centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1227

Procedimiento de Empleo Seguro
Deep Discovery Inspector

Febrero 2024

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

Pº de la Castellana 109, 28046 Madrid

CCN 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
2024.03.01 11:19:15 +01'00'

NIPO: 083-24-099-7.
Fecha de Edición: febrero de 2024

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. Deep Discovery Inspector es una sonda de red anti-APT diseñada para detectar de manera temprana ciberataques en el vector de red (ej.: malware de día 0, movimientos laterales, comunicaciones C&C, exfiltración de datos, explotación de vulnerabilidades etc.).
2. La detección la realiza combinando técnicas de Reputación, *Machine Learning* y *Sandboxing*.
3. Está disponible en formato *appliance* físico o virtual, con distintos niveles de escalado de ancho de banda y configuración de puertos, facilita su implementación en redes con distintos niveles de complejidad.
4. Se puede integrar con la plataforma *XDR Trend Vision One*, que aporta telemetría y detecciones, conforma la plataforma NDR perfecta para hacer frente a los complejos ataques recibidos por el cibercrimen moderno.

2. OBJETO Y ALCANCE

6. Esta guía ha sido elaborada para el producto Deep Discovery Inspector, tanto en formato hardware como virtual en su versión 6.5 y subversiones contenidas dentro de la misma.

7. **Este producto ha sido cualificado e incluido en el Catálogo de Producto y Servicios de Seguridad TIC (CPSTIC), para categoría MEDIA, en las familias "IDS, IPS y AntiDDoS" y "Herramientas de Sandbox".**

3. ORGANIZACIÓN DEL DOCUMENTO

8. El documento está formado de 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 referencias de la documentación mencionada a lo largo del documento.

   e) Apartado **8**. En este apartado se recogen las abreviaturas utilizadas.

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

9. Para asegurarse que el producto no ha sido modificado durante su transporte, realizar las siguientes revisiones.
10. Revisión Exterior:
    - Comprobar que el embalaje exterior está en buenas condiciones.
    - Comprobar la cinta de embalar y etiquetas del embalaje de cartón exterior.
11. Revisión de contenido:
    - La caja del dispositivo debe contener una pegatina con los datos del producto, modelo y número de serie, de igual forma.
    - El dispositivo debe tener el logotipo de Trend Micro además de una pegatina con el mismo número de serie y modelo.
12. Comprobación y descarga en formato virtual:
    - En caso de que el producto se haya adquirido en formato virtual para su instalación (formato OVA de máquina virtual) este se debe descargar desde el portal de cliente Trend Micro:
    - URL del portal. https://success.trendmicro.com/dcx/s/dashboard
    - Menu del portal (xxx -> xxx -> xxx).Productos/ Deep Discovery Inspector:

    - Se comprobará la validez de los certificados del portal para asegurar la autenticidad del software descargado.

4.2 ENTORNO DE INSTALACIÓN SEGURO

13. La solución de Deep Discovery es un producto que debe instalarse en un Centro de Proceso de Datos (CPD), cuyo acceso estará limitado a un conjunto de personas que posean una autorización expresa.
14. Se recomienda que los puertos de comunicación del producto (descritos más adelante) estén limitados a recibir conexiones desde los entornos de gestión.
15. La sonda de red necesita conexión a internet hacia el dominio de Trend Micro para la actualización de patrones y comportamientos.
16. La sonda de red dispone de *sandbox* virtual para el tráfico de red, también se dispone de *appliance* dedicado para *sandboxing*. Dicha *sandbox* requiere de conexión a internet de forma aislada para la ejecución de malware (Línea sucia).

4.3 REGISTRO Y LICENCIAS

17. Durante el proceso de compra de licencias, el cliente recibirá un certificado de licenciamiento donde se listarán las claves de registro asociadas al producto.

18. A continuación, se adjunta un ejemplo de certificado:

> ¡¡LEA CON ATENCIÓN!!
>
> 1. Si una de las líneas de la licencia incluye solamente una Clave de Registro en el formato XX-XXXX-XXXX-XXXX-XXXX, tiene que registrar esta clave en https://clp.trendmicro.com/FullRegistration?T=TM
> conseguir un Código de Activación.
> Para registrar Smart Protection Suite, diríjase a: https://success.trendmicro.com/technical-support
> 2. En cambio, si una de las líneas de la licencia incluye una Clave de Registro y también un Código de Activación: XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX, no tiene que registrar la Clave de Registro, ya que la actualización será ejecutada de forma automática. Le rogamos que compruebe que la consola del producto incluya los detalles actualizados de esta licencia.
>
> Podría resultar necesaria una espera de 24 a 48 horas para que la información incluida en este certificado de licencia sea automáticamente actualizada en la consola del producto. Para comprobar que la información de la licencia está correctamente actualizada en su consola, siga por favor los siguientes pasos:
> Abra la Consola Web -> Preferencias/Administración -> Licencia del Producto, introduzca el Código de Activación y/o pulse en "Controlar Estado en Línea"/"Actualizar Información". 3. Para descargar la última versión de todos los productos de Trend Micro vaya a: https://downloadcenter.trendmicro.com/index.php?regs=emea
>
> Para más información visite nuestra amplia knowledge base: https://success.trendmicro.com/solution/0116326

4.4 CONSIDERACIONES PREVIAS

19. De cara a disponer de un rendimiento óptimo, se recomienda dimensionar correctamente el modelo de la sonda, acorde al *throughput* que se va a inspeccionar.

20. Se debe contemplar el espacio en RACK para la sonda de red. En el caso de ser todo virtual, no debe contemplarse espacio en RACK.

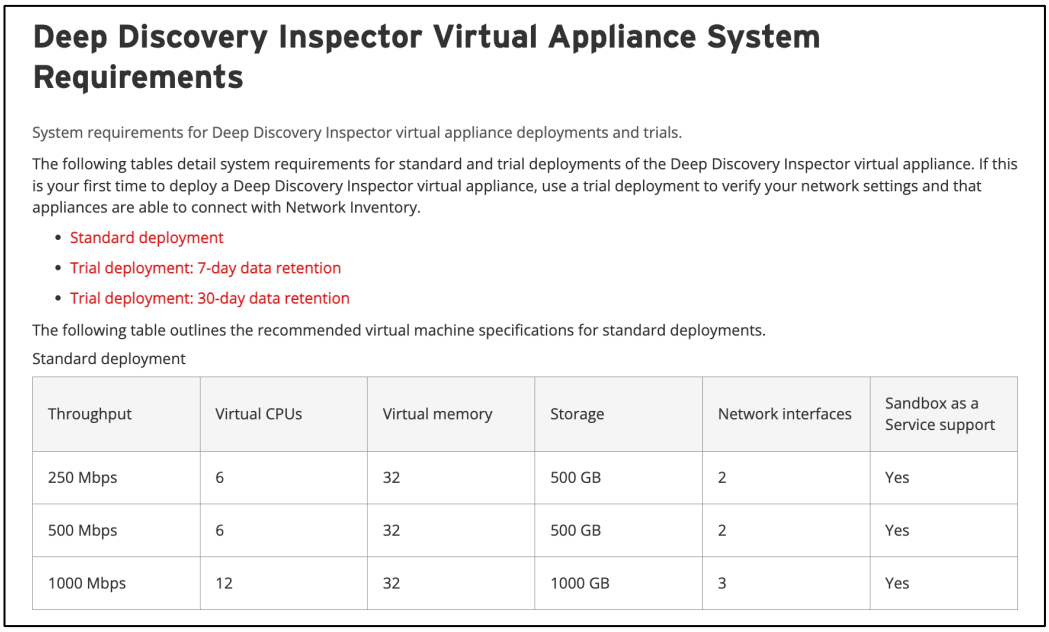
21. Se debe analizar el tráfico que se desea inspeccionar por parte de la sonda de red y realizar las configuraciones a nivel de electrónica de red (*switches*) para que estos realicen un *portmirror* (copia del tráfico) hacia la sonda. También esta soportado que la copia del tráfico lo realice un dispositivo TAP en vez de los switches.

