CHAPTER 7

Manage Digital Certificates

Revised: July 29, 2014

You can manage the digital certificates for a Cisco Show and Share and Cisco DMM appliances from the local instance of Appliance Administration Interface (AAI). Furthermore:

- You can import multiple CA chain certificates simultaneously:
  - Inside a single *.ZIP archive (CSCth65646).
  - Inside a single certificate file (CSCti11768).

  However, we do not support these methods for the import of identity certificates. All identity certificates must remain separate during import.
- You can now correctly import a certificate that includes an extra carriage return (CSCth53389).
- You can now configure a Cisco DMS appliance to notify you daily that an imported CA certificate or identity certificate will expire soon. Such notifications begin 10 days before the actual expiration date. To access this feature in the web-based user interface for DMS-Admin, go to Alerts > Notification Rules > Certificate is about to expire (CSCth18904).
- We now support the P7B certitude format in addition to the PEM certificate format.

Note

- Subject Alternative Names (SANs) are supported in Cisco Show and Share and Cisco Digital Media Manager. To use a SAN name, you must generate a Certificate Signing Request (CSR) as described in the Generate and Submit Certificate Signing Requests (CSR) procedure. For the SAN option, when requesting the signing certificate from the certificate authority, the SAN name should be added at the same time and will be included in the certificate.

Activation

We add and improve features often. This chapter describes options and features that do not necessarily exist in all releases. You must upgrade older software as needed before such enhancements can be available to you.

Concepts

Glossary

Timesaver Go to terms that start with... [**A** | **C** | **D** | **K** | **P** | **S** | **X**].

A

asymmetric key exchange Asymmetric or *public key* cryptography is based on the concept of a key pair. Each half of the pair (one key) can encrypt information so that only the other half (the other key) can decrypt it. One part of the key pair, the private key, is known only by the designated owner; the other part, the public key, is published widely but is still associated with the owner.

C

Return to Top

CA *certification authority.* Authority in a network that issues and manages security credentials and public keys for message encryption and decryption. As part of a public key infrastructure (PKI), a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can then issue a certificate.

CA signature Digital code that vouches for the authenticity of a digital certificate. The certification authority (CA) that issues a certificate also signs it.

certificate chain Hierarchical list of public-key certificates, each signed by the subsequent certificate, ending with a Root CA certificate.

CSR *certificate signing request*. A block of ciphertext that (**1.**) describes an entity to a CA and (**2.**) requests a digital identity certificate to authenticate the entity for SSL. The CSR includes encrypted information to identify the entity, such as its location, serial number, and public key. This example shows a CSR.

