



Licenses: Product Authorization Key Licensing

A license specifies the options that are enabled on a given Cisco ASA. This document describes product authorization key (PAK) licenses for all physical ASAs. For the ASAv, see [Licenses: Smart Software Licensing \(ASAv, ASA on Firepower\)](#).

- [About PAK Licenses, on page 1](#)
- [Guidelines for PAK Licenses, on page 12](#)
- [Configure PAK Licenses, on page 14](#)
- [Configure a Shared License \(AnyConnect 3 and Earlier\), on page 18](#)
- [Supported Feature Licenses Per Model, on page 24](#)
- [Monitoring PAK Licenses, on page 40](#)
- [History for PAK Licenses, on page 41](#)

About PAK Licenses

A license specifies the options that are enabled on a given ASA. 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.

Preinstalled License

By default, your ASA 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.

Related Topics

[Monitoring PAK Licenses, on page 40](#)

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 ASA combines the permanent and time-based licenses into a running license.

Related Topics

[How Permanent and Time-Based Licenses Combine, on page 2](#)

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 AnyConnect Premium 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.



Note The ASA 5506-X and ASA 5506W-X do not support time-based licenses.

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 AnyConnect Premium license, and a 2500-session AnyConnect Premium 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 AnyConnect Premium license, you cannot also activate a standalone time-based 2500-session AnyConnect Premium license.

How the Time-Based License Timer Works

- The timer for the time-based license starts counting down when you activate it on the ASA.
- 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 ASA, then the timer stops counting down. The time-based license only counts down when the ASA is running. The system clock setting does not affect the license; only ASA uptime counts towards the license duration.

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. The following table 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: Time-Based License Combination Rules

Time-Based Feature	Combined License Rule
AnyConnect Premium 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.

Related Topics

[Monitoring PAK Licenses](#), on page 40

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 ASA allows you to *stack* time-based licenses so that 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 AnyConnect Premium 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 AnyConnect Premium 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.

Although non-identical licenses do not combine, when the current license expires, the ASA automatically activates an installed license of the same feature if available.

Related Topics

[Activate or Deactivate Keys](#), on page 17

[Time-Based License Expiration](#), on page 4

Time-Based License Expiration

When the current license for a feature expires, the ASA 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 ASA 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 ASA activated, then you must manually activate the license you prefer.

For example, you have a time-based 2500-session AnyConnect Premium license (active), a time-based 1000-session AnyConnect Premium license (inactive), and a permanent 500-session AnyConnect Premium license. While the 2500-session license expires, the ASA activates the 1000-session license. After the 1000-session license expires, the ASA uses the 500-session permanent license.

Related Topics

[Activate or Deactivate Keys](#), on page 17

License Notes

The following sections include additional information about licenses.

AnyConnect Plus and Apex Licenses

The AnyConnect Plus or Apex license is a multi-use license that you can apply to multiple ASAs, all of which share a user pool as specified by the license. See <https://www.cisco.com/go/license>, and assign the PAK separately to each ASA. When you apply the resulting activation key to an ASA, it toggles on the VPN features to the maximum allowed, but the actual number of unique users across all ASAs sharing the license should not exceed the license limit. For more information, see:

- [Cisco AnyConnect Ordering Guide](#)
- [AnyConnect Licensing Frequently Asked Questions \(FAQ\)](#)



Note The AnyConnect Apex license is required for multiple context mode. Moreover, in multiple context mode, this license must be applied to each unit in a failover pair; the license is not aggregated.

Other VPN License

Other VPN sessions include the following VPN types:

- IPsec remote access VPN using IKEv1
- IPsec site-to-site VPN using IKEv1
- IPsec site-to-site VPN using IKEv2

This license is included in the Base license.

Total VPN Sessions Combined, All Types

- Although the maximum VPN sessions add up to more than the maximum VPN AnyConnect and Other VPN sessions, the combined sessions should not exceed the VPN session limit. If you exceed the maximum VPN sessions, you can overload the ASA, 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.

VPN Load Balancing

VPN load balancing requires a Strong Encryption (3DES/AES) License.

Legacy VPN Licenses

Refer to the [Supplemental end User License Agreement for AnyConnect](#) for all relevant information on licensing.



Note The AnyConnect Apex license is required for multiple context mode; you cannot use the default or legacy license.

Encryption License

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 strong encryption.

Carrier License

The Carrier license enables the following inspection features:

- Diameter
- GTP/GPRS
- SCTP

Total TLS Proxy Sessions

Each TLS proxy session for Encrypted Voice Inspection is counted against the TLS license limit.

Other applications that use TLS proxy sessions do not count toward the TLS limit, for example, Mobility Advantage Proxy (which does not require a license).

Some 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.

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 TLS proxy license that is higher than the default TLS proxy limit, the ASA automatically sets the TLS proxy limit to match the license. The TLS proxy limit takes precedence over the license limit; if you set the TLS proxy limit to be less than the license, then you cannot use all of the sessions in your 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 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 no limit.



Note Only calls that require encryption/decryption for media are counted toward the SRTP limit; if passthrough is set for the call, even if both legs are SRTP, they do not count toward the limit.

VLANs, Maximum

For an interface to count against the VLAN limit, you must assign a VLAN to it.

Botnet Traffic Filter License

Requires a Strong Encryption (3DES/AES) License to download the dynamic database.

IPS Module License

The IPS module license lets you run the IPS software module on the ASA. You also need the IPS signature subscription on the IPS side.

See the following guidelines:

- To buy the IPS signature subscription you need to have the ASA with IPS pre-installed (the part number must include “IPS”, for example ASA5515-IPS-K9); you cannot buy the IPS signature subscription for a non-IPS part number ASA.
- For failover, you need the IPS signature subscription on both units; this subscription is not shared in failover, because it is not an ASA license.
- For failover, the IPS signature subscription requires a unique IPS module license per unit. Like other ASA licenses, the IPS module license is technically shared in the failover cluster license. However, because of the IPS signature subscription requirements, you must buy a separate IPS module license for each unit in failover.

Shared AnyConnect Premium Licenses (AnyConnect 3 and Earlier)



Note The shared license feature on the ASA is not supported with AnyConnect 4 and later licensing. AnyConnect licenses are shared and no longer require a shared server or participant license.

