

Guía de Seguridad de las TIC

CCN-STIC 1443

Procedimiento de Empleo Seguro FortiManager



Julio 2023



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

cpage.mpr.gob.es

Edita:



Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2023

NIPO: 083-23-281-3

Fecha de Edición: julio 2023

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

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

ÍNDICE.....	2
1. INTRODUCCIÓN	3
2. OBJETO Y ALCANCE	4
3. ORGANIZACIÓN DEL DOCUMENTO	5
4. FASE DE DESPLIEGUE E INSTALACIÓN	6
4.1 ENTREGA SEGURA DEL PRODUCTO	6
4.2 ENTORNO DE INSTALACIÓN SEGURO	6
4.3 REGISTRO Y LICENCIAS	6
4.4 CONSIDERACIONES PREVIAS	6
4.5 INSTALACIÓN.....	7
5. FASE DE CONFIGURACIÓN	9
5.1 MODO DE OPERACIÓN SEGURO	9
5.1.1 CIFRADO DE DATOS	9
5.2 AUTENTICACIÓN.....	9
5.3 SERVIDORES DE AUTENTICACIÓN EXTERNOS.....	10
5.4 ADMINISTRACIÓN DEL PRODUCTO	10
5.4.1 ADMINISTRACIÓN LOCAL Y REMOTA	10
5.4.2 CONFIGURACIÓN DE ADMINISTRADORES	11
5.4.3 PARÁMETROS DE SEGURIDAD.....	12
5.4.4 CONFIGURACIÓN DEL BANNER DE ACCESO.....	12
5.5 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS.....	13
5.6 CONFIGURACIÓN DE PROTOCOLOS SEGUROS	13
5.7 GESTIÓN DE CERTIFICADOS.....	13
5.8 SINCRONIZACIÓN HORARIA	14
5.9 ACTUALIZACIONES	14
5.10 AUTO-CHEQUEOS.....	14
5.11 ALTA DISPONIBILIDAD.....	15
5.12 AUDITORÍA	15
5.12.1 REGISTRO DE EVENTOS	15
5.13 COPIAS DE SEGURIDAD	16
5.14 FUNCIONES DE SEGURIDAD	16
6. FASE DE OPERACIÓN	17
7. CHECKLIST.....	18
8. REFERENCIAS	19
9. ABREVIATURAS	20

1. INTRODUCCIÓN

1. Los equipos FortiManager permiten gestionar de manera centralizada cualquier número de dispositivos de seguridad Fortinet, desde unos pocos hasta varios miles, incluidos FortiGate, FortiWifi y FortiSwitchs. Los administradores de red pueden controlar mejor sus redes agrupando sus dispositivos en dominios de administración (ADOMS), aplicando políticas de forma más eficiente y distribuyendo actualizaciones de firmware y contenidos de seguridad. FortiManager es uno de los dispositivos de seguridad más versátiles que proporciona una diversa gama de despliegues, flexibilidad de crecimiento, personalización avanzada por medio de APIs y licenciamiento sencillo.
2. FortiManager proporciona las siguientes funcionalidades:
 - Creación de configuraciones centralizadas, políticas de provisión, gestión de actualizaciones y monitorización extremo a extremo para tu infraestructura Fortinet.
 - Separa de una forma fácil y segura la gestión de grandes entornos agrupando los dispositivos y agentes en dominios de administración geográficos o funcionales.
 - Reduce la carga de administración y costes de operación con una provisión rápida de agentes y dispositivos, seguimiento detallado de revisiones y capacidad de auditoria profunda.
 - Administración sencilla de entornos VPN complejos en malla y en estrella al tiempo que aprovecha FortiManager como el punto local de distribución de actualizaciones de software y políticas.
 - La perfecta integración con FortiAnalyzer permite el descubrimiento, análisis, priorización e informes de los eventos de seguridad de la red.
 - Rápida creación y modificación de objetos y políticas con un editor visual consolidado y con capacidades de arrastrar y soltar.
 - Provisión de dispositivos programable y automática, instalación de políticas, etc. con una API JSON o capacidad para construir portales web personalizados con el API XML.
 - Aprovisionamiento y configuración masivos de dispositivos gestionados aprovechando las capacidades para crear completos perfiles de dispositivos.
 - Control centralizado de actualizaciones de firmware y contenidos de seguridad para dispositivos gestionados.
 - Posibilidad de despliegue en físico y también en virtual con múltiples opciones para aumentar el almacenamiento de forma dinámica.

