News Multifactor authentication Microsoft Entra
**8 min read**

# Automatic Conditional Access policies in Microsoft Entra streamline identity protection

By Alex Weinert, Vice President, Identity Security

**November 6, 2023**

Zero Trust

Microsoft Entra ID

Microsoft Entra ID Protection

*Extending our commitment to help customers be secure by default, today we're announcing the auto-rollout of Microsoft Entra Conditional Access policies that will automatically protect tenants based on risk signals, licensing, and usage.*

*We've designed these policies based on our deep knowledge of the current cyberthreat landscape to help our customers strengthen their security baseline, and we'll adapt them over time to keep the security bar high. These policies are part of a broader initiative to strengthen security, which includes key engineering advances.*

*This blog post explains why we decided to create these policies, how they work, how they differ from security defaults, and what Microsoft Entra customers can expect as we roll them out.*

**Microsoft Entra Conditional Access**

Increase protection without compromising productivity.

**Try for free**

Buckle up, we're going for a ride. I have a great security story to share—about multifactor authentication, seat belts, radical ideas, and the pit of success.

Ten years ago, in 2013, we had just started the identity security team and had a radical idea: We changed the policy in our Microsoft account ecosystem (the consumer identity system behind things like Outlook.com, Skype, Xbox, and OneDrive) to require multifactor authentication factors for every single account. Today, **100 percent of consumer Microsoft accounts older than 60 days have multifactor authentication—and it's been this way for 10 years.** We give accounts 60 days to meet this policy requirement, then we **block sign-ins until the user adds a strong authentication factor**.

This move caused a huge stir. Many of the teams within Microsoft that relied on consumer identity were convinced multifactor authentication would add too much friction. They feared users would hate it. Pundits predicted catastrophe, but by virtually all metrics, **the multifactor authentication requirement was a smashing success**. Because we could safely challenge suspicious sign-ins, Microsoft account hacking plummeted by more than 80 percent, and good user recovery increased from 57 percent to 81

percent when accounts *were* hacked.

Securing an email or phone number to use as a multifactor authentication factor raised costs for fraudsters enough that synthetic account creation plummeted by 99 percent. Before we enacted this policy, users who forgot their passwords recovered their accounts at a rate of only 16 percent. Under the new policy, unaided password recovery jumped to more than 90 percent. And the policy didn't drive customers away. In fact, the multifactor authentication policy had such a positive effect on integrity, security, and recoverability that **customer retention improved by more than 5 percent**. Good security ***reduces*** friction.

When Microsoft account joined forces with the team responsible for Microsoft Entra ID (formerly Azure Active Directory) late in 2014, we sought to replicate the success of this consumer-focused program. But we found the going much harder in the commercial space because we weren't in control of account policies—customers were. Not only did identity admins fear user friction the way we had, but they were also grappling with budget constraints and talent shortages, as well as security and technical backlogs (none of this has gotten easier!). If we wanted to help our enterprise customers adopt multifactor authentication, we'd need to do more.

We tried all kinds of promotional campaigns. We offered the same kind of risk-based multifactor authentication challenges we used to protect our consumer users in a commercial product, Microsoft Entra ID Protection (formerly Azure AD Identity Protection). Disappointingly, these efforts barely moved the needle. When Nitika Gupta (Principal Group Product Manager, Microsoft) and I presented monthly multifactor authentication usage rates at Microsoft Ignite in 2017, it was just 0.7 percent of monthly active users. And we calculated this metric with lenience, counting users who carry a multifactor authentication claim from any source—on-premises federation, third-party providers, or Microsoft Entra multifactor authentication.

To make progress, we needed another radical idea, so in 2018, we made **multifactor authentication available at no additional cost for all customers** at all license levels. Even trial accounts included multifactor authentication. Over the next year—now that price wasn't a barrier—multifactor authentication adoption rates only increased to 1.8 percent. At this rate, unless something changed, we wouldn't reach 100 percent adoption for another 50 years. It was time to get even more radical.

