Risoluzione dei problemi relativi alle chiavi di opzione sugli endpoint registrati nel cloud

Sommario

Introduzione

In questo documento viene descritto come gestire le chiavi di opzioni in un endpoint registrato nel cloud.

Prerequisiti

Requisiti

Si consiglia di familiarizzare con questi argomenti:

- Control Hub Platform
- Amministrazione degli endpoint tramite l'interfaccia grafica utente (GUI) dell'endpoint e sezione "Devices" dell'hub di controllo
- SO room

Componenti usati

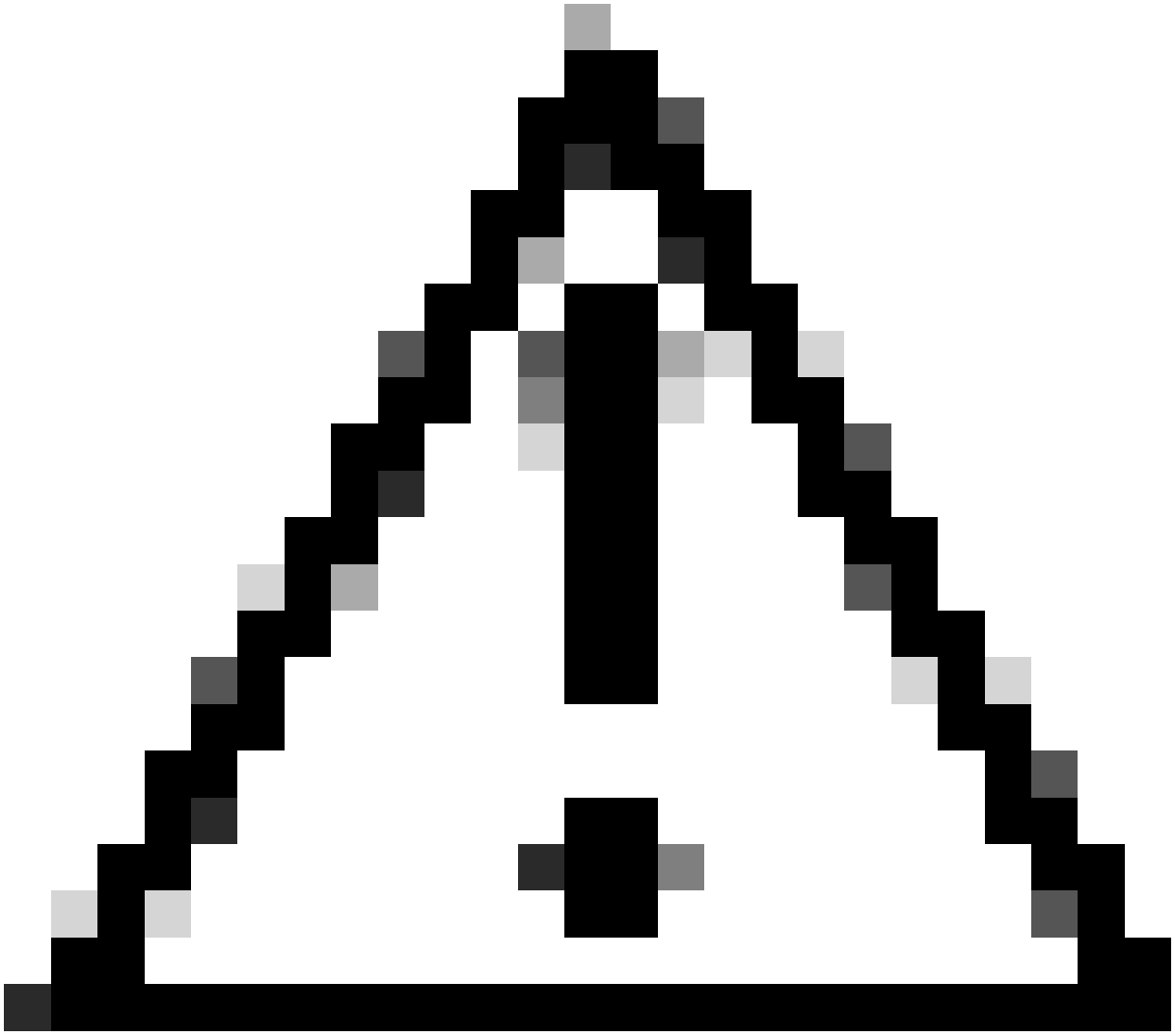
Le apparecchiature qui elencate sono state utilizzate per eseguire i test e produrre i risultati descritti nel presente documento:

- Organizzazione hub di controllo
- Endpoint SX80
- Endpoint Codec Pro

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.

Che cos'è un tasto di opzione?

Le chiavi di opzione sono valori stringa alfanumerici che è possibile applicare a un endpoint per migliorarne le funzionalità. Le parti alfanumeriche della chiave (generalmente 3 parti) sono separate da trattini (-). Un esempio di chiave di opzione è 1S050-1-79FDE3AC.



Attenzione: il valore della chiave dell'opzione mostrato nell'esempio non è utilizzabile e non corrisponde a una chiave dell'opzione reale generata in passato. Si tratta di una stringa casuale di numeri alfanumerici utilizzati come esempio.

Le chiavi di opzione non vengono utilizzate dall'endpoint per scaricare nuove funzionalità da Internet. Quando viene consegnato, l'endpoint è dotato di tutte le funzionalità disponibili e dispone di tutte le funzionalità hardware e software necessarie per consentirne l'esecuzione. Tuttavia, a seconda di parametri quali il contratto, le opzioni di acquisto effettuate dal cliente quando si contatta il proprio rappresentante commerciale e alcune limitazioni specifiche del paese applicabili, alcune delle funzionalità che l'endpoint è in grado di utilizzare non sono disponibili e sono state disattivate.

Questo può accadere, ad esempio, quando si decide di acquistare un endpoint ma si è certi che alcune delle funzionalità opzionali offerte insieme ad esso non verranno utilizzate nel proprio ambiente. In seguito, è possibile decidere di procedere con l'acquisto dell'endpoint senza pagare le opzioni extra offerte. È possibile acquistare una chiave di opzione che abilita qualsiasi funzionalità aggiuntiva necessaria in futuro.

È importante notare che non è necessario acquistare separatamente ogni chiave di opzione. Alcuni di essi possono essere acquistati senza costi aggiuntivi. Per ulteriori informazioni sui costi delle chiavi di opzione, è necessario contattare il Customer Success Manager, il rappresentante commerciale o il partner oppure rivolgersi a un agente del team di gestione delle licenze aprendo una richiesta di assistenza al team di gestione delle licenze (vedere questa sezione) o a TAC.

Molti endpoint, inoltre, sono dotati di chiavi di opzione preinstallate e pronte all'uso. Ciò significa che agli endpoint sono già state applicate alcune chiavi di opzione.

Come ottenere una chiave di opzione?

Per ottenere la chiave di opzione, rivolgersi al team che gestisce le licenze o a TAC. In precedenza, è possibile contattare il Customer Success Manager (CSM), il DSM o il partner per discutere i potenziali costi di addebito.

Avviso: gli amministratori esperti possono ricordare che il team che gestisce le licenze può essere contattato all'indirizzo e-mail licensing@cisco.com. Questa condizione può essere

