

& ; の設定SLUPを使用したCatalyst 9800スマートライセンス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](#)

[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ワイヤレスLANコントローラ(WLC)でのポリシー(SLUP)を使用したスマートライセンス(SLUP)の設定とトラブルシューティングの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。

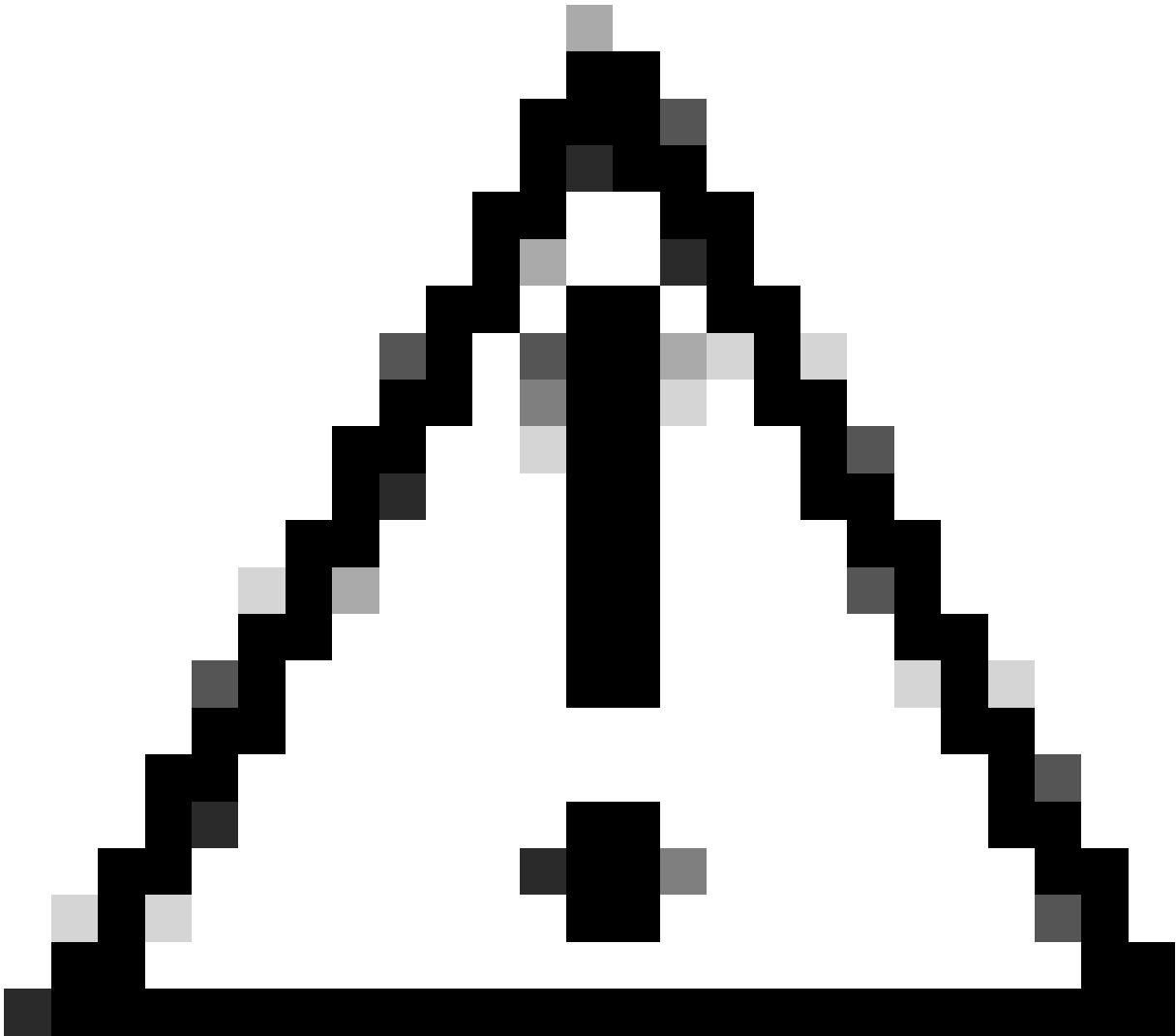
- ポリシーを使用したスマートライセンス(SLUP)
- Catalyst 9800ワイヤレスLANコントローラ(WLC)

