

Entra Directory Documentation

centrelsolutionsdemo.onmicrosoft.com

Company Confidential

Document Properties

Author	CSDemo\Administrator
Product	XIA Configuration Express [18.1.6.0]
Date	22 September 2026 10:28:42
Version	1.00



Table of Contents

General Information.....	3
Organization.....	4
Applications.....	5
Applications - C.....	6
centrelsolutionsdemo.int.....	7
API.....	8
App Roles.....	9
Authentication.....	10
Credentials.....	11
Federated Credentials.....	12
Optional Claims.....	13
centrelsolutionsdemo.int.....	14
API.....	15
App Roles.....	16
Authentication.....	17
Credentials.....	18
Federated Credentials.....	19
Optional Claims.....	20
Applications - E.....	21
emea.centrelsolutionsdemo.int.....	22
API.....	23
App Roles.....	24
Authentication.....	25
Credentials.....	26
Federated Credentials.....	27
Optional Claims.....	28
emea.centrelsolutionsdemo.int.....	29
API.....	30
App Roles.....	31
Authentication.....	32
Credentials.....	33
Federated Credentials.....	34
Optional Claims.....	35
ExchangeServerApp-1594abbd-9de4-4330-b1c7-fcf0036c8e6d.....	36
API.....	37
App Roles.....	38
Authentication.....	39
Credentials.....	40
Federated Credentials.....	41

Optional Claims.....	42
Applications - G.....	43
GSA-Internettrafficforwardingprofile.....	44
API.....	45
App Roles.....	46
Authentication.....	47
Credentials.....	48
Federated Credentials.....	49
Optional Claims.....	50
GSA-Microsoft365trafficforwardingprofile.....	51
API.....	52
App Roles.....	53
Authentication.....	54
Credentials.....	55
Federated Credentials.....	56
Optional Claims.....	57
GSA-Privateaccesstrafficforwardingprofile.....	58
API.....	59
App Roles.....	60
Authentication.....	61
Credentials.....	62
Federated Credentials.....	63
Optional Claims.....	64
Applications - T.....	65
Test Evaluation Agent (Microsoft Copilot Studio).....	66
Authentication.....	68
Federated Credentials.....	69
Optional Claims.....	70
Applications - X.....	71
XIA Configuration Client.....	72
API.....	73
App Roles.....	74
Authentication.....	75
Credentials.....	76
Federated Credentials.....	77
Optional Claims.....	78
XIA Configuration Client (SQL Server).....	79
API.....	80
App Roles.....	81
Authentication.....	82
Credentials.....	83
Federated Credentials.....	84

Optional Claims.....	85
Branding.....	86
Localizations.....	87
Conditional Access.....	88
Authentication Contexts.....	89
Authentication Strengths.....	90
Multifactor authentication.....	91
Passwordless MFA.....	92
Phishing-resistant MFA.....	93
Sample Authentication Strength.....	94
Policies.....	95
Agents Policy.....	96
Assignments.....	97
Conditions.....	98
Grant Controls.....	99
Session Controls.....	100
Continuous Access Evaluation Policy.....	101
Assignments.....	102
Conditions.....	103
Grant Controls.....	104
Session Controls.....	105
Global Secure Access Policy.....	106
Assignments.....	107
Conditions.....	108
Grant Controls.....	109
Session Controls.....	110
Sample Policy 1.....	111
Assignments.....	112
Conditions.....	113
Grant Controls.....	114
Session Controls.....	115
Sample Policy 2.....	116
Assignments.....	117
Conditions.....	118
Grant Controls.....	120
Session Controls.....	121
Workloads Policy.....	122
Assignments.....	123
Conditions.....	124
Grant Controls.....	125
Session Controls.....	126
Named Locations.....	127

Sample IP Location.....	128
Sample IP Location.....	129
Terms Of Use.....	130
Sample terms of use.....	131
Enterprise Applications.....	132
Enterprise Applications - E.....	134
ExchangeServerApp-1594abbd-9de4-4330-b1c7-fcf0036c8e6d.....	135
Admin Consented Permissions.....	136
App Roles.....	137
App Role Assignments.....	138
Enterprise Applications - G.....	139
Graph Explorer.....	140
Admin Consented Permissions.....	141
App Roles.....	142
App Role Assignments.....	143
Enterprise Applications - M.....	144
Microsoft Graph Command Line Tools.....	145
Admin Consented Permissions.....	146
App Roles.....	147
App Role Assignments.....	148
Enterprise Applications - X.....	149
XIA Configuration Client.....	150
Admin Consented Permissions.....	151
App Roles.....	152
App Role Assignments.....	153
XIA Configuration Client (SQL Server).....	154
Admin Consented Permissions.....	155
App Roles.....	156
App Role Assignments.....	157
XIA Configuration Express.....	158
Admin Consented Permissions.....	159
App Roles.....	160
App Role Assignments.....	161
XIA Configuration Express Management API.....	162
Admin Consented Permissions.....	163
App Roles.....	164
App Role Assignments.....	165
XIA Configuration Tools.....	166
Admin Consented Permissions.....	167
App Roles.....	168
App Role Assignments.....	169
Entra Connect.....	170

Cloud Sync.....	171
Agents.....	172
Configurations.....	173
centrelsolutionsdemo.int (AD to Microsoft Entra ID).....	174
Scoping Filters.....	175
Object Mappings.....	176
contact.....	177
group.....	183
inetOrgPerson.....	188
user.....	196
emea.centrelsolutionsdemo.int (AD to Microsoft Entra ID).....	204
Scoping Filters.....	205
Object Mappings.....	206
contact.....	207
group.....	213
inetOrgPerson.....	218
user.....	226
centrelsolutionsdemo.int (Microsoft Entra ID to AD).....	234
Scoping Filters.....	235
Object Mappings.....	236
Group.....	237
User.....	239
emea.centrelsolutionsdemo.int (Microsoft Entra ID to AD).....	241
Scoping Filters.....	242
Object Mappings.....	243
Group.....	244
User.....	246
Groups.....	248
Groups - A.....	250
All Company.....	251
All Company.....	252
All Users.....	253
Groups - C.....	254
Compliance Management.....	255
Groups - D.....	256
Demonstration Distribution Group.....	257
Demonstration Security Group.....	258
Demonstration Security Group.....	259
Deprecated - All Company.....	260
DnsAdmins.....	261
DnsAdmins.....	262
DnsUpdateProxy.....	263

DnsUpdateProxy.....	264
Groups - E.....	265
EntralLicenseGroup.....	266
Exchange Install Domain Servers.....	267
Exchange Servers.....	268
Exchange Trusted Subsystem.....	269
Exchange Windows Permissions.....	270
ExchangeLegacyInterop.....	271
Groups - G.....	272
Group for Answers in Viva Engage – DO NOT DELETE 59131330561.....	273
Group for Answers in Viva Engage – DO NOT DELETE 63717335041.....	274
Groups - H.....	275
Help Desk.....	276
Groups - I.....	277
IT.....	278
IT Management.....	279
Groups - M.....	280
Managed Availability Servers.....	281
Groups - S.....	282
SQL Administrators.....	283
Groups - T.....	284
TestSite.....	285
Groups - W.....	286
Windows Admin Center CredSSP.....	287
Licenses.....	288
Microsoft 365 Business Premium.....	289
Microsoft Copilot Studio Viral Trial.....	293
Microsoft Entra ID P2.....	294
Microsoft Power Automate Free.....	295
Roles.....	296
Agent ID Administrator.....	301
PIM Settings.....	304
Agent ID Developer.....	306
PIM Settings.....	307
Agent Registry Administrator.....	309
PIM Settings.....	310
AI Administrator.....	312
PIM Settings.....	315
AI Reader.....	317
PIM Settings.....	320
Application Administrator.....	322
PIM Settings.....	325

Application Developer.....	327
PIM Settings.....	328
Attack Payload Author.....	330
PIM Settings.....	331
Attack Simulation Administrator.....	333
PIM Settings.....	334
Attribute Assignment Administrator.....	336
PIM Settings.....	338
Attribute Assignment Reader.....	340
PIM Settings.....	341
Attribute Definition Administrator.....	343
PIM Settings.....	344
Attribute Definition Reader.....	346
PIM Settings.....	347
Attribute Log Administrator.....	349
PIM Settings.....	350
Attribute Log Reader.....	352
PIM Settings.....	353
Attribute Provisioning Administrator.....	355
PIM Settings.....	356
Attribute Provisioning Reader.....	358
PIM Settings.....	359
Authentication Administrator.....	361
PIM Settings.....	363
Authentication Extensibility Administrator.....	365
PIM Settings.....	366
Authentication Extensibility Password Administrator.....	368
PIM Settings.....	369
Authentication Policy Administrator.....	371
PIM Settings.....	373
Azure AD Joined Device Local Administrator.....	375
PIM Settings.....	376
Azure DevOps Administrator.....	378
PIM Settings.....	379
Azure Information Protection Administrator.....	381
PIM Settings.....	382
B2C IEF Keyset Administrator.....	384
PIM Settings.....	385
B2C IEF Policy Administrator.....	387
PIM Settings.....	388
Billing Administrator.....	390
PIM Settings.....	391

Cloud App Security Administrator.....	393
PIM Settings.....	394
Cloud Application Administrator.....	396
PIM Settings.....	399
Cloud Device Administrator.....	401
PIM Settings.....	403
Compliance Administrator.....	405
PIM Settings.....	406
Compliance Data Administrator.....	408
PIM Settings.....	410
Conditional Access Administrator.....	412
PIM Settings.....	414
Customer Delegated Admin Relationship Administrator.....	416
PIM Settings.....	417
Customer LockBox Access Approver.....	419
PIM Settings.....	420
Desktop Analytics Administrator.....	422
PIM Settings.....	423
Device Join.....	425
PIM Settings.....	426
Device Managers.....	428
PIM Settings.....	430
Device Users.....	432
PIM Settings.....	433
Directory Readers.....	435
PIM Settings.....	438
Directory Synchronization Accounts.....	440
PIM Settings.....	441
Directory Writers.....	443
PIM Settings.....	446
Domain Name Administrator.....	448
PIM Settings.....	449
Dragon Administrator.....	451
PIM Settings.....	453
Dynamics 365 Administrator.....	455
PIM Settings.....	456
Dynamics 365 Business Central Administrator.....	458
PIM Settings.....	460
Edge Administrator.....	462
PIM Settings.....	463
Entra Backup Administrator.....	465
PIM Settings.....	466

Entra Backup Reader.....	468
PIM Settings.....	469
Entra Customer Lockbox Approver.....	471
PIM Settings.....	472
Entra SOC Identity Responder.....	474
PIM Settings.....	475
Exchange Administrator.....	477
PIM Settings.....	479
Exchange Backup Administrator.....	481
PIM Settings.....	483
Exchange Recipient Administrator.....	485
PIM Settings.....	486
Extended Directory User Administrator.....	488
PIM Settings.....	489
External ID User Flow Administrator.....	491
PIM Settings.....	492
External ID User Flow Attribute Administrator.....	494
PIM Settings.....	495
External Identity Provider Administrator.....	497
PIM Settings.....	498
Fabric Administrator.....	500
PIM Settings.....	501
Global Administrator.....	503
PIM Settings.....	510
Global Reader.....	512
PIM Settings.....	516
Global Secure Access Administrator.....	518
PIM Settings.....	520
Global Secure Access Log Reader.....	522
PIM Settings.....	523
Groups Administrator.....	525
PIM Settings.....	527
Guest Inviter.....	529
PIM Settings.....	531
Guest User.....	533
PIM Settings.....	535
Helpdesk Administrator.....	537
PIM Settings.....	539
Hybrid Identity Administrator.....	541
PIM Settings.....	544
Identity Governance Administrator.....	546
PIM Settings.....	548

Insights Administrator.....	550
PIM Settings.....	551
Insights Analyst.....	553
PIM Settings.....	554
Insights Business Leader.....	556
PIM Settings.....	557
Intune Administrator.....	559
PIM Settings.....	562
IoT Device Administrator.....	564
PIM Settings.....	566
Kaizala Administrator.....	568
PIM Settings.....	569
Knowledge Administrator.....	571
PIM Settings.....	573
Knowledge Manager.....	575
PIM Settings.....	577
License Administrator.....	579
PIM Settings.....	581
Lifecycle Workflows Administrator.....	583
PIM Settings.....	584
Message Center Privacy Reader.....	586
PIM Settings.....	587
Message Center Reader.....	589
PIM Settings.....	590
Microsoft 365 Backup Administrator.....	592
PIM Settings.....	594
Microsoft 365 Migration Administrator.....	596
PIM Settings.....	597
Microsoft Graph Data Connect Administrator.....	599
PIM Settings.....	600
Microsoft Hardware Warranty Administrator.....	602
PIM Settings.....	603
Microsoft Hardware Warranty Specialist.....	605
PIM Settings.....	606
Network Administrator.....	608
PIM Settings.....	609
Office Apps Administrator.....	611
PIM Settings.....	612
On Premises Directory Sync Account.....	614
PIM Settings.....	615
Organizational Branding Administrator.....	617
PIM Settings.....	618

Organizational Data Source Administrator.....	620
PIM Settings.....	621
Organizational Messages Approver.....	623
PIM Settings.....	624
Organizational Messages Writer.....	626
PIM Settings.....	627
Partner Tier1 Support.....	629
PIM Settings.....	632
Partner Tier2 Support.....	634
PIM Settings.....	637
Password Administrator.....	639
PIM Settings.....	640
People Administrator.....	642
PIM Settings.....	643
Permissions Management Administrator.....	645
PIM Settings.....	646
Places Administrator.....	648
PIM Settings.....	649
Power Platform Administrator.....	651
PIM Settings.....	653
Printer Administrator.....	655
PIM Settings.....	656
Printer Technician.....	658
PIM Settings.....	659
Privileged Authentication Administrator.....	661
PIM Settings.....	663
Privileged Role Administrator.....	665
PIM Settings.....	667
Purview Workload Content Administrator.....	669
PIM Settings.....	670
Purview Workload Content Reader.....	672
PIM Settings.....	673
Purview Workload Content Writer.....	675
PIM Settings.....	676
Reports Reader.....	678
PIM Settings.....	679
Restricted Guest User.....	681
PIM Settings.....	683
Search Administrator.....	685
PIM Settings.....	686
Search Editor.....	688
PIM Settings.....	689

Security Administrator.....	691
PIM Settings.....	694
Security Operator.....	696
PIM Settings.....	698
Security Reader.....	700
PIM Settings.....	703
Service Support Administrator.....	705
PIM Settings.....	706
SharePoint Administrator.....	708
PIM Settings.....	710
SharePoint Advanced Management Administrator.....	712
PIM Settings.....	714
SharePoint Backup Administrator.....	716
PIM Settings.....	718
SharePoint Embedded Administrator.....	720
PIM Settings.....	721
Skype for Business Administrator.....	723
PIM Settings.....	724
Teams Administrator.....	726
PIM Settings.....	729
Teams Communications Administrator.....	731
PIM Settings.....	733
Teams Communications Support Engineer.....	735
PIM Settings.....	736
Teams Communications Support Specialist.....	738
PIM Settings.....	739
Teams Devices Administrator.....	741
PIM Settings.....	742
Teams External Collaboration Administrator.....	744
PIM Settings.....	745
Teams Reader.....	747
PIM Settings.....	748
Teams Telephony Administrator.....	750
PIM Settings.....	752
Tenant Creator.....	754
PIM Settings.....	755
Tenant Governance Administrator.....	757
PIM Settings.....	759
Tenant Governance Reader.....	761
PIM Settings.....	762
Tenant Governance Relationship Administrator.....	764
PIM Settings.....	765

Tenant Governance Relationship Reader.....	767
PIM Settings.....	768
Usage Summary Reports Reader.....	770
PIM Settings.....	771
User Administrator.....	773
PIM Settings.....	776
User Experience Success Manager.....	778
PIM Settings.....	779
Virtual Visits Administrator.....	781
PIM Settings.....	782
Viva Glint Tenant Administrator.....	784
PIM Settings.....	785
Viva Goals Administrator.....	787
PIM Settings.....	788
Viva Pulse Administrator.....	790
PIM Settings.....	791
Windows 365 Administrator.....	793
PIM Settings.....	795
Windows Update Deployment Administrator.....	797
PIM Settings.....	798
Workplace Device Join.....	800
PIM Settings.....	801
Yammer Administrator.....	803
PIM Settings.....	805
Users.....	807
Users - B.....	808
Users - D.....	809
Users - F.....	810
Users - H.....	811
Users - I.....	812
Users - K.....	813
Users - O.....	814
Users - S.....	815
Users - T.....	816
Users - X.....	817



General Information

Provides general information for this item.



General Information

Name	centrelsolutionsdemo.onmicrosoft.com
Description	
Primary Owner Name	
Primary Owner Contact	

Organization

Provides information about the organization.

General

Display Name	CENTREL Solutions Demo
Identifier	157f8a9e-052c-4fc2-8b9f-11e8ccc55e96
Default Domain	centrelsolutionsdemo.onmicrosoft.com

Security Defaults

Security Defaults Enabled	True
---------------------------	------

License

License Display Name	Microsoft Entra ID P2
License Service Plan Name	AAD_PREMIUM_P2

Information

Creation Date	26 September 2023 11:10:52
Business Phone Numbers	07790248179
Preferred Language	English
Technical Contacts	demo@centrel-solutions.com

Privacy

Global Privacy Contact	privacy@centrel-solutions.com
Global Privacy Statement	

Address

Street	Innovation House
City	Oxford
State, Province, or County	Oxfordshire
ZIP or Postal Code	OX4 2JY
Country	United Kingdom

Applications

Provides information about the applications defined in the organization.

 11 Applications

First Letter	Count
 #	0
 A	0
 B	0
 C	2
 D	0
 E	3
 F	0
 G	3
 H	0
 I	0
 J	0
 K	0
 L	0
 M	0
 N	0
 O	0
 P	0
 Q	0
 R	0
 S	0
 T	1
 U	0
 V	0
 W	0
 X	2
 Y	0
 Z	0

Applications - C

Provides information about the applications defined in the organization with the specified first letter.

2 Applications

Display Name	Supported Account Types	Application Identifier
 centrelsolutionsdemo.int	Accounts in this organizational directory only (Single tenant)	5652cac8-4693-4198-a130-30be77b2c64f
 centrelsolutionsdemo.int	Accounts in this organizational directory only (Single tenant)	6a5fdb96-34f8-4070-9d29-8b23850594e9

centrelsolutionsdemo.int

Provides information about the applications defined in the organization.

General

Display Name	centrelsolutionsdemo.int
Application Identifier	5652cac8-4693-4198-a130-30be77b2c64f
Object Identifier	258d4ff9-b6c2-4ff0-a1c8-afbf9a29ec28

Properties

Homepage URL	https://account.activedirectory.windowsazure.com:444/applications/default.aspx?metadata=AD2AADProvisioning ISV9.1 primary z
Privacy Statement URL	
Terms Of Service URL	
Service Management Reference	
Notes	
Publisher Domain	centrelsolutionsdemo.onmicrosoft.com

Application Icon

The application does not have an icon assigned.

Publisher Verification

The publisher is not verified.

0 Owners

There are no owners found.

API

Provides information about the API settings for the application.

 API

Identifier URIs	
-----------------	--

 0 Permissions

There are no permissions found.

 1 Permission Scopes

Scope Name	Consent Type	Admin Consent Display Name	User Consent Display Name	Enabled
 user_impersonation	Users and Admins	Access centrelsolutionsdemo.int	Access centrelsolutionsdemo.int	True

 0 Authorized Applications

There are no authorized applications found.

App Roles

App roles in Microsoft Entra are declarative permissions defined within an application’s manifest that enable granular access control by assigning users or groups to specific roles aligned with the app’s functionality

 1 App Roles

Display Name	Allowed Member Types	Value	Enabled
 msiam_access	User		True

Authentication

Provides information about the authentication settings for the application.

 Authentication

Supported Account Types	Accounts in this organizational directory only (Single tenant)
-------------------------	--

 Public Client

Allow Public Client Flows	False
Redirect URIs	

 Single Page Application

Redirect URIs	
---------------	--

 Web

Enable Implicit Access Tokens	False
Enable Implicit ID Tokens	True
Logout URL	
Redirect URIs	

 App Instance Property Lock

App Instance Locked Properties	None
--------------------------------	------

Credentials

Provides information about the client secret and certificate credentials for the application.

 **0 Credentials**

There are no credentials found.

Federated Credentials

Microsoft Entra federated credentials let applications and services authenticate to Entra ID-protected resources without storing secrets or certificates, using trust-based identity federation instead.



0 Federated Credentials

There are no federated credentials found.

Optional Claims

Optional claims are configurable attributes that determine which pieces of user identity information are included in tokens issued to an application during authentication.

 0 Optional Claims

There are no optional claims found.

centrelsolutionsdemo.int

Provides information about the applications defined in the organization.

General

Display Name	centrelsolutionsdemo.int
Application Identifier	6a5fdb96-34f8-4070-9d29-8b23850594e9
Object Identifier	54243d76-7ecf-4ed4-86bc-10417393159d

Properties

Homepage URL	https://account.activedirectory.windowsazure.com:444/applications/default.aspx?metadata=AAD2ADProvisioning ISV9.1 primary z
Privacy Statement URL	
Terms Of Service URL	
Service Management Reference	
Notes	
Publisher Domain	centrelsolutionsdemo.onmicrosoft.com

Application Icon

The application does not have an icon assigned.

Publisher Verification

The publisher is not verified.

0 Owners

There are no owners found.

API

Provides information about the API settings for the application.

 API

Identifier URIs	
-----------------	--

 0 Permissions

There are no permissions found.

 1 Permission Scopes

Scope Name	Consent Type	Admin Consent Display Name	User Consent Display Name	Enabled
 user_impersonation	Users and Admins	Access centrelsolutionsdemo.int	Access centrelsolutionsdemo.int	True

 0 Authorized Applications

There are no authorized applications found.

App Roles

App roles in Microsoft Entra are declarative permissions defined within an application’s manifest that enable granular access control by assigning users or groups to specific roles aligned with the app’s functionality

 1 App Roles

Display Name	Allowed Member Types	Value	Enabled
 msiam_access	User		True

Authentication

Provides information about the authentication settings for the application.

 Authentication

Supported Account Types	Accounts in this organizational directory only (Single tenant)
-------------------------	--

 Public Client

Allow Public Client Flows	False
Redirect URIs	

 Single Page Application

Redirect URIs	
---------------	--

 Web

Enable Implicit Access Tokens	False
Enable Implicit ID Tokens	True
Logout URL	
Redirect URIs	

 App Instance Property Lock

App Instance Locked Properties	None
--------------------------------	------

Credentials

Provides information about the client secret and certificate credentials for the application.

 **0 Credentials**

There are no credentials found.

Federated Credentials

Microsoft Entra federated credentials let applications and services authenticate to Entra ID-protected resources without storing secrets or certificates, using trust-based identity federation instead.



0 Federated Credentials

There are no federated credentials found.

Optional Claims

Optional claims are configurable attributes that determine which pieces of user identity information are included in tokens issued to an application during authentication.

 0 Optional Claims

There are no optional claims found.

Applications - E

Provides information about the applications defined in the organization with the specified first letter.

3 Applications

Display Name	Supported Account Types	Application Identifier
 emea.centrelsolutionsdemo.int	Accounts in this organizational directory only (Single tenant)	b884cebb-d4b2-4d46-b106-51c7e2305170
 emea.centrelsolutionsdemo.int	Accounts in this organizational directory only (Single tenant)	c8ff2fd1-e2bc-4eaf-8035-2e6d207f685b
 ExchangeServerApp-1594abbd-9de4-4330-b1c7-fcf0036c8e6d	Accounts in this organizational directory only (Single tenant)	61021fe7-7182-4481-b08a-f21c6665ece4

emea.centrelsolutionsdemo.int

Provides information about the applications defined in the organization.

General

Display Name	emea.centrelsolutionsdemo.int
Application Identifier	b884cebb-d4b2-4d46-b106-51c7e2305170
Object Identifier	0d82636e-0539-4fb2-be71-28c6c58a4d1a

Properties

Homepage URL	https://account.activedirectory.windowsazure.com:444/applications/default.aspx?metadata=AAD2ADP rovisioning ISV9.1 primary z
Privacy Statement URL	
Terms Of Service URL	
Service Management Reference	
Notes	
Publisher Domain	centrelsolutionsdemo.onmicrosoft.com

Application Icon

The application does not have an icon assigned.

Publisher Verification

The publisher is not verified.

0 Owners

There are no owners found.

API

Provides information about the API settings for the application.

 API

Identifier URIs	
-----------------	--

 0 Permissions

There are no permissions found.

 1 Permission Scopes

Scope Name	Consent Type	Admin Consent Display Name	User Consent Display Name	Enabled
 user_impersonation	Users and Admins	Access emea.centrelsolutionsdemo.int	Access emea.centrelsolutionsdemo.int	True

 0 Authorized Applications

There are no authorized applications found.

App Roles

App roles in Microsoft Entra are declarative permissions defined within an application’s manifest that enable granular access control by assigning users or groups to specific roles aligned with the app’s functionality

 1 App Roles

Display Name	Allowed Member Types	Value	Enabled
 msiam_access	User		True

Authentication

Provides information about the authentication settings for the application.

 Authentication

Supported Account Types	Accounts in this organizational directory only (Single tenant)
-------------------------	--

 Public Client

Allow Public Client Flows	False
Redirect URIs	

 Single Page Application

Redirect URIs	
---------------	--

 Web

Enable Implicit Access Tokens	False
Enable Implicit ID Tokens	True
Logout URL	
Redirect URIs	

 App Instance Property Lock

App Instance Locked Properties	None
--------------------------------	------

Credentials

Provides information about the client secret and certificate credentials for the application.

 **0 Credentials**

There are no credentials found.

Federated Credentials

Microsoft Entra federated credentials let applications and services authenticate to Entra ID-protected resources without storing secrets or certificates, using trust-based identity federation instead.



0 Federated Credentials

There are no federated credentials found.

Optional Claims

Optional claims are configurable attributes that determine which pieces of user identity information are included in tokens issued to an application during authentication.

 0 Optional Claims

There are no optional claims found.

emea.centrelsolutionsdemo.int

Provides information about the applications defined in the organization.

General

Display Name	emea.centrelsolutionsdemo.int
Application Identifier	c8ff2fd1-e2bc-4eaf-8035-2e6d207f685b
Object Identifier	442d6441-031d-4327-bb91-898daae18a1c

Properties

Homepage URL	https://account.activedirectory.windowsazure.com:444/applications/default.aspx?metadata=AD2AADProvisioning ISV9.1 primary z
Privacy Statement URL	
Terms Of Service URL	
Service Management Reference	
Notes	
Publisher Domain	centrelsolutionsdemo.onmicrosoft.com

Application Icon

The application does not have an icon assigned.

Publisher Verification

The publisher is not verified.

0 Owners

There are no owners found.

API

Provides information about the API settings for the application.

 API

Identifier URIs	
-----------------	--

 0 Permissions

There are no permissions found.

 1 Permission Scopes

Scope Name	Consent Type	Admin Consent Display Name	User Consent Display Name	Enabled
 user_impersonation	Users and Admins	Access emea.centrelsolutionsdemo.int	Access emea.centrelsolutionsdemo.int	True

 0 Authorized Applications

There are no authorized applications found.

App Roles

App roles in Microsoft Entra are declarative permissions defined within an application’s manifest that enable granular access control by assigning users or groups to specific roles aligned with the app’s functionality

 1 App Roles

Display Name	Allowed Member Types	Value	Enabled
 msiam_access	User		True

Authentication

Provides information about the authentication settings for the application.



Authentication

Supported Account Types	Accounts in this organizational directory only (Single tenant)
-------------------------	--



Public Client

Allow Public Client Flows	False
Redirect URIs	



Single Page Application

Redirect URIs	
---------------	--



Web

Enable Implicit Access Tokens	False
Enable Implicit ID Tokens	True
Logout URL	
Redirect URIs	



App Instance Property Lock

App Instance Locked Properties	None
--------------------------------	------

Credentials

Provides information about the client secret and certificate credentials for the application.

