ASA のライセンス管理

シスコ スマート ソフトウェア ライセンスによって、ライセンスを購入し、ライセンスのプールを一元管理することができます。各ユニットのライセンス キーを管理する必要なく、デバイスを簡単に導入または削除できます。スマート ソフトウェア ライセンスを利用すれば、ライセンスの使用状況と要件をひと目で確認することもできます。

（注） このセクションは、Firepower 4100/9300 シャーシ上の ASA 論理デバイスにのみ該当します。Firepower Threat Defense 論理デバイスのライセンスの詳細については、『Firepower Management Center Configuration Guide』を参照してください。

- スマート ソフトウェア ライセンスについて （1 ページ）
- スマート ソフトウェア ライセンスの前提条件 （16 ページ）
- スマート ソフトウェア ライセンスのガイドライン, on page 17
- スマート ソフトウェア ライセンスのデフォルト, on page 17
- 通常スマート ソフトウェア ライセンシングの設定 （17 ページ）
- Firepower 4100/9300 シャーシのスマート ライセンス サテライト サーバの設定 （22 ページ）
- パーマネント ライセンス予約の設定 （23 ページ）
- スマート ソフトウェア ライセンシングのモニタリング （25 ページ）
- スマート ソフトウェア ライセンスの履歴, on page 27

スマート ソフトウェア ライセンスについて

ここでは、スマート ソフトウェア ライセンスの仕組みについて説明します。

（注） このセクションは、Firepower 4100/9300 シャーシ上の ASA 論理デバイスにのみ該当します。Firepower Threat Defense 論理デバイスのライセンスの詳細については、『Firepower Management Center Configuration Guide』を参照してください。

ASA のススマート ソフトウェア ライセンシング

Firepower 4100/9300 シャーシ上の ASA アプリケーションの場合、スマート ソフトウェア ライセンス設定は Firepower 4100/9300 シャーシ スーパバイザとアプリケーションの間で分割されます。

- Firepower 4100/9300 シャーシ：ライセンス認証局との通信を行うためのパラメータを含めて、スーパバイザにすべてのスマート ソフトウェア ライセンス インフラストラクチャを設定します。Firepower 4100/9300 シャーシ 自体の動作にライセンスは必要ありません。

（注） シャーシ間クラスタリングでは、クラスタ内の各シャーシで同じスマート ライセンス方式を有効にする必要があります。

- ASA アプリケーション：アプリケーションのすべてのライセンスの権限付与を設定します。

Smart Software Manager とアカウント

デバイスの 1 つ以上のライセンスを購入する場合は、Cisco Smart Software Manager で管理します。

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

Smart Software Manager では、組織のマスター アカウントを作成できます。

（注） まだアカウントをお持ちでない場合は、このリンクをクリックして新しいアカウントをセットアップしてください。Smart Software Manager では、組織のマスター アカウントを作成できます。

デフォルトでは、ライセンスはマスターアカウントの下のデフォルトの仮想アカウントに割り当てられます。アカウントの管理者として、オプションで追加の仮想アカウントを作成できます。たとえば、地域、部門、または子会社ごとにアカウントを作成できます。複数の仮想アカウントを使用することで、多数のライセンスおよびデバイスの管理をより簡単に行うことができます。

オフライン管理

デバイスにインターネット アクセスがなく、License Authority に登録できない場合は、オフライン ライセンスを設定できます。

パーマネント ライセンスの予約

デバイスがセキュリティ上の理由でインターネットにアクセスできない場合、オプションで、各 ASA の永続ライセンスを要求できます。永続ライセンスでは、License Authority への定期的なアクセスは必要ありません。PAK ライセンスの場合と同様にライセンスを購入し、ASA のライセンス キーをインストールします。PAK ライセンスとは異なり、ライセンスの取得と管理に Smart Software Manager を使用します。通常のスマート ライセンス モードと永続ライセンスの予約モード間で簡単に切り替えることができます。

すべての機能、すなわちモデルの正しい最大スループットを備えた標準ティアおよびキャリアライセンスを有効にするライセンスを取得できます。ライセンスはFirepower4100/9300 シャーシ上で管理されますが、それに加えて ASA の設定で権限付与を要求することにより、ASA でそれらを使用できるようにする必要があります。

