ManageEngine
AD360

Privilegios y permisos necesarios

Tabla de contenido

Resumen del documento

AD360 y sus componentes requieren distintos niveles de privilegios para llevar a cabo todas las operaciones deseadas. En esta guía se detallan todos los roles y permisos necesarios para las distintas funciones de cada componente integrado en AD360.

Puntos importantes a tener en cuenta

- Recomendamos configurar cada componente con una cuenta de administrador de dominio para acceder a todas las funciones sin problemas.

- AD360 sincroniza automáticamente diversos datos relacionados con la configuración de dominios, servidores de correo, etc. en todos los componentes integrados. De esta forma, cuando configure un componente —por ejemplo ADManager Plus— con privilegios de administrador de dominio, los ajustes se sincronizarán con otros componentes integrados, como ADAudit Plus y ADSelfService Plus, aunque haya configurado manualmente una cuenta de usuario con menos privilegios en esos componentes.

Permisos necesarios

Esta sección enumera los permisos requeridos por cada componente de AD360 para llevar a cabo las operaciones deseadas. En función de los componentes que haya integrado con AD360, puede conceder manualmente sólo los permisos necesarios a una cuenta de usuario y configurar dicha cuenta en los componentes integrados

Haga clic en los siguientes enlaces para ver los permisos necesarios para un componente en particular.

- ADManager Plus
- ADSelfService Plus
- ADAudit Plus Exchange
- Reporter Plus
- M365 Manager Plus
- RecoveryManager Plus
- SharePoint Manager Plus

ADManager Plus

Consulte la siguiente tabla en la que se enumeran los permisos necesarios para llevar a cabo distintas operaciones de gestión y elaboración de informes con ADManager Plus.

Operación	Permisos necesarios
Gestión de usuarios	
Crear usuarios	• Debe ser miembro del grupo de "Administradores" incorporado o del grupo de "Operadores de cuenta", o • Debe tener los permisos "Leer" y "Escribir" en todos los objetos de usuario de la OU requerida o contenedor en AD.
Modificar usuarios	• Debe ser miembro del grupo de "Administradores" incorporado o del grupo de "Operadores de cuenta", o • Debe tener los permisos "Leer", "Escribir" y "Leer todas las propiedades" en todos los objetos de usuario de la OU requerida o contenedor en AD. **Nota:** También es posible conceder los permisos para modificar atributos específicos en lugar de todo el objeto.
Eliminar usuarios	• Debe ser miembro del grupo de "Administradores" incorporado o del grupo de "Operadores de cuenta", o • Debe tener el permiso "Eliminar todos los objetos secundarios" en todos los objetos de usuario de la OU requerida.
Restaurar usuarios	• Los usuarios que modifiquen los permisos en el contenedor de objetos eliminados deben ser miembros del grupo de "Administradores de dominio". • La herramienta Active Directory Application Mode (ADAM) se debe descargar e instalar por separado en los controladores de dominio que ejecuten Windows Server 2000 y 2003.
Gestión de equipos	
Crear equipos	• Debe ser miembro del grupo de "Administradores" incorporado o del grupo de "Operadores de cuenta", o • Debe tener los permisos "Leer" y "Escribir" en todos los objetos de equipo de la OU requerida o contenedor en AD.

