FMCおよびFTDのスマートライセンス登録と一般的な問題を使用したトラブルシューティング

内容

はじめに

このドキュメントでは、Firepower Threat Defense(FTD)管理対象デバイスでのFirepower Management Center(FMC)のスマートライセンス登録の設定について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

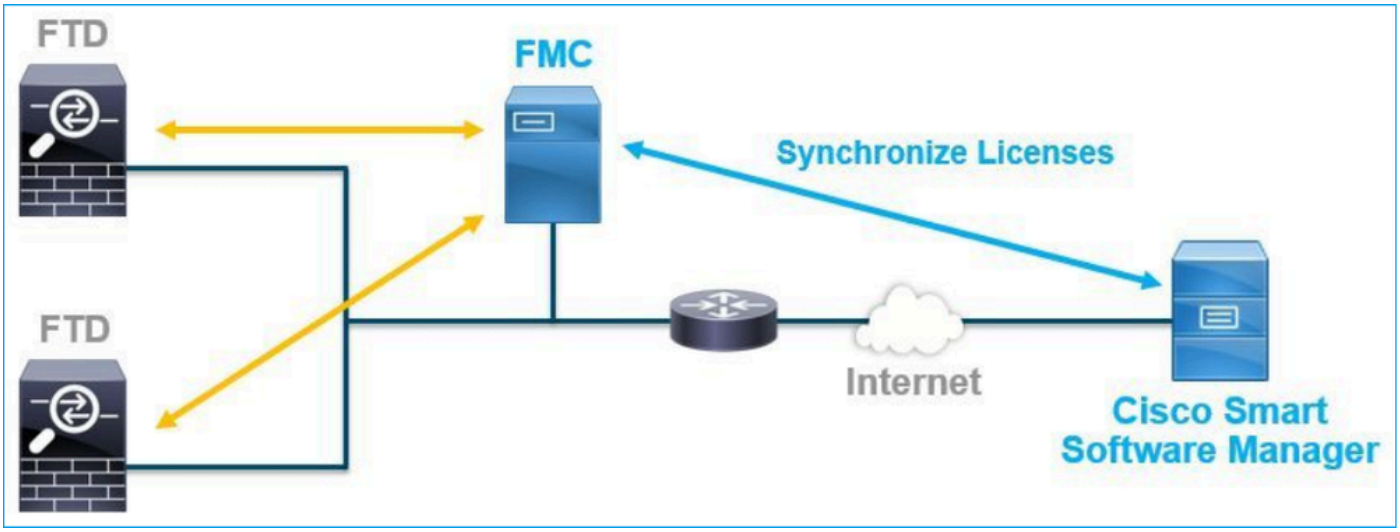
使用するコンポーネント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

FMC、FTD、およびスマートライセンスの登録

スマートライセンスの登録は、Firepower Management Center(FMC)で実行されます。FMCは、インターネット経由でCisco Smart Software Manager(CSSM)ポータルと通信します。CSSMでは、ファイアウォール管理者がスマートアカウントとそのライセンスを管理します。FMCは、管理対象のFirepower Threat Defense(FTD)デバイスにライセンスを自由に割り当てたり、削除したりできます。つまり、FTDデバイスのライセンスはFMCで一元管理されます。



FTDデバイスの特定の機能を使用するには、追加ライセンスが必要です。お客様がFTDデバイスに割り当てることができるスマートライセンスタイプについては、「FTDライセンスのタイプおよび制限」を参照してください。

BaseライセンスはFTDデバイスに含まれています。このライセンスは、FMCがCSSMに登録されると、スマートアカウントに自動的に登録されます。
期間ベースのライセンス：脅威、マルウェア、URLフィルタリングはオプションです。ライセンスに関連する機能を使用するには、ライセンスをFTDデバイスに割り当てる必要があります。

FTD管理にFirepower Management Center(FMCv)Virtual(FMCv)を使用するには、FMCvに対してCSSMのFirepower MCvデバイスライセンスも必要です。

FMCvライセンスはソフトウェアに含まれており、無期限です。

また、発生する可能性のある一般的なライセンス登録エラーのトラブルシューティングに役立つシナリオが、このドキュメントに記載されています。

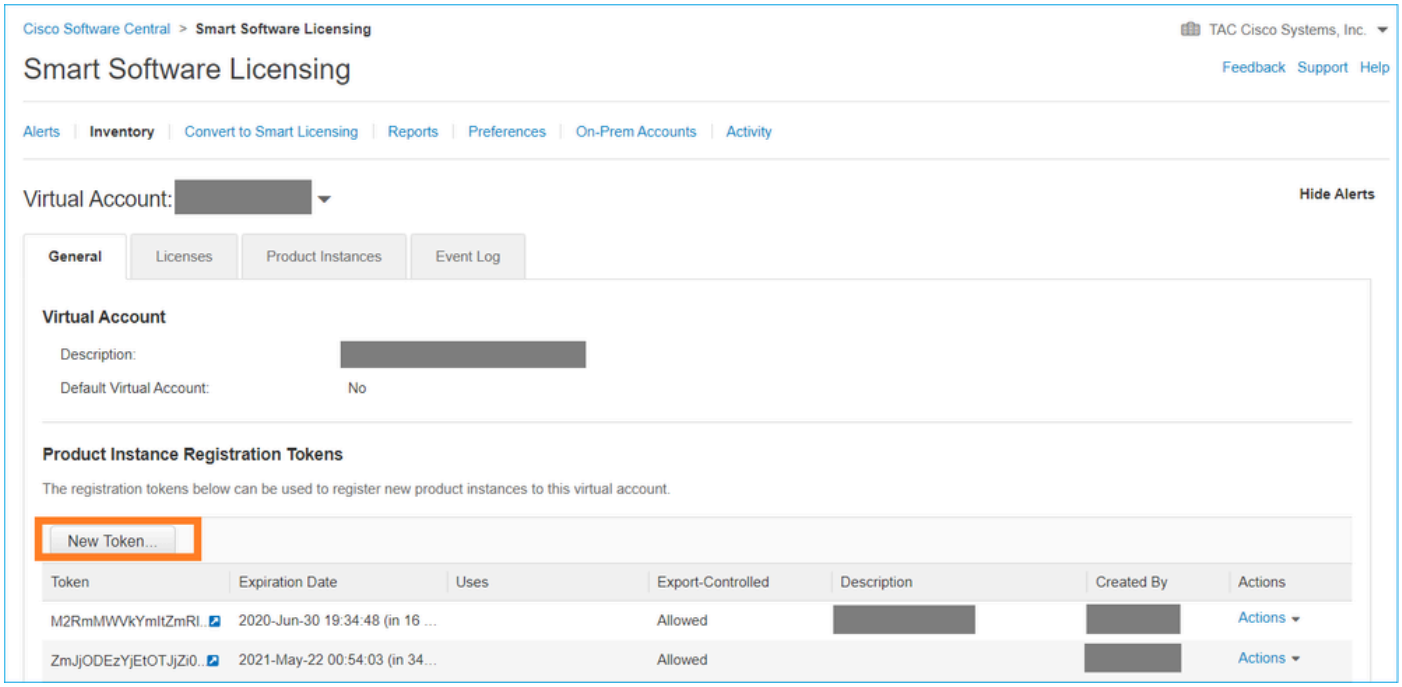
ライセンスの詳細については、「Cisco Firepowerシステム機能ライセンス」および「Firepowerライセンスに関するよく寄せられる質問(FAQ)」を参照してください。

FMCスマートライセンスの登録

前提条件

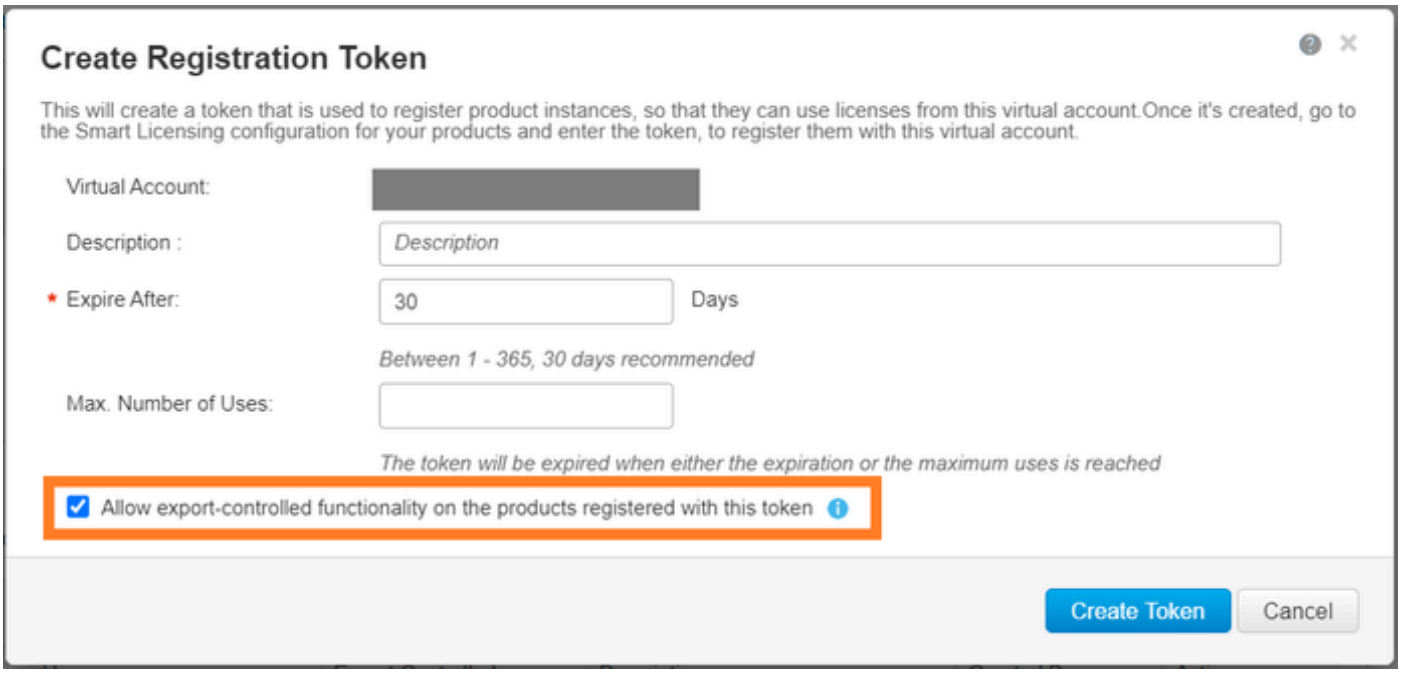
1. スマートライセンスの登録では、FMCがインターネットにアクセスする必要があります。証明書はHTTPSを使用してFMCとスマートライセンスクラウド間で交換されるため、通信に影響を与えたり、通信を変更したりする可能性のあるデバイスがパスにないことを確認します。（ファイアウォール、プロキシ、SSL復号化デバイスなど）。

