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 14
- Configure PAK Licenses, on page 16
- Configure a Shared License (AnyConnect 3 and Earlier), on page 20
- Supported Feature Licenses Per Model, on page 27
- Monitoring PAK Licenses, on page 43
- History for PAK Licenses, on page 53

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 43

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

<table>
<thead>
<tr>
<th>Time-Based Feature</th>
<th>Combined License Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnyConnect Premium Sessions</td>
<td>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.</td>
</tr>
<tr>
<td>Unified Communications Proxy Sessions</td>
<td>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.</td>
</tr>
<tr>
<td>Security Contexts</td>
<td>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.</td>
</tr>
<tr>
<td>Botnet Traffic Filter</td>
<td>There is no permanent Botnet Traffic Filter license available; the time-based license is used.</td>
</tr>
<tr>
<td>All Others</td>
<td>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.</td>
</tr>
</tbody>
</table>

### Related Topics
- Monitoring PAK Licenses, on page 43

### 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 19
- 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 19

**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](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:
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

For pre-existing deployments, the legacy licenses are still supported, including the default license that includes 2 AnyConnect premium sessions (4 sessions for the ASA 5506-X with Security Plus, 5508-X, and 5516-X). However, you should upgrade to the AnyConnect Plus or Apex license for full compatibility.

AnyConnect Essentials

The AnyConnect Essentials sessions include the following VPN types:

- SSL VPN
- IPsec remote access VPN using IKEv2
This license does not support browser-based (clientless) 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 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.

You can disable this license to use other licenses by using the `webvpn`, and then the `no anyconnect-essentials` command or in ASDM, using the **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Essentials** pane.

**AnyConnect for Cisco VPN Phone**

In conjunction with an AnyConnect Premium license, this license enables access from hardware IP phones that have built in AnyConnect compatibility.

**AnyConnect for Mobile**

This license provides access to the AnyConnect Client for touch-screen mobile devices running Windows Mobile 5.0, 6.0, and 6.1. We recommend using this license if you want to support mobile access to AnyConnect 2.3 and later versions. This license requires activation of one of the following licenses to specify the total number of SSL VPN sessions permitted: AnyConnect Essentials or AnyConnect Premium.

**Mobile Posture Support**

Enforcing remote access controls and gathering posture data from mobile devices requires an AnyConnect Mobile license and either an AnyConnect Essentials or AnyConnect Premium license to be installed on the ASA. Here is the functionality you receive based on the license you install.

- **AnyConnect Premium License Functionality**
  - Enforce DAP policies on supported mobile devices based on DAP attributes and any other existing endpoint attributes. This includes allowing or denying remote access from a mobile device.

- **AnyConnect Essentials License Functionality**
  - Enable or disable mobile device access on a per group basis and to configure that feature using ASDM.
  - Display information about connected mobile devices via CLI or ASDM without having the ability to enforce DAP policies or deny or allow remote access to those mobile devices.

**AnyConnect Premium**

AnyConnect Premium sessions include the following VPN types:
- SSL VPN
- Clientless SSL VPN
- IPsec remote access VPN using IKEv2

**AnyConnect Premium Shared**

A shared license lets the ASA act as a shared license server for multiple client ASAs. The shared license pool is large, but the maximum number of sessions used by each individual ASA cannot exceed the maximum number listed for permanent licenses.

**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.
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.

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. For example:

```
interface gigabitethernet 0/0.100
vlan 100
```

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.

<table>
<thead>
<tr>
<th>Model</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA 5506-X and ASA 5506W-X</td>
<td>• Active/Standby—Security Plus License.</td>
</tr>
<tr>
<td></td>
<td>• Active/Active—No Support.</td>
</tr>
<tr>
<td></td>
<td>Note: Each unit must have the same encryption license.</td>
</tr>
<tr>
<td>Model</td>
<td>License Requirement</td>
</tr>
<tr>
<td>-------</td>
<td>---------------------</td>
</tr>
</tbody>
</table>
| ASA 5512-X through ASA 5555-X | • ASA 5512-X—Security Plus License.  
• Other models—Base License.  
**Note**  
• 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:  
  • 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.  
  • 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. |
| ASAav | See Failover Licenses for the ASAav. |
| ASA on the Firepower 4100/9300 Chassis | See Failover Licenses for the ASA on the Firepower 4100/9300 Chassis. |
| All other models | Base License or Standard License.  
**Note**  
• 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 master unit; slave units inherit the master 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.

<table>
<thead>
<tr>
<th>Model</th>
<th>License Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA 5585-X</td>
<td>Cluster License, supports up to 16 units.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>  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).</td>
</tr>
<tr>
<td>ASA 5516-X</td>
<td>Base license, supports 2 units.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>  Each unit must have the same encryption license.</td>
</tr>
<tr>
<td>ASA 5512-X</td>
<td>Security Plus license, supports 2 units.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>  Each unit must have the same encryption license.</td>
</tr>
<tr>
<td>ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X</td>
<td>Base License, supports 2 units.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>  Each unit must have the same encryption license.</td>
</tr>
<tr>
<td>ASA on the Firepower 4100/9300 Chassis</td>
<td>See ASA Cluster Licenses for the ASA on the Firepower 4100/9300 Chassis.</td>
</tr>
<tr>
<td>All other models</td>
<td>No support.</td>
</tr>
</tbody>
</table>

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/master unit counts down its license first, and when it expires, the secondary/slave 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 43

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/master license; if the primary/master license becomes expired, only then does the secondary/slave 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/master, and 52 weeks on the secondary/slave).

3. If the units lose communication (for example the primary/master unit fails), the secondary/slave 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/master unit license. In this case, communication is restored after 4 weeks. Therefore, 4 weeks are subtracted from the primary/master 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/master and secondary/slave
licenses, leaving 84 weeks combined (36 weeks on the primary/master, and 46 weeks on the secondary/slave).

**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 19

**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 43

**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 9.

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 in the show version output. 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 webvpn, and then the no anyconnect-essentials command.
Configure PAK Licenses

This section describes how to obtain an activation key and how to activate 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 entering the following command.

```
show version | grep Serial
```

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 19](#).

---

**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](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*

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.
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 19.

## 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>
<thead>
<tr>
<th>Model</th>
<th>License Action Requiring Reload</th>
</tr>
</thead>
<tbody>
<tr>
<td>All models</td>
<td>Downgrading the Encryption license.</td>
</tr>
</tbody>
</table>

### Procedure

**Step 1** Apply an activation key to the ASA:

```
activation-key key [activate | deactivate]
```

**Example:**

```
ciscoasa# activation-key 0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490
```
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 ASA in an inactive state.

