
Resumen para soporte

Licencia de soporte

Por definir

Equipo Soffid

Técnico	Comentario
David Gómez	Técnico implantador del proyecto
Luís Aleñar	Ha participado en la supervisión del proyecto

Equipo partner

Abast

Técnico	Contacto	Comentario
Raul Portillo Piris	rportillo@abast.es	Ha participado en la implantación
Miguel Borque Gonzalez	mborque@abast.es	Ha participado en la implantación
Emilio Torrecilla	etorrecilla@abast.es	Ha participado en la implantación
Adrian Corrales Velasco	acorrales@abast.es	Ha participado en la implantación
Xavier Montero Barrio	xmontero@abast.es	Responible de equipo

Equipo cliente

Técnico	Contacto	Comentario
Daniel Torroba	dtorroba@grupoifa.es	Jefe de infraestructura y ciber. Contacto directo en el proyecto
Daniel López	dlopez@grupoifa.es	Ha participado en las reuniones, ayudando a Daniel Torroba
Lola Mozas	Lmozas@grupoifa.es	Responsable infraestructuras e IT, seguimiento proyecto, implantación y tiempos.

VPN

Para acceder al servidor de PAM del cliente donde está intalado en Launcher y el Syncserver proxy, se accede mediante VPN.

La IP del servidor de PAM es la 10.20.20.100 (pam01) y el usuario es admsoffid (credenciales guardadas en el Password Vault de Soffid).

Se necesita instalar Forticlient.

Configuración de la coneión VPN de IFA:

- Nombre de conexión: VPN SSL.
- Remote Gateway: acceso.grupoifa.es
- Puerto: 4434
- Habilitar inicio de sesión SSO

VIEW VPN

VPN SSL

VPN IPsec

XML

Nombre de Conexión	VPN SSL
Descripción	
Remote Gateway	acceso.grupoifa.es ×
	+ Adicionar Gateway Remoto
	<input checked="" type="checkbox"/> Personalizar puerto <input type="text" value="4434"/>
Inicio único de sesión	<input checked="" type="checkbox"/> Habilite el inicio de sesión único (SSO) para el túnel VPN
	<input checked="" type="checkbox"/> Use un navegador externo como agente de usuario para la autenticación de usuario SAML
	<input type="checkbox"/> Enable auto-login with Azure Active Directory
Certificado de Cliente	Ninguno ▾
	<input type="checkbox"/> Habilitar dirección Dual-stack IPv4/IPv6
Traffic Keep Strategy	Reapply route ▾

Close

Para conectar, cuando pida login, es con usuario y contraseña de Soffid. Hay que solicitar a Daniel Torroba (Grupo IFA) acceso previamente. Desmarcar la opción de usar el navegador externo

Acceso

Acceso vía cloud: <https://ifa.prod.soffid.net>

Los usuarios/contraseñas están en el [Password vault](#)

Versión

Soffid 4 (cloud).

Módulos

PAM + AM.

Arquitectura

Es cloud.

Fuente autoritativa

La fuente autoritativa es un Active Directory. Solo se realiza la carga autoritativa y reconciliación de las cuentas que están en a OU=SSO_Soffid.

Se ha programado que cada hora se realice una carga autoritativa, reconciliación. En la reconciliación, mediante un script, se vinculan automáticamente las cuentas AD con las identidades (mismo nombre de usuario y nombre de cuenta).

PAM

En la infraestructura de Grupo IFA (máquina pam01) se ha instalado un syncserver y un launcher. Desde ahí se realizan las conexiones PAM (rdp, ssh y consolas web).

Se han registrado varias redes en las cuales se ha hecho el descubrimiento (Network discovery) de los equipos. Para el descubrimiento se ha utilizado una cuenta de dominio (grupoifa\soffidAdmin) para el descubrimiento de las máquinas Windows; y para los equipos fuera de dominio (linux y redhat) se han utilizado cuentas locales con permisos de administrador (creadas por grupo IFA).

AM

Hay un idp Soffid y un idp externo (Entra ID)

Tienen un idp externo de Entra ID donde hacen login. Los usuarios internos de IFA inician sesión desde su EntraID solamente. Mientras que los externos (Abast se consideran externos) entran mediante usuario, contraseña y OTP como segundo factor.

En el idp está configurado el perfil de ESSO para aplicar doble factor..

Documentación adicional

Por definir.

Otros

Por definir.

Revision #6

Created 9 July 2026 10:30:09 by David Gómez

Updated 10 July 2026 14:32:14 by David Gómez