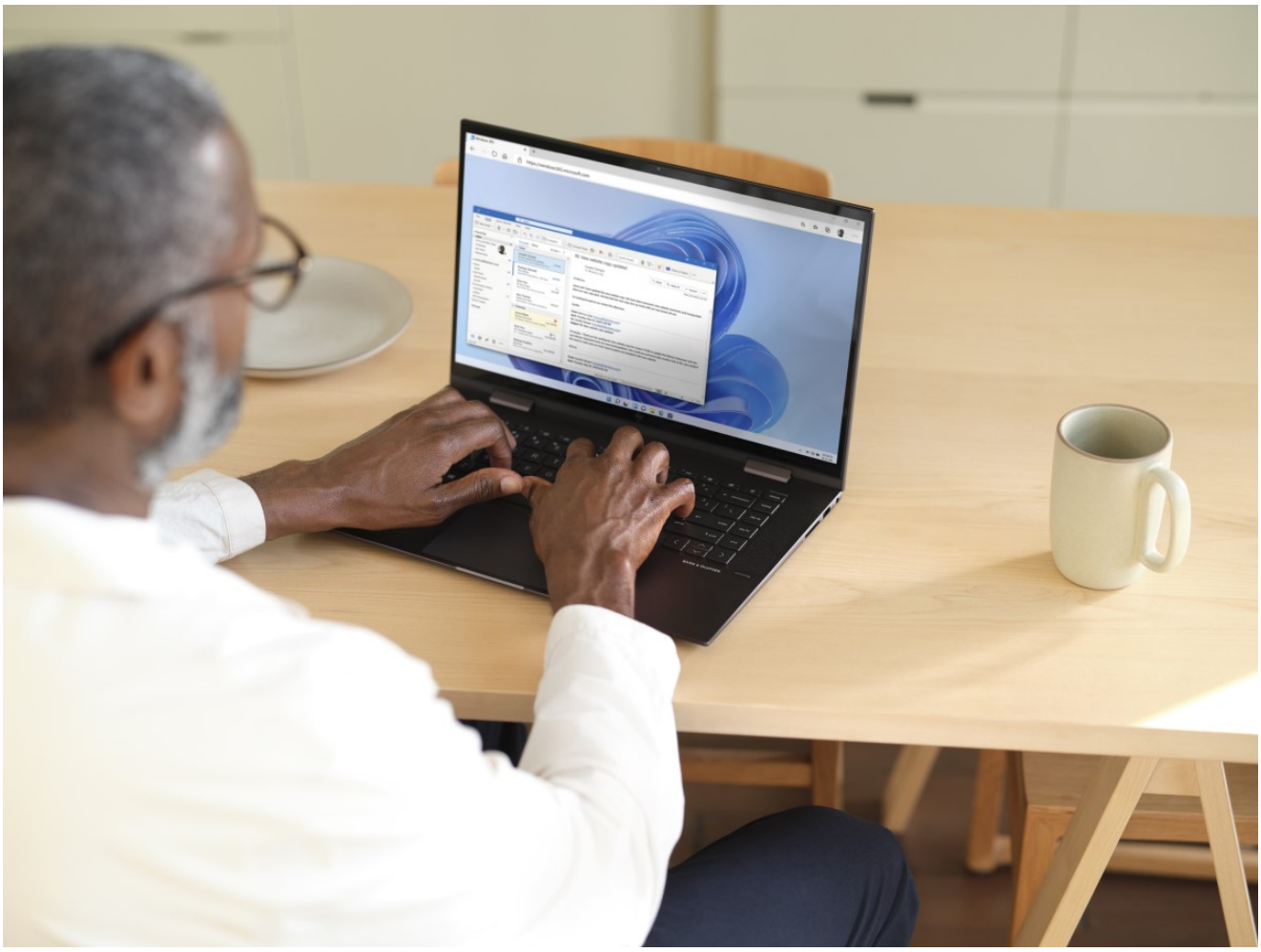
Protect your business from password sprays with Microsoft DART recommendations

microsoft.com/security/blog/2021/10/26/protect-your-business-from-password-sprays-with-microsoft-dart-recommendations/

October 26, 2021



Over the past year, the Microsoft Detection and Response Team (DART), along with Microsoft's threat intelligence teams, have observed an uptick in the use of password sprays as an attack vector. This threat is a moving target with techniques and tools always changing, and Microsoft continues to find new ways to detect these types of attacks and help protect its customers.

