Managing Feature Licenses for Cisco ASA 5500 and Cisco PIX 500 Version 8.0

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 Per Model

This section lists the feature licenses available for each model:

- ASA 5505, Table 1 on page 2
- ASA 5510, Table 2 on page 3
- ASA 5520, Table 3 on page 4
- ASA 5540, Table 4 on page 5
- ASA 5550, Table 5 on page 6
- PIX 515/515E, Table 6 on page 7
- PIX 525. Table 7 on page 8
- PIX 535, Table 8 on page 9

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

Note The ASA 5580 is not supported in Version 8.0; for ASA 5580 information, see the licensing documentation for Version 8.1 or later.

The PIX 500 series security appliance does not support temporary licenses.

Items that are in italics are separate, optional licenses with which that you can replace the Base or Security Plus 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 5505 Adaptive Security Appliance License Features

ASA 5505	Base License			Security Plus		
Users, concurrent[1]	10[2]	*Optional licenses:*		10[2]	*Optional licenses:*	
		50	*Unlimited*		*50*	*Unlimited*
Security Contexts	No support			No support		
VPN Sessions[3]	25 combined IPSec and SSL VPN			25 combined IPSec and SSL VPN		
Max. IPSec Sessions	10			25		
Max. SSL VPN Sessions	2	*Optional licenses:*		2	*Optional licenses:*	
		10	*25*		*10*	*25*
VPN Load Balancing	No support			No support		
Advanced Endpoint Assessment	None		*Optional license: Enabled*	None		*Optional license: Enabled*
Unified Communications Proxy Sessions[4]	2	*Optional license: 24*		2	*Optional license: 24*	
Failover	No support			Active/Standby (no stateful failover)		
GTP/GPRS	No support			No support		
Maximum VLANs/Zones	3 (2 regular zones and 1 restricted zone that can only communicate with 1 other zone)			20		
Maximum VLAN Trunks	No support			8 trunks		
Concurrent Firewall Conns	10 K			25 K		
Max. Physical Interfaces	Unlimited, assigned to VLANs/zones			Unlimited, assigned to VLANs/zones		
Encryption	Base (DES)		*Optional license:* *Strong (3DES/AES)*	Base (DES)		*Optional license:* *Strong (3DES/AES)*
Minimum RAM	256 MB (default)			256 MB (default)		

[1] In routed mode, hosts on the inside (Business and Home VLANs) count towards the limit when they communicate with the outside (Internet VLAN), including when the inside initiates a connection to the outside as well as when the outside initiates a connection to the inside. Note that even when the outside initiates a connection to the inside, outside hosts are *not* counted towards the limit; only the inside hosts count. Hosts that initiate traffic between Business and Home are also not counted towards the limit. The interface associated with the default route is considered to be the outside Internet interface. If there is no default route, hosts on all interfaces are counted toward the limit. In transparent mode, the interface with the lowest number of hosts is counted towards the host limit. See the **show local-host** command to view host limits.

[2] For a 10-user license, the max. DHCP clients is 32. For 50 users, the max. is 128. For unlimited users, the max. is 250, which is the max. for other models.

[3] Although the maximum IPSec and 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. When determining the session makeup of the combined limit, the number of SSL VPN sessions cannot exceed the number of licensed SSL VPN sessions on the security appliance (which is 2 by default).

[4] Phone Proxy, Mobility Proxy, Presence Federation Proxy, and TLS Proxy are all licensed under the UC Proxy umbrella, and can be mixed and matched. For example, if you configure a phone with a primary and backup Cisco Unified Communications Manager, there are 2 TLS/SRTP connections, and 2 UC Proxy sessions are used. This license was introduced in Version 8.0(4). In prior versions, TLS proxy for SIP and Skinny inspection was included in the Base License.