サテライト サーバ

デバイスがセキュリティ上の理由でインターネットにアクセスができない場合、オプションで、仮想マシン（VM）としてローカル Smart Software Manager サテライト サーバをインストールできます。サテライト（衛星）は、Smart Software Manager 機能のサブセットを提供し、これによりすべてのローカル デバイスに重要なライセンス サービスが提供可能になります。ライセンス使用を同期するために、定期的にサテライトだけが License Authority と同期する必要があります。スケジュールに沿って同期するか、または手動で同期できます。

サテライトアプリケーションをダウンロードして導入したら、インターネットを使用してCisco SSM にデータを送信しなくても、以下の機能を実行できます。

- ライセンスの有効化または登録
- 企業ライセンスの表示
- 会社のエンティティ間でのライセンス移動

詳細については、スマート アカウント マネージャ サテライトにある『Smart Software Manager satellite installation and configuration guide』を参照してください。

仮想アカウントごとに管理されるライセンスとデバイス

ライセンスとデバイスは仮想アカウントごとに管理されます。つまり、その仮想アカウントのデバイスのみが、そのアカウントに割り当てられたライセンスを使用できます。追加のライセンスが必要な場合は、別の仮想アカウントから未使用のライセンスを転用できます。仮想アカウント間でデバイスを転送することもできます。

Firepower 4100/9300 シャーシのみがデバイスとして登録され、シャーシ内の ASA アプリケーションはそれぞれ固有のライセンスを要求します。たとえば、3つのセキュリティ モジュールを搭載した Firepower 9300 シャーシでは、全シャーシが 1 つのデバイスとして登録されますが、各モジュールは合計 3 つのライセンスを別個に使用します。

評価ライセンス

Firepower 4100/9300 シャーシ は、次の 2 種類の評価ライセンスをサポートしています。

- シャーシ レベル評価モード：Firepower 4100/9300 シャーシによる Licensing Authority への登録の前に、評価モードで 90 日間（合計使用期間）動作します。このモードでは、ASA は固有の権限付与を要求できません。デフォルトの権限のみが有効になります。この期間が終了すると、Firepower 4100/9300 シャーシはコンプライアンス違反の状態になります。
- 権限付与ベースの評価モード：Firepower 4100/9300 シャーシが Licensing Authority に登録をした後、ASA に割り当て可能な時間ベースの評価ライセンスを取得できます。ASA で、通常どおりに権限付与を要求します。時間ベースのライセンスの期限が切れると、時間ベースのライセンスを更新するか、または永続ライセンスを取得する必要があります。

（注） 高度暗号化（3DES/AES）の評価ライセンスを取得することはできません。永続ライセンスのみでこの権限がサポートされます。

Smart Software Manager 通信

このセクションでは、デバイスが Smart Software Manager と通信する方法について説明します。

デバイス登録とトークン

各仮想アカウントに対し、登録トークンを作成できます。このトークンは、デフォルトで 30 日間有効です。各シャーシを導入するとき、または既存のシャーシを登録するときにこのトークン ID と権限付与レベルを入力します。既存のトークンの有効期限が切れている場合は、新しいトークンを作成できます。

導入した後、または既存のシャーシでこれらのパラメータを手動で設定した後、そのシャーシを起動するとシスコのライセンス認証局に登録されます。シャーシがトークンで登録されるとき、ライセンス認証局はシャーシとそのライセンス認証局との間で通信を行うために ID 証明書を発行します。この証明書の有効期間は 1 年ですが、6 か月ごとに更新されます。

ライセンス認証局との定期通信

デバイスはライセンス認証局と 30 日おきに通信します。Smart Software Manager に変更を加えた場合は、デバイス上で許可を更新し、すぐに変更されるようにすることができます。または、スケジュールどおりにデバイスが通信するのを待ちます。

必要に応じて、HTTP プロキシを設定できます。

Firepower 4100/9300 シャーシでは、少なくとも 90 日おきに、直接接続または HTTP プロキシを介したインターネット アクセスが必要です。通常のライセンス通信が 30 日ごとに行われますが、猶予期間によって、デバイスは Call Home なしで最大 90 日間動作します。猶予期間後、Licensing Authority に連絡しない限り、特別なライセンスを必要とする機能の設定変更を行なえませんが、動作には影響ありません。

（注） デバイスが 1 年間ライセンス認証局と通信できない場合、デバイスは強力な暗号化ライセンスを使用せずに未登録状態になります。

コンプライアンス逸脱状態

次の状況では、デバイスがコンプライアンスから逸脱している可能性があります。

- 使用超過：デバイスが利用できないライセンスを使用している場合。
- ライセンスの有効期限切れ：時間ベースのライセンスの有効期限が切れている場合。
- 通信の欠落：デバイスが再許可を得るために Licensing Authority に到達できない場合。

