AnyDesk Colombia

# Guía completa para configurar Políticas de Grupo en Windows para AnyDesk

TABLA DE CONTENIDO


- AnyDesk 6 para Windows
- AnyDesk 7+ para Windows
- Casos de Uso


# Windows Group Policy

**Índice**


| | | |
|---|---|---|
| AnyDesk 6 para Windows | AnyDesk 7+ para Windows | Casos de Uso |


**Nota:**

Lamentablemente, debido a la amplia variedad de configuraciones y políticas de seguridad, no podemos brindar soporte para la implementación de clientes de AnyDesk mediante la herramienta de Administración de Políticas de Grupo de Windows. Para preguntas sobre la implementación, por favor comuníquese con Microsoft o su administrador del sistema para conocer la implementación de paquetes MSI de terceros.

Al utilizar Políticas de Grupo, se pueden ajustar, implementar y gestionar desde un lugar central todas las configuraciones para todos los clientes de AnyDesk en un dominio.

En general, se pueden ajustar todas las configuraciones encontradas en Opciones Avanzadas del Cliente Personalizado.

**Advertencia:**

Cambiar la configuración de los clientes de AnyDesk que se están ejecutando activamente requiere reiniciar el cliente para que los cambios surtan efecto.

En general, si es una configuración que requiere que “Desbloquees las configuraciones de XXXXX” en el cliente de AnyDesk, entonces es necesario reiniciar el Servicio de AnyDesk. Esto se logra más fácilmente simplemente reiniciando la computadora o haciendo clic derecho en AnyDesk en la bandeja del sistema de Windows y cerrando AnyDesk.

Por otro lado, si las configuraciones se pueden cambiar sin credenciales administrativas, simplemente cerrar todas las ventanas abiertas de AnyDesk y volver a iniciar el cliente activará los cambios.

## AnyDesk 6 para Windows

La documentación para configurar las plantillas de Política de Grupo para trabajar con clientes personalizados, configurar contraseñas secundarias, así como las plantillas base de Política de Grupo se pueden encontrar en la pestaña de Archivos de su portal de clientes my.anydesk.com.

Volver al inicio

## AnyDesk 7+ para Windows

Debido a la introducción de la función de Perfiles de Permisos con AnyDesk 7, la función de contraseña secundaria encontrada en las plantillas originales de Política de Grupo no funciona con los clientes de AnyDesk 7.

Con AnyDesk 7, las plantillas de Política de Grupo ya no necesitan ser descargadas de my.anydesk.com y luego configuradas manualmente con su prefijo único. En su lugar, pueden generarse directamente usando un cliente personalizado de AnyDesk 7 y el Símbolo del Sistema de Windows.

Para hacerlo simplemente:

1. Descargue un cliente AnyDesk 7 o posterior EXE personalizado desde su portal de clientes my.anydesk.com. Este cliente EXE solo se utiliza para generar las plantillas de Política de Grupo. Con estas plantillas, los administradores pueden configurar tanto clientes EXE estándar como personalizados MSI.
2. En el Símbolo del Sistema de Windows, vaya a la ubicación de descarga del cliente personalizado de Anydesk
3. Ejecute el siguiente comando: <nombre_del_cliente_personalizado_AnyDesk>.exe –generate-gpt

Después, se generará un conjunto de archivos ADML y ADMX de Política de Grupo que son compatibles con nuestra función de Perfil de Permisos y funcionarán tanto con clientes estándar de nuestro sitio web como con clientes personalizados de su portal de clientes my.anydesk.com.

Para conocer las instrucciones sobre dónde colocar los archivos ADMX y ADML generados, comuníquese con su IT o administrador del sistema.

**Advertencia:**

Las claves Features.Connect y Features.Accept actualmente no funcionan para clientes personalizados.

Volver al inicio

## Casos de Uso

Algunos ejemplos de casos de uso para utilizar la herramienta de Administración de Políticas de Grupo de Windows en combinación con AnyDesk:

- Configurar múltiples contraseñas para Acceso no Atendido y vincular cada una de ellas a diferentes permisos. Consulte la documentación de Contraseña Secundaria en la pestaña de Archivos de su portal de clientes my.anydesk.com.
    - Dar acceso completo a los administradores y limitar los permisos para invitados, por ejemplo, para presentaciones.
- Prohibir sesiones entrantes/salientes.
- Cambiar configuraciones para todos los dispositivos implementados en el mismo dispositivo a la vez.
- Editar una lista de control de acceso no preestablecida.

Volver al inicio