AnyDesk México: Mayorista oficial. Mejor precio y respaldo.

Guía Completa para Maximizar la Seguridad de AnyDesk en México: Consejos Prácticos para Administradores de TI y Usuarios

TABLA DE CONTENIDO

- Contenido de la Guía
- my.anydesk II
- Gestión de Permisos y Usuarios
  - Tabla de Roles y Permisos
- Autenticación de Dos Factores para my.anydesk II
- Cliente Personalizado de AnyDesk
- Clientes Solo de Entrada y Solo de Salida
  - Configuraciones
- Lista de Control de Acceso (ACL) y Namespace Personalizado
  - Pasos para Configurar la Lista de Control de Acceso:
- Permisos para la Conexión
  - Perfiles de Permisos
  - Acceso No Asistido
  - Autenticación de Dos Factores para Acceso No Asistido
  - Forzar Inicio de Sesión de Usuario
- Caso de Uso
  - Configuración de AnyDesk para Soporte Remoto
  - Permisos en my.anydesk II

Esta guía está creada pensando en los administradores de TI y usuarios de empresas en México. Aquí encontrarás consejos prácticos para maximizar la configuración de AnyDesk y garantizar la seguridad de tus operaciones de trabajo remoto.

Contenido de la Guía

• my.anydesk II – Aprende sobre los roles y permisos básicos que se pueden asignar a los usuarios.
• Cliente personalizado de AnyDesk – Descubre cómo personalizar tus clientes de AnyDesk para incrementar su seguridad.
• Caso de uso – Revisa ejemplos de configuraciones de clientes personalizados de AnyDesk.

my.anydesk II

Cuando decides comprar o registrarte para una prueba, tu cuenta de **my.anydesk II** se crea automáticamente usando tu dirección de correo electrónico. La cuenta de Administrador te brinda acceso total a todas las configuraciones del portal de gestión, donde puedes llevar a cabo desde la configuración organizativa hasta la gestión de identidades (IDP). Además, tendrás la posibilidad de revisar el historial de sesiones y otros datos.

Te recomendamos usar esta cuenta principalmente para la configuración inicial y luego agregar usuarios, asignándoles permisos adaptados a sus necesidades específicas.

Gestión de Permisos y Usuarios

Al adquirir tu licencia, inicia sesión en el portal de gestión de **my.anydesk II** y comienza a añadir usuarios. Después de añadir a todos los colaboradores, podrás asignar roles que tienen diferentes permisos para cada usuario o para grupos de usuarios en tu licencia.
Cada rol tiene conjuntos de permisos que determinan qué información y acciones pueden realizar los usuarios dentro del portal de gestión. Esto permite no solo aumentar la productividad, sino también mejorar la seguridad al evitar accesos no autorizados.

A continuación, se presentan los roles preconfigurados disponibles para la licencia Ultimate:

Rol	Descripción
Propietario	Rol diseñado para el dueño de la licencia, quien puede ver y editar cada sección del portal de gestión.
Administrador	Permite ver y editar todas las secciones, con algunas excepciones como Licencia y Facturas.
Agente de soporte	Diseñado para el personal de soporte de TI, permite acceso a secciones relacionadas con usuarios y clientes.
Contador	Rol que permite al encargado de manejo de facturas ver las secciones de Organización y Facturas.
Responsable de protección de datos	Permite ver casi todas las secciones del portal, excepto algunas específicas.
Usuario	Rol predeterminado para todos los usuarios, que les permite ver y editar su propio perfil y acceder a algunas secciones.

Tabla de Roles y Permisos

Sección de my.anydesk II	Propietario	Administrador	Agente de soporte	Responsable de protección de datos	Contador	Usuario
Perfil personal	Ver y editar	x	x	x	x	Ver y editar
Licencia	Ver y editar	Ver	x	Ver	Ver	x
Facturas	Ver y editar	Ver	x	Ver	Ver	x
Usuarios	Ver y editar	Ver y editar	Ver	Ver	x	x
Roles	Ver y editar	Ver y editar	x	Ver	x	x
Grupos	Ver y editar	Ver y editar	Ver	Ver	x	x
Conjuntos de permisos	Ver y editar	Ver y editar	x	Ver	x	x
Libretas de direcciones	Ver y editar	Ver y editar	Ver	Ver	x	x
Clientes	Ver y editar	Ver y editar	Ver	Ver	x	Ver
Sesiones	Ver y editar	Ver y editar	x	Ver	x	x
Builds	Ver y editar	Ver y editar	x	x	x	Ver
Organización	Ver y editar	Ver y editar	x	Ver	Ver	x

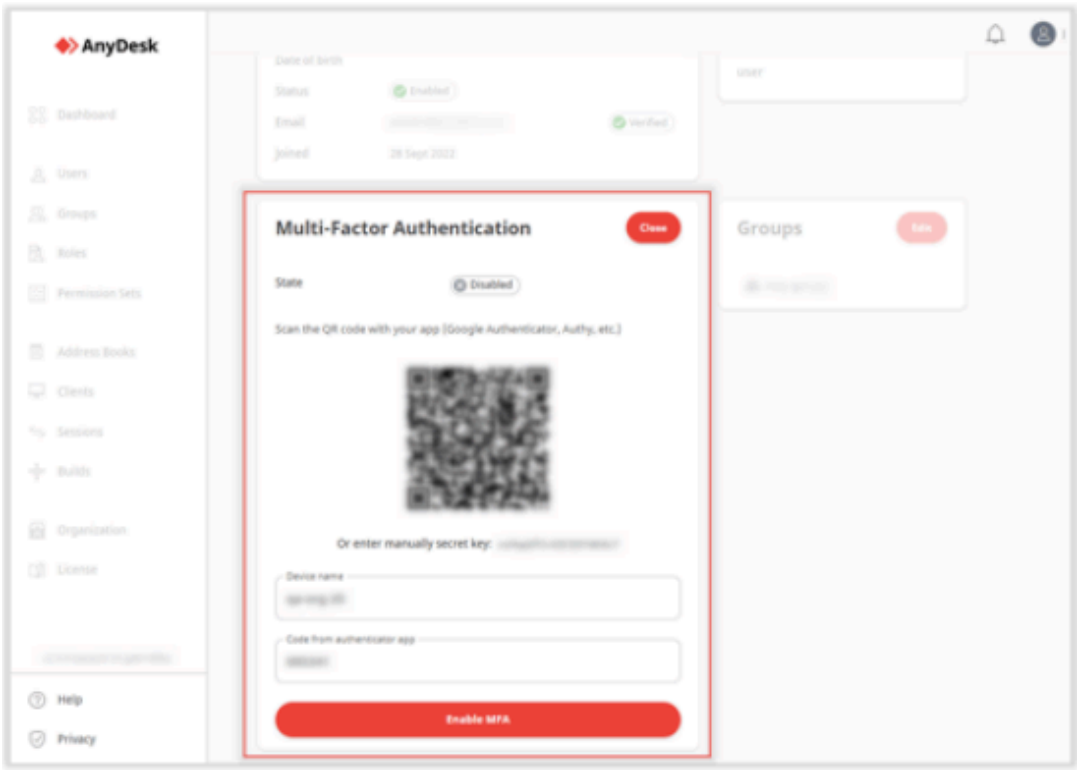
Te sugerimos crear permisos y roles personalizados, otorgando solo los mínimos necesarios. Para más información sobre la gestión de usuarios y roles, consulta los recursos adicionales o la documentación oficial.

