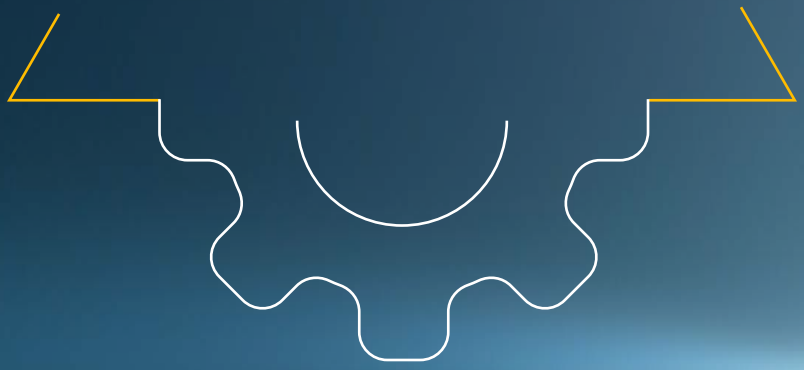
ManageEngine
ADManager Plus

La guía definitiva para la automatización de Active Directory



www.admanagerplus.com

Introducción

Active Directory (AD) es un servicio que permite a las organizaciones conectar usuarios, recursos y datos. Con él, los administradores pueden gestionar fácilmente varias cuentas de usuarios y dispositivos dentro de la red organizacional. AD ayuda a centralizar recursos y fortalecer la seguridad, además de permitir un control administrativo efectivo. Los administradores usualmente realizan funciones como aprovisionamiento y desaprovisionamiento de usuarios, manteniendo distintos grupos de usuarios en la organización, y controlando cualquier actividad sospechosa, entre otras. Realizar estas funciones repetitivas manualmente puede ser agotador y tedioso para el equipo de TI. ¡Aquí es donde la automatización entra en juego!

¿Por qué la automatización es crucial en AD?

La carga de trabajo de un administrador de AD usualmente incluye tareas redundantes, como el aprovisionamiento y desaprovisionamiento de usuarios, mantenimiento de grupos categóricos, administración de la seguridad y más. Automatizar acciones repetitivas puede ayudar a las organizaciones a reducir el tiempo y esfuerzo invertido en mantener su entorno de AD y hace la administración más eficiente y congruente.

He aquí algunas de las tareas que, cuando se automatizan, pueden garantizar un uso óptimo de los recursos:

- **Vinculación y desvinculación de empleados**
- **Restablecimiento de contraseñas**
- **Desbloqueo de cuentas**
- **Limpieza de AD**
- **Generación de informes para auditorías de cumplimiento**
- **Respaldo completo de AD**
- **Asignación de membresías de grupos**
- **Gestión de acceso de carpetas para usuarios**
- **Modificación en las propiedades de los usuarios**
- **Recordatorios sobre vencimientos de contraseñas**

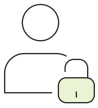
Vinculación y desvinculación de empleados

La mayoría de las organizaciones son entidades dinámicas. Tratan con empleados que se unen y dejan la compañía; cada cambio provoca una serie de cambios en los datos. Su equipo administrativo debe añadir y eliminar cuentas de usuarios, además de gestionar muchos otros cambios. Desde crear y eliminar cuentas de usuarios a asignar y eliminar licencias, hay bastante pocas operaciones de AD que realizar durante el aprovisionamiento y desaprovisionamiento de usuarios. Controlar esto en un entorno de AD manualmente puede ser un proceso arduo.

Restablecimiento de contraseñas

Por varias razones, los usuarios en la organización podrían necesitar restablecer sus contraseñas, incluyendo cuando las olvidan. Solicitar permisos para restablecer la contraseña puede ser un proceso agotador para sus empleados y el equipo de TI. El tiempo que toma restablecer manualmente contraseñas de usuarios puede aumentar los costos de su mesa de ayuda, a la vez que se afecta la productividad de sus empleados debido a contraseñas perdidas y bloqueos de cuentas.

