centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1112

Procedimiento de empleo seguro
Microsoft Defender for Identity

Diciembre 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

NIPO: 083-24-312-9
Fecha de Edición: diciembre de 2024.

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.12.23 17:36:11 +01'00'

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

ÍNDICE **2**
1. INTRODUCCIÓN **3**
2. OBJETO Y ALCANCE **4**
3. ORGANIZACIÓN DEL DOCUMENTO **5**
4. FASE PREVIA A LA 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 COMPONENTES DEL ENTORNO DE OPERACIÓN 6
4.5.1 PORTAL 7
4.5.2 SENSORES 7
4.5.3 SERVICIO EN LA NUBE 7
5. FASE DE INSTALACIÓN **9**
5.1 ALTA DEL SERVICIO EN LA NUBE 9
5.2 DESPLIEGUE DE MICROSOFT DEFENDER FOR IDENTITY 9
6. FASE DE CONFIGURACIÓN **10**
6.1 MODO DE OPERACIÓN SEGURO 10
6.2 CREACIÓN DE UNA INSTANCIA 10
6.3 AUTENTICACIÓN 10
6.4 ADMINISTRACIÓN DEL PRODUCTO 11
6.4.1 ADMINISTRACIÓN LOCAL Y REMOTA 11
6.4.2 CONFIGURACIÓN DE ADMINISTRADORES 11
6.5 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS 13
6.6 GESTIÓN DE CERTIFICADOS 13
6.7 SERVIDORES DE AUTENTICACIÓN 13
6.8 SINCRONIZACIÓN 13
6.9 ACTUALIZACIONES 14
6.10 ALTA DISPONIBILIDAD 14
6.11 AUDITORÍA 14
6.11.1 REGISTRO DE EVENTOS 14
6.11.2 ALMACENAMIENTO LOCAL 15
6.11.3 ALMACENAMIENTO REMOTO 15
6.12 BACKUP 16
6.13 FUNCIONES DE SEGURIDAD 17
7. FASE DE OPERACIÓN **18**
8. REFERENCIAS **19**
9. ABREVIATURAS **20**

1. INTRODUCCIÓN

1. Microsoft Defender for Identity forma parte de la suite de seguridad integrada Microsoft 365 Defender.
2. Microsoft Defender for Identity es una solución de seguridad basada en la nube que aprovecha las señales de Active Directory local para identificar, detectar e investigar amenazas avanzadas, identidades puestas en peligro y acciones malintencionadas dirigidas a la organización por parte de usuarios internos.
3. Microsoft Defender for Identity permite a los analistas de operaciones de seguridad y a los profesionales de la seguridad, que pueden tener problemas para detectar ataques avanzados en entornos híbridos, realizar las siguientes acciones:
    - Supervisar usuarios, el comportamiento de la entidad y las actividades con análisis basados en aprendizaje.
    - Proteger las identidades y las credenciales del usuario almacenadas en Active Directory.
    - Identificar e investigar las actividades del usuario sospechosas y los ataques avanzados a lo largo de la *Kill chain*.
    - Proporcionar información clara sobre los incidentes en una escala de tiempo sencilla para una rápida evaluación de prioridades.

2. OBJETO Y ALCANCE

4. El objeto del presente documento es servir como guía para realizar una instalación y configuración segura de la solución Microsoft Defender for Identity. Al ser una solución en la nube, este documento no afecta a una versión específica.

5. Esta solución ha sido cualificada, situándose dentro de la Familia de *Otras Herramientas* de la tipología definida por el 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, antes de proceder a la instalación del producto.

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

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

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

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

7. Al tratarse de un servicio en la nube, se darán de alta los datos del cliente en la plataforma de **Microsoft Office 365 (REF1)** y se enviarán de forma segura los accesos pertinentes a la plataforma.
8. El envío de los datos se realizará mediante correo electrónico firmado digitalmente a la cuenta que se ha proporcionado para el alta.
9. Una vez dado el alta en la plataforma se podrá activar las licencias por cada usuario dentro de la plataforma (ver sección **4.3**).

4.2 ENTORNO DE INSTALACIÓN SEGURO

10. Al tratarse de un servicio alojado en la nube, se provisionan recursos y se generan los accesos a la plataforma donde opera el producto.
11. El acceso se realiza mediante el uso de HTTPS con TLS1.2 para garantizar la seguridad de las comunicaciones.
12. Sólo los usuarios autorizados y con la licencia activa podrá acceder al producto.