2. OBJETO Y ALCANCE

3. El objeto del presente documento es servir como guía para realizar una instalación y configuración segura de la solución **FortiManager en su versión 6.2** (v6.2.8-build9589 o superior).
4. El presente documento aplica la versión FMG-VM y a los modelos *hardware*:
 - FMG-300F
 - FMG-1000F
5. Este producto está cualificado e incluido en la Familia '*Herramientas de gestión de red*' del Catálogo de Productos y Servicios de Seguridad STIC del CCN (CPSTIC).

3. ORGANIZACIÓN DEL DOCUMENTO

6. Este documento se compone de los siguientes apartados:

- a) Apartado 4. En este apartado se recogen aspectos y recomendaciones a considerar, durante la instalación del producto.
- b) Apartado 5. En este apartado se recogen las recomendaciones a 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 o 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. En este apartado se incluye el listado de documentos referenciados 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

7. El dispositivo se entrega en formato *appliance*. Tras la entrega del dispositivo, es necesario verificar que no ha sido manipulado. Para asegurarse de la autenticidad e integridad del producto se deben seguir los siguientes pasos:
 - Verificar que el embalaje contiene los cierres originales del fabricante.
 - Verificar que el embalaje se encuentra en condiciones óptimas, sin golpes ni signos de humedad o deterioro. El embalaje interno deberá ser una bolsa de plástico transparente sellada.
 - Verificar con la información comercial (documento *pdf* del pedido) que el Número de Serie del equipo corresponde con el recibido.
 - Verificar que el sello de garantía está intacto.

4.2 ENTORNO DE INSTALACIÓN SEGURO

8. Se recomienda llevar a cabo la instalación de *FortiManager* en el CPD de la organización con el fin de limitar el acceso físico al equipo. El acceso físico al producto deberá realizarse únicamente por administradores previamente autorizados.

4.3 REGISTRO Y LICENCIAS

9. Para acceder al firmware y el soporte de usuario, se debe registrar el producto en la página de Soporte de Fortinet. En el siguiente [enlace](#) se pueden consultar los pasos concretos necesarios para llevar a cabo dicho registro.

4.4 CONSIDERACIONES PREVIAS

10. Se recomienda la ejecución de las *Best Practices* proporcionadas por Fortinet en la implementación del sistema FortiManager, las cuales se pueden consultar en el siguiente [enlace](#). Adicionalmente, se recomienda situar el dispositivo detrás de un firewall, para limitar los intentos de acceso no autorizados al mismo.
11. Durante el acceso inicial al dispositivo, se solicitará configurar la contraseña del usuario *admin*. Se deberán seguir las recomendaciones indicadas en el apartado [5.4.3 PARÁMETROS DE SEGURIDAD](#), relativas a la política de contraseñas.
12. **Se deberá desactivar el usuario por defecto administrador de API.** Para ello, mediante consola, ejecutar los siguientes comandos:

```
config system admin user
  edit admin
    set rpc-permit none
  end
```

4.5 INSTALACIÓN

13. El producto debe emplear la versión **FortiManager v6.2.8 o superior**, por lo que será necesario descargar e instalar esta mediante los siguientes pasos:

- Se debe registrar el producto en <https://www.forticloud.com>, con la cuenta empleada por la organización para adquirir el producto. Para ello, pulsar sobre “Register Now”.

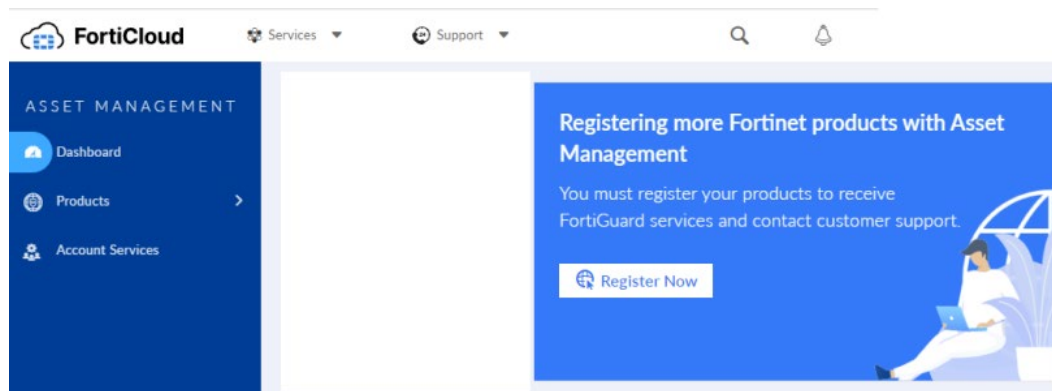


Ilustración 1. Registro del producto (I)

