

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 12
- Guidelines for Smart Software Licensing, on page 15
- Defaults for Smart Software Licensing, on page 15
- ASAv: Configure Smart Software Licensing, on page 16
- Firepower 2100: Configure Smart Software Licensing, on page 25
- Firepower 4100/9300: Configure Smart Software Licensing, on page 35
- Licenses Per Model, on page 38
- Monitoring Smart Software Licensing, on page 43
- Smart Software Manager Communication, on page 47
- History for Smart Software Licensing, on page 49

About Smart Software Licensing

This section describes how Smart Software Licensing works.

Smart Software Licensing for the ASA on the Firepower 4100/9300 Chassis

For the ASA on the Firepower 4100/9300 chassis, Smart Software Licensing configuration is split between the Firepower 4100/9300 chassis supervisor and the ASA.

- Firepower 4100/9300 chassis—Configure all Smart Software Licensing infrastructure on the chassis, including parameters for communicating with the License Authority. The Firepower 4100/9300 chassis itself does not require any licenses to operate.

Note Inter-chassis clustering requires that you enable the same Smart Licensing method on each chassis in the cluster.

- 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.

Offline Management

If your devices do not have internet access, and cannot register with the License Authority, you can configure offline licensing.

Permanent License Reservation

If your devices cannot access the internet for security reasons, you can optionally request permanent licenses for each ASA. Permanent licenses do not require periodic access to the License Authority. Like PAK licenses, you will purchase a license and install the license key for the ASA. Unlike a PAK license, you obtain and manage the licenses with the Smart Software Manager. You can easily switch between regular smart licensing mode and permanent license reservation mode.

ASAv Permanent License Reservation

You can obtain a model-specific license that enables all features: Standard tier; maximum throughput for your model; Strong Encryption (3DES/AES) license if your account qualifies; and AnyConnect client capabilities 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 5).

- ASAv5
- ASAv10

- ASAv30
- ASAv50

You must choose the model level that you want to use during ASAv deployment. That model level determines the license you request. If you later want to change the model level of a unit, you will have to return the current license and request a new license at the correct model level. To change the model of an already deployed ASAv, from the hypervisor you can change the vCPUs and DRAM settings to match the new model requirements; see the ASAv quick start guide for these values.

If you stop using a license, you must return the license by generating a return code on the ASAv, and then entering that code into the Smart Software Manager. Make sure you follow the return process correctly so you do not pay for unused licenses.

Permanent license reservation is not supported for the Azure hypervisor.

Firepower 2100 Permanent License Reservation

You can obtain a license that enables all features: Standard tier; maximum Security Contexts; Strong Encryption (3DES/AES) license if your account qualifies; and AnyConnect client capabilities 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 5) You also need to request the entitlements in the ASA configuration so that the ASA allows their use.

If you stop using a license, you must return the license by generating a return code on the ASA, and then entering that code into the Smart Software Manager. Make sure you follow the return process correctly so you do not pay for unused licenses.

Firepower 4100/9300 chassis Permanent License Reservation

You can obtain a license that enables all features: Standard tier; maximum Security Contexts; Carrier license; Strong Encryption (3DES/AES) license if your account qualifies; and AnyConnect client capabilities 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 5). The license is managed on the Firepower 4100/9300 chassis, but you also need to request the entitlements in the ASA configuration so that the ASA allows their use.

If you stop using a license, you must return the license by generating a return code on the Firepower 4100/9300 chassis, and then entering that code into the Smart Software Manager. Make sure you follow the return process correctly so you do not pay for unused licenses.

Satellite Server (Smart Software Manager On-Prem)

If your devices cannot access the internet for security reasons, you can optionally install a local Smart Software Manager satellite (also known as On-Prem) server as a virtual machine (VM). The satellite provides a subset of Smart Software Manager functionality, and allows you to provide essential licensing services for all your local devices. Only the satellite needs to connect periodically to the main License Authority to sync your license usage. You can sync on a schedule or you can sync manually.

You can perform the following functions on the satellite server:

- Activate or register a license
- View your company's licenses
- Transfer licenses between company entities

For more information, see Smart Software Manager satellite.

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 4100/9300 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 2100

Before the Firepower 2100 registers with the Licensing Authority, it operates for 90 days (total usage) in evaluation mode. Only default entitlements are enabled. When this period ends, the Firepower 2100 becomes out-of-compliance.



Note You cannot receive an evaluation license for Strong Encryption (3DES/AES); you must register with the License Authority to receive the export-compliance token that enables the Strong Encryption (3DES/AES) license.

Firepower 4100/9300 Chassis

The Firepower 4100/9300 chassis supports two types of evaluation license:

- Chassis-level evaluation mode—Before the Firepower 4100/9300 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 4100/9300 chassis becomes out-of-compliance.
- Entitlement-based evaluation mode—After the Firepower 4100/9300 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 to receive the export-compliance token that enables the Strong Encryption (3DES/AES) 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 or Satellite server, 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.

When you request the registration token for the ASAv from your Smart Software Licensing account, check the **Allow export-controlled functionality on the products registered with this token** check box so that the Strong Encryption (3DES/AES) license is applied (your account must be qualified for its use). If the ASAv becomes out-of-compliance later, as long as the export compliance token was successfully applied, the ASAv will retain the license and not revert to the rate-limited state. The license is removed if you re-register the ASAv, and export compliance is disabled, or if you restore the ASAv to factory default settings.

If you initially register the ASAv without strong encryption and later add strong encryption, then you must reload the ASAv for the new license to take effect.

For permanent license reservation licenses, the Strong Encryption (3DES/AES) license is enabled if your account qualifies for its use.

For pre-2.3.0 Satellite server versions, you must manually request the Strong Encryption license in the ASA configuration (the export compliance token is not supported); in this case, if the ASAv becomes out-of-compliance, throughput is severely limited.

Strong Encryption: Firepower 2100

Strong Encryption (3DES/AES) is available for management connections before you connect to the License Authority or Satellite server so you can launch ASDM. Note that ASDM access is only available on management-only interfaces with the default encryption. Through the box traffic is not allowed until you connect and obtain the Strong Encryption license.

When you request the registration token for the ASA from your Smart Software Licensing account, check the **Allow export-controlled functionality on the products registered with this token** check box so that the Strong Encryption (3DES/AES) license is applied (your account must be qualified for its use). If the ASA becomes out-of-compliance later, as long as the export compliance token was successfully applied, the ASA will continue to allow through the box traffic. Even if you re-register the ASA, and export compliance is disabled, the license remains enabled. The license is removed if you restore the ASA to factory default settings.

If you initially register the ASA without strong encryption and later add strong encryption, then you must reload the ASA for the new license to take effect.

For permanent license reservation licenses, the Strong Encryption (3DES/AES) license is enabled if your account qualifies for its use.

For pre-2.3.0 Satellite server versions, you must manually request the Strong Encryption license in the ASA configuration (the export compliance token is not supported); in this case, if the ASA becomes out-of-compliance, through-traffic will not be allowed.

Strong Encryption: Firepower 4100/9300 Chassis

When the ASA is deployed as a logical device, you can launch ASDM immediately. Through the box traffic is not allowed until you connect and obtain the Strong Encryption license.

When you request the registration token for the Firepower chassis from your Smart Software Licensing account, check the **Allow export-controlled functionality on the products registered with this token** check box so that the Strong Encryption (3DES/AES) license is applied (your account must be qualified for its use).

If the ASA becomes out-of-compliance later, as long as the export compliance token was successfully applied, the ASA will continue to allow through the box traffic. The license is removed if you re-register the chassis, and export compliance is disabled, or if you restore the chassis to factory default settings.

If you initially register the chassis without strong encryption and later add strong encryption, then you must reload the ASA application for the new license to take effect.

