

Licenses: Smart Software Licensing

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 not supported on ASA hardware models and the ISA 3000. They 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 18
- Guidelines for Smart Software Licensing, on page 19
- Defaults for Smart Software Licensing, on page 19
- ASAv: Configure Smart Software Licensing, on page 19
- Firepower 4100/9300: Configure Smart Software Licensing, on page 32
- Other Models: Configure Smart Software Licensing, on page 33
- Licenses Per Model, on page 45
- Monitoring Smart Software Licensing, on page 56
- Smart Software Manager Communication, on page 57
- History for Smart Software Licensing, on page 59

About Smart Software Licensing

Cisco Smart Licensing is a flexible licensing model that provides you with an easier, faster, and more consistent way to purchase and manage software across the Cisco portfolio and across your organization. And it's secure—you control what users can access. With Smart Licensing you get:

- **Easy Activation:** Smart Licensing establishes a pool of software licenses that can be used across the entire organization—no more PAKs (Product Activation Keys).
- **Unified Management:** Cisco License Central provides a complete view into all of your Cisco products and services in an easy-to-use portal, so you always know what you have and what you are using.

- **License Flexibility:** Your license is not node-locked to your hardware, so you can easily use and transfer licenses as needed.

To use Smart Licensing, you must first set up a Smart Account on Cisco License Central.

For a more detailed overview on Cisco Licensing, visit the Licensing Hub.

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 Smart Software Manager. The Firepower 4100/9300 chassis itself does not require any licenses to operate. See the FXOS configuration guide for licensing procedures.

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 Smart Software Manager, you must 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 Smart Software Manager. As with

PAK licenses, you can purchase a license and install the license key for the ASA. Unlike a PAK license, you can obtain and manage the licenses with the Smart Software Manager. You can easily switch between regular smart licensing mode and permanent license reservation mode.

Note ASA does not support Specific License Reservation (SLR). In SLR, specific feature entitlements are enabled permanently. ASA supports only PLR, where all the features are enabled permanently.

ASA Virtual Permanent License Reservation

Note Permanent license reservation is supported only on VMware and KVM.

You can obtain a model-specific license that enables all of the following features:

- Maximum throughput for your model
- Standard tier
- Strong Encryption (3DES and AES) license, if you have enabled it in your Smart Licensing account
- AnyConnect Client capabilities enabled for the platform

Note Use of AnyConnect Client features is contingent on your purchase of the AnyConnect Client license that enables the right to use AnyConnect Client (see AnyConnect Plus, AnyConnect Apex, and AnyConnect VPN Only Licenses, on page 7).

Permanent License Reservation Mode Based on Memory and vCPU

You can configure a model-specific license based on the RAM and vCPUs assigned to your ASAv. For example, an ASAv with 8 GB RAM and 4 vCPUs always uses an ASAv30 license with 2G throughput.

The vCPU and memory-to-license relationships are as follows:

- 2 GB, 1 vCPU—ASAv10 (1G)
- 8 GB, 4 vCPUs —ASAv30 (2G)
- 16 GB, 8 vCPUs—ASAv50 (10G)
- 32 GB, 16 vCPUs—ASAv100 (20G)

Later, if you 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 Virtual Getting Started Guide* for these values.

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

For more information about configuring permanent license reservation, see ASAv: Configure Permanent License Reservation, on page 28.

Firepower 1010 Permanent License Reservation

You can obtain a license that enables all features:

- Standard tier
- Security Plus
- Strong Encryption (3DES/AES) license if your account qualifies
- AnyConnect Client capabilities enabled to the platform maximum.

  Use of AnyConnect Client features is contingent on your purchase of the AnyConnect Client license that enables the right to use AnyConnect Client (see AnyConnect Plus, AnyConnect Apex, and AnyConnect VPN Only Licenses, on page 7).



Note 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 1100 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
- AnyConnect Client capabilities enabled to the platform maximum.

  Use of AnyConnect Client features is contingent on your purchase of the AnyConnect Client license that enables the right to use AnyConnect Client (see AnyConnect Plus, AnyConnect Apex, and AnyConnect VPN Only Licenses, on page 7).



Note 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 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
- AnyConnect Client capabilities enabled to the platform maximum.

  Use of AnyConnect Client features is contingent on your purchase of the AnyConnect Client license that enables the right to use AnyConnect Client (see AnyConnect Plus, AnyConnect Apex, and AnyConnect VPN Only Licenses, on page 7).



Note 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
- AnyConnect Client capabilities enabled to the platform maximum.

  Use of AnyConnect Client features is contingent on your purchase of the AnyConnect Client license that enables the right to use AnyConnect Client (see AnyConnect Plus, AnyConnect Apex, and AnyConnect VPN Only Licenses, on page 7).



Note 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. To manage the license, see the FXOS configuration guide.

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 don't pay for unused licenses.

Smart Software Manager On-Prem

If your devices cannot access the internet for security reasons, you can optionally install a local Smart Software Manager On-Prem (formerly known as "Smart Software Satellite Server") server as a virtual machine (VM).

The Smart Software Manager On-Prem provides a subset of Smart Software Manager functionality, and allows you to provide essential licensing services for all your local devices. Only the Smart Software Manager On-Prem needs to connect periodically to the main Smart Software Manager to sync your license usage. You can sync on a schedule or you can sync manually.

You can perform the following functions on the Smart Software Manager On-Prem:

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

For more information, see Cisco Smart Software Manager On-Prem Data Sheet.

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 Smart Software Manager, it operates in a severely rate-limited state.

Firepower 1000

Before the Firepower 1000 registers with the Smart Software Manager, it operates for 90 days (total usage) in evaluation mode. Only default entitlements are enabled. When this period ends, the Firepower 1000 becomes out-of-compliance.

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

Firepower 2100

Before the Firepower 2100 registers with the Smart Software Manager, 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 Smart Software Manager 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 Smart Software Manager, 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 Smart Software Manager, 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 Smart Software Manager 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 AnyConnect VPN Only Licenses

AnyConnect Client licenses are not applied directly to the ASA. However, you need to purchase licenses and add them to your Smart Account to guarantee the right to use the ASA as the AnyConnect Client headend.

- For the AnyConnect Plus and AnyConnect Apex licenses, add up the number of peers you intend to use across all the ASAs in your Smart Account and purchase license(s) for that many peers.
- For the AnyConnect VPN Only, purchase one license per ASA. Unlike the other licenses that provide a pool of peers that can be shared by multiple ASAs, the AnyConnect VPN Only license is per headend.

For more information, see:

- Cisco AnyConnect Client Ordering Guide
- AnyConnect Client Licensing Frequently Asked Questions (FAQ)

Other VPN Peers

Other VPN peers 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 Peers Combined, All Types

- The Total VPN Peers is the maximum VPN peers allowed of both AnyConnect Client and Other VPN peers combined. For example, if the total is 1000, you can allow 500 AnyConnect Client and 500 Other VPN peers simultaneously; or 700 AnyConnect Client and 300 Other VPN; or use all 1000 for AnyConnect Client. If you exceed the total VPN peers, you can overload the ASA, so be sure to size your network appropriately.
- If you start a clientless SSL VPN session and then start the 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 Smart Software Manager or Smart Software Manager On-Prem server, so you can launch ASDM and connect to the Smart Software Manager. For through-the-box traffic that requires strong encryption (such as VPN), throughput is severely limited until you connect to the Smart Software Manager 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.

If your Smart Account is not authorized for strong encryption, but Cisco has determined that you are allowed to use strong encryption, you can manually add a strong encryption license to your account.

Strong Encryption: Firepower 1000, Firepower 2100 in Appliance Mode

The ASA includes 3DES capability by default for management access only, so you can connect to the Smart Software Manager and also use ASDM immediately. You can also use SSH and SCP if you later configure SSH access on the ASA. Other features that require strong encryption (such as VPN) must have Strong Encryption enabled, which requires you to first register to the Smart Software Manager.

Note If you attempt to configure any features that can use strong encryption before you register—even if you only configure weak encryption—then your HTTPS connection will be dropped on that interface, and you cannot reconnect. The exception to this rule is if you are connected to a management-only interface, such as Management 1/1. SSH is not affected. If you lose your HTTPS connection, you can connect to the console port to reconfigure the ASA, connect to a management-only interface, or connect to an interface not configured for a strong encryption feature.

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.

If your Smart Account is not authorized for strong encryption, but Cisco has determined that you are allowed to use strong encryption, you can manually add a strong encryption license to your account.

Note Reloading a device with an expired licensing registration for over a year, will disable the export-controlled functionality. This can lead to critical issues such as VPN downtime or failover split-brain scenarios when IPsec encryption is enabled.

Strong Encryption: Firepower 2100 in Platform Mode

Strong Encryption (3DES/AES) is available for management connections before you connect to the Smart Software Manager or Smart Software Manager On-Prem 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 that requires strong encryption (such as VPN) 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.

