Turbo-IT Corporation
103 West Second Street
Irving, Texas 75060
http://www.turbo-it.com

turbo-IT Corporation

Getting the Most From Your Help Desk

Cost Reduction Strategies for Service Desk / Help Desk

Automating user password resets / unlocking user accounts

WARRANTY

The information contained in this document is subject to change without notice. turbo-IT Corporation makes no warranty of any kind with respect to this information. turbo-IT SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTY OF THE MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. turbo-IT Corporation shall not be liable for any direct, indirect, incidental, consequential, or other damage alleged in connection with the furnishing or use of this information.

TRADEMARKS

Microsoft, Active Directory, Windows, .NET Framework, Windows Server, Microsoft SQL Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All trademarks and registered trademarks used in this white paper are property of their respective owners.

web: http://www.turbo-it.com
e-mail: info@turbo-it.com

TABLE OF CONTENTS

Getting the most from your Help Desk

Cost Reduction Strategies for Service Desk / Help Desk

Help Desk Calls Landscape

Today's I.T helpdesk serves a complex and varied set of responsibilities. Helpdesk technicians are expected to address issues ranging from simple tasks such as showing users how to format documents in Microsoft Word to solving involved SAP reporting issues. Many helpdesks are setup as the "single and first point of contact" for all internal customer service issues. This presents a growing challenge on how to both utilize your helpdesk staff in the best way and how to employ technology to make helpdesk functions cost-effective.

Growing trends in I.T. are focused on leveraging Helpdesk personnel in the most optimal way. Since the cost of helpdesk employees/contractors is usually the single most significant expense for this service, it is vital that helpdesk technicians spend their time prudently.

The following trends in the industry highlight this:

- Have aggressive goals of solving customer requests on first contact
- Trend to move away from helpdesk personnel as "glorified typists" and have them be competent problem solvers
- Re-evaluation of benefits of out-sourcing helpdesk functions. Many organizations are "in-sourcing" these functions again because of questionable Return on Investments from these out-sourcing attempts.
- *Automating routine help desk tasks so that helpdesk personnel can serve more specialized requests.*

Low Hanging Fruit

Automation of Common Tasks

In the previous section, it was highlighted that one of the growing I.T. trends and goals for most effectively using helpdesk is to automate routine help desk tasks.

There are a number of tasks in this area that are candidates for automation. Some typical tasks include:

- User password resets
- Unlock of accounts that have been locked

- Users needing access to files or folders or web sites
- New user creation and set-up (including email access, etc.)
- Telephone set-up
- Increase in Quotas – file or mailbox quotas
- Uses requesting software and software provisioning

Most of these are ideal candidates for automation. Depending on the size of the organization, your I.T. infrastructure, and specific needs, some or all of these items should be automated (and involve minimal I.T. personnel in the defined processes).

Automation of these items should be one of the principal steps in the evolution of helpdesk functions from the mindset of "cost" center to being an "asset" center as a part of an organization's overall technology offerings.

Importance of Automating User Password Issues

Varying studies have been done on how expensive password related issues are for organizations. If you are involved in the I.T. functions in your organization, you should already have a good idea of how this affects your enterprise.

A Gartner Research study entitled "Password Reset: Self-Service That You Will Love" indicated that 15% to 30% of help desk calls are password reset requests. This study also asserts that each password reset request, if handled by helpdesk personnel, can cost between $51 and $147.

A Forrester Research study calculated the cost of a password reset request to be $70.

There are other studies that reflect similar thoughts.

The critical point to consider is probably more crucial: When a help desk call for a request such as this takes place, two things happen:

(1) the user having the issue is no longer being productive until issue is resolved

(2) the help desk technician is now forced to spend time on this call instead of something more "leveraged" and more effective use of technician's time

Return on Investment for solutions in this space is usually very short. For medium sized organizations (between 500 to 5000 users), the return on investment is typically 1 to 3 months. For large organizations (>5000 users), thy ROI can be lower than 1 month.

Specific Solution for Automating Password Resets / Unlocking Accounts

The previous section touched on the justification for automating reset of passwords and related user provisioning tasks. We will now discuss one such specific solution from turbo-IT Corporation – Self Management of Passwords (SMOP).

There are various strategies for automating password resets and differing solutions based on an organization's needs and ambition level.

