

# Active Roles

Administración y seguridad para Active Directory híbrido y mucho más

## Beneficios

- Protege los datos críticos de Active Directory y Azure Active Directory.
- Regula el acceso administrativo a través de un modelo de privilegios mínimos.
- Supera las limitaciones de las herramientas nativas.
- Automatiza la creación y eliminación de cuentas de grupo y usuarios.
- Administra las cuentas para Exchange Online, Lync, SharePoint Online, Office 365 y mucho más.
- Ofrece una herramienta simple e intuitiva para el entorno híbrido.
- Genera informes para auditorías.
- Se implementa velozmente para generar valor con rapidez.
- Le permite saber quién hizo quién hizo qué cambio y cuándo.
- Arquitectura modular para satisfacer las necesidades de la empresa en la actualidad y en el futuro.
- Expande la administración de identidades centrada en AD a muchos sistemas que no sean Windows ni SaaS.

## Información general

Los desafíos de la administración de cuentas en Active Directory (AD) y Azure AD son muchos y variados. Además, la seguridad de estos sistemas críticos suele ser un desafío importante. Con las herramientas nativas, la administración híbrida de AD y la seguridad son ineficientes, desarticuladas y propensas a errores.

Con el ritmo frenético de los negocios actuales, las empresas se esfuerzan por seguir el ritmo de las solicitudes para crear, cambiar o eliminar el acceso al entorno de AD híbrido. Además, se enfrentan a problemas de seguridad como, por ejemplo, que los empleados despedidos retengan el acceso a propiedad intelectual valiosa, cuestionen los requisitos de la empresa y cumplan con las solicitudes de informes de los auditores. Entonces, agregue la necesidad de controlar estrictamente el acceso administrativo a Active Directory y Azure Active Directory, así como de seguir el ritmo de la explosión de aplicaciones que no sean de Windows ni de SaaS y que también deban administrarse.

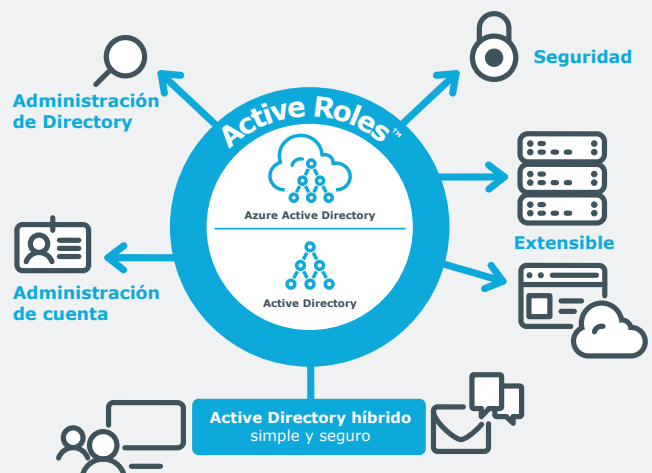
Afortunadamente, la ayuda está aquí. Con One Identity Active Roles, puede automatizar estas tareas administrativas tediosas y propensas a errores, y resolver sus problemas de seguridad. Active Roles automatiza y unifica la administración de cuentas y grupos, y a la vez asegura y protege el importantísimo acceso administrativo.

Active Roles ofrece herramientas automatizadas para la administración de cuentas de usuarios y grupos a fin de superar las carencias de las herramientas nativas de Active Directory y Azure Active Directory, lo que le permite realizar su trabajo de forma más eficiente, más precisa y con menos intervención manual. Active Roles está diseñado con una arquitectura modular, así su empresa puede cumplir fácilmente con los requisitos empresariales actuales y futuros.

## Características

### Listo para AD híbrido

Active Roles está optimizado para cubrir las necesidades de AD local y Azure AD local en una implementación híbrida. Ofrece una consola única, flujos de trabajo unificados y una experiencia administrativa uniforme en todo el entorno híbrido. Elimina la naturaleza compleja, propensa a errores y limitada del uso de herramientas separadas y procesos manuales.



## Acceso seguro

Active Roles ofrece administración de cuenta integral y privilegiada para Active Directory y Azure Active Directory, y le permite controlar el acceso a través de la delegación con un modelo de privilegios mínimos. Según las políticas administrativas definidas y los permisos asociados, genera y hace cumplir estrictamente las reglas de acceso, lo que elimina los errores y las incoherencias comunes con perspectivas nativas a la administración de AD híbrido. Además, los procedimientos de aprobación sólidos y personalizados establecen un proceso del área de TI y supervisión coherente con los requisitos de la empresa, con cadenas de responsabilidad que complementan la administración automatizada de datos del directorio.

## Automatice la administración de cuentas

Active Roles automatiza una gran variedad de tareas, que incluyen las siguientes:

- Crear cuentas de grupo y usuarios en AD y AAD.
- Amplíe fácilmente las acciones administrativas de cuentas basadas en AD/AAD a sistemas que no sean Windows y aplicaciones de SaaS.
- Crear casillas de correo en Exchange y Exchange Online.
- Poblar grupos en AD y AAD.
- Asignación de recursos en Windows.