If your Smart Account is not authorized for strong encryption, but Cisco has determined that you are allowed to use strong encryption, you can manually add a strong encryption license to your account.

Strong Encryption: Firepower 4100/9300 Chassis

When the ASA is deployed as a logical device, you can launch ASDM immediately. Through the box traffic that requires strong encryption (such as VPN) is not allowed until you connect and obtain the Strong Encryption license.

When you request the registration token for the 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.

If your Smart Account is not authorized for strong encryption, but Cisco has determined that you are allowed to use strong encryption, you can manually add a strong encryption license to your account.

DES: All Models

If you have Strong Encryption enabled, you cannot use DES.

Carrier License

The Carrier license enables the following inspection features:

- Diameter—Diameter is an Authentication, Authorization, and Accounting (AAA) protocol used in next-generation mobile and fixed telecom networks such as EPS (Evolved Packet System) for LTE (Long Term Evolution) and IMS (IP Multimedia Subsystem). It replaces RADIUS and TACACS in these networks.
- GTP/GPRS—GPRS Tunneling Protocol is used in GSM, UMTS and LTE networks for general packet radio service (GPRS) traffic. GTP provides a tunnel control and management protocol to provide GPRS network access for a mobile station by creating, modifying, and deleting tunnels. GTP also uses a tunneling mechanism for carrying user data packets.
- M3UA—MTP3 User Adaptation (M3UA) is a client/server protocol that provides a gateway to the SS7 network for IP-based applications that interface with the SS7 Message Transfer Part 3 (MTP3) layer. M3UA makes it possible to run the SS7 User Parts (such as ISUP) over an IP network. M3UA is defined in RFC 4666.
- SCTP—SCTP (Stream Control Transmission Protocol) is described in RFC 4960. The protocol supports the telephony signaling protocol SS7 over IP and is also a transport protocol for several interfaces in the 4G LTE mobile network architecture.

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 Firepower 1010

Smart Software Manager Regular and On-Prem

Both Firepower 1010 units must be registered with the Smart Software Manager or Smart Software Manager On-Prem server. Both units require you to enable the Standard license and the Security Plus license *before* you can configure failover.

Typically, you do not also need to enable the Strong Encryption (3DES/AES) feature license in the ASA, because both units should have obtained the Strong Encryption token when you registered the units. When using the registration token, both units must have the same encryption level.

If your Smart Account is not authorized for strong encryption, but Cisco has determined that you are allowed to use strong encryption, you can manually add a strong encryption license to your account. In this case, enable it on the active unit after you enable failover. 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 license from the server. The license is 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. 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, and you are not using the Strong Encryption token, then you will not be able to make configuration changes to features requiring the Strong Encryption (3DES/AES) feature license; 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 Firepower 1100

Smart Software Manager Regular and On-Prem

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:
  - Active/Standby: The Standard license includes 2 contexts; for two Firepower 1120 units, these licenses add up to 4 contexts. You configure a 3-Context license on the active unit in an Active/Standby pair. Therefore, the aggregated failover license includes 7 contexts. However, because the platform limit for one unit is 5, the combined license allows a maximum of 5 contexts only. In this case, you might only configure the active Context license to be 1 context.
  - Active/Active: The Standard license includes 2 contexts; for two Firepower 1140 units, these licenses add up to 4 contexts. You configure a 4-Context license on the primary unit in an Active/Active pair. Therefore, the aggregated failover license includes 8 contexts. One unit can use 5 contexts and the other unit can use 3 contexts, for example; but during a failure, one unit will use all 8. Because the platform limit for one unit is 10, the combined license allows a maximum of 10 contexts; the 8 contexts are within the limit.
- Strong Encryption (3DES/AES)—If your Smart Account is not authorized for strong encryption, but Cisco has determined that you are allowed to use strong encryption, you can manually add a strong encryption license to your account. 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 Firepower 2100

Smart Software Manager Regular and On-Prem

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:
  - Active/Standby: 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.

- Active/Active: 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; but during a failure, one unit will use all 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)—If your Smart Account is not authorized for strong encryption, but Cisco has determined that you are allowed to use strong encryption, you can manually add a strong encryption license to your account. 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 Firepower 4100/9300

Smart Software Manager Regular and On-Prem

Both Firepower 4100/9300 must be registered with the Smart Software Manager or Smart Software Manager On-Prem 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:

  - Active/Standby: 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.
  - Active/Active: 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; but during a failure, one unit will use all 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)—If your Smart Account is not authorized for strong encryption, but Cisco has determined that you are allowed to use strong encryption, you can manually add a strong encryption license to your account. 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 Firepower 4100/9300

Smart Software Manager Regular and On-Prem

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 Smart Software Manager Regular and On-Prem server. There is no extra cost for data 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.

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, and both units can use it due to license aggregation.
- 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 4112 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.
- Strong Encryption (3DES)—For pre-2.3.0 Cisco Smart Software Manager On-Prem deployment; or if your Smart Account is not authorized for strong encryption, but Cisco has determined that you are allowed to use strong encryption, you can manually add a strong encryption license to your account. 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.

Permanent License Reservation

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

Prerequisites for Smart Software Licensing

Smart Software Manager Regular and On-Prem Prerequisites

Firepower 4100/9300

Configure the Smart Software Licensing infrastructure on the Firepower 4100/9300 chassis before you configure the ASA licensing entitlements.

All Other Models

- Ensure internet access, or HTTP proxy access, or Smart Software Manager On-Prem server access from the device.
- Configure a DNS server so the device can resolve the name of the Smart Software Manager.
- Set the clock for the device. On the Firepower 2100 in Platform mode, you set the clock in FXOS.
- Create an 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 an account for your organization.

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. 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. The AnyConnect Client capabilities are also enabled to the platform maximum, contingent on your purchase of an AnyConnect Client license that enables the right to use AnyConnect Client (see AnyConnect Plus, AnyConnect Apex, and AnyConnect VPN Only Licenses, on page 7).
- ASAv: Permanent license reservation is not supported for the Azure hypervisor.

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

Smart Call Home Profile

The default configuration for all models except the Firepower 4100/9300 (which enables Smart Software License communication at the chassis-level) includes a Smart Call Home profile called "License" that specifies the URL for the Smart Software Manager.

ASAv

- 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.

ASAv: Configure Smart Software Licensing

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

ASAv: Configure Regular Smart Software Licensing

When you deploy ASAv, you can pre-configure the device and include a registration token so it registers with the Smart Software Manager 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.



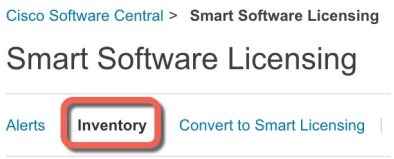
Note You may have pre-configured the HTTP proxy and license entitlements when you deployed your ASAv. You may also have included the registration token with your Day0 configuration when you deployed the ASAv; if so, you do not need to re-register using this procedure.

Procedure

Step 1 (Cisco Smart Software Manager), request and copy a registration token for the virtual account to which you want to add this device.

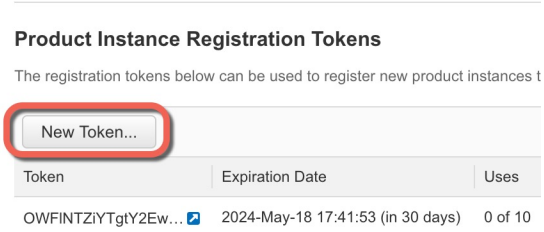
a) Click **Inventory**.

Figure 1: Inventory



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

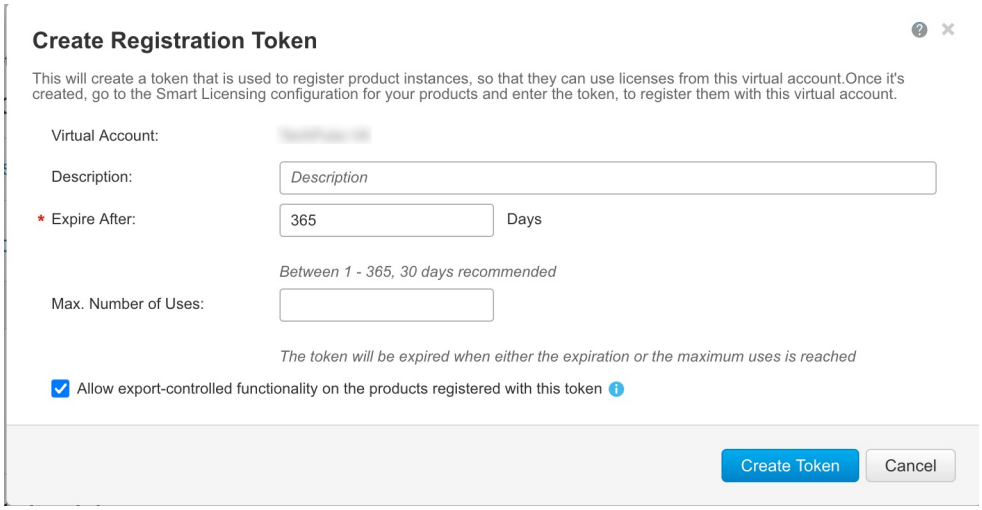
Figure 2: New Token



c) On the **Create Registration Token** dialog box enter the following settings, and then click **Create Token**:

- **Description**
- **Expire After**—Cisco recommends 30 days.
- **Max. Number of Uses**
- **Allow export-controlled functionaility on the products registered with this token**—Enables the export-compliance flag.

