# Guia de Hardening de AnyDesk para Empresas

TABLA DE CONTENIDO

Principio de mínimo privilegio en el cliente
- Controla quién puede conectar: Access Control List (ACL)
- Define qué puede hacer quien se conecta: perfiles de permisos
- Asegura el acceso no atendido
- Controla el acceso interactivo
- Bloquea la configuración del cliente

Despliegue seguro con clientes personalizados
- Qué preconfigurar en el Build
- Distribución controlada
- Windows Group Policy

Gestión centralizada desde my.anydesk II
- Central Management y la clave privada
- Roles y Permission Sets (RBAC)
- Protege el acceso al portal

Monitorización y auditoría

Endurecimiento a nivel de red
- Firewall y dominios
- On-Premises para máximo control

Offboarding y ciclo de vida

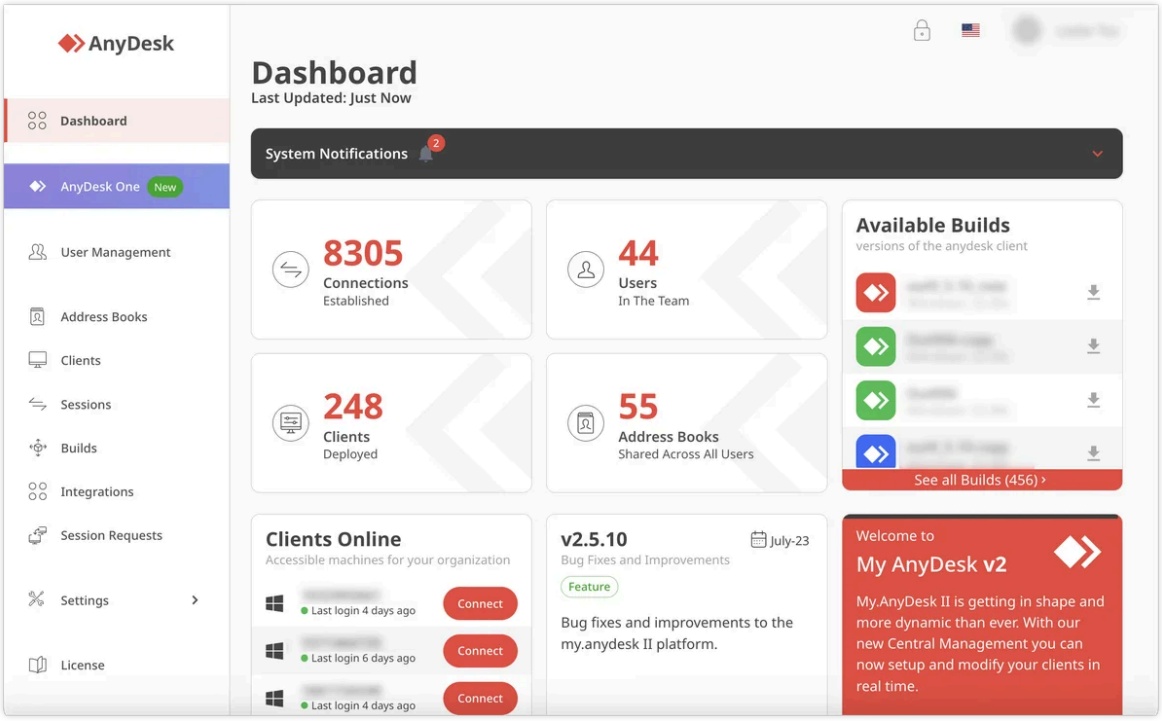
Checklist de hardening

Aviso legal

*Articulo elaborado por el equipo de investigaciones de ayuda.licencia.co.*

El hardening es el proceso de reducir la superficie de ataque de una herramienta configurándola con el mínimo privilegio necesario y bloqueando todo lo que no se usa. AnyDesk es seguro por diseño — TLS 1.2 con AEAD, identidad criptográfica por dispositivo, aceptación manual por defecto— pero su postura real de seguridad depende de cómo lo despliegues y lo bloquees.

Esta guía reúne las medidas de endurecimiento que puedes aplicar en el cliente, en el despliegue y desde el portal de gestión my.anydesk II, para dejar AnyDesk listo para un entorno empresarial exigente.