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

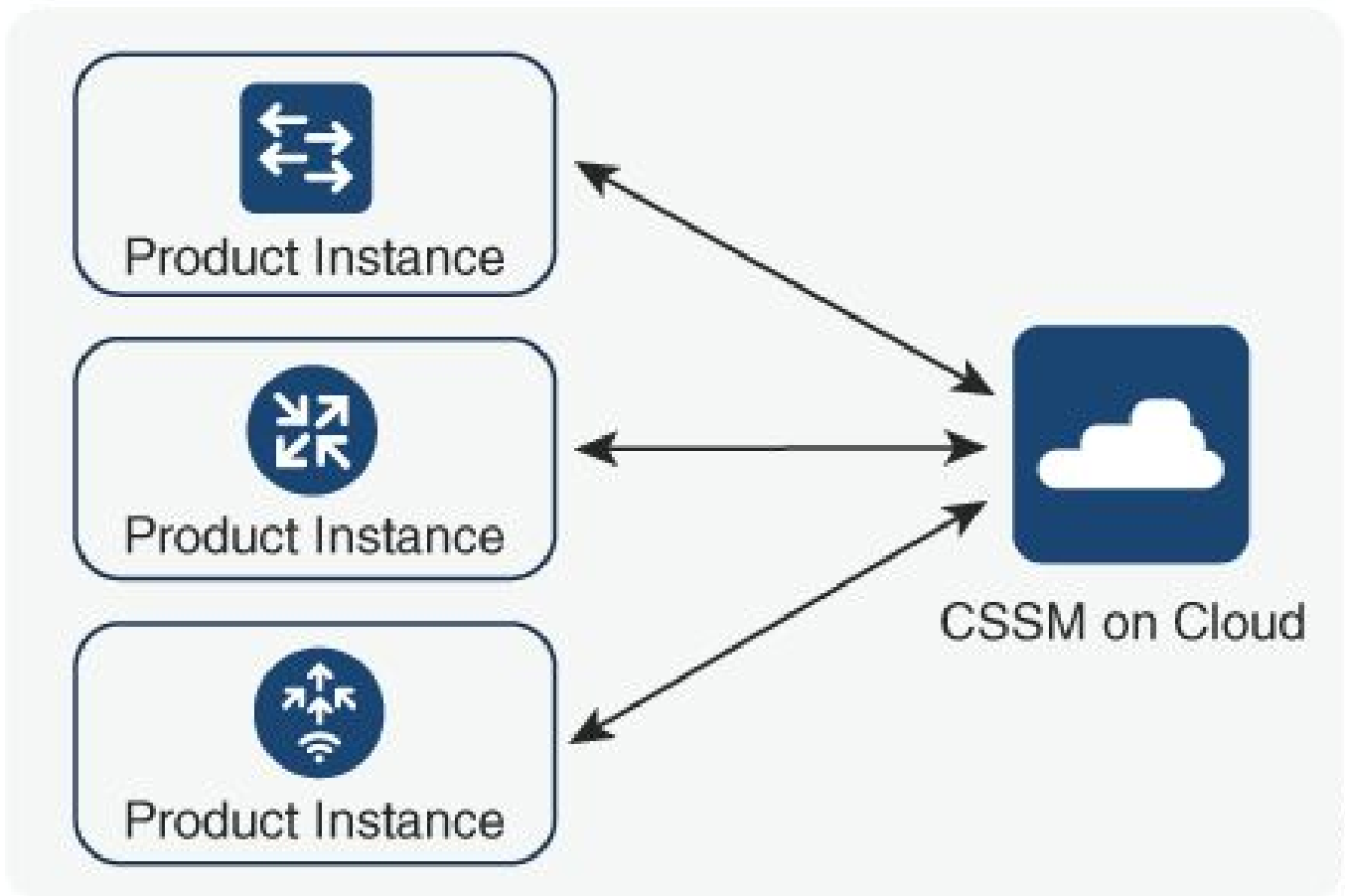


注意：この文書の注意事項には、この文書で説明されていない有用な提案や資料への参照が記載されています。それぞれの注を読むことをお勧めします。

1. [Cisco Smart Software Manager Cloud\(CSSM Cloud\)](#)への直接接続
2. [CSLU](#) (Ciscoスマートライセンスユーティリティマネージャ) 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でのスマートライセンスのシナリオをすべてカバー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](#)』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の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を示します。