- Marcar la casilla *Government User*:

The image shows a 'Register Product' form. At the top is a blue header with the text 'Register Product'. Below it is a section for 'Registration Code' with a red asterisk. A text box contains the instruction: 'Please enter your product serial number, service contract registration code or license certificate number to start the registration:'. Below this is a large empty text input field. Further down is the 'End User Type' section, also marked with a red asterisk. It states 'The product will be used by' and has two radio button options: 'A government user' (which is selected) and 'A non-government user'. Below these options is a small text block explaining that a government end-user includes central, regional, or local government departments, agencies, or other entities performing governmental functions. A list of examples follows: 1. Governmental research institutions, 2. Governmental corporations or their separate business units which are engaged in the manufacture or distribution of items or services controlled on the Wassenaar Munitions List, and 3. International governmental organizations.

Ilustración 2. Registro del producto (II)

- Descargar la **versión de software FortiManagerv6.2.8 o superior** pulsando sobre “HTTPS” según el modelo *Hardware* adquirido:

FortiCloud Services Support

Download / Firmware Images Account Name/ID: Fortinet

Firmware Images Fortinet Firmware Images And Software Releases

Welcome to the Firmware Images download center for Fortinet's extensive line of security solutions.

Select Product

FortiManager

Release Notes **Download**

Image File Path

/ FortiManager/ v6.00/ 6.2/ 6.2.8/

Image Folders/Files

[Up to higher level directory](#)

Name	Size (KB)	Date Created	Date Modified
MIB	Directory	2021-05-13 13:05:40	2021-05-13 13:05:43
FMG_1000F-v6-build1435-FORTINET.out	139,912	2021-05-13 13:05:03	2021-05-13 13:05:08 HTTPS Checksum
FMG_2000E-v6-build1435-FORTINET.out	141,033	2021-05-13 13:05:48	2021-05-13 13:05:55 HTTPS Checksum
FMG_200D-v6-build1435-FORTINET.out	139,255	2021-05-13 13:05:01	2021-05-13 13:05:06 HTTPS Checksum
FMG_200F-v6-build1435-FORTINET.out	139,578	2021-05-13 13:05:14	2021-05-13 13:05:19 HTTPS Checksum
FMG_3000F-v6-build1435-FORTINET.out	141,270	2021-05-13 13:05:56	2021-05-13 13:05:03 HTTPS Checksum

Ilustración 3. Registro del producto (III).

- Para verificar la integridad del *software* descargado, realizar el hash SHA-512 del fichero y verificar que corresponde con el indicado en la página de descarga, bajo *Get Checksum Code*:

Get Checksum Code

Image File Name: FMG_1000F-v6-build1435-FORTINET.out

MD5 Checksum Code: c8206322fd8b88ed0d90c04fbd3b049e

SHA-512 Checksum Code: 6efdef7e846aaf8d038b711459cf274fe1010116cc69a4ecb6ff9a21e39c17cc3c1418fce8cb0cd8ad8e5b2493ba6a6e32228bd0a7f88b699c99b68b668cadb7

OK

Ilustración 4. Verificación del Hash.

- Por último, seguir los pasos indicados en el apartado *Upgrading FortiManager* de la guía *Upgrade Guide – REF2*.
- Durante el arranque inicial del producto, se recomienda llevar a cabo las instrucciones contenidas en el apartado *Setting up FortiManager* de la guía *Administration Guide – REF1*.
 - El detalle de la instalación de la versión 6.2.8 de FortiManager se puede consultar en el siguiente enlace:
 - Actualizar FortiManager a 6.2.8:
<https://docs.fortinet.com/document/fortimanager/6.2.8/upgrade-guide/427568/introduction>

5. FASE DE CONFIGURACIÓN

5.1 MODO DE OPERACIÓN SEGURO

16. El producto requiere de la configuración del token de entropía *Araneus Alea II*. Este se emplea para la generación segura de claves, así como fuente confiable de valores aleatorios. Adicionalmente, se debe activar el modo de operación seguro.
17. Para llevar a cabo la instalación del token, este se debe conectar a un puerto USB disponible del producto. Una vez conectado, **se deben introducir los siguientes comandos mediante consola, que servirán para configurar el token y activar el modo seguro simultáneamente:**

```
config system fips
    set status enable
    set entropy-token enable
end
```

