



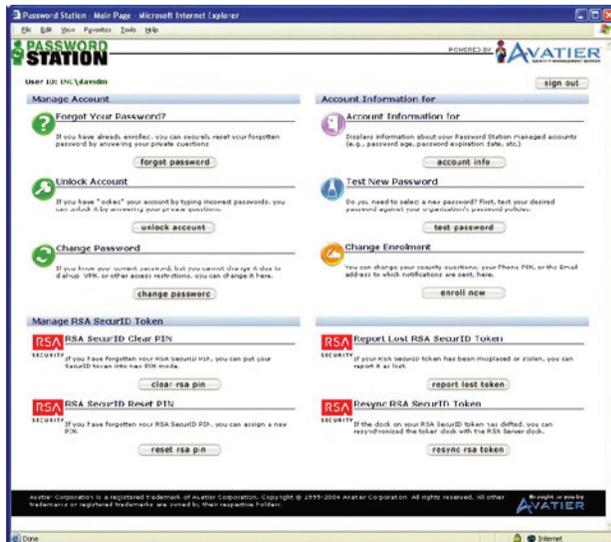
- ▶ WEB
- ▶ RSA
- ▶ PRE-LOGON
- ▶ TOUCH TONE
- ▶ VOICE PRINT

Reduce costs by eliminating all password related help desk calls

Overview

Reducing help desk calls saves your organization a significant and measurable amount of money. Avatier **Password Station™** allows your employees to securely reset their own forgotten password, unlock their account, or reset their forgotten RSA SecurID PIN in a matter of seconds. Now, you can eliminate all of your password related and RSA SecurID help desk calls by employing **Password Station's** secure self-service password management facility that also synchronizes ONE **strengthened** password across all internal enterprise systems.

With support for many languages, forgotten passwords can be securely reset from anywhere or anytime using a web browser, automated telephone system, or by simply clicking on Avatier's Forgot Password button prior to the Ctrl-Alt-Del logon window. Additionally, **Password Station™** protects your organization against identity theft by providing a unified enterprise help desk web console that guarantees end user identity validation.



Avatier's simple and intuitive Password Station web interface allows end users to reset forgotten passwords and securely synchronize them across any platform without calling the help desk.

Lower Costs Today!

As organizations strengthen password policies to make their environments more secure, it becomes more difficult for end users to remember their own complex and ever-changing passwords. As a result, password management and account unlocks generate at least 30% of all help desk requests.

Providing self-service password management has become essential to reducing the cost of enterprise password administration and improving identity confirmation of end users. With LiveUpdate, you can stay focused on your business while maintaining the latest software version without human intervention and added administrative expense. Hundreds of major organizations around the globe depend on **Password Station™** every day to deliver secure self-service password reset and synchronization.

Strategic Benefits

Reduce operational costs

Eliminate all calls to the help desk for password resets and account unlocks. Help desk call reduction allows for better response times on critical issues while decreasing administrative expenses. Password synchronization across multiple operating systems, directories, databases, or applications reduces the number of passwords end users must remember to ONE.

Increase security and accountability

Provide detailed audit logging of every operation performed by Password Station. Avatier's Silent Alarms™ technology emails critical alerts directly to designated employees and administrators. Thus, organizations are immediately made aware of any suspicious activity.

Enable strong password enforcement

Reduce user resistance to stronger password policy by providing a friendly self-service interface with detailed feedback on failed password criteria. End users who have to recall only one secure password on all their systems are more willing to adjust to a stronger centralized policy.

Facilitate security compliance

Guarantees verification of user identity through cascading personal identity challenge questions. Detailed logging of all transactions provides accurate audit trails to demonstrate compliance. Challenge questions can be required to validate user's identity prior to allowing help desk's assistance with password resets or account unlocks.

Ensure employee privacy

Encryption and secure one-way hashing of personal employee enrollment data provides increased security and privacy. End user identity verification is systematically applied through all Password Station self-service interfaces.

Increase productivity

Boost employee productivity by eliminating costly downtime caused by lack of access to system resources. Employees can complete their self-service requests immediately without having to call the help desk.

Instant Identity Management

45-day evaluation versions of Avatier Identity Management Server (AIMS) which includes Account Terminator for cross-platform account termination and Account Creator for cross-platform employee provisioning are included. All three solutions leverage centralized alerting, auditing, logging, and reporting. The entire suite can be deployed in less than a day.



