SAcM Password Synchronizer

User Guide

By Sysgem AG

June 16, 2005

Contents

Overview 1

Topology 1
Components 3
SAcM Password Synchronizer End-User Components 3
SAcM Password Synchronizer Controller 5
SEM Agents 5
Summary 6

Quick Start 7

Overview 7
Kits 7
Steps 7
Installation 7
Configuration 8

Installation 9

SAcM Password Synchronizer 9
Windows 9
SEM Agents 15
Windows 15
UNIX/Linux 20
OpenVMS 25

Controller Interface 31

Starting 31
Options 32
Settings 33
Scripts – Common 33
Scripts – Custom 33
Scripts – Executable 34
Scripts – Main 34
Scripts – Validation 35

Controller Server 37

Overview 37

Controller Database 39

Introduction 39
Multiple Controllers 39
Changes 39
Agent Definitions 39
Starting 40
Add Agent Definition 40

Import Agent Definitions from SEM....41
Add Group Definition....42
Rules Definitions....43
Starting....45
Add....45
Examples....46

Console **49**

Overview....49
Configuration File....49

Windows Interceptor **51**

Overview....51
Logfile....52
Configuring....52

OpenVMS Interceptor **55**

Overview....55
Testing....55
Customizing....55

Examples **57**

Introduction....57
Controller Not Found....57
Password Validation Error....58
Rule Not Found....58
Target Agent Not Reachable....59
Target Account Not Found....60
Target Account Updated....60
OpenVMS Interceptor....62
Full Logging....62

Message Flow **65**

Console....65
Old Password....66
New Password....67
Password Distribution....68
Interceptor....69

Testing **71**

Overview....71

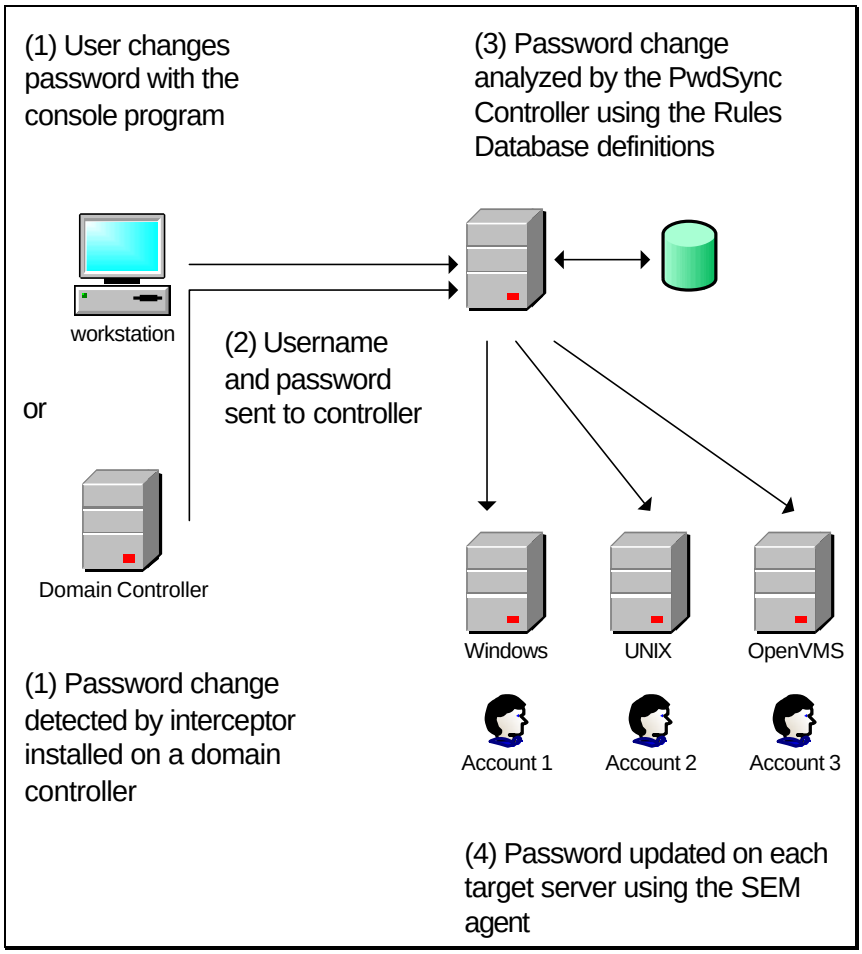
Change Log **73**

2004....73
2005....73

Overview

Topology

The following diagram gives an overview of the SAcM Password Synchronizer:



(1) An end-user changes their password on their login machine. They use either the Password Synchronizer *'Console'* program from Sysgem to change their password, or they use the standard operating system procedures and let the Password Synchronizer *'intercept'* the password change.

(2) New passwords are sent to the SAcM Password Synchronizer *Controller* which (3) checks the *Rules Database* to determine whether each new password should be distributed, and if so to which target systems it should be sent.

All network traffic is heavily encrypted to ensure that passwords cannot be detected by network monitoring devices.

(4) The *Controller* sends new passwords to the *SEM Agents* running on the target systems and the password is updated for:

- the appropriate operating system accounts on those systems,
- optional third-party application accounts such as ORACLE or MySQL.

(SEM Agents are part of the System Enterprise Manager and are installed using the platform-dependent kit.)

Components

There are three components that need to be installed on different systems:

- *SAcM Password Synchronizer End-User Components* (Interceptors, Console)

  where the end-users change their password.

- *SAcM Password Synchronizer Controller*

  on at least one Windows system used for password distribution.

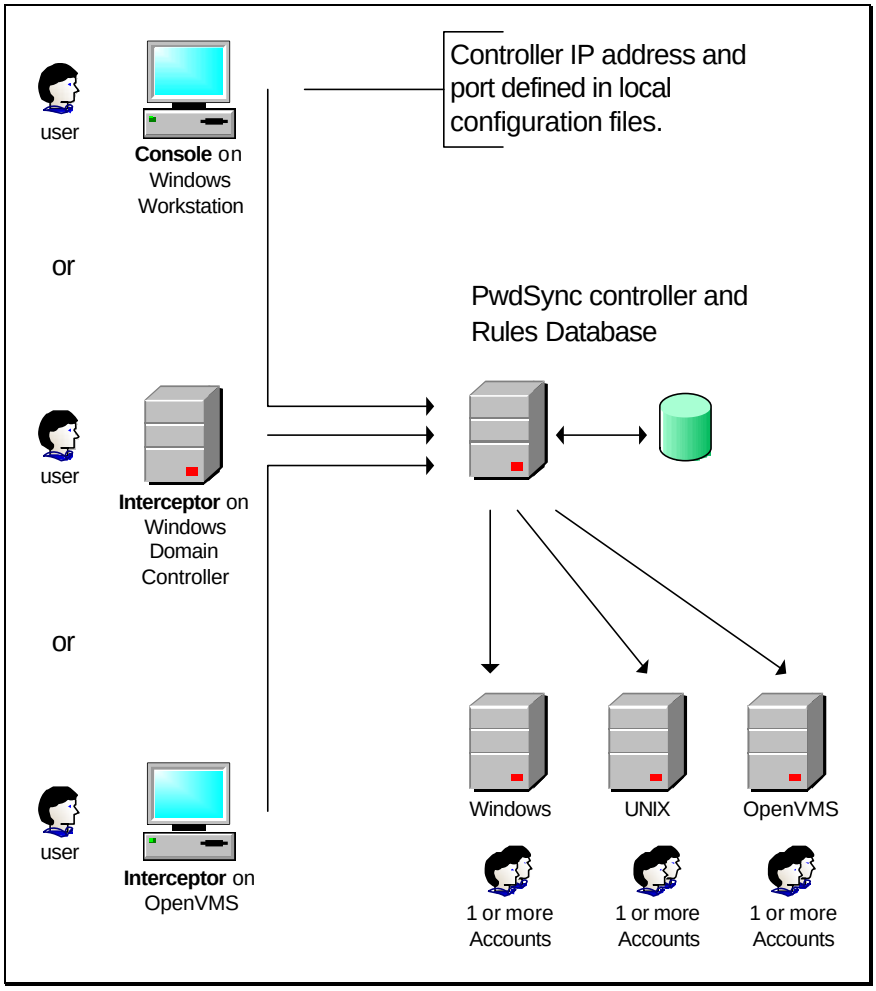
- *SEM Agents*

  where the end-user passwords are to be changed by the password synchronizer controller.

SAcM Password Synchronizer End-User Components

End-User Components consist of the SAcM Password Synchronizer *Console* and the SAcM Password Synchronizer *Interceptor*:

- The *Console* is a Sysgem-provided program that provides a command line prompt for a new password. It first changes the user's password in their local account and then sends the new password to the SAcM Password Synchronizer *Controller*.
- The *Interceptor* is a Sysgem-provided program that 'listens' for passwords being changed by the normal operating system procedures and sends the new password to the SAcM Password Synchronizer *Controller*.



Interceptors are currently available for the Windows XP/2000/NT and for the OpenVMS platforms. On OpenVMS they intercept password changes only when a user is forced to change an expired password during login.

The *Interceptor* and *Console* have configuration files that identify the location of the SAcM Password Synchronizer Controllers. If a Controller is unavailable for any reason, then the next one in sequence will be used.

On systems where the user will change passwords you install:

- Interceptor (Windows and OpenVMS only): to intercept a password that has been changed with the normal operating system procedure.
- Console programs (all platforms): a Sysgem program that prompts a user for a new password.

In Windows domains a domain password is changed on the Domain Controllers. Passwords used in Windows workgroups are local account passwords and are changed on the user's own workstation.

The normal use of Password Synchronizer is to intercept domain passwords and therefore the Interceptor is normally installed on all Domain Controllers. In an NT 4 domain install the Interceptor on the Primary Domain Controller (PDC). You may also install it on Backup Domain Controllers in case those should ever be promoted to a PDC.

SAcM Password Synchronizer Controller

The Password Synchronization Controller is installed on one or more Windows systems (workstation or server). It receives new passwords from the End-User Components and forwards them to target systems in accordance with the rules in a Rules Database. It should be installed on Windows Servers that are normally always available.

There are two parts to the controller:

1. a Windows service *SEM Password Synchronization Controller* and
2. a *Controller Interface*.

The service runs all the time, you use the controller interface to configure the service, display logfiles etc.

The interceptors are configured with a list of controllers to which password changes are sent. The interceptor tries each controller in turn until one is found which accepts the password change information.

The interceptor then remembers the controller which accepted the message and tries this one first when the next message is sent.

SEM Agents

System Enterprise Manager (SEM) agents are used as part of a SAcM Password Synchronizer installation to update the user accounts on the target systems.

These SEM agents must be installed on all the target systems where the passwords are to be updated.

The SEM Agents are installed using the standard SEM agent kit for the respective platforms.

Summary

The SAcM Password Synchronizer components can be summarized as follows:

Available Platform	Component	Description
Windows	Interceptor	This intercepts password changes made using any Windows program and forwards the new passwords to the Controller. It comprises of a DLL in the System32 directory that is called when a user changes a password. This must be installed on the system where the password is located; if in a domain then this is the PDC and BDC – all domain controllers.
OpenVMS	Interceptor	This intercepts password changes using LOGINOUT and forwards the new passwords to the Controller. A shareable image that uses the LOGINOUT (LGI) routines as described in the COMPAQ OpenVMS Utility Routines Manual to support a custom login program.
Windows	Controller	The program that receives password change requests processes them and distributes the changed password. Installed on one or more secure Windows systems. These do not have to be the Domain Controllers but usually are. The interceptor attempts to send the requests to each Controller in turn until an available Controller is found. There are two parts to the controller: a Windows service *SEM Password Synchronization Controller* and a *Controller Interface*. The service runs all the time, you use the controller interface to configure the service, display logfiles etc.
Windows UNIX OpenVMS	Console	A small utility program with which the user requests a change of password. The Console communicates directly with the Controller.

Quick Start

Overview

Kits

The kits you need are:

- **S**ysgem **P**assword **S**ynchronizer (SPS), and
- **S**ysgem **E**nterprise **M**anager (SEM) - specifically the platform-specific agents.

These are two separate kits, obtainable from you reseller or downloadable from Sysgem's website http://www.sysgem.com/ .

Kits requires a password to proceed with the installation, passwords are available from your reseller or Sysgem support mailto:support@sysgem.com .

Steps

To implement the Password Synchronizer in your environment you:

1. Install the Sysgem Password Synchronizer (SPS) components on the systems:
    a. Where the users change their passwords (Interceptors on domain controllers, Console on workstations). When you install the Interceptor a reboot will be required.
    b. Where the password will be distributed (Controllers, usually on domain controllers or other servers).
2. Install SEM Agents on the systems where the new password will be updated by the SPS controller.

A typical topology is shown on page 1.

Installation

Installation of SPS.

1. Install the *SPS Controller* on the high-reliability secure systems you will use for password distribution. The SPS Controller receives change requests and distributes them through your network to SEM Agents which update passwords.

2. Install the *SPS Interceptors* on the computers where users will change their passwords, for Windows this will be all domain controllers.
3. Optionally install the *SPS Console* on the computers where users are to change their password from the command line (DOS, terminal window).

Installation of SEM Agents. This is a standard installation, no special options are required. You should be familiar with SEM – if not please contact your reseller or Sysgem support.

1. Install the *SEM Agents* on the computers where the password will be updated by the SPS Controller(s).

Configuration

After installing SPS and the SEM agents you must define the Controller Database (page 39) which contains Agent definitions (page 39) and Rules (page 43).

Installation

SAcM Password Synchronizer

Windows

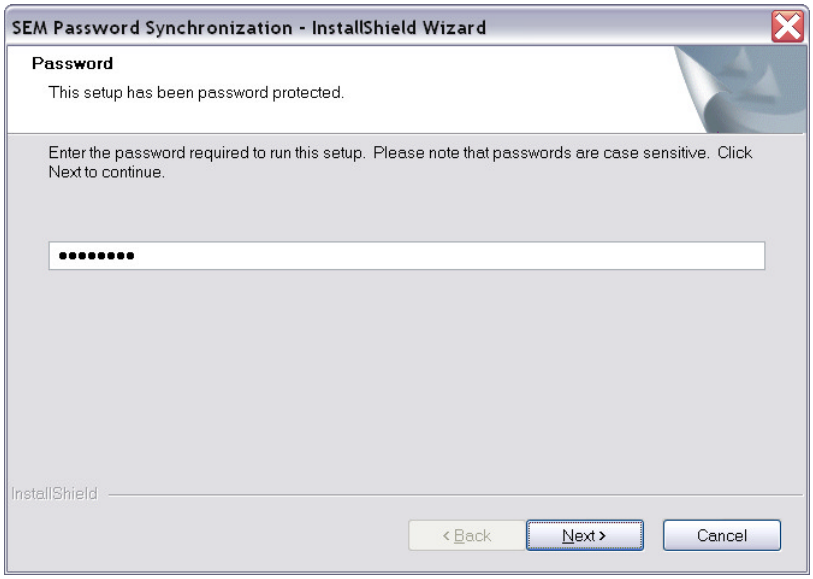
The Windows kit is SYSGEMiPwdSync.exe, if you have downloaded from the web it will be part of the PwdSyncAllKits_Build<nnnn>.zip archive where <nnnn> is the build number, for example 2619.