Modificar equipos	• Debe ser miembro del grupo de "Administradores" incorporado o del grupo de "Operadores de cuenta", o • Debe tener los permisos "Leer", "Escribir" y "Leer todas las propiedades" en todos los objetos de equipo de la OU requerida o contenedor en AD.
Eliminar equipos	• Debe ser miembro del grupo de "Administradores" incorporado o del grupo de "Operadores de cuenta", o • Debe tener el permiso "Eliminar todos los objetos secundarios" en todos los objetos de equipo de la OU requerida.
Restaurar equipos	• Los usuarios que modifiquen los permisos en el contenedor de objetos eliminados deben ser miembros del grupo de "Administradores de dominio". • La herramienta Active Directory Application Mode (ADAM) se debe descargar e instalar por separado en los controladores de dominio que ejecuten Windows Server 2000 y 2003.
Gestión de grupos	
Crear grupos	• Debe ser miembro del grupo de "Administradores" incorporado o del grupo de "Operadores de cuenta", o • Debe tener los permisos "Leer" y "Escribir" en todos los objetos de grupo de la OU requerida o contenedor en AD.
Modificar grupos	• Debe ser miembro del grupo de "Administradores" incorporado o del grupo de "Operadores de cuenta", o • Debe tener los permisos "Leer", "Escribir" y "Leer todas las propiedades" en todos los objetos de grupo de la OU requerida o contenedor en AD.
Eliminar grupos	• Debe ser miembro del grupo de "Administradores" incorporado o del grupo de "Operadores de cuenta", o • Debe tener el permiso "Eliminar todos los objetos secundarios" en todos los objetos de grupo de la OU requerida.
Restaurar grupos	• Los usuarios que modifiquen los permisos en el contenedor de objetos eliminados deben ser miembros del grupo de "Administradores de dominio". • La herramienta Active Directory Application Mode (ADAM) se debe descargar e instalar por separado en los controladores de dominio que ejecuten Windows Server 2000 y 2003.

Gestión de contactos	
Crear contactos	• Debe ser miembro del grupo de "Administradores" incorporado o del grupo de "Operadores de cuenta", o • Debe tener los permisos "Leer" y "Escribir" en todos los objetos de contacto de la OU requerida o contenedor en AD.
Modificar contactos	• Debe ser miembro del grupo de "Administradores" incorporado o del grupo de "Operadores de cuenta", o • Debe tener los permisos "Leer", "Escribir" y "Leer todas las propiedades" en todos los objetos de contacto de la OU requerida o contenedor en AD.
Eliminar contactos	• Debe ser miembro del grupo de "Administradores" incorporado o del grupo de "Operadores de cuenta", o • Debe tener el permiso "Eliminar todos los objetos secundarios" en todos los objetos de contacto de la OU requerida.
Restaurar contactos	• Los usuarios que modifiquen los permisos en el contenedor de objetos eliminados deben ser miembros del grupo de "Administradores de dominio". • La herramienta Active Directory Application Mode (ADAM) se debe descargar e instalar por separado en los controladores de dominio que ejecuten Windows Server 2000 y 2003.
Gestión e informes de GPO	
Crear GPO	• Debe ser miembro del grupo de "Propietarios creadores de directivas de grupo".
Habilitar/deshabilitar GPO	• Debe tener seleccionado el permiso **Editar ajustes** en los GPO. **Nota:** Para saber cómo delegar permisos para Editar ajustes a un grupo o usuario en un GPO, consulte este documento.
Habilitar/deshabilitar los ajustes de configuración del usuario	• Debe tener seleccionado el permiso **Editar ajustes** en los GPO. **Nota:** Para saber cómo delegar permisos a un grupo o usuario en un GPO, consulte este documento.
Habilitar/deshabilitar los ajustes de configuración del equipo	• Debe tener seleccionado el permiso **Editar ajustes** en los GPO. **Nota:** Para saber cómo delegar permisos a un grupo o usuario en un GPO, consulte este documento.
Habilitar/deshabilitar/eliminar enlaces de GPO	• Debe seleccionar Vincular GPO en la lista desplegable Permisos. **Nota:** Para saber cómo delegar permisos para vincular GPO, consulte este documento.