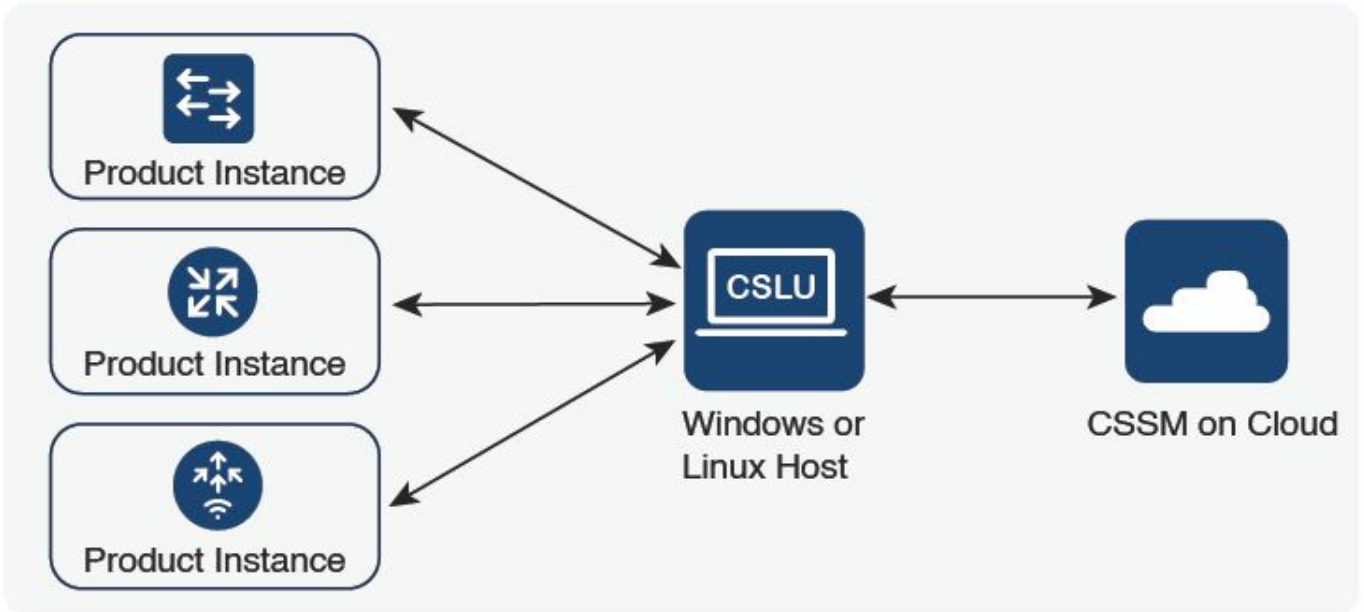
Directly Connected to CSSM



356794

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

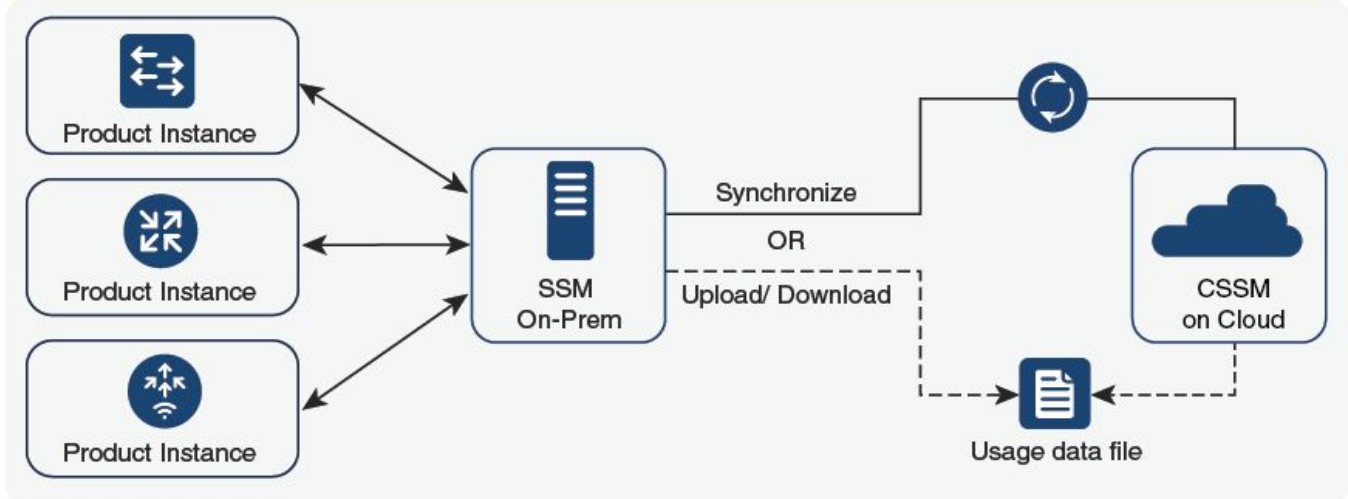
Connected to CSSM Through CSLU



