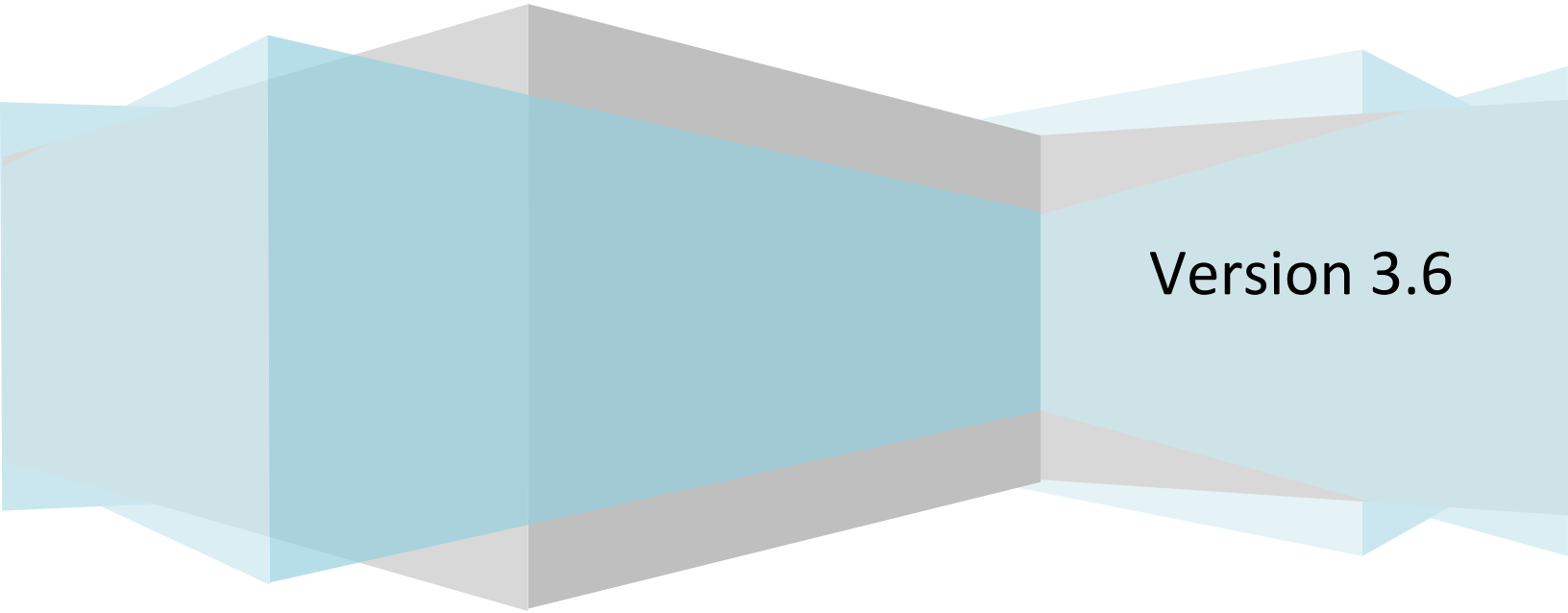
The Dot Net Factory

AD Self-Service Suite for Active Directory

Getting Started Guide for AD Password



Version 3.6

AD Self-Service Suite for Active Directory

Getting Started Guide for AD Password

Headquarters

4393 Tuller Road

Dublin, Ohio 43017

www.ADSelfServiceSuite.com

e-mail: info@TheDotNetFactory.com

U.S. and Canada: 877-996-4276

AD Self-Service Password Getting Started Guide

Updated – May 31, 2011

Software version – 3.6

ABOUT THIS GUIDE

This document has been prepared to assist you in becoming familiar with The Dot Net Factory AD Self-Service AD Password. This guide assumes that the steps outlined in the AD Self-Service Suite Quick Start Guide are complete and the AD Self-Service Suite is installed on your system and ready for configuration of the AD Password specific settings.

ABOUT THE AD SELF-SERVICE SUITE FOR ACTIVE DIRECTORY

The AD Self-Service Suite for Active Directory unlocks the productivity and collaborative potential of your network by providing web-based lookup, self-service and delegated administrative capabilities across your entire enterprise. AD Self-Service consists of three applications that can be purchased together or separately: AD WhitePages, which provides an enterprise-wide virtual directory of users, contacts, resources, shares -- any object that exists in your LDAP compliant directory; AD Info, which provides end-user self service of directory information; and AD Password, which provides password self-service and recovery.

