Informazioni sulle licenze Smart per lo switching Catalyst

Sommario

Introduzione

In questo documento viene descritta la funzionalità Smart Licensing tramite la policy sulle piattaforme di switching Catalyst e la distribuzione supportata.

Scopo

Dalle versioni 17.3.2 e 17.4.1, di Cisco IOS® XE, tutte le piattaforme di switching Catalyst della famiglia per Cat9k supportano un nuovo modello di licenza SLP (Smart Licensing using Policy). Lo scopo di questo documento è comprendere i diversi modelli supportati di implementazione e distribuzione di SLP, principalmente per le installazioni Greenfield.

Criteri di utilizzo di Smart Licensing

Con SLP, il dispositivo ha tutte le licenze 'in uso' immediatamente disponibili. I concetti precedenti, la modalità di valutazione, la registrazione e la prenotazione non sono più disponibili con SLP. Con SLP, l'obiettivo è segnalare le licenze e il loro utilizzo. Le licenze non vengono ancora applicate e i livelli di licenza rimangono invariati. Per le piattaforme dello switch Catalyst, non sono disponibili livelli di licenza soggetti ai controlli per l'esportazione, a eccezione della licenza HSECK9. L'unica modifica riguarda la funzionalità di segnalazione dell'utilizzo e del monitoraggio delle licenze. In questa sezione vengono illustrati in dettaglio la terminologia, i motivi delle modifiche, i nuovi componenti forniti con SLP, CSLU (Cisco Smart Licensing Utility) e il flusso degli ordini dei prodotti.

Terminologia

- CSM o SSM - Cisco Smart Software Manager
- SA - Smart Account
- VA - Account virtuale
- SL - Licenze intelligenti
- PLR - Prenotazione licenza permanente
- SLR - Prenotazione licenze Smart
- PID - ID prodotto
- SCH - Smart Call Home
- PI - Istanze prodotto
- CSLU - Cisco Smart Licensing Utility
- RUM - Misurazione dell'utilizzo delle risorse
- ACK - Riconoscimento
- UDI - Identificazione univoca dispositivo - PID + SN
- SLP - Criteri per l'utilizzo di licenze Smart

Perché questo cambiamento?

Con l'introduzione del modello Smart Licensing di trust and verify, Cisco ha supportato diversi meccanismi di implementazione per registrare e segnalare l'utilizzo delle licenze al CSM. Tuttavia, non era facilmente adattabile a tutti i tipi di installazione -

c'erano feedback e requisiti sul campo, per rendere le licenze Smart più favorevoli all'adozione. Alcune delle sfide sono:

- Con la registrazione SL - I dispositivi devono essere sempre connessi a Internet per raggiungere CSSM che è un problema di distribuzione.
- I server satellitari locali introducono costi più elevati per l'installazione e la manutenzione.
- SLR semplifica solo le reti con intercapedine ad aria.
- Le implementazioni che non supportano nessuno di questi modelli devono eseguire i dispositivi nello Unregistered/Eval expired stato in cui si trovano, anche dopo l'acquisto delle licenze.

Il programma SLP viene introdotto per facilitare varie richieste di questo tipo provenienti dal campo. Con SLP, non è necessario registrare il prodotto in CSM. Tutti i livelli di licenza acquistati sono immediatamente "in uso". Questo rimuove l'attrito del giorno 0 presente sul dispositivo. SLP riduce inoltre il flusso di lavoro del provisioning delle licenze e i punti di contatto in eccesso. Non è necessario che il dispositivo sia connesso al modulo CSM 24 ore su 24. SLP consente inoltre di utilizzare le licenze nella rete disconnessa, segnalare l'utilizzo delle licenze offline e segnalare le licenze a intervalli determinati dalle policy del cliente.

Licenze disponibili

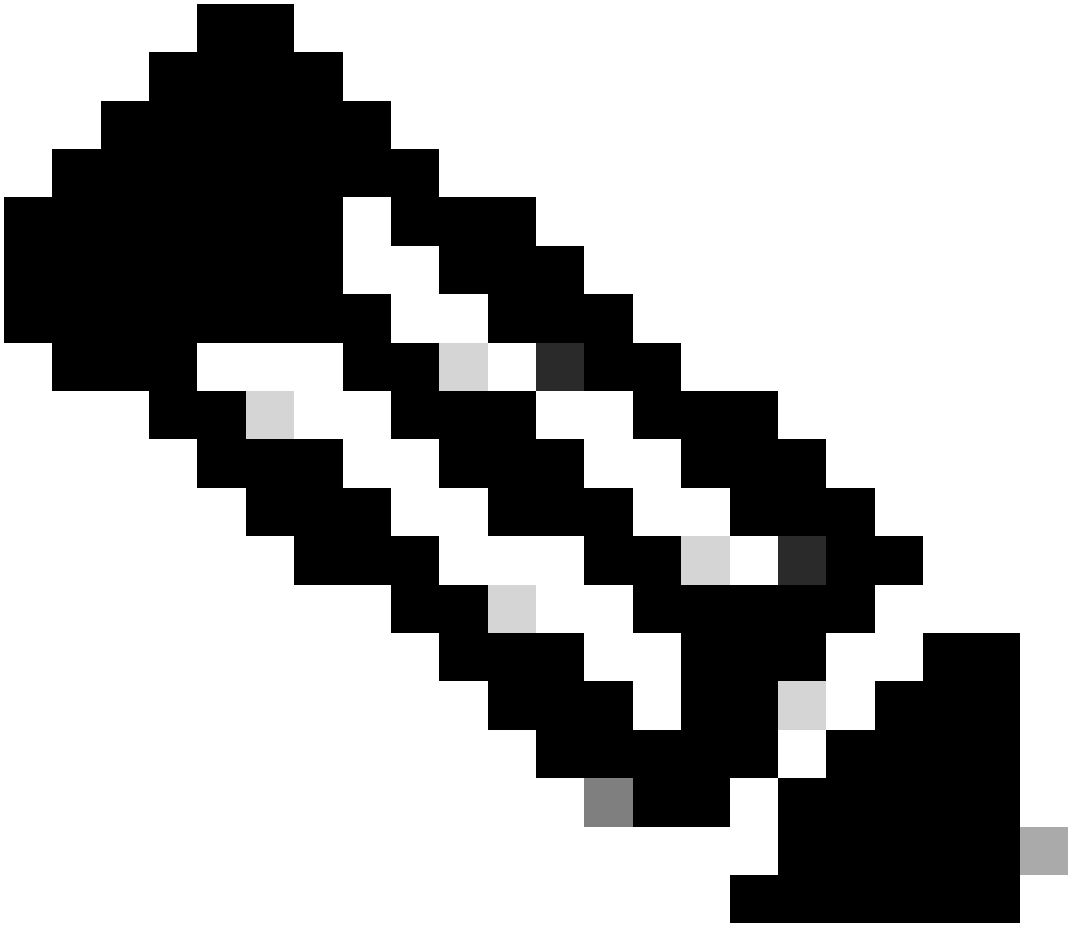
Le funzionalità software disponibili rientrano nei livelli di licenza di base o aggiuntivi. Le licenze di base sono licenze perpetue e le licenze aggiuntive sono disponibili in tre, cinque e sette anni.

Licenze base

- Caratteristiche principali della rete
- Vantaggio della rete
- HSECK9

Licenze aggiuntive

- DNA Essentials
- Vantaggio del DNA



Nota: HSECK9 è una licenza sottoposta ai controlli per l'esportazione. Per abilitare la licenza e la relativa funzionalità, è necessario uno SLAC.

I nuovi componenti

Policy

Il criterio determina quale deve essere il comportamento predefinito della PI. Indica gli attributi dei requisiti di report delle licenze per i diversi livelli e condizioni di licenza. Il criterio determina inoltre se il messaggio ACK deve essere inviato nuovamente a PI per ogni report inviato o meno a CSM. Il criterio contiene anche il nome del criterio e la data di installazione. Le policy predefinite di Cisco sono comuni e standard per tutti i prodotti Catalyst. Tuttavia, il criterio definito dal cliente è consentito anche se si desidera avere intervalli di reporting diversi e omissione di risposta ACK.

Il criterio può essere installato in una PI in diverse occasioni.

- Criterio predefinito presente nel software
- Policy installata dal reparto produzione di Cisco
- Criterio installato tramite risposta ACK
- Criteri installati manualmente tramite CLI
- Push dei criteri tramite richiesta Yang

In questo output viene illustrato l'aspetto di un criterio predefinito.

```
Policy:

Policy in use: Merged from multiple sources.
Reporting ACK required: yes (CISCO default)
Unenforced/Non-Export Perpetual Attributes:
First report requirement (days): 365 (CISCO default)
Reporting frequency (days): 0 (CISCO default)
Report on change (days): 90 (CISCO default)
Unenforced/Non-Export Subscription Attributes:
First report requirement (days): 90 (CISCO default)
Reporting frequency (days): 90 (CISCO default)
Report on change (days): 90 (CISCO default)
Enforced (Perpetual/Subscription) License Attributes:
First report requirement (days): 0 (CISCO default)
Reporting frequency (days): 0 (CISCO default)
Report on change (days): 0 (CISCO default)
Export (Perpetual/Subscription) License Attributes:
First report requirement (days): 0 (CISCO default)
Reporting frequency (days): 0 (CISCO default)
Report on change (days): 0 (CISCO default)
```

Nota: una regola non può essere cancellata quando si cancella/modifica una configurazione di sistema, si cancella una nvram o si formatta la memoria flash: filesystem. Il criterio è impostato sul valore predefinito di Cisco, al **ripristino** della licenza **Smart Factory**.

Rapporti RUM

RUM è un report di utilizzo generato e archiviato dalla PI. I rapporti RUM standard ISO19770-4 sono completati per SLP. Nei report RUM vengono archiviate tutte le modifiche apportate all'utilizzo delle licenze nella PI come file di report. I dati di utilizzo per ogni livello di licenza vengono memorizzati in report RUM separati. Le misurazioni del rapporto RUM vengono raccolte e memorizzate in PI a intervalli regolari. Ogni volta che si verifica una modifica nell'utilizzo della licenza della PI o che è stato attivato un report sull'utilizzo o quando i report hanno raggiunto le dimensioni massime/campioni, vengono generati nuovi report RUM per tutti i livelli di licenza. In altri casi, i report RUM esistenti possono essere sovrascritti con un nuovo campione e un timestamp aggiornato. La misurazione dell'utilità del report RUM predefinita è ogni 15

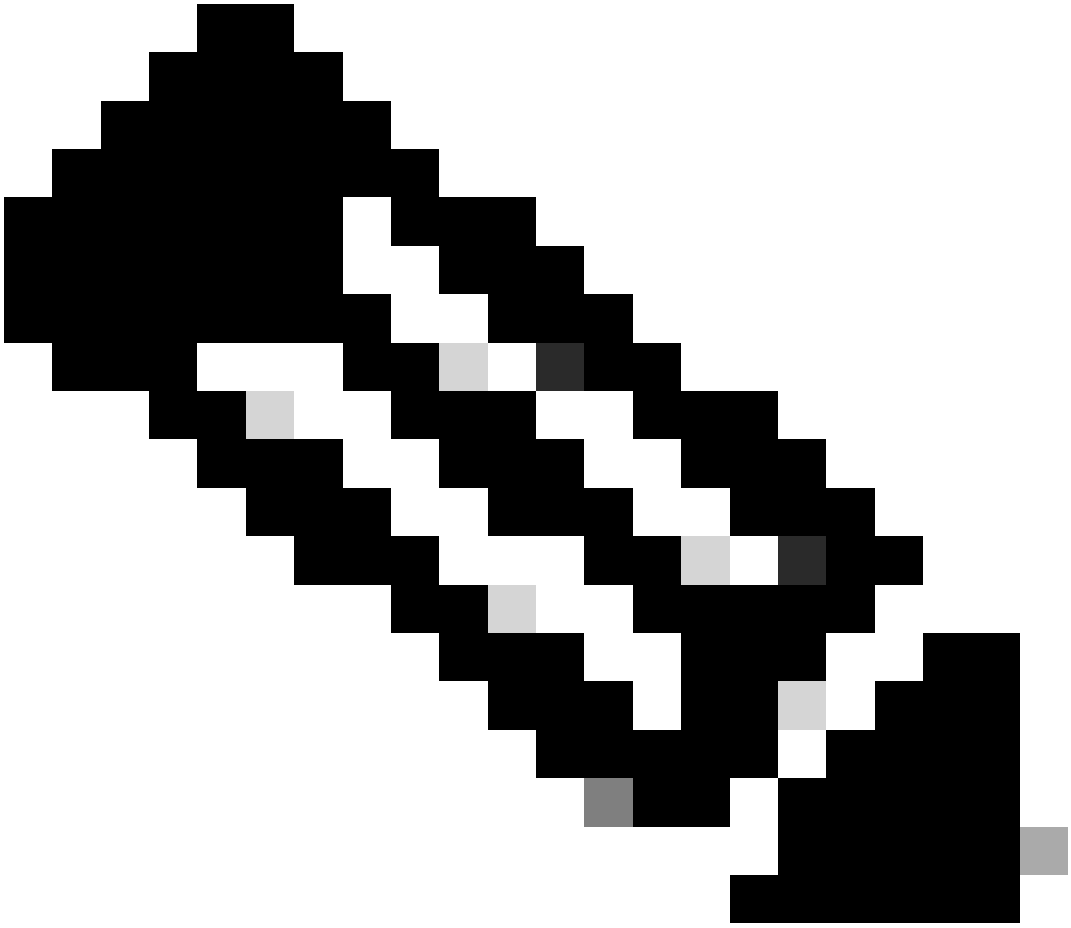
minuti. Ad ogni intervallo di report, i report RUM vengono inviati a Cisco CSM.

Tutte le relazioni RUM sono firmate dal PI e verificate dal CSSM. Quando CSSM riceve i dati del report RUM da PI, convalida il report, controlla la cronologia delle modifiche all'utilizzo della licenza e aggiorna i dati CSSM di conseguenza. Il CSSM risponde quindi alla PI tramite il messaggio di risposta ACK.

I rapporti RUM possono essere inviati al CSSM in diversi modi:

- PI invia i rapporti RUM direttamente al CSSM all'intervallo di reporting.
- PI invia il report RUM a CSLU.
- CSLU estrae i report RUM da PI a intervalli regolari tramite modelli RESTAPI eYANG.
- I report RUM vengono salvati manualmente sulla PI tramite CLI e caricati manualmente nel modulo CSM.

Nota: i rapporti RUM non possono essere cancellati quando si cancella/modifica una configurazione di sistema, si cancella la nvram o si formatta la memoria flash: filesystem. Tutti i report RUM possono essere rimossi da PI, su 'license smart factory reset'.



Nota: l'intervallo di reporting predefinito è 30 giorni.

