centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1110

Procedimiento de empleo seguro
Privileged Passwords (SPP) 6.0 LTS

Agosto 2022

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.09.08 12:30:13 +02'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-22-224-4

Fecha de Edición: agosto de 2022

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. INTRODUCCIÓN

1. **One Identity Safeguard for privileged passwords (SPP)** forma parte de una *suite* de *software* empleada para **controlar y monitorizar cuentas privilegiadas de usuario**, con el objetivo de identificar posibles actividades maliciosas, detectar riesgos en derechos de acceso a recursos y proveer evidencias de seguridad.

2. Automatiza, controla y asegura el proceso de entrega de credenciales de cuentas privilegiadas a través de flujos de trabajo automatizados y gestión de acceso basada en roles.

3. Se suministra como un dispositivo *hardware* o virtual, que admite la implementación de una solución PAM (*Privileged Access Manager*) sin la necesidad de instalar clientes o agentes en la infraestructura de la compañía.

4. El dispositivo Safeguard está diseñado además para facilitar la implantación ya que está bastionado de fábrica y tiene preinstalado el *software* de *Safeguard for Privileged Passwords*). También facilita la usabilidad, la escalabilidad y el mantenimiento de contraseñas seguras. Contiene todos los componentes necesarios para establecer la gestión de contraseñas para cuentas gestionadas asociadas a usuarios y servicios del entorno de trabajo.

5. SPP se basa en un sistema operativo Windows, que ya ha sido bastionado por *One Identity* como medida estándar. El sistema operativo subyacente no es accesible directamente por los usuarios o por aplicaciones externas. Los administradores del sistema no pueden realizar cambios en la configuración del sistema operativo que estén fuera de las capacidades proporcionadas por la interfaz de gestión de SPP. Es decir, llevar a cabo acciones tales como cambiar la configuración de red del sistema, acceder a los logs, realizar *backups*, etc, solo es posible desde la interfaz de gestión de SPP.

6. El acceso a la configuración de SPP es posible a través de un navegador estándar, una herramienta de configuración basada en Windows o directamente a través de la REST/API asociada al producto. La herramienta de configuración basada en Windows es un *software* que se puede descargar directamente desde el dispositivo, accediendo a la siguiente URL: *https://IP_Del_SP/safeguard.msi*. Este *software*, una vez instalado en un equipo de administración, permitirá conectarse y administrar *Safeguard for Privileged Password*.

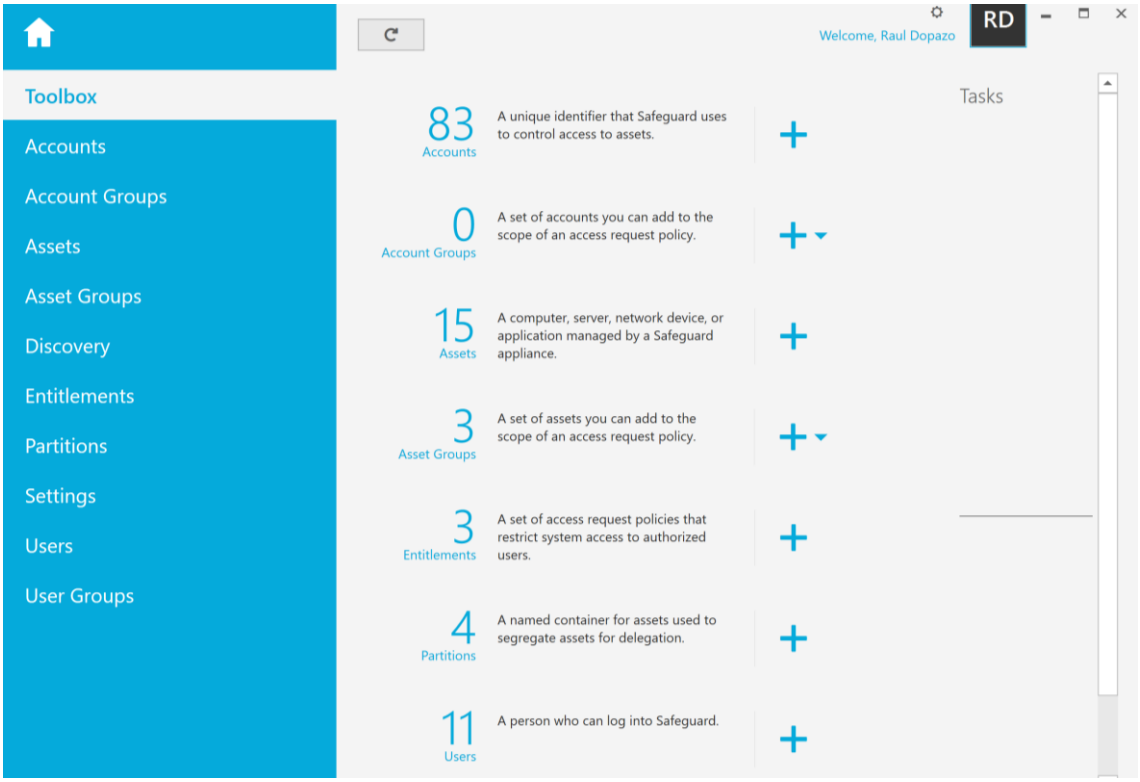

Figura 1 – Herramienta de Administración de SPP

7. SPP dispone de varias interfaces gráficas de usuario que permiten gestionar las solicitudes de acceso a credenciales, las aprobaciones de acceso a las mismas y las revisiones de sus cuentas y sistemas gestionados:

   - El cliente de escritorio de Windows consta de una vista de usuario final y una vista de administrador. El cliente de escritorio expone la funcionalidad de Safeguard de acuerdo al rol del usuario autenticado.
   - El cliente web es especialmente útil para solicitantes, revisores y aprobadores de acceso a las credenciales protegidas por SPP. También están disponibles algunas funciones de administración a través de dicho cliente.
   - La consola de administración web, solo disponible para la versión de *appliance* físico. Aparece siempre que se lleva a cabo la conexión al dispositivo físico, interfaz de red de gestión MGMT, y se utiliza **ÚNICAMENTE** para la configuración inicial del mismo en la IP de Gestión 192.168.1.105.

2. OBJETO Y ALCANCE

8. El objeto del presente documento es detallar una serie de aspectos de seguridad en la instalación y configuración de **SPP, versión 6.0 LTS**, de tal manera que se alcance una configuración considerada segura.

9. SPP ha sido cualificado para categoría ALTA del Esquema Nacional de Seguridad e incluido en el Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC), en la familia 'Gestión de acceso privilegiado (PAM)'.

3. ORGANIZACIÓN DEL DOCUMENTO

10. La estructura del presente Procedimiento de Empleo Seguro se divide en los siguientes apartados:

    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. En este apartado se muestra un *checklist* con las principales tareas a realizar.

    f) Apartado 9. Este apartado contiene la documentación a la que se ha hecho referencia a lo largo de este documento.

    g) Apartado 10. Este apartado contiene las abreviaturas que han sido empleadas a lo largo de este documento.

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

11. Como se ha comentado previamente, SPP puede desplegarse como dispositivo físico o virtual. El software es exactamente el mismo en ambos casos.

4.1.1 ENTREGA COMO DISPOSITIVO FÍSICO

12. Cuando se adquiere el dispositivo físico, el contenido del paquete de SPP incluye lo siguiente, tal como se muestra en la Figura 2:

    a) SPP 3000 Appliance o 2000 Appliance

    b) Riel (2)

    c) Cable Ethernet

    d) Soportes de instalación de rieles adicionales

    e) Cable de alimentación* (2)

    f) Cable serie DB9F/DB9F de 6 pies

13. Los cables de alimentación incluidos sólo están aprobados para su uso en determinados países o regiones. Antes de utilizar un cable de alimentación, compruebe que está clasificado y aprobado para su uso. El cable de alimentación es sólo para la instalación en la red de Aire Acondicionado.

14. Si falta algún elemento en el paquete, será necesario ponerse en contacto con el servicio de asistencia de One Identity en: *https://support.oneidentity.com* **[REF4]**.

15. En el proceso de embalaje del dispositivo físico se incluye un sello de garantía ubicado en la parte izquierda del dispositivo (figura 2) para asegurar que no ha sido manipulado desde su instalación. En caso de ausencia o signos de manipulación de dicho sello, será necesario ponerse en contacto con el servicio de asistencia de One Identity en: *https://support.oneidentity.com*

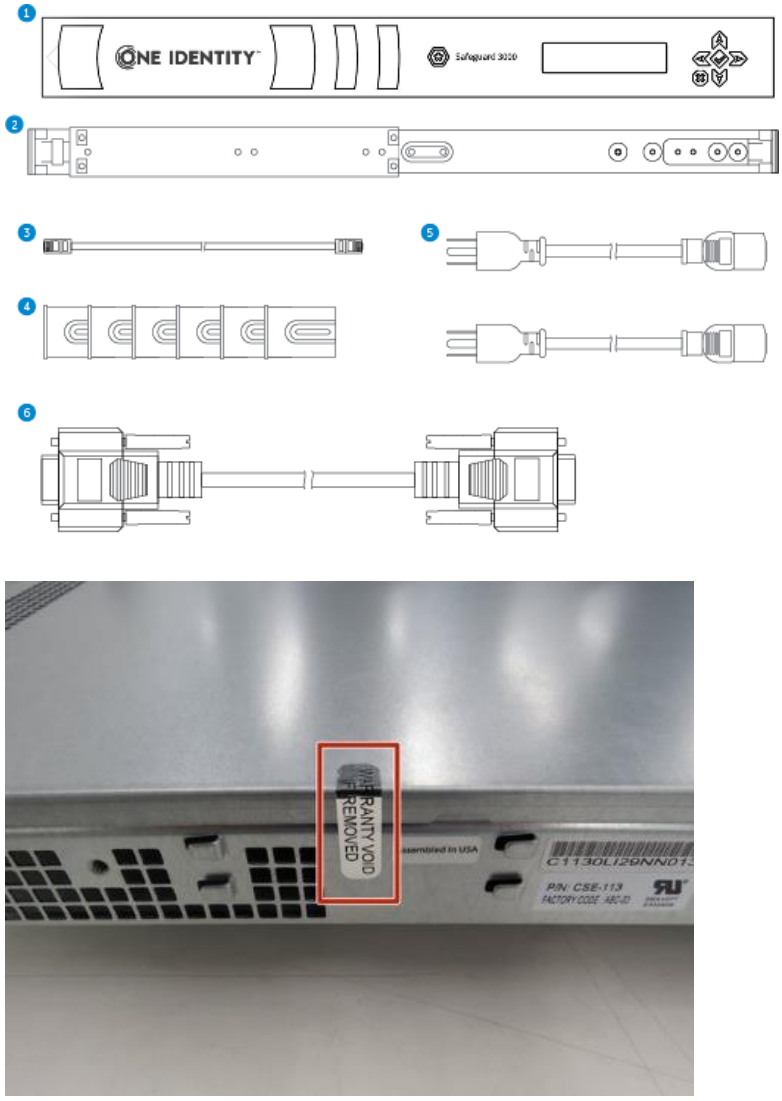

Figura 2 – Contenido del paquete que contiene el producto

3. Los siguientes diagramas muestran los paneles frontal y trasero de SPP 3000 Appliance y 2000 Appliance.

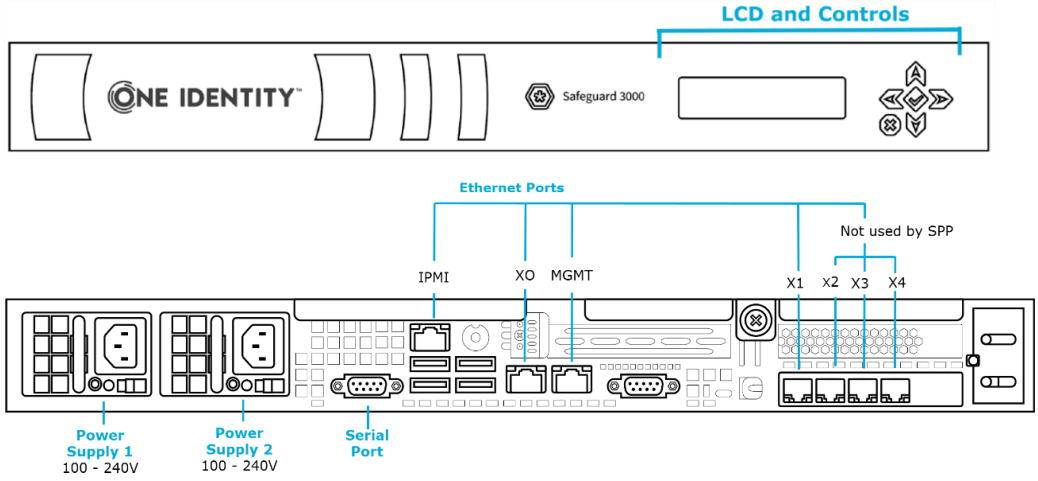

Figura 3 – Panel frontal y posterior del *appliance* 3000

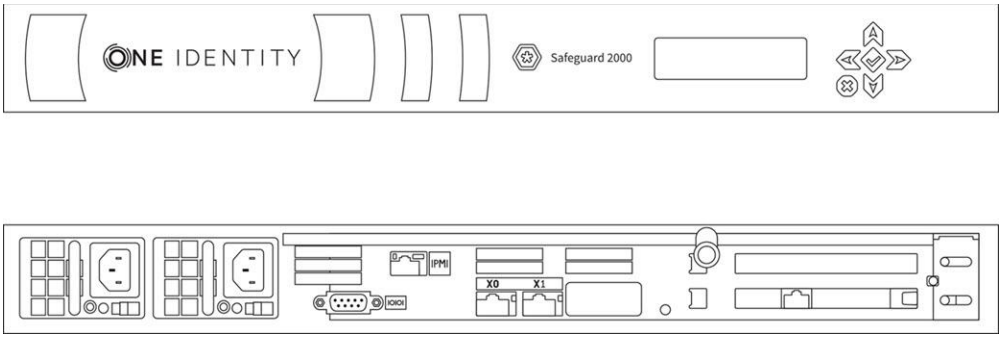

Figura 4 – Panel frontal y posterior del aparato 2000

4.1.2 ENTREGA COMO DISPOSITIVO VIRTUAL

16. Para instalar SPP en un entorno virtual, es necesario descargar la versión deseada, en este caso, la versión **6.0 LTS**, que se encuentra disponible en la web de soporte de One Identity **[REF4]**.

