

Recupere la GUI del terminal registrado en la nube cuando esté fuera de línea en Control Hub

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Descripción detallada de la situación](#)

[Reinicio de fábrica del dispositivo](#)

[Póngase en contacto con el TAC para configurar manualmente una cuenta de administrador en su terminal](#)

[Contraseña de usuario de soporte remoto no aceptada](#)

[Información Relacionada](#)

Introducción

Este documento describe la recuperación de la cuenta de terminal cuando las cuentas locales están inhabilitadas después del registro en la nube y el terminal está fuera de línea en el Centro de control.

Prerequisites

Requirements

Se recomienda que esté familiarizado con estos temas:

- Plataforma del centro de control
- Registro y administración de terminales mediante la interfaz gráfica de usuario (GUI) del terminal.

Componentes Utilizados

Este equipo se ha utilizado para realizar las pruebas y producir los resultados descritos en este documento:

- Punto final del kit de salas
- Terminal Desk Pro

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo,

asegúrese de entender el posible impacto de cualquier comando.

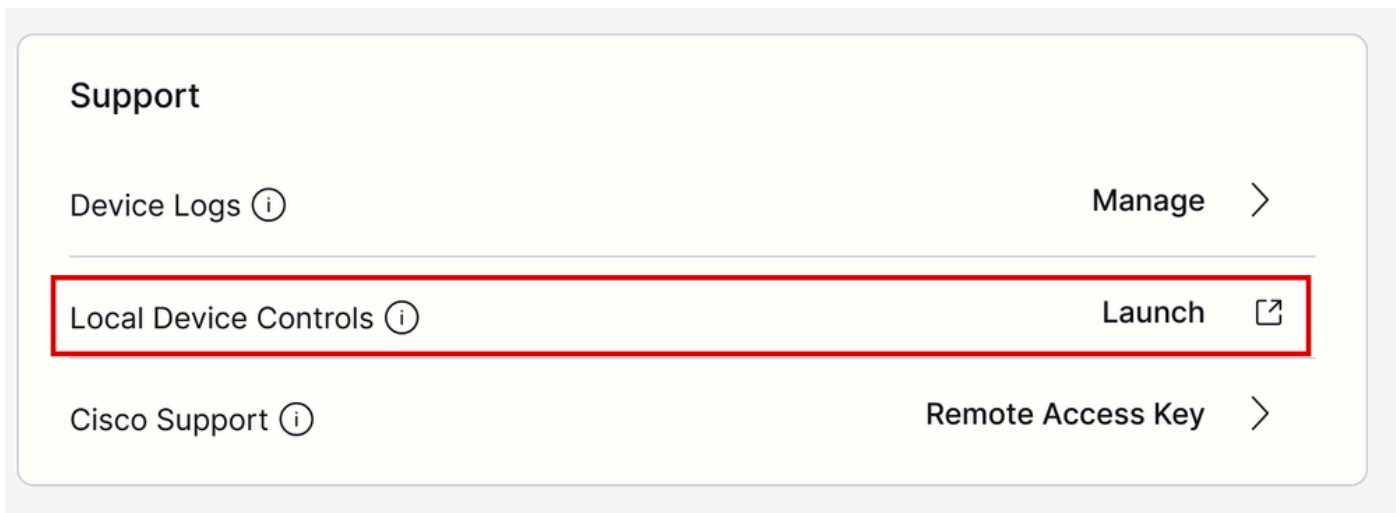
Descripción detallada de la situación

Al registrar un dispositivo en la nube, se le solicita que decida si desea mantener activas las cuentas de usuario local del propio dispositivo. De forma predeterminada, se eliminan las cuentas de usuario locales.

Este documento describe cómo recuperar la cuenta de administrador de su terminal cuando ha deshabilitado las cuentas locales en el dispositivo después del registro en la nube y su terminal está fuera de línea en el concentrador de control.