18. Una vez introducidos los comandos, el dispositivo solicitará la contraseña de administrador. Aceptar los cambios e introducir el comando *get system status* para verificar que el modo seguro ha sido activado. Para ello se deberá observar la siguiente línea: *FIPS mode: enabled*.
19. Se recomienda configurar el periodo de *re-seed* en 60 minutos, ya que por defecto es cada 24 horas. Para ello:

```
config system fips
    set re-seed-interval 60
end
```

5.1.1 CIFRADO DE DATOS

20. **Se deberá habilitar el cifrado de datos y cargar una clave para llevarlo a cabo.** Este cifrado afectará a los Parámetros de Seguridad Críticos. Para ello, emplear los siguientes comandos mediante la consola:

```
config system global
    set private-data-encryption enable
end
```

21. Una vez habilitado el cifrado de datos, el producto solicitará al administrador una clave AES de 128 bits, la cual será empleada para llevar a cabo el cifrado.

5.2 AUTENTICACIÓN

22. Desde la consola web de administración es posible monitorizar los diferentes usuarios de administración que se encuentren conectados en cada momento a FortiManager, siendo posible desconectar a dichos usuarios en caso necesario. Se muestra tanto la dirección IP del usuario de administración y el tipo de acceso (GUI, CLI), como la fecha y hora de la conexión.

23. Dicha monitorización se realiza desde *Systems Settings > Dashboard*, dentro del widget de *System information*, hacer clic en el icono de lista junto a *Current Administrators*.
24. El producto requiere la autenticación de usuarios para la gestión. Los mecanismos de autenticación empleados por el producto son los siguientes:
- Credenciales locales, mediante usuario y contraseña. Dichas credenciales se almacenan en el producto. Para la creación y gestión de usuarios locales, ver el apartado [5.4.2 CONFIGURACIÓN DE ADMINISTRADORES](#).
 - Servidor de autenticación externo. Mediante la integración con distintos servidores de autenticación. Para la configuración de dichos servidores, ver apartado [5.3 SERVIDORES DE AUTENTICACIÓN EXTERNOS](#).
25. Se recomienda **emplear únicamente la autenticación local** como método de autenticación de usuarios.

5.3 SERVIDORES DE AUTENTICACIÓN EXTERNOS

26. En caso de requerir la configuración de un servidor externo de autenticación, consultar el apartado *Authentication* de la guía *Administration Guide – REF1*.
27. Para servidores LDAP, se deberá habilitar *secure connection* y seleccionar el protocolo LDAPS o STARTTLS.

5.4 ADMINISTRACIÓN DEL PRODUCTO

5.4.1 ADMINISTRACIÓN LOCAL Y REMOTA

28. El producto dispone de las siguientes interfaces para la administración:
- Administración local por consola.
 - Administración remota de tipo CLI mediante SSH. En la versión 6.2.8 ya no es posible asociar telnet como acceso administrativo al interfaz.
 - Administración remota de tipo GUI mediante HTTPS. Este tipo de administración se encuentra deshabilitada por defecto, por lo que deberá habilitarse durante la configuración del producto, consultar apartado [5.5 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS](#). Se deberá configurar también el producto para forzar el empleo de TLS versión 1.2 o superiores, para ello consultar el apartado [5.6 CONFIGURACIÓN DE PROTOCOLOS SEGUROS](#).
29. **Se deberá habilitar la redirección de HTTP a HTTPS para evitar el empleo de HTTP considerado inseguro.** Para ello, en la interfaz GUI, desde *admin > admin settings* modificar los puertos habituales de gestión, marcando siempre *Redirects to HTTPS*.

Admin Settings		
Administration Settings		
HTTP Port	80	<input checked="" type="checkbox"/> Redirects to HTTPS
HTTPS Port	443	
HTTPS & Web Service Certificate	server.crt	
Idle Timeout	3600	(60-28800 Seconds)
Idle Timeout (API)	900	(1-28800 Seconds)
Idle Timeout (GUI)	3600	(60-28800 Seconds)

Ilustración 5. Configuración de HTTPS.

