

Recupere a GUI do endpoint registrado na nuvem quando estiver off-line no Control Hub

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Descrição detalhada do cenário](#)

[Redefinição de fábrica do dispositivo](#)

[Entre em contato com o TAC para configurar manualmente uma conta de administrador em seu endpoint](#)

[Senha de usuário de suporte remoto não aceita](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve a recuperação de conta de endpoint quando as contas locais são desabilitadas após o registro na nuvem e o endpoint fica offline no Control Hub.

Pré-requisitos

Requisitos

Recomenda-se que você tenha alguma familiaridade com estes tópicos:

- Plataforma de Hub de Controle
- Registro e administração de endpoints por meio da GUI (Graphical User Interface, interface gráfica do usuário) do endpoint.

Componentes Utilizados

Este equipamento foi usado para fazer os testes e produzir os resultados descritos neste documento:

- Ponto de extremidade do Kit de Sala
- endpoint do Desk Pro

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Descrição detalhada do cenário

Ao registrar um dispositivo na nuvem, você é solicitado a decidir se deseja manter suas contas de usuário locais no próprio dispositivo ativo. Por padrão, as contas de usuário local são excluídas.

Este documento descreve como recuperar a conta admin do seu ponto final quando você tiver desabilitado as contas locais no dispositivo após o registro na nuvem e seu ponto final estiver offline no Hub de Controle.

×

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](#).

Registre-se no pop-up do Webex a partir da GUI do endpoint

Isso significa que você não pode acessar a interface gráfica do usuário ou a GUI do dispositivo por meio do navegador usando o endereço IP do dispositivo. Você tem acesso à GUI do dispositivo somente através da plataforma de Hub de controle navegando para Dispositivos na seção Gerenciamento em seu Hub de controle. Em seguida, escolha um dos dispositivos on-line para efetuar login na GUI e clique em Local Device Control na seção Support:

Support

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

Controle de Dispositivo Local no Hub de Controle

Uma nova janela é aberta. Selecione Continuar para abrir a GUI do 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.

Cancel

Proceed

Pop-up Controles do Dispositivo Local no Hub de Controle

Em seguida, a GUI do endpoint é aberta no navegador. A partir daí, você pode criar um novo usuário e usá-lo para fazer login na GUI do dispositivo usando o endereço IP do próprio dispositivo no navegador. Todo o procedimento em detalhes é descrito neste vídeo: [Ativando contas de usuário em dispositivos registrados na nuvem](#) .



Observação: você precisa estar na mesma rede que o endpoint; caso contrário, você não poderá acessar a GUI. Se não estiver, você verá esta página no navegador depois de clicar em Continuar:

The connection has timed out

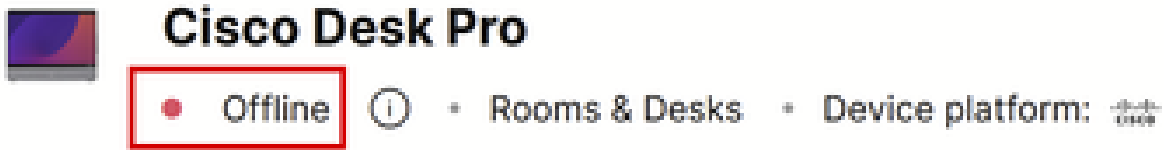
An error occurred during a connection to [redacted]

- 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](#)

Mensagem de Conexão de Tempo Limite do Navegador

Ocorre um problema quando seu endpoint é exibido como off-line no Control Hub (mostrado aqui):



Status Offline do Ponto de Extremidade no Hub de Controle

Neste cenário, você não pode acessar a GUI do endpoint a partir do Control Hub. O Controle de dispositivo local descrito anteriormente neste artigo não funcionará, pois está praticamente acessando a GUI do dispositivo via HTTP e requer que o dispositivo esteja on-line. Se você tiver optado por desabilitar contas de usuário locais durante o registro do dispositivo, deliberada ou acidentalmente, você também não poderá acessar a GUI do dispositivo usando seu endereço IP no navegador. Neste estágio, você perdeu o acesso à GUI do seu dispositivo. A menos que você possa colocar o dispositivo novamente on-line com alguma solução de problemas básica acessando fisicamente o dispositivo, você será bloqueado para fora dele.

