Sysgem AG
Lavaterstrasse 45
8002 Zurich
Switzerland

Tel: +41 (0) 44 204 6023

office@sysgem.com
www.sysgem.com

Sysgem Self-Service Password Reset

Installation and User Guide

Sysgem AG
Lavaterstrasse 45
CH-8002 Zürich
Switzerland

Aug-2011

Contents

1 Installing Sysgem Self-Service Password Reset 3
1.1 Introduction 3
1.2 Pre-requisites 4
1.3 Internet Information Services, Minimum Settings 4
1.4 Example Installation – Domain Controller 6
1.5 Installation – Workstation 10
1.6 License Management 10
1.7 Required Permissions and Troubleshooting 12
2 User Guide 14
2.1 Introduction 14
2.2 Enrolment 14
2.3 Resetting Forgotten Passwords 16

1 Installing Sysgem Self-Service Password Reset

1.1 Introduction

Sysgem Self-Service Password Reset solves the problem of end-users forgetting their Windows login passwords and having to ask the helpdesk or the system administrator to reset it. With *Sysgem Self-Service Password Reset* users can reset their own passwords after correctly replying to security questions with answers that they have previously defined themselves.

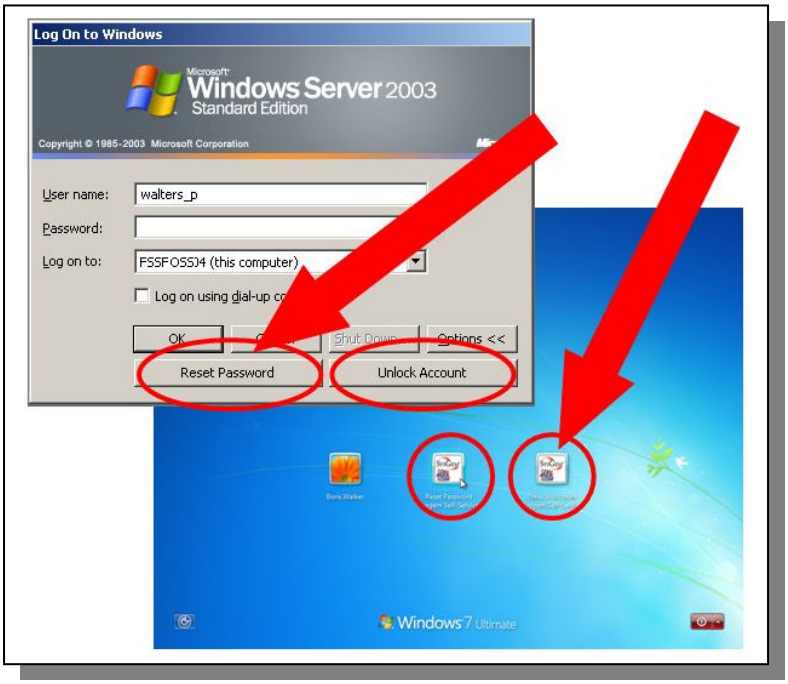
There are three components of *Sysgem Self-Service Password Reset* that are to be installed. The central service should typically reside on the domain controller; the web enrolment system can be installed on any IIS server in the domain; and the workstation component should be installed on all end-user workstations to allow users to reset their password on demand. Note that *Sysgem Self-Service Password Reset* does not work in a Windows "Workgroup" environment.

The Domain Controller runs a Windows Service which carries out the operation of resetting passwords for end-users. It also holds a database of Questions and Answers, which are created by the end-users themselves, and subsequently used to verify the authenticity of the person wishing to reset their own password.

The web enrolment system provides a web interface to the questions and answers database held on the domain controller, allowing users to log in at any time and modify their security questions.

The workstation component installs two additional buttons on the normal Windows logon screen:

- Reset Password
- Unlock Account



If a user forgets his password then selecting the “Reset Password” button on a workstation where *Sysgem Self-Service Password Reset* has been installed will allow him to change his own password after he has correctly answered his prepared questions. If the account is locked because he has tried repeatedly, too many times, to log in with an incorrect password, then he can unlock his account by using the “Unlock Account” button and again replying to the security questions.

