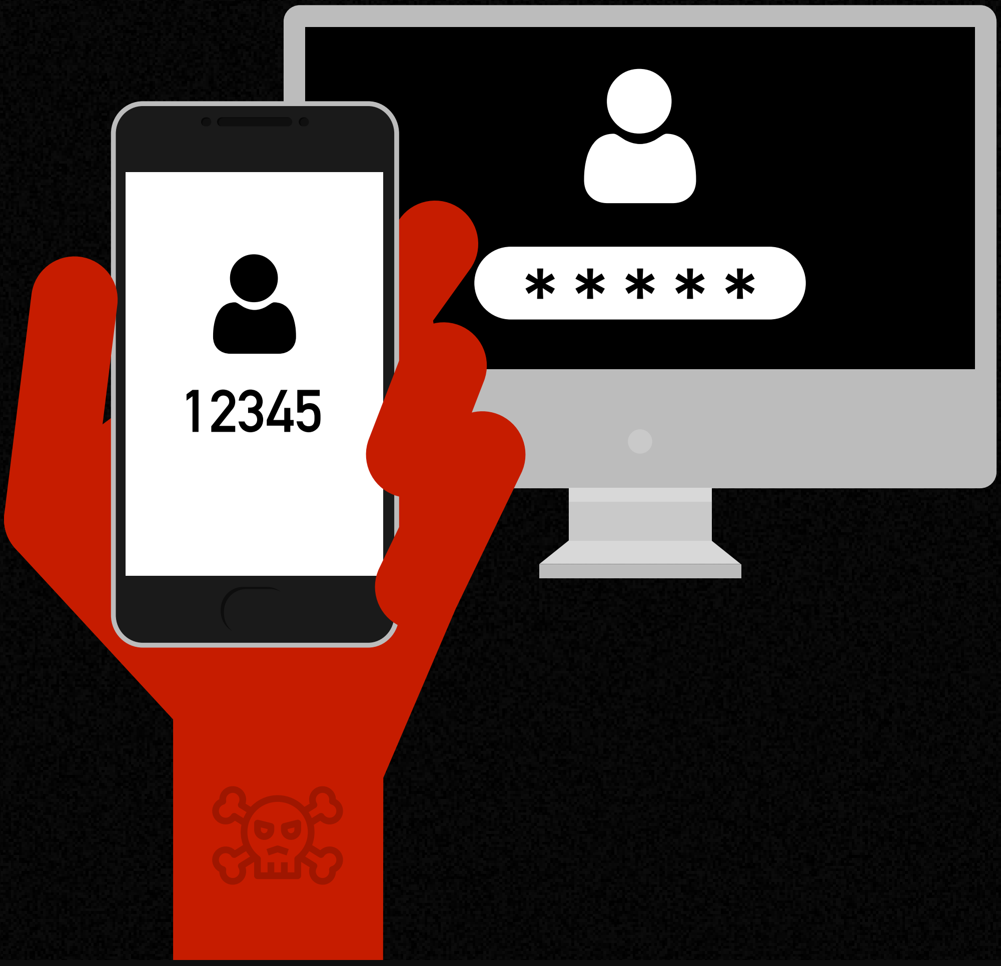
ManageEngine
ADSelfService Plus

FBI-recommended **mitigation strategies** to prevent MFA Hacks.



