

User Guide



ManageEngine
ADSelfService^{plus}

demo.adselfserviceplus.com

<http://www.adselfserviceplus.com>

Table of Contents

Welcome to ADSelfService Plus	3
Contact AdventNet.....	4
Getting Started	6
System Requirements for ADSSP	7
Installing ADSelfService Plus	8
Working with ADSelfService Plus.....	9
Installing Service Packs.....	11
Uninstalling Service Packs	12
Licensing ADSelfService Plus	13
How ADSelfService Plus Works.....	14
ADSelfService Plus Working Principle.....	15
Components of ADSelfService Plus	16
ADSelfService Plus Admin Portal.....	17
Configuring Domains on ADSelfService Plus	18
Dashboard	19
Reports	20
Admin.....	24
Policies Configuration	25
Reset Password Configuration	27
Unlock Policy Configuration.....	30
Self Update Policy Configuration.....	32
Configure a Change Password Option	33
Enrollment Settings	34
Question and Answer Settings.....	36
Import Answers	38
Configure Report Scheduler.....	39
ADSelfService Plus GINA / Credential Provider	41
Installation of ADSelfService Plus GINA / CP on Client Machines:	43
Users Reset Password / Unlock Account using ADSelfService Plus GINA / CP.....	46
General Settings	51
Customize Display Settings of ADSelfService Plus	51
Custom Attributes.....	56

NT Service..... 57

Connection Settings 58

Install SSL Certificate 60

Server Settings..... 63

Personalization..... 64

Domain User Web Portal 65

 Self Service..... 67

 Change Password..... 68

 Reset Password..... 69

 Unlock Account 70

 Users Reset Password / Unlock Account using ADSelfService Plus GINA / CP..... 71

ADSelfService Plus Deployment Scenarios..... 75

Troubleshooting Tips..... 78

ADSelfService Plus Frequently Asked Questions..... 82

Welcome to ADSelfService Plus

ADSelfService Plus is a web based product which allows end users to reset forgotten passwords securely, allowing administrators to implement stronger password policies while reducing help-desk workload. It provides a simple, secure web based solution that allows end users to reset forgotten passwords and unlock their user accounts themselves by answering configured pre-set question and answers.

The Self Service Password Reset Solution also features a client software "ADSelfService Plus GINA / CP" which facilitates end users to Reset Forgotten Passwords or Unlock Locked Out Accounts from the Windows Logon Extension of their computers by entering "**CTRL + ALT + DEL**" option.

ADSelfService Plus helps to generate comprehensive reports on Locked Out Users, Soon-to-Expire-Password-Users, Password Expired Users which provides a clear picture on the status of users and accounts present in the Domain. Also the above reports can be scheduled and email on a monthly, weekly, daily or hourly basis providing administrators control and end-users with the most needed notification on soon to expire passwords.

It also provides a detailed **audit feature** on when, by whom and which user password or accounts was modified. Further a Self Update feature where a user can update his/her own personal information from the web based console is bundled with the product. The Administrator can give controlled access to users for updating their personal contact details by themselves which may include available attributes present in the Active Directory like given name, sAM Account name etc., as well as custom Attributes based on LDAP attribute value as "employeeid" etc.,

The Admin Function of ADSelfService Plus allows the users with privileges to General Attributes, Exchange Attributes, Account Attributes, Terminal Attributes and Custom Attributes. The end user can have one or more of these privileges to be modified by himself as it is delegated by the Administrator.

The Following Sections will help you get familiar with the product:

Getting Started: Provides you the details of system requirements, product installation and startup

Contact AdventNet

- [AdventNet Headquarters](#)
 - [Sales](#)
 - [Technical Support](#)
-

AdventNet Headquarters

Web site	www.adventnet.com
AdventNet Headquarters	AdventNet, Inc. 5200 Franklin Dr, Suite 115 Pleasanton, CA 94588 USA Phone: +1-925-924-9500 Fax : +1-925-924-9600 E-mail: info@adventnet.com
AdventNet Development Center	AdventNet Development Centre (I) Private Limited 11 Sarathy Nagar, Vijayanagar, Velachery, Chennai 600 042 INDIA Phone: +91-44-22431115 (10 lines) Fax: +91-44-22435327 E-mail: info@adventnet.com

Sales

To purchase ManageEngine ADSelfService Plus from any part of the world, you can fill out the Sales Request Form. A sales person will contact you shortly. You can also send us an e-mail at sales@adventnet.com.

You can also call the AdventNet headquarters at the following numbers:

Phone: +1-925-924-9500

Fax: +1-925-924-9600 and request for Sales

Technical Support

One of the value propositions of AdventNet to its customers is excellent support. During the evaluation phase the support program is extended to you free of charge. Please send your technical queries to support@adselfserviceplus.com

- Following is the support format to be enclosed, while sending support mails:
- Edition (Free or Professional Edition) of the product
- Operating System version, such as Win 2000, 2003, etc.
- Browser version, such as Netscape 7.0, IE 5.5, etc.
- Details of the problem
- Steps to reproduce the problem.

Alternatively, select the Support tab from the client window. It has the following options that will allow you to reach us:

- Request Support - Submit your technical queries online.
- Need Features - Request for new features in ADSelfService Plus.
- User Forums - Participate in a discussion with other ADSelfService Plus users.

Contact Us - Speak to our technical team using the toll free number (1-888-720-9500)

Getting Started

The following sections describes how to get started with ADSelfService Plus.

- [System Requirements](#)
- [Installing ADSelfService Plus](#)
- [Working with ADSelfService Plus](#)
- [Installing Service Packs](#)
- [Uninstalling Service Packs](#)
- [Licensing ADSelfService Plus](#)

System Requirements for ADSSP

- [Hardware Requirements](#)
 - [Software Requirements](#)
-

Hardware Requirements

Hardware	Recommended
Processor	P4 - 1.0 GHz
RAM	512 MB
Disk Space	200 MB

Software Requirements

Supported Platforms

ManageEngine ADSelfService Plus supports the following Microsoft Windows operating system versions:

- Windows 2000.
- Windows XP.
- Windows 2003.
- Windows Vista.
- Supported Browsers

ManageEngine ADSelfService Plus requires one of the following browsers to be installed in the system for working with the client.

- Internet Explorer 5.5 and above
- Netscape 7.0 and above
- Mozilla 1.5 and above
- Firefox 1.5 and above

Preferred screen resolution 1024 x 768 pixels or higher.

Installing ADSelfService Plus

- [Installing ADSelfService Plus](#)
 - [Uninstalling ADSelfService Plus](#)
-

Installing ADSelfService Plus

ADSelfService Plus is distributed in the EXE format. ADSelfService Plus can be installed in any machine in the domain with the specified system requirements. You can install ADSelfService Plus as:

- [An Application](#)
- [A Windows Service](#)

Installing ADSelfService Plus as an Application

By Default ADSelfService Plus will be installed as an application, run the self-extracting EXE and follow the instructions.

When ADSelfService Plus is installed as an Application, starting ADSelfService Plus runs with the privileges of the user who has logged on to the system.

ADSelfService Plus as a Windows Service

To run ADSelfService Plus as a service. Do the following steps after installing.

- Go to Start Menu
- All Programs
- Select ADSelfService Plus
- Select NT Service
- Select Install ADMP Service

When ADSelfService Plus is installed as a service, starting ADSelfService Plus runs with the privileges of the system account.

Uninstalling ADSelfService Plus

To uninstall ADSelfService Plus , select Start --> Programs --> ADSelfService Plus --> Uninstall ADSelfService Plus.

Working with ADSelfService Plus

- [Starting ADSelfService Plus](#)
 - [Launching ADSelfService Plus Client](#)
 - [Stopping ADSelfService Plus](#)
-

Starting ADSelfService Plus

ADSelfService Plus can be started either in the system account (when run as service) or in user account (when run as application).

When ADSelfService Plus is installed as a Service

Option to install ADSelfService Plus as a service is available in the installation wizard.

To start ADSelfService Plus in the system account, select Start --> Programs --> ADSelfService Plus--> Start ADSelfService Plus

To start ADSelfService Plus in the user account, double-click the ADSelfService Plus desktop icon.

When ADSelfService Plus is not installed as a Service

In this case, ADSelfService Plus can only be started in the user account. To start the product, select Start --> Programs --> ADSelfService Plus --> Start ADSelfService Plus

On starting the ADSelfService Plus, the client is automatically launched in the default browser.

When ADSelfService Plus is started in Windows XP / Windows 2003 machines with firewall enabled, Windows may pop up security alerts asking whether to block or unblock the following programs as shown in the images below:

1. mysqld-nt - Database server.
2. Java(TM) 2 Platform Standard Edition binary - Java.

You should Unblock these programs to start ADSelfService Plus



Fig: MySQL Alert



Fig: Java Alert

Launching ADSelfService Plus Client

To launch the ADSelfService Plus client, open a Web browser and type `http://hostname:8888` in the address bar. Here the hostname refers to the DNS name of the machine where ADSelfService Plus is running.

Specify the user name and password as admin (for first time users) in the respective fields and click Login. If you have changed the password, you should use the changed password to login.

Stopping ADSelfService Plus

To stop ADSelfService Plus, select Start --> Programs --> ADSelfService Plus--> Stop ADSelfService Plus

Installing Service Packs

AdventNet periodically provides Service Packs which provide new features (requested by the customers), fixes for certain bugs and document updates in the form of HTML files. Service Packs can be downloaded from the Web site, and updated into ManageEngine ADSelfService Plus using the Update Manager tool.



Note: Ensure that no application is running when applying the Service Pack. This prevents any files used by the application from being over-written. For example if the ADSelfService Plus is running, stop the server and then install the service pack.

The steps to apply a Service Pack are as follows:

1. Start Update manager by executing the script **UpdateManager.bat** file located in <ADSelfService Plus Home>/bin directory.
2. Click **Browse** and select the Service Pack file (.ppm) to be installed. Click **Install** to install the Service Pack.
3. You can go through the Readme file of the Service Pack by clicking the **Readme** button.



Note: On clicking **Install**, the tool checks whether there is enough space for the installation of the service pack. If there is no enough space, the tool informs you about the lack of space. You must clear the space and then proceed with the installation

Uninstalling Service Packs

You have the option of reverting the changes incorporated by the installation of a Service Pack. You can revert to the previous version of the Service Pack or to the base version of the application. Before you start the un-installation process, make sure no application is running.