2. 次の図に示すように、CSSMにアクセスし、Inventory > General > New Tokenボタンでトークンを発行します。



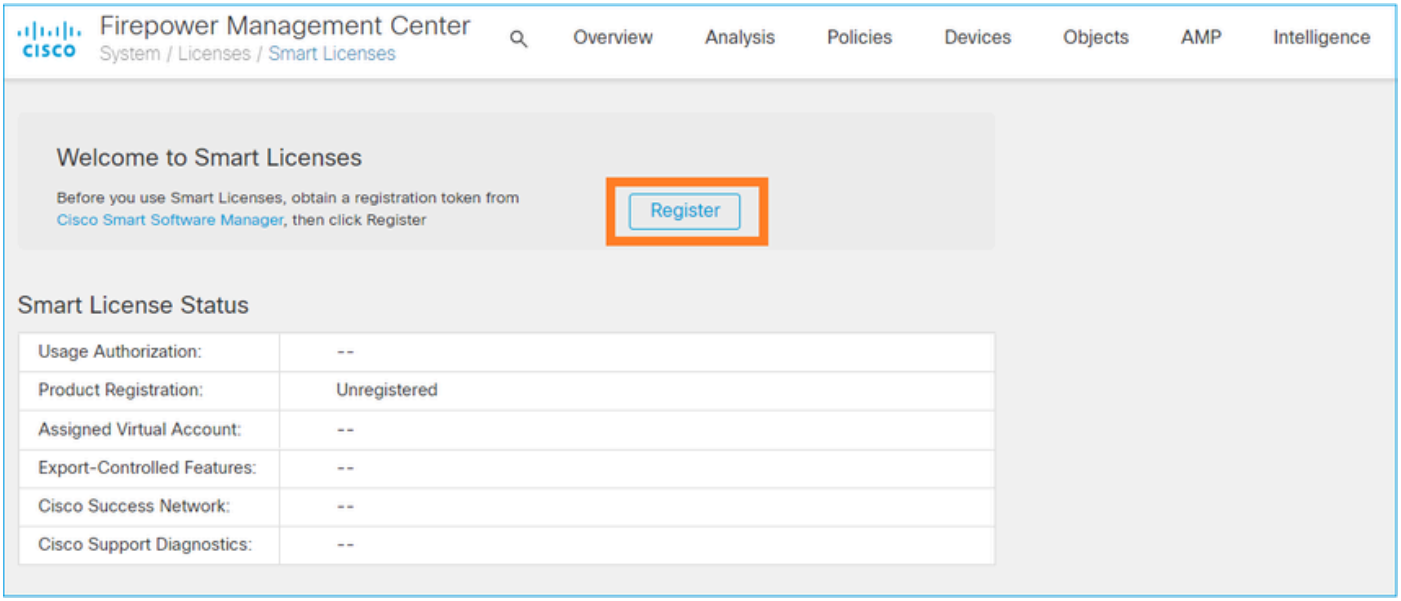
強力な暗号化を使用するには、Allow export-controlled functionality on the products registered with this tokenオプションを有効にします。有効にすると、チェックボックスにチェックマークが表示されます。

3. Create Tokenを選択します。

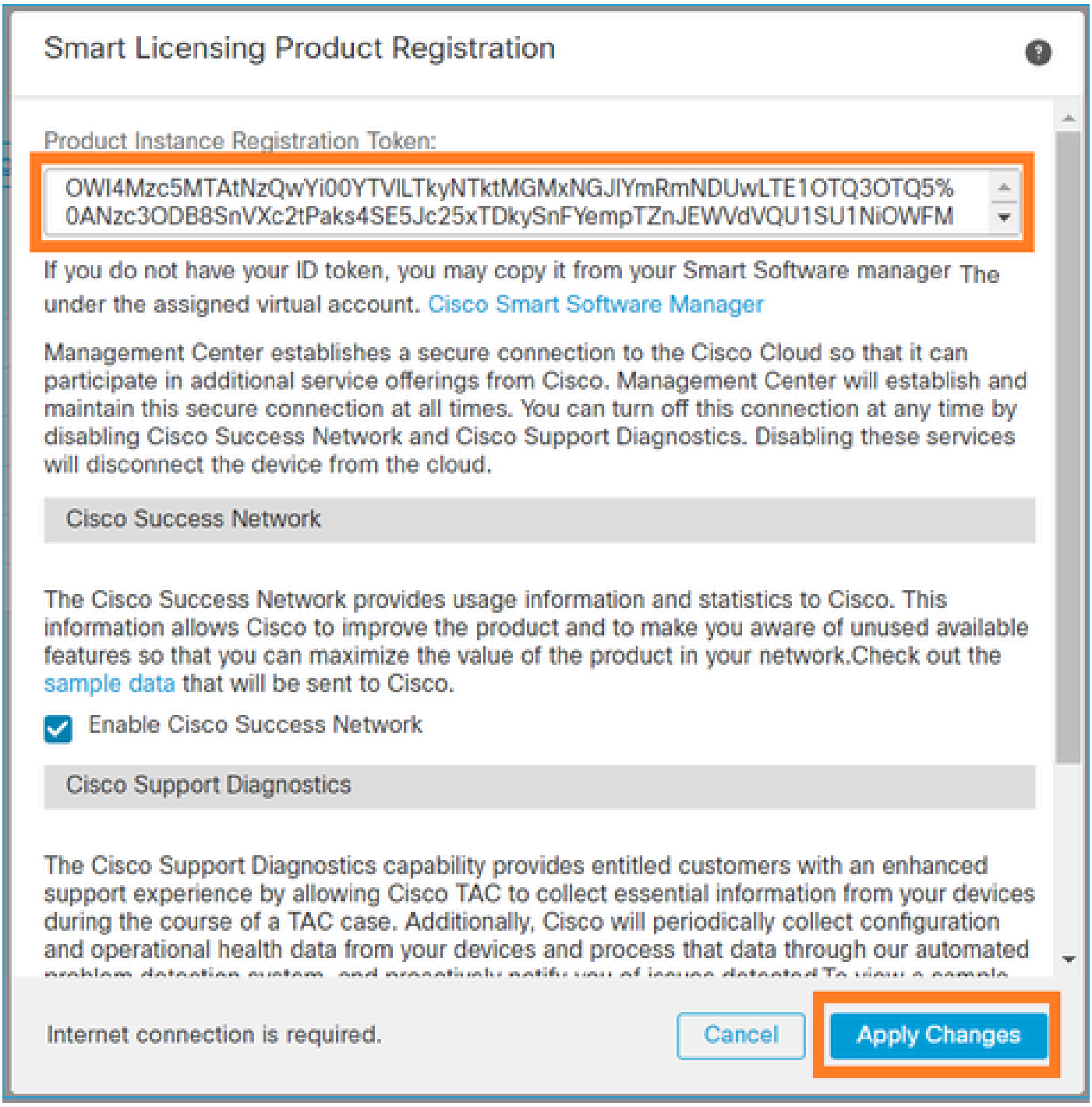


FMCスマートライセンスの登録

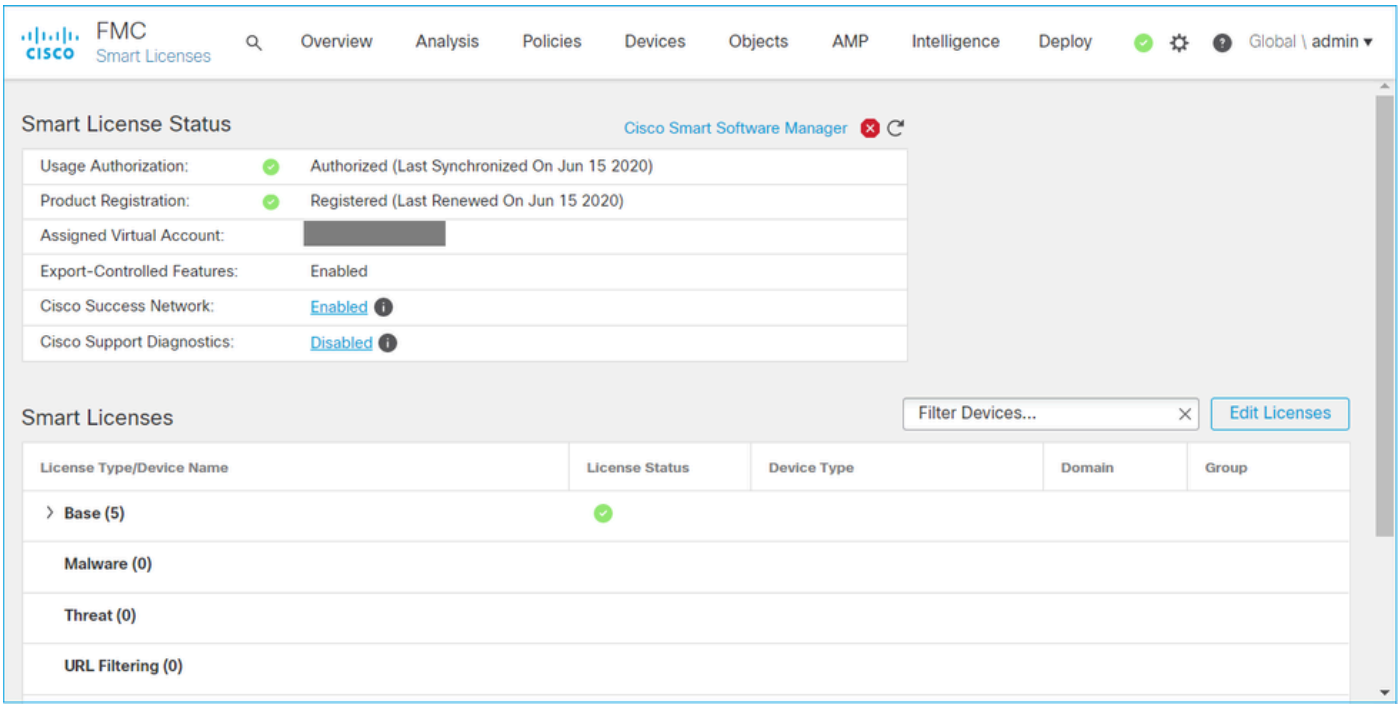
次の図に示すように、FMCでSystem> Licenses > Smart Licensesの順に移動し、Registerボタンを選択します。



