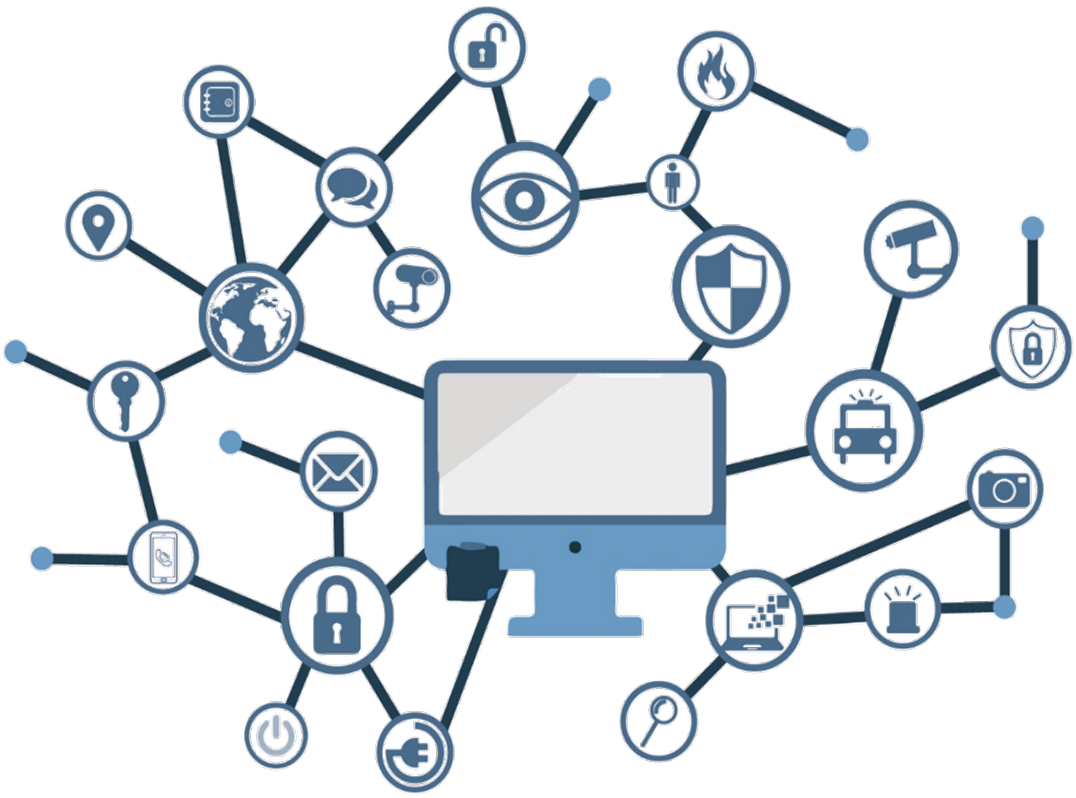
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1101

Procedimiento de Empleo Seguro
SECRET SERVER de THYCOTIC



Marzo 2020

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.01.28 11:16:17 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-20-092-0

Fecha de Edición: marzo de 2020
Las empresas ISDEFE y THYCOTIC han participado en la realización y modificación del presente documento.

ÍNDICE

a)

1. INTRODUCCIÓN

1. ***Secret Server Government Edition*** **de Thycotic** es una solución de Gestión de Acceso Privilegiado (PAM) diseñada para almacenar, distribuir, cambiar y auditar de forma *segura* las *credenciales* de la organización con diferentes conjuntos de privilegios, a los recursos y servicios de la misma.
2. *Secret Server* de Thycotic permite, además:
    - Crear y gestionar un almacén seguro (cifrado) para las credenciales con privilegios.
    - Detectar todas las cuentas de servicio, de aplicaciones, de administración, *etc. para obtener una visión completa de los accesos privilegiados que* existen en la organización, y frenar la proliferación no justificada de los mismos.
    - Gestionar las credenciales de cuentas privilegiadas de forma segura, permitiendo comprobar la complejidad de contraseñas y su rotación periódica.
    - Configurar el control de accesos basado en rol (RBAC) y gestionar un flujo de trabajo para las solicitudes de acceso y aprobaciones.
    - Controlar las sesiones que establecen los usuarios, permitiendo la supervisión y grabación de las mismas. cuentas con privilegios de una organización. Es responsable de facilitar, por lo tanto, el acceso de los usuarios
3. *Secret Server* realiza estas tareas a través del uso de objetos llamados "**secretos**". Un secreto se define como una pieza de información sensible que necesita ser protegida. Normalmente se trata de credenciales de acceso.
4. Para acceder a los activos IT y a los servicios, los usuarios acceden *a Secret Server* y se conectan a los sistemas gestionados por este, a través del secreto. Es, por tanto, *Secret Server* quien proporciona las credenciales de acceso.
5. La solución puede administrarse y configurarse de forma segura a través una interfaz GUI mediante HTTPS/TLS.

2. OBJETO Y ALCANCE

6. El objeto del presente documento es servir como guía para realizar una instalación y configuración segura de la solución ***Secret Server Government Edition 10.1 de Thycotic.***
7. El *software* recomendado para el servidor Secret Server y el servidor de Base de Datos, es el siguiente:
    - Sistema Operativo *Windows Server 2016 (x64).*
    - *Microsoft .NET Framework 4.6.2.*
    - *Microsoft Internet Information Services (IIS) 10.0.*
    - Microsoft SQL Server 2016.
8. *Secret Server* y *SQL Server* pueden instalarse en el mismo servidor, dependiendo de las necesidades de la organización. Especialmente, dependiendo de si se va a utilizar la característica de grabación de sesiones, en cuyo caso se recomienda que la Base de Datos SQL se encuentre en un servidor aparte con capacidad de almacenamiento.
9. El entorno operativo recomendado es el siguiente:
    - Servidor de Auditoría: *syslog-ng 3.9.*
    - Servidor de Autenticación: *Microsoft Windows Server 2012 R2* con *Active Directory y LDAP.*
10. Este producto se sitúa dentro de la familia **Gestión de Acceso Privilegiado (PAM)** de la tipología definida por el CCN (CPSTIC).

3. ORGANIZACIÓN DEL DOCUMENTO

11. El presente documento se divide en tres partes fundamentales, de acuerdo a distintas fases que componen el ciclo de vida del producto:

    a) Apartado 4. En este apartado se recogen aspectos y recomendaciones a considerar **antes de proceder a la instalación** del producto.

    b) Apartado 5. En este apartado se recogen recomendaciones a tener en cuenta durante la **fase de instalación** del producto.

    c) Apartado 6. En este apartado se recogen las recomendaciones a tener en cuenta durante la **fase de configuración** del producto, para lograr una configuración segura.

    d) Apartado 7. En este apartado se recogen las tareas recomendadas para la **fase de operación o mantenimiento** del producto.

    e) Apartado 8. Incluye un listado de la documentación que ha sido referenciada a lo largo del presente documento.

    f) Apartado 9. Incluye un listado de las abreviaturas empleadas a lo largo del presente documento.

    g) Anexo 1. Incluye una tabla con los eventos auditables y ejemplos de los mismos.

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

12. Para utilizar *Secret Server* (SS), es necesario descargar la versión correcta (10.1), que se encuentra disponible en la web de Thycotic (archivo *ThycoticSetup.exe*).
13. Se pueden encontrar los hashes SHA-256 disponibles en el sitio web de Thycotic. Para **verificar la integridad** del ejecutable, ejecutar el comando *Get-FileHash* en *PowerShell* sobre el fichero y comprobar que el hash obtenido a partir de este fichero coincide con el valor del hash oficial publicado.

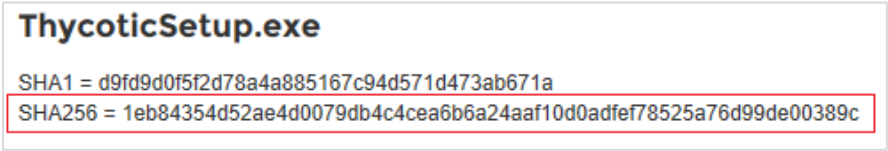


Ilustración 4 1. Valores hash en el sitio web.

14. El segundo paso que debe realizarse para comprobar la autenticidad del instalador es **verificar el certificado** para confirmar que está firmado por Thycotic. Los pasos para verificar el certificado son los siguientes:
    - Hacer clic derecho en el fichero *ThycoticSetup.exe* y seleccionar *Propiedades*.
    - Ir a la pestaña *Firmas digitales* y comprobar que el nombre del firmante es *Thycotic Software*, anotar la fecha y hora de la firma.
    - Seleccionar la entrada en la lista de Firmas y hacer clic en *Detalles*.
    - Hacer clic en *Ver Certificado*. Comprobar que ha sido emitido para *Thycotic Software* y que la *fecha y hora* de la firma anotada anteriormente, se encuentra dentro del intervalo de validez (*Valid Desde.. hasta)*.
    - En la pestaña *Detalles* del Certificado, comprobar que el campo *Uso mejorado de claves (Enhanced Key Usage)* indica que la clave es válida para la firma del código.
    - Seleccionar el campo *Información de error extendida* (*Extended Error Information)* y comprobar que el estado de revocación del certificado es *Correcto*.
    - Pasar a la pestaña *Ruta de Certificación (Certification Path)* y comprobar que cada certificado de la cadena por encima de *Thycotic Software* es válido.

4.2 SQL SERVER

15. Debe instalarse y configurarse *SQL Server* antes de realizar la instalación de *Secret Server Government Edition.*

16. Los pasos para instalar SQL Server y SQL Server Management Studio se describen en el artículo *https://thycotic.force.com/support/s/article/Adv-Install-SQL-2016*.
17. Una vez instalados ambos, se debe crear una cuenta de usuario SQL server para *Secret Server*. Para ello:
    - Abrir *Control Panel > System and Security > Administrative Tools* y hacer doble clic en *Computer Management*.
    - Expandir la carpeta *Local Users and groups* y hacer clic derecho en *Users (usuarios)* y seleccionar *New User.*
    - Proporcionar el nombre deseado y una contraseña segura que cumpla con la política de contraseñas.
    - Desactivar el valor predeterminado *User must change password at next logon* y activar *Password never expires*.
    - La cuenta se añade como un usuario en SQL Server Management Studio y se guardan sus credenciales en un archivo cifrado durante la instalación de Secret Server.
    - Añadir la cuenta de usuario creada a SQL Server, con SQL Server Management Studio.
    - Crear la cuenta de servicio (*service account*) para utilizar *Windows Authentication* para acceder a la base de datos SQL. Esta cuenta debe tener el **rol de *dbcreator***.

5. FASE DE INSTALACIÓN

5.1 INSTALACIÓN DE SECRET SERVER

18. El servidor web en el que se va a instalar *Secret Server* debe ser dedicado. Es decir, no se recomienda utilizar este servidor para otro tipo de aplicaciones.
19. El instalador automático, verifica la existencia de los siguientes componentes en el entorno:
    - *Microsoft .NET 4.6.2+ Framework* o posterior.
    - Roles de *Application* y *Web Server* habilitados en IIS. Certificado SSL.
    - Licencia *SQL* (se requiere *login* con derechos *dbcreator*).
20. Al ejecutar el instalador, en caso de no tener instalado un servidor SQL en el entorno, dará la opción de instalar *SQL Express.* ***SQL Express*** **solo está dirigido a entornos de pruebas** y no se recomienda su uso en producción. Se debe instalar SQL de la forma descrita en el apartado 4.2 SQL Server.
21. En caso de no tener instalado un certificado SSL, el instalador creará e instalará un certificado auto firmado. **No se recomienda el uso de este tipo de certificados, sino un certificado firmado por una CA de confianza** (ver apartado 6.2 Certificados X.509 V3).
22. En https://thycotic.force.com/support/s/article/SS-Installing-Secret-Server-Government-Edition se encuentra la descripción detallada de la instalación de *Secret Server*. A continuación, se incluyen algunos de los aspectos importantes a tener en cuenta.
23. Ejecutar el instalador. Al llegar al apartado *DB Server,* seleccionar la opción *Connect to an existing SQL Server*. Proporcionar el nombre de servidor o la dirección IP del servidor SQL creado.
24. Seleccionar el modo de autenticación *Windows authentication using Service Account*, lo cual llevará a una nueva pestaña llamada *Account*. En esta introducir las credenciales de la cuenta configurada previamente en el apartado 4.2 SQL Server.
25. El instalador realiza una serie de comprobaciones sobre componentes y parámetros que son necesarios. Entre ellos:
    - ***FIPS Encryption Enabled*** y ***Suitable FIPS Configuration***. Estos parámetros indican que Windows está configurado para utilizar, únicamente, algoritmos y funciones criptográficas del módulo criptográfico validado según el estándar FIPS 140-2. Estos algoritmos y funciones criptográficas son compatibles con la guía CCN-STIC-807.
    - ***HTTPS Binding*** (el certificado está correctamente asignado al servicio HTTPS).
26. Si el chequeo de estos parámetros da error durante la instalación, hacer clic en *Fix Issues.* Si tras esto sigue dando error, cerrar el instalador y volver a iniciarlo. En

caso de que el chequeo de *FIPS Encryption Enabled* continúe fallando, se puede habilitar de forma manual (ver apartado 6.1.2 Modo FIPS).

27. En la pestaña *Ciphers*, se recomienda seleccionar *Use only these TLS cipher suites* y marcar las siguientes cipher suites:

    TLS_RSA_WITH_AES_128_CBC_SHA
    TLS_RSA_WITH_AES_256_CBC_SHA
    TLS_RSA_WITH_AES_128_CBC_SHA256
    TLS_RSA_WITH_AES_256_CBC_SHA256
    TLS_RSA_WITH_AES_256_GCM_SHA384
    TLS_RSA_WITH_AES_128_GCM_SHA256

28. **Continuando con la instalación, solicita unas credenciales para crear la cuenta de administrador local de *Secret Server* con la que se llevará a cabo toda la configuración de usuarios y características del producto**. Se recomienda una contraseña de 12 caracteres o superior incluyendo tanto números como caracteres especiales.

29. Finalmente, es necesario añadir permisos adicionales a la carpeta de Secret Server. Para ello, ir a la carpeta en la que se creó el sitio web (por defecto *C:\inetpub\wwwroot\SecretServer*). Hacer clic con el botón derecho del ratón en el nombre de la carpeta, seleccionar *Properties > Pestaña Security > botón Edit*, y clic en *Add* para agregar la cuenta configurada previamente en el apartado 4.2 SQL Server. Si no están ya marcadas, macar las casillas *Allow* junto a los permisos "*Read and Execute*", "*List Folder Contents*" y "*Read*".

5.2 INSTALACIÓN CLAVES DE LICENCIA

30. Tras la instalación de *Secret Server* tendrán que instalarse las claves de licencia de la organización cuando se realice el primer *login* con la cuenta de administrador local creada.

31. Se necesitan tres claves de licencia distintas. Una para la *Secret Server Edition* que está utilizando, otra para Soporte y una para Usuarios.

32. Para instalar las claves es necesario desplazarse a *Admin > Licenses*, hacer clic en *Install New License*. Para instalar varias a la vez hacer clic en *Bulk entry Mode*.

33. Para activar las licencias recién instaladas, hacer clic en el botón *License Activation*, introducir los campos necesarios y hacer clic en *Activate*.

34. El detalle de la configuración de Licencias se puede consultar en el *Licensing* de la guía *Secret Server Administration Guide [REF1].*

6. FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

35. La configuración del modo de operación seguro en *Secret Server Government Edition* se realiza durante el proceso de instalación, de forma automática (ver apartado 5.1 Instalación de Secret Server). El modo de operación seguro, se obtiene cuando ciertas opciones estén correctamente habilitadas y configuradas. A continuación, se resumen los pasos principales para verificar que la configuración es correcta.