Customer Showcases

British Broadcasting Company (BBC)

Learn how this 30,000-user broadcasting giant rolled out Password Station in a day.

NASA Space Shuttle Operations

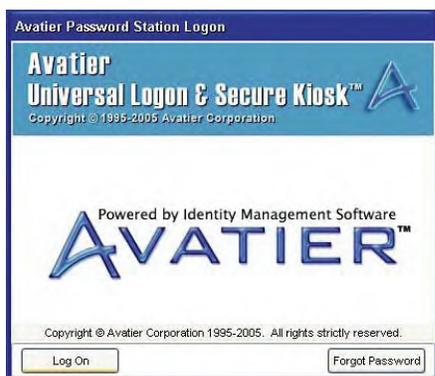
Learn how one of the most secure networks in the world validated Password Station's web page security.

AstraZeneca

Learn how this international pharmaceutical company discarded a floundering multi-million dollar solution to adopt Password Station.

Design Advantages

Secure pre-logon password reset button - Allows users to securely reset their forgotten password from the privacy and convenience of their workstation's Ctrl-Alt-Del pre-logon window without calling the help desk or disrupting a co-worker. Avatier supports Microsoft Windows NT, 2000, XP workstation and works with other Graphical Identification and Authentication (GINA) replacements.



Avatier's Secure Pre-logon Password Reset Button

Cross-platform self-service - End users can securely reset their own password or unlock their account on any directory, system, database, or application used throughout their environment.

Telephone reset - End users can quickly self-identify, verify, and securely reset their forgotten password anytime with any touch-tone telephone, cell phone, or PDA phone.

Changes locally cached passwords - Automatically synchronize your locally cached domain password credentials. This prevents your logon session from locking out and affecting access to Outlook, network resources, and directory folder replication.

Transparent synchronization - When enrolled users change their Microsoft Windows domain password, all other passwords are automatically synchronized.

LiveUpdate - Automatically maintains the latest software version without added administrative support expense.

Provide real-time account status - Help desk staff can check account status information for any user across all platforms to help resolve any logon access issues. Enrolled users can view their own account information.

| System Description | Target Account | Result |
|-------------------------------------|----------------|---|
| Microsoft Windows Domain QAD0MAIN | demo | Full Name: demo demo Account Expiration Date: Never Account Disabled: False Account Locked Out: False Password Expiration Date: 11/01/2004 Password Age: 0 Days, 0 Hours, 1 Minute |
| Sun Solaris 9.0 - Local host (L200) | demo | Full Name: Avatier Demo Description: Account Disabled: False Account Expires: Never Password Expires: Never Password Age: 0 Days Password Allow Change Date: None |
| Novell eDirectory 3.7 - LDAP (L244) | demo | Full Name: Demo & Demo Account Disabled: True Lockout Status: False Account Expiration Date: Never Password Change Allowed: True Password Expiration Date: Never |
| Microsoft SQL 2000 Server | demo | Account Created: 7/26/2004 9:30:10 AM Account Last Modified: 9/19/2004 6:26:14 PM Default Database: Cdbms Full Name: demo |

Real-Time User Account Status on Multiple Platforms

Guaranteed password reset - Ensures passwords are changed and synchronized even if the target host is initially or momentarily unreachable by queuing and retrying every transaction until complete or when the queue time expires.

Retry notification - End users and delegated administrators are automatically emailed when their transaction is queued, when it completes, or when the maximum queue time expires.

Parallel platform processing & replication - Requests are sent to all cross-platform target systems concurrently to reduce the total time for completing password resets. Replication eliminates delays in password changes inherent with distributed Microsoft network environments, so the end user can immediately logon.

Leverage existing directory store - No vulnerable external database is required. Administrators can choose the location to store one-way hashed and encrypted answers to employee's private identity questions in any LDAP or Microsoft directory without extending the schema. Additionally, Password Station supports schema extended fields.

Customizable interface - Simple integration with any existing portal by leveraging easily customizable style sheets and banners.

Mass enrollment of user identity answers - Tens of thousands of users can be rapidly enrolled en masse, so that self-service password reset and account unlock features are immediately available. This feature is popular with universities.