For permanent license reservation licenses, the Strong Encryption (3DES/AES) license is enabled if your account qualifies for its use.

For pre-2.3.0 Satellite server versions that do not support the export-compliance token: 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.

Carrier License

The Carrier license enables the following inspection features:

- Diameter
- GTP/GPRS
- SCTP

Total TLS Proxy Sessions

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

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

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

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



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

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

You might also use SRTP encryption sessions for your connections:

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

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

VLANs, Maximum

For an interface to count against the VLAN limit, you must assign a VLAN to it. 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 Firepower 2100

Regular or Satellite Smart Licensing

Only the active unit requests licenses from the server. Licenses are aggregated into a single failover license that is shared by the failover pair. There is no extra cost for secondary units.

After you enable failover for Active/Standby failover, you can only configure smart licensing on the active unit. For Active/Active failover, you can only configure smart licensing on the unit with failover group 1 as active. The configuration is replicated to the standby unit, but the standby unit does not use the configuration; it remains in a cached state. The aggregated license is also cached on the standby unit to be used if it becomes the active unit in the future.

Note Each ASA must have the same encryption license when forming a failover pair. When you register an ASA to the smart licensing server, the Strong Encryption license is automatically enabled for qualified customers when you apply the registration token. Because of this requirement, you have two choices for licensing when you use the Strong Encryption token with failover:

- Before you enable failover, register both units to the smart licensing server. In this case, both units will have strong encryption. Then, after you enable failover, continue configuring license entitlements on the active unit. If you enable encryption for the failover link, it will use AES/3DES (strong encryption).
- Before you register the active unit to the smart licensing server, enable failover. In this case, both units will not yet have strong encryption. Then configure license entitlements and register the active unit to the smart licensing server; both units will get strong encryption from the aggregated license. Note that if you enabled encryption on the failover link, it will use DES (weak encryption) because the failover link was established before the units gained strong encryption. You must reload *both* units to use AES/3DES on the link. If you only reload one unit, then that unit will try to use AES/3DES while the original unit uses DES, which will result in both units becoming active (split brain).

Each add-on license type is managed as follows:

- Standard—Although only the active unit requests this license from the server, the standby unit has the Standard license enabled by default; it does not need to register with the server to use it.
- Context—Only the active unit requests this license. However, the Standard license includes 2 contexts by default and is present on both units. The value from each unit's Standard license plus the value of the Context license on the active unit are combined up to the platform limit. For example:
  - The Standard license includes 2 contexts; for two Firepower 2130 units, these licenses add up to 4 contexts. You configure a 30-Context license on the active unit in an Active/Standby pair. Therefore, the aggregated failover license includes 34 contexts. However, because the platform limit for one unit is 30, the combined license allows a maximum of 30 contexts only. In this case, you might only configure the active Context license to be 25 contexts.
  - The Standard license includes 2 contexts; for two Firepower 2130 units, these licenses add up to 4 contexts. You configure a 10-Context license on the primary unit in an Active/Active pair. Therefore, the aggregated failover license includes 14 contexts. One unit can use 9 contexts and the other unit can use 5 contexts, for example, for a total of 14. Because the platform limit for one unit is 30, the combined license allows a maximum of 30 contexts; the 14 contexts are within the limit.
- Strong Encryption (3DES/AES) (for a pre-2.3.0 Cisco Smart Software Manager satellite deployment when you cannot use the strong encryption token, or for tracking purposes)—Only the active unit requests this license, and both units can use it due to license aggregation.

After a failover, the new active unit continues to use the aggregated license. It uses the cached license configuration to re-request the entitlement from the server. When the old active unit rejoins the pair as a standby unit, it releases the license entitlement. Before the standby unit releases the entitlement, the new active unit's license might be in a non-compliant state if there are no available licenses in the account. The failover pair can use the aggregated license for 30 days, but if it is still non-compliant after the grace period, you will not be able to make configuration changes to features requiring special licenses (i.e. add an extra context); operation is otherwise unaffected. The new active unit sends an entitlement authorization renewal request every 35 seconds until the license is compliant. If you disband the failover pair, then the active unit releases

the entitlements, and both units retain the licensing configuration in a cached state. To re-activate licensing, you need to clear the configuration on each unit, and re-configure it.

Permanent License Reservation

For permanent license reservation, you must purchase separate licenses for each chassis and enable the licenses *before* you configure failover.

Failover Licenses for the ASA on the Firepower 4100/9300 Chassis

Regular or Satellite Smart Licensing

Both Firepower 4100/9300 chassis must be registered with the License Authority or satellite server before you configure failover. There is no extra cost for secondary units.

The Strong Encryption license is automatically enabled for qualified customers when you apply the registration token. When using the token, each chassis must have the same encryption license. For the optional Strong Encryption (3DES/AES) feature license enabled in the ASA configuration, see below.

After you enable failover, for the ASA license configuration for Active/Standby failover, you can only configure smart licensing on the active unit. For Active/Active failover, you can only configure smart licensing on the unit with failover group 1 as active. The configuration is replicated to the standby unit, but the standby unit does not use the configuration; it remains in a cached state. Only the active unit requests the licenses from the server. The licenses are aggregated into a single failover license that is shared by the failover pair, and this aggregated license is also cached on the standby unit to be used if it becomes the active unit in the future. Each license type is managed as follows:

- Standard—Although only the active unit requests this license from the server, the standby unit has the Standard license enabled by default; it does not need to register with the server to use it.
- Context—Only the active unit requests this 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 the Context license on the active unit 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 active 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 active 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. Therefore, the aggregated failover license includes 30 contexts. One unit can use 17 contexts and the other unit can use 13 contexts, for example, for a total of 30. Because the platform limit for one unit is 250, the combined license allows a maximum of 250 contexts; the 30 contexts are within the limit.
- Carrier—Only the active requests this license, and both units can use it due to license aggregation.
- Strong Encryption (3DES) (for a pre-2.3.0 Cisco Smart Software Manager satellite deployment when you cannot use the strong encryption token, or for tracking purposes)—Only the active unit requests this license, and both units can use it due to license aggregation.

After a failover, the new active unit continues to use the aggregated license. It uses the cached license configuration to re-request the entitlement from the server. When the old active unit rejoins the pair as a standby unit, it releases the license entitlement. Before the standby unit releases the entitlement, the new active unit's license might be in a non-compliant state if there are no available licenses in the account. The failover

pair can use the aggregated license for 30 days, but if it is still non-compliant after the grace period, you will not be able to make configuration changes to features requiring special licenses; operation is otherwise unaffected. The new active unit sends an entitlement authorization renewal request every 35 seconds until the license is compliant. If you disband the failover pair, then the active unit releases the entitlements, and both units retain the licensing configuration in a cached state. To re-activate licensing, you need to clear the configuration on each unit, and re-configure it.

Permanent License Reservation

For permanent license reservation, you must purchase separate licenses for each chassis and enable the licenses *before* you configure failover.

ASA Cluster Licenses for the ASA on the Firepower 4100/9300 Chassis

The clustering feature itself does not require any licenses. To use Strong Encryption and other optional licenses, each Firepower 4100/9300 chassis must be registered with the License Authority or satellite server. There is no extra cost for data units. For permanent license reservation, you must purchase separate licenses for each chassis.

The Strong Encryption license is automatically enabled for qualified customers when you apply the registration token. When using the token, each chassis must have the same encryption license. For the optional Strong Encryption (3DES/AES) feature license enabled in the ASA configuration, see below.

