



Managing Feature Licenses for Cisco ASA 5500 Version 8.1

A license specifies the options that are enabled on a given security appliance. It is represented by an activation key which is a 160-bit (5 32-bit words or 20 bytes) value. This value encodes the serial number (an 11 character string) and the enabled features.

This document describes how to obtain an activation key and activate it. It also describes the available licenses for each model. This document includes the following sections:

- [Supported Feature Licenses on the ASA 5580, page 2](#)
- [Information About Feature Licenses, page 3](#)
- [Guidelines and Limitations, page 5](#)
- [Viewing Your Current License, page 5](#)
- [Obtaining an Activation Key, page 7](#)
- [Entering a New Activation Key, page 8](#)
- [Upgrading the License for a Failover Pair, page 9](#)
- [Feature History for Licensing, page 11](#)



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

© 2008 Cisco Systems, Inc. All rights reserved.

Supported Feature Licenses on the ASA 5580

Items that are in italics are separate, optional licenses with which that you can replace the Base license. You can mix and match licenses, for example, the 10 security context license plus the Strong Encryption license; or the 500 SSL VPN license plus the GTP/GPRS license; or all four licenses together.

Table 1 ASA 5580 Adaptive Security Appliance License Features

ASA 5580	Base License										
Users, concurrent	Unlimited										
Security Contexts	2										
	<i>Optional licenses:</i>										
	5	10	20	50							
VPN Sessions ¹	5000 combined IPsec and SSL VPN										
Max. IPsec Sessions	5000										
Max. SSL VPN Sessions	2										
	<i>Optional licenses:</i>										
	10	25	50	100	250	500	750	1000	2500	5000	
	<i>Optional VPN Flex licenses:²</i>				250	750	1000	2500	5000		
VPN Load Balancing	Supported										
Advanced Endpoint Assessment	None		<i>Optional license: Enabled</i>								
TLS Proxy for SIP and Skinny Inspection ³	Supported										
Failover	Active/Standby or Active/Active ⁴										
GTP/GPRS	None		<i>Optional license: Enabled</i>								
Max. VLANs	Version 8.1(1): 100										
	Version 8.1(2) and later: 250										
Concurrent Firewall Conns	650 K										
Max. Physical Interfaces	Unlimited										
Encryption	Base (DES)		<i>Optional license: Strong (3DES/AES)</i>								
Min. RAM	4 GB (default)										

- Although the maximum IPsec and Clientless SSL VPN sessions add up to more than the maximum VPN sessions, the combined sessions should not exceed the VPN session limit. If you exceed the maximum VPN sessions, you can overload the security appliance, so be sure to size your network appropriately.
- Available in Version 8.1(2) and later.
- Other Unified Communications features are not supported in Version 8.1.
- You cannot use Active/Active failover and VPN; if you want to use VPN, use Active/Standby failover.

Information About Feature Licenses

A license specifies the options that are enabled on a given security appliance. It is represented by an activation key which is a 160-bit (5 32-bit words or 20 bytes) value. This value encodes the serial number (an 11 character string) and the enabled features. Feature licenses cannot be transferred between devices (except in the case of a hardware failure). Once purchased, you cannot return a license for a refund or for an upgraded license.

This section includes the following topics:

- [Preinstalled License, page 3](#)
- [VPN Flex and Evaluation Licenses, page 3](#)

Preinstalled License

By default, your security appliance ships with a license already installed. This license might be the Base License, to which you want to add more licenses, or it might already have all of your licenses installed, depending on what you ordered and what your vendor installed for you. See the [“Viewing Your Current License” section on page 5](#) section to determine which licenses you have installed.

VPN Flex and Evaluation Licenses

In addition to permanent licenses, you can purchase a temporary VPN Flex license or receive an evaluation license that has a time-limit, if supported by your model. For example, you might buy a VPN Flex license to handle short-term surges in the number of concurrent SSL VPN users.

This section includes the following topics:

- [How the Temporary License Timer Works, page 3](#)
- [How Multiple Licenses Interact, page 4](#)
- [Failover and Temporary Licenses, page 5](#)

How the Temporary License Timer Works

- The timer for the temporary license starts counting down when you activate it on the security appliance.
- If you stop using the temporary license before it times out, for example you activate a permanent license or a different temporary license, then the timer halts. The timer only starts again when you reactivate the temporary license.
- If the temporary license is active, and you shut down the security appliance, then the timer continues to count down. If you intend to leave the security appliance in a shut down state for an extended period of time, then you should activate the permanent license before you shut down to preserve the temporary license.
- When a temporary license expires, the next time you reload the security appliance, the permanent license is used; you are not forced to perform a reload immediately when the license expires.