Registro en la ventana emergente de Webex desde la GUI del terminal

Esto significa que no puede acceder a la interfaz gráfica de usuario o GUI del dispositivo a través de su navegador mediante la dirección IP del dispositivo. Solo puede acceder a la GUI del dispositivo a través de la plataforma del centro de control. Para ello, vaya a Dispositivos en la sección Gestión del centro de control. A continuación, elija uno de los dispositivos en línea para iniciar sesión en su GUI y haga clic en Control de dispositivo local en la sección Soporte:



Control de dispositivos local en el Concentrador de control

A new window opens. Seleccione Proceed para abrir la GUI del dispositivo:

Launch Local Device Controls

x

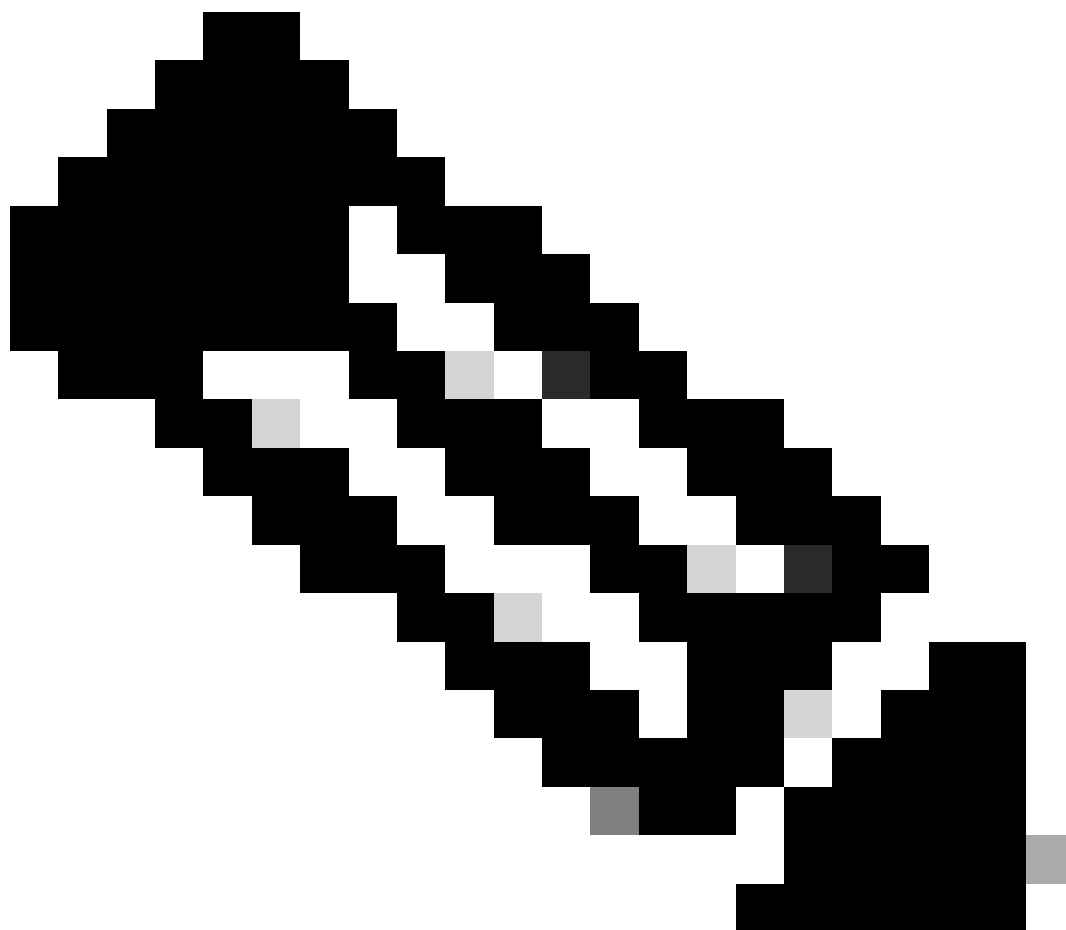
This will open Local Device Controls in a new tab.