Desbloqueo de cuentas



Las cuentas de los empleados pueden ser bloqueadas por varias razones, que incluyen ingresar la contraseña incorrecta o llegar a cierto número de intentos inválidos de inicio de sesión. Los administradores de AD necesitan asegurarse de que han implementado una política segura de bloqueo de cuentas que garantice la postura de seguridad de la organización mientras también se reducen los ataques cibernéticos, tales como ataques de fuerza bruta. Pero puede ser difícil identificar a los usuarios cuyas cuentas se hayan bloqueado usando solo herramientas nativas como scripts de PowerShell. Y el desbloqueo manual de las cuentas de usuario requeridas solo complicará este proceso arduo.

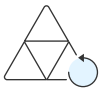
Limpieza de AD

Es necesario limpiar su entorno de AD para mantenerlo actualizado y protegido. Es importante controlar las cuentas de usuario redundantes de los empleados que han salido de la compañía o cambiado sus cargos. Dichas cuentas suponen un peligro para la seguridad de la organización, ya que posibles hackers pueden usarlas para infiltrarse en la red. Al limpiar regularmente su AD, puede evitar dichas situaciones. La limpieza de AD puede incluir un número de tareas, como eliminar cuentas inactivas o deshabilitadas, revocar permisos que no se necesitan más y encontrar cuentas de AD vencidas. Realizar manualmente estas tareas puede abrir la puerta a errores humanos.

Generación de informes

La gestión de AD requiere que controle todas las actividades que suceden en su red organizacional. Mientras que puede usar PowerShell para obtener conocimiento de su entorno de AD on-premise, puede terminar gastando tiempo innecesario gestionándolo y notificándolo en AD.

Respaldo completo de AD



El entorno de AD es un componente clave de la red de Windows Microsoft de su organización. Si su entorno de AD falla, entonces toda su organización se detendrá. Mantener un respaldo de su AD es imperativo en situaciones en que un controlador de dominio (DC) experimenta un fallo o en el caso en que se generen otros problemas que hagan que sus usuarios no puedan acceder a sus equipos. Esta es la razón por la que es necesario tener un respaldo y plan de recuperación en caso de algún desastre. Respaldar manualmente su AD puede tomar mucho tiempo a su equipo de TI.

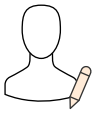
Gestión de membresías de grupos

Los grupos de AD pueden organizar usuarios, equipos e incluso otros grupos en unidades manejables para una administración y mantenimiento de la red sencillos. Se usan también para optimizar la gestión de usuarios y equipos en la organización al agruparlos y otorgarles los privilegios de acceso requeridos. Al añadir un usuario a un grupo, el administrador puede darles fácilmente acceso a todos los recursos compartidos y servicios de directorio asociados con ese grupo. Hay muchas situaciones en que las dinámicas de estos grupos deben cambiar. Por ejemplo, cuando un empleado cambia de departamento, podría requerir nuevos permisos de acceso y necesitar que se lo añada a un nuevo grupo. Ejecutar manualmente esta tarea cada vez que sea necesario modificar las membresías de un grupo puede ser un proceso tedioso para los administradores de TI.

Gestión de acceso de carpetas para usuarios

Los administradores asignan permisos de acceso a carpetas con base en sus roles, membresía de grupo y en lo que estén trabajando en la organización. Los permisos que los usuarios requieran pueden cambiar también en ocasiones según varios factores. Por ejemplo, un usuario podría empezar a trabajar en un proyecto especial que requiera que ellos tengan acceso a cierta carpeta por un periodo fijo de tiempo. Por otro lado, un cambio de roles en el lugar de trabajo puede también provocar un cambio en el acceso requerido a los recursos. Realizar esta tarea manualmente puede ser un proceso tedioso.

