PKI トラストプール管理

PKI トラストプール管理機能を使用すると、認証局（CA）と呼ばれる一般的に認識された信頼できるエージェントを使用して、デバイス間で発生する HTTPS などのセッションを認証できます。

Trustpool 証明書は、信頼を確立できる既知の CA 証明書です。IOS PKI には両方の CA が組み込まれており、trustpool バンドルをダウンロードするオプションもあります。組み込み CA 証明書は、ダウンロードされた trustpool バンドルの PKCS7 署名を検証するために使用されます。署名の検証に失敗した場合は、trustpool バンドルをダウンロードできます。組み込み trustpool 証明書は削除できます。trustpool 証明書は、SSLVPN、PnP、スマートライセンス、MacSec などのアプリケーションで使用されます。

デフォルトで有効に設定されているこの機能を使用すると、セッションのセキュリティ保護のためにブラウザが提供するサービスと同じ方法で、既知の CA の証明書のプールのプロビジョニング、保管、管理を行うスキーマを作成できます。

（注） 新しいルート証明書は、シスコのプラグ アンド プレイ アプリケーションの組み込み証明書に含まれています。

（注） Cisco IOS XE Denali 16.3 から、PKI トラストプールが管理される方法が変更されました。このリリースへのアップグレードを計画している場合は、「*PKI* トラストプールの拡張」項に含まれる次の機能に対する変更を確認してください。

PKI トラストプール管理の前提条件

証明書を使用するには、暗号化サブシステムが Cisco IOS ソフトウェア イメージに含まれている必要があります。

PKI トラストプール管理の制約事項

CA 証明書を使用するデバイス証明書は PKI トラストプールに登録できません。

トラストプール URL を介してダウンロードできるのは、シスコの署名済み PKCS7 証明書のみです。

PKI トラストプール管理の情報

PKI トラストプール内の CA 証明書の保管場所

ルータは、PKI トラストプールと呼ばれる特別な証明書ストアに格納された内蔵型 CA 証明書バンドルを使用します。これはシスコから自動的に更新されます。この PKI トラストプールは、シスコおよび他のベンダーにも知られています。CA 証明書バンドルは次の形式で提供されます。

- 公開キー暗号化メッセージ構文標準 7（pkcs7）内にエンベロープ化された、Distinguished Encoding Rules（DER）バイナリ形式の X.509 証明書。PKI でメッセージの署名と暗号化に使用します。X.509 証明書は、PKI と権限管理インフラストラクチャ（PMI）の標準で、特に、公開キー証明書の標準形式、証明書失効リスト、属性証明書、および認証パス検証アルゴリズムを指定します。
- PEM ヘッダー付きプライバシー強化メール（PEM）形式の連結型 X.509 証明書を含むファイル。

（注） また、NVRAM の代わりに、バンドルの保管場所としてフラッシュも使用できます。

PKI トラストプールの更新

PKI トラストプールは、次の条件が発生した場合に更新する必要のある単一エンティティとして処理されます。

- PKI トラストプールの証明書が期限切れまたは再発行されている。

- 公開された CA 証明書のバンドルに、特定のアプリケーションで必要な追加の信頼できる証明書が含まれている。
- 設定が破損している。

（注） PKI トラストプールに組み込まれた証明書は物理的に置き換えることができません。ただし、組み込まれた証明書の X.509 所有者名属性が CA 証明書バンドル内の証明書と一致する場合、組み込まれた証明書は無効と表示されます。

PKI トラストプールは自動または手動で更新できます。PKI トラストプールを使用するアプリケーションによっては、PKI トラストプールが証明書検証で使用される場合があります。詳細については「PKI トラストプール内の証明書の手動更新」と「PKI トラストプール ポリシー パラメータの設定」の項を参照してください。

（注） 自動更新が有効になっていると、インポート方法に関係なく、ダウンロードされている既存のすべてのトラストプール証明書（組み込まれたトラストプール証明書を除く）が削除されます。

PKI トラストプール タイマーは、最初に失効する CA 証明書と一致します。タイマーが作動しても、バンドルのロケーションが設定されておらず、明示的に無効になっていない場合、syslog 警告が発効され、PKI トラストプール ポリシー オプションが設定されていないことが管理者に警告されます。

PKI トラストプールの自動更新では設定済み URL を使用します。

PKI トラストプールが失効すると、ポリシーが読み込まれ、バンドルがロードされ、PKI トラストプールが置き換えられます。PKI トラストプールの自動更新の開始時に問題が発生した場合は、ダウンロードが成功するまで、次のスケジュールで更新が開始されます。20 日、15 日、10 日、5 日、4 日、3 日、2 日、1 日、最後に 1 時間ごとです。