Há duas sugestões de planos de ação a escolher para sair desta situação:

- Fatory Reset (Restaurar fábrica) do dispositivo.
- Entre em contato com o TAC depois de obter uma chave de acesso remoto.

Redefinição de fábrica do dispositivo

A redefinição de fábrica do dispositivo nesse cenário específico pode ser feita acessando fisicamente o dispositivo. Há duas opções possíveis:

- No painel de toque conectado ao endpoint (Navigator ou Touch 10 peripheral device), navegue até settings (Configurações) e selecione a opção Fatory Reset (Redefinição de fábrica). Para dispositivos de placa que não têm painel de toque conectado a eles, a tela de toque do endpoint tem o botão Settings no canto superior direito da tela.
- Os endpoints têm um pinhole na parte traseira ou inferior do dispositivo. O orifício do orifício, dependendo do dispositivo, pode ser coberto com uma tampa de plástico. Você pode usar um pino de segurança ou um clipe de papel e inseri-lo no orifício do orifício e pressionar por 10 a 15 segundos. Em seguida, uma redefinição de fábrica será iniciada.



Observação: quando a redefinição de fábrica for usada, todas as configurações e arquivos de dispositivo (como arquivos de log ou quadros de comunicações) salvos no dispositivo serão excluídos. Não há opção para manter um backup para a configuração e os arquivos do dispositivo e reutilizá-lo depois que o dispositivo for registrado na nuvem novamente.

Alguns detalhes adicionais sobre a redefinição de fábrica são fornecidos no artigo: [Factory-Reset-|-Secure-Data-Wipe](#) .



Aviso: você deve configurar e registrar o dispositivo na nuvem novamente desde o início se decidir executar uma redefinição de fábrica. Antes de registrar o dispositivo na nuvem, exclua seu espaço de trabalho anterior da lista de espaços de trabalho em sua organização de hub de controle e recrie-o se você planeja usar o mesmo espaço de trabalho de antes. Não é possível adicionar novamente o mesmo ponto de extremidade ao espaço de trabalho já existente. O Workspace está vendo o endpoint como off-line, mas ainda considera que ele está registrado nele. Não há suporte para a adição de um segundo ponto de extremidade a um espaço de trabalho no momento da criação deste artigo.

Depois que o dispositivo for inicializado após a redefinição de fábrica e você verificar se tem conectividade com a rede, você pode usar o IP do dispositivo para fazer login na GUI do dispositivo usando as credenciais padrão: o nome de usuário é admin e a senha está em branco. Em seguida, crie usuários adicionais neste endpoint e continue registrando o dispositivo no espaço de trabalho recém-criado em sua organização de hub de controle. Certifique-se de desmarcar essa opção quando a janela de registro for exibida:



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](#).

Registre-se no pop-up do Webex a partir da GUI do endpoint



Observação: para acessar a GUI do endpoint, você precisa inserir o endereço IP do endpoint em um navegador da Web e usar as credenciais de um administrador para fazer login. O nome de usuário padrão é admin e a senha padrão está em branco, mas apenas para um endpoint que você acabou de receber ou que você redefiniu de fábrica. Você precisa estar na mesma rede/VLAN que o endpoint que está tentando acessar ou não poderá usar a GUI do dispositivo.

Quando o dispositivo estiver registrado na nuvem, você poderá acessar a GUI por meio do Control Hub e usando o endereço IP do endpoint no navegador e fazendo login com uma de suas contas de usuário criadas ou com a conta de usuário padrão.

