



Licenses: Smart Software Licensing (ASAv, ASA on Firepower)

Cisco Smart Software Licensing lets you purchase and manage a pool of licenses centrally. Unlike product authorization key (PAK) licenses, smart licenses are not tied to a specific serial number. You can easily deploy or retire ASAs without having to manage each unit's license key. Smart Software Licensing also lets you see your license usage and needs at a glance.



Note

Smart Software Licensing is only supported on the ASAv and ASA Firepower chassis. Other models use PAK licenses. See [About PAK Licenses](#).

For more information about Smart Licensing features and behaviors per platform, see [Smart Enabled Product Families](#).

- [About Smart Software Licensing, on page 1](#)
- [Prerequisites for Smart Software Licensing, on page 6](#)
- [Guidelines for Smart Software Licensing, on page 8](#)
- [Defaults for Smart Software Licensing, on page 8](#)
- [ASAv: Configure Smart Software Licensing, on page 9](#)
- [Firepower 4100/9300: Configure Smart Software Licensing, on page 13](#)
- [Licenses Per Model, on page 15](#)
- [Monitoring Smart Software Licensing, on page 17](#)
- [Smart Software Manager Communication, on page 20](#)
- [History for Smart Software Licensing, on page 22](#)

About Smart Software Licensing

This section describes how Smart Software Licensing works.

Smart Software Licensing for the ASA on the Firepower 9300 Chassis

For the ASA on the Firepower 9300 chassis, Smart Software Licensing configuration is split between the Firepower 9300 chassis supervisor and the ASA.

- Firepower 9300 chassis—Configure all Smart Software Licensing infrastructure on the chassis, including parameters for communicating with the License Authority. The Firepower 9300 chassis itself does not require any licenses to operate.
- ASA Application—Configure all license entitlements in the ASA.

Smart Software Manager and Accounts

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>

The Smart Software Manager lets you create a master account for your organization.



Note

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

By default, your licenses are assigned to the *Default Virtual Account* under your master account. As the account administrator, you can optionally create additional virtual accounts; for example, you can create accounts for regions, departments, or subsidiaries. Multiple virtual accounts let you more easily manage large numbers of licenses and devices.

Licenses and Devices Managed per Virtual Account

Licenses and devices are managed per virtual account: only that virtual account's devices can use the licenses assigned to the account. If you need additional licenses, you can transfer an unused license from another virtual account. You can also transfer devices between virtual accounts.

For the ASA on the Firepower 9300 chassis—Only the chassis registers as a device, while the ASA applications in the chassis request their own licenses. For example, for a Firepower 9300 chassis with 3 security modules, the chassis counts as one device, but the modules use 3 separate licenses.

Evaluation License

ASAv

The ASAv does not support an evaluation mode. Before the ASAv registers with the Licensing Authority, it operates in a severely rate-limited state.

Firepower 9300 Chassis

The Firepower 9300 chassis supports two types of evaluation license:

- Chassis-level evaluation mode—Before the Firepower 9300 chassis registers with the Licensing Authority, it operates for 90 days (total usage) in evaluation mode. The ASA cannot request specific entitlements in this mode; only default entitlements are enabled. When this period ends, the Firepower 9300 chassis becomes out-of-compliance.
- Entitlement-based evaluation mode—After the Firepower 9300 chassis registers with the Licensing Authority, you can obtain time-based evaluation licenses that can be assigned to the ASA. In the ASA,

you request entitlements as usual. When the time-based license expires, you need to either renew the time-based license or obtain a permanent license.



Note You cannot receive an evaluation license for Strong Encryption (3DES/AES); you must register with the License Authority and obtain a permanent license.

About Licenses by Type

The following sections include additional information about licenses by type.

AnyConnect Plus, AnyConnect Apex, And VPN Only Licenses

The AnyConnect Plus, AnyConnect Apex, or VPN Only 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. Devices that use Smart Licensing do not require any AnyConnect license to be physically applied to the actual platform. The same licenses must still be purchased, and you must still link the Contract number to your Cisco.com ID for SW Center access and technical support. For more information, see:

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

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.

Encryption License

Strong Encryption: ASAv

Strong Encryption (3DES/AES) is available for management connections before you connect to the License Authority, so you can launch ASDM and connect to the License Authority. For through-the-box traffic,

throughput is severely limited until you connect to the License Authority and obtain the Strong Encryption license.

If the ASAv becomes out-of-compliance later, then the ASAv reverts to the rate-limited state.

