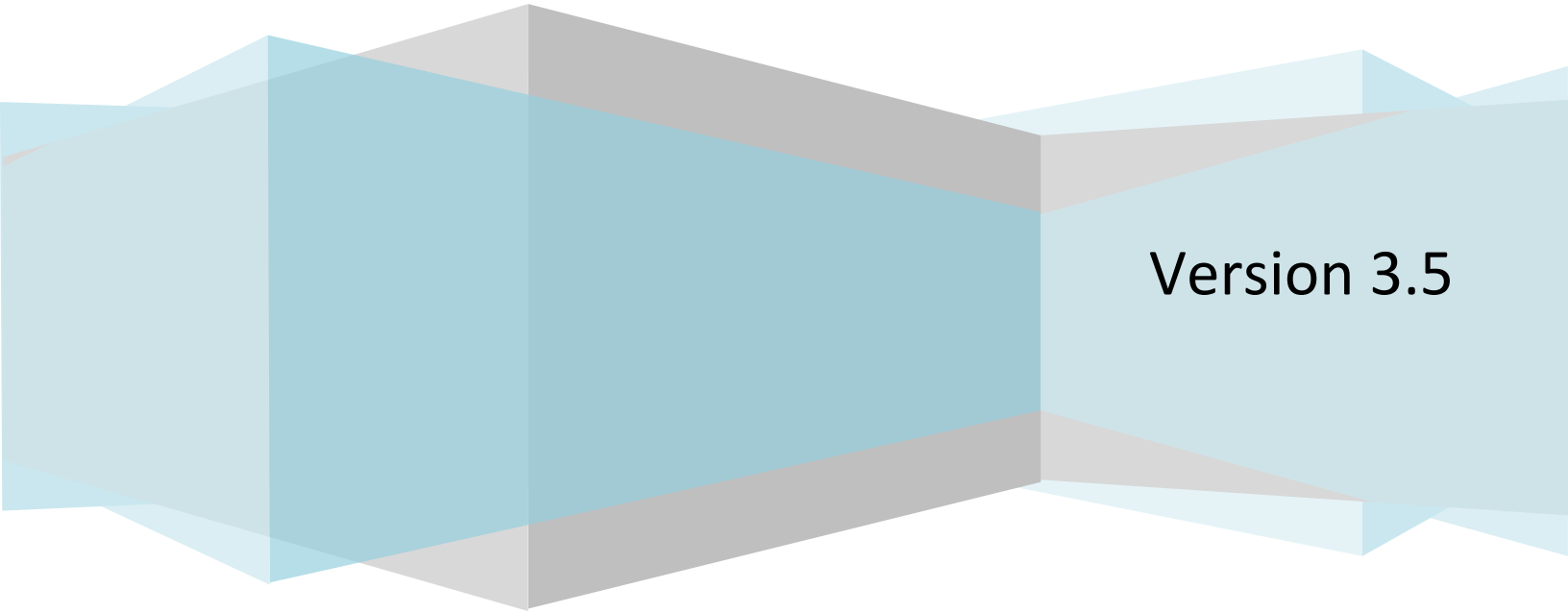
The Dot Net Factory

AD Self-Service Suite for Active Directory and ADAM

Architecture Overview White Paper



Version 3.5

TABLE OF CONTENTS

INTRODUCTION 3

BENEFITS OF DIRECTORY SELF-SERVICE AND DELEGATED ADMINISTRATION 4

THE AD SELF-SERVICE SUITE OF APPLICATIONS 4

OVERVIEW OF AD SELF-SERVICE APPLICATION COMPONENTS 5

OVERVIEW OF AD SELF-SERVICE TECHNOLOGY AND TERMINOLOGY 5

- CENTRALIZED DIRECTORY ATTRIBUTE MANAGEMENT 7
- HOW AD SELF-SERVICE PROFILES WORK 7
- EMAIL ALERTING 10
- THE AD SELF-SERVICE "ANYWHERE EVERYWHERE" DEPLOYMENT MODEL 11

