改訂：2025 年 12 月 15 日

SLP のトラブルシューティング、システム メッセージ、および FAQ

概要

この記事では、 Nexus スイッチのポリシーを使用したスマート ライセンシング（SLP）に関連するシステム メッセージとトラブルシューティングに関する情報と、よく寄せられる質問（FAQ）について説明します。

ポリシーを使用したスマート ライセンシングのトラブルシューティング

トラブルシューティングのセクションは、 Nexusスイッチの SLP の問題を解決するための段階的な手順を提供する 2 つのセクションに分かれています。

- Nexus スイッチでの SLP 問題の解決 ：このセクションでは、CSSM へのスイッチの接続に関連する一般的な問題と解決策について説明します。
- このセクションでは、発生する可能性のある SLP に関連するシステムメッセージ、考えられる失敗の理由、および推奨するアクションを示します。システム メッセージの概要 （10 ページ）

Nexus スイッチ上の SLP 問題の解決

このセクションでは、CSSM へのスイッチの接続とその解決策に関連する一般的な問題について説明します。

このセクションでは、次の問題について説明します：

- 信頼コードのインストールに失敗しました。
- CSSM、CSLU、または SSM オンプレミスのいずれかとのスマートライセンシング通信が失敗しました。
- 使用レポートの送信に失敗しました（Failed to send Crash Report）
- レポートの確認応答を取得できませんでした

問題：信頼コードのインストールに失敗しました。

失敗の理由として次が考えられます。

- 信頼コードがすでにインストールされています：信頼コードは製品インスタンスの**固有のデバイス ID**（UDI）にリンク済みです。UDI がすでに登録されている場合に別の UDI をインストールしようとすると、インストールは失敗します。
- タイムスタンプの不一致：製品インスタンスの時刻が**Cisco Smart Software Manager**（CSSM）と同期していないため、インストールが失敗する可能性があります。

推奨するアクション：

- 信頼コードはすでにインストールされています：製品インスタンスに信頼コードがすでに存在する状況で信頼コードをインストールする場合は、特権 EXEC モードで **license smart trust idtoken** *id_token_value* [**force**] コマンドを再構成し、**force** キーワードを必ず含めてください。 **force** キーワードを入力すると、すでに存在する場合でも新しい信頼コードを作成するよう CSSM に要求されます。
- タイムスタンプの不一致：グローバル コンフィギュレーション モードで **ntp server** コマンドを設定します。次に例を示します。

  switch (config)# **ntp server 10.28.13.90 prefer**

  （注）

  デバイスと CSSM の間に時間差がある場合は、1 時間未満にする必要があります。

問題：CSSM、CSLU、または SSM オンプレミスのいずれかとのスマートライセンシング通信が失敗しました。

失敗の理由として次が考えられます。

- DNS 構成が見つかりません。
- CSSM、CSLU、または SSM オンプレミスに到達できない：これは、ネットワークに問題がある可能性があることを意味します。

DNS の推奨処置：

CSSM/CSLU/ SSM オンプレミスに到達できない場合に、DNS 構成が不足している場合のトラブルシューティング手順を示します。

- SLP 用に構成された VRF で cisco.com に ping を実行すると、エラー **% Invalid host/interface <URL>** が発生します：

1. DNS を構成するには、グローバル構成モードで次のコマンドを実行します。

```
switch# config terminal
switch(config)# ip domain-lookup
switch(config)# ip domain-name cisco.com
switch(config)# ip name-server <dns-server-ip> use-vrf <vrf-name>
switch(config)# vrf context <vrf-name>
switch(config-vrf)# ip domain-name cisco.com
switch(config-vrf)# ip name-server <dns-server-ip>
```

2. **vrf** <*vrf-name*> を使用して、cisco.com への ping が機能しているかどうかを確認します。次の例は、DNS が動作しているシナリオを示しています。

```
switch(config)# ping cisco.com vrf <vrf-name>
PING cisco.com (<ip-address>): 56 data bytes
64 bytes from <ip-address>: icmp_seq=0 ttl=236 time=242.279 ms
64 bytes from <ip-address>: icmp_seq=1 ttl=236 time=242.108 ms
64 bytes from <ip-address>: icmp_seq=2 ttl=236 time=242.032 ms
64 bytes from <ip-address>: icmp_seq=3 ttl=236 time=242.278 ms
64 bytes from <ip-address>: icmp_seq=4 ttl=236 time=241.968 ms
--- cisco.com ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 241.968/242.133/242.279 ms
```

（注）

転送モード CSLU の場合は、**ip host cslu-local** <*cslu_address*> を構成または cslu-local は DNS サーバーの一部である必要があります。SSM オンプレミスの場合、スイッチに構成されたURL は、IP アドレスではなく、**完全修飾ドメイン名**（FQDN）である必要があります。

網の到達可能性に対する推奨アクション：

- 設定されている転送モードが **smart** transport の場合：

1. **show license status** コマンドの出力で、**Transport:** ヘッダーの下で次のことを確認します：
   1. **[タイプ（Type）]**：**スマート** および
   2. **URL**：は、https://smartreceiver.cisco.com/licservice/license である必要があります。次に例を示します。

      Transport：

      Type: Smart

      URL：https://smartreceiver.cisco.com/licservice/license

      プロキシ:

      未設定

      VRF：<*vrf-name*>

   そうでない場合は、グローバル構成モードで **license smart transport smart** および **license smart url smart** https://smartreceiver.cisco.com/licservice/license コマンドを使用して構成します。

2. DNS 解決を確認します。URL https://smartreceiver.cisco.com/licservice/license が ブラウザを介して到達可能であることを確認します。次の例は、スマートURLの到達可能性を示しています。

```
This is the Smart Receiver!

Environment Information:
  cisco.life = prod
  License Engine = https://swapi.cisco.com/software/csws/ssm/services
  License EngineSLE = https://swapi.cisco.com/software/csws/ssm/v2/services
  License Crypto Service = https://lcs.cisco.com/LCS
  Crypto Enabled = true
  Retry Enabled = true
  Retry Timeout = 55000
  Rate Limit Window Length = 3600
  Rate Limit Max Allowed in Window = 12
```

必要に応じて、スマートURL（https://smartreceiver.cisco.com/licservice/license）に ping を実行して確認することができます。

例：

```
bash-4.4$ ping smartreceiver.cisco.com
PING smartreceiver.cisco.com (<ip-address>) 56(84) bytes of data.
64 bytes from <ip-address> (<ip-address>): icmp_seq=1 ttl=53 time=2.57 ms
64 bytes from <ip-address> (<ip-address>): icmp_seq=2 ttl=53 time=2.79 ms
64 bytes from <ip-address> (<ip-address>): icmp _seq=3 ttl=53 time=2.54 ms
```

```
64 bytes from <ip-address> (<ip-address>): icmp_seq=4 ttl=53 time=2.43 ms
64 bytes from <ip-address> (<ip-address>): icmp_seq=5 ttl=53 time=3.23 ms
64 bytes from <ip-address> (<ip-address>): icmp_seq=6 ttl=53 time=2.100 ms
^C
--- smartreceiver.cisco.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5009ms
rtt min/avg/max/mdev = 2.429/2.757/3.231/0.289 ms
bash-4.4$
```

- 設定されている転送モードが **cslu**の場合：

1. **show license status** コマンドの出力で、**トランスポート**： ヘッダーの下で次のことを確認します：
   1. **[タイプ（Type）]**： は、CSLU である必要があり、
   2. **Cslu アドレス**：は、cslu-local である必要があります

   例

   転送：

   タイプ：CSLU

   Cslu アドレス：cslu-local

   VRF: <*vrf-name*>

   そうでない場合は、グローバル構成モードで**license smart transport cslu** および **license smart url cslu** <*cslu-local-url*> コマンドを使用します。
2. DNS 解決を確認します。設定された cslu-local-url が ブラウザから到達可能であることを確認します。

- 設定されている転送モードが callhome の場合：

1. **show license status** コマンドの出力で、 **Transport:** ヘッダーの下で次のことを確認します：
   - **タイプ**：Call Home である必要があります