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIICrTCCAZUCAQAwaDEXMBUGA1UEAxMOZHN5cy5jaXNjby5jb20xDzANBgNVBAsTBmp5Z2podjEO
MAwGA1UEChMFaGd1eWcxDzANBgNVBAcTBnV5dHlnajEOMAwGA1UECBMFbWhoanYxCzAJBgNVBAYT
AlVTMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAlz+sEkBbIoXTiE13O28FX558enM0
6tVdnNlWmySbtKulYJ+xvHlsdzbCLOPYJhOvr1JJIxaNjf2dT1fdQp4Qd1U/lk5+v9Nmqtlr9Fxl
bUkxkCaYr6H4RYrmqi0+YpLyUgMXqoQ+vFRDdKUGHD5lxQK9dggXvdJQNgylGawXkqG8WepC3XwK
Zyl9CS2S4CbnLs6yHcz86/VE1X4+DqnS3yvfko+Yyg/yUe151Hcwp97C0KtFrZnQcnIDYU4rEaV+
nqKWc52cQ0kuoJjJlzNSlVUGLGA+yPf+fz+0K5liqA6HnE22yA7SWlskcR668JCR9tjqyWnIC+yu
Cd13HUfSpwIDAQABoAAwDQYJKoZIhvcNAQEFBQADggEBAAVj0f6B6lmtVEvCaUxKAI7DDgFjBJhv
BRJMZA+3BVD6OOX8T2J8druEb18bloEX989f81124KceO8Y037/a4RPdxhXM3eeVYTMnz4QcbI6G
MU58jdHgRM1pxmYweixNTmzFTLc3uhp8JHWk286pHOMNHX2OR+cL+Cbj/mYRnmf4hg4LD0oCTS9f
pVEDgmiOpZ/go9OfAZ4nu1SwnqCaNpV+k/hM2RnlAqtaQDR89B4K18IF6odnjc9TL0kXUrsK79BD
Qp1bZQS+MElgnEqHpFjzvaopwXnZSv4CFHi6IwN2HPALY24Bo3XGW85j71HYPbwoVnZtcqdN56X6
HM0lto8=
-----END NEW CERTIFICATE REQUEST-----
```

D

Return to Top

DER A certificate encoding format that we **DO NOT SUPPORT** in any Cisco DMS release. Instead, you can use PEM. Alternatively, starting with Cisco DMS 5.2.3, you can use P7B.

Name	Type
cacert.der	Security Certificate
inter.der	Security Certificate
identity.der	Security Certificate

digital certificate Digital representation of an entity (human or otherwise), as defined in International Organization for Standardization (ISO) standard X.509. A certificate is normally issued by a CA on behalf of an entity. Common fields within a certificate include distinguished names (DN) for the entity and CA, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority, so that a recipient can verify certificate legitimacy.

DN *distinguished name*. A set of attributes that help a CA to authenticate an entity for SSL.

K

Return to Top

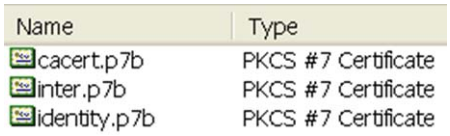
keystore An exported KEYSTORE.DAT file from your Cisco *Show and Share* appliance (or, beginning with Cisco DMS 5.2.3, your DMM appliance) contains a backup copy of its digital certificates.

P

Return to Top

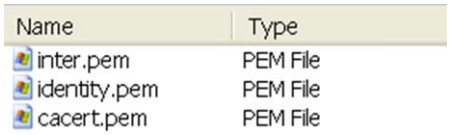
P7B

NEW IN CISCO DMS 5.2.3—An implementation of base64-encoded ASCII in X-509, used to protect identity certificates and CA certificates. **P7B certificates must NOT use binary (DER) encoding. Instead, use Base64 (ASCII) encoding.**



PEM

privacy enhanced email. An implementation of base64-encoded ASCII in X-509, used to protect identity certificates and CA certificates. **Cisco DMS 5.2.1 and 5.2.2 support PEM alone. They reject all other certificate encoding formats.**



private key

A cryptographic value to decrypt messages and digital signatures upon receipt by one authenticated entity from another. Each private key is unique and confidential to one entity. As one half of an asymmetric key pair, each private key is bound to its opposite half, a public key.

public key

A cryptographic value to encrypt messages and digital signatures for delivery from one authenticated entity to another. Each public key is verifiably unique to one entity, which can reveal it widely without compromising the private key. As one half of an asymmetric key pair, each public key is bound to its opposite half, a private key.

S

Return to Top

self-signed

Acknowledgement from an entity that its own digital certificate was not issued by, and is not signed by, any trusted certification authority. Instead, the entity issued and affixed its own signature to its digital certificate. In common practice, a self-signed digital certificate is not considered valid, authentic, or trustworthy until proven so.

signed

Endorsement from a trusted certification authority, affixed to another entity's digital certificate. In common practice, a signed digital certificate is considered valid, authentic, and trustworthy unless proven otherwise.

X

Return to Top

X-509

A standard for public key infrastructure. X.509 specifies, among other things, standard formats for public key certificates and a certification path validation algorithm.

Restrictions

- Expiration, page 7-5

Expiration

Caution

- **Before Cisco DMS 5.2.3, we did not show any advance notice that an imported certificate was approaching its expiration date.** Because most certificates are valid for years at a time, this condition is not likely to disrupt anything in a production network. Even so, in Cisco DMS 5.2.3, we added a notification service that you can enable from DMS-Admin.
- **Show and Share appliances refuse web connections unless their certificates are current and valid.** When they are not, you must import a new certificate. You can obtain and install one from your CA or—temporarily—you can generate and use a self-signed certificate.

Encoding

Caution **We support only PEM in Cisco DMS releases 5.2.1 and 5.2.2.** Certificate import to these releases fails when you use any other encoding format. Likewise for these same releases, import of PEM-compliant certificates fails when their wrapper is a ZIP archive or any binary format. (Cisco DMS 5.2.3 introduces support for P7B.)

Related Topics

- Verify That Your Certificate Format is PEM, as Needed, page 7-10

Carriage Returns

Caution **Avoid extra carriage returns in any certificate file that you import to Cisco DMS 5.2.1 or 5.2.2.** Certificate import to these releases fails whenever extra carriage returns are present. (Cisco DMS 5.2.3 forgives these carriage returns.)

Subject CN Elements

Caution

- **Do not use any wildcards** (*) **in the common name (CN) element of a certificate's subject.** Certificate import fails when a wildcard is present. For example, we would reject a certificate with ***.example.com** as its subject.
- **Do not import to Cisco DMS 5.2.1 or 5.2.2 any certificate whose subject omits the CN element.** Certificate import to these releases fails when the subject is missing its CN. At least one well known certification authority, Go Daddy, sometimes issues certificates without any CN in their subject. (Cisco DMS 5.2.3 forgives these subjects.)

Concatenation

Caution **Do not combine multiple CA certificates together in one file that you will import to Cisco DMS 5.2.1 or 5.2.2.** Import to these releases will fail for merged CA certificates. Similar restrictions apply to identity certificates. (Although Cisco DMS 5.2.3 forgives merged CA certificates, it continues to prohibit any merging of identity certificates.)

Workflows for Certificate Management

You are most likely to use AAI certificate management features in the context of a workflow.

- **Workflow A**—*Obtain and Install Provider-signed Certificates, page 7-6*
- **Workflow B**—*Your Certificates Expire or You Do Not Have Any Certificates, page 7-6*