PKI トラストプールとトラストポイントの両方での CA 処理

PKI トラストプールとトラストポイントの両方に CA が格納されている場合があります。たとえば、トラストポイントで CA を使用し、CA バンドルが同じ CA 内で後からダウンロードされたりします。このシナリオでは、PKI トラストプール管理機能がルータに実装されても、現在の動作が変更されないようにするため、トラストポイント内の CA とこのトラストポイントのポリシーが、PKI トラストプールまたは PKI トラストプール ポリシーの CA よりも優先されます。

PKI トラストプールの拡張機能

Cisco IOS XE Denali 16.3 より前のリリースでは、トラストプールは、すべてのシスコ ボックスで展開された内蔵型証明書と、公開されたバンドルからダウンロードした CA 証明書で構成さ

れています。ダウンロードした証明書は、デフォルトでは NVRAM に保存されます。ダウンロードしたトラストプールバンドルの証明書は抽出され、非効率的で多くの領域を使用する実行コンフィギュレーションに保存されていました。

Cisco IOS XE Denali 16.3 以降、PKI トラストプールの拡張機能では、これまでのリリースのような個別の証明書の代わりに、保管場所（デフォルトではNVRAM）にあるファイルと同じダウンロードしたバンドル形式でバンドルが保存されます。このため、ファイルが圧縮形式の場合は、ストレージメモリが節約されます。また、証明書は実行コンフィギュレーションでは個別に表示されません。再起動するたびに、バンドルは保存場所から読み取られ、個別の証明書がデータベースにインストールされます。

この機能は、実行コンフィギュレーションから現在のダウンロードした証明書を削除します。これらの証明書は古いNVRAMおよび新しいイメージと互換性がないため、**crypto pki certificate pool** には DER 形式の証明書を指定できません。アップグレード中、DER 形式のトラストプール証明書が失われたら、バンドルを保管場所に再インストールする必要があります。古い NVRAM ファイルの場合、これは再起動時に syslog に記されます。**show crypto pki trustpool** コマンドは、設定が削除されたことを示します。アップグレード前に、**show crypto pki trustpool** コマンドを使用し、証明書が利用可能かどうかを確認します。

Cisco IOS XE Denali 16.3 へのアップグレード前に、次の手順を実行する必要があります。

- **crypto pki trustpool clean** コマンドを使用して、ダウンロードしたトラストプール証明書を削除します
- **write memory** コマンドを使用します。
- デバイスを再起動します。
- **crypto pki trustpool import url** コマンドを使用して、トラストプールバンドルをダウンロードします。

SSHへのログインにトラストプールを使用している場合、追加の手順を実行して、特定の証明書をバンドルからトラストポイントに転送する必要があります。詳細については、「例：アップグレード中の *SSH* 接続に *PKI* トラストプールを使用」を参照してください。

（注） Cisco IOS XE Gibraltar 16.10 リリース以降では、トラストポイントで **match crlsign** コマンドを設定すると、検証中に crlsign がクロスチェックされます。

PKI トラストプール管理の設定方法

PKI トラストプールの証明書の手動更新

PKI トラストプール管理機能はデフォルトで有効で、PKI トラストプールに組み込まれた CA 証明書バンドルを使用し、シスコから自動更新を受信します。PKI トラストプール内の証明書

が最新のものではない、破損している、または特定の証明書を更新する必要がある場合は、次の作業を実行して手動で更新します。

手順の概要

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**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto pki trustpool import clean** [**terminal**	**url** *url*] 例： `Device(config)# crypto pki trustpool import clean`	（任意）ダウンロードしたすべての PKI CA 証明書を手動で削除します。 • **clean** キーワードは、新しい証明書のダウンロードの前に、ダウンロード済みの PKI トラストプール証明書の削除を指定します。 • **terminal** キーワードは、既存の CA 証明書バンドル端末設定を削除します。 • **url** キーワードおよび *url* 引数は、既存の URL ファイル システム設定を削除します。
ステップ 4	**crypto pki trustpool import** {**terminal**} {**url** *url*	**ca-bundle**} {**vrf** *vrf-name*	**source interface** *interface-name*} 例： `Device(config)# crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b`	CA 証明書バンドルを PKI トラストプールに手動でインポート（ダウンロード）したり、既存の CA 証明書バンドルを交換したりします。 • **terminal** キーワードを指定すると、端末（カットアンドペースト）を介して CA 証明書バンドルが PEM 形式でインポートされます。

