Engel IT

Mejora la Seguridad Cibernética en tu Empresa: Elimina la Carga del Usuario con Ingeniería Proactiva

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

En la era digital, la seguridad cibernética se ha convertido en un aspecto esencial para las empresas, especialmente en Colombia. En Engel, un partner autorizado con amplia experiencia en soluciones de software, creemos que la mejor estrategia es **quitar la carga de la seguridad de los hombros de los empleados**. ¿Por qué? Porque el "error humano" es, sin duda, uno de los vectores de ataque más comunes. La ingeniería social, que a menudo se basa en el engaño, explota las emociones como la urgencia o el miedo de los usuarios.

¿Por qué es crucial este enfoque?

1. **El usuario no es un experto:** Un empleado del área de finanzas o recursos humanos podría no saber cómo identificar una conexión legítima de una ilegítima, especialmente cuando está bajo presión.
2. **La fatiga de decisión:** Ante múltiples alertas o una llamada urgente de un "soporte técnico", el usuario puede optar por lo más fácil y rápido, lo que podría comprometer la seguridad de la empresa.
3. **Bloqueo Técnico vs. Bloqueo Humano:** Si dependemos de que el usuario rechace solicitudes, siempre existe el riesgo de error. Sin embargo, si configuramos el software para que **no pueda** aceptar conexiones no deseadas, eliminamos ese riesgo.

Al aplicar las medidas descritas en esta guía, transformamos la seguridad de un enfoque **reactivo** a uno **preventivo**, donde el sistema automáticamente rechaza intentos de estafa sin necesidad de intervención humana.

Protección contra Ingeniería Social y Accesos No Autorizados

Esta guía aborda la configuración técnica avanzada para entornos corporativos utilizando la licencia Standard (junto al 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 constituye una de las barreras más críticas en la seguridad. Funciona bajo el principio de "Denegar todo por defecto". Si la lista está vacía, AnyDesk permite conexiones de cualquiera, pero si hay **una sola entrada** en la lista, AnyDesk bloqueará automáticamente cualquier conexión que no coincida.

Sintaxis y Estrategia de Configuración

Es preferible el uso de **Wildcards (Comodines)** si se tiene un Namespace, o IDs específicos si no se dispone de uno.

A. Filtrado por ID Numérico (Básico)

Si tus técnicos utilizan AnyDesk genérico o no tienes un Namespace propio.

- **Formato:** 123456789 (Un ID por línea).
- **Ventaja:** Control granular.
- **Desventaja:** Necesitarás actualizar el cliente de todos los empleados si cambias el personal de TI.

B. Filtrado por Namespace y Wildcards (Avanzado)

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

- **Formato:** *@miempresa
- **Funcionamiento:** El asterisco permite que **cualquier** técnico que use un alias que termine en @miempresa pueda conectar, mientras que bloquea instantáneamente a:
    - Cualquiera con @ad (la versión gratuita/pública).
    - Cualquier usuario de otra empresa.
    - Cualquier atacante con 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 acceso de administrador).
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 se debe permitir que los empleados instalen el AnyDesk público. Es necesario generar un ejecutable MSI/EXE desde my.anydesk.com que contenga las reglas de seguridad “incrustadas”.

Pasos Críticos en el Generador (my.AnyDesk):

