Azure Active Directory Conditional Access - Adoption Kit

Contents

Awareness

This section helps you to analyze the benefits of Azure Active Directory (Azure AD) Conditional Access. You will learn about the ease of use, pricing, and licensing model, as well as customer stories about how it helped improved their business. You will also receive up-to-date announcements and access to 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 need to be able to control who has access and identify where the user is and what device is being used as well as much more.

To provide this control, **Azure Active Directory (AD) Conditional Access** allows you to specify the conditions any user must meet for access to an application, such as Multi-Factor Authentication (MFA). Using conditional access policies controls how authorized users (users that have been granted access to a cloud app) access cloud apps under specific conditions. Refer to What is conditional access in Azure Active Directory?

For information on common access scenarios for using Azure AD Conditional Access, watch this video, Enable Azure Active Directory for Conditional Access for Secure User Access

Refer to Azure AD Conditional Access FAQs for common questions on using Conditional Access service.

Pricing and Licensing Requirements

Azure AD Conditional Access capability requires you to use Azure Active Directory Premium P1, Premium P2. For more information about licensing and editions, refer to Sign up for Azure Active Directory Premium editions.

For more information on pricing, refer to Azure Active Directory pricing.

Key Benefits

The key benefits of using Azure AD Conditional Access are:

Increase Productivity
Conditional Access policies allow you to target the point at which users are prompted to use MFA, have access blocked, or are required to use a trusted device. For example, you can set policies such as only requiring users to MFA into an application when off the corporate network. This keeps users more productive than if they have to MFA in each time. Furthermore, Azure AD Conditional Access allows you to specify policies per user basis, as with Active Directory Federation Service (ADFS), and also creates app specific policies.

Manage Risk
Enabling Conditional Access policies provides you with cloud-scale identity protection, risk-based access control capabilities, and native multi-factor authentication support. Coupling Azure AD Conditional Access with Azure AD Identity Protection allows you to define when access to an application is blocked or gated.

Address Compliance and Governance
Auditing access requests and approvals for the application, as well as understanding overall application usage is easier with Azure AD because it supports native audit logs for every application access request performed. Auditing includes requester identity, requested date, business justification, approval status, and approver identity. This data is also available from an API, which will enable importation of this data into a Security Incident and Event Monitoring (SIEM) system of choice.

Manage Cost
Moving access policies to Azure AD reduces reliance on custom or on-premises solutions such as ADFS for Conditional Access, reducing the cost of running that infrastructure.

Customer stories/Case studies

Discover how most organizations use Azure AD Conditional Access to define and implement automated access control decisions to access cloud apps based on conditions. The following featured stories demonstrate how these customer needs are met.

Wipro drives mobile productivity with Microsoft cloud security tools to improve customer engagements. The conditional access 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 Conditional Access App Control feature of Cloud App Security, which uses Azure Active Directory Conditional Access to gate application access based on certain conditions. LePenske says that this feature could be useful for, say, enabling read-only file access while prohibiting downloads.

Aramex delivery limited - 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 Azure AD Conditional Access, visit - See the amazing things people are doing with Azure.

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 Active Directory?

Blogs by the Tech Community and Microsoft Identity Division:

- September 24, 2018, Azure Active Directory conditional access in Azure Databricks
- September 21, 2018, Azure AD conditional access custom controls are in public preview

- September 21, 2018, Azure AD conditional access support for limited access with Microsoft Cloud App Security is now available
- September 21, 2018, Azure AD Conditional Access: Managed browser support for iOS/Android platforms now in preview
- September 21, 2018, Azure AD conditional access for country codes is in public preview
- September 21, 2018, Azure AD terms-of-use now available

Training/Learning Resources

The section provides concepts, role-based guidance, and lists the various training resources available on Azure AD Conditional Access.

Level 100 Knowledge/Concepts

Follow the links below to get an overview of how Azure AD Conditional Access functions.

- Learn "What is conditional access in Azure Active Directory?"
- Know "What are conditions in Azure Active Directory conditional access?"
- Know "What is the location condition in Azure Active Directory conditional access?"
- Know "What are access controls in Azure Active Directory conditional access?"
- Find "What is the what if tool in Azure Active Directory conditional access?"
- Follow Best practices for conditional access in Azure Active Directory

Additionally, refer to the following links for guidance to protect access to all services that are integrated with Azure Active Directory.

- What is baseline protection (preview)? Baseline protection ensures that you have at least the baseline level of security enabled in your Azure Active Directory environment.
- Identity and device access configurations. Describes how to configure secure access to cloud services through Enterprise Mobility + Security products by implementing a recommended environment and configuration, including a prescribed set of conditional access policies and related capabilities.
- Azure Active Directory conditional access settings reference. Learn:
  - What apps use conditional access?
  - What services are enabled with conditional access?
- Enable Azure Active Directory Conditional Access for Secure User Access. Watch this video to learn how Conditional Access plays a role in other Enterprise and Mobility Suite's workloads.