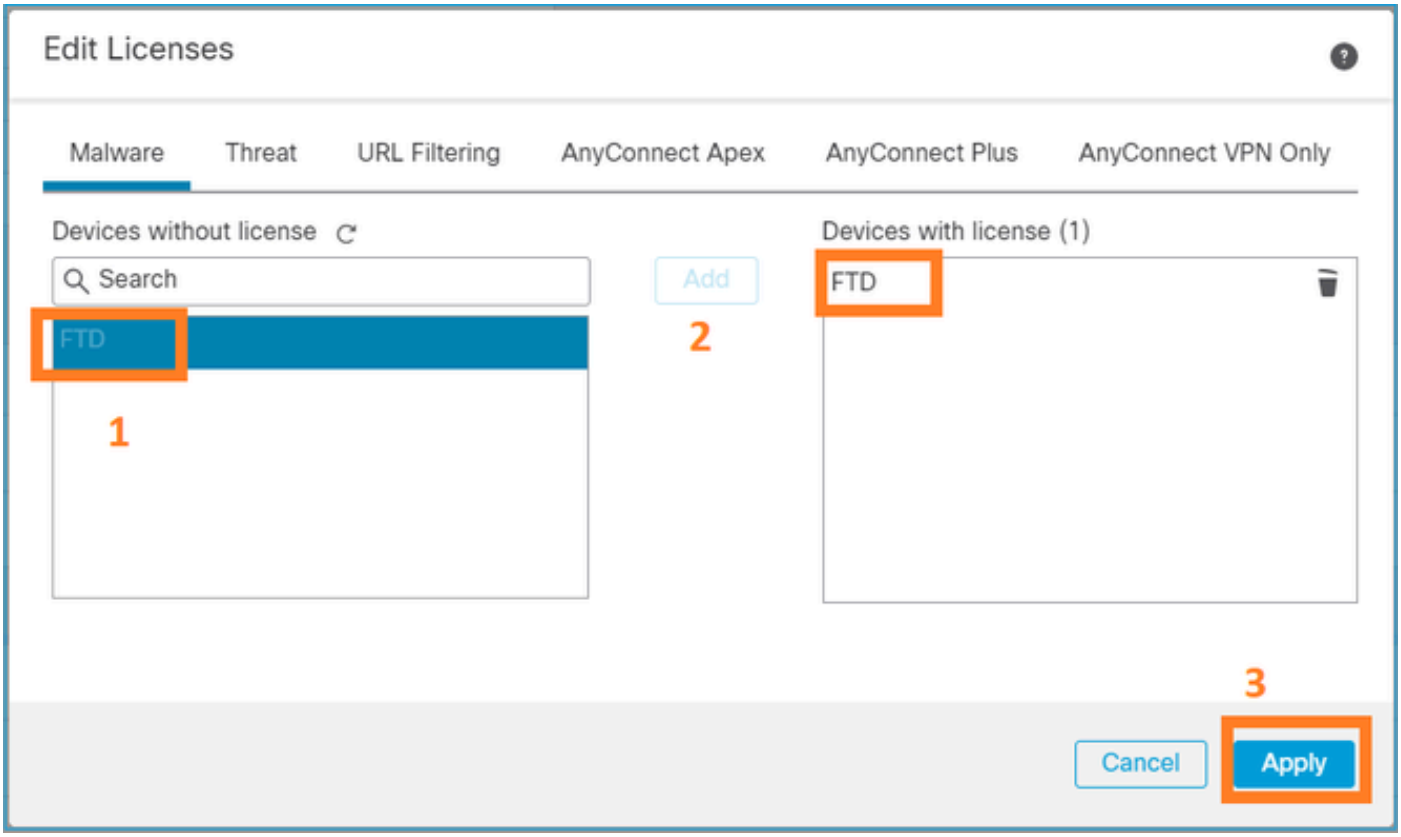
Smart Licensing Product Registrationウィンドウでトークンidを入力し、次の図に示すようにApply Changesを選択します。



スマートライセンスが正常に登録されると、次の図に示すように、製品登録のステータスが登録済みと表示されます。

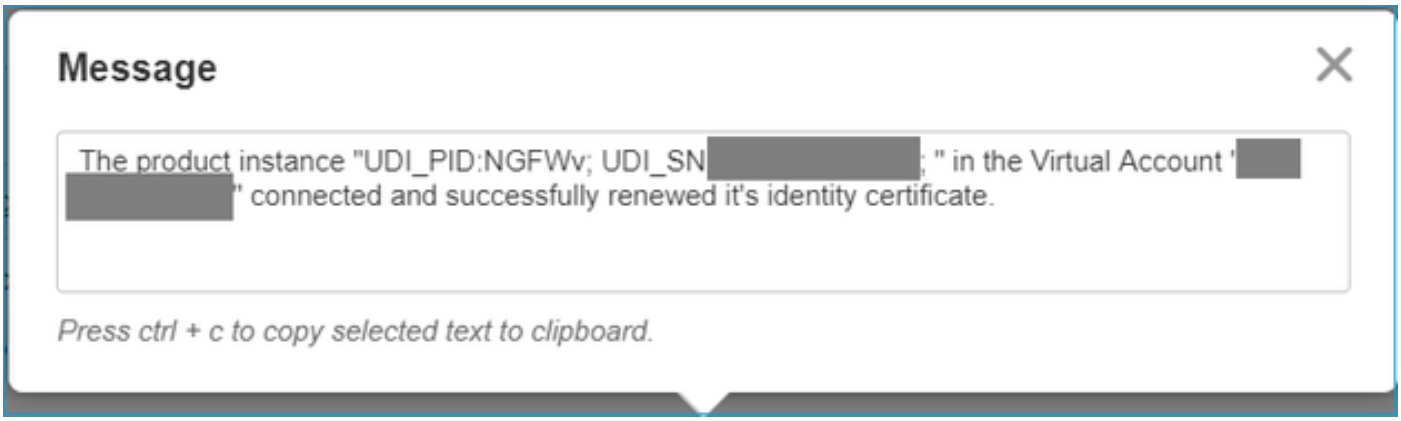


FTDデバイスに期間ベースのライセンスを割り当てるには、Edit Licensesを選択します。次に、管理対象デバイスを選択し、「ライセンスを持つデバイス」セクションに追加します。最後に、この図に示すようにApplyボタンを選択します。



Smart Software Manager(SSM)側での確認

FMCスマートライセンス登録の成功は、次の図に示すように、CSSMのInventory > Event Logで確認できます。

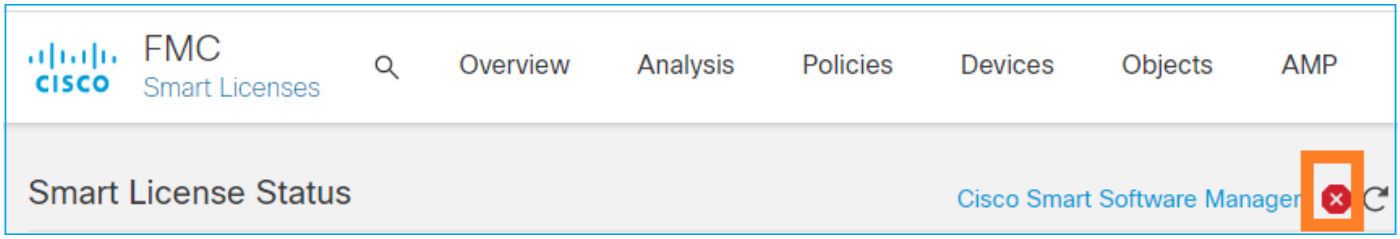


FMCの登録ステータスは、Inventory > Product Instancesで確認できます。Event Logタブでイベントログを確認します。 スマートライセンスの登録と使用状況は、インベントリ>ライセンスタブで確認できます。購入した期間ベースのライセンスが正しく使用され、ライセンス不足を示すアラートが表示されていないことを確認します。