   次に例を示します。

   転送：

   タイプ: Call Home

   そうでない場合は、グローバル構成モードで **license smart transport callhome** コマンドを使用して構成します。
2. callhome が正しく構成されているかどうかを確認してください。特権 EXEC モードで **show running-config callhome all** コマンドを活用、次のように callhome 構成を確認します。

```
switch(config)# show running-config callhome all
!Command: show running-config callhome all
!Running configuration last done at: Thu Aug  3 20:38:37 2023
!Time: Thu Aug  3 20:43:58 2023
version 10.3(1) Bios:version 05.45
callhome
  email-contact <email-address>
  destination-profile xml transport-method http
  destination-profile xml index 1 email-addr <email-address>
  destination-profile xml index 1 http https://tools.cisco.com/its/service/oddce/services/DDCEService
```

```
transport email smtp-server <ip-address> port <port-number>
transport email from <email-address>
transport email reply-to <email-address>
transport http use-vrf <vrf-name>
enable
periodic-inventory notification interval 1
```

3. DNS 解決を確認します。**ping tools.cisco.com vrf** <vrf-name> コマンドを使用して、構成された vrf を介して製品インスタンスが tools.cisco.com に ping を実行できることを確認します。

   例

```
switch(config) # ping tools.cisco.com vrf <vrf-name>
PING tools.cisco.com (<ip-address>): 56 data bytes
64 bytes from <ip-address>: icmp_seq=0 ttl=236 time=244.692 ms
64 bytes from <ip-address>: icmp_seq=1 ttl=236 time=244.532 ms
64 bytes from <ip-address>: icmp_seq=2 ttl=236 time=244.396 ms.
64 bytes from <ip-address>: icmp_seq=3 ttl=236 time=244.502 ms.
64 bytes from <ip-address>: icmp_seq=4 ttl=236 time=244.607 ms

-- tools.cisco.com ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 244.396/244.545/244.692 ms.
switch(config)#
```

   callhome URL tools.cisco.comに直接 ping を実行することもできます。

   例

```
bash-4.4$ ping tools.cisco.com
PING tools.cisco.com (<ip-address>) 56(84) bytes of data.
64 bytes from tools2.cisco.com (<ip-address>): icmp_seq=1 ttl=242 time=43.7 ms
64 bytes from tools2.cisco.com (<ip-address>): icmp_seq=2 ttl=242 time=43.7 ms
64 bytes from tools2.cisco.com (<ip-address>): icmp_seq=3 ttl=242 time=43.7 ms
64 bytes from tools2.cisco.com (<ip-address>): icmp_seq=4 ttl=242 time=43.8 ms
64 bytes from tools2.cisco.com (<ip-address>): icmp_seq=5 ttl=242 time=43.8 ms
64 bytes from tools2.cisco.com (<ip-address>): icmp_seq=6 ttl=242 time=43.7 ms
^C
--- tools.cisco.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5009ms
rtt min/avg/max/mdev = 43.656/43.703/43.770/0.214 ms
bash-4.4$
```

問題：使用状況レポートの送信に失敗する

失敗の理由として次が考えられます。

- 通信障害のため、製品インスタンスは RUM レポートを送信できませんでした。

推奨するアクション：

- **show license tech support** コマンドを使用して RUM レポートの期限が近いか確認します。近くなく、問題がダウンしているサーバーやリンクにある場合は、しばらくしてから再試行できます。
- 通信エラーが続く場合は、トポロジで必要とされるトランスポートタイプと URL が設定されているか確認してください。

問題：レポート確認応答の受信に失敗する

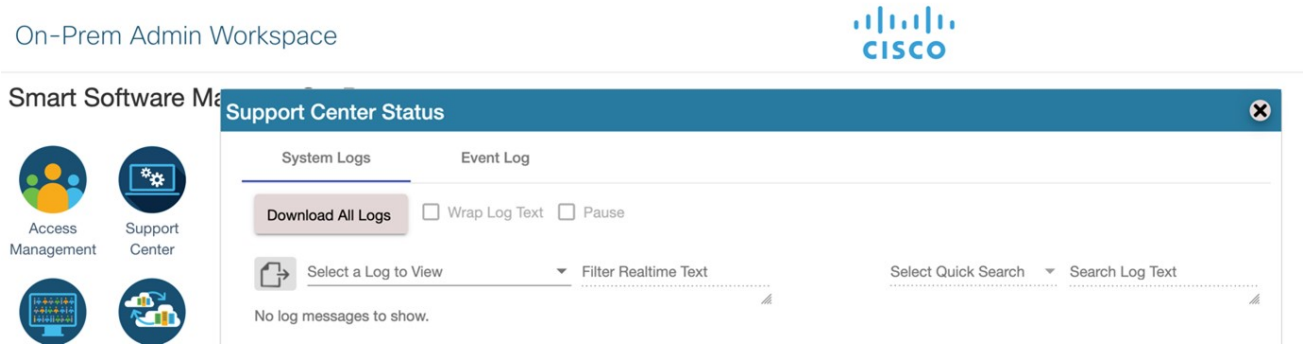
失敗の理由として次が考えられます。

- 接続の問題。トポロジによっては、CSSM、CSLU、またはSSMオンプレミスとの接続の問題を意味する場合があります。
- 通信の遅延。RUMレポートが送信されてから、製品インスタンスでRUM確認応答（ACK）が利用可能になるまでに遅延が生じる場合があります。たとえば、CSLUまたはSSMオンプレミスを使用する場合、製品インスタンスが情報を受信する時は、CSLUまたはSSMオンプレミスがCSSMと製品インスタンスと同期するようにスケジュールされている時期によって異なります。直接接続モードでは、確認応答がスイッチで更新されるまでに約15分かかります。
- 以前に製品インスタンス（スイッチ）が別のオンプレミスアカウントで登録されていた場合、受信したACKが失敗する可能性があります。

推奨するアクション：

この問題をトラブルシューティングを行うには、次の手順を実行します：

1. **[オンプレミス管理ワークスペース（On-Prem Admin Workspace）]** > **[サポートセンター（Support Center）]** に移動します。 **[サポート センターのステータス（Support Center Status）]** ウィンドウが開きます。
2. **[サポート センターのステータス（Support Center Status）]** ウィンドウで、**[システム ログ（System Logs）]** タブをクリックし、**[すべてのログのダウンロード（Download All Logs）]**をクリックします。数秒後、zipファイルを保存するためのダイアログウィンドウが開きます。
3. **AllFiles.zip** ファイルをパスワード を 変更。
4. **AllFiles.zip** アーカイブを抽出します。



5. **messages**という名前のファイル内の次の症状を確認し、**「レコードが見つかりませんでした」というエラーを検索します。**例、

```
Aug 7 17:02:36 rtp-dcrs-licensing cf881d42a1b7: 2023/08/07
 17:02:36#011[ERROR]#011adapters/pi_routes_impl.go:1322#011
 Finding SL product by UDI {<switch> FDO212100YT} failed due to the following error: record not found.
```

6. また、CSSMに製品インスタンスがなく、オンプレミスに製品インスタンスがあるという可能性もあります。

推奨するアクション：

1. 信頼コードがインストールされていることを確認します。

2. 信頼コードがインストールされている場合は、 **show license status** の **[Usage reporting:]** を確認して、レポートが同期されているかどうかを確認します。**[次のレポートプッシュ（Next report push）]** フィールドには、同期についての次の情報が表示されます：

```
Usage reporting:
         Last ACK received: <none>
         Next ACK deadline: <none>
         Reporting push interval: <none>
         Next ACK push check: <none>
         Next report push: <none>
         Last report push: <none>
         Last report file write: <none>
Trust Code installed: Jul 14 11:40:36 2023 UTC
         Active: PID: <device_pid>, SN: <device_sn>
                 Jul 14 11:40:36 2023 UTC
```

3. 同期が自動的に行われない場合は、次のように実装されたトポロジに基づいてオンデマンド同期を開始します：

   - オンライン トポロジの場合、**license smart sync** コマンドは特権 EXEC モードで使用してください。SSM オンプレミスがトポロジで使用されている場合は、さらに、 SSM オンプレミスのスイッチだけでなくシスコにも同期します。
   - オフライン トポロジの場合は、RUM レポートを CSSM にアップロードし、ACK をスイッチに再度インストールします。

