APTEAN

WHERE SOFTWARE WORKS

SUPPORTSOFT ACCOUNT MANAGER

DELIGHTING USERS, ONE PASSWORD AT A TIME!

WHITEPAPER

ABOUT

Enterprises continue to rely almost exclusively on passwords as a primary means for authenticating users, with the help desk as the primary mode of support for solving password related issues. Unfortunately, as security policies are strengthened and password complexity increases, the call volume into help desks increases and operating costs increase proportionately. *A level 1 (password reset) call to the help desk costs an estimated $25 or twice as much in case of some enterprises. Industry estimates often indicate that more than 30% of all call volume into help desks is password related, which easily makes password issue management the single most expensive activity for help desks. This cost is compounded by unproductive and dissatisfied users waiting to have passwords reset or accounts unlocked. Each time a help desk staff member has to reset a user's password, there is both a productivity cost and a security risk that the user's ID might have been compromised due to the possibility of analyst knowing the user password while resetting. Adding in the costs of lost opportunity from IT resources mired in password related activities instead of focusing on mission critical issues, the overall cost for password management skyrockets.

SupportSoft Account Manager is a convenient and safe self-service automated password solution that empowers users with the ability to perform password related activities such as password reset, account unlocking and more on their own without any assistance from the help desk.

Account Manager is part of the SupportSoft eService Suite and takes care of every aspect of password self-service, right from guiding the end-user in devising stronger security answers to performing a safe and easy password reset.

This whitepaper discusses Account Manager capabilities and also covers a customer case study on how SupportSoft Account Manager was used to considerably reduce password related issues and boost end-user satisfaction. It also demonstrates the high Return on Investment (ROI) and quick payback interval offered by the software.

*Datasource: Gartner, Help Desk Institute

BUSINESS CHALLENGES FACED & HOW ACCOUNT MANAGER ADDRESSES BUSINESS CHALLENGES

When it comes to password security, Account Manager trusts **no one!**

Passwords are the quintessential blocks of any data security structure. Mighty organizations have different layers of data security and passwords rest at the base shielding gallons of important information. Manually managing large number of user passwords and handling the imminent challenges they pose can be a herculean task all together. All this funnels down to one question:
Is there a better way of doing this?

Aptean's Account Manager is the one-stop solution to all password related issues. The table below provides clarity on various password related challenges encountered during system locking and unlocking process and how Account Manager addresses each one of them.