Table 2 ASA 5510 Adaptive Security Appliance License Features

<table>
<tr><th>ASA 5510</th><th colspan="6">Base License</th><th colspan="6">Security Plus</th></tr>
<tr><td>Users, concurrent</td><td colspan="6">Unlimited</td><td colspan="6">Unlimited</td></tr>
<tr><td rowspan="2">Security Contexts</td><td colspan="6" rowspan="2">No support</td><td rowspan="2">2</td><td colspan="5"><i>Optional licenses:</i></td></tr>
<tr><td colspan="5"><i>5</i></td></tr>
<tr><td>VPN Sessions[1]</td><td colspan="6">250 combined IPSec and SSL VPN</td><td colspan="6">250 combined IPSec and SSL VPN</td></tr>
<tr><td>Max. IPSec Sessions</td><td colspan="6">250</td><td colspan="6">250</td></tr>
<tr><td rowspan="3">Max. SSL VPN Sessions</td><td rowspan="3">2</td><td colspan="5"><i>Optional licenses:</i></td><td rowspan="3">2</td><td colspan="5"><i>Optional licenses:</i></td></tr>
<tr><td><i>10</i></td><td><i>25</i></td><td><i>50</i></td><td><i>100</i></td><td><i>250</i></td><td><i>10</i></td><td><i>25</i></td><td><i>50</i></td><td><i>100</i></td><td><i>250</i></td></tr>
<tr><td colspan="5"><i>Optional VPN Flex license:[2] 250</i></td><td colspan="5"><i>Optional VPN Flex license: 250</i></td></tr>
<tr><td>VPN Load Balancing</td><td colspan="6">No support</td><td colspan="6">Supported</td></tr>
<tr><td>Advanced Endpoint Assessment</td><td colspan="2">None</td><td colspan="4"><i>Optional license: Enabled</i></td><td colspan="2">None</td><td colspan="4"><i>Optional license: Enabled</i></td></tr>
<tr><td rowspan="2">Unified Communications Proxy Sessions[3] (introduced in 8.0(4))</td><td rowspan="2">2</td><td colspan="5"><i>Optional licenses</i></td><td rowspan="2">2</td><td colspan="5"><i>Optional licenses</i></td></tr>
<tr><td><i>24</i></td><td><i>50</i></td><td colspan="3"><i>100</i></td><td><i>24</i></td><td><i>50</i></td><td colspan="3"><i>100</i></td></tr>
<tr><td>Failover</td><td colspan="6">No support</td><td colspan="6">Active/Standby or Active/Active[4]</td></tr>
<tr><td>GTP/GPRS</td><td colspan="6">No support</td><td colspan="6">No support</td></tr>
<tr><td>Max. VLANs</td><td colspan="6">50</td><td colspan="6">100</td></tr>
<tr><td>Concurrent Firewall Conns</td><td colspan="6">50 K</td><td colspan="6">130 K</td></tr>
<tr><td>Max. Physical Interfaces</td><td colspan="6">Unlimited</td><td colspan="6">Unlimited</td></tr>
<tr><td>Interface Speed</td><td colspan="6">All: Fast Ethernet</td><td colspan="6">Ethernet 0/0 and 0/1: Gigabit Ethernet[5]
Ethernet 0/2, 0/3, and 0/4: Fast Ethernet</td></tr>
<tr><td>Encryption</td><td colspan="2">Base (DES)</td><td colspan="4"><i>Optional license: Strong (3DES/AES)</i></td><td colspan="2">Base (DES)</td><td colspan="4"><i>Optional license: Strong (3DES/AES)</i></td></tr>
<tr><td>Min. RAM</td><td colspan="6">256 MB (default)</td><td colspan="6">256 MB (default)</td></tr>
</table>

[1] Although the maximum IPSec and 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. When determining the session makeup of the combined limit, the number of SSL VPN sessions cannot exceed the number of licensed SSL VPN sessions on the security appliance (which is 2 by default).

[2] Available in Version 8.0(4) and later.