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

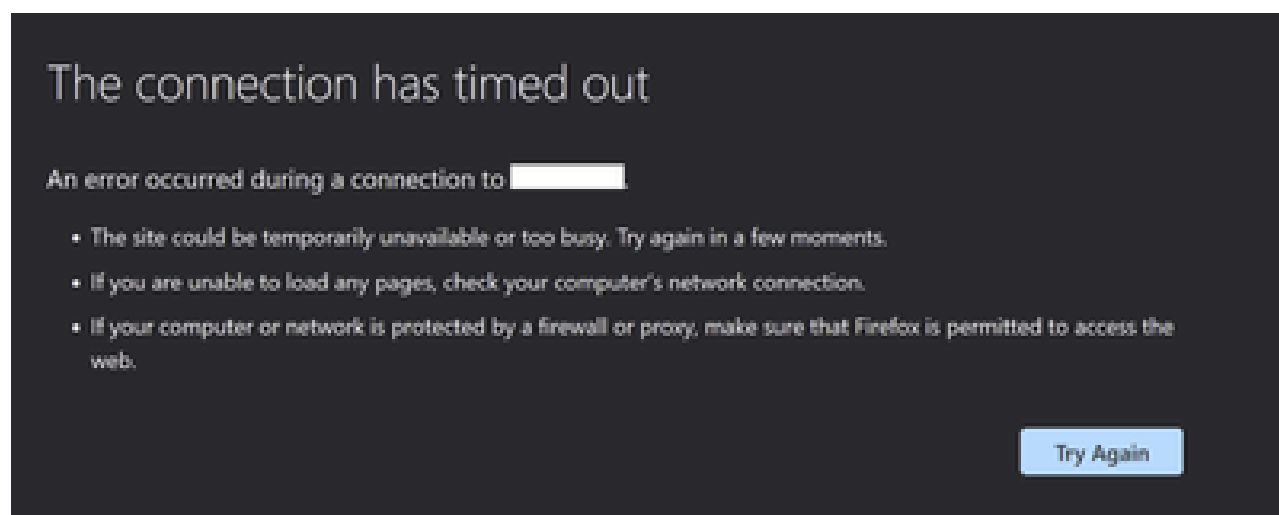


Ventana emergente Controles de dispositivo local en el concentrador de control

A continuación, la GUI del terminal se abre en el navegador. A partir de ahí, puede crear un nuevo usuario y utilizarlo para iniciar sesión en la GUI de su dispositivo mediante la dirección IP propia del dispositivo en su navegador. El procedimiento completo en detalle se describe en este video:

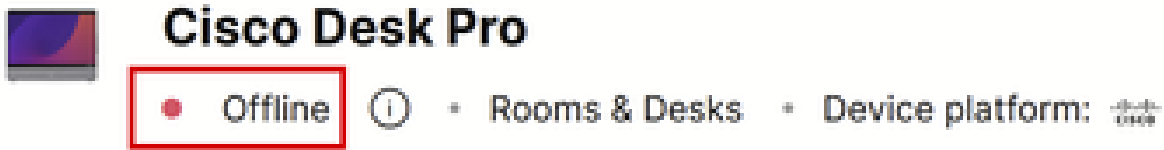


Nota: Debe estar en la misma red que el terminal; de lo contrario, no podrá acceder a la GUI. Si no lo está, verá esta página en el explorador después de hacer clic en Proceed :



Mensaje de conexión de tiempo de espera del explorador

Se produce un problema cuando el terminal se muestra como desconectado en el concentrador de control (mostrado aquí):



Estado desconectado del terminal en el concentrador de control

En esta situación, no puede acceder a la GUI del terminal desde el concentrador de control. El Control de dispositivo local descrito anteriormente en este artículo no va a funcionar ya que prácticamente está accediendo a la GUI del dispositivo a través de HTTP y requiere que el dispositivo esté en línea. Si ha optado por desactivar las cuentas de usuario locales durante el registro del dispositivo, ya sea de forma deliberada o accidental, tampoco podrá acceder a la GUI del dispositivo mediante su dirección IP en el navegador. En esta etapa, ha perdido el acceso a la GUI del dispositivo. A menos que pueda volver a conectar el dispositivo con algún procedimiento básico de solución de problemas accediendo físicamente al dispositivo, no podrá acceder a él.

