Managing Certificates

This chapter includes the following sections:

- Managing Server Certificates, page 1
- Managing LDAP Certificates, page 3

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, on page 1
- Generating Certificate Signing Request, on page 2
- Retrieving the Status of a Certificate Signing Request, on page 2
- Generating Self-Signed Certificate, on page 2
- Uploading a Signed Certificate, on page 3

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, on page 4
- Disabling Binding of CA Certificate, on page 4
- Downloading LDAP CA Certificate using TFTP Protocol, on page 4
- Exporting LDAP CA Certificate, on page 5
- Testing LDAP Binding, on page 5
- Deleting LDAP CA Certificate, on page 6

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>
```