PKI Trustpool Management

The PKI Trustpool Management feature is used to authenticate sessions, such as HTTPS, that occur between devices by using commonly recognized trusted agents called certificate authorities (CAs). This feature, which is enabled by default, is used to create a scheme to provision, store, and manage a pool of certificates from known CAs in a way similar to the services a browser provides for securing sessions.

Note Effective with Cisco IOS XE Denali 16.3, the way PKI Trustpools are managed have changed. If you are planning to upgrade to this release, please review the changes to the feature captured below as part of *PKI Trustpool Enhancements* section.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for PKI Trustpool Management

The use of certificates requires that a crypto subsystem is included in the Cisco IOS software image.

Restrictions for PKI Trustpool Management

Device certificates that use CA certificates cannot be enrolled in a PKI trustpool.

A bundle cannot have two certificates with the same issuer-name and subject-name pair.

Information About PKI Trustpool Management

CA Certificate Storage in a PKI Trustpool

The router uses a built-in CA certificate bundle that is contained in a special certificate store called a PKI trustpool, which is updated automatically from Cisco. This PKI trustpool is known by Cisco and other vendors. A CA certificate bundle can be in the following formats:

- X.509 certificates in Distinguished Encoding Rules (DER) binary format enveloped within a public-key cryptographic message syntax standard 7 (pkcs7), which is used to sign and encrypt messages under a PKI. An X.509 certificate is a PKI and Privilege Management Infrastructure (PMI) standard that specifies, among other things, standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm.
- A file containing concatenated X.509 certificates in Privacy Enhanced Mail (PEM) format with PEM headers.

Note Flash can also be used as the storage location for the bundles instead of NVRAM.

PKI Trustpool Updating

The PKI trustpool is treated as a single entity that needs to be updated when the following conditions occur:

- A certificate in the PKI trustpool is due to expire or has been reissued.
- The published CA certificate bundle contains additional trusted certificates that are needed by a given application.
- The configuration has been corrupted.

Note A built-in certificate in the PKI trustpool cannot be physically replaced. However, a built-in certificate is rendered inactive after an update if its X.509 subject-name attribute matches the certificate in the CA certificate bundle.

The PKI trustpool can be updated automatically or manually. The PKI trustpool may be used by certficate validation depending upon the application using it. See the "Manually Updating Certificates in the PKI Trustpool" and "Configuring Optional PKI Trustpool Policy Parameters" sections for more information.

Note During auto-update all the existing downloaded trustpool certificates must be deleted.

The PKI trustpool timer matches the CA certificate with the earliest expiration time. If the timer is running and a bundle location is not configured and not explicitly disabled, syslog warnings are issued to alert the administrator that the PKI trustpool policy option is not set.

Automatic PKI trustpool updates use the configured URL.

When the PKI trustpool expires, the policy is read, the bundle is loaded, and the PKI trustpool is replaced. If the automatic PKI trustpool update encounters problems when initiating, then the following schedule is used to initiate the update until the download is successful: 20 days, 15 days, 10 days, 5 days, 4 days, 3 days, 2 days, 1 day, and then once every hour.

CA Handling in Both PKI Trustpool and Trustpoint

There may be circumstances where a CA resides in both PKI trustpool and trustpoint; for example, a trustpoint uses a CA and a CA bundle is downloaded later with the same CA inside. In this scenario, the CA in the trustpoint and the policy of this trustpoint is considered before the CA in the PKI trustpool or PKI trustpool policy to ensure that any current behavior is not altered when the PKI Trustpool Management feature is implemented on the router.

PKI Trustpool Enhancements

In releases earlier than Cisco IOS XE Denali 16.3, the trustpool consists of built-in certificates deployed with every Cisco box and downloaded CA certificates from published bundles. The downloaded certificates are saved in NVRAM, by default. The certificates from the downloaded trustpool bundle would be extracted and stored in the running configuration which was inefficient and utilized too much space.

From Cisco IOS XE Denali 16.3, the PKI trustpool enhancements stores the bundles in the same downloaded bundle format as one file in the storage location (default is NVRAM) instead of individual certificates like in the previous releases. This helps in saving storage memory as the file is in compressed format. Also, the certificates are not displayed individually in the running configuration. On every reboot the bundles are read from the storage location and individual certificates are installed in the database.

