

Configurazione di & Risoluzione dei problemi di Catalyst 9800 Smart Licensing con SLUP

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Licenze tradizionali e SLUP](#)

[Configurazione](#)

[CSSM Direct Connect](#)

[Connesso a CSLU](#)

[Avviato dall'istanza del prodotto](#)

[avviata da CSLU](#)

[Connesso a SSM locale](#)

[Configurazione di Smart Transport tramite un proxy HTTPS](#)

[Frequenza di comunicazione](#)

[Reset License Factory](#)

[In caso di RMA o sostituzione hardware](#)

[Aggiornamento da SLR \(Specific License Registration\)](#)

[Risoluzione dei problemi](#)

[Accesso a Internet, verifiche delle porte e ping](#)

[Syslog](#)

[Acquisizioni pacchetti](#)

[Comandi show](#)

[Debug/btrace](#)

[Problemi comuni](#)

[Il WLC non ha accesso a Internet o il firewall blocca/altera il traffico](#)

[Avviso CA sconosciuto nelle acquisizioni pacchetti](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare Smart Licensing con criteri (SLUP) e risolvere i relativi problemi su Catalyst 9800 Wireless LAN Controller (WLC) .

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

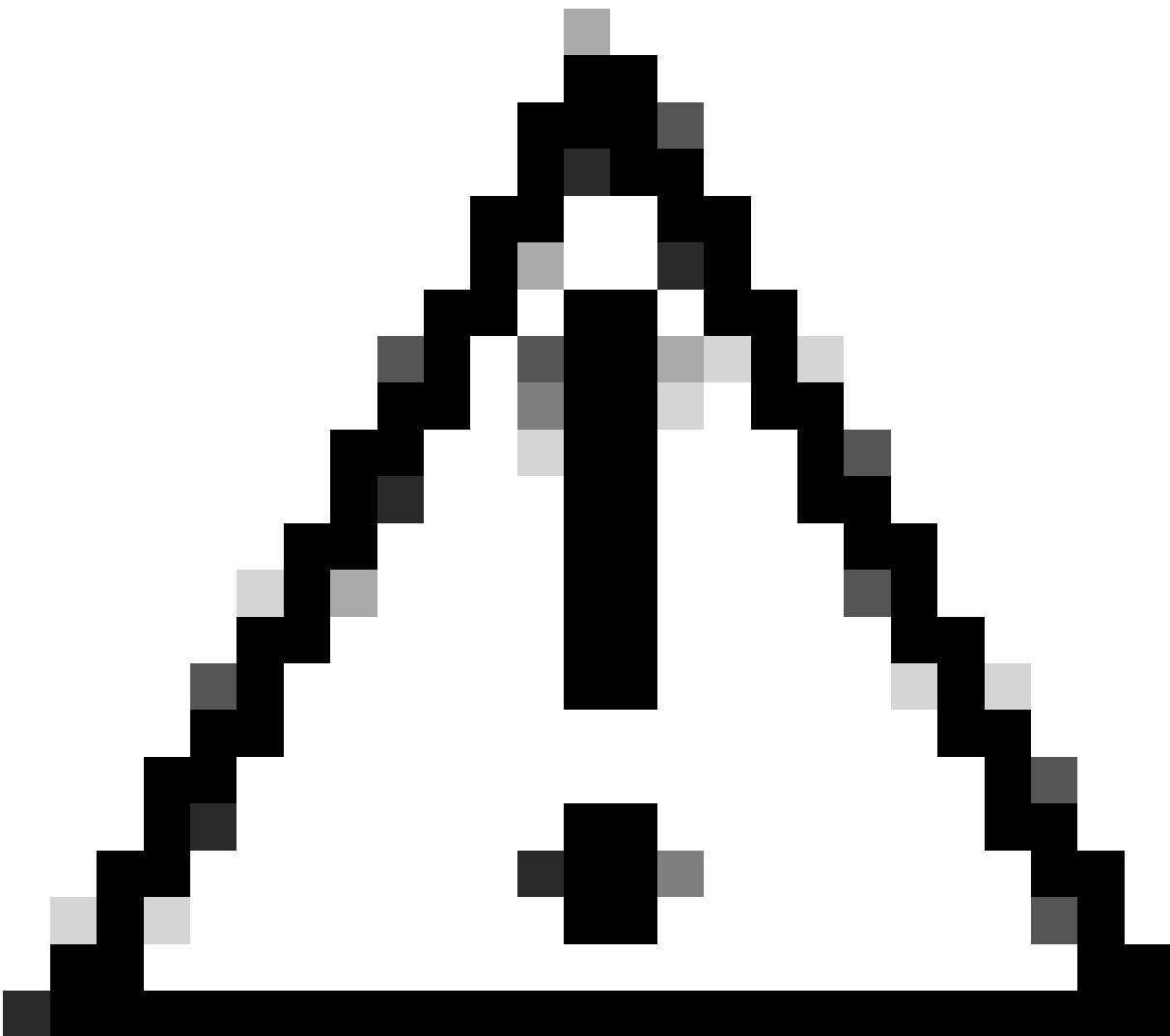
- Criteri di utilizzo delle licenze Smart (SLUP)
- Catalyst 9800 Wireless LAN Controller (WLC)