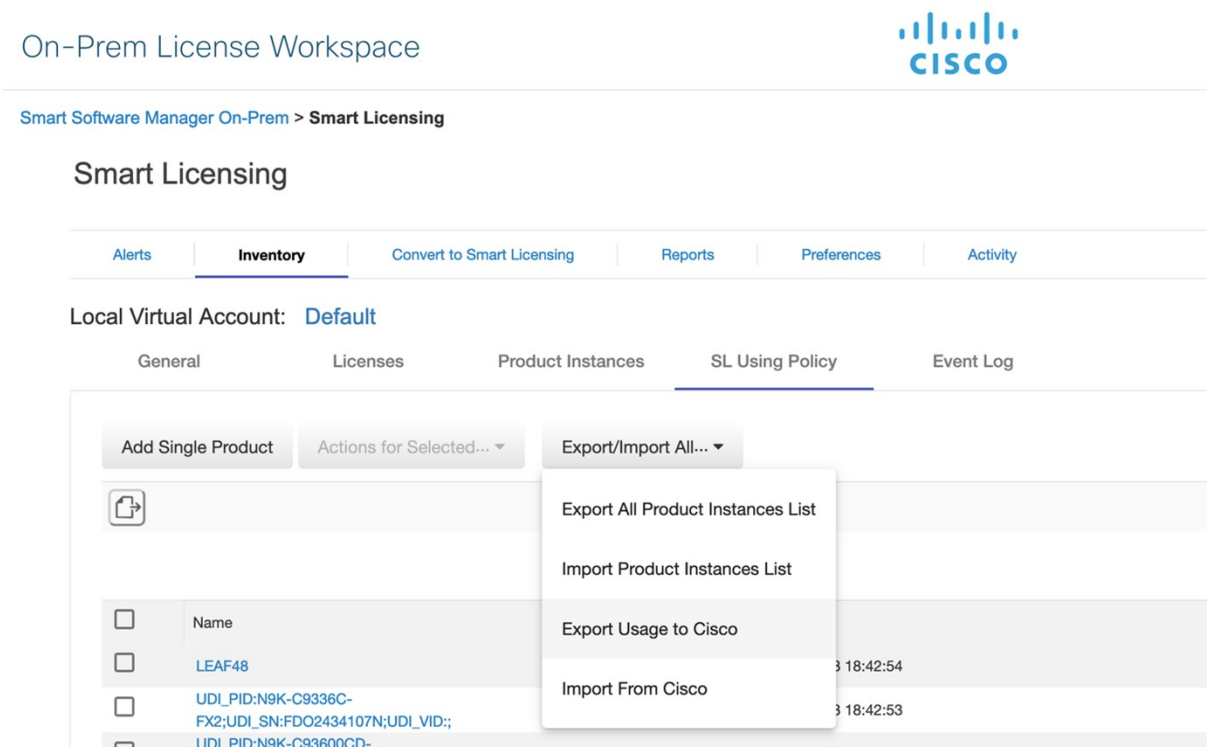
4. 同期の完了後、CSSM の確認応答を受信するまで 15 分間待機します。

5. オンプレミスにすでに登録されているデバイスの理由により確認応答が失敗した場合は、オンプレミス レポートの同期アウトオブバンド（**Export/Import Cisco Usage Report/ACK**）を実行します。

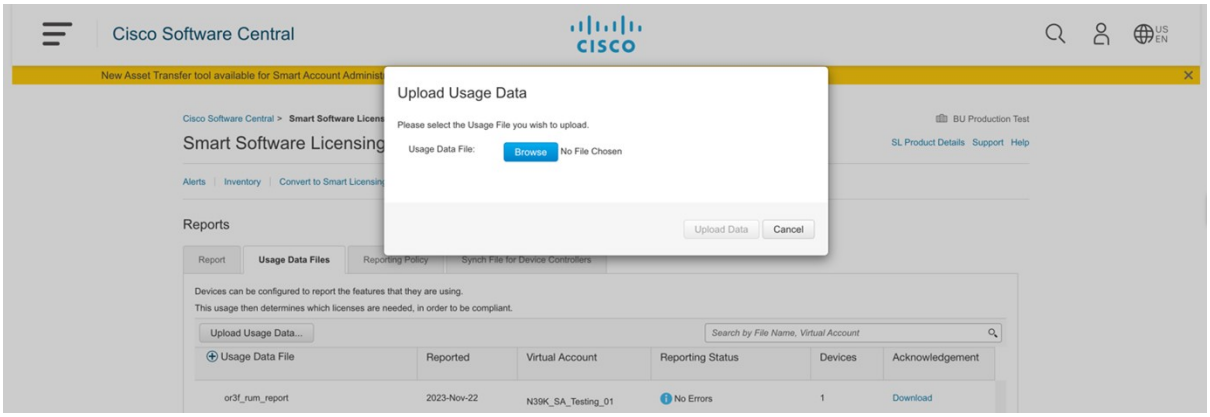
   1. オンプレミスサーバーで、 **[Smart Software Manager オンプレミス（Smart Software Manager On-Prem）]** > **[スマートライセンス（Smart Licensing ）]** > **[インベントリ（Inventory）]** > **[ポリシーを使用するSL（SL Using Policy）]**に移動します。

      次に、確認応答が必要な製品名を選択します。

      次に、 **[すべてをエクスポート/インポート（Export/Import All）]** ドロップダウン メニューで **[シスコに使用状況をエクスポート（Export Usage to Cisco）]** を選択し、エクスポートしたレポートをシステムにダウンロードします。



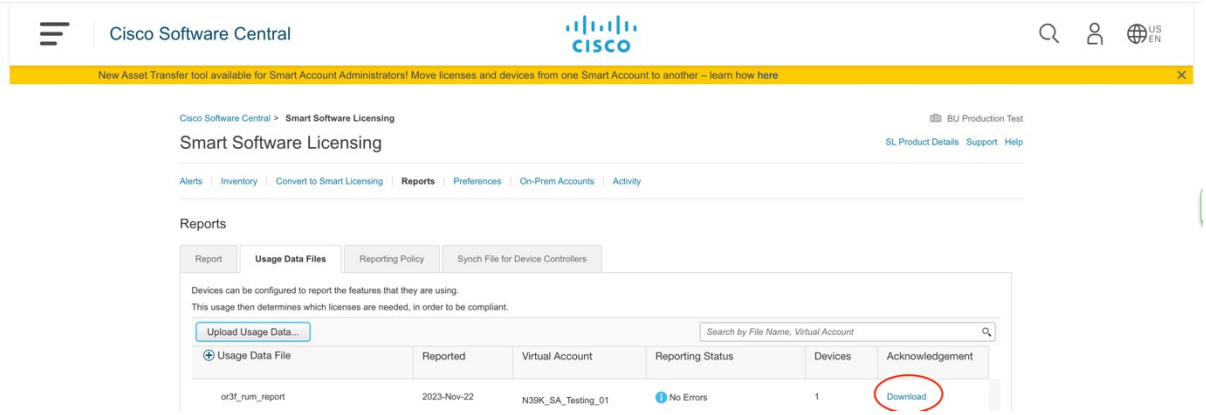
2. ダウンロードしたレポートをアップロードして ACK レポートを生成するには、それぞれの CSSM オンプレミス アカウントに移動し、**[レポート（Reports）]** > **[使用状況データ ファイル（Usage Data Files）]** > **[使用状況データ ファイルのアップロード（Upload Usage Data File）]** に移動します。**[使用状況データのアップロード（Upload Usage Data）]** ボタンをクリックします。**[使用データのアップロード（Upload Usage Data）]** ダイアログ ボックスが表示されます。



3. **[使用状況データのアップロード（Upload Usage Data）]** ダイアログ ボックスで、**[参照（Browse）]** ボタンをクリックし、アップロードする（以前にダウンロードした）システムからアップロードするレポートを選択して、 **[データのアップロード（Upload Data）]** ボタンをクリックします。

