

Cloud-Registered Endpoint GUI herstellen wanneer offline in Control Hub

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Nadere beschrijving van het scenario](#)

[Fabrieksinstellingen Het apparaat opnieuw instellen](#)

[Neem contact op met TAC om handmatig een admin-account op uw endpoint te configureren](#)

[Gebruikerswachtwoord voor externe ondersteuning niet geaccepteerd](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft het herstel van een endpointaccount wanneer lokale accounts uitgeschakeld zijn nadat de cloud is geregistreerd en het endpoint offline is in Control Hub.

Voorwaarden

Vereisten

Aanbevolen wordt dat u enigszins vertrouwd bent met de volgende onderwerpen:

- Control Hub-platform
- Endpoint Registratie en beheer via de grafische gebruikersinterface (GUI) van het eindpunt.

Gebruikte componenten

Deze apparatuur is gebruikt om de tests uit te voeren en de in dit document beschreven resultaten te produceren:

- Room Kit-endpoint
- Desktop Pro-endpoint

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Nadere beschrijving van het scenario

Bij het registreren van een apparaat in de cloud wordt u gevraagd om te beslissen of u uw lokale gebruikersaccounts op het apparaat zelf actief wilt houden. De standaardinstelling is dat de lokale gebruikersaccounts worden verwijderd.

Dit document beschrijft hoe u de admin-account van uw endpoint kunt herstellen wanneer u de lokale accounts op het apparaat hebt uitgeschakeld na cloudregistratie en uw endpoint offline is in Control Hub.

×

Register to Webex

Enter your 16 digits Webex activation code or get a code from settings.webex.com.

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](#).

Registreren in Webex pop-up vanaf endpoint GUI

Dit betekent dat u niet in staat bent om toegang te krijgen tot de grafische gebruikersinterface of GUI van het apparaat via uw browser door gebruik te maken van het IP-adres van het apparaat. U hebt alleen via het Control Hub-platform toegang tot de GUI van het apparaat door te navigeren naar Apparaten onder de sectie Management in uw Control Hub. Kies vervolgens een van de online apparaten om in te loggen op de GUI en klik op Local Device Control in het gedeelte Support:

Support

Device Logs ⓘ	Manage >
Local Device Controls ⓘ	Launch ↗
Cisco Support ⓘ	Remote Access Key >

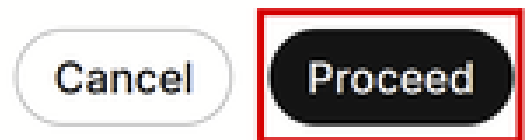
Er wordt een nieuw venster geopend. Selecteer Doorgaan om de GUI van het apparaat te openen:

Launch Local Device Controls

x

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.



pop-upvenster Local Device Controls in Control Hub

Vervolgens wordt de GUI voor het eindpunt geopend in uw browser. Van daaruit kunt u een nieuwe gebruiker aanmaken en deze gebruiker gebruiken om in te loggen op uw apparaat GUI door het eigen IP-adres van het apparaat te gebruiken in uw browser. De hele procedure wordt in detail beschreven in deze video: [Gebruikersaccounts activeren op cloudgeregistreerde apparaten](#)



Opmerking: u moet in hetzelfde netwerk als het eindpunt staan, anders hebt u geen toegang tot de GUI. Als u niet bent, ziet u deze pagina in uw browser nadat u op Doorgaan hebt geklikt:

The connection has timed out

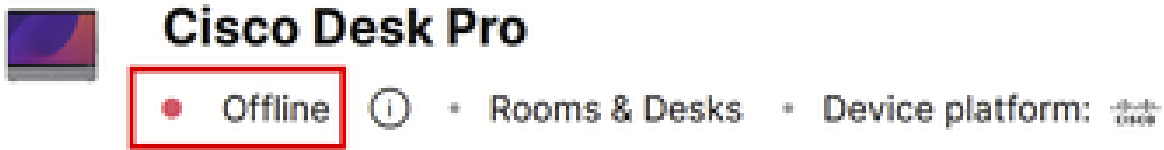
An error occurred during a connection to [redacted]

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

Try Again

Bericht over time-out verbinding met browser

Een probleem ontstaat wanneer uw eindpunt offline wordt weergegeven in Control Hub (hier getoond):