Entre em contato com o TAC para configurar manualmente uma conta de administrador em seu endpoint

Se você não quiser perder a configuração que já existe em seu endpoint, em vez de executar uma redefinição de fábrica, abra um ticket no TAC e descreva seu problema. O engenheiro do TAC pedirá que você faça login em sua organização de hub de controle, navegue até a guia Devices na seção Management e selecione o endpoint ao qual você perdeu o acesso:

The screenshot displays the 'Devices' management interface in Cisco Control Hub. The left sidebar contains navigation menus for 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. The 'Devices' section is active, with filters for Online (11), Expired (0), Offline (21), and Issues (3). A search bar and an 'Add device' button are at the top right. The device list has columns for Type, Product, Status, Platform, and Belongs to. One device, 'Cisco Desk Pro', is highlighted with a red box and marked as '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] |

Seção Dispositivos no Hub de Controle

Em seguida, navegue até a seção Suporte e clique em Chave de acesso remoto. Aparece uma janela que contém uma chave longa parecida com a que aparece na imagem (essa chave foi redefinida no dispositivo de teste e não é mais válida) abaixo:

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

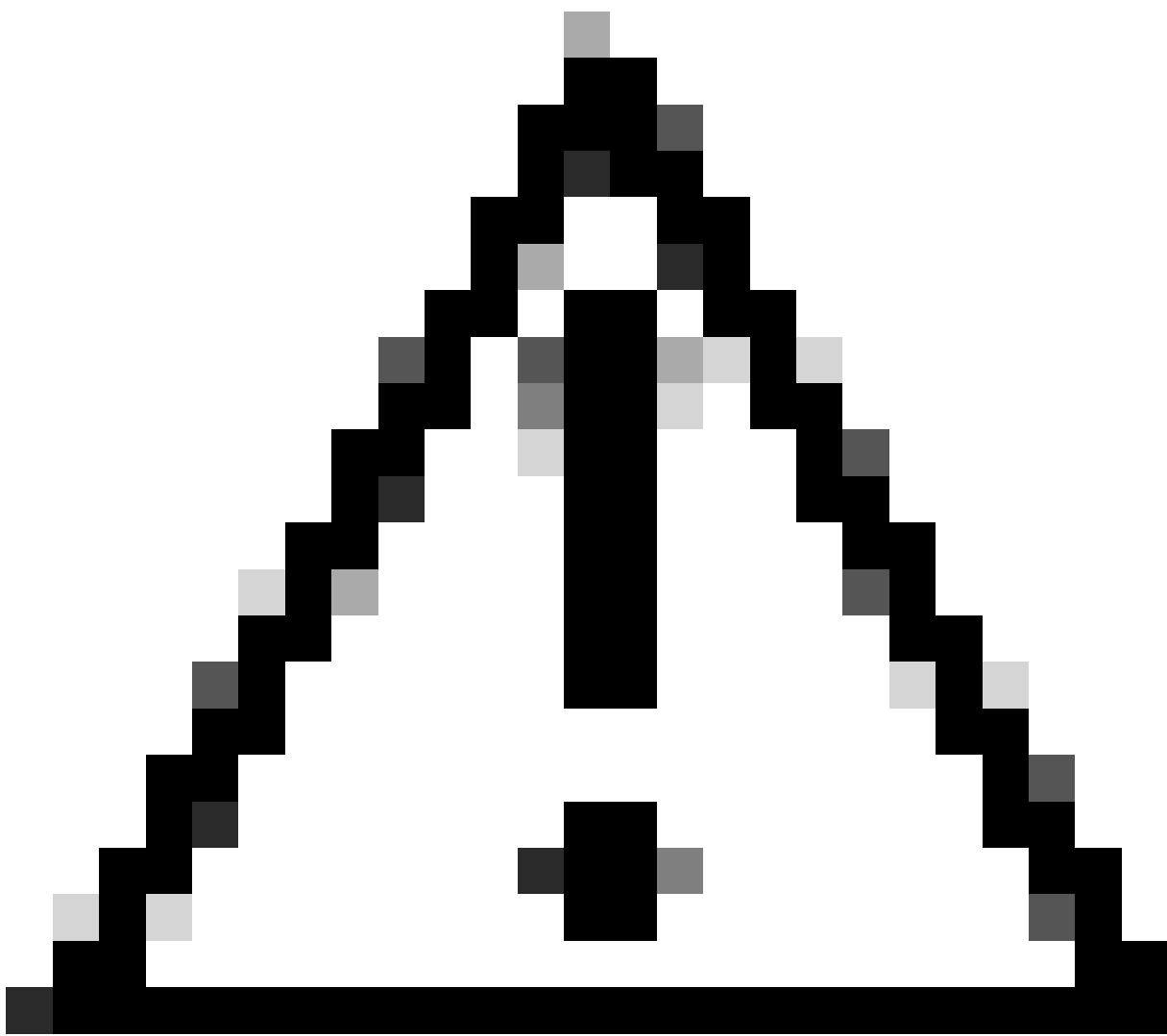
 Copy to Clipboard

 Reset Key

Done

Pop-up Chave de Acesso Remoto no Hub de Controle

Copie essa chave e compartilhe-a com o engenheiro do TAC designado ao seu caso. O engenheiro usará essa chave para gerar uma senha exclusiva que pode ser usada junto com a conta de usuário de suporte remoto (que já existe no dispositivo por padrão) para ajudá-lo a criar uma nova conta de administrador.



Cuidado: não solicite que o engenheiro do TAC forneça a senha gerada pela chave de acesso remoto. Não é permitido compartilhar a senha.

Nesse estágio, entre em contato com o engenheiro do TAC para criar a conta em uma reunião. Verifique se o endpoint tem conectividade de rede e se você pode executar SSH para ele. No aplicativo SSH que você está usando, o engenheiro do TAC assume o controle da tela remotamente e insere o nome de usuário remotesupport e a senha gerada pela chave de acesso remoto fornecida. Em seguida, o engenheiro cria a nova conta admin no dispositivo usando um shell de comando especial no endpoint.