A shared license lets you purchase a large number of AnyConnect Premium sessions and share the sessions as needed among a group of ASAs by configuring one of the ASAs as a shared licensing server, and the rest as shared licensing participants.

Failover or ASA Cluster Licenses

With some exceptions, failover and cluster units do not require the same license on each unit. For earlier versions, see the licensing document for your version.

Failover License Requirements and Exceptions

Failover units do not require the same license on each unit. If you have licenses on both units, they combine into a single running failover cluster license. There are some exceptions to this rule. See the following table for precise licensing requirements for failover.

Model	License Requirement
ASA 5506-X and ASA 5506W-X	<ul style="list-style-type: none"> • Active/Standby—Security Plus License. • Active/Active—No Support. <p>Note Each unit must have the same encryption license.</p>
ASA 5512-X through ASA 5555-X	<ul style="list-style-type: none"> • ASA 5512-X—Security Plus License. • Other models—Base License. <p>Note</p> <ul style="list-style-type: none"> • Each unit must have the same encryption license. • In multiple context mode, each unit must have the the same AnyConnect Apex license. • Each unit must have the same IPS module license. You also need the IPS signature subscription on the IPS side for both units. See the following guidelines: <ul style="list-style-type: none"> • To buy the IPS signature subscription you need to have the ASA with IPS pre-installed (the part number must include “IPS”, for example ASA5525-IPS-K9); you cannot buy the IPS signature subscription for a non-IPS part number ASA. • You need the IPS signature subscription on both units; this subscription is not shared in failover, because it is not an ASA license. • The IPS signature subscription requires a unique IPS module license per unit. Like other ASA licenses, the IPS module license is technically shared in the failover cluster license. However, because of the IPS signature subscription requirements, you must buy a separate IPS module license for each unit in.
ASAv	See Failover Licenses for the ASAv .
Firepower 4100/9300	See Failover Licenses for the ASA on the Firepower 4100/9300 Chassis .
All other models	<p>Base License or Standard License.</p> <p>Note</p> <ul style="list-style-type: none"> • Each unit must have the same encryption license. • In multiple context mode, each unit must have the the same AnyConnect Apex license.



Note A valid permanent key is required; in rare instances, your PAK 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.

ASA Cluster License Requirements and Exceptions

Cluster units do not require the same license on each unit. Typically, you buy a license only for the control unit; data units inherit the control unit license. If you have licenses on multiple units, they combine into a single running ASA cluster license.

There are exceptions to this rule. See the following table for precise licensing requirements for clustering.

Model	License Requirement
ASA 5585-X	Cluster License, supports up to 16 units. Note Each unit must have the same encryption license; each unit must have the same 10 GE I/O/Security Plus license (ASA 5585-X with SSP-10 and -20).
ASA 5516-X	Base license, supports 2 units. Note Each unit must have the same encryption license.
ASA 5512-X	Security Plus license, supports 2 units. Note Each unit must have the same encryption license.
ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X	Base License, supports 2 units. Note Each unit must have the same encryption license.
Firepower 4100/9300 Chassis	See ASA Cluster Licenses for the ASA on the Firepower 4100/9300 Chassis .
All other models	No support.

How Failover or ASA Cluster Licenses Combine

For failover pairs or ASA clusters, the licenses on each unit are combined into a single running cluster license. If you buy separate licenses for each unit, then the combined license uses the following rules:

- For licenses that have numerical tiers, such as the number of sessions, the values from each unit's licenses are combined up to the platform limit. If all licenses in use are time-based, then the licenses count down simultaneously.

For example, for failover:

- You have two ASAs with 10 TLS Proxy sessions installed on each; the licenses will be combined for a total of 20 TLS Proxy sessions.
- You have an ASA 5545-X with 1000 TLS Proxy sessions, and another with 2000 sessions; because the platform limit is 2000, the combined license allows 2000 TLS Proxy sessions.

- You have two ASA 5545-X ASAs, one with 20 contexts and the other with 10 contexts; the combined license allows 30 contexts. For Active/Active failover, the contexts are divided between the two units. One unit can use 18 contexts and the other unit can use 12 contexts, for example, for a total of 30.

For example, for ASA clustering:

- You have 2 ASA 5516-X ASAs with the default 2 contexts. Because the platform limit is 5, the combined license allows a maximum of 4 contexts. Therefore, you can configure up to 4 contexts on the primary unit; each secondary unit will also have 4 contexts through configuration replication.
- You have four ASA 5516-X ASAs, three units with 5 contexts each, and one unit with the default 2 contexts. Because the platform limit is 5, the licenses will be combined for a total of 5 contexts. Therefore, you can configure up to 5 contexts on the primary unit; each secondary unit will also have 5 contexts through configuration replication.

- 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 all licenses. The primary/control unit counts down its license first, and when it expires, the secondary/data unit(s) start counting down its license, and so on. This rule also applies to Active/Active failover and ASA clustering, even though all units are actively operating.

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

Related Topics

[Monitoring PAK Licenses](#), on page 40

Loss of Communication Between Failover or ASA Cluster Units

If the 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 all units.

If you restore communication during the 30-day grace period, then for time-based licenses, the time elapsed is subtracted from the primary/control license; if the primary/control license becomes expired, only then does the secondary/data 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 all unit licenses, if installed. They are treated as separate licenses and do not benefit from the 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 two units. The combined running license allows a total duration of 104 weeks.
2. The units operate as a failover unit/ASA cluster for 10 weeks, leaving 94 weeks on the combined license (42 weeks on the primary/control, and 52 weeks on the secondary/data).
3. If the units lose communication (for example the primary/control unit fails), the secondary/data 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/control unit license. In this case, communication is restored after 4 weeks. Therefore, 4 weeks are subtracted from the primary/control 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/control and secondary/data licenses, leaving 84 weeks combined (36 weeks on the primary/control, and 46 weeks on the secondary/data).

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, then you can fail over to the other unit while you reload. If both units require reloading, then you can reload them separately so that you have no downtime.

