



AliSEC

CISCO DUO VIA GPO

Alisec Soluciones

AliSEC Soluciones S.L.

Edificio Asipo II, Plaza Santa Bárbara 4, oficinas 28-19, Parque Empresarial de Asipo, 33426 Llanera, Asturias
T: 984 28 28 30
Correo el: contacto@alisec.es

Contactos

Nombre	Función	Teléfono	Correo electrónico
Alejandro Muñoz	Consultor seguridad	984 282 830	Alejandro.munoz@alisec.es

Control documental

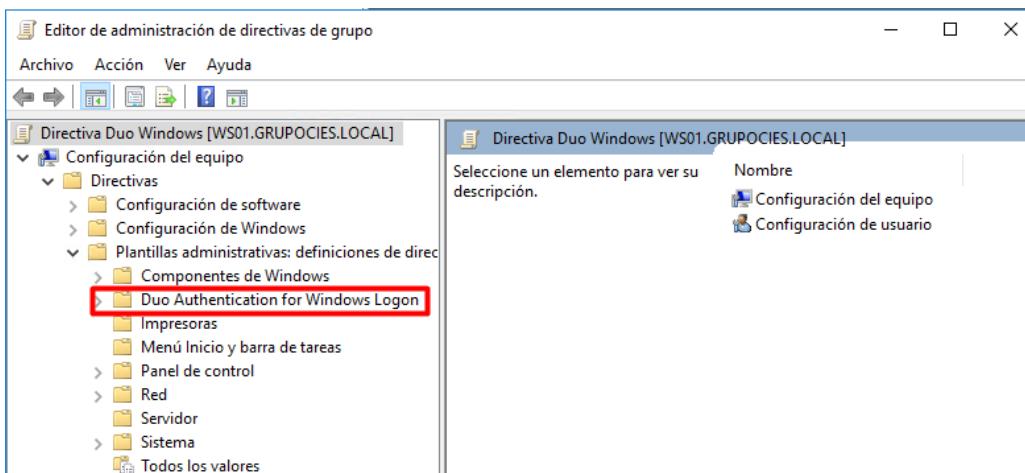
Versión	Descripción	Fecha
1	Versión 1.0	29/11/2022

A. Importación de las plantillas para GPO

1. Descargar las templates desde el siguiente enlace:
https://dl.duosecurity.com/DuoWinLogon_MSIs_Policies_and_Documentation-latest.zip
2. Descomprimir el zip y extraer los dos archivos en las siguientes ubicaciones:

DuoWindowsLogon.admx
 C:\Windows\PolicyDefinitions
 DuoWindowsLogon.adml
 C:\Windows\PolicyDefinitions\en-us\

3. En el administrador de directivas de grupo, al crear una GPO, nos debería aparecer las opciones de CISCO DUO. Si no, reiniciar el DC. Las opciones están en **Configuración de equipo>Plantillas administrativas>Duo Authentication for Windows Logon**



B. Despliegue y config vía GPO.

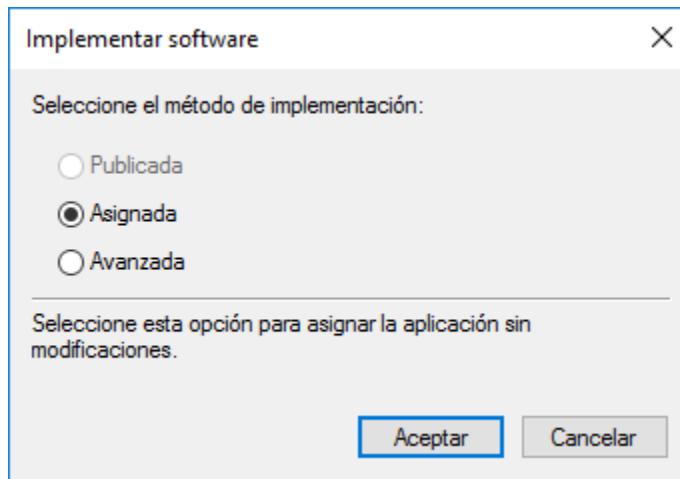
1. Creamos una GPO que desplegará el agente y lo configurará. Tenemos que descargar el .msi del instalador y meterlo en la carpeta de Software que hay en \tudominio.local (sustituir por nombre de tu dominio). Para acceder a ella ir a Ejecutar y escribir \tudominio.local (o el que sea).
2. En la carpeta de Software, meter el msi del instalador.