Autenticación de Dos Factores para my.anydesk II

Agregar autenticación de dos factores es un excelente enfoque para incrementar la seguridad en tu cuenta de **my.anydesk**. Al iniciar sesión, tendrás que proporcionar tus credenciales y un código de seguridad extra.

Pasos para activar la autenticación de dos factores:

1. Inicia sesión en **my.anydesk II** con tu cuenta de AnyDesk.
2. Haz clic en tu nombre en la esquina superior derecha y selecciona **Mi perfil**.
3. En la sección de **Autenticación multifactor**, haz clic en **Editar**.
4. Abre la app de autenticación en tu dispositivo móvil, escanea el código QR y proporciona un nombre para el dispositivo y el código de la app.



5. Finalmente, haz clic en **Habilitar MFA**.

Cliente Personalizado de AnyDesk

AnyDesk te ofrece opciones para instalar diferentes tipos de clientes en tus dispositivos:

- **Cliente AnyDesk predeterminado**: Esta aplicación viene con configuraciones estándar que están disponibles para todos los usuarios. Puedes descargarla desde nuestro sitio web.
- **Cliente personalizado de AnyDesk**: Permite una personalización total de acuerdo con las necesidades de tu organización, a través del portal de gestión **my.anydesk II**.

Para más información sobre cómo personalizar tu cliente de AnyDesk, visita nuestra página web.

Clientes Solo de Entrada y Solo de Salida

Dependiendo de las funciones requeridas, puedes definir tu cliente de AnyDesk en tres modalidades:

- **Solo de entrada**: Permite conexiones entrantes únicamente.

- **Solo de salida**: Permite solamente iniciar conexiones hacia otros dispositivos.
- **Bidireccional**: Permite tanto conexiones entrantes como salientes.

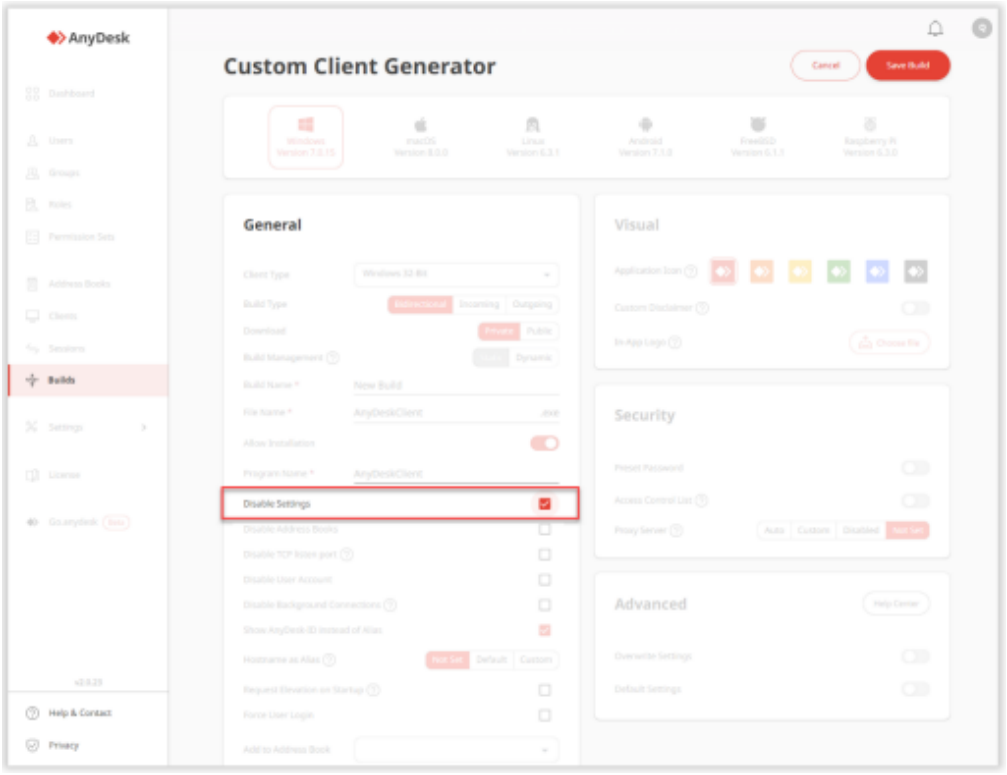
Para un soporte técnico más eficaz, se recomienda que el personal utilice un cliente **solo de salida**, ya que generalmente no necesitan recibir conexiones. En contraste, los empleados que requieren asistencia técnica deberían contar con un cliente **solo de entrada** para garantizar un adecuado nivel de seguridad. Para más detalles, accede a esta página.