Strong Encryption: Firepower 9300 Chassis

You must manually request the Strong Encryption license in the ASA configuration using the CLI because ASDM requires 3DES. If the ASA becomes out-of-compliance, neither management traffic nor through-traffic requiring this license will be allowed.

DES: All Models

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.

Total UC Proxy Sessions

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

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

Some applications might use multiple sessions for a connection. For example, if you configure a phone with a primary and backup Cisco Unified Communications Manager, there are 2 TLS proxy connections.

You independently set the TLS proxy limit using the **tls-proxy maximum-sessions** command or in ASDM, using the **Configuration > Firewall > Unified Communications > TLS Proxy** pane. To view the limits of your model, enter the **tls-proxy maximum-sessions ?** command. When you apply a TLS proxy license that is higher than the default TLS proxy limit, the ASA automatically sets the TLS proxy limit to match the license. The TLS proxy limit takes precedence over the license limit; if you set the TLS proxy limit to be less than the license, then you cannot use all of the sessions in your license.



Note

For license part numbers ending in “K8” (for example, licenses under 250 users), TLS proxy sessions are limited to 1000. For license part numbers ending in “K9” (for example, licenses 250 users or larger), the TLS proxy limit depends on the configuration, up to the model limit. K8 and K9 refer to whether the license is restricted for export: K8 is unrestricted, and K9 is restricted.

If you clear the configuration (using the **clear configure all** command, for example), then the TLS proxy limit is set to the default for your model; if this default is lower than the license limit, then you see an error message to use the **tls-proxy maximum-sessions** command to raise the limit again (in ASDM, use the **TLS Proxy** pane). If you use failover and enter the **write standby** command or in ASDM, use **File > Save Running Configuration to Standby Unit** on the primary unit to force a configuration synchronization, the **clear configure all** command is generated on the secondary unit automatically, so you may see the warning message on the secondary unit. Because the configuration synchronization restores the TLS proxy limit set on the primary unit, you can ignore the warning.

You might also use SRTP encryption sessions for your connections:

- For K8 licenses, SRTP sessions are limited to 250.
- For K9 licenses, there is no limit.



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

VLANs, Maximum

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

Failover or ASA Cluster Licenses

Failover Licenses for the ASAv

The standby unit requires the same model license as the primary unit.

Failover Licenses for the ASA on the Firepower 9300 Chassis

Each Firepower 9300 chassis must be registered with the License Authority or satellite server. There is no extra cost for the secondary unit. For permanent license reservation, you must purchase separate licenses for each chassis.

Each ASA must have the same encryption license. For regular Smart Software Manager users, the Strong Encryption license is automatically enabled for qualified customers when you apply the registration token on the Firepower 9300 chassis. For older Cisco Smart Software Manager satellite deployments, see below.

In the ASA licensing configuration, other licenses do not need to match on each failover unit, and you can configure licensing separately on each unit. Each unit requests its own licenses from the server. The licenses requested by both units are aggregated into a single failover license that is shared by the failover pair, and this aggregated license is cached on the standby unit to be used if it becomes the active unit in the future. Typically, you only need to configure licenses on the primary unit.

Each license type is managed as follows:

- **Standard**—Each unit includes the Standard license by default, so for a failover pair, 2 Standard licenses are requested from the server.
- **Context**—Each unit can request its own Context license. However, the Standard license includes 10 contexts by default and is present on both units. The value from each unit's Standard license plus the value of any optional Context licenses on both units are combined up to the platform limit. For example:
 - The Standard license includes 10 contexts; for 2 units, these licenses add up to 20 contexts. You configure a 250-Context license on the primary unit in an Active/Standby pair. Therefore, the aggregated failover license includes 270 contexts. However, because the platform limit for one unit is 250, the combined license allows a maximum of 250 contexts only. In this case, you should only configure the primary Context license to be 230 contexts.

- The Standard license includes 10 contexts; for 2 units, these licenses add up to 20 contexts. You configure a 10-Context license on the primary unit in an Active/Active pair, and a 10-Context license on the secondary unit. Therefore, the aggregated failover license includes 40 contexts. One unit can use 22 contexts and the other unit can use 18 contexts, for example, for a total of 40. Because the platform limit for one unit is 250, the combined license allows a maximum of 250 contexts; the 40 contexts are within the limit.
- Carrier—Only one unit needs to request this license, and both units can use it.
- Strong Encryption (3DES) (for a pre-2.3.0 Cisco Smart Software Manager satellite deployment only)—Each unit must request its own license from the server; unlike the other license configurations, this configuration is replicated to the standby unit. For Smart Software Manager satellite deployments, to use ASDM and other strong encryption features, after you deploy the cluster you must enable the Strong Encryption (3DES) license on the primary unit using the ASA CLI. The Strong Encryption (3DES) license is not available with any type of evaluation license.