Editar los ajustes de GPO	• Debe tener seleccionado el permiso Editar ajustes en los GPO. **Nota:** Para saber cómo delegar permisos a un grupo o usuario en un GPO, consulte este documento.
Imponer enlaces de GPO	• Debe seleccionar Vincular GPO en la lista desplegable Permisos. **Nota:** Para saber cómo delegar permisos para vincular GPO, consulte este documento.
Informes	• Debe tener el permiso "Leer" en los objetos de sitio, dominio y OU (atributo gPlink). Debe tener el permiso "Leer" en los objetos de sitio, dominio y OU (atributo gPOptions). Debe tener el permiso "Leer" en los objetos de GPO (atributos flags, versionNumber, modifyTimeStamp, createTimeStamp). **Nota:** Por defecto: ◦ El grupo "Usuarios de dominio" tendrá estos derechos para generar informes. ◦ Los "Administradores de dominio" y los "Administradores de empresa" tendrán todos los derechos mencionados para realizar todas las operaciones de gestión e informes.
Modificar/eliminar permisos de NTFS	• Debe tener el permiso "Leer" y "Escribir" en las carpetas relevantes.
Modificar/eliminar permisos de uso compartido	• Se debe poder acceder al recurso compartido desde el equipo en el que está instalado ADManager Plus.
Informes de AD	
Generar informes	• Debe tener el permiso "Ver" en las OU y dominios deseados.
Informes de NTFS	• Debe tener el permiso "Leer" en las carpetas relevantes.

Gestión de Exchange **Crear buzones de Exchange mientras se crea la cuenta de usuario correspondiente en AD**	
Exchange 2007	• Debe tener el rol de "Administrador de destinatarios de Exchange" y el rol de "Operador de cuentas".
Exchange 2010	• Debe formar parte del grupo de "Administración de la organización".
Exchange 2013	• Debe formar parte del grupo de "Administración de la organización".
Crear buzones de Exchange para usuarios existentes de AD	
Exchange 2007	• Debe tener el rol de "Administrador de destinatarios de Exchange" y el rol de "Operador de cuentas".
Exchange 2010	• Debe formar parte del grupo de "Administración de la organización".
Exchange 2013	• Debe formar parte del grupo de "Administración de la organización".
Establecer los derechos de buzón	
Exchange 2007	• Debe tener el rol de "Administrador de sólo vista de Exchange", permiso de "Administración del almacén de información" y permiso de "Escritura" en el almacén de buzones donde se encuentra el buzón.
Exchange 2010	• Debe formar parte del grupo de "Administración de la organización".
Exchange 2013	• Debe formar parte del grupo de "Administración de la organización".
Informes de Exchange	
Informes de Exchange	• Debe tener el rol de "Administrador de solo vista de Exchange".

Gestión e informes de Microsoft 365

Gestión

Recomendado: Usar una cuenta que tenga el rol de "Administrador global".

Operación	Nombre del rol
Gestionar usuarios, contactos y grupos	• Administrador de usuarios
Restablecer contraseñas, y bloquear o desbloquear administradores	• Administrador de autenticación privilegiado
Gestionar la asignación de roles en Azure AD	• Administrador de rol privilegiado
Actualizar las propiedades del buzón	• Administrador de Exchange
Gestionar Microsoft Teams	• Administrador de Teams
Obtener informes sobre todos los servicios de Microsoft 365	• Lector global

Informes

Operación	Ámbito
Obtener logs de auditoría e informes de buzón	• Lector de seguridad
Informes de Exchange Online	• Administrador de Exchange

A continuación se enumeran los roles y permisos (alcance mínimo) necesarios para una aplicación de Azure AD configurada en ADManager Plus.

Módulo	Nombre de API	Permiso	Ámbito
Gestión	Gráficos de Microsoft	User.ReadWrite.All	Crear, modificar, eliminar o restaurar usuarios.
		Group.ReadWrite.All	Crear, modificar, eliminar o restaurar grupos. Añadir o eliminar miembros y propietarios de grupos.
Informes	Gráficos de Microsoft	User.Read.All	Obtener informes de usuarios y miembros de grupos.
		Group.Read.All	Obtener informes de grupo.
		Contacts.Read	Obtener informes de contacto.
		Reports.Read.All	Obtener informes de uso.
		Organization.Read.All	Obtener informes detallados de licencias
		AuditLog.Read.All	Obtener informes basados en el log de auditoría.
	Gráficos de Azure Active Directory	Domain.Read.All	Obtener informes basados en el dominio.

