ManageEngine
ADSelfService Plus

How to prevent **password mismanagement of remote employees**

www.adselfserviceplus.com

Table of Contents

Introduction

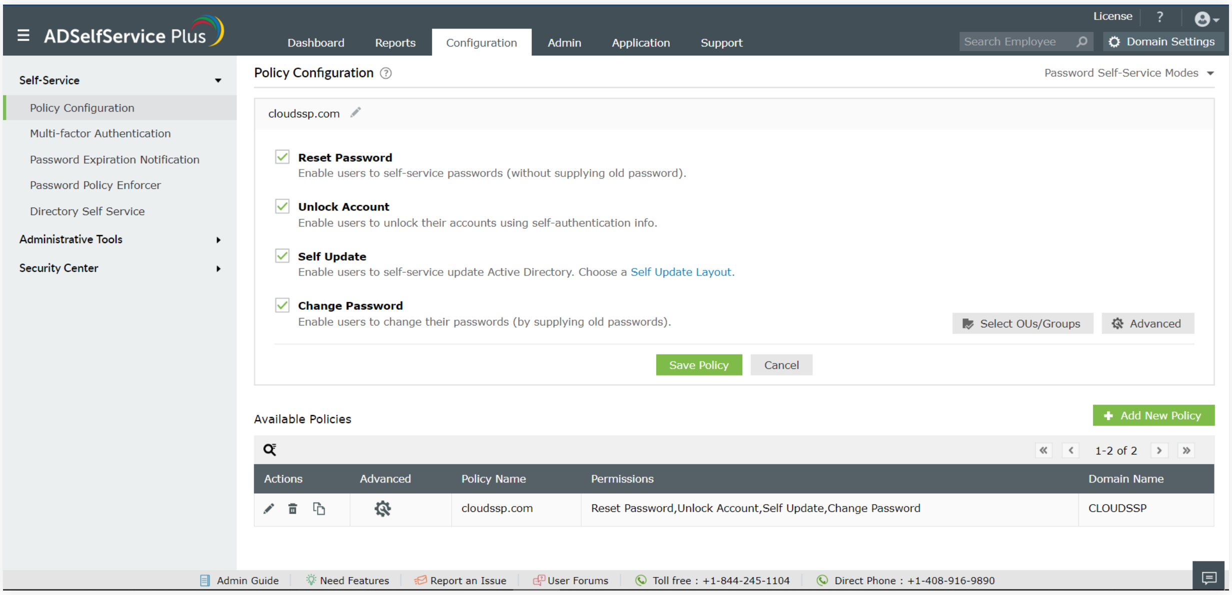
Now that everyone has come to terms with remote working, it feels like things can't get much worse. Unfortunately, hackers are leveraging the buzzing topic of the pandemic as bait.

Compromised passwords are one of the more common ways by which hackers can get into your organization. So, it's imperative that your organization has a solid password management and security system. Remote work brings with it a new set of password management issues and loopholes. Let's take a look at how we can tackle these remote work woes.

Employees can't change their account passwords

Under normal circumstances, most employees would be in the office. Should their passwords expire or their accounts get locked out, they would just contact the help desk to get things fixed. However, the process becomes cumbersome while working from home, and it can cost time, which can end up costing your business.

To tackle this challenge, admins can enable remote users to change their passwords or unlock their accounts by themselves. Solutions like ADSelfService Plus allow admins to enable password self-service for remote users. This allows users to change their passwords right from their logon screens. This saves time and reduces help desk costs of your organization.



Policy Configuration

cloudssp.com

☑ **Reset Password**
Enable users to self-service passwords (without supplying old password).

☑ **Unlock Account**
Enable users to unlock their accounts using self-authentication info.

☑ **Self Update**
Enable users to self-service update Active Directory. Choose a Self Update Layout.

☑ **Change Password**
Enable users to change their passwords (by supplying old passwords).