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

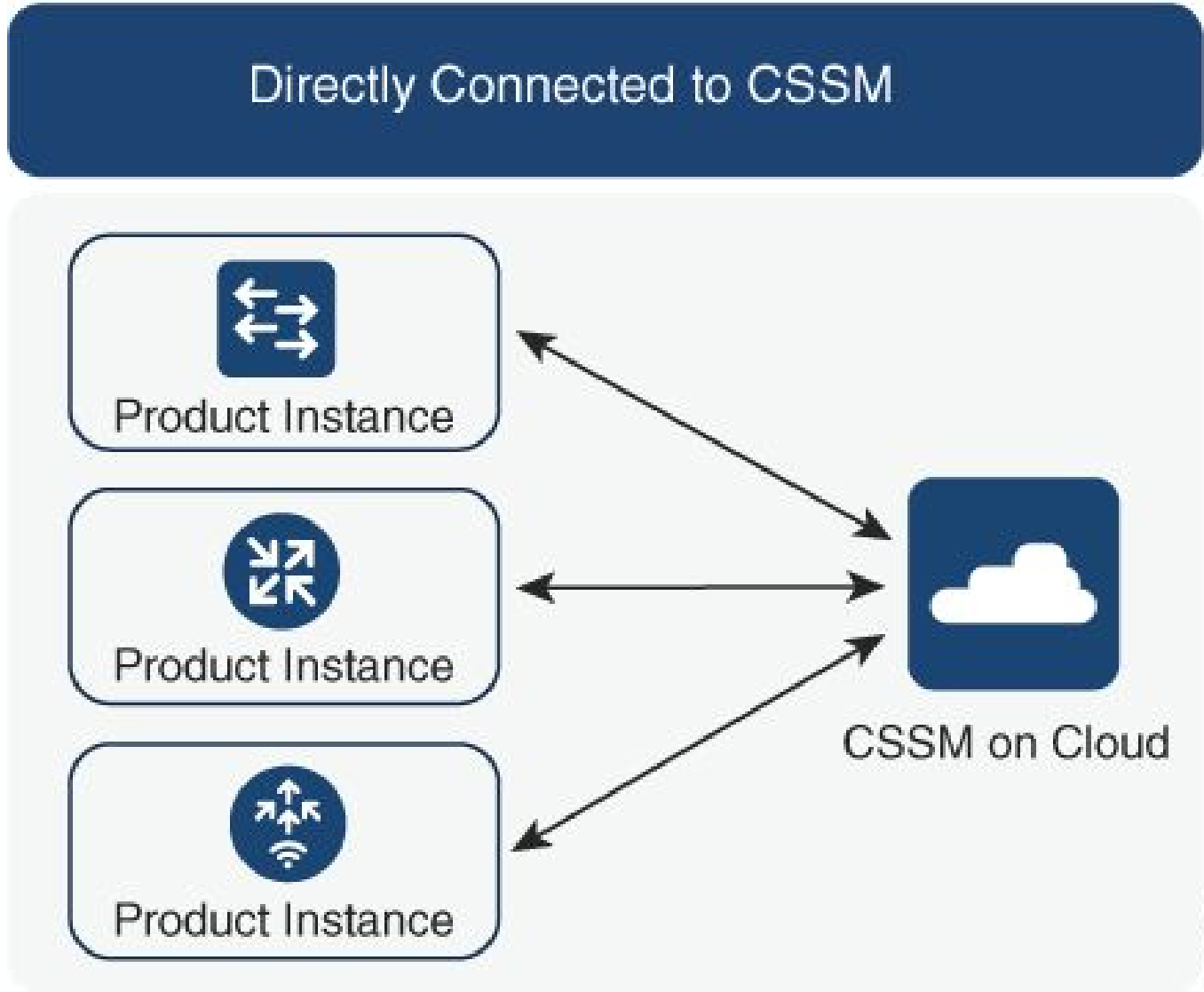
Premesse



Attenzione: le note di questo articolo contengono utili suggerimenti o riferimenti a materiale non trattato nel documento. Si consiglia di leggere ogni nota.