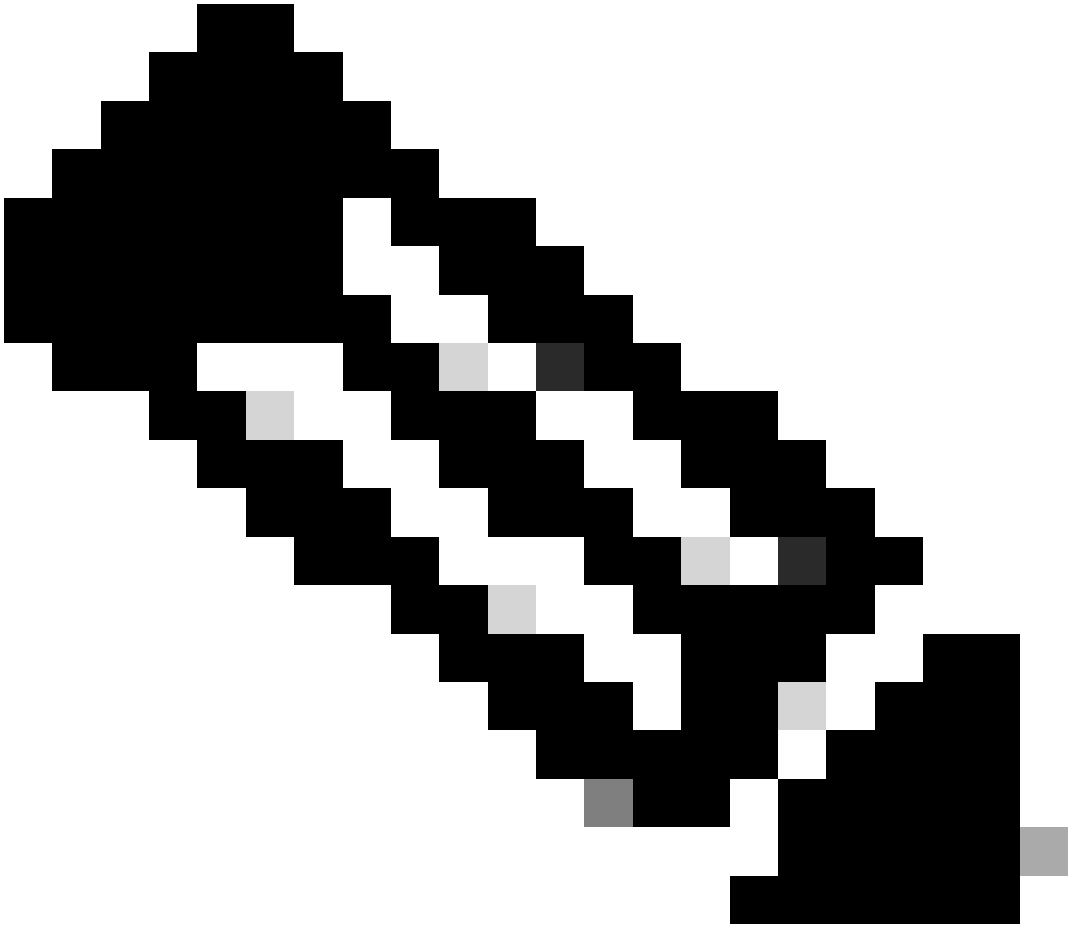
Flusso di produzione per un caso di distribuzione Greenfield

Una volta che un nuovo ordine di prodotti è stato effettuato presso Cisco CCW (Cisco Commerce Workspace), il PI passa attraverso il flusso di operazioni effettuate dal team di produzione. In questo modo si semplifica il processo protetto di firma dei rapporti RUM e si rimuove l'attrito del giorno 0 nella registrazione della PI. Una volta effettuato l'ordine, qualsiasi SA/VA esistente o nuova SA/VA creata viene associata al prodotto. Il team di produzione Cisco si occupa di queste operazioni prima di spedire il prodotto al cliente:

- Installare il codice di protezione nel dispositivo. La firma del codice di trust è installata in base all'UDI del dispositivo. È installato su tutti i prodotti.

- Installa codice acquisto: informazioni sui livelli di licenza acquistati insieme al prodotto. È installato su tutti i prodotti.
- SLAC - Smart License Auth Code (Codice di autorizzazione licenza Smart) - Non applicabile alle piattaforme Catalyst.
- Installa criterio - Criterio predefinito o personalizzato in base ai dati immessi.
- Segnalare l'utilizzo della licenza a CSSM - SA/VA.

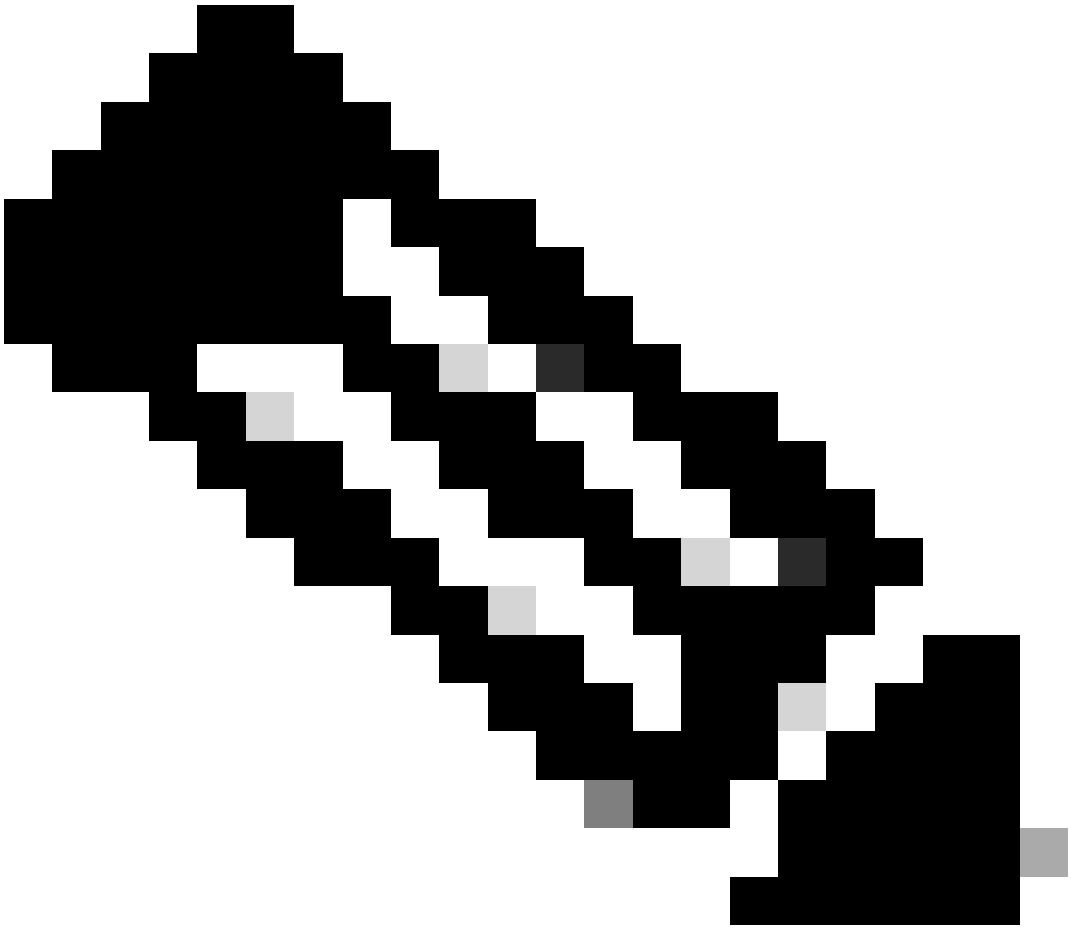
Nota: nella release 17.3.3, questo flusso viene seguito per tutte le piattaforme di switching Catalyst ad eccezione di C9200/C9200L.



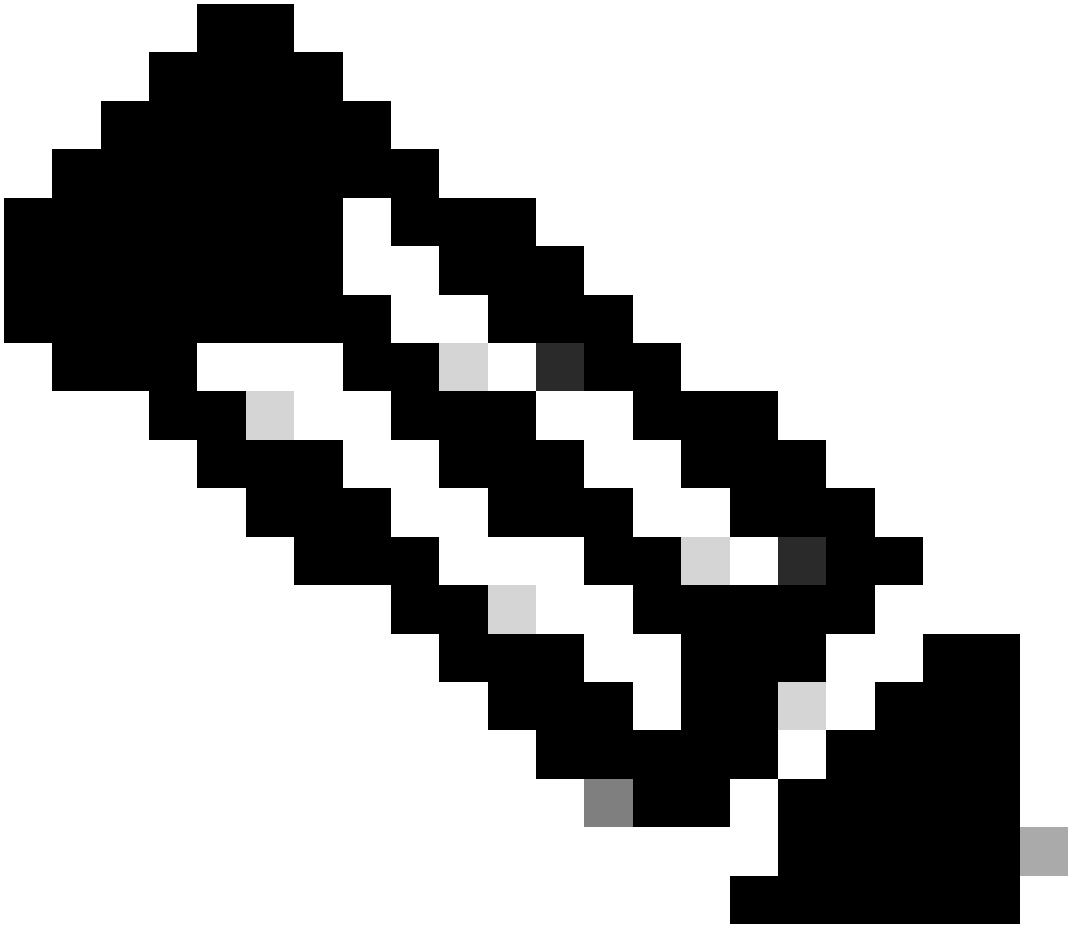
Nota: il codice di attendibilità viene installato solo nella produzione con 17.7.1 per tutte le piattaforme di switching Catalyst ad eccezione di C9200/C9200L.

CSLU

SLP introduce un nuovo, semplice ma potente strumento CSLU. CSLU è uno strumento basato su GUI, che funziona su Windows 10 Operating System o versione Linux basata su RHEL/Debian. La CSLU, che può essere eseguita sulla rete privata locale, è responsabile della raccolta delle porte RUM dalle PI associate a CSSM. Il provisioning di CSLU deve essere eseguito in modo da raccogliere i report RUM sui PI nella rete locale e anche per inviare periodicamente il report RUM al CSSM attraverso Internet. CSLU è uno strumento semplice che visualizza solo i dettagli degli UDI dei dispositivi con provisioning. Tutti i dati relativi all'utilizzo delle licenze per PI, licenze acquistate e licenze non utilizzate nel pool vengono visualizzati solo in SA/VA di CSSM, da verificare. È potente perché può raccogliere report di utilizzo fino a 10.000 PI. CSLU è anche responsabile del push dei messaggi ACK da CSSM a PI.



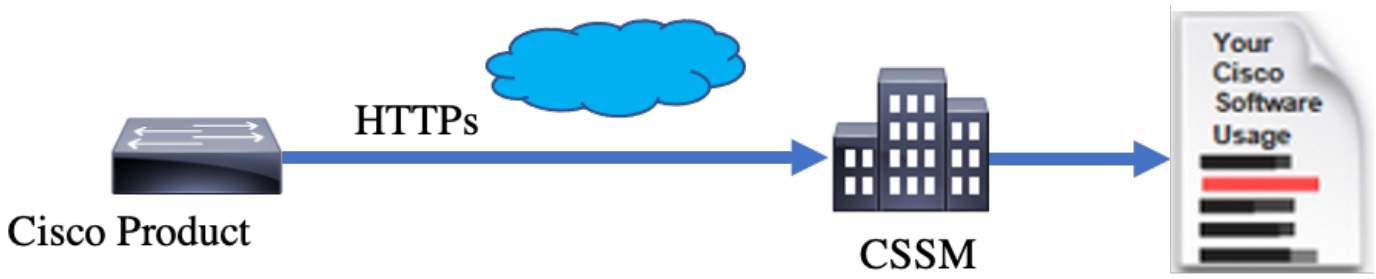
Nota: per la configurazione dettagliata e le modalità operative supportate della CSLU, consultare la sezione Topologia basata su CSLU.

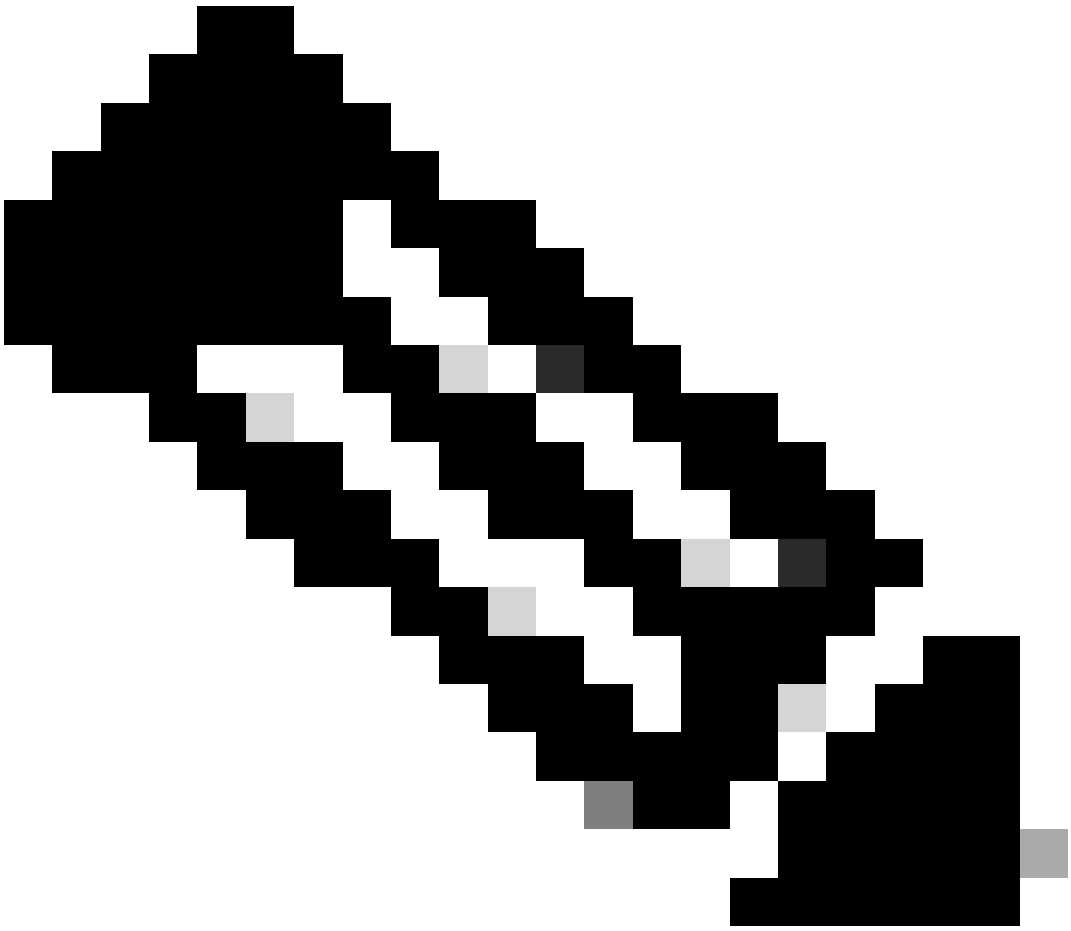


Nota: la versione Linux di CSLU è supportata dalla versione 17.7.1.

