and HTTP.

Response:

```
<configConfMo dn="sys/ldap-ext/ldap-ca-cert-mgmt/ldap-ca-cert-download"
cookie="1470032930/13a3ed5e-38fd-18fd-800f-ad7c7d74a254" response="yes">
 <outConfig>
  <downloadLdapCACertificate dn="sys/ldap-ext/ldap-ca-cert-mgmt/ldap-ca-cert-download"
  protocol="none" remoteServer="" remoteFile="" user="" pwd=""
 downloadStatus="COMPLETED"  downloadProgress="100%" status="modified" >
  </downloadLdapCACertificate>
 </outConfig>
</configConfMo>
```

Exporting LDAP CA Certificate

Request:

```
<configConfMo cookie='1463635956/27a0d4af-332c-132c-8004-9206a0395bfc'
dn='sys/ldap-ext/ldap-ca-cert-mgmt/ldap-ca-cert-export' inHierarchical='false'>
 <inConfig>
  <exportLdapCACertificate protocol='tftp' remoteServer='10.10.10.10'
  remoteFile='fasfsaf.csr'dn='sys/ldap-ext/ldap-ca-cert-mgmt/ldap-ca-cert-export'/>
 </inConfig>
</configConfMo>"
```

Response:

```
<configConfMo dn="sys/ldap-ext/ldap-ca-cert-mgmt/ldap-ca-cert-export"
cookie="1470032930/13a3ed5e-38fd-18fd-800f-ad7c7d74a254" response="yes">
 <outConfig>
  <exportLdapCACertificate dn="sys/ldap-ext/ldap-ca-cert-mgmt/ldap-ca-cert-export"
   protocol="none" remoteServer="" remoteFile="" user="" pwd=""
   exportStatus="COMPLETED" exportProgress="100%" status="modified" >
  </exportLdapCACertificate>
 </outConfig>
</configConfMo>
```

TFTP used in the preceding example is the default protocol. You can also download the LDAP CA certificate using the other available protocols such as the FTP, SFTP, SCP and HTTP.

Testing LDAP Binding

Request:

```
<configConfMo cookie='1470032930/13a3ed5e-38fd-18fd-800f-ad7c7d74a254'
dn='sys/ldap-ext/ldap-ca-cert-mgmt/ldap-ca-cert' inHierarchical='false'>
 <inConfig>
  <ldapCACertificate adminAction='test-ldap-binding' user='user' pwd='Test123'
  dn='sys/ldap-ext/ldap-ca-cert-mgmt/ldap-ca-cert'/>
 </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/ldap-ext/ldap-ca-cert-mgmt/ldap-ca-cert"
cookie="1470032930/13a3ed5e-38fd-18fd-800f-ad7c7d74a254" response="yes">
 <outConfig>
  <ldapCACertificate dn="sys/ldap-ext/ldap-ca-cert-mgmt/ldap-ca-cert"
  adminAction="" user="" pwd="" status="modified" >
  </ldapCACertificate>
 </outConfig>
</configConfMo>
```

Deleting LDAP CA Certificate

Request:

```
<configConfMo cookie='1457746251/9ec8b64d-2dd0-1dd0-8008-515545067ff0'
dn='sys/ldap-ext/ldap-ca-cert-mgmt/ldap-ca-cert' inHierarchical='false'>
 <inConfig>
  <ldapCACertificate adminAction='delete-ca-certificate'
  dn='sys/ldap-ext/ldap-ca-cert-mgmt/ldap-ca-cert'/>
 </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/ldap-ext/ldap-ca-cert-mgmt/ldap-ca-cert"
cookie="1470032930/13a3ed5e-38fd-18fd-800f-ad7c7d74a254" response="yes">
 <outConfig>
  <ldapCACertificate dn="sys/ldap-ext/ldap-ca-cert-mgmt/ldap-ca-cert"
   adminAction="" user="" pwd="" status="modified" >
  </ldapCACertificate>
 </outConfig>
</configConfMo>
```

Configuring KMIP Tasks

The examples in this section show how to use the Cisco IMC XML API to configure Key Management Interoperability Protocol (KMIP) functions. Each example shows the XML API request followed by the response from Cisco IMC.