6.1.1 OPCIONES DPAPI ACTIVADAS

36. DPAPI (*Data Protection API*) es una API criptográfica que existe en los sistemas operativos Windows. Permite cifrar datos y ficheros de configuración usando la clave de máquina (*machine key*). Con la opción DPAPI activada, se protege la clave de cifrado AES utilizada por *Secret Server* para cifrar los datos sensibles almacenados en el servidor (las credenciales de administrador y los secretos).
37. Para comprobar que está activado el cifrado DPAPI:
38. Desplazarse hasta *Admin > Configuration > Security*.
39. Comprobar que existe el botón *Decrypt Key to not Use DPAPI*. Si DPAPI no se encontrase activado, este botón mostrará *Encript Key to Use DPAPI*. En dicho caso, activarlo.

6.1.2 MODO FIPS ACTIVADO

40. *Secret Server* utiliza las funcionalidades criptográficas proporcionadas por la biblioteca de primitivas criptográficas de *Windows*. Concretamente, *Windows Server 2016 Standard Edition*, utiliza *Cryptographic Primitives Library (bcryptprimitives.dll and ncryptsslp.dll)*. Este módulo cumple con el estándar FIPS 140 (*Cryptographic Module Validation Program, CMVP*). Este módulo criptográfico utiliza algoritmos FIPS-Approved y acordes también con los requisitos establecidos en la CCN-STIC-807.
41. Para verificar que se encuentra activado el módulo criptográfico FIPS:
    - Desplazarse hasta *Admin > Configuration > Security*.
    - Comprobar que la línea de *Enable FIPS Compliance* está configurada como *Yes*.
42. En caso de que no estuviese activado, se puede activar de forma manual en el servidor Windows:
    - Ir a *Windows Local Security Policy Editor* (secpol.msc).
    - Utilizando el panel izquierdo, navegar hasta *Security Settings > Local Policies > Security Options*.

- Ir a las propiedades de *System Criptography: Use FIPS Compliant algorithms for encryption, hashing and signing…*
- Seleccionar *Enable* y después *OK*.
- Reiniciar el servidor con *iisreset*.

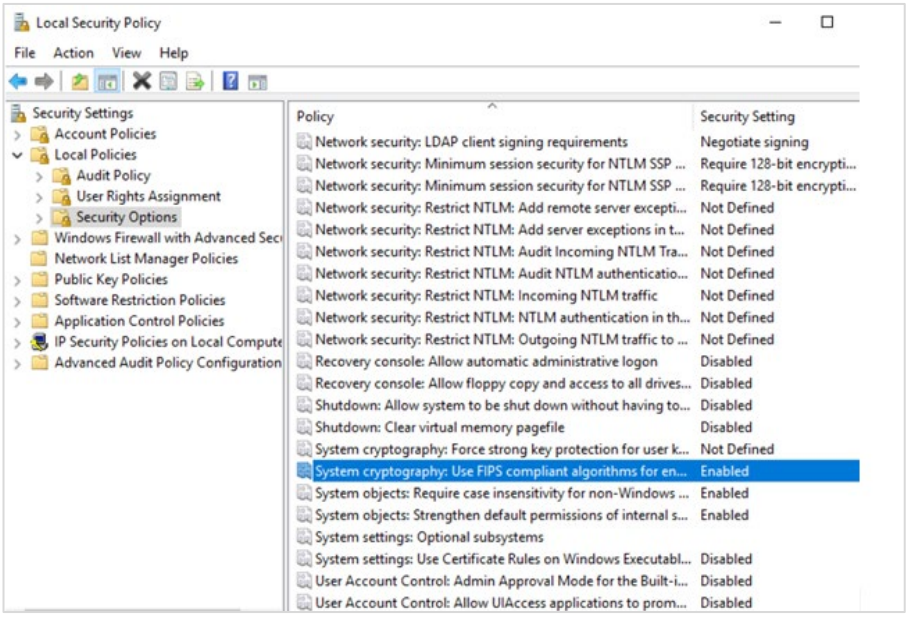


Ilustración 6-1. Modo FIPS habilitado en Windows.

6.1.3 HTTPS / TLS

43. Debe configurarse *Secret Server* para que haga uso de HTTPS para todas las conexiones al sitio web. Para ello:

    - Desplazarse a *Admin* > *Configuration* > *Security* y hacer clic en *Edit*.
    - Activar la casilla *Force HTTPS/SSL*, seguida de *Enable HSTS*.
      HTST (*Strict Trasport Security*) introduce una capa adicional de seguridad en HTTPS. Permite a Secret Server informar a los navegadores (browsers) de que sólo será accesible a través de HTTPS. Con este parámetro activo, los usuarios serán redireccionados por el navegador, al sitio habilitado HTTPS.
      Además del check de HSTS está el parámetro *Maximum Age* que especifica, en segundos, el tiempo que esta política estará activa. Se recomienda configurar este parámetro al máximo tiempo posible (1 año, 31.536.000 seg). Esto significa que, incluso si el parámetro HSTS no estuviese activado, el navegador continúa redireccionando al sitio HTTPS durante ese tiempo.

44. Para utilizar TLS 1.2, se debe desactivar el uso de TLS 1.0 y TLS 1.1 de forma que IIS no intente negociar estas versiones de protocolo:

- Acceder al editor de registros de Windows (*regedit*).
- Localizar la siguiente clave de registro: *HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server*
- Hacer clic en *Add Value* en el menú *Edit* para cada subclave.
- Hacer clic en *DWORD* en la lista *Data Type* para cada subclave.
- Escribir *Enabled* en el cuadro *Value Name* para cada subclave y a continuación hacer clic en *OK*.
- Escribir 00000000 en el *Binary Editor* para ajustar el valor de la nueva clave a "0".
- Hacer clic en *OK* y reiniciar el servidor.
- Realizar los mismos pasos con la clave de registro correspondiente a TLS 1.1.

45. Algunas de las cipher suites utilizadas por TLS, hacen uso de Diffie-Hellman (DH) como mecanismo de intercambio de claves. Para lograr una seguridad equivalente a 128 bits, es necesario el uso de parámetros DH de, al menos, 3072 bits. Esto se logra con el siguiente comando:

reg add "HKey_Local_Machine\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\Diffie-Hellman" /f /v ServerMinKeyBitLength /t REG_DWORD /d 0x00000C00

6.2 CERTIFICADOS X.509 V3

46. Los certificados utilizados en *Secret Server* deben seguir el estándar de certificado digital X.509v3. **No se recomienda el uso de certificados autofirmados. Se recomienda usar certificados firmados por una CA (*Certificate Authority*) de confianza.**

47. A continuación, se indican los aspectos a tener en cuenta a la hora de instalar y configurar los certificados.

6.2.1 INSTALACIÓN DE UN CERTIFICADO CA RAÍZ EN TRUST STORE

48. Para llevar a cabo la autenticación de servidor cuando los usuarios se conecten a *Secret Server* por HTTPS, es necesario instalar en el servidor web *Secret Server* un certificado emitido por una autoridad de certificación (CA) de confianza. A su vez, el certificado raíz de la CA emisora (*root* CA) deberá instalarse en todos los equipos de usuario para que confíen en el certificado del servidor.

49. Para instalar el certificado CA raíz (*root* CA) en los equipos de usuario, existen las siguientes opciones:

- Importarlo al almacén de certificados *Trusted People* si se ha utilizado IIS para su creación.
- Si ha utilizado OpenSSL y configurado una CA raíz personalizada (root CA), el certificado de la root CA debe ser importado al almacén de *Trusted People Certification Authorities.*
- Si se usa una CA intermedia (*intermediate CA*), su certificado debe ser importado también al almacén de *Intermediate Certification Authorities*.

50. *Secret Server* también puede comunicarse con otras entidades IT a través de TLS (como servidores *syslog* y LDAP). En este caso *Secret Server* actuará de cliente TLS y debe verificar el certificado del servidor TLS (la entidad IT). Por lo tanto, es necesario importar e instalar también los certificados CA raíz (y CA intermedia), de las CAs emisoras de los certificados de estas entidades.

51. Para instalar estos certificados raíz en el almacén de *Trust Store*, seguir los siguientes pasos:

    - En el equipo abrir mmc.exe, seleccionar *File > Add/Remove Snap-In…*
    - Seleccionar *Certificates > Add*. Seleccionar *Computer Account > Local Computer* y hacer clic en *Finish*.
    - Abrir *Certificates (Local Computer)* y abrir la carpeta *Trusted Root Certification Authorities* desde el panel izquierdo y seleccionar *Certificates*, luego en el panel derecho *Actions > More Actions > All Tasks > Import…*
    - Hacer clic en *Next* y seleccionar el certificado que se desea importar.

    Se pueden seguir los mismos pasos para la instalación de los certificados de las CA intermedias seleccionando *Intermediate Certification Authorities* en lugar de *Trusted Root Certification Authorities.*

6.2.2 INSTALACIÓN DEL CERTIFICADO DEL SERVIDOR SECRET SERVER

52. Para importar el certificado de servidor que va a ser utilizado por IIS:

    - Abrir el *IIS Manager* haciendo *Start > Run > inetmgr > OK*.
    - Hacer clic en el nodo del servidor y hacer doble clic en *Server Certificates*.
    - Hacer clic en *Import* en el panel *Actions*.
    - Seleccionar el certificado que desea usarse e introducir la contraseña, seleccionar *Web Hosting* en *Select Certificate Store* y hacer clic en *OK*.

53. Una vez importado el certificado, es necesario configurar el IIS para que lo utilice:

    - En el *IIS Manager*, hacer clic en *Bindings*.
    - Si HTTPS no se encuentra listado, hacer clic en *Add*, seleccionar *HTTPS*, seleccionar el certificado adecuado y hacer clic en *OK*.
    - Si HTTPS ya está listado, seleccionarlo y hacer clic en *Edit*, y seleccionar el certificado adecuado.

6.2.3 CONFIGURACIÓN DE CERTIFICADOS CLIENTE

54. El servidor *Secret Server* necesitará un certificado de cliente para aquellas conexiones que requieran autenticación de cliente. Estas podrían ser: conexiones con los servidores Directorio Activo (LDAP) y *syslog (Secure TCP Syslog)*, en caso de que estas entidades requieran la autenticación de cliente.

55. Para instalar un certificado de cliente en el servidor web *Secret Server*, seguir los siguientes pasos:

    - Abrir mmc.exe, seleccionar *File > Add/Remove Snap-in…*
    - Seleccionar *Certificates > Add > Computer Account > Local computer > Finish*.
    - Abrir *Certificates* e importar el certificado seleccionando el *almacén/carpeta Personal o Web Hosting > All Tasks > Import…* y seguir el asistente para completar la instalación del certificado.

56. Para permitir que *Secret Server* envíe el certificado de cliente a los servidores remotos, primero tiene que obtener la huella del certificado. Para obtener dicha huella:

    - Hacer clic derecho en el certificado y seleccionar *Open*.
    - Seleccionar la pestaña *Details*.
    - Buscar el campo *Thumbprint* y copiar su contenido.
    - En Secret Server ir a *Admin > Configuration > Security* e ir a *Edit*.
    - En *TLS Auditing* activar *Apply TLS Certificate Chain Policy and Error Auditing*.
    - Hacer clic en *Advanced* y pegar la huella en *Client Certificate Thumbprint*.

6.3 PROTECCIÓN DE LAS COMUNICACIONES

57. La comunicación entre los usuarios y administradores y *Secret Server* se realizará a través de protocolo HTTPS / TLS 1.2. Esta configuración se puede consultar en el apartado 6.1.3 HTTPS / TLS.

58. La comunicación entre *Secret Server* y el servidor externo de auditoría (*syslog*), se realizará a través de protocolo *Secure TCP Syslog/CEF*. Esta configuración se puede consultar en el apartado 6.7.3 Servidor de Auditoría externo.

59. La comunicación entre *Secret Server* y Directorio Activo (AD), se realizará a través de protocolo LDAPS sobre TLS. Esta configuración se puede consultar en el apartado 6.4.2 Autenticación en Dominio.

6.4 AUTENTICACIÓN

60. El producto permite la autenticación de usuarios tanto de forma local, como haciendo uso de Directorio Activo.

6.4.1 AUTENTICACIÓN LOCAL

61. *Secret Server* almacena y gestiona las cuentas de usuarios en una base de datos local. Para realizar la autenticación con éxito, el usuario introducir un nombre de usuario y contraseña válidos. Estas credenciales serán verificadas contra la base de datos interna de usuarios autorizados.

62. Para crear, editar o eliminar una cuenta de usuario local, desplazarse hasta *Admin > Users* y buscar aquellos usuarios cuyo dominio aparece como Local.

63. El detalle de la configuración de usuarios locales se puede consultar en el capítulo *Users* de la guía *Secret Server Administration Guide* [REF1].

6.4.2 AUTENTICACIÓN EN DOMINIO

64. *Secret Server* almacena y gestiona las cuentas de usuarios de dominio. Estas cuentas están sujetas a los cambios realizados en el Directorio Activo. Para realizar la autenticación con éxito, el usuario debe iniciar sesión con una cuenta del Directorio Activo que también exista en *Secret Server*, e introducir las credenciales correctas.

65. Al realizar la autenticación en dominio, *Secret Server* lanza una petición de autenticación al controlador de dominio (Directorio Activo) usando LDAP sobre TLS. Solo se autorizará el acceso tras recibir una respuesta exitosa.

66. El detalle de la configuración de *Secret Server* y Directorio Activo se puede consultar en el capítulo *Active Directory Synchronization* de la guía *Secret Server Administration Guide* [REF1]. A continuación, se indican los aspectos más importantes a tener en cuenta.

67. El acceso de *Secret Server* a Directorio Activo utiliza el protocolo LDAPv3 (RFC 2251).

68. Para poder configurar el uso de Directorio Activo en *Secret Server*, hay que seguir los siguientes pasos:

    a) Crear un *Sync Secret*.

    b) Especificar el dominio contra el que realizar la autenticación. Configurar el uso de TLS en la conexión con el Directorio Activo.

    c) Establecer *Synchronization Groups*.

    d) Activar *Active Directory Sync*.

    A continuación, se indican con más detalle estos pasos.

69. Para la creación de un *Sync Secret*, se requiere disponer de las credenciales de administrador de dominio (o de una cuenta con permisos de lectura sobre todos los objetos del Directorio Activo). Los pasos son los siguientes:

    - Dirigirse a *Create Secret Widget* en el panel de control.

- En el apartado *Create New*, seleccionar *Active Directory Account* desde la lista desplegable.

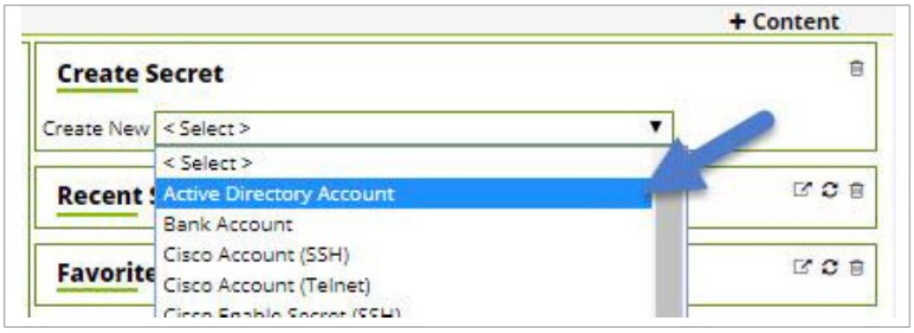


Ilustración 6-2. Creación de Sync Secret (I).

- Añadir un secreto y proporcionar un *Domain Name, Username* y *Password* para el *Sync Secret* que podrá acceder al directorio activo con credenciales de Admin. Hacer click en *Save*.