The steps to revert to a previous version are as follows.

1. Start Update manager by executing the script **UpdateManager.bat** file located in <ADSelfService Plus Home>/bin directory.
2. Select the service pack, which needs to be uninstalled, from the Installed Service Pack list. Click **Uninstall** to proceed with the uninstallation.
3. The list of dependent service packs if any will be shown for your confirmation before proceeding with the process.
4. Click **Finish** to proceed.

The specified Service Pack will be uninstalled from the application. You can now continue with the screen (like Uninstalling another Service Pack) or quit the tool by clicking **Exit**.

Licensing ADSelfService Plus

ADSelfService Plus is available in two editions - Free and Standard Editions

Download the product from the Website.

The Free Edition and the Standard Edition, both come packaged as a single download. During the evaluation phase, the Standard Edition is installed and can be evaluated for 30 days. After 30 days, it is automatically converted to the Free Edition, unless the Standard Edition license is purchased.

For purchasing the license or any queries, please contact sales@adventnet.com. The license file will be sent through e-mail.

To upgrade from a Trial Edition or Free Edition to Standard Edition

1. Click the License link available in the top right corner of the ADSelfService Plus client. This opens the License details of the product.
2. Click the Upgrade Now link and select the license file received from [AdventNet](#) using the Browse button.
3. Click Upgrade button to upgrade from Trial or Free Edition to Standard Edition.

Trial Version of ADSelfService Plus

The Trial edition of ADSelfService Plus provides access to 50 users to be enrolled with ADSelfService Plus.

The 50 users will be able to have complete functionality the trial version is valid for a period of 30 days after which it becomes a free edition.

During the evaluation period ADSelfService Plus will provide mail and phone support.

How ADSelfService Plus Works

ADSelfService Plus is a Web Based Self service solution to allow domain users to reset their forgotten passwords or unlock locked out accounts from a web browser without the intervention of an administrator. The below topics will help one understand the principle and Working of ADSelfService Plus.

- [ADSelfService Plus Working Principle](#)
- [Components of ADSelfService Plus](#)

ADSelfService Plus Working Principle

To use ADSelfService Plus for Password Reset, all domain users must enroll into ADSelfService Plus by logging into ADSelfService Plus Web Portal, and define answers for administrator / self defined challenge questions. Any enrolled domain user can reset his or her own password, by answering the defined challenge questions that were enrolled. ADSelfService Plus validates the domain user for password reset by comparing both the answers mentioned above.

Once the user is validated as an enrolled user, ADSelfService Plus accepts the new password provided by him / her and will contact the Active Directory to reset the user password. ADSelfService Plus must be provided with domain administrator credentials in-order to access the Active Directory for performing self service functions.

The challenge questions will be of the type :Who was your Childhood Hero? What is the name of your favorite TV Show? etc.,

Components of ADSelfService Plus

ADSelfService Plus is a Web Based Self Service Password Reset, Account Unlock and Active Directory Self Update solution. The product has two portals

1. ADSelfService Plus Admin Portal.
2. Domain User Web Portal.

ADSelfService Plus Admin Portal

The Admin Portal of ADSelfService Plus is used by the system administrator to install, manage, configure and monitor the ADSelfService Plus GINA and also configure settings. From the Admin portal a system administrator can also extract reports on Account Status and Password Status from the Active Directory.

An Administrator by logging into the Admin Portal of ADSelfService Plus will be able to

- Configure Domains
- Configure Policies
- Configure other General Settings.
- Install "ADSelfService Plus GINA" on all client machines and maintain them.
- View Reports on Enrollment, Configured Policies, ADSelfService Plus GINA Installation Status, AD Password / Account Status Reports and more.





Configuring Domains on ADSelfService Plus

During startup, ADSelfService Plus adds all the domains that could be discovered. If you wish to add more domains or modify the added domains, you can do it from here.

To add more domains, follow the steps below:

- Click the Domain Settings link from the client to open the Domain Settings page.
- The domains that are already added are listed here. Click the add new domain link to open the Add Domain Details dialog.
- Specify the Domain Name.
- Click ADD link to add the Domain Controllers. ADSelfService Plus will try to discover the domain controllers from the DNS and add. Else, add all the domain controllers manually. The domain controller that appears first in the list is considered as the primary domain controller. Use the up and down arrows to move the added domain controllers in the order of priority.
- Specify the authentication details of the user as which the domain controller will be contacted.
- Click Save to add the domain.

You can perform the following actions from here:

- **Default Domain:** The domain that is first discovered is considered as default domain. The default domain is shown in bold letters. Delegating security roles can only be done to the security principals of the default domain. If you wish to change the default domain, click the  icon from the action column to make it default.
- **Modifying Domain:** To modify the domain details, click the  icon and change the required values and save.
- **Deleting a Domain:** To delete a domain, click the  icon.
- **Refreshing the Domain Details:** To synchronize the object details with the Active Directory, click the  icon.

While adding new domains, the user name and password provided will be used for management and report purpose in the product.

The user entered in the domain settings should have the privilege to perform a management operation. Read only privilege is sufficient for a users to view reports.

The first domain controller will be contacted first if it turns unsuccessful then the next domain controller in the order will be contacted.

Dashboard

The Dashboard of ADSelfService Plus provides you with Information on all the Domains that are configured in ADSelfService Plus (See how to configure Domains)

It provides latest information on the following

- Locked Out Users
- Soon-To-Expire Password Users
- Password Expired Users

This information provides a snapshot on the latest information in your DB.

Also Audit Reports are also present on your Dashboard.

The Audit Reports Include

- Reset Password Report
- Unlocked Report
- Self Update Report

Links are provided at every box to provide you with a detailed report on all of the reports present in your Dashboard.

Reports

The Reports Tab provides you with detailed information on all reports that can be generated with ADSelfService Plus.

General Reports

- LockedOut Users
- Soon-To-Expire Password Users
- Password Expired Users

Audit Reports

- Reset-Password-Audit-Report
- Unlock-Audit-Report
- Self-Update-Audit-Report

General Reports

The General Reports of ADSelfService Plus include Reports on

- LockedOut Users
- Soon-To-Expire Password Users
- Password Expired Users

LockedOut Users

View the user accounts that have been locked out based on Account Lockout policy.(how to configure Account Lockout policy in ADSelfService Plus).

How it Works:

To generate a report on the users whose accounts have been locked you can follow the below steps

- Click on the Reports Tab -->>LockedOut Users
- Select Domain -->> Click on **Add OU** link if you want to generate report specific to an OU.
- Click on “Generate” button.
- The list of All user Accounts which are LockedOut is displayed as a report.

What can I do with this report:

- View details of 25 to 100 users in a single page by selecting from **show per page**
- View **Date & Time** when report generated
- Add or Remove columns to the Report -By clicking on **Edit Column** link
- Make a **Quick Search** on specific users
- **Schedule Reports** for the LockedOut Users.
- View **Description** on what the report shows
- **Export** the Reports as a CSV, PDF, HTML, XLS and CSVDE formats.
- **Print** the Report.

Soon-To-Expire-Password-Users

View the users whose passwords will expire in another n days.

How it Works:

To generate a report on the Soon-To-Expire-Password-Users you can follow the below steps

- Click on the Reports Tab -->> Soon-To-Expire-Password-Users
- Select Domain -->> Click on Add OU link if you want to generate report specific to an OU.
- Input users whose passwords to be expired in ___ days in the box provided.
- Click on "Generate" button.

The list of All Soon-To-Expire-Password-Users in 'n' days is displayed as a report.

What can I do with this report:

- View details of 25 to 100 users in a single page by selecting from **show per page**
- View **Date & Time** when report generated
- Add or Remove columns to the Report -By clicking on **Edit Column** link
- Make a **Quick Search** on specific users
- **Schedule Reports** for the Soon-To-Expire-Password-Users.
- View **Description** on information present in the report.
- **Export** the Reports as a CSV, PDF, HTML, XLS and CSVDE formats.
- **Print** the Report.

Password-Expired-Users

View the users whose passwords had expired.

How it Works:

To generate a report on the Password-Expired-Users you can follow the below steps

- Click on the Reports Tab -->> Password-Expired-Users
- Select Domain -->> Click on **Add OU** link if you want to generate report specific to an OU.
- Click on "Generate" button.

The list of All Password-Expired-Users is displayed as a report.

What can I do with this report:

- View details of 25 to 100 users in a single page by selecting from **show per page**
- View **Date & Time** when report generated
- Add or Remove columns to the Report -By clicking on **Edit Column** link
- Make a **Quick Search** on specific users
- **Schedule Reports** for the Soon-To-Expire-Password-Users.
- View **Description** on information present in the report.
- **Export** the Reports as a CSV, PDF, HTML, XLS and CSVDE formats.
- **Print** the Report.

Audit Reports

Audit Reports of ADSelfService Plus include

- Reset-Password-Audit-Report
- Unlock-Audit-Report
- Self-Update-Audit-Report

Reset-Password-Audit-Report

The Reset Password Audit Report provides a complete insight of the list of users who have reset their password.

How it Works:

To generate the Reset Password Audit Reports, you can follow the steps given below:

- Click on the Reports Tab -->>Reset Password Audit Reports
- Select the Start Date (from when you want the report to be generated).
- Select the End Date (till when you want the report to be generated).
- Click on “Generate” button.

The list of all users who have reset their password is displayed as a report.

UnLock-Audit-Reports

The UnLock Audit Report displays the list of users who had unlocked their Locked out accounts in the specified time period.

How it Works:

To generate the UnLock Audit Reports, you can follow the steps given below:

- Click on the Reports Tab -->>UnLock Audit Reports
- Select the Start Date (from when you want the report to be generated).
- Select the End Date (till when you want the report to be generated).
- Click on “Generate” button.

The list of all users who had unlocked their password in the specified duration is displayed as a report.

Self-Update-Audit-Reports

The Self-Update Audit Report displays the list of users who had updated their personal details in the Active Directory in the specified time period.

How it Works:

To generate the Self Update Audit Reports, you can follow the steps given below:

- Click on the Reports Tab -->>Self Update Audit Report
- Select the Start Date (from when you want the report to be generated).
- Select the End Date (till when you want the report to be generated).
- Click on “Generate” button.

