Entra Conditional Access Documentation

centrelsolutionsdemo.onmicrosoft.com

Company Confidential

Document Properties

Author	CENTREL-WS01\XiaConfigurationDemo
Product	XIA Configuration Server [18.1.2.0]
Date	Tuesday, July 7, 2026 2:30:22 PM
Version	1.04

Table of Contents

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	Wednesday, December 1, 2021
Modification Date	Wednesday, December 1, 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	Wednesday, December 1, 2021
Modification Date	Wednesday, December 1, 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	Wednesday, December 1, 2021
Modification Date	Wednesday, December 1, 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	Wednesday, November 19, 2025 4:05:25 PM
Modification Date	Sunday, December 21, 2025 6:55:56 PM
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	Wednesday, December 24, 2025 10:27:56 AM
Continuous Access Evaluation Policy	Off	Wednesday, December 24, 2025 5:19:04 PM
Global Secure Access Policy	Report Only	Sunday, December 28, 2025 8:39:20 AM
Sample Policy 1	Off	Tuesday, December 2, 2025 3:41:58 PM
Sample Policy 2	Report Only	Wednesday, November 19, 2025 4:38:39 PM
Workloads Policy	Report Only	Tuesday, December 23, 2025 4:10:50 PM

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	Wednesday, December 24, 2025 10:27:56 AM
Modification Date	Wednesday, December 24, 2025 10:37:27 AM

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

The 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	Wednesday, December 24, 2025 5:19:04 PM
Modification Date	Wednesday, December 24, 2025 9:13:36 PM

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

The 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	Sunday, December 28, 2025 8:39:20 AM
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

The 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	Tuesday, December 2, 2025 3:41:58 PM
Modification Date	Tuesday, December 23, 2025 3:19:01 PM

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

The 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	Wednesday, November 19, 2025 4:38:39 PM
Modification Date	Sunday, December 21, 2025 6:57:48 PM

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	Tuesday, December 23, 2025 4:10:50 PM
Modification Date	Wednesday, December 24, 2025 9:24:25 AM

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

The 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	Tuesday, November 18, 2025 2:07:12 PM
Sample IP Location	IP Ranges	True	Tuesday, November 18, 2025 2:24:03 PM

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	Tuesday, November 18, 2025 2:07:12 PM
Modification Date	Sunday, December 21, 2025 6:52:22 PM
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	Tuesday, November 18, 2025 2:24:03 PM
Modification Date	Sunday, December 21, 2025 6:52:26 PM
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

About XIA Configuration

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