ManageEngine
Access Manager Plus

Especificaciones de seguridad

Resumen general

ManageEngine Access Manager Plus es un software web para la gestión de sesiones privilegiadas que regula el acceso a sistemas remotos mediante canales seguros desde una consola unificada.

Access Manager Plus aborda el acceso administrativo a sistemas empresariales críticos; cualquier compromiso de su marco de seguridad expondrá a la organización a riesgos graves. Por tanto, el diseño arquitectónico de Access Manager Plus tiene un conjunto de verificaciones de seguridad y privacidad que cubre varias etapas del flujo de trabajo del producto — instalación, autenticación de usuarios, control de acceso, transmisión de datos y almacenamiento. Este documento proporciona un resumen general de las especificaciones de seguridad y privacidad en Access Manager Plus.

Nota: Este documento detalla los parámetros de seguridad y privacidad específicos solo para Access Manager Plus. Para leer la políticas de seguridad general de ManageEngine, haga clic aquí .

Access Manager Plus protege los datos en varios niveles y está clasificado en las siguientes categorías:

Especificaciones de seguridad	
1. Mecanismo de almacenamiento y encriptación	• Encriptación AES-256 • Encriptación dual —primero a nivel aplicación y luego a nivel base de datos • La clave de encriptación y los datos encriptados no se pueden almacenar en un mismo lugar • Modo de cumplimiento FIPS 140-2 • SafeNet Luna PCIe HSM

2. Identificación y autenticación	**Autenticación a nivel aplicación** • Integración con almacenes de identidad como Microsoft AD, Azure AD, cualquier servicio de directorio que cumpla con LDAP, Azure AD y RADIUS • Mecanismo de autenticación local usando el algoritmo SHA2 (SHA512) • Autenticación de Smart Card • Inicio de sesión único con SAML 2.0 **Autenticación de dos factores** • PhoneFactor • RSA SecurID • Contraseña única de un solo uso enviada por correo electrónico • Google Authenticator • RADIUS Authenticator • Microsoft Authenticator • Okta Verify • Duo Security • YubiKey
3. Seguridad e integridad de los datos	**Transmisión de datos** • Encriptado y sobre HTTPS • Modo SSL para conexiones de clientes **Almacenamiento y gestión de datos** • Encriptación dual AES-256 **Validación de entrada de GUI web** • Protección contra inyecciones de SQL, scripts entre sitios, exceso de búfer y otros ataques **Restricciones de IP** • Restricciones de IP basadas en la web

	Ajustes de privacidad • Enmascaramiento de datos sensibles
4. Medidas para el control del acceso	**Control de acceso a datos** • Mecanismo para el control detallado del acceso • Flujo de trabajo de solicitud-liberación para acceso a contraseñas • Integración de sistema de tickets
5. Acceso remoto seguro	**Conexiones remotas con un solo clic** • Protocolo de desktop remoto (RDP) de Windows, SSH, SQL y sesiones VNC desde cualquier navegador compatible con HTML5 • No hay necesidad de plug-ins o software de agentes adicionales • Las conexiones remotas se enrutan a través del servidor de Access Manager Plus • Soporte de RemoteApp para Windows • Las contraseñas necesarias para establecer sesiones remotas no necesitan estar disponibles en el navegador del usuario • No hay una conectividad directa entre el dispositivo del usuario y el host remoto • Transferencia remota bidireccional de archivos
6. Gestión de sesiones privilegiadas	• Registro y repetición de sesiones privilegiadas • Monitoreo en tiempo real • Colaboración y terminación de sesiones

7. Auditorías, control de rendición de cuentas y alertas en tiempo real	**Funciones de detección y medidas de no repudio** • Alertas en tiempo real para eventos de contraseñas, usuarios y acceso • Pistas detalladas de auditoría • Compatibilidad con SIEM • SNMP traps y mensajes de syslog
8. Respaldo y recuperación de desastres	**Opción de respaldo** • Respaldo en tiempo real y periódico de la base de datos • Almacenamiento encriptado de archivos de respaldo **Recuperación del sistema ante fallos** • Recuperación ante desastres con el servidor MS SQL y el servidor PostgreSQL
9. Proceso de compilación y parcheo	• Análisis de vulnerabilidades y pruebas de penetración obligatorios • Compilaciones de hotfixes y correcciones de errores

