&；の設定SLUPを使用したCatalyst 9800 Unified LicensingおよびSmart Licensingのトラブルシューティング

内容

- はじめに
- 前提条件
  - 要件
  - 使用するコンポーネント
- 背景説明
- Unified Licensing、Enforcement、およびSLUP
- Unified LicensingでのAPコンプライアンスの確認
- 従来のライセンスとSLUP
- コンフィギュレーション
  - 直接接続CSSM
  - CSLUに接続
    - 製品インスタンス起動
    - CSLU開始
  - オンプレミスのSSMに接続
  - HTTPSプロキシによるスマートトランスポートの設定
  - 通信周波数
  - ライセンスの初期設定へのリセット
  - RMAまたはハードウェア交換の場合
  - 特定のライセンス登録(SLR)からのアップグレード
- トラブルシューティング
  - インターネットアクセス、ポートチェック、Ping
  - Syslog
  - パケット キャプチャ
  - show コマンド
  - デバッグ/btrace
- 一般的な問題
  - WLCにインターネットアクセスがない、またはファイアウォールがトラフィックをブロック/変更する
  - パケットキャプチャの不明なCAアラート
- 関連情報

はじめに

このドキュメントでは、Catalyst 9800 WLCでポリシー(SLUP)を使用してスマートライセンス(SLUP)を設定およびトラブルシューティングする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ポリシーを使用したスマートライセンス(SLUP)
- Catalyst 9800ワイヤレスLANコントローラ(WLC)

- シスコネットワーキングサブスクリプション

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

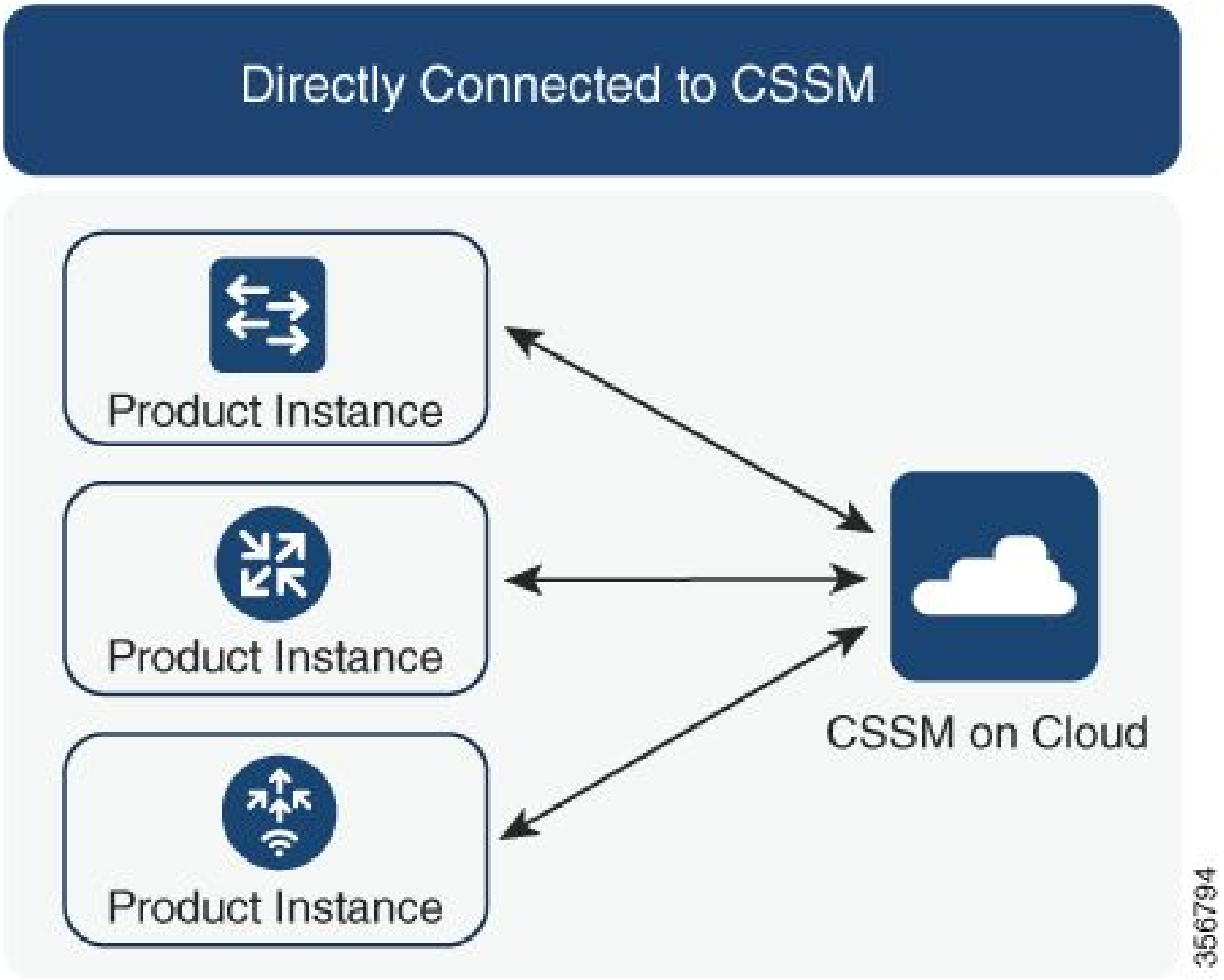
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