Before starting the installation you should plan where you will install the various components, refer to page 1 of this guide for more information

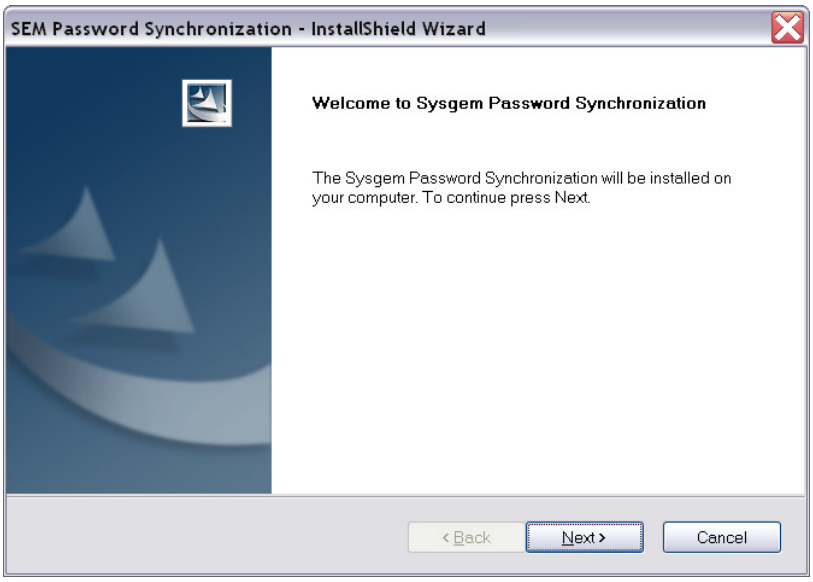
Password

When you start the installation you are prompted for the password. If you do not have a password contact your distributor of Sysgem AG.

The standard password is **Fort GT40** but this may change in future releases.

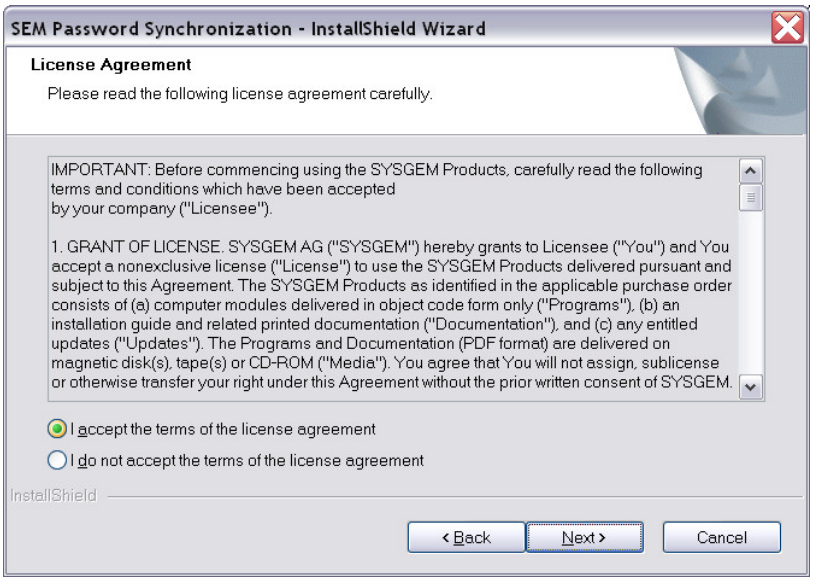


Welcome



A greeting from the development team. Press *Next* to continue.

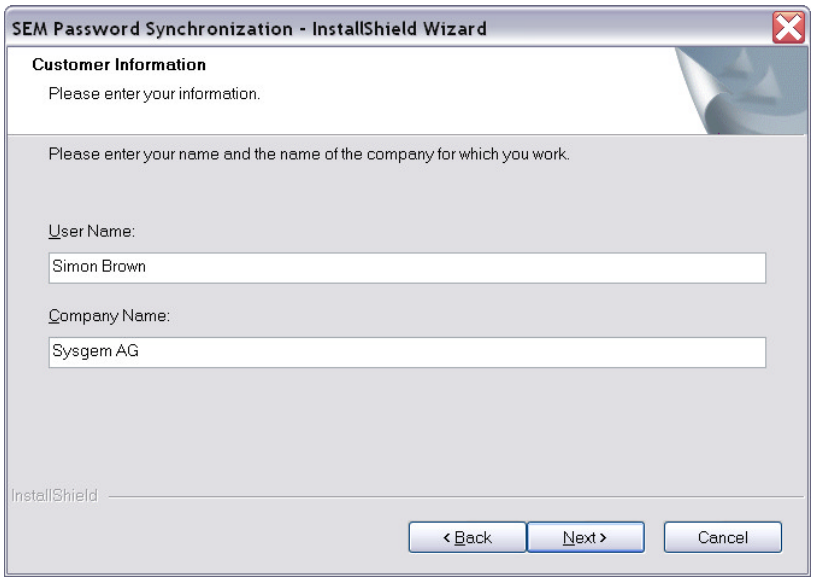
License Agreement



Displays a dialog box containing a license agreement. You can scroll up and down to read the agreement, then must choose either *I accept…*, *I do not accept…*, or the *Back* button. If you select *I accept…*, Setup will continue. If you select *I do not accept…*, Setup will display the Exit Setup dialog.

Read the license agreement carefully, then press *Next* to continue.

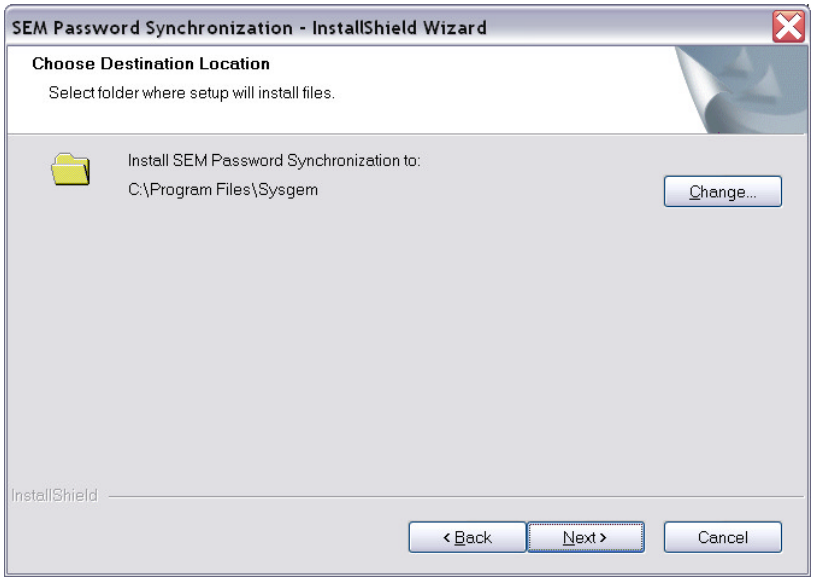
Customer Information



Displays a dialog box that retrieves the user name and company name. Setup obtains the user name and company name from the registry. The Next button becomes enabled only when data exists in both edit fields. If Setup can locate default name and company values from the system, the Next button is automatically enabled.

Enter your name and the name of the company you work for, then press *Next* to continue.

Destination Location



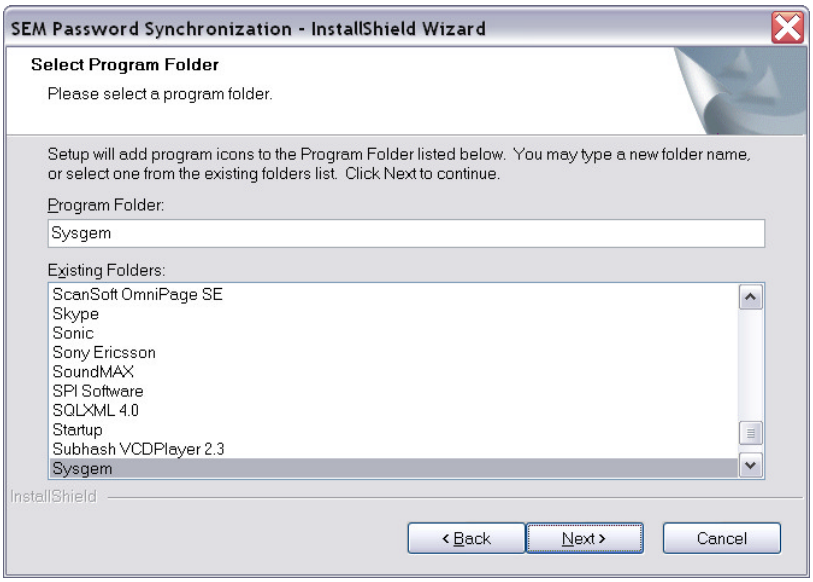
Displays a dialog box that allows you to select an alternate destination path. When you click the Browse button in that dialog box, the Choose Folder window is called to open a second dialog box that enables you to either select an existing folder or to enter a new folder name.

If you enter the name of a folder that does not exist, a message box is displayed asking whether to create a folder with that name. If you select yes, the specified directory is created.

If the default folder does not already exist on your system, it will not be created unless you press the Browse button and follow the steps to create it from the Choose Folder dialog box.

Select the folder where the files will be installed, then press *Next* to continue.

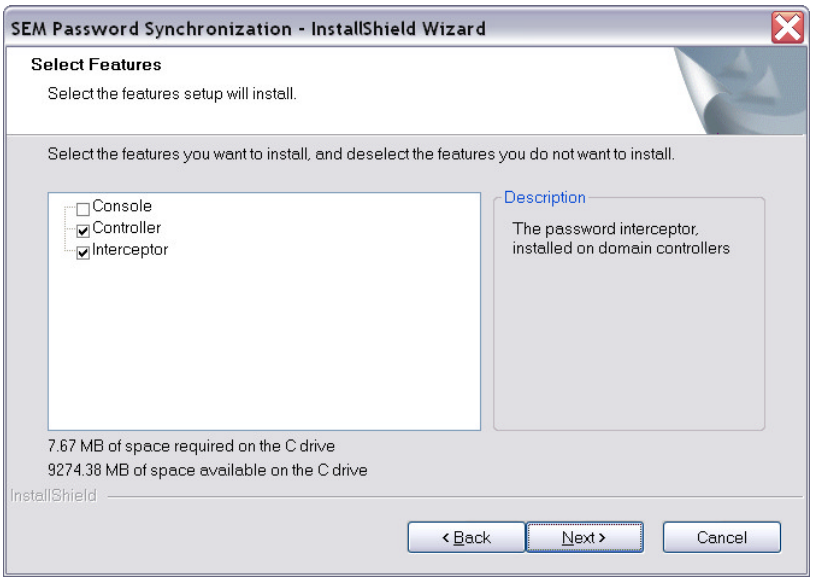
Program Folder



Displays Start menu program folders for selection. The default folder is SYSGEM. You can also enter a new folder name.

Select the program folder where the startup icons will be added, then press *Next* to continue.

Select Features



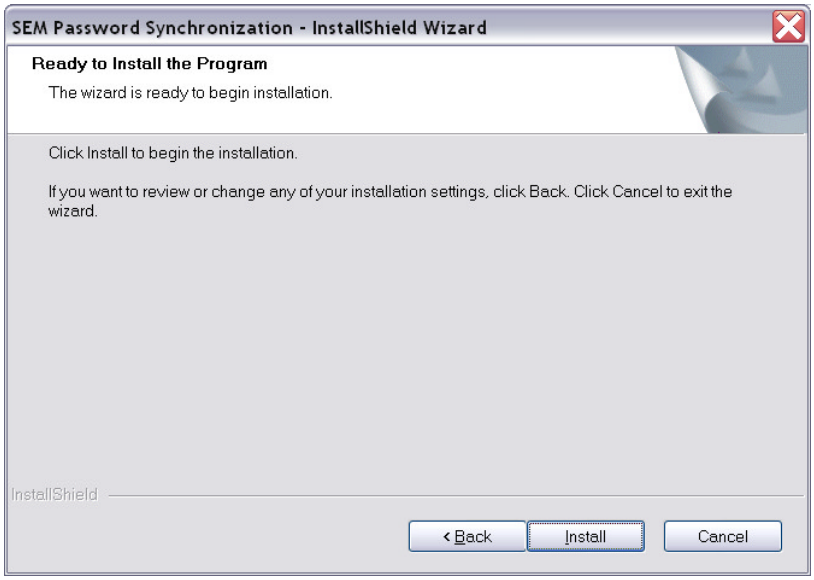
The *Console* program is an optional command-line (DOS) program which prompts for a new password. Install on a user's workstation.

The *Interceptor* 'listens' for passwords being changed by the normal operating system procedures, it is installed on all domain controllers (which is where the password is actually changed).

The *Controller* is installed on one or more Windows systems (workstation or server), usually Windows servers that are normally always available.

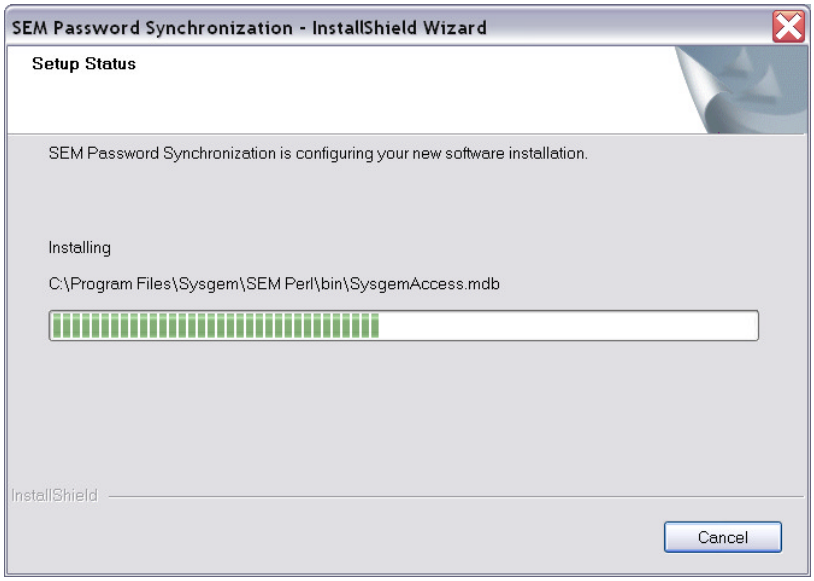
Select the features to install, press *Next* to continue.

Ready To Install



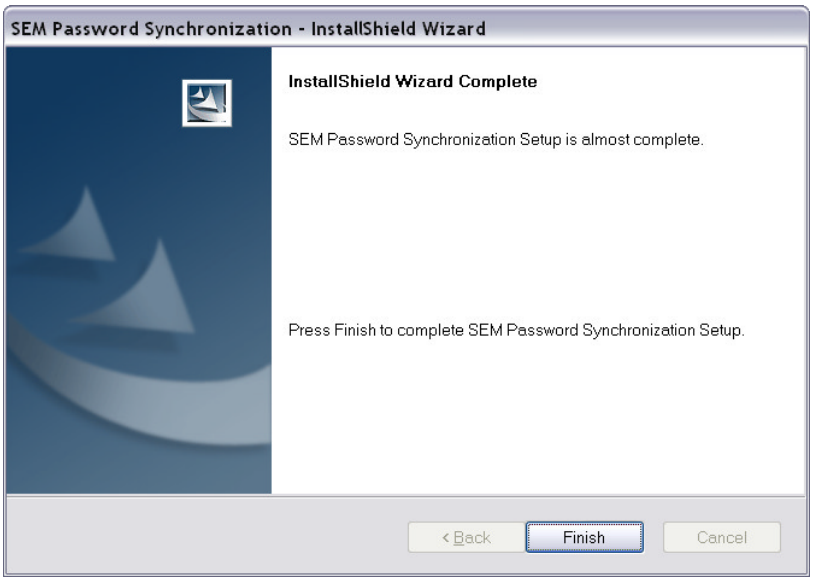
If you are ready to start the installation press *Install*.

Setup Status



While the software is being installed the Setup Status is displayed.

Completed



Press *Finish* to complete the setup.

SEM Agents

Windows

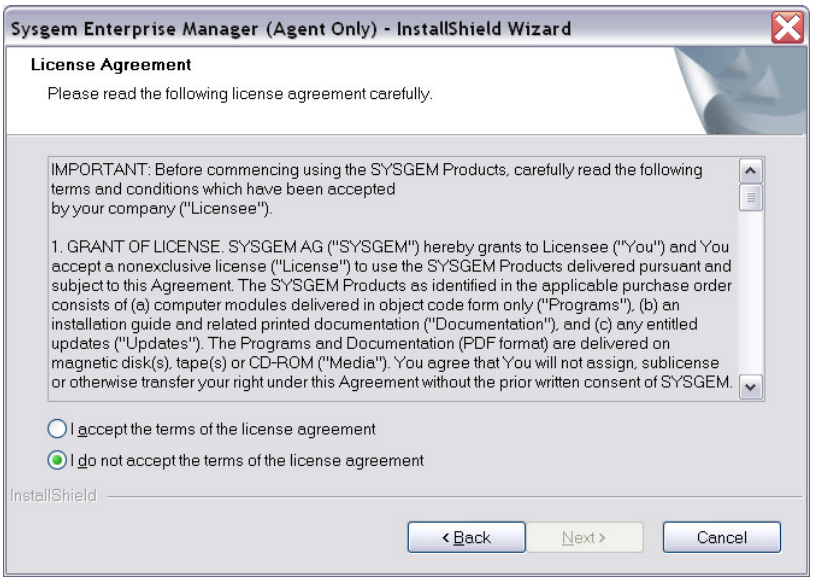
The Windows kit is SYSGEMiWindowsNTAgent_Build<nnnn>.exe where <nnnn> is the build number, for example 2610.