Figure 3: 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 4: View Token

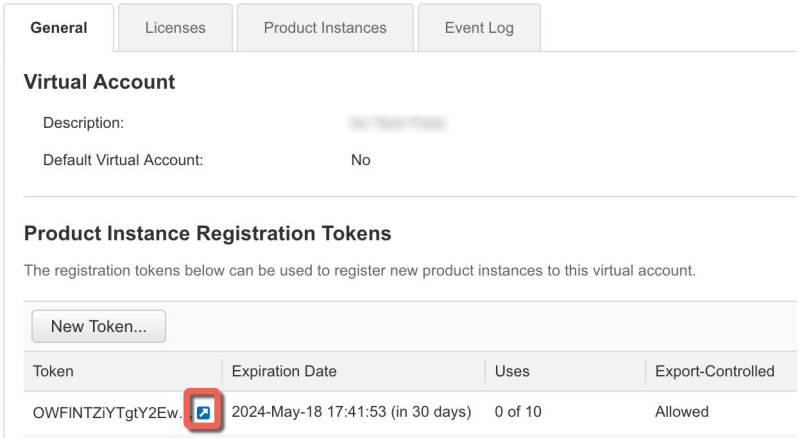
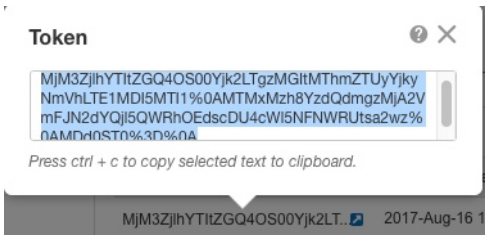


Figure 5: Copy Token



Step 2 (Optional) On the ASA, specify the HTTP Proxy URL for Call Home:

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.

Note
HTTP proxy with authentication is not supported.

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 the **Enable Smart license configuration** check box.
c) From the **Feature Tier** drop-down list, choose **Standard**.

Only the Standard tier is available, however, you need to enable it in the configuration.

d) From the **Throughput Level** drop-down list, choose one of the following: **100M**, **1G**, **2G**, **10G**, **20G**.

See the following throughput/license relationship:

- 100M—ASAv5
- 1G—ASAv10
- 2G—ASAv30
- 10G—ASAv50
- 20G—ASAv100

e) (Optional) Check the **Enable strong-encryption protocol** check box. **Do not** check this box if you receive the strong encryption token.

This license is not required if you receive the strong encryption token from the Smart Software Manager. However, if your Smart Account is not authorized for strong encryption, but Cisco has determined that you are allowed to use strong encryption, you can manually add a strong encryption license to your account. Only the active unit requests this license, and both units can use it due to license aggregation.

f) Click **Apply**.

Step 4 Register the ASAv with the Smart Software Manager.

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** check box to register the ASAv that is already registered, if it is out of sync with the Smart Software Manager.

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 Smart Software Manager and request authorization for the configured license entitlements.

When you register the ASAv, the Smart Software Manager issues an ID certificate for communication between the ASAv and the Smart Software Manager. 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. For example, the ID certificate expires because of a communication problem.

ASAv: Configure Smart Software Manager On-Prem Licensing

This procedure applies for the ASAv using a Smart Software Manager On-Prem.

Before you begin

- Download the Smart Software Manager On-Prem OVA file from Cisco.com and install and configure it on a VMwareESXi server. For more information, see the *Cisco Smart Software Manager On-Prem Data Sheet*.
- Download the crypto CA trustpool before you place the device in an air-gapped network. This trustpool is normally downloaded automatically, but may be out of date in an air-gapped network:

  crypto ca trustpool import url http://www.cisco.com/security/pki/trs/ios_core.p7b

Procedure

Step 1 Request a registration token on the Smart Software Manager On-Prem.

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

Note
HTTP proxy with authentication is not supported.

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 Smart Software Manager On-Prem.

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://*on-prem_ip_address***/Transportgateway/services/DeviceRequestHandler**

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

Step 4 On the ASAv, 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, however, you need to enable it in the configuration.

d) To determine the license requested from the Smart Software Manager, from the **Throughput Level** drop-down list, choose one of the following: **100M**, **1G**, **2G**, **10G**, **20G**.

See the following throughput/license relationship:

- 100M—ASAv5
- 1G—ASAv10
- 2G—ASAv30
- 10G—ASAv50
- 20G—ASAv100

e) (Optional) Check the **Enable strong-encryption protocol** check box. **Do not** check this box if you receive the strong encryption token.

This license is not required if you receive the strong encryption token from the Smart Software Manager. However, if your Smart Account is not authorized for strong encryption, but Cisco has determined that you are allowed to use strong encryption, you can manually add a strong encryption license to your account. Only the active unit requests this license, and both units can use it due to license aggregation.

f) Click **Apply**.

Step 5 Register the ASA with the Smart Software Manager.

a) Choose **Configuration** > **Device Management** > **Licensing** > **Smart Licensing**.
b) Click **Register**.
c) Enter the registration token in the **ID Token** field.
d) (Optional) Check the **Force registration** check box to register an ASA that is already registered, if it is out of sync with the Smart Software Manager.

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

e) Click **Register**.

The ASA registers with the Smart Software Manager and requests authorization for the configured license entitlements. The Smart Software Manager also applies the Strong Encryption (3DES/AES) license if your account allows. Choose **Monitoring > Properties > Smart License** to check the license status.

When you register the ASAv, the Smart Software Manager issues an ID certificate for communication between the ASAv and the Smart Software Manager. 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.

ASAv: Configure Utility (MSLA) Smart Software Licensing

Utility Licensing for a Managed Service License Agreement (MSLA) lets you pay for the amount of time a license is in use rather than paying a one time charge for a license subscription or a perpetual license. In Utility Licensing mode, the ASAv keeps track of license usage in units of time (15-minute intervals). The ASAv sends license usage reports (known as RUM reports) to the Smart Software Manager every four hours. The

usage reports are then forwarded to a billing server. With Utility Licensing, Smart Call Home is not used as the transport for licensing messages. Instead the messages are sent directly via HTTP/HTTPS using *Smart Transport.*

Before you begin

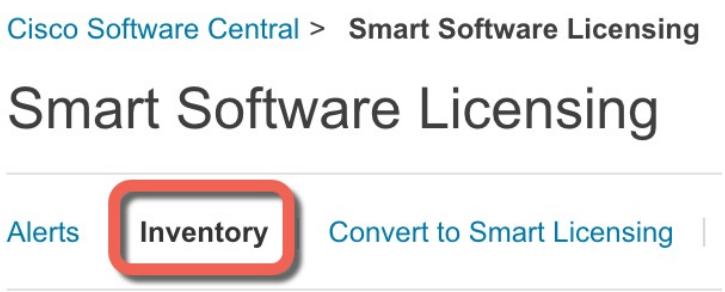
Download the Smart Software Manager On-Prem OVA file from Cisco.com and install and configure it on a VMware ESXi server. For more information, see the *Cisco Smart Software Manager On-Prem Data Sheet*.

Procedure

Step 1 In the Smart Software Manager On-Prem, request and copy a registration token for the virtual account to which you want to add this device.

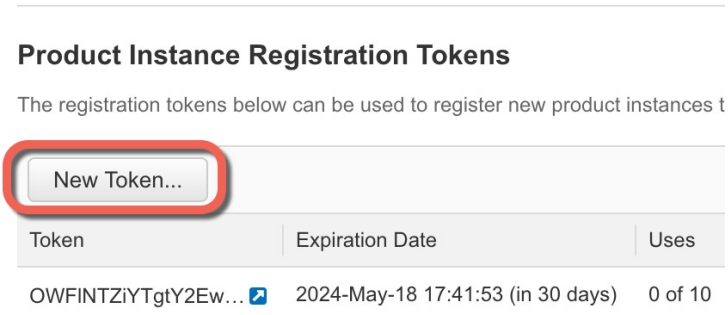
a) Click **Inventory**.