[3] Phone Proxy, Mobility Proxy, Presence Federation Proxy, and TLS Proxy are all licensed under the UC Proxy umbrella, and can be mixed and matched. For example, if you configure a phone with a primary and backup Cisco Unified Communications Manager, there are 2 TLS/SRTP connections, and 2 UC Proxy sessions are used. This license was introduced in Version 8.0(4). In prior versions, TLS proxy for SIP and Skinny inspection was included in the Base License.

[4] You cannot use Active/Active failover and VPN; if you want to use VPN, use Active/Standby failover.

[5] Although the Ethernet 0/0 and 0/1 ports are Gigabit Ethernet, they are still identified as "Ethernet" in the software.

Table 3 ASA 5520 Adaptive Security Appliance License Features

ASA 5520	Base License							
Users, concurrent	Unlimited						Unlimited	
Security Contexts	2	*Optional licenses:*						
		5	*10*	*20*				
VPN Sessions[1]	750 combined IPSec and SSL VPN							
Max. IPSec Sessions	750							
Max. SSL VPN Sessions	2	*Optional licenses:*						
		10	*25*	*50*	*100*	*250*	*500*	*750*
		Optional VPN Flex licenses:[2]				*250*		*750*
VPN Load Balancing	Supported							
Advanced Endpoint Assessment	None		*Optional license: Enabled*					
Unified Communications Proxy Sessions[3]	2	*Optional licenses*						
		24	*50*	*100*	*250*	*500*	*750*	*1000*
Failover	Active/Standby or Active/Active[4]							
GTP/GPRS	None		*Optional license: Enabled*					
Max. VLANs	150							
Concurrent Firewall Conns	280 K							
Max. Physical Interfaces	Unlimited							
Encryption	Base (DES)		*Optional license: Strong (3DES/AES)*					
Min. RAM	512 MB (default)							

[1] Although the maximum IPSec and 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. When determining the session makeup of the combined limit, the number of SSL VPN sessions cannot exceed the number of licensed SSL VPN sessions on the security appliance (which is 2 by default).

[2] Available in Version 8.0(4) and later.

[3] Phone Proxy, Mobility Proxy, Presence Federation Proxy, and TLS Proxy are all licensed under the UC Proxy umbrella, and can be mixed and matched. For example, if you configure a phone with a primary and backup Cisco Unified Communications Manager, there are 2 TLS/SRTP connections, and 2 UC Proxy sessions are used. This license was introduced in Version 8.0(4). In prior versions, TLS proxy for SIP and Skinny inspection was included in the Base License.

[4] You cannot use Active/Active failover and VPN; if you want to use VPN, use Active/Standby failover.

Table 4 ***ASA 5540 Adaptive Security Appliance License Features***

ASA 5540	Base License									
Users, concurrent	Unlimited					Unlimited				
Security Contexts	2	*Optional licenses:*								
		5	*10*	*20*	*50*					
VPN Sessions[1]	5000 combined IPSec and SSL VPN									
Max. IPSec Sessions	5000									
Max. SSL VPN Sessions	2	*Optional licenses:*								
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*
		Optional VPN Flex Licenses:[2]				*250*		*750*	*1000*	*2500*
VPN Load Balancing	Supported									
Advanced Endpoint Assessment	None		*Optional license: Enabled*							
Unified Communications Proxy Sessions[3]	2	*Optional licenses*								
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	
Failover	Active/Standby or Active/Active[4]									
GTP/GPRS	None		*Optional license: Enabled*							
Max. VLANs	200									
Concurrent Firewall Conns	400 K									
Max. Physical Interfaces	Unlimited									
Encryption	Base (DES)		*Optional license: Strong (3DES/AES)*							
Min. RAM	1 GB (default)									

[1] Although the maximum IPSec and 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. When determining the session makeup of the combined limit, the number of SSL VPN sessions cannot exceed the number of licensed SSL VPN sessions on the security appliance (which is 2 by default). This license was introduced in Version 8.0(4). In prior versions, TLS proxy for SIP and Skinny inspection was included in the Base License.