 **0 Credentials**

There are no credentials found.

Federated Credentials

Microsoft Entra federated credentials let applications and services authenticate to Entra ID-protected resources without storing secrets or certificates, using trust-based identity federation instead.



0 Federated Credentials

There are no federated credentials found.

Optional Claims

Optional claims are configurable attributes that determine which pieces of user identity information are included in tokens issued to an application during authentication.

 0 Optional Claims

There are no optional claims found.

ExchangeServerApp-1594abbd-9de4-4330-b1c7-fcf0036c8e6d

Provides information about the applications defined in the organization.

 General

Display Name	ExchangeServerApp-1594abbd-9de4-4330-b1c7-fcf0036c8e6d
Application Identifier	61021fe7-7182-4481-b08a-f21c6665ece4
Object Identifier	707b2fd3-2338-47b8-95ac-19e71867ca6b

 Properties

Homepage URL	
Privacy Statement URL	
Terms Of Service URL	
Service Management Reference	
Notes	Used by Exchange Server as part of the hybrid configuration to enable hybrid features such as Free/Busy, MailTips, and Profile Picture sharing between Exchange Server and Exchange Online.
Publisher Domain	centrelsolutionsdemo.onmicrosoft.com

 Application Icon



 Publisher Verification

The publisher is not verified.

 0 Owners

There are no owners found.

API

Provides information about the API settings for the application.

 API

Identifier URIs	
-----------------	--

 1 Permissions

Application	Permission	Type	Admin Consent Required	Admin Consent Granted
 Office 365 Exchange Online	full_access_as_app	Application	True	False

 0 Permission Scopes

There are no permission scopes found.

 0 Authorized Applications

There are no authorized applications found.

App Roles

App roles in Microsoft Entra are declarative permissions defined within an application’s manifest that enable granular access control by assigning users or groups to specific roles aligned with the app’s functionality

 **0 App Roles**

There are no app roles found.

Authentication

Provides information about the authentication settings for the application.

 Authentication

Supported Account Types	Accounts in this organizational directory only (Single tenant)
-------------------------	--

 Public Client

Allow Public Client Flows	False
Redirect URIs	

 Single Page Application

Redirect URIs	
---------------	--

 Web

Enable Implicit Access Tokens	False
Enable Implicit ID Tokens	False
Logout URL	
Redirect URIs	

 App Instance Property Lock

App Instance Locked Properties	All Properties
--------------------------------	----------------

Credentials

Provides information about the client secret and certificate credentials for the application.

 1 Credentials

Display Name	Credential Type	Identifier	Expiry
 CN=Microsoft Exchange Server Auth Certificate	Certificate	0192A56734299566BBA3A1FD9AD5928B611100D2	25 March 2031

Federated Credentials

Microsoft Entra federated credentials let applications and services authenticate to Entra ID-protected resources without storing secrets or certificates, using trust-based identity federation instead.



0 Federated Credentials

There are no federated credentials found.

Optional Claims

Optional claims are configurable attributes that determine which pieces of user identity information are included in tokens issued to an application during authentication.

 0 Optional Claims

There are no optional claims found.

Applications - G

Provides information about the applications defined in the organization with the specified first letter.

3 Applications

Display Name	Supported Account Types	Application Identifier
 GSA-Internettrafficforwardingprofile	Accounts in this organizational directory only (Single tenant)	517c694f-9e6d-4ee9-8ac0-0356d50ccfc5
 GSA-Microsoft365trafficforwardingprofile	Accounts in this organizational directory only (Single tenant)	885e13ed-b9cb-4ff5-90a7-40bae50e009e
 GSA-Privateaccesstrafficforwardingprofile	Accounts in this organizational directory only (Single tenant)	a97a17b2-eec8-4edf-b13f-1c9b0d33e40a

GSA-Internettrafficforwardingprofile

Provides information about the applications defined in the organization.

General

Display Name	GSA-Internettrafficforwardingprofile
Application Identifier	517c694f-9e6d-4ee9-8ac0-0356d50ccfc5
Object Identifier	6e45b164-e108-433a-bdfc-be72cb71fdb7

Properties

Homepage URL	
Privacy Statement URL	
Terms Of Service URL	
Service Management Reference	
Notes	
Publisher Domain	centrelsolutionsdemo.onmicrosoft.com

Application Icon

The application does not have an icon assigned.

Publisher Verification

The publisher is not verified.

1 Owners

Display Name	Identity	Type
 ZTNA Network Access Control Plane		Service Principal

API

Provides information about the API settings for the application.

 API

Identifier URIs	
-----------------	--

 0 Permissions

There are no permissions found.

 0 Permission Scopes

There are no permission scopes found.

 0 Authorized Applications

There are no authorized applications found.

App Roles

App roles in Microsoft Entra are declarative permissions defined within an application’s manifest that enable granular access control by assigning users or groups to specific roles aligned with the app’s functionality

 **0 App Roles**

There are no app roles found.

Authentication

Provides information about the authentication settings for the application.

 Authentication

Supported Account Types	Accounts in this organizational directory only (Single tenant)
-------------------------	--

 Public Client

Allow Public Client Flows	False
Redirect URIs	

 Single Page Application

Redirect URIs	
---------------	--

 Web

Enable Implicit Access Tokens	False
Enable Implicit ID Tokens	False
Logout URL	
Redirect URIs	

 App Instance Property Lock

App Instance Locked Properties	None
--------------------------------	------

Credentials

Provides information about the client secret and certificate credentials for the application.

 **0 Credentials**

There are no credentials found.

Federated Credentials

Microsoft Entra federated credentials let applications and services authenticate to Entra ID-protected resources without storing secrets or certificates, using trust-based identity federation instead.



0 Federated Credentials

There are no federated credentials found.

Optional Claims

Optional claims are configurable attributes that determine which pieces of user identity information are included in tokens issued to an application during authentication.

 0 Optional Claims

There are no optional claims found.

GSA-Microsoft365trafficforwardingprofile

Provides information about the applications defined in the organization.

General

Display Name	GSA-Microsoft365trafficforwardingprofile
Application Identifier	885e13ed-b9cb-4ff5-90a7-40bae50e009e
Object Identifier	0699e1ee-07cc-46d6-81fd-5cd6e7b1b685

Properties

Homepage URL	
Privacy Statement URL	
Terms Of Service URL	
Service Management Reference	
Notes	
Publisher Domain	centrelsolutionsdemo.onmicrosoft.com

Application Icon

The application does not have an icon assigned.

Publisher Verification

The publisher is not verified.

1 Owners

Display Name	Identity	Type
 ZTNA Network Access Control Plane		Service Principal

API

Provides information about the API settings for the application.

 API

Identifier URIs	
-----------------	--

 0 Permissions

There are no permissions found.

 0 Permission Scopes

There are no permission scopes found.

 0 Authorized Applications

There are no authorized applications found.

App Roles

App roles in Microsoft Entra are declarative permissions defined within an application’s manifest that enable granular access control by assigning users or groups to specific roles aligned with the app’s functionality

 **0 App Roles**

There are no app roles found.

Authentication

Provides information about the authentication settings for the application.

 Authentication

Supported Account Types	Accounts in this organizational directory only (Single tenant)
-------------------------	--

 Public Client

Allow Public Client Flows	False
Redirect URIs	

 Single Page Application

Redirect URIs	
---------------	--

 Web

Enable Implicit Access Tokens	False
Enable Implicit ID Tokens	False
Logout URL	
Redirect URIs	

 App Instance Property Lock

App Instance Locked Properties	None
--------------------------------	------

Credentials

Provides information about the client secret and certificate credentials for the application.

 **0 Credentials**

There are no credentials found.

Federated Credentials

Microsoft Entra federated credentials let applications and services authenticate to Entra ID-protected resources without storing secrets or certificates, using trust-based identity federation instead.



0 Federated Credentials

There are no federated credentials found.

Optional Claims

Optional claims are configurable attributes that determine which pieces of user identity information are included in tokens issued to an application during authentication.

 0 Optional Claims

There are no optional claims found.

GSA-Privateaccesstrafficforwardingprofile

Provides information about the applications defined in the organization.

 General

Display Name	GSA-Privateaccesstrafficforwardingprofile
Application Identifier	a97a17b2-eec8-4edf-b13f-1c9b0d33e40a
Object Identifier	acd42eb2-1a6e-49bd-963d-1450b99f61e3

 Properties

Homepage URL	
Privacy Statement URL	
Terms Of Service URL	
Service Management Reference	
Notes	
Publisher Domain	centrelsolutionsdemo.onmicrosoft.com

 Application Icon

The application does not have an icon assigned.

 Publisher Verification

The publisher is not verified.

 1 Owners

Display Name	Identity	Type
 ZTNA Network Access Control Plane		Service Principal

API

Provides information about the API settings for the application.

 API

Identifier URIs	
-----------------	--

 0 Permissions

There are no permissions found.

 0 Permission Scopes

There are no permission scopes found.

 0 Authorized Applications

There are no authorized applications found.

App Roles

App roles in Microsoft Entra are declarative permissions defined within an application’s manifest that enable granular access control by assigning users or groups to specific roles aligned with the app’s functionality

 **0 App Roles**

There are no app roles found.

Authentication

Provides information about the authentication settings for the application.

 Authentication

Supported Account Types	Accounts in this organizational directory only (Single tenant)
-------------------------	--

 Public Client

Allow Public Client Flows	False
Redirect URIs	

 Single Page Application

Redirect URIs	
---------------	--

 Web

Enable Implicit Access Tokens	False
Enable Implicit ID Tokens	False
Logout URL	
Redirect URIs	

 App Instance Property Lock

App Instance Locked Properties	None
--------------------------------	------

Credentials

Provides information about the client secret and certificate credentials for the application.

 **0 Credentials**

There are no credentials found.

Federated Credentials

Microsoft Entra federated credentials let applications and services authenticate to Entra ID-protected resources without storing secrets or certificates, using trust-based identity federation instead.



0 Federated Credentials

There are no federated credentials found.

Optional Claims

Optional claims are configurable attributes that determine which pieces of user identity information are included in tokens issued to an application during authentication.

 0 Optional Claims

There are no optional claims found.

Applications - T

Provides information about the applications defined in the organization with the specified first letter.

1 Applications

Display Name	Supported Account Types	Application Identifier
 Test Evaluation Agent (Microsoft Copilot Studio)	Accounts in any organizational directory (Multitenant)	8a5dea75-3c2a-49ff-aa55-8001576b6673

Test Evaluation Agent (Microsoft Copilot Studio)

Provides information about the applications defined in the organization.

This application was created by Copilot Studio.

 General

Display Name	Test Evaluation Agent (Microsoft Copilot Studio)
Application Identifier	8a5dea75-3c2a-49ff-aa55-8001576b6673
Object Identifier	f1fa2c4f-fbe0-4368-b613-ecbc8fdaf59a

 Properties

Homepage URL	
Privacy Statement URL	
Terms Of Service URL	
Service Management Reference	
Notes	
Publisher Domain	centrelsolutionsdemo.onmicrosoft.com

 Application Icon



 Publisher Verification

The publisher is not verified.

 2 Owners

Display Name	Identity	Type
 Microsoft Copilot Studio Service		Service Principal
 XIA	xia@centrelsolutionsdemo.onmicrosoft.com	User

 Tags

Tags	AI-Agent-Builder Agent-Created-By: Copilot Studio Agentic App power-virtual-agents-80d84ba5-7dfe-fab8-98dd-b3106ee0bfab
-------------	--

Authentication

Provides information about the authentication settings for the application.

 Authentication

Supported Account Types	Accounts in any organizational directory (Multitenant)
-------------------------	--

 Public Client

Allow Public Client Flows	False
Redirect URIs	

 Single Page Application

Redirect URIs	
---------------	--

 Web

Enable Implicit Access Tokens	False
Enable Implicit ID Tokens	False
Logout URL	
Redirect URIs	

 App Instance Property Lock

App Instance Locked Properties	None
--------------------------------	------

Federated Credentials

Microsoft Entra federated credentials let applications and services authenticate to Entra ID–protected resources without storing secrets or certificates, using trust-based identity federation instead.

2 Federated Credentials

Name	Description	Audiences	Issuer	Subject
 AzureADMultipleOrgs_80d84ba5-7dfe-fab8-98dd-b3106ee0bfab		api://AzureADTokenExchange	https://login.microsoftonline.com/{tenantId}/v2.0	/eid1/c/pub/t/{tenantId}/a/m1WPnYRZpEaQKq1Cceg--g/80d84ba5-7dfe-fab8-98dd-b3106ee0bfab
 AzureADMyOrg_80d84ba5-7dfe-fab8-98dd-b3106ee0bfab		api://AzureADTokenExchange	https://login.microsoftonline.com/157f8a9e-052c-4fc2-8b9f-11e8ccc55e96/v2.0	/eid1/c/pub/t/nop_FSwFwk-LnxHozMVelg/a/m1WPnYRZpEaQKq1Cceg-g/80d84ba5-7dfe-fab8-98dd-b3106ee0bfab

Optional Claims

Optional claims are configurable attributes that determine which pieces of user identity information are included in tokens issued to an application during authentication.

 1 Optional Claims

Name	Token Type	Additional Properties
 acct	Access	

Applications - X

Provides information about the applications defined in the organization with the specified first letter.

2 Applications

Display Name	Supported Account Types	Application Identifier
 XIA Configuration Client	Accounts in this organizational directory only (Single tenant)	c3d9d7a2-2832-48e1-a7c1-28f7dd3714af
 XIA Configuration Client (SQL Server)	Accounts in this organizational directory only (Single tenant)	9bfdccfa-c1f5-4e5c-b2a9-f10d36405ce3

XIA Configuration Client

Provides information about the applications defined in the organization.

General

Display Name	XIA Configuration Client
Application Identifier	c3d9d7a2-2832-48e1-a7c1-28f7dd3714af
Object Identifier	e655a0b5-3ec9-47c9-931e-f081bb90bdf2

Properties

Homepage URL	
Privacy Statement URL	
Terms Of Service URL	
Service Management Reference	
Notes	
Publisher Domain	centrelsolutionsdemo.onmicrosoft.com

Application Icon



Publisher Verification

The publisher is not verified.

0 Owners

There are no owners found.

API

Provides information about the API settings for the application.

 API

Identifier URIs	
-----------------	--

 7 Permissions

Application	Permission	Type	Admin Consent Required	Admin Consent Granted
 Microsoft Graph	RoleManagement.Read.Directory	Application	True	False
 Microsoft Graph	NetworkAccess.Read.All	Application	True	False
 Microsoft Graph	Agreement.Read.All	Application	True	False
 Microsoft Graph	Directory.Read.All	Application	True	False
 Microsoft Graph	Organization.Read.All	Application	True	False
 Microsoft Graph	Policy.Read.All	Application	True	False
 Office 365 Exchange Online	Exchange.ManageAsApp	Application	True	False

 0 Permission Scopes

There are no permission scopes found.

 0 Authorized Applications

There are no authorized applications found.

App Roles

App roles in Microsoft Entra are declarative permissions defined within an application’s manifest that enable granular access control by assigning users or groups to specific roles aligned with the app’s functionality

 **0 App Roles**

There are no app roles found.

Authentication

Provides information about the authentication settings for the application.

 Authentication

Supported Account Types	Accounts in this organizational directory only (Single tenant)
-------------------------	--

 Public Client

Allow Public Client Flows	False
Redirect URIs	

 Single Page Application

Redirect URIs	
---------------	--

 Web

Enable Implicit Access Tokens	False
Enable Implicit ID Tokens	False
Logout URL	
Redirect URIs	

 App Instance Property Lock

App Instance Locked Properties	None
--------------------------------	------

Credentials

Provides information about the client secret and certificate credentials for the application.

3 Credentials

Display Name	Credential Type	Identifier	Expiry
 CN=XIA Configuration Client	Certificate	E8E741F69F0AAD57F1CCE07EBE8FD728C47FCEA8	13 April 2027
 Demonstration client secret	Client Secret	eec7afbd-a520-4bbf-86d1-821863f539e9	08 July 2027
 Demonstration client secret 2	Client Secret	6d211d23-42e9-491f-9ab0-62ebd32b7e8b	09 January 2027

Federated Credentials

Microsoft Entra federated credentials let applications and services authenticate to Entra ID-protected resources without storing secrets or certificates, using trust-based identity federation instead.



0 Federated Credentials

There are no federated credentials found.

Optional Claims

Optional claims are configurable attributes that determine which pieces of user identity information are included in tokens issued to an application during authentication.

 0 Optional Claims

There are no optional claims found.

XIA Configuration Client (SQL Server)

Provides information about the applications defined in the organization.

 General

Display Name	XIA Configuration Client (SQL Server)
Application Identifier	9bfdccfa-c1f5-4e5c-b2a9-f10d36405ce3
Object Identifier	8f38041f-7ce4-4f0f-8e01-2a8c4c115fc8

 Properties

Homepage URL	
Privacy Statement URL	
Terms Of Service URL	
Service Management Reference	
Notes	
Publisher Domain	centrelsolutionsdemo.onmicrosoft.com

 Application Icon

The application does not have an icon assigned.

 Publisher Verification

The publisher is not verified.

 0 Owners

There are no owners found.

API

Provides information about the API settings for the application.

 API

Identifier URIs	
-----------------	--

 1 Permissions

Application	Permission	Type	Admin Consent Required	Admin Consent Granted
 Microsoft Graph	e1fe6dd8-ba31-4d61-89e7-88639da4683d	Delegated	Unknown	Unknown

 0 Permission Scopes

There are no permission scopes found.

 0 Authorized Applications

There are no authorized applications found.

App Roles

App roles in Microsoft Entra are declarative permissions defined within an application’s manifest that enable granular access control by assigning users or groups to specific roles aligned with the app’s functionality

 **0 App Roles**

There are no app roles found.

Authentication

Provides information about the authentication settings for the application.

 Authentication

Supported Account Types	Accounts in this organizational directory only (Single tenant)
-------------------------	--

 Public Client

Allow Public Client Flows	False
Redirect URIs	

 Single Page Application

Redirect URIs	
---------------	--

 Web

Enable Implicit Access Tokens	False
Enable Implicit ID Tokens	False
Logout URL	
Redirect URIs	

 App Instance Property Lock

App Instance Locked Properties	All Properties
--------------------------------	----------------

Credentials

Provides information about the client secret and certificate credentials for the application.

2 Credentials

Display Name	Credential Type	Identifier	Expiry
 New Client Secret	Client Secret	ae2608e9-5cf7-4cbd-b193-a6bbebb6f278	08 December 2026
 SQL Server Client Secret	Client Secret	aa513689-fca7-4fca-8dce-7586262292fa	07 November 2026

Federated Credentials

Microsoft Entra federated credentials let applications and services authenticate to Entra ID-protected resources without storing secrets or certificates, using trust-based identity federation instead.



0 Federated Credentials

There are no federated credentials found.

Optional Claims

Optional claims are configurable attributes that determine which pieces of user identity information are included in tokens issued to an application during authentication.

 0 Optional Claims

There are no optional claims found.

Branding

Provides information about the organizational branding.

Custom branding has not been configured for this organization.

Localizations

Localizations allow organizations to customize the sign-in experience for users based on their browser language. This ensures branding feels native and relevant across different regions and languages.

0 Localizations

There are no localizations found.

Conditional Access

Conditional Access is a security feature in Microsoft Entra that controls how identities such as users, applications, and automated agents access your organisation's apps and data. Every sign in or token request is evaluated against real time signals such as the identity, device, location, application, and risk level.

Authentication Contexts

Authentication Contexts are labels that applications can request to trigger specific Conditional Access policies for sensitive actions. Instead of applying access controls only at sign in, an Authentication Context allows an application to signal that a particular operation, workflow step, or resource requires a higher level of assurance.

 2 Authentication Contexts

Display Name	Description	Identifier	Publish To Apps
 Sample authentication context	This is a sample authentication context	c1	True
 Sample authentication context	This is a sample authentication context	c11	True

Authentication Strengths

Authentication Strength Policies define which authentication methods are considered strong enough to satisfy a Conditional Access requirement. Instead of relying on a single method like "MFA", an authentication strength specifies an approved set of methods - such as FIDO2 security keys, Windows Hello for Business, certificate based authentication, or specific combinations of password + second factor.

4 Authentication Strengths

Display Name	Type	Description
 Multifactor authentication	Built-In	Combinations of methods that satisfy strong authentication, such as a password + SMS
 Passwordless MFA	Built-In	Passwordless methods that satisfy strong authentication, such as Passwordless sign-in with the Microsoft Authenticator
 Phishing-resistant MFA	Built-In	Phishing-resistant, Passwordless methods for the strongest authentication, such as a FIDO2 security key
 Sample Authentication Strength	Custom	This is a sample authentication strength

Multifactor authentication

The authentication strength defines which sign-in methods are allowed for this policy. It specifies the approved combinations a user must use to meet the required level of authentication.

General

Description	Combinations of methods that satisfy strong authentication, such as a password + SMS
Policy Type	Built-In
Creation Date	01 December 2021
Modification Date	01 December 2021
Identifier	00000000-0000-0000-0000-000000000002

Authentication Flows

Authentication Flows	Windows Hello for Business / Platform Credential Passkeys (FIDO2) Certificate-based Authentication (Multifactor) Microsoft Authenticator (Phone Sign-in) Temporary Access Pass (One-time use) Temporary Access Pass (Multi-use) Password + Microsoft Authenticator (Push Notification) Password + Software OATH token Password + Hardware OATH token Password + X.509 Certificate (Single-factor) Password + X.509 Certificate (Multi-factor) Password + SMS Password + Voice Federated Multifactor Federated Single factor + Microsoft Authenticator (Push Notification) Federated Single factor + Software OATH token Federated Single factor + Hardware OATH token Federated Single factor + SMS Federated Single factor + Voice
----------------------	--

Passwordless MFA

The authentication strength defines which sign-in methods are allowed for this policy. It specifies the approved combinations a user must use to meet the required level of authentication.



General

Description	Passwordless methods that satisfy strong authentication, such as Passwordless sign-in with the Microsoft Authenticator
Policy Type	Built-In
Creation Date	01 December 2021
Modification Date	01 December 2021
Identifier	00000000-0000-0000-0000-000000000003



Authentication Flows

Authentication Flows	Windows Hello for Business / Platform Credential Passkeys (FIDO2) Certificate-based Authentication (Multifactor) Microsoft Authenticator (Phone Sign-in)
----------------------	---

Phishing-resistant MFA

The authentication strength defines which sign-in methods are allowed for this policy. It specifies the approved combinations a user must use to meet the required level of authentication.



General

Description	Phishing-resistant, Passwordless methods for the strongest authentication, such as a FIDO2 security key
Policy Type	Built-In
Creation Date	01 December 2021
Modification Date	01 December 2021
Identifier	00000000-0000-0000-0000-000000000004



Authentication Flows

Authentication Flows	Windows Hello for Business / Platform Credential Passkeys (FIDO2) Certificate-based Authentication (Multifactor)
-----------------------------	--

Sample Authentication Strength

The authentication strength defines which sign-in methods are allowed for this policy. It specifies the approved combinations a user must use to meet the required level of authentication.

 General

Description	This is a sample authentication strength
Policy Type	Custom
Creation Date	19 November 2025 16:05:25
Modification Date	21 December 2025 18:55:56
Identifier	c3e17391-b6bd-4cf6-916e-f5bc98dfd17c

 Authentication Flows

Authentication Flows	Passkeys (FIDO2) Certificate-based Authentication (Multifactor) Certificate-based Authentication (Single factor)
----------------------	--

 Certificate-Based Authentication (Multifactor)

Allowed Issuer SKIs	c cc
Allowed Policy OIDs	5.4.3

 Certificate-Based Authentication (Single Factor)

Allowed Issuer SKIs	c
Allowed Policy OIDs	1.2.3 4.5.6

 Passkeys (FIDO2)

Allowed AA GUIDs	12345678-0000-0000-0000-123456780011 90a3ccdf-635c-4729-a248-9b709135078f de1e552d-db1d-4423-a619-566b625cdc84
------------------	--

Policies

Conditional Access policies are the decision engine of Microsoft Entra ID. They evaluate signals about a sign in such as the user, device, location, app, and risk level and then enforce the appropriate access controls to keep the organisation secure.

One or more Conditional Access policies use Preview (BETA) features and will not be visible to Graph PowerShell or any tooling that relies on the Microsoft Graph v1.0 production endpoint.

 6 Conditional Access Policies

Display Name	State	Creation Date
 Agents Policy	Report Only	24 December 2025 10:27:56
 Continuous Access Evaluation Policy	Off	24 December 2025 17:19:04
 Global Secure Access Policy	Report Only	28 December 2025 08:39:20
 Sample Policy 1	Off	02 December 2025 15:41:58
 Sample Policy 2	Report Only	19 November 2025 16:38:39
 Workloads Policy	Report Only	23 December 2025 16:10:50

Agents Policy

A Conditional Access policy evaluates signals about a sign in such as the user, device, location, app, and risk level and then enforces the appropriate access controls.

 General

Identifier	fa7f8a45-5f7d-4a97-bb1a-b02a50c1de71
State	Report Only
Creation Date	24 December 2025 10:27:56
Modification Date	24 December 2025 10:37:27

 Template

Template Name	
---------------	--

Assignments

Conditional Access policy assignments define the scope of a policy by specifying which identities and resources are included or excluded. Assignments act as the initial trigger; a policy only evaluates its conditions and enforces access controls if the sign-in context matches these defined assignments.

Included Agent Identities

Agent Identities	All
------------------	-----

2 Excluded Agent Identities

Display Name	Identity	Type
 My Agent Identity Blueprint		Agent Identity
 My First AI Agent		Agent Identity

Agent Identities Filter

Filter Mode	Exclude
Rule	CustomSecurityAttribute.SuperAttributeSet_SuperAttribute -ne "Test"

Conditions

Conditional Access policy conditions define the contextual signals - such as device health, location, risk level, and client app - that determine when specific access controls like MFA or device compliance are enforced.

 Included Client Apps

Client Apps	All
-------------	-----

Grant Controls

Grant controls define the access requirements that must be satisfied before a sign in is allowed. They enforce conditions such as multifactor authentication, device compliance, approved client applications, or blocking access entirely.

 **Grant Controls**

Outcome	Block Access
---------	--------------

 **0 Grant Requirements**

There are no requirements found.

Session Controls

Session controls define how access is managed after it has been granted. They shape the behaviour of the active session by enforcing requirements such as sign-in frequency, persistent browser sessions, app-enforced restrictions, continuous access evaluation, and token protection.

 App Enforced Restrictions	
Enabled	False
 Conditional Access App Control	
Enabled	False
 Continuous Access Evaluation	
Mode	Not Set
 Global Secure Access Security Profile	
Enabled	False
 Persistent Browser Session	
Enabled	False
 Resilience Defaults	
Disable Resilience Defaults	False
 Require Token Protection	
Enabled	False
 Sign-In Frequency	
Enabled	False

Continuous Access Evaluation Policy

A Conditional Access policy evaluates signals about a sign in such as the user, device, location, app, and risk level and then enforces the appropriate access controls.

This Conditional Access policy uses Preview (BETA) features and will not be visible to Graph PowerShell or any tooling that relies on the Microsoft Graph v1.0 production endpoint.

General

Identifier	4daea831-d7a7-4de7-b68f-5a7757c83535
State	Off
Creation Date	24 December 2025 17:19:04
Modification Date	24 December 2025 21:13:36

Template

Template Name	
---------------	--

Assignments

Conditional Access policy assignments define the scope of a policy by specifying which identities and resources are included or excluded. Assignments act as the initial trigger; a policy only evaluates its conditions and enforces access controls if the sign-in context matches these defined assignments.

 Included Target Resources

Target Resources	All
------------------	-----

 Excluded Target Resources

Target Resources	None
------------------	------

 Included Users

Users	All
-------	-----

 Excluded Users

Users	None
-------	------

Conditions

Conditional Access policy conditions define the contextual signals - such as device health, location, risk level, and client app - that determine when specific access controls like MFA or device compliance are enforced.