Related Topics

[Activate or Deactivate Keys](#), on page 17

No Payload Encryption Models

You can purchase some models with No Payload Encryption. For export to some countries, payload encryption cannot be enabled on the Cisco ASA series. The ASA 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 Filter (which uses SSL).

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

Related Topics

[Monitoring PAK Licenses](#), on page 40

Licenses FAQ

Can I activate multiple time-based licenses, for example, AnyConnect Premium and Botnet Traffic Filter?

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

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

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 AnyConnect Premium license and a 2500-session license), the ASA automatically activates the next time-based license it finds for the feature.

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

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

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

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.

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

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.

Can I use a time-based or permanent AnyConnect Premium license in addition to a shared AnyConnect Premium license?

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 AnyConnect Premium 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 AnyConnect Premium sessions only; they cannot be added to the shared licensing pool for use by participants.

Guidelines for PAK Licenses

Context Mode Guidelines

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

Failover Guidelines

See [Failover or ASA Cluster Licenses, on page 7](#).

Model Guidelines

- Smart Licensing is supported on the ASAv only.
- Shared licenses are not supported on the ASAv, ASA 5506-X, ASA 5508-X, and ASA 5516-X.
- The ASA 5506-X and ASA 5506W-X do not support time-based licenses.

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 ASA 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

- 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.
- The serial number used for licensing is the one seen on the Activation Key page. This serial number is different from the chassis serial number printed on the outside of your hardware. The chassis serial number is used for technical support, but not for licensing.
- Once purchased, you cannot return a license for a refund or for an upgraded license.
- On a single unit, you cannot add two separate licenses for the same feature together; for example, if you purchase a 25-session SSL VPN license, and later purchase a 50-session license, you cannot use 75 sessions; you can use a maximum of 50 sessions. (You may be able to purchase a larger license at an upgrade price, for example from 25 sessions to 75 sessions; this kind of upgrade should be distinguished from adding two separate licenses together).
- Although you can activate all license types, some features are incompatible with each other. In the case of the AnyConnect Essentials license, the license is incompatible with the following licenses: AnyConnect Premium license, shared AnyConnect Premium license, and Advanced Endpoint Assessment license. By default, if you install the AnyConnect Essentials license (if it is available for your model), it is used

instead of the above licenses. You can disable the AnyConnect Essentials license in the configuration to restore use of the other licenses using the **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Essentials** pane.

Configure PAK Licenses

This section describes how to obtain an activation key and how to active it. You can also deactivate a key.

Order License PAKs and Obtain an Activation Key

To install a license on the ASA, you need Product Authorization Keys, which you can then register with Cisco.com to obtain an activation key. You can then enter the activation key on the ASA. You need a separate Product Authorization Key for each feature license. The PAKs are combined to give you a single activation key. You may have received all of your license PAKs in the box with your device. The ASA has the Base or Security Plus license pre-installed, along with the Strong Encryption (3DES/AES) license if you qualify for its use. If you need to manually request the Strong Encryption license (which is free), see <http://www.cisco.com/go/license>.

Before you begin

When you purchase 1 or more licenses for the device, you manage them in the Cisco Smart Software Manager: <https://software.cisco.com/#module/SmartLicensing>

If you do not yet have an account, [set up a new account](#). The Smart Software Manager lets you create a master account for your organization.

Procedure

Step 1 To purchase additional licenses, see <http://www.cisco.com/go/ccw>. See the following AnyConnect ordering guide and FAQ:

- [Cisco AnyConnect Ordering Guide](#)
- [AnyConnect Licensing Frequently Asked Questions \(FAQ\)](#)

After you order a license, you will then receive an email with a Product Authorization Key (PAK). For the AnyConnect licenses, you receive a multi-use PAK that you can apply to multiple ASAs that use the same pool of user sessions. The PAK email can take several days in some cases.

The ASA FirePOWER module uses a separate licensing mechanism from the ASA. See the quick start guide for your model for more information.

Step 2 Obtain the serial number for your ASA by choosing **Configuration > Device Management > Licensing > Activation Key** (in multiple context mode, view the serial number in the System execution space).

The serial number used for licensing is different from the chassis serial number printed on the outside of your hardware. The chassis serial number is used for technical support, but not for licensing.

Step 3 To obtain the activation key, 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 ASA
 - Your e-mail address

An activation key is automatically generated and sent to the e-mail 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 the process 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.
- Step 6** Install the activation key according to [Activate or Deactivate Keys, on page 17](#).
-

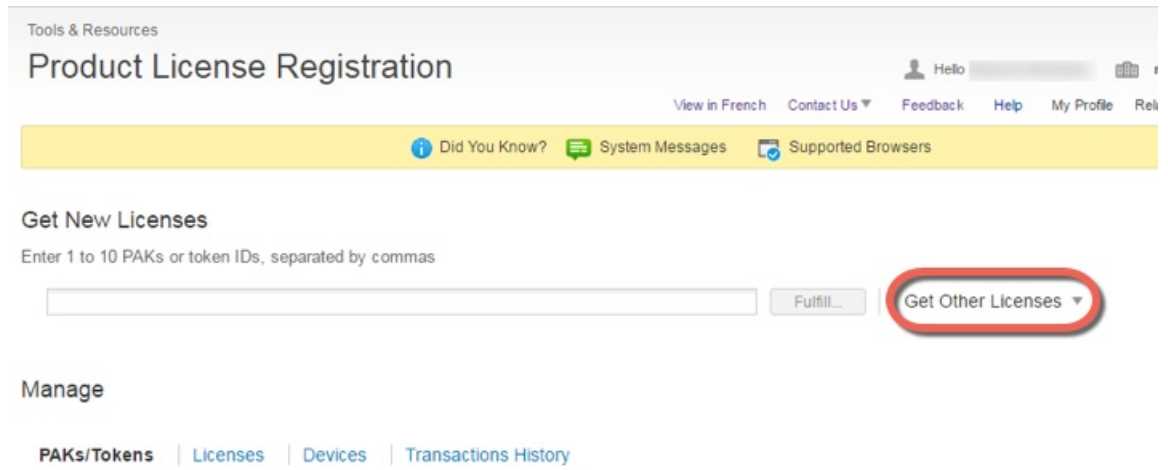
Obtain a Strong Encryption License

To use ASDM (and many other features), you need to install the Strong Encryption (3DES/AES) license. If your ASA did not come with the Strong Encryption license pre-installed, you can request one for free. You must qualify for a Strong Encryption license based on your country.