[2] Available in Version 8.0(4) and later.

[3] Phone Proxy, Mobility Proxy, Presence Federation Proxy, and TLS Proxy are all licensed under the UC Proxy umbrella, and can be mixed and matched. For example, if you configure a phone with a primary and backup Cisco Unified Communications Manager, there are 2 TLS/SRTP connections, and 2 UC Proxy sessions are used. Prior to 8.0(4), only TLS Proxy was available.

[4] You cannot use Active/Active failover and VPN; if you want to use VPN, use Active/Standby failover.

Table 5 ***ASA 5550 Adaptive Security Appliance License Features***

ASA 5550	**Base License**										
Users, concurrent	Unlimited										
Security Contexts	2	*Optional licenses:*									
		5	*10*	*20*	*50*						
VPN Sessions[1]	5000 combined IPSec and SSL VPN										
Max. IPSec Sessions	5000										
Max. SSL VPN Sessions	2	*Optional licenses:*									
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*	*5000*
		Optional VPN Flex licenses:[2]				*250*		*750*	*1000*	*2500*	*5000*
VPN Load Balancing	Supported										
Advanced Endpoint Assessment	None	*Optional license: Enabled*									
Unified Communications Proxy Sessions[3]	2	*Optional licenses*									
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*	
Failover	Active/Standby or Active/Active[4]										
GTP/GPRS	None	*Optional license: Enabled*									
Max. VLANs	250										
Concurrent Firewall Conns	650 K										
Max. Physical Interfaces	Unlimited										
Encryption	Base (DES)	*Optional license: Strong (3DES/AES)*									
Min. RAM	4 GB (default)										

[1] Although the maximum IPSec and 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. When determining the session makeup of the combined limit, the number of SSL VPN sessions cannot exceed the number of licensed SSL VPN sessions on the security appliance (which is 2 by default). This license was introduced in Version 8.0(4). In prior versions, TLS proxy for SIP and Skinny inspection was included in the Base License.

[2] Available in Version 8.0(4) and later.

[3] Phone Proxy, Mobility Proxy, Presence Federation Proxy, and TLS Proxy are all licensed under the UC Proxy umbrella, and can be mixed and matched. For example, if you configure a phone with a primary and backup Cisco Unified Communications Manager, there are 2 TLS/SRTP connections, and 2 UC Proxy sessions are used.

[4] You cannot use Active/Active failover and VPN; if you want to use VPN, use Active/Standby failover.

Table 6 PIX 515/515E Security Appliance License Features

PIX 515/515E	R (Restricted)	UR (Unrestricted)	FO (Failover)[1]	FO-AA (Failover Active/Active)[1]
Advanced Endpoint Assessment	No support	No support	No support	No support
Encryption	None *Optional licenses:* *Base (DES)* *Strong (3DES/ AES)*	None *Optional licenses:* *Base (DES)* *Strong (3DES/ AES)*	None *Optional licenses:* *Base (DES)* *Strong (3DES/ AES)*	None *Optional licenses:* *Base (DES)* *Strong (3DES/ AES)*
Failover	No support	Active/Standby Active/Active	Active/Standby	Active/Standby Active/Active
Firewall Conns, concurrent	48 K	130 K	130 K	130 K
GTP/GPRS	None *Optional license: Enabled*	None *Optional license: Enabled*	None *Optional license: Enabled*	None *Optional license: Enabled*
IPSec Sessions	2000	2000	2000	2000
Physical Interfaces, max.	3	6	6	6
RAM, min.	64 MB (default)	128 MB	128 MB	128 MB
Security Contexts	No support	2 *Optional license: 5*	2 *Optional license: 5*	2 *Optional license: 5*
SSL VPN Sessions	No support	No support	No support	No support
Unified Communications Proxy Sessions	No support	No support	No support	No support
Users, concurrent	Unlimited	Unlimited	Unlimited	Unlimited
VLANs, max.	10	25	25	25
VPN Load Balancing	No support	No support	No support	No support

[1] This license can only be used in a failover pair with another unit with a UR license. Both units must be the same model.

