The Dot Net Factory

AD Self-Service Suite for Active Directory

Getting Started Installation Guide

Version 3.6

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® AD Self-Service is a trademark 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

www.ADSelfServiceSuite.com

e-mail: info@TheDotNetFactory.com

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

The Dot Net Factory AD Self-Service Suite Quick Start Guide

Updated – April 28, 2008

Software version – 3.6
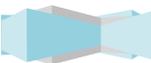
AD Self-Service Suite for Active Directory

Getting Started Installation Guide

Table of Contents

4

AD Self-Service Suite for Active Directory

Getting Started Installation Guide

ABOUT THIS GUIDE

This document has been prepared to assist you in becoming familiar with The Dot Net Factory AD Self-Service Suite for Active Directory. This guide will walk you through the steps involved in installing the AD Self-Service Suite on your system and configuring server settings using the AD Self-Service Configurator tool and the AD Self-Service Admin page. Each application in the AD Self-Service Suite has a separate Getting Started Guide that details the configuration of its specific settings. For a shorter version of this guide, please see our AD Self-Service QuickStart Guide. The QuickStart Guide covers the minimal settings needed to configure a trial version of the AD Self-Service Suite.

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

Support Link
www.ADSelfServiceSuite.com/support

Email: support@thedotnetfactory.com

5
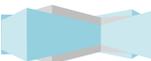
Before installing The Dot Net Factory AD Self-Service Suite, ensure your system meets the following minimum hardware requirements:

- Pentium 4 or greater processor

- At least 1 Gb RAM

- 100 MB hard disk space

Ensure your system meets the following minimum software requirements:

- Microsoft ® Windows Server™ 2003 SP1 or R2

- Microsoft® Internet Information Server 6.0 or later

- Microsoft **.NET Framework 2.0** with ASP.NET

Enabling HTTPS

It is recommended that you use HTTPS with AD Self-Service AD Password. HTTPS is a communications protocol designed to transfer encrypted information between computers over the 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 SharePoint 2003 or later

Ensure your client systems meet the following requirements:

- Microsoft Internet Explorer 6.0 or later – or Firefox 1.5 or later

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

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

- Microsoft Windows 2000 Server Service Pack 3, or Microsoft Windows Server 2003, or Microsoft Windows XP Professional Service Pack 1 or later

- Microsoft Internet Explorer version 6.0 or later

AD SELF-SERVICE SUITE USER INTERFACE OPTIONS

The AD Self-Service Suite is unique in offering multiple access point 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 or 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 Parts—all AD Self-Service Suite applications are deployable as SharePoint web parts. The web parts offer identical functionality with the added capability of being deployed many times across your various SharePoint sites.

Other AD Self-Service installable components:

- 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, web parts, toolbars, and Password Reset Center on a Windows 2003 web server. The Configurator is also used to configure the Local Administration account used for event logging.

- Application Pool—This account must be a member of the IIS_WPG local group on the AD Self-Service Server.

- AD Self-Service Event Log—the AD Self-Service Suite creates a custom event log named "AD Self-Service" upon installation. All errors and messages are written to this log.

- AD Password Windows Client (GINA Extension) —The Windows client is a separate application that may be deployed silently to your desktop PCs. The settings are managed centrally using custom Group Policy

templates. The Windows Client utilizes the Password Reset Center web site allowing locked-out users to reset their password or unlock their account from the windows logon screen.

GETTING STARTED WITH THE AD SELF-SERVICE SUITE INSTALLATION

The Dot Net Factory AD Self-Service Suite consists of the following applications:

- AD WhitePages – AD Self-Service AD WhitePages is a completely web-based directory application designed to enable Active Directory as your most easy to use, up to date and interactive source for employee collaboration.

- 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 Password – AD Self-Service AD Password is the only solution allowing end-users to reset forgotten passwords and unlock their locked-out accounts while seamlessly integrating into your existing environment. AD Password offers multiple interfaces allowing users to change their passwords or enroll in the Password Reset Service from Microsoft SharePoint, a standard web interface, and the Windows logon dialog.

### REQUIRED USER ACCOUNTS FOR THE AD SELF-SERVICE SUITE CONFIGURATOR

Installation User:

The user logged on to the AD Self-Service 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 (e.g. administrator).

Directory Connection (Proxy) Users:

The proxy user 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 Domain Administrator privileges to perform the actions used by the AD Self-Service applications.

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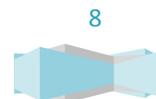
The Local Account is used to write to the event log and perform other local operations. This account must be specified on each server running the AD Self-Service Suite. This user account must be a member of the local administrators group. The local administration user may be either a local or domain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

License Connection User:

The license connection user is used by the AD Self-Service Suite to retrieve your organization's license information from the domain in which it is stored. The AD Self-Service Suite license is stored as an object in an Active Directory domain under the Program Data partition. The license connection account will need recursive read/write access to the domain Program Data container and all child objects in order to function properly.

Application Pool Identity:

This account must be a member of the IIS_WPG local group. If the identity for the application pool is not in this local group, you will receive a "Service unavailable" error message.

REQUIRED USER ACCOUNTS FOR THE AD SELF-SERVICE SUITE ADMIN WEB SITE

**Domain Connection Proxy Users:**

When enabling any of the AD Self-Service applications for a domain or LDAP directory, specific user accounts must be entered and saved in the Admin web site. One proxy user must be specified for each domain that will be used by any of the suite applications. This user account must have the necessary privileges to perform the actions required by the applications to be used. Rights will vary depending upon which combination of applications are implemented. A domain admin user may be selected for simplicity. The user name and password for this account will be stored as encrypted information and is not retrievable by users or administrators of the AD Self-Service Suite.

INSTALLING THE AD SELF-SERVICE SUITE

The account under which you run the installation must have, at a minimum, the privileges of a local administrator.

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

1. Please ensure that your AD Self-Service Suite server meets all installation requirements.

2. Locate your AD Self-Service Suite installation file.

3. Double click to run the setup program.

4. Select "Next" on all setup screens and click "Finish".
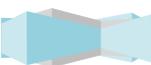
AD Self-Service Suite for Active Directory

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 in order to complete the configuration of your server.

Note: If you need to extract the contents of the installer in order to replace a corrupted file or perform troubleshooting, run the AD Self-Service Setup program with the /a parameter to unzip to a specified directory.

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, web parts, and toolbars on a Windows 2003 web server. The Configurator also allows for configuration of the AD Self-Service Suite license and license Administration account and the Local Administration account used for event logging.

