Sysgem AG
Lavaterstrasse 45
8002 Zürich
Switzerland

Tel: +41 (0) 44 204 6023

office@sysgem.com
www.sysgem.com

Sysgem Password Policy Enforcer

Installation and User Guide

Sysgem AG
Lavaterstrasse 45
CH-8002 Zürich
Switzerland

Aug-2011

Introduction

The Problems

This product addresses two problems:

1. Enforcing a complex corporate password policy and
2. Allowing employees to reset a Windows password if a series of questions can be correctly answered.

Both solutions require an extension to the Windows Logon software by adding a GINA (described later).

The password reset option uses a special service installed on domain controllers.

Password Enforcement

Overview

The password enforcer implements a domain-wide corporate password policy, for example minimum password length, minimum digits and minimum lowercase characters (see the sample rules file below).

When the user presses *Ctrl+Alt+Del* and selects *Change Password* a popup window is displayed which explains the corporate password policy.

There are two components:

1. The GINA which is integrated into the Winlogon which provides interactive logon support and password change. The GINA displays text which the user must accept before being able to change the password and also enforces the rules defined in the rules file. It is installed on user workstations.

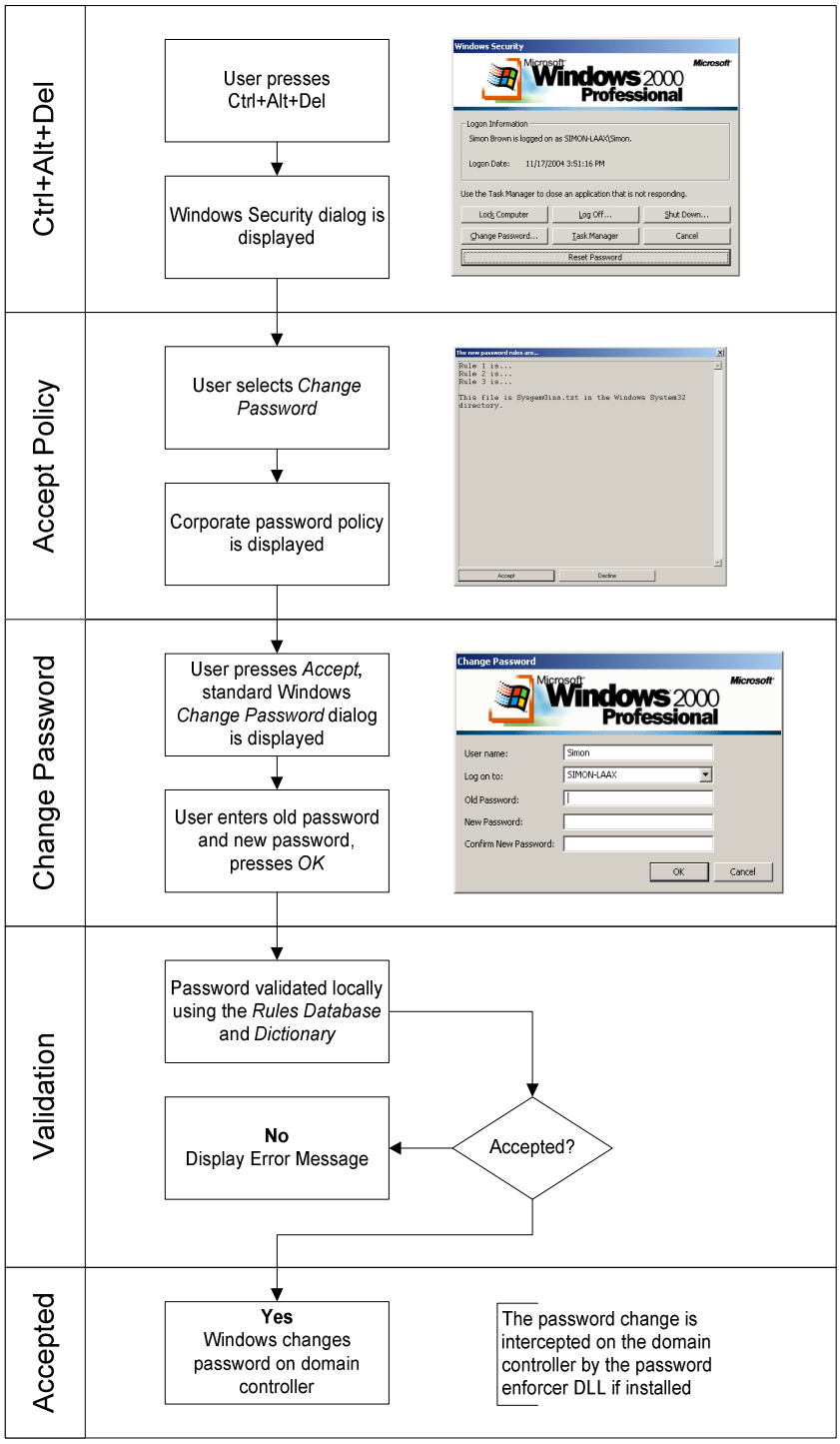
   The text is displayed in a small popup window when the user presses Ctrl+Alt+Del and selects Change Password.
2. A password change DLL which is installed on domain controllers and intercepts all password change requests. The password filter enforces the rules defined in the rules file, it is installed on domain controllers.