So, in 2019, we came up with "security defaults," which provides on-by-default multifactor authentication, and applied it to all new tenants. More than 80 percent of new tenants leave security defaults turned on, protecting tens of millions of users. Combining this uptick with pandemic-driven changes in work increased our multifactor authentication utilization to more than 25 percent. We were getting somewhere.

Our next move, starting in 2022, was to extend security defaults to existing tenants, often simpler, smaller customers, who haven't touched their security settings. We've approached this carefully to minimize customer disruption. We're still rolling out the program, but it has already protected tens of millions more users. More than 94 percent of existing tenants we've rolled security defaults out to have kept them enabled.

In just the past year, we've turned on security defaults for almost seven million new and existing tenants. These tenants experience 80 percent fewer compromises than tenants without security defaults. Today, security defaults drive more than half of today's multifactor authentication usage in Microsoft Entra ID, and we've driven overall multifactor authentication utilization up to just over 37 percent.

**But our goal is 100 percent multifactor authentication.** Given that formal studies show multifactor authentication reduces the risk of account takeover by over 99 percent, every user who authenticates should do so with modern strong authentication.[1] In a world where digital identity protects virtually every digital and physical assets and makes virtually all online experiences possible—and in a year when we've blocked more than 4,000 password attacks per second—we need to do more to drive multifactor authentication adoption. And so now, we're kicking off the next radical idea.

## Auto-rollout of Conditional Access policies

In the early 1960's, if you wanted seat belts in your car, you could certainly have them. You just had to go to the store, buy some webbing and a buckle, figure out where to drill holes, and install the backing plates. Unsurprisingly, virtually no one did that. After 1965, when all manufacturers were required to install seat belts in all models, traffic injuries plummeted. And now, your car owes its safety rating in part to the annoying ding-ding-ding of the dashboard should you forget to buckle up. This approach—of making a secure posture easy to get into and hard to get out of—is sometimes called the "pit of success."

Similarly, in the early days of cloud identity, if you wanted multifactor authentication for your accounts, you could certainly have it. You just had to pick a vendor, deploy the multifactor authentication service, configure it, and convince all your users to use it.

Unsurprisingly, virtually no one did that. But when we applied the "pit of success" philosophy for consumer accounts in 2013 with multifactor authentication on by default, and for enterprise accounts in 2019 with security defaults, account compromise plummeted as multifactor authentication usage went up. And we're incredibly excited about the next step in the journey: **the automatic roll-out of Microsoft-managed Conditional Access policies**.

Today, many customers use security defaults, but many others need more granular control than security defaults offer. Customers may not be in a position to disable legacy authentication for certain accounts (a requirement for security defaults), or they may need to make exceptions for certain automation cases. Conditional Access does a great job here, but often customers aren't sure where to start. They've told us they want a clear policy recommendation that's easy to deploy but still customizable to their specific needs. And that's exactly what we're providing with Microsoft-managed Conditional Access policies.

Microsoft-managed Conditional Access policies provide clear, self-deploying guidance. Customers can tune the policies (or disable them altogether), so even the largest, most sophisticated organizations can benefit from them. Over time, we'll offer policies tailored to specific organizations, but we're starting simple.

Because enabling multifactor authentication remains our top recommendation for improving your identity secure posture, our first three policies are multifactor authentication-related, as summarized in the table below:

| Policy | Who it's for | What it does |
|---|---|---|
| Require multifactor authentication for admin portals | All customers | This policy covers privileged admin roles and requires multifactor authentication when an admin signs into a Microsoft admin portal. |
| Require multifactor authentication for per-user multifactor authentication users | Existing per-user multifactor authentication customers | This policy applies to users with per-user multifactor authentication and requires multifactor authentication for all cloud apps. It helps organizations transition to Conditional Access. |
| Require multifactor authentication for high-risk sign-ins | Microsoft Entra ID Premium Plan 2 customers | This policy covers all users and requires multifactor authentication and reauthentication during high-risk sign-ins. |

Pay lots of attention to the first policy. It's our strong recommendation—and a policy we'll deploy your behalf—that **multifactor authentication protect all user access to admin portals** such as https://portal.azure.com, Microsoft 365 admin center, and Exchange admin center. Please note that while you can opt out of these policies, teams at Microsoft will increasingly require multifactor authentication for specific interactions, as they already do for certain Azure subscription management scenarios, Partner Center, and Microsoft Intune device enrollment.