This feature removes the current downloaded certificates from the running configuration. The **crypto pki certificate pool** will not have the DER format certificates because these certificates are incompatible with the old NVRAM file and the new images. During upgrade, the trustpool certificates in DER format are lost and the bundles must be reinstalled again in the storage. This is indicated by a syslog during reboot in case of old NVRAM files. The **show crypto pki trustpool** command indicates that the configuration has been

removed. Before you upgrade, use the **show crypto pki trustpool** command to verify that the certificates are available.

The following steps must be followed before upgrading to Cisco IOS XE Denali 16.3 :

- Remove the downloaded trustpool certificates using the **crypto pki trustpool clean** command
- Use the **write memory** command
- Reboot the device
- Download the trustpool bundles using the **crypto pki trustpool import url** command

If you are using trustpool certificates to log into SSH, then you need to follow additional steps to transfer that specific certificate from bundle to a trustpoint. See *Example: Using PKI Trustpool for SSH Connection During Upgrade* for more information.

How to Configure PKI Trustpool Management

Manually Updating Certificates in the PKI Trustpool

The PKI Trustpool Management feature is enabled by default and uses the built-in CA certificate bundle in the PKI trustpool, which receives automatic updates from Cisco. Perform this task to manually update certificates in the PKI trustpool if they are not current, are corrupt, or if certain certificates need to be updated.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpool import clean** [**terminal** | **url** *url*]
4. **crypto pki trustpool import** {**terminal**} {**url** *url* | **ca-bundle**} {**vrf** *vrf-name* | **source interface** *interface-name*}
5. **exit**
6. **show crypto pki trustpool**
7. **show crypto pki trustpool built-in**
8. **show crypto pki trustpool policy**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**crypto pki trustpool import clean** [**terminal** | **url** *url*] **Example:** `Device(config)# crypto pki trustpool import clean`	(Optional) Manually removes all downloaded PKI CA certificates. • The **clean** keyword specifies the removal of the downloaded PKI trustpool certificates before the new certificates are downloaded. • The **terminal** keyword removes the existing CA certificate bundle terminal setting. • The **url** keyword and *url* argument removes the existing URL file system setting.
Step 4	**crypto pki trustpool import** {**terminal**} {**url** *url* | **ca-bundle**} {**vrf** *vrf-name* | **source interface** *interface-name*} **Example:** `Device(config)# crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b`	Manually imports (downloads) the CA certificate bundle into the PKI trustpool to update or replace the existing CA certificate bundle. • The **terminal** keyword specifies the importation of a CA certificate bundle through the terminal (cut-and-paste) in PEM format. • The **url** keyword with the *url* argument specifies the importation of a CA certificate bundle through a URL. This URL can be through a variety of URL file systems such as HTTP. See the *PKI Trustpool Updating* section for more information. In CA bundle, you can use the **crypto pki trustpool import** command to pass the traffic through global VRF. Also, the traffic will not divert through a VRF, when you configure the **crypto pki trustpool policy** command specifying the VRF and source interface.
Step 5	**exit** **Example:** `Device(config)# exit`	Exits global configuration mode.
Step 6	**show crypto pki trustpool** **Example:** `Device(config)# show crypto pki trustpool`	Displays the PKI trustpool certificates of the router in a verbose format.

	Command or Action	Purpose
Step 7	**show crypto pki trustpool built-in** **Example:** `Device(config)# show crypto pki trustpool built-in`	Displays the built-in PKI trustpool certificates of the router in a verbose format.
Step 8	**show crypto pki trustpool policy** **Example:** `Device(config)# show crypto pki trustpool policy`	

Configuring Optional PKI Trustpool Policy Parameters

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto pki trustpool policy**
4. **cabundle url** {*url* | **none**}
5. **chain-validation**
6. **crl** {**cache** {**delete-after** {*minutes* | **none**} | **query** *url*}
7. **default** *command-name*
8. **match certificate** *certificate-map-name* [**allow expired-certificate** | **override** {**cdp directory** *ldap-location* | **ocsp** {*number* **url** *url* | **trustpool** *name number* **url** *url*} | **sia** *number url*} | **skip** [**revocation-check** | **authorization-check**]]
9. **ocsp** {**disable-nonce** | **url** *url*}
10. **revocation-check** *method1* [*method2* [*method3*]]
11. **source interface** *name number*
12. **storage** *location*
13. **vrf** *vrf-name*
14. **show**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Device> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

Step 3	**crypto pki trustpool policy**
	Example:
	`Device(config)# crypto pki trustpool policy`
	`Device(ca-trustpool)#`
		Enters ca-trustpool configuration mode where commands can be accessed to configure CA PKI trustpool policy parameters. The trustpool policy only affects the crl retrieval process and has no effect on trustpool import process.