Panel de control de my.anydesk II con información de conexiones, usuarios y clientes

## Principio de mínimo privilegio en el cliente

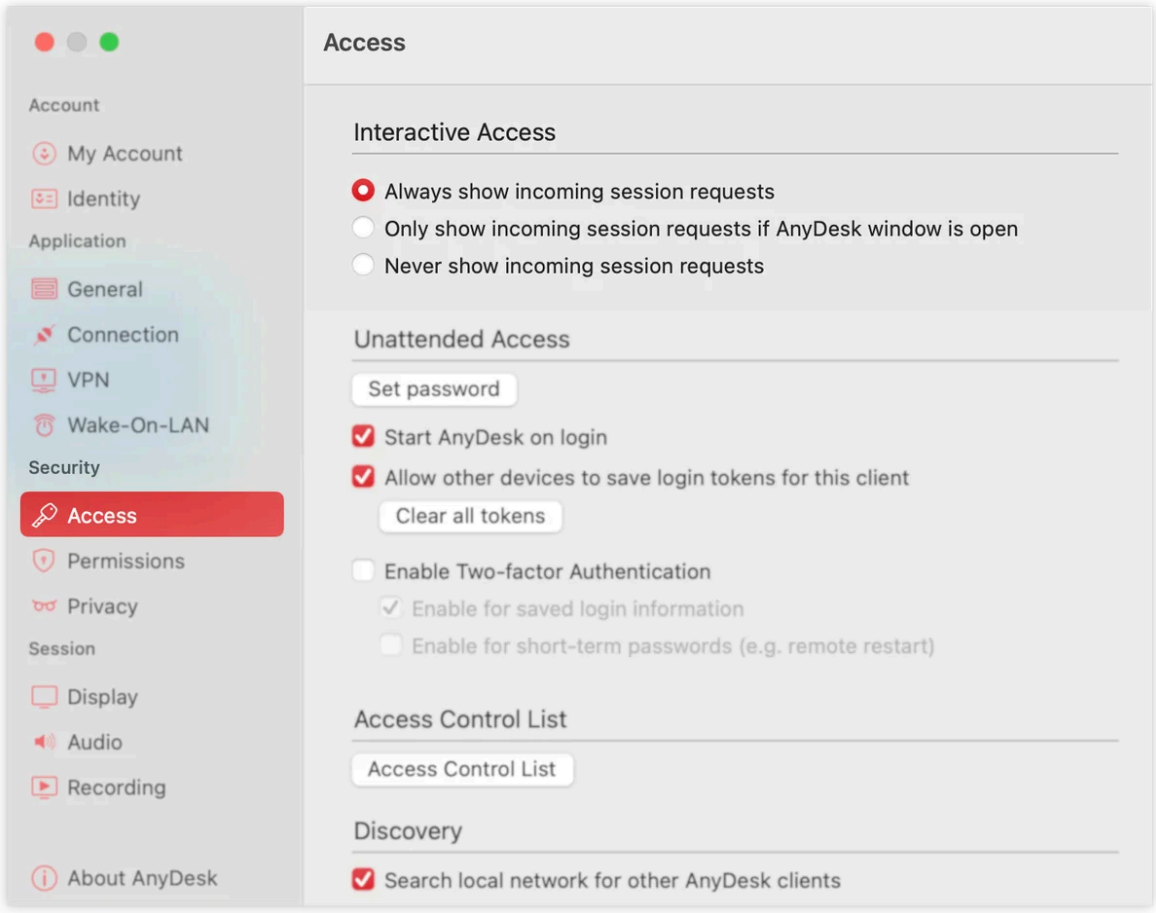
La primera línea de defensa está en el propio cliente. Todo lo que no necesites, desactívalo; todo lo que necesites, restríngelo.

### Controla quién puede conectar: Access Control List (ACL)

La **ACL** es la medida de hardening más efectiva: define qué AnyDesk-IDs o alias pueden siquiera iniciar una conexión hacia tu equipo. Aunque alguien conozca tu contraseña, no podrá conectar si su ID no está en la lista.

- En el cliente: *Settings* > *Security* > *Access Control List* y agrega solo los IDs o alias de confianza.

- La ACL soporta comodines. Con un **namespace personalizado** puedes permitir solo tu organización: `*@tuempresa`.
- En un custom client se define con `ad.security.acl_enabled=true` y `ad.security.acl_list=<ID>:true; <alias>:true`.




Configuración de acceso de AnyDesk con acceso interactivo, acceso no atendido y lista de control de acceso

