Konfiguration und Fehlerbehebung bei Catalyst 9800 Smart Licensing mit SLUP

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration und Fehlerbehebung von Smart Licensing mithilfe einer Richtlinie (SLUP) auf dem Catalyst 9800 Wireless LAN Controller (WLC) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

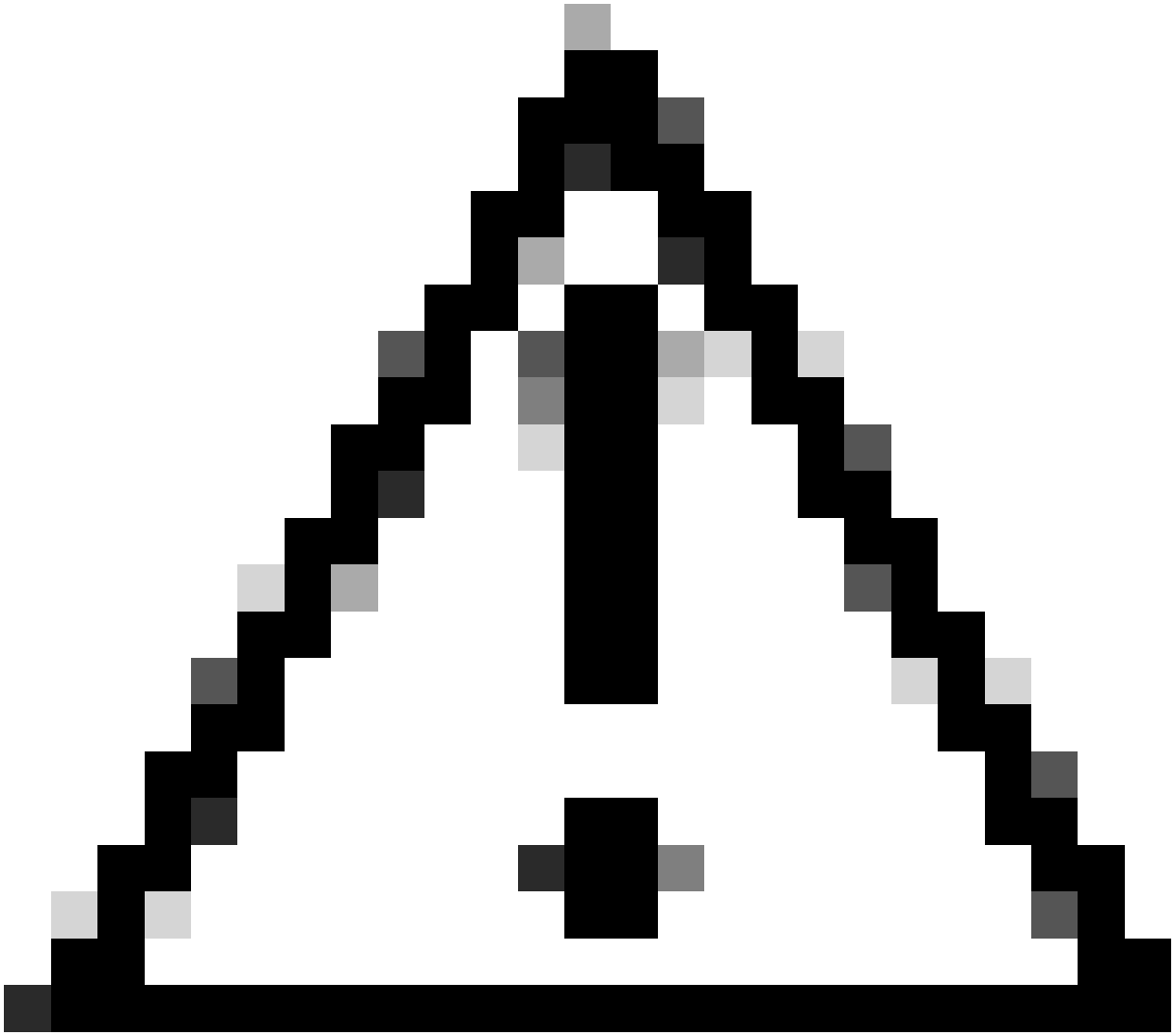
- Smart Licensing-Nutzungsrichtlinie (SLUP)
- Catalyst 9800 Wireless LAN-Controller (WLC)