Step 4	**cabundle url** {*url* | **none**}
	Example:
	`Device(ca-trustpool)# cabundle url`
	`http://www.cisco.com/security/pki/crl/crca2048.crl`
		Specifies the URL from which the PKI trustpool certificate authority CA certificate bundle is downloaded .
		• The *url* argument is the URL of the CA certificate bundle.
		• The **none** keyword specifies that autoupdates of the PKI trustpool CA are not permitted.

Step 5	**chain-validation** **Example:** `Device(ca-trustpool)# chain-validation`	Enables chain validation from the peer's certificate to the root CA certificate in the PKI trustpool. The default has validation stopping at the peer certificate's issuer.

Step 6	**crl** {**cache** {**delete-after** {*minutes* | **none**} | **query** *url*}
	Example:
	`Device(ca-trustpool)# crl query`
	`http://www.cisco.com/security/pki/crl/crca2048.crl`
		Specifies the certificate revocation list (CRL) query and CRL cache options for the PKI trustpool.
		• The **cache** keyword specifies CRL cache options.
		• The **delete-after** keyword removes the CRL from the cache after a timeout.
		• The *minutes* argument is the number of minutes from 1 to 43,200 to wait before deleting the CRL from the cache.
		• The **none** keyword specifies that CRLs are not cached.
		• The **query** keyword with the *url* argument specifies the URL published by the CA server to query the CRL.

	Command or Action	Purpose
Step 7	**default** *command-name* **Example:** `Device(ca-trustpool)# default crl query http://www.cisco.com/security/pki/crl/crca2048.crl`	Resets the value of a ca-trustpool configuration subcommand to its default . • The *command-name* argument is the ca-trustpool configuration mode command with its applicable keywords.
Step 8	**match certificate** *certificate-map-name* [**allow expired-certificate** | **override** {**cdp directory** *ldap-location* | **ocsp** {*number* **url** *url* | **trustpool** *name number* **url** *url*} | **sia** *number url*} | **skip** [**revocation-check** | **authorization-check**]] **Example:** `match certificate mycert override ocsp 1 url http://ocspts.identrust.com`	Enables the use of certificate maps for the PKI trustpool. • The *certifcate-map-name* argument matches the certificate map name. • The optional **allow expired-certificate** keyword ignores expired certificates. **Note** If this keyword is not configured, the router does not ignore expired certificates. • The **override** keyword overrides the online certificate status protocol (OCSP) or SubjectInfoAccess (SIA) attribute fields in a certificate that is in the PKI trustpool. • The **cdp** keyword overrides the certificate distribution point (CDP) in a certificate. • The **directory** keyword and *ldap-location* specifies the CDP in either the http: or ldap: URL, or LDAP directory to override in the certificate. • The **ocsp** keyword and *number* argument and **url** keyword and *url* argument specifies the OCSP sequence number from 0 to 10000 and URL to override in the certificate. • The **trustpool** keyword and *name* and *number* arguments with the **url** keyword and *url* argument override the PKI trustpool for verifying the OCSP certificate by specifying the PKI trustpool name, sequence number, and URL. • The **sia** keyword and *number* and *url* arguments override the SIA URL in a certificate by specifying the SIA sequence number and URL. • The optional **skip revocation-check** keyword combination allows the PKI trustpool to enforce certificate revocation lists (CRLs) except for specific certificates. **Note** If this keyword combination is not configured, then the PKI trustpool enforces CRLs for all certificates. • The optional **skip authorization-check** keyword combination skips the authentication, authorization, and accounting (AAA) check of a certificate when public key