Note We suggest you do not change the system clock after you install the temporary license. If you set the clock to be a later date, then if you reload, the security appliance checks the system clock against the original installation time, and assumes that more time has passed than has actually been used. If you set the clock back, and the actual running time is greater than the time between the original installation time and the system clock, then the license immediately expires after a reload.

How Multiple Licenses Interact

- When you activate a temporary license, then features from both permanent and temporary licenses combine to form the running license. The security appliance uses the highest value from each license for each feature, and displays any resolved conflicts between the licenses when you enter a temporary activation key. In the rare circumstance that a temporary license has lower capability than the permanent license, the permanent license values are used.
- When you activate a permanent license, it overwrites the currently-running permanent and temporary licenses and becomes the running license.

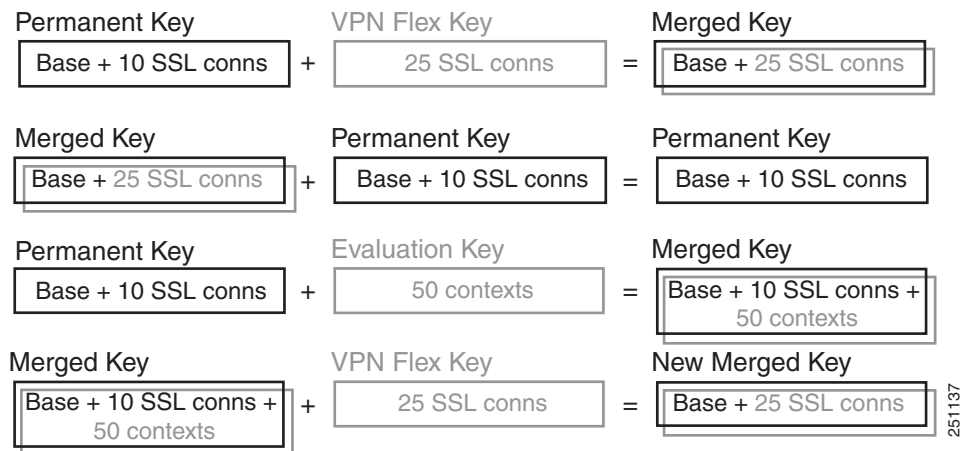


Note If the permanent license is a downgrade from the temporary license, then you need to reload the security appliance to disable the temporary license and restore the permanent license. Until you reload, the temporary license continues to count down.

- To reenble the features of the temporary license if you later activate a permanent license, simply reenter the temporary activation key. For a license upgrade, you do not need to reload.
- To switch to a different temporary license, enter the new activation key; the new license is used instead of the old temporary license and combines with the permanent license to create a new running license. The security appliance can have multiple temporary licenses installed; but only one is active at any given time.

See the following figure for examples of permanent and VPN Flex activation keys, and how they interact.

Figure 1 Permanent and VPN Flex Activation Keys



251137

Failover and Temporary Licenses

Because the temporary license continues to count down for as long as it is activated on a failover unit, we do not recommend using a temporary license in a failover situation, except in an emergency where the temporary license is activated only for a short period of time. In this case, one unit can use the permanent license and the other unit can use the temporary license if the features are equivalent between the permanent and temporary licenses. This functionality is useful if the hardware fails on a unit, and you need to replace it for a short period of time until the replacement unit arrives.

Guidelines and Limitations

See the following guidelines for activation keys.

Context Mode Guidelines

In multiple context mode, apply the activation key in the system execution space.

Firewall Mode Guidelines

Activation keys are available in both routed and transparent mode.

Failover Guidelines

Because the temporary license continues to count down for as long as it is activated on a failover unit, we do not recommend using a temporary license in a failover situation, except in an emergency where the temporary license is activated only for a short period of time. In this case, one unit can use the permanent license and the other unit can use the temporary license if the features are equivalent between the permanent and temporary licenses. This functionality is useful if the hardware fails on a unit, and you need to replace it for a short period of time until the replacement unit arrives.

Additional Guidelines and Limitations

- The activation key is not stored in your configuration file; it is stored as a hidden file in Flash memory.
- The activation key is tied to the serial number of the device. Feature licenses cannot be transferred between devices (except in the case of a hardware failure). If you have to replace your device due to a hardware failure, contact the Cisco Licensing Team to have your existing license transferred to the new serial number. The Cisco Licensing Team will ask for the Product Authorization Key reference number and existing serial number.
- Once purchased, you cannot return a license for a refund or for an upgraded license.
- You cannot add two separate licenses for the same feature together; for example, if you purchase a 25-session SSL VPN license, and later purchase a 50-session license, you cannot use 75 sessions; you can use a maximum of 50 sessions.