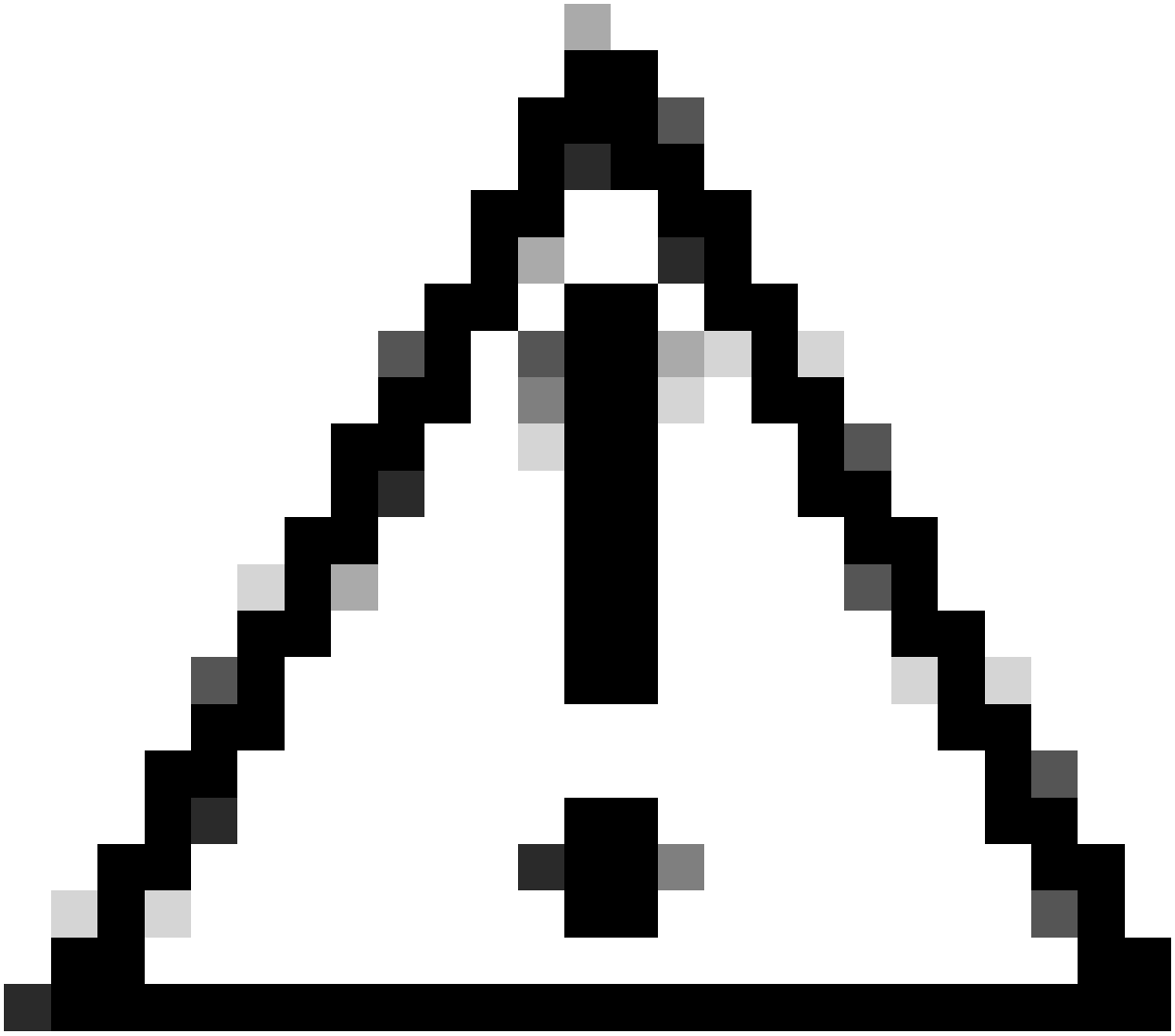
---

menzionata anche nelle guide all'amministrazione degli endpoint meno recenti. Tuttavia, questo indirizzo e-mail è stato rimosso e al momento non è più utilizzato. È necessario contattare il reparto licenze aprendo direttamente un ticket con le parole chiave appropriate per la licenza.

In caso di domande su una chiave di opzione specifica o se si desidera ottenere assistenza per applicarla da una prospettiva tecnica, è necessario aprire una richiesta con TAC.

In che modo TAC o licenze verificano l'idoneità per le chiavi di opzione?

Quando si contatta il team TAC o di licenza per ottenere una chiave di opzione, è necessario fornire alcune informazioni di base, ad esempio il numero dell'ordine di vendita, il numero di contratto o la chiave PAK. Quando si esegue un ordine, i codici di opzione ottenuti, insieme a qualsiasi altro servizio aggiuntivo, fanno parte del contratto e vengono quindi associati a questi identificatori univoci. Su richiesta, il punto di contatto per le vendite può condividere con voi questi ID.



Attenzione: se TAC o Licenza segnala che non si è idonei a ottenere una chiave di licenza, i tre motivi più comuni sono:

1) L'utente non ha acquistato la chiave di opzione richiesta e pertanto non fa parte del contratto.

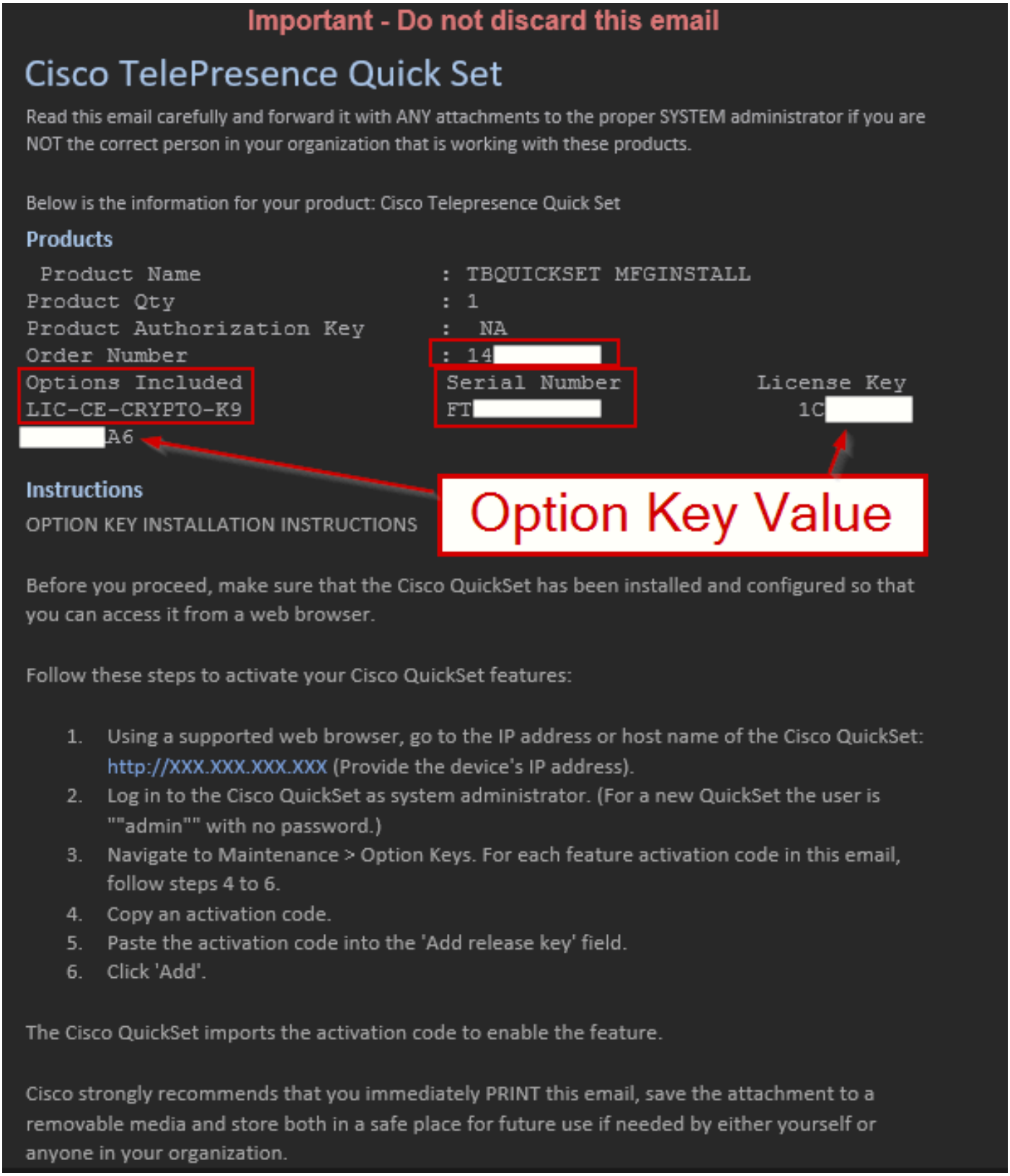
2) La chiave dell'opzione è stata acquistata, ma non è stata associata al contratto o alla chiave PAK.

3) La chiave dell'opzione è stata acquistata, ma il contratto o la chiave PAK forniti non sono validi. Accertarsi di aver condiviso con TAC o Licensing gli ID corretti associati alla chiave dell'opzione acquistata.

Per ulteriori informazioni, contattare il rappresentante commerciale. Ciò non rientra nel campo di applicazione del TAC o della licenza e gli agenti coinvolti non sono in grado di contribuire a chiarirlo.

Come si riceve la chiave di opzione una volta completata la procedura di richiesta?