 Included Client Apps

Client Apps	All
-------------	-----

Grant Controls

Grant controls define the access requirements that must be satisfied before a sign in is allowed. They enforce conditions such as multifactor authentication, device compliance, approved client applications, or blocking access entirely.

 **Grant Controls**

Outcome	Grant Access
---------	--------------

 **0 Grant Requirements**

There are no requirements found.

Session Controls

Session controls define how access is managed after it has been granted. They shape the behaviour of the active session by enforcing requirements such as sign-in frequency, persistent browser sessions, app-enforced restrictions, continuous access evaluation, and token protection.



App Enforced Restrictions

Enabled	False
---------	-------



Conditional Access App Control

Enabled	False
---------	-------



Continuous Access Evaluation

Mode	Strictly Enforce Location Policies
------	------------------------------------



Global Secure Access Security Profile

Enabled	True
Profile Name	Sample Profile
Profile Identifier	e51d5f5b-d03e-44b4-bc91-22960caf1726



Persistent Browser Session

Enabled	False
---------	-------



Resilience Defaults

Disable Resilience Defaults	False
-----------------------------	-------



Require Token Protection

Enabled	False
---------	-------



Sign-In Frequency

Enabled	False
---------	-------

Global Secure Access Policy

A Conditional Access policy evaluates signals about a sign in such as the user, device, location, app, and risk level and then enforces the appropriate access controls.

This Conditional Access policy uses Preview (BETA) features and will not be visible to Graph PowerShell or any tooling that relies on the Microsoft Graph v1.0 production endpoint.

General

Identifier	d8e9c196-4042-4cab-b95b-31f9e90e3784
State	Report Only
Creation Date	28 December 2025 08:39:20
Modification Date	[Not Configured]

Template

Template Name	
---------------	--

Assignments

Conditional Access policy assignments define the scope of a policy by specifying which identities and resources are included or excluded. Assignments act as the initial trigger; a policy only evaluates its conditions and enforces access controls if the sign-in context matches these defined assignments.

 2 Included Target Resources

Display Name	Identity	Type
 Microsoft apps with Global Secure Access	9fac4304-08f7-46de-bc2b-264bcf08faf7	Service Principal
 Internet resources with Global Secure Access	6b67f95d-421c-470d-88b8-d86f57d85915	Service Principal

 Excluded Target Resources

Target Resources	None
------------------	------

Conditions

Conditional Access policy conditions define the contextual signals - such as device health, location, risk level, and client app - that determine when specific access controls like MFA or device compliance are enforced.

 Included Client Apps

Client Apps	All
-------------	-----

Grant Controls

Grant controls define the access requirements that must be satisfied before a sign in is allowed. They enforce conditions such as multifactor authentication, device compliance, approved client applications, or blocking access entirely.

 **Grant Controls**

Outcome	Grant Access
---------	--------------

 **0 Grant Requirements**

There are no requirements found.

Session Controls

Session controls define how access is managed after it has been granted. They shape the behaviour of the active session by enforcing requirements such as sign-in frequency, persistent browser sessions, app-enforced restrictions, continuous access evaluation, and token protection.



App Enforced Restrictions

Enabled	False
---------	-------



Conditional Access App Control

Enabled	False
---------	-------



Continuous Access Evaluation

Mode	Not Set
------	---------



Global Secure Access Security Profile

Enabled	True
Profile Name	Sample Profile
Profile Identifier	e51d5f5b-d03e-44b4-bc91-22960caf1726



Persistent Browser Session

Enabled	False
---------	-------



Resilience Defaults

Disable Resilience Defaults	False
-----------------------------	-------



Require Token Protection

Enabled	False
---------	-------



Sign-In Frequency

Enabled	False
---------	-------

Sample Policy 1

A Conditional Access policy evaluates signals about a sign in such as the user, device, location, app, and risk level and then enforces the appropriate access controls.

 General

Identifier	beeb02ed-f290-4f8e-9137-c4ef6399fbf9
State	Off
Creation Date	02 December 2025 15:41:58
Modification Date	23 December 2025 15:19:01

 Template

Template Name	
---------------	--

Assignments

Conditional Access policy assignments define the scope of a policy by specifying which identities and resources are included or excluded. Assignments act as the initial trigger; a policy only evaluates its conditions and enforces access controls if the sign-in context matches these defined assignments.

1 Included Agent Identities

Display Name	Identity	Type
 My Agent Identity Blueprint		Agent Identity

1 Excluded Agent Identities

Display Name	Identity	Type
 My Agent Identity Blueprint		Agent Identity

Included Target Resources

Target Resources	All
------------------	-----

Excluded Target Resources

Target Resources	None
------------------	------

Agent Identities Filter

Filter Mode	Include
Rule	CustomSecurityAttribute.SuperAttributeSet_SuperAttribute -ne "AT"

Conditions

Conditional Access policy conditions define the contextual signals - such as device health, location, risk level, and client app - that determine when specific access controls like MFA or device compliance are enforced.

 2 Included Agent Identity Risk Levels

Agent Identity Risk Levels	High Low
----------------------------	-------------

 Included Client Apps

Client Apps	All
-------------	-----

Grant Controls

Grant controls define the access requirements that must be satisfied before a sign in is allowed. They enforce conditions such as multifactor authentication, device compliance, approved client applications, or blocking access entirely.

 **Grant Controls**

Outcome	Block Access
---------	--------------

 **0 Grant Requirements**

There are no requirements found.

Session Controls

Session controls define how access is managed after it has been granted. They shape the behaviour of the active session by enforcing requirements such as sign-in frequency, persistent browser sessions, app-enforced restrictions, continuous access evaluation, and token protection.

 App Enforced Restrictions	
Enabled	False
 Conditional Access App Control	
Enabled	False
 Continuous Access Evaluation	
Mode	Not Set
 Global Secure Access Security Profile	
Enabled	False
 Persistent Browser Session	
Enabled	False
 Resilience Defaults	
Disable Resilience Defaults	False
 Require Token Protection	
Enabled	False
 Sign-In Frequency	
Enabled	False

Sample Policy 2

A Conditional Access policy evaluates signals about a sign in such as the user, device, location, app, and risk level and then enforces the appropriate access controls.

 General

Identifier	683efb6b-f709-4cc8-baf0-ff1c11fb8ced
State	Report Only
Creation Date	19 November 2025 16:38:39
Modification Date	21 December 2025 18:57:48

 Template

Template Name	
---------------	--

Assignments

Conditional Access policy assignments define the scope of a policy by specifying which identities and resources are included or excluded. Assignments act as the initial trigger; a policy only evaluates its conditions and enforces access controls if the sign-in context matches these defined assignments.

3 Included Roles

Roles	Application Developer Attack Simulation Administrator Attribute Assignment Administrator
-------	--

2 Excluded Roles

Roles	External ID User Flow Administrator Microsoft 365 Backup Administrator
-------	---

Included Target Resources

Target Resources	All
------------------	-----

Excluded Target Resources

Target Resources	None
------------------	------

Conditions

Conditional Access policy conditions define the contextual signals - such as device health, location, risk level, and client app - that determine when specific access controls like MFA or device compliance are enforced.

Devices Filter

Filter Mode	Include
Rule	device.manufacturer -notStartsWith "HP" -and device.deviceOwnership -ne "Company"

1 Included Authentication Flows

Authentication Flows	Authentication Transfer
----------------------	-------------------------

1 Included Client Apps

Client Apps	Browser
-------------	---------

2 Included Device Platforms

Device Platforms	iOS Windows
------------------	----------------

5 Excluded Device Platforms

Device Platforms	Android iOS Linux macOS Windows Phone
------------------	---

2 Included Insider Risk Levels

Insider Risk Levels	Minor Moderate
---------------------	-------------------

Included Locations

Locations	All Trusted
-----------	-------------

Excluded Locations

Locations	None
-----------	------



2 Included Sign-In Risk Levels

Sign-In Risk Levels	Medium
	No Risk



1 Included User Risk Levels

User Risk Levels	Medium
------------------	--------

Grant Controls

Grant controls define the access requirements that must be satisfied before a sign in is allowed. They enforce conditions such as multifactor authentication, device compliance, approved client applications, or blocking access entirely.

 Grant Controls

For Multiple Controls	Require one of the selected controls
Outcome	Grant Access

 4 Grant Requirements

Display Name	Type	Identifier
 Sample Authentication Strength	Authentication Strength	c3e17391-b6bd-4cf6-916e-f5bc98dfd17c
 Require app protection policy	Built-In Control	
 Require device to be marked as compliant	Built-In Control	
 Sample terms of use	Terms Of Use	b536e1ad-4c44-4031-a9be-07a517fd6fb0

Session Controls

Session controls define how access is managed after it has been granted. They shape the behaviour of the active session by enforcing requirements such as sign-in frequency, persistent browser sessions, app-enforced restrictions, continuous access evaluation, and token protection.



App Enforced Restrictions

Enabled	False
---------	-------



Conditional Access App Control

Enabled	False
---------	-------



Continuous Access Evaluation

Mode	Not Set
------	---------



Global Secure Access Security Profile

Enabled	False
---------	-------



Persistent Browser Session

Enabled	True
Mode	Always



Resilience Defaults

Disable Resilience Defaults	False
-----------------------------	-------



Require Token Protection

Enabled	True
---------	------



Sign-In Frequency

Enabled	True
Authentication Type	Primary and secondary authentication
Frequency	Periodic reauthentication every 12 days

Workloads Policy

A Conditional Access policy evaluates signals about a sign in such as the user, device, location, app, and risk level and then enforces the appropriate access controls.

 General

Identifier	e8860f23-5011-4d18-bd2c-0a6b87944ba4
State	Report Only
Creation Date	23 December 2025 16:10:50
Modification Date	24 December 2025 09:24:25

 Template

Template Name	
---------------	--

Assignments

Conditional Access policy assignments define the scope of a policy by specifying which identities and resources are included or excluded. Assignments act as the initial trigger; a policy only evaluates its conditions and enforces access controls if the sign-in context matches these defined assignments.

Included Service Principals

Service Principals	All Owned Service Principals
--------------------	------------------------------

5 Excluded Service Principals

Display Name	Identity	Type
 Orphaned Object {0f00bca1-27f9-49c4-a790-1826c34a2fa4}	0f00bca1-27f9-49c4-a790-1826c34a2fa4	Orphaned
 Orphaned Object {ac8bc25c-fdbb-4719-85d2-2348d82ac036}	ac8bc25c-fdbb-4719-85d2-2348d82ac036	Orphaned
 GSA-Internettrafficforwardingprofile	63d88f79-7e16-48b9-b9cd-ba6d529c7936	Service Principal
 Orphaned Object {7d4b4884-1e56-4491-b4bd-b1d2b23109ec}	7d4b4884-1e56-4491-b4bd-b1d2b23109ec	Orphaned
 Orphaned Object {28ea639d-703a-4f02-8460-695b55b9b29d}	28ea639d-703a-4f02-8460-695b55b9b29d	Orphaned

Service Principals Filter

Filter Mode	Exclude
Rule	CustomSecurityAttribute.SuperAttributeSet_SuperAttribute -ne "a"

Conditions

Conditional Access policy conditions define the contextual signals - such as device health, location, risk level, and client app - that determine when specific access controls like MFA or device compliance are enforced.

 Included Client Apps

Client Apps	All
-------------	-----

 2 Included Service Principal Risk Levels

Service Principal Risk Levels	High Medium
-------------------------------	----------------

Grant Controls

Grant controls define the access requirements that must be satisfied before a sign in is allowed. They enforce conditions such as multifactor authentication, device compliance, approved client applications, or blocking access entirely.

 **Grant Controls**

Outcome	Block Access
---------	--------------

 **0 Grant Requirements**

There are no requirements found.

Session Controls

Session controls define how access is managed after it has been granted. They shape the behaviour of the active session by enforcing requirements such as sign-in frequency, persistent browser sessions, app-enforced restrictions, continuous access evaluation, and token protection.

 App Enforced Restrictions	
Enabled	False
 Conditional Access App Control	
Enabled	False
 Continuous Access Evaluation	
Mode	Not Set
 Global Secure Access Security Profile	
Enabled	False
 Persistent Browser Session	
Enabled	False
 Resilience Defaults	
Disable Resilience Defaults	False
 Require Token Protection	
Enabled	False
 Sign-In Frequency	
Enabled	False

Named Locations

Named Locations are reusable network definitions that Conditional Access policies can reference when evaluating sign ins. They allow administrators to classify traffic based on IP ranges or geographic regions, and then apply different access requirements depending on where a request originates.

 2 Named Locations

Display Name		Location Type	Trusted	Creation Date
	Sample IP Location	IP Ranges	True	18 November 2025 14:07:12
	Sample IP Location	IP Ranges	True	18 November 2025 14:24:03

Sample IP Location

Named Locations are reusable network definitions that Conditional Access policies can reference when evaluating sign ins. They allow administrators to classify traffic based on IP ranges or geographic regions, and then apply different access requirements depending on where a request originates.

 General

Location Type	IP Ranges
Creation Date	18 November 2025 14:07:12
Modification Date	21 December 2025 18:52:22
Identifier	0402619f-2fdd-4e2b-9c8d-03e241960357

 IP Settings

Trusted	True
IP Ranges	44.44.44.44/24 2a01:111::/32

Sample IP Location

Named Locations are reusable network definitions that Conditional Access policies can reference when evaluating sign ins. They allow administrators to classify traffic based on IP ranges or geographic regions, and then apply different access requirements depending on where a request originates.

 General

Location Type	IP Ranges
Creation Date	18 November 2025 14:24:03
Modification Date	21 December 2025 18:52:26
Identifier	0e0624b1-6bdf-4aa0-a586-c634a5d8912b

 IP Settings

Trusted	True
IP Ranges	45.45.45.45/24

Terms Of Use

Microsoft Entra Terms of Use policies allow organisations to require users to review and accept specific usage terms, such as acceptable use statements, legal notices, or compliance requirements, before they can access a protected resource. When a Conditional Access policy includes a Terms of Use requirement, users are prompted to accept the agreement during sign in.

 1 Terms of Use Policies

Display Name	Expire Consents	Consent On Every Device
 Sample terms of use	False	False

Sample terms of use

A Terms of Use policy requires users to review and accept specific usage terms before they can access a protected resource.

 General

Identifier	b536e1ad-4c44-4031-a9be-07a517fd6fb0
Users are required to consent on every device	False
Require users to expand the terms of use	True
Duration before re-acceptance required	12 days

 Expiry

Consents Expire	False
-----------------	-------

Enterprise Applications

Microsoft Entra enterprise applications represent service principal instances of applications within a tenant, enabling administrators to manage access, single sign-on, provisioning, and conditional access policies for each app individually.

8 Enterprise Applications

First Letter	Count
 #	0
 A	0
 B	0
 C	0
 D	0
 E	1
 F	0
 G	1
 H	0
 I	0
 J	0
 K	0
 L	0
 M	1
 N	0
 O	0
 P	0
 Q	0
 R	0
 S	0
 T	0
 U	0
 V	0
 W	0
 X	5
 Y	0

 z	0
---	---

Enterprise Applications - E

Provides information about the enterprise applications defined in the organization with the specified first letter.



1 Enterprise Applications

Display Name	Homepage URL	Application Identifier
 ExchangeServerApp-1594abbd-9de4-4330-b1c7-fcf0036c8e6d		61021fe7-7182-4481-b08a-f21c6665ece4

ExchangeServerApp-1594abbd-9de4-4330-b1c7-fcf0036c8e6d

Microsoft Entra enterprise applications represent service principal instances of applications within a tenant, enabling administrators to manage access, single sign-on, provisioning, and conditional access policies for each app individually.

 General

Display Name	ExchangeServerApp-1594abbd-9de4-4330-b1c7-fcf0036c8e6d
Application Identifier	61021fe7-7182-4481-b08a-f21c6665ece4
Identifier	448ab1de-dd2e-493a-9f7e-06f787ef24cb

 Properties

Assignment Required	False
Enabled For Sign-In	True
Homepage URL	
Notes	
Visible	False

 Enterprise Application Icon



 0 Owners

There are no owners found.

Admin Consented Permissions

Admin consented permissions for an Entra enterprise application grant access to organizational data on behalf of all users, without requiring individual user approval. These permissions are centrally managed and enforced by administrators to support secure, scalable app integration.

 1 Admin Consented Permissions

Application	Permission	Description	Type
 Office 365 Exchange Online	full_access_as_app	Allows the app to have full access via Exchange Web Services to all mailboxes without a signed-in user.	Application

App Roles

App roles in Microsoft Entra enterprise applications represent the tenant-specific assignments of declarative permissions defined in the application’s manifest. These roles enable granular access control by linking users, groups, or service principals to specific functional roles within the app instance, enforcing scoped authorization across environments.

 **0 App Roles**

There are no app roles found.

App Role Assignments

App role assignments in Microsoft Entra enterprise applications link users, groups, or service principals to specific roles defined by the application’s manifest. These assignments enforce scoped access to app functionality, enabling granular authorization across tenant environments. Each assignment reflects a declarative permission granted to an identity, ensuring that access aligns with the app’s intended operational boundaries.

 0 App Role Assignments

There are no app role assignments found.

Enterprise Applications - G

Provides information about the enterprise applications defined in the organization with the specified first letter.

1 Enterprise Applications

Display Name	Homepage URL	Application Identifier
 Graph Explorer	https://developer.microsoft.com/graph/graph-explorer	de8bc8b5-d9f9-48b1-a8ad-b748da725064

Graph Explorer

Microsoft Entra enterprise applications represent service principal instances of applications within a tenant, enabling administrators to manage access, single sign-on, provisioning, and conditional access policies for each app individually.

 General

Display Name	Graph Explorer
Application Identifier	de8bc8b5-d9f9-48b1-a8ad-b748da725064
Identifier	a1611bd7-af72-4136-89a5-cea63f9cba57

 Properties

Assignment Required	False
Enabled For Sign-In	True
Homepage URL	https://developer.microsoft.com/graph/graph-explorer
Notes	
Visible	True

 Enterprise Application Icon

The enterprise application does not have an icon assigned.

 0 Owners

There are no owners found.

Admin Consented Permissions

Admin consented permissions for an Entra enterprise application grant access to organizational data on behalf of all users, without requiring individual user approval. These permissions are centrally managed and enforced by administrators to support secure, scalable app integration.

 **0 Admin Consented Permissions**

There are no admin consented permissions found.

App Roles

App roles in Microsoft Entra enterprise applications represent the tenant-specific assignments of declarative permissions defined in the application’s manifest. These roles enable granular access control by linking users, groups, or service principals to specific functional roles within the app instance, enforcing scoped authorization across environments.

 **0 App Roles**

There are no app roles found.

App Role Assignments

App role assignments in Microsoft Entra enterprise applications link users, groups, or service principals to specific roles defined by the application’s manifest. These assignments enforce scoped access to app functionality, enabling granular authorization across tenant environments. Each assignment reflects a declarative permission granted to an identity, ensuring that access aligns with the app’s intended operational boundaries.

 1 App Role Assignments

Display Name	Identifier	Object Type	Role
 XIA	ad45c596-19d3-4cd5-a11b-c6096b1ce89d	User	Default Access

Enterprise Applications - M

Provides information about the enterprise applications defined in the organization with the specified first letter.

1 Enterprise Applications

Display Name	Homepage URL	Application Identifier
 Microsoft Graph Command Line Tools	https://docs.microsoft.com/en-us/graph/powershell/get-started	14d82eec-204b-4c2f-b7e8-296a70dab67e

Microsoft Graph Command Line Tools

Microsoft Entra enterprise applications represent service principal instances of applications within a tenant, enabling administrators to manage access, single sign-on, provisioning, and conditional access policies for each app individually.

 General

Display Name	Microsoft Graph Command Line Tools
Application Identifier	14d82eec-204b-4c2f-b7e8-296a70dab67e
Identifier	4e20611c-077b-47da-ac9c-382ecbbec9cc

 Properties

Assignment Required	False
Enabled For Sign-In	True
Homepage URL	https://docs.microsoft.com/en-us/graph/powershell/get-started
Notes	These are example notes.
Visible	True

 Enterprise Application Icon

The enterprise application does not have an icon assigned.

 0 Owners

There are no owners found.

Admin Consented Permissions

Admin consented permissions for an Entra enterprise application grant access to organizational data on behalf of all users, without requiring individual user approval. These permissions are centrally managed and enforced by administrators to support secure, scalable app integration.

 **0 Admin Consented Permissions**

There are no admin consented permissions found.

App Roles

App roles in Microsoft Entra enterprise applications represent the tenant-specific assignments of declarative permissions defined in the application’s manifest. These roles enable granular access control by linking users, groups, or service principals to specific functional roles within the app instance, enforcing scoped authorization across environments.

 **0 App Roles**

There are no app roles found.

App Role Assignments

App role assignments in Microsoft Entra enterprise applications link users, groups, or service principals to specific roles defined by the application’s manifest. These assignments enforce scoped access to app functionality, enabling granular authorization across tenant environments. Each assignment reflects a declarative permission granted to an identity, ensuring that access aligns with the app’s intended operational boundaries.

 1 App Role Assignments

Display Name	Identifier	Object Type	Role
 XIA	ad45c596-19d3-4cd5-a11b-c6096b1ce89d	User	Default Access

Enterprise Applications - X

Provides information about the enterprise applications defined in the organization with the specified first letter.

5 Enterprise Applications

Display Name	Homepage URL	Application Identifier
 XIA Configuration Client	https://www.centrel-solutions.com/xiaconfiguration	878983dd-6b8f-45ba-9f0c-10d3b423a5b6
 XIA Configuration Client (SQL Server)		9bfdccfa-c1f5-4e5c-b2a9-f10d36405ce3
 XIA Configuration Express	https://centrel-solutions.com/xiaconfiguration/express	8535662a-dd9e-439d-94aa-3b49f76994f2
 XIA Configuration Express Management API	https://centrel-solutions.com/xiaconfiguration/express	fd6d29dc-30df-4bf0-8491-e9b113cea969
 XIA Configuration Tools	https://www.centrel-solutions.com/xiaconfiguration	26d99201-dc54-4570-b16d-3e59a0307e66

XIA Configuration Client

Microsoft Entra enterprise applications represent service principal instances of applications within a tenant, enabling administrators to manage access, single sign-on, provisioning, and conditional access policies for each app individually.

 General

Display Name	XIA Configuration Client
Application Identifier	878983dd-6b8f-45ba-9f0c-10d3b423a5b6
Identifier	51d59d02-5b36-4b63-9e65-b1afb2dd8778

 Properties

Assignment Required	False
Enabled For Sign-In	True
Homepage URL	https://www.centrel-solutions.com/xiaconfiguration
Notes	
Visible	True

 Enterprise Application Icon



 0 Owners

There are no owners found.

Admin Consented Permissions

Admin consented permissions for an Entra enterprise application grant access to organizational data on behalf of all users, without requiring individual user approval. These permissions are centrally managed and enforced by administrators to support secure, scalable app integration.

 **0 Admin Consented Permissions**

There are no admin consented permissions found.

App Roles

App roles in Microsoft Entra enterprise applications represent the tenant-specific assignments of declarative permissions defined in the application’s manifest. These roles enable granular access control by linking users, groups, or service principals to specific functional roles within the app instance, enforcing scoped authorization across environments.

 **0 App Roles**

There are no app roles found.

App Role Assignments

App role assignments in Microsoft Entra enterprise applications link users, groups, or service principals to specific roles defined by the application’s manifest. These assignments enforce scoped access to app functionality, enabling granular authorization across tenant environments. Each assignment reflects a declarative permission granted to an identity, ensuring that access aligns with the app’s intended operational boundaries.

 1 App Role Assignments

Display Name	Identifier	Object Type	Role
 XIA	ad45c596-19d3-4cd5-a11b-c6096b1ce89d	User	Default Access

XIA Configuration Client (SQL Server)

Microsoft Entra enterprise applications represent service principal instances of applications within a tenant, enabling administrators to manage access, single sign-on, provisioning, and conditional access policies for each app individually.

 General

Display Name	XIA Configuration Client (SQL Server)
Application Identifier	9bfdccfa-c1f5-4e5c-b2a9-f10d36405ce3
Identifier	de11b913-d39d-4e3b-bea8-35073e72c152

 Properties

Assignment Required	False
Enabled For Sign-In	True
Homepage URL	
Notes	
Visible	False

 Enterprise Application Icon

The enterprise application does not have an icon assigned.

 0 Owners

There are no owners found.

Admin Consented Permissions

Admin consented permissions for an Entra enterprise application grant access to organizational data on behalf of all users, without requiring individual user approval. These permissions are centrally managed and enforced by administrators to support secure, scalable app integration.

 **0 Admin Consented Permissions**

There are no admin consented permissions found.

App Roles

App roles in Microsoft Entra enterprise applications represent the tenant-specific assignments of declarative permissions defined in the application’s manifest. These roles enable granular access control by linking users, groups, or service principals to specific functional roles within the app instance, enforcing scoped authorization across environments.

 **0 App Roles**

There are no app roles found.

App Role Assignments

App role assignments in Microsoft Entra enterprise applications link users, groups, or service principals to specific roles defined by the application’s manifest. These assignments enforce scoped access to app functionality, enabling granular authorization across tenant environments. Each assignment reflects a declarative permission granted to an identity, ensuring that access aligns with the app’s intended operational boundaries.

 1 App Role Assignments

Display Name	Identifier	Object Type	Role
 XIA	ad45c596-19d3-4cd5-a11b-c6096b1ce89d	User	Default Access

XIA Configuration Express

Microsoft Entra enterprise applications represent service principal instances of applications within a tenant, enabling administrators to manage access, single sign-on, provisioning, and conditional access policies for each app individually.

 General

Display Name	XIA Configuration Express
Application Identifier	8535662a-dd9e-439d-94aa-3b49f76994f2
Identifier	bf5bf99a-bef8-44a3-8371-d6b0fc748aef

 Properties

Assignment Required	False
Enabled For Sign-In	True
Homepage URL	https://centrel-solutions.com/xiaconfiguration/express
Notes	
Visible	True

 Enterprise Application Icon



 0 Owners

There are no owners found.

Admin Consented Permissions

Admin consented permissions for an Entra enterprise application grant access to organizational data on behalf of all users, without requiring individual user approval. These permissions are centrally managed and enforced by administrators to support secure, scalable app integration.

 **0 Admin Consented Permissions**

There are no admin consented permissions found.

App Roles

App roles in Microsoft Entra enterprise applications represent the tenant-specific assignments of declarative permissions defined in the application’s manifest. These roles enable granular access control by linking users, groups, or service principals to specific functional roles within the app instance, enforcing scoped authorization across environments.

 **0 App Roles**

There are no app roles found.

App Role Assignments

App role assignments in Microsoft Entra enterprise applications link users, groups, or service principals to specific roles defined by the application’s manifest. These assignments enforce scoped access to app functionality, enabling granular authorization across tenant environments. Each assignment reflects a declarative permission granted to an identity, ensuring that access aligns with the app’s intended operational boundaries.

 1 App Role Assignments

Display Name	Identifier	Object Type	Role
 XIA	ad45c596-19d3-4cd5-a11b-c6096b1ce89d	User	Default Access

XIA Configuration Express Management API

Microsoft Entra enterprise applications represent service principal instances of applications within a tenant, enabling administrators to manage access, single sign-on, provisioning, and conditional access policies for each app individually.

 General

Display Name	XIA Configuration Express Management API
Application Identifier	fd6d29dc-30df-4bf0-8491-e9b113cea969
Identifier	9b832eea-d2cd-43c2-9c0f-078e5e944296

 Properties

Assignment Required	False
Enabled For Sign-In	True
Homepage URL	https://centrel-solutions.com/xiaconfiguration/express
Notes	
Visible	True

 Enterprise Application Icon



 0 Owners

There are no owners found.

Admin Consented Permissions

Admin consented permissions for an Entra enterprise application grant access to organizational data on behalf of all users, without requiring individual user approval. These permissions are centrally managed and enforced by administrators to support secure, scalable app integration.

