ManageEngine
Access Manager Plus

Guía sobre mejores prácticas

TABLA DE CONTENIDOS

01

Resumen general

1.1 Acerca de Access Manager Plus

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. Con funciones integrales de auditoría, ofrece una visibilidad total de todos los usos de acceso privilegiado y permite a las empresas gestionar sesiones de usuarios privilegiados en tiempo real, lo que cierra la puerta a abusos de acceso. Asimismo, ayuda a demostrar el cumplimiento de regulaciones como PCI DSS, GDPR, NERC CIP y SOX.

1.2 Acerca de la guía

En esta guía se describen las mejores prácticas para empezar con Access Manager Plus en una red empresarial. A partir de nuestra experiencia en ayudar organizaciones alrededor del mundo a implementar el software correctamente, esta guía ofrece instrucciones para que los administradores de seguridad de TI establezcan un software eficiente y optimizado para la gestión de sesiones privilegiadas. Estas mejores prácticas pueden adoptarse durante todas las etapas —instalación del producto, configuración, implementación y mantenimiento— y se explican abajo con un enfoque especial en la seguridad de los datos, la escalabilidad y el rendimiento.

02

Configuración recomendada del sistema

2.1 Requisitos mínimos del sistema

Antes de instalar Access Manager Plus, necesita evaluar la configuración del sistema. Los requisitos mínimos del sistema para ejecutar Access Manager Plus se puede encontrar aquí.

En general, el rendimiento y escalabilidad dependen de los siguientes factores:

- Número de usuarios y grupos
- Número de conexiones activas
- Frecuencia de las conexiones remotas
- Número de tareas programadas
- Espacio de almacenamiento (espacio en disco libre disponible en el disco duro)

Con base en los factores anteriores, se recomiendan los siguientes parámetros de sistema para empresas pequeñas, medianas y grandes:

Requisitos de hardware

Tamaño de la organización	Procesador	RAM	Disco duro
Pequeño (<1000 servidores, <500 claves y <500 usuarios)	Dual Core / Core2 Duo o superior.	4 GB	• 200 MB para el producto • 10 GB para la base de datos
Mediano (<5000 servidores, <1000 claves y <1000 usuarios)	Quad Core o superior.	8 GB	• 500 MB para el producto • 20 GB para la base de datos
Grande (<5000 servidores, <1000 claves y >1000 usuarios)	Octa Core o superior.	16 GB	• 1 GB para el producto • 30 GB para la base de datos

Nota:

También recomendamos que instale Access Manager Plus en un servidor dedicado, fortalecido y de calidad superior para un mejor rendimiento y seguridad.

03

Instalación

3.1 Windows vs. Linux

Access Manager Plus se puede instalar en Windows o Linux. Aunque el software se ejecuta igual en ambas plataformas, la instalación en Windows proporciona una ventaja inherente con respecto a la integración de Active Directory:

Integración con Active Directory (AD):

Una instalación en Windows de Access Manager Plus puede integrarse directamente con AD/ Azure AD para importar usuarios y grupos. Además, los usuarios que han iniciado sesión en su sistema Windows usando las credenciales de cuenta del dominio pueden aprovechar el inicio de sesión único (SSO) usando el protocolo de seguridad de Windows NT LAN Manager (NTLM) para iniciar sesión automáticamente en Access Manager Plus.

3.2 Base de datos de backend

Access Manager Plus proporciona compatibilidad de backend para bases de datos PostgreSQL y servidores MS SQL. Predeterminadamente, el producto tiene integrada una base de datos PostgreSQL, que es ideal para pequeñas y medianas empresas. Entre tanto, para compañías grandes, recomendamos mucho que use un servidor MS SQL como su backend para una mejor escalabilidad, rendimiento, clustering y recuperación ante desastres.

Si está usando un servidor MS SQL como su backend, le sugerimos que lleve a cabo las siguientes prácticas:

- Access Manager Plus puede comunicarse con el servidor MS SQL solo con SSL, con una configuración de certificado válida. Por tanto, le recomendamos que tenga una instancia dedicada de SQL para Access Manager Plus y así evitar cualquier conflicto o interrupción con bases de datos existentes.
- Mientras usa el servidor MS SQL como su backend, se autogenera una clave única para la encriptación a nivel base de datos y, predeterminadamente, esta clave se almacenará en el directorio, en un archivo llamado <masterkey.key>. Le recomendamos que mueva su archivo de clave a una ubicación distinta para protegerlo de acceso no autorizado.
- Use una autenticación de Windows mientras configura el servidor MS SQL como su backend en lugar de usar una cuenta local de SQL.
- Le recomendamos usar la misma cuenta de dominio para ejecutar el servidor de Access Manager Plus y el servidor MS SQL, de forma que pueda ejecutar el servicio SQL y los servicios del agente SQL.
- La opción de encriptación obligatoria se debe habilitar para permitir que todos los clientes se conecten a esta instancia de SQL. Cuando se haga esto, toda la comunicación cliente a servidor se encriptará y se denegará el acceso a los clientes no compatibles con la encriptación.
- Deshabilite todos los protocolos distintos a TCP/IP en el equipo donde se está ejecutando el servidor MS SQL.
- Oculte esta instancia de SQL para evitar que otras herramientas la enumeren y deshabilite el acceso a esta base de datos para todos los usuarios, excepto la cuenta de servicio de Access Manager Plus.
- Establezca reglas de firewall para permitir el acceso solo a los puertos requeridos en el equipo cuando el servidor MS SQL esté en ejecución.

3.3 Proteger la clave maestra

Access Manager Plus usa una encriptación AES-256 para proteger contraseñas y otra información sensible. La clave usada para la encriptación *(amp_key.key)* se genera automáticamente y es única para cada instalación. Predeterminadamente, esta clave se almacenará en el directorio *<AMP_HOME/conf>*, en un archivo llamado *<amp_key.key>*. La ruta de esta clave se debe configurar en el archivo *manage_key.conf* presente en el directorio *<AMP_Installation_Folder>/conf*. Access Manager Plus requiere que se acceda a esta carpeta con el permiso necesario para leer el archivo *amp_key.key* cuando arranque cada vez. Luego del arranque correcto, no necesita acceder más al archivo, por lo que el dispositivo con el archivo se puede estar fuera de línea. Le recomendamos mucho que mueva esta clave a una ubicación segura diferente y la bloquee al dar acceso de lectura solo a la cuenta de servicio de Access Manager Plus. Asimismo, actualice esta ruta remota en el archivo *manage_key.conf* de forma que el producto pueda leer la clave de encriptación durante el arranque. Usted también puede proteger esta clave al almacenarla en un disco USB o disco duro. Para una seguridad extrema, cree archivos de script para copiar esta clave en una ubicación legible y luego destruir la copia tras el arranque del servicio.

3.4 Tomar control de las credenciales de la base de datos

Aparte de la encriptación AES, la base de datos de Access Manager Plus está protegida mediante una contraseña separada, que se genera automáticamente y es única para cada instalación. Esta contraseña de la base de datos se puede almacenar de manera segura en Access Manager Plus. Sin embargo, le recomendamos almacenar la contraseña en otra ubicación segura, accesible al servidor del producto. Predeterminadamente, la información de la base de datos, como JDBC URL, credenciales de inicio de sesión y otros parámetros, se almacenarán en un archivo llamado database_params.conf, que está en el directorio. Aunque la base de datos se configura para no aceptar ninguna conexión remota, le recomendamos que mueva este archivo a una ubicación segura, con acceso restringido, y lo ponga a disposición para la cuenta de servicio de Access Manager Plus. Sin embargo, tendrá una copia de nuevo en la ubicación original, (es decir, en *<AMP_Installation_Folder>/conf*) mientras realiza la actualización de la aplicación. Si pone el archivo database_params.conf fuera de la carpeta de instalación de Access Manager Plus, necesita especificar la ubicación junto con el nombre del archivo en el archivo *\conf \''wrapper.conf''* (para Windows) o *\con- f\''wrapper_lin.conf''* (para Linux). Nótese que el servicio no puede arrancar si no se especifica aquí toda la ubicación.