356791


オプション 2 CSLU経由の接続

SSM On-Prem Deployment



357508

オプション 3 オンプレミススマートソフトウェアマネージャ経由の接続 (オンプレミスSSM)

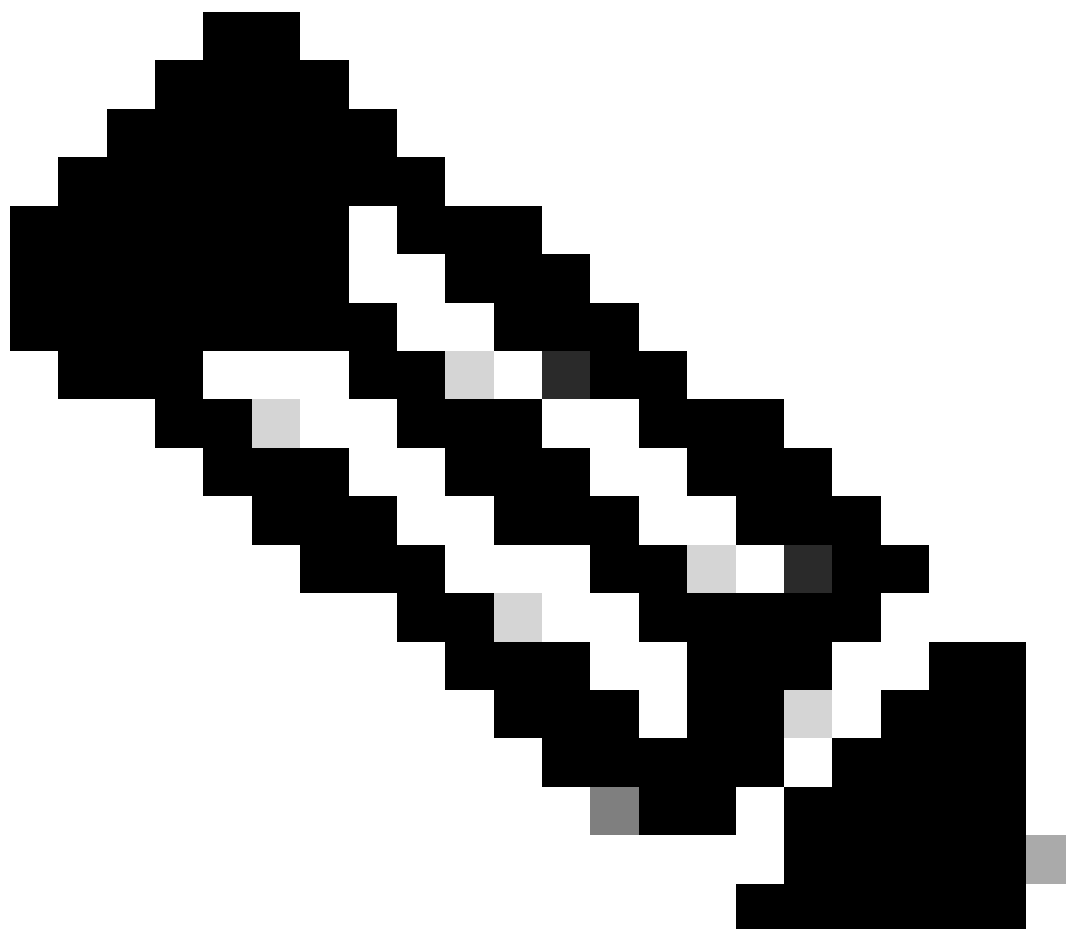
 注：この記事に記載されているすべてのコマンドは、バージョン17.3.2以降を実行するWLCにのみ適用できます。