Endpoint offline status in controlehub

In dit scenario hebt u geen toegang tot de GUI van het eindpunt via Control Hub. De lokale apparaatbesturing die eerder in dit artikel is beschreven, gaat niet werken omdat het apparaat in de praktijk via HTTP toegang heeft tot de GUI van het apparaat en het apparaat online moet zijn. Als u ervoor hebt gekozen om lokale gebruikersaccounts uit te schakelen tijdens de registratie van het apparaat, hetzij opzettelijk of per ongeluk, dan bent u ook niet in staat om toegang te krijgen tot de GUI van het apparaat door gebruik van zijn IP-adres in uw browser. In dit stadium hebt u de toegang tot de GUI van uw apparaat verloren. Tenzij u het apparaat weer online kunt brengen met een aantal fundamentele probleemoplossing door fysiek toegang te krijgen tot het apparaat, bent u uitgesloten van het.

Er zijn twee voorgestelde actieplannen te kiezen om uit deze situatie te komen:

- Fabrieksinstellingen Stel het apparaat opnieuw in.
- Contact opnemen met TAC na het verkrijgen van een Remote Access Key.

Fabrieksinstellingen Het apparaat opnieuw instellen

In dit specifieke scenario kan het apparaat in de fabriek worden hersteld door het apparaat fysiek te openen. Er zijn twee mogelijke opties:

- Ga vanuit het aanraakpaneel dat is aangesloten op het eindpunt (Navigator of Touch 10 randapparaat) naar instellingen en selecteer de optie Factory Reset. Voor Board-apparaten die geen aanraakpaneel hebben aangesloten op hen, heeft het aanraakscherm van het eindpunt de Settings Button rechtsboven in het scherm.
- De eindpunten hebben een speldengat op de rug of de bodem van het apparaat. Afhankelijk van het apparaat kan het speldengat bedekt zijn met een plastic dop. U kunt een veiligheidsspeld of paperclip gebruiken, deze in het speldengat steken en 10 tot 15 seconden indrukken. Vervolgens wordt de fabriek opnieuw ingesteld.



Opmerking: wanneer de fabrieksreset wordt gebruikt, worden alle apparaatconfiguraties en bestanden (zoals logbestanden of whiteboards) die op het apparaat zijn opgeslagen, verwijderd. Er is geen optie om een back-up te bewaren voor de apparaatconfiguratie en bestanden en deze opnieuw te gebruiken zodra het apparaat opnieuw is geregistreerd in de cloud.

Een aantal extra details over de fabrieksreset zijn te vinden in het artikel: [Factory-Reset-|-Secure-Data-Wipe](#) .



Waarschuwing: u moet het apparaat opnieuw instellen en registreren in de cloud vanaf het begin als u besluit om een fabrieksreset uit te voeren. Voordat u het apparaat naar de cloud registreert, verwijdert u de vorige werkruimte uit de lijst met werkruimtes in uw Control Hub-organisatie en voegt u deze opnieuw toe als u dezelfde werkruimte wilt gebruiken als voorheen. U kunt niet hetzelfde eindpunt opnieuw toevoegen aan de reeds bestaande werkruimte. De werkruimte ziet het eindpunt als offline, maar beschouwt het nog steeds als geregistreerd. Het toevoegen van een tweede eindpunt aan een werkruimte wordt niet ondersteund tijdens het schrijven van dit artikel.

Zodra het apparaat opstart na fabrieksreset en u controleert of u verbinding hebt met het netwerk, kunt u het apparaat IP gebruiken om in te loggen op het apparaat GUI met behulp van de standaardreferenties: gebruikersnaam is beheerder en wachtwoord is leeg. Maak vervolgens extra gebruikers op dit eindpunt en ga verder met het registreren van het apparaat naar de nieuwe werkruimte in uw Control Hub-organisatie. Schakel deze optie uit zodra het registratievenster wordt weergegeven:



Register to Webex

Enter your 16 digits Webex activation code or get a code from 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](#).