SLP - Connessione diretta

Su un prodotto predistribuito, la modalità di trasporto predefinita è configurata su CSLU. Se si desidera utilizzare il metodo Direct Connect, è necessario impostare la modalità di trasporto su Call-home o SMART in base ai requisiti. Il requisito di base per il metodo di topologia a connessione diretta è disporre di connettività Internet per la raggiungibilità a CSM. Inoltre, è necessario verificare che per la connettività a CSM nel dispositivo siano presenti le configurazioni L3, DNS e Domain richieste.





Nota: quando ci si connette direttamente a CSM, si consiglia di utilizzare il trasporto intelligente.

Report sulle licenze

Nella topologia Direct Connect i rapporti RUM vengono inviati direttamente a CSM. Per i rapporti sulle licenze è necessario che nel dispositivo sia installato un codice di attendibilità. Il codice di attendibilità viene installato dal produttore Cisco sul dispositivo prima della spedizione. È inoltre possibile installare il codice di protezione nel dispositivo.

Il codice di attendibilità è una stringa di token estratta da CSM nella pagina Account virtuale - Generale. Il codice di attendibilità può essere installato dalla CLI.

Switch#license smart trust idtoken < > all/local

Nota: tutte le opzioni devono essere utilizzate per il sistema HA o Stacking back. Per un dispositivo autonomo, è possibile utilizzare l'opzione local.

Switch#license smart trust idtoken < > all/local.

On Successful installation of policy, the same can be verified through 'show license status' CLI.

Switch#show license status

Utility:
Status: DISABLED

Smart Licensing Using Policy:
Status: ENABLED

Data Privacy:
Sending Hostname: yes
Callhome hostname privacy: DISABLED
Smart Licensing hostname privacy: DISABLED
Version privacy: DISABLED

Transport:
Type: Callhome

Policy:
Policy in use: Installed On Nov 07 22:50:04 2020 UTC
Policy name: SLP Policy
Reporting ACK required: yes (Customer Policy)
Unenforced/Non-Export Perpetual Attributes:
First report requirement (days): 60 (Customer Policy)
Reporting frequency (days): 60 (Customer Policy)
Report on change (days): 60 (Customer Policy)
Unenforced/Non-Export Subscription Attributes:
First report requirement (days): 30 (Customer Policy)
Reporting frequency (days): 30 (Customer Policy)
Report on change (days): 30 (Customer Policy)
Enforced (Perpetual/Subscription) License Attributes:
First report requirement (days): 0 (CISCO default)

Reporting frequency (days): 90 (Customer Policy)
Report on change (days): 90 (Customer Policy)
Export (Perpetual/Subscription) License Attributes:
First report requirement (days): 0 (CISCO default)
Reporting frequency (days): 90 (Customer Policy)
Report on change (days): 90 (Customer Policy)

Miscellaneous:
Custom Id: <empty>

Usage Reporting:
Last ACK received: Nov 03 12:57:01 2020 UTC
Next ACK deadline: Dec 03 12:57:01 2020 UTC
Reporting push interval: 30 days
Next ACK push check: <none>
Next report push: Nov 07 22:50:35 2020 UTC
Last report push: Nov 03 12:55:57 2020 UTC
Last report file write: <none>

Trust Code Installed:
Active: PID:C9500-24Y4C,SN:CAT2344L4GH
INSTALLED on Nov 07 22:50:04 2020 UTC
Standby: PID:C9500-24Y4C,SN:CAT2344L4GJ
INSTALLED on Nov 07 22:50:04 2020 UTC

Una volta installato correttamente il codice di attendibilità, la PI può segnalare l'utilizzo direttamente al CSM. Le seguenti condizioni generano un report sulle licenze:

- Installazione del codice di attendibilità completata
- In ogni intervallo di report predefinito
- Ricaricamento/avvio sul dispositivo
- Il passaggio al formato A
- Aggiunta o rimozione di un membro dello stack
- Attivazione manuale della sincronizzazione della licenza

Il reporting delle licenze al CSSM può essere attivato con queste CLI:

Switch#license smart sync all

La sezione Report sull'utilizzo in show license status indica le timeline dell'ultimo ACK ricevuto, la scadenza dell'ACK successivo, il push del report successivo e il push dell'ultimo report.

Usage Reporting:
Last ACK received: Nov 03 12:57:01 2020 UTC
Next ACK deadline: Dec 03 12:57:01 2020 UTC
Reporting push interval: 30 days
Next ACK push check: <none>
Next report push: Nov 07 22:50:35 2020 UTC
Last report push: Nov 03 12:55:57 2020 UTC
Last report file write: <none>

Direct Connect - Trasporto intelligente

Su una topologia in modalità di accesso diretto al cloud o di connessione diretta, se viene utilizzato SMART Transport, queste sono le configurazioni richieste sul dispositivo.

Configure the desired Transport mode using below CLI.

Switch(config)#license smart transport smart

Running config on Smart Transport Mode:
!
license smart url smart https://smartreceiver.cisco.com/licservice/license
license smart transport smart
!

Direct Connect - Trasporto Call-Home

In una topologia di modalità Direct Connect o Direct Cloud Access, se si utilizza il trasporto "call-home", queste sono le configurazioni richieste sul dispositivo.

Configure the desired Transport mode using below CLI.

Switch(config)#license smart transport callhome

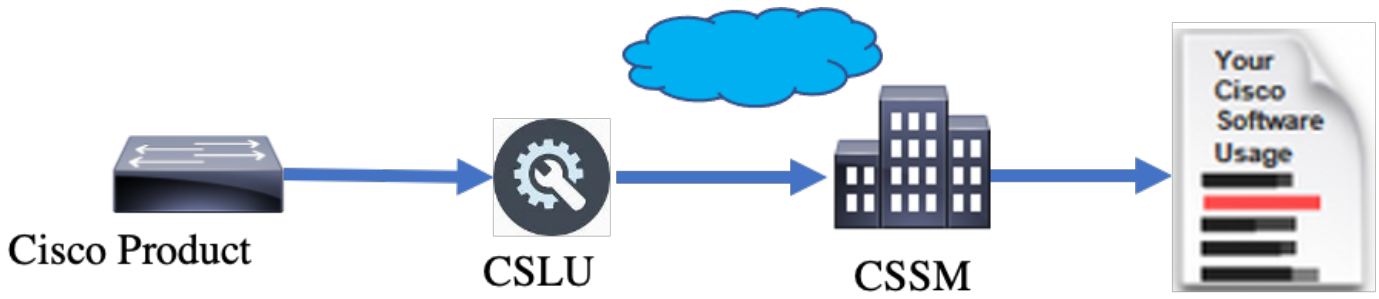
Running config on Smart Transport Mode:
!
service call-home
!
call-home
contact-email-addr shmandal@cisco.com

```
no http secure server-identity-check
profile "CiscoTAC-1"
active
reporting smart-licensing-data
destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
destination transport-method http
!
```

Nota: per impostazione predefinita, l'indirizzo di destinazione per la funzione Call-Home è configurato su URL CSM. È possibile verificare questa condizione nella show run all configurazione.

SLP - CSLU

La modalità CSLU è la modalità di trasporto predefinita sui dispositivi forniti in fabbrica con versione 17.3.2 o successive. Inoltre, se si esegue la migrazione da licenze di valutazione scadute, la modalità di trasporto dopo il passaggio a SLP sarà CSLU. Nella topologia basata su CSLU, la CSLU si trova tra la PI e il CSM. CSLU impedisce agli utenti di avere connettività di rete diretta a Cisco Cloud - CSSM. L'utilità CSLU può essere eseguita localmente in una rete privata e scaricare i report sull'utilizzo da tutte le PI associate. I report di utilizzo vengono salvati localmente nel PC Windows prima di essere inviati al CSM tramite Internet. CSLU è uno strumento leggero. È possibile visualizzare solo l'elenco delle PI associate e identificarle con l'utilizzo di UDI. CSLU non può visualizzare o contenere le informazioni sulla ridondanza di PI, i livelli di licenza o l'utilizzo della licenza.

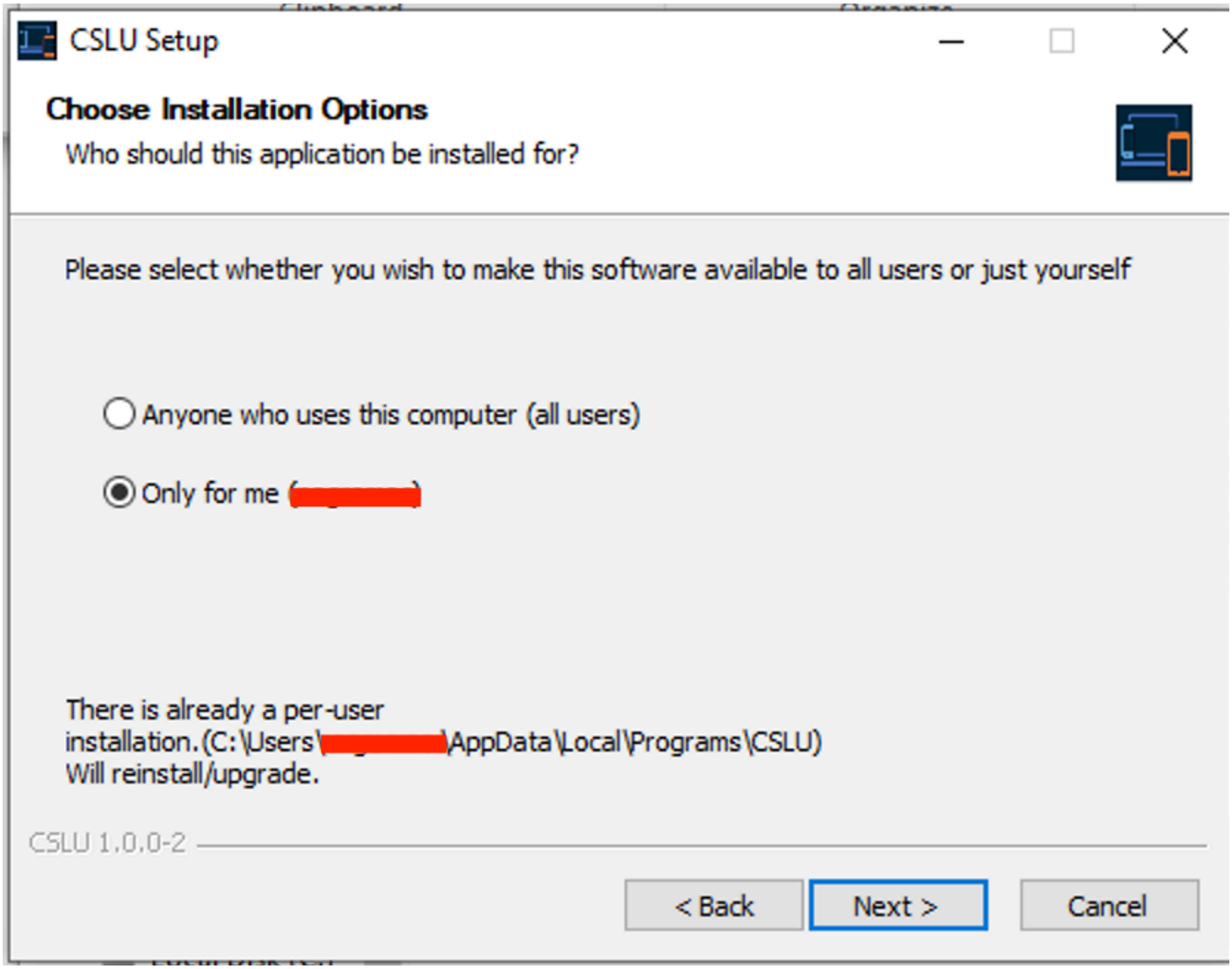


Installazione e configurazione CSLU

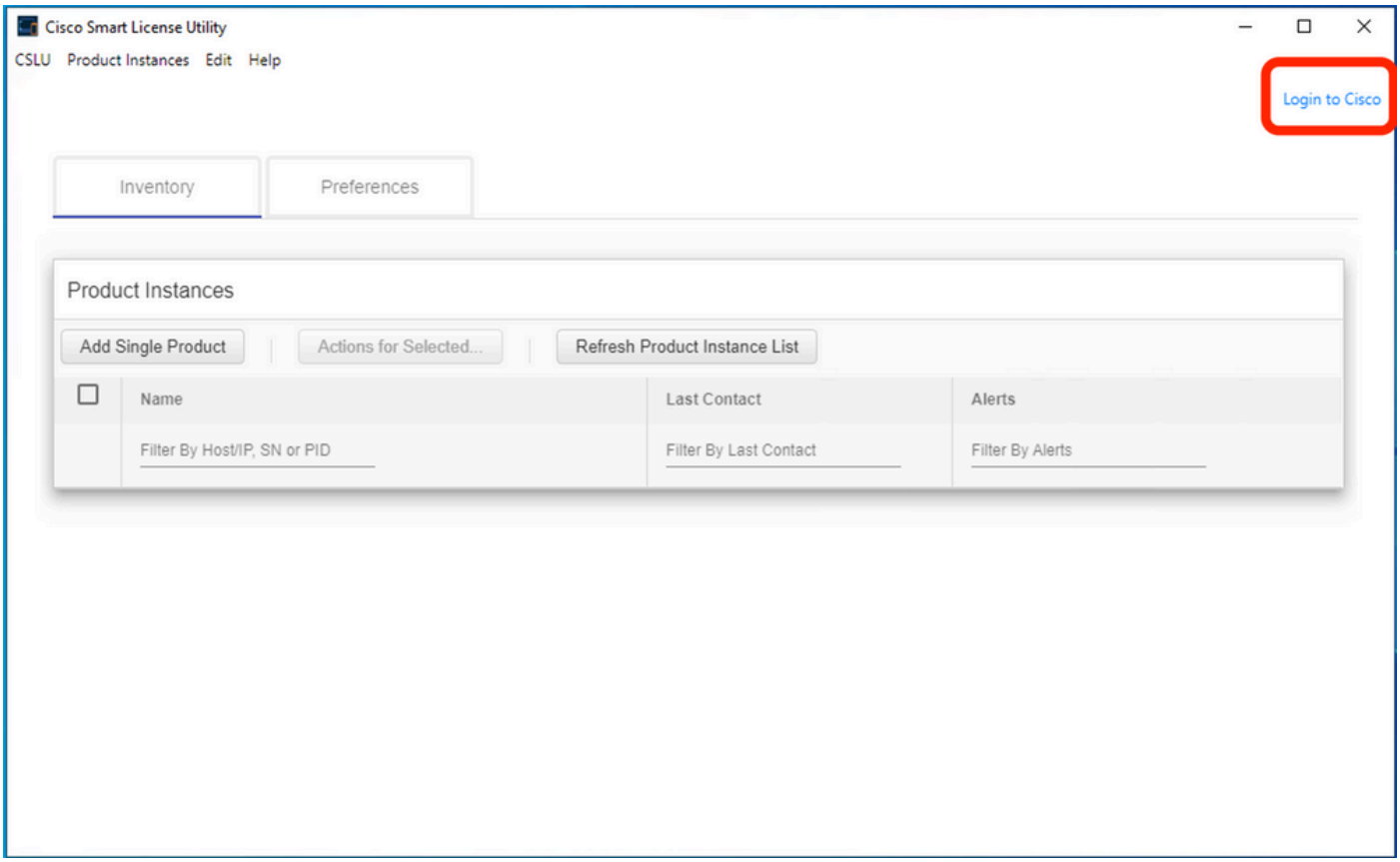
Lo strumento CSLU viene installato e utilizzato sui computer Windows 10. Il software è disponibile nel CCO per il download e l'utilizzo gratuito. Una volta installato lo strumento, è possibile scaricare la Guida introduttiva/Manuale per l'utente dal menu?, passare a Help > Download Help Manual.