This kit is derived from the standard SEM Windows kit, it is *not* password-protected.

Welcome

Displays a dialog box that welcomes the end user. Press *Next* to continue.

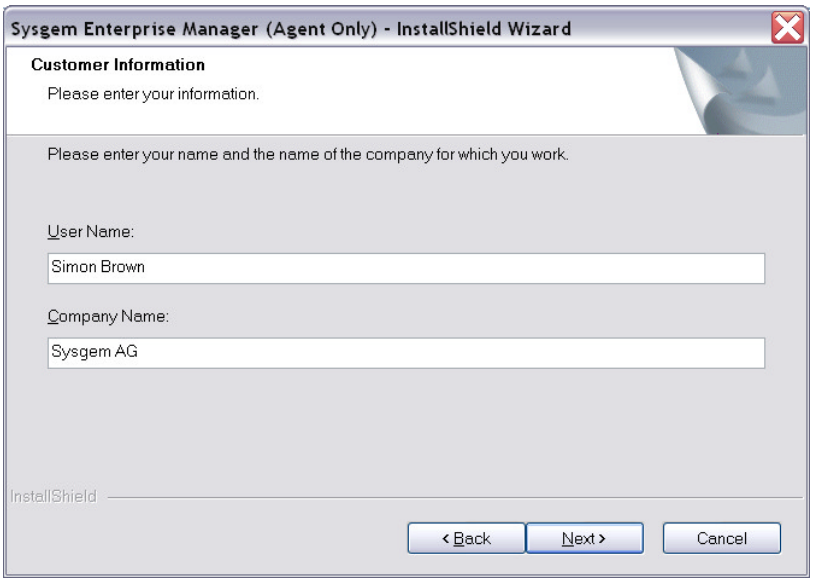
License Agreement



Displays a dialog box containing a license agreement. You can scroll up and down to read the agreement, then must choose either *I accept…*, *I do not accept…*, or the *Back* button. If you select *I accept…*, Setup will continue. If you select *I do not accept…*, Setup will display the Exit Setup dialog.

Read the license agreement carefully, then press *Next* to continue.

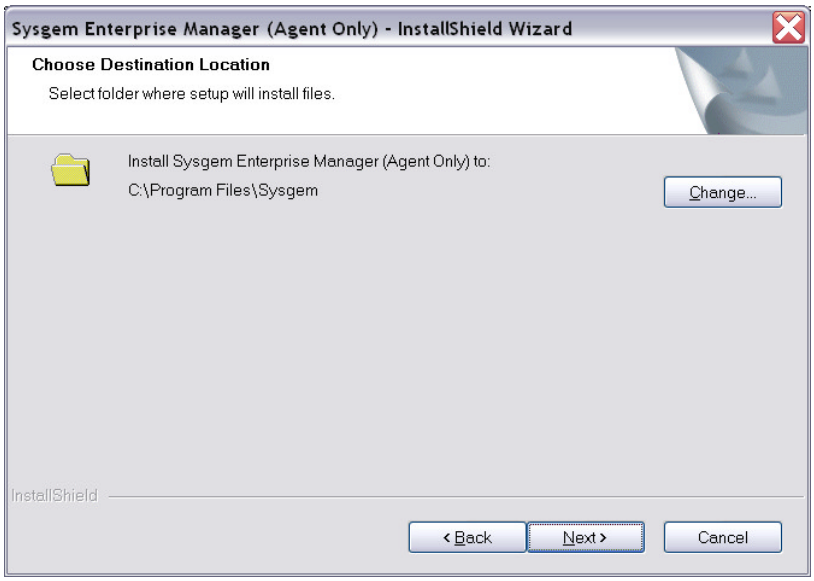
Customer Information



Displays a dialog box that retrieves the user name and company name. Setup obtains the user name and company name from the registry. The Next button becomes enabled only when data exists in both edit fields. If Setup can locate default name and company values from the system, the Next button is automatically enabled.

Enter your name and the name of the company you work for, then press *Next* to continue.

Destination Location



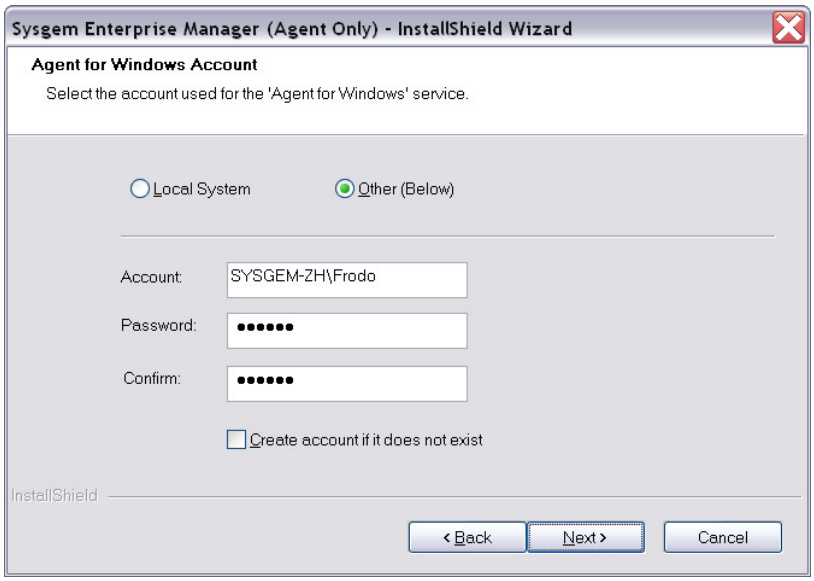
Displays a dialog box that allows you to select an alternate destination path. When you click the Browse button in that dialog box, the Choose Folder window is called to open a second dialog box that enables you to either select an existing folder or to enter a new folder name.

If you enter the name of a folder that does not exist, a message box is displayed asking whether to create a folder with that name. If you select yes, the specified directory is created.

If the default folder does not already exist on your system, it will not be created unless you press the Browse button and follow the steps to create it from the Choose Folder dialog box.

Select the folder where the files will be installed, then press *Next* to continue.

Agent for Windows Account



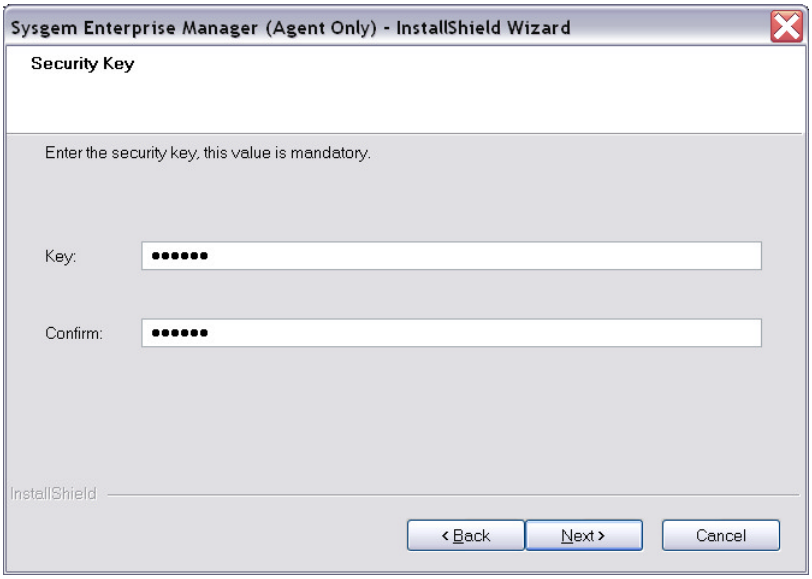
To correctly create an account the agents requires the privileges normally granted to members of the Administrators group.

Enter the account and password, then press *Next* to continue.

Agent for Windows Port

Enter the port number, the default is 7251.

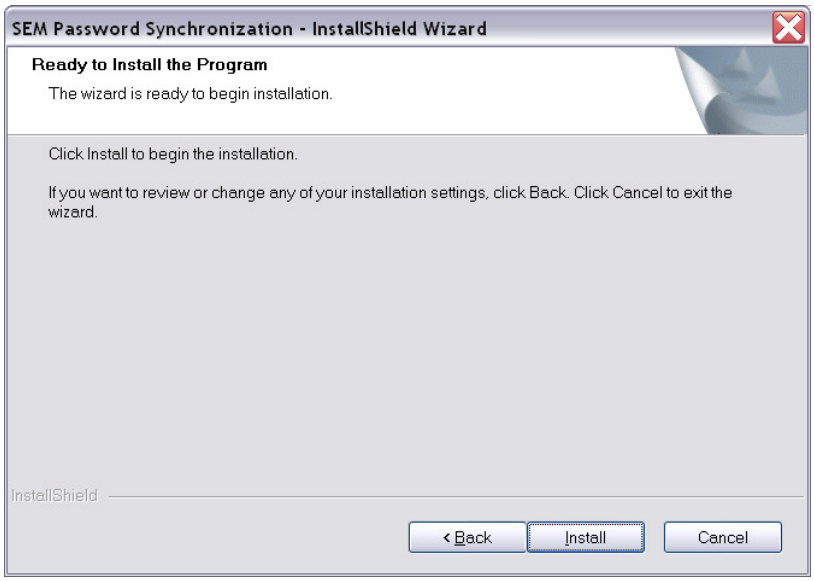
Security Key



The SEM components use a Security Key to protect the system from unauthorized components being introduced into the network.

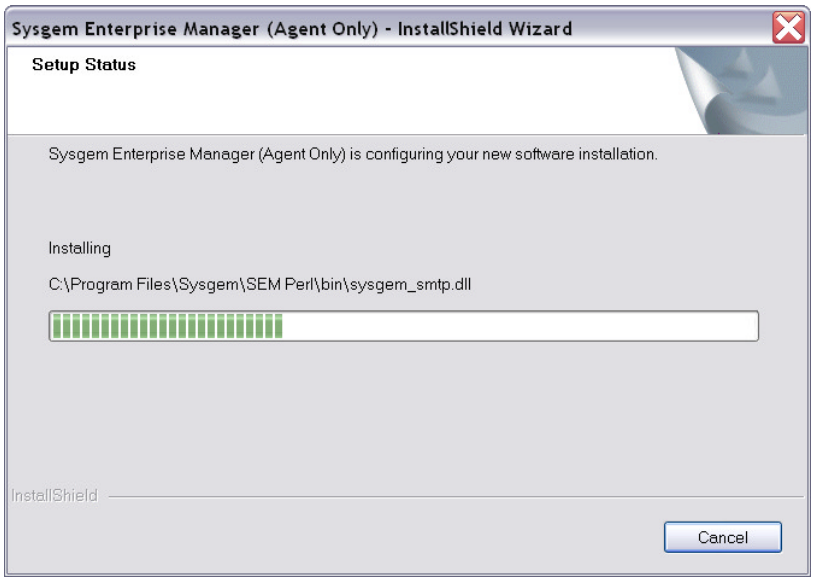
Enter the mandatory security key, then press *Next* to continue.

Ready To Install



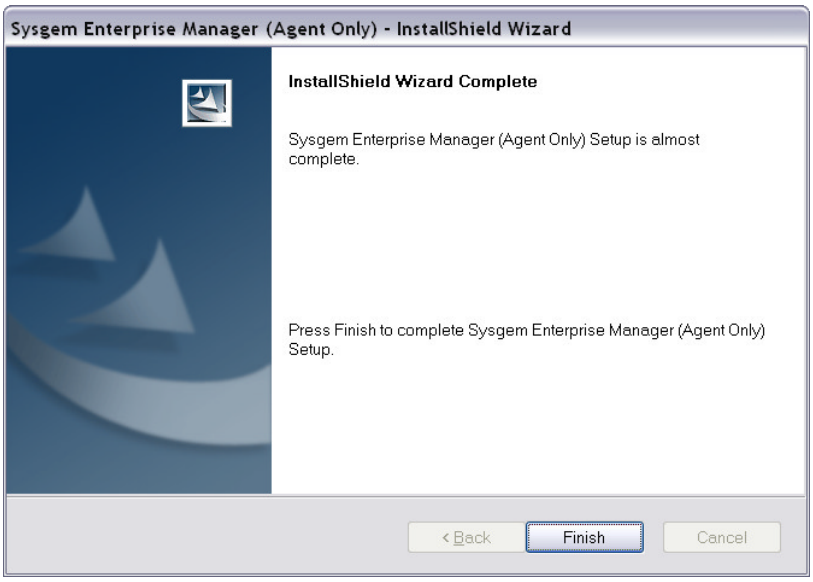
If you are ready to start the installation press *Install*.

Setup Status



While the software is being installed the Setup Status is displayed.

Completed



Press *Finish* to complete the setup.

UNIX/Linux

Introduction

Sysgem provide a common installation procedure for all UNIX/Linux platforms supported by Sysgem Enterprise Manager.

First, to install the SEM Agent on Unix/Linux systems, you need to be logged into a privileged account, such as root.

You will then need to decompress the tar archive containing the installation kit. It is suggested that a special directory is created for this purpose.

Invoke the installation procedure by running the “setup” program unpacked from the above tar file:

```
#./setup
```

The installation procedure prompts for the following information:

- The location to install the agent, is by default the following: /opt/Sysgem/SEM.
- The TCP/IP port number. By default this will be 7251. It should only need to be changed if 7251 clashes with one already in use.
- A security key. This must be the same key used for all other components on your network. It is a free-format text phrase that (similar to a password) is defined by you during the installation. It can be changed later if required. The example below uses a text phrase of “FortKnox”.
- Whether to start the Agent automatically on reboot.
- Whether to start the Agent automatically on completion of the installation.

An example is given below showing a typical installation on a Compaq Tru64 machine.

To re-install the kit, perhaps as an upgrade for a later version, simply re-run the above procedure. There is no need to stop any daemons as these will be stopped and restarted automatically during the installation.

If you have any suggestions for improving the UNIX installation of Sysgem Enterprise Manager please contact our Online Support via http://www.Sysgem.com - your input is valuable.