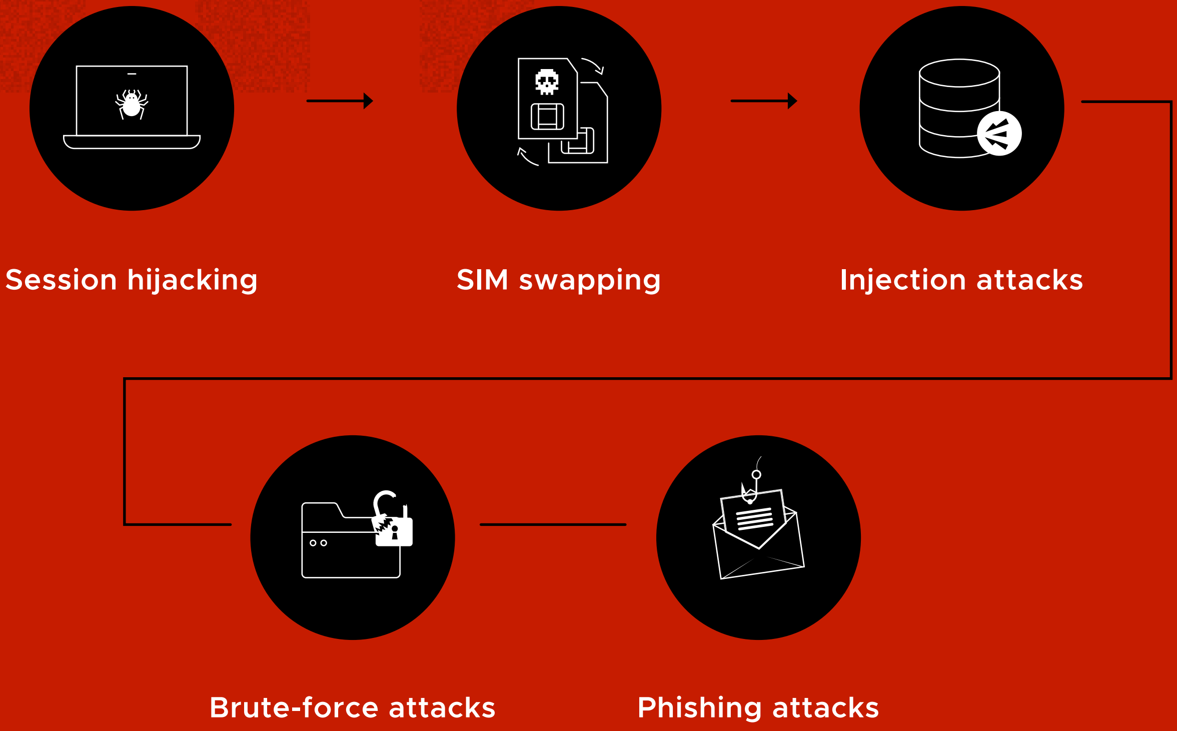
www.adselfserviceplus.com

Five ways to hack MFA and the FBI's mitigation strategy

As multi-factor authentication (MFA) has proven to be essential against credentials-based cyberattacks, many organizations are adopting MFA to secure access to their IT environments. So it comes as no surprise that attackers, looking to expose organizational data, have devised techniques to hack and circumvent MFA.

These techniques may use technical manipulation, social engineering tactics, or a mix of both. While this proves that MFA is not impenetrable, there are ways to prevent such attacks. This e-book provides an overview of the top five MFA hacking methods and details the mitigation techniques recommended by the Federal Bureau of Investigation (FBI).

Top 5 techniques attackers use to circumvent MFA



Session hijacking

SIM swapping

Injection attacks

Brute-force attacks

Phishing attacks

Session hijacking

In session hijacking, an attacker hijacks or intrudes on a client's session in a web application or browser by gaining knowledge of the session ID. The ID can be stolen by using technical loopholes or making the user click on a malicious link. Once the session ID is appropriated, the attacker can use it by tricking the web application or browser's server into believing that it is a valid client session.

The attacker assumes the identity of the hacked user for the entire client session and can perform activities that a valid user can perform in the application. If the session ID belongs to a user with administrative privileges, they can cause more damage.

SIM swapping

Cell phone service providers offer services that automatically swap an existing mobile number to a different SIM. Generally, this service is used when a customer misplaces their mobile device or moves to a new cell phone service provider. Attackers exploit this service by approaching the service providers as a legitimate customer seeking to transfer their phone number and other SIM information to another SIM card.

Once the phone number is successfully transferred, attackers can receive SMS messages, including those containing MFA verification codes. With limited information like a user's email address, application credentials, and phone number, an attacker can, using SIM swapping, complete MFA and gain access to the user's account.

Injection attacks

In injection attacks, attackers enter malicious codes or URLs in the fields provided by the web programmer. This information may be interpreted as part of a command, and the execution path of the application is altered.

In 2019, the MFA mechanism of a banking institution's website was circumvented by an attacker entering a malicious URL in the security answer field. This URL caused the computer from which the URL was entered to be assumed as trusted and allowed the attacker to misappropriate funds from multiple back accounts.

Brute-force attacks

This form of attack involves trying out different combinations of verification codes until the correct one is chanced upon. Many MFA methods involve entering verification codes or PINs.

With credential attacks becoming more sophisticated by the day, it has become easier for hackers to crack the users' account credentials and brute-force MFA PIN or verification codes. While most MFA solutions limit the number of incorrect authentication attempts via account lockouts, some MFA solutions may not include this defense mechanism.

