Managing Feature Licenses for Cisco ASA 5500 Version 8.2

December 2010

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 describes the licenses available for each model as well as important notes about licenses. This section includes the following topics:

Licenses Per Model

This section lists the feature licenses available for each model:

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

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	
Firewall Licenses				
Botnet Traffic Filter[1]	Disabled	*Optional temporary license: Available*	Disabled	*Optional temporary license: Available*
Firewall Conns, Concurrent	10 K		25 K	
GTP/GPRS	No support		No support	
Unified Comm. Sessions[1]	2	*Optional license: 24*	2	*Optional license: 24*
VPN Licenses[2]				
Adv. Endpoint Assessment	Disabled	*Optional license: Available*	Disabled	*Optional license: Available*
AnyConnect Essentials[1]	Disabled	*Optional license: Available*	Disabled	*Optional license: Available*
AnyConnect Mobile[1]	Disabled	*Optional license: Available*	Disabled	*Optional license: Available*
AnyConnect Premium SSL VPN (sessions)[1]	2	*Optional Permanent licenses:*	2	*Optional Permanent licenses:*
		10 *25*		*10* *25*
IPSec VPN (sessions)[1]	10 (max. 25 combined IPSec and SSL VPN)		25 (max. 25 combined IPSec and SSL VPN)	
VPN Load Balancing	No support		No support	
General Licenses				
Encryption	Base (DES)	*Opt. lic.: Strong (3DES/AES)*	Base (DES)	*Opt. lic.: Strong (3DES/AES)*
Failover	No support		Active/Standby (no stateful failover)	
Security Contexts	No support		No support	
Users, concurrent[3]	10[4]	*Optional licenses:*	10[4]	*Optional licenses:*
		50 *Unlimited*		*50* *Unlimited*
VLANs/Zones, Maximum	3 (2 regular zones and 1 restricted zone)		20	
VLAN Trunk, Maximum	No support		8 trunks	

1. See the “License Notes” section.
2. See the “VPN License and Feature Compatibility” section.
3. 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.
4. 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.

Table 2 ASA 5510 Adaptive Security Appliance License Features

ASA 5510	Base License					Security Plus				
Firewall Licenses										
Botnet Traffic Filter[1]	Disabled	*Optional temporary license: Available*				Disabled	*Optional temporary license: Available*			
Firewall Conns, Concurrent	50 K					130 K				
GTP/GPRS	No support					No support				
Unified Comm. Sessions[1]	2	*Optional licenses:*				2	*Optional licenses:*			
		24	*50*	*100*			*24*	*50*	*100*	
VPN Licenses[2]										
Adv. Endpoint Assessment	Disabled	*Optional license: Available*				Disabled	*Optional license: Available*			
AnyConnect Essentials[1]	Disabled	*Optional license: Available*				Disabled	*Optional license: Available*			
AnyConnect Mobile[1]	Disabled	*Optional license: Available*				Disabled	*Optional license: Available*			
AnyConnect Premium SSL VPN (sessions)	2	*Optional Permanent licenses:*				2	*Optional Permanent licenses:*			
		10	*25*	*50*	*100*		*10*	*25*	*50*	*100*
	Optional Shared licenses: Participant or Server. For the Server, these licenses are available:[1]					*Optional Shared licenses: Participant or Server. For the Server, these licenses are available:*[1]				
	500-50,000 in increments of 500	*50,000-545,000 in increments of 1000*				*500-50,000 in increments of 500*	*50,000-545,000 in increments of 1000*			
	Optional FLEX license: 250					*Optional FLEX license: 250*				
IPSec VPN (sessions)[1]	250 (max. 250 combined IPSec and SSL VPN)					250 (max. 250 combined IPSec and SSL VPN)				
VPN Load Balancing[1]	No support					Supported				
General Licenses										
Encryption	Base (DES)	*Opt. lic.: Strong (3DES/AES)*				Base (DES)	*Opt. lic.: Strong (3DES/AES)*			
Failover	No support					Active/Standby or Active/Active[1]				
Interface Speed	All: Fast Ethernet					Ethernet 0/0 and 0/1: Gigabit Ethernet[3] Ethernet 0/2, 0/3, and 0/4: Fast Ethernet				
Security Contexts	No support					2	*Optional licenses:*			
							5			
VLANs, Maximum	50					100				

1. See the “License Notes” section.
2. See the “VPN License and Feature Compatibility” section.
3. 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						
Firewall Licenses							
Botnet Traffic Filter[1]	Disabled	*Optional temporary license: Available*					
Firewall Conns, Concurrent	280 K						
GTP/GPRS	Disabled	*Optional license: Available*					
Unified Communications Proxy Sessions[1]	2	*Optional licenses:*					
		24	*50*	*100*	*250*	*500*	*750*	*1000*
VPN Licenses[2]							
Adv. Endpoint Assessment	Disabled	*Optional license: Available*					
AnyConnect Essentials[1]	Disabled	*Optional license: Available*					
AnyConnect Mobile[1]	Disabled	*Optional license: Available*					
AnyConnect Premium SSL VPN (sessions)	2	*Optional Permanent licenses:*					
		10	*25*	*50*	*100*	*250*	*500*	*750*
	Optional Shared licenses: Participant or Server. For the Server, these licenses are available:[1]						
	500-50,000 in increments of 500					*50,000-545,000 in increments of 1000*	
	Optional FLEX licenses:						
	250	*750*					
IPSec VPN (sessions)[1]	750 (max. 750 combined IPSec and SSL VPN)						
VPN Load Balancing[1]	Supported						
General Licenses							
Encryption	Base (DES)	*Optional license: Strong (3DES/AES)*					
Failover	Active/Standby or Active/Active[1]						
Security Contexts	2	*Optional licenses:*					
		5	*10*	*20*			
VLANs, Maximum	150						

