Password Reset PRO: Web Based Self Service Software for Active Directory

Software version 3.x.x

Secure, customizable, regulatory compliant, easy to use Web Based Self Service Software for Active Directory users.

Our Web Based Self Service solution allows users to quickly change or reset an expired, temporary or forgotten password, and self unlock a locked out account. Easy to deploy and does not require changes to your domain, schema or client PCs. Users can access the self service web portal via any major desktop web browser or web capable mobile device such as iPhone, Android, iPad, BlackBerry, Windows Mobile. Perfect for today's highly mobile and "BYOD" user base.

Designed for secure, public-facing extranet deployment and access by internal and external remote users. Will meet or exceed general regulatory compliance requirements such as SOX, PCI/DSS, HIPAA, GLB and others and will pass current PCI/DSS external penetration tests. Extremely small change control footprint, no databases or domain changes required.

Solution category type:
Web-based Self Service software, Active Directory user password management, Identity management software, Image-based self service software for Active Directory, password self-service for remote and mobile users.

Solution class type and environmental use:
Enterprise class. Designed for 100% public facing deployment. Designed for high availability and redundancy of services. Designed to pass current regulatory compliance requirements. Designed for MSP/ASP use. Designed for multiple redundant or segregated installations within distributed domain environments. Supports multiple domains and forests.

Works with: Windows Server 2012, 2012R2, 2008, 2008R2, Windows Server 2003, x86 and x64

Capacity: Upwards of 400,000+ users in a single domain (Largest actual customer environment reported to date)

Requirements:
Active Directory 2003/2008/2008R2/2012/2012R2 Domain and Forest Modes **|** IIS6/7/7.5/8 **|** .NET Framework 2.0 or 3.5 **|** Domain account with delegated rights to perform password resets and account unlocks on domain user accounts (used for installed service component) | At least one available domain member server for the internal secure software component **|** At least one available non-domain (DMZ) server with IIS installed for the external web portal component. **|** Both components can be installed on a single domain member server if desired. **|** 10mb disk space **|** at least 100mb avail RAM for small domains and up to 500mb avail RAM for very large domains (300k+) **|** Dedicated servers not required, VMs ok!

Price:
Priced per active password-expiring user account ("licensable users"). No charge for disabled user accounts, 'System' AD accounts and user accounts set with 'password never expires'. Our Sales Team can help determine your licensing need.

Licensing type:
Per domain and per licensable user. The license key is tied to the specific domain name it is created for and cannot be used in other domains. No added costs for multiple domains. One installation is required per domain with its own specific domain key, and each domain will require enough licenses to cover licensable users in the domain.

Licensing counts and purchase options:
Purchase options are a permanent, one time license purchase (your license key never expires), or, annual renewable licensing where the per-user cost is reduced but the key must be renewed each year on or before the annual date.

Permanent licenses, 100 Users minimum and 7500 users maximum. An 'unlimited' domain license is issued if over 7500 licensable users. User licenses can be added in counts of 25 or more at any time. No "block" requirements.

Annual licenses, minimum of 400 / max of 10,000 (Unlimited license given). Typically preferred for ASP/MSP use.

*Additional domain licenses are considered "additional user license" purchases at the 25 license minimum.

Why Password Reset PRO – What sets our product apart from the others?

The primary issues we've found with many self service password reset types of products are lack of proper perimeter security, single points of failure, lack of scalability, difficulty of installation and inability to meet current compliance requirements. *Essentially, they are designed for internal "LAN use" only, with zero though given to public deployment security or safety of data.*

Most of these "LAN" products require installation of a MySQL or SQL database that stores user enrollment logins, domain passwords, and other sensitive data *outside of Active Directory*. Some of these products cache sensitive user information inside the external web portal, require running the web portal with *domain\admin credentials*, require installation of the web portal on a domain member server, and some even provide *sensitive administrative access functions to take place within the external web portal pages*.

Ask yourself, do you want your Active Directory to be accessible directly to the outside world through a 3rd party web product?? We hope not! This could potentially present a rather large security risk and in our opinion is completely unnecessary- Our product provides a secure segregation layer between the external web portal and your internal domain. No databases are required, we use your Active Directory as-is for storing user enrollments, and we never store user data outside of AD. We use several layers of AES / RSA encryption on communications within our product, and the Web Portal can be deployed on a non-domain generic IIS web server away from the internal domain.

Let's talk about deployment planning and change control- It can be a virtual nightmare with installing some of the available self service password reset products due to odd requirements such as extending or modifying the domain schema, installing proprietary SQL/MySQL databases, running open-source web servers, deploying modified client pc software, running "agents" directly on DCs, etc. *In some cases it can take weeks or months to deploy these types of products!* Why? We find this baffling.

Password Reset PRO is specifically designed for today's environment with regards to change control, usability, perimeter security and compliance. Installation of our software takes 5 minutes **tops** and can be deployed to the enterprise *immediately*. Basically, our software is designed from the ground up for security and is easy to deploy, use and manage, with none of the aforementioned problems.