IS DIRECTORY SELF-SERVICE RIGHT FOR YOUR ORGANIZATION? 12

CONCLUSION 13

INTRODUCTION

"The true value of a directory service is derived from the applications and intra- and inter-enterprise business processes that leverage the information contained within the directory." Gartner Group

The objective of this whitepaper is to describe the architecture, components and terminology that encompass the AD Self-Service Suite of applications. It will discuss how the components interact with each other and your Active Directory Domains and LDAP Directories, including Microsoft ADAM. The intended audience of this document is technical evaluators, technical decision makers, enterprise directory architects, and security professionals.

The use of user identity management and user self-service solutions within enterprises has grown rapidly with the increasing recognition that keeping workers connected and informed is critical to productivity and business success. The need to efficiently manage user access and directory resources has also increased in response to the growing complexity of today's interconnected business environments. Network roles have expanded beyond the traditional enterprise users, to now incorporate customers, suppliers, and partners. And organizations have discovered the significant benefit of being able to use security profiles to deliver highly tailored information that enables managers to direct activity more effectively and to improve communications.

The alternative to not having an effective user identity and self-service strategy is to have administrators and helpdesk staff become increasingly consumed by routine tasks that are costly and error prone when administrating large numbers of end-users. Tasks such as resetting passwords and updating user directory entries do not scale well. The Gartner Group estimates that 40 percent of help desk calls are attributed to password management requests from users. Each password reset call can cost up to $40 in dedicated resources for resolution and associated user downtime.

The AD Self-Service Suite has been designed specifically to unlock the productivity and collaborative potential of your directories by providing web-based lookup, self-service, and delegated administrative capabilities across an entire enterprise. AD Self-Service delivers improved information accessibility to both end-users and applications, reduces the cost of managing directory data, and improves the accuracy of the data without requiring custom development or scripting.

The AD Self-Service Suite is a 3rd generation solution built on the .NET 2.0 framework offering a full range of tightly integrated look-up, self-service and delegated administrative capabilities from friendly web-based interfaces. The AD Self-Service Suite seamlessly integrates with enterprise applications, such as Sharepoint and many others. AD Self-Service's user interfaces are intuitive and maintain the look and feel of common Microsoft applications, a key element for ensuring rapid user adoption and a strong return on your investment.

From an administrative perspective, AD Self-Service's components are server based and don't require the installation of client software, a key consideration in keeping the cost of deployment low and problem-free. Another aspect of AD Self-Service's unique approach to identity management is its flexibility in offering multiple user profiles based upon user role, geography, and tasks, which offers a level of collaborative possibilities not previously available.

AD Self-Service offers comprehensive change tracking (including a complete history of all self-service and delegated administrative activities with before and after values), and email alerting that is customizable on an action by action basis, all of which additionally benefits regulatory compliance.

BENEFITS OF DIRECTORY SELF-SERVICE AND DELEGATED ADMINISTRATION

The AD Self-Service Suites provides multiple friendly web interfaces that allow end-users to query your directories and edit their own entries. Organizations can also define "process owners", individuals, such as: department administrators, HR representatives, managers and vendors -- ensuring that entries are up-to-date.

Employee self-service is a big part of keeping business value to the enterprise high while keeping deployment and content ownership costs low. With the AD Self-Service Suite, employees or delegated individuals can keep their portions of the directory current, without the intervention of dedicated staff and the inevitable delays and redundant processes that traditional directory maintenance entails.

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.