1.2 Pre-requisites

The web enrolment component of *Sysgem Self-Service Password Reset* requires Microsoft Internet Information Services (IIS) to be installed before the installation begins. If it is not, the following error window will be displayed and the installation must be aborted and restarted after IIS has been installed.

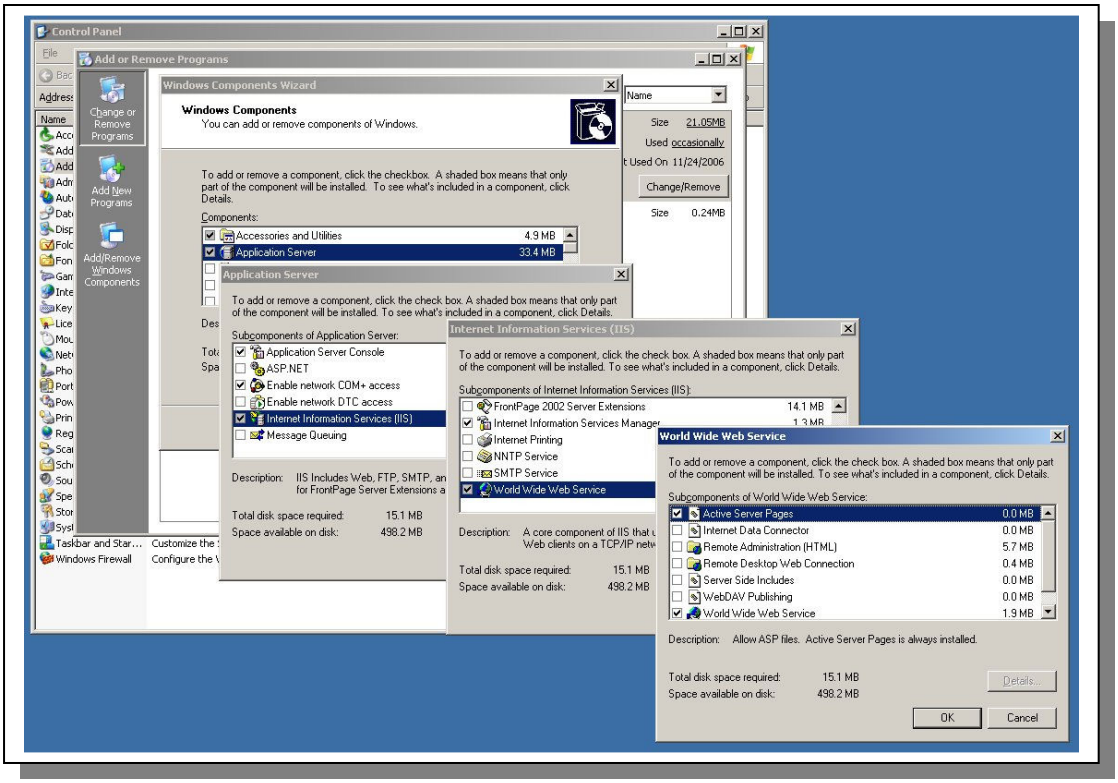
1.3 Internet Information Services, Minimum Settings

Internet Information Services (IIS) should be configured using Windows Administrator tools to allow Active Services Pages (ASP) scripting for the /pwdreset virtual directory created during installation.