Step 2
(Might be required.) Reload the ASA:

reload

Some permanent licenses require you to reload the ASA after entering the new activation key. 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.

---

**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.

1. 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.

2. 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 22

**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**

Set the shared secret:

```
license-server secret secret
```

*Example:*

```
ciscoasa(config)# license-server secret farscape
```

The `secret` is a string between 4 and 128 ASCII characters. Any participant with this secret can use the licensing server.

**Step 2**

(Optional) Set the refresh interval:

```
license-server refresh-interval seconds
```

*Example:*

```
ciscoasa(config)# license-server refresh-interval 100
```

The interval is between 10 and 300 seconds; this value is provided to participants to set how often they should communicate with the server. The default is 30 seconds.

**Step 3**

(Optional) Set the port on which the server listens for SSL connections from participants:

```
license-server port port
```

*Example:*

```
ciscoasa(config)# license-server port 40000
```

The `port` is between 1 and 65535. The default is TCP port 50554.

**Step 4**

(Optional) Identify the backup server IP address and serial number:
Configure the Shared Licensing Backup Server (Optional)

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

**Before you begin**

The backup server must have a shared licensing participant key.

**Procedure**

**Step 1**

Identify the shared licensing server IP address and shared secret:

```
license-server address address secret secret [port port]
```

**Example:**

```
ciscoasa(config)# license-server address 10.1.1.2 address JMX0916L0Z4 secret secret
```

If the backup server is part of a failover pair, identify the standby unit serial number as well. You can only identify 1 backup server and its optional standby unit.

**Step 5**

Enable this unit to be the shared licensing server:

```
license-server enable interface_name
```

**Example:**

```
ciscoasa(config)# license-server enable inside
```

Specify the interface on which participants contact the server. You can repeat this command for as many interfaces as desired.

**Examples**

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

```
ciscoasa(config)# license-server secret farscape
```

```
ciscoasa(config)# license-server refresh-interval 100
```

```
ciscoasa(config)# license-server port 40000
```

```
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id JMX1378N0W3
```

```
ciscoasa(config)# license-server enable inside
```

```
ciscoasa(config)# license-server enable dmz
```

---

**Configure the Shared Licensing Backup Server (Optional)**

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

**Before you begin**

The backup server must have a shared licensing participant key.

**Procedure**

**Step 1**

Identify the shared licensing server IP address and shared secret:

```
license-server address address secret secret [port port]
```

**Example:**

```
ciscoasa(config)# license-server address 10.1.1.2 address JMX0916L0Z4 secret secret
```

If the backup server is part of a failover pair, identify the standby unit serial number as well. You can only identify 1 backup server and its optional standby unit.

**Step 5**

Enable this unit to be the shared licensing server:

```
license-server enable interface_name
```

**Example:**

```
ciscoasa(config)# license-server enable inside
```

Specify the interface on which participants contact the server. You can repeat this command for as many interfaces as desired.

**Examples**

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

```
ciscoasa(config)# license-server secret farscape
```

```
ciscoasa(config)# license-server refresh-interval 100
```

```
ciscoasa(config)# license-server port 40000
```

```
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id JMX1378N0W3
```

```
ciscoasa(config)# license-server enable inside
```

```
ciscoasa(config)# license-server enable dmz
```

---

**Configure the Shared Licensing Backup Server (Optional)**

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

**Before you begin**

The backup server must have a shared licensing participant key.

**Procedure**

**Step 1**

Identify the shared licensing server IP address and shared secret:

```
license-server address address secret secret [port port]
```

**Example:**

```
ciscoasa(config)# license-server address 10.1.1.2 address JMX0916L0Z4 secret secret
```

If the backup server is part of a failover pair, identify the standby unit serial number as well. You can only identify 1 backup server and its optional standby unit.

**Step 5**

Enable this unit to be the shared licensing server:

```
license-server enable interface_name
```

**Example:**

```
ciscoasa(config)# license-server enable inside
```

Specify the interface on which participants contact the server. You can repeat this command for as many interfaces as desired.

**Examples**

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

```
ciscoasa(config)# license-server secret farscape
```

```
ciscoasa(config)# license-server refresh-interval 100
```

```
ciscoasa(config)# license-server port 40000
```

```
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id JMX1378N0W3
```

```
ciscoasa(config)# license-server enable inside
```

```
ciscoasa(config)# license-server enable dmz
```
Configure the Shared Licensing Participant

This section configures a shared licensing participant to communicate with the shared licensing server.

Before you begin

The participant must have a shared licensing participant key.

Procedure

Step 1

Identify the shared licensing server IP address and shared secret:

```
license-server address address secret secret [port port]
```

Example:

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
```

If you changed the default port in the server configuration, set the port for the participant to match.

Step 2

(Optional) If you configured a backup server, enter the backup server address:

```
license-server backup address address
```

Examples

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

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

ciscoasa(config)# license-server backup address 10.1.1.2

Examples

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

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

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 13 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.

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base License</th>
<th>Security Plus License</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Licenses</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Botnet Traffic Filter</td>
<td>No support</td>
<td>No Support</td>
</tr>
<tr>
<td>Licenses</td>
<td>Base License</td>
<td>Security Plus License</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Firewall Conns, Concurrent</td>
<td>20,000</td>
<td>50,000</td>
</tr>
<tr>
<td>Carrier</td>
<td>No Support</td>
<td>No Support</td>
</tr>
<tr>
<td>Total TLS Proxy Sessions</td>
<td>160</td>
<td>160</td>
</tr>
</tbody>
</table>

**VPN Licenses**

<table>
<thead>
<tr>
<th>AnyConnect peers</th>
<th>Disabled</th>
<th>Optional AnyConnect Plus or Apex license: 50 maximum</th>
<th>Disabled</th>
<th>Optional AnyConnect Plus or Apex license: 50 maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other VPN Peers</td>
<td>10</td>
<td>50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total VPN Peers, combined all types</td>
<td>50</td>
<td>50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VPN Load Balancing</td>
<td>No support</td>
<td>No support</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**General Licenses**

<table>
<thead>
<tr>
<th>Encryption</th>
<th>Base (DES)</th>
<th>Opt. lic.: Strong (3DES/AES)</th>
<th>Base (DES)</th>
<th>Opt. lic.: Strong (3DES/AES)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failover</td>
<td>No support</td>
<td>Active/Standby</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Contexts</td>
<td>No support</td>
<td>No support</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clustering</td>
<td>No Support</td>
<td>No Support</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLANS, Maximum</td>
<td>5</td>
<td>30</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**ASA 5506H-X License Features**

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

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base License</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Licenses</td>
<td></td>
</tr>
</tbody>
</table>

---

ASA 5506H-X License Features

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

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base License</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall Licenses</td>
<td></td>
</tr>
<tr>
<td>Licenses</td>
<td>Base License</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Botnet Traffic Filter</td>
<td>No Support</td>
</tr>
<tr>
<td>Firewall Conns, Concurrent</td>
<td>50,000</td>
</tr>
<tr>
<td>Carrier</td>
<td>No Support</td>
</tr>
<tr>
<td>Total UC Proxy Sessions</td>
<td>160</td>
</tr>
<tr>
<td><strong>VPN Licenses</strong></td>
<td></td>
</tr>
<tr>
<td>AnyConnect Plus or Apex</td>
<td>50</td>
</tr>
<tr>
<td>(purchased separately),</td>
<td></td>
</tr>
<tr>
<td>maximum premium peers</td>
<td></td>
</tr>
<tr>
<td>Total VPN Peers, combined</td>
<td>50</td>
</tr>
<tr>
<td>all types</td>
<td></td>
</tr>
<tr>
<td>Other VPN Peers</td>
<td>50</td>
</tr>
<tr>
<td>VPN Load Balancing</td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>General Licenses</strong></td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td>Base (DES)</td>
</tr>
<tr>
<td></td>
<td>Opt. lic.: Strong (3DES/AES)</td>
</tr>
<tr>
<td>Failover</td>
<td>Active/Standby or</td>
</tr>
<tr>
<td></td>
<td>Active/Active</td>
</tr>
<tr>
<td>Security Contexts</td>
<td>No Support</td>
</tr>
<tr>
<td>Clustering</td>
<td>No Support</td>
</tr>
<tr>
<td>VLANs, Maximum</td>
<td>30</td>
</tr>
</tbody>
</table>

**ASA 5508-X License Features**

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

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base License</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Firewall Licenses</strong></td>
<td></td>
</tr>
<tr>
<td>Botnet Traffic Filter</td>
<td>No Support</td>
</tr>
</tbody>
</table>
### ASA 5512-X License Features

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

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base License</th>
<th>Security Plus License</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Firewall Licenses</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Botnet Traffic Filter</td>
<td>Disabled</td>
<td>Optional Time-based license: Available</td>
</tr>
<tr>
<td>Firewall Conns, Concurrent</td>
<td>100,000</td>
<td></td>
</tr>
<tr>
<td>Carrier</td>
<td>No Support</td>
<td></td>
</tr>
<tr>
<td>Total TLS Proxy Sessions</td>
<td>320</td>
<td></td>
</tr>
<tr>
<td><strong>VPN Licenses</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AnyConnect peers</td>
<td>Disabled</td>
<td>Optional AnyConnect Plus or Apex license: 100 maximum</td>
</tr>
<tr>
<td>Total VPN Peers, combined all types</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>Other VPN Peers</td>
<td>100</td>
<td></td>
</tr>
<tr>
<td>VPN Load Balancing</td>
<td>Enabled</td>
<td></td>
</tr>
<tr>
<td><strong>General Licenses</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td>Base (DES)</td>
<td>Opt. lic.: Strong (3DES/AES)</td>
</tr>
<tr>
<td>Failover</td>
<td>Active/Standby or Active/Active</td>
<td></td>
</tr>
<tr>
<td>Security Contexts</td>
<td>2</td>
<td>Optional licenses: 5</td>
</tr>
<tr>
<td>Clustering</td>
<td>No Support</td>
<td></td>
</tr>
<tr>
<td>VLANs, Maximum</td>
<td>50</td>
<td></td>
</tr>
</tbody>
</table>

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

**VPN Licenses**

<table>
<thead>
<tr>
<th>AnyConnect peers</th>
<th>Disabled</th>
<th>Optional AnyConnect Plus or Apex license: 250 maximum</th>
<th>Disabled</th>
<th>Optional AnyConnect Plus or Apex license: 250 maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other VPN Peers</td>
<td>250</td>
<td></td>
<td>250</td>
<td></td>
</tr>
<tr>
<td>Total VPN Peers, combined all types</td>
<td>250</td>
<td>250</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| VPN Load Balancing | No support | Enabled |

**General Licenses**

<table>
<thead>
<tr>
<th>Encryption</th>
<th>Base (DES)</th>
<th>Opt. lic.: Strong (3DES/AES)</th>
<th>Base (DES)</th>
<th>Opt. lic.: Strong (3DES/AES)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failover</td>
<td>No support</td>
<td>Active/Standby or Active/Active</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Contexts</td>
<td>No support</td>
<td>2</td>
<td>Optional licenses:</td>
<td>5</td>
</tr>
<tr>
<td>Clustering</td>
<td>No Support</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPS Module</td>
<td>Disabled</td>
<td>Optional license: Available</td>
<td>Disabled</td>
<td>Optional license: Available</td>
</tr>
<tr>
<td>VLANs, Maximum</td>
<td>50</td>
<td>100</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**ASA 5515-X License Features**

The following table shows the licensed features for the ASA 5515-X.
<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base License</th>
</tr>
</thead>
<tbody>
<tr>
<td>Botnet Traffic Filter</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>Optional Time-based license: Available</td>
</tr>
<tr>
<td>Firewall Conns, Concurrent</td>
<td>250,000</td>
</tr>
<tr>
<td>Carrier</td>
<td>No Support</td>
</tr>