In the ASA license configuration, you can only configure smart licensing on the control unit. The configuration is replicated to the data units, but for some licenses, they do not use the configuration; it remains in a cached state, and only the control unit requests the license. The licenses are aggregated into a single cluster license that is shared by the cluster units, and this aggregated license is also cached on the data units to be used if one of them becomes the control unit in the future. Each license type is managed as follows:

- Standard—Only the control unit requests the Standard license from the server. Because the data units have the Standard license enabled by default, they do not need to register with the server to use it.
- Context—Only the control unit requests the Context license from the server. The Standard license includes 10 contexts by default and is present on all cluster members. The value from each unit's Standard license plus the value of the Context license on the control unit are combined up to the platform limit in an aggregated cluster license. For example:
  - You have 6 Firepower 9300 modules in the cluster. The Standard license includes 10 contexts; for 6 units, these licenses add up to 60 contexts. You configure an additional 20-Context license on the control unit. Therefore, the aggregated cluster license includes 80 contexts. Because the platform limit for one module is 250, the combined license allows a maximum of 250 contexts; the 80 contexts are within the limit. Therefore, you can configure up to 80 contexts on the control unit; each data unit will also have 80 contexts through configuration replication.
  - You have 3 Firepower 4110 units in the cluster. The Standard license includes 10 contexts; for 3 units, these licenses add up to 30 contexts. You configure an additional 250-Context license on the control unit. Therefore, the aggregated cluster license includes 280 contexts. Because the platform limit for one unit is 250, the combined license allows a maximum of 250 contexts; the 280 contexts are over the limit. Therefore, you can only configure up to 250 contexts on the control unit; each data unit will also have 250 contexts through configuration replication. In this case, you should only configure the control unit Context license to be 220 contexts.
- Carrier—Required for Distributed S2S VPN. This license is a per-unit entitlement, and each unit requests its own license from the server. This license configuration is replicated to the data units.

- Strong Encryption (3DES) (for pre-2.3.0 Cisco Smart Software Manager satellite deployment, or for tracking purposes)—This license is a per-unit entitlement, and each unit requests its own license from the server.

If a new control unit is elected, the new control unit continues to use the aggregated license. It also uses the cached license configuration to re-request the control unit license. When the old control unit rejoins the cluster as a data unit, it releases the control unit license entitlement. Before the data unit releases the license, the control unit's license might be in a non-compliant state if there are no available licenses in the account. The retained license is valid for 30 days, but if it is still non-compliant after the grace period, you will not be able to make configuration changes to features requiring special licenses; operation is otherwise unaffected. The new active unit sends an entitlement authorization renewal request every 12 hours until the license is compliant. You should refrain from making configuration changes until the license requests are completely processed. If a unit leaves the cluster, the cached control configuration is removed, while the per-unit entitlements are retained. In particular, you would need to re-request the Context license on non-cluster units.

Prerequisites for Smart Software Licensing

Regular and Satellite Smart License Prerequisites

ASAv, Firepower 2100

- Ensure internet access, or HTTP proxy access, or satellite server 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. On the Firepower 2100, you set the clock in FXOS.
- 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 4100/9300 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

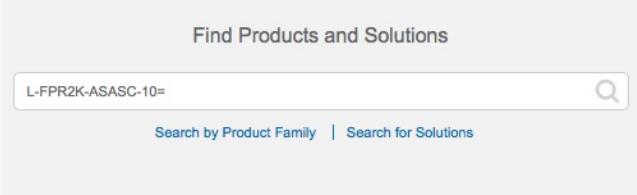
  If you do not yet have an account, click the link to set up a new account. The Smart Software Manager lets you create a master account for your organization. Even though the ASA does need internet connectivity to the Smart Licensing server for permanent license reservation, the Smart Software Manager 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 13). 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 5).
- ASAv: Permanent license reservation is not supported for the Azure hypervisor and ASAv100.

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



ASAv PIDs

ASAv Regular and Satellite Smart Licensing PIDs:

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

ASAv Permanent License Reservation PIDs:

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 5).

- ASAv5—L-ASAV5SR-K9=
- ASAv10—L-ASAV10SR-K9=
- ASAv30—L-ASAV30SR-K9=

- ASAv50—L-ASAV50SR-K9=

Firepower 2100 PIDs

Firepower 2100 Regular and Satellite Smart Licensing PIDs:

- Standard license—L-FPR2100-ASA=. The Standard license is free, but you still need to add it to your Smart Software Licensing account.
- 5 context license—L-FPR2K-ASASC-5=. Context licenses are additive; buy multiple licenses to meet your needs.
- 10 context license—L-FPR2K-ASASC-10=. Context licenses are additive; buy multiple licenses to meet your needs.
- Strong Encryption (3DES/AES) license—L-FPR2K-ENC-K9=. This license is free. Although this license is not generally rquired (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.

Firepower 2100 Permanent License Reservation PID:

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 5).

- L-FPR2K-ASA-BPU=

Firepower 4100 PIDs

Firepower 4100 Regular and Satellite Smart Licensing PIDs:

- Standard license—L-FPR4100-ASA=. The Standard license is free, but you still need to add it to your Smart Software Licensing account.
- 10 context license—L-FPR4K-ASASC-10=. Context licenses are additive; buy multiple licenses to meet your needs.
- 230 context license—L-FPR4K-ASASC-230=. Context licenses are additive; buy multiple licenses to meet your needs.
- 250 context license—L-FPR4K-ASASC-250=. Context licenses are additive; buy multiple licenses to meet your needs.
- Carrier (Diameter, GTP/GPRS, SCTP)—L-FPR4K-ASA-CAR=
- Strong Encryption (3DES/AES) license—L-FPR4K-ENC-K9=. This license is free. Although this license is not generally rquired (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.

Firepower 4100 Permanent License Reservation PID:

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 5).

- L-FPR4K-ASA-BPU=

Firepower 9300 PIDs

Firepower 9300 Regular and Satellite Smart Licensing 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 rquired (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.

Firepower 9300 Permanent License Reservation PIDs:

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 5).

- L-FPR9K-ASA-BPU=

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.
- For permanent license reservation, you must return the license before you decommission the device. If you do not officially return the license, the license remains in a used state and cannot be reused for a new device.
- 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. For permanent license reservation, you do not need to set these parameters. When you enable permanent license reservation, these commands are removed from the configuration.

```
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
```

