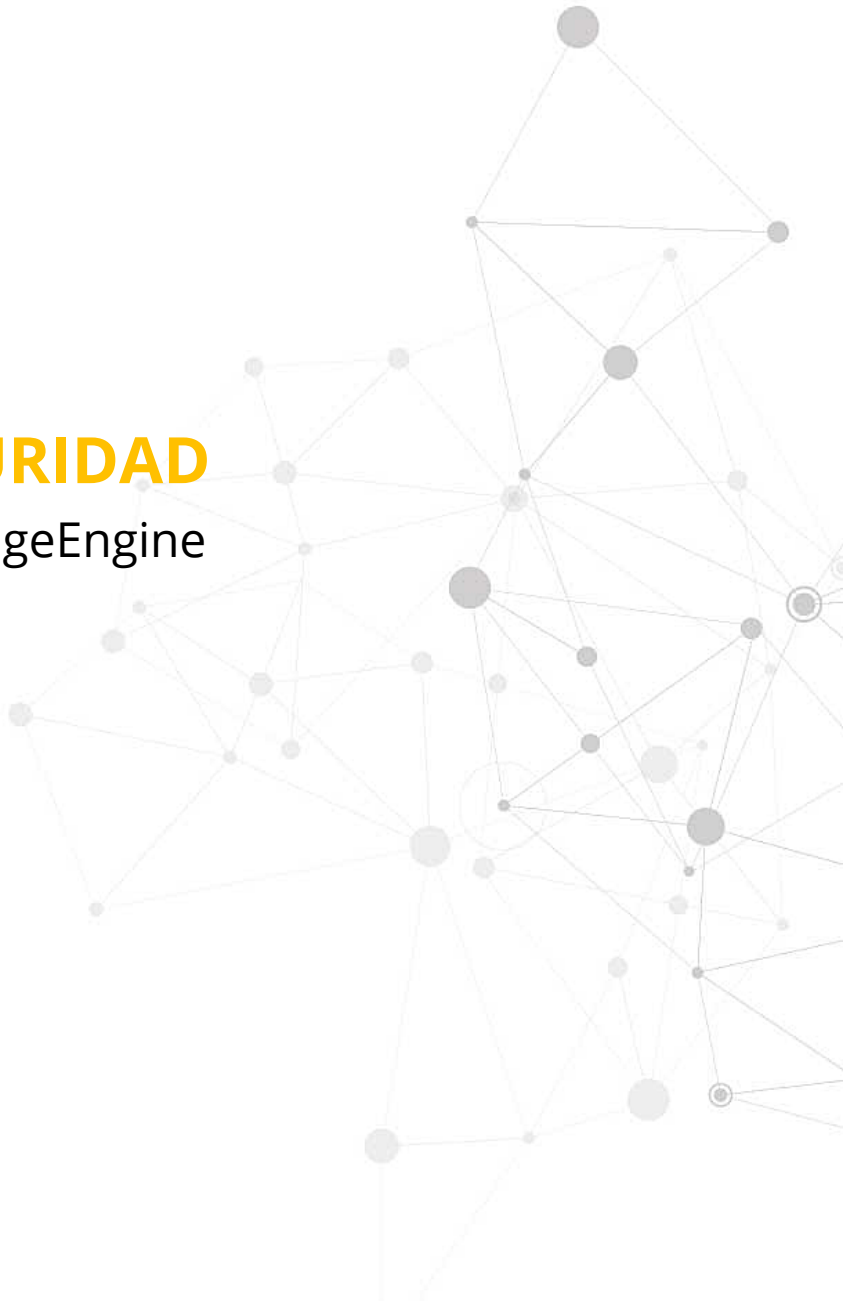
POLÍTICA DE SEGURIDAD

Productos ITOM de ManageEngine



https://www.manageengine.com/latam/herramientas-de-gestion-de-operaciones-ti.html

Índice

I. Seguridad de la información

ManageEngine, la división de software de gestión de TI empresarial de Zoho Corp., cuenta con un sistema de gestión de la seguridad de la información (ISMS) que tiene en cuenta nuestros objetivos de seguridad, así como los riesgos y la mitigación que afectan a todas las partes interesadas. Empleamos políticas y procedimientos estrictos que abarcan la seguridad, la disponibilidad, el procesamiento, la integridad y la confidencialidad de los datos de los clientes.

