Guía de Seguridad de las TIC
CCN-STIC 1303

Procedimiento de Empleo Seguro
Mcafee ATD

Agosto de 2021

MINISTERIO DE DEFENSA

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

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

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
2021.09.15 14:04:31 +02'00'

P.º de la Castellana 109, 28046 Madrid

NIPO: 083-21-173-5

Fecha de Edición: agosto de 2021

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

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Agosto de 2021

Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN 4
2. OBJETO Y ALCANCE 6
3. ORGANIZACIÓN DEL DOCUMENTO 7
4. FASE DE DESPLIEGUE E INSTALACIÓN 8
4.1 ENTREGA SEGURA DEL PRODUCTO 8
4.2 ENTORNO DE INSTALACIÓN SEGURO 9
4.3 REGISTRO Y LICENCIAS 9
4.4 CONSIDERACIONES PREVIAS 10
4.5 INSTALACIÓN 11
5. FASE DE CONFIGURACIÓN 14
5.1 MODO DE OPERACIÓN SEGURO 14
5.2 AUTENTICACIÓN 15
5.3 ADMINISTRACIÓN DEL PRODUCTO 17
5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA 17
5.3.2 CONFIGURACIÓN DE ADMINISTRADORES 18
5.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 20
5.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS 21
5.6 GESTIÓN DE CERTIFICADOS 22
5.7 SERVIDORES DE AUTENTICACIÓN 24
5.8 SINCRONIZACIÓN HORARIA 25
5.9 ACTUALIZACIONES 26
5.10 AUTO-CHEQUEOS 27
5.11 SNMP 27
5.12 ALTA DISPONIBILIDAD 28
5.13 AUDITORÍA 30
5.13.1 REGISTRO DE EVENTOS 30
5.13.2 ALMACENAMIENTO LOCAL 31
5.13.3 ALMACENAMIENTO REMOTO 31
5.14 BACKUP 31
5.15 SERVICIOS DE SEGURIDAD 32
6. FASE DE OPERACIÓN 33
7. CHECKLIST 34
8. REFERENCIAS 35
9. ABREVIATURAS 36

1. INTRODUCCIÓN

1. **McAfee Advanced Threat Defense (ATD)** es una herramienta cualificada e incluida en el CPSTIC en la familia de Sandbox.
2. Está diseñada para utilizar un enfoque por capas para detectar malware avanzado de tipo Zero-Day. Utiliza múltiples motores de detección tales como firmas conocidas, ofreciendo una solución efectiva y de coste sobre los recursos reducida, servicios de reputación en la nube y la emulación en tiempo real. De este modo puede detectar y bloquear *malware* conocido, por lo que sólo el *malware* avanzado se analiza en profundidad usando técnicas dinámicas como el Sandboxing. El objetivo es equilibrar la balanza entre la seguridad y el rendimiento mediante el filtrado de la avalancha de *malware* conocido con rapidez y eficiencia, lo que le permite al sistema asignar más recursos a las amenazas avanzadas.
3. Aunque encontrar *malware* avanzado es importante, sólo es parte de una solución integral y efectiva. Una solución integrada "*end-to-end*" que expanda la seguridad de la organización desde el perímetro, a través de la red a los puestos de trabajo es requerida no solo para identificar *malware* avanzado sino para protegerse contra él, determinar el ámbito de la filtración y desarrollo de las actividades de remediación cuando ocurra. Un ecosistema de seguridad integrado – uno que comparta información entre las contramedidas de la organización – ofrece una postura de seguridad mayor que la que componentes individuales son capaces de alcanzar.
4. *Advanced Threat Defense* ofrece tres (3) características clave: "*find*" encontrar la amenaza, "*freeze*" congelar la amenaza en el conjunto de elementos de seguridad y "*fix*" solucionar el problema sobre aquellos activos que se hayan podido ver afectados.
5. Se trata de un *appliance* que se integra fácilmente con los componentes de seguridad como *McAfee Network Security Platform, McAfee Web Gateway* y *McAfee Endpoint Protection* a través de *McAfee Threat Intelligence Exchange*.
6. ATD combina múltiples motores para la detección de *malware*:
    a) **Firmas antivirus**. Ofrece una detección rápida sobre *malware* conocido utilizando firmas antivirus para desarrollar una identificación positiva de malware conocido.
    b) ***McAfee Global Threat Intelligence (GTI).*** Analiza el comportamiento anómalo y predictivo ajustando la reputación de *Websites,* llegando a bloquear su acceso. McAfee GTI utiliza su capacidad analítica para la identificación de *malware*, mensajes de correo, direccionamiento IP, reputación sobre objetos, etc,. Esto permite a las soluciones de seguridad de McAfee, desde el puesto de trabajo al perímetro, proteger a los usuarios de las cyber amenazas.
    c) **Motor de emulación en tiempo real**. Simula la ejecución de archivos analizando los logs generados y el comportamiento asociado. La emulación

es normalmente conocida como un *Sandboxing "light"*, ya que es significativamente menos intensa en términos de recursos que el análisis dinámico pero permite la detección de malware desconocido ofreciendo resultados en tiempo real.

d) **Análisis dinámico**, implica la ejecución del código malicioso en un entorno seguro (normalmente conocido como *sandbox*) para observar su comportamiento. La solución permite a los administradores subir imágenes tipo "*gold*" que simulen las condiciones del equipo para conseguir un "*assesment*" más exacto. Sin embargo, el *malware* avanzado puede utilizar técnicas de ofuscación, de modo que el *malware* puede darse cuenta de que se ejecuta en un entorno de análisis y variar su comportamiento. Otros objetos maliciosos pueden retrasar su ejecución y permanecer indetectables durante el análisis en *sandbox*.

e) **Full Static Analysis**, implica el "*unpacking*" del código actual y su análisis para determinar cómo se ejecutará. Esto permite a los departamentos de seguridad entender para qué fue diseñada la pieza concreta de *malware* y cuándo. Este tipo de análisis ayuda a buscar *malware* evasivo y con altas capacidades de camuflaje.

7. Esta **aproximación multicapa** está diseñada para garantizar que, siempre que sea posible, el *malware* se filtre por niveles superiores y no requieran del tiempo y recursos adicionales requeridos por el análisis dinámico y las capacidades *"Full Static Analysis"*. Este acercamiento está diseñado para ofrecer ambas cosas, resultados más rápidos y mejor protección.

2. OBJETO Y ALCANCE

8. El propósito del presente documento es detallar las configuraciones de seguridad del producto **McAfee Advanced Threat Defense, versión 4.0.2**, para que su protección y funcionamiento se realice de acuerdo con unas garantías mínimas de seguridad.

3. ORGANIZACIÓN DEL DOCUMENTO

9. El documento está estructurado en los siguientes apartados:

   a) **Apartado 4.** En este apartado se recogen recomendaciones para tener en cuenta durante la fase de despliegue e instalación del producto.

   b) **Apartado 5.** En este apartado se recogen las recomendaciones para tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

   c) **Apartado 6.** En este apartado se recogen las tareas recomendadas para la fase de operación y mantenimiento del producto.

   d) **Apartado 7.** En este apartado se incluye un *checklist* para verificar las tareas de configuración segura mencionadas a lo largo del documento.

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

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

4. FASE DE DESPLIEGUE E INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

10. El procedimiento de recepción segura del producto, al tratarse de una combinación *hardware/software* está formada por dos (2) procesos:

    a) Entrega del componente *hardware* (*appliance*). Hay que tener en consideración los siguientes pasos:

        i. Cuando se recibe el dispositivo, se recomienda inspeccionar el paquete y el dispositivo en buscar de signos de daños o manipulación, incluida la cinta de embalar que protege el contenedor de envío, donde los signos de manipulación serían evidentes. Si existe algún signo de daños, manipulación incorrecta o alteración, es necesario ponerse en contacto con el Soporte de McAfee con carácter inmediato a fin de recibir instrucciones. Se recomienda dada esta situación, que no se realice la instalación del producto.

        ii. Verificar que el paquete contenga todos los elementos indicados en el albarán.

    b) Entrega del componente *software*. Al igual que sucede con todos los productos de McAfee, es necesario llevar a cabo los siguientes pasos:

        i. Una vez adquirido el producto, su recepción consiste en un correo electrónico que incluye los siguientes datos:

            1. Account Number
            2. Grant Number
            3. Purchase order Number

        ii. Estos datos proporcionan un inicio de sesión al portal de descargas oficial (cuya URL será proporcionada en el mismo correo electrónico) donde será necesario introducir el correo electrónico utilizado para la adquisición del producto, así como el *Grant Number* del mismo. Una vez se consigue el acceso al servidor de descargas, se podrán ver los productos disponibles para descargar en la sección *Products* de la página *My Products*. De este modo, se puede proceder a la descarga del producto y de sus distintos componentes.

        iii. El producto se encuentra firmado digitalmente mediante un certificado de McAfee. Para verificar que los distintos ficheros descargados han sido firmados correctamente, el usuario debe extraer los ficheros incluidos dentro de los ficheros comprimidos y comprobar, haciendo clic derecho en el fichero y, haciendo clic en la opción Propiedades, seleccionar la sección *Digital Signature*. En

el campo de *Signer Information* se podrá verificar la procedencia de dicho certificado. Además, en cada descarga, se incluye un valor *hash* haciendo uso de *SHA-256*, lo cual permite llevar a cabo una descarga segura, manteniendo la integridad de esta. De este modo, se puede dar por concluido el proceso de obtención del producto y de sus componentes.

4.2 ENTORNO DE INSTALACIÓN SEGURO

11. Los componentes del producto deben instalarse en un entorno en el que el personal técnico encargado dispone de autorización para la configuración, despliegue y mantenimiento del producto.

4.3 REGISTRO Y LICENCIAS

12. En el caso de *appliance* físico, si el equipo está instalado de fábrica y no ha sido reinstalado, tiene activa una licencia permanente. En caso contrario, será necesario licenciarlo. En la configuración de *appliance* virtual, siempre será necesario licenciarlo.
13. El procedimiento se inicia escribiendo un correo a licensing@mcafee.com con la siguiente información.
    a) *System ID*. Se obtiene vía GUI en Manage | ATD Configuration | Licensing o vía CLI ejecutando el comando *show system id*
    b) Customer Name
    c) Versión ATD
14. McAfee responderá a ese correo con el fichero de la licencia y un *Grant ID.*
15. Para activar dicha licencia, se accede a *Manage | ATD Configuration | Licensing* y se siguen los siguientes pasos:
    a) Hacer clic en *Browse* y seleccionar el fichero con la licencia.
    b) Completar el *Grant ID*.
    c) Hacer clic en *Activate*.
16. Comprobar que los siguientes datos son correctos:
    a) El estado de la licencia es *Activated*.
    b) La fecha de validez es correcta.
    c) El *System ID* es correcto.