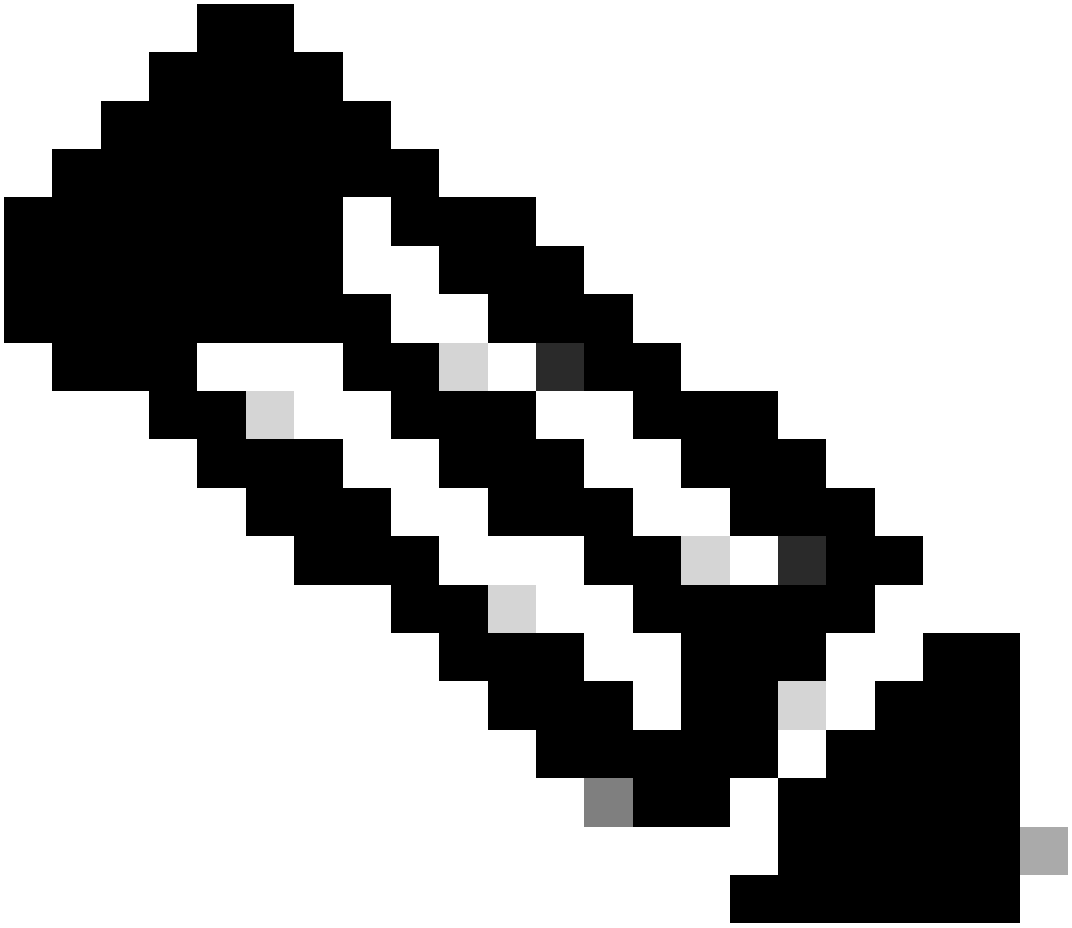
Dopo che il team che gestisce le licenze ha approvato la richiesta di ottenere una chiave di opzione, si riceve un'e-mail contenente informazioni dettagliate sulla richiesta. L'immagine è simile a questa (solo una parte dell'e-mail è fornita a scopo dimostrativo, il resto è stato omesso):



Messaggio di posta elettronica contenente il valore della chiave dell'opzione

Avviso: nell'immagine precedente è condivisa solo una parte dell'e-mail. Leggere attentamente l'e-mail prima di apportare modifiche e applicare la chiave all'endpoint. Inoltre, il valore del tasto di opzione nell'immagine viene troncato e visualizzato su due righe separate.

In questa e-mail vengono fornite informazioni importanti: il nome del prodotto, il numero di ordine associato all'ordine della chiave di opzione, le opzioni/funzionalità abilitate dalla chiave, il numero di serie dell'endpoint a cui la chiave è associata e il valore della chiave di opzione. Inoltre, sono incluse istruzioni su come applicare la chiave e i link relativi alla documentazione (la documentazione non è mostrata in questa immagine, questa parte è stata omessa).



Nota: se è stata aperta una richiesta con TAC, TAC può collaborare con un agente del team che gestisce le licenze, che può essere coinvolto attivamente, e inviare un'e-mail per condividere direttamente le informazioni sullo stato della richiesta e i dettagli necessari per generare la chiave di opzione.

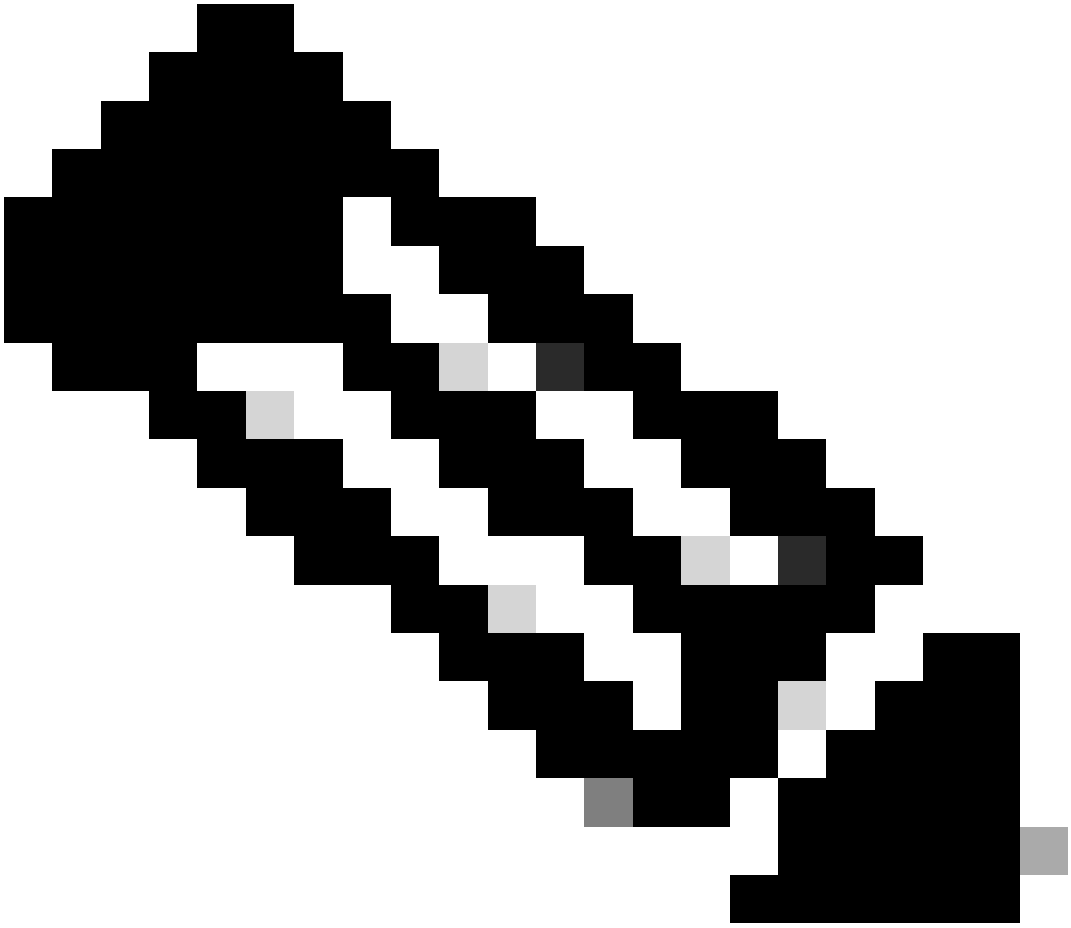
In alcuni casi non è possibile applicare una chiave di opzione?

Sì, in alcune circostanze non è possibile applicare una chiave di opzione a un endpoint:

- Ogni chiave di opzione è associata al numero di serie di un endpoint specifico. È necessario applicare ogni chiave di opzione all'endpoint per il quale è stata richiesta. Se si tenta di applicare la chiave Option a un altro endpoint, non funzionerà.
- Per ottenere i tasti di opzione per le funzionalità che si desidera abilitare, è necessario rivolgersi alle risorse Cisco ufficiali. Non utilizzare chiavi di opzione da Internet da entità non verificate.
- Poiché la chiave dell'opzione è associata a un endpoint specifico, non è possibile trasferirla

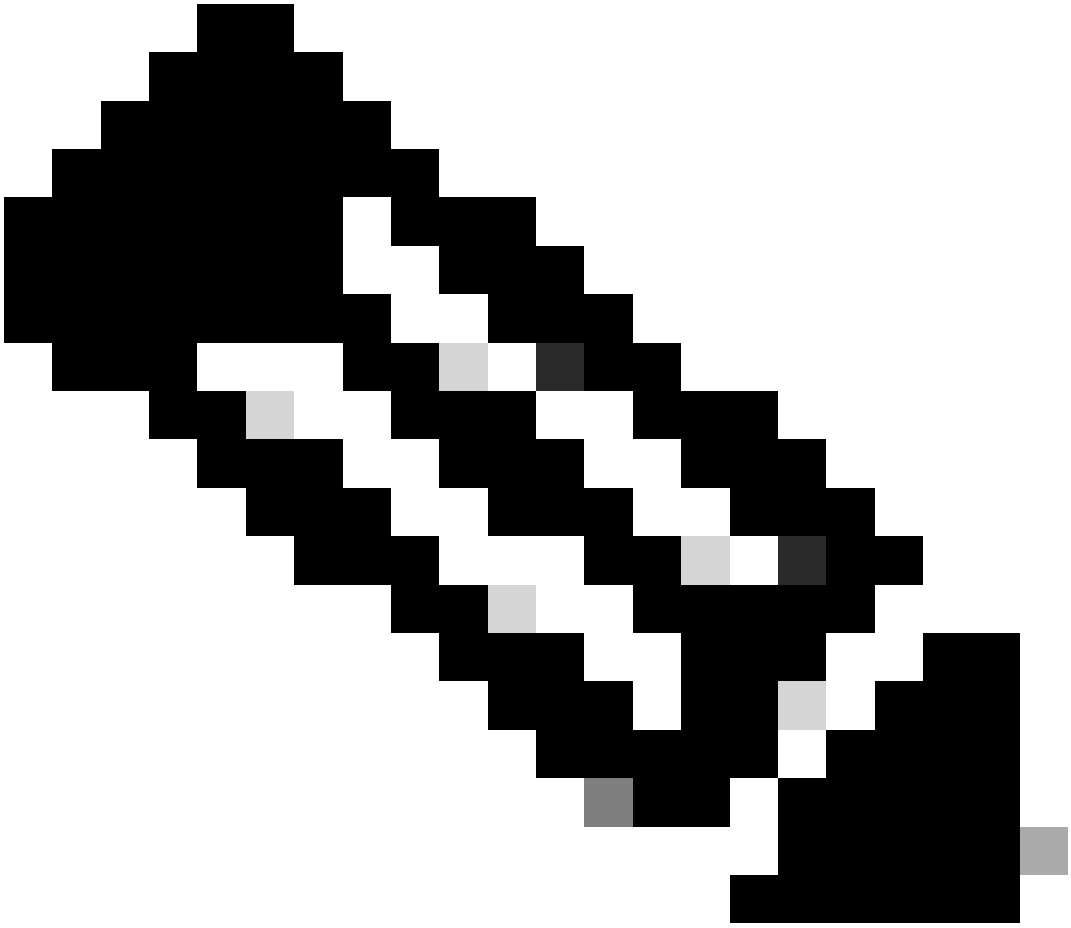
in un nuovo endpoint. Se una funzionalità attivata da una chiave di opzione non è più necessaria per un determinato endpoint, ad esempio perché è stata spostata in un'altra posizione, non è possibile utilizzare questa chiave di opzione in un altro endpoint. È necessario richiedere una chiave di opzione per ciascun endpoint separatamente. (Vi è un'eccezione a questo punto menzionata più avanti)