A. Verificación de los antecedentes de los empleados:

Cada empleado se somete a un proceso de verificación de antecedentes. Contratamos a agencias externas de gran reputación para que realicen esta verificación en nuestro nombre. Hacemos esto para verificar sus antecedentes penales, sus empleos anteriores si los hay, y sus antecedentes educativos. Hasta que no se realice esta comprobación, no se asignan al empleado tareas que puedan suponer un riesgo para los usuarios.

B. Concienciación sobre la seguridad:

Cada empleado, cuando se incorpora, firma un acuerdo de confidencialidad y una política de uso aceptable, después de lo cual recibe capacitación en seguridad de la información, privacidad y conformidad. Además, evaluamos su comprensión a través de pruebas y exámenes para determinar los temas en los que necesitan más capacitación. Proporcionamos capacitación sobre aspectos específicos de la seguridad que pueden requerir de acuerdo a sus roles. Educamos continuamente a nuestros empleados sobre la seguridad de TI, la privacidad y la conformidad en nuestra comunidad interna, donde nuestros empleados se registran regularmente para mantenerlos actualizados sobre las prácticas de seguridad de la organización. También organizamos eventos internos para concienciar e impulsar la innovación en seguridad y privacidad.

C. Personal dedicado a la seguridad y a la privacidad:

Tenemos empleados dedicados a la seguridad y la privacidad que implementan y gestionan nuestros programas de seguridad y privacidad. Regulan y mantienen los sistemas de defensa, desarrollan procesos de revisión de la seguridad y monitorean constantemente nuestras redes para detectar actividades sospechosas. Proporcionan servicios de consultoría y orientación específicos para nuestros equipos de ingeniería.

D. Auditoría interna y conformidad:

Tenemos un equipo de conformidad dedicado a examinar los procedimientos y políticas en ManageEngine para alinearlos con las normas y determinar qué controles, procesos y sistemas son necesarios para cumplir las normas. Este equipo también realiza auditorías internas periódicas y facilita la realización de auditorías y evaluaciones independientes por parte de terceros. Zoho ha obtenido las siguientes certificaciones para Aplicaciones, Sistemas, Personas, Tecnología y Procesos:

IS 642819

ISO/IEC 27001

- ISO 27001 (formalmente conocida como ISO/IEC 27001:2005) es una especificación para un sistema de gestión de la seguridad de la información (ISMS). Un ISMS es un marco de políticas y procedimientos que incluye todos los controles legales, físicos y técnicos que intervienen en los procesos de gestión del riesgo de la información de una organización.

PM 732705

ISO/IEC 27701

- La norma ISO/IEC 27701 es una extensión de las normas ISO/IEC 27001 e ISO/IEC 27002 para la gestión de la privacidad en el contexto de la organización. La norma de certificación está diseñada para mejorar el Sistema de Gestión de la Seguridad de la Información (ISMS) existente con requisitos adicionales para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de la Información sobre la Privacidad (PIMS). Esta norma permite a las organizaciones demostrar el cumplimiento de las distintas normativas de privacidad de todo el mundo que les son aplicables.

- Zoho cumple con la norma SOC 2 Tipo II. La SOC 2 es una evaluación del diseño y la efectividad operativa de los controles que cumplen los criterios de los Principios de Servicios Fiduciarios de la AICPA.

- Los informes de Signal spam ayudan a proporcionar datos de FBL, principalmente información técnica para la identificación de los spammers y el abuso de marketing, de los principales ISP como Orange.fr, SFR.fr, etc. Dispone de numerosos plug-ins de notificación de spam para navegadores y clientes de correo electrónico de terceros, enfocados a las comunidades francesas de todo el mundo. Es importante, tanto para Zoho Corporation como para nuestros clientes, conocer a todos los destinatarios que marcan o denuncian los correos electrónicos que reciben como "spam", para que podamos eliminarlos de las listas. Por lo tanto, esta certificación protege la reputación de nuestra red en la región francesa.

