



DESKTOP AUTHORITY[®] PASSWORD SELF-SERVICE™

Desktop Authority[®] Password Self-Service provides an easy-to-use, robust system for allowing users to reset their own forgotten passwords or locked accounts, eliminating the biggest source of help desk calls. The flexible, policy driven system allows administrators to define the type and number of questions that must be answered, and to tailor the requirements to the department or group. Desktop Authority Password Self-Service integrates seamlessly into the logon screen of Windows 2000, Windows XP and Windows Vista, allowing users to reset passwords right from their own workstation, even when they can't log in.

Help desks are required to support more users and more applications, often without increasing staffing. To handle the increased support load, while maintaining service levels, it's important to automate as many tasks as possible.

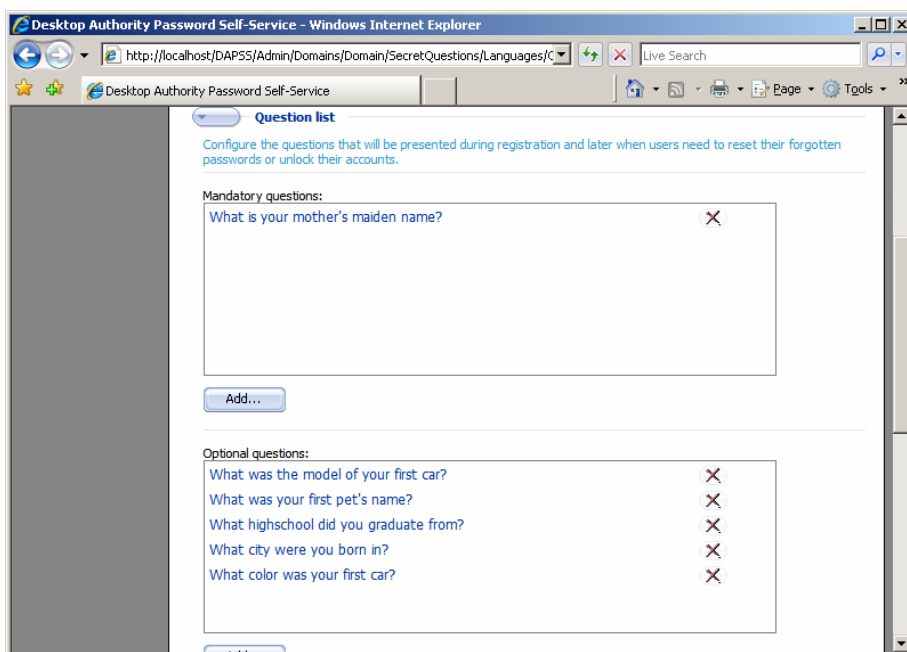
Analysts estimate that 40-60% of all help desk calls are related to forgotten passwords or locked out accounts. Implementing a password reset solution can eliminate 30-50% of these calls.

Desktop Authority Password Self-Service allows users to reset their passwords and unlock their account quickly and easily, right from the Windows Logon screen. In addition, Desktop Authority Password Self-Service provides for more robust password policies and granular security management.

COMPLETE SELF-SERVICE ACCOUNT MANAGEMENT

Desktop Authority Password Self-Service lets users sign up for the service, change passwords, reset lost passwords and unlock accounts from the self-service web portal. All password changes and resets automatically conform to password policies. The number and type of challenge questions that must be answered to reset a password, or unlock an account can be completely configured by the administrator. Emails can be sent automatically to users and administrators upon a password reset.

Desktop Authority Password Self-Service lets you customize the number, and type of questions users must answer to reset their password.



If needed, help-desk technicians can reset passwords, assign temporary passwords and reset the answers to users challenge questions.

EXTEND ACTIVE DIRECTORY PASSWORD POLICIES

Active Directory is limited to having one password policy for the entire domain. Desktop Authority Password Self-Service can extend the password policies in several ways. Using the included Policy Manager, password policies can be set at the domain, organizational unit or AD group level. Now administrators can set stronger password policies for sensitive areas like finance and human resources.

Password policies can be controlled through password length, including mandatory character combinations, prohibiting specific characters, protecting against dictionary attacks, and maintaining strict password history policies.

This granular control extends to the question and answer policies. The number, type of question and answer quality can also be set at the domain, organizational unit, and AD group level.

REDUCE WORKLOAD, IMPROVE SERVICE LEVELS

Desktop Authority Password Self-Service can reduce the help desk call volume, improve customer service levels and improve security and password policy compliance.

KEY BENEFITS

Reduce Help Desk Call Volume
Forgotten passwords represent 40-60% of all help desk calls. Eliminate most of these calls completely while providing improved service levels.

