O365 Admin Roles for Privilege Identity Management (PIM)

Detailed explanation for each role can be found at : [https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-](https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles) [roles](https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles)

| O365 Admin Role | Description | Primary Approver | Secondary Approver | Can self- approve? (If  eligible) |
| --- | --- | --- | --- | --- |
| Application Administrator | Users with this role can create and manage all aspects of app registrations and  enterprise apps | AD Enterprise systems | CIO | No |
| Application Developer | Users with this role can create application registrations independent of the ‘Users can register applications’ setting | AD Enterprise systems | CIO | No |
| Attack Payload Author | Can create attack payloads that an administrator can initiate later. | National security manager | AD Enterprise systems | yes |
| Attack Simulation Administrator | Can create and manage all aspects of attack simulation campaigns. | National security manager | AD Enterprise systems | no |
| Authentication Administrator | Can access to view, set and reset authentication method information for any non- admin user. | National security manager | AD Enterprise systems | No |
| Authentication Policy Administrator | Can create and manage all aspects of authentication methods and password protection policies. | National security manager | AD Enterprise systems | no |
| Azure AD Joined Device Local Administrator | Users assigned to this role are added to the local administrators group on Azure AD-joined devices. | National Manager, Digital Platform Services | AD Enterprise systems | no |
| Azure DevOps Administrator | Can manage Azure DevOps organization policy and settings. | AD Enterprise systems | CIO | no |
| Azure Information Protection Administrator | Can manage all aspects of the Azure Information Protection product. | National security manager | AD Enterprise systems | no |
| B2C IEF Keyset Administrator | Manage secrets for federation and encryption in the Identity Experience Framework. | Associate Director,Service Delivery, IT Client Services | CIO | No |
| B2C IEF Policy Administrator | Create and manage trust framework policies in the Identity Experience Framework. | Associate Director,Service Delivery, IT Client Services | CIO | No |
| Billing Administrator | Makes purchases, manages subscriptions, manages support tickets, and monitors  service health. | National Manager, Technology Services, Technology Services | Associate Director,Service Delivery, IT Client Services | Yes |
| Cloud Application Administrator | Users with this role can create and manage all aspects of app registrations and enterprise apps except App Proxy | National Manager, Digital Platform Services | AD Enterprise systems | No |
| Cloud Device Administrator | Full access to manage devices in Azure AD. | National Manager, Digital Platform Services | AD Enterprise systems | No |
| Compliance Administrator | Users with this role have management permissions within in the Office 365 Security & Compliance Center and Exchange Admin Center. | National security manager | AD Enterprise systems | No |
| Compliance Data Administrator | Creates and manages compliance content. | National security manager | AD Enterprise systems | No |
| Conditional Access Administrator | Users with this role have the ability to manage Azure Active Directory conditional  access settings. | National security manager | AD Enterprise systems | No |
| Customer LockBox Access Approver | Can approve Microsoft support requests to access customer organizational data | National security manager | AD Enterprise systems | No |
| Desktop Analytics Administrator | Users in this role will have access to manage Desktop Analytics and Office Customization & Policy Services. For Desktop Analytics, this includes the ability to view asset inventory, create deployment plans, and view deployment and health status. For Office Customization & Policies Services, this role will enable users to  manage Office polices. | National Manager, Digital Platform Services | AD Enterprise systems | No |
| Directory Readers | Allows access to various read only tasks in the directory. | National security manager | AD Enterprise systems | Yes |
| Directory Synchronization Accounts | Only used by Azure AD Connect service. | AD Enterprise systems | CIO | No |
| Directory Writers | Allows access read tasks and a subset of write tasks in the directory. | National security manager | AD Enterprise systems | No |
| Domain Name Administrator | Domain Name Administrator | AD Enterprise systems | CIO | no |
| Dynamics 365 Administrator | Can manage all aspects of the Dynamics 365 product. | AD Enterprise systems | CIO | no |
| Exchange Administrator | Users with this role have global permissions within Microsoft Exchange Online | National Manager, Technology Services, Technology Services | Associate Director,Service Delivery, IT Client Services | No |
| Exchange Recipient Administrator | Can create or update Exchange Online recipients within the Exchange Online organization. | National Manager, Technology Services, Technology Services | Associate Director,Service Delivery, IT Client Services | No |
| External ID User Flow Administrator | Can create and manage all aspects of user flows. | AD Enterprise systems | CIO | No |
| External ID User Flow Attribute Administrator | Can create and manage the attribute schema available to all user flows. | AD Enterprise systems | CIO | No |
| External Identity Provider Administrator | Configure identity providers for use in direct federation. | Associate Director,Service Delivery, IT Client Services | CIO | No |
| Global Administrator | Users with this role have access to all administrative features in Azure Active  Directory | AD Enterprise systems | CIO | No |
| Global Reader | Can read everything that a global admin can read but not update anything | Associate Director,Service Delivery, IT Client Services | CIO | Yes |
| Groups Administrator | Can manage all aspects of groups and group settings like naming and expiration policies. | National Manager, Technology Services, Technology Services | Associate Director,Service Delivery, IT Client Services | Yes |
| Guest Inviter | Users in this role can manage Azure Active Directory B2B guest user invitations when the “Members can invite” user setting is set to No | Associate Director,Service Delivery, IT Client Services | CIO | Yes |
| HelpDesk Administrator | Can reset passwords for non-administrators and Helpdesk (Password) Administrators. | National Manager, Technology Services, Technology Services | Associate Director,Service Delivery, IT Client Services | Yes |
