Managing Feature Licenses for Cisco ASA 5500 Version 8.3

January 2011

A license specifies the options that are enabled on a given adaptive security appliance. This document describes how to obtain a license activation key and how to activate it. It also describes the available licenses for each model.

Note This chapter describes licensing for Version 8.3; for other versions, see the licensing documentation that applies to your version:

http://www.cisco.com/en/US/products/ps6120/products_licensing_information_listing.html

This chapter 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:

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

- VPN License and Feature Compatibility, page 12

Licenses Per Model

This section lists the feature licenses available for each model:

- ASA 5505, Table 1-5 on page 3
- ASA 5510, Table 1-6 on page 4
- ASA 5520, Table 1-7 on page 5
- ASA 5540, Table 1-8 on page 6
- ASA 5550, Table 1-9 on page 7
- ASA 5580, Table 1-10 on page 8

Note The ASA 5585-X is supported in 8.2(3) and later; because these tables are for Version 8.3, the 5585-X is not included in this section. See *Managing Feature Licenses for Cisco ASA 5500 Version 8.2:* http://www.cisco.com/en/US/docs/security/asa/asa82/license/license82.html.

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 Clientless SSL VPN license plus the GTP/GPRS license; or all four licenses together.

Table 1-5 shows the licenses for the ASA 5505.

Table 1-5 ASA 5505 Adaptive Security Appliance License Features

ASA 5505	Base License		Security Plus	
Firewall Licenses				
Botnet Traffic Filter[1]	Disabled	*Optional Time-based license: Available*	Disabled	*Optional Time-based license: Available*
Firewall Conns, Concurrent	10 K		25 K	
GTP/GPRS	No support		No support	
Intercompany Media Engine[1]	Disabled	*Optional license: Available*	Disabled	*Optional license: Available*
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 Edition (sessions)[1]	2	*Optional Permanent or Time-based licenses:*	2	*Optional Permanent or Time-based 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[1]	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 on page 9.
2. See the "VPN License and Feature Compatibility" section on page 12.
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 1-6 shows the licenses for the ASA 5510.

Table 1-6 ASA 5510 Adaptive Security Appliance License Features

ASA 5510	Base License	Security Plus
Firewall Licenses		
Botnet Traffic Filter[1]	Disabled *Optional Time-based license: Available*	Disabled *Optional Time-based license: Available*
Firewall Conns, Concurrent	50 K	130 K
GTP/GPRS	No support	No support
Intercompany Media Engine[1]	Disabled *Optional license: Available*	Disabled *Optional license: Available*
Unified Comm. Sessions[1]	2 *Optional licenses:* *24* *50* *100*	2 *Optional licenses:* *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 Edition (sessions)	2 *Optional Permanent or Time-based licenses:* *10* *25* *50* *100* *250* *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*	2 *Optional Permanent or Time-based licenses:* *10* *25* *50* *100* *250* *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*
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 (and any others): Fast Ethernet
Security Contexts	No support	2 *Optional licenses:* *5*
VLANs, Maximum	50	100

1. See the "License Notes" section on page 9.
2. See the "VPN License and Feature Compatibility" section on page 12.
3. Although the Ethernet 0/0 and 0/1 ports are Gigabit Ethernet, they are still identified as "Ethernet" in the software.

Table 1-7 shows the licenses for the ASA 5520.

Table 1-7 ASA 5520 Adaptive Security Appliance License Features

ASA 5520	Base License						
Firewall Licenses							
Botnet Traffic Filter[1]	Disabled	*Optional Time-based license: Available*					
Firewall Conns, Concurrent	280 K						
GTP/GPRS	Disabled	*Optional license: Available*					
Intercompany Media Engine[1]	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 Edition (sessions)	2	*Optional Permanent or Time-based 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*	
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 on page 9.
2. See the "VPN License and Feature Compatibility" section on page 12.

Table 1-8 shows the licenses for the ASA 5540.

Table 1-8 ASA 5540 Adaptive Security Appliance License Features

ASA 5540	Base License								
Firewall Licenses									
Botnet Traffic Filter[1]	Disabled	*Optional Time-based license: Available*							
Firewall Conns, Concurrent	400 K								
GTP/GPRS	Disabled	*Optional license: Available*							
Intercompany Media Engine[1]	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 Edition (sessions)	2	*Optional Permanent or Time-based 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*			
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 on page 9.
2. See the "VPN License and Feature Compatibility" section on page 12.

Table 1-9 shows the licenses for the ASA 5550.

Table 1-9 ASA 5550 Adaptive Security Appliance License Features

ASA 5550	Base License									
Firewall Licenses										
Botnet Traffic Filter[1]	Disabled	*Optional Time-based license: Available*								
Firewall Conns, Concurrent	650 K									
GTP/GPRS	Disabled	*Optional license: Available*								
Intercompany Media Engine[1]	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 Edition (sessions)	2	*Optional Permanent or Time-based 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*			
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 on page 9.
2. See the "VPN License and Feature Compatibility" section on page 12.

Table 1-10 shows the licenses for the ASA 5580.

Table 1-10 ASA 5580 Adaptive Security Appliance License Features

ASA 5580	Base License										
Firewall Licenses											
Botnet Traffic Filter[1]	Disabled	*Optional Time-based license: Available*									
Firewall Conns, Concurrent	5580-20: 1,000 K 5580-40: 2,000 K										
GTP/GPRS	Disabled	*Optional license: Available*									
Intercompany Media Engine[1]	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 Edition (sessions)	2	*Optional Permanent or Time-based 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*				
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 on page 9.
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 on page 12.

License Notes

Table 1-11 includes common footnotes shared by multiple tables in the "Licenses Per Model" section on page 2.