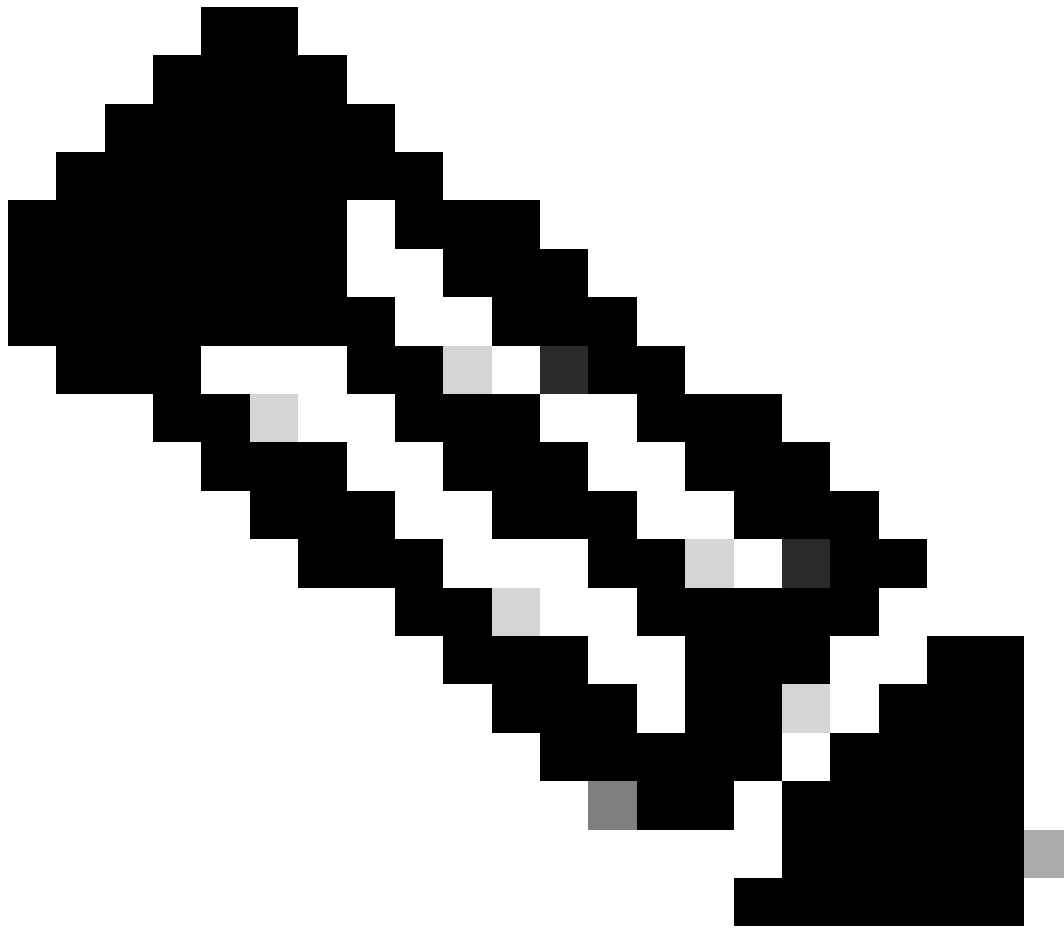
Hay dos planes de acción sugeridos para elegir con el fin de salir de esta situación:

- Reinicie el dispositivo de fábrica.
- Póngase en contacto con el TAC después de obtener una clave de acceso remoto.