FMCスマートライセンスの登録解除

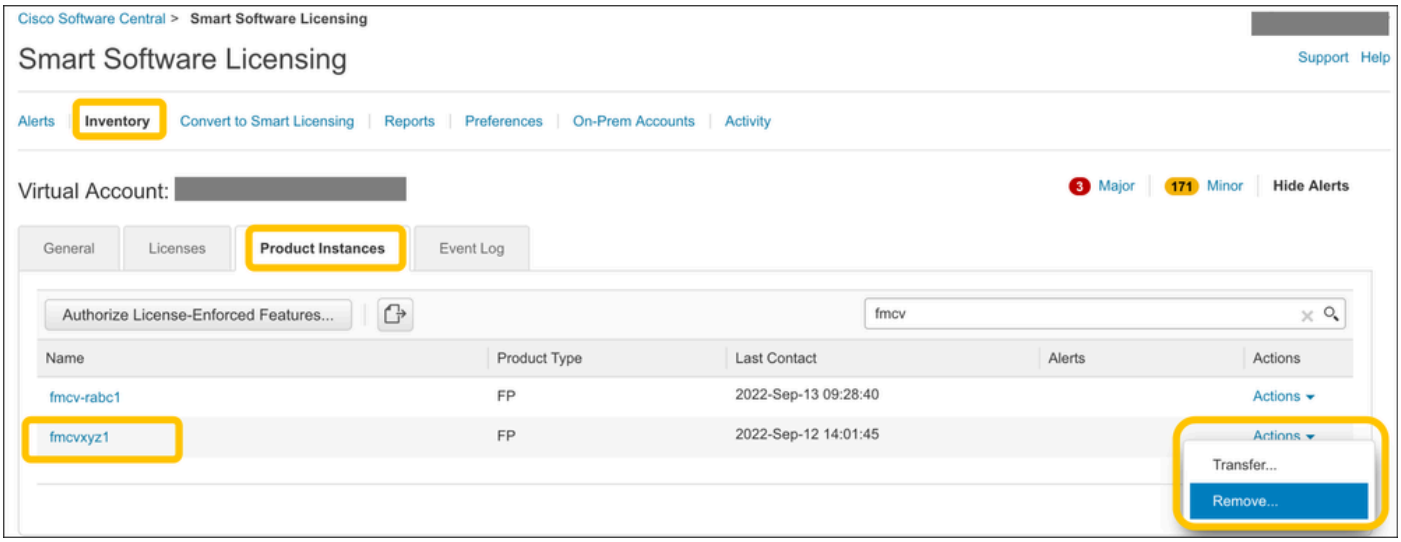
Cisco SSMからのFMCの登録解除

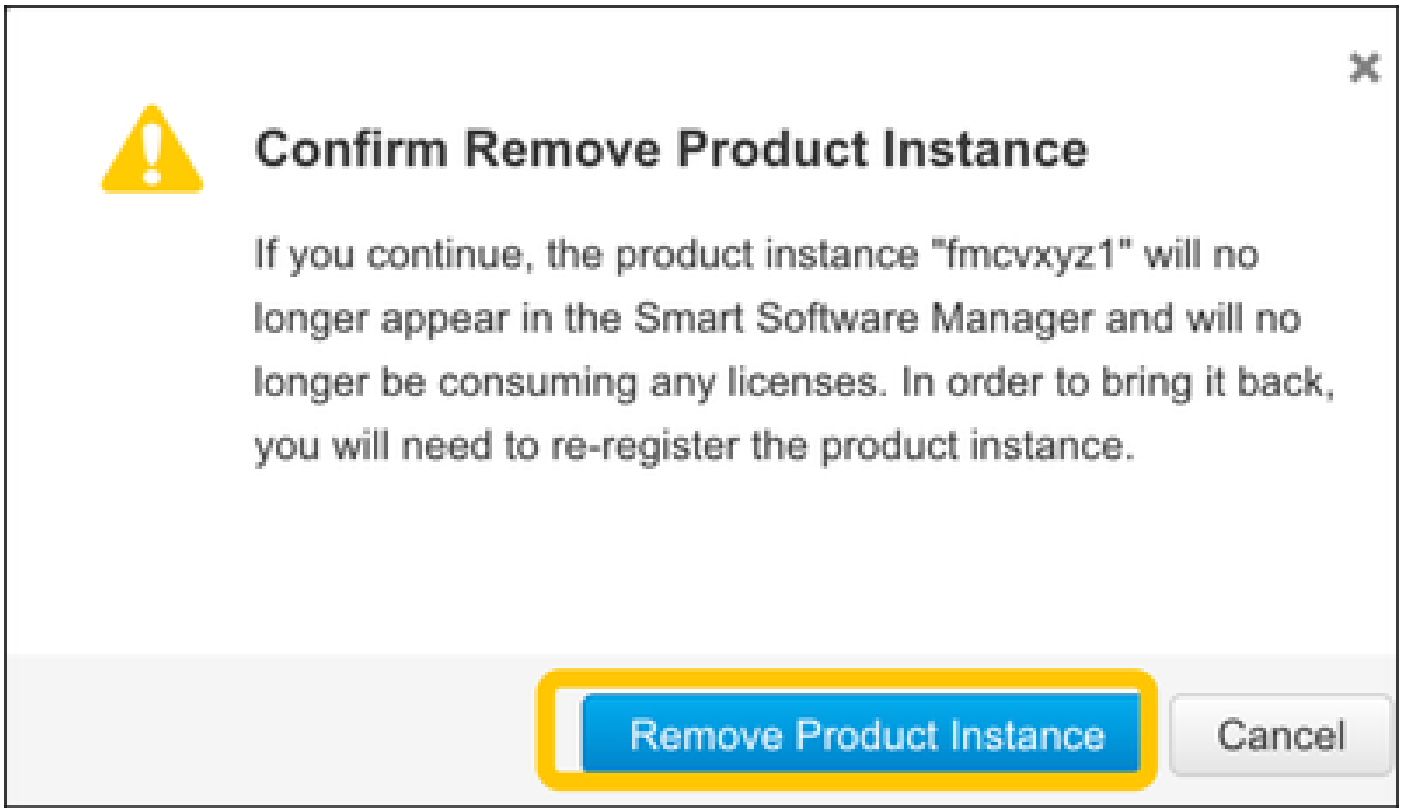
何らかの理由でライセンスをリリースするか、別のトークンを使用するには、次の図に示すように、System > Licenses > Smart Licensesの順に移動し、登録解除ボタンを選択します。



SSM側からの登録の削除

Smart Software Manager(Cisco Smart Software Manager)にアクセスし、Inventory > Product Instancesで、対象のFMCのRemoveを選択します。次に、Remove Product Instanceを選択してFMCを削除し、次の図に示すように割り当てられたライセンスを解放します。





RMA

FMCが返された場合は、「FMCスマートライセンスの登録解除> SSM側からの登録の削除」のセクションの手順を使用してCisco Smart Software Manager(CSSM)からFMCを登録解除してから、「FMCスマートライセンスの登録」のセクションの手順を使用してFMCをCSSMに再登録します。

トラブルシュート

時刻同期の検証

FMC CLI（SSHなど）にアクセスし、時刻が正しく、信頼できるNTPサーバと同期されていることを確認します。証明書はスマートライセンス認証に使用されるため、FMCに正しい時刻情報が設定されていることが重要です。

<#root>

```
admin@FMC:~$

date
Thu

 Jun 14 09:18:47 UTC 2020
admin@FMC:~$
admin@FMC:~$

ntpq -pn
```

```
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*10.0.0.2        171.68.xx.xx     2 u  387 1024  377    0.977    0.469   0.916
 127.127.1.1     .SFCL.          13 l    -   64    0    0.000    0.000   0.000
```

FMCのUIで、System > Configuration > Time Synchronizationの順に選択して、NTPサーバの値を確認します。

名前解決を有効にして、tools.cisco.comへの到達可能性を確認します(FMC 7.3以降ではsmartreceiver.cisco.com)。

FMCがFQDNを解決でき、tools.cisco.com(smartreceiver.cisco.comからFMC 7.3以降、Cisco Bug ID CSCwj95397に準拠)に到達できることを確認します。

<#root>

>

expert
admin@FMC2000-2:~$

sudo su

```
Password:
root@FMC2000-2:/Volume/home/admin# ping tools.cisco.com
PING tools.cisco.com (173.37.145.8) 56(84) bytes of data.
64 bytes from tools2.cisco.com (173.37.145.8): icmp_req=1 ttl=237 time=163 ms
64 bytes from tools2.cisco.com (173.37.145.8): icmp_req=2 ttl=237 time=163 ms
```

FMCのUIで、System > Configuration > Management Interfacesの順に選択し、管理IPとDNSサーバのIPを確認します。

FMCからtools.cisco.com(FMC 7.3+からのsmartreceiver.cisco.com)へのHTTPS(TCP 443)アクセスを確認します。

TelnetまたはcurlコマンドをFMCにtools.cisco.com(FMC 7.3以降ではsmartreceiver.cisco.com)へのHTTPSアクセスがあることを確認します。TCP 443通信が切断されている場合は、ファイアウォールによってブロックされていないこと、およびパスにSSL復号化デバイスがないことを確認します。

<#root>

root@FMC2000-2:/Volume/home/admin#

telnet tools.cisco.com 443

```
Trying 72.163.4.38...
```

Connected to tools.cisco.com.

```
Escape character is '^]'.
```

```
^CConnection closed by foreign host.
```

<--- Press Ctrl+C

カールテスト：

<#root>

```
root@FMC2000-2:/Volume/home/admin#
```

curl -vvk https://tools.cisco.com

```
*
```

Trying 72.163.4.38...

```
* TCP_NODELAY set
```

*** Connected to tools.cisco.com (72.163.4.38) port 443 (#0)**

```
* ALPN, offering http/1.1
* Cipher selection: ALL:!EXPORT:!EXPORT40:!EXPORT56:!aNULL:!LOW:!RC4:@STRENGTH
* successfully set certificate verify locations:
*   CAfile: /etc/ssl/certs/ca-certificates.crt
  CApath: none
* TLSv1.2 (OUT), TLS header, Certificate Status (22):
* TLSv1.2 (OUT), TLS handshake, Client hello (1):
* TLSv1.2 (IN), TLS handshake, Server hello (2):
* TLSv1.2 (IN), TLS handshake, Certificate (11):
* TLSv1.2 (IN), TLS handshake, Server finished (14):
* TLSv1.2 (OUT), TLS handshake, Client key exchange (16):
* TLSv1.2 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.2 (OUT), TLS handshake, Finished (20):
* TLSv1.2 (IN), TLS change cipher, Change cipher spec (1):
* TLSv1.2 (IN), TLS handshake, Finished (20):
* SSL connection using TLSv1.2 / AES128-GCM-SHA256
* ALPN, server accepted to use http/1.1
* Server certificate:
*  subject: C=US; ST=CA; L=San Jose; O=Cisco Systems, Inc.; CN=tools.cisco.com
*  start date: Sep 17 04:00:58 2018 GMT
*  expire date: Sep 17 04:10:00 2020 GMT
*  issuer: C=US; O=HydrantID (Avalanche Cloud Corporation); CN=HydrantID SSL ICA G2
*  SSL certificate verify ok.
> GET / HTTP/1.1
> Host: tools.cisco.com
> User-Agent: curl/7.62.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Wed, 17 Jun 2020 10:28:31 GMT
< Last-Modified: Thu, 20 Dec 2012 23:46:09 GMT
< ETag: "39b01e46-151-4d15155dd459d"
< Accept-Ranges: bytes
< Content-Length: 337
< Access-Control-Allow-Credentials: true
< Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
< Access-Control-Allow-Headers: Content-type, fromPartyID, inputFormat, outputFormat, Authorization, Co
< Content-Type: text/html
< Set-Cookie: CP_GUTC=10.163.4.54.1592389711389899; path=/; expires=Mon, 16-Jun-25 10:28:31 GMT; domain=
< Set-Cookie: CP_GUTC=10.163.44.92.1592389711391532; path=/; expires=Mon, 16-Jun-25 10:28:31 GMT; domai
```

```
< Cache-Control: max-age=0
< Expires: Wed, 17 Jun 2020 10:28:31 GMT
<
<html>
<head>
<script language="JavaScript">

var input = document.URL.indexOf('intellishield');
if(input != -1) {
 window.location="https://intellishield.cisco.com/security/alertmanager/";
}
else {
 window.location="http://www.cisco.com";
};

</script>
</head>

<body>
<a href="http://www.cisco.com">www.cisco.com</a>
</body>
</html>
* Connection #0 to host tools.cisco.com left intact
root@FMC2000-2:/Volume/home/admin#
```

DNSの検証

tools.cisco.com(FMC 7.3以降のsmartreceiver.cisco.com)への解決が正常に完了したことを確認します。

<#root>

```
root@FMC2000-2:/Volume/home/admin#

nslookup tools.cisco.com

Server:         192.0.2.100
Address:        192.0.2.100#53

Non-authoritative answer:

Name:   tools.cisco.com
Address: 72.163.4.38
```

プロキシの検証

apProxyを使用する場合は、FMCとプロキシサーバ側の両方の値を確認します。FMCで、FMCが正しいプロキシサーバのIPとポートを使用しているかどうかを確認します。

<#root>

```
root@FMC2000-2:/Volume/home/admin#

cat /etc/sf/smart_callhome.conf
```

```
KEEP_SYNC_ACTIVE:1
PROXY_DST_URL:https://tools.cisco.com/its/service/oddce/services/DDCEService

PROXY_SRV:192.0.xx.xx

PROXY_PORT:80
```

FMCのUIでプロキシ値を確認するには、System > Configuration > Management Interfacesの順に選択します。

FMC側の値が正しい場合は、プロキシサーバ側の値を確認します(たとえば、プロキシサーバがFMCからのアクセスとtools.cisco.comへのアクセスを許可している場合)。さらに、プロキシを介したトラフィックと証明書交換を許可します。FMCはスマートライセンスの登録に証明書を使用)。

期限切れのトークンID

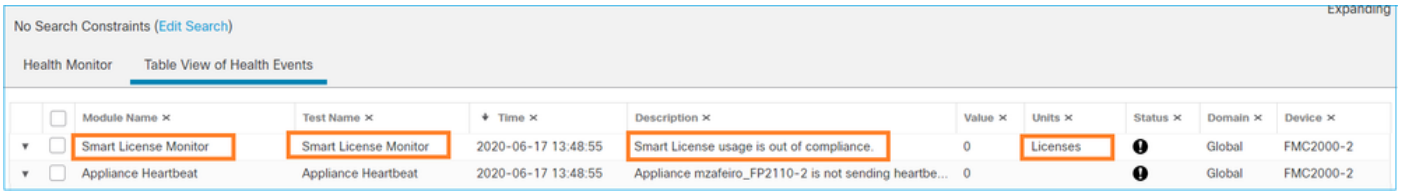
発行されたトークンIDが期限切れでないことを確認します。有効期限が切れている場合は、Smart Software Manager管理者に新しいトークンを発行し、新しいトークンIDでスマートライセンスを再登録するように依頼します。

