License Management for the ASA

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:** My Cisco Entitlements (MCE) 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 software 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 Software Central (software.cisco.com).

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide

Note This section only applies to ASA logical devices on the Firepower 4100/9300 chassis. For more information on licensing for Firepower Threat Defense logical devices, see the FMC Configuration Guide.

About Smart Software Licensing

This section describes how Smart Software Licensing works.

Note This section only applies to ASA logical devices on the Firepower 4100/9300 chassis. For more information on licensing for Firepower Threat Defense logical devices, see the FMC Configuration Guide.

Smart Software Licensing for the ASA

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

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

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

- ASA Application—Configure all license entitlements in the application.

Note Cisco Transport Gateway is not supported on Firepower 4100/9300 security appliances.

Smart Software Manager and Accounts

When you purchase 1 or more licenses for the device, you manage them in the Cisco Smart Software Manager:

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

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

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

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

Offline Management

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

Permanent License Reservation

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

You can obtain a license that enables all features: Standard tier with maximum Security Contexts and the Carrier license. 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.

Satellite Server

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

Once you download and deploy the satellite application, you can perform the following functions without sending data to Cisco SSM using the Internet:

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

For more information, see the Smart Software Manager satellite installation and configuration guides on Smart Account Manager satellite.

Licenses and Devices Managed per Virtual Account

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

Only the Firepower 4100/9300 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

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

- Chassis-level evaluation mode—Before the Firepower 4100/9300 chassis registers with the Licensing Authority, it operates for 90 days (total usage) in evaluation mode. The ASA cannot request specific entitlements in this mode; only default entitlements are enabled. When this period ends, the Firepower 4100/9300 chassis becomes out-of-compliance.
- Entitlement-based evaluation mode—After the Firepower 4100/9300 chassis registers with the Licensing Authority, you can obtain time-based evaluation licenses that can be assigned to the ASA. In the ASA,

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

Note You cannot receive an evaluation license for Strong Encryption (3DES/AES); only permanent licenses support this entitlement.

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 chassis, or when you register an existing chassis. You can create a new token if an existing token is expired.

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

Periodic Communication with the License Authority

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

You can optionally configure an HTTP proxy.

The Firepower 4100/9300 chassis must have internet access either directly or through an HTTP proxy at least every 90 days. Normal license communication occurs every 30 days, but with the grace period, your device will operate for up to 90 days without calling home. After the grace period, you must contact the Licensing Authority, or you will not be able to make configuration changes to features requiring special licenses; operation is otherwise unaffected.

Note If your device is unable to communicate with the license authority for one year, the device will enter an unregistered state but will not lose any previously enabled strong encryption capabilities.

Out-of-Compliance State

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

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

To verify whether your account is in, or approaching, an Out-of-Compliance state, you must compare the entitlements currently in use by your Firepower 4100/9300 chassis against those in your Smart Account.

In an out-of-compliance state, 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.

Smart Call Home Infrastructure

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

Note Cisco Transport Gateway is not supported on Firepower 4100/9300 security appliances.

Cisco Success Network

Cisco Success Network is a user-enabled cloud service. When you enable Cisco Success Network, a secure connection is established between the Firepower 4100/9300 chassis and the Cisco cloud to stream usage information and statistics. Streaming telemetry provides a mechanism that selects data of interest from the ASA and transmits it in a structured format to remote management stations to do the following:

- Inform you of available unused features that can improve the effectiveness of the product in your network
- Inform you of additional technical support services and monitoring that might be available for your product
- Help Cisco improve our products

You enable Cisco Success Network when you register the Firepower 4100/9300 with the Cisco Smart Software Manager. See Register the Firepower 4100/9300 chassis with the License Authority, on page 18.

You can enroll in the Cisco Success Network only if all the following conditions are met:

- Smart Software License is registered.
- Smart License Satellite mode is disabled.
- Permanent License is disabled.