In this blog, we are going to define what password sprays are, detail DART's investigation techniques and approach to responding to password spray attacks, and outline our recommendations for protecting against them.

Why are identity-based attacks suddenly so popular?

Previously, threat actors focused on attacking computers to gain access into an environment. As software becomes more intelligent at detecting abnormal programs and vulnerabilities, attacks against our customers are rapidly becoming more focused on breaking into identities rather than breaking into a network.

The approach to securing user accounts is well-intentioned, but it is often incomplete, with a large investment that typically goes into areas such as complex password policies and limiting access to resources from networks perceived as secure. While these mitigations are necessary best practices, in the case of a compromised trusted user, they are ineffective at preventing unauthorized access.

This is why identity attacks have become so popular. Once attackers have gained the credentials to an account, they can access any sensitive resources that users can access and have the malicious activity appear as normal. This creates a repeating cycle attack pattern, where one compromised account can lead to access to resources where additional credentials can be harvested, and thus even further resource access.

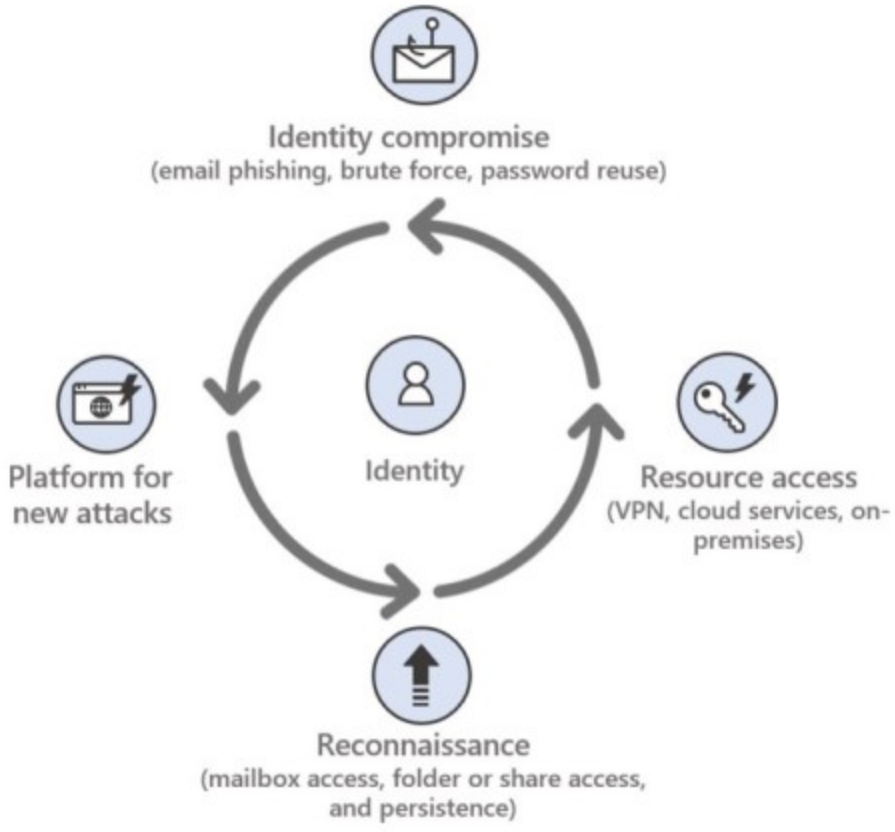


Figure 1. Identity-based attack lifecycle.

The anatomy of a password spray attack

To understand how to protect against, and investigate a password spray attack, it is important to understand what it is. Password spray attacks are authentication attacks that employ a large list of usernames and pair them with common passwords in an attempt to "guess" the correct combination for as many users as possible. These are different from brute-force attacks, which involve attackers using a custom dictionary or wordlist and attempting to attack a small number of user accounts.

