AnyDesk: Mejores prácticas de seguridad

TABLA DE CONTENIDO

my.anydesk II

Gestión de permisos y usuarios

Autenticación de dos factores para my.anydesk II

Clientes solo de entrada y solo de salida

- Configuraciones

Lista de control de acceso (ACL) y Namespace personalizado

- Para configurar la Lista de control de acceso:

Permisos para la conexión

- Acceso no atendido
- Autenticación de dos factores para Acceso no atendido
- Forzar inicio de sesión de usuario

Caso de uso

- Configuración de AnyDesk para soporte remoto
- Permisos en my.anydesk II

Esta guía está diseñada tanto para administradores de TI como para usuarios, y ofrece consejos prácticos sobre cómo optimizar la configuración de AnyDesk para una mayor seguridad.
El documento consta de los siguientes capítulos:
• **my.anydesk II** – aprende sobre los roles y permisos básicos que se pueden asignar a los usuarios.
• **Cliente personalizado de AnyDesk** – aprende a configurar clientes personalizados de AnyDesk para hacerlos más seguros.
• **Caso de uso** – revisa el ejemplo de configuración de clientes personalizados de AnyDesk.

my.anydesk II

Cuando compras o te registras para una prueba, tu cuenta de **my.anydesk II** se genera automáticamente utilizando la dirección de correo electrónico registrada. La cuenta de Administrador otorga acceso completo a todas las configuraciones dentro del portal de gestión de **my.anydesk II**, como la configuración de la organización y del Proveedor de Identidad (IDP), además de la capacidad de revisar el historial de sesiones y otros datos.
Se recomienda utilizar esta cuenta solo para el proceso de configuración inicial. Posteriormente, puedes agregar usuarios y otorgarles permisos personalizados según sus requisitos específicos.

Gestión de permisos y usuarios

Después de comprar la licencia, inicia sesión en el portal de gestión de **my.anydesk II** y agrega usuarios a tu licencia. Una vez que hayas agregado a todos los usuarios, puedes asignar roles con diferentes permisos a usuarios individuales o a grupos de usuarios en tu licencia.
Cada rol tiene diferentes conjuntos de permisos que definen qué pueden ver y hacer los usuarios dentro del portal de gestión. Dependiendo del rol que se le asigne al usuario, pueden tener solo visualización, visualización y edición, o ningún acceso a diferentes secciones del portal de gestión de **my.anydesk II**.
Asignar roles a los usuarios te ayuda a mejorar la productividad y la seguridad al reducir la posibilidad de que los usuarios accedan a funciones a las que no deberían tener acceso.

En el portal de gestión de **my.anydesk II**, existen los siguientes roles preconfigurados para la licencia Ultimate:

• **Propietario** - un rol diseñado para el dueño de la licencia. Con este rol, puede ver y editar cada sección del portal de gestión y eliminar la organización.
• **Administrador** - un rol que permite al usuario ver y editar todas las secciones del portal de gestión, excepto la Licencia, Facturas y perfil personal.
• **Agente de soporte** - un rol que permite al usuario ver las secciones de Usuarios, Grupos, Libretas de direcciones y Clientes del portal de gestión de **my.anydesk II**. Está diseñado para el personal de soporte de TI.
• **Contador** - un rol para una persona dentro de tu organización que maneja facturas. El rol otorga acceso únicamente para ver las secciones de Organización, Licencia y Facturas.
• **Responsable de protección de datos** - un rol que permite al usuario ver todas las secciones del portal de gestión de **my.anydesk II**, excepto Builds y perfil personal.
• **Usuario** - el rol predeterminado para cada usuario. Con este rol, pueden ver y editar su perfil personal, así como ver las secciones de Clientes y Builds.

En la siguiente tabla, puedes verificar los roles disponibles para la licencia Ultimate y los permisos que tiene cada rol en las secciones de **my.anydesk II**.

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

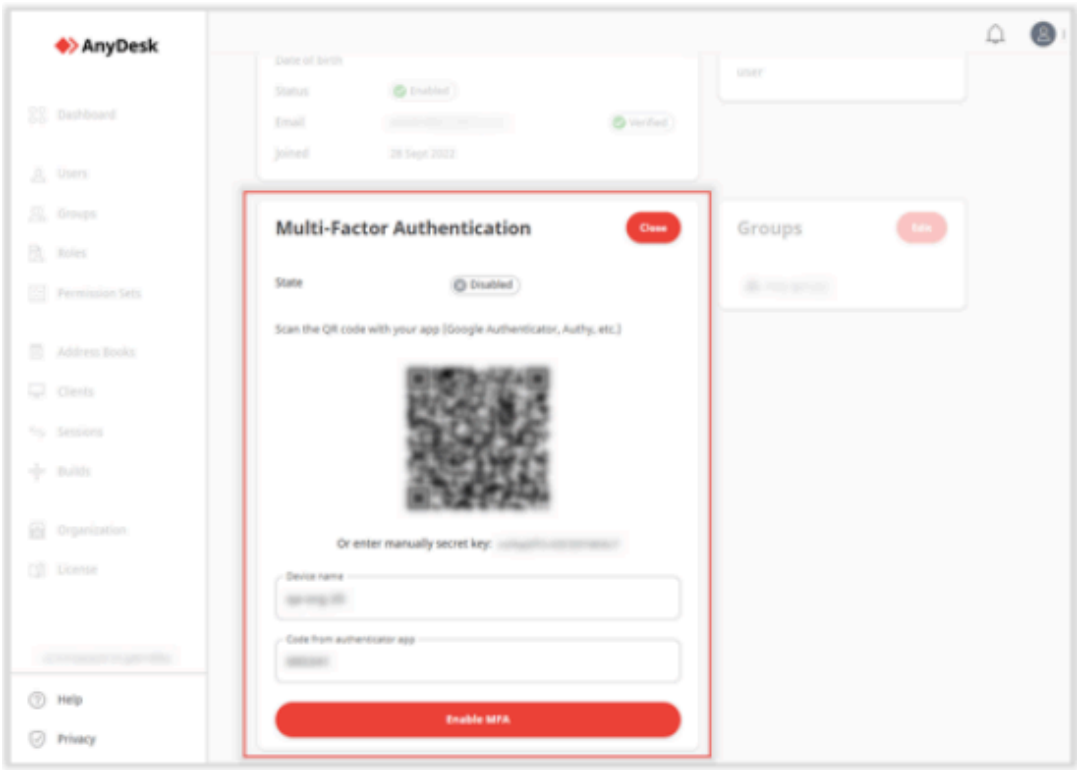
También puedes crear permisos y roles personalizados. Se recomienda otorgar los permisos mínimos necesarios. Para obtener más información sobre la configuración de la gestión de usuarios y roles, puedes consultar los recursos adicionales disponibles o la documentación oficial.