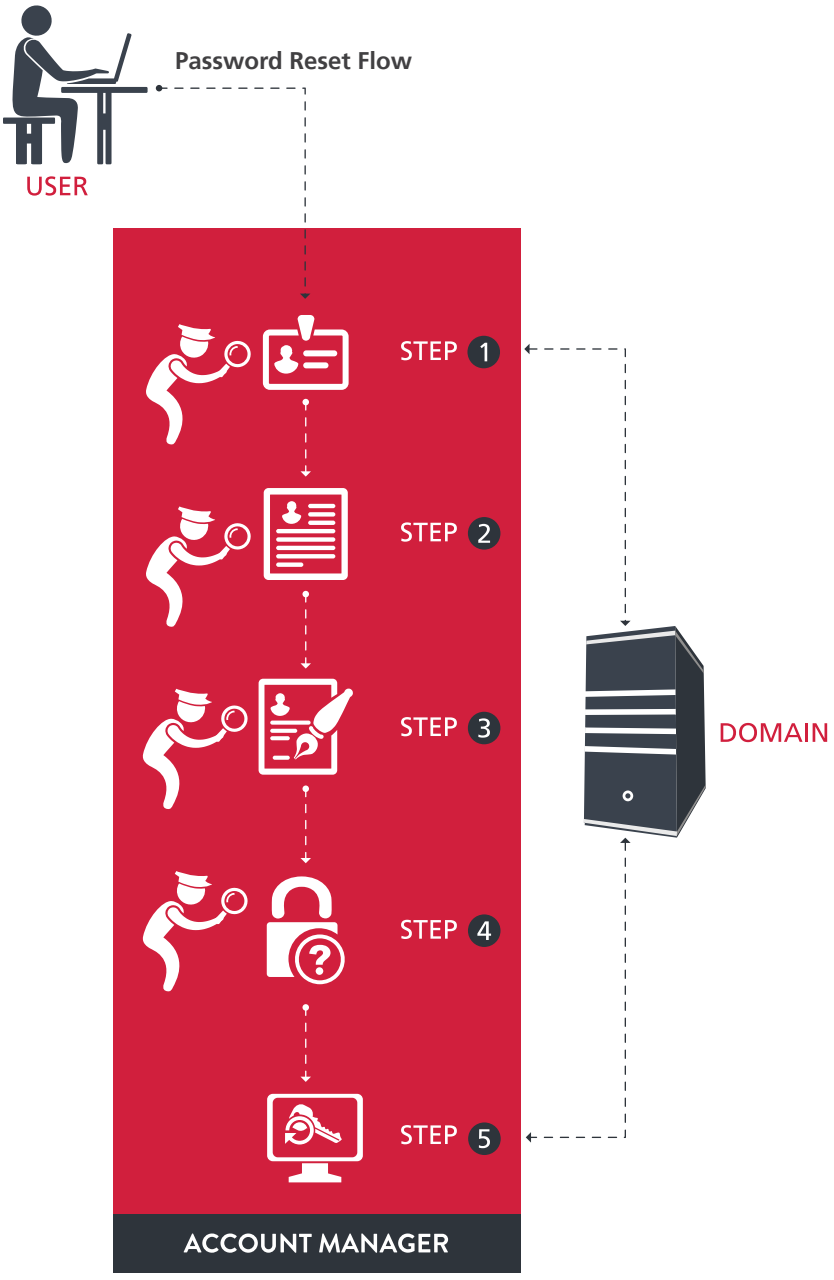
Challenges	Account Manager (AM) Solution
Weak passwords set by users Often, end-users intentionally or unknowingly treat the process of creating security answers as a tiresome or uninteresting activity. Hence, they create security questions that are easy and hackable. To prevent this, users must be compelled to set stronger passwords.	**AM offers 'Controls' that assist end-users in creating security/ challenge answers that cannot be easily hacked** Account Manager guides end-users with predefined controls by: • Disallowing users from using a 'word' from the 'question' in their answers. • Disallowing users from giving identical answers to more than one question. • Disallowing users from using the same security question multiple times. • Disallowing users from changing the challenge/security questions. • Enforcing users to adhere to the rules defined by administrators. • Imposing mandatory security questions. • Restricting users from using their previous passwords. • Allowing users (belonging to the same Account Manager's business unit) to reset or unlock their accounts even if they are moved to a different OU (Organizational Unit). • Configuring the number of questions to be answered by the user during a password reset or unlock. This is a random sub-set of the number of questions the user has registered to.
Hackable security answers During data transfers, there is a real risk of data/security breach. There is a need for stronger measures to forbid unauthorized access & to maintain user privacy.	**Security answers are hashed and can no way be retrieved by anyone** • Uses an industry standard hashing algorithm for safeguarding privacy. • Security answers cannot be retrieved during transmit or when stored in the database. • Even the administrator is disallowed from retrieving the passwords.

Challenges	Account Manager (AM) Solution
Man-in-the-middle attacks Anybody aware of security related information can pose a threat or cause security breach. Even in case of support analysts verifying security answers, the risk of information theft continues to exist	**Powerful protocols that create impassable communication platforms** • Uses HTTP over SSL for safer connections between users (web browser) and Account Manager. • Uses LDAP over SSL for secure data transfer between Active Directory and Account Manager.
Password brute force cracking Hackers try out various combinations of a password on a trial and error basis to gain unauthorized access to the system. In a brute force attack, automated software is used to generate a large number of consecutive guesses. This method is generally used by criminals to crack encrypted data or by security analysts to test an organization's network.	**Administrator controls to monitor attempt counts and verify authenticity** • Allows the administrator to define a threshold for number of invalid attempts allowed, after which the user is blocked for a specified duration. • Administrators can also configure the duration for a user to remain locked-out on failing the identification verification process. • Account Manager also includes a feature to display security questions one by one.
Cross-site scripting Cross-site scripting (XSS) is a security threat where hackers insert malicious code into a link that appears to be from a trusted entity. When the user clicks on the link, the embedded programming is transferred as part of the client's web request and can run on the user's system allowing the attacker to steal information.	**Anti-forgery tokens to avoid information theft** AM follows the best practice of using ASP.NET MVC anti-forgery tokens called request verification tokens to prevent cross-site scripting in the application.
SQL code injection Hackers use specially designed query strings which take advantage of vulnerabilities in SQL and attack the application to get access to information.	**Strong input validation to prevent SQL injection** AM supports the use of strong input validation (complete information) by the user which disallows hackers from injecting query strings to access information.

PASSWORD MANAGEMENT FLOW

Getting started with Account Manager involves the following simple steps:

- User can perform all password related activities by clicking on the options available on the Windows Logon screen or with an easy to access icon available on the home screen.
- Enrollment Process.
- Registering for the service.
- Choosing security questions from the list of questions defined by your administrator. Optionally, user may also create his/her own questions and enter the answers if the facility is available.