 **0 Admin Consented Permissions**

There are no admin consented permissions found.

App Roles

App roles in Microsoft Entra enterprise applications represent the tenant-specific assignments of declarative permissions defined in the application’s manifest. These roles enable granular access control by linking users, groups, or service principals to specific functional roles within the app instance, enforcing scoped authorization across environments.

 **0 App Roles**

There are no app roles found.

App Role Assignments

App role assignments in Microsoft Entra enterprise applications link users, groups, or service principals to specific roles defined by the application’s manifest. These assignments enforce scoped access to app functionality, enabling granular authorization across tenant environments. Each assignment reflects a declarative permission granted to an identity, ensuring that access aligns with the app’s intended operational boundaries.

 1 App Role Assignments

Display Name	Identifier	Object Type	Role
 XIA	ad45c596-19d3-4cd5-a11b-c6096b1ce89d	User	Default Access

XIA Configuration Tools

Microsoft Entra enterprise applications represent service principal instances of applications within a tenant, enabling administrators to manage access, single sign-on, provisioning, and conditional access policies for each app individually.

 General

Display Name	XIA Configuration Tools
Application Identifier	26d99201-dc54-4570-b16d-3e59a0307e66
Identifier	a068a301-46cb-4130-bff6-68e322f08485

 Properties

Assignment Required	False
Enabled For Sign-In	True
Homepage URL	https://www.centrel-solutions.com/xiaconfiguration
Notes	
Visible	True

 Enterprise Application Icon



 0 Owners

There are no owners found.

Admin Consented Permissions

Admin consented permissions for an Entra enterprise application grant access to organizational data on behalf of all users, without requiring individual user approval. These permissions are centrally managed and enforced by administrators to support secure, scalable app integration.

 **0 Admin Consented Permissions**

There are no admin consented permissions found.

App Roles

App roles in Microsoft Entra enterprise applications represent the tenant-specific assignments of declarative permissions defined in the application’s manifest. These roles enable granular access control by linking users, groups, or service principals to specific functional roles within the app instance, enforcing scoped authorization across environments.

 **0 App Roles**

There are no app roles found.

App Role Assignments

App role assignments in Microsoft Entra enterprise applications link users, groups, or service principals to specific roles defined by the application’s manifest. These assignments enforce scoped access to app functionality, enabling granular authorization across tenant environments. Each assignment reflects a declarative permission granted to an identity, ensuring that access aligns with the app’s intended operational boundaries.

 1 App Role Assignments

Display Name	Identifier	Object Type	Role
 XIA	ad45c596-19d3-4cd5-a11b-c6096b1ce89d	User	Default Access

Entra Connect

Entra Connect is the top-level product family in Microsoft Entra that groups all hybrid identity connection technologies such as Entra Cloud Sync.

 On-Premises Sync

Enabled	True
Last Password Sync Date	22 September 2026 10:21:10
Last Sync Date	22 September 2026 10:26:20

Cloud Sync

Microsoft Entra Cloud Sync is a cloud-managed directory provisioning service that synchronizes users, groups, and contacts from on-premises Active Directory to Microsoft Entra ID. It uses a lightweight on-premises provisioning agent while all synchronization logic runs in Microsoft’s cloud.

 Cloud Sync

Enabled	True
---------	------

Agents

Cloud Sync agents are lightweight on-premises components that securely connect your Active Directory environment to Microsoft Entra’s cloud-based provisioning service.

 2 Agents

Machine Name	External IP Address	Status	Resources
 CSDEMO-DC01.centrelsolutionsdemo.int	81.109.64.92	Active	centrelsolutionsdemo.int
 CSDEMO-DC03.emea.centrelsolutionsdemo.int	81.109.64.92	Inactive	emea.centrelsolutionsdemo.int

Configurations

Cloud Sync configurations define which objects and attributes are in scope for synchronization, controlling how users, groups, and contacts flow from Active Directory to Entra ID - and, where supported, how selected attributes can flow back from Entra ID to Active Directory.

4 Cloud Sync Configurations

Domain Name		Sync Direction	Status
	centresolutionsdemo.int	AD to Microsoft Entra ID	Active
	emea.centresolutionsdemo.int	AD to Microsoft Entra ID	Disabled
	centresolutionsdemo.int	Microsoft Entra ID to AD	Active
	emea.centresolutionsdemo.int	Microsoft Entra ID to AD	Disabled

centrelsolutionsdemo.int (AD to Microsoft Entra ID)

Cloud Sync configurations define which objects and attributes are in scope for synchronization, controlling how users, groups, and contacts flow from Active Directory to Entra ID - and, where supported, how selected attributes can flow back from Entra ID to Active Directory.

General

Configuration Type	AD to Microsoft Entra ID
Domain Name	centrelsolutionsdemo.int
Service Principal Identifier	48b8391b-b5fb-4781-b22b-21f744a81b18
Status	Active

Domain Information

Domain Name	centrelsolutionsdemo.int
Domain NetBIOS Name	CSDEMO
Domain Discovery Date	13 April 2026 16:35:39
Forest Name	centrelsolutionsdemo.int
Forest NetBIOS Name	CSDEMO

Settings

Email Notifications	True
Email Notifications Recipient	
Prevent Accidental Deletion	True
Accidental Deletion Threshold	500
Exchange Hybrid Writeback	False
Password Hash Sync	True

1 Agents

Machine Name	External IP Address	Status	Resources
 CSDEMO-DC01.centrelsolutionsdemo.int	81.109.64.92	Active	centrelsolutionsdemo.int

2 Job Statuses

Display Name	Status	Last Run Date/Time
Password hash sync	Active	22 September 2026 09:21:10
User and group sync	Active	22 September 2026 09:26:20

Scoping Filters

Scoping filters in Microsoft Entra Cloud Sync are conditional rules that determine which directory objects are included in a given sync flow.

 Scoping Filters

Filter Type	All users
-------------	-----------

Object Mappings

Object mappings in Microsoft Entra Cloud Sync define how attributes from on-premises Active Directory objects (such as users or groups) are matched, transformed, and synchronized with their corresponding objects in Entra ID, and where supported, how selected attributes flow back from Entra ID to Active Directory.

 4 Object Mappings

Source Object Name	Target Object Name	Enabled
 contact	Contact	True
 group	Group	True
 inetOrgPerson	User	True
 user	User	True

contact

Object mappings in Microsoft Entra Cloud Sync define how attributes from on-premises Active Directory objects (such as users or groups) are matched, transformed, and synchronized with their corresponding objects in Entra ID, and where supported, how selected attributes flow back from Entra ID to Active Directory.

 General

Source Object Name	contact
Target Object Name	Contact
Enabled	True

contact Attribute Mappings

Attribute mappings in Microsoft Entra Cloud Sync define how attributes from the specified on-premises Active Directory object are matched, transformed, and synchronized with their corresponding objects in Entra ID, and where supported, how selected attributes flow back from Entra ID to Active Directory.

89 Attribute Mappings

Target Attribute Name	Source Type	Source Value	Default Value
 Alias	Direct	mailNickname	
 Assistant	Direct	assistant	
 AuthOrig	Direct	authOrig	
 City	Expression	Trim([l])	
 Company	Expression	Trim([company])	
 Country	Expression	Trim([co])	
 CountryCode	Direct	countryCode	
 CountryLetterCode	Expression	Trim([c])	
 Department	Expression	Trim([department])	
 Description	Expression	Left(Trim([description]), 448)	
 DisplayName	Expression	IIF(IsPresent([displayName]), [displayName], [cn])	
 DLMemRejectPerms	Direct	dLMemRejectPerms	
 DLMemSubmitPerms	Direct	dLMemSubmitPerms	
 DnsDomainName	Constant	%DomainFQDN%	
 ExtensionAttribute1	Expression	Trim([extensionAttribute1])	
 ExtensionAttribute10	Expression	Trim([extensionAttribute10])	
 ExtensionAttribute11	Expression	Trim([extensionAttribute11])	

 ExtensionAttribute12	Expression	Trim([extensionAttribute12])	
 ExtensionAttribute13	Expression	Trim([extensionAttribute13])	
 ExtensionAttribute14	Expression	Trim([extensionAttribute14])	
 ExtensionAttribute15	Expression	Trim([extensionAttribute15])	
 ExtensionAttribute2	Expression	Trim([extensionAttribute2])	
 ExtensionAttribute3	Expression	Trim([extensionAttribute3])	
 ExtensionAttribute4	Expression	Trim([extensionAttribute4])	
 ExtensionAttribute5	Expression	Trim([extensionAttribute5])	
 ExtensionAttribute6	Expression	Trim([extensionAttribute6])	
 ExtensionAttribute7	Expression	Trim([extensionAttribute7])	
 ExtensionAttribute8	Expression	Trim([extensionAttribute8])	
 ExtensionAttribute9	Expression	Trim([extensionAttribute9])	
 FacsimileTelephoneNumber	Expression	Trim([facsimileTelephoneNumber])	
 GivenName	Expression	Trim([givenName])	
 HomePhone	Expression	Trim([homePhone])	
 Info	Expression	Left(Trim([info]), 448)	
 Initials	Expression	Trim([initials])	
 IPPhone	Expression	Trim([ipPhone])	
 LegacyExchangeDN	Direct	legacyExchangeDN	
 Mail	Expression	Trim([mail])	
 Manager	Direct	manager	

 MiddleName	Expression	Trim([middleName])	
 Mobile	Expression	Trim([mobile])	
 MSDSHABSeniorityIndex	Direct	msDS-HABSeniorityIndex	
 MSDSPhoneticDisplayName	Direct	msDS-PhoneticDisplayName	
 MSExchAssistantName	Direct	msExchAssistantName	
 MSExchBlockedSendersHash	Direct	msExchBlockedSendersHash	
 MSExchExtensionCustomAttribute1	Expression	Trim([msExchExtensionCustomAttribute1])	
 MSExchExtensionCustomAttribute2	Expression	Trim([msExchExtensionCustomAttribute2])	
 MSExchExtensionCustomAttribute3	Expression	Trim([msExchExtensionCustomAttribute3])	
 MSExchExtensionCustomAttribute4	Expression	Trim([msExchExtensionCustomAttribute4])	
 MSExchExtensionCustomAttribute5	Expression	Trim([msExchExtensionCustomAttribute5])	
 MSExchHideFromAddressLists	Direct	msExchHideFromAddressLists	
 MSExchLitigationHoldDate	Direct	msExchLitigationHoldDate	
 MSExchLitigationHoldOwner	Direct	msExchLitigationHoldOwner	
 MSExchModeratedByLink	Direct	msExchModeratedByLink	
 MSExchModerationFlags	Direct	msExchModerationFlags	
 MSExchRecipientDisplayType	Direct	msExchRecipientDisplayType	
 MSExchRecipientTypeDetails	Direct	msExchRecipientTypeDetails	
 MSExchRequireAuthToSendTo	Direct	msExchRequireAuthToSendTo	
 MSExchRetentionComment	Direct	msExchRetentionComment	
 MSExchRetentionUrl	Direct	msExchRetentionURL	

 MExchSafeRecipientsHash	Direct	msExchSafeRecipientsHash	
 MExchSafeSendersHash	Direct	msExchSafeSendersHash	
 MExchSenderHintTranslations	Direct	msExchSenderHintTranslations	
 MSRtcSipPrimaryUserAddress	Direct	msRTCSIP-PrimaryUserAddress	
 OnPremisesObjectIdentifier	Direct	objectGUID	
 OtherFacsimileTelephoneNumber	Expression	Trim([otherFacsimileTelephoneNumber])	
 OtherHomePhone	Expression	Trim([otherHomePhone])	
 OtherIPPhone	Expression	Trim([otherIpPhone])	
 OtherMobile	Expression	Trim([otherMobile])	
 OtherPager	Expression	Trim([otherPager])	
 OtherTelephone	Expression	Trim([otherTelephone])	
 Pager	Expression	Trim([pager])	
 PhysicalDeliveryOfficeName	Expression	Trim([physicalDeliveryOfficeName])	
 PostalCode	Expression	Trim([postalCode])	
 PostOfficeBox	Expression	IIF(IsPresent([postOfficeBox]), Left(Trim(Item([postOfficeBox], 1)), 448), "")	
 ProxyAddresses	Expression	RemoveDuplicates(Trim([proxyAddresses]))	
 PublicDelegates	Direct	publicDelegates	
 SourceAnchor	Expression	IIF(IsPresent([mS-DS-ConsistencyGuid]), [mS-DS-ConsistencyGuid], [objectGUID])	
 State	Expression	Trim([st])	
 StreetAddress	Expression	Trim([streetAddress])	
 Surname	Expression	Trim([sn])	

 TargetAddress	Direct	targetAddress	
 TelephoneNumber	Expression	Trim([telephoneNumber])	
 ThumbnailPhoto	Direct	thumbnailPhoto	
 Title	Expression	Trim([title])	
 UnauthOrig	Direct	unauthOrig	
 Url	Expression	IIF(IsPresent([url]), Left(Trim(Item([url], 1)), 448), "")	
 UserCertificate	Direct	userCertificate	
 UserSMIMECertificate	Direct	userSMIMECertificate	
 WwwHomepage	Direct	wWWHomePage	

group

Object mappings in Microsoft Entra Cloud Sync define how attributes from on-premises Active Directory objects (such as users or groups) are matched, transformed, and synchronized with their corresponding objects in Entra ID, and where supported, how selected attributes flow back from Entra ID to Active Directory.

 General

Source Object Name	group
Target Object Name	Group
Enabled	True

group Attribute Mappings

Attribute mappings in Microsoft Entra Cloud Sync define how attributes from the specified on-premises Active Directory object are matched, transformed, and synchronized with their corresponding objects in Entra ID, and where supported, how selected attributes flow back from Entra ID to Active Directory.

63 Attribute Mappings

Target Attribute Name	Source Type	Source Value	Default Value
 Alias	Direct	mailNickname	
 AuthOrig	Direct	authOrig	
 CommonName	Direct	cn	
 Description	Expression	Left(Trim([description]), 448)	
 DisplayName	Expression	IIF(IsPresent([displayName]), [displayName], [cn])	
 DLMemRejectPerms	Direct	dLMemRejectPerms	
 DLMemSubmitPerms	Direct	dLMemSubmitPerms	
 DnsDomainName	Constant	%DomainFQDN%	
 ExtensionAttribute1	Expression	Trim([extensionAttribute1])	
 ExtensionAttribute10	Expression	Trim([extensionAttribute10])	
 ExtensionAttribute11	Expression	Trim([extensionAttribute11])	
 ExtensionAttribute12	Expression	Trim([extensionAttribute12])	
 ExtensionAttribute13	Expression	Trim([extensionAttribute13])	
 ExtensionAttribute14	Expression	Trim([extensionAttribute14])	
 ExtensionAttribute15	Expression	Trim([extensionAttribute15])	
 ExtensionAttribute2	Expression	Trim([extensionAttribute2])	
 ExtensionAttribute3	Expression	Trim([extensionAttribute3])	

 ExtensionAttribute4	Expression	Trim([extensionAttribute4])	
 ExtensionAttribute5	Expression	Trim([extensionAttribute5])	
 ExtensionAttribute6	Expression	Trim([extensionAttribute6])	
 ExtensionAttribute7	Expression	Trim([extensionAttribute7])	
 ExtensionAttribute8	Expression	Trim([extensionAttribute8])	
 ExtensionAttribute9	Expression	Trim([extensionAttribute9])	
 HideDLMembership	Direct	hideDLMembership	
 Info	Expression	Left(Trim([info]), 448)	
 LegacyExchangeDN	Direct	legacyExchangeDN	
 Mail	Direct	mail	
 ManagedBy	Direct	managedBy	
 Member	Direct	member	
 MSDSHABSeniorityIndex	Direct	msDS-HABSeniorityIndex	
 MSDSPhoneticDisplayName	Direct	msDS-PhoneticDisplayName	
 MSExchBypassModerationLink	Direct	msExchBypassModerationLink	
 MSExchCoManagedByLink	Direct	msExchCoManagedByLink	
 MSExchEnableModeration	Direct	msExchEnableModeration	
 MSExchExtensionCustomAttribute1	Expression	Trim([msExchExtensionCustomAttribute1])	
 MSExchExtensionCustomAttribute2	Expression	Trim([msExchExtensionCustomAttribute2])	
 MSExchExtensionCustomAttribute3	Expression	Trim([msExchExtensionCustomAttribute3])	
 MSExchExtensionCustomAttribute4	Expression	Trim([msExchExtensionCustomAttribute4])	

 MSEchExtensionCustomAttribute5	Expression	Trim([msExchExtensionCustomAttribute5])	
 MSEchHideFromAddressLists	Direct	msExchHideFromAddressLists	
 MSEchLitigationHoldDate	Direct	msExchLitigationHoldDate	
 MSEchLitigationHoldOwner	Direct	msExchLitigationHoldOwner	
 MSEchModeratedByLink	Direct	msExchModeratedByLink	
 MSEchModerationFlags	Direct	msExchModerationFlags	
 MSEchRecipientDisplayType	Direct	msExchRecipientDisplayType	
 MSEchRecipientTypeDetails	Direct	msExchRecipientTypeDetails	
 MSEchRequireAuthToSendTo	Direct	msExchRequireAuthToSendTo	
 MSEchRetentionComment	Direct	msExchRetentionComment	
 MSEchRetentionUrl	Direct	msExchRetentionURL	
 MSEchSenderHintTranslations	Direct	msExchSenderHintTranslations	
 MSOrgIsOrganizational	Direct	msOrg-IsOrganizational	
 NetBiosName	Constant	%DomainNetBios%	
 OnPremiseSecurityIdentifier	Direct	objectSid	
 OnPremisesObjectIdentifier	Direct	objectGUID	
 OnPremisesSamAccountName	Direct	sAMAccountName	
 OofReplyToOriginator	Direct	oOFReplyToOriginator	
 ProxyAddresses	Expression	RemoveDuplicates(Trim([proxyAddresses]))	
 PublicDelegates	Direct	publicDelegates	
 ReportToOriginator	Direct	reportToOriginator	

 ReportToOwner	Direct	reportToOwner	
 SecurityEnabled	Expression	CBool(BitAnd([groupType], -2147483648))	
 SourceAnchor	Expression	IIF(IsPresent([mS-DS-ConsistencyGuid]), [mS-DS-ConsistencyGuid], [objectGUID])	
 UnauthOrig	Direct	unauthOrig	

inetOrgPerson

Object mappings in Microsoft Entra Cloud Sync define how attributes from on-premises Active Directory objects (such as users or groups) are matched, transformed, and synchronized with their corresponding objects in Entra ID, and where supported, how selected attributes flow back from Entra ID to Active Directory.

 General

Source Object Name	inetOrgPerson
Target Object Name	User
Enabled	True

inetOrgPerson Attribute Mappings

Attribute mappings in Microsoft Entra Cloud Sync define how attributes from the specified on-premises Active Directory object are matched, transformed, and synchronized with their corresponding objects in Entra ID, and where supported, how selected attributes flow back from Entra ID to Active Directory.

138 Attribute Mappings

Target Attribute Name	Source Type	Source Value	Default Value
 AccountEnabled	Expression	IIF(IsPresent([userAccountControl]), IIF(BitAnd([userAccountControl], 2)="0", "True", "False"), Not([accountDisabled]))	
 Alias	Direct	mailNickname	
 AltRecipient	Direct	altRecipient	
 Assistant	Direct	assistant	
 AuthOrig	Direct	authOrig	
 City	Expression	Trim([l])	
 CommonName	Direct	cn	
 Company	Expression	Trim([company])	
 Country	Expression	Trim([co])	
 CountryCode	Expression	IgnoreFlowIfNullOrEmpty([countryCode])	
 CountryLetterCode	Expression	Trim([c])	
 CredentialData	Direct	PasswordHash	
 Department	Expression	Trim([department])	
 Description	Expression	Left(Trim([description]), 448)	
 DisplayName	Expression	IIF(IsPresent([displayName]), [displayName], [cn])	
 DLMemRejectPerms	Direct	dLMemRejectPerms	

 DLMemSubmitPerms	Direct	dLMemSubmitPerms	
 DnsDomainName	Constant	%DomainFQDN%	
 EmployeeId	Direct	employeeId	
 EmployeeType	Direct	employeeType	
 ExtensionAttribute1	Expression	Trim([extensionAttribute1])	
 ExtensionAttribute10	Expression	Trim([extensionAttribute10])	
 ExtensionAttribute11	Expression	Trim([extensionAttribute11])	
 ExtensionAttribute12	Expression	Trim([extensionAttribute12])	
 ExtensionAttribute13	Expression	Trim([extensionAttribute13])	
 ExtensionAttribute14	Expression	Trim([extensionAttribute14])	
 ExtensionAttribute15	Expression	Trim([extensionAttribute15])	
 ExtensionAttribute2	Expression	Trim([extensionAttribute2])	
 ExtensionAttribute3	Expression	Trim([extensionAttribute3])	
 ExtensionAttribute4	Expression	Trim([extensionAttribute4])	
 ExtensionAttribute5	Expression	Trim([extensionAttribute5])	
 ExtensionAttribute6	Expression	Trim([extensionAttribute6])	
 ExtensionAttribute7	Expression	Trim([extensionAttribute7])	
 ExtensionAttribute8	Expression	Trim([extensionAttribute8])	
 ExtensionAttribute9	Expression	Trim([extensionAttribute9])	
 FacsimileTelephoneNumber	Expression	Trim([facsimileTelephoneNumber])	
 GivenName	Expression	Trim([givenName])	

 HomePhone	Expression	Trim([homePhone])	
 Info	Expression	Left(Trim([info]), 448)	
 Initials	Expression	Trim([initials])	
 IPPhone	Expression	Trim([ipPhone])	
 LastPasswordChangeTimestamp	Expression	IIF(IsPresent([pwdLastSet]), FormatDateTime(DateFromNum([pwdLastSet]), "RoundtripKind", , "yyyyMMddHHmmss.OZ"),)	
 LegacyExchangeDN	Direct	legacyExchangeDN	
 Mail	Expression	Trim([mail])	
 Manager	Direct	manager	
 MiddleName	Expression	Trim([middleName])	
 Mobile	Expression	Trim([mobile])	
 MSDSHABSeniorityIndex	Direct	msDS-HABSeniorityIndex	
 MSDSPhoneticDisplayName	Direct	msDS-PhoneticDisplayName	
 MSExchArchiveGuid	Direct	msExchArchiveGUID	
 MSExchArchiveName	Direct	msExchArchiveName	
 MSExchAssistantName	Direct	msExchAssistantName	
 MSExchAuditAdmin	Direct	msExchAuditAdmin	
 MSExchAuditDelegate	Direct	msExchAuditDelegate	
 MSExchAuditDelegateAdmin	Direct	msExchAuditDelegateAdmin	
 MSExchAuditOwner	Direct	msExchAuditOwner	
 MSExchBlockedSendersHash	Direct	msExchBlockedSendersHash	
 MSExchBypassAudit	Direct	msExchBypassAudit	

 MSEchDelegateListLink	Direct	msExchDelegateListLink	
 MSEchElcExpirySuspensionEnd	Direct	msExchELCExpirySuspensionEnd	
 MSEchElcExpirySuspensionStart	Direct	msExchELCExpirySuspensionStart	
 MSEchElcMailboxFlags	Direct	msExchELCMailboxFlags	
 MSEchEnableModeration	Direct	msExchEnableModeration	
 MSEchExtensionCustomAttribute1	Expression	Trim([msExchExtensionCustomAttribute1])	
 MSEchExtensionCustomAttribute2	Expression	Trim([msExchExtensionCustomAttribute2])	
 MSEchExtensionCustomAttribute3	Expression	Trim([msExchExtensionCustomAttribute3])	
 MSEchExtensionCustomAttribute4	Expression	Trim([msExchExtensionCustomAttribute4])	
 MSEchExtensionCustomAttribute5	Expression	Trim([msExchExtensionCustomAttribute5])	
 MSEchHideFromAddressLists	Direct	msExchHideFromAddressLists	
 MSEchImmutableId	Direct	msExchImmutableId	
 MSEchLitigationHoldDate	Direct	msExchLitigationHoldDate	
 MSEchLitigationHoldOwner	Direct	msExchLitigationHoldOwner	
 MSEchMailboxAuditEnable	Direct	msExchMailboxAuditEnable	
 MSEchMailboxAuditLogAgeLimit	Direct	msExchMailboxAuditLogAgeLimit	
 MSEchMailboxGuid	Direct	msExchMailboxGuid	
 MSEchModeratedByLink	Direct	msExchModeratedByLink	
 MSEchModerationFlags	Direct	msExchModerationFlags	
 MSEchRecipientDisplayType	Direct	msExchRecipientDisplayType	
 MSEchRecipientTypeDetails	Direct	msExchRecipientTypeDetails	

 MSEchRemoteRecipientType	Direct	msExchRemoteRecipientType	
 MSEchRequireAuthToSendTo	Direct	msExchRequireAuthToSendTo	
 MSEchResourceCapacity	Direct	msExchResourceCapacity	
 MSEchResourceDisplay	Direct	msExchResourceDisplay	
 MSEchResourceMetadata	Direct	msExchResourceMetaData	
 MSEchResourceSearchProperties	Direct	msExchResourceSearchProperties	
 MSEchRetentionComment	Direct	msExchRetentionComment	
 MSEchRetentionUrl	Direct	msExchRetentionURL	
 MSEchSafeRecipientsHash	Direct	msExchSafeRecipientsHash	
 MSEchSafeSendersHash	Direct	msExchSafeSendersHash	
 MSEchSenderHintTranslations	Direct	msExchSenderHintTranslations	
 MSEchTeamMailboxExpiration	Direct	msExchTeamMailboxExpiration	
 MSEchTeamMailboxOwners	Direct	msExchTeamMailboxOwners	
 MSEchTeamMailboxSharePointLinkedBy	Direct	msExchTeamMailboxSharePointLinkedBy	
 MSEchTeamMailboxSharePointUrl	Direct	msExchTeamMailboxSharePointUrl	
 MSEchUserHoldPolicies	Direct	msExchUserHoldPolicies	
 MSRtcSipApplicationOptions	Direct	msRTCSIP-ApplicationOptions	
 MSRtcSipDeploymentLocator	Direct	msRTCSIP-DeploymentLocator	
 MSRtcSipLine	Direct	msRTCSIP-Line	
 MSRtcSipOptionFlags	Direct	msRTCSIP-OptionFlags	
 MSRtcSipOwnerUrn	Direct	msRTCSIP-OwnerUrn	

 MSRtcSipPrimaryUserAddress	Direct	msRTCSIP-PrimaryUserAddress	
 MSRtcSipUserEnabled	Direct	msRTCSIP-UserEnabled	
 NetBiosName	Constant	%DomainNetBios%	
 OnPremisesDistinguishedName	Direct	distinguishedName	
 OnPremiseSecurityIdentifier	Direct	objectSid	
 OnPremisesObjectIdentifier	Direct	objectGUID	
 OnPremisesSamAccountName	Direct	sAMAccountName	
 OnPremisesUserPrincipalName	Expression	IIF(IsPresent([userPrincipalName]), [userPrincipalName], IIF(IsPresent([sAMAccountName]), Join("@", [sAMAccountName], %DomainFQDN%), Error("AccountName is not present"))))	
 OtherFacsimileTelephoneNumber	Expression	Trim([otherFacsimileTelephoneNumber])	
 OtherHomePhone	Expression	Trim([otherHomePhone])	
 OtherIPPhone	Expression	Trim([otherIpPhone])	
 OtherMobile	Expression	Trim([otherMobile])	
 OtherPager	Expression	Trim([otherPager])	
 OtherTelephone	Expression	Trim([otherTelephone])	
 Pager	Expression	Trim([pager])	
 PhysicalDeliveryOfficeName	Expression	Trim([physicalDeliveryOfficeName])	
 PostalCode	Expression	Trim([postalCode])	
 PostOfficeBox	Expression	IIF(IsPresent([postOfficeBox]), Left(Trim(Item([postOfficeBox], 1)), 448), "")	
 PreferredDataLocation	Direct	msDS-preferredDataLocation	
 PreferredLanguage	Expression	Trim([preferredLanguage])	
 ProxyAddresses	Expression	RemoveDuplicates(Trim([proxyAddresses]))	

 PublicDelegates	Direct	publicDelegates	
 SourceAnchor	Expression	IIF(IsPresent([mS-DS-ConsistencyGuid]), [mS-DS-ConsistencyGuid], [objectGUID])	
 State	Expression	Trim([st])	
 StreetAddress	Expression	Trim([streetAddress])	
 Surname	Expression	Trim([sn])	
 TargetAddress	Direct	targetAddress	
 TelephoneAssistant	Expression	Trim([telephoneAssistant])	
 TelephoneNumber	Expression	Trim([telephoneNumber])	
 ThumbnailPhoto	Direct	thumbnailPhoto	
 Title	Expression	Trim([title])	
 UnauthOrig	Direct	unauthOrig	
 Url	Expression	IIF(IsPresent([url]), Left(Trim(Item([url], 1)), 448), "")	
 UsageLocation	Expression	IgnoreFlowIfNullOrEmpty([msExchUsageLocation])	
 UserCertificate	Direct	userCertificate	
 UserPrincipalName	Expression	IIF(IsPresent([userPrincipalName]), [userPrincipalName], IIF(IsPresent([sAMAccountName]), Join("@", [sAMAccountName], %DomainFQDN%), Error("AccountName is not present")))	
 UserSMIMECertificate	Direct	userSMIMECertificate	
 WwwHomepage	Direct	wWWHomePage	

user

Object mappings in Microsoft Entra Cloud Sync define how attributes from on-premises Active Directory objects (such as users or groups) are matched, transformed, and synchronized with their corresponding objects in Entra ID, and where supported, how selected attributes flow back from Entra ID to Active Directory.