Phishing

Phishing entails using fake websites to manipulate users into willingly offering up information or data, such as usernames, passwords, and answers to security questions. In this method, a user can be sent a seemingly legitimate email from the application they hold an account in. A malicious URL in the e-mail can take the user to a fake website. This fake website is often indistinguishable from the original website.

The user is then asked to log in with their credentials and provide information like the answers to their security questions. The attacker can then use this information to log in to the user's account, complete MFA using the information provided by the user, and then misappropriate the data stored in the application.

Mitigation strategies proposed by the FBI

It's important to note that MFA's vulnerability to attacks and circumvention attempts cannot take away the advantages it offers in terms of data security. Organizations must configure MFA to protect their resources and, additionally, implement measures to avert MFA hacks. The FBI, in its cyber crime bulletin dated September 17, 2019, detailed MFA hack incidents and also proposed the following strategies to prevent them:

> “
>
> *Educate users and administrators to identify social engineering trickery—how to recognize fake websites, not click on rogue links in e-mail, or block those links entirely— and teach them how to handle common social engineering tactics.*

Research says that 98 percent of cyberattacks are perpetrated using social engineering. By applying the principle of "prevention is better than cure," creating user awareness is the first and most important step in the path to prevent MFA hack attempts that use social engineering.

The best way a user can avoid phishing attacks is by thinking twice before they click on fraudulent links. Regular security awareness training can help admins and users identify and report phishing attempts. Conducting tests to quiz users' knowledge on social engineering tactics helps keep an organization's endpoints safe from hacks. Admins can also implement other measures like:

- Deploying firewalls and antivirus solutions.
- Installing an anti-phishing toolbar.
- Keeping the organization's browsers updated.

> “
>
> *Consider using additional or more complex forms of multi-factor authentication for users and administrators such as biometrics or behavioral authentication methods, though this may add inconvenience to these users.*

Biometrics are considered one of the strongest methods of authentication since they authenticate based on physical characteristics like fingerprints that are unique to each user. Coupling biometrics-based authentication with other authentication measures or making biometrics-based authentication mandatory are ways to upgrade the defense.

Risk-based authentication or behavioral authentication is another method to prevent circumvention of MFA. Here, the type and number of authentication methods are dynamically changed based on risk factors like time of access, IP address used to access, and more. Risk-based authentication is an automatic process in which the context of the user access is analyzed and an appropriate MFA policy is applied.

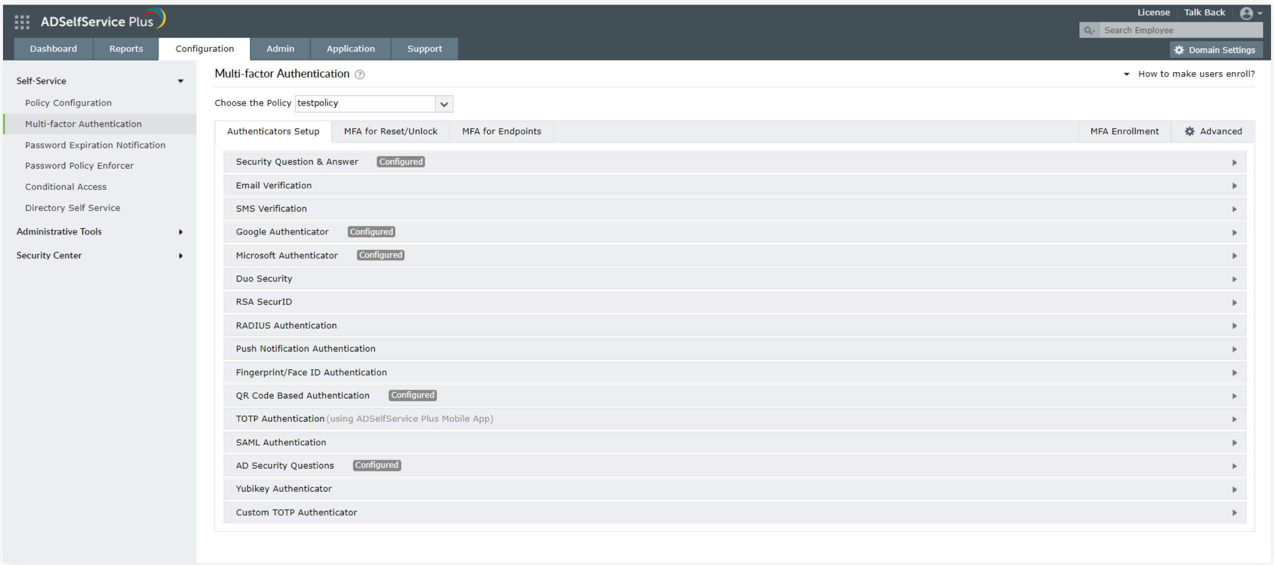
Implementing policies that enable stronger authentication methods in risky situations like accessing resources during non-business hours or accessing the domain network from an untrusted IP address is another way to prevent circumvention of MFA while securing access to your resources.