- **Workflow C**—*Back Up and Restore Certificates, page 7-6*

Workflow A

Obtain and Install Provider-signed Certificates

NEW IN CISCO DMS 5.2.1—This sequence represents the typical workflow to use digital certificates from a trusted certification authority.

1. Generate and Submit Certificate Signing Requests (CSR), page 7-7
2. Import (Install) Provider-signed Certificates, page 7-11
3. View a Certificate Chain to Verify its Certificates, page 7-16
4. Export a Keystore to Back It Up, page 7-17

Workflow B

Your Certificates Expire or You Do Not Have Any Certificates

NEW IN CISCO DMS 5.2.1—This sequence represents the typical workflow to use self-signed digital certificates.

1. Generate Self-signed Certificates, page 7-13
2. View a Certificate Chain to Verify its Certificates, page 7-16

Workflow C

Back Up and Restore Certificates

NEW IN CISCO DMS 5.2.1—This sequence represents the typical workflow to back up your digital certificates and, later, restore them.

1. Export a Keystore to Back It Up, page 7-17
2. Import a Keystore to Restore It from a Backup, page 7-18
3. View a Certificate Chain to Verify its Certificates, page 7-16

Procedures

Generate and Submit Certificate Signing Requests (CSR)

Caution **In Cisco DMS 5.2.1 and 5.2.2, we support this procedure exclusively on a *Show and Share* appliance.** Then, in Cisco DMS 5.2.3, we introduced official support for this feature on DMM appliances.

Workflow Context

This topic is part of Workflow A.

Before You Begin

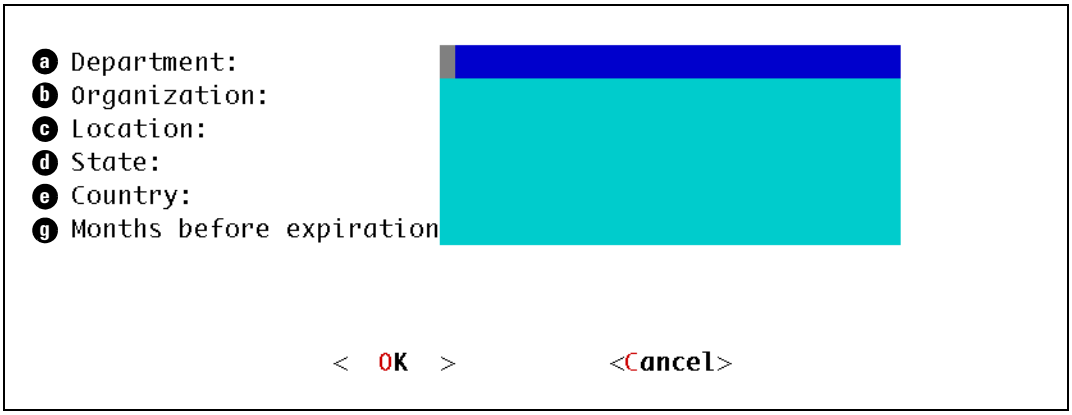
- Contact a certification authority to learn about its process to receive a request. Many CAs will expect to receive your request through their FTP or SFTP server. Although you can use any CA, these four are among the best known.
  - *VeriSign*—www.verisign.com
  - *GoDaddy*—www.godaddy.com
  - *Comodo*—www.comodo.com
  - *Network Solutions*—www.networksolutions.com
- Subject Alternative Names (SANs) are supported in Cisco Show and Share and Cisco Digital Media Manager. To use a SAN name, you must generate a Certificate Signing Request (CSR) as described in this procedure. For the SAN option, when requesting the signing certificate from the certificate authority, the SAN names should be added at the same time and will be included in the certificate.
- Log in as **admin** to the Appliance Administration Interface (AAI).

Procedure

Step 1 Choose **CERTIFICATE_MANAGEMENT > MANAGE_SIGNED_CERTS > GENERATE_CSR**.

Step 2 Enter values in the fields, as illustrated.

Note **Do not use any of these characters.**
, + = " \ ' ` < > # ;



a. Use the Department field to enter the name for your organizational unit—such as *Finance Ministry*, *Taiwan Office*, *College of Engineering*, or *Publications Department*. Then, press the **Down** (↓) key.

b. Use the Organization field to enter the full legal name for your entire organization, as it is known to your national government or intergovernmental authority—such as *Cisco Systems*, *Cambridge University*, or *Médecins Sans Frontières*. Then, press the **Down** (↓) key.

c. Use the Location field to enter the full and officially designated place name of your city, town, township, village, hamlet, civil parish, or settlement—such as *Madrid* or *Tokyo*. Then, press the **Down** (↓) key.

d. Use the State field to enter the full name of your state, province, commonwealth, territory, republic, periphery, dependency, or protectorate—such as *Montserrat*, *California*, *Tamil Nadu*, *Chechnya*, *São Paulo,* or *Crete*. Then, press the **Down** (↓) key.

e. Use the Country field to enter the 2-character country code, as managed by the Internet Assigned Names Agency (IANA).

- Even if this code **is *not* part** of your Internet domain name, it is a necessary attribute of your digital certificate.
- Even if this code **is part** of your Internet domain name, you must not prefix it here with a period.

Note **Your IANA country code might differ from all country name abbreviations that you know.** The "Internet Assigned Names Agency (IANA) Country Codes" section on page 7-19 directs you to your country code.

f. Press the **Down** (↓) key.

Note **The "Months Before Expiration" field is not useful in this procedure.** You can safely ignore it.

Step 3 Choose **OK**.

Step 4 Use this checklist to prequalify a CA.

- **Does the CA use PEM or P7B, as appropriate?**

  We require certificates that use PEM encoding (exclusively in Cisco DMS 5.2.1 and 5.2.2) or P7B encoding (alternatively to PEM, beginning with Cisco DMS 5.2.3).

- **Does the subject include a CN element in cases where it must do so?**

  We require for Cisco DMS 5.2.1 and 5.2.2 that all certificate subjects include a CN element. Cisco DMS 5.2.3 eliminates this requirement.

- **Does the CA isolate each certificate in cases where it must do so?**

  We require in Cisco DMS 5.2.1 and 5.2.2 that each imported CA certificate and each imported identity certificate has its own, standalone file.

  Although Cisco DMS 5.2.3 eliminates this restriction for CA certificates, it continues to enforce the restriction for identity certificates.

Step 5 After you choose a CA, enter values that it provides to you, which identify its server specifically and you specifically. Then, choose **OK**.

OR

If your CA does not use an FTP or SFTP server to receive CSRs, enter values to identify a server that you control. Later, you can retrieve your encrypted CSR for delivery to your CA through its alternative process. For example, you might paste your CSR ciphertext into a form on the CA website.

Note **Your CA might ask you to specify what server platform—such as Apache or Microsoft Internet Application Server (IIS)—will use your new certificate.** You must choose Apache. Otherwise, your new certificate is not encoded correctly for Cisco DMS products to use it.

Step 6 Stop. You have completed this procedure.

What to Do Next

- **OPTIONAL**—*Would you like to check whether your digital certificates use the correct format?* Go to the "Verify That Your Certificate Format is PEM, as Needed" section on page 7-10.
- **OPTIONAL**—*Would you like to install signed digital certificates that you received from a CA?* Go to the "Import (Install) Provider-signed Certificates" section on page 7-11.

Verify That Your Certificate Format is PEM, as Needed

Note We support only PEM in Cisco DMS 5.2.1 and 5.2.2. **These two releases do not support any other digital certificate encoding format, including PB7.** However, we began supporting P7B certificates as an alternative to PEM in Cisco DMS 5.2.3.

You can use an ordinary text editor, such as Notepad on Windows or TextEdit on Mac, to confirm quickly that your certificates use PEM encoding—as they must do for Cisco DMS 5.2.1 and 5.2.2.

Procedure

