

The Dot Net Factory

AD Self-Service Suite for Active Directory

Admin Guide

Table of Contents

| | |
|--|----|
| ABOUT THE DOT NET FACTORY | 3 |
| SYSTEM AND INSTALLATION REQUIREMENTS..... | 5 |
| IIS ROLES | 5 |
| REQUIRED USER ACCOUNTS FOR THE AD SELF-SERVICE SUITE..... | 6 |
| INSTALLATION USER ACCOUNT: | 6 |
| DIRECTORY CONNECTION (PROXY) ACCOUNT:..... | 6 |
| LOCAL PROXY ACCOUNT: | 6 |
| APPLICATION POOL IDENTITY: | 6 |
| INSTALLING THE AD SELF-SERVICE SUITE..... | 7 |
| THE AD SELF-SERVICE CONFIGURATOR: | 7 |
| SETTINGS TAB – CONFIGURING STORAGE AND PROXY ACCOUNTS..... | 7 |
| Local Proxy Account | 7 |
| LICENSE TAB – NOTIFICATION EMAIL | 8 |
| APPLICATION TABS – ACTIVATING USER INTERFACES..... | 9 |
| ADMIN WEBSITE | 9 |
| AD WHITEPAGES | 10 |
| AD INFO..... | 11 |
| AD PASSWORD | 12 |
| WEBPARTS – CONFIGURE AD SELF-SERVICE WEBPARTS | 13 |
| ADMINISTRATION CONSOLE | 14 |
| USING THE AD SELF-SERVICE ADMIN WEBSITE | 14 |
| GETTING STARTED..... | 14 |
| DIRECTORY CONNECTIONS: | 15 |
| ACTIVE DIRECTORY CONNECTION - FOREST | 15 |

| | |
|--|----|
| ACTIVE DIRECTORY CONNECTION – OTHER FOREST | 15 |
| GLOBAL SETTINGS | 16 |
| LICENSE CONFIGURATION..... | 16 |
| ACCESS CONTROL..... | 17 |
| DIRECTORY ATTRIBUTES | 19 |
| GENERAL | 20 |
| ADVANCED | 21 |
| CONTROL TYPES | 21 |
| LIST ITEMS | 22 |
| VALIDATORS TAB..... | 22 |
| AD WHITEPAGES | 23 |
| DIRECTORY VIEWS..... | 23 |
| AD INFO..... | 30 |
| AD INFO VIEWS | 30 |
| AD PASSWORD | 34 |
| PROFILES | 34 |
| LOCALIZATION..... | 35 |
| RECOVERY CENTER..... | 38 |
| REPORTING | 39 |
| AD PASSWORD PROFILE..... | 40 |
| INSTALLING THE AD PASSWORD WINDOWS CLIENT | 45 |
| IMPORTANT URLS | 45 |

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: <http://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

© The Dot Net Factory, LLC. 2005-2011. All rights reserved.

This guide contains proprietary information, which is protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of The Dot Net Factory, LLC.

Warranty

The information contained in this document is subject to change without notice. The Dot Net Factory makes no warranty of any kind with respect to this information. THE DOT NET FACTORY SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTY OF THE MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. The Dot Net Factory 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

The Dot Net Factory® and AD Self-Service® are trademarks of The Dot Net Factory, LLC. Other trademarks and registered trademarks used in this guide are property of their respective owners.

Headquarters

4393 Tuller Road

Dublin, Ohio 43017

<http://www.ADSelfServiceSuite.com>

e-mail: info@TheDotNetFactory.com

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

AD Self-Service Password Getting Started Guide

SYSTEM AND INSTALLATION REQUIREMENTS

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

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

Ensure that your system meets the following minimum software requirements:

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

Optional Server Components:

- Microsoft SharePoint 2010 or SharePoint 2007

Ensure that your client systems meet the following requirements:

Microsoft Internet Explorer 8 or later – Firefox 1.5 or later

Note: Admin website requires Internet Explorer

IIS ROLES

- Web Server
- Common HTTP Features
- Static Content
- Default Document
- Directory Browsing
- HTTP Errors
- Application Development
- ASP.NET
- .NET Extensibility
- ISAPI Extensions
- ISAPI Filters
- Health and Diagnostics
- HTTP Logging
- Request Monitor
- Security

- Basic Authentication
- Windows Authentication
- Request Filtering
- Performance
- Static Content Compression
- Dynamic Content Compression
- Management Tools
- IIS Management Console
- Management Service
- IIS 6 Management Compatibility
- IIS 6 Metabase Compatibility

REQUIRED USER ACCOUNTS FOR THE AD SELF-SERVICE SUITE

INSTALLATION USER ACCOUNT:

The user logged on to the AD Self-Service Suite server during installation must be a domain user that is a member of the Local Administrators group. Please do not use a domain account that also exists as a local account on the machine with the same name (ex. Administrator). The installation user will require rights to deploy a web part if the SharePoint option is going to be used.

DIRECTORY CONNECTION (PROXY) ACCOUNT:

The Directory Connection (Proxy) Accounts are used by the applications in the AD Self-Service Suite to retrieve information from your Active Directory domains or LDAP partitions and perform all account management and modification actions. These accounts must reside in their respective domain or directory and will require the necessary privileges needed to perform any action used in the AD Self-Service applications implemented. A member of the Domain Administrators group may be used for simplicity.

Note: The password for the Directory Connection Account may contain special characters, all but the & symbol

LOCAL PROXY ACCOUNT:

The Local Proxy Account is used to write to the event log and perform other local operations. This account must be specified on each server running the AD Self-Service Suite. This user account must be a member of the Local Administrators group. This account may be either a local or domain user account.

Note: The password for the Local Proxy Account may contain special characters, all but the & symbol

APPLICATION POOL IDENTITY:

The ADSelfService Application Pool Account is created **after** you deploy the web applications. The Identity needs to be set to Local System.

INSTALLING THE AD SELF-SERVICE SUITE

To install The Dot Net Factory AD Self-Service Suite:

1. Logon to the server with the "Installation User Account"
2. Locate your AD Self-Service Suite installation file
3. Right click and select "Run as administrator"
4. Click to run the setup program
5. Select "Next" on all setup screens and click "Finish"

Following installation, you will find a new "The Dot Net Factory" program group in your server's Start Menu. Please run the "AD Self-Service Configuration" shortcut by right clicking and select "Run as administrator" to complete the configuration of your server.

THE AD SELF-SERVICE CONFIGURATOR:

The AD Self-Service Configurator is a .NET 2.0 Windows application designed to activate or remove the various member applications of the AD Self-Service Suite from a server. The Configurator allows activation or deactivation of the web applications and web parts. The Configurator also allows for configuration of the Local Administration account used for event logging.

SETTINGS TAB – CONFIGURING STORAGE AND PROXY ACCOUNTS

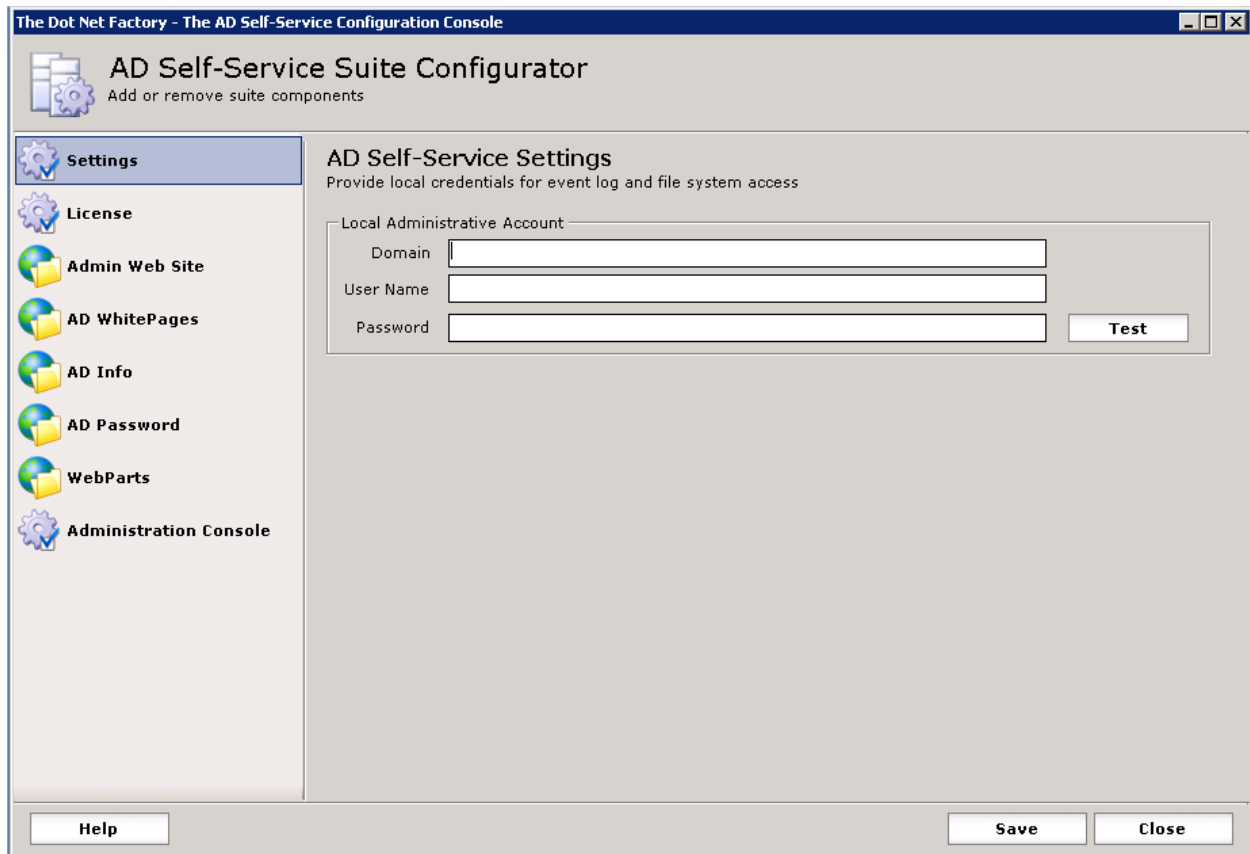
The settings tab is used to setup the account used by AD Self-Service for any local system access including writing to the event log. This account may also be referred to as the Local Proxy Account

Local Proxy Account

The local proxy account that you enter below must be a member of the local Administrators group on the AD Self-Service server.

Note: The password for the Local Proxy Account may contain special characters, all but the & symbol

Please type the NetBIOS Domain name into the first box, then the username and password into the appropriate boxes.