	Command or Action	Purpose
		infrastructure (PKI) integration with an AAA server is configured. **Note** If this keyword combination is not configured, and PKI integration with an AAA server is configured, then the AAA checking of a certificate is done.
Step 9	**ocsp** {**disable-nonce** | **url** *url*} **Example:** `Device(ca-trustpool)# ocsp url http://ocspts.identrust.com`	Specifies OCSP settings for the PKI trustpool. • The **disable-nonce** keyword disables the OCSP Nonce extension. • The **url** keyword and *url* argument specify the OCSP server URL to override (if one exists) in the Authority Info Access (AIA) extension of the certificate. All certificates associated with a configured PKI trustpool are checked by the OCSP server at the specified HTTP URL. The URL can be a hostname, IPv4 address, or an IPv6 address.
Step 10	**revocation-check** *method1* [*method2* [*method3*]] **Example:** `Device(ca-trustpool)# revocation-check ocsp crl none`	Disables revocation checking when the PKI trustpool policy is being used. The *method* argument is used by the router to check the revocation status of the certificate. Available keywords are as follows: • The **crl** keyword performs certificate checking by a certificate revocation list (CRL). This is the default behavior. • The **none** keyword does not require a certificate checking. • The **ocsp** keyword performs certificate checking by an online certificate status protocol (OCSP) server. If a second and third method are specified, each method is used only if the previous method returns an error, such as a server being down.
Step 11	**source interface** *name number* **Example:** `Device(ca-trustpool)# source interface tunnel 1`	Specifies the source interface to be used for CRL retrieval, OCSP status, or the downloading of a CA certificate bundle for the PKI trustpool . • The *name* and *number*arguments are for the interface type and number used as the source address for the PKI trustpool.
Step 12	**storage** *location* **Example:** `Device(ca-trustpool)# storage storage disk0:crca2048.crl`	Specifies a file system location where PKI trustpool certificates are stored on the router. • The *location* is the file system location where the PKI trustpool certificates are stored. The types of file system

	Command or Action	Purpose
		locations are **disk0:**, **disk1:**, **nvram:**, **unix:**, or a named file system.
Step 13	**vrf** *vrf-name* **Example:** `Device(ca-trustpool)# vrf myvrf`	Specifies the VPN routing and forwarding (VRF) instance to be used for enrolment, CRL retrieval, and OCSP status.

Step 14	**show**
	
	Example:
	`Device(ca-trustpool)# show`
	
	`Chain validation will stop at the first CA certificate in the pool`
	`  Trustpool CA certificates will expire 12:58:31 PST Apr 5 2012`
	`  Trustpool policy revocation order:  crl`
	`  Certficate matching is disabled`
	`  Policy Overrides:`
		Displays the PKI trustpool policy of the router.

Configuration examples for PKI Trustpool Management

Example: Configuring PKI Trustpool Management

The following **show crypto pki trustpool** command output displays the certificates in PKI trustpool:

Note The command output in this example is abridged because it is verbose.

```
Device# show crypto pki trustpool

CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 00D01E474000000111C38A964400000002
  Certificate Usage: Signature
  Issuer:
    cn=DST Root CA X3
    o=Digital Signature Trust Co.
  Subject:
    cn=Cisco SSCA
    o=Cisco Systems
  CRL Distribution Points:
    http://crl.identrust.com/DSTROOTCAX3.crl
  Validity Date:
    start date: 12:58:31 PST Apr 5 2007
    end   date: 12:58:31 PST Apr 5 2012

CA Certificate
  Status: Available
```

```
  Version: 3
  Certificate Serial Number (hex): 6A6967B3000000000003
  Certificate Usage: Signature
  Issuer:
    cn=Cisco Root CA 2048
    o=Cisco Systems
  Subject:
    cn=Cisco Manufacturing CA
    o=Cisco Systems
  CRL Distribution Points:
    http://www.cisco.com/security/pki/crl/crca2048.crl
  Validity Date:
    start date: 14:16:01 PST Jun 10 2005
    end   date: 12:25:42 PST May 14 2029
```

