



assystReset FAQ



Document Control

Project Name	assystReset by Axios Systems			
Customer Name				
Document Name	assystReset FAQ.docx			
Author	Greg Morgan			
Distribution	External - Customers - Prospects		Axios Systems - AGS - Business Partners	
Version History	Version	Date	Description	Sign - Off
	0.0.1	01/067/2011	Draft	Greg Morgan
	0.0.2	03/06/2011	Amendments	Greg Morgan
	0.0.3	01/07/2011	Released	Greg Morgan
	1.0.0	30/07/2011	Amendments	Mike Weymss
	1.0.1	01/08/2011	Published	Greg Morgan

Copyright Notice

© Copyright Axios Systems 2011. The information contained in this document is the property of Axios Systems Ltd. The contents of the document must not be reproduced or disclosed wholly or in part or used for purposes other than that for which it is supplied without the prior written permission of Axios Systems Ltd.

Contents

Solution Overview	4
Functional Requirement Q & A	5
Can you describe the user experience when unlocking or resetting a domain password from the Windows Logon Screen?	6
Cab you describe how assystReset will restrict access when incorrect answers have been entered into the Password Reset Tool and how many log in attempts are available before access is restricted?	8
Can you describe assystReset’s compatibility with an existing Password Policy (e.g. 1 upper case character, 1 numeric value and a minimum of 6 characters e.g. pAssw0rd)	9
How do users access and update pre populated questions and answers via a secure website?	9
How domain administration accounts are excluded from the password management tool?.....	11
What reports are generated by assystReset?	11
How is assystReset backed up and users’ questions and answers restored?	12
What are assystResets security features? in particular the security of users personal questions and answers	12
Can assystReset be scaled for an organisation of 3000+ users?	12
What support is provided for the product and where is it located?.....	12
Can you describe the User Management process?	12
What are the training requirements for your product?	13
Local Alliance Partner Information	13

Solution Overview

assystReset is a password management tool that allows users to reset their Windows password without having to contact their IT department, removing what many people believe is the number one call to a Service Desk. assystReset is straightforward to configure, easy to use, and is a safe and secure way for users to reset their password whenever they need to.

Many customers have highlighted the need for a password management tool which provides the following capabilities:

- 24/7 password reset - users can quickly and successfully reset forgotten or expired passwords even when the Service Desk is unavailable.
- Authentication through a challenge - response interaction
- Provision of an intuitive interface eliminating need for extensive user training
- Ability to meet all organisational Security Policies
- Assistance in complying with Government regulatory requirements

Once assystReset has been installed and configured, users are prompted to setup some Questions and Answers (Q&As). Once they have supplied these Q&As they can then reset their password in the future, by clicking on the "Reset" button on the logon screen. They will be prompted to answer the questions and, assuming they do so correctly, they will be able to reset their password without logging in.

This is an unobtrusive deep integration into the core of the Windows Active Directory. The deep integration provides the familiar user logon screen with an additional option - to reset their password. Delivering this feature through the standard native and familiar interface provides the user with the intuitive windows interface which eliminates the need for extensive user training. Providing it through the standard interface ensures everyone has access to it in a consistent and familiar way. For users not initially connected to the domain for authentication, a secure website provides an alternative method for changing their password.

Being provisioned through the Microsoft Active Directory it ensures that any defined security policies configured for the domain are still enforced, ensuring that all defined organisational security policies are met.

Using an automated mechanism for password resets provides a greater level of governance and auditability. It also provides the ability to meet any regulatory requirement, which may be defined from time to time by government agencies.

The assystReset solution proposes the following features and functionality.

- assystReset allows users to reset their Active Directory password in a single domain.
- On a successful password reset, a locked account will be automatically unlocked.
- Administrators define one, two or three Standard Questions, which a user must answer before they can see their Personal Questions.
- Users define their own three Personal Questions, making it easier for them to answer correctly in the future.
- Fully integrated into the logon sequence, allowing users to reset their password from their own workstation, without having to logon and without requiring a dedicated "Password Reset Workstation".
- Web-based application allowing users to set their Questions and Answers and to reset their password.
- Administrators can tailor any message that is displayed to the user, to provide their own additional help (for example, to list a Service Desk telephone number).
- Support for any language and locale on the desktop.
- Administrators can add their own non-English translations for any language.
- Fully secure application, with data transmitted across SSL and answers stored as non-decryptable MD5 double-hashed data.