Role-Based Guidance

IT Administrator Staff

Sign in to your Azure portal as global administrator, security administrator, or conditional access administrator. Refer to Administrator role permissions in Azure Active Directory.

As an IT administrator, you use Azure AD conditional access to require users to authenticate using multi-factor authentication (MFA) or sign in from a trusted network or device.

Here are useful links to help you get started:

- Best practices for conditional access in Azure Active Directory
- Use Azure AD access reviews to manage users that have been excluded from conditional access policies
- How To: Plan your conditional access deployment in Azure Active Directory
- QuickStart: Require MFA for specific apps with Azure Active Directory conditional access
- QuickStart: Require terms of use to be accepted before accessing cloud apps
- QuickStart: Block access when a session risk is detected with Azure Active Directory conditional access
- Azure AD Conditional Access FAQs

Help Desk Staff

- Refer to Azure AD Conditional Access FAQs for common questions.
- For additional questions, you can also view the MSDN forum.
- If you cannot find the answer to a problem, our support teams are always available to assist you further. Use Contact Microsoft support.

Training

Videos

- Azure videos - Azure AD and Identity Show: Conditional Access General Availability
- Channel 9 - Lock down access to Azure using identity
- YouTube - Conditional Access in Enterprise Mobility + Security
- YouTube - Device-based Conditional Access
- YouTube - Enable Azure Active Directory for Conditional Access for Secure User Access

Online Courses

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

- Pluralsight.com: 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." Azure AD Conditional Access is covered in "Using Roles and Access Control with Azure AD" module.

- Pluralsight.com: Design Authentication for Microsoft Azure
  "This course explains how to leverage Azure AD to solve all your cloud authentication requirements." Azure AD Conditional Access is covered in "Authentication Requirements for Different Scenarios" module.

- Pluralsight.com: Design Authorization for Microsoft Azure
  "This course teaches authorization options available with Azure and Azure AD." Azure AD Conditional Access is covered in "Authorization with Azure Resource Manager and Azure AD" module.

Books

- Oreilly- Implementing Azure Solutions - Second Edition.

"Get up and running with Azure services and learn how to implement them in your organization. Azure AD Conditional Access is covered in the chapter Deploying and Synchronizing Azure Active Directory."

- Amazon- Mastering Microsoft Azure Infrastructure Services
  "Here's everything you need to understand, evaluate, deploy, and maintain environments that utilize Microsoft Azure."

Tutorials

- Quickstart: Require MFA for specific apps with Azure Active Directory conditional access
  This quickstart shows how to configure an Azure AD conditional access policy that requires multi-factor authentication for a selected cloud app in your environment.

- Quickstart: Require terms of use to be accepted before accessing cloud apps
  This quickstart shows how to configure an Azure AD conditional access policy that requires a ToU to be accepted for a selected cloud app in your environment.

- Quickstart: Block access when a session risk is detected with Azure Active Directory conditional access
  This quickstart shows how to configure a conditional access policy that blocks a sign-in when a configured sign-in risk level has been detected.

- Tutorial: Migrate a classic policy that requires multi-factor authentication in the Azure portal
  This tutorial shows how to migrate a classic policy that requires multi-factor authentication (MFA) for a cloud app.

Whitepaper

- Published December 18, 2018, 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.

- Published September 18, 2018, Resources for migrating applications to Azure Active Directory
  This whitepaper includes a list of resources to help you migrate application access and authentication to Azure Active Directory (Azure AD).

- Published July 12, 2018 Azure Security and Compliance Blueprint: PaaS Web Application Hosting for UK OFFICIAL Workloads
  Azure Blueprints consist of guidance documents and automation templates that deploy cloud-based architectures to offer solutions to scenarios that have accreditation or compliance requirements.

FAQ

Refer to Azure AD Conditional Access FAQs for common questions.

End-user Readiness and Communication

This section provides customizable posters and email templates to roll out Azure AD Conditional Access to your organization.

Refer to the templates in the following end-user readiness and communication links:

- Multi-Factor Authentication rollout materials
- Self-Service Password Reset rollout materials

Planning and Change Management

This section provides the resource links to Azure AD Conditional Access deployment plan and topology to help you determine your Conditional Access strategies, and document your decisions and configurations to prepare for implementation.

