MANUAL DE USUARIO O TÉCNICO

MANUAL DE OUTH en HCM

CONTROL DE VERSIONES

VERSIÓN DOCUMENTO	VERSIÓN APLICACIÓN	FECHA	ELABORADO POR
1	7.4.2	2022-11-10	Angela Ospina

Índice

1. Introducción 3
2. Definiciones 3
3. Precondiciones 3
4. Configuración de la aplicación 4
4.1 Configuración STUNNEL 4
4.2 Configuración HCM 6

1. Introducción

Actualmente la aplicación para el envío de correos utiliza una autenticación básica hacia los sistemas de servidores de correo, este tipo de autenticación aunque maneja usuario y contraseña se ha quedado atrás y en este momento puede generar bastantes vulnerabilidades de seguridad; por lo cual Servicios de Correo como GMAIL o Microsoft 365 están desactivando este tipo de autenticación y agregando otras técnicas de autenticación que permitan validar que quien envía el correo si sea el dueño de esto.

A continuación, explicaremos la manera de configurar HCM para que se conecte a los servicios de correo a través de la técnica de autenticación DKIM.

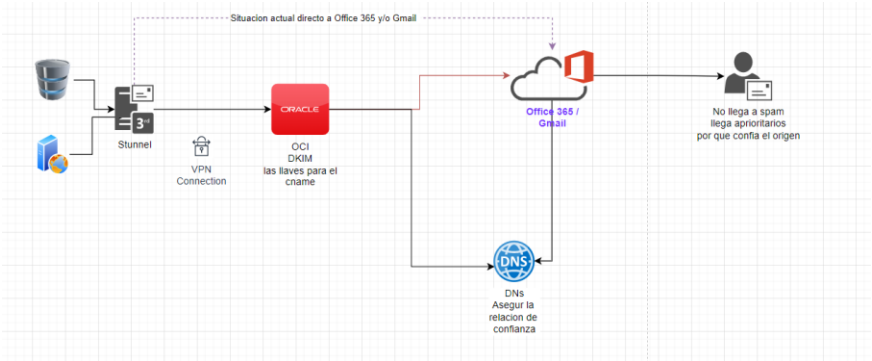
2. Definiciones

A continuación, se detallan los términos particulares que serán utilizados durante el presente documento:

- **DKIM (Domain Keys Identified Mail):** Técnica de autenticación de correo electrónico que permite al receptor ver que un correo electrónico fue sin duda, enviado y autorizado por el dueño de ese dominio. Esto es hecho al darle al correo electrónico una firma digital. La firma DKIM es un encabezado que es añadido al mensaje y está asegurado con encriptación.
- **Autenticación Básica:** Técnica de autenticación en donde el servidor verifica el usuario con nombre y contraseña
- **Vulnerabilidad de seguridad**
- **Stunnel:** Programa de computadora libre multi-plataforma, utilizado para la creación de túneles TLS/SSL
- **OCI:** Plataforma completa de infraestructura en la nube para cada carga de trabajo

3. Precondiciones

1. Configuración correcta del dominio del cliente en OCI DKIM (Validar con Soporte)



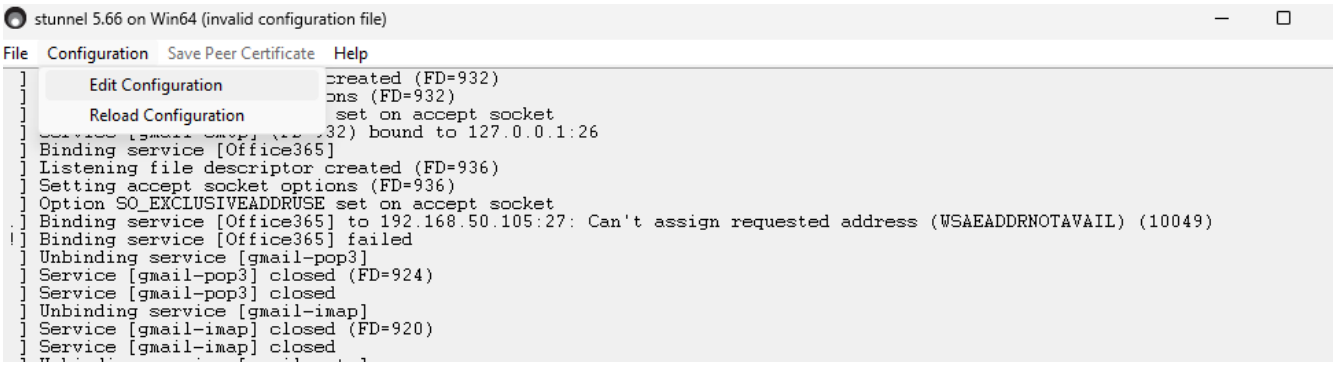
4. Configuración de la aplicación

Para el correcto funcionamiento del envío del correo se deben realizar 2 cambios a nivel de HCM:

1. A nivel del STUNNEL; esta aplicación se usa para asegurar que la autenticación de correo se realice por una conexión segura.
2. Configuración de constantes del sistema de HCM

4.1 Configuración STUNNEL

1. Ir a la carpeta de instalación de STUNNEL \stunnel\bin y abrir el ejecutable
2. Seleccionar configuración y dar click en Edición de configuración para que el archivo de configuración de stunnel se abra en un block de notas



3. Ir a la configuración SMTP de Office365 o el de Gmail; según servidor de correo que aplique

```
[Office365]
client = yes
accept = 190.72.100.65:25
connect = smtp.office365.com:587
CAfile = ca-certs.pem
;verify = 2
;CApath = /etc/ssl/certs
;checkHost = smtp.office365.com
;OCSPaia = yes
protocol=smtp
```

4. En la parte de abajo crear una nueva configuración, agregando los siguientes parámetros:

   [oci-smtp]

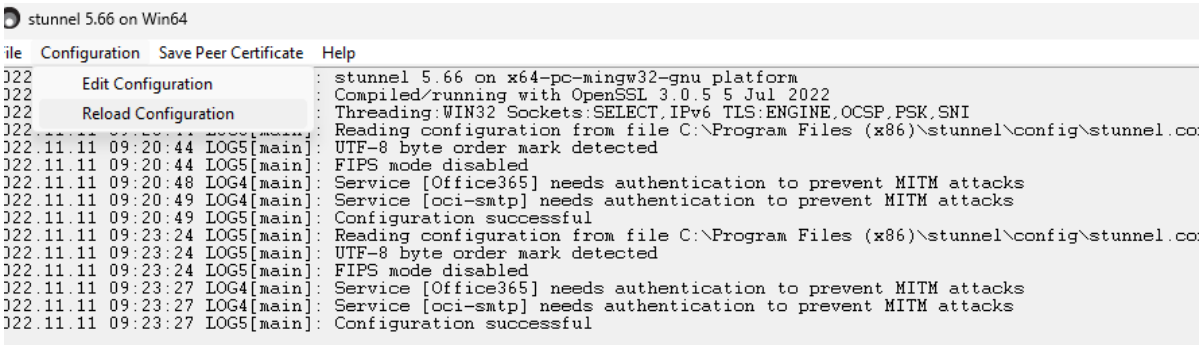
   client = yes

accept =
protocol = smtp
connect =
protocolHost =
protocolUsername =
protocolPassword =

```
[oci-smtp]
client = yes
accept = 190.72.100.65:28
protocol = smtp
connect = smtp.email.us-ashburn-1.oci.oraclecloud.com:587
debug = debug
protocolHost = smtp.email.us-ashburn-1.oci.oraclecloud.com:587
protocolUsername = ocid1.user.oc1..aaaaaaaabnr4nociay4jpwxx2cv4zlsrlttpdi6u3sb3dyzb47lg2kec
protocolPassword = sscQy1$:DgubMix}z_)8
```

Los datos:
connect
protocolHost
protocolUsername
protocolPassword
Serán enviados al cliente una vez se haya realizado la configuración de activación DKIM con el dominio.

5. Guardar el archivo y recargar la configuración de stunnel (dar click en recargar configuración)



6. Para confirmar que los servicios se hayan recargado correctamente por favor revisar el log, debe ser de la siguiente manera.

