THE COMPLETE GUIDE TO

Protecting Active Directory Against Brute-force Attacks

ManageEngine
ADSelfService Plus

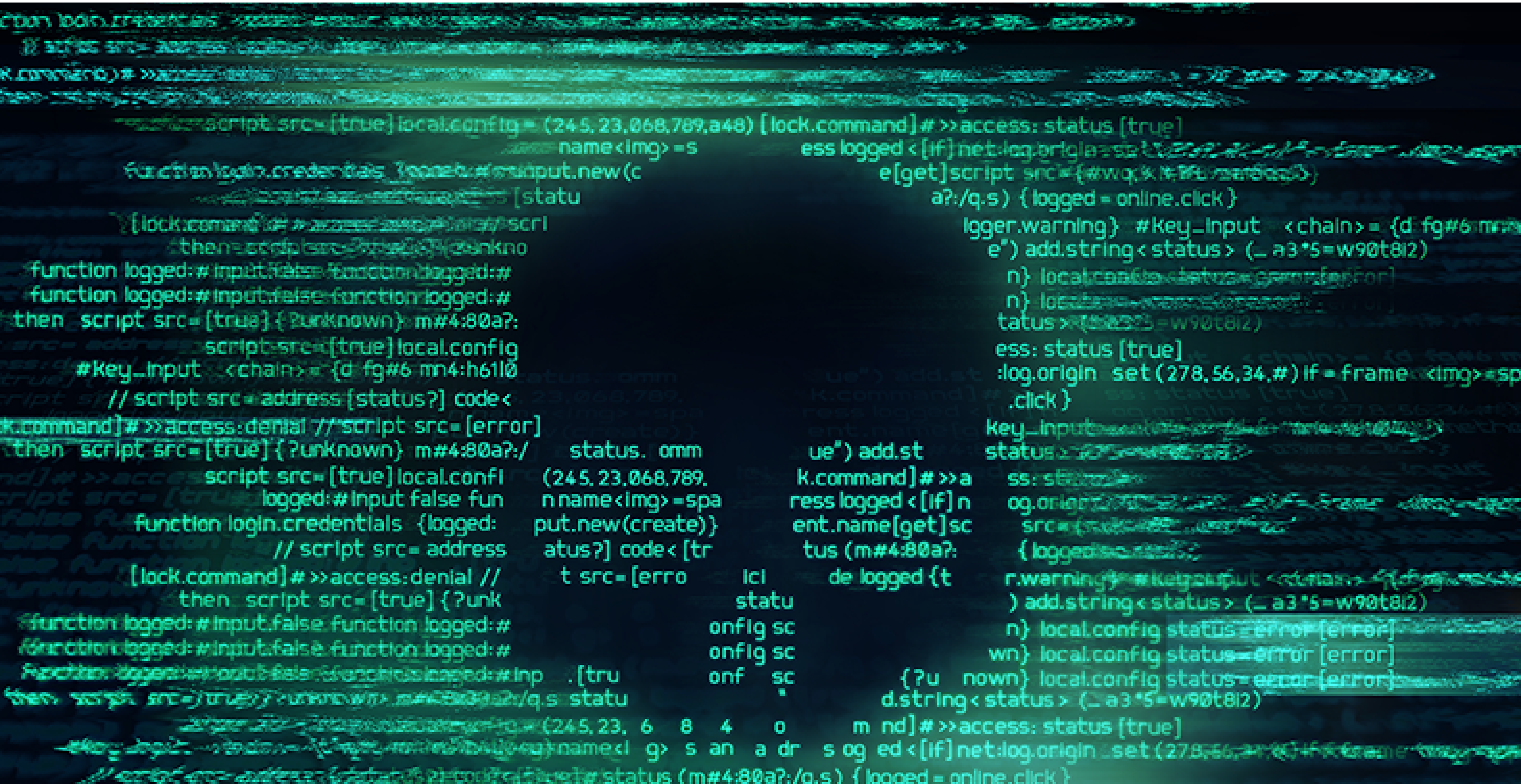


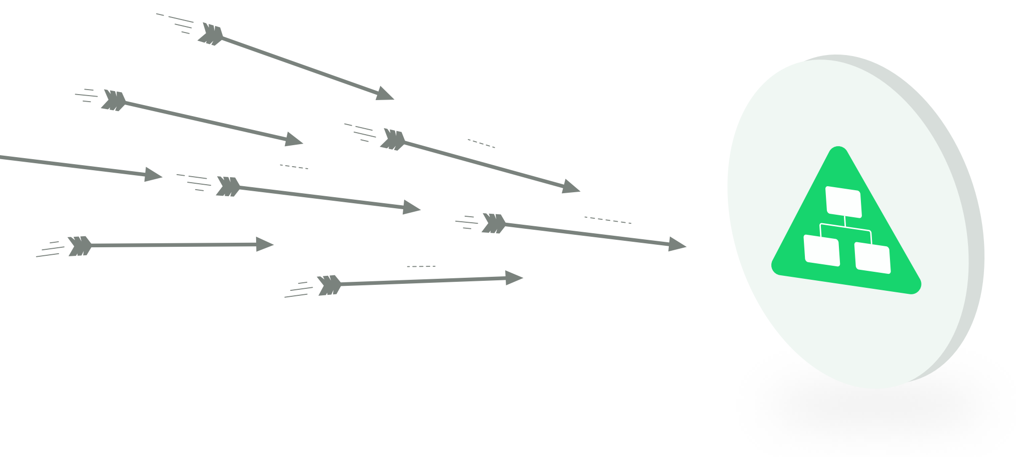
Table of contents

Introduction

Active Directory (AD), the technology that lets IT administrators manage permissions and access to network resources is a couple of decades old now. Yet, organizations continue to build their IT infrastructure around it. Because AD facilitates central management by tying together servers, workstations, applications, and other network components in an IT network, it's a key target for attackers. The volume of information stored in AD attracts the attention of attackers, and its weak passwords make them easy pickings.