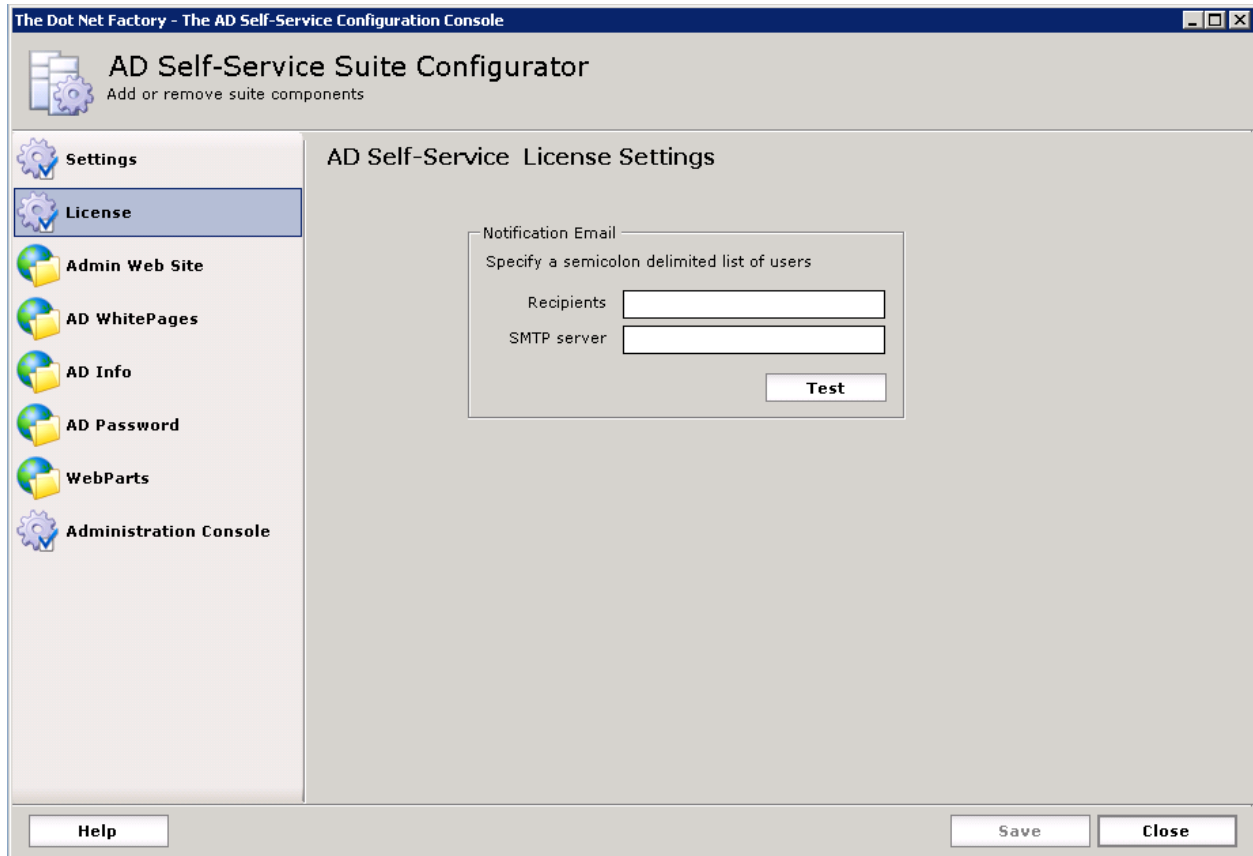
The "Test" button can be clicked to verify that the specified account has the required privileges. If the test is successful, you will see a success message. If the test fails, please re-enter the username and password or try another account.

Once you have entered an account with the necessary privileges, click the "Save" button at the bottom of the window to commit the configuration.

LICENSE TAB – NOTIFICATION EMAIL

The License tab of the Configurator is used to configure license notification emails. If this is filled out the recipient will receive an email when the License File is due to expire.

To configure the license notification emails, place the email address in the recipient's box. If there is more than one entry, separate with a semicolon. Then enter the SMTP Server name. Use the "Test" button to send a test email.



License files will be sent to you by The Dot Net Factory Support Team.

The basic process for licensing your trial copy is to copy the License.xml file that is sent to you by The Dot Net Factory Support Team into the directory of <Server AD Self-Service Suite is installed> C:\Program Files (x86)\The Dot Net Factory\AD SelfService Suite\Settings

APPLICATION TABS – ACTIVATING USER INTERFACES

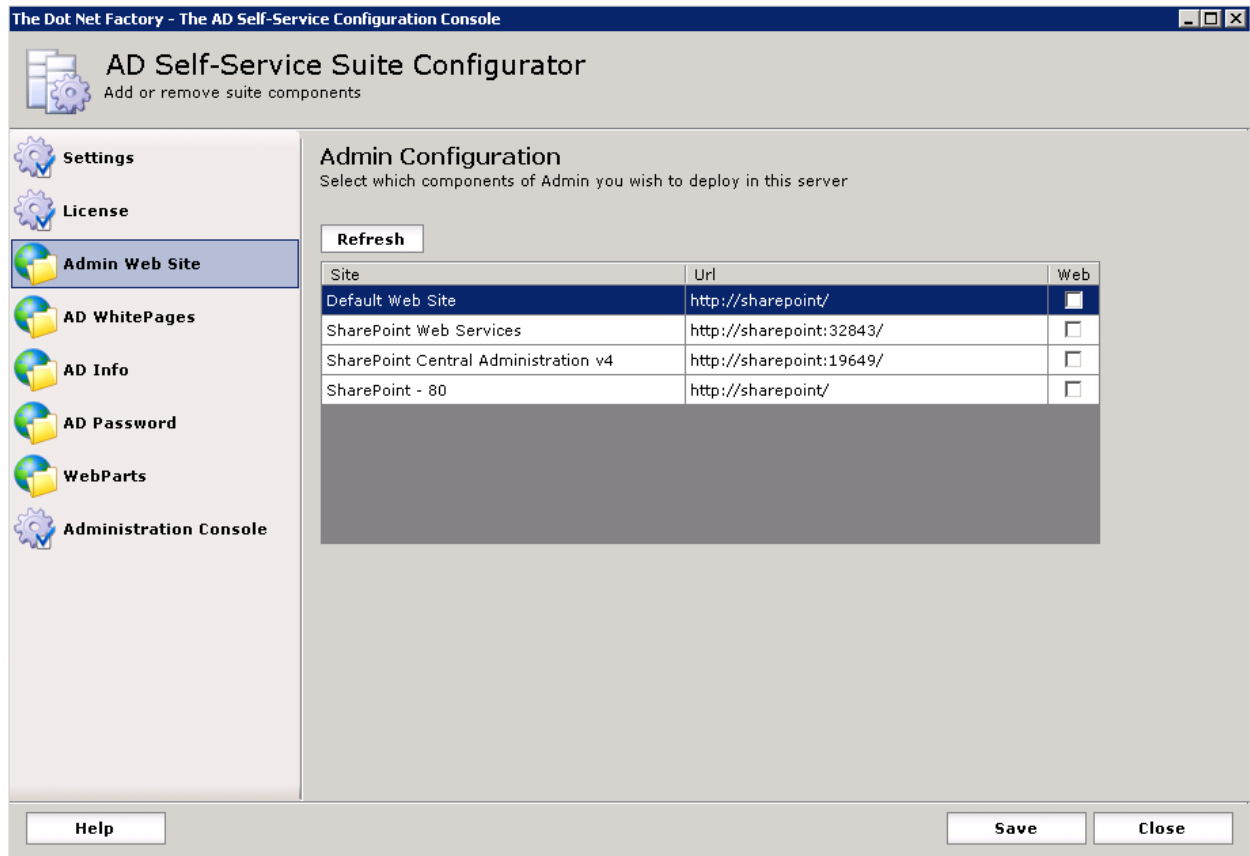
The Configurator provides a tab for each application in the suite to activate the user interface you wish to use in your environment.

ADMIN WEBSITE

The AD Self-Service Admin website is used to manage all of the settings for each application in the AD Self-Service Suite. This will only need to be deployed to one of the listed IIS sites listed below.

Note: If this is on a SharePoint server you may want to deploy this to the Central Admin website. In environments where the SharePoint sites will be load balanced, this configuration will allow you to be certain to which server you are working with.

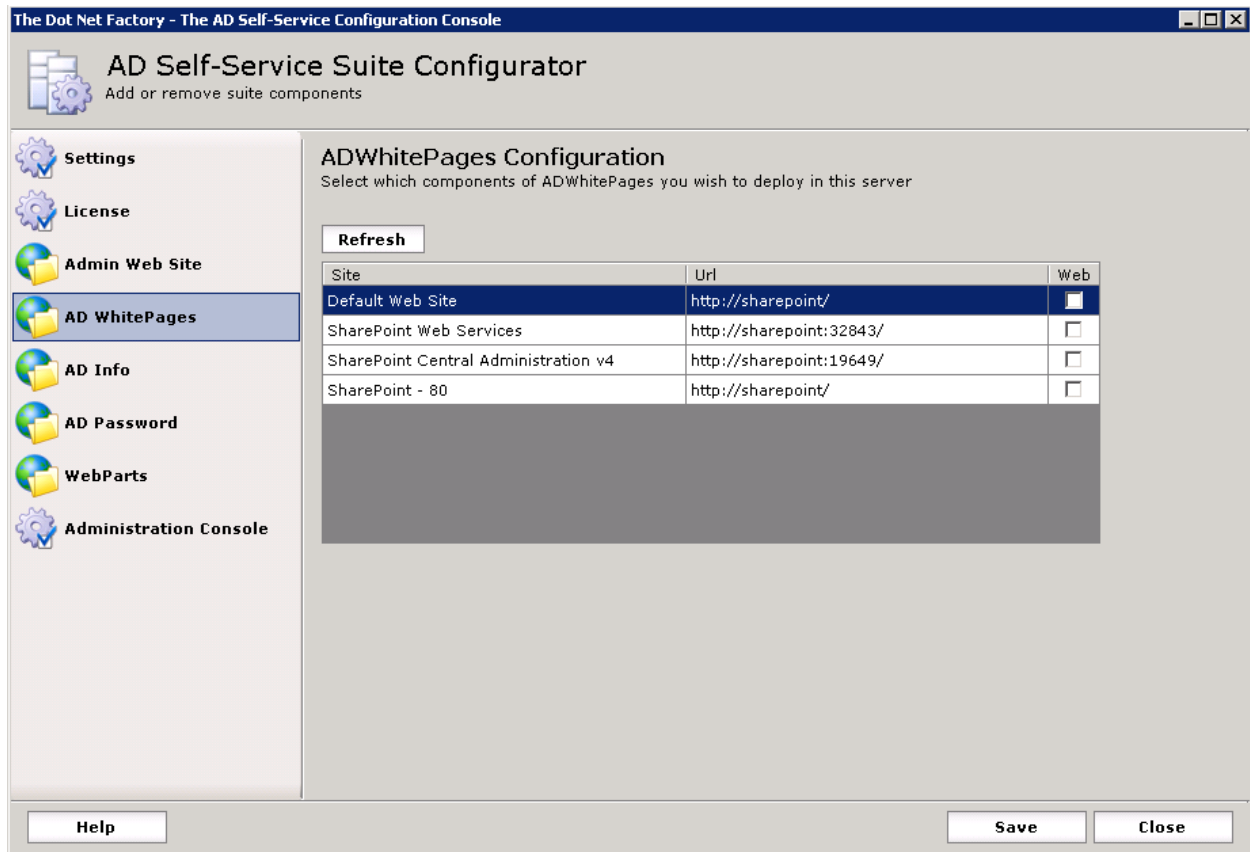
After you make your selection by checking the user interface on the desired IIS Site, click the “Save” button at the bottom of the screen to commit the changes