The AD Self-Service Suite quickly pays for itself by enabling a broad range of self-service user maintenance activities and allowing the delegation of common administrative tasks, including user and group management. The AD Self-Service Suite leverages your investment in Active Directory while significantly strengthening security, reducing infrastructure costs, streamlining IT operations, and creating better and cost-effective compliance with regulatory requirements.

ABOUT THE DOT NET FACTORY

The Dot Net Factory is a leading provider of Management, Collaboration, and Self-Service solutions for Microsoft Active Directory. The AD Self-Service Suite unlocks the value of your directory investment making it an accessible and easy to use resource for employee communication and collaboration, web-based delegated user and group management, and end-user self-service management of passwords and personal information.

Contacting The Dot Net Factory

Phone: 877-996-4276 (United States and Canada)

Email: info@TheDotNetFactory.com

Address

4393 Tuller Road

Dublin, Ohio 43017

USA

Web site: www.ADSelfServiceSuite.com

Contacting Customer Support

The Dot Net Factory's world-class support team is dedicated to ensuring successful product installation and use for all The Dot Net Factory solutions.

Support Link
http://www.adselfservicesuite.com/Support.aspx

Email at support@TheDotNetFactory.com

PASSWORD OVERVIEW

AD Self-Service AD Password is the only solution allowing end-users to manage their passwords and recover their locked-out accounts while seamlessly integrating into the applications they use every day. AD Self-Service brings the services to the user by integrating tightly into the user interfaces of many frequently used applications like Microsoft SharePoint, the Windows logon, and even custom web applications.

AD Password alerts users before their password expires and allows them to enroll in the Password Reset Service. In the Password Reset Service, users may answer multiple administrator-defined Challenge Questions. In the event a user forgets their password or becomes locked-out, they are automatically redirected to the anonymous Password Reset Center. From this friendly interface, users may reset their password or unlock their account by answering previously defined Challenge Questions. The Windows client provides access to the Recovery Center for users having issues logging on from their workstation.

SYSTEM REQUIREMENTS

Before installing The Dot Net Factory AD Self-Service Suite, ensure your system meets the following minimum hardware requirements:

- 1.4 GHz or greater processor
- 1GB RAM
- 200 MB hard disk space

Ensure your system meets the following minimum software requirements:

- Microsoft ® Windows Server™ 2003 or greater
- Microsoft® Internet Information Server 6.0 or greater
- Microsoft **.NET Framework 2.0** with ASP.NET
- Member of Domain

Enabling HTTPS

It is strongly recommended that you use HTTPS with The Dot Net Factory Password. The secure hypertext transfer protocol (HTTPS) is a communications protocol designed to transfer encrypted information between computers over the World Wide Web. To enable HTTPS for your Web server you may need to obtain a Server Certificate. For more information, see the following article: http://technet2.microsoft.com/WindowsServer/en/Library/354f4539-982a-418c-bfe7-4d5155b83f4a1033.mspx?mfr=true

Optional Server Components:

- To Use the SharePoint Web Parts: Microsoft Windows SharePoint Services 2003, SharePoint Portal Server 2003, SharePoint 2007, or SharePoint 2010

Ensure your client systems meet the following requirements:

- Microsoft® Internet Explorer 7.0 or later – or Firefox 1.5 or later (Note: the Admin web site requires Internet Explorer)

To allow password resets from the Windows logon screen using AD Password, you must install the AD Password Windows client on each client PC. The AD Password Windows client is a GINA Extension that is deployed on each client computer. The Windows client may be deployed silently using Microsoft Active Directory Group policy or a software deployment tool such as Microsoft SMS Server.

To use the AD Password Windows client, computers must meet the following minimum software requirements:

- Microsoft Windows XP x86 Service Pack 1 or later, or Microsoft Windows Vista x86 or x64, or Microsoft Windows 7 x86 or x64
- Microsoft Internet Explorer version 7.0 or later

AD PASSWORD USER INTERFACE OPTIONS

The AD Self-Service Suite is unique in offering multiple access points or user interfaces for end users. AD Self-Service brings the services to the users instead of requiring them to learn new habits and navigate to a dedicated web site to use the applications. AD Self-Service seamlessly integrates into the user interface of commonly used applications like Microsoft SharePoint providing access to directory search and self-service at any time from the applications they are accustomed to using.

Each application in the AD Self-Service Suite offers the following user interface options:

- Web application – each application may be accessed as a standard web application with a dedicated URL
- SharePoint web part — each application offers a full-featured SharePoint Web Part that may be deployed to any existing Windows SharePoint Services site or SharePoint Portal Server Area
- Toolbar button deployment – each application offers a small form factor toolbar button that may be deployed into the user interface of your SharePoint or custom ASP.NET web application. The toolbar deployment will display a button for each application to which the user has been granted access. The toolbar buttons appear as a natural part of the existing application interface. Clicking on a toolbar button will launch a small on-screen version of the respective application.