Note: When using the AD Self-Service Configurator, clicking onto a different tab when you have unsaved changes will cause the screen will turn opaque and you will be prompted with a warning dialog. If you wish to save your changes, click "Save changes" and click the Apply button. If you wish to lose the changes you have made and continue on, click "Discard changes".
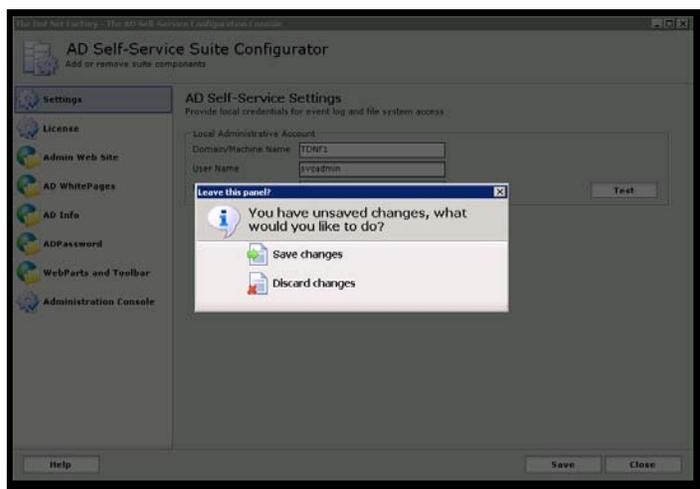
SETTINGS TAB – CONFIGURING SETTINGS MODE AND LOCAL PROXY ACCOUNTS

The settings tab is used to set up the Local Account and to configure the Settings Storage Mode. The Local Account is used by AD Self-Service for any local system access including writing to the event log. The Local Account may also be referred to as the Local Proxy Account.
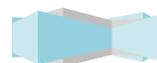
10

AD Self-Service Suite for Active Directory

LOCAL ACCOUNT CONFIGURATION

The local proxy account that you enter below must be a member of the local Administrators group on the AD Self-Service server. The account you configure here can be a domain account, as long as it is a member of a group granting it local administrative rights.

Please type the machine name or NetBIOS Domain name into the first box, then the username and password into the boxes below it.
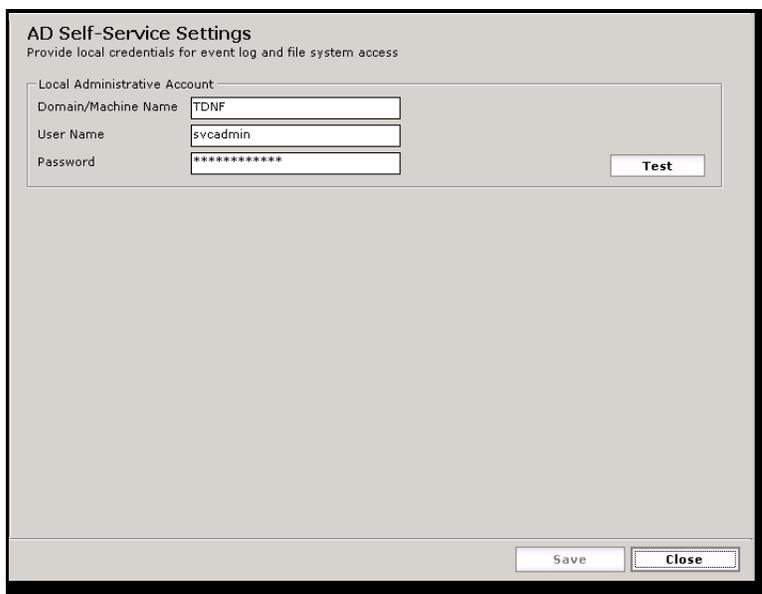

The "Test" button can be clicked to verify that the specified account has the required privileges. If the test is successful, you will see an informational dialog like the one below.

AD Self-Service Suite for Active Directory

Getting Started Installation Guide

If the account you provide does not have enough privileges you will see an error message like the one below.
Please check the account name and password for accuracy or try a different, higher privileged 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. This AD Self-Service Suite server is now set up in a Local Settings Mode. Settings configured on this server will not be shared by other AD Self-Service servers.

LICENSE TAB – LICENSING USERS AND DOMAINS

The License tab of the Configurator is used to configure license notification emails. License files will be sent to you by The Dot Net Factory support team when you request a trial or purchase an application in the AD Self-Service Suite.

To configure the license file notifications, place the email address in the Recipients box. If there is more than one entry, separate with a semicolon. Then below, enter the SMTP Server name. Use the "Test" button to send a test email to the specified email address.

All applications in the AD Self-Service Suite share the same the domain license object, so you will only have to copy one license file to register all of the AD Self-Service Suite applications. Please contact Sales at sales@thedotnetfactory.com for additional license purchasing needs.

The basic process for licensing your AD Self-Service Suite is to copy the 'license.xml' that is sent to you by The Dot Net Factory to the directory of <Server AD Self-Service Suite is installed on>C:\Program Files\The Dot Net Factory\AD SelfService Suite\Settings. Once the License file is copied to this directory, the Suite will pickup the new License criteria.
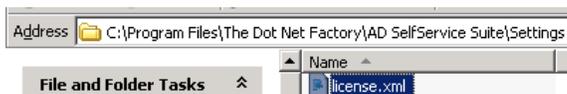
# AD Self-Service Suite for Active Directory

APPLYING A NEW LICENSE FILE

The License file for your AD Self-Service Suite will be sent to you from The Dot Net Factory Support in the form of a attached file, via email, entitled 'license.xml'. To apply this License File you will need to detach it from the email and paste it into the Directory of: <Server where AD Self-Service Suite is installed> C:\Program Files\The Dot Net Factory\AD SelfService Suite\Settings. You will replace it over the old License File.
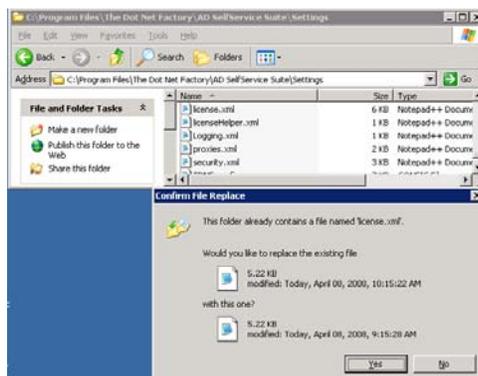
The next step is to configure the licensing notification email feature. This will keep your administrators informed of licensing issues and warn of before you exceed or reach your license limit. Enter the email addresses of the IT personnel you wish to receive this information (separated by semicolons) and a valid SMTP server. The SMTP server entered must allow the AD Self-Service server to use it as a mail relay. Click the Test button to send a sample email to the addresses listed and check the corresponding mailboxes to verify receipt.
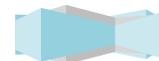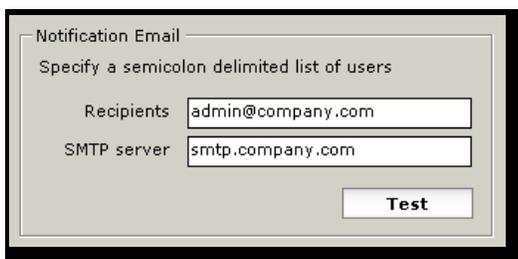
AD Self-Service Suite for Active Directory