- Se l'endpoint supporta già una funzionalità e per impostazione predefinita su di essa è installato un tasto di opzione, non è possibile utilizzare un altro tasto di opzione che abiliti la stessa funzionalità. Ad esempio, molti dispositivi supportano la crittografia preconfigurata. La chiave dell'opzione di crittografia che consente al dispositivo di utilizzare la crittografia è installata nel dispositivo per impostazione predefinita. Impossibile richiedere una chiave di opzione per abilitare la crittografia e applicarla all'endpoint. Le chiavi di opzione non possono essere impilate.
- Alcuni endpoint non supportano alcune funzionalità specifiche. Ad esempio, alcuni endpoint non supportano la crittografia. Non è possibile utilizzare una chiave di opzione di crittografia su tali endpoint. Esistono limitazioni hardware e software che impediscono all'endpoint di utilizzare questa funzionalità. Si consiglia di controllare la scheda tecnica del dispositivo specifico prima di provare ad applicare qualsiasi tasto di opzione.
- Per alcune funzionalità, è necessario utilizzare una versione minima specifica del sistema operativo affinché siano disponibili. Se un dispositivo è appena stato ricevuto tramite RMA, prima di applicare una chiave di opzione al dispositivo, accertarsi che si trovi nell'ultimo software.



Nota: per verificare se una periferica supporta la crittografia, è necessario controllare l'ID prodotto della periferica in uso. Se l'ID prodotto contiene i caratteri alfanumerici "K9", significa che supporta la crittografia e che per impostazione predefinita è abilitata la crittografia (non è necessario applicare alcuna chiave di opzione al dispositivo, in genere per i dispositivi più recenti) oppure che per il dispositivo è necessaria una chiave di opzione per poter utilizzare la crittografia (in genere per i dispositivi meno recenti). Se l'ID prodotto contiene i caratteri alfanumerici "K7", il dispositivo non supporta la crittografia e questa è una limitazione hardware. Impossibile utilizzare le chiavi di opzione per rendere l'endpoint compatibile con la crittografia.

Per i dispositivi della serie SX,MX che non hanno né "K7" né "K9" nel loro ID prodotto, è possibile verificare se supportano la crittografia controllando i log dei dispositivi e l'interfaccia utente grafica del dispositivo selezionando Software => Option Keys => Installed Option Keys. Entrambe queste modalità sono descritte più avanti in questo articolo.



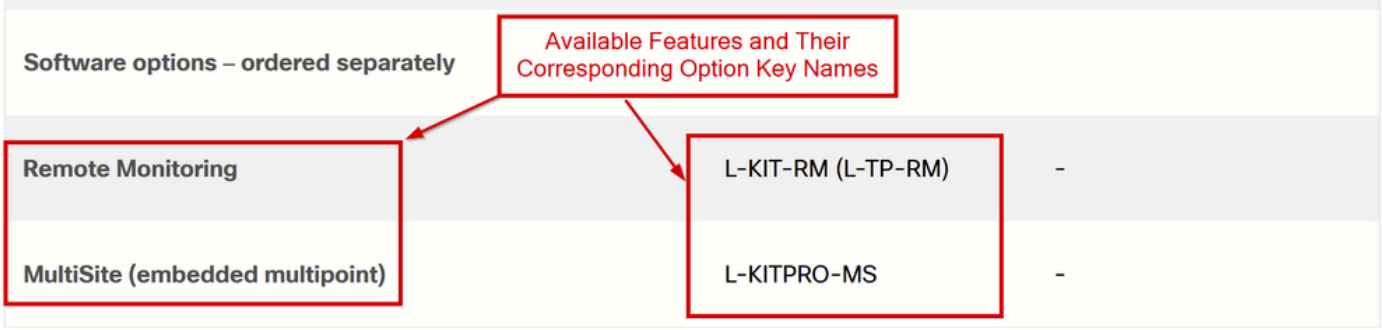
Nota: i tasti di scelta installati sull'endpoint per impostazione predefinita (non aggiunti dall'utente) e i tasti di opzione aggiunti dall'amministratore non verranno rimossi quando si esegue una reimpostazione predefinita. Una volta riavviato, l'endpoint continua ad avere le stesse funzionalità di prima.

Come verificare se un endpoint supporta una chiave di opzione specifica?

Per individuare le chiavi di opzione supportate in base a un endpoint, è possibile procedere in tre modi diversi.

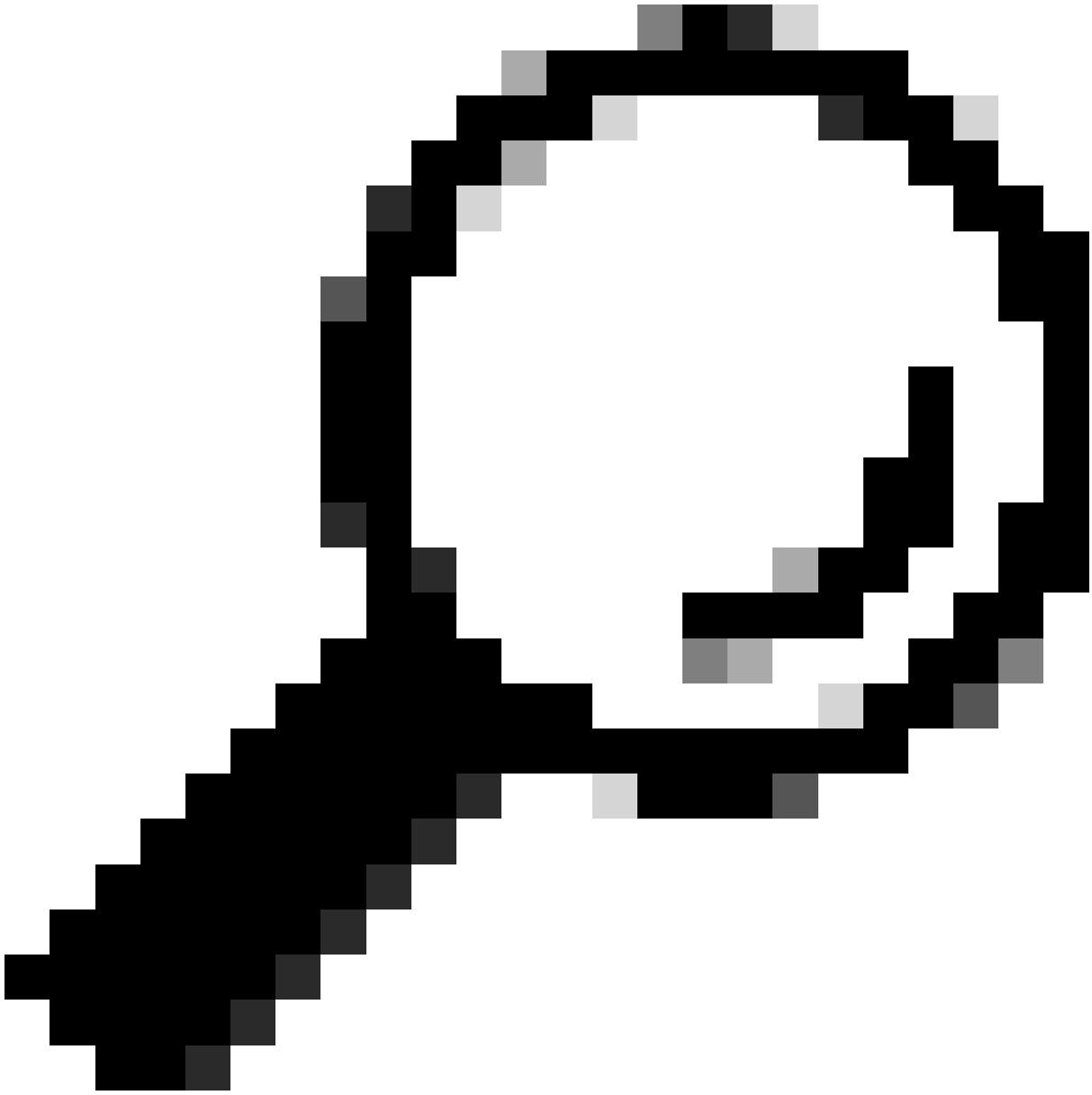
Controllare il foglio dati dell'endpoint

Per verificare se l'endpoint dispone di funzionalità aggiuntive che si desidera abilitare con una chiave di opzione, è possibile controllare il foglio dati dell'endpoint. A scopo dimostrativo, viene utilizzato il datasheet dell'endpoint Codec Pro:



Sezione Opzioni software nel foglio dati dell'endpoint

Nella sezione Informazioni per l'ordine, selezionare Opzioni software - ordinate separatamente, in cui sono elencate le funzionalità aggiuntive che è possibile aggiungere all'endpoint. Dallo screenshot fornito, è possibile visualizzare il nome della funzionalità sul lato sinistro e il nome della chiave Option sul lato destro. Si noti che la chiave di crittografia Option non è menzionata, in quanto è preinstallata sul Codec Pro.