Procedure

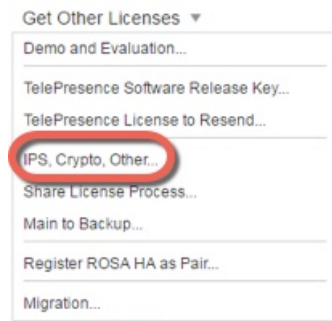
- Step 1** Obtain the serial number for your ASA by entering the following command:
- ```
show version | grep Serial
```
- This serial number is different from the chassis serial number printed on the outside of your hardware. The chassis serial number is used for technical support, but not for licensing.
- Step 2** See <https://www.cisco.com/go/license>, and click **Get Other Licenses**.

Figure 1: Get Other Licenses



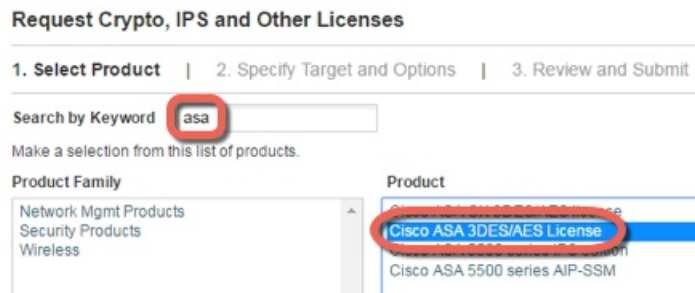
**Step 3** Choose **IPS, Crypto, Other**.

Figure 2: IPS, Crypto, Other



**Step 4** In the **Search by Keyword** field, enter **asa**, and select **Cisco ASA 3DES/AES License**.

Figure 3: Cisco ASA 3DES/AES License



**Step 5** Select your **Smart Account**, **Virtual Account**, enter the **ASA Serial Number**, and click **Next**.



Figure 4: Smart Account, Virtual Account, and Serial Number

**Request Crypto, IPS and Other Licenses**

1. Select Product | 2. Specify Target and Options

**Smart Account**  
Select one ...

**Virtual Account**  
Select one... Required with Smart Account

**Cisco ASA 3DES/AES License**

Serial Number:

- Step 6** Your Send To email address and End User name are auto-filled; enter additional email addresses if needed. Check the **I Agree** check box, and click **Submit**.

Figure 5: Submit

**Request Crypto, IPS and Other Licenses**

1. Select Product | 2. Specify Target and Options | 3. Review and Submit

**Recipient and Owner Information**

Enter multiple email addresses separated by commas. Your License Key will be emailed within the hour to the specified email addresses.

Send To:  Add...

End User:  Edit...

**License Request**

SerialNumber  
FCH1714J6HP

| Smart Account    | SKU Name        | Qty |
|------------------|-----------------|-----|
| ▶ Cisco Internal | ASA5500-ENCR-K9 | 1   |

- Step 7** You will then receive an email with the activation key, but you can also download the key right away from the **Manage > Licenses** area.

- Step 8** Apply the activation key according to [Activate or Deactivate Keys, on page 17](#).

## Activate or Deactivate Keys

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

### Before you begin

- 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 ASA after you activate them. The following table lists the licenses that require reloading.

Table 2: Permanent License Reloading Requirements

| Model      | License Action Requiring Reload     |
|------------|-------------------------------------|
| All models | Downgrading the Encryption license. |