Autenticación de dos factores para my.anydesk II

Puedes añadir una capa adicional de seguridad configurando la autenticación de dos factores para tu cuenta de **my.anydesk**. Al iniciar sesión en tu cuenta, deberás proporcionar tu inicio de sesión, contraseña y un código de seguridad adicional.

Para activar la autenticación de dos factores:

1. Inicia sesión en **my.anydesk II** con las credenciales de tu cuenta de AnyDesk.
2. En la esquina superior derecha de la página, haz clic en tu nombre y luego selecciona **Mi perfil**.
3. En la sección de **Autenticación multifactor**, haz clic en **Editar**.
4. Abre la aplicación de autenticación en tu dispositivo móvil, escanea el código QR y realiza lo siguiente:
   a. Especifica el **Nombre del dispositivo**.
   b. Ingresa el **Código** de la aplicación de autenticación.



5. Haz clic en **Habilitar MFA**.

Cliente personalizado de AnyDesk

AnyDesk ofrece dos tipos de clientes (aplicaciones) que puedes instalar en tus dispositivos:

• **Cliente AnyDesk predeterminado** – una aplicación de AnyDesk con configuraciones y ajustes predeterminados disponibles para todos los usuarios. Puedes descargarla desde nuestro sitio web.

• **Cliente personalizado de AnyDesk** – una aplicación de AnyDesk totalmente personalizada por el usuario en el portal de gestión **my.anydesk II**. Puedes personalizar la configuración y los permisos de la aplicación según tus necesidades.

Para más información sobre cómo personalizar el cliente de AnyDesk, consulta esta página.

Clientes solo de entrada y solo de salida

Dependiendo de las necesidades de los usuarios, puedes configurar tu cliente de AnyDesk en una de las siguientes opciones:
• **Solo de entrada** – un cliente que solo puede recibir conexiones desde otro dispositivo.
• **Solo de salida** – un cliente desde el cual solo puedes iniciar una conexión saliente.
• **Bidireccional** – un cliente desde el cual puedes crear conexiones hacia otro dispositivo y recibir solicitudes de conexión entrantes en tu dispositivo.

Para optimizar el proceso de soporte técnico, administradores y otros empleados que usan AnyDesk para conexiones de dispositivos, se recomienda configurar clientes AnyDesk solo de salida. Este enfoque es especialmente beneficioso porque el personal de soporte técnico generalmente no requiere conexiones entrantes desde fuentes externas. Como solo necesitan conectarse a los dispositivos de los empleados, esto previene solicitudes de conexión entrantes, lo que hace el proceso más seguro y eficiente.

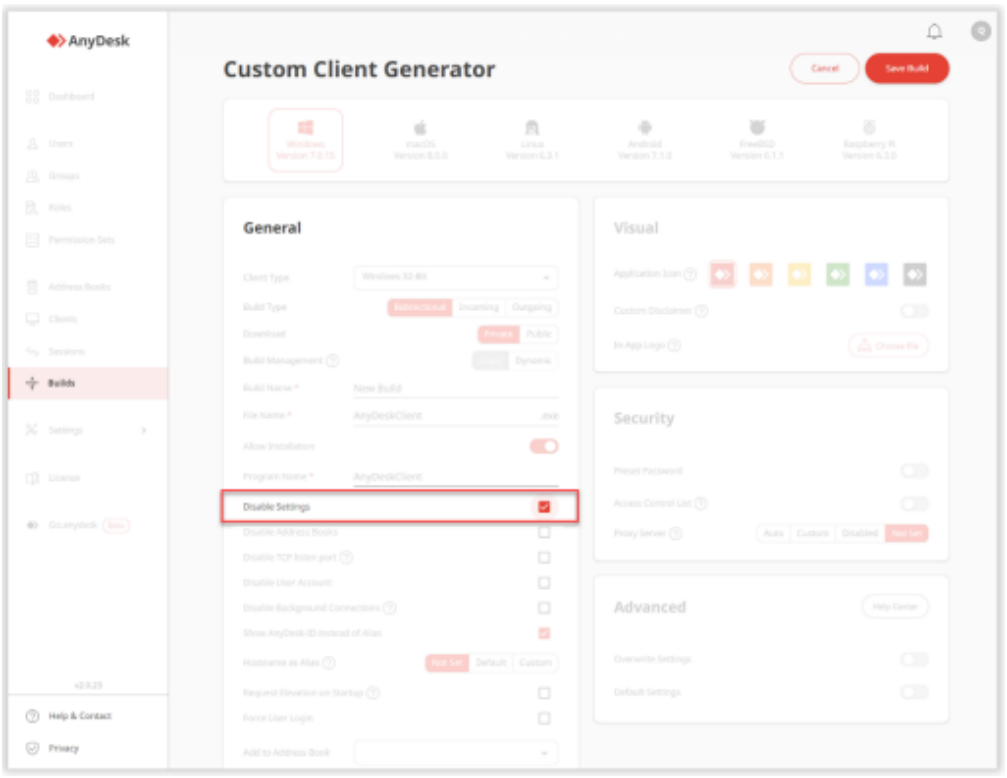
Por el contrario, los empleados que reciben soporte deben tener un cliente AnyDesk solo de entrada. De esta manera, se asegura que no se pueda establecer una conexión desde los dispositivos de los empleados. Para más información, consulta esta página.