Table 1-11 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 browser-based (clientless) SSL VPN access or Cisco Secure Desktop. For these features, activate an AnyConnect Premium SSL VPN Edition 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 Edition 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 Edition license (all types) or the Advanced Endpoint Assessment license. You can, however, run AnyConnect Essentials and AnyConnect Premium SSL VPN Edition licenses on different adaptive security appliances in the same network. By default, the adaptive security appliance uses the AnyConnect Essentials license, but you can disable it to use other licenses by using the **no anyconnect-essentials** command or in ASDM, using the Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Essentials pane. See also the "VPN License and Feature Compatibility" section on page 12.
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 of SSL VPN sessions permitted: AnyConnect Essentials or AnyConnect Premium SSL VPN Edition.
AnyConnect Premium SSL VPN Edition Shared	A shared license lets the adaptive security appliance act as a shared license server for multiple client adaptive security appliances. The shared license pool is large, but the maximum number of sessions used by each individual adaptive 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.
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 adaptive 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 1-11 License Notes (continued)

License	Notes
Intercompany Media Engine	When you enable the Intercompany Media Engine (IME) license, you can use TLS proxy sessions up to the TLS proxy limit. If you also have a Unified Communications (UC) license installed that is higher than the default TLS proxy limit, then the adaptive security appliance sets the limit to be the UC license limit plus an additional number of sessions depending on your model. You can manually configure the TLS proxy limit using the **tls-proxy maximum-sessions** command or in ASDM, using the **Configuration > Firewall > Unified Communications > TLS Proxy** pane. To view the limits of your model, enter the **tls-proxy maximum-sessions ?** command. If you also install the UC license, then the TLS proxy sessions available for UC are also available for IME sessions. For example, if the configured limit is 1000 TLS proxy sessions, and you purchase a 750-session UC license, then the first 250 IME sessions do not affect the sessions available for UC. If you need more than 250 sessions for IME, then the remaining 750 sessions of the platform limit are used on a first-come, first-served basis by UC and IME. • For a license part number ending in "K8", TLS proxy sessions are limited to 1000. • For a license part number ending in "K9", the TLS proxy limit depends on your configuration and the platform model. **Note** K8 and K9 refer to whether the license is restricted for export: K8 is unrestricted, and K9 is restricted. You might also use SRTP encryption sessions for your connections: • For a K8 license, SRTP sessions are limited to 250. • For a K9 license, there is not limit. **Note** Only calls that require encryption/decryption for media are counted towards the SRTP limit; if passthrough is set for the call, even if both legs are SRTP, they do not count towards the limit.

Table 1-11 License Notes (continued)

License	Notes
Unified Communications Proxy sessions	The following applications use TLS proxy sessions for their connections. Each TLS proxy session used by these applications (and only these applications) is counted against the UC license limit: • Phone Proxy • Presence Federation Proxy • Encrypted Voice Inspection Other applications that use TLS proxy sessions do not count towards the UC limit, for example, Mobility Advantage Proxy (which does not require a license) and IME (which requires a separate IME license). Some UC applications might use multiple sessions for a connection. For example, if you configure a phone with a primary and backup Cisco Unified Communications Manager, there are 2 TLS proxy connections, so 2 UC Proxy sessions are used. You independently set the TLS proxy limit using the **tls-proxy maximum-sessions** command or in ASDM, using the **Configuration > Firewall > Unified Communications > TLS Proxy** pane. To view the limits of your model, enter the **tls-proxy maximum-sessions ?** command. When you apply a UC license that is higher than the default TLS proxy limit, the adaptive security appliance automatically sets the TLS proxy limit to match the UC limit. The TLS proxy limit takes precedence over the UC license limit; if you set the TLS proxy limit to be less than the UC license, then you cannot use all of the sessions in your UC license. **Note** For license part numbers ending in "K8" (for example, licenses under 250 users), TLS proxy sessions are limited to 1000. For license part numbers ending in "K9" (for example, licenses 250 users or larger), the TLS proxy limit depends on the configuration, up to the model limit. K8 and K9 refer to whether the license is restricted for export: K8 is unrestricted, and K9 is restricted. If you clear the configuration (using the **clear configure all** command, for example), then the TLS proxy limit is set to the default for your model; if this default is lower than the UC license limit, then you see an error message to use the **tls-proxy maximum-sessions** command to raise the limit again (in ASDM, use the **TLS Proxy** pane). If you use failover and enter the **write standby** command or in ASDM, use **File > Save Running Configuration to Standby Unit** on the primary unit to force a configuration synchronization, the **clear configure all** command is generated on the secondary unit automatically, so you may see the warning message on the secondary unit. Because the configuration synchronization restores the TLS proxy limit set on the primary unit, you can ignore the warning. You might also use SRTP encryption sessions for your connections: • For K8 licenses, SRTP sessions are limited to 250. • For K9 licenses, there is not limit. **Note** Only calls that require encryption/decryption for media are counted towards the SRTP limit; if passthrough is set for the call, even if both legs are SRTP, they do not count towards the limit.
VPN load balancing	Requires a Strong Encryption (3DES/AES) License.

VPN License and Feature Compatibility

Table 1-12 shows how the VPN licenses and features can combine.

For a detailed list of the features supported by the AnyConnect Essentials license and AnyConnect Premium license, see *AnyConnect Secure Mobility Client Features, Licenses, and OSs*:

- Version 3.0: http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect30/feature/guide/anyconnect30features.html
- Version 2.5: http://www.cisco.com/en/US/docs/security/vpn_client/anyconnect/anyconnect25/feature/guide/anyconnect25features.html

Table 1-12 VPN License and Feature Compatibility

	Enable one of the following licenses:[1]	
Supported with:	**AnyConnect Essentials**	**AnyConnect Premium SSL VPN Edition**
AnyConnect Mobile	**Yes**	**Yes**
Advanced Endpoint Assessment	**No**	**Yes**
AnyConnect Premium SSL VPN Edition 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 adaptive 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 adaptive 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 adaptive 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 24 section to determine which licenses you have installed.