Las certificaciones mencionadas anteriormente son aplicables a todos los productos ITOM de ManageEngine. Para más detalles, consulte nuestro portafolio de conformidad.

E. Seguridad de Endpoints:

Todas las estaciones de trabajo entregadas a los empleados de ManageEngine tienen versiones actualizadas del sistema operativo y están configuradas con software antivirus. Están configuradas de tal manera que cumplen con nuestros estándares de seguridad, que requieren que todas las estaciones de trabajo estén correctamente configuradas, parcheadas y que sean supervisadas y monitoreadas por las soluciones de gestión de endpoint de ManageEngine. Estas estaciones de trabajo son seguras por defecto, ya que están configuradas para cifrar los datos en reposo, tienen contraseñas seguras y se bloquean cuando están inactivas. Los dispositivos móviles utilizados con fines empresariales se registran en el sistema de gestión de dispositivos móviles para garantizar que cumplan con nuestras normas de seguridad.

II. Seguridad de las aplicaciones

A. Seguro por diseño:

Nos adherimos a las directrices de codificación segura del ciclo de vida del desarrollo de software (SDLC) y estas directrices se comparten con todos los desarrolladores. Como siguiente paso, examinamos los cambios de código para buscar posibles problemas de seguridad, en primer lugar, revisándolos manualmente y, en segundo lugar, utilizando nuestro analizador de código y las herramientas de análisis de vulnerabilidades. Todo este proceso se lleva a cabo antes del lanzamiento de cualquier función. Si se encuentra algún problema, se comprueba y se corrige inmediatamente. Además, en la capa de aplicación se implementa un robusto marco de seguridad basado en los estándares OWASP. Este marco proporciona medios para mitigar amenazas como la inyección SQL, el scripts entre sitios y los ataques DoS de la capa de aplicación. Por si fuera poco, realizamos sesiones periódicas para educar a los desarrolladores sobre prácticas de codificación seguras.

B. Control de acceso e identidades:

- **Integración con almacenes de identidad:**

Los productos ITOM de ManageEngine se integran fácilmente con almacenes de identidad externos como Microsoft Active Directory y servidores RADIUS. Los usuarios pueden ser importados desde los almacenes de identidad y se puede aprovechar el mecanismo de autenticación respectivo. Los usuarios serán identificados de forma única a través de sus respectivas cuentas en el almacén de identidades.

- **Cuentas únicas y autenticación local segura:**

Los productos ITOM de ManageEngine vienen con un mecanismo de autenticación local en el que se crean cuentas únicas para los usuarios. Los usuarios podrán acceder a la aplicación con sus credenciales. Las credenciales tienen un hash unidireccional utilizando bcrypt, y se almacenan de forma segura en la base de datos ubicada en la configuración del cliente.

C. Cifrado:

- **En reposo:**

Los datos confidenciales, como las contraseñas, los tokens de autentificación y similares, que se almacenan en la base de datos se cifran mediante el estándar de cifrado avanzado (AES) de 256 bits. Para cada cliente, se genera una clave de instalación única que se utiliza para el cifrado.

- **Protección de la base de datos**

De manera predeterminada, la base de datos PostgreSQL incluida en OpManager sólo es accesible proporcionando credenciales específicas de la instancia y está limitada al acceso al host local.

D. Protección contra CSRF:

Un ataque de falsificación de petición en sitios cruzados (CSRF) se produce cuando un sitio web/blog malicioso o un programa hace que el navegador web utilizado realice acciones que no están autenticadas por el usuario. Esto supone una grave amenaza para los datos críticos del usuario. Por lo general, la falta de un mecanismo de autenticación adecuado hace que el navegador web de un usuario sea vulnerable a los ataques CSRF.

OpManager proporciona protección contra los ataques CSRF. Esto garantiza que la información crítica y las credenciales del cliente permanezcan protegidas y no sean propensas a las amenazas externas o a la explotación.

E. Verificación de la integridad de los parches:

En OpManager, la verificación de la integridad de los parches aplicados se realizará durante el proceso de actualización. Para mejorar la seguridad, todos los parches desconocidos aplicados a la aplicación instalada serán restringidos.

III. Seguridad operacional

A. Seguridad de los datos del cliente:

Los datos del cliente sólo residen en su entorno, ya que el producto es una solución on-premise.