Sophisticated password spray techniques include some of the following qualities:

Password spray methods:

- **Low and slow:** Patience is key for a determined threat actor. The most sophisticated password sprays will use several individual IP addresses to attack multiple accounts at the same time with a limited number of curated password guesses.
- **Availability and reuse:** With a new breach being announced publicly every month, the amount of compromised credentials posted on the dark web is rising rapidly. Attackers can utilize this tactic, also called "credential stuffing," to easily gain entry because it relies on people reusing passwords and usernames across sites.

Password spray identifiers:

- **User agents:** This is not an immutable variable and is simple to spoof, so don't always rely on the user agent string to tell the truth. That said, some example user agents often seen during a password spray are:
  - BAV2ROPC / CBAinPROD / CBAinTAR: These user agent strings represent a connection from a client that uses legacy authentication, a popular tool for a password spray attack.
  - Firefox/Chrome: More sophisticated password sprays using REST APIs often use headless browsers [a browser that doesn't have a graphical user interface (GUI)] to target the API endpoints.
  - Python requests package: This is an automation library that can be used to generate requests to a website without user interaction.
- **Targets:** Password sprays have often targeted applications that are unsecured and use legacy authentication protocols. This is due to the fact that these protocols don't offer a rich audit trail and are not able to enforce a multifactor authentication (MFA) requirement. More recently, things have changed somewhat, and we are seeing attackers switch to targeting applications that utilize the REST API, often considered to be more secure. Some commonly targeted applications are:
  - Exchange ActiveSync
  - IMAP, POP3, SMTP Auth
  - Exchange Autodiscover

Microsoft has implemented new and improved password spray detections over the last year to help continue to address password spray attacks.

Help! I've been sprayed!

DART is no stranger to password spray attacks. When it comes to investigating cybersecurity incidents, our team's primary goal is to establish the facts and see where they lead us. Here are some of the questions our team typically considers at the start of each password spray attack incident:

- **"Was the password spray successful?"** This is perhaps the most important question to ask because it determines whether there is potential unauthorized access present in the environment. If it was determined to be successful, the investigator can continue down the list to gain additional information to understand how to proceed.
- **"Which users are affected?"** Enumerating the users that were victims of the password spray attack can change the direction of our investigation. For example, if the list of users affected is particularly targeted (maybe just in one department or all the staff members of a particular project), we can assume our threat actor knows what they are looking for and has done their research. This helps us adapt an action plan based on the permissions and access rights that a particular user has. We call this "scoping" the incident—in other words, understanding what machines and resources the attackers accessed, and determining the number of compromised users. This knowledge helps us with remediation and preventing attackers from entering the environment again in the future.
- **"Were administrative accounts compromised?"** If administrative control over a tenant is lost, the situation changes. A compromised tenant is a very different situation from a compromised user and has the potential to be much more damaging, so this is an important distinction for us to make.
- **"What indicators do we have?"** Information such as the time the spray was conducted, targeted user agent and endpoint, IP addresses, and other identifying information can help us understand if this was carried out by an opportunistic attacker or determined human adversary. There is also the possibility that we can use our threat intelligence to identify some potential next steps our adversary may have taken and the overall scope of compromise.

Our password spray investigations playbook contains in-depth guidance around investigating password spray attacks and offers information about Microsoft Active Directory Federation Services (ADFS), Microsoft's solution for single sign-on (SSO), and web-based authentication.

Am I a target?

It's important to understand the targets of the password spray to correctly determine the scope of the potential compromise. Recently, DART has seen an uptick in cloud administrator accounts being targeted in password spray attacks, so understanding the

targets is a good place to start. Enumerate the users with the below permissions as the initial list to investigate, and then add users to it as the analysis proceeds:

- Security administrator
- Exchange service administrator
- Global administrator
- Conditional Access administrator
- SharePoint administrator
- Helpdesk administrator
- Billing administrator
- User administrator
- Authentication administrator
- Company administrator

In addition to privileged accounts such as these, identities with a high profile (such as C-level executives), or identities with access to sensitive data are also popular targets. It is easy to make exceptions to policy for staff who are in executive positions, but in reality, these are the most targeted accounts. Be sure to apply protection in a democratic way to avoid creating weak spots in configuration.