1. Connessione diretta a [Cisco Smart Software Manager](#) Cloud (CSM Cloud)
2. Connesso a CSM tramite [CSLU](#) (Cisco Smart License Utility Manager)
3. Connesso a CSM tramite [Smart Software Manager locale](#) (SSM locale)

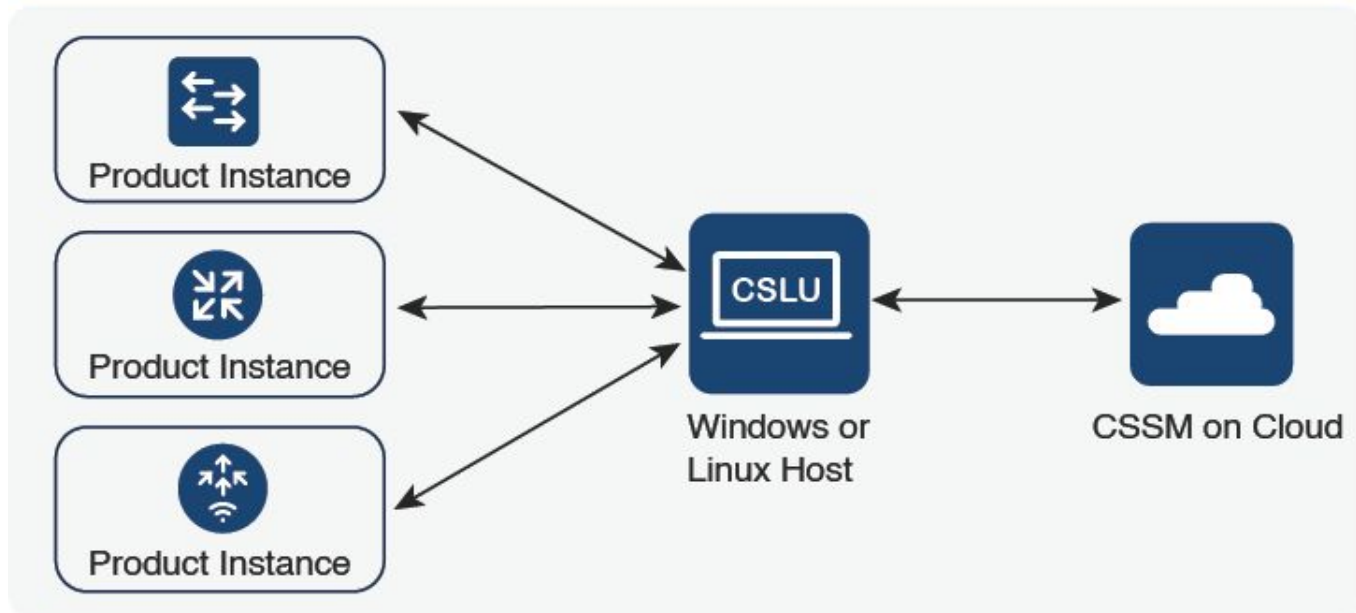
In questo articolo non vengono illustrati tutti gli scenari relativi alle licenze Smart su Catalyst 9800. Per ulteriori informazioni, consultare la [guida alla configurazione delle licenze Smart](#) tramite i [criteri](#). Tuttavia, questo articolo fornisce una serie di utili comandi per risolvere i problemi di connessione diretta, CSLU e licenze SSM Smart in locale che usano i problemi di policy su Catalyst 9800.



356794

Opzione 1. Connessione diretta a server cloud Cisco Smart Licensing (CSM)

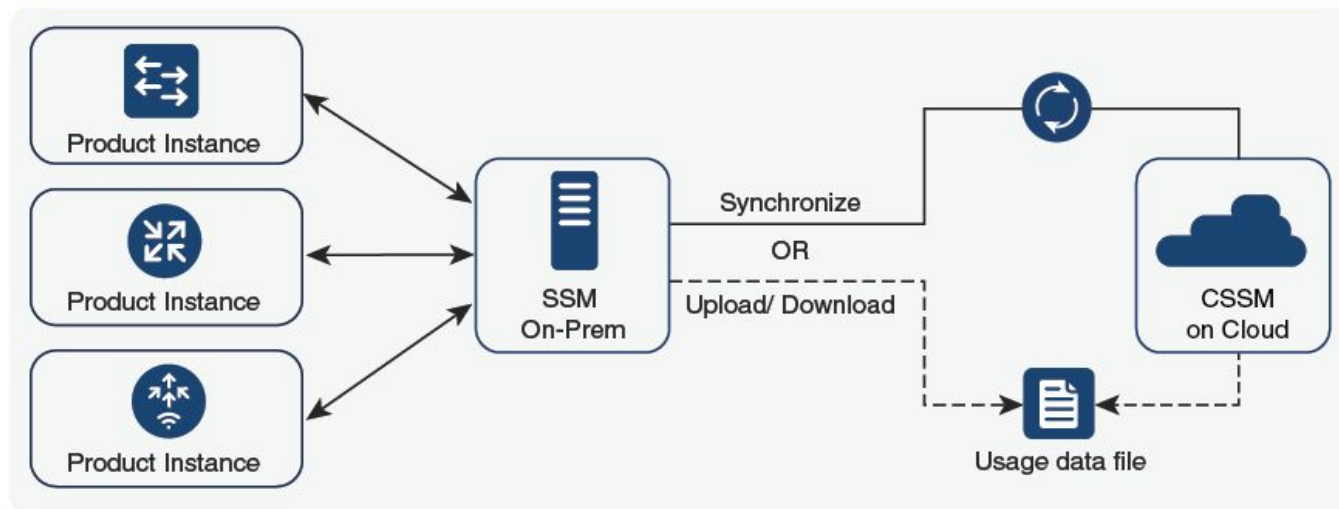
Connected to CSSM Through CSLU



356791


Opzione 2. Connessione tramite CSLU

SSM On-Prem Deployment



357508

Opzione 3. Connessione tramite Smart Software Manager locale (SSM locale)