The list of all users who had updated their personal details in the Active Directory in the specified period is displayed as a report.

Enrollment Reports

Enrollment Reports of ADSelfService Plus include:

- Enrolled Users Report
- Un-Enrolled-Users-Report

Enrolled Users Report

The Enrolled Users Report provides information of the list of users who have enrolled for the Secret Q & A.

How it Works:

To generate the Enrolled Users Reports, you can follow the steps given below:

- Click on the Reports Tab -->>Enrolled Users Report
- Select the Domain from the given list.
- Click on the Add OUs link to select specific OUs in the Selected Domain.
- Click on “Generate” button.

The list of all users who have enrolled for the Secret Q & A is displayed as a report.

Un-Enrolled Users Report

The Un-Enrolled Users Report provides information of the list of users who have **not** enrolled for the Secret Q & A.

How it Works:

To generate the Enrolled Users Reports, you can follow the steps given below:

- Click on the Reports Tab -->>Un-Enrolled Users Report
- Select the Domain from the given list.
- Click on the Add OUs link to select specific OUs in the Selected Domain.
- Click on “Generate” button.

The list of all users who have not enrolled for the Secret Q & A is displayed as a report.

Admin

The Admin Tab is divided into two important categories based on functionality.

- [Policies Configuration](#)
- [General Settings Configuration](#)

Policies Configuration :

Policies Configuration deals with various policy settings that the administrator can configure with ADSelfService Plus for a end user.

Policy Settings Configuration Include

- Reset Password Policy Configuration
- Unlock Policy Configuration
- Self Update Policy Configuration
- Question and Answer Settings (Secret Questions)
- Enrollment Settings
- Schedule Reports Configuration

General Settings Configuration

General Settings Configuration deals with the General Configurations the administrator can configure with ADSelfService Plus.

General Settings Configuration Include

- Logo Customization
- Custom Attributes Configuration Settings
- NT Service
- Connection (Port Settings)
- Server
- Personalize Settings

Policies Configuration

Policies Configuration deals with various policy settings that the administrator can configure with ADSelfService Plus. The policy settings configured are applied to all users in a selected Domain or Organizational Unit (OU). Any number of Self Service Policies can be configured and the configured policies are listed under "Available Policies" with the name specified.

Self Service Policy Configuration Settings include the combination of one or all of the below.

- Reset Password Settings Configuration
- UnLock Policy Configuration
- Self Update Policy Configuration
- Change Password Configuration

In this page we discuss

1. Adding a New Self Service Policy
2. Modifying an existing Self Service Policy
3. View details of a Policy Configured
4. Deleting a Policy


Adding a New Self Service Policy

To Add a New Self Service Policy

1. Click on Admin -->> Policy Configuration.
2. Click on the link "Add New Policy".
3. Enter the Policy Name in the Box highlighted.
4. Select one or all of the Policy Configurations highlighted above
5. Click on 'Select OU's button to select the OU's (Organizational Units).
6. Click on "Next"
7. If "**Allow Self Reset Password**" or "**Allow Self Unlock Account**" under "Advanced" Configuration for "Reset Password" or "Unlock Policy" respectively have been selected. Clicking on the "Next" button will take to the "Question and Answer Settings" Page.
8. Else Click on the "Finish" button.
9. Once the Question and Answer Settings are configured by inputting corresponding values.
10. Click on Finish
11. "Successfully Added" message is displayed.
12. The Policy will be saved under "Available Policies" and its details are listed.

Modifying a Self Service Policy

To Modify a Self Service Policy

1. Click on Admin -->> Policy Configuration.
2. Click on the  Modify Icon

3. Rename the "Policy" by clicking on the Policy Name.
4. Edit one or all of the Policy Configurations by adding or removing a check against them.
5. Click on 'Select OU's button to modify the OU's selected or to select a different OU (Organizational Units).
6. Click on "Next"
7. If "**Allow Self Reset Password**" or "**Allow Self Unlock Account**" under "Advanced" Configuration for "Reset Password" or "Unlock Policy" respectively have been selected. Clicking on the "Next" button will take to the "Question and Answer Settings" Page.
8. Else Click on the "Finish" button.
9. The values input under the "Question and Answer Settings" Page can be edited to re-configure the settings.
10. Click on Finish
11. "Successfully Updated" message is displayed.
12. The Modified Policy will be displayed under "Available Policies" and the changed details are listed.

Viewing Details of a Self Service Policy Configured

Any number of Self Service Policies can be configured with ADSelfService Plus "Policy Configuration" option and are displayed under

1. Admin -->>Policy Configuration -->> Available Policies

The Policy Name the configured domain and details of each policy configured are highlighted.


Details on

- Reset Password Policy
- Unlock Policy
- Self Update Policy and
- Change Password Policy

are set or not is tabulated and displayed with a true or false against each of them.

Deleting a Policy

Any number of Self Service Policies can be configured with ADSelfService Plus "Policy Configuration" option and are displayed under

1. Admin -->>Policy Configuration -->> Available Policies
2. Click on  icon to delete one or more of the available policies

Reset Password Configuration

The Reset Password configuration settings allows the administrator to configure different password reset options. He can configure one or all of the options below while password reset. This can be done by adding or removing the check mark against the options.

Reset Password Options Include

- Use Secret Questions
- Reset Automatically

Administrators can also force end users to Change Password at Next Logon after Password Reset has been done by one or both the options provided above.

Use Secret Questions

This feature allows an end-user to reset their own password by answering secret questions which were configured during enrollment. The administrator can configure the exact number of questions, question types and the questions to be answered by an end-user in-order to reset his password.

How to Configure Password Reset by Using Secret Questions?

1. Click on Admin -->> Policy Configuration
2. Click on "Add New Policy" Link
3. Enter the Policy name in the highlighted box
4. Provide a Check against "Reset Password" under Policy Configuration.
5. Provide a Check Against the "**Allow Self Reset Password**" option provided.
6. Click on "Select OU's" button
7. Select Domain from the Drop Down.
8. Provide a check against one or more desired OU's (From the Tree View or List View)
9. To select the entire domain provide a check against the domain
10. Click on Next to Configure "Secret Question and Answer Settings"
11. Input the Desired Values in the Boxes provided.
12. Click on Finish

Secret Question and Answer Settings

The administrator can set the below limits while configuring secret Questions or Answers.

1. Maximum and Minimum length for a question.
2. Maximum and Minimum number of questions a user can enter.
3. Maximum and Minimum length of an answer.
4. Number of User Defined Questions.
5. Number of Selectable Questions.
6. Display or not to Display the 'Answers' in Plain Text.

Thus the secret questions are configured for a user to answer while password reset.

Automatic Reset Password Configuration:

An administrator can schedule a report on "**Password Expired users**" and configure ADSelfService Plus to automatically reset the passwords of all the **Password Expired users**. ADSelfService Plus automatically resets the passwords of password expired users to a **default password value**. The Administrator can modify/change the default password value for the users whose passwords are reset.


This can be done by providing a check against the "**Automatic Reset Password**" CHECKBOX provided.


1. Click on Admin -->> Policy Configuration
2. Click on "Add New Policy" Link
3. Enter the Policy name in the highlighted box
4. Provide a Check against "Reset Password" under Policy Configuration.
5. Provide a Check Against the "**Automatic Reset Password**" option provided.
6. Enter a desired **password value** in the "TextBox" Provided within the %% symbols.
7. Select the Schedule to run a report on Password Expired Users
8. Time of Day from the Drop Down and Frequency of the Report from any of the Radio Buttons (Daily, Weekly, Monthly or Hourly)
9. Click on "Select OU's" button
10. Select Domain from the Drop Down.
11. Provide a check against one or more desired OU's (From the Tree View or List View)
12. To select the entire domain provide a check against the domain
13. Click on "Finish"

Changing the Default Password Value

On enabling **Automatic Reset Password** a "**Text Box**" appears with a default password value as **%logonName%**. The default password value can be changed to a desired value. The desired value can include one or more of the below supported attributes.

Eg: **%logonname%** can be replaced by **%sn%**

	Supported Attributes for Password value while Automatic Reset Password. { "givenName" , "sn" , "initials" , "displayName" , "userPrincipalName" , "sAMAccountName" , "name" , "mail" , "distinguishedName" }
---	---

	Note: To schedule the reset time for "Automatic Password Reset" click on " Schedule the Reset time " link below " Automatic Reset Password " CHECKBOX to schedule reset time based on Password Status Reports in ADSelfService Plus.
---	--

Change Password at Next Logon

The administrator can force all his domain users to "Change Password at Next Logon" after a password reset. This will force users to change their passwords when they login after a reset password is done using ADSelfService Plus.

To enable "Change Password at Next Logon"

- Click on Admin -- >> Policy Configuration
- Click on "Reset Password" under Policy Configuration
- Select "Allow Self Reset Password" or "Automatic Reset Password"
- Provide a Check Against the "**Change Password at Next Logon**" option provided.
- Follow the wizard to complete Self Reset Password or Automatic Reset Password.
- This will enforce a Change Password at Next Logon after a Password Reset.

Unlock Policy Configuration

The Unlock Policy configuration settings allows the administrator to configure different unlock account options. He can configure one or all of the options below while account unlock. This can be done by adding or removing the check mark against the options.

Account Unlock Options Include

- Use Secret Questions
- Unlock Automatically

Administrators can also force end users to Change Password at Next Logon after an Account Unlock has been done by any of the options provided above.

Use Secret Questions

This feature allows an end-user to unlock their own account by answering secret questions which were configured during enrollment. The administrator can configure the exact number of questions, question types and the questions to be answered by an end-user in-order to reset his password.

How to Configure Account Unlock by Using Secret Questions?

1. Click on Admin -->> Policy Configuration
2. Click on "Add New Policy" Link
3. Enter the Policy name in the highlighted box
4. Provide a Check against "Unlock Policy" under Policy Configuration.
5. Provide a Check Against the "**Allow Self Unlock Account**" option provided.
6. Click on "Select OU's" button
7. Select Domain from the Drop Down.
8. Provide a check against one or more desired OU's (From the Tree View or List View)
9. To select the entire domain provide a check against the domain
10. Click on Next to Configure "[Secret Question and Answer Settings](#)"
11. Input the Desired Values in the Boxes provided.
12. Click on Finish

Secret Question and Answer Settings

The administrator can set the below limits while configuring secret Questions or Answers.