Strengthen Password Policies
Go beyond Active Directory password policy limitations by specifying policy at the OU or Group level.

Customize Password Security
Q & A Policies let you set the number of questions a user must answer to reset their password based on the security needs of the OU or AD Group.

Provide Seamless Logon Integration
Optionally provide a "Forgot my password" button right on the Windows logon screen letting users reset their passwords quickly right from their desk.

KEY FEATURES

Comprehensive Configuration
Configure customized Q&A Policies, password policies, answer quality, account lockout policies and hacking protection at the domain, organizational unit, or AD group level.

Complete Self-Service System
Users can sign up, set up secret answers, reset passwords and change passwords right from the self-service portal.

Flexible Identification
Users can identify themselves using logon name, first or last name, and even email address to start the reset process.

Secure data storage
Encrypt user data using a variety of industry standard encryption methods..

Granular Password Policies
Go beyond the limitations of Active Directory password policies by defining password policies at the domain, organizational unit or AD group level.

Windows Logon Integration
The Secure Password Extension allows seamless integration with the logon screen of Windows 2000, Windows XP and Windows Vista.

Encourage User Registration
A variety of features encourage user registration through a registration schedule, email reminders, and other tools to encourage user registration and maximize help desk savings.

Comprehensive Reporting
Detailed reports show adoption and use of the product. See how often passwords are being reset.



DESKTOP AUTHORITY[®] PASSWORD SELF-SERVICE™

EASY, WEB-BASED INTERFACE

Users interact with Desktop Authority Password Self-Service through a familiar web interface. Users register for the service, answer their challenge questions and reset their passwords entirely through their browser. The Secure Password Extension allows access to the web interface even when they can't log on.

COMPLETE ADMINISTRATIVE CONTROL

Virtually every aspect of Desktop Authority Password Self-Service can be defined by the administrator. They can specify the number of mandatory questions, optional questions or even user-defined questions that need to be answered to sign up, and to reset a password or locked account. Administrators can define password policies, alerting options, and account protection levels that will automatically lock an account after a set number of failed reset attempts.

SECURITY FOCUSED

Desktop Authority Password Self-Service features secured communication between the client and server, and a variety of data encryption options, including a FIPS 140-2 compliant data encryption implementation. These features, combined with enhanced, flexible password policies ensure that organizational security goals are met, while service levels are improved and help desk call volume is reduced.

CENTRALIZED REPORTING

Desktop Authority Password Self-Service provides comprehensive reporting across all instances of the product, showing user adoption and password reset activities.

OTHER FEATURES

Desktop Authority Password Self-Service offers many other important features:

- Complete Integration with Windows Clients
- Email notification on password changes
- Support for 32-bit and 64-bit operating systems
- Broad Windows client support
- Strong identity verification
- Flexible identification options
- Enforced user registration
- Easy installation and deployment
- Full support for Windows Vista
- Native integration with Active Directory
- Web-based management reporting
- Comprehensive browser support
- Optional client deployment through Group Policy
- Industry leading technical support

EVALUATION VERSION

More detailed product information, including documentation and a fully-functional 50 user, 30-day evaluation copy of Desktop Authority Password Self-Service can be downloaded from our web site.

F.A.Q.

How can Desktop Authority Password Self-Service improve security?

Desktop Authority Password Self-Service allows more robust password policies than Active Directory alone, it also allows you to tailor your password reset policies to the security needs of the organizational unit or AD group. Additionally, communications with the server, and all data storage can be encrypted.

How can Desktop Authority Password Self-Service reduce support costs while improving service levels?

Desktop Authority Password Self-Service eliminates the largest source of help desk calls—the lost or forgotten password. By placing password resets into the hands of the user, they can minimize downtime by quickly restoring their account access without ever making a help desk call.

SYSTEM REQUIREMENTS

Server Requirements

Desktop Authority Password Self-Service requires:

- Windows Server 2003 (SP1) or higher
- SQL Server 2000 or 2005
- Internet Information Server
- Internet Explorer 6.0 or higher

Client Requirements

Desktop Authority Password Self-Service supports the following client OS:

- Windows 2000
- Windows XP
- Windows Vista
- Internet Explorer 6.0 or higher
- Mozilla Firefox 1.x or higher

LICENSING

Desktop Authority Password Self-Service is licensed based on the number of active users in your Active Directory.

A 30-day evaluation license is available with the evaluation download. The 30-day evaluation will support up to 5000 users in your Active Directory domain.

For pricing, contact your ScriptLogic reseller or call ScriptLogic at **1.800.813.6415** or **1.561.886.2420**.

Please refer to our web site for international information.

Desktop Authority Password Self-Service provides flexible configuration of all aspects of password resets and account lockouts.