ASA Cluster Licenses for the ASA on the Firepower 9300 Chassis

The clustering feature itself does not require any licenses. To use Strong Encryption and other optional licenses, you can only request licenses on the control unit; the licenses are aggregated with the data units. If you have licenses on multiple units, they combine into a single running ASA cluster license. License configuration completed on the control unit is not replicated to the data units. You can only configure separate license entitlements on data units if you disable clustering, configure the licensing, and then re-enable clustering.



Note

To use ASDM and other strong encryption features, after you deploy the cluster you must enable the Strong Encryption (3DES) license on the control unit using the ASA CLI. This license is inherited by the data units; you do not need to configure this license separately on each unit. The Strong Encryption (3DES) license is not available with any type of evaluation license.



Note

If the control unit fails, and does not rejoin within 30 days (the licensing grace period), then the inherited licenses disappear. You must then manually configure the missing licenses on the new control unit.

Prerequisites for Smart Software Licensing

Regular and Satellite Smart License Prerequisites

ASAv

- Ensure internet access, or HTTP proxy access from the device.
- Configure a DNS server so the device can resolve the name of the License Authority.
- Set the clock for the device.
- Create a master account on the Cisco Smart Software Manager:

<https://software.cisco.com/#module/SmartLicensing>

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

Firepower 4100/9300

Configure the Smart Software Licensing infrastructure on the Firepower 9300 chassis before you configure the ASA licensing entitlements.

Permanent License Reservation Prerequisites

- Create a master account on the Cisco Smart Software Manager:

<https://software.cisco.com/#module/SmartLicensing>

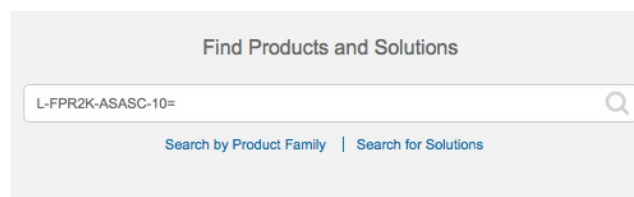
If you do not yet have an account, click the link to [set up a new account](#). The Smart Software Manager lets you create a master account for your organization. Even though the ASA does need internet connectivity to the Smart Licensing server for permanent license reservation, the Smart Software Manager is used to manage your permanent licenses.

- Obtain support for permanent license reservation from the licensing team. You must provide a justification for using permanent license reservation. If your account is not approved, then you cannot purchase and apply permanent licenses.
- Purchase special permanent licenses (see [License PIDs, on page 7](#)). If you do not have the correct license in your account, then when you try to reserve a license on the ASA, you will see an error message similar to: "The licenses cannot be reserved because the Virtual Account does not contain a sufficient surplus of the following perpetual licenses: 1 - Firepower 4100 ASA PERM UNIV(perpetual)."
- The permanent license includes all available features, including the Strong Encryption (3DES/AES) license if your account qualifies. AnyConnect client capabilities are also enabled to the platform maximum, contingent on your purchase of an AnyConnect license that enables the right to use AnyConnect (see [AnyConnect Plus, AnyConnect Apex, And VPN Only Licenses, on page 3](#)).

License PIDs

When you bought your device from Cisco or a reseller, your licenses should have been linked to your Smart Software License account. However, if you need to add licenses yourself, use the **Find Products and Solutions** search field on the [Cisco Commerce Workspace](#). Search for the following license Product IDs (PIDs).

Figure 1: License Search



Find Products and Solutions

L-FPR2K-ASASC-10=

Search by Product Family | Search for Solutions

ASAv PIDs

ASAv PIDs:

- ASAv5—L-ASAV5S-K9=
- ASAv10—L-ASAV10S-K9=
- ASAv30—L-ASAV30S-K9=
- ASAv50—L-ASAV50S-K9=

Firepower 9300 PIDs

Firepower 9300 PIDs:

- Standard license—L-F9K-ASA=. The Standard license is free, but you still need to add it to your Smart Software Licensing account.
- 10 context license—L-F9K-ASA-SC-10=. Context licenses are additive; buy multiple licenses to meet your needs.
- Carrier (Diameter, GTP/GPRS, SCTP)—L-F9K-ASA-CAR=
- Strong Encryption (3DES/AES) license—L-F9K-ASA-ENCR-K9=. This license is free. Although this license is not generally required (for example, ASAs that use older Satellite Server versions (pre-2.3.0) require this license), you should still add it to your account for tracking purposes.