Gestión e informes de Google Workspace	
Gestión	Ámbitos de API: https://www.googleapis.com/auth/admin.directory.user https://www.googleapis.com/auth/admin.directory.group https://www.googleapis.com/auth/admin.directory.orgunit
Informes	Ámbitos de API: https://www.googleapis.com/auth/admin.directory.user
Respaldo y recuperación	
AD	• Debe ser miembro del grupo de "Operadores de cuentas".
Google Workspace	• Debe tener una cuenta de servicio con privilegios de "Administrador global" para su inquilino de Google Workspace.

Migración de AD	
Migración de usuario	• Administrador de empresa
Integraciones	
ServiceNow	• Para realizar acciones de gestión de AD desde la consola de ServiceNow, el usuario debe tener asignados los roles ITIL y x_manen_admanager.admanager_admin en ServiceNow. • Para solicitar acciones de gestión de AD en ServiceNow, el usuario debe tener asignado el rol x_manen_admanager.admanager_requester en ServiceNow.
Zendesk	• Debe ser un administrador para configurar los detalles del servidor de ADManager Plus. • Debe tener privilegios del rol "Personal" para realizar acciones de AD desde los tickets.
MSSQL	• Debe tener el permiso "Seleccionar" para la tabla y el esquema.
Oracle	• Debe tener el permiso "Seleccionar" para la tabla y el esquema.
Workday	• Debe tener acceso a los servicios web de Workday y derechos para ver los detalles de los usuarios en la organización.
Ultipro	• Debe ser una cuenta de servicio web y tener permisos para acceder a los campos utilizados en el mapeo entre Fuente de datos - LDAP durante la configuración.
BambooHr	• Debe tener permisos para acceder a los campos utilizados en el mapeo entre Fuente de datos - LDAP durante la configuración.

Para obtener más información sobre cómo otorgar los privilegios necesarios a la cuenta de servicio, consulte este documento.

ADSelfService Plus

Consulte la siguiente tabla en la que se enumeran los permisos necesarios para llevar a cabo distintas operaciones de autoservicio y aprovechar otras funciones de ADSelfService Plus.

Operación	Permisos necesarios
Autoservicio de restablecimiento de contraseñas	• Restablecer la contraseña para los objetos de usuario. • Leer pwdLastSet para los objetos de usuario. • Escribir pwdLastSet para los objetos de usuario.
Autoservicio de desbloqueo de cuentas	• Leer lockoutTime para los objetos de usuario. • Escribir lockoutTime para los objetos de usuario.
Autoservicio de actualización de los atributos del usuario	• Leer para los objetos de usuario. • Escribir para los objetos de usuario. **Nota:** También es posible conceder los permisos para modificar, leer y escribir atributos específicos en lugar de todo el objeto.
Sincronizar los objetos de usuario de AD eliminados	• Permiso para replicar los cambios de directorio.
Mostrar la política de contraseña granular	• Leer para los objetos msDS-PasswordSettings. • Leer para los objetos msDS-PasswordSettingsContainer.
Autoservicio de suscripción a grupos de correo	• Leer miembros para los objetos de grupo. • Escribir miembros para los objetos de grupo.
Inicio de sesión único NTLM	• Crear para los objetos de equipo. • Leer para los objetos de equipo.
Forzar la inscripción mediante un script de inicio de sesión	• Leer scriptPath para los objetos de usuario. • Escribir scriptPath para los objetos de usuario.
Ver el informe de usuarios eliminados	• Membresía al grupo de "Administradores de dominio".
Instalación de GINA	• Membresía al grupo de "Administradores de dominio".
Configuración de alta disponibilidad	• Membresía al grupo de "Administradores de dominio".

Para obtener más información sobre cómo otorgar los privilegios necesarios a la cuenta de servicio, consulte este documento.

ADAudit Plus

Consulte la siguiente tabla en la que se enumeran los permisos necesarios para auditar AD, Azure AD y los servidores de archivos de su entorno utilizando ADAudit Plus.