	コマンドまたはアクション	目的
		• **url** キーワードと *url* 引数を指定すると、URL を介して CA 証明書バンドルがインポートされます。この URL は、HTTP などのさまざまな URL ファイル システムを経由できます。詳細については、「*PKI* トラストプールの更新」の項を参照してください。CA バンドルで、**crypto pki trustpool import** コマンドを使用すると、グローバル VRF を介してトラフィックを転送できます。また、VRF と送信元インターフェイスを指定する **crypto pki trustpool policy** コマンドを設定すると、トラフィックが VRF を介して転送されることはありません。
ステップ 5	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 6	**show crypto pki trustpool** 例： `Device(config)# show crypto pki trustpool`	冗長形式でルータの PKI トラストプール証明書を表示します。

オプション PKI トラストプール ポリシー パラメータの設定

手順の概要

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**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 3	**crypto pki trustpool policy**
	例：
	`Device(config)# crypto pki trustpool policy`
	`Device(ca-trustpool)#`
		CA PKI トラストプール ポリシー パラメータを設定するコマンドにアクセスできる、ca-trustpool コンフィギュレーション モードを入力します。トラストプール ポリシーは crl 検索プロセスにのみ影響し、トラストプール インポート プロセスには影響しません。

ステップ 4	**cabundle url** {*url* | **none**}
	例：
	`Device(ca-trustpool)# cabundle url`
	`http://www.cisco.com/security/pki/crl/crca2048.crl`
		PKI トラストプール認証局の CA 証明書バンドルのダウンロード元となる URL を指定します。
		• *url* 引数は CA 証明書バンドルの URL です。
		• **none** キーワードを指定すると、PKI トラストプール CA の自動更新が許可されません。

ステップ 5	**chain-validation** 例： `Device(ca-trustpool)# chain-validation`	ピアの証明書から PKI トラストプールのルート CA 証明書までチェーン検証を有効にします。デフォルトの検証はピア証明書の発行者で停止します。

ステップ 6	**crl** {**cache** {**delete-after** {*minutes* | **none**} | **query** *url*}
	例：
	`Device(ca-trustpool)# crl query`
	`http://www.cisco.com/security/pki/crl/crca2048.crl`
		PKI トラストプールの証明書失効リスト（CRL）クエリおよび CRL キャッシュ オプションを指定します。
		• **cache** キーワードは CRL キャッシュオプションを指定します。
		• **delete-after** キーワードは、タイムアウト後にキャッシュから CRL を削除します。
		• *minutes* 引数は、キャッシュから CRL が削除されるまで待機する分数（1 ～ 43,200）です。
		• **none** キーワードを指定すると、CRL がキャッシュ化されません。

	コマンドまたはアクション	目的
		• *url* 引数の **query** キーワードは、CRL を照会するために CA サーバーによって公開される URL を指定します。
ステップ 7	**default** *command-name* 例： `Device(ca-trustpool)# default crl query http://www.cisco.com/security/pki/crl/crca2048.crl`	ca-trustpool コンフィギュレーション サブコマンドの値をデフォルト値にリセットします。 • *command-name* 引数は、その適用可能なキーワードを設定した ca-trustpool コンフィギュレーション モード コマンドです。
ステップ 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**]] 例： `match certificate mycert override ocsp 1 url http://ocspts.identrust.com`	PKI トラストプールの証明書マップを使用できるようにします。 • *certifcate-map-name* 引数は証明書マップ名と一致します。 • オプションの **allow expired-certificate** キーワードは、失効した証明書を無視します。 （注） このキーワードを設定しないと、ルータは失効した証明書を無視しません。 • **override** キーワードは、PKI トラストプール内にある証明書の Online Certificate Status Protocol（OCSP）または SubjectInfoAccess（SIA）属性フィールドを上書きします。 • **cdp** キーワードは、証明書の証明書分散ポイント（CDP）を上書きします。 • **directory** キーワードおよび *ldap-location* は、証明書内で上書きする http: または ldap: URL の CDP、あるいは LDAP ディレクトリを指定します。 • **ocsp** キーワードと *number* 引数および **url** キーワードと *url* 引数は、証明書内で上書きする OCSP シーケンス番号（0～10000）および URL を指定します。 • **trustpool** キーワードと *name* や *number* 引数および **url** キーワードと *url* 引数は、PKI トラストプール名、シーケンス番号、URL を指定することで、OCSP 証明書を確認するための PKI トラストプールを上書きします。

