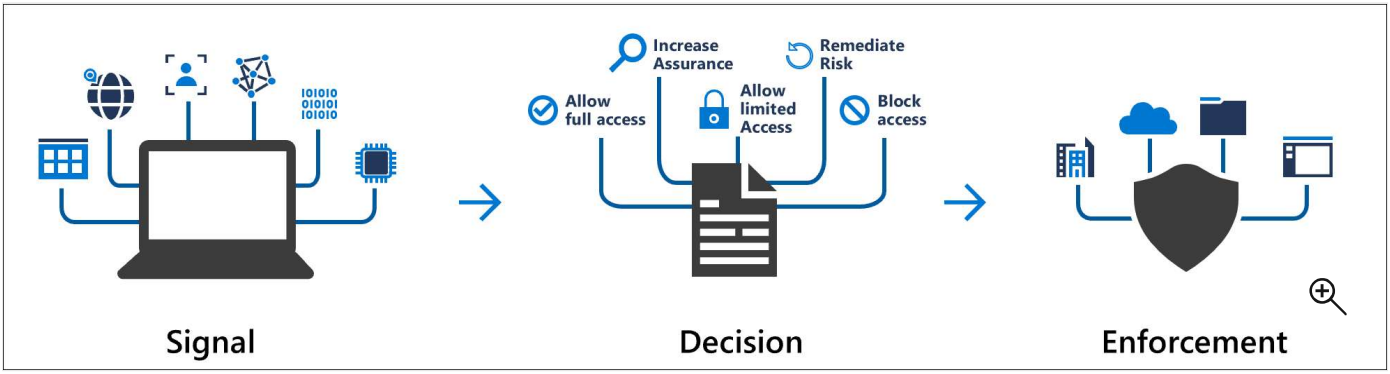
# What is Conditional Access?

03/04/2025

Modern security extends beyond an organization's network perimeter to include user and device identity. Organizations now use identity-driven signals as part of their access control decisions. Microsoft Entra Conditional Access brings signals together, to make decisions, and enforce organizational policies. Conditional Access is Microsoft's Zero Trust policy engine taking signals from various sources into account when enforcing policy decisions.




Conditional Access policies at their simplest are if-then statements; **if** a user wants to access a resource, **then** they must complete an action. For example: If a user wants to access an application or service like Microsoft 365, then they must perform multifactor authentication to gain access.

Administrators are faced with two primary goals:

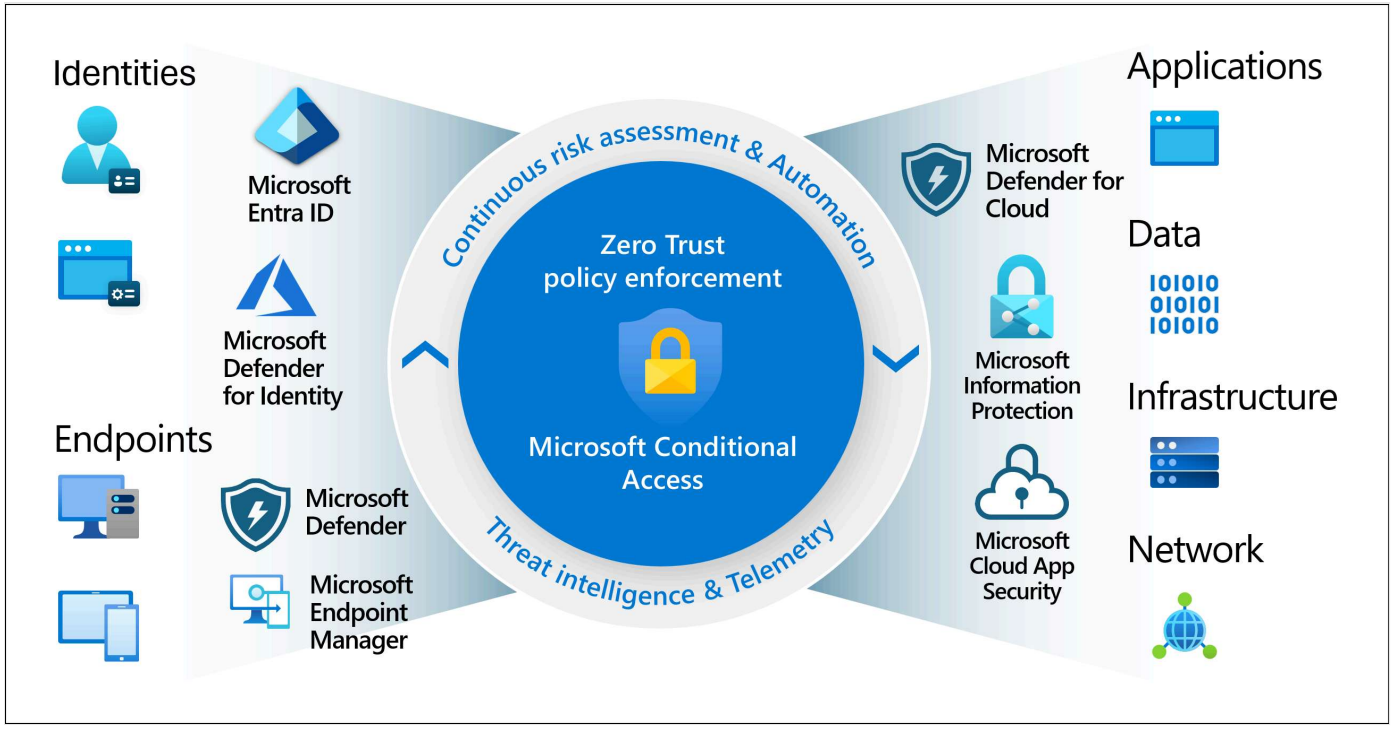
- Empower users to be productive wherever and whenever
- Protect the organization's assets