Figura 5 – Descarga de la OVA virtual para One Identity SPP

17. Existen dos (2) versiones para descargar respecto al dispositivo virtual: la versión para Hyper-V y la versión para VMware, las cuales se pueden descargar desde la siguiente URL **[REF9]**:

    https://support.oneidentity.com/es-es/one-identity-safeguard-for-privileged-passwords/6.0%20lts/download-new-releases

18. Al ser un dispositivo virtual, lo que se descarga es una imagen virtual con el sistema operativo configurado y el *software* preinstalado. Esta imagen virtual es la que se tiene desplegar en los entornos virtuales de Hyper-V o VMware, a través de las herramientas de administración de estas plataformas:

    - Imagen virtual para entornos Microsoft Hyper-V (VHDX) versión 8 o superior. El Zip descargado contiene la imagen virtual a desplegar en Hyper-V:

        a) spp-hyperv-6.0.0.12276.zip

        b) Hash SHA256:

        2FB34A31912C4B65FEBBE27D338E80AD96D0C09C498E3498522C11AE012ABBFF

        El hash del archivo puede ser verificado en la siguiente web **[REF10]**:

https://support.oneidentity.com/es-es/download-install-detail/6103860

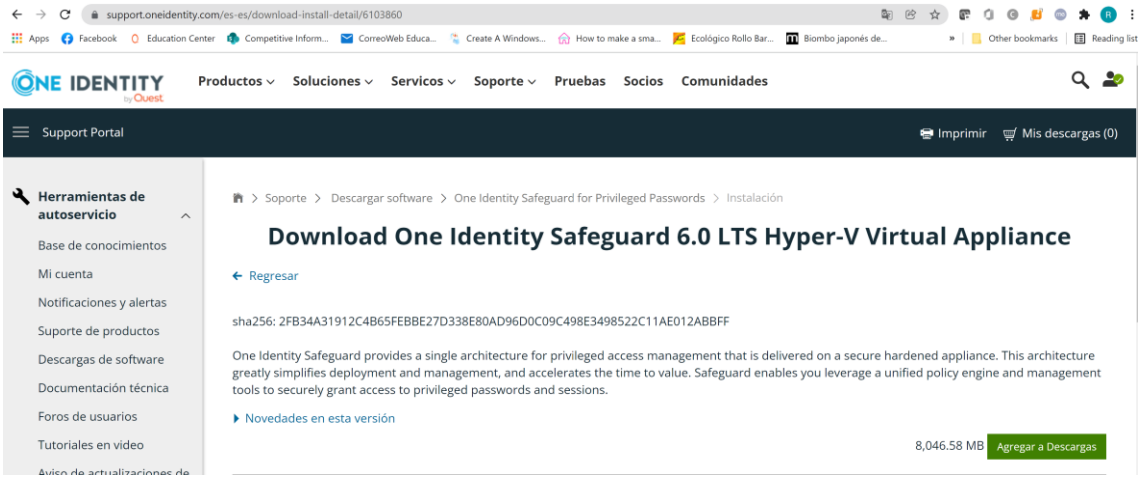

Figura 6 – Página de soporte con la información del hash de imagen Hyper-V

- Imagen virtual para entornos VMware vSphere con vSphere Hypervisor (ESXi) versión 6.5 o superior. La OVA descargada es directamente importada en entornos VMware, para desplegar máquinas virtuales preinstaladas y configuradas:

  a) spp-vmware-6.0.0.12276.ova

  b) Hash SHA256:

  2FADD6C2E9DB4EF288F232F1E4B4A76776AFBE88C27EBD5713C12504D5F7129E

  El hash del archivo puede ser verificado en la siguiente web **[REF11]**:

  https://support.oneidentity.com/es-es/download-install-detail/6103861

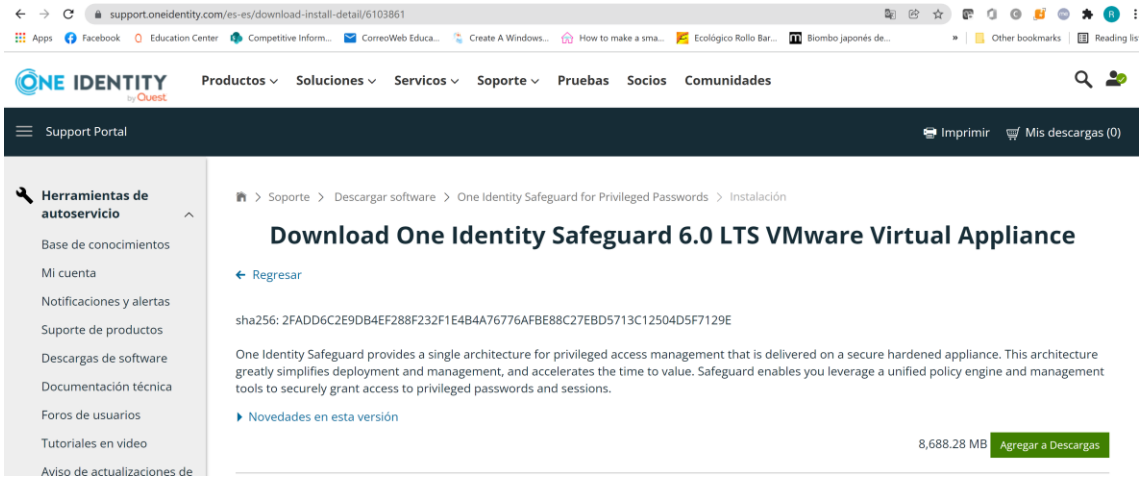

Figura 7 – Página de soporte con la información del hash de imagen VMware

19. A continuación, se muestran los comandos que se pueden emplear en cualquier equipo con sistema operativo Windows y Powershell instalado donde se hayan podido descargar las imágenes virtuales para Hyper-V o VMware desde la página de soporte de One Identity, para confirmar el hash de los archivos descargados:

```
Get-FileHash spp-vmware-6.0.0.12276.ova |Format-List
```

Get-FileHash spp-hyperv-6.0.0.12276.zip |Format-List

4.2 ENTORNO DE INSTALACIÓN SEGURO

20. Si se ha adquirido el dispositivo físico, este debe ser instalado en el CPD del cliente, con el adecuado control de acceso físico.

21. Para una correcta instalación, se debe revisar la sección "Hardware Appliance" de la Guía de "One Identity Safeguard for Privileged Passwords 6.0 LTS – "Appliance Setup Guide" **[REF6]**.

4.3 REGISTRO Y LICENCIAS

22. Si se ha adquirido el producto SPP, los archivos de licencia correspondientes habrán sido enviados a la dirección de correo electrónico empleada para el proceso de registro en la página de soporte de One Identity **[REF4]**. Si no se ha recibido dicho correo electrónico, será necesario visitar la página de soporte de One Identity **[REF5]**.

23. La Instalación de las licencias se realiza desde el cliente de administración – *Settings* > *Appliance* > *Licensing*. Hacer *click* en el símbolo de "*Más*", y añadir el fichero de licencia obtenido desde One Identity.

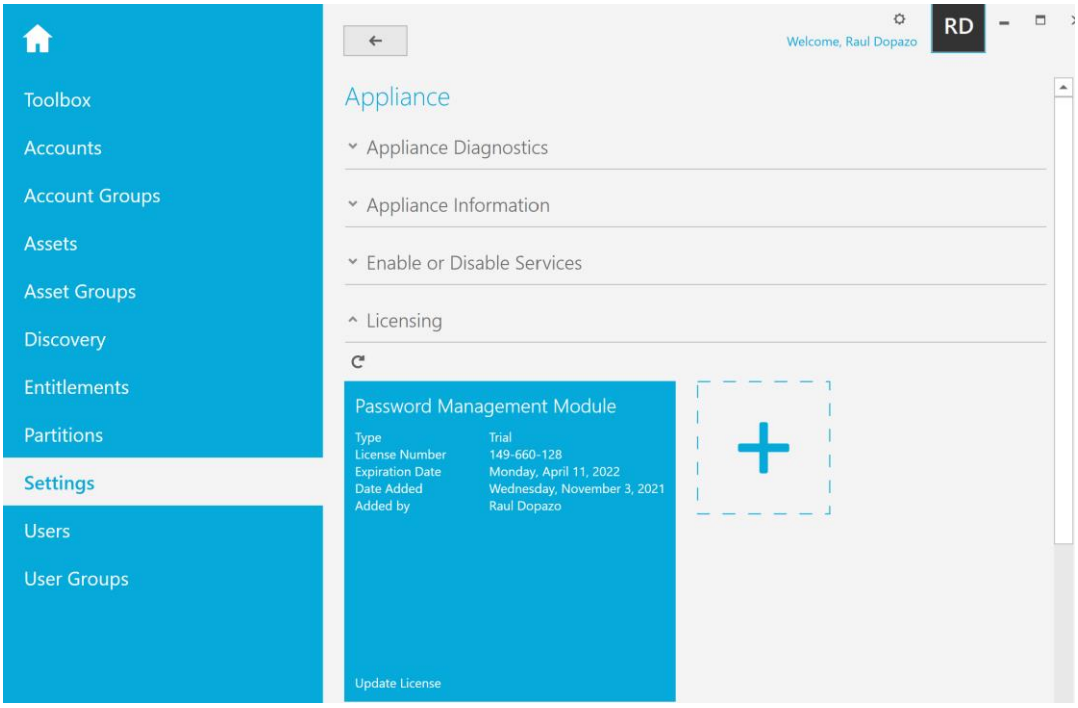

Figura 8 – Sección de licencias de la consola de administración

4.3.1 LICENCIAS – *APPLIANCE HARDWARE*

24. El *appliance* físico de SPP se envía con el módulo "*Privileged Passwords*" incluido. Dicho módulo requiere para su funcionamiento una licencia válida. Si dicha licencia no está instalada en el appliance, no se podrán llevar a cabo solicitudes de contraseñas privilegiadas.

25. El *appliance* físico de SPP incluye la licencia del sistema operativo subyacente.

4.3.2 LICENCIAS – DISPOSITIVO VIRTUAL

26. Es necesario licenciar el sistema operativo subyacente en los dispositivos virtuales con una licencia de Microsoft Windows. Se recomienda emplear bien el método MAK, o el método KMS. Para más información acerca del método MAK **[REF12]** o KMS **[REF13]**, se recomienda consultar los siguientes enlaces:

    https://docs.microsoft.com/es-es/licensing/products-keys-faq#qu--es-una-clave-de-activaci-n-m-ltiple--mak

    https://docs.microsoft.com/es-es/licensing/products-keys-faq#-qu--es-una-clave-kms-host

27. El *appliance* virtual de SPP se envía con el módulo "*Privileged Passwords*" incluido. Dicho módulo requiere para su funcionamiento una licencia válida. Si dicha licencia no está instalada en el *appliance*, no se podrán llevar a cabo solicitudes de contraseñas privilegiadas.

28. La licencia de Microsoft Windows requerida por el dispositivo virtual de SPP es Windows 10 LTSC **[REF14]**.

29. En el apartado "*Operating system licensing*", de la Guía de Administración **[REF1]** del producto se encuentran los pasos a seguir para gestionar la licencia del sistema operativo del dispositivo virtual.

4.3.3 EXPIRACIÓN DE LICENCIAS

30. Si el usuario Administrador del *appliance* recibe una notificación de expiración de licencia, será necesario aplicar una licencia nueva empleando un enlace de Actualización de Licencia. En el apartado "*License expiration notice*" de la Guía de Administración **[REF1]** del producto se describen los pasos a seguir para actualizar la licencia.

31. Para más información, se recomienda consultar el apartado "*License: hardware, virtual, expiration*", de la Guía de Administración **[REF1]** del producto.

4.4 CONSIDERACIONES PREVIAS

32. Al configurar un entorno virtual, es necesario considerar cuidadosamente los aspectos de la configuración, como la CPU, la disponibilidad de memoria, el subsistema de E/S y la infraestructura de red, para asegurarse de que la capa

virtual dispone de los recursos necesarios. Se recomienda consultar las políticas de soporte de productos de One Identity para obtener más información sobre la virtualización del entorno.

33. A continuación, se introducen los recursos mínimos necesarios para el despliegue del producto: 4 CPU, 10 GB de RAM y 1 disco duro de 300 GB.

    Nota. Cuando se importan las imágenes virtuales en VMware o Hyper-V, estas están configuradas para usar unos recursos (memoria, CPU y disco) menores a los mínimos necesarios, por lo que hay que asegurarse de que se amplían los recursos asignados a la máquina virtual para que se cumplan estos recursos mínimos.

5. FASE DE INSTALACIÓN

5.1 INSTALACION DEL DISPOSITIVO *HARDWARE*

5.1.1 ADVERTENCIAS Y PRECAUCIONES

34. Se recomienda leer el Anexo "*Warnings and precautions*" del *Appliance Setup Guide* **[REF6]** del producto, antes de comenzar con el proceso de instalación del dispositivo hardware.

5.1.2 CONSIDERACIONES SOBRE EL DISPOSITIVO Y EL MONTAJE

35. En el apartado "*Appliance and mounting considerations*" del *Appliance Setup Guide* **[REF6]** se encuentran una serie de consideraciones sobre el aparato y su montaje, que han de tenerse en cuenta a la hora de la instalación del *appliance* físico.

5.1.3 ASPECTOS A TENER EN CUENTA DURANTE EL PROCESO DE INSTALACIÓN DEL DISPOSITIVO *HARDWARE*

36. A continuación, se enumeran una serie de aspectos a tener en cuenta durante el proceso de instalación y configuración inicial del dispositivo One Identity SPP:

- Conexión del equipo de gestión al dispositivo:
  - El puerto utilizado para la configuración inicial del dispositivo es el puerto de gestión (MGMT). La dirección IP asignada a este puerto es fija y no puede ser modificada. Siempre estará disponible en caso de que la interfaz primaria (interfaz X0) no esté disponible. La dirección IP del puerto de gestión del dispositivo es 192.168.1.105. Esta dirección IP no puede ser modificada.
  - Será necesario modificar la dirección IP de la interfaz primaria (X0) para hacerla coincidir con la configuración de red correspondiente.
  - Será necesario establecer la dirección IP del equipo de gestión en 192.168.1.100, la máscara de subred en 255.255.255.0, y ninguna puerta de enlace predeterminada. Esta configuración IP en el equipo de gestión es obligatoria para tener conectividad por cable con el puerto de gestión de Safeguard con IP 192.168.1.105.
- Inicio de sesión en SPP:
  - Para iniciar sesión, será necesario acceder a la URL https://192.168.1.105 desde el equipo de gestión.
  - Para mantener la seguridad del dispositivo SPP, se recomienda cambiar la contraseña predeterminada de la cuenta del Administrador de *Bootstrap* (*Bootstrap Administrator*). Para obtener más información, consultar "*Step 6: Log in to Safeguard for*

Privileged Passwords" del documento de *"Appliance Setup Guide"* **[REF6]**.

- Configuración de la interfaz de red primaria (X0):
    - Será necesario iniciar sesión y descargar el cliente de escritorio para completar los siguientes pasos del proceso de instalación. Para obtener más información al respecto, se recomienda consultar el apartado "Cómo completar la configuración del dispositivo" del documento de "Appliance Setup Guide" **[REF6]**.

37. La información completa referente al proceso de instalación del dispositivo hardware (appliance) puede encontrarse en el apartado *"Setting up the hardware appliance"*, del Appliance Setup Guide **[REF6]**.