Operación	Permisos necesarios
Leer logs de eventos	• Privilegio para gestionar el log de auditoría y seguridad • Membresía al grupo de "Lectores del log de eventos" • Permiso de DCOM • Permiso de WMI
Configurar la política de auditoría automáticamente	Membresía al grupo de "Propietarios creadores de directivas de grupo".
Auditar los archivos compartidos	Membresía al grupo de "Administradores locales".
Auditar Azure AD	Permisos de la API de gráficos de Microsoft: • Application.Read.All • AuditLog.Read.All • Directory.Read.All • IdentityRiskEvent.Read.All • Group.Read.All • User.Read.All

Exchange Reporter Plus

Exchange Reporter Plus requiere una cuenta que disponga de los permisos indicados en la siguiente tabla.

Operación	Permisos necesarios
Recopilación de datos esenciales **Nota:** Este es un requisito obligatorio para realizar otras operaciones.	• Privilegio de lectura LDAP sobre todos los objetos de GC • Privilegio de lectura para Invoke-Command PowerShell • Privilegio de lectura para consultas WMI • Privilegio de lectura para archivos de la base de datos
Membresía a la lista de distribución de Exchange Server	• Privilegio de lectura para LDAP • Permiso de solo vista para destinatarios RBAC
Propiedades de la cuenta de buzón de Exchange Server	• Privilegio de lectura para LDAP • Permiso de solo vista para destinatarios RBAC
Propiedades de la carpeta pública de Exchange Server	• Privilegio de lectura para LDAP • Permiso de solo vista para destinatarios RBAC
Logs de tráfico de Exchange Server	• Privilegio de lectura para LDAP • Acceso a la carpeta de logs de IIS • Permiso de solo vista para destinatarios RBAC para informes de Active Sync
Logs de OWA fallido de los logs de OWA de Exchange Server	• Privilegio de lectura para LDAP • Permiso de solo vista para destinatarios RBAC
Permiso de buzón de Exchange Server	• Privilegio de lectura para LDAP • Permiso de solo vista para destinatarios RBAC
Permiso de grupo de distribución de Exchange Server	• Privilegio de lectura para LDAP • Permiso de solo vista para destinatarios RBAC
Generación de informes de contenido de Exchange Server	• Privilegio de lectura para LDAP • Privilegio de lectura para Exchange Web Services
Informes de auditoría de Exchange Server	• Privilegio de lectura para logs de eventos de Exchange Server • Privilegio de lectura para logs de eventos del controlador de dominio

Informes de auditoría avanzada de Exchange Server	• Permiso de solo vista para logs de auditoría RBAC • Permiso de solo vista para la configuración RBAC
Monitoreo de Exchange Server	• Privilegio de lectura para consultas WMI • Acceso de lectura para la ruta de la carpeta de la base de datos • Acceso de lectura - Almacenamiento para Invoke-Command PowerShell • Monitoreo • Permiso de solo vista para la configuración - Todas las demás categorías
Búsqueda de contenido de Exchange Server	• Permisos de acceso total para todos los buzones, o • Roles de ApplicationImpersonation

Exchange Online

Operación	Nombre del rol	Ámbito
Informes	Lector global	Obtener informes sobre todos los servicios de Microsoft 365.
	Lector de seguridad	Obtener logs de auditoría e informes de buzón.
Auditoría	Lector de seguridad	Obtener logs de auditoría e informes de inicio de sesión.

A continuación se enumeran los roles y permisos, o alcance mínimo, necesarios para una aplicación de Azure AD configurada en Exchange Reporter Plus.

Módulo	Nombre de API	Permiso	Ámbito
Informes	Gráficos de Microsoft	User.Read.All	Obtener informes de usuarios y miembros de grupos.
		Group.Read.All	Obtener informes de grupo.
		Contacts.Read	Obtener informes de contacto.
		Files.Read.All	Obtener informes de OneDrive for Business.
		Reports.Read.All	Obtener informes de uso.