1. See the “License Notes” section.
2. See the “VPN License and Feature Compatibility” section.

Table 4 ASA 5540 Adaptive Security Appliance License Features

ASA 5540	Base License								
Firewall Licenses									
Botnet Traffic Filter[1]	Disabled	*Optional temporary license: Available*							
Firewall Conns, Concurrent	400 K								
GTP/GPRS	Disabled	*Optional license: Available*							
Unified Communications Proxy Sessions[1]	2	*Optional licenses:*							
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*
VPN Licenses[2]									
Adv. Endpoint Assessment	Disabled	*Optional license: Available*							
AnyConnect Essentials[1]	Disabled	*Optional license: Available*							
AnyConnect Mobile[1]	Disabled	*Optional license: Available*							
AnyConnect Premium SSL VPN (sessions)	2	*Optional Permanent licenses:*							
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*
	Optional Shared licenses: Participant or Server. For the Server, these licenses are available:[1]								
	500-50,000 in increments of 500					*50,000-545,000 in increments of 1000*			
	Optional FLEX licenses:								
	250	*750*	*1000*	*2500*					
IPSec VPN (sessions)[1]	5000 (max. 5000 combined IPSec and SSL VPN)								
VPN Load Balancing[1]	Supported								
General Licenses									
Encryption	Base (DES)	*Optional license: Strong (3DES/AES)*							
Failover	Active/Standby or Active/Active[1]								
Security Contexts	2	*Optional licenses:*							
		5	*10*	*20*	*50*				
VLANs, Maximum	200								

1. See the “License Notes” section.
2. See the “VPN License and Feature Compatibility” section.

Table 5 ASA 5550 Adaptive Security Appliance License Features

ASA 5550	Base License									
Firewall Licenses										
Botnet Traffic Filter[1]	Disabled	*Optional temporary license: Available*								
Firewall Conns, Concurrent	650 K									
GTP/GPRS	Disabled	*Optional license: Available*								
Unified Communications Proxy Sessions[1]	2	*Optional licenses:*								
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*
VPN Licenses[2]										
Adv. Endpoint Assessment	Disabled	*Optional license: Available*								
AnyConnect Essentials[1]	Disabled	*Optional license: Available*								
AnyConnect Mobile[1]	Disabled	*Optional license: Available*								
AnyConnect Premium SSL VPN (sessions)	2	*Optional Permanent licenses:*								
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*	*5000*
	Optional Shared licenses: Participant or Server. For the Server, these licenses are available:[1]									
	500-50,000 in increments of 500						*50,000-545,000 in increments of 1000*			
	Optional FLEX licenses:									
	250	*750*	*1000*	*2500*	*5000*					
IPSec VPN (sessions)[1]	5000 (max. 5000 combined IPSec and SSL VPN)									
VPN Load Balancing[1]	Supported									
General Licenses										
Encryption	Base (DES)	*Optional license: Strong (3DES/AES)*								
Failover	Active/Standby or Active/Active[1]									
Security Contexts	2	*Optional licenses:*								
		5	*10*	*20*	*50*					
VLANs, Maximum	250									

1. See the “License Notes” section.
2. See the “VPN License and Feature Compatibility” section.

Table 6 ASA 5580 Adaptive Security Appliance License Features

ASA 5580	Base License										
Firewall Licenses											
Botnet Traffic Filter[1]	Disabled	*Optional temporary license: Available*									
Firewall Conns, Concurrent	5580-20: 1,000 K 5580-40: 2,000 K										
GTP/GPRS	Disabled	*Optional license: Available*									
Unified Communications Proxy Sessions[1]	2	*Optional licenses:*									
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*	*5000*	*10000*[2]
VPN Licenses[3]											
Adv. Endpoint Assessment	Disabled	*Optional license: Available*									
AnyConnect Essentials[1]	Disabled	*Optional license: Available*									
AnyConnect Mobile[1]	Disabled	*Optional license: Available*									
AnyConnect Premium SSL VPN (sessions)	2	*Optional Permanent licenses:*									
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*	*5000*
	Optional Shared licenses: Participant or Server. For the Server, these licenses are available:[1]										
	500-50,000 in increments of 500						*50,000-545,000 in increments of 1000*				
	Optional FLEX licenses:										
	250	*750*	*1000*	*2500*	*5000*						
IPSec VPN (sessions)[1]	5000 (max. 5000 combined IPSec and SSL VPN)										
VPN Load Balancing[1]	Supported										
General Licenses											
Encryption	Base (DES)	*Optional license: Strong (3DES/AES)*									
Failover	Active/Standby or Active/Active[1]										
Security Contexts	2	*Optional licenses:*									
		5	*10*	*20*	*50*						
VLANs, Maximum	250										

1. See the “License Notes” section.
2. With the 10,000-session license, the total combined sessions can be 10,000, but the maximum number of Phone Proxy sessions is 5000.
3. See the “VPN License and Feature Compatibility” section.

Table 7 ASA 5585-X Adaptive Security Appliance License Features

ASA 5585-X	Base License										
Firewall Licenses											
Botnet Traffic Filter[1]	Disabled	*Optional temporary license: Available*									
Firewall Conns, Concurrent	5585-X with SSP-10: 750 K 5585-X with SSP-20: 1,000 K 5585-X with SSP-40: 2,000 K 5585-X with SSP-60: 2,000 K										
GTP/GPRS	Disabled	*Optional license: Available*									
Unified Communications Proxy Sessions[1]	2	*Optional licenses:*									
		24	*50*	*100*	*250*	*500*	*750*	*1000*	*2000*	*3000*	*5000*	*10000*[2]
VPN Licenses[3]											
Adv. Endpoint Assessment	Disabled	*Optional license: Available*									
AnyConnect Essentials[1]	Disabled	*Optional license: Available*									
AnyConnect Mobile[1]	Disabled	*Optional license: Available*									
AnyConnect Premium SSL VPN (sessions)	2	*Optional Permanent licenses:*									
		10	*25*	*50*	*100*	*250*	*500*	*750*	*1000*	*2500*	*5000*	*10000*
	Optional Shared licenses: Participant or Server. For the Server, these licenses are available:[1]										
	500-50,000 in increments of 500						*50,000-545,000 in increments of 1000*				
	Optional FLEX licenses:										
	250	*750*	*1000*	*2500*	*5000*	*10000*					
IPSec VPN (sessions)[1]	5000 (max. 10000 combined IPSec and SSL VPN)										
VPN Load Balancing[1]	Supported										
General Licenses											
Encryption	Base (DES)	*Optional license: Strong (3DES/AES)*									
Failover	Active/Standby or Active/Active[1]										
10 GE I/O for SSP-10 and SSP-20[4]	Disabled; fiber ifcs run at 1 GE					*Optional license: Available; fiber ifcs run at 10 GE*					
Security Contexts	2	*Optional licenses:*									
		5	*10*	*20*	*50*						
VLANs, Maximum	250										

1. See the “License Notes” section.
2. With the 10,000-session license, the total combined sessions can be 10,000, but the maximum number of Phone Proxy sessions is 5000.
3. See the “VPN License and Feature Compatibility” section.
4. The ASA 5585-X with SSP-40 and -60 support 10-Gigabit Ethernet speeds by default.