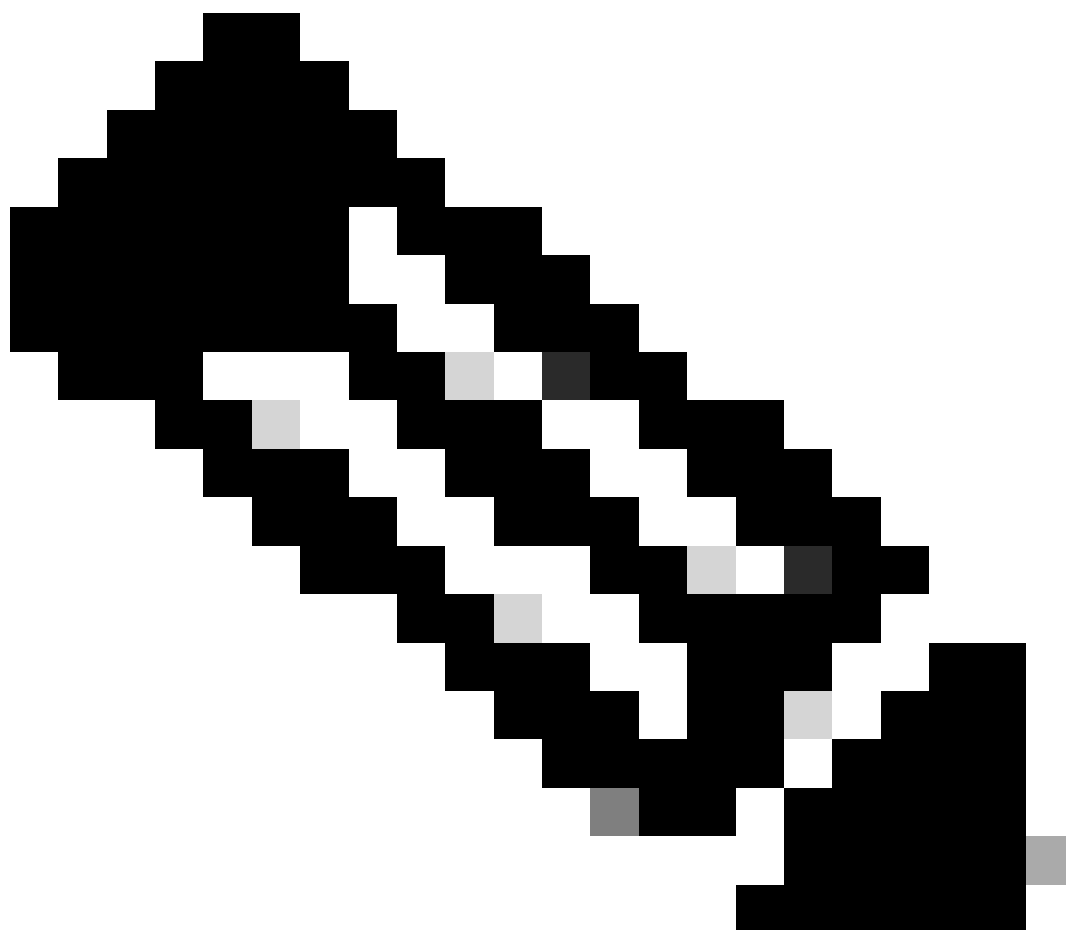
 Nota: tutti i comandi menzionati in questo articolo sono applicabili solo ai WLC con versione 17.3.2 o successive.

Licenze tradizionali e SLUP

La funzionalità Smart Licensing Using Policy è stata introdotta in Catalyst 9800 con la versione di codice 17.3.2. Nella versione 17.3.2 iniziale non è presente il menu di configurazione SLUP nel

WebUI del WLC, introdotto con la versione 17.3.3. La SLUP è diversa dalle licenze intelligenti tradizionali in due modi:

- WLC comunica ora con CSM tramite il dominio smartreceiver.cisco.com, anziché tramite il dominio tools.cisco.com.
 - Anziché registrarsi, il WLC ora stabilisce un trust con il CSM o l'SSM locale.
 - i comandi CLI sono stati leggermente modificati.
 - SLR (Smart Licensing Reservation) non è più disponibile. È invece possibile segnalare periodicamente l'utilizzo manualmente.
 - Non è più disponibile una modalità di valutazione. Il WLC continua a funzionare a piena capacità anche senza licenza. Il sistema è basato sull'onore e l'utente è tenuto a segnalare periodicamente l'utilizzo della licenza (in modo automatico o manuale in caso di reti con airgapped).
-




Avviso: se si usa un controller wireless Cisco Catalyst 9800-CL, verificare di conoscere i requisiti obbligatori dell'ACK che iniziano con Cisco IOS® XE Cupertino 17.7.1. Vedere [Requisito per la segnalazione e la conferma della gestione RUM per Cisco Catalyst 9800-CL Wireless Controller](#).

