Resolución de problemas y recopilación de información básica para el equipo de soporte de acceso seguro

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Antecedentes

Localice La ID De La Organización De Secure Access

Herramienta Cisco Secure Client Diagnostic and Reporting Tool (DART)

Activar registros de depuración para módulos ZTNA y SWG

- Habilitar registros de depuración para ZTNA
- Activar registros de depuración para SWG
- Habilitar registros de depuración para DUO

Recopilar registros KDF para ZTNA y SWG, módulos DNS (Windows)

- Prerequisites

Capturas de archivo HTTP (HAR)

Capturas de paquetes

Resultado de depuración de políticas

Comandos comunes Resolución de problemas del túnel de sitio a sitio

Comandos comunes Resolución de problemas del conector de recursos

Cargar Resultados En La Solicitud Del Servicio De Asistencia De Cisco

Información Relacionada

Introducción

Este documento describe la información básica que se debe recopilar mientras se trabaja con el equipo de soporte de Cisco Secure Access

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Acceso seguro de Cisco
- Cliente seguro de Cisco

- Capturas de paquetes mediante Wireshark y tcpdump

Componentes Utilizados

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.

Antecedentes

Mientras trabaja en Cisco Secure Access, puede tener problemas cuando necesite ponerse en contacto con el equipo de soporte de Cisco o desee realizar una investigación básica del problema e intentar revisar los registros e aislar el problema. En este artículo se explica cómo recopilar los registros básicos de solución de problemas relacionados con el acceso seguro. tenga en cuenta que no todos los pasos se aplican a todos los escenarios.

Localice La ID De La Organización De Secure Access

Para que el ingeniero de Cisco localice su cuenta, proporcione su ID de organización, que se puede encontrar en la URL una vez que haya iniciado sesión en el panel de acceso seguro.

Pasos para localizar la ID de organización:

1. Inicie sesión en sse.cisco.com
2. Si tiene varias organizaciones, cambie a la correcta.
3. El ID de la organización se puede encontrar en la URL en este patrón: https://dashboard.sse.cisco.com/org/{7_digit_org_id}/overview

Herramienta Cisco Secure Client Diagnostic and Reporting Tool (DART)

Cisco Secure Client Diagnostic and Reporting Tool (DART) es una herramienta que se instala con el paquete Secure Client y ayuda a recopilar información importante sobre el terminal del usuario.

Ejemplo de información recopilada por el paquete DART:

- Registros ZTNA
- Registros de clientes seguros e información de perfil
- Información del sistema
- Otros registros de complementos o complementos de Secure Client instalados en