Table 7 PIX 525 Security Appliance License Features

PIX 525	R (Restricted)	UR (Unrestricted)	FO (Failover)[1]	FO-AA (Failover Active/Active)[1]
Advanced Endpoint Assessment	No support	No support	No support	No support
Encryption	None *Optional licenses:* *Base (DES)* *Strong (3DES/ AES)*	None *Optional licenses:* *Base (DES)* *Strong (3DES/ AES)*	None *Optional licenses:* *Base (DES)* *Strong (3DES/ AES)*	None *Optional licenses:* *Base (DES)* *Strong (3DES/ AES)*
Failover	No support	Active/Standby Active/Active	Active/Standby	Active/Standby Active/Active
Firewall Conns, concurrent	140 K	280 K	280 K	280 K
GTP/GPRS	None *Optional license: Enabled*	None *Optional license: Enabled*	None *Optional license: Enabled*	None *Optional license: Enabled*
IPSec Sessions	2000	2000	2000	2000
Physical Interfaces, max.	6	10	10	10
RAM, min.	128 MB (default)	256 MB	256 MB	256 MB
Security Contexts	No support	2 *Optional licenses:* *5* *10* *20* *50*	2 *Optional licenses:* *5* *10* *20* *50*	2 *Optional licenses:* *5* *10* *20* *50*
SSL VPN Sessions	No support	No support	No support	No support
Unified Communications Proxy Sessions	No support	No support	No support	No support
Users, concurrent	Unlimited	Unlimited	Unlimited	Unlimited
VLANs, max.	25	100	100	100
VPN Load Balancing	No support	No support	No support	No support

[1] This license can only be used in a failover pair with another unit with a UR license. Both units must be the same model.

Table 8 PIX 535 Security Appliance License Features

PIX 535	R (Restricted)	UR (Unrestricted)	FO (Failover)[1]	FO-AA (Failover Active/Active)[1]
Advanced Endpoint Assessment	No support	No support	No support	No support
Encryption	None *Optional licenses:* *Base (DES)* *Strong (3DES/AES)*	None *Optional licenses:* *Base (DES)* *Strong (3DES/AES)*	None *Optional licenses:* *Base (DES)* *Strong (3DES/AES)*	None *Optional licenses:* *Base (DES)* *Strong (3DES/AES)*
Failover	No support	Active/Standby Active/Active	Active/Standby	Active/Standby Active/Active
Firewall Conns, concurrent	250 K	500 K	500 K	500 K
GTP/GPRS	None *Optional license: Enabled*	None *Optional license: Enabled*	None *Optional license: Enabled*	None *Optional license: Enabled*
IPSec Sessions	2000	2000	2000	2000
Physical Interfaces, max.	8	14	14	14
RAM, min.	512 MB (default)	1024 MB	1024 MB	1024 MB
Security Contexts	No support	2 *Optional licenses:* *5* *10* *20* *50*	2 *Optional licenses:* *5* *10* *20* *50*	2 *Optional licenses:* *5* *10* *20* *50*
SSL VPN Sessions	No support	No support	No support	No support
Unified Communications Proxy Sessions	No support	No support	No support	No support
Users, concurrent	Unlimited	Unlimited	Unlimited	Unlimited
VLANs, max.	50	150	150	150
VPN Load Balancing	No support	No support	No support	No support

[1] This license can only be used in a failover pair with another unit with a UR license. Both units must be the same model.

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.

This section includes the following topics:

- Preinstalled License, page 10
- VPN Flex and Evaluation Licenses, page 10

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 12 section to determine which licenses you have installed.

VPN Flex and Evaluation Licenses

Note The PIX 500 series security appliance does not support temporary licenses.