アカウントのステータスがコンプライアンス違反状態なのか、違反状態に近づいているのかを確認するには、Firepower 4100/9300 シャーシで現在使用中の権限付与とスマートアカウントのものを比較する必要があります。

コンプライアンス違反の場合、特別なライセンスが必要な機能への設定変更はできなくなりますが、その他の動作には影響ありません。たとえば、標準のライセンス制限を超える既存のコンテキストは実行を継続でき、その構成を変更することもできますが、新しいコンテキストを追加することはできません。

Smart Call Home インフラストラクチャ

デフォルトで、Smart Call Home のプロファイルは、ライセンス認証局の URL を指定する FXOS 設定内にあります。このプロファイルは削除できません。ライセンスプロファイルの設定可能なオプションは、ライセンス機関の宛先アドレス URL のみであることに注意してください。Cisco TAC に指示されない限り、License Authority の URL は変更しないでください。

Cisco Success Network

Cisco Success Network はユーザ対応のクラウド サービスです。Cisco Success Network を有効にすると、Firepower 4100/9300 シャーシ と Cisco Cloud 間にセキュアな接続が確立され、使用状況に関する情報と統計情報がストリーミングされます。テレメトリのストリーミングにより、対象データを ASA から選択して、構造化形式でリモート管理ステーションに送信するメカニズムが提供されるため、次のことが実現します。

- ネットワーク内の製品の有効性を向上させるために利用可能な未使用の機能が通知されます。
- 製品に付随する追加のテクニカル サポート サービスとモニタリングについて通知されます。
- シスコ製品の改善に役立ちます。

Cisco Smart Software Manager に Firepower 4100/9300 を登録するときは、Cisco Success Network を有効にします。Firepower セキュリティ アプライアンスの License Authority への登録 （19 ページ）を参照してください。

次の条件がすべて満たされている場合にのみ、Cisco Success Network に登録できます。

- スマート ソフトウェア ライセンスが登録されている
- スマートライセンスのサテライトモードが無効になっている
- パーマネントライセンスが無効になっている

Cisco Success Network に登録すると、シャーシは常にセキュアな接続を確立して維持します。Cisco Success Network を無効にすることで、いつでもこの接続をオフにできます。これにより、デバイスが Cisco Success Network クラウドから接続解除されます。

[System] > **[Licensing]** > **[Cisco Success Network]** ページで Cisco Success Network の登録ステータスを表示できます。また、登録ステータスを変更することもできます。Cisco Success Network の登録の変更 （20 ページ） を参照してください。

Cisco Success Network テレメトリ データ

Cisco Success Network により、シャーシの設定と動作状態に関する情報を 24 時間ごとに Cisco Success Network クラウドにストリーミングすることができます。収集およびモニタ対象のデータには、次の情報が含まれます。

- **登録済みデバイス情報**：Firepower 4100/9300 シャーシ のモデル名、製品 ID、シリアル番号、UUID、システム稼働時間、およびスマートライセンス情報。登録済みデバイス データ （7 ページ）を参照してください。
- **ソフトウェア情報**：Firepower 4100/9300 シャーシで実行されているソフトウェアのタイプとバージョン番号。ソフトウェア バージョン データ （7 ページ）を参照してください。
- **ASA デバイス情報**：Firepower 4100/9300 の セキュリティ モジュール/エンジン で稼動している ASA デバイスに関する情報。Firepower 4100 シリーズ の場合は、単一の ASA デバイスに関する情報のみが対象になることに注意してください。ASA デバイス情報には、各デバイス、デバイスモデル、シリアル番号、およびソフトウェアバージョンに使用されるスマートライセンスが含まれます。ASA デバイスデータ （8 ページ）を参照してください。
  - **パフォーマンス情報**：ASA デバイスのシステム稼働時間、CPU 使用率、メモリ使用率、ディスク容量の使用率、および帯域幅の使用状況に関する情報。パフォーマンス データ （8 ページ）を参照してください。
  - **使用状況**：機能ステータス、クラスタ、フェールオーバー、およびログイン情報。
    - **機能ステータス**：設定済みまたはデフォルトで有効になっている ASA 機能のリスト。
    - **クラスタ情報**：ASA デバイスがクラスタモードの場合は、クラスタ情報が表示されます。ASA デバイスがクラスタモードではない場合、この情報は表示されません。クラスタ情報には、ASA デバイスのクラスタグループ名、クラスタインター