Modificación de cuentas de usuarios



La carga de trabajo de mantener a un usuario en su entorno de AD organizacional no se detiene con automatizar la creación de objetos de usuarios. Durante su contrato, varios atributos de su cuenta de usuario pueden cambiar. Podrían obtener un ascenso o cambio de departamento, lo que conlleva un cambio en las propiedades del usuario. Modificar manualmente estas propiedades puede ser tedioso y agotador.

Recordatorios sobre vencimientos de contraseñas

La seguridad tiene una importancia crítica en cualquier organización. Garantizar que sus empleados tengan contraseñas robustas y complejas es uno de los pasos más sencillos hacia la seguridad informática. No solo necesitan contraseñas robustas que no se puedan descifrar fácilmente, sino que los usuarios también necesitan recordar cuándo estas están por vencer, de forma que las cambien efectivamente. No hacerlo puede conllevar bloqueos de cuentas. Enviar recordatorios sobre vencimientos de contraseñas a los respectivos usuarios puede ser una tarea demandante para los administradores.

Automatización con AD

AD solo le permite automatizar la tarea de respaldo de AD. Aunque pueda programar el respaldo de AD usando la aplicación de respaldo de Windows Server, está limitada a un respaldo completo de AD o un respaldo por volumen. No permite un respaldo y recuperación a nivel ítem, ni implementa un sistema para automatizar restablecimientos de contraseñas y bloqueos de cuentas para los usuarios.

El poder de ADManager Plus

ManageEngine ADManager Plus es una solución empresarial para todas sus necesidades de gobernanza y administración de identidades. Ofrece potentes funciones que pueden ayudarlo a gestionar, administrar e informar sobre su entorno de AD. Con esta función de automatización, puede garantizar una gestión eficiente y fácil de AD para su organización.

Cómo ADManager Plus simplifica la automatización

Debido a su naturaleza sensible, los administradores de TI realizan la mayoría de las tareas de AD meticulosa y manualmente o al usar métodos tradicionales como PowerShell. Cuando las organizaciones crecen constantemente, estas tareas pueden ser extremadamente demandantes. Las funciones de automatización de ADManager Plus se ocupan de esta carga al permitirle automatizar tareas repetitivas y tediosas de AD.

- Automatice fácilmente operaciones repetitivas de AD, como crear usuarios, eliminar usuarios inactivos, mover grupos, programar recordatorios de notificaciones de contraseñas y más.
- Controle el estado de las tareas automatizadas.
- Genere más de 200 informes integrales e intuitivos sobre varios aspectos de su entorno de AD.
- Programe informes para que se generen automáticamente en el momento conveniente para usted.
- Automatice una serie de tareas de seguimiento vinculadas a una tarea primaria, organícelas en un orden específico y designe intervalos de tiempo para su ejecución.
- Refuerce la seguridad al automatizar cambios de contraseñas periódicos para los usuarios.
- Establezca un flujo de trabajo basado en aprobaciones para solicitudes de restablecimiento de contraseñas, todo con un solo clic.
- Controle a los usuarios con cuentas bloqueadas y automatice un sistema para desbloquear las cuentas de AD sin problemas.