Guidelines for Smart Software Licensing

- Only Smart Software Licensing is supported. For older software on the ASAv, if you upgrade an existing PAK-licensed ASAv, then the previously installed activation key will be ignored, but retained on the device. If you downgrade the ASAv, the activation key will be reinstated.
- (Firepower 9300 ASA security module) To use ASDM and other strong encryption features such as VPN, after you deploy the ASA you must enable the Strong Encryption (3DES) license on the control unit using the ASA CLI. For clustering, configure the license on the control unit. This license is inherited by the data units; you do not need to configure this license separately on each unit.
- Because the Cisco Transport Gateway uses a certificate with a non-compliant country code, you cannot use HTTPS when using the ASA in conjunction with that product. You must use HTTP with Cisco Transport Gateway.

Defaults for Smart Software Licensing

ASAv

- The ASAv default configuration includes a Smart Call Home profile called “License” that specifies the URL for the Licensing Authority.

```
call-home
  profile License
    destination address http
    https://tools.cisco.com/its/service/oddce/services/DDCEService
```


- When you deploy the ASAv, you set the feature tier and throughput level. Only the standard level is available at this time.

```
license smart
  feature tier standard
  throughput level {100M | 1G | 2G}
```

- Also during deployment, you can optionally configure an HTTP proxy.

```
call-home
  http-proxy ip_address port port
```

ASA on the Firepower 9300 Chassis

There is no default configuration. You must manually enable the standard license tier and other optional licenses.

ASAv: Configure Smart Software Licensing

This section describes how to configure Smart Software Licensing for the ASAv.

Procedure

[ASAv: Configure Smart Software Licensing, on page 9.](#)

ASAv: Configure Smart Software Licensing

When you deploy the ASAv, you can pre-configure the device and include a registration token so it registers with the License Authority and enables Smart Software Licensing. If you need to change your HTTP proxy server, license entitlement, or register the ASAv (for example, if you did not include the ID token in the Day0 configuration), perform this task.



Note

You may have pre-configured the HTTP proxy and license entitlements when you deployed your ASAv. You may also have included the registration token with your Day0 configuration when you deployed the ASAv; if so, you do not need to re-register using this procedure.

Procedure

Step 1

In the Smart Software Manager ([Cisco Smart Software Manager](#)), request and copy a registration token for the virtual account to which you want to add this device.

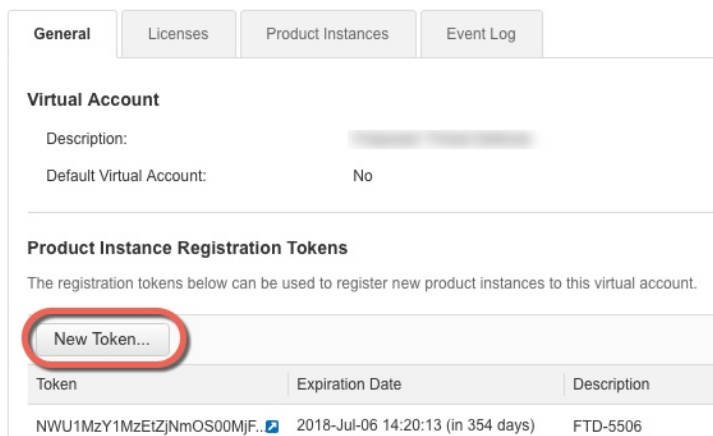
- a) Click **Inventory**.

Figure 2: Inventory



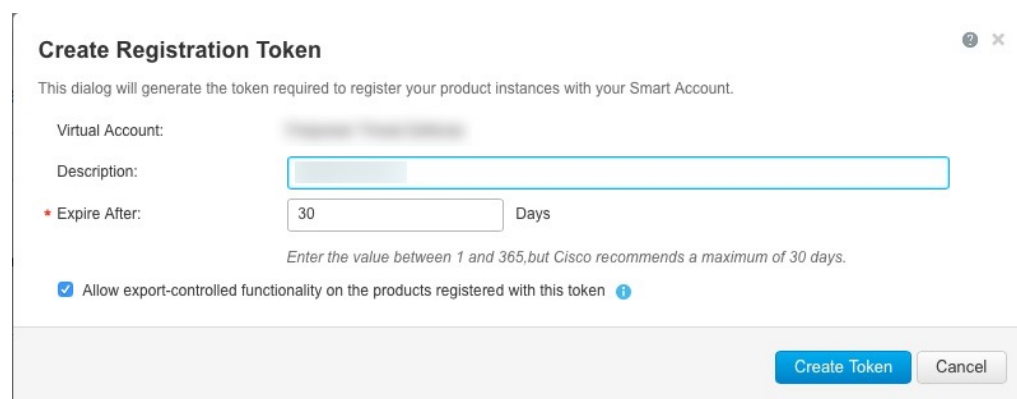
- b) On the **General** tab, click **New Token**.