Once you enroll in the Cisco Success Network, the chassis establishes and maintains the secure connection at all times. You can turn off this connection at any time by disabling Cisco Success Network, which disconnects the device from the Cisco Success Network cloud.

You can view your current Cisco Success Network enrollment status on the **System** > **Licensing** > **Cisco Success Network** page, and you can change your enrollment status. See Change Cisco Success Network Enrollment, on page 19.

Cisco Success Network Telemetry Data

Cisco Success Network allows the chassis to stream configuration and operating state information once in every 24 hours to the Cisco Success Network cloud. Collected and monitored data include the following:

- **Enrolled device information**—Firepower 4100/9300 chassis model name, product identifier, serial number, UUID, system uptime, and Smart Licensing information. See Enrolled Device Data, on page 6.
- **Software information**—Type and version number for the software running on the Firepower 4100/9300 chassis. See Software Version Data, on page 7.
- **ASA device information**—Information about the ASA devices running on the security module/engine of the Firepower 4100/9300. Note that for the Firepower 4100 series, only the information about a single ASA device is included. ASA device information includes smart licenses in use for each device, device models, serial numbers, and software version. See ASA Device Data, on page 7.
  - **Performance information**—System uptime, CPU usage, memory usage, disk space usage, and bandwidth usage information of the ASA devices. See Performance Data, on page 7.
  - **Usage information**—Feature status, cluster, failover, and login information:
    - **Feature status**—List of enabled ASA features that you have configured or are enabled by default.
    - **Cluster information**—Includes cluster information if the ASA device is in clustered mode. If the ASA device is not in clustered mode, this information is not displayed. The cluster information includes the cluster group name of the ASA device, cluster interface mode, unit name, and state. For the other peer ASA devices in the same cluster, the information includes the name, state, and serial number.
    - **Failover information**—Includes failover information if the ASA is in failover mode. If the ASA is not in failover mode, this information is not displayed. The failover information includes the role and state of the ASA, and the role, state, and serial number of the peer ASA device.
    - **Login history**—User login frequency, login time, and date stamp for the most recent successful login on the ASA device. However, the login history does not include the user login name, credentials, or any other personal information.

  See Usage Data, on page 8 for more information.

Enrolled Device Data

Once you enroll the Firepower 4100/9300 chassis in Cisco Success Network, select telemetry data about the chassis is streamed to the Cisco cloud. The following table describes the collected and monitored data.

Table 1: Enrolled Device Telemetry Data

Data Point	Example Value
Device model	Cisco Firepower FP9300 Security Appliance
Serial number	GMX1135L01K
Smart license PIID	752107e9-e473-4916-8566-e26d0c4a5bd9
Smart license virtual account name	FXOS-general
System uptime	32115
UDI product identifier	FPR-C9300-AC

Software Version Data

Cisco Success Network collects software information that pertains to the chassis including type and software version. The following table describes the collected and monitored software information.

Table 2: Software Version Telemetry Data

Data Point	Example Value
Type	package_version
Version	2.7(1.52)

ASA Device Data

Cisco Success Network collects information about the ASA devices running on the security module/engine of the Firepower 4100/9300. The following table describes the collected and monitored information about ASA devices.

Table 3: ASA Device Telemetry Data

Data Point	Example Value
ASA device PID	FPR9K-SM-36
ASA device model	Cisco Adaptive Security Appliance
ASA device serial number	XDQ311841WA
Deployment type (native or container)	Native
Security context mode (single or multiple)	Single

ASA software version	{
	type: "asa_version",
	ersion: "9.13.1.5"
	}

Device manager version	{
	type: "device_mgr_version",
	version: "7.10.1"
	}

Activated smart licenses in use	{
	"type": "Strong encryption",
	"tag":
	"regid.2016-05.com.cisco.ASA-GEN-STRONG-ENCRYPTION,
	5.7_982308k4-74w2-5f38-64na-707q99g10cce",
	"count": 1
	}

Performance Data

Cisco Success Network collects the performance-specific information for the ASA devices. The information includes system uptime, CPU usage, memory usage, disk space usage, and bandwidth usage information.