		Organization.Read.All	Obtener informes detallados de licencias.
		AuditLog.Read.All	Obtener informes basados en el log de auditoría.
		ChannelMember.Read.All (not available in Chinese tenant)	Obtener informes de miembros del canal de Microsoft Teams.
		Application.Read.All	Obtener los detalles de la aplicación Azure AD.
		Sites.Read.All	Obtener los detalles del sitio de SharePoint.
		Policy.Read.All	Configurar los detalles de la política de acceso condicional.
		Calendars.Read	Obtener los detalles del calendario de los usuarios.
	Gestión de Office 365	ActivityFeed.Read	Leer los datos de auditoría de la organización.
Auditoría	Gestión de Office 365	ActivityFeed.Read	Leer los datos de actividad de la organización.

Informes de Skype for Business Server

Informes de Skype for Business Server	• El usuario debe ser miembro del grupo CsAdministrator o CsViewOnlyAdministrator.

Para obtener más información sobre cómo otorgar los privilegios necesarios a la cuenta de servicio, consulte este documento.

M365 Manager Plus

A continuación se enumeran los roles y permisos, o alcance mínimo, necesarios para una cuenta de servicio configurada en M365 Manager Plus.

Operación	Nombre del rol	Ámbito
Gestión	Administrador de usuarios	Gestionar usuarios, contactos y grupos.
	Administrador de autenticación privilegiado	Restablecer contraseñas, y bloquear o desbloquear administradores.
	Administrador de rol privilegiado	Gestionar la asignación de roles en Azure AD.
	Administrador de Exchange	Actualizar las propiedades del buzón.
	Administrador de Teams	Gestionar Microsoft Teams.
Informes	Lector global	Obtener informes sobre todos los servicios de Microsoft 365.
	Lector de seguridad	Obtener logs de auditoría e informes de buzón.
Auditoría y alertas	Lector de seguridad	Obtener logs de auditoría e informes de inicio de sesión.

Nota:

- Si una aplicación de Azure AD no está configurada para M365 Manager Plus, se requiere el rol **Administrador de soporte de servicios** para la función de monitoreo.
- Es necesario configurar una aplicación de Azure AD para M365 Manager Plus con el fin de utilizar la función de **Búsqueda de contenido.**

A continuación se enumeran los roles y permisos, o alcance mínimo, necesarios para una aplicación de Azure AD configurada en M365 Manager Plus.

Módulo	Nombre de API	Permiso	Ámbito
Gestión	Gráficos de Microsoft	User.ReadWrite.All	Crear, modificar, eliminar o restaurar usuarios.
		Group.ReadWrite.All	Crear, modificar, eliminar o restaurar grupos. Añadir o eliminar miembros y propietarios de grupos.
		AdminsitrativeUnit. ReadWrite.All	Añadir miembros a las unidades administrativas.
		RoleManagement. ReadWrite.Directory	Añadir roles de directorio a los usuarios.
Informes	Gráficos de Microsoft	User.Read.All	Obtener informes de usuarios y miembros de grupos.
		Group.Read.All	Obtener informes de grupo.
		Contacts.Read	Obtener informes de contacto.
		Files.Read.All	Obtener informes de OneDrive for Business.
		Reports.Read.All	Obtener informes de uso.
		Organization.Read.All	Obtener informes detallados de licencias.
		AuditLog.Read.All	Obtener informes basados en el log de auditoría.
		ChannelMember.Read.All (no disponible en inquilino chino)	Obtener informes de miembros del canal de Microsoft Teams.
		Application.Read.All	Obtener los detalles de la aplicación Azure AD.
		Sites.Read.All	Obtener los detalles del sitio de SharePoint.
		Policy.Read.All	Configurar los detalles de la política de acceso condicional.
		Calendars.Read	Obtener los detalles del calendario de los usuarios.
	Gestión de Office 365	ActivityFeed.Read	Leer los datos de auditoría de la organización.