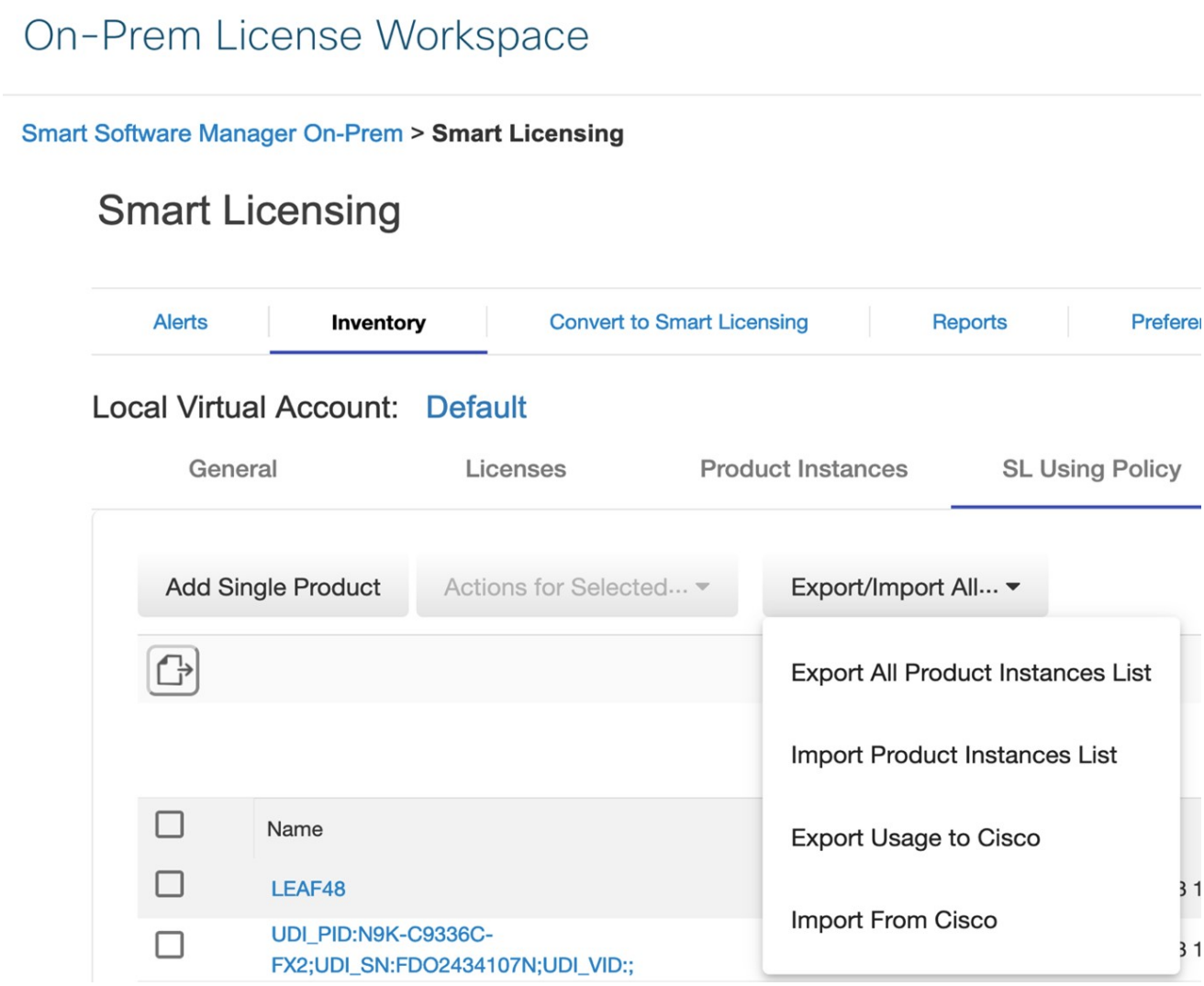
   処理に時間がかかるため、しばらく待ちます。表示されるエラーは無視してください。ファイルが **[使用状況データ ファイル（Usage Data Files）]** タブにアップロードされます。

4. アップロードした使用状況データファイルの ACK レポートをダウンロードするには、ファイルを選択し、**[確認（Acknowledgment）]** 列の **[ダウンロード（Download）]** リンクをクリックします。



5. ダウンロードした ACK ファイルをオンプレミスにアップロードします。これを行うには、**[Smart Software Manager オンプレミス（Smart Software Manager On-Prem）]** > **[スマートライセンス（Smart Licensing）**] > **[インベントリ（Inventory）]** > **[ポリシーを使用するSL（SL Using Policy）]**に移動します。

   次に、**[全てをエクスポート/インポート（Export/Import All）]** ドロップダウンメニューで**[シスコからインポート（Import From Cisco）]** を選択し、ダウンロードした確認応答レポートをアップロードします。



6. レポートがアップロードされると、それぞれのデバイスに受信した確認応答ステータスが反映されます。

（注）

確認応答が受信されなくても、スイッチの機能は影響を受けません。設定されたポリシーに従ってレポート期間が期限切れになった場合、または期限切れに近づくと、レポートを行わない場合の syslog を受信できます。確認応答が表示されない場合は、シスコのテクニカル サポート担当者にお問い合わせください。

システム メッセージの概要

システムメッセージは、システムソフトウェアからコンソール（および任意で別のシステムのロギングサーバー）に送信されます。すべてのシステム メッセージがシステムの問題を示すわけではありません。通知目的のメッセージもあれば、通信回線、内蔵ハードウェア、またはシステム ソフトウェアの問題を診断するうえで役立つメッセージもあります。

システム メッセージの読み方

システムログメッセージには最大 80 文字を含めることができます。各システム メッセージはパーセント記号（%）から始まります。構成は次のとおりです。

図 *1:*

%FACILITY

メッセージが参照するファシリティを示す 2 文字以上の大文字です。ファシリティはハードウェア デバイス、プロトコル、またはシステム ソフトウェアのモジュールである可能性があります。

SEVERITY

0 ～ 7 の 1 桁のコードで、状態の重大度を表します。この値が小さいほど、重大な状況を意味します。

表 *1:* メッセージの重大度

重要度	説明
0：緊急	システムが使用不可能です。
1：アラート	ただちに対応が必要な状態。
2：クリティカル	危険な状態。
3：エラー	エラー条件。
4：警告	警告条件。
5：通知	正常だが注意を要する状態。
6：情報	情報メッセージのみ。
7：デバッグ	デバッグ時に限り表示されるメッセージのみ。

MNEMONIC

メッセージを一意に識別するコード。

メッセージ テキスト

メッセージテキストは、状態を説明したテキスト文字列です。メッセージのこの部分には、端末ポート番号、ネットワーク アドレス、またはシステム メモリ アドレス空間の位置に対応するアドレスなど、イベントの詳細情報が含まれることがあります。この可変フィールドの情報はメッセージごとに異なるので、ここでは角カッコ（[ ]）で囲んだ短い文字列で示します。たとえば 10 進数は [dec] で表します。

表 *2:* メッセージの変数フィールド

重要度	説明
[char]	1 文字

重要度	説明
[chars]	文字列
[dec]	10 進数
[enet]	イーサネット アドレス（たとえば 0000.FEED.00C0）
[hex]	16 進数
[inet]	インターネット アドレス（10.0.2.16）
[int]	整数
[node]	アドレス名またはノード名
[t-line]	8 進数のターミナルライン番号（10 進数 TTY サービスが有効な場合は 10 進数）
[clock]	クロック（例：01:20:08 UTC Tue Mar 2 1993）

システムメッセージ

このセクションでは、発生する可能性のある SLP 関連のシステムメッセージ、考えられる理由失敗の（失敗メッセージの場合）、および推奨するアクション（アクションが必要な場合）を示します。

すべてのエラーメッセージについて、問題を解決できない場合は、シスコのテクニカルサポート担当者に次の情報をお知らせください。

- コンソールまたはシステムログに出力されたとおりのメッセージ。
- show license tech support および show license history message コマンドからの出力。

SLP 関連のシステム メッセージ:

- %LICMGR-3-LOG_SMART_LIC_POLICY_INSTALL_FAILED
- %LICMGR-3-LOG_SMART_LIC_AUTHORIZATION_INSTALL_FAILED
- %LICMGR-3-LOG_SMART_LIC_COMM_FAILED
- %LICMGR-3-LOG_SMART_LIC_COMM_RESTORED
- %LICMGR-3-LOG_SMART_LIC_POLICY_REMOVED
- %LICMGR-3-LOG_SMART_LIC_TRUST_CODE_INSTALL_FAILED
- %LICMGR-4-LOG_SMART_LIC_REPORTING_NOT_SUPPORTED
- %LICMGR-6-LOG_SMART_LIC_POLICY_INSTALL_SUCCESS
- %LICMGR-6-LOG_SMART_LIC_AUTHORIZATION_INSTALL_SUCCESS
- %LICMGR-6-LOG_SMART_LIC_AUTHORIZATION_REMOVED
- %LICMGR-6-LOG_SMART_LIC_REPORTING_REQUIRED

- %LICMGR-6-LOG_SMART_LIC_TRUST_CODE_INSTALL_SUCCESS

エラーメッセージ

`%LICMGR-3-LOG_SMART_LIC_POLICY_INSTALL_FAILED`：新しいライセンス ポリシーのインストールは、失敗しました:`[chars]`。

説明：ポリシーがインストールされましたが、ポリシーコードの解析中にエラーが検出され、インストールに失敗しました。[chars] はエラーの詳細を示すエラー文字列です。

失敗の理由として次が考えられます。

- 署名の不一致：これは、システムクロックが正確でないことを意味します。
- タイムスタンプの不一致：製品インスタンスのシステムクロックが CSSM と同期していないことを意味します。