- **CPU usage**—CPU usage information for the past five minutes

- **Memory usage**—Free, used, and total memory of the system
- **Disk usage**—Free, used, and total disk space information
- **System uptime**—System uptime information
- **Bandwidth usage**—System bandwidth usage; aggregated from all nameif-ed interfaces

  This shows the statistics for received and transmitted packets (or bytes) per second since system up time.

The following table describes the collected and monitored information.

Table 4: Performance Telemetry Data

Data Point	Example Value

System CPU usage in past five minutes	<pre>{
	“fiveSecondsPercentage”:0.2000000,
	“oneMinutePercentage”: 0,
	“fiveMinutesPercentage”: 0
	
	}</pre>

System memory usage	<pre>{
	“freeMemoryInBytes”:225854966384,
	“usedMemoryInBytes”: 17798281616,
	“totalMemoryInBytes”:243653248000
	
	}</pre>

System disk usage	<pre>{
	"freeGB": 21.237285,
	"usedGB": 0.238805,
	"totalGB": 21.476090
	
	}</pre>

System uptime	99700000

System bandwidth usage	<pre>{
	"receivedPktsPerSec": 3,
	"receivedBytesPerSec": 212,
	"transmittedPktsPerSec": 3,
	"transmittedBytesPerSec": 399
	}</pre>

Usage Data

Cisco Success Network collects feature status, cluster, failover, and login information for the ASA devices running on the security module/engine of the chassis. The following table describes the collected and monitored data about ASA device usage.

Table 5: Usage Telemetry Data

Data Point	Example Value

Feature status	[{
	"name": "cluster",
	"status": "enabled"
	},
	{
	"name": "webvpn",
	"status": "enabled"
	},
	{
	"name": "logging-buffered",
	"status": "debugging"
	}]

Cluster information	{
	"clusterGroupName": "asa-cluster",
	"interfaceMode": "spanned",
	"unitName": "unit-3-3",
	"unitState": "SLAVE",
	"otherMembers": {
	"items": [
	{
	"memberName": "unit-2-1",
	"memberState": "MASTER",
	
	"memberSerialNum": "DAK391674E"
	}
	]
	}
	
	}

Failover information	{
	myRole: "Primary",
	peerRole: "Secondary",
	myState: "active",
	peerState: "standby",
	peerSerialNum:
	"DAK39162B"
	}

Login history	{
	"loginTimes": "1 times in last 1 days",
	"lastSuccessfulLogin": "12:25:36 PDT Mar 11
	2019"
	}

Telemetry Example File

Firepower 4100/9300 chassis aggregates the data received from all ASA devices that have telemetry enabled and are online with the chassis-specific information and additional fields before sending the data to Cisco cloud. If there are no applications with telemetry data, then telemetry is still sent to the Cisco cloud with the chassis information.