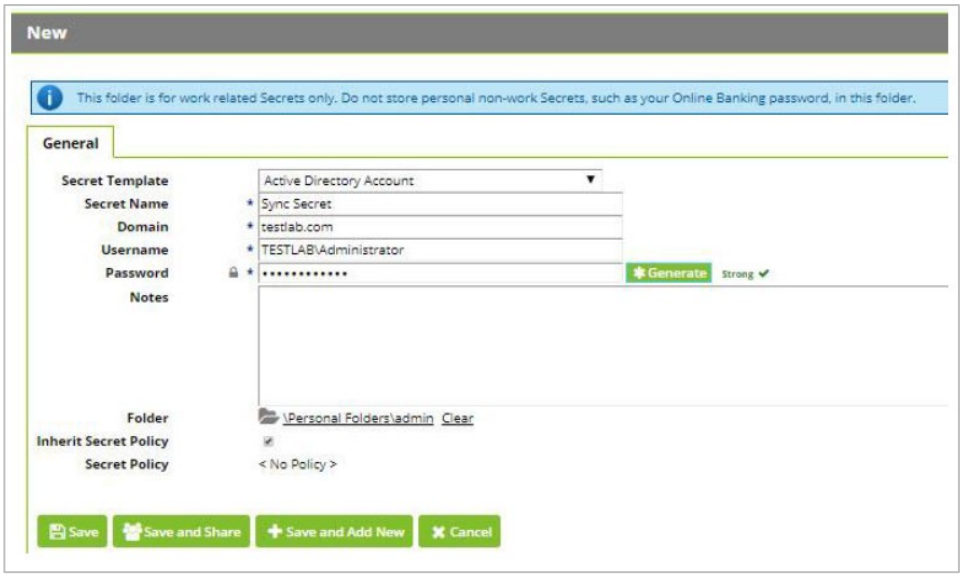


Ilustración 6-3. Creación de Sync Secret (II).

70. Una vez creado el *Sync Secret*, es necesario especificar el dominio y activar la sincronización con el Directorio Activo, de tal forma que todos los cambios en el Directorio Activo se vean reflejados en *Secret Server*, para lo cual:

    - Hacer clic en *Admin > Active Directory*.
    - Una vez en la página de *AD Configuration*, hacer clic en *Edit*.
    - Activar las casillas *Enable Active Directory Integration* y *Enable Synchronization of Active Directory*.
    - En la lista desplegable de *User Account Options* seleccionar *User status mirrors Active Directory (Automatic)*. Hacer clic en *Save*. Esto permite a

Secret Server reflejar de forma automática, cualquier cambio realizado en Directorio Activo.

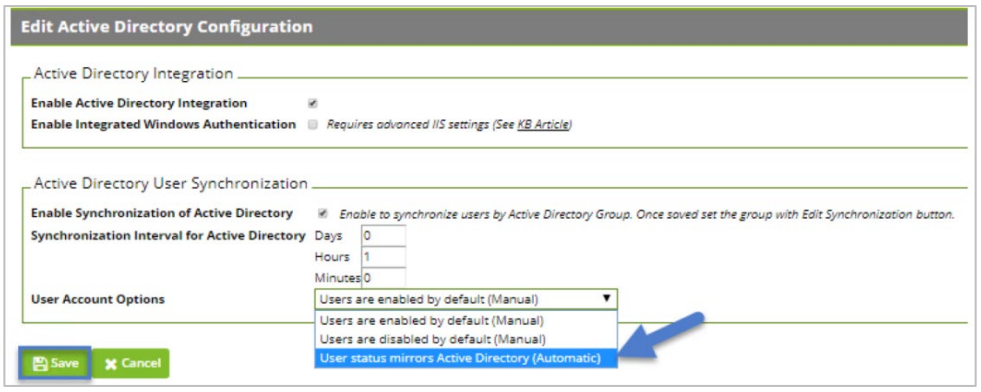


Ilustración 6-4. Activar sincronización con AD (I).

- Hacer clic en *Edit Domains* > *Create New*. Proporcionar un Nombre de Dominio FQDN (*Fully Qualified Domain Name*) y un *Friendly Name*. Activar las casillas "*Active*" y "*Allow Logins From Domain*".
- Seleccionar el *Sync Secret* creado haciendo clic en *No Selected Secret* y buscando el correspondiente.

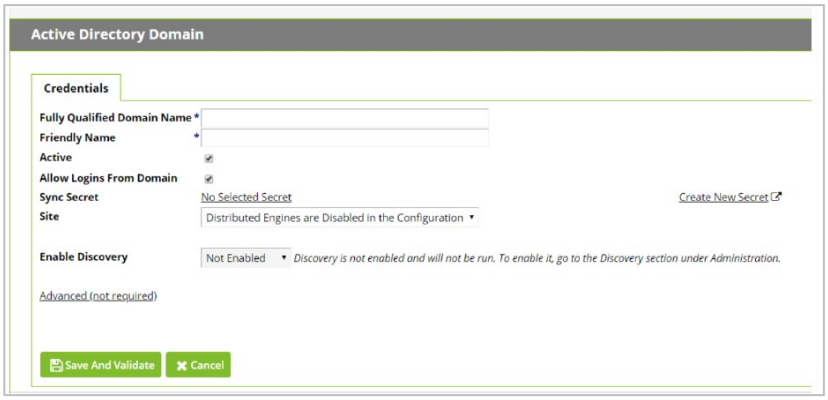


Ilustración 6-5. Activar sincronización con AD (II).

71. Verificar el uso del protocolo LDAPS sobre TLS, que se debe encontrar activado por defecto. No obstante, para comprobar que, efectivamente, está activo:
    - Desde *Admin* > *Active Directory* > *Edit Domains* > *Create New*, pulsar en *Advanced* y comprobar que la opción *Use LDAPS* se encuentra marcada. En caso negativo, activarla.
72. Para configurar la sincronización de grupos:
    - Hacer clic en *Edit Synchronization* en la página de *Active Directory Configuration*.
    - En la lista de *Available Groups* se encuentran todos los grupos accesibles en el dominio de Directorio Activo especificado. Debe seleccionarse el

grupo deseado que contenga las cuentas de Directorio Activo para los usuarios que queremos crear en Secret Server, y moverlo al área de *Syncronized Groups*. Una vez hecho esto, *Save*.

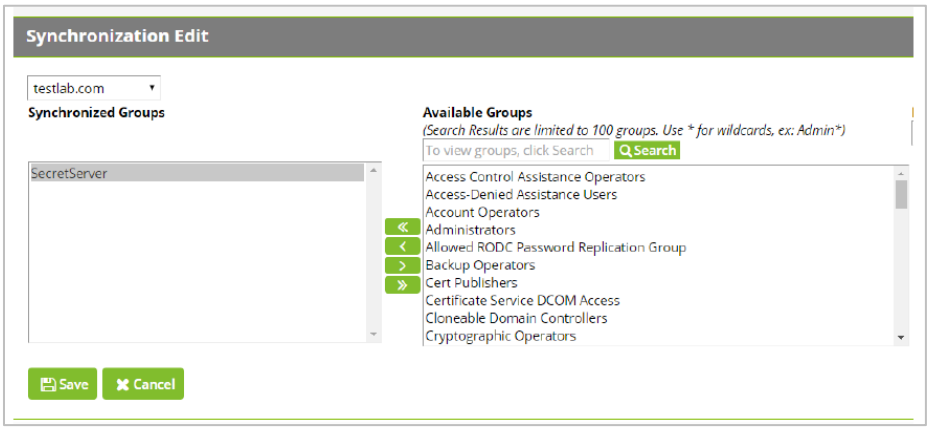


Ilustración 6-6. Sincronización de grupos AD.

73. La actualización de credenciales se producirá en Directorio Activo y se sincronizarán en *Secret Server*, según una planificación (*schedule*). Se puede forzar una sincronización manual en cualquier momento, a través *de Admin > Active Directory > Synchronize Now*. No se podrán añadir o modificar credenciales de Directorio Activo a través de *Secret Server*.

74. En caso de que la conexión entre *Secret Server* y Directorio Activo falle, Secret Server genera un registro de auditoría al respecto y notifica al usuario el fallo. *Secret Server* no intentará la reconexión TLS de forma automática. Lo intentará la próxima vez que el usuario intente conectarse de nuevo con el AD.

6.5 ADMINISTRACIÓN

75. Tanto la administración del producto, como el acceso por parte de los usuarios, se realiza a través de la interfaz gráfica GUI del servidor IIS de *Secret Server.*

76. En el apartado 6.1.3 HTTPS / TLS, se encuentra cómo configurar el uso de HTTPS/TLS para estas conexiones.

77. En el proceso de instalación se crea la cuenta de administrador local con la que se llevará a cabo la configuración inicial de *Secret Server* (ver apartado 5.1 Instalación de *Secret Server*). Con esta cuenta se pueden crear otras cuentas de administración si fuese necesario, así como las cuentas de usuarios.

6.5.1 PARÁMETROS DE ADMINISTRACIÓN

78. En *Secret Server* se pueden configurar, desde el módulo de administración, varios parámetros relacionados con funciones de seguridad del producto. Se puede encontrar una lista detallada de estos parámetros en el capítulo *Administration Tabs* de la guía *Secret Server Administration Guide* [REF1]. A continuación, se indican los más relevantes.

79. En la página *Security Tab* se deberán activar las siguientes opciones:
    - **Enable FIPS Compliance**: Activa el modo de operación seguro (FIPS). Se encuentra activado por defecto. Ver apartado 6.1.2 Modo FIPS activado.
    - **Enable HSTS**: Activa la política HSTS, la cual obliga a que todas las conexiones con la GUI hagan uso de HTTPS. Ver apartado 6.1.3 HTTPS / TLS.
    - **Encrypt Key using DPAPI**: Permite proteger la clave de cifrado de Secret Server, con el cifrado DAPI (que usa la clave de máquina, machine key). Ver apartado 6.1.1 Opciones DPAPI activadas.
    - **Force HTTPS/SSL**: Obliga el uso de HTTPS, por lo que los usuarios no pueden acceder usando HTTP. Esto protege la confidencialidad de las credenciales, obligando a que se envíen cifradas. Ver apartado 6.1.3 HTTPS / TLS.
    - **Frame Blocking**: Evita la carga de la página de Secret Server en un iFrame.
80. En la página *General Tab* se recomienda activar las siguientes opciones:
    - **Allow Automatic Checks for Software Updates**: Se envía una notificación a los administradores cuando se encuentra una actualización disponible.
    - **Allow Syslog/CEF Logging**: Permite a Secret Server enviar los logs de auditoría a un servidor syslog externo.
81. En la página *General Tab* se deben activar las siguientes opciones:
    - **Force Inactivity Timeout**: Obliga a los usuarios a iniciar sesión de nuevo tras un periodo de inactividad.
    - **Force Password Masking**: fuerza a que todos los cuadros de texto de los secretos correspondientes a contraseñas, estén enmascarados.
    - **Maximum Time for Offline Access on Mobile Devices:** Cantidad de tiempo que puede estar desconectado un dispositivo móvil antes de que Secret Server elimine sus datos de caché.
82. En la página *Login Tab* se recomienda configurar las siguientes opciones:
    - **Allow AutoComplete**: El auto completado es una característica proporcionada por los navegadores que recuerda y rellena automáticamente los formularios de *login. Secret Server* permite activar y desactivar esta característica en su página de *login*. Es recomendable desactivarlo para aumentar la seguridad de las credenciales y evitar inicios de sesión no deseados.

- **Allow Remember me**: se recomienda desactivar esta opción. Esto impide que aparezca el check de *Remember me* en la página de login.
- **Enable Login Failure CAPTCHA**: Al activarlo, se obliga a resolver una imagen CAPTCHA si el usuario realiza uno o más inicios de sesión erróneos. Junto con el bloqueo de las cuentas, ayuda a prevenir los ataques de fuerza bruta contra las credenciales de los usuarios.
- **Maximum Login Failures**: Define el número de inicios de sesión erróneos que pueden realizarse antes del bloqueo de la cuenta.
- **Require Two Factor for these Login Types**: Obliga el uso de doble factor de autenticación para los tipos de inicio de sesión seleccionados. Es recomendable activarlo para incrementar la seguridad de las cuentas de usuario.
- **Visual Encrypted Keyboard Required**: Obliga el uso del teclado en pantalla para los inicios de sesión. Esto se utiliza para evitar ataques del tipo "keylogger", los cuales registran las pulsaciones del teclado.

83. En la página *Local User Passwords Tab* se recomienda configurar la política de contraseñas apropiada para la organización. Ver apartado 6.5.3 Política de Contraseñas.

6.5.2 CUENTAS DE USUARIOS

84. Los roles que ofrece el sistema se pueden consultar en *Admin* | *Roles*. Hay tres (3) roles por defecto:
    - Administrador.
    - Usuario.
    - Usuario de solo lectura.
85. Los permisos asociados a cada rol, se pueden ver seleccionando el rol > Edit. Son los indicados en la siguiente tabla:

ROL	FUNCIONES DE GESTIÓN
Usuario de Solo Lectura	Buscar y listar secretos
Usuario	Utilizar secretos / Iniciar sesión
Usuario	Solicitar acceso a secretos
Administrador	Crear, ver, finalizar, editar y asignar secretos
Administrador	Realizar operaciones globales sobre secretos
Administrador	Crear y gestionar grupos
Administrador	Crear y gestionar roles, asignar roles a usuarios

ROL	FUNCIONES DE GESTIÓN
Administrador	Crear y gestionar contenedores (carpetas)
Administrador	Crear y gestionar la política de secretos
Administrador	Configurar las funciones de seguridad del producto.
Administrador	Crear, gestionar y desbloquear cuentas locales
Administrador	Configurar IIS, SQL y syslog
Administrador	Actualizar el producto

Tabla 6-1. Funciones de gestión de los roles.

86. En caso de que deba haber más de un administrador, debe configurarse una cuenta para cada uno, no deben utilizarse cuentas compartidas.

87. Para asociar un rol a un usuario, desplazarse a la pestaña *Admin* > *Roles* y hacer clic en *Assign Roles*.

88. Se recomienda no configurar ningún rol por defecto para los usuarios nuevos. De esta forma se evita asignar más privilegios de los necesarios. Para ello, desplazarse a *Admin* > *General* > sección *User Experience*. Seleccionar "*None*" en la opción "*Default New User role*".

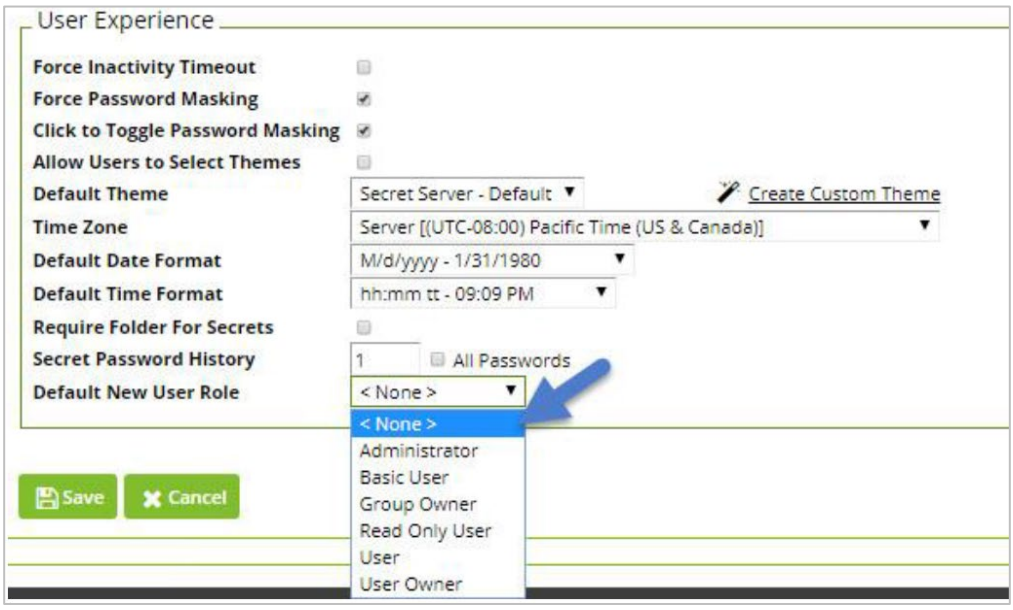


Ilustración 6-7. Configuración de rol para nuevos usuarios.