****Nota:** En caso de que algún cliente requiera ayuda para resolver algún problema, podemos requerir los logs del cliente. El cliente carga los logs a través de un portal seguro de nuestra propiedad, al que sólo puede acceder el personal autorizado, y nos concede permiso para acceder a ellos. Los logs se borrarán automáticamente después de cinco días desde el momento de la carga.

B. Mitigación de la vulnerabilidad y gestión de parches:

Contamos con un proceso de vulnerabilidad dedicado que analiza activamente las amenazas o vulnerabilidades de seguridad utilizando una combinación de herramientas de análisis de terceros certificados y herramientas internas. Posteriormente, se realizan pruebas automatizadas y manuales. Además, el equipo de seguridad revisa activamente los informes de seguridad entrantes y monitorea las listas de correo públicas, las entradas de los blogs y las wikis para identificar los incidentes de seguridad que puedan afectar a la empresa. Una vez que identificamos una vulnerabilidad que requiere reparación, se registra, se prioriza según la gravedad y se le asigna un propietario. Además, identificamos los riesgos asociados y los mitigamos poniendo parches a los sistemas vulnerables. Tras evaluar la gravedad de la vulnerabilidad basándonos en el análisis de impacto, nos comprometemos a resolver el problema dentro de nuestro SLA definido. Dependiendo de la gravedad, enviamos avisos de seguridad a todos nuestros clientes describiendo la vulnerabilidad, el parche y las medidas que debe tomar el cliente.

C. Continuidad de la actividad del negocio:

- Disponemos de energía de reserva, sistemas de control de temperatura y sistemas de supresión y protección contra incendios para garantizar la continuidad de la actividad del negocio. Existen planes de continuidad de la actividad del negocio específico para las principales operaciones, como la gestión de infraestructuras y la asistencia técnica.

- Disponemos de un plan de continuidad de la actividad del negocio y de recuperación de desastres bien planificado para ayudarnos en caso de calamidades naturales, desastres provocados por el hombre, etc. El plan abarca todas nuestras operaciones internas que garantizan la continuidad de los servicios a nuestros clientes. Contamos con tres equipos de recuperación, a saber, el Equipo de Gestión de Emergencias (EMT), el Equipo de Recuperación de Catástrofes (DRT) y el equipo de Servicios Técnicos de TI (IT), para una mejor coordinación y apoyo entre los distintos equipos.

D. Divulgación responsable:

Existe un programa de notificación de vulnerabilidades en "Bug Bounty", para llegar a la comunidad de investigadores, que reconoce y recompensa el trabajo de los investigadores de seguridad. Nos comprometemos a trabajar con la comunidad para verificar, reproducir, responder, legitimar e implementar soluciones apropiadas para las vulnerabilidades reportadas. Si por casualidad encuentra alguna, por favor envíela a https://bugbounty.zoho.com

Si quiere informarnos directamente de las vulnerabilidades, envíe un correo a security@zohocorp.com