Viewing Your Current License

This section describes how to view your current license, and for temporary activation keys, how much time the license has left.

Detailed Steps

Command	Purpose
show activation-key detail Example: hostname# show activation-key detail	Shows the installed licenses, including information about temporary licenses.

Examples

The following is sample output from the **show activation-key detail** command that shows a permanent activation license, an active temporary license, the merged running license, and also the activation keys for inactive temporary licenses:

```
hostname# show activation-key detail
```

```
Serial Number: JMX0916L0Z4
```

```
Permanent Flash Activation Key: 0xf412675d 0x48a446bc 0x8c532580 0xb000b8c4 0xcc21f48e
```

```
Licensed features for this platform:
```

```
Maximum Physical Interfaces : Unlimited
Maximum VLANs              : 200
Inside Hosts                : Unlimited
Failover                    : Active/Active
VPN-DES                     : Enabled
VPN-3DES-AES                : Enabled
Security Contexts          : 2
GTP/GPRS                    : Disabled
VPN Peers                   : 5000
WebVPN Peers                : 2
AnyConnect for Mobile       : Disabled
AnyConnect for Linksys phone : Disabled
Advanced Endpoint Assessment : Disabled
UC Proxy Sessions           : 2
```

```
Temporary Flash Activation Key: 0xcb0367ce 0x700dd51d 0xd57b98e3 0x6ebcf553 0x0b058aac
```

```
Licensed features for this platform:
```

```
Maximum Physical Interfaces : Unlimited
Maximum VLANs              : 200
Inside Hosts                : Unlimited
Failover                    : Active/Active
VPN-DES                     : Enabled
VPN-3DES-AES                : Disabled
Security Contexts          : 2
GTP/GPRS                    : Disabled
VPN Peers                   : 5000
WebVPN Peers                : 500
AnyConnect for Mobile       : Disabled
AnyConnect for Linksys phone : Disabled
Advanced Endpoint Assessment : Disabled
UC Proxy Sessions           : 2
```

```
This is a time-based license that will expire in 27 day(s).
```

```
Running Activation Key: 0xcb0367ce 0x700dd51d 0xd57b98e3 0x6ebcf553 0x0b058aac
```

```
Licensed features for this platform:
```

```
Maximum Physical Interfaces : Unlimited
Maximum VLANs              : 200
```

```

Inside Hosts                : Unlimited
Failover                    : Active/Active
VPN-DES                     : Enabled
VPN-3DES-AES               : Enabled
Security Contexts          : 2
GTP/GPRS                   : Disabled
VPN Peers                   : 5000
WebVPN Peers                : 500
AnyConnect for Mobile      : Disabled
AnyConnect for Linksys phone : Disabled
Advanced Endpoint Assessment : Disabled
UC Proxy Sessions          : 2

```

This platform has an ASA 5540 VPN Premium license.
This is a time-based license that will expire in 27 day(s).

The flash activation key is the SAME as the running key.

```

Non-active temporary keys:                Time left
-----
0x2a53d6 0xfc087bfe 0x691b94fb 0x73dc8bf3 0xcc028ca2 28 day(s)
0xa13a46c2 0x7c10ec8d 0xad8a2257 0x5ec0ab7f 0x86221397 27 day(s)

```

Obtaining an Activation Key

To obtain an activation key, you need a Product Authorization Key, which you can purchase from your Cisco account representative. You need to purchase a separate Product Activation Key for each feature license. For example, if you have the Base License, you can purchase separate keys for Advanced Endpoint Assessment and for additional SSL VPN sessions.



Note

For a failover pair, you need separate activation keys for each unit. Make sure the licenses included in the keys are the same for both units.

After obtaining the Product Authorization Keys, register them on Cisco.com by performing the following steps:

Step 1 Obtain the serial number for your security appliance by entering the following command:

```
hostname# show activation-key
```

Step 2 Access one of the following URLs.

- Use the following website if you are a registered user of Cisco.com:
<http://www.cisco.com/go/license>
- Use the following website if you are not a registered user of Cisco.com:
<http://www.cisco.com/go/license/public>

Step 3 Enter the following information, when prompted:

- Product Authorization Key (if you have multiple keys, enter one of the keys first. You have to enter each key as a separate process.)
- The serial number of your security appliance

- Your email address

An activation key is automatically generated and sent to the email address that you provide. This key includes all features you have registered so far for permanent licenses. For VPN Flex licenses, each license has a separate activation key.

Step 4 If you have additional Product Authorization Keys, repeat [Step 3](#) for each Product Authorization Key. After you enter all of the Product Authorization Keys, the final activation key provided includes all of the permanent features you registered.