Configurazione


CSSM Direct Connect

Dopo aver creato il token sul CSM, per stabilire la fiducia, è necessario eseguire questi comandi:

 Nota: Token Max. Il numero di utilizzi deve essere almeno 2 in un caso di 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
```

- Il comando `ip http client-interface` specifica l'interfaccia L3 da cui verranno originati i pacchetti correlati alle licenze
- Il comando `ip http client secure-trustpoint` specifica il trust point/certificato utilizzato per la comunicazione CSM. Il nome del trust point può essere trovato utilizzando il comando `show crypto pki trustpoints`. Si consiglia di utilizzare un certificato autofirmato `TP-xxxxxxxxxx` o un certificato installato dal produttore (noto anche come MIC, disponibile solo su 9800-40, 9800-80 e 9800-L), generalmente denominato `CISCO_IDEVID_SUDI`.
- Il comando `Terminal Monitor` consente al WLC di stampare i registri sulla console e di verificare che la relazione di trust sia stata stabilita correttamente. Può essere disattivato usando il terminale sul monitor.
- La parola chiave `all` nell'ultimo comando indica a tutti i WLC nel cluster HA SSO di stabilire la relazione di trust con il CSM.
- La forza della parola chiave indica al WLC di ignorare una qualsiasi delle relazioni di trust precedentemente stabilite e tentarne una nuova.

 Nota: se il trust non viene stabilito, lo switch 9800 riprova 1 minuto dopo, dopo che il comando è stato eseguito, e non riprova per qualche tempo. Immettere nuovamente il comando `token` per forzare una nuova definizione di trust.

Connesso a CSLU

Cisco Smart License Utility Manager (CSLU) è un'applicazione basata su Windows (disponibile anche in Linux) che consente ai clienti di amministrare le licenze e le istanze del prodotto associate dalla propria sede anziché dover connettere direttamente le proprie istanze del prodotto con licenza Smart a Cisco Smart Software Manager (CSSM).

Questa sezione riguarda solo la configurazione wireless 9800. Per configurare la licenza con CSLU, è necessario eseguire altri passaggi (ad esempio, installare CSLU, configurare il software CSLU e così via), descritti nelle [Guide alla configurazione](#). Se si desidera implementare un metodo di comunicazione avviato dall'istanza del prodotto o da CSLU oppure completare la sequenza di attività corrispondente.

Avviato dall'istanza del prodotto

1. Garantire la raggiungibilità della rete dal controller alla CSLU
2. Verificare che il tipo di trasporto sia impostato su cslu:

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

3. Se si desidera che la CSLU venga rilevata dal controller, è necessario eseguire l'azione. Se si desidera individuare la CSLU utilizzando il DNS, non è necessaria alcuna azione. Se si desidera individuarlo utilizzando un URL, immettere questi comandi:

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

avviata da CSLU

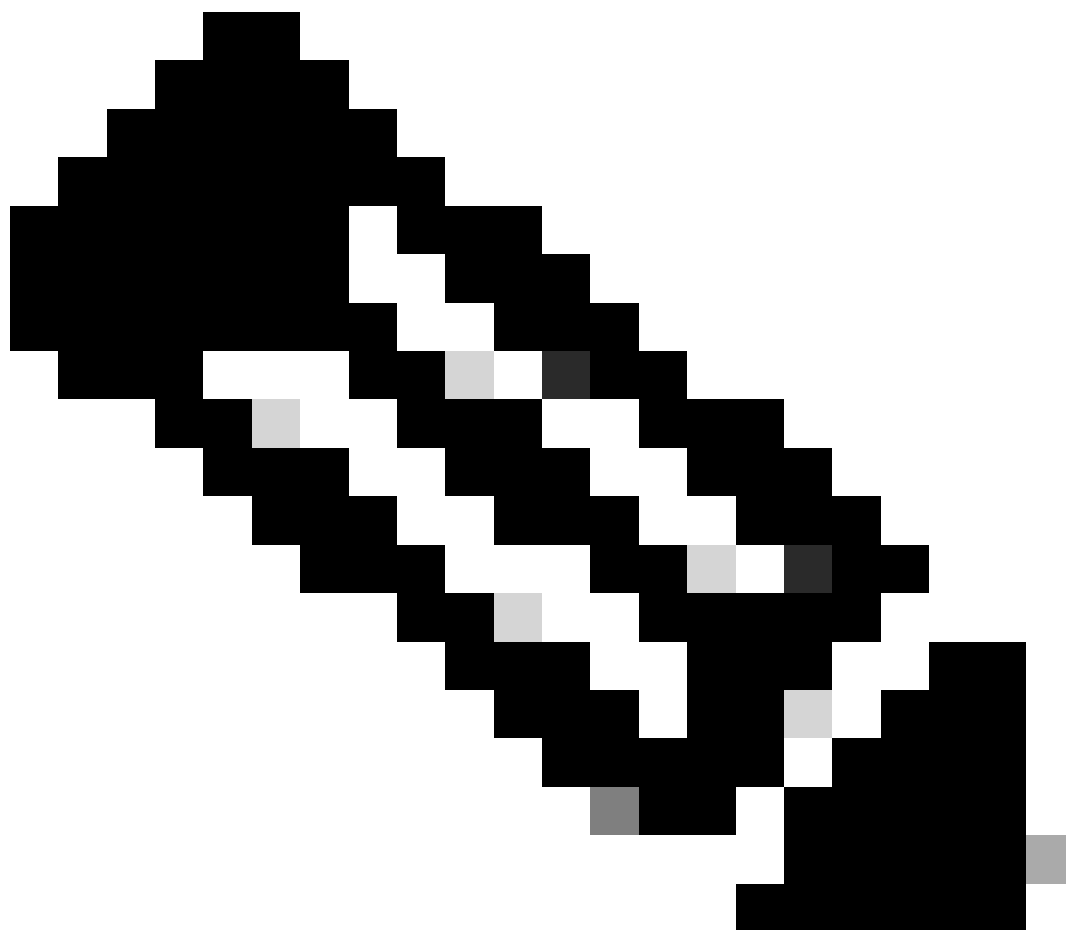
Quando si configura la comunicazione avviata dalla CSLU, l'unica azione necessaria è verificare la presenza di CSLU e garantire la raggiungibilità della rete da parte del controller.

Connesso a SSM locale

La configurazione con SSM locale è simile alla connessione diretta. È necessario eseguire on-prem la versione 8-202102 o successiva. Per le versioni SLUP (17.3.2 e successive), si consiglia di utilizzare l'URL CSLU e il tipo di trasporto. L'URL può essere ottenuto dall'interfaccia WebUI locale nella sezione **Smart Licensing > Inventario > <Account virtuale> Generale**.

