ManageEngine
ADSelfService Plus

Self-Service Password Reset (SSPR) for remote users

www.adselfserviceplus.com

Table of contents

1. The state of remote work

According to a recent survey by Buffer, 90 percent of remote workers plan on working remotely for the rest of their careers, and 94 percent encourage others to give remote jobs a shot. Companies are opening their gates to employees who work remotely, as organizations that allow remote work are seeing better retention rates. Some CEOs like Dave Nevogt of Hubstaff, a company that helps others hire remote talent, believe that remote employees stay longer, work harder, and offer better ROI over co-located employees.

For companies that use Active Directory (AD) to manage their IT, supporting remote work through client machines is not a problem thanks to password caches.

2. What are cached credentials in Active Directory and how do they work?

When a user tries to log on to a client machine by entering their credentials, the credentials are passed to the nearest domain controller for authentication. If there are no domain controllers available in the network, like in the case of remote workers, the error message *"There are currently no logon servers available to service the logon request."* appears.

To avoid this, a local copy of the user's credentials can be stored on the client's machine. The number of credentials stored in the client machine can range from 0 to 50, depending on the set registry value. To ensure security, the client machine stores an encrypted verifier of the password instead of the actual password. This verifier is a salted MD4 hash that is computed two times.

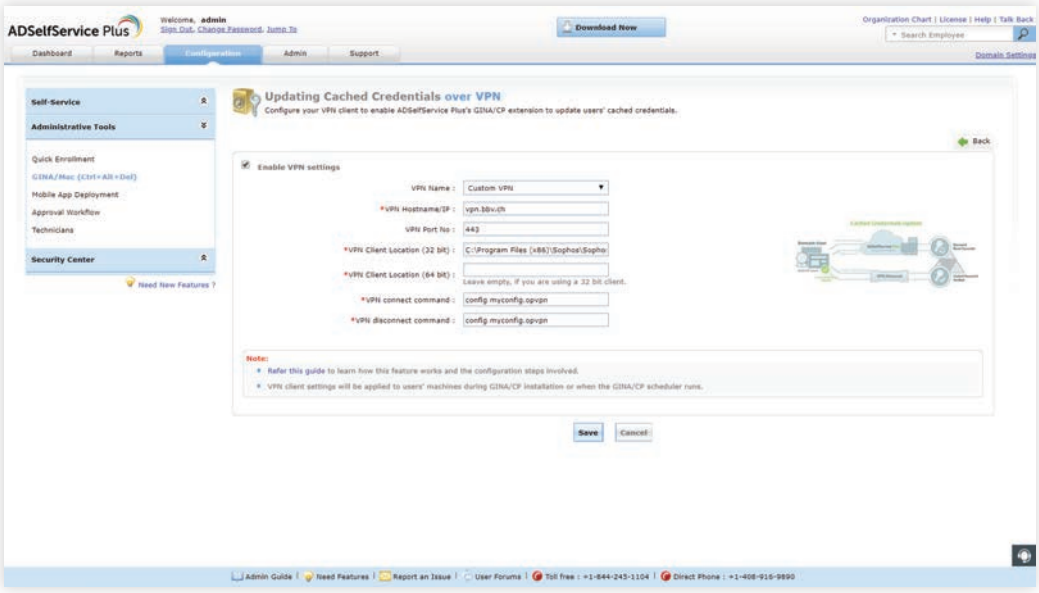
Storing the encrypted verifier locally helps users log in to their machines even when they're not connected to the network. However, while the cached credential feature can be helpful, it falls short in one critical aspect.

3. Where the Active Directory cache process falls short

AD's inability to update cached credentials on client machines is a major hinderance when users forget their passwords or get locked out of their accounts while working remotely. In such cases, the password resets done by the IT help desk don't get reflected on the client machines unless the user is connected to the domain controller's network. This leaves the user unable to access their machine, and stalls their work.

4. The solution: ADSelfService Plus

ADSelfService Plus, a secure, web-based end-user password reset management and single sign-on solution, resolves this problem by updating the cached credentials when users reset their AD passwords through a "forgot password" link.



4.1 How it works

4.1.1 Prerequisites

- ADSelfService Plus' server and the VPN's server have to be hosted over the internet. However, Active Directory need not be hosted.
- The VPN provider should be command-line based and the VPN's client should be installed in the end-user client machine of Active Directory. You can also refer to this step by step guide to learn about the feature and the configuration steps involved.

4.1.2 The process

After a successful password reset, the cached password is updated on the user's machine.

- ADSelfService Plus places a Reset Password/Account Unlock button right on the Windows logon screen through its GINA/CP client. Remote users can use this button to reset their forgotten passwords.
- ADSelfService Plus resets the password in AD and notifies the GINA/CP client that the reset operation was successful.
- The GINA/CP client establishes a secure connection with AD through a VPN client, such as Fortinet and Cisco AnyConnect, and initiates a request for updating the local cached credentials.
- After the request is approved by AD, the cached credentials are updated on the user's machine.

4.2 Benefits of implementing cached credential update using ADSelfService Plus

- Users can work on the go without worrying about forgotten passwords, locked out accounts, or expired passwords.
- The CP client displays the password complexity requirements users have to meet while resetting passwords.
- Users in different parts of the globe don't have to worry about whether the IT help desk is available, as there's zero dependency on them for password requests.
- IT help desks can focus on critical tasks that require their expertise, rather than servicing password reset tickets.

5. Other handy features of ADSelfService Plus

With ADSelfService Plus you can:

- Restrict self-service password reset, account unlock, and other privileges based on users' group or OU memberships.
- Implement multi-factor authentication for self-service password resets.
- Implement two-factor authentication for Windows logons.
- Notify users about their soon-to-expire passwords or accounts, and prompt them to update their accounts.
- Enable single sign-on to over 100 enterprise applications.
- Synchronize passwords of over 10 cloud applications with AD passwords.
- Empower users to update their details into AD directly and supervise them through approval workflows.