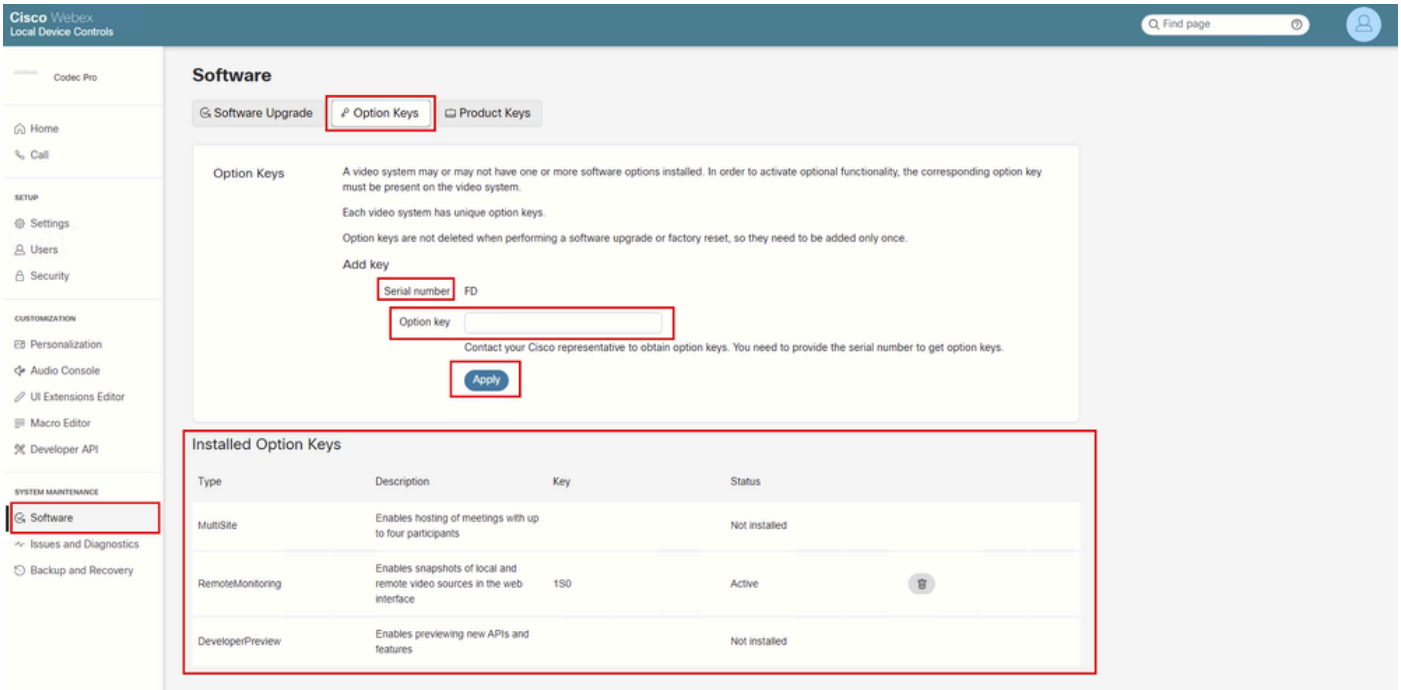
Suggerimento: i fogli dati degli endpoint precedenti possono contenere queste informazioni in sezioni diverse. Leggere attentamente per individuare le opzioni software aggiuntive descritte.

Controllare l'interfaccia utente dell'endpoint

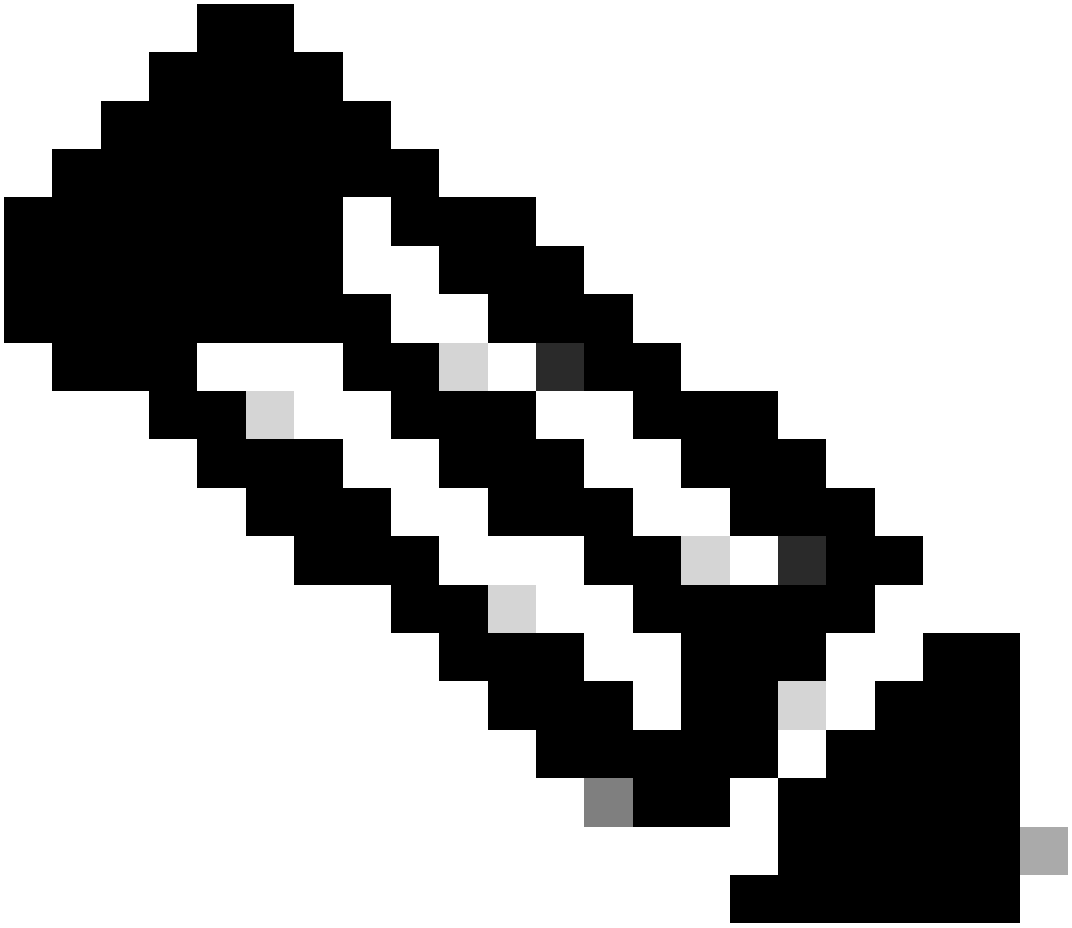
È necessario accedere all'interfaccia utente dell'endpoint digitandone l'indirizzo IP sul browser o accedendo a Control Hub e navigando su Dispositivi, selezionare il dispositivo desiderato dall'elenco e sotto la sezione Supporto fare clic su Avvia accanto a Controlli dispositivo locale. La GUI dell'endpoint verrà aperta in una nuova scheda del browser. Entrambi questi metodi di accesso all'interfaccia utente dell'endpoint richiedono un accesso diretto alla rete dell'endpoint.

Accesso all'interfaccia utente dell'endpoint tramite Control Hub - Sezione supporto

Passare a Software nella sezione Manutenzione sistema. Fare clic su Option Keys. Da questo menu, è possibile aggiungere il valore di Option Key nella casella di testo e fare clic su Apply.