```
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
```

SSM locale non richiede l'utilizzo di un token di attendibilità.



Nota: se viene visualizzato il messaggio %PKI-3-CRL_FETCH_FAIL: Recupero CRL per SLA-TrustPoint del trust point non riuscito. Non è stato configurato alcun controllo di revoca in SLA-TrustPoint. Questo è il trust utilizzato per Smart Licensing. Nel caso di un certificato locale, il certificato sul server di licenze è spesso un certificato autofirmato per il quale non è possibile eseguire la verifica CRL. Di conseguenza, non è necessario configurare alcun controllo delle revoche.

Configurazione di Smart Transport tramite un proxy HTTPS



Nota: i proxy autenticati non sono ancora supportati dalla versione 17.9.2 del codice. Se si utilizzano proxy autenticati nell'infrastruttura, si consiglia di utilizzare [Cisco Smart License Utility Manager \(CSLU\)](#) per il supporto di questo tipo di server.

Per utilizzare un server proxy per comunicare con CSM quando si utilizza la modalità di trasporto intelligente, attenersi alla seguente procedura:

```
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
```

Frequenza di comunicazione

L'intervallo di report che è possibile configurare nella CLI o nella GUI non ha alcun effetto.

9800 WLC comunica con CSM o con Smart Software Manager in locale ogni 8 ore, indipendentemente dall'intervallo di reporting configurato tramite interfaccia Web o CLI. Ciò significa che i punti di accesso appena aggiunti possono essere visualizzati sul CSM fino a 8 ore dopo l'iniziale aggiunta.

Per individuare la prossima volta che le licenze vengono calcolate e segnalate, usare il comando `show license air entities summary`. Questo comando non fa parte dell'output tipico di `show tech` o `show license all`:

<#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
```

Reset License Factory

Catalyst 9800 WLC può avere tutta la configurazione della licenza e il trust factory reimpostato e mantenere tutte le altre configurazioni. È necessario un ricaricamento WLC:

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

In caso di RMA o sostituzione hardware

Se il WLC 9800 deve essere sostituito, il nuovo dispositivo deve essere registrato con CSM/On-Prem Smart Software Manager e viene percepito come un nuovo dispositivo. Per rilasciare il numero di licenze del dispositivo precedente, è necessario eseguire l'eliminazione manuale in Istanze prodotto:

Smart Software Licensing

Alerts | Inventory | Convert to Smart Licensing | Reports | Preferences | On-Prem Accounts | Activity

Virtual Account: [Wireless TAC](#)

3 Major | Hide Alerts

The screenshot shows the 'Product Instances' tab in the Cisco Software Central interface. At the top, there are tabs for 'General', 'Licenses', 'Product Instances', and 'Event Log'. Below the tabs, there is a search bar with the text 'Authorize License-Enforced Features...' and a search icon. To the right of the search bar, there is a search input field containing '9V4ZP2PN8DW'. Below the search bar, there is a table with the following columns: 'Name', 'Product Type', 'Last Contact', 'Alerts', and 'Actions'. The table contains one row with the following data: 'UDI_PID:C9800-CL-K9; UDI_SN:9V4ZP2PN8DW', 'C9800CL', '2021-May-21 21:37:46', and 'Actions'. A dropdown menu is open under the 'Actions' column, showing two options: 'Transfer...' and 'Remove...'.