UPDATING A LICENSE FILE

When additional user licenses or applications of the AD Self-Service Suite are purchased, the license file must be updated from the licensed domain. To update a License File, take the new 'license.xml' sent to you by The Dot Net Factory and paste it over the one located at <Server where AD Self-Service Suite is installed> C:\Program Files\The Dot Net Factory\AD Selfservice Suite\Settings. You will need to save it over the old License.xml.
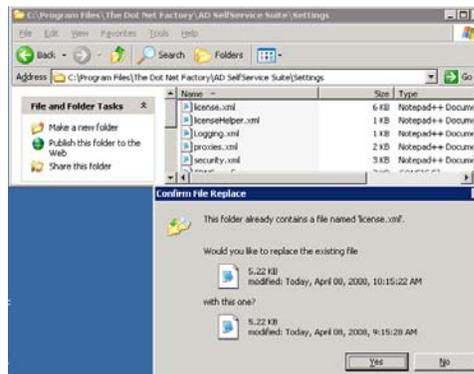
To purchase additional licenses, please contact your sales representative, or email sales@thedotnetfactory.com.

After replacing current license file, it may be necessary to go into the AD Self-Service Admin web site and ensure your domain connectivity is still present. If it is not, you will need to re-add the connection.
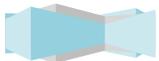
AD Self-Service Suite for Active Directory

The AD Self-Service Admin web site is used to manage all of the settings for each application in the AD Self-Service Suite. In local settings mode, an instance of the Admin web site is required on each server in order to modify the settings. In domain settings mode, only one installation of the Admin web site is required to manage the shared settings for multiple AD Self-Service servers.

Click the Web check box for each IIS web site you wish to install the Admin Web Site on and click the Apply button as shown below. The Admin web site will be deployed onto each of the IIS web sites selected and will be available for immediate use.
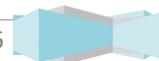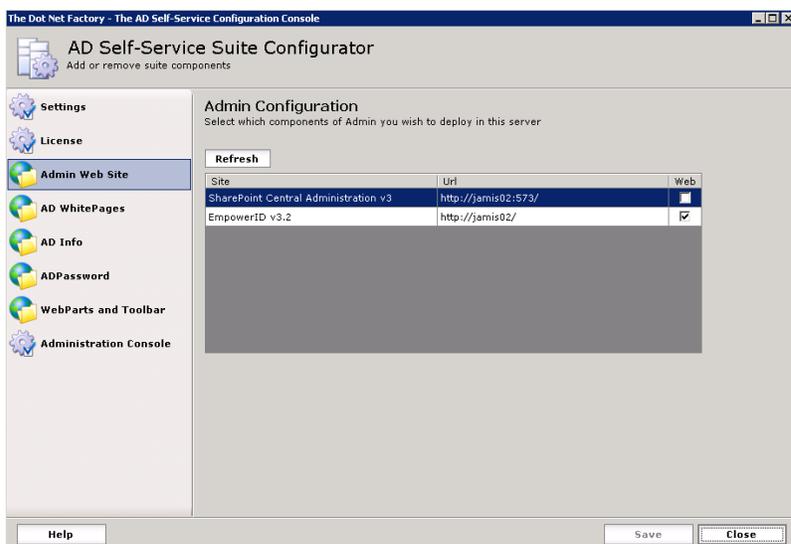
AD Self-Service Suite for Active Directory

(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)
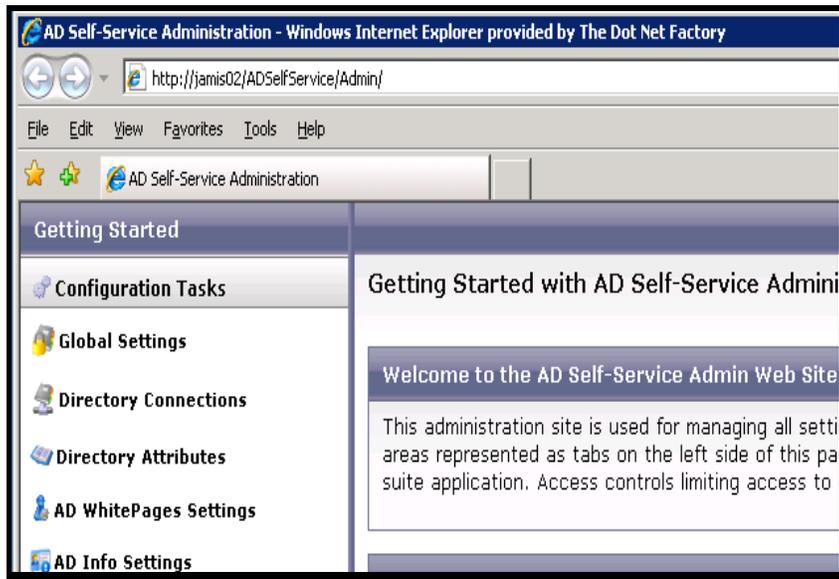
(Note: The remaining AD Self-Service applications are installable as individual modules and are not dependent upon each other. If you wish to trial any of the AD Self-Service Suite applications, please contact Sales at sales@thedotnetfactory.com)

ANYWHERE EVERYWHERE DEPLOYMENT – ACTIVATING USER INTERFACES

The AD Self-Service Suite is unique by offering many user interface options. The goal is to provide users with the same services in a consistent interface from wherever they may be interacting with your network. The AD Self-Service Suite licenses by user so any of the web user interfaces may be used at no additional charge.

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 Parts—all AD Self-Service Suite applications are deployable as SharePoint web parts. The web parts offer identical functionality with the added capability of being deployed many times across your various SharePoint sites.

16

AD Self-Service Suite for Active Directory

The Configurator provides a Web Parts and Toolbar tab to activate the additional web interfaces you wish to use in your environment. The SharePoint and user interface may only be activated on servers hosting this application. AD Password includes an additional web site called the Password Reset Center. This is the anonymous site users are redirected to in the event of a logon failure.