5.4.2 CONFIGURACIÓN DE ADMINISTRADORES

30. El detalle de configuración de administradores se puede consultar en el apartado *Administrators* de la guía *Administration Guide – REF1*.
31. Para crear un nuevo usuario, ir a *System Settings > Admin > Administrators* y seleccionar *Create New*. El parámetro *Admin Type* se deberá configurar con el valor *Local*. Seleccionar la casilla *Force this administrator to change password upon next login*, de tal forma que deba modificar su contraseña en el primer acceso.
32. Los privilegios de acceso de los administradores se definen a través de un perfil de administración. Por defecto el sistema proporciona cinco (5) perfiles de acceso con diferentes niveles de acceso:
 - *Restricted_user*: Los perfiles de usuario restringidos no tienen privilegios del sistema habilitados y tienen acceso de solo lectura para todos los privilegios del dispositivo.
 - *Standard_user*: Los perfiles de usuario estándar no tienen habilitados los privilegios del sistema, pero tienen acceso de lectura/escritura para todos los privilegios del dispositivo.
 - *Super_user*: Los perfiles de superusuario tienen habilitados todos los privilegios del sistema y del dispositivo.
 - *Package_user*: El perfil de usuario del paquete tiene paquetes de política de lectura/escritura y privilegios de objetos habilitados, y tiene acceso de solo lectura para el sistema y otros privilegios.
 - *No_Permission_user*: Los perfiles de usuario sin permisos no tienen privilegios de sistema o dispositivo habilitados.
33. Adicionalmente se pueden crear perfiles de administración nuevos, en los que se pueden determinar los permisos específicos. Para ello ir a *System settings > Admin > Profile* y seleccionar *Create new*.

5.4.3 PARÁMETROS DE SEGURIDAD

34. Se deberá establecer un tiempo de inactividad, tras el cual se después del cual se desconecte a los usuarios. Para ello, desde *Admin > Admin Settings*, configurar los distintos parámetros *Idle Timeout* en un valor de cinco minutos (300 segundos).
35. El producto permite limitar el acceso de los usuarios administradores desde uno o varios dispositivos únicamente. Para ello ir a *Admin > Administrator > (usuario)*.
36. Se debe configurar una política de contraseñas segura. Para ello ir a *Admin > Admin Settings > Password Policy* y configurar los siguientes parámetros:
- Activar la casilla *Password Policy*.
 - *Minimum Length*: establecer un valor de doce (12) caracteres de longitud mínimo.
 - *Must Contain*: activar todas las casillas para forzar el empleo de, al menos, una letra mayúscula, una minúscula, un número y un carácter especial.
 - *Admin Password Expires after*: establecer un valor de 60 días, tras el cual se deberá modificar la contraseña de usuario.
37. Adicionalmente el administrador del sistema **deberá exigir a los usuarios la siguiente política de contraseñas de manera procedural**:
- No reutilizar las últimas 5 contraseñas.
 - No permitir un nuevo cambio de contraseñas antes de pasados 10 días.
38. Se debe configurar el bloqueo de cuentas de usuarios tras tres intentos fallidos de acceso, durante cinco minutos. Para ello, emplear los siguientes comandos:

```
config system global
set admin-lockout-threshold 3
set admin-lockout-duration 300
end
```

5.4.4 CONFIGURACIÓN DEL BANNER DE ACCESO

39. **Se debe configurar el mensaje de aviso antes de la autenticación en el producto.** Para ello, primero debe habilitarse empleando los siguientes comandos mediante consola:

```
config system global
set pre-login-banner enable
end
```

40. Una vez habilitado, se puede modificar el mensaje que se muestra empleando los siguientes comandos:

```
config system global
set pre-login-banner-message <mensaje>
end
```

5.5 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

41. Por defecto, el acceso remoto a la plataforma se encuentra desactivado. Por ello, se deberá habilitar el acceso remoto mediante HTTPS. Para ello, se puede configurar la interfaz *port1* para permitir el acceso mediante HTTPS y SSH, por ejemplo:

```
config system interface
    edit port1
        set allowaccess https ssh
    end
```

42. Posteriormente, desde la interfaz GUI, es posible configurar todas las interfaces. **Se recomienda deshabilitar todas aquellas que no vayan a emplearse.** Para aquellas en uso, se deben limitar los protocolos a *HTTPS*, *SSH* y *Web Service*.