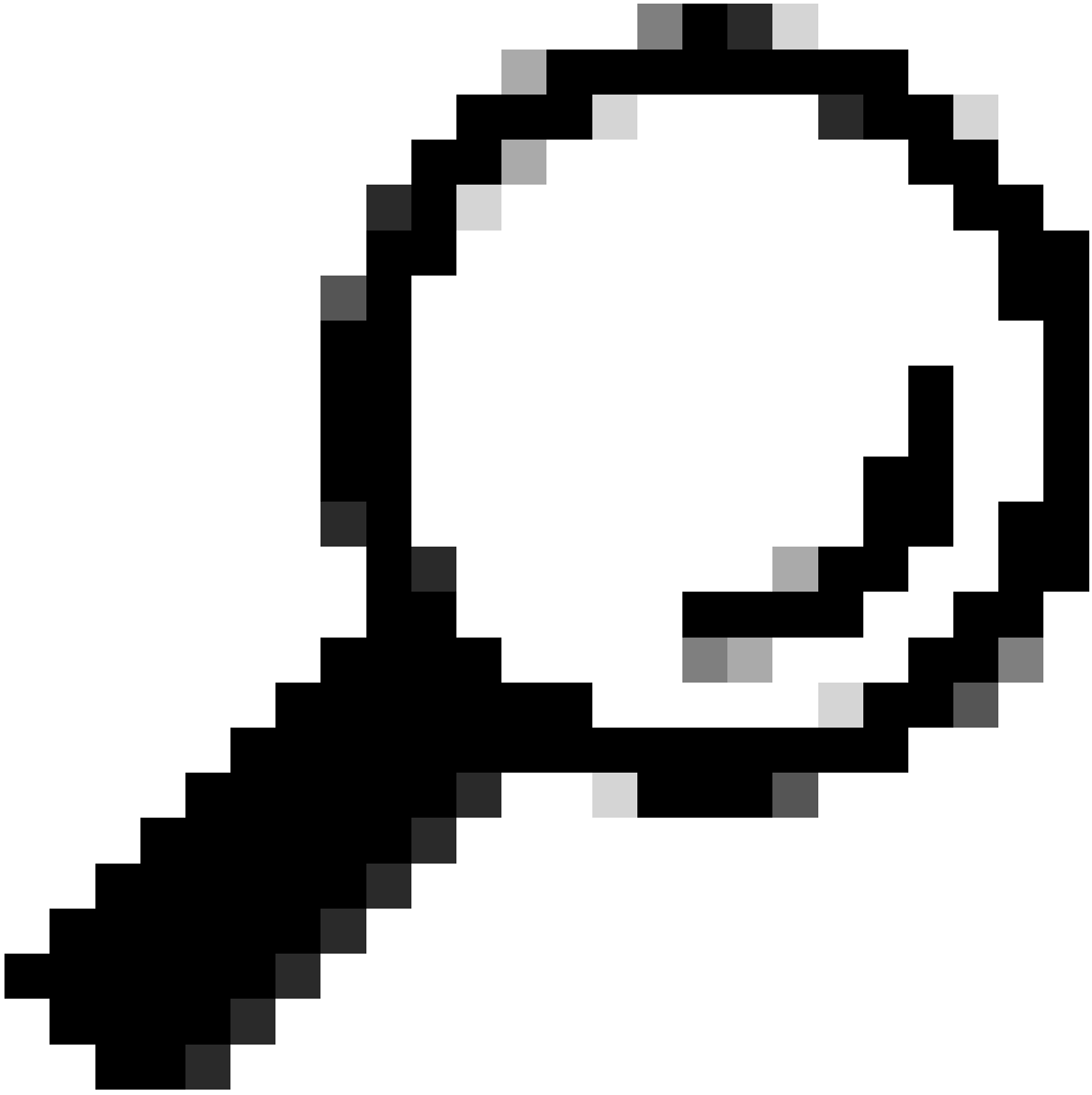
Instrucciones para recopilar DART:

Paso 1. Inicie DART.

