AAD role fulfillment (appropriate account types and change practices) copy--original lives in 644- MI internal docs)

NOTE: Do not edit this page without explicit approval from Brian or Nathan.

This page discusses Azure AD roles. The table in the Request Fulfillment section below lists all Azure AD roles for the purpose of guiding role fulfillment operations. In some cases, there are specific restrictions on the appropriate type of accounts for a given role. Azure AD-only accounts are one such restriction, so there is also a section covering AAD-only account credential & lifecycle management practices.

The policy represented by this page was established via several approved Changes: CHG0036291 & CHG0037718.

Note: the existing Microsoft data model only allows Azure AD users and servicePrincipals to be members of a role. This document moves beyond that to discuss specific types of user accounts within the UW NetID system.

Relevant Microsoft role documentation (background info)

- **AAD admin roles: https://docs.microsoft.com/en-us/azure/active-directory/active-directory-assign-admin-roles-azure-portal**
- About O365 admin roles: https://support.office.com/en-us/article/about-office-365-admin-roles-da585eea-f576-4f55-a1e0-87090b6aaa9d
- About the Exchange Online admin role: https://support.office.com/en-us/article/about-the-exchange-online-admin-role-097ae285-c4af-4319-9770-e2559d66e4c8
- Permissions in Exchange Online: https://docs.microsoft.com/en-us/exchange/permissions-exo/permissions-exo
- Exchange built-in management roles: https://technet.microsoft.com/EN-US/library/dd638077(v=exchg.150).aspx
- Manage Exchange role groups: https://technet.microsoft.com/en-us/library/jj657480(v=exchg.150).aspx
- Exchange built-in role groups: https://technet.microsoft.com/EN-US/library/dd351266(v=exchg.150).aspx

AAD-only account credential and lifecycle management practices

- Accounts with admin roles listed above should only be in the uwnetid.onmicrosoft.com domain.
- Accounts should be named in the following form: tadm_<personal UW NetID>, e.g. tadm_barkills
- Credential issuance/binding should be strong. In person assignment of a password, immediately followed by enabling 2FA (where an exception is not present). See relevant CHG records about 2FA expectations.
- MI should review AAD-only accounts in AAD roles for continued health on a short cycle. Health is determined by:
    - <personal UW NetID> continues to have an employee affiliation. If it does not, an alert is raised to consider deprovisioning the role membership and possibly the account itself.
    - No known security alerts implicating this account. If there are, an alert is raised to determine whether mitigating actions are needed, such as removal from role membership, enabling 2FA, or other actions as circumstances suggest.
    - If servicePrincipal, credential has not expired.

Request Fulfillment

Roles are grouped with similar roles to help us more quickly understand their nature. Some roles have restrictions on which type of accounts are appropriate. Some roles have special notes. If a role has more than one name, other names are listed in parenthesis.

Note: unless otherwise noted as a CHG practice, the default expectation for role requests is that a comprehensive CHG is required, i.e. AAD CAB approval. Where the phrase "silent fulfillment" is used, this means that MI does not inform the CAB, i.e. there is a customer REQ. Where "MI fulfills as a routine CHG" is used, this is allowed to also be a REQ, provided MI has a clear tagging protocol to allow easy searching for role approvals in the future.

Name	Description	Grouping	Permitted account types	Notes	CHG practices
Partner Tier1 Support	"Retired" roles	Don't use (per Microsoft)	None	Microsoft has retired these roles and recommends no use of them	
Partner Tier2 Support	"Retired" roles	Don't use (per Microsoft)	None	Microsoft has retired these roles and recommends no use of them	
Device Managers	"Retired" roles	Don't use (per Microsoft)	None	Microsoft has retired these roles and recommends no use of them	
Device Users	"Retired" roles	Don't use (per Microsoft)	None	Microsoft has retired these roles and recommends no use of them	