Individuazione dei tasti di opzione dall'interfaccia utente dell'endpoint



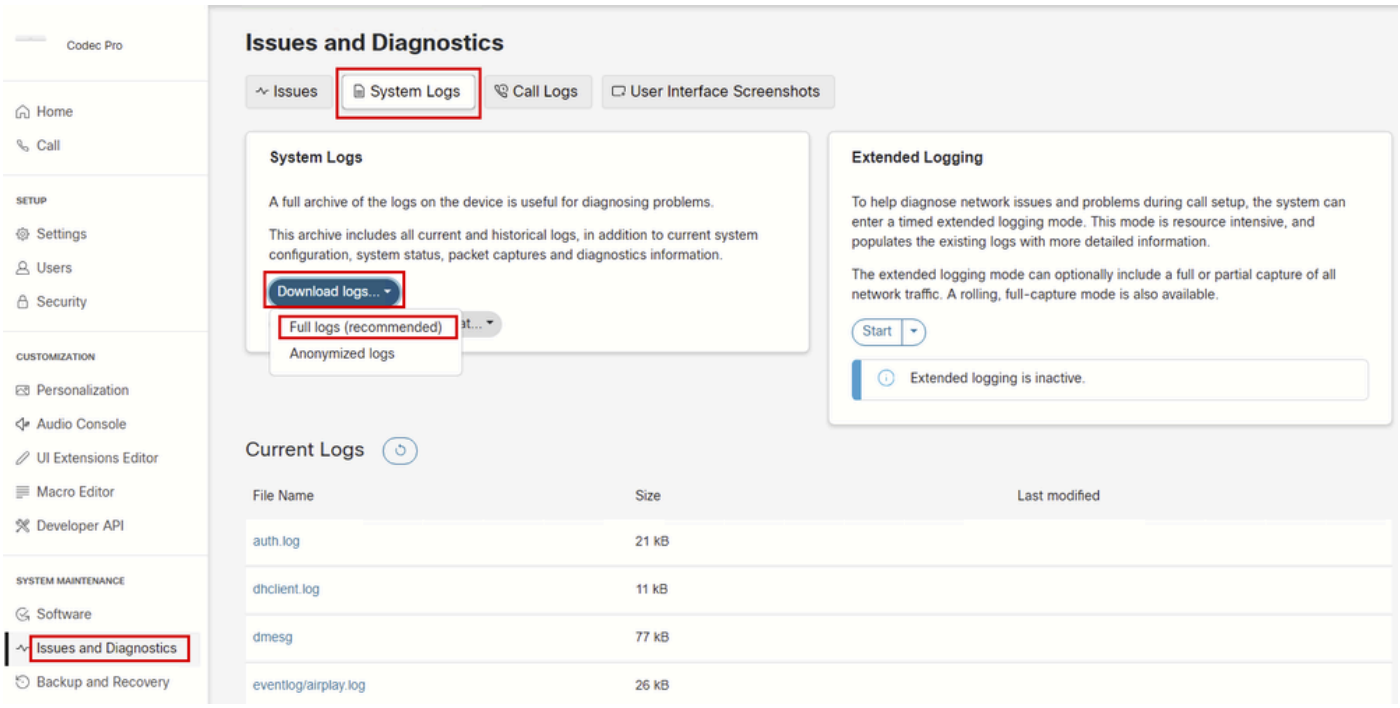
Nota: dopo aver applicato una chiave di opzione, si consiglia di riavviare l'endpoint.

Nella sezione Chiavi opzione installate è possibile visualizzare tutte le chiavi opzione installate dall'endpoint. Nella colonna Status (Stato) viene visualizzato quale di questi tasti è Active (Attivo), ossia se sono già stati installati.

In questa sezione è inoltre possibile eliminare una chiave di opzione facendo clic sull'icona del cestino accanto a ciascuna chiave installata.

Controllare I Registri Degli Endpoint

Accedere all'interfaccia utente del dispositivo e selezionare Problemi e diagnostica nella sezione Manutenzione sistema. Fare clic su Log di sistema. Quindi, fare clic sulla freccia in giù accanto a Download logs e fare clic su Full logs (consigliato). Verrà scaricato un bundle di log compresso nel computer.



Raccolta log dalla GUI dell'endpoint

Decomprimere il bundle di log raccolto e individuare il file xstatus.txt. Aprire il file in un'applicazione per la gestione delle note e cercare la parola chiave OptionKeys. È possibile trovare tutte le chiavi di opzione disponibili per l'endpoint e verificare quali di esse sono state aggiunte e sono attive, il che è indicato dal valore True o False accanto alla riga di registro corrispondente:

```
*s SystemUnit Software OptionKeys DeveloperPreview: False
*s SystemUnit Software OptionKeys Encryption: True
*s SystemUnit Software OptionKeys MultiSite: False
*s SystemUnit Software OptionKeys RemoteMonitoring: True
```

Righe log chiavi di opzione da bundle di log raccolto

Perché alcuni tasti di opzione non sono elencati nella sezione Option Key sull'interfaccia utente dell'endpoint?

L'immagine mostra i tasti di opzione riportati nei file di registro di un Codec Pro con ID prodotto contenente il carattere "K9". Ciò significa che l'endpoint supporta la crittografia.

```
*s SystemUnit Software OptionKeys DeveloperPreview: False
*s SystemUnit Software OptionKeys Encryption: True
*s SystemUnit Software OptionKeys MultiSite: False
*s SystemUnit Software OptionKeys RemoteMonitoring: True
```

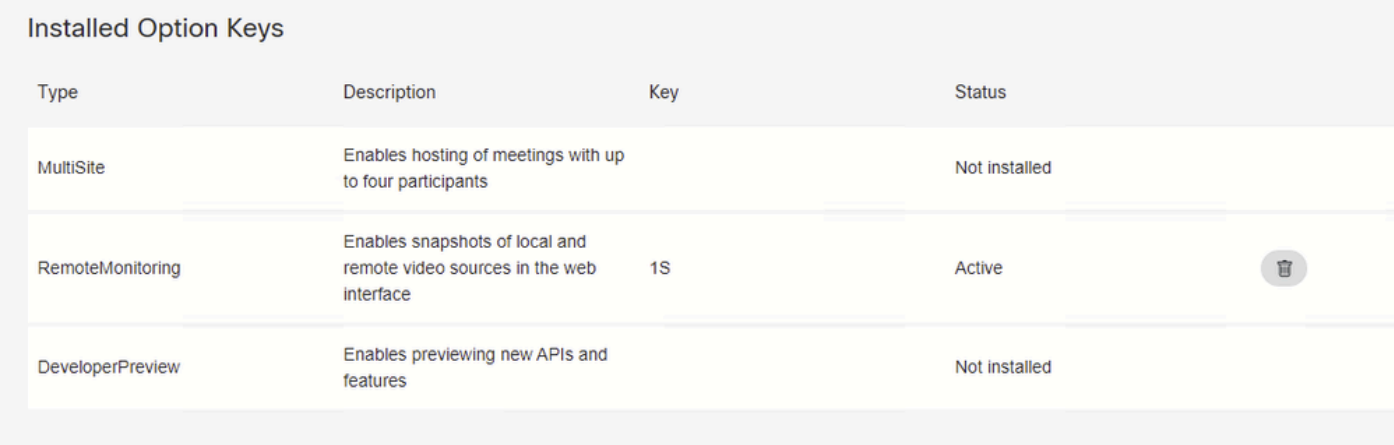
Righe log chiavi di opzione da bundle di log raccolto

Notate lo snippet:

```
*s SystemUnit Software OptionKeys Encryption: True
```

È possibile verificare che l'opzione Encryption Key sia impostata su True. Ciò significa che la chiave di opzione è stata applicata all'endpoint.

Dalla GUI dell'endpoint, selezionare Software nella sezione System Maintenance (Manutenzione sistema). Fare clic su Option Keys. Questa è la sezione Chiavi di opzione installate di questo endpoint:

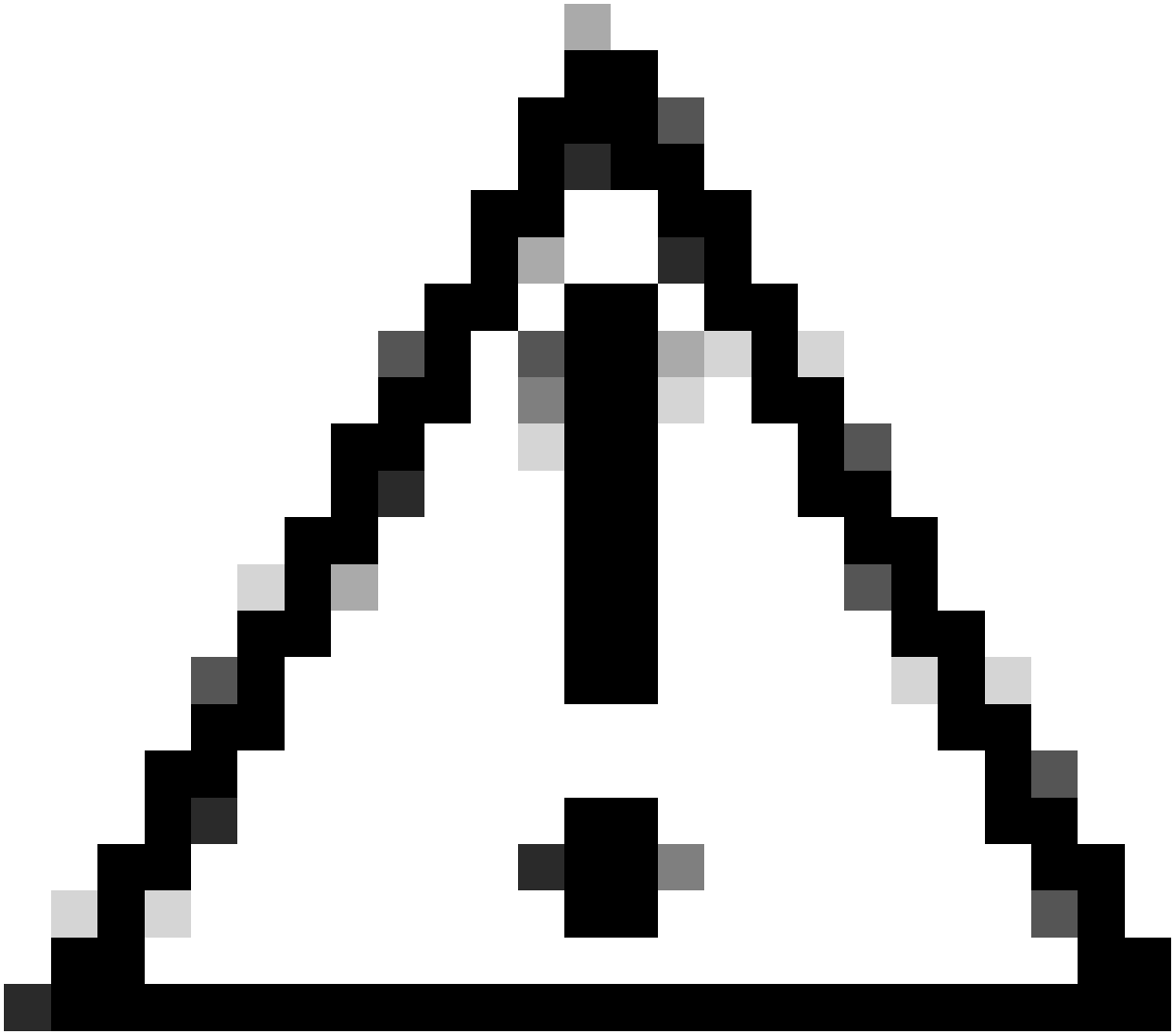


Sezione Option Keys installata sull'interfaccia utente dell'endpoint

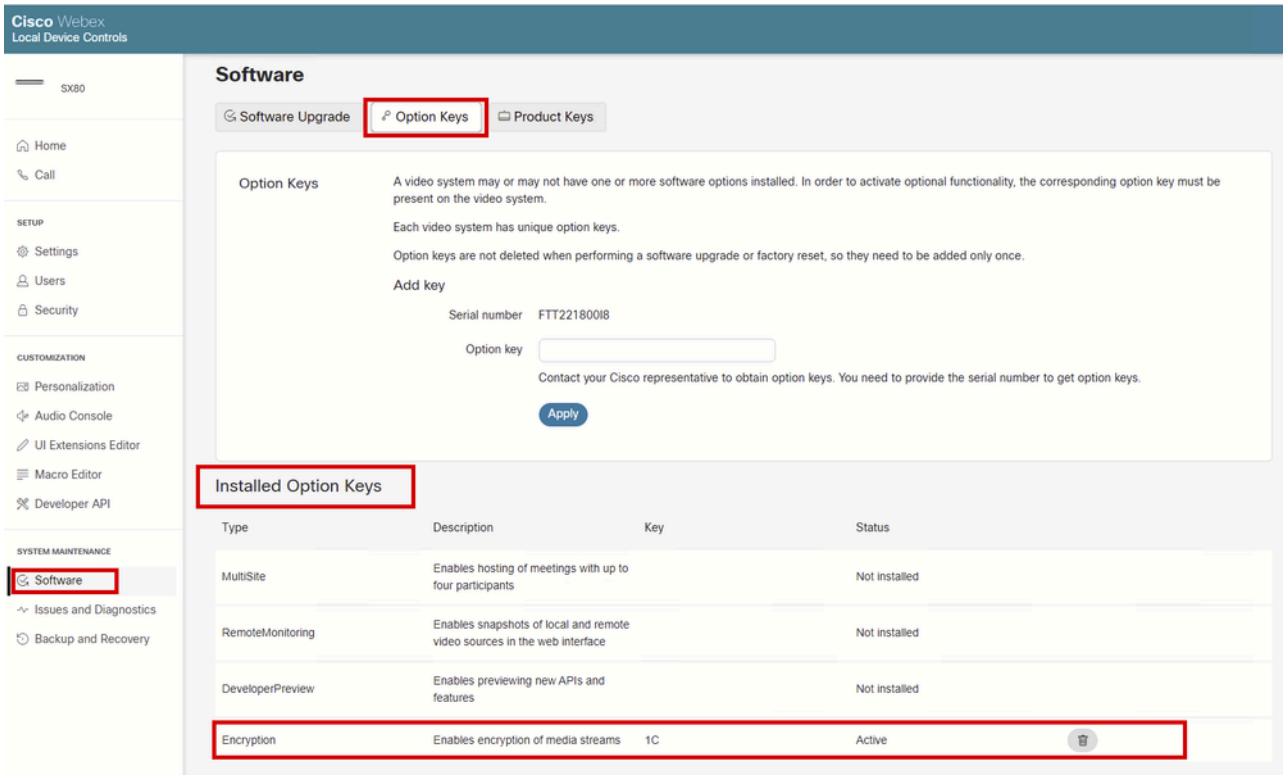
È possibile notare che la chiave Encryption Option, visualizzata nei log, non è presente in questa sezione. Non solo non viene visualizzato come installato, ma è assente dall'elenco.

Si tratta di un comportamento previsto. Alcune chiavi di opzione sono preinstallate sugli endpoint, ad esempio le chiavi di opzione di crittografia. Essendo preinstallati, non sono elencati nella sezione Installed Option Keys dell'interfaccia utente di Endpoint. La sezione Chiavi di opzione installate mostra solo le chiavi di opzione che un amministratore può aggiungere manualmente. La crittografia è disponibile per impostazione predefinita e non viene pertanto visualizzata in questa sezione.

In queste situazioni, l'unica fonte di informazione è rappresentata dai log dell'endpoint, se si desidera verificare se una determinata chiave di opzione è abilitata o meno. Se si ripristina una periferica, le chiavi di opzione predefinite non vengono rimosse. Anche le chiavi di opzioni installate dall'amministratore e non presenti per impostazione predefinita non vengono rimosse dopo la reimpostazione predefinita.



Attenzione: per gli endpoint precedenti, il risultato non è sempre identico a quello descritto sopra. Possono esistere piccole differenze a seconda della versione del sistema operativo e del tipo di dispositivo. Ad esempio, su un dispositivo SX80 registrato nel cloud, la chiave di crittografia è visibile nella sezione Installed Option Keys sull'interfaccia utente dell'endpoint, mentre per Codec Pro non è:



Chiave dell'opzione di crittografia sull'interfaccia utente dell'endpoint

Sugli endpoint serie SX e MX, le chiavi di opzione sono state gestite in modo diverso, pertanto è possibile notare le differenze minori.

Regola generale per le chiavi di opzione di crittografia

Le chiavi delle opzioni di crittografia costituiscono un tipo di eccezione in quanto le funzionalità di crittografia sono controllate dalle caratteristiche hardware e software degli endpoint. Esiste una regola generale che è possibile utilizzare per determinare se l'endpoint supporta la crittografia e se è abilitato o meno, nei casi in cui non si è certi del numero di ID del prodotto. Si presume che l'utente abbia letto le sezioni precedenti di questo articolo per essere in grado di eseguire i passaggi descritti:

- Cercare innanzitutto la parola chiave OptionKeys nel file di registro xstatus.txt dell'endpoint.
- Se l'opzione Encryption Key è impostata su True, la crittografia è supportata e attivata. Se è impostata su False, è possibile che l'endpoint supporti la crittografia ma non sia abilitato.
- Quindi, controllare l'interfaccia utente dell'endpoint nella sezione Installed Option Keys.
- Se la chiave di crittografia è installabile nella GUI, è necessario ottenere una chiave e applicarla per abilitare la crittografia.
- Se la chiave di crittografia non può essere installata nella GUI (non è elencata tra le chiavi di opzione disponibili), l'endpoint non supporta la crittografia e non è possibile utilizzarla per abilitarla.

Per concludere che un endpoint non supporta la crittografia quando l'ID prodotto non è disponibile:

- Questo frammento deve essere visualizzato nei log degli endpoint:

```
*s SystemUnit Software OptionKeys Encryption: False
```

- La chiave Encryption Option non può essere visualizzata come installabile nell'interfaccia utente dell'endpoint.