- La ruta de este archivo se configura en el archivo ***"wrapper.conf"*** en el directorio. Edite este archivo y busque la línea:

wrapper.java.additional.9=-Ddatabaseparams.file.

- Si está usando una instalación de Linux, tendrá que editar el archivo

"wrapper_lin.conf" en el directorio.

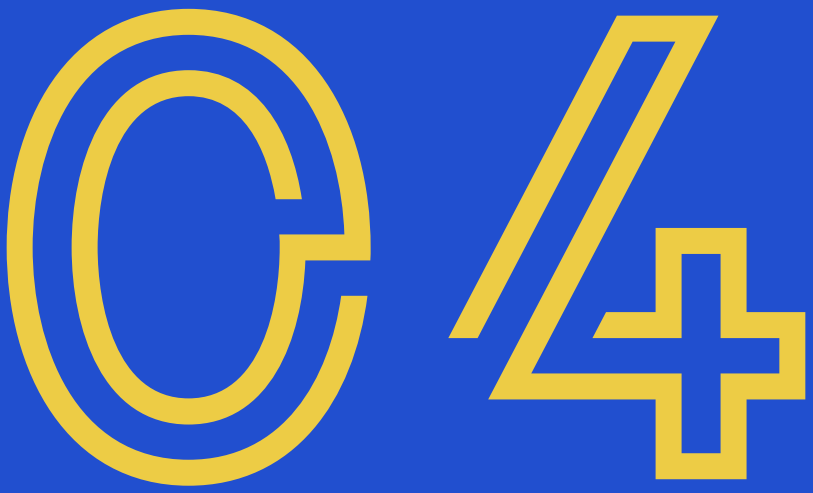
La ruta predeterminada se configurará como ***./../conf/database_params.conf***. Mueva el archivo ***"database_ params.conf"*** a una ubicación segura y especifique su ruta en el archivo anterior. Por ejemplo,

wrapper.java.additional.9=-Ddatabaseparams.file=\\remoteserver1\tapedrive\sharedfiles\database_params.conf.

- Guarde el archivo y reinicie Access Manager Plus para que el cambio surta efecto.

Nota:

Los pasos anteriores son aplicables para PostgreSQL y MySQL. Si está usando un servidor MS SQL como su backend, consulte la sección 3.2.



Parámetros del servidor y del entorno

4.1 Fortalecimiento del servidor

Predeterminadamente, todos los componentes requeridos para que Access Manager Plus funcione se almacenan en el directorio de instalación *(ManageEngine/AMP)*. Por tanto, le recomendamos mucho que fortalezca el servidor donde está instalado Access Manager Plus. Algunos de los pasos básicos que debe llevar a cabo son los siguientes:

- Deshabilite el acceso remoto a este servidor para todos los usuarios regulares del dominio en su organización usando políticas de grupo de dominio. Restrinja los permisos de lectura para todos los administradores regulares y suministre permisos de escritura al disco o directorios de Access Manager Plus para solo uno o dos administradores de dominio.
- Establezca firewalls de entrada y de salida para protegerse ante el tráfico entrante y saliente, respectivamente. Al usar estos parámetros, usted puede también especificar qué puertos del servidor deben abrirse y usarse para realizar varias operaciones de gestión de sesiones, como acceso remoto.

4.2 Usar una cuenta de servicio dedicada

Cree una cuenta de servicio separada para Access Manager Plus en su controlador de dominio. Para empezar a usar esta cuenta de servicio, vaya a la consola de servicio *(services.msc)* en el servidor donde se instaló Access Manager Plus y revise las propiedades. Reemplace la cuenta de sistema local configurada con la cuenta de servicio creada. Esta misma cuenta de servicio se puede usar para importar usuarios y recursos de AD.

4.3 Configurar una dirección IP vinculada para el servidor web

Predeterminadamente, el servidor web de Access Manager Plus se vinculará a todas las direcciones IP disponibles del servidor en que se instale la aplicación. Debido a esto, se puede llegar a Access Manager Plus en cualquiera o todas las direcciones IP con el puerto configurado (9292). Para restringir esto, le recomendamos que configure el servidor web para que se vincule a una sola dirección IP y reciba la comunicación entrante solo desde dicha dirección IP. Se pueden llevar a cabo los siguientes pasos para configurar la IP vinculada:

- Detener Access Manager Plus si está en ejecución.
- Abrir el archivo *"server.xml"* presente en la carpeta \conf.
- Buscar la línea de código:

<Connector SSLEnabled="true" URIEncoding="UTF-8" acceptCount="100" ciphers="TLS_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256" clientAuth="false" debug="0" disableUploadTimeout="true" enableLookups="false" keystoreFile="conf/server.keystore" keystorePass="passtrix" maxHttpHeaderSize="32768" maxSpareThreads="75" maxThreads="150" minSpareThreads="25" port="9292" scheme="https" secure="true" server="PMP" sslProtocol="TLS" truststoreFile="-jre/lib/security/cacerts" truststorePass="changeit" truststoreType="JKS" useBodyEncodingForURI="true"/>

En la línea anterior, junto al puerto de valor = "9292", añada la dirección del atributo = "127.0.0.1". Reemplace 127.0.0.1 con la dirección IP real del servidor que desea usar para el vínculo.

4.4Restringir el acceso del servidor web al poner direcciones IP en listas negras o blancas

Se puede acceder a Access Manager Plus desde cualquier sistema cliente, tanto como haya conectividad. Le recomendamos restringir y aprovisionar solo un número limitado de sistemas clientes con acceso a Access Manager Plus. Para configurar las restricciones basadas en direcciones IP; vaya a ***Administrar > Restricciones de IP > Acceso web***. Las restricciones con IP se pueden establecer en varios niveles y combinaciones, como intervalos de IP definidos o direcciones IP individuales. Usted puede escoger si permite el acceso web a intervalos y direcciones IP específicos o, de forma alternativa, restringir el acceso al añadirlos al campo de direcciones IP bloqueadas.

05

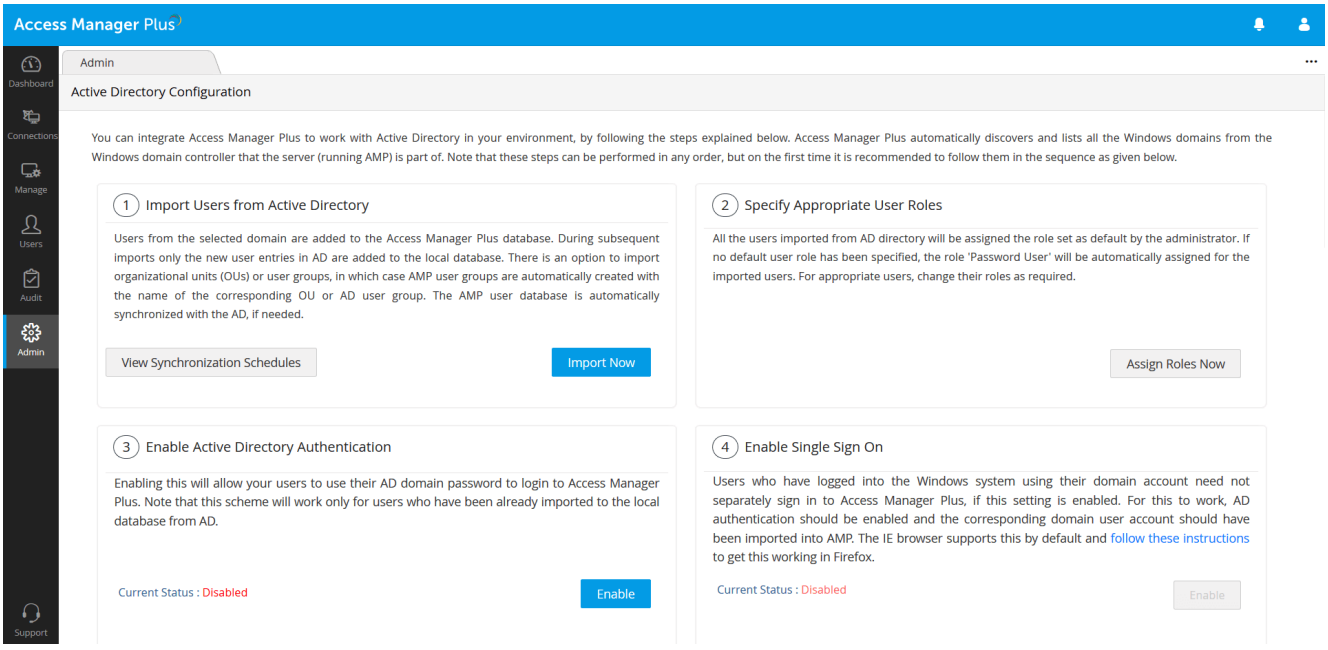
Vinculación y gestión de usuarios

5.1 Aprovechar la integración con AD/LDAP/Azure AD para la autenticación y aprovisionamiento

Aprovechar la integración con AD/LDAP/Azure AD para la autenticación y aprovisionamiento