The following is an example of a Cisco Success Network telemetry file that includes the information sent to the Cisco cloud for two ASA devices on a Firepower 9300.

```
{
  "version": "1.0",
```

```
"metadata": {
  "topic": "ASA.telemetry",
  "contentType": "application/json",
  "msgID": "2227"
},
"payload": {
  "recordType": "CST_ASA",
  "recordVersion": "1.0",
  "recordedAt": 1560868270055,
  "FXOS": {
    "FXOSdeviceInfo": {
      "deviceModel": "Cisco Firepower FP9300 Security Appliance",
      "serialNumber": "HNY4475P01K",
      "smartLicenseProductInstanceIdentifier": "413509m0-f952-5822-7492-r62c0a5h4gf4",
      "smartLicenseVirtualAccountName": "FXOS-general",
      "systemUptime": 32115,
      "udiProductIdentifier": "FPR-C9300-AC"
    },
    "versions": {
      "items": [
        {
          "type": "package_version",
          "version": "2.7(1.52)"
        }
      ]
    }
  },
  "asaDevices": {
    "items": [
      {
        "CPUUsage": {
          "fiveMinutesPercentage": 0,
          "fiveSecondsPercentage": 0,
          "oneMinutePercentage": 0
        },
        "bandwidthUsage": {
          "receivedBytesPerSec": 1,
          "receivedPktsPerSec": 0,
          "transmittedBytesPerSec": 1,
          "transmittedPktsPerSec": 0
        },
        "deviceInfo": {
          "deploymentType": "Native",
          "deviceModel": "Cisco Adaptive Security Appliance",
          "securityContextMode": "Single",
          "serialNumber": "ADG2158508T",
          "systemUptime": 31084,
          "udiProductIdentifier": "FPR9K-SM-24"
        },
        "diskUsage": {
          "freeGB": 19.781810760498047,
          "totalGB": 20.0009765625,
          "usedGB": 0.21916580200195312
        },
        "featureStatus": {
          "items": [
            {
              "name": "aaa-proxy-limit",
              "status": "enabled"
            },
            {
              "name": "firewall_user_authentication",
              "status": "enabled"
            },
```

```
{
  "name": "IKEv2 fragmentation",
  "status": "enabled"
},
{
  "name": "inspection-dns",
  "status": "enabled"
},
{
  "name": "inspection-esmtp",
  "status": "enabled"
},
{
  "name": "inspection-ftp",
  "status": "enabled"
},
{
  "name": "inspection-hs232",
  "status": "enabled"
},
{
  "name": "inspection-netbios",
  "status": "enabled"
},
{
  "name": "inspection-rsh",
  "status": "enabled"
},
{
  "name": "inspection-rtsp",
  "status": "enabled"
},
{
  "name": "inspection-sip",
  "status": "enabled"
},
{
  "name": "inspection-skinny",
  "status": "enabled"
},
{
  "name": "inspection-snmp",
  "status": "enabled"
},
{
  "name": "inspection-sqlnet",
  "status": "enabled"
},
{
  "name": "inspection-sunrpc",
  "status": "enabled"
},
{
  "name": "inspection-tftp",
  "status": "enabled"
},
{
  "name": "inspection-xdmcp",
  "status": "enabled"
},
{
  "name": "management-mode",
  "status": "normal"
},
```

```
        {
          "name": "mobike",
          "status": "enabled"
        },
        {
          "name": "ntp",
          "status": "enabled"
        },
        {
          "name": "sctp-engine",
          "status": "enabled"
        },
        {
          "name": "smart-licensing",
          "status": "enabled"
        },
        {
          "name": "static-route",
          "status": "enabled"
        },
        {
          "name": "threat_detection_basic_threat",
          "status": "enabled"
        },
        {
          "name": "threat_detection_stat_access_list",
          "status": "enabled"
        }
      ]
    },
    "licenseActivated": {
      "items": []
    },
    "loginHistory": {
      "lastSuccessfulLogin": "05:53:18 UTC Jun 18 2019",
      "loginTimes": "1 times in last 1 days"
    },
    "memoryUsage": {
      "freeMemoryInBytes": 226031548496,
