

# Ripristino della GUI dell'endpoint registrato nel cloud offline in Control Hub

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Descrizione dettagliata dello scenario](#)

[Ripristina il dispositivo](#)

[Contattare TAC per configurare manualmente un account amministratore sull'endpoint](#)

[Password utente del supporto remoto non accettata](#)

[Informazioni correlate](#)

---

## Introduzione

In questo documento viene descritto il ripristino dell'account dell'endpoint quando gli account locali vengono disabilitati dopo la registrazione del cloud e quando l'endpoint è offline nell'hub di controllo.

## Prerequisiti

### Requisiti

Si consiglia di familiarizzare con questi argomenti:

- piattaforma Control Hub
- Registrazione e amministrazione degli endpoint tramite l'interfaccia grafica dell'endpoint.

### Componenti usati

Questa apparecchiatura è stata utilizzata per eseguire i test e produrre i risultati descritti nel presente documento:

- Endpoint Room Kit
- Endpoint Desk 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.

## Descrizione dettagliata dello scenario

Quando si registra un dispositivo nel cloud, viene richiesto di decidere se mantenere attivi gli account utente locali sul dispositivo stesso. Per impostazione predefinita, gli account utente locali vengono eliminati.

In questo documento viene descritto come ripristinare l'account admin dell'endpoint quando sono stati disabilitati gli account locali nel dispositivo dopo la registrazione del cloud e l'endpoint è offline in Control Hub.

Registrati alla schermata popup di Webex dall'interfaccia utente dell'endpoint

Ciò significa che non è possibile accedere all'interfaccia grafica dell'utente o alla GUI del dispositivo tramite il browser utilizzando l'indirizzo IP del dispositivo. È possibile accedere alla GUI del dispositivo solo tramite la piattaforma Control Hub passando a Devices nella sezione Management dell'hub di controllo. Quindi, scegliere uno dei dispositivi online per accedere alla GUI e fare clic su Local Device Control nella sezione Support:

Controllo dispositivo locale nell'hub di controllo

Viene visualizzata una nuova finestra. Selezionare Proceed per aprire l'interfaccia utente del dispositivo:

## Launch Local Device Controls



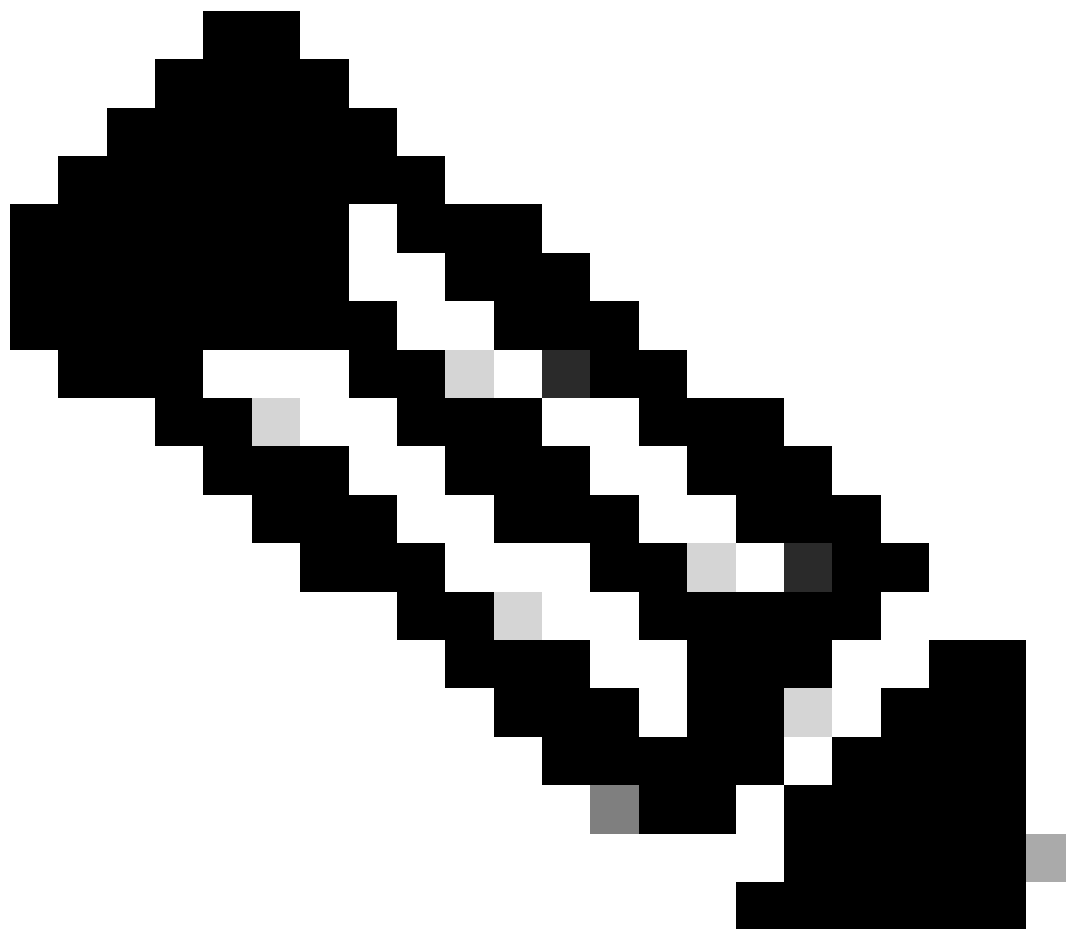
This will open Local Device Controls in a new tab.