1. Maximum and Minimum length for a question.
2. Maximum and Minimum number of questions a user can enter.
3. Maximum and Minimum length of an answer.
4. Number of User Defined Questions.
5. Number of Selectable Questions.
6. Display or not to Display the 'Answers' in Plain Text.

Thus the secret questions are configured for a user to answer while Account Unlock.

Automatic Unlock Configuration

An administrator can schedule a report on "**Locked Out Users**" and configure ADSelfService Plus to automatically unlock all the **Locked Out Accounts**.

This can be done by providing a check against the "**Automatic Reset Password**" CHECKBOX provided.

1. Click on Admin -->> Policy Configuration
2. Click on "Add New Policy" Link
3. Enter the Policy name in the highlighted box
4. Provide a Check against "Reset Password" under Policy Configuration.
5. Provide a Check Against the "**Automatic Unlock**" option provided.
6. Select the Schedule to run a report on Password Expired Users
7. Time of Day from the Drop Down and Frequency of the Report from any of the Radio Buttons (Daily, Weekly, Monthly or Hourly)
8. Click on "Select OU's" button
9. Select Domain from the Drop Down.
10. Provide a check against one or more desired OU's (From the Tree View or List View)
11. To select the entire domain provide a check against the domain
12. Click on "Finish".

Self Update Policy Configuration

Self Update Portal enables end users to view and update their own Information in Active Directory without the intervention of the Administrator.

The Update information is categorized under User Profile, Account Details, Contact Details, Exchange Server and Terminal Services Details. A users who logs into Self Service Portal can modify the value of any of the fields that an administrator has configured for self update.

Administrators can provide controlled access to one or more of all the attributes from the above listed fields for an end user to self update. This is configured in the Self Update Policy Settings. Self Update can be restricted not only to fields but also to within a selected OU.

How to Configure Self Update Settings?

1. Click on Admin -->> Policy Configuration
2. Click on "Add New Policy" Link
3. Enter the Policy name in the highlighted box
4. Provide a Check against "Self Update" under Policy Configuration.
5. Click on the "Select Attributes Link" and provide a Check against attributes needed for a Self Update.
6. Click on "Select OU's" button (To Self Update information only for a selected OU)
7. Select Domain from the Drop Down.
8. Provide a check against one or more desired OU's (From the Tree View or List View)
9. To select the entire domain provide a check against the domain
10. Click on Finish

These will Configure Self Update Settings for an End User to Update.

Configure a Change Password Option

Change Password

Configuring a Change Password facility allows end users the option to change their own passwords by logging in into ADSelfService Plus web portal.

To Configure Change Password option for users in a Organizational Unit:

1. Click on Admin -->> Policy Configuration
2. Click on "Add New Policy" Link
3. Enter the Policy name in the highlighted box
4. Provide a Check against "Change Password" under Policy Configuration.
5. Select Domain from the Drop Down.
6. Click on "Select OU's" button
7. Provide a check against one or more desired OU's (From the Tree View or List View)
8. To select the entire domain provide a check against the domain
9. Click on "Finish"

This allows end users in the selected OU's of the domain to change their own passwords by logging in into ADSelfService Plus web portal.

Enrollment Settings

ADSelfService Plus facilitates an administrator to notify one or all his users by email to enroll into the application and perform self service functions. To facilitate inviting users for enrollment the administrator must configure enrollment settings.

Enrollment Settings Include

- Notify Users by selecting their "Domain / OU".
- Notify Users by Selecting the "Self Service Policy Configured" in ADSelfService Plus.
- Notifying Users by Typing their "Email addresses".

Notify Users by selecting their Domain /OU :

Before notifying users by selecting their Domain or OU the administrator must Configure a mail server.

Steps to Notify users by selecting their Domain or OU.

- Click on "admin" -->"enrollment settings"
- Select a "**Domain**" from the pull down menu.
- To select an OU within a Domain click on "**Add OU**" link and select one or more OU's from the Pop Up by providing a check against the OUs and close the Pop-Up Window.
- Enter your mail content in the Text box provided.
- Click on Send Mail to send emails to all users in the Domain / OU.

The message typed can be modified by the administrator as desired. The administrator can select one or more of the below supported attributes (Naming Formats) while addressing a user when mailing users through a configured mail server.

To address a user the administrator has to change the variable held within the % symbol.

Eg: %**user**% can be replaced by %**sn**%

Also multiple instances of supported attributes in the message, is supported while notifying users.

Eg: **FirstName_LastName** can be specified as %**initial**%_%**sn**%



Supported Attributes while notifying users

```
{"givenName", "sn", "initials", "displayName", "userPrincipalName",
"sAMAccountName", "name", "mail", "distinguishedName" }
```

Notify Users by Selecting the "Self Service Policy Configured" in ADSelfService Plus.

To notify users based on the Self Service Policy OU settings Configured

- Click on "admin" Tab --> "Enrollment Settings" to the left of the page
- Select a "Policy Name" from the pull down menu under Policies.
- Input the email address for the user notification is to be sent. (For multiple users separate each email address with a "," (comma)
- Type the email address of the user in the Text Box provided.
- Enter your mail content
- Click on Send Mail to send an email to the individual.



Each Self Service Policy can include one or more selected OUs in a Domain. Check how to Configure a Self Service Policy in ADSelfService Plus.

Notify Users by typing their Email addresses :

To notify an individual by email for enrollment

- Click on "admin" Tab -->> "Enrollment Settings" to the left of the page
- Select a "Type email address" from the pull down menu under Manual.
- Input the email address for the user notification is to be sent. (For multiple users separate each email address with a "," (comma)
- Type the email address of the user in the Text Box provided.
- Enter your mail content
- Click on Send Mail to send an email to the individual.



For users who are notified for enrollment using their email addresses, the text message in the email will be addressed using the default %user%. Other attributes are not supported.

Question and Answer Settings

Question and Answer Settings of ADSelfService Plus allows the administrator to limit / allow question and answer options for end user enrolment. The administrator can define different question and answers settings under the Advanced option under Reset password and Unlock Account Configurations.

- Accessing Question and Answer Settings
- Question Settings
- Answer Settings

Accessing Question and Answer Settings

A workflow is followed to access the question and answer settings. ADSelfService Plus has followed such a workflow to access "Question and Answer Settings" based on OUs. OU based Question and Answer Settings for Password Reset and Account Unlock.

The Question and Answer Settings will be common for any created OU Based Password Reset / Account Unlock Policy Configured.

- Admin -->> Policy Configuration -->> Reset Password -->>Select OUs -->>Question and Answer Settings.
- Admin -->> Policy Configuration -->> Unlock Account -->> Select OUs -->> Question and Answer Settings.

Question Settings

The question Settings include the following options

1. Set the number of predefined questions

This is the list of questions that the administrator has already framed to provide to his end-users.

End users when they are to enrol into ADSelfService Plus will be able to select any of the questions from the list that appears from the Pull Down Menu while enrolment.

This option deals with the number of questions that appear in the pull down while enrolment.

2. Number of User-Defined Questions

The user will be able to frame their own personal questions with ADSelfService Plus end-user portal while enrolment. The maximum number of questions that an end-user can frame by himself for him to answer.

Add / View User Defined Questions:

An administrator can add any number of desired questions using this option. He / She can Add or Delete any number of Questions of Preference by using the Add and Delete option respectively.

3. Minimum Question Length

The administrator can set the minimum characters that can be input while framing a question.

4. Maximum Question Length

The administrator can set the maximum characters that can be input while framing a question.

Answer Settings

1. Minimum Answer Length

The administrator can set the minimum characters that can be input while a user is framing an answer for a question.

2. Maximum Answer Length

The administrator can set the Maximum characters that can be input while a user is framing an answer for a question.

3. Don't display 'Answer' in plain text

On checking this option the Answers entered by a user while password reset using ADSelfService Plus Self Service Portal will be in an encrypted form.

Import Answers

ADSelfService Plus offers the facility to import answers for users in bulk via a CSV file import. This facilitates auto enrollment of users for Reset Password and Unlock Account options. The following steps will guide you through the import process.

To Import answers for Auto Enrollment,

1. Click on the **Admin** tab.
2. Select the **Import Answers** link under Policies. This opens the 'Import Answers' Dialog.
3. Select the Domain from the given list.
4. Select your choice of Question from list or as the one stored in your database.
5. Click on Browse and import the CSV file containing the details of the users and their respective answers.(For more details, refer to the sample CSV file)
6. Enable **Overwrite Users' Q & A** checkbox if you want the CSV file values to override the user specified ones.In case you want to retain User specified values, leave the checkbox unchecked.
7. Click on **Save** to complete the 'Import Answers' process.

Configure Report Scheduler

Schedule Reports generated on Soon to Expire Password Users and Password Expired Users and Account Locked Out Users with ADSelfService Plus.

ADSelfService Plus allows to Schedule Reports for

- Soon to Expire Password Users

Configure Report Scheduler for Soon to Expire Password Users

With ADSelfService Plus the administrator will be able to schedule reports for Soon to Expire Password Users in his Domain.

In-order to Schedule Reports for Soon to Expire Password Users the administrator has to configure settings on when the reports are to be scheduled and preset a time when the LockedOut Users report is to be scheduled.

1. Click on Admin Tab --->> Schedule Reports
2. Select the Domains --->>Choose the OU
3. From the Pull Down List select "Soon to Expire Password Users"
4. Select the number of days for Password to be expired.
5. Select the Option from the buttons provided to Schedule LockedOut Users Report
 - **Daily AT** - Specify time of Day
 - **Weekly ON and AT** - Specify the day of week and time of the day
 - **Monthly ON and AT** - Specify Date and Time
 - **Hourly EVERY** - Specify the reports to be scheduled in every *** hrs.

Once this configuration is set. ADSelfService Plus runs a report on Soon to Expire Password Users as per Scheduled Time.

Enable Password Expiry Notification:

ADSelfService will be able to send e-mail notification to all members enrolled in ADSelfService Plus to notify them on a Soon To Expire Password.

ADSelfService Plus sends a message on password expiry notification with a preset Subject and Message that is configured by the administrator.

