PRIASOFT™
Experts in Exchange Migration and Management

Technical Details of Priasoft's Credential Manager

Priasoft's tools have the ability to store and persist credentials that are used to access Active Directory. The storage of such credentials is private to the Priasoft applications and is encrypted using RSA encryption and stored in the current user's profile on disk – this means that in order to use the credentials, a user must logon as the specific user where the credentials were saved. This prevents multiple users from gaining access to the saved credentials.

What can be done with the stored credentials?

The stored credentials allow a user of Priasoft applications to select previously saved credentials to allow Priasoft's tools access to required remote systems. The access provided depends upon the selected Priasoft application, however NONE of Priasoft's applications allow you to perform any destructive changes in the source environment – no deletes, no password changes, no group assignment changes, etc. Furthermore, no other non-Priasoft tools can utilize the stored credentials and there is no way to expose the password in plain text. Additionally, if one were to edit the saved credentials, the password would have to be re-entered again – this prevents a user from reusing a set of credentials for a different resource.

Priasoft does not provide any generalized AD tools that also use the saved credentials. Only the Priasoft Exchange Migration Suite tools have access to the saved credentials.

Why use Priasoft's credential storage?

In some environments, access to Active Directory – especially as a Domain Admin – can be highly restrictive. In an effort to provide tools that are not only simple to use but also simple to deploy and implement, it was determined that in more restrictive environments that one or both of the environments might not be willing to let a 3rd party have knowledge of an account with Domain Admin privileges. For instance, if the source environment that is involved in a migration were itself a high security environment, like law enforcement or military environments, the owner of such an environment is not likely to supply a username and password of an account with sufficient privilege to allow the migration to succeed. In these cases, the ability to safely store the credential, for use only for the migration tool eases the burden of trying to umbrella the 3rd party with the source environment's security policies (which could mean a dedicated resource from the source environment to shadow the migration team – such is cumbersome and potentially expensive).

Using Priasoft's credential storage allows the source environment to have control over the migration team's ability to migrate (the supplied account can be disabled at any time or the password changed). This feature allows the tools to do the work necessary for the migration without requiring a member of the source environment being present during the migration, while at the same time protecting the source environment from security risks.

What is the process to store the source environment credentials?

The process is quite easy. At some time during the planning and testing stage of the migration, a member of the source environment should gain access to the migration computer and enter the server, domain, username and password required. In most cases this can be done by a remote desktop session or by a webcasting tool (like Webex). If such is not acceptable, the Priasoft tools can be installed on a computer in the source environment for the sole purpose of creating the cached credentials, then the credentials can be saved to a file (using Regedit) and then imported into the migration team's workstation. Because the credentials are encrypted before being saved in the registry, it is safe to persist them in this way.

If there are any further questions about the Priasoft Credential Storage feature, please contact a member of our support team at: support@priasoft.com.