The following **show crypto pki trustpool verbose** command output displays the certificates in PKI trustpool:

```
Device# show crypto pki trustpool verbose

CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=Licensing Root - DEV
    o=Cisco
  Subject:
    cn=Licensing Root - DEV
    o=Cisco
  Validity Date:
    start date: 03:25:43 IST Apr 25 2013
    end   date: 03:25:43 IST Apr 25 2033
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (2048 bit)
  Signature Algorithm: SHA256 with RSA Encryption
  Fingerprint MD5: 432CBFA0 32D2983A 8A56A319 FD28C6F9
  Fingerprint SHA1: 6341FCAF 19CE9FEE 961D92A5 D47390B5 2DD6D94D
  X509v3 extensions:
    X509v3 Key Usage: 6000000
      Key Cert Sign
      CRL Signature
    X509v3 Subject Key ID: 43214521 B5FB217A 1A4D1BB7 0236E664 CBEC8B65
    X509v3 Basic Constraints:
        CA: TRUE
    Authority Info Access:
  Associated Trustpoints: Trustpool
  Trustpool: Built-In
```

The following **show crypto pki trustpool built-in** command output displays the built-in certificates in PKI trustpool:

Note The command output in this example is abridged because it is verbose.

```
Device# show crypto pki trustpool built-in

CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 02
  Certificate Usage: Signature
  Issuer:
    cn=Cisco Root CA M2
```

```
    o=Cisco
  Subject:
    cn=Cisco Manufacturing CA SHA2
    o=Cisco
  CRL Distribution Points:
    http://www.cisco.com/security/pki/crl/crcam2.crl
  Validity Date:
    start date: 19:20:58 IST Nov 12 2012
    end   date: 12:02:01 IST Oct 7 1901
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (2048 bit)
  Signature Algorithm: SHA256 with RSA Encryption
  Fingerprint MD5: AC14F08F C3780F8F D9EEE6C9 39111280
  Fingerprint SHA1: 90B2E06B 7AD5DAFF CFD43187 2909F381 37471BF8
    X509v3 Key Usage: 6000000
      Key Cert Sign
      CRL Signature
    X509v3 Subject Key ID: 7AD77995 CABB482B B85514FD A3C00FBC A70F9619
    X509v3 Basic Constraints:
        CA: TRUE
  X509v3 Authority Key ID: C900F91F 8A1FC266 BDA5D26D 650E222E 34C305A0
    Authority Info Access:
    X509v3 CertificatePolicies:
        Policy: 1.3.6.1.4.1.9.21.1.18.0
            Qualifier ID: 1.3.6.1.5.5.7.2.1
            Qualifier Info: http://www.cisco.com/security/pki/policies/index.html
  Associated Trustpoints: Trustpool
  Trustpool: Built-In
```

The following **show crypto pki trustpool policy** command output displays the certificates in PKI trustpool:

```
Device# show crypto pki trustpool policy

Trustpool Policy

   Chain validation will stop at the first CA certificate in the pool
   Trustpool CA certificates will expire 05:29:59 IST Aug 3 2028
   Trustpool policy revocation order:      crl
   Certficate matching is disabled
   Policy Overrides:
```

The following **show crypto pki certificate pool** command output displays the certificates in PKI trustpool:

```
Device# show crypto pki certificate pool

! ('certificate ca' cmd has been deprecated. Downloaded
! Trustpool certificates should be re-downloaded
! using 'crypro pki trustpool import url')
cabundle nvram:ios_core.p7b
```

