Configure and Troubleshoot Catalyst 9800 Unified Licensing and Smart Licensing with SLUP

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Unified Licensing, Enforcement, and SLUP

Checking AP Compliance on Unified Licensing

Traditional Licensing vs SLUP

Configuration

- Direct Connect Cisco License Central
  - Product Instance-initiated
  - CSLU-initiated
- Connected to Cisco License Central On-prem
- Configuring Smart Transport Through an HTTPS Proxy
- Communication Frequency
- License Factory Reset
- In Case of RMA or Hardware Replacement
- Upgrading From Specific License Registration (SLR)

Troubleshooting

- Internet Access, Port Checks & Pings
- Syslog
- Packet Captures
- Show Commands
- Debugs/btrace

Common Issues

- WLC Has No Internet Access or Firewall Blocks/alters Traffic
- Unknown CA Alert in Packet Captures

Related Information

Introduction

This document describes configuring and troubleshooting Smart Licensing Using Policy (SLUP) on Catalyst 9800 WLC.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

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

- Cisco Networking Subscription

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

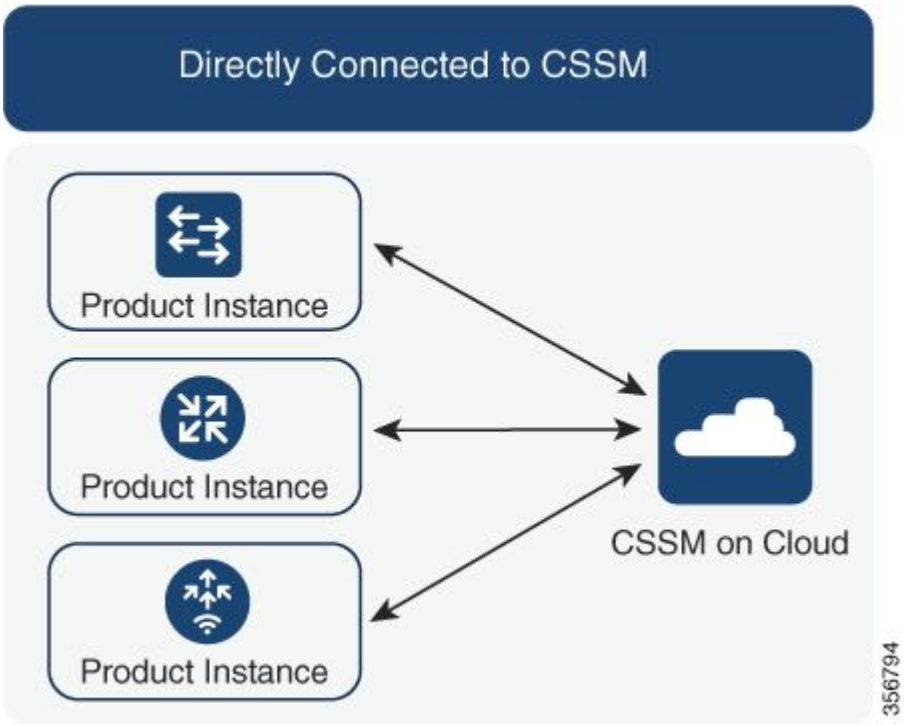
Background Information

Caution: Notes in this article contain helpful suggestions or references to material not covered in the document. It is recommended that you read each Note.

