ManageEngine
ADAudit Plus

Un auditor de cambios centrado en el UBA

Haga que su Active Directory, servidores de Windows, servidores de archivos y estaciones de trabajo estén seguros y conformes

www.adauditplus.com

¿Qué es ADAudit Plus?

ManageEngine ADAudit Plus es un software de auditoría e informes de cambios en tiempo real que puede:

- **Monitorear su Active Directory (AD), Azure AD, servidores de archivos de Windows, servidores miembros y estaciones de trabajo, y ayudarlo a cumplir con las regulaciones como HIPAA, GDPR, SOX, CCPA y GLBA, entre otras**
- **Transformar los datos del log de eventos ruidosos y sin procesar en informes procesables que le muestren quién hizo qué, cuándo y desde qué parte de su entorno de Windows con solo unos pocos clics**
- **Identificar actividades anómalas y detectar amenazas potenciales para su empresa utilizando las funciones de análisis del comportamiento de los usuarios (UBA)**

Cómo ADAudit Plus puede ayudar a su organización

Con ManageEngine ADAudit Plus, puede:

1. **Ver informes detallados sobre los cambios realizados en Azure AD y on-premises**
2. **Visualizar la actividad de inicio de sesión de los usuarios de Windows**
3. **Generar informes, analizar y solucionar los problemas de bloqueos de cuentas de AD**
4. **Monitorear de cerca las actividades de los usuarios privilegiados en su dominio**
5. **Rastrear los inicios de sesión / cierres de sesión, cambios a usuarios, grupos, etc.**
6. **Auditar la actividad de archivos en Windows, NetApp, EMC y el almacenamiento de Synology**
7. **Mejorar la detección de amenazas usando la función de análisis del comportamiento de los usuarios (UBA)**
8. **Obtener informes de auditoría preempaquetados para SOX, HIPAA, PCI DSS, GDPR y otras regulaciones**

Funciones destacadas de ADAudit Plus

1. **Informes y auditoría de cambios de AD y Azure AD**
2. **Auditoría del servidor de archivos (Windows, NetApp, EMC, Synology)**
3. **Auditoría de los cambios en los ajustes de la directiva de grupo**
4. **Auditoría e informes del servidor de Windows y del servidor miembro**
5. **Auditoría de las estaciones de trabajo**
6. **Análisis del comportamiento de los usuarios (UBA)**
7. **Monitoreo de usuarios privilegiados**

Auditoría de Active Directory

Informe sobre los cambios realizados en los objetos de AD y GPO; rastree la actividad de inicio de sesión de los usuarios, analice los bloqueos de cuentas y mucho más