フェイスモード、ユニット名、および状態が含まれます。同じクラスタ内の他のピア ASA デバイスの場合、クラスタ情報には名前、状態、およびシリアル番号が含まれます。

- **フェールオーバー情報**：ASA がフェールオーバーモードの場合、フェールオーバー情報が表示されます。ASA がフェールオーバーモードではない場合、この情報は表示されません。フェールオーバー情報には、ASA のロールと状態、およびピア ASA デバイスのロール、状態、およびシリアル番号が含まれます。
- **ログイン履歴**：ASA デバイスで最後にログインに成功したユーザのログイン頻度、ログイン時間、および日付スタンプ。ただし、ログイン履歴にはユーザのログイン名、ログイン情報、その他の個人情報は含まれません。

詳細については、使用状況データ （9 ページ）を参照してください。

登録済みデバイス データ

Cisco Success Network に Firepower 4100/9300 シャーシ を登録したら、シャーシに関するテレメトリデータの Cisco Cloud へのストリーミングを選択します。収集およびモニタ対象のデータを次の表に示します。

表 *1*：登録済みデバイスのテレメトリ データ

データ ポイント	値の例
デバイス モデル	Cisco Firepower FP9300 セキュリティ アプライアンス
シリアル番号	GMX1135L01K
スマートライセンス PIID	752107e9-e473-4916-8566-e26d0c4a5bd9
スマートライセンスの仮想アカウント名	FXOS-general
システムの動作期間	32115
UDI 製品 ID	FPR-C9300-AC

ソフトウェア バージョン データ

Cisco Success Network には、タイプやソフトウェアバージョンといったソフトウェア情報が収集されます。収集およびモニタ対象のソフトウェア情報を次の表に示します。

表 *2*：ソフトウェア バージョンのテレメトリ データ

データ ポイント	値の例
タイプ	package_version
Version	2.7(1.52)

ASA デバイスデータ

Cisco Success Network には、 Firepower 4100/9300 の セキュリティ モジュール/エンジン で稼動している ASA デバイスに関する情報が収集されます。収集およびモニタ対象の ASA デバイス情報を次の表に示します。

表 *3: ASA* デバイステレメトリデータ

データ ポイント	値の例
ASA デバイス PID	FPR9K-SM-36
ASA デバイスモデル	Cisco Adaptive Security Appliance
ASA デバイスのシリアル番号	XDQ311841WA
展開タイプ（ネイティブまたはコンテナ）	Native
セキュリティ コンテキスト モード（シングルまたはマルチ）	シングル

ASA のソフトウェアバージョン	{
	type: "asa_version",
	ersion: "9.13.1.5"
	}

デバイスマネージャのバージョン	{
	type: "device_mgr_version",
	version: "7.10.1"
	}

使用中の有効なスマートライセンス	{
	"type": "Strong encryption",
	"tag":
	"regid.2016-05.com.cisco.ASA-GEN-STRONG-ENCRYPTION,
	5.7_982308k4-74w2-5f38-64na-707q99g10cce",
	"count": 1
	}

パフォーマンス データ

Cisco Success Network には、ASA デバイス固有のパフォーマンス情報が収集されます。この情報には、システム稼働時間、CPU使用率、メモリ使用率、ディスク容量の使用率、および帯域幅の使用状況が含まれます。

- **CPU 使用率**：過去 5 分間の CPU 使用率情報
- **メモリ使用率**：システムの空きメモリ、使用メモリ、および合計メモリ
- **ディスク使用率**：ディスクの空き容量、使用済み容量、および合計容量の情報
- **システムの稼働時間**：システムの稼働時間情報
- **帯域幅の使用状況**：システム帯域幅の使用状況（nameif が設定されたすべてのインターフェイスから集約）

これは、システムの稼働時間以降に受信および送信された1秒あたりのパケット（またはバイト）の統計情報を示します。

収集およびモニタ対象の情報を次の表に示します。

表 *4:* パフォーマンス テレメトリデータ

データ ポイント	値の例
過去 5 分間のシステム CPU 使用率	{ “fiveSecondsPercentage”:0.2000000, “oneMinutePercentage”: 0, “fiveMinutesPercentage”: 0 }
システム メモリ使用率	{ “freeMemoryInBytes”:225854966384, “usedMemoryInBytes”: 17798281616, “totalMemoryInBytes”:243653248000 }
システムのディスク使用率	{ "freeGB": 21.237285, "usedGB": 0.238805, "totalGB": 21.476090 }
システムの動作期間	99700000
システム帯域幅の使用状況	{ "receivedPktsPerSec": 3, "receivedBytesPerSec": 212, "transmittedPktsPerSec": 3, "transmittedBytesPerSec": 399 }

