Entra Directory Roles & PIM Security Documentation

centrelsolutionsdemo.onmicrosoft.com

Company Confidential

Document Properties

Author	CENTREL-WS01\XiaConfigurationDemo
Product	XIA Configuration Server [18.1.2.0]
Date	Wednesday, July 8, 2026 2:28:49 PM
Version	1.07

Table of Contents

Roles

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

143 Roles

Display Name	Assigned Principals
Agent ID Administrator	
Agent ID Developer	
Agent Registry Administrator	
AI Administrator	
AI Reader	
Application Administrator	
Application Developer	
Attack Payload Author	
Attack Simulation Administrator	
Attribute Assignment Administrator	
Attribute Assignment Reader	
Attribute Definition Administrator	XIA
Attribute Definition Reader	
Attribute Log Administrator	
Attribute Log Reader	
Attribute Provisioning Administrator	
Attribute Provisioning Reader	
Authentication Administrator	
Authentication Extensibility Administrator	
Authentication Extensibility Password Administrator	
Authentication Policy Administrator	
Azure AD Joined Device Local Administrator	
Azure DevOps Administrator	
Azure Information Protection Administrator	
B2C IEF Keyset Administrator	
B2C IEF Policy Administrator	
Billing Administrator	

Cloud App Security Administrator	
Cloud Application Administrator	XIA
Cloud Device Administrator	
Compliance Administrator	
Compliance Data Administrator	
Conditional Access Administrator	
Customer Delegated Admin Relationship Administrator	
Customer LockBox Access Approver	
Desktop Analytics Administrator	
Device Join	
Device Managers	
Device Users	
Directory Readers	Microsoft.Azure.SyncFabric
Directory Synchronization Accounts	On-Premises Directory Synchronization Service Account
Directory Writers	
Domain Name Administrator	
Dragon Administrator	
Dynamics 365 Administrator	
Dynamics 365 Business Central Administrator	
Edge Administrator	
Entra Backup Administrator	
Entra Backup Reader	
Entra Customer Lockbox Approver	
Exchange Administrator	
Exchange Backup Administrator	
Exchange Recipient Administrator	
Extended Directory User Administrator	
External ID User Flow Administrator	
External ID User Flow Attribute Administrator	
External Identity Provider Administrator	
Fabric Administrator	
Global Administrator	Backup Global Admin XIA

Global Reader	
Global Secure Access Administrator	
Global Secure Access Log Reader	
Groups Administrator	
Guest Inviter	
Guest User	
Helpdesk Administrator	
Hybrid Identity Administrator	
Identity Governance Administrator	
Insights Administrator	
Insights Analyst	
Insights Business Leader	
Intune Administrator	
IoT Device Administrator	
Kaizala Administrator	
Knowledge Administrator	
Knowledge Manager	
License Administrator	
Lifecycle Workflows Administrator	
Message Center Privacy Reader	
Message Center Reader	
Microsoft 365 Backup Administrator	
Microsoft 365 Migration Administrator	
Microsoft Graph Data Connect Administrator	
Microsoft Hardware Warranty Administrator	
Microsoft Hardware Warranty Specialist	
Network Administrator	
Office Apps Administrator	
On Premises Directory Sync Account	
Organizational Branding Administrator	
Organizational Data Source Administrator	
Organizational Messages Approver	
Organizational Messages Writer	

Partner Tier1 Support	
Partner Tier2 Support	
Password Administrator	
People Administrator	
Permissions Management Administrator	
Places Administrator	
Power Platform Administrator	
Printer Administrator	
Printer Technician	
Privileged Authentication Administrator	
Privileged Role Administrator	
Purview Workload Content Administrator	
Purview Workload Content Reader	
Purview Workload Content Writer	
Reports Reader	XIA
Restricted Guest User	
Search Administrator	
Search Editor	
Security Administrator	XIA
Security Operator	
Security Reader	
Service Support Administrator	
SharePoint Administrator	
SharePoint Advanced Management Administrator	
SharePoint Backup Administrator	
SharePoint Embedded Administrator	
Skype for Business Administrator	
Teams Administrator	
Teams Communications Administrator	
Teams Communications Support Engineer	
Teams Communications Support Specialist	
Teams Devices Administrator	
Teams External Collaboration Administrator	

Teams Reader	
Teams Telephony Administrator	
Tenant Creator	
Tenant Governance Administrator	
Tenant Governance Reader	
Tenant Governance Relationship Administrator	
Tenant Governance Relationship Reader	
Usage Summary Reports Reader	
User Administrator	
User Experience Success Manager	
Virtual Visits Administrator	
Viva Glint Tenant Administrator	
Viva Goals Administrator	
Viva Pulse Administrator	
Windows 365 Administrator	
Windows Update Deployment Administrator	
Workplace Device Join	
Yammer Administrator	

Agent ID Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Manage all aspects of agents in a tenant including identity lifecycle operations for agent blueprints, agent identity blueprint principals, agent identities, and agentic users.
Identifier	db506228-d27e-4b7d-95e5-295956d6615f
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	db506228-d27e-4b7d-95e5-295956d6615f
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.directory/agentIdentities/allProperties/read microsoft.directory/agentIdentities/appRoleAssignedTo/update microsoft.directory/agentIdentities/authentication/update microsoft.directory/agentIdentities/basic/update microsoft.directory/agentIdentities/create microsoft.directory/agentIdentities/delete microsoft.directory/agentIdentities/disable microsoft.directory/agentIdentities/enable microsoft.directory/agentIdentities/owners/update microsoft.directory/agentIdentities/tag/update microsoft.directory/agentIdentityBlueprintPrincipals/allProperties/read microsoft.directory/agentIdentityBlueprintPrincipals/appRoleAssignedTo/update microsoft.directory/agentIdentityBlueprintPrincipals/authentication/update microsoft.directory/agentIdentityBlueprintPrincipals/basic/update microsoft.directory/agentIdentityBlueprintPrincipals/create microsoft.directory/agentIdentityBlueprintPrincipals/delete microsoft.directory/agentIdentityBlueprintPrincipals/disable microsoft.directory/agentIdentityBlueprintPrincipals/enable microsoft.directory/agentIdentityBlueprintPrincipals/owners/update microsoft.directory/agentIdentityBlueprintPrincipals/tag/update microsoft.directory/agentIdentityBlueprints/allProperties/read microsoft.directory/agentIdentityBlueprints/allProperties/update microsoft.directory/agentIdentityBlueprints/appRoles/update microsoft.directory/agentIdentityBlueprints/audience/update microsoft.directory/agentIdentityBlueprints/authentication/update microsoft.directory/agentIdentityBlueprints/basic/update microsoft.directory/agentIdentityBlueprints/create microsoft.directory/agentIdentityBlueprints/credentials/update microsoft.directory/agentIdentityBlueprints/delete microsoft.directory/agentIdentityBlueprints/owners/update microsoft.directory/agentIdentityBlueprints/permissions/update microsoft.directory/agentIdentityBlueprints/tag/update microsoft.directory/agentUsers/assignLicense microsoft.directory/agentUsers/basic/update microsoft.directory/agentUsers/create microsoft.directory/agentUsers/delete microsoft.directory/agentUsers/disable microsoft.directory/agentUsers/enable microsoft.directory/agentUsers/invalidateAllRefreshTokens microsoft.directory/agentUsers/lifeCycleInfo/read microsoft.directory/agentUsers/lifeCycleInfo/update microsoft.directory/agentUsers/manager/update microsoft.directory/agentUsers/photo/update microsoft.directory/agentUsers/reprocessLicenseAssignment microsoft.directory/agentUsers/restore microsoft.directory/agentUsers/revokeSignInSessions microsoft.directory/agentUsers/sponsors/update microsoft.directory/agentUsers/usageLocation/update microsoft.directory/agentUsers/userPrincipalName/update microsoft.directory/auditLogs/allProperties/read microsoft.directory/deletedItems.agentIdentities/delete microsoft.directory/deletedItems.agentIdentities/restore

	microsoft.directory/deletedItems.agentIdentityBlueprintPrincipals/delete microsoft.directory/deletedItems.agentIdentityBlueprintPrincipals/restore microsoft.directory/deletedItems.agentIdentityBlueprints/delete microsoft.directory/deletedItems.agentIdentityBlueprints/restore microsoft.directory/externalUserProfiles/standard/read microsoft.directory/groups.unified/createAsOwner microsoft.directory/groups/hiddenMembers/read microsoft.directory/organization/standard/read microsoft.directory/policies/standard/read microsoft.directory/signInReports/allProperties/read microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Agent ID Developer

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Create an agent identity blueprint and its agent identity blueprint principal in a tenant. User will be added as an owner of the created agent identity blueprint and its agent identity blueprint principal.
Identifier	adb2368d-a9be-41b5-8667-d96778e081b0
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	adb2368d-a9be-41b5-8667-d96778e081b0
Version	1

Inheritance

Inherited Roles	

Allowed Permissions

Allowed Permissions	microsoft.directory/agentIdentityBlueprints/createAsOwner microsoft.directory/servicePrincipals/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Agent Registry Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Manage all aspects of the Agent Registry service in Microsoft Entra ID
Identifier	6b942400-691f-4bf0-9d12-d8a254a2baf5
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	6b942400-691f-4bf0-9d12-d8a254a2baf5
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.agentRegistry/allEntities/allProperties/allTasks

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

AI Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Manage all aspects of Microsoft 365 Copilot and AI-related enterprise services in Microsoft 365.
Identifier	d2562ede-74db-457e-a7b6-544e236ebb61
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	d2562ede-74db-457e-a7b6-544e236ebb61
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.directory/agentUsers/assignLicense microsoft.directory/agentUsers/basic/update microsoft.directory/agentUsers/create microsoft.directory/agentUsers/delete microsoft.directory/agentUsers/disable microsoft.directory/agentUsers/enable microsoft.directory/agentUsers/invalidateAllRefreshTokens microsoft.directory/agentUsers/lifeCycleInfo/read microsoft.directory/agentUsers/lifeCycleInfo/update microsoft.directory/agentUsers/manager/update microsoft.directory/agentUsers/photo/update microsoft.directory/agentUsers/reprocessLicenseAssignment microsoft.directory/agentUsers/restore microsoft.directory/agentUsers/revokeSignInSessions microsoft.directory/agentUsers/sponsors/update microsoft.directory/agentUsers/usageLocation/update microsoft.directory/agentUsers/userPrincipalName/update microsoft.directory/entitlementManagement/allProperties/read microsoft.directory/subscribedSkus/standard/read microsoft.directory/users/allProperties/read microsoft.office365.copilot/allEntities/allProperties/allTasks microsoft.office365.messageCenter/messages/read microsoft.office365.network/performance/allProperties/read microsoft.office365.search/content/manage microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.usageReports/allEntities/allProperties/read microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

AI Reader

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Read all aspects of Microsoft 365 Copilot and AI-related enterprise services in Microsoft 365.
Identifier	1fe13547-53f6-408d-ac04-7f8eed167b38
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	1fe13547-53f6-408d-ac04-7f8eed167b38
Version	1

Inheritance

Inherited Roles	

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.directory/administrativeUnits/members/read microsoft.directory/administrativeUnits/standard/read microsoft.directory/agentIdentities/allProperties/read microsoft.directory/agentIdentityBlueprintPrincipals/allProperties/read microsoft.directory/agentIdentityBlueprints/allProperties/read microsoft.directory/agentUsers/lifeCycleInfo/read microsoft.directory/applicationPolicies/standard/read microsoft.directory/applications/owners/read microsoft.directory/applications/policies/read microsoft.directory/applications/standard/read microsoft.directory/contacts/memberOf/read microsoft.directory/contacts/standard/read microsoft.directory/contracts/standard/read microsoft.directory/domains/standard/read microsoft.directory/entitlementManagement/allProperties/read microsoft.directory/groups/appRoleAssignments/read microsoft.directory/groups/memberOf/read microsoft.directory/groups/members/read microsoft.directory/groups/owners/read microsoft.directory/groups/settings/read microsoft.directory/groups/standard/read microsoft.directory/groupSettings/standard/read microsoft.directory/groupSettingTemplates/standard/read microsoft.directory/oAuth2PermissionGrants/standard/read microsoft.directory/organization/standard/read microsoft.directory/organization/trustedCAsForPasswordlessAuth/read microsoft.directory/roleAssignments/standard/read microsoft.directory/roleDefinitions/standard/read microsoft.directory/servicePrincipals/appRoleAssignedTo/read microsoft.directory/servicePrincipals/appRoleAssignments/read microsoft.directory/servicePrincipals/memberOf/read microsoft.directory/servicePrincipals/oAuth2PermissionGrants/read microsoft.directory/servicePrincipals/ownedObjects/read microsoft.directory/servicePrincipals/owners/read microsoft.directory/servicePrincipals/policies/read microsoft.directory/servicePrincipals/standard/read microsoft.directory/subscribedSkus/standard/read microsoft.directory/users/allProperties/read microsoft.office365.copilot/allEntities/allProperties/read microsoft.office365.messageCenter/messages/read microsoft.office365.network/performance/allProperties/read microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Application Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can create and manage all aspects of app registrations and enterprise apps.
Identifier	9b895d92-2cd3-44c7-9d02-a6ac2d5ea5c3
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	9b895d92-2cd3-44c7-9d02-a6ac2d5ea5c3
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.directory/adminConsentRequestPolicy/allProperties/allTasks microsoft.directory/appConsent/appConsentRequests/allProperties/read microsoft.directory/applicationPolicies/basic/update microsoft.directory/applicationPolicies/create microsoft.directory/applicationPolicies/delete microsoft.directory/applicationPolicies/owners/read microsoft.directory/applicationPolicies/owners/update microsoft.directory/applicationPolicies/policyAppliedTo/read microsoft.directory/applicationPolicies/standard/read microsoft.directory/applications/applicationProxy/read microsoft.directory/applications/applicationProxy/update microsoft.directory/applications/applicationProxyAuthentication/update microsoft.directory/applications/applicationProxySslCertificate/update microsoft.directory/applications/applicationProxyUrlSettings/update microsoft.directory/applications/appRoles/update microsoft.directory/applications/audience/update microsoft.directory/applications/authentication/update microsoft.directory/applications/basic/update microsoft.directory/applications/create microsoft.directory/applications/credentials/update microsoft.directory/applications/delete microsoft.directory/applications/disablement/update microsoft.directory/applications/extensionProperties/update microsoft.directory/applications/notes/update microsoft.directory/applications/owners/update microsoft.directory/applications/permissions/update microsoft.directory/applications/policies/update microsoft.directory/applications/synchronization/standard/read microsoft.directory/applications/tag/update microsoft.directory/applications/verification/update microsoft.directory/applicationTemplates/instantiate microsoft.directory/auditLogs/allProperties/read microsoft.directory/connectorGroups/allProperties/read microsoft.directory/connectorGroups/allProperties/update microsoft.directory/connectorGroups/create microsoft.directory/connectorGroups/delete microsoft.directory/connectors/allProperties/read microsoft.directory/connectors/create microsoft.directory/customAuthenticationExtensions/allProperties/allTasks microsoft.directory/deletedItems.applications/delete microsoft.directory/deletedItems.applications/restore microsoft.directory/oAuth2PermissionGrants/allProperties/allTasks microsoft.directory/provisioningLogs/allProperties/read microsoft.directory/servicePrincipals/appRoleAssignedTo/update microsoft.directory/servicePrincipals/audience/update microsoft.directory/servicePrincipals/authentication/update microsoft.directory/servicePrincipals/basic/update microsoft.directory/servicePrincipals/create microsoft.directory/servicePrincipals/credentials/update microsoft.directory/servicePrincipals/delete microsoft.directory/servicePrincipals/disable microsoft.directory/servicePrincipals/enable

	microsoft.directory/servicePrincipals/getPasswordSingleSignOnCredentials microsoft.directory/servicePrincipals/managePasswordSingleSignOnCredentials microsoft.directory/servicePrincipals/managePermissionGrantsForAll.microsoft-application-admin microsoft.directory/servicePrincipals/notes/update microsoft.directory/servicePrincipals/owners/update microsoft.directory/servicePrincipals/permissions/update microsoft.directory/servicePrincipals/policies/update microsoft.directory/servicePrincipals/synchronization.cloudTenantToExternalSystem/credentials/manage microsoft.directory/servicePrincipals/synchronization.cloudTenantToExternalSystem/jobs/manage microsoft.directory/servicePrincipals/synchronization.cloudTenantToExternalSystem/schema/manage microsoft.directory/servicePrincipals/synchronization/standard/read microsoft.directory/servicePrincipals/synchronizationCredentials/manage microsoft.directory/servicePrincipals/synchronizationJobs/manage microsoft.directory/servicePrincipals/synchronizationSchema/manage microsoft.directory/servicePrincipals/tag/update microsoft.directory/signInReports/allProperties/read microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Application Developer