You can view the policies and their impact using the new policy view user experience, which includes a policy summary, alerts, recommended actions, and a policy impact summary. You can also monitor them using sign-in and audit logs. You can customize the policies by excluding users, groups, or roles that you want to be exceptions, such as emergency and break glass accounts. If you require more extensive customizations, you can clone a policy and then make as many changes as you want.

We'll begin a gradual rollout of these policies to all eligible tenants starting next week. We'll notify you in advance, of course. Once the policies are visible in your tenant, you'll have 90 days to review and customize (or disable) them before we turn them on. For those 90 days, the policies will be in report-only mode, which means Conditional Access will log the policy results without enforcing them.

## The Conditional Access policies you need, based on the latest cyberthreat information

As with security defaults, we've carefully considered the managed policies we're rolling out automatically. We want the experience to feel like consulting directly with Microsoft's identity security team, as though we examined your environment and said, based on everything we've learned from securing thousands of customers, "These are the policies you need."

What's more, we'll keep improving the policies over time. Our eventual goal is to combine machine learning-based policy insights and recommendations with automated policy rollout to strengthen your security posture on your behalf with the right controls. In other words, as the cyberthreat landscape evolves, we'd not only recommend policy changes based on the trillions of signals we process every day, but we'd also safely apply them for you ahead of bad actors.

Not only will the seat belts already be in your car, but we'll also help you fasten them to keep everyone safer. That way, you can keep your eyes on the road ahead.

## Learn more

Learn more about Microsoft Entra Conditional Access.

The auto-rollout of Conditional Access policies is just one initiative we're taking to strengthen your security. Learn about engineering advances we're making in a recent memo to all Microsoft engineers from Charlie Bell, Executive Vice President, Microsoft Security.

To learn more about Microsoft Security solutions, visit our website. Bookmark the Security blog to keep up with our expert coverage on security matters. Also, follow us on LinkedIn (Microsoft Security) and X (formerly known as "Twitter") (@MSFTSecurity) for the latest news and updates on cybersecurity.

---

*All statistics listed throughout this blog are based on Microsoft internal data.*

[1] How effective is multifactor authentication at deterring cyberattacks? Microsoft.


## Get started with Microsoft Security

Microsoft is a leader in cybersecurity, and we embrace our responsibility to make the world a safer place.

**Learn more**

Connect with us on social

**What's new**

Surface Laptop Studio 2

Surface Laptop Go 3

Surface Pro 9

Surface Laptop 5

Microsoft Copilot

Copilot in Windows

Explore Microsoft products

Windows 11 apps

**Microsoft Store**

Account profile

Download Center

Microsoft Store support

Returns

Order tracking

Certified Refurbished

Microsoft Store Promise

Flexible Payments

## Education

Microsoft in education

Devices for education

Microsoft Teams for Education

Microsoft 365 Education

How to buy for your school

Educator training and development

Deals for students and parents

Azure for students

## Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power Platform

Microsoft Teams

Copilot for Microsoft 365

Small Business

## Developer & IT

Azure

Developer Center

Documentation

Microsoft Learn

Microsoft Tech Community

Azure Marketplace

AppSource

Visual Studio

## Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Sustainability

English (United States)

Your Privacy Choices

Consumer Health Privacy

Sitemap Contact Microsoft Privacy Terms of use Trademarks Safety & eco Recycling About our ads © Microsoft 2024