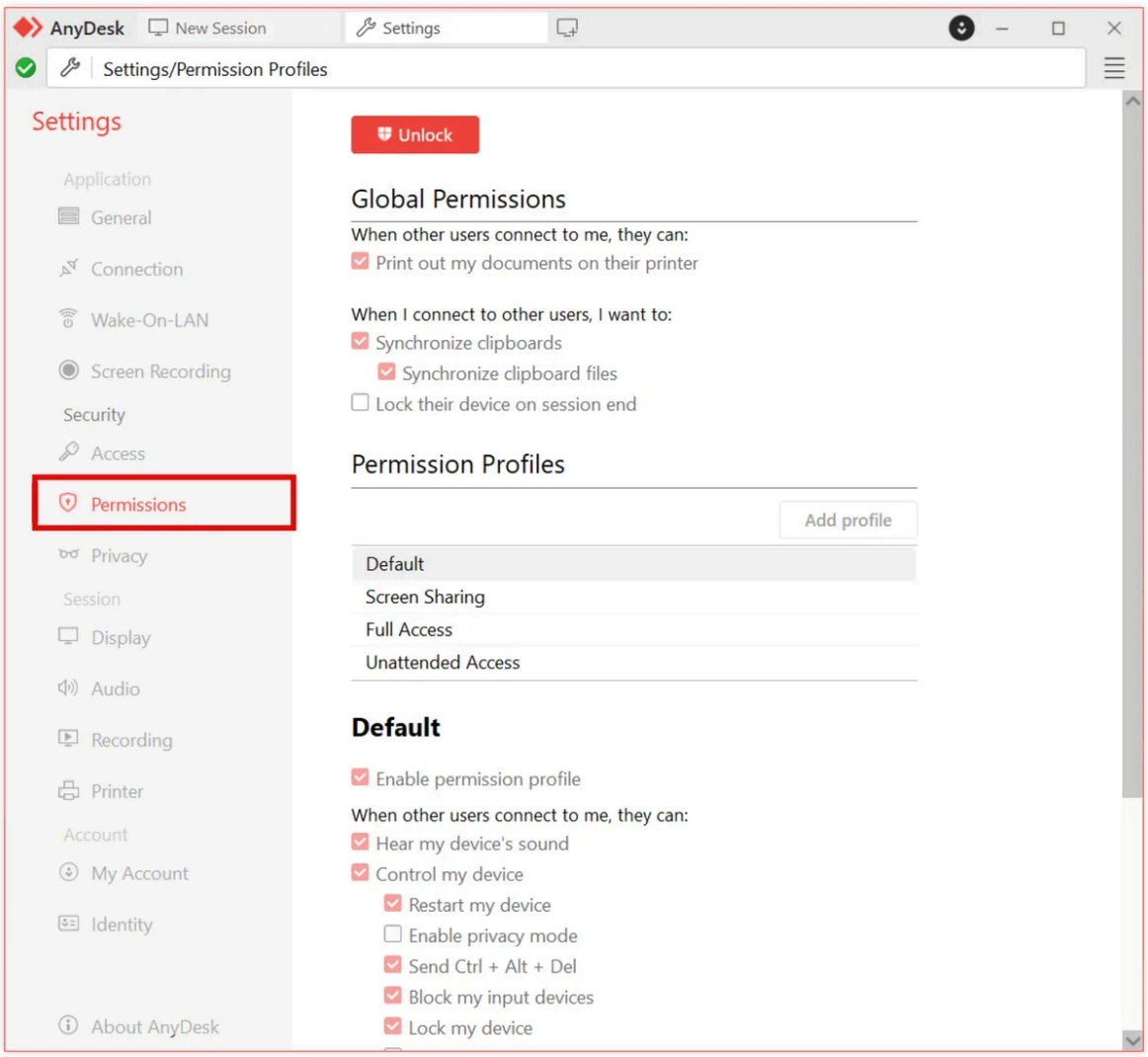
## Define qué puede hacer quien se conecta: perfiles de permisos

Los **Permission Profiles** determinan las acciones permitidas en una sesión: ver pantalla, controlar teclado y ratón, portapapeles, transferencia de archivos, túneles TCP, modo privacidad, reinicio, etc. AnyDesk incluye perfiles predefinidos (Default, Screen Sharing, Full Access, Unattended Access) y permite crear hasta 10 personalizados.

Aplica mínimo privilegio:

- No uses **Full Access** como perfil por defecto.
- Desactiva la **transferencia de archivos**, los **túneles TCP** y el **modo privacidad** si no son necesarios.

- Usa **Screen Sharing** (solo visualización) para soporte de solo lectura.
- En custom clients, define los permisos por perfil con `ad.security.permission_profiles.<perfil>.permissions.<permiso>=0` e impide que se cambien en la ventana de aceptación con `changeable_in_accept_window.<permiso>=0`.




Configuración de perfiles de permisos en AnyDesk

## Asegura el acceso no atendido

El acceso no atendido permite conectar sin que nadie acepte, así que debe ir con la máxima protección:

- **Contraseña fuerte**: mínimo 12 caracteres, única por dispositivo o por grupo.
- **2FA obligatorio**: activa *Enable Two-Factor Authentication* en *Settings* > *Access* > *Unattended Access* para exigir un código de 6 dígitos además de la contraseña.
- **Prohíbe guardar tokens**: desmarca *Allow other computers to save login information* (o `ad.security.allow_logon_token=false`) para que nadie pueda guardar un token de inicio de