38. Como mejor práctica, después de haber creado un clúster de SPP (o si sólo utiliza una única Máquina Virtual), se recomienda cambiar la configuración de servidores de confianza, para prevenir que otros servidores puedan realizar peticiones externas CORS (*Cross Origin Resource Sharing*) **[REF16]** y redirecciones de inicio de sesión en Safeguard. Haciendo esto, se proporcionará una lista de servidores aceptados por Safeguard para integrar las aplicaciones que sean de confianza. Por defecto, en Safeguard se permiten estas peticiones externas desde cualquier IP. Para obtener más detalles, se puede consultar la Guía de Administración del producto **[REF1],** apartado "Servidores de confianza, CORS y Redirecciones".

5.2 INSTALACIÓN DEL DISPOSITIVO VIRTUAL

39. Esta sección cubre los requerimientos y los pasos necesarios para configurar la máquina virtual en la que se va a desplegar el *software Safeguard* por primera vez.

40. Se debe de disponer de una licencia de Windows 10 LTS para licenciar la Máquina Virtual. Se recomienda utilizar el método MAK **[REF12]** o KMS **[REF13]**.

    https://docs.microsoft.com/es-es/licensing/products-keys-faq#qu--es-una-clave-de-activaci-n-m-ltiple--mak

    https://docs.microsoft.com/es-es/licensing/products-keys-faq#-qu--es-una-clave-kms-host

41. Como se ha descrito anteriormente, el a*ppliance* virtual no funcionará a no ser que el sistema operativo sea debidamente licenciado.

42. Tal y como se ha mencionado anteriormente en este documento, la licencia de Microsoft Windows requerida por el dispositivo virtual de SPP es Windows 10 LTSC.

43. Para un correcto despliegue de la OVA de SPP en el sistema de virtualización correspondiente, se recomienda seguir el apartado *"Setting up the virtual appliance"* de la guía "*Appliance Setup Guide*" **[REF6].**

44. Una vez desplegada la OVA, desde la consola del hipervisor se accede a la consola *Safeguard Virtual Kiosk*, la cual solo está disponible en los dispositivos virtuales

para poder hacer la configuración inicial de Safeguard, con los siguientes *Wizards* disponibles:

- Configuración inicial: se utiliza para configurar el dispositivo virtual por primera vez.
- Configuración: después de la primera configuración, las actualizaciones de nombre, y de red de *One Identity Safeguard for Privileged Passwords* se pueden realizar a través del *Virtual Kiosk* haciendo clic en Configuración.
- Quiosco de soporte: El quiosco de soporte se utiliza para diagnosticar y resolver problemas con SPP. Para más información, consultar el apartado "*Support Kiosk*", de la Guía de Administración **[REF1]** del producto.

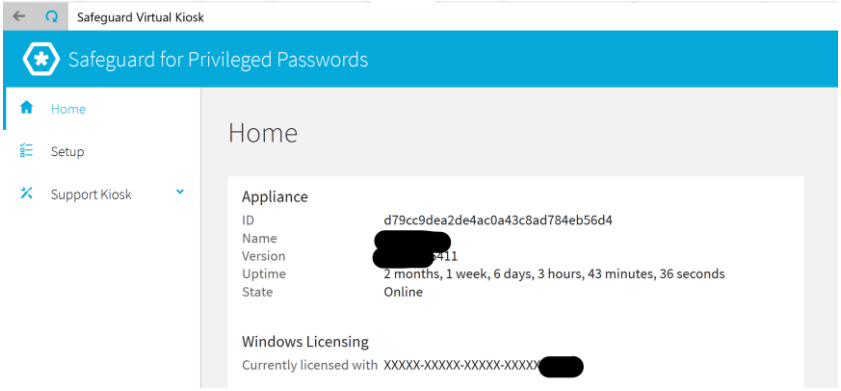

Figura 9 – Web del Kiosko Virtual

45. Los pasos a seguir para llevar a cabo el despliegue del appliance Virtual, así como su acceso y configuración inicial se encuentran en el apartado "*Setting up the virtual appliance*", del *Appliance Setup Guide* **[REF6]**.

46. Para más información al respecto, se recomienda consultar el apartado "*Step 5: Log in and configure Safeguard for Privileged Passwords*" de la Guía de Administración **[REF1]** del producto.

5.3 INSTALACIÓN DE LA CONSOLA DE ADMINISTRACION

47. Para la administración de SPP se requiere la instalación de un **cliente de escritorio** en un puesto de trabajo que vaya a ser utilizado para la administración del producto. Esta consola de administración puede instalarse en los equipos que sean necesarios. Los requisitos para su instalación son:

- Microsoft .NET Framework 4.6 (o superior)
- Versiones de arquitectura de 64 bits de:
  - Windows 7
  - Windows 8.1
  - Windows 10
  - Windows Server 2008 R2

- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

48. Si en la configuración de Safeguard, TLSv1.2 está habilitada (dicha configuración puede comprobarse en *Herramientas administrativas > Configuración > Dispositivo > Información del dispositivo*), **es necesario asegurarse de que el cliente de escritorio también tenga TLSv1.2 habilitado**. Si el cliente tiene una versión anterior de TLS habilitada, se bloqueará el acceso al cliente y no podrá conectarse a SPP.

49. Para descargar el archivo *.msi* del instalador de **Windows del cliente de escritorio** de SPP, es necesario abrir el navegador e ir a: *https: // <IP del dispositivo> /Safeguard.msi*

50. A continuación, se debe guardar el archivo Safeguard.msi en la ubicación elegida y seguir los siguientes pasos:

    - Ejecutar el paquete MSI.
    - Seleccionar '*Siguiente'* en el cuadro de diálogo de bienvenida.
    - Aceptar el Acuerdo de licencia de usuario final y seleccionar '*Siguiente'*.
    - Seleccionar '*Instalar'* para comenzar la instalación.
    - Seleccione '*Finalizar'* para salir del asistente de configuración del cliente de escritorio.

51. Para más información al respecto, se recomienda consultar el apartado "*Completing the appliance setup*", de la *Appliance Setup Guide* **[REF6]**.

6. FASE DE CONFIGURACION

6.1 MODO DE OPERACIÓN SEGURO

52. **SPP es un producto preinstalado y bastionado de fábrica**. Toda la seguridad aplicada al dispositivo (físico o virtual) está basada en un conjunto de buenas prácticas de seguridad.

53. Para obtener una referencia completa de estas medidas de seguridad, consultar el siguiente documento **[REF2]**:

    https://www.oneidentity.com/docs/understanding-the-security-architecture-of-the-one-identity-safeguard-appliance-technical-brief-25629.pdf

54. La única manera de acceder a Safeguard (ya sea en formato físico o virtual) es mediante HTTPS, a través de la REST API que se expone. No es posible acceder al sistema operativo contenido en el Dispositivo.

55. Para habilitar solo clientes que soporten TLSv1.2, desde la consola de administración del producto, se debe habilitar la opción *TLS 1.2 Only*.

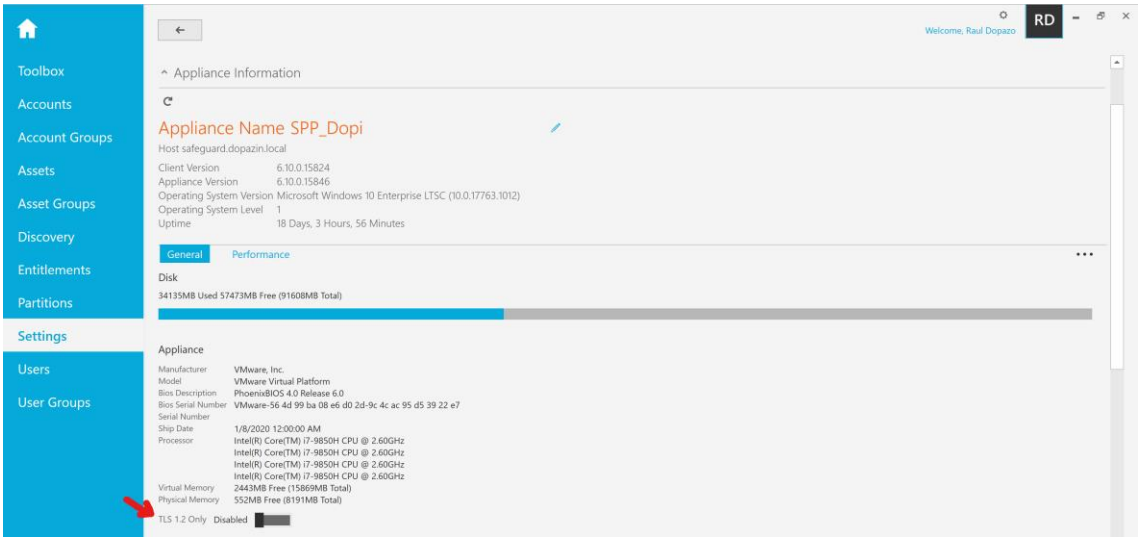

Figura 10 – Settings > Appliance Information > TLS 1.2 Only

6.2 IDENTIDAD Y AUTENTICACIÓN

56. SPP permite crear varios tipos de proveedores de identidad y autenticación para integrarlos con los servicios de directorio existentes. Esto ayuda a gestionar eficazmente a los usuarios y la forma en que iniciarán sesión en Safeguard. Es posible crear proveedores para *Active Directory*, LDAP 2.4, cualquier servicio federado SAML 2.0 o RADIUS.

57. Para ser gestionado, *Active Directory* debe añadirse como sistema final y como proveedor de identidad. Como sistema final a gestionar, se refiere a poder administrar las cuentas privilegiadas y sus contraseñas de Active Directory. Como proveedor de identidad, se refiere a que una vez añadidos los usuarios de Active

Directory en Safeguard, estos usuarios podrán autenticarse en Safeguard mediante sus cuentas de AD.

58. SPP implementa control de acceso basado en roles, empleando una jerarquía de conjuntos de permisos de administración. Existen diferentes roles de usuario administrador. Los roles de auditor y administrador de activos (*Asset Administrator*) tienen permiso para acceder a las cuentas. El rol de Auditor otorga permisos para poder leer la información: activos, cuentas, logs de actividad, etc.

59. Es responsabilidad del autorizador (*Authorizer Administrator,* rol en Safeguard que permite asignar permisos en Safeguard a otros usuarios), o del administrador de usuarios (*User* Administrator, rol en Safeguard que permite crear y gestionar usuarios) configurar una cuenta de usuario para que utilice la autenticación de dos factores al iniciar sesión en Safeguard para contraseñas privilegiadas.

60. Adición de proveedores de identidad y autenticación. Es responsabilidad del administrador de activos añadir repositorios de usuarios o cuentas basados en LDAP (ya sea AD de Microsoft u otros LDAP) a Safeguard para utilizarlos como proveedores de identidad y autenticación. Una vez añadidos estos directorios, se podrán añadir en Safeguard usuarios basados estos proveedores de autenticación para poder autenticarse en Safeguard. Para más información sobre cómo llevar a cabo el proceso de adición de proveedores de identidad y autenticación, se recomienda consultar el apartado "*Adding identity and authentication providers*", de la Guía de Administración **[REF1]** del producto.

61. Es responsabilidad de un administrador de usuarios (*User Administrator*) o de un administrador de dispositivos crear un proveedor de federación externa o de RADIUS para utilizarlo para la autenticación.

62. La autenticación basada en RADIUS es válida tanto para autenticación de usuarios con contraseñas, como para ejercer el papel de doble factor de autenticación. Es posible crear y configurar un servidor RADIUS, para usarlo como proveedor de autenticación principal o como proveedor de autenticación secundario. Para usar un servidor RADIUS para la autenticación primaria y secundaria, será necesario crear dos proveedores de autenticación diferentes. Para información detallada acerca de cómo añadir un servidor RADIUS como proveedor de autenticación, se puede consultar la sección de *"Adding identity and authentication providers" Radius Settings*, de la Guía de Administración **[REF1]** del producto.

63. Configuración de la federación externa. SPP es compatible con el perfil SAML 2.0 Web Browser SSO **[REF17]** (https://en.wikipedia.org/wiki/SAML_2.0), lo que permite configurar la autenticación federada con muchos servidores y servicios STS (Servicio de Token de Seguridad) diferentes, como AD FS (Servicios de Federación de *Active Directory*) de Microsoft. Esta configuración permitirá iniciar sesion en SPP usando una cuenta de un *Identity Provider* externo. Mediante el intercambio de los metadatos de federación, es posible crear una relación de confianza entre los dos sistemas, Safeguard y el IDP de autenticación. A continuación, se creará una cuenta de usuario de SPP que se asociará a la cuenta federada. Este proceso consiste en dar de alta un usuario en Safeguard, siendo

este usuario un usuario del sistema federado, pudiéndole así asignar los permisos requeridos en Safeguard para su uso, así como el permiso de autenticación en SPP usando esa cuenta externa del dominio federado. Cuando un usuario final inicie sesión, será redirigido al STS externo para que introduzca sus credenciales y realice cualquier autenticación de dos factores que pueda requerir ese STS. Una vez que la autenticación sea satisfactoria, se le redirigirá de nuevo a SPP y se iniciará la sesión.

NOTA: Se puede asignar una autenticación de dos (2) factores adicionales a la cuenta de usuario de SPP asociada, para que el usuario se autentique de nuevo, después de ser redirigido desde el STS externo. Esta opción se configura desde el cliente de Administración de Safeguard, en Configuración > Usuarios, en las opciones de un usuario concreto en la sección '*Authentication*':

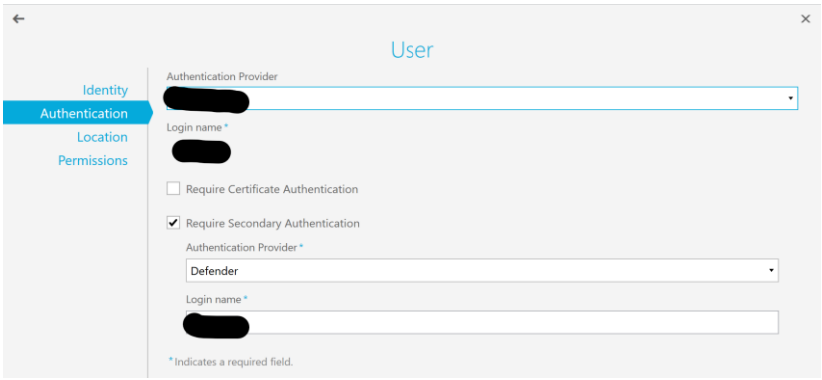

Figura 11 – Método de autenticación del usuario – doble factor

64. Para utilizar la federación externa, primero es necesario descargar el XML de metadatos de federación para su STS y guardarlo en un archivo. Por ejemplo, para AD FS de Microsoft, es posible descargar el XML de metadatos de federación desde *https://<servidoradfs>/FederationMetadata/2007-06/FederationMetadata.xml*.

65. Para más información sobre cómo añadir un proveedor de identidad externo, se recomienda consultar el apartado "*How do I add an external federation provider trust*" de la Guía de Administración **[REF1]** del producto.

66. El producto también soporta la creación de usuarios locales. Para crear usuarios locales, desde la herramienta de administración, en '*Usuarios*' pulsar el botón '*Añadir*' y seleccionar el proveedor local.