推奨するアクション：

考えられる両方の失敗の理由に関しては、システムクロックが正確で、CSSM と同期していることを確認します。グローバル構成モードで ntp server を設定します。次に例を示します。

Device(config)# **ntp server 198.51.100.100 version 2 prefer**

前述の手順を実行しても、ポリシーのインストールが失敗する場合は、シスコのテクニカルサポート担当者にお問い合わせください。

エラーメッセージ

`%LICMGR-3-LOG_SMART_LIC_AUTHORIZATION_INSTALL_FAILED`：新しいライセンス承認コードのインストールは、`[chars]: [chars]`で失敗しました。

このメッセージは、Cisco Nexus スイッチには該当しません。これらの製品インスタンスには輸出規制ライセンスや適用ライセンスがないためです。

エラーメッセージ

`%LICMGR-3-LOG_SMART_LIC_COMM_FAILED： [chars] : [chars]` の通信障害

説明：CSSM または CSLU とのスマートライセンシング通信が失敗しました。最初の [chars] は現在設定されている転送タイプで、2 番めの [chars] はエラーの詳細を示すエラー文字列です。このメッセージは、失敗した通信の試行ごとに表示されます。

失敗の理由として次が考えられます。

- CSSM または CSLU に到達できない：これは、ネットワーク到達可能性の問題があることを意味します。
- 404 ホストが見つからない：これは CSSM サーバーがダウンしていることを意味します。

製品インスタンスが RUM レポート（CSLU を介した CSSM への接続：製品インスタンス開始型通信、CSSM に直接接続、CSLU は CSSM から切断：製品インスタンス開始型通信）の送信を開始するトポロジの場合、この通信障害メッセージがスケジュールされたレポート（**license smart usage interval** `interval_in_days` グローバル コンフィギュレーション コマンド）と一致するときに、製品インスタンスは、スケジュールされた時間が経過した後、最大 4 時間にわたって RUM レポートを送信しようとします。（通信障害が続くために）それでもレポートを送信できない場合、システムは間隔を 15 分にリセットします。通信障害が解消されると、レポート間隔はユーザが最後に設定した値に戻ります。

推奨するアクション：

CSSM に到達できない場合、および CSLU に到達できない場合のトラブルシューティング手順を説明します。CSSM が到達不能で、設定されている転送タイプが smart の場合：

1. スマート URL が正しく設定されているかどうかを確認します。特権 EXEC モードで **show license status** コマンドを使用して、URL が次のようになっているかどうかを確認します。https://smartreceiver.cisco.com/licservice/licenseそうでない場合は、グローバル コンフィギュレーション モードで **license smart url smart**`smart_URL` コマンドを再設定します。

2. DNS 解決を確認します。製品インスタンスが smartreceiver.cisco.com または nslookup で変換された IP に対して ping を実行できることを確認します。次の例は、変換された IP に対して ping を実行する方法を示しています。

```
Device# ping 171.70.168.183 Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 171.70.168.183, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

CSSM が到達不能で、設定されている転送タイプが **callhome** の場合：

1. URL が正しく入力されているかどうかを確認します。特権 EXEC モードで **show license status** コマンドを使用して、URL が https://tools.cisco.com/its/service/oddce/services/DDCEService のとおりであるかどうかを確認します。

2. Call Home プロファイル **CiscoTAC-1** がアクティブで、接続先 URL が正しいことを確認します。**show call-home profile all** コマンドは特権 EXEC モードで使用してください。

```
Current smart-licensing transport settings: Smart-license messages: enabled
Profile: CiscoTAC-1 (status: ACTIVE)
Destination  URL(s): https://tools.cisco.com/its/service/oddce/services/DDCEService
```

3. DNS 解決を確認します。製品インスタンスが tools.cisco.com または nslookup で変換された IP に対して ping を実行できることを確認します。

```
Device# ping tools.cisco.com Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 173.37.145.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 41/41/42 ms
```

   上記の方法で解決しない場合は、製品インスタンスが設定されているかどうか、製品インスタンスの IP ネットワークが稼働しているかどうかを確認します。ネットワークが稼働していることを確認するには、インターフェイス コンフィギュレーション モードで **no shutdown** コマンドを設定します。

   デバイスがサブネット IP でマスクされたサブネットかどうか、また DNS IP が設定されているかどうかを確認します。

4. HTTPS クライアントの送信元インターフェイスが正しいことを確認します。

   現在の設定を表示するには、特権 EXEC モードで **show ip http client** コマンドを使用します。グローバル コンフィギュレーション モードで **ip http client source-interface** コマンドを使用して、再設定します。上記の方法で解決しない場合は、ルーティングルール、およびファイアウォール設定を再確認します。

CSLU に到達できない場合：

- CSLU 検出が機能するかどうかを確認します。
  - cslu-local のゼロタッチ DNS 検出またはドメインの DNS 検出。

show license all コマンドの出力で、[最終 ACK 受信：（Last ACK received:）] フィールドを確認します。このフィールドに最新のタイムスタンプがある場合は、製品インスタンスがCSLUと接続されていることを意味します。ない場合は、次のチェックに進みます。

製品インスタンスが **cslu-local** に対して ping を実行できるかどうかを確認します。ping が成功すると、製品インスタンスが到達可能であることが確認されます。

上記の方法で解決しない場合は、ホスト名 **cslu-local** が CSLU の IP アドレス（CSLU をインストールした Windows ホスト）にマッピングされているエントリを使用してネームサーバーを構成します。グローバル コンフィギュレーション モードで **ip domain name** domain-name コマンドと **ip name-server** server-address コマンドを設定します。この例では、CSLU IP は 192.168.0.1 で、name-server によってエントリ **cslu-local.example.com** が作成されます。

```
Device(config)# ip domain name example.com
Device(config)# ip name-server 192.168.0.1
```

- CSLU URL が設定されています。

  show license all コマンド出力の **Transport:** ヘッダーで、次の点を確認します。 **Type:** は **cslu** で、**Cslu address:** は CSLU をインストールした Windows ホストのホスト名または IP アドレスになっている必要があります。残りのアドレスが下記のように設定されているかどうかを確認するとともに、ポート番号が 8182 であるかどうかを確認します。

  ```
  Transport:
  Type: cslu
  Cslu address: http://192.168.0.1:8182/cslu/v1/pi
  ```

  そうでない場合は、グローバル コンフィギュレーション モードで **license smart transport cslu** および **license smart url cslu** *http://<cslu_ip_or_host>:8182/cslu/v1/pi* コマンドを設定します。

前述の手順を実行しても、ポリシーのインストールが失敗する場合は、シスコのテクニカルサポート担当者にお問い合わせください。

エラーメッセージ