22. Como se indica en apartados anteriores, es recomendable dotar al *sandbox* de una salida a internet dedicada y aislada para la ejecución de malware.

23. Se debe contemplar una imagen de S.O para incluirla a nivel de *sandbox* para la ejecución de malware. Dicha máquina virtual puede ser customizada para asemejarse al máximo posible al entorno de producción.

24. La sonda no requiere estar implementada en alta disponibilidad ya que se implementará en modo offline, aunque también permite implementarla de forma online, pero en este caso se debería contemplar alta disponibilidad o disponer de tarjetas en Bypass para no cortar tráfico en caso de caída de la sonda.

25. Si la sonda es en formato virtual se deben contemplar los siguientes requerimientos de *hardware*:



Deep Discovery Inspector Virtual Appliance System Requirements

System requirements for Deep Discovery Inspector virtual appliance deployments and trials.

The following tables detail system requirements for standard and trial deployments of the Deep Discovery Inspector virtual appliance. If this is your first time to deploy a Deep Discovery Inspector virtual appliance, use a trial deployment to verify your network settings and that appliances are able to connect with Network Inventory.

- Standard deployment
- Trial deployment: 7-day data retention
- Trial deployment: 30-day data retention

The following table outlines the recommended virtual machine specifications for standard deployments.

Standard deployment

Throughput	Virtual CPUs	Virtual memory	Storage	Network interfaces	Sandbox as a Service support
250 Mbps	6	32	500 GB	2	Yes
500 Mbps	6	32	500 GB	2	Yes
1000 Mbps	12	32	1000 GB	3	Yes

https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-virtual-deepdiscover

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

26. Autenticación: La sonda de red soporta autenticación basada en SAML, ADFS u Okta.
27. Notificaciones: SMTP para utilizar notificaciones vía correo electrónico.
28. Monitorización mediante SNMP V1 o V2, permitiendo *Traps* (Disparadores) y Consultas para monitorizar el estado de los servicios de la sonda. También soporta el envío de logs mediante SYSLOG en formato: CEF, LEEF y TMEF.
29. Gestión: La gestión de la sonda de red está integrada tanto en la sonda física o virtual. Dicha interface está basada en HTTPS y permite importar el certificado de la compañía que esté desplegando la solución.
30. Los puertos de conexión para realizar la gestión, monitorización, autenticación, notificación etc, se listan en la tabla que se encuentra a continuación. Para más información ver **[INS_DEP]** sección "*Ports used by appliance*".

PORT	SERVICE	FROM	TO	DESCRIPTION
DDI ports				
22/TCP	SSH	Client	DDI	CLI Management of DDI
25/TCP	SMTP	DDI	Email Server	Notificaciones
465/TCP	SMTPS	DDI	Email Server	Notificaciones cifradas SSL/TLS

PORT	SERVICE	FROM	TO	DESCRIPTION
587/TCP	SMTPS	DDI	Email Server	Notificaciones cifradas STARTTLS
53/TCP/UDP	Resolución DNS	DDI	Internal and external networs	Resolución DNS
514/UDP **6514/TCP** **8514/UDP**	SYSLOG SYSLOGS	DDI	Syglog Server	Envio de logs
67 y 68/UDP	DHCP	DDI	DHCP	Para configurar IP dinámica de management.
123/UDP	NTP	DDI	NTP Server	System time mediante NTP
137/UDP	Netbios	DDI	DC	Usa Netbios para convertir IPs en nombre de host.
161/UDP	DDI SNMP Agent	SNMP Server	DDI SNMP Agent	Consultas SNMP
162/UDP	DDI SNMP	SNMP Server	DDI SNMP Agent	Traps SNMP
389/TCP/UDP	DDI Autentication	DDI	LDAP Servers	Autenticacion
3268, 3269/TCP	DDI Autentication	DDI	LDAP Servers	Autenticacion
636/UDP	DDI Autentication	DDI	LDAP Servers	Autenticacion
443/TCP	Managment HTTPS	Client	DDI	Gestión.
4343/TCP	Smart protection server	DDI	SPS Server	Inteligencia de Trend Micro en local
5275/TCP	Smart protection Network SSL	DDI	SPS Server	Inteligencia de Trend Micro en cloud y SSL.

PORT	SERVICE	FROM	TO	DESCRIPTION
8080/TCP	Compartir inteligencia IOCs con terceros	Productos de terceros	DDI	Obtención de IOCs por parte de terceros hacia el DDI.

5. FASE DE INSTALACIÓN

31. En este apartado se documenta la instalación del *appliance* (versión *hardware*). En el caso de ser en formato virtual, se debe descargar la imagen en formato OVA desde el portal de cliente de Trend Micro (ver sección 4.1).

32. La instalación y despliegue del producto, está especificada en la sección "*Part II*" del documento **[INS_DEP]** para la versión Hardware y en la sección "*Part III*" del mismo documento para su versión virtual.

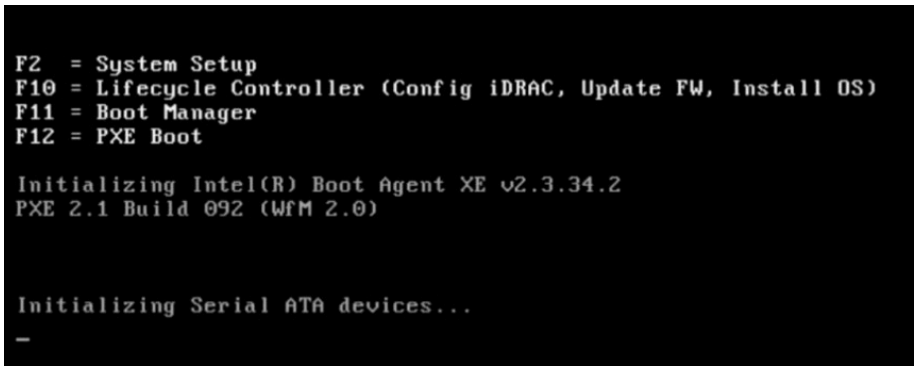
33. En el formato hardware, el *appliance* viene ya pre-configurado. Solo se debe realizar una actualización del software a la versión actual (ver sección 6.8).

34. Para realizar la instalación desde cero del *appliance*, se debe grabar la ISO en un DVD o descargar la imagen de recuperación desde el portal de cliente de Trend Micro.

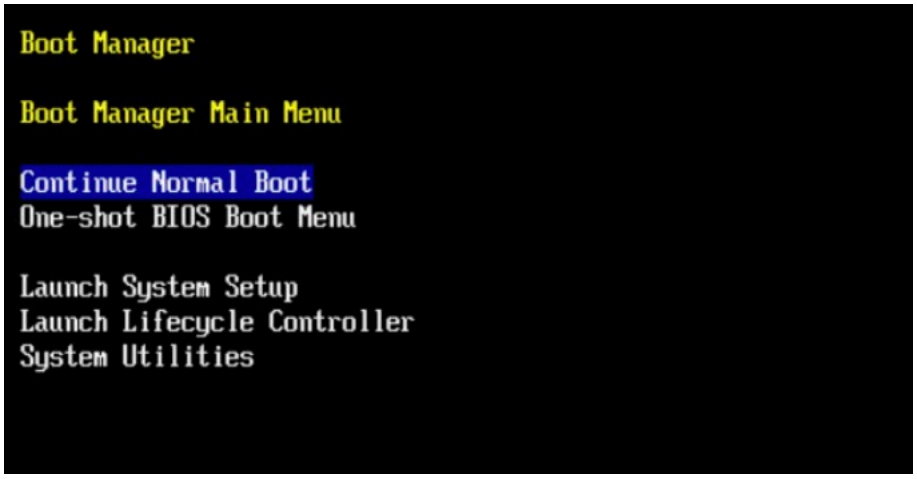
35. A continuación, se describe el proceso de instalación del firmware desde cero:

    a) Lo primero que se debe realizar es conectar una pantalla y teclado al *appliance*, una vez conectado procedemos a encender el *appliance*.