Step 1: Domain user status verification
The user enters his/her username and domain name. Account Manager checks if the user is valid and exists in the domain.

Step 2: Enrollment status verification
If the user is valid, Account Manager checks if the user is enrolled for the selected Account Manager service.

Step 3: Policy setting verification
Thereafter, if the user is enrolled, Account Manager checks the policy setting for the user. It checks if the user is allowed to do the operation.

Step 4: Identity check through security questions
After verifying the policy settings, Account Manager retrieves the security questions defined for the user and displays them to the user according to the settings. The answers are validated against the answers provided by the user during enrollment.

Step 5: Password management phase
If the security answers provided are correct, the password management page is displayed and allows the user to perform activities such as reset password, account unlocking and others.

CASE STUDY

This case study discusses how one of the large IT Managed Service Providers leveraged SupportSoft Account Manager solution to solve password related issues in a major healthcare organization.

About MSP

A global technology company that delivers solutions across a wide range of verticals such as Automotive, Banking, Chemical, Energy and Utility, Consumer Electronics, Life Sciences, Healthcare and more. With more than 1,00,000 employees and a revenue of $5 billion, the organization operates in 31 countries across Americas, Europe, Asia Pacific, Middle East and Africa. It is also listed as one of the 21st century technology companies in the world.

About Healthcare organization

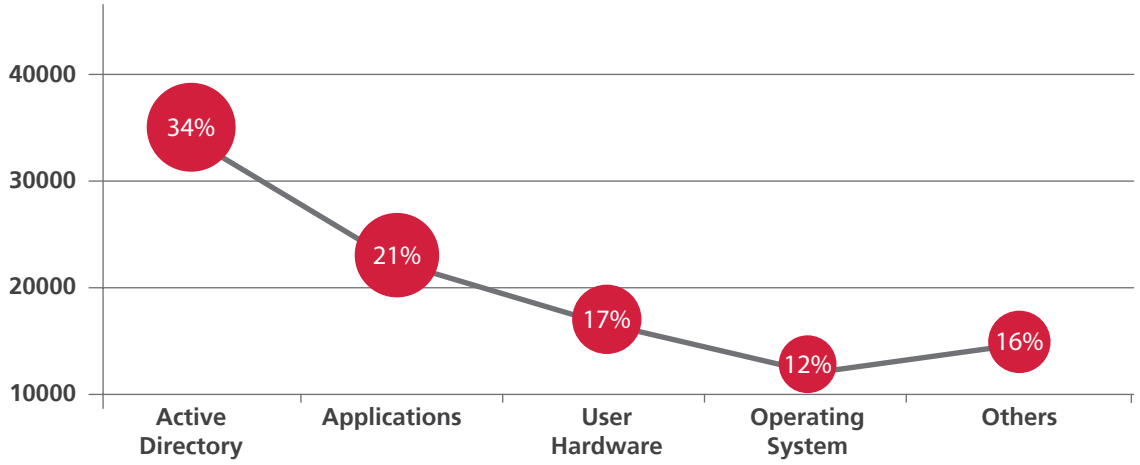
It is one of the leading health benefits companies transforming healthcare with trusted and caring solutions. With a total operating revenue of $73 billion, it serves nearly 71 million people through its affiliated companies including more than 38 million enrolled in its family of health plans.

Business challenge

The healthcare major which is home to a large, dynamic and rapidly growing workforce relied heavily on passwords as a primary means for authenticating users. As the workforce continued to grow in number, the call volume into help desks and operating cost increased proportionately. There was a need for an innovative solution that not only controlled the help desk cost but also provided a better support experience for the users. An analysis of the help desk calls revealed that 34% of the total support calls recorded at the help desk were related to password reset and account unlock. Adequate steps were required to address unproductive and dissatisfied users waiting to have password reset or accounts unlocked and in turn improve staff efficiency.

The table below provides details on the type of calls recorded at the help desk for a period of one month:

Category	Type	Item	Volume/Month	Percentage
Active Directory	**Domain**	**Password related**	**36300**	**34%**
Applications	SOE Software	Software	22421	21%
User Hardware	Computer	Laptop PC	18150	17%
Operating System	Windows	Configuration	12812	12%
Others	-	-	17082	16%
Total Records Categorized			**106765**	**100%**



Solution

SupportSoft Account Manager by Aptean provided the much needed powerful platform for the organization to tackle support problems efficiently. Account Manager served as a comprehensive password management solution that not only provided easy and secure self-service option for the users to reset their own passwords but significantly brought down the support cost, time and effort.