This guide explores the various ways in which threat actors exploit poor password security, and how you can thwart their plans. We will walk you through how ManageEngine's solutions help you strengthen your password management.

Why are attackers after AD credentials?



What is AD? Imagine a box filled with every computer, user, application and service that runs in an organization's network. That box is AD, a critical application because it stores large amounts of data, and controls and organizes everything residing in it. AD is of high value to attackers because within it they can find identity-related information, including user permissions, passwords, and devices in the network.

To gain a foothold into your network, all the attacker needs to do is to compromise the domain user credentials of one of the thousands of accounts that might reside in your AD.

This explains why the bulk of cyberattacks today involve targeting the employee credentials of the increasing number of remote workers. 61% of all the attacks in 2021 involved credential data[1]. With remote work, Active Directory platform has become more vulnerable to attacks as it tries to serve the authentication request from users who use their unsecured personal devices to connect to corporate network and or use their home or other public wifi-networks to establish a connection. Also, the number of cloud applications and services organizations use are only growing and enabling authentication for these services through AD is a priority for many organizations. If the AD passwords in use are weak or are compromised passwords, then they put AD under great risk. These challenges have made AD more vulnerable than ever before.

In the next chapter, we will see, when the security defenses are not configured properly, how easy it is for attackers to compromise accounts using just one technique and the various tools that they use.

03

How threat actors take over AD accounts

Attackers usually take down domain user accounts with basic privileges. However after intrusion, attackers have plenty of tricks up their sleeves to raise the compromised account's privileges or move laterally in the network to discover vulnerable high privileged accounts.

For instance, dumping the passwords of domain admins stored in SYSVOL is one of the common methods attackers use to compromise local administrator accounts. SYSVOL is a folder that exists in every domain controller. It's a shared folder and every authenticated user of the domain has read access to it.

The passwords present in SYSVOL XML files are usually the local admin passwords and are also often encrypted using the AES-256 encryption standard.

Yet, attackers have access to PowerShell functions like the Get-GPPPassword, using which they can decrypt passwords. As you can see, within a few steps, the adversaries can get hold of a local admin account.

Once attackers have access to a domain admin account the possibilities are endless— they can either create backdoor accounts, in the local or systems within the domain to lurk in the network or install a malware on the compromised system for extorting sensitive data.

The consequences of an AD breach are dire. If you are looking to improve your AD security, the best place to start is by understanding attack techniques that are being used to compromise networks and take measures that can prevent them . Brute force attacks are the most common technique attackers are leveraging to infiltrate into corporate networks. They were used in over 80% of the data breaches in 2020[2].The low barrier to entry for carrying out brute force attacks is why it's such a widely used technique. Skilled adversaries usually build their own versions of the available tools. However script kiddies too can do more damage than what organizations would want.

04

Brute-force attacks and why you should never let your guard down against them

In a brute force attack, attackers persistently pound an account with multiple combinations of credentials until they can unlock it.

Understanding brute-force attacks, the most common hacking technique in an attacker's arsenal, will enable you to understand the risks they pose and the ways you can safeguard your organization against them.

Common types of brute-force attacks

Simple brute-force attack

In a simple brute-force attack a large combination of random values are input as passwords and they are iterated one after the other until the target cracks. The iteration is accomplished with the help of automated scripts. Attackers don't use this method while targeting resources that might be covered by an account lockout policy. Instead it's used to crack local files in systems that are protected by passwords.

Dictionary attacks

Here, common words or phrases are input as passwords. Today's attackers also use tools that can make minor substitutions to the password list available, say replacing "w" with "W" or "a" with "@" to improve their chances of cracking an account.

Hybrid brute-force attacks

This is a combination of a dictionary attack and a simple brute-force attack. Often the phrases that would be used in a dictionary attack are appended with a pattern of numbers, usually a birth year. This technique is particularly effective when the attacker has performed social profiling on the target.

Password spray attacks

In contrast to the multiple password bombardment style of other brute-force attacks, a password spray attack tries only one password but against multiple accounts. Since the attack resembles a normal login pattern, often times it goes undetected and won't disturb any account lockout policy in place.

Popular tools used in brute-force attacks

Here are basic details, provided for educational purposes, about five popular open source tools used in brute-force attacks.

1 **NL Brute:** A tool that's used in almost all Remote Desktop Protocol (RDP) attacks. In particular, it's used to crack local accounts in the system after the initial compromise.

2 **JohnTheRipper:** A password cracking software that can be used for over 15 different operating systems including Unix, Windows and DOS. It's an attacker's favorite as it can easily identify hashes of encrypted passwords.

3 **THC Hydra:** A tool used to take down network authentication protocols including RADIUS and Lightweight Directory Access Protocol (LDAP). It can also perform dictionary attacks on over 30 protocols, including HTTP, HTTPS, and the Server Message Block (SMB) protocol that's used to communicate with remote computers and servers.