In addition to permanent licenses, you can purchase a temporary VPN Flex license or receive an evaluation license that has a time-limit. 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 10
- How Multiple Licenses Interact, page 11
- Failover and Temporary Licenses, page 12

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 are merged to form the running license. Note that the adaptive security appliance only uses the highest value from each license for each feature; the values are not added together. The adaptive security appliance 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.

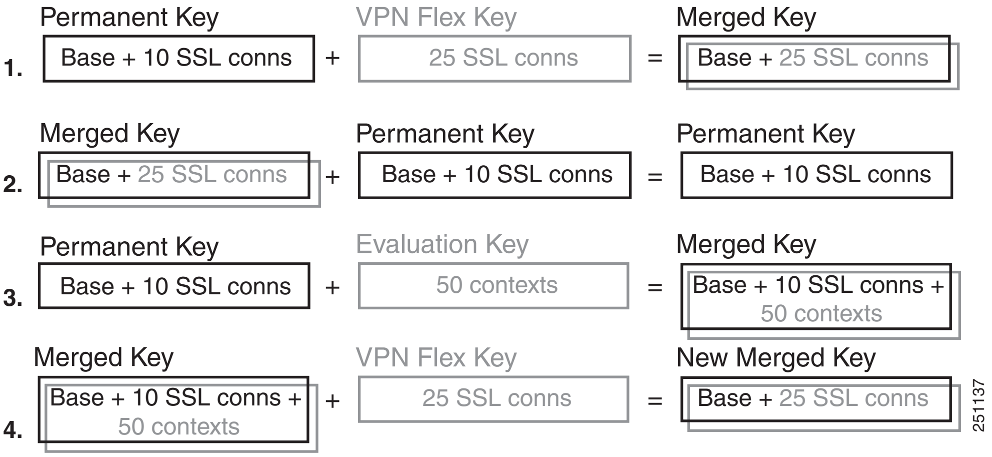
Note If the permanent license is a *downgrade* from the temporary license, then you need to reload the security appliance to disable the temporary license and restore the permanent license. Until you reload, the temporary license continues to count down.

Interim release 8.0(4.16) includes an enhancement so that you do not need to reload the security appliance after reactivating the already installed permanent license; this enhancement stops the temporary license from continuing to count down with no disruption of traffic.

- To reenable 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



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. (You may be able to purchase a larger license at an upgrade price, for example from 25 sessions to 75 sessions; this kind of upgrade should be distinguished from adding two separate licenses together).

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 If you are not already registered with Cisco.com, create an account.

Step 3 Go to the following licensing website:

http://www.cisco.com/go/license

Step 4 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 5 If you have additional Product Authorization Keys, repeat Step 4 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 9 lists the licenses that require reloading.

Table 9 License Reloading Requirements

Model	License Action Requiring Reload
ASA 5505 and ASA 5510	Changing between the Base and Security Plus license.
PIX 500 series	Changing between R, UR, FO, and FO-AA licenses.
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`** *`key`*
	Example:
	`hostname(config)# activation-key 0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490`
		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.
		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 10 for more information. To change the running activation key, enter the **activation-key** command with a new key value.

Step 2	**`reload`**
	Example:
	`hostname(config)# reload`
		(Might be required.) Reloads the security appliance. Some licenses require you to reload the security appliance after entering the new activation key. See Table 9 on page 15 for a list of licenses that need reloading. 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.`

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 9 on page 15 for more information about licenses requiring a reload. This section includes the following topics:

- Upgrading the License for a Failover (No Reload Required), page 16
- Upgrading the License for a Failover (Reload Required), page 17

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 9 on page 15 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:
	`active(config)# no failover`
		Disables failover on the active unit. The standby unit remains in standby mode.