Configuraciones

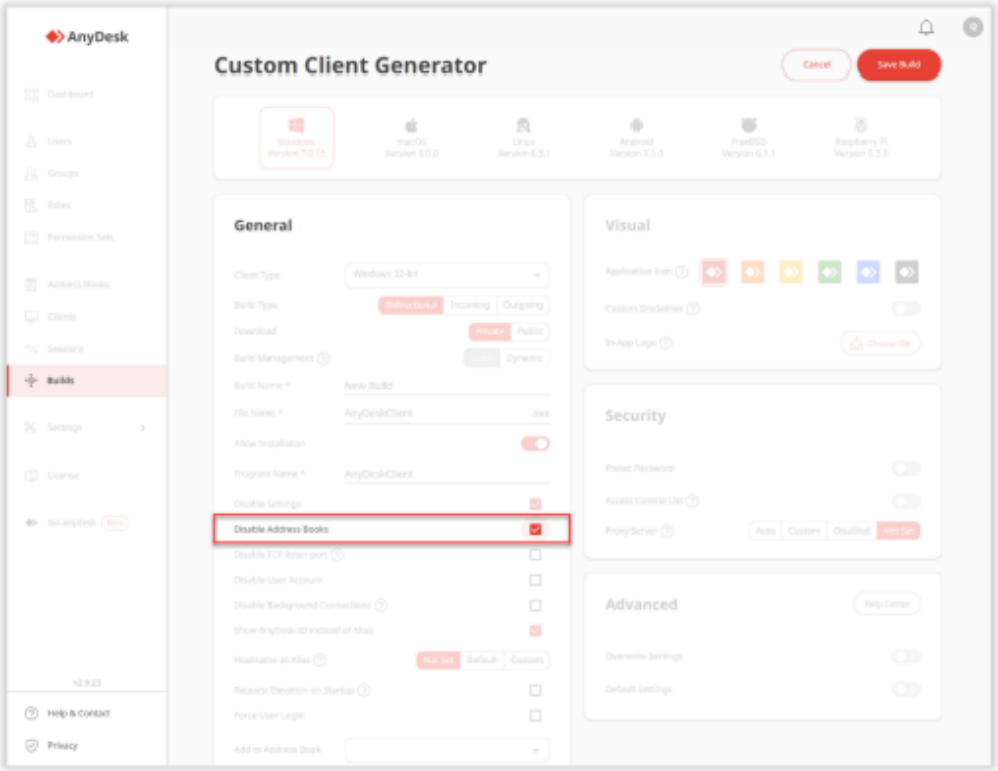
Las configuraciones en el cliente de AnyDesk están protegidas por el **Control de cuentas de usuario (UAC)** y necesitan derechos administrativos para ser modificadas. Sin embargo, puedes establecer preconfiguraciones para evitar que los usuarios realicen cambios indeseados tras la instalación.

Te sugerimos desactivar el acceso a las siguientes secciones en el cliente de AnyDesk:

- **Configuraciones**: Desactiva esta opción ya que no es necesario modificar el cliente una vez instalado, salvo para la configuración de autenticación de dos factores.

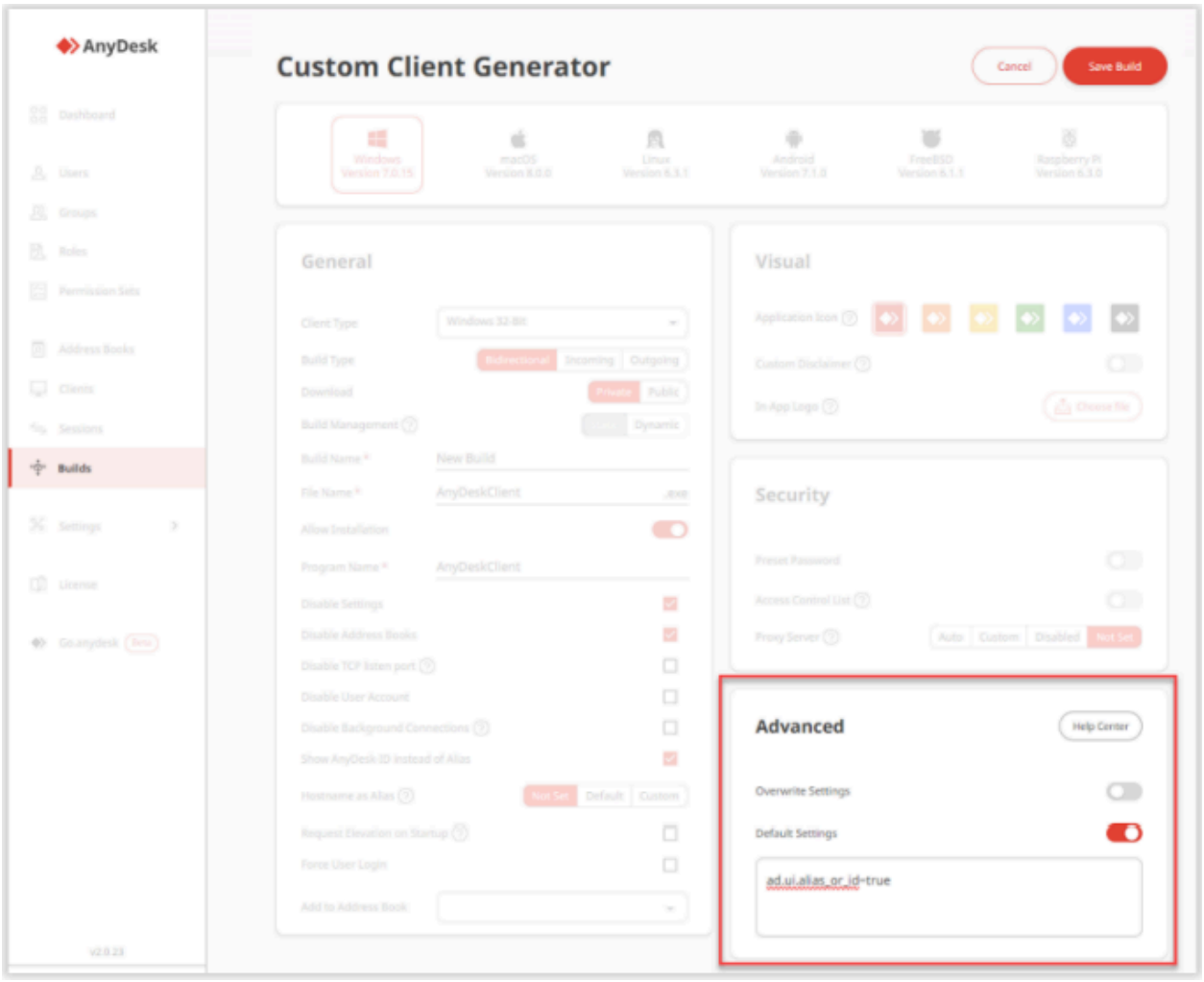


- **Libreta de direcciones para clientes solo de entrada**: Evita la libreta de direcciones en clientes que solo recibirán conexiones.