For Windows 2003 / IIS 6, ensure that the “Active Service Pages” is enabled before the installation of Self Service Password Reset commences by using the Windows Administrative tools:

- Control Panel
  - Add Remove Programs
    - Windows Components Wizard
      - Application Server
        - Internet Information Services (IIS)
          - World Wide Web Service
            - “ check the box: ‘Active Services Pages’ “ (see the following)

The following is a screenshot of the Windows 2003 installed components wizard:



For Windows 2008 / IIS 7, the following IIS features (listed in Bold) to be installed and enabled before the start of the Password Reset installation:

Web Management Tools
- IIS 6 Management Compatibility
  - * **IIS 6 Scripting Tools**
  - * **IIS 6 WMI Compatibility**
  - * **IIS 6 Metabase and IIS6 configuration compatibility**

World Wide Web Services
- Application Development Features
  - * **ASP**
  - * **ISAPI Extensions** (required by ASP)
- Common HTTP Features
  - * **Default Document**
  - * **Static Content**
- Security
  - * **Request Filtering** (required by ASP)
  - * **Windows Authentication** (optional, for single sign-on support in the web enrollment interface)

1.4 Example Installation – Domain Controller

1.4.1 Start the Installation

Browse for the installation kit and double click on the installation file.

1.4.2 Enter an 'Unpack' Password

The first question asked is for the 'Unpack password". Your supplier or Sysgem will be able to give you this password if you do not know it:

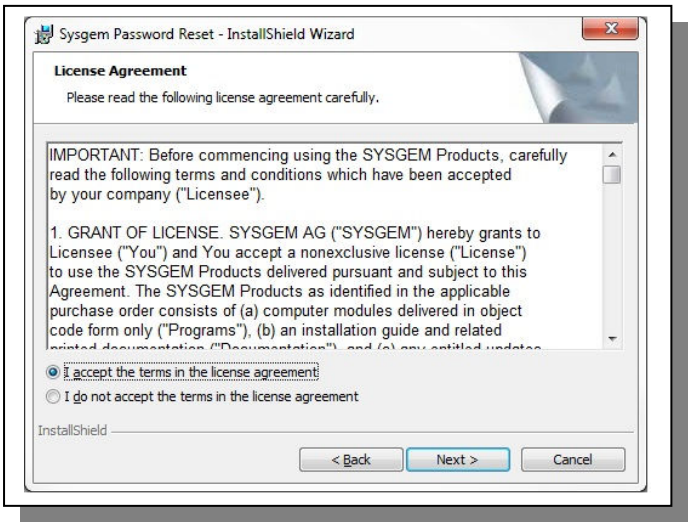
1.4.3 Welcome and Copyright

The following InstallShield welcome screen is displayed:

Press Next.

1.4.4 Accept License Agreement

Accept the license agreement, and press Next:

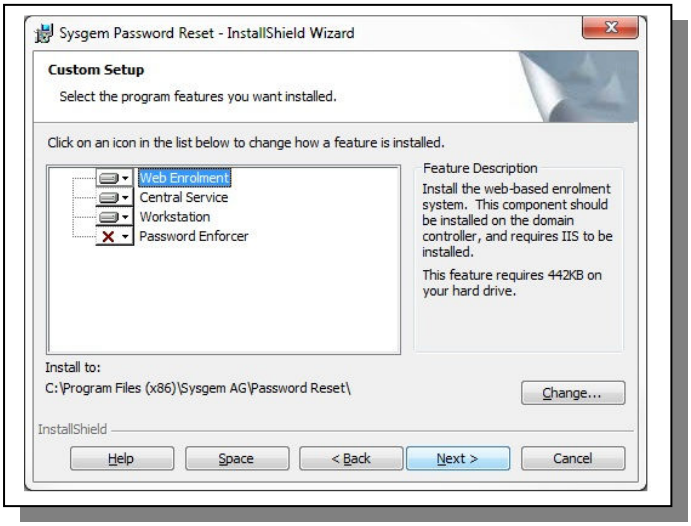


1.4.5 Custom Setup

Deselect the Workstation option (as shown in the screenshot). The workstation installation is described later.

The “Central Service” is installed on the Domain Controller.

The “Web Enrolment” component can be installed on the Domain Controller, however if the network is large, then you may want to consider installing the “Web Enrolment” component on a separate server to the Domain Controller.



