Tech Brief

Password Power 8
Active Directory Self-Service
Password Recovery Plug-In

PistolStar, Inc.
PO Box 1226
Amherst, NH 03031
USA

Phone: 603.546.2300
Fax: 603.546.2309
E-mail: salesteam@pistolstar.com
Website: www.pistolstar.com

Password Power 8
Active Directory Self-Service
Password Recovery Plug-In

Summary

The Password Power Active Directory Self-Service Password Recovery Plug-In enables end-users who have forgotten their network password to reset it themselves or view it right from their workstation. If it is reset, the new password is available for immediate use.

Typically, when end-users forget their network password, they must contact and engage an administrator or the Help Desk to manually reset the password for them. With the Password Power Password Recovery Plug-In, the IT department is relieved of the task of resetting or recovering end-users' passwords.

The following provides a step-by-step explanation on how the Password Recovery Plug-In works and corresponds with the steps outlined in Figures 1 and 2 contained in this document. The green rectangles in Figures 1 and 2 denote actual steps in the process, while the yellow diamonds denote decision points.

How It Works

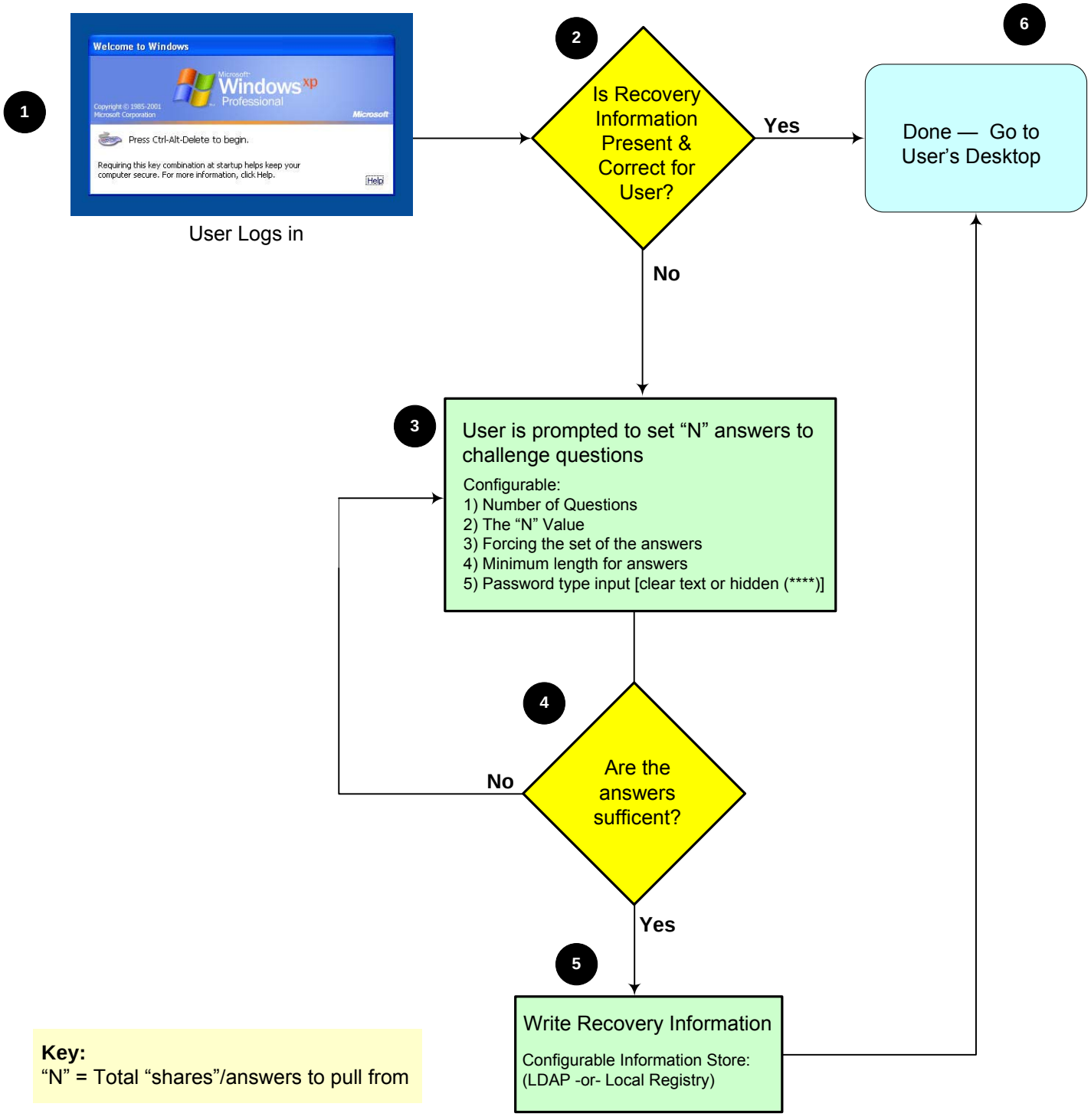
Setting Recovery Information **(see Figure 1 on page 2)**
The end-user's network password is part of the set of credentials they provide for initially accessing Microsoft Windows. These credentials could be either locally defined or domain accounts (e.g. Microsoft Active Directory, Novell eDirectory).