- **Categorías específicas**: Puedes desactivar funciones específicas del cliente de AnyDesk incluyendo valores clave en la sección Avanzada. Encuentra la lista de todos los valores clave

disponibles aquí.



Lista de Control de Acceso (ACL) y Namespace Personalizado

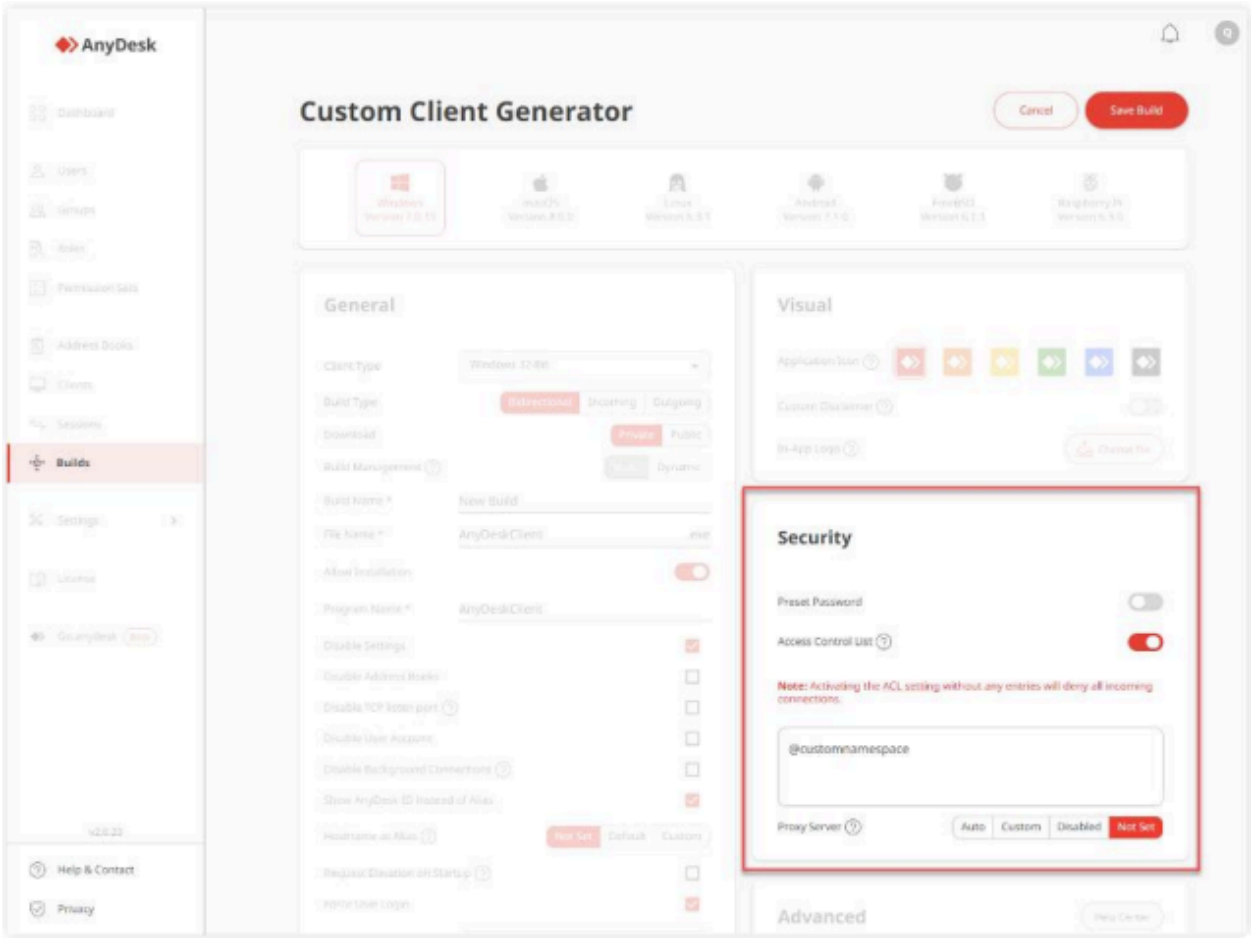
Con la **Lista de Control de Acceso (ACL)**, asegúrate de que tu dispositivo solo reciba conexiones de clientes que estén en la lista blanca. Esta lista debe aplicarse a cualquier cliente de AnyDesk que recibirá conexiones.

Para conectarte a dispositivos remotos a través de AnyDesk, es necesario conocer el ID o Alias del dispositivo. Este Alias consiste en tu nombre de usuario seguido de un Namespace (por ejemplo, **Juan@ad**).

El Namespace predeterminado es **@ad**, utilizado por todos los usuarios. Al activar un Namespace personalizado, puedes especificar un nombre único solo para ti, como **TuNombre@NombreDeEmpresa**, permitiendo así la conexión únicamente a dispositivos registrados bajo este Namespace.

Pasos para Configurar la Lista de Control de Acceso:

1. En el **Generador de Cliente Personalizado**, accede a la sección de **Seguridad** y activa la **Lista de Control de Acceso**.
2. Especifica la lista de clientes que podrán conectarse a este cliente. Puedes incluir solo tu Namespace personalizado para limitar las conexiones a tu organización.