Both of these components provide *independent* password enforcement.

Workstation

The workflow on the workstation is shown below. The SysgemGINA.dll is responsible for this processing. The DLL knows both the old and new passwords so it is able make comparisons.

The DLL on the domain controller has no knowledge of the old password.



Domain Controller

The password change DLL SEMPwdEnforcer.dll uses the Windows PasswordFilter function which is supported by Windows password filters.

Password filters are used to enforce password policy. Filters validate new passwords and indicate if the new password conforms to the implemented password policy.

The password is validated using the *Rules Database* and the *Dictionary*.

Unlike the checks made using the workstation components the password filter DLL only knows about the new password so it is not possible to compare the old and new password.

Rules File

The rules file is SEMPwdEnforcerRules.txt located in the Windows System32 folder. It is used by both workstation and domain controller components.

The domain controller code does not know about the old password so it is unable to make comparisons, for example *Maximum consecutive characters also in old password*.

The supported rules are:

Rule	Description
ACTIVE	If set to 1 then the rules checking is activated
DICTIONARY	If set to 1 then the dictionary checking is enabled
MIN_INIT_ALPHA	Minimum initial alphabetic characters
MIN_INIT_DIGIT	Minimum initial digits
MIN_ALPHA	Minimum alphabetic characters
MAX_ALPHA	Maximum alphabetic characters
MIN_DIGIT	Minimum digits
MAX_DIGIT	Maximum digits
MIN_LOWER	Minimum lowercase characters
MAX_LOWER	Maximum lowercase characters
MIN_UPPER	Minimum uppercase characters
MAX_UPPER	Maximum uppercase characters
ALLOW_MIXED_CASE	Allow mixed case characters
MIN_SPECIAL	Minimum special characters
MAX_SPECIAL	Maximum special characters
MIN_UNQIUE	Minimum unique characters
MAX_UNQIUE	Maximum unique characters
MIN_LENGTH	Minimum password length
MAX_LENGTH	Maximum password length
MAX_CONSEC_OLD_PWD_FWD	Maximum consecutive characters also in old password
MAX_CONSEC_OLD_PWD_REV	Maximum consecutive characters also in reversed password
MAX_CONSEC_USERNAME_FWD	Maximum consecutive characters also in username
MAX_CONSEC_USERNAME_REV	Maximum consecutive characters also in reversed username
MAX_CONSEC_FULLNAME_FWD	Maximum consecutive characters also in full name
MAX_CONSEC_FULLNAME_REV	Maximum consecutive characters also in reversed full name