How can I check for suspicious activity?

To perform a thorough cloud investigation, exportation of logs and installation of PowerShell modules is inevitable and discussed in detail in our password spray investigation playbook, but there are other methods to gain insights quickly.

Microsoft Cloud App Security

The Microsoft Cloud App Security portal is a great first place to check for suspicious activity. If you have Cloud App Security enabled, follow these steps to check for suspicious activity.

1. Go to the Cloud App Security portal and sign in with the Security Administrator credentials.
2. Go to **Alerts**.
3. Filter for the users that you enumerated in the first step, check for any alerts associated with these users.

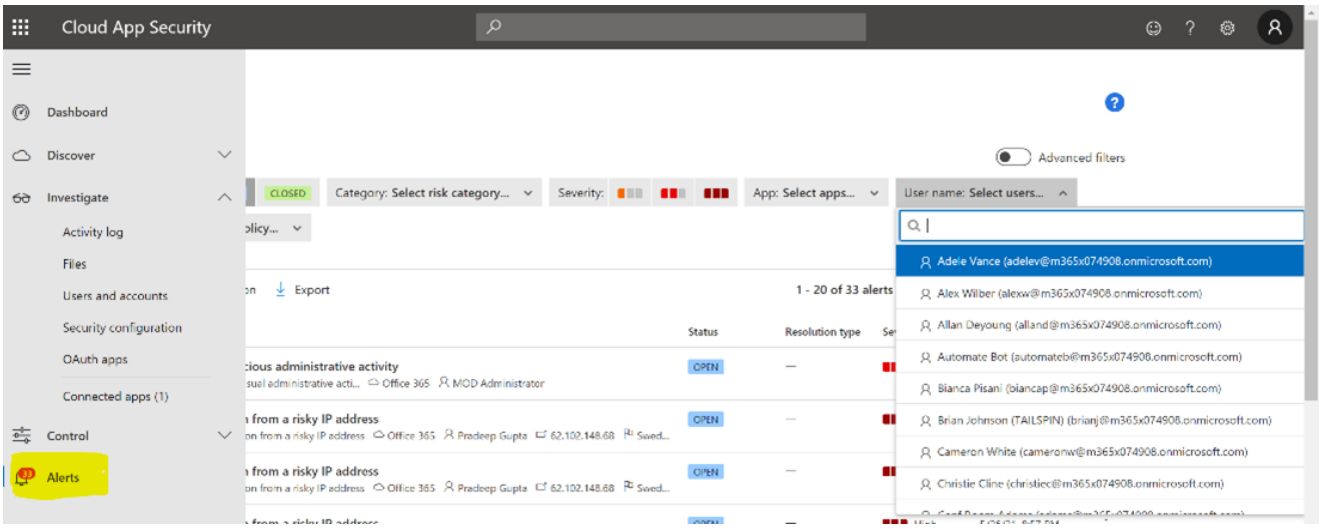


Figure 2. Sample alerts in Cloud App Security related to possible password spray attacks.

Here are some alerts that could be associated with a password spray incident:

- Activity from anonymous IP address.
- Activity from infrequent country.
- Activity from suspicious IP address.
- Impossible travel.

We describe additional Cloud App Security alerts in our documentation.

User investigation priority

For the accounts of interest, check the Cloud App Security investigation priority by navigating to the account under **Users and accounts**. The investigation priority score is based on security alerts, abnormal activities, and potential business and asset impact related to each user to help you assess how urgent it is to investigate each specific user.

1. Go to the Cloud App Security portal.
2. Go to **Investigate** then **Users and accounts**.
3. Check the investigation priority for all users of interest and, if needed, view related activity.