4.3 REGISTRO Y LICENCIAS

13. Los servicios prestados son mediante contratación y no es necesario la instalación.
14. El administrador asigna las licencias por cada usuario dentro de la suscripción contratada.
15. En cuanto al registro de los sensores encargados de recopilar los datos, durante la instalación de estos (ver sección **5.2**) requieren de una “clave de acceso” proporcionada por el propio portal de Microsoft Defender for Identity que servirá para vincularlos a la instancia correspondiente del servicio contratado.

4.4 CONSIDERACIONES PREVIAS

16. Al tratarse de un servicio alojado en la nube, la principal consideración previa es tener conexión a internet y estar dado de alta en la plataforma para hacer uso del producto.
17. Los prerrequisitos necesarios para la implementación del producto están descritos en **Requisitos previos de Microsoft Defender for Identity** (ver **REF2**).

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

18. El producto consta de los siguientes componentes:
    - Portal
    - Sensores
    - Servicio en la nube

4.5.1 PORTAL

19. El portal del producto permite la creación de instancias, muestra los datos recibidos de los sensores y está habilitado para supervisar, gestionar e investigar las amenazas en el entorno de red.

20. La funcionalidad del portal es la siguiente:

    - Crear la instancia del producto
    - Integración con otros servicios de Microsoft Security
    - Administrar la configuración de los sensores.
    - Ver los datos recibidos de los sensores.
    - Supervisar las actividades sospechosas detectadas y los presuntos ataques basados en el modelo de ataques kill-chain.
    - Se puede configurar para enviar correos electrónicos y eventos cuando se detecten alertas de seguridad o problemas de salud.

4.5.2 SENSORES

21. Los sensores pueden ser instalados en los siguientes tipos de servidores:

    - **Controladores de dominio**: El sensor monitoriza directamente el tráfico del controlador de dominio, sin necesidad de un servidor dedicado o configuración de puerto espejo.
    - **ADFS**: El sensor monitoriza directamente el tráfico de red y servidores de autenticación.

22. El sensor accede a los registros de eventos que necesita directamente desde los servidores. Tras analizar los registros y el tráfico de red, el sensor envía únicamente la información analizada al servicio en la nube (sólo se envía un porcentaje de los registros).

23. La funcionalidad del sensor es:

    - Capturar e inspeccionar el tráfico de red del controlador de dominio (tráfico local del controlador de dominio).
    - Recibir eventos de Windows directamente de los controladores de dominio.
    - Recibir información de cuentas de RADIUS del proveedor VPN.
    - Recuperar datos sobre usuarios y ordenadores del dominio.
    - Realizar la resolución de entidades de red (usuarios, grupos y ordenadores).
    - Transferir datos relevantes al servicio en la nube.

4.5.3 SERVICIO EN LA NUBE

24. El servicio en la nube se ejecuta en la infraestructura de Azure y está conectado a la plataforma de seguridad inteligente de Microsoft.

25. El producto es gestionado por usuarios autorizados con los permisos adecuados basados en el RBAC proporcionado por los roles de Azure AD. Sólo los usuarios con el rol de administrador pueden realizar las tareas de seguridad y modificar la configuración del producto.

26. El producto es accesible mediante acceso web utilizando el Microsoft Defender Portal y estableciendo una conexión segura utilizando TLS1.2 o superior. Los datos se cifran en

tránsito y en reposo. El producto utiliza tecnologías de protección de datos de última generación que se basan en la infraestructura de Microsoft Azure. En todos los escenarios, los datos se cifran utilizando cifrado AES de 256 bits.

27. El producto almacenará la información en una instancia específica del cliente y segregada para el servicio con fines de administración, seguimiento e informes. Los datos se aíslan mediante autenticación de acceso y segregación lógica basada en el identificador del cliente a través de Azure Active Directory y se audita el acceso.

5. FASE DE INSTALACIÓN

28. En este apartado se describe la implementación del producto. Consta de los siguientes pasos:

    - Alta del servicio en la nube
    - Despliegue de Microsoft Defender for Identity.

5.1 ALTA DEL SERVICIO EN LA NUBE

29. Al tratarse de un servicio en la nube, lo único que se requiere para ser utilizado en que el proveedor del servicio asigne un usuario en el sistema.