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。
- CLICOMMANDは若干変更されています。
- スマートライセンス予約(SLR)は廃止されました。代わりに、使用状況を定期的に手動でレポートできます。
- 評価モードはなくなりました。WLCは、ライセンスがなくてもフル機能で機能し続けます。このシステムは自己申告ベースであり、定期的に (エアギャップのあるネットワークの場合は自動または手動で) ライセンスの使用状況をレポートします。




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 Cupertino 17.7.1以降の必須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 Reporting and Acknowledgment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 <interface>
ip http client secure-trustpoint <TP>
license smart transport smart
license smart url default
exit
write memory
terminal monitor
license smart trust idtoken <token> all force
```

- ip http client source-interfaceコマンドでは、ライセンス関連の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コマンドでは、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表示させ、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は、WLCに対して、以前に確立された信頼のいずれかを上書きして、新しい信頼を試行するように指示します。

 注：信頼が確立されていない場合、9800はコマンドが実行されてから1分後に再試行し、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)は、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、ライセンスおよび関連する製品インスタンスを自社で管理できます。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カバーしています。CSLUを使用してライセンスを設定するには他の手順 (CSLUのインストール、CSLUソフトウェアの設定など) も実行します。これについては『[設定ガイド](#)』を参照してください。製品インスタンスから開始する方法とCSLUから開始する方法のいずれの方法を実装するか、または対応する一連のタスクを実行するか、を選択します。

製品インスタンス起動

1. コントローラからCSLUへのネットワーク到達可能性の確認
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://<cslu_ip>:8182/cslu/v1/pi
(config)#exit
#copy running-config startup-config
```

CSLU開始

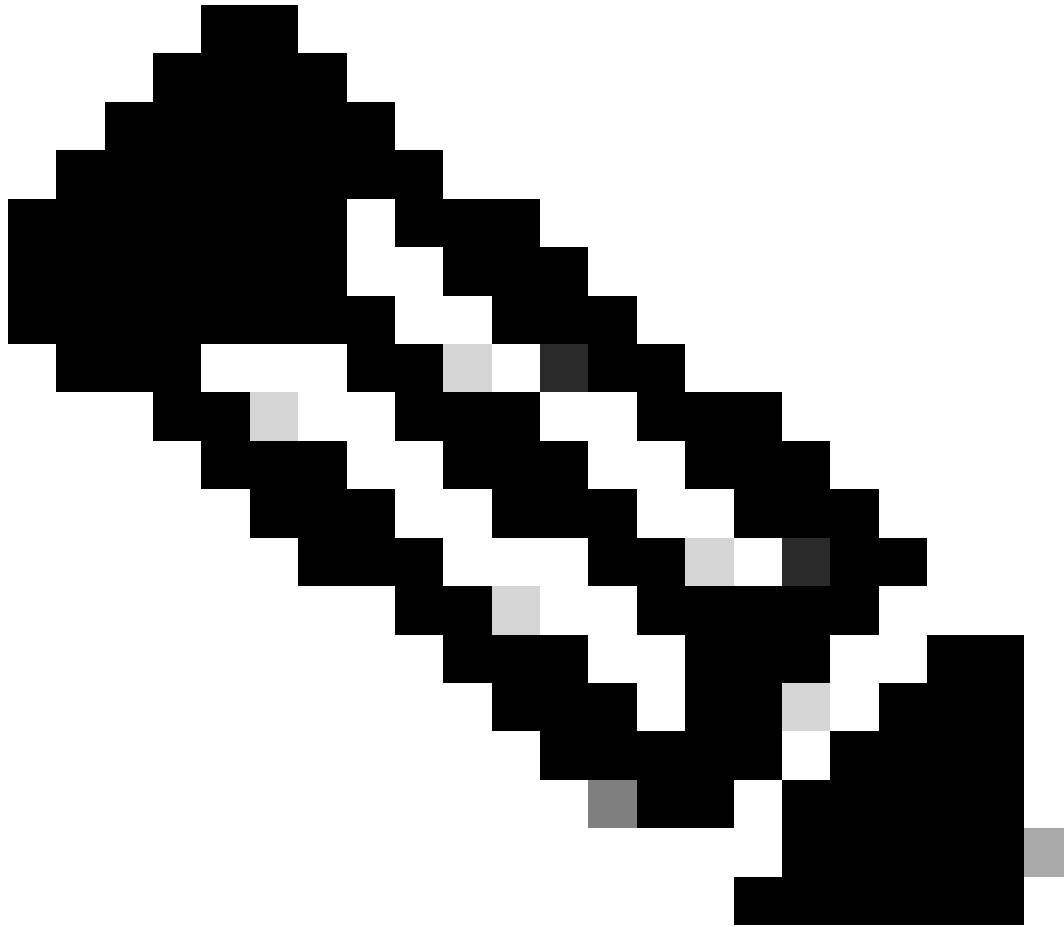
CSLU開始通信を設定する場合、必要な唯一のアクションは、コントローラからCSLUへのネットワーク到達可能性を確認し、確認することです。