The method for activating the user interfaces for any of the AD Self-Service Suite applications is the same. When you select the tab for the application, the Configurator will load a grid displaying all of the IIS web sites on the server. Each Web application you wish to use may be clicked for activation under the Web grid for the respective IIS web site. SharePoint webparts are activated separately under the WebParts tab. After you make all of your desired selections, click the "Save" button at the bottom of the screen to commit the changes and deploy the virtual directories to your IIS Site(s).
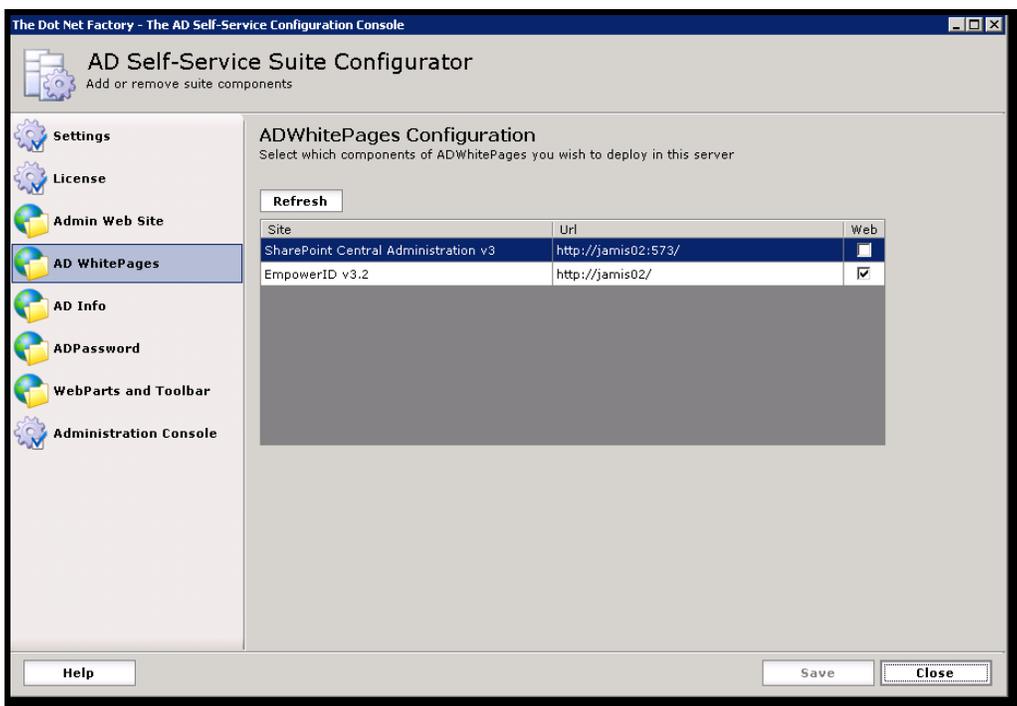
Note: The URLs for the web applications are:

- http(s)://servername/ADSelfService/Admin

- http(s)://servername/ADSelfService/ADWhitePages

- http(s)://servername/ADSelfService/ADInfo

17

- http(s)://servername/ADSelfService/ADPassword

- http(s)://servername/ADSelfService/RecoveryCenter

WEBPARTS TAB – SHAREPOINT

The WebParts tab is used to deploy SharePoint web parts to SharePoint. Check the interface options desired for your Windows SharePoint services, SharePoint Server Sites and click Save to commit the changes to the server.

(Note: The global toolbar and web part toolbar cannot be displayed together on the same SharePoint page. Please keep this point in mind when implementing your web part layout.)
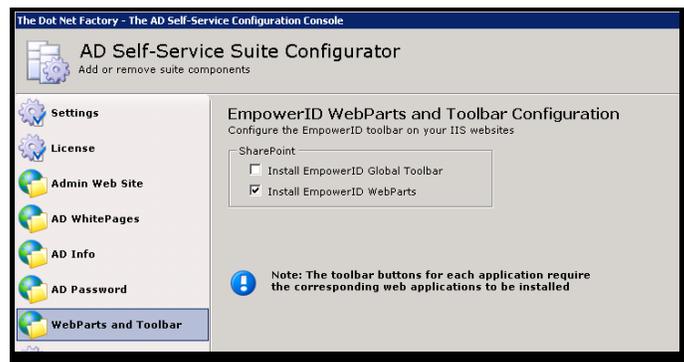
Once all administration settings have been configured and all of the applications have been licensed, the global toolbar will appear on your Windows SharePoint services or SharePoint Portal Server sites.

If you do not wish to have the toolbar appear globally on all SharePoint sites, the AD Self-Service Toolbar web part may be installed and dragged onto individual SharePoint pages.

From the SharePoint page on which you wish to deploy the web part, click on Modify Shared Page, then Add Web Parts, then Browse.
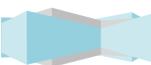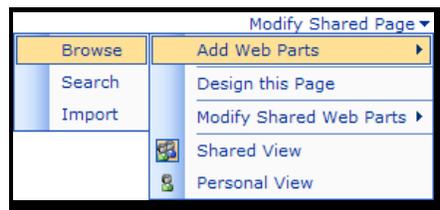
18

AD Self-Service Suite for Active Directory

Click on Server Gallery and then drag and drop the AD Self-Service Toolbar web part under the Web Part List onto the SharePoint page. The web part will automatically inherit the theme of the SharePoint site.
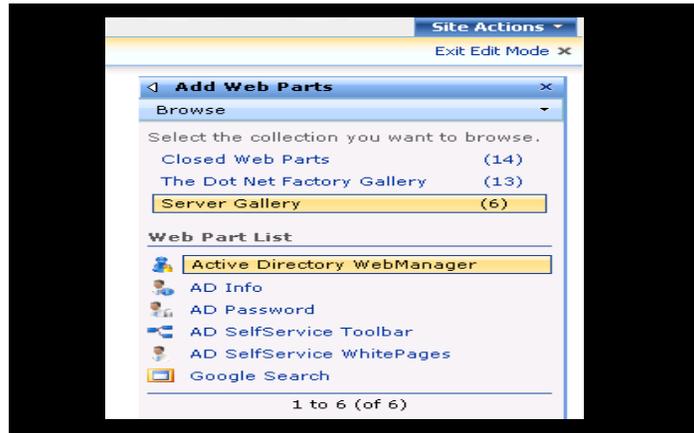
Once you are finished dragging the web part onto the SharePoint page, click the **X** on the Add Web Parts dialog.

To leave Design Mode and return to your SharePoint site, click Modify Shared Page, then Design this Page.
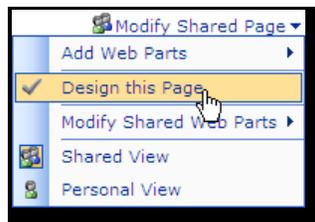
Upon leaving design mode, the Toolbar web part you have deployed will appear on the SharePoint page.

19

ADMINISTRATION CONSOLE TAB – CONVENIENT ACCESS LINKS

Click on the Administration Console tab to gain access to the AD Self-Service Admin Web Site, a URL that has been customized for your environment during installation. Click this link to proceed to AD Self-Service Administration.