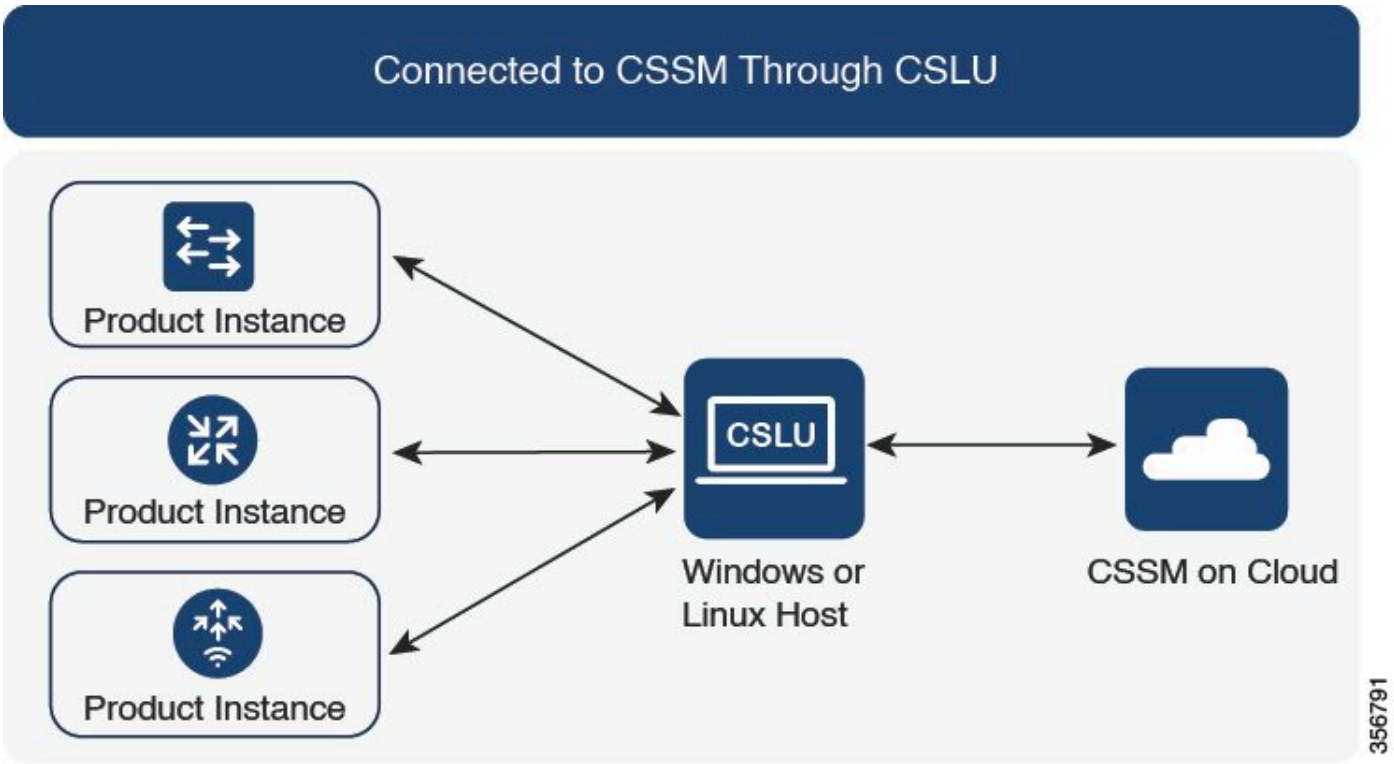
注意：この記事の注意事項には、このドキュメントで取り上げられていない役立つ情報や参照資料が記載されています。各注を読むことをお勧めします。

1. Cisco Smart Software Manager Cloud(CSSM Cloud)への直接接続
2. CSLU(Cisco Smart License Utility Manager)経由でCSSMに接続
3. オンプレミスのSmart Software Manager(SSM)経由でCSSMに接続（オンプレミスSSM）

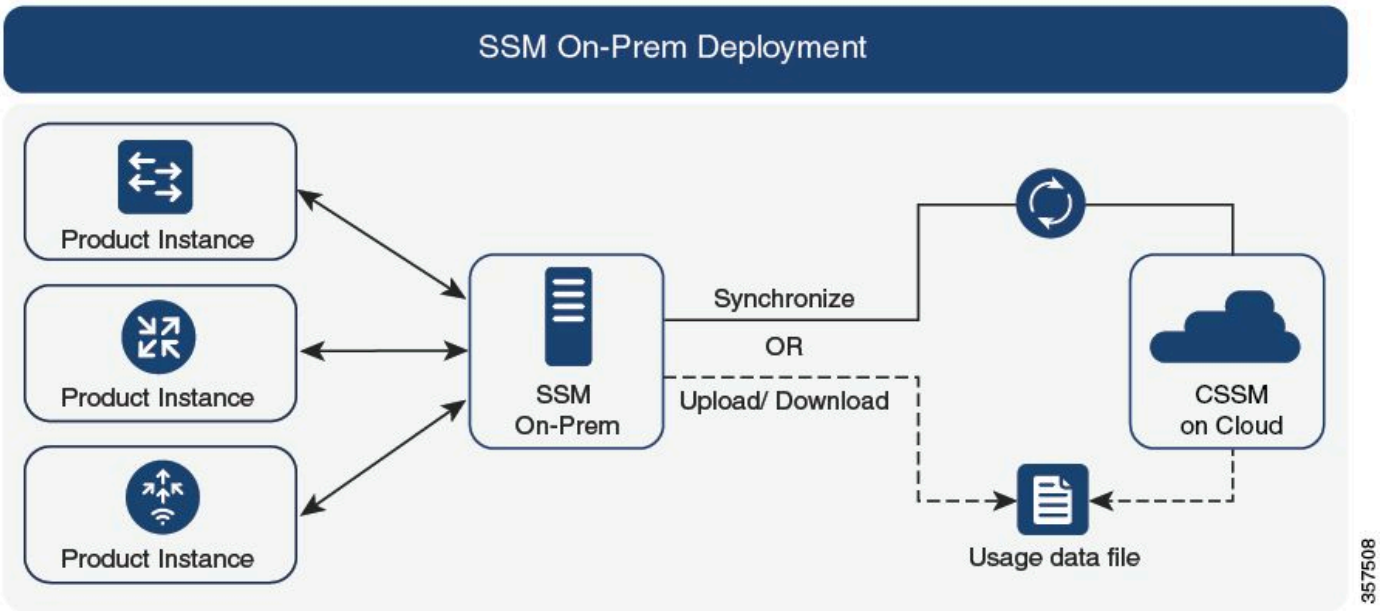
この記事では、Catalyst 9800のすべてのスマートライセンスのシナリオについて説明しているわけではありません。詳細については、『ポリシー設定を使用したスマートライセンスの設定ガイド』を参照してください。ただし、この記事では、Catalyst 9800でのポリシーの問題を使用した直接接続、CSLU、およびオンプレミスSSMスマートライセンスのトラブルシューティングに役立つ一連のコマンドについて説明します。



オプション 1Cisco Smart Licensing Cloud Server(CSSM)への直接接続



オプション 2CSLU経由の接続



オプション 3オンプレミスのSmart Software Manager（オンプレミスSSM）経由の接続

注：この記事に記載されているすべてのコマンドは、バージョン17.3.2以降を実行するWLCにのみ適用できます。

Unified Licensing、Enforcement、およびSLUP

シスコネットワーキングサブスクリプションで利用できるUnified Licensingは、オンプレミスのお客様にライセンスを適用します。

- IOS XE 17.15.2（2024年12月）は、統合ライセンスで最初にサポートされたリリースで、デバイス単位のライセンスレポートとコンプライアンスステータスが導入されました。
- 将来のIOS XEリリースでは、ライセンス不要のAPに対してはDay 0が、ライセンス期限切れのデバイスに対してはDay Nが適用されます。コンプライアンス違反のデバイスでは、ソフトウェアイメージが更新されたときに適用されます。

デバイスがIOS XEソフトウェアイメージのアップグレード時に強制の対象とならないように、このガイドの手順を完了することは、デバイスがSLUPを使用して正しく構成されていることを確認するために重要です。