Aprovisionamiento y desaprovisionamiento de usuarios

Con la integración con AD/LDAP/Azure AD, añadir un usuario en Access Manager Plus es rápido y fácil. Una vez integrado, puede importar directamente los perfiles de usuarios y grupos o unidades organizacionales (OU) desde su directorio a Access Manager Plus. Además, el aprovisionamiento de cuentas de usuarios en el producto se vuelve un proceso simple. Por ejemplo, si importa una OU existente de "Administradores de bases de datos" desde su directorio a Access Manager Plus, puede asignar fácilmente las contraseñas de la base de datos a ese grupo importado. Por si fuera poco, puede habilitar la sincronización mientras integra Access Manager Plus con su directorio, de forma que cualquier cambio, como un usuario recién añadido o movido entre OU en su directorio, se reflejará automáticamente en Access Manager Plus. Sincronizar Access Manager Plus con su directorio también lo mantendrá notificado cuando se elimine permanentemente un usuario del correspondiente directorio de usuario. Access Manager Plus deshabilita y bloquea dichas cuentas de usuarios y lo notifica de ello mediante un correo electrónico y notificación de alerta, tras lo cual puede escoger si elimina o reactiva estas cuentas.



5.1 Configurar los parámetros de AD para la vinculación y autenticación de usuarios.

Configurar los parámetros de AD para la vinculación y autenticación de usuarios.

Otra ventaja es que puede aprovechar el mecanismo de autenticación respectivo de su directorio y dar a sus usuarios opciones de inicio de sesión único (SSO). Una vez activa esta opción, los usuarios se autenticarán automáticamente en Access Manager Plus (usando autenticación basada en NTLM) en tanto hayan iniciado sesión en el sistema con sus credenciales de directorio. Usar credenciales de AD para la autenticación de Access Manager Plus garantiza que las contraseñas de inicio de sesión no se almacenan localmente en Access Manager Plus, ya que los usuarios se autenticarán directamente desde el directorio.

Nota:

Aparte de la autenticación de AD/Azure AD/ LDAP, Access Manager Plus también es compatible con:

- Cualquier autenticación basada en RADIUS (servicio de usuario de marcación para autenticación remota)
- Infraestructura de clave pública (PKI)/autenticación de certificado de smart card
- SSO basado en lenguaje de marcado para confirmaciones de seguridad (SAML) (incluyendo Okta, Azure AD y Active Directory Federation Services (ADFS))

5.2 Deshabilitar la autenticación local

Luego de integrar Access Manager Plus con AD/Azure AD/su directorio que cumple con LDAP, le aconsejamos que deshabilite la autenticación local y permita que los usuarios inicien sesión en Access Manager Plus usando sus credenciales de AD/LDAP/Azure AD. Para deshabilitar la autenticación local, vaya a Administrador > Ajustes del servidor > Ajustes generales > Gestión de usuarios, y habilite la casilla Deshabilitar la autenticación local. Sin embargo, si ha configurado una cuenta local de Access Manager Plus para fines de emergencia, no puede deshabilitar la autenticación local. En dichos casos, si aún desea tener solo la autenticación de AD/LDAP/Azure AD, le recomendamos que deshabilite la opción "Olvidé mi contraseña" en la misma sección (opción usada para restablecer la contraseña de autenticación local para todos los usuarios en Access Manager Plus). Deshabilitar esta opción garantizará que los usuarios puedan iniciar sesión en Access Manager Plus usando solo sus credenciales de AD/LDAP/Azure AD, incluso si la autenticación local está habilitada.

5.3 Usar autenticación de dos factores

Una capa adicional de protección para la autenticación de usuarios garantiza que solo las personas correctas tengan acceso a recursos sensibles. Access Manager proporciona varias opciones para configurar un segundo nivel de autenticación antes de dar acceso a la interfaz web del producto. Las opciones para un segundo factor son: PhoneFactor, tokens de RSA SecurID, Duo Security, Google Authenticator, contraseñas únicas por correo electrónico, cualquier autenticación que cumpla con RADIUS, Microsoft Authenticator, Okta Verify y YubiKey. Se recomienda mucho que configure la autenticación de dos factores para sus usuarios.

5.4 Asignar roles de usuarios con base en las responsabilidades del cargo

Luego de añadir usuarios, asígneles los roles adecuados. Access Manager Plus tiene dos roles de usuario predefinidos: Administrador y Usuario estándar. El rol de administrador debe limitarse solo a unas pocas personas que necesiten realizar la vinculación y desvinculación de usuarios. Aparte de estos roles predeterminados, Access Manager Plus también le permite añadir roles personalizados desde cero. Haga clic aquí para obtener más información sobre los roles personalizados. Para más seguridad, cualquier nuevo rol personalizado añadido por un administrador debe recibir la aprobación de otro administrador.

5.5 Crear grupos de usuarios

técnicos, etc. El agrupamiento de usuarios ayuda a mejorar la eficiencia cuando comparte recursos y delega contraseñas. Si ha integrado Access Manager Plus con AD/LDAP/Azure AD, puede importar grupos de usuarios directamente desde el directorio y usar la misma estructura jerárquica.

5.6 Eliminar las cuentas de usuarios predeterminadas

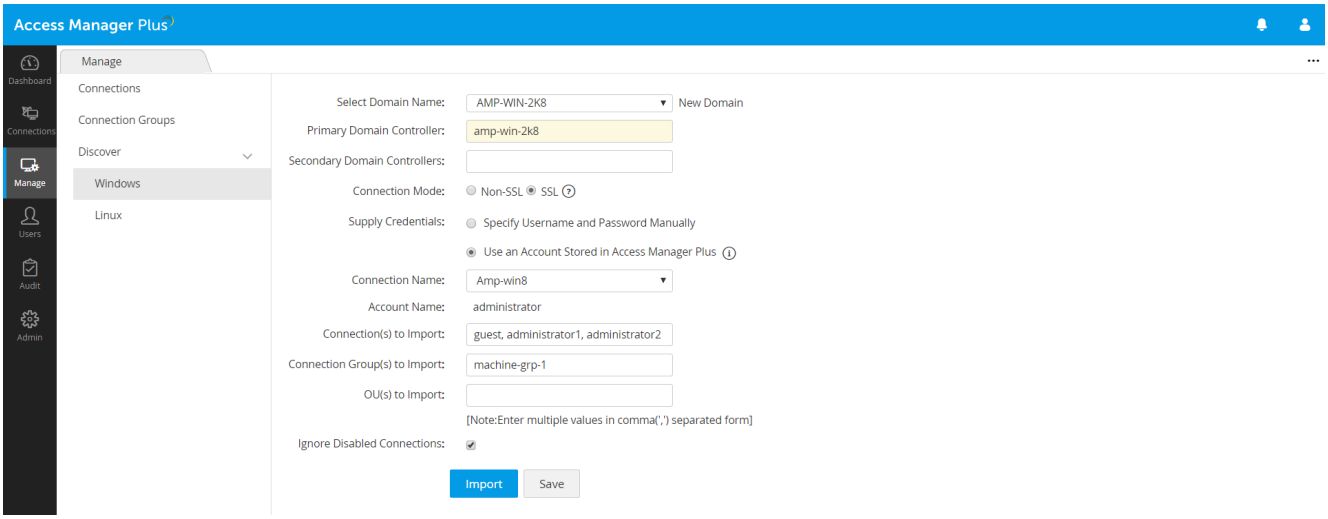
Por razones de seguridad, recomendamos mucho que elimine las cuentas de usuarios predeterminadas, como cuentas administrativas y de invitado en Access Manager Plus, luego de añadir uno o más usuarios con el rol de administrador.