- (Optional) Full integration with the assyst ITSM solution, allowing administrators to configure support to log and even automatically close Incidents for successful or failed password resets (and providing greater reporting coverage).
- (Optional) Automated incident logging to the assyst ITSM solution ensures that Service Desk can demonstrate an increased number of First-Time-Fix incidents, adding to overall greater customer satisfaction.

Functional Requirement Q & A

How is assystReset compatible with the following technologies?

Technology	Compatibility
Active Directory 2003 / Active Directory 2008 R2 on 64-bit	assystReset relies on a Windows Active Directory domain to provide the listing of users and the primary user authentication mechanism. assystReset is compatible with AD 2003 and AD 2008 directory schemas. Both platforms of 32bit or 64bit are supported. assystReset must be installed on a Domain Controller. assystReset can be configured with additional assystReset servers to manage additional AD domains.
Windows Server 2008 R2	assystReset will operate with and is compatible with Windows 2008 R2.
Microsoft Internet Explorer 8.0, Microsoft Internet Explorer 6.0 and any other browsers	assystReset web interface can be accessed via MS IE 6, 7, 8 and 9. The Web interface is also accessible via any standard browser that supports HTTP over SSL (HTTPS), for example Firefox 2 and 3, Google Chrome and Safari. A native Windows interface deeply integrated into the core of the Operating System is also provided to compliment the web interface.
Microsoft Windows 7 and Microsoft XP Service Pack 3	assystReset deeply integrates with the core of the Windows operating system. In Windows XP and earlier the GINA is used, and Windows 7 the Credentials Provider is used. assystReset provides a chainable GINA for windows versions that use this approach. assystReset provides a pluggable Credentials Provider for windows versions that use this approach. Windows XP is supported in 32 bit while Windows 7 is supported in both 32 and 64 bit.
Citrix and Microsoft Forefront UAG (MyRemote)	Citrix environments correctly pass-through credential management to the target machine. If the target machine is installed with the relevant assystReset client, then assyst Reset will interoperate in its native form (via the Windows interface), as an additional backup to this, the secure website will be available to manage passwords. Forefront Unified Access Gateway (MyRemote) correctly pass-through credential management to the target

	<p>machine. If the target machine is installed with the relevant assystReset client, then assystReset will interoperate in its native form (via the Windows interface), as an additional backup to this, the secure website will be available to manage passwords.</p>
<p>Microsoft .Net Framework 4.0</p>	<p>assystReset is fully compatible with the .Net Framework 4.0.</p>
<p>Microsoft Internet Information Services (IIS) 7.5</p>	<p>assystReset relies on a Microsoft Internet Information Services IIS web server. Version 7.0 and 7.5 are supported</p>
<p>Microsoft SQL Server 2008 R2 64-bit</p>	<p>assystReset relies on a Microsoft SQL Server database as its primary data repository. Version 2008 R2 64-bit is supported. An alternative of MS SQL Express is also supported, although this has limitations to size and scalability.</p>
<p>Microsoft Remote Desktop Services and Microsoft RemoteApp</p>	<p>Microsoft Remote Desktop Connection (RDC) / Services correctly pass-through credential management to the target machine. If the target machine is installed with the relevant assystReset client, then assyst Reset will interoperate in its native form (via the Windows interface), as an additional backup to this, the secure website will be available to manage passwords.</p>
<p>Inline transparent proxy and Caching proxy</p>	<p>assystReset supports inline Transparent proxy and Caching proxy with the following conditions;</p> <p>Inline transparent proxy to pass through all HTTP over SSL communication requests directly to the assystReset URL on the configured port (443 by default).</p> <p>Caching proxy respects the 'HTTP-EQUIV' headers in particular the 'Pragma: No-Cache' metatag. Preventing the caching of assystReset password reset web pages.</p>
<p>VMWare ESX 4.1i</p>	<p>VMWare ESX 4.x environments correctly pass-through credential management to the target machine. If the target machine is installed with the relevant assystReset client, then assyst Reset will interoperate in its native form (via the Windows interface), as an additional backup to this, the secure website will be available to manage passwords.</p>

Can you describe the user experience when unlocking or resetting a domain password from the Windows Logon Screen?