AD WHITEPAGES

AD WhitePages is a web-based directory application designed to make Active Directory an easy to use, up to date and interactive source for employee information

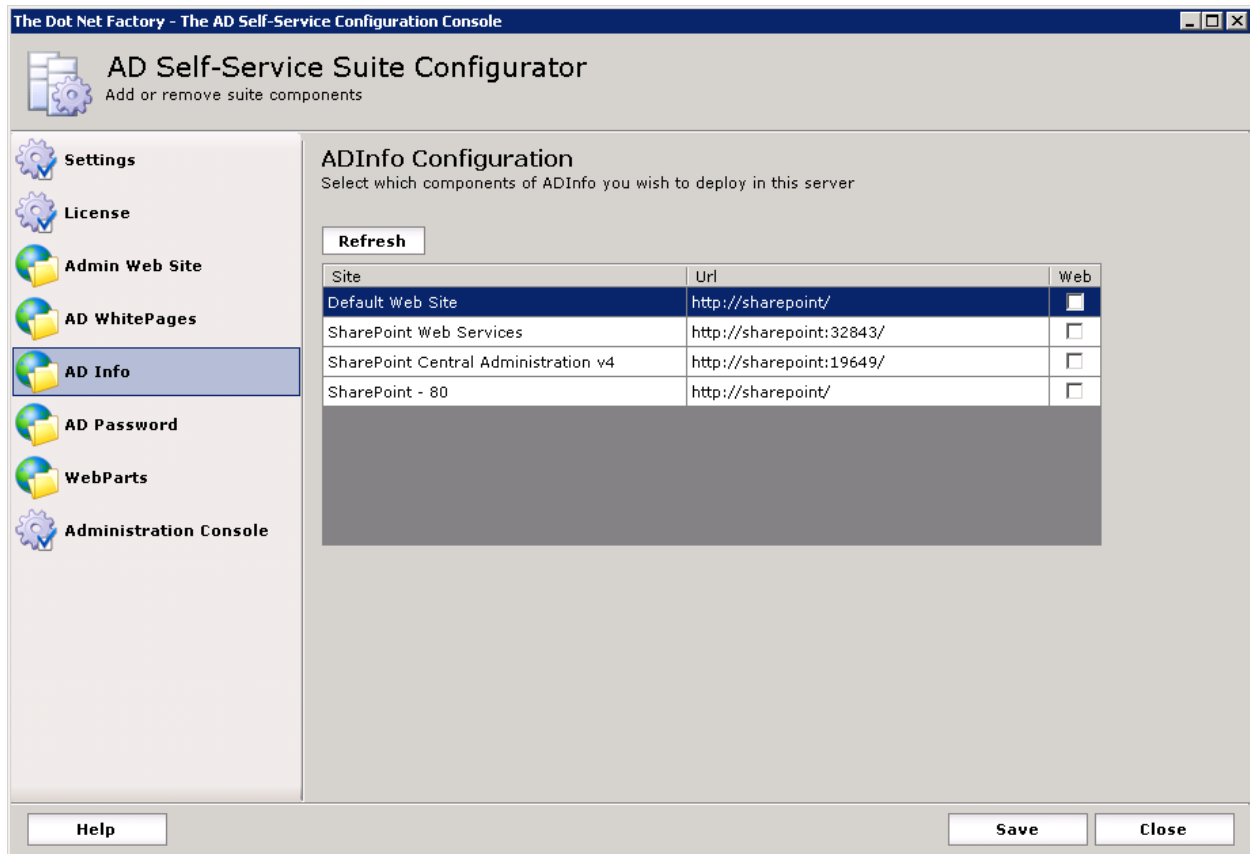
After you make your selection by checking the user interface on the desired IIS Site, click the "Save" button at the bottom of the screen to commit the changes



AD INFO

AD Info is a web-based self-service application that lets users update their own directory information with restrictions set by the Administrator

After you make your selection by checking the user interface on the desired IIS Site, click the "Save" button at the bottom of the screen to commit the changes



AD PASSWORD

AD Password is a web-based self-service application that allows users to reset forgotten passwords and unlock their locked-out accounts. AD Password offers multiple interfaces allowing users to change their passwords or enroll in the AD Password Reset Service eliminating the source of the number one help desk call

WEB

Web interface where Authenticated users can change their passwords and Enroll for the AD Password Reset Service

RECOVERY CENTER

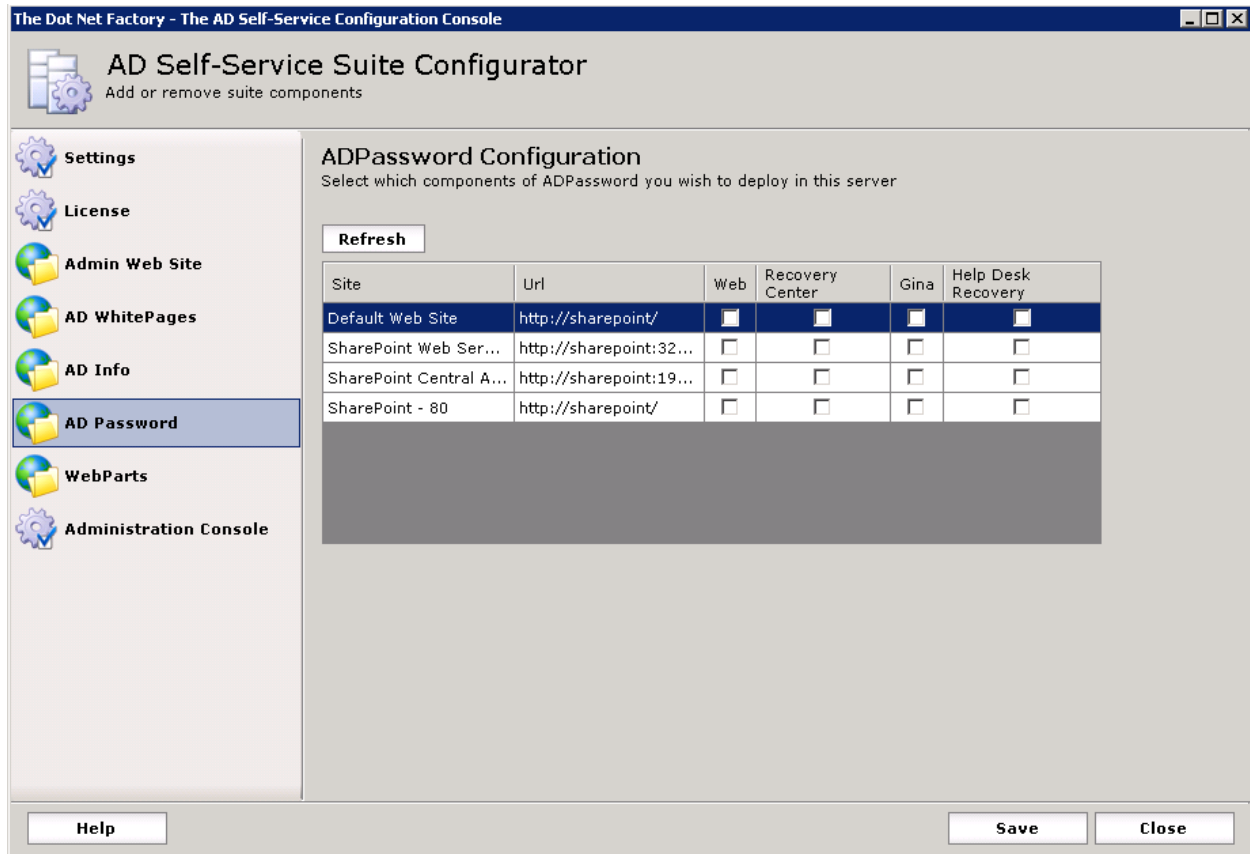
Web interface for users to reset their forgotten passwords and unlock their locked-out accounts

GINA

Web interface for users to utilize the Recovery Center via the CTRL ALT Del login screen

HELP DESK RECOVERY

Web interface for your Help Desk Team to reset passwords and unlock accounts for the end users

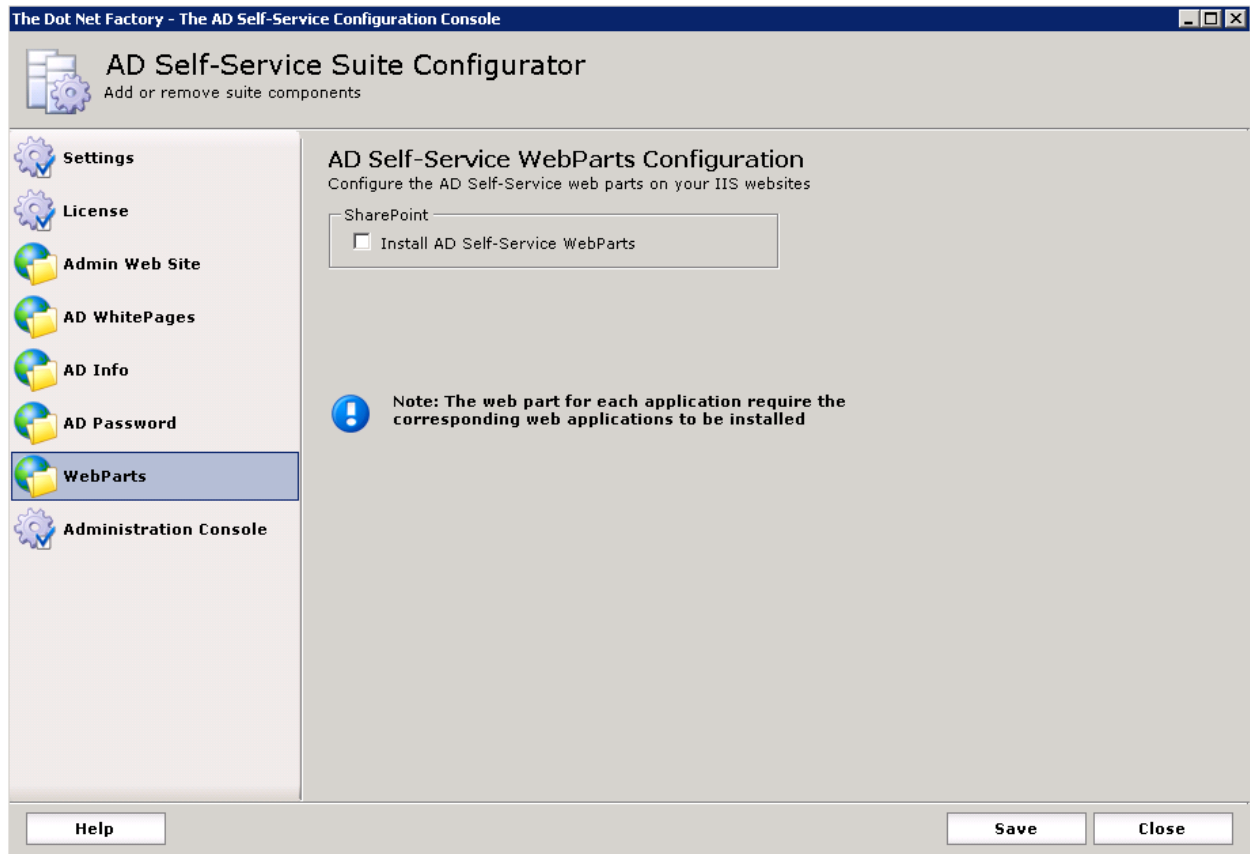


After you make your selection by checking the user interface on the desired IIS Site, click the “Save” button at the bottom of the screen to commit the changes

WEBPARTS – CONFIGURE AD SELF-SERVICE WEBPARTS

To utilize the WebPart Feature, the AD Self-Service Suite will need to be installed on a server running Microsoft SharePoint 2007 or 2010.