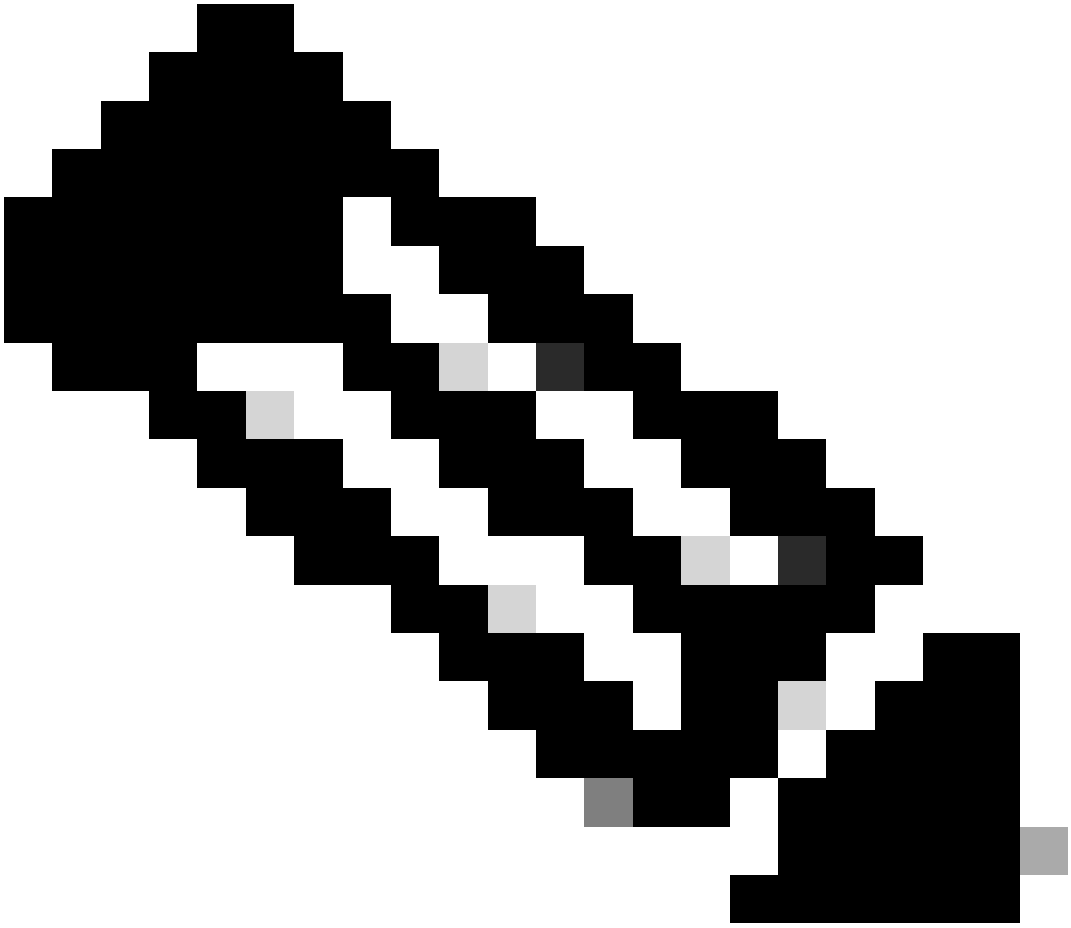
1. Para un ordenador con Windows, inicie Cisco Secure Client.
2. Para una computadora Linux, elija **Applications** > **Internet** > **Cisco DART**O /opt/cisco/anyconnect/dart/dartui.
3. Para un ordenador Mac, seleccioneApplications > Cisco > Cisco DART.

Paso 2. Haga clic en la pestaña Estadísticas y luego haga clic en Detalles.

Paso 3. Elija la creación de paquetes predeterminada o personalizada.



Consejo: El nombre predeterminado del paquete es DARTBundle.zip y se guarda en el escritorio local.



Nota: Si selecciona Predeterminado, DART comenzará a crear el paquete. Si selecciona Personalizado, continúe con las indicaciones del asistente para especificar registros, archivos de preferencias, información de diagnóstico y cualquier otra personalización

Activar registros de depuración para módulos ZTNA y SWG

En algunos escenarios, el equipo de soporte técnico necesitaría habilitar registros de nivel de seguimiento o depuración para identificar problemas más complejos.

complete los pasos proporcionados en esta sección para habilitar las depuraciones para cada uno de los módulos.

Habilitar registros de depuración para ZTNA

Paso 1. Cree un archivo json con el nombre logconfig.json

Paso 2. Introduzca este texto dentro del archivo

```
{ "global": "DBG_TRACE" }
```

Paso 3. Coloque el archivo en el directorio correcto basado en el sistema operativo

- Windows: C:\ProgramData\Cisco\Cisco Secure Client\ZTA
- MacOS: /opt/cisco/secureclient/zta

Paso 4. Reinicie el módulo ZTNA o Cisco Secure Client para que los registros tengan efecto.

Activar registros de depuración para SWG

Paso 1. Cree un archivo json con el nombre SWGConfigOverride.json

Paso 2. Introduzca este texto dentro del archivo

```
{"logLevel": "1"}□
```

Paso 3. Coloque el archivo en el directorio correcto basado en el sistema operativo

- Windows: C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\SWG\
- MacOS: /opt/cisco/secureclient/umbrella/swg

Paso 4. Reinicie el módulo SWG o Cisco Secure Client para que los registros tengan efecto.

Habilitar registros de depuración para DUO

Habilitar registros KDF DUO (solución de problemas de estado, problemas de inscripción)

```
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Duo\Duo Device Health” /v verbose_logging_enabled /d 1 /f
```

Deshabilitar registros KDF DUO

```
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Duo\Duo Device Health” /v verbose_logging_enabled /d 0 /f
```

Recopilar registros KDF para ZTNA y SWG, módulos DNS (Windows)

En algunos de los escenarios, el equipo de soporte requeriría recopilar registros de kdf para identificar problemas más complejos.

complete los pasos proporcionados en esta sección para configurar y recopilar los registros de kdf.