Other AD Self-Service installable components:

- Admin web site – the admin web site must be installed on at least one site on each server.
- Configurator – the AD Self-Service Configurator is a Windows application used to deploy and un-deploy the AD Self-Service user interface components. Using the Configurator, the AD Self-Service application web sites, web parts, and toolbars may be installed and uninstalled from the IIS web sites on a server.
- AD Password Reset Center — this anonymous web site is used by users to reset forgotten/expired passwords and unlock locked-out accounts. The Password Reset Center may be installed on any number of servers.

- AD Password for Windows client (GINA Extension) — The Windows client is an application that may be deployed silently to your desktop PCs. The settings for the GINA are managed centrally via available custom Group Policy templates. The Windows Client utilizes the Recovery Center web site and must be configured with the URL of the web site it should use.

BEFORE YOU START: CHECKLIST

Please see the AD Self-Service Suite Getting Started Guide for installation and basic setup instructions. This guide covers more detailed configuration of the AD Password application and assumes that all application components, applications pools, web applications, toolbars, and web parts have been deployed using the Configurator as outlined in the AD Self-Service Suite QuickStart Guide. This guide also assumes that proxy user accounts for all relevant domains have been configured in the Admin web site as per the AD Self-Service Suite QuickStart Guides If these steps have not yet been completed, please refer to the AD Self-Service Suite QuickStart Guide before proceeding with the AD Password specific settings.

Steps to complete before using this guide:

- Install the AD Self-Service Suite on your desired server
- Using the Configurator:
    - Assign the service account
    - Deploy all web applications, toolbars, web parts and Recovery Centers to your desired IIS web sites
- From the Admin web site:
    - Configure Directory Connections with proxy user accounts for all domains you wish to enable for AD Password
    - Assign users or groups as administrators to grant or restrict access to the Admin web site

Following completion of these steps, you may configure the required and optional settings for AD Self-Service AD Password.

CONFIGURING THE AD SELF-SERVICE AD PASSWORD SETTINGS

The following sections detail the configuration of the AD Self-Service AD Password-specific settings using the AD Self-Service Suite Admin web site.

USING THE AD SELF-SERVICE ADMIN WEB SITE:

The AD Self-Service Admin web site is used to manage all of the settings for each application in the AD Self-Service Suite. The Admin web site may be installed and activated on any domain member server meeting the installation requirements listed previously.