FMCゲートウェイの変更

リレープロキシやSSL復号化デバイスの影響により、スマートライセンス認証を正しく実行できない場合があります。可能であれば、FMCインターネットアクセスのルートを変更してこれらのデバイスを回避し、スマートライセンスの登録を再試行します。

FMCのヘルスイベントのチェック

FMCで、System > Health > Eventsの順に移動し、Smart License Monitorモジュールのステータスにエラーがないかを確認します。たとえば、証明書の期限切れが原因で接続が失敗すると、次の図に示すように、id certificated expiredなどのエラーが生成されます。



SSM側のイベントログの確認

FMCがCSSMに接続できる場合は、Inventory > Event Logで接続のイベントログを確認します。CSSMにそのようなイベントログまたはエラーログがあるかどうかを確認します。FMCサイトの値/動作に問題がなく、CSSM側にイベントログがない場合は、FMCとCSSM間のルートに問題がある可能性があります。

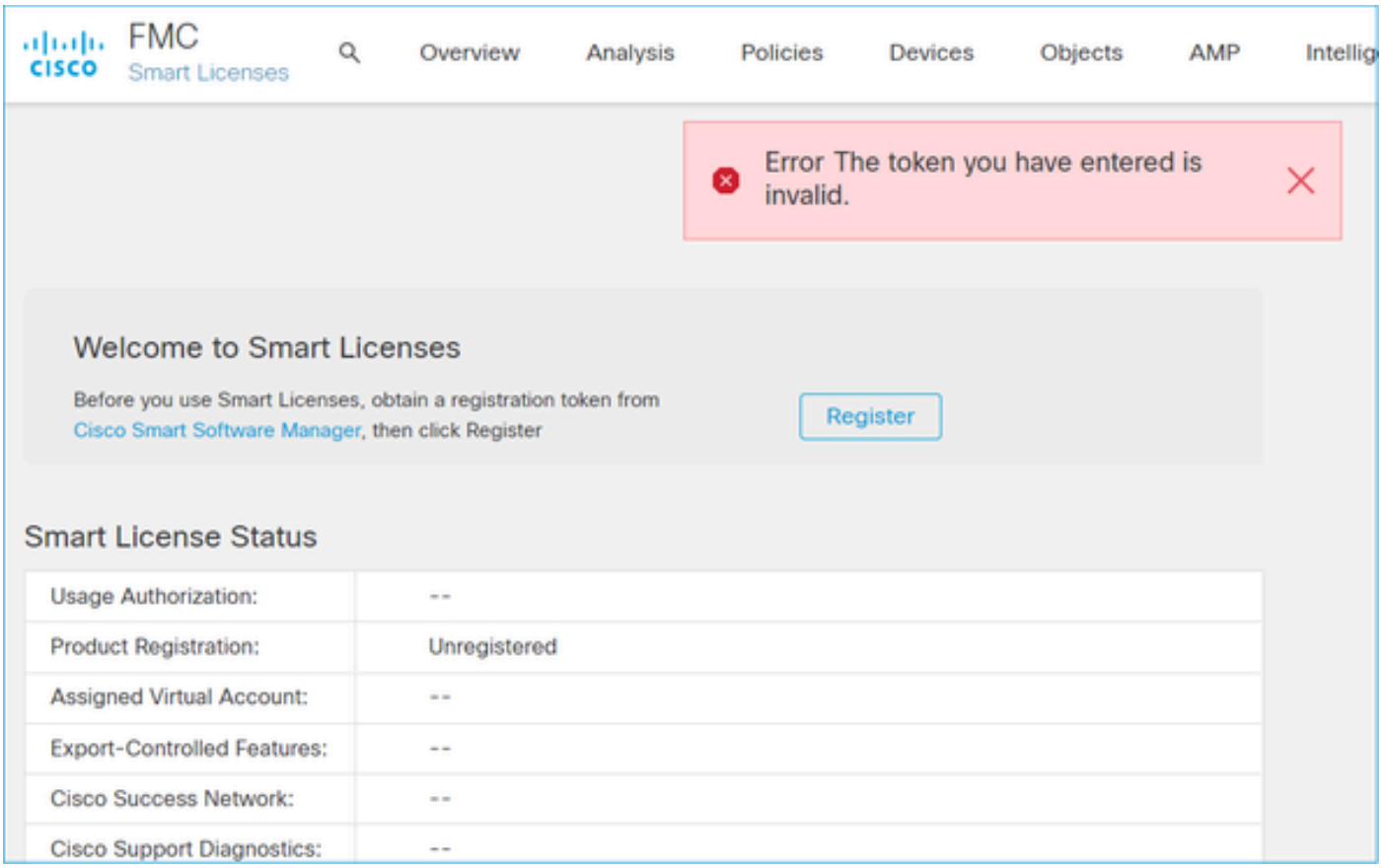
一般的な問題

登録および承認の状態の概要：

製品登録状態	使用許可状態	注釈
未登録	—	FMCが登録モードでも評価モードでもない。これは、FMCのインストール後、または評価ライセンスの有効期限が90日後の初期状態です。
登録済み	承認済み	FMCはCisco Smart Software Manager(CSSM)に登録されており、有効なサブスクリプションで登録されているFTDデバイスがあります。
登録済み	認証が期限切れ	FMCは90日以上シスコライセンスバックエンドとの通信に失敗しました。
登録済み	未登録	FMCはCisco Smart Software Manager(CSSM)に登録されていますが、FMCにはFTDデバイスが登録されていません。
登録済み	コンプライアンス違反	FMCはCisco Smart Software Manager(CSSM)に登録されていますが、無効なサブスクリプションに登録されているFTDデバイスがあります。 たとえば、FTD(FP4112)デバイスはTHREATサブスクリプションを使用しますが、Cisco Smart Software Manager(CSSM)を使用する場合、FP4112で使用できるTHREATサブスクリプションはありません。
評価（90日）	N/A	評価期間は使用中ですが、FMCに登録されているFTDデバイスはありません。

ケース スタディ 1無効トークン

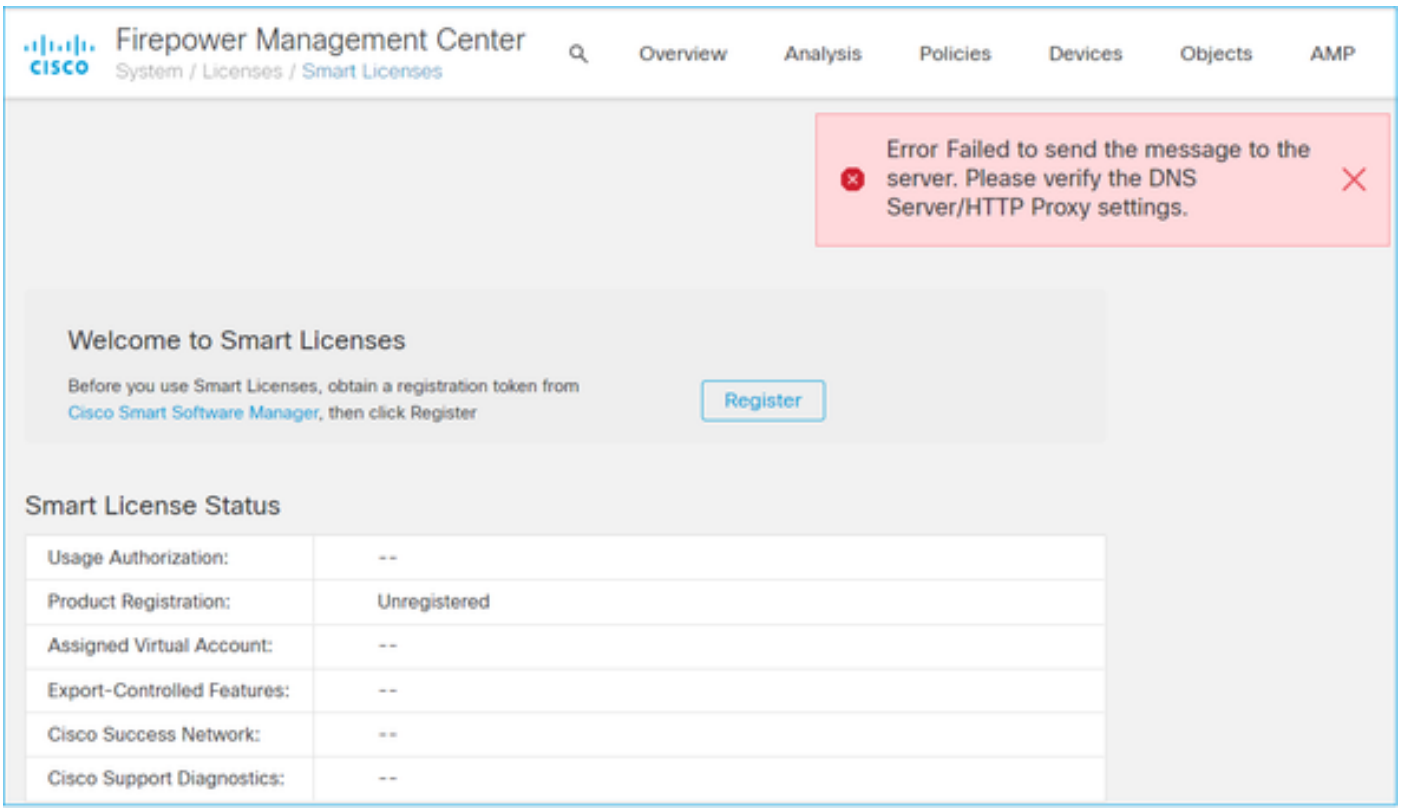
症状：次の図に示すように、無効なトークンが原因でCSSMへの登録がすばやく失敗します（10秒以内）。



