PRODUCT LEAFLET

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

PASSWORD COMPLEXITY MANAGER (PCM)

WHEN IT COMES TO SETTING PASSWORD COMPLEXITY RULES, OPTIONS ARE A GOOD THING. WITH PCM FROM TOOLS4EVER, YOU HAVE THE FLEXIBILITY TO CREATE RULES THAT WORK FOR YOUR ORGANIZATION RATHER THAN CONFORMING YOUR ORGANIZATION TO A PRE-DEFINED SET OF SOMEONE ELSE'S RULES.

Standard security policies for password complexity are fine for some organizations, but if your requirements call for the implementation of a higher level of password complexity, then you should consider Password Complexity Manager (PCM) from Tools4ever. PCM presents a complete, user-friendly alternative to Microsoft's Fine Grained Password Policies and it's compliant with HIPAA and SOX security requirements.

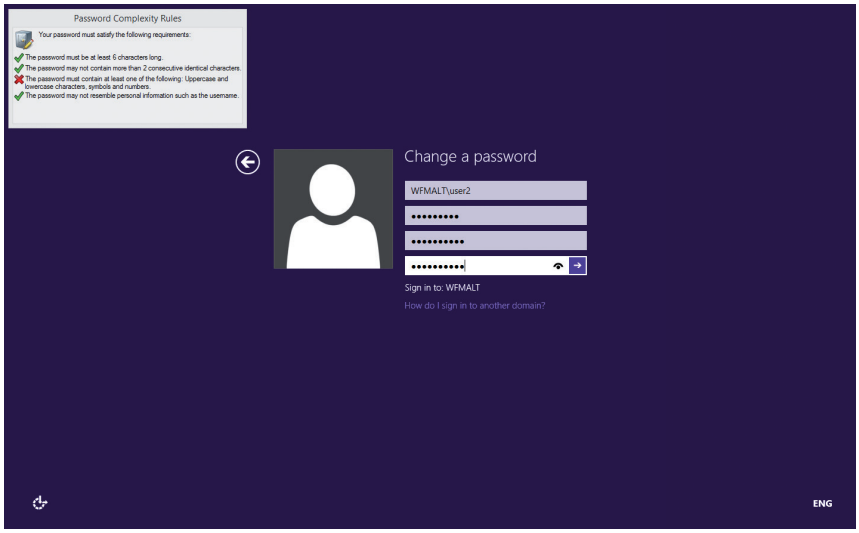
PCM OF TOOLS4EVER

With PCM, system administrators can:

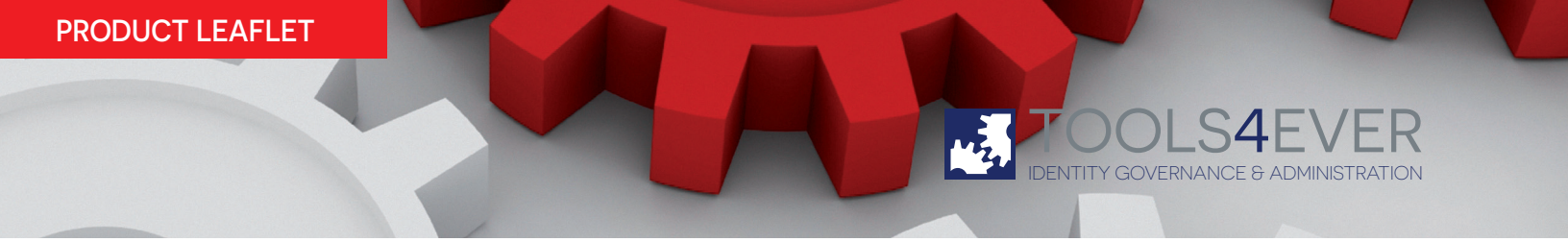
- Set different levels of complexity for various user groups.
- Prohibit certain types of passwords, such as company name.
- Prevent the use of sequences e.g. 1; 2; 3; Jan; Feb; Mar.
- Ensure 100% compliance with HIPAA and SOX.

PCM is easy to configure and provides end users with an overview of complexity rules that have and have not been met during the password reset process, so they can see immediate feedback as to whether they are in compliance with password complexity rules as they are setting up their passwords. This immediate on-screen feedback helps reduce the burden on your support teams related to password complexity questions. For added convenience, PCM can also be integrated with Self Service Reset Password Manager (SSRPM) to enable end users to reset their own pass

WHEN THE END-USER ENTERS A NEW PASSWORD, THE RULES THE NEW PASSWORD MUST COMPLY WITH ARE SHOWN STEP BY STEP



WITH ADDED CAPABILITIES BEYOND THE ACTIVE DIRECTORY STANDARD, PCM GIVES YOU THE POWER TO CREATE AND MANAGE THE RULES YOUR ORGANIZATION NEEDS TO ENSURE THE HIGHEST LEVEL OF SECURITY.



TOP THREE ADVANTAGES OF PCM

PCM offers three key features above and beyond the standard Windows complexity rules including:

- The option to set the password complexity at the OU level in the AD domain where a distinction can be made between various end-users and the degree of complexity of the password that must be used.
- An infinite number of combinations for password rules so that it's possible, for example, to provide a list of words that cannot be used, or to require that the password not contain a common or recognizable term or expression.
- Providing end users with on-screen feedback as to whether the rules were complied with during the reset password.

WINDOWS 2008 (OR LATER) VERSUS TOOLS4EVER PCM

PASSWORD COMPLEXITY RULES	PRE MS WINDOWS 2008	MS WINDOWS 2008 OR LATER	TOOLS4EVER PCM
USER-FRIENDLY ERROR NOTIFICATION	-	-	✔
Configurable at domain level	✔	✔	✔
Configurable at users/group level	-	✔	✔
CONFIGURABLE AT OU LEVEL	-	-	✔
Remembers password history (old passwords cannot be re-used)	✔	✔	✔
Maximum validity of password	✔	✔	✔
Minimum validity of password	✔	✔	✔
Maximum length of password	-	-	✔
Minimum length of password	✔	✔	✔
Exclude words	-	-	✔
Repeat characters	-	-	✔
Require specific characters	-	-	✔
Password similarity	-	-	✔

CONTACT TOOLS4EVER TODAY TO LEARN MORE ABOUT HOW PCM CAN GIVE YOU CONTROL OVER YOUR ORGANIZATION'S PASSWORD RULES.

CONTACT US: EAST – 866-482-4414 EMAIL: NASALES@TOOLS4EVER.COM
WEST – 888-770-4242 EMAIL: NWSALES@TOOLS4EVER.COM