AD Self-Service Suite for Active Directory

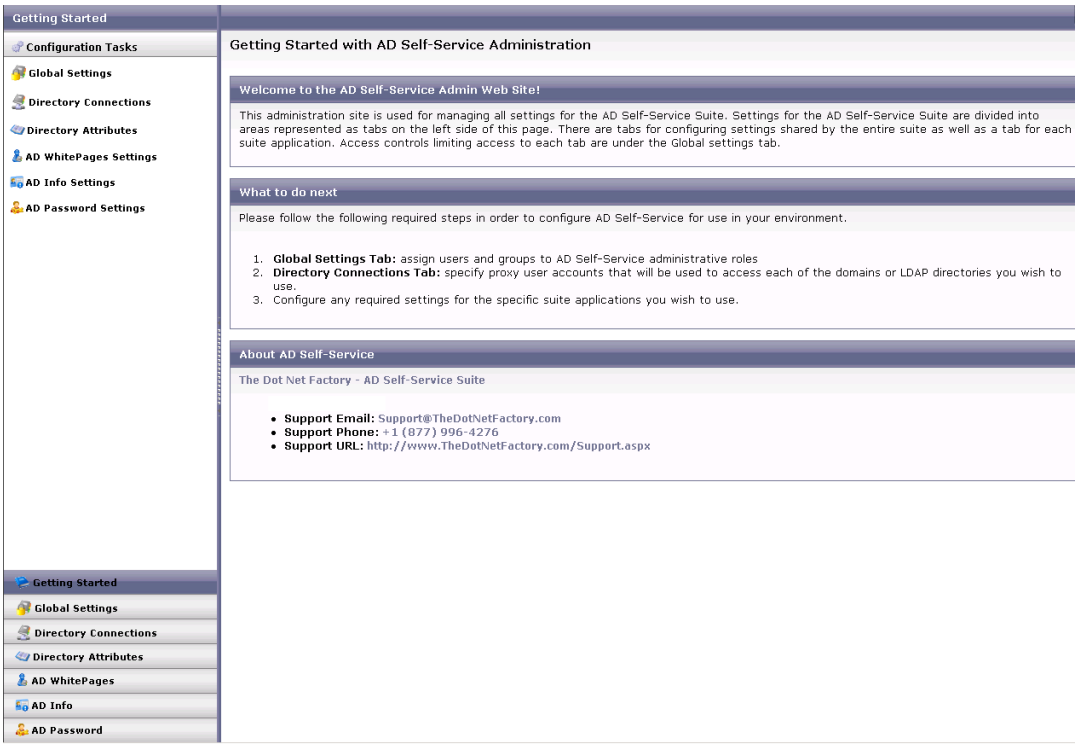
Getting Started Guide for AD Password

Note: The AD Self-Service Admin web site may be found at the following URL on any server it has been activated using the Configurator: http(s)://servername/ADSelfService/Admin/default.aspx

1. Navigate to the Admin web site using Internet Explorer 7.0 or greater: http://servername/ADSelfService/Admin/default.aspx

2. Upon initial installation, the Admin web site is accessible by any user. This should be changed immediately upon installation.

3. Click on the Password tab entry under the Configuration Tasks pane to navigate to the AD Password settings area.



AD PASSWORD SETTINGS OVERVIEW

The AD Password Administration site is divided into four tabs:

- Profiles
- Localization
- Recovery Center
- Reporting

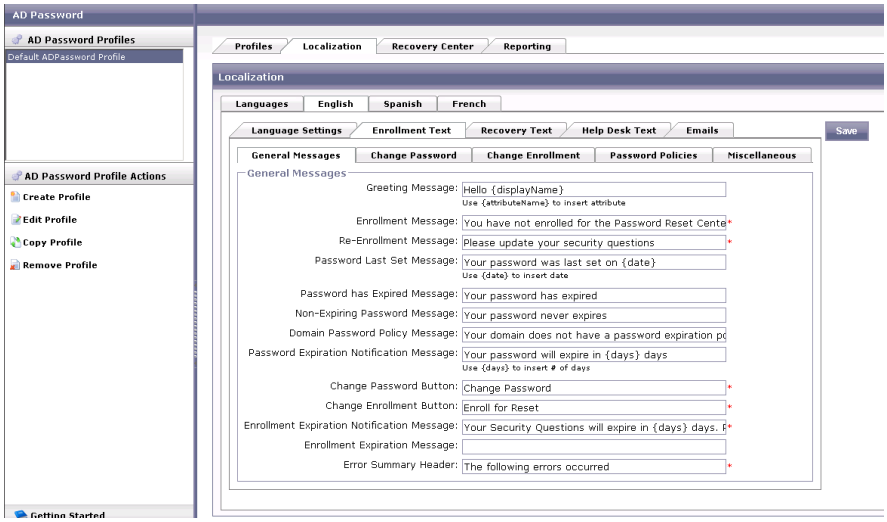
After these tabs are configured, select the 'Default ADPassword Profile' to modify. It also has four unique tabs: General, Access Control, Policies, Questions.

Note: AD Password is localizable into multiple languages. Selecting the corresponding language tab under Localization will allow configuration of language specific settings.

TAB ONE—PROFILES

The profile tab is for reference, it needs no modification. It has useful tips listed for the AD Password Profile.

TAB TWO—LOCALIZATION



The localization tab allows for customization of any and all the text used as labels or messages during the password enrollment and change password process. You may also change the password policy text to better reflect your environment's security and legal policies. Customization is on a per language basis and will modify the text in the configuration of the language currently selected with the flag at the top of the administration site.

AD Self-Service Password exposes all text used as labels, buttons or messages in the Password Reset Center for customization. The text, messages, and button labels used in each step of the recovery process may be fully customized. A customizable legal disclaimer is also provided in step 1 of the recovery process. This verbiage may be customized to use your own legal language to validate users before using the Password Reset Service. Customization is on a per language basis and will modify the text in the configuration of the language currently selected with the flag at the top of the administration site.