      "totalMemoryInBytes": 241583656960,
      "usedMemoryInBytes": 15552108464
    },
    "versions": {
      "items": [
        {
          "type": "asa_version",
          "version": "9.13(1)248"
        },
        {
          "type": "device_mgr_version",
          "version": "7.13(1)31"
        }
      ]
    }
  },
  {
    "CPUUsage": {
      "fiveMinutesPercentage": 0,
      "fiveSecondsPercentage": 0,
      "oneMinutePercentage": 0
    },
    "bandwidthUsage": {
      "receivedBytesPerSec": 1,
      "receivedPktsPerSec": 0,
```

```
  "transmittedBytesPerSec": 1,
  "transmittedPktsPerSec": 0
},
"deviceInfo": {
  "deploymentType": "Native",
  "deviceModel": "Cisco Adaptive Security Appliance",
  "securityContextMode": "Single",
  "serialNumber": "RFL21764S1D",
  "systemUptime": 31083,
  "udiProductIdentifier": "FPR9K-SM-24"
},
"diskUsage": {
  "freeGB": 19.781543731689453,
  "totalGB": 20.0009765625,
  "usedGB": 0.21943283081054688
},
"featureStatus": {
  "items": [
    {
      "name": "aaa-proxy-limit",
      "status": "enabled"
    },
    {
      "name": "call-home",
      "status": "enabled"
    },
    {
      "name": "crypto-ca-trustpoint-id-usage-ssl-ipsec",
      "status": "enabled"
    },
    {
      "name": "firewall_user_authentication",
      "status": "enabled"
    },
    {
      "name": "IKEv2 fragmentation",
      "status": "enabled"
    },
    {
      "name": "inspection-dns",
      "status": "enabled"
    },
    {
      "name": "inspection-esmtp",
      "status": "enabled"
    },
    {
      "name": "inspection-ftp",
      "status": "enabled"
    },
    {
      "name": "inspection-hs232",
      "status": "enabled"
    },
    {
      "name": "inspection-netbios",
      "status": "enabled"
    },
    {
      "name": "inspection-rsh",
      "status": "enabled"
    },
    {
      "name": "inspection-rtsp",
```

```
        "status": "enabled"
      },
      {
        "name": "inspection-sip",
        "status": "enabled"
      },
      {
        "name": "inspection-skinny",
        "status": "enabled"
      },
      {
        "name": "inspection-snmp",
        "status": "enabled"
      },
      {
        "name": "inspection-sqlnet",
        "status": "enabled"
      },
      {
        "name": "inspection-sunrpc",
        "status": "enabled"
      },
      {
        "name": "inspection-tftp",
        "status": "enabled"
      },
      {
        "name": "inspection-xdmcp",
        "status": "enabled"
      },
      {
        "name": "management-mode",
        "status": "normal"
      },
      {
        "name": "mobike",
        "status": "enabled"
      },
      {
        "name": "ntp",
        "status": "enabled"
      },
      {
        "name": "sctp-engine",
        "status": "enabled"
      },
      {
        "name": "smart-licensing",
        "status": "enabled"
      },
      {
        "name": "static-route",
        "status": "enabled"
      },
      {
        "name": "threat_detection_basic_threat",
        "status": "enabled"
      },
      {
        "name": "threat_detection_stat_access_list",
        "status": "enabled"
      }
    ]
  },
```

```
        "licenseActivated": {
          "items": []
        },
        "loginHistory": {
          "lastSuccessfulLogin": "05:53:16 UTC Jun 18 2019",
          "loginTimes": "1 times in last 1 days"
        },
        "memoryUsage": {
          "freeMemoryInBytes": 226028740080,
          "totalMemoryInBytes": 241581195264,
          "usedMemoryInBytes": 15552455184
        },
        "versions": {
          "items": [
            {
              "type": "asa_version",
              "version": "9.13(1)248"
            },
            {
              "type": "device_mgr_version",
              "version": "7.13(1)31"
            }
          ]
        }
      }
    ]
  }
 }
}
```