1. Mecanismo de almacenamiento y encriptación: Seguridad por diseño

1.1 Instalación de la clave maestra

- Access Manager Plus usa una encriptación AES-256 (la encriptación más fuerte conocida que el gobierno de EE. UU. ha aprobado). La clave usada para la encriptación se genera automáticamente y es única para cada instalación. Esto sirve como la clave de encriptación de primer nivel.

- No se permite mantener la clave de encriptación de primer nivel con la instalación de Access Manager Plus. Esto se hace para garantizar que la clave de codificación y los datos codificados, en la base de datos en tiempo real y de respaldo, no se almacenan juntos.

- Se recomienda almacenar la clave de instalación en un servidor o dispositivo físicamente separado para garantizar que está disponible para el servidor durante el arranque de la aplicación. Por tanto, la clave se mantiene solo en la memoria del servidor y nunca escrita en cualquier lugar.

- Access Manager Plus también es compatible con la rotación periódica de la clave de encriptación, donde se genera una nueva clave y se aplica a los datos existentes y luego la anterior se desecha. Más información

1.2 Clave de la base de datos

- La base de datos de Access Manager Plus está protegida mediante una clave separada, que se genera automáticamente y es única para cada instalación.

- La clave para la base de datos se puede almacenar de manera segura dentro de Access Manager Plus.

- Access Manager Plus también permite a los usuarios almacenar la clave de la base de datos en cualquier ubicación segura, dejando la clave accesible solo al servidor.

- El RDBMS está siempre configurado para aceptar solo conexiones protegidas (fuerza el modo SSL para conexiones con el cliente) y los clientes solo se pueden conectar desde

el mismo host local. En los casos en que el servidor web y el RDBMS deban estar en servidores separados, la configuración aplica conexiones solo de direcciones IP configuradas.

1.3 Modo de cumplimiento de FIPS

Access Manager Plus puede ajustarse para ejecutarse en modo de cumplimiento FIPS 140-2 (usando un servidor SQL como la base de datos de backend) donde toda la encriptación se realiza a través de sistemas y bibliotecas de FIPS 140-2.

1.4 SafeNet Luna PCIe HSM

- Access Manager Plus también es compatible con SafeNet Luna PCIe HSM para dar a los administradores la opción de habilitar la encriptación de datos de hardware.
- SafeNet HSM maneja todos los métodos de encriptación y descifrado, y almacena la clave y los datos de encriptación en su módulo de hardware, lo que se ajusta a un equipo o servidor de red.

2. Identificación y autenticación

2.1. Autenticación robusta a nivel aplicación: varias opciones

Access Manager Plus proporciona varias opciones para identificar de manera única a los usuarios que accederán a la aplicación. Todas las alternativas se complementan con varias opciones de autenticación de dos factores, lo que da una capa extra de seguridad.

- **Integración con almacenes de identidades:** Access Manager Plus se integra de inmediato con almacenes de identidad externos como Microsoft Active Directory, cualquier servicio de directorio que cumpla con LDAP (Novell eDirectory y Oracle OID) y RADIUS. Se puede importar a los usuarios desde almacenes de identidad y se puede aprovechar el respectivo mecanismo de autenticación. Se identificará a los usuarios de manera particular mediante sus respectivas cuentas en el almacén de identidad. Más información.

- **Cuentas únicas y autenticación local segura:** Access Manager Plus tiene un mecanismo de autenticación local en el que se crean cuentas únicas para los usuarios. Los usuarios serán capaces de acceder a la aplicación con sus credenciales. Access Manager Plus emplea el algoritmo SHA2 para generar contraseñas, lo que garantiza que cada contraseña de inicio de sesión es única y protegida irreversiblemente.

- **Tarjeta de acceso común:** compatible con autenticación de Smart Card. El usuario debe poseer una smart card y conocer también el número de identificación personal (PIN). Para conocer más detalles, haga clic aquí.