使用状況データ

Cisco Success Network には、シャーシの セキュリティ モジュール/エンジン で稼動しているASAデバイスの機能ステータス、クラスタ、フェールオーバー、およびログイン情報が収集されます。ASA デバイス使用率に関して収集およびモニタされる情報を次の表に示します。

表 *5:* テレメトリデータの使用率

データ ポイント	値の例

機能ステータス	[{
	"name": "cluster",
	"status": "enabled"
	},
	{
	"name": "webvpn",
	"status": "enabled"
	},
	{
	"name": "logging-buffered",
	"status": "debugging"
	}]

クラスタ情報	{
	"clusterGroupName": "asa-cluster",
	"interfaceMode": "spanned",
	"unitName": "unit-3-3",
	"unitState": "SLAVE",
	"otherMembers": {
	"items": [
	{
	"memberName": "unit-2-1",
	"memberState": "MASTER",
	
	"memberSerialNum": "DAK391674E"
	}
	]
	}
	
	}

フェールオーバー情報	{
	myRole: "Primary",
	peerRole: "Secondary",
	myState: "active",
	peerState: "standby",
	peerSerialNum:
	"DAK39162B"
	}

ログイン履歴	{
	"loginTimes": "1 times in last 1 days",
	"lastSuccessfulLogin": "12:25:36 PDT Mar 11
	2019"
	}

テレメトリ ファイルの例

Firepower 4100/9300 シャーシ テレメトリが有効でオンライン状態にあるすべての ASA デバイスから受信されたデータは、シャーシ固有の情報やその他のフィールドと集約されてから Cisco Cloud に送信されます。テレメトリデータを持つアプリケーションがない場合でも、テレメトリはシャーシ情報とともに Cisco Cloud に送信されます。

以下は、Cisco Success Network テレメトリファイルの例です。このファイルには、Cisco Cloud に送信された Firepower 9300 の 2 台の ASA デバイスの情報が保存されています。

```
{
  "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"
            }
          ]
        }
      }
    ]
  }
 }
}
```


スマート ソフトウェア ライセンスの前提条件

- この章は、Firepower 4100/9300 シャーシ上の ASA 論理デバイスにのみ該当します。Firepower Threat Defense 論理デバイスのライセンスの詳細については、『Firepower Management Center Configuration Guide』を参照してください。
- Cisco Smart Software Manager でマスター アカウントを作成します。

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

  まだアカウントをお持ちでない場合は、このリンクをクリックして新しいアカウントをセットアップしてください。Smart Software Manager では、組織のマスター アカウントを作成できます。
- Cisco Commerce Workspace から 1 つ以上のライセンスを購入します。ホーム ページの [製品とソリューションを検索（Find Products and Solutions）] フィールドで、該当するプラットフォームを検索します。一部のライセンスは無料ですが、スマート ソフトウェア ライセンス アカウントにそれらを追加する必要があります。
- シャーシがライセンス機関と通信できるように、シャーシからのインターネットアクセスまたは HTTP プロキシ アクセスを確保します。
- シャーシがライセンス機関の名前を解決できるように、DNS サーバを設定します。

- シャーシのための時間を設定します。
- ASA ライセンス資格を設定する前に、Firepower 4100/9300 シャーシでスマート ソフトウェア ライセンス インフラストラクチャを設定します。

スマート ソフトウェア ライセンスのガイドライン

フェイルオーバー クラスタリングのための ASA ガイドライン

各 Firepower 4100/9300 シャーシは、License Authority またはサテライト サーバに登録される必要があります。セカンダリ ユニットに追加費用はかかりません。 永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入する必要があります。

スマート ソフトウェア ライセンスのデフォルト

Firepower 4100/9300 シャーシ のデフォルト設定には、ライセンス認証局の URL を指定する「SLProfile」という Smart Call Home のプロファイルが含まれています。

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

通常スマート ソフトウェア ライセンシングの設定

Cisco License Authority と通信するため、必要に応じて HTTP プロキシを設定できます。License Authority に登録するには、スマート ソフトウェア ライセンス アカウントから取得した Firepower 4100/9300 シャーシ の登録トークン ID を入力する必要があります。

