RSA および証明書コマンド

この章は、次の項で構成されています。

crypto key generate dsa

crypto key generate dsa グローバル コンフィギュレーション モード コマンドは、SSH 公開キーの認証用に DSA キーペアを生成します。

構文

crypto key generate dsa

デフォルト設定

アプリケーションがデフォルト キーを自動的に作成します。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

作成された DSA キーのサイズは 1,024 ビットです。

DSA キーはペアで作成されます。1 つは DSA 公開キー、もう 1 つは DSA 秘密キーです。

デバイスにすでにデフォルトまたはユーザ定義の DSA キーがある場合は、警告が表示され、既存のキーを新しいキーに置き換えるように求められます。

スタートアップ コンフィギュレーションを消去するか、工場出荷時の初期状態に戻すと、デフォルト キーは自動的に削除され、これらはデバイスの初期化中に再作成されます。

このコマンドは、実行コンフィギュレーション ファイルに保存されません。ただし、このコマンドで生成されたキーは実行コンフィギュレーション ファイルに保存されます。

例

次の例では、DSA キー ペアを生成しています。

```
switchxxxxxx(config)# crypto key generate dsa
The SSH service is generating a private DSA key.
This may take a few minutes, depending on the key size.
.....
```

crypto key generate rsa

crypto key generate rsa グローバル コンフィギュレーション モード コマンドは SSH 公開キー認証の RSA キーペアを生成します。

構文

crypto key generate rsa

デフォルト設定

アプリケーションがデフォルト キーを自動的に作成します。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

作成した RSA キーのサイズは 2048 ビットです。

RSA キーはペアで作成されます。1 つは RSA 公開キー、もう 1 つは RSA 秘密キーです。

デバイスにデフォルトまたはユーザ定義の RSA キーがすでにある場合は、警告が表示され、既存のキーを新しいキーに置換するように求められます。

スタートアップ コンフィギュレーションを消去するか、工場出荷時の初期状態に戻すと、デフォルト キーは自動的に削除され、これらはデバイスの初期化中に再作成されます。

このコマンドは、実行コンフィギュレーション ファイルに保存されません。ただし、このコマンドで生成されたキーは実行コンフィギュレーション ファイルに保存されます。

例

次の例では、RSA キーがすでに存在している場合に、RSA キー ペアを生成しています。

```
switchxxxxxx(config)# crypto key generate rsa
Replace Existing RSA Key [y/n]? N
switchxxxxxx(config)#
```