30. Una vez dado de alta, los usuarios autorizados podrán acceder al portal y proceder a la implementación de los demás componentes.

5.2 DESPLIEGUE DE MICROSOFT DEFENDER FOR IDENTITY

31. Este apartado esta descrito en la sección 2 de la guía **CCN-STIC 885F Guía de configuración segura para Microsoft Defender for Identity** (**REF7**).

6. FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

32. Al tratarse de un servicio alojado en la nube, se provisionan recursos y se generan los accesos a la plataforma donde opera el producto.

33. El acceso se realiza mediante el uso de HTTPS con TLS1.2 o superior para las comunicaciones seguras y sólo los usuarios autorizados podrán acceder al producto. Todos los usuarios deben ser autenticados por Azure AD antes de interactuar con el producto.

34. El producto es gestionado por usuarios autorizados con los permisos adecuados basados en el RBAC proporcionado por los roles de Azure AD. Sólo los usuarios con el rol de administrador pueden realizar las tareas de seguridad y modificar la configuración del producto.

35. Respecto al cliente no es necesario ninguna configuración segura ya que todo se realiza desde el portal de Microsoft 365 Defender.

36. El sensor que se instala en la infraestructura del cliente establece por defecto una conexión segura con el servicio en la nube mediante el uso de TLS1.2.

37. El uso de un gestor de eventos externo mediante syslog deberá ser configurado a través de un canal de comunicación seguro que utilice TLS1.2

6.2 CREACIÓN DE UNA INSTANCIA

38. El acceso al portal (portal.atp.azure.com) solo está permitido para un usuario de Azure AD que tenga el rol de directorio de administrador global o administrador de seguridad. La primera vez que se accede a dicho portal con el rol adecuado, se da la opción de crear una instancia para usar Defender for Identity. Una vez configurada la instancia, todos los accesos al portal serán redirigidos a la nueva URL:

    - https://<instancia>.atp.azure.com

6.3 AUTENTICACIÓN

39. El producto usa Azure Active Directory para que los usuarios se autentiquen antes de cualquier interacción con el producto cuando el acceso se realiza a través de la interfaz web.

40. En el caso del sensor, se utilizan las credenciales locales del sistema operativo y se autentica mediante el uso de claves API para ser autenticado durante las operaciones.

41. Los permisos se basan en el modelo de permisos de control de acceso basado en roles (RBAC). Un rol concede los permisos para realizar un conjunto de tareas y un grupo de roles es un conjunto de roles que permite a los usuarios realizar las tareas en el producto. Un usuario puede ser miembro de un rol.

42. Azure Multi-Factor Authentication (MFA) protege el acceso a los datos y aplicaciones, ya que requiere una segunda forma de autenticación.

43. Más información en la guía **CCN-STIC-884A Guía de configuración segura para Azure (REF8).**

6.4 ADMINISTRACIÓN DEL PRODUCTO

6.4.1 ADMINISTRACIÓN LOCAL Y REMOTA

44. Al tratarse de un servicio en la nube siendo parte de la infraestructura de Microsoft Azure, la administración del producto se realiza de forma remota utilizando el protocolo seguro HTTPS con TLSv1.2 o superior para el establecimiento de las comunicaciones seguras.

45. La administración de los sensores se realiza a través del portal de administración de Microsoft Defender for Identity en la página dedicada a Sensores donde se podrá ver un listado de todos los sensores implementados. Esto está descrito en la sección 3.1.2.1 de la guía **CCN-STIC 885F Guía de configuración segura para Microsoft Defender for Identity (REF7)**. Para ampliar la información se puede consultar el enlace **Configurar el sensor de Microsoft Defender for Identity (REF9)**.

46. Los certificados usados por el servidor usan RSA con una longitud de clave de 2048 bits.

47. Para ampliar la información, se puede consultar las secciones 3.1.1.4 y 3.1.1.5 de la guía **CCN-STIC 885F Guía de configuración segura para Microsoft Defender for Identity (REF7).**

6.4.2 CONFIGURACIÓN DE ADMINISTRADORES

48. Al tratarse de un servicio en la nube siendo parte de la infraestructura de Microsoft Azure, la administración del producto se realiza de forma remota.