With assystReset, on the Windows Logon Screen, the user will see an option to reset their password. This experience varies slightly for the different versions of Windows that might be in use, but the process remains the same.

A User goes through a simple 4 step process.

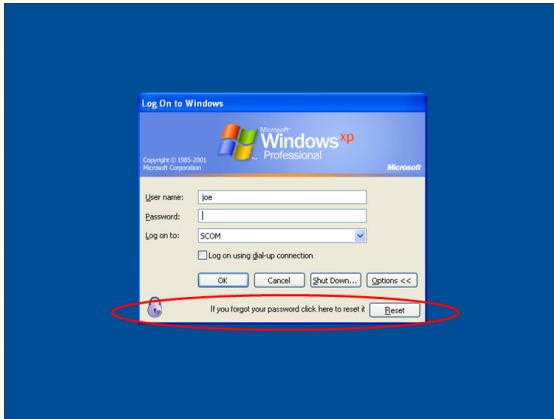
1. Click the Button or Link to begin the password reset process.

2. Answer the General Questions (questions everyone is required to answer), these questions are defined globally, and answers are unique to the user.
3. Answer the Personal Questions (questions that the user must define and answer), these are unique questions and answers per user.
4. Enter a new password.

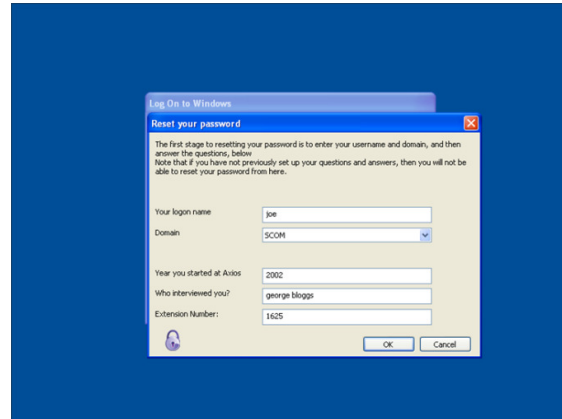
Assuming the user answers all questions correctly, the password will be reset to the newly entered password. This password will need to conform to any defined Windows password strength requirements. Onscreen instructions guide the user through the steps involved. If answers are incorrect it will not proceed onto the next steps, limiting the ability to block a user's account through multiple incorrect attempts. Incorrect attempts at password changing are logged and recorded in the audit trail.

In Windows up to Windows XP the Graphical Identification and Authentication (GINA) was used to log users into Windows. In more recent versions of Windows (Vista and Windows 7) the Credentials Provider is used. Each has slightly different methods of displaying the assystReset functionality, and this is best shown in some screen grabs.

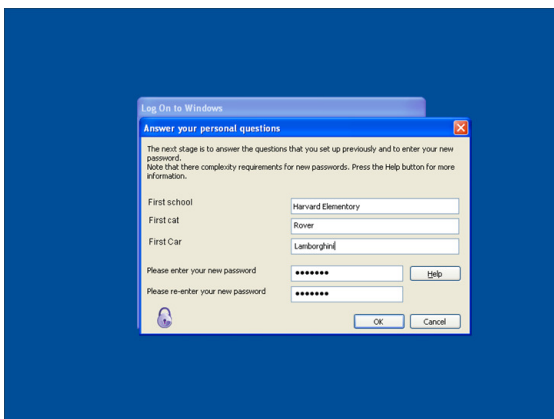
Windows using GINA (NT3.51, 4.0, 2000 and XP).