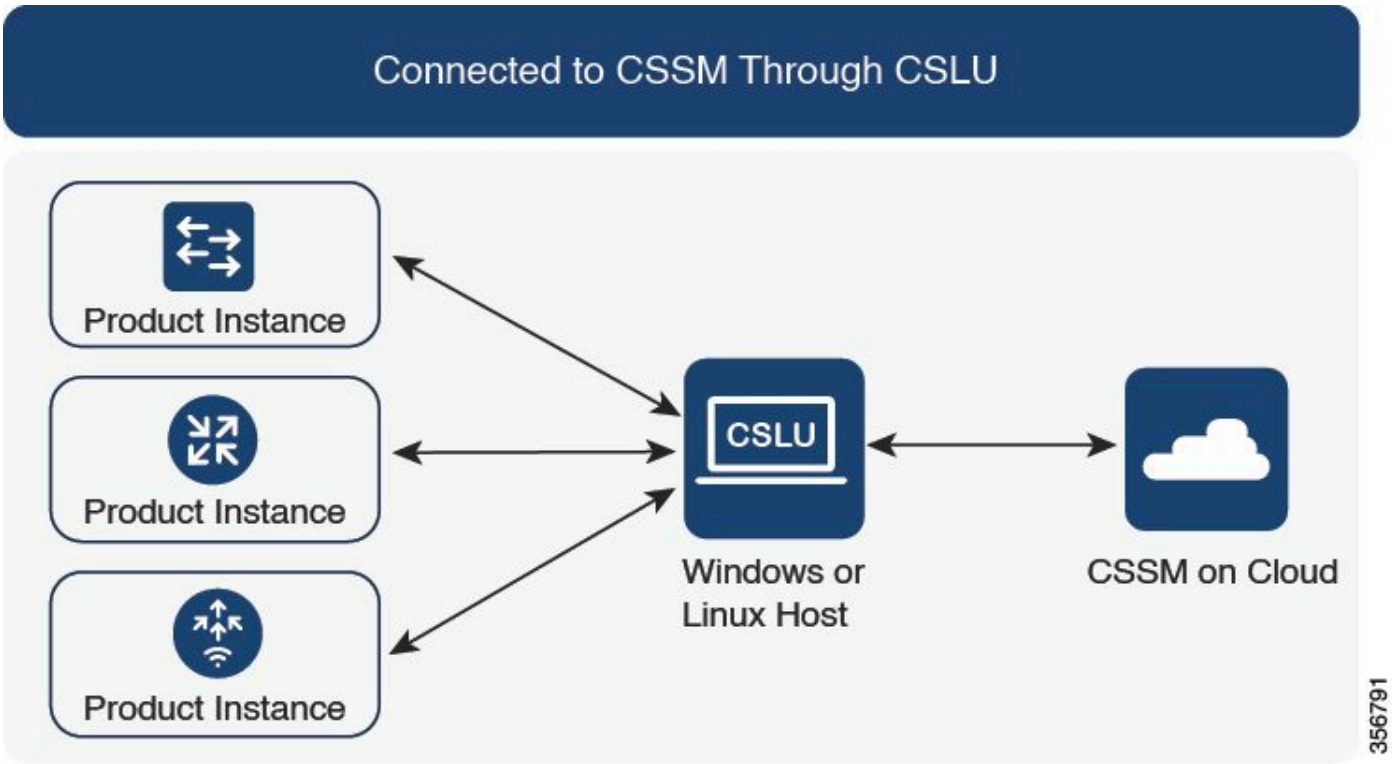
---

1. Direct connect to Cisco License Central
2. Connected to Cisco License Central via CSLU (Cisco Smart License Utility Manager)
3. Connected via Cisco License Central (On-prem)