Reinicio de fábrica del dispositivo

El restablecimiento de fábrica del dispositivo en esta situación específica se puede realizar accediendo físicamente al dispositivo. Hay dos opciones posibles:

- En el panel táctil conectado al terminal (navegador o dispositivo periférico Touch 10), desplácese hasta la configuración y seleccione la opción Factory Reset. En el caso de los dispositivos de placa que no tienen panel táctil conectado, la pantalla táctil del terminal tiene el botón Settings en la esquina superior derecha de la pantalla.
- Los terminales tienen un agujero en la parte posterior o inferior del dispositivo. El agujero de alfiler, dependiendo del dispositivo, podría estar cubierto con una tapa de plástico. Puede utilizar un pasador de seguridad o un clip de papel e insertarlo en el orificio y presionar durante 10-15 segundos. A continuación, se iniciará un restablecimiento de fábrica.



Nota: cuando se utilice el restablecimiento de fábrica, se eliminarán todas las configuraciones de dispositivos y todos los archivos (como archivos de registro o pizarras) guardados en el dispositivo. No existe la opción de realizar una copia de seguridad de la configuración y los archivos del dispositivo y reutilizarla una vez que el dispositivo se haya registrado de nuevo en la nube.

Algunos detalles adicionales sobre el restablecimiento de fábrica se proporcionan en el artículo: [Factory-Reset-|-Secure-Data-Wipe](#) .



Advertencia: debe volver a configurar y registrar el dispositivo en la nube desde el principio si decide restablecer los parámetros de fábrica. Antes de registrar el dispositivo en la nube, elimine su espacio de trabajo anterior de la lista de espacios de trabajo de la organización del centro de control y vuelva a crearlo si tiene pensado utilizar el mismo espacio de trabajo que antes. No puede volver a agregar el mismo terminal al espacio de trabajo existente. El espacio de trabajo ve el extremo como desconectado, pero sigue considerando que está registrado en él. En el momento de escribir este artículo no se admite agregar un segundo punto final a un área de trabajo.

Una vez que el dispositivo se inicia después del restablecimiento de fábrica y verifica que tiene conectividad a la red, puede utilizar la IP del dispositivo para iniciar sesión en la GUI del dispositivo con las credenciales predeterminadas: el nombre de usuario es admin y la contraseña está en blanco. A continuación, cree usuarios adicionales en este terminal y registre el dispositivo en el espacio de trabajo recién creado de la organización del centro de control. Asegúrese de desactivar esta opción cuando aparezca la ventana de registro:



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](#).

Registro en la ventana emergente de Webex desde la GUI del terminal



Nota: para acceder a la GUI del terminal, debe introducir la dirección IP del terminal en un navegador web y utilizar las credenciales de un administrador para iniciar sesión. El nombre de usuario predeterminado es admin y la contraseña predeterminada está en blanco, pero sólo para un terminal que acaba de recibir o que ha restablecido la configuración de fábrica. Debe encontrarse en la misma red/VLAN que el terminal al que intenta acceder o, de lo contrario, no podrá utilizar la GUI del dispositivo.

Una vez que el dispositivo esté registrado en la nube, puede acceder a la GUI a través del concentrador de control y mediante la dirección IP del terminal en el navegador e iniciando sesión con una de las cuentas de usuario creadas o con la cuenta de usuario predeterminada.

Póngase en contacto con el TAC para configurar manualmente una cuenta de administrador en su terminal

Si no desea perder la configuración que ya existe en su terminal, en lugar de realizar un restablecimiento de fábrica, abra un ticket con TAC y describa su problema. El ingeniero del TAC le pedirá que inicie sesión en la organización del centro de control, acceda a la ficha Devices en la sección Management y, a continuación, seleccione el terminal al que ha perdido el acceso:

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 is titled 'Devices' and shows a search bar, a filter for '35 devices', and a table of devices. The table has columns for Type, Product, Status, Platform, and Belongs to. The 'Cisco Desk Pro' device is highlighted with a red box, and its status is 'Offline'.