06

Diligenciamiento y gestión de datos

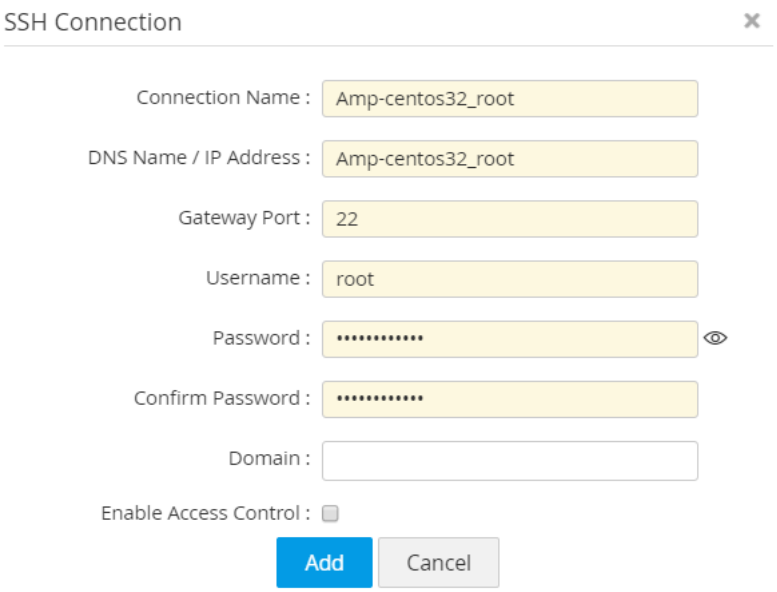
6.1 Añadir conexiones: escoger un método conveniente

El primer paso para empezar con la gestión de acceso en Access Manager Plus es añadir sistemas objetivo remotos como “Conexiones” para iniciar conexiones remotas seguras. La forma más rápida y conveniente de hacer esto es el descubrimiento automatizado en sistemas remotos Windows y Linux.



6.1.1 Descubrimiento automático de conexiones de Windows

Las otras formas son la adición manual y la importación a CSV. Use la función de importación a CSV si ha usado otra herramienta antes de cambiar a Access Manager Plus o si tiene los detalles de los recursos almacenados en hojas de cálculo.



6.1.2 Adición manual de una conexión SSH

6.2 Eliminar cuentas privilegiadas no gestionadas, no deseadas y desconocidas

Cuando use la función de descubrimiento automático para inventariar una conexión en Windows o Linux en su red, Access Manager Plus, por defecto, añadirá cada cuenta asociada como una conexión. Algunas cuentas pueden estar no gestionadas, ser no deseadas o huérfanas. Por ejemplo, cuando añade una conexión de Windows, también se buscarán todas las cuentas de invitados.
Desde una perspectiva de seguridad, dichas cuentas se deben identificar y eliminar para evitar cualquier vulnerabilidad no prevista en el futuro. Le recomendamos que mantenga al mínimo el número de cuentas privilegiadas. Además, eliminar cuentas indeseadas puede saturar la base de datos y hacer de la organización de los datos una tarea tediosa. Por tanto, es ideal eliminar estas cuentas no deseadas en el equipo objetivo en sí antes de ejecutar el descubrimiento automático en Access Manager Plus.

6.3 Aprovechar la potencia de los grupos de conexión

Access Manager Plus le permite crear grupos de conexión para facilitar ediciones y configuraciones de parámetros masivas a todas las conexiones asociadas con ese grupo particular. Los grupos de conexión también sirven como medio para combinar tipos similares de conexiones bajo un mismo techo y verlos separados de la pestaña Conexiones.

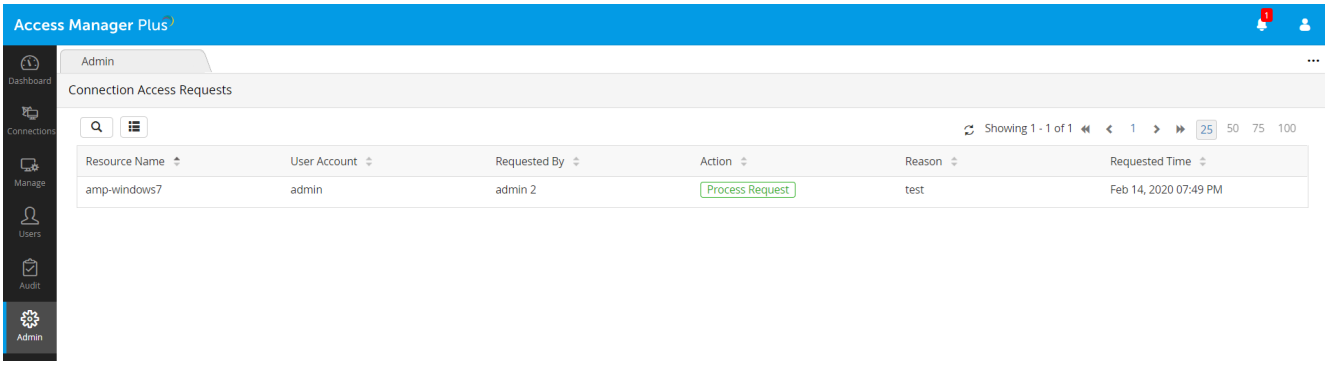
Esta función le proporciona la flexibilidad para consolidar conexiones que satisfagan criterios en un solo grupo. Una vez se crea el grupo de conexión, use la opción Acción de grupo para realizar cambios masivos en los parámetros sobre todas las conexiones que son parte del grupo.

07

Controles de acceso detallados

7.1 Usar los flujos de trabajo de control de acceso

El control de acceso en Access Manager Plus es un mecanismo de solicitud-liberación que no permite a los usuarios acceder directamente a sistemas remotos. En su lugar, los usuarios deben generar una solicitud al administrador de TI para que apruebe el acceso. Esta función también le ayuda a introducir otras restricciones para sus recursos, como acceso por tiempo limitado y controles de simultaneidad. Le recomendamos mucho habilitar esta función para sus recursos críticos.



7.1 Mecanismo de solicitud-liberación en Access Manager Plus

Los controles de acceso se pueden configurar al ir a **Gestionar > Conexiones > Acciones de conexión > Editar conexión > Habilitar control de acceso.**

7.2 Requerir que los usuarios den motivos para recuperar contraseñas

Predeterminadamente, todas las operaciones relacionadas con el acceso se registran en las pistas de auditoría de Access Manager Plus, se completan con la fecha y los detalles de la dirección IP. Otra opción es obligar a los usuarios a dar una razón para obtener el acceso remoto. Estas razones también se registrarán en las pistas de auditoría, que se pueden usar para una verificación cruzada y validación en investigaciones forenses. Por tanto, cuando un usuario intente acceder a una conexión, le recomendamos exigir que dé una razón creíble para solicitar el acceso, sin importar si los controles de acceso están configurados. Esta opción se puede activar bajo **Administrador > Ajustes del servidor > Ajustes generales > Recuperación de la contraseña.**

7.3 Integrar Access Manager Plus con sistemas de tickets empresariales

Access Manager Plus da la opción de integrar un conjunto de sistemas de ticket para validar automáticamente solicitudes de servicios relacionadas con el acceso privilegiado. La integración garantiza que los usuarios pueden acceder a un sistema remoto solo con una ID de ticket válida. Con el fin de habilitar un flujo de trabajo de acceso remoto más seguro, le sugerimos que integre Access Manager Plus con su sistema de tickets empresarial. Actualmente, Access Manager Plus ya se integra con ManageEngine ServiceDesk Plus On-Demand, ServiceDesk Plus MSP, ServiceDesk Plus, ServiceNow y JIRA. Puede integrar Access Manager Plus con los sistemas de tickets arriba mencionados al ir a **Administrador > Parámetros de sesión > Integración de sistema de tickets.**