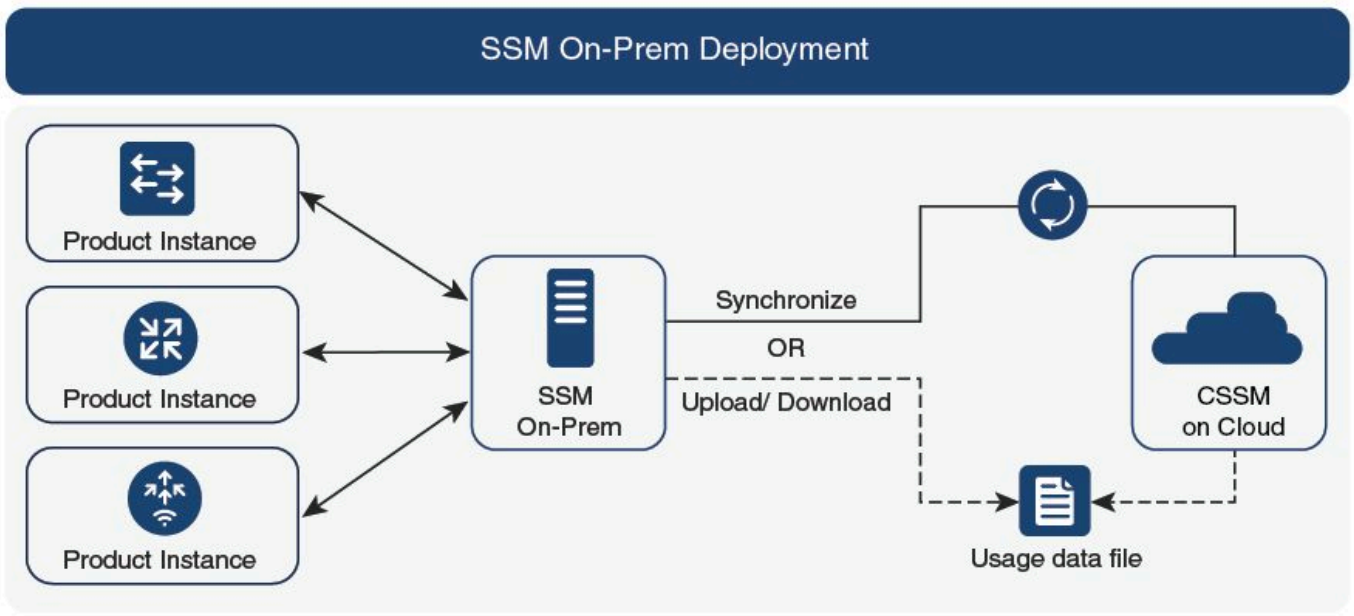
This article does not cover all the Smart Licensing scenarios on Catalyst 9800, refer to the Smart Licensing Using Policy Configuration Guide for additional information. However, this article does give a series of useful commands to troubleshoot direct connect, CSLU and On-prem Smart Licensing Using Policy issues on the Catalyst 9800.



Option 1. Direct connect to Cisco License Central:



Option 2. Connection via CSLU:



Option 3. Connect using Cisco License Central (On-prem).

Note: All commands mentioned in this article are applicable only to WLCs that run version 17.3.2 or later.

Unified Licensing, Enforcement, and SLUP

Unified licensing, available in Cisco Networking Subscriptions, introduces license enforcement to on-premises customers.

- **Cisco IOS® XE 17.15.2** (December 2024) was the first supported release for unified licensing and introduced per-device license reporting and compliance status.
- Future Cisco IOS XE releases introduce Day 0 enforcement for unlicensed APs and Day N enforcement for devices with expired licenses. on any out-of-compliance devices, enforcement takes place when the software image is updated.

Completing the steps in this guide is critical to ensure that your devices are configured correctly using SLUP, so that your devices are not subject to enforcement upon Cisco IOS XE software image upgrade.

Checking AP Compliance on Unified Licensing

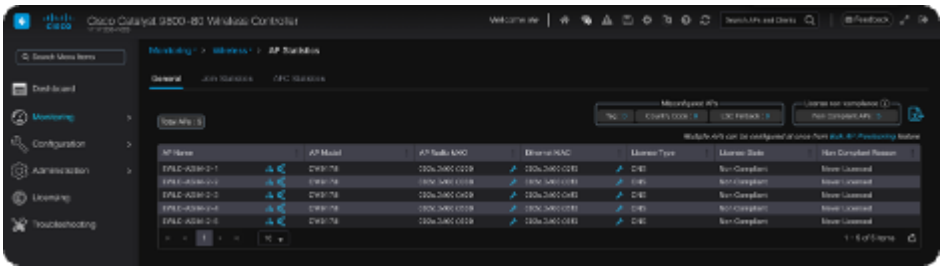


Figure 1: Web UI AP Compliance (non-compliant)

AP compliance information is available on-controller (Meraki Dashboard, Catalyst Center 2.3.7.9) and on-device (Web UI, CLI).

Figure 1 shows an example of AP compliance information on Web UI. Out-of-compliance APs have a *Non-Compliant* license state, with reasoning provided that the AP is “Never Licensed.”

After SLUP has been correctly configured, your APs reflect an updated compliant status.