While the first strategy mentioned above can help avoid social engineering attacks like phishing, the second strategy helps prevent technical cyberattacks dependent on text fields and passcodes like brute-force attacks and injection attacks. It also helps avoid SIM swapping and other SIM-dependent attacks. Additionally, the MFA solution needs to be well-equipped to avoid technical attacks like session hijacking.

An all-rounded MFA solution designed to thwart MFA hacks

ManageEngine ADSelfService Plus, a self-service password management solution, provides an MFA feature that helps avoid MFA hack attempts. Here are the benefits to opting for ADSelfService Plus:

- Choose from 16 authentication methods, including Google Authenticator, YubiKey Authenticator, fingerprint and face ID-based authentication, and more.

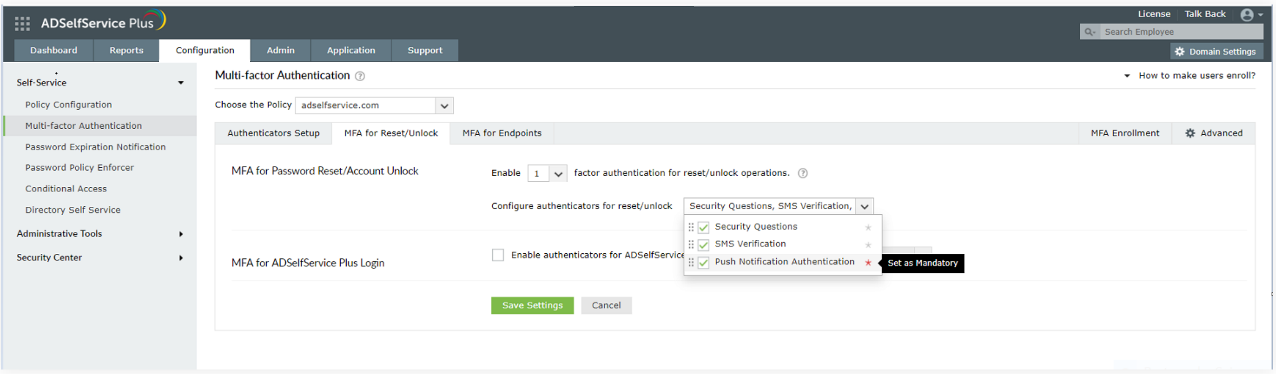


Multi-factor Authentication

Choose the Policy testpolicy

Security Question & Answer Configured
Email Verification
SMS Verification
Google Authenticator Configured
Microsoft Authenticator Configured
Duo Security
RSA SecurID
RADIUS Authentication
Push Notification Authentication
Fingerprint/Face ID Authentication
QR Code Based Authentication Configured
TOTP Authentication (using ADSelfService Plus Mobile App)
SAML Authentication
AD Security Questions Configured
Yubikey Authenticator
Custom TOTP Authenticator

- Mandate the use of certain authentication methods like biometrics and YubiKey Authenticator.



Multi-factor Authentication

Choose the Policy: adselfservice.com

MFA for Password Reset/Account Unlock

Enable 1 factor authentication for reset/unlock operations.