The AD Self-Service Suite provides the following benefits:

- Improved process management – self service, including directory updates, Password Reset, and account lockout resolution can be executed without the need for a system administrator.
- Task controls and refinement -- user customizable templates ensure that elements of complex tasks can be defined and access to unrelated data is prevented, improving accuracy and data integrity.
- Time savings and lowered administrative burden -- system administrators can spend less time on repetitive tasks and increased time on higher value tasks and projects.
- Lower costs—Operational costs are lower due to the reduction in trained IT staff needed to respond to routine maintenance requests.
- Increased employee satisfaction – an end-user's downtime can be vastly reduced by an account lockout, allowing them to resume their work quickly and easily without being dependent on contacting an IT staff member.
- Vendor self-management – vendors who must have access to enterprise systems can have secure, web-based user provisioning tasks securely delegated to them, allowing them to have responsive interaction with your system.

THE AD SELF-SERVICE SUITE OF APPLICATIONS

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 your Microsoft directories (Active Directory and ADAM) 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 and ADAM. 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's 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.

OVERVIEW OF AD SELF-SERVICE APPLICATION 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 licensing, and the Local Administration account used for event logging.

- ASP.NET Web Applications—the full AD Self-Service Suite currently consists of the following web applications: Admin, AD WhitePages, AD Info, AD Password, and the Password Reset Center.

- 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.

- Application Pool—AD Self-Service utilizes an application pool named “AD Self-Service” for operations and the optional SQL logging.

- 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.

OVERVIEW OF AD SELF-SERVICE TECHNOLOGY AND TERMINOLOGY

- Connected Directories—AD Self-Service supports connecting to multiple Active Directory Domains, even those in untrusted Forests. AD Self-Service can also connect to Microsoft ADAM. Additional LDAP-compliant directories are currently undergoing validation for full support.

- Directory Connections—all applications in the AD Self-Service Suite utilize shared Directory Connections to communicate with each of the Connected Directories. A Directory Connection consists of a server fully qualified DNS name, a domain name or LDAP partition, and a proxy account to use for authentication and access.

- Proxy Accounts—the proxy accounts saved as part of the Directory Connections are used by the applications in the AD Self-Service Suite to retrieve information from the Connected Directory and perform all account management actions. Proxy accounts require all the necessary privileges needed to perform any of the actions performed by the AD Self-Service Suite applications deployed. A member of the Domain Administrators group may be used for simplicity.

- Centralized Attribute Management—AD Self-Service's centralized attribute management allows complete management and control over directory attribute usage for any object types (objectClass) used in the AD Self-Service Suite. The attributes for each object type are individually managed and may be enabled or disabled for use, given default list item values, and assigned with a selection of custom regular expression validators.

- Multi-Profile Configuration System—a profile is a single complete configuration set for a member application of the AD Self-Service Suite. It contains all necessary settings and has its own access control explicitly limiting which users or groups are granted or denied access to the profile. Administrators can create many profiles, each with alternate settings targeted to different audiences or roles. End users receive only those profiles to which they have been granted access.

- Query Scopes—query scopes provide a flexible mechanism for limiting the information and object types included in the AD WhitePages profile. Each query scope consists of: the object types (users, contacts, printers, etc.) to include from each domain or directory; a per object type LDAP path below which objects should be listed; and a search filter to further limit which of the resulting objects to include.

- Visual Form Designer—the Visual Form Designer is a "what you see is what you get" (WYSIWYG) editing tool for designing the read-only and edit views displayed when a directory object (user, group, etc…) is selected. This tool is used by AD WhitePages and AD Info.

- AD WhitePages Directory Views (read-only and "Editor")—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 are not limited to a single domain or directory but can include information from any number of directories including untrusted forests and ADAM directories. 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 a specific Directory View.

- AD Info Views—AD Info Views are much like the Editor mode of a AD WhitePages Directory View. The difference is that a AD Info View restricts the user to editing only their personal information.

- AD Password Enrollment Profile— an AD Password enrollment profile is the encrypted information stored in the user's object after they enroll for Password Reset. The information contains the specific questions they answered, as well as their corresponding answers. The questions are encrypted using a two-way algorithm while the answers use a one-way algorithm.

- Web Applications—the AD Self-Service applications are ASP.NET 2.0 web applications utilizing a shared AD Self-Service application pool.