1.4.6 Configure the Web Enrolment components:

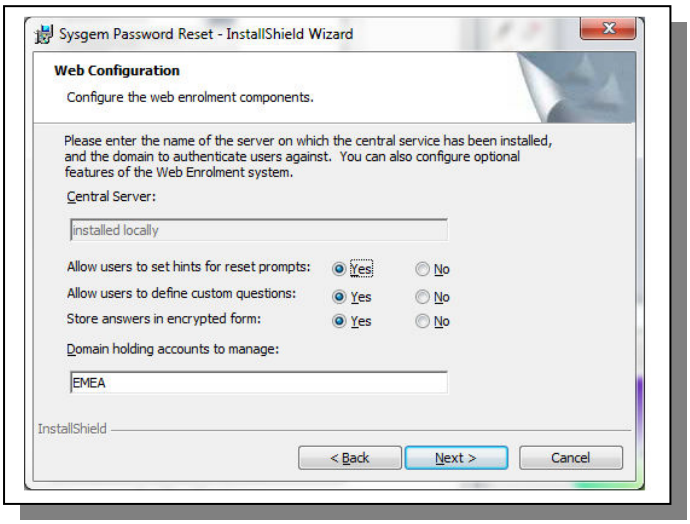
If the Web Enrolment component is installed on a separate server to the Central Service, then the server name of the machine that holds the Central Service (i.e. the Domain Controller) needs to be identified when installing the Web Enrolment component.

There are three configuration options that can be set at this point:

- Allow / disallow "hints": hints allow the user to define a set of prompts to be made for the set of security authentication questions.
- Allow / disallow custom questions: the administrator can elect to prevent users from defining their own security questions, instead only allowing the question to be selected from a list of presets.
- Store answers in encrypted format: by default, the answers to questions are stored under one-way encryption to prevent the discovery of a user's possibly sensitive information. This encryption can be disabled, for instance to allow for auditing of security responses.

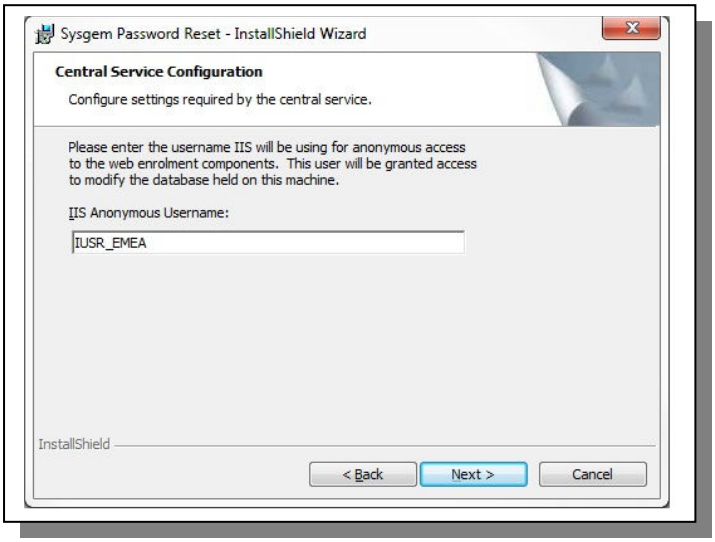
These settings can also be changed after the installation by modifying the configuration file held in the following location:

```
Program Files\Sysgem AG\Password Reset\Web\pwdreset.ini
```