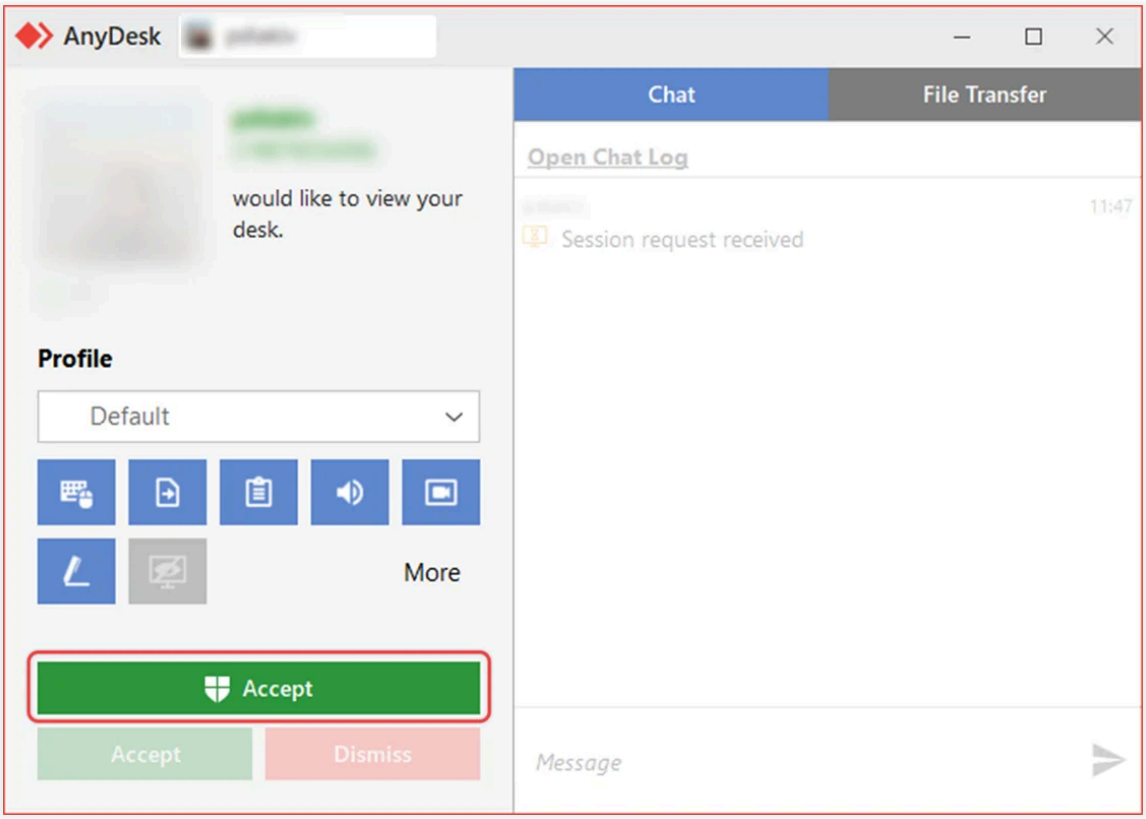
sesión.
- Si un equipo **no** debe recibir acceso no atendido, desactívalo por completo (`ad.features.unattended=false`).

## Controla el acceso interactivo

En *Settings* > *Access* > *Interactive Access* decides cuándo se muestran las solicitudes entrantes:

- **Always show** — toda solicitud requiere aceptación manual. Es la opción más segura para equipos de usuario.
- **Never show** — bloquea las solicitudes interactivas; solo entra el acceso no atendido autenticado. Ideal para servidores y equipos gestionados.

En custom clients se fuerza con `ad.security.interactive_access=2` (desactivar la ventana de aceptación).




Ventana de solicitud de sesión entrante de AnyDesk con opciones de aceptar o rechazar

## Bloquea la configuración del cliente

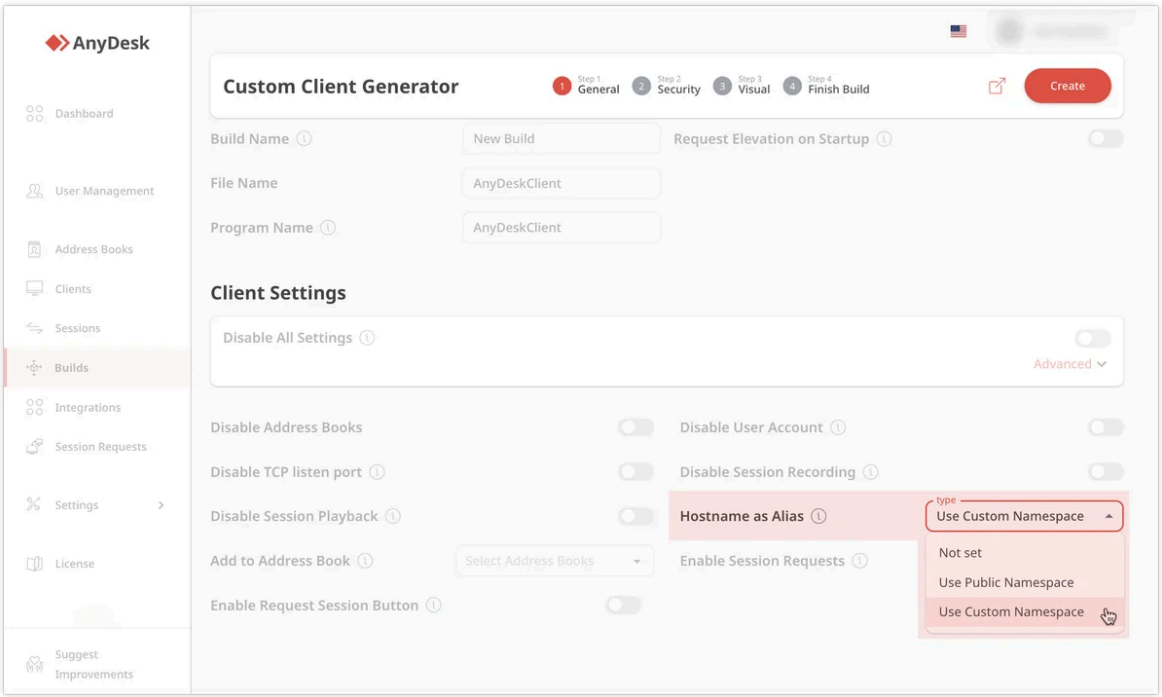
De nada sirve endurecer si el usuario puede revertirlo. AnyDesk permite bloquear la interfaz de configuración:

- `ad.ui.cfg_enabled=false` — desactiva todos los ajustes.
- `ad.ui.cfg_enable_security=false`, `ad.ui.cfg_enable_access=false`, `ad.ui.cfg_enable_permission_profiles=false` — bloquea secciones concretas.
- `ad.license.permissions=0` — impide que el usuario quite la licencia.

> **Clave:** en el Custom Client Generator usa **"Override settings"** en lugar de "Default settings" para las opciones de seguridad. Un override no puede cambiarse desde la interfaz del cliente; un default sí.

## Despliegue seguro con clientes personalizados

La forma más eficaz de aplicar hardening a escala es distribuir un **custom client (Build)** ya endurecido desde my.anydesk II, en lugar de configurar cada equipo a mano.



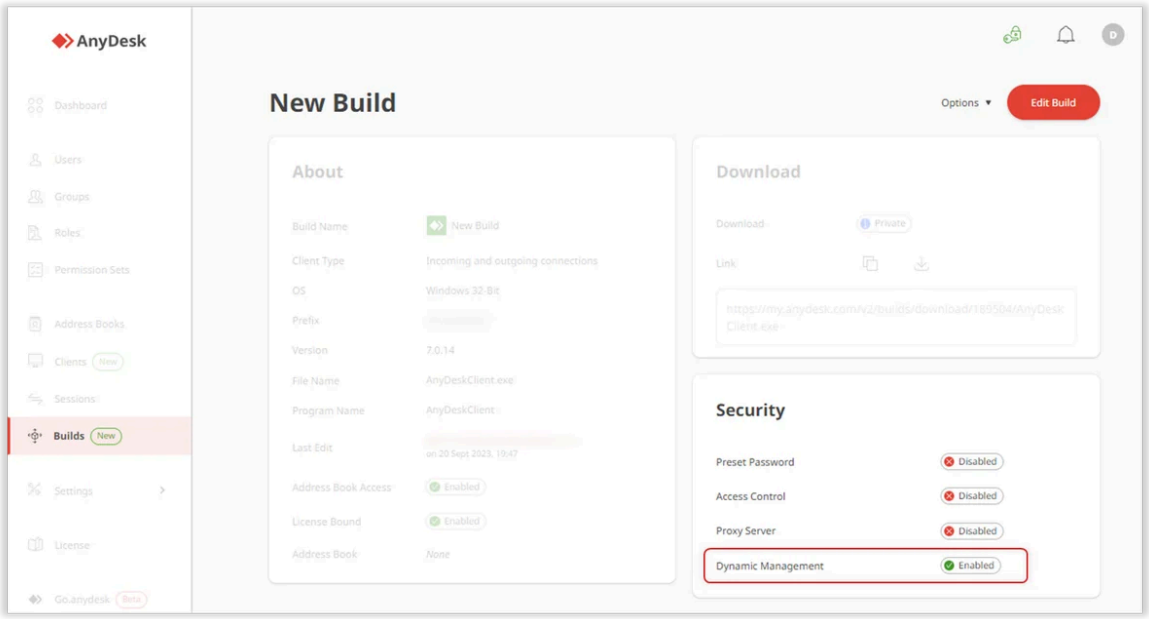

Generador de clientes personalizados de AnyDesk con la configuración de namespace

### Qué preconfigurar en el Build

En *my.anydesk II* > *Builds* puedes crear un cliente con tu seguridad ya aplicada:

- **Namespace personalizado** para que los alias sean `equipo@tuempresa` y la ACL pueda usar `*@tuempresa`.
- **ACL predefinida** con los IDs/alias autorizados.
- **Acceso no atendido** con contraseña preestablecida y 2FA.
- **Perfiles de permisos** endurecidos.

- **Funciones desactivadas**: File Manager, VPN, TCP tunneling, chat, Wake-on-LAN, Discovery.
- **Grabación automática de sesiones entrantes** ( `ad.recording.auto_start.incoming=1` ).
- **Disclaimer de sesión** ( `ad.session_warning.show=1` ) para mostrar un aviso antes de aceptar.
- **Límite de sesiones entrantes** ( `ad.session.limit_incoming=1` ).