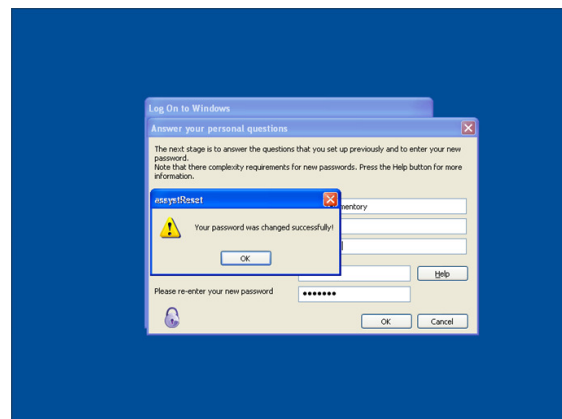
Screen 1 - Windows Logon Screen, this shows an additional “Reset” button to reset the user password.



Screen 2 - General Questions, are answered. Everyone is asked to answer 3 general questions which are system wide.

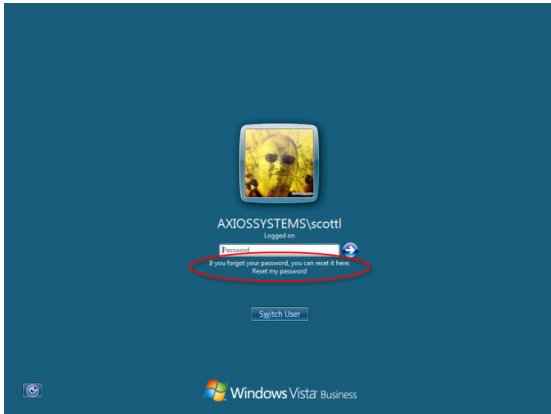


Screen 3 - Personal Questions & Password. Everyone is also offered the ability to store and record 3 personal questions and answers, which must also be answered in the reset cycle.

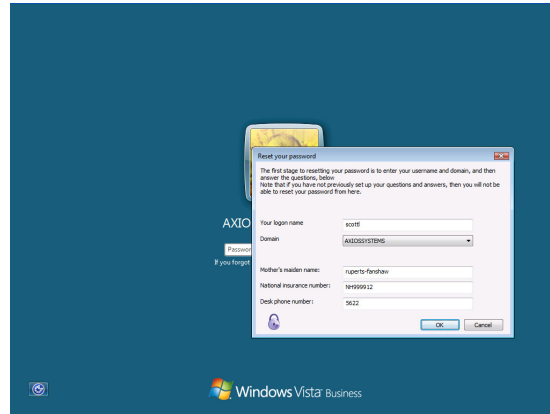


Screen 4 - Password is reset. After the new password is entered in the previous screen, the password is reset or unlocked, which depends on security policies in place.

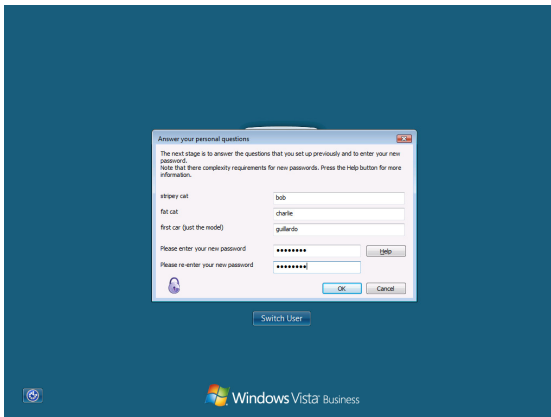
Windows using Credentials Provider (Vista and 7)



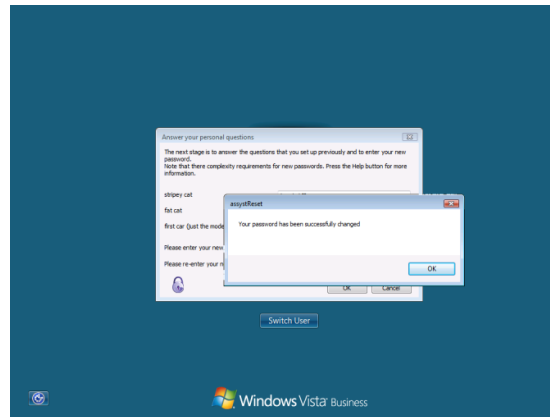
Screen 1 - Windows Logon Screen, this shows an additional “Reset my password” text to reset the user password.



Screen 2 - General Questions, are answered. Everyone is asked to answer 3 general questions which are system wide.



