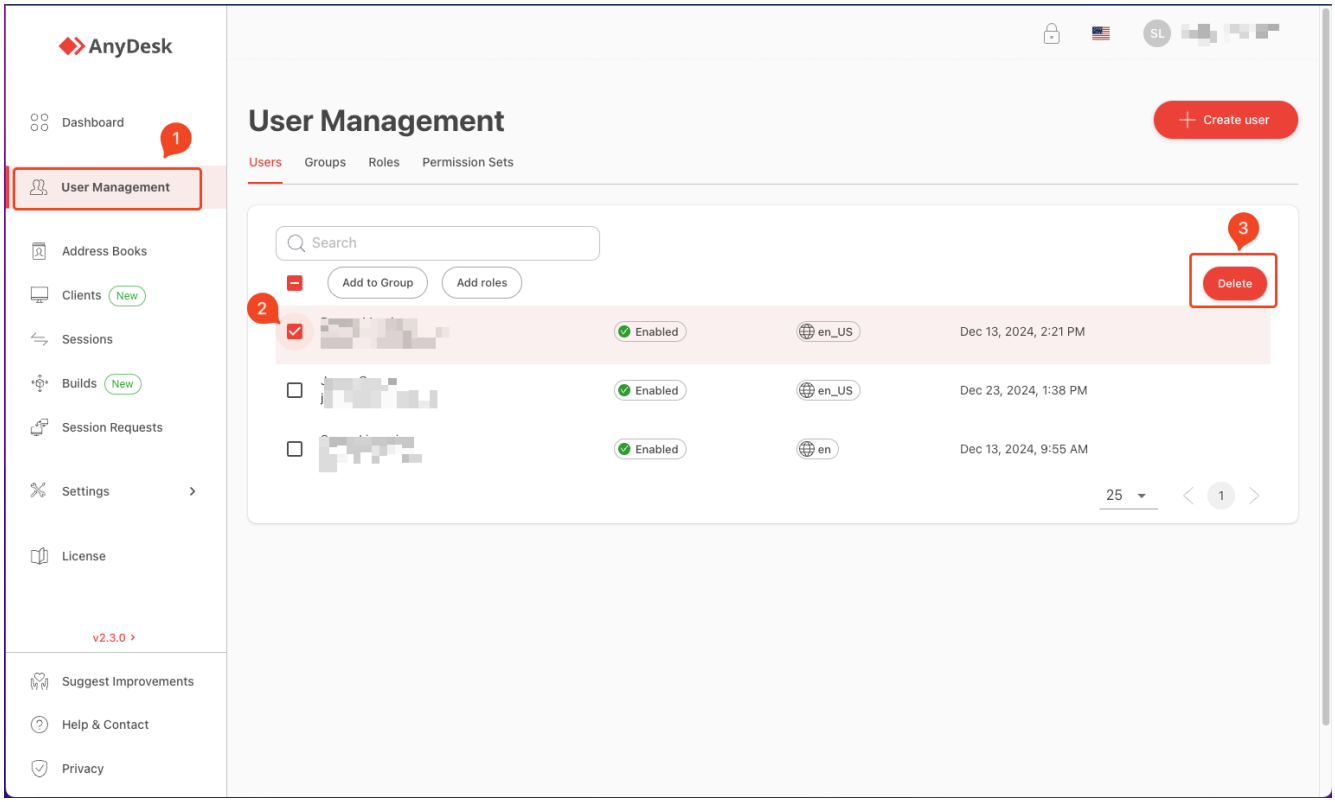
Ayuda de AnyDesk en Español

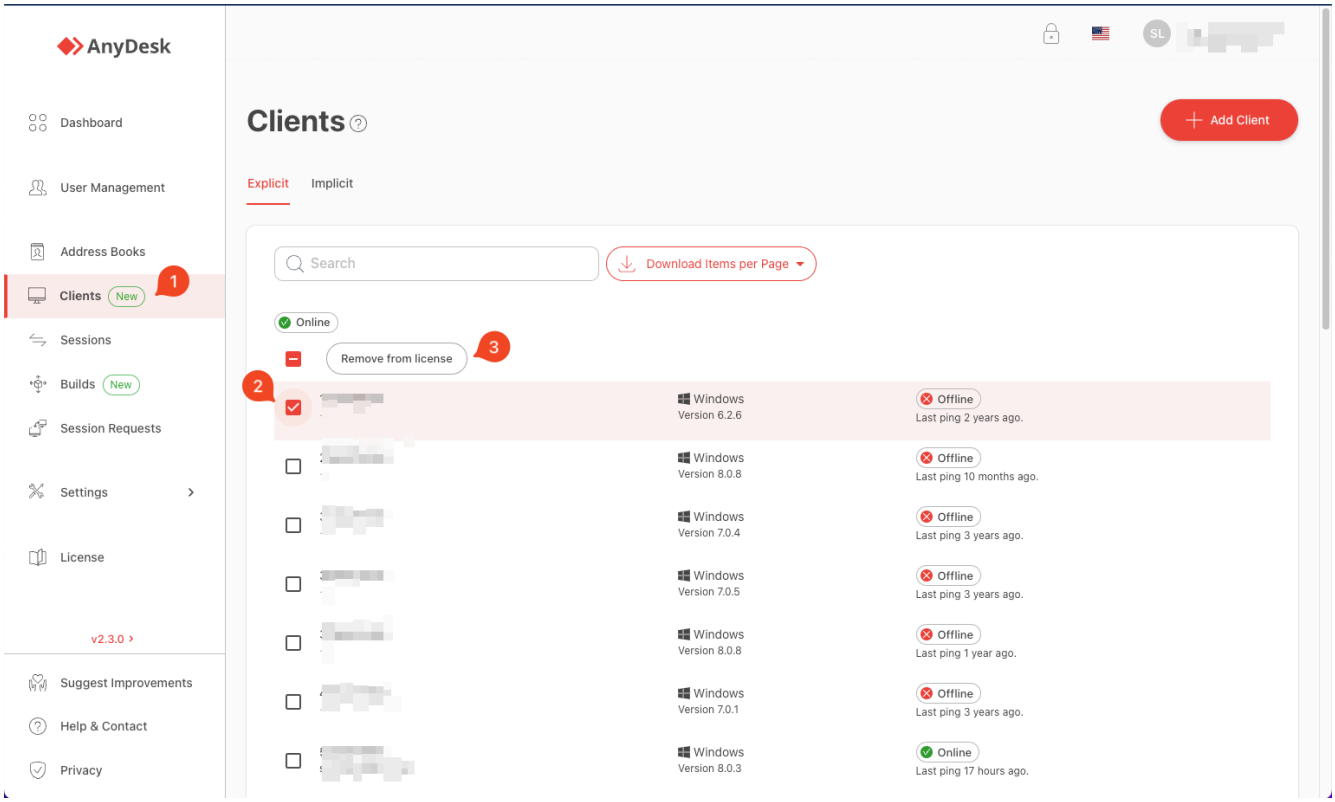
Que hacer si un empleado con acceso a la licencia de AnyDesk deja la empresa?

Cuando un empleado que tiene acceso a AnyDesk deja de trabajar contigo, es esencial tomar medidas preventivas para proteger la seguridad de tus sistemas. A continuación, te compartimos los pasos clave que debes seguir para garantizar que el ex-empleado no pueda seguir utilizando AnyDesk:

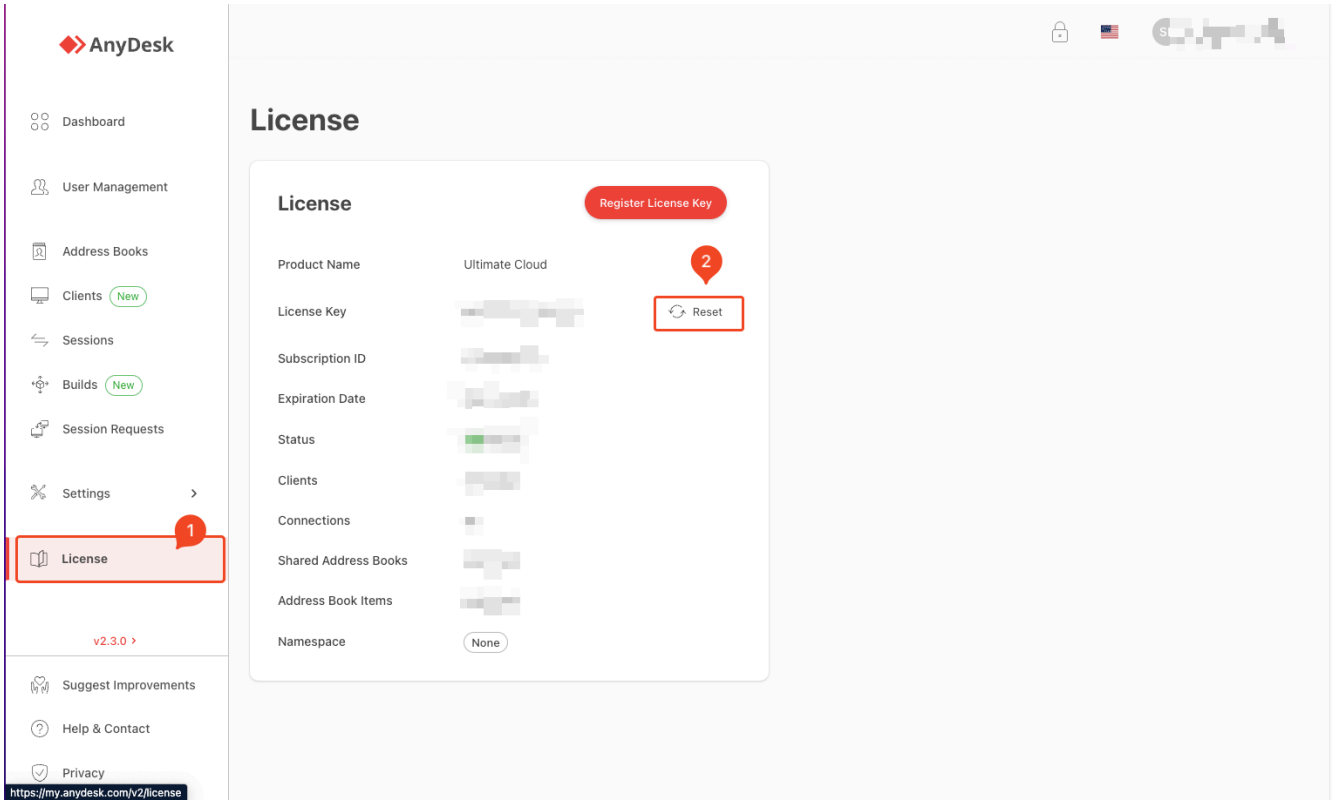
1. Eliminar el cliente y usuario de my.AnyDesk Si creaste un usuario para el empleado en el portal de clientes de AnyDesk, es crucial eliminarlo. Dirígete a **User management**, busca al usuario, **selecciónalo** y elimínalo. De esta forma, ya no podrá acceder al portal ni iniciar sesión en el cliente de AnyDesk.