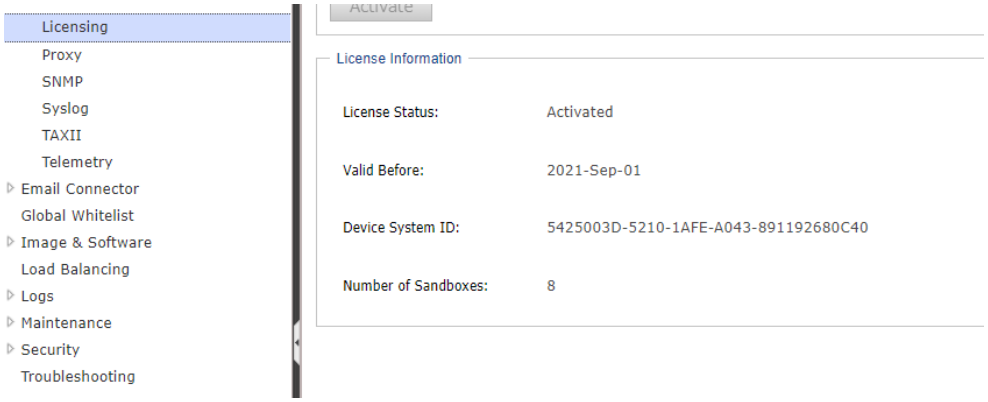

Ilustración 1. Licenciamiento

4.4 CONSIDERACIONES PREVIAS

17. En primer lugar se ha de considerar qué tipo de instalación es necesaria, física o virtual. *McAfee Advanced Threat Defense* está disponible tanto en *appliance* físico como *appliance* virtual.

18. En ambas opciones, tanto el sistema operativo como el *software* vienen preinstalados. En la configuración de *appliance* virtual, está disponible un archivo OVA en la página de descargas (https://secure.mcafee.com/apps/downloads/my-products/login.aspx?region=us) para su despliegue en la infraestructura virtual.

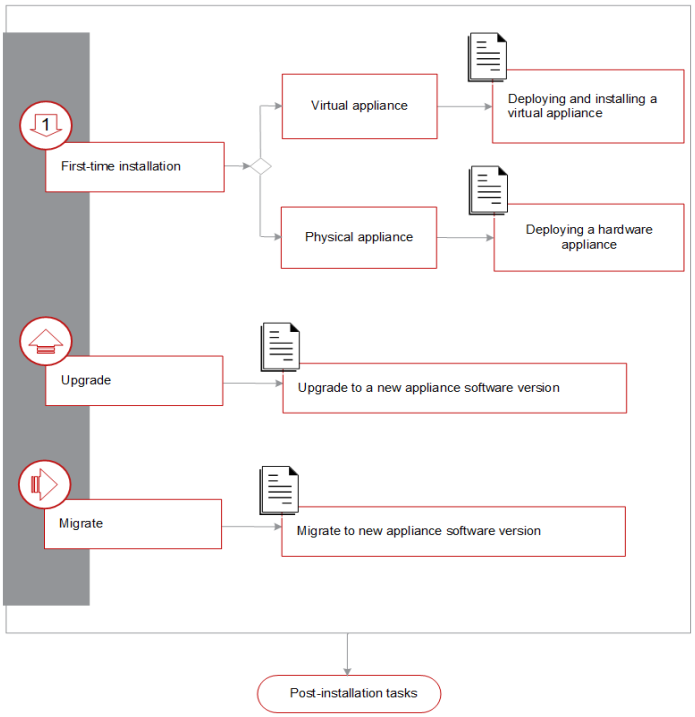

Ilustración 2. Pasos para la instalación

19. También ha de considerarse qué otros dispositivos estarán integrados con ATD, con los que se comunicará para el envío de ficheros de forma automática para su

análisis. Las opciones más habitualmente consideradas son una o una combinación de las siguientes:

a) *Standalone*. Esta es una forma sencilla de implementar McAfee ATD. En este caso, no está integrado con otros productos de McAfee instalados externamente y los ficheros a analizar se pueden enviar manualmente o mediante un cliente FTP. Este uso del ATD es habitual durante la fase de configuración de las máquinas virtuales de análisis y también como investigación de ciertos ficheros para análisis complementario por parte de los equipos del Centro de Operaciones de Seguridad (SOC).

b) Integración con *McAfee Network Security Platform (NSP)*: Según cómo se haya configurado el NSP, el sensor de IPS detecta la descarga de un archivo y envía una copia del archivo a McAfee ATD para su análisis. Si McAfee ATD detecta un *malware* en unos segundos, el sensor puede bloquear la descarga. Si el análisis por parte del ATD requiere más tiempo, el sensor permite descargar el archivo. Si a posteriori la muestra es malware, ATD informa a NSP y el sensor puede poner en cuarentena el *host* hasta que se limpie y repare.

c) Integración con *McAfee Web Gateway (MWG)*: puede configurar McAfee ATD como otro motor de protección *antimalware*. Cuando un usuario descarga un archivo, el motor *antimalware* nativo de MWG analiza el archivo y determina una puntuación de *malware*. Según esta puntuación y el tipo de archivo, MWG envía una copia del archivo a ATD para una inspección más profunda y un análisis dinámico.

d) Integración con McAfee ePO y TIE. Está integración permite a los equipos con protección EPP de McAfee enviar a ATD los ficheros de tipo PE que resulten desconocidos en la organización.

e) API. McAfee ATD dispone de un interface de programación que permite el envío de muestras vía REST.

4.5 INSTALACIÓN

20. El *appliance* se entrega de fábrica con el sistema operativo y con el *software* de ATD instalado. El conector SMTP deberá ser instalado de forma separada.

21. Es posible hacer una instalación nueva tanto del sistema operativo como de *software*. Para ello será necesario descargar el SO y copiarlo a un dispositivo USB, acceder físicamente al *appliance* e instalarlo. El procedimiento paso por paso es el siguiente:

    a) Descargar el instalador del sistema operativo de la página web de McAfee y copiarlo a un dispositivo de almacenamiento USB. Para descargarlo:

    b) Inicie sesión en *https://secure.mcafee.com/apps/downloads/my-products/login.aspx?region=us*. El certificado que presenta y su ruta de certificación son:

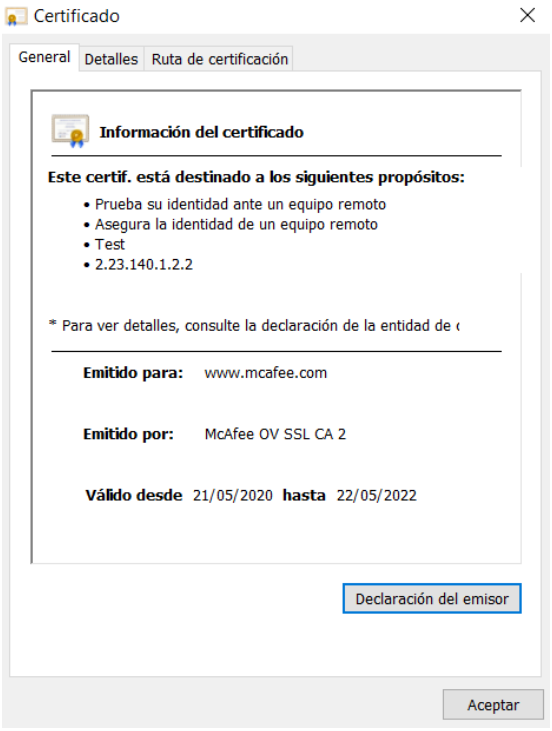

Ilustración 3. Información del certificado

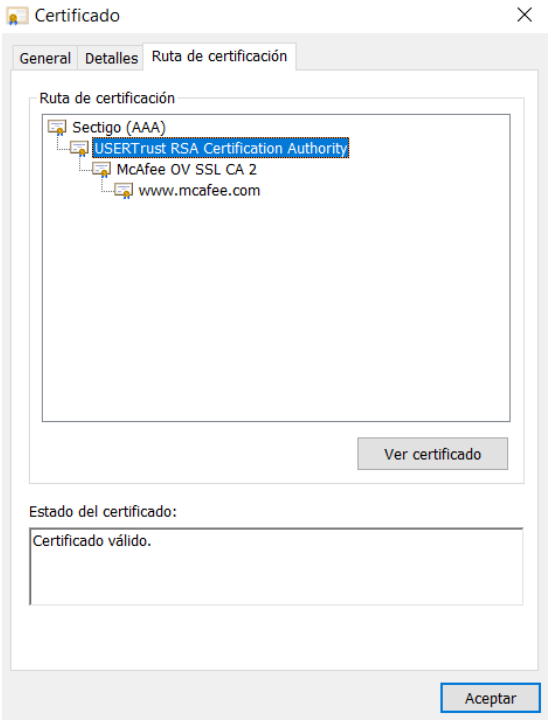

Ilustración 4. Ruta del certificado

c) Completar el *Grant Number* y dirección de correo (explicado en el apartado Entrega Segura del producto), luego hacer clic en Enviar.

d) Descargar los instaladores de SO y ATD.

e) Instalador de SO: ATD_installer.62756.x86_64.iso (*SHA C66E3EDA992F11790E5A00C26216F0D50D8956FBFBAB2BC38F057AC7F7E4A354*).

f) Instalador de ATD: system-4.0.2.42.61877.msu (*SHA 5C34FF3C8191A2881AAC22E2F7CD20065DDCD38CC2C403CED73D03A8E35B5C6B*)

Nota: Se debe verificar la integridad del instalador comparando el valor del hash de los instaladores descargados y el valor SHA aquí indicado.

g) En un USB de arranque, copiar la imagen ISO *ATD_installer* (62756.x86_64.iso) y conectar al ATD. Las instrucciones concretas para hacerlo están en *https://docs.mcafee.com/es-ES/bundle/advanced-threat-defense-4.0.0-installation-guide-unmanaged/page/GUID-F6597CC3-3F79-4A6F-A223-FB7F51C0B908.html*

h) Conectar el USB con el instalador del SO en el ATD, así como pantalla y teclado o terminal RMM y encender el dispositivo.

i) Durante el arranque del *appliance* presionar F6 para entrar en el menú de inicio y seleccionar el dispositivo USB como arranque. En ese momento, se inicia la instalación del sistema operativo.

j) Una vez completada la instalación del sistema operativo, se puede comenzar la instalación del último software ATD:

k) Iniciar sesión en el *interface* de línea de comandos (CLI) del ATD con el usuario por defecto: *cliadmin* y contraseña: *atdadmin*.

l) set appliance ip <xxx.xxx.xxx.xxx> <xxx.xxx.xxx.xxx.>

m) set appliance gateway <xxx.xxx.xxx.xxx>

n) Cargar el instalador de ATD (system-4.0.2.42.61877.msu) en su dispositivo realizando los siguientes pasos.

o) Con uso de un cliente FTP, conectarse al ATD (vía SFTP) con el nombre de usuario por defecto: *atdadmin* y contraseña: *atdadmin*.

p) Subir el fichero *.msu en la carpeta raíz del usuario *atdadmin*.

q) Instalar ATD con el siguiente comando: *install msu system-4.0.2.42.61877.msu 0*

r) Después de la instalación, iniciar sesión en la interfaz web de ATD para verificar la versión del *software*.