4 **Hashcat:** A CPU-based password cracking tool. It's used to carry out various types of brute-force attacks, including dictionary and hybrid attacks.

5 **LOphtCrack:** A tool tailor-made for cracking Windows passwords. It can not only perform various types of brute-force attacks such as dictionary and hybrid attacks, but can also extract hashes of 64-bit Windows operating systems and decode them.

How botnets are used to carry out brute-force attacks

Besides manual operation, adversaries also use botnets to automate brute force attacks. Botnets are a group of computers that are infected by malware and are centrally controlled by a hacker. Attackers might choose to brute-force target several websites. Say attackers choose to hack into some websites of an organization using a brute force attack technique.

Because, in all the brute force attack techniques, the attacker is only going to try out various combinations of credentials mostly from the same IP address. However, if security systems website are configured to limit the login attempts after a specific number of failed logins from an IP address, the attack will fail or take too long to succeed.

In a botnet brute force attack, each bot receives a list of target IP addresses or websites and two or three credential pairs from botnet master or command and control (C2C) server. The botnets try out these credential pair on a target IP address. If they are unable to crack the password, the target IP address is passed on to another bot having a different IP address tries to break in. With bots, not only the number of attempts is kept below the account lockout threshold, but the attacks also don't originate from the same IP address, making them harder to detect.

05

How the Dharma ransomware leverages brute-force attacks

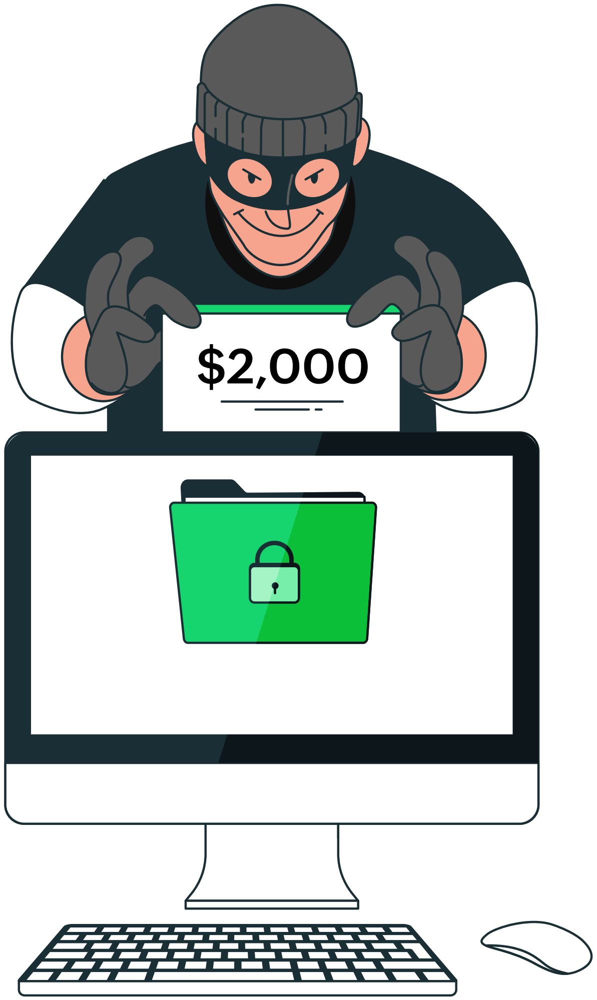
The Dharma ransomware, a variant of the CrySIS malware, was first discovered in 2016. It continues to be active even today due to its ability to intrude into victim's systems through multiple vectors. Though it spread using phishing campaigns and malware vulnerabilities in the beginning, RDP became it's most favored delivery vehicle.

Over 85% of all Dharma attacks[3] conducted so far have exploited open RDP connections. In most cases, attackers used brute-force techniques to barge in, while in others they made use of leaked RDP credentials available from the dark web.

Dharma has been thriving for so long due to the unique Ransomware-as-a-Service (RaaS) model it's part of. Experienced malware developers create new variants of Dharma just by making minimal changes to the source code such as changes to the encryption key used in the attack or the message the ransomware note displays.

Security researchers say this strategy of not chopping and changing few things in the source code is what makes it difficult to identity which threat group carried out a particular Dharma attack, since there is no unique signature.

Dharma malware developers add a package of tools and best practices that affiliates can follow and execute attacks without much hassle. Affiliates are mostly entry-level cyberattackers. The package consists of prebuilt scripts and tools that leverage built-in Windows tools, publicly available exploits, and third-party freeware tools all tied together with PowerShell, batch, and AutoIT scripts.



The key stages in a Dharma attack

1 Intrusion

Access to the target's device, and eventually the network, is mostly through exploitation of the open RDP ports- 3389. Simple brute-forcing or password spraying is the usual tactic deployed. Attackers either take over a user workstation or, in some cases, the domain controller if they can break into a domain admin's account. With the latter, they can affect multiple systems at once.

2 Creating a stronghold

Once the initial infection is complete, in most dharma attacks, attackers proceed to make entries in the Windows registry to enable persistence. The Windows registry is a database that stores information used by the operating system and the programs in it. Details of the software programs, hardware devices present, operating system configurations, everything can be found in the Windows registry.