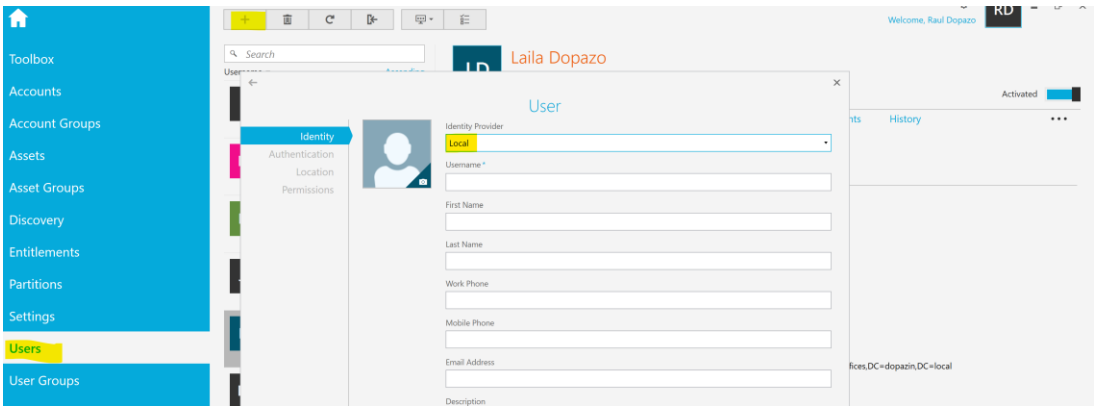

Figura 12 – Creación de un usuario final en Safeguard

67. Es posible configurar SPP para autenticarse en un sistema empleando claves SSH. SPP requiere autenticarse en los sistemas finales gestionados. Aquellos que soporten SSH y claves SSH, podrán ser usadas por Safeguard para conectar y gestionar ese sistema final.

68. Asimismo, SPP hace uso de certificados SSL auto-firmados, y utilizados para las conexiones HTTPS, empleadas para la conexión con el producto.

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

69. El único método de acceso para la administración del producto es mediante la REST API proporcionada por SPP, a través del protocolo HTTPS. Tanto la consola de administración como la consola web (empleada durante el proceso de configuración inicial del producto) hacen uso del protocolo HTTPS para sus comunicaciones. Todas las funciones de administración están expuestas a través de esta REST API.

70. Es necesario instalar el cliente de escritorio para la administración del producto. Este cliente de escritorio se conecta a SPP a través de la misma REST API. Está disponible un tutorial sobre REST API, ubicado en GitHub, en el siguiente enlace **[REF7]**: https://github.com/oneidentity/safeguard-api-tutorial. Las consolas proporcionadas para la configuración inicial del producto también acceden a Safeguard a través de su REST API.

71. **El producto no permite la configuración local**. Por motivos de seguridad, Safeguard está diseñado para que ningún componente interno (sistema operativo, servicios de bases de datos, etc) del producto sea expuesto, y además está bloqueado el acceso al sistema operativo contenido en el dispositivo (físico o virtual).

72. Como se ha mencionado anteriormente, parte de la configuración inicial de SPP consiste en asignarle una IP de servicio. Esta IP de servicio es la única manera de comunicarse con SPP y, además, solo a través del protocolo HTTPS accediendo a la REST API expuesta sobre la IP de servicio. Por tanto, una vez que el dispositivo físico ha sido configurado a través del puerto de MGMT (puerto de gestión), la única manera de llevar a cabo su administración es a través de la REST API, desde cualquier estación de trabajo que tenga conectividad HTTPS a la IP del dispositivo y un usuario con rol de administración (además del cliente de administración de escritorio instalado). El cliente de escritorio puede hacer uso del protocolo TLSv1.1 o TLSv1.2 para la conexión con el Safeguard, dependiendo de cómo se configure SPP. No obstante, **se debe configurar SPP para que solo acepte conexiones TLSv1.2.** Para más información al respecto, se recomienda consultar los siguientes enlaces:

[REF18] https://support.oneidentity.com/one-identity-safeguard-for-privileged-passwords/kb/316464/enabling-tls-1-2-only-option-on-appliances

[REF19] https://support.oneidentity.com/technical-documents/one-identity-safeguard-for-privileged-passwords/6.7.3/release-notes/2#TOPIC-1788353

73. Para la administración (gestión de las contraseñas de las cuentas privilegiadas) de activos (*sistemas finales)*, el producto emplea para la conexión al sistema final pares de claves SSHv2, generadas empleando claves RSA. Safeguard soporta claves RSA de longitudes: 1024, 2048, 4096 y 8192. **Por motivos de seguridad, se deben emplear longitudes de clave RSA Iguales o superiores a 3072 bits.**

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

74. La administración basada en roles está basada en la seguridad de su propia REST API. El modelo de seguridad del producto identifica una serie de roles de administración. Esto significa que no importe qué herramienta se usa para administrar Safeguard, toda comunicación es a través del API y aplica RBAC (*Role-Based Access Control*).

75. En este sentido, las conexiones a Safeguard siempre serán remotas, independientemente de si se accede usando la consola de administración o si se hace la conexión mediante llamadas directamente a través de la REST API. Se aplicará siempre un modelo de permisos basado en los siguientes roles:

- *Authorizer Administrator:* permite al usuario otorgar permisos a otros usuarios, así como cambiar sus propios permisos. Para más información, se recomienda consultar el apartado "*Authorizer Administrator permissions*", de la Guía de Administración **[REF1]** del producto.
- *User Administrator:* permite la creación de nuevos usuarios, desbloquear y resetear contraseñas de usuarios que no tienen rol de administración. Para más información, se recomienda consultar el apartado "*User Administrator permissions*", de la Guía de Administración **[REF1]** del producto.
- *Help Desk Administrator:* permite desbloquear y establecer contraseñas para usuarios que no tienen rol de administración. Para más información, se recomienda consultar el apartado "*Help Desk Administrator permissions*", de la Guía de Administración **[REF1]** del producto.
- *Appliance Administrator:* permite editar y actualizar el *appliance*, así como editar parámetros de configuraciones externas, como email, *Syslog*, etc. Para más información, se recomienda consultar el apartado "*Appliance Administrator permissions*", de la Guía de Administración **[REF1]** del producto.
- *Operations Administrator:* permite reiniciar y monitorizar el *appliance*. Para más información, se recomienda consultar el apartado *"Operations Administrator permissions"*, de la Guía de Administración **[REF1]** del producto.

- *Auditor:* otorga al usuario permisos de solo-lectura. Para más información, se recomienda consultar el apartado "*Auditor permissions*", de la Guía de Administración **[REF1]** del producto.
- *Asset Administrator:* permite al usuario añadir, editar y eliminar particiones, activos y cuentas. Para más información, se recomienda consultar el apartado "*Asset Administrator permissions*", de la Guía de Administración **[REF1]** del producto.
- *Security Policy Administrator:* permite al usuario añadir editar y eliminar derechos (*entitlements*) y políticas que controlan el acceso a cuentas y activos. Para más información, se recomienda consultar el apartado "Security Policy Administrator permissions", de la Guía de Administración **[REF1]** del producto.

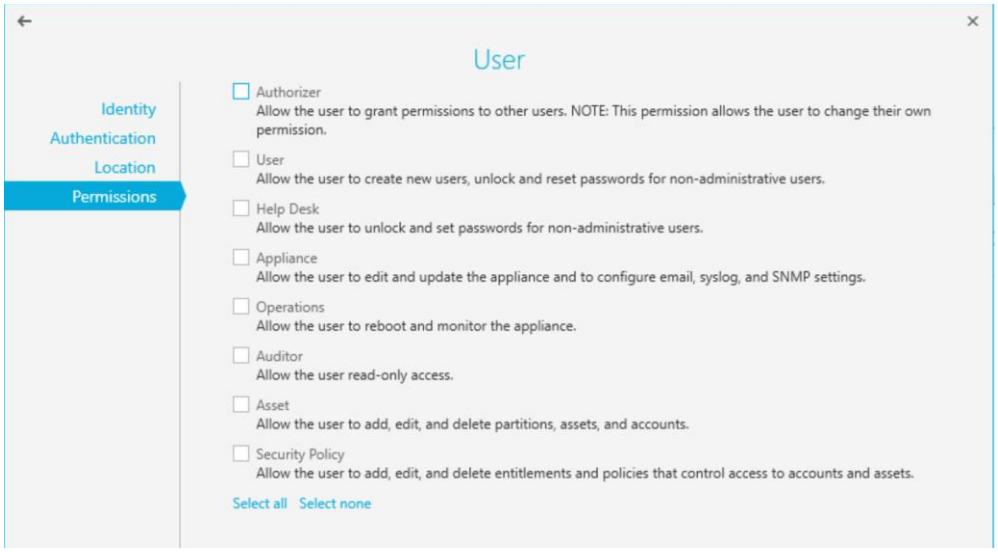

Figura 13 – Roles de Administración de One Identity Safeguard for Privileged Passwords

76. Un usuario puede tener más de un conjunto de permisos. Para ver una lista de permisos otorgados a los diferentes administradores de SPP, se puede consultar el apartado "*Administrator permissions*", de la Guía de Administración **[REF1]**.

77. A través del menú *Administrative Tools > Settings > Safeguard Access*, se puede acceder a las opciones de control de acceso al producto. Para más información acerca de todos los parámetros posibles en el control de *login*, se recomienda consultar el apartado "*Local Login Control*" de la Guía de Administración **[REF1]** del producto.

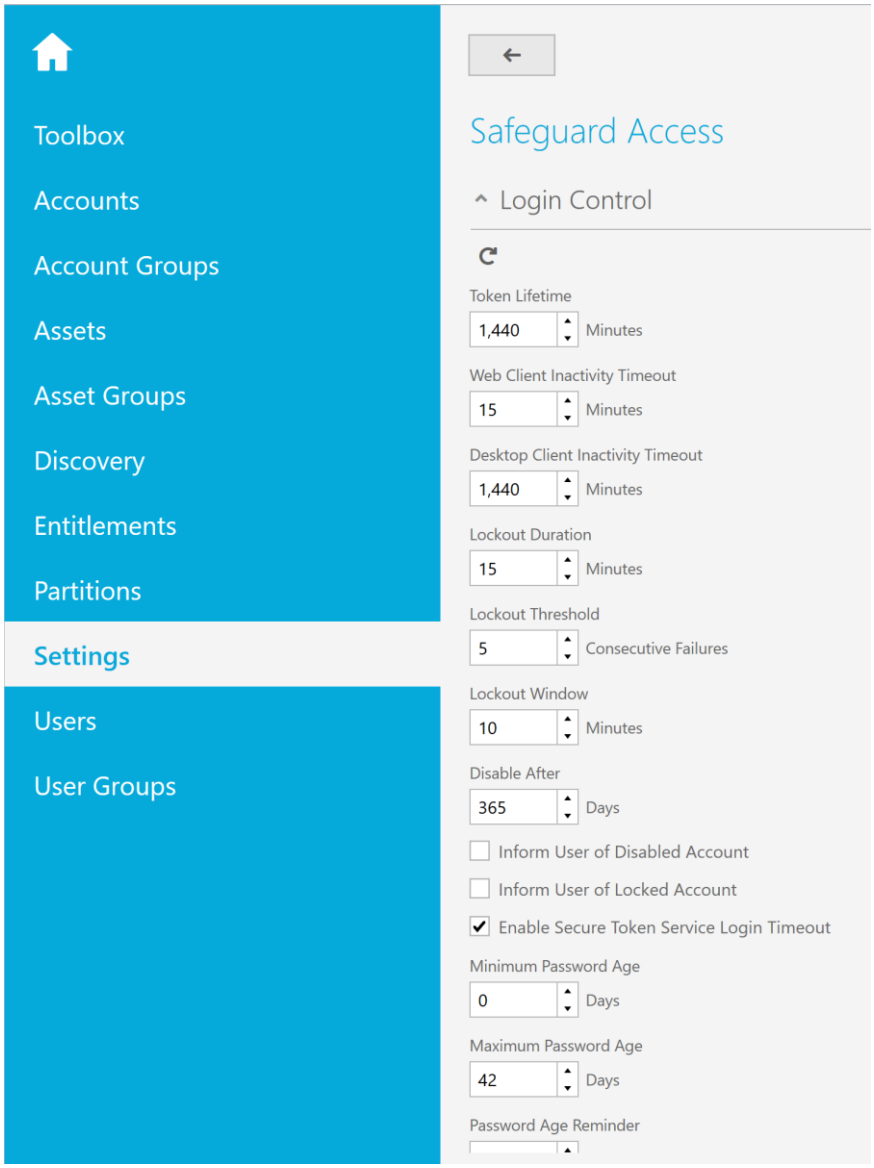

Figura 14 – Parámetros de control de *login* en *Safeguard*

78. A continuación, se introduce una serie de recomendaciones de seguridad relacionadas con los parámetros de control de *login* (ver Figura 14):

- Establecimiento del **tiempo de validez de las contraseñas en 60 días**. Por defecto, este valor está configurado en 42 días.
- Establecimiento del **tiempo de inactividad** de las sesiones en **5 minutos** (300 segundos). Por defecto, este parámetro está configurado en 15 minutos.
- Establecimiento del **umbral de intentos fallidos** de autenticación en **5 intentos**. Para este parámetro, el valor recomendado ya está configurado por defecto.
- Establecimiento del **tiempo de bloqueo** tras superar el umbral de intentos fallidos de autenticación en **5 minutos** (300 segundos). Por defecto, este parámetro está configurado en 15 minutos.

– No permitir la reutilización de (al menos) las últimas 5 contraseñas empleadas. Para este parámetro, este ya es el valor configurado por defecto.

79. Para más información acerca de estos parámetros de control de *login*, se recomienda consultar el apartado "*Login Control*", de la Guía de Administración **[REF1]** del producto.

6.3.2.1 POLÍTICA DE CONTRASEÑAS

80. Las reglas de contraseñas únicamente son aplicables a los usuarios locales del producto. Al menú de configuración de reglas de contraseñas se accede desde *Administrative Tools > Settings > Safeguard Access*. Dicho menú ofrece las siguientes opciones:

- Configuración de la longitud de la contraseña. **Se debe configurar una longitud mínima de 12 caracteres.**
- Tipo del primer y último carácter.
- Obligatoriedad en la utilización de mayúsculas, minúsculas, números u otros símbolos ASCII, así como el mínimo de cada uno de ellos. **Como mínimo, las contraseñas han de contar con un carácter en minúscula, un carácter en mayúscula, un número y un carácter especial.**
- Identificar exclusiones como letras mayúsculas o minúsculas, números y símbolos.
- Identificar el uso de letras, números u otros símbolos consecutivos si son repetidos, y si son permitidos el número máximo de repeticiones permitidas.