To deploy the WebParts simply check the user interface and click the “Save” button at the bottom of the screen.



ADMINISTRATION CONSOLE

This final tab will give you a link to the Admin website.

USING THE AD SELF-SERVICE ADMIN WEBSITE

The AD Self-Service Admin website is used to manage all of the settings for each application in the AD Self-Service Suite

The Admin website is divided into navigation sections on the left of the screen. These sections are used to navigate between the various application settings. The Global Settings, Directory Connections, and Directory Attributes tabs manage settings shared by the entire suite. The remaining tabs manage the application-specific settings.

Note: Make sure to use Internet Explorer in Compatibility Mode

GETTING STARTED


The Getting Started Tab is the first page that you will see and contains important information about your current version and methods of contacting support for any questions/concerns.

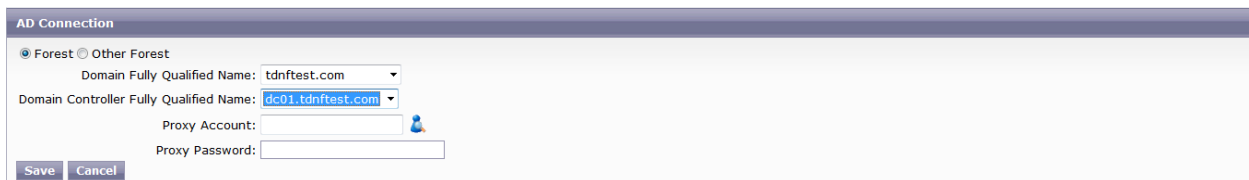
DIRECTORY CONNECTIONS:

In order to activate the AD Self-Service applications for domains in your environment, you must add the domain(s) and proxy account(s) by clicking the Add New Connection Button. This will need to be completed before any other configurations



ACTIVE DIRECTORY CONNECTION - FOREST

Select the domain you wish to add from the Domain drop down dialog box, and then select the Domain Controller you wish the AD Self-Service Suite to contact when performing actions. To setup the "Directory Connection Account" click on the blue pawn icon 



The Search for users and groups dialog box will appear in a pop up window. This window will allow you to search your domain(s) for the "Directory Connection Account"

Type in the "Directory Connection Account" password and click the "Save" button

ACTIVE DIRECTORY CONNECTION – OTHER FOREST

To manually connect to a Forest fill out the boxes blow using the Fully Qualified Naming convention

AD Connection

Forest
 Other Forest

Domain Fully Qualified Name: (i.e. thedotnetfactory.local)

Domain Controller Fully Qualified Name: (i.e. DC01.thedotnetfactory.local)

Proxy Account Name: (DOMAIN\USER)

Proxy Password:

GLOBAL SETTINGS

The Global Settings tab is used to apply licenses to the applications and to apply permissions to the Admin website and to the web applications.

Global Settings

Global Settings Actions

 License Configuration

 Access Control

Getting Started

 Global Settings

 Directory Connections

 Directory Attributes

 AD WhitePages

 AD Info

 AD Password

Global Settings

License Configuration
 Access Control

ADWhitePages
 ADPassword
 ADInfo

ADWhitePages License

Allowed AD User Accounts: 3700
 Allowed ADAM and Other LDAP Accounts: 0

Drag a column to this area to group by it.

| Domain Name | Domain Type | License Mode |
|-------------|-------------|--------------|
| | | |

LICENSE CONFIGURATION

All applications must have their licenses activated in order to function. Each application of the AD Self-Service Suite must be activated separately here.

LICENSE CONFIGURATION – LICENSE ALL

On each of the AD Self-Service applications listed, click the Add Domain button. Click on the Licensed Domain drop down and select a domain NetBIOS name to license **every** active account in the domain. This will include all service accounts

License Domain

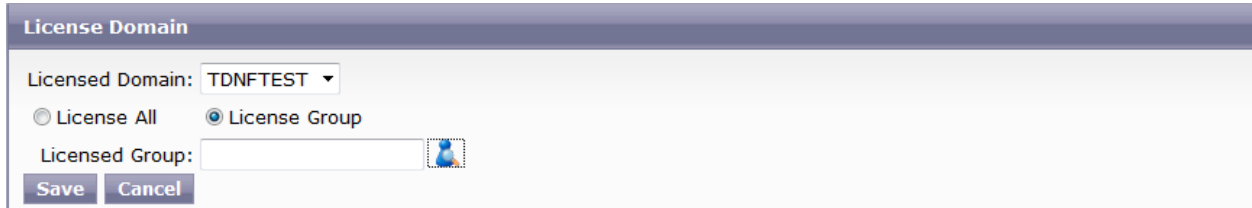
Licensed Domain: TDNFTEST

License All
 License Group


Click Save to commit the configuration to the server and activate the domain specified

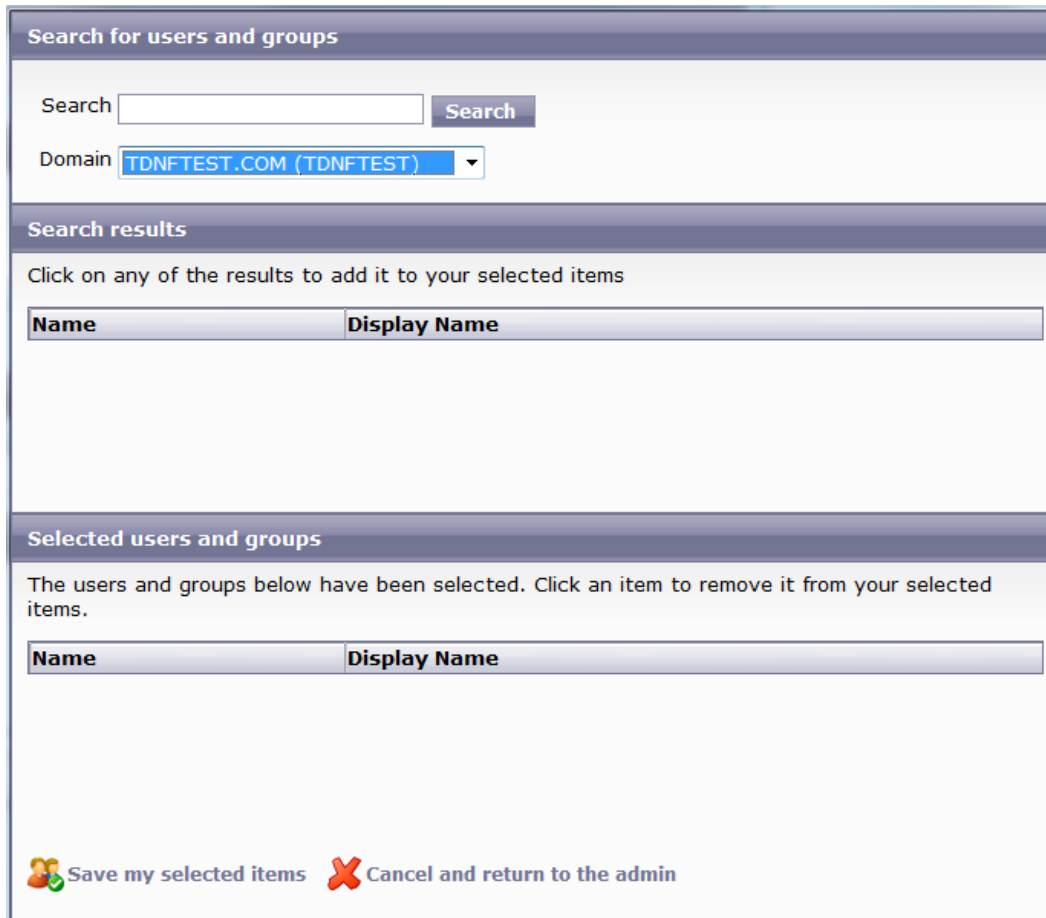
LICENSE CONFIGURATION – LICENSE GROUP

To license by group you can select the License Group option.



The screenshot shows a window titled "License Domain". It contains a dropdown menu for "Licensed Domain" set to "TDFNFTEST". Below this are two radio buttons: "License All" (unselected) and "License Group" (selected). Under "License Group", there is a text input field for "Licensed Group" and a small blue pawn icon. At the bottom are "Save" and "Cancel" buttons.

To do this click on the blue pawn icon  and search for you single layer (This option does not support nested groups) security group



The screenshot shows a window titled "Search for users and groups". It has a search input field and a "Search" button. Below is a domain dropdown menu showing "TDFNFTEST.COM (TDFNFTEST)". The "Search results" section contains the instruction "Click on any of the results to add it to your selected items" and a table with headers "Name" and "Display Name". The "Selected users and groups" section contains the instruction "The users and groups below have been selected. Click an item to remove it from your selected items." and another table with headers "Name" and "Display Name". At the bottom are two buttons: "Save my selected items" with a green checkmark icon and "Cancel and return to the admin" with a red X icon.

Click "Save my selected items"

Click Save to commit the configuration to the server and activate the domain specified

ACCESS CONTROL

By default, any user in the domain configured can access the Admin website and will be able to access any of the licensed applications.

ADMINISTRATION ACCESS CONTROL

It is recommended to lock down the Administration by specifying a user/group in the “Able to access admin website”. Using this method you can leave all the other options to “Allow All”

Global Settings

License Configuration / Access Control

Access Control Configuration

Save Cancel

Administration Access Control / Application Access Control

Able to access admin website

Deny All

Allow All

Select...