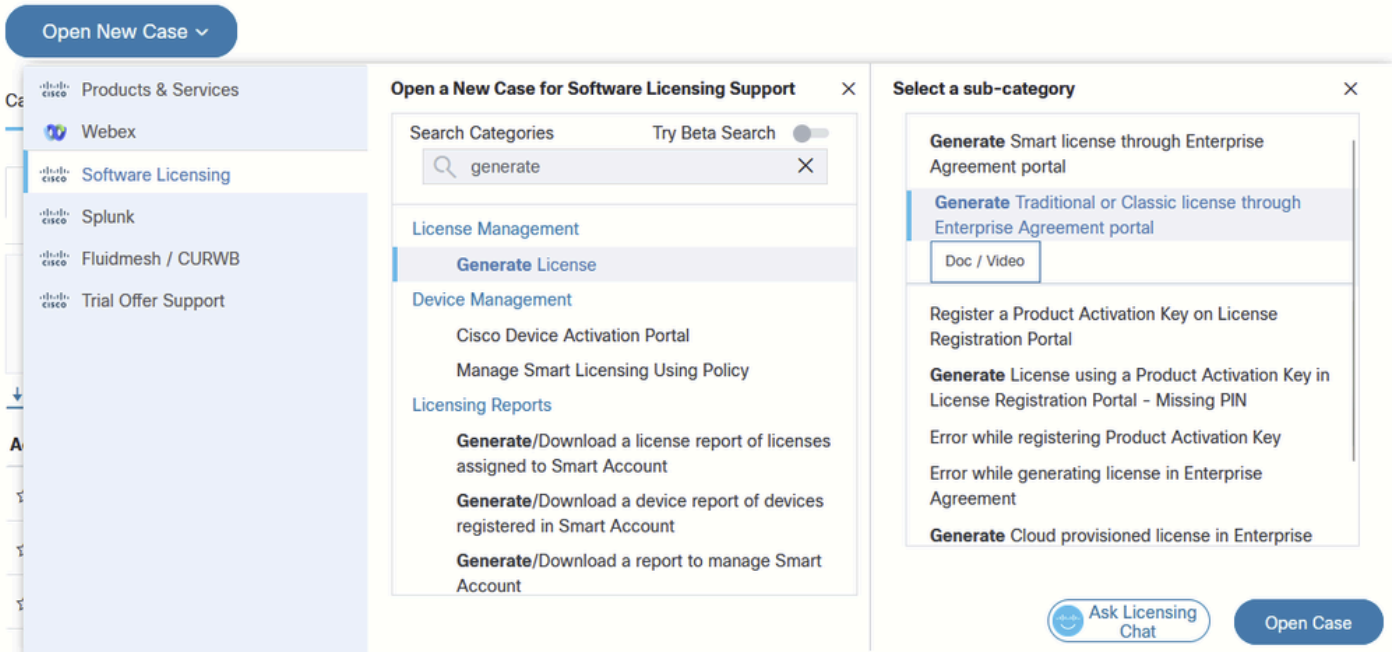
Cosa succede dopo l'esecuzione di una procedura di autorizzazione al reso (RMA)?

In una sezione precedente è stato accennato che le chiavi di opzione generate e fornite all'utente sono associate in modo univoco al numero di serie dell'endpoint. Nei casi in cui un endpoint si trovi di fronte a un problema hardware e sia idoneo per il processo RMA (Return Material Authorization - Autorizzazione restituzione materiale), è necessario restituire il dispositivo a Cisco e riceverne uno nuovo. Il nuovo endpoint ricevuto non includerà alcuna chiave di opzione tra quelle aggiunte manualmente. Le devi aggiungere ancora.

In questi casi, contattare il team che gestisce le licenze o il TAC e spiegare la situazione con un nuovo biglietto o con il biglietto esistente in cui è stata approvata la RMA. Il team che gestisce le licenze condividerà con il cliente una nuova chiave associata al nuovo dispositivo. È necessario applicare questa chiave al dispositivo. La vecchia chiave diventa obsoleta e non può più essere utilizzata. Qualsiasi tentativo di utilizzare la vecchia chiave di opzione sul nuovo dispositivo ricevuto da RMA non avrà esito positivo e non è consigliato.

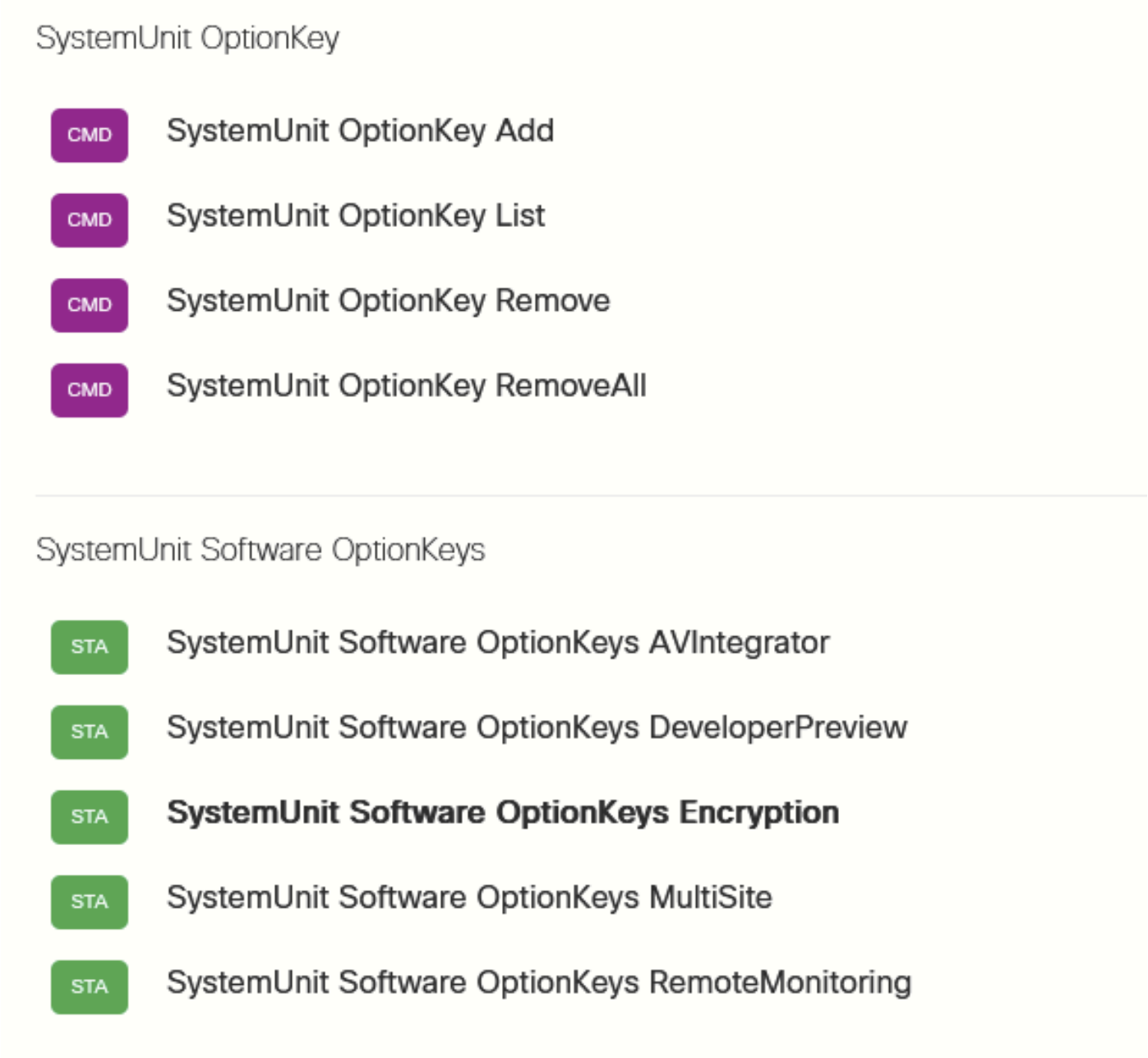
Come aprire una richiesta di assistenza in Licensing Team?

Passare a Support Case Manager. Accedere con l'account Cisco e fare clic su Open New Case (Apri nuova richiesta). Passare a Licenze software e selezionare Genera licenza. Quindi fare clic su Genera licenza tradizionale o classica tramite Enterprise Agreement Portal. Fare clic su Open Case.



Gestione delle chiavi di opzione con i comandi xAPI

È possibile visitare questo collegamento per leggere la documentazione xAPI che elenca i comandi disponibili che possono essere utilizzati per gestire le chiavi di opzione su un endpoint. Si noti che, a parte l'aggiunta e la rimozione di ogni chiave singolarmente, è possibile eliminare tutte le chiavi di opzione da un endpoint: SystemUnit OptionKey RemoveAll. Non è possibile aggiungere più chiavi contemporaneamente. L'aggiunta di chiavi deve essere eseguita manualmente una alla volta.



Comando xAPI per la gestione delle chiavi di opzione

Confronto tra codici "Product Key" e codici "Option Key"

Un codice Product Key è diverso da un codice di opzione. I codici "Product Key" vengono utilizzati per trasformare un determinato dispositivo endpoint in un altro dispositivo endpoint con un comportamento diverso e talvolta con funzionalità diverse. Ad esempio, un codice Product Key può essere utilizzato per trasformare un Mini Room Kit in un USB per ambiente. Con i codici "Product Key" non si aggiungono nuove funzionalità a un dispositivo. Stai trasformando un prodotto in un tipo diverso di prodotto. Non è supportato da tutti gli endpoint. Molti dispositivi possono passare da un prodotto all'altro all'interno delle proprie impostazioni di configurazione.

I codici Product Key sono associati al numero di serie del dispositivo.

Informazioni correlate

- Data sheet Codec Pro

- Support Case Manager
- Documentazione xAPI per sistema operativo Room

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).