- **Servicio conforme con SAML:** Access Manager Plus ofrece compatibilidad para SAML 2.0, lo que facilita la integración con soluciones para la gestión de identidades federadas para inicio de sesión único. Access Manager Plus actúa como el proveedor de servicio (SP) y se integra con el proveedor de identidad (IdP) al usar SAML 2.0. La integración básicamente involucra proporcionar detalles sobre el SP y el IdP, y viceversa. Luego de que integre Access Manager Plus con un IdP, los usuarios que han iniciado sesión pueden hacerlo desde la respectiva GUI del proveedor de identidad sin dar de nuevo sus credenciales. Para conocer más detalles, haga clic aquí.

2.2. Mecanismo de garantía: autenticación de dos factores (2FA)

Para introducir un nivel adicional de seguridad, Access Manager Plus proporciona la autenticación de dos factores. Se solicitará a los usuarios que se autentiquen mediante dos etapas sucesivas para acceder a la interfaz web. El segundo nivel de autenticación se puede hacer usando una de las siguientes opciones:

- **PhoneFactor:** este proveedor mundial líder de 2FA basado en teléfonos permite una seguridad simple y efectiva al hacer una llamada de confirmación a su teléfono durante el proceso de inicio de sesión.

- **SecurID de RSA:** integra RSA SecurID con Access Manager Plus más para generar un token de validación de un solo uso que cambia cada 60 segundos.

- **Contraseña única por correo electrónico:** autentica al enviar por correo electrónico contraseñas únicas a los usuarios. Las contraseñas validan al usuario para un inicio de sesión y luego vencen.

- **Google Authenticator:** tokens numéricos basados en tiempo que se pueden recibir al instalar la aplicación Google Authenticator en su smartphone o tablet.

- **Autenticador de RADIUS:** aproveche los mecanismos de autenticación de cualquier sistema conforme con RADIUS, como Vasco Digipass, para crear contraseñas de un solo uso.

- **Microsoft Authenticator:** proporciona un token de seis dígitos en la aplicación Microsoft Authenticator.

- **Okta Verify:** usa un token de seis dígitos en la aplicación Okta Verify.

- **Duo Security:** aprovecha la autenticación de Duo security.

- **YubiKey:** genera contraseñas de único uso con YubiKey.

- Aparte de estos, Access Manager Plus es compatible con cualquier autenticador basado en TOTP.

Para conocer más detalles, haga clic aquí.

3. Seguridad e integridad de los datos

3.1 Transmisión de datos

- Toda la transmisión de datos entre la interfaz de usuario de Access Manager Plus y el servidor se encripta y tiene lugar mediante HTTPS.

- Toda la transmisión de datos entre el servidor y la base de datos de Access Manager Plus se da en SSL.

- La comunicación entre los servidores primario y secundario se encripta en HTTPS.

3.2 Almacenamiento y gestión de datos

- Access Manager Plus está diseñado como una aplicación web con un servidor web para lógica corporativa y RDBMS para almacenamiento de datos.

- Tras aplicar vectores de iniciación adecuados y otras buenas prácticas estándar en torno a la encriptación, se genera la clave de encriptación de primer nivel con el algoritmo AES-256 en el servidor web.

- Los datos encriptados se envían a RDBMS para almacenamiento mediante el uso de consultas SQL. Luego, Access Manager Plus encripta los datos con funciones de RDBMS para AES integradas para capas duales de encriptación.

- Los datos registrados de las sesiones privilegiadas también se encriptan antes de almacenarlos y solo el reproductor propietario los puede reproducir debido a que los datos se almacenen en el formato del propietario.

3.3 Validación de entrada de GUI web

- Access Manager Plus valida integralmente todas las entradas de la GUI. El uso de caracteres especiales y código HTML se filtra, por lo que la aplicación está protegida contra ataques frecuentes como inyecciones de SQL, scripts entre sitios, desbordamientos de búfer y otros ataques.