Firepower 2100

The Firepower 2100 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
```

ASA on the Firepower 4100/9300 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. Choose one of the following methods:

Procedure

Step 1 ASAv: Configure Regular Smart Software Licensing, on page 16.

Step 2 ASAv: Configure Satellite Smart Software Licensing, on page 20.

Step 3 ASAv: Configure Permanent License Reservation, on page 21.

ASAv: Configure Regular 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.

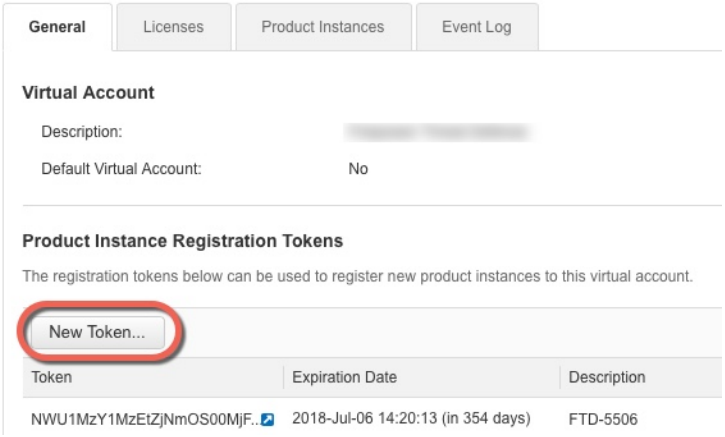
a) Click **Inventory**.

Figure 2: Inventory



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

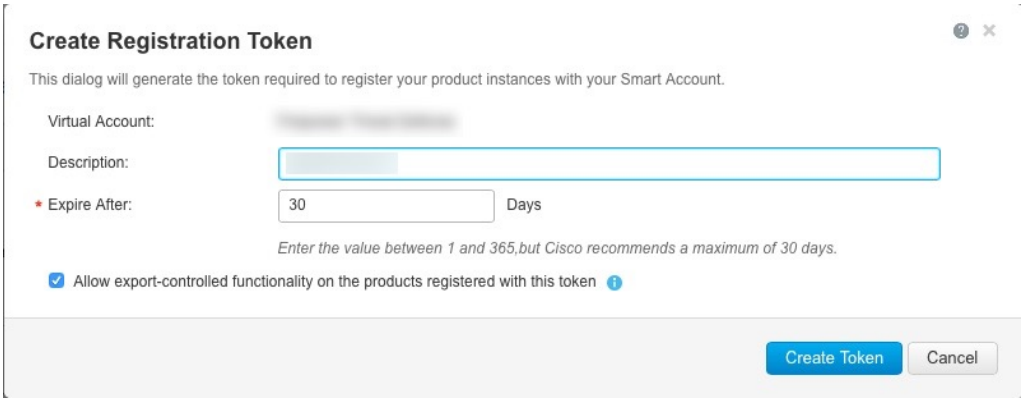
Figure 3: New Token



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 functionaility 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

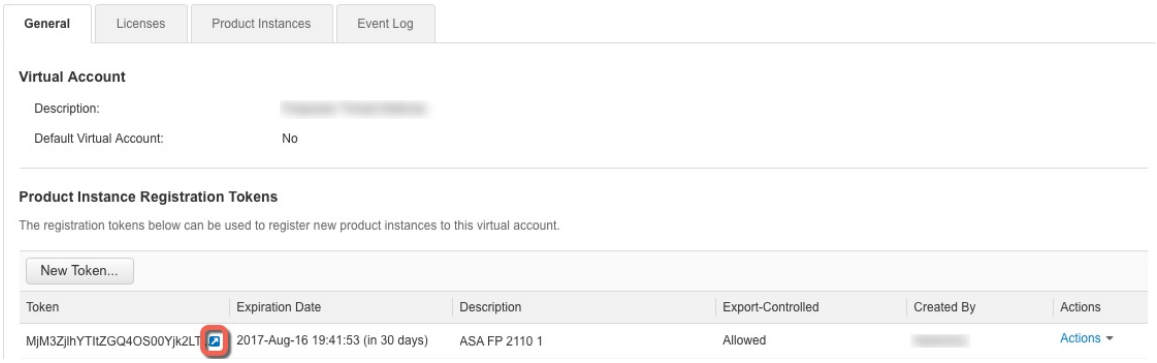
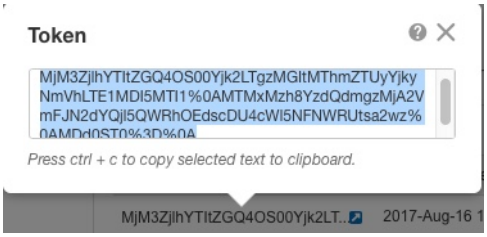


Figure 6: Copy Token



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** | **10G**}

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 YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

ASAv: Configure Satellite Smart Software Licensing

This procedure applies for an ASAv using a satellite Smart Software Licensing server.

Before you begin

Download the Smart Software Manager satellite OVA file from Cisco.com and install and configure it on a VMwareESXi server. For more information, see Smart Software Manager satellite.

Procedure

Step 1 Request a registration token on the satellite server.

Step 2 (Optional) On the ASA, 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 Change the license server URL to go to the satellite server.

call-home

profile License

destination address http https://*satellite_ip_address***/Transportgateway/services/DeviceRequestHandler**

Example:

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile License
ciscoasa(cfg-call-home-profile) destination address http
https://10.1.5.5/Transportgateway/services/DeviceRequestHandler
```

Step 4 Register the ASA using the token you requested in Step 1:

license smart register idtoken *id_token*

Example:

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

The ASA registers with the satellite server and requests authorization for the configured license entitlements. The satellite server also applies the Strong Encryption (3DES/AES) license if your account allows. Use the **show license summary** command to check the license status and usage.

Example:

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: Biz1
  Virtual Account: IT
  Export-Controlled Functionality: Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:29 2018 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Oct 23 01:41:26 2017 UTC

License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  regid.2014-08.com.ci... (FP2110-ASA-Std)                    1 AUTHORIZED
```

ASAv: Configure Permanent License Reservation

You can assign a permanent license to an ASAv. This section also describes how to return a license if you retire the ASAv or change model tiers and need a new license.

Procedure

Step 1 Install the ASAv Permanent License, on page 21

Step 2 (Optional) (Optional) Return the ASAv Permanent License, on page 23

Install the ASAv Permanent License

For ASAvs that do not have Internet access, you can request a permanent license from the Smart Software Manager.

Note For permanent license reservation, you must return the license before you decommission the ASAv. If you do not officially return the license, the license remains in a used state and cannot be reused for a new ASAv. See (Optional) Return the ASAv Permanent License, on page 23.

Note If you clear your configuration after you install the permanent license (for example using **write erase**), then you only need to reenable permanent license reservation using the **license smart reservation** command without any arguments as shown in step 1; you do not need to complete the rest of this procedure.

Before you begin

- Purchase permanent licenses so they are available in the Smart Software Manager. Not all accounts are approved for permanent license reservation. Make sure you have approval from Cisco for this feature before you attempt to configure it.
- You must request a permanent license after the ASAv starts up; you cannot install a permanent license as part of the Day 0 configuration.

Procedure

Step 1 At the ASAv CLI, enable permanent license reservation:

license smart reservation

Example:

```
ciscoasa (config)# license smart reservation
ciscoasa (config)#
```

The following commands are removed:

```
license smart
  feature tier standard
  throughput level {100M | 1G | 2G | 10G}
```

To use regular smart licensing, use the **no** form of this command, and re-enter the above commands. Other Smart Call Home configuration remains intact but unused, so you do not need to re-enter those commands.

Step 2 Request the license code to enter in the Smart Software Manager:

license smart reservation request universal

Example:

```
ciscoasa# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
ciscoasa#
```

You must choose the model level (ASAv5/ASAv10/ASAv30/ASAv50/ASAv100) that you want to use during ASAv deployment. That model level determines the license you request. If you later want to change the model level of a unit, you will have to return the current license and request a new license at the correct model level. To change the model of an already deployed ASAv, from the hypervisor you can change the vCPUs and DRAM settings to match the new model requirements; see the ASAv quick start guide for these values. To view your current model, use the **show vm** command.

If you re-enter this command, then the same code is displayed, even after a reload. If you have not yet entered this code into the Smart Software Manager and want to cancel the request, enter:

license smart reservation cancel

If you disable permanent license reservation, then any pending requests are canceled. If you already entered the code into the Smart Software Manager, then you must complete this procedure to apply the license to the ASAv, after which point you can return the license if desired. See (Optional) Return the ASAv Permanent License, on page 23.

Step 3 Go to the Smart Software Manager Inventory screen, and click the **Licenses** tab:

https://software.cisco.com/#SmartLicensing-Inventory

The **Licenses** tab displays all existing licenses related to your account, both regular and permanent.

Step 4 Click **License Reservation**, and type the ASAv code into the box. Click **Reserve License**.

The Smart Software Manager generates an authorization code. You can download the code or copy it to the clipboard. At this point, the license is now in use according to the Smart Software Manager.

If you do not see the **License Reservation** button, then your account is not authorized for permanent license reservation. In this case, you should disable permanent license reservation and re-enter the regular smart license commands.

Step 5 On the ASAv, enter the authorization code:

license smart reservation install *code*

Example:

```
ciscoasa# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
ciscoasa#
```

Your ASAv is now fully licensed.

(Optional) Return the ASAv Permanent License

If you no longer need a permanent license (for example, you are retiring an ASAv or changing its model level so it needs a new license), you must officially return the license to the Smart Software Manager using this procedure. If you do not follow all steps, then the license stays in a used state and cannot easily be freed up for use elsewhere.

Procedure

Step 1 On the ASAv, generate a return code:

license smart reservation return

Example:

```
ciscoasa# license smart reservation return
Enter this return code in the Cisco Smart Software Manager portal:
Au3431rGRS00Ig5HQl2vpcg{uXiTRfVrp7M/zDpirLwYCaq8oSv60yZJuFDVBS2QliQ=
```

The ASAv immediately becomes unlicensed and moves to the Evaluation state. If you need to view this code again, re-enter this command. Note that if you request a new permanent license (**license smart reservation request universal**) or change the ASAv model level (by powering down and changing the vCPUs/RAM), then you cannot re-display this code. Be sure to capture the code to complete the return.

Step 2 View the ASAv universal device identifier (UDI) so you can find this ASAv instance in the Smart Software Manager:

show license udi

Example:

```
ciscoasa# show license udi
UDI: PID:ASAv,SN:9AHV3KJBEKE
ciscoasa#
```

Step 3 Go to the Smart Software Manager Inventory screen, and click the **Product Instances** tab:

https://software.cisco.com/#SmartLicensing-Inventory

The **Product Instances** tab displays all licensed products by the UDI.

Step 4 Find the ASAv you want to unlicense, choose **Actions** > **Remove**, and type the ASAv return code into the box. Click **Remove Product Instance**.

The permanent license is returned to the available pool.

(Optional) Deregister the ASAv (Regular and Satellite)

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 (Regular and Satellite)

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 2100: Configure Smart Software Licensing

This section describes how to configure Smart Software Licensing for the Firepower 2100. Choose one of the following methods:

Procedure

Step 1 Firepower 2100: Configure Regular Smart Software Licensing, on page 25.

You can also (Optional) Deregister the Firepower 2100 (Regular and Satellite), on page 35 or (Optional) Renew the Firepower 2100 ID Certificate or License Entitlement (Regular and Satellite), on page 35.

Step 2 Firepower 2100: Configure Satellite Smart Software Licensing, on page 29.

You can also (Optional) Deregister the Firepower 2100 (Regular and Satellite), on page 35 or (Optional) Renew the Firepower 2100 ID Certificate or License Entitlement (Regular and Satellite), on page 35.

Step 3 Firepower 2100: Configure Permanent License Reservation, on page 31.

Firepower 2100: Configure Regular Smart Software Licensing

This procedure applies for an ASA using the License Authority.

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.

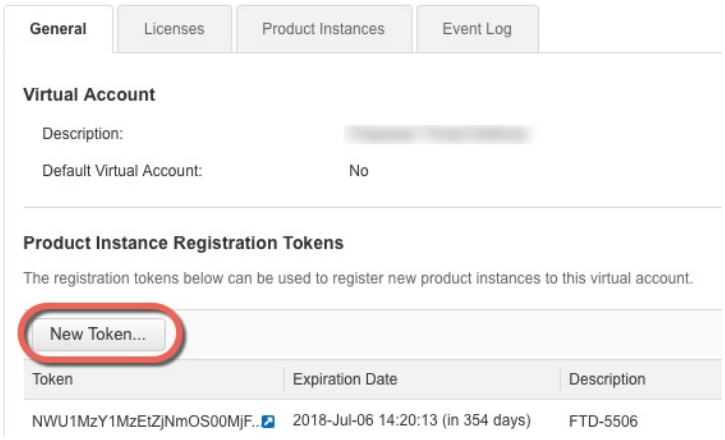
a) Click **Inventory**.

Figure 7: Inventory



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

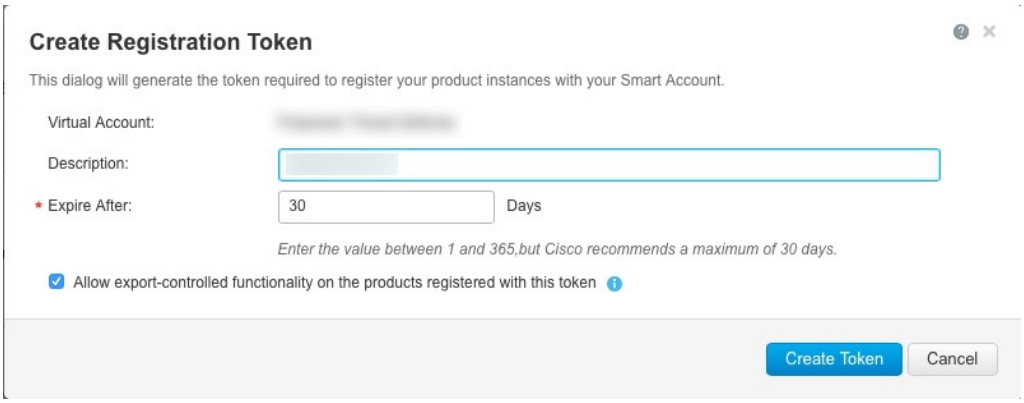
Figure 8: New Token



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 functionaility on the products registered with this token**—Enables the export-compliance flag.

Figure 9: 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 10: View Token

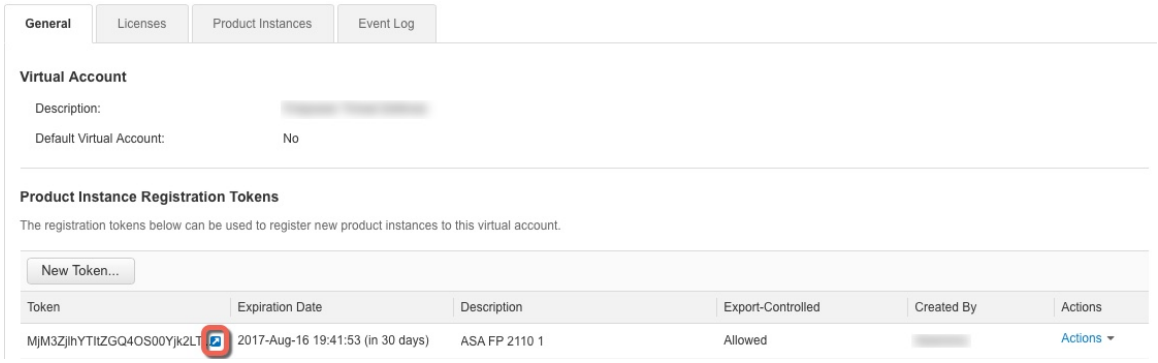
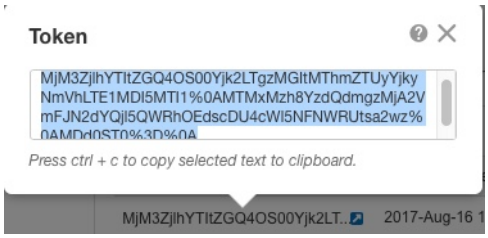


Figure 11: Copy Token



Step 2 (Optional) On the ASA, 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 Request license entitlements on the ASA.

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. A tier license is a prerequisite for adding other feature licenses.

c) Request the security context license.

feature context *number*

By default, the ASA supports 2 contexts, so you should request the number of contexts you want minus the 2 default contexts. The maximum number of contexts depends on your model:

- Firepower 2110—25 contexts
- Firepower 2120—25 contexts
- Firepower 2130—30 contexts
- Firepower 2140—40 contexts

For example, to use the maximum of 25 contexts on the Firepower 2110, enter 23 for the number of contexts; this value is added to the default of 2.

Example:

```
ciscoasa(config-smart-lic)# feature context 18
```

d) (Optional) The Strong Encryption (3DES/AES) license is generally not required; for example, ASAs that use older Satellite Server versions (pre-2.3.0) require this license, but you can enable this feature if you know you need to, or if you want to track usage of this license in your account.

feature strong-encryption

Example:

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

Step 4 Register the ASA using the token you copied in Step 1:

license smart register idtoken *id_token*

Example:

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

The ASA registers with the License Authority and requests authorization for the configured license entitlements. The License Authority also applies the Strong Encryption (3DES/AES) license if your account allows. Use the **show license summary** command to check the license status and usage.

Example:

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: Biz1
  Virtual Account: IT
```

```
  Export-Controlled Functionality: Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:29 2018 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Oct 23 01:41:26 2017 UTC

License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  regid.2014-08.com.ci... (FP2110-ASA-Std)                     1 AUTHORIZED
```

Firepower 2100: Configure Satellite Smart Software Licensing

This procedure applies for an ASA using a satellite Smart Software Licensing server.