L'installazione di CSLU richiede l'accettazione del Contratto di Licenza.

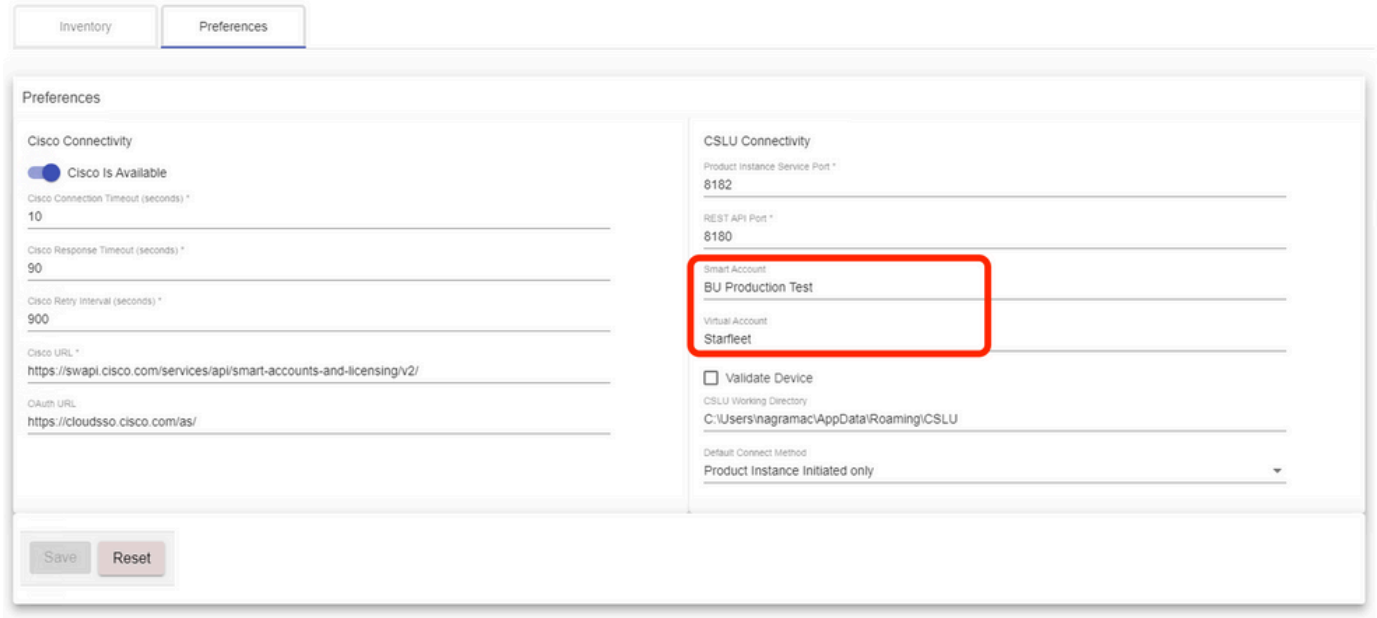
È consigliabile che l'applicazione venga installata solo per l'utente corrente e non per tutti gli utenti che utilizzano il computer. Se sul PC è già presente una versione precedente di CSLU, è buona norma disinstallarla in anticipo. Tuttavia, la nuova installazione è in grado di aggiornare il software.



Dopo l'installazione, accedere a Cisco, usando l'opzione di accesso presente nell'angolo in alto a destra dell'applicazione. Verranno utilizzate le credenziali CEC. Inoltre, tramite l'accesso, viene stabilita la fiducia tra CSLU e CSSM.



Dopo aver effettuato l'accesso a Cisco, verificare che i dettagli SA e VA siano selezionati correttamente tramite il menu a discesa nel riquadro Preferenze dello strumento. Assicurarsi di salvare le configurazioni.

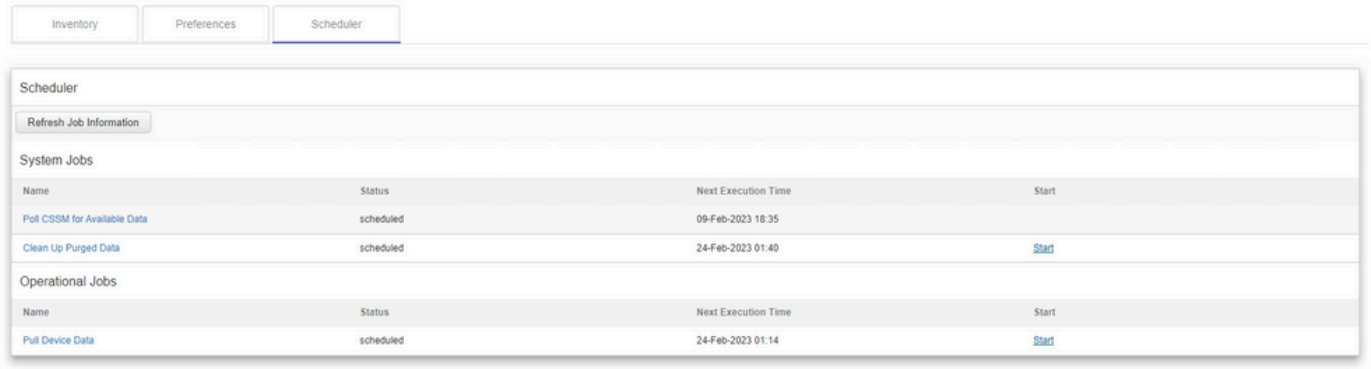


Scheda Programmazione su CSLU - Tramite la scheda Programmazione su CSLU, è possibile configurare quanto segue:

- Esegui polling CSSM per dati disponibili: visualizza gli intervalli dei job, l'ora dell'ultimo pull e il successivo tempo di pull dei dati da CSSM.

- Clean up purged data: rimuove tutti i dati eliminati dall'archivio dati CSLU. Può essere attivato anche manualmente.

- Pull device data (Dati dispositivo pull) - Attiva la modalità di pull CSLU.



CSLU in modalità PUSH

Per impostazione predefinita, CSLU funziona in modalità PUSH. In modalità PUSH, la PI invia i report sull'utilizzo alla CSLU a intervalli regolari. Dal dispositivo, accertarsi che la rete L3 sia raggiungibile dalla CSLU. Affinché la PI parli con CSLU, è necessario configurare l'indirizzo IP del computer Windows che esegue CSLU.

Switch(config)#license smart url cslu http://<IP_of_CSLU>:8182/cslu/v1/pi

The same can be verified through 'show license status' CLI

Switch#show license status

Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%

No time source, 20:59:25.156 EDT Sat Nov 7 2020

Utility:

Status: DISABLED

Smart Licensing Using Policy:

Status: ENABLED

Data Privacy:

Sending Hostname: yes

Callhome hostname privacy: DISABLED

Smart Licensing hostname privacy: DISABLED

Version privacy: DISABLED

Transport:

Type: cslu

Cslu address: http://<IP_of_CSLU>:8182/cslu/v1/pi

Proxy:

Not Configured

Policy:

Policy in use: Merged from multiple sources.

Reporting ACK required: yes (CISCO default)

Unenforced/Non-Export Perpetual Attributes:

First report requirement (days): 365 (CISCO default)

Reporting frequency (days): 0 (CISCO default)

Report on change (days): 90 (CISCO default)

Unenforced/Non-Export Subscription Attributes:

First report requirement (days): 90 (CISCO default)

Reporting frequency (days): 90 (CISCO default)

Report on change (days): 90 (CISCO default)

Enforced (Perpetual/Subscription) License Attributes:

First report requirement (days): 0 (CISCO default)

Reporting frequency (days): 0 (CISCO default)

Report on change (days): 0 (CISCO default)

Export (Perpetual/Subscription) License Attributes:

First report requirement (days): 0 (CISCO default)

Reporting frequency (days): 0 (CISCO default)

Report on change (days): 0 (CISCO default)

Miscellaneous:

Custom Id: <empty>

Usage Reporting:

Last ACK received: <none>

Next ACK deadline: Feb 05 15:32:51 2021 EDT

Reporting push interval: 30 days

Next ACK push check: <none>

Next report push: Nov 07 15:34:51 2020 EDT

Last report push: <none>

Last report file write: <none>

Trust Code Installed: <none>

I report vengono inviati a CSLU da PI alle seguenti condizioni:

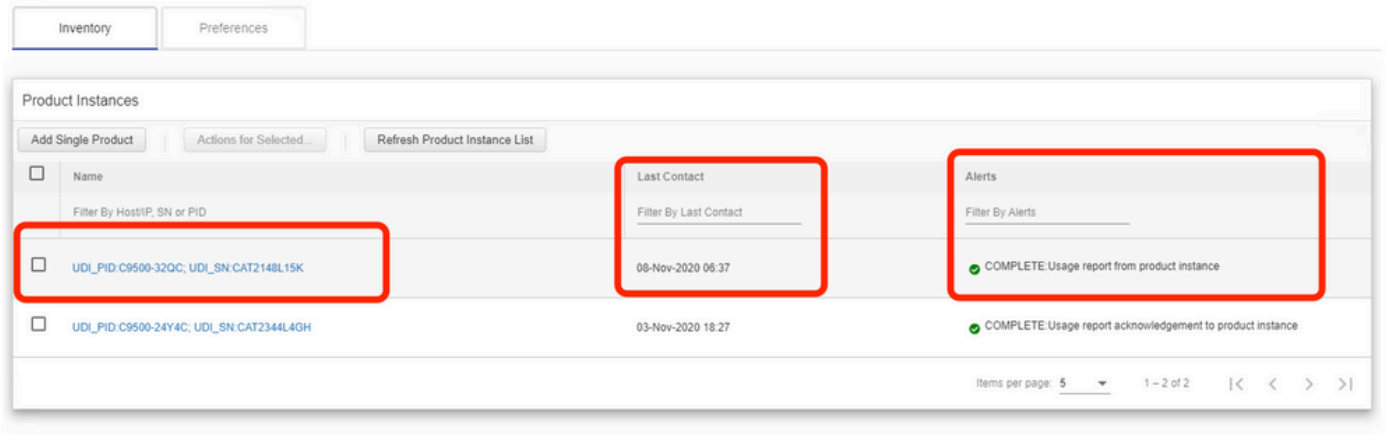
- A ogni intervallo di report predefinito
- Ricaricamento/avvio sul dispositivo
- Allo switchover
- All'aggiunta o alla rimozione di un membro dello stack
- All'attivazione manuale della sincronizzazione della licenza

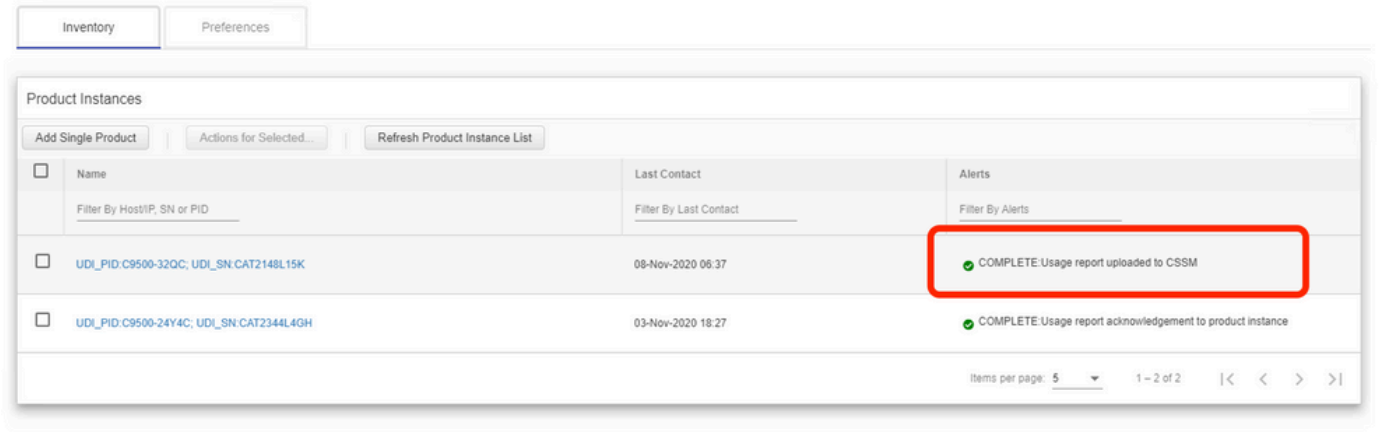
In CSLU, la pagina di inventario elenca i dispositivi attualmente associati a CSLU. I dispositivi nell'elenco possono essere identificati tramite l'UDI. I dispositivi possono essere filtrati in base al PID o al SN dall'elenco per identificare un particolare dispositivo.

La pagina Inventario CSLU contiene anche altre due colonne:

- La colonna **Ultimo contatto** mostra l'indicatore orario più recente quando lo stato della segnalazione è cambiato.
- **Colonna Avviso**: visualizza lo stato del rapporto più recente della PI.

Una volta che la PI invia il report a CSLU, la CSLU crea la voce PI in CSSM. Verranno aggiornati il TS ultimo contatto e lo stato degli avvisi.





CSSM elabora i report inviati da CSLU e aggiunge/aggiorna l'istanza del prodotto su CSSM, in base all'utilizzo della licenza. Una volta che il CSSM elabora e aggiorna la data, invia il messaggio ACK alla CSLU. CSLU a sua volta memorizza e inoltra il messaggio a PI.

Il messaggio ACK è composto da:

- Conferma per tutte le segnalazioni inviate
- Policy
- Codice trust

Se nel modulo CSM è disponibile un nuovo criterio, questo viene aggiornato anche al PI. Se il criterio non viene modificato, lo stesso viene inviato a PI.

Nota: se la segnalazione dei messaggi ACK non è richiesta in base alla policy, il messaggio ACK non viene inviato.

La colonna dei messaggi di avviso può avere uno dei seguenti stati:

- Report utilizzo da istanza prodotto
- Report sull'utilizzo caricato su Cisco
- Richiesta di sincronizzazione da istanza prodotto
- Richiesta di sincronizzazione caricata in CSM
- Conferma ricevuta da CSSM
- Conferma report utilizzo all'istanza del prodotto

Nota: in CSLU su un sistema HA, la voce è sempre visibile solo per UDI di Attivo. Solo il modulo CSM dispone di tutti gli UDI per i singoli dispositivi del sistema.

Ricerca automatica CSLU

Per supportare implementazioni scalabili con configurazioni minime, è supportato il rilevamento automatico della CSLU. Ciò significa che non è necessario configurare specificamente l'indirizzo IP o l'URL della CSLU. A tale scopo, è sufficiente aggiungere una voce al server DNS. In questo modo il dispositivo, che dispone della modalità di trasporto CSLU (impostazione predefinita), individua automaticamente CSLU e invia i report.

Ecco un paio di cose da fare:

- Creare una voce nel server DNS. L'indirizzo IP della CSLU deve essere mappato al nome cslu-local.
- Verificare che il server dei nomi e le configurazioni DNS siano presenti nel dispositivo per la raggiungibilità.

In questo modo, senza ulteriori configurazioni, i dispositivi nella rete possono raggiungere la CSLU e inviare rapporti RUM a intervalli regolari.