解決策：有効なトークンを使用します。

ケース スタディ 2無効なDNS

症状：次の図に示すように、しばらく（25秒以内）後にCSSMへの登録が失敗しました。



/var/log/process_stdout.logファイルをチェックします。DNSの問題が見られます。

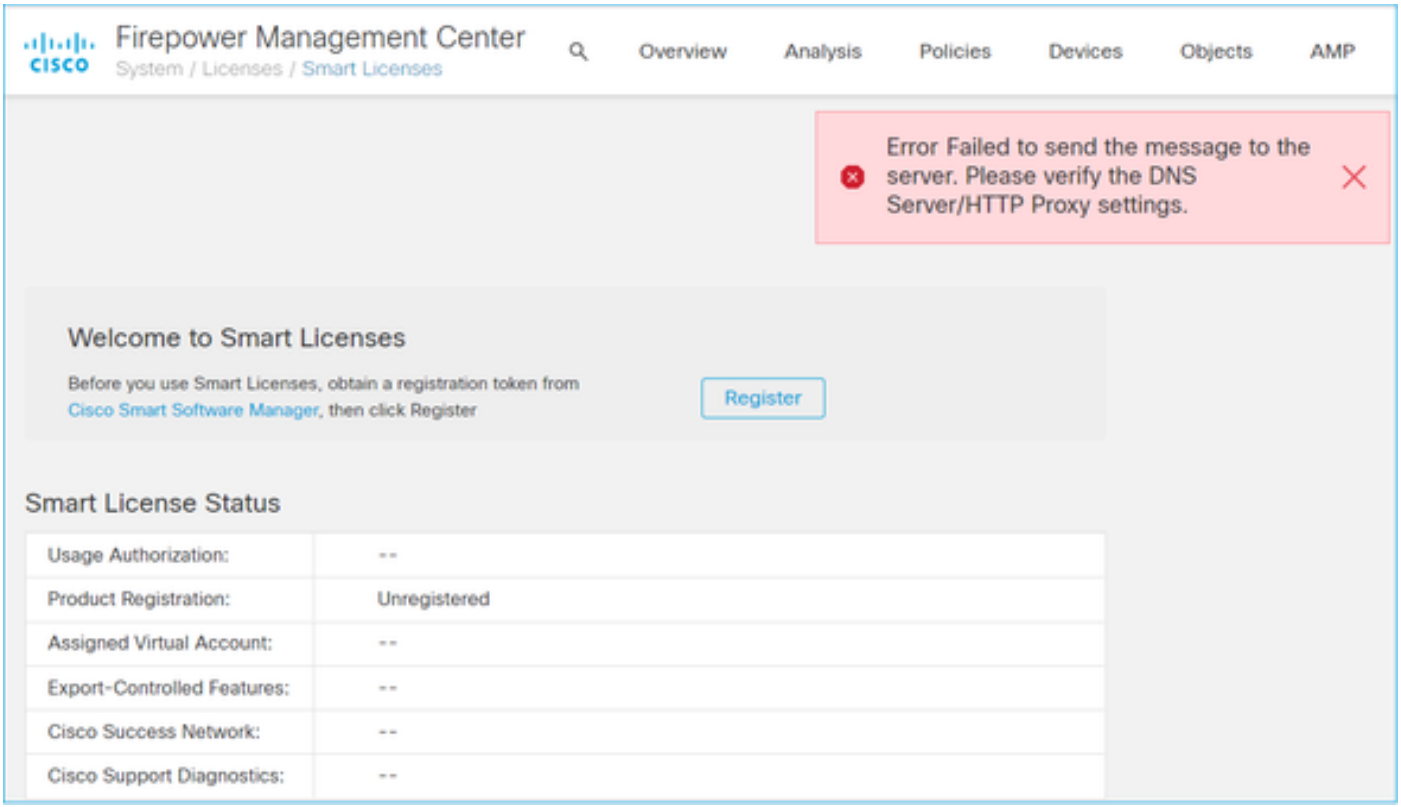
<#root>

```
root@FMC2000-2:/Volume/home/admin#

cat /var/log/process_stdout.log

2020-06-25 09:05:21 sla[24043]: *Thu Jun 25 09:05:10.989 UTC: CH-LIB-ERROR: ch_pf_curl_send_msg[494],
failed to perform, err code 6, err string

"Couldn't resolve host name"
```

解決策：CSSMホスト名の解決に失敗しました。解決策は、DNSが設定されていない場合はDNSを設定し、DNSの問題を修正することです。

ケース スタディ 3無効な時間値

症状：次の図に示すように、しばらく（25秒以内）後にCSSMへの登録が失敗しました。



/var/log/process_stdout.logファイルをチェックします。証明書の問題が発生します。

<#root>

```
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:39.716 UTC: CH-LIB-TRACE: ch_pf_curl_request_init[59]
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:39.716 UTC: CH-LIB-TRACE: ch_pf_curl_post_prepare[299
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:39.716 UTC: CH-LIB-TRACE: ch_pf_curl_post_prepare[302
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:39.716 UTC: CH-LIB-TRACE: ch_pf_curl_head_init[110],
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:40.205 UTC: CH-LIB-ERROR: ch_pf_curl_send_msg[494],
```

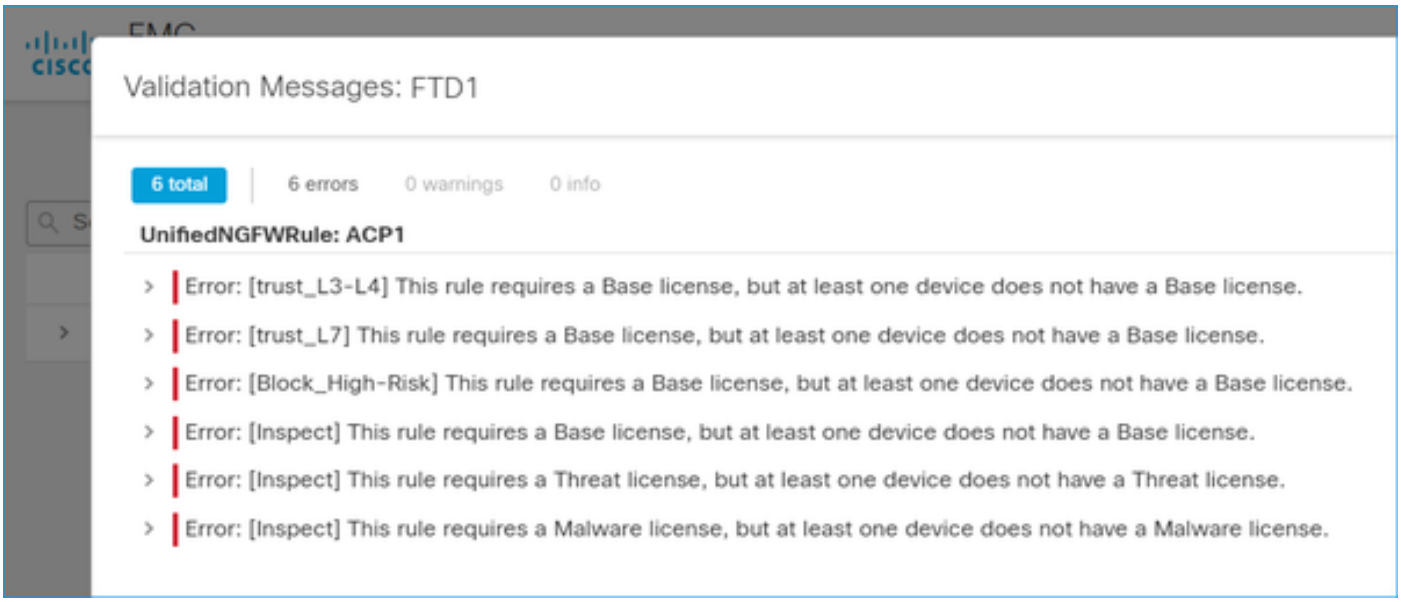
```
failed to perform, err code 60, err string "SSL peer certificate or SSH remote key was not OK"

2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:40.205 UTC: CH-LIB-TRACE: ch_pf_http_unlock[330], unl
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:40.205 UTC: CH-LIB-TRACE: ch_pf_send_http[365], send
2021-06-25 09:22:51 sla[24043]: *Fri Jun 25 09:22:40.205 UTC: CH-LIB-TRACE: ch_pf_curl_is_cert_issue[51

cert issue checking, ret 60, url https://tools.cisco.com/its/service/oddce/services/DDCEService
```

FMC時間の値をチェックします。

```
<#root>

root@FMC2000-2:/Volume/home/admin#

date

Fri Jun 25 09:27:22 UTC 2021
```

ケース スタディ 4サブスクリプションなし

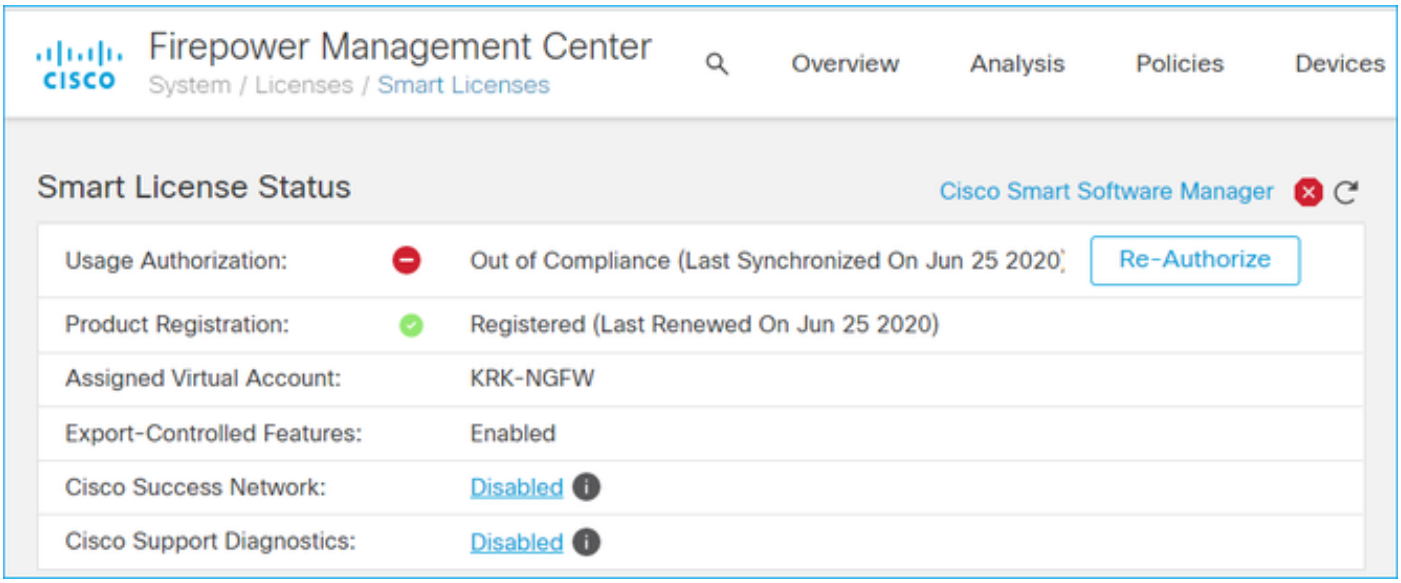
特定の機能のライセンスサブスクリプションがない場合、FMCの導入は不可能です。



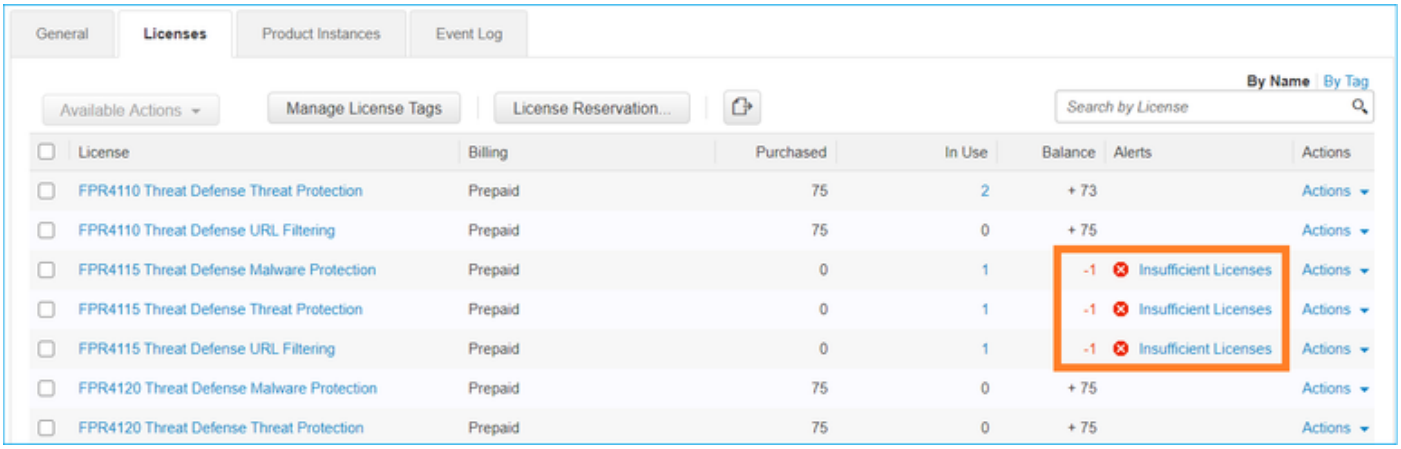
解決策：必要なサブスクリプションを購入してデバイスに適用する必要があります。

ケース スタディ 5コンプライアンス違反(OOC)