Compartir Vista

Red > ws01 > Software

Nombre	Fecha de modificación	Tipo	Tamaño
7zz107-x04	08/06/2022 10:38	Paquete de Windows	1.820 KB
DuoWindowsLogon64	02/11/2020 12:22	Paquete de Windows	4.071 KB

3. Crear una GPO para el despliegue, llamarla por ejemplo “Windows DUO Logon” y vincularla a una Unidad organizativa (o a donde corresponda). Esta se aplicará a todos los equipos que estén en esa unidad organizativa. En la configuración de esa GPO, crear la directiva para instalación del msi, dentro de **Config. Del equipo > Directivas> Config de software>Instalación de software**.
4. Botón derecho>Nuevo>Paquete y se abrirá ventana para seleccionar el msi que colocamos en la ubicación compartida.
5. En Implementar Software, seleccionamos asignada y damos a aceptar:



6. Se creará el paquete correctamente:

Nombre	Versión	Estado de la i...	Origen
Duo Authentication f...	4.1	Asignado	\\ws01\Software\ DuoWindowsLo...

7. Configuramos las claves de API. Dentro de la propia GPO vamos a **Configuración de equipo>Plantillas administrativas>Duo Authentication for Windows Logon**

8. En **Duo Service Settings** vamos a configurar las API Key que nos proporciona DUO. Para ello tenemos que configurar las siguientes directivas:

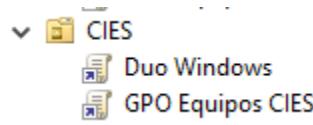
Configuración	Estado
Duo Service: Enable Smart Cards	No configurada
Duo Service: Fail Open if Unable to Contact Duo	Habilitada
Duo Service: Duo API Hostname	Habilitada
Duo Service: HTTP Proxy Hostname	No configurada
Duo Service: HTTP Proxy Port	No configurada
Duo Service: Duo Integration Key	Habilitada
Duo Service: Log File Max Count	No configurada
Duo Service: Log File Max Size MB	No configurada
Duo Service: Duo Secret Key	Habilitada
Duo Service: Specify format of username sent to Duo service	No configurada
Duo Service: Wrap Smart Cards	No configurada

Con la configuración que nos da DUO (API Hostname, Integration Key y Secret key) y habilitamos el Fail Open If unable to contact DUO, en caso de que haya fallo de conexión con DUO.

9. En **Client Settings**, deshabilitamos el “Enable auto push” y configuramos a nuestra imagen y semejanza si queremos habilitar el acceso offline o el número máximo de usuarios Offline, u otras que fueran menester.

Configuración	Estado
Client: Enable Auto Push	Deshabilitada
Client: Enable Debug Logging	No configurada
Client: Enable Offline Access for User Elevation	No configurada
Client: Enable Offline Enrollment during User Elevation	No configurada
Client: Specifies the Protection Mode for User Elevation	No configurada
Client: Offline Access Available	Habilitada
Client: Enable Max Offline Users	Habilitada
Client: Limit Two-Factor to RDP Logons Only	No configurada

10. Aplicar la GPO donde corresponda (Puede ser en una OU concreta con determinados equipos). También podemos aplicar filtros de seguridad para aplicarlos solo en determinados equipos dentro de una misma OU o la organización entera.



11. Una vez aplicada la GPO, hacer un **gpupdate /force** desde cmd en los equipos de esa OU donde se vaya a instalar el DUO y reiniciar. Una vez reiniciados, se deberían aplicar los cambios y aparecer la consola de DUO para enviar el push.