Prerequisites

Es necesario instalar DebugView para recopilar los registros correctamente. que se puede instalar mediante esta fuente: https://learn.microsoft.com/en-us/sysinternals/downloads/debugview

Habilitar la clave de registro DNS

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\acsock" /v DebugFlags /d 0x20801FF /t reg
```

Activar clave de registro SWG

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\acsock" /v DebugFlags /d 0x70C01FF /t reg
```

Habilitar clave de registro ZTNA

```
"%ProgramFiles(x86)%\Cisco\Cisco Secure Client\acsocktool.exe" -sdf 0x40018EF52
```

Deshabilitar todos los indicadores

```
"%ProgramFiles(x86)%\Cisco\Cisco Secure Client\acsocktool.exe" -cdf
```

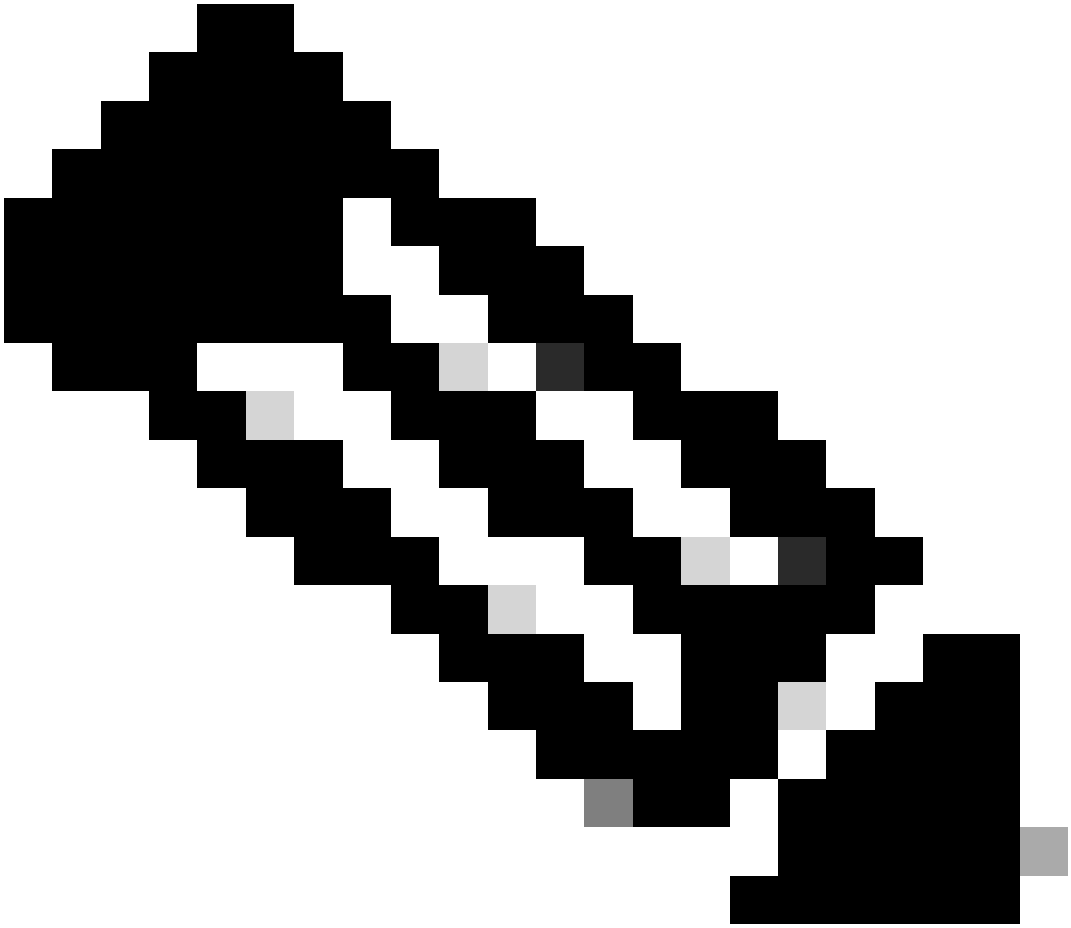
Capturas de archivo HTTP (HAR)