89. Para gestionar un usuario local, hacer click en el *Username* para ver los detalles. Secret Server mostrará información incluyendo el nombre de usuario, email address, Dominio al que está afiliado, si el usuario tiene doble factor de autenticación (*Two Factor*), si el usuario está habilitado para conexión (*Enabled*) o, por el contrario, está bloqueado (*Locked out*), si se trata de una cuenta de usuario o de aplicación (*Application Account*). Desde la página de *View user* se puede ver

también la información del Grupo y Roles para el usuario. Para editar y modificar estos datos, y para bloquear o desbloquear el usuario, utilizar el botón *Edit*.

90. El detalle de la configuración de usuarios se puede consultar en el capítulo *Users* de la guía *Secret Server Administration Guide* [REF1].

6.5.3 POLÍTICA DE CONTRASEÑAS

91. Se recomienda definir una política de contraseñas y aplicarla por defecto a todas las cuentas de usuarios locales. La política de contraseñas definida en Secret Server, **solo afecta a los usuarios creados localmente**, no a aquellos sincronizados con el Directorio Activo. Es recomendable, por lo tanto, que la política de contraseñas del directorio activo esté alineada con la de Secret Server.
92. La política de contraseñas se define desde *Admin > Configuration > Local User Password > Edit*.
93. Se recomienda que las contraseñas estén formadas por subconjuntos de los siguientes grupos: letras en mayúscula, letras en minúscula, números y caracteres especiales. Los parámetros a definir serán los siguientes:
    - El tamaño mínimo de las contraseñas. Recomendado 12 caracteres.
    - Requisitos de vigencia y expiración de contraseñas. Recomendado 30 días.
94. Para asignar el valor del número de contraseñas antiguas que no pueden reutilizarse, activar el check de *Enable Local User Password History* y rellenar el número de contraseñas antiguas que queremos bloquear. Si seleccionamos el check "*All*", bloqueará todas las contraseñas anteriores que haya utilizado el usuario.

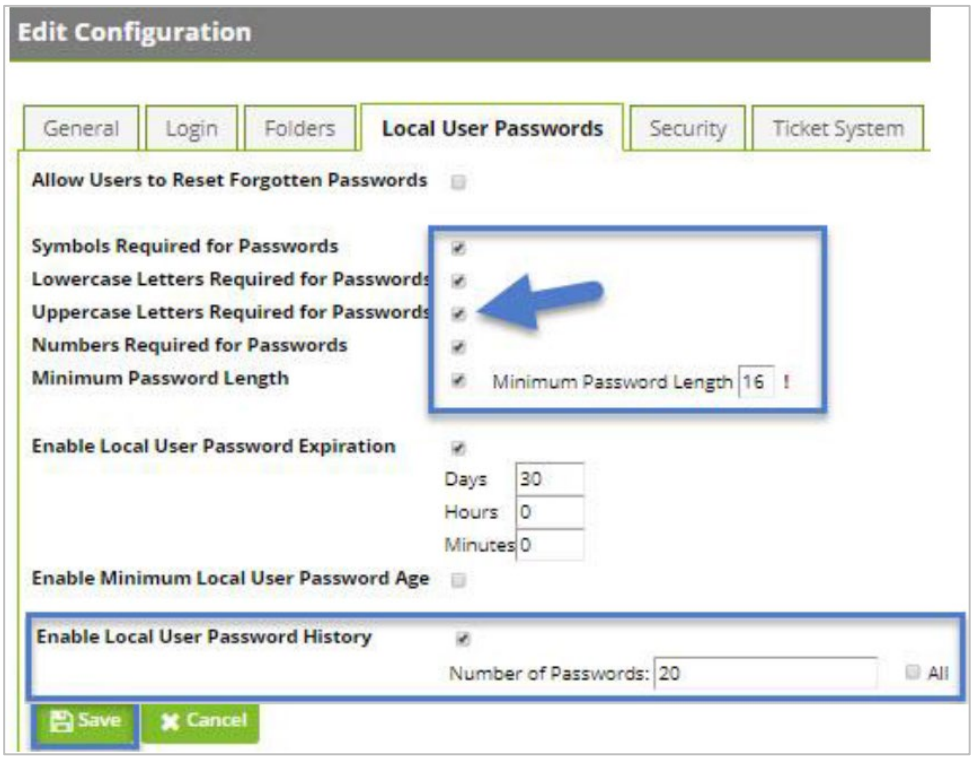


Ilustración 6-8. Configuración de la política de contraseñas.

95. Para resetear una contraseña:

    - Si se trata de una cuenta de Directorio Activo, esto debe hacerse desde Directorio Activo.

    - Si se trata de una cuenta local de Secret Server, seleccionar el usuario en *Admin > User* y seleccionar *Edit*. Escribir una nueva contraseña (dos veces). Esta contraseña es temporal y debe proporcionarse al usuario. Cuando este inicie sesión con esta nueva contraseña, Secret Server le pedirá el cambio de contraseña.

96. **Se deberá configurar un número máximo de intentos fallidos de autenticación**, tras lo cual la cuenta del usuario será bloqueada durante 60 minutos. Esta configuración se realiza desde *Admin > Configuration > Login > Edit*. Rellenar el "*Maximum Login Failures*" (por defecto estará a 5).

97. Para desbloquear un usuario que haya alcanzado en número máximo de intentos fallidos de autenticación, desde *Admin > Users*, seleccionar el usuario y pulsar *Edit*. Cambiar el valor de *Locked out* a *No*, y seleccionar *Save*.

98. **No se deberá configurar la característica de recordar la contraseña del usuario**. Para ello, desde *Admin > Configuration > Login*, verificar que la opción "*Allow Remember Me*" está a NO.

99. Se recomienda configurar un mensaje de aviso y consentimiento en el inicio de sesión (***Login Banner***). Para ello, desde *Admin > Configuration > Login*, dirigirse al final de la página y seleccionar *Login Policy Agreement*. Seleccionar *Edit* y activar

los check de *Login Policy* y *Force Login Policy*. Al habilitar estos *checks*, se mostrará el mensaje de aviso y consentimiento en la página de *login* y se forzará a los usuarios a aceptar esta política para poder proceder al *login*.

100. Este mensaje se puede configurar desde el servidor web de *Secret Server*, abriendo un explorador y editando el fichero "*policy.txt*" (la ruta por defecto de este fichero es *C:\inetpub\wwwroot\SecretServer\policy.txt*). Este fichero se puede editar con un *Notepad* y configurar el texto deseado para el mensaje.

6.5.4 CONFIGURACIÓN DE PARÁMETROS DE SESIÓN

101. A continuación, se indican las recomendaciones respecto a la configuración de los parámetros de sesión.

102. Se deberá configurar un **tiempo de inactividad de sesión**, de forma que transcurrido dicho tiempo, expire la sesión y sea necesario volver a hacer login. Para configurar el tiempo de inactividad de la sesión:

- Desplazarse hasta la pestaña *Admin > Configuration > General* y hacer clic en *Edit*.
- En la sección de *User Experience* activar la casilla *Force Inactivity Timeout.*
- Después ajustar el tiempo de inactividad deseado y hacer clic en *Save*.

103. Se recomienda configurar **restricciones de direcciones IP** para los diferentes usuarios, de tal forma que, si se intenta acceder a la cuenta desde una IP que se encuentre fuera del rango especificado, se deniega el acceso. Para configurar las restricciones de direcciones IP:

- Desplazarse a la pestaña *Admin > More… > IP Adresses* y hacer clic en *Create New*.
- Proporcionar el *IP Address User/Network Name* (nombre descriptivo para el rango de IPs) y el *IP Address Range* (rango de IPs deseado) y hacer clic en *Save*.

104. En *IP Address Range* se pueden introducir IPs individuales (10.0.0.1), un rango de IPs separado por un guion (10.0.0.1-10.0.0.255) y un rango en formato CIDR (10.0.0.0/24). Una vez configurado el rango de IPs, es necesario asignarlo a uno o varios usuarios:

- Desplazarse a *Admin > Users*. Seleccionar el usuario.
- Hacer clic en *Change IP Restrictions* y aparecerá el menú para seleccionar la restricción IP, pulsar *Save*. En caso de no seleccionar ninguno el usuario podrá acceder desde cualquier dirección IP.
- Si se quiere aplicar la restricción de IP a un grupo de usuario, seleccionar *Admin > Groups > Create New*. Seleccionar los usuarios o grupos de usuarios a los que aplicar la restricción y moverlos a la izquierda, a la

sección *Members*. Hacer click en el botón de *Change IP Restrictions*, seleccionar la restricción IP a aplicar y aplicar *Save*.

6.6 GESTIÓN DE LOS SECRETOS

105. Los objetos principales que maneja y protege Secret Server son los Secretos. Un secreto se define como una pieza de información sensible que necesita ser protegida. Normalmente se trata de credenciales de acceso a recursos IT, pero un secreto puede consistir también en un fichero sensible (claves privadas, certificados, licencias, documentos, etc.), información de contacto, etc.

106. En el presente apartado se indican los aspectos más relevantes a tener en cuenta sobre la creación y gestión de los secretos. Para obtener más información, consultar el capítulo *Secrets* de la guía *Secret Server Administration Guide [].*

107. Los secretos se crean usando plantillas (*Secret Templates*). Hay una plantilla para cada tipo de secreto con una serie de objetos que definen el secreto.

108. Las plantillas se pueden activar y desactivar en *Admin > Secret Templates*, a través del botón *Activate Templates*. Las plantillas más comunes son las siguientes:

    - *Active Directory Account* (Cuenta de *Active Directory*).
    - *Combination Lock* (Cerradura de combinación Numérica).
    - *Contact* (Contacto).
    - *Credit Card* (Tarjeta de Crédito).
    - *Password* (Contraseña).
    - Pin.
    - *Product License Key* (Clave de Licencia del producto).
    - *Security Alarm Code* (Código de Alarma de Seguridad).
    - *Social Security Number* (Número de Seguridad Social).
    - *Unix Account (SSH Key Rotation)* (Cuenta Unix).

    También se pueden crear nuevas plantillas o modificar las existentes.

109. Los secretos cuentan con:

    - Atributos heredados de las plantillas**.**
    - Restricciones de comandos (*Command Restrictions*). Solo para el caso de sesiones SSH, los administradores pueden crear menús de comandos específicos de forma que los usuarios no lanzarán los comandos directamente sobre el recurso IT.
    - Campos de datos (*Field Data*). Cada campo dentro del secreto puede ser tipo texto, contraseña o notas. Los campos de contraseña pueden estar

ocultos a los usuarios y ser actualizados de forma automática. Los campos de texto son estándar y pueden incluir información como el dominio o el nombre de usuario.

- Carpetas (*Folders*). Las carpetas almacenan secretos individuales. Los permisos que se apliquen a la carpeta determinan qué usuarios pueden ver los secretos dentro de esa carpeta.
- Requisitos de contraseñas (*Password requirements*). En cada plantilla se pueden especificar requisitos de contraseña que aplicarán a todos los secretos creados con esa plantilla. Los usuarios no podrán introducir contraseñas no cumplan con esos requisitos.
- Identificador de política (*Policy Identifier*). Se pueden configurar políticas que especifiquen ciertos parámetros de seguridad aplicables sobre secretos individuales o sobre carpetas que contengan secretos (*folders*). Por ejemplo, opciones como el cambio automático de contraseñas (*Remote Password Changing AutoChange*) o aprobación de acceso al secreto (*Requires Approval for Access*).

110. Las plantillas de secretos (Secret Templates) determinan:
    - Los campos que tendrán los secretos (*Field parameters)*.
    - La política de expiración de secretos (*Secret Expiration Policy*).
    - La política de cambio de contraseñas (*Password Change Policy*).
    - Requisitos de contraseñas (*Password Strength Policy*).
111. Para crear un secreto:
    - Se utilizará la opción *Create Secret* seleccionando el tipo de secreto a crear, a través de la plantilla.

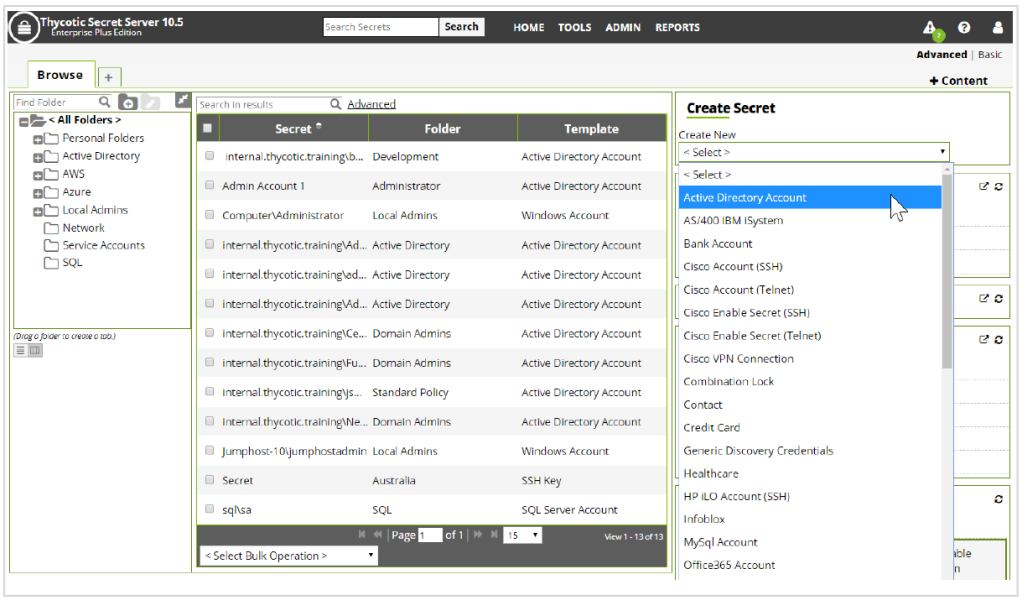


Ilustración 6-9. Crear un secreto (I)

- Se rellenarán todos los datos del secreto.