Aggiornamento da SLR (Specific License Registration)

Nelle versioni precedenti, precedenti alla 17.3.2, veniva usato uno speciale metodo di licenza offline chiamato SLR (Specific License Registration). Questo metodo di licenza è stato deprecato nelle versioni che usano SLUP (17.3.2 e versioni successive).

Se si aggiorna un controller 9800 che utilizzava SLR a una versione successiva alla 17.3.2 o alla 17.4.1, si consiglia di passare al reporting SLUP offline anziché basarsi sui comandi SLR. Salvare il file RUM relativo all'utilizzo della licenza e registrarlo sul portale delle licenze Smart. Poiché SLR non esiste più nelle nuove versioni, questo comando indica il numero di licenze corretto e rilascia tutte le licenze non utilizzate. Le licenze non vengono più bloccate, ma viene visualizzato il numero esatto di utilizzi.

Risoluzione dei problemi

Accesso a Internet, verifiche delle porte e ping

Anziché il `tools.cisco.com` utilizzato dalle licenze intelligenti tradizionali, il nuovo SLUP utilizza il dominio `smartreceiver.cisco.com` per stabilire la relazione di trust. Al momento della stesura di questo articolo, il dominio viene risolto in più indirizzi IP diversi. Non è possibile eseguire il ping di tutti gli indirizzi. I ping non devono essere utilizzati come test di raggiungibilità su Internet dal WLC. Il fatto di non poter eseguire il ping di questi server non significa che non funzionino correttamente.

Per verificare la raggiungibilità, usare telnet over porta 443 anziché i ping. Telnet può essere confrontato con il dominio `smartreceiver.cisco.com` o direttamente con gli indirizzi IP del server. Se il traffico non viene bloccato, la porta deve apparire come aperta nell'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

Se il comando terminal monitor è abilitato mentre il token è in fase di configurazione, il WLC stampa i log pertinenti nella CLI. Per visualizzare questi messaggi, è possibile eseguire il comando show logging. I registri di un trust stabilito correttamente hanno il seguente aspetto:

```
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
```

Registri di un WLC senza un server DNS definito o con un server DNS non funzionante:

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

Registri di un WLC con un server DNS funzionante, ma senza accesso a Internet:

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

Acquisizioni pacchetti

Anche se la comunicazione tra WLC e CSSM/SSM in locale è crittografata e passa attraverso HTTPS, l'esecuzione di acquisizioni di pacchetti può rivelare le cause del mancato accertamento del trust. Il modo più semplice per raccogliere le acquisizioni dei pacchetti è tramite l'interfaccia Web WLC.

Selezionare Risoluzione dei problemi > Acquisizione pacchetti. Creare un nuovo punto di acquisizione:

Troubleshooting > Packet Capture

+ Add × Delete

Capture Name	Interface	Monitor Control Plane	Buffer Size	Filter by	Limit	Status	Action
◀ 0 ▶ 10 items per page							No items to display

Verificare che la casella di controllo Controlla piano di controllo sia abilitata. Aumentare le dimensioni del buffer fino a un massimo di 100 MB. Aggiungere l'interfaccia che deve essere acquisita. Il traffico delle licenze Smart viene inviato dall'interfaccia di gestione wireless per

impostazione predefinita o dall'interfaccia definita con il comando `ip http client source-interface:`

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

Avviare le acquisizioni ed eseguire il comando `license smart trust idtoken <token>` all force:

Troubleshooting > Packet Capture

Capture Name	Interface	Monitor Control Plane	Buffer Size	Filter by	Limit	Status	Action
<input checked="" type="checkbox"/> license	Vlan39	Yes	<input type="text" value="0%"/>	any	<input type="text" value="3600"/> secs	Inactive	<input checked="" type="button" value="Start"/>

1 10 items per page 1 - 1 of 1 items

Le acquisizioni di pacchetti di uno stabilimento di attendibilità devono contenere i seguenti passaggi:

1. Sessione TCP stabilita tramite SYN, SYN-ACK e sequenza ACK
2. Sessione TLS stabilita con scambio di certificati sia server che client. L'installazione termina con il pacchetto New Session Ticket
3. Encrypted packet exchange (Application Data frames) dove WLC segnala l'utilizzo della licenza
4. Fine sessione TCP tramite sequenza FIN-PSH-ACK, FIN-ACK e ACK

Nota: le acquisizioni dei pacchetti contengono molti più frame, inclusi multipli di

aggiornamenti di finestre TCP e frame di dati applicazioni

Poiché CSM Cloud usa 3 diversi indirizzi IP pubblici, per filtrare tutte le acquisizioni di pacchetti tra WLC e CSM, usare questo filtro wireshark:

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

Se si utilizza un SSM locale, filtrare l'indirizzo IP del SSM:

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

Esempio: acquisizioni di pacchetti di una relazione di trust stabilita con CSM con connessione diretta con tutte le acquisizioni di pacchetti significative filtrate:

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

Comandi show

I comandi show riportati di seguito contengono informazioni utili sulla definizione del trust:

```
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)
```

Il comando `show license history message` è uno dei comandi più utili in quanto può visualizzare i messaggi effettivi inviati dal WLC e ricevuti nuovamente dal CSM.