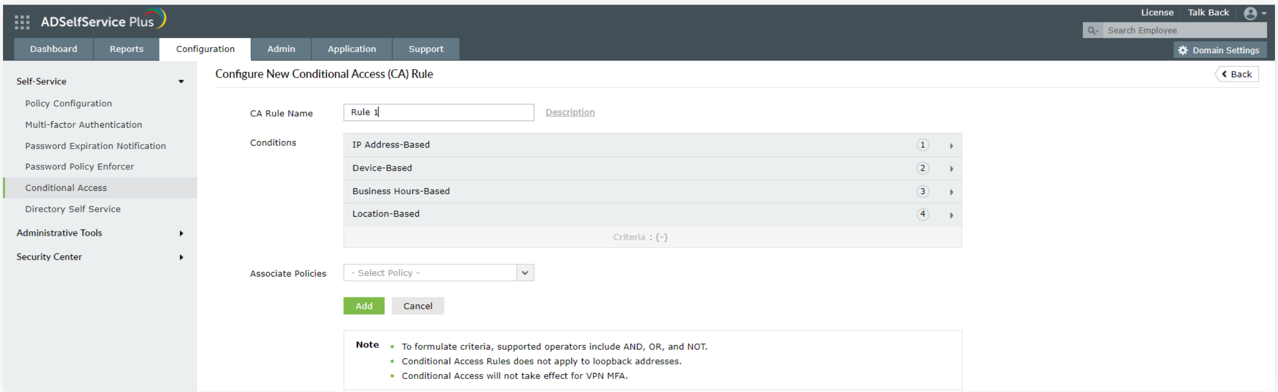
Configure authenticators for reset/unlock: Security Questions, SMS Verification,

☑ Security Questions
☑ SMS Verification
☑ Push Notification Authentication

MFA for ADSelfService Plus Login

□ Enable authenticators for ADSelfServic

- Use conditional access to apply specific MFA methods based on time of access, IP address, geolocation, and device.



Configure New Conditional Access (CA) Rule

CA Rule Name: Rule 1   Description

Conditions

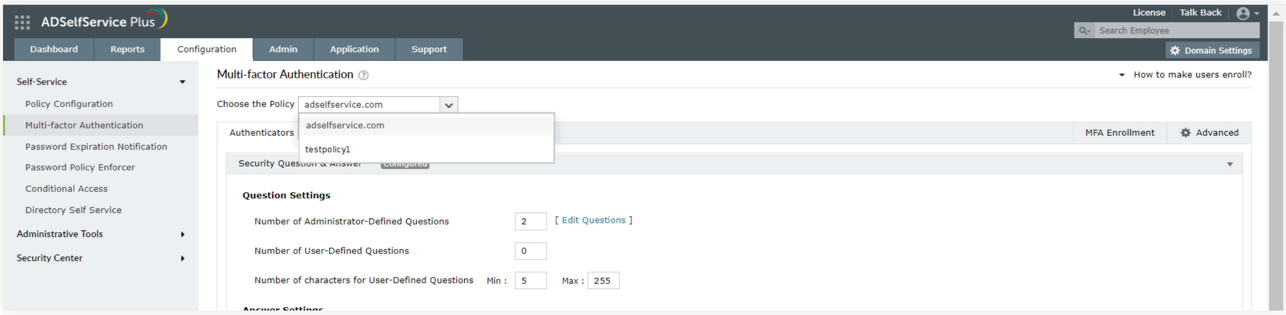
IP Address-Based	1
Device-Based	2
Business Hours-Based	3
Location-Based	4

Criteria : (-)

Associate Policies: - Select Policy -

Note
- To formulate criteria, supported operators include AND, OR, and NOT.
- Conditional Access Rules does not apply to loopback addresses.
- Conditional Access will not take effect for VPN MFA.

- Configure specific authentication methods for specific groups, organizational units (OUs), or domains using policies.



Multi-factor Authentication

Choose the Policy: adselfservice.com
adselfservice.com
testpolicy1

Security Question & Answer

Question Settings

Number of Administrator-Defined Questions: 2

Number of User-Defined Questions: 0

Number of characters for User-Defined Questions Min : 5 Max : 255

Answer Settings

ADSelfService Plus avoids session hijacking by implementing an HttpOnly flag and the secure flag for session cookies. Doing so makes the browser return an empty string as a result when a client-side script attempts to read cookies.

ADSelfService Plus' MFA feature can be used to secure:

1. Remote and local machine (Windows, macOS, and Linux) logins.
2. VPN logins.
3. Logins to SAML-based enterprise applications using single sign-on.
4. Self-service actions like password reset and account unlock using ADSelfService Plus.

Other features offered by ADSelfService Plus to amp up security in your Active Directory environment:

- **Password Policy Enforcer:**
  ADSelfService Plus allows the creation of custom password policies for specific groups, OUs, and domains. You can implement password rules that prevent patterns, restrict repetition of characters and old passwords, mandate inclusion of specific numbers of multiple character types, and more.

- **Integration with Have I Been Pwned? service:**
  ADSelfService Plus can be integrated with Have I Been Pwned? to prevent users from employing previously leaked passwords while resetting or changing their password.