License Notes

Table 8 lists footnotes for the tables in the "Licenses Per Model" section on page 1.

Table 8 License Notes

License	Notes
Active/Active failover	You cannot use Active/Active failover and VPN; if you want to use VPN, use Active/Standby failover.
AnyConnect Essentials	This license enables AnyConnect VPN client access to the adaptive security appliance. This license does not support deploy browser-based SSL VPN access or Cisco Secure Desktop. For these features, activate an AnyConnect Premium SSL VPN license instead of the AnyConnect Essentials license. **Note** With the AnyConnect Essentials license, VPN users can use a Web browser to log in, and download and start (WebLaunch) the AnyConnect client. The AnyConnect client software offers the same set of client features, whether it is enabled by this license or an AnyConnect Premium SSL VPN license. The AnyConnect Essentials license cannot be active at the same time as the following licenses on a given adaptive security appliance: AnyConnect Premium SSL VPN license (all types) or the Advanced Endpoint Assessment license. You can, however, run AnyConnect Essentials and AnyConnect Premium SSL VPN licenses on different adaptive security appliances in the same network. By default, the security appliance uses the AnyConnect Essentials license, but you can disable it to use other licenses by using the **no anyconnect-essentials** command.
AnyConnect Mobile	This license provides access to the AnyConnect Client for touch-screen mobile devices running Windows Mobile 5.0, 6.0, and 6.1. We recommend using this license if you want to support mobile access to AnyConnect 2.3 and later versions. This license requires activation of one of the following licenses to specify the total number SSL VPN sessions permitted: AnyConnect Essentials or AnyConnect Premium SSL VPN.
AnyConnect Premium SSL VPN Shared	A shared license lets the security appliance act as a shared license server for multiple client security appliances. The shared license pool is large, but the maximum number of sessions used by each individual security appliance cannot exceed the maximum number listed for permanent licenses.
Botnet Traffic Filter	Requires a Strong Encryption (3DES/AES) License to download the dynamic database.
Encryption	The DES license cannot be disabled. If you have the 3DES license installed, DES is still available. To prevent the use of DES when you want to only use strong encryption, be sure to configure any relevant commands to use only string encryption.
Combined IPSec and SSL VPN sessions	• 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. • If you start a clientless SSL VPN session and then start an AnyConnect client session from the portal, 1 session is used in total. However, if you start the AnyConnect client first (from a standalone client, for example) and then log into the clientless SSL VPN portal, then 2 sessions are used.

Table 8 License Notes

License	Notes
Unified Communications Proxy sessions	Phone Proxy, Mobility Advantage 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, so 2 UC Proxy sessions are used. **Note** In Version 8.2(2) and later, Mobility Advantage Proxy no longer requires the UC Proxy license.
VPN load balancing	Requires a Strong Encryption (3DES/AES) License.

VPN License and Feature Compatibility

Table 9 shows how the VPN licenses and features can combine.

Table 9 VPN License and Feature Compatibility

	Enable one of the following licenses:[1]	
Supported with:	**AnyConnect Essentials**	**AnyConnect Premium SSL VPN**
AnyConnect Mobile	**Yes**	**Yes**
Advanced Endpoint Assessment	**No**	**Yes**
AnyConnect Premium SSL VPN Shared	**No**	**Yes**
Client-based SSL VPN	**Yes**	**Yes**
Browser-based (clientless) SSL VPN	**No**	**Yes**
IPsec VPN	**Yes**	**Yes**
VPN Load Balancing	**Yes**	**Yes**
Cisco Secure Desktop	**No**	**Yes**

1. You can only have one license type active, either the AnyConnect Essentials license or the AnyConnect Premium license. By default, the security appliance includes an AnyConnect Premium license for 2 sessions. If you install the AnyConnect Essentials license, then it is used by default. See the **no anyconnect-essentials** command or in ASDM, the Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Essentials pane to enable the Premium license instead.

Information About Feature Licenses

A license specifies the options that are enabled on a given security appliance. It is represented by an activation key that 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

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 19 section to determine which licenses you have installed.

Temporary, VPN Flex, and Evaluation Licenses

In addition to permanent licenses, you can purchase a temporary 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, or you might order a Botnet Traffic Filter temporary license that is valid for 1 year.

This section includes the following topics:

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 security appliance only uses the *highest* value from each license for each feature; the values are not added together. The 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 you install a new permanent license, and it 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.

If you reactivate the *already installed* permanent license, you do not need to reload the security appliance; the temporary license does not continue to count down, and there is 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

1. In example 1 in the above figure, you apply a temporary key with 25 SSL sessions; because the VPN Flex value is greater than the permanent key value of 10 sessions, the resulting running key is a merged key that uses the VPN Flex value of 25 sessions, and not a combined total of 35 sessions.
2. In example 2 above, the merged key from example 1 is replaced by the permanent key, and the VPN Flex license is disabled. The running key defaults to the permanent key value of 10 sessions.

3. In example 3 above, an evaluation license including 50 contexts is applied to the permanent key, so the resulting running key is a merged key that includes all the features of the permanent key plus the 50 context license.
4. In example 4 above, the merged key from example 3 has the VPN Flex key applied. Because the security appliance can only use one temporary key at a time, the VPN flex key replaces the evaluation key, so the end result is the same as the merged key from example 1.

Failover and Temporary Licenses

With failover, identical licenses are required. For failover purposes, temporary and permanent licenses appear to be identical, so you can have a permanent license on one unit and a temporary license on the other unit. This functionality is useful in an emergency situation; for example, if one of your units fails, and you have an extra unit, you can install the extra unit while the other one is repaired. If you do not normally use the extra unit for SSL VPN, then a VPN Flex license is a perfect solution while the other unit is being repaired.

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 permanent failover installation; when the temporary license expires, failover will no longer work.