Per una relazione di trust stabilita correttamente vengono stampati sia messaggi "RICHIESTA: 23 ago 10:18:08 2021 centrale" che messaggi "RISPOSTA: 23 ago 10:18:10 2021 centrale". Se non vi è nulla dopo la riga RESPONSE, significa che il WLC non ha ricevuto una risposta dal CSM.

Questo è un esempio di output del messaggio show license history per un trust stabilito correttamente:

```
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_identfier":"","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":"NB"},"timestamp":1629713888600,"nonce":"11702702165338740293","product_instance_identfier":"original_request_type":"LICENSE_USAGE","original_pid":"2e84a42f-c903-44c5-83b2-e62e258c780f","signature":{"type":"SHA256","key":"59152896","value":"eiJ7IuQaTCFxgUkwls76WZxa5DRI5A0gMqQd5POU6VNSH2j9dHco4T1NJ/aCmBR1MRmkfxyVSWsx41mjJL1mp0Si3ZS4FBMv1F/EBOUfowREe2oz21rQp1cAFpPn5S1aFezW/Nu6SQZfIW+IdF+2qnJeNFAIZbNpgOB5d5HIJvDmDIvDu3bMRHhQAWr2KKzGFr6jPz0hs7bGY/+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==","pid":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_identfier":["DLC","AppHA","EXPORT_2","POLICY_USAGE","UTILITY"],"additional_info":"","signing_cert_serial_number":"59152896","product_instance_identfier":"","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}}
```

Debug/btrace

Eseguire questo comando pochi minuti dopo il tentativo di stabilire un trust con un comando license smart trust idtoken all force. I registri IOSRP sono estremamente dettagliati. Aggiungi | include smart-agent" al comando per ottenere solo i log delle licenze smart.

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

È inoltre possibile eseguire questi debug e quindi riconfigurare i comandi di gestione licenze per forzare una nuova connessione:

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

Problemi comuni

Il WLC non ha accesso a Internet o il firewall blocca/altera il traffico

Le acquisizioni dei pacchetti incorporati sul WLC sono un modo facile per vedere se il WLC riceve qualcosa dal CSM o dal SSM in locale. Se non è stata ricevuta alcuna risposta, è possibile che il firewall stia bloccando qualcosa.


Il comando `show license history message` stampa una risposta vuota 1 secondo dopo l'invio della richiesta se non è stata ricevuta alcuna risposta dal cloud CSM o dal modulo di gestione del servizio di archiviazione locale.

Ad esempio, questo può indurvi a credere che sia stata ricevuta una risposta vuota, ma in realtà non c'è stata alcuna risposta:

```
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
```

 Nota: una richiesta di miglioramento dell'ID bug Cisco [CSCvy84684](#) fa sì che il messaggio `show license history` venga stampato come risposta vuota in assenza di risposta. In questo modo si migliora l'output del comando `show license history message`

Avviso CA sconosciuto nelle acquisizioni pacchetti

La comunicazione con il modulo CSM o il modulo SSM locale richiede un certificato valido sul lato 9800. Può essere autofirmato, ma non può essere non valido o scaduto. In questo caso, l'acquisizione di un pacchetto mostra un avviso TLS per una CA sconosciuta inviato da CSSM quando il certificato client HTTP 9800 è scaduto.

Smart Licensing utilizza la configurazione del client `http ip`, che è diversa dal server `http ip` utilizzato dall'interfaccia Web WLC. Ciò significa che questi comandi devono essere configurati correttamente:


```
ip http client source-interface <interface>
```

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

Il nome del trust point può essere trovato con il comando `show crypto pki trustpoints`. Si consiglia di utilizzare un certificato autofirmato `TP-xxxxxxxxxxxx` o un certificato di installazione del produttore (MIC), generalmente denominato `CISCO_IDEVID_SUDI` ed disponibile solo sui modelli

9800-80, 9800-40 e 9800-L.

È importante notare che i dispositivi che eseguono l'intercettazione TLS, ad esempio un firewall con la funzione di decrittografia SSL, possono impedire a C9800 di stabilire un handshake con il server licenze Cisco, in quanto il certificato HTTPS presentato è il certificato firewall anziché il certificato del server licenze Cisco.

 Nota: accertarsi di configurare i comandi `source-interface` e `secure-trustpoint`. Un comando `source-interface` è necessario anche se il WLC ha solo un'interfaccia L3.

Informazioni correlate

- [Smart Licensing con modalità Air Gap su 9800](#)
- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).