- Web Parts—all members of the AD Self-Service Suite offer SharePoint web parts. The SharePoint web parts offer identical functionality and may be deployed any number of times across your Windows SharePoint Services sites or SharePoint Portal Areas.

- Toolbars—the AD Self-Service Toolbar is a small form-factor deployment option presenting users with a button for each application in the AD Self-Service Suite to which they have access. Clicking on any of the buttons launches an onscreen version of the application appearing above their current page for quick and convenient access. The Toolbar may be deployed as a web part, or deployed using the AD Self-Service Global Deployment method in SharePoint and many other web applications.

- Global Deployment—the Global Deployment option allows the AD Self-Service Toolbar to be deployed as an embedded component within the user interface of other applications. This non-invasive deployment

model allows the toolbar to seem as if it is a part of another application SharePoint or other applications running on Windows Server 2003. This integration is possible without requiring modifications to the host application's source code. This unique deployment model allows the full power of the AD Self-Service Suite to be seamlessly integrated into existing and custom web applications.

CENTRALIZED DIRECTORY ATTRIBUTE MANAGEMENT

All applications in the AD Self-Service Suite operate in some fashion by editing or managing directory objects and their attributes. The Directory Attribute management section of the admin web site offers a robust centralized attribute management facility enabling flexible management of attributes for any object type. The AD Self-Service Suite supports any LDAP objectClass you wish to manage existing in your LDAP or Active Directory domain (users, contacts, computers, nisNetgroup, etc…). The schema of each objectClass is not modified using the AD Self-Service tool but rather administrators can manage the usage of objectClasses and their attributes already existing in the connected directories.

From the Admin web site, administrators can add new attributes to the AD Self-Service Suite and configure how they will be used and represented. For new, added or existing attributes, administrators may define the attribute name, friendly label, and available control used to represent this attribute to end users.

Available attribute controls include (as applicable):

- Label (read-only)
- Lookup
- DateSelector
- Textbox
- Textarea
- RichTextEditor
- Checkbox
- Tri-stateBoolean
- Listbox
- DropdownList
- RadiobuttonList

Default list items can be entered for the following attribute controls: listboxes, dropdown lists, and radiobutton lists. This capability is useful for fields like department, division, or job title, where it is advantageous to enforce data consistency by not allowing free-text entry. This ensures that one user may not enter "Sales Department" while the next enters "sales". The attribute management tool also allows validators to be assigned to attributes. Multiple validators (US Zip code, French postal code, etc...) may be made available for an attribute. They will then be selectable when designing editable directory views.

HOW AD SELF-SERVICE PROFILES WORK

Applications in the AD Self-Service Suite implement a unique multi-profile system allowing dynamic flexibility, personalization, security, and privacy even in the largest and most complex organizations. A profile is a single

complete configuration set in a member application of the AD Self-Service Suite. It contains all necessary settings and has its own access control limiting which users or groups may access the profile and which are explicitly denied access to the profile.

This base unit of replicable functionality is used throughout the AD Self-Service Suite as Directory Views in AD WhitePages, AD Info Views in AD Info, and the AD Password Profile in AD Password. In each of these applications, an unlimited number of profiles may be created and presented to various organizational roles or audiences. Unlike single profile applications, this allows different roles in the organization to view or manage completely different sets of objects with different layouts and themes. It also allows user to receive multiple profiles so that multiple views can be presented and a single user granted vastly different rights and capabilities, depending upon the sets of directory objects contained in the profile. For example: a departmental manager is not assigned as an Editor for a Directory View showing all users or other objects in the directory, but he or she might be an Editor for a Directory View listing just their direct reports. This flexibility in controlling both the objects to be displayed in a Directory View as well as the attributes to be visible and editable is made possible by AD Self-Service Query Scopes and the Visual Form Designer.