While sending a password expiry notification to Domain Users. The notification message can be changed as desired by the administrator. Also the administrator can email a user either by his "initials", "displayName" or any of the below supported attributes.

This can be done by Replacing the variable held within the % symbol with a desired variable.
Eg: %user% can be replaced by %sn%

Also multiple instances of supported attributes in the message, is supported while notifying users.

Eg: **FirstName_LastName** can be specified as %initial%_%sn%



Supported Attributes while notifying users

```
{"givenName", "sn", "initials", "displayName", "userPrincipalName",  
"sAMAccountName", "name", "mail", "distinguishedName" }
```

Schedule Reports on Locked Out Users and Password Expired Users :

Reports on Locked Out Users and Password Expired Users are configured during Self Service Policy Configuration. Check how to schedule reports on Locked Out Users and Password Expired Users.

ADSelfService Plus GINA / Credential Provider

- ADSelfService Plus GINA / CP
- How to Install ADSelfService Plus GINA / CP on Client Machines
- Domain Users Reset Password / Unlock Account using ADSelfService Plus GINA / CP

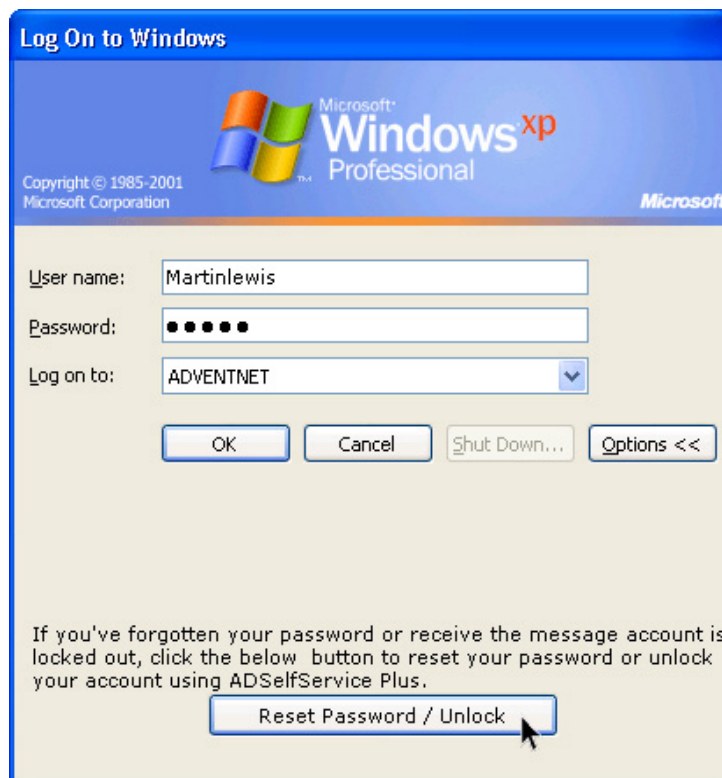
ADSelfService Plus GINA / CP

ADSelfService Plus GINA/ CP is a client side self-service application that provides the ability for end-users to reset their own password or to unlock their own account without the involvement of Administrator or any help desk technicians. It is done through a simplified, web based portal and it is integrated with the CTRL + ALT + DEL screen (simply known as CAD screen or Winlogon screen).

ADSelfService Plus GINA supports Windows XP, Windows 2000 and Windows 2003 Server. ADSelfService Plus Credential Provider supports Windows Vista. Both will extend the Winlogon screen with a button "Reset Password/ Unlock".

Any user can access the ADSelfService Plus web portal to self reset his own password by clicking on the "Reset Password / Unlock" button on the "Windows Logon Screen Extension" installed.

ADSelfService Plus GINA and Credential Provider Extensions for Password Reset on Windows



XP and Vista Machines

Fig1 : ADSelfService Plus GINA for Windows XP

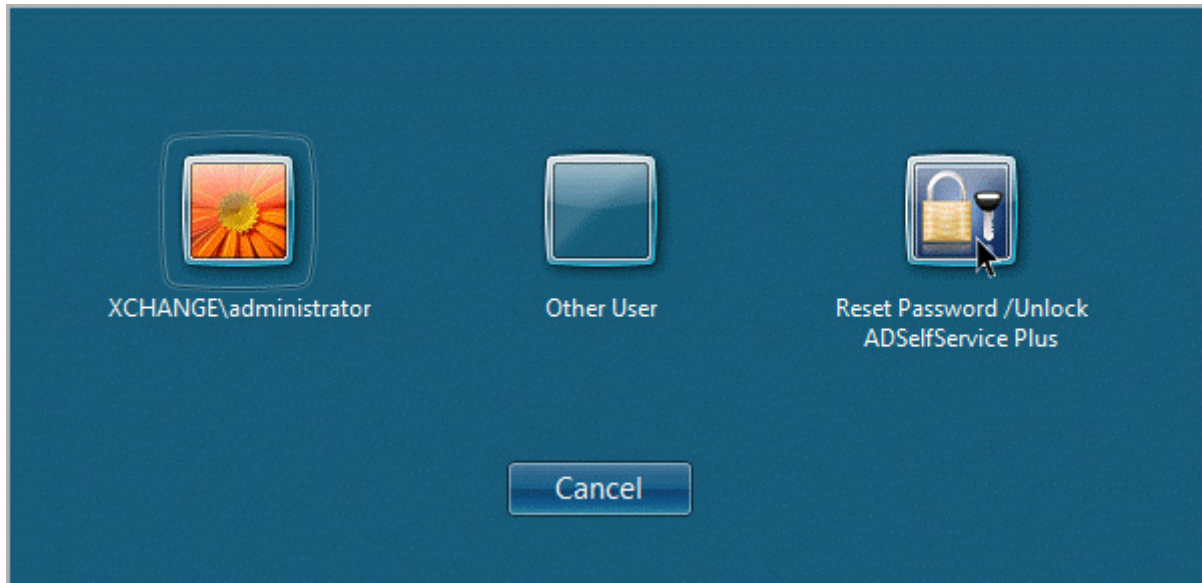


Fig2: ADSelfService Plus Credential Provider for Windows Vista

The Admin Console of the ADSelfService Plus Web Portal also provides the status of the "Windows Logon Extension" installation. This feature to include "ADSelfService Plus GINA" extension on client machines is possible only with the Professional edition of ADSelfService Plus. Detailed information on

1. User machines on which the Windows Logon Extension is to be Installed.(ADSelfService Plus GINA / CP yet to be installed machines) .
2. User machines on which the Windows Logon Extension is installed. (i.e.)ADSelfService Plus GINA / CP installed machines.
3. Error occurred machines while installation.

This facilitates easy installation, re-installation and un-installation of the Winlogon Extension.

Installation of ADSelfService Plus GINA / CP on Client Machines:

- Installation of ADSelfService Plus GINA / CP on client machines
- Reversal of Changes made while ADSelfService Plus Client Software Installation
- Information available on the Admin Console of ADSelfService Plus

Installation of ADSelfService Plus GINA/CP on client machines

Installation of "ADSelfService Plus GINA" on client machines to facilitate password reset from the Winlogon Extension is available only with the Professional Edition of ADSelfService Plus. ADSelfServicePlusClientSoftware.msi will install the ADSelfService Plus GINA/CP on client machines. The client software is a small package that has information about the installation, uninstallation of ADSelfService Plus GINA/CP and also register the GINA/CP with winlogon. The msi is pushed and executed into the client machine automatically during the installation.

1. How to Install ADSelfService Plus GINA on one or all Client Machines.
2. [View all](#) ADSelfService Plus GINA Installed Machines.



For easy understanding **GINA** and **Credential Provider** are represented as **GINA** or **GINA Tool** in this document for the Winlogon Extension. We request the reader to substitute Credential Provider in case of a Windows Vista machine.

How to Install GINA on one or all Client Machines:

The GINA or Winlogon extension can be installed on a selected or the entire domain user's machines from a centralized ADSelfService Plus console in bulk or single. To install GINA or Winlogon extension one must login ADSelfService Plus by providing administrator credentials.

1. Install GINA on a Selected list of Client Machines in the Domain
2. New Installation of GINA on all client machines in the Organizational Unit (OU).

Install GINA on a Selected list of Client Machines in the Domain

1. Click on Admin -->GINA / CP Installation (Under "Policies")
2. Click on 'New Installation '
3. "Select Domain" from the Drop Down list
4. Click on "List All Computers" (The Complete list of Computers in the Domain where GINA is not yet installed is displayed a drop down allows to select the number of computers that are actually displayed in a single page".)
5. Select Computers from the list where GINA extension must be installed by providing a Check against the computer Names.
6. Click on Install (This will install the GINA extension on all the selected computers)



ADSelfService Plus also allows an administrator to Search for Specific Computer Names in a Domain using the Quick Search Option and Install GINA extension.

To Install GINA on the Entire list of Computers in the page, provide a check against the Header beside "Computer Name" and click on Install. This will install GINA extension on the list of **25, 50, 75 or 100** machines listed in the page.

New Installation of GINA on all client machines in the Organizational Unit (OU):

1. Click on Admin -->>GINA / CP Installation (Under “Policies”)
2. Click on “New Installation”
3. “Select Domain” from the Drop Down list
4. Click on “OU Based Filter”
5. Select “List View” to view the List of Organizational Units (OU’s) in the Domain.
6. The list view contains “OU Name” and “Location” of OU as the Header.
7. Administrator can perform a quick search to filter and find desired OUs.
8. Check against the desired “OU” and click on “Get Computers”
9. This will display the list of computers in the selected OU where GINA is to be installed.
10. Check against Computers and Click on Install.
11. This will install GINA on all the selected Computers.
12. The status of Installation will be displayed and Tick Symbol appears on successful Installation.
13. A wrong (Cross) symbol indicates an unsuccessful installation.

View all GINA Installed Machines:

Once GINA is installed it is important to know the Computer Names which GINA has been installed.

To list all “GINA Installed Machines” in the Domain

- Click on Admin -->> GINA / CP Installation -->>Installed Machines
- Select the Domain from the Drop Down.

This lists all the Computers in which GINA Tool is installed.

Reversal of Changes made while ADSelfService Plus Client Software Installation

If the ADSelfService Plus GINA/CP installed machines faces any issues during logon, either of the below steps revert the changes made in client machines.