Configuraciones

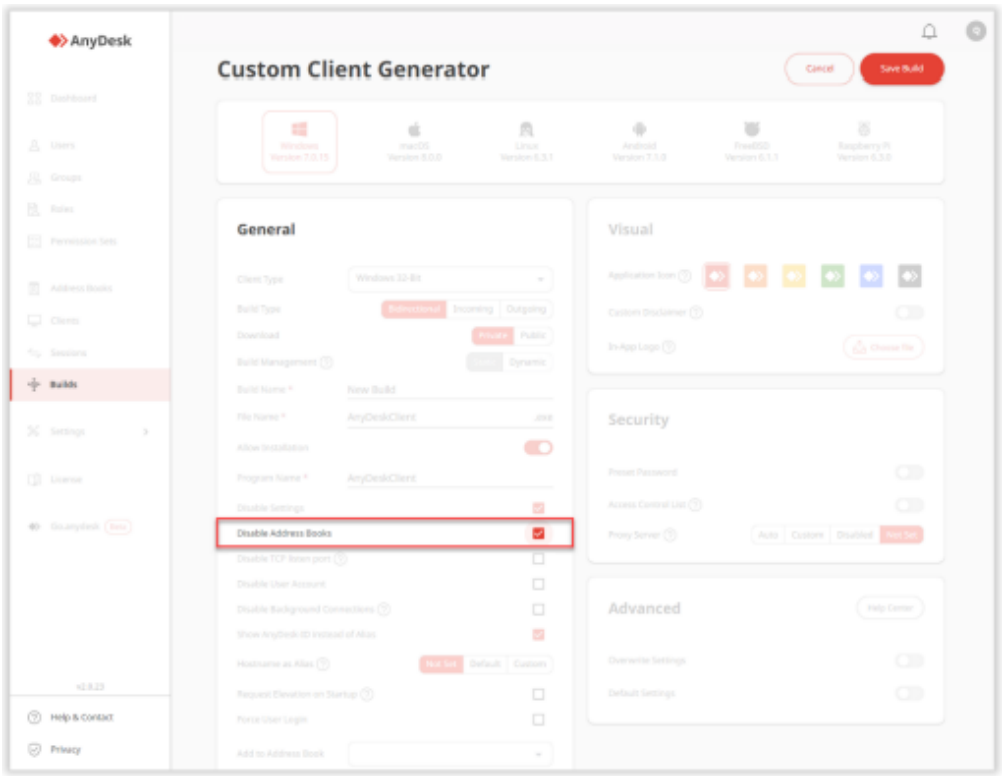
Las configuraciones de seguridad y de conexión en el cliente de AnyDesk están protegidas por el **Control de cuentas de usuario (UAC)** y requieren derechos administrativos para ser modificadas. Sin embargo, puedes preconfigurarlas y bloquearlas para que el usuario no pueda cambiar ninguna configuración dentro del cliente de AnyDesk después de la instalación.

Al crear un cliente personalizado de AnyDesk en el portal de gestión **my.anydesk II**, se recomienda desactivar el acceso a las siguientes secciones del cliente de AnyDesk:
• **Configuraciones**. Se recomienda desactivar el acceso a la configuración en el cliente, ya que no es necesario modificar el cliente de AnyDesk una vez instalado, salvo que se configure la autenticación de

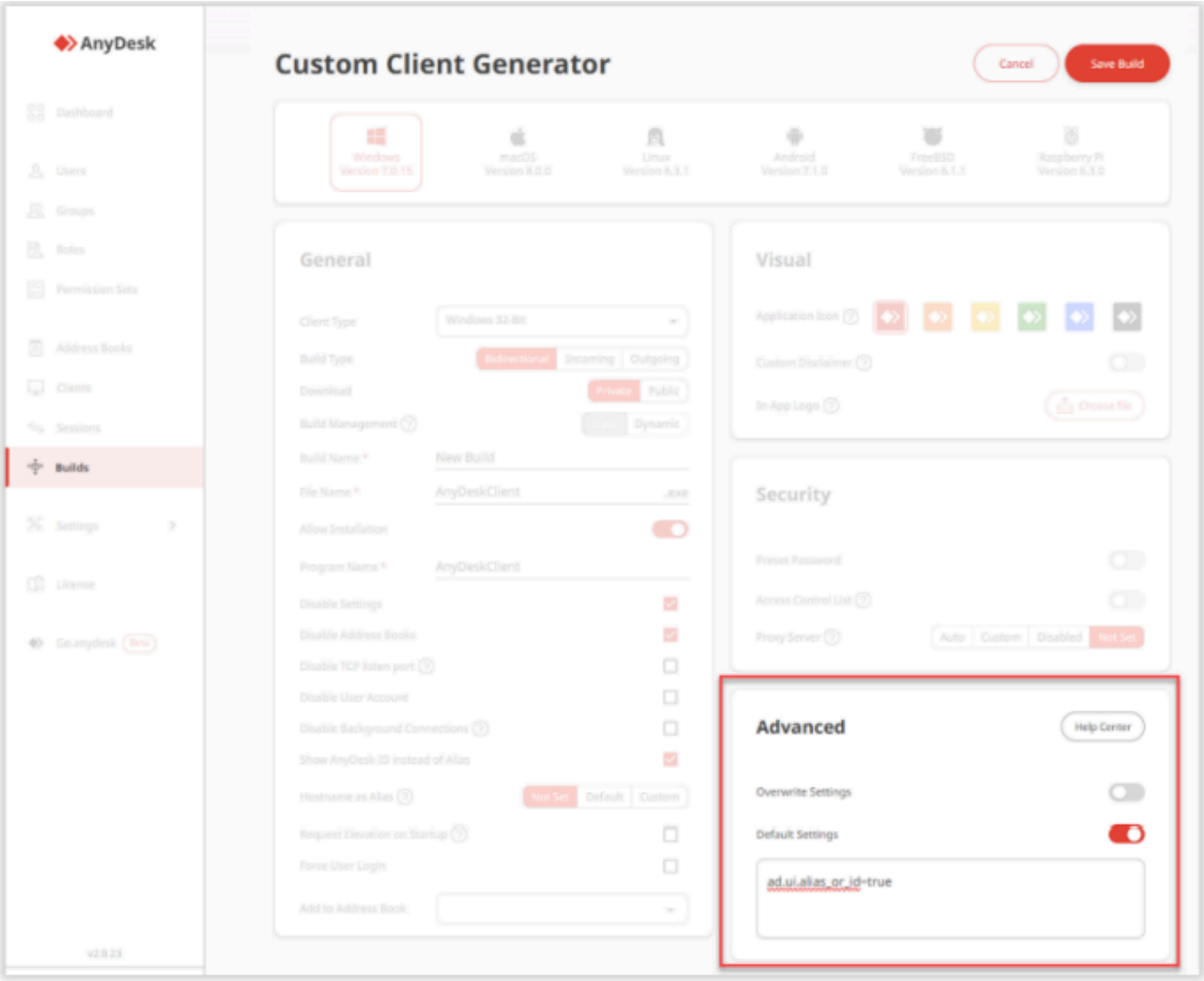
dos factores.