5.6 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

43. Se deberá configurar el grupo *Diffie-Hellman* empleado por el producto empleando los siguientes comandos. El producto dispone de distintas opciones, **se recomienda emplear 3072 bits.**

```
config sytem global
    set dh-params 3072
end
```

44. El producto emplea únicamente SSHv2 por defecto.

45. Se deberá configurar el producto para emplear únicamente algoritmos y versiones de TLS seguras. Para ello emplear los siguientes comandos:

```
config system global
    set fgfm-ssl-protocol [tlsv1.2 or tlsv1.3]
    set oftp-ssl-protocol [tlsv1.2 or tlsv1.3]
    set ssl-protocol [tlsv1.2 or tlsv1.3]
    set webservice-proto [tlsv1.2 or tlsv1.3]
    set ssl-low-encryption disable
end
```

```
config fmupdate fds-setting
    set fds-ssl-protocol [tlsv1.2 or tlsv1.3]
end
```

5.7 GESTIÓN DE CERTIFICADOS

46. El detalle de configuración de los certificados se puede consultar en el apartado *Certificates* de la guía *Administration Guide – REF1*. El producto emplea un único certificado de servidor para las comunicaciones de la interfaz GUI a través de HTTPS y con el servidor externo de auditoría a través de TLS.

47. Deberán seguirse los siguientes pasos generales:

- Importar el certificado de la CA que se utilizará para generar el certificado de servidor. Deberá incluir las extensiones *Basic Constraint X509* y *CRLSign* con valor *True*.
- Crear un CSR (*Certificate Signing Request*). **Se deberá utilizar uno de los siguientes parámetros para la creación del certificado:**
 - Tipo de clave ECDSA, con un tamaño de 256 bits o superior.
- Importar el certificado de servidor una vez recibido.
- Se recomienda configurar la lista de revocación de certificados (CRL) correspondiente, para permitir al producto verificar el estado de los certificados.

5.8 SINCRONIZACIÓN HORARIA

48. **Se recomienda que todos los sistemas utilizados por la organización se encuentren sincronizados** para permitir una alta fiabilidad en los sistemas de auditoría y *logging*.

49. Se deberá deshabilitar el protocolo NTP de sincronización horaria debido a que no permite el uso de claves de autenticación. Para ello, emplear los siguientes comandos:

```
config system ntp
    set status disable
end
```

50. Por lo tanto, **se recomienda emplear la hora local del dispositivo**. Para ello, ir a *System Settings > Dashboard* y pulsar sobre el icono de *System Information* y después sobre el botón de editar al lado de *System time*. Finalmente configurar los valores de *Time Zone* y *Set Time*.

5.9 ACTUALIZACIONES

51. El producto permite la actualización manual del *Firmware* desde un fichero descargado en el dispositivo del administrador o directamente desde el servicio de conexión segura *FortiGuard* de Fortinet. El detalle sobre el proceso de actualización se puede consultar en la guía *Upgrade Guide – REF2*.

52. Una vez descargado el paquete de *firmware*, **se debe verificar la integridad del paquete de firmware descargado mediante su hash SHA-512**. Este debe coincidir con el mostrado en la página de descarga.

5.10 AUTO-CHEQUEOS

53. El producto dispone de una serie de pruebas, durante el arranque o bajo ciertas condiciones, que verifican el correcto funcionamiento de los algoritmos criptográficos y la integridad del firmware.

54. Adicionalmente, un usuario administrador puede ejecutar dichos test manualmente en cualquier momento. Para ejecutar todas las pruebas, emplear el comando *execute fips kat all*. En caso de desear ejecutar solo una prueba específica, *execute fips kat <test_name>*.
55. En caso de fallar alguno de los chequeos de algoritmos criptográficos, el dispositivo procederá a apagarse, impidiendo así su uso. En caso de entrar en modo de *error*, el producto entrará en un modo seguro que no permitirá el paso de datos.

5.11 ALTA DISPONIBILIDAD

56. Es posible configurar un clúster de hasta cinco dispositivos FortiManager del mismo modelo. Uno de los equipos actúa como primario o master del clúster y los demás actúan de reserva. Todos los equipos son visibles en la red. Los integrantes del clúster pueden estar en la misma red o en redes geográficamente separadas, siempre y cuando exista comunicación entre ellos.
57. El administrador se conectará siempre al nodo que este como master. Desde *System Settings > HA* se puede monitorizar el estado de las unidades que forman un clúster.
58. El detalle de configuración en alta disponibilidad se puede consultar en el apartado *High Availability* de la guía *Administration Guide – REF1*.

5.12 AUDITORÍA

5.12.1 REGISTRO DE EVENTOS

59. El producto genera registros de auditoría para las distintas acciones realizadas por los usuarios. Estos están almacenados en la memoria o en el disco duro interno y se pueden consultar desde *System Settings > Event Log*.