1. Using our ADSelfService Plus Web console, you can uninstall GINA/CP on the corresponding machine. The uninstallation of GINA/CP automatically revert the changes made while installing the software on Client machines.
2. We also provide the Batch file, “Uninstall.bat” by which you can revert the changes from the remote machine.

Using ADSelfService Plus Web Console to Uninstall GINA / CP

1. Remove /Re-install GINA Tool from the List of Installed Machines.
2. View Error Occurred Machines while Installation.
3. Remove / Re-Install GINA from the List of Error Occurred Machines.

Remove / Re-install GINA Tool from the List of Installed Machines:

To Remove "ADSelfService Plus GINA" from an Installed Machine.

- View all GINA Installed Machines.
- To select a specific computer use the Quick Find option.
- Click on **Un-install** (This will remove the GINA Tool from all the Machines one selects from the list).
- Click in **Re-install** (This will re-install GINA on machines that require a fresh installation over the already installed machines or on machines where installation is partially completed but displayed under Installed Machines List.)

View Error Occurred Machines while Installation:

To View Error Occurred Machines while installing GINA

- Click on Admin --> GINA / CP Installation --> Error Occurred Machines --> Select the Domain from the Drop Down (This lists all the Machines which showed an error while trying to install GINA.)

The Computer Name, IP ADDRESS, Location of the Computer and the Reason for GINA not being installed on a computer is displayed.

Remove /Re-Install GINA from the List of Error Occurred Machines

- View the error occurred machines and re-install GINA by selecting computers for re-installation
- Click on **Un-install** (This will automatically remove the GINA Tool on the selected Machines / Computers available in the list of Error Occurred Machines where the installation process was interrupted or partially completed).
- Click on **Re-Install** (This will automatically re-install the GINA Tool on the selected Machines / Computers available in the list of Error Occurred Machines where the installation process was interrupted or partially completed).



To select a specific computer use the Quick Find option.

Installation Information available on the Admin Console of ADSelfService Plus

The Admin Console of the ADSelfService Plus Web Portal provides the status of the "Windows Logon Extension" installation. Detailed information on

- User machines on which the Windows Logon Extension is to be Installed.(ADSelfService Plus GINA / CP yet to be installed machines) .
- User machines on which the Windows Logon Extension is installed. (i.e.)ADSelfService Plus GINA / CP installed machines.
- Error occurred machines while installation.

This facilitates easy installation, re-installation and un-installation of the Winlogon Extension.

Users Reset Password / Unlock Account using ADSelfService Plus GINA / CP

Any domain user who has enrolled into ADSelfService Plus web console by answering validation questions can use the 'Forgot Password' extension (ADSelfService Plus GINA / CP extension) displayed on the Windows Logon Screen to Reset his password or Unlock his account.

1. An Enrolled Domain user when forgets his/her domain login password or domain account is locked-out can click on the "Ctrl + Alt + Del" button on his Windows machine. This opens the GINA extension or Winlogon extension on the login screen with a 'Reset Password / Unlock' button on the extension.
2. The user in-order to reset his forgotten password to a new password using ADSelfService Plus web console must click on the 'Forgot Password' Button on the Winlogon / GINA extension. The 'Forgot Password' link automatically directs the user to the 'Reset Your Password' Screen of ADSelfService Plus Web Console.
3. The User must enter his domain name and click on continue, this takes the user to the 'Security Questions' screen on the Web Browser.
4. He /She must answer the 'Security Questions' as per his/her enrollment profile and click on 'Continue'
5. The next screen is the 'Reset Password' Screen where the user enters his new password by conforming the password policy requirements that is displayed on the screen.
6. The password is reset to a new password that is set by the user and a successfully reset message appears.
7. The domain user can now use this new password to login into his domain. Kindly check the screen shots below for easy understanding of Password Reset with ADSelfService Plus GINA / CP.
8. This feature to for a user to access "ADSelfService Plus GINA" extension from their Winlogon Extension is facilitated only with the Professional edition of ADSelfService Plus.



GINA is installed Windows 2000 and XP Machines only. For Windows Vista Machines a Credential Provider model is installed which requires the same process for resetting the password as GINA tool.

Screen shots for better understanding of Password Reset / Unlock Account with ADSelfService Plus GINA / CP

GINA and Credential Provider Extensions for Windows XP and Windows Vista Machines Respectively



Fig.1. ADSelfService Plus GINA Extension For Windows XP

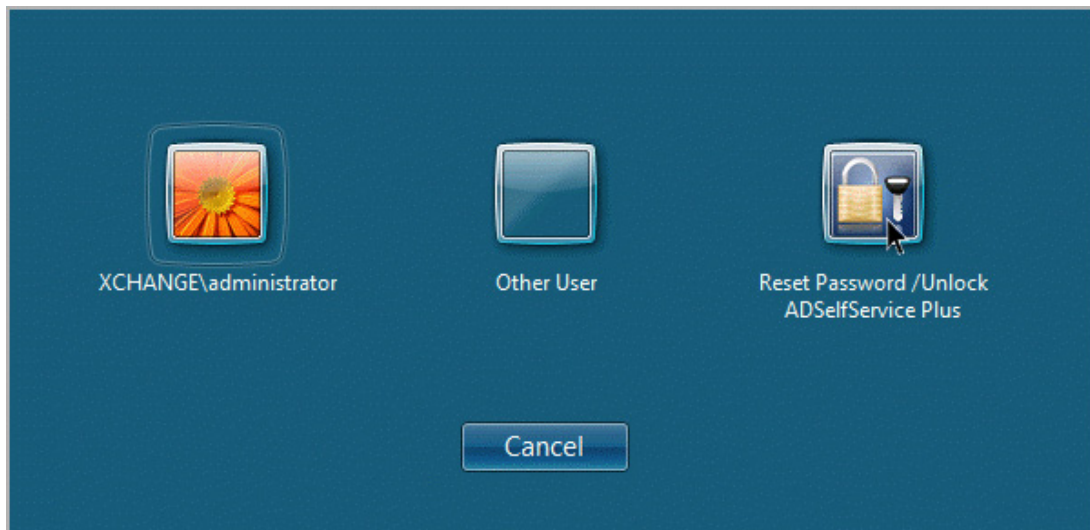


Fig.2. ADSelfService Plus Credential Provider extension for Vista

Reset Password and Unlock Account Selection in Windows XP and Windows Vista Machines Respectively

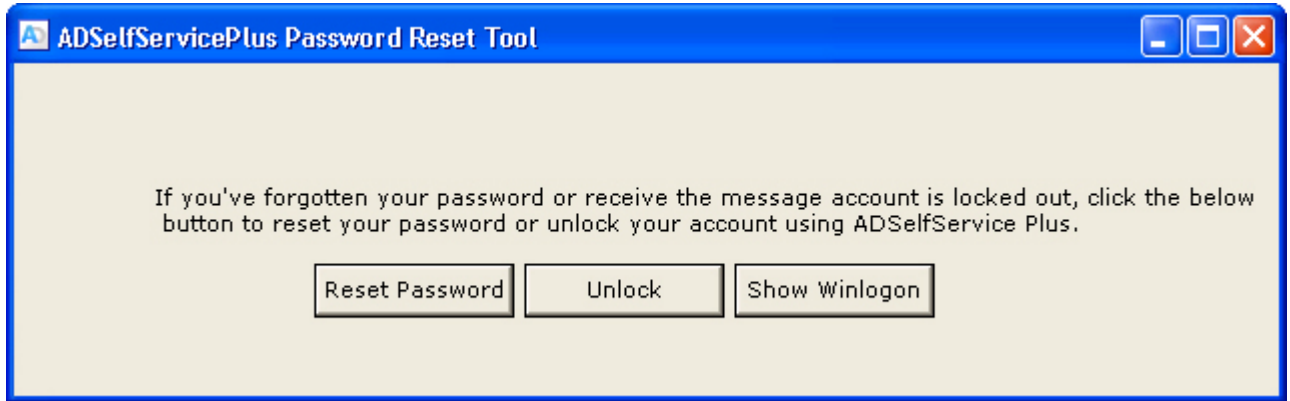


Fig.3. Selection of Reset Password and Unlock Account in Windows XP

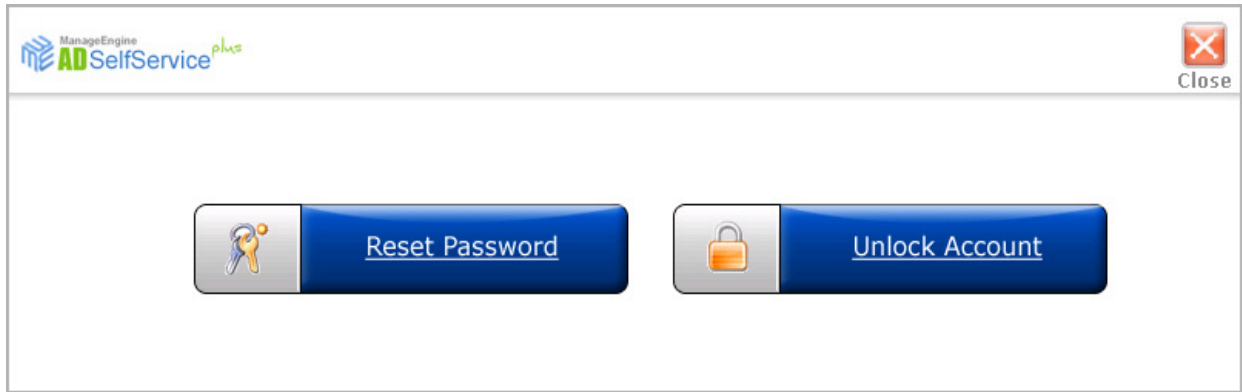


Fig.4. Selection of Reset Password and Unlock Account in Windows Vista

On clicking on the Reset Password / Unlock Account button provided above the user is connected to a Web Browser from where he can provide his Domain Name, Answer the Secret Questionnaire Reset his Password or Unlock his locked out account. Screen Shots are provided below.

Domain User Name Input for Reset Password / Unlock Accounts & Answering Security Questionnaire.

