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

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 4).

- ASAv5

- ASAv10

- ASAv30

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 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 4). 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 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 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.

Botnet Traffic Filter License

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

Failover or ASA Cluster Licenses

Failover Licenses for the ASAv

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

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

Each Firepower 4100/9300 chassis must be registered with the License Authority or satellite server. There is no extra cost for the secondary unit. For permanent license reservation, you must purchase separate licenses for each chassis.

Each ASA must have the same encryption license. For regular Smart Software Manager users, the Strong Encryption license is automatically enabled for qualified customers when you apply the registration token on the Firepower 4100/9300 chassis. For older Cisco Smart Software Manager satellite deployments, see below.

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

Each license type is managed as follows:

- Standard—Each unit includes the Standard license by default, so for a failover pair, 2 Standard licenses are requested from the server.

- Context—Each unit can request its own Context license. However, the Standard license includes 10 contexts by default and is present on both units. The value from each unit's Standard license plus the value of any optional Context licenses on both units are combined up to the platform limit. For example:

  - The Standard license includes 10 contexts; for 2 units, these licenses add up to 20 contexts.You configure a 250-Context license on the primary unit in an Active/Standby pair. Therefore, the aggregated failover license includes 270 contexts. However, because the platform limit for one unit is 250, the combined license allows a maximum of 250 contexts only. In this case, you should only configure the primary Context license to be 230 contexts.

- The Standard license includes 10 contexts; for 2 units, these licenses add up to 20 contexts. You configure a 10-Context license on the primary unit in an Active/Active pair, and a 10-Context license on the secondary unit. Therefore, the aggregated failover license includes 40 contexts. One unit can use 22 contexts and the other unit can use 18 contexts, for example, for a total of 40. Because the platform limit for one unit is 250, the combined license allows a maximum of 250 contexts; the 40 contexts are within the limit.

- Carrier—Only one unit needs to request this license, and both units can use it.

- Strong Encryption (3DES) (for a pre-2.3.0 Cisco Smart Software Manager satellite deployment only)—Each unit must request its own license from the server; unlike the other license configurations, this configuration is replicated to the standby unit. For Smart Software Manager satellite deployments, to use ASDM and other strong encryption features, after you deploy the cluster you must enable the Strong Encryption (3DES) license on the primary unit using the ASA CLI. The Strong Encryption (3DES) license is not available with any type of evaluation license.

ASA Cluster Licenses for the ASA on the Firepower 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

- Ensure internet access, or HTTP proxy access from the device.

- Configure a DNS server so the device can resolve the name of the License Authority.

- Set the clock for the device.

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

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

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

Firepower 4100/9300

Configure the Smart Software Licensing infrastructure on the Firepower 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 10). 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 4).

- 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
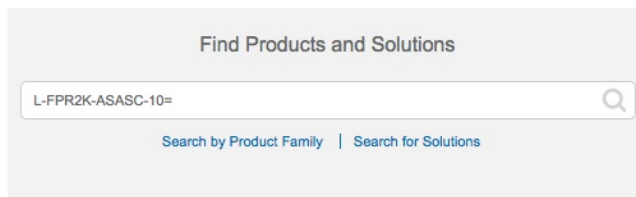
ASAv PIDs

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 4).

- ASAv5—L-ASAV5SR-K9=

- ASAv10—L-ASAV10SR-K9=

- ASAv30—L-ASAV30SR-K9=

- ASAv50—L-ASAV50SR-K9=

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).

- 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 4).

- 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.

- 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.

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

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

Step 2

Step 3

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

Cisco Software Central > Smart Software Licensing

Smart Software Licensing

Alerts | Inventory | License Conversion | Reports | Email Notification | Satellites | Activity

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.
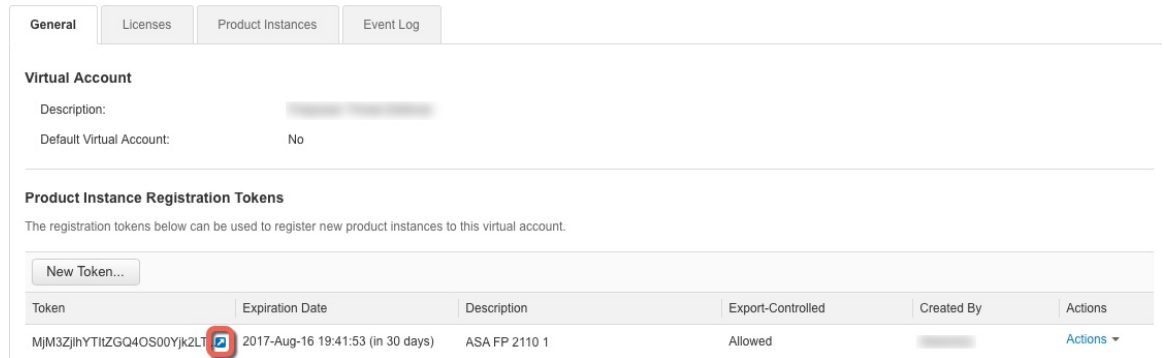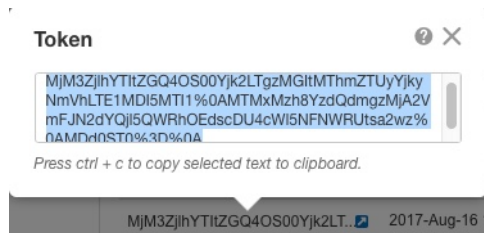
Figure 5: View Token

Figure 6: Copy Token

Step 2 (Optional) Specify the HTTP Proxy URL.