CSLU in modalità PULL

La modalità PULL è la modalità in cui la CSLU avvia il processo di recupero dei report RUM dai dispositivi. Qui i dettagli del dispositivo vengono aggiunti alla CSLU e la CSLU recupera i dati su tutti i dispositivi aggiunti a intervalli regolari. Il PULL da CSLU può anche essere attivato manualmente. La CSLU a sua volta invia il report RUM al CSSM e i messaggi ACK ricevuti dal CSSM vengono inviati alla PI. La modalità PULL è supportata in tre modi diversi: RESTAPI, NETCONF e RESTCONF.

Modalità PULL tramite RESTAPI

Per consentire il corretto funzionamento della modalità PULLRESTAPI, le configurazioni richieste dal dispositivo e dalla CSLU sono:

Configs on PI:

Ensure the network reachability from PI to CSLU is available and working.

```
!
 ip http server
 ip http authentication local
 ip http secure-server
!
 aaa new-model
 aaa authentication login default local
 aaa authorization exec default local
 username admin privilege 15 password 0 lab
!
```

Nota: l'utente deve disporre dell'accesso di livello 15 di accesso privato.

CSLU - Procedura di configurazione

Per sincronizzare automaticamente i report, è necessario che CSLU abbia eseguito l'accesso a CSSM.

Passaggio 1. Scegliere Add Single Product nella pagina Inventory.

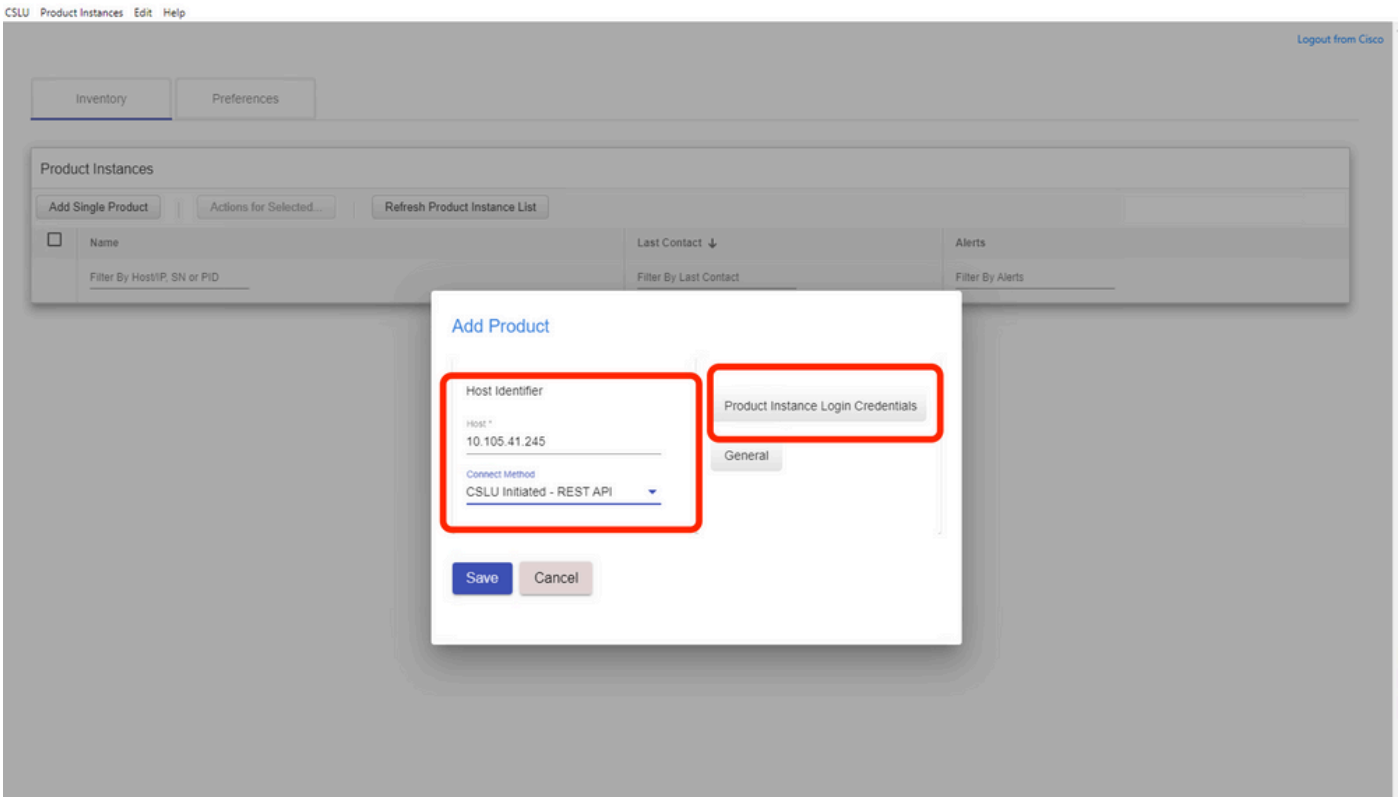
Passaggio 2. Immettere l'indirizzo IP del dispositivo.

Passaggio 3. Scegliere il metodo di connessione come RestAPI.

Passaggio 4. Scegliere le credenziali di accesso dell'istanza del prodotto.

Passaggio 5. Immettere le credenziali dell'utente con accesso Priv 15.

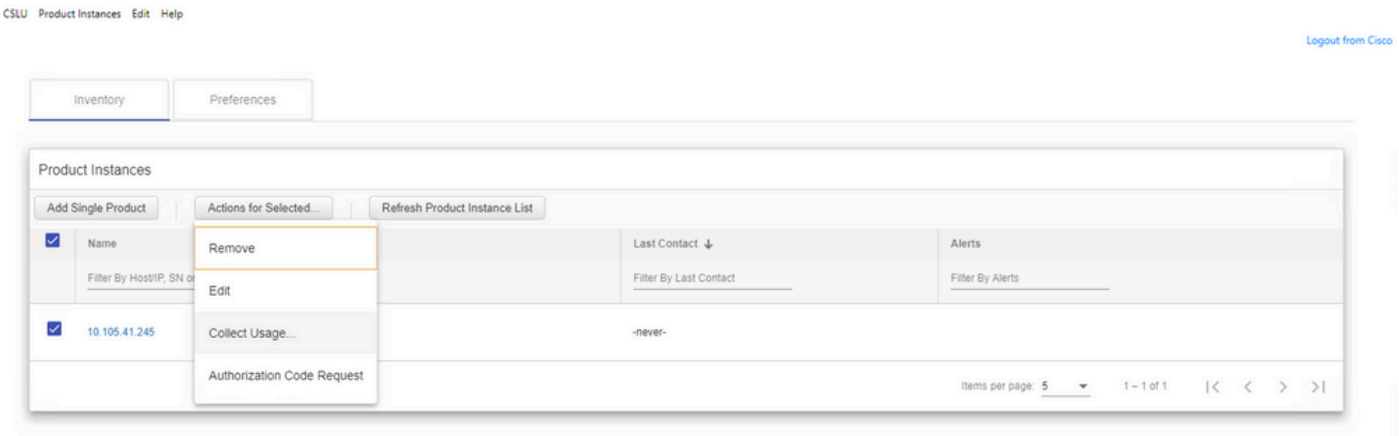
Passaggio 6. Salvare le configurazioni.

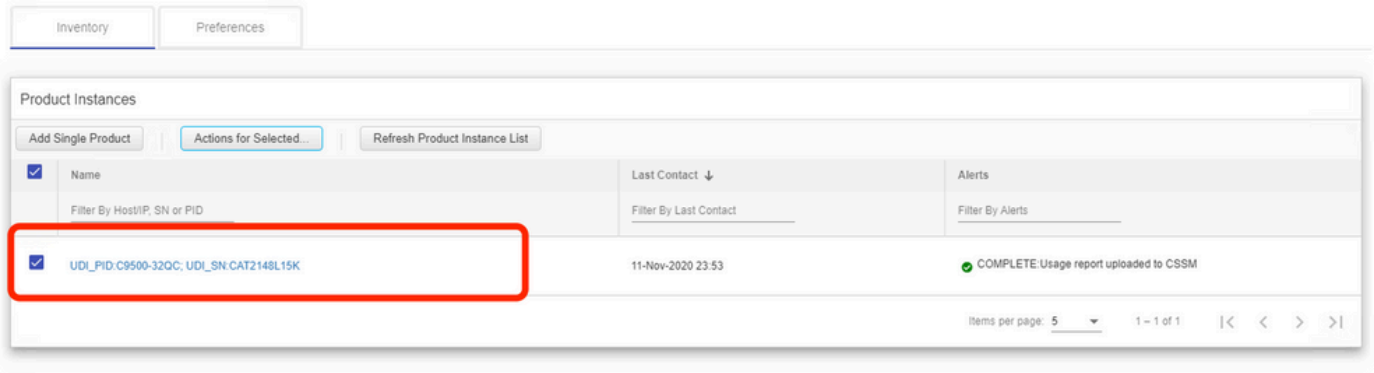


Il dispositivo viene aggiunto con un solo indirizzo IP nel campo Nome.

Scegliere il dispositivo e passare a Actions for Selected > Collect Usage.

Una volta raccolti correttamente i dati di utilizzo, il campo Nome viene aggiornato in base all'UDI della PI e viene aggiornato anche l'indicatore orario. Il campo dell'avviso riflette lo stato più recente.





Se il dispositivo è ancora disponibile quando il messaggio ACK viene ricevuto dal CSM, l'ACK viene inviato nuovamente al PI. In caso contrario, ACK viene inviato al successivo intervallo di pull.

Modalità PULL con RESTCONF

Per il corretto funzionamento della modalità PULLRESTCONF , le configurazioni richieste dal dispositivo e i passaggi da CSLU sono:

Configs on PI:

```
!
restconf
!
 ip http secure-server
 ip http authentication local
 ip http client source-interface GigabitEthernet 0/0
!
 username admin privilege 15 password 0 lab
!
```

Nota: queste configurazioni sono per l'autenticazione locale. È possibile utilizzare anche l'autenticazione remota.

CSLU - Procedura di configurazione

Per sincronizzare automaticamente i report, è necessario che CSLU abbia eseguito l'accesso a CSSM. L'impostazione CSLU è identica a quella RESTAPI per la raccolta e la creazione di rapporti RUM.

Passaggio 1. Scegliere Add Single Product nella pagina Inventory.

Passaggio 2. Immettere l'indirizzo IP del dispositivo.

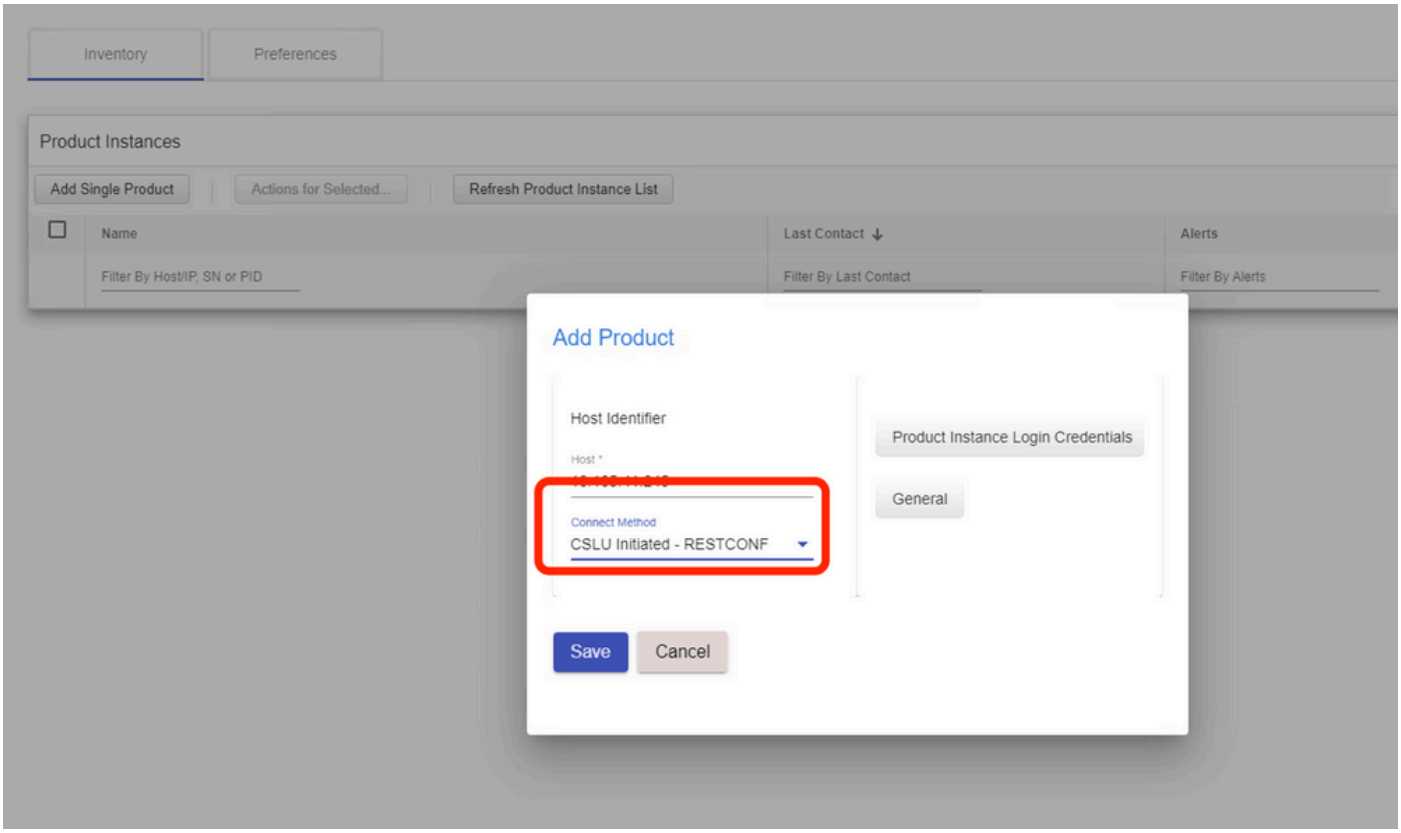
Passaggio 3. Scegliere il metodo di connessione come RESTCONF.

Passaggio 4. Scegliere le credenziali di accesso dell'istanza del prodotto.

Passaggio 5. Immettere le credenziali dell'utente con accesso Priv 15.

Passaggio 6. Salvare le configurazioni.

Passaggio 7. Raccoglie i dati sull'utilizzo per il dispositivo selezionato.



Modalità PULL con NETCONF

Per consentire il corretto funzionamento della modalità PULLNETCONF, le configurazioni richieste dal dispositivo e i passaggi da CSLU sono:

Configs on PI:

```
!
 ip ssh version
!
 netconf-yang
 netconf ssh
 netconf-yang feature candidate-datastore
!
 username admin privilege 15 password 0 lab
!
```

To ensure yang process is running, execute the command:

```
Switch#show platform software yang-management process
confd : Running
nesd : Running
syncfd : Running
ncsshd : Running
```

dmiauthd : Running
nginx : Running
ndbmand : Running
pubd : Running
gnmib : Not Running

Nota: queste configurazioni sono per l'autenticazione locale. È possibile utilizzare anche l'autenticazione remota.

CSLU - Procedura di configurazione

Per sincronizzare automaticamente i report, è necessario che CSLU abbia eseguito l'accesso a CSSM. L'impostazione CSLU è identica a quella RESTAPI per la raccolta e la creazione di rapporti RUM.

Passaggio 1. Scegliere Add Single Product nella pagina Inventory.

Passaggio 2. Immettere l'indirizzo IP del dispositivo.