Step 1 Start your text editor.

Step 2 Use its **Open** command to load your unaltered certificate file for viewing.

Step 3 Examine the certificate.

- Does its first line say exactly `-----BEGIN CERTIFICATE-----` and nothing else?
- Does its last line say exactly `-----END CERTIFICATE-----` and nothing else?

When an unaltered certificate meets these requirements, it is encoded correctly for use with this release. You can import it.

Note **Do not merely add the BEGIN and END statements to a certificate file that lacks them.** Their presence does not—by itself—change how a certificate is encoded.

Step 4 Otherwise, do not import the certificate. We cannot use it with Cisco DMS 5.2.1 or 5.2.2. Contact your CA instead and request a replacement certificate that uses PEM encoding.

Step 5 Stop. You have completed this procedure.

What to Do Next

- **OPTIONAL**—*Would you like to install signed digital certificates that you received from a CA?* Go to the "Import (Install) Provider-signed Certificates" section on page 7-11.

Import (Install) Provider-signed Certificates

Caution **In Cisco DMS 5.2.1 and 5.2.2, we support this procedure exclusively on a *Show and Share* appliance.** Then, in Cisco DMS 5.2.3, we introduced official support for this feature on DMM appliances.

When you import certificates, they overwrite all others.

Workflow Context

This topic is part of Workflow A.

Before You Begin

- Request and obtain a digital certificate from a trusted CA.
- Log in as **admin** to the Appliance Administration Interface (AAI).
- Consider certificate restrictions for:
  - Expiration
  - Encoding
  - Carriage Returns
  - Subject CN Elements
  - Concatenation

Procedure

Step 1 Choose **CERTIFICATE_MANAGEMENT > MANAGE_SIGNED_CERTS > IMPORT_CERTIFICATE**.

Step 2 Choose **Yes** at the prompt to overwrite your active certificates with their replacements.

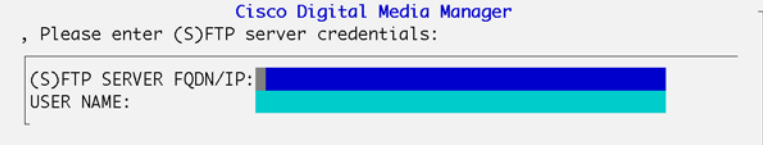
Step 3 Enter information about the FTP or SFTP server where you store your digital certificates.

a. Use the first field to enter a routable IP address or DNS-resolvable FQDN for the server.

b. Press the **Down** (↓) key.

c. Use the second field to enter a username that has sufficient permissions to read your certificates from the server.

d. Choose **OK**.



Step 4 Enter your password for the FTP or SFTP server, and then choose **OK**.

Step 5 Enter absolute file paths, as prompted.

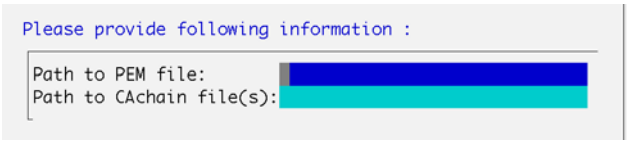
a. Use the first field to specify the path to one or more PEM files. If you will specify more than one file, comma-separate the filenames.

Note Do not specify a ZIP archive that contains your PEM files. If you do, an error message will state that the certificate chain is damaged and at least one of your certificates is not formatted correctly.

b. Press the **Down** (↓) key.

c. Use the second field to specify the path to one or more CAchain files.

d. Choose **OK**.



Note An error message might state that AAI could not retrieve any CAchain files from the remote server. If so, several additional messages might load in sequence. In this case, you must choose OK after each message to dismiss it. For example, a sequence of messages might say:

- `Failed to get file usage: from remote server.`
- `Failed to get file tokenize from remote server.`
- `Failed to get file [separator] from remote server.`
- `Failed to get file [string_to_tokneize] from remote server.`
- `1 MISSING_CA_CERTIFICATE`

If access failed after AAI exceeded that maximum number of retries, please check that the server is running and reachable, and that you entered both paths correctly.

Step 6 Stop. You have completed this procedure.

What to Do Next

- **MANDATORY**—*The appliance identity has changed. You must now re-establish trust among your Cisco DMS appliances.* Go to the "Pair Your Appliances" section on page 11-2.
- **OPTIONAL**—*Would you like to verify any of your digital certificates?* Go to the "View Identity Certificates" section on page 7-15.

Related Topics

- Generate and Submit Certificate Signing Requests (CSR), page 7-7

Generate Self-signed Certificates

Caution **In Cisco DMS 5.2.1 and 5.2.2, we support this procedure exclusively on a *Show and Share* appliance.** Then, in Cisco DMS 5.2.3, we introduced official support for this feature on DMM appliances.

Workflow Context

This topic is part of Workflow B.

Before You Begin

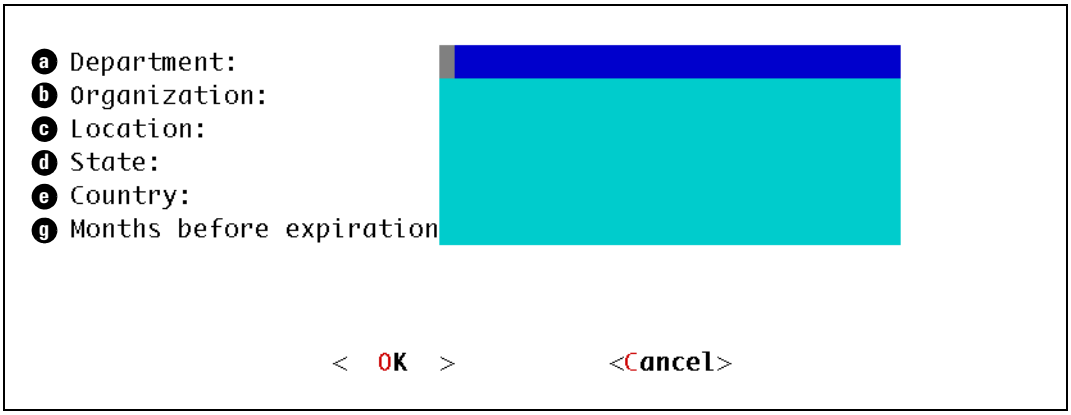
- Log in as **admin** to the Appliance Administration Interface (AAI).

Procedure

Step 1 Choose **CERTIFICATE_MANAGEMENT > MANAGE_SELF_SIGNED_CERTS > GENERATE_NEW_CERT**.

Step 2 Enter values in the fields, as illustrated.

Note **Do not use any of these characters.**
, + = " \ ' ` < > # ;



a. Use the Department field to enter the name for your organizational unit—such as *Finance Ministry*, *Taiwan Office*, *College of Engineering*, or *Publications Department*. Then, press the **Down** (↓) key.

b. Use the Organization field to enter the full legal name for your entire organization, as it is known to your national government or intergovernmental authority—such as *Cisco Systems*, *Cambridge University*, or *Médecins Sans Frontières*. Then, press the **Down** (↓) key.

c. Use the Location field to enter the full and officially designated place name of your city, town, township, village, hamlet, civil parish, or settlement—such as *Madrid* or *Tokyo*. Then, press the **Down** (↓) key.

d. Use the State field to enter the full name of your state, province, commonwealth, territory, republic, periphery, dependency, or protectorate—such as *Montserrat*, *California*, *Tamil Nadu*, *Chechnya*, *São Paulo,* or *Crete*. Then, press the **Down** (↓) key.

e. Use the Country field to enter the 2-character country code, as managed by the Internet Assigned Names Agency (IANA).

- Even if this code **is *not* part** of your Internet domain name, it is a necessary attribute of your digital certificate.
- Even if this code **is part** of your Internet domain name, you must not prefix it here with a period.

Note **Your IANA country code might differ from all country name abbreviations that you know.** The "Internet Assigned Names Agency (IANA) Country Codes" section on page 7-19 directs you to your country code.

f. Press the **Down** (↓) key.

g. Use the Months Before Expiration field to count the months until your digital certificate should expire.

- Briefer durations improve security at the cost of convenience.
- Longer durations improve convenience at the cost of security.
- Permitted values range from **1** to **999**.

Step 3 Choose **OK**.

Step 4 Stop. You have completed this procedure.

What to Do Next

- **MANDATORY**—*The appliance identity has changed. You must now re-establish trust among your Cisco DMS appliances.* Go to the "Pair Your Appliances" section on page 11-2.