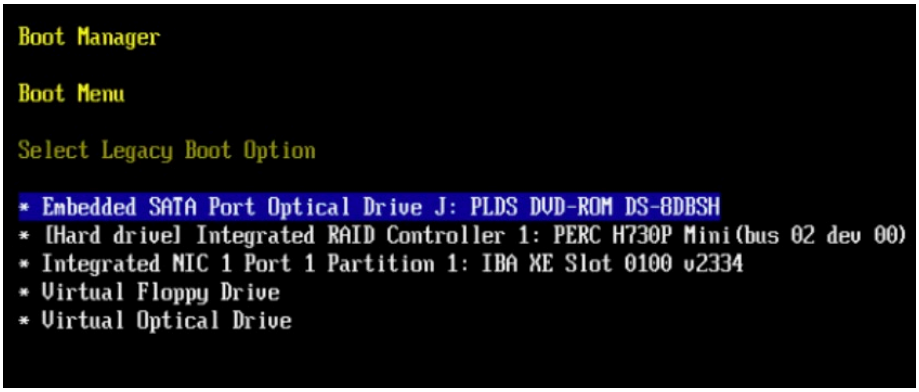
    b) Cuando aparezca la opción F11 debemos pulsarla para acceder a la BIOS.



    c) A continuación, se puede seleccionar "*Continue Normal Boot*" para arrancar de forma normal, pero para cambiar el arranque desde el disco se debe pulsar la opción de "*One-Shot BIOS Boot Menu*"



    d) En el menú de arranque debemos seleccionar el DVD del appliance para que arranque desde el disco:



e) Una vez arrancado desde el DVD, aparecerá el siguiente menú donde podemos seleccionar la instalación de Deep Discovery Inspector:

f) Una vez terminado el proceso de instalación, aparece el menú del DDI de Preconfiguración donde podemos configurar:

- IP Estática o dinámica, en caso de estática configurar la IP (IPv4 o IPv6),
- Default Gateway y rutas de red.
- DNS,
- Habilitar SSH.
- Configuración de interface: *Half/Full Duplex*, velocidad del Puerto…
- Pruebas de diagnóstico de resolución DNS, Ping, etc…

g) Por último, comprobamos el acceso vía GUI a la consola del DDI.

h) A partir de aquí, empieza la configuración del *appliance*.

6. FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

36. Seguir la guía de *best practices* de Deep Discovery Inspector para el cumplimiento de Common Criteria **[BESTP]**.

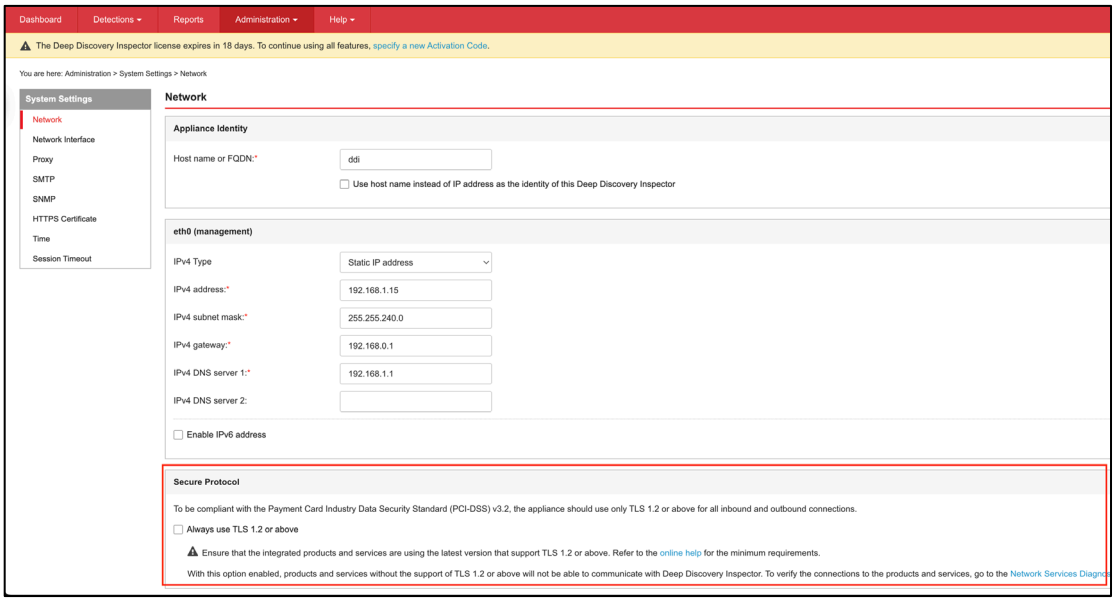
6.2 AUTENTICACIÓN

37. Deep Discovery Inspector soporta varios métodos de autenticación:
    - Local.
    - SAML (*Single Sign On*)
    - Mediante integración con *Active Directory*
38. En la sección "*Accounts*" del documento **[ADMIN]** se pueden encontrar las siguientes configuraciones de seguridad:
    - Los tipos de roles y los distintos permisos.
    - Como añadir cuentas locales.
    - Como añadir cuentas de *Active Directory*.
    - Como añadir cuentas de SAML.
39. A nivel de consola de administración permite modificar el certificado de la GUI HTTPS en formato X509 – PEM. La configuración se puede realizar siguiendo la sección "*Service Provider Metadata and Certificate"* en el manual **[ADMIN]**.

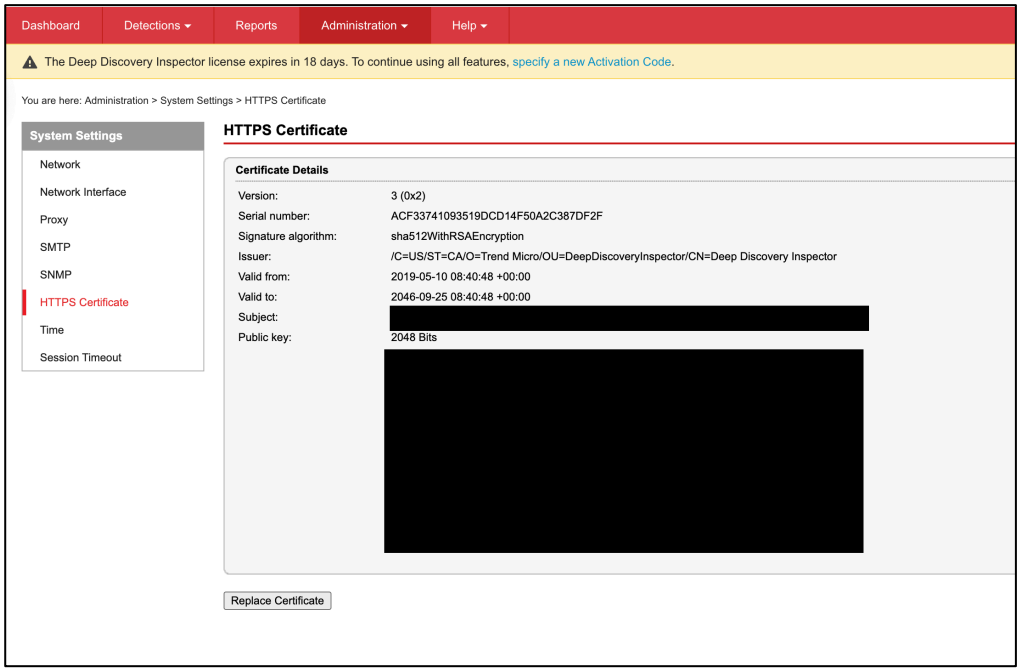
6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

40. El producto a nivel de gestión solo soporta HTTPS y SSH. Se requiere modificar el certificado y solo permitir TLS 1.2.
41. Para restringir la versión de TLS a 1.2 y superior se seguirán las instrucciones de la sección "*System Settings*" del manual **[ADMIN]**. A continuación, se muestra el interfaz de configuración de esta característica:



42. El procedimiento para generar e importar un certificado se encuentra descrito en la sección "*HTTPS Certificate*" del documento **[ADMIN]**. A continuación, se muestra el interfaz de configuración de esta característica:



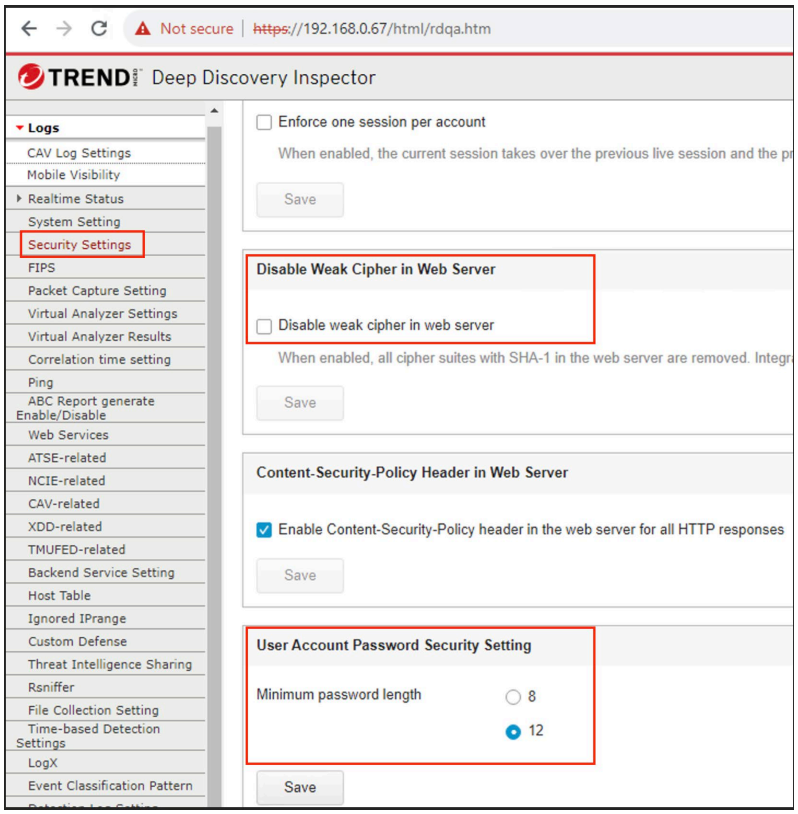
6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

43. Deep Discovery dispone de dos roles predefinidos, Administrado y Auditor (viewer o solo lectura)

44. Tener en cuenta los siguientes aspectos:

    - **Configuración de la Política segura de contraseñas**. Deberá cumplir con los siguientes requisitos mínimos:

- Longitud mínima de la contraseña: doce (12) caracteres. Se configura en interface avanzada RDQA. Para acceder a esta configuración acceder al interfaz web https://x.x.x.x/html/rdqa.htm de su producto.



- Requisitos de contraseñas no configurables (Deberá de hacerse de manera procedimental)
  - Composición de la contraseña: letras mayúsculas, letras minúsculas, números y símbolos especiales. Recomendar el uso de los cuatro (4) grupos si el producto lo permite, y al menos un mínimo de tres (3) grupos.
  - Número de contraseñas anteriores que no se permite utilizar: al menos, cinco (5).
  - Tiempo de validez en días de las contraseñas tras el cual expiran: sesenta (60) días.
  - Número de días que deben transcurrir tras el cambio de una contraseña antes de poder modificarla de nuevo: diez (10) días.

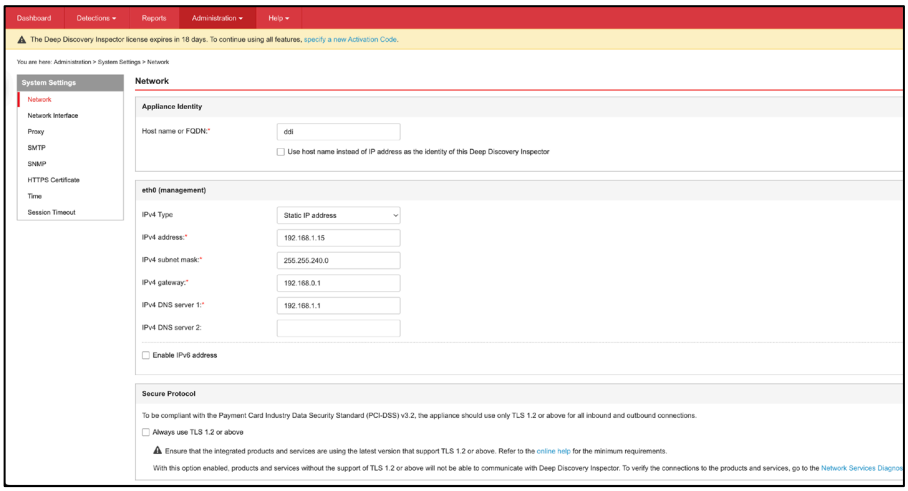
6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

45. Se recomienda dedicar una interface para gestión, otra para la línea sucia del *sandbox* y las correspondientes interfaces para realizar la ingesta de tráfico hacia la sonda, dicha copia de tráfico se puede realizar a nivel de *switch* mediante un *port mirror* o implementando un dispositivo en modo TAP.

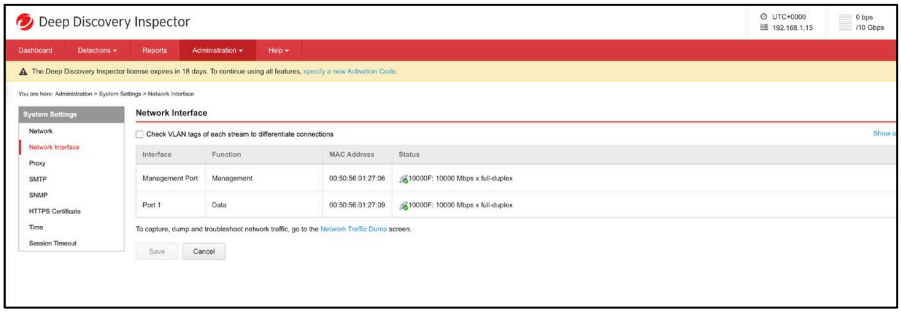
46. A continuación, se describe la configuración a realizar para cada una de las interfaces mencionadas:

a) Interface de *management* (Interfaz Web sección: Administración/*system settings/Network*):

Configuración IP, default Gateway, DNS y Seguridad TLS de la GUI: Se recomienda habilitar TLS 1.2



b) Interfaces de sniffer (Data) (*Interfaz Web sección: Administración/system settings/Network interface*) Desde el menú interfaces se puede modificar la función del interface y la velocidad de los puertos.



c) A nivel de configuración del sandbox interno del DDI, se debe configurar y dedicar una línea de salida a internet para la ejecución de malware, dicha interface esta separa a nivel de kernel. Para realizar dicha configuración se realiza desde el siguiente menú: *Administration/Virtual Analyzer/setup*.

d) Se debe configurar como sandbox interno y especificar la IP, DNS y Gateway de la interface.