Before you begin

Download the Smart Software Manager satellite OVA file from Cisco.com and install and configure it on a VMwareESXi server. For more information, see Smart Software Manager satellite.

Procedure

Step 1 Request a registration token on the satellite server.

Step 2 (Optional) On the ASA, 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 Change the license server URL to go to the satellite server.

call-home

profile License

destination address http https://*satellite_ip_address***/Transportgateway/services/DeviceRequestHandler**

Example:

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile License
ciscoasa(cfg-call-home-profile) destination address http
```

```
https://10.1.5.5/Transportgateway/services/DeviceRequestHandler
```

Step 4 Request license entitlements on the ASA.

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. A tier license is a prerequisite for adding other feature licenses.

c) Request the security context license.

feature context *number*

By default, the ASA supports 2 contexts, so you should request the number of contexts you want minus the 2 default contexts. The maximum number of contexts depends on your model:

- Firepower 2110—25 contexts
- Firepower 2120—25 contexts
- Firepower 2130—30 contexts
- Firepower 2140—40 contexts

For example, to use the maximum of 25 contexts on the Firepower 2110, enter 23 for the number of contexts; this value is added to the default of 2.

Example:

```
ciscoasa(config-smart-lic)# feature context 18
```

d) (Optional) The Strong Encryption (3DES/AES) license is generally not required; for example, ASAs that use older Satellite Server versions (pre-2.3.0) require this license, but you can enable this feature if you know you need to, or if you want to track usage of this license in your account.

feature strong-encryption

Example:

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

Step 5 Register the ASA using the token you requested in Step 1:

license smart register idtoken *id_token*

Example:

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
```

```
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

The ASA registers with the satellite server and requests authorization for the configured license entitlements. The satellite server also applies the Strong Encryption (3DES/AES) license if your account allows. Use the **show license summary** command to check the license status and usage.

Example:

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: Biz1
  Virtual Account: IT
  Export-Controlled Functionality: Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:29 2018 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Oct 23 01:41:26 2017 UTC

License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  regid.2014-08.com.ci... (FP2110-ASA-Std)                    1 AUTHORIZED
```

Firepower 2100: Configure Permanent License Reservation

You can assign a permanent license to a Firepower 2100. This section also describes how to return a license if you retire the ASA.

Procedure

Step 1 Install the Firepower 2100 Permanent License, on page 31.

Step 2 (Optional) (Optional) Return the Firepower 2100 Permanent License, on page 34.

Install the Firepower 2100 Permanent License

For ASAs that do not have internet access, you can request a permanent license from the Smart Software Manager. The permanent license enables all features: Standard tier with maximum Security Contexts.

Note For permanent license reservation, you must return the license before you decommission the ASA. If you do not officially return the license, the license remains in a used state and cannot be reused for a new ASA. See (Optional) Return the Firepower 2100 Permanent License, on page 34.

Before you begin

Purchase permanent licenses so they are available in the Smart Software Manager. Not all accounts are approved for permanent license reservation. Make sure you have approval from Cisco for this feature before you attempt to configure it.

Procedure

Step 1 At the ASA CLI, enable permanent license reservation:

license smart reservation

Example:

```
ciscoasa (config)# license smart reservation
ciscoasa (config)#
```

Step 2 Request the license code to enter in the Smart Software Manager:

license smart reservation request universal

Example:

```
ciscoasa# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
BB-ZFPR-2140:JAD200802RR-AzKmHcc71-2A
ciscoasa#
```

If you re-enter this command, then the same code is displayed, even after a reload. If you have not yet entered this code into the Smart Software Manager and want to cancel the request, enter:

license smart reservation cancel

If you disable permanent license reservation, then any pending requests are canceled. If you already entered the code into the Smart Software Manager, then you must complete this procedure to apply the license to the ASA, after which point you can return the license if desired. See (Optional) Return the Firepower 2100 Permanent License, on page 34.

Step 3 Go to the Smart Software Manager Inventory screen, and click the **Licenses** tab:

https://software.cisco.com/#SmartLicensing-Inventory

The **Licenses** tab displays all existing licenses related to your account, both regular and permanent.

Step 4 Click **License Reservation**, and type the ASA code into the box. Click **Reserve License**.

The Smart Software Manager generates an authorization code. You can download the code or copy it to the clipboard. At this point, the license is now in use according to the Smart Software Manager.

If you do not see the **License Reservation** button, then your account is not authorized for permanent license reservation. In this case, you should disable permanent license reservation and re-enter the regular smart license commands.

Step 5 On the ASA, enter the authorization code:

license smart reservation install *code*

Example:

```
ciscoasa# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
ciscoasa#
```

Step 6 Request license entitlements on the ASA.

You need to request the entitlements in the ASA configuration so that the ASA allows their use.

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. A tier license is a prerequisite for adding other feature licenses.

c) Request the security context license.

feature context *number*

By default, the ASA supports 2 contexts, so you should request the number of contexts you want minus the 2 default contexts. The maximum number of contexts depends on your model:

- Firepower 2110—25 contexts
- Firepower 2120—25 contexts
- Firepower 2130—30 contexts
- Firepower 2140—40 contexts

For example, to use the maximum of 25 contexts on the Firepower 2110, enter 23 for the number of contexts; this value is added to the default of 2.

Example:

```
ciscoasa(config-smart-lic)# feature context 18
```

d) (Optional) The Strong Encryption (3DES/AES) license is generally not required; for example, ASAs that use older Satellite Server versions (pre-2.3.0) require this license, but you can enable this feature if you know you need to, or if you want to track usage of this license in your account.

feature strong-encryption

Example:

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

(Optional) Return the Firepower 2100 Permanent License

If you no longer need a permanent license (for example, you are retiring an ASA), you must officially return the license to the Smart Software Manager using this procedure. If you do not follow all steps, then the license stays in a used state and cannot easily be freed up for use elsewhere.

Procedure

Step 1 On the ASA, generate a return code:

license smart reservation return

Example:

```
ciscoasa# license smart reservation return
Enter this return code in the Cisco Smart Software Manager portal:
Au3431rGRS00Ig5HQl2vpcg{uXiTRfVrp7M/zDpirLwYCaq8oSv60yZJuFDVBS2QliQ=
```

The ASA immediately becomes unlicensed and moves to the Evaluation state. If you need to view this code again, re-enter this command. Note that if you request a new permanent license (**license smart reservation request universal**), then you cannot re-display this code. Be sure to capture the code to complete the return.

Step 2 View the ASA universal device identifier (UDI) so you can find this ASA instance in the Smart Software Manager:

show license udi

Example:

```
ciscoasa# show license udi
UDI: PID:FPR-2140,SN:JAD200802RR
ciscoasa#
```

Step 3 Go to the Smart Software Manager Inventory screen, and click the **Product Instances** tab:

https://software.cisco.com/#SmartLicensing-Inventory

The **Product Instances** tab displays all licensed products by the UDI.