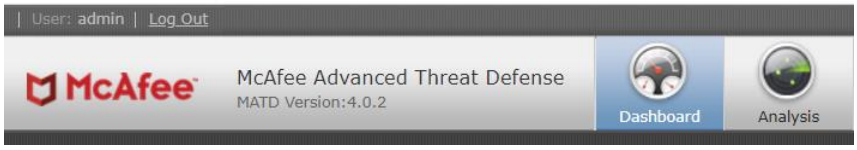

Ilustración 5. Versión del *software* instalado

5. FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

22. **Se debe habilitar el modo Common Criteria (CC) en el producto ATD**. Al habilitar el modo CC:

    a) La versión de TLS está fijada en 1.2.

    b) Se deshabilitan protocolos no seguros FTP y HTTP.

    c) Solo se utilizarán conexiones SSL en la integración con NSP.

23. Como requisito para habilitar el Modo Common Criteria, se debe previamente habilitar el *logging* de auditoría contra un servidor syslog vía TLS y con validación del servidor de syslog. En caso contrario, se obtiene el siguiente mensaje.

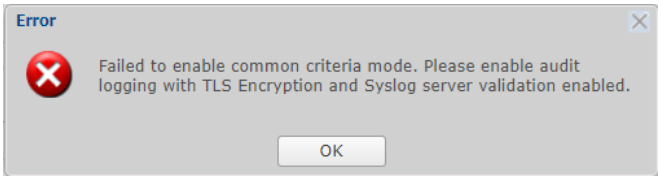

Ilustración 6. Mensaje de error para habilitar *logging*

24. El procedimiento de activación es el siguiente:

    a) Como primer punto, es necesario activar el log de auditoría en la configuración del servicio de *syslog*:

    b) Acceder al ATD vía interfaz gráfico (SSL).

    c) Navegar a las opciones Manage | ATD Configuration | Syslog, y seleccionar Enable Logging.

    d) Configurar el *System Log Server* y hacer clic en *Test connection* para verificar conectividad con el servidor syslog. El certificado cargado es validado por longitud de clave, algoritmo y fecha de expiración. En caso de un problema con el certificado será notificado mediante un mensaje de error.

    e) La configuración final de *logging* quedará del siguiente modo:

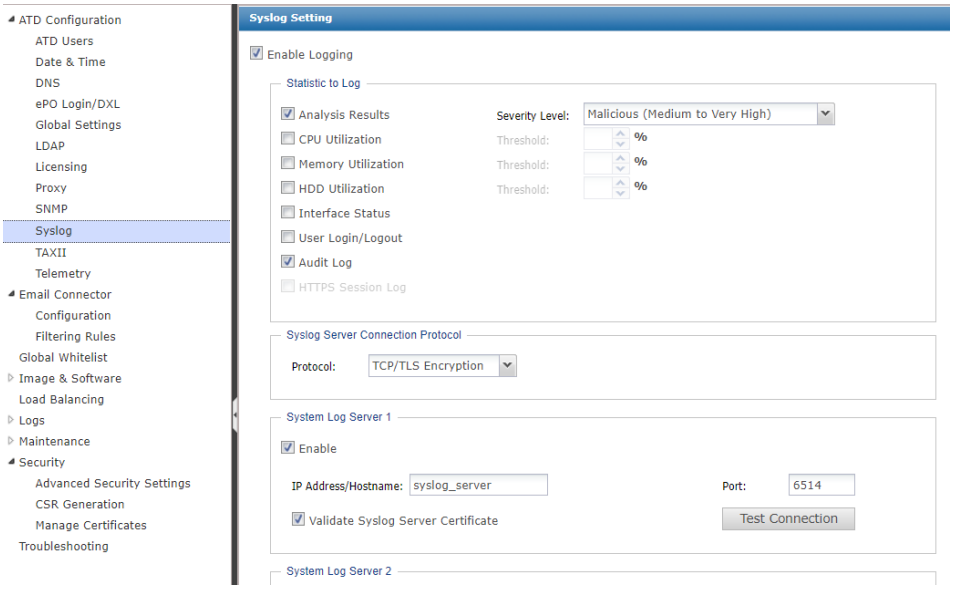

Ilustración 6. Configuración *logging*

f) Una vez activado el log de auditoría, se debe activar el modo CC:

g) Ir a Manage | Security | Advanced Security Settings, y seleccionar Common Criteria Mode

25. El modo CC se activa cuando el ATD se inicia y se detiene cuando el ATD se apaga. Además, se reinicia en uno de estos dos (2) supuestos:

    a) Cambio en el certificado de *syslog*.

    b) Cambio manual en la fecha y hora.

5.2 AUTENTICACIÓN

26. El ATD requiere dos (2) tipos de usuario.

    a) Usuarios administradores del sistema.

    b) Usuarios autenticados para la integración (envío de muestras) entre ATD y el resto de la infraestructura cliente (por ejemplo *McAfee Web Gateway* para análisis en *sandbox* de los ficheros descargados desde internet, conector de correo para análisis en *sandbox* de mails recibidos/enviados…).

27. Para ambos tipos de usuario existen dos (2) mecanismos de autenticación: la autenticación local o con un servidor LDAP.

28. A continuación, se enumeran los usuarios locales configurados por defecto, así como su propósito:

    a) **Usuario *admin***. Usuario administrador de la consola GUI de ATD.

    b) **Usuario *nsp***. Usuario utilizado para la integración entre *McAfee Network Security Platform* y ATD.

c) **Usuario *atdadmin*** utilizado para la subida de imágenes y actualizaciones de software

d) **Usuario *mwg***. Usuario utilizado para la integración entre McAfee Web Gateway y ATD.

e) ***Usuario vnsp***. Usuario utilizado para la integración entre *McAfee Virtual Network Security Platform* y ATD.

f) **Usuario *tie***. Usuario utilizado para la integración *entre McAfee Threat Intelligence Platform* y ATD.

29. Estos usuarios no se pueden borrar, pero se debe reducir al máximo posible los permisos de aquellos que no estén en uso, así como cambiar las contraseñas por defecto. A modo de ejemplo, se ilustra el procedimiento para el usuario *tie*. En primer lugar, dentro de la opción *Manage* del interfaz gráfico de usuario, seleccionar *ATD Configuration -> ATD Users*. A continuación, seleccionar el usuario *tie* y hacer clic en la opción Edit. Las modificaciones propuestas son:

a) En *User Credentials,* cambiar la contraseña. Se deben utilizar contraseñas con al menos 12 caracteres que incluyan mayúsculas, minúsculas, números y símbolos

b) Dentro de la sección *Roles*, desmarcar todos.

c) Las figuras de abajo muestran el proceso.

Ilustración 7. Selección de usuario para su configuración

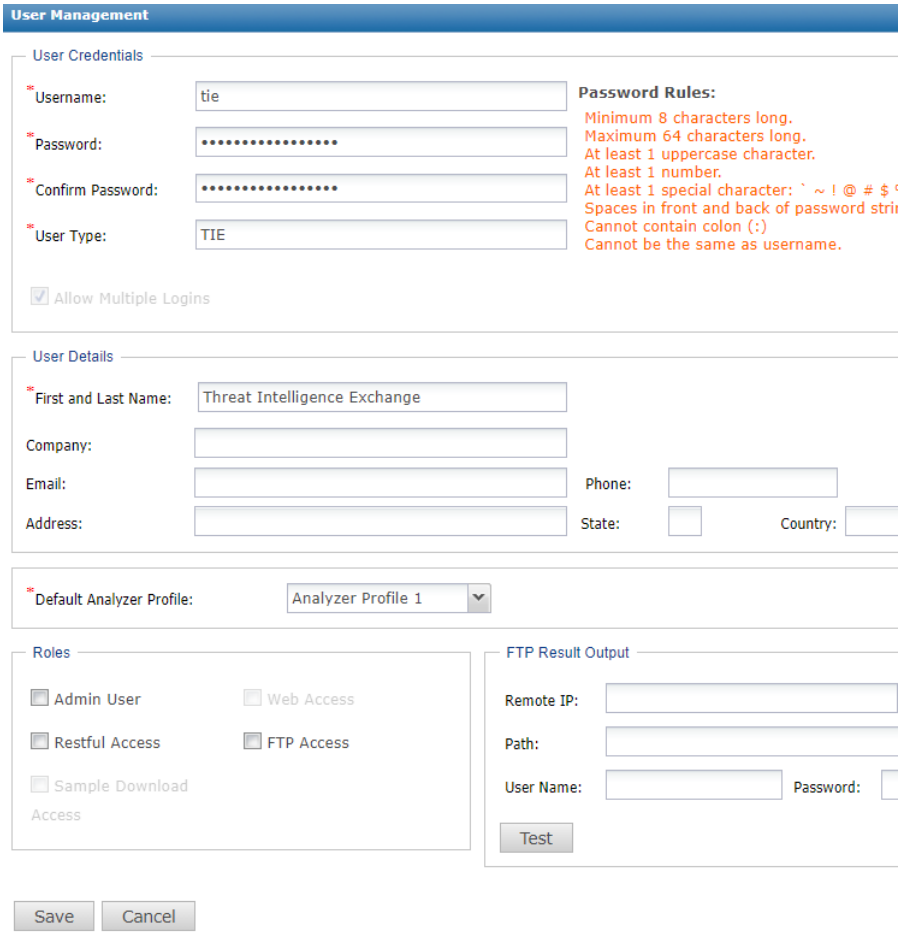

Ilustración 8. Menú de configuración de un usuario

30. Además de autenticar usuarios localmente, es posible también hacerlo vía LDAP (ver sección SERVIDORES DE AUTENTICACIÓN)

