



Exporting and Importing RSA Keys

The Exporting and Importing RSA Keys feature allows you to transfer security credentials between devices by exporting and importing Rivest, Shamir, and Adelman (RSA) keys. The keypair that is shared between two devices will allow one device to immediately and transparently take over the functionality of the other router.

Feature Specifications for the Exporting and Importing RSA Keys Feature

Feature History

Release	Modification
12.2(15)T	This feature was introduced.

Supported Platforms

For platforms supported in Cisco IOS Release 12.2(15)T, consult Cisco Feature Navigator.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at <http://www.cisco.com/go/fn>. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

- [Prerequisites for Exporting and Importing RSA Keys, page 2](#)
- [Restrictions for Exporting and Importing RSA Keys, page 2](#)
- [Information About Exporting and Importing RSA Keys, page 2](#)
- [How to Export and Import RSA Keys, page 3](#)
- [Configuration Examples for Using the Exporting and Importing RSA Keys Feature, page 7](#)
- [Additional References, page 9](#)
- [Command Reference, page 11](#)
- [Glossary, page 18](#)

Prerequisites for Exporting and Importing RSA Keys

You must generate RSA keys that have been specified as exportable before you can import them.

Restrictions for Exporting and Importing RSA Keys

You cannot export and import RSA keys that existed on the router before your system was upgraded to Cisco IOS Release 12.2(15)T or higher. You have to generate new RSA keys after you upgrade the Cisco IOS software.

After you have exported RSA keys and imported them to a target router, you cannot then export the RSA keys from the target router to another router.

When you import a PKCS12 file that was generated by a third-party application, the PKCS12 file must include a root certification authority (CA) certificate.

Information About Exporting and Importing RSA Keys

Before configuring and implementing the Exporting and Importing RSA Keys feature, you should understand the following concepts:

- [Benefits of Exporting and Importing RSA Keys, page 2](#)
- [Passphrase Protection, page 2](#)

Benefits of Exporting and Importing RSA Keys

The Exporting and Importing RSA Keys feature allows you to share the private RSA key pair of a router with standby routers, therefore transferring the security credentials between networking devices. The key pair that is shared between two routers will allow one router to immediately and transparently take over the functionality of the other router. If the main router were to fail, the standby router could be dropped into the network to replace the failed router without the need to regenerate keys, reenroll in CA, or manually redistribute keys.

You can also use the Exporting and Importing RSA Keys feature to place the same RSA key pair on multiple routers, so that all management stations using Secure Shell (SSH) can be configured with a single public RSA key.

Passphrase Protection

You have to include a passphrase to encrypt the pkcs12 file that has been exported, and the same passphrase has to be entered when the PKCS12 file is imported, in order to decrypt it. Encrypting the PKCS12 file when it is being exported or imported protects the file from unauthorized access and use while it is on a local device.

**Caution**

Passphrase protection protects the PKCS12 file from unauthorized access and use, but it cannot protect the RSA keypair from a user who has full enable access to the running router.

The passphrase can be any phrase and can include spaces and punctuation, excluding the question mark (?), which has special meaning to the Cisco IOS parser.

How to Export and Import RSA Keys

This section contains the following procedures:

- [Generating and Verifying the RSA Key Pair, page 3](#)
- [Exporting the RSA Key Pair, page 4](#)
- [Importing the RSA Key Pair to the Target Router, page 5](#)
- [Verifying the Importation of the RSA Key Pair to the Target Router, page 6](#)

Generating and Verifying the RSA Key Pair

This section provides the steps necessary to generate and label an RSA key pair and verify that it has been generated.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto key generate rsa {general-keys | usage-keys} [label *key-label*] exportable**
4. **exit**
5. **show crypto key mypubkey rsa**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto key generate rsa {general-keys usage-keys} [label <i>key-label</i>] exportable Example: Router(config)# crypto key generate rsa general-keys label mykeys exportable	Generates RSA key pairs.

	Command or Action	Purpose
Step 4	<code>exit</code> Example: Router(config)# <code>exit</code>	Returns to EXEC mode.
Step 5	<code>show crypto key mypubkey rsa</code> Example: Router(config)# <code>show crypto key mypubkey rsa</code>	Displays the RSA public key(s) of your router.

Exporting the RSA Key Pair

This section provides the steps necessary to export the RSA key pair.


Internet Key Exchange (IKE) can use RSA keys directly, but for exporting or importing RSA key pairs, you must create a trustpoint that is associated with the key pair. When you export the trustpoint, you are in effect exporting the RSA key pair associated with the trustpoint.