Figure 3: New Token



- c) On the **Create Registration Token** dialog box enter the following settings, and then click **Create Token**:
- **Description**
 - **Expire After**—Cisco recommends 30 days.
 - **Allow export-controlled functionality on the products registered with this token**—Enables the export-compliance flag.

Figure 4: Create Registration Token



The token is added to your inventory.

- d) Click the arrow icon to the right of the token to open the **Token** dialog box so you can copy the token ID to your clipboard. Keep this token ready for later in the procedure when you need to register the ASA.

Figure 5: View Token

General | Licenses | Product Instances | Event Log

Virtual Account

Description: ASA FP 2110 1

Default Virtual Account: No

Product Instance Registration Tokens

The registration tokens below can be used to register new product instances to this virtual account.

New Token...

Token	Expiration Date	Description	Export-Controlled	Created By	Actions
MjM3ZjJhYThtZGQ4OS00Yjk2LT...	2017-Aug-16 19:41:53 (in 30 days)	ASA FP 2110 1	Allowed	...	Actions

Figure 6: Copy Token

Token

MjM3ZjJhYThtZGQ4OS00Yjk2LTgzMGitMThtMTUyYjkyNmVhLTE1MDI5MTI1%0AMTMxMzh8YzdQdmgzMjA2VmFjN2dYQjI5QWRhOEpscDU4cWl5NFNWRUtsa2wz%0AMTd0STN%3D%0A

Press ctrl + c to copy selected text to clipboard.

MjM3ZjJhYThtZGQ4OS00Yjk2LT... 2017-Aug-16 19:41:53

Step 2 (Optional) On the ASAv, specify the HTTP Proxy URL:

call-home

http-proxy ip_address port port

If your network uses an HTTP proxy for internet access, you must configure the proxy address for Smart Software Licensing. This proxy is also used for Smart Call Home in general.

Example:

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

Step 3 Configure the license entitlements.

- a) Enter license smart configuration mode:

license smart

Example:

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

- b) Set the feature tier:

feature tier standard

Only the standard tier is available.

- c) Set the throughput level:

throughput level {100M | 1G | 2G}

Example:

```
ciscoasa(config-smart-lic)# throughput level 2G
```

- a) Exit license smart mode to apply your changes:

exit

Your changes do not take effect until you exit the license smart configuration mode, either by explicitly exiting the mode (**exit** or **end**) or by entering any command that takes you to a different mode.

Example:

```
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

Step 4 Register the ASAv with the License Authority.

When you register the ASAv, the License Authority issues an ID certificate for communication between the ASAv and the License Authority. It also assigns the ASAv to the appropriate virtual account. Normally, this procedure is a one-time instance. However, you might need to later re-register the ASAv if the ID certificate expires because of a communication problem, for example.

- a) Enter the registration token on the ASAv:

license smart register idtoken *id_token* [force]

Example:

Use the **force** keyword to register an ASAv that is already registered, but that might be out of sync with the License Authority. For example, use **force** if the ASAv was accidentally removed from the Smart Software Manager.

The ASAv attempts to register with the License Authority and request authorization for the configured license entitlements.

Example:

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMj00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAY%0AODQzNz18NXk2bzV3SDE0ZkgwQk
dYRmZlNTNCGlvrnBHUFpjcm02WTB4TU4w%0Ac2NmMD0%3D%0A
```

(Optional) Deregister the ASAv

Deregistering the ASAv removes the ASAv from your account. All license entitlements and certificates on the ASAv are removed. You might want to deregister to free up a license for a new ASAv. Alternatively, you can remove the ASAv from the Smart Software Manager.

Procedure

Deregister the ASAv:

license smart deregister

The ASAv then reloads.

(Optional) Renew the ASAv ID Certificate or License Entitlement

By default, the ID certificate is automatically renewed every 6 months, and the license entitlement is renewed every 30 days. You might want to manually renew the registration for either of these items if you have a limited window for Internet access, or if you make any licensing changes in the Smart Software Manager, for example.

