Guía de Endurecimiento de Seguridad en AnyDesk

TABLA DE CONTENIDO

Filosofía de Seguridad: Eliminar la Decisión del Usuario
¿Por qué es crucial este enfoque?
Protección contra Ingeniería Social y Accesos No Autorizados
1. Profundización en ACL (Listas de Control de Acceso)
Sintaxis y Estrategia de Configuración
Ubicación en la Configuración
2. Configuración del Cliente Personalizado (Custom Client)
Pasos Críticos en el Generador (my.AnyDesk):
2.1. Gestión Avanzada: Clientes Dinámicos (Dynamic Configuration)
¿Qué son y cómo funcionan?
Ventajas Críticas (Cero Re-despliegue)
Cómo Implementar Clientes Dinámicos
3. El Addon “Namespace” (Espacio de Nombres)
¿Por qué es la herramienta definitiva contra la suplantación?
Costo e Implementación
Resumen de la Arquitectura Propuesta
Notas adicionales sobre la implementación

Filosofía de Seguridad: Eliminar la Decisión del Usuario

El pilar fundamental de esta estrategia es **quitar la carga de la seguridad de los hombros del empleado**. En la ciberseguridad moderna, sabemos que el “error humano” es el vector de ataque más común. La ingeniería social (el engaño) funciona porque explota la voluntad de ayuda, la urgencia o el miedo del usuario.

¿Por qué es crucial este enfoque?

1. **El usuario no es un experto:** No se puede esperar que un empleado de finanzas o recursos humanos distinga técnicamente entre una ventana de conexión legítima y una ilegítima, especialmente bajo presión.
2. **La fatiga de decisión:** Ante múltiples alertas o una llamada telefónica urgente y agresiva de un supuesto “soporte técnico”, el usuario tiende a ceder para resolver el problema rápido.
3. **Bloqueo Técnico vs. Bloqueo Humano:** Si dependemos de que el usuario diga “No”, existe un margen de error. Si configuramos el software para que técnicamente **no pueda** decir “Sí” (aunque quiera), eliminamos el riesgo.

Al implementar las medidas de esta guía, transformamos la seguridad de **reactiva** (esperar que el usuario detecte la estafa) a **preventiva** (el sistema rechaza la estafa automáticamente sin intervención humana).

Protección contra Ingeniería Social y Accesos No Autorizados

Esta guía detalla la configuración técnica avanzada para entornos corporativos utilizando la licencia Standard (y el addon de Namespace), con el objetivo de prevenir que atacantes externos engañen a los empleados para obtener acceso remoto.

1. Profundización en ACL (Listas de Control de Acceso)

La ACL es la barrera más crítica. Funciona bajo un principio de “Denegar todo por defecto”. Si la lista está vacía, AnyDesk permite conexiones de cualquiera (con confirmación). Si hay **una sola entrada** en la lista, AnyDesk bloquea automáticamente cualquier conexión que no coincida con esa entrada.

Sintaxis y Estrategia de Configuración

En lugar de agregar IDs numéricos individuales (lo cual es difícil de mantener si rota el personal de TI), se recomienda el uso de **Wildcards (Comodines)** si posees un Namespace, o IDs específicos si no.

A. Filtrado por ID Numérico (Básico)

Si tus técnicos usan AnyDesk genérico o no tienes Namespace propio.

- **Formato:** 123456789 (Un ID por línea).
- **Ventaja:** Control granular.
- **Desventaja:** Debes actualizar el cliente de todos los empleados si contratas un nuevo técnico.

B. Filtrado por Namespace y Wildcards (Avanzado)

Si tu empresa adquirió el addon de Namespace (ej. @miempresa).

- **Formato:** *@miempresa
- **Funcionamiento:** El asterisco actúa como comodín. Esto permite que **cualquier** técnico cuyo usuario termine en @miempresa pueda conectar, pero bloquea instantáneamente a:
    - Cualquier usuario @ad (la versión gratuita/pública).
    - Cualquier usuario de otra empresa.
    - Cualquier atacante usando cuentas robadas de otros dominios.

Ubicación en la Configuración

Para pruebas locales antes de desplegar:

1. Ir a **Configuración** > **Seguridad**.
2. Desbloquear el candado de seguridad (requiere admin).
3. Sección **Lista de Control de Acceso**.
4. Activar **Restringir acceso a las siguientes ID y alias**.
5. Ingresar los patrones (ej. *@miempresa o los IDs).