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。この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 <interface>
ip http client secure-trustpoint <TP>
license smart transport cslu
license smart url https://<on-prem-ssm-domain>/SmartTransport
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、失効チェックを設定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。CSLU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 <interface>
  ip http client secure-trustpoint <TP>
  license smart transport smart
  license smart url default
  license smart proxy address <proxy ip/fqdn>
  license smart proxy port <proxy port>
exit
write memory
terminal monitor
```

```
license smart trust idtoken <token> 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ト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。

ライセンスが次回計算され、レポートされる時刻は、show license air entities summaryコマンドで表示できます。このコマンドは、一般的なshow techコマンドやshow license allコマンド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されます。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
```

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。

Smart Software Licensing

[Feedback](#) [Support](#) [Help](#)[Alerts](#) | [Inventory](#) | [Convert to Smart Licensing](#) | [Reports](#) | [Preferences](#) | [On-Prem Accounts](#) | [Activity](#)Virtual Account: [Wireless TAC](#)3 Major | [Hide Alerts](#)

| Name | Product Type | Last Contact | Alerts | Actions |
|---|--------------|----------------------|--------|--------------------------|
| UDI_PID:C9800-CL-K9; UDI_SN:9V4ZP2PN8DW | C9800CL | 2021-May-21 21:37:46 | | Transfer... Remove... |

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非推奨となっています。

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コマンドを使用するのではなく、オフラインのSLUPレポートに移行することをお勧めします。ライセンス使用状況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すが、正確な使用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で使用されていたtools.cisco.comの代わりに、新しいSLUPでは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。WLCからのインターネット到達可能性テストとしてpingを使用することはできません。これらのサーバに対してpingを実行できないことは、サーバが正常に動作していないことを意味するものではありません。

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、またはサーバのIPアドレスに対して直接確認できます。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コマンドが有効になっている場合、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 store
Aug 22 12:13:08.952: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named SLA-KeyPair has been generated or imported
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 installed
```

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 Manager
```

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 Manager
```

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。

Troubleshooting > Packet Capture

| Capture Name | Interface | Monitor Control Plane | Buffer Size | Filter by | Limit | Status | Action |
|---------------------|-----------|-----------------------|-------------|-----------|-------|--------|--------|
| 0 items per page | | | | | | | |
| No items to display | | | | | | | |

Monitor Control Planeチェックボックスがオン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。キャプチャする必要があるインターフェイスを追加します。スマートライセンスのトラフィックは、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。

Create Packet Capture ✕

Capture Name*

Filter*

Monitor Control Plane

Buffer Size (MB)*

Limit by* secs == 1.00 hour

Available (3)

- GigabitEthernet1 →
- GigabitEthernet2 →
- Vlan1 →

Selected (1)