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can create application registrations independent of the 'Users can register applications' setting.
Identifier	cf1c38e5-3621-4004-a7cb-879624dced7c
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	cf1c38e5-3621-4004-a7cb-879624dced7c
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/applications/createAsOwner microsoft.directory/oAuth2PermissionGrants/createAsOwner microsoft.directory/servicePrincipals/createAsOwner

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Attack Payload Author

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can create attack payloads that an administrator can initiate later.
Identifier	9c6df0f2-1e7c-4dc3-b195-66dfbd24aa8f
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	9c6df0f2-1e7c-4dc3-b195-66dfbd24aa8f
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.office365.protectionCenter/attackSimulator/payload/allProperties/allTasks microsoft.office365.protectionCenter/attackSimulator/reports/allProperties/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Attack Simulation Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can create and manage all aspects of attack simulation campaigns.
Identifier	c430b396-e693-46cc-96f3-db01bf8bb62a
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	c430b396-e693-46cc-96f3-db01bf8bb62a
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.office365.protectionCenter/attackSimulator/payload/allProperties/allTasks microsoft.office365.protectionCenter/attackSimulator/reports/allProperties/read microsoft.office365.protectionCenter/attackSimulator/simulation/allProperties/allTasks

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Attribute Assignment Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Assign custom security attribute keys and values to supported Microsoft Entra objects.
Identifier	58a13ea3-c632-46ae-9ee0-9c0d43cd7f3d
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	58a13ea3-c632-46ae-9ee0-9c0d43cd7f3d
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/attributeSets/allProperties/read microsoft.directory/azureManagedIdentities/customSecurityAttributes/read microsoft.directory/azureManagedIdentities/customSecurityAttributes/update microsoft.directory/customSecurityAttributeDefinitions/allProperties/read microsoft.directory/devices/customSecurityAttributes/read microsoft.directory/devices/customSecurityAttributes/update microsoft.directory/servicePrincipals/customSecurityAttributes/read microsoft.directory/servicePrincipals/customSecurityAttributes/update microsoft.directory/users/customSecurityAttributes/read microsoft.directory/users/customSecurityAttributes/update

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Attribute Assignment Reader

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Read custom security attribute keys and values for supported Microsoft Entra objects.
Identifier	ffd52fa5-98dc-465c-991d-fc073eb59f8f
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	ffd52fa5-98dc-465c-991d-fc073eb59f8f
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/attributeSets/allProperties/read microsoft.directory/azureManagedIdentities/customSecurityAttributes/read microsoft.directory/customSecurityAttributeDefinitions/allProperties/read microsoft.directory/devices/customSecurityAttributes/read microsoft.directory/servicePrincipals/customSecurityAttributes/read microsoft.directory/users/customSecurityAttributes/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Attribute Definition Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Define and manage the definition of custom security attributes.
Identifier	8424c6f0-a189-499e-bbd0-26c1753c96d4
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	8424c6f0-a189-499e-bbd0-26c1753c96d4
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/attributeSets/allProperties/allTasks microsoft.directory/customSecurityAttributeDefinitions/allProperties/allTasks

Excluded Permissions

Excluded Permissions	

1 Role Assignments

Display Name	Principal Type	Scope	Membership	State	Start Time	End Time
XIA	User	Directory	Direct	Assigned	[Not Configured]	Permanent

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Attribute Definition Reader

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Read the definition of custom security attributes.
Identifier	1d336d2c-4ae8-42ef-9711-b3604ce3fc2c
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	1d336d2c-4ae8-42ef-9711-b3604ce3fc2c
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/attributeSets/allProperties/read microsoft.directory/customSecurityAttributeDefinitions/allProperties/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Attribute Log Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Read audit logs and configure diagnostic settings for events related to custom security attributes.
Identifier	5b784334-f94b-471a-a387-e7219fc49ca2
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	5b784334-f94b-471a-a387-e7219fc49ca2
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.customSecurityAttributeDiagnosticSettings/allEntities/allProperties/allTasks microsoft.directory/customSecurityAttributeAuditLogs/allProperties/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Attribute Log Reader

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Read audit logs related to custom security attributes.
Identifier	9c99539d-8186-4804-835f-fd51ef9e2dcd
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	9c99539d-8186-4804-835f-fd51ef9e2dcd
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/customSecurityAttributeAuditLogs/allProperties/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Attribute Provisioning Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Read and edit the provisioning configuration of all active custom security attributes for an application.
Identifier	ecb2c6bf-0ab6-418e-bd87-7986f8d63bbe
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	ecb2c6bf-0ab6-418e-bd87-7986f8d63bbe
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/servicePrincipals/synchronization.customSecurityAttributes/schema/read microsoft.directory/servicePrincipals/synchronization.customSecurityAttributes/schema/update

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Attribute Provisioning Reader

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Read the provisioning configuration of all active custom security attributes for an application.
Identifier	422218e4-db15-4ef9-bbe0-8afb41546d79
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	422218e4-db15-4ef9-bbe0-8afb41546d79
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/servicePrincipals/synchronization.customSecurityAttributes/schema/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Authentication Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can access to view, set and reset authentication method information for any non-admin user.
Identifier	c4e39bd9-1100-46d3-8c65-fb160da0071f
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	c4e39bd9-1100-46d3-8c65-fb160da0071f
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.directory/deletedItems.users/restore microsoft.directory/users/authenticationMethods/basic/update microsoft.directory/users/authenticationMethods/create microsoft.directory/users/authenticationMethods/delete microsoft.directory/users/authenticationMethods/standard/restrictedRead microsoft.directory/users/basic/update microsoft.directory/users/delete microsoft.directory/users/disable microsoft.directory/users/enable microsoft.directory/users/invalidateAllRefreshTokens microsoft.directory/users/manager/update microsoft.directory/users/password/update microsoft.directory/users/restore microsoft.directory/users/userPrincipalName/update microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Authentication Extensibility Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Customize sign in and sign up experiences for users by creating and managing custom authentication extensions.
Identifier	25a516ed-2fa0-40ea-a2d0-12923a21473a
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	25a516ed-2fa0-40ea-a2d0-12923a21473a
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/customAuthenticationExtensions/allProperties/allTasks

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Authentication Extensibility Password Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Trigger a password submit event for custom authentication.
Identifier	0b00bede-4072-4d22-b441-e7df02a1ef63
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	0b00bede-4072-4d22-b441-e7df02a1ef63
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/onPasswordSubmitCustomAuthenticationExtension/allProperties/allTasks

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Authentication Policy Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can create and manage the authentication methods policy, tenant-wide MFA settings, password protection policy, and verifiable credentials.
Identifier	0526716b-113d-4c15-b2c8-68e3c22b9f80
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	0526716b-113d-4c15-b2c8-68e3c22b9f80
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.supportTickets/allEntities/allTasks microsoft.directory/organization/strongAuthentication/allTasks microsoft.directory/userCredentialPolicies/basic/update microsoft.directory/userCredentialPolicies/create microsoft.directory/userCredentialPolicies/delete microsoft.directory/userCredentialPolicies/owners/read microsoft.directory/userCredentialPolicies/owners/update microsoft.directory/userCredentialPolicies/policyAppliedTo/read microsoft.directory/userCredentialPolicies/standard/read microsoft.directory/userCredentialPolicies/tenantDefault/update microsoft.directory/verifiableCredentials/configuration/allProperties/read microsoft.directory/verifiableCredentials/configuration/allProperties/update microsoft.directory/verifiableCredentials/configuration/contracts/allProperties/read microsoft.directory/verifiableCredentials/configuration/contracts/allProperties/update microsoft.directory/verifiableCredentials/configuration/contracts/cards/allProperties/read microsoft.directory/verifiableCredentials/configuration/contracts/cards/revoke microsoft.directory/verifiableCredentials/configuration/contracts/create microsoft.directory/verifiableCredentials/configuration/create microsoft.directory/verifiableCredentials/configuration/delete

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Azure AD Joined Device Local Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Users assigned to this role are added to the local administrators group on Microsoft Entra joined devices.
Identifier	9f06204d-73c1-4d4c-880a-6edb90606fd8
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	9f06204d-73c1-4d4c-880a-6edb90606fd8
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/groupSettings/standard/read microsoft.directory/groupSettingTemplates/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Azure DevOps Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can manage Azure DevOps organization policy and settings.
Identifier	e3973bdf-4987-49ae-837a-ba8e231c7286
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	e3973bdf-4987-49ae-837a-ba8e231c7286
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.devOps/allEntities/allTasks

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Azure Information Protection Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can manage all aspects of the Azure Information Protection product.
Identifier	7495fdc4-34c4-4d15-a289-98788ce399fd
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	7495fdc4-34c4-4d15-a289-98788ce399fd
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.informationProtection/allEntities/allTasks microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.directory/authorizationPolicy/standard/read microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	Azure MFA
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

B2C IEF Keyset Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can manage secrets for federation and encryption in the Identity Experience Framework (IEF).
Identifier	aaf43236-0c0d-4d5f-883a-6955382ac081
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	aaf43236-0c0d-4d5f-883a-6955382ac081
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/b2cTrustFrameworkKeySet/allProperties/allTasks

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

B2C IEF Policy Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can create and manage trust framework policies in the Identity Experience Framework (IEF).
Identifier	3edaf663-341e-4475-9f94-5c398ef6c070
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	3edaf663-341e-4475-9f94-5c398ef6c070
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/b2cTrustFrameworkPolicy/allProperties/allTasks

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Billing Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can perform common billing related tasks like updating payment information.
Identifier	b0f54661-2d74-4c50-afa3-1ec803f12efe
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	b0f54661-2d74-4c50-afa3-1ec803f12efe
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.commerce.billing/allEntities/allProperties/allTasks microsoft.directory/organization/basic/update microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	Azure MFA
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Cloud App Security Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can manage all aspects of the Cloud App Security product.
Identifier	892c5842-a9a6-463a-8041-72aa08ca3cf6
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	892c5842-a9a6-463a-8041-72aa08ca3cf6
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/cloudAppSecurity/allProperties/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Cloud Application Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can create and manage all aspects of app registrations and enterprise apps except App Proxy.
Identifier	158c047a-c907-4556-b7ef-446551a6b5f7
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	158c047a-c907-4556-b7ef-446551a6b5f7
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.directory/adminConsentRequestPolicy/allProperties/allTasks microsoft.directory/appConsent/appConsentRequests/allProperties/read microsoft.directory/applicationPolicies/basic/update microsoft.directory/applicationPolicies/create microsoft.directory/applicationPolicies/delete microsoft.directory/applicationPolicies/owners/read microsoft.directory/applicationPolicies/owners/update microsoft.directory/applicationPolicies/policyAppliedTo/read microsoft.directory/applicationPolicies/standard/read microsoft.directory/applications/appRoles/update microsoft.directory/applications/audience/update microsoft.directory/applications/authentication/update microsoft.directory/applications/basic/update microsoft.directory/applications/create microsoft.directory/applications/credentials/update microsoft.directory/applications/delete microsoft.directory/applications/disablement/update microsoft.directory/applications/extensionProperties/update microsoft.directory/applications/notes/update microsoft.directory/applications/owners/update microsoft.directory/applications/permissions/update microsoft.directory/applications/policies/update microsoft.directory/applications/synchronization/standard/read microsoft.directory/applications/tag/update microsoft.directory/applications/verification/update microsoft.directory/applicationTemplates/instantiate microsoft.directory/auditLogs/allProperties/read microsoft.directory/deletedItems.applications/delete microsoft.directory/deletedItems.applications/restore microsoft.directory/oAuth2PermissionGrants/allProperties/allTasks microsoft.directory/provisioningLogs/allProperties/read microsoft.directory/servicePrincipals/appRoleAssignedTo/update microsoft.directory/servicePrincipals/audience/update microsoft.directory/servicePrincipals/authentication/update microsoft.directory/servicePrincipals/basic/update microsoft.directory/servicePrincipals/create microsoft.directory/servicePrincipals/credentials/update microsoft.directory/servicePrincipals/delete microsoft.directory/servicePrincipals/disable microsoft.directory/servicePrincipals/enable microsoft.directory/servicePrincipals/getPasswordSingleSignOnCredentials microsoft.directory/servicePrincipals/managePasswordSingleSignOnCredentials microsoft.directory/servicePrincipals/managePermissionGrantsForAll.microsoft-application-admin microsoft.directory/servicePrincipals/notes/update microsoft.directory/servicePrincipals/owners/update microsoft.directory/servicePrincipals/permissions/update microsoft.directory/servicePrincipals/policies/update microsoft.directory/servicePrincipals/synchronization.cloudTenantToExternalSystem/credentials/manage microsoft.directory/servicePrincipals/synchronization.cloudTenantToExternalSystem/jobs/manage microsoft.directory/servicePrincipals/synchronization.cloudTenantToExternalSystem/schema/manage microsoft.directory/servicePrincipals/synchronization/standard/read

	microsoft.directory/servicePrincipals/synchronizationCredentials/manage microsoft.directory/servicePrincipals/synchronizationJobs/manage microsoft.directory/servicePrincipals/synchronizationSchema/manage microsoft.directory/servicePrincipals/tag/update microsoft.directory/signInReports/allProperties/read microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

1 Role Assignments

Display Name	Principal Type	Scope	Membership	State	Start Time	End Time
XIA	User	Microsoft Graph Command Line Tools (Service Principal)	Direct	Assigned	[Not Configured]	Permanent

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	Azure MFA
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Cloud Device Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Limited access to manage devices in Microsoft Entra ID.
Identifier	7698a772-787b-4ac8-901f-60d6b08affd2
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	7698a772-787b-4ac8-901f-60d6b08affd2
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.directory/auditLogs/allProperties/read microsoft.directory/authorizationPolicy/standard/read microsoft.directory/bitlockerKeys/key/read microsoft.directory/deletedItems.devices/delete microsoft.directory/deletedItems.devices/restore microsoft.directory/deviceLocalCredentials/password/read microsoft.directory/deviceManagementPolicies/basic/update microsoft.directory/deviceManagementPolicies/standard/read microsoft.directory/deviceRegistrationPolicy/basic/update microsoft.directory/deviceRegistrationPolicy/standard/read microsoft.directory/devices/delete microsoft.directory/devices/disable microsoft.directory/devices/enable microsoft.directory/devices/permissions/update microsoft.directory/deviceTemplates/owners/read microsoft.directory/deviceTemplates/owners/update microsoft.directory/signInReports/allProperties/read microsoft.office365.serviceHealth/allEntities/allTasks

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Compliance Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can read and manage compliance configuration and reports in Microsoft Entra ID and Microsoft 365.
Identifier	17315797-102d-40b4-93e0-432062caca18
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	17315797-102d-40b4-93e0-432062caca18
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.directory/entitlementManagement/allProperties/read microsoft.office365.complianceManager/allEntities/allTasks microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	Azure MFA
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Compliance Data Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Creates and manages compliance content.
Identifier	e6d1a23a-da11-4be4-9570-befc86d067a7
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	e6d1a23a-da11-4be4-9570-befc86d067a7
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.informationProtection/allEntities/allTasks microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.directory/authorizationPolicy/standard/read microsoft.directory/cloudAppSecurity/allProperties/allTasks microsoft.office365.complianceManager/allEntities/allTasks microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Conditional Access Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can manage Conditional Access capabilities.
Identifier	b1be1c3e-b65d-4f19-8427-f6fa0d97feb9
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	b1be1c3e-b65d-4f19-8427-f6fa0d97feb9
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/conditionalAccessPolicies/basic/update microsoft.directory/conditionalAccessPolicies/create microsoft.directory/conditionalAccessPolicies/delete microsoft.directory/conditionalAccessPolicies/owners/read microsoft.directory/conditionalAccessPolicies/owners/update microsoft.directory/conditionalAccessPolicies/policyAppliedTo/read microsoft.directory/conditionalAccessPolicies/standard/read microsoft.directory/conditionalAccessPolicies/tenantDefault/update microsoft.directory/namedLocations/basic/update microsoft.directory/namedLocations/create microsoft.directory/namedLocations/delete microsoft.directory/namedLocations/standard/read microsoft.directory/resourceNamespaces/resourceActions/authenticationContext/update

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	Azure MFA
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Customer Delegated Admin Relationship Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Manage all aspects of granular delegated admin privileges (GDAP) relationships in a customer tenant.
Identifier	fc8ad4e2-40e4-4724-8317-bcda7503ecbf
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	fc8ad4e2-40e4-4724-8317-bcda7503ecbf
Version	1

Inheritance

Inherited Roles	

Allowed Permissions

Allowed Permissions	microsoft.commerce.tenantRelationships/customerDelegatedAdminPrivileges/allProperties/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Customer LockBox Access Approver