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]

Sección Dispositivos del concentrador de control


A continuación, vaya a la sección Support y haga clic en Remote Access Key. Aparece una ventana que contiene una clave larga que se parece a la que se ve en la imagen (esta clave se ha restablecido en el dispositivo de prueba y ya no es válida) a continuación:

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

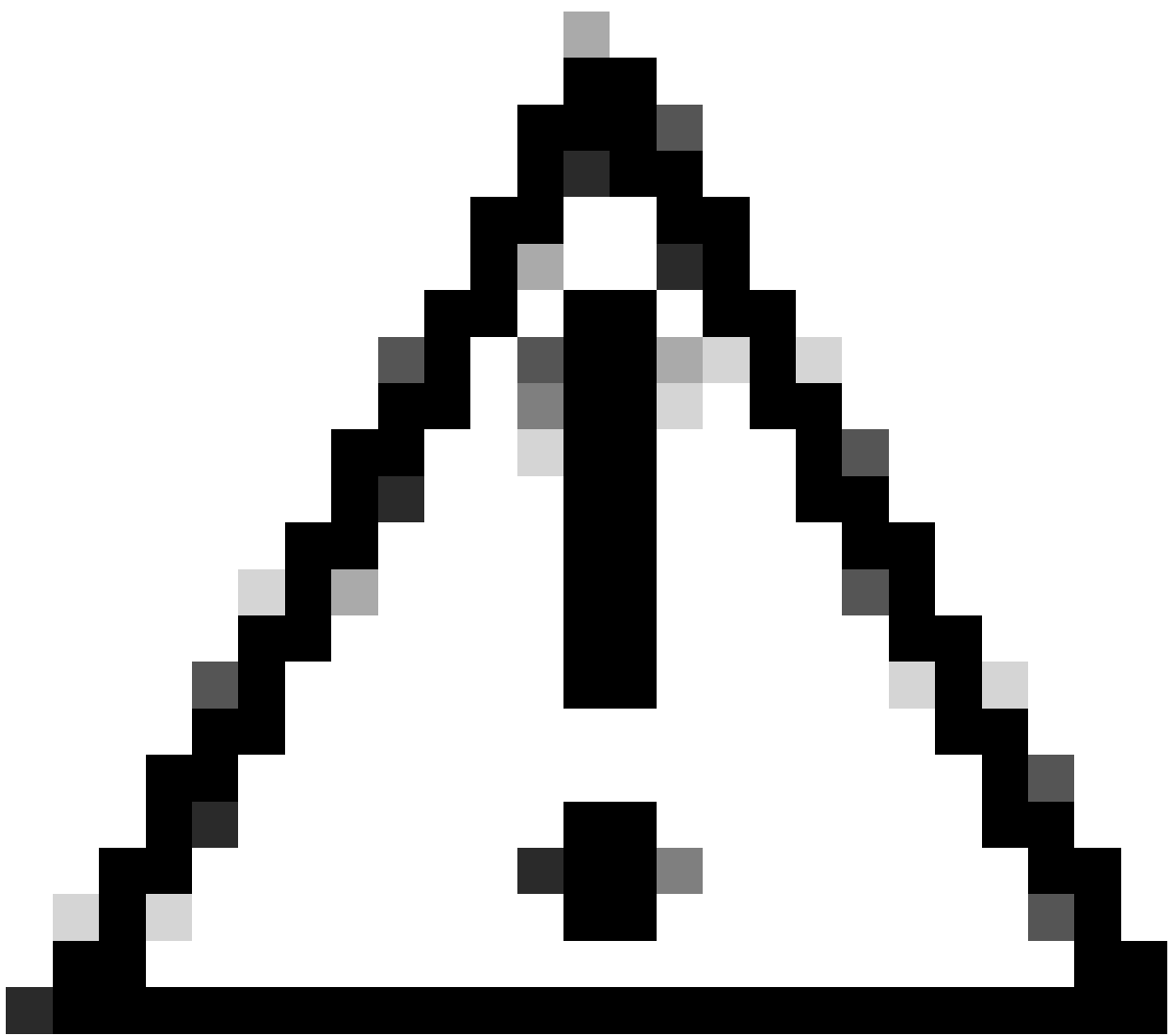
 Copy to Clipboard

 Reset Key

Done

Tecla de acceso remoto emergente en el concentrador de control

Copie esta clave y compártala con el ingeniero del TAC asignado a su caso. El ingeniero va a utilizar esta clave para generar una contraseña única que se puede utilizar junto con la cuenta de usuario de soporte remoto (que ya existe en el dispositivo de forma predeterminada) para ayudarle a crear una nueva cuenta de administrador.