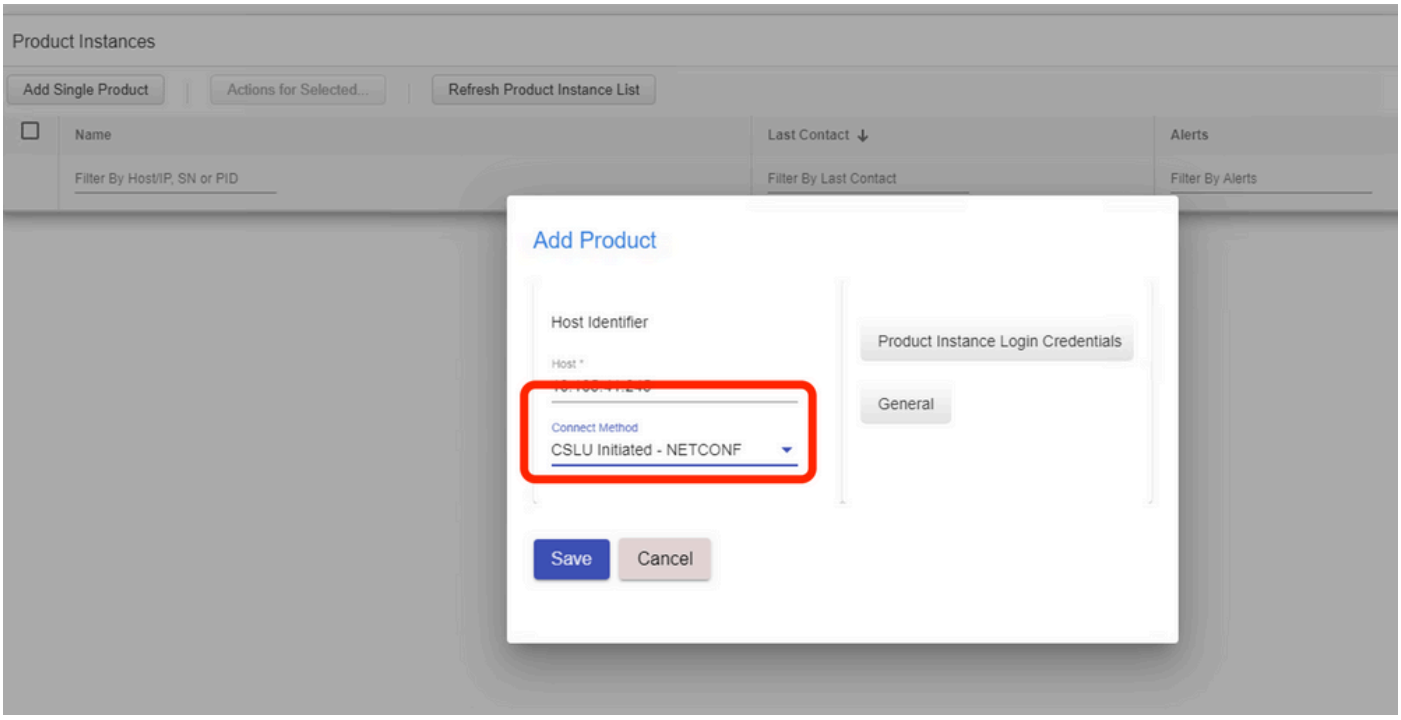
Passaggio 3. Scegliere il metodo di connessione come NETCONF.

Passaggio 4. Scegliere le credenziali di accesso dell'istanza del prodotto.

Passaggio 5. Immettere le credenziali dell'utente con accesso Priv 15.

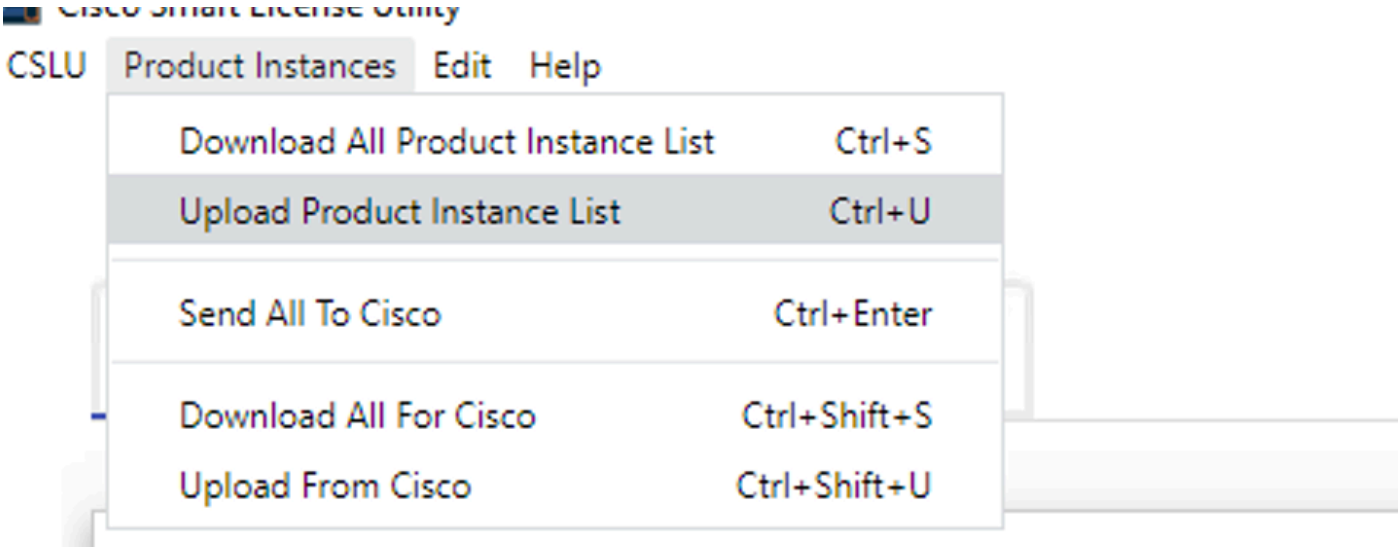
Passaggio 6. Salvare le configurazioni.

Passaggio 7. Raccoglie i dati sull'utilizzo per il dispositivo selezionato.

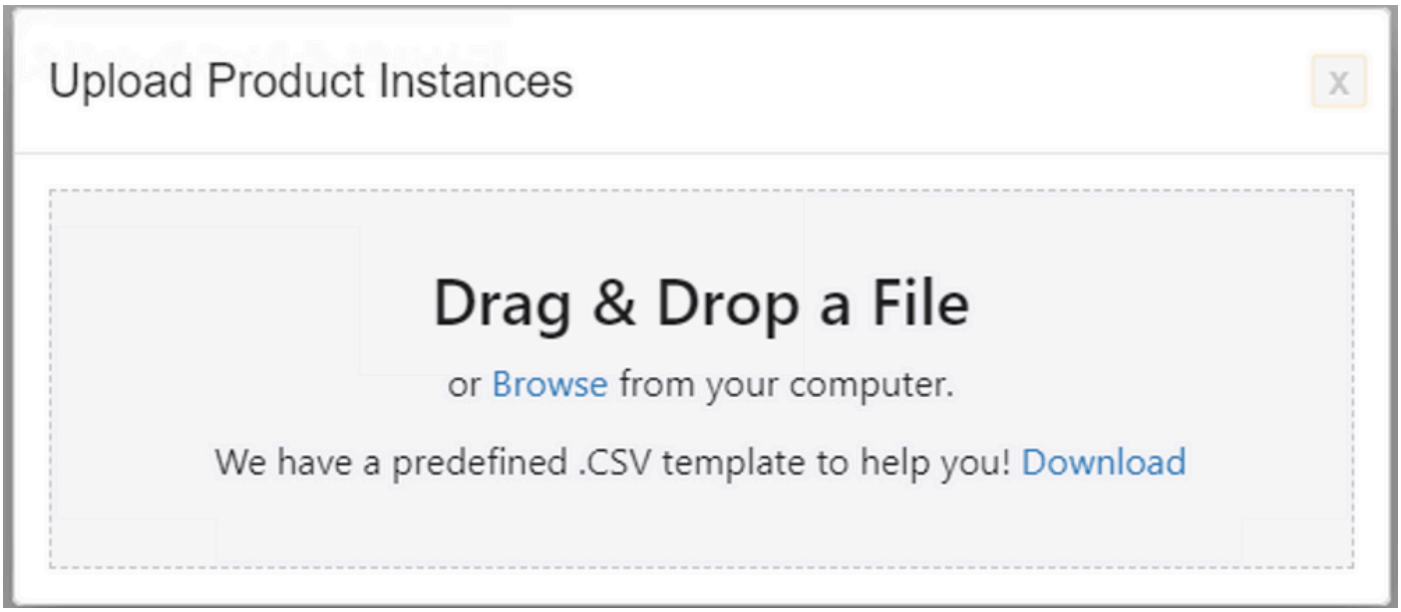


Nota: per tutti i modelli, NETCONF, RESTCONF eRESTAPI, l'elenco dei dispositivi può essere aggiunto in blocco.

Per eseguire il caricamento di massa, sulla Menu barra, passare a Product Instance > Upload Product Instance List, come mostrato in questa immagine.



Viene visualizzata una nuova finestra popup. Il file modello può essere scaricato da esso. Nel file in formato CSV, immettere i dettagli relativi ai dispositivi nell'elenco dei dispositivi e caricarli in CSLU per aggiungere più dispositivi.



Nota: per tutti i tipi di modalità PULL CSLU, si consiglia di impostare il trasporto su Off sulla PI. a tale scopo, è possibile utilizzare la CLI.

Switch(config)#license smart transport off

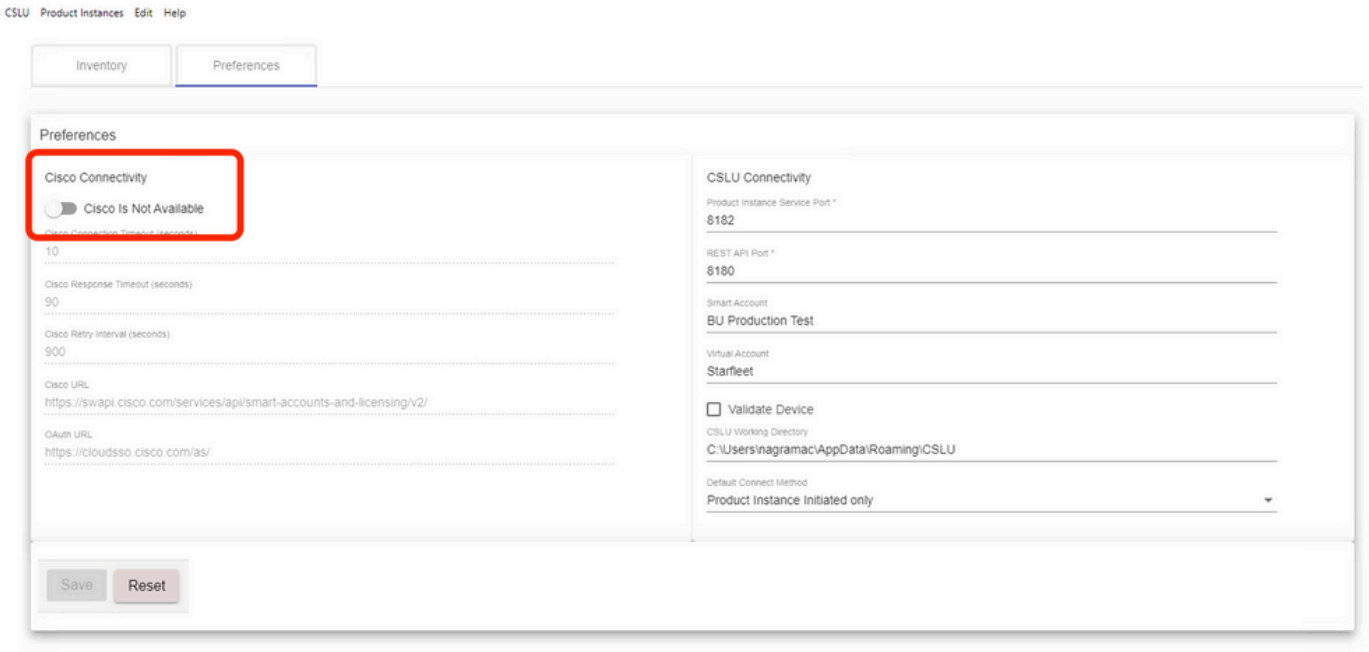
CSLU in modalità disconnessa

CSLU può funzionare in modalità disconnessa da CSM. Ciò è valido per tutte le distribuzioni che non consentono la connessione della CSLU a Internet. In modalità disconnessa, i report di tutti i dispositivi vengono scaricati manualmente da CSLU e caricati in CSM. A sua volta, i

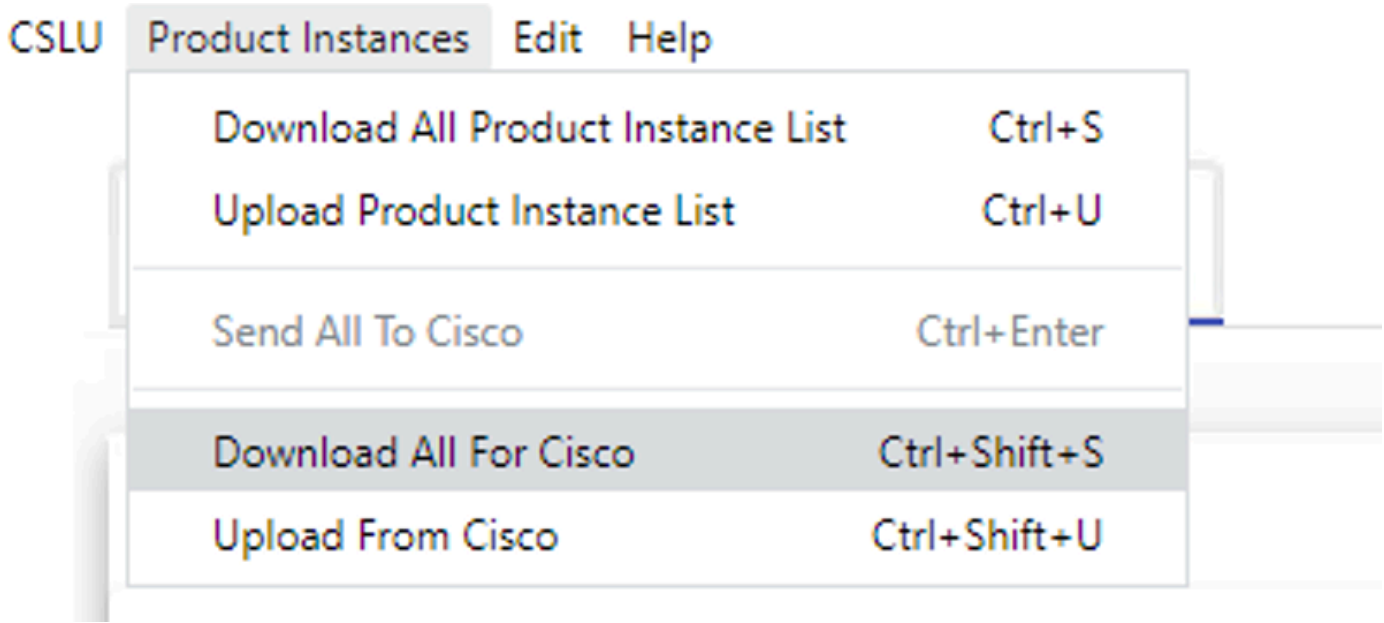
messaggi ACK vengono scaricati da CSM e caricati in CSLU. CSLU continua comunque a eseguire il PULL/PUSH delle date di utilizzo dalle PI e invia il messaggio ACK a PI.