SUMMARY STEPS

1. `enable`
2. `configure terminal`
3. `crypto ca trustpoint name`
4. `rsa keypair key-label [key-size [encryption-key-size]]`
5. `exit`
6. `crypto ca export trustpointname pkcs12 destination url passphrase`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code> Example: Router> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	<code>configure terminal</code> Example: Router# <code>configure terminal</code>	Enters global configuration mode.
Step 3	<code>crypto ca trustpoint name</code> Example: Router(config)# <code>crypto ca trustpoint mytp</code>	Declares the CA that your router should use. Creates the trustpoint name to be associated with the RSA key pair and enters CA trustpoint mode.

	Command or Action	Purpose
Step 4	<pre>rsakeypair key-label [key-size [encryption-key-size]]</pre> <p>Example: Router(ca-trustpoint)# rsakeypair southkeys</p>	<p>Specifies which key pair to associate with the certificate.</p> <p>Names the key pair to be used with the trustpoint.</p>
Step 5	<pre>exit</pre> <p>Example: Router(ca-trustpoint)# exit</p>	<p>Returns to global configuration mode.</p>
Step 6	<pre>crypto ca export trustpointname pkcs12 destination url passphrase</pre> <p>Example: Router(config)# crypto ca export mytp pkcs12 flash:myexport companyname</p>	<p>Exports the RSA keys via the trustpoint name.</p> <p> Note You can export the trustpoint to any of the following places:</p> <ul style="list-style-type: none"> • Flash • FTP • Null • NVRAM • RCP • SCP • System • TFTP • Webflash • Xmodem • Ymodem

Importing the RSA Key Pair to the Target Router

This section provides the steps necessary to import the RSA key pair on the target router and verify the importation.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **crypto ca import trustpointname pkcs12 source url passphrase**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	crypto ca import trustpointname pkcs12 source-url passphrase Example: Router(config)# crypto ca import mytrustpoint pkcs12 www.mycompany.com newpassphrase	Imports RSA keys.

Verifying the Importation of the RSA Key Pair to the Target Router

Use the **show crypto key mykey rsa** command - modified output will show RSA key information, including whether or not the key is exportable. Some new lines of output indicate the time of import (if the RSA key was imported), the last time of export.

SUMMARY STEPS

1. **enable**
2. **show crypto ca trustpoints**
3. **show crypto key mypubkey rsa**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	show crypto ca trustpoints Example: Router# show crypto ca trustpoints	Displays the trustpoints that are configured in the router.
Step 3	show crypto key mypubkey rsa Example: Router# show crypto key mypubkey rsa	Displays the RSA public key(s) of your router.

Examples

The following example shows confirms that the trustpoint “mytp” has been imported to the target router:

```
Router# show crypto ca trustpoints
```

```
Trustpoint yni-u10:
  Subject Name:
    CN = nsca-r1 Cert Manager
    OU = pki
    O = cisco.com
    C = US
    Serial Number: 01
  Certificate configured.
  CEP URL: http://yni-u10
```

```
Trustpoint mytp:
```

```
Trustpoint mynewtp:
```

The following example confirms that the RSA key pair “mykeys” has been imported to the target router:

```
router# show crypto key mypubkey rsa
```

```
!
!
% Key pair was generated at: 17:26:55 GMT Feb 18 2003
Key name: mykeys
Usage: General Purpose Key
Key is exportable.
Key Data:
05C300D 06092A86 4886F70D 01010105 00034B00 30480241 00AEF991 332BDC26
 61084DB5 9E23D198 A39A9B54 42311593 4240D5BF C1D430A9 69ADF1BD 6C3F2113
  D25B226B F5332098 D91461AC EFF832D4 9E5B3459 185A8DA5 E7020301 0001
Key name: mynewtp
Usage: General Purpose Key
Key is not exportable.
Key Data:
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00AEF991 332BDC26
 61084DB5 9E23D198 A39A9B54 42311593 4240D5BF C1D430A9 69ADF1BD 6C3F2113
  D25B226B F5332098 D91461AC EFF832D4 9E5B3459 185A8DA5 E7020301 0001
```

Troubleshooting Tips

You can use the **debug crypto pki** command to trouble-shoot the Exporting and Importing RSA Keys feature.

Configuration Examples for Using the Exporting and Importing RSA Keys Feature

- [Exporting and Importing RSA Keys Example, page 8](#)

Exporting and Importing RSA Keys Example

In the following example, an RSA key pair “mynewkp” is generated on Router A, and a trustpoint name “mynewtp” is created and associated with the RSA key pair. The trustpoint is exported to a TFTP server, so that it can be imported on Router B. By importing the trustpoint “mynewtp” to Router B, the user has imported the RSA key pair “mynewkp” to Router B.