Permanent License

You can have one permanent activation key installed. The permanent activation key includes all licensed features in a single key. If you also install time-based licenses, the adaptive security appliance combines the permanent and time-based licenses into a running license. See the "How Permanent and Time-Based Licenses Combine" section on page 14 for more information about how the adaptive security appliance combines the licenses.

Time-Based Licenses

In addition to permanent licenses, you can purchase time-based licenses or receive an evaluation license that has a time-limit. For example, you might buy a time-based SSL VPN license to handle short-term surges in the number of concurrent SSL VPN users, or you might order a Botnet Traffic Filter time-based license that is valid for 1 year.

This section includes the following topics:

Time-Based License Activation Guidelines

- You can install multiple time-based licenses, including multiple licenses for the same feature. However, only one time-based license per feature can be *active* at a time. The inactive license remains installed, and ready for use. For example, if you install a 1000-session SSL VPN license, and a 2500-session SSL VPN license, then only one of these licenses can be active.
- If you activate an evaluation license that has multiple features in the key, then you cannot also activate another time-based license for one of the included features. For example, if an evaluation license includes the Botnet Traffic Filter and a 1000-session SSL VPN license, you cannot also activate a standalone time-based 2500-session SSL VPN license.

How the Time-Based License Timer Works

- The timer for the time-based license starts counting down when you activate it on the adaptive security appliance.
- If you stop using the time-based license before it times out, then the timer halts. The timer only starts again when you reactivate the time-based license.

- If the time-based license is active, and you shut down the adaptive security appliance, then the timer continues to count down. If you intend to leave the adaptive security appliance in a shut down state for an extended period of time, then you should deactivate the time-based license before you shut down.

Note We suggest you do not change the system clock after you install the time-based license. If you set the clock to be a later date, then if you reload, the adaptive 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 Permanent and Time-Based Licenses Combine

When you activate a time-based license, then features from both permanent and time-based licenses combine to form the running license. How the permanent and time-based licenses combine depends on the type of license. Table 1-13 lists the combination rules for each feature license.

Note Even when the permanent license is used, if the time-based license is active, it continues to count down.

Table 1-13 Time-Based License Combination Rules

Time-Based Feature	Combined License Rule
SSL VPN Sessions	The higher value is used, either time-based or permanent. For example, if the permanent license is 1000 sessions, and the time-based license is 2500 sessions, then 2500 sessions are enabled. Typically, you will not install a time-based license that has less capability than the permanent license, but if you do so, then the permanent license is used.
Unified Communications Proxy Sessions	The time-based license sessions are added to the permanent sessions, up to the platform limit. For example, if the permanent license is 2500 sessions, and the time-based license is 1000 sessions, then 3500 sessions are enabled for as long as the time-based license is active.
Security Contexts	The time-based license contexts are added to the permanent contexts, up to the platform limit. For example, if the permanent license is 10 contexts, and the time-based license is 20 contexts, then 30 contexts are enabled for as long as the time-based license is active.
Botnet Traffic Filter	There is no permanent Botnet Traffic Filter license available; the time-based license is used.
All Others	The higher value is used, either time-based or permanent. For licenses that have a status of enabled or disabled, then the license with the enabled status is used. For licenses with numerical tiers, the higher value is used. Typically, you will not install a time-based license that has less capability than the permanent license, but if you do so, then the permanent license is used.

To view the combined license, see the "Viewing Your Current License" section on page 24.

Stacking Time-Based Licenses

In many cases, you might need to renew your time-based license and have a seamless transition from the old license to the new one. For features that are only available with a time-based license, it is especially important that the license not expire before you can apply the new license. The adaptive security appliance allows you to *stack* time-based licenses so you do not have to worry about the license expiring or about losing time on your licenses because you installed the new one early.

When you install an identical time-based license as one already installed, then the licenses are combined, and the duration equals the combined duration.

For example:

1. You install a 52-week Botnet Traffic Filter license, and use the license for 25 weeks (27 weeks remain).
2. You then purchase another 52-week Botnet Traffic Filter license. When you install the second license, the licenses combine to have a duration of 79 weeks (52 weeks plus 27 weeks).

Similarly:

1. You install an 8-week 1000-session SSL VPN license, and use it for 2 weeks (6 weeks remain).
2. You then install another 8-week 1000-session license, and the licenses combine to be 1000-sessions for 14 weeks (8 weeks plus 6 weeks).

If the licenses are not identical (for example, a 1000-session SSL VPN license vs. a 2500-session license), then the licenses are *not* combined. Because only one time-based license per feature can be active, only one of the licenses can be active. See the "Activating or Deactivating Keys" section on page 30 for more information about activating licenses.

Although non-identical licenses do not combine, when the current license expires, the adaptive security appliance automatically activates an installed license of the same feature if available. See the "Time-Based License Expiration" section on page 15 for more information.

Time-Based License Expiration

When the current license for a feature expires, the adaptive security appliance automatically activates an installed license of the same feature if available. If there are no other time-based licenses available for the feature, then the permanent license is used.

If you have more than one additional time-based license installed for a feature, then the adaptive security appliance uses the first license it finds; which license is used is not user-configurable and depends on internal operations. If you prefer to use a different time-based license than the one the adaptive security appliance activated, then you must manually activate the license you prefer. See the "Activating or Deactivating Keys" section on page 30.

For example, you have a time-based 2500-session SSL VPN license (active), a time-based 1000-session SSL VPN license (inactive), and a permanent 500-session SSL VPN license. While the 2500-session license expires, the adaptive security appliance activates the 1000-session license. After the 1000-session license expires, the adaptive security appliance uses the 500-session permanent license.

Shared SSL VPN Licenses

A shared license lets you purchase a large number of SSL VPN sessions and share the sessions as needed among a group of adaptive security appliances by configuring one of the adaptive 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 adaptive security appliance should be the shared licensing server, and purchase the shared licensing server license using that device serial number.
2. Decide which adaptive 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 adaptive 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 adaptive 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 adaptive 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

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 adaptive 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.