Device Join	"Retired" roles	Don't use (per Microsoft)	None	Microsoft has retired these roles and recommends no use of them	
Workplace Device Join	"Retired" roles	Don't use (per Microsoft)	None	Microsoft has retired these roles and recommends no use of them	
Adhoc License Administrator	"Retired" roles	Don't use (per Microsoft)	None	Microsoft has retired these roles and recommends no use of them	
Email Verified User Creator	"Retired" roles	Don't use (per Microsoft)	None	Microsoft has retired these roles and recommends no use of them	
Mailbox Administrator	"Retired" roles	Don't use (per Microsoft)	None	Microsoft has retired these roles and recommends no use of them	
User	Guests are a special case and may or may not be considered a role.	General Purpose: Basic roles	any account type OK		N/A
Guest	Guests are a special case and may or may not be considered a role. Guests can be either UW accounts or accounts homed elsewhere, and fulfillment is not determined by the MI team.	General Purpose: Basic roles	N/A		N/A
Application Developer	Can create application registrations independent of the 'Users can register applications' setting.	General General Purpose: Basic roles	any account type OK		N/A
Guest Inviter	Can invite guest users independent of the ‘members can invite guests’ setting.	General Purpose: Basic roles	any account type OK		
Directory Readers	Can read basic directory information. Commonly used to grant directory read access to applications and guests.	General Purpose: Basic roles for applications	servicePrincipals + other account types considered upon request		MI uses existing access request form to manage. Silent fulfillment.
Directory Writers	This is a legacy role that is to be assigned to applications that do not support the Consent Framework. It should not be assigned to any users.	General Purpose: Basic roles for applications	servicePrincipals + other account types considered upon request	Use of this role should be carefully considered given that it does not use the consent framework.	MI uses existing access request form to manage. Silent fulfillment.
Directory Synchronization Accounts	Generally: Only used by Azure AD Connect service.	General Purpose: Basic roles for applications	servicePrincipals + other account types considered upon request	Use of this role should be carefully considered given that it is designed for a very specific purpose.	MI uses existing access request form to manage. Silent fulfillment.
Message Center Reader	Can read messages and updates for their organization in Office 365 Message Center only.	General Purpose: Basic roles	any account type OK		No CHG required; MI authorized to fulfill for any employee. Silent fulfillment.
Service Support Administrator (Service Administrator)	Can read service health information and manage support tickets.	Tier 2	any account type OK		If REQ comes for MI /MSCA service team member, then MI silently fulfills. Note: this is current practice as approved prior to AAD CAB
Helpdesk Administrator (Password Admin)	Can reset passwords for non-administrators and Helpdesk administrators.	Tier 2	sadm or servicePrincipals		If REQ comes in from IAM business team member, MI fulfills as a routine CHG
Exchange Service Administrator	Can manage all aspects of the Exchange product.	T3: Single App scoped	sadm or servicePrincipals		If REQ comes from MSCA, MI silently fulfills
Sharepoint Service Administrator	Can manage all aspects of the SharePoint service.	T3: Single App scoped	sadm or servicePrincipals		If REQ comes from MSCA, MI silently fulfills

Skype for Business administrator (Lync Service Administrator)	Can manage all aspects of the Skype for Business product.	T3: Single App scoped	sadm or servicePrincipals		If REQ comes from MSCA, MI silently fulfills
Intune Service Administrator	Can manage all aspects of the Intune product.	T3: Single App scoped	sadm or servicePrincipals		If REQ comes from MI/MWS, MI silently fulfills
CRM Service Administrator (Dynamics 365 Administrator)	Can manage all aspects of the Dynamics 365 product.	T3: Single App scoped	sadm or servicePrincipals		If REQ comes from MSCA, MI silently fulfills
PowerBI Service Administrator (PowerBI Administrator)	Can manage all aspects of the Power BI product.	T3: Single App scoped	sadm or servicePrincipals		If REQ comes from MSCA, MI silently fulfills
Customer LockBox Access Approver	Can approve Microsoft support requests to access customer organizational data.	T3: Single App scoped	sadm or servicePrincipals	Released but full AAD role documentation has been removed. Description: "Customer LockBox Access Approver has approval access to user data requests." https://www.microsoft.com/en-us/microsoft-365/blog/2015/04/21/announcing-customer-lockbox-for-office-365/. Intended purpose: add UW approval authority to grant Microsoft read level access to all O365 data in our tenant–if and only if, we turn on the customer lockbox setting (which we currently have not). As currently configured, Microsoft does not need any UW approval for this access.	If REQ comes from MSCA, MI silently fulfills
Cloud Application Administrator	Can create and manage all aspects of app registrations and enterprise apps except App Proxy.	T3: IAM integration: App Setup	sadm or servicePrincipals		If REQ comes in for IAM business team member, MI silently fulfills. Note: this is current practice as approved by prior CHG
Application Administrator	Can create and manage all aspects of app registrations and enterprise apps.	T3: IAM integration: App Setup	sadm or servicePrincipals		If REQ comes in for IAM business team member, MI silently fulfills. Note: this is current practice as approved by prior CHG
Billing Administrator	Can perform common billing related tasks like updating payment information.	T3: Broadly scoped	sadm or servicePrincipals		No use outside MI /MWS /MSCA teams allowed until scoped delegation is possible. MI silently fulfills.
Device Administrators		T3: Broadly scoped	wadm or servicePrincipals	No use of this role allowed until AU scoping is available and proven to work. Large sets of devices with the same account as admin is a recipe for large incident; this must be avoided.	No use outside MI /MWS /MSCA teams allowed until scoped delegation is possible. MI silently fulfills.