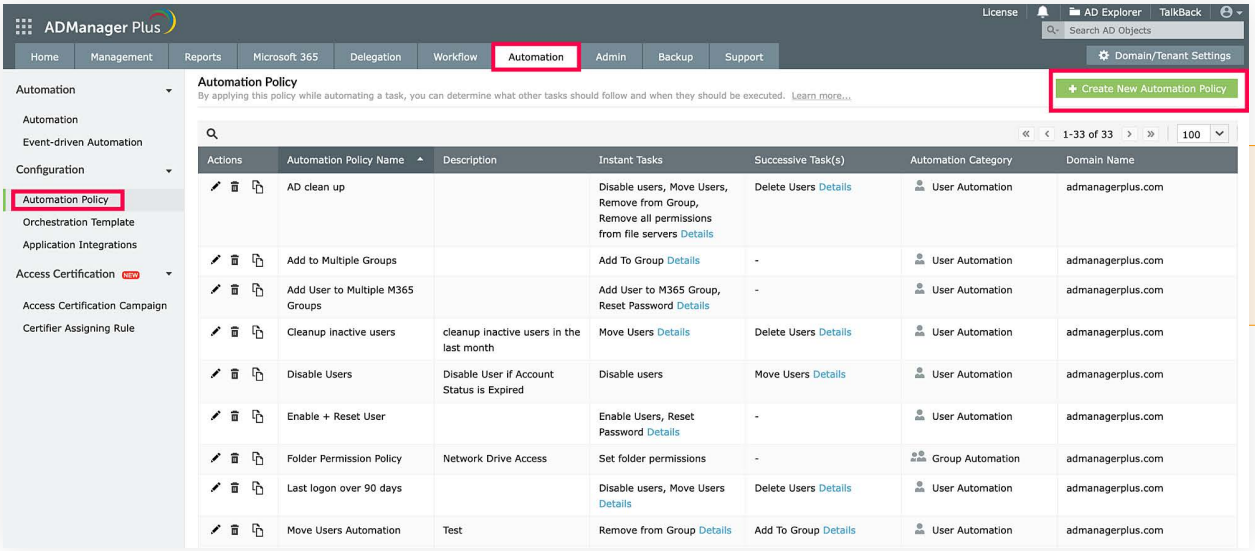
Caso de uso: Limpieza de AD

Permita que su organización tenga un sistema para mover todas las cuentas de usuarios inactivas a una OU separada al final de cada mes, reteniéndolas por un periodo de 100 días, después de los cuales se eliminan permanentemente.

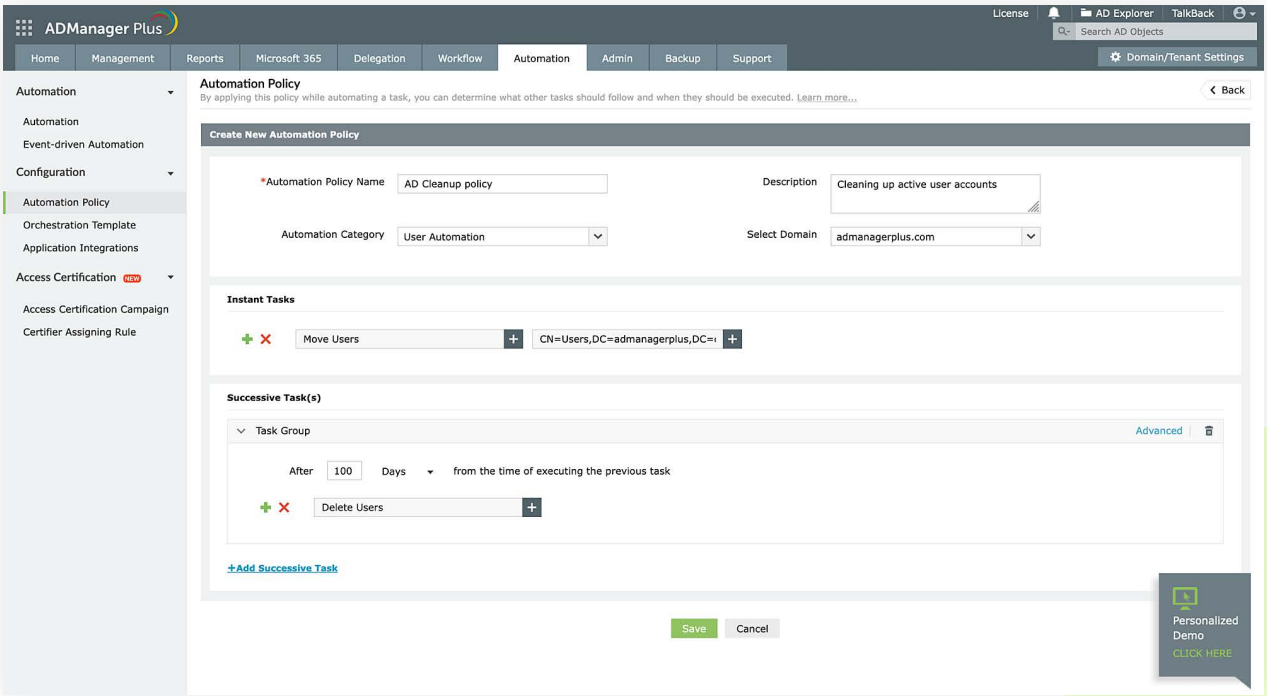
¡Con ADManager Plus puede optimizar esta tarea monótona fácilmente!