Add Filter		Last 1 Day May 28 To May 29		Download Raw Log Historical Log		
#	Date Time	Level	User	Sub Type	Description	Message
1	2018-05-29 14:20:18	notice	admin-GUI(172.18.26.1)	System manager event	CLI execution info	path=system.log-fetch.clien mP34AgCu6bvsx64BD8OF //otJysxG1cKhWj5f7mPjIm
2	2018-05-29 14:08:31	information	system	FortiAnalyzer system event	Configuration database object changed	[create] configuration datab
3	2018-05-29 13:36:14	notice	admin-GUI(172.18.26.1)	Device manager event	Device Manager dvm log at notice level	Edited device FG-152 (FGV
4	2018-05-29 13:33:26	notice	admin-GUI(172.18.26.1)	Device manager event	Device Manager dvm log at notice level	Edited device FG-152 (FGV
5	2018-05-29 13:33:15	information	admin	Device manager event	Device manager generic information log	Device FG-152 add succeec
6	2018-05-29 13:33:14	notice	admin-GUI(172.18.26.1)	Device manager event	Device Manager dvm log at notice level	Added device FG-152 (FGV

Ilustración 6. Registros de auditoría

60. Desde *System Settings > Advanced > File Management*, se pueden configurar los periodos de retención de los registros de auditoría.
61. El detalle de configuración de los registros de auditoría se puede consultar en el apartado *Event Log* de la guía *Administration Guide – REF1*.

62. El producto permite el envío de los registros de auditoría a un servidor externo mediante Syslog. Sin embargo, dicho envío se realiza en claro por lo que, **en caso de emplearse, deberá situarse el servidor al que se envíen los registros en la misma red local que el producto.**
63. Para configurar el envío de registros a un servidor de auditoría externo, ir a *System Settings > Advanced > Syslog Server* e introducir los datos del servidor al que se desea realizar el envío de registros. Por último, se deberán emplear los siguientes comandos para habilitar el envío de registros a dicho servidor:

```
config system locallog syslogd setting
    set severity information
    set status enable
    set syslog-name <syslog server name>
end
```

5.13 COPIAS DE SEGURIDAD

64. **Se recomienda realizar copias de seguridad periódicas de la configuración del producto** para, en caso de ser necesario, poder recuperar el estado de la máquina. Para ello es posible crear copias de seguridad locales. Será recomendable llevar copias de seguridad a cabo tras un cambio de configuración relevante.
65. Dichas copias pueden llevarse a cabo manualmente o con una periodicidad programada. Para hacer una copia de seguridad de la configuración de FortiManager, ir a *System Settings > System Information (widget) > Backup*. Activar la casilla *Encryption* para almacenar las copias cifradas e introducir la contraseña deseada:
66. En caso de necesitar restaurar el sistema a partir de una copia de seguridad, ir a *System Settings > Dashboard > System Information (widget)*. Pulsar sobre el botón de restauración, próximo a *System Configuration* y seleccionar el archivo de copia de seguridad que se desea restaurar.

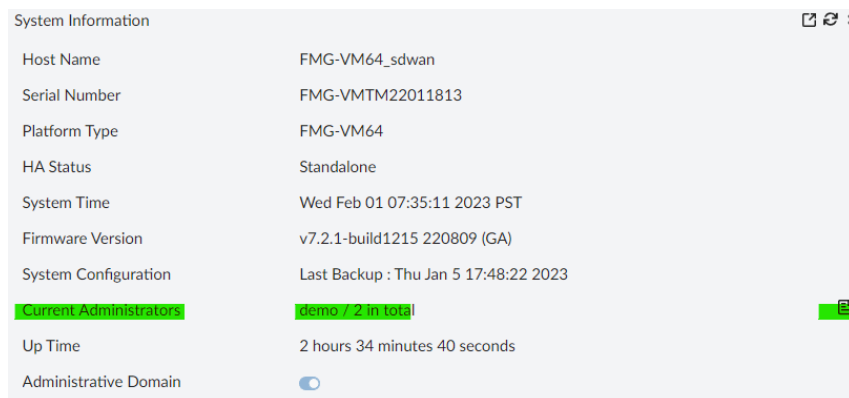
5.14 FUNCIONES DE SEGURIDAD

67. El producto permite la creación de dominios administrativos (ADOMs), empleados para agrupar los productos gestionados y permitir una gestión más simple y centralizada, pudiendo modificar todos los dispositivos de un dominio simultáneamente.
68. El detalle de configuración de los dominios se puede consultar en el apartado *Administrative domains* de la guía *Administrative Guide – REF1*.