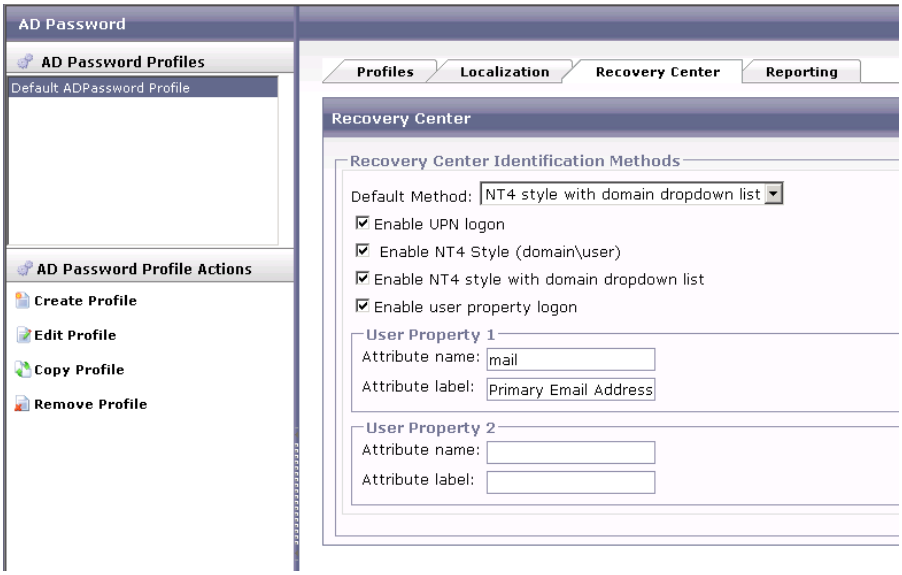
Email Alerts

Alert notifications can be triggered by various events, some of which provide the user with confirmation of their actions and others that enhance security by warning administrators of possible brute force or takeover attempts. You may configure each of the following to be an Administrator Email Alert, a User Email Alert, or both by checking the appropriate boxes. Also, note that each Email Alert is fully customizable, including active fields such as {displayName} that will propagate with the users' information when the Email Alert is sent.

- Reset Password: Triggered when a user completes the recovery process through the Recovery Center. (You may want to send the user an Email Alert informing them that they have completed Password Reset and to contact the Help Desk if they did not reset it themselves)
- Change Password: Triggered when a user changes their password through the AD Password webpage or web part. (You may want to send the user an Email Alert informing them of the password change and to contact the Help Desk if they did not change it themselves)
- User Enrollment: Triggered every time the user completes the enrollment process. (You may want to send the user an Email Alert congratulating them on enrolling, as well as information on the enrollment process and a note to contact the Help Desk if they did not enroll themselves)
- Unlock Account: Triggered when a user unlocks their account by completing the recovery process through the Recovery Center. (You may want to send the user an Email Alert congratulating them on unlocking their own account and to contact the Help Desk if they did not unlock it themselves)
- Failed Recovery: Triggered when a user incorrectly answers their enrollment questions. (You may want to send the user an Email Alert informing them that there has been a failed attempt to answer their enrollment questions and to re-enroll immediately if they were not the one attempting to use the Recovery Console)
- Recovery Center Lockout: Triggered when a user locks themselves out of the Recovery Center by answering the enrollment questions incorrectly a set number of times over a certain period of time, definable under the Policies tab. (You may want to send the user an Email Alert informing them that they have been locked out due to an excessive amount of failed attempts to answer their enrollment questions and to re-enroll immediately if they were not the one attempting to use the Recovery Console)

- Successful Recovery: Triggered when a user answers their enrollment questions correctly. (You may want to send the user an Email Alert congratulating them for answering the enrollment questions correctly)

TAB THREE—RECOVERY CENTER

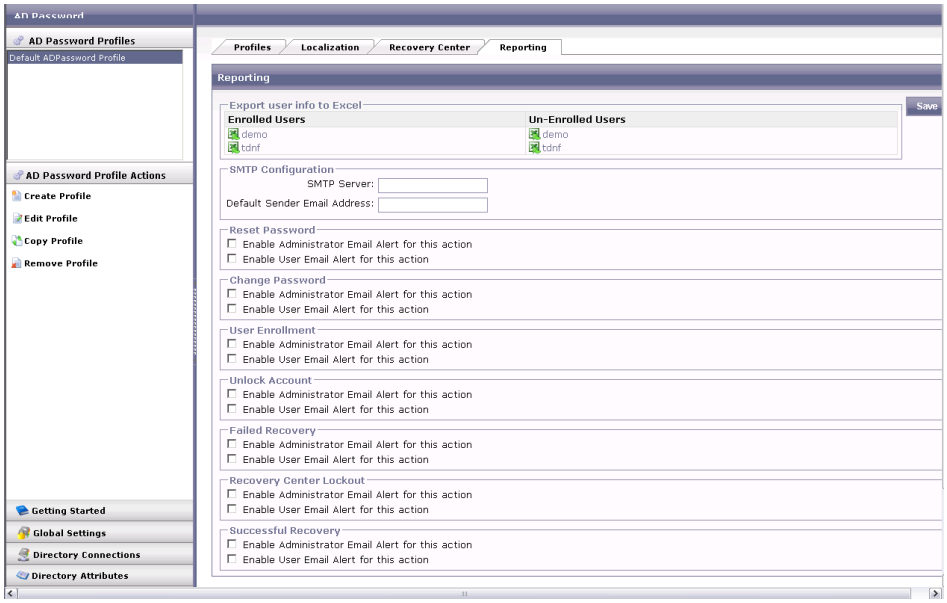


Recovery Center identification methods

There are four unique Recovery Center identification methods that can be enabled or disabled through the administration page. This changes the manner in which a user will authenticate during the Password Reset process. *It is recommended that you select one of these for your users to avoid confusion*