Able to manage global settings

Deny All

Allow All

Select...

Able to manage directory connections

Deny All

Allow All

Select...

Able to manage directory attributes

Deny All

Allow All

Select...

Able to manage AD Info settings

Deny All

Allow All

Select...

Able to manage AD Password settings

Deny All

Allow All

Select...

Able to manage AD WhitePages settings

Deny All

Allow All

Select...

APPLICATION ACCESS CONTROL

Using the Application Access Control you can configure which licensed user/groups are able to access the AD Self-Service Suite applications.

Global Settings

The screenshot shows the 'Access Control Configuration' dialog box with the 'Administration Access Control' tab selected. It contains four sections, each with radio button options for 'Deny All', 'Allow All', and 'Select...':

- Able to use AD Info:** Deny All, Allow All, Select...
- Able to use AD Password:** Deny All, Allow All, Select...
- Able to use Help Desk Recovery:** Deny All, Allow All, Select...
- Able to use AD WhitePages:** Deny All, Allow All, Select...

DIRECTORY ATTRIBUTES

All of the applications in the AD Self-Service Suite function in some fashion by editing or managing directory objects and their attributes. From the Admin website, administrators can add their custom attributes to the AD Self-Service Suite and configure how they will be used and represented. For newly added or existing attributes, administrators may define the attribute name, friendly label, and available control used to represent this attribute to end users. To help with consistency, each attribute may be assigned with a selection of custom regular expression validators.

The screenshot shows the 'Directory Attributes - User' interface. On the left is a sidebar with navigation options: 'Getting Started', 'Global Settings', 'Directory Connections', 'Directory Attributes' (selected), 'AD WhitePages', 'AD Info', and 'AD Password'. The main area displays a table of attributes with columns for Name, Label, Category, Formatting, and AD Type. A search bar is located at the top right of the table area.

| Name | Label | Category | Formatting | AD Type |
|---|-----------------------|---------------------|-------------|-----------------|
| <input checked="" type="checkbox"/> accountExpires | Account Expires | Admin | time | GeneralizedTime |
| <input checked="" type="checkbox"/> AddressMap | Address Map | Visual Enhancements | addressIcon | none |
| <input checked="" type="checkbox"/> altRecipient | Forwarding Address | Exchange | DN | DN |
| <input checked="" type="checkbox"/> altRecipientBL | Forwarded from... | Exchange | MDN | DN |
| <input checked="" type="checkbox"/> altSecurityIdentities | altSecurityIdentities | Admin | Mstring | DirectoryString |
| <input checked="" type="checkbox"/> assistant | Assistant | Organization | DN | DN |
| <input checked="" type="checkbox"/> authOrig | Accept eMail From... | Exchange | MDN | DN |
| <input checked="" type="checkbox"/> authOrigBL | eMail accepted by... | Exchange | MDN | DN |

Page 1 of 22 (170 items)

The Directory Attributes screen as shown above displays a tab for each objectClass (user, group, etc...) supported by the AD Self-Service Suite. When a tab is clicked, the grid loads all of the currently defined attributes for this objectClass. The AD Self-Service Suite schema contains almost all of the configurable attributes for Windows Server 2003 R2 with the Live Communication Server and Exchange Server schema extensions. Any custom schema extension you may have already added to Active Directory or ADAM can also be added. The AD Self-Service attribute management tool allows AD Self-Service to use already existing attributes, but does not extend the schema or add new attributes.

GENERAL



The screenshot shows a configuration window titled "Office Location". It has a tabbed interface with tabs for "General", "Advanced", "Control Types", "List Items", and "Validators". The "General" tab is selected. The configuration options are:

- Active:
- Required Value:
- Attribute Label: Office Location
- Attribute Category: Address
- Browsing: Letters

Buttons for "Cancel" and "Save" are visible in the top right corner.

The General tab contains the following options:

- Active (true/false) – The Active value may be toggled between true or false to control whether this attribute will be available for use by the AD Self-Service Suite. Inactive attributes will not appear anywhere in the suite applications for viewing or editing
- Required Value (true/false) – The Required Value setting may be toggled to control whether the selected attribute must never be blank in an edit view for AD WhitePages or AD Info. If Required Value is selected, this attribute can never be blank if it is selected in one of these editable views
- Attribute Label – The Attribute Label allows a friendly label to be designated for an attribute. Unused attributes can be used for organizationally-specific purposes by relabeling them. The Exchange custom schema attributes are often used for this type of purpose
- Attribute Category – The Attribute Category is used to organize attributes into sub lists so that they may be more easily identified and selected when being added to an AD WhitePages or AD Info view.
- Browsing – The Browsing option controls whether an attribute should be available for Browse By in the AD WhitePages interface. AD WhitePages allows users to Browse By attributes like Last Name, Department, etc... Some attributes like distinguishedName are not browsable and should be marked as such. When adding custom attributes you should specify if an attribute is browsable and if so how
 - Attributes that will be integer values should be set as Numbers. If Numbers is selected, a 0-9 dropdown will show in the Browse By menu when this attribute is selected. Letters attributes will show an A-Z dropdown list to be used for browsing. Attributes having list items defined can opt to use the List Items Browsing option. This option displays the defined list item values in the Browse By menu when this attribute is selected

ADVANCED

The Advanced tab contains the settings for an attribute that should be modified with caution. The Advanced settings control the definition of the attribute as an Active Directory or LDAP data type. These values should match the values for this attribute in Active Directory or ADAM



Office Location

General | **Advanced** | Control Types | List Items | Validators

Attribute Name (case-sensitive): physicalDeliveryOfficeName

Max-Length: 128

Multi Value:

AD Type: Unicode String

Formatting: String

Cancel Save

The Advanced tab contains the following options:

- Attribute Name – The Attribute Name represents the name of the attribute as it was defined in Active Directory or ADAM. This value is case sensitive and should not be modified for existing attributes
- Max-Length – The Max Length denotes any max length that was defined for the object when it was created
- Multi Value – The Multi Value option specifies whether or not the attribute is a multi-valued attribute
- AD Type – The AD Type is the data type as it was defined upon creation. This value can easily be viewed using the Microsoft ADSI Edit tool
- Formatting – The Formatting value tells AD Self-Service how to format the data stored in this attribute when rendered in any of the AD Self-Service user interfaces. Attributes holding hyperlinks should be formatted as hyperlinks, email addresses as email, etc...

CONTROL TYPES

The Control Types tab contains the settings for defining the controls that may be selected when adding this attribute to an editable AD WhitePages or AD Info view.



Office Location

General | Advanced | **Control Types** | List Items | Validators

| Default | Name |
|--|-----------------|
| <input checked="" type="checkbox"/> <input type="radio"/> | Label |
| <input checked="" type="checkbox"/> <input checked="" type="radio"/> | TextBox |
| <input type="checkbox"/> <input type="radio"/> | TextArea |
| <input checked="" type="checkbox"/> <input type="radio"/> | ListBox |
| <input checked="" type="checkbox"/> <input type="radio"/> | DropDownList |
| <input type="checkbox"/> <input type="radio"/> | RadioButtonList |

Cancel Save

Control types can be marked as available by checking the checkbox. Unchecked control types will not be available as options when adding an attribute to an editable view. A default control type should be selected using the radio button. This will be the control type used if none is specifically selected when it is added to an editable view. Control types should be selected that are valid for the AD Type of the attribute. The AD lookup control should only be selected for distinguished name attributes and Boolean control or tri-state control should only be selected for Boolean data type attributes. The ListBox,

DropDownList, and RadioButtonList controls will display any list items configured for this attribute and require the user to select one of the defined values

LIST ITEMS

The List Items tab contains the settings for defining list items that may be selected when a user is editing this attribute in an editable AD WhitePages or AD Info view

TEXT TAB

Build your dropdown list on the Text Tab. The list order is bottom to top. A best practice would be to put PLEASE SELECT ONE at the bottom to make it the default



LIST TAB

The List tab has Label and Value columns. The Label is what is returned to the end user. The Value is what will be entered into Active Directory or ADAM. A best practice would be to set the PLEASE SELECT ONE as the label and set the Value to be blank



Note: If you add to this list later you will need to go back to the List tab to remove the Value from the PLEASE SELECT ONE again

VALIDATORS TAB

The Validators tab allows validators to be made available for use with an attribute. Multiple validators can be selected for use with an attribute and will appear as selectable options when an attribute is added to an editable view. Pre-defined validators appear in the dropdown list for selection. The validators are all standard regular expressions. The existing validators may be modified or any number of new validators may be added. The Message box allows customization for the error message presented to the end user upon validation failure

AD WHITEPAGES

AD WhitePages is a web-based directory application designed to make Active Directory an easy to use, up to date, and interactive source for employee information

DIRECTORY VIEWS

AD WhitePages Directory Views represent profiles made available to end-users using the multi-profile AD Self-Service Suite technology. A Directory View presents a logical business view of your directory or directories to end-users. A Directory View may be created to display a single department or division or even to show only the direct reports of the current user. Directory views offer both a read-only and “Editor” (read-write) view when an object is selected. The Editor view is only visible to select users of the specific Directory View

GENERAL

The General tab allows configuration of the Directory View Title as shown in the Admin website, the Tab Label as displayed to the end users, a description (for documentation only), and the cache settings for the Directory View. Caching may be enabled on a per Directory View basis and a cache refresh timeout set. Caching can dramatically improve performance in Directory Views containing data from a large number of different directories.

The screenshot displays the 'Entire Company' Directory View configuration page. At the top, there are navigation tabs: 'General', 'Access Control', 'Scope', 'Grid Fields', 'Detail Layout', and 'Edit Layout'. The 'General' tab is active. Below the tabs, there are two main sections: 'General Information' and 'Cache Settings'. The 'General Information' section contains three fields: 'Title' (Entire Company), 'Tab Label' (Entire Company), and 'Description' (Directory view that displays all users and contacts in the organization). The 'Cache Settings' section includes a note about caching, a checkbox for 'Use Cache' (which is unchecked), and a 'Cache Interval (minutes)' field set to 15.

ACCESS CONTROL

The Access Control tab is used for limiting user access to particular Directory Views as well as limiting their rights to features within a view. Access to a Directory View and to each feature can be granted or denied globally or on a per user/group basis

By default, all users have read-only access to each of the AD WhitePages Directory Views. In order to edit information within AD WhitePages, Allow All or specific user or groups must be selected in the Access Control tab under the “Who can edit object information” section

Entire Company

General Access Control Scope Grid Fields Detail Layout Edit Layout

Who can access this Directory View

Deny All
 Allow All
 Select...

Who can edit object information

Deny All
 Allow All
 Select...

Who can export data

Deny All
 Allow All
 Select...

SCOPE

The Scope tab in a Directory View controls which information will be visible and included in that view. Directories may be added for inclusion on a per objectClass basis. Some Directory Views may include users and contacts while other might only include printers, computers, and network shares.