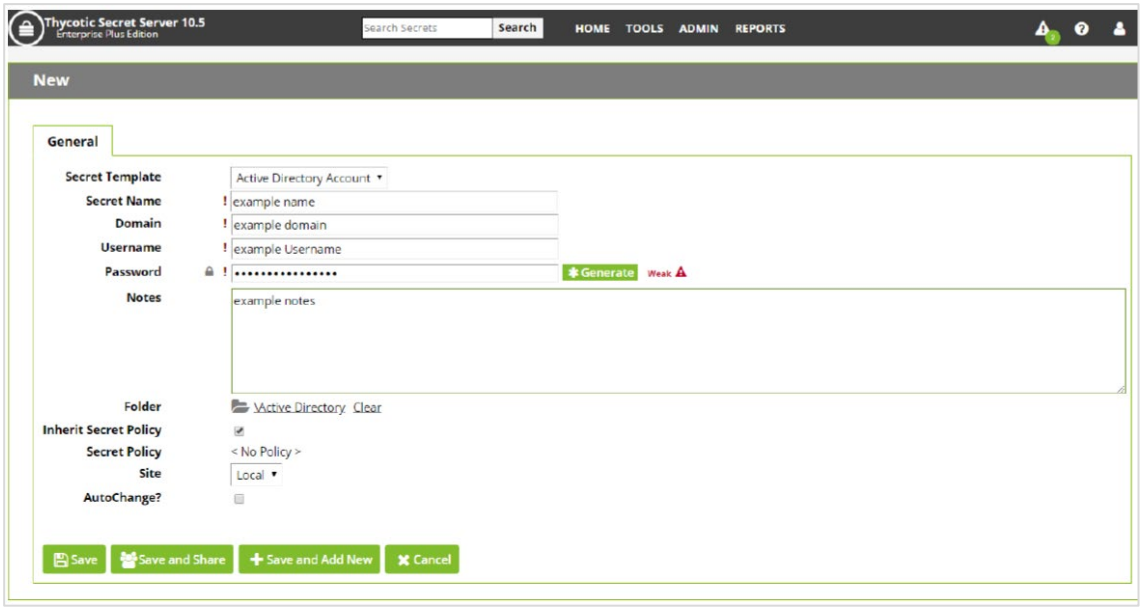


Ilustración 6-10. Crear un secreto (II)

112. Las plantillas tienen asociada una política de contraseñas que aplicará a todos **aquellos campos del secreto que correspondan a contraseñas. Para definir esta** política de contraseñas:

- Desplazarse a *Admin > Secret Templates*. Aparece la pantalla de *Manage Secret Templates*.

- Seleccionar la plantilla deseada y pulsar en *Password Requirements.*

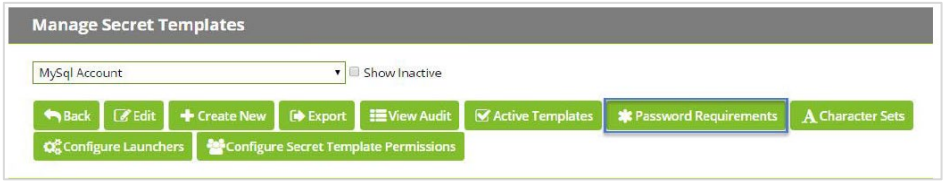


Ilustración 6-11. Requisitos de contraseñas de secretos (I)

- Seleccionar *Default* para especificar los requisitos que tendrán, por defecto, las contraseñas de todas las *Secret Templates* de la organización. Seleccionar *Create New* si queremos crear un requisito de contraseña específico para esta plantilla.

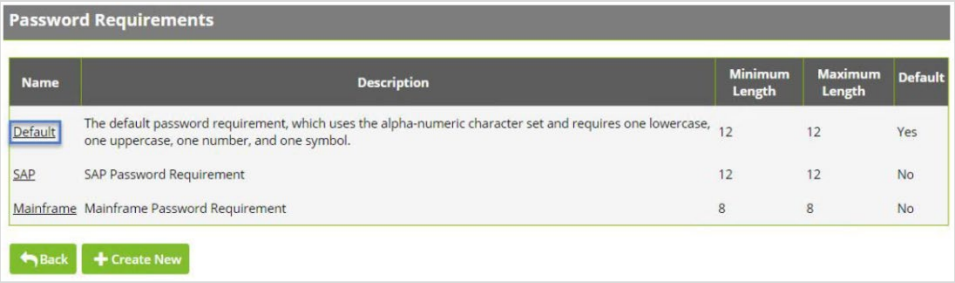


Ilustración 6-12. Requisitos de contraseñas de secretos (II)

- Especificar los requisitos de longitud de contraseña y de tipo de caracteres.
- Estos requisitos de contraseña se forzarán tanto para los secretos creados por los usuarios, como los creados de forma automática por *Secret Server.*

113. Se recomienda, también, forzar a que todos los cuadros de texto correspondientes a contraseñas de los secretos estén enmascarados. Para ello, desplazarse *a Admin > Configuration* y activar *Force Password Masking*. De esta forma se mostrarán asteriscos en estos cuadros, además, por seguridad, el número de asteriscos no corresponderá con la longitud de la contraseña.
114. En la pestaña Security de los secretos, se pueden configurar los siguientes ajustes de seguridad:
    - ***Require Check Out***: impide que dos usuarios accedan simultáneamente al mismo secreto.
    - ***Enable DoubleLock***: el usuario debe introducir una contraseña "doubleLock" para descifrar y ver un secreto. Ver apartado 6.6.4 Uso de DoubleLock.
    - ***Enable Requires Aproval for Access****:* el usuario debe solicitar el acceso y este ser aprobado, para poder ver el secreto.
    - ***Require Comment****:* el usuario debe añadir un comentario cada vez que acceda a un secreto. Este comentario se almacena en los logs de auditoría de ese secreto.
    - ***Enable Session Recording***: activa la característica de grabación de la sesión de usuario. Aplica sólo si la plantilla a la que pertenece el secreto tiene esta característica de grabación (*Launcher*) activada.
    - ***Hide Launcher Password****:* impide a los usuarios con permisos "View", copiar las contraseñas al portapapeles o desenmascarar el cuadro de texto de la contraseña del secreto. Como en el caso anterior, solo aplica a los secretos cuya plantilla tenga la opción de grabación activada (*Launcher*).
    - ***Customize Password Requirement****:* permite definir los requisitos de contraseña (*password requirements*) para todos los cuadros de texto correspondientes a contraseñas dentro del secreto.

115. Para obtener más información al respecto al apartado *Secrets > Secret Security Tab* de la guía *Secret Server Administration Guide [].*

6.6.1 EXPIRACIÓN DE LOS SECRETOS

116. Un secreto expira o caduca cuando uno de sus campos de texto expira. Normalmente, el campo correspondiente a la contraseña. La caducidad del secreto, por lo tanto, se configura en la plantilla correspondiente y para ello se selecciona un campo como el objeto de caducidad. Por ejemplo, la plantilla para cuentas de *Active Directory* puede requerir que se cambie el campo de contraseña cada 90 días. A este campo es al que se añade la caducidad, de forma que, si no ha sido cambiado el secreto, transcurridos los 90 días, se considerará que el secreto ha expirado y aparecerá en el panel de "*Expired Secrets*".

117. Para habilitar la caducidad en una plantilla de secretos:

    - Desplazarse hasta *Administration > Secret Templates*.
    - Seleccionar la plantilla deseada, haciendo clic en *Edit*.
    - Hacer clic en *Change.* Activar la casilla de *Expiration Enabled.*

- Introducir el intervalo de caducidad, así como el campo del secreto que se desea que caduque.

118. Una vez activada la caducidad en las plantillas, queda activada la caducidad para todos los secretos que fueron creados con dicha plantilla, así como los nuevos que se creen. Es posible cambiar el valor de esta caducidad para cada secreto individual en la pestaña *Expiration*, dentro de la página *Secret View*.

119. Para reestablecer un secreto expirado solo es necesario modificar el campo que ha expirado y que requiere ser cambiado. En caso de no saber cuál es el campo expirado, deberá consultarse en la *Secret Template* del secreto.

120. Se puede forzar que un secreto expire de forma inmediata, independientemente de su intervalo configurado. Para ello desde la página de *Secret View*, hacer click en *Expire Now*.

121. El cambio de contraseña cuando el secreto expira, puede ser realizado por Secret Server de forma automática. Para ello se deben habilitar las opciones de *RPC* y *AutoChange* en el secreto (ver apartado 6.6.2 Cambio Remoto de Contraseña (RPC)).

122. Secret Server chequea la existencia de secretos expirados cada minuto. En caso de que esté configurado el cambio remoto automático de contraseña por parte de Secret Server, si un cambio de contraseña ha fallado, Secret Server no intentará cambiarla de nuevo de forma inmediata la próxima vez que chequee los secretos expirados. En lugar de ello, usará el valor de "*Retry Interval*", que indica cada cuánto tiempo debe reintentar el cambio de una contraseña fallida. El intervalo por defecto es de una hora. Para modificarlo:

    - Desde *Admin > Secret Templates*, se selecciona la plantilla y se pulsa *Edit*.

- Desde la página de *Secret Template Designer*, seleccionar *Configure Password Changing*.
- En la página *Secret Template Edit Password Changing*, pulsar *Edit*. Especificar el "*retry interval*" en días, horas y minutos. También se puede ajustar aquí el valor de máximos intentos (*Maximum Attempts*) para indicar a Secret Server que, tras ese número de intentos fallidos, deje de intentar el cambio de contraseña.

6.6.2 CAMBIO REMOTO DE CONTRASEÑA (RPC)

123. La característica de ***Remote Password Changing (RPC)*** permite que Secret Server modifique de forma automática la contraseña del secreto y de su correspondiente cuenta en el recurso IT, para mantener ambas sincronizadas en Secret Server.

124. Esta característica se habilita desde *Admin > Remote Password Changing > Edit*.

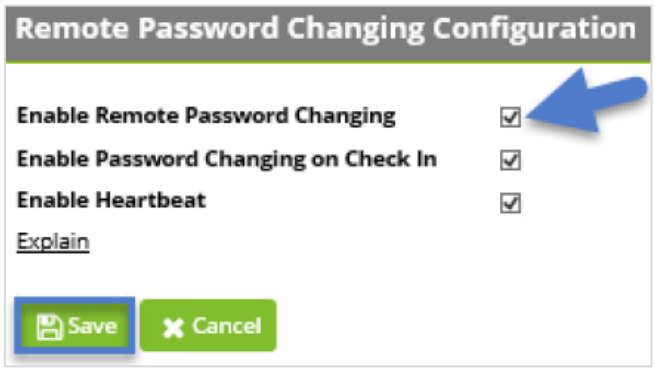


Ilustración 6-13. Activación de RPC

125. Se recomienda también activar las opciones de *Heartbeat y Password Changing on Check in*. *Heartbeat* permite a Secret Server comprobar, cada cierto tiempo configurado, la validez real de las credenciales del secreto en la cuenta del recurso IT. Permite alertar a los administradores en caso de que las credenciales de la cuenta hayan sido cambiadas fuera de Secret Server. *Password Changing on Check in* impide que dos usuarios puedan acceder al mismo secreto a la vez.

126. Cuando RPC está activo y la *Secret Template* lo tiene configurado, en la pestaña *Remote Password Changing* de cada secreto, se pueden configurar los parámetros para RPC.

127. Para que RPC se realice de forma automática y Secret Server pueda modificar la contraseña de un secreto al llegar al tiempo de expiración, debe habilitarse la opción *AutoChange* de forma individual en el secreto. Esto solo lo puede hacer el Owner del secreto.

128. Cuando RPC y AutoChange están habilitados en el secreto, en la pestaña de RPC se observan los parámetros para especificar cuándo debe producirse el cambio automático (*AutoChange schedule*). Así se pueden especificar intervalos en los que no exista actividad en el recurso IT (por ejemplo, por las noches). Hay que

tener en cuenta que el secreto puede haber expirado, pero al no haber llegado el momento indicado en *AutoChange schedule*, Secret Server no ha cambiado la contraseña. Hasta entonces el secreto figura como expirado (*Out of Sync*). Si *AutoChange schedule* es "None", *Secret Server* modifica la contraseña de forma inmediata en cuanto expire.

129. Se puede consultar más información sobre RPC en el capítulo *Remote Password Changing (RPC)* de la guía *Secret Server Administration Guide [REF1].*

6.6.3 SECRETOS DEL TIPO UNIX ACCOUNT (SSH KEY ROTATION)

130. Las plantillas "*Unix Account (SSH Key Rotation)"* se utilizan para crear los secretos correspondientes a cuentas SSH en equipos Unix. Se utilizan claves pública/privada RSA, junto con una "*passphrase*" para proteger la clave privada, y las credenciales de usuario/contraseña.

131. Para configurar la longitud de clave RSA a emplear, desde la plantilla *Unix Account (SSH Key Rotation):*

- Acceder a la pestaña *Admin > Secret Templates* y seleccionar *Unix Account (SSH Key Rotation).*
- Hacer clic en *Edit* y seleccionar el tamaño de clave del menú desplegable en el campo "*SSH Key Bit Size*". **Se recomienda el uso de claves RSA de longitud 3072 bits o superior.**
- Hacer clic en *Save*.

6.6.3.1 CREACIÓN DE UNIX ACCOUNT (SSH KEY ROTATION)

132. Para crear un secreto del tipo *Unix Account (SSH Key Rotation)* se deben seguir los siguientes pasos:

- Desde *Home*, seleccionar la plantilla *Unix Account (SSH Key Rotation)*, seleccionar *Create Secret*.
- Rellenar los datos de la cuenta (secreto): *Secret name, machine* (equipo unix al que nos conectaremos a través del secreto), *username /password*.
- Instalar la clave privada RSA, seleccionando el archivo correspondiente. Rellenar la passphrase, si se ha empleado una para cifrar la clave privada. Instalar, también, la clave pública correspondiente.
- Seleccionar *Save*.

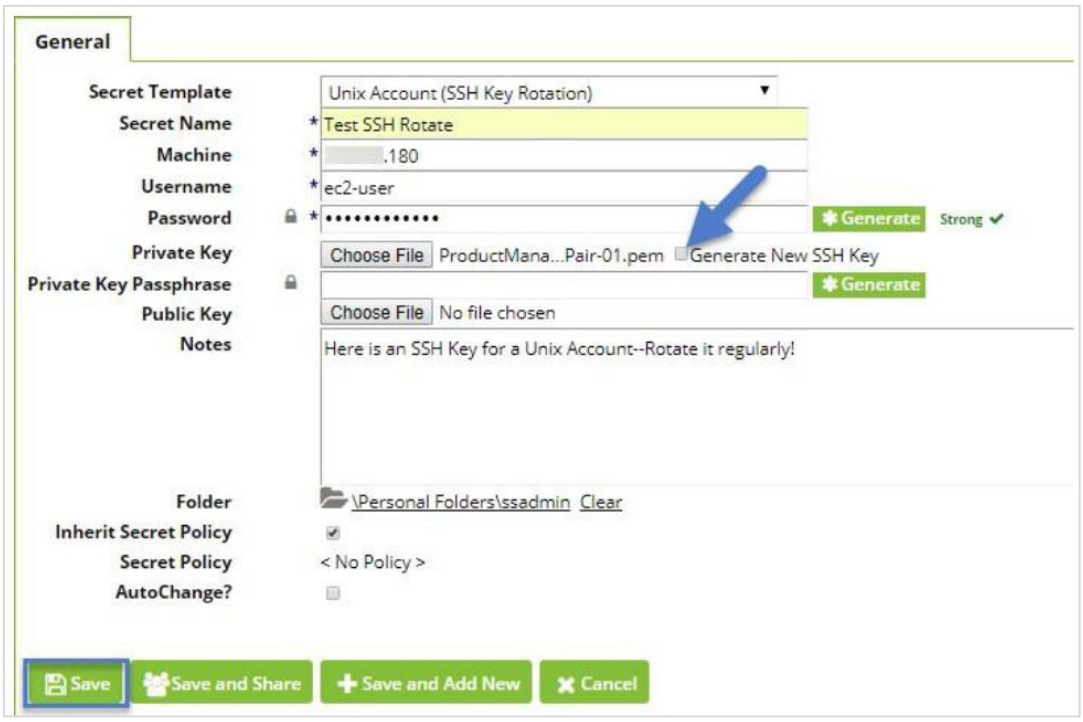


Ilustración 6-14. Creación de Unix Account (SSH Key Rotation)

6.6.3.2 CAMBIO REMOTO DE CONTRASEÑA SSH KEY ROTATION

133. Se recomienda activar *Remote Password Changing* (RPC) en los secretos del tipo *Unix Account* (ver apartado 6.6.2 Cambio Remoto de contraseña (RPC).

134. Al activar RPC, se producirá la rotación de claves SSH *(SSH Key Rotation*). Esto permite que, cuando se cambie la contraseña del secreto, se regeneren también las claves pública/privada y que la clave privada se cifre con una nueva passphrase.