6.3.2.2 REGLAS PARA CONTRASEÑAS ASOCIADAS A CUENTAS

81. Para gestionar las reglas de creación de contraseñas para cuentas, se debe ir al menú *Administrative Tools > Settings > Profile > Account Password Rules*. Dicho menú ofrece las siguientes opciones:

- La longitud de la contraseña debe tener entre 3 y 225 caracteres. **Se debe configurar una longitud mínima de 12 caracteres.**
- Selección del tipo del primer y último carácter de la contraseña.
- Permitir mayúsculas, minúsculas, número y/o otros símbolos ASCII, así como la cantidad mínima de cada uno de ellos. **Como mínimo, las contraseñas han de contar con un carácter en minúscula, un carácter en mayúscula, un número y un carácter especial.**
- Identificar caracteres excluidos, como letras mayúsculas, minúsculas, números y símbolos.
- Identificar si letras, números y/o símbolos consecutivos pueden ser repetidos secuencialmente y, si está permitido, indicar el número máximo permitido de repeticiones.

6.3.2.3 CONFIGURACIÓN DEL MENSAJE DE AVISO Y CONSENTIMIENTO EN EL INICIO DE SESIÓN

82. Se debe configurar el mensaje de aviso y consentimiento en el inicio de sesión. Para ello, se debe acceder a: *Settings > Messaging > Login Notification.*

83. La responsabilidad de configurar el mensaje de aviso que se muestra al usuario en el momento de hacer *login* recae en el Administrador del *appliance*. A continuación, se enumeran los pasos a seguir para configurar dicho mensaje:

    - Ir a *Administrative Tools > Settings > Messaging > Login Notifications.*
    - Seleccionar la opción *Message*, e introducir el mensaje.
    - Hacer click en *OK*.

6.4 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

84. Para el uso seguro de conexiones HTTPS, es requerido instalar un certificado de confianza en SPP. Para ello, se debe acceder, desde el cliente de administración, al menú *Settings > Certificates > SSL Certificates.*

85. Se puede importar un certificado generado por una CA de confianza o generar un CSR (*Certificate Signing Request*) para poder ser completada en una CA de confianza. La recomendación es **generar un CSR con una longitud de clave superior a 3072 bits.**

86. Se debe habilitar TLS 1.2 Only desde cliente de administración – *Settings > Appliance Information >TLS 1.2 Only > Enable*

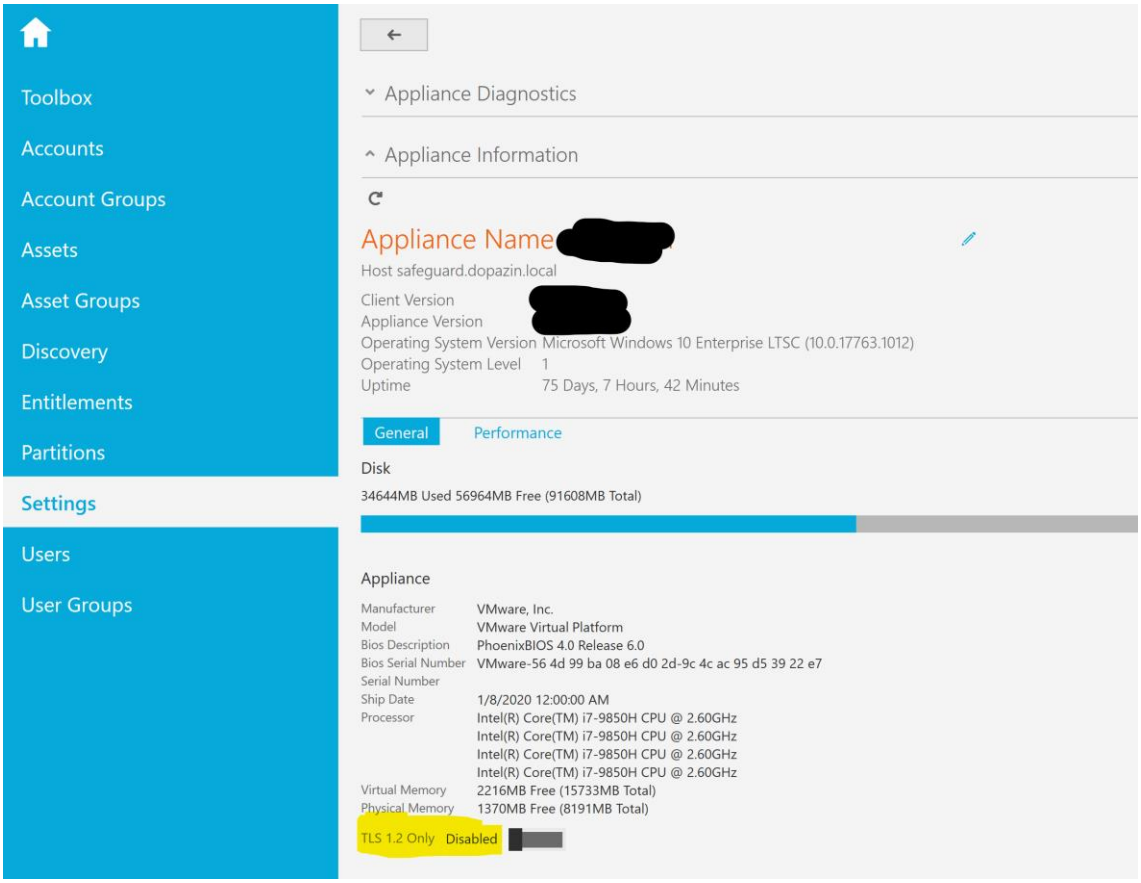

Figura 15 – Habilitación de TLS 1.2 Only

6.5 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

87. Safeguard no permite configurar interfaces, puertos y servicios. Estas configuraciones vienen establecidas de fábrica, y no es posible modificarlas.

88. Para más información acerca de los puertos involucrados en la operación del producto, se recomienda consultar el apartado "*Safeguard ports*", de la Guía de Administración **[REF1]** del producto.

6.6 GESTIÓN DE CERTIFICADOS

89. Al menú de gestión de certificados se puede acceder *desde Administrative Tools > Settings > Certificates.* A continuación, se enumeran los tipos de certificados que componen la estructura de certificados de SPP.

6.6.1 CERTIFICADOS A REEMPLAZAR

90. SPP incorpora por defecto una serie de certificados, destinados a ser reemplazados por motivos de seguridad:

    – Un certificado SSL auto-firmado, empleado para comunicaciones HTTPS. El nombre de este certificado coincide con el *hostname* del *appliance*, y utiliza

la dirección IP por defecto del *appliance* como el *Subject Alternative Name* (SAN).

- Un certificado de firma, empleado para validar que los ficheros de auditoría archivados en un servidor de archivos externo han sido creados en el *appliance*.

6.6.2 PETICION DE FIRMA DE CERTIFICADOS (CSR)

91. SPP admite solicitudes de firma de certificados (CSR) para inscribir cualquier tipo de certificado. Los CSR utilizan el estándar de criptografía de clave pública (PKCS) Formato # 10. Todas las peticiones CSR que se generen se podrán visualizar en la sección del cliente de administración - *Settings > Certificates > Certificate Signing Resquests.*

92. Una vez obtenido el certificado de la CA correspondiente, para las importaciones de certificados, SPP debe acceder a la red correspondiente para validar los CRL (*Certificate Revocation Lists*) especificados en el CSR firmado.

93. Para certificados SSL, SPP permite cargar o usar un CSR para inscribir varios certificados que luego se pueden aplicar a diferentes dispositivos.

94. SPP proporciona un almacén de certificados SSL que le permite asignar cualquier certificado SSL cargado o inscrito a cualquier dispositivo Safeguard (físico o virtual).

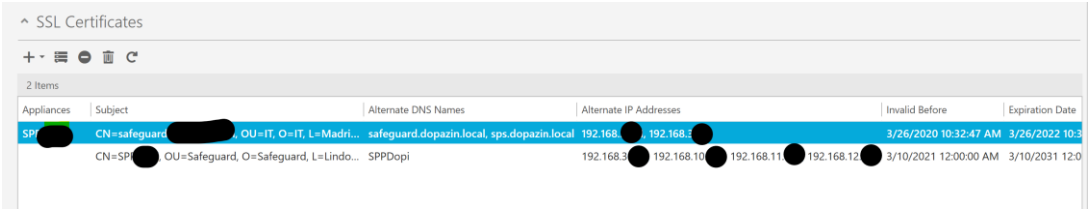

Figura 16 – Asignación de certificados SSL a dispositivos Safeguard

6.6.3 CERTIFICADOS DE CONFIANZA

95. Para cargar certificados con claves privadas, SPP admite archivos .pfx (o .p12) que siguen el estándar PKCS # 12.

96. Para importar estos certificados como certificados de confianza, ir a *Trusted Certificates* y pinchar en el icono de Mas (+) para poder seleccionar el pfx o p12 y cargarlo en Safeguard. Si la clave está protegida por una contraseña, esta deberá ser especificada en este proceso.

97. Para más información al respecto, se recomienda consultar el apartado "*Trusted Certificates*", de la Guía de Administración **[REF1]** del producto.

6.6.4 CERTIFICADO DE FIRMA DE ARCHIVOS DE AUDITORÍA

98. Este certificado es empleado para firmar los archivos de auditoría almacenados en un servidor de ficheros externo. Este certificado sirve para asegurar que dichos ficheros de auditoría proceden de un clúster de SPP en particular.

99. La clave pública de este certificado debe estar disponible si se desea validar el fichero de auditoría fichado.

100. Cada archivo de auditoría está firmado empleando el algoritmo SHA256. El hash está firmado con la clave privada del certificado de firma de archivos de auditoría, empleando el algoritmo RSA. Se deben emplear claves RSA con una longitud mínima de 3072 bits.

101. En caso de que se desee sustituir este certificado por uno propio, se han de seguir las siguientes indicaciones:

    Extensión Enhanced Key Usage con Server Authentication (OID 1.3.6.1.5.5.7.3.1).

    Extensión Digital Signature key Usage con Server Authentication (OID 2.5.29.37.3).

102. Solo puede haber un único certificado definido para la firma de ficheros de auditoría.

103. Para más información, se recomienda consultar el apartado "*Audit Log Signing Certificate*", así como sus subapartados, de la Guía de Administración **[REF1]** del producto.

6.6.4.1 INSTALACIÓN DE UN CERTIFICADO DE FIRMA DE ARCHIVOS DE AUDITORÍA

104. Los pasos a seguir para llevar a cabo la instalación de un certificado de firma de archivos de auditoría, se puede encontrar en el apartado "*Installing an audit log signing certificate*", de la Guía de Administración [REF1] del producto.

6.6.4.2 CREACIÓN DE UNA CSR PARA ARCHIVOS DE AUDITORÍA

105. **Los certificados por defecto del *appliance* SPP deben ser actualizados**. Para ello, se da la posibilidad de crear una *Certificate Sign Request* (CSR). Los pasos a seguir para crear un CSR para archivos de auditoría, puede encontrarse en el apartado *"Creating a Certificate Signing Request for audit logs*", de la Guía de Administración **[REF1]** del producto.

106. Las longitudes de clave de 1024 y 2048 bits son consideradas inseguras. **Se debe utilizar longitudes de clave iguales o superiores a 3072 bits.**

6.6.5 CERTIFICADOS SSL

107. SPP permite a un usuario con rol de Administrador de Appliance (*Appliance Administrator*) cargar certificados SSL con clave privada o añadir nuevos certificados SSL a través de *Certificate Sign Requests* (CSRs).

108. **El certificado SSL proporcionado por defecto por SPP, que es empleado para comunicaciones HTTPS, no es considerado como confiable, y debe ser reemplazado.**

109. Para gestionar este tipo de certificados, ir a *Administrative Tools > Settings > Certificates > SSL Certificates.*

110. Para más información sobre la función y los procesos de gestión de certificados SSL, se recomienda consultar el apartado "*SSL Certificates*", así como sus subapartados, de la Guía de Administración **[REF1]** del producto.

6.6.5.1 INSTALACIÓN DE CERTIFICADOS SSL

111. Los pasos a seguir para la instalación de certificados SSL, se pueden encontrar en el apartado "*Installing an SSL certificate*", de la Guía de Administración **[REF1]** del producto.

6.6.5.2 CREACIÓN DE CSR PARA CERTIFICADOS SSL

112. Los pasos a seguir para la creación de CSRs para certificados SSL se puede encontrar en el apartado "*Creating a Certificate Signing Request*", de la Guía de Administración **[REF1]** del producto.

113. La longitud por defecto del par de claves es de 2048 bits. **Se debe elegir siempre una longitud superior o igual a 3072 bits, al ser las otras longitudes disponibles consideradas inseguras.** Se emplea RSA para firmar los certificados. Para más información al respecto, se recomienda consultar el siguiente enlace:

    https://support.oneidentity.com/es-es/technical-documents/one-identity-safeguard-for-privileged-passwords/6.13.1/administration-guide/92

6.6.5.3 ASIGNACIÓN DE CERTIFICADO SSL A APPLIANCES

114. Los pasos a seguir para llevar a cabo la asignación de certificados SSL a *appliances*, se pueden consultar en el apartado "*Assigning a certificate to appliances*" de la Guía de Administración **[REF1]** del producto.

6.7 SERVIDORES DE AUTENTICACIÓN

6.7.1 *ACTIVE DIRECTORY*

115. El método recomendado de autenticación remota es *Active Directory*. La autenticación recae en el propio sistema operativo subyacente. Desde un punto de vista de gestión de usuarios y grupos, Safeguard puede sacar provecho a la seguridad nativa de *Active Directory* para el modelo de acceso a Safeguard, además de poder contar con los protocolos de autenticación seguros de *Active Directory (Kerberos).*

116. Para emplear este tipo de autenticación, primero es necesario añadir un Directorio Activo de Microsoft dentro de la sección *Settings > Identity and Authentication* a

SPP. Para más información, consultar el apartado "*Identity and Authentication*" de la Guía de Administración **[REF1]** del producto.

117. Para poder añadir un *Active Directory* como proveedor de identidad y autenticación, hay que proporcionar los siguientes datos:

   - Nombre del dominio de AD
   - Nombre de la cuenta de AD que servirá para poder conectarse al dominio (Cuenta de servicio). Basta que esta cuenta tenga permisos de lectura sobre el *Active Directory*.
   - Contraseña de la cuenta de servicio.

118. Para más información al respecto, se recomienda consultar el apartado *"Adding identity and authentication providers"*, de la Guía de Administración **[REF1]** del producto.

6.7.2 LDAP

119. Otro posible proveedor de identidad para la autenticación en Safeguard es cualquier otro directorio basado en el estándar LDAP. Este se debe dar de alta desde el menú *Settings > Identity and Authentication*.

120. Para poder añadir un LDAP como proveedor de identidad y autenticación, hay que proporcionar los siguientes datos:

   - Nombre del dominio del LDAP
   - Dirección IP del servidor LDAP
   - Nombre de la cuenta del LDAP que servirá para poder llevar a cabo la conexión al dominio (Cuenta de servicio). Basta que esta cuenta tenga permisos de lectura sobre el LDAP
   - Contraseña de la cuenta de servicio

121. En la configuración del servidor de autenticación basado en LDAP, se pueden configurar los siguientes dos (2) parámetros para realizar una conexión segura:

   - *Use SSL Encryption*: seleccionar esta opción para cifrar las comunicaciones con un directorio LDAP. Safeguard se conecta a través de LDAP en los puertos TCP/389 y TCP/3268. Estas conexiones utilizan Kerberos/GSS-API y SASL para autenticar y cifrar las comunicaciones LDAP. Este es el mismo mecanismo utilizado por los inicios de sesión de AD de escritorio de Windows.
   - *Verify SSL Certificate*: si se selecciona esta opción, se comparará el certificado presentado con el almacenado en el almacén de certificados de confianza de SPP. Esta opción solo está disponible cuando la opción "*Use SSL Encryption*" ha sido seleccionada.