<tr>
<td>Total TLS Proxy Sessions</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Optional licenses: 24 50 100 250 500</td>
</tr>
</tbody>
</table>

**VPN Licenses**

| AnyConnect peers     | Disabled  |
|                       | Optional AnyConnect Plus or Apex license: 250 maximum                       |
| Other VPN Peers       | 250       |
| Total VPN Peers, combined all types | 250 |
| VPN Load Balancing   | Enabled   |

**General Licenses**

| Encryption            | Base (DES)  |
|                       | Optional license: Strong (3DES/AES)                                        |
| Failover              | Active/Standby or Active/Active                                             |
| Security Contexts     | 2  |
|                       | Optional licenses: 5                                                        |
| Clustering            | 2  |
| IPS Module            | Disabled  |
|                       | Optional license: Available                                                 |
| VLANs, Maximum        | 100       |
ASA 5516-X License Features

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

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base License</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Firewall Licenses</strong></td>
<td></td>
</tr>
<tr>
<td>Botnet Traffic Filter</td>
<td>No Support</td>
</tr>
<tr>
<td>Firewall Conns, Concurrent</td>
<td>250,000</td>
</tr>
<tr>
<td>Carrier</td>
<td>No Support</td>
</tr>
<tr>
<td>Total TLS Proxy Sessions</td>
<td>1000</td>
</tr>
<tr>
<td><strong>VPN Licenses</strong></td>
<td></td>
</tr>
<tr>
<td>AnyConnect peers</td>
<td>Disabled</td>
</tr>
<tr>
<td>Other VPN Peers</td>
<td>300</td>
</tr>
<tr>
<td>Total VPN Peers, combined all types</td>
<td>300</td>
</tr>
<tr>
<td>VPN Load Balancing</td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>General Licenses</strong></td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td>Base (DES)</td>
</tr>
<tr>
<td>Failover</td>
<td>Active/Standby or Active/Active</td>
</tr>
<tr>
<td>Security Contexts</td>
<td>2 Optional licenses: 5</td>
</tr>
<tr>
<td>Clustering</td>
<td>2</td>
</tr>
<tr>
<td>VLANs, Maximum</td>
<td>150</td>
</tr>
</tbody>
</table>

ASA 5525-X License Features

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

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base License</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Firewall Licenses</strong></td>
<td></td>
</tr>
<tr>
<td>Licenses</td>
<td>Base License</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Botnet Traffic Filter</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>Optional Time-based license: Available</td>
</tr>
<tr>
<td>Firewall Conns, Concurrent</td>
<td>500,000</td>
</tr>
<tr>
<td>Carrier</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td>Optional license: Available</td>
</tr>
<tr>
<td>Total TLS Proxy Sessions</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>Optional licenses:</td>
</tr>
<tr>
<td></td>
<td>24 50 100 250 500 750 1000</td>
</tr>
</tbody>
</table>

VPN Licenses

| AnyConnect peers         | Disabled                                          |
|                          | Optional AnyConnect Plus or Apex license: 750 maximum |
| Other VPN Peers          | 750                                               |
| Total VPN Peers, combined all types | 750 |
| VPN Load Balancing       | Enabled                                           |

General Licenses

| Encryption               | Base (DES)                                        |
|                          | Optional license: Strong (3DES/AES)               |
| Failover                 | Active/Standby or Active/Active                   |
| Security Contexts        | 2                                                 |
|                          | Optional licenses:                                |
|                          | 5 10 20                                           |
| Clustering               | 2                                                 |
| IPS Module               | Disabled                                          |
|                          | Optional license: Available                       |
| VLANs, Maximum           | 200                                               |
ASA 5545-X License Features

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

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base License</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Firewall Licenses</strong></td>
<td></td>
</tr>
<tr>
<td>Botnet Traffic Filter</td>
<td>Disabled, Optional Time-based license: Available</td>
</tr>
<tr>
<td>Firewall Conns, Concurrent</td>
<td>750,000</td>
</tr>
<tr>
<td>Carrier</td>
<td>Disabled, Optional license: Available</td>
</tr>
<tr>
<td><strong>VPN Licenses</strong></td>
<td></td>
</tr>
<tr>
<td>AnyConnect peers</td>
<td>Disabled, Optional AnyConnect Plus or Apex license: 2500 maximum</td>
</tr>
<tr>
<td>Other VPN Peers</td>
<td>2500</td>
</tr>
<tr>
<td><strong>General Licenses</strong></td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td>Base (DES), Optional license: Strong (3DES/AES)</td>
</tr>
<tr>
<td>Failover</td>
<td>Active/Standby or Active/Active</td>
</tr>
<tr>
<td>Security Contexts</td>
<td>2, Optional licenses: 5, 10, 20, 50</td>
</tr>
<tr>
<td>Clustering</td>
<td>2</td>
</tr>
<tr>
<td>IPS Module</td>
<td>Disabled, Optional license: Available</td>
</tr>
</tbody>
</table>
## ASA 5555-X License Features

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

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base License</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Firewall Licenses</strong></td>
<td></td>
</tr>
<tr>
<td>Botnet Traffic Filter</td>
<td>Disabled</td>
</tr>
<tr>
<td>Firewall Conn, Concurrent</td>
<td>1,000,000</td>
</tr>
<tr>
<td>Carrier</td>
<td>Disabled</td>
</tr>
<tr>
<td>Total TLS Proxy Sessions</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>VPN Licenses</strong></td>
<td></td>
</tr>
<tr>
<td>AnyConnect peers</td>
<td>Disabled</td>
</tr>
<tr>
<td>Other VPN Peers</td>
<td>5000</td>
</tr>
<tr>
<td>Total VPN Peers, combined all types</td>
<td>5000</td>
</tr>
<tr>
<td>VPN Load Balancing</td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>General Licenses</strong></td>
<td></td>
</tr>
<tr>
<td>Encryption</td>
<td>Base (DES)</td>
</tr>
<tr>
<td>Failover</td>
<td>Active/Standby or Active/Active</td>
</tr>
</tbody>
</table>
### 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.

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base License</th>
<th>Firewall Licenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Contexts</td>
<td>Optional licenses: 5, 10, 20, 50, 100</td>
<td>Botnet Traffic Filter Disabled Optional Time-based license: Available</td>
</tr>
<tr>
<td>Clustering</td>
<td>2</td>
<td>Firewall Conns, Concurrent 1,000,000</td>
</tr>
<tr>
<td>IPS Module</td>
<td>Disabled</td>
<td>Carrier Disabled Optional license: Available</td>
</tr>
<tr>
<td>VLANs, Maximum</td>
<td>500</td>
<td>Total TLS Proxy Sessions 2 Optional licenses: 24, 50, 100, 250, 500, 750, 1000, 2000, 3000</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base and Security Plus Licenses</th>
<th>VPN Licenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN Peers</td>
<td>5000</td>
<td>AnyConnect peers Disabled Optional AnyConnect Plus or Apex license: 5000 maximum</td>
</tr>
<tr>
<td>Total VPN Peers, combined all types</td>
<td>5000</td>
<td></td>
</tr>
</tbody>
</table>
