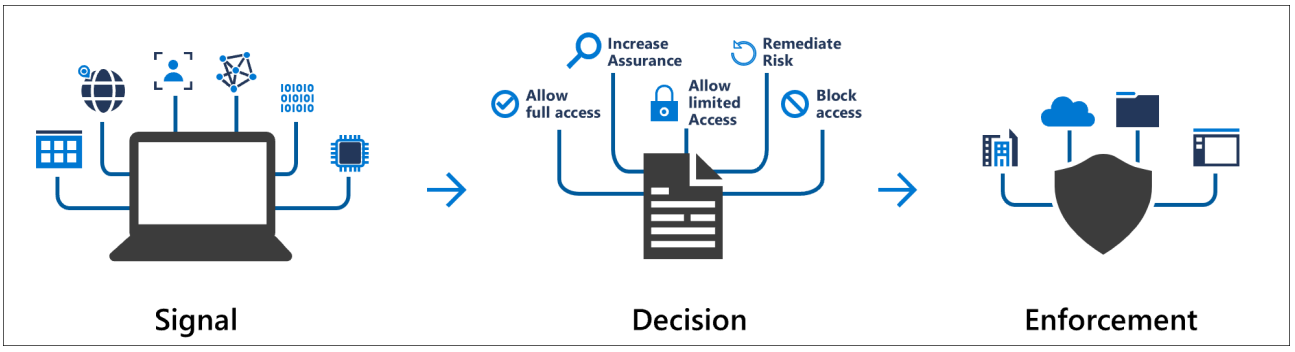
Microsoft Entra Conditional Access: Zero Trust Policy Engine - Microsoft Entra ID

By kenwith

Archived: 2026-04-05 12:37:49 UTC

Overview

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.

Admins are faced with two primary goals:

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

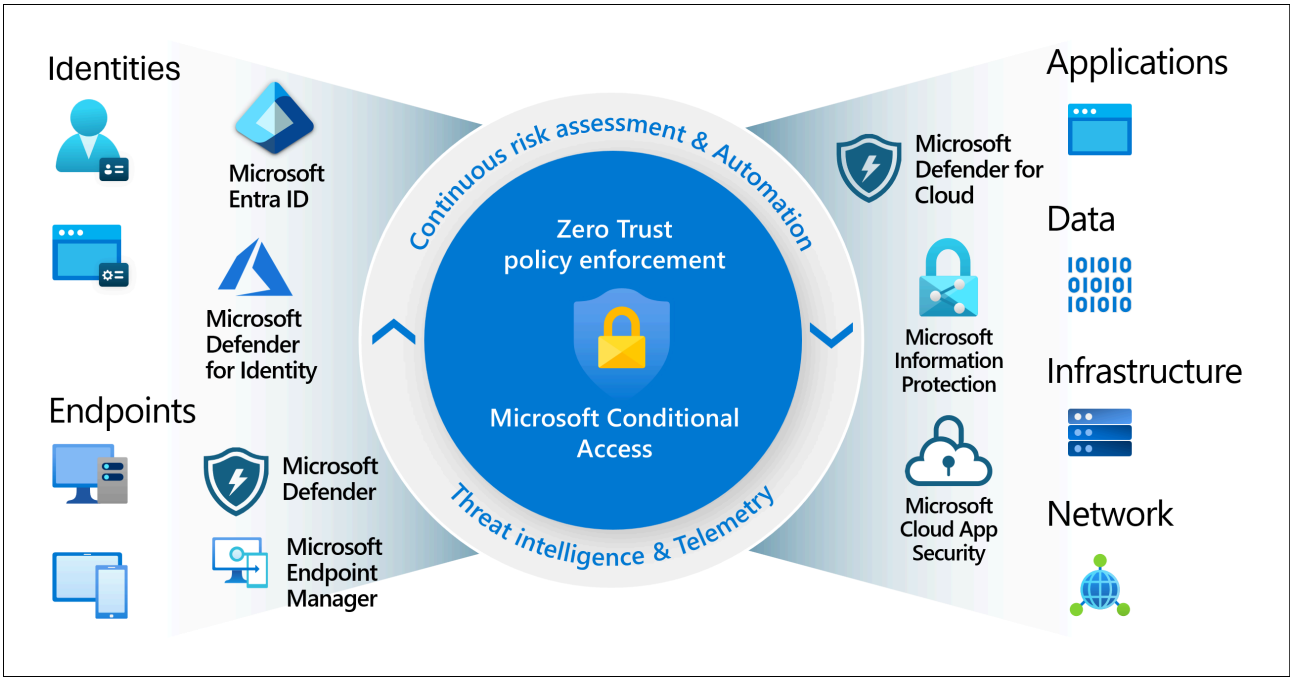
Use Conditional Access policies to apply the right access controls when needed to keep your organization secure and don't interfere with productivity.