crypto key import

crypto key import グローバル コンフィギュレーション モード コマンドは、DSA/RSA キー ペアをインポートします。

ユーザ キーを削除し、代わりに新しいデフォルトを生成するには、このコマンドの no 形式を使用します。

構文

crypto key import {dsa| rsa}

encrypted crypto key import {dsa| rsa}

no crypto key {**dsa| rsa**}

デフォルト設定

DSA および RSA キー ペアは存在しません。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

インポートされるキーは、RFC 4716 で定義されている形式に従う必要があります。

インポートの DSA キーサイズは 512 ～ 1024 ビットです。

インポートの RSA キーサイズは 1024 ー 2048 ビットです。

DSA/RSA キーはペアでインポートされます。1 つは DSA/RSA 公開キーで、もう 1 つは DSA/RSA 秘密キーです。

デバイスにすでに DSA/RSA キーがある場合は、警告が表示され、既存のキーを新しいキーに置き換えるように求められます。

このコマンドは、実行コンフィギュレーション ファイルに保存されます。

暗号化されたキーワードを使用すると、秘密キーがその暗号化形式でインポートされます。

例

```
switchxxxxxx(config)# encrypted crypto key import rsa
---- BEGIN SSH2 ENCRYPTED PRIVATE KEY ----
switchxxxxxx(config)# encrypted crypto key import rsa
---- BEGIN SSH2 ENCRYPTED PRIVATE KEY ----
Comment: RSA Private Key
84et9C2XUfcRlpemuGINAygnLwfkKJcDM6m2OReALHScqqLhi0wMSSYNlT1IWFZP1kEVHH
Fpt1aECZi7HfGLcp1pMZwjn1+HaXBtQjPDiEtbpScXqrg6ml1/OEnwpFK2TrmUy0Iifwk8
E/mMfX3i/2rRZLkEBea5jrA6Q62gl5naRw1ZkOges+GNeibtvZYSk1jzr56LUr6fT7Xu5i
KMcU2b2NsuSD5yW8R/x0CW2elqDDz/biA2gSgd6FfnW2HV48bTC55eCKrsId2MmjbExUdz
+RQRhzjcGMBYp6HzkD66z8HmShOU+hKd7M1K9U4Sr+Pr1vyWUJlEkOgz9O6aZoIGp4tgm4
VDy/K/G/sI5nVL0+bR8LFUXUO/U5hohBcyRUFO2fHYKZrhTiPT5Rw+PHt6/+EXKG9E+TRs
```

```
lUADMltCRvs+lsB33IBdvoRDdl98YaA2htZay1TkbMqCUBdfl0+74UOqa/b+bp67wCYKe9
yen418MaYKtcHJBQmF7sUQZQGP34VPmOMyZzon68S/ZoT77cy0ihRZx9wcI1yYhJnDiYxP
dgXHYhW6kCTcTj6LrUSQuxCJ9su89ZIWNn5OwdgonLSpvfnabv2GHmmelaveL7JJ/7UcfO
61q5D4PJ67Vk2xL7PqyHXN931rseTzPuJplkSLCFZ5uqTMbWWyQEKmHDlOx35vlGou5tky
9LgIwG4d+9edctZZaggeq5cgjnsZWJgUoB4Bn4hIreyOdHDiFUPPRxkoyhGOGnJuvxC9T9
K6BF1wBTdDQS+Gu47/0/gRoD/50q4sGkzqHsRJJ53WOT0Q1bHMTMLPpwn2nXzvfGxWL/bu
QhZZSqRonG6MX1cP7KT7i4TPq2w2k3TGtNBnVYHx6OoNcaTHmg1N2s5OgRsyXD9tF++6nY
RfMN8CsV+9jQKQP7ZaGc8Ju+d72jvSwppSr032HY+IpzZ4ujkK+/X5oawZL5NnkaEQTQKX
RSL55S4O5NPOjS/pC9hg7GaVjoY2mQ7HDpSUBeTIDTlvOwC2kskA9C6aF/Axj2dXLweQd5
lxk7m0/mMNaiJsNk6y33LcuKjIxpNNjK9n9KzRPkGNMFObprfenWKteDftjQ==
---- END SSH2 PRIVATE KEY ----
---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAABIwAAAIEAvRHsKry6NKMKymb+yWEp9042vupLvYVq3ngt1sB9JH
OcdK/2nw7lCQguy1mLsX8/bKMXYSk/3aBEvaoJQ82+r/nRf0y3HTy4Wp9zV0SiVC8jLD+7
7t0aHejzfUhr0FRhWWcLnvYwr+nmrYDpS6FADMC2hVA85KZRye9ifxT7otE=
---- END SSH2 PUBLIC KEY ----
```

show crypto key

show crypto key 特権 EXEC モード コマンドは、デフォルトとユーザ定義の両方のキーについて、デバイスの SSH 秘密キーおよび公開キーを表示します。

構文

show crypto key [*mypubkey*] [**dsa**| **rsa**]

パラメータ

- ***mypubkey***：公開キーのみを表示します。
- **rsa**：RSA キーを表示します。
- **dsa**：DSA キーを表示します。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このキーペアを表示およびコピーする方法については、「**キーおよび証明書**」を参照してください。

例

次に、デバイスの SSH 公開 DSA キーを表示する例を示します。

```
switchxxxxxx# show crypto key mypubkey dsa
---- BEGIN SSH2 PUBLIC KEY ----
Comment: RSA Public Key
AAAAB3NzaC1yc2EAAAABIwAAAIEAzN31fu56KSEOZdrGVPIJHpAs8G8NDIkB
dqZ2q0QPiKCnLPw0Xsk9tTVKaHZQ5jJbXn81QZpolaPLJIIH3B1cc96D7IFf
VkbPbMRbz24dpuWmPVVLUlQy5nCKdDCui5KKVD6zj3gpuhLhMJor7AjAAu5e
BrIi2IuwMVJuak5M098=
---- END SSH2 PUBLIC KEY ----
Public Key Fingerprint: 6f:93:ca:01:89:6a:de:6e:ee:c5:18:82:b2:10:bc:1e
```

crypto certificate generate

crypto certificate generate グローバル コンフィギュレーション モード コマンドは、HTTPS 用の自己署名証明書を生成します。

構文

crypto certificate *number* **generate** [**key-generate** [*length*]] [**cn** *common- name*] [**ou** *organization-unit*] [**or** *organization*] [**loc** *location*] [**st** *state*] [**cu** *country*] [**duration** *days*]

パラメータ

- ***number***：証明書番号を指定します。(範囲：1 ～ 2)
- **key-generate rsa** *length*：SSL RSA キーを再生成してキー長を指定します（サポートされる長さ：2048（ビット）または 3092（ビット））。

  次の要素は、キーに関連付けることができます。キーが表示されると、それらも表示されます。

  cn *common- name*：完全修飾デバイス URL または IP アドレスを指定します。（長さ：1 ～ 64 文字）。指定しない場合、デフォルトでデバイスの最小の IP アドレスになります（証明書が生成されるとき）。

  ou *organization-unit*：部門または部署名を指定します。（長さ：1 ～ 64 文字）

  or *organization*：組織名を指定します。（長さ：1 ～ 64 文字）

  loc *location*：場所または市区町村名を指定します。（長さ：1 ～ 64 文字）

  st *state*：都道府県名を指定します。（長さ：1 ～ 64 文字）

  cu *country*：国名を指定します。（長さ：2 文字）

  duration *days*：証明書が有効な日数を指定します。（範囲：30 ー 1095）

デフォルト設定

key-generate パラメータを使用しない場合、証明書は既存のキーを使用して生成されます。

SSL の RSA キーのデフォルト長は 2048 です。

デフォルト SSL の EC キーの長さは 256 です。

cn *common- name* を指定しないと、デフォルトでは（証明書の生成時に）デバイスの最小のスタティック IPv6 アドレス、スタティック IPv6 アドレスがない場合にはデバイスの最小のスタティック IPv4 アドレス、スタティック IP アドレスがない場合には 0.0.0.0 に設定されます。

duration *days* を指定しない場合、デフォルトは 730 日です。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