Screen 3 - Personal Questions & Password. Everyone is also offered the ability to store and record 3 personal questions and answers, which must also be answered in the reset cycle.



Screen 4 - Password is reset. After the new password is entered in the previous screen, the password is reset or unlocked, which depends on security policies in place.

Can you describe how assystReset will restrict access when incorrect answers have been entered into the Password Reset Tool and how many log in attempts are available before access is restricted?

Using assystReset we already assume the user account is restricted in some way. The account is either locked out due to incorrect login attempts or the user has forgotten their password and is receiving a message to that cause. In either of these approaches the legitimate user cannot access their account.

The password reset process described in answer 4.2.2 (above) outlines the steps required in order to reset a password. If during the general Question and Answer stage (Step 2) the user enters incorrect information it will not proceed onto the next step, Personal Questions and Answers (Step3). This mechanism facilitates a legitimate user needing to unlock/reset their password without restrictions on attempts.

An illegitimate user will not pass the first round of Question and Answer checks, and this will be recorded as a failed password reset attempt.

Restricting access to the password reset capability, when failed attempts are identified, will unnecessarily also restrict the legitimate user from resetting their password or unlocking their account. It is for this reason we do not restrict access to the password reset tool or interface.

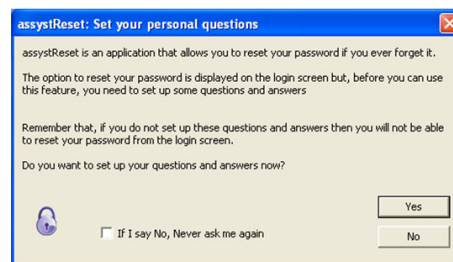
Can you describe assystReset's compatibility with an existing Password Policy (e.g. 1 upper case character, 1 numeric value and a minimum of 6 characters e.g. pAssw0rd)

assystReset conforms with any existing Windows defined password strength policy. If the current policy is defined within Windows Active Directory and the Windows Active Directory can enforce this policy (for example, 1 upper case character, 1 numeric value and a minimum of 6 characters e.g. pAssw0rd), then assystReset will conform to it.

How do users access and update pre populated questions and answers via a secure website?

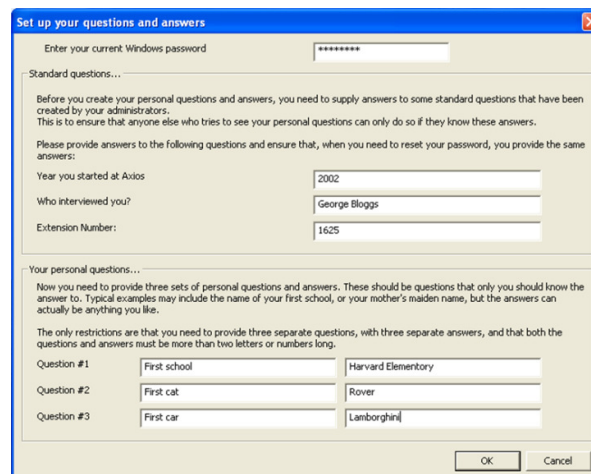
When assystReset is released to users for the first time it prompts users to setup and establish answers to general questions as well as setup personal questions and answers. This is performed within a standard Windows interface, and occurs right after login.

See screen shot (below) of user initiation of assystReset.



Once the user accepts to setup assystReset, they are prompted to enter their current password to verify themselves again. They then answer the general questions, they then define and answer their personal questions.

See screen shot (below) of the windows interface to user questions and answers in assystReset.



Once this information is entered the setup is complete the user has established the requirements for using assystReset.

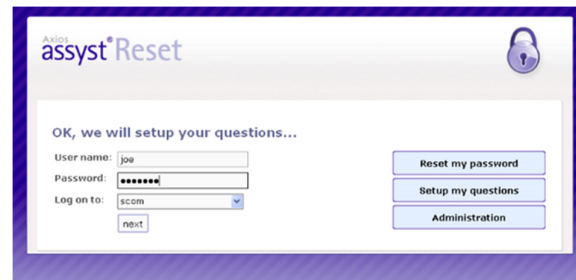
assystReset also provides a secure website with HTTP over SSL (HTTPS). The website is protected with an SSL certificate certified by a Certificate Authority within the organisations Active Directory. The secure website provides the ability for users to access and update answers to the general questions and personal questions and answers.