Sección Security del New Build en my.anydesk II con Dynamic Management, Preset Password y Access Control List

## Distribución controlada

- Usa **Download type: Private** para que solo usuarios con cuenta vinculada puedan descargar el build. Un enlace público comprometido permite a cualquiera descargar tu cliente preconfigurado.
- Desde la ficha del build puedes ver **Clients Linked To This Build** para saber en qué dispositivos está instalado.
- Prefiere el cliente **instalado** (servicio) sobre el portable: mantiene la configuración tras reinicios, soporta UAC y arranca con el sistema.

## Windows Group Policy

En dominios Windows puedes gestionar AnyDesk de forma centralizada con **Group Policy**: genera las plantillas ADMX/ADML ejecutando tu custom client con `--generate-gpt` y aplícalas por GPO. Permite definir contraseñas de acceso no atendido por perfil, deshabilitar conexiones entrantes/salientes y aplicar ACLs de forma consistente en toda la flota.

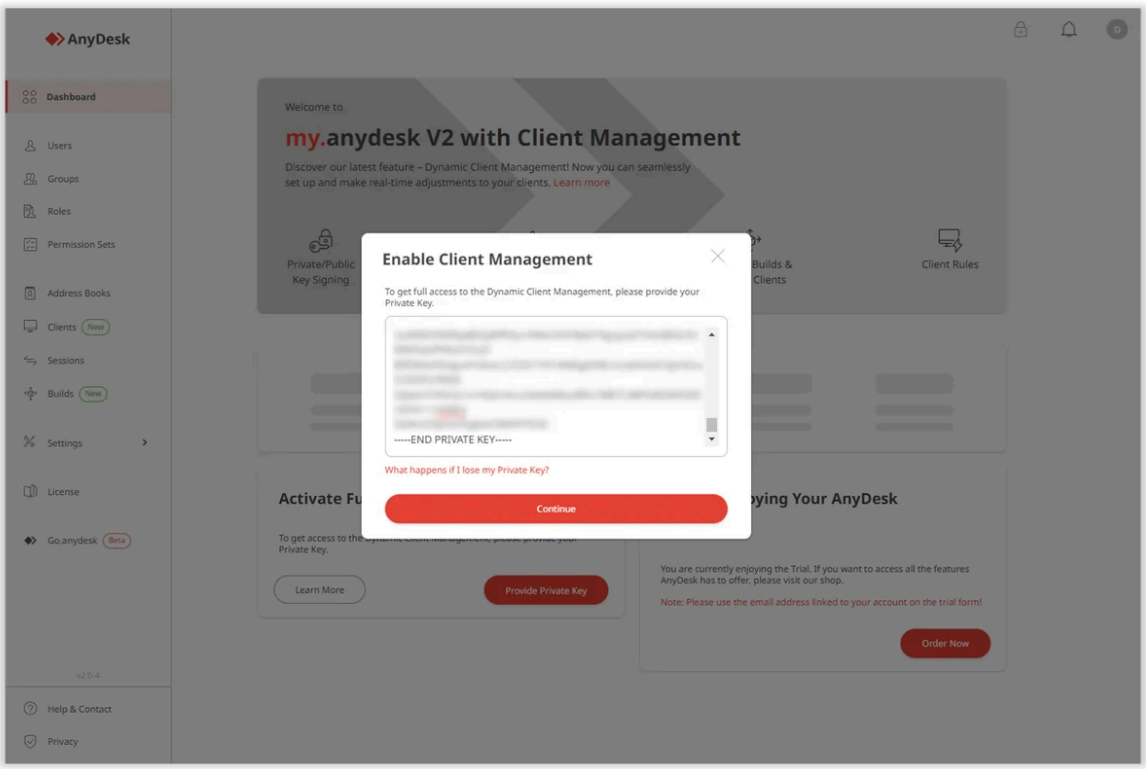
# Gestión centralizada desde my.anydesk II

El portal my.anydesk II es el centro de control del hardening organizacional.

## Central Management y la clave privada

**Central Management (Dynamic Management)** permite modificar la configuración de los clientes en tiempo real desde el portal, sin reinstalarlos. Todos los cambios se firman digitalmente con una **Private Key** que solo tú controlas.

- Actívalo en *Organization* > *General* > *Dynamic Management* y genera la Private Key en el Dashboard.
- **Guárdala de forma segura: se genera una sola vez y no se puede recuperar.** La necesitas en cada inicio de sesión para usar la gestión central.
- Con ella puedes aplicar cambios a todos los clientes de un build (Dynamic Builds) o a clientes individuales.