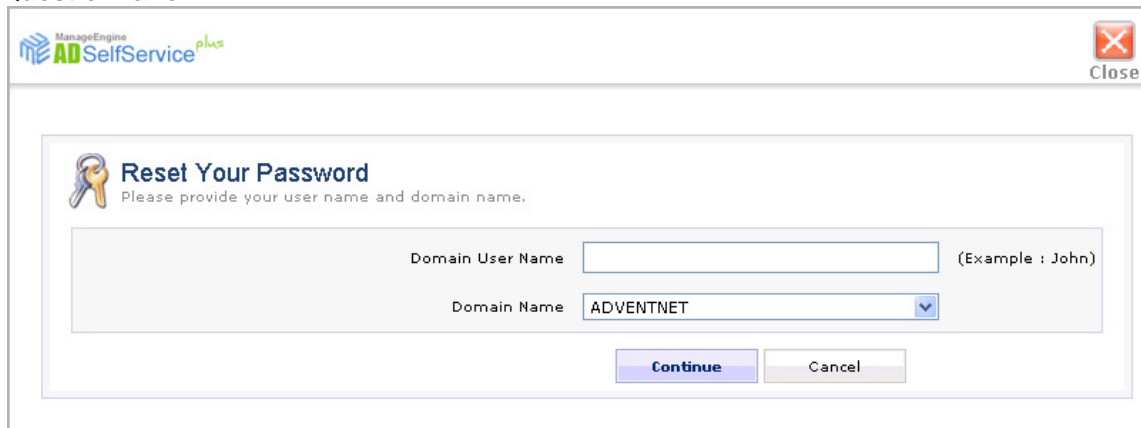


Fig.5. Entering Domain User Name to Reset Password

ManageEngine
ADSelfService plus

Unlock Your Account
Please provide your user name and domain name.

Domain User Name (Example : John)

Domain Name

Fig.6. Entering Domain User Name to Unlock Account

ManageEngine
ADSelfService plus

Security Questions
Please answer the following question as per your enrollment profile to reset your password.

What was the name of your elementary / primary school ?

What is your spouse's mother's maiden name ?

Fig.7. Answering Secret Questions

Reset Password and Account Unlock Screens

ManageEngine
ADSelfService plus

Reset Password
Please enter a new password in the boxes below:

Domain Password Policy Requirements

- ✓ Minimum Password Age : 1
- ✓ Maximum Password Age : 30
- ✓ Minimum Password Length : 7
- ✓ Password History : 3
- ✓ Password Complexity : Enabled

Reset Password

Password :

Confirm Password :

Fig.8. Enter the password to Reset

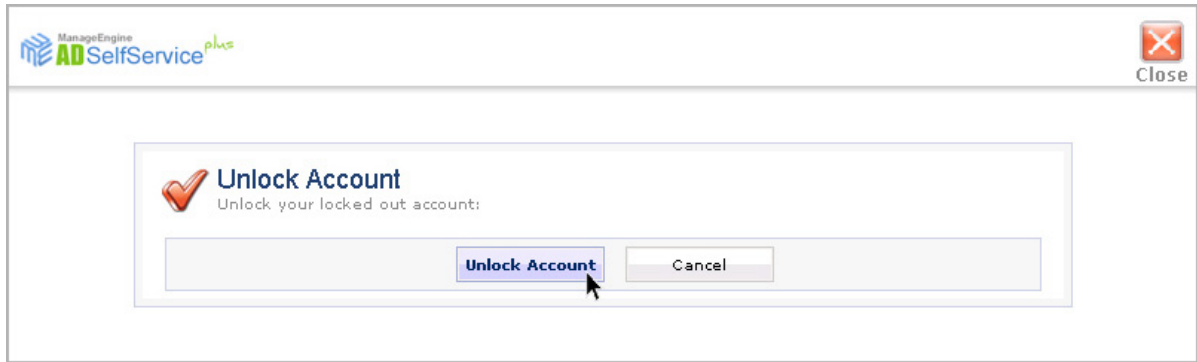


Fig.9. Unlock Account

General Settings

General Settings with ADSelfService Plus includes all the general settings which the administrator can set in ADSelfService Plus.

General Settings Include

- Customize Display Settings
- Custom Attributes Settings
- NT Service
- Connection
- Server
- Personalization Settings.

Customize Display Settings of ADSelfService Plus

Customize Display Settings of ADSelfService Plus

The Customize Display Settings option in ADSelfService Plus assists an administrator to customize one or more of the below display characteristics in the application.

- Change Image / Logo for Admin Users
- Change Image /Logo for Domain User
- Hide "Self Service Admin Login"
- Customize Password Policy messages
- Hide CAPTCHA (Word Verification Image)
- Edit Theme
- Customize messages at Reset Password /Unlock Account pages.

Change Image / Logo for Admin Users:

An administrator can replace the default ADSelfService Plus logo with his corporate logo or an image of his choice. The modified image present at the top left corner of the Application will then be viewed by all Self-Service Users.

To replace the default ADSelfService Plus logo

- Login ADSelfService Plus
- Click on the "Admin Tab"
- Click on Customize display Settings
- Click on "Browse" and provide a check against the "Change Image / Logo" box provided and select your corporate image or logo.
- Click on "Save" to save the changes.

Change Image / Logo for Domain Users

This will be enabled only when the administrator enables the "Hide Self-Service Admin Login" option.

The Default ADSelfService Plus logo or any existing image on the domain user login can be replaced by an image /logo of choice. This image will remain the same for all the domain users.

Substitution of the default logo for an end user login can be achieved in 2 ways:

- Replacing the existing logo present at

<installation directory>\webapps\adssp\images\blue\logo.gif

With any desired image of choice. (Use the save as option)

- Saving a new image and editing the file "DomainLogin.html"

Save the desired image at the below provided location

<installation directory>\webapps\adssp\images\blue

To replace the logo edit the file "DomainLogin.html" at the location provided below.

<installation directory>\webapps\adssp\html

The administrator can edit the html file "DomainLogin.html" by replacing the "logo.gif"

image with any other desired image "abc.gif" saved.

Save a Backup of the existing file "DomainLogin.html" before editing.

Hide "Self Service Admin Login"

ADSelfService Plus facilitates hiding the "Self Service Admin login" from being viewed by normal users.

To enable this option:

- Login ADSelfService Plus
- Click on Admin Tab
- Click on Customize display Settings
- Provide a check against the "Check Box" provided to Hide "Self Service Admin Login"
- Click on "Save" to save the changes.

How to customize the user login page layout?

To customize the user login page layout to your own settings, edit the "html" file at the location provided below,

<installation directory>\webapps\html\DomainLogin.html

(Note : Save a BackUp of the existing file **DomainLogin.html** before editing).

How to Access "Self Service Admin Login" Screen, after hiding it from normal users?

To Access "Self Service Admin Login" Screen, after hiding it from normal users,

- Right Click the ADSelfService Plus icon on the Task Bar of the installed machine.
- Click Start Client.

This will take the administrator to the "Self Service Admin Login" Screen.

Customize Password Policy messages

ADSelfService Plus allows customizing the subject matter on the "Domain Password Policy Requirements" box present in the Reset Password / Change Password pages.

To enable a custom password policy message

- Login ADSelfService Plus
- Click on Admin Tab
- Click on Customize display Settings
- Check against the "Check Box" provided to "Customize Password Policy messages"
- Click on Save to save the changes.



If the checkbox against "Customize Password Policy messages" is not checked the "Default Domain Password policy" will be displayed to the end-users when password reset or account unlock.

How to customize the subject matter on the "Domain Password Policy Requirements" box?

To customize the subject matter on the "Domain Password Policy Requirements" box present in the Reset Password / Change Password pages, edit the ".html" file at the location provided below,

<installation_directory>\webapps\adssp\html\<your_domain_name>_PasswordPolicy.html

Hide CAPTCHA (Word Verification Image)

ADSelfService Plus can be customized at the Reset Password / Change Password pages by enabling or hiding CAPTCHA (Word Verification Image).

To disable CAPTCHA (Word Verification Image)

- Login ADSelfService Plus
- Click on Admin Tab
- Click on Customize display Settings.
- Check against the "Check Box" provided to "Hide CAPTCHA (Word Verification Image)"
- Click on Save to save the changes.

CAPTCHA can be enabled by removing the "Check" against this "Check Box"

Edit Theme :

ADSelfService Plus facilitates customizing the existing theme by allowing users to themes defined by them.

For an administrator to edit a theme

- Login ADSelfService Plus
- Click on Admin Tab
- Click on Customize display Settings.
- Edit the "Text Box" provided against edit theme and rename the " existing directory name" with the "directory name which contains your desired theme".
- Click on Save to apply the latest theme.

Steps for users to define User defined themes.

Create a new directory at the destination provided below

```
<installation_directory>\webapps\adssp\styles\
```



Note: Each directory (or) Folder saved at the above specified location must include the following css files (**style.css, dialog.css & calendar.css**).

Customize messages at Reset Password /Unlock Account pages

An Administrator can customize the header and footer messages on one or all pages in ADSelfService Plus, directing a user to perform a password reset (Using "Forgot your Password" link) or account unlock (Using "Unlock your Account" link). Customization of header and footer is done by providing links, or text messages within a HTML Table element.

To customize the Header and Footer Messages in one or all the pages edit the file "**CustomLayout.txt**" from the location provided below,

```
<installation_directory>\webapps\adssp\html\
```

Each page directing to Password Reset or Unlock Account has different names as described below.

"url-reset" : "Reset Your Password" Page where users enter their name & select their domain. Enter your text messages in the file "CustomLayout.txt" within the open and close Tags provided below.

```
<url-reset-header>Enter Message or Link </url-reset-header>
<url-reset-footer> Enter Message or Link </url-reset-footer>
```

"url-validateuser" : "Security Questions" Page where users answer secret questions. Enter your text messages in the file "CustomLayout.txt" within the open and close Tags provided below.

```
<url-validateuser-header> Enter Message or Link </url-validateuser-header>
<url-validateuser-footer>Enter Message or Link </url-validateuser-footer>
```

"url-resetpassword" : This is the Page which provides "Domain Password Policy requirements" for users when Password Reset / Unlock Accounts. Enter your text messages in the file "CustomLayout.txt" within the open and close Tags provided below.

```
<url-resetpassword-header> Enter Message or Link </url-resetpassword-header>
```

```
<url-resetpassword-footer> Enter Message or Link </url-resetpassword-footer>
```

"url-resetresult" : This page shows the status of a "password reset" or "account unlock". Enter your text messages in the file "CustomLayout.txt" within the open and close Tags provided below.

```
<url-resetresult-header>Enter Message or Link </url-resetresult-header>
```

```
<url-resetresult-footer> Enter Message or Link </url-resetresult-footer>
```

Example:

```
<url-reset-header>
```

```
<table>
```

```
<tr>
```

```
<td class = "blacktxt">Enter your text message</td>
```

```
</tr>
```

```
</table>
```

```
</url-reset-header>
```

(Note: Save a BackUp copy of the existing file CustomLayout.txt before editing.)