QUERY SCOPES

The flexibility of creating various Directory or Management Views, each showing different objects from different domains or directories, is used throughout the AD Self-Service Suite to provide fine-grained control for directory lookups, self-service, and delegated edits and administration. The technology used to provide this fine-grained control is called Query Scopes. Query Scopes are configurable using the Admin web site. When creating a Query Scope for a Directory or Management View, administrators add connections for the various directories in order to include them in the View. When adding each connection, the administrator specifies or selects:

- the Active Directory domain or LDAP directory
- the object type (user, contact, group, etc…) or for this connection – one connection is added per objectClass.
- the LDAP path below which objects of this type should be listed – select an organizational unit or container.
- a search filter to further limit which objects should be included in the Directory or Management View
- a list of acceptable actions for this connection (edit, list in lookups, list in grid, etc…)

The combination of these five options allows very granular control over exactly the information to be included for viewing or editing in a Directory or Management View. This coupled with the multi-profile system (which allows users to receive multiple profiles - but only those to which they have been granted access) permits almost any security or delegation scenario to be achieved.

A sample Directory View named “My Department” could be configured that only displays user objects existing below a particular organizational unit, where the user objects have the same value in the department attribute as the user viewing the application. Another common Directory View would be named “Entire Company”. This view would show all directory objects (users, contacts, groups, shares, rooms, documents, etc…) but only show a limited set of attributes permitted to be viewed by anyone in the organization. A single search box in this view would allow users to search or browse any object from any connected directory. These various views are easily created in the admin web site using an administrative version of the advanced search control used in AD WhitePages.

THE VISUAL FORM DESIGNER

The flexibility in the AD Self-Service Suite multi-profile system is greatly enhanced in AD WhitePages, and AD Info by the ability to design multiple unique user interface layouts. AD WhitePages support creating a read-only and an edit view for each object type to be included in a profile. This mean that the attributes displayed when viewing a contact would be distinct and relevant for a contact, whereas the details for a computer would show a different layout with different attributes. These layouts are unique per profile and are easily designed in a “what you see is what you get" environment using the AD Self-Service Visual Form Designer.

The Visual Form Designer is a component of the Admin web site and is used when creating the user interface layout for Directory Views, AD Info Views, and Management Views. When designing the edit view for user objects displayed in a particular Directory View, the Visual Form Designer allows user interface tabs to be created, along with groupings of fields, and the selection of individual attributes themselves. Attributes may be reordered within a grouping of fields by simply dragging and dropping them. When adding an attribute to an edit view, any available control types, default values, and validators may be selected. For example, when adding the telephone attribute, it could be represented as a textbox with a US phone number validator. When using a field like department, the administrator may choose to have the department attribute appear as a dropdown list of values. When creating a Directory View to be used by employees in the Brazil office, the Visual Form Designer would allow selection of just the values relevant for users of this Directory View. It would not have to display every available list item including irrelevant values for other geographies. Available field representations (textbox, listbox, etc...), default values, and validators are pulled from the shared settings created using AD Self-Service’s centralized directory attribute management capabilities.

AD WHITEPAGES PROFILES – “DIRECTORY VIEWS”

In AD WhitePages, profiles are known as Directory Views and presented to end users as tabs in the web-based user interface. Each tab is given a friendly name to describe the information or view of the organization it represents. Users see only those tabs (each tab is a profile or Directory View) to which they have been granted access. When a tab is clicked, it loads the directory information and displays the users, contacts or other objects that have been configured to display in that Directory View.

The attributes to be displayed in the grid or in the details view when an object is selected, and those shown in the “Editors” mode are completely customizable and unique per Directory View. The flexibility in the AD Self-Service Profile system allows each Directory View to display a completely different set of objects from a different set of OUs, domains, or LDAP directories, granting users a different set of rights or capabilities per Directory View.