### 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. |

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base and Security Plus Licenses</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Base License</strong></td>
<td><strong>Security Plus License</strong></td>
</tr>
<tr>
<td>10 GE I/O</td>
<td>Disabled; fiber ifcs run at 1 GE</td>
</tr>
<tr>
<td>Encryption</td>
<td>Optional license: Strong (3DES/AES)</td>
</tr>
<tr>
<td>Failover</td>
<td>Active/Standby or Active/Active</td>
</tr>
<tr>
<td>Security Contexts</td>
<td>Optional licenses: 2 5 10 20 50 100</td>
</tr>
<tr>
<td>Clustering</td>
<td>Disabled</td>
</tr>
<tr>
<td>VLANs, Maximum</td>
<td>1024</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base and Security Plus Licenses</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Firewall Licenses</strong></td>
<td></td>
</tr>
<tr>
<td>Botnet Traffic Filter</td>
<td>Disabled</td>
</tr>
<tr>
<td>Firewall Conns, Concurrent</td>
<td>2,000,000</td>
</tr>
<tr>
<td>Carrier</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
### Licenses: Base and Security Plus Licenses

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base and Security Plus Licenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total TLS Proxy Sessions</td>
<td>2</td>
</tr>
<tr>
<td>Optional licenses:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>24</td>
</tr>
<tr>
<td></td>
<td>50</td>
</tr>
<tr>
<td></td>
<td>100</td>
</tr>
<tr>
<td></td>
<td>250</td>
</tr>
<tr>
<td></td>
<td>500</td>
</tr>
<tr>
<td></td>
<td>750</td>
</tr>
<tr>
<td></td>
<td>1000</td>
</tr>
<tr>
<td></td>
<td>2000</td>
</tr>
<tr>
<td></td>
<td>3000</td>
</tr>
<tr>
<td></td>
<td>5000</td>
</tr>
<tr>
<td></td>
<td>10,000</td>
</tr>
</tbody>
</table>

### VPN Licenses

<table>
<thead>
<tr>
<th>AnyConnect peers</th>
<th>Disabled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optional AnyConnect Plus or Apex license: 10,000 maximum</td>
<td></td>
</tr>
<tr>
<td>Other VPN Peers</td>
<td>10,000</td>
</tr>
<tr>
<td>Total VPN Peers, combined all types</td>
<td>10,000</td>
</tr>
</tbody>
</table>

### General Licenses

<table>
<thead>
<tr>
<th>I/O</th>
<th><strong>Base License</strong>: Disabled; fiber ifcs run at 1 GE</th>
<th><strong>Security Plus License</strong>: Enabled; fiber ifcs run at 10 GE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>Base (DES)</td>
<td>Optional license: Strong (3DES/AES)</td>
</tr>
<tr>
<td>Failover</td>
<td>Active/Standby or Active/Active</td>
<td></td>
</tr>
<tr>
<td>Security Contexts</td>
<td>2</td>
<td>Optional licenses: 5 10 20 50 100 250</td>
</tr>
<tr>
<td>Clustering</td>
<td>Disabled</td>
<td>Optional license: Available for 16 units</td>
</tr>
<tr>
<td>VLANs, Maximum</td>
<td>1024</td>
<td></td>
</tr>
</tbody>
</table>

### 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.
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.

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base License</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Firewall Licenses</strong></td>
<td></td>
</tr>
<tr>
<td>Botnet Traffic Filter</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td><em>Optional Time-based license: Available</em></td>
</tr>
<tr>
<td>Firewall Conns, Concurrent</td>
<td>5585-X with SSP-40: 4,000,000</td>
</tr>
<tr>
<td></td>
<td>5585-X with SSP-60: 10,000,000</td>
</tr>
<tr>
<td>Carrier</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td><em>Optional license: Available</em></td>
</tr>
<tr>
<td>Total TLS Proxy Sessions</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>*Optional licenses:</td>
</tr>
<tr>
<td></td>
<td>24 50 100 250 500 750 1000 2000 3000 5000 10,000</td>
</tr>
<tr>
<td><strong>VPN Licenses</strong></td>
<td></td>
</tr>
<tr>
<td>AnyConnect peers</td>
<td>Disabled</td>
</tr>
<tr>
<td></td>
<td><em>Optional AnyConnect Plus or Apex license: 10,000 maximum</em></td>
</tr>
<tr>
<td>Other VPN Peers</td>
<td>10,000</td>
</tr>
<tr>
<td>Total VPN Peers, combined all types</td>
<td>10,000</td>
</tr>
<tr>
<td>VPN Load Balancing</td>
<td>Enabled</td>
</tr>
<tr>
<td><strong>General Licenses</strong></td>
<td></td>
</tr>
<tr>
<td>10 GE I/O</td>
<td>Enabled; fiber ifcs run at 10 GE</td>
</tr>
<tr>
<td>Encryption</td>
<td>Base (DES)</td>
</tr>
<tr>
<td></td>
<td><em>Optional license: Strong (3DES/AES)</em></td>
</tr>
<tr>
<td>Failover</td>
<td>Active/Standby or Active/Active</td>
</tr>
<tr>
<td>Security Contexts</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>*Optional licenses:</td>
</tr>
<tr>
<td></td>
<td>5 10 20 50 100 250</td>
</tr>
</tbody>
</table>
### 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.

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base License</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clustered</td>
<td>Disabled</td>
</tr>
<tr>
<td>VLANs, Maximum</td>
<td>1024</td>
</tr>
</tbody>
</table>

### Firewall Licenses

<table>
<thead>
<tr>
<th>License Type</th>
<th>Base License</th>
</tr>
</thead>
<tbody>
<tr>
<td>Botnet Traffic Filter</td>
<td>Disabled</td>
</tr>
<tr>
<td>Firewall Conns, Concurrent</td>
<td>10,000,000</td>
</tr>
<tr>
<td>Carrier</td>
<td>Disabled</td>
</tr>
<tr>
<td>Total TLS Proxy Sessions</td>
<td>2</td>
</tr>
<tr>
<td>24</td>
<td>50</td>
</tr>
</tbody>
</table>

### VPN Licenses

<table>
<thead>
<tr>
<th>License Type</th>
<th>Base License</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnyConnect peers</td>
<td>Disabled</td>
</tr>
<tr>
<td>Other VPN Peers</td>
<td>10,000</td>
</tr>
<tr>
<td>Total VPN Peers, combined all types</td>
<td>10,000</td>
</tr>
</tbody>
</table>
### ISA 3000 License Features

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

<table>
<thead>
<tr>
<th>Licenses</th>
<th>Base License</th>
<th>Security Plus License</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Firewall Licenses</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Botnet Traffic Filter</td>
<td>No support</td>
<td>No Support</td>
</tr>
<tr>
<td>Firewall Conns, Concurrent</td>
<td>20,000</td>
<td>50,000</td>
</tr>
<tr>
<td>Carrier</td>
<td>No Support</td>
<td>No Support</td>
</tr>
<tr>
<td>Total TLS Proxy Sessions</td>
<td>160</td>
<td>160</td>
</tr>
<tr>
<td><strong>VPN Licenses</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AnyConnect peers</td>
<td>Disabled</td>
<td>Optional AnyConnect Plus or Apex license: 25 maximum</td>
</tr>
<tr>
<td></td>
<td>Disabled</td>
<td>Optional AnyConnect Plus or Apex license: 25 maximum</td>
</tr>
<tr>
<td>Other VPN Peers</td>
<td>10</td>
<td>50</td>
</tr>
<tr>
<td>Licenses</td>
<td>Base License</td>
<td>Security Plus License</td>
</tr>
<tr>
<td>----------</td>
<td>--------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>Total VPN Peers, combined all types</td>
<td>25</td>
<td>50</td>
</tr>
<tr>
<td>VPN Load Balancing</td>
<td>No support</td>
<td>No support</td>
</tr>
</tbody>
</table>

**General Licenses**

<table>
<thead>
<tr>
<th>Encryption</th>
<th>Base (DES)</th>
<th>Opt. lic.: Strong (3DES/AES)</th>
<th>Base (DES)</th>
<th>Opt. lic.: Strong (3DES/AES)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failover</td>
<td>No support</td>
<td></td>
<td>Active/Standby</td>
<td></td>
</tr>
<tr>
<td>Security Contexts</td>
<td>No support</td>
<td></td>
<td>No Support</td>
<td></td>
</tr>
<tr>
<td>Clustering</td>
<td>No Support</td>
<td></td>
<td>No Support</td>
<td></td>
</tr>
<tr>
<td>VLANs, Maximum</td>
<td>5</td>
<td></td>
<td>25</td>
<td></td>
</tr>
</tbody>
</table>

**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 13 for more information.

**Procedure**

Show the permanent license, active time-based licenses, and the running license, which is a combination of the permanent license and active time-based licenses:

```
show activation-key [detail]
```

The `detail` keyword also shows inactive time-based licenses.
For failover or cluster units, this command also shows the “cluster” license, which is the combined keys of all units.

Examples

Example 1: Standalone Unit Output for the show activation-key command

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

```plaintext
ciscoasa# show activation-key
Serial Number: JMX1232L11M
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Running Timebased Activation Key: 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2
Licensed features for this platform:
Maximum Physical Interfaces : Unlimited perpetual
Maximum VLANs : 150 perpetual
Inside Hosts : Unlimited perpetual
Failover : Active/Active perpetual
VPN-DES : Enabled perpetual
VPN-3DES-AES : Enabled perpetual
Security Contexts : 10 perpetual
GTP/GPRS : Enabled perpetual
AnyConnect Premium Peers : 2 perpetual
AnyConnect Essentials : Disabled perpetual
Other VPN Peers : 750 perpetual
Total VPN Peers : 750 perpetual
Shared License : Enabled perpetual
Shared AnyConnect Premium Peers : 12000 perpetual
AnyConnect for Mobile : Disabled perpetual
AnyConnect for Cisco VPN Phone : Disabled perpetual
Advanced Endpoint Assessment : Disabled perpetual
UC Phone Proxy Sessions : 12 62 days
Total UC Proxy Sessions : 12 62 days
Botnet Traffic Filter : Enabled 646 days
Intercompany Media Engine : Disabled perpetual
This platform has a Base license.
The flash permanent activation key is the SAME as the running permanent key.
Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter : Enabled 646 days
0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2
Total UC Proxy Sessions : 10 62 days
```

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

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

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

Licensed features for this platform:
- Maximum Physical Interfaces : 8 perpetual
- VLANs : 20 DMZ Unrestricted
- Dual ISPs : Enabled perpetual
- VLAN Trunk Ports : 8 perpetual
- Inside Hosts : Unlimited perpetual
- Failover : Active/Standby perpetual
- VPN-DES : Enabled perpetual
- VPN-3DES-AES : Enabled perpetual
- AnyConnect Premium Peers : 2 perpetual
- AnyConnect Essentials : Disabled perpetual
- Other VPN Peers : 25 perpetual
- Total VPN Peers : 25 perpetual
- AnyConnect for Mobile : Disabled perpetual
- AnyConnect for Cisco VPN Phone : Disabled perpetual
- Advanced Endpoint Assessment : Disabled perpetual
- UC Phone Proxy Sessions : 2 perpetual
- Total UC Proxy Sessions : 2 perpetual
- Botnet Traffic Filter : Enabled 39 days
- Intercompany Media Engine : Disabled perpetual

This platform has an ASA 5512-X Security Plus license.

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

Licensed features for this platform:
- Maximum Physical Interfaces : 8 perpetual
- VLANs : 20 DMZ Unrestricted
- Dual ISPs : Enabled perpetual
- VLAN Trunk Ports : 8 perpetual
- Inside Hosts : Unlimited perpetual
- Failover : Active/Standby perpetual
- VPN-DES : Enabled perpetual
- VPN-3DES-AES : Enabled perpetual
- AnyConnect Premium Peers : 25 perpetual
- AnyConnect for Mobile : Disabled perpetual
- AnyConnect for Cisco VPN Phone : Disabled perpetual
- Advanced Endpoint Assessment : Disabled perpetual
- UC Phone Proxy Sessions : 2 perpetual
- Total UC Proxy Sessions : 2 perpetual
- Botnet Traffic Filter : Enabled 39 days
- Intercompany Media Engine : Disabled perpetual

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

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

Inactive Timebased Activation Key:
0xyadayada3 0xyadayada3 0xyadayada3 0xyadayada3 0xyadayada3
AnyConnect Premium Peers : 25 7 days
Example 3: Primary Unit Output in a Failover Pair for show activation-key detail

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

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

ciscoasa# show activation-key detail

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

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

This platform has an ASA 5520 VPN Plus license.

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

This platform has an ASA 5520 VPN Plus license.

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

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

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

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

Inactive Timebased Activation Key:
0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3
Security Contexts : 2 7 days
AnyConnect Premium Peers : 100 7 days

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

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

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

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

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

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

This platform has an ASA 5520 VPN Plus license.

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

This platform has an ASA 5520 VPN Plus license.

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

Licensed features for this platform:
Maximum Physical Interfaces: Unlimited perpetual
Maximum VLANs: 150 perpetual
Inside Hosts: Unlimited perpetual
Failover: Active/Active perpetual
VPN-DES: Enabled perpetual
VPN-3DES-AES: Disabled perpetual
Security Contexts: 2 perpetual
Example 5: 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 ASA. 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).