- Enable UPN logon: Allows a user to login using UPN credentials. UPN logon names are typically in the format of (username@DOMAIN)
- Enable user property logon: Allows a user to login by entering the values for their Active Directory attributes such as e-mail, last name, and employee ID. You may also enter a custom attribute name here (which is case sensitive).
- Enable NT4-style logon: Allows a user to login using a NT4-style logon (DOMAIN\username). This option does not show a list of domains that are available, which enhances security by requiring a user to know the domain name in order to login.
- Enable NT4-style logon with domain drop down list: Allows a user to login using NT4-style logon, but with a selectable domain drop down box. This method is the most user friendly and most widely used.

TAB FOUR—REPORTING



AD Self-Service AD Password has powerful reporting tools that you may utilize in order to meet your internal audit policies. Any domain that you configure under Directory Connections will appear in the Reporting tab. You can also send e-mails to both the administrator and user for any event triggered by AD Password. A best practice is to enable the Administrator Email Alerts for the Recovery Center Lockout

Export user info to Excel

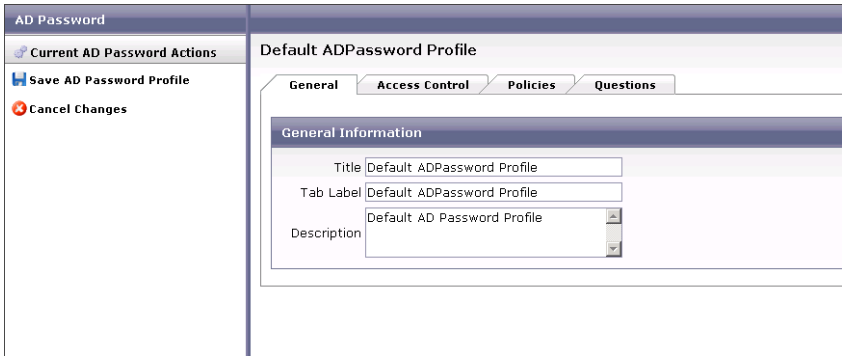
Note: If Microsoft Excel is not installed, you may rename the report's extension to .htm and open it with a web browser.

- **Enrolled Users:** To export a spreadsheet of all enrolled users for a particular domain, simply click on the domain name you wish to audit under the Enrolled Users column.
- **Un-Enrolled Users:** To export a spreadsheet of all users who have not yet enrolled for a particular domain, click on the domain name you wish to audit under the Un-Enrolled Users column.

SMTP Configuration

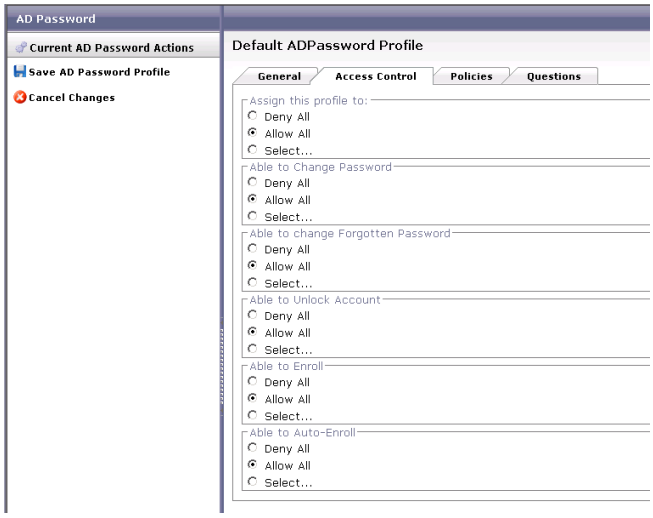
A valid SMTP Server is a pre-requisite for any of the Email Alert features listed below. (Example: smtp.company.com)

AD PASSWORD PROFILE TAB 1 —GENERAL TAB



The General tab allows configuration of the Title as shown in the Admin website along with Tab Label and Description.