135. Para ello, el equipo unix a gestionar debe cumplir con los siguientes requisitos:

- Los inicios de sesión con claves SSH deben haber sido activados para claves en formato OpenSSH.
- Las claves públicas deben almacenarse en *[~userhome]/.ssh/ authorized_keys*.
- El equipo debe tener instaladas las utilidades *Grep* y *Sed*.

136. *Para rotar las claves SSH remotamente, navegar hasta la pantalla SSH Key Rotation Secret's View y hacer clic en Change Password Remotely. A continuación:*

- Introducir la nueva contraseña (*password*) de forma manual, o hacer click en *Generate* para generar una nueva de forma aleatoria.

- Seleccionar "*Generate New SSH Key*" para generar una nueva pareja de claves pública/privada de forma aleatoria, e introducir la nueva *passphrase* (o generarla de forma automática), para el cifrado de la clave privada.
- Si queremos introducir nuestra propia SSH Key, quitar el check de "*Generate New SSH Key*" e insertar la clave en el campo "*Next Private Key*" que aparece. Introducir la passphrase que se utilizó para cifrar esta clave privada. O dejar este campo en blanco si no se utilizó ninguna.
- Pulsar *Change* para que se inicie la rotación de claves y el cambio de *password*. Secret Server hará los cambios correspondientes en el equipo unix.

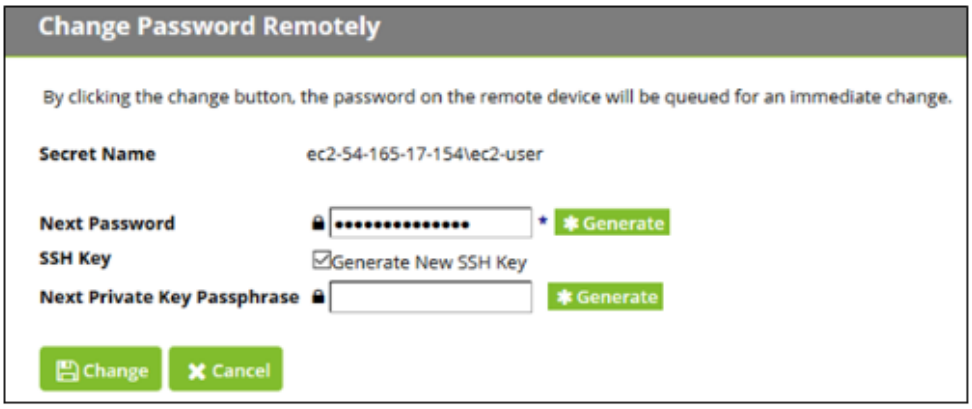


Ilustración 6-15. Cambio remoto de credenciales SSH.

6.6.3.3 PUTTY LAUNCHER

137. *Putty Launcher* es la aplicación que se lanza (*launcher*) desde el equipo de usuario para la conexión al equipo *unix* a través de SSH, utilizando el secreto del tipo *Unix Account (SSH Key Rotation)* creado para tal efecto.
138. Este lanzador está habilitado por defecto. Se puede comprobar desde *Admin* > *Configuration*, verificando que *Enable Launcher* está activo.
139. Para utilizarlo, el usuario deberá seleccionar el secreto, hacer click en *View Secret* y pulsar el icono "*Putty Launcher*". La primera vez que realice esta acción, saldrá una pantalla con el error "*Protocol Handler Failed to Launch*". Esto indica que debe instalarse el lanzador la primera vez. Desde la pantalla de error, permite seleccionar qué versión instalar (64-bit, 32-bit, etc.). Seleccionar la versión adecuada. Una vez descargado, cerrar la ventana de error, actualizar el navegador y volver a lanzarlo.

6.6.4 USO DE DOUBLELOCK

140. ***DoubleLock*** es una característica de Secret Server que permite añadir una capa adicional de seguridad a los secretos, cifrándolos con una nueva clave que solo es accesible mediante una contraseña adicional (independiente de la contraseña

configurada dentro del secreto). DoubleLock utiliza la tecnología de claves pública/privada para compartir de forma segura el acceso al secreto.

141. El sistema *DoubleLock* consta de los siguientes objetos:

- *DoubleLock Password*: Es una contraseña cifrada, asociada a un usuario.
- *DoubleLock*: Es el objeto que da acceso a uno o varios secretos. Al objeto *DoubleLock* se accede a través de una contraseña asociada a un usuario (*DoubleLock Password*) o, también, al mismo objeto *DoubleLock* se puede acceder a través de varias contraseñas (*DoubleLock Password*), cada una de ellas asociada a un usuario. De esta forma establece a qué secretos puede acceder, qué usuario o usuarios.
- Los secretos solo pueden ser accedidos a través de un único *DoubleLock*, aunque el mismo *DoubleLock* puede dar acceso a varios secretos.
- Los usuarios tienen una única "*DoubleLock Password*", que les puede dar acceso a varios *DoubleLocks*.

142. En la imagen que se muestra a continuación se encuentra un ejemplo de las relaciones entre los objetos vistos.

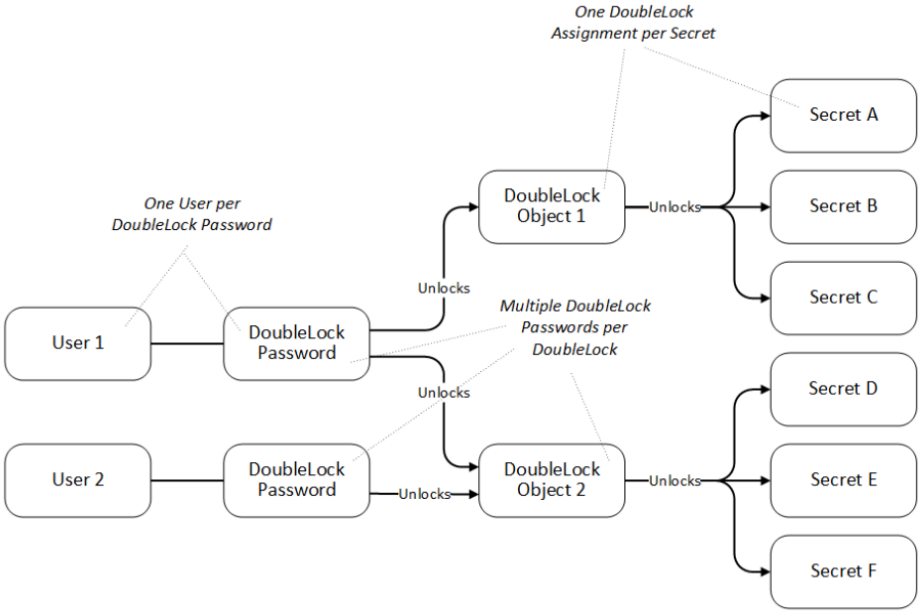


Ilustración 6-16. Relación de objetos en DoubleLock

143. Debido a que las contraseñas *DoubleLock* son personales, en caso de pérdida la única opción es establecer una nueva contraseña. En caso de ser el único usuario asignado a un *DoubleLock*, los secretos asignados a este **serán borrados** al reestablecer la contraseña. En otro caso, se deberá pedir acceso de nuevo a los *DoubleLocks*.

144. Para obtener más información sobre el uso y configuración de DoubleLock dirigirse al capítulo *Secret DoubleLocks* de la guía *Secret Server Administration Guide [].*

6.7 AUDITORÍA

6.7.1 REGISTRO DE EVENTOS

145. Secret Server mantiene un registro de todas las acciones llevadas a cabo en el producto. En el ANEXO 1. Registros de eventos y auditoría se muestran los eventos auditables y ejemplos de los mismos.

146. El producto tiene definidos varios permisos relacionados con acciones de auditoría, que pueden asignarse a usuarios o administradores. Son los siguientes:

- ***Add Secret Custom Audit*:** Un usuario con este permiso puede grabar una entrada de auditoría personalizada cuando acceda a un secreto utilizando la API de servicios web.
- ***User Audit Expire Secret:*** este permiso permite ver el informe de *User Audit Report*, que muestra todos los secretos a los cuales un usuario en concreto ha accedido en un intervalo de tiempo específico. También permite forzar la caducidad de todos estos secretos, lo cual haría que Secret Server cambie la contraseña de manera automática.
- ***View Configuration Unlimited Admin*:** Permite ver la configuración de la característica de *Unlimited Admin Mode* y el registro de auditoría correspondiente. Esta característica permite a los administradores tener permisos de acceso sobre todos los secretos. No se recomienda su uso salvo en casos de emergencia. Se recomienda que esté configurado el modo *Limited Administrator Mode* (configuración por defecto) de forma que los administradores solo puedan acceder a los secretos para los que tengan permisos.
- ***View Secret Audit*:** Permite ver el registro de auditoría de los secretos (*Secret Audit),* que mostrará todas las acciones que se hayan realizado sobre el secreto.
- *View User Audit Report:* Permite a un usuario ver, pero no editar, el *User Audit Report*.

6.7.2 ALMACENAMIENTO LOCAL

147. *Secret Server* almacena de manera local los registros de auditoría. Genera registros detallados para usuarios y secretos. La información de auditoría se puede visualizar de diversas formas.

148. El detalle de administración de la auditoría se puede consultar en el capítulo *Administration Auditing* de la guía *Secret Server Administration Guide [REF1].* En este apartado se indican los aspectos más destacados.

149. Para ver un listado de todos los informes de auditoría disponibles, desde una cuenta de administrador acceder a *Reports > General*. Desde esta pantalla se pueden crear, también, informes a medida.

150. En *Reports*, accediendo a la pestaña de *User Audit* se pueden ver los registros de auditoría del usuario seleccionado, en el intervalo de tiempo seleccionado. Mostrará todos los secretos que el usuario ha visualizado o editado.

151. En la pantalla de visualización de cada secreto (*Secret View*), pulsando el botón de *View Audit* se verán, también todas las acciones realizadas sobre ese secreto.

152. Para ver las acciones de configuración realizadas por los administradores, desde cada pantalla de configuración (por ejemplo, *Admin > Configuration*), pulsar en *View Audit*.

153. Por defecto no se elimina ninguno de los registros de auditoría. No obstante, se deberá configurar una política de retención de datos para que, en caso de que el espacio de almacenamiento esté llegando a su máximo, se puedan eliminar los registros más antiguos. Para configurar la política de retención de datos se debe disponer del permiso de *Administer Data Retention,* y se deben seguir los siguientes pasos:

    - Acceder a *Admin > Data Retention Management*.
    - Hacer clic en *Edit* en el apartado *Enabled*, y seleccionar la casilla *Enabled* para activar la política de retención de datos.
    - Hacer clic en *Edit* en el apartado *Max Record Age* para configurar el tiempo que desea retenerse la información.

6.7.2.1 WINDOWS EVENT LOG

154. *Secret Server* también puede enviar los registros de auditoría al *Windows Event Log* de Windows Server.

155. El *Windows Event Log* está vinculado a la implementación del *syslog*, por lo que este tiene que encontrarse activado para poder funcionar:

    - Desplazarse hasta *Admin > Configuration > Edit*.
    - Marcar *Enable Syslog/CEF Logging* seguido de *Write Syslogs As Windows Events*.

156. Cuando la base de datos se encuentre inaccesible, Secret Server tratará de registrar los errores en el *Windows Event Log*. De manera predeterminada, el servicio de red y las cuentas de servicio estándar no tienen acceso al “Event Log”, por lo que es necesario añadir estos permisos manualmente.

157. Esta configuración se puede consultar con detalle en el artículo *https://thycotic.force.com/support/s/article/Giving-Application-Pool-Access-to-Event-Log*.

158. Tras configurar el *Windows Event Log* para el registro de logs de Secret Server, se puede acceder a estos desde *Windows Event Log Event Viewer* en el servidor local. Para ello, abrir el visor de eventos del servidor (*Event Viewer*), e ir a *Windows Log > Application.* Los logs de Secret Server se mostrarán como [SecretServer] en la columna Source.

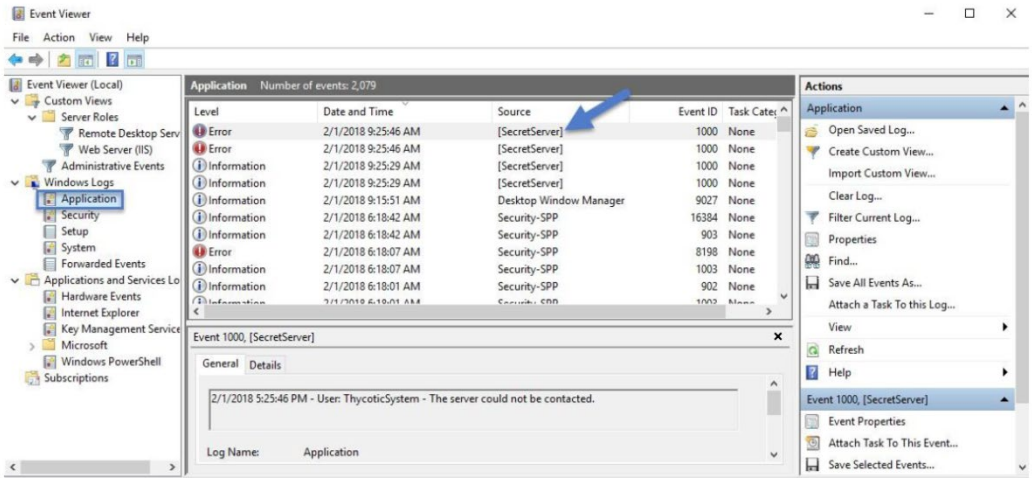


Ilustración 6-17. Visualización de eventos en Windows Log

6.7.3 SERVIDOR DE AUDITORÍA EXTERNO

159. A través del protocolo *Secure TCP syslog/CEF Protocol*, *Secret Server* puede enviar los registros de auditoría a un servidor externo *syslog*. Se utilizará el protocolo TLS 1.2 o 1.1.

160. Los servidores de auditoría externos compatibles son: *Syslog-NG* o cualquier servidor que acepte mensajes cifrados TLS utilizando el Protocolo *BSD Syslog*.

161. Si el servidor de auditoría externo requiere autenticación de cliente, será necesario instalar un certificado de cliente en el servidor *Secret Server*. Consultar el apartado 6.2.3 Configuración de Certificados de Clientes.

162. *Secret Server* deberá autenticar al servidor de auditoría externo, por lo que debe confiar en su certificado. Para ello, deberá tener instalado el certificado de la CA raíz emisora del certificado del servidor de auditoría. Consultar el apartado 6.2.1 Instalación de un certificado CA raíz.

163. En caso de error de conexión entre *Secret Server* y el servidor externo *syslog*, *Secret Server* generará un registro con el error, y pasará a almacenar los registros de auditoría en la base de datos local de *Secret Server*, intentando reestablecer la conexión y reenviarlos de forma periódica (por defecto, cada 60 segundos).

164. Para configurar el servidor de auditoría externo:

- En primer lugar, indicar que Syslog/CEF puede requerir una clave de licencia adicional. Para ello desde *Admin > Licenses*, seleccionar Install *New License*. Una vez instalada, debe activarse.
- Indicar, también, que debe existir conectividad entre Secret Server y el servidor externo *syslog*.
- Ir a *Admin > Configuración > Edit*.
- En la pestaña *General*, debajo de *Application Settings,* seleccionar la casilla *Enable Syslog/CEF Logging*.
- Configurar la dirección IP del externo Syslog, en el campo *Syslog/CEF Server*.
- Configurar el número de puerto del servidor Syslog al que se deben enviar los logs, en el cuadro *Syslog/CEF Port*. El puerto 6514 se utiliza por defecto para Secure TCP Syslog.
- Configurar el *Syslog/CEF Protocol* a Secure TCP. Este parámetro forzará el uso de TLS 1.2 o 1.1. Aunque se aplique esta configuración para forzar la no utilización de SSLv3 o TLS 1.0, se recuerda que solo se debe utilizar TLS 1.2, según se describe en el apartado 6.1.3.
- Configurar la *Syslog/CEF Time Zone a UTC Time o Server Time*.