手順

ステップ 1 （任意）HTTP プロキシの設定 （18 ページ）。

ステップ 2 （任意）Call Home URL の削除 （18 ページ）

ステップ 3 Firepower セキュリティ アプライアンスの License Authority への登録 （19 ページ）。

（任意）HTTP プロキシの設定

ネットワークでインターネット アクセスに HTTP プロキシを使用する場合、スマート ソフトウェア ライセンシング用のプロキシ アドレスを設定する必要があります。このプロキシは、一般に Smart Call Home にも使用されます。

（注） 認証を使用する HTTP プロキシはサポートされません。

手順

ステップ 1 HTTP プロキシを有効化します。

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

例：

```
scope monitoring
  scope call-home
    set http-proxy-server-enable on
```

ステップ 2 プロキシ URL を設定します。

set http-proxy-server-url *url*

url はプロキシ サーバの http または https アドレスです。

例：

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

ステップ 3 ポートを設定します。

set http-proxy-server-port *port*

例：

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

ステップ 4 バッファをコミットします。

commit-buffer

（任意）Call Home URL の削除

以前に設定された Call Home URL を削除するには、次の手順を実行します。

手順

ステップ 1 モニタリング範囲を入力します。

scope monitoring

ステップ 2 Call Home 範囲を入力します。

scope callhome

ステップ 3 SLProfile を探します。

scope profile SLProfile

ステップ 4 宛先を表示します。

show destination

例：

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

ステップ 5 URL を削除します。

delete destination SLDest

ステップ 6 バッファを確定します。

commit-buffer

Firepower セキュリティ アプライアンスの License Authority への登録

Firepower 4100/9300 シャーシ を登録すると、ライセンス認証局によって Firepower 4100/9300 シャーシ とライセンス認証局との間の通信に使用される ID 証明書が発行されます。また、Firepower4100/9300 シャーシが該当する仮想アカウントに割り当てられます。通常、この手順は 1 回限りのインスタンスです。ただし、通信の問題などが原因で ID 証明書の期限が切れた場合は、Firepower 4100/9300 シャーシ の再登録が必要になります。

手順

ステップ 1 Smart Software Manager または Smart Software Manager Satellite で、このFirepower 4100/9300 シャーシの追加先となるバーチャル アカウントの登録トークンを要求してコピーします。

スマート ソフトウェア マネージャ サテライトを使用して登録トークンを要求する方法について詳しくは、『Cisco Smart Software Manager Satellite User Guide』（https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html）を参照してください。

ステップ 2 Firepower 4100/9300 シャーシ の登録トークンを入力します。

scope license

register idtoken *id-token*

例：

```
scope license
  register idtoken ZGFmNWM5NjgtYmNjYS00ZWI3L
WE3NGItMWJkOGExZjIxNGQ0LTE0NjI2NDYx%0AMDIzNT
V8N3R0dXM1Z0NjWkdpR214eFZhMldBOS9CVnNEYnVKM1
g3R3dvemRD%0AY29NQT0%3D%0A
```

ステップ 3 後からデバイスの登録を解除するには、次を入力します。

scope license

deregister

Firepower 4100/9300 シャーシの登録を解除すると、アカウントからデバイスが削除されます。さらに、デバイス上のすべてのライセンス資格と証明書が削除されます。登録を解除することで、ライセンスを新しい Firepower 4100/9300 シャーシ に利用することもできます。または、Smart Software Manager からデバイスを削除することもできます。

ステップ 4 ID 証明書を更新し、すべてのセキュリティ モジュールの資格を更新するには、次を入力します。

scope license

scope licdebug

renew

デフォルトでは、アイデンティティ証明書は 6 ヵ月ごと、ライセンス資格は 30 日ごとに自動的に更新されます。インターネット アクセスの期間が限られている場合や、Smart Software Manager でライセンスを変更した場合などは、これらの登録を手動で更新することもできます。

Cisco Success Network の登録の変更

Cisco Smart Software Manager に Firepower 4100/9300 を登録するときは、Cisco Success Network を有効にします。その後、次の手順を使用して、登録ステータスを表示または変更します。