49. El producto es gestionado por usuarios autorizados con los permisos adecuados basados en el RBAC proporcionado por los roles de Azure AD. Sólo los usuarios con el rol de administrador pueden realizar las tareas de seguridad y modificar la configuración del producto.

50. Algunos de estos roles y funciones pueden ser los siguientes:

    - Global administrator: Puede administrar todos los aspectos del identificador de Azure AD y los servicios de Microsoft que usan identidades de Azure AD.
    - Security administrator: Puede leer información e informes de seguridad, y administrar la configuración en Azure AD y Office 365.
    - Global reader: Puede leer todo lo que puede leer un administrador global, pero no actualizar nada.

51. Para ampliar la información, se puede consultar la información proporcionada por el fabricante en el enlace **Built-in roles REF5**.

52. Algunos de los parámetros del producto que puede modificar el administrador son:

    - Administración de los sensores.
    - Administración de las cuentas de servicio de Directorio Activo.
    - Administración de las cuentas de acción.
    - Administración de las cuentas de Honeytoken.

53. El producto forma parte de la infraestructura de Azure y usa Azure AD para administrar las cuentas de usuario. Las sesiones expiran después de un período establecido por el administrador en Azure AD. Los valores predeterminados son:

    - Duración máxima de la sesión: 1440 minutos
    - Duración mínima de la sesión: 60 minutos
    - Cuánto tiempo antes de que expire la sesión antes de que se muestre la advertencia de tiempo de espera: 20 minutos

54. El producto utiliza Azure AD para las cuentas, y se aplican diferentes mecanismos de seguridad como la tecnología Smart Lockout. El bloqueo inteligente protege las cuentas de usuario de los ataques que intentan adivinar las contraseñas de los usuarios o utilizan métodos de fuerza bruta para entrar. Los valores predeterminados de bloqueo inteligente son los siguientes:

    - Umbral de bloqueo (número de intentos de inicio de sesión fallidos antes de que se bloquee a un usuario): 10
    - Duración del bloqueo: 60 segundos

55. El producto utiliza la infraestructura de Azure y puede administrar la directiva de contraseñas mediante las directivas de Azure AD. Se aplica una directiva de contraseñas a todas las cuentas de usuario y administrador que se crean y administran directamente en Azure AD. Los siguientes requisitos de directiva de contraseñas de Azure AD se aplican a todas las contraseñas que se crean, cambian o restablecen en Azure AD:

Propiedad	Requisitos
Caracteres permitidos	Mayúsculas (A - Z) Minúsculas (a - z) Números (0 - 9) Símbolos: - @ # $ % ^ & * - _ ! + = [ ] { } | \ : ' , . ? / ` ~ " ( ) ; < > Espacio en blanco
Caracteres no permitidos	Caracteres unicode
Longitud de la contraseña	Un mínimo de 8 caracteres y un máximo de 256.
Complejidad de contraseñas	Las contraseñas requieren 3 categorías de las 4 siguientes: - Mayúsculas - Minúsculas - Números - Símbolos

Propiedad	Requisitos
Contraseña no utilizada recientemente	Cuando un usuario cambia o restablece su contraseña, la nueva contraseña no puede ser la misma que las contraseñas actuales o usadas recientemente.

56. Para ampliar la información, se puede consultar la guía **CCN-STIC-884A - Guía de configuración segura para Azure (REF8)** y la información proporcionada por el fabricante en el enlace **Authentication documentation REF6**.

6.5 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

57. Todo acceso al producto se realiza mediante el uso de HTTPS con TLS1.2 o superior. esto está descrito en la sección 1.7.2 de la guía **CCN-STIC-884 – Guía de configuración segura para Azure (REF8)**.

58. Para la configuración de los puertos correspondientes se puede consultar la sección 1.7.8 de la guía **CCN-STIC-884 – Guía de configuración segura para Azure (REF8).** En esta sección se listan los puertos necesarios para que el producto se comunique correctamente entre sus componentes.

6.6 GESTIÓN DE CERTIFICADOS

59. Al tratarse de un servicio en la nube siendo parte de la infraestructura de Microsoft Azure los certificados que se usan, emplean RSA con longitud de clave de 2048 bits.

60. El producto usa la autenticación mutua basada en certificados entre cada sensor y el back-end en la nube de Defender for Identity.