• **Libreta de direcciones para clientes solo de entrada.** Desactiva la libreta de direcciones para los clientes que se instalarán en dispositivos que solo recibirán conexiones.



• **Categorías específicas**. Puedes desactivar funciones o secciones específicas del cliente de AnyDesk agregando valores clave en la sección Avanzada. Puedes encontrar una lista de todos los valores clave disponibles aquí.



Lista de control de acceso (ACL) y Namespace personalizado

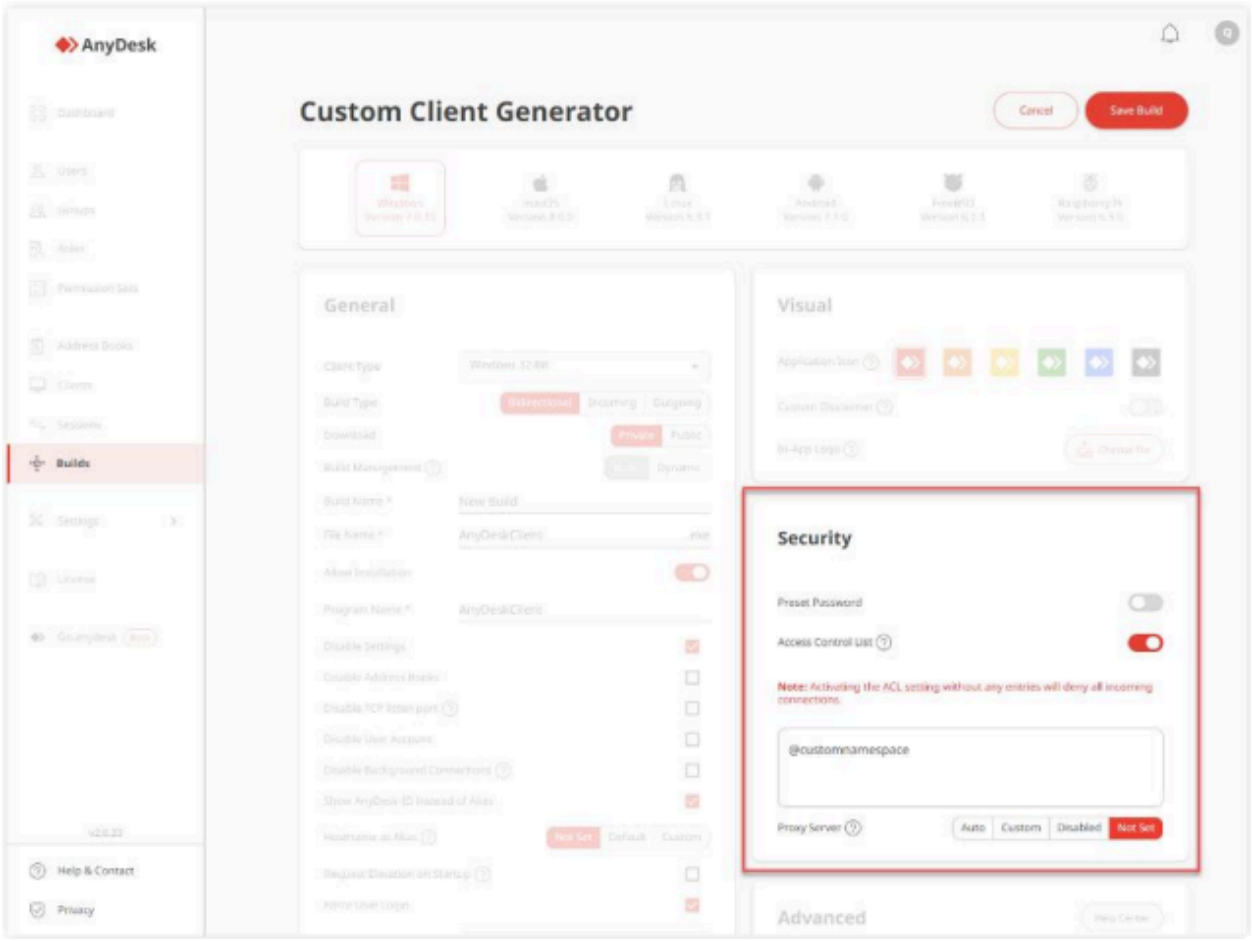
Con la **Lista de control de acceso (ACL)**, puedes asegurarte de que el dispositivo solo reciba solicitudes de conexión de clientes de AnyDesk que estén en la lista blanca. La **Lista de control de acceso** debe aplicarse a cualquier cliente de AnyDesk que vaya a recibir conexiones.

Para conectarte a dispositivos remotos con AnyDesk, necesitas conocer el ID o Alias (Dirección AnyDesk) del dispositivo remoto. El Alias de AnyDesk se compone del nombre de usuario de tu dispositivo y un Namespace, por ejemplo, **John@ad**.
El Namespace predeterminado es **@ad**, que hace referencia a AnyDesk, y se asigna a todos los usuarios que han instalado la aplicación de AnyDesk. **AnyDesk portable** (no instalado) solo tiene un ID.