### Procedure

- 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:
- ```
ASA0xd11b3d48 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.
- Step 4** Click **Update Activation Key**.
- Some permanent licenses require you to reload the ASA after entering the new activation key. You will be prompted to reload if it is required.

Related Topics

[Time-Based Licenses](#), on page 2

Configure a Shared License (AnyConnect 3 and Earlier)



Note The shared license feature on the ASA is not supported with AnyConnect 4 and later licensing. AnyConnect licenses are shared and no longer require a shared server or participant license.

This section describes how to configure the shared licensing server and participants.

About Shared Licenses

A shared license lets you purchase a large number of AnyConnect Premium sessions and share the sessions as needed among a group of ASAs by configuring one of the ASAs as a shared licensing server, and the rest as shared licensing participants.

About the Shared Licensing Server and Participants

The following steps describe how shared licenses operate:

1. Decide which ASA should be the shared licensing server, and purchase the shared licensing server license using that device serial number.
2. Decide which ASAs 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 ASA 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 ASA 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 ASA 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.

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.

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 ASA, 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.



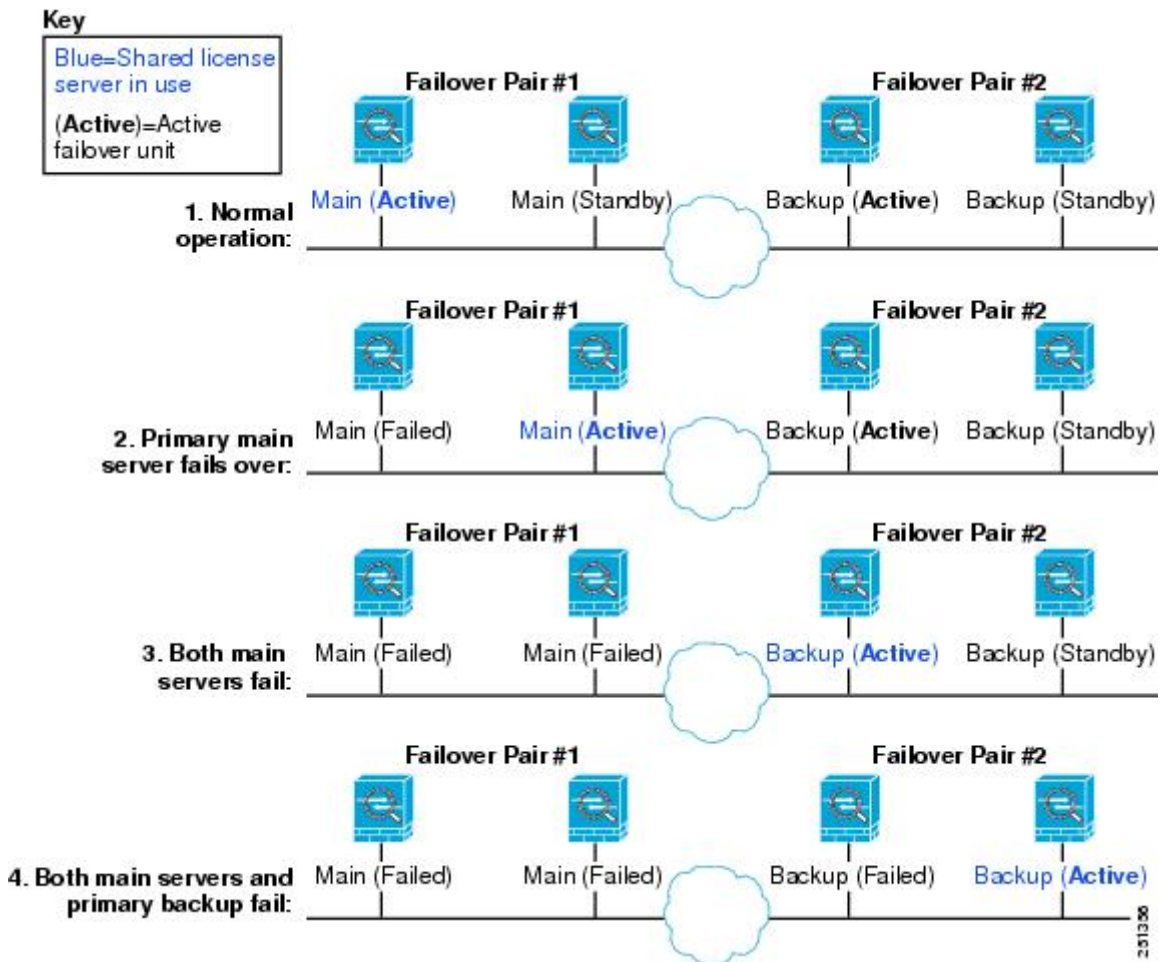
Note The backup server mechanism is separate from, but compatible with, failover.

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 the following figure).

Figure 6: 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.

Related Topics

[About the Shared Licensing Backup Server](#), on page 20

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 ASA 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.

Configure the Shared Licensing Server

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

Before you begin

The server must have a shared licensing server key.

Procedure

- 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:
- In the **Backup server IP address** field, enter the backup server IP address.
 - In the **Primary backup server serial number** field, enter the backup server serial number.
 - 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**.
-

Configure the Shared Licensing Participant and the Optional Backup Server

This section configures a shared licensing participant to communicate with the shared licensing server. This section also describes how you can optionally configure the participant as the backup server.

Before you begin

The participant must have a shared licensing participant key.

Procedure

- 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:
- Click the **Backup Server** radio button.
 - Check the **Shares Licenses** check box for any interfaces on which participants contact the backup server.
- Step 5** Click **Apply**.

Supported Feature Licenses Per Model

This section describes the licenses available for each model as well as important notes about licenses.

Licenses Per Model

This section lists the feature licenses available for each model:

Items that are in *italics* are separate, optional licenses that can replace the Base (or Security Plus, and so on) license version. You can mix and match optional licenses.



Note Some features are incompatible with each other. See the individual feature chapters for compatibility information.

If you have a No Payload Encryption model, then some of the features below are not supported. See [No Payload Encryption Models, on page 11](#) for a list of unsupported features.

For detailed information about licenses, see [License Notes, on page 4](#).

ASA 5506-X and ASA 5506W-X License Features

The following table shows the licensed features for the ASA 5506-X and ASA 5506W-X.

Licenses	Base License	Security Plus License
Firewall Licenses		
Botnet Traffic Filter	No support	No Support
Firewall Conns, Concurrent	20,000	50,000
Carrier	No Support	No Support

Licenses	Base License		Security Plus License	
Total TLS Proxy Sessions	160		160	
VPN Licenses				
AnyConnect peers	Disabled	<i>Optional AnyConnect Plus or Apex license: 50 maximum</i>	Disabled	<i>Optional AnyConnect Plus or Apex license: 50 maximum</i>
Other VPN Peers	10		50	
Total VPN Peers, combined all types	50		50	
VPN Load Balancing	No support		No support	
General Licenses				
Encryption	Base (DES)	<i>Opt. lic.: Strong (3DES/AES)</i>	Base (DES)	<i>Opt. lic.: Strong (3DES/AES)</i>
Failover	No support		Active/Standby	
Security Contexts	No support		No support	
Clustering	No Support		No Support	
VLANs, Maximum	5		30	

ASA 5506H-X License Features

The following table shows the licensed features for the ASA 5506H-X.

Licenses	Base License
Firewall Licenses	
Botnet Traffic Filter	No Support
Firewall Conns, Concurrent	50,000

Licenses	Base License	
Carrier	No Support	
Total UC Proxy Sessions	160	
VPN Licenses		
AnyConnect Plus or Apex license (purchased separately), maximum premium peers	50	
Total VPN Peers, combined all types	50	
Other VPN Peers	50	
VPN Load Balancing	Enabled	
General Licenses		
Encryption	Base (DES)	<i>Opt. lic.: Strong (3DES/AES)</i>
Failover	Active/Standby or Active/Active	
Security Contexts	No Support	
Clustering	No Support	
VLANs, Maximum	30	

ASA 5508-X License Features

The following table shows the licensed features for the ASA 5508-X.

Licenses	Base License	
Firewall Licenses		
Botnet Traffic Filter	No Support	
Firewall Conns, Concurrent	100,000	
Carrier	No Support	

Licenses	Base License			
Total TLS Proxy Sessions	320			
VPN Licenses				
AnyConnect peers	Disabled		<i>Optional AnyConnect Plus or Apex license: 100 maximum</i>	
Total VPN Peers, combined all types	100			
Other VPN Peers	100			
VPN Load Balancing	Enabled			
General Licenses				
Encryption	Base (DES)		<i>Opt. lic.: Strong (3DES/AES)</i>	
Failover	Active/Standby or Active/Active			
Security Contexts	2	<i>Optional licenses:</i>		5