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

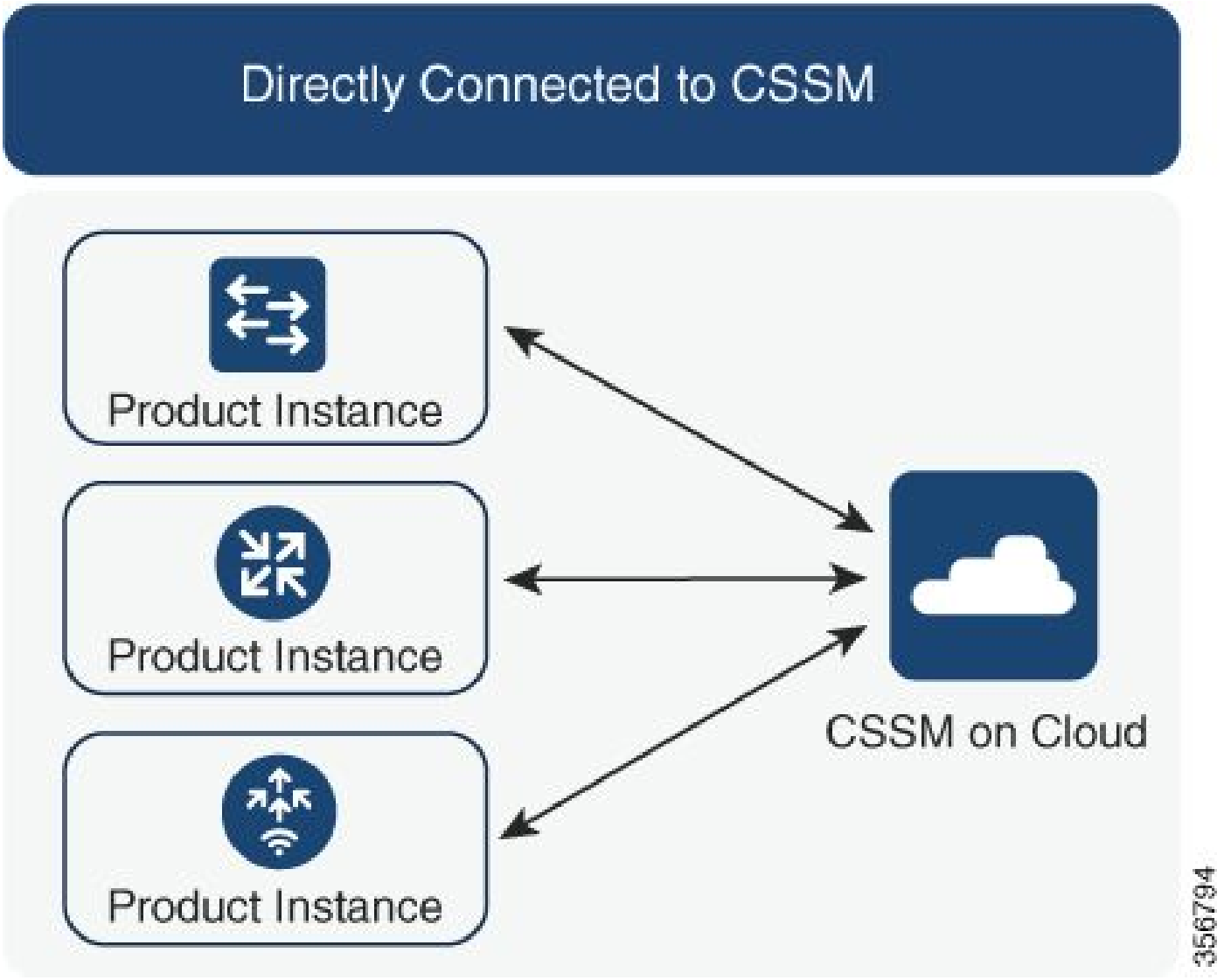


Vorsicht: Hinweise in diesem Artikel enthalten nützliche Vorschläge oder Verweise auf Material, das nicht in diesem Dokument behandelt wird. Es wird empfohlen, dass Sie jede

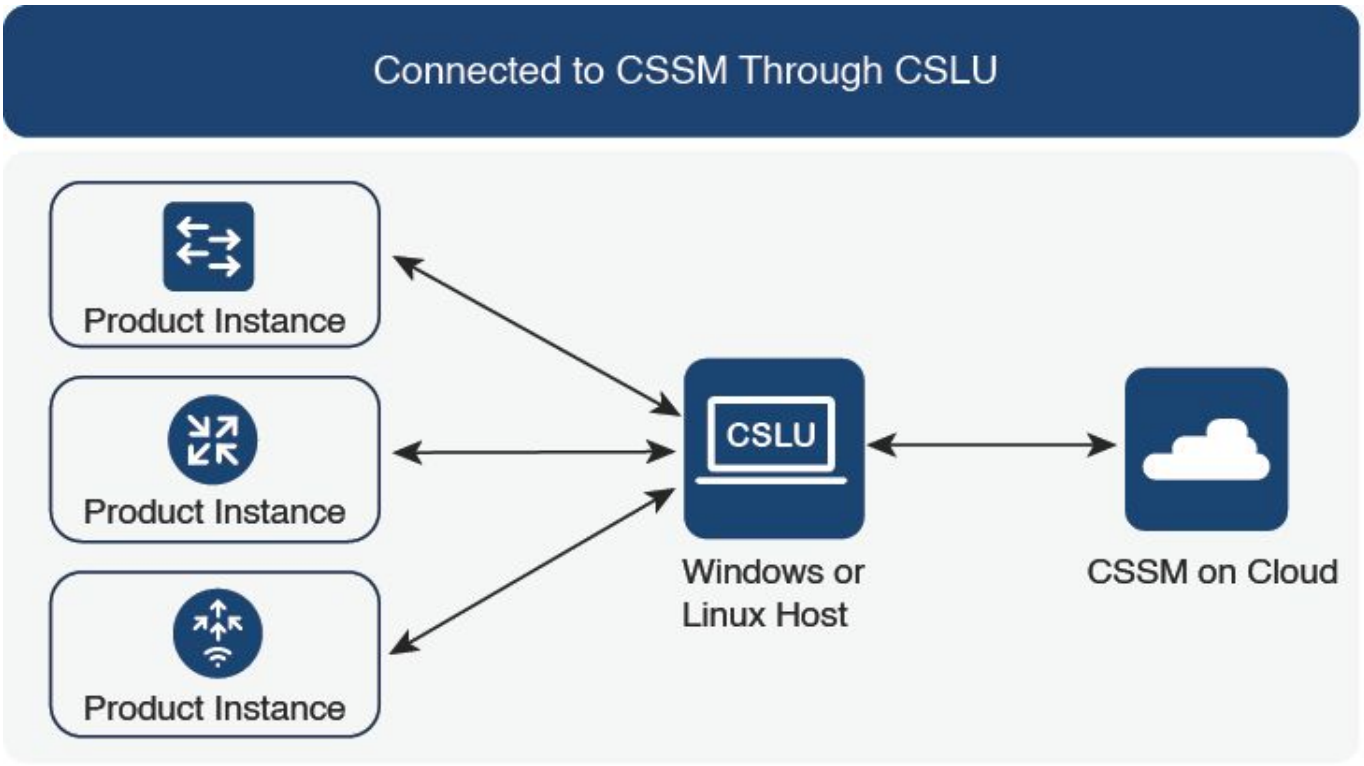
Note lesen.

1. Direkte Verbindung zur Cisco Smart Software Manager Cloud (CSSM Cloud)
2. Mit CSSM über CSLU verbunden (Cisco Smart License Utility Manager)
3. Verbindung zum CSSM über Smart Software Manager vor Ort (SSM vor Ort)