3 Disabling security products

After establishing persistence, PCHunter and ProcessHacker, two freely available utilities that help detect, monitor and remove malware, are run to disable all security software that are installed in the system. From endpoint security systems, to SIEM alerting software, they can disable them all. In addition, PowerShell programs like Disable-WinDefend.ps1 are also executed to disable Windows Defender functions.

It doesn't stop there. To ensure maximum impact, attackers use more tools from their toolkit to brute-force into any local user accounts, get access to passwords stored in encrypted files—NirSoft CredentialsFileView tool does the job for them—and attempt to compromise more systems in the network.

Before executing the ransomware payload, any host backups and system logs present are erased, and existing services are halted, to ensure the data parts of those services can also be encrypted. For instance, dharma ransomware attacks are known to terminate database services such as sqlwriter, mssqlserver, sqlserveradhelper, to ensure data files that are in process by these services are also encrypted.

4 The encryption and the ransom note

The payload that encrypts data is often an executable file (.exe). In the case of the domain controller being compromised, attackers always create a script to alter the Default Domain Policy so this file is run during startup in each machine connected to the domain.

All files in the host infected with the ransomware are encrypted using AES-256 combined with a RSA-1024 asymetric encryption. Only the malware files and the system files are spared. Once the encryption is complete, a ransom note is left with two email addresses that the victim can contact.

06

5 steps you should take to protect yourself from brute-force attacks

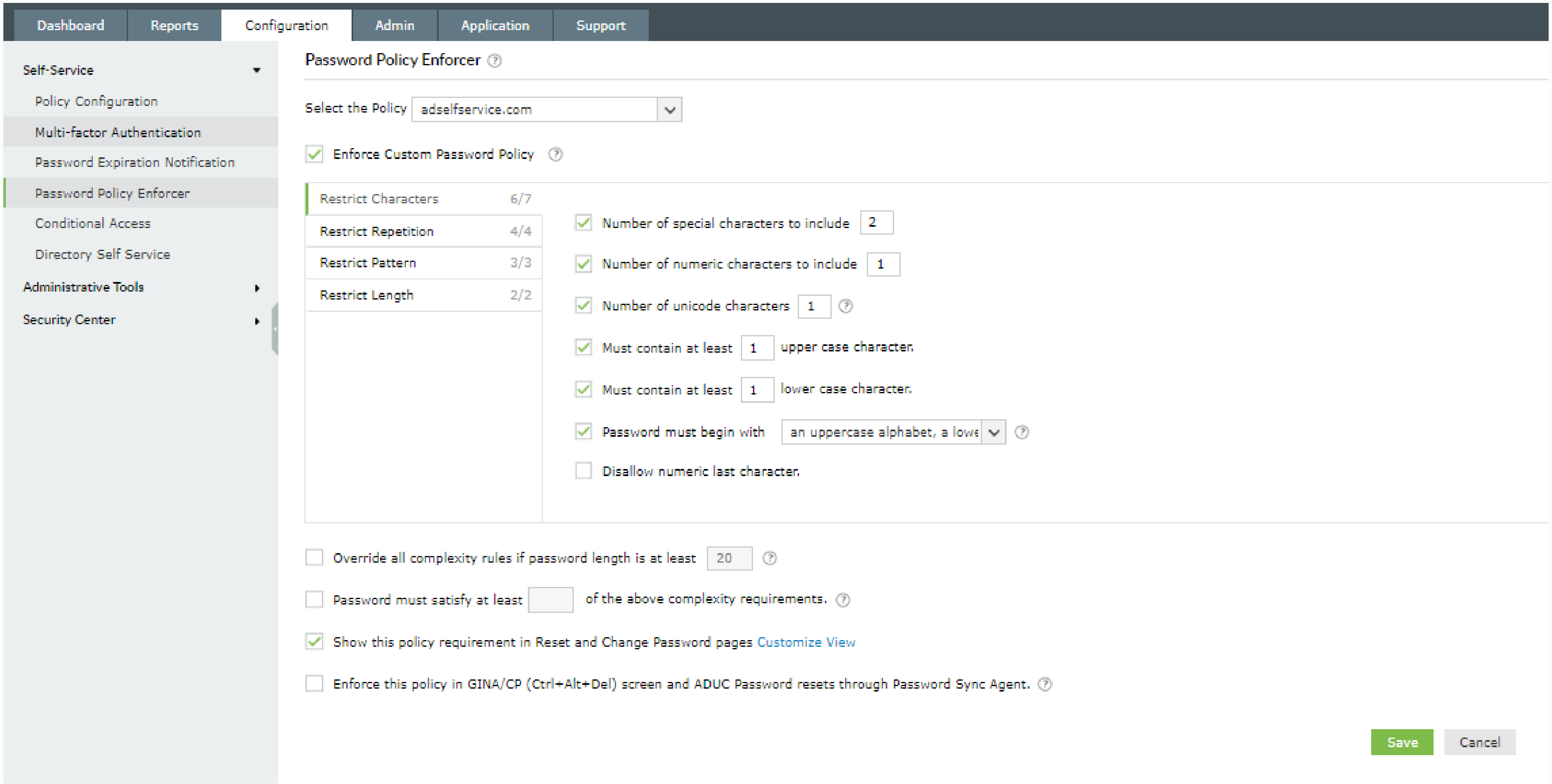
1. Enforce strong custom password policies

password best practices, like setting long and complex passwords, skipping passwords that are common dictionary words, and avoiding already compromised passwords.