Unified LicensingでのAPコンプライアンスの確認

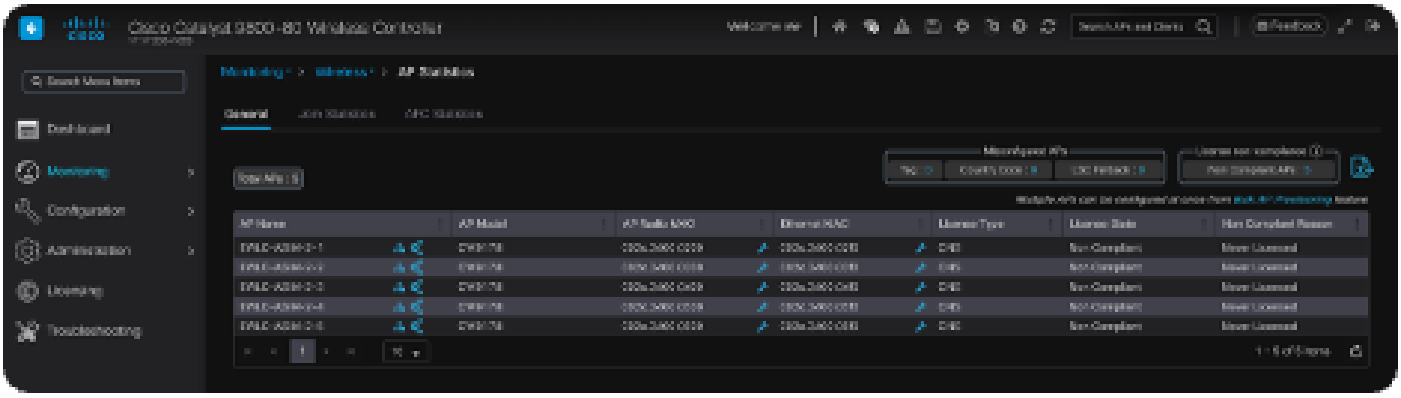


図1:Web UI AP準拠（非準拠）

APコンプライアンス情報は、コントローラ（Merakiダッシュボード、Catalyst Center 2.3.7.9）およびデバイス(Web UI、CLI)で入手できます。

図1は、Web UI上のAPコンプライアンス情報の例を示しています。コンプライアンスに違反しているAPには、非準拠のライセンス状態があり、そのAPに「ライセンスがない」という推論が与えられます。

SLUPが正しく設定されると、APは更新された準拠ステータスを反映します。

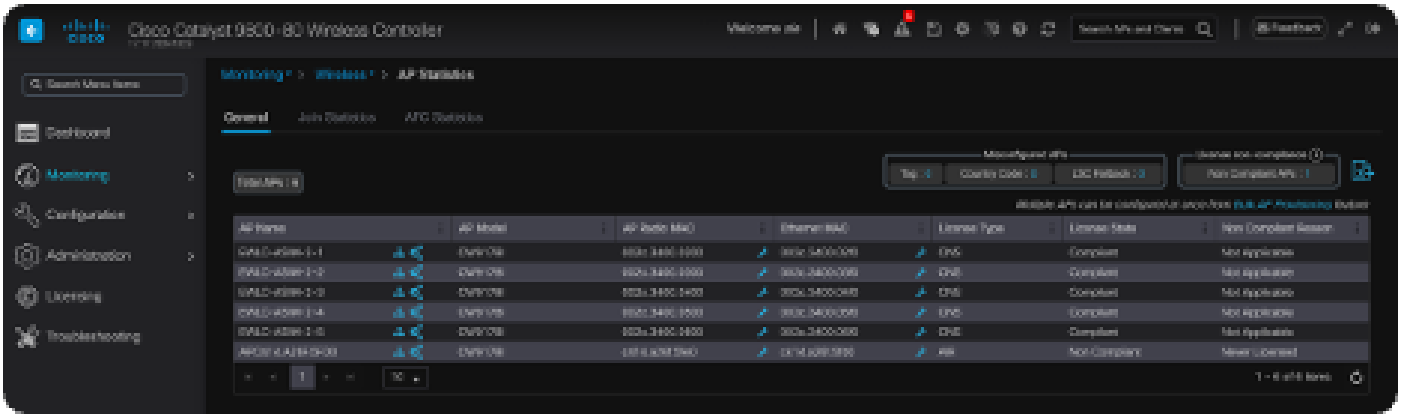


図1:Web UI AP準拠（準拠）

注： SLUPを正常に設定してもアクセスポイントで非準拠のステータスが表示される場合は、十分なライセンスを購入していること、およびそれらのライセンスが正しいスマートアカウント

(SA)とバーチャルアカウント(VA)に預けられていることを確認してください。

従来のライセンスとSLUP

ポリシーを使用したスマートライセンス機能は、コードバージョン17.3.2でCatalyst 9800に導入されました。最初の17.3.2リリースでは、17.3.3リリースで導入されたWLC WebUIのSLUP設定メニューが表示されません。SLUPは、いくつかの点で従来のスマートライセンスと異なります。

- WLCは、smartreceiver.cisco.comドメインではなく、tools.cisco.comドメインを介してCSSMと通信します。
- 登録する代わりに、WLCはCSSMまたはオンプレミスSSMとの信頼を確立します。
- CLIコマンドは若干変更されています。
- Smart Licensing Reservation(SLR)は、もはや存在しません。代わりに、使用状況を手動で定期的にレポートできます。

警告: Cisco Catalyst 9800-CLワイヤレスコントローラを使用している場合は、Cisco

IOS® XE Cuppertino 17.7.1以降の必須のACK要件を十分に理解してください。「Cisco Catalyst 9800-CLワイヤレスコントローラのRUMレポートおよび確認要件」を参照してください。

コンフィギュレーション

直接接続CSSM

CSSMでトークンが作成されたら、信頼を確立するために次のコマンドを実行する必要があります。

注：Token Max.HA SSOのWLCの場合、使用数は2以上である必要があります。

```
configure terminal
ip http client source-interface



ip http client secure-trustpoint



license smart transport smart
license smart url default
exit
write memory
terminal monitor
license smart trust idtoken


          all force
```

- ip http client source-interfaceコマンドでは、ライセンス関連パケットの送信元となるL3インターフェイスを指定します
- ip http client secure-trustpointコマンドは、CSSM通信に使用するトラストポイント/証明書を指定します。トラストポイント名は、show crypto pki trustpointsコマンドを使用して確認できます。自己署名証明書TP-self-signed-xxxxxxxxxx証明書または製造元でインストールされる証明書（MICとも呼ばれ、9800-40、9800-80、および9800-Lでのみ使用可能）を使用することをお勧めします。通常はCISCO_IDEVID_SUDIと呼ばれます。