Figure 6: Inventory



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

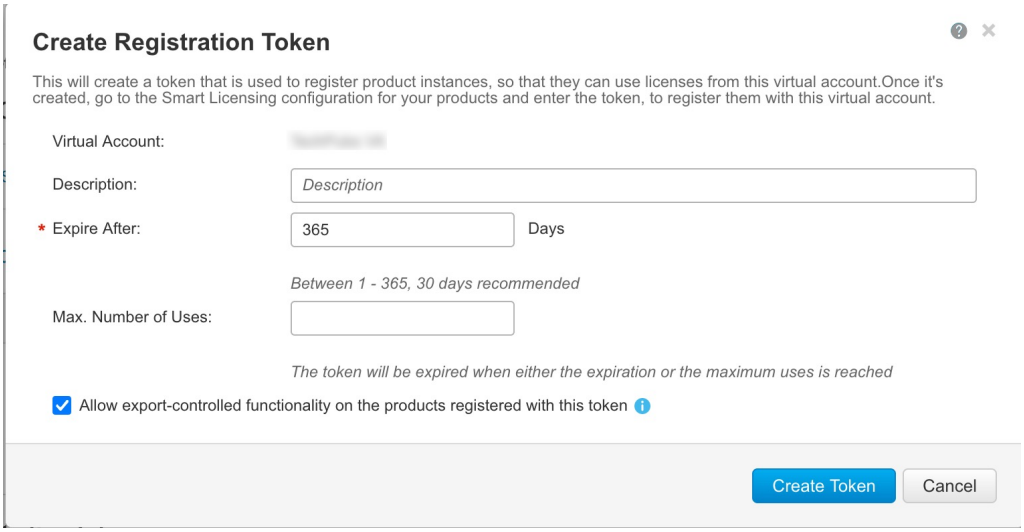
Figure 7: New Token



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 8: 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 9: View Token

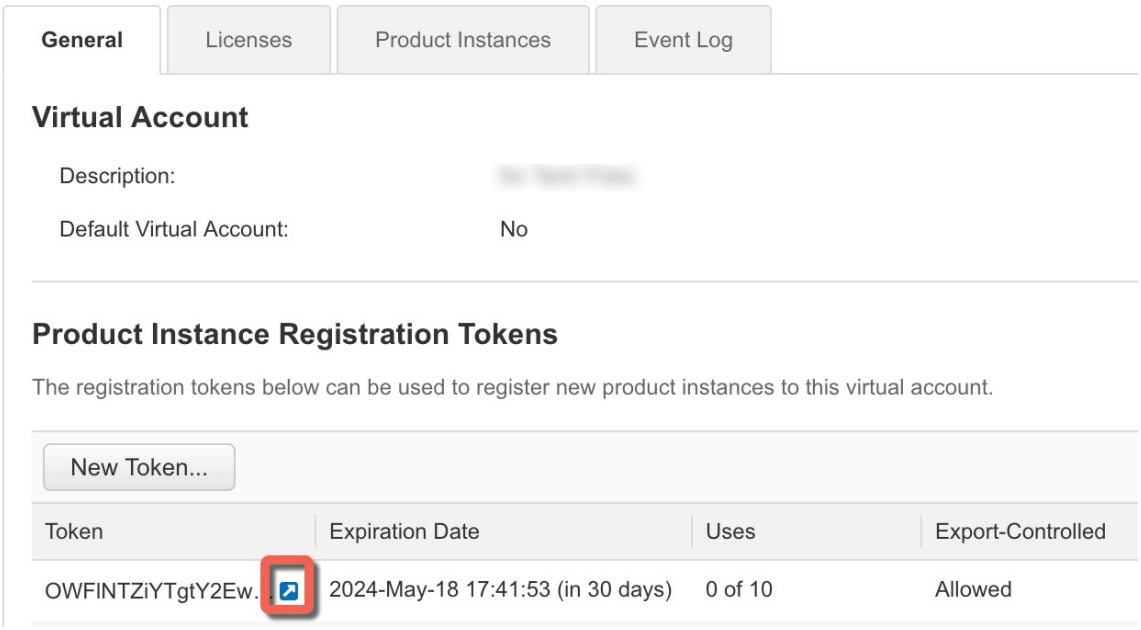
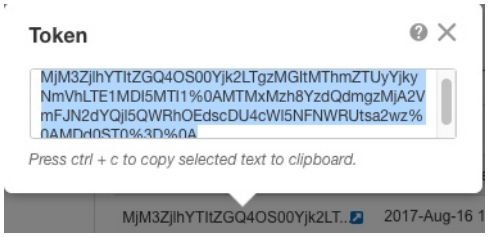


Figure 10: Copy Token



Step 2 Choose **Configuration** > **Device Management** > **Licensing** > **Smart Licensing**.

Step 3 Configure the license entitlements:

a) Check the **Enable Smart license configuration** check box.

b) From the **Feature Tier** drop-down menu, choose **Standard**.

Only the **Standard** tier is available, however, you need to enable it in the configuration.

c) To determine the license requested from the Smart Software Manager, from the **Throughput Level** drop-down list, choose one of the following: **100M**, **1G**, **2G**, **10G**, **20G**.

See the following throughput and license relationship:

- 100M—ASAv5
- 1G—ASAv10
- 2G—ASAv30
- 10G—ASAv50
- 20G—ASAv100

d) (Optional) Check the **Enable strong-encryption protocol** check box.

This license is not required if you receive the strong encryption token from the Smart Software Manager. However, if your Smart Account is not authorized for strong encryption, but Cisco has determined that you are allowed to use strong encryption, you can manually add a strong encryption license to your account. Only the active unit requests this license, and both units can use it due to license aggregation.

Step 4 (Optional) If you want to suppress the licensing device's hostname or Smart Agent version number in the licensing messages, check the following check boxes:

a) **Host Name**.

b) **Version**.

Step 5 Click the **Smart Transport** radio button.

Step 6 Configure the URLs for Smart Transport.

a) Click the **Custom URL** radio button and enter the URL in the **URL** field.

b) In the **Registration** field, paste the Smart Software Manager Regular or On-Prem registration token.

c) In the **Utility** field, specify the URL of the Smart Software Manager Regular or On-Prem.

d) (Optional) In the **Proxy URL** field, specify the URL of the proxy if the licensing server or satellite is only reachable via a proxy.

Note
HTTP proxy with authentication is not supported.

e) (Optional) In the **Proxy Port** field, specify the proxy port number.

Step 7 Check the **Enable Standard Utility Mode** check box.

Step 8 Configure the utility licensing information, which includes customer information necessary for billing purposes.

a) In the **Custom ID** field, specify a unique customer identifier. This identifier is included in Utility Licensing usage report messages.

b) Complete the customer profile by entering the appropriate information in the remaining fields, including **Customer Company Identifier**, **Customer Company Name**, **Customer Street**, **Customer City**, **Customer State**, **Customer Country**, and **Customer Postal Code**.

Step 9 Click **Apply**.

Step 10 Click **Register** to register the ASAv with the Smart Software Manager Regular or On-Prem.

The ASA registers with the Smart Software Manager and requests authorization for the configured license entitlements. Choose **Monitoring > Properties > Smart License** to check the license status.

ASAv: Configure Permanent License Reservation

You can assign a permanent license to the 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 28

Step 2 (Optional) Return the ASAv Permanent License, on page 30

Install the ASAv Permanent License

For an ASAv that does not have internet access, you can request a permanent license from the Smart Software Manager. For more information about ASAv permanent license reservation, see ASA Virtual Permanent License Reservation, on page 3.

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 30.
- If you clear your configuration after you install the permanent license, for example, by using the **write erase** command, you only have to re-enable permanent license reservation using the **license smart reservation** command without any arguments, you do not need to complete the rest of this procedure.

Before you begin

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

license smart reservation

Example:

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

To use regular smart licensing, use the **no** form of this command.

