Autenticación de Dos Factores: Guía Completa para AnyDesk y MyAnyDesk

TABLA DE CONTENIDO

Autenticación de Dos Factores
Cliente
- Configuración
- Estableciendo una sesión
- Configuraciones

my.AnyDesk.com
Aplicaciones de autenticación recomendadas
Casos de Uso
- Oficina en Casa
- Limitar el Acceso

Autenticación de Dos Factores

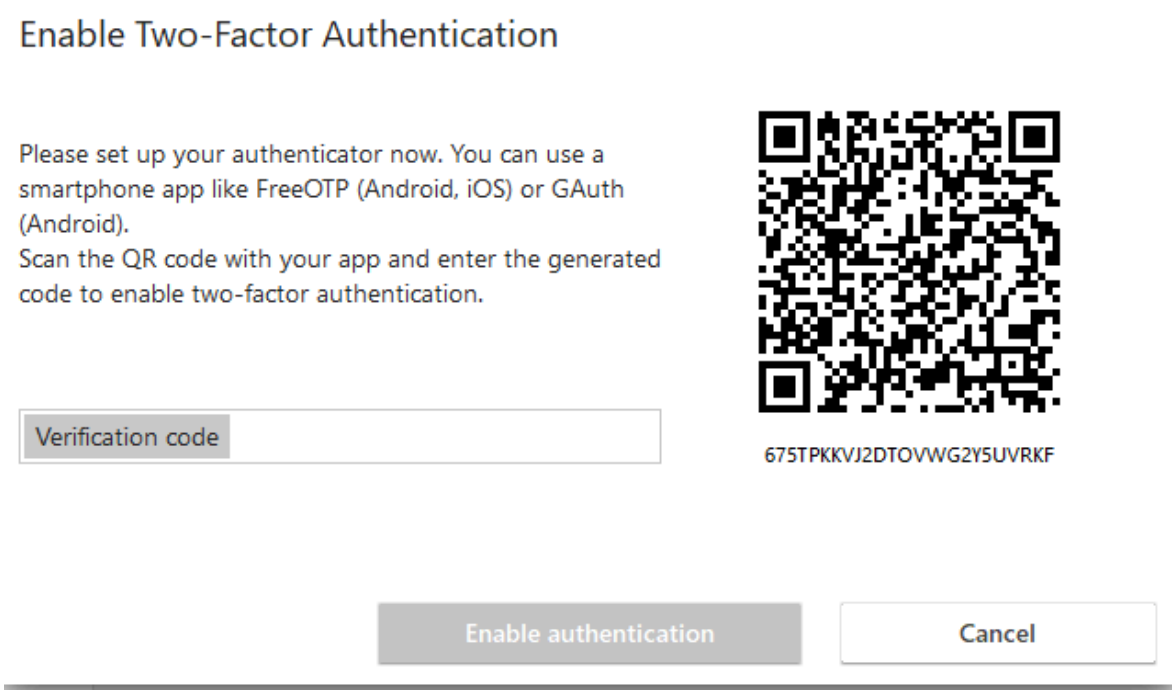
AnyDesk ofrece Autenticación de Dos Factores (2FA) para conexiones de acceso sin supervisión a un cliente específico de AnyDesk, así como para acceder al portal de clientes MyAnyDesk.

Nota: El uso de esta función requiere una aplicación de autenticación que admita “contraseñas de un solo uso basadas en el tiempo” (TOTP por sus siglas en inglés).

Cliente

Para requerir un código de verificación 2FA al conectar a su cliente usando Acceso no Supervisado, se deben completar los siguientes pasos:

Configuración



VirtualBoxVM_ruFnNywIpQ

1. Habilitar “Habilitar autenticación de dos factores” en *Configuración* > *Seguridad* > *Permisos*.
2. Aparecerá una ventana donde el usuario puede escanear el código QR o pegar la clave en uno de nuestros autenticadores recomendados.
3. Ingresar el código de autorización del autenticador y hacer clic en “Habilitar autorización”.

Advertencia:

Si se proporciona el código de autenticación correcto pero el botón “Habilitar autorización” permanece desactivado, asegúrese de que los horarios tanto del autenticador como del dispositivo AnyDesk estén sincronizados. Debido a que los códigos de verificación se basan en el tiempo, no se autenticarán si los horarios no están sincronizados.

Estableciendo una sesión



VirtualBoxVM_J7Vpls2g94

Al conectar a un cliente de AnyDesk con 2FA habilitado, se solicita directamente una clave de autorización de 6 dígitos del autenticador después de que se envía la contraseña de acceso no supervisado de forma manual o automática.

Configuraciones

Si bien AnyDesk entiende la necesidad de 2FA y el nivel de seguridad que aporta, también entendemos que este nivel de autenticación es innecesario para muchos después de la etapa de verificación inicial. Por lo tanto, AnyDesk ofrece dos situaciones en las que el administrador del cliente puede permitir que los usuarios que se conectan omitan la verificación 2FA:

1. Inicio de sesión automático - Si “Habilitar para la información de inicio de sesión guardada” está **desmarcado**, entonces AnyDesk **no** pedirá el código de verificación 2FA cuando el usuario que se conecta esté estableciendo una sesión utilizando el token de Inicio de sesión automático.
2. Contraseñas a corto plazo - Si “Habilitar para contraseñas a corto plazo (por ejemplo, reinicio remoto)” está **desmarcado**, entonces AnyDesk **no** pedirá el código de verificación 2FA al reconectar automáticamente la sesión. Por ejemplo, en el caso de Reinicio remoto.

Regresar al inicio

my.AnyDesk.com

La autenticación de dos factores para MyAnyDesk se puede activar en *Configuración* > *General* > *Autenticación de dos factores* de su portal de cliente MyAnyDesk.

Advertencia:

Imprima o guarde la clave de recuperación en un lugar seguro para restaurar el acceso a su cuenta cuando sea necesario. **NO CONTINÚE SIN GUARDAR O IMPRIMIR LA CLAVE DE RECUPERACIÓN.** La clave de recuperación no se puede recuperar ni restablecer.

En caso de que pierda el acceso a su dispositivo de autenticación y no tenga acceso a la clave de recuperación, comuníquese con el Soporte Técnico de AnyDesk.

Regresar al inicio

Aplicaciones de autenticación recomendadas

Las siguientes aplicaciones de autenticación han sido probadas y se recomiendan para su uso con AnyDesk:

- Google Authenticator
- Microsoft Authenticator
- FreeOTP

Regresar al inicio

Casos de Uso

Oficina en Casa

Configure un teléfono móvil, tableta o PC de la empresa con 2FA para un acceso único para que solo su empleado pueda acceder a la computadora de la oficina.

Además, puede configurar varios dispositivos de autenticación escaneando el mismo código QR con más de un autenticador.

Limitar el Acceso

Limite el acceso a dispositivos seleccionados, como sus servidores, solo a la persona que tiene el dispositivo de autenticación.

Regresar al inicio