（注） Cisco Success Network は評価モードでは機能しません。

手順

ステップ 1 システム範囲を入力します。

scope system

例：

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

ステップ 2 サービス範囲を入力します。

scope services

例：

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

ステップ 3 テレメトリ範囲を入力します。

scope telemetry

例：

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

ステップ 4 Cisco Success Network 機能の有効化または無効化

{enable | disable}

例：

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

ステップ 5 Firepower 4100/9300 Chassis で Cisco Success Network のステータスを確認します。

show detail

例：

Admin State に Cisco Success Network の正しいステータスが表示されていることを確認します。

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

例：

Oper State に **OK** が表示されることを確認します。これはテレメトリデータが送信済みであることを示します。

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

Firepower 4100/9300 シャーシのスマート ライセンス サテライト サーバの設定

スマート ライセンス サテライト サーバを使用するように Firepower 4100/9300 シャーシを設定するには、次の手順に従います。

始める前に

- スマート ソフトウェア ライセンスの前提条件 （16 ページ）に記載のすべての前提条件を満たす必要があります。
- Smart Software Satellite Server を展開して設定します。

  スマート ライセンス サテライト OVA ファイルを Cisco.com からダウンロードし、VMwareESXi サーバにインストールおよび設定します。詳細については、『Smart Software Manager satellite Install Guide』を参照してください。
- 内部 DNS サーバによって Smart Software Satellite Server の FQDN が解決できることを確認します。
- サテライト トラストポイントがすでに存在しているかどうかを確認します。

  scope security

  show trustpoint

  FXOS バージョン 2.4(1) 以降では、トラストポイントはデフォルトで追加されることに注意してください。トラストポイントが存在しない場合は、次の手順を使用して手動で追加する必要があります。

  1. http://www.cisco.com/security/pki/certs/clrca.cer に移動し、SSL 証明書の本文全体（"-----BEGIN CERTIFICATE-----" から "-----END CERTIFICATE-----" まで）を、設定中にアクセスできる場所にコピーします。
  2. セキュリティ モードを開始します。

     scope security
  3. トラスト ポイントを作成して名前を付けます。

     create trustpoint *trustpoint_name*
  4. トラスト ポイントの証明書情報を指定します。証明書は、Base64 エンコード X.509（CER）フォーマットである必要があることに注意してください。

     set certchain *certchain*

     certchain 変数には、ステップ 1 でコピーした証明書のテキストを貼り付けます。

     コマンドで証明書情報を指定しない場合、ルート認証局（CA）への認証パスを定義するトラストポイントのリストまたは証明書を入力するように求められます。入力内容の次の行に、**ENDOFBUF** と入力して終了します。

5. 設定をコミットします。

   commit-buffer

手順

ステップ 1 callhome の接続先としてサテライト サーバをセットアップします。

scope monitoring

scope callhome

scope profile SLProfile

scope destination SLDest

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

ステップ 2 Firepower 4100/9300 シャーシ をライセンス認証局に登録します（Firepower セキュリティ アプライアンスの License Authority への登録 （19 ページ）を参照）。スマート ライセンス マネージャ サテライトの登録トークンを要求し、コピーする必要があることに注意してください。

パーマネント ライセンス予約の設定

Firepower 4100/9300 シャーシにパーマネント ライセンスを割り当てることができます。このユニバーサル予約では、デバイスで無制限の数の使用権を使用できるようになります。

（注） Smart Software Manager で使用できるように、開始前にパーマネント ライセンスを購入する必要があります。すべてのアカウントがパーマネント ライセンスの予約について承認されているわけではありません。設定を開始する前にこの機能についてシスコの承認があることを確認します。

パーマネント ライセンスのインストール

以下の手順は、Firepower 4100/9300 シャーシにパーマネント（永続）ライセンスを割り当てる方法を示しています。

手順

ステップ 1 FXOS CLI から、ライセンスの予約を有効化します。

scope license

enable reservation

ステップ 2 ライセンス予約を開始します。

scope license

scope reservation

ステップ 3 予約リクエスト コードを生成します。

request universal

show license resvcode

ステップ 4 Cisco Smart Software Manager ポータルの Smart Software Manager インベントリ画面に移動して、**Licenses** タブをクリックします。

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

Licenses タブにアカウントに関連するすべての既存のライセンスが、標準およびパーマネントの両方とも表示されます。

ステップ 5 **License Reservation** をクリックして、生成された予約リクエスト コードをボックスに入力します。

ステップ 6 **Reserve License** をクリックします。

Smart Software Manager が承認コードを生成します。コードをダウンロードまたはクリップボードにコピーできます。この時点で、ライセンスは、Smart Software Manager に従って使用中です。