2. Configuración del Cliente Personalizado (Custom Client)

No debes permitir que los empleados instalen el AnyDesk público. Debes generar un ejecutable MSI/EXE desde my.anydesk.com que contenga las reglas de seguridad “incrustadas”.

Pasos Críticos en el Generador (my.AnyDesk):

Al crear un nuevo cliente en la pestaña **Clients**, configura lo siguiente:

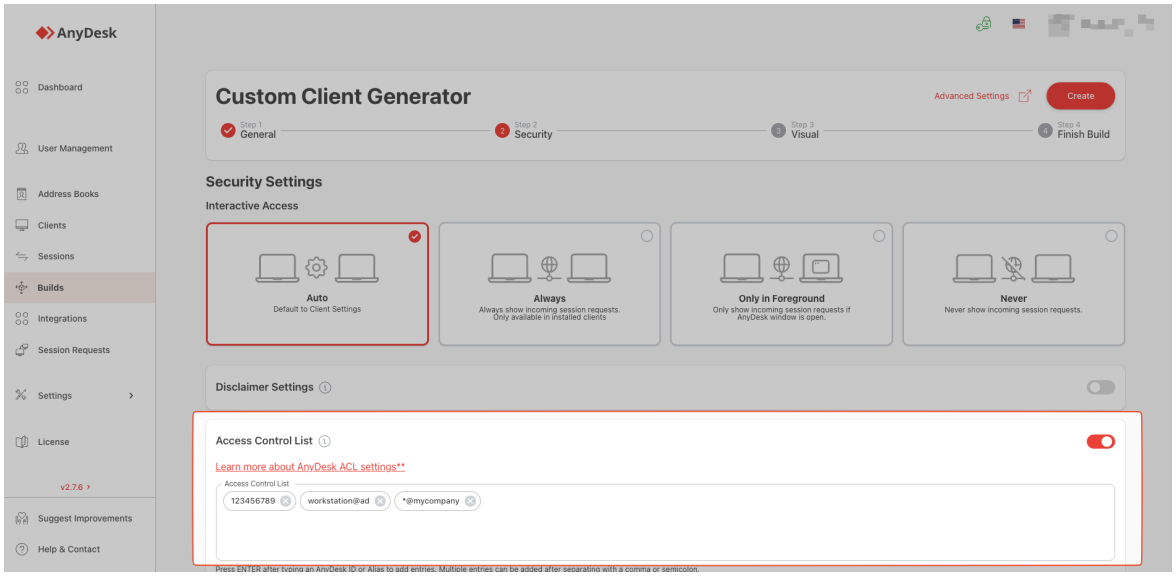
A. Sección “Options” (Opciones)

- **Disable Settings (Desactivar configuración): RADICAL**. Usualmente esta configuración no es necesaria si la empresa gestiona bien los privilegios de sus usuarios (administradores y usuarios regulares aparte), pero si quieres que el acceso remoto esté protegido aun ante un mal uso de una cuenta de administrador, debes marcar esta casilla. Esto elimina la pestaña de configuración del menú del usuario.
    - *Por qué:* Evita que un atacante, mediante ingeniería social (“Señora, por favor vaya a configuración y borre la lista para que pueda ayudarla”), logre evadir la seguridad.

- **Request Elevation at Startup:** Recomendado habilitar. Esta opción solicita elevación de privilegios (UAC) al iniciar, evitando que Windows bloquee al técnico al ejecutar tareas administrativas. **Importante**: Solo aplica para versiones portables o que no requieren instalación, ya que la instalación de AnyDesk de por sí necesita privilegios de administrador.

B. Sección “Security” (Seguridad)

- **Access Control List (ACL):** Aquí es donde “quemamos” la lista blanca en el instalador.
  - Introduce aquí los IDs de tus técnicos o el comodín *@miempresa.
  - Al instalarse este cliente en la PC del empleado, la lista ya estará activa y bloqueada.
- **Interactive Access:** Déjalo en “Always Show Incoming Session Requests” (Siempre mostrar solicitudes). Nunca permitas acceso sin vigilancia a menos que sea un servidor.



Activar ACL

C. Sección “Program Name & Icon” (Identidad Visual)

- Sube el logotipo de tu empresa.
- Cambia el nombre de “AnyDesk” a “Soporte Remoto [TuEmpresa]”.
- *Efecto Psicológico:* Entrena a los usuarios: “Si el programa no tiene el logo azul de nuestra empresa, es un virus/estafa”.