User Administrator	Can manage all aspects of users and groups, including resetting passwords for limited admins.	T3: Broadly scoped	sadm or servicePrincipals		If REQ comes in from IAM business team member or MSCA team member, MI silently fulfills.
Security Reader	Can read security information and reports in Azure AD and Office 365.	T3: Security	sadm or servicePrincipals		If REQ comes in for CISO or UWM Security team member, MI silently fulfills. Note: this is current practice as approved by prior CHG If REQ comes in for MSCA or IAM business team member, MI silently fulfills.
Reports Reader	Can read sign-in and audit reports.	T3: Security	sadm or servicePrincipals		If REQ comes in for CISO or UWM Security team member, MI silently fulfills. Note: this is current practice as approved by prior CHG If REQ comes in for MSCA or IAM business team member, MI silently fulfills.
Security Administrator	Can read security information and reports, and manage configuration in Azure AD and Office 365.	T3: Security	sadm or servicePrincipals		No use outside MI team allowed. MI fulfills requests as routine CHG.
Azure Information Protection Administrator (Information Protection Administrator)	Can manage all aspects of the Azure Information Protection product.	T3: IAM: Grant	AAD only[1] or servicePrincipals	Azure Information Protection is a single application, but has potential integrations to many applications. This role by itself does not allow enabling those integrations–only setting data protection policies for those applications which have chosen to integrate & leverage AIP.	No use outside MI team allowed. MI fulfills requests as routine CHG.
Privileged Role Administrator	Can manage role assignments in Azure AD, and all aspects of Privileged Identity Management.	T3: IAM: Grant	AAD only[1] or servicePrincipals	Can control other roles in some significant fashion, either directly managing them, controlling their authentication methods, or ability to sign in.	No use outside MI team allowed. MI fulfills requests as routine CHG.
Conditional Access Administrator	Can manage conditional access capabilities.	T3: IAM: Grant	AAD only[1] or servicePrincipals	Can control other roles in some significant fashion, either directly managing them, controlling their authentication methods, or ability to sign in.	No use outside MI team allowed. MI fulfills requests as routine CHG.