08

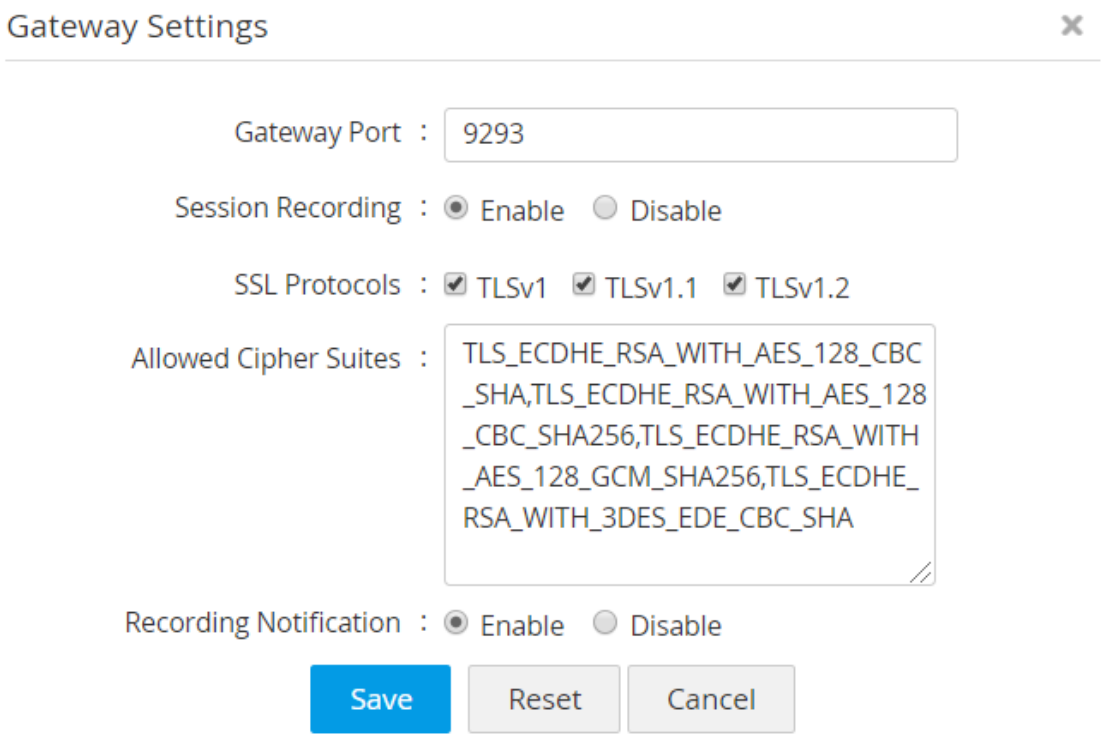
Acceso remoto seguro

8.1 Permitir que los usuarios inicien sesión automáticamente en sistemas remotos sin revelar contraseñas en texto sin formato

Luego de configurar las opciones de inicio de sesiên automÄtico para conectarse remotamente a los equipos, Access Manager Plus permite a los usuarios establecer una conexiên directa con el sistema remoto con solo un clic, eliminando la necesidad de copiar y pegar contraseèas. En dichos casos, recomendamos que evite que los usuarios recuperen sus contraseèas en texto sin formato, ya que no se requiere. La recuperaciên de contraseèas en texto sin formato se puede deshabilitar en**Administrador > Ajustes del servidor > Ajustes generales > Recuperación de la contraseña.**

8.2 Configurar los parámetros de gateway

Access Manager Plus le permite personalizar los parÄmetros de gateway. Usted puede editar y controlar los paquetes de cifrado usados para la comunicaciên de SSL, establecer un puerto diferente, escoger que se usen protocolos SSL para proteger conexiones iniciadas desde el producto y personalizar parÄmetros de log de cabeceras HTTP, etc. Para editar los parÄmetros de gateway, vaya a **Administrador > Ajustes de sesión > Ajustes de gateway**. Aparte de esto, usted puede también ver el archivo *gateway.conf* en la ruta *<AMP_installation_directory>\conf* para una personalizaciên mÄs extensiva y para otros detalles técnicos.



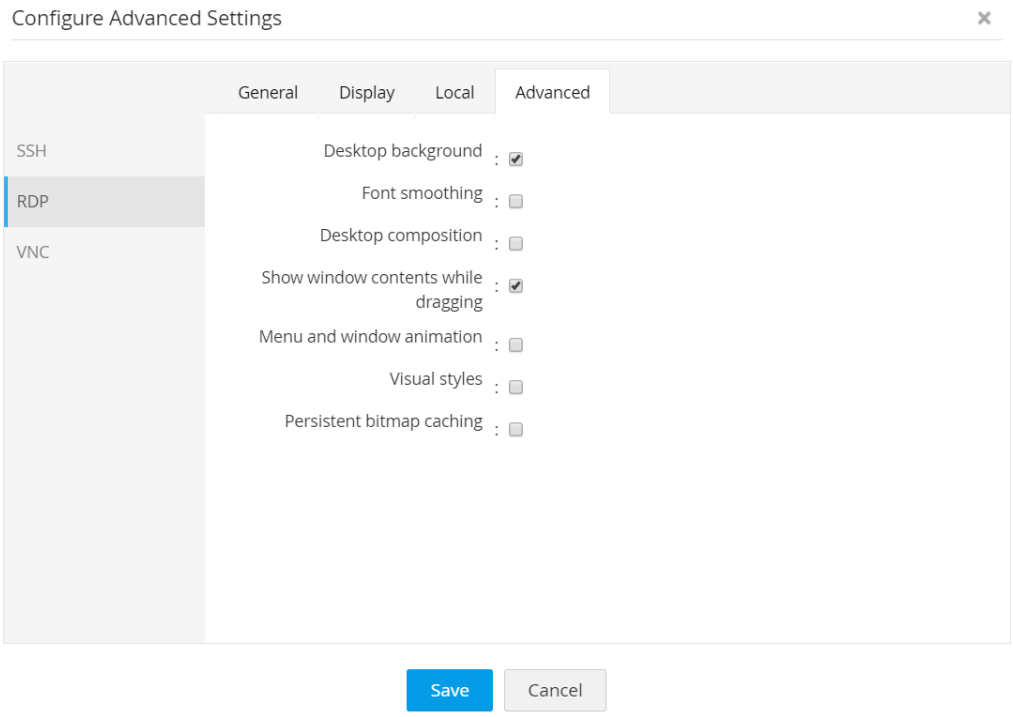
8.2 Configuración ajustes del gateway

8.3 Aprovechar los parámetros avanzados para conexiones

Access Manager Plus ofrece parÄmetros avanzados de configuraciên para conexiones que se pueden personalizar y asã mejorar la velocidad y rendimiento de las conexiones remotas iniciadas desde dentro del producto. Estas mejoras estÄn disponibles para conexiones SSH, RDP y VNC para una configuraciên centralizada y facilidad de uso. Todos los cambios hechos aquã a los parÄmetros se aplicarÄn también localmente en el sistema remoto. Algunos de los parÄmetros avanzados incluyen la capa de teclado, segundo plano de desktop, discos de mapas, compatibilidad de audio remoto, etc.

Para configurar estos parámetros, para una conexión, haga clic en el menú desplegable **Acciones** al lado del nombre de cualquier conexión y escoja **Ajustes avanzados**. Para configurar los parámetros de forma masiva, seleccione las conexiones requeridas y haga clic en **Ajustes** en el menú desplegable **Más acciones**.

Haga clic aquí para obtener más información sobre los ajustes avanzados.