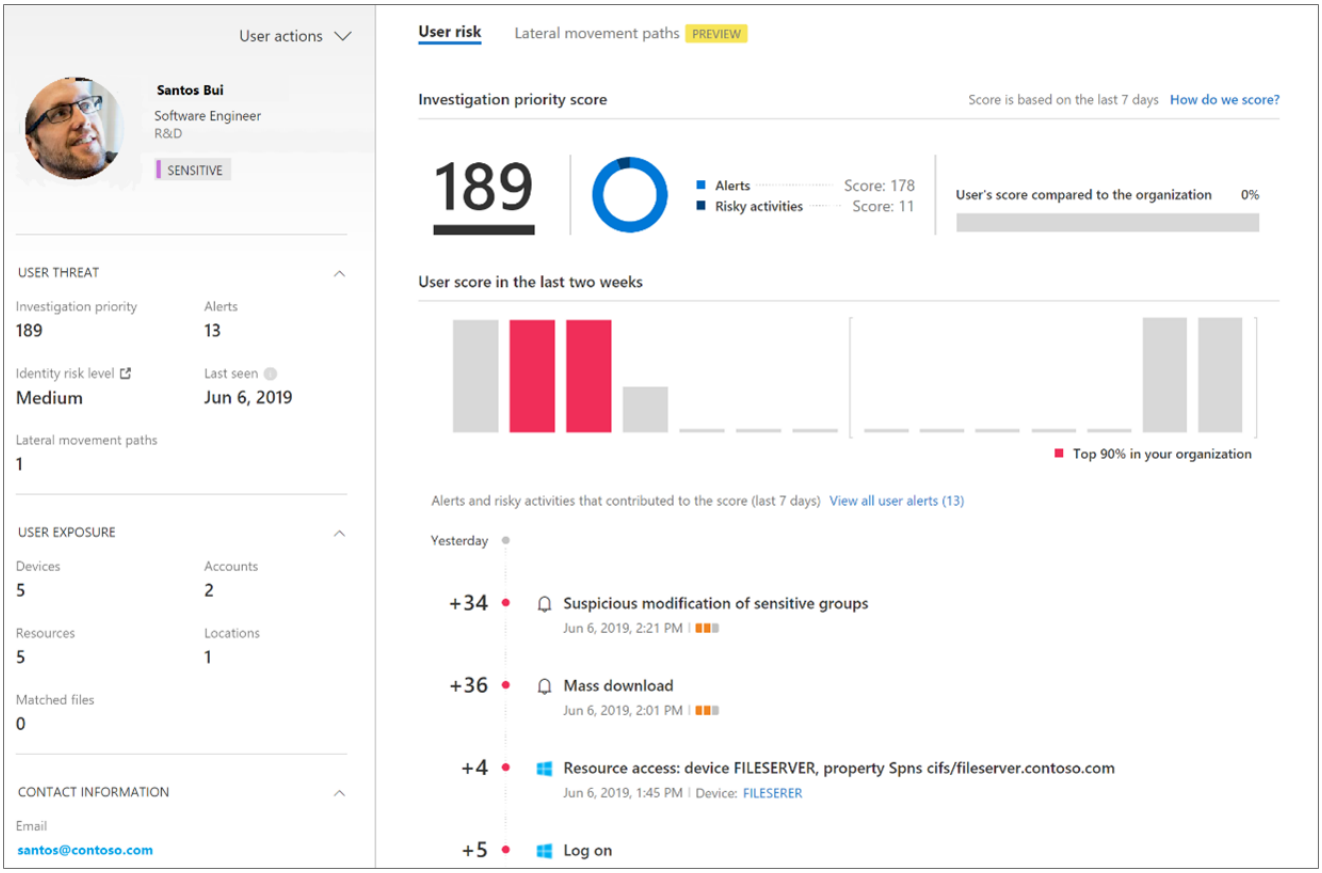


Figure 3. The user page in Cloud App Security shows the investigation priority.

Azure Active Directory

Microsoft Azure Active Directory (Azure AD) incorporates behavioral analysis algorithms into its detection logic natively, so there is a chance that an alert already exists about a password spray attack. Below are several places to check within the portals before going through the hassle of log exporting. Use the indicators of compromise (IOCs) from these alerts to further pivot such as user, IP address, time range, and more.