2.1. Gestión Avanzada: Clientes Dinámicos (Dynamic Configuration)

Existe una limitación operativa con los clientes personalizados tradicionales (Estáticos): la configuración queda “quemada” dentro del archivo .exe o .msi al momento de descargarlo. Si

necesitas cambiar la lista de acceso (ACL) porque un técnico se fue o cambiaste una política de seguridad, **debes generar un nuevo instalador y volver a desplegarlo en toda la empresa**, lo cual es costoso y lento.

Para resolver esto, AnyDesk (versión 8.0.3 o superior) ofrece la **Configuración de Cliente Dinámica**.

¿Qué son y cómo funcionan?

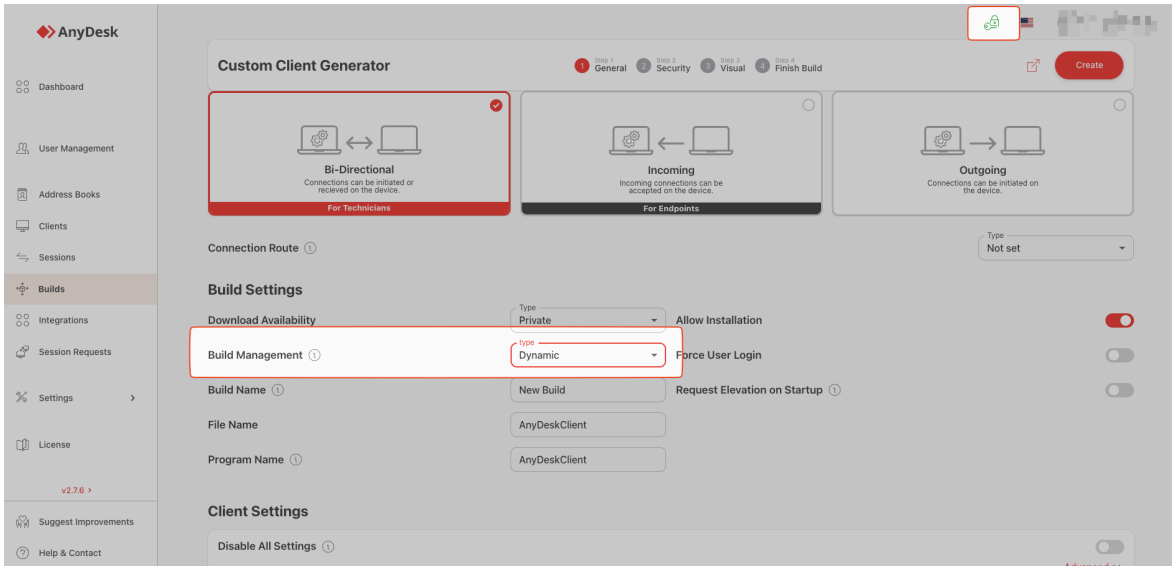
A diferencia del cliente estático, el cliente dinámico no tiene la configuración incrustada de forma permanente. En su lugar, el cliente instalado consulta periódicamente los servidores de AnyDesk (my.anydesk.com) para descargar su configuración más reciente.

Ventajas Críticas (Cero Re-despliegue)

1. **Actualización de ACL en Tiempo Real:**
    - **Escenario:** Despides a un técnico con acceso crítico o detectas que una ID fue comprometida.
    - **Solución:** Entras a la consola web, eliminas esa ID de la ACL del perfil y guardas.
    - **Resultado:** Automáticamente, todos los ordenadores de la empresa actualizan su lista y bloquean al técnico. No necesitas tocar los PCs de los usuarios ni enviar actualizaciones por GPO.
2. **Flexibilidad en Políticas:**
    - Puedes endurecer la seguridad sobre la marcha (ej. desactivar el portapapeles globalmente ante una amenaza de fuga de datos) sin reinstalar el software.
3. **Facilidad de Gestión:**
    - Mantienes una “fuente única de verdad” en la nube. Sabes que todos los clientes tienen la misma configuración de seguridad, independientemente de cuándo se instalaron.