The screen shot (below) shows the initial welcome screen to the website for user setup, reset password, or administration.



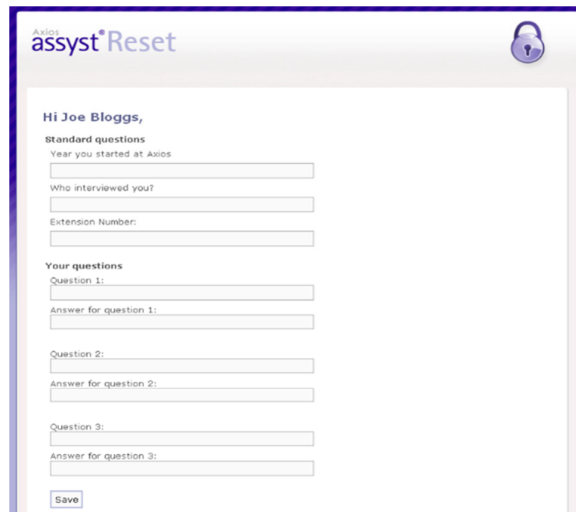
Following the “Setup my questions” path produces a login screen that requests the user authenticate against the Active Directory domain.

See screen shot (below) for the initial web login when setting up assystReset.



Finally the user is presented with a user screen that prompt the user for answers to the general questions and definition of the personal questions and answers.

See screen shot (below) of the web interface to user questions and answers in assystReset.



Once this information is entered the setup is complete the user has established the requirements for using assystReset.

How domain administration accounts are excluded from the password management tool?

User accounts that reside in the assystReset Administrative Group can be excluded from using the password management tool. Furthermore, the workstation component (agent footprint) can be excluded from installation on defined workstations, meaning it will not appear on servers or workstations in Administrative OUs within the Active Directory.

What reports are generated by assystReset?

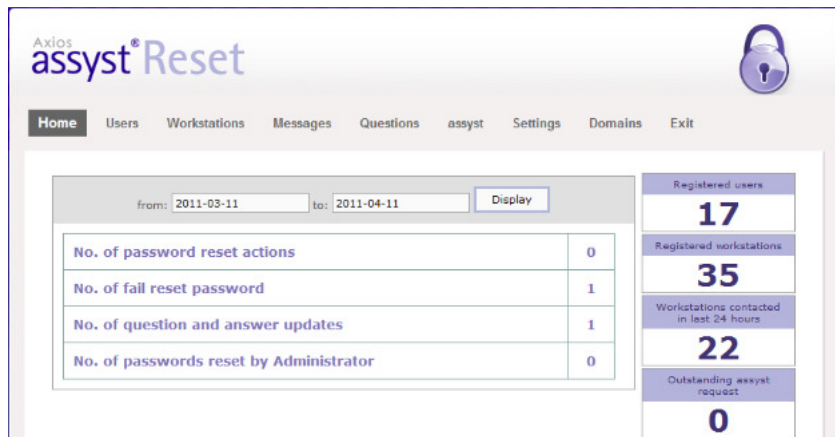
There are defined reports that are available from the solution including;

- Number of successful password resets performed by the user
- Number of unsuccessful password resets performed by the user
- Number of successful password resets performed by the Service Desk
- Number of unsuccessful password resets performed by the Service Desk

A range of dynamic (by date range) dashboards also display useful real-time statistics like;

- Number of Password reset actions
- Number of failed reset actions
- Number of questions and answer updates
- Number of passwords reset by Administrator (Service Desk)
- Number of Registered users
- Number of Registered workstations
- Number of workstation contacted (updated) in the last 24 hours
- Number of actions logged to the assyst ITSM solution

See the screen shot (below) for a view of the administrative display (dashboard) of current reported user information.



All information that is contained within the solution is able to be extracted and defined in static reports that can be scheduled to run at prescribed times.

With an optional integration with the assyst ITSM solution, additional reports are available.