Example

The following example shows the installation on Compaq Tru64, having first unpacked the tar archive into a directory /kits/SEM_kit.

```
# ./setup
SEM Agent for UNIX
------------------

[8] Platform is OSF1
[7] Data file is _kit.4
[6] Creating /kits/SEM_kit/tmp
[5] Copying _kit.4 to /kits/SEM_kit/tmp
[4] Changing to /kits/SEM_kit/tmp
[3] Unpacking _kit.4
[2] Removing temporary files
[1] Launching SEMInstaller

Sysgem SEM Agent UNIX Installer

  Agent ......: Sysgem SEM Agent v2.0 build 1165
  Target .....: OSF1
  Hostname ...: DigUnix.Sysgem.ch
  Processor ..: alpha

Step 1/6 - Checking Inventory

  Unpacking _data.0...

Step 2/6 - Directory

  Enter the directory where the agent is to be installed.
  The recommended default is /opt/Sysgem/SEM

Enter the directory [/opt/Sysgem/SEM]

Step 3/6 - Port Number

  Enter the TCP/IP port number. The default is 7251.

Enter the port number [7251]

Step 4/6 - Security Key

  This product uses a powerful security model to guard against attack.

  As part of the installation you MUST enter a security key.

  The key is a free format text string (case sensitive) which is unique
  in your network and MUST be the same as that entered for other components
  of this product on your network.

Enter the security key [] FortKnox

Step 5/6 - Autostart

  If you want the agent to start when you boot this system then enter YES,
  otherwise NO.

  If you select NO then you must start the agent interactively each time
  you boot this system.

Start the agent when the system boots? [Yes]

Step 6/6 - Start Agent

  If you want to use the agent now then it must be started after the,
  installation is complete.

  If you do not start the agent now then you must start it by either rebooting
  the system (if you have selected this option) or by starting it interactively.

Start the agent after the installation? [Yes]

Confirmation
  Directory .....: /opt/Sysgem/SEM
  Port number ...: 7251
  Security key ..: FortKnox
  Autostart .....: Yes
  Start agent ...: Yes
```

```
Is this correct? [Yes]

Start the installation now? [Yes]

Creating Directory
  /opt... Exists
  /opt/Sysgem... Exists
  /opt/Sysgem/SEM... Exists
  /opt/Sysgem/SEM/library... Exists

Stopping Agent
  If the agent is running it will be stopped.
  Agent process:   543 root         0:00.07 /opt/Sysgem/SEM/SysgemSEMAgent
  Stopping agent, pid=543, status=Success

Copying Files
  SysgemSEMAgent...
  SysgemSEMAgent.cfg... Exists (not overwritten)
  SysgemSEMStart...
  SEMInstaller...
  ssm-accounts...
  ssm-commander...
  ssm-perf...
  ssm-syslog...
  AddStartup...
  RemoveStartup...
  init.tcl...

Installing Security Key
  Installing SCSA Security Key
  ----------------------------
  Index ....: 0
  Value ....: FortKnox
  File .....: /opt/Sysgem/SEM/Digital_security_key_0.arc
  Status ...: OK

  SCSA Security Keys
  ------------------
  Key 0 ...: Valid


Updating Autostart Tables
  Removing: /sbin/rc3.d/S99Sysgem...
  Removing: /sbin/init.d/SysgemSEMStart...
  Copying:  /sbin/init.d/SysgemSEMStart...
  Linking:  /sbin/rc3.d/S99Sysgem...

Starting The Agent
    PID USER            TIME COMMAND
    664 root         0:00.07 /opt/Sysgem/SEM/SysgemSEMAgent

Installation completed.
#
```

The above example from an installation on Tru64 is true for all variants of supported UNIX systems except IBM AIX.

The Autostart procedures are different for AIX. The "Updating Autostart Tables" section of the AIX installation displays the following:

```
Updating Autostart Tables
  Inittab Entry
  -------------
  Sysgem_sem:2:wait:/opt/Sysgem/SEM/SysgemSEMStart
```

Files Installed

Root Directory:

Platform	Directory
AIX	/opt/Sysgem/SEM
COMPAQ (Digital)	/opt/Sysgem/SEM
HP	/opt/Sysgem/SEM
LINUX Intel	/opt/Sysgem/SEM
SUN Solaris	/opt/Sysgem/SEM

Agent Files:

File	Description
AddStartup	Adds the agent to the system's initialization tables.
RemoveStartup	Removes the agent from the system's initialization tables.
Sysgem-Agent-Logfile-Oct-00.txt	The agent logfile for October 2000.
SysgemSEMAgent	The agent executable image.
SysgemSEMAgent.cfg	The configuration file, contains entries which overwrites the default settings: Port number - the default is 7251. Debug level - the default is 0. Temporary directory for script files - the default is Sysgem_Script_<machine name>
SysgemSEMStart	The startup script that is invoked as part of the system initialization.
library/init.tcl	Required by ssm-commander (below).
ssm-accounts	A support module that lists the contents of the password and group files.
ssm-commander	A support module used to run UNIX commands that prompt the user for input.
ssm-perf	A support module that returns performance information - CPU loading, memory usage and list of processes.
ssm-syslog	A support module which returns entries from the syslog database.

AutoStart

So that the agent starts when the system is booted you must add entries to the initialization tables.

To make life easy, two files are provided in the root directory: *AddStartup* and *RemoveStartup*.

AddStartup is platform-dependent, as follows:

Platform	Method
AIX	Adds an entry to /etc/inittab (see inittab(4) for more information). An example of the /etc/inittab entry is shown below: *Sysgem_sem:2:wait:/usr/sbin/SYSGEM/SEM /SysgemSEMStart*
COMPAQ (Digital)	Copies *SysgemSEMStart* from the root directory to */sbin/init.d/SysgemSEMStart*, then creates a symbolic link */sbin/rc3.d/S99Sysgem* to *SysgemSEMStart*.
HP	Copies *SysgemSEMStart* from the root directory to */sbin/init.d/SysgemSEMStart*, then creates a symbolic link */sbin/rc3.d/S99Sysgem* to *SysgemSEMStart*.
LINUX Intel	Copies SysgemSEMStart from the root directory to /etc/init.d/SysgemSEMStart if possible, otherwise to /etc/rc.d/init.d/SysgemSEMStart, then creates a symbolic link /etc/rc.d/rc3.d/S99Sysgem to SysgemSEMStart.
SUN Solaris	Copies *SysgemSEMStart* from the root directory to */etc/init.d/SysgemSEMStart*, then creates a symbolic link */etc/rc3.d/S99Sysgem* to *SysgemSEMStart*.

OpenVMS

The OpenVMS agent is installed using VMSINSTAL.

The saveset containing the agents for both Alpha and VAX is VMSSVR020.A.

The saveset is saved as a zip file. You must unzip this file on an OpenVMS system to restore the original file attributes of the saveset.

If you do not have “Unzip” on OpenVMS, a copy of the Alpha and VAX unzip programs can be found under the “Extras” folder on the CD, or downloaded from the Sysgem website Download zone. Copy the appropriate one of these programs to your system, and define a “Foreign Command” to run the unzip program, e.g. after copying the file UNZIPAXP.EXE to SYS$MANAGER on an Alpha-VMS system, and the VMS_AGENT_020_A.ZIP zip archive file to a temporary directory, enter the following

```
$ UNZIP :== $SYS$MANAGER:UNZIPAXP.EXE
$ UNZIP  VMS_AGENT_020_A.ZIP
```

If you have received the saveset inside a zip file, then you must either unzip this file on an OpenVMS system to restore the original file attributes of the saveset, or invoke the command file ATTRIBUTES.COM.

The default OpenVMS agent port is 7251.

To override the default define the logical SEM-SERVER-PORT-NO before starting the agent.

To set the OpenVMS port to 7000 enter:

```
$ define SEM-SERVER-PORT-NO 7000
```

Example Installation

To install SEM, Log in the System account and type the following:

```
$ @sys$update:vmsinstal VMSAGENT020 products:[Sysgem.kits]
```

An OpenVMS v 6.1 installation logfile is shown below.

```
$ @sys$update:vmsinstal vmsagent020 SYS$SYSDEVICE:[SCHOFIELD.SYSGEM.BUILD_1190 i


       OpenVMS AXP Software Product Installation Procedure V6.2-1H3


It is 16-MAY-2001 at 16:11.

Enter a question mark (?) at any time for help.

%VMSINSTAL-W-NOTSYSTEM, You are not logged in to the SYSTEM account.
%VMSINSTAL-W-ACTIVE, The following processes are still active:
       UCX$NTPD
       ucx$esnmp
       ucx$os_mibs
       UCX$FTPD
       UCX$FTPC_1
       SEM-AGENT-AXP
       SEM-AGENT-AXP


The following products will be processed:

  VMSAGENT V2.0


        Beginning installation of VMSAGENT V2.0 at 16:11

%VMSINSTAL-I-RESTORE, Restoring product save set A ...

        ************************************
        *                                  *
        *    Installing agent for ALPHA    *
        *                                  *
        ************************************


  ************************************************************
  *                                                          *
  *  A directory will be created to store the agent files.   *
  *                                                          *
  ************************************************************

  -> If you are installing on a cluster then the directory
     must be created on a disk which is mounted cluster-wide.

  -> If you change this directory after you have installed this
     product you must also update:

       *  SYS$STARTUP:SEM-AGENT-STARTUP.COM

  -> See the User Guide for more information.

* Enter the device and directory [SYS$SYSROOT:[SYSGEM-SEM-AGENT]]:
%VMSINSTAL-I-SYSDIR, This product creates system disk directory  SYS$SYSROOT:[SYSGEM-
SEM-AGENT].
%CREATE-I-EXISTS, SYS$SYSROOT:[SYSGEM-SEM-AGENT] already exists

    Installed Files
    ===============

    SEM-AGENT-AXP.EXE         will be created in SYS$SYSROOT:[SYSGEM-SEM-AGENT]
    SSM-ACCESS-AXP.EXE        will be created in SYS$SYSROOT:[SYSGEM-SEM-AGENT]
    SSM-ACCOUNTS-AXP.EXE      will be created in SYS$SYSROOT:[SYSGEM-SEM-AGENT]
    SSM-AUDIT-EVENT-AXP.EXE   will be created in SYS$SYSROOT:[SYSGEM-SEM-AGENT]
    SSM-AUDIT-TRAIL-AXP.EXE   will be created in SYS$SYSROOT:[SYSGEM-SEM-AGENT]
    SSM-PERF-INFO-AXP.EXE     will be created in SYS$SYSROOT:[SYSGEM-SEM-AGENT]
    SSM-PROCESSES-AXP.EXE     will be created in SYS$SYSROOT:[SYSGEM-SEM-AGENT]
    SSM-QUEUES-AXP.EXE        will be created in SYS$SYSROOT:[SYSGEM-SEM-AGENT]
    SSM-SECURITY-AXP.EXE      will be created in SYS$SYSROOT:[SYSGEM-SEM-AGENT]
    SEM-AGENT-STARTUP.COM     will be created in SYS$STARTUP
    SEM-START-AGENT.COM       will be created in SYS$SYSROOT:[SYSGEM-SEM-AGENT]
    SEM-STOP-AGENT.COM        will be created in SYS$SYSROOT:[SYSGEM-SEM-AGENT]
    SEM-DEINSTALL.COM         will be created in SYS$SYSROOT:[SYSGEM-SEM-AGENT]
```

```
  ***********************************************
  *                                             *
  *  SECURITY - Installation Key - SECURITY.    *
  *                                             *
  ***********************************************

  This product uses a powerful security model to guard
  against attack.

  If this is the first time that you have installed this
  agent on this host then you must enter a key.

  The key is a free format text string (case sensitive) which is
  unique for your network and MUST be the same as that entered for
  other software components of this product on this network.

  For more information read the user guide.

* Enter the security key: FortKnox

    Installing Security Key...

Sysgem SEM Agent v2.0 build 1190
Copyright (c) 2000 by SYSGEM AG.

Initializing logfile
--------------------
Filename ...: PIPPIN$DKA0:[SYS0.][SYSGEM-SEM-AGENT.12-60]SysGem-Agent-Logfile-Ma
Status .....: %RMS-S-NORMAL, normal successful completion

Cluster nodename .....: PIPPIN
DECNET address .......: 12.60
OpenVMS version ......: V6.2-1H3
Hardware type ........: ALPHAbook 1
Active CPUs ..........: 1
Username .............: SCHOFIELD
Process name .........: SCHOFIELD
Process id ...........: 000000AD
Base priority ........: 4
Working set extent ...: 32768
Paging file quota ....: 400000
Software version .....: Sysgem SEM Agent v2.0 build 1190
SCSA compliant .......: Yes
Build date ...........: May  2 2001 at 12:47:09

Installing SCSA Security Key
----------------------------
Index ......: 0
Value ......: FortKnox
Filename ...: PIPPIN$DKA0:[SYS0.][SYSGEM-SEM-AGENT.12-60]security_key_0.arc;1
Status .....: OK


  The selected agent startup command files will be
  added to the SYSMAN startup database.

  Enter YES to add this file (recommended):
  $ MCR SYSMAN STARTUP ADD FILE SEM-AGENT-STARTUP.COM  /PHASE=END

  Enter NO to remove this file (if registered):
  $ MCR SYSMAN STARTUP REMOVE FILE SEM-AGENT-STARTUP.COM  /PHASE=END

* Enter YES or NO [YES]? YES
* Start the agent now ? [YES]? YES

!==============================================================================
!
!    Agent startup file
!    ------------------
!
!    Copyright (c) 1998-2000 SYSGEM AG.
!
!
!    P1 - port number
!
```

```
!    You can also override the default port numbers by defining a logical name
!    before calling this file.
!
!        Logical name: SEM-AGENT-PORT-NO
!
!    Example: $ define /system SEM-AGENT-PORT-NO 7000
!
!==============================================================================

EXECUTABLE ...: SYS$SYSROOT:[SYSGEM-SEM-AGENT]SEM-AGENT-AXP.EXE

Start New Process
=================
%RUN-S-PROC_ID, identification of created process is 000000AF

        ********************************************
        *                                          *
        *    Installation successfully completed   *
        *                                          *
        ********************************************


        Installation of VMSAGENT V2.0 completed at 16:12

    Adding history entry in VMI$ROOT:[SYSUPD]VMSINSTAL.HISTORY

    Creating installation data file: VMI$ROOT:[SYSUPD]VMSAGENT020.VMI_DATA


        VMSINSTAL procedure done at 16:13
```

Files Installed

SYS$STARTUP:

File	Description
SEM-AGENT-STARTUP.COM	Invokes the start-up file SEM-AGENT-AXP.COM located in the SEM Agent work directory.

SYS$SYSROOT:[SYSGEM-SEM-AGENT]:

File	Description
nn.nn.DIR	A subdirectory is created in the SEM root directory to provide a machine specific area into which temporary work files will be stored, or files that need to be machine specific for any reason, in a clustered OpenVMS environment. “nn.nn” is the DECnet executor node (area and number), and is system specific.
SEM-AGENT-AXP.COM	A command file to start the agent process (as a detached OpenVMS process).
SEM-AGENT-AXP.EXE	The SEM agent executable image.
SEM-AGENT-AXP.LIS	This gives a log file of the current Agent session. It begins a log of the start-up command file, giving information such as TCP/IP port in use, which security keys have been defined, TCP/IP address, etc.

SEM-DEINSTALL.COM	A command file for removing SEM from the system.
SEM-START-AGENT.COM SEM-STOP-AGENT.COM	Command files that may be used to manually stop and restart the agent process.
SSM-ACCESS-AXP.EXE SSM-ACCOUNTS-AXP.EXE SSM-PERF-INFO-AXP.EXE SSM-PROCESSES-AXP.EXE SSM-QUEUES-AXP.EXE SSM-SECURITY-AXP.EXE	SEM executable images to return data such as file access, user accounts, Audit Journal, performance, OpenVMS processes, queues, security. These images will be invoked from script files transmitted from the SEM client and will return data for display into the SEM display windows.
SSM-AUDIT-EVENT-AXP.EXE SSM-AUDIT-TRAIL-AXP.EXE	SEM executable images used for recording information into and extracting information from the OpenVMS audit journal files. This information gives details of the SEM user when transaction are conducted on this OpenVMS machine at the request of the SEM user logged into the SEM Management Console workstation.

(The default SYS$SYSROOT:[SYSGEM-SEM-AGENT] can be changed during installation).

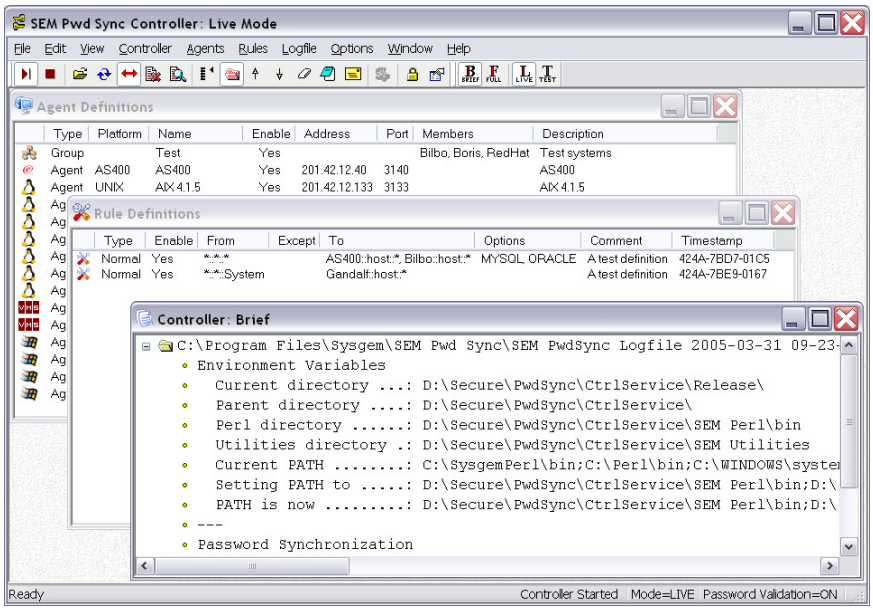
Controller Interface

Starting

The Controller Interface is used to configure and manage the Controller, the processing of password change requests is performed by the Controller Server.