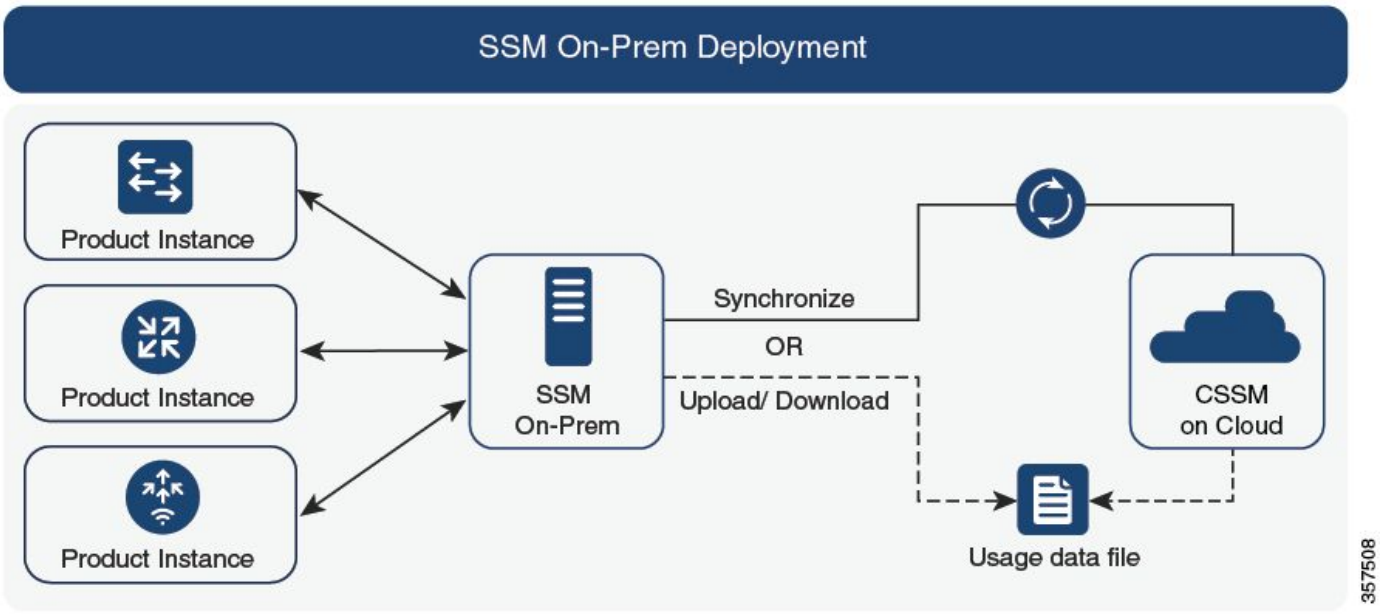
Dieser Artikel behandelt nicht alle Smart Licensing-Szenarien für Catalyst 9800. Weitere Informationen finden Sie im Konfigurationsleitfaden für Smart Licensing mit Richtlinien. Dieser Artikel enthält jedoch eine Reihe nützlicher Befehle zur Fehlerbehebung bei Problemen mit Direct Connect, CSLU und standortbasierten SSM Smart Licensing Using Policy auf dem Catalyst 9800.



Option 1: Direkte Verbindung zu Cisco Smart Licensing Cloud-Servern (CSSM)



Option 2: Verbindung über CSLU



Option 3. Verbindung über standortinternen Smart Software Manager (standortinternes SSM)

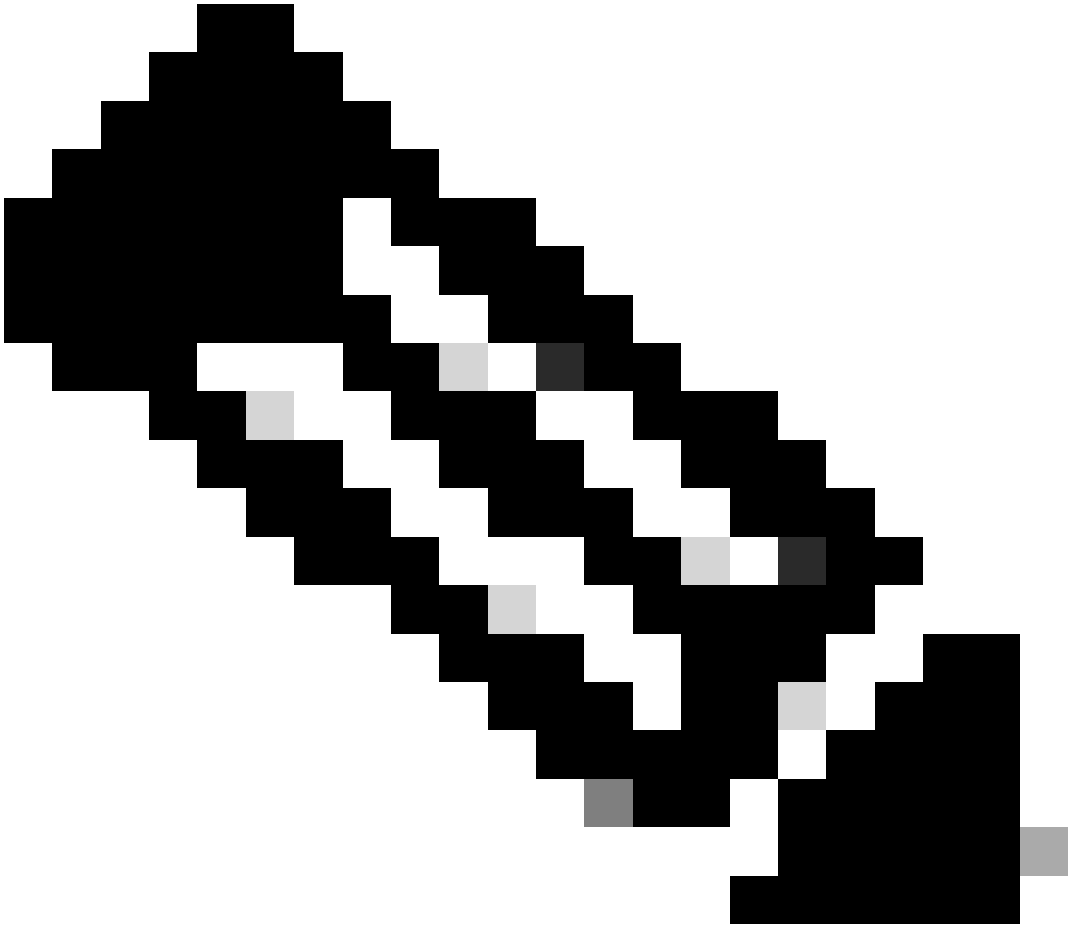
Hinweis: Alle in diesem Artikel erwähnten Befehle gelten nur für WLCs mit Version 17.3.2 oder höher.

Traditionelle Lizenzierung im Vergleich zu SLUP

Die Funktion "Smart Licensing Using Policy" wurde in Catalyst 9800 mit der Codeversion 17.3.2 eingeführt. In der ersten Version 17.3.2 fehlt das SLUP-Konfigurationsmenü in der WLC-

Webbenutzeroberfläche, das mit der Version 17.3.3 eingeführt wurde. Das SLUP unterscheidet sich in vielerlei Hinsicht von herkömmlichen Smart Licensing-Lösungen:

- WLC kommuniziert jetzt mit CSSM über die Domäne smartreceiver.cisco.com und nicht über die Domäne tools.cisco.com.
- Anstatt sich zu registrieren, richtet der WLC nun eine Vertrauensstellung zum CSSM oder standortbasierten SSM ein.
- CLI-Befehle wurden leicht geändert.
- Es gibt keine Smart Licensing Reservation (SLR) mehr. Stattdessen können Sie Ihre Nutzung regelmäßig manuell melden.
- Es gibt keinen Evaluierungsmodus mehr. Der WLC arbeitet auch ohne Lizenz mit voller Leistung weiter. Das System ist honorbasiert und Sie sollen Ihre Lizenznutzung regelmäßig (automatisch oder manuell im Falle von Airgap-Netzwerken) melden.