特定の証明書キーが存在しない場合は、**key-generate** パラメータを使用する必要があります。

証明書 1 と 2 の両方が生成されている場合は、**ip https certificate** コマンドを使用して、どちらか一方の証明書を有効化します。

このキーペアを表示およびコピーする方法については、「**キーおよび証明書**」を参照してください。

スタートアップ コンフィギュレーションを消去するか、工場出荷時の初期状態に戻すと、デフォルト キーは自動的に削除され、これらはデバイスの初期化中に再作成されます。

例

次に、キーの長さが 2048 バイトの HTTPS の自己署名証明書を生成する例を示します。

```
switchxxxxxx(config)# crypto certificate 1 generate key-generate 2048
```

crypto certificate request

crypto certificate request 特権 EXEC モード コマンドは、HTTPS 用の証明書要求を生成して表示します。

構文

crypto certificate *number* **request** *[***cn** *common- name*] [**ou** *organization-unit*] [**or** *organization*] [**loc** *location*] [**st** *state*] [**cu** *country]*

パラメータ

- ***number***：証明書番号を指定します。(範囲：1 ～ 2)
- 次の要素は、キーに関連付けることができます。キーが表示されると、それらも表示されます。

  cn *common- name*：完全修飾デバイス URL または IP アドレスを指定します。（長さ：1 ～ 64 文字）。指定しない場合、デフォルトでデバイスの最小の IP アドレスになります（証明書が生成されるとき）。

  ou *organization-unit*：部門または部署名を指定します。（長さ：1 ～ 64 文字）

  or *organization*：組織名を指定します。（長さ：1 ～ 64 文字）

  loc *location*：場所または市区町村名を指定します。（長さ：1 ～ 64 文字）

  st *state*：都道府県名を指定します。（長さ：1 ～ 64 文字）

  cu *country*：国名を指定します。（長さ：2 文字）

デフォルト設定

cn common-name を指定しない場合、デフォルトでは（証明書が生成されたときの）デバイスの最小静的 IPv6 アドレスに設定されるか、または静的 IPv6 アドレスがない場合はデバイスの最小静的 IPv4 アドレスに、静的 IP アドレスがない場合は 0.0.0.0 に設定されます。

コマンド モード

特権 EXEC モード

使用上のガイドライン

このコマンドは、証明機関に証明書要求をエクスポートする場合に使用します。証明書要求は、Base64 でエンコードされた X.509 形式で生成されます。

証明書要求を生成する前に、まず **crypto cerificate generate** コマンドを使用して、自己署名証明書を生成してキーを生成します。証明書のフィールドを再入力する必要があります。

証明機関から証明書を受信したら、**crypto cerificate import** コマンドを使用して、デバイスに証明書をインポートします。この証明書は、自己署名証明書と置き換わります。

例

次の例では、HTTPS 用の証明書要求を表示します。

```
switchxxxxxx# crypto certificate 1 request
-----BEGIN CERTIFICATE REQUEST-----
MIwTCCASoCAQAwYjELMAkGA1UEBhMCUFAxCzAJBgNVBAgTAkNDMQswCQYDVQQH
EwRDEMMAoGA1UEChMDZGxkMQwwCgYDVQQLEwNkbGQxCzAJBgNVBAMTAmxkMRAw
DgKoZIhvcNAQkBFgFsMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC8ecwQ
HdML0831i0fh/F0MV/Kib6Sz5p+3nUUenbfHp/igVPmFM+1nbqTDekb2ymCu6K
aKvEbVLF9F2LmM7VPjDBb9bb4jnxkvwW/wzDLvW2rsy5NPmH1QVl+8Ubx3GyCm
/oW93BSOFwxwEsP58kf+sPYPy+/8wwmoNtDwIDAQABoB8wHQYJKoZIhvcNAQkH
MRDjEyMwgICCAgICAICAgIMA0GCSqGSIb3DQEBBAUAA4GBAGb8UgIx7rB05m+2
m5ZZPhIwl8ARSPXwhVdJexFjbnmvcacqjPG8pIiRV6LkxryGF2bVU3jKEipcZa
g+uNpyTkDt3ZVU72pjz/fa8TF0n3
-----END CERTIFICATE REQUEST-----
```

crypto certificate import

crypto certificate import グローバル コンフィギュレーション モード コマンドは、HTTPS 用の証明機関によって署名された証明書をインポートします。さらに、関連するキーペアもインポートできます。