Example: Using PKI Trustpool for SSH Connection During Upgrade

Before upgrading to Cisco IOS XE Denali 16.3, copy the certificate from trustpool to a new trustpoint.

```
Device # show run | sec pool
crypto pki trustpool policy
 revocation-check none
 source interface GigabitEthernet0/0/0
crypto pki certificate pool
 certificate ca 01
  308204FA 308202E2 A0030201 02020101 300D0609 2A864886 F70D0101 0C050030
  0E310C30 0A060355 04031303 61626330 1E170D31 36303730 35303435 3935335A
  170D3136 30373035 30353535 35335A30 0E310C30 0A060355 04031303 61626330
```

```
  82022230 0D06092A 864886F7 0D010101 05000382 020F0030 82020A02 82020100
  C78AA144 8EC1D18A 4EECC3E8 81450CC7 A85A4C57 AF59E584 5C1EA888 6EF70DA8
  33327D93 E1F6CED7 32BB4FCF 693F60E0 37000225 40F6F9C5 0462C4AD 899E5BDD
  ED779180 D6C75E1B FBE97D42 E2A7B35D DDC18C4D 4CCDE401 68F67A6D E40FD744
  904EE49F 40820640 C6E0B072 510BC40E A0883F6C E8DF5128 EFF3B5F4 B31E5C16
  217652FF AFC30EBF 593CB19C 56C0E793 2814D504 0E079E0C 8E9E856A BCADB19C
  F2376994 A0A040C1 7BC1E88F CF80F218 9C48B4D9 F84ED5C0 79827BD1 32448478
  8F1F82F2 C91A9479 692B6456 C53CF937 777D0C31 1B8A1F5E 24B33553 047C2448
  855CF974 DFA21665 8AD8A0E5 81ED8068 81688997 FF05118C 93A59CA0 7FD594F6
  B7B1898C 272E089A 3392A2C4 22A22625 2BC1E16F 95B2FC15 207CCA49 378AD3A6
  0C574197 C5E94D8C E6736271 CE0BA9AB ACB380E3 A8084243 4E038DD1 8E86E206
  E2269290 F1AFB29A D28CFB3A 5ABADE4A 21A59728 7174E7A3 2FF59C90 E6100C6E
  E2E8CB4C 91BD574D 57B5E18A 78F9CE75 624C4A2E 1A6EFCC3 7D1BB20B 1CC79024
  CD2FBC4D 46BE1B7A 6EFD8F05 6FD84E91 51215E9B E5E952A4 6E2D1388 10075706
  7D6FAF9B 3F7F8994 F39B9B5D 0C7CD5BC 40738877 5D9985AC 5AB6363D 811BA440
  41A1639F 352F4F01 1994300A A4B85B75 01486CA0 4C4B3175 82038B26 BEFE1D2A
  4AC0D577 7784FACF A6877D68 5D73DD04 DC8D942B DE3FC9FE 4C1FF715 A2E7A5AB
  02030100 01A36330 61300F06 03551D13 0101FF04 05300301 01FF300E 0603551D
  0F0101FF 04040302 0186301F 0603551D 23041830 168014CA 195EDBF1 51753A92
  71342CA8 36DDABA9 63A93130 1D060355 1D0E0416 0414CA19 5EDBF151 753A9271
  342CA836 DDABA963 A931300D 06092A86 4886F70D 01010C05 00038202 0100553B
  FB77A348 C4447C40 BEB2DDFD 63C82441 3CBDC198 B5D5B1AB DF17C4E2 98AEAF2F
  CD570939 BCC116E0 33CFF471 E91EE308 8B29B5BD 11DFACF9 A3AC3135 8BE81B22
  ED205587 5DE04654 A051CC14 CA8D2A6E 81F924DA 001BB1C4 7F85F177 4E75D8EA
  797CCAEF 1502492D 17627CD1 E39E295B 44C55884 8E6DFF68 2129B222 18E3187D
  AB97B4A7 6F838E75 A8908566 AD9E6687 35B150DE 0C8C1B37 6F17FDAC 7A7C53A4
  434F5CF3 6EB71957 E65EC5D2 7685B05B A9D8C0D3 2DB8F97E E6B37E11 C9E26F4F
  BFB97745 83E1A214 461B0E49 0FFDEF21 A7CA5364 44416002 03A01F0C 2BC098D3
  B50A4071 AC4D2234 4E55C5D4 0FD9C308 63F2A8D4 24D34613 B73EAA1B B407D56F
  90EEF5C7 AE61C0D8 13FB493D 0E1C8F9B 1D2D6DEA 458CDE18 8753FF14 F8C75213
  35557FCC 50405056 D9790AF0 EAC21646 2D9AF88D 59C05434 45F21248 0BB72191
  74D951DD 9D23997E 1134611E 837137E6 C40C694E 7AB4A05F E8470E87 E0F6D924
  A69A98A8 5AA2B9B3 B7446883 94A7230D EE3C6EDA 4A348351 FC40C16D 6FDC91EC
  CEFF580B F7826DD1 1D1D07DB 17CA3298 8C510826 D2712E04 EB669909 3D8106EB
  5391A5BA 80B7E981 B41AAEB9 CE4A5236 20E30AE7 01D5FDB3 604C5505 0F8C96DC
  8F5CF569 5D90C1FB F5679221 B7B922C0 5F11C379 9EBA283C 45A209F7 132B8DA2
  EAF4751B 290A1CAC C3E7978B 760FB05A 185991FE 4884FA1A D3EEDD7C 63
  3B
        quit
```