6. FASE DE OPERACIÓN

69. Durante la fase de operación del producto, el administrador debe llevar a cabo las siguientes tareas de mantenimiento:

- Se debe verificar regularmente la existencia de nuevo *firmware* para mantenerlo actualizado.
- En caso de conexión de múltiples administradores de forma simultánea se debe verificar identidad de dichos administradores:



The screenshot shows the 'System Information' page in FortiManager. The 'Current Administrators' row is highlighted in green, showing 'demo / 2 in total'. The 'Administrative Domain' is also highlighted in green and has a toggle switch.

System Information	
Host Name	FMG-VM64_sdwan
Serial Number	FMG-VM64_22011813
Platform Type	FMG-VM64
HA Status	Standalone
System Time	Wed Feb 01 07:35:11 2023 PST
Firmware Version	v7.2.1-build1215 220809 (GA)
System Configuration	Last Backup : Thu Jan 5 17:48:22 2023
Current Administrators	demo / 2 in total
Up Time	2 hours 34 minutes 40 seconds
Administrative Domain	<input checked="" type="checkbox"/>

Ilustración 7. Conexiones de administradores

- Comprobaciones periódicas del *hardware* y *software* para asegurar que no se ha introducido hardware o software no autorizado.
- Mantenimiento de los registros de auditoría.

7. CHECKLIST

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la integridad de la descarga	<input type="checkbox"/>	<input type="checkbox"/>	
Registro de licencias	<input type="checkbox"/>	<input type="checkbox"/>	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Activación del modo seguro	<input type="checkbox"/>	<input type="checkbox"/>	
Configuración del cifrado de disco	<input type="checkbox"/>	<input type="checkbox"/>	
ADMINISTRACIÓN DEL PRODUCTO			
Configuración de roles y usuarios	<input type="checkbox"/>	<input type="checkbox"/>	
Configuración de la política de contraseñas	<input type="checkbox"/>	<input type="checkbox"/>	
Configuración de los parámetros de sesión	<input type="checkbox"/>	<input type="checkbox"/>	
CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS			
Deshabilitar las interfaces y servicios no empleados	<input type="checkbox"/>	<input type="checkbox"/>	
CONFIGURACIÓN DE PROTOCOLOS SEGUROS			
Configuración de TLSv1.2	<input type="checkbox"/>	<input type="checkbox"/>	
Configuración de SSHv2	<input type="checkbox"/>	<input type="checkbox"/>	
GESTIÓN DE CERTIFICADOS			
Importar CA, crear CSR e importar el certificado de servidor	<input type="checkbox"/>	<input type="checkbox"/>	
COPIAS DE SEGURIDAD			
Creación de los backups	<input type="checkbox"/>	<input type="checkbox"/>	
AUDITORÍA			
Configuración del envío de los logs a un servidor Syslog	<input type="checkbox"/>	<input type="checkbox"/>	

8. REFERENCIAS

70. El enlace principal de guías del producto contiene acceso a toda la documentación:
<https://docs.fortinet.com/product/fortimanager/6.2>

REF1 *Administration Guide*

<https://docs.fortinet.com/document/fortimanager/6.2.8/administration-guide>

REF2 *Upgrade Guide*

<https://docs.fortinet.com/document/fortimanager/6.2.8/upgrade-guide/427568/introduction>

9. ABREVIATURAS

ADOM	<i>Administrative Domain (Dominios Administrativos)</i>
API	<i>Application Programming Interface</i>
CCN	Centro Criptológico Nacional
CLI	<i>Command Line Interface</i>
CPD	Centro de Proceso de Datos
CPSTIC	Catálogo de Productos y Servicios TIC
CRL	<i>Certificate Revocation List</i>
ENS	Esquema Nacional de Seguridad.
FMG	<i>FortiManager</i>
GUI	<i>Graphical User Interface</i>
HA	<i>High Availability</i>
HTTPS	<i>Hypertext Transfer Protocol Secure</i>
NTP	<i>Network Time Protocol</i>
SMTP	<i>Simple Mail Transfer Protocol</i>
SSH	<i>Secure Shell</i>
TLS	<i>Transport Layer Security</i>
URL	<i>Uniform Resource Locator</i>
VM	<i>Virtual Machine</i>
VPN	<i>Virtual Private Network</i>