The following commands are removed:

```
license smart
  feature tier standard
  throughput level {100M | 1G | 2G | 10G | 20G}
```

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#
```

If you change the memory or vCPUs, you will have to return the current license and request a new license at the new model level. The license requested must match the installed memory and vCPUs. For more information about the vCPU and memory-to-license matrix for ASAv permanent license reservation, see ASA Virtual Permanent License Reservation, on page 3.

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 30.

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 enter the ASAv code in the **Reservation Request Code** field.

Step 5 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 6 From the ASAv CLI, run the following command and enter the authorization code:

license smart reservation install *code*

Example:

```
ciscoasa# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
INFO: ASAv platform license state is Licensed.
ciscoasa#
```

Your ASAv is now fully licensed.

Step 7 Run this command to save the running configuration to the startup configuration to avoid any loss of configuration during reboot.

write memory

Step 8 From the ASAv, run this command to display and confirm that the ASA has the permanent license.

show license features

(Optional) Return the ASAv Permanent License

If you no longer need a permanent license, for example, you are retiring the ASAv or changing its model level, because of which 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 the steps, the license stays in a used state and cannot be freed up for use elsewhere.

Procedure

Step 1 From the ASAv CLI, 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 enter the ASAv return code in the **Reservation Return Code** field.

The permanent license is returned to the available pool.

Step 5 Click **Remove Product Instance**.

Step 6 To disable permanent license reservation, do the following:

a) Run the following command to disable permanent license reservation:

no license smart reservation

b) Run the following command to confirm that the license is deregistered:

show license features

The command output shows `No active entitlement`.

Step 7 Run this command to save the running configuration to the startup configuration to avoid any loss of configuration during reboot.

write memory

(Optional) Deregister the ASAv (Regular and On-Prem)

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.

Note If you deregister the ASAv, then it will revert to a severely rate-limited state after you reload the ASAv.

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 On-Prem)

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 procedure applies for a chassis using the Smart Software Manager, Smart Software Manager On-Prem, or for Permanent License Reservation; see the FXOS configuration guide to pre-configure licensing communication.

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.

Before you begin

For an ASA cluster, you need to access the control node for configuration. Check the Firewall Chassis Manager to see which node is the control node.

Procedure

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

Step 2 From the **Feature Tier** drop-down list, 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 (Optional) Check the **Enable strong-encryption protocol** check box. **Do not** check this box if you receive the strong encryption token.

This license is not required if you receive the strong encryption token from the Smart Software Manager. However, if your Smart Account is not authorized for strong encryption, but Cisco has determined that you are allowed to use strong encryption, you can manually add a strong encryption license to your account. Only the active unit requests this license, and both units can use it due to license aggregation.

Step 4 (Optional) Check the **Carrier** check box.

Step 5 (Optional) From the **Context** drop-down list, 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.

Other Models: Configure Smart Software Licensing

This section describes how to configure Smart Software Licensing for the following models:

- Firepower 1010
- Firepower 1100
- Firepower 2100

Choose one of the following methods:

- Other Models: Configure Regular Smart Software Licensing, on page 34

  You can also (Optional) Other Models: Deregister the ASA (Regular and On-Prem), on page 45 or (Optional) Other Models: Renew the ASA ID Certificate or License Entitlement (Regular and On-Prem), on page 45.