ユーザ定義のキーおよび証明書を削除するには、このコマンドの no 形式を使用します。

構文

crypto certificate *number* **import**

encrypted crypto certificate *number* **import**

no crypto certificate *number*

パラメータ

- ***number***：証明書番号を指定します。（範囲：1 ～ 2）。

コマンド モード

グローバル コンフィギュレーション モード

使用上のガイドライン

証明書は PEM エンコーディング/ファイル拡張子からインポートする必要があります

セッションを終了する（コマンドラインに戻って次のコマンドを入力する）には、空白行を入力します。

インポートする証明書は、**crypto cerificate request** コマンドで作成される証明書要求に基づく必要があります。

証明書のみをインポートする場合に、証明書にある公開キーがデバイスの SSL キーに一致しないと、コマンドは失敗します。公開キーと証明書の両方をインポートする場合で、証明書にある公開キーがインポートしたキーに一致しない場合、コマンドは失敗します。

このコマンドは、実行コンフィギュレーション ファイルに保存されます。

このコマンドの暗号化形式を使用するときは、秘密キーのみを暗号化形式にする必要があります。

例 1：次の例では、HTTPS の証明機関によって署名された証明書をインポートしています。

```
switchxxxxxx(config)# crypto certificate 1 import
Please paste the input now, add a period (.) on a separate line after the input,and press
 Enter.
-----BEGIN CERTIFICATE-----
MIIBkzCB/QIBADBUMQswCQYDVQQGEwIgIDEKMAgGA1UECBMBIDEKMAgGA1UEBxMB
IDEVMBMGA1UEAxMMMTAuNS4yMzQuMjA5MQowCAYDVQQKEwEgMQowCAYDVQQLEwEg
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDK+beogIcke73sBSL7tC2DMZrY
```

```
OOg9XM1AxfOiqLlQJHd4xP+BHGZWwfkjKjUDBpZn52LxdDu1KrpB/h0+TZP0Fv38
7mIDqtnoF1NLsWxkVKRM5LPka0L/ha1pYxp7EWAt5iDBzSw5sO4lv0bSN7oaGjFA
6t4SW2rrnDy8JbwjWQIDAQABoAAwDQYJKoZIhvcNAQEEBQADgYEAuqYQiNJst6hI
XFDxe7I8Od3Uyt3Dmf7KE/AmUV0Pif2yUluy/RuxRwKhDp/lGrK12tzLQz+s5Ox7
Klft/IcjzbBYXLvih45ASWG3TRv2WVKyWs89rPPXu5hKxggEeTvWqpuS+gXrIqjW
WVZd0n1fXhMacoflgnnEmweIzmrqXBs=
.
-----END CERTIFICATE-----
Certificate imported successfully.
Issued by : C=  , ST= , L= , CN=0.0.0.0, O= , OU=
 Valid From: Jan 24 18:41:24 2011 GMT
Valid to: Jan 24 18:41:24 2012 GMT
Subject: C=US , ST= , L= , CN=router.gm.com, O= General Motors, OU=
 SHA1 Finger print: DC789788 DC88A988 127897BC BB789788
```