Access to Local Device Controls requires that you are on the same network as the device.

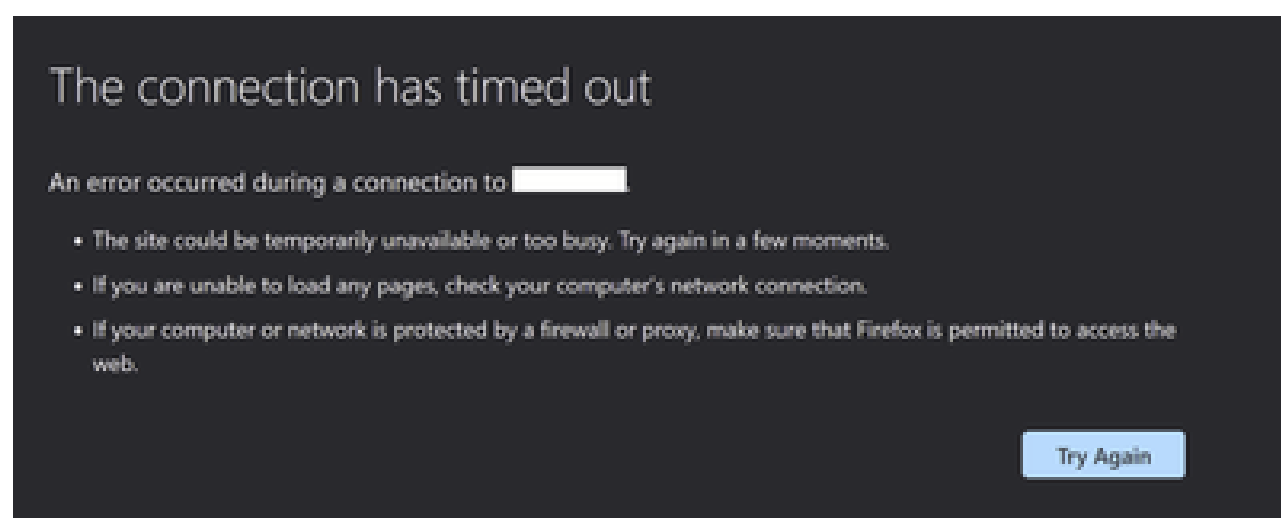


Popup Controlli dispositivo locale in Control Hub

Quindi, nel browser viene visualizzata l'interfaccia utente dell'endpoint. Da qui, è possibile creare un nuovo utente e utilizzare questo utente per accedere alla GUI del dispositivo utilizzando il proprio indirizzo IP nel browser. L'intera procedura è descritta in dettaglio in questo video: [Activating User Accounts on Cloud Registered Devices](#) .