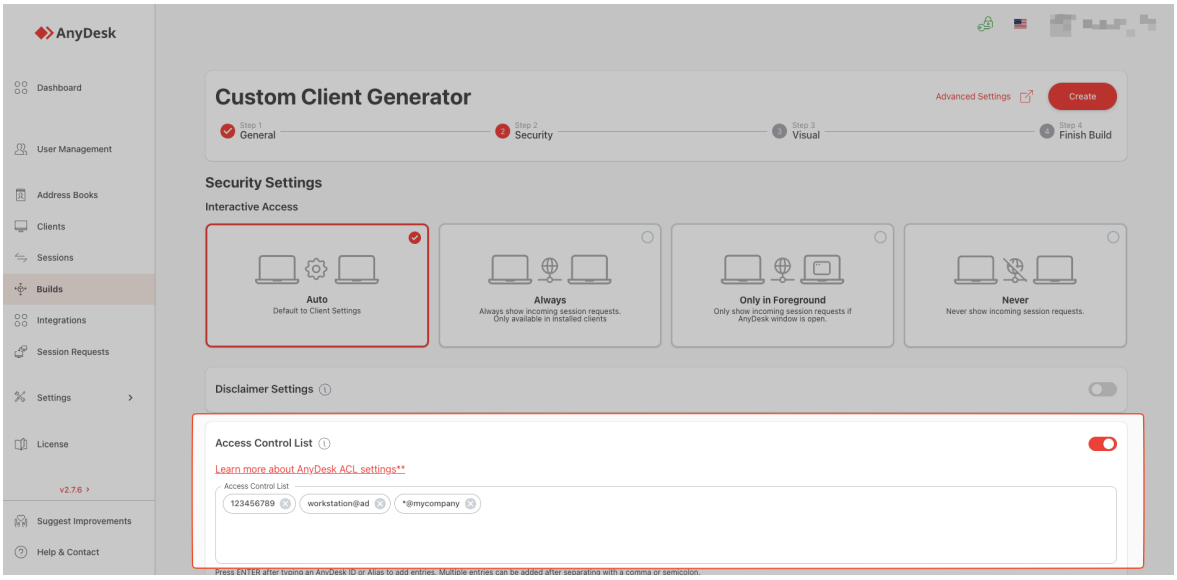
Al crear un nuevo cliente en la pestaña **Clients**, configure lo siguiente:

A. Sección “Options” (Opciones)

- **Disable Settings (Desactivar configuración):** Esta modificación es **RADICAL**. Aunque no siempre es necesaria en empresas con buena gestión de privilegios, si deseas proteger el acceso remoto contra un mal uso, debes marcar esta casilla. Esto eliminará la pestaña de configuración del menú del usuario.
  - *Por qué:* Evita que un atacante, a través de ingeniería social, logre evadir la seguridad.
- **Request Elevation at Startup:** Recomendado habilitar. Esta opción solicita elevación de privilegios al iniciar, evitando que Windows bloquee al técnico al ejecutar tareas administrativas.

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). No 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:* Enseña a los usuarios que si el programa no tiene el logo azul de su empresa, puede tratarse de un virus o una estafa.

2.1. Gestión Avanzada: Clientes Dinámicos (Dynamic Configuration)

Los clientes personalizados tradicionales tienen una limitación operativa: la configuración queda “quemada” dentro del archivo .exe o .msi al momento de descargarlo. Si necesitas realizar cambios en la lista de acceso, **debes generar un nuevo instalador y volver a desplegarlo**, lo que puede ser costoso y lento.

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, consulta periódicamente los servidores de AnyDesk para descargar su configuración más reciente.

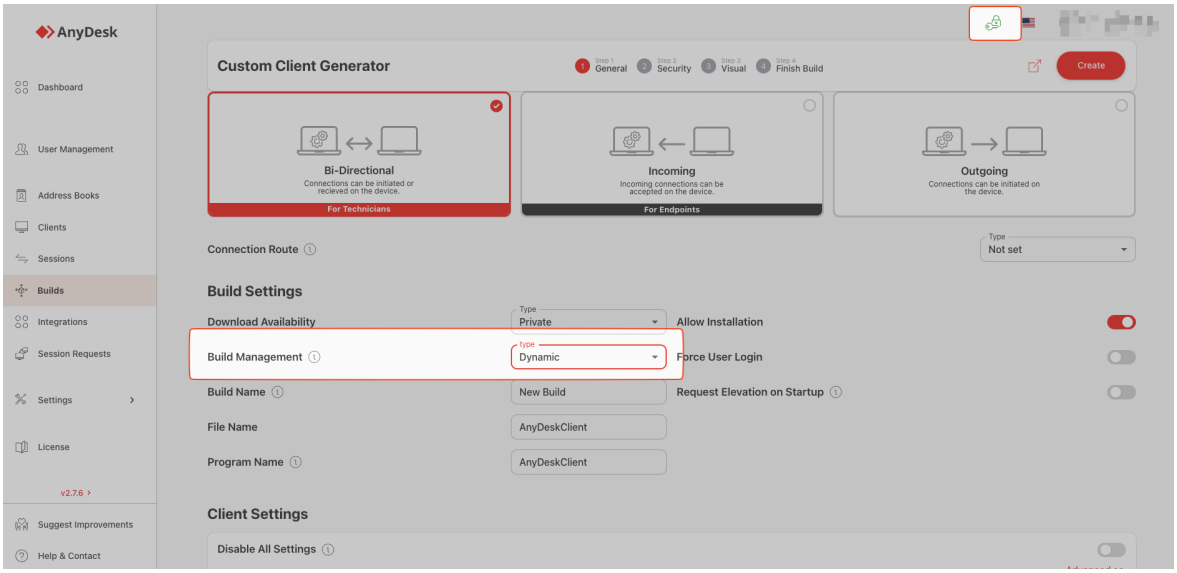
Ventajas Críticas (Cero Re-despliegue)