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can approve Microsoft support requests to access customer organizational data.
Identifier	5c4f9dcd-47dc-4cf7-8c9a-9e4207cbfc91
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	5c4f9dcd-47dc-4cf7-8c9a-9e4207cbfc91
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.office365.lockbox/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	Azure MFA
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Desktop Analytics Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can access and manage Desktop management tools and services.
Identifier	38a96431-2bdf-4b4c-8b6e-5d3d8abac1a4
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	38a96431-2bdf-4b4c-8b6e-5d3d8abac1a4
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.directory/authorizationPolicy/standard/read microsoft.office365.desktopAnalytics/allEntities/allTasks

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Device Join

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Deprecated - Do Not Use.
Identifier	9c094953-4995-41c8-84c8-3ebb9b32c93f
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	9c094953-4995-41c8-84c8-3ebb9b32c93f
Version	1

Inheritance

Inherited Roles	

Allowed Permissions

Allowed Permissions	

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Device Managers

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Deprecated - Do Not Use.
Identifier	2b499bcd-da44-4968-8aec-78e1674fa64d
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	2b499bcd-da44-4968-8aec-78e1674fa64d
Version	1

Inheritance

Inherited Roles	

Allowed Permissions

Allowed Permissions	microsoft.directory/devices/basic/update microsoft.directory/devices/extensionAttributeSet1/update microsoft.directory/devices/extensionAttributeSet2/update microsoft.directory/devices/extensionAttributeSet3/update microsoft.directory/devices/memberOf/read microsoft.directory/devices/registeredOwners/read microsoft.directory/devices/registeredOwners/update microsoft.directory/devices/registeredUsers/read microsoft.directory/devices/registeredUsers/update microsoft.directory/devices/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Device Users

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Deprecated - Do Not Use.
Identifier	d405c6df-0af8-4e3b-95e4-4d06e542189e
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	d405c6df-0af8-4e3b-95e4-4d06e542189e
Version	1

Inheritance

Inherited Roles	

Allowed Permissions

Allowed Permissions	

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Directory Readers

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can read basic directory information. Commonly used to grant directory read access to applications and guests.
Identifier	88d8e3e3-8f55-4a1e-953a-9b9898b8876b
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	88d8e3e3-8f55-4a1e-953a-9b9898b8876b
Version	1

Inheritance

Inherited Roles	

Allowed Permissions

Allowed Permissions	microsoft.directory/administrativeUnits/members/read microsoft.directory/administrativeUnits/standard/read microsoft.directory/applicationPolicies/standard/read microsoft.directory/applications/owners/read microsoft.directory/applications/policies/read microsoft.directory/applications/standard/read microsoft.directory/contacts/memberOf/read microsoft.directory/contacts/standard/read microsoft.directory/contracts/standard/read microsoft.directory/devices/memberOf/read microsoft.directory/devices/registeredOwners/read microsoft.directory/devices/registeredUsers/read microsoft.directory/devices/standard/read microsoft.directory/directoryRoles/eligibleMembers/read microsoft.directory/directoryRoles/members/read microsoft.directory/directoryRoles/standard/read microsoft.directory/domains/standard/read microsoft.directory/groups/appRoleAssignments/read microsoft.directory/groups/memberOf/read microsoft.directory/groups/members/read microsoft.directory/groups/owners/read microsoft.directory/groups/settings/read microsoft.directory/groups/standard/read microsoft.directory/groupSettings/standard/read microsoft.directory/groupSettingTemplates/standard/read microsoft.directory/oAuth2PermissionGrants/standard/read microsoft.directory/organization/standard/read microsoft.directory/organization/trustedCAsForPasswordlessAuth/read microsoft.directory/roleAssignments/standard/read microsoft.directory/roleDefinitions/standard/read microsoft.directory/servicePrincipals/appRoleAssignedTo/read microsoft.directory/servicePrincipals/appRoleAssignments/read microsoft.directory/servicePrincipals/memberOf/read microsoft.directory/servicePrincipals/oAuth2PermissionGrants/read microsoft.directory/servicePrincipals/ownedObjects/read microsoft.directory/servicePrincipals/owners/read microsoft.directory/servicePrincipals/policies/read microsoft.directory/servicePrincipals/standard/read microsoft.directory/subscribedSkus/standard/read microsoft.directory/users/appRoleAssignments/read microsoft.directory/users/deviceForResourceAccount/read microsoft.directory/users/directReports/read microsoft.directory/users/invitedBy/read microsoft.directory/users/licenseDetails/read microsoft.directory/users/manager/read microsoft.directory/users/memberOf/read microsoft.directory/users/oAuth2PermissionGrants/read microsoft.directory/users/ownedDevices/read microsoft.directory/users/ownedObjects/read microsoft.directory/users/photo/read microsoft.directory/users/registeredDevices/read microsoft.directory/users/scopedRoleMemberOf/read microsoft.directory/users/sponsorOf/read microsoft.directory/users/sponsors/read

	microsoft.directory/users/standard/read

Excluded Permissions

Excluded Permissions	

1 Role Assignments

Display Name	Principal Type	Scope	Membership	State	Start Time	End Time
Microsoft.Azure.SyncFabric	Service Principal	Directory	Direct	Assigned	[Not Configured]	Permanent

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Directory Synchronization Accounts

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Only used by Microsoft Entra Connect service.
Identifier	d29b2b05-8046-44ba-8758-1e26182fcf32
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	d29b2b05-8046-44ba-8758-1e26182fcf32
Version	1

Inheritance

Inherited Roles	

Allowed Permissions

Allowed Permissions	microsoft.directory/onPremisesSynchronization/standard/read

Excluded Permissions

Excluded Permissions	

1 Role Assignments

Display Name	Principal Type	Scope	Membership	State	Start Time	End Time
On-Premises Directory Synchronization Service Account	User	Directory	Direct	Assigned	[Not Configured]	Permanent

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Directory Writers

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can read and write basic directory information. For granting access to applications, not intended for users.
Identifier	9360feb5-f418-4baa-8175-e2a00bac4301
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	9360feb5-f418-4baa-8175-e2a00bac4301
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/applications/extensionProperties/update microsoft.directory/contacts/create microsoft.directory/groups/assignedLabels/update microsoft.directory/groups/assignLicense microsoft.directory/groups/basic/update microsoft.directory/groups/classification/update microsoft.directory/groups/create microsoft.directory/groups/dynamicMembershipRule/update microsoft.directory/groups/groupType/update microsoft.directory/groups/members/update microsoft.directory/groups/onPremWriteBack/update microsoft.directory/groups/owners/update microsoft.directory/groups/reprocessLicenseAssignment microsoft.directory/groups/settings/update microsoft.directory/groups/visibility/update microsoft.directory/groupSettings/basic/update microsoft.directory/groupSettings/create microsoft.directory/groupSettings/delete microsoft.directory/oAuth2PermissionGrants/basic/update microsoft.directory/oAuth2PermissionGrants/create microsoft.directory/servicePrincipals/appRoleAssignedTo/update microsoft.directory/servicePrincipals/synchronization.cloudTenantToCloudTenant/credentials/manage microsoft.directory/servicePrincipals/synchronization.cloudTenantToCloudTenant/jobs/manage microsoft.directory/servicePrincipals/synchronization.cloudTenantToCloudTenant/schema/manage microsoft.directory/servicePrincipals/synchronization.cloudTenantToExternalSystem/credentials/manage microsoft.directory/servicePrincipals/synchronization.cloudTenantToExternalSystem/jobs/manage microsoft.directory/servicePrincipals/synchronization.cloudTenantToExternalSystem/schema/manage microsoft.directory/servicePrincipals/synchronizationCredentials/manage microsoft.directory/servicePrincipals/synchronizationJobs/manage microsoft.directory/servicePrincipals/synchronizationSchema/manage microsoft.directory/users/assignLicense microsoft.directory/users/basic/update microsoft.directory/users/create microsoft.directory/users/disable microsoft.directory/users/enable microsoft.directory/users/invalidateAllRefreshTokens microsoft.directory/users/inviteGuest microsoft.directory/users/manager/update microsoft.directory/users/photo/update microsoft.directory/users/reprocessLicenseAssignment microsoft.directory/users/sponsors/update microsoft.directory/users/userPrincipalName/update

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	Azure MFA
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Domain Name Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can manage domain names in cloud and on-premises.
Identifier	8329153b-31d0-4727-b945-745eb3bc5f31
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	8329153b-31d0-4727-b945-745eb3bc5f31
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/domains/allProperties/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Dragon Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Manage all aspects of the Microsoft Dragon admin center.
Identifier	e93e3737-fa85-474a-aee4-7d3fb86510f3
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	e93e3737-fa85-474a-aee4-7d3fb86510f3
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.healthPlatform/allEntities/allProperties/allTasks microsoft.office365.network/performance/allProperties/read microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.usageReports/allEntities/allProperties/read microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Dynamics 365 Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can manage all aspects of the Dynamics 365 product.
Identifier	44367163-eba1-44c3-98af-f5787879f96a
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	44367163-eba1-44c3-98af-f5787879f96a
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.dynamics365/allEntities/allTasks microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	Azure MFA
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Dynamics 365 Business Central Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Access and perform all administrative tasks on Dynamics 365 Business Central environments.
Identifier	963797fb-eb3b-4cde-8ce3-5878b3f32a3f
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	963797fb-eb3b-4cde-8ce3-5878b3f32a3f
Version	1

Inheritance

Inherited Roles	

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.directory/domains/standard/read microsoft.directory/organization/standard/read microsoft.directory/subscribedSkus/standard/read microsoft.directory/users/standard/read microsoft.dynamics365.businessCentral/allEntities/allProperties/allTasks microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Edge Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Manage all aspects of Microsoft Edge.
Identifier	3f1acade-1e04-4fbc-9b69-f0302cd84aef
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	3f1acade-1e04-4fbc-9b69-f0302cd84aef
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.edge/allEntities/allProperties/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Entra Backup Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Manage all aspects of Microsoft Entra Backup, such as create recovery jobs and manage backup snapshots.
Identifier	b6a27b2b-f905-4b2e-81b5-0d90e0ef1fdb
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	b6a27b2b-f905-4b2e-81b5-0d90e0ef1fdb
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/backup/preview/cancel microsoft.directory/backup/preview/create microsoft.directory/backup/recovery/cancel microsoft.directory/backup/recovery/create microsoft.directory/backup/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Entra Backup Reader

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Read all aspects of Microsoft Entra Backup, such as list all preview jobs, recovery jobs, backup snapshots, and create preview jobs.
Identifier	f42252d9-5400-4d7b-b9ef-cc582dbb8577
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	f42252d9-5400-4d7b-b9ef-cc582dbb8577
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/backup/preview/cancel microsoft.directory/backup/preview/create microsoft.directory/backup/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Entra Customer Lockbox Approver

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can approve customer lockbox requests for accessing customer data in Entra ID.
Identifier	d35481f7-cda1-4fa2-8344-5a21f7f3724d
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	d35481f7-cda1-4fa2-8344-5a21f7f3724d
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/lockbox/requests/update

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Exchange Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can manage all aspects of the Exchange product.
Identifier	29232cdf-9323-42fd-ade2-1d097af3e4de
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	29232cdf-9323-42fd-ade2-1d097af3e4de
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.backup/exchangeProtectionPolicies/allProperties/allTasks microsoft.backup/exchangeRestoreSessions/allProperties/allTasks microsoft.backup/restorePoints/userMailboxes/allProperties/allTasks microsoft.backup/userMailboxProtectionUnits/allProperties/allTasks microsoft.backup/userMailboxRestoreArtifacts/allProperties/allTasks microsoft.directory/contacts/allProperties/read microsoft.directory/contacts/memberOf/read microsoft.directory/contacts/standard/read microsoft.directory/groups.unified/assignedLabels/update microsoft.directory/groups.unified/basic/update microsoft.directory/groups.unified/create microsoft.directory/groups.unified/delete microsoft.directory/groups.unified/members/update microsoft.directory/groups.unified/owners/update microsoft.directory/groups.unified/restore microsoft.directory/groups/hiddenMembers/read microsoft.directory/onPremisesSynchronization/standard/read microsoft.office365.exchange/allEntities/basic/allTasks microsoft.office365.network/performance/allProperties/read microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.usageReports/allEntities/allProperties/read microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	Azure MFA
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Exchange Backup Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Back up and restore content (including granular restore) for Exchange in Microsoft 365 Backup
Identifier	49eb8f75-97e9-4e37-9b2b-6c3ebfcffa31
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	49eb8f75-97e9-4e37-9b2b-6c3ebfcffa31
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.backup/exchangeProtectionPolicies/allProperties/allTasks microsoft.backup/exchangeRestoreSessions/allProperties/allTasks microsoft.backup/restorePoints/userMailboxes/allProperties/allTasks microsoft.backup/userMailboxProtectionUnits/allProperties/allTasks microsoft.backup/userMailboxRestoreArtifacts/allProperties/allTasks microsoft.office365.network/performance/allProperties/read microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.usageReports/allEntities/allProperties/read microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Exchange Recipient Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can create or update Exchange Online recipients within the Exchange Online organization.
Identifier	31392ffb-586c-42d1-9346-e59415a2cc4e
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	31392ffb-586c-42d1-9346-e59415a2cc4e
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.office365.exchange/migration/allProperties/allTasks microsoft.office365.exchange/recipients/allProperties/allTasks

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Extended Directory User Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Manage all aspects of external user profiles in the extended directory for Teams.
Identifier	dd13091a-6207-4fc0-82ba-3641e056ab95
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	dd13091a-6207-4fc0-82ba-3641e056ab95
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/externalUserProfiles/basic/update microsoft.directory/externalUserProfiles/delete microsoft.directory/externalUserProfiles/standard/read microsoft.directory/pendingExternalUserProfiles/basic/update microsoft.directory/pendingExternalUserProfiles/create microsoft.directory/pendingExternalUserProfiles/delete microsoft.directory/pendingExternalUserProfiles/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

External ID User Flow Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can create and manage all aspects of user flows.
Identifier	6e591065-9bad-43ed-90f3-e9424366d2f0
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	6e591065-9bad-43ed-90f3-e9424366d2f0
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/b2cUserFlow/allProperties/allTasks

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

External ID User Flow Attribute Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can create and manage the attribute schema available to all user flows.
Identifier	0f971eea-41eb-4569-a71e-57bb8a3eff1e
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	0f971eea-41eb-4569-a71e-57bb8a3eff1e
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/b2cUserAttribute/allProperties/allTasks

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

External Identity Provider Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can configure identity providers for use in direct federation.
Identifier	be2f45a1-457d-42af-a067-6ec1fa63bc45
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	be2f45a1-457d-42af-a067-6ec1fa63bc45
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/domains/federation/update microsoft.directory/identityProviders/allProperties/allTasks

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Fabric Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Manages all aspects of Microsoft Fabric.
Identifier	a9ea8996-122f-4c74-9520-8edcd192826c
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	a9ea8996-122f-4c74-9520-8edcd192826c
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read microsoft.powerApps.powerBI/allEntities/allTasks