FTDサブスクリプションの権限がない場合、FMCスマートライセンスはコンプライアンス違反(OOC)状態になります。

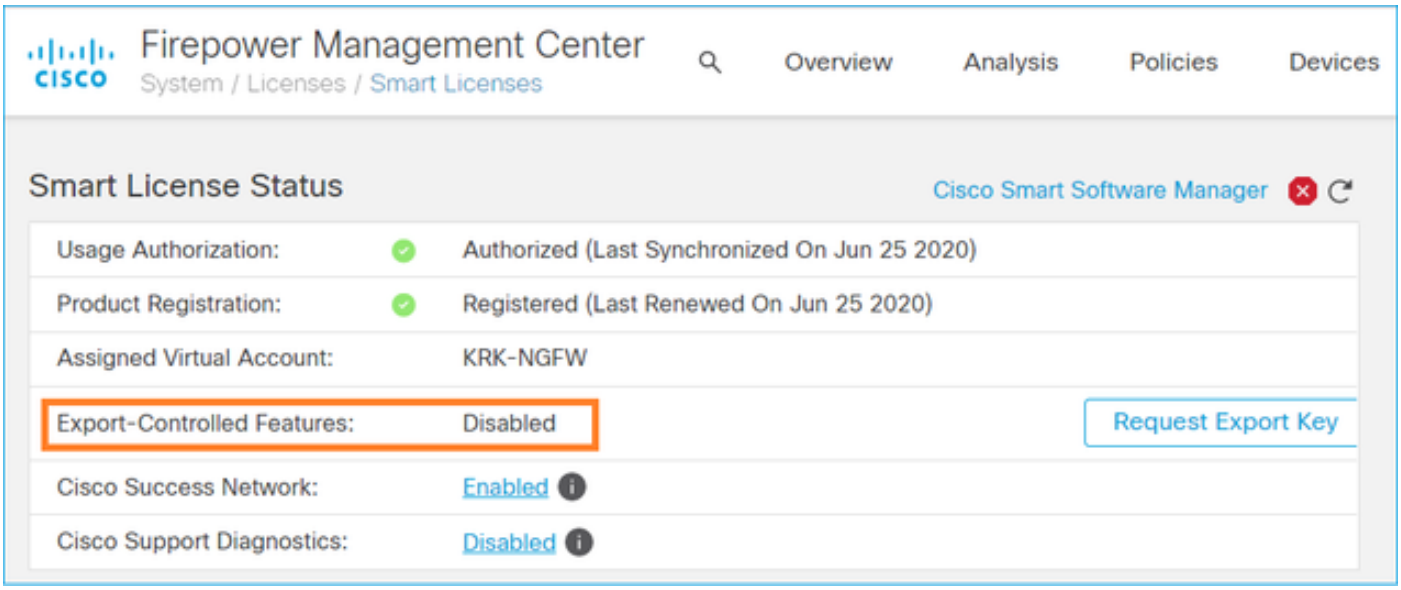


CSSMで、エラーのアラートを確認します。



ケース スタディ 6強力な暗号化なし

Baseライセンスのみを使用する場合、FTD LINAエンジンでData Encryption Standard(DES)暗号化が有効になります。この場合、より強力なアルゴリズムを使用したL2Lバーチャルプライベートネットワーク(VPN)のような展開は失敗します。



解決策：CSSMにFMCを登録し、強力な暗号化属性を有効にします。

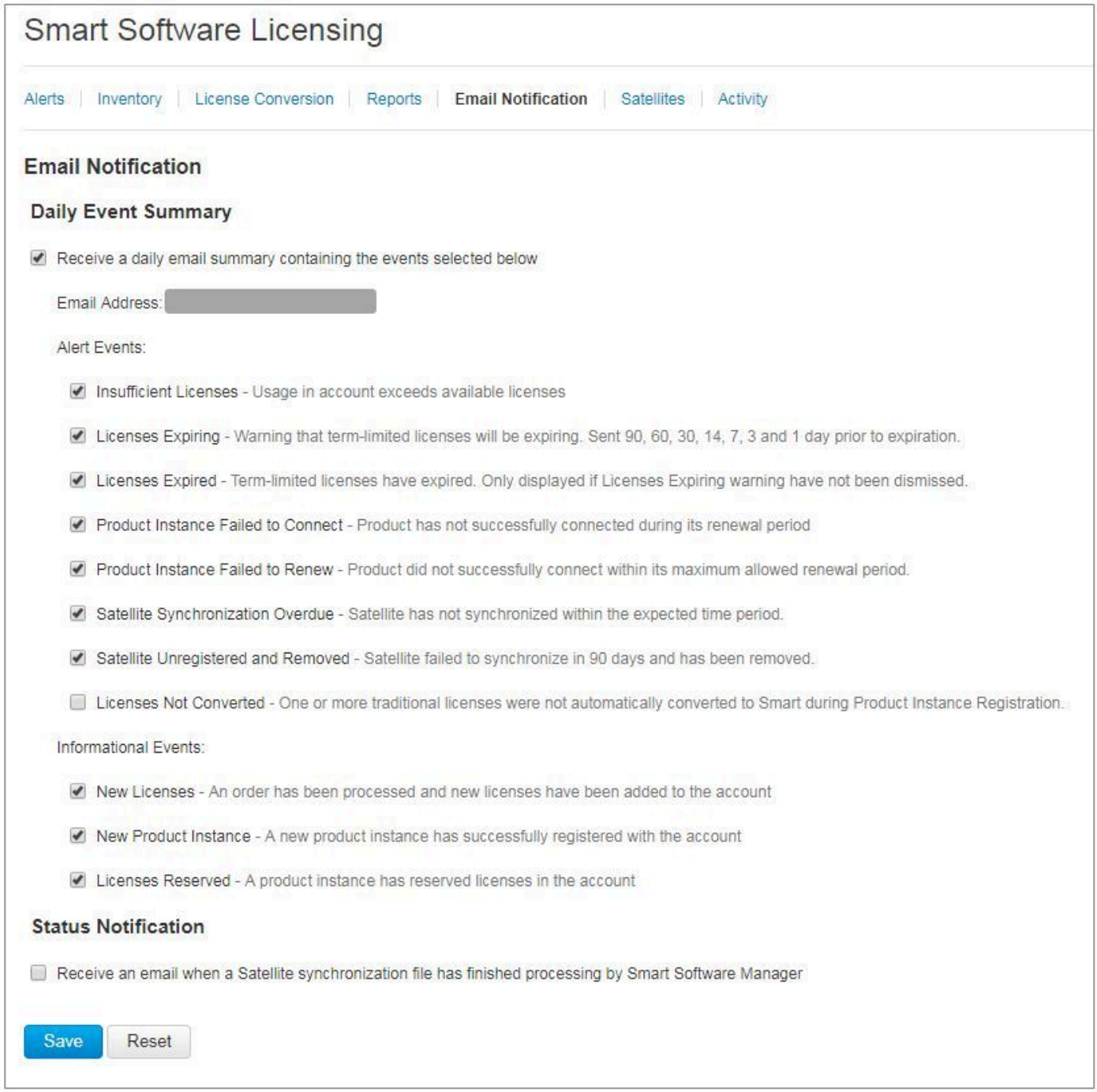
追加情報

スマートライセンスの状態の通知の設定

SSMによる電子メール通知

SSM側では、SSM Eメール通知により、さまざまなイベントの要約Eメールを受信できます。たとえば、ライセンスの不足やライセンスの有効期限が近づいていることについての通知です。製品インスタンスの接続または更新の失敗の通知を受け取ることができます。

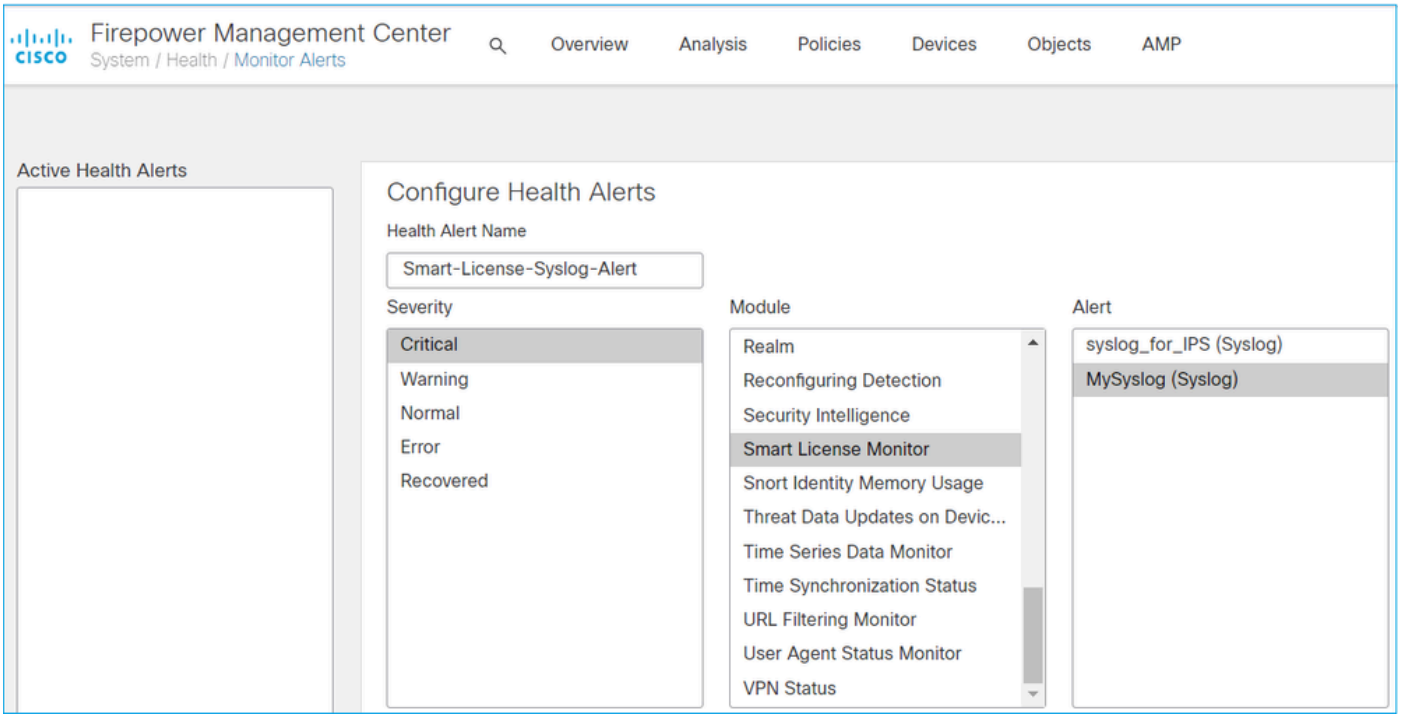
この機能は、ライセンスの期限切れによる機能制限の発生を通知および防止するのに非常に便利です。