Warnung: Wenn Sie einen Cisco Catalyst 9800-CL Wireless Controller verwenden, stellen Sie sicher, dass Sie mit der obligatorischen ACK-Anforderung vertraut sind, die mit Cisco IOS® XE Cupertino 17.7.1 beginnt. Siehe RUM Reporting and Acknowledgment Requirement für Cisco Catalyst 9800-CL Wireless Controller.

Konfiguration

Direct Connect-CSSM

Nachdem das Token auf dem CSSM erstellt wurde, müssen zur Einrichtung der Vertrauenswürdigkeit die folgenden Befehle ausgeführt werden:

Hinweis: Max. Token Die Anzahl der Verwendungen muss bei WLC in HA SSO mindestens 2 betragen.

```
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
```

- Der Befehl ip http client source-interface gibt die L3-Schnittstelle an, von der lizenzbezogene Pakete bezogen werden.
- Der Befehl ip http client secure-trustpoint gibt an, welcher Trustpoint/welches Zertifikat für die CSSM-Kommunikation verwendet wird. Der Name des Vertrauenspunkts kann mit dem Befehl show crypto pki trustpoints gefunden werden. Es wird empfohlen, ein selbstsigniertes Zertifikat (TP-self-signed-xxxxxxxxxx) oder ein vom Hersteller installiertes Zertifikat (auch als MIC bezeichnet, nur verfügbar auf den Geräten 9800-40, 9800-80 und 9800-L) mit der Bezeichnung CISCO_IDEVID_SUDI zu verwenden.
- Der Befehl Terminal Monitor veranlasst den WLC, die Protokolle auf der Konsole auszudrucken und zu überprüfen, ob die Vertrauenswürdigkeit erfolgreich eingerichtet wurde. Es kann mit Terminal auf Monitor deaktiviert werden.
- Das Schlüsselwort all im letzten Befehl weist alle WLCs im HA SSO-Cluster an, die Vertrauensstellung zum CSSM herzustellen.
- Keyword Force weist den WLC an, einen der zuvor eingerichteten Trusts zu überschreiben und einen neuen zu versuchen.

Hinweis: Wenn die Vertrauensstellung nicht hergestellt wird, versucht es der 9800 1 Minute später nach der Ausführung des Befehls erneut und versucht es dann einige Zeit lang nicht mehr. Geben Sie den Token-Befehl erneut ein, um eine neue Vertrauensstellung zu erzwingen.

Mit CSLU verbunden

Cisco Smart License Utility Manager (CSLU) ist eine Windows-basierte Anwendung (auch unter

Linux verfügbar), mit der Kunden Lizenzen und zugehörige Produktinstanzen von ihrem Standort aus verwalten können, anstatt ihre Smart Licensed-fähigen Produktinstanzen direkt mit Cisco Smart Software Manager (CSSM) zu verbinden.

In diesem Abschnitt wird nur die Wireless-Konfiguration des 9800 behandelt. Es gibt noch weitere Schritte, um die Lizenzierung mit CSLU zu konfigurieren (z. B. Installation von CSLU, Konfiguration der CSLU-Software usw.). Diese Schritte werden in den Konfigurationsanleitungen behandelt. Ob Sie eine von einer Produktinstanz initiierte oder von einer CSLU initiierte Kommunikationsmethode implementieren oder die entsprechende Abfolge von Aufgaben durchführen möchten.

Durch Produktinstanz initiiert

1. Sicherstellung der Netzwerkerreichbarkeit vom Controller zur CSLU
2. Stellen Sie sicher, dass der Transporttyp auf cslu eingestellt ist:

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

3. Wenn die CSLU vom Controller erkannt werden soll, müssen Sie die Aktion ausführen. Wenn CSLU mithilfe von DNS erkannt werden soll, ist keine Aktion erforderlich. Wenn Sie eine URL zur Erkennung verwenden möchten, geben Sie den folgenden Befehl ein:

```
(config)#license smart url cslu http://<cslu_ip>:8182/cslu/v1/pi
(config)#exit
#copy running-config startup-config
```

von CSLU initiiert

Wenn Sie eine CSLU-initiierte Kommunikation konfigurieren, müssen Sie lediglich überprüfen, ob der Controller das Netzwerk über CSLU erreichbar ist.