Prerequisites for Smart Software Licensing

- Note that this chapter only applies to ASA logical devices on the Firepower 4100/9300 chassis. For more information on licensing for Firepower Threat Defense logical devices, see the FMC Configuration Guide.
- 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.
- Purchase 1 or more licenses from the Cisco Commerce Workspace. On the home page, search for your platform in the **Find Products and Solutions** search field. Some licenses are free, but you still need to add them to your Smart Software Licensing account.
- Ensure internet access or HTTP proxy access from the chassis, so the chassis can contact the Licensing Authority.
- Configure a DNS server so the chassis can resolve the name of the Licensing Authority.
- Set the time for the chassis.
- Configure the Smart Software Licensing infrastructure on the Firepower 4100/9300 chassis before you configure the ASA licensing entitlements.

Guidelines for Smart Software Licensing

ASA Guidelines for Failover and Clustering

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

Defaults for Smart Software Licensing

The Firepower 4100/9300 chassis default configuration includes a Smart Call Home profile called "SLProfile" that specifies the URL for the Licensing Authority.

```
scope monitoring
  scope callhome
    scope profile SLProfile
      scope destination SLDest
        set address https://tools.cisco.com/its/service/oddce/services/DDCEService
```

Configure Regular Smart Software Licensing

To communicate with the Cisco License Authority, you can optionally configure an HTTP proxy. To register with the License Authority, you must enter the registration token ID on the Firepower 4100/9300 chassis that you obtained from your Smart Software License account.

Procedure

Step 1 (Optional) Configure the HTTP Proxy, on page 16.

Step 2 (Optional) Delete the Call Home URL, on page 17

Step 3 Register the Firepower 4100/9300 chassis with the License Authority, on page 18.

(Optional) Configure the HTTP Proxy

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.

Procedure

Step 1 Enable the HTTP proxy:

scope monitoring
scope callhome
set http-proxy-server-enable on

Example:

```
scope monitoring
  scope callhome
    set http-proxy-server-enable on
```

Step 2 Set the proxy URL:

set http-proxy-server-url *url*

where *url* is the http or https address of the proxy server.

Example:

```
set http-proxy-server-url https://10.1.1.1
```

Step 3 Set the port:

set http-proxy-server-port *port*

Example:

```
set http-proxy-server-port 443
```

Step 4 Commit the buffer:

commit-buffer

(Optional) Delete the Call Home URL

Use the following procedure to delete a previously configured Call Home URL.

Procedure

Step 1 Enter the monitoring scope:

scope monitoring

Step 2 Enter the callhome scope:

scope callhome

Step 3 Look for the SLProfile:

scope profile SLProfile

Step 4 Show the destination:

show destination

Example:

```
SLDest https https://tools.cisco.com/its/oddce/services/DDCEService
```

Step 5 Delete the URL:

delete destination SLDest

Step 6 Commit the buffer:

commit-buffer

Register the Firepower 4100/9300 chassis with the License Authority

When you register the Firepower 4100/9300 chassis, the License Authority issues an ID certificate for communication between the Firepower 4100/9300 chassis and the License Authority. It also assigns the Firepower 4100/9300 chassis to the appropriate virtual account. Normally, this procedure is a one-time instance. However, you might need to later re-register the Firepower 4100/9300 chassis if the ID certificate expires because of a communication problem, for example.

Procedure

Step 1 In the Smart Software Manager or the Smart Software Manager Satellite, request and copy a registration token for the virtual account to which you want to add this Firepower 4100/9300 chassis.

For more information on how to request a registration token using the Smart Software Manager Satellite, see the Cisco Smart Software Manager Satellite User Guide (https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html).

Step 2 Enter the registration token on the Firepower 4100/9300 chassis:

scope license

register idtoken *id-token*

(Optional) Enable the **force** option. If the device registration fails due to communication failure between the device and the portal or satellite, CTC waits for 24 hours before attempting to register the device again. Use the **force** option to force the registration:

register idtoken *id-token* **force**

Example:

```
scope license
  register idtoken ZGFmNWM5NjgtYmNjYS00ZWI3L
WE3NGItMWJkOGExZjIxNGQ0LTE0NjI2NDYx%0AMDIzNT
```

```
V8N3R0dXM1Z0NjWkdpR214eFZhMldBOS9CVnNEYnVKM1
g3R3dvemRD%0AY29NQT0%3D%0A
```

Step 3 To later unregister the device, enter:

scope license

deregister

Deregistering the Firepower 4100/9300 chassis removes the device from your account. All license entitlements and certificates on the device are removed. You might want to deregister to free up a license for a new Firepower 4100/9300 chassis. Alternatively, you can remove the device from the Smart Software Manager.

Step 4 To renew the ID certificate and update the entitlements on all security modules, enter:

scope license

scope licdebug

renew

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.