When an end-user first logs on to Windows after the Password Recovery Plug-In has been installed **(Step One)**, they will be prompted to set their recovery information **(Step Two)**. The recovery information comprises the answers the end-user has provided to multiple challenge questions. These questions, as well as the minimum number of them the end-user must later answer to recover their password, are established by the administrator.

The end-user is then prompted to set answers to a specific number ("N") of the questions presented **(Step Three)**. "N" represents the total "shares" or questions the end-user must answer when setting their recovery information. The administrator can also configure a minimum length requirement for the answers.

After the end-user has entered their answers to the selected challenge questions, the Password Recovery Plug-In will validate whether the answers are sufficient **(Step Four)**. If they are, the Plug-In will attempt to save their recovery information in the configurable information store (the end-user's LDAP directory account and/or the local registry) **(Step Five)** and provide them with a confirmation if the save is successful. From there, the end-user can proceed to their desktop **(Step Six)**.

Figure 1.



Using Recovery Information **(see figure 2 on page 4)**
When an end-user has forgotten their network password and wants to perform password recovery, they just need to click on "Cancel" at the Windows logon dialog box **(Step One)**. Pressing the Esc key will achieve the same result, which is to launch the Password Power Recovery wizard. A window then appears asking the end-user if they would like to continue with the password recovery process to reset their password **(Step Two)**. After they hit the "Ok" button, the end-user is prompted for their network username and domain **(Step Three)**. If they hit "Cancel" during either of these two prompts, the end-user will be returned to the Windows logon dialog box.

After the end-user has provided their identity, the Password Recovery Plug-In searches for their password recovery information **(Step Four)**. If no recovery information is found for that end-user, they are prompted to contact the Help Desk. If they mistyped their name, they do have the opportunity to correct it.

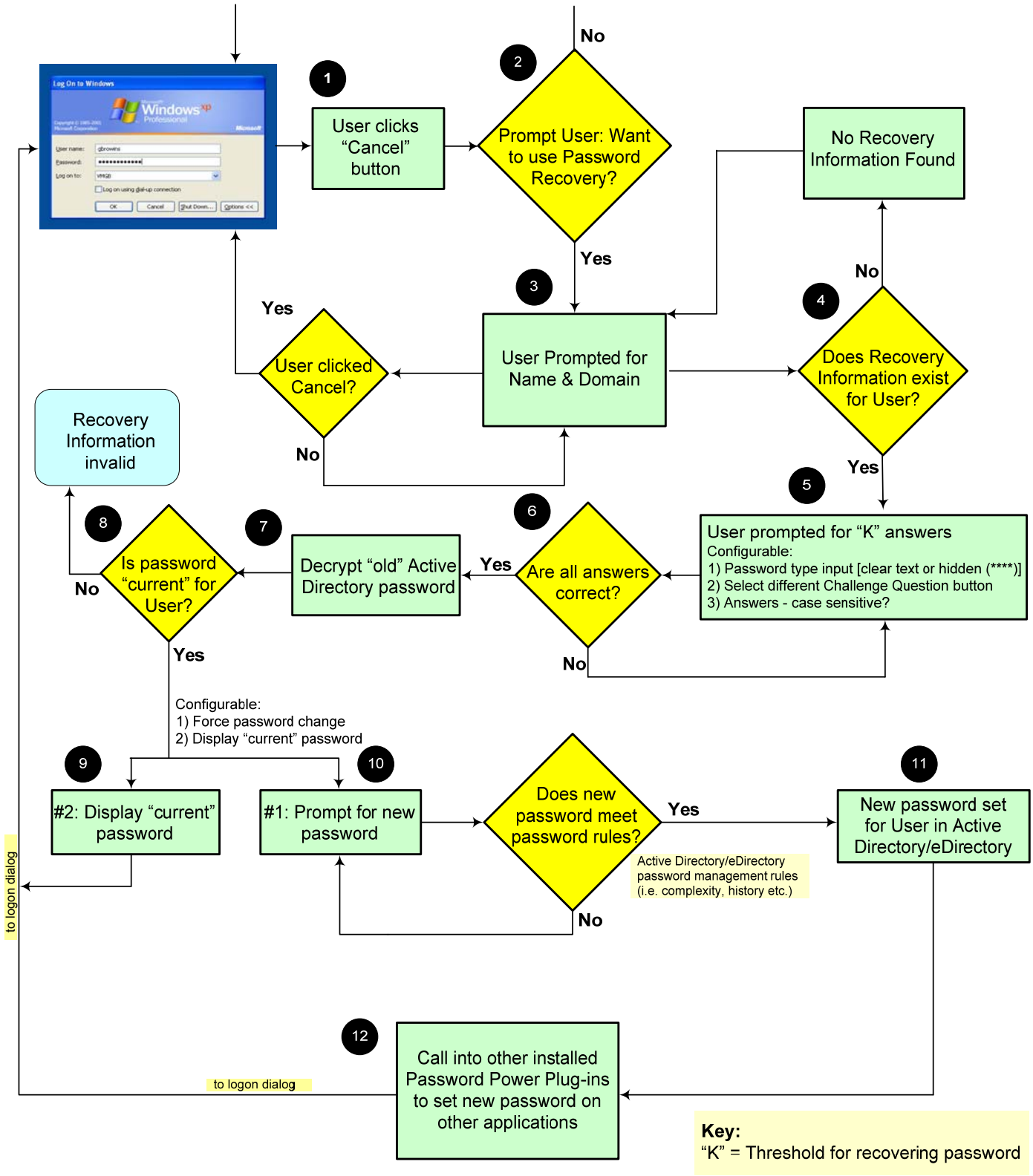
If the recovery information for that end-user is found, the end-user will then be prompted to answer a subset of the questions they previously answered when setting their recovery information **(Step Five)**. The number of questions ("K") to which they must provide answers is the "threshold" and is configurable.