5.3 ADMINISTRACIÓN DEL PRODUCTO

5.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

31. La administración del producto se realiza esencialmente vía GUI (*https*), aunque la plataforma también tiene un interfaz de línea de comandos (CLI) con protocolo SSH y sobre el puerto tcp 2222, que permite diagnóstico avanzado y ciertas configuraciones exclusivas de CLI. Este interface (SSH) está deshabilitado en modo Common Criteria.
32. Adicionalmente, los paquetes de análisis de contenidos, actualizaciones de *software* y máquinas virtuales se cargan en el ATD vía SFTP.
33. El ATD permite otros interfaces de gestión, equivalentes a los anteriores pero utilizando protocolos no seguros (http, ftp,…) por lo que se deben desactivar en *Manage | Security | Advanced Security Settings.*

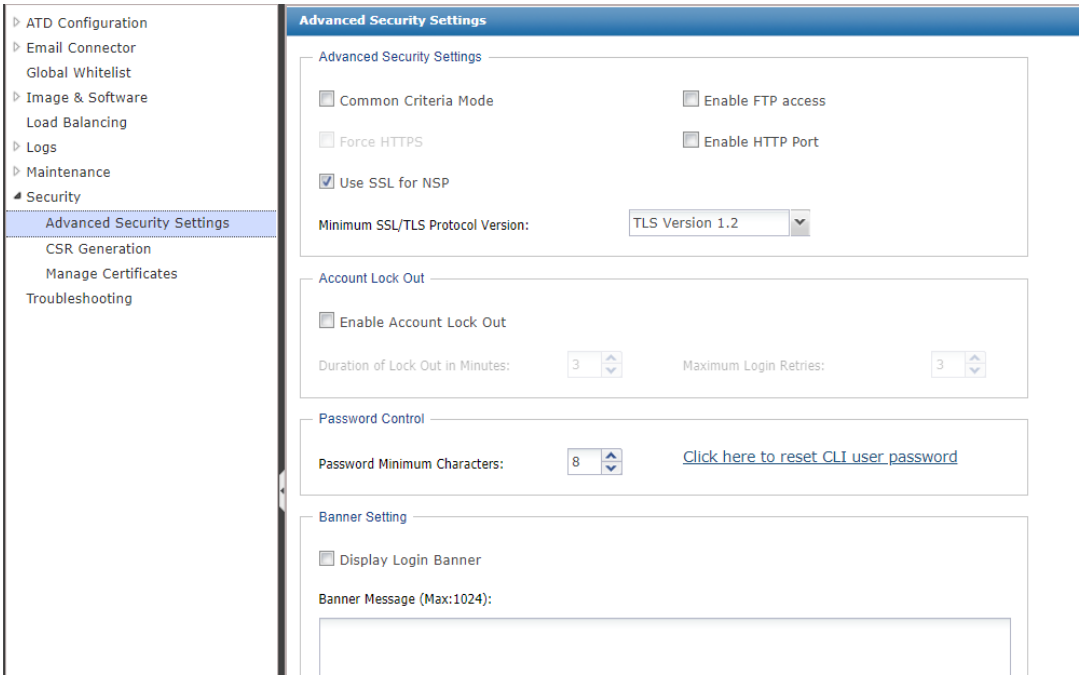

Ilustración 9. Configuración avanzada de seguridad

5.3.2 CONFIGURACIÓN DE ADMINISTRADORES

34. El ATD tiene los siguientes roles:

    a) ***Admin User***. Usuario administrador de la herramienta, este rol permite cambios de configuración de cualquier *setting* del producto.

    b) ***Web Access***. Permite el acceso al interface web solo en modo lectura.

    c) ***Restful Access.*** Permite interacción *Restful* para la subida de muestras a analizar en el ATD.

    d) ***FTP Access***. Permite el acceso vía *FTP/SFTP* para cargar ficheros de contenido, paquetes de actualización, imágenes de máquinas virtuales y muestras a analizar.

    e) ***Sample Download***. Permite la descarga de muestras analizadas.

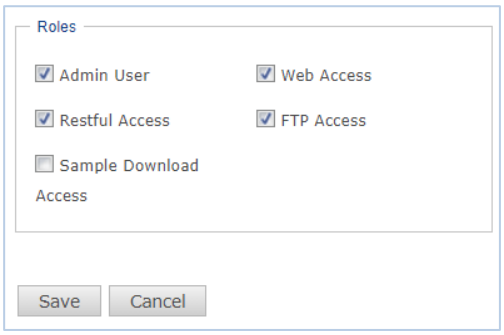

Ilustración 10. Roles de usuario

35. Estos roles y sus privilegios no son configurables. Tampoco se pueden crear roles distintos. Cualquier usuario de ATD puede tener uno o más roles.

36. La política de seguridad a nivel de cuentas de usuario se realiza de modo global, no por rol o perfil de usuario. Para hacerlo, ir *a Manage | Security | Advanced Security Settings* y definir la política de seguridad, actualmente solo se puede forzar el número mínimo de caracteres (se recomienda **mínimo 12 caracteres**) pero no su complejidad. La política de seguridad no permite la configurar de ningún otro parámetro de complejidad de contraseñas.

37. ATD permite configurar de manera global el *timeout* de inactividad de las sesiones. Para hacerlo, se accede *vía ssh* (tcp 2222) o a través del CLI (en formato físico, usando teclado y monitor, o en formato virtual usando el hipervisor de virtualización), y ejecutar el comando:

    a) *set timeout xxx* Establece en segundos el *timeout* de inactividad de sesiones *ssh*. Esta configuración es global, no por usuario o perfil de usuario.

    b) *set ui-timeout xxx* Establece en segundos el *timeout* de inactividad de sesiones *web*. Esta configuración es global, no por usuario o perfil de usuario.

    Se recomienda la configuración a través de CLI local dado que *ssh* no ha sido incluido en la certificación de seguridad y, por tanto, no forma parte del alcance de la cualificación.

38. EL ATD permite sesiones simultáneas para el mismo usuario, esto es debido a que son los usuarios configurados en los dispositivos integrados con ATD los que suben las muestras a analizar. Esta configuración *(Allow Multiple Logins)* está habilitada por defecto en el perfil de los usuarios que se utilizan en la integración (ver apartado 5.2). Para el resto de los usuarios, esta **deshabilitada** por defecto siendo esta **la configuración recomendada**.

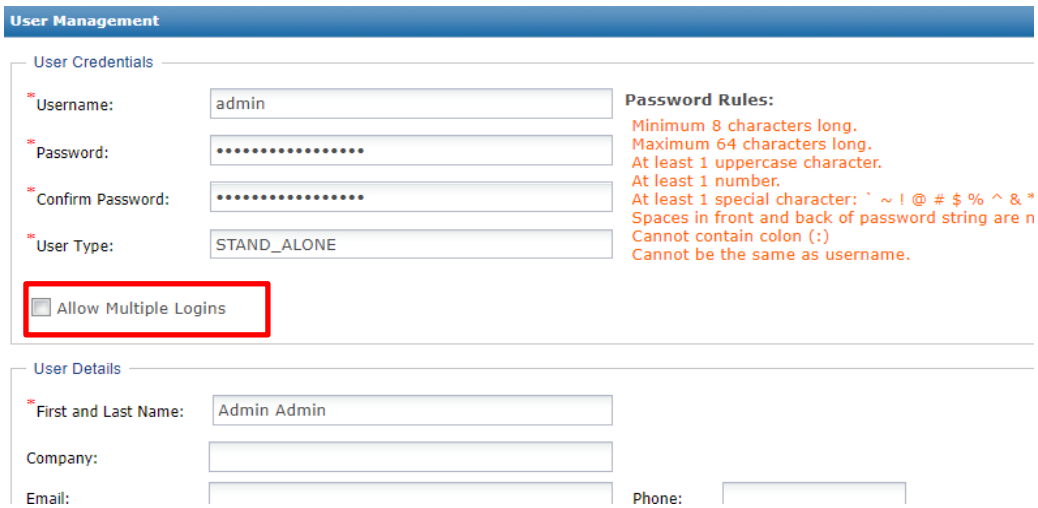

Ilustración 11. Configuración de sesiones simultáneas

39. **Se debe configurar también el bloqueo temporal de un usuario que ha tenido sucesivos intentos de autenticación fallidos**. La configuración recomendada es

de, al menos, tres (3) minutos ante tres (3) fallos consecutivos de autenticación. Esta configuración se realiza en *Manage | Security | Advanced Security Settings:*

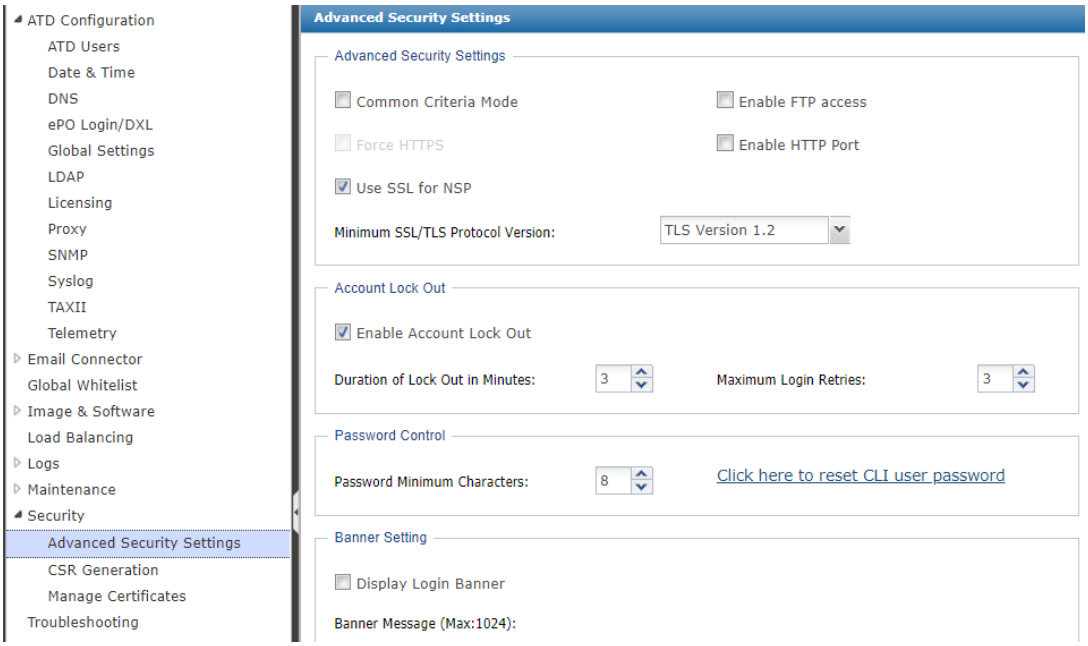

Ilustración 12. Bloqueo de usuarios y configuración de *banner*

40. **Se debe configurar un banner de *login***. McAfee ATD permite añadir un *banner* de inicio de sesión con texto personalizado. Para ello, hay que acceder también a *Manage | Security | Advanced Security Settings.*

5.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

41. McAfee ATD dispone de un interfaz de gestión, denominado *mgmt*, e interfaces adicionales que no son necesarios, salvo por requisitos de arquitectura/diseño específicos. **La recomendación general es deshabilitar todos los interfaces que no estén en uso**. Para ello, desde línea de comandos, se debe ejecutar *set intfport n disable,* donde *'n'* es el identificador del interfaz.