```
%LICMGR-3-LOG_SMART_LIC_COMM_RESTORED: Communications with the [chars] restored. [chars] - depends on the
transport type
-  Cisco Smart Software Manager (CSSM)
-  Cisco Smart License utility (CSLU)
Smart Agent communication with either the Cisco Smart Software Manager (CSSM) or the Cisco Smart License
utility (CSLU) has been restored. No action required.
```

説明：CSSM または CSLU との製品インスタンス通信が復元されます。

推奨するアクション：アクションは必要ありません。

エラーメッセージ

`%LICMGR-3-LOG_SMART_LIC_POLICY_REMOVED`：ライセンシング ポリシーが削除されました。

説明：以前にインストールされたライセンスポリシーが削除されました。Cisco default ポリシーが自動的に有効になります。これにより、スマート ライセンシングの動作が変更される可能性があります。

失敗の理由として次が考えられます。

特権 EXEC モードで **license smart factory reset** コマンドを入力すると、ポリシーを含むすべてのライセンス情報が削除されます。

推奨するアクション：

ポリシーが意図的に削除された場合、それ以上のアクションは不要です。

ポリシーが誤って削除された場合は、ポリシーを再適用できます。実装したトポロジに応じて、該当するメソッドに従ってポリシーを取得します。

- CSSM に直接接続：

  show license status を入力し、[**Trust Code Installed:**] フィールドを確認します。信頼が確立されると、CSSM は再度ポリシーを自動的に返します。ポリシーは、対応するバーチャル アカウントのすべての製品インスタンスに自動的に再インストールされます。

  信頼が確立されていない場合は、次のタスクを実行します：*CSSM* からの信頼コード用新規トークンの生成および ポリシーを使用してスマート ライセンシングを設定するための一般的なタスク 内の 信頼コードのインストール トピックを参照します。これらのタスクを完了すると、CSSM は再度ポリシーを自動的に返します。その後、バーチャル アカウントのすべての製品インスタンスにポリシーが自動的にインストールされます。
- CSLU を介して CSSM に接続：
  - 製品インスタンス開始型通信の場合は、特権 EXEC モードで **license smart sync** コマンドを入力します。同期要求により、CSLU は欠落している情報（ポリシーまたは承認コード）を製品インスタンスにプッシュします。
- CSLU は CSSM から切断：
  - 製品インスタンス開始型通信の場合は、特権 EXEC モードで **license smart sync** コマンドを入力します。同期要求により、CSLU は欠落している情報（ポリシーまたは承認コード）を製品インスタンスにプッシュします。次に、次のタスクを指定された順序で実行します： **Download All For Cisco (CSLU インターフェイス) > CSSM への使用状況データのアップロードと ACK のダウンロード > Cisco からのアップロード (CSLU インターフェイス)**「への使用状況データのアップロード」 を参照してください「ポリシーを使用してスマートライセンスを設定するための共通タスク」の「CSSM および ACK タスクのダウンロード」。。
- CSSM への接続なし、CSLU なし

  完全に外部との接続性がないネットワークにいる場合は、インターネットと CSSM に接続できるワークステーションから次のタスクを実行します：ポリシーを使用してスマート ライセンシングを設定するための一般的なタスク 内の*CSSM* からのポリシーファイルのダウンロード および スイッチへのファイルのインストール トピックを参照します。

エラーメッセージ

`%LICMGR-3-LOG_SMART_LIC_TRUST_CODE_INSTALL_FAILED`：新しいライセンス信頼コードのインストールは、`[chars]: [chars]` で失敗しました。

説明：信頼コードのインストールに失敗しました。最初の [chars] は、信頼コードのインストールが試行された UDI です。2 番目の [chars] は、エラーの詳細を示すエラー文字列です。

失敗の理由として次が考えられます。

- 信頼コードがすでにインストールされています。信頼コードは製品インスタンスの UDI にノードロックされています。UDI がすでに登録されている場合に別の UDI をインストールしようとすると、インストールは失敗します。
- スマート アカウントとバーチャル アカウントの不一致：これは、（トークン ID が生成された）スマート アカウントまたはバーチャル アカウントに、信頼コードをインストールした製品インスタンスが含まれていないことを意味します。CSSM で生成されたトークンは、スマート アカウントまたはバーチャル アカウントレベル、で適用され、そのアカウントのすべての製品インスタンスにのみ適用されます。
- 署名の不一致：これは、システムクロックが正確でないことを意味します。
- タイムスタンプの不一致：このことは、タイム製品インスタンスの時刻が CSSM と同期していないため、インストールが失敗する可能性があることを示します。

推奨処置：

- 信頼コードはすでにインストールされています。製品インスタンスに信頼コードがすでに存在する状況で信頼コードをインストールする場合は、特権 EXEC モードで **license smart trust idtoken** `id_token_value` {**local**|**all**} [**force**] コマンドを再設定します。再設定の際、**force** キーワードを必ず含めてください。**force** キーワードを入力すると、CSSM に送信されるメッセージに強制フラグが設定され、すでに存在する場合でも新しい信頼コードが作成されます。
- スマートアカウント-仮想アカウントの不一致：https://software.cisco.com/software/smart-licensing/alerts で CSSM Web UI にログインし、**[スマート ソフトウェア ライセンシング（Smart Software Licensing）]** > **[インベントリ（Inventory）]** > **[製品インスタンス（Product Instances）]**をクリックします。
- トークンを生成する製品インスタンスが、選択したバーチャル アカウントにリストされているかどうかを確認します。リストされている場合は、次のステップに進みます。リストされていない場合は、正しいスマート アカウントとバーチャルアカウントを確認して選択します。次に、次のタスクを再度実行します。*CSSM* からの信頼コードの新しいトークンの生成と信頼コードのインストール。https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/nx-os/licensing/guide/cisco-nexus-nx-os-smart-licensing-using-policy-user-guide/m-tasks-slp.html
- タイムスタンプと署名の不一致: グローバル設定モードで、ntp server コマンドを構成します。次に例を示します。