The product from turbo-IT Corporation, SMOP, serves as a good compromise between features and complexity. It offers a large amount of customization features for administrators while allowing the implementation to be simple and requiring minimal expertise and maintenance overhead.

Technical Solutions Overview

Features to look for in a self service password reset tool

When investigating which tool will work best in your environment, following considerations should be taken:

- Type of user directory database in use: For example, many organizations have Microsoft Active Directory to store and manage their user accounts.
- Web-based or client/server architecture: Care should be taken to see if the tool supports your internal standards for computing such as Win32, Unix, Apple, or web-based technologies.
- Auditing Features: Does the tool allow the administrators to track reset password activity?
- Security: Does the tool store user information in a secure way? Does the information cross the network in a secure way?
- Flexible Options: Does the tool allow administrators to configure the challenge questions? Does it allow administrator to specify how many challenge questions to answer?
- Complexity: How difficult is the tool to manage? Will it cost more to keep running and manage then the cost savings it will provide? How easy is it to deploy?
- Language support: Does the tool support your organization's standard computing language(s).

SMOP from turbo-IT

The software from turbo-IT Corporation – Self Management of Passwords (SMOP) – is one such tool that addresses the self service needs for organizations. Although there are a number of tools that aim to solve this business need, we will discuss the use of SMOP in this paper. SMOP strikes a good balance between power/flexibility and ease of use.

Many of the discussions and implementation details will apply regardless of the tool chosen to solve your password reset / account lockout automated workflow.

Feature Set

The following key features are provided by SMOP:

- Support for Microsoft Active Directory
- Support for Windows 2000 / Windows 2003 Active Directory
- Secure 128 bit encryption
- Use of standard SQL Server technologies (SQL Server 2000, SQL Server 2005, MSDE, SQL Server Express Editions)
- Flexible Options
    - Customize and Create Challenge Questions

    - Configure Minimum and Maximum Number of Challenge /Responses
    - Configure for case sensitivity
    - Support of multiple domains
    - Different Password Reset behaviors
- Email notifications
- Ease of deployment
- Completely web based – both user section and admin section

How It Works

SMOP and other products in this category (with some minor differences in implementation) work by asking users a set of Challenge/Response questions that uniquely identify the user. Once the user has been identified, SMOP can fix the user's password or account issue by resetting the password to a new password or unlocking the user account.

The enrollment answers and other information is stored in a SQL Server database with encryption.

The use of SMOP follows the following two step process:

1. **Enrollment:** Users have to answer a set of Enrollment questions with their own unique answers. Common questions that users are asked:
    - What is your mother's maiden name?
    - What high school did you graduate from?
    - What is the name of your first pet?
2. **Reset Your Password:** Once the user is enrolled, the user can use the SMOP web site to unlock his account. The user will be prompted to answer the Enrollment questions. If the user answers these questions correctly, he is allowed access to his account where he can now set his new password or unlock his account.

SMOP has some additional features such as allowing the user to also *change* his password from the same web interface. There are some other value additions that SMOP provides (e.g. additional customization features) and those can be referenced from the turbo-IT web site. For our discussion here, it is sufficient to understand the workflow.

Deployment Strategies

Deploying a solution such as SMOP should follow these general guidelines:

Feasibility: Test product in a lab environment and make sure it meets your organization's requirements

Design Solution: Factors such as configuration options and policies should be decided here

Install Solution: Install and configure options and integrate with your help desk web sites

Pilot: Run pilot group of users. This should be representative of your organization and include as large variety of users as possible.

User Training: Train users on how to use the product. This could be as simple as an email explaining how to use the product or face to face sessions.

Deployment: Should include end user communication, production deployment of the tool, and a plan to encourage user adoption of the tool

Post Deployment Review: Identify improvements and study benefits. If changes are needed to improve process, this review should identify and implement changes

In Preparation of Deployment

There are a number of options and policies you will need to decide before implementing your password reset tool. This section enumerates these options and provides some best practices and guidelines for these options.

1. Web Server: The SMOP application is a web-based tool. The server application will need to be installed on a server running Microsoft Internet Information Server (IIS). Thus, before deployment, the target server will need to be decided and secured.