Available Policies

Actions	Advanced	Policy Name	Permissions	Domain Name
		cloudssp.com	Reset Password,Unlock Account,Self Update,Change Password	CLOUDSSP

Fig 1: Self-service policy configuration tab in ADSelfService Plus

Employees aren't able to update their passwords

Now that there's a way to let remote users update their passwords, there's still the issue of their passwords not being updated in the directory network. While in office, employee devices are connected to your organization's directory network, which means updating their passwords isn't be a problem. While working remotely, their cached passwords can't be updated, and the users might be locked out of their accounts.

Updating users' cached credentials over the users' home network can fix this problem. However, the users' home network may not be as secure as your organization's network. Solutions such as ADSelfService Plus have a neat function that securely updates the cached credentials through a VPN. This negates the possibility of bad actors gaining users' credentials through insecure home networks.

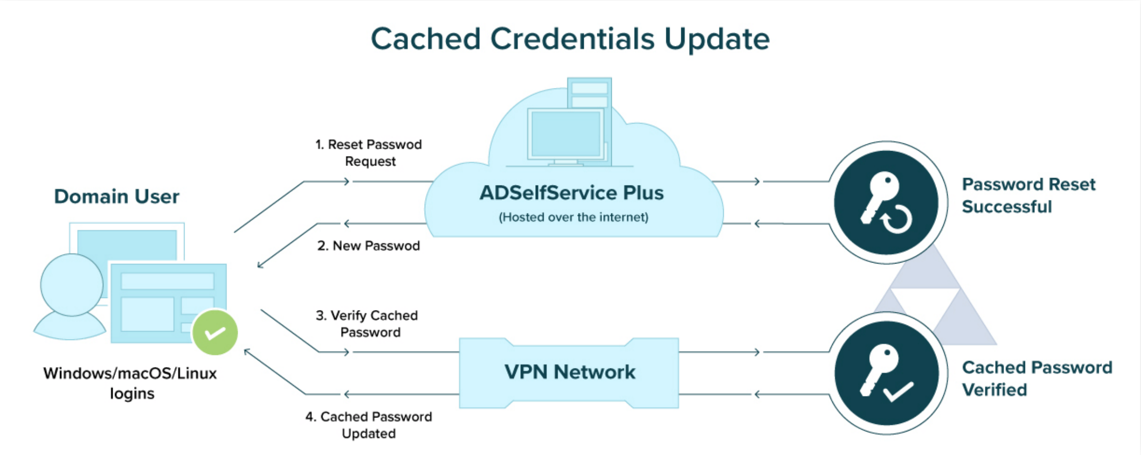

Cached Credentials Update
Domain User
Windows/macOS/Linux logins
1. Reset Passwod Request
2. New Passwod
3. Verify Cached Password
4. Cached Password Updated
ADSelfService Plus
(Hosted over the internet)
VPN Network
Password Reset Successful
Cached Password Verified