A sample rules file is shown below.

```
#
#   SEM Password Enforcer rules.
```

```
#
#   Note: the old password is only available for comparison if the
#   user is changing the account's password and entering 'Old
password'
#   and 'New password'.
#
#   If the password is being changed by an account management
program
#   such as the Windows User Manager then the old password is an
#   empty zero-length string.
#

#
#   Set TRACE to 1 for exhaustive logfile information.
#
ACTIVE     1
TRACE      0
DICTIONARY 1

#
#   The options are:
#
#   ACTIVE                      Is active
#   TRACE                       Display more information in the
logfile
#   DICTIONARY                  User the dictionary file
#   MIN_ALPHA                   Minimum alphabetic characters
#   MAX_ALPHA                   Maximum alphabetic characters
#   MIN_DIGIT                   Minimum digits
#   MAX_DIGIT                   Maximum digits
#   MIN_LOWER                   Minimum lowercase characters
#   MAX_LOWER                   Maximum lowercase characters
#   MIN_UPPER                   Minimum uppercase characters
#   MAX_UPPER                   Maximum uppercase characters
#   ALLOW_MIXED_CASE            Allow mixed case characters
#   MIN_SPECIAL                 Minimum special characters
#   MAX_SPECIAL                 Maximum special characters
#   MIN_UNQIUE                  Minimum unique characters
#   MAX_UNQIUE                  Maximum unique characters
#   MIN_LENGTH                  Minimum password length
#   MAX_LENGTH                  Maximum password length
#   MAX_CONSEC_OLD_PWD_FWD      Maximum consecutive characters also
in old password
#   MAX_CONSEC_OLD_PWD_REV      Maximum consecutive characters also
in reversed password
#   MAX_CONSEC_USERNAME_FWD     Maximum consecutive characters also
in username
#   MAX_CONSEC_USERNAME_REV     Maximum consecutive characters also
in reversed username
#   MAX_CONSEC_FULLNAME_FWD     Maximum consecutive characters also
in full name
#   MAX_CONSEC_FULLNAME_REV     Maximum consecutive characters also
in reversed full name
#
#   Rules file ..: SEMPwdEnforcerRules.txt      in the System32
directory.
#   Dictionary ..: SEMPwdEnforcerDictionary.txt in the System32
directory.
#   Log file ....: SEMPwdEnforcerRules.log      in the System32
directory.
#
#   To use an alternate directory for the logfile add the token
LOGDIR
#
#   For example: LOGDIR D:\PwdEnf\Logs
#
#   The directory must exist. If the logfile cannot be created in
this directory
#   then System32 will be used.
#
MIN_ALPHA 4
MAX_ALPHA 20

MIN_DIGIT 2
MAX_DIGIT 3
```

Dictionary

The dictionary is used to exclude passwords. Checking is case-insensitive, the * wildcard may be used at the start of end of an entry to match any number of characters.

For example *hard* matches **hard**, c**hard**, **hard**y, **hard**ly and c**hard**y.

To enable the dictionary you must enable the DICTIONARY rule.

An except from a dictionary file is shown below.

```
1*
2*
3*
4*
5*
6*
7*
8*
9*
0*
-----a-----
abc*
*accord*
*account*
*admin*
*agenda*
*ajax*
*alex*
*alfa*
*akzo*
*anna*
*anne*
*appel*
*apple*
*arian*
*asdfgh*
*audi*
*austin*
*azerty*
-----b-----
*banaan*
*bart*
bas*
*belgi*
ben*
bert*
bloem*
*bmw*
*brava*
*bravo*
```

Reset Password

Overview

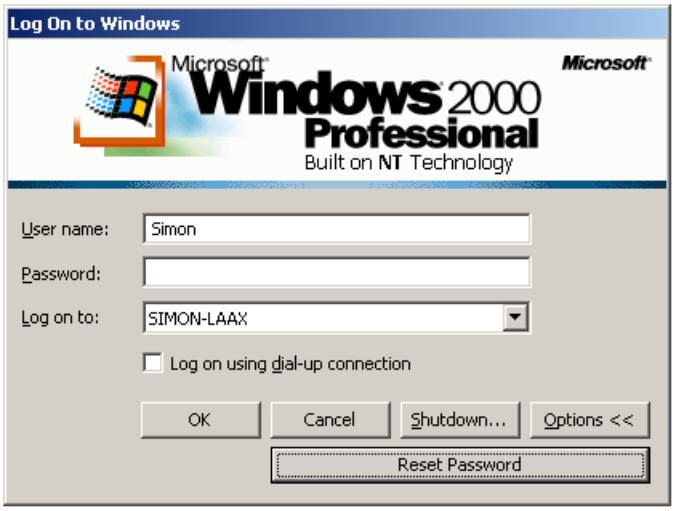
The reset password technology allows an employee to reset a Windows password from a secure attention sequence (SAS) window.

SAS: A key sequence that begins the process of logging on or off. The default sequence is Ctrl+Alt+Del.