61. Los certificados usados por el producto no se pueden modificar y son gestionados por el proveedor.

62. Para ampliar la información, se puede consultar la información proporcionada por el fabricante en el enlace **MDI-DOC REF3**.

6.7 SERVIDORES DE AUTENTICACIÓN

63. El producto usa Azure Active Directory para que los usuarios se autentiquen antes de cualquier interacción con el producto cuando el acceso se realiza a través de la interfaz web. En el caso del sensor, se utilizan las credenciales locales del sistema operativo y se autentica mediante la sesión de inicio de sesión.

6.8 SINCRONIZACIÓN

64. Al tratarse de un servicio en la nube, los servidores donde está alojado el servicio se sincronizan mediante el uso de NTP con el proveedor de servicios en la nube.

6.9 ACTUALIZACIONES

65. El proveedor de servicios en la nube actualiza el software en sus servicios administrados, y se encarga de mantener sus sistemas actualizados sin la intervención del usuario. Entre estos sistemas se incluyen todos los componentes del producto, incluyendo los sensores que se actualizan sin intervención del usuario.

6.10 ALTA DISPONIBILIDAD

66. Al tratarse de un servicio en la nube, el proveedor de servicios en la nube brinda el servicio de alta disponibilidad sobre los servidores donde se aloja el servicio y las conexiones para el acceso al mismo.

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

67. El producto genera registros de auditoría clasificados por actividades que se auditan en Microsoft 365. Puede buscar estos eventos buscando en el registro de auditoría en el portal de seguridad y cumplimiento seleccionando la categoría:

    - Proceso de inicio de sesión del personal autorizado (estos eventos son de la integración con Azure AD). Debido a la arquitectura y el modo de funcionamiento de la infraestructura de Azure, la plataforma usa la funcionalidad de sesiones y no hay eventos de cierre de sesión. Los inicios de sesión (sing-ins) se registran con los siguientes estados descritos:
        - Éxito: inicio de sesión exitoso.
        - Error: Error al validar las credenciales debido a un nombre de usuario o contraseña no válidos.
        - Interrumpido: la contraseña del usuario ha caducado y, por lo tanto, su inicio de sesión o sesión ha finalizado. Donde se le pregunta a un usuario si desea permanecer conectado a este navegador para facilitar los inicios de sesión posteriores.
    - Cambio en las credenciales de usuario (estos eventos son de la integración con Azure AD)
    - Cambios en la configuración del producto seleccionando la categoría adecuada:
        - Sensores añadidos/eliminados.
        - Cuentas de servicios de directorio agregadas/eliminadas.
    - Eventos relacionados con la funcionalidad del producto buscando la categoría adecuada en las actividades:
        - Uso de las cuentas Sensitive y Honeytoken.
        - Incidentes y alertas sobre activos impactados (reporte de actividades anómalas).
        - Usuarios deshabilitados cuando se informa de una cuenta comprometida.

68. El registro de auditoría se muestra en la página de búsqueda del registro de auditoría. Los resultados de una búsqueda en el registro de auditoría se muestran con la siguiente información:

    - Fecha: la fecha y hora en que ocurrió el evento

- Dirección IP: la dirección IP del dispositivo que se utilizó cuando se registró la actividad. La dirección IP se muestra en formato de dirección IPv4 o IPv6.
- Usuario: el usuario (o cuenta de servicio) que realizó la acción que desencadenó el evento.
- Actividad: La actividad realizada por el usuario. Este valor corresponde a las actividades seleccionadas en la lista desplegable Actividades. En el caso de un evento del registro de auditoría de administración de Exchange, el valor de esta columna es un cmdlet de Exchange.
- Elemento: El objeto que se creó o modificó como resultado de la actividad correspondiente. Por ejemplo, el archivo que se ha visto o modificado o la cuenta de usuario que se ha actualizado. No todas las actividades tienen un valor en esta columna.
- Detalle: Información adicional sobre una actividad. Una vez más, no todas las actividades tienen un valor.

69. Se puede ver más detalles sobre un evento haciendo clic en el registro del evento en la lista de resultados de búsqueda. Se muestra una página flotante que contiene las propiedades detalladas del registro de eventos. Las propiedades que se muestran dependen del servicio en el que se produce el evento.