```
Device(config)# ntp server 198.51.100.100 version 2 prefer
```

エラーメッセージ

`%LICMGR-4-LOG_SMART_LIC_REPORTING_NOT_SUPPORTED`：この接続された CSSM オンプレミスはダウン rev で、拡張ポリシーと使用状況レポート モードをサポートしていません。

説明：Cisco Smart Software Manager オンプレミス（旧称 Cisco Smart Software Manager サテライト）は、SLP 環境ではサポートされていません。製品インスタンスは次のように動作します。

- 登録の更新と承認の更新の送信を停止します。
- 使用状況の記録を開始し、RUM レポートをローカルに保存します。

推奨処置：代わりに、サポートされているトポロジを参照し、いずれかを実装します。サポートされる展開モデルとトポロジを参照してください。

エラーメッセージ

`%LICMGR-6-LOG_SMART_LIC_POLICY_INSTALL_SUCCESS`：新しいライセンスポリシーが正常にインストールされました。

説明：次の方法でポリシーがインストールされました。

- ACK 応答の一部として

推奨するアクション：アクションは必要ありません。適用されているポリシー（使用中のポリシー）とそのレポート要件を確認するには、特権 EXEC モードで **show license all** コマンドを入力します。

`Error Message %LICMGR-6-LOG_SMART_LIC_AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization code was successfully installed on: [chars].`

このメッセージは、Cisco Nexus スイッチには該当しません。これらの製品インスタンスには輸出規制ライセンスや適用ライセンスがないためです。

エラーメッセージ

`%LICMGR-6-LOG_SMART_LIC_AUTHORIZATION_REMOVED:` ライセンス認証コードが `[chars]` から削除されました

説明： [chars] は、承認コードがインストールされた UDI です。承認コードが削除されました。これにより、製品インスタンスからライセンスが削除され、スマート ライセンシングとライセンスを使用する機能の動作が変更される可能性があります。

推奨するアクション：アクションは必要ありません。ライセンスの現在の状態を確認するには、特権 EXEC モードで **show license all** コマンドを入力します。

エラーメッセージ

`%LICMGR-6-LOG_SMART_LIC_REPORTING_REQUIRED`：使用状況レポートの確認は`[dec]`日以内に必要になります。

説明：これは、シスコへの RUM レポートが必要であることを意味するアラートです。[dec] は、このレポート要件を満たすために残された時間（日数）です。

推奨するアクション：要求された時間内に RUM レポートが送信されるようにします。

- 製品インスタンスが CSSM または CSLU に直接接続され、通信を開始し製品インスタンスでこのステップを完了するよう製品インスタンスが設定されている場合、製品インスタンスはスケジュールされた時間に使用状況情報を自動的に送信します。
- 技術的な問題により、スケジュールされた時間に送信されない場合は、特権 EXEC モードで **license smart sync** コマンドを実行できます。シンタックスの詳細については、コマンドリファレンスで license smart（特権 EXEC）コマンドを参照してください。
- 製品インスタンスが CSLU に接続されているが、CSLU が CSSM から切断されている場合は、次のタスクを実行します：**Cisco のすべてをダウンロード（CSLU インターフェイス）**、**CSSM への使用状況データのアップロードと ACK のダウンロード、および Cisco からのアップロード（CSLU インターフェイス）**。「ポリシーを使用してスマートライセンスを設定するための一般的なタスク」 の 「*Usage Data to CSSM* へのアップロードと *ACK* タスクのダウンロード」を参照してください。
- 製品インスタンスが CSSM から切断され、CSLU も使用していない場合は、特権 EXEC モードで **license smart save usage** コマンドを入力して、必要な使用状況情報をファイルに保存します。次に、CSSM に接続できるワークステーションから、次のタスクを実行します：*CSSM* への使用状況データのアップロードと *ACK* のダウンロード タスクを最初に実行して、ポリシーを使用してスマート ライセンシングを構成するための一般的なタスクの製品インスタンスへのファイルのインストール タスクを次に実行します。。

エラーメッセージ

`%LICMGR-6-LOG_SMART_LIC_TRUST_CODE_INSTALL_SUCCESS`：新しいライセンス信頼コードが `[chars]` に正常にインストールされました。

説明：[chars] は、信頼コードが正常にインストールされた UDI です。

推奨するアクション：アクションは必要ありません。信頼コードがインストールされていることを確認するには、特権 EXEC モードで show license status コマンドを入力します。出力のヘッダー **Trust Code Installed:** で更新されたタイムスタンプを探します。

ポリシーを使用したスマート ライセンシング FAQ

1. ポリシーを使用したスマート ライセンシングとは?

Smart Licensing Using Policy（SLP）はスマートライセンスの進化版です。

ポリシーを使用したスマートライセンシングにより、お客様のデイゼロ運用が簡素化されます。製品は評価モードで起動せず、製品ソフトウェアごとの登録は不要で、30 日ごとに Cisco Cloud と継続的に通信する必要はありません。ただし、ライセンス使用の遵守にはソフトウェアレポートが必要です。次の方法でレポートを実行できます。

- シスコの工場から。すべての新規購入が注文のスマート アカウントを含む場合
- Smart Software Manager（SSM）オンプレミス（バージョン XXXX）
- Cisco Smart License Utility （CSLU） Lite - Windows アプリケーション
- サード パーティ システム用の API/CLI 経由
- スマート アカウントに直接

2. Smart Licensing Using Policy は、どのプラットフォームとソフトウェアリリースでサポートされますか。

Cisco NX-OS リリース 10.2（1）F 以降、ポリシーを使用したスマート ライセンシングが必要です。そして、Cisco Nexus 9000 および 3000 プラットフォーム スイッチで有効です。強制ライセンスとエクスポート ライセンスは、Cisco Nexus9000 プラットフォーム スイッチではサポートされていません。

3. スマート ライセンシングとポリシーを使用したスマート ライセンシングの主な違いは何ですか。

ポリシーを使用したスマートライセンス	スマートライセンス
必須評価モード	登録なし、評価モードなし
ソフトウェアの遵守のためにデバイスごとに実行する CSSM または SSM オンプレミスへのデイゼロ登録	適用されていないライセンスの変更は可能ですが、レポートが必要です
30 日ごとの継続的なライセンスレポート	変更時のレポートポリシーとお客様固有レポートポリシー
ソフトウェアの遵守は、使用前の製品ごとのアクティビティ要件です	ソフトウェアの遵守は変更時にのみ管理され、SW を支援する自動化ツールが提供されます

4. Cisco NX-OS リリース 10.1（2）と Cisco Nexus リリース 10.2（1）F の CSSM の違いは何ですか。

CSSM では、ユーザーは使用前にデバイスを登録する必要がなくなります。ただし、自動レポートを設定するには、シスコツール、API レポート、または CSSM への信頼できる接続を使用する製品からの直接接続を使用できます。または、[レポート（Reporting）] タブと [使用状況データファイル（Usage Data Files）] タブの [使用状況データのアップロード（Upload Usage Data）] ボタンを使用して、ソフトウェア使用記録（RUM レポート）を CSSM に直接手動でアップロードできます。ソフトウェア使用 RUM レポートを送信するには、アクティブなスマート アカウントが必要です。

5. レポートはどれほどの頻度で必要ですか。

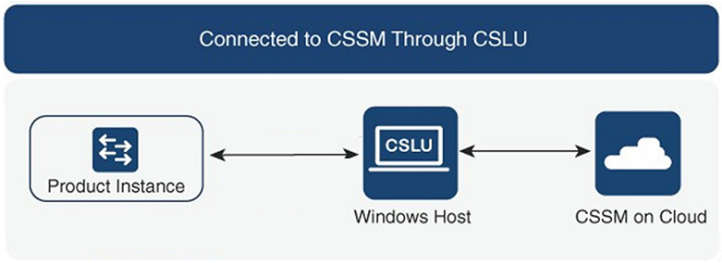
- レポートは、ソフトウェアの使用に変更があった場合にのみ、90 日以内に必要となります。
- 継続的なレポート頻度：365 日
- 非強制/非輸出、最初のレポートは 90 日以内に必要です。

6. Cisco Smart Software Manager（CSSM）に接続するためにサポートされているトポロジは何ですか。

サポートされているトポロジは次のとおりです。

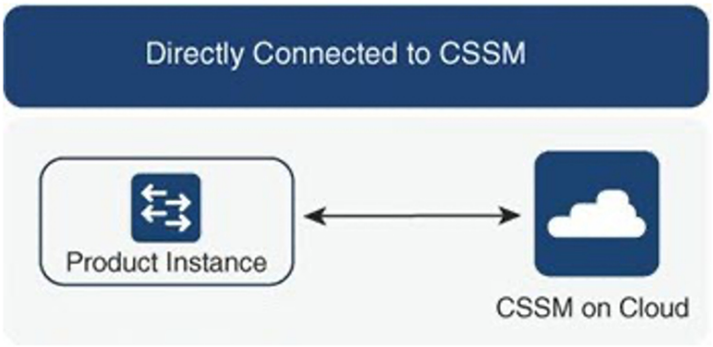
トポロジ 1: CSLU を介して CSSM に接続

図 *2：*



トポロジ 2: CSSM に直接接続

図 *3：*

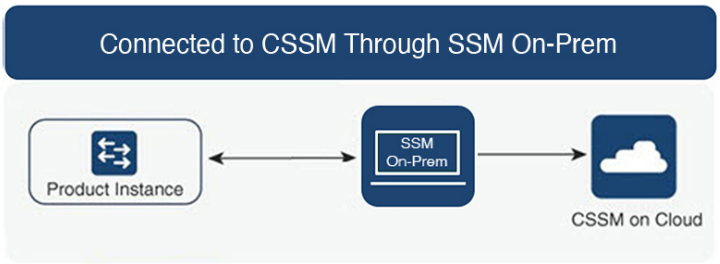


（注）

このトポロジには、信頼トークンがのみ必要です。

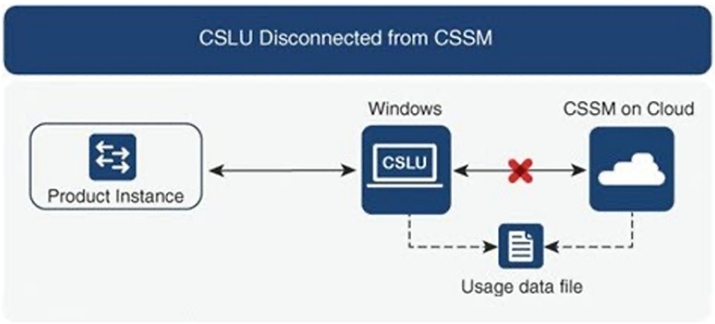
トポロジ 3：SSM オンプレミスを介して CSSM に接続

図 *4*：



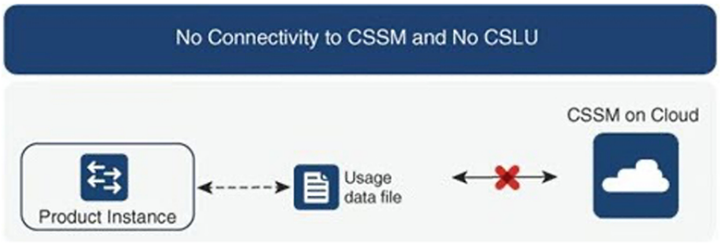
トポロジ 4: CSLU は CSSM から切断

図 *5*：



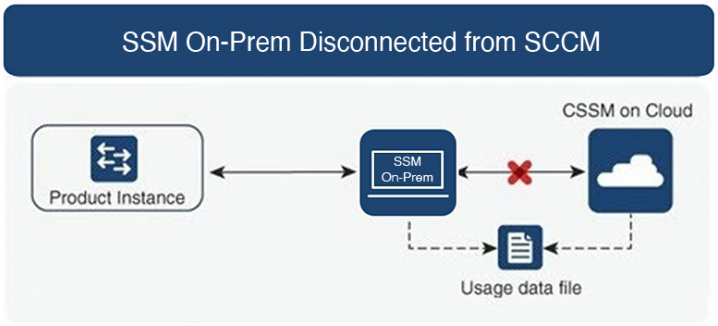
トポロジ 5: CSSM への接続なし、CSLU なし

図 *6*：



トポロジ 6：SSM オンプレミスは CSSM から切断

図 *7*：