Paste the certificate in config mode by creating a new trustpoint.

```
Device(config)#cry pki trust abc
Device(ca-trustpoint)#cry pki cert chain abc
Device(config-cert-chain)#certificate ca 01
```

Enter the certificate in hexadecimal representation

```
Device(config-pki-hexmode)#  308204FA 308202E2 A0030201 02020101 300D0609 2A864886 F70D0101
 0C050030
Device(config-pki-hexmode)#  0E310C30 0A060355 04031303 61626330 1E170D31 36303730 35303435
 3935335A
Device(config-pki-hexmode)#  170D3136 30373035 30353535 35335A30 0E310C30 0A060355 04031303
 61626330
Device(config-pki-hexmode)#  82022230 0D06092A 864886F7 0D010101 05000382 020F0030 82020A02
 82020100
Device(config-pki-hexmode)#  C78AA144 8EC1D18A 4EECC3E8 81450CC7 A85A4C57 AF59E584 5C1EA888
 6EF70DA8
Device(config-pki-hexmode)#  33327D93 E1F6CED7 32BB4FCF 693F60E0 37000225 40F6F9C5 0462C4AD
 899E5BDD
Device(config-pki-hexmode)#  ED779180 D6C75E1B FBE97D42 E2A7B35D DDC18C4D 4CCDE401 68F67A6D
 E40FD744
Device(config-pki-hexmode)#  904EE49F 40820640 C6E0B072 510BC40E A0883F6C E8DF5128 EFF3B5F4
 B31E5C16
Device(config-pki-hexmode)#  217652FF AFC30EBF 593CB19C 56C0E793 2814D504 0E079E0C 8E9E856A
 BCADB19C
Device(config-pki-hexmode)#  F2376994 A0A040C1 7BC1E88F CF80F218 9C48B4D9 F84ED5C0 79827BD1
 32448478
Device(config-pki-hexmode)#  8F1F82F2 C91A9479 692B6456 C53CF937 777D0C31 1B8A1F5E 24B33553
```

```
 047C2448
Device(config-pki-hexmode)#  855CF974 DFA21665 8AD8A0E5 81ED8068 81688997 FF05118C 93A59CA0
 7FD594F6
Device(config-pki-hexmode)#  B7B1898C 272E089A 3392A2C4 22A22625 2BC1E16F 95B2FC15 207CCA49
 378AD3A6
Device(config-pki-hexmode)#  0C574197 C5E94D8C E6736271 CE0BA9AB ACB380E3 A8084243 4E038DD1
 8E86E206
Device(config-pki-hexmode)#  E2269290 F1AFB29A D28CFB3A 5ABADE4A 21A59728 7174E7A3 2FF59C90
 E6100C6E
Device(config-pki-hexmode)#  E2E8CB4C 91BD574D 57B5E18A 78F9CE75 624C4A2E 1A6EFCC3 7D1BB20B
 1CC79024
Device(config-pki-hexmode)#  CD2FBC4D 46BE1B7A 6EFD8F05 6FD84E91 51215E9B E5E952A4 6E2D1388
 10075706
Device(config-pki-hexmode)#  7D6FAF9B 3F7F8994 F39B9B5D 0C7CD5BC 40738877 5D9985AC 5AB6363D
 811BA440
Device(config-pki-hexmode)#  41A1639F 352F4F01 1994300A A4B85B75 01486CA0 4C4B3175 82038B26
 BEFE1D2A
Device(config-pki-hexmode)#  4AC0D577 7784FACF A6877D68 5D73DD04 DC8D942B DE3FC9FE 4C1FF715
 A2E7A5AB
Device(config-pki-hexmode)#  02030100 01A36330 61300F06 03551D13 0101FF04 05300301 01FF300E
 0603551D
Device(config-pki-hexmode)#  0F0101FF 04040302 0186301F 0603551D 23041830 168014CA 195EDBF1
 51753A92
Device(config-pki-hexmode)#  71342CA8 36DDABA9 63A93130 1D060355 1D0E0416 0414CA19 5EDBF151
 753A9271
Device(config-pki-hexmode)#  342CA836 DDABA963 A931300D 06092A86 4886F70D 01010C05 00038202
 0100553B
Device(config-pki-hexmode)#  FB77A348 C4447C40 BEB2DDFD 63C82441 3CBDC198 B5D5B1AB DF17C4E2
 98AEAF2F
Device(config-pki-hexmode)#  CD570939 BCC116E0 33CFF471 E91EE308 8B29B5BD 11DFACF9 A3AC3135
 8BE81B22
Device(config-pki-hexmode)#  ED205587 5DE04654 A051CC14 CA8D2A6E 81F924DA 001BB1C4 7F85F177
 4E75D8EA
Device(config-pki-hexmode)#  797CCAEF 1502492D 17627CD1 E39E295B 44C55884 8E6DFF68 2129B222
 18E3187D
Device(config-pki-hexmode)#  AB97B4A7 6F838E75 A8908566 AD9E6687 35B150DE 0C8C1B37 6F17FDAC
 7A7C53A4
Device(config-pki-hexmode)#  434F5CF3 6EB71957 E65EC5D2 7685B05B A9D8C0D3 2DB8F97E E6B37E11
 C9E26F4F
Device(config-pki-hexmode)#  BFB97745 83E1A214 461B0E49 0FFDEF21 A7CA5364 44416002 03A01F0C
 2BC098D3
Device(config-pki-hexmode)#  B50A4071 AC4D2234 4E55C5D4 0FD9C308 63F2A8D4 24D34613 B73EAA1B
 B407D56F
Device(config-pki-hexmode)#  90EEF5C7 AE61C0D8 13FB493D 0E1C8F9B 1D2D6DEA 458CDE18 8753FF14
 F8C75213
Device(config-pki-hexmode)#  35557FCC 50405056 D9790AF0 EAC21646 2D9AF88D 59C05434 45F21248
 0BB72191
Device(config-pki-hexmode)#  74D951DD 9D23997E 1134611E 837137E6 C40C694E 7AB4A05F E8470E87
 E0F6D924
Device(config-pki-hexmode)#  A69A98A8 5AA2B9B3 B7446883 94A7230D EE3C6EDA 4A348351 FC40C16D
 6FDC91EC
Device(config-pki-hexmode)#  CEFF580B F7826DD1 1D1D07DB 17CA3298 8C510826 D2712E04 EB669909
 3D8106EB
Device(config-pki-hexmode)#  5391A5BA 80B7E981 B41AAEB9 CE4A5236 20E30AE7 01D5FDB3 604C5505
 0F8C96DC
Device(config-pki-hexmode)#  8F5CF569 5D90C1FB F5679221 B7B922C0 5F11C379 9EBA283C 45A209F7
 132B8DA2
Device(config-pki-hexmode)#  EAF4751B 290A1CAC C3E7978B 760FB05A 185991FE 4884FA1A D3EEDD7C
 63
Device(config-pki-hexmode)#  3B
Device(config-pki-hexmode)#        quit
```