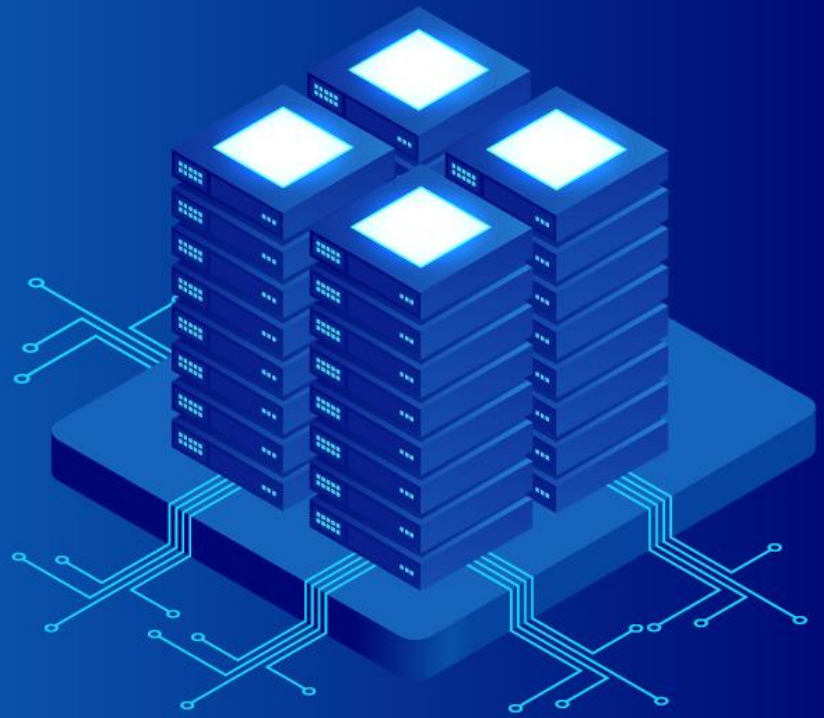
www.adauditplus.com

Auditoría de AD

- **Audite todos los cambios de los objetos de AD:** Supervise los cambios realizados en las unidades organizativas, usuarios, grupos, equipos y otros objetos de AD con detalles como los valores nuevos y anteriores de los atributos modificados
- **Supervise los cambios en la configuración de los GPO:** Audite los cambios realizados en los GPO y sus ajustes, incluidos los cambios en la configuración del equipo, la contraseña y los cambios en la política de bloqueo de cuentas, etc.
- **Monitoree la actividad de inicio de sesión del usuario:** Obtenga informes detallados sobre los intentos de inicio de sesión exitosos y fallidos de los usuarios
- **Solucione problemas relacionados con el bloqueo de cuentas:** Detecte los bloqueos de cuentas rápidamente con alertas e identifique la fuente a partir de una extensa lista de componentes de Windows
- **Obtenga visibilidad sobre el uso de privilegios:** Monitoree de cerca el uso de privilegios en su empresa auditando continuamente las cuentas de usuarios privilegiados y manteniendo una pista de auditoría detallada
- **Audite el entorno de AD híbrido:** Obtenga una vista única y correlacionada de todas las actividades que suceden en los entornos híbridos con alertas para los eventos críticos

Auditoría del servidor de archivos

Audite e informe sobre los accesos a archivos y modificaciones en dispositivos de almacenamiento de Windows, NetApp, EMC y Synology



www.adauditplus.com

Auditoría del servidor de archivos

- **Monitoree los accesos a archivos y carpetas:** Supervise toda la actividad de los archivos en tiempo real, incluidos leer, eliminar, modificar, copiar y pegar, mover y mucho más
- **Detecte intentos fallidos de acceso a archivos:** Reciba informes sobre los intentos fallidos para acceder a archivos o carpetas
- **Audite los cambios de permisos:** Supervise los cambios en los permisos de NTFS y uso compartido junto con detalles como sus valores nuevos y anteriores
- **Monitoree la integridad de archivos:** Detecte fácilmente eventos críticos, como los cambios realizados en un archivo específico, por un usuario en particular, o más con alertas por correo electrónico y SMS sobre estos eventos
- **Audite los archivos compartidos:** Supervise cada acceso y cambio realizado en las carpetas y archivos compartidos en su dominio con detalles sobre quién accedió a qué, cuándo y desde dónde

Auditoría de los cambios en los ajustes de la directiva de grupo

Audite los cambios realizados en los ajustes de la directiva de grupo, incluidos los cambios en la política de bloqueo de cuentas y contraseñas, cambios en la computadora, etc.

Auditoría de los cambios en los ajustes de la directiva de grupo

- **Audite los objetos de directiva de grupo:** Audite y genere informes sobre la creación, eliminación, modificación y más de los objetos de directiva de grupo (GPO)
- **Supervise los cambios en los ajustes de los GPO:** Monitoree de cerca quién cambia qué ajustes de los GPO, cuándo y desde dónde con informes completos
- **Configure alertas para los cambios críticos:** Reciba alertas instantáneas por correo electrónico y SMS para los cambios críticos, como cambios en la configuración de la computadora, cambios en la política de bloqueo de cuentas y contraseñas, etc.
- **Mantenga una pista de auditoría:** Genere informes sobre los valores de los ajustes de GPO antes y después de cada cambio para detectar instantáneamente los cambios no deseados