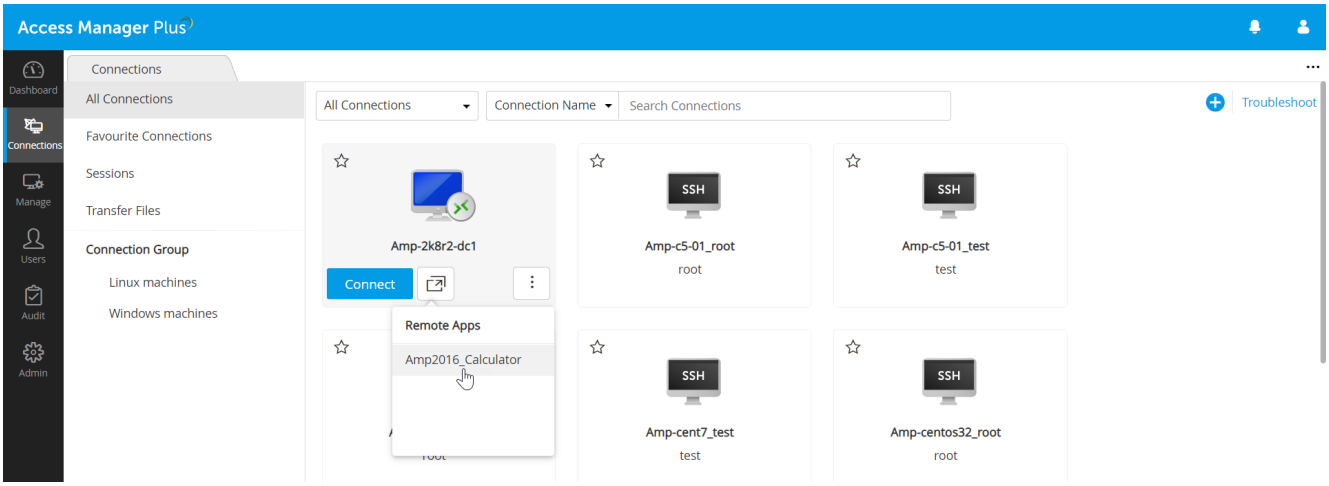
8.3 Ajustes avanzados para RDP

8.4 Descubrir y configurar RemoteApp para servidores de Windows

Nota:

Necesita instalar las RemoteApps requeridas en los servidores objetivo remotos para usar esta funciên.

Aparte de establecer conexiones directas a sistemas remotos, usted puede permitir que los usuarios se conecten a aplicaciones particulares que estÄn configuradas como RemoteApps en los sistemas objetivo. Puede descubrir automÄticamente las RemoteApps configuradas en los sistemas objetivo de Windows o aèadirlas manualmente en Access Manager Plus. Configurar RemoteApps para conexiones de Windows vuelve mÄs segura la gestiên de sesiones privilegiadas de RDP, ya que limita el acceso de los usuarios a la aplicaciên particular que se inicia, en lugar de todo el desktop remoto. Por ejemplo, considere que puso una aplicaciên en una lista blanca, digamos SQL Studio, para un usuario particular. Ahora, cuando el usuario inicie una sesiên, abrirÄ automÄticamente SQL Studio y el usuario puede solo usar esa aplicaciên. No puede ver la barra de tareas, ir a otra Ärea o realizar ninguna otra operaciên distinta a usar SQL Studio.



8.4 Conexión a una RemoteApp durante una sesión RDP

09

Acceso privilegiado a terceros

9.1 Gestionar el acceso de terceros a sistemas corporativos

Con mucha frecuencia terceros como contratistas, consultores y proveedores requieren acceso a recursos corporativos de TI debido a varios deberes contractuales y otras necesidades corporativas. Cuando proporciona acceso privilegiado a un tercero, le recomendamos que siempre les dé solo acceso temporal y restringido con estipulaciones de tiempo y privilegios mínimos necesarios. Además, he aquí otras prácticas sugeridas para realizar mientras comparte información crítica con terceros:

- Ya que los contratistas se conectan remotamente a sus recursos, añada todos sus terceros como usuarios en Access Manager Plus y pídales que establezcan sesiones directas a los sistemas objetivos solo mediante Access Manager Plus.
- Luego de configurar el inicio de sesión automático para el recurso, la mejor práctica es compartir las credenciales de inicio de sesión sin mostrar las contraseñas en texto sin formato.
- Asimismo, configure los flujos de trabajo de control de acceso para dichos recursos. Esto ayuda a implementar límites de tiempo para acceder a los sistemas.
- Supervise las sesiones regularmente para detectar cualquier traza de comportamiento malicioso y adopte instantáneamente medidas de corrección.
- Cuando termine el contrato con un proveedor, ejecute inmediatamente restablecimientos de contraseña para todas las conexiones a las que ha tenido acceso —ya sea manualmente o con la ayuda de una herramienta para la gestión de contraseñas— y actualice las contraseñas de conexión en Access Manager Plus.

10

Acceso remoto a centros de datos

10.1 Evitar la rotación de credenciales del servidor de salto

Por lo general, conectarse a recursos de un centro de datos remoto es un proceso tedioso, ya que el acceso directo estÄ restringido desde una perspectiva de seguridad. Para superar estas barreras de acceso, usualmente los usuarios van a través de varios servidores de salto antes de conectarse finalmente al dispositivo objetivo. Este proceso de varios saltos requiere que los usuarios den credenciales separadas para cada servidor de salto con el fin de iniciar una conexiên al centro de datos. Rotar todas las credenciales entre los usuarios para facilitar una conexiên a un centro de datos remoto no es una prÄctica segura. En su lugar, usted puede usar la funciên de configuraciên del servidor de acceso para forzar a sus usuarios a que se conecten a los centros de datos solo mediante Access Manager Plus. La aplicaciên proporciona un acceso automatizado, seguro y con un solo clic a los recursos del centro de datos mediante servidores de salto RDP y SSH (servidor de un salto para Windows y varios servidores de salto para Linux). Esto elimina la necesidad de la autenticaciên manual en cada salto. Access Manager Plus le permite almacenar todas las credenciales del servidor de salto en una ïnica consola centralizada.