1. **Actualización de ACL en Tiempo Real:**
    - **Escenario:** Despides a un técnico con acceso crítico.
    - **Solución:** Entras a la consola web, eliminas su ID de la ACL y guardas.
    - **Resultado:** Todos los ordenadores actualizan su lista automáticamente sin necesidad de intervención manual.
2. **Flexibilidad en Políticas:**
    - Puedes endurecer la seguridad sobre la marcha sin reinstalar el software.
3. **Facilidad de Gestión:**
    - Mantienes una “fuente única de verdad” en la nube, asegurando que todos los clientes tengan la misma configuración de seguridad.

Cómo Implementar Clientes Dinámicos

1. En my.anydesk.com, dirígete a la pestaña **Files** o **Clients**.
2. Asegúrate de activar la opción “**Private key**”.

3. Crea una nueva configuración de cliente.
4. Activa la opción de **Dynamic Configuration**.
5. Al instalar este cliente en los equipos, se vinculará a ese perfil en la nube.



Generar cliente dinámico

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

El Namespace te permite personalizar los alias en AnyDesk, por ejemplo, nombre@miempresa.

¿Por qué es la herramienta definitiva contra la suplantación?

1. Verificación de Identidad (Anti-Spoofing)

Nadie puede crear un alias que termine en @tuempresa, salvo tú. AnyDesk verifica la propiedad del dominio.

- **Escenario de ataque:** Un hacker intenta hacerse pasar por soporte técnico. Su ID será algo como hacker@ad.
- **Defensa:** Si tu ACL está configurada como *@tuempresa, su conexión será bloqueada automáticamente.

2. Gestión Escalable

Sin Namespace, cada vez que entra un técnico nuevo, debes actualizar la ACL de todos los empleados.
Con Namespace, simplemente asignas el nuevo alias y los empleados pueden conectarse inmediatamente.

3. Auditoría Forense

Los logs de conexión muestran claramente quién se conectó, por lo que es mucho más fácil auditar y gestionar accesos.

Costo e Implementación

El Namespace es un “Add-on” sobre la licencia Standard o Advanced, aunque algunas veces se incluye en licencias Enterprise. Se adquiere una sola vez por nombre.

Resumen de la Arquitectura Propuesta

Para una seguridad sólida:

1. **Adquirir Namespace:** Comprar el @miempresa.
2. **Asignar Alias:** Proporcionar a cada técnico su alias corporativo.
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 o MDM en todos los equipos.
5. **Resultado:** Solo los técnicos con alias @miempresa pueden iniciar una conexión.

Notas adicionales sobre la implementación

1. **Despliegue vía GPO:**
   Puedes utilizar un comando de instalación silenciosa en tu Directorio Activo o herramienta de gestión: `AnyDesk_Custom_Client.msi /qn`

   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 utilizar la estrategia, pero la ACL del cliente personalizado deberá ser una lista estática de IDs. Esto hará que gestionar el acceso sea más complicado y riesgoso.

3. **Seguridad Física del Técnico:**
   Asegúrate de que tus técnicos tengan activada la Autenticación de Doble Factor (2FA) y una contraseña fuerte en su sesión de Windows.

Si estás buscando mejorar la seguridad de tu empresa y aprovechar al máximo las funcionalidades de AnyDesk, te invitamos a probarlo gratis. ¡Contáctanos en Engel para asesorar tu proyecto y conocer más sobre la compra de AnyDesk en Colombia!