Authentication Administrator	Has access to view, set, and reset authentication method information for any non-admin user.	T3: IAM: Grant	sadm	Not released or fully documented, but discoverable. Account types based on description in Azure AD role template. Description: "Allowed to view, set and reset authentication method information for any non-admin user." & "Allowed to view, set and reset authentication method information for any user (admin or non-admin)."	If REQ comes in from IAM business team member, MI silently fulfills.
Privileged Authentication Administrator	Allowed to view, set and reset authentication method information for any user (admin or non-admin).	T3: IAM: Grant	AAD only[1] or servicePrincipals	Can control other roles in some significant fashion, either directly managing them, controlling their authentication methods, or ability to sign in. 6/2018: Not released or fully documented, but discoverable. Account types based on description in Azure AD role template. Description: "Allowed to view, set and reset authentication method information for any non-admin user." & "Allowed to view, set and reset authentication method information for any user (admin or non-admin)."	No use outside MI team allowed. MI fulfills requests as routine CHG.
Compliance Administrator	Can read and manage compliance configuration and reports in Azure AD and Office 365.	T3: IAM: Grant	AAD only[1] or servicePrincipals	Documented intended scope is Office 365, but UW believes the actual scope is broader.	No use outside MI /MSCA /MWS teams allowed. MI fulfills requests as routine CHG.
Company Administrator (Global Administrator)	Can manage all aspects of Azure AD and Microsoft services that use Azure AD identities.	T3: Tenant admin	AAD only[1] or servicePrincipals		No use outside MI /MSCA teams allowed. MI only fulfills requests as comprehensive CHG, requiring AAD CAB approval.
Desktop Analytics Administrator	Can access and manage Desktop management tools and services	T3: Broadly scoped	sadm or servicePrincipals, except as noted	Use of this role at this time is restricted to UW-IT, due to broad scoping.	Delegate fulfillment decision to MI. Silent fulfillment.
License Administrator	Users in this role can add, remove, and update license assignments on users, groups (using group-based licensing), and manage the usage location on users. The role does not grant the ability to purchase or manage subscriptions, create or manage groups, or create or manage users beyond the usage location. This role has no access to view, create, or manage support tickets.	T3: Broadly scoped	sadm or servicePrincipals, except as noted		Delegate fulfillment decision to MI. Silent fulfillment.
Cloud Device Administrator	Users in this role can enable, disable, and delete devices in Azure AD and read Windows 10 BitLocker keys (if present) in the Azure portal. The role does not grant permissions to manage any other properties on the device.	T3: Broadly scoped	sadm or servicePrincipals, except as noted		No use outside MI /MWS /MSCA teams allowed until scoped delegation is possible. Delegate fulfillment decision to MI. Silent fulfillment.
Teams Service Administrator	Can manage the Microsoft Teams service	T3: Single App scoped	sadm or servicePrincipals		If REQ comes in from MSCA, MI silently fulfills
Teams Communications Administrator	Can manage calling and meetings features within the Microsoft Teams service	T3: Single App scoped	sadm or servicePrincipals		If REQ comes in from MSCA, MI silently fulfills
Teams Communications Support Engineer	Can troubleshoot communications issues within Teams using advanced tools	T3: Single App scoped	sadm or servicePrincipals		If REQ comes in from MSCA, MI silently fulfills
Teams Communications Support Specialist	Can troubleshoot communications issues within Teams using basic tools	T3: Single App scoped	sadm or servicePrincipals		If REQ comes in from MSCA, MI silently fulfills

