Managing Feature Licenses for Cisco ASA Services Module Version 8.5

Released: July 7, 2011

A license specifies the options that are enabled on a given ASASM. 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 8.5; 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

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

Licenses

Items that are in italics are separate, optional licenses with which that you can replace the Base license. You can mix and match licenses.

Table 1-6 shows the licenses for the ASASM. All ASASM licenses for this release are No Payload Encryption licenses. See the "No Payload Encryption Models" section on page 7 for more information.

Table 1-6   ASASM License Features

Licenses	Description (Base License in Plain Text)					
Firewall Licenses						
Botnet Traffic Filter[1]	Disabled	*Optional Time-based license: Available*				
Firewall Conns, Concurrent	8,000,000					
GTP/GPRS	Disabled	*Optional license: Available*				
Intercompany Media Engine	No support.					
Unified Communications Proxy Sessions	No support.					
VPN Licenses						
Adv. Endpoint Assessment	No support.					
AnyConnect Essentials	No support.					
AnyConnect Mobile	No support.					
AnyConnect Premium (sessions)	No support.					
Combined VPN sessions of all types, Maximum	No support.					
Other VPN (sessions)	No support.					
VPN Load Balancing	No support.					
General Licenses						
Encryption	Base (DES)	*Optional license: Strong (3DES/AES)*				
Failover	Active/Standby or Active/Active					
Interfaces of all types, Max.[1]	4128					
Security Contexts	2	*Optional licenses:*				
		5	10	20	50	100	250
VLANs, Maximum	1000					

1. See the "License Notes" section on page 3.

License Notes

Table 1-7 includes common footnotes shared by multiple tables in the "Licenses" section on page 2.

Table 1-7   *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.
Botnet Traffic Filter	Requires a Strong Encryption (3DES/AES) License to download the dynamic database.
Encryption	The DES license cannot be disabled. If you have the 3DES license installed, DES is still available. To prevent the use of DES when you want to only use strong encryption, be sure to configure any relevant commands to use only string encryption.
Interfaces of all types, Max.	The maximum number of combined interfaces; for example, VLANs, physical, redundant, bridge group, and EtherChannel interfaces.

Information About Feature Licenses

A license specifies the options that are enabled on a given ASASM. 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, page 3
- Permanent License, page 3
- Time-Based Licenses, page 4
- Failover Licenses, page 6
- No Payload Encryption Models, page 7
- Licenses FAQ, page 8

Preinstalled License

By default, your ASASM 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 "Monitoring Licenses" section on page 12 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 ASASM combines the permanent and time-based licenses into a running license. See the "How Permanent and Time-Based Licenses Combine" section on page 4 for more information about how the ASASM 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 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.

- 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.

How the Time-Based License Timer Works

- The timer for the time-based license starts counting down when you activate it on the ASASM.

- 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 ASASM, then the timer continues to count down. If you intend to leave the ASASM 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 ASASM 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 1-8 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 1-8   Time-Based License Combination Rules

Time-Based Feature	Combined License Rule
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 "Monitoring Licenses" section on page 12.

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 ASASM 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).

If the licenses are not identical, 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 10 for more information about activating licenses.

Although non-identical licenses do not combine, when the current license expires, the ASASM automatically activates an installed license of the same feature if available. See the "Time-Based License Expiration" section on page 5 for more information.

Time-Based License Expiration

When the current license for a feature expires, the ASASM 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 ASASM 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 ASASM activated, then you must manually activate the license you prefer. See the "Activating or Deactivating Keys" section on page 10.

Failover Licenses

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

This section includes the following topics:

Failover License Requirements

Failover units do not require the same license on each unit. The exception is both units must have the same encryption license.

Note   A valid permanent key is required; in rare instances, your authentication key can be removed. If your key consists of all 0's, then you need to reinstall a valid authentication key before failover can be enabled.

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 ASASMs, one with 20 contexts and the other with 10 contexts; the combined license allows 30 contexts. For Active/Active failover, one unit can use 18 contexts and the other unit can use 12 contexts, for example, for a total of 30; the combined usage cannot exceed the failover cluster license (in this case, 30).

- 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 "Monitoring Licenses" section on page 12.

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 1-9 on page 10), 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.

No Payload Encryption Models

The ASASM is only available as a No Payload Encryption model for this release. The ASASM software senses a No Payload Encryption model, and disables the following features:

- Unified Communications
- VPN

You can still install the Strong Encryption (3DES/AES) license for use with management connections. For example, you can use ASDM HTTPS/SSL, SSHv2, Telnet and SNMPv3. You can also download the dynamic database for the Botnet Traffic Filer (which uses SSL).

When you view the license (see the), VPN and Unified Communications licenses will not be listed.

Licenses FAQ

Q. Can I activate multiple time-based licenses?

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, the ASASM 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. Do I need to buy the same licenses for the secondary unit in a failover pair?

A. No, 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, the licenses are combined into a running failover cluster license, up to the model limits.

Guidelines and Limitations

See the following guidelines for activation keys.

Context Mode Guidelines

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

Firewall Mode Guidelines

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

Failover Guidelines

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

  Older versions of ASASM 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.