HAR se puede recopilar de diferentes navegadores. proporciona información múltiple que incluye:

1. Versión descifrada de las solicitudes HTTPS.
2. Información interna sobre mensajes de error, detalles de solicitud y encabezados.
3. Información sobre plazos y retrasos
4. Otra información diversa sobre solicitudes basadas en navegador.

Para recopilar capturas de HAR, siga los pasos descritos en esta fuente:

https://toolbox.googleapps.com/apps/har_analyzer/



Nota: Debe actualizar la sesión del navegador para recopilar los datos adecuados

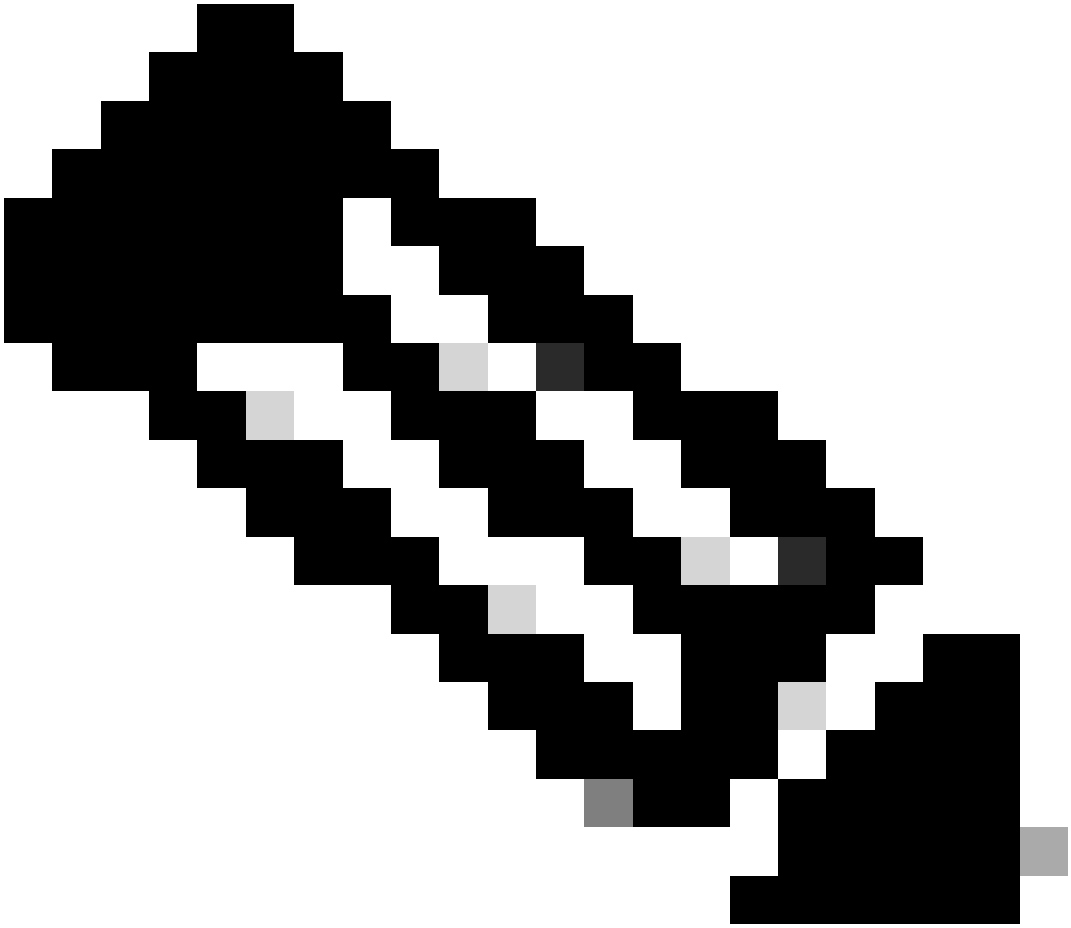
Capturas de paquetes

Las capturas de paquetes son útiles en un escenario donde se detecta un problema de rendimiento o una pérdida de paquetes, o una interrupción total de la red. Las herramientas más comunes para recopilar capturas son wireshark y **tcpdump**. O bien, una capacidad integrada para recopilar archivos en formato pcap dentro del propio dispositivo, como un firewall o router de Cisco.