Start the Controller Interface from the Windows Start menu (the default entry is *Start > Programs > Sysgem > Pwd Sync > Controller*).

A window will start similar to the following:



Options

The options available from the menu and toolbar are:

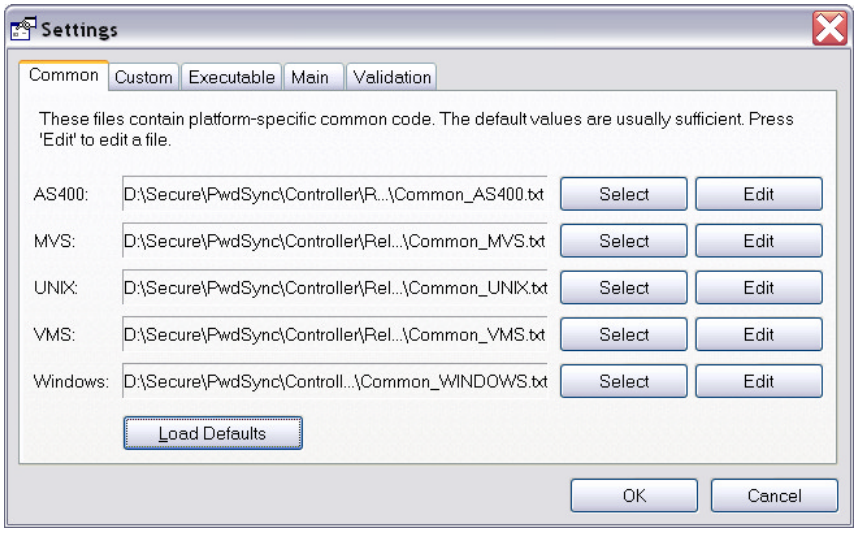
Option	Icon	Menu	Description
Run		Controller > Run	Start listening for incoming password validation and change requests.
Stop		Controller > Stop	Stop listening.
Open logfile		Logfile > Open	Open a logfile for display in this window.
Refresh logfile		Logfile > Refresh	Refresh the contents of the window, if new entries have been added to the logfile then they are displayed.
Enable Auto-updates		Options > Auto-Update	If selected then new entries in the current logfile are automatically displayed.
Erase current disk logfile		Options > Erase Current Logfile	Erase the contents of the disk logfile.
View disk logfile		Options > View Current Logfile	View the contents of the disk logfile with Notepad.
Collapse			Close all open branches in the logfile tree.
Expand on Error		Controller > Expand on Error	Automatically open folders in the logfile window if the folder contains error text.
Top of window			Move to the top of the window.
Bottom of window			Move to the bottom of the window.
Erase window contents		Controller > Erase	Erase the contents of the window.
Display window contents with Notepad		View > Logfile	Display the contents of the window with Notepad.
Send window contents with e-mail		Options > E-mail Output	Set the contents of the window with e-mail.
Set password		Options > Set Password	Set a password – this is a test window. Only available if running (listening for incoming messages).
Verbose tracing		Controller > Verbose	Enable verbose tracing of messages and display to the logfile window.
Settings		Options > Settings	See below in the section *Settings*.
Close		File > Close	Close program – continues running in the system tray.
Exit		File > Exit	Exit program (stops).

Settings

To display the settings window select the settings icon in the toolbar or *Options > Settings* menu entry.

Scripts – Common

When a script is create to change a password on a SEM agent the script is prefixed with the platform-specific common code which contains the functions used by the script.



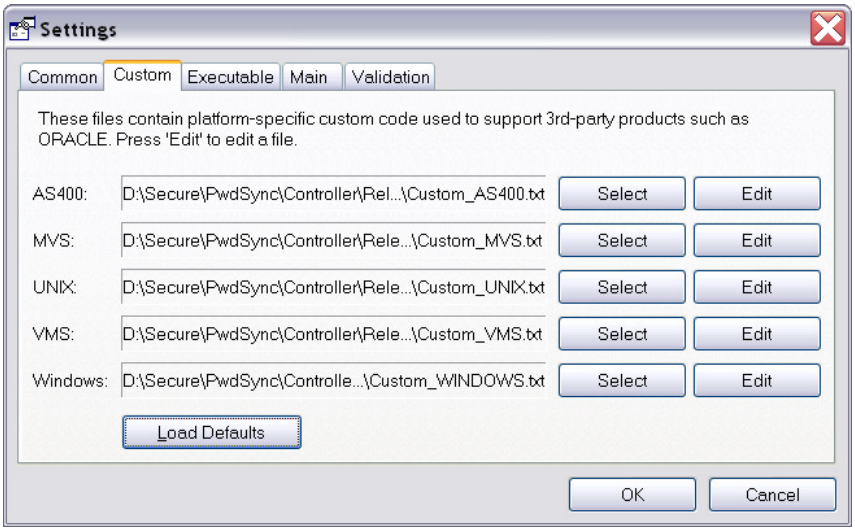
Press *Load Defaults* to load the default files shipped with this product.

There are no user-definable values in these scripts.

Scripts – Custom

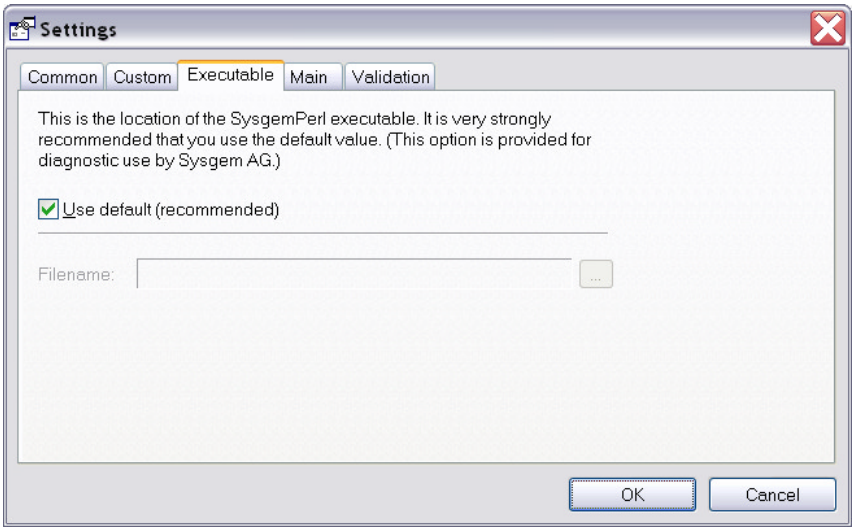
The custom scripts add support for third-party applications such as ORACLE. The functions in the custom script files correspond to the options are defined in Rules Database entries.

For each option which you define in a rule there must be a corresponding Set_<option> function in the Custom scripts, for example if the option is ORACLE then the function is Set_OPTION. For more information see the Custom scripts shipped with the Controller.



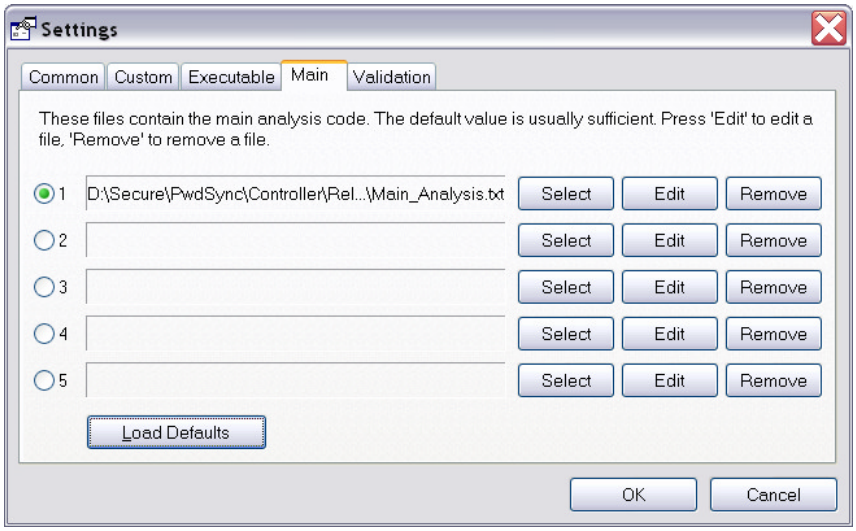
Scripts – Executable

The Controller scripts use Perl. For testing purposes only you can change the default location where the Controller looks to find the Perl executable.



Scripts – Main

This is the main script which runs when a change request is received. You can define up to 5 different scripts but only one script can be active at a time. This is to assist in developing new scripts and making it easy to switch between your own script and the script supplied by Sysgem.

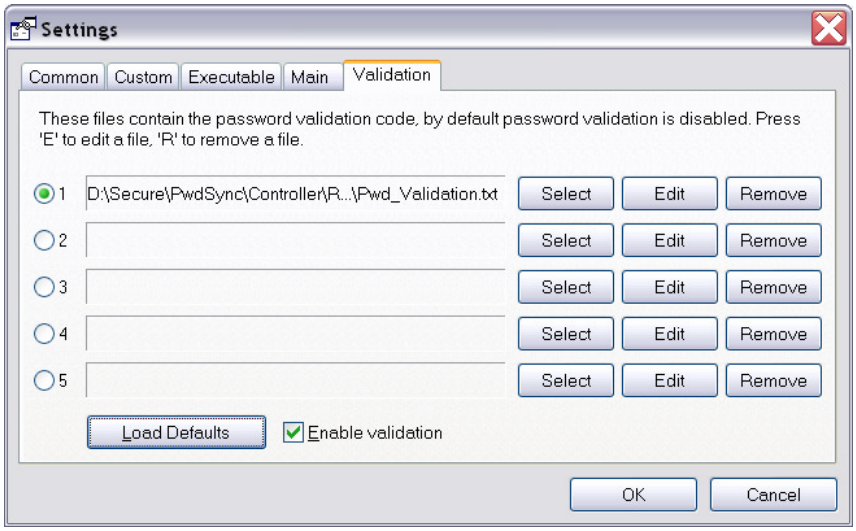


Press *Load Defaults* to load the default files shipped with this product.

There are no user-definable values in these scripts.

Scripts – Validation

This is the script which runs in response to a password validation request. You can define up to 5 different scripts but only one script can be active at a time. This is to assist in developing new scripts and making it easy to switch between your own script and the script supplied by Sysgem.



Press *Load Defaults* to load the default files shipped with this product.

The options you would typically change are:

- Minimum length
- Maximum length
- Password may not be same as username

Contact your reseller for more options.

To enable password validation:

- Check Enable validation in the Validation window (above).

- Make sure the validation script header contains the line: “use constant PWD_ENABLE => 1”. If validation is disabled it will be “use constant PWD_ENABLE => 0.”
- The Windows interceptor must have validation enabled, use the *Interceptor Configuration* utility described on page 52.

Controller Server

Overview

The processing of password change requests is performed by the Controller Server.

The server is installed as a standard Windows service *SEM Password Synchronization Controller*.

The server is used to validate old Windows passwords when the Console program is used. The server must be able to enable the privilege “Act as part of the operating system”. To be able to do this the account used for the service must use the Local System account or an account with the ability to enable the above privilege.

All configuration and management is performed using the Controller Interface.

Controller Database

Introduction

The database is maintained with the Controller user interface.

There are two displays:

- Agents, and
- Rules.

The database is accessed via ODBC, the DSN is *Sysgem Pwd Sync.* There is no real need for a high performance database solution, Access (the default) is fine.

Multiple Controllers

If you are maintaining multiple controllers (which is recommended) consider defining the database on one system then copying the database between controllers or using a network/shared database such as SQL Server.

Changes

07-October-2004: With the addition of Options to the Rules Database the table name has been changed from TABLE_RULES_V3 to TABLE_RULES_V4. Existing entries in TABLE_RULES_V3 are copied to TABLE_RULES_V4 if TABLE_RULES_V4 is empty.

21-December-2004: The *Except* rules field is now of unlimited length, as a result the Rules Database the table name has been changed from TABLE_RULES_V4 to TABLE_RULES_V5. Existing entries in TABLE_RULES_V3 or TABLE_RULES_V4 are copied to TABLE_RULES_V5 if TABLE_RULES_V5 is empty.

Agent Definitions

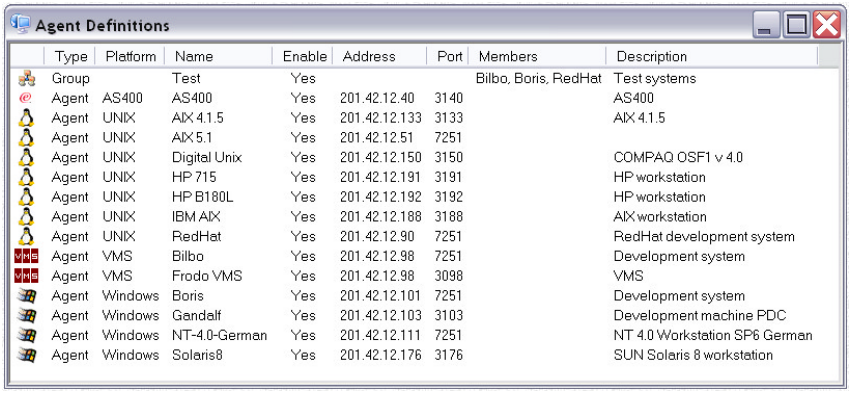
This display maintains a list of agent and group definitions on each Windows NT system where the password synchronization Controller is installed.

Each agent entry defines a remote system to which the Controller sends password changes (you must install the SEM Agent on each remote system).

Each group entry is simply a list of one or more agent definitions, for example 'Development Systems' or 'Test Systems'. You can select a group as part of a Rules Database entry (later in this chapter).

The agent and group definitions are used when you define rules (later in this chapter).

You can even import definitions from the list of agents defined in the SEM Management Console.



Agent Definitions

Type	Platform	Name	Enable	Address	Port	Members	Description
Group		Test	Yes			Bilbo, Boris, RedHat	Test systems
Agent	AS400	AS400	Yes	201.42.12.40	3140		AS400
Agent	UNIX	AIX 4.1.5	Yes	201.42.12.133	3133		AIX 4.1.5
Agent	UNIX	AIX 5.1	Yes	201.42.12.51	7251		
Agent	UNIX	Digital Unix	Yes	201.42.12.150	3150		COMPAQ OSF1 v 4.0
Agent	UNIX	HP 715	Yes	201.42.12.191	3191		HP workstation
Agent	UNIX	HP B180L	Yes	201.42.12.192	3192		HP workstation
Agent	UNIX	IBM AIX	Yes	201.42.12.188	3188		AIX workstation
Agent	UNIX	RedHat	Yes	201.42.12.90	7251		RedHat development system
Agent	VMS	Bilbo	Yes	201.42.12.98	7251		Development system
Agent	VMS	Frodo VMS	Yes	201.42.12.98	3098		VMS
Agent	Windows	Boris	Yes	201.42.12.101	7251		Development system
Agent	Windows	Gandalf	Yes	201.42.12.103	3103		Development machine PDC
Agent	Windows	NT-4.0-German	Yes	201.42.12.111	7251		NT 4.0 Workstation SP6 German
Agent	Windows	Solaris8	Yes	201.42.12.176	3176		SUN Solaris 8 workstation

The layout of this display is:

Field	Description	
Type	Agent	Group
Name	A unique name, usually the name of the host system, for example: *BILBO*.	Any name which identifies the agents, for example: *Windows Servers*.
Platform	The platform type. This is one of: AS400, Windows, UNIX and OpenVMS. This must be entered correctly so that the Controller is able to create the correct script to change the password on this system. Unlike SEM, the Controller does not determine the platform type in advance, instead it relies on the value in this field.	*Not used.*
Address	The name or IP address.	*Not used.*
Port	The port assigned to the SEM agent, this is usually 7251.	*Not used.*
Enabled	Whether the entry is enabled.	
Description	A free-format description of the entry.	
Members	*Not used.*	The members of the group.