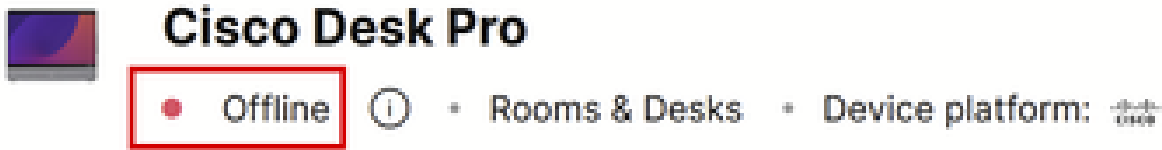
Nota: è necessario essere nella stessa rete dell'endpoint, altrimenti non sarà possibile accedere alla GUI. In caso contrario, la pagina verrà visualizzata nel browser dopo aver fatto clic su Continua:



Messaggio di connessione timeout browser

---

Si verifica un problema quando l'endpoint viene visualizzato come non in linea nell'hub di controllo (mostrato di seguito):



Stato offline endpoint nell'hub di controllo

In questo scenario, non è possibile accedere alla GUI dell'endpoint da Control Hub. Il Controllo dispositivo locale descritto in precedenza in questo articolo non funzionerà poiché accede praticamente all'interfaccia utente del dispositivo tramite HTTP e richiede che il dispositivo sia online. Se si è scelto di disabilitare gli account utente locali durante la registrazione del dispositivo, in modo deliberato o accidentale, non sarà possibile accedere alla GUI del dispositivo utilizzando il relativo indirizzo IP sul browser. In questa fase, non è più possibile accedere alla GUI del dispositivo. A meno che non sia possibile riportare in linea il dispositivo con alcune procedure di risoluzione dei problemi di base accedendo fisicamente al dispositivo, il dispositivo viene bloccato.

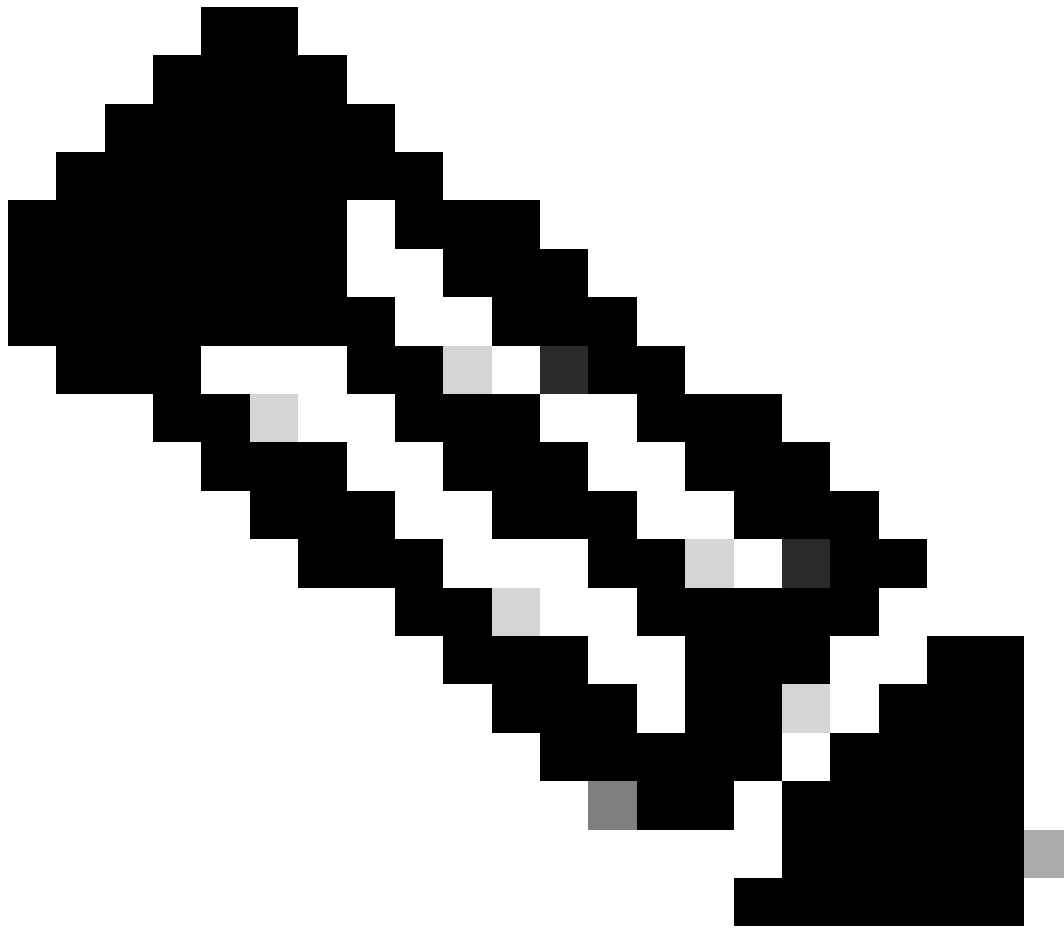
Per uscire da questa situazione, si propongono due piani d'azione:

- Ripristina il dispositivo.
- Contattare TAC dopo aver ottenuto una chiave di accesso remoto.