Be aware that if you changed your page to SSL (https://) the link will no longer function. To get to the admin webpage please go directly to the url (https://servername/ADSelfService/Admin).
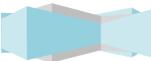
Admin Links

http://jamis02/ADSelfService/Admin

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/activated on any Windows Server 2003 IIS Server meeting the installation requirements listed previously. In local settings mode an instance of the Admin web site is required on each server in order to modify the settings. In domain settings mode, only one installation of the Admin web site is required to centrally manage the shared settings for multiple AD Self-Service servers.

Navigate to the Admin web site *http(s)://servername/ADSelfService/Admin* to complete the configuration. If you receive an error message when navigating to the Admin web site, please refer to the Troubleshooting section in the Appendix.

NAVIGATING THE ADMIN PAGE

Once you successfully authenticate, you will see the AD Self-Service Suite Admin web site as shown below.
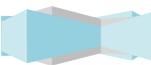
AD Self-Service Suite for Active Directory
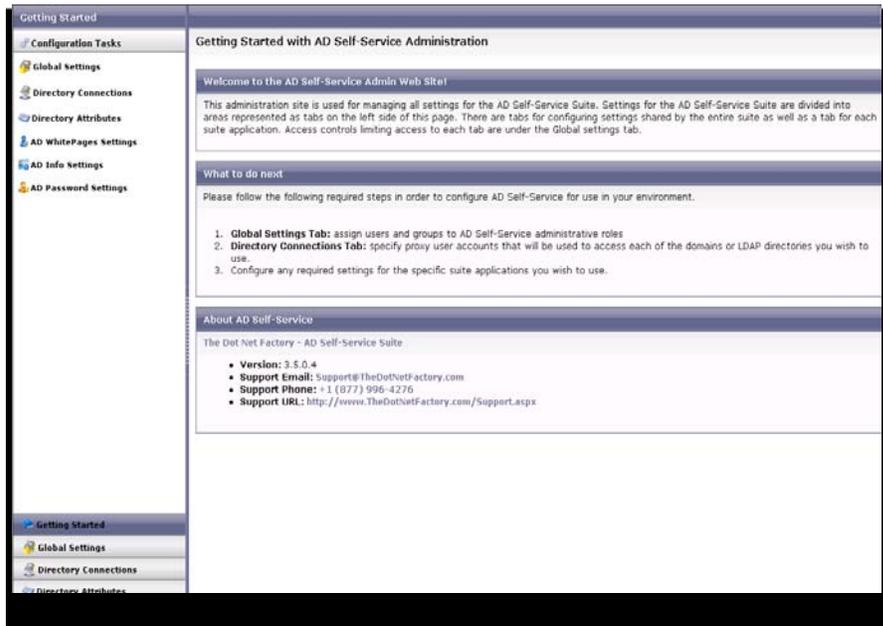
The Admin web site is divided into navigational sections on the left side of the screen. These sections are used to navigate between the various application settings. The Global Settings, Directory Connections, and Directory Attributes tabs manage settings shared by the entire suite. The remaining tabs manage the application-specific settings.

ACTIVATING AND MANAGING AD SELF-SERVICE SUITE LICENSES

Once the encrypted license has been copied to the C: Directory, the AD Self-Service Suite Admin page is used to activate each product license for the domains purchased or being trialed. Each application must be activated for the specific domains desired to be used with the product . To activate and manage AD Self-Service Suite licenses, click the Global Settings entry in the Configuration Tasks pane.

Click on the License Configuration tab to navigate to the License Configuration page.

Click the tab of the AD Self-Service Suite application to activate any trial or purchased licenses. *(Each application of the AD Self-Service Suite must be activated separately.)* Click the Add Domain button.

AD Self-Service Suite for Active Directory

Getting Started Installation Guide
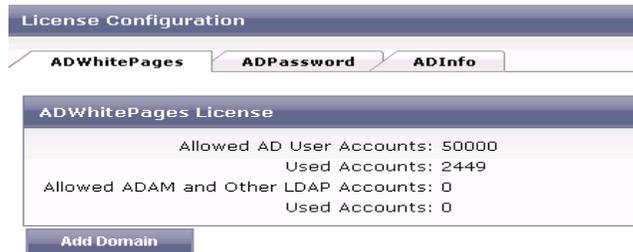
Click the Licensed Domain drop down and select a domain NetBIOS name to license *every* active user account in the domain. This will include all service accounts. Click Save to commit the configuration to the server.
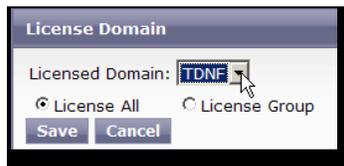
To license a specific primary group membership instead of the entire domain, click the License Group radio button and click the blue pawn icon to search the selected domain.
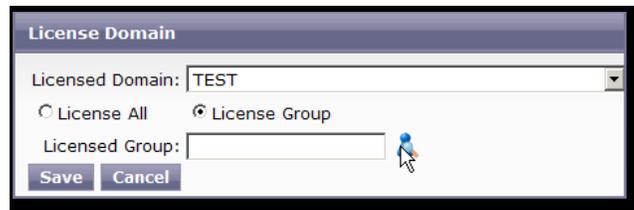
The Search for users and groups dialog will appear in a bubble window. This window will allow you to search for the group you wish to license on the selected domain.

Type in a search query and click the Search button. Find the group you wish to activate licenses for in the search results below. Once the group is listed in the Selected users and groups dialog box, click Save my selected items to return to the Application Access Control page. Click the Save button to commit the configuration to the server and activate the user accounts within the group specified.
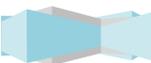

(Note: Domain group licensing will only check the direct membership of the group specified here. To best license your AD Self-Service Suite applications, create a new group within your Active Directory and add any and all users you wish to be managed or use the AD Self-Service Suite to this group, then license that group using this License Configuration process.)

Click the Validate button below the Allowed Accounts text to check the current amount of active users in the group or domain specified against the number of licenses you have acquired. If the amount of available licenses is sufficient for the domain selected, you will see an informational dialog like the one below.

If the amount of active user accounts in the domain or group specified is more than the valid amount of purchased or trial licenses, you will see the error dialog as shown below. Please contact Sales at sales@thedotnetfactory.com for additional license purchasing needs.
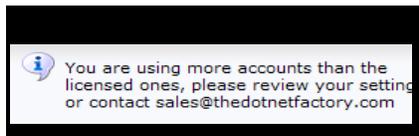
INCLUDING AND EXCLUDING SPECIFIC USERS FOR THE AD SELF-SERVICE APPLICATIONS

By default, any user in a domain configured with a proxy connection in the AD Self-Service Suite Admin page can access any licensed application in the suite. To grant or deny specific users or groups access to any of the AD Self-Service applications, click on the Access Control tab to navigate to the Access Control Configuration.