E. Controles del cliente para la seguridad:

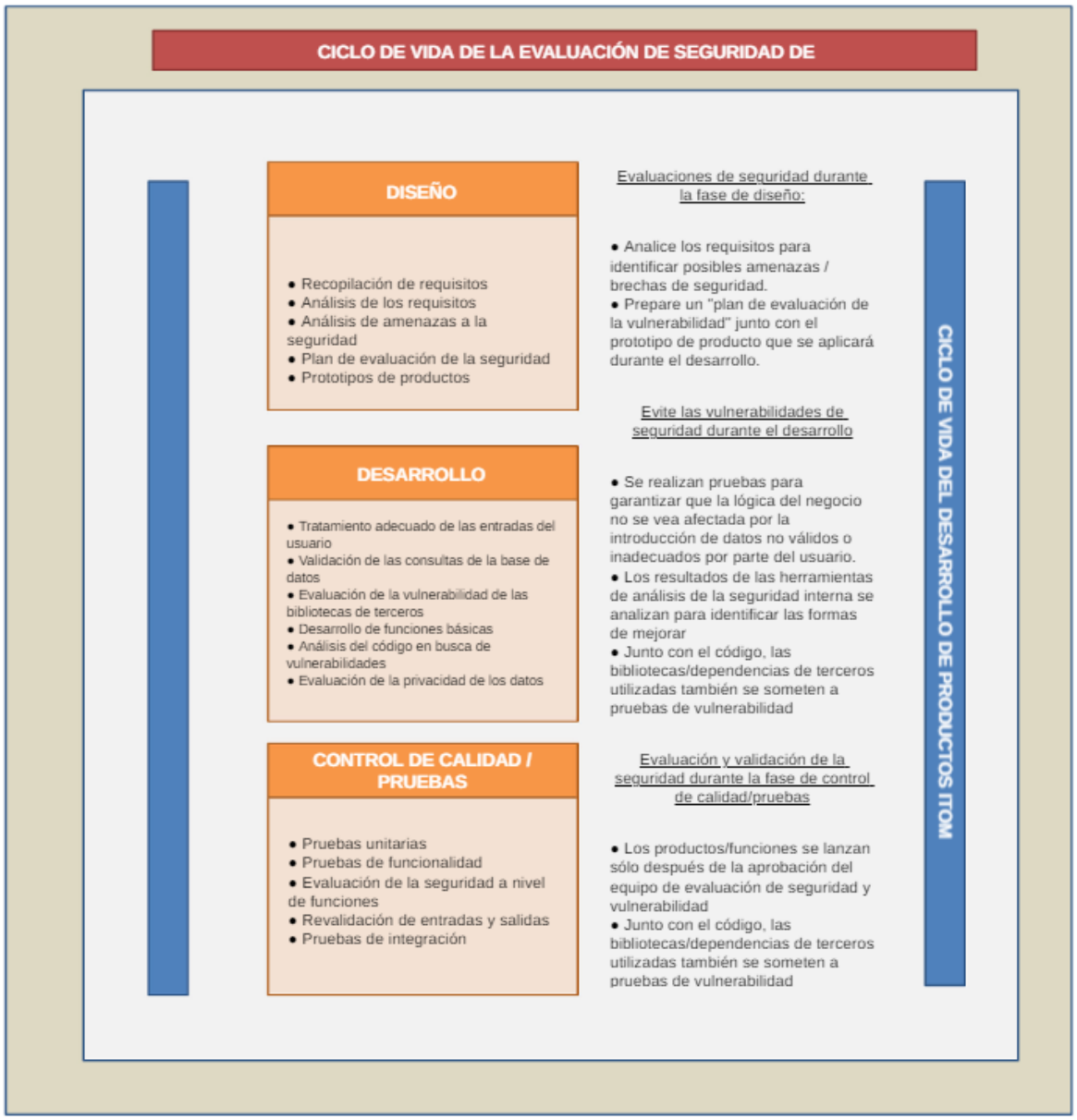
Hasta ahora hemos hablado de lo que hacemos para mejorar la seguridad de nuestros clientes en varios frentes. Estas son las cosas que usted, como cliente, puede hacer para garantizar la seguridad desde su lado:

1. Asegúrese de que la aplicación esté instalada con los privilegios necesarios.
2. Para garantizar la seguridad de las conexiones, active el modo de comunicación HTTPS y utilice únicamente certificados de terceros de confianza.
3. Cambie la contraseña de administrador predeterminada tan pronto como se haya completado la configuración.
4. Utilice contraseñas complejas y cambie las contraseñas de los usuarios periódicamente.
5. Habilite la autenticación de dos factores (TFA) como una capa de seguridad adicional para evitar el acceso no autorizado.
6. Monitoree los usuarios que tienen acceso a la aplicación en la sección Gestión de Usuarios y verifíquelos periódicamente.
7. Si las "Carpetas compartidas en red" están configuradas en el producto, asegúrese de que las carpetas estén protegidas.

1. Mantenga sus aplicaciones actualizadas.
2. Revise los logs de auditoría periódicamente.
3. Realice periódicamente copias de seguridad de los datos de la aplicación y de la base de datos.
4. Habilite el failover/disco de reserva para una alta disponibilidad que ayude a monitorear sus redes 24x7.

