

Cisco ISR G2 SEC and HSEC Licensing

General

Q. What do you mean by a tunnel?

A. In the context of the security licensing and export restrictions that are discussed in this document, a tunnel is a construct established between two routers (peers) to transport insecure payloads using data-encryption techniques.

Q. The end customer is in the United States, so why does this customer need to comply with export control?

A. Customers in the United States can order any of these products without any restrictions. Cisco does not have direct control over where the platform is shipping, so the licenses have to be enforced on all orders regardless of their final destination.

Q. What should I do if I purchased a Cisco® Integrated Services Routers Generation 2 (ISR G2) router on Cisco IOS® Software Release 15.0(1)M before the limitation was imposed and I need to upgrade my Cisco IOS Software?

A. Assuming that you already have purchased the securityk9 package for encryption, you must purchase a HSEC-K9 license as a spare.

Q. How does this restriction affect Federal Information Processing Standards (FIPS) or Common Criteria compliance?

A. FIPS and Common Criteria do not address export restrictions. These certifications just verify that a vendor can meet government requirements and that the router can do what it claims it can do.

Q. Does this restriction apply to the current generation of Cisco Integrated Services Routers?

A. Yes, the current generation of ISRs, the 1800, 2800 and 3800 platforms, are also subject to the same restrictions, depending on the encryption configuration.

Q. Do the same export-restriction rules apply to the Cisco ASA (Adaptive Security Appliances) product family?

A. The Cisco ASA platform is also restricted for export. This platform already goes through these same export checks and requirements.

Q. What other products are affected by the United States export restrictions?

A. All products containing encryption technology are subjected to U.S. export restrictions. Refer to <http://tools.cisco.com/legal/export/pepd/Search.do> for a list of products based on the hardware and software configuration.

SEC-K9 License

Q. What is the SEC-K9 license for the Cisco ISR G2 routers?

A. The SEC-K9 license enables standard encryption (VPN payload and secure voice) on the ISR G2 platforms. The SEC-K9 license is designed to comply with both local and U.S. export requirements for global distribution to all countries. This license enforces a curtailment on the maximum number of encrypted tunnels and the maximum encrypted throughput on the ISR G2 platforms.

Q. Why is the SEC-K9 license an unrestricted license?

A. The SEC-K9 license limits the number of concurrent encrypted sessions and maximum encrypted throughput per device. This limit helps ensure that the ISR G2 complies with U. S. government export restrictions regardless of the final destination country.

Q. What tunnel count and performance throughput are available on the Cisco ISR G2 routers with the SEC-K9 license?

A. The SEC-K9 permanent licenses apply to the Cisco 1900, 2900, and 3900 ISR G2 platforms; these licenses limit all encrypted tunnel counts to 225 tunnels maximum for IP Security (IPsec), Secure Sockets Layer VPN (SSL VPN), a secure time-division multiplexing (TDM) gateway, and secure Cisco Unified Border Element (CUBE) and 1000 tunnels for Transport Layer Security (TLS) sessions.

The SEC-K9 license limits encrypted throughput to less than or equal to 85-Mbps unidirectional traffic in or out of the ISR G2 router, with a bidirectional total of 170 Mbps. This requirement applies for the Cisco 1900, 2900, and 3900 ISR G2 platforms.

Q. What security features are supported on the Cisco ISR G2 with the SEC-K9 license?

A. All threat defense and VPN features that are supported on the Cisco ISR G2 routers are functionally available for configuration with the SEC-K9. The image that includes this license is the universal-k9 image. For example, the Cisco IOS release version is c3900-universalk9-mz.SPA.150-1.M1.

Q. Does the router require a reload after installing the SEC-K9 or the HSEC-K9 license?

A. Reload is needed only for technology package licenses such as datak9, uck9, and securityk9/securityk9_npe. Installing the SEC-K9 or the HSEC-K9 license does not require a reload. Also, moving from a temporary license to a permanent license does not require a reload.

Q. Why do I need to purchase the SEC-K9 license as a spare?

A. If you purchase a Cisco ISR G2 chassis and later decide to turn on security features, you must buy a SEC-K9 license. The administrator must download the license to the router and follow the license installation instructions that come with the license to be able to use the security features on the router.

Q. What information do I need to order either the SEC-K9 or the HSEC-K9 license as a spare for my ISR G2 router?

A. To order the licenses as spares, you need the output of the following command-line interface (CLI) command: **show license udi**, shown at the end of this section. You must enter the product ID (PID) and the serial number into the tool to complete the order. This information makes the license unique for a particular router, and the license is not transferrable between routers.