Click on the Application Access Control tab to continue.
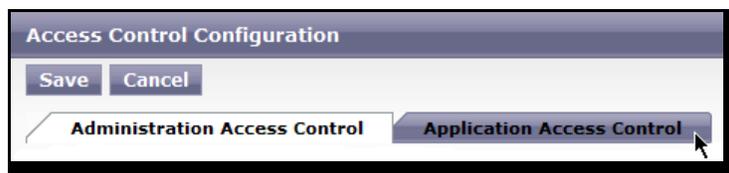
Click Deny All to deny access to all users and groups for that particular application, or click Allow All to allow access to all users and groups for that particular application. For more in-depth access control, you can click on the
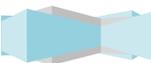
24

AD Self-Service Suite for Active Directory

Select… radio button for each individual application and choose a specific set of groups or users by clicking on the blue pawn icon.

The Search for users and groups dialog will appear in a bubble. This window will allow you to search your domain(s) for users and groups you wish to have access to this application.

Once all of the desired users and groups are listed in the Selected users and groups dialog box, click Save my selected items to return to the Application Access Control page.

Click Save again to commit the configuration to the server.
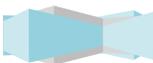
AD Self-Service Suite for Active Directory

Getting Started Installation Guide
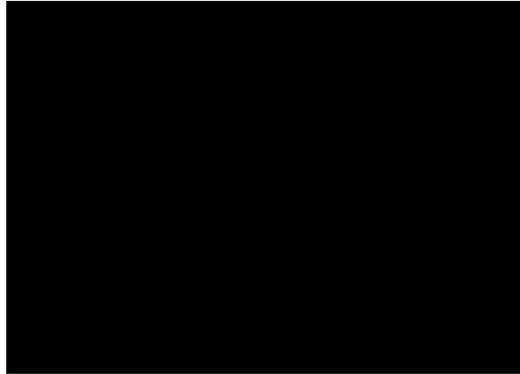
CONFIGURING DOMAINS FOR USE IN AD SELF-SERVICE

In order for the AD Self-Service Suite to provide service to your environment, you must add your domain(s) and proxy account(s) for it to connect to in the Directory Connections entry in the Configuration Tasks pane.

Click on the Directory Connections entry in the Configuration Tasks pane.

Click the Active Directory Connections tab to add a trusted or un-trusted Active Directory domain.

ACTIVE DIRECTORY CONNECTIONS

On the Active Directory Connections tab, click on the Add New Connection button.
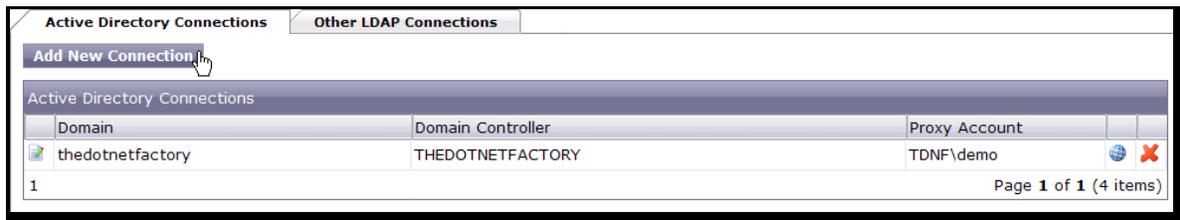
ADDING A TRUSTED DOMAIN

To set up a trusted domain, click the Forest radio button. 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 first from the Domain Controller drop down dialog. To set up the proxy account for this domain, click on the blue pawn icon.
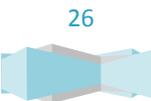
AD Self-Service Suite for Active Directory
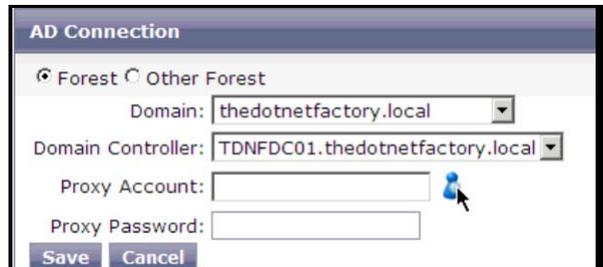
The Search for users and groups dialog will appear in a bubble. This window will allow you to search your domain(s) for a proxy account.

(Note: The proxy user accounts are used by the applications in the AD Self-Service Suite to retrieve information from your Active Directory domains and perform all account management and modification actions. A member of the Domain Administrators group may be used for simplicity.)

Search for and single click on the user you wish to use for the proxy account and the name will appear in the Selected users and groups box below. Click Save my selected items to confirm the proxy account selection and return to the Active Directory Connections page.

Type in the Proxy Account password and click Save to commit the configuration to the server.
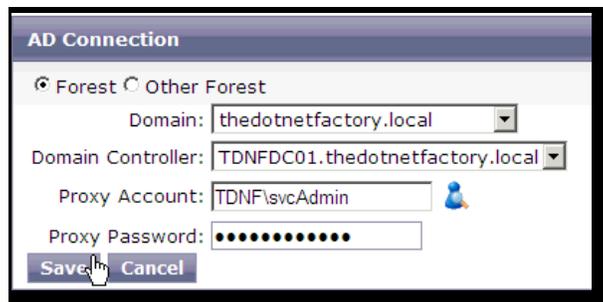
ADDING A DOMAIN IN AN UNTRUSTED FOREST

The AD Self-Service Suite now supports adding an un-trusted domain to the directory connections used by all applications. To set up an un-trusted domain, click the Other Forest radio button. Type the fully qualified name of both the domain and the domain controller you wish to connect to, then type the proxy account (in NT4 format) into the Proxy Account Name textbox. Type the proxy account password and click Save to commit the configuration to the server.

# AD Self-Service Suite for Active Directory

ADDING AN AD/AM LDAP CONNECTION

The AD Self-Service Suite now supports Active Directory Application Mode (AD/AM or ADAM) as a data source for AD WhitePages.