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.

a) Choose **Configuration** > **Device Management** > **Smart Call-Home**.
b) Check **Enable HTTP Proxy**.
c) Enter the proxy IP address and port in the **Proxy server** and **Proxy port** fields. For example, enter port 443 for an HTTPS server.
d) Click **Apply**.

Step 3 Configure the license entitlements.

a) Choose **Configuration** > **Device Management** > **Licensing** > **Smart Licensing**.
b) Check **Enable Smart license configuration**.
c) From the **Feature Tier** drop-down menu, choose **Standard**.

Only the standard tier is available.

d) From the **Throughput Level** drop-down menu, choose **100M**, **1G**, **2G**.

Note Do *not* check the **Enable strong-encryption protocol** check box. This setting is only for pre-2.3.0 satellite servers.

e) Click **Apply**.

Step 4 Register the ASAv with the License Authority.

a) Choose **Configuration** > **Device Management** > **Licensing** > **Smart Licensing**.
b) Click **Register**.
c) Enter the registration token in the **ID Token** field.

d) (Optional) Click the **Force registration** checkbox to register an ASAv that is already registered, but that might be out of sync with the License Authority.

For example, use **Force registration** if the ASAv was accidentally removed from the Smart Software Manager.

e) Click **Register**.

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

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) In ASDM, specify the HTTP Proxy URL.

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.

a) Choose **Configuration** > **Device Management** > **Smart Call-Home**.
b) Check **Enable HTTP Proxy**.
c) Enter the proxy IP address and port in the **Proxy server** and **Proxy port** fields. For example, enter port 443 for an HTTPS server.
d) Click **Apply**.

Step 3   Change the license server URL to go to the satellite server.

a) Choose **Configuration** > **Device Management** > **Smart Call-Home**.
b) In the **Configure Subscription Profiles** area, edit the **License** profile.
c) In the **Deliver Subscriptions Using HTTP transport** area, select the **Subscribers** URL, and click **Edit**.
d) Change the **Subscribers** URL to the following value, and click **OK**:

   https://*satellite_ip_address***/Transportgateway/services/DeviceRequestHandler**

e) Click **OK**, and then click **Apply**.

Step 4   Register the ASA with the License Authority.

a) Choose **Configuration** > **Device Management** > **Licensing** > **Smart Licensing**.
b) Click **Register**.
c) Enter the registration token in the **ID Token** field.
d) (Optional) Click the **Force registration** checkbox to register an ASA that is already registered, but that might be out of sync with the License Authority.

For example, use **Force registration** if the ASA was accidentally removed from the Smart Software Manager.

e) Click **Register**.

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. Choose **Monitoring > Properties > Smart License** to check the license status.

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 17

Step 2 (Optional) (Optional) Return the ASAv Permanent License, on page 19

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 19.

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}
```

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/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

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

Step 1   Choose **Configuration** > **Device Management** > **Licensing** > **Smart Licensing**.

Step 2   Click **Unregister**.

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   Choose **Configuration** > **Device Management** > **Licensing** > **Smart Licensing**.

Step 2   To renew the ID certificate, click **Renew ID Certificate**.

Step 3   To renew the license entitlement, click **Renew Authorization**.

Firepower 4100/9300: Configure Smart Software Licensing

This section describes how to configure Smart Software Licensing for the Firepower 4100/9300 chassis.

Procedure

Step 1 Firepower 4100/9300: Configure Pre-2.3.0 Satellite Smart Software Licensing, on page 21.For a chassis using a pre-2.3.0 satellite server, you must initally configure ASA licensing at the CLI; see the FXOS configuration guide to pre-configure license communication.

Step 2 Firepower 4100/9300: Configure Smart Software Licensing, on page 23

Firepower 4100/9300: Configure Pre-2.3.0 Satellite Smart Software Licensing

For a chassis using a pre-2.3.0 satellite server, you must initally configure ASA licensing at the CLI; see the FXOS configuration guide to pre-configure license communication.

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.

enable
configure terminal

Example:

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

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

show cluster info

Example:

```
asa(config)# show cluster info
Cluster stbu: On
  This is "unit-1-1" in state SLAVE
    ID : 0
    Version : 9.5(2)
    Serial No.: P3000000025
    CCL IP : 127.2.1.1
    CCL MAC : 000b.fcf8.c192
    Last join : 17:08:59 UTC Sep 26 2015
    Last leave: N/A
Other members in the cluster:
  Unit "unit-1-2" in state SLAVE
    ID : 1
    Version : 9.5(2)
    Serial No.: P3000000001
    CCL IP : 127.2.1.2
    CCL MAC : 000b.fcf8.c162
    Last join : 19:13:11 UTC Sep 23 2015
    Last leave: N/A
  Unit "unit-1-3" in state MASTER
    ID : 2
    Version : 9.5(2)
    Serial No.: JAB0815R0JY
    CCL IP : 127.2.1.3
    CCL MAC : 000f.f775.541e
    Last join : 19:13:20 UTC Sep 23 2015
    Last leave: N/A
```

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

Step 4   Enter license smart configuration mode:

license smart

Example:

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

Step 5   Set the feature tier:

feature tier standard

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

Step 6   Request one or more of the following features:

- 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).

- Strong Encryption (3DES/AES)

    feature strong-encryption

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.

Firepower 4100/9300: Configure Smart Software Licensing

This procedure applies for a chassis using the License Authority, for post-2.3.0 Satellite server users, or for Permanent License Reservation; see the FXOS configuration guide to pre-configure licensing communication. For pre-2.3.0 Satellite servers, you must initially configure licensing at the CLI. Satellite server Version 2.3.0 and later supports the Strong Encryption (3DES/AES) export-compliance token, so you can run ASDM before you request other license entitlements.

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 satellite server users, see Firepower 4100/9300: Configure Pre-2.3.0 Satellite Smart Software Licensing, on page 21 to configure licensing at the CLI.

Before you begin

For an ASA cluster, you need to access the primary unit for configuration. Check the Firepower Chassis Manager to see which unit is the primary.

Procedure

Step 1   In ASDM, choose **Configuration** > **Device Management** > **Licensing** > **Smart Licensing**.

Step 2   From the **Feature Tier** drop-down menu, choose **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 3 **For pre-2.3.0 satellite server users only:** Do not disable the **Strong Encryption** license; it is required for ASDM access.

Step 4 (Optional) Check **Carrier**.

Step 5 (Optional) From the **Context** drop-down menu, choose the number of contexts you want.

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

Step 6 Click **Apply**.

Step 7 Quit ASDM and relaunch it.

When you change licenses, you need to relaunch ASDM to show updated screens.

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
Carrier	Enabled
Total TLS Proxy Sessions	ASAv5: 500 ASAv10: 500 ASAv30: 1000
VPN Licenses	

Licenses	Standard License	
AnyConnect peers	Unlicensed	*Optional AnyConnect Plus or Apex license, Maximums:* *ASAv5: 50* *ASAv10: 250* *ASAv30: 750*
Other VPN Peers	ASAv5: 50 ASAv10: 250 ASAv30: 1000	
Total VPN Peers, combined all types	ASAv5: 50 ASAv10: 250 ASAv30: 1000	
General Licenses		
Throughput Level	ASAv5: 100 Mbps ASAv10: 1 Gbps ASAv30: 2 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	
RAM, vCPUs	ASAv5: 1 GB, 1 vCPU ASAv10: 2 GB, 1 vCPU ASAv30: 8 GB, 4 vCPUs	

Firepower 4100 Series ASA Application

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

Licenses	Standard License
Firewall Licenses	

Licenses	Standard License	
Botnet Traffic Filter	No Support.	
Firewall Conns, Concurrent	Firepower 4110: 10,000,000 Firepower 4120: 15,000,000 Firepower 4140: 25,000,000 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	
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.

Licenses	Standard License	
Firewall Conns, Concurrent	Firepower 9300 SM-44: 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	
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 followingscreen for viewing your license:

- **Configuration > Device Management > Licensing > Smart Licensing** pane and view the **Effective Running Licenses** area.

Viewing Smart License Status

See the following commands for viewing license status:

- **Monitoring > Properties > Smart License**

  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.

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#
```

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 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 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 **Automatic Import** area of the **Configuration** > **Remote Access VPN** > **Certificate Management** > **Trusted Certificate Pool** > **Edit Trusted Certificate Pool Policy** screen 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
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 screens.
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 screens.
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** No ASDM support.

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 **Configuration > Device Management > Licensing > Smart Licensing** page with the **Force registration** option; obtain the ID token from the Smart Software Manager. We did not change any screens.
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 modified the following screen: **Configuration** > **Device Management** > **Licensing** > **Smart License**
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 modified the following screen: **Configuration** > **Remote Access VPN** > **Certificate Management** > **Trusted Certificate Pool** > **Edit Trusted Certificate Pool Policy**
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 modified the following screen: **Configuration** > **Device Management** > **Licensing** > **Smart License**

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 modified the following screen: **Configuration** > **Device Management** > **Licensing** > **Smart License**
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 or modified the following screens: **Configuration > Device Management > Licensing > Smart License** **Configuration > Device Management > Smart Call-Home Monitoring > Properties > Smart License**