Nota: Se aconseja en el mejor interés de los clientes leer las mejores prácticas de seguridad enumeradas en nuestro sitio y ejercerlas mientras se utiliza el producto.

IV. Ciclo de vida de la evaluación de la seguridad



El ciclo de vida de la evaluación de la seguridad forma parte del proceso completo del SDLC (ciclo de vida del desarrollo de software) al que se someten todas las aplicaciones del ITOM antes de salir al mercado. La evaluación de la seguridad y la vulnerabilidad se realiza en cada parte del proceso de desarrollo de la aplicación (diseño, desarrollo y control de calidad).

Algunas de las comprobaciones previas más importantes que se realizan en el ciclo de vida de la evaluación de la seguridad para garantizar que la aplicación no sea víctima de ningún problema de seguridad son:

- Todas las dependencias de terceros en el código se someten a herramientas de comprobación de vulnerabilidades antes de ser introducidas en el código.
- Todas las entradas de los usuarios se someten a una validación adecuada.
- El sistema de privilegios de acceso se adopta firmemente en todas las fases de las aplicaciones.
- Todos los módulos del código son compatibles con OWASP.
- El lanzamiento de cada función del producto está sujeta a la aprobación del equipo de evaluación de la seguridad y la vulnerabilidad y también a la aprobación del propietario del módulo que se encarga de garantizar que el producto esté bien protegido de cualquier vulnerabilidad.
- Los informes de las herramientas de seguridad internas se analizan periódicamente para identificar las posibles mejoras que pueden introducirse en el ciclo de vida de la evaluación de la seguridad.

El ciclo de vida de la evaluación de seguridad del ITOM se centra en las siguientes vulnerabilidades de seguridad importantes:

1. Vulnerabilidad XSS
2. Inyección SQL
3. Path traversal (Recorrido de rutas)
4. Inclusión de archivos locales
5. Ejecución remota de código
6. Inyección XML
7. Otras vulnerabilidades comunes como la deserialización de datos no confiables, la carga de clases dinámicas no confiables, algoritmos débiles, bomba zip, etc.

V. Preguntas frecuentes sobre prácticas de seguridad

P. ¿Cómo se garantiza la seguridad en el ciclo de vida del desarrollo de productos?

Los productos ITOM de ManageEngine son desarrollados únicamente por nuestros empleados, que son ingenieros calificados. Seguimos las mejores prácticas de desarrollo de software del sector para garantizar la integridad del código y del producto. Cada línea de código desarrollada pasa por dos niveles de control de seguridad. En primer lugar, el código es revisado por el Líder\Director tanto para el rendimiento como para la seguridad. En segundo lugar, contamos con equipos de seguridad dedicados a auditar la compilación que se lleva a cabo para el lanzamiento, a fin de garantizar que no haya puertas abiertas para los ataques/hacks. Si alguno de ellos no está satisfecho con las medidas de seguridad, esa compilación en particular no se lanzará.

P. ¿Cómo se introducen los componentes de terceros en el producto?

Los componentes de terceros (JAR, .js, etc.,) son revisados exhaustivamente por el equipo de seguridad en busca de CVE o problemas de seguridad. Cualquier componente de terceros que se utilice en el desarrollo del producto se integra sólo tras la aprobación de los equipos de seguridad.

P. ¿Cómo garantizamos la seguridad en el proceso de lanzamiento?

Una vez que la compilación está lista para su lanzamiento, se somete a múltiples pruebas de vulnerabilidad. Sólo se lanzan las compilaciones que superan las pruebas. Esto nos ayuda a ofrecer productos de software altamente seguros. Garantizamos que los cambios realizados sólo después de la compilación anterior se integren en la próxima versión.

P. Dada la situación actual, ¿cómo garantiza ManageEngine la integridad de las compilaciones disponibles para su descarga en su dominio?

Cada producto ITOM (.exe/.bin) disponible para su descarga en el dominio de ManageEngine es verificado por Checksum para garantizar su integridad. Una vez más, se descargaron las compilaciones y se comprobó manualmente la presencia de cualquier código malicioso, para mejorar la seguridad. Las compilaciones disponibles en nuestro sitio web se encuentran intactas.

Para cualquier consulta, envíe un correo electrónico a opmanager-support@manageengine.com