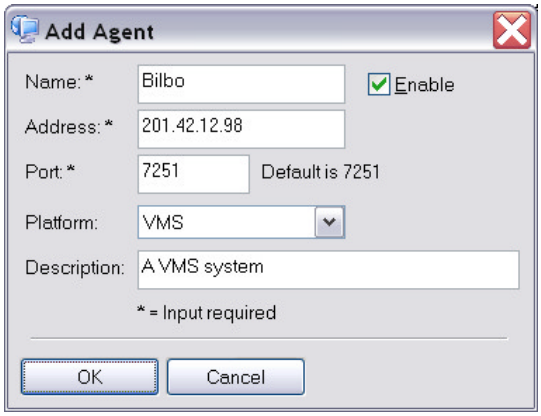
For the very latest information see the online help for this display.

Starting

Select *Agents*, *Display* from the main menu.

Add Agent Definition

From the *Agents* menu select *Add Agent*. Each agent definition is effectively a description of where each SEM Agent is installed together with its address.



Enter values in the fields:

- *Name*: The agent name – normally the hostname (recommended).
- *Address*: Either the name or IP address.
- *Port*: The port number assigned to the agent when installed.
- *Platform*: As appropriate.
- *Enable*: Check the box to enable the definition.
- *Description*: Free-format text.

Then press *OK*.

Import Agent Definitions from SEM

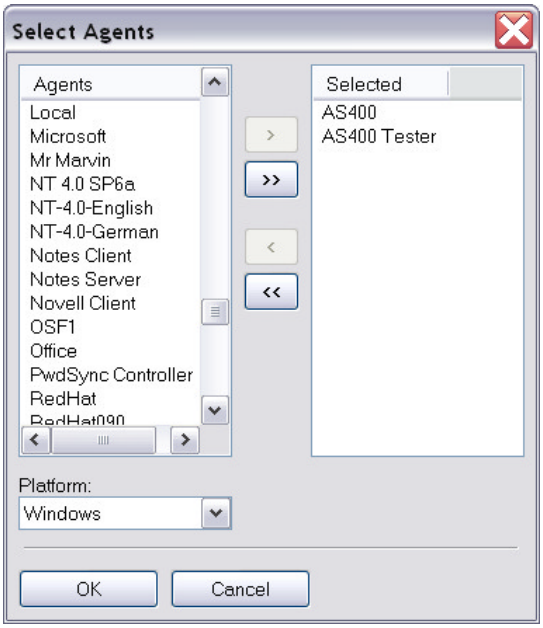
From the *Agents* menu *select Import*. Agent definitions are imported one platform at a time – the platform information is not available in the SEM Management Console definitions so it must be added here.

It is easiest to export Agent definitions from the SEM Management Console to a known file.

To export:

- Start the SEM Management Console,
- Select *Agents* from the *Managers* menu.
- From the *Export* menu select *To File*.

The file you create is a coded plain ASCII file from which the agent definitions are loaded.



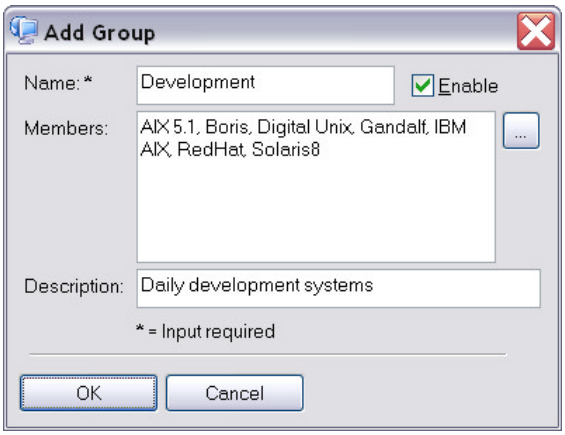
Select:

- the definitions to be added,
- the platform,

then press *OK*.

Add Group Definition

From the *Agents* menu select *Add Group*. Each definition assigns one or more agent definitions to a group, for example *Development* or *Production*.



Enter values in the fields:

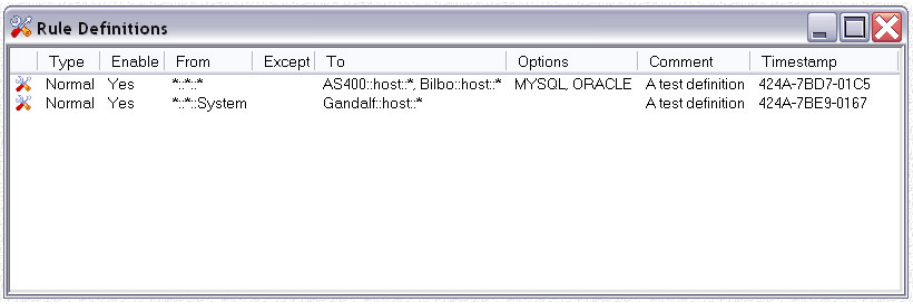
- *Name*: The name of the group.
- *Member(s)*: The members of the group.
- *Enable*: Check the box to enable the definition.
- *Description*: Free-format text.

Then press *OK*.

Rules Definitions

This display maintains the Rules Database, which defines what happens when a password change request is received.

An example of a simple database with two rules:



Each entry in the database consists of:

Field	Description
Enable	Whether the entry is enable (tick) or disabled (cross).
From	The format of the *from* entry is hostname::platform::username
Except	The format of the *except* entry is hostname::platform::username
To	The format of the *to* entry is hostname::account-type::username
Options	Options which correspond to functions in the Custom scripts, used for third-party application support such as ORACLE.
Comment	A free-format description of the entry.
Timestamp	The creation date (for internal use by Sysgem).

From (Password Change Request)

The format of a *from* entry is: hostname::platform::username, where:

- *Hostname* is the name of the host (agent), this does not have to be defined by the *Agents and Groups* displays.
- *Platform* is one of AS400, Windows, UNIX and OpenVMS.
- *Username* identifies the account which has requested the password change.

Note: you can use the * wildcard in any of these fields.

Except (Exception to From Entries)

The format of an *except* entry is: hostname::platform::username, where:

- *Hostname* is the name of the host (agent), this does not have to be defined by the *Agents and Groups* displays.
- *Platform* is one of AS400, Windows, UNIX and OpenVMS.
- *Username* identifies the account which is *not* to have its password changed.

Note: you can use the * wildcard in any of these fields. The username field supports the * and % wildcards, where % matches a single character and * matches any number or characters.

To (Password Change Target)

The format of a *to* entry is: hostname::account-type::username, where:

- *Hostname* is the name of the host (agent), and must already be defined by the *Agents and Groups* displays.
- *Account-type* is one of host, SAP, Lotus Notes, ... (note: in the first release only *host* accounts are supported).
- *Username* identifies the account which is to have its password updated.

Options (Third-Party Application Support)

To enable support for applications such as ORACLE you add an option – a text string such as ORACLE or MySQL – which corresponds to a function in the Custom scripts.

For each option which you define there must be a corresponding Set_<option> function in the Custom scripts, for example if the option is ORACLE then the function is Set_OPTION. For more information see the Custom scripts shipped with the Controller.

Matching Rules

When a change request is received, the rules are read, analyzed in sequence (1, 2…) until one or matches are match made with rules which meet the criteria below:

Seq	Hostname	Platform	Username
1	Exact	Exact	Exact
2	Exact	*	Exact
3	Exact	Exact	*
4	Exact	*	*
5	*	*	*

So if the first match is found at Seq 3 then *all rules at Seq 3 which match are used*.

An example of a rule's *From* clause which matches Seq 3 is: BILBO::VMS::* .

This logic was changed on June 16th, 2005 so that many rules can be defined for the same user(s).

Except Syntax

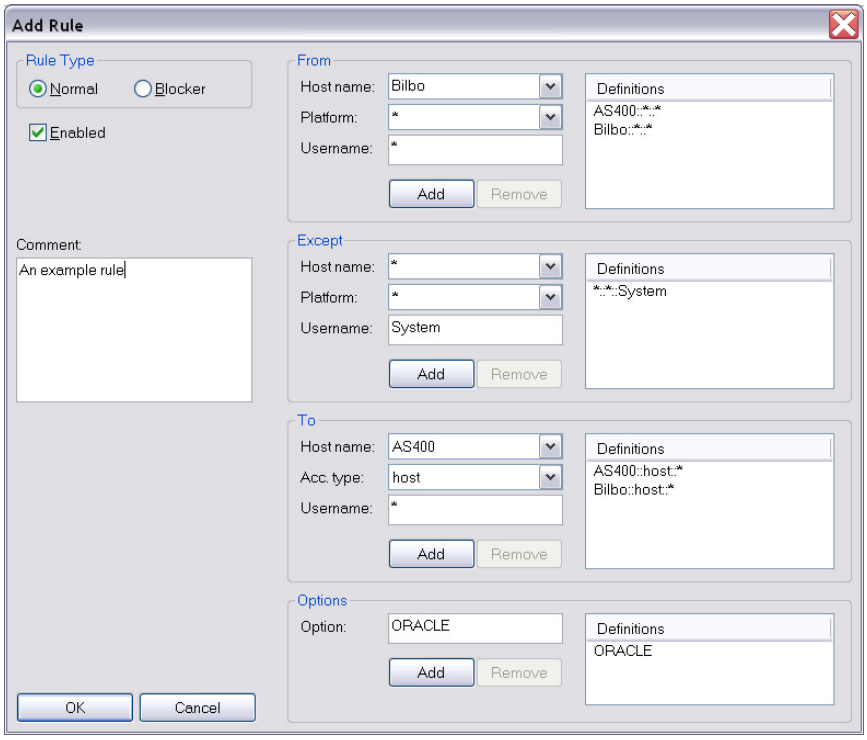
Pattern	Result
%	Match exactly one character, % is replaced with \S.
*	Match any characters, * is replaced with \S+.
[0-9]	Match a single digit.
[a-z]	Match a lowercase letter.
[A-Z]	Match an uppercase letter.
\d	Matches a digit, same as [0-9]
\s	Matches a whitespace character (space, tab...)
[1|2]	Matches 1 or 2
+	Match the proceeding symbol one or more times.

Starting

Select *Rules, Display* from the main menu.

Add

From the *Options* menu select *Add Agent*. Each definition contains: Rule Type, Enabled, Comment, From, Except, To, and Options fields.



General

- *Rule type*: Normal or Blocker.
- *Enabled*: Check to enable the definition.
- *Comment*: Free-format text.

From

Here you define one of more entries where each entry identifies an account (or accounts if the * wildcard is used) which requests a password change.

Enter values in the fields:

- *Host name*: The host from which the password request is received.
- *Platform*: As appropriate.
- *Username*: Name of the account or the * wildcard.

Then press *Add* to add the entry to the *Current Entries* list. Repeat as necessary – each rule can have one or more *From* entries.

Except

Here you define one of more entries where each entry identifies an account (or accounts if the * wildcard is used) which is an exception to the definitions in the *From* list.

Enter values in the fields:

- *Host name*: The host from which the password request is received.
- *Platform*: As appropriate.
- *Username*: Name of the account, this can contain the * (matches any number of characters) or % (matches a single character) wildcards.

Then press *Add* to add the entry to the *Current Entries* list. Repeat as necessary – each rule can have one or more *Except* entries.

To

Enter values in the fields.

- *Host name*: The system where the password will be updated.
- *Account type*: Select either *host*, *NIS* or *None*. If set to None the operating system account is not updated, only the accounts associated with 3rd-party applications are updated (see *Options*).
- *Username*: The account to be updated.

Enter an option then press *Add* to add the entry to the *Current Entries* list. Repeat as necessary.

Options

For each option you add here there must be a corresponding *Set_<Option>* entry in the Custom script for the Agent's platform.

For example if the option is ORACLE then the function is Set_OPTION. For more information see the Custom scripts shipped with the Controller

When you have finished press *OK*.

Examples

Here are examples of rules definitions and the associated logic.

From	Except	To	Options
PIPPIN::*::SMITH_JOHN		BILBO::host::SMITHJ	
John Smith's new password on PIPPIN is updated on BILBO where his account is SMITHJ.			

PIPPIN::*::SMITH*		BILBO::host::SMITH*	ORACLE
All password changes for accounts starting with SMITH on system PIPPIN are sent to BILBO, but the account name that will be updated is SMITH*. This is obviously wrong – the *To* field contains a partial wildcard. The Rules Database display has now been updated so that a partial wildcard cannot be entered in the *To* field. The ORACLE account is also updated using the function Set_ORACLE in the Custom script for BILBO's platform.			
PIPPIN::*::*	*::*::SYS*	BILBO::host::*	
All accounts on PIPPIN *except* for accounts starting SYS (such as SYSTEM, SYSTEST) are updated on BILBO.			
VMS::*::SMITH_J		UNIX::host::smith_j UNIX::host::j_smith	
In this example John Smith has an account SMITH_J on a VMS system which must be mapped through to two UNIX accounts: smith_j and j_smith. Because UNIX accounts are case-sensitive (unlike VMS) the rule must explicitly specify the UNIX accounts, it is not possible to use the * wildcard as this will result in an attempt being made to update the UNIX account SMITH_J. An alternative would be to modify the scripts supplied with this product to dynamically update To account list.			

If you need extensions to the Rules Database please contact your distributor or Sysgem AG.

Console

Overview

The console program is a standard DOS / command-line program for Windows, UNIX and OpenVMS. It is used as an alternative to the interceptor.

The console program makes direct contact with the Controller when the password is changed.

```
SEM Password Synchronization v2 build 2444
------------------------------------------
Sysgem AG Corporate Password Policy
Minimum chars: 8
Maximum chars: 14
At least 1 digit is required
---
You are logged in as: SIMON-LAAX\Simon on BORIS

Old password: #####
New password: ########
Retype new password: ########

Changed password for Simon
Connecting to 201.42.12.101
Reply: OK

Press Enter to continue . . .
```

Configuration File

The console uses a configuration file which contains tokens and values:

Token	Value
LOCAL	*Windows only:* If set to ***No*** or ***Off*** or ***0*** then the local password is not changed.
NOTICE	*Windows only:* Text displayed when the console program starts, for example you can display your corporate password policy.
ADDRESS	The address and port number of a Controller.

The file is SEMPwdSync.cfg in the same folder as the console program, usually this is C:\Program Files\Sysgem\SEM Pwd Sync.

Edit this file with Notepad or Wordpad.

Example:

```
#################################################################
#
#   Sample configuration file for the SEM Password Synchronizer.
#
#   Format of address entries is shown below.
#
#   This file is used by the Console only.
#

#
#   Change the local default (on by default)
#
LOCAL Yes
#
#   Banner
#
NOTICE Sysgem AG Password Policy
NOTICE Minimum password length is 8 characters
NOTICE Maximum password length is 14 characters
#
#   Controllers
#
ADDRESS 201.42.12.101:7260
ADDRESS 201.42.12.102:7260
```

The console program tries all controllers in turn until one is found which is available to service the change request.

Windows Interceptor

Overview

The Windows interceptor consists of:

- SEMPwdWSync.dll in the Windows system directory, usually \WINNT\System32.

This conforms to the Microsoft standard for a password filter DLL. It supports:

Function	Description
InitializeChangeNotify	The function is implemented by the password filter DLL. It returns TRUE or FALSE, indicating if the password filter DLL is loaded.
PasswordChangeNotify	The function is implemented by the password filter. It is used to notify the DLL that a password change was made.
PasswordFilter	The function is implemented by the password filter DLL. It returns TRUE or FALSE, indicating that the new password is valid.

The DLL in 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).