Identity Protection

Identity Protection is a tool in Azure AD designed to identify potential risky behavior surrounding authentication events. Users with an Azure AD Premium P2 license may follow these steps to check for suspicious activity:

1. Go to the Microsoft Azure portal.
2. Use the search bar to locate **Azure AD**.
3. Select **Security** from the left blade.
4. Review the reports under **Risky sign-ins** and **Risky users** for any of the users that you enumerated from the list.

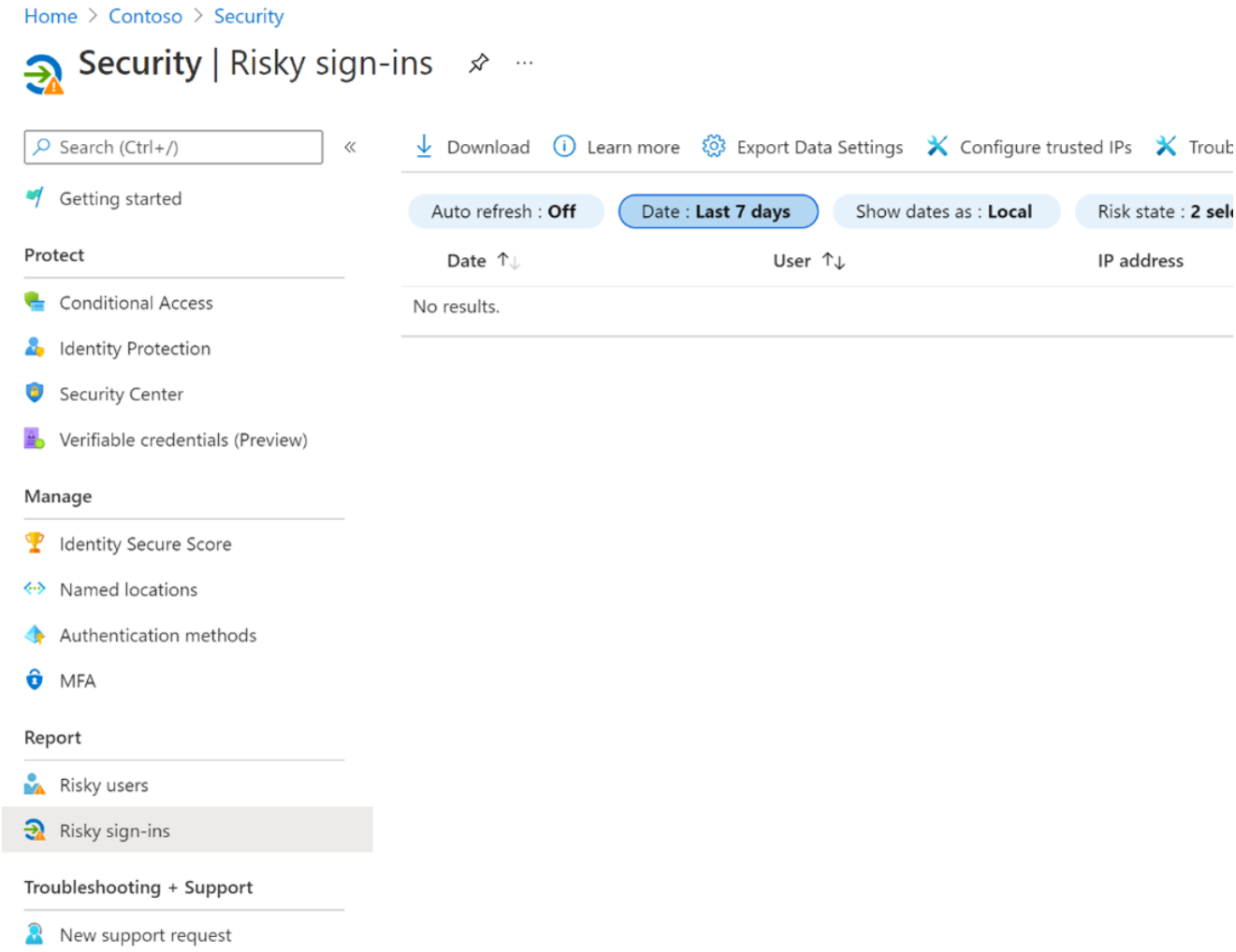


Figure 4. Azure AD can display a list of risky sign-ins to identify potential risky behavior.