122. Para más información, se recomienda consultar el apartado "*Adding identity and authentication providers*", así como su subapartado *"Active Directory and LDAP settings*" de la Guía de Administración **[REF1]** del producto.

6.7.3 RADIUS

123. A continuación, se enumeran los pasos a seguir para crear y configurar un servidor RADIUS, para su uso como proveedor de autenticación (ya sea primario o secundario). Para esto, será necesario crear dos (2) proveedores de autenticación:

    - En la pantalla de diálogo "*Radius*", proporcionar la siguiente información:
        - Nombre: el nombre que se mostrará para el proveedor de identidad.
        - Tipo: elegir entre designar este servidor como Medio Primario de Autenticación o Medio Secundario de Autenticación.
        - Dirección del servidor: introducir el nombre de DNS o la dirección IP empleada para conectarse al servidor en el entorno de red.
        - Dirección secundaria de servidor (opcional): Nombre de DNS o dirección IP para un servidor adicional o redundante.
        - Secreto Compartido: introducir la clave secreta del servidor.
        - Puerto: introducir el puerto que el servidor RADIUS emplea para recibir las solicitudes de autenticación. Por defecto, el puerto empleado es el 1812.
        - Tiempo de *timeout*: especificar el tiempo de espera antes de que una petición de autenticación Radius expire. Por defecto, este valor es de 20 segundos.
        - Pre-Autenticación para *Challenge/Response*: este parámetro es únicamente aplicable cuando el servidor RADIUS es empleado como un proveedor de autenticación secundario. Esta configuración no tiene efecto sobre proveedores de autenticación primarios.
        - Enmascarar el input del usuario: si esta opción es seleccionada, la contraseña aparecerá en pantalla como un conjunto de puntos, no como texto claro.
        - Descripción.
    - Hacer click en OK.

124. Para más información al respecto, se recomienda consultar el apartado *"Radius settings",* de la Guía de Administración **[REF1]** del producto.

125. El proceso para añadir un servidor RADIUS con un proveedor de identidad y autenticación se puede consultar en el apartado *"Adding identity and authentication providers"*, de la Guía de Administración **[REF1]** del producto.

6.8 SINCRONIZACIÓN HORARIA

126. **Es necesario que SPP utilice la misma referencia horaria que el resto de dispositivos de la red**. Para ello, el producto permite habilitar la sincronización horaria mediante NTP desde el cliente de administración - *Settings* > *Appliance* >

Time pudiendo configurar un servidor primario y otro secundario, con información de la última sincronización.

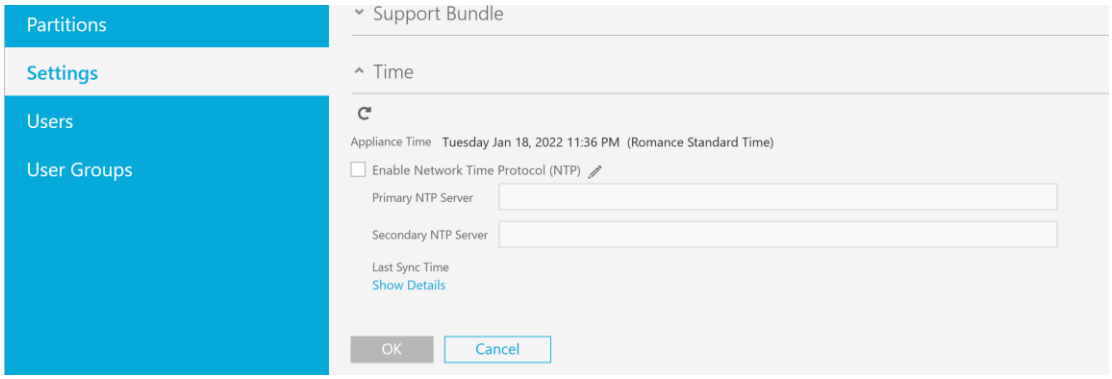

Figura 17 – Configuración NTP

127. A continuación, se enumeran los pasos a seguir para habilitar el protocolo NTP, así como habilitar los servidores NTP primario y secundario:
    - Ir a *Time*.
    - En el cliente web, hacer *click* en Settings. Se desplegará la página *Settings:Appliance*. A continuación, hacer *click* en Time.
    - En el cliente de escritorio, ir a *Administrative Tools > Settings > Appliance > Time.*
    - Seleccionar la opción *Enable Network Time Protocol (NTP)* para habilitar el protocolo NTP.
    - Proporcionar la siguiente información:
        - *Primary NTP Server.* Introducir la dirección IP o nombre de DNS del servidor NTP primario.
        - *Secondary NTP Server* (opcional). Introducir la dirección IP o nombre de DNS del servidor NTP secundario.
    - Hacer click en OK o *Save* para guardar la configuración.
128. El fabricante recomienda el uso de servidores NTP.
129. Para más información, consultar el apartado "*Time*" de la Guía de Administración **[REF1]** del producto.

6.9 ACTUALIZACIONES

130. Las actualizaciones se realizan mediante la subida del fichero correspondiente a una nueva versión del producto a través de: *Cliente de administración – Settings > Appliance > Update > Upload a File.*
131. Cuando el fichero de actualización es seleccionado, SPP sube dicho fichero al servidor, pero no lo instala.

132. Una vez que el fichero ha sido subido con éxito, se debe seleccionar una de las siguientes opciones:

    - *Install now*: seleccionar esta opción para instalar el fichero de actualización. Una vez que el fichero de actualización ha sido instalado, este no puede ser desinstalado.
    - *Remove*: seleccionar esta opción para eliminar el archivo de actualización del servidor sin instalarlo.

133. El panel de actualizaciones mostrará el progreso de la actualización, e indicará en su caso el éxito en el proceso de actualización.

134. El fichero de actualización contiene tanto mejoras de producto y parches como actualizaciones necesarias del sistema operativo de base. El proceso de actualización es realizado de manera automática y controlada por SPP. La descarga de los ficheros de actualización puede llevarse a cabo desde la página web del fabricante.

135. La verificación de la integridad de las actualizaciones es realizada internamente por el SPP, cuando se carga la actualización, de forma transparente al usuario. Para dicha verificación, el producto utiliza el hash SHA-256.

136. Para más información, consultar el apartado "*Updates*", de la Guía de Administración **[REF1]** del producto.

6.10 SNMP

137. *Simple Network Management Protocol* (SNMP) es un protocolo de internet empleado para gestionar dispositivos en redes IP. SPP permite configurar suscripciones SNMP para enviar alertas a la consola SNMP en caso de que se produzcan ciertos eventos.

138. El producto soporta la configuración de SNMP v1 y v2. Estas versiones del protocolo SNMP son consideradas inseguras, por lo que no se recomienda su uso. Actualmente, no es posible emplear SNMPv3. **Por tanto, no se recomienda su uso.**

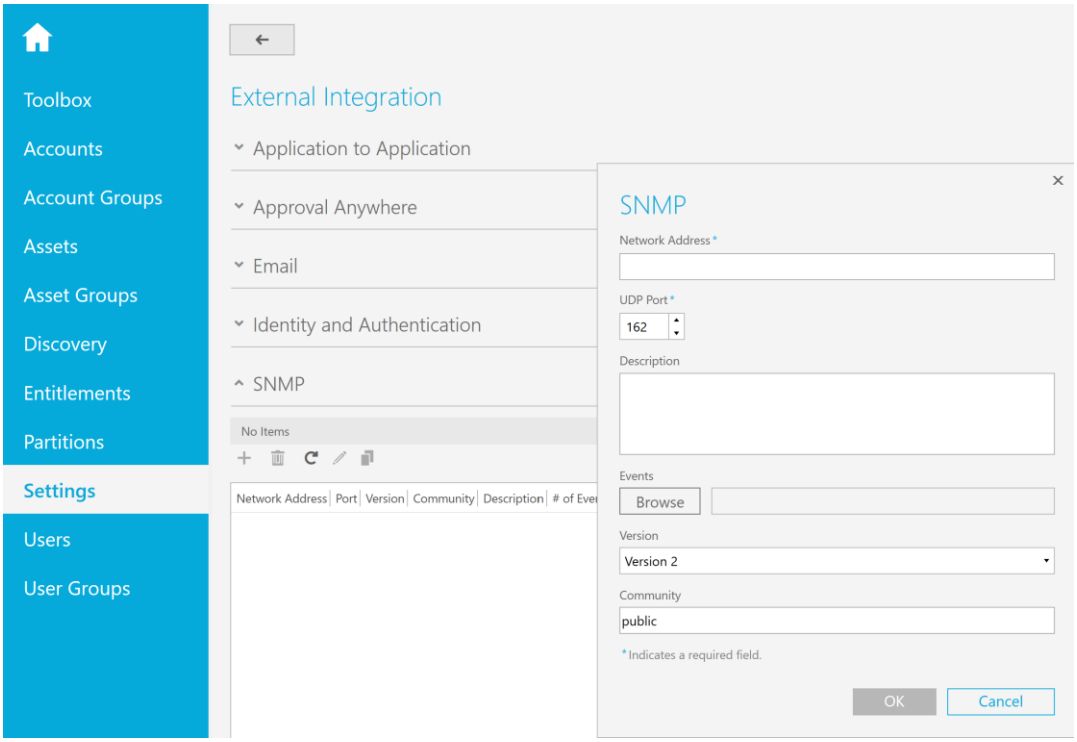

Figura 18 – Configuración SNMP del SPP

139. Para acceder a las propiedades de esta funcionalidad, acceder al menú *Administrative Tools > Settings > External Integration > SNMP.*

140. Para más información, consultar el apartado "*SNMP*", de la Guía de Administración [REF1] del producto.

6.11 ALTA DISPONIBILIDAD

141. Para permitir la recuperación o la continuación de la infraestructura y los sistemas tecnológicos vitales después de un desastre natural o inducido por el hombre, SPP ofrece una solución para escenarios de recuperación de desastres, al permitirle configurar un grupo de dispositivos en clúster para ofrecer una configuración de alta disponibilidad.

142. Un clúster Safeguard consta de tres o más dispositivos Safeguard configurados para comunicarse a través del puerto TCP 655. Un dispositivo en el clúster se designa como "primario". Los dispositivos no primarios se denominan "réplicas".

143. Todos los datos vitales almacenados en el dispositivo primario también se almacenan en las réplicas. En el caso de un desastre, donde el dispositivo primario ya no funciona, se puede promover una réplica para que sea el nuevo dispositivo primario. Esto reduce el tiempo de inactividad y la pérdida de datos. Si bien solo puede tener un dispositivo primario, se puede tener hasta cuatro réplicas. Las réplicas proporcionan una vista de solo lectura de la configuración de la política de seguridad; sin embargo, los usuarios pueden iniciar sesión en réplicas para solicitar acceso, generar informes o auditar los datos.

144. Todos los nodos del clúster son activos. El siguiente sería un escenario normal:

Figura 19 – Clúster de tres nodos de SPP

145. En las siguientes imágenes se ven diferentes fallos, pero aún hay consenso:

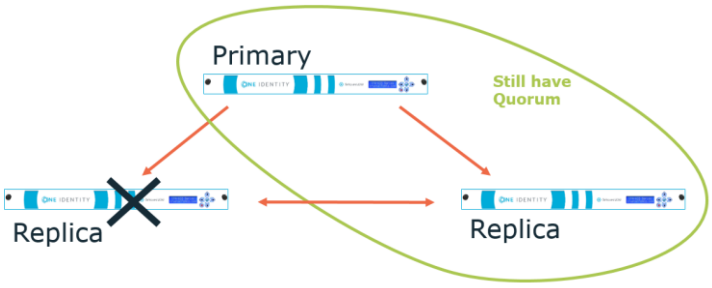

Figura 20 – Clúster de tres nodos de SPP con consenso

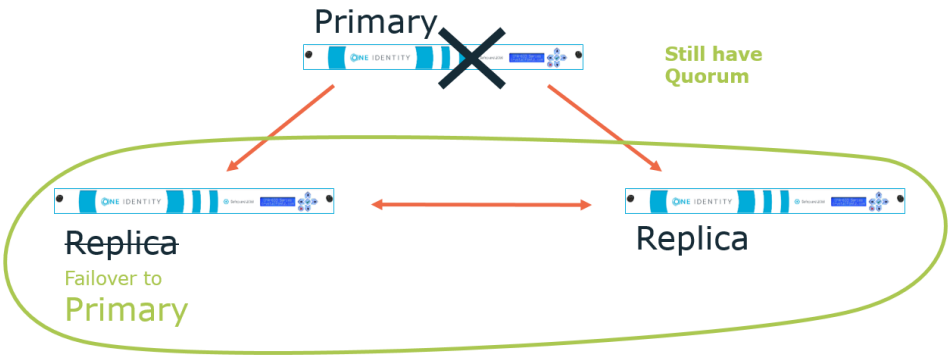

Figura 21 – Clúster de tres nodos de SPP con consenso

146. En caso de que fallen dos nodos, ya no habría consenso y el último nodo activo entraría en modo lectura. El nodo en modo lectura seguiría dando servicio a los usuarios de Safeguard, pero no se podría realizar ningún cambio de configuración ni de gestión de contraseñas en sistemas finales hasta que el clúster se restaurase.

147. Una vez restaurados el resto de nodos, incluido el primario, se podría volver a funcionar con normalidad. El papel de nodo primario nunca se asigna a otro nodo de manera automática. Solo es posible reasignar el nodo primario de manera manual. Esto no afecta al servicio de *clustering* desde un punto de vista de servicio, pues solo afecta a la capacidad de introducir cambios en el sistema.

148. Si el nodo primario no pudiera ser restaurado, se podría desplegar un nuevo nodo, asignarlo al clúster, y manualmente asignarle el rol de nodo primario. Para más información acerca del proceso a seguir para añadir un nodo réplica, se recomienda consultar el apartado "*Enrolling replicas into a cluster*", de la Guía de Administración **[REF1]** del producto.