Additional Guidelines and Limitations

- The activation key is not stored in your configuration file; it is stored as a hidden file in flash memory.

- The activation key is tied to the serial number of the device. Feature licenses cannot be transferred between devices (except in the case of a hardware failure). If you have to replace your device due to a hardware failure and it is covered by Cisco TAC, contact the Cisco Licensing Team to have your existing license transferred to the new serial number. The Cisco Licensing Team will ask for the Product Authorization Key reference number and existing serial number.

- Once purchased, you cannot return a license for a refund or for an upgraded license.

Configuring Licenses

This section includes the following topics:

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.

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 ASASM 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 ASASM

- 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 ASASM after you activate them. Table 1-9 lists the licenses that require reloading.

Table 1-9   Permanent License Reloading Requirements

Model	License Action Requiring Reload
All models	Changing the Encryption license.
All models	Downgrading any permanent license (for example, going from 10 contexts to 2 contexts).

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 ASASM. 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 ASASM in an inactive state. See the "Time-Based Licenses" section on page 4 for more information.

Step 2	(Might be required.)
	
	`reload`
	
	Example:
	`hostname# reload`
		Reloads the ASASM. Some permanent licenses require you to reload the ASASM after entering the new activation key. See Table 1-9 on page 10 for a list of licenses that need reloading. If you need to reload, you will see the following message:
		
		`WARNING: The running activation key was not updated with`
		`the requested key. The flash activation key was updated`
		`with the requested key, and will become active after the`
		`next reload.`

For ASDM:

Step 1   Choose **Configuration > Device Management**, and then choose the **Licensing > Activation Key** or **Licensing Activation Key** pane, depending on your model.

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 4 for more information.

Step 4   Click **Update Activation Key**.

Some permanent licenses require you to reload the ASASM after entering the new activation key. See Table 1-9 on page 10 for a list of licenses that need reloading. You will be prompted to reload if it is required.

Monitoring Licenses

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 6 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   Primary Unit Output for the ASA Services Module in a Failover Pair for show
activation-key***

The following is sample output from the **show activation-key** 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 ASASM. The values in this license that
  reflect the combination of the primary and secondary licenses are in bold.

- The primary unit installed time-based licenses (active and inactive).

```
hostname# show activation-key

erial Number:  SAL144705BF
Running Permanent Activation Key: 0x4d1ed752 0xc8cfeb37 0xf4c38198 0x93c04c28 0x4a1c049a
Running Timebased Activation Key: 0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880

Licensed features for this platform:
Maximum Interfaces             : 1024          perpetual
Inside Hosts                   : Unlimited     perpetual
Failover                       : Active/Active perpetual
DES                            : Enabled       perpetual
3DES-AES                       : Enabled       perpetual
Security Contexts              : 25            perpetual
GTP/GPRS                       : Enabled       perpetual
Botnet Traffic Filter          : Enabled       330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.


Failover cluster licensed features for this platform:
Maximum Interfaces             : 1024          perpetual
Inside Hosts                   : Unlimited     perpetual
Failover                       : Active/Active perpetual
DES                            : Enabled       perpetual
3DES-AES                       : Enabled       perpetual
Security Contexts              : 50            perpetual
GTP/GPRS                       : Enabled       perpetual
Botnet Traffic Filter          : Enabled       330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.

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

Active Timebased Activation Key:
0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880
Botnet Traffic Filter          : Enabled    330 days
```

***Example 1-2   Secondary Unit Output for the ASA Services Module in a Failover Pair for show
activation-key***

The following is sample output from the **show activation-key** 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 ASASM. The values in this license that reflect the combination of the primary and secondary licenses are in bold.

- 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:  SAD143502E3
Running Permanent Activation Key: 0xf404c46a 0xb8e5bd84 0x28c1b900 0x92eca09c 0x4e2a0683

Licensed features for this platform:
Maximum Interfaces              : 1024          perpetual
Inside Hosts                    : Unlimited     perpetual
Failover                        : Active/Active perpetual
DES                             : Enabled       perpetual
3DES-AES                        : Enabled       perpetual
Security Contexts               : 25            perpetual
GTP/GPRS                        : Disabled      perpetual
Botnet Traffic Filter           : Disabled      perpetual


This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.


Failover cluster licensed features for this platform:
Maximum Interfaces              : 1024          perpetual
Inside Hosts                    : Unlimited     perpetual
Failover                        : Active/Active perpetual
DES                             : Enabled       perpetual
3DES-AES                        : Enabled       perpetual
Security Contexts               : 50            perpetual
GTP/GPRS                        : Enabled       perpetual
Botnet Traffic Filter           : Enabled       330 days


This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.

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

Feature History for Licensing

Table 1-10 lists each feature change and the platform release in which it was implemented. ASDM is backwards-compatible with multiple platform releases, so the specific ASDM release in which support was added is not listed.