Auditoría del servidor de Windows

Monitoree los servidores miembros con informes y alertas en tiempo real para vigilar de cerca la actividad en su red de Windows

www.adauditplus.com

Auditoría del servidor de Windows

- **Audite los servidores de Windows:** Monitoree los cambios en las membresías de grupos administrativos locales, usuarios locales, derechos de usuario, políticas locales y mucho más
- **Supervise las tareas y los procesos programados:** Audite la creación, eliminación y modificación de tareas y procesos programados
- **Monitoree el uso de dispositivos extraíbles:** Identifique los complementos USB y las actividades de transferencia de archivos a dispositivos de almacenamiento extraíbles
- **Audite los procesos de PowerShell:** Monitoree los procesos de PowerShell que se ejecutan en sus servidores de Windows junto con los comandos ejecutados en ellos
- **Audite los servicios de federación de AD (ADFS):** Genere informes sobre los intentos de autenticación ADFS exitosos y fallidos en tiempo real

Auditoría de estaciones de trabajo

Haga un seguimiento de la información de inicio y cierre de sesión de los usuarios, horas productivas, detalles del historial de inicio de sesión, uso de almacenamiento extraíble y mucho más

Auditoría de estaciones de trabajo

- **Audite la actividad de inicio y cierre de sesión:** Supervise la actividad de inicio y cierre de sesión en su red de Windows, registre la duración de la sesión e identifique a los usuarios que actualmente están conectados
- **Rastree el historial de inicio de sesión de los usuarios:** Registre cada actividad de inicio de sesión, identifique a los usuarios que hayan iniciado sesión en varios equipos, monitoree los inicios de sesión RADIUS y mucho más
- **Identifique los inicios de sesión fallidos:** Realice un seguimiento de todos los intentos de inicio de sesión fallidos con información sobre quién intentó iniciar sesión, en qué equipo intentó iniciar sesión, cuándo y el motivo de la falla
- **Monitoree la integridad de los archivos:** Reciba informes detallados sobre todos los cambios realizados en los archivos del sistema y del programa
- **Mida la productividad de los empleados:** Supervise el tiempo de inactividad de los empleados y las horas de trabajo reales para garantizar una alta productividad en toda su empresa

Análisis del comportamiento de los usuarios

Detecte y mitigue las amenazas como inicios de sesión maliciosos, movimientos laterales, abuso de privilegios, violaciones de datos y malware

www.adauditplus.com

Cacería de amenazas con UBA

- **Procese logs de todo su entorno:** Recopile y procese logs de los DC, servidores miembros y estaciones de trabajo configurados
- **Identifique una línea de base segura:** Los datos de log procesados se utilizan para crear una línea de base específica del usuario para las actividades normales de inicio de sesión, archivo, gestión de usuarios y procesamiento
- **Identifique anomalías y alerte a los administradores:** Los datos de log entrantes y las líneas de base procesadas se comparan para detectar anomalías y notificar a los administradores, para que puedan investigar más a fondo
- **Detecte posibles amenazas de seguridad:** Detecte rápidamente los posibles casos de inicios de sesión maliciosos, abuso de privilegios, escalamiento de privilegios, robo de datos, ataques de malware y mucho más
- **Automatice las respuestas a incidentes:** Reduzca el tiempo que lleva mitigar el daño apagando instantáneamente los dispositivos, cerrando las sesiones de los usuarios o más en función del incidente de seguridad

Monitoreo de usuarios privilegiados

Audite las cuentas de usuarios privilegiados en su dominio y mantenga una pista de auditoría para detectar rápidamente los comportamientos sospechosos

www.adauditplus.com

Monitoreo de usuarios privilegiados

- **Audite la actividad del administrador:** Supervise las acciones administrativas del usuario en el esquema de Active Directory (AD), la configuración, los usuarios, los grupos, las unidades organizativas (OU), los objetos de directiva de grupo (GPO) y mucho más

- **Revise la actividad de los usuarios privilegiados:** Cumpla con varias regulaciones de TI al mantener una pista de auditoría de las actividades realizadas por los usuarios privilegiados en su dominio

- **Detecte el escalamiento de privilegios:** Identifique el escalamiento de privilegios con informes que documenten el uso de privilegios por primera vez de los usuarios y verifique si son necesarios para el rol y las obligaciones del usuario

- **Detecte anomalías de comportamiento:** Identifique las acciones que se desvíen de los patrones de acceso normales para encontrar los atacantes que usan credenciales robadas o compartidas de cuentas privilegiadas