Important

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

Common signals

Conditional Access uses signals from various sources to make access decisions.



Some of these signals include:

- **User, group, or agent**
  - Policies can be targeted to specific users, groups, and agents (Preview) giving admins fine-grained control over access.
  - Support for agent identities and agent users extends Zero Trust principles to AI workloads.
- **IP location information**
  - Organizations can create IP address ranges that can be used when making policy decisions.
  - Admins can specify entire countries/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**
  - Trigger different Conditional Access policies when users attempt to access specific applications.
  - Apply policies to traditional cloud apps, on-premises applications, and agent resources.
- **Real-time and calculated risk detection**
  - Integrates signals from Microsoft Entra ID Protection to identify and remediate risky users, sign-in behavior, and agent activities.
- **Microsoft Defender for Cloud Apps**
  - Monitors and controls user application access and sessions in real time. This integration improves visibility and control over access and activities in your cloud environment.

Common decisions

- Block access is the most restrictive decision.
- Grant access
- A less restrictive decision that might require one or more of the following options:
    - Require multifactor authentication
    - Require authentication strength
    - Require the device to be marked as compliant
    - Require a Microsoft Entra hybrid joined device
    - Require an approved client app
    - Require an app protection policy
    - Require a 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 who try 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

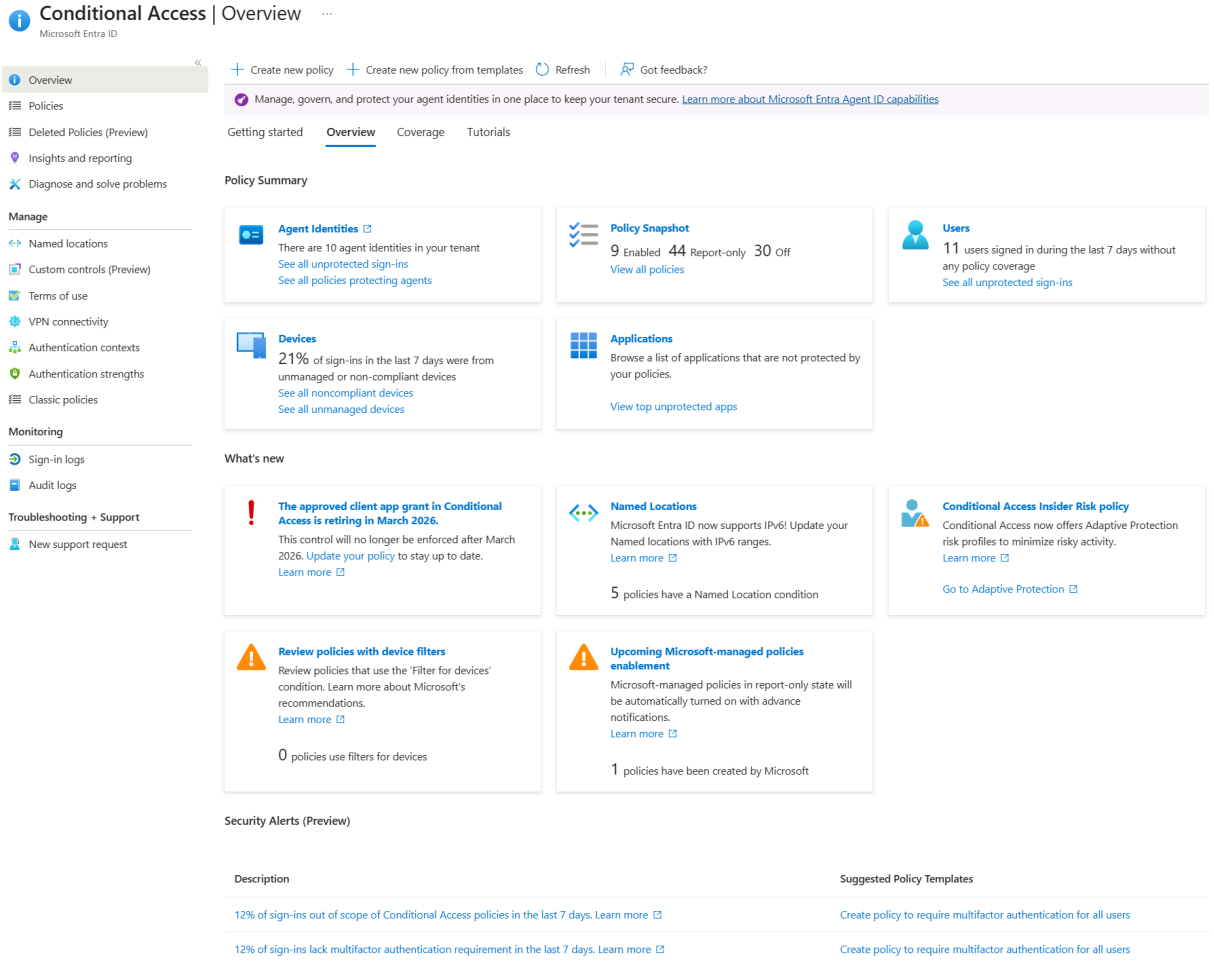
Admins can create policies from scratch or start with a template policy in the portal or by using the Microsoft Graph API.