This section includes the following examples:

Enabling or Disabling Secure Key Management

Request:

```
<configConfMo dn="sys/chassis-1/server-1/kmip-mgmt"
cookie="1486744606/2436e891-3048-1830-8002-be18652a6ca4" inHierarchical="false" >
 <inConfig>
  <kmipManagement dn="sys/chassis-1/server-1/kmip-mgmt" secureKeyManagement="enabled">
  </kmipManagement>
 </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/chassis-1/server-1/kmip-mgmt"
cookie="1486744606/2436e891-3048-1830-8002-be18652a6ca4" response="yes">
 <outConfig>
  <kmipManagement dn="sys/chassis-1/server-1/kmip-mgmt"
  description="Key Management Interoperability Protocol"
  secureKeyManagement="enabled" serverRootCACertificate="Available"
  clientCertificate="Available" clientPrivateKey="Available"
  adminAction="no-op" status="modified"/>
 </outConfig>
</configConfMo>
```

Note To disable Secure Key Management, use secureKeyManagement="disabled" in the command.

Configuring KMIP Server

Request:

```
<configConfMo dn="sys/chassis-1/server-1/kmip-mgmt/kmip-server"
cookie="1478249230/3d18c6f9-4076-1076-8002-e8374190b1d8" inHierarchical="false">
 <inConfig>
    <kmipServer dn="sys/chassis-1/server-1/kmip-mgmt/kmip-server"
    ipAddress="10.10.10.10" port="6000" timeout="25">
    </kmipServer>
 </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/chassis-1/server-1/kmip-mgmt/kmip-server"
cookie="1478249230/3d18c6f9-4076-1076-8002-e8374190b1d8" response="yes">
 <outConfig>
   <kmipServer id="1" ipAddress="10.10.10.10" port="6000" timeout="25"
   testConnectionStatus="Unavailable" adminAction="no-op"
   dn="sys/chassis-1/server-1/kmip-mgmt/kmip-server" status="modified"/>
```

```
 </outConfig>
</configConfMo>
```

Deleting KMIP Server

Request:

```
<configConfMo dn="sys/chassis-1/server-1/kmip-mgmt/kmip-server"
cookie="1478249230/3d18c6f9-4076-1076-8002-e8374190b1d8" inHierarchical="false">
  <inConfig>
    <kmipServer dn="sys/chassis-1/server-1/kmip-mgmt/kmip-server" adminAction="delete" >
    </kmipServer>
  </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/chassis-1/server-1/kmip-mgmt/kmip-server"
cookie="1478249230/3d18c6f9-4076-1076-8002-e8374190b1d8" response="yes">
  <outConfig>
    <kmipServer id="1" ipAddress="" port="5696" timeout="5"
   adminAction="no-op" dn="sys/chassis-1/server-1/kmip-mgmt/kmip-server" status="modified"/>

  </outConfig>
</configConfMo>
```

Viewing Secure Key Management Settings

Request:

```
< <configResolveClass dn="sys/chassis-1/server-1/kmip-mgmt"
cookie="1478234140/28bb863a-4073-1073-8002-e8374190b1d8" inHierarchical="false"
classId="kmipManagement">
```

Response:

```
<configResolveClass dn="sys/chassis-1/server-1/kmip-mgmt/"
cookie="1478235085/94b63d5a-4072-1072-8002-e8374190b1d8" response="yes" >
 <outConfig>
  <kmipManagement dn="sys/chassis-1/server-1/kmip-mgmt" description="Key Management
Interoperability Protocol"
  secureKeyManagement="enabled" serverRootCACertificate="Available"
  clientCertificate="Not Available" clientPrivateKey="Available"
  adminAction="no-op"/>
 </outConfig>
</configResolveClass>
```

Downloading Root CA Certificate (tftp)