Router A

```
Router(config)# crypto key generate rsa general label mykeys exportable

!The name for the keys will be: mynewkp
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]:
% Generating 512 bit RSA keys ...[OK]
!
Router(config)#cr ca trustpoint mynewtp
Router(ca-trustpoint)#rsa keypair mykeys
Router(ca-trustpoint)#exit
Router(config)#cr ca export mytp pkcs12 flash:myexport companyname
Destination filename [myexport]?
Writing pkcs12 file to tftp://mytftpserver/myexport
CRYPTO_PKI: Exported PKCS12 file successfully.
Verifying checksum... OK (0x3307)
!
Feb 18 17:30:09 GMT: %CRYPTO-6-PKCS12EXPORT_SUCCESS: PKCS #12 Successfully
Exported.
```

Router B

```
Router(config)# crypto ca import mynewtp pkcs12 flash:myexport companyname
Source filename [myexport]?
CRYPTO_PKI: Imported PKCS12 file successfully.
!
Feb 18 18:07:50 GMT: %CRYPTO-6-PKCS12IMPORT_SUCCESS: PKCS #12 Successfully
Imported.
```

Additional References

For additional information related to the Exporting and Importing RSA Keys feature, refer to the following references:

Related Documents

Related Topic	Document Title
Configuring Security Features	<i>Cisco IOS Security Configuration Guide</i> , Release 12.2
Cisco IOS Security Commands	<i>Cisco IOS Security Command Reference</i> , Release 12.2 T

Standards

Standards	Title
PKCS12 #12 v1.0	“Personal Information Exchange Syntax Standard,” RSA Laboratories, June 24, 1999.

MIBs

MIBs	MIBs Link
None	To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at the following URL: http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

<http://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

RFCs	Title
None	—

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

Command Reference

This section documents new and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.2 T command reference publications.

New Commands

- [crypto ca export pkcs12](#)
- [crypto ca import pkcs12](#)

Modified Commands

- [crypto key generate rsa \(IKE\)](#)

crypto ca export pkcs12

To export Rivest, Shamir, and Adelman (RSA) keys within a PKCS12 file at a specified location, use the **crypto ca export pkcs12** command in global configuration mode.

crypto ca export *trustpointname* **pkcs12** *destination url* *passphrase*

Syntax Description

<i>trustpointname</i>	Name of the trustpoint who issues the certificate that user is going to export. When you export the PKCS12 file, the trustpoint name is the RSA key name.
pkcs12	Specifies the PKCS12 file to be exported.
<i>destination url</i>	Location of the PKCS12 file where user wants to import the RSA key pair.
<i>passphrase</i>	Passphrase that is used to encrypt the PKCS12 file for export.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

The **crypto ca export pkcs12** command creates a pkcs12 file that contains an RSA keypair. The PKCS12 file, along with a CA, is exported to the location you specify with the destination url. If you decide not to import the file to another router, you need to delete the file.

Security Measures

Keep the PKCS12 file stored in a secure place with restricted access.

An RSA keypair is more secure than a passphrase because the private key in the keypair is not known by multiple parties. When you export an RSA keypair to a PKCS#12 file, the RSA keypair now is only as secure as the passphrase.

To create a good passphrase, be sure to include numbers, as well as both lower and upper case letters. Avoid publicizing the passphrase by mentioning it E-mail or cell phone communications since the information could be accessed by an unauthorized user.

Examples

The following example exports an RSA key pair with a trustpoint name “mytp” to a Flash file:

```
Router(config)# crypto ca export mytp pkcs12 flash:myexport
```

Related Commands

Command	Description
<code>crypto ca import pkcs12</code>	Imports RSA keys.

crypto ca import pkcs12

To import RSA keys, use the **crypto ca import pkcs12** command in global configuration mode.

crypto ca import *trustpointname* **pkcs12** *source url* *passphrase*

Syntax Description

<i>trustpointname</i>	Name of the trustpoint who issues the certificate that user is going to export or import. When importing, the trustpoint name will become the RSA key name.
pkcs12	Specifies the PKCS#12 file to be imported.
<i>source url</i>	The location of the PKCS#12 file where user wants to export the RSA key pair.
<i>passphrase</i>	Passphrase that must be entered in order to undo encryption when the RSA keys are imported.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.

Usage Guidelines

When you enter the **crypto ca import pkcs12** command, a keypair and a trustpoint are generated. If you then decide you want to remove the keypair and trustpoint that were generated, enter the **crypto key zeroize rsa** command to zeroize the keypair and enter the **no crypto ca trustpoint** command to remove the trustpoint.



Note

After you import RSA keys to a target router, you cannot export those keys from the target router to another router.