Admin experience

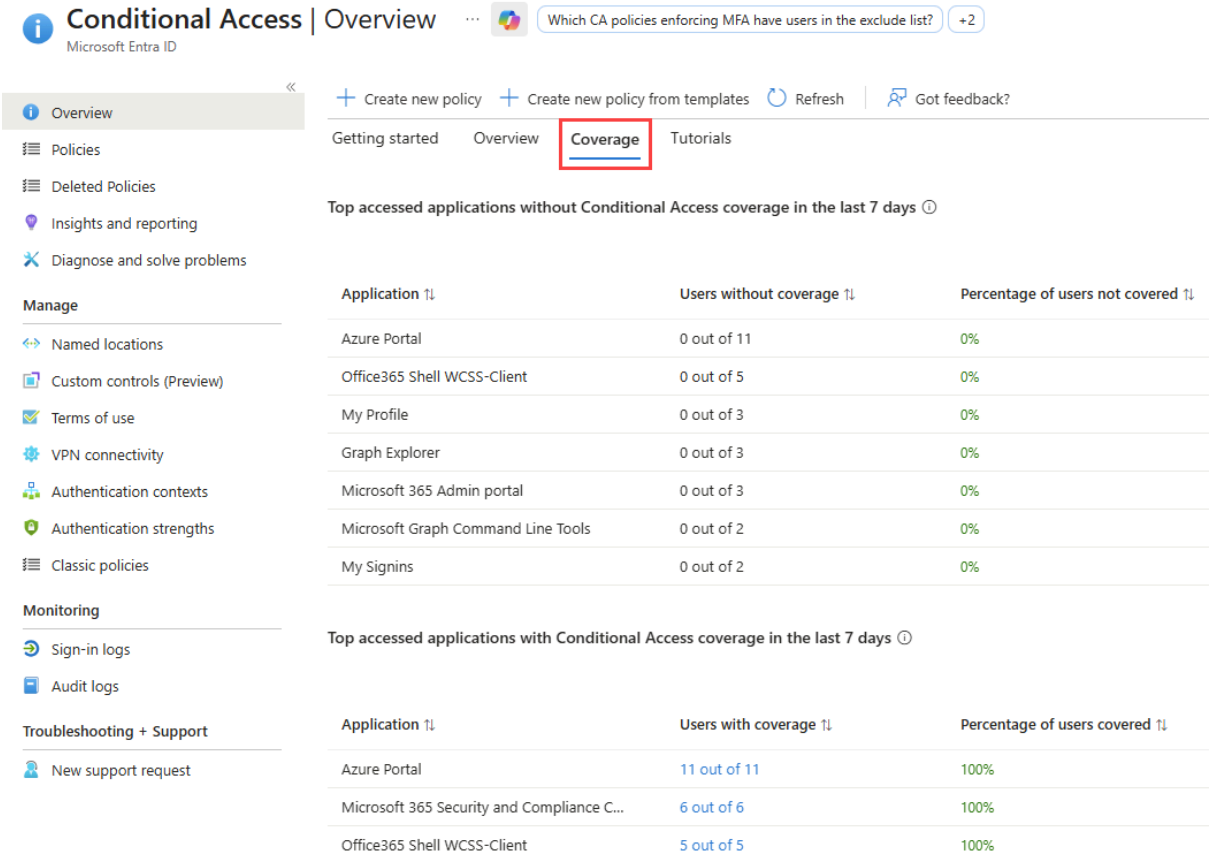
Admins with at least the Security Reader role can find Conditional Access in the Microsoft Entra admin center under **Entra ID** > **Conditional Access**.