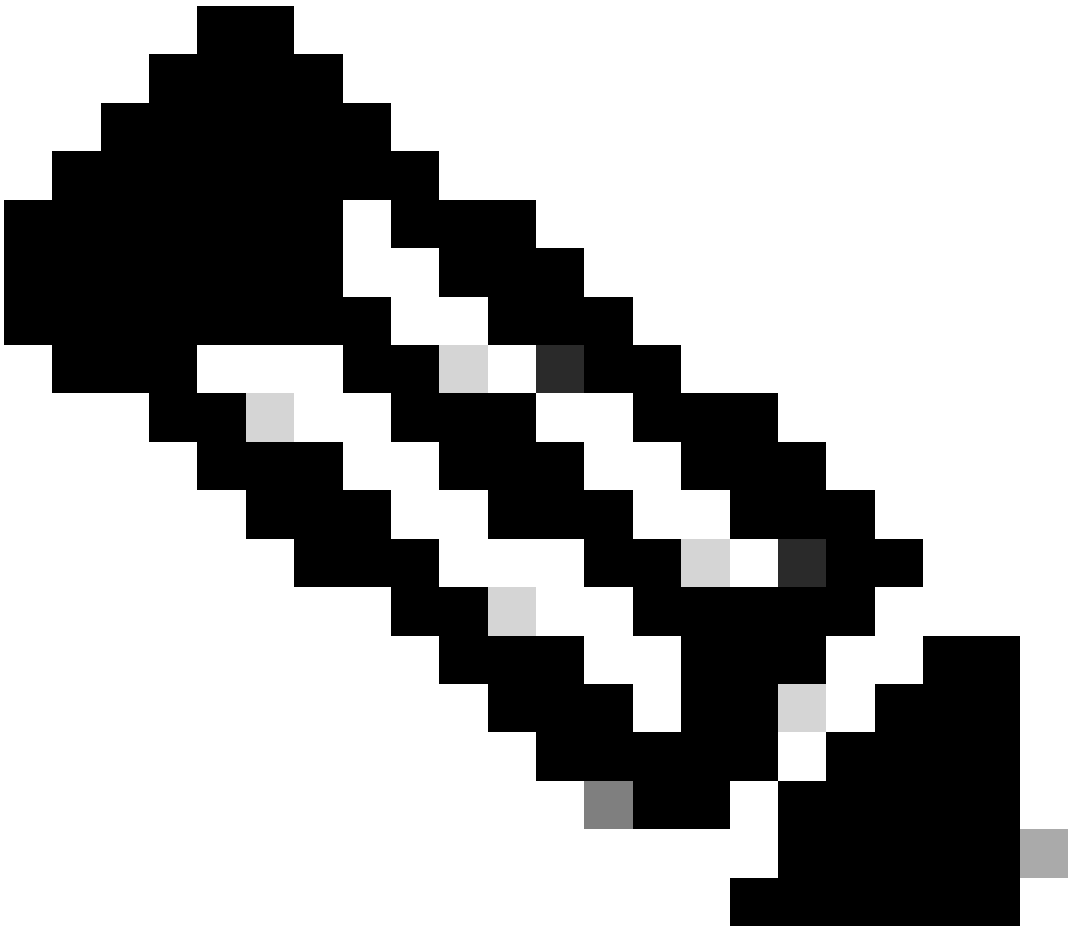
Mit SSM vor Ort verbunden

Die Konfiguration mit standortbasiertem SSM ähnelt der Direktverbindung. Vor Ort muss Version 8-202102 oder höher ausgeführt werden. Für SLUP-Versionen (17.3.2 und höher) wird empfohlen, die CSLU-URL und den Transporttyp zu verwenden. Die URL steht im Abschnitt "**Smart Licensing > Inventory > <Virtual Account> > General" (Smart Lizenzierung > Bestand > <Virtuelles Konto> > Allgemein)** über die WebUI-Benutzeroberfläche **zur Verfügung**.

```
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
```

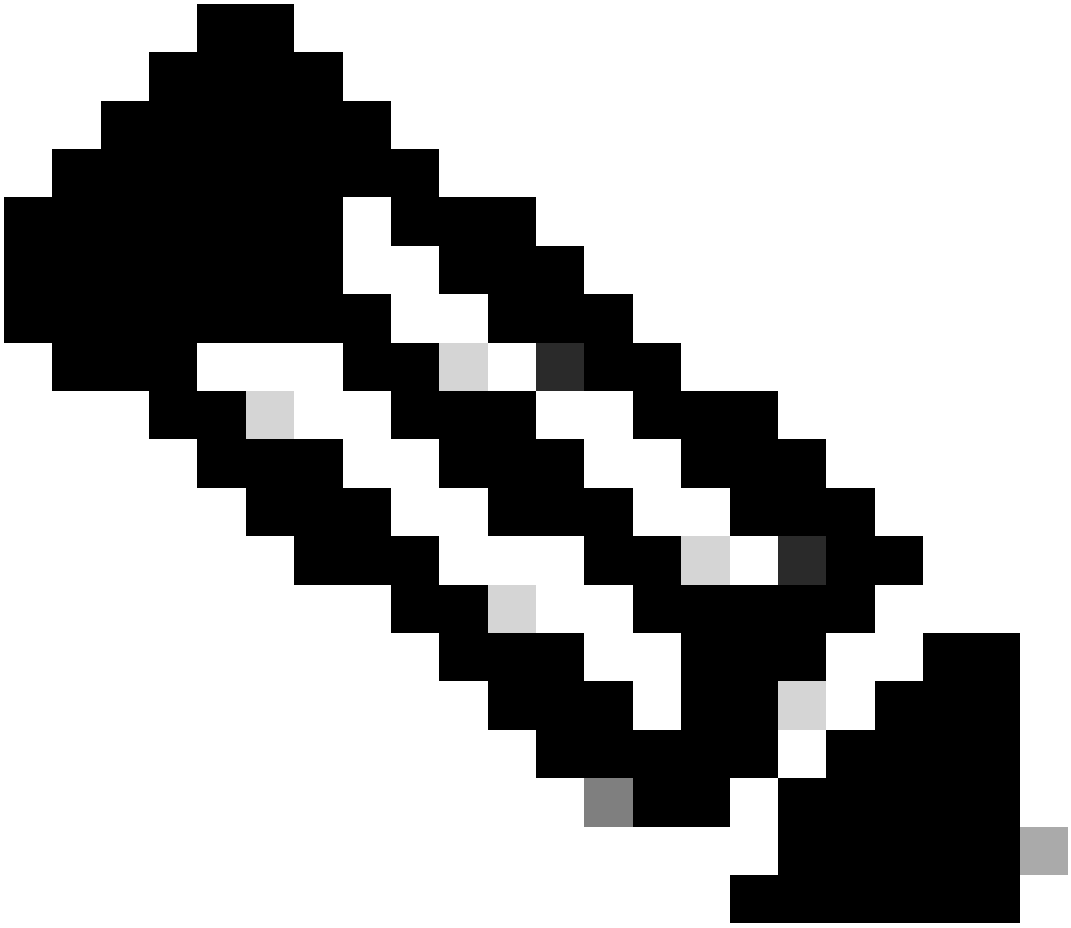
```
 crypto pki trustpoint SLA-TrustPoint
  revocation-check none
 exit
write memory
terminal monitor
```

Für standortbasiertes SSM ist die Verwendung eines Vertrauenstokens nicht erforderlich.



> Hinweis: Wenn Sie die Nachricht erhalten, %PKI-3-CRL_FETCH_FAIL: Fehler beim Abrufen der Zertifikatsperrliste für Trustpoint SLA-TrustPoint, weil Sie keine Sperrüberprüfung unter SLA-TrustPoint konfiguriert haben. Dies ist der Vertrauenspunkt für Smart Licensing. Im Fall von On-Prem ist das Zertifikat auf dem Lizenzserver in der Regel ein selbstsigniertes Zertifikat, für das eine CRL-Überprüfung nicht möglich ist. Daher ist es erforderlich, keine Widerrufsprüfungen zu konfigurieren.

Konfigurieren von intelligentem Transport über einen HTTPS-Proxy



Hinweis: Authentifizierte Proxys werden seit Version 17.9.2 des Codes noch nicht unterstützt. Wenn Sie in Ihrer Infrastruktur authentifizierte Proxys verwenden, erwägen Sie die Verwendung des Cisco Smart License Utility Manager (CSLU), der diese Servertypen unterstützt.

Führen Sie die folgenden Schritte aus, um mit dem CSSM über einen Proxyserver zu kommunizieren, wenn Sie den intelligenten Transportmodus verwenden:

```
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
```

Kommunikationsfrequenz

Das Berichtsintervall, das Sie in CLI oder GUI konfigurieren können, hat keine Auswirkungen.