149. En la siguiente imagen se puede observar la pantalla de gestión del clúster en Safeguard. A dicha pantalla se accede desde el menú *Administrative Tools > Settings > Cluster.*

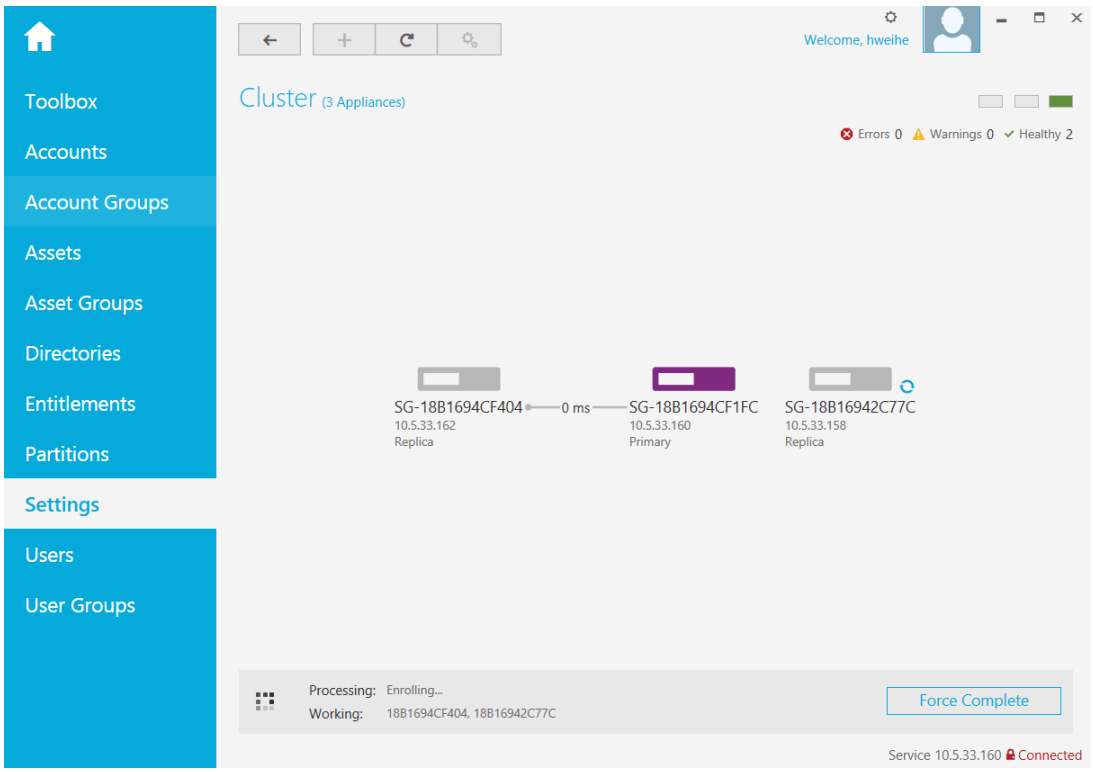

Figura 22 – Gestión del clúster de SPP

150. Para más información, consultar los apartados "*Cluster Settings*", "*Disaster recovery and clusters*" y "*Cluster Management*", de la Guía de Administración **[REF1]** del producto.

6.12 AUDITORÍA

6.12.1 REGISTRO DE EVENTOS

151. SPP registra todos los eventos referentes a acceso, gestión de secretos, uso de secretos, eventos internos y de sistema. Estos eventos se almacenan internamente en registros de logs. Estos logs originales no son accesibles de ninguna manera.

152. Se pueden obtener estos logs mediante la creación de un "*Support bundle*" para la resolución de problemas. Para más información acerca del proceso de creación

de un *Support Bundle*, consultar la sección "*Support Bundle*", de la Guía de Administración **[REF1]** del producto.

153. Estos eventos pueden ser consultados mediante la consola de administración > *Activity Center.*

154. Cualquier administrador tiene acceso a la información de los registros de auditoría, sin embargo, los permisos asignados a cada rol de administración determinan el tipo de información de auditoría a la que se tiene acceso.

155. Además de poder auditar la actividad producida en el sistema, es posible emplear el *Activity Center* para auditar las transacciones ocurridas durante el proceso de solicitud de acceso a credenciales, desde el proceso de solicitud hasta el proceso de revisión y aprobación.

156. Para más información acerca de este proceso, se recomienda consultar el apartado "*Auditing request workflow*", de la Guía de Administración **[REF1]** del producto.

6.12.2 ALMACENAMIENTO LOCAL

157. SPP almacena localmente los logs de la aplicación. Los logs almacenados localmente están protegidos frente a accesos no autorizados.

158. La gestión de los logs puede configurarse desde la sección: *Administrative Tools > Settings > Backup and Retention > Audit Log Management.*

159. Desde esta sección se puede programar una limpieza y archivado de los logs de auditoría en un servidor de archivos, en base a la antigüedad. Los pasos a seguir para programar una tarea de archivado de registros de auditoría se pueden consultar en el apartado "*Audit Log Management*", de la Guía de Administración **[REF1]** del producto.

160. **Se debe asegurar que el producto no deja de operar cuando el espacio destinado a almacenamiento local de archivos de auditoría se llene** (comportamiento por defecto). Para prevenir que se ocupe todo el espacio de almacenamiento en el disco duro, un usuario con rol de Administrador puede ejecutar de forma manual una tarea de mantenimiento de archivos de auditoría (*Audit Log Maintenance*).

161. Asimismo, también es posible programar tareas automatizadas de mantenimiento de archivos de auditoría (por ejemplo, enviar archivos de auditoría con cierto período de antigüedad a un servidor de archivos externo, tras lo que dichos archivos serían eliminados del *appliance*). Para más información al respecto, consultar la sección *Settings > Backup and retention settings > Audit Log Maintenance > Manually run Audit Log Maintenance* de la Guía de Administración **[REF1]** del producto.

6.12.3 ALMACENAMIENTO REMOTO

162. SPP permite el reenvío de logs a servidores remotos mediante Syslog. Para la configuración de la conexión contra el servidor de destino **se debe hacer uso de los protocolos TCP y TLS v1.2.**

163. Esto se configura en la sección *de Administrative Tools > Settings > External Integration > Syslog* al dar de alta el servidor de Syslog. En la sección *Settings > External Integration settings > Syslog > Configuring and verifying a Syslog server* de la Guía de Administración [REF1] del producto se proporciona una guía para definir uno o más servidores destinados al almacenamiento remoto de mensajes relacionados con eventos del producto.

164. A continuación, se enumeran los pasos necesarios para configurar un servidor Syslog:

    - Ir a *Administrative Tools > Settings > External Integration > Syslog.*
    - Hacer click en *New* para desplegar la caja de diálogo *Syslog*.
    - En dicha caja de diálogo, introducir la siguiente información:
        - *Network Address*: introducir la dirección IP o FQDN del servidor Syslog. Tiene un límite de longitud de 255 caracteres.
        - *UDP Port*: introducir el puerto UDP del servidor Syslog. Por defecto, es el puerto 514, aunque puede cambiarse el puerto por uno entre el 1 y el 32767.
        - *Description*: introducir una descripción para la configuración del servidor Syslog. Dicha descripción tiene un límite de 255 caracteres.
        - *Events*: hacer click en Browse para seleccionar los eventos que serán incluidos en el servidor Syslog. Una vez seleccionados los eventos deseados, hacer click en OK.
        - *Facility*: elegir el tipo de programa empleado para registrar mensajes de log. Por defecto: mensajes de nivel de usuario (*user-level messages*).
    - Hacer click en OK para guardar y añadir la configuración del servidor Syslog.

165. Para enviar eventos a un servidor Syslog, es necesario configurar SPP para que envíe alertas. Para más información al respecto, consultar el apartado "*Configuring alerts*", de la Guía de Administración **[REF1]** del producto.

166. Para más información, consultar el apartado "*Syslog*", de la Guía de Administración **[REF1]** del producto.

6.13 BACKUP

167. SPP permite la realización programada de backups para la recuperación ante desastres, con los siguientes datos:

- Todos los ajustes y configuraciones, excepto:
  - Dirección IP del dispositivo
  - Configuraciones del protocolo de tiempo de red (NTP)
  - Configuración del sistema de nombres de dominio (DNS)
- Historial de transacciones
- Toda la información sobre los objetos SPP:
  - Cuentas
  - Grupos de cuentas
  - Activos
  - Grupos de activos
  - Derechos
  - Particiones
  - Usuarios
  - Grupos de usuarios

168. **Los backups debe ser protegidos para evitar accesos no autorizados**. SPP puede proteger los *backups* antes de que estén disponibles para descargar a un servidor de archivos externo. Existen tres (3) maneras de proteger los archivos de copia de seguridad:
    - Solo protección de dispositivo: esta es la opción predeterminada, y no incluye contraseña ni protección de clave GPG de la copia de seguridad.
    - Agregar protección con contraseña: una vez seleccionada esta opción, ingrese la contraseña en el cuadro de texto *"Contraseña de respaldo"*.
    - Agregar protección de clave GPG.
169. Para más información, consultar el apartado "*Backup and Retention settings*", de la Guía de Administración **[REF1]**.
170. Como paso previo a la restauración de una copia de seguridad de un dispositivo SPP en otro, se llevará a cabo la verificación de la firma en dicho dispositivo de destino, asegurando que es una copia de seguridad auténtica de SPP.
171. La configuración de los *backups* se realiza desde *Administrative Tools > Settings > Backup and Retention.*
172. **Se recomienda el almacenamiento de *backups* locales en dispositivo durante un período de al menos 7 días**. El tiempo de retención de archivos de auditoría es configurable.
173. Para más información sobre cómo configurar el tiempo de retención de registros de auditoría, revisar el apartado "*Audit Log Management*", de la Guía de Administración **[REF1]** del producto**.**

174. Es necesario indicar que los logs de auditoría almacenados en el *appliance* durante un período de tiempo superior al valor determinado serán almacenados en un servidor de archivos externo, y eliminados del *appliance*.

175. A continuación, se introducen los pasos a seguir para crear una nueva copia de seguridad:

    - Ir a *Administrative Tools > Settings > Backup and Retention > Safeguard Backup and Restore.*
    - Hacer click en "***Run Now***". SPP creará una copia de la base de datos actual.

      Nota: Si se restaura una copia de seguridad más antigua que el período de validez establecido para las contraseñas en los parámetros de Control de Login, todas las cuentas de usuario (incluyendo al *Bootstrap Administrator*) serán bloqueadas, y las contraseñas correspondientes deberán ser reseteadas. Para evitar esta situación, se recomienda establecer el período máximo de validez de contraseñas al valor 0, antes de llevar a cabo la copia de seguridad, y posteriormente restaurar el valor deseado.

176. Asimismo, es posible programar la generación de copias de seguridad. Esta opción solo está disponible si se ha configurado previamente un servidor de archivos. Para más información al respecto, se recomienda consultar el apartado "*Adding an archive server*", de la Guía de Administración **[REF1]** del producto.

177. Es necesario indicar que copias de seguridad de un *appliance hardware* no pueden ser restaurados en un *appliance* virtual, y viceversa.

178. Para más información sobre cómo llevar a cabo la descarga de copias de seguridad, subir una copia de seguridad a un *appliance*, restaurar una copia de seguridad en un *appliance* y archivar una copia de seguridad en un servidor de archivos externo, se recomienda consultar el apartado "*Backup and Restore*", de la Guía de Administración **[REF1]** del producto.

6.14 SEGURIDAD EN SPP

179. En este apartado se mencionan los mecanismos de seguridad presentes en todos los SPP.

180. Cada dispositivo tiene un **cortafuegos integrado** para proteger las conexiones de red, que está configurado para permitir el acceso sólo a los servicios más necesarios. Además, el dispositivo puede activar alertas y notificaciones a través de SMTP y SNMP.

181. El cifrado de las conexiones HTTP/S utiliza por defecto el algoritmo de cifrado AES256. A continuación, se enumeran las diferentes suites de cifrado (*ciphersuites*) que emplea el producto, cuando emplea TLSv1.2 para las comunicaciones:

    - Si está habilitada la opción "solo TLSv1.2":
        - *ECDHE_RSA_WITH_AES_256_GCM_SHA384*

- *ECDHE_RSA_WITH_AES_256_CBC_SHA384*
- *ECDHE_RSA_WITH_AES_128_GCM_SHA256*
- *ECDHE_RSA_WITH_AES_128_CBC_SHA256*
- *RSA_WITH_AES_128_CBC_SHA256*

Se debe consultar la guía *CCN-STIC-807 Criptología de empleo en el Esquema Nacional de Seguridad* para conocer cuáles de las anteriores ciphersuites están recomendadas por el Centro Criptológico Nacional.

182. Todo el dispositivo cifra los soportes de datos con Bitlocker, utilizando también AES256. Estas medidas garantizan que, incluso si el aparato es robado, el acceso a los datos no puede ser obtenido por personas no autorizadas. A continuación, se incluyen las suites de cifrado (*ciphersuites*) empleadas:

    - AES-CBC 128-bit
    - AES-CBC 256-bit
    - XTS-AES 128-bit
    - XTS-AES 256-bit

Se debe consultar la guía *CCN-STIC-807 Criptología de empleo en el Esquema Nacional de Seguridad* para conocer cuáles de las anteriores *ciphersuites* están recomendadas por el Centro Criptológico Nacional.

183. Seguridad de la base de datos. La comunicación entre la interfaz de usuario de *Safeguard Management* y las bases de datos internas está protegida y no es posible el acceso directo a la base de datos. Solo se puede llamar a la API, que establece la conexión final con la base de datos. Esto significa que tampoco es posible ejecutar consultas, *scripts* o procedimientos SQL de libre configuración. Además, el acceso a través de la API requiere la autenticación obligatoria del usuario según las especificaciones definidas, por ejemplo, mediante un certificado o una contraseña válida.

184. Seguridad interna: SPP utiliza un modelo interno de derechos basado en funciones que puede utilizarse para asignar diferentes capacidades a los usuarios con privilegios administrativos en el producto. Esto permite limitar el nivel de actividad al mínimo necesario y minimizar los errores y fallos de funcionamiento.

185. Acceso al dispositivo SPP**:** Todo el acceso al sistema operativo o servicios de está desactivado por defecto. Sólo hay un "quiosco de emergencia (*quiosco de recuperación*)", que se utiliza principalmente con fines de diagnóstico y, en caso necesario, permite reiniciar el sistema o restablecer el estado de entrega (*estado de fábrica*). El acceso a estas funciones, sin embargo, requiere un apoyo adicional (por parte del departamento de soporte de One Identity) y más información por parte de One Identity (seguridad a través del procedimiento de contraseña de respuesta al desafío). Las operaciones de mantenimiento y configuración se realizan únicamente a través de la interfaz de administración o a través de la API. La supervisión o monitorización del *hardware* (en el supuesto del modelo de

Safeguard físico) y el acceso remoto a las funciones de monitorización del *hardware* están disponibles a través de *Lights-Out-Management* (LOM) **[REF8]**, por lo que la comunicación está cifrada mediante el uso de certificados SSL (RSA) con longitudes soportadas de 1024, 2048 (por defecto) o 4096 bits. **Se recuerda que se deben emplear longitudes de clave superior o igual a 3072 bits.**

186. Acceso de emergencia al aparato: En caso de fallo total del sistema, también es posible acceder al "Kiosco de Recuperación" a través del puerto serie. Esto permite acceder a los datos de diagnóstico para que el servicio de asistencia de One Identity los investigue más a fondo para identificar la causa del fallo.

187. Alta disponibilidad: Todos los dispositivos pueden funcionar en una configuración de alta disponibilidad.

188. Almacenamiento de contraseñas: Un uso clave de SPP es como almacén de contraseñas, mediante el cual Safeguard almacena las contraseñas de las cuentas gestionadas, eliminando la necesidad de compartir contraseñas entre un gran número de usuarios. Safeguard también permite transferir al almacén de contraseñas la información crítica almacenada en aplicaciones o archivos de configuración, eliminando el riesgo de un incidente de seguridad al acceder a esta información.