Enable Syslog/CEF Logging	Yes
Syslog/CEF Server	Syslog.Example.com
Syslog/CEF Port	6514
Syslog/CEF Protocol	SECURE TCP
Syslog/CEF Time Zone	Server Time

165. Para obtener más información sobre cómo configurar el servidor de auditoría externo dirigirse al artículo https://thycotic.force.com/support/s/article/SS-Secure-Syslog-CEF-Logging.

6.7.4 AUDITORÍA DE LAS CONEXIONES TLS

166. Para hacer un seguimiento de las conexiones TLS incluyendo cualquier fallo de las mismas, debe habilitarse esta auditoría de la siguiente forma:

- *Desde Admin > Configuration > Security.* Navegar hasta la sección *TLS Auditing* y activar las siguientes opciones *(Yes):*
  - *Apply TLS Certificate Chain Policy and Error Auditing*. Si no está a Yes, no se pueden utilizar certificados de cliente.
  - *Enable TLS Debugging and Conexion Tracking*. Cuando está a Yes, Secret Server enviará logs al servidor de auditoría, indicando cuando se establecen y se finalizan las conexiones TLS. Si el logging a nivel de depuración (*debug logging*) está habilitado en el fichero

web-log4net.config, también se registrará información detallada sobre la cadena de validación del certificado X.509. Indicar que esta opción puede generar gran cantidad de información extra en los mensajes de log.

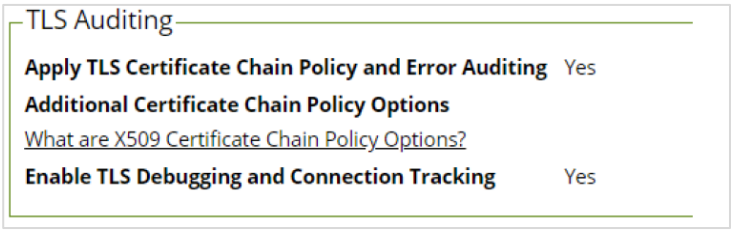
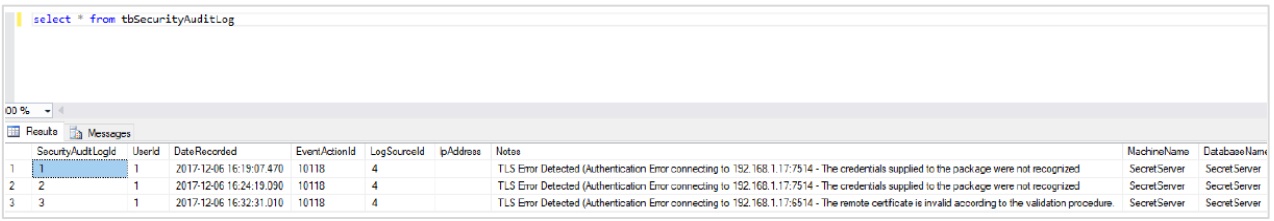


Ilustración 6-18. Auditoría de las conexiones TLS (I).

167. Para ver el log de errores de las conexiones TLS:

- Abrir *Microsoft SQL Server Management Studio.* Ir a la base de datos de Secret Server *(DBMachineName > Databases > SecretServer).*
- Ejecutar una nueva Query*: select * from tbSecurityAuditLog.*



	SecurityAuditLogId	UserId	DateRecorded	EventActionId	LogSourceId	IpAddress	Notes	MachineName	DatabaseName
1	1	1	2017-12-06 16:19:07.470	10118	4		TLS Error Detected (Authentication Error connecting to 192.168.1.17:7514 - The credentials supplied to the package were not recognized	SecretServer	SecretServer
2	2	1	2017-12-06 16:24:19.090	10118	4		TLS Error Detected (Authentication Error connecting to 192.168.1.17:7514 - The credentials supplied to the package were not recognized	SecretServer	SecretServer
3	3	1	2017-12-06 16:32:31.010	10118	4		TLS Error Detected (Authentication Error connecting to 192.168.1.17:6514 - The remote certificate is invalid according to the validation procedure.	SecretServer	SecretServer

Ilustración 6-19. Auditoría de las conexiones TLS (II)

168. Para más detalle sobre estos *logs*, se pueden revisar los ficheros de log en el servidor web de *Secret Server* (*C:\inetpub\wwwroot\SecretServer\log)* que incluyen *SS.log, SS-BSSR.log, SS-BSWR.log.*

6.8 GRABACIÓN DE SESIONES

169. La grabación de sesiones (*session recording*) es una característica *de Secret Server* que requiere licencia. Puede ser de dos tipos: básica o avanzada. La diferencia entre ambas es que la grabación de sesión avanzada captura más información de la sesión establecida por el usuario.

170. La grabación de sesiones se basa en el manejador de protocolo configurado en el equipo del usuario a través del lanzador (*launcher*) de *Secret Server*. Utilizando el lanzador (*launcher*), *Secret Server* captura segundo a segundo pantallazos del equipo del cliente (cada vez que se produzca algún cambio en la pantalla) durante toda la sesión que se está grabando. Las imágenes de las pantallas del usuario se compilan en un vídeo que los administradores pueden descargar y visualizar para cuestiones de auditoría.

171. Si la opción de *session recording* está activado en el secreto, el administrador puede visualizar la sesión del usuario en tiempo real. Los administradores

pueden buscar en sesiones activas o finalizadas, a través de *Admin > Session Monitoring.*

172. El detalle de la configuración de la grabación de sesión se puede consultar en el capítulo *Session Recording* de la guía *Secret Server Administration Guide* [REF1].

6.9 ACTUALIZACIONES

173. El resumen de la versión actual instalada de *Secret Server* figura en la esquina superior izquierda de la pantalla de usuario o de administrador.

174. La versión completa se puede obtener en la sección *Secret Server Enviroment,* desplazándonos a *Admin > Diagnostics.*

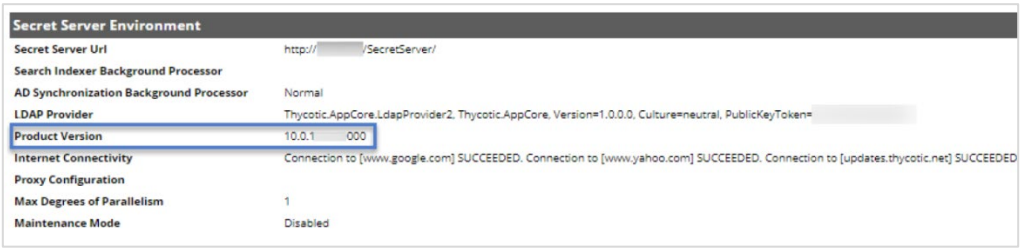


Ilustración 6-20. Detalle de la versión de SS instalada

175. *Secret Server* está configurado por defecto para notificar cuando se encuentren actualizaciones disponibles. Se crea un aviso en la parte superior de la pantalla del Administrador cuando haya disponible una nueva actualización. Para verificar esta configuración:

- Desplazarse a *Admin > Configuration > General*.
- Comprobar que se encuentra activado *Allow Automatic Checks for Software Updates*. En caso negativo, activarlo.

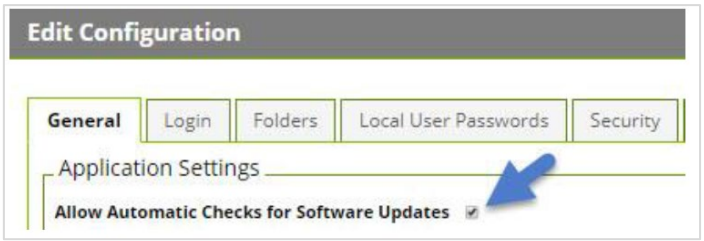


Ilustración 6-21. Verificación de chequeo automático de versión.

176. Tras recibir la notificación, el administrador puede descargar la actualización. Antes de iniciar la instalación, se debe verificar la autenticidad de los ficheros descargados siguiendo los pasos descritos en el apartado 4.1 Entrega segura del producto

177. Si el servidor *Secret Server* no tiene salida a internet, se pueden consultar las actualizaciones a través del portal de *Thycotic Support*.

6.10 BACKUP

178. *Secret Server* permite la configuración de *backups* manuales y automáticos cada cierto intervalo de tiempo especificado. Estos *backups* pueden almacenarse de forma local, o enviarse a una ubicación en red.

179. Existen dos componentes en un *backup* de *Secret Server*:

    - Los ficheros de la aplicación web.
    - La base de datos.

180. La configuración de las copias de seguridad se realiza desde *Tools > Backup*. Es necesario especificar:

    - ***Backup Database File Path***: Ruta accesible desde el servidor SQL, en la que se almacenará el fichero "database.bak".
    - ***Backup File Path***: Ruta accesible desde Secret Server, en la que se almacenará el fichero ".zip" con los directorios de la aplicación.
    - **Keep Number of Backups**: Número de copias de seguridad antiguas que se deben almacenar. Es necesario tener en cuenta que si se escoge un número elevado podría consumirse mucho espacio en disco.
    - ***Enable Scheduled Backup***: Habilita la copia de seguridad automática en las fechas que sean elegidas.

181. Para realizar una copia de seguridad de forma manual, desde *Backup > Administration* hacer clic en *Backup Now*.

182. También es posible exportar los secretos en formato CSV. Desde *Administration > Export*, seleccionar la carpeta que necesita exportarse. Por defecto, si no se selecciona ninguna carpeta, se exportan todos los secretos. Como medida de seguridad, es necesario introducir la contraseña de administración para poder exportar los datos.

183. El detalle de la configuración de Backups se puede consultar en el capítulo *Backup and Disaster Recovery* de la guía *Secret Server Administration Guide [REF1].*

7. FASE DE OPERACIÓN

184. Durante la fase de operación de *Secret Server* se recomienda llevar a cabo, al menos, las siguientes tareas para una gestión segura del producto:

a) Comprobaciones periódicas del software para asegurar que no se ha introducido software no autorizado.

b) Programar *backups* automáticos para realizar copias de seguridad de los datos y de la configuración del sistema.

c) Configurar tareas automáticas para la gestión de los logs de auditoría, eliminándolos periódicamente. Evitando de esta forma llegar al límite de almacenamiento, lo que podría llevar a la perdida de información de auditoría.

d) Comprobar que los ficheros de auditoría están protegidos frente al borrado o la modificación no autorizados.

e) Control de acceso a la información de auditoría, de tal forma que únicamente el personal designado pueda acceder a ella.

f) Asegurar que se reciben correctamente las notificaciones de las actualizaciones y mantener el sistema actualizado siempre a la última versión.

g) Auditar, al menos, los eventos especificados en la normativa de referencia y aquellos otros extraídos del análisis de riesgos.

8. REFERENCIAS

REF1 *Secret Server Administration Guide*
https://updates.thycotic.net/secretserver/documents/Secret Server-ADM-EXT-Admin-Guide.pdf

REF2 CCN-STIC-807 Criptología de empleo en el ENS

REF.3 CCN-STIC-105 Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación

9. ABREVIATURAS

API	*Application Programming Interface*
CA	Autoridad de Certificación *(Certification Authority)*
CC	*Common Criteria*
CCN	Centro Criptológico Nacional
CIDR	*Classless Inter-Domain Routing*
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación
CSV	*Comma-Separated Values (Valores Separados por Coma)*
DPAPI	*Data Protection API*
ENS	Esquema Nacional de Seguridad
FIPS	*Federal Information Processing Standard*
HSTS	*HTTP Strict Transport Security*
HTTPS	*Hypertext Transfer Protocol Secure*
IIS	*Internet Information Services*
LDAP	*Lightweight Directory Access Protocol*
SAML	*Security Assertion Markup Language*
SS	*Secret Server*
SSH	*Secure Shell*
SSL	*Secure Socket Layer*
TCP	*Transmission Control Protocol*
TLS	*Transport Layer Security*

ANEXO 1. REGISTROS DE EVENTOS Y AUDITORÍA

185. A continuación, se incluye una tabla con los eventos auditables y ejemplos de los mismos, cuando el sistema funciona en el modo de operación seguro.

Evento	Ejemplo de registro generado
Definición de atributos de objetos.	May 22 2018 15:30:37 - User: SecretServer Administrator - [SecretServer] Event: [Secret] Action: [Create] By User: SSAdmin Item Name: Unix Account SSH Test Container Name: SecretServer Administrator May 22 2018 20:20:57 - User: SecretServer Administrator - [SecretServer] Event: [Secret] Action: [Edit] By User: SSAdmin Item Name: Unix Account SSH Test Container Name: SecretServer Administrator Details: testparent.thycotic.com\Children of Homer (Granted View) May 22 2018 20:57:41 - User: SecretServer Administrator - [SecretServer] Event: [Secret] Action: [Edit] By User: SSAdmin Item Name: Unix Account SSH Test [BARRY] Container Name: SecretServer Administrator Details: testparent.thycotic.com\Children of Homer (Revoked View) May 23 2018 11:33:32 - User: admin - [SecretServer] Event: [Secret Template] Action: [Create] By User: admin Item Name: Test Template Details: Secret Template "Test Template" was created.
Asociación de atributos con objetos	Jan 04 10:25:54 WIN-3SS887QA4R4 CEF:0|Thycotic Software|Secret Server|10.4.000001|10005|SECRET - EDIT|2|msg=[SecretServer] Event: [Secret] Action: [Edit] By User: admin Item Name: My Active Directory Secret Name Details: Fields: (Username) suid=2 suser=admin cs4=admin cs4Label=suser Display Name src=10.12.30.4 rt=Jan 04 2018 10:25:36 fname=My Active Directory Secret Name fileType=Secret fileId=26 May 23 2018 11:34:35 - User: admin - [SecretServer] Event: [Secret Template] Action: [Create] By User: admin Item Name: Test Template Details: Active: true to false;
Uso del mecanismo de autenticación	May 22 2018 15:59:11 - User: qaparent.thycotic.com\Matt testuser 1 - [SecretServer] Event: [User] Action: [Login] By User: qaparent.thycotic.com\md_testuser1 Item Name: qaparent.thycotic.com\md_testuser1 May 22 2018 16:05:46 - User: ThycoticSystem - Login Failure - User balhblah does not exist May 22 2018 16:08:25 - User: qaparent.thycotic.com\Matt testuser 3 - [SecretServer] Event: [User] Action: [Login Failure] By User: qaparent.thycotic.com\md_testuser3 Item Name: qaparent.thycotic.com\md_testuser3 Details: AuthenticationFailed
Creación o modificación de datos de identidad y credenciales	Jan 04 10:37:27 WIN-3SS887QA4R4 CEF:0|Thycotic Software|Secret Server|10.4.000001|19|USER - PASSWORDCHANGE|2|msg=[SecretServer] Event: [User] Action: [Password Change] By User: admin Item Name: admin suid=2 suser=admin cs4=admin cs4Label=suser Display Name duser=admin duid=2 fname=admin fileType=User fileId=2 src=10.12.30.4 rt=Jan 04 2018 10:37:24
Creación y modificación de datos de identidad y credenciales	Jan 04 12:46:26 WIN-3SS887QA4R4 CEF:0|Thycotic Software|Secret Server|10.4.000001|1|USER - CREATE|2|msg=[SecretServer] Event: [User] Action: [Create] By User: admin Item Name: New User suid=2 suser=admin cs4=admin cs4Label=suser Display Name duser=New User duid=6 fname=New User fileType=User fileId=6 src=10.12.30.4 May 24 2018 15:21:49 - User: Marrio Thycotic - [SecretServer] Event: [Domain] Action: [Create] By User: admin Item Name: testparent.thycotic.com Details: Groups Added to Synchronization: secretserver May 24 2018 15:28:06 - User: ThycoticSystem - [SecretServer] Event: [User] Action: [Added To Group] By User: ThycoticSystem Item Name: testparent.thycotic.com\jsmithson Container Name: testparent.thycotic.com\secretserver