11

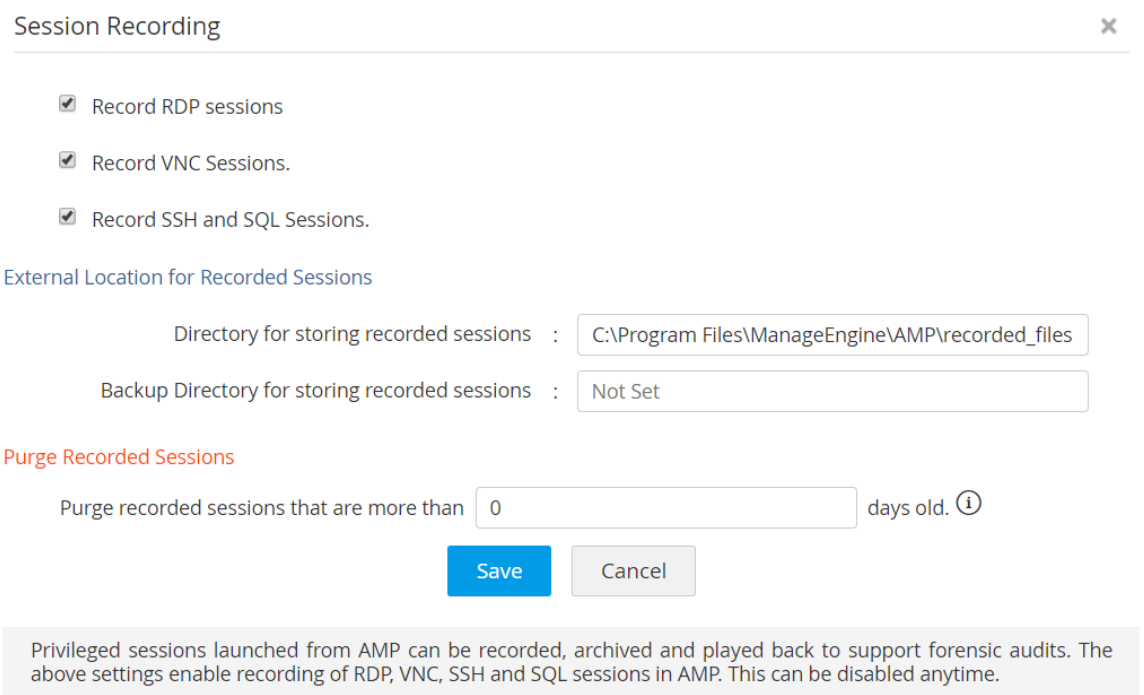
Gestión y monitoreo de sesiones

11.1 Monitorear sesiones críticas en tiempo real

Access Manager Plus ofrece seguimiento de sesiones, lo que se puede usar para establecer controles duales en sesiones privilegiadas. Use esta función para monitorear sesiones remotas en tiempo real y supervise la actividad de los usuarios. Los controles duales son útiles para suministrar ayuda remota y enfrentar actividades maliciosas. Si es un administrador, puede supervisar sesiones críticas iniciadas desde la aplicación al unirse a sesiones activas y observar simultáneamente, sin afectar al usuario final. Puede unirse a una sesión activa al ir a **Conexiones > Sesiones > Unirse**. Cuando un usuario inicie una sesión remota, varios usuarios pueden unirse a la misma sesión y colaborar. Esto puede hacerse al ir a **Conexiones > Sesiones**, hacer clic en Colaborar al lado de la sesión activa requerida. La colaboración de sesiones será especialmente útil para la resolución de problemas, ya que todos los usuarios serán capaces de controlar el cursor del mouse y trabajar de forma colaborativa en la misma sesión RDP o SSH. En el caso de detectar cualquier actividad sospechosa, usted puede terminar la sesión inmediatamente para evitar cualquier abuso de acceso privilegiado. Esto se puede hacer al ir a **Auditoría > Sesiones de usuarios**, hacer clic en **Terminar** al lado de la sesión requerida.

11.2 Grabar toda sesión privilegiada

Predeterminadamente, Access Manager Plus graba todas las sesiones RDP, VNC, SSH y SQL iniciadas desde la aplicación. Recomendamos que configure la grabación de sesiones para todas las sesiones privilegiadas y personalice la ubicación de almacenamiento externo al ir a Administrador > Ajustes de sesión > Grabación de sesión. Todas las sesiones grabadas se mostrarán en Conexiones> Sesiones > Completadas. Usted puede seguir las sesiones usando cualquier detalle, como el nombre de la conexión, el usuario que inició la sesión o la hora en que se lanzó la sesión.



11.2 Configurar la grabación de sesiones para conexiones RDP, VNC, SSH y SQL

11.3 Depuración regular de sesiones grabadas

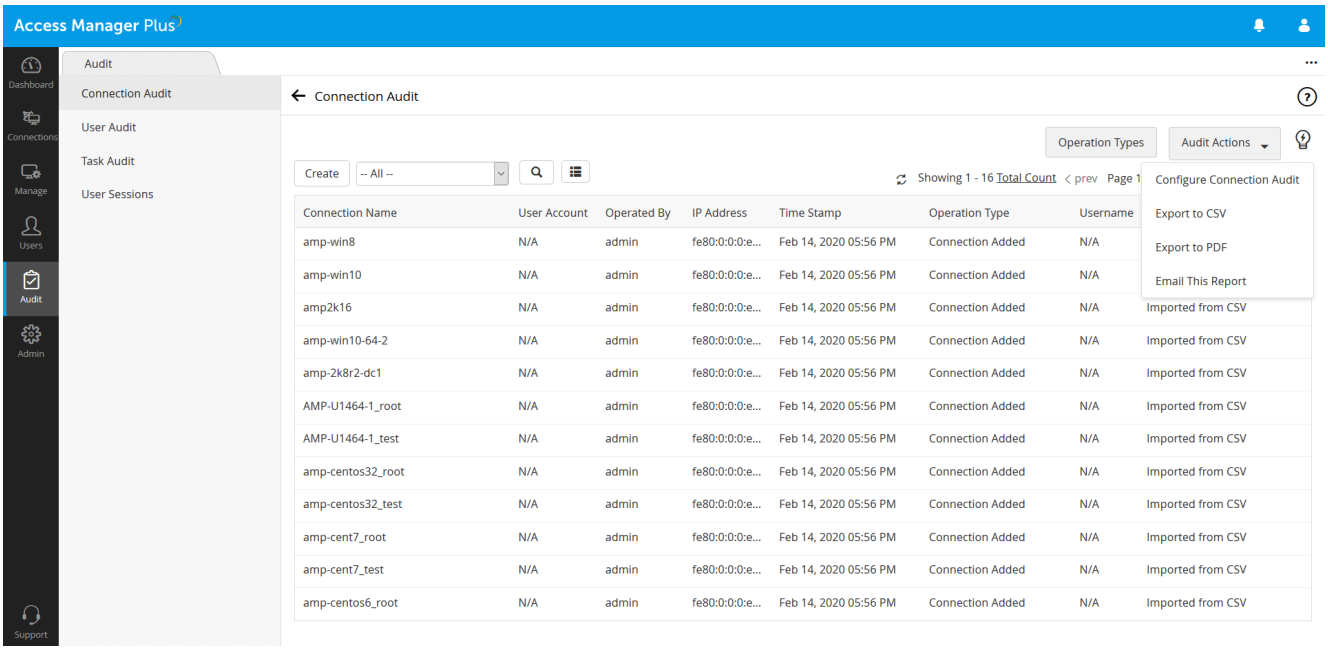
Si su organización es grande y tiene un amplio abanico de recursos para los cuales la grabación de sesiones está habilitada, las sesiones grabadas crecerán naturalmente a una tasa más rápida. Si no necesita grabaciones anteriores a un número especificado de días, le recomendamos eliminarlas para mantener libre el espacio en disco. Asimismo, puede almacenar estas grabaciones en el disco local, de forma que pueda pasarlas a otros lugares. Si desea eliminar una sesión específica o el historial de chat de una sesión particular, puede hacerlo al ir a **Administrador > Ajustes de sesión > Grabación de sesión > Eliminar sesiones guardadas**. Para eliminar las grabaciones anteriores a un número específico de días, ingrese el número en **Eliminar sesiones guardadas anteriores a _ días**. Puede deshabilitar la eliminación al dejar el campo de texto vacío o al ingresar "0" como valor.

12

Auditorías

12.1 Facilitar las auditorías internas regulares

Use las pistas de auditorãa de Access Manager Plus para registrar instantÄneamente todos los eventos alrededor de las cuentas privilegiadas, intentos de inicio de sesiên y tareas programadas o completadas. Con estos datos usted puede facilitar auditorãas internas regulares e investigaciones forenses, descubrir fÄcilmente quián accede a quá recurso, dênde y cuÄndo.



12.1 Pistas de auditoría basadas en conexiones en Access Manager Plus

12.2 Controlar actividades seleccionadas con alertas instantáneas

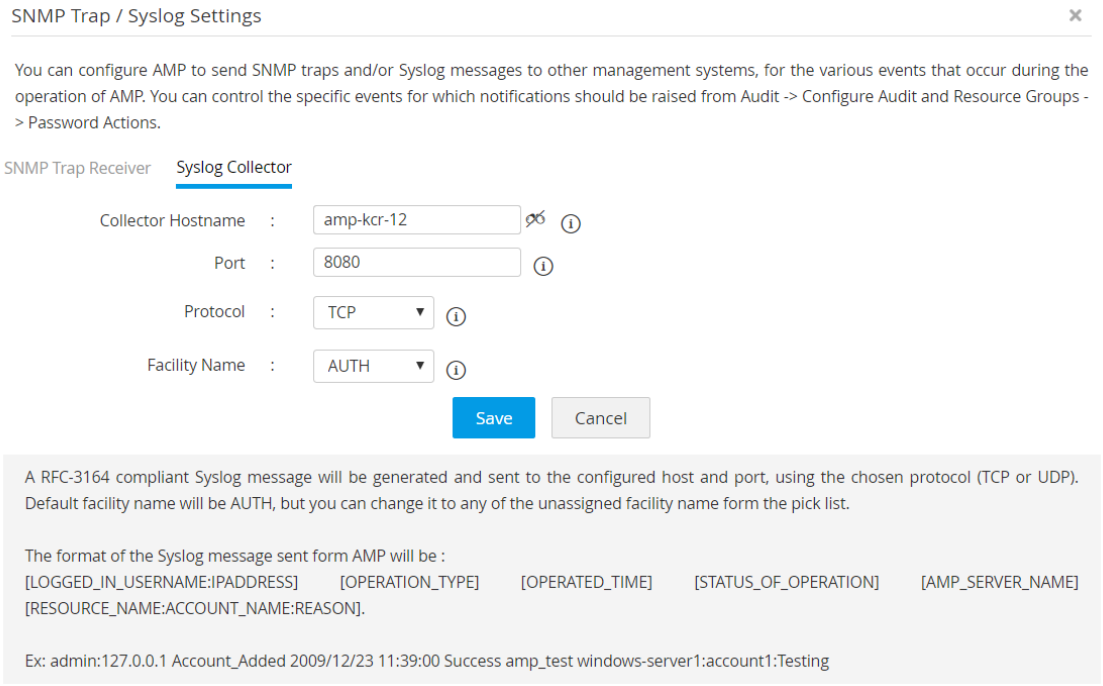
Access Manager Plus también le permite enviar notificaciones por correo electrónico instantáneas a receptores elegidos cuando ciertos eventos tengan lugar. Esta opción es muy útil para permanecer siempre al tanto de lo que sus usuarios están haciendo. Le recomendamos que configure alertas para operaciones importantes, como adición de nuevos usuarios, eliminación de conexión y más. Se pueden habilitar las alertas por correo electrónico al ir a Auditoría > Auditoría de conexión (por ejemplo) > Acciones de auditoría > Configurar auditoría.