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	Azure MFA
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Global Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can manage all aspects of Microsoft Entra ID and Microsoft services that use Microsoft Entra identities.
Identifier	62e90394-69f5-4237-9190-012177145e10
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	62e90394-69f5-4237-9190-012177145e10
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.agentRegistry/allEntities/allProperties/allTasks microsoft.azure.advancedThreatProtection/allEntities/allTasks microsoft.azure.informationProtection/allEntities/allTasks microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.backup/allEntities/allProperties/allTasks microsoft.cloudPC/allEntities/allProperties/allTasks microsoft.commerce.billing/allEntities/allProperties/allTasks microsoft.commerce.billing/purchases/standard/read microsoft.commerce.tenantRelationships/customerDelegatedAdminPrivileges/allProperties/allTasks microsoft.directory/accessReviews/allProperties/allTasks microsoft.directory/accessReviews/definitions/allProperties/allTasks microsoft.directory/adminConsentRequestPolicy/allProperties/allTasks microsoft.directory/administrativeUnits/allProperties/allTasks microsoft.directory/agentIdentities/allProperties/read microsoft.directory/agentIdentities/appRoleAssignedTo/update microsoft.directory/agentIdentities/authentication/update microsoft.directory/agentIdentities/basic/update microsoft.directory/agentIdentities/create microsoft.directory/agentIdentities/delete microsoft.directory/agentIdentities/disable microsoft.directory/agentIdentities/enable microsoft.directory/agentIdentities/owners/update microsoft.directory/agentIdentities/tag/update microsoft.directory/agentIdentityBlueprintPrincipals/allProperties/read microsoft.directory/agentIdentityBlueprintPrincipals/appRoleAssignedTo/update microsoft.directory/agentIdentityBlueprintPrincipals/authentication/update microsoft.directory/agentIdentityBlueprintPrincipals/basic/update microsoft.directory/agentIdentityBlueprintPrincipals/create microsoft.directory/agentIdentityBlueprintPrincipals/delete microsoft.directory/agentIdentityBlueprintPrincipals/disable microsoft.directory/agentIdentityBlueprintPrincipals/enable microsoft.directory/agentIdentityBlueprintPrincipals/owners/update microsoft.directory/agentIdentityBlueprintPrincipals/tag/update microsoft.directory/agentIdentityBlueprints/allProperties/read microsoft.directory/agentIdentityBlueprints/allProperties/update microsoft.directory/agentIdentityBlueprints/appRoles/update microsoft.directory/agentIdentityBlueprints/audience/update microsoft.directory/agentIdentityBlueprints/authentication/update microsoft.directory/agentIdentityBlueprints/basic/update microsoft.directory/agentIdentityBlueprints/create microsoft.directory/agentIdentityBlueprints/credentials/update microsoft.directory/agentIdentityBlueprints/delete microsoft.directory/agentIdentityBlueprints/owners/update microsoft.directory/agentIdentityBlueprints/permissions/update microsoft.directory/agentIdentityBlueprints/tag/update microsoft.directory/appConsent/appConsentRequests/allProperties/read microsoft.directory/applications/allProperties/allTasks microsoft.directory/applications/disablement/update microsoft.directory/applications/synchronization/standard/read microsoft.directory/applicationTemplates/instantiate microsoft.directory/auditLogs/allProperties/read microsoft.directory/authorizationPolicy/allProperties/allTasks microsoft.directory/backup/preview/cancel

	microsoft.directory/backup/preview/create microsoft.directory/backup/recovery/cancel microsoft.directory/backup/recovery/create microsoft.directory/backup/standard/read microsoft.directory/bitlockerKeys/key/read microsoft.directory/bulkJobs/basic/update microsoft.directory/bulkJobs/create microsoft.directory/bulkJobs/standard/read microsoft.directory/cloudAppSecurity/allProperties/allTasks microsoft.directory/conditionalAccessPolicies/allProperties/allTasks microsoft.directory/connectorGroups/allProperties/read microsoft.directory/connectorGroups/allProperties/update microsoft.directory/connectorGroups/create microsoft.directory/connectorGroups/delete microsoft.directory/connectors/allProperties/read microsoft.directory/connectors/create microsoft.directory/contacts/allProperties/allTasks microsoft.directory/contracts/allProperties/allTasks microsoft.directory/crossTenantAccessPolicy/allowedCloudEndpoints/update microsoft.directory/crossTenantAccessPolicy/basic/update microsoft.directory/crossTenantAccessPolicy/default/b2bCollaboration/update microsoft.directory/crossTenantAccessPolicy/default/b2bDirectConnect/update microsoft.directory/crossTenantAccessPolicy/default/crossCloudMeetings/update microsoft.directory/crossTenantAccessPolicy/default/standard/read microsoft.directory/crossTenantAccessPolicy/default/tenantRestrictions/update microsoft.directory/crossTenantAccessPolicy/partners/b2bCollaboration/update microsoft.directory/crossTenantAccessPolicy/partners/b2bDirectConnect/update microsoft.directory/crossTenantAccessPolicy/partners/create microsoft.directory/crossTenantAccessPolicy/partners/crossCloudMeetings/update microsoft.directory/crossTenantAccessPolicy/partners/delete microsoft.directory/crossTenantAccessPolicy/partners/identitySynchronization/basic/update microsoft.directory/crossTenantAccessPolicy/partners/identitySynchronization/create microsoft.directory/crossTenantAccessPolicy/partners/identitySynchronization/standard/read microsoft.directory/crossTenantAccessPolicy/partners/standard/read microsoft.directory/crossTenantAccessPolicy/partners/templates/multiTenantOrganizationIdentitySynchronization/basic/update microsoft.directory/crossTenantAccessPolicy/partners/templates/multiTenantOrganizationIdentitySynchronization/resetToDefaultSettings microsoft.directory/crossTenantAccessPolicy/partners/templates/multiTenantOrganizationIdentitySynchronization/standard/read microsoft.directory/crossTenantAccessPolicy/partners/templates/multiTenantOrganizationPartnerConfiguration/basic/update microsoft.directory/crossTenantAccessPolicy/partners/templates/multiTenantOrganizationPartnerConfiguration/resetToDefaultSettings microsoft.directory/crossTenantAccessPolicy/partners/templates/multiTenantOrganizationPartnerConfiguration/standard/read microsoft.directory/crossTenantAccessPolicy/partners/tenantRestrictions/update microsoft.directory/crossTenantAccessPolicy/standard/read microsoft.directory/customAuthenticationExtensions/allProperties/allTasks microsoft.directory/deletedItems/delete microsoft.directory/deletedItems/restore microsoft.directory/deviceLocalCredentials/password/read microsoft.directory/deviceManagementPolicies/basic/update microsoft.directory/deviceManagementPolicies/standard/read microsoft.directory/deviceRegistrationPolicy/basic/update microsoft.directory/deviceRegistrationPolicy/standard/read microsoft.directory/devices/allProperties/allTasks microsoft.directory/devices/permissions/update

	microsoft.directory/deviceTemplates/owners/read microsoft.directory/deviceTemplates/owners/update microsoft.directory/directoryRoles/allProperties/allTasks microsoft.directory/directoryRoleTemplates/allProperties/allTasks microsoft.directory/domains/allProperties/allTasks microsoft.directory/domains/federationConfiguration/basic/update microsoft.directory/domains/federationConfiguration/create microsoft.directory/domains/federationConfiguration/delete microsoft.directory/domains/federationConfiguration/standard/read microsoft.directory/entitlementManagement/allProperties/allTasks microsoft.directory/externalUserProfiles/basic/update microsoft.directory/externalUserProfiles/delete microsoft.directory/externalUserProfiles/standard/read microsoft.directory/groups/allProperties/allTasks microsoft.directory/groupsAssignableToRoles/allProperties/update microsoft.directory/groupsAssignableToRoles/assignLicense microsoft.directory/groupsAssignableToRoles/create microsoft.directory/groupsAssignableToRoles/delete microsoft.directory/groupsAssignableToRoles/reprocessLicenseAssignment microsoft.directory/groupsAssignableToRoles/restore microsoft.directory/groupSettings/allProperties/allTasks microsoft.directory/groupSettingTemplates/allProperties/allTasks microsoft.directory/hybridAuthenticationPolicy/allProperties/allTasks microsoft.directory/identityProtection/allProperties/allTasks microsoft.directory/lifecycleWorkflows/workflows/allProperties/allTasks microsoft.directory/lockbox/requests/update microsoft.directory/loginOrganizationBranding/allProperties/allTasks microsoft.directory/multiTenantOrganization/basic/update microsoft.directory/multiTenantOrganization/create microsoft.directory/multiTenantOrganization/joinRequest/organizationDetails/update microsoft.directory/multiTenantOrganization/joinRequest/standard/read microsoft.directory/multiTenantOrganization/standard/read microsoft.directory/multiTenantOrganization/tenants/create microsoft.directory/multiTenantOrganization/tenants/delete microsoft.directory/multiTenantOrganization/tenants/organizationDetails/read microsoft.directory/multiTenantOrganization/tenants/organizationDetails/update microsoft.directory/multiTenantOrganization/tenants/standard/read microsoft.directory/namedLocations/basic/update microsoft.directory/namedLocations/create microsoft.directory/namedLocations/delete microsoft.directory/namedLocations/standard/read microsoft.directory/oAuth2PermissionGrants/allProperties/allTasks microsoft.directory/onPremisesSynchronization/basic/update microsoft.directory/onPremisesSynchronization/standard/read microsoft.directory/organization/allProperties/allTasks microsoft.directory/passwordHashSync/allProperties/allTasks microsoft.directory/pendingExternalUserProfiles/basic/update microsoft.directory/pendingExternalUserProfiles/create microsoft.directory/pendingExternalUserProfiles/delete microsoft.directory/pendingExternalUserProfiles/standard/read microsoft.directory/permissionGrantPolicies/basic/update microsoft.directory/permissionGrantPolicies/create microsoft.directory/permissionGrantPolicies/delete microsoft.directory/permissionGrantPolicies/standard/read microsoft.directory/policies/allProperties/allTasks microsoft.directory/privilegedIdentityManagement/allProperties/read

	microsoft.directory/provisioningLogs/allProperties/read microsoft.directory/resourceNamespaces/resourceActions/authenticationContext/update microsoft.directory/roleAssignments/allProperties/allTasks microsoft.directory/roleDefinitions/allProperties/allTasks microsoft.directory/scopedRoleMemberships/allProperties/allTasks microsoft.directory/serviceAction/activateService microsoft.directory/serviceAction/disableDirectoryFeature microsoft.directory/serviceAction/enableDirectoryFeature microsoft.directory/serviceAction/getAvailableExtentionProperties microsoft.directory/servicePrincipalCreationPolicies/basic/update microsoft.directory/servicePrincipalCreationPolicies/create microsoft.directory/servicePrincipalCreationPolicies/delete microsoft.directory/servicePrincipalCreationPolicies/standard/read microsoft.directory/servicePrincipals/allProperties/allTasks microsoft.directory/servicePrincipals/managePermissionGrantsForAll.microsoft-company-admin microsoft.directory/servicePrincipals/synchronization.cloudTenantToCloudTenant/credentials/manage microsoft.directory/servicePrincipals/synchronization.cloudTenantToCloudTenant/jobs/manage microsoft.directory/servicePrincipals/synchronization.cloudTenantToCloudTenant/schema/manage microsoft.directory/servicePrincipals/synchronization.cloudTenantToExternalSystem/credentials/manage microsoft.directory/servicePrincipals/synchronization.cloudTenantToExternalSystem/jobs/manage microsoft.directory/servicePrincipals/synchronization.cloudTenantToExternalSystem/schema/manage microsoft.directory/servicePrincipals/synchronization/standard/read microsoft.directory/signInReports/allProperties/read microsoft.directory/subscribedSkus/allProperties/allTasks microsoft.directory/tenantManagement/tenants/create microsoft.directory/users/allProperties/allTasks microsoft.directory/users/authenticationMethods/basic/update microsoft.directory/users/authenticationMethods/create microsoft.directory/users/authenticationMethods/delete microsoft.directory/users/authenticationMethods/standard/read microsoft.directory/users/convertExternalToInternalMemberUser microsoft.directory/verifiableCredentials/configuration/allProperties/read microsoft.directory/verifiableCredentials/configuration/allProperties/update microsoft.directory/verifiableCredentials/configuration/contracts/allProperties/read microsoft.directory/verifiableCredentials/configuration/contracts/allProperties/update microsoft.directory/verifiableCredentials/configuration/contracts/cards/allProperties/read microsoft.directory/verifiableCredentials/configuration/contracts/cards/revoke microsoft.directory/verifiableCredentials/configuration/contracts/create microsoft.directory/verifiableCredentials/configuration/create microsoft.directory/verifiableCredentials/configuration/delete microsoft.dynamics365/allEntities/allTasks microsoft.edge/allEntities/allProperties/allTasks microsoft.flow/allEntities/allTasks microsoft.graph.dataConnect/allEntities/allProperties/allTasks microsoft.hardware.support/shippingAddress/allProperties/allTasks microsoft.hardware.support/shippingStatus/allProperties/read microsoft.hardware.support/warrantyClaims/allProperties/allTasks microsoft.healthPlatform/allEntities/allProperties/allTasks microsoft.insights/allEntities/allProperties/allTasks microsoft.intune/allEntities/allTasks microsoft.microsoft365.organizationalData/allEntities/allProperties/allTasks microsoft.networkAccess/allEntities/allProperties/allTasks microsoft.networkAccess/trafficLogs/standard/read microsoft.office365.complianceManager/allEntities/allTasks microsoft.office365.copilot/allEntities/allProperties/allTasks microsoft.office365.desktopAnalytics/allEntities/allTasks

	microsoft.office365.exchange/allEntities/basic/allTasks microsoft.office365.fileStorageContainers/allEntities/allProperties/allTasks microsoft.office365.knowledge/contentUnderstanding/allProperties/allTasks microsoft.office365.knowledge/contentUnderstanding/analytics/allProperties/read microsoft.office365.knowledge/knowledgeNetwork/allProperties/allTasks microsoft.office365.knowledge/knowledgeNetwork/topicVisibility/allProperties/allTasks microsoft.office365.knowledge/learningSources/allProperties/allTasks microsoft.office365.lockbox/allEntities/allTasks microsoft.office365.messageCenter/messages/read microsoft.office365.messageCenter/securityMessages/read microsoft.office365.migrations/allEntities/allProperties/allTasks microsoft.office365.network/performance/allProperties/read microsoft.office365.organizationalMessages/allEntities/allProperties/allTasks microsoft.office365.protectionCenter/allEntities/allProperties/allTasks microsoft.office365.search/content/manage microsoft.office365.securityComplianceCenter/allEntities/allTasks microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.sharePoint/allEntities/allTasks microsoft.office365.sharePointAdvancedManagement/allEntities/allProperties/allTasks microsoft.office365.skypeForBusiness/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.usageReports/allEntities/allProperties/read microsoft.office365.userCommunication/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read microsoft.office365.yammer/allEntities/allProperties/allTasks microsoft.people/users/photo/read microsoft.people/users/photo/update microsoft.peopleAdmin/organization/allProperties/read microsoft.peopleAdmin/organization/allProperties/update microsoft.permissionsManagement/allEntities/allProperties/allTasks microsoft.powerApps.powerBI/allEntities/allTasks microsoft.powerApps/allEntities/allTasks microsoft.teams/allEntities/allProperties/allTasks microsoft.virtualVisits/allEntities/allProperties/allTasks microsoft.viva.glint/allEntities/allProperties/allTasks microsoft.viva.goals/allEntities/allProperties/allTasks microsoft.viva.pulse/allEntities/allProperties/allTasks microsoft.windows.defenderAdvancedThreatProtection/allEntities/allTasks microsoft.windows.updatesDeployments/allEntities/allProperties/allTasks

Excluded Permissions

Excluded Permissions	

2 Role Assignments

Display Name	Principal Type	Scope	Membership	State	Start Time	End Time
Backup Global Admin	User	Directory	Direct	Assigned	[Not Configured]	Permanent
XIA	User	Directory	Direct	Assigned	[Not Configured]	Permanent

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	Azure MFA
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Global Reader