How ADSelfService Plus can help:

With ManageEngine ADSelfService Plus' password policy enforcer, IT admins can ensure users follow one or all of these rules when the password is set:

- Meets a minimum length
- Includes both upper and lower case letters
- Includes special characters
- Includes numbers
- Begins with either a letter, a number, or a special character
- Blocks dictionary words, or patterns that are easy to crack
- Create a custom list of weak passwords which new password resets will be checked against
- Prevents the use of breached passwords through an integration with the "Have I been Pwned?" service that checks passwords against a continuously updated list of compromised passwords



Password Policy Enforcer

Select the Policy: adselfservice.com

☑ Enforce Custom Password Policy

Restrict Characters	6/7
Restrict Repetition	4/4
Restrict Pattern	3/3
Restrict Length	2/2

☑ Number of special characters to include: 2

☑ Number of numeric characters to include: 1

☑ Number of unicode characters: 1

☑ Must contain at least 1 upper case character.

☑ Must contain at least 1 lower case character.

☑ Password must begin with: an uppercase alphabet, a lowe

□ Disallow numeric last character.

□ Override all complexity rules if password length is at least 20

□ Password must satisfy at least ___ of the above complexity requirements.

☑ Show this policy requirement in Reset and Change Password pages Customize View

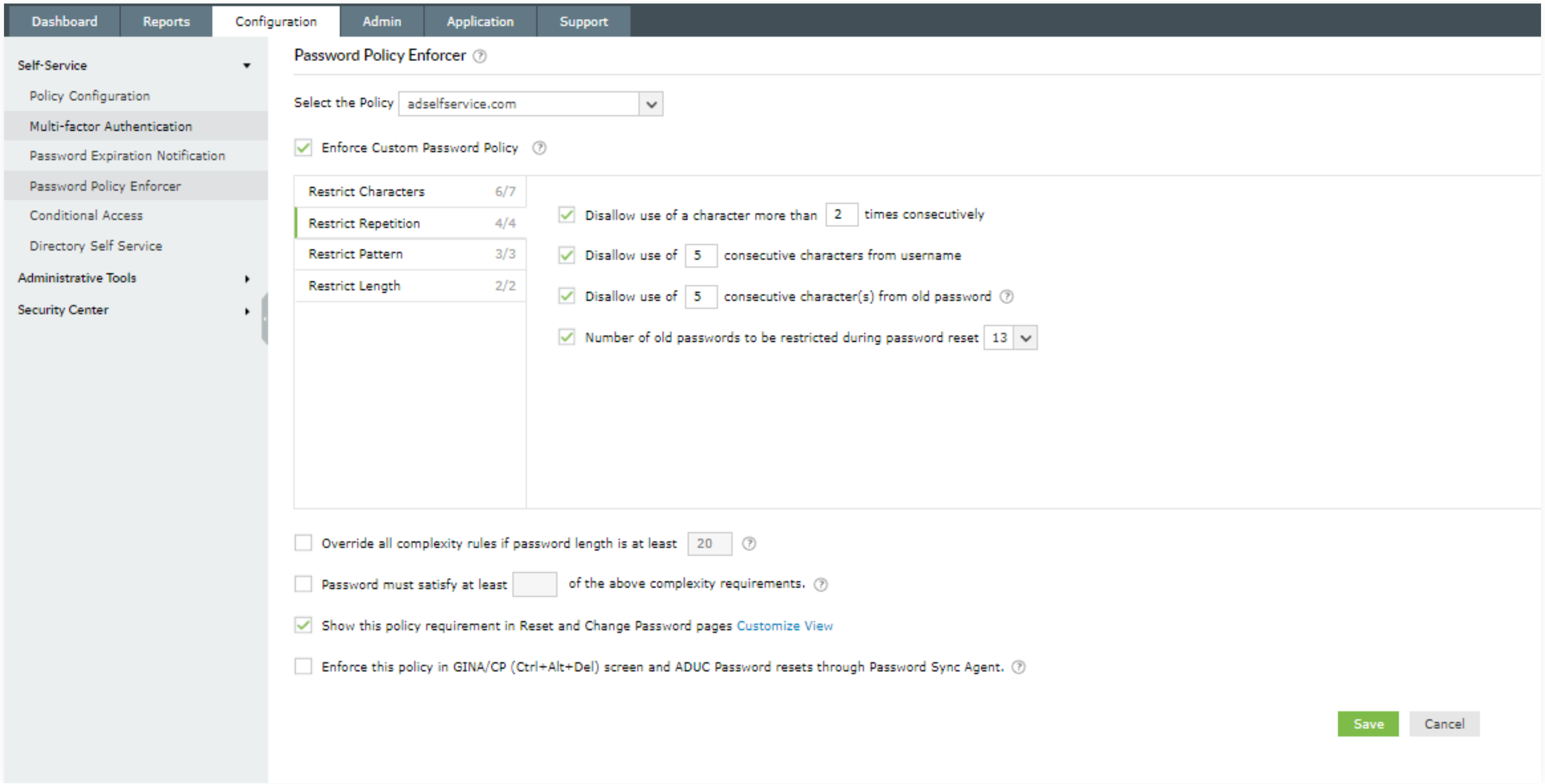
□ Enforce this policy in GINA/CP (Ctrl+Alt+Del) screen and ADUC Password resets through Password Sync Agent.