3.4 Restricciones de IP

- Access Manager Plus permite que los administradores limiten conexiones entrantes al servidor de Access Manager Plus al aplicar restricciones basadas en IP para minimizar el tráfico indeseado.
  Proporciona una capa extra de seguridad al permitir que el administrador escoja exactamente a qué sistemas se les debe permitir o bloquear el acceso y enviar solicitudes al servidor de Access Manager Plus.

3.5 Ajustes de privacidad

- Access Manager Plus proporciona ajustes de privacidad para mejorarla dentro del producto. Los ajustes de privacidad ayudan a enmascarar o controlar la inclusión de información de identificación personal (PII) en el producto. Esta información puede ser un nombre de usuario, número de teléfono o ubicación, o el nombre de DNS de un recurso, departamento, URL o nombre de controlador de un dominio secundario.

4. Medidas para el control del acceso

4.1 Control de acceso a datos

- Todo acceso a los datos en Access Manager Plus está sujeto al mecanismo para el control detallado del acceso. La propiedad de los recursos y las prácticas de intercambio están bien definidas, y los usuarios solo obtienen acceso a contraseñas autorizadas.

- Para activos altamente sensibles, se podría aplicar una capa extra de seguridad al forzar a los usuarios autorizados a ir a través de un mecanismo de solicitud-liberación. Cuando se necesite acceder a un recurso de TI sensible, se debe realizar una solicitud, la cual va a al administrador (personas designadas para autorizar el acceso) para su aprobación y se libera por un tiempo limitado. Más información.

- Todo acceso a los recursos (quién accede a qué recurso y cuándo) y todas las operaciones realizadas por los usuarios en cualquier recursos se registra en las pistas de auditoría, garantizando la aprobación para todos los usuarios y acciones.

- **Integración de sistema de tickets:** Access Manager Plus también se integra con un amplio conjunto de sistemas de tickets para validar automáticamente solicitudes de servicios relacionadas con el acceso privilegiado. La integración garantiza que solo los usuarios con una ID de ticket válida puedan acceder a los recursos. Esta integración también se extiende al flujo de trabajo de Access Manager Plus, lo que ayuda a otorgar aprobaciones a solicitudes de acceso a contraseñas tras la validación automática de las correspondientes solicitudes de servicio en el sistema de tickets.

5. Acceso remoto seguro

5.1 Conexiones remotas con un solo clic

- Access Manager permite a los usuarios iniciar sesiones altamente seguras, confiables y completamente emuladas de Windows RDP, SSH, SQL y VNC desde cualquier navegador compatible con HTML5 sin la necesidad de plug-ins o software de agentes adicionales. Más información.

- Las conexiones remotas a los endpoints se canalizan a través del servidor de Access Manager Plus sin requerir una conectividad directa entre el dispositivo del usuario y el host remoto.

- Además de una fiabilidad superior, la conectividad canalizada proporciona una seguridad extrema, ya que las contraseñas necesarias para establecer sesiones remotas no necesitan estar disponibles en el navegador del usuario.

- **Compatibilidad con RemoteApp:** Access Manager Plus permite a los usuarios conectarse a aplicaciones particulares que están configuradas como RemoteApps en los sistemas objetivo. Añadir RemoteApps a conexiones RDP aumenta la accesibilidad y facilidad de uso cuando se conecta a equipos remotos, y facilita a los administradores de TI las sesiones privilegiadas, ya que limita el acceso del usuario a la aplicación particular que se inicia. Más información.

- **Transferencia remota bidireccional de archivos:** Access Manager Plus permite a los usuarios cargar y descargar archivos hacia y desde cualquier sistema remoto. Access Manager Plus puede realizar la transferencia bidireccional de archivos, es decir, usted puede transferir archivos entre distintas rutas en dos sistemas. La transferencia bidireccional de archivos se logra usando el protocolo de transferencia segura de archivos (SFTP). Más información.

6. Gestión de sesiones privilegiadas

- Todas las acciones que los usuarios realizan durante la sesión privilegiada se graban en video y se almacenan de forma segura para futuros análisis forenses. Más información.