6.11.2 ALMACENAMIENTO LOCAL

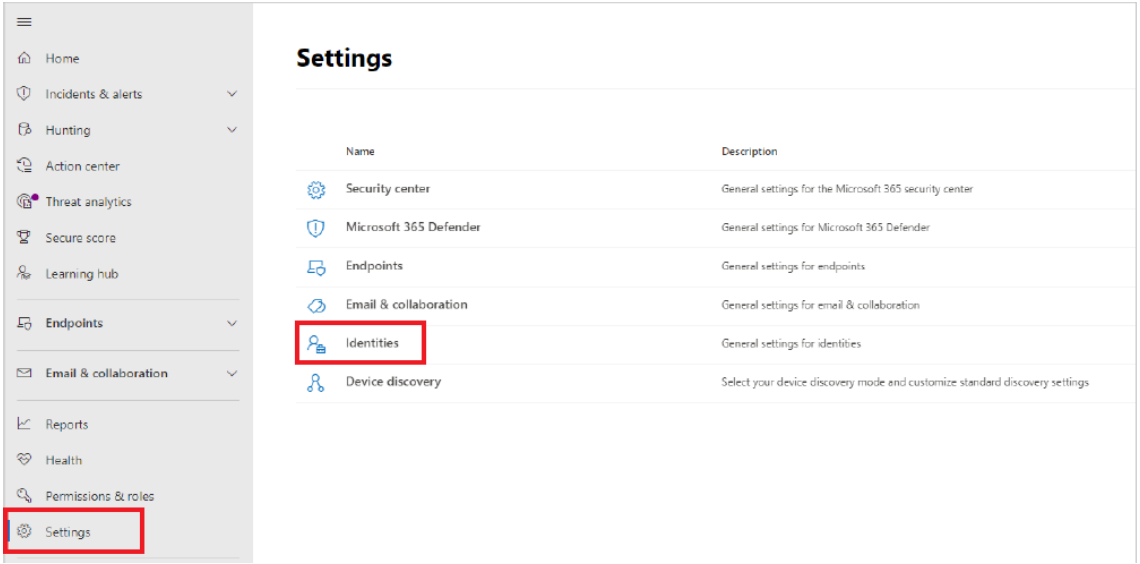
70. Al tratarse de un servicio en la nube, el almacenamiento es proporcionado por el proveedor de servicios en la nube, guardándose de forma cifrada. El almacenamiento en reposo de la información se lleva a cabo mediante el uso de la infraestructura de Azure empleando el cifrado con AES-256 bits.

6.11.3 ALMACENAMIENTO REMOTO

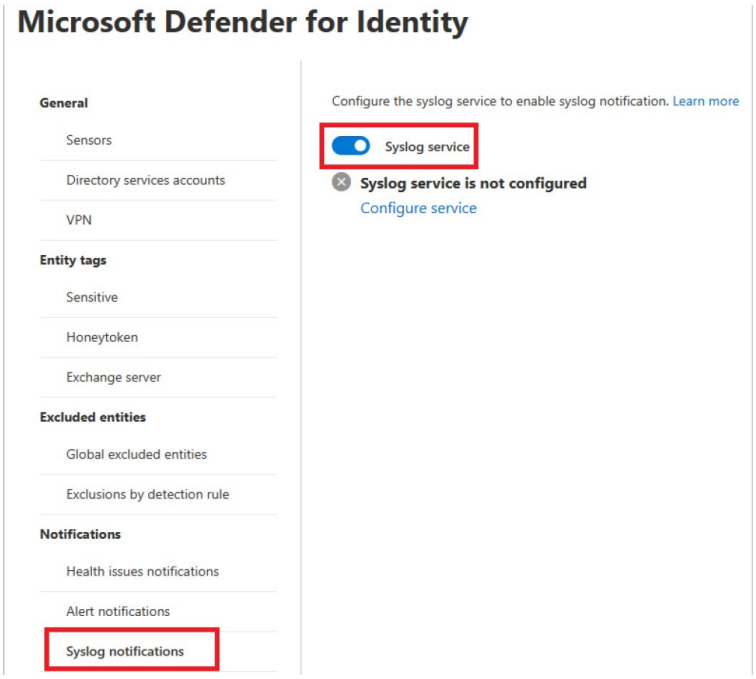
71. El producto puede conectarse con gestor de eventos externo usando syslog y usando TLS1.2 para las comunicaciones seguras.