Entire Company

General Access Control Scope Grid Fields Detail Layout Edit Layout

Scopes

Include Directory

Directories in use

| Domain | Object | LDAP Path | Access options |
|--------|--------|-----------|----------------|
| | | | |

Page 1 of 0 (0 items)

GENERAL

General Grid Path Grid Filter Selector Path Selector Filter

Cancel Accept

Directory: TDNFTEST

Object Type: User

List

List Selector

Allow Edit

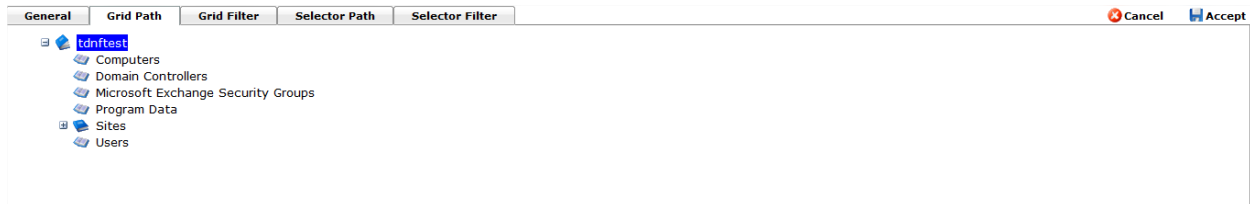
The options for the General tab are as follows:

- Directory – Allows you to select a specific Active Directory Domain or LDAP partition for inclusion
- Object Type – Select the objectClass you wish to include in this view from this domain or directory
- List (true/false) – This selection determines whether objects of this type will be displayed in the AD WhitePages grid as browsable objects
- List Selector (true/false) – This selection is used to allow object types that are not displayed in the grid of this Directory View to still be visible when viewing the details of a user or another object. Ex. A user may own groups and this would be displayed when viewing the details of a user. However, if Use in Grid is not selected for this object type, they will not be displayed in the grid results
- Edit (true/false) – This selection enables the editor access control to apply for this scope for the object type specified. In order to edit information in AD WhitePages, this option must be

enabled for the scope and a user or group has to be specified as an editor on the Access Control tab

GRID PATH

The Grid Path tab is used to limit grid results for a particular objectClass to only those of this type that exist below a specific Organizational Unit path in the Directory or domain added



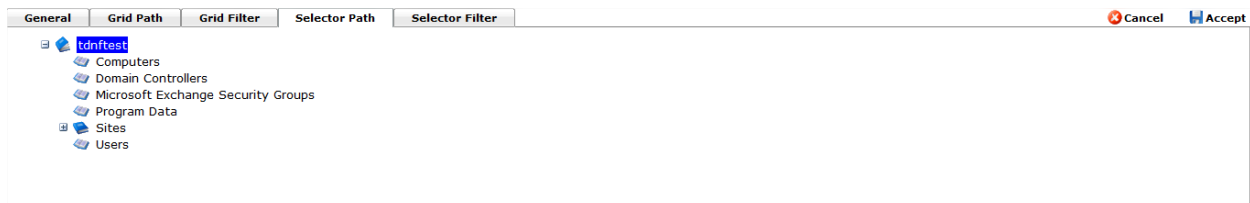
GRID FILTER

The Grid Filter tab further limits grid results to only those objects of the type selected, below the path selected, matching a specific search or filter criteria. Filters can be used to only show users in specific departments or that are members of particular groups, etc... Any of your directory attributes marked active may be used to filter which objects will be displayed in a particular Directory view. The Filter interface allows complex search criteria to be defined with operands



SELECTOR PATH

The Selector Path tab is used to limit which objects will be selectable in the Object Selector pop up. The Object Selector popup is used when editing distinguishedName attributes like manager and directReports. The selector path limits which objects of the type selected will be searchable and visible in this popup. Only those objects of this type that exist below the specified OU path in the Directory or Domain will be searchable



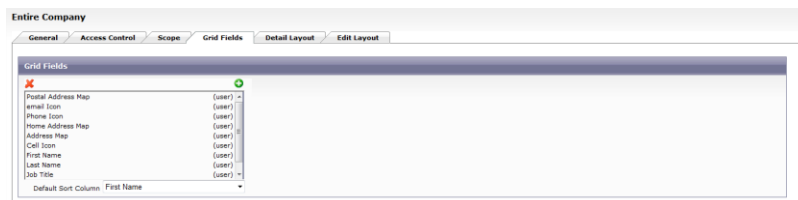
SELECTOR FILTER

The Selector Filter tab further limits selector results to only those objects of the type selected, below the path selected, or matching a specific search or filter criteria. Any of your directory attributes marked active may be used to filter which objects will be displayed in the Object Selector pop up



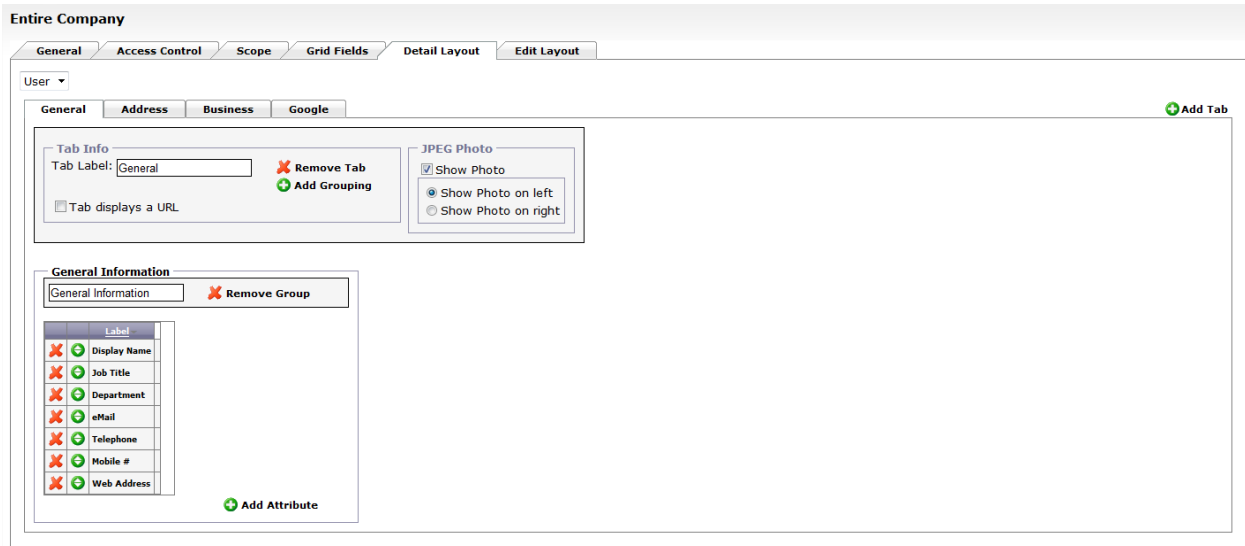
GRID FIELDS

The Grid Fields tab is the next required settings section to configure for a Directory View. The attributes added here are the attributes that will be displayed in the AD WhitePages grid. Any attribute for the object types added under the scope option are available to be added to the grid. Attributes may be added using the green + image and removed using the red X image. Attributes may be reordered from left to right on the grid by reordering them up and down in the list box displayed on the screen. An attribute may be selected as the Default Sort Column used when results are rendered in the AD WhitePages user interface

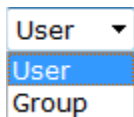


DETAIL LAYOUT

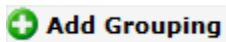
The Detail Layout tab is the next required settings section. On this tab you may use our 'What you see is what you get' (WYSIWYG) designer to layout the attributes into tabs and groupings that will be displayed when an object is selected in the AD WhitePages grid



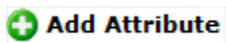
A dropdown list displays each of the objectClasses that have been added on the Scope tab for this Directory View. Each objectClass has its own unique details layout displaying different attributes and information when that object type is selected. For example, users can display user attributes and information whereas selecting a printer object will display printer-specific attributes in its own layout



- Creates a new tab that can be named and attributes can be added for display



- Creates groupings for the attributes



- Adds the attributes to the groupings

Note: Keep the number of attributes per grouping to 9 or less

Any of the red X icons on the screen can be used to remove attributes, groupings, or tabs



The green icon with the up and down arrows displayed beside each attribute can be grabbed and dragged with your mouse. This allows attributes to be reordered within a grouping



Other options available on the Tab Info section are to show the JPEG photo of a user on this tab or display a URL in this tab instead of displaying directory attributes

JPEG Photo

Show Photo

Show Photo on left

Show Photo on right

When adding a URL to be displayed in a tab, you may enter attribute names within {} braces and these will be resolved to the actual user or object values at run time

Web | **Address** | **Business**

Tab Info

Tab Label: ✖ Remove Tab

Tab displays a URL

URL:

➕ Append Attribute

- Address
- Admin
- Exchange
- General**
 - Description
 - Display Name**
 - eMail
 - Enrollment
 - First Name
 - Generational Suffix
 - Initials
 - Last Name
 - Middle Name
 - Name
 - Other Mailbox
 - User Account Control
- Group Access Request
- LCS
- Organization
- Other
- Personal
- Telephones
- Unix
- Visual Enhancements

EDIT LAYOUT

The Edit Layout tab is identical in function to the Detail Layout with the addition of a few more configuration options. The Edit Layout tab is used to design the view users assigned as Editors will see when editing the specific object type you are currently configuring the edit layout for. For example, Editors editing user objects may have a completely different layout than when they are editing groups

Entire Company

General Access Control Scope Grid Fields Detail Layout Edit Layout

User

General Address Business Telephones Add Tab

Tab Info
 Tab Label: Remove Tab Add Grouping
 Tab displays a URL

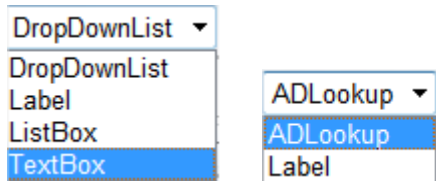
JPEG Photo
 Show Photo
 Edit Photo
 Show Photo on left
 Show Photo on right

Name
 Remove Group

| | Label | Type | |
|-------------------------------------|---------------------|--------------|--|
| <input checked="" type="checkbox"/> | Display Name | TextBox | |
| <input checked="" type="checkbox"/> | First Name | TextBox | |
| <input checked="" type="checkbox"/> | Middle Name | TextBox | |
| <input checked="" type="checkbox"/> | Last Name | TextBox | |
| <input checked="" type="checkbox"/> | Generational Suffix | DropDownList | |
| <input checked="" type="checkbox"/> | Initials | TextBox | |
| <input checked="" type="checkbox"/> | Web Address | TextBox | |

Add Attribute

The additional configuration options on this screen are used to control how the attributes selected for the edit view will be displayed and editable



As seen above, when an attribute is added you may select from any of the available Control Types defined for this attribute in the Directory Attributes section of the Admin website

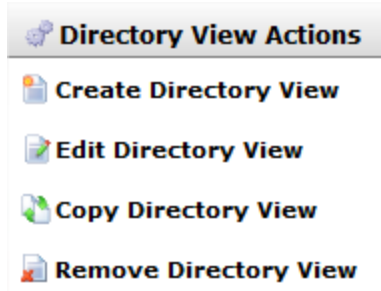
Note: Label will make the value read-only. TextBox will make the value free text etc...