Message Center Privacy Reader	Users in this role can monitor all notifications in the Message Center, including data privacy messages. Message Center Privacy Readers get email notifications including those related to data privacy and they can unsubscribe using Message Center Preferences. Only the Global Administrator and the Message Center Privacy Reader can read data privacy messages. Additionally, this role contains the ability to view groups, domains, and subscriptions. This role has no permission to view, create, or manage service requests	T3: Security	sadm or servicePrincipals		If REQ comes in from CISO or UWM Security, MI fulfills as a routine CHG
B2C User Flow Administrator	Users with this role can create and manage B2C User Flows (aka "built-in" policies) in Azure Portal. By creating or editing user flows, these users can change the html/CSS/javascript content of the user experience, change MFA requirements per user flow, change claims in the token and adjust session settings for all policies in the tenant. On the other hand, this role does not include the ability to review user data, or make changes to the attributes that are included in the tenant schema. Changes to Identity Experience Framework (aka Custom) policies is also outside the scope of this role.	T3: IAM integration: App Setup	sadm or servicePrincipals		If REQ comes in from IAM business team member, MI silently fulfills
B2C User Flow Attribute Administrator	Users with this role add or delete custom attributes available to all user flows in the tenant. As such, users with this role can change or add new elements to the end user schema and impact the behavior of all user flows and indirectly result in changes to what data may be asked of end users and ultimately sent as claims to applications. This role cannot edit user flows.	T3: IAM integration: App Setup	sadm or servicePrincipals		If REQ comes in from IAM business team member, MI silently fulfills
B2C IEF Keyset Administrator	User can create and manage policy keys and secrets for token encryption, token signatures, and claim encryption/decryption. By adding new keys to existing key containers, this limited administrator can rollover secrets as needed without impacting existing applications. This user can see the full content of these secrets and their expiration dates even after their creation. **Important:** This is a sensitive role. The keyset administrator role should be carefully audited and assigned with care during preproduction and production.	T3: IAM integration: App Setup	AAD only user account	AAD only user account	If REQ comes in from IAM business team member, MI silently fulfills
External Identity Provider Administrator (B2C IEF Policy Administrator)	Users in this role have the ability to create, read, update, and delete all custom policies in Azure AD B2C and therefore have full control over the Identity Experience Framework in the relevant Azure AD B2C tenant. By editing policies, this user can establish direct federation with external identity providers, change the directory schema, change all user-facing content (HTML, CSS, JavaScript), change the requirements to complete an authentication, create new users, send user data to external systems including full migrations, and edit all user information including sensitive fields like passwords and phone numbers. Conversely, this role cannot change the encryption keys or edit the secrets used for federation in the tenant. **Important:** The B2 IEF Policy Administrator is a highly sensitive role which should be assigned on a very limited basis for tenants in production. Activities by these users should be closely audited, especially for tenants in production.	T3: IAM integration: App Setup	AAD only user account	AAD only user account	If REQ comes in from IAM business team member, MI silently fulfills
Compliance Data Administrator	Users with this role have permissions to protect and track data in the Microsoft 365 compliance center, Microsoft 365 admin center, and Azure. Users can also manage all features within the Exchange admin center, Compliance Manager, and Teams & Skype for Business admin center and create support tickets for Azure and Microsoft 365.	T3: Security	sadm or servicePrincipals	Note: this can only view data, not make changes like Compliance Admin can.	If REQ comes in from CISO /UWM Security /MSCA/MI /MWS, MI fulfills as a routine CHG
Security Operator	Users with this role can manage alerts and have global read-only access on security-related feature, including all information in Microsoft 365 security center, Azure Active Directory, Identity Protection, Privileged Identity Management and Office 365 Security & Compliance Center. More information about Office 365 permissions is available at Permissions in the Office 365 Security & Compliance Center.	T3: Security	sadm or servicePrincipals		If REQ comes in from CISO or UWM Security, MI fulfills as a routine CHG
Kaizala Administrator	Users with this role have global permissions to manage settings within Microsoft Kaizala, when the service is present, as well as the ability to manage support tickets and monitor service health. Additionally, the user can access reports related to adoption & usage of Kaizala by Organization members and business reports generated using the Kaizala actions.	T3: Single App scoped	sadm or servicePrincipals		If REQ comes in from MSCA, MI silently fulfills
Search Administrator	Users in this role have full access to all Microsoft Search management features in the Microsoft 365 admin center. Search Administrators can delegate the Search Administrators and Search Editor roles to users, and create and manage content, like bookmarks, Q&As, and locations. Additionally, these users can view the message center, monitor service health, and create service requests.	T3: Broadly scoped	sadm or servicePrincipals, except as noted		If REQ comes in from MSCA, MI silently fulfills
Search Editor	Users in this role can create, manage, and delete content for Microsoft Search in the Microsoft 365 admin center, including bookmarks, Q&As, and locations.	T3: Broadly scoped	sadm or servicePrincipals, except as noted		If REQ comes in from MSCA, MI silently fulfills
Printer Administrator	Can manage all aspects of printers and printer connectors	T3: Broadly scoped	sadm or servicePrincipals, except as noted	Information about this role is very limited at this time.	Delegate fulfillment decision to MI. Silent fulfillment.
Printer Technician	Can manage all aspects of printers and printer connectors	T3: Broadly scoped	sadm or servicePrincipals, except as noted	Information about this role is very limited at this time.	Delegate fulfillment decision to MI. Silent fulfillment.
Global reader	Can read everything that a global administrator can, but not update anything.	None (yet)		New AAD Roles as of 11/19/2019	None (yet)

Groups administrator	Can manage all aspects of groups and group settings like naming and expiration policies.	None (yet)		New AAD Roles as of 11/19/2019	None (yet)
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.	None (yet)		New AAD Roles as of 11/19/2019	None (yet)
Power platform administrator	Can create and manage all aspects of Microsoft Dynamics 365, PowerApps, and Microsoft Flows.	None (yet)		New AAD Roles as of 11/19/2019	None (yet)
Azure DevOps administrator	Can manage Azure DevOps organization policy and settings.	None (yet)			None (yet)

Footnotes:

[1] Accounts here have broad enterprise administration capabilities granted with significant potential impacts should it be compromised. We have separate Admin UW NetID types to segregate the impact should an account be compromised. In this case, segregation outside the UW NetID system, using AAD only acccounts improves both security and business continuity:

- If our hybrid authentication architecture fails, having a global administrator account which is unable to login poses a significant obstacle to business continuity.
- To provide Privileged Access Workstations for Azure AD tier 0, if federated accounts are used and we follow the trusted source principles that Microsoft strongly recommends, we'd have to pull a lot of IAM systems and staff accounts into that regimen, which would be very costly.

For these reasons, AAD only accounts are preferred. See AAD-only account section for relevant credential and lifecycle management practices.