Request:

```
<configConfMo dn="sys/chassis-1/server-1/kmip-mgmt/kmip-ca-cert-download"
cookie="1478184218/cf931a62-4066-1066-8003-e8374190b1d8" inHierarchical="false">
 <inConfig>
   <downloadRootCACertificate dn="sys/chassis-1/server-1/kmip-mgmt/kmip-ca-cert-download"
   protocol="tftp" remoteServer="10.10.10.10"
   remoteFile="/home/ss/cert/RootCA.pem">
   </downloadRootCACertificate>
 </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/chassis-1/server-1/kmip-mgmt/kmip-ca-cert-download"
cookie="1478184218/cf931a62-4066-1066-8003-e8374190b1d8" response="yes">
 <outConfig>
  <downloadRootCACertificate dn="sys/chassis-1/server-1/kmip-mgmt/kmip-ca-cert-download"
  protocol="none" remoteServer="" remoteFile="" user="" pwd=""
 downloadStatus="COMPLETED" downloadProgress="100%" status="modified"/>
 </outConfig>
</configConfMo>
```

Exporting Root CA Certificate (scp)

Request:

```
<configConfMo dn="sys/chassis-1/server-1/kmip-mgmt/kmip-ca-cert-export"
cookie="1478189648/3db712b5-4068-1068-8004-e8374190b1d8" inHierarchical="false" >
  <inConfig>
    <exportRootCACertificate dn="sys/chassis-1/server-1/kmip-mgmt/kmip-ca-cert-export"
    protocol="scp" remoteServer="10.10.10.10" user="jsmith" pwd="johnpwd1980"
    remoteFile="/home/jsmith/cert/RootCA.pem">
    </exportRootCACertificate>
  </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/chassis-1/server-1/kmip-mgmt/kmip-ca-cert-export"
cookie="1478189648/3db712b5-4068-1068-8004-e8374190b1d8" response="yes">
  <outConfig>
    <exportRootCACertificate dn="sys/chassis-1/server-1/kmip-mgmt/kmip-ca-cert-export"
    protocol="none" remoteServer="" remoteFile="" user="" pwd=""
    exportStatus="COMPLETED" exportProgress="100%" status="modified"/>
  </outConfig>
</configConfMo>
```

Deleting Root CA Certificate

Request:

```
<configConfMo dn="sys/chassis-1/server-1/kmip-mgmt"
cookie="1478237721/12423b5d-4073-1073-8002-e8374190b1d8" inHierarchical="false">
 <inConfig>
    <kmipManagement dn="sys/chassis-1/server-1/kmip-mgmt"
    adminAction="delete-root-ca-certificate" >
    </kmipManagement>
 </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/chassis-1/server-1/kmip-mgmt"
cookie="1478237721/12423b5d-4073-1073-8002-e8374190b1d8" response="yes">
  <outConfig>
     <kmipManagement dn="sys/chassis-1/server-1/kmip-mgmt"
     description="Key Management Interoperability Protocol"
     secureKeyManagement="enabled" serverRootCACertificate="Not Available"
     clientCertificate="Not Available" clientPrivateKey="Not Available"
     adminAction="no-op" status="modified"/>
  </outConfig>
</configConfMo>
```

Testing Connection with KMIP Server

Request:

```
<configConfMo dn="sys/chassis-1/server-1/kmip-mgmt/kmip-server"
cookie="1478249230/3d18c6f9-4076-1076-8002-e8374190b1d8" inHierarchical="false">
 <inConfig>
  <kmipServer dn="sys/chassis-1/server-1/kmip-mgmt/kmip-server" adminAction="test-connection"
 >
  </kmipServer>
 </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/chassis-1/server-1/kmip-mgmt/kmip-server"
cookie="1478249230/3d18c6f9-4076-1076-8002-e8374190b1d8" response="yes">
 <outConfig>
  <kmipServer id="1" ipAddress="10.10.10.10" port="5696"
   timeout="5"  adminAction="no-op" dn="sys/chassis-1/server-1/kmip-mgmt/kmip-server"
  status="modified"/>
 </outConfig>
</configConfMo>
```