Registreren in Webex pop-up vanaf endpoint GUI

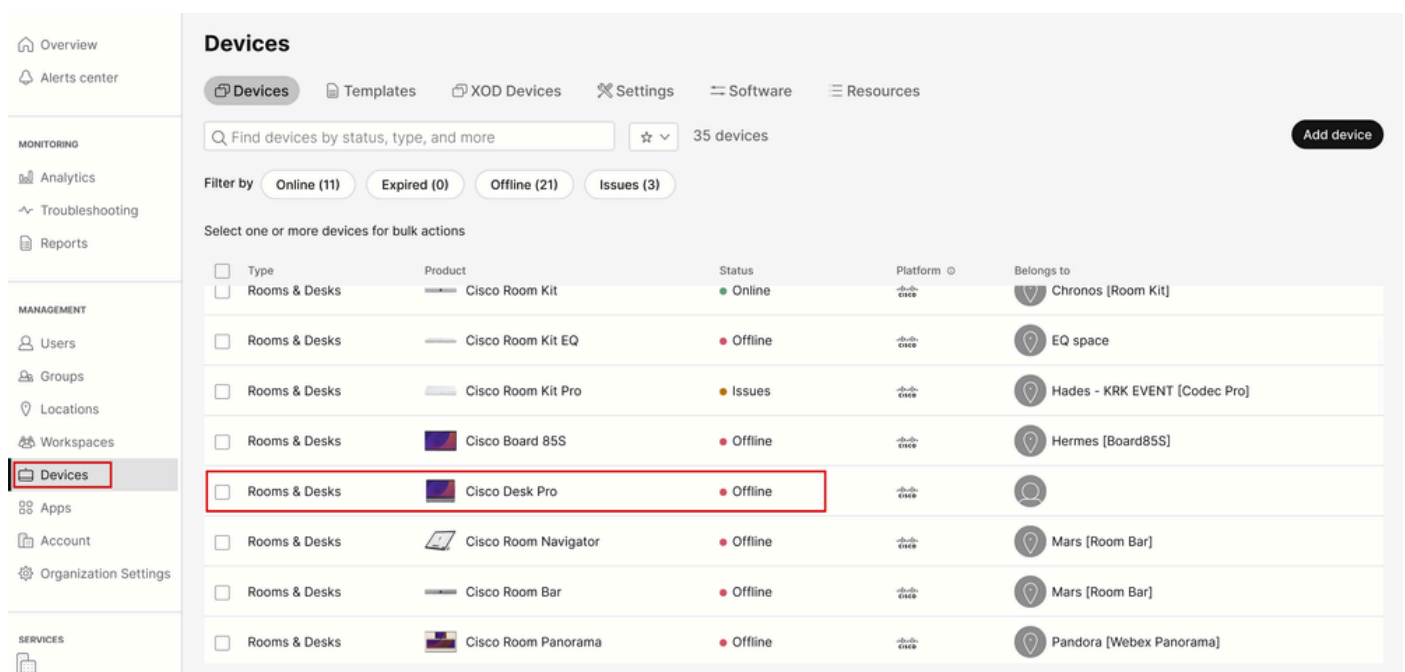


Opmerking: om toegang te krijgen tot de GUI van het eindpunt, moet u het IP-adres van het eindpunt invoeren in een webbrowser en de aanmeldingsgegevens van een beheerder gebruiken om in te loggen. De standaardgebruikersnaam is admin en het standaardwachtwoord is leeg, maar alleen voor een eindpunt dat u zojuist hebt ontvangen of dat u fabrieksinstellingen hebt hersteld. U moet op hetzelfde netwerk\VLAN staan als het eindpunt waartoe u toegang probeert te krijgen, of u kunt de GUI van het apparaat niet gebruiken.

Zodra het apparaat is geregistreerd in de cloud, kunt u de GUI benaderen via Control Hub en door het IP-adres van het eindpunt in uw browser te gebruiken en in te loggen met een van uw gemaakte gebruikersaccounts of de standaardgebruikersaccount.

Neem contact op met TAC om handmatig een admin-account op uw endpoint te configureren

Als u de configuratie niet wilt verliezen die al bestaat op uw eindpunt, in plaats van het uitvoeren van een fabrieksreset, open een ticket met TAC en beschrijf uw probleem. De TAC engineer gaat u vervolgens vragen om in te loggen bij uw Control Hub Organisation, te navigeren naar het tabblad Apparaten onder de sectie Management en vervolgens het eindpunt te selecteren dat u niet meer kunt gebruiken:



The screenshot displays the 'Devices' management interface in Control Hub. The left sidebar contains navigation options: Overview, Alerts center, MONITORING (Analytics, Troubleshooting, Reports), MANAGEMENT (Users, Groups, Locations, Workspaces, **Devices**, Apps, Account, Organization Settings), and SERVICES. The main content area shows a list of 35 devices, filtered by status: Online (11), Expired (0), Offline (21), and Issues (3). The table below lists several devices, with the 'Cisco Desk Pro' device highlighted by a red box.