42. **También se debe habilitar *http_redirect*** que permite redirigir peticiones de protocolo *http* no seguro a *https*. Al habilitar *http_redirect* las muestras que sean enviadas a McAfee ATD vía *Restful* utilizando *http* son descartadas. Para habilitar en *http_redirect,* ejecutar desde línea de comandos *set http_redirect enable.*

43. Finalmente, cuando una muestra se ejecuta en *sandbox* conviene permitir el acceso a internet para la máquina virtual que está ejecutando esa muestra. El interfaz por el que las máquinas virtuales se conectan a Internet **debe estar conectado a una red aislada del resto de la empresa.** A partir de ese requisito físico, se debe definir cuál de los interface del *appliance* es ese interface de *malware*. Esta configuración se realiza mediante línea de comandos ejecutando:

    a) *set intfport <n> ip <ip> <mask>* donde *<n>* es el identificador de interfaz, *<ip>* es la dirección IP y *<mask>* es su máscara. El formato correcto es *set intfport (1|2|3) ip A.B.C.D E.F.G.H*

b) Una vez configurado nivel 3, se debe definir ese interfaz como *malware-interface* con el comando '*set malware-intfport <n> gateway <ip>*' donde *<n>* es el identificador del interface e *<ip>* es la dirección IP del *default gateway* para las máquinas virtuales que ejecutan malware.

c) Por último, en los perfiles de análisis de las muestras se indica si se permite el acceso a internet para las máquinas virtuales. Esta configuración se realiza en *Policy | Analycer Profile,* hacer clic en el perfil que se quiere modificar y *Edit*. La configuración para permitir acceso a Internet para el *malware* se consigue habilitando la opción *Internet Options | Enable Malware Internet Access***.** La siguiente figura muestra la opción concreta:

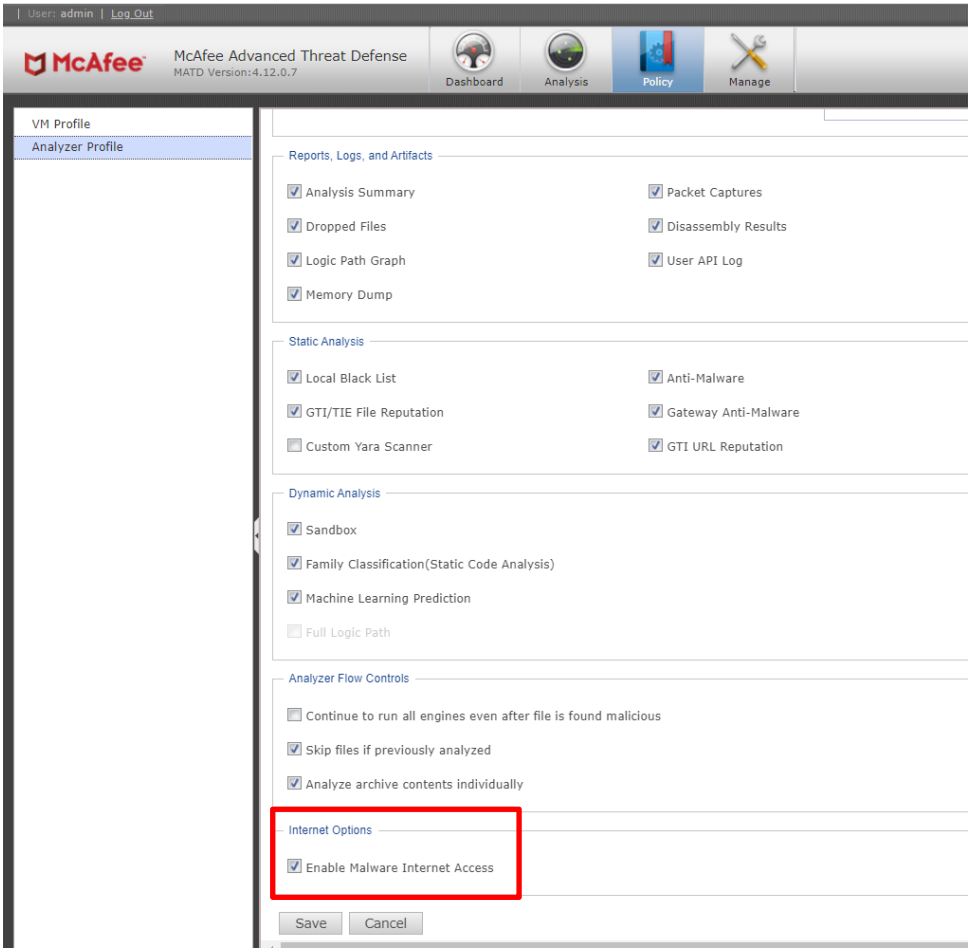

Ilustración 13. Configuración de acceso a internet desde las MV

5.5 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

44. Como se ha descrito a lo largo del documento, McAfee ATD permite comunicaciones seguras y no seguras. **Se deben utilizar únicamente comunicaciones seguras** y para ello:

a) Deshabilitar protocolos no seguros en *Manage | Security | Advanced Security Settings.*

b) Utilizar mínimo TLS 1.2 o superior en *Manage | Security | Advanced Security Settings.*

c) Usar SSL para la comunciación con el NSP en *Manage | Security | Advanced Security Settings.*

45. La siguiente figura muestra esta configuración:

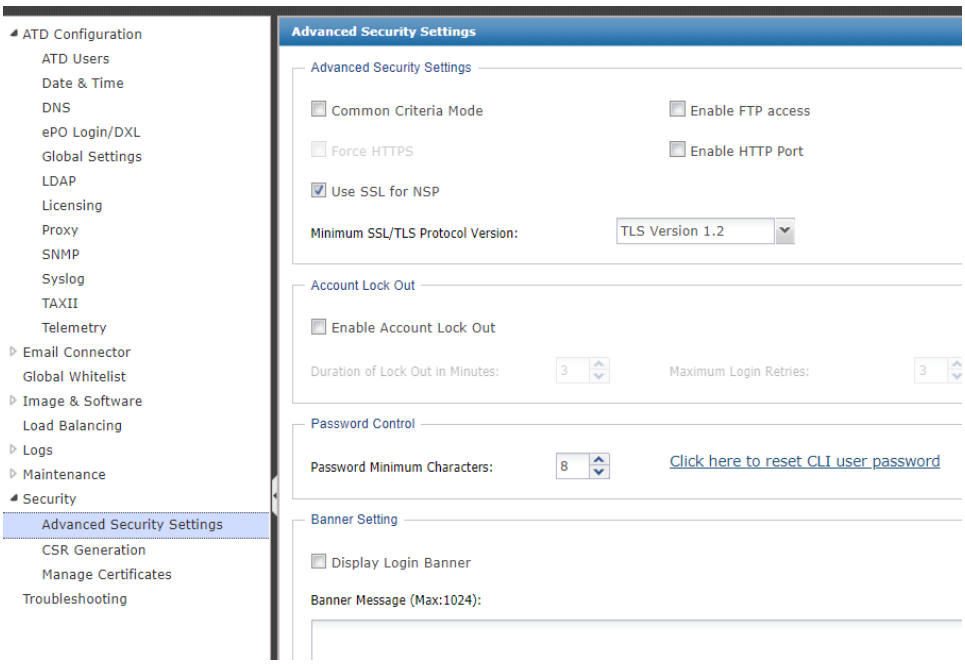

Ilustración 14. Configuración de protocolos seguros

5.6 GESTIÓN DE CERTIFICADOS

46. **Se deben sustituir los certificados autofirmados por certificados firmados por la CA de la organización**. Para ello se debe generar una solicitud de certificado (CSR) en *Manage | Security | CSR Generation*, completar los campos de la solicitud y hacer clic en *Generate*. **Debe tenerse en cuenta que los certificados deberán usar algoritmos y funciones criptográficas admitidos por la guía CCN-STIC-807**. Esto significa que solo podrán usarse los siguientes algoritmos y funciones:

- RSA con claves de, al menos, 3072 bits de longitud.
- ECDSA con curvas P-256 o superior.
- DSA con claves de, al menos, 3072 bits de longitud.
- Funciones Hash SHA-256 o superior.

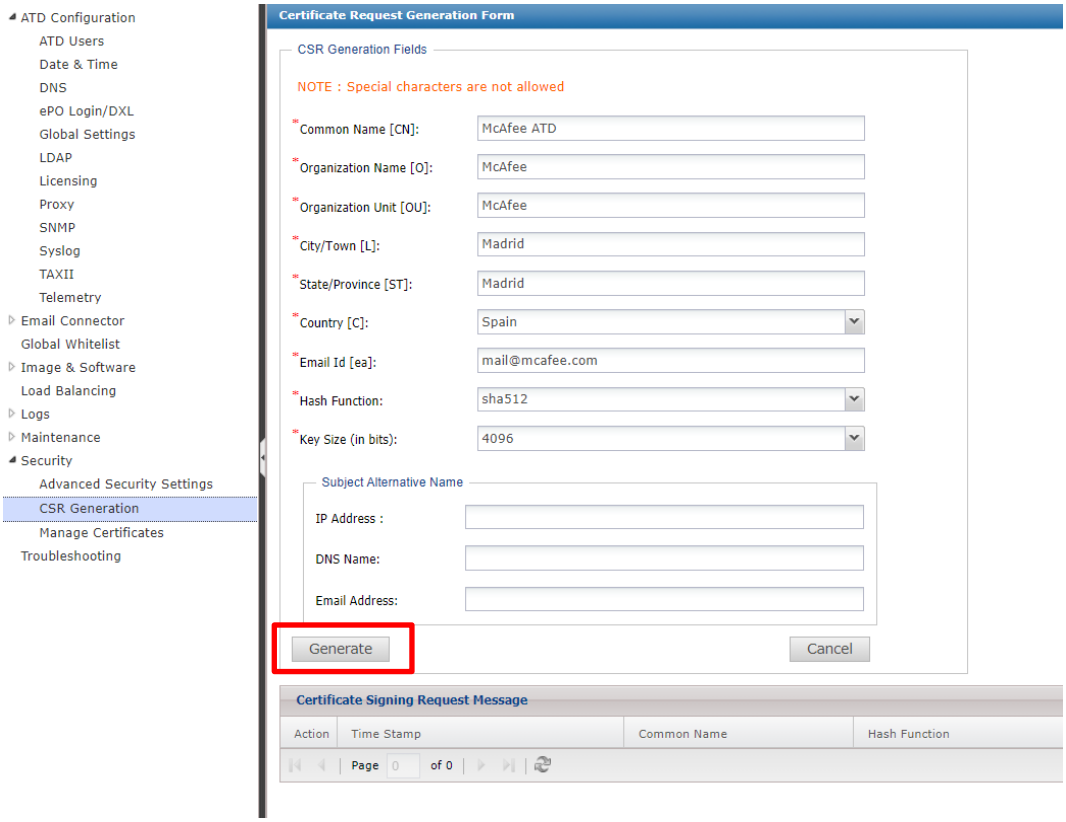

Ilustración 15. Menú gestión de certificados

47. Una vez generada la solicitud, se puede descargar el *request* en la misma ubicación en la sección ***Certificate Signing Request Message*** haciendo clic en el icono ***Action*** y seleccionando ***Export.***