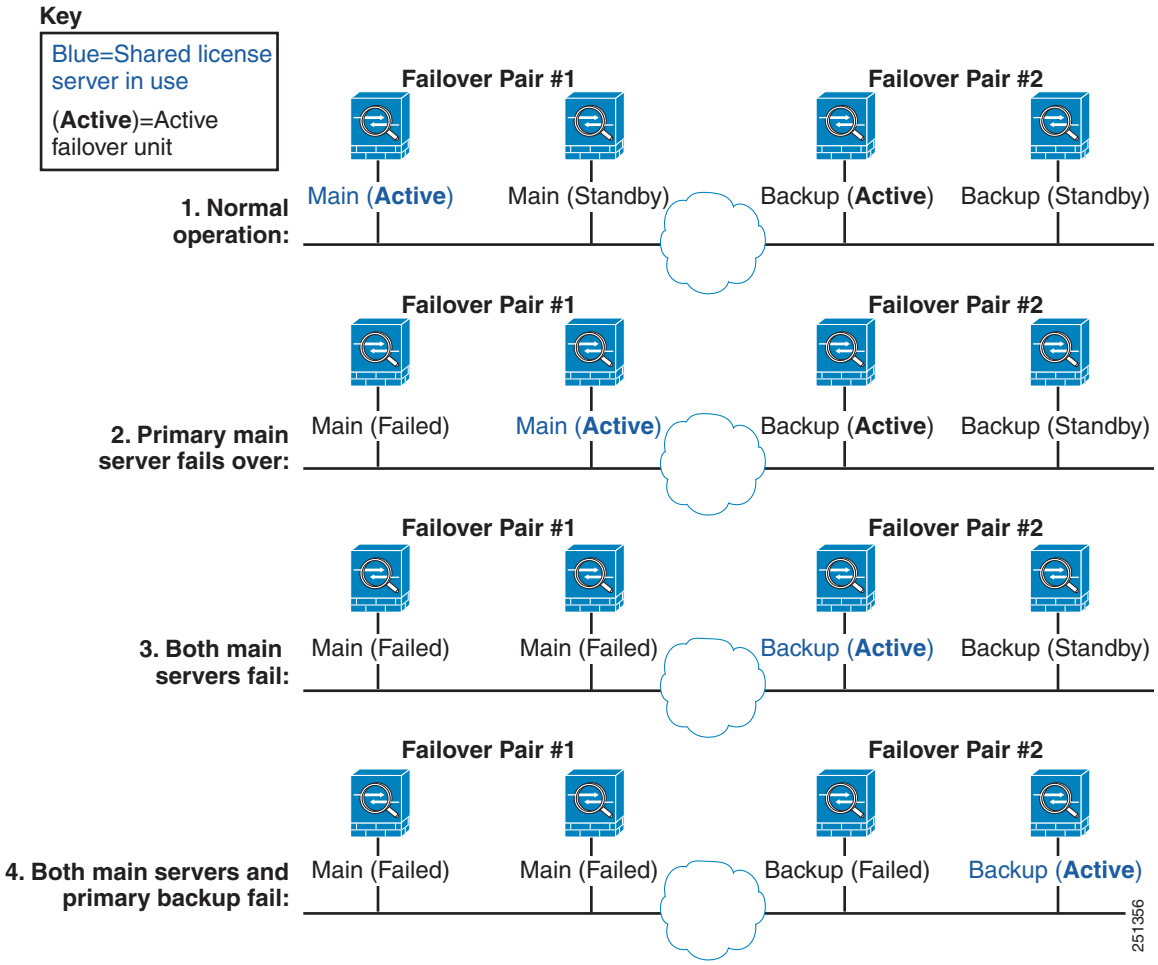
Note The backup server mechanism is separate from, but compatible with, failover.

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

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. 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 1-8).

Figure 1-8 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 17 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 adaptive 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.

Failover Licenses (8.3(1) and Later)

In Version 8.3(1) and later, failover units do not require the same license on each unit. For earlier versions, see the licensing document for your version.

This section includes the following topics:

Failover License Requirements

- Failover units do not require the same license on each unit.

  Older versions of adaptive security appliance software required that the licenses match on each unit. Starting with Version 8.3(1), you no longer need to install identical licenses. Typically, you buy a license only for the primary unit; for Active/Standby failover, the secondary unit inherits the primary license when it becomes active. If you have licenses on both units, they combine into a single running failover cluster license.

- For the ASA 5505 and 5510 adaptive security appliances, both units require the Security Plus license; the Base license does not support failover, so you cannot enable failover on a standby unit that only has the Base license.

How Failover Licenses Combine

For failover pairs, the licenses on each unit are combined into a single running failover cluster license. For Active/Active failover, the license usage of the two units combined cannot exceed the failover cluster license.

If you buy separate licenses for the primary and secondary unit, then the combined license uses the following rules:

- For licenses that have numerical tiers, such as the number of sessions, the values from both the primary and secondary licenses are combined up to the platform limit. If both licenses in use are time-based, then the licenses count down simultaneously.

  For example, you have two ASA 5520 adaptive security appliances with 500 SSL VPN sessions each; because the platform limit is 750, the combined license allows 750 SSL VPN sessions.

  Note In the above example, if the SSL VPN licenses are time-based, you might want to disable one of the licenses so you do not “waste” a 500 session license from which you can only use 250 sessions because of the platform limit.

  Or you have two ASA 5540 adaptive security appliances, one with 20 contexts and the other with 10 contexts; the combined license allows 30 contexts. For Active/Active failover, for example, one unit can use 18 contexts and the other unit can use 12 contexts, for a total of 30; the combined usage cannot exceed the failover cluster license.

- For licenses that have a status of enabled or disabled, then the license with the enabled status is used.