Downloading a Client Private Key

Request:

```
<configConfMo dn="sys/chassis-1/server-1/kmip-mgmt/kmip-private-key-download"
cookie="1478184218/cf931a62-4066-1066-8003-e8374190b1d8" inHierarchical="false">
 <inConfig>
  <downloadClientPrivateKey dn="sys/chassis-1/server-1/kmip-mgmt/kmip-private-key-download"

   protocol="scp" remoteServer="10.10.10.10" user="jsmith" pwd="pwd1234"
   remoteFile="/home/ss/cert/client_private.pem">
  </downloadClientPrivateKey>
 </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/chassis-1/server-1/kmip-mgmt/kmip-private-key-download"
cookie="1478184218/cf931a62-4066-1066-8003-e8374190b1d8" response="yes">
 <outConfig>
  <downloadClientPrivateKey dn="sys/chassis-1/server-1/kmip-mgmt/kmip-private-key-download"

  protocol="none" remoteServer="" remoteFile="" user="" pwd=""
  downloadStatus="COMPLETED" downloadProgress="100%" status="modified"/>
 </outConfig>
</configConfMo>
```

Exporting a Client Private Key

Request:

```
<configConfMo dn="sys/chassis-1/server-1/kmip-mgmt/kmip-private-key-export"
cookie="1478247863/eb2fa9cd-4075-1075-8002-e8374190b1d8" inHierarchical="false" >
 <inConfig>
  <exportClientPrivateKey dn="sys/chassis-1/server-1/kmip-mgmt/kmip-private-key-export"
  protocol="scp" remoteServer="10.10.10.10" user="jsmith" pwd="Johnpwd1982"
  remoteFile="/home/ss/cert/KMIP/Client-Pvt-Key.pem">
  </exportClientPrivateKey>
 </inConfig>
```

```
</configConfMo>
```

Response:

```
<configConfMo dn="sys/chassis-1/server-1/kmip-mgmt/kmip-private-key-export"
cookie="1478247863/eb2fa9cd-4075-1075-8002-e8374190b1d8" response="yes">
 <outConfig>
  <exportClientPrivateKey dn="sys/chassis-1/server-1/kmip-mgmt/kmip-private-key-export"
  protocol="none" remoteServer="" remoteFile="" user="" pwd=""
  exportStatus="COMPLETED" exportProgress="100%" status="modified"/>
 </outConfig>
</configConfMo>
```

Deleting a Client Private Key

Request:

```
<configConfMo dn="sys/chassis-1/server-1/kmip-mgmt"
cookie="1478236687/46db1685-4073-1073-8003-e8374190b1d8" inHierarchical="false" >
 <inConfig>
  <kmipManagement dn="sys/chassis-1/server-1/kmip-mgmt"
adminAction="delete-client-private-key" >
  </kmipManagement>
 </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/chassis-1/server-1/kmip-mgmt"
cookie="1478236687/46db1685-4073-1073-8003-e8374190b1d8" response="yes">
 <outConfig>
   <kmipManagement dn="sys/chassis-1/server-1/kmip-mgmt"
   description="Key Management Interoperability Protocol"
   secureKeyManagement="enabled" serverRootCACertificate="Not Available"
   clientCertificate="Not Available" clientPrivateKey="Not Available"
   adminAction="no-op" status="modified"/>
 </outConfig>
</configConfMo>
```

Downloading a Client Certificate

Request:

```
<configConfMo dn="sys/chassis-1/server-1/kmip-mgmt/kmip-client-cert-download"
cookie="1478184218/cf931a62-4066-1066-8003-e8374190b1d8" inHierarchical="false" >
  <inConfig>
   <downloadClientCertificate dn="sys/chassis-1/server-1/kmip-mgmt/kmip-client-cert-download"

   protocol="scp" remoteServer="10.10.10.10" user="jsmith" pwd="Johnpwd1982"
   remoteFile="/home/ss/cert/Client_cert.pem">
   </downloadClientCertificate>
  </inConfig>
</configConfMo>


<configConfMo dn="sys/chassis-1/server-1/kmip-mgmt/kmip-client-cert-download"
cookie="1478184218/cf931a62-4066-1066-8003-e8374190b1d8" response="yes">
  <outConfig>
   <downloadClientCertificate dn="sys/chassis-1/server-1/kmip-mgmt/kmip-client-cert-download"

    protocol="none" remoteServer="" remoteFile="" user="" pwd=""
    downloadStatus="COMPLETED" downloadProgress="100%" status="modified"/>
  </outConfig>
</configConfMo>
```