The command output follows:

```
3925-perf#sh license udi
Device#      PID                      SN                      UDI
-----
*0           C3900-SPE100/K9          FOC133037J9           C3900-SPE100/K9:FOC133037J9
```

For more information about software license activation on the ISR G2 platforms, please visit:

http://www.cisco.com/en/US/docs/routers/access/sw_activation/SA_on_ISR.html.

NPE-K9 Image

Q. What features does the npe-k9 image support?

- A.** The SECNPE image supports Cisco IOS Firewall, Integrated Protection Services (IPS), and URL Filtering (basically all the threat-defense functions). Standard encryption features are not supported on the ISR G2 platforms with this image.

HSEC-K9 License

Q. What is the HSEC-k9 license?

- A.** The HSEC-K9 license removes the curtailment enforced by the U.S. government export restrictions on the encrypted tunnel count and encrypted throughput. HSEC-K9 is available only on the Cisco 2921, Cisco 2951, Cisco 3925, Cisco 3945, Cisco 3925E, and Cisco 3945E. With the HSEC-K9 license, the ISR G2 router can go over the curtailment limit of 225 tunnels maximum for IP Security (IPsec) and encrypted throughput of 85-Mbps unidirectional traffic in or out of the ISR G2 router, with a bidirectional total of 170 Mbps.

The Cisco 1941, 2901, and 2911 already have maximum encryption capacities within export limits.

Q. Which Cisco IOS Software image version did the curtailment go in?

- A.** The HSEC license and curtailment was introduced in the Cisco IOS Software Release 15.0(1)M1 and will be enforced on all images following that release.

Q. I see the following error message on my ISR G2 router console: **“*Mar 22 21:17:23.611: %CERM-4-RX_BW_LIMIT: Maximum Rx Bandwidth limit of 85000 Kbps reached for Crypto functionality with securityk9 technology package license”**. What does this error message mean?

- A.** If you do not have a HSEC-k9 license installed on your ISR G2 router, you will see the following error message on the console if the traffic exceeds 85-Mbps unidirectional or 170-Mbps bidirectional.

```
3925-perf#
```

```
*Mar 22 21:17:23.611: %CERM-4-RX_BW_LIMIT: Maximum Rx bandwidth limit of 85,000 kbps
reached for cryptography functions with the securityk9 technology package license.
```

The **show license** executed on your ISR G2 router will show that the router is missing the HSEC license (gray highlighted text) that is required to unlock the curtailment imposed by the U.S. export restrictions as described previously.

```
3925-perf#sh license
```

```
Index 1 Feature: ipbasek9
    Period left: Life time
    License Type: Permanent
    License State: Active, In Use
    License Count: Non-Counted
    License Priority: Medium
Index 2 Feature: securityk9
    Period left: Life time
    License Type: Permanent
    License State: Active, In Use
    License Count: Non-Counted
    License Priority: Medium
```

Index 3 Feature: uck9

Period left: Life time
License Type: Permanent
License State: Active, In Use
License Count: Non-Counted
License Priority: Medium

Index 4 Feature: datak9

Period left: Life time
License Type: Permanent
License State: Active, In Use
License Count: Non-Counted
License Priority: Medium

Index 5 Feature: gatekeeper

Period left: 8 weeks 4 days
License Type: Evaluation
License State: Active, Not in Use, EULA not accepted
License Count: Non-Counted
License Priority: None

Index 6 Feature: LI

Index 7 Feature: SSL_VPN

Period left: 8 weeks 4 days
License Type: Evaluation
License State: Active, Not in Use, EULA not accepted
License Count: 200/0/0 (Active/In-use/Violation)
License Priority: None

Index 8 Feature: ios-ips-update

Index 9 Feature: SNASw

Period left: 8 weeks 4 days
License Type: Evaluation
License State: Active, Not in Use, EULA not accepted
License Count: Non-Counted
License Priority: None

Index 10 Feature: hseck9

Q. How do I install a HSEC license on the Cisco ISR G2 router?

A. You can order the HSEC-k9 license from the Cisco.com website for the Cisco 2900, 3900 ISR G2 , 3925E and 3945E platforms. You can order the HSEC license as a spare for e-delivery.

After you complete the ordering, the license is delivered as an attachment in an email message. The attachment has a ".lic" suffix. For example, FOC133037J9_20100322212822257.lic is a license file generated for a specific ISR G2 router.