For attributes where list items have been defined, you may select to include all list items to be displayed or only particular list items that are appropriate for the users or other objects being edited in this Directory View

Once you have configured a read-only and edit view for each objectClass used in this Directory View, click Save Directory View to commit the configuration to the server

OPTIONS FOR MANAGING EXISTING DIRECTORY VIEWS

The Directory View Actions area displays tasks that may be performed when managing Directory Views. These actions are visible in the top left of the screen when using the AD WhitePages section of the Admin website



Available actions for existing Directory Views include:

- Create Directory View – Creates a blank new view. In addition to configuring access control and scope options you will need to configure Detail and Edit Layouts as they will be blank
- Edit Directory View – To modify an existing view
- Copy Directory View – Creates a new view using an existing view as a template
- Remove Directory View – This will remove the view from AD WhitePages as well as from the Admin website

AD INFO

Empower your users with AD Info personal information self-service for Active Directory. AD Info is an easy to use, web-based self-service application that lets users update their own directory information with restrictions set by the administrator

AD INFO VIEWS

AD Info Views represent a self-service profile made available to end users. AD Info Views are much like the Editor mode of an AD WhitePages Directory View. The difference is that an AD Info View restricts the user to editing only their personal information. An AD Info View may be created to display any Active Directory attribute, organized by logical tabs

GENERAL

The General tab allows configuration of the AD Info View title as shown in the Admin website and a description (for documentation only) of the AD Info View

The Access radio button area is used for limiting user access to particular AD Info Views. Access to an AD Info View can be granted or denied globally or on a per user or group basis. By default, all users have read and write access to any Active Directory attribute included in the Edit Layout of the Default AD Info View

A screenshot of a web-based configuration interface for a "Default ADInfo View". The interface has three tabs: "General", "Edit Layout", and "Selector Scope", with "General" selected. Below the tabs is a "General Information" section with two input fields: "Title" (containing "Default ADInfo View") and "Description" (containing "Default ADInfo View"). Below this section is an "ACCESS" section with three radio buttons: "Deny All", "Allow All" (which is selected), and "Select...".

EDIT LAYOUT

The Edit Layout tab is the next required settings section. On this tab you may use our 'What you see is what you get' WYSIWYG designer to layout the attributes into tabs and groupings that will be displayed in the AD Info View. The configuration options on these screens are used to control how the attributes selected for the AD Info View will be displayed and editable

Default ADInfo View

General Edit Layout Selector Scope

General Address Business + Add Tab

Tab Info
Tab Label: General Remove Tab Add Grouping
 Tab displays a URL

JPEG Photo
 Show Photo
 Edit Photo
 Show Photo on left
 Show Photo on right

Name
Name Remove Group

| Label | Type |
|--|--------------|
| Remove Add First Name | Label |
| Remove Add Middle Name | Label |
| Remove Add Last Name | Label |
| Remove Add Generational Suffix | DropDownList |
| Remove Add Initials | Label |

Add Attribute

Contact Info
Contact Info Remove Group

| Label | Type |
|--|---------|
| Remove Add Telephone | TextBox |
| Remove Add Mobile # | TextBox |
| Remove Add Web Address | TextBox |

Add Attribute

Add Tab - Creates a new tab that can be named and attributes can be added for display

Clicking on the Add Grouping button will add a grouping of attributes that you may name. Clicking the Add Attribute button will allow specific attributes for this object type to be selected.

Add Grouping - Creates groupings for the attributes

Add Attribute - Adds the attributes to the groupings

Note: Keep the number of attributes per grouping to 9 or less

Any of the red X icons on the screen can be used to remove Attributes, Groupings, or Tabs



The green icon with the up and down arrows displayed beside each attribute can be grabbed and dragged with your mouse. This allows attributes to be reordered within a grouping



Other options available on the Tab Info section are to show the JPEG photo of a user on this tab or display a URL in this tab instead of displaying directory attributes.

JPEG Photo

Show Photo

Show Photo on left

Show Photo on right

When adding a URL to be displayed in a tab, you may enter attribute names within {} braces and these will be resolved to the actual user or objects values at run time

Web | **Address** | **Business**

Tab Info

Tab Label: **Remove Tab**

Tab displays a URL

URL:

Append Attribute

- Address
- Admin
- Exchange
- General**
 - Description
 - Display Name**
 - eMail
 - Enrollment
 - First Name
 - Generational Suffix
 - Initials
 - Last Name
 - Middle Name
 - Name
 - Other Mailbox
 - User Account Control
- Group Access Request
- LCS
- Organization
- Other
- Personal
- Telephones
- Unix
- Visual Enhancements

The additional configuration options on this screen are used to control how the attributes selected for the edit view will be displayed and editable

DropDownList ▾

DropDownList

Label

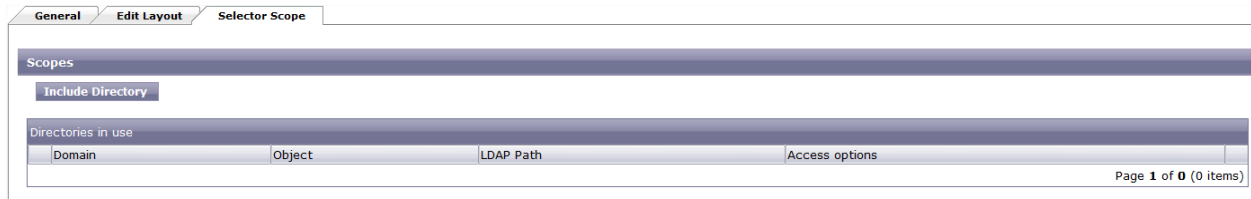
ListBox

TextBox

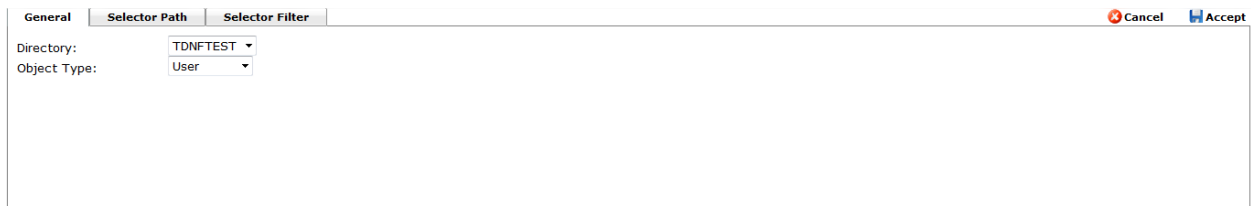
For attributes where list items have been defined, you may select to include all list items to be displayed or only particular list items that are appropriate for the users or other objects being edited in this AD Info View

SELECTOR SCOPE

The Selector Scope tab in the AD Info View is used to control which users will be visible and included. To add a specific Directory, click Include Directory and you will see the options presented below



GENERAL



The options on the General Tab are as follows:

- Directory – Allows you to select a specific Active Directory Domain or LDAP partition for inclusion
- Object Type – Select the objectClass you wish to include in this view from this domain or directory


SELECTOR PATH

The Selector Path tab is used to limit which objects will be selectable in the Object Selector pop up. The Objects Selector pop up is used when editing distinguishedName attributes like manager and directReports. The Selector Path limits which objects of the type selected will be searchable and visible in this pop up. Only those objects of this type that exist below the specified OU path in the Directory or Domain will be able to be used by AD Info



SELECTOR FILTER

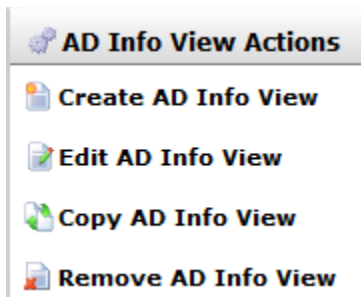
The Selector Filter tab further limits selector results to only those objects of the type selected, below the path selected, matching a specific search or filter criteria. Any of your directory attributes marked active may be used to filter which objects will be displayed in the Object Selector pop up

The image shows a software window with three tabs: "General", "Selector Path", and "Selector Filter". The "Selector Filter" tab is active. It contains a form with a dropdown menu labeled "[Select an attribute...]", a text input field, and a green plus icon. In the top right corner of the window, there are "Cancel" and "Accept" buttons.

Once you have configured all of the settings required for the AD Info View, click “Save AD Info Layout” to commit the configuration to the server

OPTIONS FOR MANAGING EXISTING AD INFO VIEWS

The AD Info View Actions area displays tasks that may be performed when managing AD Info Views



Available actions for existing AD Info Views include:

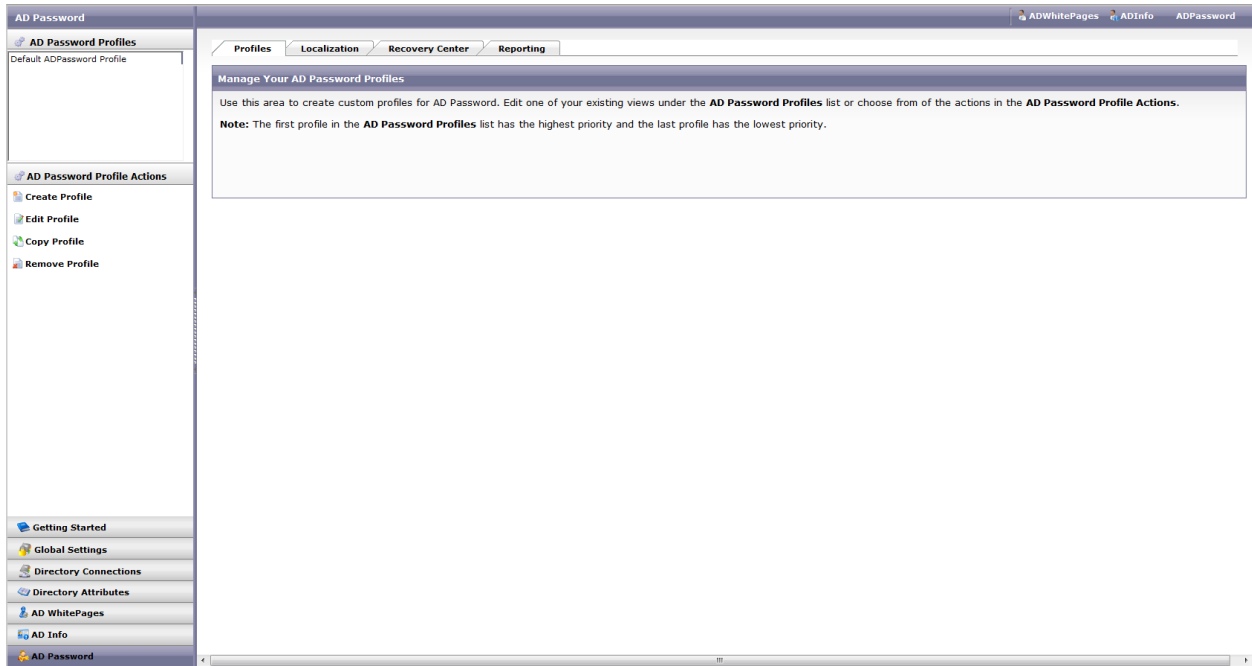
- Create AD Info View – Creates a blank new view. In addition to configuring access control and scope options you will need to configure Edit Layouts as they will be blank
- Edit AD Info View – To modify an existing view
- Copy AD Info View – Creates a new view using an existing view as a template
- Remove AD Info View – This will remove the view from the Admin website