- terminal monitorコマンドは、WLCにログをコンソールに出力させ、信頼が正常に確立されたことを確認できるようにします。terminal no monitorを使用して無効にできます。
- 最後のコマンドのキーワードallは、HA SSOクラスタ内のすべてのWLCに対して、CSSMとの信頼を確立するように指示します。
- キーワードforceを指定すると、WLCは以前に確立された信頼のいずれかを上書きし、新しい信頼を試行します。

注：信頼が確立されていない場合、9800はコマンドの実行後1分後に再試行し、その後しばらく再試行しません。新しい信頼確立を強制するには、再度tokenコマンドを入力します。

CSLUに接続

Cisco Smart License Utility Manager(CSLU):Windowsベースのアプリケーション（Linuxでも使用可能）です。このアプリケーションを使用すると、お客様は、ライセンスとそれに関連付けられている製品インスタンスを各自の構内から管理できます。スマートライセンス対応の製品インスタンスをCisco Smart Software Manager(CSSM)に直接接続する必要はありません。

このセクションでは、9800ワイヤレス設定のみを取り上げます。CSLUを使用してライセンスを設定するために実行する手順は他にもあります（CSLUのインストール、CSLUソフトウェアの設定など）。これについては設定ガイドで説明しています。製品のインスタンス開始による通信方法とCSLU開始による通信方法のどちらを実装するか、または対応する一連のタスクを実行するか。

製品インスタンス起動

1. コントローラからCSLUへのネットワークの到達可能性を確認する
2. トランスポートタイプがcsluに設定されていることを確認します。

```
(config)#license smart transport cslu
(config)#exit
#copy running-config startup-config
```

3. コントローラでCSLUを検出する場合は、次の操作を実行する必要があります。DNSを使用してCSLUを検出する場合は、何もする必要はありません。URLを使用して検出する場合は、次のコマンドを入力します。

```
(config)#license smart url cslu http://

          :8182/cslu/v1/pi
(config)#exit
#copy running-config startup-config
```

CSLU開始

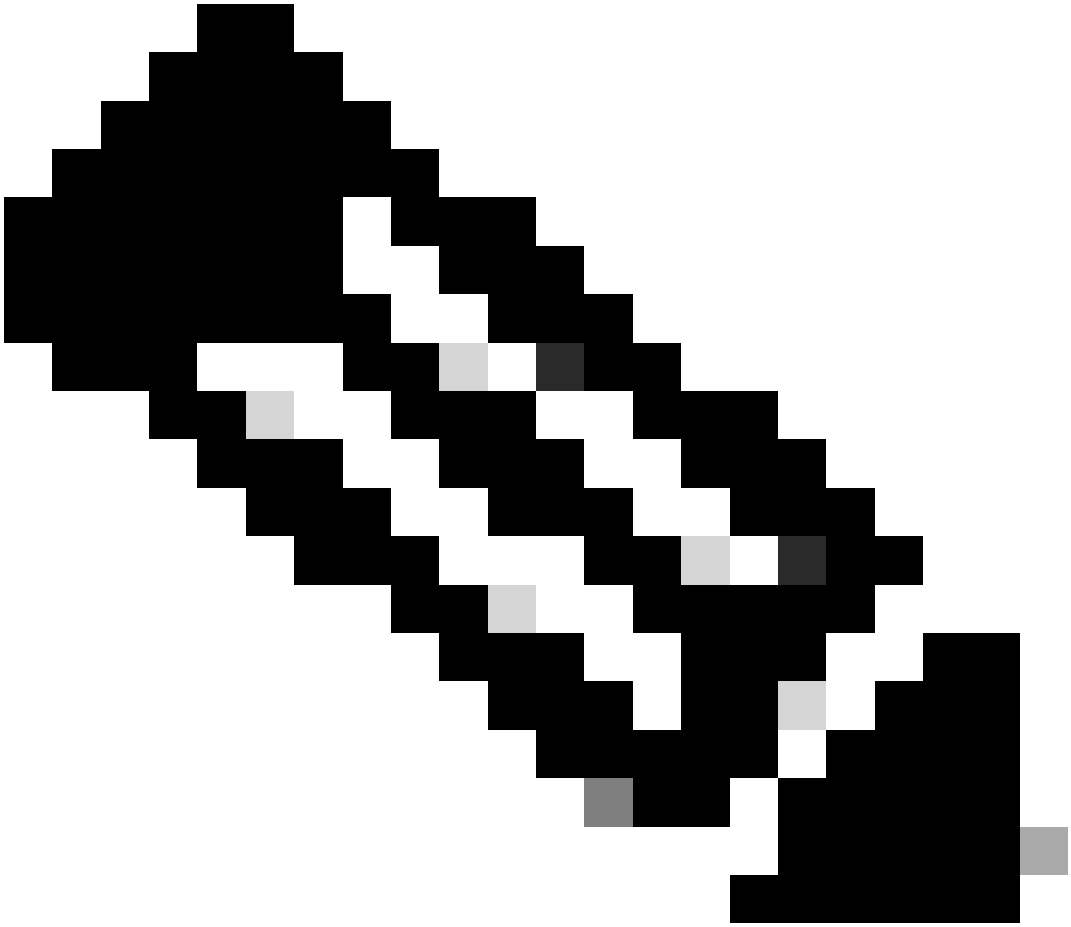
CSLUが開始する通信を設定する場合に必要な唯一のアクションは、コントローラからCSLUへのネットワーク到達可能性を確認し、確認することです。

オンプレミスのSSMに接続

オンプレミスSSMでの設定は、直接接続に非常によく似ています。オンプレミスでは、バージョン8-202102以降を実行する必要があります。SLUPリリース（17.3.2以降）では、CSLU URLとトランスポートタイプを使用することを推奨します。URLは、オンプレミスWebUIインターフェイスの**Smart Licensing > Inventory > <Virtual Account> > General**セクションから取得できます。

```
configure terminal
 ip http client source-interface




 ip http client secure-trustpoint




 license smart transport cslu
 license smart url cslu http://



         /cslu/v1/pi/



           (see previous paragraph on how to get exact URL)
 crypto pki trustpoint SLA-TrustPoint
  revocation-check none
 exit
write memory
terminal monitor
```

オンプレミスSSMでは、信頼トークンを使用する必要はありません。



注:「%PKI-3-CRL_FETCH_FAIL: CRL fetch for trustpoint SLA-TrustPoint failed」というメッセージが表示される場合、SLA-TrustPointでrevocation-check noneを設定していないことが原因です。これは、スマートライセンスに使用されるトラストポイントです。オンプレミスの場合、ライセンスサーバー上の証明書は、ほとんどの場合、CRL検証が不可能な自己署名証明書です。したがって、失効チェックを構成する必要はありません。

HTTPSプロキシによるスマートトランスポートの設定

注:認証済みプロキシは、コードリリース17.9.2ではまだサポートされていません。インフラストラクチャで認証済みプロキシを使用している場合は、Cisco Smart License Utility Manager(CSLU)の使用を検討してください。このマネージャは、このタイプのサーバをサポートします。