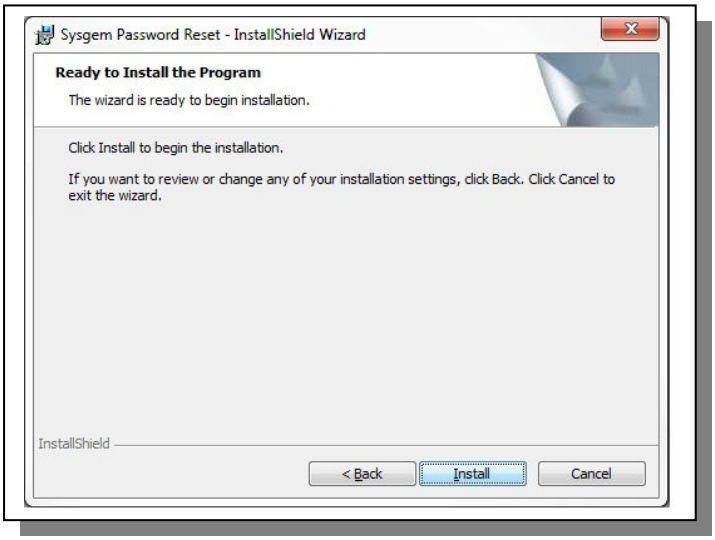
1.4.7 Configure the Central Service:

Enter the name of the Windows user account that is used to access this computer when an anonymous user connects to the site. In Windows versions prior to Windows Server 2008, this is normally the name of the computer with a prefix of "IUSR_". In Windows Server 2008 and later the name of the account is usually just "IUSR. If in doubt examine the "Default Web Site" Properties under the Internet Services Manager.



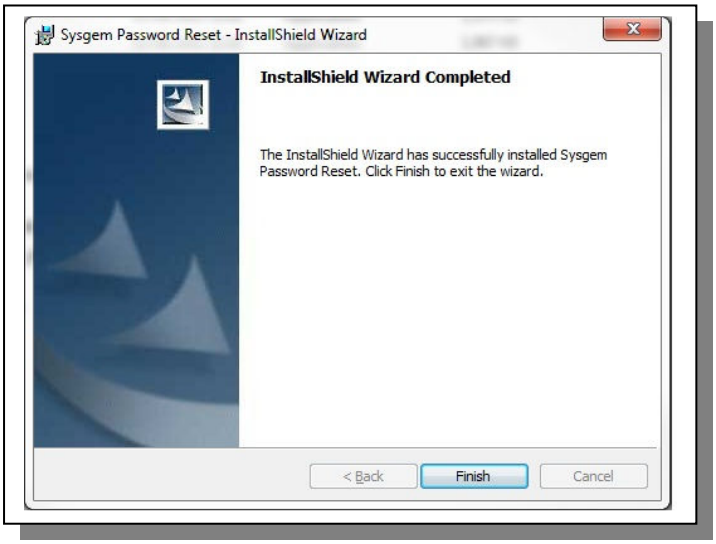
1.4.8 Ready to Install

You are now ready to complete the installation; press “Install” to proceed.



1.4.9 Progress and Finish

The installation will now progress to completion.



1.5 Installation – Workstation

Follow the same steps as for the Domain Controller installation, except in the Custom Setup window select the "Workstation" option instead of "Web Enrolment" and "Central Service".

The workstation component can also be installed independently and automatically, using an MSI file available from Sysgem or your distributor. In most cases, this MSI file can simply be installed using whatever deployment system you have in place on your network for distributing software upgrades. The installation will assume the Central Service is installed on the domain controller by default; this can be overridden by specifying a server name in the CENTRALSERVER property.

For example, to silently install the workstation components from the command line:

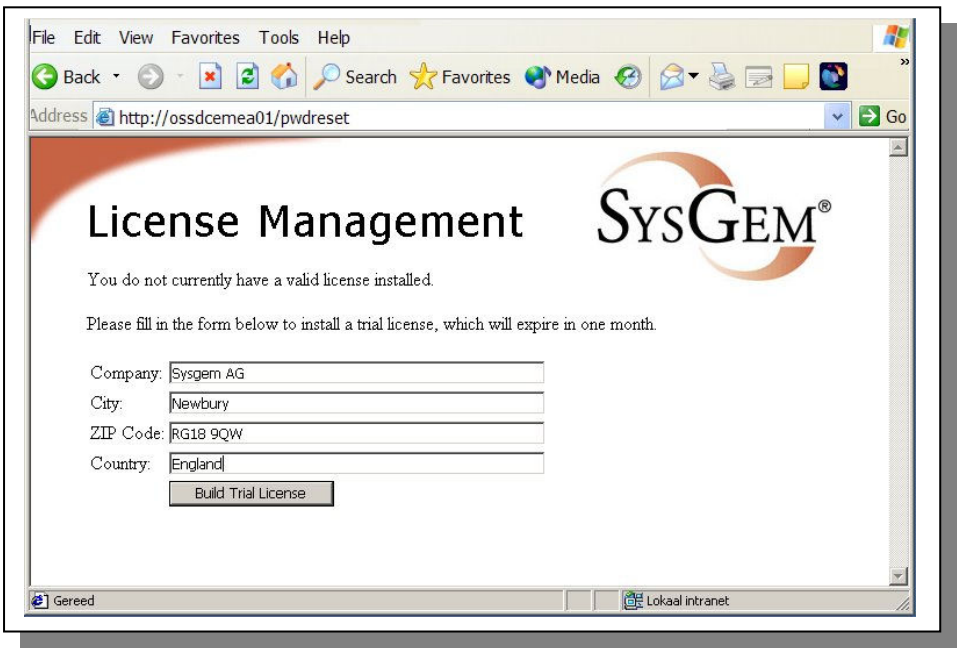
```
MSIEXEC /i X:\Apps\SysgemPasswordReset_workstation.msi /q CENTRALSERVER=SALES_DC
```

1.6 License Management

After *Sysgem Self-Service Password Reset* has been installed the product needs to be licensed. To do this, log into Windows and start a web browser. Enter the following address:

```
http://<Web Server Name>/pwdreset/
```

(*<Web Server Name>* is the name of the Windows machine where the web enrolment component has been installed).



Enter your company's details and press the "Build Trial License" button. A license file will be created on the web server, and the license information will be displayed in the License Management page. This page can be reached at any time by opening the following URL:

```
http://<Web Server Name>/pwdreset/license.asp
```

Your trial license will expire one month after installation; at this point, the web enrolment system will stop allowing logins and end-users will be unable to change their configured questions. The "Reset Password" and "Unlock Account" functions on workstations will be unaffected.

To request that the trial license be extended, send the license file to your Sysgem supplier and the file will be returned with either an extended expiry date, or a non-terminating expiry date. The location of the file on the web server is shown under the Export License heading on the License Management page; the default location is:

```
Program Files\Sysgem AG\Password Reset\Web\license.txt
```

After you have received an updated license, this file needs to be copied back into the location shown in the previous paragraph before following the instructions under the Import License heading on the License Management page:

1.7 Required Permissions and Troubleshooting

To aid in troubleshooting problems with an installation, the security permissions required by various components are described below.

1.7.1 Central Service

The central service is responsible for resetting passwords and clearing account lockouts, and as such needs administrative rights over the domain. It is recommended that the service is run as a Domain Administrator account.

The central service also holds the database of users' questions and answers. This database is typically stored in the `SEMPwdResetSvr.txt` file in the following directory on the machine where the central service is installed:

```
Program Files\Sysgem AG\Password Reset\Database
```

The permissions on this file should be set so that the web enrolment system can read from and write to the file. For details on determining or changing the username that the web server will use to access the file, see the section below.

When the web enrolment system has been installed on a different machine, the directory containing the database file is also shared using the share name `SysgemPasswordReset$`.

1.7.2 Web Enrolment System

The web enrolment system runs as ASP pages within Microsoft IIS, and by default is configured to use IIS's Anonymous access. On a typical IIS installation, the anonymous account is called `IUSR_<machinename>`; this value can be checked by:

- opening Internet Information Services Manager (for IIS 6) or Internet Services Manager (for previous versions);
- right-clicking on the `/pwdreset` virtual directory (under Default Web Site) and selecting Properties;
- clicking the first Edit button on the Directory Security tab;
- either noting the account name listed under Enable Anonymous Access (for IIS 6), or after clicking Edit under Anonymous Access (IIS 5 or older).