- **OPTIONAL**—*Would you like to verify any of your digital certificates?* Go to the "View Identity Certificates" section on page 7-15.

View Identity Certificates

Caution **In Cisco DMS 5.2.1 and 5.2.2, we support this procedure exclusively on a *Show and Share* appliance.** Then, in Cisco DMS 5.2.3, we introduced official support for this feature on DMM appliances.

Workflow Context

This topic is not part of any workflow.

Before You Begin

- Log in as **admin** to the Appliance Administration Interface (AAI).
- Obtain and install certificates.

Procedure

Step 1 Choose **CERTIFICATE_MANAGEMENT > VIEW_CERTIFICATE**.

Step 2 Examine the certificate.

Step 3 Choose **EXIT** when you are done.

Step 4 Stop. You have completed this procedure.

What to Do Next

- **OPTIONAL**—*Would you like to back up your digital certificates?* Go to the "Export a Keystore to Back It Up" section on page 7-17.

Related Topics

- Generate and Submit Certificate Signing Requests (CSR), page 7-7
- Import (Install) Provider-signed Certificates, page 7-11
- Generate Self-signed Certificates, page 7-13

View a Certificate Chain to Verify its Certificates

Caution **In Cisco DMS 5.2.1 and 5.2.2, we support this procedure exclusively on a *Show and Share* appliance.** Then, in Cisco DMS 5.2.3, we introduced official support for this feature on DMM appliances.

Workflow Context

This topic is part of Workflow A, Workflow B, and Workflow C.

Before You Begin

- Log in as **admin** to the Appliance Administration Interface (AAI).
- Obtain and install certificates.

Procedure

Step 1 Choose **CERTIFICATE_MANAGEMENT > VIEW_CERT_CHAIN**.

Step 2 Examine the certificate chain.

Step 3 Choose **EXIT** when you are done.

Step 4 Stop. You have completed this procedure.

What to Do Next

- **OPTIONAL**—*Would you like to back up your digital certificates?* Go to the "Export a Keystore to Back It Up" section on page 7-17.

Related Topics

- Generate and Submit Certificate Signing Requests (CSR), page 7-7
- Import (Install) Provider-signed Certificates, page 7-11
- Generate Self-signed Certificates, page 7-13

Export a Keystore to Back It Up

Your certificates are included whenever you back up your appliance from its local instance of AAI.

Caution **In Cisco DMS 5.2.1 and 5.2.2, we support this procedure exclusively on a *Show and Share* appliance.** Then, in Cisco DMS 5.2.3, we introduced official support for this feature on DMM appliances.

Workflow Context

This topic is part of Workflow A and Workflow C.

Before You Begin

- Log in as **admin** to the Appliance Administration Interface (AAI).
- Obtain and install certificates.
- Delete any old keystore *.DAT file from your FTP or SFTP server before you export a new one.

Procedure

Step 1 Choose **CERTIFICATE_MANAGEMENT > EXPORT_KEYSTORE**.

Step 2 Enter the passphrase from which your private key was derived.

Step 3 Press **Enter**.

Step 4 Use the first field to enter a routable IP address or DNS-resolvable FQDN for the FTP or SFTP server where you will transfer an exported copy of your digital certificates.

Step 5 Press the **Down** ( ) key.

Step 6 Use the second field to enter a username that has read-write permissions on the server that you specified. Then, press **Enter**.

Step 7 Enter the password that authenticates the username. Then, press **Enter**.

Step 8 Enter the full pathname where to save your keystore file on the remote server. Then, press **Enter**.

Step 9 Stop. You have completed this procedure.

What to Do Next

- **OPTIONAL**—*Would you like to restore certificates from a backup?* Go to the "Import a Keystore to Restore It from a Backup" section on page 7-18.

Related Topics

- Generate and Submit Certificate Signing Requests (CSR), page 7-7
- Import (Install) Provider-signed Certificates, page 7-11
- Generate Self-signed Certificates, page 7-13

Import a Keystore to Restore It from a Backup

Caution **In Cisco DMS 5.2.1 and 5.2.2, we support this procedure exclusively on a *Show and Share* appliance.** Then, in Cisco DMS 5.2.3, we introduced official support for this feature on DMM appliances.

Workflow Context

This topic is part of Workflow C.

Before You Begin

- Log in as **admin** to the Appliance Administration Interface (AAI).
- Export a keystore.

Procedure

Step 1 Choose **CERTIFICATE_MANAGEMENT > IMPORT_KEYSTORE**.

Step 2 Enter the passphrase from which your private key was derived.

Step 3 Press **Enter**.

Step 4 Use the first field to enter a routable IP address or DNS-resolvable FQDN for the FTP or SFTP server where you store your digital certificates.

Step 5 Press the down key.

Step 6 Use the second field to enter a username that has sufficient permissions to read your certificates from the server that you specified. Then, press **Enter**.

Step 7 Enter the password that authenticates the username. Then, press **Enter**.

Step 8 Enter the full pathname that points to your keystore file on the remote server. Then, press **Enter**.

Step 9 Stop. You have completed this procedure.

What to Do Next

- **MANDATORY**—*The appliance identity has changed. You must now re-establish trust among your Cisco DMS appliances.* Go to the "Pair Your Appliances" section on page 11-2.
- **OPTIONAL**—*Would you like to verify any of your digital certificates?* Go to the "View Identity Certificates" section on page 7-15.

Related Topics

- Export a Keystore to Back It Up, page 7-17

Reference

Internet Assigned Names Agency (IANA) Country Codes

Digital certificates use one standard set of codes to describe the international locations of entities whose identities are certified. IANA assigns these codes. IANA closely derives almost all of its codes from "A2" country and region codes, which the *ISO 3166-1 alpha-2* standard defines. However, the set of IANA-assigned codes is not perfectly identical to the set of A2 codes. In some cases, IANA has defined new country and region codes for its own purposes. Some of these, in turn, were then added to ISO 3166.

Furthermore, geopolitical changes over time cause governmental federations to develop and dissolve. Lands are conquered, colonized, reapportioned, renamed, and so on. Slow but continual changes like these can create confusion about which country and region code to use in a certificate signing request (CSR). And while there are precedents for deleting country codes from ISO 3166, removal there does not result in immediate removal also from the country code top-level domains (ccTLDs) that exist in DNS.

Table 7-1 sorts countries and regions alphabetically by their names in English. Its cross-references redirect you in cases where geopolitical events, shared governance, or other factors might lead to confusion about which code to use.