スマートトランスポートモードの使用時にプロキシサーバを使用してCSSMと通信するには、次の手順を実行します。

```
configure terminal
  ip http client source-interface



  ip http client secure-trustpoint
```

```
  license smart transport smart
  license smart url default
  license smart proxy address




  license smart proxy port




exit
write memory
terminal monitor
license smart trust idtoken



            all force
```

通信周波数

CLIまたはGUIで設定できるレポート間隔は影響しません。

9800 WLCは、WebインターフェイスまたはCLIを使用してどのレポーティングインターバルが設定されていても、CSSMまたはオンプレミスのSmart Software Manager(SSM)と8時間ごとに通信します。つまり、新しく加入したアクセスポイントは、最初に加入してから最大8時間後までCSSMに表示されます。

次回ライセンスが計算されて報告されるタイミングは、show license air entities summaryコマンドで確認できます。このコマンドは、一般的なshow techまたはshow license allの出力には含まれていません。

<#root>

WLC#

```
show license air entities summary


Last license report time.......................: 07:38:15.237 UTC Fri Aug 27 2021
Upcoming license report time...................: 15:38:15.972 UTC Fri Aug 27 2021
```

```
No. of APs active at last report................: 3
No. of APs newly added with last report.........: 0
No. of APs deleted with last report.............: 0
```

ライセンスの初期設定へのリセット

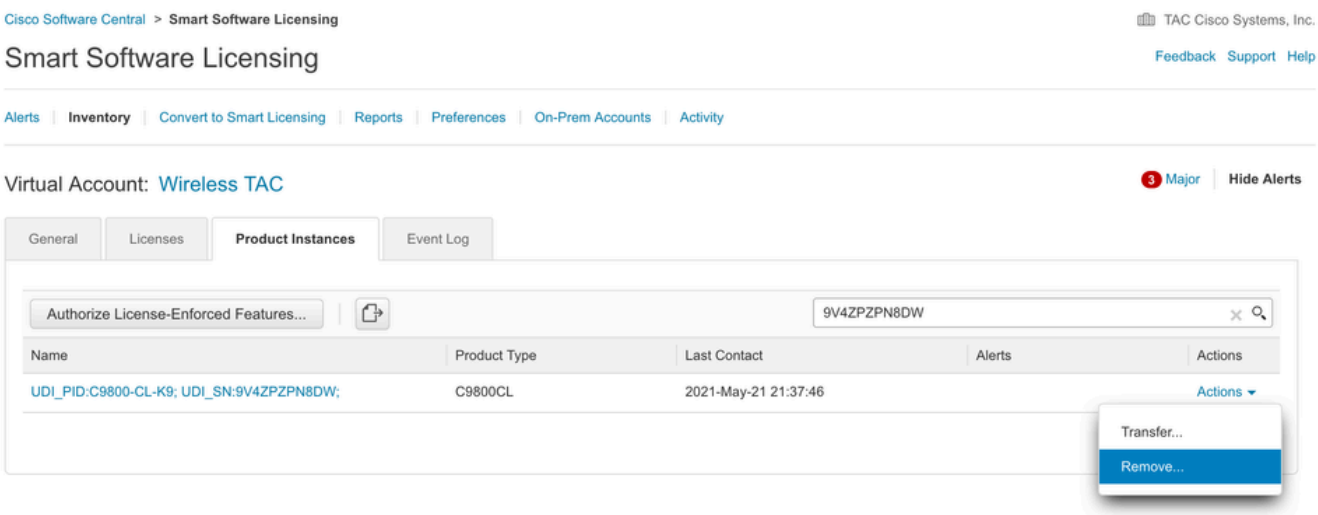
Catalyst 9800 WLCでは、すべてのライセンス設定とtrust factoryによるリセットを使用でき、その他の設定は保持できます。これにはWLCのリロードが必要です。

```
WLC-1#license smart factory reset
%Warning: reload required after "license smart factory reset" command
```

ライセンスを工場出荷時状態にリセットした後、AirGapモードの場合は、WLCのライセンスを再度取得する前に1時間待機する必要があることに注意してください。

RMAまたはハードウェア交換の場合

9800 WLCを交換する必要がある場合、新しいデバイスはCSSM/オンプレミスSmart Software Manager(SSM)に登録する必要があり、新しいデバイスとして認識されます。以前のデバイスのライセンス数をリリースするには、「製品インスタンス」で手動で削除する必要があります。



特定のライセンス登録(SLR)からのアップグレード

17.3.2よりも前の古いWLCリリースでは、Specific License Registration(SLR)と呼ばれる特別なオフラインライセンス方式が使用されていました。 このライセンス方式は、SLUP（17.3.2以降）を使用するリリースでは廃止されています。

SLRを使用していた9800コントローラをリリース17.3.2または17.4.1以降にアップグレードする場合は、SLRコマンドに依存するのではなく、オフラインSLUPレポートに移行することをお勧めします。ライセンスの使用状況RUMファイルを保存し、スマートライセンスポータルに登録しま

す。新しいリリースではSLRが存在しなくなったため、正しいライセンス数が報告され、未使用のライセンスが解放されます。ライセンスはブロックされなくなりましたが、正確な使用回数がレポートされます。

トラブルシューティング

インターネットアクセス、ポートチェック、Ping

従来のスマートライセンスが使用していたtools.cisco.comの代わりに、新しいSLUPはsmartreceiver.cisco.comドメインを使用して信頼を確立します。この記事を書いている時点で、このドメインは複数の異なるIPアドレスに解決されます。すべてのアドレスにpingが通るわけではありません。pingは、WLCからのインターネット到達可能性テストとして使用しないでください。これらのサーバに対してpingを実行できないからといって、サーバが正常に動作していないということにはなりません。

pingの代わりに、到達可能性テストとしてポート443経由のtelnetを使用する必要があります。Telnetは、smartreceiver.cisco.comドメインに対してチェックすることも、サーバのIPアドレスに対して直接チェックすることもできます。トラフィックがブロックされていない場合、ポートは出力でオープンとして表示される必要があります。

```
WLC-1#telnet smartreceiver.cisco.com 443
Trying smartreceiver.cisco.com (192.330.220.90, 443)... Open <-------
[Connection to 192.330.220.90 closed by foreign host]
```

Syslog

トークンの設定中にterminal monitorコマンドを有効にすると、WLCはCLIで関連ログを出力します。これらのメッセージは、show loggingコマンドを実行して取得することもできます。信頼が正常に確立された場合のログは次のようになります。

```
WLC-1#license smart trust idtoken <token> all force
Aug 22 12:13:08.425: %CRYPTO_ENGINE-5-KEY_DELETED: A key named SLA-KeyPair has been removed from key st
Aug 22 12:13:08.952: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named SLA-KeyPair has been generated or impor
Aug 22 12:13:08.975: %PKI-6-CONFIGAUTOSAVE: Running configuration saved to NVRAM
Aug 22 12:13:11.879: %SMART_LIC-6-TRUST_INSTALL_SUCCESS: A new licensing trust code was successfully in
```