2. URL: Users will connect to the SMOP application through a web location and will require a web location. If this is an intranet deployment, you will need to decide the URL for this. Many organizations will simply use the name of the server (for example, http://smopserver/smop). Other organizations will want to use a more descriptive name, such as http://resetpassword/smop. In either case, you will want to make sure the appropriate DNS settings are decided and registered before deployment.

3. Service Account: SMOP will use an Active Directory account to reset user passwords and unlock accounts. This account will need the right level of permissions. The account can be as simple as a Domain Administrator account. Your organization may want to however restrict the account to Account Operator rights. This account should be configured so that it cannot be used to log in.

4. SMOP Administrator Group: The SMOP administration is done through a web interface. Access to this web interface is controlled by an Active Directory group. This group can be an existing group (like Administrators) or one you create specifically for this purpose such as “SMOP Administrators”. The group should be created on the domain and not on the local server. Best practice is to create a separate group for this purpose and add the users that need access to the SMOP Administrator web pages to this group.

5. Database: SMOP will require a database to store configuration information. If this is an intranet deployment (internal to your organization and not exposed to the internet), it is recommended that the database is locally on the same system as the SMOP application. If however, you will deploy SMOP for use over the Internet, you will want to put the database on a secure network. It is recommended that you use SQL Server 2005 versions or higher. This database should be installed and configured correctly (for network access) before continuing with the SMOP deployment.

6. Email Settings: SMOP allows you to configure email notifications so that administrators can be notified of password reset activity. Before deployment, your organization will need to decide which events you would like to be notified of. The different events are as follows:

    a. Password Reset Success / Failure

b. Account Unlock Success / Failure

c. User Enrollment Success / Failure

d. User Account Update Success / Failure

e. User Logon Success / Failure

It is recommended that initially the administrator monitors all the events. This will allow the administrator to see any abnormal activity and also see to what extent users are using the tool and when. After the initial deployment, the events can be tuned downwards.

7. Email SMTP Settings: For email notifications, the server where SMOP is installed will need the ability to send email. Thus, the SMTP server name and/or IP address should be obtained and relay permissions for the SMOP server should be granted before deployment.

8. Number of Questions: SMOP uses a challenge response paradigm where users are asked a number of security questions. The number of questions that are asked and that are REQUIRED are both configurable. Before deployment, the minimum of questions that a user MUST answer should be decided. It is recommended that the number is between 3 and 5 to balance the need for security and ease of enrollment.

9. Text of Questions: The actual questions can be customized. There are a set of default questions that are provided (such as "What is your mother's maiden name?"), but your organization may have some specific questions that are pertinent to ask (e.g. for a university, asking the student ID number). If these customizations are needed, this should be decided before deployment.

10. Case Sensitivity: Answers to questions can be case sensitive. This will mean that users will need to enter the answers the same way including case as when they enrolled. Generally, challenge/response questions are NOT case sensitive.

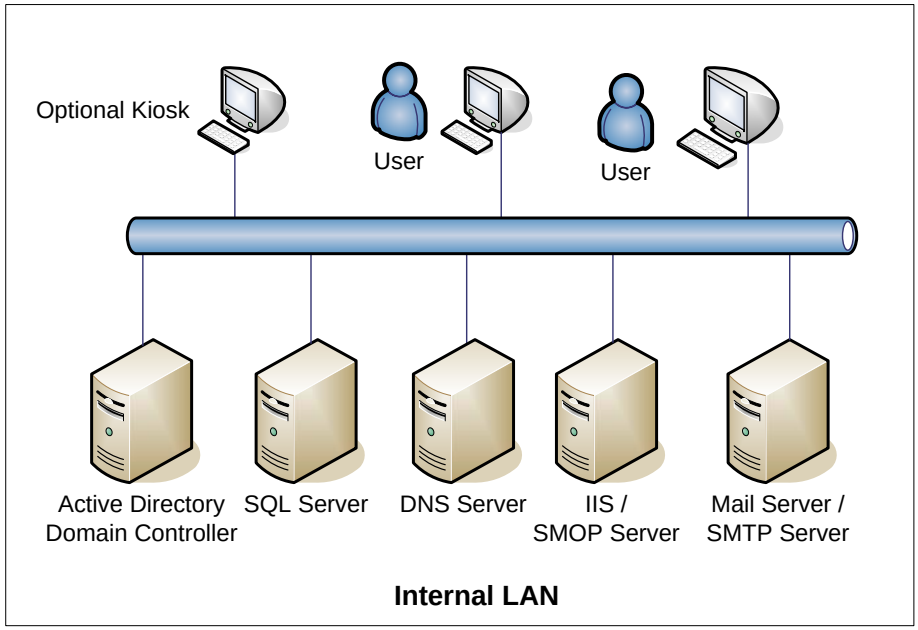
11. Password Policy Message: When users reset their passwords, a message is shown to the user. This is the opportunity for the I.T. organization to remind the user of the password policy for your organization. This text should be configured before deployment. For example, if your organization requires passwords to be longer than 8 characters and include one alphanumeric character, this should be stated in this password policy message.