HKEY_LOCAL_MACHINE
\SYSTEM
\CurrentControlSet
\Control
\Lsa
\Notification Packages (add new value of type REG_MULTI_SZ)

This is done when the interceptor is installed. After updating the registry the system must be rebooted, this is a Windows requirement.

- 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.

Logfile

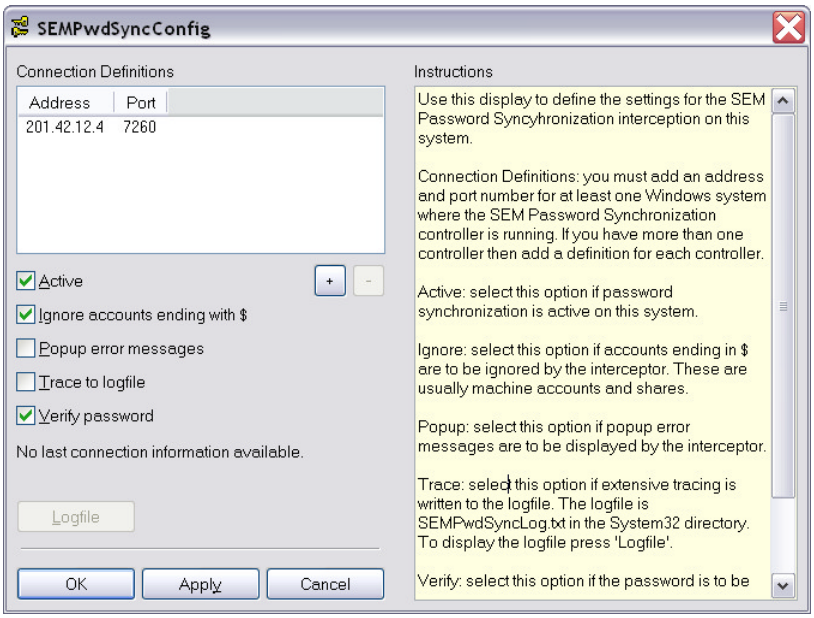
The logfile is SEMPwdSyncLog.txt in the same directory as the DLL. The easiest way to view the contents of the logfile is to use the *Interceptor Configuration* utility.

Configuring

To assist with the configuration a small the *Interceptor Configuration* utility is installed when you install the Windows interceptor.

This is started from the Start menu, the file is:

- SEMPwdSyncConfig.exe in the Windows system directory, usually \WINNT\System32.



The options are:

- Connection Definitions: you must add an address and port number for at least one Windows system where the SEM Password Synchronization controller is running. If you have more than one controller then add a definition for each controller.

- Active: select this option if password synchronization is active on this system.
- Ignore accounts ending with $: select this option if accounts ending in $ are to be ignored by the interceptor. These are usually machine accounts and shares.
- Popup error messages: select this option if popup error messages are to be displayed by the interceptor.
- Trace to logfile: select this option if extensive tracing is written to the logfile. The logfile is SEMPwdSyncLog.txt in the System32 directory. To display the logfile press 'Logfile'.
- Verify password: select this option if the password is to be verified by the controller. Use this option if you want to enforce a corporate password policy.

Press 'OK' when you have finished making changes.

OpenVMS Interceptor

Overview

The OpenVMS interceptor consists of:

- SEM-PWDSYNC-LOGINOUT.EXE in SYS$SYSTEM.

This has been written in accordance with the *OpenVMS Utility Routines Manual, LOGINOUT (LGI) Routines, (c) COMPAQ.*

The OpenVMS kit is shipped as:

- vms_pwdsync_020_a.zip – VAX and AXP saveset (requires unzip),
- vms_pwdsync_020_axp.exe – AXP self-extracting executable,
- vms_pwdsync_020_vax.exe – VAX self-extracting executable.

Testing

When you connect to a remote system with the interceptor installed (for example by using SET HOST) the string

```
%SEM-I-PWDSYNCINIT, SEM Password Synchronizer initialized
```

is displayed. This confirms that SEM-PWDSYNC-LOGINOUT.EXE has been started correctly by LOGINOUT.

Customizing

You can customize the text displayed during the phases of SEM-PWDSYNC-LOGINOUT.EXE by using logical names defined in executive mode in the system logical name table (define /system /executive).

Logical Name	Phase
SEM_PWD_SYNC_IDENTIFY	Callout identify
SEM_PWD_SYNC_AUTHENTICATE	Callout authenticate
SEM_PWD_SYNC_FINISH	Callout finish
SEM_PWD_SYNC_START	Callout iact start
SEM_PWD_SET_PWD	Setting password on local system

This is provided for diagnostic purposes by Sysgem.

For example, to add extra text when starting:

```
$ define /system /exec SEM_PWD_SYNC_START_0 "Using Pwd Sync"
$ define /system /exec SEM_PWD_SYNC_START_1 "--------------"
```

You can define up to 100 logical names (SEM_PWD_SYNC_START_0 to SEM_PWD_SYNC_START_99), gaps are not permitted.

Examples

Introduction

These examples show the output you can expect when the program works successfully *and* when you encounter errors.

Controller Not Found

In this example a LINUX Mandrake user (Walter) changes his password. The configuration file contains three entries:

```
#################################################################
#
#   Sample configuration file for the SEM Password Synchronizer.
#
#   Format of address entries is shown below.
#
ADDRESS 201.42.12.104:7260
ADDRESS 201.42.12.105:7260
ADDRESS 201.42.12.103:7260
```

The Controller on 201.42.12.104 is not started, and 201.42.12.105 is currently down for maintenance. Only 201.42.12.103 is available.

```
# ./pwdsync
SEM Password Synchronization v2 build 1455
You are logged in as: Walter on Mandrake

New password:
Retype new password:

Connecting to 201.42.12.104
Error establishing connection with 201.42.12.104:7260, Connection refused

Connecting to 201.42.12.105
Error establishing connection with 201.42.12.105:7260, No route to host

Connecting to 201.42.12.103
Reply: OK
#
```

The sequence of connection attempts is:

1. IP address 201.42.12.104 port 7260. This fails because the Controller is not listening on port 7260, hence the error message *Connection refused*.
2. IP address 201.42.12.105 port 7260. This fails because the host is not available, hence the error message *No route to host*.

3. IP address 201.42.12.103 port 7260. This succeeds – the change request is sent.

Password Validation Error

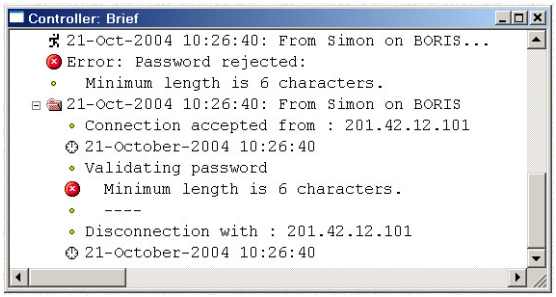
In this example the password validation fails (password is too short).

```
# ./pwdsync
SEM Password Synchronization v2 build 1455
You are logged in as: Simon on Mandrake

New password:
Retype new password:

Connecting to 201.42.12.104
Password error: Minimum length is 6 characters.
#
```

The user enters a new password of ABC (typed characters are not echoed on the screen).

A connection is made with the first Controller in the configuration file, and the new password is rejected.

The output in the Controller window is shown below:



To change the password validation criteria you must open the Controller's Settings window, select the Scripts – Validation pane and edit the selected script.

For assistance please contact your distributor or Sysgem AG.

Rule Not Found

In this example a rule is not found for the supplied hostname / platform / username.

```
# ./pwdsync
SEM Password Synchronization v2 build 1455
You are logged in as: Simon on Mandrake

New password:
Retype new password:

Connecting to 201.42.12.104
Reply: OK
#
```

The output in the Controller window is shown below:

```
Controller: Brief
21-Oct-2004 10:28:58: From Simon on BORIS...
21-Oct-2004 10:28:58: From Simon on BORIS
  Connection accepted from : 201.42.12.101
21-October-2004 10:28:58
  Validating password
  Validation disabled
21-October-2004 10:28:58
  Password forward request from Simon on BORIS (Windows)
  Processing
  Processing>
    Rule not found for BORIS::Windows::Simon
  Distributing to 0 agent(s)
  Finished
  Disconnection with : 201.42.12.101
21-October-2004 10:28:59
```

The new password is validated, but the Controller fails to find a rule that matches the account requesting the password change.

Target Agent Not Reachable

In this example the target agent Treebeard is not reachable.

```
# ./pwdsync
SEM Password Synchronization v2 build 1455
You are logged in as: Simon on Mandrake

New password:
Retype new password:

Connecting to 201.42.12.104
Reply: OK
#
```

The output in the Controller window is shown below:

```
Controller: Brief
Agent 3/4: RedHat090
  Platform ......: Linux (UNIX)
  Nodename ......: redhat
  Current dir ...: /opt/Sysgem/SEM
  Current user ..: root
  Executable ....: ./ssm-commander
  Account sysgemtest found in /etc/passwd.
  Username ......: sysgemtest
  NIS ...........: false
  Password set.
  Setting the DEMOAPP password for sysgemtest
  DEMOAPP: Not yet supported
  ----
Agent 4/4: Treebeard
  Error establishing connection with 201.42.12.105:7251 - A connection
  ----
Finished
Disconnection with : 201.42.12.101
21-October-2004 10:33:57
```

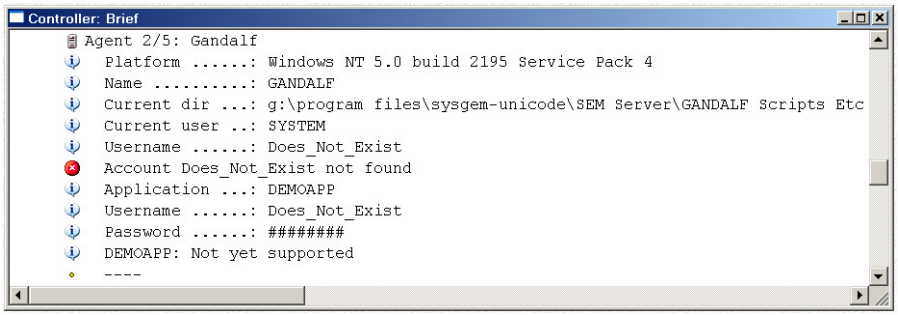
The Controller fails to connect to *Treebeard* because the computer is not part of the network. The full error text is:

Error establishing connection with 201.42.12.105:7251 - A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond.

Target Account Not Found

In this example the target account in the matching rule does not exist on the Windows server Gandalf.

The Controller connects to Gandalf, sends the script to change the password but the script returns an error.

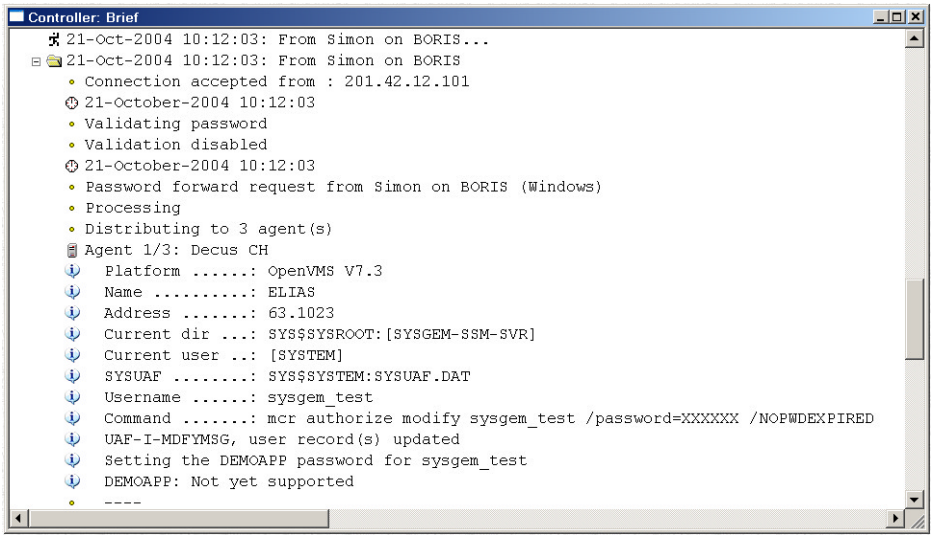


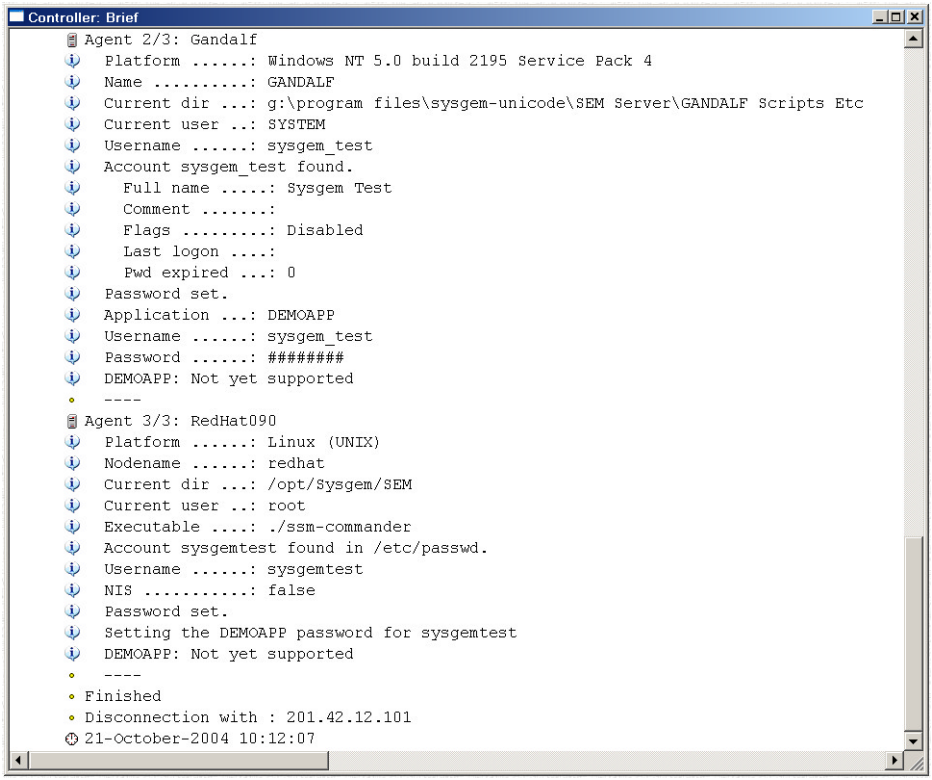
Target Account Updated

In this example the target account is updated successfully. Three target agents are updated:

1. Agent 1 is *Decus CH*, an OpenVMS 7.3 system used by the Digital User's group in Switzerland. The account updated is *Sysgem_Test*.
2. Agent 2 is *Gandalf*, a Windows 2000 test domain controller. The account updated is *Sysgem_Test*.
3. Agent 3 is *RedHat090*, a RedHat LINUX 9.0 workstation also used for testing. The account updated is *sysgemtest* (RedHat does not willingly support usernames which include punctuation).