Table 7-1 IANA Country and Region Codes

Code	Country or Region
A	
AF	Afghanistan, Islamic State of
AX	Åland Islands *see also* Finland
AL	Albania
DZ	Algeria, Democratic Popular Republic of
AS	American Samoa, Territory of *see also* Guam, Territory of; Northern Mariana Islands, Commonwealth of the; Puerto Rico, Commonwealth of; Samoa, Independent State of; United States of America, Federal Union of the; and Virgin Islands, U.S. Territory of the
For *Andaman*, see India	
AD	Andorra, Principality of
AO	Angola
AI	Anguilla
AQ	Antarctica
AG	Antigua and Barbuda
For *Aosta Valley*, see Italy	
AR	Argentina

Table 7-1 IANA Country and Region Codes (continued)

Code	Country or Region
AM	Armenia
AW	Aruba
For *Ascension*, see Saint Helena, Ascension and Tristan da Cunha	
AC	Ascension Island *see also* Saint Helena, Ascension and Tristan da Cunha
For *Assam*, see India	
AU	Australia **Note All subdomains that previously used OZ as their country code top-level domain were transitioned to OZ.AU.**
AT	Austria
AZ	Azerbaijan
B	
BS	Bahamas, Commonwealth of
BH	Bahrain, Emirate of
For *Bali*, see Indonesia	
BD	Bangladesh
For *Bangui*, see Central African Republic	
BB	Barbados
For *Barbuda*, see Antigua and Barbuda	
BY	Belarus
BE	Belgium, Kingdom of
BZ	Belize
For *Bengal*, see Bangladesh and India	
BJ	Benin
BM	Bermuda
BT	Bhutan, Kingdom of
For *Bodoland Territory*, see India	
BO	Bolivia
For *Bolzano-Bozen (Alto Adige-South Tyrol)*, see Austria; Germany, Federal Republic of; Hungary; and Italy	
For *Borneo*, see Indonesia	
BA	Bosnia and Herzegovina
BW	Botswana
For *Bougainville*, see Papua New Guinea, Independent State of	
BV	Bouvet Island, Territory of **Note Although the BV country code exists in *ISO-3166-1 alpha-2*, and exists as a country code top-level domain in DNS, it does not contain any subdomains.**

Table 7-1 IANA Country and Region Codes (continued)

Code	Country or Region
BR	Brazil, Federative Republic of
For *Britain*, see Ireland and United Kingdom of Great Britain and Northern Ireland	
IO	British Indian Ocean Territory
BN	Brunei Darussalam, Sultanate of
For *Brussels*, see Belgium, Kingdom of	
For *Buenos Aires*, see Argentina	
BG	Bulgaria
BF	Burkina Faso
For *Burma*, see Myanmar	
BI	Burundi
C	
For *Caicos Islands*, see Turks and Caicos Islands, Territory of	
KH	Cambodia, Kingdom of
CM	Cameroon
CA	Canada
CV	Cape Verde
KY	Cayman Islands
CF	Central African Republic
For *Ceuta*, see Spain	
For *Ceylon*, see Sri Lanka	
TD	Chad
For *Chakma Autonomous District*, see India	
For *Channel Islands*, see Guernsey, Bailiwick of and Jersey, Bailiwick of	
For *Chiapas*, see Mexico	
CL	Chile
CN	China, People's Republic of *see also* Hong Kong; Macau, Special Administrative Region of; and Taiwan, Republic of China
CX	Christmas Island, Territory of
CC	Cocos (Keeling) Islands
CO	Colombia
KM	Comoros
CG	Congo *see also* Congo, the Democratic Republic of the
CD	Congo, the Democratic Republic of the *see also* Congo

Table 7-1 IANA Country and Region Codes (continued)

Code	Country or Region
CK	Cook Islands
For *Corsica, Territorial Collectivity of*, see France, Metropolitan	
CR	Costa Rica
CI	Cote d'Ivoire
HR	Croatia
CU	Cuba
CY	Cyprus
For *Czechoslovalia*, see Czech Republic	
CZ	Czech Republic *see also* Slovakia

D

For *Darjeeling Gorkha Hills*, see India	
DK	Denmark, Kingdom of *see also* Faroe Islands and Greenland
DJ	Djibouti
DM	Dominica, Commonwealth of *see also* Dominican Republic
DO	Dominican Republic *see also* Dominica, Commonwealth of

E

For *East Bengal*, see Bangladesh and Pakistan, Islamic Republic of	
For *East Indies*, see Indonesia; Malaysia, Kingdom of; Philippines; and Solomon Islands	
For *East Timor*, see Timor-Leste	
EC	Ecuador
EG	Egypt, Arab Republic of
SV	El Salvador
GQ	Equatorial Guinea
For *Ghana*, see Ghana	
For *Guiana*, see French Guiana, Overseas Department of	
For *Guinea*, see Guinea	
For *Guyana*, see Guyana, Cooperative Republic of	
ER	Eritrea
EE	Estonia
ET	Ethiopia, Federal Democratic Republic of

Table 7-1 IANA Country and Region Codes (continued)

Code	Country or Region
EU	European Union
F	
FK	Falkland Islands (Malvinas Islas), Colony of
FO	Faroe Islands
FJ	Fiji
FI	Finland *see also* Åland Islands
FR	France
FX	France, Metropolitan
GF	French Guiana, Overseas Department of
For *Equatorial Guinea*, see Equatorial Guinea For *Ghana*, see Ghana For *Guinea*, see Guinea For *Guyana*, see Guyana, Cooperative Republic of	
PF	French Polynesia, Overseas Territory of
TF	French Southern Territories
For *Friuli-Venezia Giula*, see Croatia; Italy; and Slovenia	
G	
GA	Gabon
GM	Gambia
For *Garo Hills Autonomous District*, see India	
GE	Georgia *see also* South Georgia and the South Sandwich Islands
DE	Germany, Federal Republic of
GH	Ghana
For *Equatorial Guinea*, see Equatorial Guinea For *Guiana*, see French Guiana, Overseas Department of For *Guinea*, see Guinea For *Guyana*, see Guyana, Cooperative Republic of	
GI	Gibraltar
For *Gilbert Islands*, see Kiribati	
For *Great Britain*, see United Kingdom of Great Britain and Northern Ireland	
GR	Greece

Table 7-1 IANA Country and Region Codes (continued)

Code	Country or Region
GL	Greenland *see also* Denmark, Kingdom of and Faroe Islands
GD	Grenada *see also* Saint Vincent and the Grenadines
For *Grenadines*, see Saint Vincent and the Grenadines	
GP	Guadeloupe and Dependencies, Overseas Department of
GU	Guam, Territory of *see also* American Samoa, Territory of; Northern Mariana Islands, Commonwealth of the; Puerto Rico, Commonwealth of; United States of America, Federal Union of the; and Virgin Islands, U.S. Territory of the
For *Guangxi Zhung Autonomous Region*, see China, People's Republic of	
GT	Guatemala
GG	Guernsey, Bailiwick of *see also* Jersey, Bailiwick of
For *Guiana*, see French Guiana, Overseas Department of	
GN	Guinea *see also* Guinea-Bissau
GW	Guinea-Bissau *see also* Guinea
GY	Guyana, Cooperative Republic of
For *Equatorial Guinea*, see Equatorial Guinea	
For *Ghana*, see Ghana	
For *Guiana*, see French Guiana, Overseas Department of	
For *Guinea*, see Guinea	
H	
HT	Haiti
HM	Heard and McDonald Islands, Territory of
For *Herzegovina*, see Bosnia and Herzegovina	
VA	Holy See, State of Vatican City *see also* Italy
HN	Honduras
HK	Hong Kong *see also* China, People's Republic of; Macau, Special Administrative Region of; and Taiwan, Republic of China
HU	Hungary

Table 7-1 IANA Country and Region Codes (continued)

Code	Country or Region
I	
IS	Iceland
IN	India
ID	Indonesia
For *Inner Mongolia Autonomous Region*, see China, People's Republic of	
IR	Iran, Islamic Republic of
IQ	Iraq
For *Iraqi Kurdistan*, see Iraq	
IE	Ireland
IM	Isle of Man, Territory of
IL	Israel, State of *see also* Palestine, Occupied Territory of
IT	Italy *see also* Holy See, State of Vatican City
For *Ivory Coast*, see Cote d'Ivoire	