例 2：次の例では、HTTPS の証明機関によって署名された証明書、および RSA キーペアをインポートしています。

```
switchxxxxxx(config)# crypto certificate 1 import
Please paste the input now, add a period (.) on a separate line after the input,and press
 Enter.

-----BEGIN RSA PRIVATE KEY-----
ACnrqImEGlXkwxBuZUlAO9nHq9IGJsnkf7/MauGPVqxt5vfDf77uQ5CPf49JWQhu07cVXh
2OwrBhJgB69vLUlJujM9p1IXFpMk8qR3NS7JzlInYAWjHKKbEZBMsKSA6+t/UzVxevKK6H
TGB7vMxi+hv1bL9zygvmQ6+/6QfqA51c4nP/8a6NjO/ZOAgvNAMKNr2Wa+tGUOoAgL0b/C
11EoqzpCq5mT7+VOFhPSO4dUU+NwLv1YCb1Fb7MFoAa0N+y+2NwoGp0pxOvDA9ENYl7qsZ
MWmCfXu52/IxC7fD8FWxEBtks4V81Xqa7K6ET657xS7m8yTJFLZJyVawGXKnIUs6uTzhhW
dKWWc0e/vwMgPtLlWyxWynnaP0fAJ+PawOAdsK75bo79NBim3HcNVXhWNzqfg2s3AYCRBx
WuGoazpxHZ0s4+7swmNZtS0xI4ek43d7RaoedGKljhPqLHuzXHUon7Zx15CUtP3sbHl+XI
B3u4EEcEngYMewy5obn1vnFSot+d5JHuRwzEaRAIKfbHa34alVJaN+2AMCb0hpI3IkreYo
A8Lk6UMOuIQaMnhYf+RyPXhPOQs01PpIPHKBGTi6pj39XMviyRXvSpn5+eIYPhve5jYaEn
UeOnVZRhNCVnruJAYXSLhjApf5iIQr1JiJb/mVt8+zpqcCU9HCWQqsMrNFOFrSpcbHu5V4
ZX4jmd9tTJ2mhekoQf1dwUZbfYkRYsK70ps8u7BtgpRfSRUr7g0LfzhzMuswoDSnB65pkC
ql7yZnBeRS0zrUDgHLLRfzwjwmxjmwObxYfRGMLp4=
-----END RSA PRIVATE KEY-----
-----BEGIN RSA PUBLIC KEY-----
MIGHAoGBAMVuFgfJYLbUzmbm6UoLD3ewHYd1ZMXY4A3KLF2SXUd1TIXq84aME8DIitSfB2
Cqy4QB5InhgAobBKC96VRsUe2rzoNG4QDkj2L9ukQOvoFBYNmbzHc7a+7043wfVmH+QOXf
TbnRDhIMVrZJGbzl1c9IzGky1l21Xmicy0/nwsXDAgEj

-----END RSA PUBLIC KEY-----
-----BEGIN CERTIFICATE-----
MIIBkzCB/QIBADBUMQswCQYDVQQGEwIgIDEKMAgGA1UECBMBIDEKMAgGA1UEBxMB
IDEVMBMGA1UEAxMMMTAuNS4yMzQuMjA5MQowCAYDVQQKEwEgMQowCAYDVQQLEwEg
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDK+beogIcke73sBSL7tC2DMZrY
OOg9XM1AxfOiqLlQJHd4xP+BHGZWwfkjKjUDBpZn52LxdDu1KrpB/h0+TZP0Fv38
7mIDqtnoF1NLsWxkVKRM5LPka0L/ha1pYxp7EWAt5iDBzSw5sO4lv0bSN7oaGjFA
6t4SW2rrnDy8JbwjWQIDAQABoAAwDQYJKoZIhvcNAQEEBQADgYEAuqYQiNJst6hI
XFDxe7I8Od3Uyt3Dmf7KE/AmUV0Pif2yUluy/RuxRwKhDp/lGrK12tzLQz+s5Ox7
Klft/IcjzbBYXLvih45ASWG3TRv2WVKyWs89rPPXu5hKxggEeTvWqpuS+gXrIqjW
WVZd0n1fXhMacoflgnnEmweIzmrqXBs=
-----END CERTIFICATE-----
.
Certificate imported successfully.
Issued by : C=  , ST= , L= , CN=0.0.0.0, O= , OU=
 Valid From: Jan 24 18:41:24 2011 GMT
Valid to: Jan 24 18:41:24 2012 GMT
Subject: C=US , ST= , L= , CN=router.gm.com, O= General Motors, OU=
 SHA1 Finger print: DC789788 DC88A988 127897BC BB789788
```