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can read everything that a Global Administrator can, but not update anything.
Identifier	f2ef992c-3afb-46b9-b7cf-a126ee74c451
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	f2ef992c-3afb-46b9-b7cf-a126ee74c451
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.agentRegistry/allEntities/allProperties/read microsoft.azure.serviceHealth/allEntities/allTasks microsoft.backup/allEntities/allProperties/read microsoft.cloudPC/allEntities/allProperties/read microsoft.commerce.billing/allEntities/allProperties/read microsoft.commerce.billing/purchases/standard/read microsoft.directory/accessReviews/allProperties/read microsoft.directory/accessReviews/definitions/allProperties/read microsoft.directory/adminConsentRequestPolicy/allProperties/read microsoft.directory/administrativeUnits/allProperties/read microsoft.directory/agentIdentities/allProperties/read microsoft.directory/agentIdentityBlueprintPrincipals/allProperties/read microsoft.directory/agentIdentityBlueprints/allProperties/read microsoft.directory/appConsent/appConsentRequests/allProperties/read microsoft.directory/applications/allProperties/read microsoft.directory/applications/synchronization/standard/read microsoft.directory/auditLogs/allProperties/read microsoft.directory/authorizationPolicy/standard/read microsoft.directory/bitlockerKeys/key/read microsoft.directory/bulkJobs/standard/read microsoft.directory/cloudAppSecurity/allProperties/read microsoft.directory/conditionalAccessPolicies/allProperties/read microsoft.directory/connectorGroups/allProperties/read microsoft.directory/connectors/allProperties/read microsoft.directory/contacts/allProperties/read microsoft.directory/crossTenantAccessPolicy/default/standard/read microsoft.directory/crossTenantAccessPolicy/partners/identitySynchronization/standard/read microsoft.directory/crossTenantAccessPolicy/partners/standard/read microsoft.directory/crossTenantAccessPolicy/partners/templates/multiTenantOrganizationIdentitySynchronization/standard/read microsoft.directory/crossTenantAccessPolicy/partners/templates/multiTenantOrganizationPartnerConfiguration/standard/read microsoft.directory/crossTenantAccessPolicy/standard/read microsoft.directory/customAuthenticationExtensions/allProperties/read microsoft.directory/deviceLocalCredentials/standard/read microsoft.directory/deviceManagementPolicies/standard/read microsoft.directory/deviceRegistrationPolicy/standard/read microsoft.directory/devices/allProperties/read microsoft.directory/directoryRoles/allProperties/read microsoft.directory/directoryRoleTemplates/allProperties/read microsoft.directory/domains/allProperties/read microsoft.directory/domains/federationConfiguration/standard/read microsoft.directory/entitlementManagement/allProperties/read microsoft.directory/externalUserProfiles/standard/read microsoft.directory/groups/allProperties/read microsoft.directory/groupSettings/allProperties/read microsoft.directory/groupSettingTemplates/allProperties/read microsoft.directory/identityProtection/allProperties/read microsoft.directory/lifecycleWorkflows/workflows/allProperties/read microsoft.directory/loginOrganizationBranding/allProperties/read microsoft.directory/multiTenantOrganization/joinRequest/standard/read microsoft.directory/multiTenantOrganization/standard/read microsoft.directory/multiTenantOrganization/tenants/organizationDetails/read microsoft.directory/multiTenantOrganization/tenants/standard/read microsoft.directory/namedLocations/standard/read

	microsoft.directory/oAuth2PermissionGrants/allProperties/read microsoft.directory/onPremisesSynchronization/standard/read microsoft.directory/organization/allProperties/read microsoft.directory/pendingExternalUserProfiles/standard/read microsoft.directory/permissionGrantPolicies/standard/read microsoft.directory/policies/allProperties/read microsoft.directory/privilegedIdentityManagement/allProperties/read microsoft.directory/provisioningLogs/allProperties/read microsoft.directory/roleAssignments/allProperties/read microsoft.directory/roleDefinitions/allProperties/read microsoft.directory/scopedRoleMemberships/allProperties/read microsoft.directory/serviceAction/getAvailableExtentionProperties microsoft.directory/servicePrincipalCreationPolicies/standard/read microsoft.directory/servicePrincipals/allProperties/read microsoft.directory/servicePrincipals/synchronization/standard/read microsoft.directory/signInReports/allProperties/read microsoft.directory/subscribedSkus/allProperties/read microsoft.directory/users/allProperties/read microsoft.directory/users/authenticationMethods/standard/restrictedRead microsoft.directory/verifiableCredentials/configuration/allProperties/read microsoft.directory/verifiableCredentials/configuration/contracts/allProperties/read microsoft.directory/verifiableCredentials/configuration/contracts/cards/allProperties/read microsoft.edge/allEntities/allProperties/read microsoft.graph.dataConnect/allEntities/allProperties/read microsoft.hardware.support/shippingAddress/allProperties/read microsoft.hardware.support/shippingStatus/allProperties/read microsoft.hardware.support/warrantyClaims/allProperties/read microsoft.healthPlatform/allEntities/allProperties/read microsoft.insights/allEntities/allProperties/read microsoft.microsoft365.organizationalData/allEntities/allProperties/read microsoft.networkAccess/allEntities/allProperties/read microsoft.office365.copilot/allEntities/allProperties/read microsoft.office365.fileStorageContainers/allEntities/allProperties/read microsoft.office365.messageCenter/messages/read microsoft.office365.messageCenter/securityMessages/read microsoft.office365.network/performance/allProperties/read microsoft.office365.organizationalMessages/allEntities/allProperties/read microsoft.office365.protectionCenter/allEntities/allProperties/read microsoft.office365.securityComplianceCenter/allEntities/read microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.usageReports/allEntities/allProperties/read microsoft.office365.webPortal/allEntities/standard/read microsoft.office365.yammer/allEntities/allProperties/read microsoft.permissionsManagement/allEntities/allProperties/read microsoft.teams/allEntities/allProperties/read microsoft.virtualVisits/allEntities/allProperties/read microsoft.viva.glint/allEntities/allProperties/read microsoft.viva.goals/allEntities/allProperties/read microsoft.viva.pulse/allEntities/allProperties/read microsoft.windows.updatesDeployments/allEntities/allProperties/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Global Secure Access Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Create and manage all aspects of Global Secure Internet Access and Microsoft Global Secure Private Access, including managing access to public and private endpoints.
Identifier	ac434307-12b9-4fa1-a708-88bf58caabc1
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	ac434307-12b9-4fa1-a708-88bf58caabc1
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.supportTickets/allEntities/allTasks microsoft.directory/applicationPolicies/standard/read microsoft.directory/applications/applicationProxy/read microsoft.directory/applications/owners/read microsoft.directory/applications/policies/read microsoft.directory/applications/standard/read microsoft.directory/auditLogs/allProperties/read microsoft.directory/conditionalAccessPolicies/standard/read microsoft.directory/connectorGroups/allProperties/read microsoft.directory/connectors/allProperties/read microsoft.directory/crossTenantAccessPolicy/default/standard/read microsoft.directory/crossTenantAccessPolicy/partners/standard/read microsoft.directory/crossTenantAccessPolicy/standard/read microsoft.directory/namedLocations/standard/read microsoft.directory/signInReports/allProperties/read microsoft.networkAccess/allEntities/allProperties/allTasks microsoft.office365.messageCenter/messages/read microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Global Secure Access Log Reader

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Provides designated security personnel with read-only access to network traffic logs in Microsoft Entra Internet Access and Microsoft Entra Private Access for detailed analysis.
Identifier	843318fb-79a6-4168-9e6f-aa9a07481cc4
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	843318fb-79a6-4168-9e6f-aa9a07481cc4
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.networkAccess/trafficLogs/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Groups Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Members of this role can create/manage groups, create/manage groups settings like naming and expiration policies, and view groups activity and audit reports.
Identifier	fdd7a751-b60b-444a-984c-02652fe8fa1c
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	fdd7a751-b60b-444a-984c-02652fe8fa1c
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.directory/bulkJobs.groups/basic/update microsoft.directory/bulkJobs.groups/create microsoft.directory/bulkJobs.groups/standard/read microsoft.directory/deletedItems.groups/delete microsoft.directory/deletedItems.groups/restore microsoft.directory/groups/assignedLabels/update microsoft.directory/groups/assignLicense microsoft.directory/groups/basic/update microsoft.directory/groups/classification/update microsoft.directory/groups/create microsoft.directory/groups/delete microsoft.directory/groups/dynamicMembershipRule/update microsoft.directory/groups/groupType/update microsoft.directory/groups/hiddenMembers/read microsoft.directory/groups/members/update microsoft.directory/groups/onPremWriteBack/update microsoft.directory/groups/owners/update microsoft.directory/groups/reprocessLicenseAssignment microsoft.directory/groups/restore microsoft.directory/groups/settings/update microsoft.directory/groups/visibility/update microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Guest Inviter

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can invite guest users independent of the 'members can invite guests' setting.
Identifier	95e79109-95c0-4d8e-aee3-d01accf2d47b
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	95e79109-95c0-4d8e-aee3-d01accf2d47b
Version	1

Inheritance

Inherited Roles	Guest User

Allowed Permissions

Allowed Permissions	microsoft.directory/users/appRoleAssignments/read microsoft.directory/users/deviceForResourceAccount/read microsoft.directory/users/directReports/read microsoft.directory/users/invitedBy/read microsoft.directory/users/inviteGuest microsoft.directory/users/licenseDetails/read microsoft.directory/users/manager/read microsoft.directory/users/memberOf/read microsoft.directory/users/oAuth2PermissionGrants/read microsoft.directory/users/ownedDevices/read microsoft.directory/users/ownedObjects/read microsoft.directory/users/photo/read microsoft.directory/users/registeredDevices/read microsoft.directory/users/scopedRoleMemberOf/read microsoft.directory/users/sponsorOf/read microsoft.directory/users/sponsors/read microsoft.directory/users/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Guest User

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Default role for guest users. Can read a limited set of directory information.
Identifier	10dae51f-b6af-4016-8d66-8c2a99b929b3
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	10dae51f-b6af-4016-8d66-8c2a99b929b3
Version	1

Inheritance

Inherited Roles	

Allowed Permissions

Allowed Permissions	microsoft.directory/applications/owners/limitedRead microsoft.directory/applications/policies/limitedRead microsoft.directory/applications/standard/limitedRead microsoft.directory/directoryRoleTemplates/allProperties/read microsoft.directory/domains/standard/read microsoft.directory/groups/appRoleAssignments/limitedRead microsoft.directory/groups/memberOf/limitedRead microsoft.directory/groups/members/limitedRead microsoft.directory/groups/owners/limitedRead microsoft.directory/groups/settings/limitedRead microsoft.directory/groups/standard/limitedRead microsoft.directory/multiTenantOrganization/standard/read microsoft.directory/multiTenantOrganization/tenants/standard/read microsoft.directory/organization/basicProfile/read microsoft.directory/servicePrincipals/appRoleAssignedTo/limitedRead microsoft.directory/servicePrincipals/appRoleAssignments/limitedRead microsoft.directory/servicePrincipals/memberOf/limitedRead microsoft.directory/servicePrincipals/oAuth2PermissionGrants/limitedRead microsoft.directory/servicePrincipals/ownedObjects/limitedRead microsoft.directory/servicePrincipals/owners/limitedRead microsoft.directory/servicePrincipals/policies/limitedRead microsoft.directory/servicePrincipals/standard/limitedRead microsoft.directory/users/guestBasicProfile/limitedRead microsoft.directory/users/inviteGuest

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Helpdesk Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can reset passwords for non-administrators and Helpdesk Administrators.
Identifier	729827e3-9c14-49f7-bb1b-9608f156bbb8
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	729827e3-9c14-49f7-bb1b-9608f156bbb8
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.directory/bitlockerKeys/key/read microsoft.directory/deviceLocalCredentials/standard/read microsoft.directory/users/invalidateAllRefreshTokens microsoft.directory/users/password/update microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Hybrid Identity Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can manage Active Directory to Microsoft Entra cloud provisioning, Microsoft Entra Connect, and federation settings.
Identifier	8ac3fc64-6eca-42ea-9e69-59f4c7b60eb2
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	8ac3fc64-6eca-42ea-9e69-59f4c7b60eb2
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.directory/applications/appRoles/update microsoft.directory/applications/audience/update microsoft.directory/applications/authentication/update microsoft.directory/applications/basic/update microsoft.directory/applications/create microsoft.directory/applications/delete microsoft.directory/applications/disablement/update microsoft.directory/applications/notes/update microsoft.directory/applications/owners/update microsoft.directory/applications/permissions/update microsoft.directory/applications/policies/update microsoft.directory/applications/synchronization/standard/read microsoft.directory/applications/tag/update microsoft.directory/applicationTemplates/instantiate microsoft.directory/auditLogs/allProperties/read microsoft.directory/cloudProvisioning/allProperties/allTasks microsoft.directory/deletedItems.applications/delete microsoft.directory/deletedItems.applications/restore microsoft.directory/domains/allProperties/read microsoft.directory/domains/federation/update microsoft.directory/domains/federationConfiguration/basic/update microsoft.directory/domains/federationConfiguration/create microsoft.directory/domains/federationConfiguration/delete microsoft.directory/domains/federationConfiguration/standard/read microsoft.directory/hybridAuthenticationPolicy/allProperties/allTasks microsoft.directory/onPremisesSynchronization/basic/update microsoft.directory/onPremisesSynchronization/standard/read microsoft.directory/organization/dirSync/update microsoft.directory/passwordHashSync/allProperties/allTasks microsoft.directory/provisioningLogs/allProperties/read microsoft.directory/servicePrincipals/appRoleAssignedTo/update microsoft.directory/servicePrincipals/audience/update microsoft.directory/servicePrincipals/authentication/update microsoft.directory/servicePrincipals/basic/update microsoft.directory/servicePrincipals/create microsoft.directory/servicePrincipals/delete microsoft.directory/servicePrincipals/disable microsoft.directory/servicePrincipals/enable microsoft.directory/servicePrincipals/notes/update microsoft.directory/servicePrincipals/owners/update microsoft.directory/servicePrincipals/permissions/update microsoft.directory/servicePrincipals/policies/update microsoft.directory/servicePrincipals/synchronization.cloudTenantToCloudTenant/credentials/manage microsoft.directory/servicePrincipals/synchronization.cloudTenantToCloudTenant/jobs/manage microsoft.directory/servicePrincipals/synchronization.cloudTenantToCloudTenant/schema/manage microsoft.directory/servicePrincipals/synchronization.cloudTenantToExternalSystem/credentials/manage microsoft.directory/servicePrincipals/synchronization.cloudTenantToExternalSystem/jobs/manage microsoft.directory/servicePrincipals/synchronization.cloudTenantToExternalSystem/schema/manage microsoft.directory/servicePrincipals/synchronization/standard/read microsoft.directory/servicePrincipals/synchronizationCredentials/manage microsoft.directory/servicePrincipals/synchronizationJobs/manage

	microsoft.directory/servicePrincipals/synchronizationSchema/manage microsoft.directory/servicePrincipals/tag/update microsoft.directory/signInReports/allProperties/read microsoft.directory/users/authorizationInfo/update microsoft.office365.messageCenter/messages/read microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Identity Governance Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Manage access using Microsoft Entra ID for identity governance scenarios.
Identifier	45d8d3c5-c802-45c6-b32a-1d70b5e1e86e
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	45d8d3c5-c802-45c6-b32a-1d70b5e1e86e
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/accessReviews/allProperties/allTasks microsoft.directory/accessReviews/definitions.applications/allProperties/allTasks microsoft.directory/accessReviews/definitions.entitlementManagement/allProperties/allTasks microsoft.directory/accessReviews/definitions.groups/allProperties/read microsoft.directory/accessReviews/definitions.groups/allProperties/update microsoft.directory/accessReviews/definitions.groups/create microsoft.directory/accessReviews/definitions.groups/delete microsoft.directory/entitlementManagement/allProperties/allTasks microsoft.directory/groups/members/update microsoft.directory/servicePrincipals/appRoleAssignedTo/update

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Insights Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Has administrative access in the Microsoft 365 Insights app.
Identifier	eb1f4a8d-243a-41f0-9fbd-c7cdf6c5ef7c
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	eb1f4a8d-243a-41f0-9fbd-c7cdf6c5ef7c
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.insights/allEntities/allProperties/allTasks microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Insights Analyst

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Access the analytical capabilities in Microsoft Viva Insights and run custom queries.
Identifier	25df335f-86eb-4119-b717-0ff02de207e9
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	25df335f-86eb-4119-b717-0ff02de207e9
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.insights/queries/allProperties/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Insights Business Leader

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can view and share dashboards and insights via the M365 Insights app.
Identifier	31e939ad-9672-4796-9c2e-873181342d2d
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	31e939ad-9672-4796-9c2e-873181342d2d
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.insights/programs/allProperties/update microsoft.insights/reports/allProperties/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Intune Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can manage all aspects of the Intune product.
Identifier	3a2c62db-5318-420d-8d74-23affee5d9d5
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	3a2c62db-5318-420d-8d74-23affee5d9d5
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.supportTickets/allEntities/allTasks microsoft.cloudPC/allEntities/allProperties/allTasks microsoft.directory/bitlockerKeys/key/read microsoft.directory/contacts/basic/update microsoft.directory/contacts/create microsoft.directory/contacts/delete microsoft.directory/deletedItems.devices/delete microsoft.directory/deletedItems.devices/restore microsoft.directory/deviceLocalCredentials/password/read microsoft.directory/deviceManagementPolicies/standard/read microsoft.directory/deviceRegistrationPolicy/standard/read microsoft.directory/devices/basic/update microsoft.directory/devices/create microsoft.directory/devices/delete microsoft.directory/devices/disable microsoft.directory/devices/enable microsoft.directory/devices/extensionAttributeSet1/update microsoft.directory/devices/extensionAttributeSet2/update microsoft.directory/devices/extensionAttributeSet3/update microsoft.directory/devices/registeredOwners/update microsoft.directory/devices/registeredUsers/update microsoft.directory/groups.security/assignedLabels/update microsoft.directory/groups.security/basic/update microsoft.directory/groups.security/classification/update microsoft.directory/groups.security/create microsoft.directory/groups.security/delete microsoft.directory/groups.security/dynamicMembershipRule/update microsoft.directory/groups.security/members/update microsoft.directory/groups.security/owners/update microsoft.directory/groups.security/visibility/update microsoft.directory/groups/hiddenMembers/read microsoft.directory/users/basic/update microsoft.directory/users/manager/update microsoft.directory/users/photo/update microsoft.intune/allEntities/allTasks microsoft.office365.organizationalMessages/allEntities/allProperties/read microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	Azure MFA
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