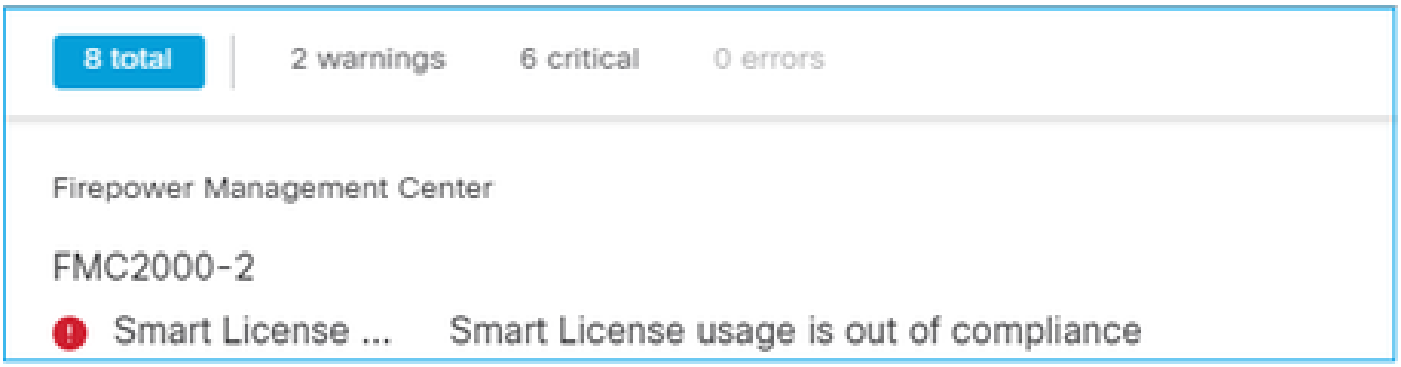
FMCからのヘルスアラート通知の取得

FMC側では、ヘルスモニタアラートを設定し、ヘルスイベントのアラート通知を受信することができます。モジュールスマートライセンスモニタを使用して、スマートライセンスのステータスを確認できます。モニタアラートは、Syslog、電子メール、およびSNMPトラップをサポートします。

スマートライセンスモニタイベントが発生したときにSyslogメッセージを取得する設定例を次に示します。



ヘルスアラートの例を次に示します。



FMCによって生成されるSyslogメッセージは次のとおりです。

<#root>

```
Mar 13 18:47:10 xx.xx.xx.xx Mar 13 09:47:10 FMC :
```

HMNOTIFY: Smart License Monitor (Sensor FMC)

```
: Severity: critical: Smart License usage is out of compliance
```

ヘルスモニタアラートの詳細については、『ヘルスモニタリング』を参照してください。

同じスマートアカウントの複数のFMC

同じスマートアカウントで複数のFMCを使用する場合、各FMCホスト名は一意である必要があります。CSSMで複数のFMCが管理されている場合、各FMCを区別するために、各FMCのホスト名

は一意である必要があります。これは、動作中のFMCスマートライセンスメンテナンスに役立ちます。

FMCがインターネット接続を維持する必要がある

登録後、FMCはスマートライセンスクラウドとライセンスのステータスを30日ごとに確認します。FMCが90日間通信できない場合、ライセンスされた機能は維持されますが、Authorization Expiredステータスのままになります。この状態でも、FMCは継続してスマートライセンスクラウドへの接続を試みます。

複数のFMCvの導入

Firepowerシステムを仮想環境で使用する場合、クローン（ホットまたはコールド）は正式にはサポートされません。各Firepower Management Center(FMC)仮想(FMCv)は、内部に認証情報を持つため、一意です。複数のFMCvを導入するには、Open Virtualization Format(OVF)ファイルからFMCvを1つずつ作成する必要があります。この制限の詳細については、『Cisco Firepower Management Center Virtual for VMware導入クイックスタートガイド』を参照してください。

FAQ

FTD HAでは、必要なデバイスライセンスはいくつですか。

ハイアベイラビリティで2つのFTDを使用する場合は、デバイスごとにライセンスが必要です。たとえば、侵入防御システム(IPS)と高度なマルウェア防御(AMP)機能をFTD HAペアで使用する場合は、2つの脅威およびマルウェアライセンスが必要です。

AnyConnectライセンスがFTDで使用されないのはなぜですか。

FMCをスマートアカウントに登録した後、AnyConnectライセンスが有効になっていることを確認します。 ライセンスを有効にするには、FMC > Devicesの順に選択し、使用しているデバイスを選択してLicenseを選択します。鉛筆アイコンを選択しますで、スマートアカウントに保存されているライセンスを選択し、Saveを選択します。

100人のユーザが接続しているときに、スマートアカウントで1つのAnyConnectライセンスだけが「使用中」になるのはなぜですか。

スマートアカウントでは、このライセンスが有効で、アクティブユーザが接続していないデバイスの数が追跡されるため、これは正常な動作です。

FMCによるリモートアクセスVPNの設定と展開の後にDevice does not have the AnyConnect Licenseエラーが発生するのはなぜですか。

FMCがスマートライセンスクラウドに登録されていることを確認します。想定される動作は、FMCが未登録または評価モードの場合に、リモートアクセス設定を導入できないことです。FMCが登録されている場合は、AnyConnectライセンスがスマートアカウントに存在し、デバイスに割り当てられていることを確認します。

ライセンスを割り当てるには ナビゲート からFMCデバイス、デバイスを選択、ライセンス（鉛

筆アイコン）.スマートアカウントでライセンスを選択し、 保存します。.

リモートアクセスVPN設定の展開があるときに「Remote Access VPN with SSL cannot be deployed when Export-Controlled Features (Strong-crypto) are disabled」エラーが表示されるのはなぜですか。

FTDに導入されたリモートアクセスVPNでは、強力な暗号化ライセンスを有効にする必要があります。ENfmcで強力な暗号化ライセンスが有効になっていることを確認します。 強力な暗号化ライセンスのステータスを確認するには、 ナビゲート 「 FMCシステム>ライセンス>スマートライセンスエクスポート制御機能が有効になっていることを確認します。

Export-Controlled Featuresが無効の場合に強力な暗号化ライセンスを有効にする方法

この機能は、スマートアカウントクラウドへのFMCの登録時に使用されたトークンで、Allow export-controlled functionality on the products registered with this tokenオプションが有効になっている場合に、自動的に有効になります。 トークンでこのオプションが有効になっていない場合は、FMCの登録を解除し、このオプションを有効にして再登録します。

トークンの生成時に、[このトークンに登録されている製品で工クスポート制御機能を許可する]オプションを使用できない場合は、どうすればよいですか。

シスコアカウントチームにお問い合わせください。

「Strong crypto（ つまり、DESよりも大きい暗号化アルゴリズム） for VPN topology s2s is not supported」という工ラーが表示されるのはなぜですか。

このエラーは、FMCが評価モードを使用している場合、またはスマートライセンスアカウントが強力な暗号化ライセンスを持っていない場合に表示されます。VFMCがライセンス認証局(RA)に登録されていることを確認し、このトークンに登録されている製品で工クスポート制御機能を許可するが有効になっていることを確認します。 スマートアカウントに強力な暗号化ライセンスの使用が許可されていない場合、DESよりも強力な暗号を使用したVPNサイト間設定の展開は許可されません。

FMCの「Out of Compliance」ステータスが受信されるのはなぜですか。

管理対象デバイスの1つが使用不可能なライセンスを使用すると、デバイスがコンプライアンス違反になる可能性があります。

「Out of Compliance」ステータスを修正するにはどうすればよいですか。

『Firepowerコンフィギュレーションガイド』で説明されている手順に従ってください。

1. ページ下部の「スマートライセンス」セクションで、必要なライセンスを確認します。

2. 通常のチャネルで必要なライセンスを購入します。

3. Cisco Smart Software Manager(https://software.cisco.com/#SmartLicensing-Inventory)を選択し、仮想アカウントにライセンスが表示されることを確認します。

4. FMCで、System > Licenses > Smart Licensesの順に選択します。

5. Re-Authorizeを選択します。

手順の詳細については、「Firepowerシステムのライセンス取得」を参照してください。

Firepower Threat Defense Baseの機能とは何ですか。

Baseライセンスでは次のことが可能です。

- スイッチおよびルーティングするFTDデバイスの設定（DHCPリレーおよびNATを含む）。
- ハイアベイラビリティ(HA)モードでのFTDデバイスの設定。
- Firepower 9300シャーシ内のクラスタとしてのセキュリティモジュールの設定（シャーシ内クラスタ）。
- Firepower 9300またはFirepower 4100シリーズデバイス(FTD)をクラスタ（シャーシ間クラスタ）として設定します。
- ユーザおよびアプリケーション制御の設定、およびアクセス制御規則へのユーザおよびアプリケーションの条件の追加。

Firepower Threat Defense Base機能ライセンスの取得方法を教えてください。

基本ライセンスは、Firepower Threat DefenseまたはFirepower Threat Defense仮想デバイスを購入するたびに自動的に含まれます。FTDがFMCに登録されると、スマートアカウントに自動的に追加されます。

FMCとスマートライセンスクラウド間のパスで許可する必要があるIPアドレスはどれか？

FMCはIPアドレス スマートライセンスクラウドと通信するためにポート443で設定します。

そのIPアドレス(https://tools.cisco.com)次のIPアドレスに解決されます。

- 72.163.4.38
- 173.37.145.8

バージョン7.3以降のFMCでは、https://smartreceiver.cisco.comに接続し、次のIPアドレスに解決されます。

- 146 .112. 59. 81

関連情報

- Firepower Management Center(FMC)設定ガイド
- Cisco Liveスマートライセンスの概要：BRKARC-2034

- Cisco Secure Firewall Management Centerフィーチャライセンス
- Cisco Smart Software Licensingに関してよく寄せられる質問(FAQ)

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。