例 3：暗号化されたキーで証明書をインポートしています。

```
switchxxxxxx(config)# encrypted crypto certificate 1 import
-----BEGIN RSA ENCRYPTED PRIVATE KEY-----
```

```
wJIjj/tFEI/Z3GFkTl5C+SFOeSyTxnSsfssNo9CoHJ6X9Jg1SukjtXU49kaUbTjoQVQatZ
AdQwgWM5mnjUhUaJ1MM3WfrApY7HaBL3iSXS9jDVrf++Q/KKhVH6Pxlv6cKvYYzHg43Unm
CNI2n5zf9oisMH0U6gsIDs4ysWVD1zNgoVQwD7RqKpL9wo3+YVFVS6XCB7pDb7iPePefa6
GD/crN28vTLGf/NpyKoOhdAMRuwEQoapMo0Py2Cvy+sqLiv4ZKck1FPlsVFV7X7sh+zVa3
We84pmzyjGiY9S0tPdBSGhJ2xDNcqTyvUpffFEJJYrdGKGybqD0o3tD/ioUQ3UJgxDbGYw
aLlLoavSjMYiWkdPjfcbn5MVRdU5iApCQJXWv3MYC8GQ4HDa6UDN6aoUBalUhqjT+REwWO
DXpJmvmX4T/u5W4DPvELqTHyETxgQKNErlO7gRi2yyLcybUokh+SP+XuRkG4IKnn8KyHtz
XeoDojSe6OYOQww2R0nAqnZsZPgrDzj0zTDL8qvykurfW4jWa4cv1Sc1hDEFtHH7NdDLjQ
FkPFNAKvFMcYimidapG+Rwc0m3lKBLcEpNXpFEE3v1mCeyN1pPe6eSqMcBXa2VmbInutuP
CZM927oxkb41g+U5oYQxGhMK7OEzTmfS1FdLOmfqv0DHZNR4lt4KgqcSjSWPQeYSzB+4PW
Qmy4fTF4wQdvCLy+WlvEP1jWPbrdCNxIS13RWucNekrm9uf5Zuhd1FA9wf8XwSRJWuAq8q
zZFRmDMHPtey9ALO2alpwjpHOPbJKiCMdjHT94ugkF30eyeni9sGN6Y063IvuKBy0nbWsA
J0sxrvt3q6cbKJYozMQE5LsgxLNvQIH4BhPtUz+LNgYWb3V5SI8D8kRejqBM9eaCyJsvLF
+yAI5xABZdTPqz0l7FNMzhIrXvCqcCCCx+JbgP1PwYTDyD+m2H5v8Yv6sT3y7fZC9+5/Sn
Vf8jpTLMWFgVF9U1Qw9bA8HA7K42XE3R5Zr1doOeUrXQUkuRxLAHkifD7ZHrE7udOmTiP9
W3PqtJzbtjjvMjm5/C+hoC6oLNP6qp0TEn78EdfaHpMMutMF0leKuzizenZQ==
-----END RSA PRIVATE KEY-----
-----BEGIN RSA PUBLIC KEY-----
MIGJAoGBAMoCaK+b9hTgrzEeWjdz55FoWwV8s54k5VpuRtv1e5r1zp7kzIL6mvCCXk6J9c
kkr+TMfX63b9t5RgwGPgWeDHw3q5QkaqInzz1h7j2+A++mwCsHui1BhpFNFY/gmENiGq9f
puukcnoTvBNvz7z3VOxv6hw1UHMTOeO+QSbe7WwVAgMBAAE=
-----END RSA PUBLIC KEY-----
-----BEGIN CERTIFICATE-----
MIICHDCCAYUCEFCcI4/dhLsUhTWxOwbzngMwDQYJKoZIhvcNAQEEBQAwTzELMAkG
A1UEBhMCICAxCjAIBgNVBAgTASAxCjAIBgNVBAcTASAxEDAOBgNVBAMTBzAuMC4w
LjAxCjAIBgNVBAoTASAxCjAIBgNVBAsTASAwHhcNMTIwNTIxMTI1NzE2WhcNMTMw
NTIxMTI1NzE2WjBPMQswCQYDVQQGEwIgIDEKMAgGA1UECBMBIDEKMAgGA1UEBxMB
IDEQMA4GA1UEAxMHMC4wLjAuMDEKMAgGA1UEChMBIDEKMAgGA1UECxMBIDCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAygJor5v2FOCvMR5aN3PnkWhbBXyzniTl
Wm5G2/V7mvXOnuTMgvqa8IJeTon1ySSv5Mx9frdv23lGDAY+BZ4MfDerlCRqoifP
PWHuPb4D76bAKwe6LUGGkU0Vj+CYQ2Iar1+m66RyehO8E2/PvPdU7G/qHDVQcxM5
475BJt7tbBUCAwEAATANBgkqhkiG9w0BAQQFAAOBgQBOknTzas7HniIHMPeC5yC0
2rd7c+zqQOe1e4CpEvVlOC0QGvPa72pz+m/zvoFmAC5WjQngQMMwH8rNdvrfaSyE
dkB/761PpeKkUtgyPHfTzfSMcJdBOPPnpQcqbxCFh9QSNa4ENSXqC5pND02RHXFx
wS1XJGrhMUoNGz1BY5DJWw==
-----END CERTIFICATE-----
.
Certificate imported successfully.
Issued by : C=  , ST= , L= , CN=0.0.0.0, O= , OU=
 Valid From: Jan 24 18:41:24 2011 GMT
Valid to: Jan 24 18:41:24 2012 GMT
Subject: C=US , ST= , L= , CN=router.gm.com, O= General Motors, OU=
 SHA1 Finger print: DC789788 DC88A988 127897BC BB789788