- The **Overview** page shows a summary of recent activity that relates to Conditional Access policies. Here you can see how many policies are enabled vs report-only, agent and user activity, applications, devices,

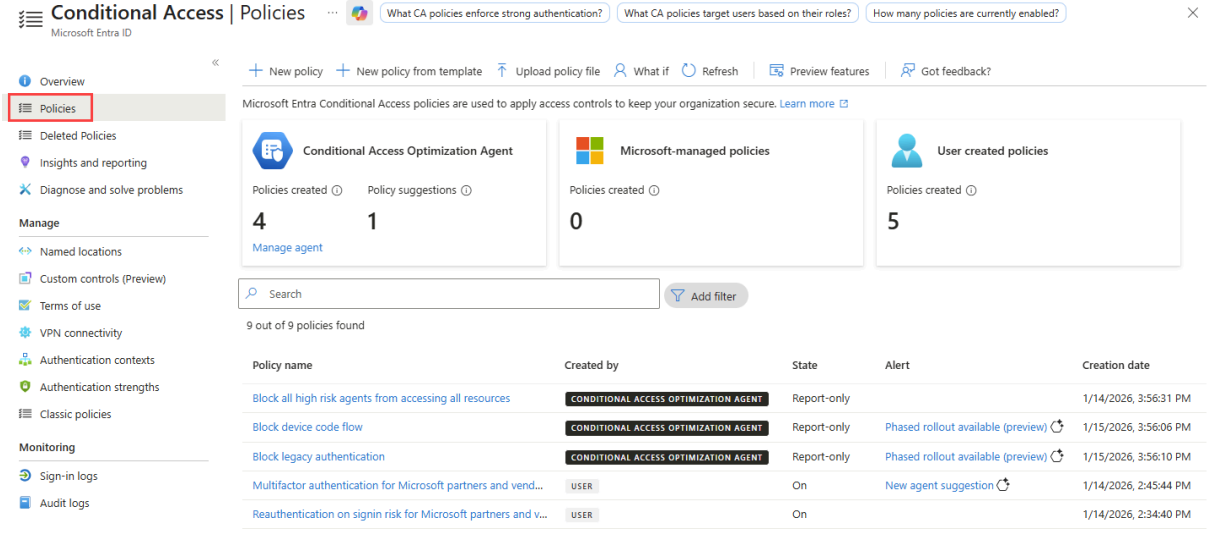
and general security alerts with suggestions.



- The **Coverage** tab shows a summary of applications with and without Conditional Access policy coverage over the past seven days.



- The **Policies** page lists all of the polices in your tenant, including report-only policies and policies created by the Conditional Access Optimization Agent (if applicable). Options to filter, view "What if" scenarios, and create new policies are available here.



Conditional Access Optimization Agent

The Conditional Access Optimization Agent with Microsoft Security Copilot suggests new policies and changes to existing ones based on Zero Trust principles and Microsoft best practices. With one click, apply the suggestion to automatically update or create a Conditional Access policy. The agent needs at least the Microsoft Entra ID P1 license and security compute units (SCU).

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 can also use Conditional Access features.

Other products and features that interact with Conditional Access policies require appropriate licensing for those products and features, including Microsoft Entra Workload ID, Microsoft Entra ID Protection, and Microsoft Purview.

When the licenses required for Conditional Access expire, policies aren't automatically disabled or deleted. This graceful state lets customers migrate away from Conditional Access policies without a sudden change in their security posture. You can view and delete remaining policies, but you can't update them.

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

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

Plan your Conditional Access deployment