Workstation

Starting

To start the reset password software press Ctrl+Alt+Del. One of the two SAS windows shown below is displayed depending on whether you are currently logged on:



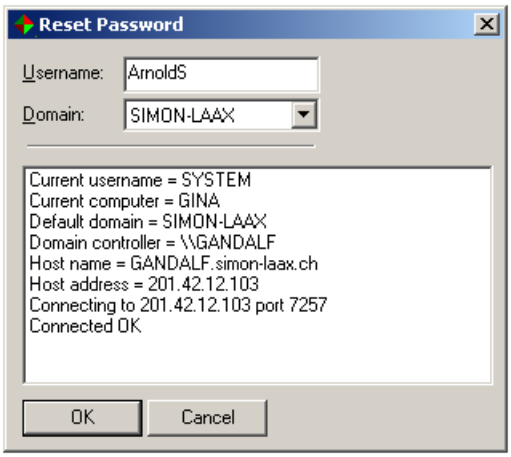
The standard logon window.

The window displayed by pressing Ctrl+Alt+Del while logged-on.

In both windows you see the *Reset Password* button added by the Sysgem WinLogon GINA.

Reset Password Window

When the users presses see the *Reset Password* button the Reset Password window is displayed:

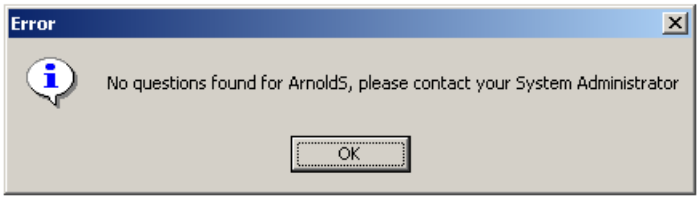


In the status window you see information about the computer and the default domain.

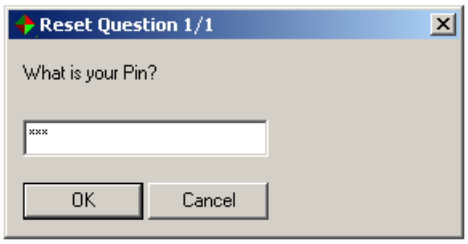
Enter the username of the account for which a new password is required, then press *OK*.

Q & A

If the Question and Answer entries are not defined in the central server database an error message is displayed:



If an error is not displayed you are prompted with the questions previously defined for the *ArnoldS* account. For this example there is only one question, the corporate badge number or *Pin*.



Enter the correct answer, then press *OK*.

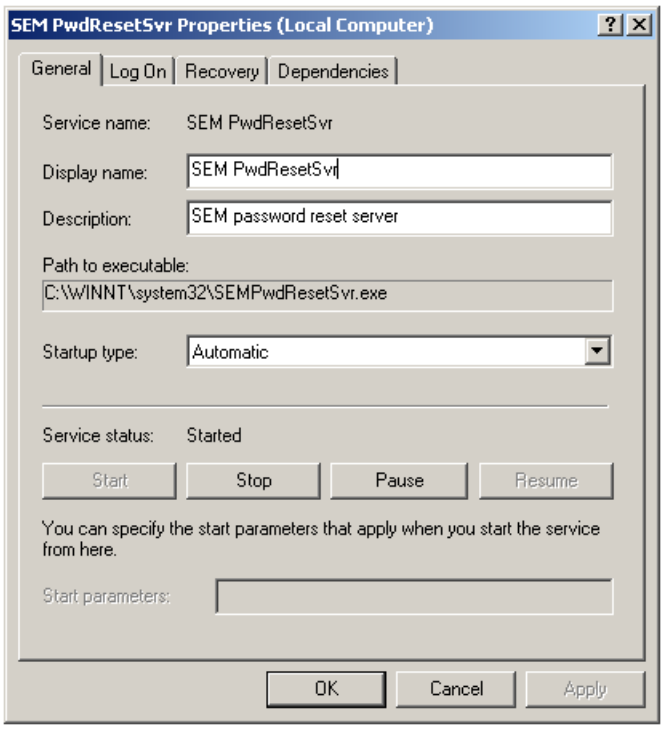
New Password

When all questions have been answered correctly the New Password window is displayed. Here you enter the new password for the *ArnoldS* account, then press *OK*.

If the password meets your corporate password policy the *ArnoldS* account is updated with the new password.

Domain Controller

A service is installed on the domain controller which processes requests from the workstation.