```
ciscoasa# show activation-key

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

Example 6: 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 ASA. 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.

ciscoasa# 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.

Example 7: Output in a Cluster for show activation-key

ciscoasa# show activation-key
Serial Number: JMX1504LZTD
Running Permanent Activation Key: 0x4a3eea7b 0x54b9f61a 0x4e2a0683

Licensed features for this platform:
Maximum Physical Interfaces : Unlimited perpetual
Maximum VLANs : 100 perpetual
Inside Hosts : Unlimited perpetual
Failover : Active/Active perpetual
Encryption-DES : Enabled perpetual
Encryption-3DES-AES : Enabled perpetual
Security Contexts : 2 perpetual
GTP/GPRS : Disabled perpetual
AnyConnect Premium Peers : 2 perpetual
AnyConnect Essentials : Disabled perpetual
Other VPN Peers : 250 perpetual
Total VPN Peers : 250 perpetual
Shared License : Disabled perpetual
AnyConnect for Mobile : Disabled perpetual
AnyConnect for Cisco VPN Phone : Disabled perpetual
Advanced Endpoint Assessment : Disabled perpetual
UC Phone Proxy Sessions : 2 perpetual
Total UC Proxy Sessions : 2 perpetual
Botnet Traffic Filter : Disabled perpetual
Intercompany Media Engine : Disabled perpetual
Cluster : Enabled perpetual

This platform has an ASA 5585-X base license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces : Unlimited perpetual
Maximum VLANs : 100 perpetual
Inside Hosts : Unlimited perpetual
Failover : Active/Active perpetual
Encryption-DES : Enabled perpetual
Encryption-3DES-AES : Enabled perpetual
Security Contexts : 4 perpetual
GTP/GPRS : Disabled perpetual
AnyConnect Premium Peers : 4 perpetual
AnyConnect Essentials : Disabled perpetual
Other VPN Peers : 250 perpetual
Total VPN Peers : 250 perpetual
Shared License : Disabled perpetual
AnyConnect for Mobile : Disabled perpetual
AnyConnect for Cisco VPN Phone : Disabled perpetual
Advanced Endpoint Assessment : Disabled perpetual
UC Phone Proxy Sessions : 4 perpetual
Total UC Proxy Sessions : 4 perpetual
Botnet Traffic Filter : Disabled perpetual
Intercompany Media Engine : Disabled perpetual
Cluster : Enabled perpetual

This platform has an ASA 5585-X base license.

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

**Monitoring the Shared License**

To monitor the shared license, enter one of the following commands.

- **show shared license [detail | client [hostname] | backup]**

  Shows shared license statistics. Optional keywords are available only for the licensing server: the **detail** keyword shows statistics per participant. To limit the display to one participant, use the **client** keyword. The **backup** keyword shows information about the backup server.

  To clear the shared license statistics, enter the **clear shared license** command.
The following is sample output from the `show shared license` command on the license participant:

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

Shared license utilization:
SSLVPN:
  Total for network : 5000
  Available : 5000
  Utilized : 0
This device:
  Platform limit : 250
  Current usage : 0
  High usage : 0

Messages Tx/Rx/Error:
  Registration : 0 / 0 / 0
  Get : 0 / 0 / 0
  Release : 0 / 0 / 0
  Transfer : 0 / 0 / 0

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

ciscoasa> show shared license detail
Backup License Server Info:

Device ID : ABCD
Address : 10.1.1.2
Registered : NO
HA peer ID : EFGH
Registered : NO

Messages Tx/Rx/Error:
  Hello : 0 / 0 / 0
  Sync : 0 / 0 / 0
  Update : 0 / 0 / 0

Shared license utilization:
SSLVPN:
  Total for network : 500
  Available : 500
  Utilized : 0
This device:
  Platform limit : 250
  Current usage : 0
  High usage : 0

Messages Tx/Rx/Error:
  Registration : 0 / 0 / 0
  Get : 0 / 0 / 0
  Release : 0 / 0 / 0
  Transfer : 0 / 0 / 0

Client Info:

Hostname : 5540-A
Device ID : XXXXXXXXXXX
SSLVPN:
  Current usage : 0
  High : 0

Messages Tx/Rx/Error:
  Registration : 1 / 1 / 0
  Get : 0 / 0 / 0
• show activation-key
  Shows the licenses installed on the ASA. The show version command also shows license information.

• show vpn-sessiondb
  Shows license information about VPN sessions.