- For time-based licenses that are enabled or disabled (and do not have numerical tiers), the duration is the combined duration of both licenses. The primary unit counts down its license first, and when it expires, the secondary unit starts counting down its license. This rule also applies to Active/Active failover, even though both units are actively operating.

  For example, if you have 48 weeks left on the Botnet Traffic Filter license on both units, then the combined duration is 96 weeks.

To view the combined license, see the "Viewing Your Current License" section on page 24.

Loss of Communication Between Failover Units

If the failover units lose communication for more than 30 days, then each unit reverts to the license installed locally. During the 30-day grace period, the combined running license continues to be used by both units.

If you restore communication during the 30-day grace period, then for time-based licenses, the time elapsed is subtracted from the primary license; if the primary license becomes expired, only then does the secondary license start to count down.

If you do not restore communication during the 30-day period, then for time-based licenses, time is subtracted from both primary and secondary licenses, if installed. They are treated as two separate licenses and do not benefit from the failover combined license. The time elapsed includes the 30-day grace period.

For example:

1. You have a 52-week Botnet Traffic Filter license installed on both units. The combined running license allows a total duration of 104 weeks.
2. The units operate as a failover unit for 10 weeks, leaving 94 weeks on the combined license (42 weeks on the primary, and 52 weeks on the secondary).
3. If the units lose communication (for example the primary unit fails over to the secondary unit), the secondary unit continues to use the combined license, and continues to count down from 94 weeks.
4. The time-based license behavior depends on when communication is restored:

- Within 30 days—The time elapsed is subtracted from the primary unit license. In this case, communication is restored after 4 weeks. Therefore, 4 weeks are subtracted from the primary license leaving 90 weeks combined (38 weeks on the primary, and 52 weeks on the secondary).
- After 30 days—The time elapsed is subtracted from both units. In this case, communication is restored after 6 weeks. Therefore, 6 weeks are subtracted from both the primary and secondary licenses, leaving 84 weeks combined (36 weeks on the primary, and 46 weeks on the secondary).

Upgrading Failover Pairs

Because failover pairs do not require the same license on both units, you can apply new licenses to each unit without any downtime. If you apply a permanent license that requires a reload (see Table 1-14 on page 31), then you can fail over to the other unit while you reload. If both units require reloading, then you can reload them separately so you have no downtime.

Licenses FAQ

Q. Can I activate multiple time-based licenses, for example, SSL VPN and Botnet Traffic Filter?

A. Yes. You can use one time-based license per feature at a time.

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

A. Yes. For identical licenses, the time limit is combined when you install multiple time-based licenses. For non-identical licenses (for example, a 1000-session SSL VPN license and a 2500-session license), the adaptive security appliance automatically activates the next time-based license it finds for the feature.

Q. Can I install a new permanent license while maintaining an active time-based license?

A. Yes. Activating a permanent license does not affect time-based licenses.

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 has the same running license as the primary unit; in the case of the shared licensing server, they require a server license. The backup server requires a participant license. The backup server 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?

A. No. Starting with Version 8.3(1), you do not have to have matching licenses on both units. Typically, you buy a license only for the primary unit; the secondary unit inherits the primary license when it becomes active. In the case where you also have a separate license on the secondary unit (for example, if you purchased matching licenses for pre-8.3 software), the licenses are combined into a running failover cluster license, up to the model limits.

Q. Can I use a time-based 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 (time-based or permanent) are used up. **Note**: On the shared licensing server, the permanent SSL VPN license is not used; you can however use a time-based license at the same time as the shared licensing server license. In this case, the time-based 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

- Shared licenses are not supported in Active/Active mode. See the "Failover and Shared Licenses" section on page 18 for more information.
- Failover units do not require the same license on each unit.

Older versions of adaptive security appliance software required that the licenses match on each unit. Starting with Version 8.3(1), you no longer need to install identical licenses. Typically, you buy a license only for the primary unit; for Active/Standby failover, the secondary unit inherits the primary license when it becomes active. If you have licenses on both units, they combine into a single running failover cluster license.

Note Failover units do require the same RAM on both units.

- For the ASA 5505 and 5510 adaptive security appliances, both units require the Security Plus license; the Base license does not support failover, so you cannot enable failover on a standby unit that only has the Base license.

Upgrade and Downgrade Guidelines

Your activation key remains compatible if you upgrade to the latest version from any previous version. However, you might have issues if you want to maintain downgrade capability:

- Downgrading to Version 8.1 or earlier—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 adaptive 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.
- Downgrading to Version 8.2 or earlier—Version 8.3 introduced more robust time-based key usage as well as failover license changes:
  - If you have more than one time-based activation key active, when you downgrade, only the most recently activated time-based key can be active. Any other keys are made inactive. If the last time-based license is for a feature introduced in 8.3, then that license still remains the active license even though it cannot be used in earlier versions. Reenter the permanent key or a valid time-based key.
  - If you have mismatched licenses on a failover pair, then downgrading will disable failover. Even if the keys are matching, the license used will no longer be a combined license.
  - If you have one time-based license installed, but it is for a feature introduced in 8.3, then after you downgrade, that time-based license remains active. You need to reenter the permanent key to disable the time-based license.

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.

- 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 or in ASDM, using the Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Essentials pane.

Viewing Your Current License

This section describes how to view your current license, and for time-based 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`	This command shows the permanent license, active time-based licenses, and the running license, which is a combination of the permanent license and active time-based licenses. The **detail** keyword also shows inactive time-based licenses. For failover units, this command also shows the "Failover cluster" license, which is the combined keys of the primary and secondary units.

For ASDM:

Step 1 To view the running license, which is a combination of the permanent license and any active time-based licenses, choose the **Configuration > Device Management > Licensing > Activation Key** pane and view the Running Licenses area.

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

For a failover pair, the running license shown is the combined license from the primary and secondary units. See the "How Failover Licenses Combine" section on page 20 for more information. For time-based licenses with numerical values (the duration is not combined), the License Duration column displays the shortest time-based license from either the primary or secondary unit; when that license expires, the license duration from the other unit displays.