Example 3 - Import certificate with encrypted key
encrypted crypto certificate 1 import
-----BEGIN RSA ENCRYPTED PRIVATE KEY-----
wJIjj/tFEI/Z3GFkTl5C+SFOeSyTxnSsfssNo9CoHJ6X9Jg1SukjtXU49kaUbTjoQVQatZ
AdQwgWM5mnjUhUaJ1MM3WfrApY7HaBL3iSXS9jDVrf++Q/KKhVH6Pxlv6cKvYYzHg43Unm
CNI2n5zf9oisMH0U6gsIDs4ysWVD1zNgoVQwD7RqKpL9wo3+YVFVS6XCB7pDb7iPePefa6
GD/crN28vTLGf/NpyKoOhdAMRuwEQoapMo0Py2Cvy+sqLiv4ZKck1FPlsVFV7X7sh+zVa3
We84pmzyjGiY9S0tPdBSGhJ2xDNcqTyvUpffFEJJYrdGKGybqD0o3tD/ioUQ3UJgxDbGYw
aLlLoavSjMYiWkdPjfcbn5MVRdU5iApCQJXWv3MYC8GQ4HDa6UDN6aoUBalUhqjT+REwWO
DXpJmvmX4T/u5W4DPvELqTHyETxgQKNErlO7gRi2yyLcybUokh+SP+XuRkG4IKnn8KyHtz
XeoDojSe6OYOQww2R0nAqnZsZPgrDzj0zTDL8qvykurfW4jWa4cv1Sc1hDEFtHH7NdDLjQ
FkPFNAKvFMcYimidapG+Rwc0m3lKBLcEpNXpFEE3v1mCeyN1pPe6eSqMcBXa2VmbInutuP
CZM927oxkb41g+U5oYQxGhMK7OEzTmfS1FdLOmfqv0DHZNR4lt4KgqcSjSWPQeYSzB+4PW
Qmy4fTF4wQdvCLy+WlvEP1jWPbrdCNxIS13RWucNekrm9uf5Zuhd1FA9wf8XwSRJWuAq8q
zZFRmDMHPtey9ALO2alpwjpHOPbJKiCMdjHT94ugkF30eyeni9sGN6Y063IvuKBy0nbWsA
J0sxrvt3q6cbKJYozMQE5LsgxLNvQIH4BhPtUz+LNgYWb3V5SI8D8kRejqBM9eaCyJsvLF
+yAI5xABZdTPqz0l7FNMzhIrXvCqcCCCx+JbgP1PwYTDyD+m2H5v8Yv6sT3y7fZC9+5/Sn
Vf8jpTLMWFgVF9U1Qw9bA8HA7K42XE3R5Zr1doOeUrXQUkuRxLAHkifD7ZHrE7udOmTiP9
W3PqtJzbtjjvMjm5/C+hoC6oLNP6qp0TEn78EdfaHpMMutMF0leKuzizenZQ==
-----END RSA PRIVATE KEY-----
-----BEGIN RSA PUBLIC KEY-----
```

```
MIGJAoGBAMoCaK+b9hTgrzEeWjdz55FoWwV8s54k5VpuRtv1e5r1zp7kzIL6mvCCXk6J9c
kkr+TMfX63b9t5RgwGPgWeDHw3q5QkaqInzz1h7j2+A++mwCsHui1BhpFNFY/gmENiGq9f
puukcnoTvBNvz7z3VOxv6hw1UHMTOeO+QSbe7WwVAgMBAAE=
-----END RSA PUBLIC KEY-----
-----BEGIN CERTIFICATE-----
MIICHDCCAYUCEFCcI4/dhLsUhTWxOwbzngMwDQYJKoZIhvcNAQEEBQAwTzELMAkG
A1UEBhMCICAxCjAIBgNVBAgTASAxCjAIBgNVBAcTASAxEDAOBgNVBAMTBzAuMC4w
LjAxCjAIBgNVBAoTASAxCjAIBgNVBAsTASAwHhcNMTIwNTIxMTI1NzE2WhcNMTMw
NTIxMTI1NzE2WjBPMQswCQYDVQQGEwIgIDEKMAgGA1UECBMBIDEKMAgGA1UEBxMB
IDEQMA4GA1UEAxMHMC4wLjAuMDEKMAgGA1UEChMBIDEKMAgGA1UECxMBIDCBnzAN
BgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAygJor5v2FOCvMR5aN3PnkWhbBXyzniTl
Wm5G2/V7mvXOnuTMgvqa8IJeTon1ySSv5Mx9frdv23lGDAY+BZ4MfDerlCRqoifP
PWHuPb4D76bAKwe6LUGGkU0Vj+CYQ2Iar1+m66RyehO8E2/PvPdU7G/qHDVQcxM5
475BJt7tbBUCAwEAATANBgkqhkiG9w0BAQQFAAOBgQBOknTzas7HniIHMPeC5yC0
2rd7c+zqQOe1e4CpEvV1OC0QGvPa72pz+m/zvoFmAC5WjQngQMMwH8rNdvrfaSyE
dkB/761PpeKkUtgyPHfTzfSMcJdBOPPnpQcqbxCFh9QSNa4ENSXqC5pND02RHXFx
wS1XJGrhMUoNGz1BY5DJWw==
-----END CERTIFICATE-----
.
Certificate imported successfully.
Issued by : C=  , ST= , L= , CN=0.0.0.0, O= , OU=
 Valid From: Jan 24 18:41:24 2011 GMT
Valid to: Jan 24 18:41:24 2012 GMT
Subject: C=US , ST= , L= , CN=router.gm.com, O= General Motors, OU=
 SHA1 Finger print: DC789788 DC88A988 127897BC BB789788
```