| Hybrid Identity Administrator | Can manage AD to Azure AD cloud provisioning, Azure AD Connect, and federation settings. | AD Enterprise systems | CIO | No |
| Insights Administrator | Has administrative access in the Microsoft 365 Insights app. | Associate Director,Service Delivery, IT Client Services | CIO | Yes |
| Insights Business Leader | Can view and share dashboards and insights via the M365 Insights app. | Associate Director,Service Delivery, IT Client Services | CIO | Yes |
| Intune Service Administrator | Users with this role have global permissions within Microsoft Intune Online | Gordon  Howell | AD Enterprise systems | Yes |
| Kaizala Administrator | Can manage settings for Microsoft Kaizala. | National Manager, Digital Platform Services | AD Enterprise systems | Yes |
| Knowledge Administrator | Can configure knowledge, learning, and other intelligent features. | Associate Director,Service Delivery, IT Client Services | CIO | Yes |
| License Administrator | Users with this role can manage product licenses on users and groups | National Manager, Technology Services, Technology Services | Associate Director,Service Delivery, IT Client Services | Yes |
| Message center privacy reader | Can read Message Center posts, data privacy messages, groups, domains and subscriptions. | National security manager | AD Enterprise systems | Yes |
| Message Center Reader | Users with this role can read messages and updates for their organization in Office 365 Message Center only | National Manager, Technology Services, Technology Services | Associate Director,Service Delivery, IT Client Services | Yes |
| Modern Commerce User | Can manage commercial purchases for a company, department or team. | Associate Director,Service Delivery, IT Client Services | CIO | Yes |
| Network Administrator | Can manage network locations and review enterprise network design insights for Microsoft 365 Software as a Service applications. | AD Enterprise systems | CIO | Yes |
| Office Apps Administrator | Can manage Office apps' cloud services, including policy and settings management, and manage the ability to select, unselect and publish "what's new" feature content to end-user’s devices. | National Manager, Digital Platform Services | AD Enterprise systems | Yes |
| Password Administrator | Users with this role can change passwords, manage service requests, and monitor  service health. | National Manager, Technology Services, Technology Services | Associate Director,Service Delivery, IT Client Services | Yes |
| Power BI Administrator | Users with this role have global permissions within Microsoft Power BI | AD Enterprise systems | CIO | Yes |
| Power Platform Administrator | Can create and manage all aspects of Microsoft Dynamics 365, PowerApps and Microsoft Flow. | AD Enterprise systems | CIO | Yes |
| Printer Administrator | Can manage all aspects of printers and printer connectors. | National Manager, Digital Platform Services | AD Enterprise systems | Yes |
| Printer Technician | Can register and unregister printers and update printer status. | National Manager, Digital Platform Services | AD Enterprise systems | Yes |
| Privileged Authentication Administrator | Can access to view, set and reset authentication method information for any user (admin or non-admin). | National security manager | AD Enterprise systems | No |
| Privileged Role Administrator | Users with this role can manage role assignments in Azure Active Directory and Azure AD Privileged Identity Management. | National security manager | AD Enterprise systems | No |
| Reports Reader | Users with this role can view usage reporting data and the reports dashboard in Office 365 admin center and the adoption context pack in PowerBI. | National Manager, Technology Services | Associate Director,Service Delivery, IT Client Services | Yes |
| Search Administrator | Can create and manage all aspects of Microsoft Search settings. | National Manager, Digital Platform Services | AD Enterprise systems | Yes |
| Search Editor | Can create and manage the editorial content such as bookmarks, Q and As, locations, floorplan. | National Manager, Digital Platform Services | AD Enterprise systems | Yes |
| Security Administrator | Users with this role have all of the read-only permissions of the Security reader role, plus the ability to manage configuration for security-related service | National security manager | AD Enterprise systems | No |
| Security Operator | Creates and manages security events. | National security manager | AD Enterprise systems | No |
| Security Reader | Users with this role have global read-only access, including all information in Azure Active Directory, Identity Protection, Privileged Identity Management | National security manager | AD Enterprise systems | Yes |
| Service Support Administrator | Users with this role can open support requests with Microsoft for Azure and Office 365 services | National Manager, Technology Services | Associate Director,Service Delivery, IT Client Services | Yes |
| SharePoint Administrator | Users with this role have global permissions within Microsoft SharePoint Online | Gordon  Howell | AD Enterprise systems | No |
| Skype for Business Administrator | Users with this role have global permissions within Microsoft Skype for Business | National Manager, Digital Platform Services | AD Enterprise systems | No |
| Teams Communications Administrator | Can manage calling and meetings features within the Microsoft Teams service | National Manager, Digital Platform Services | AD Enterprise systems | No |
| Teams Communications Support Engineer | Can troubleshoot communications issues within Teams using advanced tools | National Manager, Digital Platform Services | AD Enterprise systems | Yes |
| Teams Communications Support Specialist | Can troubleshoot communications issues within Teams using basic tools | National Manager, Digital Platform Services | AD Enterprise systems | Yes |
| Teams Devices Administrator | Can perform management related tasks on Teams certified devices. | National Manager, Digital Platform Services | AD Enterprise systems | Yes |
| Teams Administrator | Can manage the Microsoft Teams service | National Manager, Digital Platform Services | AD Enterprise systems | No |
| Usage Summary Reports Reader | Can see only tenant level aggregates in Microsoft 365 Usage Analytics and Productivity Score. | National Manager, Technology Services, Technology Services | Associate Director,Service Delivery, IT Client Services | Yes |
| User Administrator | Users with this role can create and manage all aspects of users and groups. | National Manager, Technology Services, Technology Services | Associate Director,Service Delivery, IT Client Services | Yes |
| Yammer Administrator | Manage all aspects of the Yammer service. | National Manager, Digital Platform Services | AD Enterprise systems | no |