And there's more- We allow you *full access* to the actual web pages, images and CSS file, allowing you to completely re-brand and customize the entire web interface as well as much of the enrollment processes. This allows you to deploy a service that looks like you built it vs bought it, and allows you to tailor the experience to your unique community. In addition, you can run multiple web portals simultaneously in different modes, with different branding, to address different communities within the domain. For example, Executives can have a different web portal vs. general users.

Download Password Reset PRO today from our website at www.sysoptools.com, use the full production version free for a month and judge for yourself. It is specifically designed for safe testing in your domain. We think you'll be pleased!

Common Questions:

Can we limit scope of software to only a portion of AD users?
Yes. One or more OU-specific license keys can be added to the software to only allow access to specific portions of your Active Directory structure and user accounts. Or, we can instruct on using native AD permissions to restrict scope.

Mobile device access supported? Yes, all self service features are accessible on current web-capable devices

Are all users forced to use the same single web portal?
No. Version 3.x.x provides three different deployable access modes. An image-based enrollment mode, a question/answer Active Directory based no-enrollment-required mode, and a fast, basic domain authentication mode. All three modes can be deployed and run simultaneously, providing unique access portals for different user communities as needed.

Load Balancing, failover and enrollment data redundancy provided? Yes

Database installations required? No. Our product uses Active Directory as the redundant data store.

Administrative pages within the Web Portal, must run the Web process with domain credentials, or must install the Web Portal on a domain member server? No

Any changes to the domain required, must install agents on DCs or deploy client software? No

Password Reset PRO Fast Facts:

- Easy to deploy- No changes to schema or client PC's required, no software on DCs, no databases to install!
- Uses AD as your "database", no user data is stored outside of AD (no security / compliance issues introduced), your schema and domain is used as-is (no changes needed)
- Uses IIS6/7/7.5/8 for the external web portal, installs as a regular ASP.NET / AJAX website- manage and edit the Self Service portal as easy as any commercial ASP.NET website
- Easy load balancing and redundancy for the external self service web portal by placing two or more instances behind load balancers- Just like any regular website.
- Uses regular SSL certs, settings and perfmon counters through IIS
- Stellar performance- can handle up to 300,000+ users in a single domain from one installation
- Install on 2003/2008/2008R2/2012/2012R2 x86 or x64 platform - Runs as a native 64 bit app on x64 OS
- Web portal designed to pass PCI/DSS external scan tests and Payment Card Industry requirements
- Image based ID enrollment like banking websites- No outdated question/answer methods which are time consuming, ineffective, forgotten or compromised by bot scripts
- Very easy for users to enroll & remember their login. We actually provide THREE different access modes!
- Intrusion detection alerting methods. A real time email sent to admin if hack attempts to the web portal are detected, includes remote computer's IP
- Complete event auditing including client IP address of web portal visitor. Easy to poll events for custom alerting
- Complete disaster recovery, scalability and redundancy built in by design. User enrollments will never be lost
- Web 2.0 design. Edit the web portal css files and aspx pages just like a regular website to give it a company look/feel instead of being forced onto 3rd party product branding
- Most importantly- No "admin access" pages inside the web portal, no sensitive user data stored in the web portal or outside of AD, and no client software to deploy and maintain.

Password Reset PRO Key Product Highlights – 3 Access Modes to Choose From!

Deployment Mode #1: Modern, Image-based ID Security Enrollment
Password Reset PRO uses the modern "online banking" approach to portal identity creation and login. A user initially enrolls with their domain username and a current domain password, an expired domain password, or a temporary domain password. The user is then guided to choose a memorable security image tile and create a security word to establish their return logon to the self service system. Enrollment is fast, simple, and easy to remember. The user's returning self service logon is their domain username, security image and security word.

The improved enrollment process provided by Password Reset PRO is completely customizable. The security images can be changed, and the "Create a security word" portion can be changed to anything desired such as "Create a six digit PIN", "Enter the last four of your SSN", "Enter your Employee ID", etc.

This enrollment data (chosen image + security word) is stored as an encrypted token in AD under the user's account, in the 'altSecurityIdentities' schema field. This token is not readable by anything other than our software, and is automatically redundantly stored due to replication in Active Directory. It is impossible to "lose" enrollments due to a failed server.

Deployment Mode #2: Active Directory Data Mode
No pre-enrollment is required. The user can access self service at any time by entering their domain username and correctly answering one or more control questions. These questions are set up by the administrator, and each question is "mapped" to your choice of an Active Directory field that contains existing data. The web portal user must answer the control questions with answers that match each question's mapped data field in Active Directory.

Example question presented to user: "What is your Employee ID?" This question is mapped to the AD field for "employeeID" under the user's account, and contains the number 00-2351. The user must answer the question correctly by typing 00-2351, which matches the data in AD. This is the easiest method of self service access for your users if you already leverage Active Directory for data storage. You can publish one question or as many questions as you prefer. The user must answer all presented questions correctly.

Deployment Mode #3: Domain Basic Authentication Mode
A very basic access mode which has no enrollment component and does not have the ability to unlock a locked out account. It is solely used to allow quick user access to change an existing password, reset an expired password, or change a temporary password to a permanent one. The process is simply, enter domain username > enter domain password > change or reset domain password. Great for use with Mac users on the LAN and new hire orientations. Renders great on mobile devices, can be i-framed inside MOSS or other pre-authenticated system. We do not recommend publishing this mode externally since it does not us a 3rd factor method of authentication.