 General

Source Object Name	user
Target Object Name	User
Enabled	True

user Attribute Mappings

Attribute mappings in Microsoft Entra Cloud Sync define how attributes from the specified on-premises Active Directory object are matched, transformed, and synchronized with their corresponding objects in Entra ID, and where supported, how selected attributes flow back from Entra ID to Active Directory.

138 Attribute Mappings

Target Attribute Name	Source Type	Source Value	Default Value
 AccountEnabled	Expression	IIF(IsPresent([userAccountControl]), IIF(BitAnd([userAccountControl], 2)="0", "True", "False"), Not([accountDisabled]))	
 Alias	Direct	mailNickname	
 AltRecipient	Direct	altRecipient	
 Assistant	Direct	assistant	
 AuthOrig	Direct	authOrig	
 City	Expression	Trim([l])	
 CommonName	Direct	cn	
 Company	Expression	Trim([company])	
 Country	Expression	Trim([co])	
 CountryCode	Expression	IgnoreFlowIfNullOrEmpty([countryCode])	
 CountryLetterCode	Expression	Trim([c])	
 CredentialData	Direct	PasswordHash	
 Department	Expression	Trim([department])	
 Description	Expression	Left(Trim([description]), 448)	
 DisplayName	Expression	IIF(IsPresent([displayName]), [displayName], [cn])	
 DLMemRejectPerms	Direct	dLMemRejectPerms	

 DLMemSubmitPerms	Direct	dLMemSubmitPerms	
 DnsDomainName	Constant	%DomainFQDN%	
 EmployeeId	Direct	employeeId	
 EmployeeType	Direct	employeeType	
 ExtensionAttribute1	Expression	Trim([extensionAttribute1])	
 ExtensionAttribute10	Expression	Trim([extensionAttribute10])	
 ExtensionAttribute11	Expression	Trim([extensionAttribute11])	
 ExtensionAttribute12	Expression	Trim([extensionAttribute12])	
 ExtensionAttribute13	Expression	Trim([extensionAttribute13])	
 ExtensionAttribute14	Expression	Trim([extensionAttribute14])	
 ExtensionAttribute15	Expression	Trim([extensionAttribute15])	
 ExtensionAttribute2	Expression	Trim([extensionAttribute2])	
 ExtensionAttribute3	Expression	Trim([extensionAttribute3])	
 ExtensionAttribute4	Expression	Trim([extensionAttribute4])	
 ExtensionAttribute5	Expression	Trim([extensionAttribute5])	
 ExtensionAttribute6	Expression	Trim([extensionAttribute6])	
 ExtensionAttribute7	Expression	Trim([extensionAttribute7])	
 ExtensionAttribute8	Expression	Trim([extensionAttribute8])	
 ExtensionAttribute9	Expression	Trim([extensionAttribute9])	
 FacsimileTelephoneNumber	Expression	Trim([facsimileTelephoneNumber])	
 GivenName	Expression	Trim([givenName])	

 HomePhone	Expression	Trim([homePhone])	
 Info	Expression	Left(Trim([info]), 448)	
 Initials	Expression	Trim([initials])	
 IPPhone	Expression	Trim([ipPhone])	
 LastPasswordChangeTimestamp	Expression	IIF(IsPresent([pwdLastSet]), FormatDateTime(DateFromNum([pwdLastSet]), "RoundtripKind", , "yyyyMMddHHmmss.OZ"),)	
 LegacyExchangeDN	Direct	legacyExchangeDN	
 Mail	Expression	Trim([mail])	
 Manager	Direct	manager	
 MiddleName	Expression	Trim([middleName])	
 Mobile	Expression	Trim([mobile])	
 MSDSHABSeniorityIndex	Direct	msDS-HABSeniorityIndex	
 MSDSPhoneticDisplayName	Direct	msDS-PhoneticDisplayName	
 MSExchArchiveGuid	Direct	msExchArchiveGUID	
 MSExchArchiveName	Direct	msExchArchiveName	
 MSExchAssistantName	Direct	msExchAssistantName	
 MSExchAuditAdmin	Direct	msExchAuditAdmin	
 MSExchAuditDelegate	Direct	msExchAuditDelegate	
 MSExchAuditDelegateAdmin	Direct	msExchAuditDelegateAdmin	
 MSExchAuditOwner	Direct	msExchAuditOwner	
 MSExchBlockedSendersHash	Direct	msExchBlockedSendersHash	
 MSExchBypassAudit	Direct	msExchBypassAudit	

 MSEchDelegateListLink	Direct	msExchDelegateListLink	
 MSEchElcExpirySuspensionEnd	Direct	msExchELCExpirySuspensionEnd	
 MSEchElcExpirySuspensionStart	Direct	msExchELCExpirySuspensionStart	
 MSEchElcMailboxFlags	Direct	msExchELCMailboxFlags	
 MSEchEnableModeration	Direct	msExchEnableModeration	
 MSEchExtensionCustomAttribute1	Expression	Trim([msExchExtensionCustomAttribute1])	
 MSEchExtensionCustomAttribute2	Expression	Trim([msExchExtensionCustomAttribute2])	
 MSEchExtensionCustomAttribute3	Expression	Trim([msExchExtensionCustomAttribute3])	
 MSEchExtensionCustomAttribute4	Expression	Trim([msExchExtensionCustomAttribute4])	
 MSEchExtensionCustomAttribute5	Expression	Trim([msExchExtensionCustomAttribute5])	
 MSEchHideFromAddressLists	Direct	msExchHideFromAddressLists	
 MSEchImmutableId	Direct	msExchImmutableId	
 MSEchLitigationHoldDate	Direct	msExchLitigationHoldDate	
 MSEchLitigationHoldOwner	Direct	msExchLitigationHoldOwner	
 MSEchMailboxAuditEnable	Direct	msExchMailboxAuditEnable	
 MSEchMailboxAuditLogAgeLimit	Direct	msExchMailboxAuditLogAgeLimit	
 MSEchMailboxGuid	Direct	msExchMailboxGuid	
 MSEchModeratedByLink	Direct	msExchModeratedByLink	
 MSEchModerationFlags	Direct	msExchModerationFlags	
 MSEchRecipientDisplayType	Direct	msExchRecipientDisplayType	
 MSEchRecipientTypeDetails	Direct	msExchRecipientTypeDetails	

 MSEchRemoteRecipientType	Direct	msExchRemoteRecipientType	
 MSEchRequireAuthToSendTo	Direct	msExchRequireAuthToSendTo	
 MSEchResourceCapacity	Direct	msExchResourceCapacity	
 MSEchResourceDisplay	Direct	msExchResourceDisplay	
 MSEchResourceMetadata	Direct	msExchResourceMetaData	
 MSEchResourceSearchProperties	Direct	msExchResourceSearchProperties	
 MSEchRetentionComment	Direct	msExchRetentionComment	
 MSEchRetentionUrl	Direct	msExchRetentionURL	
 MSEchSafeRecipientsHash	Direct	msExchSafeRecipientsHash	
 MSEchSafeSendersHash	Direct	msExchSafeSendersHash	
 MSEchSenderHintTranslations	Direct	msExchSenderHintTranslations	
 MSEchTeamMailboxExpiration	Direct	msExchTeamMailboxExpiration	
 MSEchTeamMailboxOwners	Direct	msExchTeamMailboxOwners	
 MSEchTeamMailboxSharePointLinkedBy	Direct	msExchTeamMailboxSharePointLinkedBy	
 MSEchTeamMailboxSharePointUrl	Direct	msExchTeamMailboxSharePointUrl	
 MSEchUserHoldPolicies	Direct	msExchUserHoldPolicies	
 MSRtcSipApplicationOptions	Direct	msRTCSIP-ApplicationOptions	
 MSRtcSipDeploymentLocator	Direct	msRTCSIP-DeploymentLocator	
 MSRtcSipLine	Direct	msRTCSIP-Line	
 MSRtcSipOptionFlags	Direct	msRTCSIP-OptionFlags	
 MSRtcSipOwnerUrn	Direct	msRTCSIP-OwnerUrn	

 MSRtcSipPrimaryUserAddress	Direct	msRTCSIP-PrimaryUserAddress	
 MSRtcSipUserEnabled	Direct	msRTCSIP-UserEnabled	
 NetBiosName	Constant	%DomainNetBios%	
 OnPremisesDistinguishedName	Direct	distinguishedName	
 OnPremiseSecurityIdentifier	Direct	objectSid	
 OnPremisesObjectIdentifier	Direct	objectGUID	
 OnPremisesSamAccountName	Direct	sAMAccountName	
 OnPremisesUserPrincipalName	Expression	IIF(IsPresent([userPrincipalName]), [userPrincipalName], IIF(IsPresent([sAMAccountName]), Join("@", [sAMAccountName], %DomainFQDN%), Error("AccountName is not present"))))	
 OtherFacsimileTelephoneNumber	Expression	Trim([otherFacsimileTelephoneNumber])	
 OtherHomePhone	Expression	Trim([otherHomePhone])	
 OtherIPPhone	Expression	Trim([otherIpPhone])	
 OtherMobile	Expression	Trim([otherMobile])	
 OtherPager	Expression	Trim([otherPager])	
 OtherTelephone	Expression	Trim([otherTelephone])	
 Pager	Expression	Trim([pager])	
 PhysicalDeliveryOfficeName	Expression	Trim([physicalDeliveryOfficeName])	
 PostalCode	Expression	Trim([postalCode])	
 PostOfficeBox	Expression	IIF(IsPresent([postOfficeBox]), Left(Trim(Item([postOfficeBox], 1)), 448), "")	
 PreferredDataLocation	Direct	msDS-preferredDataLocation	
 PreferredLanguage	Expression	Trim([preferredLanguage])	
 ProxyAddresses	Expression	RemoveDuplicates(Trim([proxyAddresses]))	

 PublicDelegates	Direct	publicDelegates	
 SourceAnchor	Expression	IIF(IsPresent([mS-DS-ConsistencyGuid]), [mS-DS-ConsistencyGuid], [objectGUID])	
 State	Expression	Trim([st])	
 StreetAddress	Expression	Trim([streetAddress])	
 Surname	Expression	Trim([sn])	
 TargetAddress	Direct	targetAddress	
 TelephoneAssistant	Expression	Trim([telephoneAssistant])	
 TelephoneNumber	Expression	Trim([telephoneNumber])	
 ThumbnailPhoto	Direct	thumbnailPhoto	
 Title	Expression	Trim([title])	
 UnauthOrig	Direct	unauthOrig	
 Url	Expression	IIF(IsPresent([url]), Left(Trim(Item([url], 1)), 448), "")	
 UsageLocation	Expression	IgnoreFlowIfNullOrEmpty([msExchUsageLocation])	
 UserCertificate	Direct	userCertificate	
 UserPrincipalName	Expression	IIF(IsPresent([userPrincipalName]), [userPrincipalName], IIF(IsPresent([sAMAccountName]), Join("@", [sAMAccountName], %DomainFQDN%), Error("AccountName is not present")))	
 UserSMIMECertificate	Direct	userSMIMECertificate	
 WwwHomepage	Direct	wWWHomePage	

emea.centrelsolutionsdemo.int (AD to Microsoft Entra ID)

Cloud Sync configurations define which objects and attributes are in scope for synchronization, controlling how users, groups, and contacts flow from Active Directory to Entra ID - and, where supported, how selected attributes can flow back from Entra ID to Active Directory.

General

Configuration Type	AD to Microsoft Entra ID
Domain Name	emea.centrelsolutionsdemo.int
Service Principal Identifier	f07b2721-e57c-4a6f-b686-22f857537170
Status	Disabled

Domain Information

Information is not available for this section because the object does not support the providing of this information or it is not relevant to this object.

Settings

Email Notifications	True
Email Notifications Recipient	
Prevent Accidental Deletion	True
Accidental Deletion Threshold	500
Exchange Hybrid Writeback	False
Password Hash Sync	True

1 Agents

Machine Name	External IP Address	Status	Resources
 CSDEMO-DC03.emea.centrelsolutionsdemo.int	81.109.64.92	Inactive	emea.centrelsolutionsdemo.int

2 Job Statuses

Display Name	Status	Last Run Date/Time
 Password hash sync	Paused	[Not Configured]
 User and group sync	Paused	[Not Configured]

Scoping Filters

Scoping filters in Microsoft Entra Cloud Sync are conditional rules that determine which directory objects are included in a given sync flow.

 Scoping Filters

Filter Type	All users
-------------	-----------

Object Mappings

Object mappings in Microsoft Entra Cloud Sync define how attributes from on-premises Active Directory objects (such as users or groups) are matched, transformed, and synchronized with their corresponding objects in Entra ID, and where supported, how selected attributes flow back from Entra ID to Active Directory.

4 Object Mappings

Source Object Name	Target Object Name	Enabled
 contact	Contact	True
 group	Group	True
 inetOrgPerson	User	True
 user	User	True

contact

Object mappings in Microsoft Entra Cloud Sync define how attributes from on-premises Active Directory objects (such as users or groups) are matched, transformed, and synchronized with their corresponding objects in Entra ID, and where supported, how selected attributes flow back from Entra ID to Active Directory.

 General

Source Object Name	contact
Target Object Name	Contact
Enabled	True

contact Attribute Mappings

Attribute mappings in Microsoft Entra Cloud Sync define how attributes from the specified on-premises Active Directory object are matched, transformed, and synchronized with their corresponding objects in Entra ID, and where supported, how selected attributes flow back from Entra ID to Active Directory.

89 Attribute Mappings

Target Attribute Name	Source Type	Source Value	Default Value
 Alias	Direct	mailNickname	
 Assistant	Direct	assistant	
 AuthOrig	Direct	authOrig	
 City	Expression	Trim([l])	
 Company	Expression	Trim([company])	
 Country	Expression	Trim([co])	
 CountryCode	Direct	countryCode	
 CountryLetterCode	Expression	Trim([c])	
 Department	Expression	Trim([department])	
 Description	Expression	Left(Trim([description]), 448)	
 DisplayName	Expression	IIF(IsPresent([displayName]), [displayName], [cn])	
 DLMemRejectPerms	Direct	dLMemRejectPerms	
 DLMemSubmitPerms	Direct	dLMemSubmitPerms	
 DnsDomainName	Constant	%DomainFQDN%	
 ExtensionAttribute1	Expression	Trim([extensionAttribute1])	
 ExtensionAttribute10	Expression	Trim([extensionAttribute10])	
 ExtensionAttribute11	Expression	Trim([extensionAttribute11])	

 ExtensionAttribute12	Expression	Trim([extensionAttribute12])	
 ExtensionAttribute13	Expression	Trim([extensionAttribute13])	
 ExtensionAttribute14	Expression	Trim([extensionAttribute14])	
 ExtensionAttribute15	Expression	Trim([extensionAttribute15])	
 ExtensionAttribute2	Expression	Trim([extensionAttribute2])	
 ExtensionAttribute3	Expression	Trim([extensionAttribute3])	
 ExtensionAttribute4	Expression	Trim([extensionAttribute4])	
 ExtensionAttribute5	Expression	Trim([extensionAttribute5])	
 ExtensionAttribute6	Expression	Trim([extensionAttribute6])	
 ExtensionAttribute7	Expression	Trim([extensionAttribute7])	
 ExtensionAttribute8	Expression	Trim([extensionAttribute8])	
 ExtensionAttribute9	Expression	Trim([extensionAttribute9])	
 FacsimileTelephoneNumber	Expression	Trim([facsimileTelephoneNumber])	
 GivenName	Expression	Trim([givenName])	
 HomePhone	Expression	Trim([homePhone])	
 Info	Expression	Left(Trim([info]), 448)	
 Initials	Expression	Trim([initials])	
 IPPhone	Expression	Trim([ipPhone])	
 LegacyExchangeDN	Direct	legacyExchangeDN	
 Mail	Expression	Trim([mail])	
 Manager	Direct	manager	

 MiddleName	Expression	Trim([middleName])	
 Mobile	Expression	Trim([mobile])	
 MSDSHABSeniorityIndex	Direct	msDS-HABSeniorityIndex	
 MSDSPhoneticDisplayName	Direct	msDS-PhoneticDisplayName	
 MSExchAssistantName	Direct	msExchAssistantName	
 MSExchBlockedSendersHash	Direct	msExchBlockedSendersHash	
 MSExchExtensionCustomAttribute1	Expression	Trim([msExchExtensionCustomAttribute1])	
 MSExchExtensionCustomAttribute2	Expression	Trim([msExchExtensionCustomAttribute2])	
 MSExchExtensionCustomAttribute3	Expression	Trim([msExchExtensionCustomAttribute3])	
 MSExchExtensionCustomAttribute4	Expression	Trim([msExchExtensionCustomAttribute4])	
 MSExchExtensionCustomAttribute5	Expression	Trim([msExchExtensionCustomAttribute5])	
 MSExchHideFromAddressLists	Direct	msExchHideFromAddressLists	
 MSExchLitigationHoldDate	Direct	msExchLitigationHoldDate	
 MSExchLitigationHoldOwner	Direct	msExchLitigationHoldOwner	
 MSExchModeratedByLink	Direct	msExchModeratedByLink	
 MSExchModerationFlags	Direct	msExchModerationFlags	
 MSExchRecipientDisplayType	Direct	msExchRecipientDisplayType	
 MSExchRecipientTypeDetails	Direct	msExchRecipientTypeDetails	
 MSExchRequireAuthToSendTo	Direct	msExchRequireAuthToSendTo	
 MSExchRetentionComment	Direct	msExchRetentionComment	
 MSExchRetentionUrl	Direct	msExchRetentionURL	

 MExchSafeRecipientsHash	Direct	msExchSafeRecipientsHash	
 MExchSafeSendersHash	Direct	msExchSafeSendersHash	
 MExchSenderHintTranslations	Direct	msExchSenderHintTranslations	
 MSRtcSipPrimaryUserAddress	Direct	msRTCSIP-PrimaryUserAddress	
 OnPremisesObjectIdentifier	Direct	objectGUID	
 OtherFacsimileTelephoneNumber	Expression	Trim([otherFacsimileTelephoneNumber])	
 OtherHomePhone	Expression	Trim([otherHomePhone])	
 OtherIPPhone	Expression	Trim([otherIpPhone])	
 OtherMobile	Expression	Trim([otherMobile])	
 OtherPager	Expression	Trim([otherPager])	
 OtherTelephone	Expression	Trim([otherTelephone])	
 Pager	Expression	Trim([pager])	
 PhysicalDeliveryOfficeName	Expression	Trim([physicalDeliveryOfficeName])	
 PostalCode	Expression	Trim([postalCode])	
 PostOfficeBox	Expression	IIF(IsPresent([postOfficeBox]), Left(Trim(Item([postOfficeBox], 1)), 448), "")	
 ProxyAddresses	Expression	RemoveDuplicates(Trim([proxyAddresses]))	
 PublicDelegates	Direct	publicDelegates	
 SourceAnchor	Expression	IIF(IsPresent([mS-DS-ConsistencyGuid]), [mS-DS-ConsistencyGuid], [objectGUID])	
 State	Expression	Trim([st])	
 StreetAddress	Expression	Trim([streetAddress])	
 Surname	Expression	Trim([sn])	

 TargetAddress	Direct	targetAddress	
 TelephoneNumber	Expression	Trim([telephoneNumber])	
 ThumbnailPhoto	Direct	thumbnailPhoto	
 Title	Expression	Trim([title])	
 UnauthOrig	Direct	unauthOrig	
 Url	Expression	IIF(IsPresent([url]), Left(Trim(Item([url], 1)), 448), "")	
 UserCertificate	Direct	userCertificate	
 UserSMIMECertificate	Direct	userSMIMECertificate	
 WwwHomepage	Direct	wWWHomePage	

group

Object mappings in Microsoft Entra Cloud Sync define how attributes from on-premises Active Directory objects (such as users or groups) are matched, transformed, and synchronized with their corresponding objects in Entra ID, and where supported, how selected attributes flow back from Entra ID to Active Directory.

 General

Source Object Name	group
Target Object Name	Group
Enabled	True

group Attribute Mappings

Attribute mappings in Microsoft Entra Cloud Sync define how attributes from the specified on-premises Active Directory object are matched, transformed, and synchronized with their corresponding objects in Entra ID, and where supported, how selected attributes flow back from Entra ID to Active Directory.

63 Attribute Mappings

Target Attribute Name	Source Type	Source Value	Default Value
 Alias	Direct	mailNickname	
 AuthOrig	Direct	authOrig	
 CommonName	Direct	cn	
 Description	Expression	Left(Trim([description]), 448)	
 DisplayName	Expression	IIF(IsPresent([displayName]), [displayName], [cn])	
 DLMemRejectPerms	Direct	dLMemRejectPerms	
 DLMemSubmitPerms	Direct	dLMemSubmitPerms	
 DnsDomainName	Constant	%DomainFQDN%	
 ExtensionAttribute1	Expression	Trim([extensionAttribute1])	
 ExtensionAttribute10	Expression	Trim([extensionAttribute10])	
 ExtensionAttribute11	Expression	Trim([extensionAttribute11])	
 ExtensionAttribute12	Expression	Trim([extensionAttribute12])	
 ExtensionAttribute13	Expression	Trim([extensionAttribute13])	
 ExtensionAttribute14	Expression	Trim([extensionAttribute14])	
 ExtensionAttribute15	Expression	Trim([extensionAttribute15])	
 ExtensionAttribute2	Expression	Trim([extensionAttribute2])	
 ExtensionAttribute3	Expression	Trim([extensionAttribute3])	

 ExtensionAttribute4	Expression	Trim([extensionAttribute4])	
 ExtensionAttribute5	Expression	Trim([extensionAttribute5])	
 ExtensionAttribute6	Expression	Trim([extensionAttribute6])	
 ExtensionAttribute7	Expression	Trim([extensionAttribute7])	
 ExtensionAttribute8	Expression	Trim([extensionAttribute8])	
 ExtensionAttribute9	Expression	Trim([extensionAttribute9])	
 HideDLMembership	Direct	hideDLMembership	
 Info	Expression	Left(Trim([info]), 448)	
 LegacyExchangeDN	Direct	legacyExchangeDN	
 Mail	Direct	mail	
 ManagedBy	Direct	managedBy	
 Member	Direct	member	
 MSDSHABSeniorityIndex	Direct	msDS-HABSeniorityIndex	
 MSDSPhoneticDisplayName	Direct	msDS-PhoneticDisplayName	
 MSExchBypassModerationLink	Direct	msExchBypassModerationLink	
 MSExchCoManagedByLink	Direct	msExchCoManagedByLink	
 MSExchEnableModeration	Direct	msExchEnableModeration	
 MSExchExtensionCustomAttribute1	Expression	Trim([msExchExtensionCustomAttribute1])	
 MSExchExtensionCustomAttribute2	Expression	Trim([msExchExtensionCustomAttribute2])	
 MSExchExtensionCustomAttribute3	Expression	Trim([msExchExtensionCustomAttribute3])	
 MSExchExtensionCustomAttribute4	Expression	Trim([msExchExtensionCustomAttribute4])	

 MSEchExtensionCustomAttribute5	Expression	Trim([msExchExtensionCustomAttribute5])	
 MSEchHideFromAddressLists	Direct	msExchHideFromAddressLists	
 MSEchLitigationHoldDate	Direct	msExchLitigationHoldDate	
 MSEchLitigationHoldOwner	Direct	msExchLitigationHoldOwner	
 MSEchModeratedByLink	Direct	msExchModeratedByLink	
 MSEchModerationFlags	Direct	msExchModerationFlags	
 MSEchRecipientDisplayType	Direct	msExchRecipientDisplayType	
 MSEchRecipientTypeDetails	Direct	msExchRecipientTypeDetails	
 MSEchRequireAuthToSendTo	Direct	msExchRequireAuthToSendTo	
 MSEchRetentionComment	Direct	msExchRetentionComment	
 MSEchRetentionUrl	Direct	msExchRetentionURL	
 MSEchSenderHintTranslations	Direct	msExchSenderHintTranslations	
 MSOrgIsOrganizational	Direct	msOrg-IsOrganizational	
 NetBiosName	Constant	%DomainNetBios%	
 OnPremiseSecurityIdentifier	Direct	objectSid	
 OnPremisesObjectIdentifier	Direct	objectGUID	
 OnPremisesSamAccountName	Direct	sAMAccountName	
 OofReplyToOriginator	Direct	oOFReplyToOriginator	
 ProxyAddresses	Expression	RemoveDuplicates(Trim([proxyAddresses]))	
 PublicDelegates	Direct	publicDelegates	
 ReportToOriginator	Direct	reportToOriginator	

 ReportToOwner	Direct	reportToOwner	
 SecurityEnabled	Expression	CBool(BitAnd([groupType], -2147483648))	
 SourceAnchor	Expression	IIF(IsPresent([mS-DS-ConsistencyGuid]), [mS-DS-ConsistencyGuid], [objectGUID])	
 UnauthOrig	Direct	unauthOrig	

inetOrgPerson

Object mappings in Microsoft Entra Cloud Sync define how attributes from on-premises Active Directory objects (such as users or groups) are matched, transformed, and synchronized with their corresponding objects in Entra ID, and where supported, how selected attributes flow back from Entra ID to Active Directory.

 General

Source Object Name	inetOrgPerson
Target Object Name	User
Enabled	True

inetOrgPerson Attribute Mappings

Attribute mappings in Microsoft Entra Cloud Sync define how attributes from the specified on-premises Active Directory object are matched, transformed, and synchronized with their corresponding objects in Entra ID, and where supported, how selected attributes flow back from Entra ID to Active Directory.