- Además de la grabación de sesiones, Access Manager Plus permite a los administradores monitorear las sesiones privilegiadas en tiempo real. Si se encuentra alguna actividad sospechosa, el administrador puede interrumpir la conexión inmediatamente.

7. Auditorías, control de rendición de cuentas y alertas en tiempo real

7.1 Funciones de detección

- Access Manager Plus proporciona alertas y notificaciones en tiempo real sobre varios eventos, incluyendo acceso, modificación, eliminación, cambios en permisos de intercambio y otros eventos específicos. Más información.

- El módulo de auditoría, que registra cada acción de cada usuario y cada sistema, también permite configurar qué eventos se deben enviar a los sistemas de gestión de eventos e información de seguridad (SIEM). Las alertas de eventos se pueden enviar como mensajes de syslog estándar o SNMP traps. Más información.

7.2 Medidas de no repudio

- Se audita cada acción y tarea programada ejecutada por los usuarios en la interfaz de usuario.

- La información de auditorías, que contiene detalles como quién hizo qué operación, cuándo y desde dónde se almacena en la misma base de datos. Los logs de auditorías son a prueba de alteraciones, lo que garantiza su no repudio.

- El RDBMS está siempre configurado para aceptar solo conexiones protegidas (fuerza el modo SSL para conexiones con el cliente) y los clientes solo se pueden conectar desde el mismo host local. En casos donde el servidor web y el RDBMS deban estar en servidores separados, la configuración permite conexiones solo de direcciones IP específicas.

8. Respaldo y recuperación de desastres

8.1 Opción de respaldo

- Access Manager Plus ofrece opciones para respaldos en tiempo real de la base de datos y respaldos periódicos mediante tareas programadas.

- Todos los datos sensibles en el archivo de respaldo se almacenan de forma encriptada en un archivo ZIP en el directorio de respaldo predeterminado o bajo el directorio de destino configurado por el administrador.

- La copia de respaldo no tendrá la clave maestra de encriptación debido a que Access Manager Plus no permite que la clave de encriptación y los datos encriptados en la base de datos en tiempo real y de respaldo se alojen en el mismo lugar. A menos que se presente la clave de encriptación, los datos sensibles no se pueden descifrar desde la copia de respaldo.

- Mientras que la operación de respaldo de la base de datos está en progreso, no se pueden realizar cambios en la configuración en Access Manager Plus. Más información.

8.2 Fallos y recuperación del sistema

- En el caso de un desastre o pérdida de datos, los usuarios pueden hacer una instalación reciente de la misma versión de Access Manager Plus y restaurar los datos respaldados a la base de datos.

- La recuperación ante desastres para Access Manager Plus con el servidor MS SQL o el servidor PostgreSQL como la base de datos de backend puede realizarse solo con la clave maestra usada inicialmente para la encriptación tras la instalación. Más información.

9. Proceso de compilación y parcheo

- El equipo de Access Manager Plus trabaja de cerca con MESRC para ejecutar análisis obligatorios de vulnerabilidades y pruebas de penetración antes de cada publicación importante con el fin de garantizar que las últimas compilaciones sean completamente infalibles. Además, el equipo también ejecuta evaluaciones continuas de vulnerabilidad en estas compilaciones para garantizar que están libres de cualquier nueva vulnerabilidad.

- Se notifica a los usuarios inmediatamente para actualizar a la última versión como y cuando haya un nuevo parche o actualización de seguridad.

- En el caso de una preocupación o escalamiento de seguridad, se pide a los usuarios presentar un informe detallado de la vulnerabilidad o error de seguridad. Mientras tanto, el equipo del producto evalúa la validez y riesgos asociados con el error y prioriza la liberación con base en la gravedad.

- Las compilaciones de hotfix se liberan entre 24 y 72 horas tras la notificación de un problema, según su gravedad, y el equipo aprobará las compilaciones para publicación solo después de evaluar en busca de otras vulnerabilidades o errores.

www.manageengine.com/latam
/privileged-session-management

Technical support
Email: tech-latam@manageengine.com

ManageEngine
Access Manager Plus