Shared Licenses

A shared license lets you purchase a large number of SSL VPN sessions and share the sessions as needed amongst a group of security appliances by configuring one of the security appliances as a shared licensing server, and the rest as shared licensing participants. This section describes how a shared license works, and includes the following topics:

Information About the Shared Licensing Server and Participants

The following steps describe how shared licenses operate:

1. Decide which security appliance should be the shared licensing server, and purchase the shared licensing server license using that device serial number.
2. Decide which security appliances should be shared licensing participants, including the shared licensing backup server, and obtain a shared licensing participant license for each device, using each device serial number.
3. (Optional) Designate a second security appliance as a shared licensing backup server. You can only specify one backup server.

Note The shared licensing backup server only needs a participant license.

4. Configure a shared secret on the shared licensing server; any participants with the shared secret can use the shared license.
5. When you configure the security appliance as a participant, it registers with the shared licensing server by sending information about itself, including the local license and model information.

Note The participant needs to be able to communicate with the server over the IP network; it does not have to be on the same subnet.

6. The shared licensing server responds with information about how often the participant should poll the server.
7. When a participant uses up the sessions of the local license, it sends a request to the shared licensing server for additional sessions in 50-session increments.
8. The shared licensing server responds with a shared license. The total sessions used by a participant cannot exceed the maximum sessions for the platform model.

Note The shared licensing server can also participate in the shared license pool. It does not need a participant license as well as the server license to participate.

   a. If there are not enough sessions left in the shared license pool for the participant, then the server responds with as many sessions as available.
   b. The participant continues to send refresh messages requesting more sessions until the server can adequately fulfill the request.
9. When the load is reduced on a participant, it sends a message to the server to release the shared sessions.

Note The security appliance uses SSL between the server and participant to encrypt all communications.

Communication Issues Between Participant and Server

See the following guidelines for communication issues between the participant and server:

- If a participant fails to send a refresh after 3 times the refresh interval, then the server releases the sessions back into the shared license pool.
- If the participant cannot reach the license server to send the refresh, then the participant can continue to use the shared license it received from the server for up to 24 hours.
- If the participant is still not able to communicate with a license server after 24 hours, then the participant releases the shared license, even if it still needs the sessions. The participant leaves existing connections established, but cannot accept new connections beyond the license limit.
- If a participant reconnects with the server before 24 hours expires, but after the server expired the participant sessions, then the participant needs to send a new request for the sessions; the server responds with as many sessions as can be reassigned to that participant.

Information About the Shared Licensing Backup Server

The shared licensing backup server must register successfully with the main shared licensing server before it can take on the backup role. When it registers, the main shared licensing server syncs server settings as well as the shared license information with the backup, including a list of registered participants and the current license usage. The main server and backup server sync the data at 10 second intervals. After the initial sync, the backup server can successfully perform backup duties, even after a reload.

When the main server goes down, the backup server takes over server operation. The backup server can operate for up to 30 continuous days, after which the backup server stops issuing sessions to participants, and existing sessions time out. Be sure to reinstate the main server within that 30-day period. Critical-level syslog messages are sent at 15 days, and again at 30 days.

When the main server comes back up, it syncs with the backup server, and then takes over server operation.

When the backup server is not active, it acts as a regular participant of the main shared licensing server.

Note When you first launch the main shared licensing server, the backup server can only operate independently for 5 days. The operational limit increases day-by-day, until 30 days is reached. Also, if the main server later goes down for any length of time, the backup server operational limit decrements day-by-day. When the main server comes back up, the backup server starts to increment again day-by-day. For example, if the main server is down for 20 days, with the backup server active during that time, then the backup server will only have a 10-day limit left over. The backup server "recharges" up to the maximum 30 days after 20 more days as an inactive backup. This recharging function is implemented to discourage misuse of the shared license.

Failover and Shared Licenses

This section describes how shared licenses interact with failover, and includes the following topics:

- "Failover and Shared License Servers" section on page 15
- "Failover and Shared License Participants" section on page 17

Failover and Shared License Servers

This section describes how the main server and backup server interact with failover. Because the shared licensing server is also performing normal duties as the security appliance, including performing functions such as being a VPN gateway and firewall, then you might need to configure failover for the main and backup shared licensing servers for increased reliability.

Note The backup server mechanism is separate from, but compatible with, failover.

Shared licenses are supported only in single context mode, so Active/Active failover is not supported.

Both main shared licensing server units in the failover pair need to have the same license. So if you purchase a 10,000 session shared license for the primary main server unit, you must also purchase a 10,000 session shared license for the standby main server unit. Because the standby unit does not pass traffic when it is in a standby state, the total number of sessions remains at 10,000 in this example, *not* a combined 20,000 sessions.

For Active/Standby failover, the primary unit acts as the main shared licensing server, and the standby unit acts as the main shared licensing server after failover; because both units need to have the same license, both units can act as the main licensing server. The standby unit does *not* act as the backup shared licensing server. Instead, you can have a second pair of units acting as the backup server, if desired.

For example, you have a network with 2 failover pairs. Pair #1 includes the main licensing server. Pair #2 includes the backup server. When the primary unit from Pair #1 goes down, the standby unit immediately becomes the new main licensing server. The backup server from Pair #2 never gets used. Only if both units in Pair #1 go down does the backup server in Pair #2 come into use as the shared licensing server. If Pair #1 remains down, and the primary unit in Pair #2 goes down, then the standby unit in Pair #2 comes into use as the shared licensing server (see Figure 2).

Figure 2 Failover and Shared License Servers

The standby backup server shares the same operating limits as the primary backup server; if the standby unit becomes active, it continues counting down where the primary unit left off. See the "Information About the Shared Licensing Backup Server" section on page 15 for more information.

Failover and Shared License Participants

For participant pairs, both units register with the shared licensing server using separate participant IDs. The active unit syncs its participant ID with the standby unit. The standby unit uses this ID to generate a transfer request when it switches to the active role. This transfer request is used to move the shared sessions from the previously active unit to the new active unit.

Maximum Number of Participants

The security appliance does not limit the number of participants for the shared license; however, a very large shared network could potentially affect the performance on the licensing server. In this case, you can increase the delay between participant refreshes, or you can create two shared networks.