AD PASSWORD PROFILE TAB 2 — ACCESS CONTROL TAB



AD Self-Service allows granular permission assignment for features and actions in the AD Password Access Control tab, granular control is offered over which users may change their password, unlock their accounts, or enroll for Password Reset.

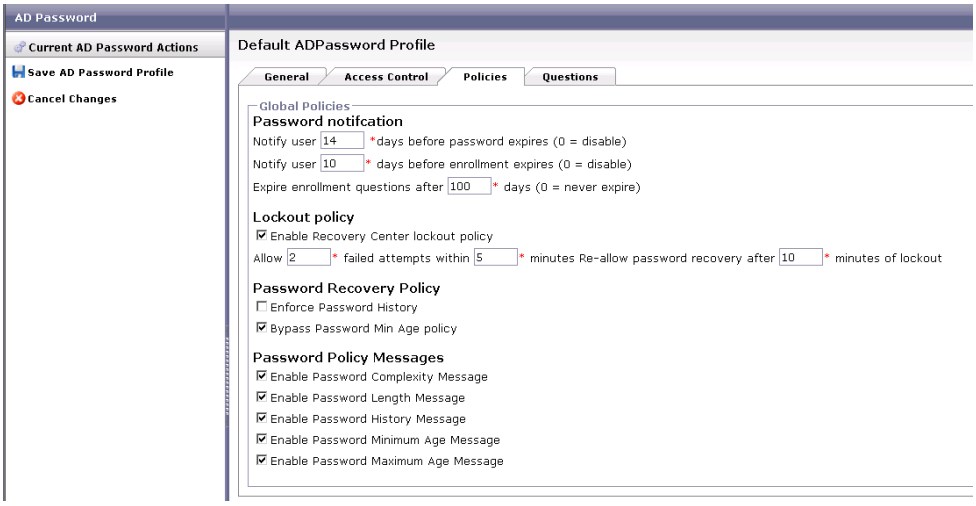
Permissions may be assigned in the following manner:

- Deny All – Denies all users or groups the ability to perform the action or access the feature. If this option is selected, ALL users and groups will be denied the feature or task and the corresponding user interface button or element will disappear from the AD Password user interfaces.
- Allow All – Allows ALL users or groups to perform the action or feature.

- Select… – Allow or deny the ability to perform the action or feature for specific users or groups. (Clicking on the person icon with the magnifying glass will allow you to search the domain)

  It is a best practice if you are going to use the Auto-Enroll feature to Allow Domain Users and Deny Domain Admins

AD PASSWORD PROFILE TAB 3 — POLICIES TAB



The Policies tab is where you can specify values for expiration notification bubbles, define recovery center lockout policies and choose recovery center identification methods.

Password notification

- Expire enrollment questions after [ ] days: Allow enrollment questions to expire after a specified number of days. (Use 0 to have questions never expire)

- Notify User [ ] days before password expires: Specify the number of days a user will be notified that their password is going to expire. (Use 0 to disable)

- Notify User [ ] days before enrollment expires: Specify the number of days a user will be notified that their enrollment answers are going to expire. (Use 0 to disable)

Lockout policy

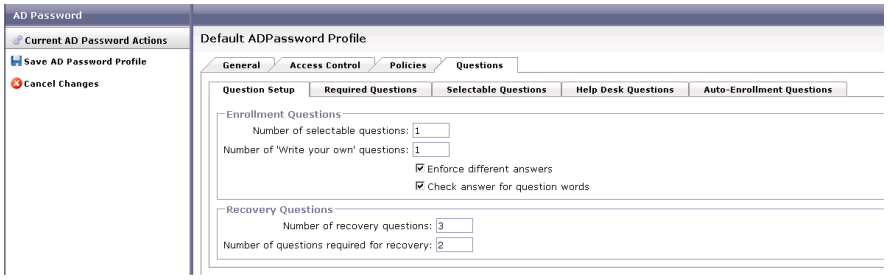
- Enable Recovery Center lockout policy: Enables a specified Recovery Center lockout policy. You may allow a certain, configurable amount of failed attempts at Password Reset over a certain period of time before locking out an account for a specified amount of time. (This is an optional security feature you may wish to enable in order to prevent brute force attempts on enrollment answers)