How is assystReset backed up and users' questions and answers restored?

assystReset utilises an underlying Microsoft SQL database, backup and restore is performed via a backup solution that allows for online backup of the database. Any existing backup solution that provides this capability can be used.

What are assystResets security features? in particular the security of users personal questions and answers

assystReset provides a secure website with SSL encryption for web based activation and password management. The website uses an SSL certificate provided by a CA installed in the organisation's Active Directory. The windows interface provides a chained GINA for Windows XP and earlier and a pluggable Credentials Provider for Windows Vista and 7.

The SQL Server provides additional security in the form of username and passwords that can access the database directly. The content of the database is double hash MD5 encrypted ensuring answers to general questions and personal questions and answers are thoroughly protected from unwarranted access.

Can assystReset be scaled for an organisation of 3000+ users?

assystReset requires a very small footprint on user workstations. The timeframe that assystReset polls the server for updates can be configured, so that a large number of users and workstations does not overload the server. Additionally the assystReset server can be scaled to cater for increased demand and resilience. The demand on the assystReset server is relatively light, the main load is when users are registering themselves. This can be overcome by a staged release to selective workstations throughout the domain. The assystReset solution can be scaled appropriately to cater for any sized Active Directory user base.

What support is provided for the product and where is it located?

Axios Systems provides a 24 x 7 Service Desk to provide support to users. An extensive wiki based website also provides a great deal of user and administrative information to support the administration of the solution.

Local implementation and support of assystReset is provided by our local alliance partners.

If any onsite administration is required this will be relayed to our local partner who can carry out the required activities. If onsite support is required, representatives from the local partner office will attend.

Can you describe the User Management process?

assystReset provides a very simple yet comprehensive user management process. Users can perform three tasks related to their identity.

1. Establish their credentials with assystReset
2. Administer their credentials with assystReset
3. Reset their password (unlocking their account in the process) with assystReset

assystReset can be accessed via the secure native Windows interface using the Windows Login screen to access this method. assystReset can also be accessed via a secure website that provides the same features and functionality.

What are the training requirements for your product?

a. What is the overall approach to training?

Axios Systems and our partners prefer to look at the holistic approach of identity management and rather than just train the users in the use of another tool or function. At Axios Systems we opt to teach and inform people about identity management and this often leads to a greater cultural shift with greater awareness about password management as a result. With this in mind we aim to work with your staff to deliver an overall Socialisation and Awareness program for the new password reset service. The awareness program details several concepts that will drive user behaviour and reinforce the cultural shift towards self-management of user identity.

Concepts such as a staff awareness profile, which contains desk stickers, laminated Quick Reference Guides, Global screen savers which contain news and information about the new password reset functionality are but a few techniques to drive the message of the new service, and train the end user population.

Administration Staff will receive hands on training through the involvement in the actual implementation. Service Desk staff will receive instruction and documentation on the correct process for dealing with Service Desk assisted password resets.

b. What is the scope of the training programme?

Axios Systems or the local alliance partner will train local support staff and a Program Manager in the use of the tool and concepts of the socialisation and awareness program. Axios Systems or the local alliance partner will also train assystReset Administrators in the installation (through hands-on implementation shadowing) of the tool, and then with on-going management and maintenance of the solution. An Axios Systems or the local alliance partner consultant will also install and test the assystReset solution on a select range of computer workstations to ensure correct functionality. The Program Manager can then direct the staged release of the solution to other groups of people within the Active Directory.

End User Training will not be provided as part of the training programme.

c. Can you describe a sample training plan?

After the successful installation and testing of the assystReset solution (which approximates 5 days) the training can begin. A sample training plan with timeframe follows;

Day 1 - Workshop to define to map out the awareness campaign

Day 2 - Train Administrators on remaining solution functionality.

Day 3 - Train Program Manager and Support Staff on assystReset solution.

Depending on availability of the required organisational staff, some activities may be carried out in parallel with other components of the implementation.

For further Information about assystReset please contact your account manager or our local alliance partner.

Local Alliance Partner Information

Focus On Business (www.focusapac.com) has offices across Asia Pacific with their New Zealand office located in Auckland. They can be contacted at the following email address info@focusapac.com or telephone 09 363 9550.