It is recommended that the machine running the web enrolment system is a member of the domain, and that the account being used for anonymous access is a domain account.

To ensure the web enrolment system has access to the question database file, check the `pwdreset.ini` file (typically in `Program Files\Sysgem AG\Password Reset\Web`) for a `DatabaseLocation=` directive. If the database is located on another machine, the path listed should be of the form:

```
DatabaseLocation=\\machinename\SysgemPasswordReset$
```

where `machinename` is the name of the machine on which the central service was installed. The file `\\machinename\SysgemPasswordReset$\SEMPwdResetSvr.txt` should be accessible by the user IIS is using for anonymous access.

The `Program Files\Sysgem AG\Password Reset\Web\license.txt` file on the web server should also be writable by the anonymous user account, as it is overwritten with a trial license when the web system is first accessed.

1.7.3 Two Stage Reset

To ensure that the password history is maintained, a 'two stage' reset operation is performed, but sometimes this can give problems which may result in the following message being displayed to the user who is trying to reset their password:

> *"Configuration information could not be read from the Domain Controller, either because the machine is unavailable, or access has been denied".*

To overcome the problem and disable the 'two-stage' reset, add the following entry to the registry where the Password Reset 'Central Server' has been installed:

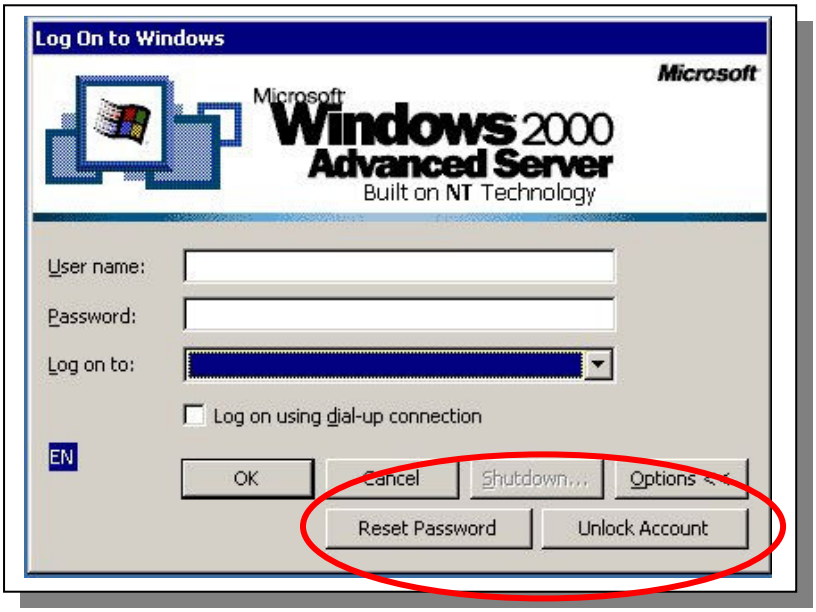
Key: HKEY_LOCAL_MACHINE\Software\Sysgem AG\Sysgem Password Reset
Value: TwoStageReset
Type: DWORD
Data: 00000000

2 User Guide

2.1 Introduction

Sysgem Self-Service Password Reset solves the problem of end-users forgetting their Windows login passwords and having to ask the helpdesk or the system administrator to reset it. With *Sysgem Self-Service Password Reset* users can reset their own passwords after correctly replying to security questions with answers that they have previously defined themselves.