- Other Models: Configure Smart Software Manager On-Prem Licensing, on page 38

  You can also (Optional) Other Models: Deregister the ASA (Regular and On-Prem), on page 45 or (Optional) Other Models: Renew the ASA ID Certificate or License Entitlement (Regular and On-Prem), on page 45.

• Other Models: Configure Permanent License Reservation, on page 41

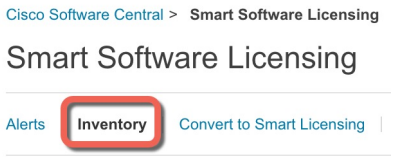
Other Models: Configure Regular Smart Software Licensing

This procedure applies for an ASA using the Smart Software Manager.

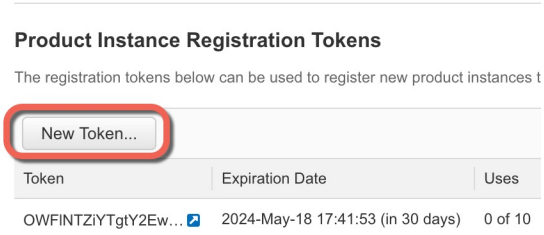
Procedure

Step 1 In the Cisco Smart Software Manager, request and copy a registration token for the virtual account to which you want to add this device.

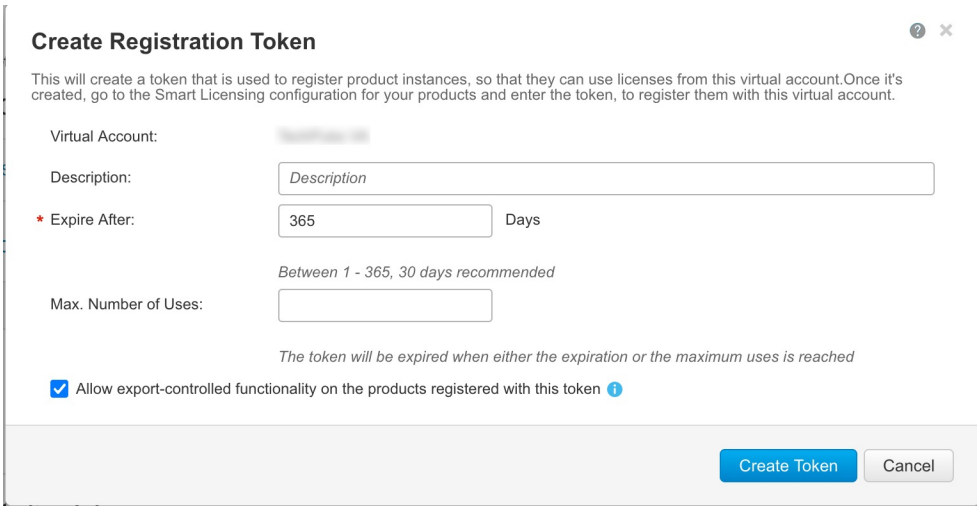
a. Click **Inventory**.



b. On the **General** tab, click **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.
- **Max. Number of Uses**
- **Allow export-controlled functionaility on the products registered with this token**—Enables the export-compliance flag.

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 11: View token

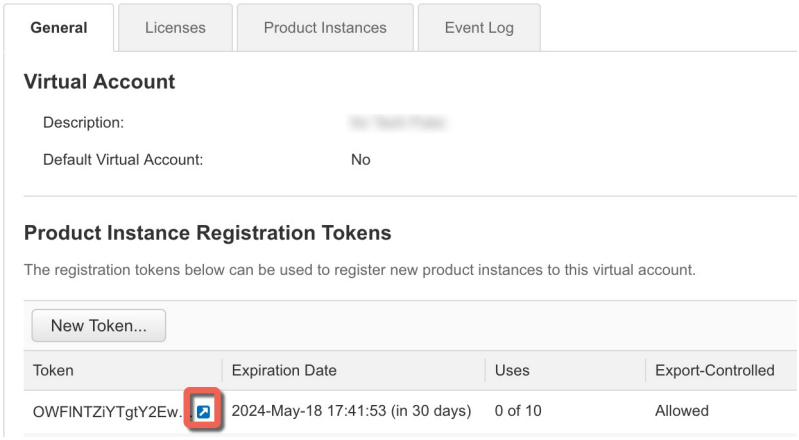
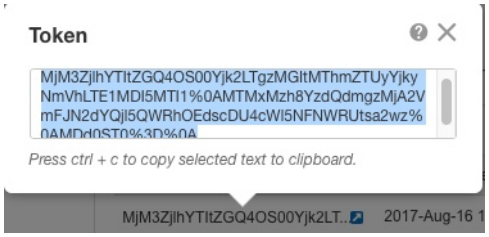


Figure 12: Copy token



Step 2 (Optional) On the ASA, specify the HTTP Proxy URL for Call Home:

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.

Note
HTTP proxy with authentication is not supported.

a) Choose **Configuration** > **Device Management** > **Smart Call-Home**.
b) Check the **Enable HTTP Proxy** check box.
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 the **Enable Smart license configuration** check box.
c) From the **Feature Tier** drop-down menu, choose **Standard**.

   Only the **Standard** tier is available, however, you need to enable it in the configuration; a tier license is a prerequisite for adding other feature licenses.

d) (Optional) (Firepower 1010) Check the **Enable Security Plus** check box.

   The Security Plus tier enables failover.

e) (Optional) (Supported models) For the **Context** license, enter the number of contexts.

   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 1120—5 contexts
   - Firepower 1140—10 contexts
   - Firepower 1150—25 contexts
   - Firepower 2110—25 contexts
   - Firepower 2120—25 contexts
   - Firepower 2130—30 contexts
   - Firepower 2140—40 contexts

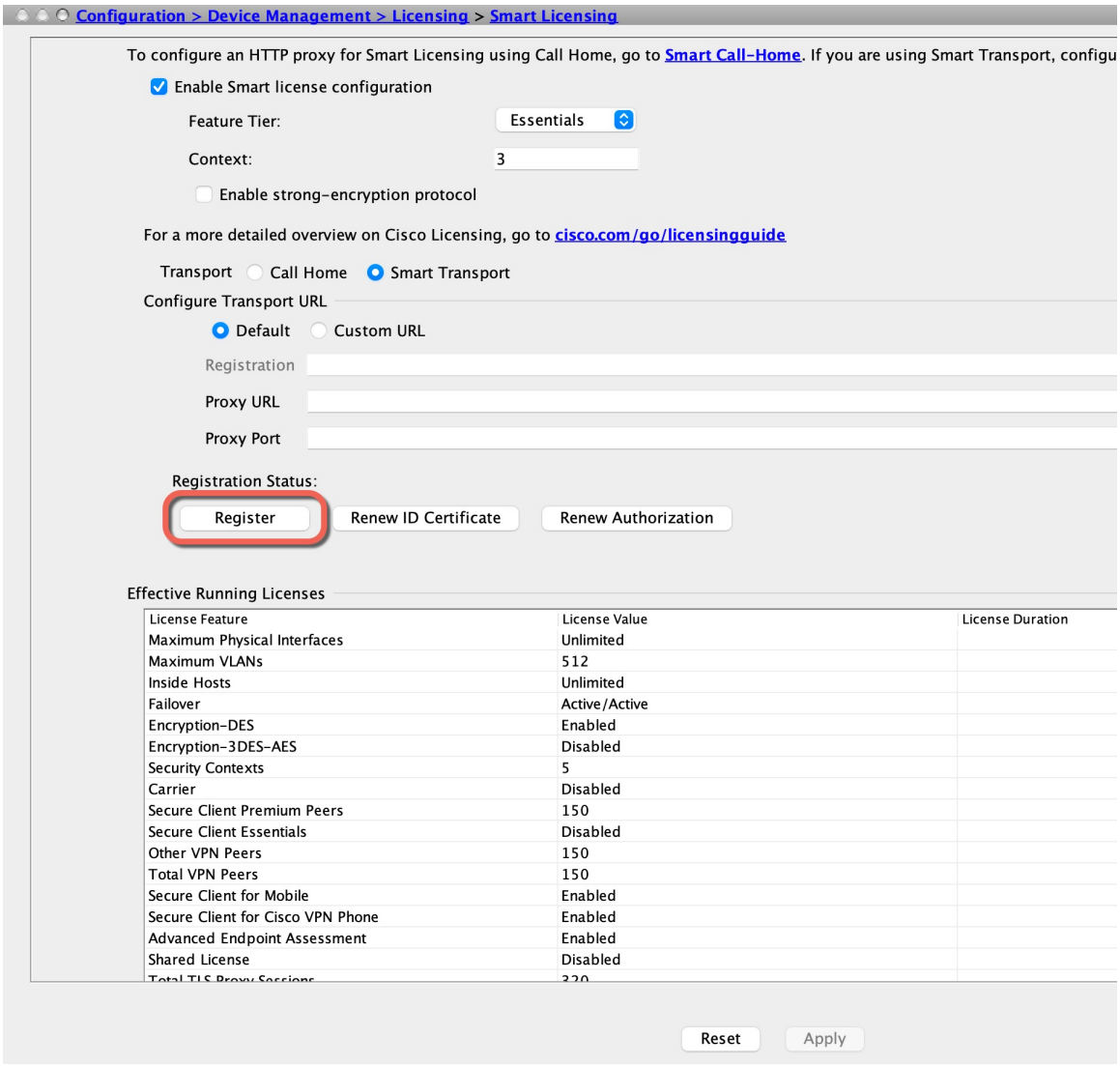
   For example, to use the maximum of 25 contexts on the Firepower 1150, enter 23 for the number of contexts; this value is added to the default of 2.

f) (Optional) Check the **Enable strong-encryption protocol** check box. **Do not** check this box if you receive the strong encryption token.

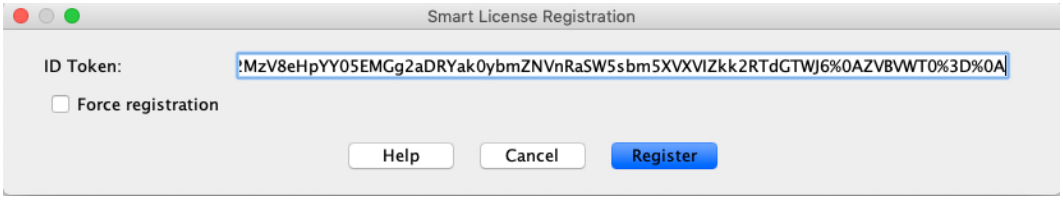
   This license is not required if you receive the strong encryption token from the Smart Software Manager. However, if your Smart Account is not authorized for strong encryption, but Cisco has determined that you are allowed to use strong encryption, you can manually add a strong encryption license to your account. Only the active unit requests this license, and both units can use it due to license aggregation.

g) Click **Apply**.

Step 4 Click **Register**.



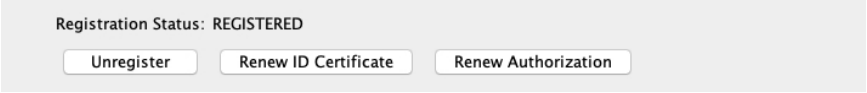
Step 5 Enter the registration token from the Cisco Smart Software Manager in the **ID Token** field.



(Optional) Click the **Force registration** check box to register an ASA that is already registered, but that might be out of sync with the Smart Software Manager. For example, use **Force registration** if the ASA was accidentally removed from the Smart Software Manager.

Step 6 Click **Register**.

ASDM refreshes the page when the license status is updated. You can also choose **Monitoring** > **Properties** > **Smart License** to check the license status, particularly if the registration fails.



Step 7 Quit ASDM and relaunch it.

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

Other Models: Configure Smart Software Manager On-Prem Licensing

This procedure applies for an ASA using a Smart Software Manager On-Prem.

Before you begin

- Download the Smart Software Manager On-Prem OVA file from Cisco.com and install and configure it on a VMwareESXi server. For more information, see the *Cisco Smart Software Manager On-Prem Data Sheet*.
- Download the crypto CA trustpool before you place the device in an air-gapped network. This trustpool is normally downloaded automatically, but may be out of date in an air-gapped network:

  crypto ca trustpool import url http://www.cisco.com/security/pki/trs/ios_core.p7b