AD INFO PROFILES – “INFO VIEWS”

AD Info allows end-users to manage and update their personal directory information. In most organizations, different roles are granted the ability to edit different numbers of their own attributes. Roles with fewer privileges may only be allowed to edit a few personal information fields such as telephone, mobile phone, pager, description, and homepage URL. Roles with greater privileges might be allowed to edit many additional fields such as addresses, titles, and other information. In addition to providing different roles with different levels of editing capability, there are also divisional or geographic differences to consider. An organization spanning Europe would need to support a variety of languages and consequently would have many dropdown list values for an attribute like department or job title. Each language or locality might have its own set of values for these and other fields.

AD Info easily handles the complexities of varying levels of user privileges and geographic differences using the AD Self-Service multi-profile architecture. In AD WhitePages users see any Directory Views to which they have been granted access as browsable tabs in the web-based user interfaces. Each of these Directory Views will have a completely distinct set of grid fields, object detail layouts, and edit views. The various views are easily designed using the Visual Form Designer.

AD Info uses this same technology to implement its own multi-profile system. Administrators can easily design multiple AD Info Views using the same mechanisms as those found in AD WhitePages. The difference with AD Info is that a user only receives a single AD Info View. Users receive the first AD Info View to which they have been granted access. AD Info Views are assigned priorities in the Admin web to control the order in which they are evaluated. Each has an Allow and Deny access list based upon user or group identity. The AD Info View received defines which attributes a user may edit and how those attributes are displayed in the interface. Administrators design AD Info Views by selecting which attributes to show, which are editable, how they may be edited (dropdown list or textbox entry), which default values are available -- if any, and what validators are to be applied. This flexibility easily allows different roles to have different editing capabilities and allows users in different geographies to receive only those validators and default value selection items relevant to them.

AD PASSWORD PROFILES – "AD PASSWORD PROFILE"

AD Self-Service AD Password offers users the ability to change their passwords while online from a friendly web interface, as well as the ability to recover their account if they become locked-out or forget their password. Users are able to recover their account by correctly answering questions they answered during enrollment from one of the authenticated AD Password interfaces. From the admin web site, administrators define how many questions and of what types (required, selectable, write your own) users must answer during enrollment and later account recovery. Users can be required to answer any number -- or none -- of each type of question.

The specific questions answered by a user along with their answers are considered an enrollment profile. This information is stored encrypted in an attribute of their user object in Active Directory. The questions answered are stored using two-way encryption so they may be retrieved during the recovery process. The answers are stored using a one-way encryption that does not allow them to be decrypted. The answers a user enters while trying to recover their account from the Recovery Center are validated against these stored answers. If the user answers all questions correctly, they may then unlock their account, reset their password, or perform both actions, depending upon the situation and the rights they have been granted through the AD Password admin settings. AD Password offers a Password Reset Center lockout policy to prevent unauthorized attempts to guess another user's enrollment answers and reset their password. The lockout policy bars recovery attempts for a user account after failing a specified number of times within a specified number of minutes. The user account may again access the Recovery Center after a specified amount of time has passed.

AD Password also supports advanced password policy enforcement when users are changing their password while authenticated or when resetting their passwords from the anonymous Password Reset Center. Password policies are read directly from the Active Directory domain of the user. All policies are enforced including password history and minimum password age. Password history is enforced even during the account recovery process. However, one additional password is aged out of the user's history on each Password Reset. The minimum password age policy and password history may be selectively enabled or disabled on the admin web site. Minimum password age may be disabled for users using the Recovery Center if you wish to always allow account recovery. Disabling minimum age for these users will bypass password history enforcement in these scenarios.

EMAIL ALERTING

AD Self-Service offers customizable email notifications for AD Password. AD Password notifications may be enabled for any action performed in the application. For each action, a customizable HTML message may be sent to the end user or a group of administrators. The end user and administrator emails are independent and may be customized separately.