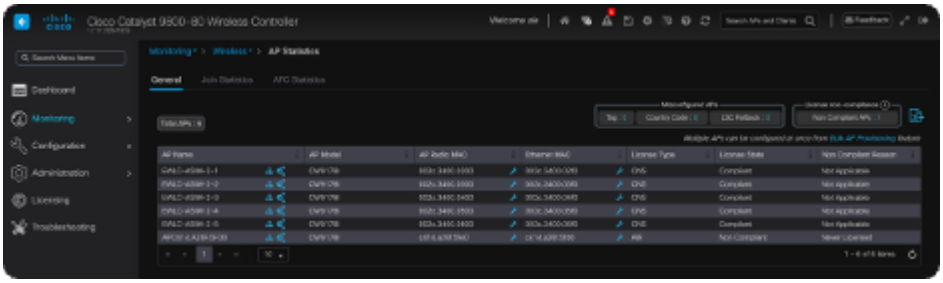


Figure 1: Web UI AP Compliance (compliant)

Note: If you have successfully configured SLUP and still see Non-Compliant status on your access points, then confirm you have purchased sufficient licensing and that these licenses have been deposited into the correct Smart Account (SA) and Virtual Account (VA).

Traditional Licensing vs SLUP

The Smart Licensing Using Policy feature has been introduced to the Catalyst 9800 with the code version 17.3.2. The initial 17.3.2 release misses SLUP configuration menu in the WLC WebUI, which was introduced with the 17.3.3 release. The SLUP is different from traditional smart licensing in couple of ways:

- WLC now communicates with Cisco License Central through the smartreceiver.cisco.com domain, instead of the tools.cisco.com domain.
- Instead of Registering, the WLC now Establishes Trust with the Cisco License Central or On-prem.
- CLI commands have been slightly altered.

- There is no Smart Licensing Reservation (SLR) anymore. Instead you can periodically report your usage manually.

Warning: If you are using a Cisco Catalyst 9800-CL Wireless Controller, ensure that you are familiar with the mandatory ACK requirement that starts with Cisco IOS® XE Cupertino 17.7.1. See RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller.

Configuration

Direct Connect Cisco License Central

Once the token has been created on the Cisco License Central, in order to establish trust, these commands need to be executed.

Note: Token Max. Number of Uses count must be at least 2 in a case of WLC in HA SSO.

```
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
```

- The **ip http client source-interface** command specifies the L3 interface that licensing related packets are going to be sourced from.
- The **ip http client secure-trustpoint** command specifies which trustpoint/certificate is used for Cisco License Central communication. The trustpoint name can be found using the **show crypto pki trustpoints** command. It is recommended to use a self-signed cert **TP-self-signed-xxxxxxxxxx** certificate or Manufacturer Installed Certificate (also known as MIC, available only on 9800-40, 9800-80 and 9800-L), usually called **CISCO_IDEVID_SUDI**.
- **Terminal monitor** command makes the WLC print the logs to the console and help confirm that trust has been successfully established. It can be disabled using terminal no monitor.
- Keyword **all** in the last command tells tells all of the WLCs in the HA SSO cluster to establish the trust with the Cisco License Central.
- Keyword **force** tells the WLC to override any of the previously established trusts and attempt a new one.

Note: If the trust is not being established, the 9800 tries again 1 minute later after the command is executed and then does not try again for some time. Enter the token command again to force a new

---

trust establishment.

Connected to CSLU

Cisco Smart License Utility Manager (CSLU) is a Windows-based application (also available on Linux) that enables customers to administer licenses and their associated Product Instances from their premises instead of having to directly connect their Smart Licensed enabled Product Instances to Cisco License Central.

This section only covers the 9800 Wireless configuration. There are others steps to perform to configure licensing with CSLU (such as install CSLU, configure the CSLU software and so on), which is covered in the Configuration Guides .Whether you want to implement a product instance-initiated or CSLU-initiated method of communication, or complete the corresponding sequence of tasks.

Product Instance-initiated

1. Ensure network reachability from the controller to CSLU.
2. Ensure that transport type is set to **cslu**:

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

3. If you want CSLU to be discovered by the controller, you need to perform the action. If you want CSLU to be discovered using DNS, no action is required. If you want to discover it using an URL, please enter these command:

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

CSLU-initiated

When you configure CSLU-initiated communication, the only action needed is to check for and ensure network reachability to CSLU from the controller.