189. Proceso de acceso configurable (flujo de trabajo): El acceso a las contraseñas almacenadas sólo puede tener lugar mediante un proceso configurable (flujo de trabajo).

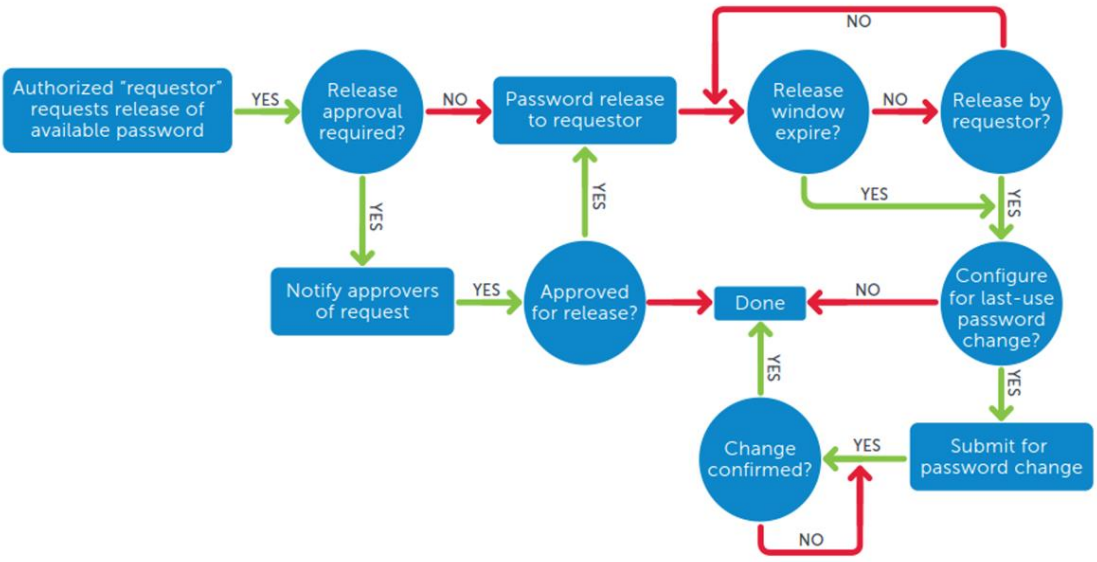

Figura 23 – Proceso de solicitud de información del SPP

190. Almacenamiento seguro de contraseñas: SPP almacena las contraseñas cifradas con AES256. Admite AES CBC y AES GCM (128 y 256 bits) para el cifrado/descifrado de datos. Además, Safeguard puede comprobar automáticamente las contraseñas, sincronizarlas y, si es necesario, también regenerarlas o bloquearlas en función de los requisitos de seguridad. En particular, Safeguard asegura que

todas las contraseñas generadas por Safeguard cumplan siempre con los requisitos de seguridad vigentes, por ejemplo, en términos de complejidad y longitud, definidas en las políticas de complejidad de contraseñas dentro de las particiones de Safeguard. Además de almacenar de forma segura contraseñas, Safeguard es capaz de almacenar y gestionar claves SSH para el acceso a servidores y sistemas Unix & Linux. Para más información sobre el establecimiento de políticas de complejidad de contraseñas, se recomienda consultar el apartado "*Adding an account password rule*", de la Guía de Administración **[REF1]** del producto.

191. Aprobaciones de uno o varios niveles: Safeguard admite la aprobación de uno o varios niveles cuando se solicitan las contraseñas gestionadas de cuentas y activos (sistemas finales gestionados). Es decir, cuando un usuario solicita una contraseña o clave SSH almacenada en Safeguard, existe la posibilidad de añadir flujos de aprobación para que estas solicitudes tengan que ser aceptadas por un responsable antes de entregar la contraseña o clave SSH. Estos flujos de aprobación se definen en la política de petición de acceso (*Access request policy*), dentro de la pestaña del rol de usuario *Approver (Administrative Tools | Entitlements | Access Request Policies | <nombre de política>),* desde la que se puede especificar las opciones de configuración de este rol para una política de control de acceso. Esto significa que se pueden definir diferentes niveles en los flujos de aprobación de acceso a contraseñas, como se puede observar en la siguiente imagen. En este ejemplo, para que un usuario de Safeguard que haya solicitado una contraseña la obtenga, la solicitud debe haber sido aprobada previamente por tres usuarios.

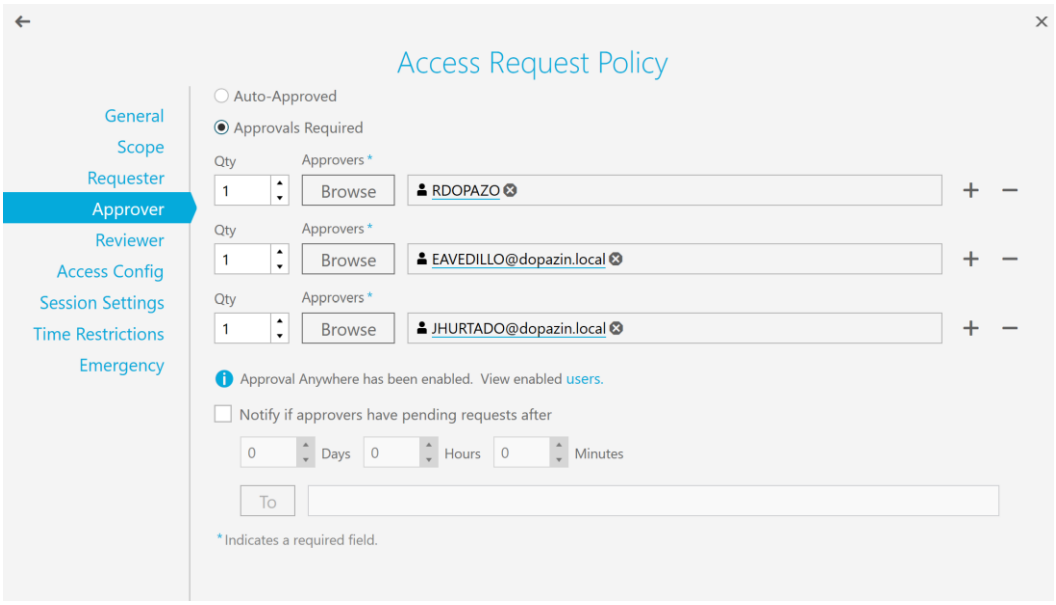

Figura 24 – Configuración de la política de aprobación de accesos

192. Cambio automático de contraseñas: Safeguard proporciona un mecanismo configurable que permite cambiar automáticamente las contraseñas gestionadas según diferentes criterios. De este modo, Safeguard puede adaptarse con flexibilidad a la política de seguridad correspondiente. Estas políticas de

conmutación también pueden establecerse para diferentes subconjuntos de activos y cuentas, en función de las especificaciones internas. En cualquier caso, por motivos de seguridad, **se recomienda llevar a cabo cambios de contraseñas cada 60 días.**

193. Gestión de contraseñas configuradas o incrustadas: La gestión de las contraseñas almacenadas o incrustadas en las aplicaciones o sistemas puede lograrse en Safeguard mediante la integración de aplicación a aplicación (A2A, *Application to Application*). El objetivo es que sea la propia aplicación que lanza un proceso la que acceda en tiempo real a Safeguard a través de la REST API, y obtenga la contraseña que requiera, para su procesado de manera segura. Para más información, se puede consultar el apartado "*Application to Application*" de la Guía de Administración **[REF1]** del producto.

7. FASE DE OPERACIÓN

194. *Safeguard for Privileged Passwords* proporciona control seguro de cuentas, almacenando las contraseñas hasta que son solicitadas y únicamente son accesibles para individuos autorizados. Asimismo, el producto actualizará las contraseñas de las cuentas gestionadas, en base a una serie de parámetros configurables.

195. El flujo de trabajo que sigue una petición de acceso a credenciales puede ser consultado en el apartado "*Password release request workflow*", de la Guía de Usuario **[REF3]** del producto.

196. A continuación, se enumera una serie de procedimientos operativos que deberán llevarse a cabo durante la fase de operación y mantenimiento del producto:

- **Comprobaciones periódicas del *hardware* y *software*** para asegurar que no se ha introducido *hardware* o *software* no autorizado.
- **Verificación periódica del *firmware* del producto y su integridad**, para comprobar que está libre de software malicioso.
- **Aplicación regular de parches de seguridad**, con objeto de mantener una configuración segura.
- **Gestión y archivado de los backups** con una periodicidad diaria.
- **Gestión y archivado de los registros de auditoría** con una periodicidad diaria. Estos registros estarán protegidos de borrados y modificaciones no autorizadas, y solamente el personal de seguridad autorizado podrá acceder a ellos.
- **Revisión de las nuevas versiones o *fixes* del producto** para realizar al menos, una actualización al año.

8. CHECKLIST

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto	☐	☐	
Instalación en un entorno seguro	☐	☐	
Registro de las licencias	☐	☐	
Configuración de comunicaciones seguras (uso de TLS v1.2 con *ciphersuites* recomendadas, según CCN-STIC-807)	☐	☐	
CONFIGURACIÓN			
Aplicación de la política de robustez de contraseñas	☐	☐	
Actualización de los certificados por defecto	☐	☐	
Sincronización del dispositivo	☐	☐	
Gestión segura de los registros de auditoría	☐	☐	
Configuración el almacenamiento remoto de logs	☐	☐	
Realización de backups	☐	☐	
CONFIGURACIÓN			
Comprobaciones periódicas del *hardware* y *software*	☐	☐	
Verificación periódica del *firmware* del producto y su integridad	☐	☐	
Aplicación regular de parches de seguridad	☐	☐	
Gestión y archivado de los *backups*	☐	☐	
Gestión y archivado de los registros de auditoría	☐	☐	
Revisión de las nuevas versiones o *fixes* del producto	☐	☐	

9. REFERENCIAS

REF1 *One Identity safeguard for Privileged Passwords 6.0LTS - Administration Guide*
https://support.oneidentity.com/technical-documents/one-identity-safeguard-for-privileged-passwords/6.0%20lts/administration-guide

REF2 *Understanding the security architecture of the one identity safeguard appliance technical brief 25629*
https://www.oneidentity.com/docs/understanding-the-security-architecture-of-the-one-identity-safeguard-appliance-technical-brief-25629.pdf

REF3 *One Identity Safeguard for Privileged Passwords 6.0.7 LTS* – Guía de Usuario
https://support.oneidentity.com/technical-documents/one-identity-safeguard-for-privileged-passwords/6.0.7%20lts/user-guide

REF4 *Página de soporte de OneIdentity*
https://support.oneidentity.com

REF5 Comunicación con el equipo de soporte de OneIdentity
https://support.oneidentity.com/es-es/contact-us/licensing

REF6 *One Identity Safeguard for Privileged Passwords 6.0 LTS Appliance Setup Guide*
https://support.oneidentity.com/technical-documents/one-identity-safeguard-for-privileged-passwords/6.0%20lts/appliance-setup-guide

REF7 *Safeguard API Tutorial*
https://github.com/oneidentity/safeguard-api-tutorial

REF8 *Lights-Out Management (LOM)*
https://searchdatacenter.techtarget.com/definition/lights-out-management

REF9 *One Identity Safeguard for Privileged Passwords* – Descargar software
https://support.oneidentity.com/es-es/one-identity-safeguard-for-privileged-passwords/6.0%20lts/download-new-releases

REF10 *Download One Identity Safeguard 6.0 LTS Hyper-V Virtual Appliance*
https://support.oneidentity.com/es-es/download-install-detail/6103860

REF11 *Download One Identity Safeguard 6.0 LTS VMware Virtual Appliance*
https://support.oneidentity.com/es-es/download-install-detail/6103861

REF12 ¿Qué es una clave de activación múltiple (MAK)?
https://docs.microsoft.com/es-es/licensing/products-keys-faq#qu--es-una-clave-de-activaci-n-m-ltiple--mak

REF13 ¿Qué es una clave KMS host?
https://docs.microsoft.com/es-es/licensing/products-keys-faq#-qu--es-una-clave-kms-host

REF14 Windows 10 LTSC
https://docs.microsoft.com/es-es/windows/whats-new/ltsc/

REF15 *Standardized warning statements for AC systems*
https://support.oneidentity.com/es-es/technical-documents/one-identity-safeguard-for-privileged-passwords/6.0%20lts/appliance-setup-guide/2#TOPIC-1430829

REF16 *What is CORS (Cross-Origin resource sharing)*
https://portswigger.net/web-security/cors

REF17 SAML 2.0 Web Browser SSO
https://en.wikipedia.org/wiki/SAML_2.0

REF18 *Enabling "TLS 1.2 Only" option on appliances (316464)*
https://support.oneidentity.com/es-es/one-identity-safeguard-for-privileged-passwords/kb/316464/enabling-tls-1-2-only-option-on-appliances

REF19 *One Identity Safeguard for Privileged Passwords 6.7.3 – Release Notes*
https://support.oneidentity.com/technical-documents/one-identity-safeguard-for-privileged-passwords/6.7.3/release-notes/2#TOPIC-1788353

REF20 *One Identity Safeguard for Privileged Passwords 6.13.1 – Administration Guides*
https://support.oneidentity.com/es-es/technical-documents/one-identity-safeguard-for-privileged-passwords/6.13.1/administration-guide/92

10.ABREVIATURAS

AD	*AD Active Directory*
AC	*Alternating Current*
AD FS	*Active Directory Federation Services*
AES	*Advanced Encryption Standard*
API	*Application Programming Interface*
A2A	*Application to Application*
CCN	Centro Criptológico Nacional
CORS	*Cross-Origin Resource Sharing*
CPU	*Central processing unit*
CPD	Centro de Proceso de Datos
CSR	*Certificate Signing Request*
DNS	*Domain Name System*
ENS	Esquema Nacional de Seguridad.
HTTP	*Hypertext Transfer Protocol*
HTTPS	*Secure Hypertext Transfer Protocol*
KMS	*Key Management Service*
LDAP	*Lightweight Directory Access Protocol*
LOM	*lights out management*
LTSC	*Long-Term Servicing Channel*
MAK	*Multiple Activation Key*
MSI	*Microsoft System Installer*
NTP	*Network Time Protocol*
OVA	*Open virtualization Appliance*
PKCS	*Public Key Cryptography Standards*
RBAC	*Role Base Access Control*
REST	*Representational State Transfer*
RSA	*Rivest–Shamir–Adleman*
SAML	*Security Assertion Markup Language*
SATA	*Serial AT Attachment*
SDK	*Software Delevopment Kit*
SMTP	*Simple Mail Transfer Protocol*

SNMP	*Simple Network Management Protocol*
STS	*Security Token System*
SSH	*Secure Shell*
SSO	*Single Sign On*
SSL	*Secure Socket Layer*
TLS	*Transport Layer Security*
XML	*Extensible Markup Language*

PUBLICACIONES DE DEFENSA

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