Procedure

Step 1 Renew the ID certificate:

license smart renew id

Step 2 Renew the license entitlement:

license smart renew auth

Firepower 4100/9300: Configure Smart Software Licensing

This procedure applies for a chassis using the License Authority, Satellite server users; see the FXOS configuration guide to configure your method as a prerequisite.



Note The Strong Encryption (3DES/AES) license is not enabled by default so you cannot use ASDM to configure your ASA until you request the Strong Encryption license using the ASA CLI. Other strong encryption features are also not available until you do so.

Before you begin

For an ASA cluster, you need to access the control unit for configuration. Check the Firepower Chassis Manager to see which unit is the control unit. You can also check from the ASA CLI, as shown in this procedure.

Procedure

Step 1 Connect to the Firepower 9300 chassis CLI (console or SSH), and then session to the ASA:

connect module *slot* console

connect asa

Example:

```
Firepower> connect module 1 console
Firepower-module1> connect asa

asa>
```

The next time you connect to the ASA console, you go directly to the ASA; you do not need to enter **connect asa** again.

For an ASA cluster, you only need to access the control unit for license configuration and other configuration. Typically, the control unit is in slot 1, so you should connect to that module first.

Step 2 At the ASA CLI, enter global configuration mode. By default, the enable password is blank.

enable

configure terminal

Example:

```
asa> enable
Password:
asa# configure terminal
asa(config)#
```

Step 3 If required, for an ASA cluster confirm that this unit is the control unit:

show cluster info

Example:

```
asa(config)# show cluster info
Cluster stbu: On
  This is "unit-1-1" in state SLAVE
    ID : 0
    Version : 9.5(2)
    Serial No.: P3000000025
    CCL IP : 127.2.1.1
    CCL MAC : 000b.fcf8.c192
    Last join : 17:08:59 UTC Sep 26 2015
    Last leave: N/A
Other members in the cluster:
  Unit "unit-1-2" in state SLAVE
    ID : 1
    Version : 9.5(2)
    Serial No.: P3000000001
    CCL IP : 127.2.1.2
    CCL MAC : 000b.fcf8.c162
    Last join : 19:13:11 UTC Sep 23 2015
    Last leave: N/A
  Unit "unit-1-3" in state MASTER
    ID : 2
    Version : 9.5(2)
    Serial No.: JAB0815R0JY
```

```
CCL IP : 127.2.1.3
CCL MAC : 000f.f775.541e
Last join : 19:13:20 UTC Sep 23 2015
Last leave: N/A
```

If a different unit is the control unit, exit the connection and connect to the correct unit. See below for information about exiting the connection.

Step 4 Enter license smart configuration mode:

license smart

Example:

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

Step 5 Set the feature tier:

feature tier standard

Only the standard tier is available. A tier license is a prerequisite for adding other feature licenses. You must have sufficient tier licenses in your account. Otherwise, you cannot configure any other feature licenses or any features that require licenses.

Step 6 Request one or more of the following features:

- Mobile SP (GTP/GPRS)

feature mobile-sp

- Security Contexts

feature context <1-248>

- Strong Encryption (3DES/AES)

feature strong-encryption

Example:

```
ciscoasa(config-smart-lic)# feature strong-encryption
ciscoasa(config-smart-lic)# feature context 50
```

Step 7 To exit the ASA console, enter ~ at the prompt to exit to the Telnet application. Enter **quit** to exit back to the supervisor CLI.

Licenses Per Model

This section lists the license entitlements available for the ASAv and Firepower 9300 chassis ASA security module.

ASAv

The following table shows the licensed features for the ASAv series.

Licenses	Standard License	
Firewall Licenses		
Botnet Traffic Filter	Enabled	
Firewall Conns, Concurrent	ASAv5: 100,000 ASAv10: 100,000 ASAv30: 500,000	
GTP/GPRS	Enabled	
Total UC Proxy Sessions	ASAv5: 500 ASAv10: 500 ASAv30: 1000	
VPN Licenses		
AnyConnect peers	Unlicensed	Optional AnyConnect Plus or Apex license, Maximums: ASAv5: 50 ASAv10: 250 ASAv30: 750
Other VPN Peers	ASAv5: 250 ASAv10: 250 ASAv30: 1000	
Total VPN Peers, combined all types	ASAv5: 250 ASAv10: 250 ASAv30: 1000	
General Licenses		
Throughput Level	ASAv5: 1 Gbps ASAv10: 1 Gbps ASAv30: 2 Gbps	
Encryption	Strong (3DES/AES)	
Failover	Active/Standby	
Security Contexts	No support	

Licenses	Standard License
Clustering	No support
VLANs, Maximum	ASAv5: 50 ASAv10: 50 ASAv30: 200
RAM, vCPUs	ASAv5: 2 GB, 1 vCPU ASAv10: 2 GB, 1 vCPU ASAv30: 8 GB, 4 vCPUs

Firepower 9300 ASA Application

The following table shows the licensed features for the Firepower 9300 ASA application.

Licenses	Standard License	
Firewall Licenses		
Botnet Traffic Filter	No Support.	
Firewall Conns, Concurrent	Firepower 9300 SM-36: 60,000,000, up to 70,000,000 for a chassis with 3 modules Firepower 9300 SM-24: 55,000,000, up to 70,000,000 for a chassis with 3 modules	
GTP/GPRS	Disabled	Optional License: Mobile SP
Total UC Proxy Sessions	15,000	
VPN is not supported with Firepower Chassis Manager 1.1.2 and earlier.		
General Licenses		
Encryption	Base (DES) or Strong (3DES/AES)	
Security Contexts	10	Optional License: Maximum of 250, in increments of 10
Clustering	Enabled	
VLANs, Maximum	1024	

Monitoring Smart Software Licensing

You can monitor the license features, status, and certificate, as well as enable debug messages.

Viewing Your Current License

See the following commands for viewing your license:

- **show license features**

The following example shows an ASAv with only a base license (no current license entitlement):

```
Serial Number: 9AAHGx8514R

ASAv Platform License State: Unlicensed
No active entitlement: no feature tier configured

Licensed features for this platform:
Maximum Physical Interfaces      : 10           perpetual
Maximum VLANs                   : 50           perpetual
Inside Hosts                    : Unlimited     perpetual
Failover                        : Active/Standby perpetual
Encryption-DES                  : Enabled      perpetual
Encryption-3DES-AES            : Enabled      perpetual
Security Contexts               : 0            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           : Enabled      perpetual
Intercompany Media Engine       : Disabled     perpetual
Cluster                        : Disabled     perpetual
```

- **show license entitlement**

Displays detailed information about each entitlement in use, its handle (i.e. integer id), its count, tag, enforcement mode (e.g. in compliance, out of compliance, etc.), version and time at which the entitlement was requested.

Viewing Smart License Status

See the following commands for viewing license status:

- **show license all**

Displays the state of Smart Software Licensing, Smart Agent version, UDI information, Smart Agent state, global compliance status, the entitlements status, licensing certificate information, and scheduled Smart Agent tasks.

The following example shows an ASAv license:

```
ciscoasa# show license all

Cisco Smart Licensing Agent, Version 1.1.1

Smart Licensing Enabled: Yes
```

```

UDI:
PID:ASAv,SN:9AC5KH5H9FW

Compliance Status: In Compliance

Assigned License Pool: ASAv Internal Users

Grace period: Not in use

Entitlement:
  Tag: regid.2014-08.com.cisco.ASAv-STD-1G,1.0_4fd3bdbd-29ae-4cce-ad82-45ad3db1070c,
  Version: 1.0, Enforce Mode: Authorized
  Requested Time: Sep 15 13:08:23 2015 UTC, Requested Count: 1
  Vendor String: (null)

Smart Licensing State: authorized (4)

Licensing Certificates:
  ID Cert Info:
    Start Date: Sep 15 12:59:29 2015 UTC. Expiry Date: Sep 14 12:59:29 2016 UTC
    Serial Number: 214929
    Version: 3
    Subject/SN: 16cab27f-a239-4d2d-a8db-d81dc48ec6bb
    Common Name: 55d246e3160a5dab39ec218f0b6b00f03422ef0d::1,2
  Signing Cert Info:
    Start Date: Jun 14 20:18:52 2013 UTC. Expiry Date: Apr 24 21:55:42 2033 UTC
    Serial Number: 3
    Version: 3

Upcoming Scheduled Jobs:
  Certificate Renewal: Mar 13 13:03:06 2016 UTC (172 days, 11 hours, 24 minutes, 8
seconds remaining)
  Certificate Expiration: Sep 14 13:00:03 2016 UTC (357 days, 11 hours, 21 minutes,
5 seconds remaining)
  Authorization Renewal: Oct 22 18:58:18 2015 UTC (29 days, 17 hours, 19 minutes, 20
seconds remaining)
  Authorization Expiration: Dec 21 18:55:28 2015 UTC (89 days, 17 hours, 16 minutes,
30 seconds remaining)
  Daily Job: Sep 23 13:09:27 2015 UTC (11 hours, 30 minutes, 29 seconds remaining)

HA Info:    HA not available
HA Sudi: Not Available

```

- **show license registration**

Displays the current Smart License registration status.