Passaggio 1. Nella paginaCSLU Preference disattivare l'opzione Cisco Connectivity. Ciò conferma che Cisco non è disponibile.

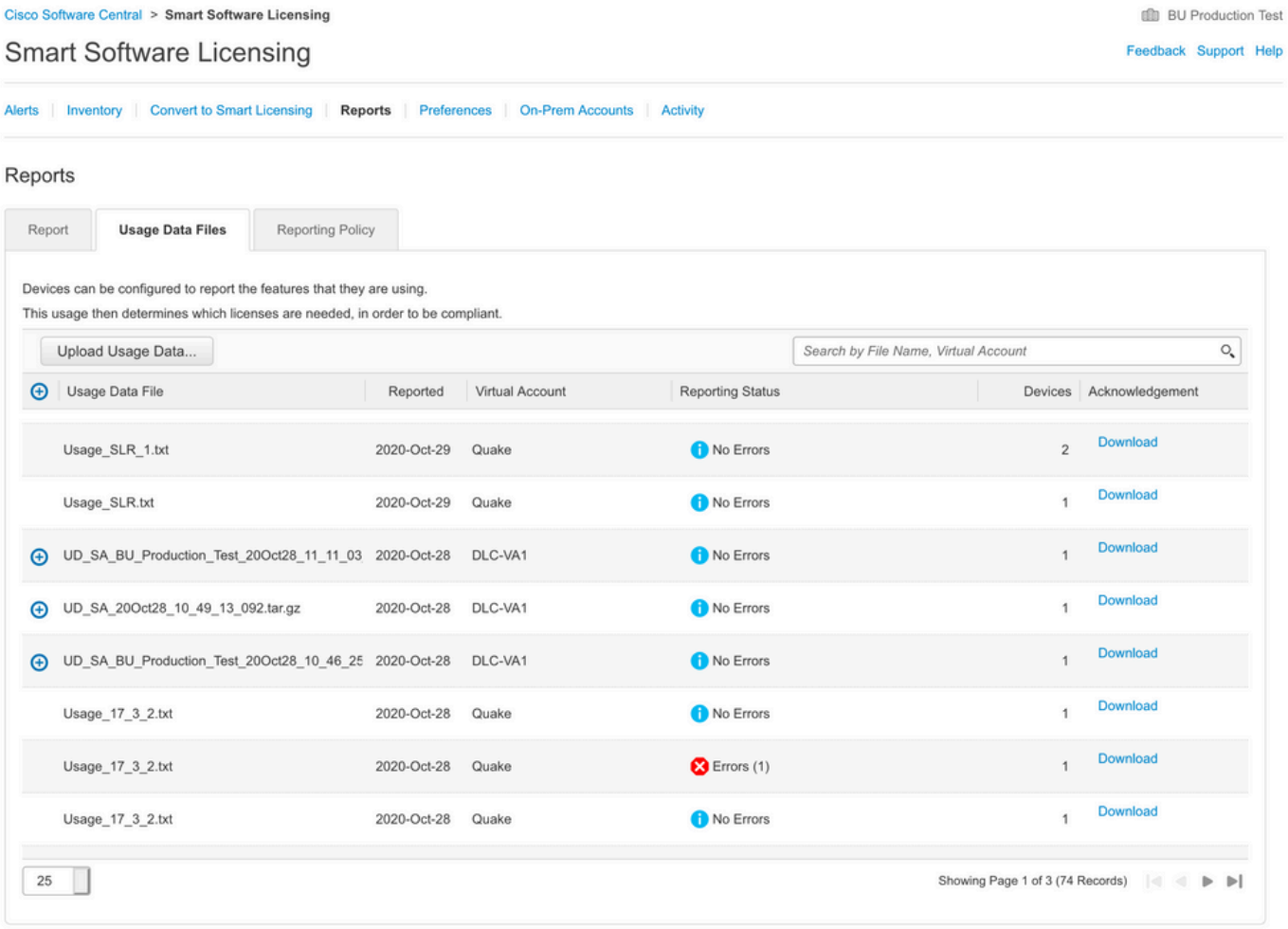
Passaggio 2. Salvare le impostazioni.

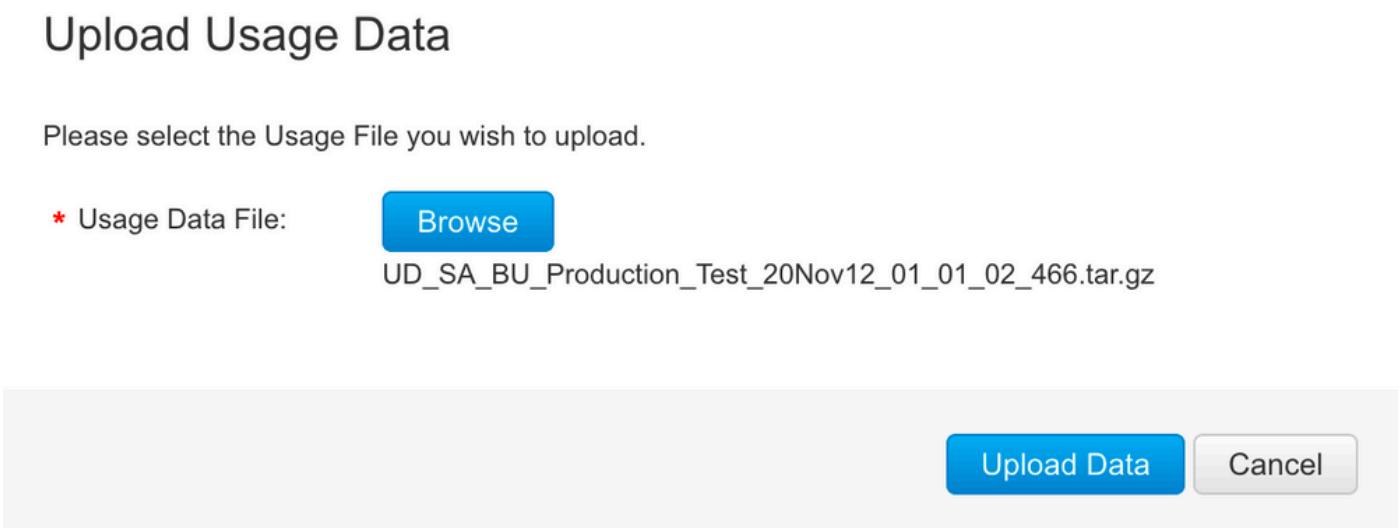


Passaggio 3. Nella barra,Menu fare clic su Product Instances > Download All for Cisco. In questo modo viene scaricato un tar.gz file nella CSLU.

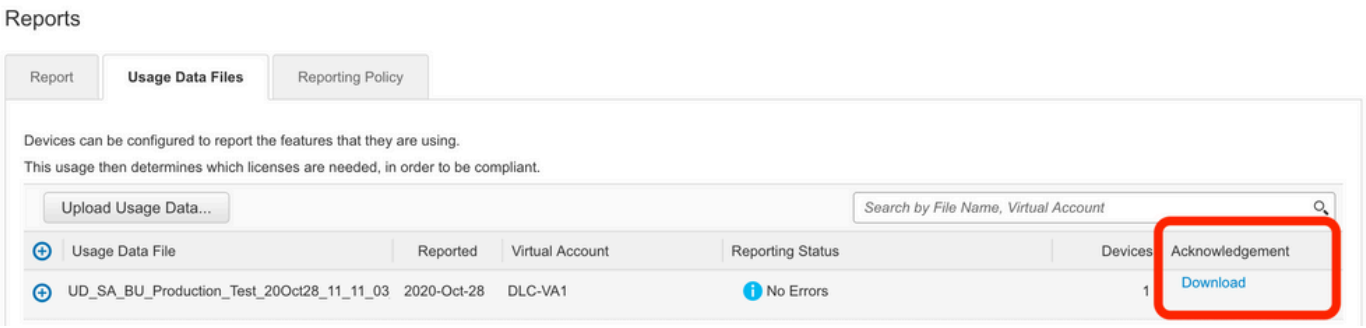


Passaggio 4. Caricare il file in CSM. Nella pagina Smart Account CSM passare a Report > Usage Data Files > Upload usage data. Nel popup, caricare il tar.gz file.

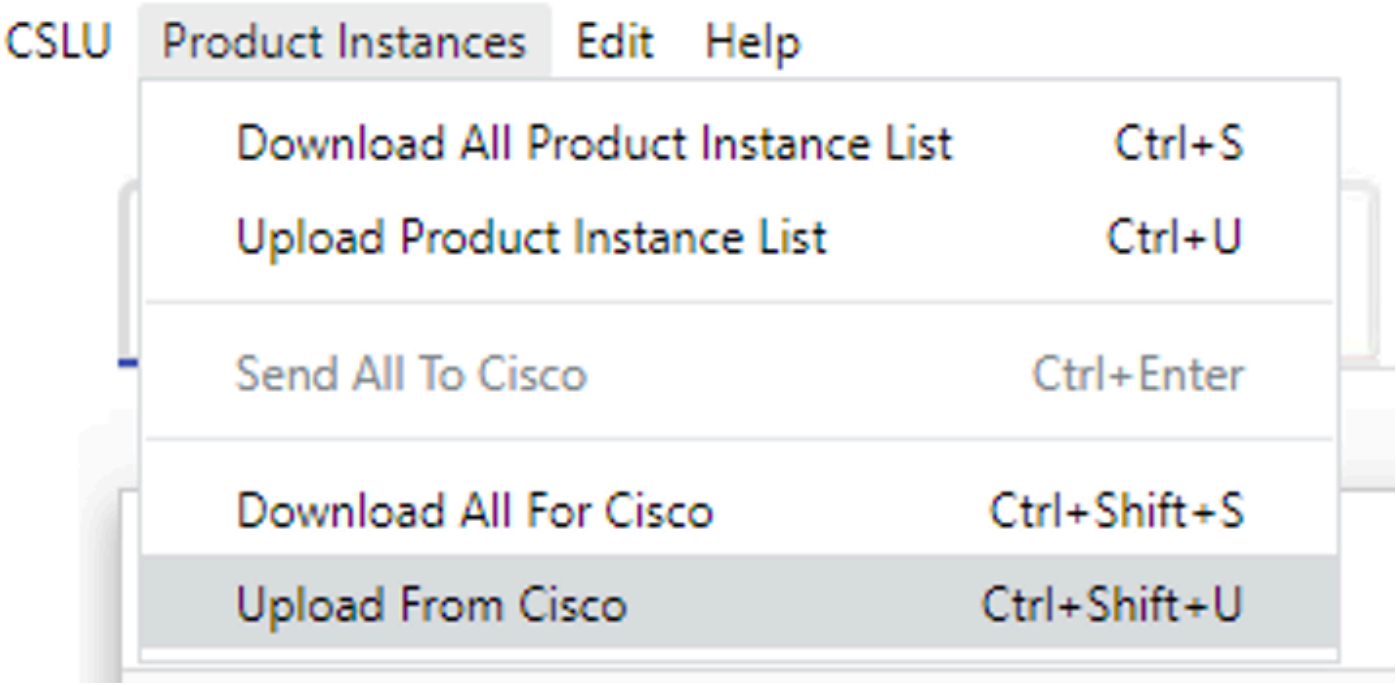




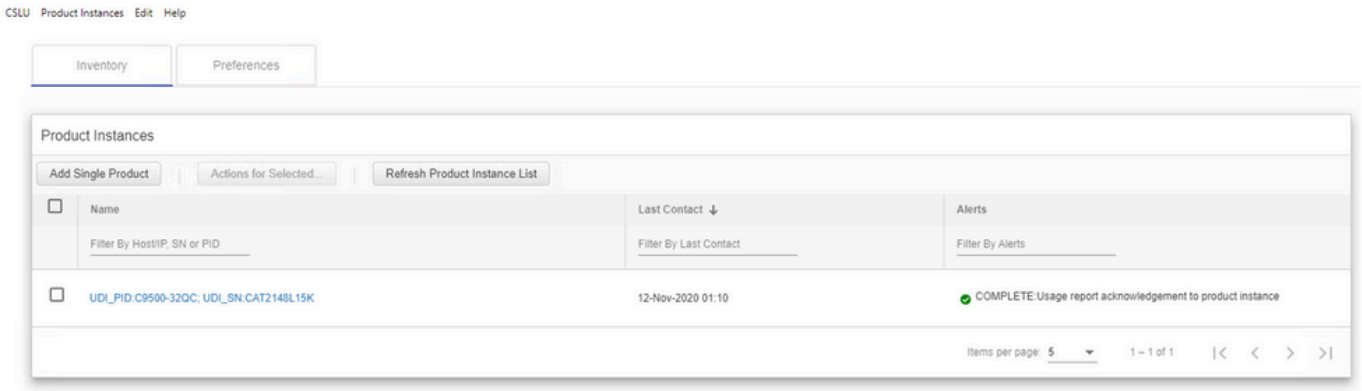
Passaggio 5. Una volta elaborati i dati, viene generato il messaggio di conferma. Scaricare il file ACK e caricarlo su CSLU.



Passaggio 6. In CSLU, importare il file ACK dalla barra dei menu e passare aProduct Instances > Upload from Cisco, come mostrato in questa immagine.



Passaggio 7. Una volta caricato l'ACK, il messaggio viene inviato alle PI. La stessa condizione può essere verificata dalla colonna Avvisi.



SLP - Modalità offline

SLP può funzionare anche in modalità totale offline. Questo è principalmente per le reti air-gapped, che non preferiscono la connettività a Internet e scelgono anche di non utilizzare CSLU. In modalità non in linea, il trasporto è impostato su Off.

Switch(config)#license smart transport off

Same can be verified through, 'show license status'

Switch#show license status

Utility:
Status: DISABLED

Smart Licensing Using Policy:
Status: ENABLED

Data Privacy:
Sending Hostname: yes
Callhome hostname privacy: DISABLED
Smart Licensing hostname privacy: DISABLED
Version privacy: DISABLED

Transport:
Type: Transport Off

Policy:
Policy in use: Merged from multiple sources.
Reporting ACK required: yes (CISCO default)
Unenforced/Non-Export Perpetual Attributes:
First report requirement (days): 365 (CISCO default)
Reporting frequency (days): 0 (CISCO default)
Report on change (days): 90 (CISCO default)
Unenforced/Non-Export Subscription Attributes:
First report requirement (days): 90 (CISCO default)
Reporting frequency (days): 90 (CISCO default)
Report on change (days): 90 (CISCO default)
Enforced (Perpetual/Subscription) License Attributes:
First report requirement (days): 0 (CISCO default)
Reporting frequency (days): 0 (CISCO default)
Report on change (days): 0 (CISCO default)
Export (Perpetual/Subscription) License Attributes:
First report requirement (days): 0 (CISCO default)
Reporting frequency (days): 0 (CISCO default)
Report on change (days): 0 (CISCO default)

Miscellaneous:
Custom Id: <empty>

Usage Reporting:
Last ACK received: Nov 11 15:41:10 2020 EDT
Next ACK deadline: Dec 11 15:41:10 2020 EDT
Reporting push interval: 30 days
Next ACK push check: <none>
Next report push: Dec 07 21:42:30 2020 EDT
Last report push: Nov 07 21:42:30 2020 EDT
Last report file write: <none>

Trust Code Installed: <none>

Ogni volta che si desidera segnalare i dati di utilizzo a CSSM, i report di utilizzo devono essere scaricati come file e caricati manualmente in CSSM. In un sistema ad alta disponibilità, active raccoglie l'utilizzo dei dispositivi di standby/membro.

To download the usage data from PI -

Switch#license smart save usage unreported file bootflash:<file-name>

Above option 'unreported' is recommended to use. This downloads only the files that are yet to be reported
and discard old usage reports, that were Acknowledged.