Cómo Implementar Clientes Dinámicos

1. En my.anydesk.com, ve a la pestaña **Files** o **Clients** (dependiendo de tu versión).
2. Asegúrese de activar la opción “**Private key**”; de lo contrario, no podrá seleccionar el tipo de cliente.
3. Crea una nueva configuración de cliente.
4. Asegúrate de que la opción de **Dynamic Configuration** (o asignar a un perfil centralizado) esté activa.
5. Al instalar este cliente en los equipos, se vinculará a ese perfil en la nube. Cualquier cambio futuro que realices en el perfil web se replicará a los agentes instalados.
6. **Importante**: Un cliente estático no puede convertirse en dinámico. Si ya ha desplegado uno estático, deberá reinstalar AnyDesk utilizando el cliente dinámico que generó previamente.



Generar cliente dinámico

3. El Addon “Namespace” (Espacio de Nombres)

En AnyDesk, todos los usuarios públicos tienen el alias nombre@ad. El Namespace te permite tener tu propio sufijo, ej. nombre@miempresa.

¿Por qué es la herramienta definitiva contra la suplantación?

1. Verificación de Identidad (Anti-Spoofing)

Nadie en el mundo puede crear un alias que termine en @tuempresa excepto tú (el administrador de la licencia). AnyDesk verifica la propiedad del dominio/nombre.

- **Escenario de ataque:** Un hacker llama diciendo ser de “Soporte TI”. Su ID será hacker@ad o un número 332-112-445.
- **Defensa:** Si tu ACL está configurada como *@tuempresa, la conexión del hacker rebota automáticamente. Ni siquiera suena la alerta en la PC del empleado.

2. Gestión Escalable

Sin Namespace, cada vez que entra un técnico nuevo, debes actualizar la ACL de 500 empleados para agregar el ID del nuevo técnico.
Con Namespace:

1. Creas el alias del nuevo técnico en tu consola (nuevo.tecnico@tuempresa).
2. Como la ACL de los empleados dice *@tuempresa, el nuevo técnico tiene acceso inmediato sin tocar las configuraciones de los usuarios.

3. Auditoría Forense

En los logs de conexión (my.anydesk.com > Sessions), verás claramente juan@miempresa conectó a recepcion@miempresa. Es mucho más fácil de auditar que ver ID 445212 conectó a ID 998212.

Costo e Implementación

El Namespace es un “Add-on” (costo adicional) sobre la licencia Standard o Advanced, aunque a veces viene incluido en licencias Enterprise. Se compra una sola vez por nombre.

Resumen de la Arquitectura Propuesta

Para una seguridad tipo “Fortaleza”:

1. **Adquirir Namespace:** Comprar @miempresa.
2. **Asignar Alias:** Dar a cada técnico su alias corporativo (tecnico1@miempresa).
3. **Crear Cliente Personalizado Dinámico:**
    - Logo corporativo.
    - Configuración deshabilitada para el usuario.
    - Vinculado a perfil dinámico en la nube.
    - **ACL Centralizada:** *@miempresa.
4. **Despliegue:** Instalar este MSI vía GPO (Políticas de Grupo) o MDM (Intune/ManageEngine) en todos los equipos.
5. **Resultado:** Solo los técnicos con alias @miempresa pueden iniciar una conexión. El resto del internet está bloqueado y puedes revocar accesos en segundos desde la consola web.

Notas adicionales sobre la implementación

1. Despliegue vía GPO (Políticas de Grupo):
   Una vez descargues el archivo .msi de tu cliente personalizado, no necesitas ir PC por PC. Puedes usar un comando de instalación silenciosa en tu Directorio Activo o herramienta de gestión:
   AnyDesk_Custom_Client.msi /qn

   Al ser un cliente personalizado con la configuración “incrustada”, no necesitas scripts adicionales para configurar la contraseña o la ACL; el MSI ya lo lleva dentro.

2. Si no compras el Namespace:
   Aún puedes usar la estrategia, pero la ACL del cliente personalizado deberá ser una lista estática de IDs:

111222333, 444555666, 777888999
El riesgo es operativo: si el técnico 111222333 se va de la empresa y se lleva su laptop, deberás actualizar urgentemente los clientes de los empleados para revocar su acceso (a menos que uses Clientes Dinámicos para actualizar la lista remotamente).

3. Seguridad Física del Técnico:
   Recuerda que con esta configuración, la “llave maestra” son las laptops de tus técnicos. Asegúrate de que tus técnicos tengan:
   - Autenticación de Doble Factor (2FA) activada en su acceso a AnyDesk.
   - Contraseña fuerte en su propia sesión de Windows.