The service uses the database SEMPwdResetSvr.txt located in the Windows System32 folder.

An example with just a single entry for ArnoldS:

```
#++
#
#   SEM Password Reset database
#   ---------------------------
#
#   Format of each entry:
#
#       Username<tab>Question<tab>Answer
#       Answer may be plain text or an MD5 checksum.
#
#
#   Maximum of five questions per username.
#
#--
#
ArnoldS         What is your Pin?      666
ArnoldS         What is your dog's name?      Fido
ArnoldS         What is your Favourite colour?       Green
```

The answers are either plain text (not recommended except for testing) or as a MD5 checksum.

When the workstation connects to the service the database file is loaded and the questions and answers are returned.

When the user has correctly answered the questions and requests a new password the service checks that password meets the corporate password policy and if it does it sets the new password.

Installing

Overview

The components are installed with a standard kit.

Installation Details

Overview

The software is packaged in a standard installation kit.

This chapter also describes the manual installation of the various components for your reference as it is important that you understand exactly what happens during the installation.

WinLogon Gina DLL

(From MSDN, copyright Microsoft)

The GINA is a replaceable DLL component that is loaded by Winlogon. The GINA implements the authentication policy of the interactive logon model, and is expected to perform all identification and authentication user interactions. For example, replacement GINA DLLs can implement smart-card, retinal-scan, or other authentication mechanisms in place of the standard Windows NT/Windows 2000 user name and password authentication.

The GINA displays text which the user must accept before being able to change the password and also enforces the rules defined in the rules file. It is installed on user workstations.

- GINA: SysgemGina.dll,
- Text: SysgemGina.Txt.

Both files are installed in the Windows System32 folder.

Enable

To enable the Sysgem GINA modify the registry:

- Key: HKEY_LOCAL_MACHINE
  Software
  Microsoft
  Windows NT
  CurrentVersion
  Winlogon
- Value name: GinaDLL
- Value type: [REG_SZ]
- Value data: SysgemGina.dll

then restart Windows.

Be careful when editing the registry – if you enter the name of a DLL which does not exist in the Value data (above) then you will be unable to login to your computer after you restart.

Change / Remove

To change or remove the file you must either:

Delete the GinaDLL value from the registry then restart Windows, or

Change the name of the dll and the GinaDLL value, for example from SysgemGina.dll to SysgemGina002.dll.

Be careful when editing the registry – if you enter the name of a DLL which does not exist in the Value data (above) then you will be unable to login to your computer after you restart.

Password Filter DLL

(From MSDN, copyright Microsoft)

A DLL that provides password policy enforcement and change notification. The functions implemented by password filters are called by the Local Security Authority.

Password notification and filtering only take place on the computer that houses the updated account. Notification on domain accounts only takes place on the primary domain Controller for the Windows NT 4.0 domains. In addition to the primary domain Controller, the password filter packages should be installed on all backup domain Controllers to allow notifications to continue in the event of server role changes.

On Windows 2000, all domain Controllers are writeable, therefore the interceptor must be present on all domain Controllers.

The interceptor functions run in the security context of the local system account.

The password filter enforces the rules defined in the rules file, it is installed on domain controllers.

- File: SEMPwdEnforcer.dll

Enable

The Password Filter DLL is enabled by updating the following registry key in the Windows NT Registry. If Notification Packages exist, the name of the DLL is added to the existing value (existing values may not be overwritten).

- Key: HKEY_LOCAL_MACHINE
  SYSTEM
  CurrentControlSet
  Control\Lsa
- Value name: Notification Packages
- Value type: REG_MULTI_SZ

Add SEMPwdEnforcer to Notification Packages. After updating the registry the system must be rebooted.

Change / Remove

To change or remove the file you must either:

- Remove SEMPwdEnforcer value from the Notification Packages registry entry then restart Windows, or
- Change the name of the dll and the Notification Packages value, for example from SEMPwdEnforcer.dll to SysgemGina002.dll.

Do NOT delete the Notification Packages entry from the registry unless SEMPwdEnforcer is the only entry, otherwise you will compromise your system's security.

Support Files

All files are located in the System32 directory.

- SysgemGina.Txt - contains the accept /decline text used by the GINA.
- SEMPwdEnforcerRules.txt - the enforcer rules file.
- SEMPwdEnforcerDictionary.txt - the enforcer dictionary file.