However, there are other options available for the amount of data that needs to be reported.
For downloading all the available report use option all,
# of daya can be specified

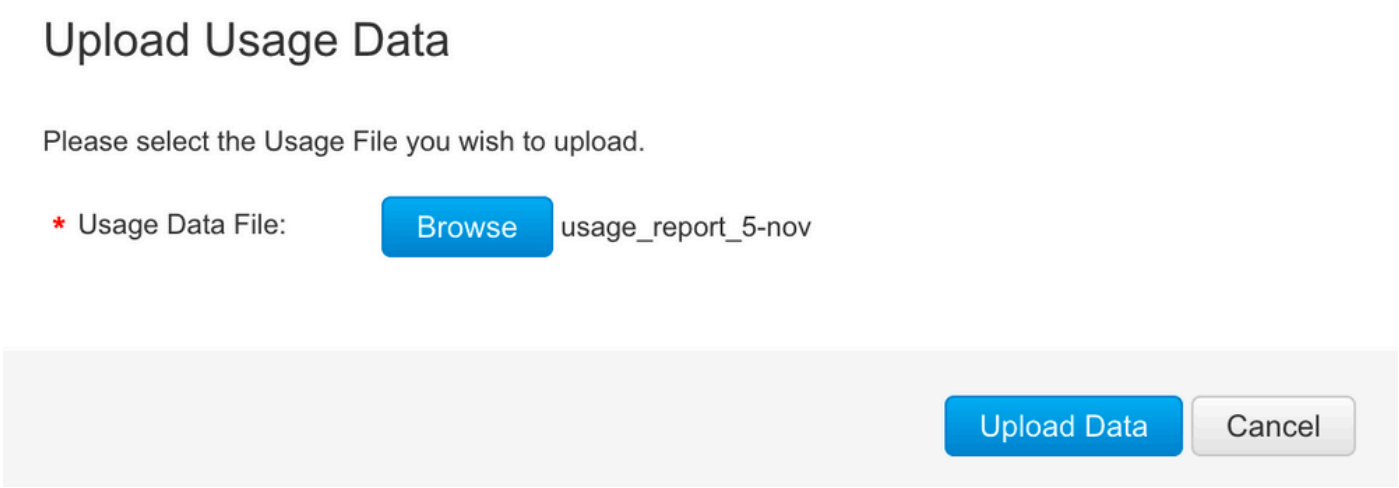
Switch#license smart save usage ?
all Save all reports
days Save reports from last n days
rum-Id Save an individual RUM report
unreported Save all previously un reported reports

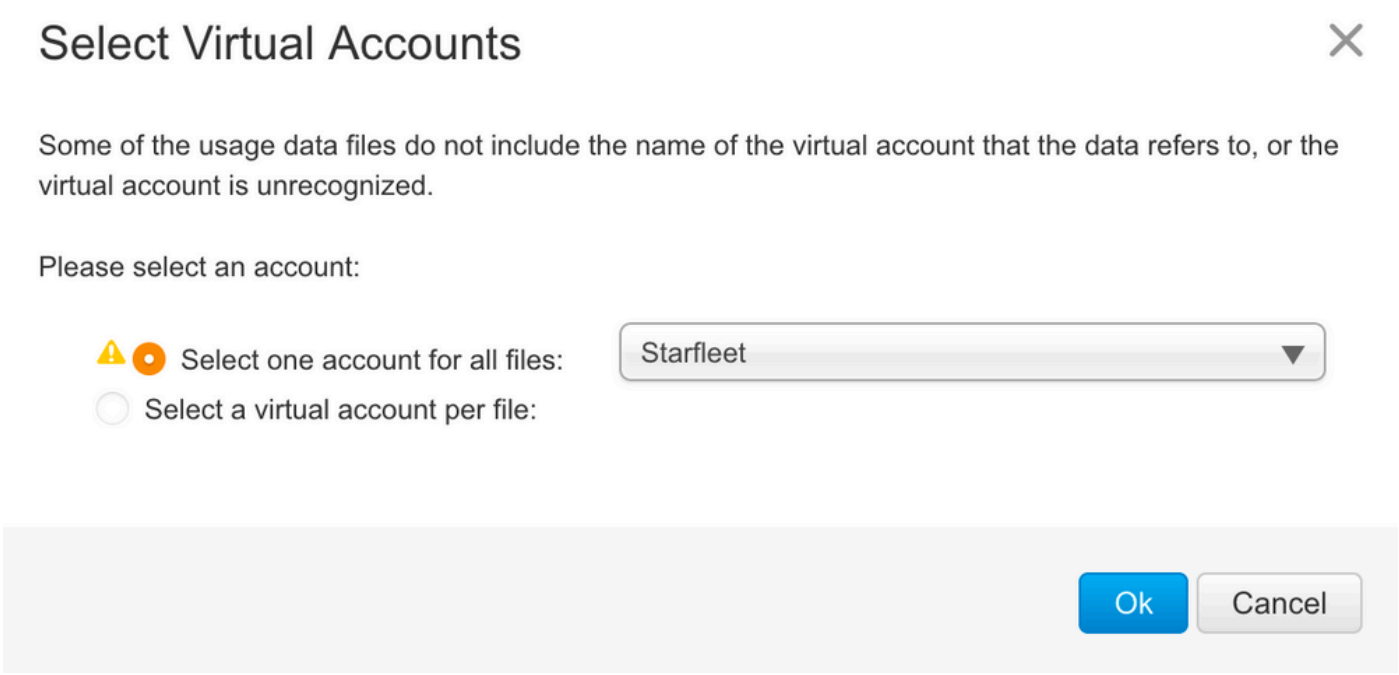
A questo punto, il report deve essere caricato manualmente in CSM.

Esporta i dati di utilizzo salvati dalla PI al desktop.

Nella pagina Smart Account CSM passare a Report > Usage Data Files > Upload usage data. Nella finestra popup, scegliere il report di utilizzo e fare clic su upload.

Una volta caricato il file, è necessario scegliere la VA corretta a cui è associato il dispositivo.





Una volta che i dati sono stati elaborati completamente e la conferma è pronta, scaricare il file e caricarlo sulla PI.

To import the ACK to PI,
Switch#license smart import bootflash:<file-name>
Import Data Successful

Switch#
Nov 11 20:23:06.783: %SMART_LIC-6-POLICY_INSTALL_SUCCESS: A new licensing policy was successfully installed
Switch#

Policy Installed syslog is displayed on console if successful.

Also, the same can be verified using CLI, 'show license all'. The field 'Last ACK received' tells the
last TimeStamp when ACK message was received.

Switch#show license all
Load for five secs: 0%/0%; one minute: 1%; five minutes: 0%
No time source, 16:23:22.294 EDT Wed Nov 11 2020

Smart Licensing Status
======================

Smart Licensing is ENABLED

Export Authorization Key:
Features Authorized:
<none>

Utility:
Status: DISABLED

Smart Licensing Using Policy:
Status: ENABLED

Data Privacy:
Sending Hostname: yes
Callhome hostname privacy: DISABLED
Smart Licensing hostname privacy: DISABLED
Version privacy: DISABLED

Transport:
Type: Transport Off

Miscellaneous:
Custom Id: <empty>

Policy:
Policy in use: Installed On Nov 11 16:23:06 2020 EDT
Policy name: SLP Policy
Reporting ACK required: yes (Customer Policy)
Unenforced/Non-Export Perpetual Attributes:
First report requirement (days): 60 (Customer Policy)
Reporting frequency (days): 60 (Customer Policy)
Report on change (days): 60 (Customer Policy)
Unenforced/Non-Export Subscription Attributes:
First report requirement (days): 30 (Customer Policy)
Reporting frequency (days): 30 (Customer Policy)
Report on change (days): 30 (Customer Policy)
Enforced (Perpetual/Subscription) License Attributes:
First report requirement (days): 0 (CISCO default)
Reporting frequency (days): 90 (Customer Policy)
Report on change (days): 90 (Customer Policy)
Export (Perpetual/Subscription) License Attributes:
First report requirement (days): 0 (CISCO default)
Reporting frequency (days): 90 (Customer Policy)
Report on change (days): 90 (Customer Policy)

Usage Reporting:
Last ACK received: Nov 11 16:23:06 2020 EDT
Next ACK deadline: Dec 11 16:23:06 2020 EDT
Reporting push interval: 30 days
Next ACK push check: <none>
Next report push: Dec 07 21:42:30 2020 EDT
Last report push: Nov 07 21:42:30 2020 EDT
Last report file write: <none>

Trust Code Installed: <none>

License Usage
==========

network-advantage (C9500 Network Advantage):
Description: network-advantage
Count: 1
Version: 1.0
Status: IN USE
Export status: NOT RESTRICTED
Feature Name: network-advantage
Feature Description: network-advantage
Enforcement type: NOT ENFORCED
License type: Perpetual

dna-advantage (C9500 32QC DNA Advantage):

Description: C9500-32QC DNA Advantage
Count: 1
Version: 1.0
Status: IN USE
Export status: NOT RESTRICTED
Feature Name: dna-advantage
Feature Description: C9500-32QC DNA Advantage
Enforcement type: NOT ENFORCED
License type: Subscription

Product Information
==========
UDI: PID:C9500-32QC,SN:CAT2148L15K

Agent Version
==========
Smart Agent for Licensing: 5.0.6_rel/47

License Authorizations
==========
Overall status:
Active: PID:C9500-32QC,SN:CAT2148L15K
Status: NOT INSTALLED

Purchased Licenses:
No Purchase Information Available

Modifiche al comportamento

Le modifiche vengono apportate alla funzione Smart Licensing sulle versioni successive:

- **Sincronizzazione attendibilità** - Dalla versione 17.7.1, il codice di attendibilità viene installato sullo switch su tutte le topologie supportate, quali CSLU e i metodi offline.
- **Modifiche alla privacy** - Dalla versione 17.7.1, le informazioni sulla stringa della versione e sul nome host dalla versione 17.9.1 sono incluse nei rapporti RUM inviati a CSSM, se le rispettive impostazioni di privacy sono disabilitate.
- **Dettagli account**: dalla versione 17.7.1, il messaggio ACK da CSSM include le informazioni sull'account e i dettagli SA/VA.
- **Limitazione dei report RUM** -Da 17.9.1, l'intervallo di segnalazione di quando la PI avvia la comunicazione è limitato. La frequenza minima di segnalazione è limitata a un giorno. Ciò significa che l'istanza del prodotto non invia i rapporti RUM più di una volta al giorno.

Risoluzione dei problemi

Questionario generico per la risoluzione dei problemi

Scenario 1: alcuni protocolli (ossia HSRP) non funzionano più dopo l'aggiornamento di Cisco IOS XE da una versione molto recente (ossia 16.9.x).

Controllare il livello di avvio della licenza per verificare se è ancora lo stesso di prima di aggiornare Cisco IOS XE. È possibile che il livello di avvio della licenza sia stato reimpostato su Networking-Essentials, che probabilmente non supporta i protocolli in errore (ovvero, HSRP).

Scenario 2: Stato della licenza con i messaggi "Motivo dell'errore: impossibile inviare il messaggio HTTP della chiamata iniziale" o "Ultimo tentativo di comunicazione: IN SOSPESO"

Ciò può essere dovuto a problemi di connettività di base. Per risolvere il controllo:

- Connettività di rete per raggiungere CSM: indirizzo IP, percorsi e così via.
- Il fileip http client source interface è configurato correttamente.
- Differenza di tempo. (NTP deve essere configurato per fornire un fuso orario corretto)
- Se la configurazione interna del firewall blocca il traffico verso CSM

Scenario 3: What if log error "%SMART_LIC-3-AUTH_RENEW_FAILED: Authorization RENEW with the Cisco Smart Software Manager (CSSM): dopo un anno di registrazione viene rilevato il metodo non definito 'each' per nil:NilClass".

Registrare nuovamente il prodotto. Generare un nuovo Token ID sul modulo CSM e registrare nuovamente l'istanza del prodotto nel modulo CSM**.**

Scenario 4: messaggio di errore "%SMART_LIC-3-COMM_FAILED: Communications failure" (Errore di comunicazione), quando non sono presenti errori di connettività con Cisco.

Quando non si verificano problemi di connettività al modulo CSM e se non è presente una PI, l'errore indicato può essere dovuto al fatto che il certificato è stato rimosso a causa del recente aggiornamento del server. Il certificato è necessario per l'autenticazione TLS dei due lati in comunicazione. In tal caso, configurare CLI ip http client secure-trustpoint SLA-TrustPoint sulla PI e riprovare.

Debug IP

Per risolvere i problemi, i comandi raccolti da PI sono:

show license all
show license tech support
show license eventlog
show license history message
show license tech events
show license rum id all

For debugging Trust Installation/Sync -

Switch#show license tech support | s Trust
Trust Establishment:
Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
Last Response: <none>
Failure Reason: <none>
Last Success Time: <none>

Last Failure Time: <none>
Trust Acknowledgement:
Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
Last Response: <none>
Failure Reason: <none>
Last Success Time: <none>
Last Failure Time: <none>
Trust Sync:
Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0
Last Response: <none>
Failure Reason: <none>
Last Success Time: <none>
Last Failure Time: <none>
Trusted Store Interface: True
Local Device: No Trust Data
Overall Trust: No ID

For debugging Usage reporting timers/intervals -

Switch#show license tech support | in Utility
Utility:
Start Utility Measurements: Nov 11 16:46:09 2020 EDT (7 minutes, 34 seconds remaining)
Send Utility RUM reports: Dec 07 21:42:30 2020 EDT (26 days, 5 hours, 3 minutes, 55 seconds remaining)
Process Utility RUM reports: Nov 12 15:32:51 2020 EDT (22 hours, 54 minutes, 16 seconds remaining)

For Collecting all btrace logs for debugging -

Step 1. Switch#request platform software trace rotate all
Step 2. Switch#show logging process iosrp internal start last boot to-file bootflash:<file-name>

If there are any failues on PULL mode, ensure server SL_HTTP is Acive

```
HTTP server application session modules:
  Session module Name  Handle Status   Secure-status     Description
SL_HTTP                2      Active   Active          HTTP REST IOS-XE Smart License Server
HOME_PAGE              4      Active   Active          IOS Homepage Server
OPENRESTY_PKI          3      Active   Active          IOS OpenResty PKI Server
SSI7FBDE91B27B0-web    8      Active   Active          wsma infra
HTTP_IFS               1      Active   Active          HTTP based IOS File Server
BANNER_PAGE            5      Active   Active          HTTP Banner Page Server
WEB_EXEC               6      Active   Active          HTTP based IOS EXEC Server
SSI7FBDED27A1A8-lic    7      Active   Active          license agent app
SSI7FBDF0BD4CA0-web    9      Active   Active          wsma infra
NG_WEBUI               10     Active   Active          Web GUI
```

Debug della CSLU

Se viene eseguito il debug di un qualsiasi problema relativo alla CSLU, è importante che venga utilizzato il file di registro presente in questa directory del PC installato con CSLU.

C:\Users\<user-name>\AppData\Roaming\CSLU\var\logs

Riferimenti correlati

- Migrazione a SSL tramite criteri - Migrazione delle licenze SL/SLR/PLR legacy a SL tramite criteri
- Note di rilascio: RN-9200, RN-9300, RN-9400, RN-9500, RN-9600
- Guide alla configurazione: Cat9200-CG, Cat9300-CG, Cat9400-CG, Cat9500-CG, Cat9600-CG
- Riferimenti per i comandi: Cat9200-CR, Cat9300-CR, Cat9400-CR, Cat9500-CR, Cat9600-CR
- Documentazione e supporto tecnico – Cisco Systems

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).