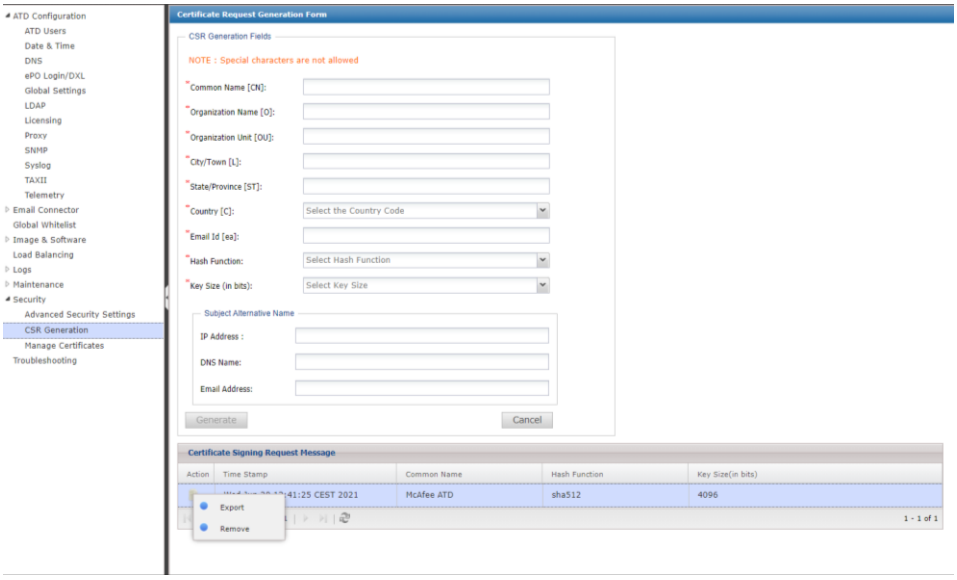

Ilustración 16. Generación de CSR

48. Para importar el certificado generado por la CA, se debe acceder a *Manage | Security | Manage Certificates* y en la sección *Web Certificates Upload*, seleccionar el certificado generado y hacer clic en *Upload*.

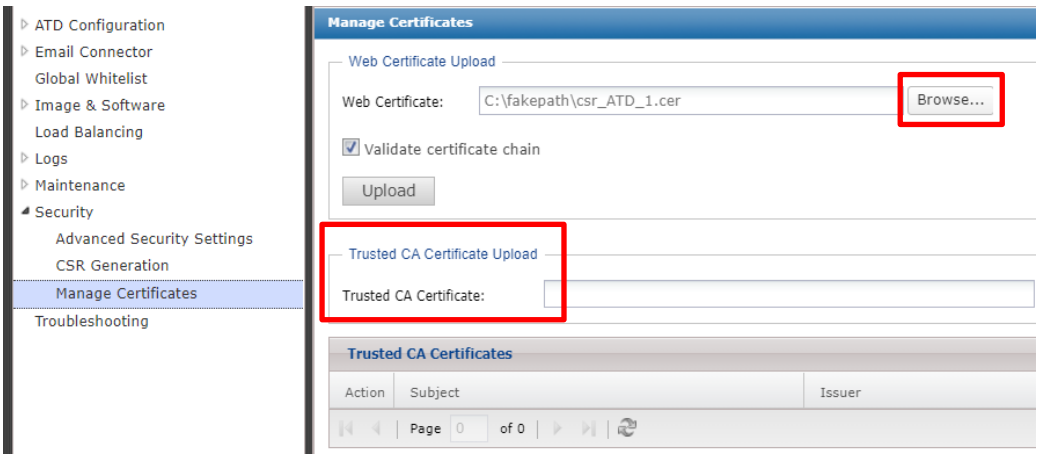

Ilustración 17. Importación de certificados

49. Se recomienda también importar los certificados de las entidades de certificación de confianza (*root CA certificate*). Esta opción está disponible en *Manage | Security | Manage Certificates*, seleccionando el *certificado dentro de la sección Trusted CA Certificate Upload* y haciendo clic en *Upload.*

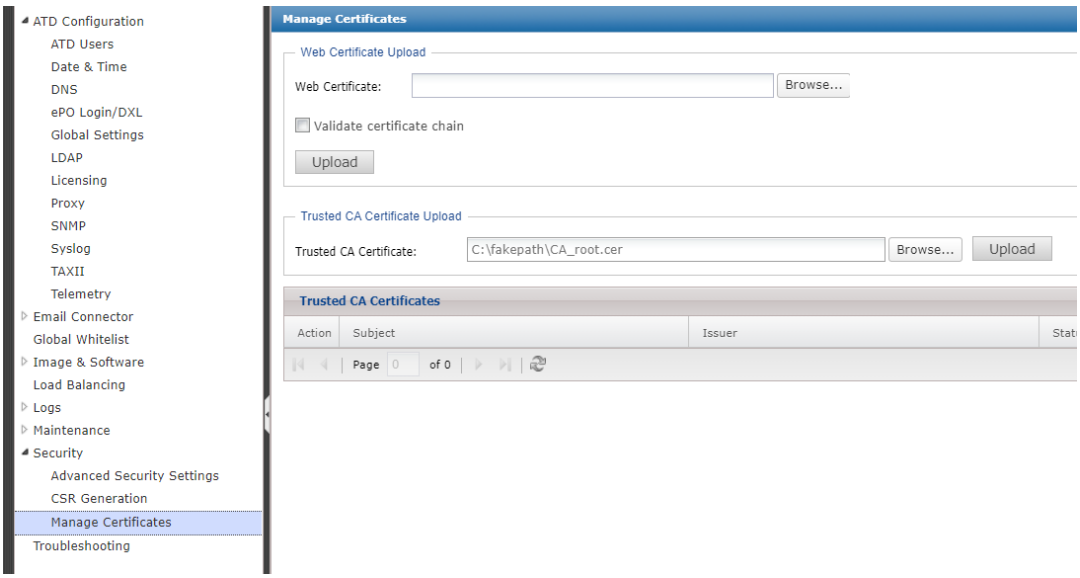

Ilustración 18. Importación de certificados CA

5.7 SERVIDORES DE AUTENTICACIÓN

50. McAfee ATD permite la autenticación contra un servidor LDAP. Un servidor de autenticación separado facilita un sistema de autenticación seguro y centralizado.

51. Se deben crear en el servidor LDAP las mismas cuentas de usuario que las del dispositivo ATD:

a) *Base Distinguished Name (BaseDN)*: crear un BaseDN específico para los usuarios de ATD que actúa como raíz bajo el cual se agregan todos los usuarios de ATD.

b) Credenciales de administrador: para habilitar la opción LDAP, se debe proporcionar las credenciales de usuario administrador en la interfaz web de ATD. Si no se ha creado el usuario administrador, se debe crear en el directorio del servidor LDAP.

c) Creación de usuarios – Se debe crear los siguientes usuarios manualmente en el servidor LDAP.

i. *admin*, usuario administrador GUI de la consola

ii. *cliadmin*, usuario administrador CLI de la consola

iii. *atdamin*, usuario con permisos SFTP para actualizar contenidos, software, máquinas virtuales…

52. Una vez configurado lo anterior, se habilita la autenticación LDAP en el ATD en *Manage | ATD Configuration | LDAP*. **Se debe utilizar un protocolo seguro en la comunicación con el LDAP.** Para ello, se debe configurar su autentación tal y como se muestra a continuación:

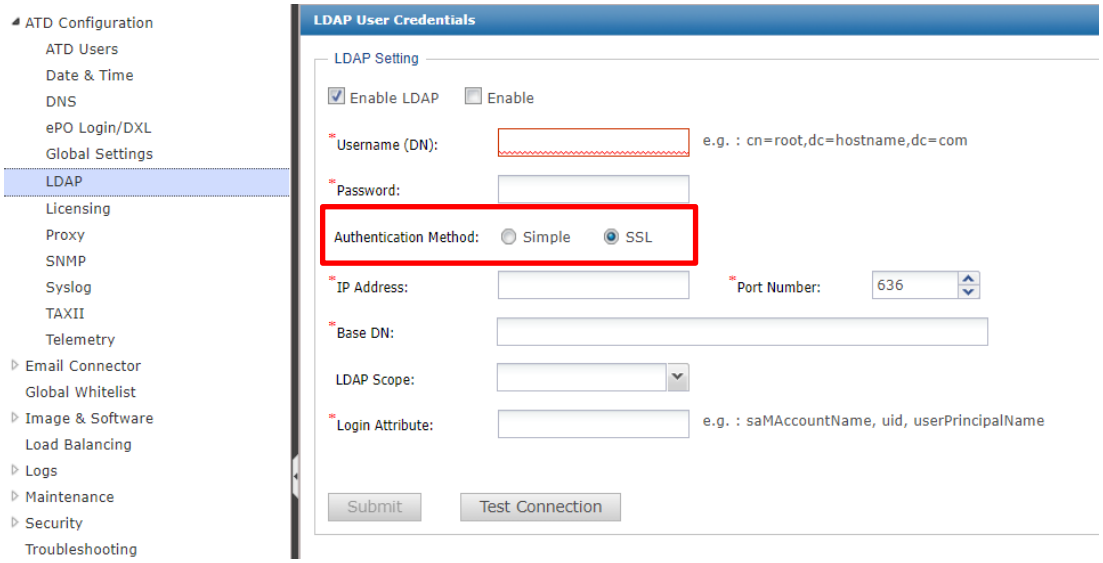

Ilustración 19. Configuración autenticación LDAP

5.8 SINCRONIZACIÓN HORARIA

53. McAfee ATD utiliza la fecha y hora para todas sus funciones y propósitos principales (información en web, análisis e informes de malware…). La fecha y hora se puede configurar tanto manualmente como mediante un servidor de tiempos en red que es la **opción recomendada**. Para utilizar **un servidor NTP**, McAfee ATD debe tener configurado un servidor DNS puesto que se configura por nombre.