DNSサーバが定義されていない、または機能していないDNSサーバがあるWLCのログ：

```
Aug 23 09:19:43.486: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart Software Man
```

この場合は、有効なDNSサーバが設定されていることを確認します。使用可能な任意のパブリックDNSサーバIPを自由に使用できます。

```
ip name-server
```

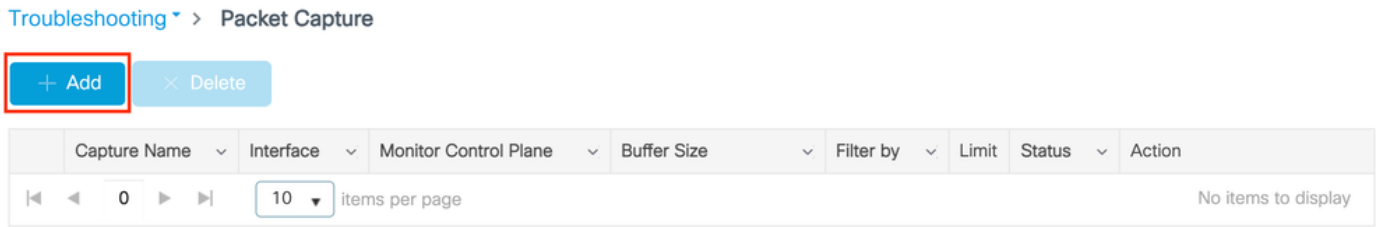
DNSサーバは機能しているが、インターネットにアクセスできないWLCのログ：

```
Aug 23 09:23:30.701: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart Software Man
```

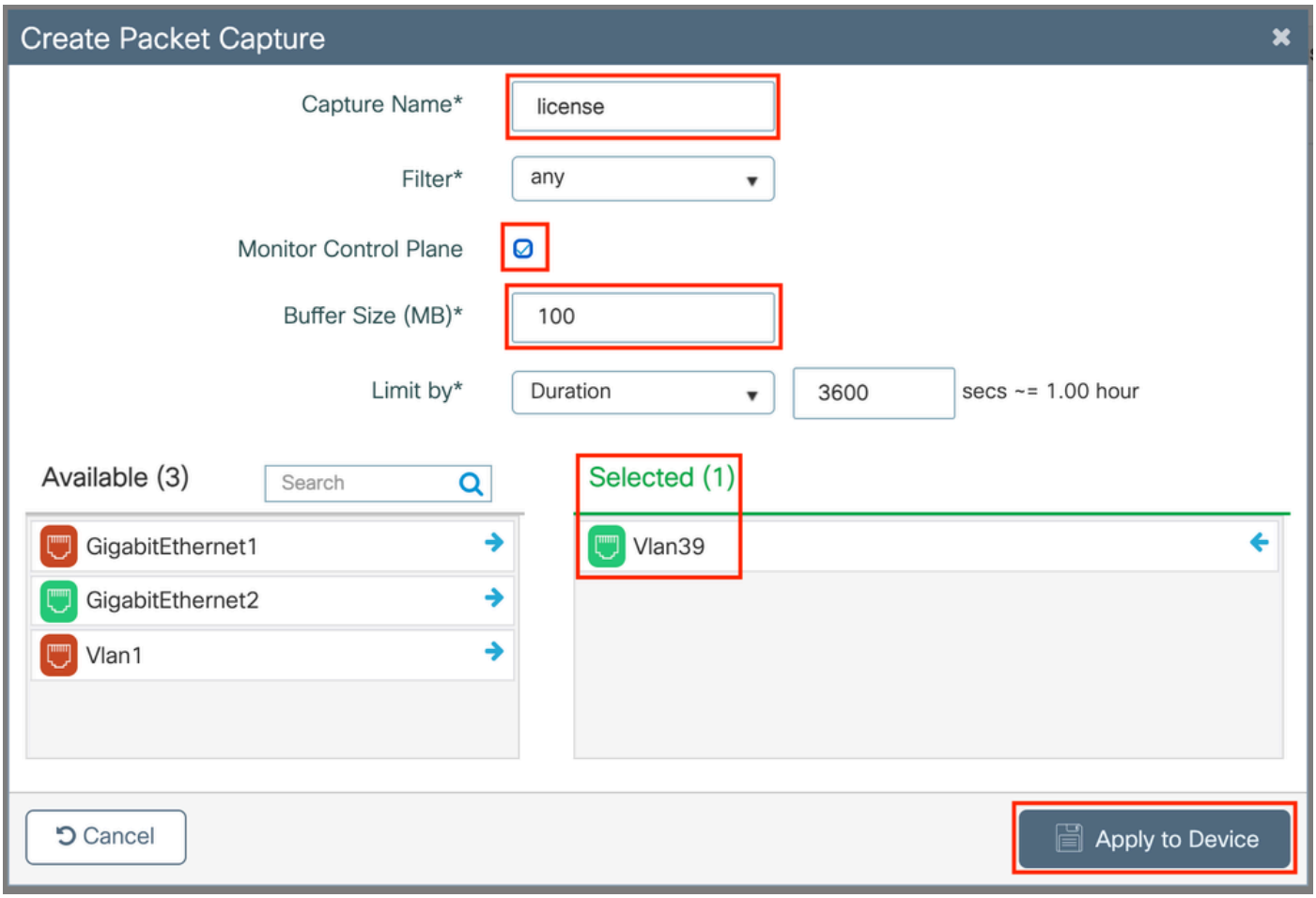
パケット キャプチャ

WLCとCSSM/オンプレミスSSM間の通信は暗号化され、HTTPSを経由しますが、パケットキャプチャを実行すると、信頼が確立されない原因が明らかになります。パケットキャプチャを収集する最も簡単な方法は、WLC Webインターフェイスを使用する方法です。