Change Cisco Success Network Enrollment

You enable Cisco Success Network when you register the Firepower 4100/9300 with the Cisco Smart Software Manager. After that, use the following procedure to view or change enrollment status.

Note Cisco Success Network does not work in evaluation mode.

Procedure

Step 1 Enter the system scope.

scope system

Example:

```
Firepower# scope system
Firepower /system #
```

Step 2 Enter the services scope.

scope services

Example:

```
Firepower /system # scope services
Firepower /system/services #
```

Step 3 Enter the telemetry scope.

scope telemetry

Example:

```
Firepower /system/services # scope telemetry
Firepower /system/services/telemetry #
```

Step 4 Enable or disable the Cisco Success Network feature.

{enable | disable}

Example:

```
Firepower /system/services/telemetry # enable
```

Step 5 Verify the Cisco Success Network status in the Firepower 4100/9300 Chassis.

show detail

Example:

Verify that the **Admin State** shows the correct status of Cisco Success Network.

```
Telemetry:
    Admin State: Enabled
    Oper State: Registering
    Error Message:
    Period: 86400
    Current Task: Registering the device for Telemetry
    (FSM-STAGE:sam:dme:CommTelemetryDataExchSeq:RegisterforTelemetry)
```

Example:

Verify that the **Oper State** shows **OK**, which indicates that telemetry data is sent.

```
Telemetry:
    Admin State: Enabled
    Oper State: Ok
    Error Message:
    Period: 86400
    Current Task:
```

Configure a Smart License Satellite Server for the Firepower 4100/9300 chassis

The following procedure shows how to configure the Firepower 4100/9300 chassis to use a Smart License satellite server.

Before you begin

- Complete all prerequisites listed in the Prerequisites for Smart Software Licensing, on page 15.
- Deploy and set up a Smart Software Satellite Server:

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

- Verify that the FQDN of the Smart Software Satellite Server can be resolved by your internal DNSserver.
- Verify whether the satellite trustpoint is already present:

  scope security

  show trustpoint

  Note that the trustpoint is added by default in FXOS version 2.4(1) and later. If the trustpoint is not present, you must add one manually using the following steps:

  1. Go to http://www.cisco.com/security/pki/certs/clrca.cer and copy the entire body of the SSL certificate (from "-----BEGIN CERTIFICATE-----" to "-----END CERTIFICATE-----") into a place you can access during configuration.
  2. Enter security mode:

     scope security
  3. Create and name a trusted point:

     create trustpoint *trustpoint_name*
  4. Specify certificate information for the trust point. Note: the certificate must be in Base64 encoded X.509 (CER) format.

     set certchain *certchain*

     For the *certchain* variable, paste the certificate text that you copied in step 1.

     If you do not specify certificate information in the command, you are prompted to enter a certificate or a list of trust points defining a certification path to the root certificate authority (CA). On the next line following your input, type **ENDOFBUF** to finish.
  5. Commit the configuration:

     commit-buffer

Procedure

Step 1 Set up the satellite server as the callhome destination:

scope monitoring

scope callhome

scope profile SLProfile

scope destination SLDest

set address https://*[FQDN of Satellite server]***/Transportgateway/services/DeviceRequestHandler**

Step 2 Register the Firepower 4100/9300 chassis with the License Authority (see Register the Firepower 4100/9300 chassis with the License Authority, on page 18). Note that you must request and copy the registration token from the Smart License Manager satellite.

Configure Permanent License Reservation

You can assign a permanent license to your Firepower 4100/9300 chassis. This universal reservation allows you to use any entitlement for an unlimited count on your device.

Note Before you begin, you must purchase the 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.

Install the Permanent License

The following procedure shows how to assign a permanent license to your Firepower 4100/9300 chassis.

Procedure

Step 1 From the FXOS CLI, enable license reservation:

scope license

enable reservation

Step 2 Scope to the license reservation:

scope license

scope reservation

Step 3 Generate a reservation request code:

request universal

show license resvcode

Step 4 Go to the Smart Software Manager Inventory screen in the Cisco Smart Software Manager portal, 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 5 Click **License Reservation**, and type the generated reservation request code into the box.