54. La configuración segura de NTP se habilita seleccionando *Secure* en *Manage | ATD Configuration | Date & Time.*

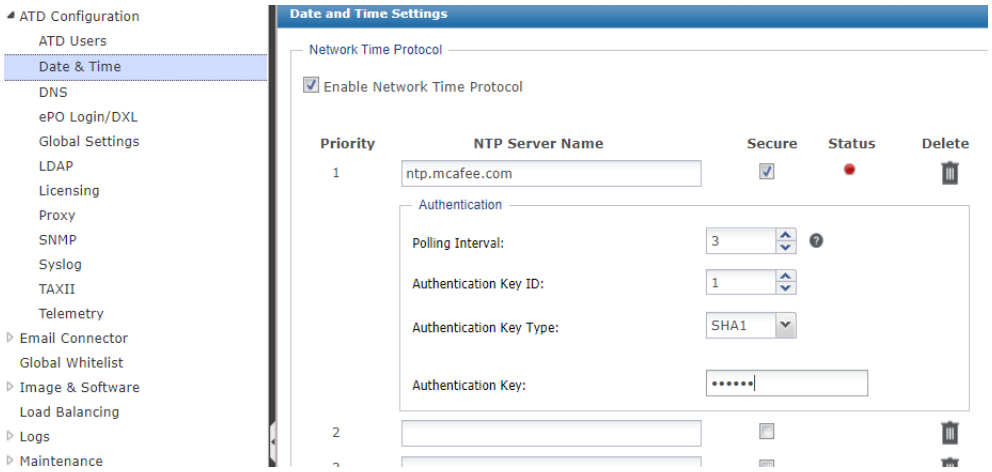

Ilustración 20. Configuración servidor NTP

55. Es posible configurar hasta tres (3) servidores NTP.

5.9 ACTUALIZACIONES

56. El servidor ATD se conecta de forma segura (*https*) y periódica con servicios en *cloud* de McAfee para descargar actualizaciones de contenidos y *software*. Los requisitos a nivel de comunicaciones para esta funcionalidad son:

Puerto	Protocolo	Servicio	Observaciones
443	TCP (HTTPS)	*Updates for McAfee Gateway Anti-Malware Engine and McAfee Anti-Malware Engine:* *wpm.webwasher.com,* *wpm1-2.webwasher.com* *wpm1-3.webwasher.com,* *wpm1-4.webwasher.com* *wpm-usa.webwasher.com,* *wpm-usa1.webwasher.com* *wpm-usa2.webwasher.com,* *wpm-asia.webwasher.com* *tau.mcafee.com, tau1-2.mcafee.com* *tau1-3.mcafee.com,* *tau1-4.mcafee.com* *tau-usa.mcafee.com,* *tau-usa1.mcafee.com* *tau-usa2.mcafee.com,* *tau-manual.mcafee.com* *tau-ldv1.securelabs.webwasher.com* *tau-ldv2.securelabs.webwasher.com* *tau-ldv3.securelabs.webwasher.com* *tau-europe.mcafee.com*	Estas comunicaciones pueden ser proxificadas

Puerto	Protocolo	Servicio	Observaciones
		tau-dnv1.securelabs.webwasher.com *tau-dnv2.securelabs.webwasher.com* *tau-dnv3.securelabs.webwasher.com* *tau-asia.mcafee.com* *rpns.mcafee.com,* *mwg-update.mcafee.com*	
443	TCP (HTTPS)	*atdupdate.mcafee.com*	Actualización de *software* de ATD y de contenidos relativos al paquete de detección de *malware*.

5.10 AUTO-CHEQUEOS

57. McAfee ATD no tiene esta la funcionalidad.

5.11 SNMP

58. ATD permite la monitorización de los servicios y el *hardware* vía SNMP. **Se recomienda la configuración de SNMP v3**. Para ello se debe acceder *Manage | ATD Configuration | SNMP* y completar los siguientes campos:

    a) Habilitar SNMP Monitoring y SNMP Traps

    b) Seleccionar SNMP v3. En el Security Level indicar Authenticacion and Privacy y en Authentication Type indicar SHA.

    c) Completar los campos de Password (Authentication and Privacy)

    d) Seleccionar el destino de los *Traps* por *IP*, así como aquellos aspectos que se quieran monitorizar por Traps.

    e) Hacer clic en *Submit*. Las siguientes pantallas muestran la configuración.

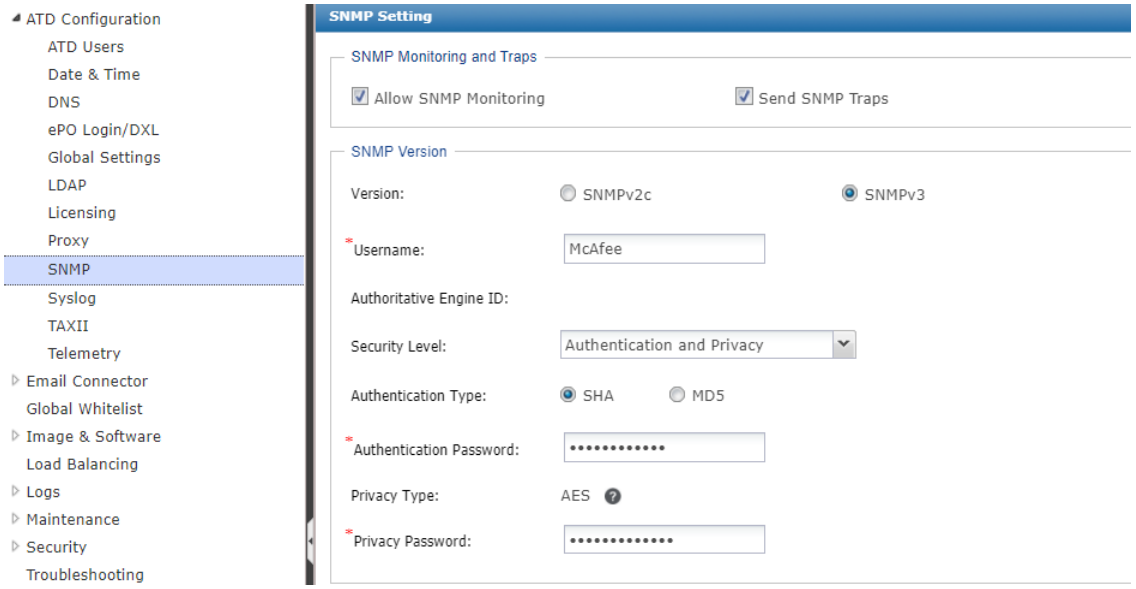

Ilustración 20. Configuración SNMP (I/II)

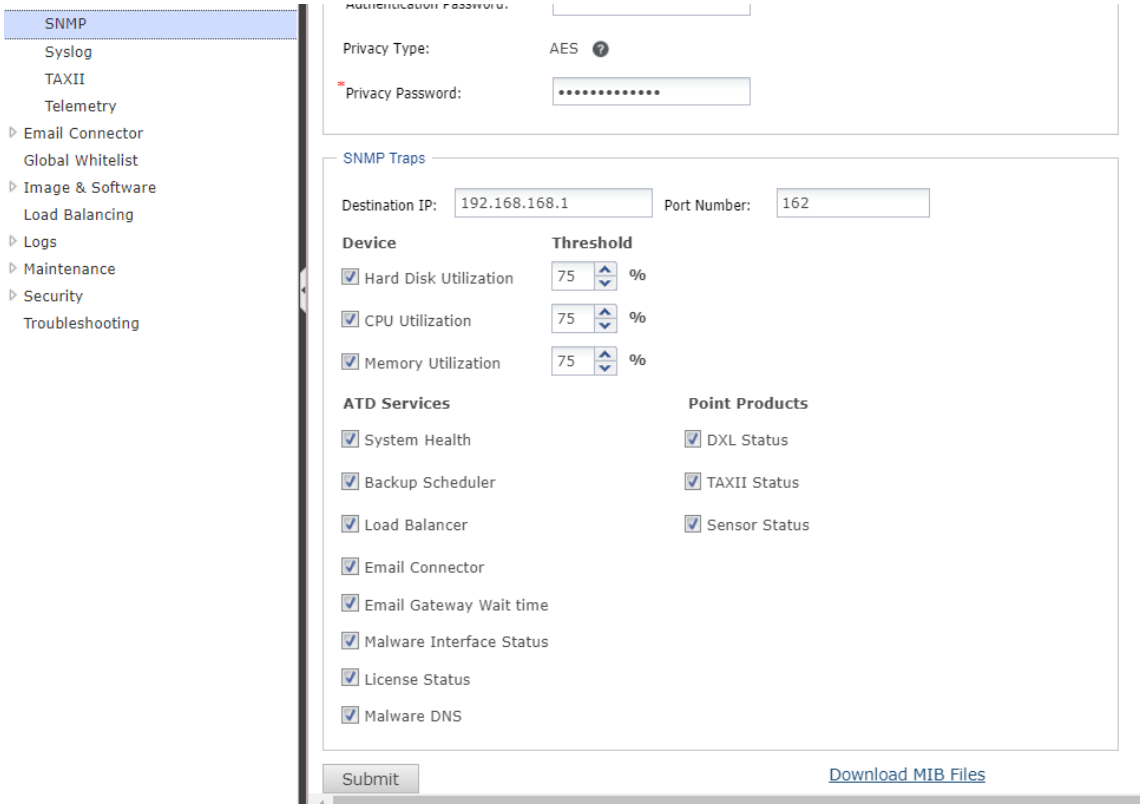

Ilustración 21. Configuración SNMP (II/II)

5.12 ALTA DISPONIBILIDAD

59. McAfee ATD permite agrupar dos o más dispositivos por razones de dimensionamiento y escalabilidad. Por lo tanto, la carga de análisis se equilibra de manera eficiente entre los nodos del clúster.