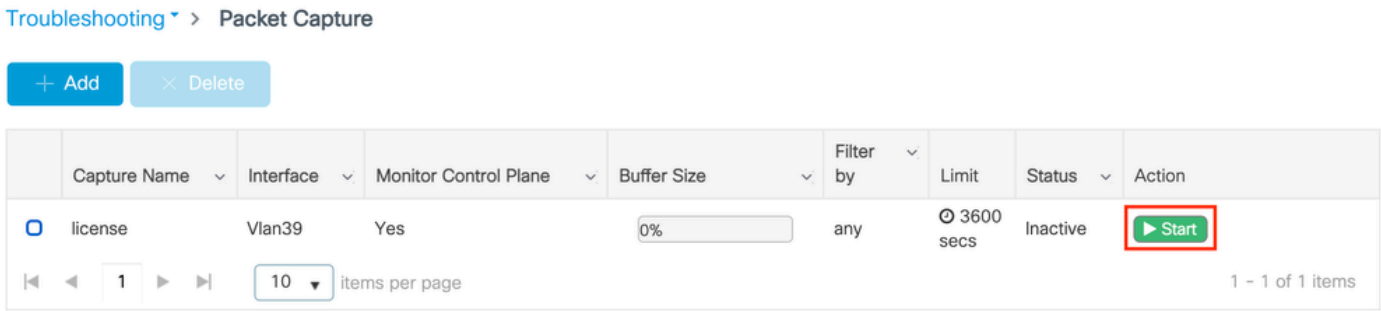
Troubleshooting > Packet Captureの順に移動します。新しいキャプチャポイントを作成します。



Monitor Control Planeチェックボックスが有効になっていることを確認します。バッファサイズを最大100 MBに増やします。キャプチャするインターフェイスを追加します。スマートライセンストラフィックは、デフォルトではワイヤレス管理インターフェイスから、またはip http client source-interfaceコマンドで定義されたインターフェイスから、送信されます。



キャプチャを開始し、license smart trust idtoken <token> all forceコマンドを実行します。



信頼確立のパケットキャプチャには、次の手順を含める必要があります。

1. SYN、SYN-ACK、およびACKシーケンスを使用したTCPセッションの確立
2. サーバとクライアントの両方の証明書交換によるTLSセッションの確立確立は、新しいセッションチケットパケットで終了します
3. WLCがライセンス使用状況をレポートする暗号化パケット交換(アプリケーションデータフレーム)
4. FIN-PSH-ACK、FIN-ACK、およびACKシーケンスによるTCPセッションの終了

注：パケットキャプチャには、TCPウィンドウ更新フレームとアプリケーションデータフレームの倍数を含む、さらに多くのフレームが含まれています

CSSMクラウドは3つの異なるパブリックIPアドレスを使用するため、WLCとCSSM間のすべてのパケットキャプチャをフィルタリングするには、次のWiresharkフィルタを使用します。

```
ip.addr==172.163.15.144 or ip.addr==192.168.220.90 or ip.addr==172.163.15.144
```

オンプレミスSSMを使用している場合は、SSMのIPアドレスをフィルタリングします。

```
ip.addr==
```

例：フィルタリングされたすべての重要なパケットキャプチャを使用して、直接接続されたCSSMを使用した、正常な信頼確立のパケットキャプチャ。

No.	Arrival Time	Source	Destination	Protocol	Info
559	Aug 23, 2021 11:31:13.35…	192.168.10.150	192.133.220.90	TCP	22425 → 443 [SYN] Seq=0 Win=4128 Len=0 MSS=536
576	Aug 23, 2021 11:31:13.46…	192.133.220.90	192.168.10.150	TCP	443 → 22425 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1390
578	Aug 23, 2021 11:31:13.46…	192.168.10.150	192.133.220.90	TCP	22425 → 443 [ACK] Seq=1 Ack=1 Win=4128 Len=0
580	Aug 23, 2021 11:31:13.46…	192.168.10.150	192.133.220.90	TLSv1.2	Client Hello
608	Aug 23, 2021 11:31:13.58…	192.133.220.90	192.168.10.150	TLSv1.2	Server Hello
612	Aug 23, 2021 11:31:13.58…	192.168.10.150	192.133.220.90	TCP	[TCP Window Update] 22425 → 443 [ACK] Seq=168 Ack=537 Win=4128 Len=0
614	Aug 23, 2021 11:31:13.58…	192.133.220.90	192.168.10.150	TCP	443 → 22425 [ACK] Seq=537 Ack=168 Win=31953 Len=536 [TCP segment of a reassembled PDU]
673	Aug 23, 2021 11:31:13.70…	192.133.220.90	192.168.10.150	TLSv1.2	Certificate [TCP segment of a reassembled PDU]
675	Aug 23, 2021 11:31:13.70…	192.133.220.90	192.168.10.150	TLSv1.2	Server Key Exchange [TCP segment of a reassembled PDU]
695	Aug 23, 2021 11:31:13.71…	192.133.220.90	192.168.10.150	TLSv1.2	Certificate Request, Server Hello Done
711	Aug 23, 2021 11:31:13.85…	192.168.10.150	192.133.220.90	TLSv1.2	Certificate, Client Key Exchange
718	Aug 23, 2021 11:31:14.01…	192.168.10.150	192.133.220.90	TLSv1.2	Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
737	Aug 23, 2021 11:31:14.13…	192.133.220.90	192.168.10.150	TLSv1.2	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
745	Aug 23, 2021 11:31:14.13…	192.168.10.150	192.133.220.90	TLSv1.2	Application Data
747	Aug 23, 2021 11:31:14.13…	192.168.10.150	192.133.220.90	TLSv1.2	Application Data
749	Aug 23, 2021 11:31:14.13…	192.168.10.150	192.133.220.90	TLSv1.2	Application Data, Application Data
22…	Aug 23, 2021 11:31:45.00…	192.168.10.150	192.133.220.90	TCP	22425 → 443 [FIN, PSH, ACK] Seq=4306 Ack=9738 Win=3625 Len=0
22…	Aug 23, 2021 11:31:45.11…	192.133.220.90	192.168.10.150	TCP	443 → 22425 [FIN, ACK] Seq=9738 Ack=4307 Win=31250 Len=0
22…	Aug 23, 2021 11:31:45.11…	192.168.10.150	192.133.220.90	TCP	22425 → 443 [ACK] Seq=4307 Ack=9739 Win=3625 Len=0

show コマンド

次のshowコマンドには、信頼の確立に関する有用な情報が含まれています。

```
show license status
show license summary
show tech-support license
show license tech-support
show license air entities summary

show license history message (useful to see the history and content of messages sent to SL)

show tech wireless (actually gets show log and show run on top of the rest which can be useful)
```

show license history messageコマンドは、WLCから送信されCSSMから受信した実際のメッセージを表示できるため、より便利なコマンドの1つです。

信頼が正常に確立されると、「REQUEST: Aug 23 10:18:08 2021 Central」と「RESPONSE:

Aug 23 10:18:10 2021 Central」の両方のメッセージが表示されます。RESPONSE行の後に何もない場合は、WLCがCSSMから応答を受信しなかったことを意味します。

