



# Easy VPN Remote RSA Signature Support

---

**First Published: March 1, 2004**

**Last Updated: August 21, 2007**

The Easy VPN Remote RSA Signature Support feature provides for the support of Rivest, Shamir, and Adelman (RSA) signatures on Easy VPN remote devices. The support is provided through RSA certificates that can be stored on or off the remote device.

## **Finding Feature Information in This Module**

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the “[Feature Information for Easy VPN Remote RSA Signature Support](#)” section on page 5.

## **Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images**

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

## Contents

- [Prerequisites for Easy VPN Remote RSA Signature Support, page 2](#)
- [Restrictions for Easy VPN Remote RSA Signature Support, page 2](#)
- [Information About Easy VPN Remote RSA Signature Support, page 2](#)
- [How to Configure Easy VPN Remote RSA Signature Support, page 2](#)
- [Additional References, page 3](#)



---

**Americas Headquarters:**

**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2004–2007 Cisco Systems, Inc. All rights reserved.

## Prerequisites for Easy VPN Remote RSA Signature Support

- You must have a Cisco Virtual Private Network (VPN) remote device and be familiar with configuring the device.
- You must have a certification authority (CA) available to your network before you configure this interoperability feature. The CA must support the public key infrastructure (PKI) protocol of Cisco Systems, which is the Simple Certificate Enrollment Protocol (SCEP) (formerly called certificate enrollment protocol [CEP]).
- You should be familiar with IP Security (IPSec) and PKI.
- You should be familiar with configuring RSA key pairs.
- You should be familiar with configuring CAs.

## Restrictions for Easy VPN Remote RSA Signature Support

- This feature should be configured only when you also configure both IPSec and Internet Key Exchange (IKE) in your network.
- The Cisco IOS software does not support CA server public keys greater than 2048 bits.

## Information About Easy VPN Remote RSA Signature Support

To configure the Easy VPN Remote RSA Signature Support feature, you should understand the following concept:

- [Easy VPN Remote RSA Signature Support Overview, page 2](#)

## Easy VPN Remote RSA Signature Support Overview

The Easy VPN Remote RSA Signature Support feature allows you to configure RSA signatures on your Easy VPN remote device. The signatures can be stored on or off your remote device.

## How to Configure Easy VPN Remote RSA Signature Support

This section contains the following procedure:

- [Configuring Easy VPN Remote RSA Signature Support, page 2](#)

## Configuring Easy VPN Remote RSA Signature Support

The RSA signatures for an Easy VPN remote device are configured the same way that you would configure RSA signatures for any other Cisco device. (For information about configuring RSA signatures, refer to the “Configuring Certification Authority Interoperability” chapter of the “IP Security and Encryption” section of the *Cisco IOS Security Configuration Guide*, Release 12.4.)

To enable the RSA signatures, when you are configuring the Easy VPN remote and assigning the configuration to the outgoing interface, you must omit the **group** command. The content of the first Organizational Unit (OU) field will be used as the group. (For information about configuring Cisco Easy VPN remote devices, refer to the feature document “[Cisco Easy VPN Remote](#),” Release 12.4(11)T.)

To troubleshoot your Easy VPN remote RSA signature configuration, you can use the following **debug** commands. The **debug** commands can be used in any order or individually.

## SUMMARY STEPS

1. **enable**
2. **debug crypto ipsec client ezvpn**
3. **debug crypto isakmp**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>debug crypto ipsec client ezvpn</b>  <b>Example:</b> Router# debug crypto ipsec client ezvpn	Displays information about the VPN tunnel as it relates to the Easy VPN remote configuration.
Step 3	<b>debug crypto isakmp</b>  <b>Example:</b> Router# debug crypto isakmp	Displays messages about IKE events.

## Additional References

The following sections provide references related to Easy VPN Remote RSA Signature Support.

## Related Documents

Related Topic	Document Title
Configuring IPsec	“IP Security and Encryption Overview” chapter of the <a href="#">Cisco IOS Security Configuration Guide</a> , Release 12.4
Configuring IKE	“Configuring Internet Key Exchange Security Protocol” chapter of the “IP Security and Encryption” section of the <a href="#">Cisco IOS Security Configuration Guide</a> , Release 12.4
Configuring RSA key pairs	Feature document “ <a href="#">Exporting and Importing RSA Keys</a> ,” Release 12.2(15)T

Related Topic	Document Title
Declaring a CA	“Configuring Certification Authority Interoperability” chapter of the “IP Security and Encryption” section of the <i>Cisco IOS Security Configuration Guide</i> , Release 12.4
Configuring a Cisco Easy VPN remote device	Feature document “ <i>Cisco Easy VPN Remote</i> ,” Release 12.4(11)T
Security commands	<i>Cisco IOS Security Command Reference</i> , Release 12.4 T

## Standards

Standards	Title
There are no new or modified standards associated with this feature.	—

## MIBs

MIBs	MIBs Link
There are no new or modified MIBs associated with this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## RFCs

RFCs	Title
There are no new or modified RFCs associated with this feature.	—

## Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of 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.	<a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a>

# Feature Information for Easy VPN Remote RSA Signature Support

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



## Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

**Table 1** Feature Information for Easy VPN Remote RSA Signature Support

Feature Name	Releases	Feature Information
Easy VPN Remote RSA Signature Support	12.3(7)T1 12.2(33)SRA 12.2(33)SXH	<p>The Easy VPN Remote RSA Signature Support feature provides for the support of Rivest, Shamir, and Adelman (RSA) signatures on Easy VPN remote devices. The support is provided through RSA certificates that can be stored on or off the remote device.</p> <p>The following sections provide information about this feature:</p> <ul style="list-style-type: none"> <li>“Easy VPN Remote RSA Signature Support Overview” section on page 2</li> <li>“Configuring Easy VPN Remote RSA Signature Support” section on page 2</li> </ul>

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2004–2007 Cisco Systems, Inc. All rights reserved.