IoT Device Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Provision new IoT devices, manage their lifecycle, configure certificates, and manage device templates.
Identifier	2ea5ce4c-b2d8-4668-bd81-3680bd2d227a
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	2ea5ce4c-b2d8-4668-bd81-3680bd2d227a
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/certificateBasedDeviceAuthConfigurations/create microsoft.directory/certificateBasedDeviceAuthConfigurations/credentials/update microsoft.directory/certificateBasedDeviceAuthConfigurations/delete microsoft.directory/certificateBasedDeviceAuthConfigurations/standard/read microsoft.directory/deviceTemplates/create microsoft.directory/deviceTemplates/createDeviceFromTemplate microsoft.directory/deviceTemplates/delete microsoft.directory/deviceTemplates/deviceInstances/read microsoft.directory/deviceTemplates/owners/read microsoft.directory/deviceTemplates/owners/update

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Kaizala Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can manage settings for Microsoft Kaizala.
Identifier	74ef975b-6605-40af-a5d2-b9539d836353
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	74ef975b-6605-40af-a5d2-b9539d836353
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/authorizationPolicy/standard/read microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Knowledge Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can configure knowledge, learning, and other intelligent features.
Identifier	b5a8dcf3-09d5-43a9-a639-8e29ef291470
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	b5a8dcf3-09d5-43a9-a639-8e29ef291470
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/groups.security/basic/update microsoft.directory/groups.security/create microsoft.directory/groups.security/createAsOwner microsoft.directory/groups.security/delete microsoft.directory/groups.security/members/update microsoft.directory/groups.security/owners/update microsoft.office365.knowledge/contentUnderstanding/allProperties/allTasks microsoft.office365.knowledge/knowledgeNetwork/allProperties/allTasks microsoft.office365.knowledge/learningSources/allProperties/allTasks microsoft.office365.protectionCenter/sensitivityLabels/allProperties/read microsoft.office365.sharePoint/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Knowledge Manager

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Has access to topic management dashboard and can manage content.
Identifier	744ec460-397e-42ad-a462-8b3f9747a02c
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	744ec460-397e-42ad-a462-8b3f9747a02c
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/groups.security/basic/update microsoft.directory/groups.security/create microsoft.directory/groups.security/createAsOwner microsoft.directory/groups.security/delete microsoft.directory/groups.security/members/update microsoft.directory/groups.security/owners/update microsoft.office365.knowledge/contentUnderstanding/analytics/allProperties/read microsoft.office365.knowledge/knowledgeNetwork/topicVisibility/allProperties/allTasks microsoft.office365.sharePoint/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

License Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can manage product licenses on users and groups.
Identifier	4d6ac14f-3453-41d0-bef9-a3e0c569773a
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	4d6ac14f-3453-41d0-bef9-a3e0c569773a
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.directory/authorizationPolicy/standard/read microsoft.directory/groups/assignLicense microsoft.directory/groups/reprocessLicenseAssignment microsoft.directory/users/assignLicense microsoft.directory/users/reprocessLicenseAssignment microsoft.directory/users/usageLocation/update microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Lifecycle Workflows Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Create and manage all aspects of workflows and tasks associated with Lifecycle Workflows in Microsoft Entra ID.
Identifier	59d46f88-662b-457b-bceb-5c3809e5908f
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	59d46f88-662b-457b-bceb-5c3809e5908f
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/lifecycleWorkflows/workflows/allProperties/allTasks microsoft.directory/organization/strongAuthentication/read microsoft.directory/users/lifeCycleInfo/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Message Center Privacy Reader

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can read security messages and updates in Office 365 Message Center only.
Identifier	ac16e43d-7b2d-40e0-ac05-243ff356ab5b
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	ac16e43d-7b2d-40e0-ac05-243ff356ab5b
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.office365.messageCenter/messages/read microsoft.office365.messageCenter/securityMessages/read microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Message Center Reader

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can read messages and updates for their organization in Office 365 Message Center only.
Identifier	790c1fb9-7f7d-4f88-86a1-ef1f95c05c1b
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	790c1fb9-7f7d-4f88-86a1-ef1f95c05c1b
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.office365.messageCenter/messages/read microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Microsoft 365 Backup Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Back up and restore content across supported services (SharePoint, OneDrive, and Exchange Online) in Microsoft 365 Backup
Identifier	1707125e-0aa2-4d4d-8655-a7c786c76a25
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	1707125e-0aa2-4d4d-8655-a7c786c76a25
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.backup/allEntities/allProperties/allTasks microsoft.office365.network/performance/allProperties/read microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.usageReports/allEntities/allProperties/read microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Microsoft 365 Migration Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Perform all migration functionality to migrate content to Microsoft 365 using Migration Manager.
Identifier	8c8b803f-96e1-4129-9349-20738d9f9652
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	8c8b803f-96e1-4129-9349-20738d9f9652
Version	1

Inheritance

Inherited Roles	

Allowed Permissions

Allowed Permissions	microsoft.office365.migrations/allEntities/allProperties/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Microsoft Graph Data Connect Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Manage aspects of Microsoft Graph Data Connect service in a tenant.
Identifier	ee67aa9c-e510-4759-b906-227085a7fd4d
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	ee67aa9c-e510-4759-b906-227085a7fd4d
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.graph.dataConnect/allEntities/allProperties/allTasks microsoft.office365.messageCenter/messages/read microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Microsoft Hardware Warranty Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Create and manage all aspects warranty claims and entitlements for Microsoft manufactured hardware, like Surface and HoloLens.
Identifier	1501b917-7653-4ff9-a4b5-203eaf33784f
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	1501b917-7653-4ff9-a4b5-203eaf33784f
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.hardware.support/shippingAddress/allProperties/allTasks microsoft.hardware.support/shippingStatus/allProperties/read microsoft.hardware.support/warrantyClaims/allProperties/allTasks microsoft.office365.messageCenter/messages/read microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Microsoft Hardware Warranty Specialist

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Create and read warranty claims for Microsoft manufactured hardware, like Surface and HoloLens.
Identifier	281fe777-fb20-4fbb-b7a3-ccebce5b0d96
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	281fe777-fb20-4fbb-b7a3-ccebce5b0d96
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.hardware.support/shippingAddress/allProperties/read microsoft.hardware.support/warrantyClaims/createAsOwner microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Network Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can manage network locations and review enterprise network design insights for Microsoft 365 Software as a Service applications.
Identifier	d37c8bed-0711-4417-ba38-b4abe66ce4c2
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	d37c8bed-0711-4417-ba38-b4abe66ce4c2
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.office365.network/locations/allProperties/allTasks microsoft.office365.network/performance/allProperties/read microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Office Apps Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	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.
Identifier	2b745bdf-0803-4d80-aa65-822c4493daac
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	2b745bdf-0803-4d80-aa65-822c4493daac
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.office365.messageCenter/messages/read microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.userCommunication/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

On Premises Directory Sync Account

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Only used by Microsoft Entra Connect Sync Account.
Identifier	a92aed5d-d78a-4d16-b381-09adb37eb3b0
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	a92aed5d-d78a-4d16-b381-09adb37eb3b0
Version	1

Inheritance

Inherited Roles	

Allowed Permissions

Allowed Permissions	microsoft.directory/onPremisesSynchronization/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Organizational Branding Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Manage all aspects of organizational branding in a tenant.
Identifier	92ed04bf-c94a-4b82-9729-b799a7a4c178
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	92ed04bf-c94a-4b82-9729-b799a7a4c178
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/loginOrganizationBranding/allProperties/allTasks

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Organizational Data Source Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Set up and manage the ingestion of organizational data into Microsoft 365.
Identifier	9d70768a-0cbc-4b4c-aea3-2e124b2477f4
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	9d70768a-0cbc-4b4c-aea3-2e124b2477f4
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.microsoft365.organizationalData/allEntities/allProperties/allTasks microsoft.office365.messageCenter/messages/read microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Organizational Messages Approver

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Review, approve, or reject new organizational messages for delivery in the Microsoft 365 admin center before they are sent to users.
Identifier	e48398e2-f4bb-4074-8f31-4586725e205b
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	e48398e2-f4bb-4074-8f31-4586725e205b
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.office365.organizationalMessages/allEntities/allProperties/read microsoft.office365.organizationalMessages/allEntities/allProperties/update microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Organizational Messages Writer

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Write, publish, manage, and review the organizational messages for end-users through Microsoft product surfaces.
Identifier	507f53e4-4e52-4077-abd3-d2e1558b6ea2
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	507f53e4-4e52-4077-abd3-d2e1558b6ea2
Version	1

Inheritance

Inherited Roles	

Allowed Permissions

Allowed Permissions	microsoft.office365.organizationalMessages/allEntities/allProperties/allTasks microsoft.office365.usageReports/allEntities/standard/read microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Partner Tier1 Support

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Do not use - not intended for general use.
Identifier	4ba39ca4-527c-499a-b93d-d9b492c50246
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	4ba39ca4-527c-499a-b93d-d9b492c50246
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.directory/applications/appRoles/update microsoft.directory/applications/audience/update microsoft.directory/applications/authentication/update microsoft.directory/applications/basic/update microsoft.directory/applications/credentials/update microsoft.directory/applications/notes/update microsoft.directory/applications/owners/update microsoft.directory/applications/permissions/update microsoft.directory/applications/policies/update microsoft.directory/applications/tag/update microsoft.directory/contacts/basic/update microsoft.directory/contacts/create microsoft.directory/contacts/delete microsoft.directory/deletedItems.groups/restore microsoft.directory/deletedItems.users/restore microsoft.directory/groups.unified/assignedLabels/update microsoft.directory/groups/create microsoft.directory/groups/delete microsoft.directory/groups/members/update microsoft.directory/groups/owners/update microsoft.directory/groups/restore microsoft.directory/oAuth2PermissionGrants/allProperties/allTasks microsoft.directory/servicePrincipals/appRoleAssignedTo/update microsoft.directory/users/assignLicense microsoft.directory/users/basic/update microsoft.directory/users/create microsoft.directory/users/delete microsoft.directory/users/disable microsoft.directory/users/enable microsoft.directory/users/invalidateAllRefreshTokens microsoft.directory/users/manager/update microsoft.directory/users/password/update microsoft.directory/users/photo/update microsoft.directory/users/restore microsoft.directory/users/userPrincipalName/update microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	Azure MFA
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Partner Tier2 Support

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Do not use - not intended for general use.
Identifier	e00e864a-17c5-4a4b-9c06-f5b95a8d5bd8
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	e00e864a-17c5-4a4b-9c06-f5b95a8d5bd8
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.directory/applications/appRoles/update microsoft.directory/applications/audience/update microsoft.directory/applications/authentication/update microsoft.directory/applications/basic/update microsoft.directory/applications/credentials/update microsoft.directory/applications/notes/update microsoft.directory/applications/owners/update microsoft.directory/applications/permissions/update microsoft.directory/applications/policies/update microsoft.directory/applications/tag/update microsoft.directory/contacts/basic/update microsoft.directory/contacts/create microsoft.directory/contacts/delete microsoft.directory/deletedItems.groups/restore microsoft.directory/deletedItems.users/restore microsoft.directory/domains/allProperties/allTasks microsoft.directory/groups.unified/assignedLabels/update microsoft.directory/groups/create microsoft.directory/groups/delete microsoft.directory/groups/members/update microsoft.directory/groups/owners/update microsoft.directory/groups/restore microsoft.directory/oAuth2PermissionGrants/allProperties/allTasks microsoft.directory/organization/basic/update microsoft.directory/roleAssignments/allProperties/allTasks microsoft.directory/roleDefinitions/allProperties/allTasks microsoft.directory/scopedRoleMemberships/allProperties/allTasks microsoft.directory/servicePrincipals/appRoleAssignedTo/update microsoft.directory/subscribedSkus/standard/read microsoft.directory/users/assignLicense microsoft.directory/users/basic/update microsoft.directory/users/create microsoft.directory/users/delete microsoft.directory/users/disable microsoft.directory/users/enable microsoft.directory/users/invalidateAllRefreshTokens microsoft.directory/users/manager/update microsoft.directory/users/password/update microsoft.directory/users/photo/update microsoft.directory/users/restore microsoft.directory/users/userPrincipalName/update microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	Azure MFA
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Password Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can reset passwords for non-administrators and Password Administrators.
Identifier	966707d0-3269-4727-9be2-8c3a10f19b9d
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	966707d0-3269-4727-9be2-8c3a10f19b9d
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/users/password/update microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

People Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Manage profile photos of users and people settings for all users in the organization.
Identifier	024906de-61e5-49c8-8572-40335f1e0e10
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	024906de-61e5-49c8-8572-40335f1e0e10
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.office365.webPortal/allEntities/standard/read microsoft.people/users/photo/read microsoft.people/users/photo/update microsoft.peopleAdmin/organization/allProperties/read microsoft.peopleAdmin/organization/allProperties/update

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Permissions Management Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Manage all aspects of Entra Permissions Management.
Identifier	af78dc32-cf4d-46f9-ba4e-4428526346b5
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	af78dc32-cf4d-46f9-ba4e-4428526346b5
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.permissionsManagement/allEntities/allProperties/allTasks

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Places Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Manage all aspects of the Microsoft Places service.
Identifier	78b0ccd1-afc2-4f92-9116-b41aedd09592
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	78b0ccd1-afc2-4f92-9116-b41aedd09592
Version	1

Inheritance

Inherited Roles	

Allowed Permissions

Allowed Permissions	microsoft.places/allEntities/allProperties/allTasks

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Power Platform Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can create and manage all aspects of Microsoft Dynamics 365, PowerApps and Microsoft Flow.
Identifier	11648597-926c-4cf3-9c36-bcebb0ba8dcc
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	11648597-926c-4cf3-9c36-bcebb0ba8dcc
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.dynamics365/allEntities/allTasks microsoft.flow/allEntities/allTasks microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read microsoft.powerApps/allEntities/allTasks

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Printer Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can manage all aspects of printers and printer connectors.
Identifier	644ef478-e28f-4e28-b9dc-3fdde9aa0b1f
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	644ef478-e28f-4e28-b9dc-3fdde9aa0b1f
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.print/allEntities/allProperties/allTasks

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Printer Technician

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can register and unregister printers and update printer status.
Identifier	e8cef6f1-e4bd-4ea8-bc07-4b8d950f4477
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	e8cef6f1-e4bd-4ea8-bc07-4b8d950f4477
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.print/connectors/allProperties/read microsoft.azure.print/printers/allProperties/read microsoft.azure.print/printers/basic/update microsoft.azure.print/printers/register microsoft.azure.print/printers/unregister

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Privileged Authentication Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can access to view, set and reset authentication method information for any user (admin or non-admin).
Identifier	7be44c8a-adaf-4e2a-84d6-ab2649e08a13
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	7be44c8a-adaf-4e2a-84d6-ab2649e08a13
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.directory/deletedItems.users/restore microsoft.directory/users/authenticationMethods/basic/update microsoft.directory/users/authenticationMethods/create microsoft.directory/users/authenticationMethods/delete microsoft.directory/users/authenticationMethods/standard/read microsoft.directory/users/authorizationInfo/update microsoft.directory/users/basic/update microsoft.directory/users/delete microsoft.directory/users/disable microsoft.directory/users/enable microsoft.directory/users/invalidateAllRefreshTokens microsoft.directory/users/manager/update microsoft.directory/users/password/update microsoft.directory/users/restore microsoft.directory/users/userPrincipalName/update microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Privileged Role Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can manage role assignments in Microsoft Entra ID, and all aspects of Privileged Identity Management.
Identifier	e8611ab8-c189-46e8-94e1-60213ab1f814
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	e8611ab8-c189-46e8-94e1-60213ab1f814
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/accessReviews/definitions.applications/allProperties/read microsoft.directory/accessReviews/definitions.directoryRoles/allProperties/allTasks microsoft.directory/accessReviews/definitions.groups/allProperties/read microsoft.directory/accessReviews/definitions.groupsAssignableToRoles/allProperties/update microsoft.directory/accessReviews/definitions.groupsAssignableToRoles/create microsoft.directory/accessReviews/definitions.groupsAssignableToRoles/delete microsoft.directory/administrativeUnits/allProperties/allTasks microsoft.directory/authorizationPolicy/allProperties/allTasks microsoft.directory/directoryRoles/allProperties/allTasks microsoft.directory/groupsAssignableToRoles/allProperties/update microsoft.directory/groupsAssignableToRoles/assignLicense microsoft.directory/groupsAssignableToRoles/create microsoft.directory/groupsAssignableToRoles/delete microsoft.directory/groupsAssignableToRoles/reprocessLicenseAssignment microsoft.directory/groupsAssignableToRoles/restore microsoft.directory/oAuth2PermissionGrants/allProperties/allTasks microsoft.directory/permissionGrantPolicies/allProperties/read microsoft.directory/permissionGrantPolicies/allProperties/update microsoft.directory/permissionGrantPolicies/create microsoft.directory/permissionGrantPolicies/delete microsoft.directory/privilegedIdentityManagement/allProperties/allTasks microsoft.directory/roleAssignments/allProperties/allTasks microsoft.directory/roleDefinitions/allProperties/allTasks microsoft.directory/scopedRoleMemberships/allProperties/allTasks microsoft.directory/servicePrincipals/appRoleAssignedTo/update microsoft.directory/servicePrincipals/managePermissionGrantsForAll.microsoft-company-admin microsoft.directory/servicePrincipals/permissions/update microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	Azure MFA
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Purview Workload Content Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Manage or purge data from Microsoft 365 when accessing from the Microsoft Purview portal.
Identifier	3f04f91a-4ad7-4bd3-bcfa-49882ea1a88a
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	3f04f91a-4ad7-4bd3-bcfa-49882ea1a88a
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Purview Workload Content Reader