### History for PAK Licenses

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increased Connections and VLANs</td>
<td>7.0(5)</td>
<td>Increased the following limits:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ASA5510 Base license connections from 32000 to 5000; VLANs from 0 to 10.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ASA5510 Security Plus license connections from 64000 to 130000; VLANs from 10 to 25.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ASA5520 connections from 130000 to 280000; VLANs from 25 to 100.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ASA5540 connections from 280000 to 400000; VLANs from 100 to 200.</td>
</tr>
<tr>
<td>SSL VPN Licenses</td>
<td>7.1(1)</td>
<td>SSL VPN licenses were introduced.</td>
</tr>
<tr>
<td>Increased SSL VPN Licenses</td>
<td>7.2(1)</td>
<td>A 5000-user SSL VPN license was introduced for the ASA 5550 and above.</td>
</tr>
<tr>
<td>Increased interfaces for the Base license on the ASA 5510</td>
<td>7.2(2)</td>
<td>For the Base license on the ASA 5510, the maximum number of interfaces was increased from 3 plus a management interface to unlimited interfaces.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Platform Releases</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Increased VLANs</td>
<td>7.2(2)</td>
<td>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).</td>
</tr>
<tr>
<td>Gigabit Ethernet Support for the ASA 5510 Security Plus License</td>
<td>7.2(3)</td>
<td>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. <strong>Note</strong> The interface names remain Ethernet 0/0 and Ethernet 0/1. Use the <code>speed</code> command to change the speed on the interface and use the <code>show interface</code> command to see what speed is currently configured for each interface.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Platform Releases</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| 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 ASA. The ASA 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 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)            | 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>
<thead>
<tr>
<th>Feature Name</th>
<th>Platform Releases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Botnet Traffic Filter License</td>
<td>8.2(1)</td>
<td>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.</td>
</tr>
<tr>
<td>AnyConnect Essentials License</td>
<td>8.2(1)</td>
<td>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. 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 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. By default, the ASA uses the AnyConnect Essentials license, but you can disable it to use other licenses by using the <code>webvpn</code>, and then the <code>no anyconnect-essentials</code> command.</td>
</tr>
<tr>
<td>SSL VPN license changed to AnyConnect Premium SSL VPN Edition license</td>
<td>8.2(1)</td>
<td>The SSL VPN license name was changed to the AnyConnect Premium SSL VPN Edition license.</td>
</tr>
<tr>
<td>Shared Licenses for SSL VPN</td>
<td>8.2(1)</td>
<td>Shared licenses for SSL VPN were introduced. Multiple ASAs can share a pool of SSL VPN sessions on an as-needed basis.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Platform Releases</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Mobility Proxy application no longer requires Unified Communications Proxy license</td>
<td>8.2(2)</td>
<td>The Mobility Proxy no longer requires the UC Proxy license.</td>
</tr>
<tr>
<td>10 GE I/O license for the ASA 5585-X with SSP-20</td>
<td>8.2(3)</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> The ASA 5585-X is not supported in 8.3(x).</td>
</tr>
<tr>
<td>10 GE I/O license for the ASA 5585-X with SSP-10</td>
<td>8.2(4)</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note</strong> The ASA 5585-X is not supported in 8.3(x).</td>
</tr>
<tr>
<td>Non-identical failover licenses</td>
<td>8.3(1)</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>We modified the following commands: show activation-key and show version.</td>
</tr>
<tr>
<td>Stackable time-based licenses</td>
<td>8.3(1)</td>
<td>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 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.</td>
</tr>
<tr>
<td>Intercompany Media Engine License</td>
<td>8.3(1)</td>
<td>The IME license was introduced.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Platform Releases</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Multiple time-based licenses active at the same time</td>
<td>8.3(1)</td>
<td>You can now install multiple time-based licenses, and have one license per feature active at a time. We modified the following commands: <strong>show activation-key</strong> and <strong>show version</strong>.</td>
</tr>
<tr>
<td>Discrete activation and deactivation of time-based licenses.</td>
<td>8.3(1)</td>
<td>You can now activate or deactivate time-based licenses using a command. We modified the following commands: **activation-key [activate</td>
</tr>
<tr>
<td>AnyConnect Premium SSL VPN Edition license changed to AnyConnect Premium SSL VPN license</td>
<td>8.3(1)</td>
<td>The AnyConnect Premium SSL VPN Edition license name was changed to the AnyConnect Premium SSL VPN license.</td>
</tr>
<tr>
<td>No Payload Encryption image for export</td>
<td>8.3(2)</td>
<td>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. <strong>Note</strong> 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.</td>
</tr>
<tr>
<td>Increased contexts for the ASA 5550, 5580, and 5585-X</td>
<td>8.4(1)</td>
<td>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.</td>
</tr>
<tr>
<td>Increased VLANs for the ASA 5580 and 5585-X</td>
<td>8.4(1)</td>
<td>For the ASA 5580 and 5585-X, the maximum VLANs was increased from 250 to 1024.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Platform Releases</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Increased connections for the ASA 5580 and 5585-X</td>
<td>8.4(1)</td>
<td>We increased the firewall connection limits:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ASA 5580-20—1,000,000 to 2,000,000.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ASA 5580-40—2,000,000 to 4,000,000.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ASA 5585-X with SSP-10: 750,000 to 1,000,000.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ASA 5585-X with SSP-20: 1,000,000 to 2,000,000.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ASA 5585-X with SSP-40: 2,000,000 to 4,000,000.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ASA 5585-X with SSP-60: 2,000,000 to 10,000,000.</td>
</tr>
<tr>
<td>AnyConnect Premium SSL VPN license changed to AnyConnect Premium license</td>
<td>8.4(1)</td>
<td>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.”</td>
</tr>
<tr>
<td>Increased AnyConnect VPN sessions for the ASA 5580</td>
<td>8.4(1)</td>
<td>The AnyConnect VPN session limit was increased from 5,000 to 10,000.</td>
</tr>
<tr>
<td>Increased Other VPN sessions for the ASA 5580</td>
<td>8.4(1)</td>
<td>The other VPN session limit was increased from 5,000 to 10,000.</td>
</tr>
<tr>
<td>IPsec remote access VPN using IKEv2</td>
<td>8.4(1)</td>
<td>IPsec remote access VPN using IKEv2 was added to the AnyConnect Essentials and AnyConnect Premium licenses.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: The following limitation exists in our support for IKEv2 on the ASA: We currently do not support duplicate security associations.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Platform Releases</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>No Payload Encryption hardware for export</td>
<td>8.4(1)</td>
<td>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.</td>
</tr>
<tr>
<td>Dual SSPs for SSP-20 and SSP-40</td>
<td>8.4(2)</td>
<td>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.</td>
</tr>
<tr>
<td>IPS Module license for the ASA 5512-X through ASA 5555-X</td>
<td>8.6(1)</td>
<td>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.</td>
</tr>
<tr>
<td>Clustering license for the ASA 5580 and ASA 5585-X.</td>
<td>9.0(1)</td>
<td>A clustering license was added for the ASA 5580 and ASA 5585-X.</td>
</tr>
<tr>
<td>Support for VPN on the ASASM</td>
<td>9.0(1)</td>
<td>The ASASM now supports all VPN features.</td>
</tr>
<tr>
<td>Unified communications support on the ASASM</td>
<td>9.0(1)</td>
<td>The ASASM now supports all Unified Communications features.</td>
</tr>
<tr>
<td>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</td>
<td>9.0(1)</td>
<td>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.</td>
</tr>
<tr>
<td>Support for 16 cluster members for the ASA 5585-X</td>
<td>9.2(1)</td>
<td>The ASA 5585-X now supports 16-unit clusters.</td>
</tr>
<tr>
<td>Feature Name</td>
<td>Platform Releases</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>-------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ASAv4 and ASAv30 Standard and Premium model licenses introduced</td>
<td>9.2(1)</td>
<td>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.</td>
</tr>
</tbody>
</table>