Have it your way:
All three of the above modes can be run simultaneously on separate web servers, load balanced, etc.

Additional Data

Wizard Driven User Interface:
System enrollment is "wizard driven" and easy to use for even the most non-tech end user. A returning user logs in to the self service portal by simply entering their NT Account Name + Security Image + Matching Security Word. Once the user is logged in, an "activity page" shows their account status and guides them through necessary activities such as changing / resetting a password or unlocking an account. If a user's password is expired or account is locked out, they are automatically taken to that function page. Everything is made easy / automated for the user, there is no guessing involved.

Admin Auditing and Reporting:
Web portal activities are logged in real time for SOX / HIPAA / GLB / PCI regulatory compliance needs. The administrator receives a daily summary report email of past 24hr events in the self service system. There is a complete Reporting Console which the administrator may use to review all event history and status of all domain user accounts. Events are logged to the server's event log with specific event ID's, and can be integrated with an existing server monitoring system. An admin can see which domain users have not yet enrolled in the portal, reset a user portal ID and ban accounts from using the portal.

Company Branding and Complete Customization:
Customize the web portal logo banner, browser title bar text, global footer and other specific messages in the web portal to your company's needs. Deploy multiple web portals and brand each one separately for different user groups.

If you have skills with editing .aspx and .css files (basic Web 2.0 / html stuff) you can further customize the look / feel of the Web Portal as well as other textual areas of pages. Your users will feel like they are using a company-developed system vs. a 3rd-party software product.

Designed for External Deployment with Two-Tier Architecture Security:
Deployment of the self service Web Portal is fast, simple and requires minimal change control planning. The Web Portal component can be deployed on a non-domain DMZ web IIS server (Extranet), and connects to the internal Master Service server (Intranet) via a single encrypted TCP port published through your firewall. Port connectivity between these two components uses an RSA authentication handshake and encryption at the session layer, and layer 3 data packets are blowfish-encrypted.

Of course, both components can be installed on a single server for use in smaller environments if necessary. SSL certs are fully supported through IIS manager native processes. The Web Portal is as simple to manage as any asp.net website.

No Externally Stored User AD Data, No Exposed Administrative Access:
Self service portal administration is managed separately through a internal secure application called the "Master Service". All sensitive user account enrollments and data resides in Active Directory only.

No user account data or passwords are stored on the web self service portal server, registry or external databases, ensuring ultimate web perimeter security and security of your Active Directory data. If a would-be hacker compromises the web portal server itself, there is no data to obtain from our application (assuming you have the web portal component installed on a non-domain DMZ server).

Unique "Works Anywhere" Product Architecture:
Our software uses your existing Active Directory with no changes required. No schema extensions or modified client GINA deployments are required. No SQL databases. The web portal self service application is 100% web-based written in ASP.NET 2.0, runs directly on IIS6/7/8 and is accessible by any OS / web browser. Typical installation time is 5 minutes not including setup of your IIS SSL certificate. If your company is under strict change control guidelines, has a mixed OS or older domain environment and needs the ultimate in product flexibility, you'll greatly appreciate Password Reset PRO.

Scalable, Redundant by Design:
A single installation of Password Reset PRO can handle over 300,000 users within a single domain. Adding failover / redundancy is a snap- Simply install more Web Portals on other IIS servers and place them behind a load balanced VIP with persistent sessions enabled. User enrollments are stored safely in Active Directory under each enrolled user account- If you were to completely lose the self service system due to server crash etc, simply re-install our software and all user enrollments remain preserved!

PCI / DSS Scan Tested:
The public facing self service Web Portal component has been developed to pass Payment Card Industry external scan testing, which means you can deploy our solution with confidence of maintaining your compliance requirements. Additionally, all processes and workflows within Password Reset PRO are designed to pass general current regulatory compliance requirements from PCI/DSS, SAS70, SOX, HIPAA, GLBA, and similar.

Password Reset PRO is a favorite choice among Gov, Mil, DOD and Edu sectors due to the high perimeter security of the user-facing web portal, and overall non-invasiveness of software operation in the domain environment.

The Best Tool for the Job, Period:
Affordable, easy to deploy, easy to use, secure, scalable and redundant. What's not to love? Password Reset PRO is the best-of-breed when it comes to enterprise-class web-based password self service and identity management software, and is a true "set it and forget it" solution. Download Password Reset PRO Web Based Self Service Software today and use it free for a month!

Download Password Reset PRO today > https://www.sysoptools.com/password-reset-pro/

Have more questions? Contact our knowledgeable Support Team M-F 8am-6pm PST 1-877-SYSOPTOOLS (USA) or +1-310-598-3885 (Direct & Int'l)

Additional Resources:

Purchase Information
Support Information
Reference Material and Knowledge Base
Signup and Download Software

SysOp Tools, Inc. is a privately held company located in Los Angeles, California – Software sales, support and development are handled by experienced in-house staff. We do not outsource any of our operations.