CONFIDENTIAL

Microsoft Entra ID Configuration

Comprehensive Identity & Access Management Documentation

Generated: 11/2/2025

Author: IT Security Team

Configuration Summary

Directory Roles: 3

Conditional Access Policies: 4

Applications: 6

Identity Governance Items: 11

PIM Schedules: 6

This document contains sensitive information about identity configurations.

Executive Summary

Conditional Access Policies	Directory Roles	Applications
4	3	6
4 enabled	6 members	3 registrations

Governance Items	PIM Schedules	Terms of Use
7	5	3
4 packages	3 role eligible	active agreements

Security Posture

MFA Coverage: 75% 3 of 4 enabled policies

Risk Indicators

Stale Policies (not modified in 90+ days)	1

Table of Contents

Directory Role Assignments

Total Roles: 3

Global Administrator

Can manage all aspects of Azure AD and Microsoft services that use Azure AD identities.

Role Type	Built-in
Role ID	62e90394-69f5-4237-9190-012177145e10
Template ID	62e90394-69f5-4237-9190-012177145e10
Total Members	2
Members	John Smith (john.smith@contoso.com) Sarah Johnson (sarah.johnson@contoso.com)

Security Administrator

Can read security information and reports, and manage configuration in Azure AD and Office 365.

Role Type	Built-in
Role ID	194ae4cb-b126-40b2-bd5b-6091b380977d
Template ID	194ae4cb-b126-40b2-bd5b-6091b380977d
Total Members	1

Members	Michael Chen (michael.chen@contoso.com)

Application Administrator

Can create and manage all aspects of app registrations and enterprise apps.

Role Type	Built-in
Role ID	9b895d92-2cd3-44c7-9d02-a6ac2d5ea5c3
Template ID	9b895d92-2cd3-44c7-9d02-a6ac2d5ea5c3
Total Members	3
Members	Emily Davis (emily.davis@contoso.com) David Wilson (david.wilson@contoso.com) Lisa Anderson (lisa.anderson@contoso.com)

Conditional Access Policies

Total Policies: 4

Require MFA for All Users

Created: 10/3/2025
Modified: 11/2/2025

State	enabled
Include Users	All

Exclude Users	None
Include Groups	None
Exclude Groups	breakglass-accounts
Include Roles	None
Exclude Roles	None
Include Applications	All
Exclude Applications	None
Include Locations	All
Exclude Locations	TrustedNetworks
Grant Operator	OR
Built-in Controls	mfa
Custom Authentication Factors	None
Terms of Use	None

Block Legacy Authentication

Created: 10/3/2025
Modified: 11/2/2025

State	enabled
Include Users	All
Exclude Users	None
Include Groups	None
Exclude Groups	None
Include Roles	None
Exclude Roles	None
Include Applications	All
Exclude Applications	None
Client App Types	exchangeActiveSync, other
Grant Operator	OR
Built-in Controls	block

Custom Authentication Factors	None
Terms of Use	None

Require Compliant Device for Admins

Created: 10/3/2025
Modified: 11/2/2025

State	enabled
Include Users	None
Exclude Users	None
Include Groups	None
Exclude Groups	None
Include Roles	62e90394-69f5-4237-9190-012177145e10, 194ae4cb-b126-40b2-bd5b-6091b380977d
Exclude Roles	None
Include Applications	All
Exclude Applications	None

Grant Operator	AND
Built-in Controls	compliantDevice, mfa
Custom Authentication Factors	None
Terms of Use	None

Require MFA from Untrusted Locations

Created: 7/25/2025
Modified: 7/25/2025

State	enabled
Include Users	All
Exclude Users	None
Include Groups	None
Exclude Groups	None
Include Roles	None
Exclude Roles	None
Include Applications	Office365

Exclude Applications	None
Include Locations	All
Exclude Locations	AllTrusted, OfficeLocations
Grant Operator	OR
Built-in Controls	mfa
Custom Authentication Factors	None
Terms of Use	None

Applications

Enterprise Applications

HR Management System

Application ID	a0b1c2d3-e4f5-6789-0123-456789abcdef
Service Principal Type	Application
Account Enabled	No
Sign-in Audience	Not specified

Home Page URL	None
Reply URLs	None
Tags	None

Salesforce

Application ID	d3e4f5a6-b7c8-9012-3456-789abcdef012
Service Principal Type	Application
Account Enabled	No
Sign-in Audience	Not specified
Home Page URL	None
Reply URLs	None
Tags	None

Microsoft 365

Application ID	e4f5a6b7-c8d9-0123-4567-89abcdef0123

Service Principal Type	Application
Account Enabled	No
Sign-in Audience	Not specified
Home Page URL	None
Reply URLs	None
Tags	None

App Registrations

HR Management System

Created: 10/3/2025

Application ID	a0b1c2d3-e4f5-6789-0123-456789abcdef
Sign-in Audience	AzureADMyOrg
API Permissions	Resource: 00000003-0000-0000-c000-000000000000 (Scope, Scope)
Owners	None

Customer Portal API

Created: 10/3/2025

Application ID	b1c2d3e4-f5a6-7890-1234-56789abcdef0
Sign-in Audience	AzureADMultipleOrgs
API Permissions	Resource: 00000003-0000-0000-c000-000000000000 (Role, Role)
Owners	None

Mobile Employee App

Created: 10/3/2025

Application ID	c2d3e4f5-a6b7-8901-2345-6789abcdef01
Sign-in Audience	AzureADMyOrg
API Permissions	Resource: 00000003-0000-0000-c000-000000000000 (Scope)
Owners	None

Application Policies

claims Mapping Policies

Employee ID Claims Mapping

definition	{"ClaimsMappingPolicy":{"Version":1,"IncludeBasicClaimSet":"true","ClaimsSchema":[{"Source":"user","ID":"extensionattribute1","SamlClaimType":"http://contoso.com/claims/employeeid"}]}}

token Lifetime Policies

Extended Session for HR App

definition	{"TokenLifetimePolicy":{"Version":1,"AccessTokenLifetime":"08:00:00"}}

permission Grant Policies

Require Admin Approval for High-Risk Permissions

Requires administrator approval for applications requesting high-risk permissions

Identity Governance

Access Packages

HR Systems Access

Access to HR applications and resources

Created: 10/3/2025
Modified: 11/2/2025

Catalog	Unknown
Is Hidden	No
State	Unknown

Sales Team Resources

Access package for sales team members

Created: 10/3/2025
Modified: 11/2/2025

Catalog	Unknown
Is Hidden	No

State	Unknown

Engineering Development Tools

Access to development environments and tools

Created: 10/3/2025
Modified: 11/2/2025

Catalog	Unknown
Is Hidden	No
State	Unknown

Finance System Access

Access to financial applications and reporting

Created: 10/3/2025
Modified: 11/2/2025

Catalog	Unknown
Is Hidden	No
State	Unknown

Catalogs

General Access Catalog

General catalog for access packages

Created: 10/3/2025

Catalog Type	Unknown

State	Unknown
Is Externally Visible	Yes

Engineering Resources

Catalog for technical and development resources

Created: 10/3/2025

Catalog Type	Unknown
State	Unknown
Is Externally Visible	No

Access Reviews

Quarterly Admin Roles Review

Quarterly review of administrative role assignments

Created: 10/3/2025

Status	Unknown
Scope	Unknown
Recurrence Type	absoluteMonthly
Duration in Days	0
Auto Apply Decisions	Disabled

Default Decision	None

Monthly Guest User Access Review

Review guest user access to resources

Created: 10/3/2025

Status	Unknown
Scope	Unknown
Recurrence Type	absoluteMonthly
Duration in Days	0
Auto Apply Decisions	Disabled
Default Decision	None

Semi-Annual Application Permissions Review

Review of application permissions and consent grants

Created: 10/3/2025

Status	Unknown
Scope	Unknown
Recurrence Type	absoluteMonthly

Duration in Days	0
Auto Apply Decisions	Disabled
Default Decision	None

Connected Organizations

Partner Organization

External partner for collaboration

Created: 10/3/2025

state	configured

Vendor Collaboration Portal

Vendor access for specific projects

Created: 10/3/2025

state	configured

Privileged Identity Management

Role Eligibility Schedules

User - Role

Principal	user-007
Role	62e90394-69f5-4237-9190-012177145e10

Directory Scope	/
Status	Unknown
Start DateTime	Not specified
Expiration Type	noExpiration

User - Role

Principal	user-008
Role	194ae4cb-b126-40b2-bd5b-6091b380977d
Directory Scope	/
Status	Unknown
Start DateTime	Not specified
Expiration Type	afterDuration

User - Role

Principal	user-010

Role	9b895d92-2cd3-44c7-9d02-a6ac2d5ea5c3
Directory Scope	/
Status	Unknown
Start DateTime	Not specified
Expiration Type	afterDuration

Role Assignment Schedules

Unnamed PIM Role Assignment

principal Id	user-011
role Definition Id	fe930be7-5e62-47db-91af-98c3a49a38b1
directory Scope Id	/
member Type	Direct
start Date Time	2025-10-03T12:06:53.981Z
schedule Info	expiration: type: afterDuration, duration: PT8H

Group Eligibility Schedules

Unnamed PIM Group Eligibility

principal Id	user-009
group Id	group-001
member Type	member
start Date Time	2025-10-03T12:06:53.981Z
schedule Info	expiration: type: noExpiration

Unnamed PIM Group Eligibility

principal Id	user-012
group Id	group-002
member Type	owner
start Date Time	2025-10-03T12:06:53.981Z
schedule Info	expiration: type: afterDuration, duration: P90D

Terms of Use Agreements

Corporate Data Access Terms

Created: 10/3/2025
Modified: 11/2/2025

Is Per Device Acceptance Required	No
Is Viewing Before Acceptance Required	No

GDPR Data Processing Agreement

Created: 10/3/2025
Modified: 11/2/2025

Is Per Device Acceptance Required	Yes
Is Viewing Before Acceptance Required	No

Remote Access Policy Acknowledgment

Created: 10/3/2025
Modified: 11/2/2025

Is Per Device Acceptance Required	No
Is Viewing Before Acceptance Required	No