Web services infrastructure with open APIs - Easily extend self-service functionality to integrate with workflow, portals, and additional enterprise applications.

Avatier Identity Management Server (AIMS) - Architecture includes cross-platform account termination and provisioning with templates. Modules are instantly available with license activation.

Languages Supported

| | | | |
|---------------|---------------------|------------|---------------------|
| French | Chinese (Taiwan) | Greek | Polish |
| German | Czech | Hungarian | Portuguese (Brazil) |
| Italian | Danish | Indonesian | Russian |
| Portuguese | Dutch (Netherlands) | Japanese | Spanish (Catalan) |
| Spanish | Finnish | Korean | Swedish |
| Chinese (PRC) | French (Canadian) | Norwegian | Turkish |

Avatier Corporation Proudly Sponsors



Platforms Supported

Password synchronization, real-time account status, account termination, and employee provisioning are natively supported on the following platforms.

| Platforms | Supported Versions |
|---------------------------------|----------------------|
| Operating Systems | |
| Microsoft Windows NT/AD | 4.0, 2000, 2003 |
| Microsoft Windows Server | 4.0, 2000, XP, 2003 |
| Sun Solaris | 2.6 and above |
| HP/UX | 11 and above |
| IBM AIX | 4.3 and above |
| Redhat Linux | 7.1 and above |
| SUSE & Other Linux | All Versions |
| IBM iSeries (IBM AS/400) | V4R5 and above |
| IBM zSeries (IBM OS/390) | V2R8 and above |
| Digital VMS and Tru64 | 7.3-1, 5.1 and above |
| Directories | |
| RSA SecurID ACE/Server | 5.2 and above |
| Sun Java System Directory | 4.2 and above |
| Novell NDS | 4.01 and above |
| Novell eDirectory | 6x and above |
| Oracle Internet Directory | All Versions |
| Microsoft ADAM | All Versions |
| IBM IBM Directory Server | 3.x, 4.x, and 5.x |
| OpenLDAP | 2.1 and above |
| Databases | |
| Microsoft SQL Server | 7.0 and above |
| Oracle | 8.x and above |
| Sybase | 10.x, 11.x, 12.x |
| IBM IBM DB2/UDB | 6.x, 7.x, and 8.1 |
| IBM Informix | 7.x, and 9.x |
| Applications | |
| IBM Lotus Notes | R4 and above |
| Oracle E-Business Suite | 8.x and above |
| PeopleSoft | 8.x and above |
| SAP | 4.5B, 4.6C, and 4.7 |

Minimum Requirements

Hardware

AIMS Administration Server:

- 400 MHz CPU speed or higher
- 256 MB RAM
- 100 MB for program files and auditing database
- Monitor capable of displaying 16-bit color or greater and a resolution of 800 x 600 or higher

Software

AIMS Administration Server:

- Microsoft XP Professional, Windows 2000 Server, Windows 2003 Server - Standard Edition. When managing either a Microsoft Windows NT or Active Directory domain, we recommend making the AIMS Administration Server a member in at least one of the managed domains.
- Not intended for Microsoft Windows 2003 - Web Edition or domain controllers
- Microsoft Internet Information Server (IIS) 5.0 or later
- Microsoft SQL Server (optional)
- Microsoft Data Access Control (MDAC) 2.8 or later
- Microsoft .NET Framework 1.1 extensions or later

Primary User Directory Store:

- Microsoft Windows NT
- Microsoft Active Directory
- Microsoft Active Directory Application Mode (ADAM)
- Novell eDirectory
- Sun Java System Directory Server (Formerly Sun One Directory Server and iPlanet Directory Server)
- IBM Directory Server
- Oracle Internet Directory
- Any LDAP Server

Web Clients:

- Microsoft Internet Explorer 5.5 or later
- NetScape 4.0 or later
- Mozilla 1.0 or later

Contact

Worldwide Headquarters

Avatier Corporation
12647 Alcosta Blvd, Suite 400
San Ramon, CA 94583

925-217-5170 main
925-275-0853 fax
800-609-8610 sales

info@avatier.com
www.avatier.com
www.passwordstation.net



Copyright © 1995-2005 Avatier Corporation. All rights reserved. All other trademarks or registered trademarks are owned by their respective holders.