Use Conditional Access policies to apply the right access controls when needed to keep your organization secure.

> ⓘ **Important**
>
> Conditional Access policies are enforced after first-factor authentication is completed. Conditional Access isn't intended to be an organization's first line of defense for scenarios like denial-of-service (DoS) attacks, but it can use signals from these events to determine access.

## Common signals

Conditional Access takes signals from various sources into account when making access decisions.




These signals include:

- User or group membership
  - Policies can be targeted to specific users and groups giving administrators fine-grained control over access.
- IP Location information
  - Organizations can create trusted IP address ranges that can be used when making policy decisions.
  - Administrators can specify entire countries or regions IP ranges to block or allow traffic from.
- Device
  - Users with devices of specific platforms or marked with a specific state can be used when enforcing Conditional Access policies.
  - Use filters for devices to target policies to specific devices like privileged access workstations.
- Application
  - Users attempting to access specific applications can trigger different Conditional Access policies.
- Real-time and calculated risk detection
  - Signals integration with Microsoft Entra ID Protection lets Conditional Access policies identify and remediate risky users and sign-in behavior.
- Microsoft Defender for Cloud Apps

- Lets user application access and sessions be monitored and controlled in real time. This integration increases visibility and control over access to and activities done within your cloud environment.

# Common decisions

- Block access
  - Most restrictive decision
- Grant access
- Less restrictive decision that can require one or more of the following options:
  - Require multifactor authentication
  - Require authentication strength
  - Require device to be marked as compliant
  - Require Microsoft Entra hybrid joined device
  - Require approved client app
  - Require app protection policy
  - Require password change
  - Require terms of use

# Commonly applied policies

Many organizations have common access concerns that Conditional Access policies can help with, such as:

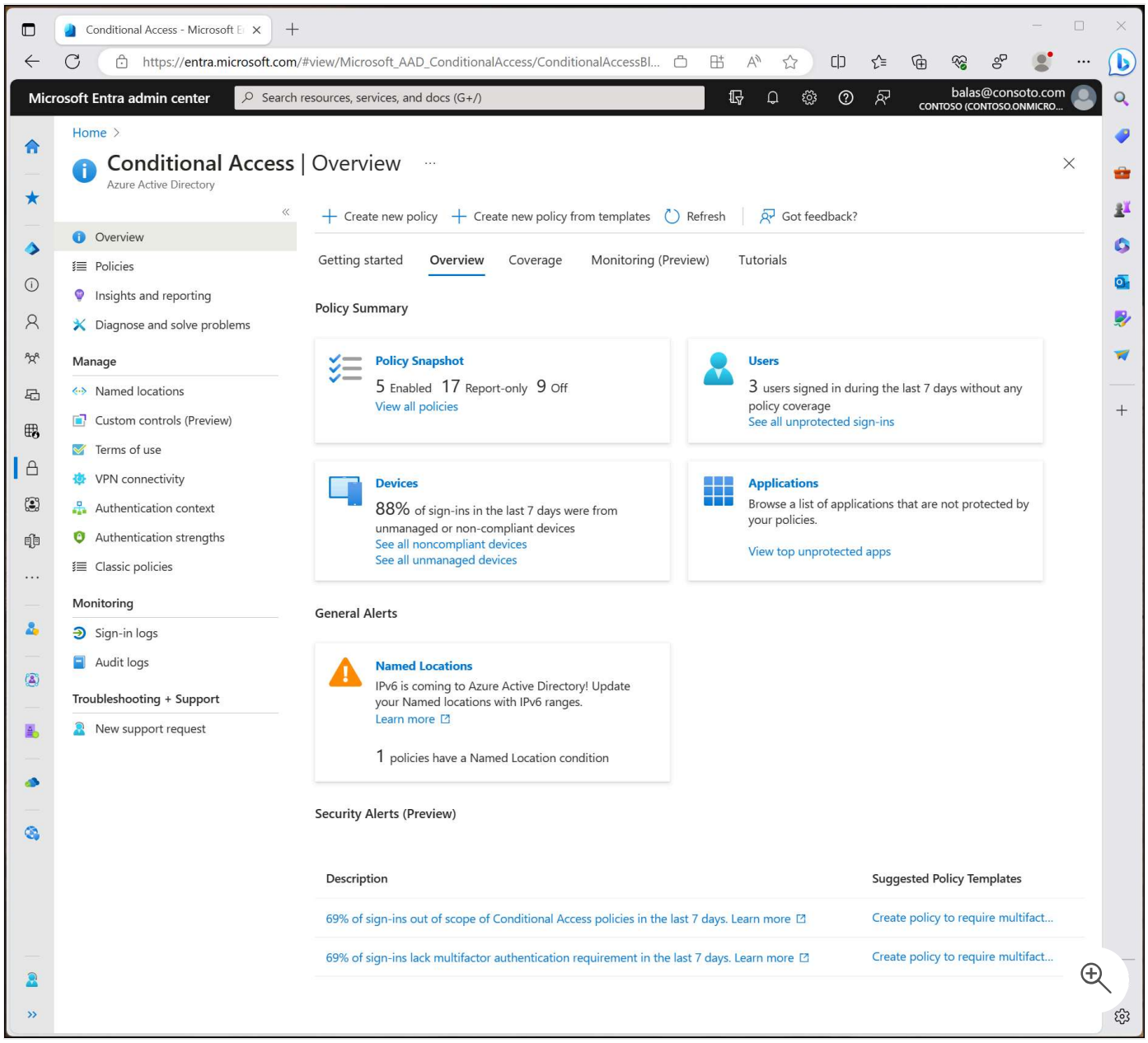
- Requiring multifactor authentication for users with administrative roles
- Requiring multifactor authentication for Azure management tasks
- Blocking sign-ins for users attempting to use legacy authentication protocols
- Requiring trusted locations for security information registration
- Blocking or granting access from specific locations
- Blocking risky sign-in behaviors
- Requiring organization-managed devices for specific applications

Admins can create policies from scratch or start from a template policy in the portal or using the Microsoft Graph API.

# Administrator experience

Administrators with the Conditional Access Administrator role can manage policies.

Conditional Access is found in the Microsoft Entra admin center under **Entra ID** > **Conditional Access**.




- The **Overview** page provides a summary of policy state, users, devices, and applications, as well as general and security alerts with suggestions.
- The **Coverage** page provides a synopsis of applications with and without Conditional Access policy coverage over the last seven days.
- The **Monitoring** page allows administrators to see a graph of sign-ins that can be filtered to see potential gaps in policy coverage.

Conditional Access policies on the **Policies** page can be filtered by administrators based on items like the actor, target resource, condition, control applied, state, or date. This filtering ability lets administrators find specific policies based on their configuration quickly.

# License requirements

Using this feature requires Microsoft Entra ID P1 licenses. To find the right license for your requirements, see Compare generally available features of Microsoft Entra ID .

Customers with Microsoft 365 Business Premium licenses also have access to Conditional Access features.

Risk-based policies require access to Microsoft Entra ID Protection, which requires P2 licenses.

Other products and features that interact with Conditional Access policies require appropriate licensing for those products and features.

When licenses required for Conditional Access expire, policies aren't automatically disabled or deleted. This lets customers migrate away from Conditional Access policies without a sudden change in their security posture. Remaining policies can be viewed and deleted, but no longer updated.

Security defaults help protect against identity-related attacks and are available for all customers.

# Zero Trust

This feature helps organizations to align their identities with the three guiding principles of a Zero Trust architecture:

- Verify explicitly
- Use least privilege
- Assume breach

To find out more about Zero Trust and other ways to align your organization to the guiding principles, see the Zero Trust Guidance Center.

# Next steps

- Building a Conditional Access policy piece by piece
- Plan your Conditional Access deployment