138 Attribute Mappings

Target Attribute Name	Source Type	Source Value	Default Value
 AccountEnabled	Expression	IIF(IsPresent([userAccountControl]), IIF(BitAnd([userAccountControl], 2)="0", "True", "False"), Not([accountDisabled]))	
 Alias	Direct	mailNickname	
 AltRecipient	Direct	altRecipient	
 Assistant	Direct	assistant	
 AuthOrig	Direct	authOrig	
 City	Expression	Trim([l])	
 CommonName	Direct	cn	
 Company	Expression	Trim([company])	
 Country	Expression	Trim([co])	
 CountryCode	Expression	IgnoreFlowIfNullOrEmpty([countryCode])	
 CountryLetterCode	Expression	Trim([c])	
 CredentialData	Direct	PasswordHash	
 Department	Expression	Trim([department])	
 Description	Expression	Left(Trim([description]), 448)	
 DisplayName	Expression	IIF(IsPresent([displayName]), [displayName], [cn])	
 DLMemRejectPerms	Direct	dLMemRejectPerms	

 DLMemSubmitPerms	Direct	dLMemSubmitPerms	
 DnsDomainName	Constant	%DomainFQDN%	
 EmployeeId	Direct	employeeId	
 EmployeeType	Direct	employeeType	
 ExtensionAttribute1	Expression	Trim([extensionAttribute1])	
 ExtensionAttribute10	Expression	Trim([extensionAttribute10])	
 ExtensionAttribute11	Expression	Trim([extensionAttribute11])	
 ExtensionAttribute12	Expression	Trim([extensionAttribute12])	
 ExtensionAttribute13	Expression	Trim([extensionAttribute13])	
 ExtensionAttribute14	Expression	Trim([extensionAttribute14])	
 ExtensionAttribute15	Expression	Trim([extensionAttribute15])	
 ExtensionAttribute2	Expression	Trim([extensionAttribute2])	
 ExtensionAttribute3	Expression	Trim([extensionAttribute3])	
 ExtensionAttribute4	Expression	Trim([extensionAttribute4])	
 ExtensionAttribute5	Expression	Trim([extensionAttribute5])	
 ExtensionAttribute6	Expression	Trim([extensionAttribute6])	
 ExtensionAttribute7	Expression	Trim([extensionAttribute7])	
 ExtensionAttribute8	Expression	Trim([extensionAttribute8])	
 ExtensionAttribute9	Expression	Trim([extensionAttribute9])	
 FacsimileTelephoneNumber	Expression	Trim([facsimileTelephoneNumber])	
 GivenName	Expression	Trim([givenName])	

 HomePhone	Expression	Trim([homePhone])	
 Info	Expression	Left(Trim([info]), 448)	
 Initials	Expression	Trim([initials])	
 IPPhone	Expression	Trim([ipPhone])	
 LastPasswordChangeTimestamp	Expression	IIF(IsPresent([pwdLastSet]), FormatDateTime(DateFromNum([pwdLastSet]), "RoundtripKind", , "yyyyMMddHHmmss.OZ"),)	
 LegacyExchangeDN	Direct	legacyExchangeDN	
 Mail	Expression	Trim([mail])	
 Manager	Direct	manager	
 MiddleName	Expression	Trim([middleName])	
 Mobile	Expression	Trim([mobile])	
 MSDSHABSeniorityIndex	Direct	msDS-HABSeniorityIndex	
 MSDSPhoneticDisplayName	Direct	msDS-PhoneticDisplayName	
 MSExchArchiveGuid	Direct	msExchArchiveGUID	
 MSExchArchiveName	Direct	msExchArchiveName	
 MSExchAssistantName	Direct	msExchAssistantName	
 MSExchAuditAdmin	Direct	msExchAuditAdmin	
 MSExchAuditDelegate	Direct	msExchAuditDelegate	
 MSExchAuditDelegateAdmin	Direct	msExchAuditDelegateAdmin	
 MSExchAuditOwner	Direct	msExchAuditOwner	
 MSExchBlockedSendersHash	Direct	msExchBlockedSendersHash	
 MSExchBypassAudit	Direct	msExchBypassAudit	

 MSEchDelegateListLink	Direct	msExchDelegateListLink	
 MSEchElcExpirySuspensionEnd	Direct	msExchELCExpirySuspensionEnd	
 MSEchElcExpirySuspensionStart	Direct	msExchELCExpirySuspensionStart	
 MSEchElcMailboxFlags	Direct	msExchELCMailboxFlags	
 MSEchEnableModeration	Direct	msExchEnableModeration	
 MSEchExtensionCustomAttribute1	Expression	Trim([msExchExtensionCustomAttribute1])	
 MSEchExtensionCustomAttribute2	Expression	Trim([msExchExtensionCustomAttribute2])	
 MSEchExtensionCustomAttribute3	Expression	Trim([msExchExtensionCustomAttribute3])	
 MSEchExtensionCustomAttribute4	Expression	Trim([msExchExtensionCustomAttribute4])	
 MSEchExtensionCustomAttribute5	Expression	Trim([msExchExtensionCustomAttribute5])	
 MSEchHideFromAddressLists	Direct	msExchHideFromAddressLists	
 MSEchImmutableId	Direct	msExchImmutableId	
 MSEchLitigationHoldDate	Direct	msExchLitigationHoldDate	
 MSEchLitigationHoldOwner	Direct	msExchLitigationHoldOwner	
 MSEchMailboxAuditEnable	Direct	msExchMailboxAuditEnable	
 MSEchMailboxAuditLogAgeLimit	Direct	msExchMailboxAuditLogAgeLimit	
 MSEchMailboxGuid	Direct	msExchMailboxGuid	
 MSEchModeratedByLink	Direct	msExchModeratedByLink	
 MSEchModerationFlags	Direct	msExchModerationFlags	
 MSEchRecipientDisplayType	Direct	msExchRecipientDisplayType	
 MSEchRecipientTypeDetails	Direct	msExchRecipientTypeDetails	

 MSEchRemoteRecipientType	Direct	msExchRemoteRecipientType	
 MSEchRequireAuthToSendTo	Direct	msExchRequireAuthToSendTo	
 MSEchResourceCapacity	Direct	msExchResourceCapacity	
 MSEchResourceDisplay	Direct	msExchResourceDisplay	
 MSEchResourceMetadata	Direct	msExchResourceMetaData	
 MSEchResourceSearchProperties	Direct	msExchResourceSearchProperties	
 MSEchRetentionComment	Direct	msExchRetentionComment	
 MSEchRetentionUrl	Direct	msExchRetentionURL	
 MSEchSafeRecipientsHash	Direct	msExchSafeRecipientsHash	
 MSEchSafeSendersHash	Direct	msExchSafeSendersHash	
 MSEchSenderHintTranslations	Direct	msExchSenderHintTranslations	
 MSEchTeamMailboxExpiration	Direct	msExchTeamMailboxExpiration	
 MSEchTeamMailboxOwners	Direct	msExchTeamMailboxOwners	
 MSEchTeamMailboxSharePointLinkedBy	Direct	msExchTeamMailboxSharePointLinkedBy	
 MSEchTeamMailboxSharePointUrl	Direct	msExchTeamMailboxSharePointUrl	
 MSEchUserHoldPolicies	Direct	msExchUserHoldPolicies	
 MSRtcSipApplicationOptions	Direct	msRTCSIP-ApplicationOptions	
 MSRtcSipDeploymentLocator	Direct	msRTCSIP-DeploymentLocator	
 MSRtcSipLine	Direct	msRTCSIP-Line	
 MSRtcSipOptionFlags	Direct	msRTCSIP-OptionFlags	
 MSRtcSipOwnerUrn	Direct	msRTCSIP-OwnerUrn	

 MSRtcSipPrimaryUserAddress	Direct	msRTCSIP-PrimaryUserAddress	
 MSRtcSipUserEnabled	Direct	msRTCSIP-UserEnabled	
 NetBiosName	Constant	%DomainNetBios%	
 OnPremisesDistinguishedName	Direct	distinguishedName	
 OnPremiseSecurityIdentifier	Direct	objectSid	
 OnPremisesObjectIdentifier	Direct	objectGUID	
 OnPremisesSamAccountName	Direct	sAMAccountName	
 OnPremisesUserPrincipalName	Expression	IIF(IsPresent([userPrincipalName]), [userPrincipalName], IIF(IsPresent([sAMAccountName]), Join("@", [sAMAccountName], %DomainFQDN%), Error("AccountName is not present"))))	
 OtherFacsimileTelephoneNumber	Expression	Trim([otherFacsimileTelephoneNumber])	
 OtherHomePhone	Expression	Trim([otherHomePhone])	
 OtherIPPhone	Expression	Trim([otherIpPhone])	
 OtherMobile	Expression	Trim([otherMobile])	
 OtherPager	Expression	Trim([otherPager])	
 OtherTelephone	Expression	Trim([otherTelephone])	
 Pager	Expression	Trim([pager])	
 PhysicalDeliveryOfficeName	Expression	Trim([physicalDeliveryOfficeName])	
 PostalCode	Expression	Trim([postalCode])	
 PostOfficeBox	Expression	IIF(IsPresent([postOfficeBox]), Left(Trim(Item([postOfficeBox], 1)), 448), "")	
 PreferredDataLocation	Direct	msDS-preferredDataLocation	
 PreferredLanguage	Expression	Trim([preferredLanguage])	
 ProxyAddresses	Expression	RemoveDuplicates(Trim([proxyAddresses]))	

 PublicDelegates	Direct	publicDelegates	
 SourceAnchor	Expression	IIF(IsPresent([mS-DS-ConsistencyGuid]), [mS-DS-ConsistencyGuid], [objectGUID])	
 State	Expression	Trim([st])	
 StreetAddress	Expression	Trim([streetAddress])	
 Surname	Expression	Trim([sn])	
 TargetAddress	Direct	targetAddress	
 TelephoneAssistant	Expression	Trim([telephoneAssistant])	
 TelephoneNumber	Expression	Trim([telephoneNumber])	
 ThumbnailPhoto	Direct	thumbnailPhoto	
 Title	Expression	Trim([title])	
 UnauthOrig	Direct	unauthOrig	
 Url	Expression	IIF(IsPresent([url]), Left(Trim(Item([url], 1)), 448), "")	
 UsageLocation	Expression	IgnoreFlowIfNullOrEmpty([msExchUsageLocation])	
 UserCertificate	Direct	userCertificate	
 UserPrincipalName	Expression	IIF(IsPresent([userPrincipalName]), [userPrincipalName], IIF(IsPresent([sAMAccountName]), Join("@", [sAMAccountName], %DomainFQDN%), Error("AccountName is not present")))	
 UserSMIMECertificate	Direct	userSMIMECertificate	
 WwwHomepage	Direct	wWWHomePage	

user

Object mappings in Microsoft Entra Cloud Sync define how attributes from on-premises Active Directory objects (such as users or groups) are matched, transformed, and synchronized with their corresponding objects in Entra ID, and where supported, how selected attributes flow back from Entra ID to Active Directory.

 General

Source Object Name	user
Target Object Name	User
Enabled	True

user Attribute Mappings

Attribute mappings in Microsoft Entra Cloud Sync define how attributes from the specified on-premises Active Directory object are matched, transformed, and synchronized with their corresponding objects in Entra ID, and where supported, how selected attributes flow back from Entra ID to Active Directory.

138 Attribute Mappings

Target Attribute Name	Source Type	Source Value	Default Value
 AccountEnabled	Expression	IIF(IsPresent([userAccountControl]), IIF(BitAnd([userAccountControl], 2)="0", "True", "False"), Not([accountDisabled]))	
 Alias	Direct	mailNickname	
 AltRecipient	Direct	altRecipient	
 Assistant	Direct	assistant	
 AuthOrig	Direct	authOrig	
 City	Expression	Trim([l])	
 CommonName	Direct	cn	
 Company	Expression	Trim([company])	
 Country	Expression	Trim([co])	
 CountryCode	Expression	IgnoreFlowIfNullOrEmpty([countryCode])	
 CountryLetterCode	Expression	Trim([c])	
 CredentialData	Direct	PasswordHash	
 Department	Expression	Trim([department])	
 Description	Expression	Left(Trim([description]), 448)	
 DisplayName	Expression	IIF(IsPresent([displayName]), [displayName], [cn])	
 DLMemRejectPerms	Direct	dLMemRejectPerms	

 DLMemSubmitPerms	Direct	dLMemSubmitPerms	
 DnsDomainName	Constant	%DomainFQDN%	
 EmployeeId	Direct	employeeId	
 EmployeeType	Direct	employeeType	
 ExtensionAttribute1	Expression	Trim([extensionAttribute1])	
 ExtensionAttribute10	Expression	Trim([extensionAttribute10])	
 ExtensionAttribute11	Expression	Trim([extensionAttribute11])	
 ExtensionAttribute12	Expression	Trim([extensionAttribute12])	
 ExtensionAttribute13	Expression	Trim([extensionAttribute13])	
 ExtensionAttribute14	Expression	Trim([extensionAttribute14])	
 ExtensionAttribute15	Expression	Trim([extensionAttribute15])	
 ExtensionAttribute2	Expression	Trim([extensionAttribute2])	
 ExtensionAttribute3	Expression	Trim([extensionAttribute3])	
 ExtensionAttribute4	Expression	Trim([extensionAttribute4])	
 ExtensionAttribute5	Expression	Trim([extensionAttribute5])	
 ExtensionAttribute6	Expression	Trim([extensionAttribute6])	
 ExtensionAttribute7	Expression	Trim([extensionAttribute7])	
 ExtensionAttribute8	Expression	Trim([extensionAttribute8])	
 ExtensionAttribute9	Expression	Trim([extensionAttribute9])	
 FacsimileTelephoneNumber	Expression	Trim([facsimileTelephoneNumber])	
 GivenName	Expression	Trim([givenName])	

 HomePhone	Expression	Trim([homePhone])	
 Info	Expression	Left(Trim([info]), 448)	
 Initials	Expression	Trim([initials])	
 IPPhone	Expression	Trim([ipPhone])	
 LastPasswordChangeTimestamp	Expression	IIF(IsPresent([pwdLastSet]), FormatDateTime(DateFromNum([pwdLastSet]), "RoundtripKind", , "yyyyMMddHHmmss.OZ"),)	
 LegacyExchangeDN	Direct	legacyExchangeDN	
 Mail	Expression	Trim([mail])	
 Manager	Direct	manager	
 MiddleName	Expression	Trim([middleName])	
 Mobile	Expression	Trim([mobile])	
 MSDSHABSeniorityIndex	Direct	msDS-HABSeniorityIndex	
 MSDSPhoneticDisplayName	Direct	msDS-PhoneticDisplayName	
 MSExchArchiveGuid	Direct	msExchArchiveGUID	
 MSExchArchiveName	Direct	msExchArchiveName	
 MSExchAssistantName	Direct	msExchAssistantName	
 MSExchAuditAdmin	Direct	msExchAuditAdmin	
 MSExchAuditDelegate	Direct	msExchAuditDelegate	
 MSExchAuditDelegateAdmin	Direct	msExchAuditDelegateAdmin	
 MSExchAuditOwner	Direct	msExchAuditOwner	
 MSExchBlockedSendersHash	Direct	msExchBlockedSendersHash	
 MSExchBypassAudit	Direct	msExchBypassAudit	

 MSEchDelegateListLink	Direct	msExchDelegateListLink	
 MSEchElcExpirySuspensionEnd	Direct	msExchELCExpirySuspensionEnd	
 MSEchElcExpirySuspensionStart	Direct	msExchELCExpirySuspensionStart	
 MSEchElcMailboxFlags	Direct	msExchELCMailboxFlags	
 MSEchEnableModeration	Direct	msExchEnableModeration	
 MSEchExtensionCustomAttribute1	Expression	Trim([msExchExtensionCustomAttribute1])	
 MSEchExtensionCustomAttribute2	Expression	Trim([msExchExtensionCustomAttribute2])	
 MSEchExtensionCustomAttribute3	Expression	Trim([msExchExtensionCustomAttribute3])	
 MSEchExtensionCustomAttribute4	Expression	Trim([msExchExtensionCustomAttribute4])	
 MSEchExtensionCustomAttribute5	Expression	Trim([msExchExtensionCustomAttribute5])	
 MSEchHideFromAddressLists	Direct	msExchHideFromAddressLists	
 MSEchImmutableId	Direct	msExchImmutableId	
 MSEchLitigationHoldDate	Direct	msExchLitigationHoldDate	
 MSEchLitigationHoldOwner	Direct	msExchLitigationHoldOwner	
 MSEchMailboxAuditEnable	Direct	msExchMailboxAuditEnable	
 MSEchMailboxAuditLogAgeLimit	Direct	msExchMailboxAuditLogAgeLimit	
 MSEchMailboxGuid	Direct	msExchMailboxGuid	
 MSEchModeratedByLink	Direct	msExchModeratedByLink	
 MSEchModerationFlags	Direct	msExchModerationFlags	
 MSEchRecipientDisplayType	Direct	msExchRecipientDisplayType	
 MSEchRecipientTypeDetails	Direct	msExchRecipientTypeDetails	

 MSEchRemoteRecipientType	Direct	msExchRemoteRecipientType	
 MSEchRequireAuthToSendTo	Direct	msExchRequireAuthToSendTo	
 MSEchResourceCapacity	Direct	msExchResourceCapacity	
 MSEchResourceDisplay	Direct	msExchResourceDisplay	
 MSEchResourceMetadata	Direct	msExchResourceMetaData	
 MSEchResourceSearchProperties	Direct	msExchResourceSearchProperties	
 MSEchRetentionComment	Direct	msExchRetentionComment	
 MSEchRetentionUrl	Direct	msExchRetentionURL	
 MSEchSafeRecipientsHash	Direct	msExchSafeRecipientsHash	
 MSEchSafeSendersHash	Direct	msExchSafeSendersHash	
 MSEchSenderHintTranslations	Direct	msExchSenderHintTranslations	
 MSEchTeamMailboxExpiration	Direct	msExchTeamMailboxExpiration	
 MSEchTeamMailboxOwners	Direct	msExchTeamMailboxOwners	
 MSEchTeamMailboxSharePointLinkedBy	Direct	msExchTeamMailboxSharePointLinkedBy	
 MSEchTeamMailboxSharePointUrl	Direct	msExchTeamMailboxSharePointUrl	
 MSEchUserHoldPolicies	Direct	msExchUserHoldPolicies	
 MSRtcSipApplicationOptions	Direct	msRTCSIP-ApplicationOptions	
 MSRtcSipDeploymentLocator	Direct	msRTCSIP-DeploymentLocator	
 MSRtcSipLine	Direct	msRTCSIP-Line	
 MSRtcSipOptionFlags	Direct	msRTCSIP-OptionFlags	
 MSRtcSipOwnerUrn	Direct	msRTCSIP-OwnerUrn	

 MSRtcSipPrimaryUserAddress	Direct	msRTCSIP-PrimaryUserAddress	
 MSRtcSipUserEnabled	Direct	msRTCSIP-UserEnabled	
 NetBiosName	Constant	%DomainNetBios%	
 OnPremisesDistinguishedName	Direct	distinguishedName	
 OnPremiseSecurityIdentifier	Direct	objectSid	
 OnPremisesObjectIdentifier	Direct	objectGUID	
 OnPremisesSamAccountName	Direct	sAMAccountName	
 OnPremisesUserPrincipalName	Expression	IIF(IsPresent([userPrincipalName]), [userPrincipalName], IIF(IsPresent([sAMAccountName]), Join("@", [sAMAccountName], %DomainFQDN%), Error("AccountName is not present"))))	
 OtherFacsimileTelephoneNumber	Expression	Trim([otherFacsimileTelephoneNumber])	
 OtherHomePhone	Expression	Trim([otherHomePhone])	
 OtherIPPhone	Expression	Trim([otherIpPhone])	
 OtherMobile	Expression	Trim([otherMobile])	
 OtherPager	Expression	Trim([otherPager])	
 OtherTelephone	Expression	Trim([otherTelephone])	
 Pager	Expression	Trim([pager])	
 PhysicalDeliveryOfficeName	Expression	Trim([physicalDeliveryOfficeName])	
 PostalCode	Expression	Trim([postalCode])	
 PostOfficeBox	Expression	IIF(IsPresent([postOfficeBox]), Left(Trim(Item([postOfficeBox], 1)), 448), "")	
 PreferredDataLocation	Direct	msDS-preferredDataLocation	
 PreferredLanguage	Expression	Trim([preferredLanguage])	
 ProxyAddresses	Expression	RemoveDuplicates(Trim([proxyAddresses]))	

 PublicDelegates	Direct	publicDelegates	
 SourceAnchor	Expression	IIF(IsPresent([mS-DS-ConsistencyGuid]), [mS-DS-ConsistencyGuid], [objectGUID])	
 State	Expression	Trim([st])	
 StreetAddress	Expression	Trim([streetAddress])	
 Surname	Expression	Trim([sn])	
 TargetAddress	Direct	targetAddress	
 TelephoneAssistant	Expression	Trim([telephoneAssistant])	
 TelephoneNumber	Expression	Trim([telephoneNumber])	
 ThumbnailPhoto	Direct	thumbnailPhoto	
 Title	Expression	Trim([title])	
 UnauthOrig	Direct	unauthOrig	
 Url	Expression	IIF(IsPresent([url]), Left(Trim(Item([url], 1)), 448), "")	
 UsageLocation	Expression	IgnoreFlowIfNullOrEmpty([msExchUsageLocation])	
 UserCertificate	Direct	userCertificate	
 UserPrincipalName	Expression	IIF(IsPresent([userPrincipalName]), [userPrincipalName], IIF(IsPresent([sAMAccountName]), Join("@", [sAMAccountName], %DomainFQDN%), Error("AccountName is not present")))	
 UserSMIMECertificate	Direct	userSMIMECertificate	
 WwwHomepage	Direct	wWWHomePage	

centrelsolutionsdemo.int (Microsoft Entra ID to AD)

Cloud Sync configurations define which objects and attributes are in scope for synchronization, controlling how users, groups, and contacts flow from Active Directory to Entra ID - and, where supported, how selected attributes can flow back from Entra ID to Active Directory.

 General

Configuration Type	Microsoft Entra ID to AD
Domain Name	centrelsolutionsdemo.int
Service Principal Identifier	1376c4a4-e4b4-40ff-afd2-6dfac6534695
Status	Active

 Domain Information

Domain Name	centrelsolutionsdemo.int
Domain NetBIOS Name	CSDEMO
Domain Discovery Date	13 April 2026 16:36:40
Forest Name	centrelsolutionsdemo.int
Forest NetBIOS Name	CSDEMO

 Settings

Email Notifications	True
Email Notifications Recipient	
Prevent Accidental Deletion	True
Accidental Deletion Threshold	500

 1 Agents

Machine Name	External IP Address	Status	Resources
 CSDEMO-DC01.centrelsolutionsdemo.int	81.109.64.92	Active	centrelsolutionsdemo.int

 1 Job Statuses

Display Name	Status	Last Run Date/Time
Group provisioning to Active Directory	Active	22 September 2026 09:24:34

Scoping Filters

Scoping filters in Microsoft Entra Cloud Sync are conditional rules that determine which directory objects are included in a given sync flow.

Groups

Groups Scope	All security groups
--------------	---------------------

Target Container

Target Container	CN=Users,DC=centrelsolutionsdemo,DC=int
------------------	---

1 Attribute Filters

Clause	Name	Scoping Phrase
	Cloud Owned Security Groups	

Object Mappings

Object mappings in Microsoft Entra Cloud Sync define how attributes from on-premises Active Directory objects (such as users or groups) are matched, transformed, and synchronized with their corresponding objects in Entra ID, and where supported, how selected attributes flow back from Entra ID to Active Directory.

 2 Object Mappings

Source Object Name	Target Object Name	Enabled
 Group	group	True
 User	user	True

Group

Object mappings in Microsoft Entra Cloud Sync define how attributes from on-premises Active Directory objects (such as users or groups) are matched, transformed, and synchronized with their corresponding objects in Entra ID, and where supported, how selected attributes flow back from Entra ID to Active Directory.

 General

Source Object Name	Group
Target Object Name	group
Enabled	True

Group Attribute Mappings

Attribute mappings in Microsoft Entra Cloud Sync define how attributes from the specified on-premises Active Directory object are matched, transformed, and synchronized with their corresponding objects in Entra ID, and where supported, how selected attributes flow back from Entra ID to Active Directory.

9 Attribute Mappings

Target Attribute Name	Source Type	Source Value	Default Value
 adminDescription	Expression	Append("Group_", [objectId])	
 cn	Expression	Append(Append(Left(Trim([displayName]), 51), "_"), Mid([objectId], 25, 12))	
 description	Expression	Left(Trim([description]), 448)	
 displayName	Direct	displayName	
 isSecurityGroup	Constant	"True"	
 member	Direct	members	
 msDS-ExternalDirectoryObjectId	Expression	Append("Group_", [objectId])	
 parentDistinguishedName	Constant	"CN=Users,DC=centrelsolutionsdemo,DC=int"	CN=Users,DC=centrelsolutionsdemo,DC=int
 universalScope	Constant	"True"	

User

Object mappings in Microsoft Entra Cloud Sync define how attributes from on-premises Active Directory objects (such as users or groups) are matched, transformed, and synchronized with their corresponding objects in Entra ID, and where supported, how selected attributes flow back from Entra ID to Active Directory.

 General

Source Object Name	User
Target Object Name	user
Enabled	True

User Attribute Mappings

Attribute mappings in Microsoft Entra Cloud Sync define how attributes from the specified on-premises Active Directory object are matched, transformed, and synchronized with their corresponding objects in Entra ID, and where supported, how selected attributes flow back from Entra ID to Active Directory.

 1 Attribute Mappings

Target Attribute Name	Source Type	Source Value	Default Value
 msDS-ExternalDirectoryObjectId	Expression	Append("User_", [objectId])	

emea.centrelsolutionsdemo.int (Microsoft Entra ID to AD)

Cloud Sync configurations define which objects and attributes are in scope for synchronization, controlling how users, groups, and contacts flow from Active Directory to Entra ID - and, where supported, how selected attributes can flow back from Entra ID to Active Directory.

General

Configuration Type	Microsoft Entra ID to AD
Domain Name	emea.centrelsolutionsdemo.int
Service Principal Identifier	2324d490-ddef-4578-8c3b-0d77feaac9d
Status	Disabled

Domain Information

Information is not available for this section because the object does not support the providing of this information or it is not relevant to this object.

Settings

Email Notifications	True
Email Notifications Recipient	
Prevent Accidental Deletion	True
Accidental Deletion Threshold	500

1 Agents

Machine Name	External IP Address	Status	Resources
 CSDEMO-DC03.emea.centrelsolutionsdemo.int	81.109.64.92	Inactive	emea.centrelsolutionsdemo.int

1 Job Statuses

Display Name	Status	Last Run Date/Time
 Group provisioning to Active Directory	Paused	[Not Configured]

Scoping Filters

Scoping filters in Microsoft Entra Cloud Sync are conditional rules that determine which directory objects are included in a given sync flow.

Groups

Groups Scope	All security groups
--------------	---------------------

Target Container

Target Container	CN=Users,DC=emea,DC=centrelsolutionsdemo,DC=int
------------------	---

1 Attribute Filters

Clause	Name	Scoping Phrase
	Cloud Owned Security Groups	

Object Mappings

Object mappings in Microsoft Entra Cloud Sync define how attributes from on-premises Active Directory objects (such as users or groups) are matched, transformed, and synchronized with their corresponding objects in Entra ID, and where supported, how selected attributes flow back from Entra ID to Active Directory.

 2 Object Mappings

Source Object Name	Target Object Name	Enabled
 Group	group	True
 User	user	True

Group

Object mappings in Microsoft Entra Cloud Sync define how attributes from on-premises Active Directory objects (such as users or groups) are matched, transformed, and synchronized with their corresponding objects in Entra ID, and where supported, how selected attributes flow back from Entra ID to Active Directory.

 General

Source Object Name	Group
Target Object Name	group
Enabled	True

Group Attribute Mappings

Attribute mappings in Microsoft Entra Cloud Sync define how attributes from the specified on-premises Active Directory object are matched, transformed, and synchronized with their corresponding objects in Entra ID, and where supported, how selected attributes flow back from Entra ID to Active Directory.