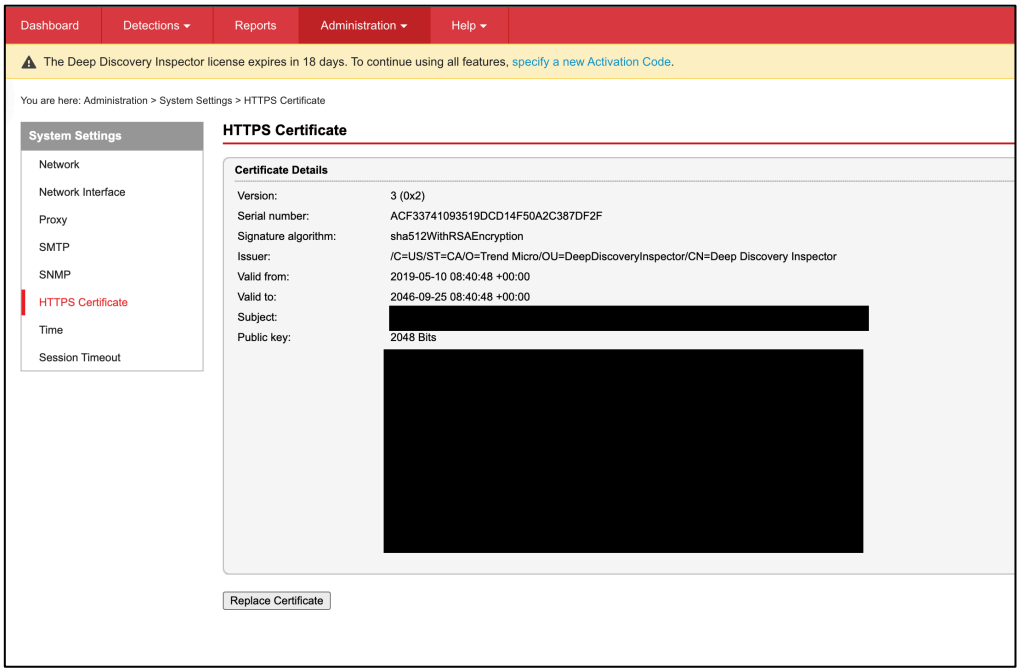
e) Se recomienda pulsar el botón para testear conectividad hacia internet desde las VMs.

47. Por ejemplo: deshabilitar los servicios no utilizados en el dispositivo, introducir una etiqueta que identifique el uso para el que está destinado cada interfaz, asociar a cada interfaz la dirección IP y MAC de la máquina conectada, etc. Para deshabilitar/habilitar servicios como el SSH, Servicio http para compartir inteligencia con terceros, excepciones… debe realizarse desde la interface avanzada de DDI, llamada RDQA (https://x.x.x.x/html/rdqa.htm)

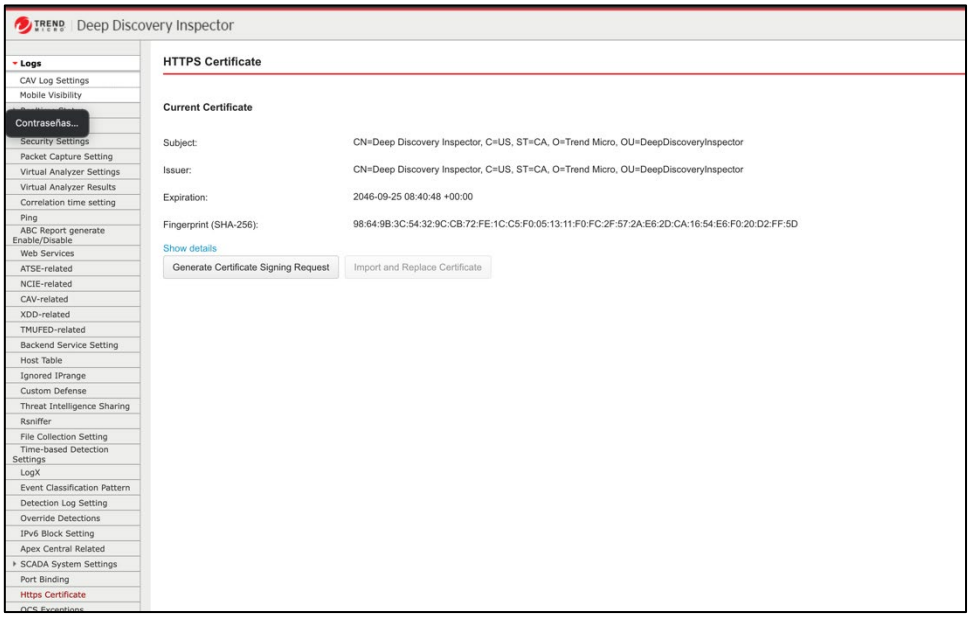
6.5 GESTIÓN DE CERTIFICADOS

48. Los certificados gestionables del DDI, se utilizan únicamente para la interface grafica mediante HTTPS. Se recomienda utilizar RSA con claves de al menos 3072 con función hash SHA 512.

49. Para realizar la configuración de los certificados, seguir las instrucciones del manual **[ADMIN]** en la sección "*System settings*".



Desde la interface avanzada RDQA descrita anteriormente, en la sección "*HTTPS Certificate*", permite generar un CSR para firmalo con una CA e importar el certificado ya firmado:



6.6 SERVIDORES DE AUTENTICACIÓN

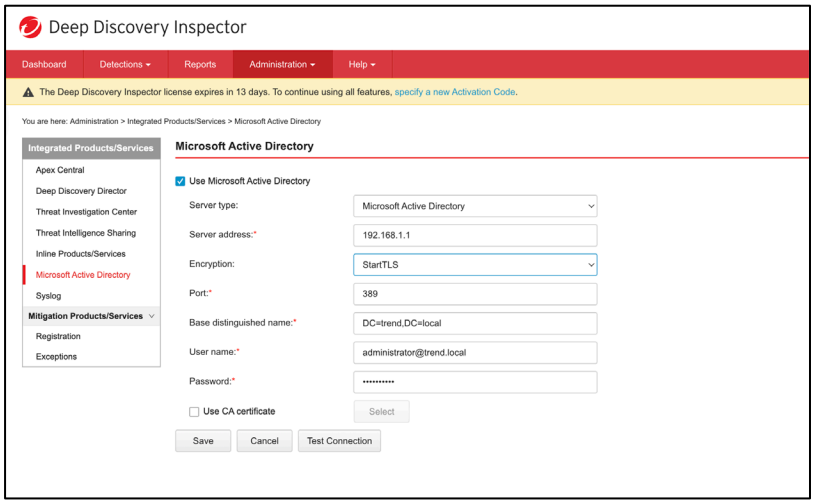
50. Deep Discovery soporta dos métodos de autenticación mediante Active Directory:

51. LDAP y LDAPS mediante SSL. Se recomienda habilitar TLS 1.2 a nivel de gestión para mejorar la seguridad y el cumplimiento de PCIDSS. A continuación, se adjunta la documentación para su configuración además de dos ejemplos de configuración tanto a nivel de LDAP y LDAPS:

52. Las configuraciones que se muestran a continuación están descritas en el manual **[ADMIN]**

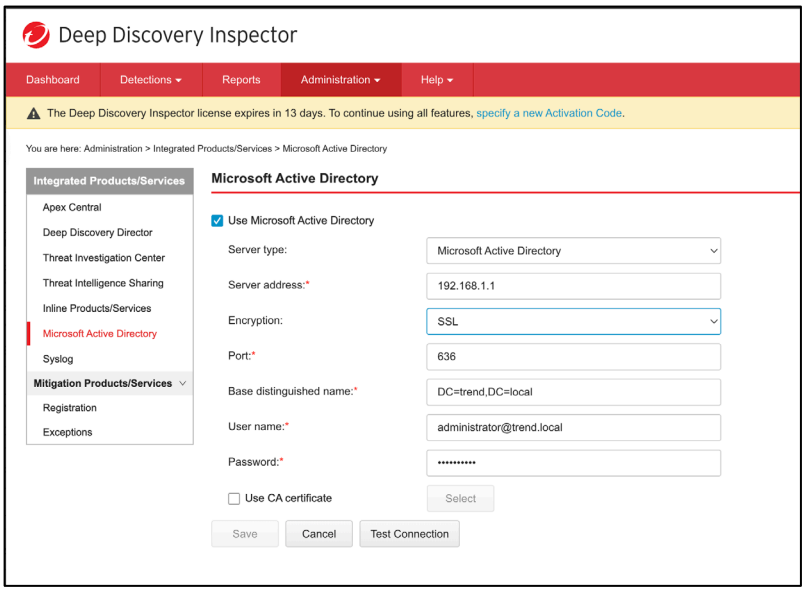
a) Autenticación AD StartTLS:

Administration/Integrated Products/Services/Microsoft Active Directory



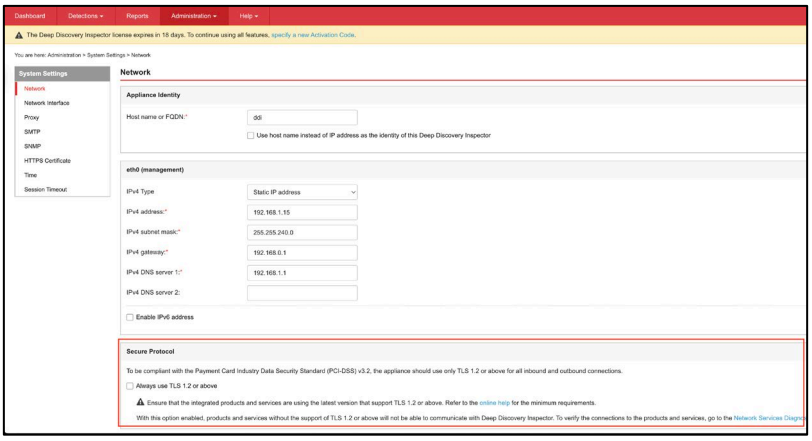
b) Autenticación AD SSL:

Administration/Integrated Products/Services/Microsoft Active Directory



c) Habilitar TLS 1.2:

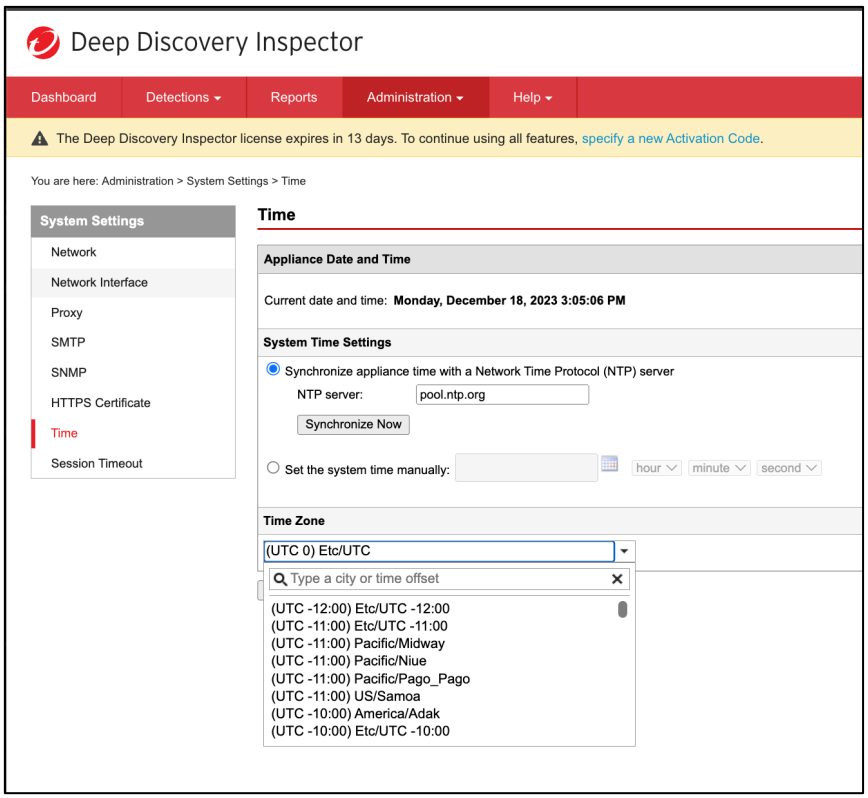
Administration/system settings/network



6.7 SINCRONIZACIÓN

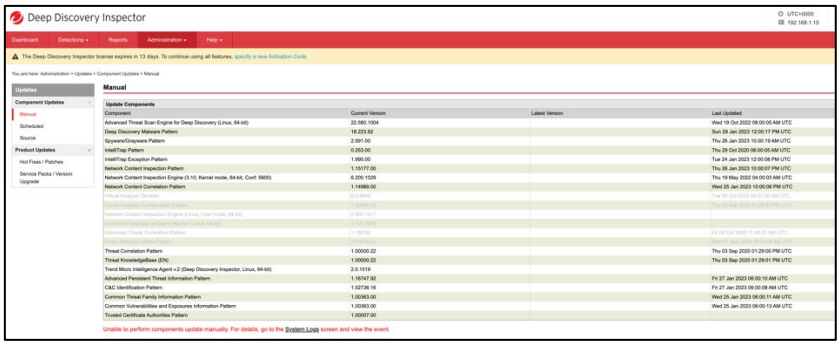
53. Deep Discovery Inspector soporta NTP, para sincronizar la hora del sistema. a continuación, la documentación que se puede consultar para la configuración es **[ADMIN]** en su sección "*Time*".

54. La solución permite asignar la hora del sistema de forma manual, pero se recomienda el uso de un NTP:



6.8 ACTUALIZACIONES

55. Deep Discovery inspector permite actualizar de forma programada los motores de seguridad, también permite revisar la versión de cada uno de los motores tanto a nivel de sonda como a nivel de *sandbox*:

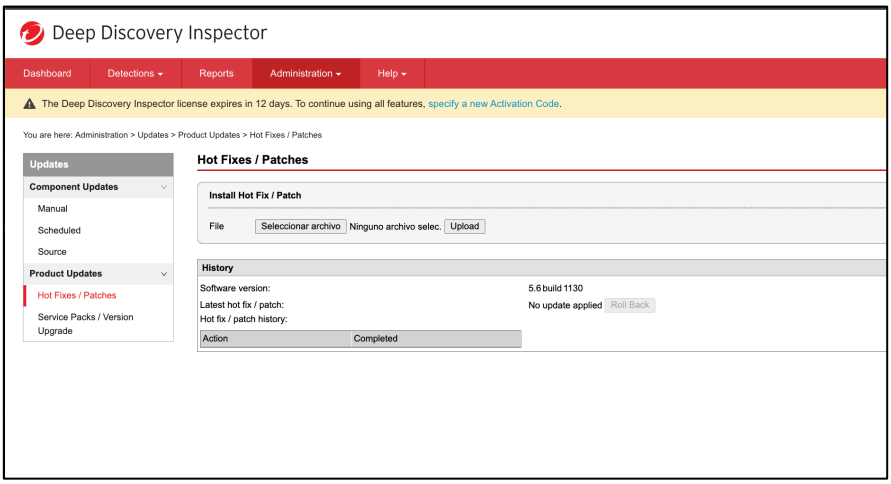


56. En **[UPDATE]** se incluye el procedimiento para realizar un upgrade de parche y de versión mayor. A continuación, se muestran las comprobaciones de seguridad que se han de realizar antes de hacer una actualización, así como volver a un estado seguro en caso de que las actualizaciones no se completen de forma satisfactoria.

6.8.1 UPGRADE DE PARCHE

57. Antes de realizar el *upgrade* se debe revisar el *upgradepatch* y la reléase notes de la versión para ver la compatibilidad con la versión actual.

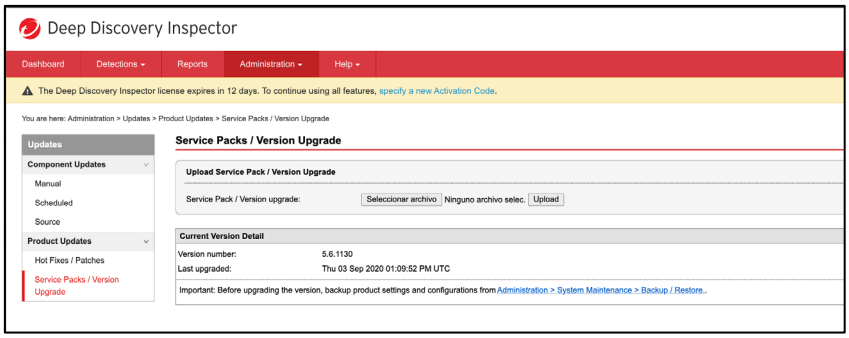
58. Al subir un parche la consola permite realizar un *rollback* en caso de detectar cualquier problema.