Entering a New Activation Key

Before entering the activation key, ensure that the image in Flash memory and the running image are the same. You can do this by reloading the security appliance before entering the new activation key.

Prerequisites

- If you are already in multiple context mode, enter the activation key in the system execution space.
- Some licenses require you to reload the security appliance after you activate them. [Table 2](#) lists the licenses that require reloading.

Table 2 License Reloading Requirements

Model	License Action Requiring Reload
ASA 5505 and ASA 5510	Changing between the Base and Security Plus license.
All models	Changing the Encryption license.
All models	Downgrading any license (for example, going from 10 contexts to 2 contexts). Note If a temporary license expires, and the permanent license is a downgrade, then you do not need to immediately reload the security appliance; the next time you reload, the permanent license is restored.

Detailed Steps

	Command	Purpose
Step 1	activation-key <i>key</i> Example: <pre>hostname(config)# activation-key 0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490</pre>	<p>Applies an activation key to the security appliance. The key is a five-element hexadecimal string with one space between each element. The leading 0x specifier is optional; all values are assumed to be hexadecimal.</p> <p>You can enter one permanent key, and multiple temporary keys. The last temporary key entered is the active one. See the “VPN Flex and Evaluation Licenses” section on page 3 for more information. To change the running activation key, enter the activation-key command with a new key value.</p>
Step 2	reload Example: <pre>hostname(config)# reload</pre>	<p>(Might be required.) Reloads the security appliance. Some licenses require you to reload the security appliance after entering the new activation key. See Table 2 on page 8 for a list of licenses that need reloading. If you need to reload, you will see the following message:</p> <pre>WARNING: The running activation key was not updated with the requested key. The flash activation key was updated with the requested key, and will become active after the next reload.</pre>

Upgrading the License for a Failover Pair

If you need to upgrade the license on a failover pair, you might have some amount of downtime depending on whether the license requires a reload. See [Table 2 on page 8](#) for more information about licenses requiring a reload. This section includes the following topics:

- [Upgrading the License for a Failover \(No Reload Required\)](#), page 9
- [Upgrading the License for a Failover \(Reload Required\)](#), page 10

Upgrading the License for a Failover (No Reload Required)

Use the following procedure if your new license does not require you to reload. See [Table 2 on page 8](#) for more information about licenses requiring a reload. This procedure ensures that there is no downtime.

Detailed Steps

	Command	Purpose
	On the active unit:	
Step 1	no failover Example: <pre>active(config)# no failover</pre>	Disables failover on the active unit. The standby unit remains in standby mode.

	Command	Purpose
Step 2	activation-key <i>key</i> Example: active(config)# activation-key 0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490	Installs the new license on the active unit.
	On the standby unit:	
Step 3	activation-key <i>key</i> Example: standby(config)# activation-key 0xc125727f 0x903de1ee 0x8c838928 0x92dc84d4 0x003a2ba0	Installs the new license on the standby unit.
	On the active unit:	
Step 4	failover Example: active(config)# failover	Reenables failover.

Upgrading the License for a Failover (Reload Required)

Use the following procedure if your new license requires you to reload. See [Table 2 on page 8](#) for more information about licenses requiring a reload. Reloading the failover pair causes a loss of connectivity during the reload.

Detailed Steps

	Command	Purpose
	On the active unit:	
Step 1	no failover Example: active(config)# no failover	Disables failover on the active unit. The standby unit remains in standby mode.
Step 2	activation-key <i>key</i> Example: active(config)# activation-key 0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490	Installs the new license on the active unit. If you need to reload, you will see the following message: WARNING: The running activation key was not updated with the requested key. The flash activation key was updated with the requested key, and will become active after the next reload. If you do not need to reload, then follow the “Upgrading the License for a Failover (No Reload Required)” section on page 9 instead of this procedure.
	On the standby unit:	

	Command	Purpose
Step 3	activation-key <i>key</i> Example: standby(config)# activation-key 0xc125727f 0x903de1ee 0x8c838928 0x92dc84d4 0x003a2ba0	Installs the new license on the standby unit.
Step 4	reload Example: standby(config)# reload On the active unit:	Reloads the standby unit.
Step 5	reload Example: active(config)# reload	Reloads the active unit. When you are prompted to save the configuration before reloading, answer No . This means that when the active unit comes back up, failover will still be enabled.

Feature History for Licensing

Table 3 lists the release history for this feature.

Table 3 Feature History for Licensing

Feature Name	Releases	Feature Information
VPN Flex and Temporary Licenses	8.1(2)	Support for temporary licenses was introduced.

CCDE, CCENT, Cisco Eos, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0809R)

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.

© 2008 Cisco Systems, Inc. All rights reserved.