THE AD SELF-SERVICE "ANYWHERE EVERYWHERE" DEPLOYMENT MODEL

The traditional model for identity and self-service applications is to have a single web URL to which users must navigate in order to perform self-service or delegated administrative functions. The AD Self-Service Suite has a new and unique approach offering many user interface options that can be deployed as traditional web applications or integrated into commonly used web applications. This delivers services to where users work, instead of requiring them to learn new habits and to navigate to a dedicated web site to use the applications. AD Self-Service seamlessly integrates into the user interface of commonly used applications, such as Microsoft SharePoint or Outlook Web Access. AD Self-Service provides users with 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:

SharePoint web parts

Each application offers a full-featured SharePoint Web Part that may be deployed to any existing Windows SharePoint Services site or SharePoint Portal Server Area.

Toolbars

Each AD Self-Service Suite application offers a small form factor toolbar button that may be deployed into the user interface of your SharePoint or custom ASP.NET web application. The toolbar deployment will display a button for each application to which the user has been granted access. The toolbar buttons appear as a natural part of the existing application interface. Clicking on a toolbar button will launch a small on-screen version of the respective application. The Toolbar may be deployed as a SharePoint web part or using the AD Self-Service Global Deployment technology. Global Deployment allows the toolbar to be installed once on a server and automatically be visible for users on every page, without modifying the web pages of the server and without requiring maintenance as new pages or sites are added. Many custom applications are also supported with minor manual configuration changes.

Windows Client (GINA Extension)

The Windows client is a separate application that may be deployed silently to your Windows XP or Windows Vista 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.

Web Applications

Each application may be accessed as a standard web application with a dedicated URL. In addition, the following web sites are included as part of the suite:

- **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 meeting the installation requirements listed previously. In standalone settings mode, the AD Self-Service settings on stored on the local file system of the AD Self-Service server. In this mode, an instance of the Admin web site is required to modify the settings. When running in shared settings mode, settings are stored as objects in an Active Directory domain or ADAM directory. In this mode, only one installation of the Admin web site is required to manage the settings for multiple AD Self-Service servers. See the AD Self-Service QuickStart Guide for instructions on activating the Admin site on additional servers or websites.

- **AD Password Reset Center —** this anonymous web site is used by AD Password users to reset forgotten passwords and unlock locked-out accounts. The Password Reset Center maybe installed on any number of

servers. Alternately, web servers requiring Windows credentials may be configured to automatically redirect failed logon attempts to any other installation of the Password Reset Center.

IS DIRECTORY SELF-SERVICE RIGHT FOR YOUR ORGANIZATION?

Organizations continue to seek a competitive advantage by offering identity services on a stable, scalable infrastructure, while keeping the associated costs low to maximize profitability. The AD Self-Service Suite is an integrated, yet modular platform that enables self service functionality in several critical areas of identity management. The benefit of the AD Self-Service Suite is that an organization can acquire any one or combination of its components (AD Password, AD Info, or AD WhitePages) and acquire any of the other components when needed.

AD Self-Service is appropriate for organizations with Active Directory or ADAM seeking to automate self-service and provide transaction and activity tracking for regulatory compliance. There are numerous situations in which deployment of the AD Self-Service Suite can be justified, and the following are common considerations:

- **Forgotten passwords and account lockouts** – this common problem is costly to support for local users, but is especially difficult for mobile users who are frequently 24 hour workers who often have no facility for changing passwords while connected remotely. AD Password addresses this need while allowing IT support staff to focus on higher value tasks.

- **AD WhitePages directory access** – increasing awareness and accessibility to an organization's employees is a key need for many of today's businesses who size and geographical dispersion works directly against productivity. Having a AD WhitePages that is up to date, flexible, electronically distributed and offers rapid lookup is essential in today's business environment. Having a product that can draw from and augment the key information store for a system's user identities (Active Directory, ADAM or any LDAP directory) is of immense value. Contextual actions when looking up a person, a department or a job function can include: sending an email, dialing a phone number, inviting to a meeting, instant messaging, adding to a contact list, locating on a map, and other actions that encourage communication.