Configure una política de automatización

1. En ADManager Plus, vaya a la pestaña Automatización y escoja Política de automatización en el panel izquierdo.
2. Haga clic en **Crear nueva política de automatización**.



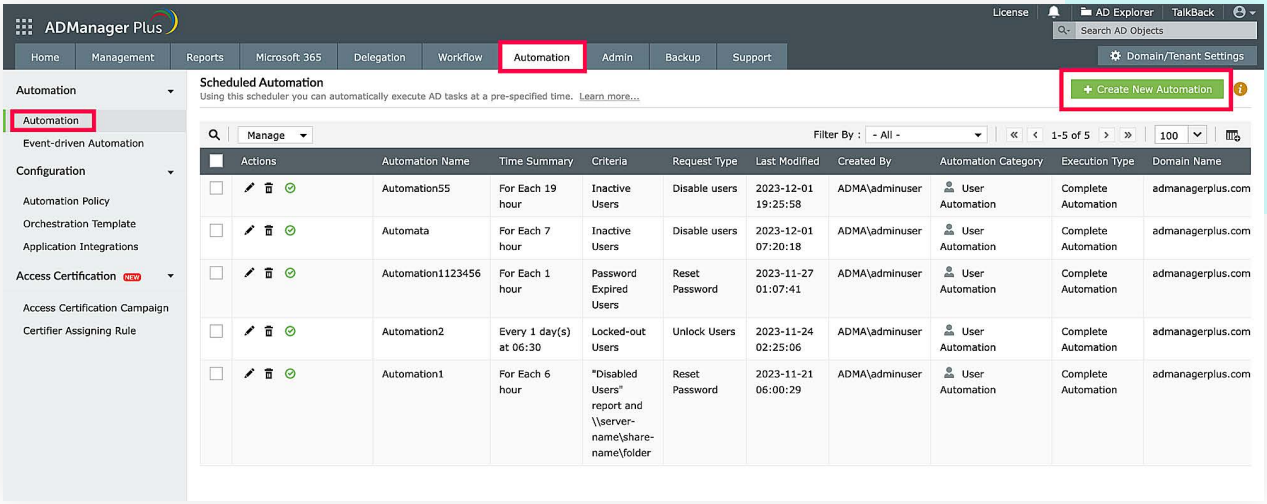
3. En la página que aparezca, configure el Nombre de la política de automatización, la Descripción y el Nombre del dominio.
4. En el menú desplegable Categoría de Automatización, escoja Automatización de usuarios.
5. En Tareas instantáneas escoja Mover usuarios y seleccione la OU requerida.
6. Haga clic en Añadir tareas sucesivas y escoja el tiempo (por ejemplo, 100 días) luego del cual se realizarán las tareas sucesivas.
7. En este caso seleccione Eliminar usuarios como la tarea sucesiva.