Revoke user access

If an identity is considered compromised, action should be taken immediately to ensure that access is revoked. This should include disabling the user's device(s), a password reset, account disablement, and token revocation in Azure AD.

Recommendations for protecting against password sprays

Password sprays are worrisome but when we look at the statistics according to the Digital Shadows report "From Exposure to Takeover," there are over five billion unique credential pairs available for sale worldwide, with new caches of credentials being exposed on a regular basis.[1] This kind of volume tells us that we should assume that a breach will occur and consider that a compromised username or password in any given organization is inevitable.

This doesn't mean we should give up on passwords altogether, but the rabbit hole of password policies, and the potentially endless discussions about complexity, length, and "correct battery horse staple" (Don't know what we are talking about? Look it up!) should be avoided in favor of applying Zero Trust logic to identity and authentication. This includes areas like:

- **MFA and legacy authentication:** You have probably heard this recommendation before: disabling legacy authentication and enabling MFA for all users is a critical step in securing your identity infrastructure and should be a priority if it has not already been done.
- **Rethinking the password policy:** The future is a world without passwords because it is too common that people reuse them between applications or create easily discoverable passwords. Passwordless authentication methods such as the Microsoft Authenticator App, Windows Hello for Business, and Fast Identity Online (FIDO) keys help improve both the user experience and security level of an authentication event. If a password must be used, ensure that the password policy does not allow key phrases related to the organization or commonly used passwords. Having a password policy of eight characters with an uppercase, lowercase, number, and symbol, is no longer secure with today's graphics processing unit (GPU) capabilities. Attackers can crack a password with these elements in a matter of hours. 20-character small sentences may be easy for users to remember and are more secure than a complex 8-character password!
- **MFA registration:** The most effective way to protect against a password spray leading to a successful authentication is by using MFA. However, if the user is enabled for MFA, but never completes the registration process, they are left unprotected. Even worse, if a threat actor signs in and is prompted for MFA, they can register their own MFA details. This is an excellent cover for a threat actor because the authentication event is much less suspicious when MFA is satisfied. DART doesn't recommend using location-based MFA policies (like only applying MFA when outside the corporate network) as this leaves room for this kind of loophole. Additionally, DART recommends that customers configure an MFA registration policy if possible to ensure that all enabled users register for MFA.
- **Mailbox auditing:** Use this script to ensure that the recommended mailbox auditing actions are configured on every mailbox in the organization. This ensures that post-exploitation auditing is as robust as possible, allowing for a more effective investigation.
- **Administrative accounts:** These are the keys to the kingdom and should have an extra level of protection. Ensure that administrative accounts are cloud-only and are not synchronized from Activity Directory. MFA should always be applied, and emergency access accounts should be created also.

- **Policy gaps:** Ensuring that weaknesses do not exist in your identity policies and processes is critical. All too often, DART finds that small misconfigurations can lead to an entry point for a threat actor. Let's explore this idea further:
    - **Conditional Access policies:** These policies are a great way to apply access control logic to complex environments, helping customers walk the tightrope between protecting the organization and allowing staff to get on with their jobs. With complexity comes risk, and as previously mentioned, misconfigurations are all too common. Some pitfalls to watch out for:
        - **Cloud Apps:** Let's look at a real-world example. A DART customer experienced a cloud identity breach and had in place an MFA policy for administrative accounts, applied to the Office 365 cloud app. However, the threat actor used the Azure Service Management API to connect to the environment. This cloud app was outside of the scope of the MFA Conditional Access policy, giving the threat actor access to the environment without requiring MFA. Make sure to have in place a Conditional Access policy that covers all cloud apps and applies MFA to give you a base level of protection.