La opción de Namespace personalizado te permite especificar un nombre individual disponible solo para ti, por ejemplo, **TuNombre@NombreDeEmpresa**. Tener un Namespace personalizado te permite agregar a la lista blanca todo el Namespace con un comodín (*@namespace).
Tu dominio personal de AnyDesk mejora la identificación de dispositivos y la seguridad. Puedes incluir el Namespace personalizado en la configuración de la **Lista de control de acceso** y solo los dispositivos registrados en tu Namespace podrán conectarse a ti.

Para configurar la Lista de control de acceso:

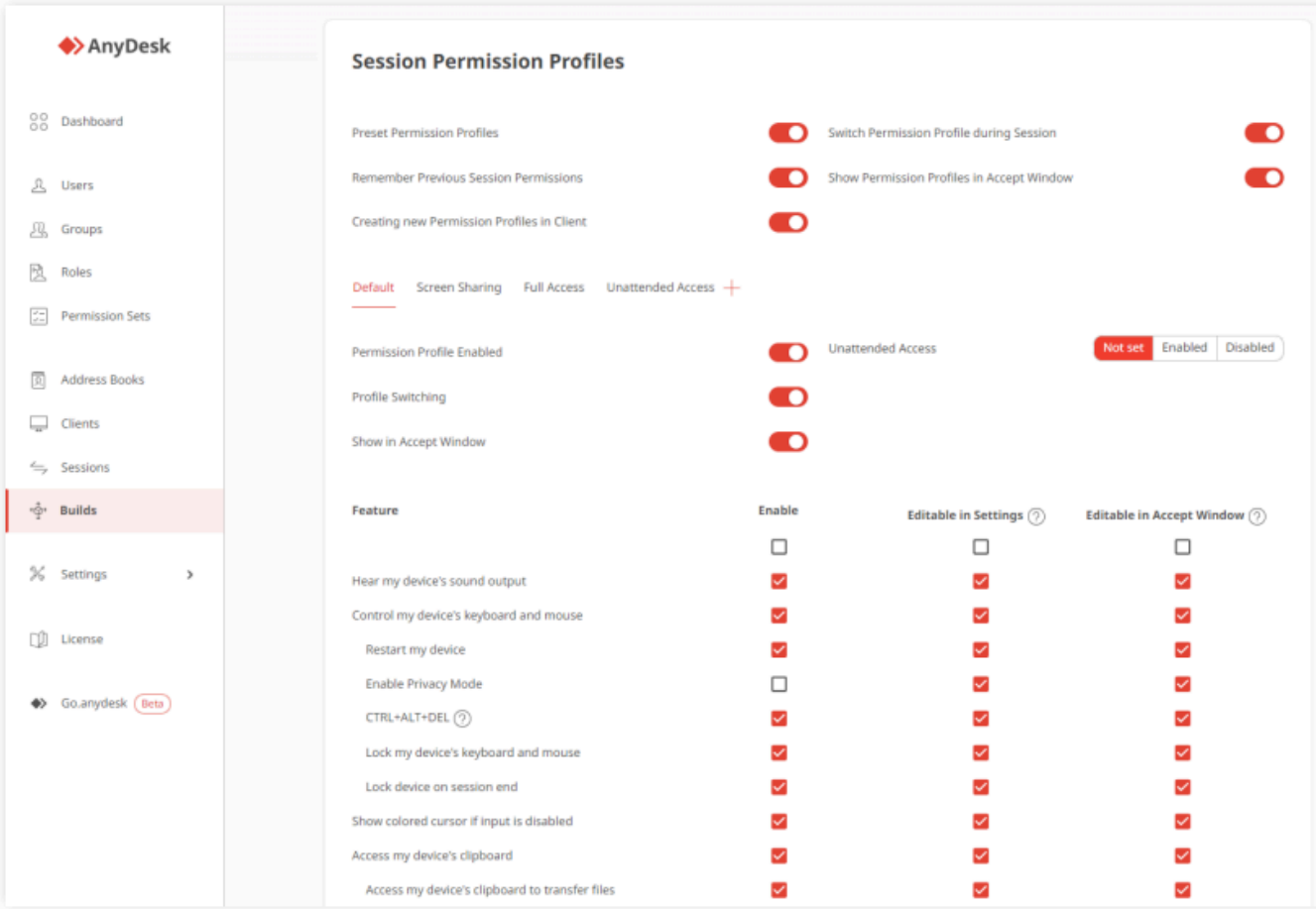
1. En el **Generador de cliente personalizado**, ve a la sección de **Seguridad** y activa el interruptor de la **Lista de control de acceso**.
2. En el campo de texto, proporciona la lista de clientes que tienen permitido conectarse a este cliente personalizado. Puedes incluir solo tu Namespace personalizado (por ejemplo, **@nombredeempresa**) y solo los usuarios dentro de tu organización podrán solicitar una conexión.



Permisos para la conexión

Puedes controlar lo que el usuario que se conecta al dispositivo remoto puede acceder en el dispositivo remoto.

Para gestionar los permisos de sesión:
• En el **Generador de cliente personalizado**, ve a **Perfiles de permisos de sesión**.



Los perfiles se configuran para el cliente de AnyDesk en el dispositivo remoto, no para el cliente de AnyDesk que se usa para conectarse.

Perfiles de permisos

Se recomienda eliminar todos los perfiles existentes y configurar uno personalizado si ninguno de los perfiles preestablecidos se ajusta a las necesidades. Para más información sobre los Perfiles de Permisos, consulta esta página.

Acceso no atendido

El **Acceso no atendido** solo debe concederse para dispositivos que estén monitoreados o si el caso de uso es trabajo remoto / oficina en casa para conectarse mediante una contraseña.
Las contraseñas para el Acceso no atendido se configuran en base a perfiles de permisos, lo que

permite crear múltiples perfiles de permisos con diferentes contraseñas para otorgar diferentes niveles de acceso y permisos según las necesidades del personal que se conecta. Para más información sobre el Acceso no atendido, consulta esta página.