- **show license pool**

Displays the entitlement pool to which this device is assigned.

Displaying ID Certificate Information

See the following command to view the license ID certificate:

- **show license cert**

Displays the ID certificate content, date issued, and the date it expires.

Debugging Smart Software Licensing

See the following commands for debugging clustering:

- **debug license agent** {**error** | **trace** | **debug** | **all**}

Turns on debugging from the Smart Agent.

- **debug license level**

Turns on various levels of Smart Software Licensing Manager debugs.

Smart Software Manager Communication

This section describes how your device communicates with the Smart Software Manager.

Device Registration and Tokens

For each virtual account, you can create a registration token. This token is valid for 30 days by default. Enter this token ID plus entitlement levels when you deploy each device, or when you register an existing device. You can create a new token if an existing token is expired.



Note

Firepower 9300 chassis—Device registration is configured in the chassis, not on the ASAv logical device.

At startup after deployment, or after you manually configure these parameters on an existing device, the device registers with the Cisco License Authority. When the device registers with the token, the License Authority issues an ID certificate for communication between the device and the License Authority. This certificate is valid for 1 year, although it will be renewed every 6 months.

Periodic Communication with the License Authority

The device communicates with the License Authority every 30 days. If you make changes in the Smart Software Manager, you can refresh the authorization on the device so the change takes place immediately. Or you can wait for the device to communicate as scheduled.

You can optionally configure an HTTP proxy.

ASAv

The ASAv must have internet access either directly or through an HTTP proxy at least every 30 days. The ASAv does not have a grace period. You must contact the Licensing Authority, or the ASAv will be severely rate-limited until you are able to successfully reauthorize.

Firepower 9300

The Firepower 9300 must have internet access either directly or through an HTTP proxy at least every 90 days. Normal license communication occurs every 30 days, but with the grace period, your device will operate for up to 90 days without calling home. After the grace period, you must contact the Licensing Authority, or

you will not be able to make configuration changes to features requiring special licenses; operation is otherwise unaffected.

Out-of-Compliance State

The device can become out of compliance in the following situations:

- Over-utilization—When the device uses unavailable licenses.
- License expiration—When a time-based license expires.
- Lack of communication—When the device cannot reach the Licensing Authority for re-authorization.

To verify whether your account is in, or approaching, an Out-of-Compliance state, you must compare the entitlements currently in use by your device against those in your Smart Account.

In an out-of-compliance state, the device might be limited, depending on the model:

- ASAv—The ASAv will be severely rate-limited until you are able to successfully reauthorize.
- Firepower 9300—You will not be able to make configuration changes to features requiring special licenses, but operation is otherwise unaffected. For example, existing contexts over the Standard license limit can continue to run, and you can modify their configuration, but you will not be able to add a *new* context. If you do not have sufficient Standard licenses when you first register, you cannot configure any licensed features, including strong encryption features.

Smart Call Home Infrastructure

By default, a Smart Call Home profile exists in the configuration that specifies the URL for the Licensing Authority. You cannot remove this profile. Note that the only configurable option for the License profile is the destination address URL for the License Authority. Unless directed by Cisco TAC, you should not change the License Authority URL.



Note For the Firepower 9300 chassis, Smart Call Home for licensing is configured in the Firepower 9300 chassis supervisor, not on the ASA.

You cannot disable Smart Call Home for Smart Software Licensing. For example, even if you disable Smart Call Home using the **no service call-home** command, Smart Software Licensing is not disabled.

Other Smart Call Home functions are not turned on unless you specifically configure them.

History for Smart Software Licensing

Feature Name	Platform Releases	Description
Cisco Smart Software Licensing for the ASA on the Firepower 9300	9.4(1.150)	We introduced Smart Software Licensing for the ASA on the Firepower 9300. We introduced the following commands: feature strong-encryption, feature mobile-sp, feature context
Cisco Smart Software Licensing for the ASAv	9.3(2)	Smart Software Licensing lets you purchase and manage a pool of licenses. Unlike PAK licenses, smart licenses are not tied to a specific serial number. You can easily deploy or retire ASAvs without having to manage each unit's license key. Smart Software Licensing also lets you see your license usage and needs at a glance. We introduced the following commands: clear configure license, debug license agent, feature tier, http-proxy, license smart, license smart deregister, license smart register, license smart renew, show license, show running-config license, throughput level