Microsoft Security

Conditional Access in Azure Active Directory

Enforce granular access control

As more and more companies adopt cloud computing, hybrid work, and the use of non–corporate owned devices on company networks, it has become increasingly difficult to control access to enterprise resources. Conditional Access is an intelligent security policy engine built for this challenge—with its robust controls, you can define specific conditions for how users authenticate and gain access to applications and data.

Redefine how enterprise resources are accessed with Conditional Access

Enhanced security:

Enforce access controls with adaptive polices for security that goes beyond basic username and password authentication.

Improved user experience:

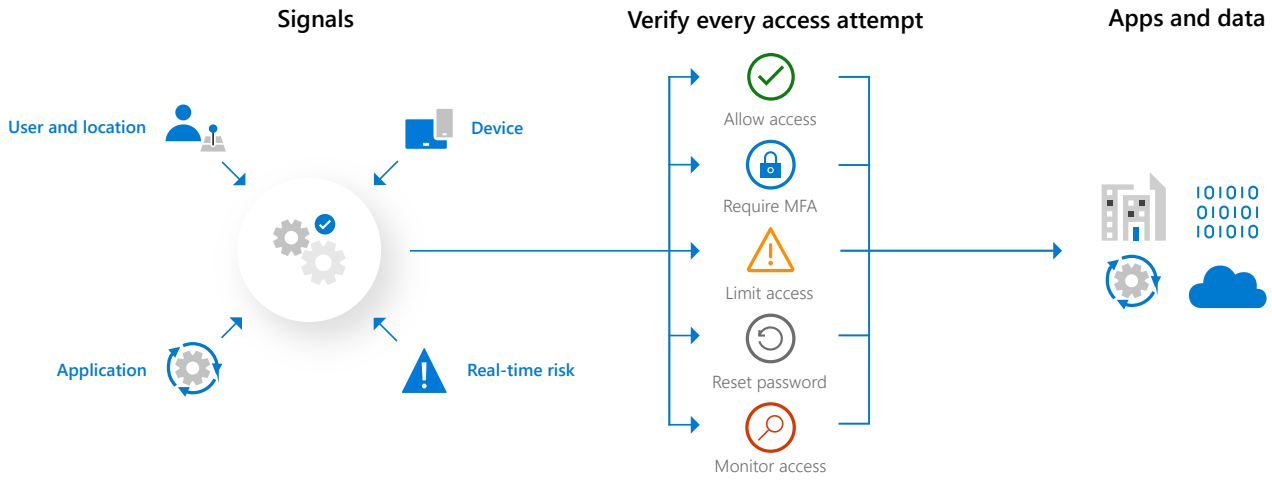
Create security conditions that support—rather than inhibit—your organization's daily workflows.

Increased flexibility:

Grant the right people uninterrupted access to your apps and data—from anywhere.

How does Conditional Access work?

At their simplest, Conditional Access policies are if-then statements.
If a user wants to access a resource, then they must complete an action.



The Conditional Access process: First, real-time signals from users, devices, locations, apps, data labels, and risk analyses are aggregated. Then, decisions are enforced based on the aggregated signals. Common decisions are based on signals, including block, limit, allow access, or require additional steps (such as multifactor authentication or password reset). Finally, the decisions are enforced on apps and data once Conditional Access has determined the appropriate action.

Note: Conditional Access policies are enforced after first-factor authentication has been completed.

Integration capabilities

Conditional Access can integrate with Microsoft Defender and Microsoft Endpoint Manager to provide more control—for example, to enforce a read-only decision inside an app or block access from a compromised device.

Conditional Access can be used to:

Enforce access controls

Adopt a robust Zero Trust strategy that uses policies and real-time signals to determine when to allow, block, or limit access, or when to provide additional proofs like multifactor authentication.

Help protect data inside apps

Monitor and control sessions and sensitive data in real time across your organization based on user behavior in apps (both on-premises and in the cloud).

Restrict access to vulnerable and compromised devices

Once devices are enrolled in Microsoft Intune, you can enforce more granular, risk-based access policies with Conditional Access—like blocking access to vulnerable devices or limiting access to unmanaged devices.

Fine-tune access policies based on actionable insights

Quickly see the impact of one or more policies over a specific period in the insights and reporting dashboard to understand the impact of Conditional Access policies over time.

"

Identity is the new firewall of the future. We can't continue to use our old way of controlling application access because business isn't happening exclusively in our network anymore. With Azure Active Directory Premium, we can stay in control no matter where our users roam.

— Will Lamb, Infrastructure Coordinator, Whole Foods Market

Get started with
Azure Active Directory

©2022 Microsoft Corporation. All rights reserved.