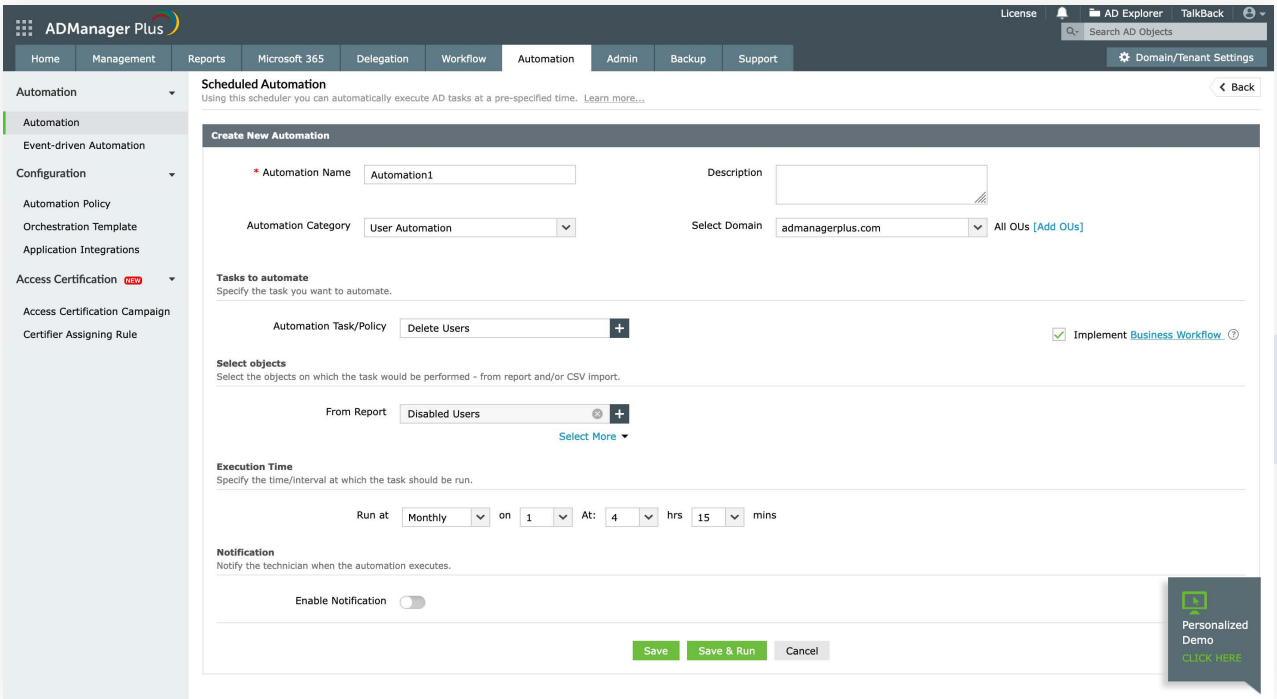
8. Guarde la política de automatización.

Ahora puede crear una automatización para implementar esta política automáticamente.

1. En ADManager Plus, vaya a la pestaña Automatización y escoja Automatización en el panel izquierdo.
2. Haga clic en Crear nueva automatización.



3. En la página que aparezca, configure el Nombre de la política de automatización, la Descripción y el Nombre del dominio.
4. En el menú desplegable Categoría de Automatización, escoja Automatización de usuarios.
5. En Tarea/política de automatización, escoja la política de automatización que ha creado.
6. En Desde informes escoja el informe Usuarios inactivos.
7. Seleccione un tiempo de ejecución para la automatización. Por ejemplo, puede escoger ejecutar la tarea el primer día de cada mes, a las 2 horas y 0 minutos.



8. Guarde la automatización.

Luego de configurar y guardar la automatización, los usuarios inactivos se moverán automáticamente a una OU separada el primero de cada mes y se programarán las tareas de seguimiento.

¿Listo para revolucionar su entorno de AD con ADManager Plus? ¡Empiece con una prueba gratuita de 30 días de ADManager Plus o programe una sesión de demostración personalizada con uno de nuestros expertos en productos hoy!