Step 4 Find the ASA you want to unlicense, choose **Actions** > **Remove**, and type the ASA return code into the box. Click **Remove Product Instance**.

The permanent license is returned to the available pool.

(Optional) Deregister the Firepower 2100 (Regular and Satellite)

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

Procedure

Deregister the ASA:

license smart deregister

(Optional) Renew the Firepower 2100 ID Certificate or License Entitlement (Regular and Satellite)

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, or for Permanent License Reservation; see the FXOS configuration guide to configure your method as a prerequisite.

For Permanent License Reservation, the license enables all features: Standard tier with maximum Security Contexts and the Carrier license. However, for the ASA to "know" to use these features, you need to enable them on the ASA.

Note For pre-2.3.0 Smart Software Manager satellite users: 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, including VPN.

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 4100/9300 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 unless you set it when you deployed the logical device, but you are prompted to change the password the first time you enter the **enable** command.

enable
configure terminal

Example:

```
asa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat 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:

- Carrier (GTP/GPRS, Diameter, and SCTP inspection)

  feature carrier

- Security Contexts

  feature context *<1-248>*

  For Permanent License Reservation, you can specify the maximum contexts (248).

- **For pre 2.3.0 satellite server users only:** Strong Encryption (3DES/AES)

  feature strong-encryption

Example:

```
ciscoasa(config-smart-lic)# feature carrier
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 4100/9300 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: 50,000 ASAv10: 100,000 ASAv30: 500,000 ASAv50: 2,000,000	
Carrier	Enabled	
Total TLS Proxy Sessions	ASAv5: 500 ASAv10: 500 ASAv30: 1000 ASAv50: 10,000	
VPN Licenses		
AnyConnect peers	Unlicensed	*Optional AnyConnect Plus or Apex license, Maximums:* *ASAv5: 50* *ASAv10: 250* *ASAv30: 750* *ASAv50: 10,000*

Licenses	Standard License
Other VPN Peers	ASAv5: 50 ASAv10: 250 ASAv30: 1000 ASAv50: 10,000
Total VPN Peers, combined all types	ASAv5: 50 ASAv10: 250 ASAv30: 1000 ASAv50: 10,000
General Licenses	
Throughput Level	ASAv5: 100 Mbps ASAv10: 1 Gbps ASAv30: 2 Gbps ASAv50: 10 Gbps
Encryption	Base (DES) or Strong (3DES/AES), depending on the account's export compliance setting
Failover	Active/Standby
Security Contexts	No support
Clustering	No support
VLANs, Maximum	ASAv5: 25 ASAv10: 50 ASAv30: 200 ASAv50: 1024
RAM, vCPUs	ASAv5: 1 GB, 1 vCPU (Optional) ASAv5: 1.5 GB, 1 vCPU (9.8(2) and later). You may want to assign more memory if your ASAv5 experiences memory exhaustion. ASAv10: 2 GB, 1 vCPU ASAv30: 8 GB, 4 vCPUs ASAv50: 16 GB, 8 vCPUs

Firepower 2100 Series

The following table shows the licensed features for the Firepower 2100 series.

Licenses	Standard License	
Firewall Licenses		
Botnet Traffic Filter	No Support.	
Firewall Conns, Concurrent	Firepower 2110: 1,000,000 Firepower 2120: 1,500,000 Firepower 2130: 2,000,000 Firepower 2140: 3,000,000	
Carrier	No support. Although SCTP inspection maps are not supported, SCTP stateful inspection using ACLs is supported.	
Total TLS Proxy Sessions	Firepower 2110: 4,000 Firepower 2120: 8,000 Firepower 2130: 8,000 Firepower 2140: 10,000	
VPN Licenses		
AnyConnect peers	Unlicensed	*Optional AnyConnect Plus or Apex license, Maximums:* *Firepower 2110: 1,500* *Firepower 2120: 3,500* *Firepower 2130: 7,500* *Firepower 2140: 10,000*
Other VPN Peers	Firepower 2110: 1,500 Firepower 2120: 3,500 Firepower 2130: 7,500 Firepower 2140: 10,000	
Total VPN Peers, combined all types	Firepower 2110: 1,500 Firepower 2120: 3,500 Firepower 2130: 7,500 Firepower 2140: 10,000	
General Licenses		
Encryption	Base (DES) or Strong (3DES/AES), depending on the account's export compliance setting	

Licenses	Standard License	
Security Contexts	2	*Optional License, Maximums in increments of 5 or 10:* *Firepower 2110: 25* *Firepower 2120: 25* *Firepower 2130: 30* *Firepower 2140: 40*
Clustering	No support.	
VLANs, Maximum	1024	

Firepower 4100 Series ASA Application

The following table shows the licensed features for the Firepower 4100 series ASA application.

Licenses	Standard License	
Firewall Licenses		
Botnet Traffic Filter	No Support.	
Firewall Conns, Concurrent	Firepower 4110: 10,000,000 Firepower 4115: 15,000,000 Firepower 4120: 15,000,000 Firepower 4125: 25,000,000 Firepower 4140: 25,000,000 Firepower 4145: 40,000,000 Firepower 4150: 35,000,000	
Carrier	Disabled	*Optional License: Carrier*
Total TLS Proxy Sessions	Firepower 4110: 10,000 All others: 15,000	
VPN Licenses		
AnyConnect peers	Unlicensed	*Optional AnyConnect Plus or Apex license:* *Firepower 4110: 10,000* *All others: 20,000*
Other VPN Peers	Firepower 4110: 10,000 All others: 20,000	

Licenses	Standard License	
Total VPN Peers, combined all types	Firepower 4110: 10,000 All others: 20,000	
General Licenses		
Encryption	Base (DES) or Strong (3DES/AES), depending on the account's export compliance setting	
Security Contexts	10	*Optional License: Maximum of 250, in increments of 10*
Clustering	Enabled	
VLANs, Maximum	1024	

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-56: 60,000,000, up to 70,000,000 for a chassis with 3 modules Firepower 9300 SM-48: 60,000,000, up to 70,000,000 for a chassis with 3 modules Firepower 9300 SM-44: 60,000,000, up to 70,000,000 for a chassis with 3 modules Firepower 9300 SM-40: 60,000,000, up to 70,000,000 for a chassis with 3 modules 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	
Carrier	Disabled	*Optional License: Carrier*
Total TLS Proxy Sessions	15,000	
VPN Licenses		
AnyConnect peers	Unlicensed	*Optional AnyConnect Plus or Apex license: 20,000 maximum*
Other VPN Peers	20,000	

Licenses	Standard License	
Total VPN Peers, combined all types	20,000	
General Licenses		
Encryption	Base (DES) or Strong (3DES/AES), depending on the account's export compliance setting	
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
```

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
Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: ASA
  Virtual Account: ASAv Internal Users
  Export-Controlled Functionality: Not Allowed
  Initial Registration: SUCCEEDED on Sep 21 20:26:29 2015 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:28 2016 UTC
  Registration Expires: Sep 20 20:23:25 2016 UTC

License Authorization:
  Status: AUTHORIZED on Sep 21 21:17:35 2015 UTC
  Last Communication Attempt: SUCCEEDED on Sep 21 21:17:35 2015 UTC
  Next Communication Attempt: Sep 24 00:44:10 2015 UTC
  Communication Deadline: Dec 20 21:14:33 2015 UTC

License Usage
==============

regid.2014-08.com.cisco.ASAv-STD-1G,1.0_4fd3bdbd-29ae-4cce-ad82-45ad3db1070c
(ASAv-STD-1G):
  Description: This entitlement tag was created via Alpha Extension application
  Count: 1
  Version: 1.0
  Status: AUTHORIZED

Product Information
===================
UDI: PID:ASAv,SN:9AHV3KJBEKE

Agent Version
=============
Smart Agent for Licensing: 1.6_reservation/36
```

- **show license status**

  Shows the smart license status.