2. Restrict users from reusing old passwords

54% of all employees reuse passwords for many of their work accounts, a recent survey[4] by hardware authentication device manufacturer Yubico revealed. Thanks to password reuse, attackers need to compromise only one pair of corporate credentials to sneak into your network.

How ADSelfService Plus can help:

With ADSelfService Plus' password history check feature, IT admins can ensure that users can't reuse any of their past 24 AD passwords.



Password Policy Enforcer

Select the Policy: adselfservice.com

☑ Enforce Custom Password Policy

Restrict Characters	6/7
Restrict Repetition	4/4
Restrict Pattern	3/3
Restrict Length	2/2

☑ Disallow use of a character more than 2 times consecutively

☑ Disallow use of 5 consecutive characters from username

☑ Disallow use of 5 consecutive character(s) from old password

☑ Number of old passwords to be restricted during password reset 13

□ Override all complexity rules if password length is at least 20

□ Password must satisfy at least of the above complexity requirements.

☑ Show this policy requirement in Reset and Change Password pages Customize View

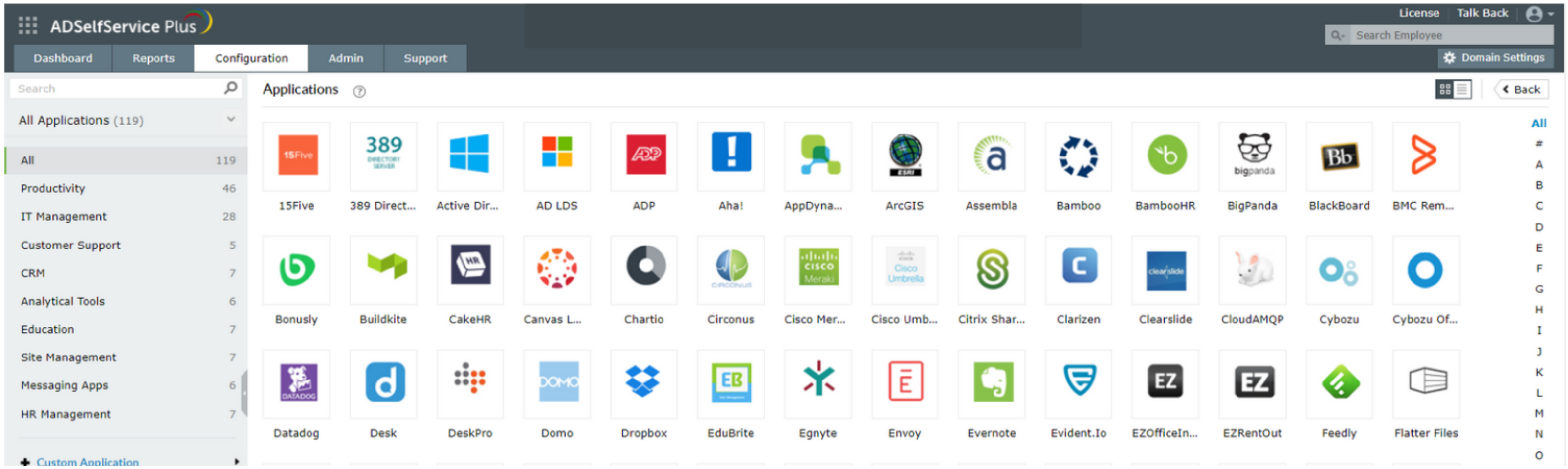
□ Enforce this policy in GINA/CP (Ctrl+Alt+Del) screen and ADUC Password resets through Password Sync Agent.

3. Set up single sign-on (SSO) for your applications and secure it with multi-factor authentication (MFA)

In addition to internal applications, today's organizations use multiple cloud applications and services. SSO is crucial if you are looking to improve user experience and identity security. With SSO, since employees need to remember only one pair of credentials, which in most cases is their AD credentials, the danger of password reuse is averted. However, an SSO implementation without MFA does more harm than good from a security standpoint as it only makes the job for attackers easier. All they have to do is compromise one account to gain access to all your applications.

How ADSelfService Plus can help:

With ADSelfService Plus, you can enable SSO for over 100 pre-integrated applications and for any custom application that supports Security Assertion Markup Language (SAML)-based authentication. It also shows the user all the applications they have access to in a single dashboard. Access to applications can be secured using MFA. Additionally, IT admins can decide who has access to which applications by creating policies based on AD organizational units and groups.