## Ripristina il dispositivo

Il ripristino in fabbrica del dispositivo in questo scenario specifico può essere eseguito accedendo fisicamente al dispositivo. Sono disponibili due opzioni:

- Dal touch panel collegato all'endpoint (navigatore o periferica Touch 10), passare alle impostazioni e selezionare l'opzione Factory Reset (Ripristino in fabbrica). Per i dispositivi della scheda che non dispongono di un touch panel collegato, lo schermo tattile dell'endpoint ha il pulsante Settings (Impostazioni) nell'angolo superiore destro dello schermo.
- Gli endpoint hanno un foro sul retro o sulla parte inferiore del dispositivo. Il foro, a seconda del dispositivo, potrebbe essere coperto da un cappuccio in plastica. È possibile utilizzare un perno di sicurezza o una graffetta e inserirla nel foro e premere per 10-15 secondi. Poi, inizierà un reset di fabbrica.



Nota: quando si esegue il reset di fabbrica, tutte le configurazioni e i file del dispositivo (come i file di registro o le lavagne) salvati sul dispositivo verranno eliminati. Non è disponibile alcuna opzione per mantenere un backup per la configurazione e i file del dispositivo e riutilizzarlo una volta che il dispositivo è registrato di nuovo nel cloud.

---

Ulteriori dettagli sul ripristino di fabbrica sono forniti nell'articolo: [Factory-Reset-|-Secure-Data-Wipe](#) .



Avviso: se si decide di eseguire un reset di fabbrica, è necessario configurare e registrare nuovamente il dispositivo nel cloud dall'inizio. Prima di registrare il dispositivo nel cloud, eliminare il workspace precedente dall'elenco dei workspace nell'organizzazione dell'hub di controllo e ricrearlo se si intende utilizzare lo stesso workspace utilizzato in precedenza. Non è possibile aggiungere nuovamente lo stesso endpoint all'area di lavoro esistente. In Workspace l'endpoint viene visualizzato come non in linea, ma viene comunque considerato registrato. L'aggiunta di un secondo endpoint a un oggetto Workspace non è supportata al momento della scrittura di questo articolo.

---

Una volta avviato il dispositivo dopo il reset di fabbrica e dopo aver verificato la connettività alla rete, è possibile usare l'indirizzo IP del dispositivo per accedere alla GUI del dispositivo usando le credenziali predefinite: username is admin and password is blank. Creare quindi altri utenti sull'endpoint e procedere con la registrazione del dispositivo nell'area di lavoro appena creata nell'organizzazione Control Hub. Accertarsi di deselezionare questa opzione quando viene visualizzata la finestra di registrazione:



## Register to Webex

Enter your 16 digits Webex activation code or get a code from [settings.webex.com](https://settings.webex.com).

XXXX-XXXX-XXXX-XXXX

Register

Disable local users and integrations ⓘ



After a successful registration, any existing user accounts on the device will be disabled and logged out. Macros will be removed. Users and macros can be enabled again via [Cisco Webex Control Hub](#).

