Template - Resumen para soporte

Licenciamiento

Fecha de inicio de soporte

Está previsto para finales de julio de 2026.

Cliente en producción desde hace años.

SLA

Soporte 24x7.

Soporte 8x5.

Plataforma

Soffid cloud.

Soffid on premise instalación.

Soffid on premise docker.

Soffid on premise docker compose.

Soffid on premise docker compose + swarm.

Soffid on premise cloud kubernetes.

Soffid on premise cloud openshit.

Versión

Soffid 3.

Soffid 4.

Módulos

IGA + AM + PAM + IRC.

Participantes

Equipo Soffid

Equipo de soporte.

Técnico	Comentario
Daniel Company	Responsable del canal de soporte
Monsterrat Prieto	Responsable del servicio de soporte

Equipo de proyectos.

Técnico	Comentario
Nombre técnico 1	Técnico implantador del proyecto
Nombre técnico 2	Técnico que ha participado en algunas tareas
Nombre responsable	Ha participado en la supervisión del proyecto

Equipo partner

No hay partner.

El partner es **Partner**.

Todas las operativas las realiza el partner.

El parner no ejecuta ninguna operativa.

Técnico	Contacto	Comentario
Partner técnico 1	111@partner.com	Ha participado en la implantación, técnico más proactivo

Partner técnico 2	222@partner.com	Ha participado en la implantación
Partner responsable	333@partner.com	Responsable de equipo

Equipo cliente

Técnico	**Contacto**	**Comentario**
Cliente técnico 1	111@cliente.com	Jefe de infraestructura y ciber. Contacto directo en el proyecto
Cliente técnico 2	222@cliente.com	Ha participado en las reuniones, ayudando a Daniel Torroba
Cliente responsable	333@cliente.com	Responsable infraestructuras e IT, seguimiento proyecto, implantación y tiempos.

Acceso

VPN

Para acceder a su sistema tenemos que conectarnos por VPN, documentado en el siguiente enlace.

Entornos

Tienen solo el entorno de **producción**.

Hay tres entornos: **DES**, **PRE** y **PROD**.

Acceso web

Consola en on premise (requiere VPN): URL

Consola en Soffid cloud: URL

Los usuarios/contraseñas están en el Password vault

Acceso ssh

Como es un proyecto cloud, tienen una máquina jump server que tiene los siguientes componentes instalados:

- Sync server proxy (docker)

- PAM launcher (docker compose)

Para acceder a la máquina, primero hay que conectarse por VPN y luego ejecutar:

```
ssh usuario@ip-maquina
```

Los usuarios/contraseñas están en el Password vault

Implantación

Arquitectura

No hay Soffid cloud demo.

Soffid cloud producción:

- Consola + syncserver + store.
- Máquina cliente: syncserverproxy + launcher.

La instalación se realizó sobre la máquina **10.7.254.200**.

La instalación está realizado en docker compose, aquí los comandos para verificar los contenedores.

```
cd /opt/soffid
docker compose ps
```

Los componentes instalados.

- Traefik -> los usan para exponer la Consola 8080 como cie.automotive.com 443
- Consola
- Syncserver principal
- Soffid LDAP

Componentes

Tienen el componente **LDAP de Soffid** instalado y tienen varias aplicaciones que autentican sobre él.

También tiene el **sincronizador de contraseñas** instalado en los domain controllers.

IGA

La fuente autoritativa es un Active DIrectory. Solo se realiza la carga autoritativa y reconcilación de las cuentas que están en el grupo **SSO_Soffid**, y cuentas administradores de los grupos **Admins_IFA** y el grupo **Admins_Abast**.

Añadir pantallazo?

Se ha programado que cada hora se realice una carga autoritativa y reconciliación. Hay script de entrada que filtran por grupos y se vinculan identidades con cuentas (mismo nombre de usuario y nombre de cuenta).

Añadir pantallazo?

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.

Se ha incluido el componente ESSO en el proyecto En el idp está configurado el perfil de ESSO para aplicar doble factor. Esta característica está aun pendiente de realizarse.

PAM

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

Se han registrado varias redes en las cuales se ha hecho el descubirmiento (Network discovery) de los equipos. Para el descubirmiento se ha utilizado una cuenta de dominio (grupoifa\soffidAdmin) para el descubirmiento 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).

IRC

No se utiliza ninguna funcionalidad de este módulo.

Otros

Documentación

No hay nada en Drive. Solo se está trabjando en un manual de configuración PAM, cuando esté listo se subirá al Drive.

No hay nada en owncloud.

Actualizaciones

La **Consola** y el **Syncserver** los actualizaremos mediente **docker compose** actualizando la versión en el **docker-compose.yaml**.

¿Cómo actualizamos el Soffid LDAP?

Temas a tener en cuenta

- Actualmente no hay **bolsa de horas** contratada, todo se hace a través de soporte.
- Sobre IGA, a los **ADs** no sincronizamos nada, solo recuperamos información.
- Los usuarios del **Soffid LDAP** los gestiona Soffid: creación , actualización, cambio de contraseña, etc.
- El los agentes de AD tienen scripts para **vincular** las identidades.
- En los windows realizan **elevación de permisos** con usuarios adm que tienen asociados en Soffid como cuentas compartidas.

Revision #8
Created 14 July 2026 14:29:44 by Sion Vives
Updated 14 July 2026 16:22:18 by Sion Vives