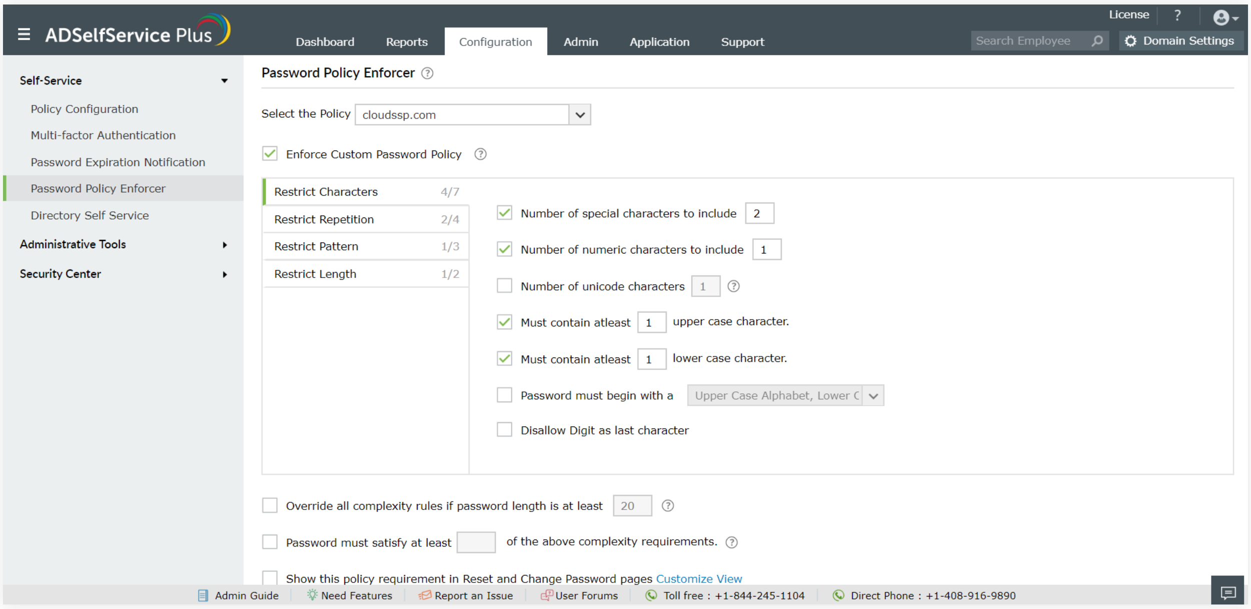
Fig 2: Cached credentials update process in ADSelfService Plus

Employees are setting weak/compromised passwords

Passwords are the first line of defense against an intruder attempting to get inside an organization. While working from home without proper monitoring and policies in place, users may be tempted to set weak passwords. This compromises the security of the entire organization. An organization's security is only as strong as its weakest password.

To prevent users from setting weak and compromised passwords, stringent password policies can be implemented across your organization, even for remote employees.

With a solution like ADSelfService Plus, not only can admins set strong password policies, they can also configure different policies to different OUs and groups based on their privilege. This way, user accounts with higher privileges get better security. Admins can also ensure that users don't set dictionary words and already compromised passwords; they can even upload their own dictionary of breached passwords.



Password Policy Enforcer

Select the Policy: cloudssp.com

☑ Enforce Custom Password Policy

Restrict Characters	4/7
Restrict Repetition	2/4
Restrict Pattern	1/3
Restrict Length	1/2

☑ Number of special characters to include 2

☑ Number of numeric characters to include 1

□ Number of unicode characters 1

☑ Must contain atleast 1 upper case character.

☑ Must contain atleast 1 lower case character.