Auditoría y alertas	Gestión de Office 365	ActivityFeed.Read	Leer los datos de actividad de la organización.
Monitoreo	Gráficos de Microsoft	ServiceHealth.Read.All	Obtener informes de salud y rendimiento.
Búsqueda de contenido	Gráficos de Microsoft	Mail.Read	Obtener informes de búsqueda de contenido.
Configuración	Gráficos de Microsoft	Application.ReadWrite.All	Modificar los detalles de la aplicación.

RecoveryManager Plus

En la siguiente tabla se explica el nivel de privilegios necesarios para realizar copias de seguridad y restauraciones con RecoveryManager Plus.

Operación	Nombre del rol	Ámbito
Respaldo y recuperación de AD	• Administrador del dominio • Administrador del esquema*	* Si desea almacenar las contraseñas de las cuentas de usuario cuando se eliminen, asegúrese de que la cuenta configurada en RecoveryManager Plus tiene asignado el rol de "Administrador del esquema". Si opta por guardar las contraseñas de las cuentas de usuario, RecoveryManager Plus modificará el esquema de AD e indicará a AD que conserve el atributo Unicode-pwd cuando se elimine un usuario. Se necesita el rol de "Administrador del esquema" para modificar el esquema respectivamente.
Respaldo y recuperación de Azure AD	Administrador con el rol de administrador global	
Respaldo y recuperación de Exchange	Administrador que es miembro del grupo de rol de gestión de la organización	
Respaldo y recuperación de Exchange Online	Administrador de SharePoint	
Respaldo y recuperación de Google Workspace	Administrador del dominio de Google Workspace	

SharePoint Manager Plus

SharePoint Manager Plus requiere que se asignen los siguientes roles y permisos de Microsoft 365 a la cuenta de usuario.

SharePoint on-premises

Nota: Se necesita el permiso de "Administrador de la colección de sitios" para que las respectivas colecciones de sitios puedan realizar cualquier operación.

Operación	Permisos necesarios
Informes, gestión y migración	• El usuario debe ser miembro del grupo de "Administradores" integrado en el servidor de SharePoint. • El usuario debe ser miembro del grupo de "Administradores de granjas". Abra la administración web central y añada el usuario al grupo de "Administradores de granjas". • Se necesita esta configuración de GPO si el producto no está instalado en un servidor de SharePoint.
Auditoría	Los ajustes de auditoría de colecciones de sitios deben estar habilitados para las respectivas colecciones de sitios.
Informes del log de IIS	El usuario debe ser miembro del grupo de "Administradores" integrado en el servidor de IIS.

Microsoft 365 SharePoint

Nota: Se necesita el permiso de "Administrador de la colección de sitios" para que las respectivas colecciones de sitios puedan realizar cualquier operación.

Para la cuenta de servicio utilizada para configurar SharePoint Manager Plus

Informes, gestión y migración	Rol de administrador de SharePoint
Auditoría	Roles de "Log de auditoría" y "Solo ver log de auditoría"

Para aplicaciones Azure	
Informes, gestión y migración	Sites.FullControl.All
Auditoría	Office 365 Exchange Online
Monitoreo	API de gestión de Office 365
Servidor de correo	Gráficos de Microsoft

Nuestros productos

Log360 | ADManager Plus | ADAudit Plus | ADSelfService Plus

Exchange Reporter Plus | RecoveryManager Plus

Acerca de ManageEngine AD360

AD360 es una solución unificada de gestión de accesos e identidades que ayuda a gestionar identidades, proteger el acceso y garantizar el cumplimiento. Viene con potentes funciones como la gestión automatizada del ciclo de vida de la identidad, inicio de sesión único seguro, MFA adaptativa, flujos de trabajo basados en aprobación, protección contra amenazas de identidad basada en UBA e informes de auditoría históricos de AD, Exchange Server y Microsoft 365. La interfaz intuitiva de AD360 y sus potentes funciones la convierten en la solución ideal para todas sus necesidades de IAM, incluyendo el fomento de un entorno de confianza cero.

$ Cotizar Descargar