Step 6 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 7 In the FXOS CLI, enter the licensing scope:

scope license

Step 8 Enter the reservation scope:

scope reservation

Step 9 Enter the authorization code:

install *code*

Your Firepower 4100/9300 chassis is now fully licensed with PLR.

Step 10 Enable feature entitlements on the ASA logical device. See the ASA licensing chapter to enable entitlements.

(Optional) Return the Permanent License

If you no longer need a permanent license, you must officially return it to the Smart Software Manager using this procedure. If you do not follow all steps, the license stays in an in-use state and cannot be used elsewhere.

Procedure

Step 1 From the FXOS CLI, enter the license scope:

scope license

Step 2 Enter the reservation scope:

scope reservation

Step 3 Return the permanent license:

return

The Firepower 4100/9300 chassis immediately becomes unlicensed and moves to the Evaluation state.

Step 4 View and copy the return reservation code:

show license resvcode

Step 5 View and copy the FXOS universal device identifier (UDI) so you can find your FXOS instance in the Smart Software Manager:

show license udi

Step 6 Go to the Smart Software Manager Inventory screen, and click on the **Product Instances** tab:

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

Step 7 Search for your Firepower 4100/9300 chassis using its universal device identifier (UDI).

Step 8 Choose **Actions** > **Remove**, and type the generated return reservation code into the box.

Step 9 Click **Remove Product Instance**.

The permanent license is returned to the available pool.

Step 10 Reboot the system. For details on how to reboot your Firepower 4100/9300 chassis, see Rebooting the Firepower 4100/9300 Chassis.

Monitoring Smart Software Licensing

See the following commands for viewing license status:

- **show license all**

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

Note Migration from QuoVadis Root CA 2 to the IdenTrust Commercial Root CA 1 for SSL certificates affects smart licensing of FXOS. For FXOS 2.8.x or later, the issue can be resolved using the auto-import feature without an upgrade to the FXOS software. For devices that run any version of FXOS software, the issue can be resolved using the manual certificate import procedure without an upgrade to the FXOS software. For more information, see FXOS: QuoVadis Root CA 2 Decommission Might Affect Smart Licensing.

- **show license status**
- **show license techsupport**

History for Smart Software Licensing

Feature Name	Platform Releases	Description
Cisco Success Network	2.7.1	Cisco Success Network is a user-enabled cloud service. When you enable Cisco Success Network, a secure connection is established between the Firepower 4100/9300 chassis and the Cisco cloud to stream usage information and statistics. Streaming telemetry provides a mechanism that selects data of interest from the ASA and transmits it in a structured format to remote management stations to do the following: • Inform you of available unused features that can improve the effectiveness of the product in your network • Inform you of additional technical support services and monitoring that might be available for your product • Help Cisco improve our products Once you enroll in the Cisco Success Network, the chassis establishes and maintains the secure connection at all times. You can turn off this connection at any time by disabling Cisco Success Network, which disconnects the device from the Cisco Success Network cloud. We introduced the following commands: **scope telemetry {enable | disable}** We introduced the following screens: **System** > **Licensing** > **Cisco Success Network**
Cisco Smart Software Licensing for the Firepower 4100/9300 chassis	1.1(1)	Smart Software Licensing lets you purchase and manage a pool of licenses. Smart licenses are not tied to a specific serial number. You can easily deploy or retire devices without having to manage each unit's license key. Smart Software Licensing also lets you see your license usage and needs at a glance. Smart Software Licensing configuration is split between the Firepower 4100/9300 chassis supervisor and the security module. We introduced the following commands: **deregister, register idtoken, renew, scope callhome, scope destination, scope licdebug, scope license, scope monitoring, scope profile, set address, set http-proxy-server-enable on, set http-proxy-server-url, set http-proxy-server-port, show license all, show license status, show license techsupport**