Now you can upgrade to Cisco IOS XE Denali 16.3. The certificate from trustpool would disappear but would still stay in trustpoint. Install the certificate in trustpool after the upgrade.

Additional References for PKI Trustpool Management

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Security commands	• Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for PKI Trustpool Management

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for PKI Trustpool Management

Feature Name	Releases	Feature Information
PKI Trustpool Management		The PKI Trustpool Management feature is used to authenticate sessions, such as HTTPS, that occur between devices by using commonly recognized trusted agents called certificate authorities (CAs). This feature, which is enabled by default, is used to create a scheme to provision, store, and manage a pool of certificates from known CAs in a way similar to the services a browser provides for securing sessions. The following commands were introduced or modified: **cabundle url**, **chain-validation (ca-trustpool)**, **crypto pki trustpool import**, **crypto pki trustpool policy**, **crl**, **default (ca-trustpool)**, **match certificate (ca-trustpool)**, **ocsp**, **show (ca-trustpool)**, **show crypto pki trustpool**, **source interface (ca-trustpool)**, **storage**, **vrf (ca-trustpool)**, **show crypto pki trustpool built-in**, **crypto pki trustpool import clean ca-bundle**.
PKI Trustpool Enhancements	Cisco IOS XE Denali 16.3.1	The PKI Trustpool Enhancements feature is used for authentication of HTTPS connections built from the router. The following commands were introduced or modified: **show crypto pki trustpool built-in**, **crypto pki trustpool import clean ca-bundle**.