J	
For *Jaintia Hills Autonomous District*, see India	
JM	Jamaica
For *Jammu*, see India	
For *Jan Mayen*, see Svalbard and Jan Mayen Islands, Territory of	
JP	Japan, Imperial State of
For *Java*, see Indonesia	
For *Jeju-do*, see Korea, Republic of	
JE	Jersey, Bailiwick of *see also* Guernsey, Bailiwick of
For *Jewish Autonomous Oblast*, see Russia, Federation of	
JO	Jordan, Hashemite Kingdom of
K	
For *Kampuchea*, see Cambodia, Kingdom of	
For *Karbi Anglong Autonomous Council*, see India	
For *Kashmir*, see China, People's Republic of; India; and Pakistan, Islamic Republic of	
KZ	Kazakhstan
For *Keeling Islands*, see Cocos (Keeling) Islands	
KE	Kenya

Table 7-1 IANA Country and Region Codes (continued)

Code	Country or Region
	For *Khasi Hills Autonomous District*, see India
KI	Kiribati *see also* Marshall Islands; Micronesia, Federated States of; and Nauru
KP	Korea, Democratic People's Republic of *see also* Korea, Republic of
KR	Korea, Republic of *see also* Korea, Democratic People's Republic of
	For *Kosovo*, see Serbia
	For *Kurdistan*, see Armenia; Iran, Islamic Republic of; Iraq; Syria, Arab Republic of; and Turkey
KW	Kuwait, Emirate of
KG	Kyrgyzstan
L	
	For *Ladakh Autonomous Hill Development*, see India
	For *Lai Autonomous District*, see India
LA	Lao People's Democratic Republic
LV	Latvia
LB	Lebanon
LS	Lesotho, Kingdom of
LR	Liberia
LY	Libyan Arab Jamahiriya, Socialist People's
LI	Liechtenstein, Principality of
LT	Lithuania
LU	Luxembourg, Grand Duchy of
	For *Luzon*, see Philippines
M	
MO	Macau, Special Administrative Region of *see also* China, People's Republic of; Hong Kong; and Taiwan, Republic of China
MK	Macedonia, the former Yugoslav Republic of
MG	Madagascar
	For *Madeira*, see Portugal
MW	Malawi
	For *Malay Archipelago*, see Malaysia, Kingdom of and Philippines
	For *Malay Peninsula*, see Malaysia, Kingdom of; Myanmar; Philippines; Singapore; and Thailand, Kingdom of

Table 7-1 IANA Country and Region Codes (continued)

Code	Country or Region
MY	Malaysia, Kingdom of *see also* Singapore
MV	Maldives
ML	Mali
MT	Malta
For *Malvinas*, see Falkland Islands (Malvinas Islas), Colony of	
For *Mara Autonomous District*, see India	
MH	Marshall Islands *see also* Kiribati and Micronesia, Federated States of
For *Mariana Islands*, see Northern Mariana Islands, Commonwealth of the	
MQ	Martinique, Overseas Department of the
MR	Mauritania, Islamic Republic of *see also* Mauritius
MU	Mauritius *see also* Mauritania, Islamic Republic of
YT	Mayotte, Territorial Collectivity of
For *McDonald Islands*, see Heard and McDonald Islands, Territory of	
For *Meghalaya*, see India	
For *Melilla*, see Spain	
MX	Mexico
FM	Micronesia, Federated States of *see also* Kiribati; Marshall Islands; and Northern Mariana Islands, Commonwealth of the
For *Mindanao*, see Philippines	
For *Miquelon*, see Saint Pierre and Miquelon, Overseas Territorial Collectivity of	
For *Mizoram*, see India	
For *Moldavia*, see Moldova, Republic of	
MD	Moldova, Republic of
MC	Monaco, Principality of
MN	Mongolia
ME	Montenegro
MS	Montserrat, Territory of
MA	Morocco, Kingdom of
For *Mount Athos*, see Greece	
MZ	Mozambique
MM	Myanmar

Table 7-1 IANA Country and Region Codes (continued)

Code	Country or Region
N	
NA	Namibia *see also* South Africa
NR	Nauru *see also* Kiribati; Marshall Islands; and Micronesia, Federated States of
NP	Nepal, Kingdom of
NL	Netherlands, Kingdom of the *see also* Netherlands Antilles
AN	Netherlands Antilles *see also* Netherlands, Kingdom of the
For *Nevis*, see Saint Kitts and Nevis	
NC	New Caledonia and Dependencies, Overseas Territory of
For *New Guinea*, see Papua New Guinea, Independent State of	
For *New Hebrides*, see Vanuatu	
NZ	New Zealand *see also* Cook Islands; Niue; and Tokelau
NI	Nicaragua
For *Nicobar Islands*, see India	
NE	Niger *see also* Nigeria, Federal Republic of
NG	Nigeria, Federal Republic of *see also* Niger
For *Ningxia Hui Autonomous Region*, see China, People's Republic of	
NU	Niue *see also* Cook Islands; New Zealand; and Tokelau
NF	Norfolk Island, Territory of
For *North Cachar Hills Autonomous District*, see India	
For *North Korea*, see Korea, Democratic People's Republic of	
For *North Sentinel Island*, see India	
MP	Northern Mariana Islands, Commonwealth of the *see also* American Samoa, Territory of, Guam, Territory of, Puerto Rico, Commonwealth of, United States of America, Federal Union of the, and Virgin Islands, U.S. Territory of the
NO	Norway, Kingdom of
O	
OM	Oman, Sultanate of

Table 7-1 IANA Country and Region Codes (continued)

Code	Country or Region
P	
PK	Pakistan, Islamic Republic of
PW	Palau
PS	Palestine, Occupied Territory of *see also* Israel, State of
PA	Panama, Unified Republic of
PG	Papua New Guinea, Independent State of
PC	Paracel Islands, Territory of
PY	Paraguay
For *Peninsular Malaysia*, see Malaysia, Kingdom of	
PE	Peru
PH	Philippines
PN	Pitcairn
PL	Poland
For *Polynesia*, see French Polynesia, Overseas Territory of	
PT	Portugal
TP	*Portuguese Timor* (being phased out)
For *Principe*, see Sao Tome and Principe	
PR	Puerto Rico, Commonwealth of *see also* American Samoa, Territory of, Guam, Territory of, Northern Mariana Islands, Commonwealth of the, United States of America, Federal Union of the, and Virgin Islands, U.S. Territory of the
Q	
QA	Qatar, Emirate of
R	
RE	Reunion, Overseas Department of the
For *Rhodesia*, see Zambia and Zimbabwe	
For *Rodrigues*, see Mauritius	
RO	Romania
RU	Russia, Federation of
RW	Rwanda

Table 7-1 IANA Country and Region Codes (continued)

Code	Country or Region
S	
For *Sahara*, see Western Sahara	
BL	Saint Barthelemy **Note** Although the BL country code exists in *ISO-3166-1 alpha-2*, and exists as a country code top-level domain in DNS, it does not contain any subdomains.
SH	Saint Helena, Ascension and Tristan da Cunha *see also* Ascension Island
KN	Saint Kitts and Nevis
LC	Saint Lucia
MF	Saint Martin **Note** Although the MF country code exists in *ISO-3166-1 alpha-2*, and exists as a country code top-level domain in DNS, it does not contain any subdomains.
PM	Saint Pierre and Miquelon, Overseas Territorial Collectivity of
VC	Saint Vincent and the Grenadines *see also* Grenada
WS	Samoa, Independent State of *see also* American Samoa, Territory of
SM	San Marino
For *Sandwich Islands*, see South Georgia and the South Sandwich Islands	
ST	Sao Tome and Principe
For *Sardinia*, see Italy	
SA	Saudi Arabia, Kingdom of
For *Scotland*, see United Kingdom of Great Britain and Northern Ireland	
SN	Senegal
RS	Serbia
SC	Seychelles
For *Siam*, see Thailand, Kingdom of	
For *Sicily*, see Italy	
SL	Sierra Leone
SG	Singapore *see also* Malaysia, Kingdom of
SK	Slovakia *see also* Czech Republic
SI	Slovenia *see also* Macedonia, the former Yugoslav Republic of
SB	Solomon Islands