Table 1-10   *Feature History for Licensing*

Feature Name	Platform 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 was increased from 5 (3 fully functional; 1 failover; one restricted to a backup interface) to 20 fully functional interfaces. In addition, the number of trunk ports was increased from 1 to 8. Now there are 20 fully functional interfaces, you do not need to use the backup interface command to cripple a backup ISP interface; you can use a fully-functional interface for it. The backup interface command is still useful for an Easy VPN configuration. VLAN limits were also increased for the ASA 5510 (from 10 to 50 for the Base license, and from 25 to 100 for the Security Plus license), the ASA 5520 (from 100 to 150), the ASA 5550 (from 200 to 250).

Table 1-10   *Feature History for Licensing (continued)*

Feature Name	Platform Releases	Feature Information
Gigabit Ethernet Support for the ASA 5510 Security Plus License	7.2(3)	The ASA 5510 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 ASASM. The ASASM 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 ASASM 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 1-10 *Feature History for Licensing (continued)*

Feature Name	Platform 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 ASASM. This license does not support browser-based SSL VPN access or Cisco Secure Desktop. For these features, activate an AnyConnect Premium 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 license.
		The AnyConnect Essentials license cannot be active at the same time as the following licenses on a given ASASM: AnyConnect Premium license (all types) or the Advanced Endpoint Assessment license. You can, however, run AnyConnect Essentials and AnyConnect Premium licenses on different ASASMs in the same network.
		By default, the ASASM 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.
SSL VPN license changed to AnyConnect Premium SSL VPN Edition license	8.2(1)	The SSL VPN license name was changed to the AnyConnect Premium SSL VPN Edition license.
Shared Licenses for SSL VPN	8.2(1)	Shared licenses for SSL VPN were introduced. Multiple ASASMs 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 1-10 *Feature History for Licensing (continued)*

Feature Name	Platform 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. We modified the following commands: **show activation-key** and **show version**. We modified the following ASDM screen: 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 ASASM 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 command was modified: **activation-key** [**activate**	**deactivate**]. The following ASDM screen was modified: Configuration > Device Management > Licensing > Activation Key.
AnyConnect Premium SSL VPN Edition license changed to AnyConnect Premium SSL VPN license	8.3(1)	The AnyConnect Premium SSL VPN Edition license name was changed to the AnyConnect Premium SSL VPN license.

Table 1-10 **Feature History for Licensing (continued)**

Feature Name	Platform Releases	Feature Information
No Payload Encryption image for export	8.3(2)	If you install the No Payload Encryption software on the ASA 5505 through 5550, then you disable Unified Communications, strong encryption VPN, and strong encryption management protocols.
		Note This special image is only supported in 8.3(x); for No Payload Encryption support in 8.4(1) and later, you need to purchase a special hardware version of the ASASM.
Increased contexts for the ASA 5550, 5580, and 5585-X	8.4(1)	For the ASA 5550 and ASA 5585-X with SSP-10, the maximum contexts was increased from 50 to 100. For the ASA 5580 and 5585-X with SSP-20 and higher, the maximum was increased from 50 to 250.
Increased VLANs for the ASA 5580 and 5585-X	8.4(1)	For the ASA 5580 and 5585-X, the maximum VLANs was increased from 250 to 1024.
Increased connections for the ASA 5580 and 5585-X	8.4(1)	We increased the firewall connection limits: • ASA 5580-20—1,000,000 to 2,000,000. • ASA 5580-40—2,000,000 to 4,000,000. • ASA 5585-X with SSP-10: 750,000 to 1,000,000. • ASA 5585-X with SSP-20: 1,000,000 to 2,000,000. • ASA 5585-X with SSP-40: 2,000,000 to 4,000,000. • ASA 5585-X with SSP-60: 2,000,000 to 10,000,000.
AnyConnect Premium SSL VPN license changed to AnyConnect Premium license	8.4(1)	The AnyConnect Premium SSL VPN license name was changed to the AnyConnect Premium license. The license information display was changed from "SSL VPN Peers" to "AnyConnect Premium Peers."
Increased AnyConnect VPN sessions for the ASA 5580	8.4(1)	The AnyConnect VPN session limit was increased from 5,000 to 10,000.
Increased Other VPN sessions for the ASA 5580	8.4(1)	The other VPN session limit was increased from 5,000 to 10,000.
IPsec remote access VPN using IKEv2	8.4(1)	IPsec remote access VPN using IKEv2 was added to the AnyConnect Essentials and AnyConnect Premium licenses. IKEv2 site-to-site sessions were added to the Other VPN license (formerly IPsec VPN). The Other VPN license is included in the Base license.

Table 1-10　　***Feature History for Licensing (continued)***

Feature Name	Platform Releases	Feature Information
No Payload Encryption hardware for export	8.4(1)	For models available with No Payload Encryption (for example, the ASA 5585-X), the ASASM software disables Unified Communications and VPN features, making the ASASM available for export to certain countries.
Dual SSPs for SSP-20 and SSP-40	8.4(2)	For SSP-40 and SSP-60, you can use two SSPs of the same level in the same chassis. Mixed-level SSPs are not supported (for example, an SSP-40 with an SSP-60 is not supported). Each SSP acts as an independent device, with separate configurations and management. You can use the two SSPs as a failover pair if desired. When using two SSPs in the chassis, VPN is not supported; note, however, that VPN has not been disabled.