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]

Sectie Apparaten in Control Hub

Navigeer vervolgens naar het gedeelte Ondersteuning en klik op Remote Access Key. Er verschijnt een venster met een lange toets die eruitziet zoals deze in het beeld (deze toets is gereset op het testapparaat en is niet meer geldig) hieronder:



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/mtQs5ogJvI5Y8xd7EoMdiY8TOATAew3cEwCwyvxBHX2id2XjsZhk29KUDu+1NvCH52h7uMc

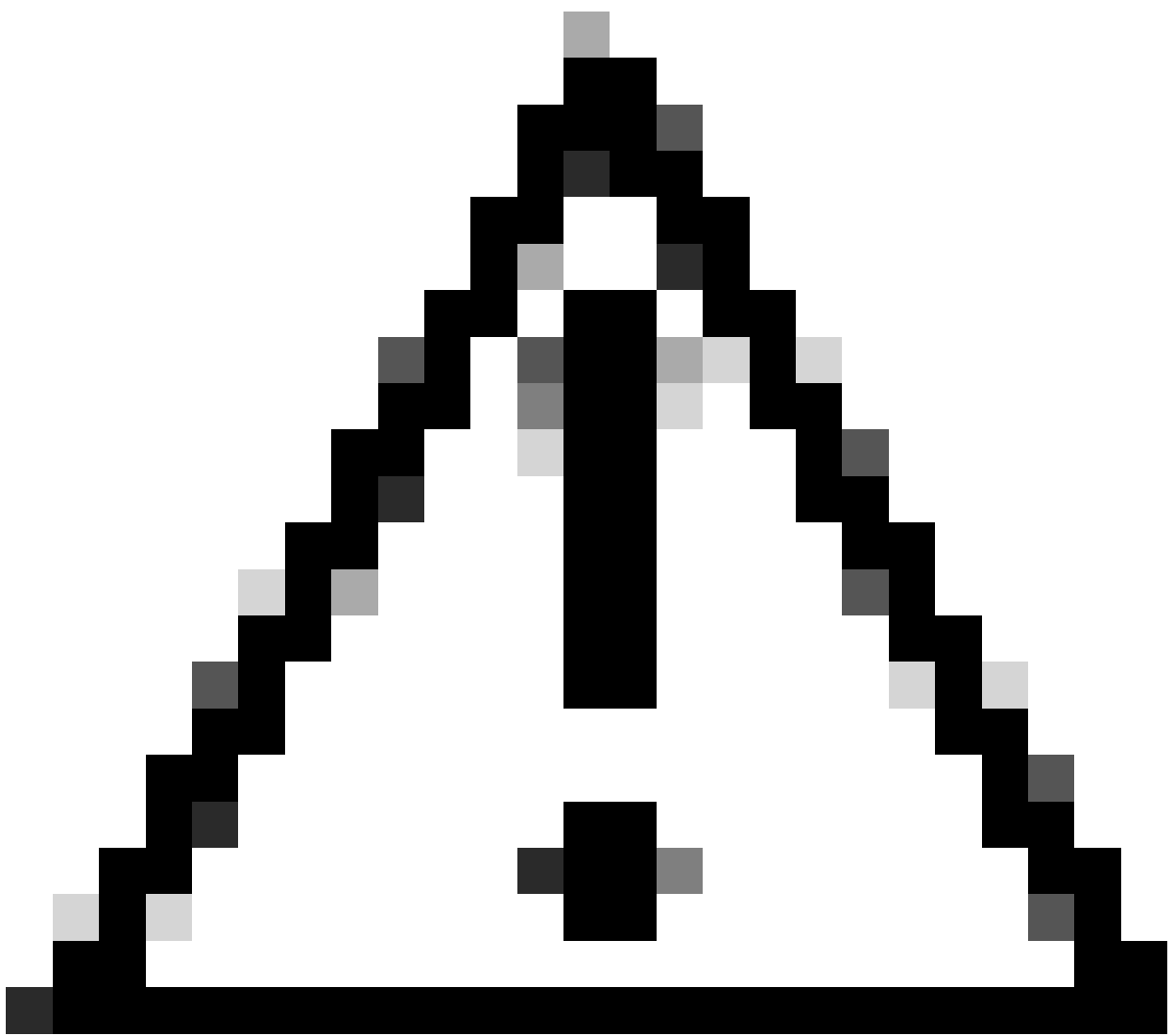
Copy to Clipboard

Reset Key

Done

Remote Access Key, pop-up in Control Hub

Kopieer deze sleutel en deel hem met de TAC Engineer die is toegewezen aan uw case. De engineer gaat deze sleutel gebruiken om een uniek wachtwoord te genereren dat gebruikt kan worden samen met de remote support user account (die standaard al bestaat op het apparaat) om u te helpen een nieuwe admin account aan te maken.