- **Reciba alertas sobre actividades sospechosas:** Detecte y responda rápidamente frente a los eventos críticos, como la eliminación de logs de auditoría o el acceso a datos críticos fuera del horario comercial, al configurar alertas

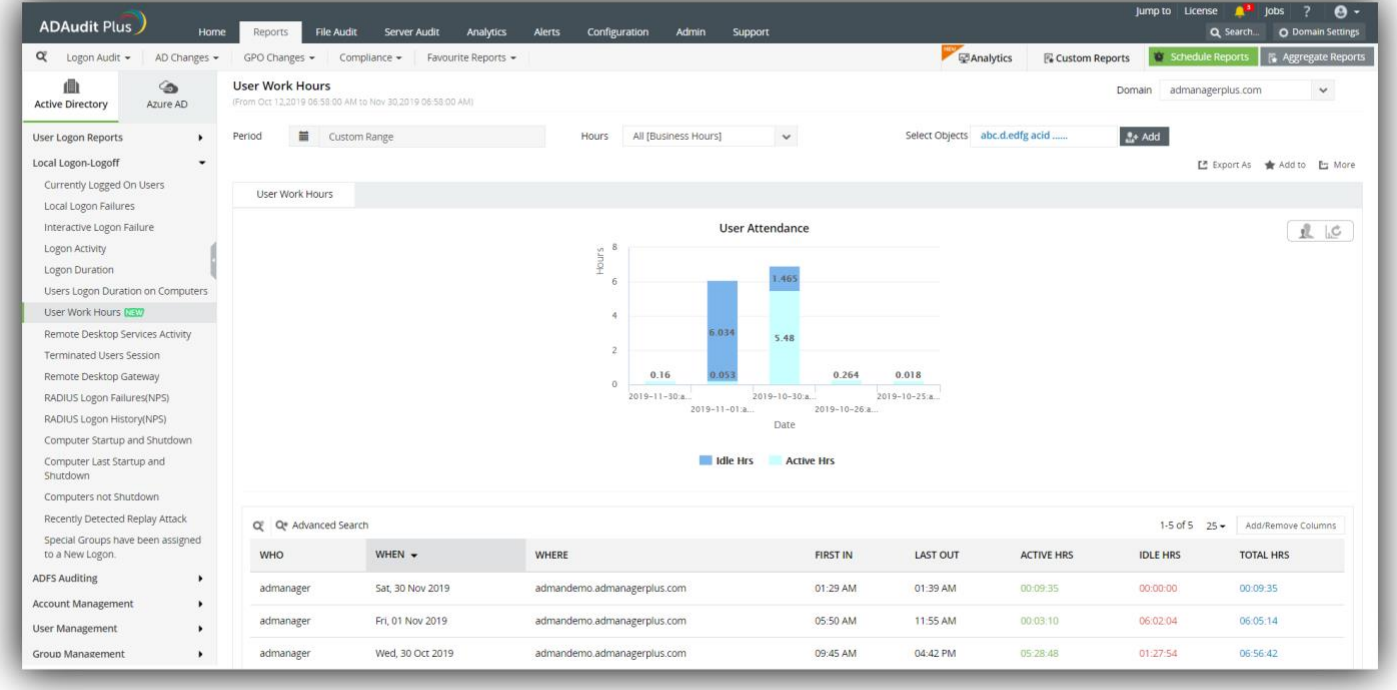
Funciones más populares

Una vista general de las funciones que aman nuestros clientes

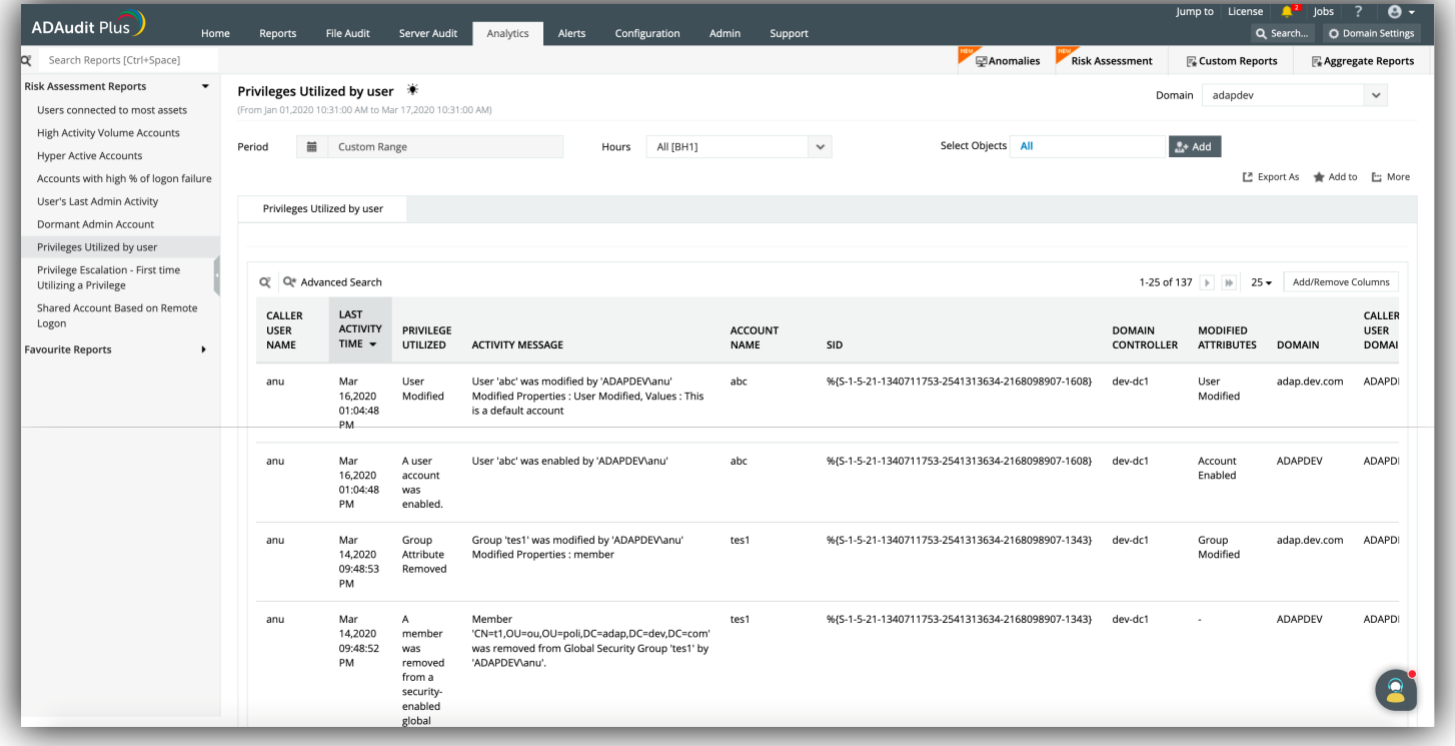
www.adauditplus.com

Más funciones que adoran nuestros clientes

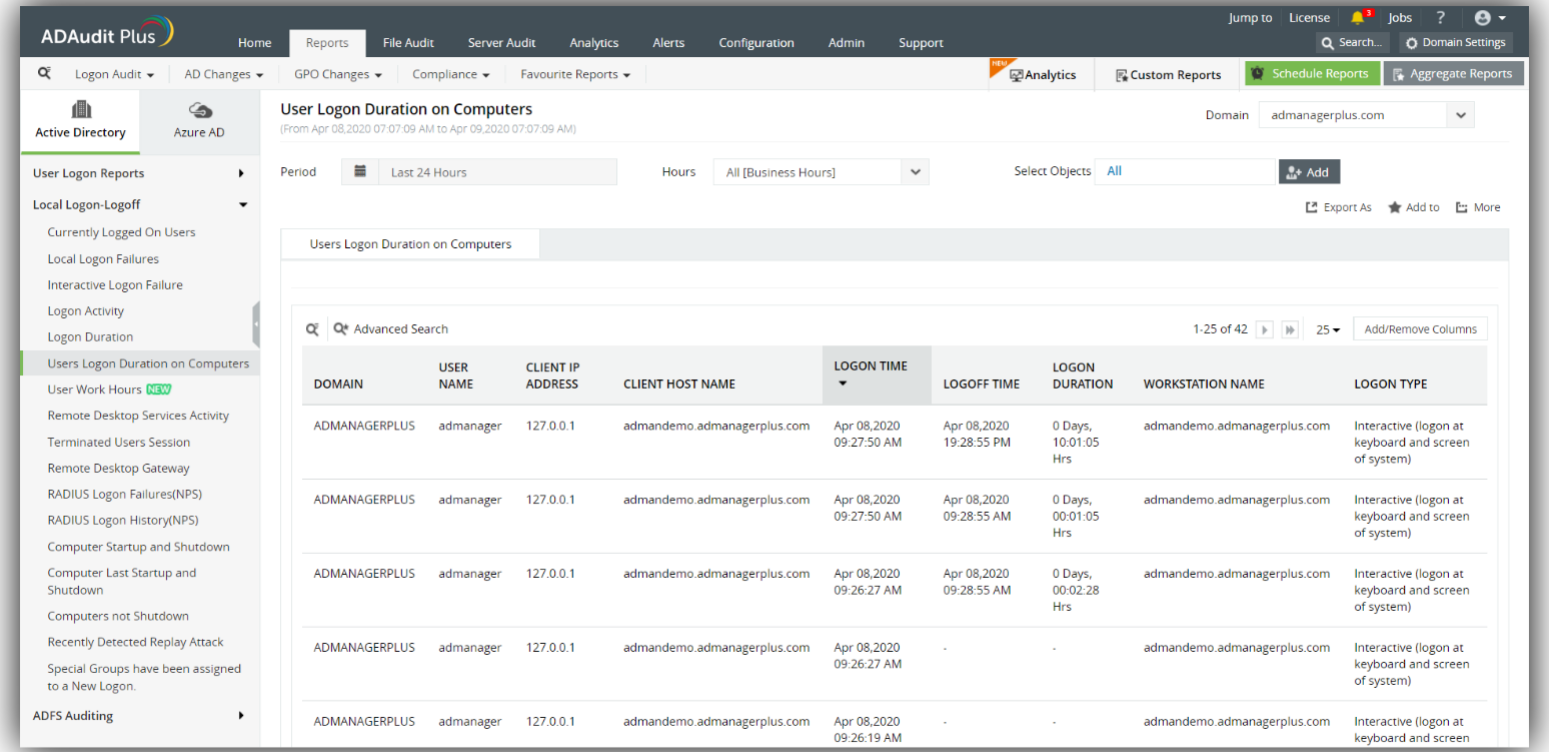
- **Monitoreo de las horas laborales de los usuarios:** Supervise la asistencia, las horas activas, las horas inactivas y las horas productivas de los empleados que usan cualquier computadora dentro de su entorno