You should perform all of the following steps on a Windows PC or laptop. Using an Apple Macintosh has been found to cause problems with loading and installation of the license on the router.

The email containing the license file also contains instructions to load and install the HSEC-k9 license on the ISR G2 router. Please follow the instructions carefully.

To begin with, the ISR G2 router should have a SEC-K9 security feature license that has already been installed on the router. If the router does not have a SEC-K9 license installed, you can purchase the license as a spare using the ordering tool from the Cisco.com website. Follow the instructions to install the SEC-k9 license on the router.

```
3925-perf#copy tftp: flash:
Address or name of remote host []? 171.69.1.129
Source filename []? /tftpboot/shsastry/FOC133037J9_20100322212822257.lic
Destination filename [FOC133037J9_20100322212822257.lic]?
Accessing tftp://171.69.1.129//tftpboot/shsastry/FOC133037J9_20100322212822257.lic...
Loading /tftpboot/shsastry/FOC133037J9_20100322212822257.lic from 171.69.17.19 (via
GigabitEthernet0/0): !
[OK - 1230 bytes]
```

```
1230 bytes copied in 0.440 secs (2795 bytes/sec)
```

```
3925-perf#sh flash
-#- --length-- -----date/time----- path
1      55203528 Mar 22 2010 18:05:12 c3900-universalk9-mz.SPA.150-1.M1
2      56977900 Mar 15 2010 23:37:10 c3900-universalk9-mz.SPA.151-0.26.T0.5
3           1230 Mar 23 2010 01:47:38 FOC133037J9_20100322212822257.lic
```

```
147984384 bytes available (112189440 bytes used)
```

```
3925-perf#license install flash:FOC133037J9_20100322212822257.lic
Installing licenses from "flash:FOC133037J9_20100322212822257.lic"
```

```
Expiring licenses are being installed in the device with
UDI "C3900-SPE100/K9:FOC133037J9" for the following features:
```

```
Feature Name: hseck9
```

```
PLEASE READ THE FOLLOWING TERMS CAREFULLY. INSTALLING THE LICENSE OR
LICENSE KEY PROVIDED FOR ANY CISCO PRODUCT FEATURE OR USING SUCH
```

PRODUCT FEATURE CONSTITUTES YOUR FULL ACCEPTANCE OF THE FOLLOWING TERMS. YOU MUST NOT PROCEED FURTHER IF YOU ARE NOT WILLING TO BE BOUND BY ALL THE TERMS SET FORTH HEREIN.

You hereby acknowledge and agree that the product feature license is terminable and that the product feature enabled by such license may be shut down or terminated by Cisco after expiration of the applicable term of the license (e.g., 30-day trial period). Cisco reserves the right to terminate or shut down any such product feature electronically or by any other means available. While alerts or such messages may be provided, it is your sole responsibility to monitor your terminable usage of any product feature enabled by the license and to ensure that your systems and networks are prepared for the shut down of the product feature. You acknowledge and agree that Cisco will not have any liability whatsoever for any damages, including, but not limited to, direct, indirect, special, or consequential damages related to any product feature being shutdown or terminated. By clicking the "accept" button or typing "yes" you are indicating you have read and agree to be bound by all the terms provided herein.

ACCEPT? [yes/no]: yes

Installing...Feature:hseck9...Successful:Supported

1/1 licenses were successfully installed

0/1 licenses were existing licenses

0/1 licenses were failed to install

3925-perf#

*Mar 23 01:48:27.878: %LICENSE-6-EULA_ACCEPTED: EULA for feature hseck9 1.0 has been accepted. UDI=C3900-SPE100/K9:FOC133037J9; StoreIndex=4:Primary License Storage

*Mar 23 01:48:28.118: %LICENSE-6-INSTALL: Feature hseck9 1.0 was installed in this device. UDI=C3900-SPE100/K9:FOC133037J9; StoreIndex=4:Primary License Storage

3925-perf#sh license

Index 1 Feature: ipbasek9

Period left: Life time

License Type: Permanent

License State: Active, In Use

License Count: Non-Counted

License Priority: Medium

Index 2 Feature: securityk9

Period left: Life time
License Type: Permanent
License State: Active, In Use
License Count: Non-Counted
License Priority: Medium

Index 3 Feature: uck9

Period left: Life time
License Type: Permanent
License State: Active, In Use
License Count: Non-Counted
License Priority: Medium

