

Falcon Shield: Building Controls into MFA Registration

Prevent threat actors from exploiting conditional access policies by registering their own MFA methods on compromised accounts

Multifactor authentication (MFA) is a strongly recommended security mechanism that secures accounts even after a user's credentials have been compromised. However, when users are able to register their own MFA methods without restriction because they have triggered conditional access (CA) policies, companies may be inadvertently increasing their level of risk.



The challenge

1. A corporation introduces a CA policy requiring MFA from users who access an application from an untrusted location. However, they do not require MFA for all access.
2. A threat actor compromises the corporation's Microsoft 365 account. This account doesn't have a registered MFA method, and if the user is accessing the account from an untrusted location, the CA policy is triggered, allowing — in fact, requiring — the threat actor to register their own MFA method.
3. The threat actor then registers their own MFA method.



The impact

1. With a registered MFA method in hand, the threat actor can easily move between services.
2. When sessions expire, threat actors can repeatedly log in using their MFA method.
3. Threat actors can reset passwords, escalating their access and compromising the account. If this is an admin account, the impact can be far-reaching.



General prevention

- Only allow MFA registrations from trusted locations or from a domain-joined device.
- Register MFA methods during account provisioning.
- Require MFA even on trusted sites so that all accounts have an MFA method associated with them.

Scenarios

Application CA forces threat actor to get MFA

A threat actor gained credentials to a software as a service (SaaS) app through a password spray attack but lacked the MFA needed to access the app. The threat actor used the same credentials to access a second app, whose CA compelled the threat actor to register their own MFA method. Once registered, the attacker went back to the original application, logged in using the stolen credentials and MFA, and was granted access.

Untrusted location CA allows attacker to register MFA

An adversary logging in to an application using stolen credentials from an unusual IP address triggered a CA requiring MFA. The targeted account lacked MFA, so the attacker was prompted to register their own MFA method. Once registered, the attacker was able to move laterally through the target's organization.

Azure CA requires MFA on high-risk sign-in

When Azure noted a risky sign-in, the CA triggered an MFA request. However, since the account didn't have a registered MFA method, it prompted the threat actor to register their own MFA method.

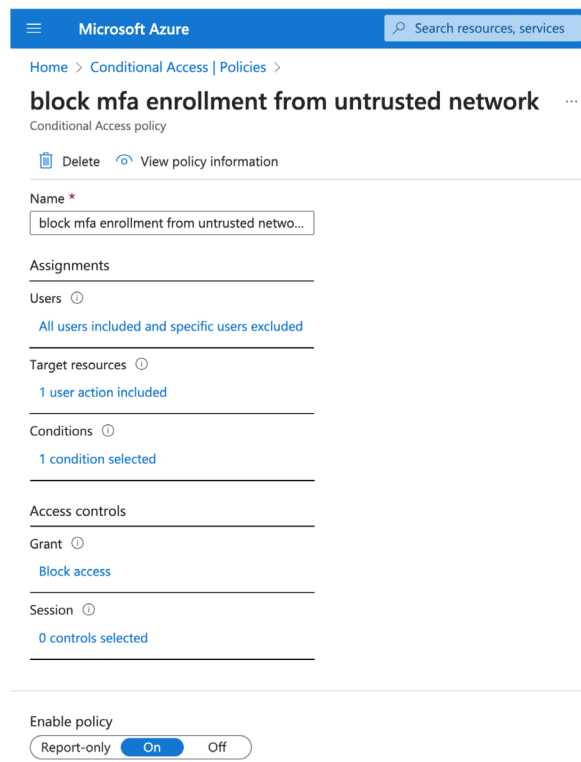
Default setting for My Sign-Ins triggers MFA enrollment

By default, Microsoft My Sign-Ins always prompts for MFA. When there is no registered MFA method, the application prompts the user to register their own method. Once the registered MFA method is in place, a threat actor can use it to access other Microsoft 365 applications.

Mitigation for Microsoft Entra ID (formerly Microsoft Azure Active Directory)

To strengthen MFA security, configure settings to only permit MFA registration during active authenticated sessions while validating the user's identity throughout the enrollment process. Additionally, establish and maintain a list of approved IP ranges from which security information modifications are allowed, blocking any attempts to alter security settings from unauthorized IP addresses.

1. Sign in to the Microsoft Entra ID admin center as at least a Conditional Access Administrator, and then go to Conditional Access → New policy
2. Go to the "Block MFA enrollment from untrusted network" configuration
3. Enter a name for the policy
4. Under Users, select All Users
5. Under Target Resources, select User actions → Register security information
6. Under Conditions, select Locations → Exclude "All trusted locations"
7. Under Grant, select Block access
8. Go to Enable policy and select On

[Learn more](#)

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: <https://www.crowdstrike.com/>

Start a free trial today: <https://www.crowdstrike.com/free-trial-guide/>