Step 2 (Optional) To view time-based license details, such as the features included in the license and the duration, in the Time-Based License Keys Installed area, choose a license key, and then click **Show License Details**.

Step 3 (Optional) For a failover unit, to view the license installed on this unit (and not the combined license from both primary and secondary units), in the Running Licenses area, click **Show information of license specifically purchased for this device alone**.

Examples

Example 1-1 Standalone Unit Output for show activation-key

The following is sample output from the **show activation-key** command for a standalone unit that shows the running license (the combined permanent license and time-based licenses), as well as each active time-based license:

```
hostname# show activation-key

Serial Number:  JMX1232L11M
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Running Timebased Activation Key: 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2

Licensed features for this platform:
Maximum Physical Interfaces  : Unlimited  perpetual
Maximum VLANs                : 50         perpetual
Inside Hosts                 : Unlimited  perpetual
Failover                     : Disabled   perpetual
VPN-DES                      : Enabled    perpetual
VPN-3DES-AES                 : Enabled    perpetual
Security Contexts            : 0          perpetual
GTP/GPRS                     : Disabled   perpetual
SSL VPN Peers                : 2          perpetual
Total VPN Peers              : 250        perpetual
Shared License               : Disabled   perpetual
AnyConnect for Mobile        : Disabled   perpetual
AnyConnect for Linksys phone : Disabled   perpetual
AnyConnect Essentials        : Enabled    perpetual
Advanced Endpoint Assessment : Disabled   perpetual
UC Phone Proxy Sessions      : 12         62 days
Total UC Proxy Sessions      : 12         62 days
Botnet Traffic Filter        : Enabled    646 days

This platform has a Base license.

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

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter        : Enabled    646 days

0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2
Total UC Proxy Sessions      : 10         62 days
```

Example 1-2 Standalone Unit Output for show activation-key detail

The following is sample output from the **show activation-key detail** command for a standalone unit that shows the running license (the combined permanent license and time-based licenses), as well as the permanent license and each installed time-based license (active and inactive):

```
hostname# show activation-key detail

Serial Number:  88810093382
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285

Licensed features for this platform:
Maximum Physical Interfaces    : 8              perpetual
VLANs                          : 20             DMZ Unrestricted
```

```
Dual ISPs                       : Enabled        perpetual
VLAN Trunk Ports                : 8              perpetual
Inside Hosts                    : Unlimited      perpetual
Failover                        : Active/Standby perpetual
VPN-DES                         : Enabled        perpetual
VPN-3DES-AES                    : Enabled        perpetual
SSL VPN Peers                   : 2              perpetual
Total VPN Peers                 : 25             perpetual
Shared License                  : Disabled       perpetual
AnyConnect for Mobile           : Disabled       perpetual
AnyConnect for Cisco VPN Phone  : Disabled       perpetual
AnyConnect Essentials           : Disabled       perpetual
Advanced Endpoint Assessment    : Disabled       perpetual
UC Phone Proxy Sessions         : 2              perpetual
Total UC Proxy Sessions         : 2              perpetual
Botnet Traffic Filter           : Enabled        39 days
Intercompany Media Engine       : Disabled       perpetual

This platform has an ASA 5505 Security Plus license.

Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c

Licensed features for this platform:
Maximum Physical Interfaces     : 8              perpetual
VLANs                           : 20             DMZ Unrestricted
Dual ISPs                       : Enabled        perpetual
VLAN Trunk Ports                : 8              perpetual
Inside Hosts                    : Unlimited      perpetual
Failover                        : Active/Standby perpetual
VPN-DES                         : Enabled        perpetual
VPN-3DES-AES                    : Enabled        perpetual
SSL VPN Peers                   : 2              perpetual
Total VPN Peers                 : 25             perpetual
Shared License                  : Disabled       perpetual
AnyConnect for Mobile           : Disabled       perpetual
AnyConnect for Cisco VPN Phone  : Disabled       perpetual
AnyConnect Essentials           : Disabled       perpetual
Advanced Endpoint Assessment    : Disabled       perpetual
UC Phone Proxy Sessions         : 2              perpetual
Total UC Proxy Sessions         : 2              perpetual
Botnet Traffic Filter           : Disabled       perpetual
Intercompany Media Engine       : Disabled       perpetual

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

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter           : Enabled    39 days

Inactive Timebased Activation Key:
0xyadayada3 0xyadayada3 0xyadayada3 0xyadayada3 0xyadayada3
SSL VPN Peers                   : 100        7 days
```

Example 1-3 Primary Unit Output in a Failover Pair for show activation-key detail

The following is sample output from the **show activation-key detail** command for the primary failover unit that shows:

- The primary unit license (the combined permanent license and time-based licenses).