Precaución: no solicite al ingeniero del TAC que le proporcione la contraseña generada por la clave de acceso remoto. No se permite compartir la contraseña.

En esta etapa, póngase en contacto con el ingeniero del TAC para crear la cuenta en una reunión. Verifique que el terminal tenga conectividad de red y que pueda utilizar SSH para conectarlo. En la aplicación SSH que está utilizando, el ingeniero del TAC toma el control de su pantalla de forma remota e ingresa el nombre de usuario remotesupport y la contraseña generada por la clave de acceso remoto que proporcionó. A continuación, el ingeniero crea la nueva cuenta de administrador en el dispositivo mediante un shell de comandos especial en el terminal.



Advertencia: No intervenga con la aplicación SSH mientras el ingeniero está creando la cuenta de usuario y no revoque el control de pantalla del ingeniero del TAC. Este shell es estrictamente utilizado por el TAC. Corre el riesgo de ser elegible para una RMA si ejecuta algún comando que pueda dañar el dispositivo durante este procedimiento.

Después de crear la nueva cuenta de administrador, utilícela para iniciar sesión en la GUI del

dispositivo en el navegador mediante la dirección IP del terminal. Si es necesario, podrá crear más cuentas de usuario desde la GUI.

Contraseña de usuario de soporte remoto no aceptada

Existe la posibilidad de que cuando los ingenieros del TAC intenten escribir la contraseña en la aplicación SSH para iniciar sesión en la consola del terminal, vea un error Invalid Password . Es probable que el ingeniero haya escrito correctamente la contraseña, pero no se aceptó. Esto suele suceder porque, en su equipo local, no ha cambiado el idioma al inglés. Ha estado utilizando un idioma diferente y, por tanto, la contraseña que ha escrito el ingeniero que tiene el control de su PC no está en inglés. Debido a esto, no puede iniciar sesión en la consola. Asegúrese de que el idioma local del PC está establecido en inglés antes de iniciar la resolución de problemas.

Además, es posible que caracteres como la barra diagonal inversa (\) o la barra diagonal (/) se puedan asignar de forma diferente en el teclado. Por ejemplo, esto significa que el ingeniero escribe una barra diagonal inversa (\), pero en realidad, se escribe una barra diagonal (/). Si el idioma local está establecido en inglés y la contraseña parece seguir sin funcionar, genere una clave de acceso remoto nueva desde el concentrador de control y compártala con el ingeniero. El ingeniero genera una nueva contraseña y comprueba si existen caracteres especiales. Se puede probar un nuevo inicio de sesión con la nueva contraseña.

```
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
```

Mensaje SSH de acceso denegado



Advertencia: En algunos teclados, hay casos en los que el carácter y se asigna al carácter z y viceversa. Para no tener dudas sobre la contraseña escrita, el ingeniero puede intentar escribir esta cadena en la barra de búsqueda del navegador o en una aplicación de notas:

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

Esto no se debe copiar y pegar, sino escribir. Si los caracteres aparecen en un orden distinto al que se han escrito, significa que hay una discordancia de caracteres en el teclado.

Además, las máquinas con teclados que no sean QWERTY pueden tener resultados similares. Asegúrese de informar al ingeniero acerca de su configuración en tales situaciones.

Información Relacionada

[Reinicio de fábrica / borrado de datos seguro](#)

[Activar cuentas de usuario en dispositivos registrados en la nube](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).