Waarschuwing: vraag de TAC engineer niet om u het wachtwoord te geven dat door de afstandsbediening is gegenereerd. Het delen van het wachtwoord is niet toegestaan.

In dit stadium, contacteer de TAC ingenieur om de rekening in een vergadering samen tot stand te brengen. Controleer dat het eindpunt netwerkconnectiviteit heeft en u kunt SSH aan het. In de SSH-applicatie die u gebruikt, neemt de TAC engineer vervolgens de controle over uw scherm op afstand en voert de gebruikersnaam op afstand ondersteuning in en het wachtwoord dat gegenereerd wordt door de toets voor externe toegang die u hebt opgegeven. Vervolgens creëert de engineer de nieuwe admin-account op het apparaat met behulp van een speciale opdrachtshell op het eindpunt.



Waarschuwing: intervenieer niet met de SSH-app terwijl de engineer de gebruikersaccount aanmaakt en trek de schermbesturing niet in van de TAC engineer. Deze schelp wordt strikt gebruikt door TAC. U loopt het risico om in aanmerking te komen voor een RMA als u zelf opdrachten uitvoert die mogelijk schade aan het apparaat kunnen veroorzaken tijdens deze procedure.

Na het aanmaken van de nieuwe admin-account, gebruik deze om in te loggen op de GUI van het apparaat in uw browser met behulp van het IP-adres van het eindpunt. U kunt indien nodig meer gebruikersaccounts maken vanuit de GUI.

Gebruikerswachtwoord voor externe ondersteuning niet geaccepteerd

Er is een kans dat wanneer de TAC engineers proberen om het wachtwoord in de SSH-app te typen om in te loggen op de endpointconsole, u een Ongeldige fout Wachtwoord ziet. Het wachtwoord is waarschijnlijk door de engineer correct getypt, maar is niet geaccepteerd. Dit gebeurt meestal omdat je op je lokale machine de taal niet hebt veranderd in het Engels. U hebt een andere taal gebruikt en het wachtwoord dat is ingevoerd door de engineer die de controle heeft over uw PC, is niet in het Engels. Hierdoor kunt u niet inloggen op de console. Zorg ervoor dat de lokale taal op uw pc in het Engels is ingesteld voordat de probleemoplossing wordt gestart.

Daarnaast kunnen tekens zoals de backslash (\) of de voorwaartse slash (/) mogelijk op een andere manier op het toetsenbord worden toegewezen. Dit betekent bijvoorbeeld dat de engineer een backslash (\) typt, maar in werkelijkheid wordt een forward slash (/) getypt. Als de lokale taal is ingesteld op Engels en het wachtwoord nog steeds niet lijkt te werken, genereert u een nieuwe externe toegangssleutel vanuit Control Hub en deelt u deze met de engineer. De engineer genereert een nieuw wachtwoord en controleert of er speciale tekens bestaan. Een nieuwe login kan dan met het nieuwe wachtwoord worden geprobeerd.

```
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 voor geweigerde SSH-toegang



Waarschuwing: er zijn gevallen waarin het teken y aan het teken z is toegewezen en vice versa op sommige toetsenborden. Om geen twijfel over het getypte wachtwoord te hebben, kan de ingenieur proberen typend dit koord in uw browser zoekbalk of een nota toepassing:

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

Dit hoeft niet te worden gekopieerd, maar moet worden getypt. Als tekens in een andere volgorde verschijnen dan de volgorde waarin ze zijn getypt, is er een tekenfout op het toetsenbord.

Bovendien kunnen machines met toetsenborden zonder QWERTY vergelijkbare resultaten hebben. Zorg ervoor dat u de engineer in dergelijke scenario's op de hoogte stelt van uw setup.

Gerelateerde informatie

[Fabrieksinstellingen opnieuw instellen/beveiligde gegevenswissing](#)

[Gebruikersaccounts activeren op cloudgeregistreerde apparaten](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.