- **Detección de amenazas internas:** Detecta al instante indicadores de amenazas internas como inicios de sesión maliciosos, abuso de privilegios, movimientos laterales, uso indebido de datos y mucho más



- **Seguimiento de los inicios / cierres de sesión:** Obtenga información específica del usuario sobre las acciones de inicio y cierre de sesión, vea qué usuarios han iniciado sesión en varias computadoras y vea las direcciones IP y los tiempos de inicio de sesión



Por qué se destaca ADAudit Plus

- **Alertas instantáneas:** Reciba notificaciones instantáneas por correo electrónico y SMS sobre los eventos o actividades críticas por parte de un usuario crítico

- **Detección y respuesta a amenazas:** El motor de UBA detecta rápidamente el abuso de privilegios, ataques internos, malware y otras amenazas, y ejecuta respuestas personalizadas

- **Más de 250 informes:** Optimice el cumplimiento de varias regulaciones, incluidas PCI DSS, HIPAA, SOX, GDPR, GLBA, ISO 27001 y más con informes listos para auditoría

- **Archivado de logs y análisis forense:** Archive los datos de auditoría en una ubicación definida por el usuario y genere informes basados en esos datos cuando sea necesario

- **Equipo de atención al cliente de primer nivel:** Nuestro equipo de asistencia está a solo un correo electrónico, llamada telefónica o chat de distancia