Deployment Plan

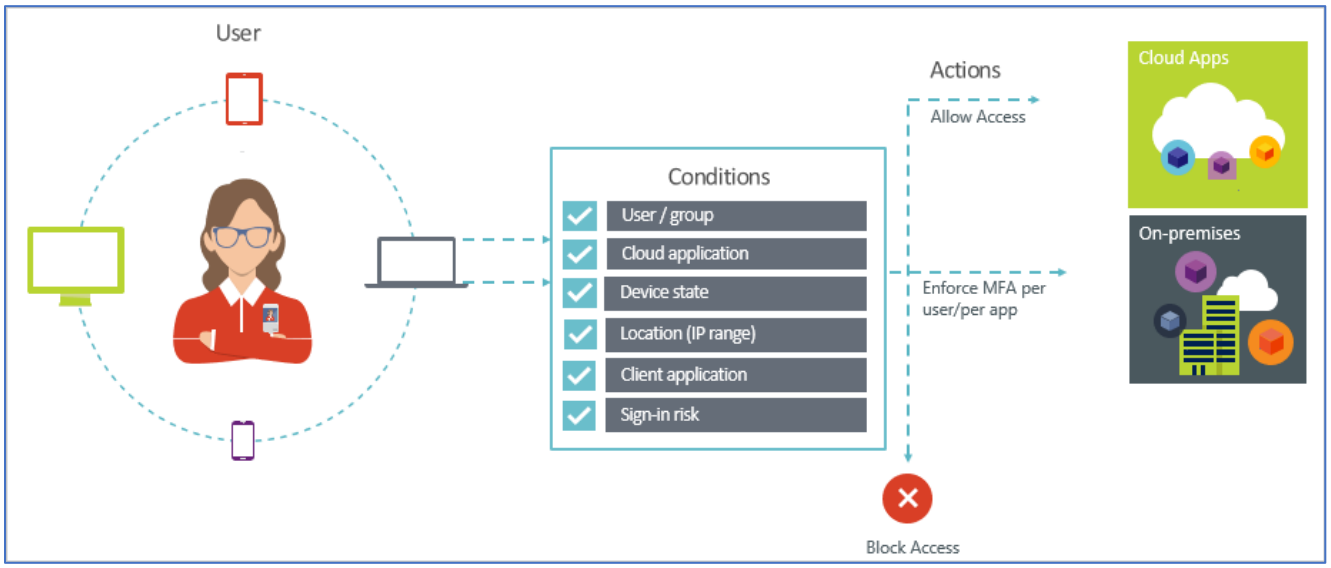
Planning your conditional access deployment is critical to make sure you achieve the required access strategy for apps and resources in your organization. You should spend most of your time during the planning phase of deployment to design the various policies you require to grant or block access to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

Refer to the following links:

- The step-by-step Azure AD Conditional Access Deployment Plan
- How To: Plan your conditional access deployment in Azure Active Directory

Architecture Plan/Topology

With conditional access, you can implement automated access control decisions for accessing your cloud apps that are based on conditions.



Testing

This section provides the plan to test the functionality of Azure AD Conditional Access in a sandbox or test lab environment before the customer rolls it into production.

We recommend starting with a set of pilot users and groups before rolling out a Conditional Access policy to the entire set of users and groups that the policy covers.

Refer to the following links:

- Test your policy section of How To: Plan your conditional access deployment in Azure Active Directory.
- QuickStart: Block access when a session risk is detected with Azure Active Directory Identity Protection

Deployment

How can I get Azure AD Conditional Access deployed in my environment? This section provides resource links to help with implementation of your solution.

Deployment

To set up and use Azure AD Conditional Access, follow the guidance under "Implementing Your Solution" section in the Azure AD Conditional Access deployment plan.

You can also refer to the following links:

- Move to production section of How To: Plan your conditional access deployment in Azure Active Directory
- How should you deploy a new policy?
- Policy deployment
- How To: Set up SharePoint Online and Exchange Online for Azure Active Directory conditional access
- What is a policy migration in Azure Active Directory conditional access?

Readiness Checklist

Follow the readiness checklist under "Implementing Your Solution" section in the Azure AD Conditional Access Deployment Plan.

Design Template

Follow the design template under "Implementing Your Solution" section in the Azure AD Conditional Access Deployment Plan.

Operations

How do I manage and maintain Azure AD Conditional Access? This section provides troubleshooting info, Azure AD User Provisioning operation and management details, and other important references.

Operations

Follow the guidance under "Manage Your Solution" section in the Azure AD Conditional Access Deployment Plan.

Other useful links:

- Best practices for conditional access in Azure Active Directory
- What is a policy migration in Azure Active Directory conditional access?

Monitoring

Refer to the following Azure AD Conditional Access reporting links:

- Sign-in activity reports in the Azure Active Directory portal
- Reports in Azure Multi-Factor Authentication

How-To Guides

- How to: Block legacy authentication to Azure AD with conditional access
- How To: Set up SharePoint Online and Exchange Online for Azure Active Directory conditional access
- How To: Require approved client apps for cloud app access with conditional access
- How To: Require managed devices for cloud app access with conditional access
- How to: Require MFA for access from untrusted networks with conditional access

Troubleshooting

Refer to the following links:

- Azure Active Directory conditional access FAQs for frequent questions.
- What is the "what if" tool in Azure Active Directory conditional access? Use this tool to assess your conditional access policies.

References

Refer to Azure Active Directory conditional access settings reference. This article provides you with support information for the following configuration options in a conditional access policy:

- Cloud applications assignments
- Device platform condition
- Client applications condition
- Approved client application requirement

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.