Clustering	No Support			
VLANs, Maximum	50			

ASA 5512-X License Features

The following table shows the licensed features for the ASA 5512-X.

Licenses	Base License					Security Plus License						
Firewall Licenses												
Botnet Traffic Filter	Disabled		<i>Optional Time-based license: Available</i>			Disabled		<i>Optional Time-based license: Available</i>				
Firewall Conns, Concurrent	100,000					250,000						
Carrier	No support					No Support						
Total TLS Proxy Sessions	2	<i>Optional licenses:</i>					2	<i>Optional licenses:</i>				
		24	50	100	250	500		24	50	100	250	500

Licenses	Base License		Security Plus License	
VPN Licenses				
AnyConnect peers	Disabled	<i>Optional AnyConnect Plus or Apex license: 250 maximum</i>	Disabled	<i>Optional AnyConnect Plus or Apex license: 250 maximum</i>
Other VPN Peers	250		250	
Total VPN Peers, combined all types	250		250	
VPN Load Balancing	No support		Enabled	
General Licenses				
Encryption	Base (DES)	<i>Opt. lic.: Strong (3DES/AES)</i>	Base (DES)	<i>Opt. lic.: Strong (3DES/AES)</i>
Failover	No support		Active/Standby or Active/Active	
Security Contexts	No support		2	<i>Optional licenses:</i> 5
Clustering	No Support		2	
IPS Module	Disabled	<i>Optional license: Available</i>	Disabled	<i>Optional license: Available</i>
VLANs, Maximum	50		100	

ASA 5515-X License Features

The following table shows the licensed features for the ASA 5515-X.

Licenses	Base License	
Firewall Licenses		
Botnet Traffic Filter	Disabled	<i>Optional Time-based license: Available</i>
Firewall Conns, Concurrent	250,000	

Licenses	Base License						
Carrier	No Support						
Total TLS Proxy Sessions	2	<i>Optional licenses:</i>	24	50	100	250	500
VPN Licenses							
AnyConnect peers	Disabled	<i>Optional AnyConnect Plus or Apex license: 250 maximum</i>					
Other VPN Peers	250						
Total VPN Peers, combined all types	250						
VPN Load Balancing	Enabled						
General Licenses							
Encryption	Base (DES)	<i>Optional license: Strong (3DES/AES)</i>					
Failover	Active/Standby or Active/Active						
Security Contexts	2	<i>Optional licenses:</i>	5				
Clustering	2						
IPS Module	Disabled	<i>Optional license: Available</i>					
VLANs, Maximum	100						

ASA 5516-X License Features

The following table shows the licensed features for the ASA 5516-X.

Licenses	Base License
Firewall Licenses	

Licenses	Base License		
Botnet Traffic Filter	No Support		
Firewall Conns, Concurrent	250,000		
Carrier	No Support		
Total TLS Proxy Sessions	1000		
VPN Licenses			
AnyConnect peers	Disabled	<i>Optional AnyConnect Plus or Apex license: 300 maximum</i>	
Other VPN Peers	300		
Total VPN Peers, combined all types	300		
VPN Load Balancing	Enabled		
General Licenses			
Encryption	Base (DES)	<i>Opt. lic.: Strong (3DES/AES)</i>	
Failover	Active/Standby or Active/Active		
Security Contexts	2	<i>Optional licenses:</i>	5
Clustering	2		
VLANs, Maximum	150		

ASA 5525-X License Features

The following table shows the licensed features for the ASA 5525-X.

Licenses	Base License		
Firewall Licenses			
Botnet Traffic Filter	Disabled	<i>Optional Time-based license: Available</i>	

Licenses	Base License								
Firewall Conns, Concurrent	500,000								
Carrier	Disabled	<i>Optional license: Available</i>							
Total TLS Proxy Sessions	2	<i>Optional licenses:</i>	24	50	100	250	500	750	1000
VPN Licenses									
AnyConnect peers	Disabled	<i>Optional AnyConnect Plus or Apex license: 750 maximum</i>							
Other VPN Peers	750								
Total VPN Peers, combined all types	750								
VPN Load Balancing	Enabled								
General Licenses									
Encryption	Base (DES)	<i>Optional license: Strong (3DES/AES)</i>							
Failover	Active/Standby or Active/Active								
Security Contexts	2	<i>Optional licenses:</i>	5	10	20				
Clustering	2								
IPS Module	Disabled	<i>Optional license: Available</i>							
VLANs, Maximum	200								

ASA 5545-X License Features

The following table shows the licensed features for the ASA 5545-X.

Licenses	Base License									
Firewall Licenses										
Botnet Traffic Filter	Disabled	<i>Optional Time-based license: Available</i>								
Firewall Conns, Concurrent	750,000									
Carrier	Disabled	<i>Optional license: Available</i>								
Total TLS Proxy Sessions	2	<i>Optional licenses:</i>	24	50	100	250	500	750	1000	2000
VPN Licenses										
AnyConnect peers	Disabled	<i>Optional AnyConnect Plus or Apex license: 2500 maximum</i>								
Other VPN Peers	2500									
Total VPN Peers, combined all types	2500									
VPN Load Balancing	Enabled									
General Licenses										
Encryption	Base (DES)	<i>Optional license: Strong (3DES/AES)</i>								
Failover	Active/Standby or Active/Active									
Security Contexts	2	<i>Optional licenses:</i>	5	10	20	50				
Clustering	2									
IPS Module	Disabled	<i>Optional license: Available</i>								
VLANs, Maximum	300									

ASA 5555-X License Features

The following table shows the licensed features for the ASA 5555-X.

Licenses	Base License									
Firewall Licenses										
Botnet Traffic Filter	Disabled		<i>Optional Time-based license: Available</i>							
Firewall Conns, Concurrent	1,000,000									
Carrier	Disabled		<i>Optional license: Available</i>							
Total TLS Proxy Sessions	2		<i>Optional licenses:</i>							
	24	50	100	250	500	750	1000	2000	3000	
VPN Licenses										
AnyConnect peers	Disabled		<i>Optional AnyConnect Plus or Apex license: 5000 maximum</i>							
Other VPN Peers	5000									
Total VPN Peers, combined all types	5000									
VPN Load Balancing	Enabled									
General Licenses										
Encryption	Base (DES)		<i>Optional license: Strong (3DES/AES)</i>							
Failover	Active/Standby or Active/Active									
Security Contexts	2	<i>Optional licenses:</i>			5	10	20	50	100	
Clustering	2									
IPS Module	Disabled		<i>Optional license: Available</i>							

Licenses	Base License
VLANs, Maximum	500

ASA 5585-X with SSP-10 License Features

The following table shows the licensed features for the ASA 5585-X with SSP-10.

You can use two SSPs of the same level in the same chassis. Mixed-level SSPs are not supported (for example, an SSP-10 with an SSP-20 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.

Licenses	Base and Security Plus Licenses									
Firewall Licenses										