Plataformas compatibles

Auditoría de servidores miembro y DC	Auditoría de archivos	Otros componentes
Versiones de Windows Server: • **2003/2003 R2** • **2008/2008 R2** • **2012/2012 R2** • **2016/2016 R2** • **2019**	• **Auditoría del servidor de Windows: Windows Server 2003 y superior** • **Auditoría de EMC: VNX, VNXe, Celerra, Unity, Isilon** • **Auditoría de Synology: DSM 5.0 y superior** • **Auditoría del archivador NetApp: Datos ONTAP 7.2 y superior** • **Auditoría del cluster de NetApp: Datos ONTAP 8.2.1 y superior**	• **Auditoría de AD FS: AD FS 2.0 y superior** • **Auditoría de estaciones de trabajo: Windows 10, 8, 7, Vista y XP** • **Auditoría de PowerShell: PowerShell versión 4.0, 5.0**

Versiones disponibles

Standard	Professional	Gratuita
Descargar una prueba gratuita de 30 días	Descargar una prueba gratuita de 30 días	Descargar versión gratuita
Informes y alertas sobre los datos del log de eventos recopilados de los siguientes componentes con licencia: • Controladores de dominio • Inquilinos de Azure AD • Servidores Windows • Estaciones de trabajo • Servidores de archivos de Windows • Servidores NAS de Synology • Archivadores de NetApp • Servidores de archivos EMC	Incluye todas las funciones de la versión Standard, más: • Análisis de bloqueo de cuentas • Control de los cambios en los ajustes de la directiva de grupo • Los valores nuevos y anteriores de los cambios del objeto / atributo de AD • Auditoría de los cambios de permisos de AD • Control de cambios de DNS • Control de cambios de configuraciones, esquema de AD, etc.	Incluye todas las funciones de la versión Professional durante 30 días a partir de la fecha de instalación. Además: • Nunca expira • Proporciona informes de auditoría para hasta 25 estaciones de trabajo • Permite generar informes para los datos del log de eventos recopilados durante el período de evaluación / licencia

Detalles de la licencia

La licencia de ADAudit Plus para el componente de Auditoría de Active Directory se basa en la cantidad de controladores de dominio.

Otros add-ons se basan en la cantidad de:

- **Inquilinos de Azure AD**
- **Servidores de archivos**
- **Servidores de archivos EMC / Archivadores NetApp / Servidores Synology NAS**
- **Servidores miembros**
- **Estaciones de trabajo**

Asistencia para la evaluación

Podemos ayudarlo de varias maneras durante su evaluación de ADAudit Plus. Esto incluye:

- **Una prueba gratuita de 30 días completamente funcional**
- **Extensión de la licencia de evaluación, si es necesario**
- **Soporte técnico 24x5 y opciones de demostración guiada**
- **Una demostración en vivo alojada en demo.adauditplus.com**
- **Guías detalladas de instalación y configuración**
- **Una amplia base de conocimiento**

Nueve de cada diez compañías de Fortune 100 confían en nosotros para gestionar su TI

Y tenemos las credenciales para demostrarlo

ADAudit Plus fue nombrado como la Elección de los Clientes para SIEM de Gartner Peers Insights 2019

ManageEngine
ADAudit Plus

Gartner
peerinsights
customers'
choice™

Testimonios de los clientes

Una buena solución basada en la web y rentable. Nos gusta la opción de auditoría en el archivador NetApp. Además, en parte tiene que ver con nuestra satisfacción con otros productos en los que se destaca ManageEngine.

Ricky Chand

Ingeniero de Sistemas, Banco del Pacífico Sur, Fiji

Antes de ADAudit Plus, no podíamos ver nuestra infraestructura de AD. Ahora podemos monitorear todas las transacciones de AD en cuanto a cambios de grupo, creación de usuarios, seguridad, logs de autenticación y mucho más.

Calixto Muanya,

Administrador de Windows, Harvard Medical School

Detalles de contacto

Teléfono

+ 1-925-924-9500

Equipo comercial

latam-sales@manageengine.com

Visite nuestra página

www.manageengine.com/latam/

Dirección

ZOHO Corporation 4141 Hacienda Drive, Pleasanton, CA 94588, EE. UU.