Para recopilar capturas útiles de paquetes en un terminal, asegúrese de incluir:

1. Interfaz de loopback para capturar el tráfico enviado a través de los complementos de Secure Client.

2. Todas las demás interfaces involucradas en el trayecto del paquete.
3. Aplique filtros mínimos o ningún filtro para asegurarse de que se recopilan todos los datos.



> Nota: Cuando se recopilan capturas en un dispositivo de red, asegúrese de filtrar por el origen y el destino del tráfico, y limite las capturas a los puertos y servicios relacionados solamente, para evitar cualquier rendimiento causado por esta actividad.

Resultado de depuración de políticas

La salida de depuración de políticas es una salida de diagnóstico enviada a través del navegador del usuario cuando está protegida por Secure Access. que incluye información crítica sobre la implementación.

1. ID de la organización
2. Tipo de implementación
3. Proxy conectado
4. Dirección IP pública y privada

5. Otra información relacionada con el origen del tráfico.

Para ejecutar los resultados de la prueba de políticas, inicie sesión en este enlace desde un terminal protegido: https://policy.test.sse.cisco.com/

Asegúrese de que confía en el certificado raíz de acceso seguro si aparece un mensaje de error de certificado en su navegador.

Para Descargar El Certificado Raíz De Acceso Seguro:

Desplácese hasta Acceso seguro Dashboard > Secure > Settings > Certificate > (Internet Destinations tab)

Comandos comunes Resolución de problemas del túnel de sitio a sitio

<#root>

```
# Tunnel Establishment


asa>show crypto ikev1 sa
asa>show crypto ikev2 sa
asa>show crypto ipsec sa
asa>show crypto session


#BGP Troubleshooting


asa>show running-config router bgp
asa>show bgp summary
asa>show ip bgp neighbors


#Routes Advertisements


asa>show bgp ipv4 unicast neighbors <sse-dc-ip> advertised-routes
asa>show bgp ipv4 unicast neighbors <sse-dc-ip> received-routes
asa>show bgp ipv4 unicast neighbors <sse-dc-ip> routes


#Debug BGP events


asa>debug ip bgp
asa>debug ip bgp events
asa>debug ip bgp updates
asa>debug ip routing


#Disable Debugs


asa>undebug all
```

Comandos comunes Resolución de problemas del conector de recursos

La lista proporcionada proporciona una vista completa del conector de recursos y detalles importantes de solución de problemas para el equipo de soporte de acceso seguro

<#root>

```
#DNS and connectivity tests on the local IP address, gateway, Secure Access APIs

rc-cli> diagnostic
#Software version, VPN tunnel state, system health, sysctl settings, routes and iptables

rc-cli> techsupport
#Packet captures

rc-cli> tcpdump <host>
```

Cargar Resultados En La Solicitud Del Servicio De Asistencia De Cisco

Puede cargar archivos en un caso de soporte mediante estos pasos:

Paso 1. Inicie sesión en SCM.

Paso 2. Para ver y editar el caso, haga clic en el número o título del caso en la lista. Se abre la página de resumen del caso.

Paso 3. Haga clic en Agregar archivos para elegir un archivo y cargarlo como un archivo adjunto al caso. El sistema muestra la herramienta Cargador de archivos SCM.

Paso 4. En el cuadro de diálogo Elegir archivos para cargar, arrastre los archivos que desea cargar o haga clic dentro para examinar el equipo local en busca de archivos para cargar.

Paso 5. Agregue una descripción y especifique una categoría para todos los archivos, o individualmente.

Información Relacionada

- Soporte técnico y descargas de Cisco
- Documentación de Secure Access y guía del usuario
- Descarga del software Cisco Secure Client

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).