Exporting a Client Certificate

Request:

```
<configConfMo dn="sys/chassis-1/server-1/kmip-mgmt/kmip-client-cert-export"
cookie="1478187971/13b8e805-4068-1068-8003-e8374190b1d8" inHierarchical="false">
  <inConfig>
    <exportClientCertificate dn="sys/chassis-1/server-1/kmip-mgmt/kmip-client-cert-export"

    protocol="scp" remoteServer="10.10.10.10" user="jsmith" pwd="Johnpwd1982"
    remoteFile="/home/ss/cert/KMIP/ClientCert.pem">
   </exportClientCertificate>
  </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/chassis-1/server-1/kmip-mgmt/kmip-client-cert-export"
cookie="1478247863/eb2fa9cd-4075-1075-8002-e8374190b1d8" response="yes">
  <outConfig>
    <exportClientCertificate dn="sys/chassis-1/server-1/kmip-mgmt/kmip-client-cert-export"

    protocol="none" remoteServer="" remoteFile="" user="" pwd=""
    exportStatus="COMPLETED" exportProgress="100%" status="modified"/>
  </outConfig>
</configConfMo>
```

Deleting a Client Certificate

Request:

```
<configConfMo dn="sys/chassis-1/server-1/kmip-mgmt"
cookie="1478237721/12423b5d-4073-1073-8002-e8374190b1d8" inHierarchical="false">
  <inConfig>
    <kmipManagement dn="sys/chassis-1/server-1/kmip-mgmt"
adminAction="delete-client-certificate" >
    </kmipManagement>
  </inConfig>
</configConfMo>
```

Reponse:

```
<configConfMo dn="sys/chassis-1/server-1/kmip-mgmt"
cookie="1478237721/12423b5d-4073-1073-8002-e8374190b1d8" response="yes">
  <outConfig>
    <kmipManagement dn="sys/chassis-1/server-1/kmip-mgmt" description="Key Management
Interoperability Protocol"
    secureKeyManagement="enabled" serverRootCACertificate="Not Available"
    clientCertificate="Not Available" clientPrivateKey="Not Available" adminAction="no-op"
 status="modified"/>
  </outConfig>
</configConfMo>
```

Deleting KMIP Server Login Details

Request:

```
<configConfMo dn="sys/chassis-1/server-1/kmip-mgmt/kmip-login"
cookie="1478254180/02b1c8b1-4077-1077-8003-e8374190b1d8" inHierarchical="false" >
  <inConfig>
   <kmipServerLogin dn="sys/chassis-1/server-1/kmip-mgmt/kmip-login" adminAction="clear">
   </kmipServerLogin>
  </inConfig>
```

```
</configConfMo>
```

Response:

```
<configConfMo dn="sys/chassis-1/server-1/kmip-mgmt/kmip-login"
cookie="1478254180/02b1c8b1-4077-1077-8003-e8374190b1d8" response="yes">
  <outConfig>
   <kmipServerLogin dn="sys/chassis-1/server-1/kmip-mgmt/kmip-login"
   accountStatus="disabled" name="" pwd="" adminAction="no-op" status="modified"/>
 </outConfig>
</configConfMo>
```

Unlocking Foreign Configuration on a Self Encrypted Drive

Request:

```
<configConfMo dn='sys/chassis-1/server-1/board/storage-SAS-SBMezz1/ctr-self-encrypt'
cookie='1480557066/0583da3f-4290-1290-8021-127a1e1b0ff4' inHierarchical='false'>
 <inConfig>
  <selfEncryptStorageController
dn='sys/chassis-1/server-1/board/storage-SAS-SBMezz1/ctr-self-encrypt'
  adminAction='unlock-secured-drives'/>
 </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/chassis-1/server-1/board/storage-SAS-SBMezz1/ctr-self-encrypt"
cookie="1480557066/0583da3f-4290-1290-8021-127a1e1b0ff4" response="yes">
 <outConfig>
  <selfEncryptStorageController
dn="sys/chassis-1/server-1/board/storage-SAS-SBMezz1/ctr-self-encrypt"
  keyId="UCSC-MRAID12G_SV53647770_1fd23aac" securityKey="Security key"
  existingSecurityKey="Existing security key" keyManagement=""
  adminAction="no-op" status="modified" >
  </selfEncryptStorageController>
 </outConfig>
</configConfMo>
```