7. お客様は、どのようにソフトウェア使用状況を報告しますか。

Cisco Smart Licensing Using Policy には、ソフトウェアの使用状況をレポートするための、オンラインモードとオフラインモードを使用するさまざまなレポートオプションが用意されています。

- オフラインまたは直接接続モードのスイッチから。
- Cisco Smart License Utility（CSLU）Lite - Windows アプリケーション
- SSM オンプレミス
- API 経由で CSSM に直接接続

8. お客様はトラストトークンをインストールする必要がありますか。

いいえ。お客様が CSSM への直接接続を使用していない限り、1 回ごとに信頼できる情報交換が確立されます。

9. お客様が、レガシー ライセンスから、またはスマート ライセンシングから-輸出管理対象外ソフトウェアのポリシーを使用したスマート ライセンシングにアップグレードするとどうなりますか。

お客様が（PAK（製品アクティベーションキー）ファイルや従来のスマート ライセンスなどの）レガシー ライセンス スキームからポリシーを使用したスマート ライセンスに移行する場合、ライセンス転換が自動的に行われることが期待されます。

（注）

- トポロジ 5：CSSM への接続なし、CSLU なしの場合、ポリシーを使用したスマートライセンシングの移行後、最初の RUM レポートが生成されるまで 1 時間待つことをお勧めします。
- トランスポート モードがオフの場合、PAK ベースのライセンス変換をサポートするために、SLP への移行から 1 時間後に最初の rum レポートを収集する必要があります。rum レポートを収集する前に、ライセンス データの変換が空白でないことを確認してください。

10. スマート アカウント/バーチャル アカウントは、デフォルトでポリシーを使用したスマート ライセンシングに移行されますか。それともリクエストが必要ですか。

2020 年 11 月以降、スマート アカウント/バーチャル アカウントでは、ポリシーを使用したスマート ライセンシング機能が有効になります。スマート アカウントの移行は不要です。

11. スマート アカウント内のすべてのバーチャル アカウントで、Smart Licensing Using Policy が有効になっていますか。

はい。

12. ポリシーを使用したスマート ライセンシング対応 SA/VA は、ポリシーを使用したスマート ライセンシング以外のイメージを処理できますか。

はい

13. ポリシーを使用したスマートライセンシング以外の場合は、ポリシーを使用したスマートライセンシング SA/VA に接続できますか？

はい。

14. 既存のソフトウェア サブスクリプション階層に変更はありますか。

ソフトウェア サブスクリプション階層に変更はなく、同じままです。

15. リリース 10.2（1）F は、ポリシーを使用したスマート ライセンシングのみをサポートしますか？

リリース 10.2(1)F 以降のデバイスでは、ポリシーを使用したスマートライセンシングのみがサポートされます。このリリースでは、従来のライセンシングとスマート ライセンシングはサポートされていません。

16. ポリシーを使用したスマートライセンシングに移行した後、最初のレポートを送信するまで最大どれくらいの時間がかけられますか。

Nexus の 1 つ以上の機能にライセンスが必要な場合、90 日以内のレポートが必要です。

17. 誰がポリシーを決定しますか。また、1 台のデバイスにいくつのポリシーを適用できますか。

CSSM は、製品に適用されるポリシーを決定します。特定の時点で使用されているポリシーは 1 つだけです。

18. ポリシーはハード要件ですか。

ポリシーはシスコからの要件です。これはデバイスのソフト要件であり、機能制限ではありません。高度な VXLAN 機能の限られたセットを除き、ライセンスが不十分なために Nexus によって機能が無効になることはありません。

19. Cisco Smart Licensing Utility（CSLU）とは何ですか。

Cisco Smart Licensing Utility（CSLU）は、シスコ製品からのソフトウェア使用状況レポートの受信または収集を自動化し、ソフトウェア使用状況を Cisco Smart Software Manager（CSSM）のスマート アカウントにレポートするために使用される Windows アプリケーションです。

20. CSLU をインストールするための最小 Windows システム要件は何ですか。

コンポーネント	最小	推奨
ハードディスク	100 GB	200 GB
RAM	8 GB	8 GB
CPU	x86 デュアルコア	x86 クワッドコア
イーサネット NIC	1	1

21. CSLU の主な機能は何ですか。

- 製品インスタンスからプッシュモードまたはプルモードでライセンス使用状況レポートを収集します。
- 課金情報および分析のために使用状況レポートを CSSM に保存および転送します。
- CSSM からポリシーと承認コードを取得します。
- スタンドアロンのマイクロサービスとして展開できます。
  - Windows ホスト（最大 10,000 製品インスタンス（PI））
- ソフトウェア コンポーネントとしてコントローラ ベースの製品と統合することもできます。
- マイクロサービスの展開方法に関係なく、ライセンスデータのオンラインまたはオフライン接続モデルを提供できます。

22. CSLU のレポート形式は何ですか？

CSLU レポート形式は、ISO 19770-4 標準 RUM レポート形式に基づいています。JSON 形式で提供され、信頼モデルごとに署名されます。

23. ソフトウェア使用レポートを収集するためのさまざまなツールにはどのようなものがありますか。

お客様は、NX -OS で利用可能なさまざまな API のセットを使用できオン

24. シスコはどのようなデータを取得しますか。

ポリシーを使用したスマート ライセンシングをサポートする各シスコ製品のソフトウェア調整に必要なデータフィールドを以下に示します。

UDI	**ハードウェア製品シリアル番号**
SN	ソフトウェア固有 ID シリアル番号
ソフトウェアパッケージと登録 ID	ソフトウェア製品パッケージおよび権限付与タグ
カウント	ライセンス権限ごとのソフトウェア使用カウント
タイムスタンプ	ソフトウェア利用資格ごとの変更と使用

以下は、ポリシーを使用したスマート ライセンシングをサポートする各シスコ製品のソフトウェア調整用オプションのデータフィールドです。

SA-VA レベル 1	**例：エンティティ（SA にマップ）**
SA-VA レベル 2	例：GEO（SA にマップ）
SA-VA レベル 3	例：部門（SA にマップ）
SA-VA レベル 4	例：建物（SA にマップ）
SA-VA レベル 5	例：部屋（SA にマップ）

SA-VA レベル 1	例：エンティティ（SA にマップ）
フリーフォーム	データがシスコに戻らない
フリーフォーム	データがシスコに戻らない

（SA = スマート アカウント、VA = バーチャル アカウント）

25. ポリシーを使用したスマート ライセンシングはどのようにデバイス交換（RMA）と連携しますか。

交換されたデバイスのポリシーを使用したスマートライセンシング構成を、交換用デバイスに適用する必要があります。既存の構成が新しいデバイスで使用できない、または機能しない場合は、サポートされる展開モデルとトポロジ および ポリシーを使用したスマート ライセンシングへの移行を参照してください。

26. ライセンスの機能施行タイプにはどんなものがありますか。

機能制限タイプは、ライセンスを使用する前に認証が必要かどうかを示します。ライセンス施行には次の 3 つのタイプがあります。

- 非強制ライセンスは、非強制ライセンスは、外部との接続がないネットワークで、または接続されたネットワークで使用する前の承認を必要としません。このようなライセンスの使用条件は、シスコ エンド ユーザ ライセンス契約（EULA）に従います。
- 強制：この強制タイプに属するライセンスは、使用前に認証が必要です。必要な承認は承認コードの形式であり、対応する製品インスタンスにインストールする必要があります。

（注）

リリース 10.2（1）F では、強制されていないライセンスのみがサポートされています。

27. ライセンスと一緒にハードウェアを注文した場合、割り当て後、特定のスマート アカウントにスマート ライセンスが反映されるまでにどのくらいの時間がかかりますか？

スマート ライセンスは、約 24 ～ 96 時間で CSSM に反映されます。

28. お客様が、スマート ライセンシングから輸出管理対象外ソフトウェアから SLP にアップグレードするとどうなりますか？

お客様がレガシー ライセンスか SLP にアップグレードする場合、運用上の変更はありません。すべてのキーはアップグレード中も保持されます。

29. ASCII リロード後に SLP レポートが自動的に同期しない場合、同期を手動でトリガーする必要がありますか？

これは稀なシナリオです。SLP トランスポート モードが SMART で、信頼が確立され、レポートが同期され、ACK が受信された場合、**copy r s** と **reload** コマンドが発行された場合、ボックスが起動すると、レポートが自動的に同期され、期待どおりに ACK が受信されます。ただし、**ascii reload** コマンドが発行され、ボックスが表示されたときにレポートが自動的に同期されない場合は、 **license smart sync all** コマンドを実行してプロセスを開始します。

30. vPC ピアの間で、SLP に登録するのは 1 つの vPC ピア スイッチだけで十分ですか？

いいえ。SLPに関しては、すべてのvPCピアスイッチが個別のエンティティとして機能するため、両方のスイッチを登録する必要があります。

参照先

SLPの詳細については、[ポリシー ユーザー ガイドを使用したCisco Nexus 9000 および 3000 シリーズ NX-OS スマートライセンス（Cisco Nexus 9000 and 3000 Series NX-OS Smart Licensing Using Policy User Guide）] を参照してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。