Además, busca el cliente del usuario en la sección de **Clients**, márcalo y selecciona **Remove from license**. Esto desvinculará el cliente de tu licencia y evitará que se beneficie de sus funciones.



2. Cambiar la clave de la licencia Si el empleado tenía acceso a la clave de la licencia de AnyDesk, es recomendable restablecerla. Al hacerlo, se impedirá que se activen manualmente nuevos clientes con esa clave, aunque los ya licenciados seguirán funcionando. Para restablecerla, accede a la sección de **License** en el portal de AnyDesk y haz clic en **Reset**.



3. Gestión de clientes personalizados Si utilizas clientes personalizados públicos que registran automáticamente los dispositivos en tu licencia, considera hacerlos privados o recrearlos con un nuevo enlace. Esto impedirá que el ex-empleado siga registrando clientes en tu licencia. Como medida de seguridad, **nunca** publiques clientes que permitan conexiones salientes. Solo aquellos que reciben conexiones entrantes deberían ser públicos, asegurando el control de tu licencia.

4. Limpiar los tokens AnyDesk permite guardar contraseñas para facilitar las conexiones futuras. Sin embargo, puedes optar por limpiar todos los tokens en la configuración de seguridad. Esto forzará a que se ingrese la contraseña en cada nueva conexión. No obstante, si el ex-empleado conoce o tiene anotada la contraseña, esta medida por sí sola no será suficiente.

5. Cambiar las contraseñas de acceso no supervisado Si el ex-empleado tenía acceso a las contraseñas de acceso no supervisado y utilizas la gestión centralizada de AnyDesk, cambia las contraseñas de acceso desatendido. Este cambio es inmediato y bloqueará cualquier intento de conexión del empleado.

6. Usar la Lista de Control de Acceso La opción más segura es utilizar la Lista de Control de Acceso para restringir quién puede conectarse a tus dispositivos. Elimina manualmente el AnyDesk-ID o Alias del ex-empleado para bloquear su acceso y proteger tus dispositivos.

7. Adquirir un espacio de nombres personalizado Una opción efectiva es adquirir un espacio de nombres personalizado. Con esta función, puedes configurar la lista de control de acceso para aceptar conexiones solo desde direcciones como “*@tuempresa”. Al eliminar la licencia del cliente del ex-empleado, también eliminarás su Alias asociado al espacio de nombres, bloqueando automáticamente su acceso.

Para más información sobre las ACL y los espacios de nombres personalizados. Puedes encontrar información adicional aquí.

Conclusión Proteger tu infraestructura tecnológica cuando un empleado deja de trabajar en tu empresa es esencial para evitar riesgos de seguridad. Siguiendo estos pasos, podrás garantizar que su acceso a AnyDesk quede completamente revocado, manteniendo a salvo la información y los sistemas de tu organización.