(Note: Support for other LDAP compliant directories are currently in development and will be included in a future version of the AD Self-Service Suite.)
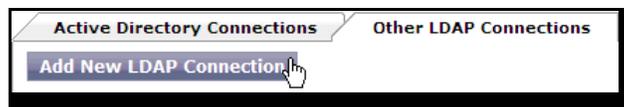
To set up an AD/AM LDAP connection, click the AD/AM radio button. Type the fully qualified server name you wish to connect to and the port number of the server that AD/AM is listening on, then type the proxy account (in NT4 format) into the Proxy Account textbox. For simplicity, the proxy account entered here should have administrative privileges on the AD/AM directory. Type the proxy account password and click Check to test the account.
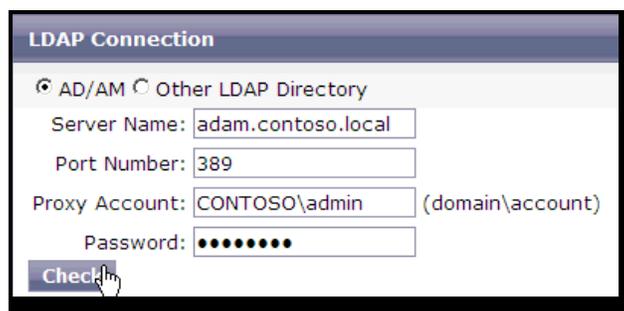
If the test connection to the AD/AM server fails, a bubble message will appear with troubleshooting information. Please check the account name and password for accuracy, try a different, higher privileged account, and ensure the AD/AM server name and port number are accurate and correctly configured.
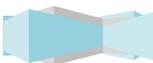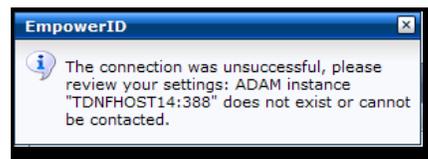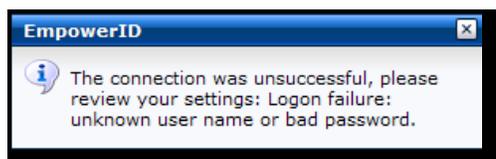
28

If the connection is successful, a drop down menu of partitions on the AD/AM server will appear.
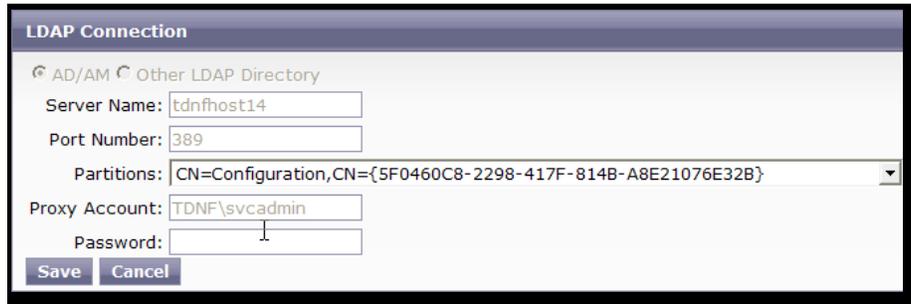
Select the AD/AM partition to bind to, re-enter the proxy account password and click Save to commit the configuration to the server.
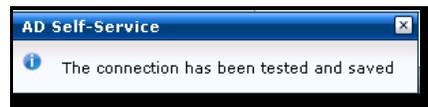
CONFIGURING THE AD SELF-SERVICE DIRECTORY ATTRIBUTES SETTINGS

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 web site, 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.

To configure your directory attribute settings, click on the Directory Attributes section of the Admin web site Configuration Tasks pane.

AD Self-Service Suite for Active Directory

The Directory Attributes screen as shown above displays a tab for each objectClass (user, group, etc…) supported by the AD Self-Service Suite. Additional objectClasses can be added with the assistance of our support department. When a tab is clicked, the grid loads all of the currently defined attributes for this objectClass. The AD Self-Service 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 be also added to AD Self-Service. 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.

After clicking on an existing attribute you will see the details section shown below.


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 to for use. 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 a 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.

  o Attributes can 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 items values in the Browse By menu when this attribute is selected.
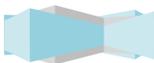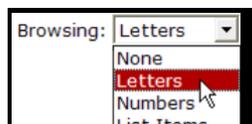
The **Advanced** tab contains the settings for an attribute that should be modified with caution. The Advanced settings control the definition of the attribute as an Active Directory or LDAP data type. These values should match the values for this attribute in Active Directory or ADAM in order for AD WhitePages to be able to read and write this attribute.
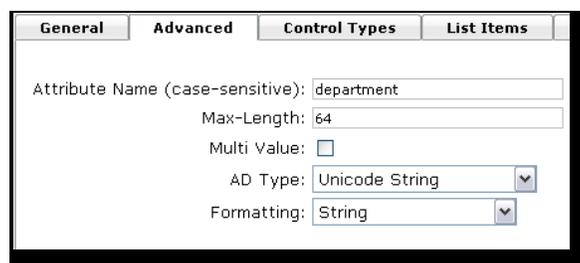
The Advanced tab contains the following options:

- 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.

- 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…

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.
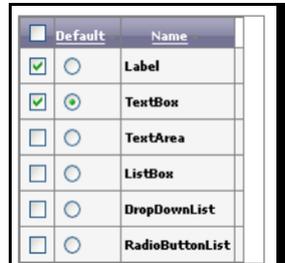
Control types can be marked as available by checking the checkbox. Unchecked control types will not be available as options when adding an attribute to an editable view. A default control type should be selected using the radio button. This will be the control type used if none is specifically selected 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 the 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.

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.

List items can be pasted into the text area when the text tab is selected or they may be individually added if the list tab is selected. These list item will appear as selectable options when creating an editable view. Specific list items may be selected for use in a view as not all list items are required for use in all editable views.

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 of the error message presented to the end user upon validation failure.
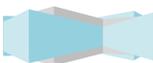
For additional information or questions concerning objectClass and attribute customization, please feel free to contact our support department.

MONITORING THE EVENT LOG

The AD Self-Service Suite uses a custom event log to log all events and actions from all members of the suite.

To view the AD Self-Service Event Log:

1. Click Start, click Run, type "eventvwr.msc" without quotes and click OK.

2. Click on the EmpowerID event log on the left hand side.
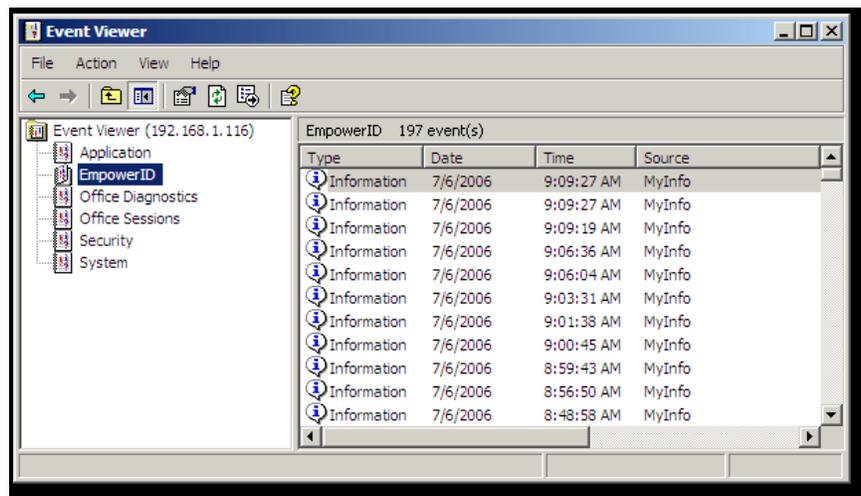
3. Double click any event on the right hand side that you wish to view. All actions performed by the AD Self-Service Suite are logged here, as well as any error messages and troubleshooting information generated by the suite.