También automatiza el proceso de reasignación y eliminación de derechos de acceso del usuario en AD y sistemas unidos a AD (que incluye la falta de aprovisionamiento de grupo y usuarios) para asegurar un proceso administrativo seguro y eficiente de los tiempos de vida de grupo y usuario. Cuando es necesario cambiar o eliminar el acceso de un usuario, las actualizaciones se realizan automáticamente en todos los sistemas y aplicaciones pertinentes en el entorno híbrido de AD/AAD, así como en cualquier sistema unido a AD, como Unix, Linux y Mac OS X, además de un amplio y creciente conjunto de muchas aplicaciones de SaaS populares a través de la solución One Identity Starling Connect.

## Administración diaria de directorios

Con Active Roles, puede administrar fácilmente todo lo siguiente para los entornos locales y de Azure AD:

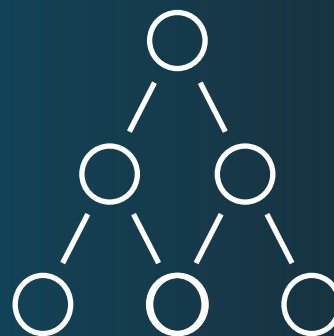
- Destinatarios de Exchange, incluidos la administración de la lista de distribución y permisos, eliminación, movimiento, creación y asignación de OCS/buzón de correo
- Grupos
- Equipos, incluidos los recursos compartidos, impresoras, usuarios y grupos locales
- Active Directory y Azure Active Directory

Active Roles incluye interfaces intuitivas para optimizar la administración diaria y las operaciones de la mesa de ayuda del entorno híbrido de AD/AAD a través de una interfaz de MMC y una interfaz web.

Active Roles también admite las opciones de personalización más populares y relevantes, como PowerShell, para ofrecer la máxima flexibilidad y la posibilidad de utilizar Active Roles de la forma más ventajosa para su empresa.

## Amplíe el alcance administrativo

Active Roles es compatible con el estándar SCIM, que permite que cualquier aplicación de SaaS compatible con SCIM (a través de One Identity Starling Connect) se incluya en las capacidades de administración de cuentas y grupos de Active Roles basadas en AD.



**Quando es necesario cambiar o eliminar el acceso de un usuario, las actualizaciones se realizan de forma automática en AD, AAD, Exchange Online, SharePoint Online, OCS, Skype for Business y Windows, así como en cualquier sistema unido a AD, como Unix, Linux y Mac OS X y aplicaciones de SaaS.**

## Administración de grupos y usuarios en un entorno alojado

Sincronice clientes de dominio de AD con un dominio de host de AD en entornos alojados. Active Roles permite la administración de cuentas de usuario y de grupo, a la vez que sincroniza los atributos y las contraseñas, desde el dominio de cliente al dominio alojado. Utilice conectores listos para usar para sincronizar sus cuentas de AD locales con Microsoft Office 365, Lync Online/Skype for Business y SharePoint Online.

## Consolidación de los puntos de administración a través de la integración

Active Roles complementa su tecnología existente y estrategia de administración de acceso e identidad. Simplifica y consolida los puntos de administración al garantizar una integración sencilla con muchos productos de One Identity, que incluyen Identity Manager, Safeguard, Authentication Services, Password Manager y ChangeAuditor. Active Roles también automatiza y extiende las capacidades de PowerShell, ADSI, SPML y las interfaces web personalizables.

Active Roles viene con toda la tecnología de sincronización necesaria para administrar y proteger:

- Lync/Skype for Business
- Exchange
- One Drive
- SharePoint
- AD LDS
- Office 365 (incluidos roles y grupos)
- Azure AD
- Microsoft SQL Server
- Base de datos de OLE (MS Access)
- Archivo sin formato

## Acerca de One Identity

One Identity, una empresa de Quest Software, ayuda a las empresas a lograr una estrategia de seguridad centrada en identidades. Con un portafolio excepcionalmente amplio de ofertas de administración de identidades y acceso que incluye gestión de identidades, administración de accesos con privilegios y administración de cuentas, todo ello aumentado por una estrategia de entrega híbrida en la nube, One Identity ayuda a las empresas a alcanzar todo su potencial, sin obstáculos de seguridad, pero a la vez protegidas contra las amenazas. One Identity ha demostrado ser inigualable en su compromiso con el éxito a largo plazo de sus clientes. Más de 7500 empresas de todo el mundo dependen de las soluciones de One Identity para administrar más de 125 millones de identidades, lo que mejora su agilidad y eficiencia y, a la vez, asegura el acceso a sus sistemas y datos (locales, híbridos o en la nube). Para obtener más información, visite [www.oneidentity.com](http://www.oneidentity.com)

© 2019 One Identity LLC TODOS LOS DERECHOS RESERVADOS. One Identity y el logotipo de One Identity son marcas comerciales y marcas comerciales registradas de One Identity LLC en Estados Unidos y otros países. Para obtener una lista completa de las marcas comerciales de One Identity, visite nuestro sitio web en [www.oneidentity.com/legal](http://www.oneidentity.com/legal). Todas las demás marcas comerciales, marcas de servicio, marcas comerciales registradas y marcas de servicio registradas son propiedad de sus respectivos dueños.  
Datashet\_2019\_ActiveRoles74\_US\_RS\_42104