Importing Foreign Configuration to a Self Encrypted Drive

Request:

```
<configConfMo dn='sys/chassis-1/server-1/board/storage-SAS-SBMezz1'
cookie='1480557066/0583da3f-4290-1290-8021-127a1e1b0ff4' inHierarchical='false'>
  <inConfig>
   <storageController dn='sys/chassis-1/server-1/board/storage-SAS-SBMezz1'
   adminAction='import-foreign-config'/>
  </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn='sys/chassis-1/server-1/board/storage-SAS-SBMezz1'
cookie="1480557500/2d74a062-428f-128f-8022-127a1e1b0ff4" response="yes" >
 <outConfig>
  <storageController id="SBMezz1" model="Cisco 12G SAS Modular Raid Controller"
  pciSlot="SBMezz1" presence="equipped" raidSupport="yes" serial="SV53647770"
  type="SAS" vendor="LSI Logic" selfEncryptEnabled="yes" adminAction="no-op"
  dn="sys/chassis-1/server-1/board/storage-SAS-SBMezz1" >
  </storageController>
 </outConfig>
</configConfMo>
```

Enabling Self Encrypted Drive with Key Management as Local and KMIP Disabled

Request:

```
<configConfMo dn="sys/chassis-1/server-1/board/storage-SAS-SBMezz1/ctr-self-encrypt"
cookie="1478342437/3c993fcb-408c-108c-8002-e8374190b1d8" inHierarchical="false" >
 <inConfig>
  <selfEncryptStorageController
dn="sys/chassis-1/server-1/board/storage-SAS-SBMezz1/ctr-self-encrypt"
  keyId="test123" securityKey="test123" adminAction="enable-self-encrypt"
keyManagement="local">
  </selfEncryptStorageController>
 </inConfig>
</configConfMo>
```

Response:

As the configuration takes time, you see an empty response.

```
<configConfMo dn="sys/chassis-1/server-1/board/storage-SAS-SBMezz1/ctr-self-encrypt"
cookie="1478342437/3c993fcb-408c-108c-8002-e8374190b1d8" response="yes">
  <outConfig>
  </outConfig>
</configConfMo>
```

After the configuration is completed, send the following request:

```
<configResolveClass
cookie="1490834627/de1ed316-4be8-1be8-92d4-20be7d8bf200" inHierarchical="false"
classId="selfEncryptStorageController"/>
```

You see the following response:

```
<configResolveClass
cookie="1490834627/de1ed316-4be8-1be8-92d4-20be7d8bf200" response="yes"
classId="selfEncryptStorageController">
 <outConfig>
  <selfEncryptStorageController
dn="sys/chassis-1/server-1/board/storage-SAS-SBMezz1/ctr-self-encrypt"
  keyId="testkeyid" securityKey="Security key" existingSecurityKey="Existing security key"

  keyManagement="" adminAction="no-op" >
  </selfEncryptStorageController>
 </outConfig>
</configResolveClass>
```

Enabling Self Encrypted Drive with Key Management as Remote and KMIP Enabled

Request:

```
<configConfMo dn="sys/chassis-1/server-1/board/storage-SAS-SBMezz1/ctr-self-encrypt"
cookie="1478340466/cde62027-408b-108b-8002-e8374190b1d8" inHierarchical="false">
 <inConfig>
  <selfEncryptStorageController
dn="sys/chassis-1/server-1/board/storage-SAS-SBMezz1/ctr-self-encrypt"
  adminAction="enable-self-encrypt" keyManagement="remote">
  </selfEncryptStorageController>
 </inConfig>
</configConfMo>
```

Response:

As the configuration takes time, you see an empty response.

```
<configConfMo dn="sys/chassis-1/server-1/board/storage-SAS-SBMezz1/ctr-self-encrypt"
```

```
cookie="1478340466/cde62027-408b-108b-8002-e8374190b1d8" response="yes">
  <outConfig>
  </outConfig>
</configConfMo>
```