Registriati alla schermata popup di Webex dall'interfaccia utente dell'endpoint

---



---

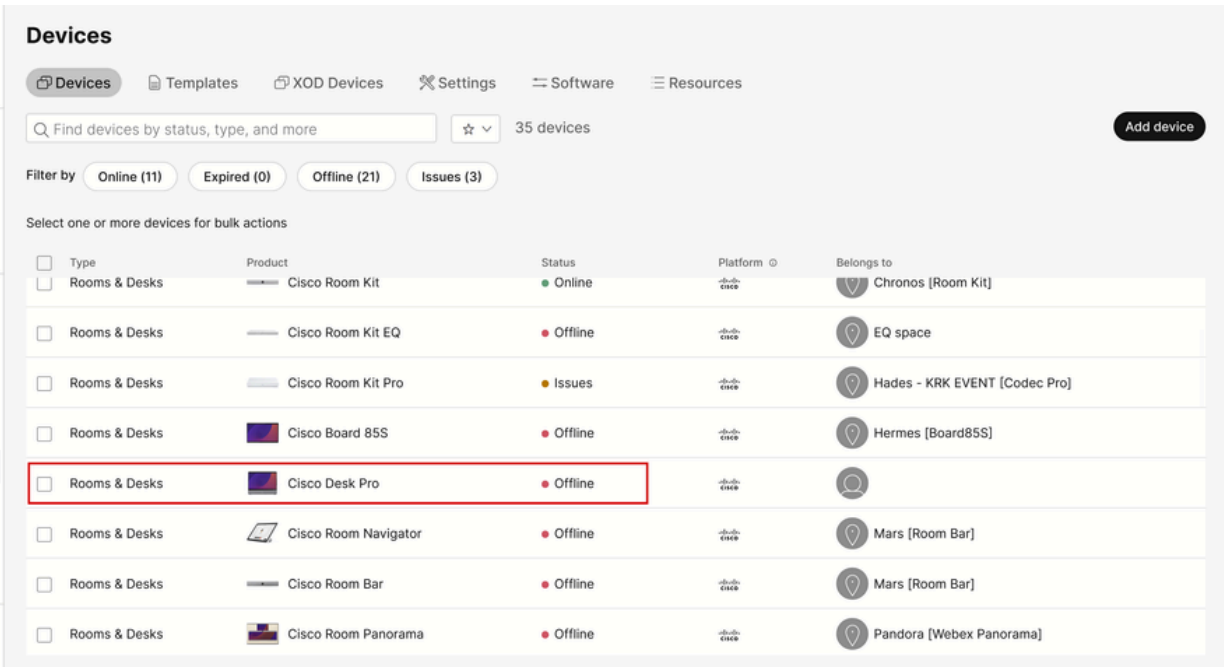


Nota: per accedere alla GUI dell'endpoint, è necessario immettere l'indirizzo IP dell'endpoint in un browser Web e utilizzare le credenziali di un amministratore per eseguire il login. Il nome utente predefinito è admin e la password predefinita è vuota, ma solo per un endpoint appena ricevuto o reimpostato in fabbrica. È necessario essere sulla stessa rete/VLAN dell'endpoint a cui si sta tentando di accedere, altrimenti non sarà possibile utilizzare la GUI del dispositivo.

Una volta registrato il dispositivo nel cloud, è possibile accedere alla GUI sia tramite Control Hub sia utilizzando l'indirizzo IP dell'endpoint sul browser e accedendo con uno degli account utente creati o con l'account utente predefinito.

## Contattare TAC per configurare manualmente un account amministratore sull'endpoint

Se non si desidera perdere la configurazione già esistente sull'endpoint, invece di eseguire un ripristino della fabbrica, aprire un ticket con TAC e descrivere il problema. Il tecnico TAC chiederà di accedere all'organizzazione dell'hub di controllo, passare alla scheda Dispositivi nella sezione Gestione, quindi selezionare l'endpoint a cui non è più possibile accedere:



The screenshot shows the 'Devices' section of the Cisco Control Hub interface. The left sidebar contains navigation options like Overview, Alerts center, MONITORING (Analytics, Troubleshooting, Reports), MANAGEMENT (Users, Groups, Locations, Workspaces, **Devices**, Apps, Account, Organization Settings), and SERVICES. The main content area displays a table of devices with the following columns: Type, Product, Status, Platform, and Belongs to. The table lists several devices, with the 'Cisco Desk Pro' device highlighted by a red box. This device is currently 'Offline'. Other devices include Cisco Room Kit, Cisco Room Kit EQ, Cisco Room Kit Pro, Cisco Board 85S, Cisco Room Navigator, Cisco Room Bar, and Cisco Room Panorama.

Type	Product	Status	Platform	Belongs to
Rooms & Desks	Cisco Room Kit	Online	cisco	Chronos [Room Kit]
Rooms & Desks	Cisco Room Kit EQ	Offline	cisco	EQ space
Rooms & Desks	Cisco Room Kit Pro	Issues	cisco	Hades - KRK EVENT [Codec Pro]
Rooms & Desks	Cisco Board 85S	Offline	cisco	Hermes [Board85S]
Rooms & Desks	Cisco Desk Pro	Offline	cisco	
Rooms & Desks	Cisco Room Navigator	Offline	cisco	Mars [Room Bar]
Rooms & Desks	Cisco Room Bar	Offline	cisco	Mars [Room Bar]
Rooms & Desks	Cisco Room Panorama	Offline	cisco	Pandora [Webex Panorama]

Sezione Dispositivi in Control Hub

Passare quindi alla sezione Supporto e fare clic su Chiave di accesso remoto. Viene visualizzata una finestra che contiene una chiave lunga simile a quella visualizzata nell'immagine (la chiave è stata reimpostata sul dispositivo di prova e non è più valida) di seguito:

## Remote Access Key

Share this key with Cisco Support by pasting it in a message.