Licenses FAQ

Q. Can I activate multiple temporary licenses, for example, VPN Flex and Botnet Traffic Filter?

A. No. You can only use one temporary license at a time. The last license you activate is the one in use. In the case of evaluation licenses that group multiple features into one activation key, then multiple features are supported at the same time. But temporary licenses for sale by Cisco are limited to one feature per activation key.

Q. Can I "stack" temporary licenses so that when the time limit runs out, it will automatically use the next license?

A. No. You can install multiple temporary licenses, but only the last activated license is active. When the active license expires, you need to manually activate the new one. Be sure to activate it shortly *before* the old one expires so you do not lose functionality. (Any remaining time on the old license remains unused; for example, if you use 10 months of a 12-month license, and activate a new 12-month license, then the remaining 2 months of the first license goes unused unless you later reactivate it. We recommend that you activate the new license as close as possible to the end of the old license to maximize the license usage.)

Q. Can I install a new permanent license while maintaining an active temporary license?

A. No. The temporary license will be deactivated when you apply a permanent license. You have to activate the permanent license, and then reactivate the temporary license to be able to use the new permanent license along with the temporary license. This will cause temporary loss of functionality for the features reliant on the temporary license.

Q. For failover, can I use a shared licensing server as the primary unit, and the shared licensing backup server as the secondary unit?

A. No. The secondary unit must also have a shared licensing server license. The backup server, which has a participant license, can be in a separate failover pair of two backup servers.

Q. Do I need to buy the same licenses for the secondary unit in a failover pair? Even for a shared licensing server?

A. Yes. Both units need the same licenses. For a shared licensing server, you need to buy the same shared licensing server license for both units. **Note:** In Active/Standby failover, for licenses that specify the number of sessions, the sessions for both units are not added to each other; only the

active unit sessions can be used. For example, for a shared SSL VPN license, you need to purchase a 10,000 user session for both the active and the standby unit; the total number of sessions is 10,000, *not* 20,000 combined.

Q. Can I use a VPN Flex or permanent SSL VPN license in addition to a shared SSL VPN license?

A. Yes. The shared license is used only after the sessions from the locally installed license (VPN Flex or permanent) are used up. **Note**: On the shared licensing server, the permanent SSL VPN license is not used; you can however use a VPN Flex license at the same time as the shared licensing server license. In this case, the VPN Flex license sessions are available for local SSL VPN sessions only; they cannot be added to the shared licensing pool for use by participants.

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.
- Shared licenses are not supported in multiple context mode.

Firewall Mode Guidelines

All license types are available in both routed and transparent mode.

Failover Guidelines

- You must have the same licenses activated on the primary and secondary units.

  Note For failover purposes, there is no distinction between permanent and temporary licenses as long as the feature set is the same between the two units. See the "Failover and Temporary Licenses" section on page 13 for more information.

- Shared licenses are not supported in Active/Active mode. See the "Failover and Shared Licenses" section on page 15 for more information.

Upgrade Guidelines

Your activation key remains compatible if you upgrade to Version 8.2 or later, and also if you later downgrade. After you upgrade, if you activate additional feature licenses that were introduced *before 8.2*, then the activation key continues to be compatible with earlier versions if you downgrade. However if you activate feature licenses that were introduced in *8.2 or later*, then the activation key is not backwards compatible. If you have an incompatible license key, then see the following guidelines:

- If you previously entered an activation key in an earlier version, then the security appliance uses that key (without any of the new licenses you activated in Version 8.2 or later).
- If you have a new system and do not have an earlier activation key, then you need to request a new activation key compatible with the earlier version.

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 and it is covered with Cisco TAC, 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).
- Although you can activate all license types, some features are incompatible with each other; for example, multiple context mode and VPN. In the case of the AnyConnect Essentials license, the license is incompatible with the following licenses: full SSL VPN license, shared SSL VPN license, and Advanced Endpoint Assessment license. By default, the AnyConnect Essentials license is used instead of the above licenses, but you can disable the AnyConnect Essentials license in the configuration to restore use of the other licenses using the **no anyconnect-essentials** command.

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

For the CLI:

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

For ASDM:

To view the current license, choose Configuration > Device Management > Licensing > Activation Key.

In multiple context mode, view the activation key in the System execution space by choosing Configuration > Device Management > Activation Key.

Examples

The following is sample output from the **show activation-key detail** command that shows a permanent activation license with 2 SSL VPN peers (in bold), an active temporary license with 5000 SSL VPN peers (in bold), the merged running license with the SSL VPN peers taken from the temporary license (in bold), 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                    : 2
SSL VPN Peers                : 2
Total VPN Peers              : 250
Shared License               : Enabled
  Shared SSL VPN Peers       : 5000
AnyConnect for Mobile        : Disabled
AnyConnect for Linksys phone : Disabled
AnyConnect Essentials        : Disabled
Advanced Endpoint Assessment : Disabled
UC Phone Proxy Sessions      : 24
Total UC Proxy Sessions      : 24
Botnet Traffic Filter        : Enabled

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                 : Enabled
Security Contexts            : 2
GTP/GPRS                     : Disabled
SSL VPN Peers                : 5000
Total VPN Peers              : 250
Shared License               : Enabled
  Shared SSL VPN Peers       : 10000
AnyConnect for Mobile        : Disabled
AnyConnect for Linksys phone : Disabled
AnyConnect Essentials        : Disabled
Advanced Endpoint Assessment : Disabled
UC Phone Proxy Sessions      : 24
Total UC Proxy Sessions      : 24
Botnet Traffic Filter        : Enabled

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
SSL VPN Peers                : 5000
Total VPN Peers              : 250
Shared License               : Enabled
  Shared SSL VPN Peers       : 10000
AnyConnect for Mobile        : Disabled
```

```
AnyConnect for Linksys phone : Disabled
AnyConnect Essentials        : Disabled
Advanced Endpoint Assessment : Disabled
UC Phone Proxy Sessions      : 24
Total UC Proxy Sessions      : 24
Botnet Traffic Filter        : Enabled


This platform has an ASA 5540 VPN Premium license.
This is a Shared SSL VPN License server.

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 (for ASDM) choosing Configuration > Device Management > Licensing > Activation Key (in multiple context mode, view the serial number in the System execution space) or 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

This section describes how to enter a new activation key.