Evento	Ejemplo de registro generado
***Enrollment* o modificación de un sujeto**	May 22 2018 13:43:22 - User: admin - [SecretServer] Event: [Role] Action: [Assign User Or Group] By User: admin Item Name: User Container Name: user3 May 22 2018 14:00:06 - User: admin - [SecretServer] Event: [Configuration] Action: [Edit] By User: admin Details: EnableMinimumPasswordAge: false to true; MinimumPasswordAgeInMinutes: 43200 to 3; May 22 2018 14:09:55 - User: admin - [SecretServer] Event: [Configuration] Action: [Edit] By User: admin Details: MinimumPasswordAgeInMinutes: 3 to 2; PasswordHistoryDepth: 5 to 4; May 22 2018 14:24:17 - User: admin - [SecretServer] Event: [Secret Template] Action: [Create] By User: admin Item Name: Active Directory Account Details: ValidatePasswordRequirementsOnCreate: false to true; ValidatePasswordRequirementsOnEdit: false to true; May 22 2018 14:23:30 - User: admin - [SecretServer] Event: [Password Requirement] Action: [Create] By User: admin Item Name: Default Details: IsDefault: false to true; May 22 2018 20:59:04 - User: admin - [SecretServer] Event: [Secret] Action: [Edit] By User: admin Item Name: testparent\mufasa Container Name: admin Details: qaparent.thycotic.com\StephGroup (Granted View) May 22 2018 21:03:08 - User: admin - [SecretServer] Event: [Secret] Action: [Edit] By User: admin Item Name: testparent\mufasa Container Name: admin Details: qaparent.thycotic.com\StephGroup (Revoked View) May 23 2018 13:20:54 - User: admin - [SecretServer] Event: [Configuration] Action: [Edit] By User: admin Details: ADUserSyncOption: ImportEnabled to MirrorAD; AllowSynchronizedAccountDisabling: false to true; May 23 2018 14:51:37 - User: admin - [SecretServer] Event: [Domain] Action: [Create] By User: admin Item Name: testparent.thycotic.com Details: Groups Added to Synchronization: HelpDeskTier1 May 23 2018 14:52:16 - User: admin - [SecretServer] Event: [Domain] Action: [Synchronize] By User: admin Details: Active Directory Sync Initiated May 23 2018 14:52:20 - User: ThycoticSystem - [SecretServer] Event: [User] Action: [Added To Group] By User: ThycoticSystem Item Name: testparent.thycotic.com\gman Container Name: testparent.thycotic.com\HelpDeskTier1 May 23 2018 14:26:16 - User: ThycoticSystem - [SecretServer] Event: [User] Action: [Edit] By User: ThycoticSystem Item Name: testparent.thycotic.com\gman Details: Enabled: true to false; May 23 2018 15:13:55 - User: ThycoticSystem - [SecretServer] Event: [User] Action: [Disable] By User: ThycoticSystem Item Name: testparent.thycotic.com\gman May 22 2018 12:53:53 - User: admin - [SecretServer] Event: [User] Action: [Edit] By User: admin Item Name: user1 Details: IsLockedOut: false to true; May 22 2018 12:54:51 - User: user1 - [SecretServer] Event: [User] Action: [Login Failure] By User: user1 Item Name: user1 Details: UserIsLockedOut May 22 2018 12:55:09 - User: admin - [SecretServer] Event: [User] Action: [Edit] By User: admin Item Name: user1 Details: IsLockedOut: true to false; Apr 04 21:32:02 THY616-PC CEF:0|Thycotic Software|Secret Server|10.4.000001|15|CONFIGURATION - EDIT|2|msg=[SecretServer] Event: [Configuration] Action: [Edit] By User: admin Details: MinLength: 1 to 8; RequireLowercase: false to true; RequireNumbers: false to true; suid=1 suser=admin cs4=Display Name cs4Label=suser Display Name src=::1 rt=Apr 04 2018 21:31:44 Apr 04 21:33:32 THY616-PC CEF:0|Thycotic Software|Secret Server|10.4.000001|500|System Log|7|msg=System.Exception: API_InvalidPassword at Thycotic.ihawu.Business.Rest.Logic.Users. UserLogic. UpdateAndSetPassword(IUser user, IUserUpdateArgs updatedUser) in C:\\development\\VSO\\Thycotic.Ihawu\\src\\Thycotic.ihawu.B usiness \Rest\\Logic\\Users\\UserLogic.cs:line 269 at Thycotic.ihawu.Business.Rest.Services.Api.V1.User.UserServi ce. <UpdateUser>d_15`1.MoveNext() in C:\\development\\VSO\\Thycotic.Ihawu\\src\\Thycotic.ihawu.B usiness \\Rest\\Services\\Api\\V1\\User\\UserService.cs:line 227 src=::1 rt=Apr 04 2018 21:33:32

Evento	Ejemplo de registro generado
Transmisión de identidad y credenciales a entidades externas	May 23 2018 6:54:41 - User: user1 - [SecretServer] Event: [Secret] Action: [Launch] By User: user1 Item Name: user1@centos7-001 Container Name: Administrators Details: PuTTY May 23 2018 7:54:46 - User: user1 - [SecretServer] Event: [Secret] Action: [Edit] By User: user1 Item Name: user1@centos7-001 Container Name: Administrators Details: Settings: (Change Password Remotely, Auto Change Next Password) May 23 2018 7:55:09 - User: ThycoticSystem - [SecretServer] Event: [Secret] Action: [Password Change] By User: ThycoticSystem Item Name: user1@centos7-001 Container Name: Administrators Details: Remote Password Change - Fields: (Password) May 23 2018 19:33:55 - User: Marrio Thycotic - [SecretServer] Event: [Secret] Action: [Delete] By User: admin Item Name: Will Be Deleted Container Name: Marrio Thycotic
Arranque y parada de auditoría	**N/D – No se pueden desactivar las funciones de auditoría interna dentro de Secret Server mientras que Secret Server continúa funcionando por razones de Seguridad** **Para activar las funciones de auditoría de Syslog:** Jan 08 8:11:58 WIN-3SS887QA4R4 CEF:0|Thycotic Software|Secret Server|10.4.000001|15|CONFIGURATION - EDIT|3|msg=[SecretServer] Event: [Configuration] Action: [Edit] By User: admin Details: EnableCefLogging: false to true; suid=2 suser=admin cs4=admin cs4Label=suser Display Name src=10.12.30.4 rt=Jan 08 2018 08:11:43 May 23 2018 7:34:33 - User: ThycoticSystem - WIN- GNDNGLV41TD: Application initialized and started. May 23 2018 7:34:40 - User: ThycoticSystem - Starting CEF/SysLog Auditing in the EventQueueMonitor thread... May 23 2018 12:57:13 - User: admin - Secure TCP Syslog: could not get existing conexión to 13.92.231.152:65140, and failed to create new conexión: TLS Error Detected (Authentication Error connecting to 13.92.231.152:65140 - A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond 13.92.231.152:65140)
Establecimiento y fin de conexión con el servidor de auditoría	Apr 05 19:52:10 THY616-PC CEF:0|Thycotic Software|Secret Server|10.4.000001|15|CONFIGURATION - EDIT|2|msg=[SecretServer] Event: [Configuration] Action: [Edit] By User: admin Details: EnableCefLogging: false to true; CefPort: 514 to 9999; CefServer: 127.0.0.1 to 192.168.0.100; suid=1 suser=admin cs4=Display Name cs4Label=suser Display Name src=::1 rt=Apr 05 2018 19:52:04 Apr 05 19:51:05 THY616-PC CEF:0|Thycotic Software|Secret Server|10.4.000001|15|CONFIGURATION - EDIT|2|msg=[SecretServer] Event: [Configuration] Action: [Edit] By User: admin Details: EnableCefLogging: True to False; suid=1 suser=admin cs4=Display Name cs4Label=suser Display Name rt=Apr 05 2018 19:51:05 src=::1

Evento	Ejemplo de registro generado
Fallo, establecimiento o fin de sesión TLS	Apr 05 19:53:25 THY642 CEF:0|Thycotic Software|Secret Server|10.0.104.000001|100|TLS Audit|2|msg=Domain [testparent.thycotic.com]: TLS Connect: Created new secure conexión to Active Directory Server testparent.thycotic.com:636 rt=Apr 05 2018 19:53:18 Apr 05 19:53:25 THY642 CEF:0|Thycotic Software|Secret Server|10.0.104.000001|100|TLS Audit|2|msg=Domain [testparent.thycotic.com]: TLS Disconnect: Destroying secure connection to Active Directory Server testparent.thycotic.com:636 rt=Apr 05 2018 19:53:18 Apr 04 16:58:16 THY642 CEF:0|Thycotic Software|Secret Server|10.0.104.000001|100|TLS Error Detected|8|msg=TLS Error Detected - ActiveDirectory: TLS Error Detected (qaparent): The revocation function was unable to check revocation because the revocation server was offline. src=::1 rt=Apr 04 2018 16:58:16
Máximo número de intentos fallidos de autenticación	May 23 2018 20:22:43 - User: User1 - [SecretServer] Event: [User] Action: [Login Failure] By User: user1 Item Name: user1 Details: UserIsLockedOut May 23 2018 20:51:41 - User: ThycoticSystem - [SecretServer] Event: [User] Action: [Edit] By User: ThycoticSystem Item Name: user1 Details: LoginFailures: 4 to 5; IsLockedOut: false to true;
Asignación de Usuario-Sujeto y de usuario-Rol	May 24 2018 15:21:49 - User: Marrio Thycotic - [SecretServer] Event: [Domain] Action: [Create] By User: admin Item Name: testparent.thycotic.com Details: Groups Added to Synchronization: secretserver May 24 2018 15:28:06 - User: ThycoticSystem - [SecretServer] Event: [User] Action: [Added To Group] By User: ThycoticSystem Item Name: testparent.thycotic.com\jsmithson Container Name: testparent.thycotic.com\secretserver May 23 2018 20:56:08 - User: admin - [SecretServer] Event: [Role Permission] Action: [Added To Role] By User: admin Item Name: Administer Active Directory Container Name: Gov_Administrator May 23 2018 20:59:15 - User: admin - [SecretServer] Event: [Role] Action: [Assign User Or Group] By User: admin Item Name: Gov_Administrator Container Name: gov_admin
Gestión de datos	May 23 2018 19:35:36 - User: admin - [SecretServer] Event: [Secret] Action: [Create] By User: admin Item Name: User1 Secret Container Name: admin Details: user1 (Granted Edit) May 23 2018 19:40:15 - User: admin - [SecretServer] Event: [Role] Action: [Assign User Or Group] By User: admin Item Name: Administrator Container Name: admin1
Modificaciones a la configuración de seguridad	Apr 05 20:15:11 THY616-PC CEF:0|Thycotic Software|Secret Server|10.4.000001|100|BACKUPCONFIGURATION - EDIT|2|msg=[SecretServer] Event: [Backup Configuration] Action: [Edit] By User: admin Details: BackupHistoryLength: 5 to 7; BackupStartTime: 1 to 300; BackupDate: 1/1/2005 12:00:00 AM to 12/31/2004 12:00:00 AM; suid=1 suser=admin cs4=Display Name cs4Label=suser Display Name src=::1 rt=Apr 05 2018 20:15:06 Apr 05 20:17:11 THY616-PC CEF:0|Thycotic Software|Secret Server|10.4.000001|10014|UNLIMITEDADMIN - ENABLE|2|msg=[SecretServer] Event: [Unlimited Administrator] Action: [Enable] By User: admin Details: Testing suid=1 suser=admin cs4=Display Name cs4Label=suser Display Name src=::1 rt=Apr 05 2018 20:17:06 Apr 05 20:17:21 THY616-PC CEF:0|Thycotic Software|Secret Server|10.4.000001|15|CONFIGURATION - EDIT|2|msg=[SecretServer] Event: [Configuration] Action: [Edit] By User: admin Details: UnlimitedAdministrator: true to false; suid=1 suser=admin cs4=Display Name cs4Label=suser Display Name src=::1 rt=Apr 05 2018 20:17:18 Apr 05 20:17:21 THY616-PC CEF:0|Thycotic Software|Secret Server|10.4.000001|10015|UNLIMITEDADMIN - DISABLE|2|msg=[SecretServer] Event: [Unlimited Administrator] Action: [Disable] By User: admin Details: End testing suid=1 suser=admin cs4=Display Name cs4Label=suser Display Name src=::1 rt=Apr 05 2018 20:17:18

Evento	Ejemplo de registro generado
Uso de las funciones de gestión	Jan 08 11:59:50 WIN-3SS887QA4R4 CEF:0|Thycotic Software|Secret Server|10.4.000001|15|CONFIGURATION - EDIT|3|msg=[SecretServer] Event: [Configuration] Action: [Edit] By User: admin Details: AllowTwoFactorRememberMe: false to true; TwoFactorRememberMeDurationDays: 0 to 1; suid=2 suser=admin cs4=admin cs4Label=suser Display Name src=10.12.30.4 rt=Jan 08 2018 11:59:37
Modificación de los miembros de los roles de gestión	Apr 05 20:18:41 THY616-PC CEF:0|Thycotic Software|Secret Server|10.4.000001|10|ROLE - ASSIGNUSERORGROUP|2|msg=[SecretServer] Event: [Role] Action: [Assign User Or Group] By User: admin Item Name: Administrator Container Name: User One suid=1 suser=admin cs4=Display Name cs4Label=suser Display Name fname=Administrator fileType=Role fileId=1 cs2Label=Group or User cs2=User One src=::1 rt=Apr 05 2018 20:18:37 Apr 05 20:18:51 THY616-PC CEF:0|Thycotic Software|Secret Server|10.4.000001|11|ROLE - UNASSIGNUSERORGROUP|2|msg=[SecretServer] Event: [Role] Action: [Unassign User Or Group] By User: admin Item Name: Administrator Container Name: User One suid=1 suser=admin cs4=Display Name cs4Label=suser Display Name fname=Administrator fileType=Role fileId=1 cs2Label=Group or User cs2=User One src=::1 rt=Apr 05 2018 20:18:45
Bloqueo de sesión por *timeout* de inactividad	May 23 2018 11:36:56 - User: admin - [SecretServer] Event: [Configuration] Action: [Edit] By User: admin Details: AllowLogoutTimeout: false to true; TimeoutInMinutes: 5 to 1; May 23 2018 11:38:56 - User: ThycoticSystem - [SecretServer] Event: [User] Action: [Logout] By User: ThycoticSystem Item Name: admin
Interrupción de una sesión activa	May 23 2018 21:46:49 - User: admin - [SecretServer] Event: [User] Action: [Login] By User: admin Item Name: admin May 23 2018 21:48:14 - User: admin - [SecretServer] Event: [User] Action: [Logout] By User: admin Item Name: admin
Configuración del *banner* de acceso	May 23 2018 14:39:24 - User: SecretServer Administrator - [SecretServer] Event: [Configuration] Action: [Edit] By User: SSAdmin Details: EnableLoginPolicy: false to true; ForceLoginPolicy: false to true;
Fallo de establecimiento de sesión	May 24 2018 14:50:47 - User: operator - [SecretServer] Event: [User] Action: [Login Failure] By User: operator Item Name: operator Details: InvalidIpAddress

Tabla 0-1. Eventos auditables y ejemplos

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL