Azure Active Directory Conditional Access - Adoption Kit

Version: 3.0

For the latest version, please check https://aka.ms/aadadoptionkits

Contents

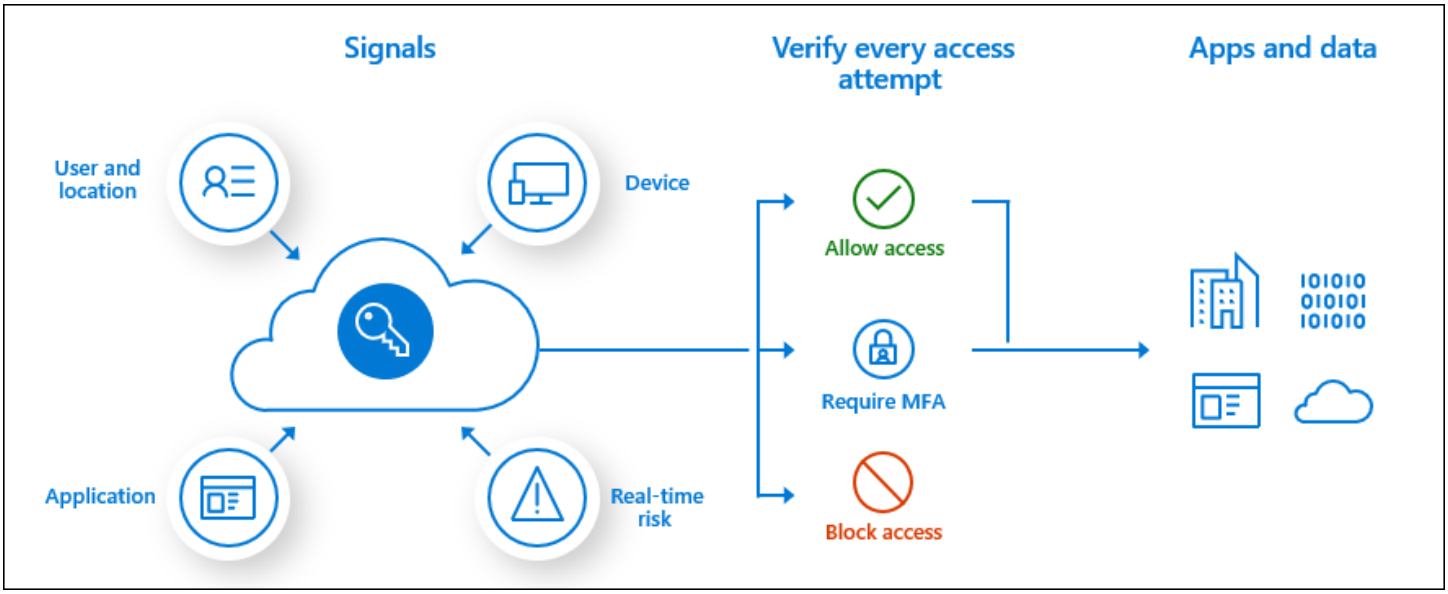
Awareness

This section helps you to analyze the benefits of Azure Active Directory Conditional Access. You will learn about the ease of use, benefits, pricing, and licensing model. You can also access up-to-date announcements and blogs that discuss ongoing improvements.

Business overview

In a mobile-first, cloud-first world, users can access your organization's resources from anywhere using a variety of devices and apps. As a result, just focusing on who can access a resource is no longer enough. You also need to be able to identify where the user is, the device being used, the app resource being accessed, and more.

To provide this control, Azure Active Directory (Azure AD) Conditional Access (CA) analyses signals such as user, device, and location to automate decisions and enforce organizational access policies for resource. For example, you can use CA policies to apply access controls such as Microsoft Azure Multi-Factor Authentication when needed to keep your organization secure and stay out of your users' way when not needed.



Key benefits

Using Conditional Access gives you the following benefits:

Increase productivity
CA policies allow you to control which users are prompted to use Multi-Factor Authentication, have access blocked, or when they must use a trusted device. They only interrupt users with Multi-Factor Authentication when one or more signals warrants it.

Manage risk
Coupling Conditional Access with Azure AD Identity Protection which detects anomalies and suspicious events, allows you to target when access to resources is blocked or gated. Automating risk assessment with policy conditions means risky sign-ins are at once identified and then remediated or blocked.

Address compliance and governance
Conditional Access enables you to audit access requests and approvals for the application, present terms of use for consent, and restrict access based on compliance policies.

Manage cost
Moving access policies to Azure AD reduces the reliance on custom or on-premises solutions for Conditional Access, and their infrastructure costs.

Pricing and licensing requirements

See Conditional Access license requirements. If additional features are required, you might also need related licenses.
For more information on pricing, see Azure AD pricing.

Announcements/blogs

Azure AD receives improvements on an ongoing basis. To stay up to date with the most recent developments, refer to What's new in Azure AD?

Training/learning resources

The following resources would be a good start to learn about Conditional Access. They include level 100 concepts, videos by our experts, books, link to online courses, and useful whitepapers for reference.

Level 100 concepts

Microsoft understands that some organizations have unique environment requirements or complexities. If yours is one of these organizations, use these recommendations as a starting point. However, most organizations can implement these recommendations as suggested.

- Find what is the identity secure score in Azure AD?
- Know the five steps to securing your identity infrastructure.
- Understand identity and device access configurations.

Refer to the following links to get started with Conditional Access:

- Read the Conditional Access overview
- Learn how to build a CA policy
- Learn about the common CA policies used
- Know how can you determine the impact of CA policies
- What are the best practices?
- Know what are classic policies
- Frequently Asked Questions (FAQs) on Conditional Access

For more information, deep-dive into Conditional Access documentation.

Training resources

Videos

Video	Description
How to get started with identity security	Learn about identity security, why is it important, and what you can do to get it more secure
How to improve your identity security posture with Secure Score	Get a walk-through of the identity secure score in the Azure AD portal.
What is Conditional Access?	Get an overview on Conditional Access.
How to deploy Conditional Access?	Learn to configure CA policies in the Azure portal.
How to roll out CA policies to end users?	Learn to roll out CA policies to end users in an organization.
Conditional Access with device controls	Learn the mechanics of how Azure AD works when you access a service connector such as Office 365, a line of business application, or a third party SaaS application using device controls, such as Intune compliant device or a hybrid Azure AD- join as a parameter.

Conditional Access with Multi-Factor Authentication	Learn the mechanics of how Azure AD works when you access a service connector such as Office 365, a line of business application, or a third party SaaS application when you tie it to a CA policy requiring Multi-Factor Authentication.
Enable Azure Active Directory Conditional Access for Secure User Access.	Learn how conditional access plays a role in other Enterprise and Mobility Suite's workloads.
How to upgrade your security with Multi-Factor Authentication	Learn how to use Multi-Factor Authentication with Conditional Access
How to start your journey to Zero Trust	Planning your CA policies in advance and having a set of active *and* fallback policies is a foundational pillar of your Access Policy enforcement in a Zero Trust deployment. Learn about zero trust, how it is implemented, and the components.
How to roll out recommended policies for identity security	Get an overview of Microsoft's recommended policies for establishing security while deploying Microsoft 365. You will also learn how to configure prescriptive policy recommendations for M365 security.

Books

Source: Oreilly- Implementing Azure Solutions - Second Edition.

Refer to the chapter **Deploying and Synchronizing Azure Active Directory** to learn about the role of Azure AD Conditional Access as a way to control and secure access to resources in the cloud and on-premises.

Online courses

Refer to the following courses on Conditional Access at pluralsight.com:

Course	Description
Design Identity Management in Microsoft Azure	This course guides you through the key items you need to know to design your identity management solution with Azure AD. Refer to **Using Roles and Access Control with Azure AD** module.
Design Authentication for Microsoft Azure	This course explains how to leverage Azure AD to solve all your cloud authentication requirements. Refer to **Authentication Requirements for Different Scenarios** module.
Design Authorization for Microsoft Azure	This course teaches authorization options available with Azure and Azure AD.