33

EMPOWERID URLS FOR END USERS

AD WhitePages URLs

- http(s)://<server where AD WhitePages is installed>/ADSelfService/ADWhitePages/

- AD WhitePages is also available as a web part that may be deployed on any WSS site or Portal Area

- AD WhitePages is also available as a toolbar button that may be deployed in the header of SharePoint

AD Info URLs

- http(s)://<server where AD Info is installed>/ADSelfService/ADInfo

- AD Info is also available to end users as an embedded button in the AD WhitePages user interface.

- AD Info is also available as a web part that may be deployed on any WSS site or Portal Area

- AD Info is also available as a toolbar button that may be deployed in the header of SharePoint

AD Password URLs

- To change passwords or enroll for Password Reset:

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

- 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 may be deployed on any WSS site or Portal Area

- AD Password is also available as a toolbar button that may be deployed in the header of SharePoint

To reset their password or unlock their user account:

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

Note: the Configurator will automatically redirect users to the Password Reset Center from any web application configured to use it. In most cases users will not have to remember this URL and will automatically be redirected their upon logon failure.
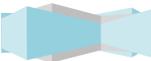
AD Self-Service Suite for Active Directory

Getting Started Installation Guide

TROUBLESHOOTING

AD SELF-SERVICE ADMIN WEB SITE LOGON - UNABLE TO BIND TO ACTIVE DIRECTORY

If you receive the error message shown below, there was a failure to create a secure Kerberos connection to Active Directory. This is most likely due to your machine not being part of the same domain, a DNS issue, or your Internet Explorer security zone settings not passing your credentials.

If you receive the error page above, a good troubleshooting step is to check if the Internet Explorer security zone settings are passing your credentials. To do this, click Tools, then Internet Options, then the Security tab. Click on the Local intranet zone, then the Sites button.
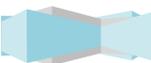
In the Local intranet zone dialog, ensure that Automatically detect intranet network is checked, and then click the Advanced button.
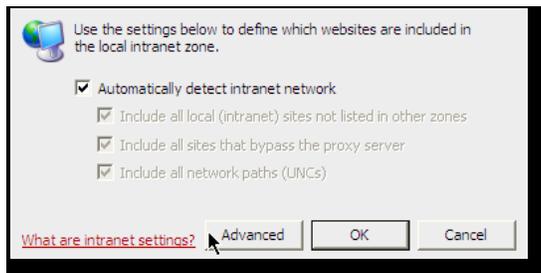
Type the URL of the server that is running the AD Self-Service Suite (http(s)://servername) into the text box and click the Add button to add the site to your Local intranet zone. All Internet Explorer security settings from the Local Intranet zone will now apply to any page viewed from that server.
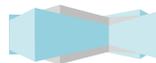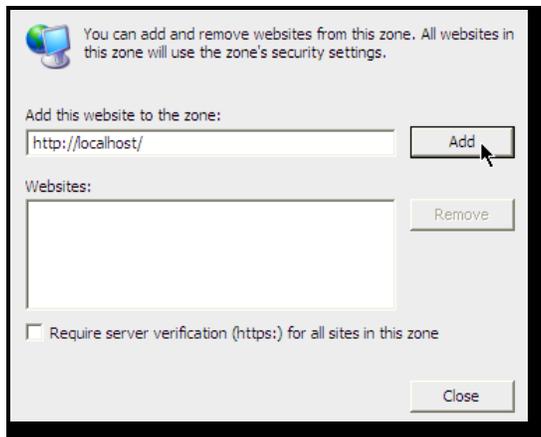

36

Click Close, and then click OK to return to the Internet Explorer Security tab. The next step is to adjust the security level of the Local intranet zone to automatically pass the credentials of the currently logged in user. Ensure that Local intranet is still highlighted, then click the Custom level… button.
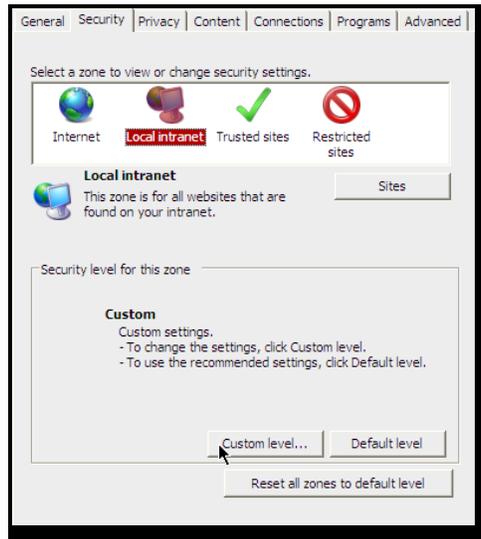
Scroll down to the User Authentication section, and then locate the Logon section below it. Click on the Automatic Logon with current user name and password radio button, then click OK to close the dialog.
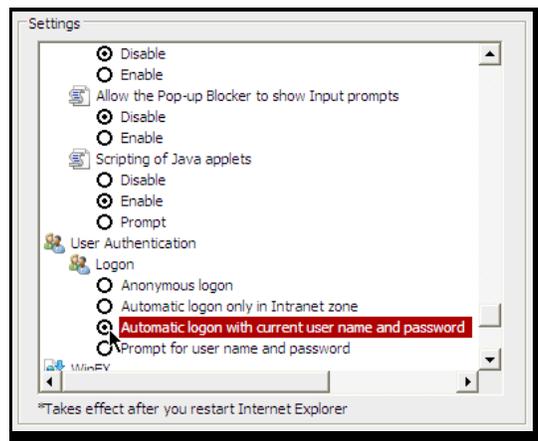

Click Yes at the warning prompt to confirm the change to the Local intranet zone, and then click OK to close the Internet Explorer security settings dialog. Close your current browser window and re-launch Internet Explorer in order for the changes to take effect.
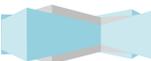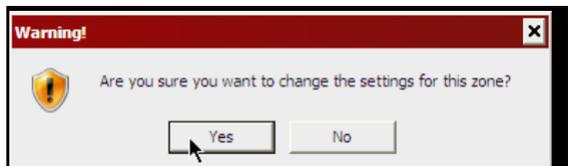
AD SELF-SERVICE ADMIN WEB SITE LOGON - DOMAIN NETBIOS RESOLVES LOCALLY

If you receive the error message shown below, the credentials of the currently logged on user is resolving locally to the server. This is most likely due to the server not being a member of the domain, the server experiencing DNS issues, or you are trying to logon to the AD Self-Service admin web site as the Administrator account or another account that has an identical name on the domain. Please join the server to the domain, logon with a domain admin that does not have an identical local and domain username, and check for DNS resolution issues.