Doing so will give Cisco Support full access to your device. Use 'Reset Key' to create a new Remote Support Access Key and invalidate any previous key you may have shared with Cisco Support.

```
KRTWuCIBBtMeTtN6wvOJhCnAly/q/mtQs5ogJvl5Y8xd7EoMdiY8TOATAew3cEwCwyvxBHX2id2XjsZhk29KUDu+1NvCH52h7uMc
```

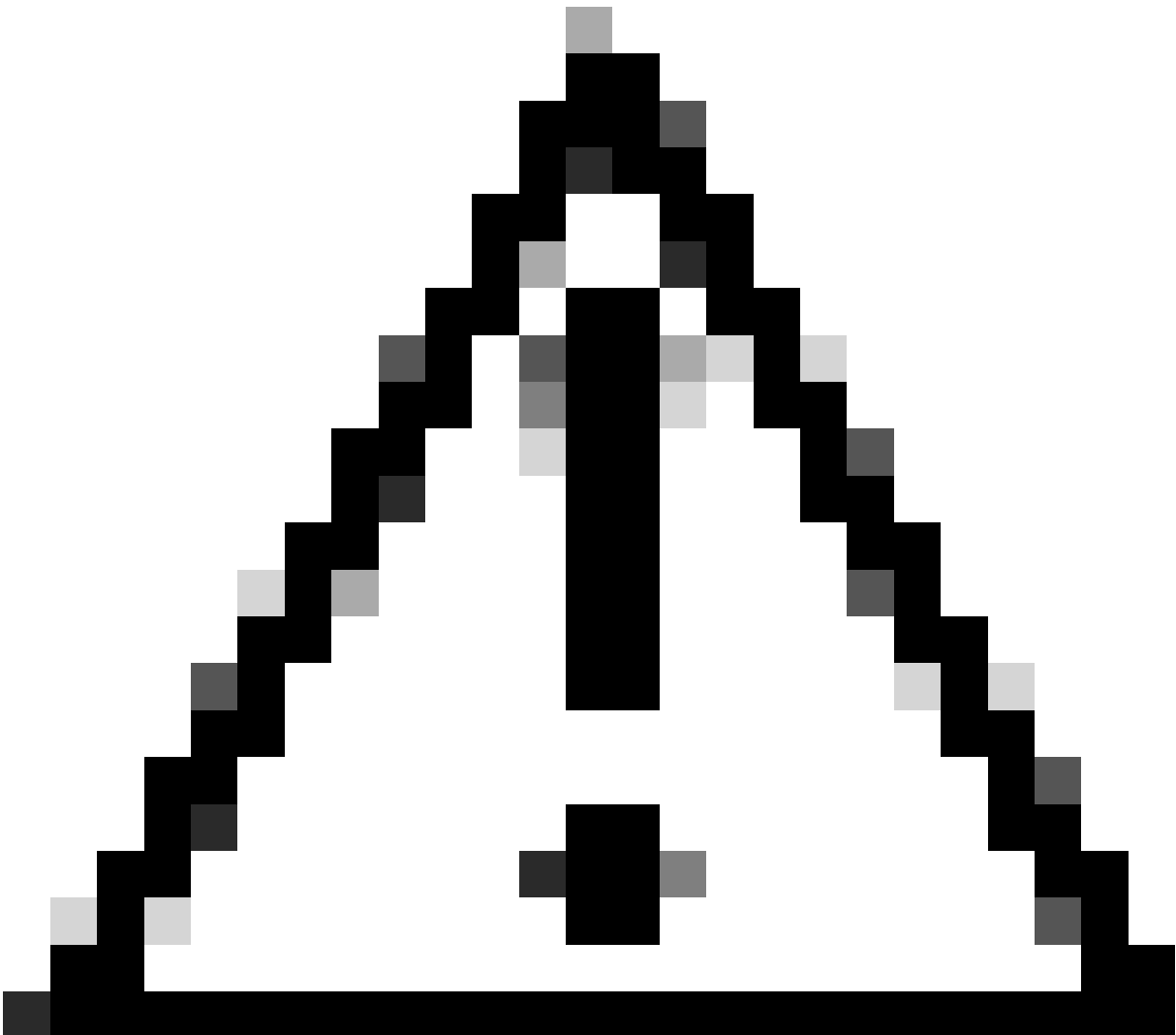
 Copy to Clipboard

 Reset Key

Done

Popup Chiave di accesso remoto in Control Hub

Copiare questa chiave e condividerla con il tecnico TAC assegnato alla richiesta. Il tecnico utilizzerà questa chiave per generare una password univoca che potrà essere utilizzata insieme all'account utente del supporto remoto (già esistente nel dispositivo per impostazione predefinita) per facilitare la creazione di un nuovo account amministratore.



---

Attenzione: non richiedere al tecnico TAC di fornire la password generata dalla chiave di accesso remoto. La condivisione della password non è consentita.

---

A questo punto, contattare il tecnico TAC per creare l'account insieme in una riunione. Verificare che l'endpoint disponga di connettività di rete e che sia possibile eseguire il protocollo SSH su di esso. Nell'applicazione SSH in uso, il tecnico TAC controlla lo schermo in modalità remota e immette il nome utente, il supporto remoto e la password generati dalla chiave di accesso remoto fornita. Il tecnico crea quindi il nuovo account admin sul dispositivo utilizzando una speciale shell dei comandi sull'endpoint.

---



Avviso: non intervenire con l'app SSH durante la creazione dell'account utente da parte del tecnico e non revocare il controllo dello schermo al tecnico TAC. Questa shell è utilizzata esclusivamente da TAC. Si rischia di essere ammessi a un'autorizzazione al reso (RMA) se si eseguono personalmente comandi che potrebbero danneggiare il dispositivo durante questa procedura.

---

Dopo la creazione del nuovo account admin, utilizzarlo per accedere alla GUI del dispositivo nel browser utilizzando l'indirizzo IP dell'endpoint. Se necessario, è possibile creare più account utente dalla GUI.