You first need to enrol with the service whilst being logged into your account. Thereafter, if you forget your password you can reset it yourself using the "Reset Password" button on the login screen:



2.2 Enrolment

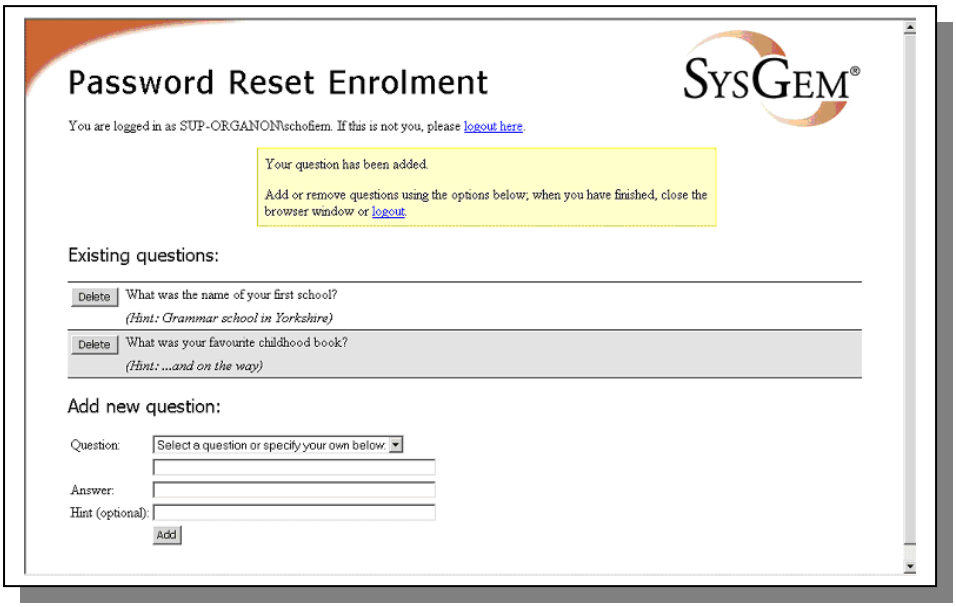
To set up the security authentication questions and answers, you need to visit the following address using a web browser:

```
http://<Web Server Name>/pwdreset/
```

where <Web Server Name> is either the name of your domain controller or another web server on your network. If in doubt, your network administrator can provide this.

This gives the following login screen within the web browser:

Enter your Windows username and password and press the "Login" button. The Enrolment screen will be displayed:

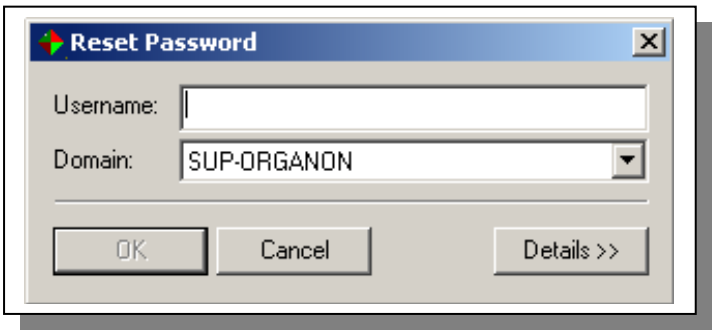


New questions, hints and answers may be added, and old ones may be deleted. When you use *Sysgem Self-Service Password Reset* to reset your password, you will need to answer all the questions correctly.

2.3 Resetting Forgotten Passwords

If you forget your password to your Windows user account then you can change it to a new password using *Sysgem Self-Service Password Reset* as follows:

On the Windows login screen (see above) of a workstation that has *Sysgem Self-Service Password Reset* installed, press the "Reset Password" button. The following screen will be shown:



Enter your username (and select the Domain). Each of the questions you have included in your list of security authentication questions will now be displayed, one at a time, in the following window:

Enter each question correctly and you will be able to enter and confirm a new password. This password will be set into your Windows user account, and you can then immediately log into the account with the new password. If, however, you have repeatedly tried and failed to log in with an incorrect password, then your account may be "locked". In this case you will need to unlock it using the "Unlock Password" button from the Windows login screen (shown above).

If you press the "Unlock Password" button then the same dialogue windows (as described for Password Reset) are shown. The same security questions need to be answered again.

When you log in for the first time after resetting your password, you will be asked to change your password once more – since your account has been set as "Password Expired". Setting the password on this occasion will follow the full password policy rules normally applied on your system.