	コマンドまたはアクション	目的
		• **sia** キーワードと *number* や *url* 引数は、SIA シーケンス番号と URL を指定することで、証明書内の SIA URL を上書きします。 • オプションの **skip revocation-check** キーワードを組み合わせると、PKI トラストプールが特定の証明書を除いた証明書失効リスト（CRL）を適用できます。 （注） このキーワードの組み合わせを設定しないと、PKI トラストプールはすべての証明書に CRL を適用します。 • オプションの **skip authorization-check** キーワードを組み合わせると、公開キーインフラストラクチャ（PKI）と AAA サーバーとの統合を設定した場合に、証明書の認証、許可、アカウンティング（AAA）の確認をスキップします。 （注） このキーワードの組み合わせを設定せずに、PKI と AAA サーバとの統合を設定すると、証明書の AAA の確認が行われます。
ステップ 9	**ocsp** {**disable-nonce** | **url** *url*} 例： `Device(ca-trustpool)# ocsp url http://ocspts.identrust.com`	PKI トラストプールの OCSP 設定を指定します。 • **disable-nonce** キーワードは OCSP ナンス拡張部を無効にします。 • **url** キーワードと *url* 引数は、証明書の Authority Info Access（AIA）拡張部で上書きする（存在する場合）OCSP サーバーの URL を指定します。設定した PKI トラストプールに関連するすべての証明書は、指定した HTTP URL の OCSP サーバによって確認されます。使用可能な URL は、ホスト名、IPv4 アドレス、または IPv6 アドレスです。
ステップ 10	**revocation-check** *method1* [*method2* [*method3*]] 例：	PKI トラストプール ポリシー使用時の失効確認を無効にします。*method* 引数は、ルータが証明書の失効ステータスを確認するために使用されます。使用可能なキーワードは次のとおりです。

	コマンドまたはアクション	目的
	`Device(ca-trustpool)# revocation-check ocsp crl none`	• **crl** キーワードは、証明書失効リスト（CRL）で証明書の確認を行います。これはデフォルトの動作です。 • **none** キーワードでは、証明書の確認が必要ありません。 • **ocsp** キーワードは、Online Certificate Status Protocol（OCSP）サーバによって証明書の確認を行います。 2 番目と 3 番目の方法を指定した場合、各方法はその直前の方法でエラーが返された場合（サーバがダウンしている場合など）にだけ使用されます。
ステップ 11	**source interface** *name number* 例： `Device(ca-trustpool)# source interface tunnel 1`	CRL の取得、OCSP ステータス、または PKI トラストプールの CA 証明書バンドルのダウンロードに使用する送信元インターフェイスを指定します。 • *name* および *number* 引数は、PKI トラストプールの送信元アドレスとして使用されるインターフェイスのタイプと数値です。
ステップ 12	**storage** *location* 例： `Device(ca-trustpool)# storage storage disk0:crca2048.crl`	PKI トラストプール証明書がルータ上で保存される場合のファイル システム ロケーションを指定します。 • *location* は、PKI トラストプール証明書が保存されるファイル システム ロケーションです。ファイルシステム ロケーションのタイプには、**disk0:**、**disk1:**、**nvram:**、**unix:**、または名前付きファイル システムがあります。
ステップ 13	**vrf** *vrf-name* 例： `Device(ca-trustpool)# vrf myvrf`	登録、CRL の取得、および OCSP ステータスに使用される VPN ルーティングおよび転送（VRF）インスタンスを指定します。

ステップ 14	**show**
	例：
	`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:`
		ルータの PKI トラストプール ポリシーを表示します。

PKI トラストプール管理の設定例

例：PKI トラストプール管理の設定

次の **show crypto pki trustpool** コマンド出力は、PKI トラストプールの証明書を表示します。

（注） この例のコマンド出力は、デバッグのためなので省略されています。

```
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
```

次の **show crypto pki trustpool verbose** コマンド出力は、PKI トラストプールの証明書を表示します。

```
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
```

例：アップグレード中の SSH 接続に PKI トラストプールを使用

Cisco IOS XE Denali 16.3 へアップグレードの前に、トラストプールから新しいトラストポイントに証明書をコピーします。

```
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
```

新しいトラストポイントを作成し、設定モードで証明書を貼り付けます。

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

16 進数で証明書を入力します

```
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
```

これで Cisco IOS XE Denali 16.3 にアップグレードできるようになりました。トラストプールの証明書は消えていますが、トラストポイントにはまだ保管されています。アップグレード後にトラストプールに証明書をインストールします。

PKI トラストプール管理の追加資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』
セキュリティ コマンド	• 『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』[英語]

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

PKI トラストプール管理の機能情報

表 *1 : PKI* トラストプール管理の機能情報

機能名	リリース	機能情報
PKI トラストプール管理		次のコマンドが導入または変更されました。**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**。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。