Index 4 Feature: datak9

Period left: Life time
License Type: Permanent
License State: Active, In Use
License Count: Non-Counted
License Priority: Medium

Index 5 Feature: gatekeeper

Period left: 8 weeks 4 days
License Type: Evaluation
License State: Active, Not in Use, EULA not accepted
License Count: Non-Counted
License Priority: None

Index 6 Feature: LI

Index 7 Feature: SSL_VPN

Period left: 8 weeks 4 days
License Type: Evaluation
License State: Active, Not in Use, EULA not accepted
License Count: 200/0/0 (Active/In-use/Violation)
License Priority: None

Index 8 Feature: ios-ips-update

Index 9 Feature: SNASw

Period left: 8 weeks 4 days
License Type: Evaluation
License State: Active, Not in Use, EULA not accepted
License Count: Non-Counted
License Priority: None

Index 10 Feature: hseck9

Period left: 8 weeks 4 days

License Type: Evaluation

License State: Active, In Use

License Count: Non-Counted

License Priority: Low

Export Control

Q. What are the rules for ordering and stocking the ISR G2 HSEC-K9 license in the EU license-free countries?

A. All customers in the EU license-free countries (EULF)—government, military, or civilian—can order the HSEC-K9 license. Customers in the EU license-free countries can order both system and spare licenses without any restrictions. The Cisco ISR G2 platforms, associated ISR G2 bundles, and the standard encryption enabling license SEC-K9 on the ISR G2 currently have a U.S. unrestricted export classification. In other words, with the exception of the U.S. embargoed countries (Sudan, Syria, Iran, Cuba, and North Korea), distributors are authorized to stock Cisco 1900, 2900, and 3900 ISR portfolio and associated bundles.

Q. What countries are classified license-free zones?

A. Countries belonging to the EU license-free zone include Australia, Austria, Belgium, Bulgaria, Canada, Cypress, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, United Kingdom, and the United States.

Q. What are the rules for ordering and stocking the ISR G2 HSEC-K9 license outside the EU license-free countries?

A. Civilian customers outside the EULF zones can order the HSEC-k9 license as part of the ISR G2 system part numbers or they can order the HSEC-K9 licenses as spares if they decide to do so at a later time. Install-site information is required at the time these spare images are ordered.

Government and military customers outside the EULF countries can order the ISR G2 system part numbers with the HSEC-K9 license as part of the system part number. However, they will not be able to order the HSEC-K9 licenses as spares. The HSEC-K9 license is export-restricted and because of U.S. government export inspection regulations, you should order it only at the time of initial router purchase if you are a government or military entity located outside the EULF.

Q. Where can I find more information about export control or request specific export compliance information regarding a customer's order?

A. If you have questions about export, please contact export@cisco.com.

Q. Why is my customer's order of the HSEC license on export hold?

A. All spare HSEC feature license orders that require an export license are reviewed by Cisco Global Export Trade. If the order cannot go forward because of the information in the order, Export Operations will contact you. You can also contact Export Operations via email: exportops@cisco.com. Please remember that orders for spares that are going to government and military sites outside the EULF will be rejected. For more information about export controls and U.S. export restrictions, please visit :

http://www.cisco.com/web/about/doing_business/legal/global_export_trade/export_hold/exportops.html.

Q. Where can my customer find information regarding the U.S. export restrictions for Cisco products and software?

A. More information regarding export compliance is available at:

http://www.cisco.com/web/about/doing_business/legal/global_export_trade/general_export_contract_compliance.html.

Q. What can my customer do to avoid export restrictions and licensing problems?

A. Customers located in a country that is inside the EULF can buy whatever they want and whenever they want it, regardless of whether they are a military, government, or a civilian customer.

If the country is outside the EULF, then it is a bit more complicated. For civilian customers, the same rules stated previously also apply; that is, they can buy a spare license after the initial hardware purchase. If however, they are government or military customers outside the EULF, then they must purchase the HSEC-K9 license along with the hardware. These government and military customers outside the EULF cannot add an HSEC license as a spare unless they purchase the software with the router.

To summarize, the options for these affected customers follow:

- Order the HSEC-K9 feature license along with the router.
- Order the SEC-K9 technology package license as a spare; this license offers less than 90 Mbps of unidirectional encrypted payload traffic and less than 180 Mbps of bidirectional encrypted payload traffic, and it supports 225 concurrent encrypted media tunnels.
- Order the SECNPE-K9 license as a spare; this license offers threat-defense capabilities but does not support encrypted media tunnels or encrypted payload.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1005R)