After the configuration is completed, send the following request:

```
<configResolveClass
cookie="1490834627/de1ed316-4be8-1be8-92d4-20be7d8bf200" inHierarchical="false"
classId="selfEncryptStorageController"/>
```

You see the following response:

```
<configResolveClass
cookie="1490834627/de1ed316-4be8-1be8-92d4-20be7d8bf200" response="yes"
classId="selfEncryptStorageController">
 <outConfig>
  <selfEncryptStorageController
dn="sys/chassis-1/server-1/board/storage-SAS-SBMezz1/ctr-self-encrypt"
  keyId="testkeyid" securityKey="Security key" existingSecurityKey="Existing security key"

  keyManagement="" adminAction="no-op" >
  </selfEncryptStorageController>
 </outConfig>
</configResolveClass>
```

Switching Key Management From Local to Remote with Existing Security Key

Request:

```
<configConfMo dn="sys/chassis-1/server-1/board/storage-SAS-SBMezz1/ctr-self-encrypt"
cookie="1478343933/7da81dea-408c-108c-8002-e8374190b1d8" inHierarchical="false">
 <inConfig>
   <selfEncryptStorageController
dn="sys/chassis-1/server-2/board/storage-SAS-SBMezz1/ctr-self-encrypt"
   adminAction="switch-local-to-remote" existingSecurityKey="SecurityKey">
   </selfEncryptStorageController>
 </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/chassis-1/server-1/board/storage-SAS-SBMezz1/ctr-self-encrypt"
cookie="1478343933/7da81dea-408c-108c-8002-e8374190b1d8" response="yes">
 <outConfig>
  <selfEncryptStorageController
dn="sys/chassis-1/server-1/board/storage-SAS-SBMezz1/ctr-self-encrypt"
  keyId="UCSC-MRAID12G_SV52731947_1fb07b15" securityKey="Security key"
  existingSecurityKey="Existing security key" keyManagement=""
  adminAction="no-op" status="modified"/>
 </outConfig>
</configConfMo>
```

Switching Key Management From Remote to Local with Key ID and Security Key

Request:

```
<configConfMo dn="sys/chassis-1/server-1/board/storage-SAS-SBMezz1/ctr-self-encrypt"
cookie="1478343933/7da81dea-408c-108c-8002-e8374190b1d8" inHierarchical="false">
  <inConfig>
   <selfEncryptStorageController
dn="sys/chassis-1/server-2/board/storage-SAS-SBMezz1/ctr-self-encrypt"
   keyId="KeyId" securityKey="SecurityKey" adminAction="switch-remote-to-local">
   </selfEncryptStorageController>
```

```
  </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/chassis-1/server-1/board/storage-SAS-SBMezz1/ctr-self-encrypt"
cookie="1478343933/7da81dea-408c-108c-8002-e8374190b1d8" response="yes">
 <outConfig>
  <selfEncryptStorageController
dn="sys/chassis-1/server-1/board/storage-SAS-SBMezz1/ctr-self-encrypt"
  keyId="test1234" securityKey="Security key" existingSecurityKey="Existing security key"
  keyManagement="" adminAction="no-op" status="modified"/>
 </outConfig>
</configConfMo>
```

Disabling Security Enabled Drive when Key Management is Local

Request:

```
<configConfMo dn="sys/chassis-1/server-1/board/storage-SAS-SBMezz1/ctr-self-encrypt"
cookie="1478342437/3c993fcb-408c-108c-8002-e8374190b1d8" inHierarchical="false">
 <inConfig>
  <selfEncryptStorageController
dn="sys/chassis-1/server-1/board/storage-SAS-SBMezz1/ctr-self-encrypt"
  adminAction="disable-self-encrypt" >
  </selfEncryptStorageController>
 </inConfig>
</configConfMo>
```

Response:

```
<configConfMo dn="sys/chassis-1/server-1/board/storage-SAS-SBMezz1/ctr-self-encrypt"
cookie="1478342437/3c993fcb-408c-108c-8002-e8374190b1d8" response="yes">
 <outConfig>
 </outConfig>
</configConfMo>
```