The rule also updates the DEMOAPP account, as you see in the logfile the custom scripts display the standard 'Not yet supported' text.





```
Controller: Brief
Agent 2/3: Gandalf
  Platform ......: Windows NT 5.0 build 2195 Service Pack 4
  Name ..........: GANDALF
  Current dir ...: g:\program files\sysgem-unicode\SEM Server\GANDALF Scripts Etc
  Current user ..: SYSTEM
  Username ......: sysgem_test
  Account sysgem_test found.
    Full name .....: Sysgem Test
    Comment .......:
    Flags .........: Disabled
    Last logon ....:
    Pwd expired ...: 0
  Password set.
  Application ...: DEMOAPP
  Username ......: sysgem_test
  Password ......: ########
  DEMOAPP: Not yet supported
  ----
Agent 3/3: RedHat090
  Platform ......: Linux (UNIX)
  Nodename ......: redhat
  Current dir ...: /opt/Sysgem/SEM
  Current user ..: root
  Executable ....: ./ssm-commander
  Account sysgemtest found in /etc/passwd.
  Username ......: sysgemtest
  NIS ...........: false
  Password set.
  Setting the DEMOAPP password for sysgemtest
  DEMOAPP: Not yet supported
  ----
Finished
Disconnection with : 201.42.12.101
21-October-2004 10:12:07
```

OpenVMS Interceptor

In this example a user connects to 12.99 and logs on as GERARD:

```
$ set h 12.99
%SEM-I-PWDSYNCINIT, SEM Password Synchronizer initialized

      Go Away

Username: GERARD
Password:

Sysgem Enterprise Manager - Password Synchronization
----------------------------------------------------
Your password has expired; you must set a new password to log in

New password:
Verification:
%SEM-I-CONNECT, Connecting to 201.42.12.104 -
%SEM-I-VALDPWD, Validating password on 201.42.12.104 -
%SEM-I-REPLYOK, reply = OK

%SEM-I-UPDSUAF, updating local SYSUAF record -
%SEM-I-PWDOK, New password set OK

%SEM-I-CONNECT, Connecting to 201.42.12.104 -
%SEM-I-FWRDPWD, Forwarding password to 201.42.12.104 -
%SEM-I-REPLYOK, reply = OK


            Good Morning!


      42 failures since last successful login
$
```

First of all, the string

```
%SEM-I-PWDSYNCINIT, SEM Password Synchronizer initialized
```

is displayed. This confirms that SEM-PWDSYNC-LOGINOUT.EXE has been started correctly by LOGINOUT.

After the user has logged in using the GERARD account he is prompted for a new password by SEM-PWDSYNC-LOGINOUT.EXE because the account's password is detected as having expired.

```
Sysgem Enterprise Manager - Password Synchronization
----------------------------------------------------
Your password has expired; you must set a new password to log in
```

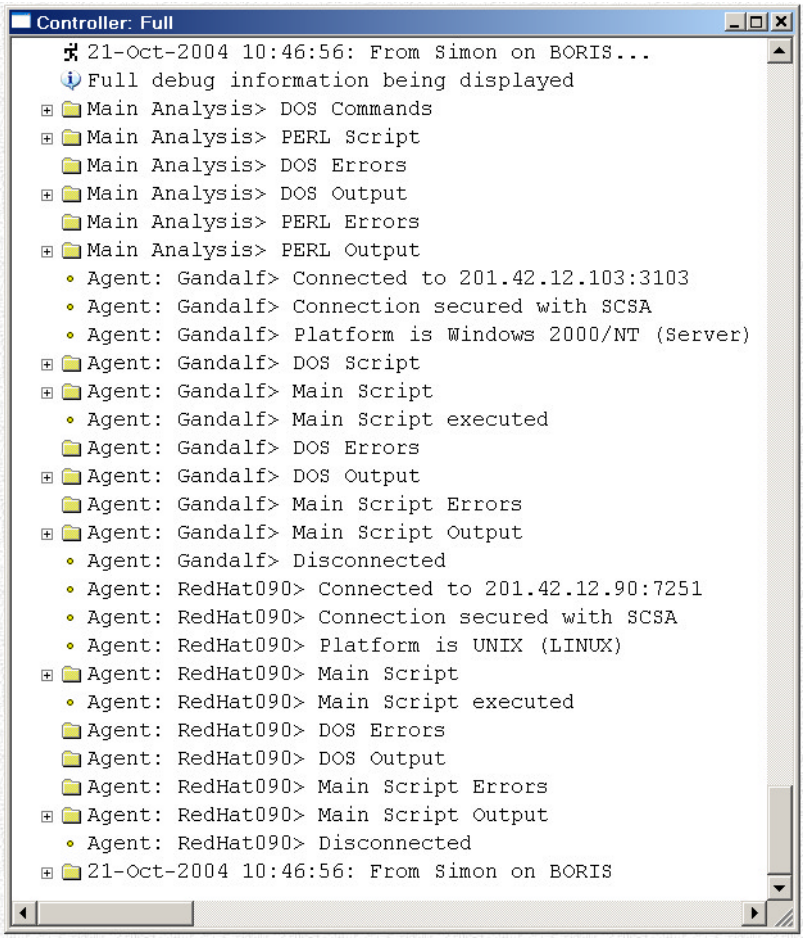
The new password is set and then sent to the Controller.

Full Logging

In general Full logging will only be used to detect errors in scripts or in the configuration.

When full logging is enabled by selecting the Full option in the Controller menu all scripts send and received are displayed in the logfile window.

This adds considerably to the size of the logfile and slows down the password synchronization.



There are two categories of script:

1. The *Main Analysis* which processing the incoming request, returning a list of target agents and accounts to be updated, and
2. The target Agent scripts, in this example the agents *Gandalf* and *RedHat090* are updated.

Message Flow

Console

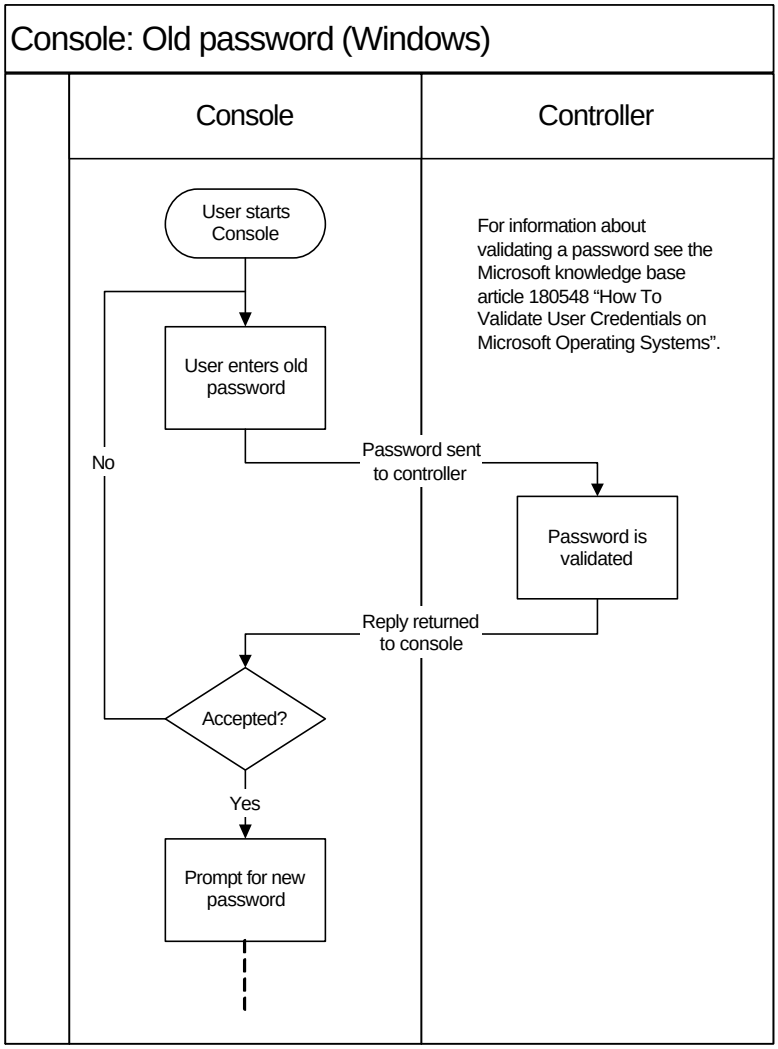
A sample message flow where the console is used to change a password on a Windows system is shown below.

The only difference between Windows and other platforms is that the old password is validated using the controller as a normal Windows user does not have sufficient Windows privileges / rights to do this.

For information about validating a password see the Microsoft knowledge base article 180548 “How To Validate User Credentials on Microsoft Operating Systems”.

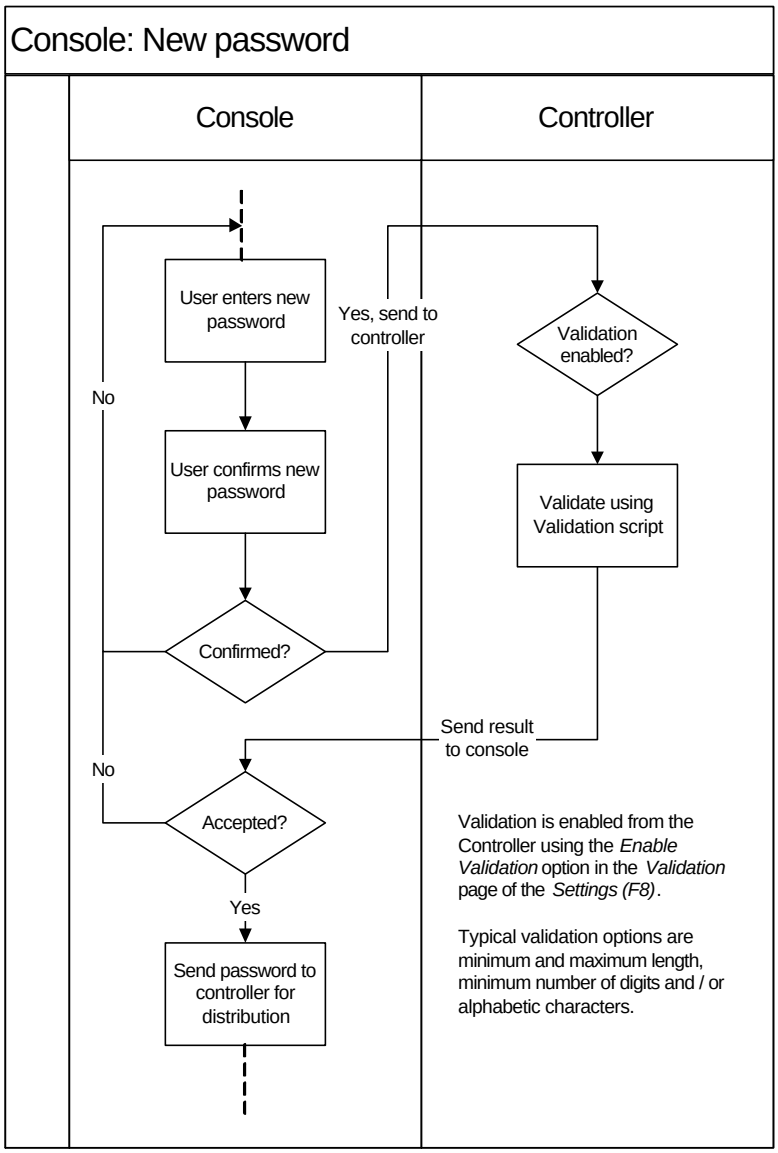
Old Password

When the user enters the old password is is validated by the controller as a normal user will not have sufficient Windows privilege to do this.



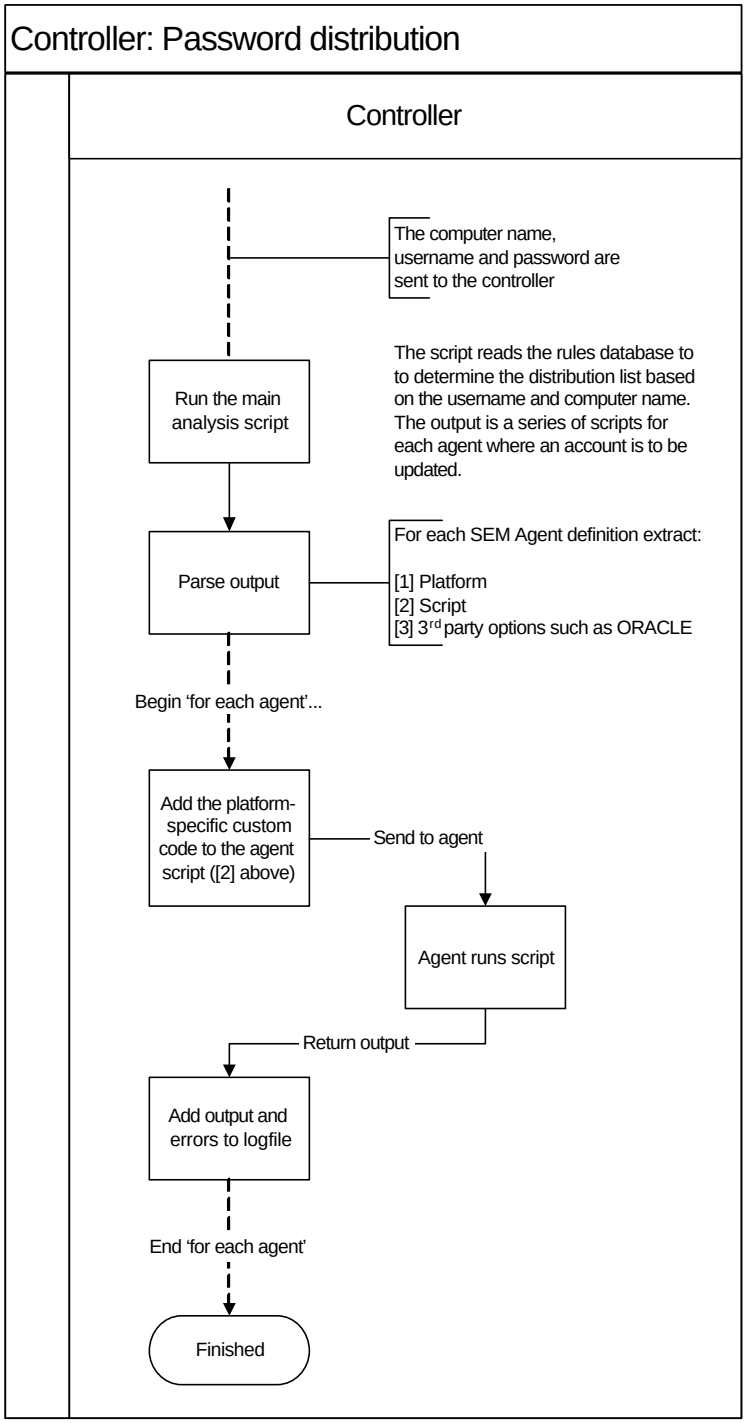
New Password

The new password is validated by the controller using the validation script.



Password Distribution

The controller distributes the password by preparing the script which is sent to the agents where accounts are to be updated.



Interceptor

In this example a user in a Windows domain changes his password. The interceptor is installed on the PDC, the Controller on a Windows system (this could be the PDC, BDC or any workstation).

The logic flow is show below.

Step	Where	Description
1	Workstation	User changes password
2	PDC (or BDC)	The Password Filter routine in the interceptor is called. (This routine can reject the new password.) If password validation is enabled, a connection is established with a Controller, and the password is sent over for validation.
3	Windows Server	The Controller receives the request to validate the password. The script selected in the Scripts – Validation runs. The script either accepts or rejects the proposed password.
4	Windows Server	Assuming the password is not rejected, the password is changed on the local system, then sent to the Controller for propagation.
5	Windows Server	The Controller receives the hostname, username and new password.
6	Windows Server	The script selected in the Scripts – Main runs, the output is one script file for each agent where the new password is to be applied.
7	Windows Server	A reply is sent back to the interceptor.
8	SEM Agents	The output scripts (above) run on each agent.

Testing

Overview

Testing password synchronization is very straightforward. A simple Windows installation can be used to ensure that you have correctly installed and configured the software components.

Change Log

2004

Date	Change
December 20, 2004	Fixed problem defining the alternate folder for the controller logfiles. Enabled Windows XP Themes. Re-worked the documentation.

2005

Date	Change
March 10, 2005	Fixed problem where the password was replaced with ######## if ***Full*** was selected in the Password Synchronization Controller.
March 30, 2005	Added *Agent* and *Rule* definitions to the Controller interface, so it is now no longer necessary to use the SEM PwdSync module to define agents and rules. • The Controller service runs the DefineDatabase Perl script to ensure the database has been defined and if already exists is upgraded to the latest definition. • When the Controller user interface starts the Agents and Rules windows are displayed. • For a list of options either right-click in the Agents or Rules window or select options from the main menu.
June 16, 2005	The logic for matching rules has been enhanced. In the Rules Definitions on page 43 the logic for finding the first matching rule is explained. As of this release the first match is returned together with all other matches with rules at the same level in the table on page 44. The result of this change is that you can now define as many rules for the same From definition as you want. An example of a From definition is ***::*::System**.