- **User ability to maintain their information in the directory** – user information is only of value when it is current and accurate. When dealing with a dynamic source of information with so many inputs, successful maintenance depends on delegating it to the user. And the user's success hinges on the intuitiveness and ease of use of the interface, all of which AD Info achieves.

- **Security, control and tracking for identity** management – of great concern to enterprises is the ability to control a user's view to sensitive information. AD Self-Service Suite allows you to control a view at the group, user and attribute levels. The AD Self-Service Suite provides comprehensive change management with full logging to the event log and the ability to track all events and changes by users and locations with full SQL reporting. This is an important consideration for firms that want to incorporate these features into their plans for regulatory compliance.

- **Enterprise-wide functionality** – the AD Self-Service Suite has the ability to pull directory information from across disparate systems, including multiple forests, trusted and untrusted sources, independent ADAM instances into a single searchable results set called Directory Views, which users can query and browse. The suite also offers fully scalable and optimized performance that doesn't degrade in directories with very large user counts.

- **Large organizations that are deploying a Microsoft ADAM LDAP directory** – AD Self-Service Suite is the only product offering full ADAM support for password self-service and recovery, directory information self-service, corporate WhitePages and delegated administration. Many organizations are deploying

ADAM for extranet applications where they don't require the additional overhead or licensing expense of Active Directory, but until now there has been a dearth of tools to enable this. AD Self-Service fulfills a key role in the rollout of ADAM services.

- **High user adoption rates** – the rate of return that can be expected for any new application deployed in the enterprise hinges on the rates of user adoption. The AD Self-Service Suite was specifically designed to generate high user acceptance: it incorporates a simple and intuitive user interface; it deploys as a transparent element within existing web applications and custom applications; it features seamless visibility via a toolbar to all of the actions permitted to the user throughout the components of the suite; and incorporates a master detail layout system so that users can contextually track more information about the objects that they are viewing, aiding the user's interaction with the information displayed on their screen.

- **Low cost and ease of deployment** – you can deploy the AD Self-Service Suite in a matter of hours not weeks. AD Self-Service's server-centric architecture and simplified deployment translates into dozens of saved hours and saved expenses in key tasks that must be performed by IT staff, including: proof of concept trials, live system deployment and any minimal debugging that occurs. The Dot Net Factory prides itself on providing immediate implementation support over the phone, rather than scheduling weeks ahead for complex installs that are typical of products that deliver portions of the functionality within the AD Self-Service Suite.

CONCLUSION

The AD Self-Service Suite for Active Directory and ADAM leverages one of the most valuable and underutilized stores of information within businesses – your Microsoft directories -- to create significant business capabilities, cost-savings, and user satisfaction. AD Self-Service employs a robust, state of the art architecture and interface that seamlessly integrate with LDAP directories and a wide range of business applications.

The AD Self-Service Suite solves many of the critical issues for businesses seeking identity management and self service solutions, including: scalability, cross directory integration, immensely flexible and detailed delegated administrative capabilities, a user directory with enormous adjustability based on the viewer, and an integrated platform and server-centric architecture that simplifies deployment and end-user adoption.

Each modular application in the integrated Suite is designed to help you deliver user services while reducing operating costs, increasing user satisfaction and productivity. The impact can extend to improving the efficiency and the access of network services provided to business partners.

AD Self-Service focuses on improving productivity and information quality and accessibility for a variety of user identity management needs. The method of approach was to focus on the quality of the user experience while building on a robust state of the art platform that meets a wide set of demanding management control, security and reporting needs within an enterprise environment. The AD Self-Service Suite distinguishes itself in its innovative use of server centric design and desktop controls to minimize IT implementation and maintenance costs and to maximize management control and the richness of the user experience.

For more information on The AD Self-Service Suite, including an overview and videos visit http://www.adselfservicesuite.com/ or our online Demo Center at http://www.adselfservicesuite.com/DemoCenter.aspx .