9 Attribute Mappings

Target Attribute Name	Source Type	Source Value	Default Value
 adminDescription	Expression	Append("Group_", [objectId])	
 cn	Expression	Append(Append(Left(Trim([displayName]), 51), "_"), Mid([objectId], 25, 12))	
 description	Expression	Left(Trim([description]), 448)	
 displayName	Direct	displayName	
 isSecurityGroup	Constant	"True"	
 member	Direct	members	
 msDS-ExternalDirectoryObjectId	Expression	Append("Group_", [objectId])	
 parentDistinguishedName	Constant	"CN=Users,DC=emea,DC=centrelsolutionsdemo,DC=int"	CN=Users,DC=emea,DC=centrelsolutionsdemo,DC=int
 universalScope	Constant	"True"	

User

Object mappings in Microsoft Entra Cloud Sync define how attributes from on-premises Active Directory objects (such as users or groups) are matched, transformed, and synchronized with their corresponding objects in Entra ID, and where supported, how selected attributes flow back from Entra ID to Active Directory.

 General

Source Object Name	User
Target Object Name	user
Enabled	True

User Attribute Mappings

Attribute mappings in Microsoft Entra Cloud Sync define how attributes from the specified on-premises Active Directory object are matched, transformed, and synchronized with their corresponding objects in Entra ID, and where supported, how selected attributes flow back from Entra ID to Active Directory.

1 Attribute Mappings

Target Attribute Name	Source Type	Source Value	Default Value
 msDS-ExternalDirectoryObjectId	Expression	Append("User_", [objectId])	

Groups

Microsoft Entra groups are directory objects used to centrally manage access and permissions for users, devices, and service principals within Microsoft Entra ID. They enable administrators to assign access to applications, resources, and directory roles at scale, reducing the need for individual user configuration and ensuring consistent, least-privilege access across the environment.

 27 Groups

First Letter	Count
 #	0
 A	3
 B	0
 C	1
 D	8
 E	6
 F	0
 G	2
 H	1
 I	2
 J	0
 K	0
 L	0
 M	1
 N	0
 O	0
 P	0
 Q	0
 R	0
 S	1
 T	1
 U	0
 V	0
 W	1
 X	0
 Y	0

 z	0
---	---

Groups - A

Provides information about the groups defined in the organization with the specified first letter.

 **3 Groups**

Display Name	Group Type	Membership Type
 All Company	Microsoft 365	Assigned
 All Company	Microsoft 365	Assigned
 All Users	Security	Dynamic

All Company

Microsoft Entra groups are directory objects used to centrally manage access and permissions for users, devices, and service principals within Microsoft Entra ID. They enable administrators to assign access to applications, resources, and directory roles at scale, reducing the need for individual user configuration and ensuring consistent, least-privilege access across the environment.

 General

Microsoft Entra Roles Can Be Assigned	False
Creation Date	16 October 2023 16:50:36
Description	This is the default group for everyone in the network
Email	allcompany@centrelsolutionsdemo.onmicrosoft.com
Group Type	Microsoft 365
Membership Type	Assigned
Identifier	2c5828b0-bdd2-4e01-819e-409daa0b2e22
Security Identifier	S-1-12-1-743975088-1308736978-2638257793-573442986

 Expiration

Expiration Date	[Not Configured]
-----------------	------------------

 On-Premises Settings

Synced From Active Directory	False
------------------------------	-------

 1 Owners

Display Name	Identity	Type
 XIA	xia@centrelsolutionsdemo.onmicrosoft.com	User

 1 Direct Group Members

Display Name	Member Type
 XIA	User

All Company

Microsoft Entra groups are directory objects used to centrally manage access and permissions for users, devices, and service principals within Microsoft Entra ID. They enable administrators to assign access to applications, resources, and directory roles at scale, reducing the need for individual user configuration and ensuring consistent, least-privilege access across the environment.

General

Microsoft Entra Roles Can Be Assigned	False
Creation Date	29 January 2024 09:16:31
Description	This is the default group for everyone in the network
Email	allcompany107@centrelsolutionsdemo.onmicrosoft.com
Group Type	Microsoft 365
Membership Type	Assigned
Identifier	4624c2c1-5b70-4808-978e-d0277d5c6f6b
Security Identifier	S-1-12-1-1176814273-1208507248-667979415-1802460285

Expiration

Expiration Date	[Not Configured]
-----------------	------------------

On-Premises Settings

Synced From Active Directory	False
------------------------------	-------

1 Owners

Display Name	Identity	Type
 XIA	xia@centrelsolutionsdemo.onmicrosoft.com	User

1 Direct Group Members

Display Name	Member Type
 XIA	User

All Users

Microsoft Entra groups are directory objects used to centrally manage access and permissions for users, devices, and service principals within Microsoft Entra ID. They enable administrators to assign access to applications, resources, and directory roles at scale, reducing the need for individual user configuration and ensuring consistent, least-privilege access across the environment.

 General

Microsoft Entra Roles Can Be Assigned	False
Creation Date	26 September 2023 15:24:07
Description	
Email	
Group Type	Security
Membership Type	Dynamic
Identifier	4cd51e16-de7a-4f6d-93ba-70e3bbb8e255
Security Identifier	S-1-12-1-1289035286-1332600442-3815815827-1440921787

 Expiration

Expiration Date	[Not Configured]
-----------------	------------------

 Dynamic Membership Rules

Membership Rule	All Users
Membership Rule Processing State	On

 On-Premises Settings

Synced From Active Directory	False
------------------------------	-------

 0 Owners

There are no owners found.

Groups - C

Provides information about the groups defined in the organization with the specified first letter.

 1 Groups

Display Name	Group Type	Membership Type
 Compliance Management	Security	Assigned

Compliance Management

Microsoft Entra groups are directory objects used to centrally manage access and permissions for users, devices, and service principals within Microsoft Entra ID. They enable administrators to assign access to applications, resources, and directory roles at scale, reducing the need for individual user configuration and ensuring consistent, least-privilege access across the environment.

General

Microsoft Entra Roles Can Be Assigned	False
Creation Date	10 July 2026 15:24:02
Description	This role group will allow a specified user, responsible for compliance, to properly configure and manage compliance settings within Exchange in accordance with their policy.
Email	
Group Type	Security
Membership Type	Assigned
Identifier	d78a1443-c7bd-4634-854a-158ae0499f82
Security Identifier	S-1-12-1-3616150595-1177864125-2316651141-2191477216

Expiration

Expiration Date	[Not Configured]
-----------------	------------------

On-Premises Settings

Synced From Active Directory	True
Last Sync Date	10 July 2026 15:24:02
Domain Name	centrelsolutionsdemo.int
SAM Account Name	Compliance Management
Security Identifier	S-1-12-1-3616150595-1177864125-2316651141-2191477216

0 Owners

There are no owners found.

0 Direct Group Members

There are no direct group members found.
--

Groups - D

Provides information about the groups defined in the organization with the specified first letter.

 **8 Groups**

Display Name	Group Type	Membership Type
 Demonstration Distribution Group	Distribution	Assigned
 Demonstration Security Group	Security	Assigned
 Demonstration Security Group	Security	Assigned
 Deprecated - All Company	Microsoft 365	Assigned
 DnsAdmins	Security	Assigned
 DnsAdmins	Security	Assigned
 DnsUpdateProxy	Security	Assigned
 DnsUpdateProxy	Security	Assigned

Demonstration Distribution Group

Microsoft Entra groups are directory objects used to centrally manage access and permissions for users, devices, and service principals within Microsoft Entra ID. They enable administrators to assign access to applications, resources, and directory roles at scale, reducing the need for individual user configuration and ensuring consistent, least-privilege access across the environment.

General

Microsoft Entra Roles Can Be Assigned	False
Creation Date	20 April 2026 12:21:58
Description	
Email	DemonstrationDistributionGroup@centrelsolutionsdemo.onmicrosoft.com
Group Type	Distribution
Membership Type	Assigned
Identifier	4cc4ec41-41ad-42c9-8343-8afa323ccf27
Security Identifier	S-1-12-1-1287973953-1120485805-4203365251-667892786

Expiration

Expiration Date	[Not Configured]
-----------------	------------------

On-Premises Settings

Synced From Active Directory	True
Last Sync Date	17 July 2026 15:31:21
Domain Name	centrelsolutionsdemo.int
SAM Account Name	Demonstration Distribution Group-1432885019
Security Identifier	S-1-12-1-1287973953-1120485805-4203365251-667892786

0 Owners

There are no owners found.

0 Direct Group Members

There are no direct group members found.
--

Demonstration Security Group

Microsoft Entra groups are directory objects used to centrally manage access and permissions for users, devices, and service principals within Microsoft Entra ID. They enable administrators to assign access to applications, resources, and directory roles at scale, reducing the need for individual user configuration and ensuring consistent, least-privilege access across the environment.

 General

Microsoft Entra Roles Can Be Assigned	False
Creation Date	27 August 2026 17:15:55
Description	
Email	DemonstrationSecurityGroup0348@centrelsolutionsdemo.onmicrosoft.com
Group Type	Security
Membership Type	Assigned
Identifier	32702327-ea12-4d2d-8db2-daca2b689828
Security Identifier	S-1-12-1-846209831-1294854674-3403330189-681076779

 Expiration

Expiration Date	[Not Configured]
-----------------	------------------

 On-Premises Settings

Synced From Active Directory	True
Last Sync Date	27 August 2026 17:15:55
Domain Name	centrelsolutionsdemo.int
SAM Account Name	Demonstration Security Group-1250642761
Security Identifier	S-1-12-1-846209831-1294854674-3403330189-681076779

 0 Owners

There are no owners found.

 0 Direct Group Members

There are no direct group members found.
--

Demonstration Security Group

Microsoft Entra groups are directory objects used to centrally manage access and permissions for users, devices, and service principals within Microsoft Entra ID. They enable administrators to assign access to applications, resources, and directory roles at scale, reducing the need for individual user configuration and ensuring consistent, least-privilege access across the environment.

 General

Microsoft Entra Roles Can Be Assigned	False
Creation Date	21 July 2026 08:52:53
Description	This is a demonstration mail enabled security group.
Email	demonstrationsecuritygroup@centrelsolutionsdemo.onmicrosoft.com
Group Type	Security
Membership Type	Assigned
Identifier	d05f0065-c523-423d-997a-1def7da3caec
Security Identifier	S-1-12-1-3495886949-1111344419-4011686553-3972703101

 Expiration

Expiration Date	[Not Configured]
-----------------	------------------

 On-Premises Settings

Synced From Active Directory	False
------------------------------	-------

 0 Owners

There are no owners found.

 0 Direct Group Members

There are no direct group members found.

Deprecated - All Company

Microsoft Entra groups are directory objects used to centrally manage access and permissions for users, devices, and service principals within Microsoft Entra ID. They enable administrators to assign access to applications, resources, and directory roles at scale, reducing the need for individual user configuration and ensuring consistent, least-privilege access across the environment.

General

Microsoft Entra Roles Can Be Assigned	False
Creation Date	08 July 2026 13:53:48
Description	All Company
Email	AllCompany.63717335041.nqmosuyc@centrelsolutionsdemo.onmicrosoft.com
Group Type	Microsoft 365
Membership Type	Assigned
Identifier	67476002-a533-4dec-9363-8f2fd76e0382
Security Identifier	S-1-12-1-1732730882-1307354419-797926291-2181263063

Expiration

Expiration Date	[Not Configured]
-----------------	------------------

On-Premises Settings

Synced From Active Directory	False
------------------------------	-------

2 Owners

Display Name	Identity	Type
 Backup Global Admin	sysadmin@centrelsolutionsdemo.onmicrosoft.com	User
 XIA	xia@centrelsolutionsdemo.onmicrosoft.com	User

0 Direct Group Members

There are no direct group members found.
--

DnsAdmins

Microsoft Entra groups are directory objects used to centrally manage access and permissions for users, devices, and service principals within Microsoft Entra ID. They enable administrators to assign access to applications, resources, and directory roles at scale, reducing the need for individual user configuration and ensuring consistent, least-privilege access across the environment.

 General

Microsoft Entra Roles Can Be Assigned	False
Creation Date	13 April 2026 17:36:25
Description	DNS Administrators Group
Email	
Group Type	Security
Membership Type	Assigned
Identifier	5a71cbcd-f3d2-40fb-ab39-4e5d78bb3496
Security Identifier	S-1-12-1-1517407181-1090253778-1565407659-2520038264

 Expiration

Expiration Date	[Not Configured]
-----------------	------------------

 On-Premises Settings

Synced From Active Directory	True
Last Sync Date	08 July 2026 14:05:45
Domain Name	emea.centrelsolutionsdemo.int
SAM Account Name	DnsAdmins
Security Identifier	S-1-12-1-1517407181-1090253778-1565407659-2520038264

 0 Owners

There are no owners found.

 0 Direct Group Members

There are no direct group members found.

DnsAdmins

Microsoft Entra groups are directory objects used to centrally manage access and permissions for users, devices, and service principals within Microsoft Entra ID. They enable administrators to assign access to applications, resources, and directory roles at scale, reducing the need for individual user configuration and ensuring consistent, least-privilege access across the environment.

 General

Microsoft Entra Roles Can Be Assigned	False
Creation Date	13 April 2026 17:35:48
Description	DNS Administrators Group
Email	
Group Type	Security
Membership Type	Assigned
Identifier	82874107-ff7d-43e1-b267-4cc2612e225b
Security Identifier	S-1-12-1-2189902087-1138884477-3259787186-1528966753

 Expiration

Expiration Date	[Not Configured]
-----------------	------------------

 On-Premises Settings

Synced From Active Directory	True
Last Sync Date	13 April 2026 17:43:06
Domain Name	centrelsolutionsdemo.int
SAM Account Name	DnsAdmins
Security Identifier	S-1-12-1-2189902087-1138884477-3259787186-1528966753

 0 Owners

There are no owners found.

 0 Direct Group Members

There are no direct group members found.

DnsUpdateProxy

Microsoft Entra groups are directory objects used to centrally manage access and permissions for users, devices, and service principals within Microsoft Entra ID. They enable administrators to assign access to applications, resources, and directory roles at scale, reducing the need for individual user configuration and ensuring consistent, least-privilege access across the environment.

 General

Microsoft Entra Roles Can Be Assigned	False
Creation Date	13 April 2026 17:36:25
Description	DNS clients who are permitted to perform dynamic updates on behalf of some other clients (such as DHCP servers).
Email	
Group Type	Security
Membership Type	Assigned
Identifier	d043b89e-8366-4558-9436-85b16580375d
Security Identifier	S-1-12-1-3494099102-1163428710-2978297492-1563918437

 Expiration

Expiration Date	[Not Configured]
-----------------	------------------

 On-Premises Settings

Synced From Active Directory	True
Last Sync Date	08 July 2026 14:05:45
Domain Name	emea.centrelsolutionsdemo.int
SAM Account Name	DnsUpdateProxy
Security Identifier	S-1-12-1-3494099102-1163428710-2978297492-1563918437

 0 Owners

There are no owners found.

 0 Direct Group Members

There are no direct group members found.
--

DnsUpdateProxy

Microsoft Entra groups are directory objects used to centrally manage access and permissions for users, devices, and service principals within Microsoft Entra ID. They enable administrators to assign access to applications, resources, and directory roles at scale, reducing the need for individual user configuration and ensuring consistent, least-privilege access across the environment.

 General

Microsoft Entra Roles Can Be Assigned	False
Creation Date	13 April 2026 17:35:48
Description	DNS clients who are permitted to perform dynamic updates on behalf of some other clients (such as DHCP servers).
Email	
Group Type	Security
Membership Type	Assigned
Identifier	9f82cbe4-e4c0-41cc-b315-c5ed8798d67b
Security Identifier	S-1-12-1-2676149220-1103946944-3989116339-2077661319

 Expiration

Expiration Date	[Not Configured]
-----------------	------------------

 On-Premises Settings

Synced From Active Directory	True
Last Sync Date	13 April 2026 17:43:06
Domain Name	centrelsolutionsdemo.int
SAM Account Name	DnsUpdateProxy
Security Identifier	S-1-12-1-2676149220-1103946944-3989116339-2077661319

 0 Owners

There are no owners found.

 0 Direct Group Members

There are no direct group members found.
--

Groups - E

Provides information about the groups defined in the organization with the specified first letter.

 **6 Groups**

Display Name	Group Type	Membership Type
 EntraLicenseGroup	Security	Assigned
 Exchange Install Domain Servers	Security	Assigned
 Exchange Servers	Security	Assigned
 Exchange Trusted Subsystem	Security	Assigned
 Exchange Windows Permissions	Security	Assigned
 ExchangeLegacyInterop	Security	Assigned

EntraLicenseGroup

Microsoft Entra groups are directory objects used to centrally manage access and permissions for users, devices, and service principals within Microsoft Entra ID. They enable administrators to assign access to applications, resources, and directory roles at scale, reducing the need for individual user configuration and ensuring consistent, least-privilege access across the environment.

 General

Microsoft Entra Roles Can Be Assigned	False
Creation Date	22 January 2026 15:21:39
Description	Gets Entra licenses
Email	
Group Type	Security
Membership Type	Assigned
Identifier	6cbe99cc-bf7d-48b7-a159-f142050d90aa
Security Identifier	S-1-12-1-1824430540-1220001661-1123113377-2861567237

 Expiration

Expiration Date	[Not Configured]
-----------------	------------------

 On-Premises Settings

Synced From Active Directory	False
------------------------------	-------

 0 Owners

There are no owners found.	
----------------------------	--

 1 Direct Group Members

Display Name	Member Type
 XIA	User

Exchange Install Domain Servers

Microsoft Entra groups are directory objects used to centrally manage access and permissions for users, devices, and service principals within Microsoft Entra ID. They enable administrators to assign access to applications, resources, and directory roles at scale, reducing the need for individual user configuration and ensuring consistent, least-privilege access across the environment.

General

Microsoft Entra Roles Can Be Assigned	False
Creation Date	20 April 2026 11:07:37
Description	This group is used during Exchange setup and is not intended to be used for other purposes.
Email	
Group Type	Security
Membership Type	Assigned
Identifier	fd313b44-a91e-4c22-a12a-b03a1761ef31
Security Identifier	S-1-12-1-4247862084-1277339934-984623777-837771543

Expiration

Expiration Date	[Not Configured]
-----------------	------------------

On-Premises Settings

Synced From Active Directory	True
Last Sync Date	20 April 2026 11:27:30
Domain Name	centrelsolutionsdemo.int
SAM Account Name	\$441000-DV6QPG27PNM2
Security Identifier	S-1-12-1-4247862084-1277339934-984623777-837771543

0 Owners

There are no owners found.

0 Direct Group Members

There are no direct group members found.
--

Exchange Servers

Microsoft Entra groups are directory objects used to centrally manage access and permissions for users, devices, and service principals within Microsoft Entra ID. They enable administrators to assign access to applications, resources, and directory roles at scale, reducing the need for individual user configuration and ensuring consistent, least-privilege access across the environment.

General

Microsoft Entra Roles Can Be Assigned	False
Creation Date	20 April 2026 11:07:37
Description	This group contains all the Exchange servers. This group shouldn't be deleted.
Email	
Group Type	Security
Membership Type	Assigned
Identifier	4320deec-5c7e-409b-b5b9-28003e439488
Security Identifier	S-1-12-1-1126227692-1083923582-2668981-2291417918

Expiration

Expiration Date	[Not Configured]
-----------------	------------------

On-Premises Settings

Synced From Active Directory	True
Last Sync Date	20 April 2026 11:27:30
Domain Name	centrelsolutionsdemo.int
SAM Account Name	Exchange Servers
Security Identifier	S-1-12-1-1126227692-1083923582-2668981-2291417918

0 Owners

There are no owners found.

1 Direct Group Members

Display Name	Member Type
 Exchange Install Domain Servers	Group

Exchange Trusted Subsystem

Microsoft Entra groups are directory objects used to centrally manage access and permissions for users, devices, and service principals within Microsoft Entra ID. They enable administrators to assign access to applications, resources, and directory roles at scale, reducing the need for individual user configuration and ensuring consistent, least-privilege access across the environment.

General

Microsoft Entra Roles Can Be Assigned	False
Creation Date	20 April 2026 11:07:37
Description	This group contains Exchange servers that run Exchange cmdlets on behalf of users via the management service. Its members have permission to read and modify all Exchange configuration, as well as user accounts and groups. This group should not be deleted.
Email	
Group Type	Security
Membership Type	Assigned
Identifier	0931ab90-86b5-4ba8-a962-03446ce68af7
Security Identifier	S-1-12-1-154250128-1269335733-1141072553-4153075308

Expiration

Expiration Date	[Not Configured]
-----------------	------------------

On-Premises Settings

Synced From Active Directory	True
Last Sync Date	20 April 2026 16:07:55
Domain Name	centrelsolutionsdemo.int
SAM Account Name	Exchange Trusted Subsystem
Security Identifier	S-1-12-1-154250128-1269335733-1141072553-4153075308

0 Owners

There are no owners found.

0 Direct Group Members

There are no direct group members found.

Exchange Windows Permissions

Microsoft Entra groups are directory objects used to centrally manage access and permissions for users, devices, and service principals within Microsoft Entra ID. They enable administrators to assign access to applications, resources, and directory roles at scale, reducing the need for individual user configuration and ensuring consistent, least-privilege access across the environment.

General

Microsoft Entra Roles Can Be Assigned	False
Creation Date	20 April 2026 11:07:37
Description	This group contains Exchange servers that run Exchange cmdlets on behalf of users via the management service. Its members have permission to read and modify all Windows accounts and groups. This group should not be deleted.
Email	
Group Type	Security
Membership Type	Assigned
Identifier	c6811fe5-bddf-42da-9138-64c60aa1abbe
Security Identifier	S-1-12-1-3330351077-1121631711-3328456849-3198918922

Expiration

Expiration Date	[Not Configured]
-----------------	------------------

On-Premises Settings

Synced From Active Directory	True
Last Sync Date	20 April 2026 11:07:38
Domain Name	centresolutionsdemo.int
SAM Account Name	Exchange Windows Permissions
Security Identifier	S-1-12-1-3330351077-1121631711-3328456849-3198918922

0 Owners

There are no owners found.	
----------------------------	--

1 Direct Group Members

Display Name	Member Type
 Exchange Trusted Subsystem	Group

ExchangeLegacyInterop

Microsoft Entra groups are directory objects used to centrally manage access and permissions for users, devices, and service principals within Microsoft Entra ID. They enable administrators to assign access to applications, resources, and directory roles at scale, reducing the need for individual user configuration and ensuring consistent, least-privilege access across the environment.

General

Microsoft Entra Roles Can Be Assigned	False
Creation Date	20 April 2026 11:07:37
Description	This group is for interoperability with Exchange 2003 servers within the same forest. This group should not be deleted.
Email	
Group Type	Security
Membership Type	Assigned
Identifier	c0c8e586-b024-4581-a105-6a1052c21468
Security Identifier	S-1-12-1-3234391430-1166127140-275383713-1746190930

Expiration

Expiration Date	[Not Configured]
-----------------	------------------

On-Premises Settings

Synced From Active Directory	True
Last Sync Date	20 April 2026 11:07:37
Domain Name	centrelsolutionsdemo.int
SAM Account Name	ExchangeLegacyInterop
Security Identifier	S-1-12-1-3234391430-1166127140-275383713-1746190930

0 Owners

There are no owners found.

0 Direct Group Members

There are no direct group members found.
--

Groups - G

Provides information about the groups defined in the organization with the specified first letter.

 **2 Groups**

Display Name	Group Type	Membership Type
 Group for Answers in Viva Engage – DO NOT DELETE 59131330561	Microsoft 365	Assigned
 Group for Answers in Viva Engage – DO NOT DELETE 63717335041	Microsoft 365	Assigned

Group for Answers in Viva Engage – DO NOT DELETE

59131330561

Microsoft Entra groups are directory objects used to centrally manage access and permissions for users, devices, and service principals within Microsoft Entra ID. They enable administrators to assign access to applications, resources, and directory roles at scale, reducing the need for individual user configuration and ensuring consistent, least-privilege access across the environment.

 General

Microsoft Entra Roles Can Be Assigned	False
Creation Date	25 November 2023 01:20:16
Description	Group that stores content and metadata for Answers in Viva Engage in network 59131330561. Deleting this this group will disrupt Answers in Viva Engage.
Email	groupforanswersinvivaengagedonotdelete59131330561118@centrelsolutionsdemo.onmicrosoft.com
Group Type	Microsoft 365
Membership Type	Assigned
Identifier	80a0ac32-5726-4050-adce-da5132e4b270
Security Identifier	S-1-12-1-2158013490-1079007014-1373294253-1890772018

 Expiration

Expiration Date	[Not Configured]
-----------------	------------------

 On-Premises Settings

Synced From Active Directory	False
------------------------------	-------

 1 Owners

Display Name	Identity	Type
 XIA	xia@centrelsolutionsdemo.onmicrosoft.com	User

 0 Direct Group Members

There are no direct group members found.
--

Group for Answers in Viva Engage – DO NOT DELETE 63717335041

Microsoft Entra groups are directory objects used to centrally manage access and permissions for users, devices, and service principals within Microsoft Entra ID. They enable administrators to assign access to applications, resources, and directory roles at scale, reducing the need for individual user configuration and ensuring consistent, least-privilege access across the environment.

General

Microsoft Entra Roles Can Be Assigned	False
Creation Date	31 January 2025 07:33:47
Description	Group that stores content and metadata for Answers in Viva Engage in network 63717335041. Deleting this this group will disrupt Answers in Viva Engage.
Email	groupforanswersinvivaengagedonotdelete63717335041744@centrelsolutionsdemo.onmicrosoft.com
Group Type	Microsoft 365
Membership Type	Assigned
Identifier	befd91a1-ec38-409a-9669-46a3a65dae54
Security Identifier	S-1-12-1-3204288929-1083894840-2739300758-1420713382

Expiration

Expiration Date	[Not Configured]
-----------------	------------------

On-Premises Settings

Synced From Active Directory	False
------------------------------	-------

1 Owners

Display Name	Identity	Type
 XIA	xia@centrelsolutionsdemo.onmicrosoft.com	User

0 Direct Group Members

There are no direct group members found.
--

Groups - H

Provides information about the groups defined in the organization with the specified first letter.

 **1 Groups**

Display Name	Group Type	Membership Type
 Help Desk	Security	Assigned

Help Desk

Microsoft Entra groups are directory objects used to centrally manage access and permissions for users, devices, and service principals within Microsoft Entra ID. They enable administrators to assign access to applications, resources, and directory roles at scale, reducing the need for individual user configuration and ensuring consistent, least-privilege access across the environment.

General

Microsoft Entra Roles Can Be Assigned	False
Creation Date	08 September 2026 15:18:53
Description	Members of this management role group can view and manage the configuration for individual recipients and view recipients in an Exchange organization. Members of this role group can only manage the configuration each user can manage on his or her own mailbox. Additional permissions can be added by assigning additional management roles to this role group.
Email	
Group Type	Security
Membership Type	Assigned
Identifier	69d4084b-18b7-4ae9-b4ad-a6c2d600b25c
Security Identifier	S-1-12-1-1775503435-1256790199-3265703348-1555169494

Expiration

Expiration Date	[Not Configured]
-----------------	------------------

On-Premises Settings

Synced From Active Directory	True
Last Sync Date	08 September 2026 15:18:53
Domain Name	centresolutionsdemo.int
SAM Account Name	Help Desk
Security Identifier	S-1-12-1-1775503435-1256790199-3265703348-1555169494

0 Owners

There are no owners found.	
----------------------------	--

1 Direct Group Members

Display Name	Member Type
 Demonstration User	User

Groups - I

Provides information about the groups defined in the organization with the specified first letter.

 **2 Groups**

Display Name	Group Type	Membership Type
 IT	Microsoft 365	Assigned
 IT Management	Security	Assigned

IT

Microsoft Entra groups are directory objects used to centrally manage access and permissions for users, devices, and service principals within Microsoft Entra ID. They enable administrators to assign access to applications, resources, and directory roles at scale, reducing the need for individual user configuration and ensuring consistent, least-privilege access across the environment.