Aviso: Não intervenha com o aplicativo SSH enquanto o engenheiro estiver criando a conta de usuário e não revogue o controle de tela do engenheiro TAC. Este shell é estritamente usado pelo TAC. Você corre o risco de ser elegível para uma RMA se executar você mesmo qualquer comando que possivelmente danifique o dispositivo durante este procedimento.

Após a criação da nova conta de administrador, use-a para fazer login na GUI do dispositivo em seu navegador usando o endereço IP do ponto final. Você poderá criar mais contas de usuário na GUI, se necessário.

Senha de usuário de suporte remoto não aceita

Há uma chance de que quando os engenheiros do TAC tentam digitar a senha no aplicativo SSH para fazer login no console do endpoint, você veja um erro Senha inválida. A senha provavelmente foi digitada corretamente pelo engenheiro, mas não foi aceita. Isso geralmente acontece porque, na sua máquina local, você não alterou o idioma para inglês. Você tem usado um idioma diferente e, portanto, a senha digitada pelo engenheiro que controla seu PC não está em inglês. Por causa disso, você não pode fazer login no console. Verifique se o idioma local no PC está definido em inglês antes do início da solução de problemas.

Além disso, caracteres como barra invertida (\) ou barra (/) podem ser mapeados de forma diferente no teclado. Por exemplo, isso significa que o engenheiro digita uma barra invertida (\), mas, na realidade, uma barra (/) é digitada. Se o idioma local estiver definido como inglês e a senha parecer ainda não funcionar, gere uma nova chave de acesso remoto a partir do Control Hub e compartilhe-a com o engenheiro. O engenheiro gera uma nova senha e verifica se existem caracteres especiais. Um novo login pode ser tentado com a nova senha.

```
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 de acesso negado



Aviso: há casos em que o caractere y é mapeado para o caractere z e vice-versa em alguns teclados. Para não ter dúvidas sobre a senha digitada, o engenheiro pode tentar digitar essa string na barra de pesquisa do navegador ou em um aplicativo de anotações:

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

Ele não deve ser copiado e colado, mas digitado. Se os caracteres aparecerem em ordem diferente daquela em que foram digitados, haverá uma incompatibilidade de caracteres no teclado.

Além disso, máquinas com teclados não QWERTY podem ter resultados semelhantes. Certifique-se de informar o engenheiro sobre sua configuração nesses cenários.

[Redefinição de fábrica/Apagamento seguro de dados](#)

[Ativando contas de usuário em dispositivos registrados na nuvem](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.