6.8.2 UPGRADE DE VERSIÓN MAYOR (*SERVICE PACK*)

59. Antes de realizar el *upgrade* se debe revisar el *upgrade version* y la reléase notes de la versión para ver la compatibilidad con la versión actual.

60. En caso de problema se debe reinstalar la ISO con la versión deseada, ya que al actualizar el *kernel* de S.O no permite realizar *rollback*.



6.9 AUTO-CHEQUEOS

61. Al arrancar el DDI (Deep Discovery Inspector), el firmware realiza un auto chequeo en el arranque, en caso de problema con los chequeos de arranque se debe reinstalar la ISO de DDI. **En caso de que el auto chequeo falle, se notificará al administrador durante el arranque.**

62. Seguir la guía de *best practices* **[BESTP]** para que el administrador pueda realizar un chequeo a nivel de configuración.

6.10 ALTA DISPONIBILIDAD

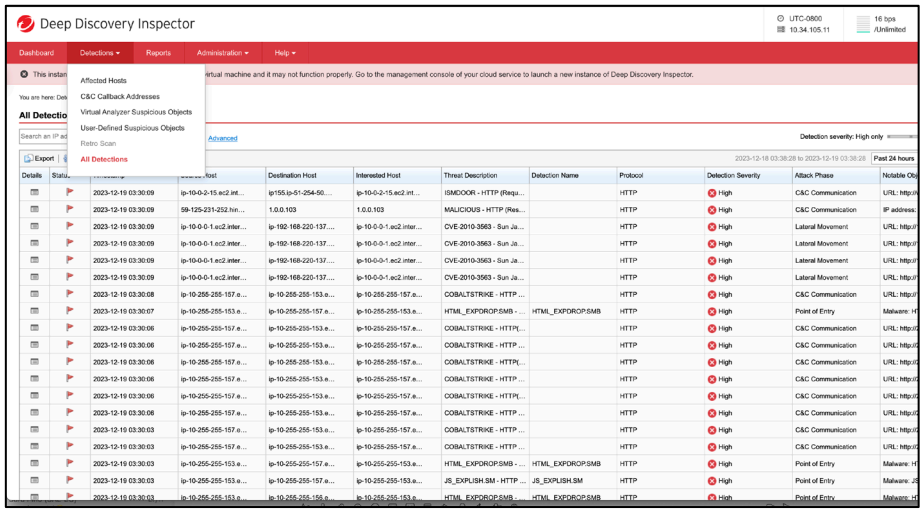
63. El Deep Discovery Inspector al ser una sonda fuera del camino de la comunicación, no requiere ni soporta alta disponibilidad.

6.11 AUDITORÍA

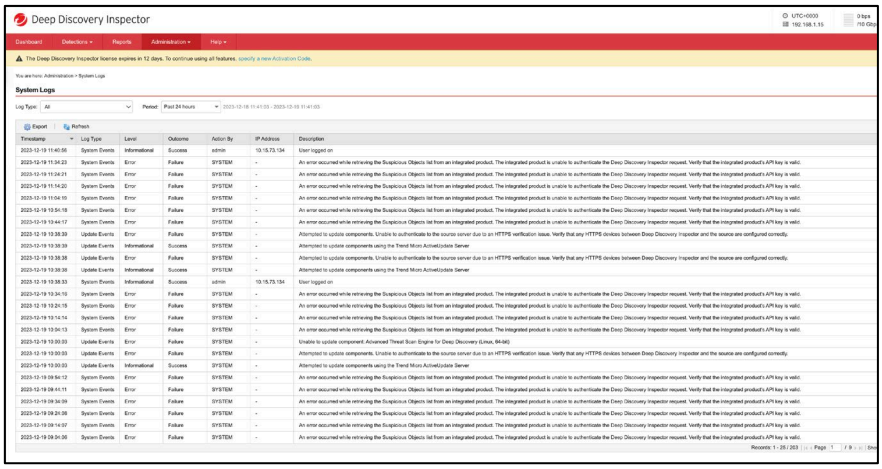
6.11.1 REGISTRO DE EVENTOS

64. A nivel de registros, Deep Discovery Inspector dispone de varias vistas en el menú de detecciones: (host afectados, Comand and control, sandboxing, IOCs y todas las detecciones) para filtrar los eventos generados por la sonda de red y su sandbox.

65. A continuación, se adjunta un ejemplo de filtrando por todos los eventos:



66. Si se quieren revisar los eventos de sistema se debe ir a la sección de la consola: Administración/System logs. Desde esta sección se ven los cambios de configuración, acciones y errores realizados por el DDI

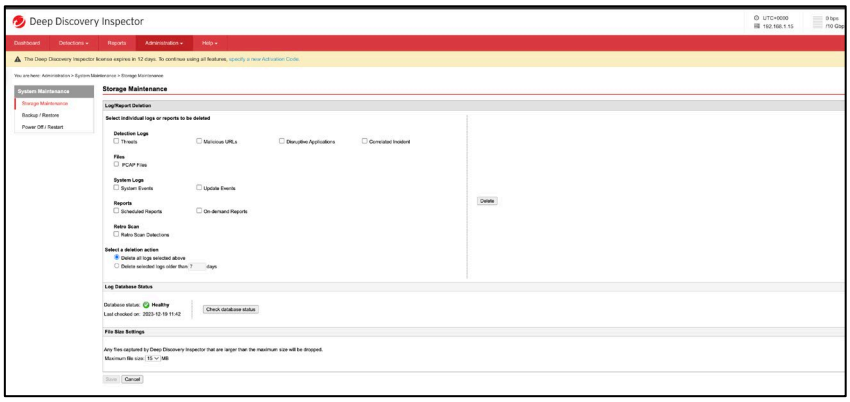


6.11.2 ALMACENAMIENTO LOCAL

67. Deep Discovery Inspector dispone de una sección de la consola para revisar los logs de Sistema como se ha mencionado en el párrafo 66.

68. La configuración a nivel de log, permite realizar un purgado de la base de datos, también permite borrar los reportes antiguos de la herramienta. Se adjunta un pantallazo a modo ejemplo. Para más información revisar la guía de Administración **[ADMIN]** sección Administración/System logs pagina 369.

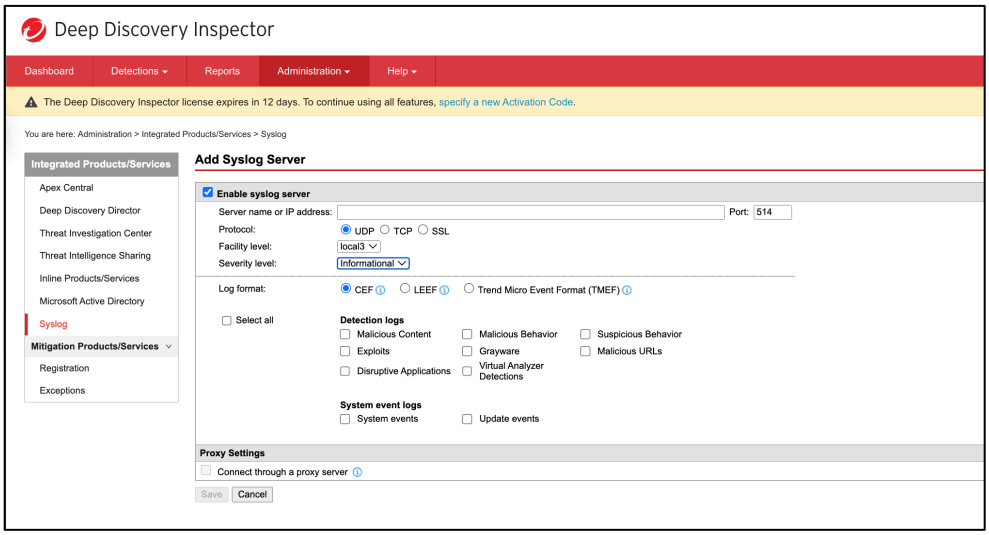
    Menu de configuración: Administration/system maintenance/storage maintenance