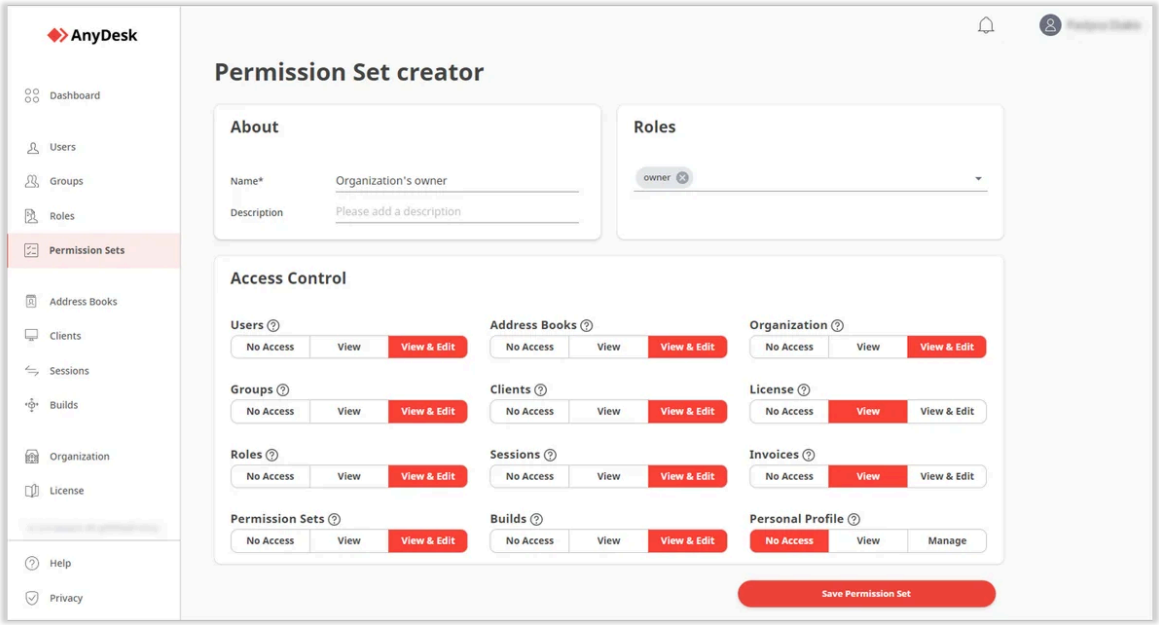



Diálogo de my.anydesk II solicitando la clave privada para habilitar la gestión de clientes

## Roles y Permission Sets (RBAC)

No todos los administradores deben poderlo todo. Con licencia Ultimate Cloud, los **Permission Sets** definen qué secciones del portal puede ver o editar cada usuario (Usuarios, Grupos, Roles, Builds,

etc.), con niveles *No Access / View / View & Edit*. Asigna los permission sets a **Roles** y los roles a los usuarios para aplicar mínimo privilegio también en la consola de gestión.




Creador de conjuntos de permisos en my.anydesk II con control de acceso por sección

### Protege el acceso al portal

- **MFA en la cuenta**: activa la autenticación multifactor para el acceso a my.anydesk.
- **SSO / IdP**: integra el inicio de sesión con tu proveedor de identidad (Single Sign-On) para centralizar el control de acceso y aplicar tus políticas corporativas.
- Revisa periódicamente los usuarios con rol **Owner/Admin**, que son los únicos con acceso a los Activity Logs.

## Monitorización y auditoría

El hardening no termina en la configuración: hay que vigilar.

- **Sessions**: la pestaña *Sessions* de my.anydesk II lista todas las sesiones con origen, destino, estado, inicio y fin. Revísala para detectar conexiones que no reconoces.
- **Activity Logs** (Ultimate Cloud): registran quién creó/editó/eliminó usuarios, grupos, roles, permission sets y builds, incluidos los cambios por REST API. Exportables a CSV.
- **Grabación de sesiones**: activa la grabación automática de sesiones entrantes para tener evidencia de lo que ocurrió.
- **Logs locales**: `connection_trace.txt` y los archivos `ad.trace` / `ad_svc.trace` documentan cada solicitud y sesión en el propio equipo.