Prerequisites

- Before entering the activation key, ensure that the image in Flash memory and the running image are the same by entering the show activation-key command. You can do this by reloading the security appliance before entering the new activation key.
- 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 10 lists the licenses that require reloading.

Table 10 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.

Limitations and Restrictions

Your activation key remains compatible if you upgrade to Version 8.2 or later, and also if you later downgrade. After you upgrade, if you activate additional feature licenses that were introduced *before 8.2*, then the activation key continues to be compatible with earlier versions if you downgrade. However if you activate feature licenses that were introduced in *8.2 or later*, then the activation key is not backwards compatible. If you have an incompatible license key, then see the following guidelines:

- If you previously entered an activation key in an earlier version, then the security appliance uses that key (without any of the new licenses you activated in Version 8.2 or later).
- If you have a new system and do not have an earlier activation key, then you need to request a new activation key compatible with the earlier version.

Detailed Steps

For the CLI:

	Command	Purpose
Step 1	**activation-key** *key* **Example:** `hostname# 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 "Temporary, VPN Flex, and Evaluation Licenses" section on page 11 for more information. To change the running activation key, enter the **activation-key** command with a new key value.
Step 2	**reload** **Example:** `hostname# 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 10 on page 22 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.`

For ASDM:

Step 1 Choose Configuration > Device Management > Licensing > Activation Key.

Step 2 Enter the new activation key in the New Activation Key field.

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. For example:

```
0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490
```

You can enter one permanent key, and multiple temporary keys. The last temporary key entered is the active one. See the "Temporary, VPN Flex, and Evaluation Licenses" section on page 11 for more information. To change the running activation key, enter a new value.

Step 3 Click **Update Activation Key**.

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 10 on page 22 for more information about licenses requiring a reload. This section includes the following topics:

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 10 on page 22 for more information about licenses requiring a reload. This procedure ensures that there is no downtime.

Prerequisites

Before you upgrade the license, be sure that both units are operating correctly, the Failover LAN interface is up, and there is not an imminent failover event; for example, monitored interfaces are operating normally.

On each unit, enter the **show failover** command or in ASDM go to Monitoring > Properties > Failover > Status to view the failover status and the monitored interface status.

Detailed Steps

For the CLI:

	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 a pseudo-standby state. Deactivating failover on the active unit prevents the standby unit from attempting to become active during the period when the licenses do not match.
Step 2	**activation-key** *key* **Example:** `active(config)# activation-key 0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490`	Installs the new license on the active unit. Make sure this license is for the active unit serial number.
	On the standby unit:	
Step 3	**activation-key** *key* **Example:** `standby# activation-key 0xc125727f 0x903de1ee 0x8c838928 0x92dc84d4 0x003a2ba0`	Installs the new license on the standby unit. Make sure this license is for the standby unit serial number.
	On the active unit:	
Step 4	**failover** **Example:** `active(config)# failover`	Reenables failover.

For ASDM:

Step 1 On the active unit, choose Configuration > Device Management > High Availability > Failover > Setup, and uncheck the **Enable Failover** check box.

The standby unit remains in a pseudo-standby state. Deactivating failover on the active unit prevents the standby unit from attempting to become active during the period when the licenses do not match.

Step 2 Click **Apply**.

Step 3 Choose Configuration > Device Management > Licensing > Activation Key, and enter the new activation key that you obtained with the active unit serial number.

Step 4 Click **Update Activation Key**.

Step 5 Log into the standby unit by double-clicking its address in the Device List.

If you the device is not in the Device List, click **Add** to add the device. You might be prompted for credentials to log in.

Step 6 Choose Configuration > Device Management > Licensing > Activation Key, and enter the new activation key that you obtained with the standby unit serial number.

Step 7 Click **Update Activation Key**.

Step 8 Log into the active unit again by double-clicking its address in the Device List.

Step 9 Choose Configuration > Device Management > High Availability > Failover > Setup, and re-check the **Enable Failover** check box.

Step 10 Click **Apply**.

Upgrading the License for a Failover (Reload Required)

Use the following procedure if your new license requires you to reload. See Table 10 on page 22 for more information about licenses requiring a reload. Reloading the failover pair causes a loss of connectivity during the reload.

Prerequisites

Before you upgrade the license, be sure that both units are operating correctly, the Failover LAN interface is up, and there is not an imminent failover event; for example, monitored interfaces are operating normally.

On each unit, enter the **show failover** command or in ASDM choose Monitoring > Properties > Failover > Status to view the failover status and the monitored interface status.

Detailed Steps

For the CLI:

	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 a pseudo-standby state. Deactivating failover on the active unit prevents the standby unit from attempting to become active during the period when the licenses do not match.

	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. 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 24 instead of this procedure.
	On the standby unit:	
Step 3	**activation-key** *key* **Example:** `standby# activation-key 0xc125727f 0x903de1ee 0x8c838928 0x92dc84d4 0x003a2ba0`	Installs the new license on the standby unit.
Step 4	**reload** **Example:** `standby# 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.

For ASDMI:

Step 1 On the active unit, choose Configuration > Device Management > High Availability > Failover > Setup, and uncheck the **Enable Failover** check box.

The standby unit remains in a pseudo-standby state. Deactivating failover on the active unit prevents the standby unit from attempting to become active during the period when the licenses do not match.

Step 2 Click **Apply**.

Step 3 Choose Configuration > Device Management > Licensing > Activation Key, and enter the new activation key that you obtained with the active unit serial number.

Step 4 Click **Update Activation Key**.

Step 5 Log into the standby unit by double-clicking its address in the Device List.

If you the device is not in the Device List, click **Add** to add the device. You might be prompted for credentials to log in.

Step 6 Choose Configuration > Device Management > Licensing > Activation Key, and enter the new activation key that you obtained with the standby unit serial number.

Step 7 Click **Update Activation Key**.

Step 8 Log into the active unit again by double-clicking its address in the Device List.

Step 9 Choose Configuration > Device Management > High Availability > Failover > Setup, and recheck the **Enable Failover** check box.

Step 10 Click **Apply**.

Step 11 Schedule a reload of the security appliance by choosing Tools > System Reload.

Step 12 Choose the reload options to reload the security appliance at a time you desire, and click **Schedule Reload**.

Choose a time when the loss of service has the least impact.

Step 13 Log into the standby unit again by double-clicking its address in the Device List.