72. Para activar este servicio se deben seguir los siguientes pasos:

    1. En el portal de Microsoft 365 Defender, ir a **Settings > Identities**.



2. Seleccionar **Syslog notifications**.
3. Para habilitar las notificaciones al syslog, establecer el valor en activo del **Syslog service**.



4. Seleccionar Configure service. Introducir la información para configurar el servicio de syslog:
   - Sensor: En la lista desplegable, elija el sensor que enviará las alertas.
   - Service endpoint and Port: Introducir la dirección IP o el nombre de dominio completo (FQDN) para el servidor syslog y especificar el número de puerto. Solo puede configurar un punto de conexión de Syslog.
   - Transport: Seleccionar el protocolo de transporte (TLS secured sysLog).
   - Format: Seleccionar el formato (RFC 3164 or RFC 5424).
5. Seleccionar Send test SIEM notification y luego verificar si el mensaje se ha recibido en el servidor de syslog.
6. Seleccionar Save.
7. Una vez configurado se pueden seleccionar los tipos de notificaciones que se desean enviar (alerts o health issues)

73. Para ampliar la información, se puede consultar la información proporcionada por el fabricante en el enlace **MDI-DOC REF3**.

6.12 BACKUP

74. Al tratarse de un servicio en la nube, las copias de seguridad son realizadas por el proveedor en su plataforma de Microsoft Azure.

6.13 FUNCIONES DE SEGURIDAD

75. Este apartado se debe consultar en la **CCN-STIC 885F Guía de configuración segura para Microsoft Defender for Identity (REF7).**

7. FASE DE OPERACIÓN

76. Al tratarse de un servicio en la nube, las consideraciones para realizar una operación segura del mismo deben ser tenidas en cuenta por el proveedor del servicio.

77. No obstante, el cliente deberá tener en cuenta las siguientes tareas para una operación segura del producto:

    - Analizar periódicamente los registros de auditoría generados por el servicio con el objetivo de detectar cualquier comportamiento anómalo del mismo.
    - Los administradores deben estar correctamente formados en el uso y la correcta operación del producto.
    - Los administradores mantendrán sus credenciales de acceso al producto seguras y protegidas.
    - Gestionar los usuarios siguiendo el principio de mínimo privilegio, permitiendo el acceso solo a los usuarios necesarios en cada momento.

8. REFERENCIAS

REF1 Microsoft Office 365
https://www.microsoft.com/en-us/microsoft-365/enterprise-mobility-security/compare-plans-and-pricing

REF2 Requisitos previos de Microsoft Defender for Identity
https://learn.microsoft.com/es-es/defender-for-identity/deploy/prerequisites

REF3 MDI-DOC
https://learn.microsoft.com/en-us/defender-for-identity/

REF4 Getting Started with Group Managed Service Accounts
https://learn.microsoft.com/es-es/windows-server/security/group-managed-service-accounts/getting-started-with-group-managed-service-accounts

REF5 Built-in roles
https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

REF6 Authentication Documentation
https://learn.microsoft.com/en-us/entra/identity/authentication/

REF7 CCN-STIC 885F Guía de configuración segura para Microsoft Defender for Identity
https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/6302-ccn-stic-885f-guia-de-configuracion-segura-para-microsoft-defender-for-identity/file.html

REF8 CCN-STIC-884A Guía de configuración segura para Azure
https://www.ccn-cert.cni.es/es/800-guia-esquema-nacional-de-seguridad/4253-ccn-stic-884a-guia-de-configuracion-segura-para-azure/file.html

REF9 Configurar el sensor de Microsoft Defender for Identity
https://learn.microsoft.com/es-es/defender-for-identity/deploy/configure-sensor-settings

9. ABREVIATURAS

AD	Active Directory
ADFS	Active Directory Federation Services
AES	Advanced Encryption Standard
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación
FQDN	Fully Qualified Domain Name
HTTP	Hyper Text Transfer Protocol
IP	Internet Protocol
MFA	Multi-Factor Authentication
NTP	Network Time Protocol
RBAC	Role Based Access Control
RFC	Request for Comments
STIC	Seguridad TIC
TLS	Transport Layer Security
URL	Uniform Resource Locator
VPN	Virtual Private Network

PUBLICACIONES DE DEFENSA

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