	Refer to **Authorization with Azure Resource Manager and Azure AD** module.

Whitepaper

Whitepaper	Description
Create a resilient access control management strategy with Azure Active Directory	This document provides guidance on strategies an organization might adopt to provide resilience to reduce the risk of lockout during unforeseen disruptions. For example, implement Multi-Factor Authentication using Conditional Access rather than per-user Multi-Factor Authentication.
Migrating your apps to Azure AD	This whitepaper details the planning for and benefits of migrating your application authentication to Azure AD. See how you can improve secure user access to applications and associated corporate data using CA policies.
Zero Trust Deployment Guide for Microsoft Azure Active Directory	This guidance is to assist you if you are engaging in Microsoft's Zero Trust security strategy.

Plan and change management

In this section, you deep-dive into planning and deploying CA policies for your organization.

Deployment plan

Planning your Conditional Access deployment is critical to make sure you achieve the required access strategy for apps and resources in your organization. You should spend most of your time during the planning phase of deployment to design the various policies you require to grant or block access to users under the conditions you choose.

Refer to Azure AD Conditional Access Deployment Plan - a comprehensive guide to plan and implement your CA policies. It includes the following sections:

Sections	Description
Prerequisites	Get prepared for the deployment
Plan the deployment project	Guidance to determine the strategy for this deployment in your environment
Understand CA policy components	How does an organization create these policies? What is required?
Follow best practices	Review each configuration policy before releasing it to avoid undesirable results.
Common policies	Typical policies deployed by organizations
Build and test policies	When new policy is ready, deploy them in phases in your environment
Manage access to cloud apps	Use the Manage options to control and manage your CA policies
Troubleshoot Conditional Access	Collect information to ease troubleshooting and follow the instructions

Quickstarts

Follow the step-by-step guidance to configure CA policy for these scenarios:

- Secure user sign-in events with Multi-Factor Authentication
- Require terms of use to be accepted before accessing cloud apps
- Block access when a session risk is detected

Customer stories/case studies

Discover how most organizations use Conditional Access to define and implement automated access control decisions to access cloud apps based on conditions.

The following featured stories demonstrate these needs:

Wipro drives mobile productivity with Microsoft cloud security tools to improve customer engagements. The CA policies in Azure AD have enabled the company to share documents, resources, and applications with trusted outside entities who can use their own credentials while maintaining control over its own corporate data.

Accenture safeguards its move to the cloud with Microsoft Cloud App security Accenture is evaluating the CA App Control feature of Cloud App Security, which uses Conditional Access to gate application access based on certain conditions. This feature could be useful for, say, enabling read-only file access while prohibiting downloads.

Aramex delivery unlimited - Global logistics and transportation company creates cloud-connected office with identity and access management solution. Ensuring secure access was especially difficult with Aramex's remote employees. The company is now applying Conditional Access to let these remote employees access their SaaS applications from outside the network. The Conditional Access rule will decide whether to enforce Multi-Factor Authentication, giving only the right people the right access.

To learn more about customer and partner experiences on Conditional Access, visit - See the amazing things people are doing with Azure.

Support and feedback

How can we improve Azure AD Conditional Access? This section provides links to discussion forums and technical community support email IDs.

We encourage you to join our Technical Community, a platform to Microsoft Azure Active Directory users and Microsoft to interact. It is a central destination for education and thought leadership on best practices, product news, live events, and roadmap.

If you have technical questions or need help with Azure, please try StackOverflow or visit the MSDN Azure AD forums.

Tell us what you think of Azure and what you want to see in the future. If you have suggestions, please submit an idea or vote up an idea at our User Voice Channel - feedback.azure.com.

Next steps

- Learn more about Multi-Factor Authentication
- Learn more about Identity Protection
- Manage CA policies with Microsoft Graph API