Connected to Cisco License Central On-prem

Configuration with On-prem Cisco License Central is fairly similar to direct connection. On-prem needs to run version 8-202102 or newer. For SLUP releases (17.3.2 and later), it is advised to use the CSLU URL and transport type. The URL can be obtained from the On-prem webUI interface under **Smart Licensing** > **Inventory** > <**Virtual Account**> > **General** section.

```
configure terminal
 ip http client source-interface <interface>
 ip http client secure-trustpoint <TP>
 license smart transport cslu
 license smart url cslu http://<SSMOn-PremIP>/cslu/v1/pi/<tenantID> (see previous paragraph on how to g
 crypto pki trustpoint SLA-TrustPoint
  revocation-check none
 exit
write memory
terminal monitor
```

On-prem Cisco License Central does not require the use of a trust token.



Note: If you are getting the message, %PKI-3-CRL_FETCH_FAIL: CRL fetch for trustpoint SLA-TrustPoint failed, it is because you have not configured revocation-check none under the SLA-TrustPoint. This is the trustpoint used for Smart Licensing. In case of On-prem, the certificate on the licensing server is most often a self-signed certificate for which CRL verification is not possible, hence the requirement to configure no revocation checks.

Configuring Smart Transport Through an HTTPS Proxy



Note: Authenticated proxies are not yet supported as of code release 17.9.2. If you are using authenticated proxies in your infrastructure, consider using the Cisco Smart License Utility Manager (CSLU), it supports this type of servers.

To use a proxy server to communicate with Cisco License Central when using the Smart transport mode, complete these steps:

```
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
```

Communication Frequency

The reporting interval you can configure in CLI or GUI has no effect.

The 9800 WLC communicates with Cisco License Central or On-prem every 8 hours, no matter what reporting interval is configured via web interface or CLI. This means that newly joined access points can appear on Cisco License Central up to 8 hours after they initially joined.

You can figure out the next time licenses are calculated and reported with the **show license air entities summary** command. This command is not part of the typical **show tech** or **show license all** output:

<#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
```

License Factory Reset

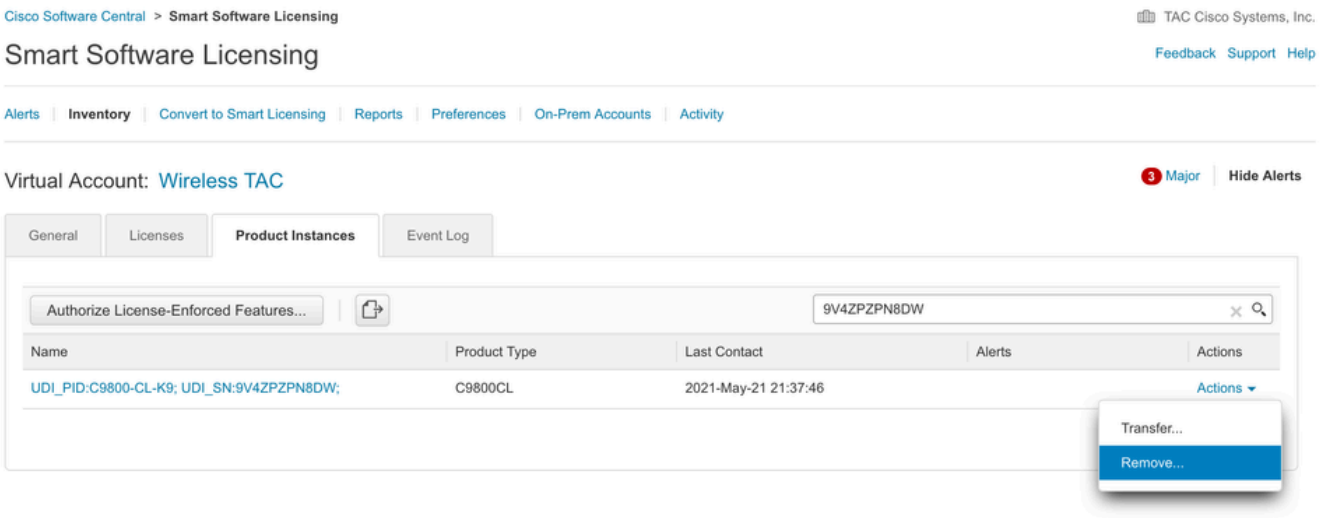
Catalyst 9800 WLC can have all of its licensing configuration and trust factory reset and still keep all the other configurations. This requires a WLC reload:

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

It is important to note that after a license factory reset, you need to wait one hour before licensing the WLC again in case it is in AirGap mode.

In Case of RMA or Hardware Replacement

If the 9800 WLC needs to be replaced, the new device has to register with Cisco License Central/On-prem and it is perceived as a new device. Releasing the license count of the previous device requires manual deletion under **Product Instances**:



Upgrading From Specific License Registration (SLR)

Older WLC releases, earlier than 17.3.2, used a special offline licensing method called Specific License Registration (SLR). This licensing method has been deprecated in the releases using SLUP (17.3.2 and later).

If you upgrade a 9800 controller that was using SLR to a release post 17.3.2 or 17.4.1, it is recommended that you move to offline SLUP reporting rather than relying on the SLR commands. Save the license usage RUM file and register that with the Smart Licensing Portal. Since SLR does not exist anymore in newer releases, this reports the correct license count and releases any unused license. Licenses are not blocked anymore but the exact usage count is reported.

Troubleshooting

Internet Access, Port Checks & Pings

Instead of the tools.cisco.com that traditional smart licensing used, the new SLUP uses smartreceiver.cisco.com domain to establish trust. At the time of writing of this article, this domain resolves to multiple different IP addresses. Not all of this addresses are pingable. Pings **must not** be used as an internet reachability test from WLC. Not being able to ping these servers does not mean that they are not working properly.

Instead of pings, telnet over port 443 must be used as a reachability test. Telnet can be checked either against smartreceiver.cisco.com domain or directly against the server IP addresses. If traffic is not being blocked, port must show up as open in the output:

```
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

If **terminal monitor** command is enabled while the token is being configured, the WLC prints out the relevant logs in the CLI. These messages can also be obtained if you run the **show logging** command. Logs of a successfully established trust looks like this:

```
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
```

Logs of a WLC without a defined DNS server or with a nonfunctioning DNS server:

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

In this case verify that you have a valid DNS server configured. Feel free to use any public DNS server IP available :

```
ip name-server <ip address>
```

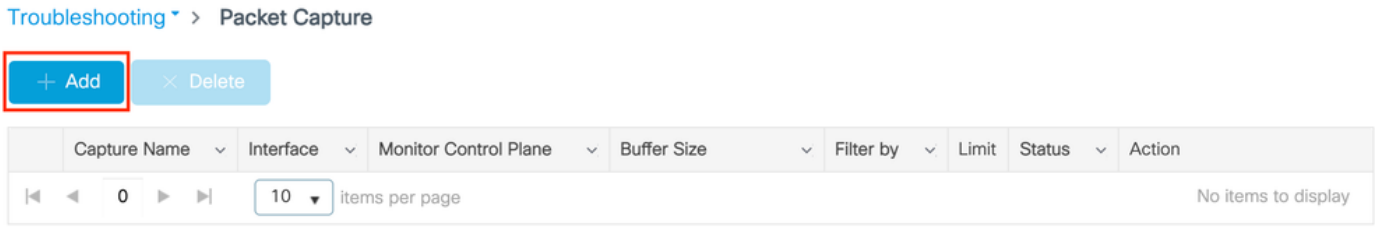
Logs of a WLC with a functioning DNS server, but without internet access:

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

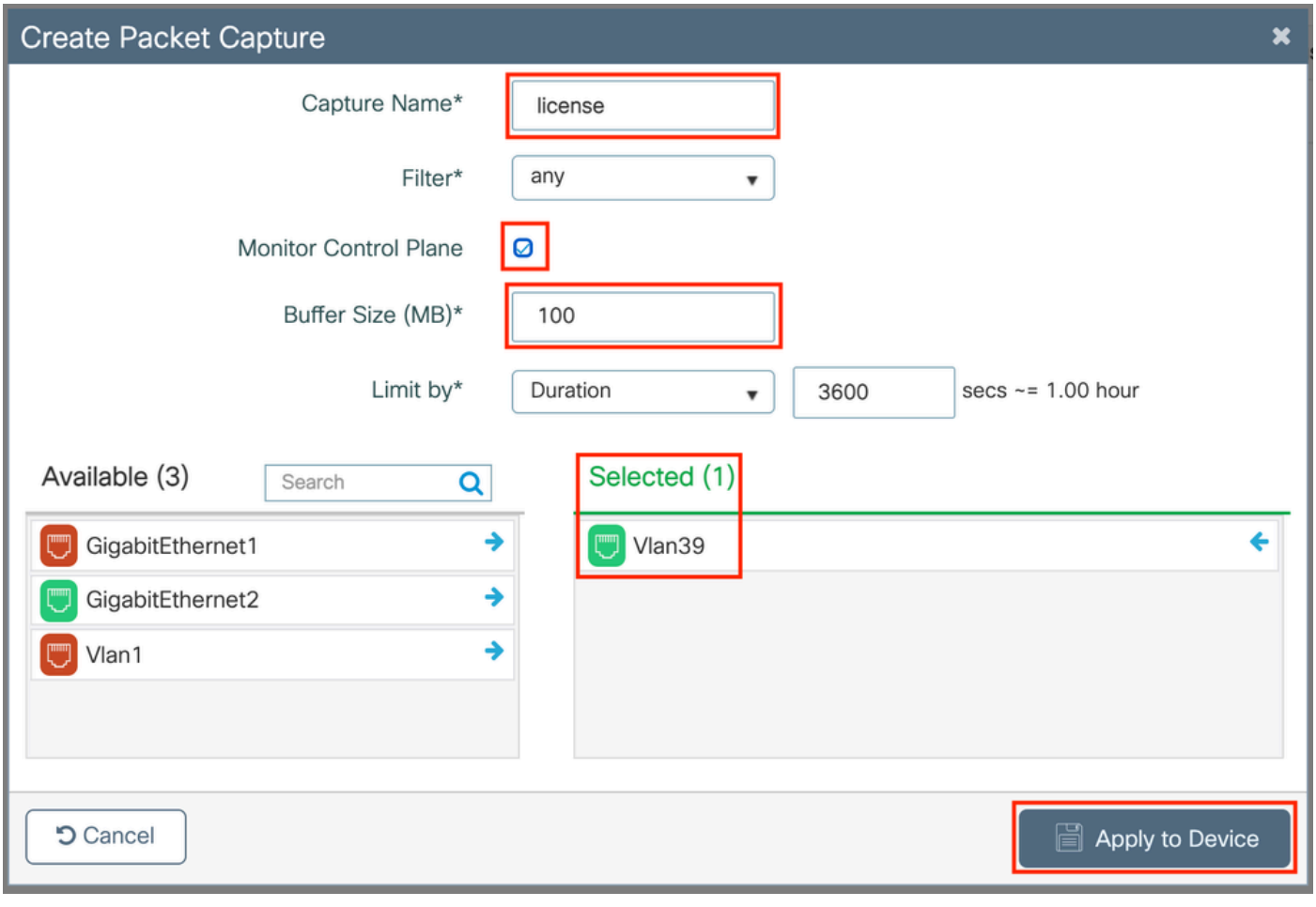
Packet Captures

Even though communication between WLC and Cisco License Central/On-prem is encrypted and going over HTTPS, performing packet captures can reveal what causes the trust not to be established. The easiest way to collect packet captures is through the WLC Web interface.

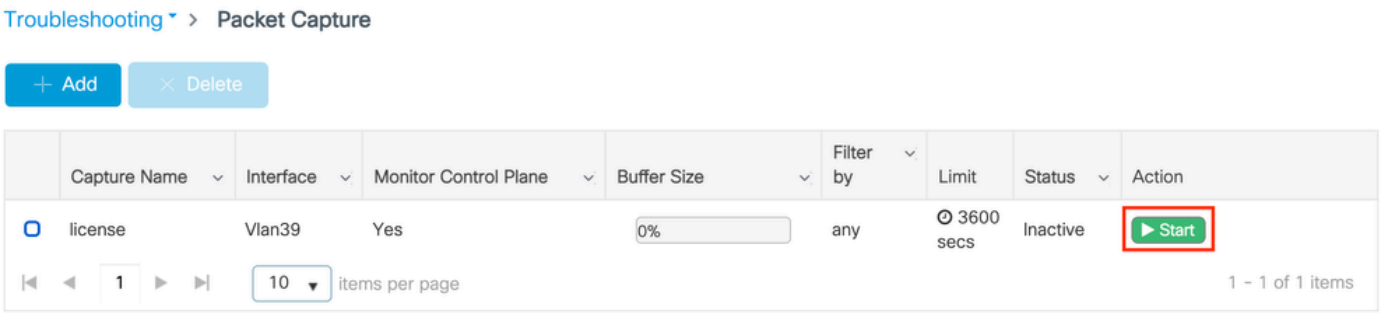
Navigate to **Troubleshooting** > **Packet Capture**. Create a new capture point:



Ensure that **Monitor Control Plane** checkbox is enabled. Increase the buffer size to the maximum 100MB. Add the interface which must be captured. Smart licensing traffic is sourced out of the wireless management interface by default or from the interface defined with the **ip http client source-interface** command:



Start the captures and run the **license smart trust idtoken <token> all force** command:



The packet captures of a trust establishment must contain these steps:

1. TCP session establishment using SYN, SYN-ACK & ACK sequence
2. TLS session establishment with both server and client certificate exchange. Establishment ends with the **New Session Ticket** packet
3. Encrypted packet exchange (**Application Data** frames) where WLC reports license usage
4. TCP session termination via FIN-PSH-ACK, FIN-ACK & ACK sequence

---

Note: The packet captures contain a lot more frames, including multiples of TCP window update and **Application Data** frames

---

Since Cisco License Central Cloud uses 3 different public IP addresses, in order to filter out all of the packet captures between WLC and Cisco License Central, use these wireshark filter:

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

If using an On-prem Cisco License Central, filter for the Cisco License Central IP address:

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

Example: Packet captures of a successful trust establishment with directly connected Cisco License Central with all of the significant packet captures filtered:

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 Commands

These **show** commands contain useful information about trust establishment:

```
show license status
show license summary
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)
```

The **show license history message** command is one of the more useful commands since it can display the actual messages sent from WLC and received back from Cisco License Central.

A successful trust establishment has both "REQUEST: Aug 23 10:18:08 2021 Central" and "RESPONSE: Aug 23 10:18:10 2021 Central" messages printed. If there is nothing after the RESPONSE line, that means that the WLC did not receive a response from the Cisco License Central.

This is an example of a **show license history message** output for a successful trust establishment:


```
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":"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}
```


Debugs/btrace

Run this command a few minutes after a trust establishment has been attempted using a **license smart trust idtoken all force** command. IOSRP logs are extremely verbose. Append | include smart-agent" to the command to get only smart licensing logs.

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

You can also run these debugs and then reconfigure the licensing commands to force a new connection:

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

Common Issues

WLC Has No Internet Access or Firewall Blocks/alters Traffic

Embedded packet captures on the WLC are an easy way to see if WLC receives anything back from the Cisco License Central or On-prem. If there was no response, chances are that the firewall is blocking something.

The **show license history message** command prints an empty response 1 second after the request is sent out if **no response** was received from the Cisco License Central Cloud or On-prem.

For example, this can lead you to believe that an empty response was received, but in reality there was no response at all:

```
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
```

Note: There is currently an enhancement request Cisco bug ID CSCvy84684 that makes show license history message print an empty response when there are no response. This is to enhance the output of the **show license history message** command

---

Unknown CA Alert in Packet Captures

Communication with Cisco License Central or On-prem requires a decent certificate on the 9800 side. It can be self-signed, but it cannot be invalid or expired. In such a case, a packet capture shows a TLS alert for **unknown CA** sent by Cisco License Central when the 9800 HTTP client certificate has expired.

Smart licensing uses the **ip http client** configuration, which is different from the **ip http server** that WLC Web interface uses. This means that these commands need to be configured properly:

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

The trustpoint name can be found with the **show crypto pki trustpoints** command. It is recommended to use a self signed cert **TP-self-signed-xxxxxxxxxx** certificate or Manufacturer Installed Certificate (MIC) which is usually called **CISCO_IDEVID_SUDI** and is available only on 9800-80, 9800-40 and 9800-L.

It is important to note that devices that do TLS interception, such as a firewall with the SSL decrypt feature, can prevent the C9800 from establishing a successful handshake with the Cisco Licensing server as the HTTPS certificate presented is the firewall certificate instead of the Cisco Licensing server certificate.



Note: Make sure you configure both source-interface and secure-trustpoint commands. A source-interface command is needed even if WLC has only one L3 interface.

Related Information

- Smart Licensing with Air Gap mode on 9800
- Cisco Technical Support & Downloads