□ Password must begin with a Upper Case Alphabet, Lower C

□ Disallow Digit as last character

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

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

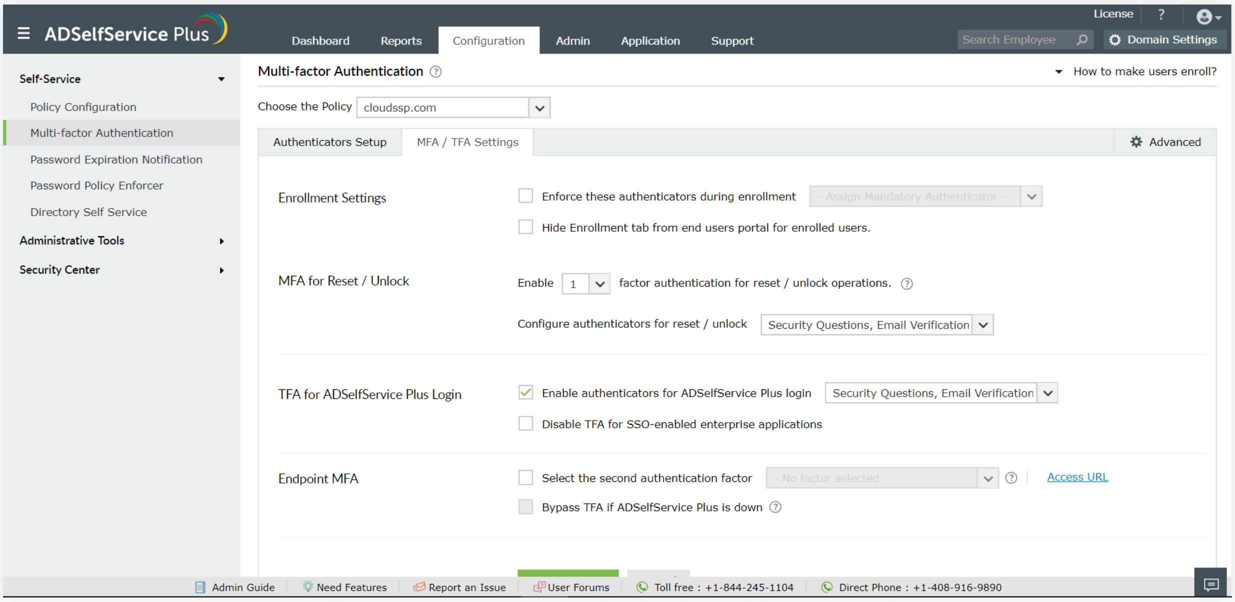
□ Show this policy requirement in Reset and Change Password pages Customize View

Fig 3: Password policy enforcer tab in ADSelfService Plus

There is no secure way to authenticate employees

There shouldn't be just one line of security to protect your organization. There should always be a second factor in case a users' password gets compromised, so that a malicious actor can't get inside your organization with stolen credentials alone. Users need to authenticate themselves in more than one way.

Enabling two-factor authentication for remote users can bolster the security of your organization. Authentication mechanisms like fingerprints or one-time passwords (OTPs) ensure that only legitimate users can gain access to their accounts. Solutions like ADSelfService Plus enable two-factor authentication right in the users' logon screens, and it supports strong authentication mechanisms such as RADIUS authentication, push notifications, and fingerprint authentication among many others. The tool also allows admins to set up multi-factor authentication for all SAML-enabled applications combined with enterprise single sign-on, so users don't have to remember multiple passwords.



Multi-factor Authentication

How to make users enroll?

Choose the Policy: cloudssp.com

Authenticators Setup | MFA / TFA Settings | Advanced

Enrollment Settings
- □ Enforce these authenticators during enrollment: - Assign Mandatory Authenticator -
- □ Hide Enrollment tab from end users portal for enrolled users.

MFA for Reset / Unlock
- Enable 1 factor authentication for reset / unlock operations.
- Configure authenticators for reset / unlock: Security Questions, Email Verification

TFA for ADSelfService Plus Login
- ☑ Enable authenticators for ADSelfService Plus login: Security Questions, Email Verification
- □ Disable TFA for SSO-enabled enterprise applications

Endpoint MFA
- □ Select the second authentication factor: - No factor selected -
- Access URL
- □ Bypass TFA if ADSelfService Plus is down

Fig 4: Multi-factor authentication tab in ADSelfService Plus

Summary

Without necessary security measures, organizations working remotely can become an easy target for hackers. To ensure that the hackers don't take advantage of the current situation, your organization must have a strong security infrastructure. Since passwords play such an important role in security, having a strong password management solution, especially for remote working conditions, can go a long way in keeping your organization secure.

ManageEngine
ADSelfService Plus

ADSelfService Plus is an integrated self-service password management and single sign-on solution. It offers password self-service, password expiration reminders, a self-service directory updater, two-factor authentication for Windows logons, a multiplatform password synchronizer, and single sign-on for cloud applications. ADSelfService Plus' Android and iOS mobile apps, as well as Windows, macOS, and Linux login agents, facilitate self-service actions for end users anywhere, at any time.

$ Get Quote

Download