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Read data from Microsoft 365 when accessing from the Microsoft Purview portal.
Identifier	e07494ad-1654-4dd2-922e-6f81a71bf00f
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	e07494ad-1654-4dd2-922e-6f81a71bf00f
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Purview Workload Content Writer

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Read and edit data from Microsoft 365 when accessing from the Microsoft Purview portal.
Identifier	02d5655b-c1cf-4e5f-98da-5fb919085bf6
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	02d5655b-c1cf-4e5f-98da-5fb919085bf6
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Reports Reader

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can read sign-in and audit reports.
Identifier	4a5d8f65-41da-4de4-8968-e035b65339cf
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	4a5d8f65-41da-4de4-8968-e035b65339cf
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.directory/auditLogs/allProperties/read microsoft.directory/provisioningLogs/allProperties/read microsoft.directory/signInReports/allProperties/read microsoft.office365.network/performance/allProperties/read microsoft.office365.usageReports/allEntities/allProperties/read microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

1 Role Assignments

Display Name	Principal Type	Scope	Membership	State	Start Time	End Time
XIA	User	Microsoft Graph Command Line Tools (Service Principal)	Direct	Assigned	[Not Configured]	Permanent

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Restricted Guest User

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Restricted role for guest users. Can read a limited set of directory information.
Identifier	2af84b1e-32c8-42b7-82bc-daa82404023b
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	2af84b1e-32c8-42b7-82bc-daa82404023b
Version	1

Inheritance

Inherited Roles	

Allowed Permissions

Allowed Permissions	microsoft.directory/applications/owners/limitedRead microsoft.directory/applications/policies/limitedRead microsoft.directory/applications/standard/limitedRead microsoft.directory/directoryRoleTemplates/allProperties/read microsoft.directory/domains/standard/read microsoft.directory/organization/basicProfile/read microsoft.directory/servicePrincipals/appRoleAssignedTo/limitedRead microsoft.directory/servicePrincipals/appRoleAssignments/limitedRead microsoft.directory/servicePrincipals/memberOf/limitedRead microsoft.directory/servicePrincipals/oAuth2PermissionGrants/limitedRead microsoft.directory/servicePrincipals/ownedObjects/limitedRead microsoft.directory/servicePrincipals/owners/limitedRead microsoft.directory/servicePrincipals/policies/limitedRead microsoft.directory/servicePrincipals/standard/limitedRead

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Search Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can create and manage all aspects of Microsoft Search settings.
Identifier	0964bb5e-9bdb-4d7b-ac29-58e794862a40
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	0964bb5e-9bdb-4d7b-ac29-58e794862a40
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.office365.messageCenter/messages/read microsoft.office365.search/content/manage microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Search Editor

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can create and manage the editorial content such as bookmarks, Q and As, locations, floorplan.
Identifier	8835291a-918c-4fd7-a9ce-faa49f0cf7d9
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	8835291a-918c-4fd7-a9ce-faa49f0cf7d9
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.office365.messageCenter/messages/read microsoft.office365.search/content/manage microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Security Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can read security information and reports, and manage configuration in Microsoft Entra ID and Office 365.
Identifier	194ae4cb-b126-40b2-bd5b-6091b380977d
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	194ae4cb-b126-40b2-bd5b-6091b380977d
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.agentRegistry/allEntities/allProperties/read microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.directory/applications/policies/update microsoft.directory/auditLogs/allProperties/read microsoft.directory/authorizationPolicy/standard/read microsoft.directory/bitlockerKeys/key/read microsoft.directory/bulkJobs/standard/read microsoft.directory/conditionalAccessPolicies/basic/update microsoft.directory/conditionalAccessPolicies/create microsoft.directory/conditionalAccessPolicies/delete microsoft.directory/conditionalAccessPolicies/owners/read microsoft.directory/conditionalAccessPolicies/owners/update microsoft.directory/conditionalAccessPolicies/policyAppliedTo/read microsoft.directory/conditionalAccessPolicies/standard/read microsoft.directory/conditionalAccessPolicies/tenantDefault/update microsoft.directory/crossTenantAccessPolicy/allowedCloudEndpoints/update microsoft.directory/crossTenantAccessPolicy/basic/update microsoft.directory/crossTenantAccessPolicy/default/b2bCollaboration/update microsoft.directory/crossTenantAccessPolicy/default/b2bDirectConnect/update microsoft.directory/crossTenantAccessPolicy/default/crossCloudMeetings/update microsoft.directory/crossTenantAccessPolicy/default/standard/read microsoft.directory/crossTenantAccessPolicy/default/tenantRestrictions/update microsoft.directory/crossTenantAccessPolicy/partners/b2bCollaboration/update microsoft.directory/crossTenantAccessPolicy/partners/b2bDirectConnect/update microsoft.directory/crossTenantAccessPolicy/partners/create microsoft.directory/crossTenantAccessPolicy/partners/crossCloudMeetings/update microsoft.directory/crossTenantAccessPolicy/partners/delete microsoft.directory/crossTenantAccessPolicy/partners/identitySynchronization/basic/update microsoft.directory/crossTenantAccessPolicy/partners/identitySynchronization/create microsoft.directory/crossTenantAccessPolicy/partners/identitySynchronization/standard/read microsoft.directory/crossTenantAccessPolicy/partners/standard/read microsoft.directory/crossTenantAccessPolicy/partners/templates/multiTenantOrganizationIdentitySynchronization/basic/update microsoft.directory/crossTenantAccessPolicy/partners/templates/multiTenantOrganizationIdentitySynchronization/resetToDefaultSettings microsoft.directory/crossTenantAccessPolicy/partners/templates/multiTenantOrganizationIdentitySynchronization/standard/read microsoft.directory/crossTenantAccessPolicy/partners/templates/multiTenantOrganizationPartnerConfiguration/basic/update microsoft.directory/crossTenantAccessPolicy/partners/templates/multiTenantOrganizationPartnerConfiguration/resetToDefaultSettings microsoft.directory/crossTenantAccessPolicy/partners/templates/multiTenantOrganizationPartnerConfiguration/standard/read microsoft.directory/crossTenantAccessPolicy/partners/tenantRestrictions/update microsoft.directory/crossTenantAccessPolicy/standard/read microsoft.directory/deviceLocalCredentials/standard/read microsoft.directory/domains/federation/update microsoft.directory/domains/federationConfiguration/basic/update microsoft.directory/domains/federationConfiguration/create microsoft.directory/domains/federationConfiguration/delete microsoft.directory/domains/federationConfiguration/standard/read microsoft.directory/entitlementManagement/allProperties/read microsoft.directory/identityProtection/allProperties/read microsoft.directory/identityProtection/allProperties/update microsoft.directory/multiTenantOrganization/basic/update

	microsoft.directory/multiTenantOrganization/create microsoft.directory/multiTenantOrganization/joinRequest/organizationDetails/update microsoft.directory/multiTenantOrganization/joinRequest/standard/read microsoft.directory/multiTenantOrganization/standard/read microsoft.directory/multiTenantOrganization/tenants/create microsoft.directory/multiTenantOrganization/tenants/delete microsoft.directory/multiTenantOrganization/tenants/organizationDetails/read microsoft.directory/multiTenantOrganization/tenants/organizationDetails/update microsoft.directory/multiTenantOrganization/tenants/standard/read microsoft.directory/namedLocations/basic/update microsoft.directory/namedLocations/create microsoft.directory/namedLocations/delete microsoft.directory/namedLocations/standard/read microsoft.directory/policies/basic/update microsoft.directory/policies/create microsoft.directory/policies/delete microsoft.directory/policies/owners/update microsoft.directory/policies/tenantDefault/update microsoft.directory/privilegedIdentityManagement/allProperties/read microsoft.directory/provisioningLogs/allProperties/read microsoft.directory/resourceNamespaces/resourceActions/authenticationContext/update microsoft.directory/servicePrincipals/policies/update microsoft.directory/signInReports/allProperties/read microsoft.networkAccess/allEntities/allProperties/allTasks microsoft.office365.protectionCenter/allEntities/basic/update microsoft.office365.protectionCenter/allEntities/standard/read microsoft.office365.protectionCenter/attackSimulator/payload/allProperties/allTasks microsoft.office365.protectionCenter/attackSimulator/reports/allProperties/read microsoft.office365.protectionCenter/attackSimulator/simulation/allProperties/allTasks microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

1 Role Assignments

Display Name	Principal Type	Scope	Membership	State	Start Time	End Time
XIA	User	Directory	Direct	Assigned	[Not Configured]	Permanent

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	Azure MFA
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Security Operator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Creates and manages security events.
Identifier	5f2222b1-57c3-48ba-8ad5-d4759f1fde6f
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	5f2222b1-57c3-48ba-8ad5-d4759f1fde6f
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.advancedThreatProtection/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.directory/auditLogs/allProperties/read microsoft.directory/authorizationPolicy/standard/read microsoft.directory/bulkJobs/standard/read microsoft.directory/cloudAppSecurity/allProperties/allTasks microsoft.directory/identityProtection/allProperties/allTasks microsoft.directory/privilegedIdentityManagement/allProperties/read microsoft.directory/provisioningLogs/allProperties/read microsoft.directory/signInReports/allProperties/read microsoft.directory/users/disable microsoft.directory/users/enable microsoft.directory/users/invalidateAllRefreshTokens microsoft.directory/users/password/update microsoft.intune/allEntities/read microsoft.office365.securityComplianceCenter/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.windows.defenderAdvancedThreatProtection/allEntities/allTasks

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Security Reader

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can read security information and reports in Microsoft Entra ID and Office 365.
Identifier	5d6b6bb7-de71-4623-b4af-96380a352509
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	5d6b6bb7-de71-4623-b4af-96380a352509
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.agentRegistry/allEntities/allProperties/read microsoft.azure.serviceHealth/allEntities/allTasks microsoft.directory/accessReviews/definitions/allProperties/read microsoft.directory/auditLogs/allProperties/read microsoft.directory/authorizationPolicy/standard/read microsoft.directory/bitlockerKeys/key/read microsoft.directory/bulkJobs/standard/read microsoft.directory/conditionalAccessPolicies/owners/read microsoft.directory/conditionalAccessPolicies/policyAppliedTo/read microsoft.directory/conditionalAccessPolicies/standard/read microsoft.directory/crossTenantAccessPolicy/partners/templates/multiTenantOrganizationIdentitySynchronization/standard/read microsoft.directory/crossTenantAccessPolicy/partners/templates/multiTenantOrganizationPartnerConfiguration/standard/read microsoft.directory/deviceLocalCredentials/standard/read microsoft.directory/domains/federationConfiguration/standard/read microsoft.directory/entitlementManagement/allProperties/read microsoft.directory/identityProtection/allProperties/read microsoft.directory/multiTenantOrganization/joinRequest/standard/read microsoft.directory/multiTenantOrganization/standard/read microsoft.directory/multiTenantOrganization/tenants/organizationDetails/read microsoft.directory/multiTenantOrganization/tenants/standard/read microsoft.directory/namedLocations/standard/read microsoft.directory/policies/owners/read microsoft.directory/policies/policyAppliedTo/read microsoft.directory/policies/standard/read microsoft.directory/privilegedIdentityManagement/allProperties/read microsoft.directory/provisioningLogs/allProperties/read microsoft.directory/signInReports/allProperties/read microsoft.networkAccess/allEntities/allProperties/read microsoft.office365.protectionCenter/allEntities/standard/read microsoft.office365.protectionCenter/attackSimulator/payload/allProperties/read microsoft.office365.protectionCenter/attackSimulator/reports/allProperties/read microsoft.office365.protectionCenter/attackSimulator/simulation/allProperties/read microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Service Support Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can read service health information and manage support tickets.
Identifier	f023fd81-a637-4b56-95fd-791ac0226033
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	f023fd81-a637-4b56-95fd-791ac0226033
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.office365.network/performance/allProperties/read microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

SharePoint Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can manage all aspects of the SharePoint service.
Identifier	f28a1f50-f6e7-4571-818b-6a12f2af6b6c
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	f28a1f50-f6e7-4571-818b-6a12f2af6b6c
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.backup/oneDriveForBusinessProtectionPolicies/allProperties/allTasks microsoft.backup/oneDriveForBusinessRestoreSessions/allProperties/allTasks microsoft.backup/restorePoints/sites/allProperties/allTasks microsoft.backup/restorePoints/userDrives/allProperties/allTasks microsoft.backup/sharePointProtectionPolicies/allProperties/allTasks microsoft.backup/sharePointRestoreSessions/allProperties/allTasks microsoft.backup/siteProtectionUnits/allProperties/allTasks microsoft.backup/siteRestoreArtifacts/allProperties/allTasks microsoft.backup/userDriveProtectionUnits/allProperties/allTasks microsoft.backup/userDriveRestoreArtifacts/allProperties/allTasks microsoft.directory/groups.unified/assignedLabels/update microsoft.directory/groups.unified/basic/update microsoft.directory/groups.unified/create microsoft.directory/groups.unified/delete microsoft.directory/groups.unified/members/update microsoft.directory/groups.unified/owners/update microsoft.directory/groups.unified/restore microsoft.directory/groups/hiddenMembers/read microsoft.office365.migrations/allEntities/allProperties/allTasks microsoft.office365.network/performance/allProperties/read microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.sharePoint/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.usageReports/allEntities/allProperties/read microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	Azure MFA
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

SharePoint Advanced Management Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Manage all aspects of SharePoint Advanced Management.
Identifier	99009c4a-3b3f-4957-82a9-9d35e12db77e
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	99009c4a-3b3f-4957-82a9-9d35e12db77e
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.backup/oneDriveForBusinessProtectionPolicies/allProperties/allTasks microsoft.backup/oneDriveForBusinessRestoreSessions/allProperties/allTasks microsoft.backup/restorePoints/sites/allProperties/allTasks microsoft.backup/restorePoints/userDrives/allProperties/allTasks microsoft.backup/sharePointProtectionPolicies/allProperties/allTasks microsoft.backup/sharePointRestoreSessions/allProperties/allTasks microsoft.backup/siteProtectionUnits/allProperties/allTasks microsoft.backup/siteRestoreArtifacts/allProperties/allTasks microsoft.backup/userDriveProtectionUnits/allProperties/allTasks microsoft.backup/userDriveRestoreArtifacts/allProperties/allTasks microsoft.directory/groups.unified/assignedLabels/update microsoft.directory/groups.unified/basic/update microsoft.directory/groups.unified/create microsoft.directory/groups.unified/delete microsoft.directory/groups.unified/members/update microsoft.directory/groups.unified/owners/update microsoft.directory/groups.unified/restore microsoft.directory/groups/hiddenMembers/read microsoft.office365.migrations/allEntities/allProperties/allTasks microsoft.office365.network/performance/allProperties/read microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.sharePoint/allEntities/allTasks microsoft.office365.sharePointAdvancedManagement/allEntities/allProperties/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.usageReports/allEntities/allProperties/read microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

SharePoint Backup Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Back up and restore content (including granular restore) for SharePoint and OneDrive in Microsoft 365 Backup
Identifier	9d3e04ba-3ee4-4d1b-a3a7-9aef423a09be
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	9d3e04ba-3ee4-4d1b-a3a7-9aef423a09be
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.backup/oneDriveForBusinessProtectionPolicies/allProperties/allTasks microsoft.backup/oneDriveForBusinessRestoreSessions/allProperties/allTasks microsoft.backup/restorePoints/sites/allProperties/allTasks microsoft.backup/restorePoints/userDrives/allProperties/allTasks microsoft.backup/sharePointProtectionPolicies/allProperties/allTasks microsoft.backup/sharePointRestoreSessions/allProperties/allTasks microsoft.backup/siteProtectionUnits/allProperties/allTasks microsoft.backup/siteRestoreArtifacts/allProperties/allTasks microsoft.backup/userDriveProtectionUnits/allProperties/allTasks microsoft.backup/userDriveRestoreArtifacts/allProperties/allTasks microsoft.office365.network/performance/allProperties/read microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.usageReports/allEntities/allProperties/read microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