License Reservation ボタンが表示されない場合、お使いのアカウントにはパーマネント ライセンスの予約が許可されていません。この場合、パーマネント ライセンスの予約を無効にして標準のスマート ライセンス コマンドを再入力する必要があります。

ステップ 7 FXOS CLI で、ライセンスの適用範囲を入力します。

scope license

ステップ 8 予約範囲を入力します。

scope reservation

ステップ 9 承認コードを入力します。

install *code*

これで Firepower 4100/9300 シャーシには PLR で完全にライセンスが適用されました。

ステップ 10 ASA 論理デバイスで機能のライセンス資格を有効にします。ライセンス資格を有効にするには、ASA ライセンスの章を参照してください。

（任意）パーマネント ライセンスの返却

パーマネント ライセンスが不要になった場合、この手順で Smart Software Manager に正式に返却する必要があります。すべてのステップに従わないと、ライセンスが使用状態のままになり、別の場所で使用できません。

手順

ステップ 1 FXOS CLI で、ライセンスの適用範囲を入力します。

scope license

ステップ 2 予約範囲を入力します。

scope reservation

ステップ 3 パーマネント ライセンスを返却します。

return

ただちに Firepower 4100/9300 シャーシ のライセンスがなくなり、評価状態に移行します。

ステップ 4 返却予約コードを表示してコピーします。

show license resvcode

ステップ 5 FXOS ユニバーサル デバイス識別子（UDI）を表示してコピーします。これで、Smart Software Manager で FXOS インスタンスを見つけることができます。

show license udi

ステップ 6 Smart Software Manager インベントリ画面に移動して、**Product Instances** タブをクリックします。

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

ステップ 7 ユニバーサル デバイス識別子（UDI）を使用して Firepower 4100/9300 シャーシを検索します。

ステップ 8 **Actions** > **Remove** の順に選択して、生成された返却予約コードをボックスに入力します。

ステップ 9 **Remove Product Instance** をクリックします。

パーマネント ライセンスが使用可能なライセンスのプールに戻されます。

ステップ 10 システムをリブートします。Firepower 4100/9300 シャーシの再起動の方法については、Firepower 4100/9300 Chassis の再起動を参照してください。

スマート ソフトウェア ライセンシングのモニタリング

ライセンスのステータスを表示するには、次のコマンドを参照してください。

- **show license all**

  スマート ソフトウェア ライセンシングの状態、スマート エージェントのバージョン、UDI 情報、スマート エージェントの状態、グローバル コンプライアンス ステータス、権限付与ステータス、ライセンス証明書情報、およびスマート エージェント タスクのスケジュールを表示します。

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

スマート ソフトウェア ライセンスの履歴

機能名	プラットフォーム リリース	説明
Cisco Success Network	2.7.1	Cisco Success Network はユーザ対応のクラウド サービスです。Cisco Success Network を有効にすると、Firepower 4100/9300 シャーシと Cisco Cloud 間にセキュアな接続が確立され、使用状況に関する情報と統計情報がストリーミングされます。テレメトリのストリーミングにより、対象データを ASA から選択して、構造化形式でリモート管理ステーションに送信するメカニズムが提供されるため、次のことが実現します。 • ネットワーク内の製品の有効性を向上させるために利用可能な未使用の機能が通知されます。 • 製品に付随する追加のテクニカル サポート サービスとモニタリングについて通知されます。 • シスコ製品の改善に役立ちます。 Cisco Success Network に登録すると、シャーシは常にセキュアな接続を確立して維持します。Cisco Success Network を無効にすることで、いつでもこの接続をオフにできます。これにより、デバイスが Cisco Success Network クラウドから接続解除されます。 次のコマンドを導入しました。 **scope telemetry {enable | disable}** 次の画面が導入されました。 **[システム（System）] > [ライセンス（Licensing）] > [Cisco Success Network]**

機能名	プラットフォーム リリース	説明
Firepower 4100/9300 シャーシ向けシスコ スマート ソフトウェア ライセンシング	1.1(1)	スマート ソフトウェア ライセンスによって、ライセンスを購入し、ライセンスのプールを管理することができます。スマートライセンスは特定のシリアル番号に結び付けられていません。各ユニットのライセンス キーを管理する必要なく、デバイスを簡単に導入または削除できます。スマート ソフトウェア ライセンスを利用すれば、ライセンスの使用状況と要件をひと目で確認することもできます。スマート ソフトウェア ライセンスの設定は、Firepower 4100/9300 シャーシ スーパバイザとセキュリティ モジュール間で分割されます。 **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** コマンドが導入されました