## Password utente del supporto remoto non accettata

È possibile che quando i tecnici TAC provano a digitare la password sull'app SSH per accedere alla console dell'endpoint, venga visualizzato un errore di password non valida. La password è stata probabilmente digitata correttamente dal tecnico ma non è stata accettata. Questo accade di solito perché sul computer locale non è stata cambiata la lingua in inglese. Poiché si utilizza una lingua diversa, la password digitata dal tecnico che ha il controllo del PC non è in inglese. Per questo motivo, non è possibile accedere alla console. Prima di avviare la risoluzione dei problemi, verificare che la lingua locale del PC sia impostata in inglese.

Inoltre, i caratteri come la barra rovesciata (\) o la barra (/) possono essere mappati in modo diverso sulla tastiera. Ciò significa, ad esempio, che l'ingegnere digita una barra rovesciata (\), mentre in realtà viene digitata una barra (/). Se la lingua locale è impostata su Inglese e la password non funziona ancora, generare una nuova chiave di accesso remoto da Control Hub e condividerla con il tecnico. Il tecnico genera una nuova password e verifica se esistono caratteri speciali. È quindi possibile tentare un nuovo accesso con la nuova password.

```
login as: remotesupport
Keyboard-interactive authentication prompts from server:
Password:
End of keyboard-interactive prompts from server
Access denied
Keyboard-interactive authentication prompts from server:
Password:
End of keyboard-interactive prompts from server
Access denied
```

Prompt SSH accesso negato



Avviso: in alcuni casi il carattere y è mappato al carattere z e viceversa su alcune tastiere. Per non avere dubbi sulla password digitata, il tecnico può provare a digitare questa stringa nella barra di ricerca del browser o in un'applicazione per la creazione di note:

```
abcdefghijklmnopqrstuvwxyz1234567890!@#$%^&*()-_+=:;'"<,>./?
```

Non da copiare ma da digitare. Se i caratteri vengono visualizzati in un ordine diverso da quello in cui sono stati digitati, significa che non corrispondono.

Inoltre, i computer con tastiere non QWERTY possono avere risultati simili. Assicurarsi di informare il tecnico della configurazione in tali scenari.

---

## Informazioni correlate

[Ripristino in fabbrica/Eliminazione sicura dei dati](#)

[Attivazione degli account utente sui dispositivi registrati nel cloud](#)

## 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).