SharePoint Embedded Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Manage all aspects of SharePoint Embedded containers.
Identifier	1a7d78b6-429f-476b-b8eb-35fb715fffd4
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	1a7d78b6-429f-476b-b8eb-35fb715fffd4
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.office365.fileStorageContainers/allEntities/allProperties/allTasks microsoft.office365.network/performance/allProperties/read microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.usageReports/allEntities/allProperties/read microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Skype for Business Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can manage all aspects of the Skype for Business product.
Identifier	75941009-915a-4869-abe7-691bff18279e
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	75941009-915a-4869-abe7-691bff18279e
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.skypeForBusiness/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.usageReports/allEntities/allProperties/read microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	Azure MFA
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Teams Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can manage the Microsoft Teams service.
Identifier	69091246-20e8-4a56-aa4d-066075b2a7a8
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	69091246-20e8-4a56-aa4d-066075b2a7a8
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.directory/authorizationPolicy/standard/read microsoft.directory/crossTenantAccessPolicy/allowedCloudEndpoints/update microsoft.directory/crossTenantAccessPolicy/default/crossCloudMeetings/update microsoft.directory/crossTenantAccessPolicy/default/standard/read microsoft.directory/crossTenantAccessPolicy/partners/create microsoft.directory/crossTenantAccessPolicy/partners/crossCloudMeetings/update microsoft.directory/crossTenantAccessPolicy/partners/standard/read microsoft.directory/crossTenantAccessPolicy/standard/read microsoft.directory/externalUserProfiles/basic/update microsoft.directory/externalUserProfiles/delete microsoft.directory/externalUserProfiles/standard/read microsoft.directory/groups.unified/assignedLabels/update microsoft.directory/groups.unified/basic/update microsoft.directory/groups.unified/create microsoft.directory/groups.unified/delete microsoft.directory/groups.unified/members/update microsoft.directory/groups.unified/owners/update microsoft.directory/groups.unified/restore microsoft.directory/groups/hiddenMembers/read microsoft.directory/pendingExternalUserProfiles/basic/update microsoft.directory/pendingExternalUserProfiles/create microsoft.directory/pendingExternalUserProfiles/delete microsoft.directory/pendingExternalUserProfiles/standard/read microsoft.directory/permissionGrantPolicies/standard/read microsoft.office365.network/performance/allProperties/read microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.skypeForBusiness/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.usageReports/allEntities/allProperties/read microsoft.office365.webPortal/allEntities/standard/read microsoft.teams/allEntities/allProperties/allTasks

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Teams Communications Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can manage calling and meetings features within the Microsoft Teams service.
Identifier	baf37b3a-610e-45da-9e62-d9d1e5e8914b
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	baf37b3a-610e-45da-9e62-d9d1e5e8914b
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.directory/authorizationPolicy/standard/read microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.skypeForBusiness/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.usageReports/allEntities/allProperties/read microsoft.office365.webPortal/allEntities/standard/read microsoft.teams/callQuality/allProperties/read microsoft.teams/meetings/allProperties/allTasks microsoft.teams/voice/allProperties/allTasks

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Teams Communications Support Engineer

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can troubleshoot communications issues within Teams using advanced tools.
Identifier	f70938a0-fc10-4177-9e90-2178f8765737
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	f70938a0-fc10-4177-9e90-2178f8765737
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.directory/authorizationPolicy/standard/read microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.skypeForBusiness/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read microsoft.teams/callQuality/allProperties/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Teams Communications Support Specialist

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can troubleshoot communications issues within Teams using basic tools.
Identifier	fcf91098-03e3-41a9-b5ba-6f0ec8188a12
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	fcf91098-03e3-41a9-b5ba-6f0ec8188a12
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.directory/authorizationPolicy/standard/read microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.skypeForBusiness/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read microsoft.teams/callQuality/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Teams Devices Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can perform management related tasks on Teams certified devices.
Identifier	3d762c5a-1b6c-493f-843e-55a3b42923d4
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	3d762c5a-1b6c-493f-843e-55a3b42923d4
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.office365.webPortal/allEntities/standard/read microsoft.teams/devices/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Teams External Collaboration Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Manage external collaboration policies and settings for Teams, including configuring external domains and controlling which groups and users can interact with the organization.
Identifier	2fe872fb-daa8-4afc-8f6c-53c4565cfef4
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	2fe872fb-daa8-4afc-8f6c-53c4565cfef4
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.supportTickets/allEntities/allTasks microsoft.directory/authorizationPolicy/standard/read microsoft.office365.webPortal/allEntities/standard/read microsoft.teams/policies/externalAccessPolicy/allTasks

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Teams Reader

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Read everything in the Teams admin center, but not update anything.
Identifier	1076ac91-f3d9-41a7-a339-dcdf5f480acc
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	1076ac91-f3d9-41a7-a339-dcdf5f480acc
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.office365.webPortal/allEntities/standard/read microsoft.teams/allEntities/allProperties/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Teams Telephony Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Manage voice and telephony features and troubleshoot communication issues within the Microsoft Teams service.
Identifier	aa38014f-0993-46e9-9b45-30501a20909d
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	aa38014f-0993-46e9-9b45-30501a20909d
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.directory/authorizationPolicy/standard/read microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.skypeForBusiness/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.usageReports/allEntities/allProperties/read microsoft.office365.webPortal/allEntities/standard/read microsoft.teams/callQuality/allProperties/read microsoft.teams/voice/allProperties/allTasks

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Tenant Creator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Create new Microsoft Entra or Azure AD B2C tenants.
Identifier	112ca1a2-15ad-4102-995e-45b0bc479a6a
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	112ca1a2-15ad-4102-995e-45b0bc479a6a
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/tenantManagement/tenants/create

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Tenant Governance Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Manage all capabilities in the Microsoft Entra Tenant Governance service.
Identifier	1981f584-96e9-4a6f-95b0-f522373f8fae
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	1981f584-96e9-4a6f-95b0-f522373f8fae
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/crossTenantAccessPolicy/basic/update microsoft.directory/crossTenantAccessPolicy/default/standard/read microsoft.directory/crossTenantAccessPolicy/partners/create microsoft.directory/crossTenantAccessPolicy/partners/delete microsoft.directory/crossTenantAccessPolicy/partners/standard/read microsoft.directory/crossTenantAccessPolicy/standard/read microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Tenant Governance Reader

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can read all tenant governance data.
Identifier	e0a4caa6-fe82-443f-b92f-d87341d17b2e
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	e0a4caa6-fe82-443f-b92f-d87341d17b2e
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Tenant Governance Relationship Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can initiate governance relationships and terminate them.
Identifier	b8e31d83-1534-480f-9b10-0338ded51b7e
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	b8e31d83-1534-480f-9b10-0338ded51b7e
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Tenant Governance Relationship Reader

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can read tenant governance relationships and relevant objects.
Identifier	124577f8-48ed-456a-839f-13b419002e33
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	124577f8-48ed-456a-839f-13b419002e33
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Usage Summary Reports Reader

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can see only tenant level aggregates in Microsoft 365 Usage Analytics and Productivity Score.
Identifier	75934031-6c7e-415a-99d7-48dbd49e875e
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	75934031-6c7e-415a-99d7-48dbd49e875e
Version	1

Inheritance

Inherited Roles	

Allowed Permissions

Allowed Permissions	microsoft.office365.network/performance/allProperties/read microsoft.office365.usageReports/allEntities/standard/read microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

User Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can manage all aspects of users and groups, including resetting passwords for limited admins.
Identifier	fe930be7-5e62-47db-91af-98c3a49a38b1
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	fe930be7-5e62-47db-91af-98c3a49a38b1
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.directory/accessReviews/definitions.applications/allProperties/allTasks microsoft.directory/accessReviews/definitions.directoryRoles/allProperties/read microsoft.directory/accessReviews/definitions.entitlementManagement/allProperties/allTasks microsoft.directory/accessReviews/definitions.groups/allProperties/read microsoft.directory/accessReviews/definitions.groups/allProperties/update microsoft.directory/accessReviews/definitions.groups/create microsoft.directory/accessReviews/definitions.groups/delete microsoft.directory/contacts/basic/update microsoft.directory/contacts/create microsoft.directory/contacts/delete microsoft.directory/deletedItems.groups/restore microsoft.directory/deletedItems.users/restore microsoft.directory/entitlementManagement/allProperties/allTasks microsoft.directory/groups.unified/assignedLabels/update microsoft.directory/groups/assignLicense microsoft.directory/groups/basic/update microsoft.directory/groups/classification/update microsoft.directory/groups/create microsoft.directory/groups/delete microsoft.directory/groups/dynamicMembershipRule/update microsoft.directory/groups/groupType/update microsoft.directory/groups/hiddenMembers/read microsoft.directory/groups/members/update microsoft.directory/groups/onPremWriteBack/update microsoft.directory/groups/owners/update microsoft.directory/groups/reprocessLicenseAssignment microsoft.directory/groups/restore microsoft.directory/groups/settings/update microsoft.directory/groups/visibility/update microsoft.directory/oAuth2PermissionGrants/allProperties/allTasks microsoft.directory/onPremisesSynchronization/standard/read microsoft.directory/policies/standard/read microsoft.directory/servicePrincipals/appRoleAssignedTo/update microsoft.directory/users/assignLicense microsoft.directory/users/basic/update microsoft.directory/users/convertExternalToInternalMemberUser microsoft.directory/users/create microsoft.directory/users/delete microsoft.directory/users/disable microsoft.directory/users/enable microsoft.directory/users/invalidateAllRefreshTokens microsoft.directory/users/inviteGuest microsoft.directory/users/lifeCycleInfo/read microsoft.directory/users/manager/update microsoft.directory/users/password/update microsoft.directory/users/photo/update microsoft.directory/users/reprocessLicenseAssignment microsoft.directory/users/restore microsoft.directory/users/sponsors/update microsoft.directory/users/usageLocation/update microsoft.directory/users/userPrincipalName/update microsoft.office365.serviceHealth/allEntities/allTasks

	microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	Azure MFA
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

User Experience Success Manager

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	View product feedback, survey results, and reports to find training and communication opportunities.
Identifier	27460883-1df1-4691-b032-3b79643e5e63
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	27460883-1df1-4691-b032-3b79643e5e63
Version	1

Inheritance

Inherited Roles	

Allowed Permissions

Allowed Permissions	microsoft.commerce.billing/purchases/standard/read microsoft.office365.messageCenter/messages/read microsoft.office365.network/performance/allProperties/read microsoft.office365.organizationalMessages/allEntities/allProperties/read microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.usageReports/allEntities/standard/read microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Virtual Visits Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Manage and share Virtual Visits information and metrics from admin centers or the Virtual Visits app.
Identifier	e300d9e7-4a2b-4295-9eff-f1c78b36cc98
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	e300d9e7-4a2b-4295-9eff-f1c78b36cc98
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.office365.webPortal/allEntities/standard/read microsoft.virtualVisits/allEntities/allProperties/allTasks

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Viva Glint Tenant Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Manage and configure Microsoft Viva Glint settings in the Microsoft 365 admin center.
Identifier	0ec3f692-38d6-4d14-9e69-0377ca7797ad
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	0ec3f692-38d6-4d14-9e69-0377ca7797ad
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.serviceHealth/allEntities/allTasks microsoft.azure.supportTickets/allEntities/allTasks microsoft.office365.messageCenter/messages/read microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.usageReports/allEntities/allProperties/read microsoft.office365.webPortal/allEntities/standard/read microsoft.viva.glint/allEntities/allProperties/allTasks

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Viva Goals Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Manage and configure all aspects of Microsoft Viva Goals.
Identifier	92b086b3-e367-4ef2-b869-1de128fb986e
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	92b086b3-e367-4ef2-b869-1de128fb986e
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.webPortal/allEntities/standard/read microsoft.viva.goals/allEntities/allProperties/allTasks

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Viva Pulse Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can manage all settings for Microsoft Viva Pulse app.
Identifier	87761b17-1ed2-4af3-9acd-92a150038160
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	87761b17-1ed2-4af3-9acd-92a150038160
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.office365.messageCenter/messages/read microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.usageReports/allEntities/allProperties/read microsoft.office365.webPortal/allEntities/standard/read microsoft.viva.pulse/allEntities/allProperties/allTasks

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Windows 365 Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can provision and manage all aspects of Cloud PCs.
Identifier	11451d60-acb2-45eb-a7d6-43d0f0125c13
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	11451d60-acb2-45eb-a7d6-43d0f0125c13
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.azure.supportTickets/allEntities/allTasks microsoft.cloudPC/allEntities/allProperties/allTasks microsoft.directory/deletedItems.devices/delete microsoft.directory/deletedItems.devices/restore microsoft.directory/deviceManagementPolicies/standard/read microsoft.directory/deviceRegistrationPolicy/standard/read microsoft.directory/devices/basic/update microsoft.directory/devices/create microsoft.directory/devices/delete microsoft.directory/devices/disable microsoft.directory/devices/enable microsoft.directory/devices/extensionAttributeSet1/update microsoft.directory/devices/extensionAttributeSet2/update microsoft.directory/devices/extensionAttributeSet3/update microsoft.directory/devices/registeredOwners/update microsoft.directory/devices/registeredUsers/update microsoft.directory/groups.security/assignedLabels/update microsoft.directory/groups.security/basic/update microsoft.directory/groups.security/classification/update microsoft.directory/groups.security/create microsoft.directory/groups.security/delete microsoft.directory/groups.security/dynamicMembershipRule/update microsoft.directory/groups.security/members/update microsoft.directory/groups.security/owners/update microsoft.directory/groups.security/visibility/update microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.usageReports/allEntities/allProperties/read microsoft.office365.webPortal/allEntities/standard/read

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Windows Update Deployment Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Can create and manage all aspects of Windows Update deployments through the Windows Update for Business deployment service.
Identifier	32696413-001a-46ae-978c-ce0f6b3620d2
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	32696413-001a-46ae-978c-ce0f6b3620d2
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.windows.updatesDeployments/allEntities/allProperties/allTasks

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Workplace Device Join

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Deprecated - Do Not Use.
Identifier	c34f683f-4d5a-4403-affd-6615e00e3a7f
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	c34f683f-4d5a-4403-affd-6615e00e3a7f
Version	1

Inheritance

Inherited Roles	

Allowed Permissions

Allowed Permissions	

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Yammer Administrator

Users are assigned to Entra roles to give them the permissions required to manage specific resources - for example, adding or modifying users, resetting passwords, or managing domain names.

General

Description	Manage all aspects of the Yammer service.
Identifier	810a2642-a034-447f-a5e8-41beaa378541
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	810a2642-a034-447f-a5e8-41beaa378541
Version	1

Inheritance

Inherited Roles	Directory Readers

Allowed Permissions

Allowed Permissions	microsoft.directory/groups.unified/assignedLabels/update microsoft.directory/groups.unified/basic/update microsoft.directory/groups.unified/create microsoft.directory/groups.unified/delete microsoft.directory/groups.unified/members/update microsoft.directory/groups.unified/owners/update microsoft.directory/groups.unified/restore microsoft.directory/groups/hiddenMembers/read microsoft.office365.messageCenter/messages/read microsoft.office365.network/performance/allProperties/read microsoft.office365.serviceHealth/allEntities/allTasks microsoft.office365.supportTickets/allEntities/allTasks microsoft.office365.usageReports/allEntities/allProperties/read microsoft.office365.webPortal/allEntities/standard/read microsoft.office365.yammer/allEntities/allProperties/allTasks

Excluded Permissions

Excluded Permissions	

0 Role Assignments

There are no role assignments found.

0 Role Eligible Assignments

There are no role eligible assignments found.

PIM Settings

Privileged Identity Management (PIM) settings for a role define the guardrails that govern how a user can activate and operate that role in Entra ID.

Activation

Activation Maximum Duration	8 hours
Activation Requirement Type	None
Require Justification	True
Require Ticket Information	False
Approval Required	False

Activation

Eligible Assignments Expiry	Permanent
Active Assignments Expiry	Permanent
Require Azure Multi-Factor Authentication On Active Assignment	False
Require Justification On Active Assignment	True

Send notifications when: Eligible members activate the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as active to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

Send notifications when: Members are assigned as eligible to the role

Type	Include Default Recipients	Additional Recipients	Level
Notification to the assigned user (assignee)	True		All
Request to approve a role assignment renewal/extension	True		All
Role assignment alert	True		All

About XIA Configuration

XIA Configuration is an IT infrastructure audit and documentation tool that automates the process of collecting and documenting network configurations.