Step 14 Schedule a reload of the security appliance by choosing Tools > System Reload.

Step 15 Choose the reload options to reload the security appliance at the same time you choose for the active unit, and click **Schedule Reload**.

Both units will reload at the same time, and the new licenses will be in effect.

Configuring a Shared License

This section describes how to configure the shared licensing server and participants. For more information about shared licenses, see the "Shared Licenses" section on page 13.

This section includes the following topics:

Configuring the Shared Licensing Server

This section describes how to configure the security appliance to be a shared licensing server.

Prerequisites

The server must have a shared licensing server key.

Detailed Steps

For the CLI:

	Command	Purpose
Step 1	**license-server secret** *secret* **Example:** `hostname(config)# license-server secret farscape`	Sets the shared secret, a string between 4 and 128 ASCII characters. Any participant with this secret can use the licensing server.
Step 2	(Optional) **license-server refresh-interval** *seconds* **Example:** `hostname(config)# license-server refresh-interval 100`	Sets the refresh interval between 10 and 300 seconds; this value is provided to participants to set how often they should communicate with the server. The default is 30 seconds.
Step 3	(Optional) **license-server port** *port* **Example:** `hostname(config)# license-server port 40000`	Sets the port on which the server listens for SSL connections from participants, between 1 and 65535. The default is TCP port 50554.
Step 4	(Optional) **license-server backup** *address* **backup-id** *serial_number* [**ha-backup-id** *ha_serial_number*] **Example:** `hostname(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id JMX1378N0W3`	Identifies the backup server IP address and serial number. If the backup server is part of a failover pair, identify the standby unit serial number as well. You can only identify 1 backup server and its optional standby unit.
Step 5	**license-server enable** *interface_name* **Example:** `hostname(config)# license-server enable inside`	Enables this unit to be the shared licensing server. Specify the interface on which participants contact the server. You can repeat this command for as many interfaces as desired.

For ASDM:

Step 1 Choose **Configuration > Device Management > Licenses > Shared SSL VPN Licenses**.

Step 2 In the Shared Secret field, enter the shared secret as a string between 4 and 128 ASCII characters.

Any participant with this secret can use the license server.

Step 3 (Optional) In the TCP IP Port field, enter the port on which the server listens for SSL connections from participants, between 1 and 65535.

The default is TCP port 50554.

Step 4 (Optional) In the Refresh interval field, enter the refresh interval between 10 and 300 seconds.

This value is provided to participants to set how often they should communicate with the server. The default is 30 seconds.

Step 5 In the Interfaces that serve shared licenses area, check the **Shares Licenses** check box for any interfaces on which participants contact the server.

Step 6 (Optional) To identify a backup server, in the Optional backup shared SSL VPN license server area:

a. In the Backup server IP address field, enter the backup server IP address.

b. In the Primary backup server serial number field, enter the backup server serial number.

c. If the backup server is part of a failover pair, identify the standby unit serial number in the Secondary backup server serial number field.

You can only identify 1 backup server and its optional standby unit.

Step 7 Click **Apply**.

Examples

The following example sets the shared secret, changes the refresh interval and port, configures a backup server, and enables this unit as the shared licensing server on the inside interface and dmz interface.

```
hostname(config)# license-server secret farscape
hostname(config)# license-server refresh-interval 100
hostname(config)# license-server port 40000
hostname(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
hostname(config)# license-server enable inside
hostname(config)# license-server enable dmz
```

What to Do Next

See the "Configuring the Shared Licensing Backup Server (Optional)" section on page 29 (CLI only), or the "Configuring the Shared Licensing Participant and, for ASDM, the Optional Backup Server" section on page 30.

Configuring the Shared Licensing Backup Server (Optional)

(CLI Procedure Only)

This section enables a shared license participant to act as the backup server if the main server goes down.

Prerequisites

The backup server must have a shared licensing participant key.

Detailed Steps

	Command	Purpose
Step 1	**license-server address** *address* **secret** *secret* [**port** *port*] **Example:** `hostname(config)# license-server address 10.1.1.1 secret farscape`	Identifies the shared licensing server IP address and shared secret. If you changed the default port in the server configuration, set the port for the backup server to match.
Step 2	**license-server backup enable** *interface_name* **Example:** `hostname(config)# license-server backup enable inside`	Enables this unit to be the shared licensing backup server. Specify the interface on which participants contact the server. You can repeat this command for as many interfaces as desired.

Examples

The following example identifies the license server and shared secret, and enables this unit as the backup shared license server on the inside interface and dmz interface.

```
hostname(config)# license-server address 10.1.1.1 secret farscape
hostname(config)# license-server backup enable inside
hostname(config)# license-server backup enable dmz
```

What to Do Next

See the "Configuring the Shared Licensing Participant and, for ASDM, the Optional Backup Server" section on page 30.

Configuring the Shared Licensing Participant and, for ASDM, the Optional Backup Server

This section configures a shared licensing participant to communicate with the shared licensing server; for ASDM, this section also describes how you can optionally configure the participant as the backup server. To configure a backup server in the CLI, see the "Configuring the Shared Licensing Backup Server (Optional)" section on page 29.

Prerequisites

The participant must have a shared licensing participant key.

Detailed Steps

For the CLI:

	Command	Purpose
Step 1	**license-server address** *address* **secret** *secret* [**port** *port*] **Example:** `hostname(config)# license-server address 10.1.1.1 secret farscape`	Identifies the shared licensing server IP address and shared secret. If you changed the default port in the server configuration, set the port for the participant to match.
Step 2	(Optional) **license-server backup address** *address* **Example:** `hostname(config)# license-server backup address 10.1.1.2`	If you configured a backup server, enter the backup server address.

For ASDM:

Step 1 Choose the Configuration > Device Management > Licenses > Shared SSL VPN Licenses pane.

Step 2 In the Shared Secret field, enter the shared secret as a string between 4 and 128 ASCII characters.

Step 3 (Optional) In the TCP IP Port field, enter the port on which to communicate with the server using SSL, between 1 and 65535.

The default is TCP port 50554.

Step 4 (Optional) To identify the participant as the backup server, in the Select backup role of participant area:

a. Click the **Backup Server** radio button.

b. Check the **Shares Licenses** check box for any interfaces on which participants contact the backup server.

Step 5 Click **Apply**.