Autenticación de dos factores para Acceso no atendido

Se puede añadir autenticación de dos factores al Acceso no atendido para asegurar el acceso mediante contraseña. Al conectarse al dispositivo remoto usando Acceso no atendido, se te pedirá que proporciones una contraseña de Acceso no atendido y un código de seguridad adicional.
Para configurar 2FA, puedes usar cualquier aplicación de autenticación común como **Microsoft Authenticator** o **Google Authenticator**. La configuración debe realizarse localmente en **Configuración** del cliente de AnyDesk. Para más información sobre cómo configurar 2FA para Acceso no atendido, consulta esta página.

Forzar inicio de sesión de usuario

Se recomienda habilitar la opción **Forzar inicio de sesión de usuario** para los clientes de AnyDesk que se utilizarán para crear conexiones a dispositivos remotos. Esta función asegura que cada empleado que necesite establecer conexiones remotas deberá iniciar sesión en su cuenta en el cliente de AnyDesk. Si una persona no autorizada obtiene acceso a un dispositivo con el cliente de AnyDesk, no podrá conectarse a otros dispositivos en este caso.
Para utilizar esta funcionalidad, todos los empleados que deban iniciar conexiones deben tener una cuenta en **my.anydesk II**.

Caso de uso

Para demostrar posibles configuraciones con las opciones mencionadas anteriormente, consulta el caso de uso de soporte remoto a continuación.

Configuración de AnyDesk para soporte remoto

Los requisitos para el caso de uso de 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.

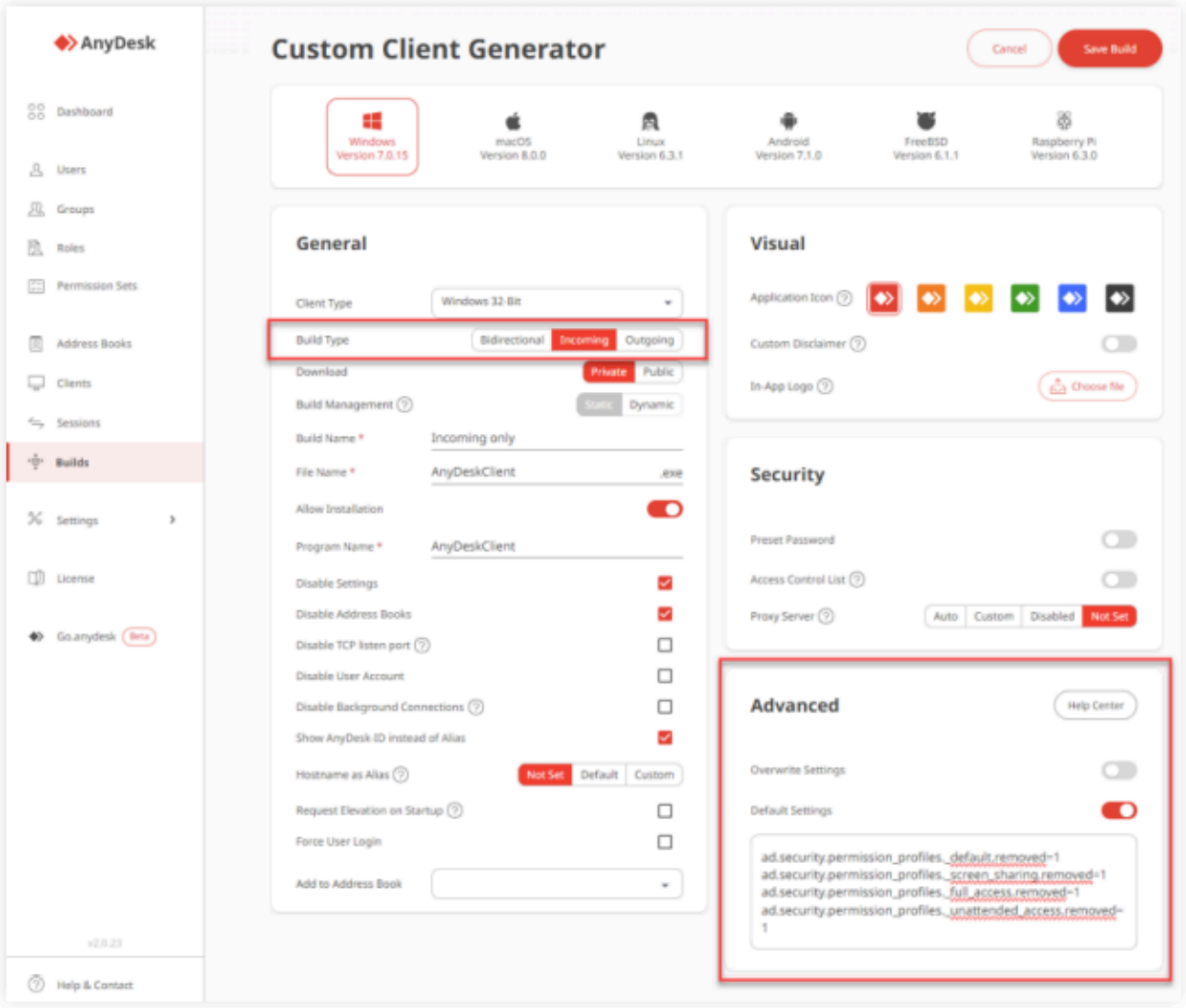
Cliente solo de entrada

Para crear un cliente de AnyDesk solo de entrada:

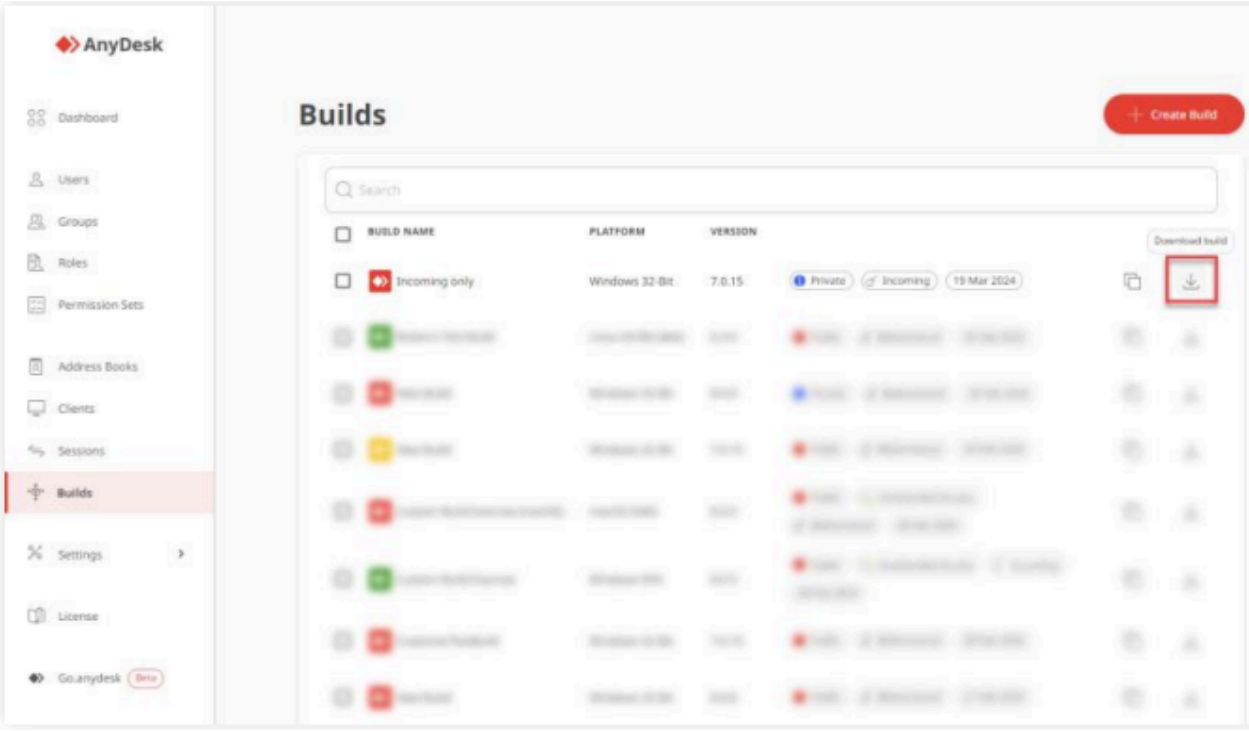
1. Inicia sesión en **my.anydesk II** y ve a la pestaña **Builds**.

2. Haz clic en **Crear Build** y proporciona la siguiente información:
   a. Selecciona el sistema operativo.
   b. En el campo **Tipo de Build**, selecciona **Incoming** (Entrada).
   c. En la sección **Avanzada**, elimina los perfiles de permisos preconfigurados añadiendo los siguientes valores clave:

   ad.security.permission_profiles._default.removed=1
   ad.security.permission_profiles._screen_sharing.removed=1
   ad.security.permission_profiles._full_access.removed=1
   ad.security.permission_profiles._unattended_access.removed=1