AD PASSWORD

AD Password is a web-based self-service application that allows users to reset forgotten passwords and unlock their locked-out accounts. AD Password offers multiple interfaces allowing users to change their passwords or enroll in the AD Password Reset Service eliminating the source of the number one help desk call

PROFILES

The Profiles tab is for reference and needs no modification



LOCALIZATION

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

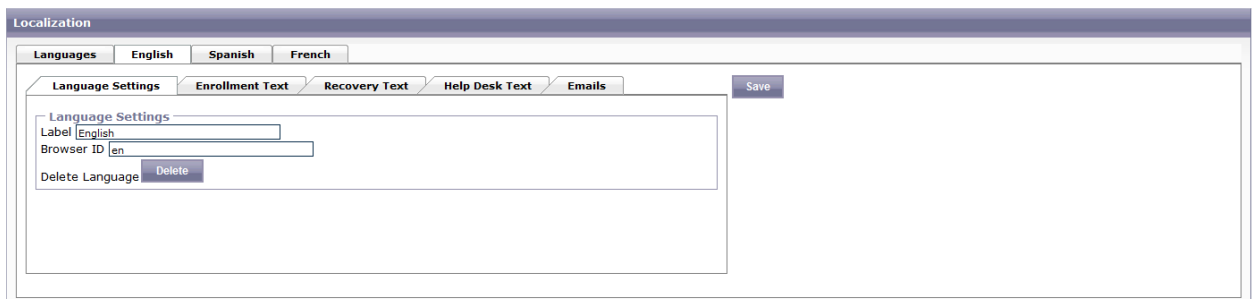
LANGUAGES

The Languages tab is used to add additional languages by clicking the “Add Language” button



LANGUAGE SETTINGS

The Language Settings tab allows configuration of the selected Language



- Label - The Label is what will be displayed in the Admin website
- Browser ID - The Browser ID is case sensitive and is used by the browser to determine which language should be used
- Delete Language – This button will remove the selected language

ENROLLMENT, RECOVERY, AND HELP DESK TEXT

These tabs allow for customization of the text used as labels, buttons, and 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

Note: Text in {} braces are queries to bring back dynamic data to the user interface and should not be modified

The screenshot shows the 'Localization' configuration page for the 'English' language. The 'General Messages' tab is active, displaying various message and button configurations. The fields are as follows:

- Greeting Message:** Hello {displayName}
- Enrollment Message:** You have not enrolled for the Password Reset Center
- Re-Enrollment Message:** Please update your security questions
- Password Last Set Message:** Your password was last set on {date}
- Password has Expired Message:** Your password has expired
- Non-Expiring Password Message:** Your password never expires
- Domain Password Policy Message:** Your domain does not have a password expiration policy
- Password Expiration Notification Message:** Your password will expire in {days} days
- Change Password Button:** Change Password
- Change Enrollment Button:** Enroll for Reset
- Enrollment Expiration Notification Message:** Your Security Questions will expire in {days} days.
- Enrollment Expiration Message:** (Empty field)
- Error Summary Header:** The following errors occurred

EMAILS

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)

Localization

Reset Password

Administrator Email Alert for this action

Email Subject:

Email Body:

| Arial | 6 pt |

B *I* U |

The following user {displayName} has successfully reset their password via the following website - {TDFNF_URL}

Thank you,

User Email Alert for this action

Email Subject:

Email Body:

| Arial | 6 pt |

B *I* U |

Hello {displayName},

Your password has been successfully recovered.

Thank you,

RECOVERY CENTER

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.

Note: It is recommended that you select one of these identification methods for your users to avoid confusion

Profiles Localization Recovery Center Reporting

Recovery Center

Recovery Center Identification Methods Save

Default Method: NT4 style with domain dropdown list ▼

Enable UPN logon

Enable NT4 Style (domain/user)

Enable NT4 style with domain dropdown list

Enable user property logon

User Property 1

Attribute name:

Attribute label:

User Property 2

Attribute name:

Attribute label:

- 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.

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

Profiles Localization Recovery Center Reporting

Reporting

Export user info to Excel

| Enrolled Users | Un-Enrolled Users |
|----------------|-------------------|
| tdnftest | tdnftest |

SMTP Configuration

SMTP Server:

Default Sender Email Address:

Save

Reset Password

Enable Administrator Email Alert for this action

Enable User Email Alert for this action

Change Password

Enable Administrator Email Alert for this action

Enable User Email Alert for this action

User Enrollment

Enable Administrator Email Alert for this action

Enable User Email Alert for this action

Unlock Account

Enable Administrator Email Alert for this action

Enable User Email Alert for this action

Failed Recovery

Enable Administrator Email Alert for this action

Enable User Email Alert for this action

Recovery Center Lockout

Enable Administrator Email Alert for this action

Enable User Email Alert for this action

Successful Recovery

Enable Administrator Email Alert for this action

Enable User Email Alert for this action

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

AD Password allows you to create multiple profiles to accommodate for the different security levels

GENERAL

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

| General | Access Control | Policies | Questions |
|----------------------------|-----------------------------|----------|-----------|
| General Information | | | |
| Title | Default ADPassword Profile | | |
| Tab Label | Default ADPassword Profile | | |
| Description | Default AD Password Profile | | |

ACCESS CONTROL

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)

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

POLICIES

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

General Access Control Policies Questions

Global Policies

Password notification

Notify user * days before password expires (0 = disable)

Notify user * days before enrollment expires (0 = disable)

Expire enrollment questions after * days (0 = never expire)

Lockout policy

Enable Recovery Center lockout policy

Allow * failed attempts within * minutes Re-allow password recovery after * minutes of lockout

Password Recovery Policy

Enforce Password History

Bypass Password Min Age policy

Password Policy Messages

Enable Password Complexity Message

Enable Password Length Message

Enable Password History Message

Enable Password Minimum Age Message

Enable Password Maximum Age Message

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.

QUESTIONS

The Questions tab allows complete management of your enrollment questions. Options such as how many selectable questions, how many “Write your own”, and where you will choose to Enforce different answers and/or Check answer for question words

Out of the box questions are provided but others may be added, modified, deleted and classified. Classifications include Required, Selectable or Write your own. 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.

The screenshot shows the 'Question Setup' configuration page. At the top, there are five tabs: 'Question Setup', 'Required Questions', 'Selectable Questions', 'Help Desk Questions', and 'Auto-Enrollment Questions'. The 'Question Setup' tab is active. Below the tabs, there are two main sections: 'Enrollment Questions' and 'Recovery Questions'. In the 'Enrollment Questions' section, there are two input fields: 'Number of selectable questions:' with a value of '1' and 'Number of 'Write your own' questions:' with a value of '1'. Below these are two checkboxes: 'Enforce different answers' (checked) and 'Check answer for question words' (checked). In the 'Recovery Questions' section, there are two input fields: 'Number of recovery questions:' with a value of '3' and 'Number of questions required for recovery:' with a value of '2'.

Required Questions will always appear for users to answer when enrolling in the Password Reset Service.

The screenshot shows the 'Required Questions' configuration page. At the top, there are five tabs: 'Question Setup', 'Required Questions', 'Selectable Questions', 'Help Desk Questions', and 'Auto-Enrollment Questions'. The 'Required Questions' tab is active. Below the tabs, there are three language selection buttons: 'English', 'Spanish', and 'French'. The 'English' button is selected. Below the language buttons, there is a list of questions. The first question is 'Your Mother's maiden name?'. To the left of the question is a red 'X' icon, and to the right is a green plus icon. The question text is inside a text input field.

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.

Question Setup Required Questions Selectable Questions Help Desk Questions Auto-Enrollment Questions

English Spanish French

✖ +

Your favorite pet's name?
 The color of your first car?
 The manufacturer of your first car?
 Who is your favorite actress?
 What is your nickname?
 The month of your mother's birthday?
 Your favorite vacation city?
 The city where you were born?
 Your favorite color?
 Your favorite sports team?

Help Desk Questions will give your help desk the ability to reverse a question/answer to give to a user that calls in to have their password reset.

Note: This question is not part of the Number of recovery questions for a user to reset their password on their own

Question Setup Required Questions Selectable Questions Help Desk Questions Auto-Enrollment Questions

English Spanish French

✖ +

What is your favorite movie

Auto-Enrollment Questions automatically enroll all your users in Active Directory based on the case sensitive AD Attribute specified here

Question Setup Required Questions Selectable Questions Help Desk Questions Auto-Enrollment Questions

English Spanish French

✖ +

New Question

Question: What is your employee id number

Answer Attribute: employeeID

Save

Questions may be edited by clicking on the pencil or deleted by clicking ✖ . Minimum answer lengths are specified for each question enforcing appropriate responses along with the option to allow failure.

+ ✖

Question: New Question

Minimum answer length: 1

Allow Failure:

Save

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

IMPORTANT URLS

- [http\(s\)://ServerName/AdSelfService/Admin](http(s)://ServerName/AdSelfService/Admin)
- [http\(s\)://ServerName/AdSelfService/ADWhitePages](http(s)://ServerName/AdSelfService/ADWhitePages)
- [http\(s\)://ServerName/AdSelfService/ADInfo](http(s)://ServerName/AdSelfService/ADInfo)
- [http\(s\)://ServerName/AdSelfService/ADPassword](http(s)://ServerName/AdSelfService/ADPassword)
- [http\(s\)://ServerName/AdSelfService/HelpDeskRecovery](http(s)://ServerName/AdSelfService/HelpDeskRecovery)
- [http\(s\)://ServerName/AdSelfService/RecoveryCenter](http(s)://ServerName/AdSelfService/RecoveryCenter)
- [http\(s\)://ServerName/AdSelfService/Gina](http(s)://ServerName/AdSelfService/Gina)

Note: You can now go into IIS to set the Application Pool Identity. Please make this change before attempting to log in to the Admin website