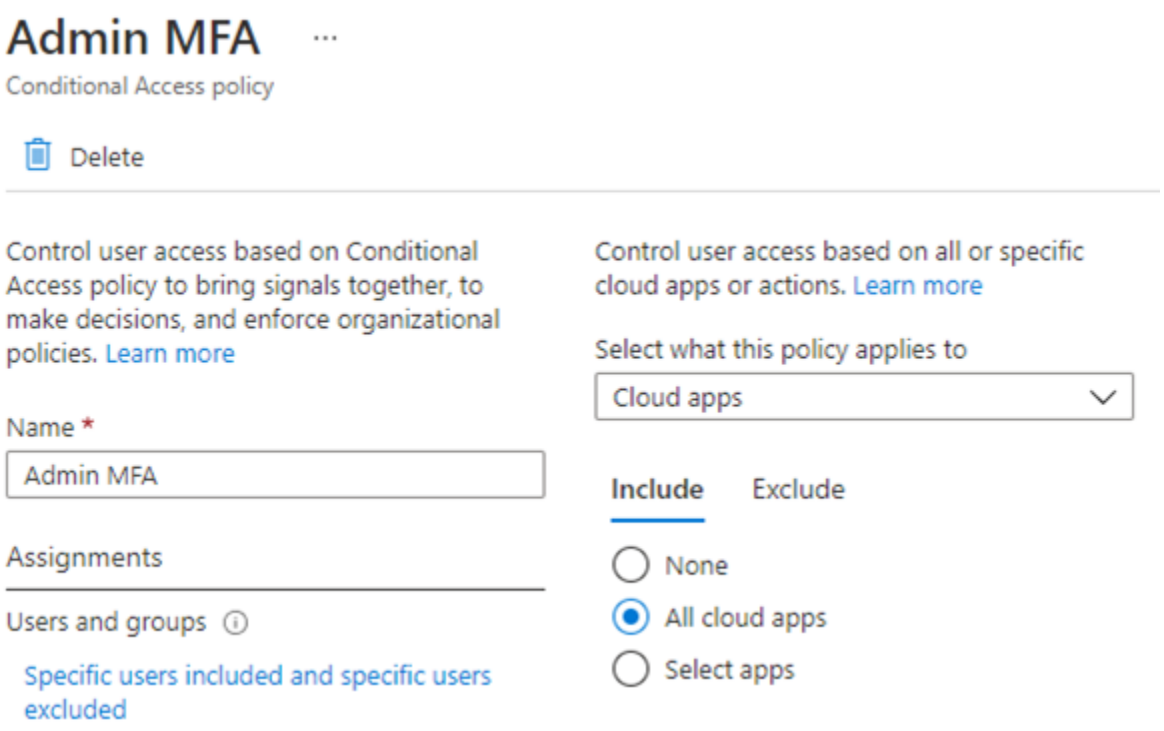


Figure 5. Conditional Access policy in Azure AD.

Policy exceptions: During day-to-day operations, changes are often made to a product configuration to facilitate business functions. One typical example of this kind of change is an account being removed or exempted from a security policy. This is something to be careful of—policy exceptions often begin as a temporary change but end up being permanent for one reason or another. It is also not uncommon for DART to observe exceptions for sensitive or high-profile accounts; the very type of account that makes an ideal target for cybercriminals. Use processes and technical solutions to ensure those policy exceptions are temporary and tracked. If they must remain, put in place some mitigating controls to reduce the attack surface of that particular account.

Assume breach

Password spray attacks are the perfect combination of low effort and high value for attackers, and even the most secure companies are likely to fall victim to them. However, preventing catastrophic damage is not a hopeless endeavor. By assessing both sides of the situation, the protection against the attack as well as the capabilities to investigate and remediate an attack, you can ensure a substantial amount of coverage against password spray destruction.

DART utilizes these strategies for everyday investigations. We encourage our customers to adopt passwordless technology and enable MFA, regardless of the provider. While attackers are most likely continuously exploring new ways to break into an environment, by assuming breach, we can help to safeguard against inevitable detrimental harm.

Learn more

Want to learn more about DART? Read our past blog posts.

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 at @MSFTSecurity for the latest news and updates on cybersecurity.

---

[1]From Exposure to Takeover: The 15 billion stolen credentials allowing account takeover, Digital Shadows Photon Research Team, Digital Shadows.