ACCOUNT MANAGER- A WISE CHOICE

ROI is a popularly used metric to evaluate the efficiency of an investment. This simple metric gives clear idea about the benefits (returns) of an investment. In this section, the ROI calculator has been used to measure the direct cost savings experienced by the healthcare major with the use of Account Manager. It clearly demonstrates the high Return on Investment (ROI) and quick payback period offered by the software.

Organizations strive towards keeping their costs low. The cost could be a direct or an indirect cost:

DIRECT COSTS

Direct costs are those costs that are directly related to a product or service. These costs are tangible and easily measureable. They include:

- Help desk (Agent) time spent in answering a query or addressing an issue.
- Saving in cost by deflecting a help desk call to self-service.

Savings in direct costs for an organization can be calculated.

INDIRECT COSTS

Indirect costs are losses incurred to an organization from factors that cannot be easily and conveniently traced to a product or service and are of far greater magnitude. They include:

- The opportunity cost that is lost in users waiting for a password reset, particularly when working on a critical project with strict deadlines- productivity loss.
- The cost of user information not being up-to-date when taking important business decisions, such as salary hikes, promotions or onsite opportunities.

These costs cannot be quantified.

PAYBACK PERIOD

Payback period is a simple financial performance measurement that determines the time it takes to recoup the original investment.

In order to show the ROI, following baseline assumptions have been made:

- Average hourly cost of an employee - $50
- Average hourly cost of Level 1 (L1) staff - $30
- Average hourly cost of Level 2 (L2) staff - $50

ROI CALCULATION

The table below calculates total cost incurred in an year for password related incidents with and without Account Manager (AM) solution:

	Without AM	With AM
Total number of users in the organization	128,000	
Average number of password incidents registered at help desk per year	435,600	**217,800***
DEFLECTING HELP DESK CALLS TO SELF-SERVICE		
% of password incidents solved by L1	75%	
Number of password incidents solved by L1 per year	326,700	163,350
Average time spent by L1 to solve a password incident (Minutes)	5	
Total L1 cost per incident (USD)	$2.50	
% of password incidents escalated to L2	25%	
Number of password incidents escalated to system administrators (L2) per year	108,900	54,450
Average time spent by L2 to solve a password incident (Minutes)	30	
Total L2 cost per incident (USD)	$25	
Total help desk cost per year (USD) for solving password incidents	$3,539,250	$1,769,625
Total savings for an year	**$1,769,625**	
USER PRODUCTIVITY GAIN		
Average hourly cost of an employee (USD)	$50	
Average time spent by the user to get a password incident solved with help desk support (Minutes)	15	
Average time spent by the user to get a password incident solved through AM (Minutes)	0	2
User productivity loss per year due to password related incidents (USD)	$5,445,000	$3,085,500
End-user productivity gain (USD)	**$2,359,500**	

ROI does not include the licensing cost of AM

*AM reduces the number of password incidents per year by 50%

ACCOUNT MANAGER BUSINESS BENEFITS

Round-the-Clock Availability

- Provides 24/7 system availability empowering employees to change their passwords at their convenience.

Enhanced Security

- Increases security while servicing password service requests through tight integration with Identity Management System.

Scalability

- Provides the flexibility to support hundreds of thousands of users.

Increased Staff Efficiency

- Eliminates one of the topmost call drivers - "password issues", allowing help desk to address important issues.
- Provides timely reminders on password expiry and empowers users to change them easily within expiration date, avoiding downtime.
- Empowers employees to manage their own network password(s) without help desk intervention.
- Uses robust encryption and configurable security policies to protect employees' systems and enhances compliance with corporate policies.

Improved Cash flows

- Eliminates IT help desk cost for password reset.
- Generates ROI within few months of deployment.

CONCLUSION

Monitoring, managing, and controlling costs are critical to an organization's growth plans. Enterprises across the globe depend on Aptean's Account Manager to reduce support incident volume and related costs. Account Manager is the right investment option for any organization that is looking for a solution that provides high Return on Investment (ROI) and has a quick payback interval. Account Manager easily integrates with existing systems and offers a solid and secure self-service option for the end-users to solve password related issues, ensuring a delightful support experience anytime, every time!

This whitepaper mapped out Aptean's key technologies and application capabilities. If you would like more information on how Aptean solutions have worked for companies like yours, please contact us using the information below.

REQUEST A DEMO: problemsolved@aptean.com

Join the list of leading players who believe in our model of sustainable growth: Non-Linear Growth the Aptean way!

About Aptean: Aptean is a leading global provider of mission critical enterprise software solutions. We build and acquire industry-focused solutions to support the evolving operational needs of our customers. Our solutions help nearly 6,500 organizations stay at the forefront of their industries by enabling them to operate more efficiently, thereby ensuring higher customer satisfaction

Aptean is where software WORKS. For more information, visit **www.aptean.com**