  The following example shows the status for an ASAv using regular smart software licensing:

```
ciscoasa# show license status

Smart Licensing is ENABLED
```

```
Registration:
  Status: REGISTERED
  Smart Account: ASA
  Virtual Account: ASAv Internal Users
  Export-Controlled Functionality: Not Allowed
  Initial Registration: SUCCEEDED on Sep 21 20:26:29 2015 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:28 2016 UTC
  Registration Expires: Sep 20 20:23:25 2016 UTC

License Authorization:
  Status: AUTHORIZED on Sep 23 01:41:26 2015 UTC
  Last Communication Attempt: SUCCEEDED on Sep 23 01:41:26 2015 UTC
  Next Communication Attempt: Oct 23 01:41:26 2015 UTC
  Communication Deadline: Dec 22 01:38:25 2015 UTC
```

The following example shows the status for an ASAv using permanent license reservation:

```
ciscoasa# show license status

Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: REGISTERED - UNIVERSAL LICENSE RESERVATION
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Jan 28 16:42:45 2016 UTC

License Authorization:
  Status: AUTHORIZED - RESERVED on Jan 28 16:42:45 2016 UTC

Licensing HA configuration error:
    No Reservation Ha config error
```

- **show license summary**

  Shows a summary of smart license status and usage.

  The following example shows the summary for an ASAv using regular smart software licensing:

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: ASA
  Virtual Account: ASAv Internal Users
  Export-Controlled Functionality: Not Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:29 2016 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Oct 23 01:41:26 2015 UTC

License Usage:
  License                Entitlement tag               Count Status
  -----------------------------------------------------------------------------
```

```
  regid.2014-08.com.ci... (ASAv-STD-1G)                    1 AUTHORIZED
```

The following example shows the summary for an ASAv using permanent license reservation:

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED - UNIVERSAL LICENSE RESERVATION
  Export-Controlled Functionality: Allowed

License Authorization:
  Status: AUTHORIZED - RESERVED
```

- **show license usage**

  Shows the smart license usage.

  The following example shows the usage for an ASAv:

```
ciscoasa# show license usage

License Authorization:
  Status: AUTHORIZED on Sep 23 01:41:26 2015 UTC

regid.2014-08.com.cisco.ASAv-STD-1G,1.0_4fd3bdbd-29ae-4cce-ad82-45ad3db1070c
(ASAv-STD-1G):
  Description: This entitlement tag was created via Alpha Extension application
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
```

Viewing the UDI

See the following command to view the universal product identifier (UDI):

show license udi

The following example shows the UDI for the ASAv:

```
ciscoasa# show license udi
UDI: PID:ASAv,SN:9AHV3KJBEKE
ciscoasa#
```

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 4100/9300 chassis—Device registration is configured in the chassis, not on the ASA 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 90 days. Normal license communication occurs every 30 days, but with the grace period, your device will stay compliant for up to 90 days without calling home. After the grace period, you should contact the Licensing Authority, or your ASAv will be out-of-compliance.

Firepower 2100

The Firepower 2100 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.

Firepower 4100/9300

The Firepower 4100/9300 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 is not affected.
- Firepower 2100—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.
- Firepower 4100/9300—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 4100/9300 chassis, Smart Call Home for licensing is configured in the Firepower 4100/9300 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.

Smart License Certificate Management

The ASA automatically creates a trustpoint containing the certificate of the CA that issued the Smart Call Home server certificate. To avoid service interruption if the issuing hierarchy of the server certificate changes,

configure the **auto-update** command to enable the automatic update of the trustpool bundle at periodic intervals.

The server certificate received from a Smart License Server must contain "ServAuth" in the Extended Key Usage field. This check will be done on non self-signed certificates only; self-signed certificates do not provide any value in this field.

History for Smart Software Licensing

Feature Name	Platform Releases	Description
Licensing changes for failover pairs on the Firepower 4100/9300 chassis	9.7(1)	Only the active unit requests the license entitlements. Previously, both units requested license entitlements. Supported with FXOS 2.1.1.
Permanent License Reservation for the ASAv Short String enhancement	9.6(2)	Due to an update to the Smart Agent (to 1.6.4), the request and authorization codes now use shorter strings. We did not modify any commands.
Satellite Server support for the ASAv	9.6(2)	If your devices cannot access the internet for security reasons, you can optionally install a local Smart Software Manager satellite server as a virtual machine (VM). We did not modify any commands.
Permanent License Reservation for the ASA on the Firepower 4100/9300 chassis	9.6(2)	For highly secure environments where communication with the Cisco Smart Software Manager is not allowed, you can request a permanent license for the ASA on the Firepower 9300 and Firepower 4100. All available license entitlements are included in the permanent license, including the Standard Tier, Strong Encryption (if qualified), Security Contexts, and Carrier licenses. Requires FXOS 2.0.1. All configuration is performed on the Firepower 4100/9300 chassis; no configuration is required on the ASA.
Permanent License Reservation for the ASAv	9.5(2.200) 9.6(2)	For highly secure environments where communication with the Cisco Smart Software Manager is not allowed, you can request a permanent license for the ASAv. In 9.6(2), we also added support for this feature for the ASAv on Amazon Web Services. This feature is not supported for Microsoft Azure. We introduced the following commands: **license smart reservation, license smart reservation cancel, license smart reservation install, license smart reservation request universal, license smart reservation return**

Feature Name	Platform Releases	Description
Smart Agent Upgrade to v1.6	9.5(2.200) 9.6(2)	The smart agent was upgraded from Version 1.1 to Version 1.6. This upgrade supports permanent license reservation and also supports setting the Strong Encryption (3DES/AES) license entitlement according to the permission set in your license account. **Note** If you downgrade from Version 9.5(2.200), the ASAv does not retain the licensing registration state. You need to re-register with the **license smart register idtoken** *id_token* **force** command; obtain the ID token from the Smart Software Manager. We introduced the following commands: **show license status, show license summary, show license udi, show license usage** We modified the following commands: **show license all, show tech-support license** We deprecated the following commands: **show license cert, show license entitlement, show license pool, show license registration**
Strong Encryption (3DES) license automatically applied for the ASA on the Firepower 9300	9.5(2.1)	For regular Cisco Smart Software Manager users, the Strong Encryption license is automatically enabled for qualified customers when you apply the registration token on the Firepower 9300. **Note** If you are using the Smart Software Manager satellite deployment, to use ASDM and other strong encryption features, after you deploy the ASA you must enable the Strong Encryption (3DES) license using the ASA CLI. This feature requires FXOS 1.1.3. We removed the following command for non-satellite configurations: **feature strong-encryption**
Validation of the Smart Call Home/Smart Licensing certificate if the issuing hierarchy of the server certificate changes	9.5(2)	Smart licensing uses the Smart Call Home infrastructure. When the ASA first configures Smart Call Home anonymous reporting in the background, it automatically creates a trustpoint containing the certificate of the CA that issued the Smart Call Home server certificate. The ASA now supports validation of the certificate if the issuing hierarchy of the server certificate changes; you can enable the automatic update of the trustpool bundle at periodic intervals. We introduced the following command: **auto-import**
New Carrier license	9.5(2)	The new Carrier license replaces the existing GTP/GPRS license, and also includes support for SCTP and Diameter inspection. For the ASA on the Firepower 9300, the **feature mobile-sp** command will automatically migrate to the **feature carrier** command. We introduced or modified the following commands: **feature carrier, show activation-key, show license, show tech-support, show version**

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**