3. Haz clic en **Guardar**, descarga la build e instálala en todos los dispositivos de los usuarios finales.

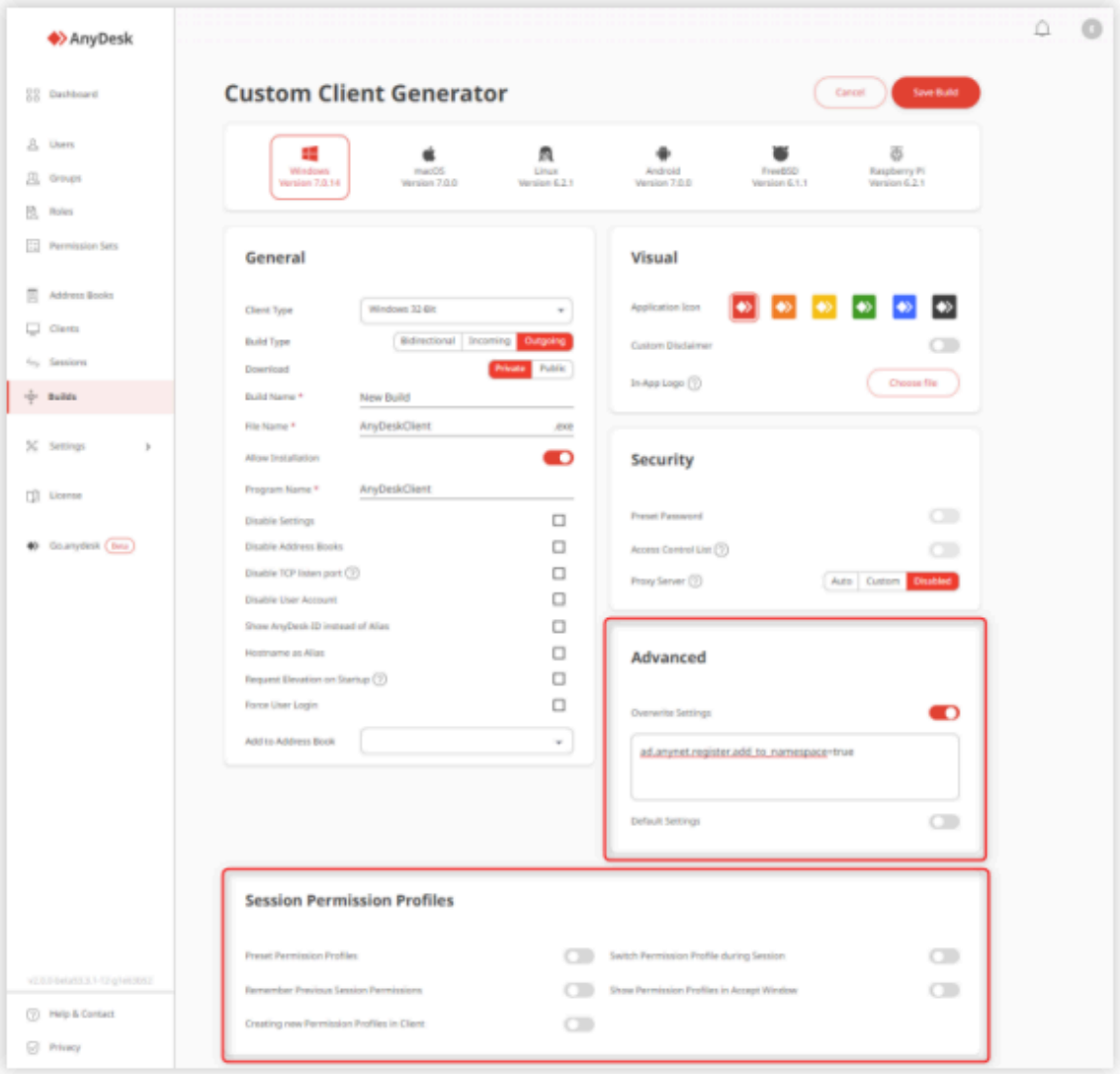


Cliente solo de salida

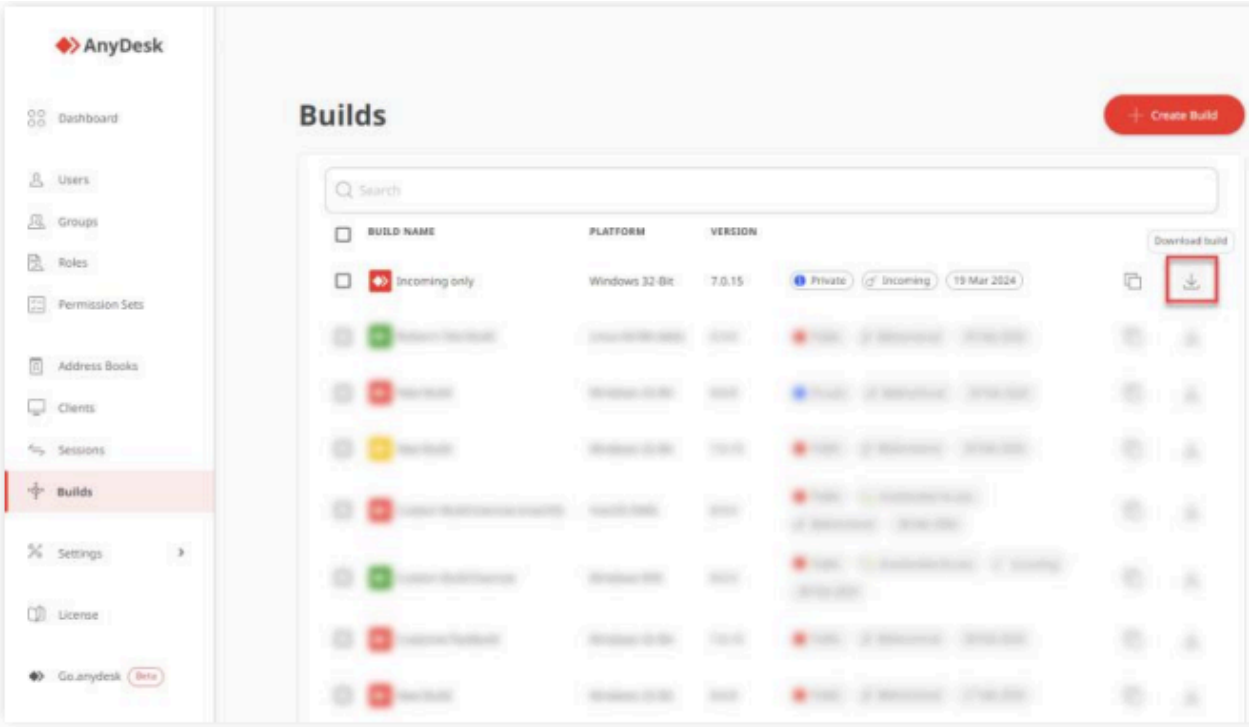
Para crear un cliente de AnyDesk solo de salida:

1. Inicia sesión en **my.anydesk II** y ve a la pestaña **Builds**.
2. Haz clic en **Crear Build** y proporciona la siguiente información:
   a. Selecciona el sistema operativo.
   b. En el campo **Tipo de Build**, selecciona **Outgoing** (Salida).
   c. Marca la casilla **Forzar inicio de sesión de usuario**.
   d. En la sección **Avanzada**, agrega el siguiente valor clave para el registro automático del Alias en el Namespace personalizado.
   ad.anynet.register.add_to_namespace=true e. En **Perfiles de permisos de sesión**, desactiva

todos los permisos ya que no se pueden establecer conexiones entrantes.



3. Haz clic en **Guardar**, descarga la build e instálala en todos los dispositivos del personal de soporte técnico.



Permisos en my.anydesk II

Los permisos otorgados a los usuarios en el portal de gestión **my.anydesk II** varían según las responsabilidades de los empleados. En este caso, asumimos que el personal de soporte técnico debería tener un acceso mínimo al portal de gestión **my.anydesk II**, ya que su principal uso de AnyDesk es para conectarse de forma remota a los dispositivos de los usuarios finales.

El administrador o el propietario de la licencia puede crear un conjunto de permisos específico y asignarlo al personal de soporte técnico. Como resultado, el personal de soporte técnico puede tener los siguientes permisos en el portal de gestión **my.anydesk II**:

• **Ver y editar las Libretas de direcciones.**
• **Ver y editar la lista de clientes** para poder eliminar un cliente de AnyDesk de la licencia en caso de que un dispositivo sea dado de baja, por ejemplo.
• **Ver y editar el perfil personal** para poder configurar la autenticación de dos factores para la cuenta.

• **Ver el historial de sesiones**, aprovechando, por ejemplo, las notas de sesión dejadas por colegas.