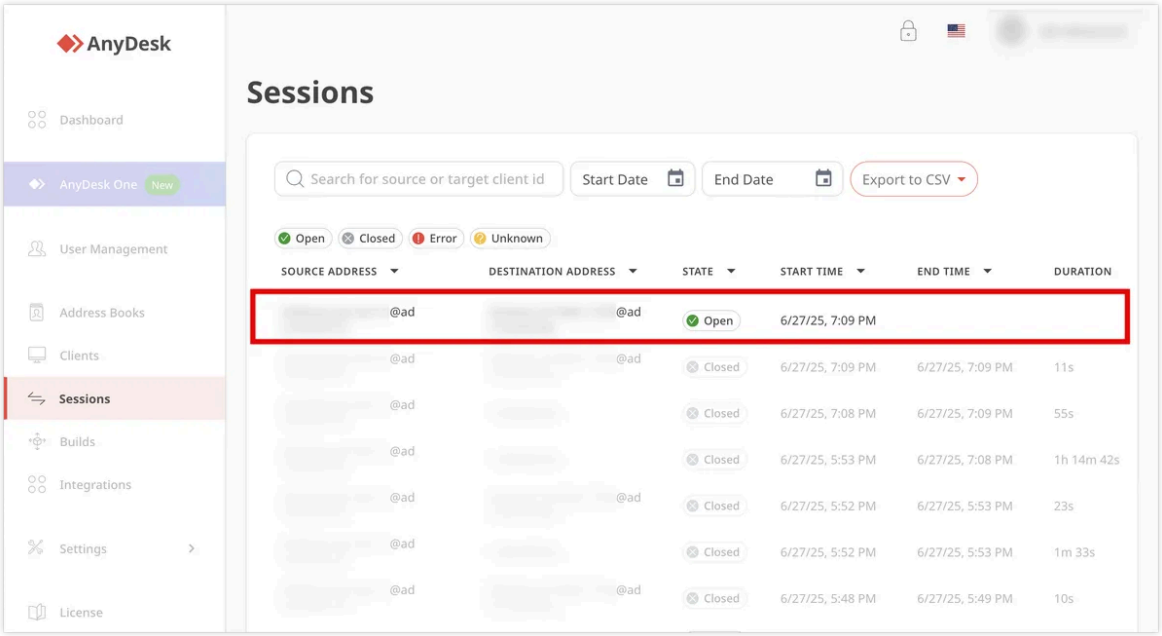



Tabla de sesiones en my.anydesk II con dirección de origen, destino, estado, inicio, fin y duración

Si al revisar las sesiones detectas una conexion que no reconoces, sigue nuestra guia sobre como investigar un presunto acceso no autorizado con AnyDesk.

# Endurecimiento a nivel de red

## Firewall y dominios

- AnyDesk necesita **TCP 80, 443 y 6568** y **UDP 50001–50003** (Discovery). En entornos restrictivos, haz whitelist solo de `*.net.anydesk.com`.
- **Excluye AnyDesk del HTTPS scanning y del DPI** en firewalls corporativos: interferir con el TLS rompe las sesiones.
- Si no usas la función Discovery en la LAN, puedes desactivarla (`ad.features.discovery=false`) para reducir la visibilidad del equipo en la red local.
- En custom clients puedes activar **Disable TCP listen port** para bloquear conexiones TCP entrantes directas.

## On-Premises para máximo control

Para entornos de alta seguridad, **AnyDesk On-Premises** aloja tu propio servidor appliance en tu red:

- Solo tus custom clients pueden conectarse entre sí; los clientes estándar o de otras organizaciones no conocen tu servidor.
- Funciona **sin internet**: basta que los equipos alcancen tu servidor local.

- Aloja el appliance en una **DMZ** y restríngelo por IP o VPN para que solo tu red interna lo encuentre.
- Puedes **bloquear los servidores cloud de AnyDesk en el firewall** y desplegar solo clientes on-prem, impidiendo que un AnyDesk estándar funcione en tu red.
- Control total sobre los datos, incluido el historial de sesiones, para cumplimiento normativo.

## Offboarding y ciclo de vida

Cuando un empleado o dispositivo sale de la organización:

1. **Elimina su cliente** en *my.anydesk II* > *Clients* para revocar su acceso a la libreta de direcciones.
2. **Resetea la clave de licencia** si la conocía (*License* > *About* > *Reset*).
3. **Cambia las contraseñas de acceso no atendido** que pudiera conocer y limpia los tokens.
4. **Bloquéalo en la ACL**. Con namespace personalizado, al quitar la licencia se elimina su alias `@tuempresa` y queda bloqueado automáticamente.
5. **Revoque los enlaces públicos de builds** comprometidos: hazlos privados o recréalos.

## Checklist de hardening

- [ ] ACL configurada, limitada a IDs/alias de confianza o `*@tuempresa`
- [ ] Acceso no atendido con contraseña de 12+ caracteres y 2FA
- [ ] Guardado de tokens deshabilitado
- [ ] Perfil de permisos de mínimo privilegio (sin Full Access por defecto)
- [ ] Transferencia de archivos, túneles TCP, VPN y modo privacidad desactivados si no se usan
- [ ] Acceso interactivo según el caso: aceptación manual o solo no atendido
- [ ] Configuración del cliente bloqueada (override, no default)
- [ ] Despliegue mediante custom client privado e instalado como servicio
- [ ] Central Management activo y Private Key guardada de forma segura
- [ ] RBAC con permission sets y MFA/SSO en el portal
- [ ] Grabación de sesiones entrantes activada
- [ ] Revisión periódica de Sessions y Activity Logs
- [ ] Firewall con whitelist de `*.net.anydesk.com` y AnyDesk excluido de DPI
- [ ] Procedimiento de offboarding documentado

# Aviso legal

Esta guía tiene fines informativos y de buenas prácticas de seguridad. No constituye asesoría de seguridad profesional ni una configuración obligatoria; aplica las medidas según los requisitos y el riesgo de tu organización. AnyDesk es una marca registrada de AnyDesk Software GmbH.

**¿Listo para endurecer tu despliegue? Descarga AnyDesk desde anydesk.com/es/downloads y centraliza la configuración desde my.anydesk II.**