General

Microsoft Entra Roles Can Be Assigned	False
Creation Date	27 March 2026 17:22:16
Description	Support for the IT team!
Email	IT@centrelsolutionsdemo.onmicrosoft.com
Group Type	Microsoft 365
Membership Type	Assigned
Identifier	a7461595-311a-410f-a4c3-e93c8f1b1e6a
Security Identifier	S-1-12-1-2806388117-1091514650-1021952932-1780358031

Expiration

Expiration Date	[Not Configured]
-----------------	------------------

On-Premises Settings

Synced From Active Directory	False
------------------------------	-------

2 Owners

Display Name	Identity	Type
 Demonstration User	DemoMailbox@centrelsolutionsdemo.onmicrosoft.com	User
 XIA	xia@centrelsolutionsdemo.onmicrosoft.com	User

2 Direct Group Members

Display Name	Member Type
 Test	User
 XIA	User

IT Management

Microsoft Entra groups are directory objects used to centrally manage access and permissions for users, devices, and service principals within Microsoft Entra ID. They enable administrators to assign access to applications, resources, and directory roles at scale, reducing the need for individual user configuration and ensuring consistent, least-privilege access across the environment.

General

Microsoft Entra Roles Can Be Assigned	False
Creation Date	20 May 2026 15:22:04
Description	
Email	
Group Type	Security
Membership Type	Assigned
Identifier	79f5d093-8391-4105-8697-08edd28d704e
Security Identifier	S-1-12-1-2046152851-1090880401-3976763270-1315999186

Expiration

Expiration Date	[Not Configured]
-----------------	------------------

On-Premises Settings

Synced From Active Directory	True
Last Sync Date	20 May 2026 15:22:04
Domain Name	centresolutionsdemo.int
SAM Account Name	IT Management
Security Identifier	S-1-12-1-2046152851-1090880401-3976763270-1315999186

0 Owners

There are no owners found.

1 Direct Group Members

Display Name	Member Type
 IT Manager	User

Groups - M

Provides information about the groups defined in the organization with the specified first letter.

 1 Groups

Display Name	Group Type	Membership Type
 Managed Availability Servers	Security	Assigned

Managed Availability Servers

Microsoft Entra groups are directory objects used to centrally manage access and permissions for users, devices, and service principals within Microsoft Entra ID. They enable administrators to assign access to applications, resources, and directory roles at scale, reducing the need for individual user configuration and ensuring consistent, least-privilege access across the environment.

 General

Microsoft Entra Roles Can Be Assigned	False
Creation Date	20 April 2026 11:07:37
Description	This group contains all the Managed Availability servers. This group shouldn't be deleted.
Email	
Group Type	Security
Membership Type	Assigned
Identifier	d3ce7af2-c144-4c02-9a44-e70f15002106
Security Identifier	S-1-12-1-3553524466-1275248964-266814618-102826005

 Expiration

Expiration Date	[Not Configured]
-----------------	------------------

 On-Premises Settings

Synced From Active Directory	True
Last Sync Date	20 April 2026 11:27:30
Domain Name	centresolutionsdemo.int
SAM Account Name	Managed Availability Servers
Security Identifier	S-1-12-1-3553524466-1275248964-266814618-102826005

 0 Owners

There are no owners found.

 1 Direct Group Members

Display Name	Member Type
 Exchange Servers	Group

Groups - S

Provides information about the groups defined in the organization with the specified first letter.

 1 Groups

Display Name	Group Type	Membership Type
 SQL Administrators	Security	Assigned

SQL Administrators

Microsoft Entra groups are directory objects used to centrally manage access and permissions for users, devices, and service principals within Microsoft Entra ID. They enable administrators to assign access to applications, resources, and directory roles at scale, reducing the need for individual user configuration and ensuring consistent, least-privilege access across the environment.

 General

Microsoft Entra Roles Can Be Assigned	False
Creation Date	13 April 2026 17:35:48
Description	
Email	
Group Type	Security
Membership Type	Assigned
Identifier	057c8b6f-93a3-40a9-abc3-de0517901f5b
Security Identifier	S-1-12-1-92048239-1084855203-98485163-1528795159

 Expiration

Expiration Date	[Not Configured]
-----------------	------------------

 On-Premises Settings

Synced From Active Directory	True
Last Sync Date	13 April 2026 17:43:06
Domain Name	centresolutionsdemo.int
SAM Account Name	SQL Administrators
Security Identifier	S-1-12-1-92048239-1084855203-98485163-1528795159

 0 Owners

There are no owners found.

 1 Direct Group Members

Display Name	Member Type
 XIA Configuration Client	User

Groups - T

Provides information about the groups defined in the organization with the specified first letter.

 **1 Groups**

Display Name	Group Type	Membership Type
 TestSite	Microsoft 365	Assigned

TestSite

Microsoft Entra groups are directory objects used to centrally manage access and permissions for users, devices, and service principals within Microsoft Entra ID. They enable administrators to assign access to applications, resources, and directory roles at scale, reducing the need for individual user configuration and ensuring consistent, least-privilege access across the environment.

General

Microsoft Entra Roles Can Be Assigned	False
Creation Date	04 October 2023 15:07:15
Description	This is a test
Email	TestSite@centrelsolutionsdemo.onmicrosoft.com
Group Type	Microsoft 365
Membership Type	Assigned
Identifier	84a906e3-5cca-4133-8d0a-23d8f87a2dfd
Security Identifier	S-1-12-1-2225669859-1093885130-3626175117-4247616248

Expiration

Expiration Date	[Not Configured]
-----------------	------------------

On-Premises Settings

Synced From Active Directory	False
------------------------------	-------

1 Owners

Display Name	Identity	Type
 XIA	xia@centrelsolutionsdemo.onmicrosoft.com	User

1 Direct Group Members

Display Name	Member Type
 XIA	User

Groups - W

Provides information about the groups defined in the organization with the specified first letter.

 **1 Groups**

Display Name	Group Type	Membership Type
 Windows Admin Center CredSSP	Security	Assigned

Windows Admin Center CredSSP

Microsoft Entra groups are directory objects used to centrally manage access and permissions for users, devices, and service principals within Microsoft Entra ID. They enable administrators to assign access to applications, resources, and directory roles at scale, reducing the need for individual user configuration and ensuring consistent, least-privilege access across the environment.

General

Microsoft Entra Roles Can Be Assigned	False
Creation Date	18 August 2026 11:16:29
Description	Members of CredSSP operations
Email	
Group Type	Security
Membership Type	Assigned
Identifier	faf59171-fd5e-4234-af72-4a502a93cb45
Security Identifier	S-1-12-1-4210397553-1110768990-1347056303-1170969386

Expiration

Expiration Date	[Not Configured]
-----------------	------------------

On-Premises Settings

Synced From Active Directory	True
Last Sync Date	18 August 2026 11:16:29
Domain Name	centresolutionsdemo.int
SAM Account Name	Windows Admin Center CredSSP
Security Identifier	S-1-12-1-4210397553-1110768990-1347056303-1170969386

0 Owners

There are no owners found.

0 Direct Group Members

There are no direct group members found.
--

Licenses

Provides information about the licenses defined in the organization.

4 Licenses

Display Name	Status	Total	Assigned	Available	Expiring Soon
 Microsoft 365 Business Premium	Enabled	1	1	0	0
 Microsoft Copilot Studio Viral Trial	Enabled	10,000	1	9,999	0
 Microsoft Entra ID P2	Enabled	1	1	0	0
 Microsoft Power Automate Free	Enabled	10,000	1	9,999	0

Microsoft 365 Business Premium

Provides information about the licenses defined in the organization.

General

Account Name	centrelsolutionsdemo
Account Identifier	157f8a9e-052c-4fc2-8b9f-11e8ccc55e96
License Status	Enabled
Total Units	1
Consumed Units	1
Subscription Identifiers	de5e5a1b-f9cc-48fc-a53f-8e291a889360
Target Class	User

SKU

SKU Part Number	SPB
SKU Identifier	cbdc14ab-d96c-4c30-b9f4-6ada7cdc1d46

Units Status

Enabled	1
Locked Out	0
Suspended	0
Warning	0

62 Service Plans

Display Name	Name	Identifier	Status
 Avatars for Teams	MESH_AVATARS_FOR_TEAMS	dcf9d2f4-772e-4434-b757-77a453cfbc02	Success
 Avatars for Teams (additional)	MESH_AVATARS_ADDITIONAL_FOR_TEAMS	3efbd4ed-8958-4824-8389-1321f8730af8	Success
 Azure Information Protection Premium P1	RMS_S_PREMIUM	6c57d4b6-3b23-47a5-9bc9-69f17b4947b3	Success
 Commercial data protection for Microsoft Copilot	Bing_Chat_Enterprise	0d0c0d31-fae7-41f2-b909-eaf4d7f26dba	Success
 Common Data Service - O365 P3	DYN365_CDS_O365_P3	28b0fa46-c39a-4188-89e2-58e979a6b014	Success
 Common Data Service for Teams_P3	CDS_O365_P3	afa73018-811e-46e9-988f-f75d2b1b8430	Success
 Data Loss Prevention	BPOS_S_DlpAddOn	9bec7e34-c9fa-40b7-a9d1-bd6d1165c7ed	Success
 DO NOT USE - Microsoft MyAnalytics (Full)	MICROSOFT_MYANALYTICS_FULL	0403bb98-9d17-4f94-b53e-eca56a7698a6	Success
 Exchange Foundation	EXCHANGE_S_FOUNDATION	113feb6c-3fe4-4440-bddc-54d774bf0318	Success
 Exchange Online (Plan 1)	EXCHANGE_S_STANDARD	9aaf7827-d63c-4b61-89c3-182f06f82e5c	Success
 EXCHANGE ONLINE ARCHIVING FOR EXCHANGE ONLINE	EXCHANGE_S_ARCHIVE_ADDON	176a09a6-7ec5-4039-ac02-b2791c6ba793	Success
 EXCHANGE_STORAGE_50GB	EXCHANGE_STORAGE_50GB	d59d7297-56ae-462e-b1ed-ad5b5c08bda7	Success
 Graph Connectors Search with Index	GRAPH_CONNECTORS_SEARCH_INDEX	a6520331-d7d4-4276-95f5-15c0933bc757	Success
 Immersive spaces for Teams	MESH_IMMERSIVE_FOR_TEAMS	f0ff6ac6-297d-49cd-be34-6dfe9f7f0c28	Success
 Insights by MyAnalytics	MYANALYTICS_P2	33c4f319-9bdd-48d6-9c4d-410b750a4a5a	Success
 Insights by MyAnalytics Backend	INSIGHTS_BY_MYANALYTICS	b088306e-925b-44ab-baa0-63291c629a91	Success
 Microsoft 365 Apps for business	OFFICE_BUSINESS	094e7854-93fc-4d55-b2c0-3ab5369ebdc1	Success
 Microsoft 365 Lighthouse (Plan 1)	M365_LIGHTHOUSE_CUSTOMER_PLAN1	6f23d6a9-adbf-481c-8538-b4c095654487	Success
 Microsoft 365 Lighthouse (Plan 2)	M365_LIGHTHOUSE_PARTNER_PLAN1	d55411c9-cfff-40a9-87c7-240f14df7da5	Success
 MICROSOFT AZURE MULTI-FACTOR AUTHENTICATION	MFA_PREMIUM	8a256a2b-b617-496d-b51b-e76466e88db0	Success
 Microsoft Bookings	MICROSOFTBOOKINGS	199a5c09-e0ca-4e37-8f7c-b05d533e1ea2	Success
 Microsoft Clipchamp	CLIPCHAMP	a1ace008-72f3-4ea0-8dac-33b3a23a2472	Success
 Microsoft Defender for Business	MDE_SMB	bfc1bbd9-981b-4f71-9b82-17c35fd0e2a4	Success

 Microsoft Defender for Cloud Apps Discovery	ADALLOM_S_DISCOVERY	932ad362-64a8-4783-9106-97849a1a30b9	Success
 Microsoft Defender for Office 365 (Plan 1)	ATP_ENTERPRISE	f20fedf3-f3c3-43c3-8267-2bfd51c0939	Success
 Microsoft Entra ID P1	AAD_PREMIUM	41781fb2-bc02-4b7c-bd55-b576c07bb09d	Success
 Microsoft Entra ID P1	AAD_SMB	de377cbc-0019-4ec2-b77c-3f223947e102	Success
 Microsoft Entra RIGHTS	RMS_S_ENTERPRISE	bea4c11e-220a-4e6d-8eb8-8ea15d019f90	Success
 MICROSOFT FORMS (PLAN E1)	FORMS_PLAN_E1	159f4cd6-e380-449f-a816-af1a9ef76344	Success
 Microsoft Intune	INTUNE_SMBIZ	8e9ff0ff-aa7a-4b20-83c1-2f636b600ac2	Success
 Microsoft Intune	INTUNE_A	c1ec4a95-1f05-45b3-a911-aa3fa01094f5	Success
 Microsoft Invoicing	DYN365BC_MS_INVOICING	39b5c996-467e-4e60-bd62-46066f572726	Success
 Microsoft Kaizala Pro Plan 2	KAIZALA_O365_P2	54fc630f-5a40-48ee-8965-af0503c1386e	Success
 Microsoft Loop	MICROSOFT_LOOP	c4b8c31a-fb44-4c65-9837-a21f55fcabda	Success
 Microsoft Planner	PROJECTWORKMANAGEMENT	b737dad2-2f6c-4c65-90e3-ca563267e8b9	Success
 Microsoft Search	MICROSOFT_SEARCH	94065c59-bc8e-4e8b-89e5-5138d471eaff	Success
 Microsoft StaffHub	Deskless	8c7d2df8-86f0-4902-b2ed-a0458298f3b3	Success
 Microsoft Stream for Office 365 E1	STREAM_O365_E1	743dd19e-1ce3-4c62-a3ad-49ba8f63a2f6	Success
 Microsoft Teams	TEAMS1	57ff2da0-773e-42df-b2af-ffb7a2317929	Success
 Mobile Device Management for Office 365	INTUNE_O365	882e1d05-acd1-4ccb-8708-6ee03664b117	Pending Activation
 Nucleus	Nucleus	db4d623d-b514-490b-b7ef-8885eee514de	Success
 Office for the Web	SHAREPOINTWAC	e95bec33-7c88-4a70-8e19-b10bd9d0c014	Success
 Office Shared Computer Activation	OFFICE_SHARED_COMPUTER_ACTIVATION	276d6e8a-f056-4f70-b7e8-4fc27f79f809	Success
 People Skills - Foundation	PEOPLE_SKILLS_FOUNDATION	13b6da2c-0d84-450e-9f69-a33e221387ca	Success
 Places Core	PLACES_CORE	1fe6227d-3e01-46d0-9510-0acad4ff6e94	Success
 Power Apps for Office 365	POWERAPPS_O365_P1	92f7a6f3-b89b-4bbd-8c30-809e6da5ad1c	Success
 Power Automate for Office 365	FLOW_O365_P1	0f9b09cb-62d1-4ff4-9129-43f4996f83f4	Success

 Power Virtual Agents for Office 365 P3	POWER_VIRTUAL_AGENTS_O365_P3	ded3d325-1bdc-453e-8432-5bac26d7a014	Success
 Project for Office (Plan E5)	PROJECT_O365_P3	b21a6b06-1988-436e-a07b-51ec6d9f52ad	Success
 Purview Discovery	PURVIEW_DISCOVERY	c948ea65-2053-4a5a-8a62-9eaaaf11b522	Success
 RETIRED - Outlook Customer Manager	O365_SB_Relationship_Management	5bfe124c-bbdc-4494-8835-f1297d457d79	Success
 SharePoint (Plan 1)	SHAREPOINTSTANDARD	c7699d2e-19aa-44de-8edf-1736da088ca1	Success
 Skype for Business Online (Plan 2)	MCOSTANDARD	0feaeb32-d00e-4d66-bd5a-43b5b83db82c	Success
 Sway	SWAY	a23b959c-7ce8-4e57-9140-b90eb88a9e97	Success
 To-Do (Plan 1)	BPOS_S_TODO_1	5e62787c-c316-451f-b873-1d05acd4d12c	Success
 Universal Print	UNIVERSAL_PRINT_01	795f6fe0-cc4d-4773-b050-5dde4dc704c9	Success
 Viva Engage Core	VIVAENGAGE_CORE	a82fbf69-b4d7-49f4-83a6-915b2cf354f4	Success
 Viva Learning Seeded	VIVA_LEARNING_SEEDED	b76fb638-6ba6-402a-b9f9-83d28acb3d86	Success
 Whiteboard (Plan 1)	WHITEBOARD_PLAN1	b8afc642-032e-4de5-8c0a-507a7bba7e5d	Success
 Windows 10/11 Business	WINBIZ	8e229017-d77b-43d5-9305-903395523b99	Success
 Windows Update for Business Deployment Service	WINDOWSUPDATEFORBUSINESS_DEPLOYMENTSERVICE	7bf960f6-2cd9-443a-8046-5dbff9558365	Success
 Yammer Enterprise	YAMMER_ENTERPRISE	7547a3fe-08ee-4ccb-b430-5077c5041653	Success

Microsoft Copilot Studio Viral Trial

Provides information about the licenses defined in the organization.

General

Account Name	centrelsolutionsdemo
Account Identifier	157f8a9e-052c-4fc2-8b9f-11e8ccc55e96
License Status	Enabled
Total Units	10,000
Consumed Units	1
Subscription Identifiers	93329940-d9c2-4b2f-847d-e7aa5897eef4
Target Class	User

SKU

SKU Part Number	CCIBOTS_PRIVPREV_VIRAL
SKU Identifier	606b54a9-78d8-4298-ad8b-df6ef4481c80

Units Status

Enabled	10,000
Locked Out	0
Suspended	0
Warning	0

3 Service Plans

Display Name	Name	Identifier	Status
 Common Data Service for CCI Bots	DYN365_CDS_CCI_BOTS	cf7034ed-348f-42eb-8bbd-dddeea43ee81	Success
 Dynamics 365 AI for Customer Service Virtual Agents Viral	CCIBOTS_PRIVPREV_VIRAL	ce312d15-8fdf-44c0-9974-a25a177125ee	Success
 Flow for CCI Bots	FLOW_CCI_BOTS	5d798708-6473-48ad-9776-3acc301c40af	Success

Microsoft Entra ID P2

Provides information about the licenses defined in the organization.

General

Account Name	centrelsolutionsdemo
Account Identifier	157f8a9e-052c-4fc2-8b9f-11e8ccc55e96
License Status	Enabled
Total Units	1
Consumed Units	1
Subscription Identifiers	62132298-d119-4385-a7b2-5398345549dd
Target Class	User

SKU

SKU Part Number	AAD_PREMIUM_P2
SKU Identifier	84a661c4-e949-4bd2-a560-ed7766fc2b

Units Status

Enabled	1
Locked Out	0
Suspended	0
Warning	0

5 Service Plans

Display Name	Name	Identifier	Status
 Exchange Foundation	EXCHANGE_S_FOUNDATION	113feb6c-3fe4-4440-bddc-54d774bf0318	Success
 MICROSOFT AZURE MULTI-FACTOR AUTHENTICATION	MFA_PREMIUM	8a256a2b-b617-496d-b51b-e76466e88db0	Success
 Microsoft Defender for Cloud Apps Discovery	ADALLOM_S_DISCOVERY	932ad362-64a8-4783-9106-97849a1a30b9	Success
 Microsoft Entra ID P1	AAD_PREMIUM	41781fb2-bc02-4b7c-bd55-b576c07bb09d	Success
 Microsoft Entra ID P2	AAD_PREMIUM_P2	eec0eb4f-6444-4f95-aba0-50c24d67f998	Success

Microsoft Power Automate Free

Provides information about the licenses defined in the organization.

General

Account Name	centrelsolutionsdemo
Account Identifier	157f8a9e-052c-4fc2-8b9f-11e8ccc55e96
License Status	Enabled
Total Units	10,000
Consumed Units	1
Subscription Identifiers	017a1d89-f1da-4bae-851b-bfe4df991e62
Target Class	User

SKU

SKU Part Number	FLOW_FREE
SKU Identifier	f30db892-07e9-47e9-837c-80727f46fd3d

Units Status

Enabled	10,000
Locked Out	0
Suspended	0
Warning	0

3 Service Plans

Display Name	Name	Identifier	Status
 Common Data Service - VIRAL	DYN365_CDS_VIRAL	17ab22cd-a0b3-4536-910a-cb6eb12696c0	Success
 Exchange Foundation	EXCHANGE_S_FOUNDATION	113feb6c-3fe4-4440-bddc-54d774bf0318	Success
 Flow Free	FLOW_P2_VIRAL	50e68c76-46c6-4674-81f9-75456511b170	Success

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.

144 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	
 Entra SOC Identity Responder	
 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/adminConsentRequestPolicy/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/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/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/entitlementManagement/allProperties/read microsoft.directory/oauth2PermissionGrants/allProperties/allTasks 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/adminConsentRequestPolicy/allProperties/read 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.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

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/mana ge 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 or password update 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 microsoft.directory/onPasswordUpdateCustomAuthenticationExtension/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-ae4-7d3fb86510f3
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	e93e3737-fa85-474a-ae4-7d3fb86510f3
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

Entra SOC Identity Responder

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 identity containment actions for SOC incident response, including disabling users, revoking sessions, and resetting passwords.
Identifier	58f930cc-fcf4-4152-852c-1d7dbf502139
Enabled	True
Privileged	True
Role Type	Built-In
Template Identifier	58f930cc-fcf4-4152-852c-1d7dbf502139
Version	1

Inheritance

Inherited Roles	Directory Readers
-----------------	-------------------

Allowed Permissions

Allowed Permissions	microsoft.directory/users/disable microsoft.directory/users/enable microsoft.directory/users/invalidateAllRefreshTokens microsoft.directory/users/password/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/mana ge
	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/tenantGovernance/policyTemplates/allProperties/update
	microsoft.directory/tenantGovernance/policyTemplates/create
	microsoft.directory/tenantGovernance/relationships/create
	microsoft.directory/tenantGovernance/requests/allProperties/update
	microsoft.directory/tenantGovernance/requests/create
	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.updateDeployments/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-ae3-d01accf2d47b
Enabled	True
Privileged	False
Role Type	Built-In
Template Identifier	95e79109-95c0-4d8e-ae3-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.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

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.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

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.directory/users/disable
	microsoft.directory/users/enable
	microsoft.directory/users/invalidateAllRefreshTokens
	microsoft.directory/users/password/update
	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 Tenant Governance, service principals, application role assignments, and permission grants through the approved Tenant Governance application.
Identifier	1981f584-96e9-4a6f-95b0-f522373f8fae
Enabled	True
Privileged	True
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.directory/signInReports/allProperties/read microsoft.directory/tenantGovernance/policyTemplates/allProperties/update microsoft.directory/tenantGovernance/policyTemplates/create microsoft.directory/tenantGovernance/relationships/create microsoft.directory/tenantGovernance/requests/allProperties/update microsoft.directory/tenantGovernance/requests/create 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.directory/signInReports/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

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.directory/signInReports/allProperties/read microsoft.directory/tenantGovernance/policyTemplates/allProperties/update microsoft.directory/tenantGovernance/policyTemplates/create microsoft.directory/tenantGovernance/relationships/create microsoft.directory/tenantGovernance/requests/create 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/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.updateDeployments/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

Users

Provides information about the users defined in the organization.

 **23 Users**

First Letter	Count
 #	0
 A	0
 B	1
 C	0
 D	2
 E	0
 F	1
 G	0
 H	3
 I	1
 J	0
 K	1
 L	0
 M	0
 N	0
 O	1
 P	0
 Q	0
 R	0
 S	8
 T	2
 U	0
 V	0
 W	0
 X	3
 Y	0
 Z	0

Users - B

Provides information about the users defined in the organization with the specified first letter.

 1 Users

Display Name		Assigned Licenses
	Backup Global Admin sysadmin@centrelsolutionsdemo.onmicrosoft.com	

Users - D

Provides information about the users defined in the organization with the specified first letter.

 2 Users

Display Name		Assigned Licenses
	Demonstration User DemoMailbox@centrelsolutionsdemo.onmicrosoft.com	
	DemonstrationPublicFoldersMailbox DemonstrationPublicFoldersMailbox@centrelsolutionsdemo.onmicrosoft.com	

Users - F

Provides information about the users defined in the organization with the specified first letter.

 1 Users

Display Name		Assigned Licenses
	FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042	
	FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042@centrelsolutionsdemo.onmicrosoft.com	

Users - H

Provides information about the users defined in the organization with the specified first letter.

 3 Users

Display Name		Assigned Licenses
	HealthMailbox-CSDEMO-EX01-001 HealthMailboxe2fbb8b92cee4460bf7dc4542afef125@centrelsolutionsdemo.onmicrosoft.com	
	HealthMailbox-CSDEMO-EX01-DemonstrationDatabase HealthMailbox91e96c8e2d204b2f9d683e544fb5e4ec@centrelsolutionsdemo.onmicrosoft.com	
	HealthMailbox-CSDEMO-EX01-DemonstrationPublicFoldersDatabase HealthMailboxa4f246f1e1ea4a99bb6f7917cf7dcf37@centrelsolutionsdemo.onmicrosoft.com	

Users - I

Provides information about the users defined in the organization with the specified first letter.

 1 Users

Display Name		Assigned Licenses
	IT Manager ITManager@centrelsolutionsdemo.onmicrosoft.com	

Users - K

Provides information about the users defined in the organization with the specified first letter.

 1 Users

Display Name		Assigned Licenses
	krbtgt_27401 krbtgt_27401@centrelsolutionsdemo.onmicrosoft.com	

Users - O

Provides information about the users defined in the organization with the specified first letter.

 1 Users

Display Name		Assigned Licenses
	On-Premises Directory Synchronization Service Account ADToAADSyncServiceAccount@centrelsolutionsdemo.onmicrosoft.com	

Users - S

Provides information about the users defined in the organization with the specified first letter.

 **8 Users**

Display Name		Assigned Licenses
	SQL Services SqlServices@centrelsolutionsdemo.onmicrosoft.com	
	SqlUser SqlUser@centrelsolutionsdemo.onmicrosoft.com	
	SystemMailbox{1f05a927-fdf8-4722-b470-72936861f2f1} SystemMailbox_1f05a927-fdf8-4722-b470-72936861f2f1_@centrelsolutionsdemo.onmicrosoft.com	
	SystemMailbox{2CE34405-31BE-455D-89D7-A7C7DA7A0DAA} SystemMailbox_2CE34405-31BE-455D-89D7-A7C7DA7A0DAA_@centrelsolutionsdemo.onmicrosoft.com	
	SystemMailbox{8cc370d3-822a-4ab8-a926-bb94bd0641a9} SystemMailbox_8cc370d3-822a-4ab8-a926-bb94bd0641a9_@centrelsolutionsdemo.onmicrosoft.com	
	SystemMailbox{bb558c35-97f1-4cb9-8ff7-d53741dc928c} SystemMailbox_bb558c35-97f1-4cb9-8ff7-d53741dc928c_@centrelsolutionsdemo.onmicrosoft.com	
	SystemMailbox{D0E409A0-AF9B-4720-92FE-AAC869B0D201} SystemMailbox_D0E409A0-AF9B-4720-92FE-AAC869B0D201_@centrelsolutionsdemo.onmicrosoft.com	
	SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9} SystemMailbox_e0dc1c29-89c3-4034-b678-e6c29d823ed9_@centrelsolutionsdemo.onmicrosoft.com	

Users - T

Provides information about the users defined in the organization with the specified first letter.

 2 Users

Display Name		Assigned Licenses
	Test test@centrelsolutionsdemo.onmicrosoft.com	
	Test\$ Test_@centrelsolutionsdemo.onmicrosoft.com	

Users - X

Provides information about the users defined in the organization with the specified first letter.

 3 Users

Display Name	Assigned Licenses
 XIA xia@centrelsolutionsdemo.onmicrosoft.com	Microsoft 365 Business Premium (Active) Microsoft Copilot Studio Viral Trial (Active) Microsoft Entra ID P2 (Active) Microsoft Power Automate Free (Active)
 XIA Configuration Client XiaClient@centrelsolutionsdemo.onmicrosoft.com	
 XIA Configuration Client XiaClient1793@centrelsolutionsdemo.onmicrosoft.com	

About XIA Configuration

XIA Configuration is an IT infrastructure audit and documentation tool that automates the process of collecting and documenting network configurations.