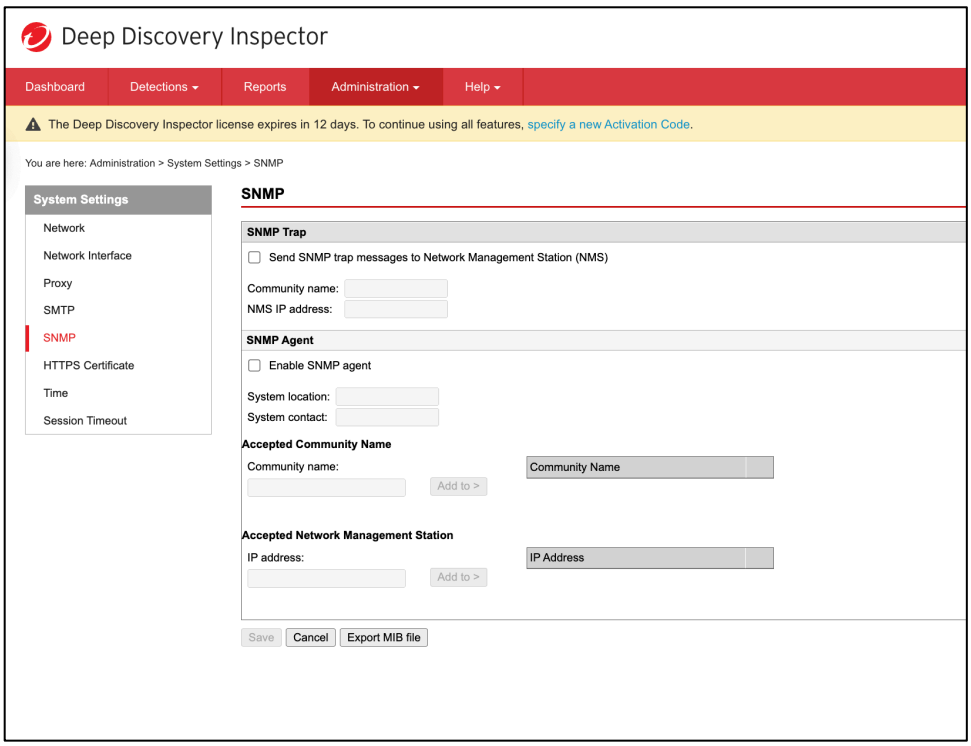
6.11.3 ALMACENAMIENTO REMOTO

69. Deep Discovery Inspector permite realizar el envío de logs mediante syslog/syslogSSL, a continuación, se adjunta un pantallazo de ejemplo del menú de configuración y sus opciones. Para más información revisar la guía de administración **[ADMIN]** sección del documento en la página 338.

    Menu de configuración: Administration/Integrated Products/services/syslog



70. También permite realizar un chequeo de salud mediante SNMP, permitiendo realizar *querys* hacia el DDI y también envío de notificaciones (*traps*):

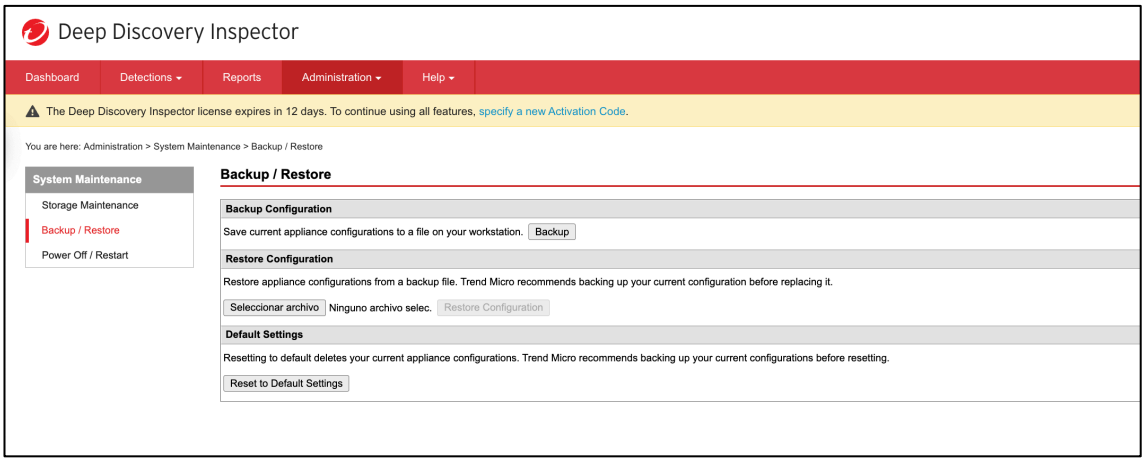


6.12 *BACKUP*

71. Deben indicarse los componentes, datos y configuraciones sobre las que han de realizarse los *backups*. Se adjunta un pantallazo a continuación indicando la forma de realizar un *backup*, *restore* o realizar un formateo a nivel de fábrica.

72. Las operaciones de *backup*, su importación y la restauración de la configuración por defecto está descrita en la sección *Backup/Restore* del manual **[ADMIN]**.

73. Se recomienda la realización de *backups* periódicos.


Deep Discovery Inspector
Dashboard
Detections
Reports
Administration
Help
The Deep Discovery Inspector license expires in 12 days. To continue using all features, specify a new Activation Code.
You are here: Administration > System Maintenance > Backup / Restore
System Maintenance
Storage Maintenance
Backup / Restore
Power Off / Restart
Backup / Restore
Backup Configuration
Save current appliance configurations to a file on your workstation.
Backup
Restore Configuration
Restore appliance configurations from a backup file. Trend Micro recommends backing up your current configuration before replacing it.
Seleccionar archivo
Ninguno archivo selec.
Restore Configuration
Default Settings
Resetting to default deletes your current appliance configurations. Trend Micro recommends backing up your current configurations before resetting.
Reset to Default Settings

7. REFERENCIAS

74. Indicar documentación que se haya referenciado a lo largo de la guía.

[DDIVReq] Requerimientos DDI virtual
https://docs.trendmicro.com/en-us/documentation/article/trend-vision-one-virtual-deepdiscover

[INS_DEP] Guía de instalación y despliegue:
https://docs.trendmicro.com/o-help/manual/96515cfe-aa03-464c-acd9-3f132e7ff962/ddi_6.7_idg.pdf

[ADMIN] Guía de administración
https://docs.trendmicro.com/o-help/manual/96515cfe-aa03-464c-acd9-3f132e7ff962/ddi_6.7_ag.pdf

[UPDATE] Guía de actualización /upgrade:
https://success.trendmicro.com/dcx/s/solution/000250600-Deep-Discovery-Inspector-DDI-Software-Upgrade-Path?language=en_US

[BESTP] Guía de mejores prácticas:
https://success.trendmicro.com/dcx/s/solution/000291206?language=en_US

8. ABREVIATURAS

CPD	Centro de Procesamiento de Datos
DDI	*Deep Discovery Inspector*
DNS	*Domain Names Systems*
GUI	*Graphical User Interface*
HTTPS	*Hypertext Transfer Protocol Secure*
IOC	*Indicator of Compromise*
NTP	*Network Time Protocol*
RDQA	*Research Development Quality Assurance*
SAML	*Security Assertion Markup Language*
SMTP	*Simple Mail Transfer Protocol*
SNMP	*Simple Network Management Protocol*
SSH	*Secure Shell*
SSL	*Secure Sockets Layer*
TLS	*Transfer Layer Security*

PUBLICACIONES DE DEFENSA

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