12.3 Optar por un resumen diario de correos electrónicos para evitar la saturación de la bandeja de entrada

Si ha habilitado alertas y actualizaciones para un número de conexiones, puede que la bandeja de entrada se vea inundada con correos electrónicos de notificaciones. En el caso de que esto suceda, usted puede escoger recibir un resumen diario por correo electrónico al final de cada día con una lista consolidada de notificaciones si las actualizaciones cada hora no son prioritarias.

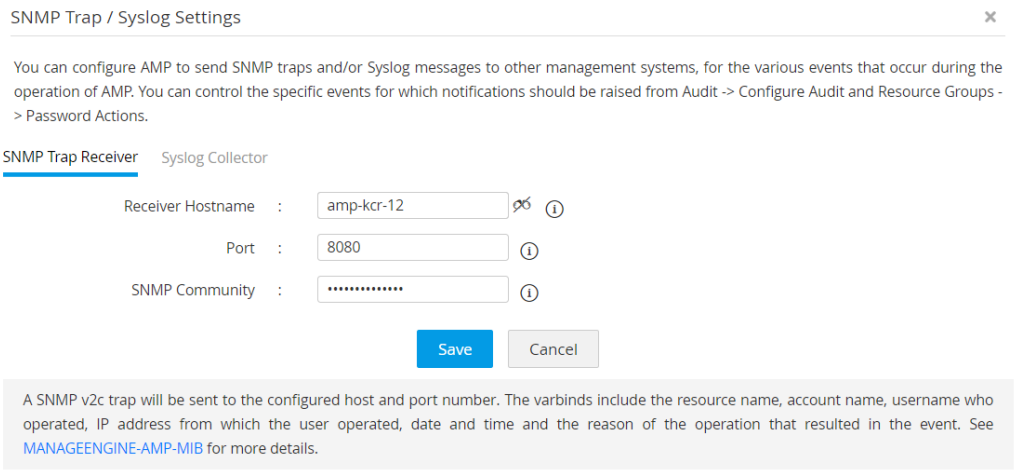
12.4 Enviar mensajes de syslog y SNMP traps a sus sistemas de gestión de eventos y red

Si usa una herramienta de SIEM externa en su organización, puede integrarla con Access Manager Plus para enviar mensajes de syslog para varios eventos que se dan durante el funcionamiento de Access Manager Plus. Puede hacer esto al ir a **Administrador > Ajustes de sesión > Ajustes de SNMP Traps / Syslog**. Puede controlar los eventos específicos para los cuales se deben generar notificaciones en **Auditoría > Configurar auditoría.**



12.4.1 Configurar mensajes syslog

También puede integrar su herramienta de gestión de redes con Access Manager Plus para recibir SNMP traps. Esto lo ayudará a adquirir una perspectiva holística del acceso privilegiado, junto con la actividad general de la red, desde una ubicación central.



12.4.2 Configurar SNMP traps

12.5 Depurar registros de auditoría

Naturalmente, cuando se audita cada operación, los registros de auditoría crecen a una tasa más rápida. Si no necesita registros de auditoría anteriores a un número específico de días, puede eliminarlos. Esto se puede configurar al ir a **Auditoría > Auditoría de conexión (por ejemplo) > Acciones de auditoría > Configurar auditoría > Eliminar registros de auditorías de conexión**. Predeterminadamente, la opción de eliminar se deshabilitará al establecer los días en cero (0).

13

Redundancia y recuperación de datos

13.1 Establecer la recuperación ante desastres

Los datos almacenados en la base de datos de Access Manager Plus son de importancia crítica. En el evento improbable de un error de configuración de producción, se podrían perder todos los datos. Por tanto, la recuperación ante desastres es esencial. La aplicación tiene opciones para respaldar datos en tiempo real y periódicamente de forma automatizada mediante tareas programadas. Escoja el método que mejor se ajuste a su organización. Asimismo, garantice que el directorio de destino configurado para el respaldo se encuentra en una ubicación segura.

14

Mantenimiento

14.1 Mantener su instalación actualizada

El equipo de Access Manager Plus libera regularmente paquetes de actualizaciên que contienen mejoras y correcciones. Idealmente las actualizaciones importantes se liberan una vez cada trimestre, mientras que las mejoras menores pueden anunciarse mensualmente. Estos paquetes de actualizaciên también contendrÄn actualizaciones del servidor web Tomcat, la base de datos PostgreSQL y JRE que vienen integrados con el producto. Para mantener adecuadamente su instalaciên de Access Manager Plus y asã obtener un rendimiento êptimo, le recomendamos que descargue e instale los paquetes de actualizaciên para Access Manager Plus como y cuando se liberen.

Actualizar el SO de Windows donde se instale Access Manager Plus:

Cuando tiene parches de Windows por instalar en el servidor de Access Manager Plus, realice los siguientes pasos:

1. Abra la consola Servicios (services.msc) y detenga el servicio Access Manager Plus.
2. Realice una copia de todo el directorio de Access Manager Plus y almacénelo en otro equipo como respaldo. Si el servidor es un equipo virtual, solo tome una instantánea.
3. Ahora, actualice el SO de Windows. Puede consultar esta documentación como guía.

14.2 Escoger su ventana de mantenimiento sabiamente

Con el fin de aplicar los paquetes de actualizaciên, Access Manager Plus debe detenerse temporalmente. Por tanto, le recomendamos mucho programar la ventana de mantenimiento durante los fines de semanas u horas no laborales. Si no puede evitar realizar una actualizaciên durante las horas laborales, puede alertar a sus usuarios antes sobre la inminente operaciên de mantenimiento.

14.3 Buscar asesorías en seguridad

Si se descubre alguna vulnerabilidad de seguridad en el producto, se dan correcciones inmediatamente a travás de los paquetes de actualizaciên. Se envãa también una asesorãa de seguridad al cliente a la direcciên de correo electrênico que registrê con nosotros. Vigile la direcciên de correo electrênico para que no se pierda ninguna asesorãa nuestra. Cuando reciba una, actïe como se aconseja en el correo electrênico.

14.4 Pasar la instalación de Access Manager Plus de un equipo a otro

Para pasar la instalaciên de Access Manager Plus de un equipo a otro, realice el siguiente procedimiento detallado.

1. Detenga el servicio Access Manager Plus en la consola de servicios si estÄ en ejecuciên.
2. Copie toda la carpeta de instalaciên de Access Manager Plus de un equipo a otro.
3. Instale Access Manager Plus en el nuevo equipo para ejecutarlo como servicio. En esta opciên, no podrÄ desinstalar el programa mediante Windows o aèadir o eliminar la consola de programas. Si desea reinstalarlo en cualquier momento, elimine toda la carpeta de instalaciên.

Para más información, consulte esta sección de nuestra documentación de ayuda.

Nota:

No elimine la instalación existente de Access Manager Plus hasta asegurarse de que la nueva instalación funciona bien. Esto garantiza que tendrá un respaldo válido listo en caso de que necesite sobreponerse ante desastres o haya una corrupción de datos durante el movimiento.