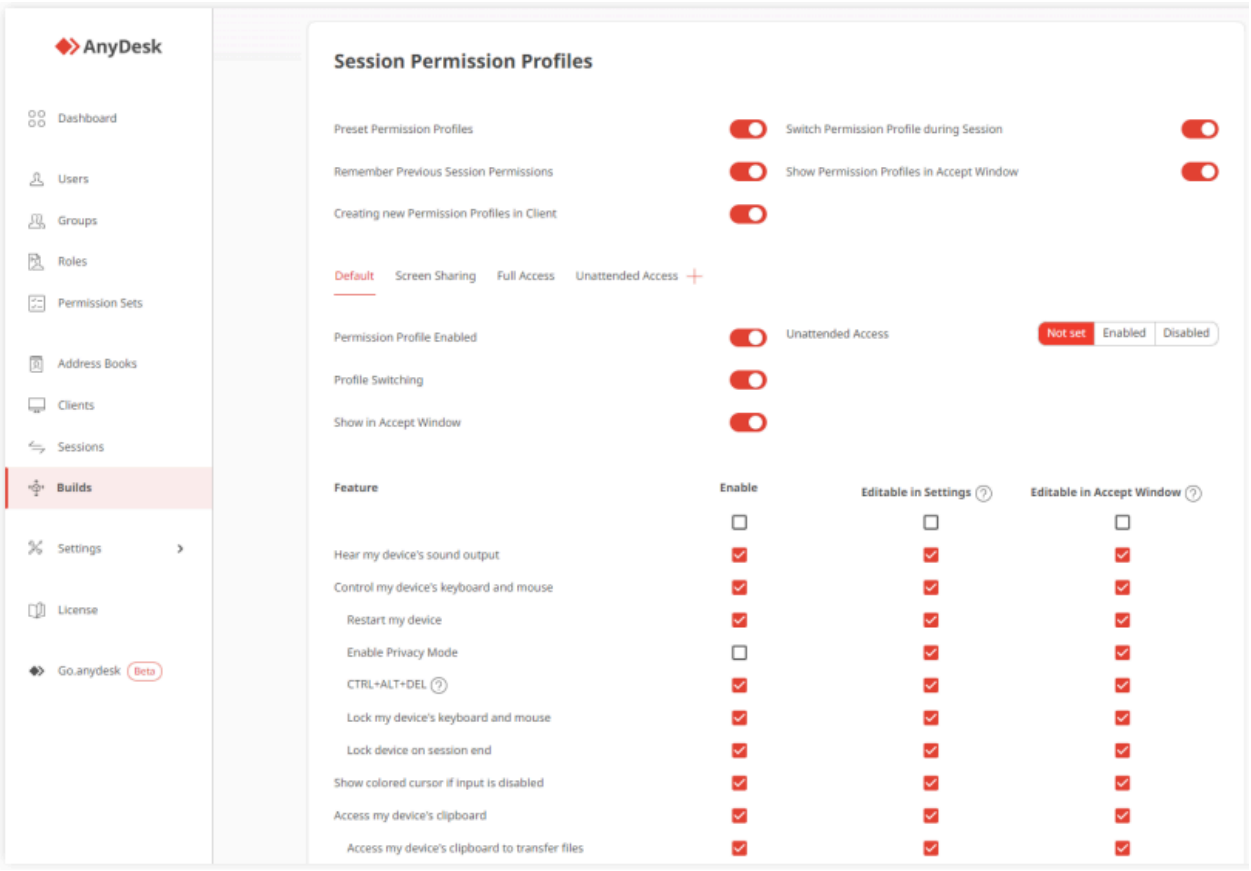


Permisos para la Conexión

Establece controles sobre lo que el usuario que se conecta a tu dispositivo remoto puede acceder.

Para gestionar los permisos de sesión:

- En el **Generador de Cliente Personalizado**, ve a **Perfiles de Permisos de Sesión**.



Perfiles de Permisos

Es recomendable eliminar perfiles existentes que no se ajusten a tus necesidades y crear uno personalizado. Para más información sobre Perfiles de Permisos, visita esta página.

Acceso No Asistido

El **Acceso no atendido** debe usarse solamente en dispositivos controlados o cuando se requiere trabajo remoto. Este acceso es seguro gracias a las contraseñas que puedes configurar, permitiéndote definir múltiples perfiles de permisos. Así, puedes otorgar diferentes niveles de acceso según las necesidades específicas de tu equipo. Consulta esta página para más información sobre el Acceso no atendido.

Autenticación de Dos Factores para Acceso No Asistido

Puedes sumar autenticación de dos factores al Acceso no atendido, garantizando así mayor seguridad. Para conectarte a un dispositivo remoto usando Acceso no atendido, necesitarás ingresar tanto una contraseña como un código de seguridad adicional. Utiliza aplicaciones de autenticación como

Microsoft Authenticator o **Google Authenticator** para configurarlo. Para más información sobre cómo establecer 2FA para Acceso no atendido, revisa esta página.

Forzar Inicio de Sesión de Usuario

Es recomendable habilitar la opción **Forzar inicio de sesión de usuario** para los clientes de AnyDesk. Esto asegura que cada empleado que necesite conectarse remotamente deba iniciar sesión en su cuenta. Si una tercera persona accede al dispositivo con el cliente de AnyDesk, no podrá establecer conexiones no autorizadas. Asegúrate de que todos los empleados que requieran iniciar conexiones tengan su cuenta en **my.anydesk II**.

Caso de Uso

Para ilustrar las configuraciones que hemos mencionado, a continuación se presenta un caso de uso específico para el soporte remoto:

Configuración de AnyDesk para Soporte Remoto

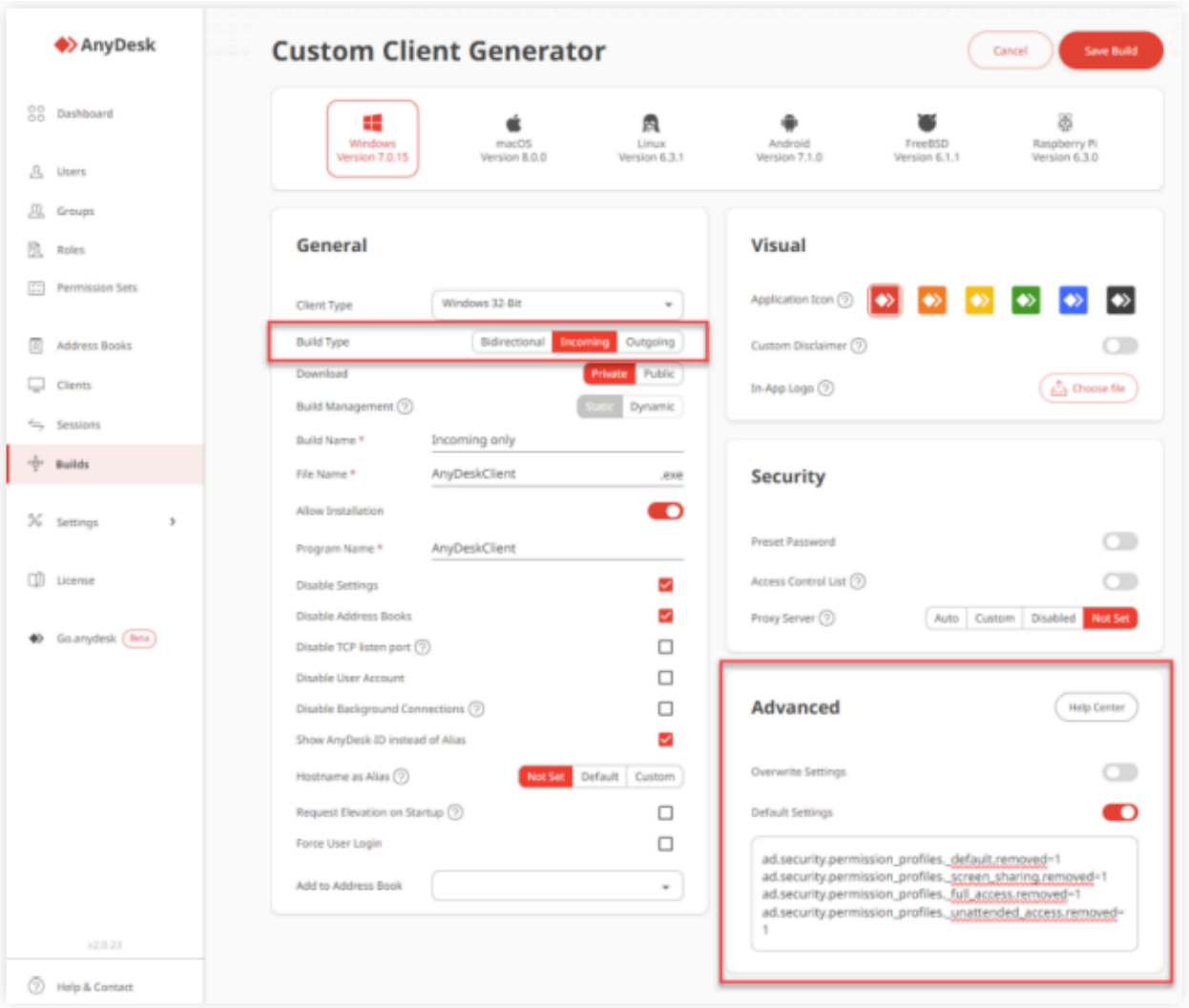
Los requisitos para implementar soporte remoto son los siguientes:

- Cliente de AnyDesk solo de entrada para todos los usuarios finales.
- Cliente de AnyDesk solo de salida para el personal de soporte técnico.
- Cuentas en **my.anydesk II** para todo el personal de soporte técnico.
- Lista de control de acceso con Namespace personalizado.

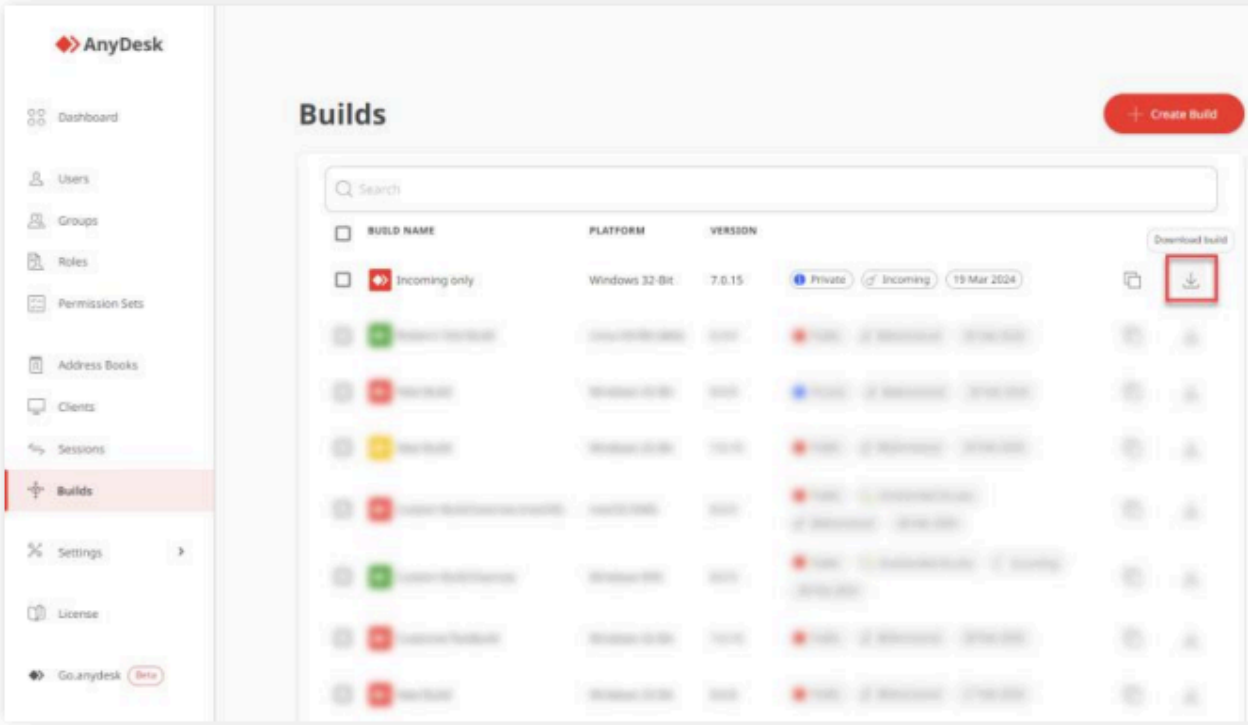
Cliente Solo de Entrada

Para crear un cliente de AnyDesk que solo permita conexiones entrantes:

1. Inicia sesión en **my.anydesk II** y ve a la pestaña **Builds**.
2. Haz clic en **Crear Build** y proporciona los siguientes datos:
    - Selecciona el sistema operativo.
    - En el campo **Tipo de Build**, selecciona **Incoming** (Entrada).
    - En la sección **Avanzada**, elimina los perfiles de permisos preconfigurados con los siguientes valores clave:



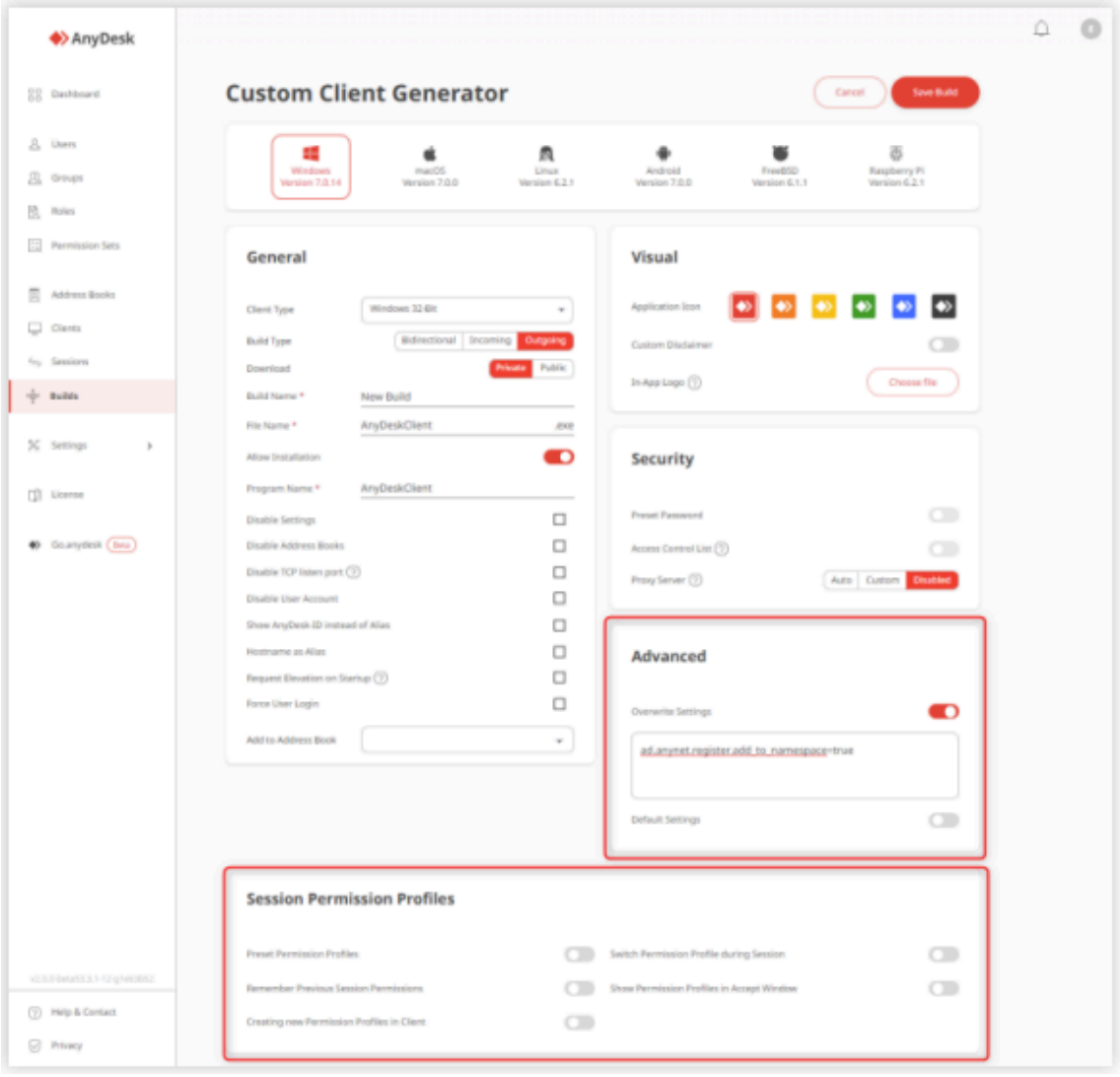
3. Guarda los cambios, descarga la build y instálala en todos los dispositivos de los usuarios finales.



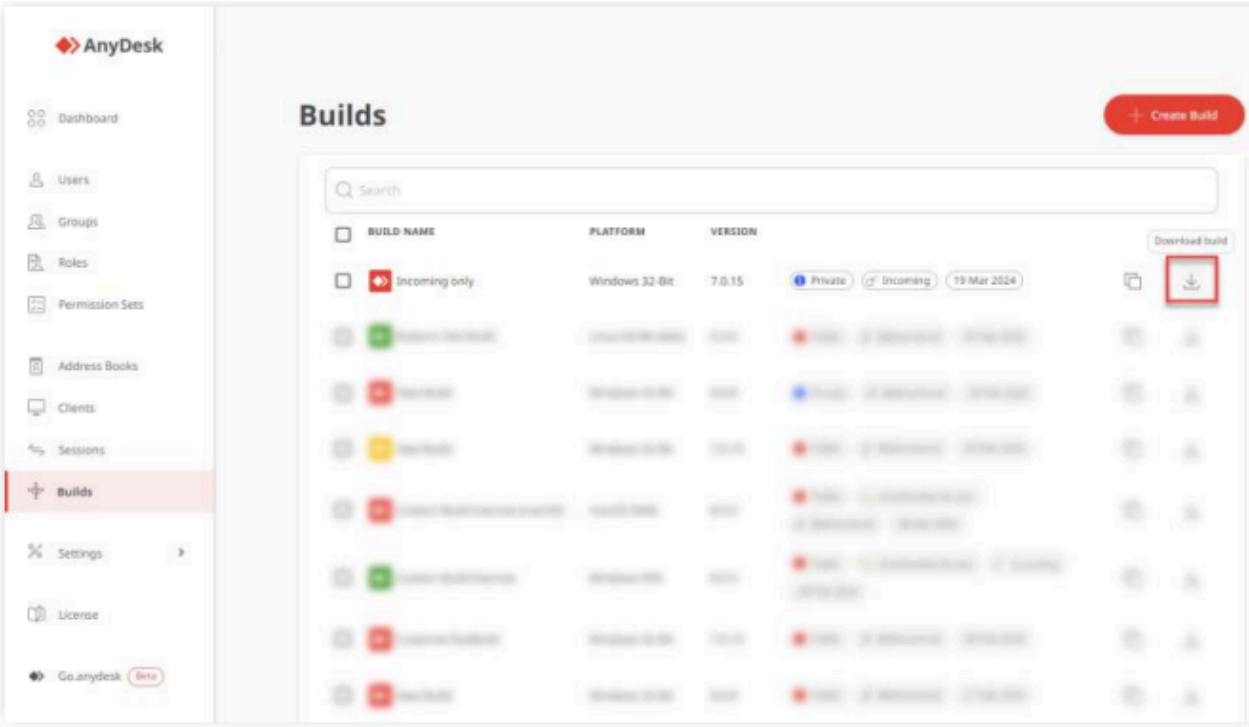
Cliente Solo de Salida

Para crear un cliente de AnyDesk para conexiones salientes:

1. Inicia sesión en **my.anydesk II** y ve a la pestaña **Builds**.
2. Haz clic en **Crear Build** y proporciona los siguientes datos:
    - Selecciona el sistema operativo.
    - En el campo **Tipo de Build**, selecciona **Outgoing** (Salida).
    - Activa la opción **Forzar inicio de sesión de usuario**.
    - En la sección **Avanzada**, agrega este valor clave para el registro automático del Alias en el Namespace personalizado:
    - En **Perfiles de permisos de sesión**, desactiva todos los permisos debido a que no se pueden establecer conexiones entrantes.



3. Guarda los cambios, descarga la build e instálala en todos los dispositivos del personal de soporte técnico.

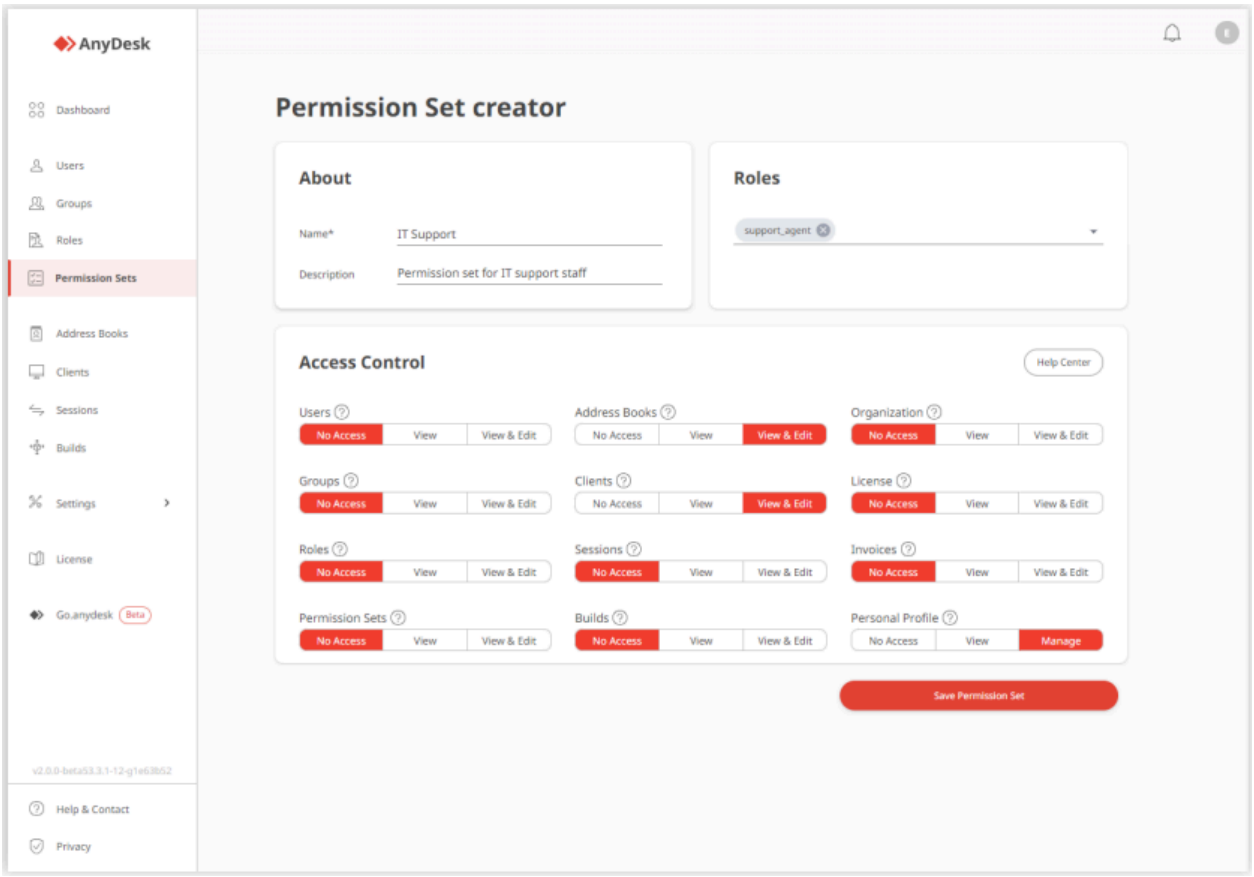


Permisos en my.anydesk II

Los permisos que se otorgan a los usuarios en el portal de gestión **my.anydesk II** deben ajustarse a sus roles específicos. En este caso, el personal de soporte técnico probablemente necesitará un acceso limitado. El administrador o propietario de la licencia puede crear un conjunto de permisos alineado a las funciones del personal de soporte.

En este escenario, el personal de soporte técnico podría tener los siguientes permisos:

- **Ver y editar las Libretas de direcciones.**
- **Ver y editar la lista de clientes** para eliminar un cliente de AnyDesk si un dispositivo es dado de baja.
- **Ver y editar el perfil personal** para habilitar autenticación de dos factores.
- **Ver el historial de sesiones**, así como las notas dejadas por otros colegas para mejorar la atención.



¡No te quedes atrás! Prueba AnyDesk gratis y descubre todos los beneficios que esta herramienta tiene para ofrecerte. Si deseas obtener más información sobre la compra de AnyDesk en México, no dudes en **contactarnos**. Estamos aquí para ayudarte.