Botnet Traffic Filter	Disabled		<i>Optional Time-based license: Available</i>							
Firewall Conns, Concurrent	1,000,000									
Carrier	Disabled		<i>Optional license: Available</i>							
Total TLS Proxy Sessions	2									
	<i>Optional licenses:</i>									
	24	50	100	250	500	750	1000	2000	3000	
VPN Licenses										
AnyConnect peers	Disabled		<i>Optional AnyConnect Plus or Apex license: 5000 maximum</i>							
Other VPN Peers	5000									
Total VPN Peers, combined all types	5000									
VPN Load Balancing	Enabled									
General Licenses										

Licenses	Base and Security Plus Licenses							
10 GE I/O	Base License: Disabled; fiber ifcs run at 1 GE				Security Plus License: Enabled; fiber ifcs run at 10 GE			
Encryption	Base (DES)	Optional license: Strong (3DES/AES)						
Failover	Active/Standby or Active/Active							
Security Contexts	2	Optional licenses:		5	10	20	50	100
Clustering	Disabled	Optional license: Available for 16 units						
VLANs, Maximum	1024							

ASA 5585-X with SSP-20 License Features

The following table shows the licensed features for the ASA 5585-X with SSP-20.

You can use two SSPs of the same level in the same chassis. Mixed-level SSPs are not supported (for example, an SSP-20 with an SSP-40 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.



Note With the 10,000-session UC license, the total combined sessions can be 10,000, but the maximum number of Phone Proxy sessions is 5000.

Licenses	Base and Security Plus Licenses											
Firewall Licenses												
Botnet Traffic Filter	Disabled	Optional Time-based license: Available										
Firewall Conns, Concurrent	2,000,000											
Carrier	Disabled	Optional license: Available										
Total TLS Proxy Sessions	2	Optional licenses:										
		24	50	100	250	500	750	1000	2000	3000	5000	10,000
VPN Licenses												
AnyConnect peers	Disabled	Optional AnyConnect Plus or Apex license: 10,000 maximum										

Licenses	Base and Security Plus Licenses								
Other VPN Peers	10,000								
Total VPN Peers, combined all types	10,000								
VPN Load Balancing	Enabled								
General Licenses									
10 GE I/O	Base License: Disabled; fiber ifcs run at 1 GE				Security Plus License: Enabled; fiber ifcs run at 10 GE				
Encryption	Base (DES)		Optional license: Strong (3DES/AES)						
Failover	Active/Standby or Active/Active								
Security Contexts	2	Optional licenses:		5	10	20	50	100	250
Clustering	Disabled		Optional license: Available for 16 units						
VLANs, Maximum	1024								

ASA 5585-X with SSP-40 and -60 License Features

The following table shows the licensed features for the ASA 5585-X with SSP-40 and -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.



Note With the 10,000-session UC license, the total combined sessions can be 10,000, but the maximum number of Phone Proxy sessions is 5000.

Licenses	Base License							
Firewall Licenses								
Botnet Traffic Filter	Disabled		Optional Time-based license: Available					

Licenses	Base License											
Firewall Conns, Concurrent	5585-X with SSP-40: 4,000,000						5585-X with SSP-60: 10,000,000					
Carrier	Disabled		<i>Optional license: Available</i>									
Total TLS Proxy Sessions	2		<i>Optional licenses:</i>									
	24	50	100	250	500	750	1000	2000	3000	5000	10,000	
VPN Licenses												
AnyConnect peers	Disabled		<i>Optional AnyConnect Plus or Apex license: 10,000 maximum</i>									
Other VPN Peers	10,000											
Total VPN Peers, combined all types	10,000											
VPN Load Balancing	Enabled											
General Licenses												
10 GE I/O	Enabled; fiber ifcs run at 10 GE											
Encryption	Base (DES)		<i>Optional license: Strong (3DES/AES)</i>									
Failover	Active/Standby or Active/Active											
Security Contexts	2		<i>Optional licenses:</i>			5	10	20	50	100	250	
Clustering	Disabled		<i>Optional license: Available for 16 units</i>									
VLANs, Maximum	1024											

ASASM License Features

The following table shows the licensed features for the ASA Services Module.



Note With the 10,000-session UC license, the total combined sessions can be 10,000, but the maximum number of Phone Proxy sessions is 5000.

Licenses		Base License											
Firewall Licenses													
Botnet Traffic Filter	Disabled	<i>Optional Time-based license: Available</i>											
Firewall Conns, Concurrent	10,000,000												
Carrier	Disabled	<i>Optional license: Available</i>											
Total TLS Proxy Sessions	2	<i>Optional licenses:</i>											
		24	50	100	250	500	750	1000	2000	3000	5000	10,000	
VPN Licenses													
AnyConnect peers	Disabled	<i>Optional AnyConnect Plus or Apex license: 10,000 maximum</i>											
Other VPN Peers	10,000												
Total VPN Peers, combined all types	10,000												
VPN Load Balancing	Enabled												
General Licenses													
Encryption	Base (DES)	<i>Optional license: Strong (3DES/AES)</i>											
Failover	Active/Standby or Active/Active												
Security Contexts	2	<i>Optional licenses:</i>											
		5	10	20	50	100	250						
Clustering	No support												

Licenses	Base License
VLANs, Maximum	1000

ISA 3000 License Features

The following table shows the licensed features for the ISA 3000.

Licenses	Base License	Security Plus License
Firewall Licenses		
Botnet Traffic Filter	No support	No Support
Firewall Conns, Concurrent	20,000	50,000
Carrier	No Support	No Support
Total TLS Proxy Sessions	160	160
VPN Licenses		
AnyConnect peers	Disabled <i>Optional AnyConnect Plus or Apex license: 25 maximum</i>	Disabled <i>Optional AnyConnect Plus or Apex license: 25 maximum</i>
Other VPN Peers	10	50
Total VPN Peers, combined all types	25	50
VPN Load Balancing	No support	No support
General Licenses		
Encryption	Base (DES) <i>Opt. lic.: Strong (3DES/AES)</i>	Base (DES) <i>Opt. lic.: Strong (3DES/AES)</i>
Failover	No support	Active/Standby

Licenses	Base License	Security Plus License
Security Contexts	No support	No Support
Clustering	No Support	No Support
VLANs, Maximum	5	25

Monitoring PAK Licenses

This section describes how to view license information.

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.

Before you begin