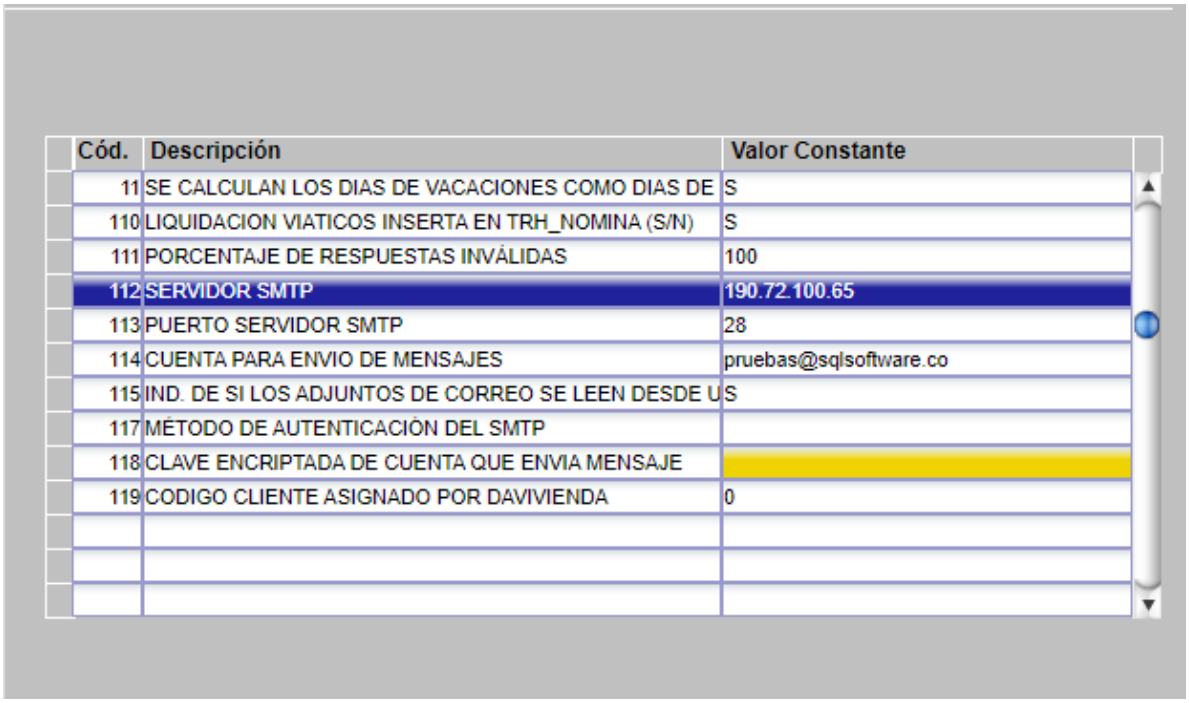
```
2022.11.10 17:43:09 LOG5[main]: Reading configuration from file C:\Program Files (x86)\stunnel\config\stunnel.conf
2022.11.10 17:43:09 LOG5[main]: UTF-8 byte order mark detected
2022.11.10 17:43:09 LOG5[main]: FIPS mode disabled
2022.11.10 17:43:12 LOG4[main]: Service [Office365] needs authentication to prevent MITM attacks
2022.11.10 17:43:13 LOG4[main]: Service [oci-smtp] needs authentication to prevent MITM attacks
2022.11.10 17:43:13 LOG5[main]: Configuration successful
```

4.2 Configuración HCM

1. Ruta del Menú de acceso: HCM – Tools - Seguridad Y Control De Acceso - Parámetros del módulo - Constantes y Variables por Usuario - Constantes del Sistema

   Configurar las variables 112, 113, 114 y 117 de la siguiente manera:

   112: IP configurada en stunnel para la recepción de correo
   113: Puerto configurado en stunnel para la recepción de correo
   114: Cuenta de correo enviada por parte de nosotros para el uso de envío de correos
   117: en el método de autenticación dejar vacío el campo



Cód.	Descripción	Valor Constante
11	SE CALCULAN LOS DIAS DE VACACIONES COMO DIAS DE	S
110	LIQUIDACION VIATICOS INSERTA EN TRH_NOMINA (S/N)	S
111	PORCENTAJE DE RESPUESTAS INVÁLIDAS	100
112	SERVIDOR SMTP	190.72.100.65
113	PUERTO SERVIDOR SMTP	28
114	CUENTA PARA ENVIO DE MENSAJES	pruebas@sqlsoftware.co
115	IND. DE SI LOS ADJUNTOS DE CORREO SE LEEN DESDE U	S
117	MÉTODO DE AUTENTICACIÓN DEL SMTP	
118	CLAVE ENCRIPTADA DE CUENTA QUE ENVIA MENSAJE	
119	CODIGO CLIENTE ASIGNADO POR DAVIVIENDA	0

2. Configurar la ACL de bases de datos creada para el SMTP con la nueva IP y puerto (Página 124 del documento SCO_T&D_Ins_Instructivo de instalación Softland HCM_V24_202110)