Consejos de seguridad y desvinculación (offboarding)

TABLA DE CONTENIDO

Funciones de seguridad en el cliente AnyDesk

Lista de control de acceso (ACL)

Solución On-Premises

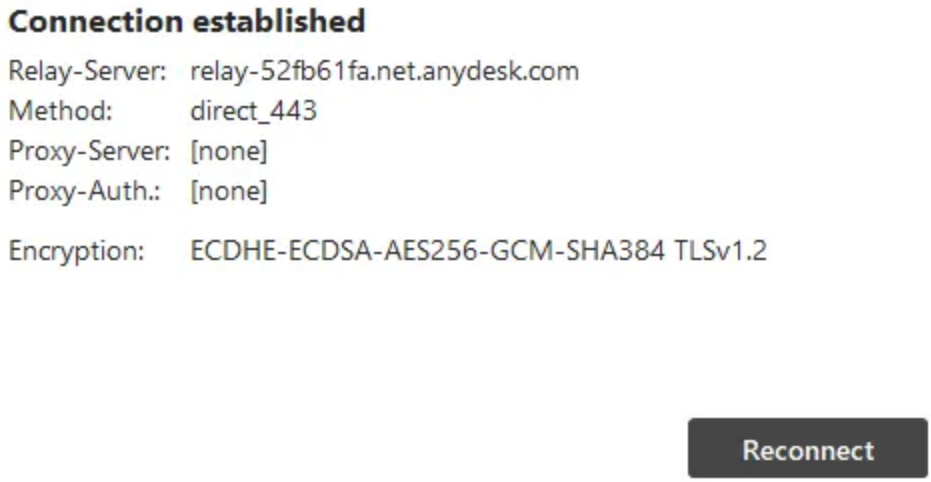
Desviculación (offboarding) de antiguos empleados

Todas las sesiones de AnyDesk están protegidas mediante **TLS 1.2** con cifrado **AEAD**.

Puede ver el tipo de conexión, el modo de cifrado aplicado, el estado de verificación del cliente y la huella digital (fingerprint) haciendo clic en



en la barra de herramientas.



Funciones de seguridad en el cliente AnyDesk

AnyDesk ofrece varias funciones de seguridad para ayudarle a proteger su entorno:

- **Ajustes del cliente personalizado**: configure políticas de seguridad en su cliente personalizado. Para más detalles, consulte Cliente AnyDesk personalizado.
- **Acceso desatendido exclusivo**: acceda al dispositivo remoto utilizando únicamente la contraseña de acceso desatendido.
- **Hash de contraseñas con sal (salted)**: las contraseñas se almacenan de forma segura mediante tokens de hash con sal.
- **Autenticación de dos factores**: proteja el acceso desatendido habilitando la autenticación de dos factores.

Lista de control de acceso (ACL)

Puede restringir las sesiones entrantes utilizando la Lista de control de acceso para permitir únicamente IDs o alias autorizados.

Solución On-Premises

Para entornos de alta seguridad, AnyDesk ofrece una opción de despliegue On-Premises. Esta versión funciona independientemente de Internet, lo que le otorga un control total sobre sus datos.

Desviculación (offboarding) de antiguos empleados

Si un empleado que utiliza AnyDesk deja su organización, siga estos pasos para proteger su entorno:

1. **Elimine su cliente**
   Si conoce el ID o alias de AnyDesk del empleado, en my.anydesk II, vaya a la pestaña *Clients* y elimine su cliente. Esto revoca su acceso a su libreta de direcciones.
2. **Restablezca su clave de licencia**
   Si tienen acceso a la clave de licencia actual, puede restablecerla en my.anydesk II > *License* > *About* > *Reset*. Al eliminar la clave de licencia de su cliente, este pasará a tener una licencia gratuita.
3. **Restrinja el acceso a los clientes personalizados públicos**
   Si las URL de sus clientes personalizados públicos se ven comprometidas, hágalas privadas o

vuelva a crearlas para generar nuevos enlaces. Las copias ya instaladas no se verán afectadas; también debe eliminarlas manualmente de su licencia.

4. **Cambie las contraseñas de acceso desatendido**
   Actualice todas las contraseñas de acceso desatendido que puedan haber sido compartidas o guardadas.
5. **Utilice la Lista de Control de Acceso (ACL)**
   La forma más eficaz de impedir el acceso es configurar la ACL en cada cliente para bloquear el ID o Alias del antiguo empleado. Aunque conozcan sus contraseñas, no podrán conectarse si no están en la lista blanca.
6. **Aprovéchese de los espacios de nombres personalizados**
   Para una gestión más sencilla, considere la posibilidad de adquirir un espacio de nombres personalizado. Las ACL admiten valores comodín, por lo que puede restringir el acceso a sesiones que coincidan con `*@nombre_de_su_empresa`. Si elimina la clave de licencia del cliente de un antiguo empleado, el alias con su espacio de nombres se elimina automáticamente, bloqueando su conexión.