Der 9800 WLC kommuniziert alle 8 Stunden mit CSSM oder dem standortbasierten Smart Software Manager, unabhängig davon, welches Berichtsintervall über die Webschnittstelle oder die CLI konfiguriert wird. Das bedeutet, dass neu verknüpfte Access Points bis zu 8 Stunden nach dem ersten Beitritt auf dem CSSM angezeigt werden können.

Mit dem Befehl show license air entity summary können Sie bestimmen, wann Lizenzen das nächste Mal berechnet und gemeldet werden. Dieser Befehl ist nicht Teil der typischen show tech oder show license all-Ausgabe:

<#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
```

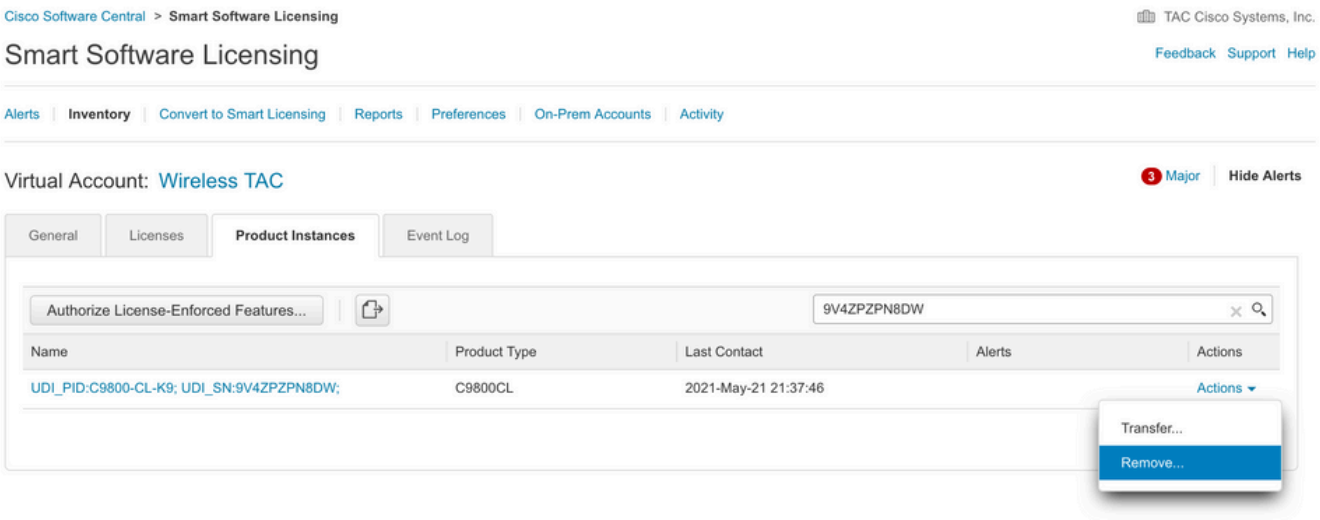
Lizenz-Zurücksetzen auf Factory

Der Catalyst 9800 WLC kann seine gesamte Lizenzkonfiguration beibehalten, auf die Werkseinstellungen vertrauen und alle anderen Konfigurationen beibehalten. Dies erfordert ein erneutes Laden des WLC:

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

Bei RMA oder Hardware-Ersatz

Wenn der 9800 WLC ersetzt werden muss, muss sich das neue Gerät beim CSSM/On-Prem Smart Software Manager registrieren, und es wird als neues Gerät wahrgenommen. Um die Lizenzanzahl des vorherigen Geräts freizugeben, müssen Sie die Lizenz unter Produktinstanzen manuell löschen:



Upgrade von spezifischer Lizenzregistrierung (SLR)

Ältere WLC-Versionen vor 17.3.2 verwendeten eine spezielle Offline-Lizenzierungsmethode namens Specific License Registration (SLR). Diese Lizenzierungsmethode wurde in den Versionen mit SLUP (17.3.2 und höher) als veraltet eingestuft.

Wenn Sie einen 9800-Controller, der SLR verwendet hat, auf eine Version nach 17.3.2 oder 17.4.1 aktualisieren, sollten Sie auf die Offline-SLUP-Berichterstellung umstellen, anstatt sich auf die SLR-Befehle zu verlassen. Speichern Sie die RUM-Datei für die Lizenznutzung, und registrieren Sie diese im Smart Licensing-Portal. Da SLR in neueren Versionen nicht mehr vorhanden ist, wird die korrekte Lizenzanzahl ausgegeben und nicht verwendete Lizenzen werden freigegeben. Die Lizenzen werden nicht mehr blockiert, aber die genaue Anzahl der genutzten Lizenzen wird gemeldet.

Fehlerbehebung

Internetzugriff, Portprüfungen und Pings

Anstelle der tools.cisco.com, die bei der herkömmlichen Smart Licensing-Methode verwendet wurde, verwendet das neue SLUP die Domäne smartreceiver.cisco.com, um eine Vertrauensstellung herzustellen. Zum Zeitpunkt der Erstellung dieses Artikels wird diese Domäne in mehrere verschiedene IP-Adressen aufgelöst. Nicht alle diese Adressen sind pingbar. Pings dürfen nicht als Test der Interneterreichbarkeit vom WLC verwendet werden. Wenn diese Server nicht gepingt werden können, bedeutet dies nicht, dass sie nicht ordnungsgemäß funktionieren.

Anstelle von Pings muss Telnet über Port 443 als Erreichbarkeitstest verwendet werden. Telnet kann entweder mit der Domäne smartreceiver.cisco.com oder direkt mit den IP-Adressen des Servers abgeglichen werden. Wenn der Datenverkehr nicht blockiert wird, muss der Port in der Ausgabe als offen angezeigt werden:

```
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

Wenn der Befehl terminal monitor während der Tokenkonfiguration aktiviert ist, druckt der WLC die relevanten Protokolle in der CLI aus. Diese Meldungen können auch abgerufen werden, wenn Sie den Befehl show logging ausführen. Protokolle einer erfolgreich eingerichteten Vertrauensstellung sehen wie folgt aus:

```
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
```

Protokolle eines WLC ohne definierten DNS-Server oder mit einem nicht funktionierenden DNS-Server:

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

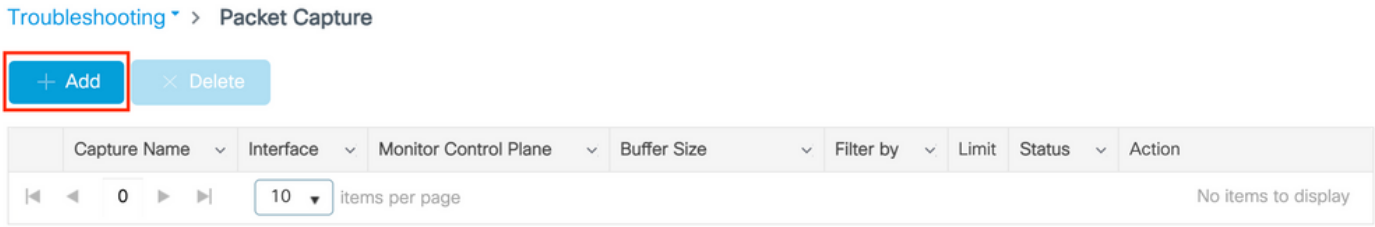
Protokolle eines WLC mit einem funktionierenden DNS-Server, jedoch ohne Internetzugang:

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

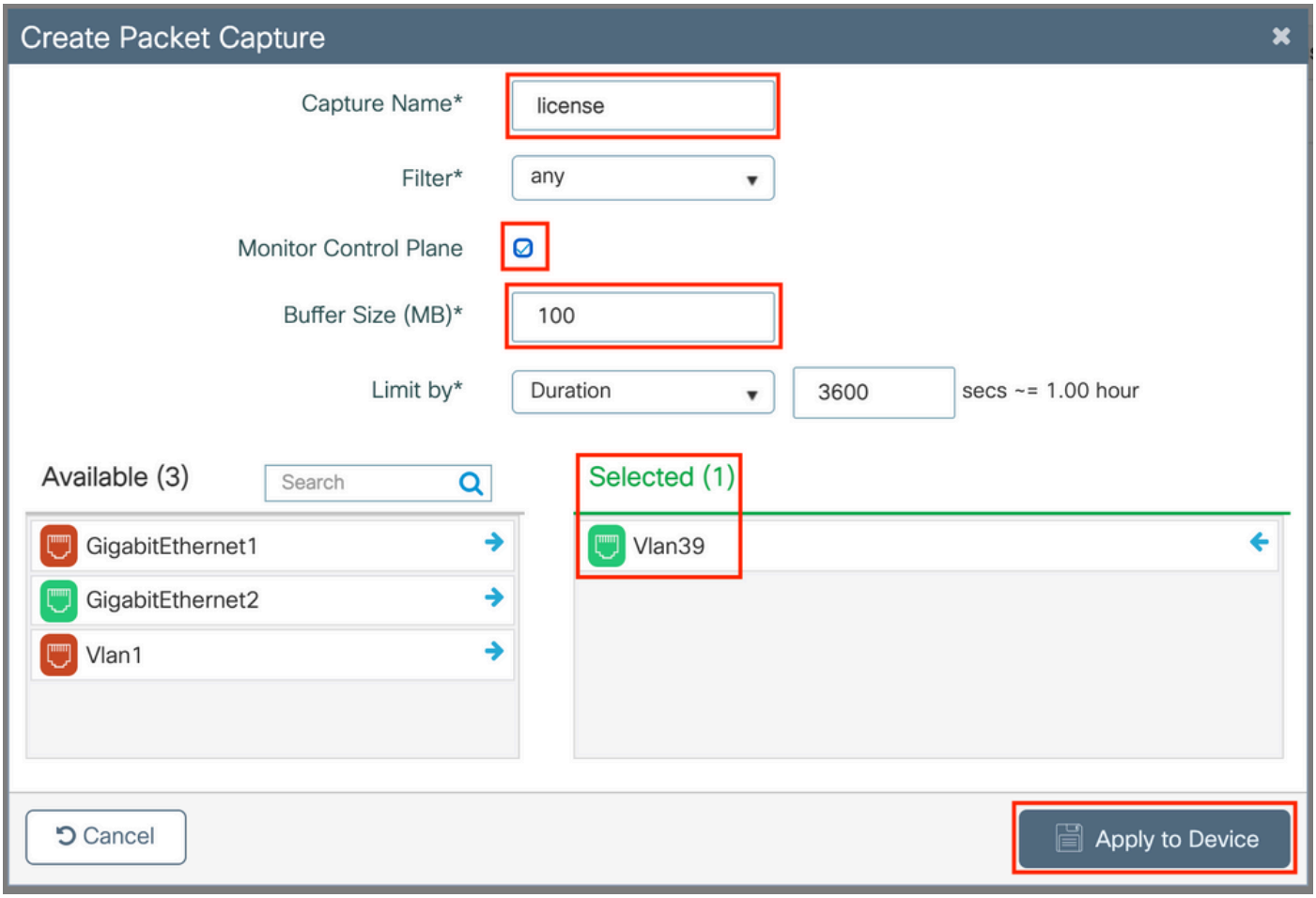
Paketerfassung

Auch wenn die Kommunikation zwischen WLC und CSSM/On-Prem SSM verschlüsselt ist und über HTTPS läuft, kann die Durchführung von Paketerfassungen zeigen, weshalb die Vertrauensstellung nicht hergestellt wird. Die einfachste Methode zum Sammeln von Paketerfassungen ist die WLC-Webschnittstelle.

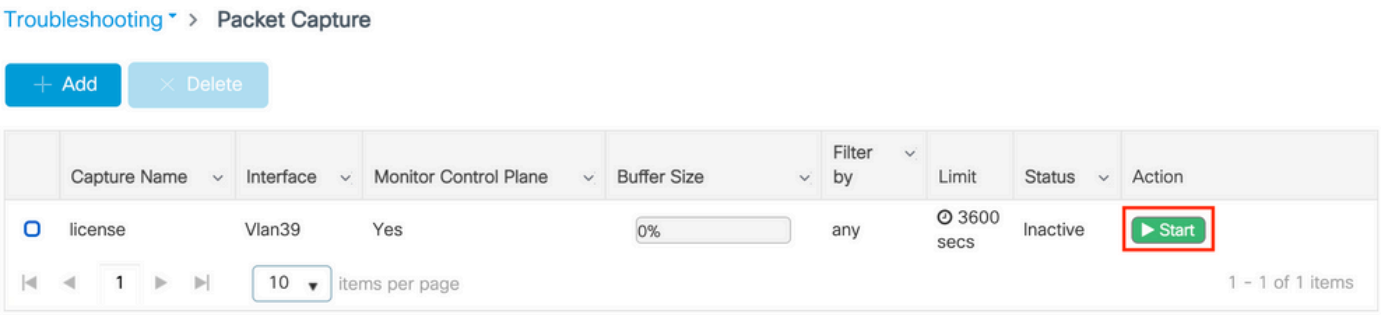
Navigieren Sie zu Fehlerbehebung > Paketerfassung. Erstellen Sie einen neuen Erfassungspunkt:



Stellen Sie sicher, dass das Kontrollkästchen Kontrollebene überwachen aktiviert ist. Erhöhen Sie die Puffergröße auf die maximale Größe von 100 MB. Fügen Sie die Schnittstelle hinzu, die erfasst werden muss. Der Smart Licensing-Datenverkehr stammt standardmäßig von der Wireless-Verwaltungsschnittstelle oder von der Schnittstelle, die mit dem Befehl ip http client source-interface definiert wurde:



Starten Sie die Erfassungen, und führen Sie den Befehl license smart trust idtoken <token> all force aus:



Die Paketerfassung einer Vertrauensstellung muss folgende Schritte enthalten:

1. TCP-Sitzungsaufbau mit SYN-, SYN-ACK- und ACK-Sequenz
2. TLS-Sitzungsaufbau mit Austausch von Server- und Clientzertifikaten. Einrichtung endet mit dem neuen Sitzungsticket-Paket
3. Verschlüsselter Paketaustausch (Anwendungsdaten-Frames), bei dem WLC die

Lizenznutzung meldet

4. TCP-Session-Terminierung über FIN-PSH-ACK-, FIN-ACK- & ACK-Sequenz

---

Hinweis: Die Paketerfassungen enthalten viel mehr Frames, einschließlich mehrerer TCP-Fensteraktualisierungen und Anwendungsdaten-Frames.

Da die CSSM Cloud drei verschiedene öffentliche IP-Adressen verwendet, können Sie zum Herausfiltern aller Paketerfassungen zwischen WLC und CSSM die folgenden Wireshark-Filter verwenden:

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

Wenn Sie ein standortbasiertes SSM verwenden, filtern Sie nach der SSM-IP-Adresse:

```
ip.addr==<on-prem-ssm-ip>
```

Beispiel: Paketerfassung einer erfolgreichen Vertrauensstellung mit direkt verbundenem CSSM mit Filterung aller signifikanten Paketerfassungen:

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

Befehle anzeigen

Diese show-Befehle enthalten nützliche Informationen zur Einrichtung der Vertrauensstellung:

```
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)
```

Der Befehl show license history message ist einer der nützlicheren Befehle, da er die tatsächlichen Nachrichten anzeigen kann, die vom WLC gesendet und vom CSSM empfangen wurden.

Eine erfolgreiche Vertrauensstelle hat sowohl die Nachrichten "ANTRAG: Aug 23 10:18:08 2021 Central" und "ANTWORT: Aug 23 10:18:10 2021 Central" gedruckt. Wenn nach der RESPONSE-Zeile nichts ist, bedeutet dies, dass der WLC keine Antwort vom CSSM erhalten hat.

Dies ist ein Beispiel für eine Ausgabe einer Lizenzverlaufsmeldung für eine erfolgreiche Vertrauensstellung:

```
REQUEST: Aug 23 10:18:08 2021 Central
{"request":"{\"header\":{\"request_type\":\"POLL_REQ\",\"sudi\":{\"udi_pid\":\"C9800-CL-K9\",\"udi_seria
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":"TXZEO34fqAul2jy9V4+HoB2hDShl9au/5sgodiCVatmu671/6MyN7kZfEzREufY8
SLrjTfO4grGeQTcH7yEjOD+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}
```

Debugger/btrace

Führen Sie diesen Befehl einige Minuten nach dem Versuch, eine Vertrauensstellung herzustellen, mit dem Befehl license smart trust idtoken all force aus. IOSRP-Protokolle sind äußerst ausführlich. Anfügen | include smart-agent" auf den Befehl ein, um nur Smart Licensing-Protokolle abzurufen.

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

Sie können auch diese Debugs ausführen und dann die Lizenzierungsbefehle neu konfigurieren, um eine neue Verbindung zu erzwingen:

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

Häufige Probleme

WLC hat keinen Internetzugang und Firewall blockiert/ändert Datenverkehr nicht

Die eingebettete Paketerfassung auf dem WLC ist eine einfache Möglichkeit, festzustellen, ob der WLC etwas vom CSSM oder On-Prem SSM zurückempfängt. Wenn es keine Antwort gab, blockiert die Firewall wahrscheinlich etwas.

Der Befehl show license history message gibt eine leere Antwort 1 Sekunde nach dem Senden der Anforderung aus, wenn keine Antwort von der CSSM Cloud oder dem standortbasierten SSM empfangen wurde.

Dies kann zum Beispiel dazu führen, dass Sie glauben, dass eine leere Antwort eingegangen ist, aber in Wirklichkeit gab es überhaupt keine Antwort:

```
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
```

Hinweis: Derzeit gibt es eine Verbesserungsanfrage unter der Cisco Bug-ID CSCvy84684, die den Ausdruck der Show-Lizenzverlaufsnachricht als leere Antwort anzeigt, wenn keine Antwort erfolgt. Hierdurch wird die Ausgabe des Befehls show license history message verbessert.

Unbekannte CA-Warnung bei Paketerfassung

Die Kommunikation mit CSSM oder standortbasiertem SSM erfordert ein anständiges Zertifikat auf der 9800-Seite. Es kann selbstsigniert sein, es kann jedoch weder ungültig noch abgelaufen sein. In diesem Fall zeigt eine Paketerfassung eine TLS-Warnung für eine unbekannte CA an, die von CSSM gesendet wurde, wenn das HTTP-Client-Zertifikat 9800 abgelaufen ist.

Bei der Smart Licensing-Lizenzierung wird die IP http-Client-Konfiguration verwendet, die sich vom IP http-Server unterscheidet, den die WLC-Webschnittstelle verwendet. Dies bedeutet, dass diese Befehle ordnungsgemäß konfiguriert werden müssen:

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

Den Namen des Vertrauenspunkts finden Sie mit dem Befehl show crypto pki trustpoints. Es wird empfohlen, ein selbstsigniertes Zertifikat TP-self-signed-xxxxxxxxxx oder ein vom Hersteller installiertes Zertifikat (Manufacturer Installed Certificate, MIC) zu verwenden. Dieses Zertifikat heißt in der Regel CISCO_IDEVID_SUDI und ist nur auf 9800-80, 9800-40 und 98000-L verfügbar.

Geräte, die TLS abfangen, z. B. eine Firewall mit der SSL-Entschlüsselungsfunktion, können verhindern, dass der C9800 einen erfolgreichen Handshake mit dem Cisco Lizenzierungsserver herstellt, da das angegebene HTTPS-Zertifikat das Firewall-Zertifikat und nicht das Cisco Lizenzierungsserverzertifikat ist.

Hinweis: Stellen Sie sicher, dass Sie sowohl Befehle der Quellschnittstelle als auch Secure TrustPoint-Befehle konfigurieren. Ein Source-Interface-Befehl ist auch dann erforderlich, wenn WLC nur über eine L3-Schnittstelle verfügt.

Zugehörige Informationen

- Smart Licensing mit Air Gap-Modus auf 9800
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.