Procedure

Step 1 Request a registration token on the Smart Software Manager On-Prem server.

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

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.

Note
HTTP proxy with authentication is not supported.

a) Choose **Configuration** > **Device Management** > **Smart Call-Home**.
b) Check the **Enable HTTP Proxy** check box.
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 Smart Software Manager On-Prem.

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://*on-prem_ip_address*/**Transportgateway/services/DeviceRequestHandler**

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

Step 4 Configure the license entitlements:

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

b) Check the **Enable Smart license configuration** check box.

c) From the **Feature Tier** drop-down menu, choose **Standard**.

Only the **Standard** tier is available, however, you need to enable it in the configuration; a tier license is a prerequisite for adding other feature licenses.

d) (Optional) (Firepower 1010) Check the **Enable Security Plus** check box.

The Security Plus tier enables failover.

e) (Optional) (Supported models) For the **Context** license, enter the number of contexts.

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 1120—5 contexts
- Firepower 1140—10 contexts
- Firepower 1150—25 contexts
- Firepower 2110—25 contexts
- Firepower 2120—25 contexts
- Firepower 2130—30 contexts
- Firepower 2140—40 contexts

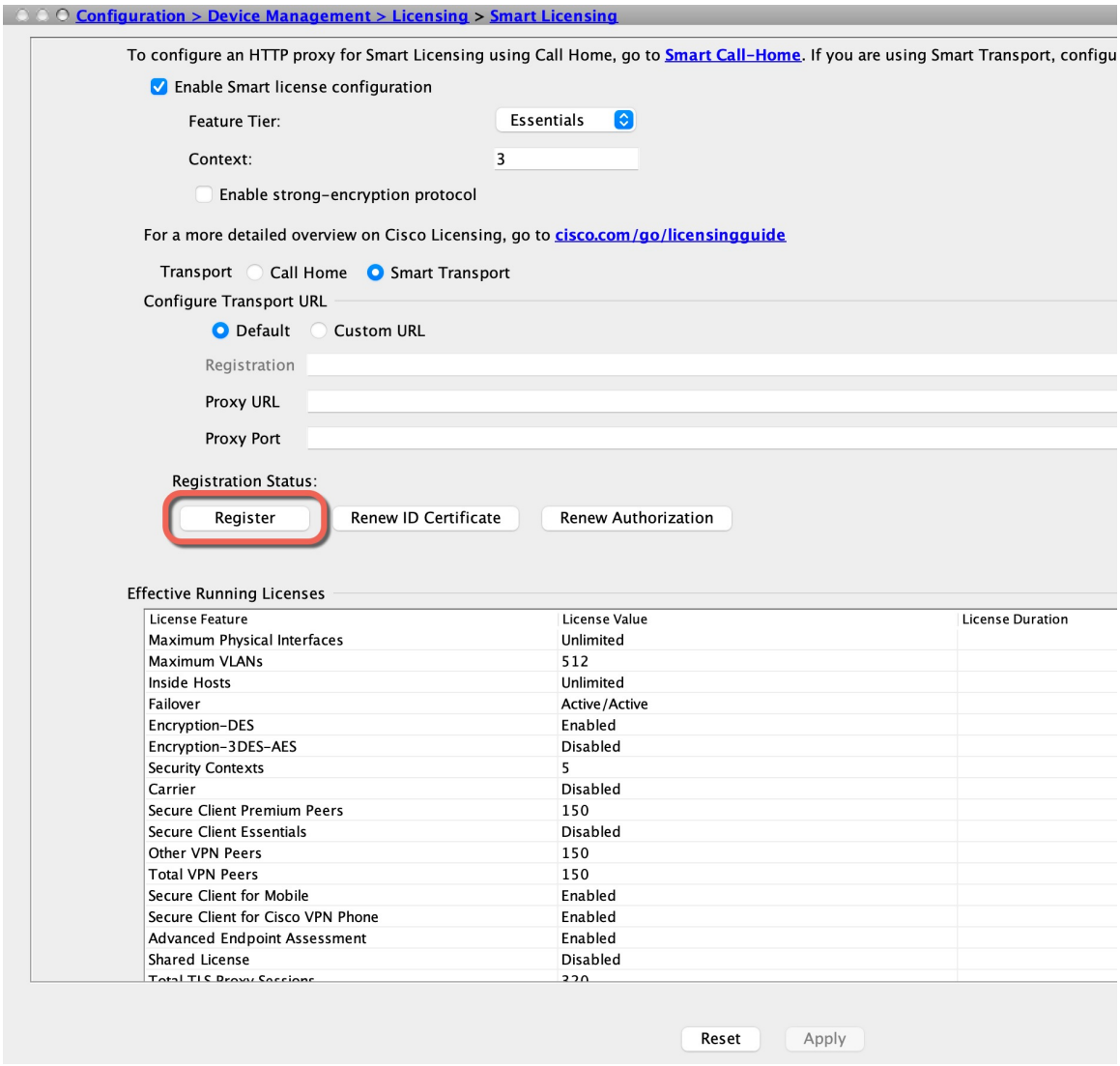
For example, to use the maximum of 25 contexts on the Firepower 1150, enter 23 for the number of contexts; this value is added to the default of 2.

f) (Optional) Check the **Enable strong-encryption protocol** check box. **Do not** check this box if you receive the strong encryption token.

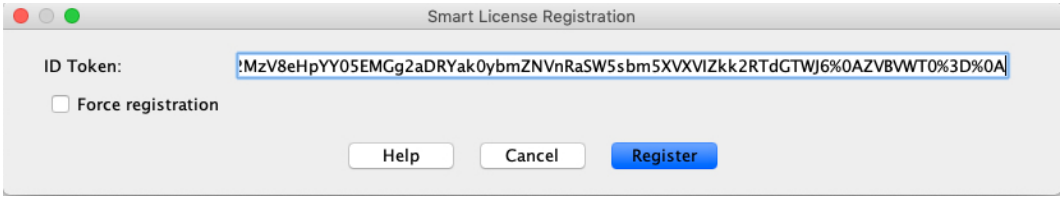
This license is not required if you receive the strong encryption token from the Smart Software Manager. However, if your Smart Account is not authorized for strong encryption, but Cisco has determined that you are allowed to use strong encryption, you can manually add a strong encryption license to your account. Only the active unit requests this license, and both units can use it due to license aggregation.

g) Click **Apply**.

Step 5 Click **Register**.



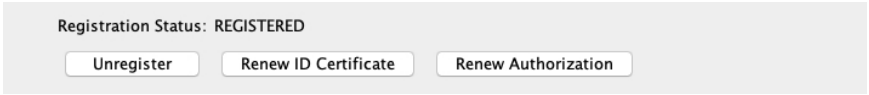
Step 6 Enter the registration token from the Cisco Smart Software Manager in the **ID Token** field.



(Optional) Click the **Force registration** check box to register an ASA that is already registered, but that might be out of sync with the Smart Software Manager. For example, use **Force registration** if the ASA was accidentally removed from the Smart Software Manager.

Step 7 Click **Register**.

ASDM refreshes the page when the license status is updated. You can also choose **Monitoring** > **Properties** > **Smart License** to check the license status, particularly if the registration fails.



Step 8 Quit ASDM and relaunch it.

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

Other Models: Configure Permanent License Reservation

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

Procedure

Step 1 Install the 1000/2100 Permanent License, on page 41.

Step 2 (Optional) Other Models: Return the Permanent License, on page 44.

Install the 1000/2100 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 license 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) Other Models: Return the Permanent License, on page 44.

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) Other Models: Return the Permanent License, on page 44.

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.

Note
Although the permanent license allows the full use of all of the licenses, you still need to turn on the entitlements in the ASA configuration so that the ASA knows it can use them.

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, however, you need to enable it in the configuration; a tier license is a prerequisite for adding other feature licenses.

c) (Optional) (Supported models) 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 default contexts. The maximum number of contexts depends on your model:

- Firepower 1120—5 contexts
- Firepower 1140—10 contexts
- Firepower 1150—25 contexts
- 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 1150, 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) (Firepower 1010) Request the Security Plus license to enable failover.

feature security-plus

Example:

```
ciscoasa(config-smart-lic)# feature security-plus
```

e) (Optional) Enable strong encryption. **Do not** enter this command if you receive the strong encryption token.

feature strong-encryption

This license is not required if you receive the strong encryption token from the Smart Software Manager. However, if your Smart Account is not authorized for strong encryption, but Cisco has determined that you are allowed to use strong encryption, you can manually add a strong encryption license to your account. Only the active unit requests this license, and both units can use it due to license aggregation.

Note
If you enter this command, your device will consume the strong encryption license, whether it's needed or not. So unless you have that license in your account, your account will go out of compliance. Since

this license is not needed when using the strong encryption token, you may accidentally put your account out of compliance without any benefit.

Example:

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

(Optional) Other Models: Return the 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. If the evaluation period has expired, then the ASA moves into an expired state. For more information about out-of-compliance states, see Out-of-Compliance State, on page 58.

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) Other Models: Deregister the ASA (Regular and On-Prem)

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. This procedure applies to the following device models:

- Firepower 1000/2100
-

Procedure

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

Step 2 Click **Unregister**.

(Optional) Other Models: Renew the ASA ID Certificate or License Entitlement (Regular and On-Prem)

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**.

Licenses Per Model

This section lists the license entitlements available for the ASAv and Firepower 4100/9300 chassis ASA security module.

ASAv

When you set the throughput level in the ASA configuration, it determines the license requested from the Smart Software Manager. See the following throughput level/license relationship:

- 100M—ASAv5
- 1G—ASAv10
- 2G—ASAv30
- 10G—ASAv50
- 20G—ASAv100

The throughput level also determines the maximum AnyConnect Client and TLS proxy sessions. However, a lower ASAv memory profile will cap your actual number of sessions, so to determine your sessions, you need to check both the throughput level and the memory installed.

The memory of your ASAv determines the maximum concurrent firewall connections and VLANs, and is not determined by the throughput level.

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

Licenses	Description
Entitlement Licenses	
Throughput Level	You set the throughput level in the ASA configuration. This level determines the license you need. 100M: ASAv5 1G: ASAv10 2G: ASAv30 10G: ASAv50 20G: ASAv100
Firewall Licenses	
Botnet Traffic Filter	Enabled
Firewall Connections, Concurrent	Firewall connections are determined by the ASAv memory. 2 GB to 7.9 GB: 100,000 8 GB to 15.9 GB: 500,000 16 GB to 31.9 GB: 2,000,000 32 GB to 64 GB: 4,000,000
Carrier	Enabled

Licenses	Description
Total TLS Proxy Sessions	TLS Proxy Sessions are determined by the throughput level and ASAv memory. 100M throughput + any memory: 500 1G throughput + any memory: 500 2G throughput: • 2 GB to 7.9 GB memory: 500 • 8 GB+ memory: 1000 10G throughput: • 2 GB to 7.9 GB memory: 500 • 8 GB to 15.9 GB memory: 1000 • 16 GB+ memory: 10,000 20G throughput: • 2 GB to 7.9 GB memory: 500 • 8 GB to 15.9 GB memory: 1000 • 16 GB to 31.9 GB memory: 10,000 • 32 GB+ memory: 20,000
VPN Licenses	

Licenses	Description	
AnyConnect Client peers	Unlicensed	AnyConnect Client peers are determined by the throughput level and ASAv memory. *Optional AnyConnect Plus or AnyConnect Apex license, Maximums:* *100M throughput + any memory: 50* *1G throughput + any memory: 250* *2G throughput:* • *2 GB to 7.9 GB memory: 250* • *8 GB+ memory: 750* *10G throughput:* • *2 GB to 7.9 GB memory: 250* • *8 GB to 15.9 GB memory: 750* • *16 GB+ memory: 10,000* *20G throughput:* • *2 GB to 7.9 GB memory: 250* • *8 GB to 15.9 GB memory: 750* • *16 GB to 31.9 GB: 10,000* • *32 GB+ memory: 20,000*

Licenses	Description
Other VPN Peers	**Note** Other VPN peers are determined by the throughput level and ASAv memory. 100M throughput + any memory: 50 1G throughput + any memory: 250 2G throughput: • 2 GB to 7.9 GB memory: 250 • 8 GB+ memory: 750 10G throughput: • 2 GB to 7.9 GB memory: 250 • 8 GB to 15.9 GB memory: 750 • 16 GB+ memory: 10,000 20G throughput: • 2 GB to 7.9 GB memory: 250 • 8 GB to 15.9 GB memory: 750 • 16 GB to 31.9 GB: 10,000 • 32 GB+ memory: 20,000

Licenses	Description
Total VPN Peers, combined all types	**Note** Total VPN peers are determined by the throughput level and ASAv memory. 100M throughput + any memory: 50 1G throughput + any memory: 250 2G throughput: • 2 GB to 7.9 GB memory: 250 • 8 GB+ memory: 750 10G throughput: • 2 GB to 7.9 GB memory: 250 • 8 GB to 15.9 GB memory: 750 • 16 GB+ memory: 10,000 20G throughput: • 2 GB to 7.9 GB memory: 250 • 8 GB to 15.9 GB memory: 750 • 16 GB to 31.9 GB: 10,000 • 32 GB+ memory: 20,000
General Licenses	
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	VLANs are determined by the ASAv memory. 2 GB to 7.9 GB—50 8 GB to 15.9 GB—200 16 GB to 31.9 GB—1024 32 GB to 64 GB—1024

Firepower 1010

The following table shows the licensed features for the Firepower 1010.

Licenses	Standard License	
Firewall Licenses		
Botnet Traffic Filter	No Support.	
Firewall Conns, Concurrent	100,000	
Carrier	No support. Although SCTP inspection maps are not supported, SCTP stateful inspection using ACLs is supported.	
Total TLS Proxy Sessions	4,000	
VPN Licenses		
AnyConnect Client peers	Unlicensed	*Optional AnyConnect Plus,AnyConnect Apex, or AnyConnect VPN Only license, Maximum: 75*
Other VPN Peers	75	
Total VPN Peers, combined all types	75	
General Licenses		
Encryption	Base (DES) or Strong (3DES/AES), depending on the account's export compliance setting	
Security Plus (failover, VPN Load Balancing)	Disabled	*Optional*
Security Contexts	No support.	
Clustering	No support.	
VLANs, Maximum	60	

Firepower 1100 Series

The following table shows the licensed features for the Firepower 1100 series.

Licenses	Standard License
Firewall Licenses	
Botnet Traffic Filter	No Support.
Firewall Conns, Concurrent	Firepower 1120: 200,000 Firepower 1140: 400,000 Firepower 1150: 600,000

Licenses	Standard License	
Carrier	No support. Although SCTP inspection maps are not supported, SCTP stateful inspection using ACLs is supported.	
Total TLS Proxy Sessions	Firepower 1120: 4,000 Firepower 1140: 8,000 Firepower 1150: 8,000	
VPN Licenses		
AnyConnect Client peers	Unlicensed	*Optional AnyConnect Plus, AnyConnect Apex, or AnyConnect VPN Only license, Maximum:* *Firepower 1120: 150* *Firepower 1140: 400* *Firepower 1150: 800*
Other VPN Peers	Firepower 1120: 150 Firepower 1140: 400 Firepower 1150: 800	
Total VPN Peers, combined all types	Firepower 1120: 150 Firepower 1140: 400 Firepower 1150: 800	
General Licenses		
Encryption	Base (DES) or Strong (3DES/AES), depending on the account's export compliance setting	
Security Contexts	2	*Optional License, Maximum:* *Firepower 1120: 5* *Firepower 1140: 10* *Firepower 1150: 25*
Clustering	No support.	
VLANs, Maximum	1024	

Firepower 2100 Series

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

Licenses	Standard License
Firewall Licenses	

Licenses	Standard License	
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 Client peers	Unlicensed	*Optional AnyConnect Plus, AnyConnect Apex, or AnyConnect VPN Only license, Maximum:* *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, Maximum:* *Firepower 2110: 25* *Firepower 2120: 25* *Firepower 2130: 30* *Firepower 2140: 40*
Clustering	No support.	
VLANs, Maximum	1024	

Firepower 4100

The following table shows the licensed features for the Firepower 4100.

Licenses	Standard License	
Firewall Licenses		
Botnet Traffic Filter	No Support.	
Firewall Conns, Concurrent	Firepower 4110: 10,000,000 Firepower 4112: 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		

Licenses	Standard License	
AnyConnect Client peers	Unlicensed	*Optional AnyConnect Plus, AnyConnect Apex, or AnyConnect VPN Only license:* *Firepower 4110: 10,000* *Firepower 4112: 10,000* *Firepower 4115: 15,000* *Firepower 4120: 15,000* *Firepower 4125: 20,000* *Firepower 4140: 20,000* *Firepower 4145: 20,000* *Firepower 4150: 20,000*
Other VPN Peers	Firepower 4110: 10,000 Firepower 4112: 10,000 Firepower 4115: 15,000 Firepower 4120: 15,000 Firepower 4125: 20,000 Firepower 4140: 20,000 Firepower 4145: 20,000 Firepower 4150: 20,000	
Total VPN Peers, combined all types	Firepower 4110: 10,000 Firepower 4112: 10,000 Firepower 4115: 15,000 Firepower 4120: 15,000 Firepower 4125: 20,000 Firepower 4140: 20,000 Firepower 4145: 20,000 Firepower 4150: 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*
Clustering	Enabled	
VLANs, Maximum	1024	

Firepower 9300

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

Licenses	Standard License	
Firewall Licenses		
Botnet Traffic Filter	No Support.	
Firewall Conns, Concurrent	Firepower 9300 SM-56: 60,000,000 Firepower 9300 SM-48: 60,000,000 Firepower 9300 SM-44: 60,000,000 Firepower 9300 SM-40: 55,000,000 Firepower 9300 SM-36: 60,000,000 Firepower 9300 SM-24: 55,000,000	
Carrier	Disabled	*Optional License: Carrier*
Total TLS Proxy Sessions	15,000	
VPN Licenses		
AnyConnect Client peers	Unlicensed	*Optional AnyConnect Plus, AnyConnect Apex, or AnyConnect VPN Only 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*
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 Smart Software Manager. When the device registers with the token, the Smart Software Manager issues an ID certificate for communication between the device and the Smart Software Manager. This certificate is valid for 1 year, although it will be renewed every 6 months.

Periodic Communication with the Smart Software Manager

The device communicates with the Smart Software Manager 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 Smart Software Manager, or your ASAv will be out-of-compliance; operation is otherwise unaffected.

All Other Models

The ASA 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 Smart Software Manager, 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—The device is using more licenses than are available.
- License expiration—A time-based license has expired.
- Lack of communication—The device cannot reach the licensing authority for re-authorization, causing the authorization to expire.

To verify whether your device is out of compliance, or approaching that status, you must compare the entitlements currently in use by your device against those in your Smart Account.

When the device is out of compliance, operations may be limited, depending on the model:

- ASAv—The system enters a restrictive state that limits concurrent AnyConnect sessions to two and throttles total throughput to 100 Kbps. This rate limiting ensures that the device continues to operate but with significantly reduced capacity until a valid license is installed. This behavior is specific to the ASA virtual model.
- All Other Models—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 Smart Software Manager. You cannot remove this profile. Note that the only configurable option for the License profile is the destination address URL for the Smart Software Manager. Unless directed by Cisco TAC, you should not change the Smart Software Manager 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 Transport or 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.



Note Reloading a device with an expired licensing registration for over a year, will disable the export-controlled functionality. This can lead to critical issues such as VPN downtime or failover split-brain scenarios when IPsec encryption is enabled.

History for Smart Software Licensing

Feature Name	Platform Releases	Description
ASAv100 permanent license reservation	9.14(1.30)	The ASAv100 now supports permanent license reservation using product ID L-ASAV100SR-K9=. **Note:** Not all accounts are approved for permanent license reservation.

Feature Name	Platform Releases	Description
ASAv MSLA Support	9.13(1)	The ASAv supports Cisco's Managed Service License Agreement (MSLA) program, which is a software licensing and consumption framework designed for Cisco customers and partners who offer managed software services to third parties. MSLA is a new form of Smart Licensing where the licensing Smart Agent keeps track of the usage of licensing entitlements in units of time. New/Modified screens: **Configuration** > **Device Management** > **Licensing** > **Smart Licensing**.
ASAv Flexible Licensing	9.13(1)	Flexible Licensing is a new form of Smart Licensing where any ASAv license now can be used on any supported ASAv vCPU/memory configuration. Session limits for AnyConnect Client and TLS proxy will be determined by the ASAv platform entitlement installed rather than a platform limit tied to a model type. New/Modified screens: **Configuration** > **Device Management** > **Licensing** > **Smart Licensing**.
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 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.

Feature Name	Platform Releases	Description
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.
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**

Feature Name	Platform Releases	Description
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**
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 ASAv's 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**