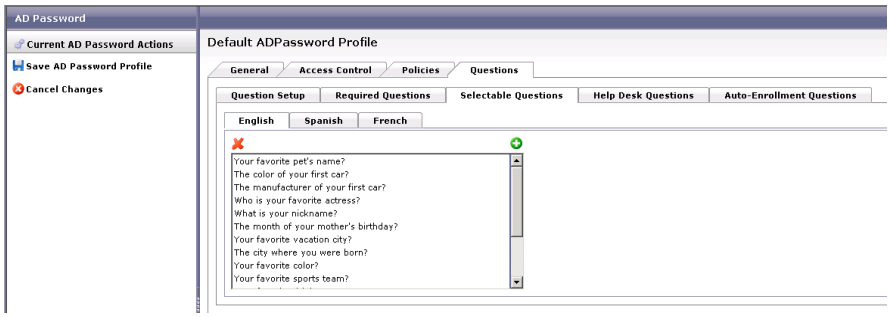
Password Recovery Policy

AD Password is unique in its support for password history enforcement. Windows password history can disallow users from reusing their last X passwords. This capability can be enabled even for users resetting their forgotten

password in the Recovery Center. Note: enabling password history enforcement in AD Password will push out one password from the history every time it resets a password.

AD PASSWORD PROFILE TAB 4 — QUESTIONS TAB





The Questions tab allows complete management of your enrollment questions. Out of the box questions are provided but others may be added, modified, deleted and classified. Classifications include Required, Selectable or Write your own. Required Questions will always appear for users to answer when enrolling in the Password Reset Service. Selectable Questions will appear as options in the dropdown lists and users must answer the number of questions specified in the Question Setup section on this tab. Questions may be edited by clicking on the pencil or deleted by clicking on the red X. Minimum answer lengths are specified for each question enforcing appropriate responses along with the option to allow failure. You may also define the total number of selectable questions and the number of 'write your own' questions under the Question Setup section, as well as enforcing different answers for each question.

DEPLOYING THE AD PASSWORD SHAREPOINT WEB PART

Once you have installed and configured AD Self-Service AD Password, you can deploy the AD Password web part on any of your SharePoint sites or pages. The AD Password web part is deployed to the Virtual server gallery if the SharePoint option was selected on the AD Password application tab in the AD Self-Service Configurator.

From the SharePoint page on which you wish to deploy the web part, simply browse the available web parts and add to your page

GIVING END USERS ACCESS TO PASSWORD

To give end users access to AD Password, use the following:

- To change passwords or enroll for Password Reset:

  http(s)://<server where AD Password is installed>/ADSelfService/ADPassword/

- To reset their password or unlock their user account:

  http(s)://<server where AD Password is installed>/ADSelfService/RecoveryCenter/

Note: the Configurator can configure any of your IIS web sites using Windows authentication (Basic or Integrated) to automatically redirect users to the Password Reset Center upon user logon failure. In most cases, users will not have to remember this URL and will automatically be redirected their upon logon failure. Other web sites or web applications using Windows accounts may be manually configured to provide the same functionality.

- AD Password is also available to end users as an embedded button in the AD WhitePages user interface.
- AD Password is also available as a web part that can be deployed on any WSS site or Portal Area
- AD Password is also available as a toolbar button that can be deployed in the header of SharePoint – the Toolbar is available as a web part or as a global deployment option. The global deployment option causes the Toolbar to automatically be loaded on every single page without repeated deployment or management.

INSTALLING THE AD PASSWORD WINDOWS CLIENT

The AD Password Windows client is a GINA (Graphical Identification and Authentication dynamic-link library) extension that must be installed on your client PCs. It may be installed manually by running the MSI file or may be deployed using Active Directory Group Policy or another software deployment tool like Microsoft SMS. All settings for the Windows client are stored in the Windows registry and may be managed directly or centrally using Custom Group Policy Templates.

Note: Installing the AD Password GINA Extension on a computer where any other third-party GINA extension is installed will disable that third-party GINA extension. When you uninstall the AD Password GINA Extension, the previous GINA extension will be re-enabled.

For the latest version of our GINA please use the links below

http://www.adselfservicesuite.com/downloads/gina.zip - Windows XP

http://www.adselfservicesuite.com/downloads/ginaX64.zip - Windows Vista/Windows 7 X64

http://www.adselfservicesuite.com/downloads/ginaX86.zip - Windows Vista/Windows 7 X86

http://www.adselfservicesuite.com/downloads/AD.Self.Service.Suite.GINA.pdf - Documentation

UPGRADING FROM PREVIOUS VERSIONS OF AD PASSWORD

The current version of AD Password and previous version know as Password Manager, stores user enrollment questions and answers as encrypted information in their user object. This information will be automatically maintained and is not affected when you upgrade, install or uninstall AD Password or Password Manager.

If you have a previous version of The Dot Net Factory AD Password, backup your settings files and remove the previous version before installing the newest version of AD Password. After installing, add password management to all of the domains that you managed before. Please contact support for questions concerning settings migration.