- Vlan39 ←

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。

Troubleshooting > Packet Capture

| Capture Name | Interface | Monitor Control Plane | Buffer Size | Filter by | Limit | Status | Action |
|----------------------------------|-----------|-----------------------|---------------------------------|-----------|-----------|----------|---|
| <input type="checkbox"/> license | Vlan39 | Yes | <input type="text" value="0%"/> | any | 3600 secs | Inactive | <input style="border: 1px solid red;" type="button" value="▶ Start"/> |

items per page
 1 - 1 of 1 items

信頼確立の packets キャプチャには、次の手順が含まれている必要があります。

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ウィンドウアップデート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==<on-prem-ssm-ip>
```

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行の後に何も無い場合は、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、信頼が正常に確立された場合の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_serial_number":"NB"},"version":"1.3","locale":"en_US.UTF-8","signing_cert_serial_number":"3","id_cert_serial_number":"","product_instance_identifier":"","connect_info":{"name":"C_agent","version":"5.0.9_release","additional_info":"","capabilities":["UTILITY","DLC","AppHA","MULTITIER","EXPORT_2","POLICY_USAGE"]},"request_data":{"sudi":{"udi_pid":"C9800-CL-K9","udi_serial_number":"","timestamp":"1629713888600","nonce":"11702702165338740293","product_instance_identifier":"original_request_type":"LICENSE_USAGE","original_piid":"2e84a42f-c903-44c5-83b2-e62e258c780f","signature":{"type":"SHA256","key":"59152896","value":"eiJ7IuQaTCFvgUkwls76WZxa5DRI5A0gMqQd5POU6VNSH2j9dHco4T1NJ/aCMBR1MRmkfxyVSWsx47mjJL1mp0Si3ZS4FBMv1F/EBOUfowREe2oz21rQp1cAFpPn5S1aFwZw/Nu6SQZfIW+IdF+2qnJenFAIZbNpg0B5d5HIJvDmDImvDu3bMRHhQAwr2KKzGFr6jPz0hs7bGY/+F1ftLQk5LFEUaKTNH/tuxJPFH1Fh9//uhsd+NaQyfdRF1udkbFUBTFkvPxHW9/5w=="}}}}
```

```
RESPONSE: Aug 23 10:18:10 2021 Central
{"signature":{"type":"SHA256","value":"TXZE034fqAu12jy9V4+HoB2hDSh19au/5sgodiCVatmu671/6MyN7kZfEzREufY8SLrjTf04grGeQTch7yEj0D+gztWXC0u8RBT7/Bo9aBs\n4x1i0E6f1PB3BP6yu7KIEUQZ8yHz1wDT+mVtJGi6TRrtYnV3KQMPcUMF5Fw0ksf3SfXreNZJuzWXzjHvtm1usCQXw7ZTBzffYsNK001kJ1r\nnvgB2Pkv7JU1sA481kpIv1Pu16IiJXqk+2PC2IzCrCLG571VN3XgX1pE12SHyQ/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","udi_serial_number":"9PJK8D70CNB"},"agent_actions":null,"connect_info":{"name":"SSM","version":"1.3","product_instance_identifier":["DLC","AppHA","EXPORT_2","POLICY_USAGE","UTILITY"],"additional_info":"","signing_cert_serial_number":"59152896","product_instance_identifier":"","status_code":"FAILURE"},"Invalid ProductInstanceIdentifier: 2e84a42f-c903-44c5-83b2-e62e258c780f provided in the polling request 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。追加 | include smart-agent コマンドを実行して、スマートライセンスのログのみを取得します。

```
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、ライセンスコマンドを再設定して、新しい接続を強制的に使用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簡単に確認する方法です。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の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秒後に空の応答が表示されます。

たとえば、空の応答を受信されたと思い込んでしまうかもしれませんが、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側でちゃんとした証明書が必要です。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、パケットキャプチャは、9800 HTTPクライアント証明書が期限切れになった際にCSSMから送信された不明なCAのTLSアラートを示します。


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、次のコマンドを正しく設定する必要があります。

```
ip http client source-interface <interface>
ip http client secure-trustpoint <TP>
```

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-xxxxxxxxx証明書、または製造元でインストールされる証明書(MIC)の使用が推奨されます。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Cisco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

- [9800でのエアギャップモードを使用した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。