次に、信頼が確立された場合のshow license historyメッセージの出力例を示します。


```
REQUEST: Aug 23 10:18:08 2021 Central
{"request":"{\"header\":{\"request_type\":\"POLL_REQ\",\"sudi\":{\"udi_pid\":\"C9800-CL-K9\",\"udi_seri
NB\"},\"version\":\"1.3\",\"locale\":\"en_US.UTF-8\",\"signing_cert_serial_number\":\"3\",\"id_cert_ser
\",\"product_instance_identifier\":\"\",\"connect_info\":{\"name\":\"C_agent\",\"version\":\"5.0.9_rel/
e,\"additional_info\":\"\",\"capabilities\":[\"UTILITY\",\"DLC\",\"AppHA\",\"MULTITIER\",\"EXPORT_2\",\
Y_USAGE\"]}},\"request_data\":\"{\\\"sudi\\\":{\\\"udi_pid\\\":\\\"C9800-CL-K9\\\",\\\"udi_serial_numbe
\"},\\\"timestamp\\\":1629713888600,\\\"nonce\\\":\\\"11702702165338740293\\\",\\\"product_instance_ide
\"original_request_type\\\":\\\"LICENSE_USAGE\\\",\\\"original_piid\\\":\\\"2e84a42f-c903-44c5-83b2-e62
":7898262236}\"}","signature":{"type":"SHA256","key":"59152896","value":"eiJ7IuQaTCFxgUkwls76WZxa5DRI5A
OgMqQd5POU6VNsH2j9dHco4T1NJ/aCMbR1MRmkfxyVSWsx4lmjJL1lmpOSi3ZS4FBMvlF/EBOUfowREe2oz2lrQp1cAFpPn5SlaFezW
/Nu6SQZfIW+IdF+2qnJeNFAIZbNpgOB5d5HIJvDmDImvDu3bMRHhQAWr2KKzGFr6jPzOhs7bGY/+FlfTLQk5LFEUaKTNH/tuxJPFHlF
h9//uhsd+NaQyfdRFludkbfUBTFkvPxHW9/5w=="}}
```

```
  RESPONSE: Aug 23 10:18:10 2021 Central
{"signature":{"type":"SHA256","value":"TXZE034fqAul2jy9V4+HoB2hDShl9au/5sgodiCVatmu671/6MyN7kZfEzREufY8
SLrjTfO4grGeQTcH7yEj0D+gztWXCOu8RBT7/Bo9aBs\n4x1iOE6flPB3BP6yu7KIEUQZ8yHzlwDT+mVtJGi6TRrtYnV3KQMpCUmF5F
wOksf3SfXreNZJuzWXzjHvtmlusCQXw7ZTBzffYsNKOOlkJlr\nvgB2PkV7JUlsA481kpIvlPul6IiJXqk+2PC2IzCrCLG57lVN3XgX
1pEl2SHyQ/DAw==","piid":null,"cert_sn":null},"response":"{\"header\":{\"version\":\"1.3\",\"locale\":\"
mp\":1629713890172,\"nonce\":null,\"request_type\":\"POLL_REQ\",\"sudi\":{\"udi_pid\":\"C9800-CL-K9\",\
9PJK8D7OCNB\"},\"agent_actions\":null,\"connect_info\":{\"name\":\"SSM\",\"version\":\"1.3\",\"producti
s\":[\"DLC\",\"AppHA\",\"EXPORT_2\",\"POLICY_USAGE\",\"UTILITY\"],\"additional_info\":\"\"},\"signing_c
\",\"id_cert_serial_number\":\"59152896\",\"product_instance_identifier\":\"\"},\"status_code\":\"FAILE
\"Invalid ProductInstanceIdentifier: 2e84a42f-c903-44c5-83b2-e62e258c780f provided in the polling reque
262236\",\"retry_time_seconds\":0,\"response_data\":\"\"}","sch_response":null}
```


デバッグ/btrace

license smart trust idtoken all forceコマンドを使用して信頼確立が試行されてから数分後にこのコマンドを実行します。IOSRPログは非常に詳細です。コマンドに| include smart-agent"を追加して、スマートライセンスのログだけを取得します。

```
show logging process iosrp start last 5 minutes
show logging process iosrp start last 5 minutes | include smart-agent
```

また、次のデバッグを実行してから、新しい接続を強制するようにライセンスコマンドを再設定することもできます。

```
debug license events
debug license errors
debug license agent all
```

一般的な問題

WLCにインターネットアクセスがない、またはファイアウォールがトラフィックをブロック/変更する

WLC上の組み込みパケットキャプチャは、WLCがCSSMまたはオンプレミスSSMから何かを受信したかどうかを確認するための簡単な方法です。応答がない場合、ファイアウォールが何かをブロックしている可能性があります。

CSSMクラウドまたはオンプレミスSSMから応答を受信していない場合、show license history messageコマンドでは、要求が送信された後1秒で空の応答が表示されます。

たとえば、空の応答が受信されたと思い込みがちですが、実際には応答が全くありませんでした。

```
REQUEST: Jun 29 11:12:39 2021 CET
{"request":"{\"header\":{\"request_type\":\"ID_TOKEN_TRUST\",\"sudi\":{\"udi_pid\":\"C9800-CL-K9\",\"ud
RESPONSE: Jun 29 11:12:40 2021 CET
```

注：現在、機能拡張要求Cisco Bug ID CSCvy84684（登録ユーザ専用）が存在します。この要求により、応答がない場合にshow license historyメッセージには空の応答が表示されます。これは、show license history messageコマンドの出力を拡張することです

パケットキャプチャの不明なCAアラート

CSSMまたはオンプレミスSSMとの通信には、9800側でまともな証明書が必要です。自己署名できますが、無効または期限切れにすることはできません。この場合、9800 HTTPクライアント証明書の期限が切れたときにCSSMから送信された不明なCAのTLSアラートがパケットキャプチャに表示されます。

スマートライセンスでは、ip http client設定を使用します。これは、WLC Webインターフェイスで使用されるip http serverとは異なります。つまり、次のコマンドを適切に設定する必要があります。

```
ip http client source-interface
```

```
ip http client secure-trustpoint
```

トラストポイント名は、show crypto pki trustpointsコマンドを使用して確認できます。自己署名証明書TP-self-signed-xxxxxxxxxx証明書または製造元でインストールされる証明書(MIC)を使用することをお勧めします。通常はCISCO_IDEVID_SUDIと呼ばれ、9800-80、9800-40、および9800-Lでのみ使用可能です。

提示されるHTTPS証明書はシスコライセンスサーバ証明書ではなくファイアウォール証明書であるため、SSL復号化機能を備えたファイアウォールなどのTLS代行受信を実行するデバイスは、C9800がシスコライセンスサーバとの正常なハンドシェイクを確立することを妨げる可能性があることに注意してください。

注：source-interfaceコマンドとsecure-trustpointコマンドの両方が設定されていることを確認してください。WLCにL3インターフェイスが1つしかない場合でも、source-interfaceコマンドが必要です。

関連情報

- Air Gapモードを使用した9800でのスマートライセンス
- シスコのテクニカルサポートとダウンロード

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。