- The “Failover Cluster” license, which is the combined licenses from the primary and secondary units. This is the license that is actually running on the adaptive security appliance. The values in this license that reflect the combination of the primary and secondary licenses are in bold.
- The primary unit permanent license.
- The primary unit installed time-based licenses (active and inactive).

```
hostname# show activation-key detail

Serial Number:  P3000000171
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 12             perpetual
GTP/GPRS                       : Enabled        perpetual
SSL VPN Peers                  : 2              perpetual
Total VPN Peers                : 750            perpetual
Shared License                 : Disabled       perpetual
AnyConnect for Mobile          : Disabled       perpetual
AnyConnect for Cisco VPN Phone : Disabled       perpetual
AnyConnect Essentials          : Disabled       perpetual
Advanced Endpoint Assessment   : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 12             perpetual
GTP/GPRS                       : Enabled        perpetual
SSL VPN Peers                  : 4              perpetual
Total VPN Peers                : 750            perpetual
Shared License                 : Disabled       perpetual
AnyConnect for Mobile          : Disabled       perpetual
AnyConnect for Cisco VPN Phone : Disabled       perpetual
AnyConnect Essentials          : Disabled       perpetual Advanced Endpoint Assessment   :
Disabled       perpetual
UC Phone Proxy Sessions        : 4              perpetual
Total UC Proxy Sessions        : 4              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
```

```
Maximum VLANs                   : 150            perpetual
Inside Hosts                    : Unlimited      perpetual
Failover                        : Active/Active  perpetual
VPN-DES                         : Enabled        perpetual
VPN-3DES-AES                    : Disabled       perpetual
Security Contexts               : 2              perpetual
GTP/GPRS                        : Disabled       perpetual
SSL VPN Peers                   : 2              perpetual
Total VPN Peers                 : 750            perpetual
Shared License                  : Disabled       perpetual
AnyConnect for Mobile           : Disabled       perpetual
AnyConnect for Cisco VPN Phone : Disabled       perpetual
AnyConnect Essentials           : Disabled       perpetual
Advanced Endpoint Assessment    : Disabled       perpetual
UC Phone Proxy Sessions         : 2              perpetual
Total UC Proxy Sessions         : 2              perpetual
Botnet Traffic Filter           : Disabled       perpetual
Intercompany Media Engine       : Disabled       perpetual

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

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter           : Enabled    33 days

Inactive Timebased Activation Key:
0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3
Security Contexts               : 2          7 days
SSL VPN Peers                   : 100        7 days

0xyadayad4 0xyadayad4 0xyadayad4 0xyadayad4 0xyadayad4
Total UC Proxy Sessions         : 100        14 days
```

Example 1-4 Secondary Unit Output in a Failover Pair for show activation-key detail

The following is sample output from the **show activation-key detail** command for the secondary failover unit that shows:

- The secondary unit license (the combined permanent license and time-based licenses).
- The “Failover Cluster” license, which is the combined licenses from the primary and secondary units. This is the license that is actually running on the adaptive security appliance. The values in this license that reflect the combination of the primary and secondary licenses are in bold.
- The secondary unit permanent license.
- The secondary installed time-based licenses (active and inactive). This unit does not have any time-based licenses, so none display in this sample output.

```
hostname# show activation-key detail

Serial Number:  P3000000011
Running Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1

Licensed features for this platform:
Maximum Physical Interfaces     : Unlimited      perpetual
Maximum VLANs                   : 150            perpetual
Inside Hosts                    : Unlimited      perpetual
Failover                        : Active/Active  perpetual
VPN-DES                         : Enabled        perpetual
VPN-3DES-AES                    : Disabled       perpetual
Security Contexts               : 2              perpetual
GTP/GPRS                        : Disabled       perpetual
```

```
SSL VPN Peers                   : 2             perpetual
Total VPN Peers                 : 750           perpetual
Shared License                  : Disabled      perpetual
AnyConnect for Mobile           : Disabled      perpetual
AnyConnect for Cisco VPN Phone  : Disabled      perpetual
AnyConnect Essentials           : Disabled      perpetual
Advanced Endpoint Assessment    : Disabled      perpetual
UC Phone Proxy Sessions         : 2             perpetual
Total UC Proxy Sessions         : 2             perpetual
Botnet Traffic Filter           : Disabled      perpetual
Intercompany Media Engine       : Disabled      perpetual

This platform has an ASA 5520 VPN Plus license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces     : Unlimited     perpetual
Maximum VLANs                   : 150           perpetual
Inside Hosts                    : Unlimited     perpetual
Failover                        : Active/Active perpetual
VPN-DES                         : Enabled       perpetual
VPN-3DES-AES                    : Enabled       perpetual
Security Contexts               : 10            perpetual
GTP/GPRS                        : Enabled       perpetual
SSL VPN Peers                   : 4             perpetual
Total VPN Peers                 : 750           perpetual
Shared License                  : Disabled      perpetual
AnyConnect for Mobile           : Disabled      perpetual
AnyConnect for Cisco VPN Phone  : Disabled      perpetual
AnyConnect Essentials           : Disabled      perpetual
Advanced Endpoint Assessment    : Disabled      perpetual
UC Phone Proxy Sessions         : 4             perpetual
Total UC Proxy Sessions         : 4             perpetual
Botnet Traffic Filter           : Enabled       33 days
Intercompany Media Engine       : Disabled      perpetual

This platform has an ASA 5520 VPN Plus license.

Running Permanent Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1

Licensed features for this platform:
Maximum Physical Interfaces     : Unlimited     perpetual
Maximum VLANs                   : 150           perpetual
Inside Hosts                    : Unlimited     perpetual
Failover                        : Active/Active perpetual
VPN-DES                         : Enabled       perpetual
VPN-3DES-AES                    : Disabled      perpetual
Security Contexts               : 2             perpetual
GTP/GPRS                        : Disabled      perpetual
SSL VPN Peers                   : 2             perpetual
Total VPN Peers                 : 750           perpetual
Shared License                  : Disabled      perpetual
AnyConnect for Mobile           : Disabled      perpetual
AnyConnect for Cisco VPN Phone  : Disabled      perpetual
AnyConnect Essentials           : Disabled      perpetual
Advanced Endpoint Assessment    : Disabled      perpetual
UC Phone Proxy Sessions         : 2             perpetual
Total UC Proxy Sessions         : 2             perpetual
Botnet Traffic Filter           : Disabled      perpetual
Intercompany Media Engine       : Disabled      perpetual

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

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.

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

Detailed Steps

Step 1 Obtain the serial number for your adaptive 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 adaptive 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 time-based 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.

Activating or Deactivating Keys

This section describes how to enter a new activation key, and how to activate and deactivate time-based keys.

Prerequisites

- If you are already in multiple context mode, enter the activation key in the system execution space.
- Some permanent licenses require you to reload the adaptive security appliance after you activate them. Table 1-14 lists the licenses that require reloading.

Table 1-14 Permanent 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 permanent license (for example, going from 10 contexts to 2 contexts).

Limitations and Restrictions

Your activation key remains compatible if you upgrade to the latest version from any previous version. However, you might have issues if you want to maintain downgrade capability:

- Downgrading to Version 8.1 or earlier—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 adaptive 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.
- Downgrading to Version 8.2 or earlier—Version 8.3 introduced more robust time-based key usage as well as failover license changes:
  - If you have more than one time-based activation key active, when you downgrade, only the most recently activated time-based key can be active. Any other keys are made inactive.
  - If you have mismatched licenses on a failover pair, then downgrading will disable failover. Even if the keys are matching, the license used will no longer be a combined license.

Detailed Steps

For the CLI:

	Command	Purpose
Step 1	**activation-key** *key* [**activate** | **deactivate**] **Example:** `hostname# activation-key 0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490`	Applies an activation key to the adaptive 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 install one permanent key, and multiple time-based keys. If you enter a new permanent key, it overwrites the already installed one. The **activate** and **deactivate** keywords are available for time-based keys only. If you do not enter any value, **activate** is the default. The last time-based key that you activate for a given feature is the active one. To deactivate any active time-based key, enter the **deactivate** keyword. If you enter a key for the first time, and specify **deactivate**, then the key is installed on the adaptive security appliance in an inactive state. See the "Time-Based Licenses" section on page 13 for more information.
Step 2	(Might be required.) **reload** **Example:** `hostname# reload`	Reloads the adaptive security appliance. Some permanent licenses require you to reload the adaptive security appliance after entering the new activation key. See Table 1-14 on page 31 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 the **Configuration > Device Management > Licensing > Activation Key** pane.

Step 2 To enter a new activation key, either permanent or time-based, 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 install one permanent key, and multiple time-based keys. If you enter a new permanent key, it overwrites the already installed one. If you enter a new time-based key, then it is active by default and displays in the Time-based License Keys Installed table. The last time-based key that you activate for a given feature is the active one.

Step 3 To activate or deactivate an installed time-based key, choose the key in the Time-based License Keys Installed table, and click either **Activate** or **Deactivate**.

You can only have one time-based key active for each feature. See the "Time-Based Licenses" section on page 13 for more information.

Step 4 Click **Update Activation Key**.

Some permanent licenses require you to reload the adaptive security appliance after entering the new activation key. See Table 1-14 on page 31 for a list of licenses that need reloading. You will be prompted to reload if it is required.

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 SSL VPN Licenses" section on page 15.

This section includes the following topics:

Configuring the Shared Licensing Server

This section describes how to configure the adaptive 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.

	Command	Purpose
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 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.

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 35 (CLI only), or the "Configuring the Shared Licensing Participant and, for ASDM, the Optional Backup Server" section on page 36.

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 36.

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 35.

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 adaptive 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 1-15 lists the release history for this feature.

Table 1-15 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.
Increased VLANs	7.2(2)	The maximum number of VLANs for the Security Plus license on the ASA 5505 adaptive 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 adaptive 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).

Table 1-15 Feature History for Licensing (continued)

Feature Name	Releases	Feature Information
Gigabit Ethernet Support for the ASA 5510 Security Plus License	7.2(3)	The ASA 5510 adaptive 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 adaptive 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.
AnyConnect for Mobile License	8.0(3)	The AnyConnect for Mobile license was introduced. It lets Windows mobile devices connect to the adaptive security appliance using the AnyConnect client.
Time-based Licenses	8.0(4)/8.1(2)	Support for time-based licenses was introduced.
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. Phone Proxy, Presence Federation Proxy, and Encrypted Voice Inspection applications use TLS proxy sessions for their connections. Each TLS proxy session is counted against the UC license limit. All of these applications are licensed under the UC Proxy umbrella, and can be mixed and matched. This feature is not available in Version 8.1.

Table 1-15 Feature History for Licensing (continued)

Feature Name	Releases	Feature Information
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)	The AnyConnect Essentials License was introduced. 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 Edition 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 Edition 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 Edition license (all types) or the Advanced Endpoint Assessment license. You can, however, run AnyConnect Essentials and AnyConnect Premium SSL VPN Edition licenses on different adaptive security appliances in the same network. By default, the adaptive security appliance uses the AnyConnect Essentials license, but you can disable it to use other licenses by using the **no anyconnect-essentials** command or in ASDM, the Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Essentials pane.
Shared Licenses for SSL VPN	8.2(1)	Shared licenses for SSL VPN were introduced. Multiple adaptive 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.
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. **Note** The ASA 5585-X is not supported in 8.3(x).

Table 1-15 Feature History for Licensing (continued)

Feature Name	Releases	Feature Information
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. **Note** The ASA 5585-X is not supported in 8.3(x).
Non-identical failover licenses	8.3(1)	Failover licenses no longer need to be identical on each unit. The license used for both units is the combined license from the primary and secondary units. The following commands were modified: **show activation-key** and **show version**. The following ASDM screen was modified: Configuration > Device Management > Licensing > Activation Key.
Stackable time-based licenses	8.3(1)	Time-based licenses are now stackable. In many cases, you might need to renew your time-based license and have a seamless transition from the old license to the new one. For features that are only available with a time-based license, it is especially important that the license not expire before you can apply the new license. The adaptive security appliance allows you to *stack* time-based licenses so you do not have to worry about the license expiring or about losing time on your licenses because you installed the new one early.
Intercompany Media Engine License	8.3(1)	The IME license was introduced.
Multiple time-based licenses active at the same time	8.3(1)	You can now install multiple time-based licenses, and have one license per feature active at a time. The following commands were modified: **show activation-key** and **show version**. The following ASDM screen was modified: Configuration > Device Management > Licensing > Activation Key.
Discrete activation and deactivation of time-based licenses.	8.3(1)	You can now activate or deactivate time-based licenses using a command. The following commands was modified: **activation-key** [**activate** | **deactivate**]. The following ASDM screen was modified: Configuration > Device Management > Licensing > Activation Key.