Examples

The following example imports an RSA key pair that has been associated with the trustpoint “forward”:

```
Router(config)# crypto ca import forward pkcs12 flash:myexport mycompany
```

Related Commands

Command	Description
crypto ca export pkcs12	Exports RSA keys.
crypto ca trustpoint	Declares the certification authority (CA) that your router should use.
crypto key zeroize rsa	Deletes all RSA keys from your router.

crypto key generate rsa (IKE)

To generate Rivest, Shamir, and Adelman (RSA) key pairs, use the **crypto key generate rsa** command in global configuration mode.

```
crypto key generate rsa {general-keys | usage-keys} [label key-label] exportable [modulus
modulus-size]
```

Syntax Description

general-keys	Specifies that the general-purpose key pair should be generated.
usage-keys	Specifies that two RSA special usage key pairs should be generated (that is, one encryption pair and one signature pair), instead of one general-purpose key pair.
exportable	Specifies that the RSA key pair can be exported to another Cisco device such as a router.
label <i>key-label</i>	Name that is used for an RSA key pair when they are being exported.
modulus <i>modulus-size</i>	Size of the key modulus in a range from 350 to 2048. If you do not enter the modulus keyword and specify a size, you will be prompted.

Defaults

RSA key pairs do not exist. If the **usage-keys** keyword is not used, general-purpose keys will be generated.

Command Modes

Global configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(15)T	The usage-keys and exportable keywords were added.

Usage Guidelines

Use this command to generate RSA key pairs for your Cisco device (such as a router).

RSA keys are generated in pairs—one public RSA key and one private RSA key.

If your router already has RSA keys when you issue this command, you will be warned and prompted to replace the existing keys with new keys.



Note

Before issuing this command, ensure that your router has a host name and IP domain name configured (with the **hostname** and **ip domain-name** commands). You will be unable to complete the **crypto key generate rsa** command without a host name and IP domain name.

This command is not saved in the router configuration; however, the RSA keys generated by this command are saved in the private configuration in NVRAM (which is never displayed to the user or backed up to another device).

There are two mutually exclusive types of RSA key pairs: special-usage keys and general-purpose keys. When you generate RSA key pairs, you can indicate whether to generate special-usage keys or general-purpose keys.

Special-Usage Keys

If you generate special-usage keys, two pairs of RSA keys will be generated. One pair will be used with any Internet Key Exchange (IKE) policy that specifies RSA signatures as the authentication method, and the other pair will be used with any IKE policy that specifies RSA encrypted keys as the authentication method.

If you plan to have both types of RSA authentication methods in your IKE policies, you might prefer to generate special-usage keys. With special-usage keys, each key is not unnecessarily exposed. (Without special usage keys, one key is used for both authentication methods, increasing that key's exposure.)

General-Purpose Keys

If you generate general-purpose keys, only one pair of RSA keys will be generated. This pair will be used with IKE policies specifying either RSA signatures or RSA encrypted keys. Therefore, a general purpose key pair might get used more frequently than a special usage key pair.

Modulus Length

When you generate RSA keys, you will be prompted to enter a modulus length. A longer modulus could offer stronger security, but takes longer to generate (see [Table 1](#) for sample times) and takes longer to use. A length of less than 512 is normally not recommended. (In certain situations, the shorter modulus may not function properly with IKE, so Cisco recommends using a minimum modulus of 1024.)

Table 1 Sample Times Required for Generating RSA Keys

Router	Modulus Length			
	360 bits	512 bits	1024 bits	2048 bits
Cisco 2500	11 seconds	20 seconds	4 minutes, 38 seconds	longer than 1 hour
Cisco 4700	less than 1 second	1 second	4 seconds	50 seconds

Examples

The following example generates special-usage RSA keys:

```
Router(config)# crypto key generate rsa usage-keys
The name for the keys will be: myrouter.example.com
```

```
Choose the size of the key modulus in the range of 360 to 2048 for your Signature Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
```

```
Choose the size of the key modulus in the range of 360 to 2048 for your Encryption Keys.
Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? <return>
Generating RSA keys.... [OK].
```

The following example generates general-purpose RSA keys:



Note

You cannot generate both special-usage and general-purpose keys; you can generate only one or the other.

```
Router(config)# crypto key generate rsa  
The name for the keys will be: myrouter.example.com
```

Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.
How many bits in the modulus[512]? **<return>**
Generating RSA keys.... [OK].

Related Commands

Command	Description
debug crypto engine	Displays debug messages about crypto engines.
hostname	Specifies or modifies the host name for the network server.
ip domain-name	Defines a default domain name to complete unqualified host names (names without a dotted-decimal domain name).
show crypto key mypubkey rsa	Displays the RSA public keys of your router.

Glossary

CA— certification authority. Entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate.

FQDN—fully qualified domain name. FQDN is the full name of a system, rather than just its host name.

IKE—Internet Key Exchange. IKE establishes a shared security policy and authenticates keys for services (such as IPSec) that require keys. service.

RSA—Public-key cryptographic system that can be used for encryption and authentication. The acronym stands for Rivest, Shamir, and Adelman, the inventors of the technique.

SSH—Secure Shell

**Note**

Refer to the [Internetworking Terms and Acronyms](#) for terms not included in this glossary.