Table 7-1 IANA Country and Region Codes (continued)

Code	Country or Region
SO	Somalia
ZA	South Africa *see also* Namibia
GS	South Georgia and the South Sandwich Islands
For *South Korea*, see Korea, Republic of	
For *South Sandwich Islands*, see South Georgia and the South Sandwich Islands	
For *South Yemen*, see Yemen	
For *Southern Sudan*, see Sudan	
SU	Soviet Union (being phased out)
ES	Spain
LK	Sri Lanka
SD	Sudan
For *Sulawesi*, see Indonesia	
For *Sumatra*, see Indonesia	
SR	Suriname
SJ	Svalbard and Jan Mayen Islands, Territory of **Note** **Although the SJ country code exists in *ISO-3166-1 alpha-2*, and exists as a country code top-level domain in DNS, it does not contain any subdomains.**
SZ	Swaziland
SE	Sweden, Kingdom of
CH	Switzerland
SY	Syria, Arab Republic of
T	
TW	Taiwan, Republic of China *see also* China, People's Republic of, Hong Kong, and Macau, Special Administrative Region of
TJ	Tajikistan
For *Tanganyika*, see Tanzania, United Republic of	
TZ	Tanzania, United Republic of
For *Tashkent*, see Uzbekistan	
TH	Thailand, Kingdom of
For *Tibet Autonomous Region*, see China, People's Republic of	
TL	Timor-Leste
For *Tobago*, see Trinidad and Tobago	
TG	Togo

Table 7-1 IANA Country and Region Codes (continued)

Code	Country or Region
TK	Tokelau *see also* Cook Islands; New Zealand; and Niue
TO	Tonga, Kingdom of
For *Trento (Trentino)*, see Austria; Germany, Federal Republic of; Hungary; and Italy	
TT	Trinidad and Tobago
For *Tripura Tribal Areas Autonomous District*, see India	
For *Tristan da Cunha*, see Saint Helena, Ascension and Tristan da Cunha	
TN	Tunisia
TR	Turkey
TM	Turkmenistan
TC	Turks and Caicos Islands, Territory of
TV	Tuvalu
U	
UG	Uganda
UA	Ukraine
AE	United Arab Emirates
GB	United Kingdom of Great Britain and Northern Ireland
UK	**Note** **Although the GB region code exists in *ISO-3166-1 alpha-2*, and exists as a country code top-level domain (ccTLD) in DNS, it contains only one subdomain.** Other United Kingdom sites use UK as their ccTLD. Nonetheless, IANA defined the UK region code, which does not exist in *ISO 3166-1 alpha-2*.
US	United States of America, Federal Union of the *see also* American Samoa, Territory of, Guam, Territory of, Northern Mariana Islands, Commonwealth of the, Puerto Rico, Commonwealth of, and Virgin Islands, U.S. Territory of the
UM	United States Minor Outlying Islands **Note** **Although the UM country code top-level domain was deactivated, it is still available with restrictions.**
UY	Uruguay
UZ	Uzbekistan
V	
VU	Vanuatu
For *Vatican*, see Holy See, State of Vatican City	
VE	Venezuela, Bolivarian Republic of
VN	Viet Nam, Socialist Republic of
VG	Virgin Islands, British Territory of the

Table 7-1 IANA Country and Region Codes (continued)

Code	Country or Region
VI	Virgin Islands, U.S. Territory of *see also* American Samoa, Territory of, Guam, Territory of, Northern Mariana Islands, Commonwealth of the, Puerto Rico, Commonwealth of, and United States of America, Federal Union of the
	For *Visayas*, see Philippines
	For *Vojvodina*, see Serbia
	For *Volta*, see Burkina Faso
W	
	For *Wales*, see United Kingdom of Great Britain and Northern Ireland
WF	Wallis and Futuna Islands, Overseas Territory of
	For *West Bengal*, see Bangladesh and India
EH	Western Sahara **Note Although the EH country code exists in *ISO-3166-1 alpha-2*, it does not exist as a country code top-level domain in DNS.**
X	
	For *Xinjiang Uyghur Autonomous Region*, see China, People's Republic of
Y	
YE	Yemen
YU	Yugoslavia, Federation of **Note Most, if not all, sites that used the YU country code top-level domain have been reassigned to Serbia or Montenegro.**
	For *Yugoslav Republic*, see Bosnia and Herzegovina; Croatia; Macedonia, the former Yugoslav Republic of; Montenegro; Serbia; Slovenia; and Yugoslavia, Federation of
Z	
	For *Zaire*, see Congo, the Democratic Republic of the
ZM	Zambia
	For *Zanzibar*, see Tanzania, United Republic of
	For *Zelaya*, see Nicaragua
ZW	Zimbabwe

FAQs and Troubleshooting

FAQs

Q. What's the difference between a provider-signed certificate and a self-signed certificate?

A. Please compare and contrast these definitions from the "Glossary" section on page 7-2.

- signed
- self-signed

Troubleshooting

Error Messages

Error messages guide you if problems affect your digital certificates. These messages describe a problem and suggest possible ways to solve it.

Error Message `Cannot process CA certificate.`

Explanation **`<exception message>`**

Recommended Action Cause unknown. We cannot recommend any workaround.

Error Message `Cannot unpack` **`<archive file path>`**`.`

Explanation The archive is corrupted or its source was not valid.

Recommended Action Cause unknown. We cannot recommend any workaround.

Error Message `Certificate import failed.`

Explanation An internal error occurred.

Recommended Action Please contact Cisco technical support.

Error Message `Certificate import failed.`

Explanation At least one parameter is not valid.

Recommended Action Cause unknown. We cannot recommend any workaround.

Error Message `Certificate is not readable or does not exist.`

Explanation **<absolute file path>**

Recommended Action Cause unknown. We cannot recommend any workaround.

Error Message `Certificate not yet valid.`

Explanation It takes effect in the future, on **<date in YYYY-MM-DD format>**.

Recommended Action Please check that it is correct.

Error Message `Certificate rejected.`

Explanation It does not match the newest certificate signing request (CSR) for **<FQDN>**.

Recommended Action Please generate a new certificate signing request (CSR), and then contact your certification authority (CA).

Error Message `Certificate rejected.`

Explanation It has expired and is no longer valid.

Recommended Action Please generate a new certificate signing request (CSR), and then contact your certification authority (CA).

Error Message `Certificate rejected.`

Explanation Its subject does not match **<FQDN>**.

Recommended Action Please confirm that you imported the correct identity certificate. Alternatively, please generate a new certificate signing request (CSR), and then contact your certification authority (CA).

Error Message `Internal Error.`

Explanation Cannot build certificate chain.

Recommended Action Confirm that no CA certificates are missing.

Error Message `The certificate chain is broken.`

Explanation An identity certificate is missing for **<FQDN>**.

Recommended Action Please edit the certificate chain to include all digital certificates that your certification authority (CA) has issued to you.

Error Message `Warning! Browsers will reject this certificate.`

Explanation It is self-signed.

Recommended Action We recommend that you use certificates from a valid certification authority (CA).