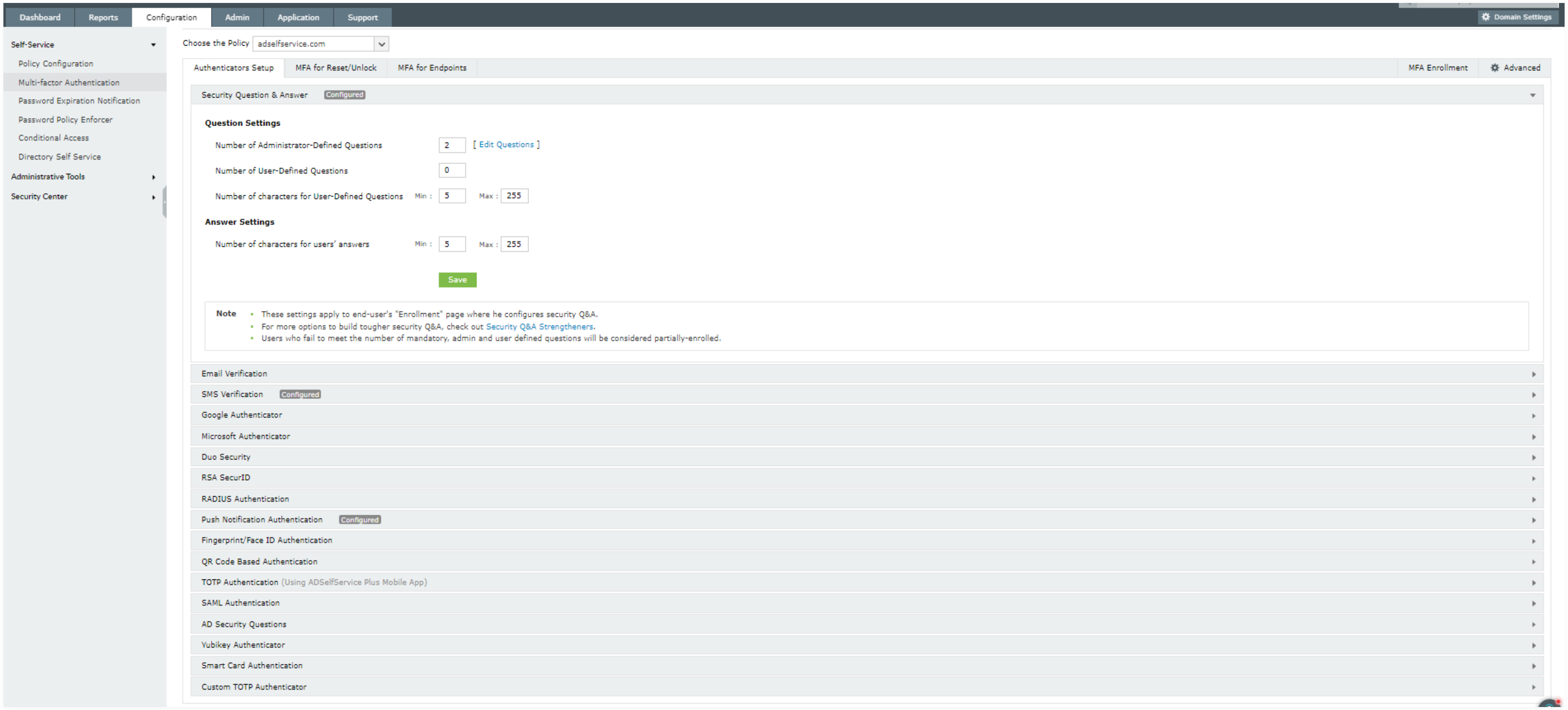
4. Enable MFA for virtual private network (VPN) logins, workstations, applications, and self-service features

Passwords, the most common authentication factor used to verify identity, is the most vulnerable one too, because users tend to set easy-to-remember passwords, and are likely to use the same weak password for other devices and services. MFA provides an extra layer of security, as it involves verification of an additional factor that the user owns, like a smartphone, or the user is, like a fingerprint or any other biometric attribute. With MFA, even if the password is compromised, the attacker can't complete the heist, as they don't have access to the additional factor.

One the best ways to protect your RDP connections from attacks like the Dharma ransomware we saw earlier, is to grant RDP access only through a VPN and further strengthen security by securing the VPN access with MFA. Other steps to take are ensuring unnecessary open RDP ports are locked down, periodically reevaluating users who can RDP into the network, and keeping the Network Level Authentication of your RDP server always ON.

How ADSelfService Plus can help:

ADSelfService Plus supports over 15 authentication techniques, including YubiKey authentication, biometrics, and RSA SecurID. With ADSelfService Plus' MFA options, IT admins can secure VPN connections, Windows, Mac, and Linux endpoints, safeguard access to SSO-enabled applications, and ensure users can use the self-service password reset or account unlock features only after their identity is verified.



Choose the Policy: adselfservice.com

Security Question & Answer — Configured

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

Number of characters for users' answers — Min : 5 Max : 255

Note

- These settings apply to end-user's "Enrollment" page where he configures security Q&A.
- For more options to build tougher security Q&A, check out Security Q&A Strengtheners.
- Users who fail to meet the number of mandatory, admin and user defined questions will be considered partially-enrolled.

Email Verification

SMS Verification — Configured

Google Authenticator

Microsoft Authenticator

Duo Security

RSA SecurID

RADIUS Authentication

Push Notification Authentication — Configured

Fingerprint/Face ID Authentication

QR Code Based Authentication

TOTP Authentication (Using ADSelfService Plus Mobile App)

