

© 2009 ManageEngine, ALL RIGHTS RESERVED



ADSelfService Plus Password Reset Process

ADSelfService Plus Password Reset Process

© 2009 ManageEngine, ALL RIGHTS RESERVED

The information provided in this document is proprietary and copyrighted under applicable laws. None of this information can be reproduced or disseminated through any means.

OBJECTIVE: To explain briefly the basic methodology of the password reset process of ADSelfService Plus.

INTRODUCTION: ADSelfService Plus is a self-service password reset application, which empowers you – the domain's end user – with capabilities to reset passwords/ unlock accounts all by yourself. Extending its capabilities, ADSelfService Plus also enables you to enter your personal information into Active Directory.

THE SAFE AND SECURE PASSWORD RESET METHOD OF ADSELFERVICE PLUS

ADSelfService Plus adopts a three-pronged approach to facilitate a password reset:

- First, it enrolls and formulates identification criteria for you, in case you are permitted (by system administrators) to reset passwords through it (Enrollment Process).
- Second, it uses these criteria to establish your identity when you request for password reset. (Verification Process)
- Third, it calls for the service of a Windows API to change the password for you. (Password Reset Process)

Given below is the detailed description of these three processes:

1. ENROLLMENT & IDENTITY CRITERIA FORMULATION:

A password reset software's aim is to help you, in case, you should forget your password – a basic identity criteria for a domain user. Thus it is imperative for such software to define identification criteria that could be easily remembered and reproduced.

To address this issue, ADSelfService Plus has defined a set of questions – called Security Questions – that elicit a very personal and unique response. Since it is personal information, you can remember it easily and others cannot guess it. ADSelfService Plus also allows you to define your own questions, enhancing security even better. But the number of questions you can define is entirely at a system administrator's discretion.

It is mandatory that you answer all the necessary questions and complete enrollment, failing which you will not be able to use the product. These answers are stored in the product's inbuilt database and referenced to establish your identity, whenever you request a password reset.

Storing answers to Security Questions: Since they are used to establish the identity of a user, the answers are stored in an encrypted format in the database to avoid any identity theft. This encryption is achieved through a one-way hash algorithm, meaning the encrypted answer cannot be traced back to its original form.

2. VERIFICATION PROCESS:

It begins right at Enrollment Process. When you attempt to enroll, ADSelf Service first verifies whether you are a legitimate member of a domain or not. If yes, you are allowed to enroll, else denied access and presented with an alert "Invalid Login Name/Password".

The domain level check is performed only during enrollment and once you get enrolled, ADSelfService Plus will always look into the enrollment list to locate you whenever you request a password reset.

If you are recognized as an enrolled user, ADSelfService asks the Questions that were selected by/ defined by/ imposed on you during Enrollment. If you answer all the questions correctly, you are allowed to reset the password, else denied access and prompted to enter correct answers.

[Users not enrolled will be prompted to enroll before continuing to use the software]

Verifying answers to Security Questions: An ordinary compare-and-verify is not possible here, as the secret answers entered during Enrollment are stored in an encrypted format using a one-way algorithm. Therefore it is necessary that the answers submitted for verification also be encrypted by the same one-way algorithm and compared with the ones in the database, something similar to comparing fingerprints. This ensures maximum password security, to the extent that not even the administrator or product could retrieve user entered passwords!

3. PASSWORD RESET PROCESS:

Once your identity is established through the processes mentioned above, ADSelfService Plus calls for the Windows API responsible for password reset and passes your new password to it. Acting much like a relay, this function deposits the new password directly into Active Directory. Neither this function nor any component of ADSelfService Plus has any provision to store/cache/reproduce the password.

Though a password reset product, ADSelfService Plus is completely sealed off from passwords that it handles, making it a safe and secure password reset software.

ADVANTAGES OF ADSELSERVICE PASSWORD RESET APPROACH

1. Wider range of secret Q&A that elicits unique answers from users and therefore stand as reliable user identification criteria.
2. Since the secret answers are encoded through a one-way (or irreversible) hash algorithm, not even the administrator or the software can retrieve them.
3. It is impossible to retrieve any user's password through ADSelfService Plus, as it does not store/cache/reproduce user passwords intrinsically or anywhere other than the Active Directory database.