12. Reset Password Behavior: When passwords are reset, the user will be prompted for their new password. SMOP has a powerful feature that allows the administrator to configure whether the user will be prompted to change their password at the next logon. Before deployment, your organization will need to decide which option to use. The SMOP documentation has more details on the different behavior. The best practice is to force the user to change password at next logon.

Implementation Overview

Implementing Self Service Password Reset on Intranet

The common implementation of self service password reset software will be on an organization's internal LAN (i.e. Intranet). In this scenario, SMOP can be run on an internal existing IIS server or a new IIS server specifically for this purpose. The following diagram shows the main components involved in an Intranet implementation:



One point in the above diagram is the optional kiosk. Since SMOP requires access to a computer so that password resets can be performed, a user would have to have some way to get access to another computer that can get to the SMOP web site (the user cannot use his own computer because he is locked out or cannot log in because he does not know the password!). There are two common approaches to this:

- Ask a colleague to use their computer to perform the password reset
- Use a shared kiosk (or common computing station) that is logged in with minimal permissions but can access the SMOP web site. Many times, this type of system is kept in the lobby or in a conference room for guests to use the Internet.

Implementing Self Service Password Reset over the Internet

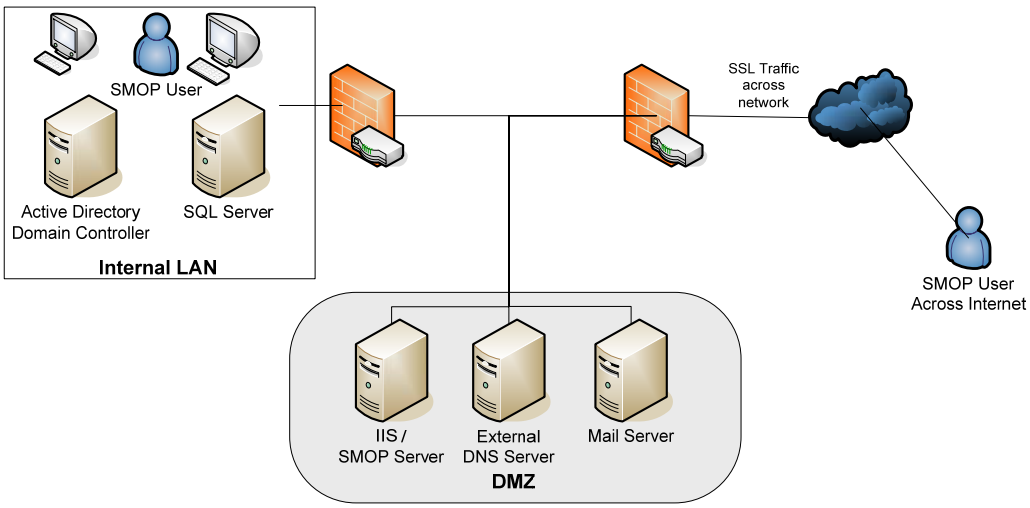
A powerful extension to using self service password reset software is to expose the software to use over the Internet. Along with the obvious security concerns, there are a host of benefits for doing this.

1. Allows users who may be traveling and in a hotel room to the password reset and user account unlocking functionality. This also allows use of self service functionality when potentially a help desk is not available.

2. By using SSL, allows encryption of data transmitted on the network giving a more robust, secure implementation

3. Continues to allow *Intranet* users the same functionality as before but also benefiting from the network encryption.

The following diagram shows a typical Internet deployment of a product like SMOP.



There are some special firewall configurations needed when putting SMOP on the DMZ (namely, LDAP communication from the SMOP Server will need to be allowed to the internal AD domain controller).