SAML Authentication

AD Security Questions

Yubikey Authenticator

Smart Card Authentication

Custom TOTP Authenticator

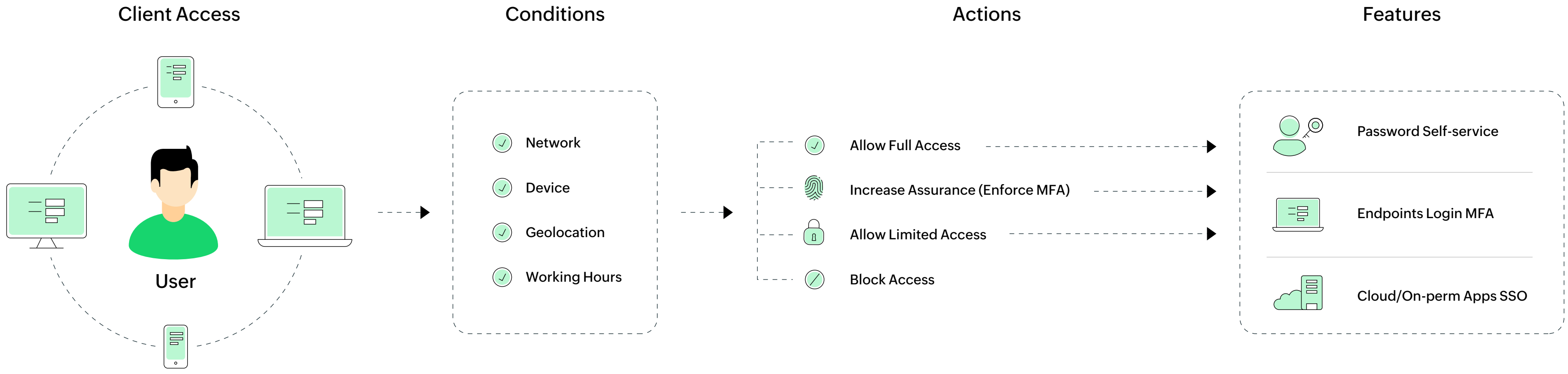
5. Enhance security with contextual authentication

In today's remote-first organizational setup, the likelihood of a cyberattack is enormous. The context behind any login attempt, especially ones after failed attempts or from an unknown location or device, should be examined and access should be provided only for those who don't pose any security threat to the organization.

For example, in many RDP attacks, threat researchers found the RDP server under attack received a barrage of authentication requests either from IP addresses that never connected to the network before, or from locations that the company didn't have employees in. Had there been a mechanism to block such authentication requests, the attacks wouldn't have made it even to the second stage.

How ADSelfService Plus can help:

Organizations can analyze various risk factors such as IP address, time of access, device and user's geolocation, and configure conditional access policies based on them. IT admins can also create policies that check either one or all of the factors. Based on the risk, a user can be asked to prove their identity by submitting an additional authentication factor, granted full or partial access, or be denied access.

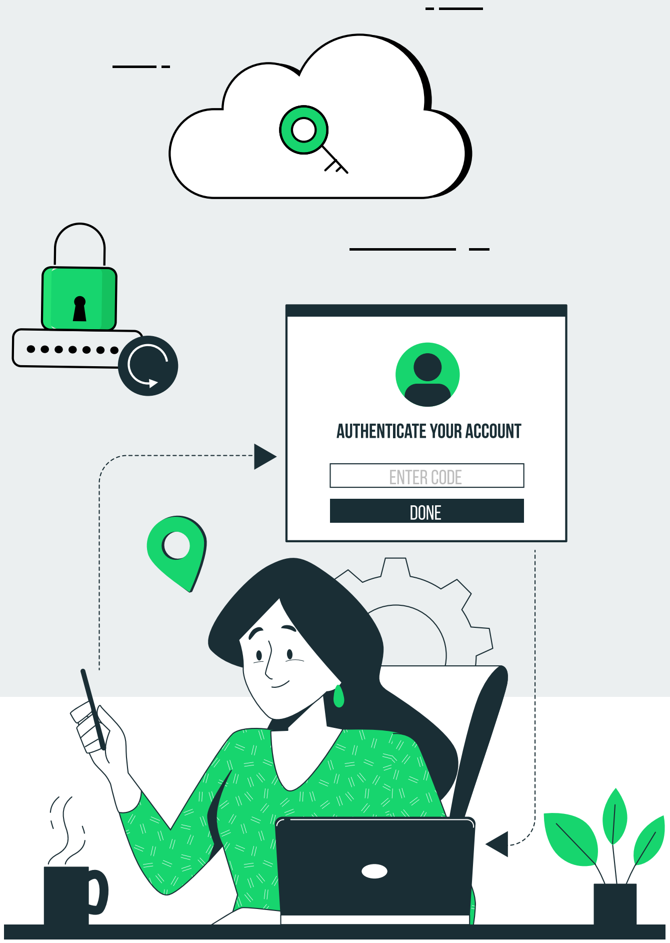


About ADSelfService Plus

ManageEngine ADSelfService Plus is a web-based self-service password management and single sign-on solutions. It offers password self-service, multi-factor authentication for endpoints, password expiration reminders, a self-service directory updater, a multi-platform password synchronizer, and single sign-on for applications. ADSelfService Plus also offers both Android and iOS mobile apps to facilitate self-service for end users anywhere, at any time. ADSelfService Plus supports IT help desks by reducing password reset tickets, and spares end users the frustration caused by computer downtime.

Download

$ Get a quote



Footnotes

[1] 2021 Data Breach Investigation Report
https://www.verizon.com/business/resources/reports/dbir/

[2] 2020 Data Breach Investigation Report
https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf

[3] Dharma ransomware attacks SMBs during COVID-19 pandemic
https://backendnews.net/dharma-ransomware-attacks-smbs-during-covid-19-pandemic/

[4] Cybersecurity in the Work From Anywhere Era report https://pages.yubico.com/cybersecurity-in-the-work-from-home-era