If the end-user forgets the answer to a specific question, they can click on the "Recycle" button to bring up another challenge question to which they might remember the answer.
The administrator can also configure whether end-users enter clear text or "password-type" answers, which allows answers to be case-sensitive.

The Password Recovery Plug-In will verify that all the answers are correct **(Step Six)**, and then decrypt the old (or current) network password **(Step Seven)**. After it's determined that the password is the current one for that end-user (and therefore valid) **(Step Eight)**, the next step — which is also configured by the administrator — is to either force the end-user to make a password change or present them with their current password **(Step Nine)**. If the current password is being presented (option #2), the administrator has the option of specifying whether a complete or partial password is displayed. The end-user is then taken back to the Windows logon dialog box to log in. Option 2 is an important one for traveling end-users who cannot connect to a domain controller to reset their password from the road.

If the end-user is prompted to set a new network password (option #1), they must enter a new password that meets password management and strength rules for their domain. When it's determined the new password meets these rules **(Step Ten)**, it is set for the end-user in their network directory (e.g. Active Directory, eDirectory) **(Step Eleven)**. As the end-user moves on to the Windows logon dialog box to log in, the Password Recovery Plug-In calls into the other installed Password Power Plug-Ins to set the new password on other applications **(Step Twelve)**.

Figure 2.



Deployment

The Password Power Password Recovery Plug-In installation is seamless and does not require changes to the LDAP/Active Directory schema or any software to be installed on the LDAP/Active Directory servers. It is installed with the Password Power client to every workstation and laptop that requires the functionality. To simplify installation and enable customers to deploy it automatically without end-user intervention, the Password Power client uses a fully compliant MSI — Microsoft Installer, which leverages the Windows Installer service. All Windows versions supported by Password Power already employ Windows Installer to facilitate software installs. By using an MSI package, Password Power enables customers to perform a "silent install," whereby end-users experience no interruptions in their workday and are not required to take any actions. Examples of other typically used deployment software include Microsoft SMS, BMC Marimba, Altiris Deployment Solution and Numara Deploy.

System Requirements

The Password Power Password Recovery Plug-In supports Microsoft Windows Vista, XP, 2003 and 2000, and passwords for the following LDAP Directories: Microsoft Active Directory, Novell eDirectory, Lotus Domino LDAP, Tivoli Directory Server and Sun ONE LDAP. No changes are required to the LDAP schema.

References

PistolStar TechNote #254
"The Advantage of Authentication Redirection Over Password Synchronization"

PistolStar White Paper
"Using Microsoft Active Directory in the Domino World"

PistolStar White Paper
"Eliminating Notes ID File Password Management: A Ground-breaking Alternative"

###