If you have a No Payload Encryption model, then you view the license, VPN and Unified Communications licenses will not be listed. See [No Payload Encryption Models, on page 11](#) for more information.

Procedure

-
- 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 [How Failover or ASA Cluster Licenses Combine, on page 9](#) 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**.
-

Monitoring the Shared License

To monitor the shared license, choose **Monitoring > VPN > Clientless SSL VPN > Shared Licenses**.

History for PAK Licenses

Feature Name	Platform Releases	Description
Increased Connections and VLANs	7.0(5)	<p>Increased the following limits:</p> <ul style="list-style-type: none"> • 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.

Feature Name	Platform Releases	Description
Increased VLANs	7.2(2)	<p>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.</p> <p>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).</p>
Gigabit Ethernet Support for the ASA 5510 Security Plus License	7.2(3)	<p>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.</p> <p>Note The interface names remain Ethernet 0/0 and Ethernet 0/1.</p>

Feature Name	Platform Releases	Description
Advanced Endpoint Assessment License	8.0(2)	<p>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 antispymware 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 ASA. The ASA uses both the user login credentials and the computer scan results to assign a Dynamic Access Policy (DAP).</p> <p>With an Advanced Endpoint Assessment License, you can enhance Host Scan by configuring an attempt to update noncompliant computers to meet version requirements.</p> <p>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.</p>
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 ASA 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)	<p>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.</p> <p>This feature is not available in Version 8.1.</p>

Feature Name	Platform Releases	Description
Botnet Traffic Filter License	8.2(1)	<p>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.</p>
AnyConnect Essentials License	8.2(1)	<p>The AnyConnect Essentials License was introduced. This license enables AnyConnect VPN client access to the ASA. 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.</p> <p>Note With the AnyConnect Essentials license, VPN users can use a Web browser to log in, and download and start (WebLaunch) the AnyConnect client.</p> <p>The AnyConnect client software offers the same set of client features, whether it is enabled by this license or an AnyConnect Premium license.</p> <p>The AnyConnect Essentials license cannot be active at the same time as the following licenses on a given ASA: AnyConnect Premium license (all types) or the Advanced Endpoint Assessment license. You can, however, run AnyConnect Essentials and AnyConnect Premium licenses on different ASAs in the same network.</p> <p>By default, the ASA uses the AnyConnect Essentials license, but you can disable it to use other licenses by using the Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Essentials pane.</p>
SSL VPN license changed to AnyConnect Premium SSL VPN Edition license	8.2(1)	<p>The SSL VPN license name was changed to the AnyConnect Premium SSL VPN Edition license.</p>

Feature Name	Platform Releases	Description
Shared Licenses for SSL VPN	8.2(1)	Shared licenses for SSL VPN were introduced. Multiple ASAs 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).
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 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 ASA allows you to <i>stack</i> time-based licenses so that 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.

Feature Name	Platform Releases	Description
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 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. We modified the following screen: 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.
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 ASA.
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.

Feature Name	Platform Releases	Description
Increased connections for the ASA 5580 and 5585-X	8.4(1)	<p>We increased the firewall connection limits:</p> <ul style="list-style-type: none"> • 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)	<p>IPsec remote access VPN using IKEv2 was added to the AnyConnect Essentials and AnyConnect Premium licenses.</p> <p>Note The following limitation exists in our support for IKEv2 on the ASA: We currently do not support duplicate security associations.</p> <p>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.</p>

Feature Name	Platform Releases	Description
No Payload Encryption hardware for export	8.4(1)	For models available with No Payload Encryption (for example, the ASA 5585-X), the ASA software disables Unified Communications and VPN features, making the ASA 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.
IPS Module license for the ASA 5512-X through ASA 5555-X	8.6(1)	The IPS SSP software module on the ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X requires the IPS module license.
Clustering license for the ASA 5580 and ASA 5585-X.	9.0(1)	A clustering license was added for the ASA 5580 and ASA 5585-X.
Support for VPN on the ASASM	9.0(1)	The ASASM now supports all VPN features.
Unified communications support on the ASASM	9.0(1)	The ASASM now supports all Unified Communications features.
ASA 5585-X Dual SSP support for the SSP-10 and SSP-20 (in addition to the SSP-40 and SSP-60); VPN support for Dual SSPs	9.0(1)	The ASA 5585-X now supports dual SSPs using all SSP models (you can use two SSPs of the same level in the same chassis). VPN is now supported when using dual SSPs.
ASA 5500-X support for clustering	9.1(4)	The ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X, and ASA 5555-X now support 2-unit clusters. Clustering for 2 units is enabled by default in the base license; for the ASA 5512-X, you need the Security Plus license.
Support for 16 cluster members for the ASA 5585-X	9.2(1)	The ASA 5585-X now supports 16-unit clusters.

Feature Name	Platform Releases	Description
ASAv4 and ASAv30 Standard and Premium model licenses introduced	9.2(1)	The ASAv was introduced with a simple licensing scheme: ASAv4 and ASAv30 permanent licenses in Standard or Premium levels. No add-on licenses are available.