	Command	Purpose
Step 2	**activation-key** *key* **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** *key* **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 9 on page 15 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** *key* **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 16 instead of this procedure.
	On the standby unit:	

	Command	Purpose
Step 3	**activation-key** *key* **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`	Reloads the standby unit.
	On the active 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 10 lists the release history for this feature.

Table 10 Feature History for Licensing

Feature Name	Releases	Feature Information
Increased Connections and VLANs	7.0(5)	Increased the following limits: • ASA5510 Base license connections from 32000 to 5000; VLANs from 0 to 10. • ASA5510 Security Plus license connections from 64000 to 130000; VLANs from 10 to 25. • ASA5520 connections from 130000 to 280000; VLANs from 25 to 100. • ASA5540 connections from 280000 to 400000; VLANs from 100 to 200.
SSL VPN Licenses for the ASA 5500 series	7.1(1)	SSL VPN licenses were introduced. This feature is not supported on the Cisco PIX 500 series.
Increased SSL VPN Licenses	7.2(1)	A 5000-user SSL VPN license was introduced for the ASA 5550 and above.
Increased interfaces for the Base license on the ASA 5510	7.2(2)	For the Base license on the ASA 5510, the maximum number of interfaces was increased from 3 plus a management interface to unlimited interfaces.

Table 10 Feature History for Licensing (continued)

Feature Name	Releases	Feature Information
Increased VLANs	7.2(2)	The maximum number of VLANs for the Security Plus License on the ASA 5505 was increased from 5 (3 fully functional; 1 failover; one restricted to a backup interface) to 20 fully functional interfaces. In addition, the number of trunk ports was increased from 1 to 8. Now there are 20 fully functional interfaces, you do not need to use the **backup interface** command to cripple a backup ISP interface; you can use a fully-functional interface for it. The **backup interface** command is still useful for an Easy VPN configuration. VLAN limits were also increased for the ASA 5510 (from 10 to 50 for the Base License, and from 25 to 100 for the Security Plus License), the ASA 5520 (from 100 to 150), the ASA 5550 (from 200 to 250).
Gigabit Ethernet Support for the ASA 5510	7.2(3)	The ASA 5510 now has the Security Plus License to enable GE (Gigabit Ethernet) for port 0 and 1. If you upgrade the license from Base to Security Plus, the capacity of the external Ethernet0/0 and Ethernet0/1 ports increases from the original FE (Fast Ethernet) (100 Mbps) to GE (1000 Mbps). The interface names will remain Ethernet 0/0 and Ethernet 0/1. Use the **speed** command to change the speed on the interface and use the **show interface** command to see what speed is currently configured for each interface.
Advanced Endpoint Assessment License for the ASA 5500 series	8.0(2)	The Advanced Endpoint Assessment License was introduced. As a condition for the completion of a Cisco AnyConnect or clientless SSL VPN connections, the remote computer scans for a greatly expanded collection of antivirus and antispyware applications, firewalls, operating systems, and associated updates. It also scans for any registry entries, filenames, and process names that you specify. It sends the scan results to the adaptive security appliance. The security appliance uses both the user login credentials and the computer scan results to assign a Dynamic Access Policy (DAP). With an Advanced Endpoint Assessment License, you can enhance Host Scan by configuring an attempt to update noncompliant computers to meet version requirements. We provide timely updates to the list of applications and versions that Host Scan supports in a package that is separate from Cisco Secure Desktop. This feature is not supported on the PIX 500 series.
VPN Load Balancing for the ASA 5510	8.0(2)	VPN load balancing is now supported on the ASA 5510 Security Plus License.

Table 10 Feature History for Licensing (continued)

Feature Name	Releases	Feature Information
VPN Flex and Temporary Licenses for the ASA 5500 series	8.0(4)	Support for temporary licenses was introduced. This feature is not supported on the PIX 500 series.
Unified Communications Proxy Sessions license for the ASA 5500 series	8.0(4)	The UC Proxy sessions license was introduced. This feature is not available in Version 8.1. This feature is not supported on the PIX 500 series.

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.