show crypto certificate

show crypto certificate 特権 EXEC モード コマンドを使用すると、デフォルト キーとユーザ定義キーの両方について、デバイスの SSH 証明書とキーペアが表示されます。

構文

show crypto certificate [mycertificate] [*number*]

パラメータ

- ***number***：証明書番号を指定します。（範囲：1、2）
- **mycertificate**：証明書のみを表示することを指定します。

デフォルト設定

両方のキーを表示します。

コマンド モード

特権 EXEC モード

例

次に、デバイスに存在する SSL 証明書番号 1 およびキー ペアを表示する例を示します。

```
switchxxxxxx# show crypto certificate 1
Certificate 1:
Certificate Source: Default
-----BEGIN CERTIFICATE-----
dHmUgUm9vdCBDZXJ0aWZpZXIwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAp4HS
nnH/xQSGA2ffkRBwU2XIxb7n8VPsTm1xyJ1t11a1GaqchfMqqe0kmfhcoHSWr
yf1FpD0MWOTgDAwIDAQABo4IBojCCAZ4wEwYJKwYBBAGCNxQCBAYeBABDAEEw
CwR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFAf4MT9BRD47
ZvKBAEL9Ggp+6MIIBNgYDVR0fBIIBLTCCASkwgdKggc+ggcyGgclsZGFwOi8v
L0VByb3h5JTIwU29mdHdhcmUlMjBSb290JTIwQ2VydGlmaWVyLENOPXNlcnZl
-----END CERTIFICATE-----

----BEGIN RSA PRIVATE KEY-----
ACnrqImEGlXkwxBuZUlAO9nHq9IGJsnkf7/MauGPVqxt5vfDf77uQ5CPf49JWQhu07cVXh
2OwrBhJgB69vLUlJujM9p1IXFpMk8qR3NS7JzlInYAWjHKKbEZBMsKSA6+t/UzVxevKK6H
TGB7vMxi+hv1bL9zygvmQ6+/6QfqA51c4nP/8a6NjO/ZOAgvNAMKNr2Wa+tGUOoAgL0b/C
11EoqzpCq5mT7+VOFhPSO4dUU+NwLv1YCb1Fb7MFoAa0N+y+2NwoGp0pxOvDA9ENYl7qsZ
MWmCfXu52/IxC7fD8FWxEBtks4V81Xqa7K6ET657xS7m8yTJFLZJyVawGXKnIUs6uTzhhW
dKWWc0e/vwMgPtLlWyxWynnaP0fAJ+PawOAdsK75bo79NBim3HcNVXhWNzqfg2s3AYCRBx
WuGoazpxHZ0s4+7swmNZtS0xI4ek43d7RaoedGKljhPqLHuzXHUon7Zx15CUtP3sbHl+XI
B3u4EEcEngYMewy5obn1vnFSot+d5JHuRwzEaRAIKfbHa34alVJaN+2AMCb0hpI3IkreYo
A8Lk6UMOuIQaMnhYf+RyPXhPOQs01PpIPHKBGTi6pj39XMviyRXvSpn5+eIYPhve5jYaEn
UeOnVZRhNCVnruJAYXSLhjApf5iIQr1JiJb/mVt8+zpqcCU9HCWQqsMrNFOFrSpcbHu5V4
ZX4jmd9tTJ2mhekoQf1dwUZbfYkRYsK70ps8u7BtgpRfSRUr7g0LfzhzMuswoDSnB65pkC
ql7yZnBeRS0zrUDgHLLRfzwjwmxjmwObxYfRGMLp4=
-----END RSA PRIVATE KEY-----
-----BEGIN RSA PUBLIC KEY-----
MIGHAoGBAMVuFgfJYLbUzmbm6UoLD3ewHYd1ZMXY4A3KLF2SXUd1TIXq84aME8DIitSfB2
```

```
Cqy4QB5InhgAobBKC96VRsUe2rzoNG4QDkj2L9ukQOvoFBYNmbzHc7a+7043wfVmH+QOXf
TbnRDhIMVrZJGbzl1c9IzGky1l21Xmicy0/nwsXDAgEj

-----END RSA PUBLIC KEY-----
Issued by: www.verisign.com
Valid from: 8/9/2003 to 8/9/2004
Subject: CN= router.gm.com, 0= General Motors, C= US
Finger print: DC789788 DC88A988 127897BC BB789788
```

show crypto certificate chain

show crypto certificate chain 特権 EXEC モードコマンドを使用すると、デフォルトキーとユーザー定義キーの両方について、デバイスの SSL 証明書とキーペアが表示されます。

構文

show crypto certificate chain [*number*]

パラメータ

- *number*（オプション）：証明書番号を指定します。（範囲：1、2）

デフォルト設定

両方のキーを表示します。

コマンド モード

特権 EXEC モード

例

次に、証明書 1 チェーンを表示する例を示します。

switchxxxxxx# show crypto certificate chain 1

Certificate Chain - server certificate 1 (Active)

==========

Sever Certificate

Status: valid

Serial Number:

00:16:c9:af:00:2c:7b:06:11:5b:39:3e:de:c4:04:d4:63:11:22:11

Issuer: cn=Intermediate 2 CA, ou=issDept, o=MyInterCA, st=NA, c=US

Subject: cn= momo.company.com, ou=Depd, o=myCompany, st=NA, c=US

Validity:

Not Before: Nov 14 21:06:28 2023 EST

Not After: Nov 09 21:06:28 2043 SET

Intermediate CA Certificate – Inter2

Status: valid

Serial Number: 55:16:c9:af:00:2c:7b:06:11:5b:39:3e:de:c4:04:d4:63:11:22:55

Issuer: cn= My Root CA, ou=RootIss, o=MyRootCA, st=NA, c=US

Subject: cn= Intermediate 2 CA, ou=issDept, o=MyInterCA, st=NA, c=US

Validity:

Not Before: Nov 14 21:06:28 2023 EST

Not After: Nov 09 21:06:28 2043 EST

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。