Examples

The following example sets the license server IP address and shared secret, as well as the backup license server IP address:

```
hostname(config)# license-server address 10.1.1.1 secret farscape
hostname(config)# license-server backup address 10.1.1.2
```

Monitoring the Shared License

To monitor the shared license, in ASDM choose Monitoring > VPN > Clientless SSL VPN > Shared Licenses or enter one of the following commands.

Command	Purpose
show shared license [**detail** | **client** [*hostname*] | **backup**]	Shows shared license statistics. Optional keywords ar available only for the licensing server: the **detail** keyword shows statistics per participant. To limit the display to one participant, use the **client** keyword. The **backup** keyword shows information about the backup server. To clear the shared license statistics, enter the **clear shared license** command.
show activation-key	Shows the licenses installed on the security appliance. The **show version** command also shows license information.
show vpn-sessiondb	Shows license information about VPN sessions.

Examples

The following is sample output from the **show shared license** command on the license participant:

```
hostname>  show shared license
Primary License Server : 10.3.32.20
  Version              : 1
  Status               : Inactive

Shared license utilization:
  SSLVPN:
    Total for network :     5000
    Available         :     5000
    Utilized          :        0
  This device:
    Platform limit    :      250
    Current usage     :        0
    High usage        :        0
  Messages Tx/Rx/Error:
    Registration    : 0 / 0 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0
```

The following is sample output from the **show shared license detail** command on the license server:

```
hostname>  show shared license detail
Backup License Server Info:

Device ID           : ABCD
Address             : 10.1.1.2
Registered          : NO
HA peer ID          : EFGH
Registered          : NO
  Messages Tx/Rx/Error:
    Hello           : 0 / 0 / 0
    Sync            : 0 / 0 / 0
    Update          : 0 / 0 / 0

Shared license utilization:
  SSLVPN:
```

```
    Total for network :      500
    Available         :      500
    Utilized          :        0
  This device:
    Platform limit    :      250
    Current usage     :        0
    High usage        :        0
  Messages Tx/Rx/Error:
    Registration    : 0 / 0 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0


Client Info:

  Hostname          : 5540-A
  Device ID         : XXXXXXXXXXX
  SSLVPN:
    Current usage   : 0
    High            : 0
  Messages Tx/Rx/Error:
    Registration    : 1 / 1 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0
...
```

Feature History for Licensing

Table 11 lists the release history for this feature.

Table 11 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	7.1(1)	SSL VPN licenses were introduced.
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 11 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 security appliance 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 security appliance (from 10 to 50 for the Base license, and from 25 to 100 for the Security Plus license), the ASA 5520 adaptive security appliance (from 100 to 150), the ASA 5550 adaptive security appliance (from 200 to 250).
Gigabit Ethernet Support for the ASA 5510 Security Plus License	7.2(3)	The ASA 5510 security appliance now supports Gigabit Ethernet (1000 Mbps) for the Ethernet 0/0 and 0/1 ports with the Security Plus license. In the Base license, they continue to be used as Fast Ethernet (100 Mbps) ports. Ethernet 0/2, 0/3, and 0/4 remain as Fast Ethernet ports for both licenses. **Note** The interface names 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	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. Cisco can provide timely updates to the list of applications and versions that Host Scan supports in a package that is separate from Cisco Secure Desktop.
VPN Load Balancing for the ASA 5510	8.0(2)	VPN load balancing is now supported on the ASA 5510 Security Plus license.

Table 11 Feature History for Licensing (continued)

Feature Name	Releases	Feature Information
AnyConnect for Mobile License	8.0(3)	The AnyConnect for Mobile license lets Windows mobile devices connect to the security appliance using the AnyConnect client.
VPN Flex and Evaluation Licenses	8.0(4)/8.1(2)	Support for temporary licenses was introduced. VPN Flex licenses provide temporary support for extra SSL VPN sessions.
Increased VLANs for the ASA 5580	8.1(2)	The number of VLANs supported on the ASA 5580 are increased from 100 to 250.
Unified Communications Proxy Sessions license	8.0(4)	The UC Proxy sessions license was introduced. This feature is not available in Version 8.1.
Botnet Traffic Filter License	8.2(1)	The Botnet Traffic Filter license was introduced. The Botnet Traffic Filter protects against malware network activity by tracking connections to known bad domains and IP addresses.
AnyConnect Essentials License	8.2(1)	This license enables AnyConnect VPN client access to the adaptive security appliance. This license does not support browser-based SSL VPN access or Cisco Secure Desktop. For these features, activate an AnyConnect Premium SSL VPN license instead of the AnyConnect Essentials license. **Note** With the AnyConnect Essentials license, VPN users can use a Web browser to log in, and download and start (WebLaunch) the AnyConnect client. The AnyConnect client software offers the same set of client features, whether it is enabled by this license or an AnyConnect Premium SSL VPN license. The AnyConnect Essentials license cannot be active at the same time as the following licenses on a given adaptive security appliance: AnyConnect Premium SSL VPN license (all types) or the Advanced Endpoint Assessment license. You can, however, run AnyConnect Essentials and AnyConnect Premium SSL VPN licenses on different adaptive security appliances in the same network. By default, the security appliance uses the AnyConnect Essentials license, but you can disable it to use other licenses by using the **no anyconnect-essentials** command.
Shared Licenses for SSL VPN	8.2(1)	Shared licenses for SSL VPN were introduced. Multiple security appliances can share a pool of SSL VPN sessions on an as-needed basis.
Mobility Proxy application no longer requires Unified Communications Proxy license	8.2(2)	The Mobility Proxy no longer requires the UC Proxy license.

Table 11 Feature History for Licensing (continued)

Feature Name	Releases	Feature Information
10 GE I/O license for the ASA 5585-X with SSP-20	8.2(3)	We introduced the 10 GE I/O license for the ASA 5585-X with SSP-20 to enable 10-Gigabit Ethernet speeds for the fiber ports. The SSP-60 supports 10-Gigabit Ethernet speeds by default.
10 GE I/O license for the ASA 5585-X with SSP-10	8.2(4)	We introduced the 10 GE I/O license for the ASA 5585-X with SSP-10 to enable 10-Gigabit Ethernet speeds for the fiber ports. The SSP-40 supports 10-Gigabit Ethernet speeds by default.