60. Un clúster de ATD se implementa de forma nativa, de modo que cada nodo tiene su propio direccionamiento IP y el clúster cuenta con una dirección IP adicional que es a la que se envían las muestras. En esta configuración, un clúster de ATD tiene los siguientes roles:

    a) Nodo Principal. Recibe los ficheros a analizar de otros dispositivos (MWG, NSM, TIE,…), los distribuye para su análisis entre los nodos del clúster y puede también analizar muestras. Gestiona la dirección IP virtual del clúster.

    b) Nodo Secundario. Recibe y analiza las muestras desde el nodo principal.

    c) Nodo de *Backup*. Recibe y analiza las muestras desde el nodo principal. Además, el nodo de *backup* monitoriza al nodo principal y se autopromociona como principal en caso de caída.

61. La configuración del clúster se realiza en *Manage | Load Balancing* según lo siguiente:

    a) Añadir la dirección del nodo *Primary* y pulsar en *Add Node.*

    b) Asignar una dirección IP del clúster y pulsar *Save*

    c) Añadir el siguiente nodo del clúster con el rol de *Backup* y pulsar *Add Node.* Después del nodo *Primary*, lo recomendado es añadir el nodo de *backup* para tener contingencia en caso de caída del primario.

    d) Añadir los siguientes nodos del clúster con el rol de *Secondary* y pulsar *Add Node.*

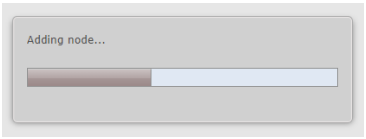

Ilustración 22. Ventana añadiendo nodo

62. Una vez se han configurado los nodos del clúster las siguientes configuraciones se sincronizan entre nodos.

    a) Perfiles de VM

    b) Tiempo de espera de umbral máximo

    c) Credenciales de usuario LDAP

    d) Configuración de *proxy*

    e) Configuración de *SNMP*

    f) Configuración de *Syslog*

    g) Entradas de la lista negra

    h) Entradas de la lista blanca

    i) Telemetría

j) Gestión de usuarios

k) Integración de *McAfee ePO*

l) Integración de McAfee Data Exchange Layer (DXL)

m) Configuración de DNS

n) Base de datos de respaldo

o) Hora del sistema

p) Configuración global

63. Las siguientes configuraciones no se sincronizan.

a) Versión del software ATD

b) *McAfee Anti-Malware Engine DAT* y versiones del motor

c) *McAfee Gateway Anti-Malware Engine DAT* y versiones del motor

d) Zona horaria

e) Zona horaria del servidor NTP

f) Reglas YARA personalizadas

g) Cambios en la configuración de CLI

5.13 AUDITORÍA

5.13.1 REGISTRO DE EVENTOS

64. El mecanismo de *syslog* transfiere los eventos de *Advanced Threat Defense* a través del canal de *syslog* al *Security Information and Event Management (SIEM)* o un servidor de registro.

65. Se pueden configurar hasta dos (2) servidores *syslog* externos a los que se envía la siguiente información según su configuración:

- Resultados de análisis (solo maliciosos o todos)
- Utilización de CPU (por encima de un porcentaje de umbral)
- Utilización de la memoria (por encima de un porcentaje de umbral)
- Utilización de HDD (por encima de un porcentaje de umbral)
- Estado de la interfaz
- Inicio de sesión / cierre de sesión de usuario
- Registro de auditoría
- Registro de sesión HTTPS

66. Una vez que se excede el umbral definido por el usuario para la utilización de la CPU, la utilización de la memoria y la utilización del disco duro, los eventos de

syslog se generan y se envían al receptor SIEM. El nivel de umbral mínimo admitido es 30%. El nivel de umbral máximo admitido es del 90%. De forma predeterminada, el porcentaje de umbral es 75%.Se pueden configurar hasta dos (2) servidores syslog externos a los que se envía la siguiente información según su configuración:

5.13.2 ALMACENAMIENTO LOCAL

67. Los eventos de auditoría se almacenan localmente sin que sea necesario un mantenimiento de los discos. En caso de necesidad por espacio, los registros más antiguos se sobrescriben.

5.13.3 ALMACENAMIENTO REMOTO

68. McAfee ATD permite la configuración de *syslog* tanto en claro como cifrado TLS. **Sin embargo, solo se debe utilizar *syslog* a través de un canal seguro, en este caso, con TLS.** Consultar el apartado MODO DE OPERACIÓN SEGURO para más detalles.

5.14 BACKUP

69. Como *backup* se pueden programar copias de la configuración y de los resultados del ATD. Los ficheros de *backup* se pueden almacenar localmente o en un servidor FTP designado, de forma diaria, semanal o mensual.
70. Cuando se realiza una restauración desde una copia de seguridad, ATD recopila los datos del archivo de *backup* y sobrescribe su base de datos con el contenido de la copia de seguridad.
71. Los datos que se salvaguardan durante el proceso de *backup* son:
    a) Local Blacklist
    b) Global Whitelist
    c) *VM profiles*. NOTA: Las imágenes de análisis o discos VMDK no son copiados en el archive de *backup.* En este caso, antes de recuperar desde *backup*, es necesario asegurarse que tanto las imágenes de máquinas virtuales o discos VMDK están disponibles en el ATD.
    d) Perfiles de análisis
    e) Información de usuarios
    f) Detalles de integración con *McAfee ePO*
    g) Configuración de *Proxy*
    h) Configuración de DNS
    i) Configuración de *Syslog*
    j) Configuración de SNMP

k) Configuración de fecha y hora, incluyendo en su caso NTP

l) Configuration de clustering

m) Reglas YARA personalizadas

72. Los datos que NO se salvaguardan durante el proceso de *backup* son:

    a) Cualquier fichero o URL que está siendo analizada mientras se ejecuta el *backup*

    b) Los discos VMDK o imágenes VMs

    c) Copia del *software*

    d) Ficheros de log del ATD o de diagnóstico

    e) Configuración de red del ATD

73. Para programar un *backup*, se accede a *Manage | Maintence | Backup & Restore | Backup.*

74. **Se recomienda programar un *backup* diario en horario fuera de trabajo, en un servidor remoto y utilizando el protocolo SFTP**. Se debe también mantener al menos, las últimas 7 copias de los ficheros de *backup* (1 semana).

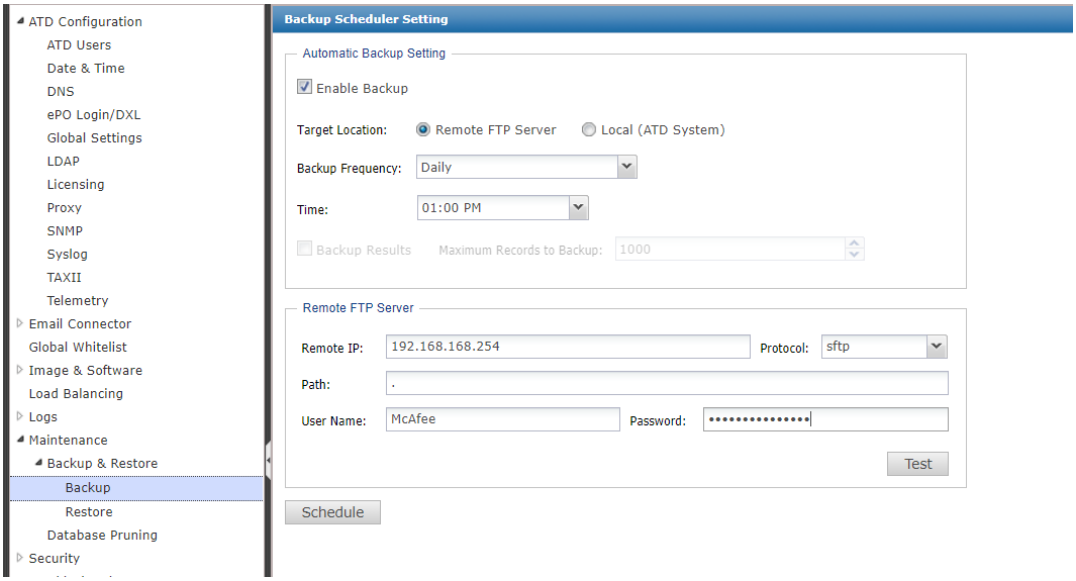

Ilustración 23. Configuración de *backup*

5.15 SERVICIOS DE SEGURIDAD

75. McAfee ATD no implementa servicios de seguridad adicionales al propio análisis de ficheros (utilizando diversos motores tanto estáticos como dinámicos) y a los servicios y configuraciones mencionados en esta guía.

6. FASE DE OPERACIÓN

76. De forma rutinaria se deberán realizar al menos las siguientes acciones.

- Comprobar y monitorizar los resultados del análisis de *malware*.
- Comprobar y monitorizar la salud de los componentes de sistema.
- Comprobar y actualizar los paquetes de contenidos de análisis:
  - Paquete de GAM y Antivirus
  - *Detection Packadge*

7. CHECKLIST

77. La siguiente *checklist* contiene el listado de los aspectos de seguridad que se deben tener en cuenta al utilizar McAfee ATD.

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la entrega segura del producto	☐	☐	
Instalación en un entorno seguro	☐	☐	
Registro de los equipos	☐	☐	
Actualización de software	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Modo de Operación seguro activado (FIPS-CC)	☐	☐	
Usuarios por defecto habilitados.	☐	☐	
Integración segura con LDAP.	☐	☐	
Interfaces de red deshabilitados.	☐	☐	
Configuración de interfaz de *malware*.	☐	☐	
Configuración de certificados de confianza.	☐	☐	
Sincronización horaria NTP.	☐	☐	
Configuración de DNS.	☐	☐	
Configuración de SNMP.	☐	☐	
Configuración de Syslog.	☐	☐	

8. REFERENCIAS

a) Guía de instalación del ATD disponible en https://docs.mcafee.com/es-ES/bundle/advanced-threat-defense-4.12.x-installation-guide

b) Guía de producto del ATD disponible en *https://docs.mcafee.com/es-ES/bundle/advanced-threat-defense-4.12.x-product-guide/*

9. ABREVIATURAS

ATD	*McAfee Advance Threat Defense*
CC	*Common Criteria*
CLI	*Command Line Interface*
DNS	*Domain Name Server*
DXL	*Data Exchange Layer*
ePO	*ePolicy Orchestrator*
GUI	*Graphical User Interface*
LDAP	*Lightweight Directory Access Protocol*
MWG	*McAfee McAfee Web Gateway*
NSP	*McAfee Network Security Platform*
NTP	*Network Time Protocol*
SNMP	*Simple Network Management Protocol*
TLS	*Transport Layer Security*

PUBLICACIONES DE DEFENSA

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