Custom Attributes

This wizard will help an administrator to add custom attributes from the extended schema of Active Directory to the existing list of AD attributes. Custom attributes are added to allow users to self update any desired information. End users can self-update these custom attributes using ADSelfService Plus self service portal once added.

To add a Custom Attribute for Self Update by End Users:

- Click on "Admin" Tab -->>Custom Attributes
- Enter the "Display Name" of the attribute in the Display Name box.
- Enter the "LDAP Name" of the attribute in LDAP Name box.
- Select the Data Type from the pull down menu.
- Provide a check against the Custom Attributes checkbox to enable it for Self Update by End Users.
- Click on the "Add" button.
- The attribute or field added will be displayed with a check box for selection under the "Admin" Tab -->>Policy Configuration -->>Self Update Active Directory Attributes -->>Custom Attributes
- Provide a check against the added custom attribute.
- Click on "Save" button to allow end users self update.

NT Service

ADSelfService Plus can also be run as a service

Steps to install ADSelfService Plus as Service

NT service installation:

To start ADSelfService Plus as a service:

1. Stop ADSelfService Plus (Start-->All Programs-->ADSelfService Plus-->Stop ADSelfService Plus).
2. Start-->All Programs-->ADSelfService Plus-->NT Service-->Install ADMP Service.
3. Start-->Run and type "services.msc".
4. Right-click on "ManageEngine ADSelfService Plus" and select Start to start ADSelfService Plus as service.

Connection Settings

The connection Settings in ADSelfService Plus allows an administrator to enable or disable the following options.

- Enable SSL port
- Enable "Pass-through" Authentication [Single Sign-On]
- Option to configure other AdventNet Products.

Enable SSL port

Connection settings include the port and time for which the service remains connected for a user.

You can Change the connection settings using this feature. Perform the following steps

1. Select the Admin tab.
2. Click the Connection settings.
3. Enter the port number
4. Check in the Enable ssl port [https] to enable secure sockets layer and enter the number. Select the session expiry time.
5. Click on save changes.
6. Click SSL Certificate Installation Guide if you require help while installation.

Enable "Pass-through" Authentication [Single Sign-On]

On enabling single sign-on, ADSelfService Plus directly authenticates a user's windows system user name and password . Hence a user need not login over again to enter ADSelfService Plus and update his personal information in the Active Directory.

To enable "Pass-through" Authentication for Domain users.

- Log in to the ADSelfService Plus application using the **user name** and **password** of a ADSelfService Plus administrator.
- Click the **Admin** tab in the header pane.
- Click on **Connection** Settings on the left bar
- Provide a Check against the Checkbox to enable or disable "Pass-through" [Single Sign-On]

Internet Settings for "Pass-through Authentication" [Single Sign On]

Before enabling "Pass-through Authentication" [Single Sign On] Check out the settings below on your Internet Explorer

1. Tools --> Internet Options -->> Security -->> Local Intranet -->> Sites -->> Provide a check against the below three options

- Include all local (intranet) sites not listed in other zones,
- Include all sites that bypass the proxy server,
- Include all network paths(UNCs)

And then click "Advanced" -->> A pop up window appears -->> "Add" the server name where ADSelfService Plus is installed. (**example:** http://w2kserver) -->> Save the settings.

2. Tools --> Internet Options --> Security --> Custom Level --> User Authentication --> choose "Automatically logon only in Intranet zone"(Under "User Authentication" --> Logon) --> Save the settings

3. Tools --> Internet Options --> Advanced --> Security(Enable Integrated Windows Authentication) --> Save the settings

4. Tools --> Internet Options --> Advanced -->check "Use HTTP 1.1 through proxy connections" (HTTP 1.1 settings) --> Save the settings

Configure other AdventNet Products

You can also configure other Adventnet products, namely ADManager Plus and ServiceDeskPlus. The product links will be available in the Jump To list once the Application name, Server name, Port Number and Protocol details are entered and saved. In-order to configure other AdventNet products.

1. Log in to the ADSelfService Plus application using the user name and **password** of a ADSelfService Plus administrator.
2. Click the **Admin** tab in the header pane.
3. Click on **Connection** Settings on the left bar
4. Select the Application name,
5. Enter the Server name, Port Number and Protocol details.
6. Save the Settings. to Configure the selected AdventNet Application



Note: Proper Authentication details ie) **username** and **password** must be provided in order to enable the above settings.

Install SSL Certificate

ADSelfService Plus runs as a HTTPS service. It requires a valid CA-signed SSL certificate with the principal name as the name of the host on which it runs. By default, on first time startup, it creates a self signed certificate. This self signed certificate will not be trusted by the user browsers. Thus, while connecting to ADSelfService Plus, you need to manually verify the certificate information and the hostname of ADSelfService Plus server carefully and should force the browser to accept the certificate.

To make the ADSelfService Plus server identify itself correctly to the web browser and the user:

- You need to obtain a new signed certificate from a CA for the ADSelfService Plus host.

You can use keytool (bundled with Java) to create your certificates, get them signed by a CA and use them with ADSelfService Plus. Detailed instructions on using keytool are provided here.

- Step 1: Startup Process
- Step 2: Certificate Request Process
- Step 3: Certificate Issuance Process
- Step 4: Associating the Certificate with ADSelfService Plus

Step 1: Startup Process:

This is the initial settings to be made in ADSelfService Plus before applying for an SSL Certificate.

1. Start ADSelfService Plus.
(Start --> All Programs --> ADSelfService Plus --> Start ADSelfService Plus).
2. Change the Port Settings from http to https.
("Admin" tab --> "Connection" (left pane) --> Check "Enable SSL Port [https]" --> Save).
3. Stop ADSelfService Plus.
(Start --> All Programs --> ADSelfService Plus --> Stop ADSelfService Plus).

Step 2: Certificate Request Process:

Before requesting for a certificate from any certifying authority one needs to Create tomcat specific ".keystore" file and ".csr" file, which will be further referred as <domainName>.keystore and <domainName>.csr respectively.

The <domainname>.keystore and <domainName>.csr will include information provided by the individual who creates the .keystore and .csr files.

To create the .keystore file follow the below steps

- Open the Command Prompt
- From the location <installation directory> \ jre \ bin execute the below command.

```
keytool -genkey -alias tomcat -keypass <your key password> -keyalg RSA -validity 1000 -keystore <domainName>.keystore
```

- This will prompt you to enter a series of values that are part of the distinguished name (DN) of the server that will host ADSelfService Plus



Note: At the end of executing the above command, you will be prompted to enter keystore password. Try giving the password same as your key password.

To create the .csr (Certificate Signing Request) file follow the below steps

- Open the Command Prompt
- From the location **<installation directory> \ jre \ bin** execute the below command.

```
keytool -certreq -alias tomcat -keyalg RSA -keystore <domainName>.keystore -file
<domainName>.csr
```

The .csr (Certificate Signing Request) file is temporary and will need to be submitted to a CA (Certifying Authority) to receive **CA-Signed Certificate** files.

Step 3: Certificate Issuance Process :

The third steps talks about the Certificate Issuance Process where the temporary files created are submitted to certifying authority to receive a **CA-Signed Certificate**.

1. Some of the prominent CAs are **Verisign** (<http://verisign.com>), **GoDaddy** (<http://www.godaddy.com/>), **Comodo** (<http://www.comodo.com>). Check their documentation / website for details on submitting CSRs and this will involve a cost to be paid to the CA
2. Submit the created temporary file **<domainName>.csr** file to the Certificate Authority (CA), to receive **<domainName>.crt** or **<domainName>.cer** file along with other certificate files in a zipped format.
3. This process usually takes a few days time and you will be returned your signed SSL certificate and the CA's root certificate as .cer files

Once the **CA-Signed Certificate** is received from the Certifying Authority (CA)

- Unzip and extract the certificate files into **<installation> \ jre \ bin** folder.
- Install the Root, Intermediate and Primary Certificate files in the same sequence as mentioned.



Note: Each time you install a certificate to your keystore you will be prompted for the keystore password, which you chose when generating your CSR.

The certificate files will vary, based on your choice of CA.

For instance if your CA is "**GoDaddy**", then the steps to follow will be :

Execute the following commands from **<installation directory> \ jre \ bin**

```
keytool -import -alias root -keystore <domainName>.keystore -trustcacerts -file gd_bundle.crt
```

```
keytool -import -alias cross -keystore <domainName>.keystore -trustcacerts -file
gd_cross_intermediate.crt
```

```
keytool -import -alias intermed -keystore <domainName>.keystore -trustcacerts -file
gd_intermediate.crt
```

```
keytool -import -alias tomcat -keystore <domainName>.keystore -trustcacerts -file
<domainName>.crt
```

For instance if your CA is "Verisign", then the steps to follow will be :

Execute the following commands from **<installation directory> \ jre \ bin**

```
keytool -import -alias intermediateCA -keystore <domainName>.keystore -trustcacerts -file
<your_intermediate_certificate>.cer
```

```
keytool -import -alias tomcat -keystore <domainName>.keystore -trustcacerts -file
<domainName>.cer
```

For instance if your CA is "Comodo", then the steps to follow will be :

Execute the following commands from **<installation directory> \ jre \ bin**

```
keytool -import -trustcacerts -alias root -file AddTrustExternalCARoot.crt -keystore
<domainName>.keystore
```

```
keytool -import -trustcacerts -alias addtrust -file UTNAddTrustServerCA.crt -keystore
<domainName>.keystore
```

```
keytool -import -trustcacerts -alias ComodoUTNServer -file ComodoUTNServerCA.crt -keystore
<domainName>.keystore
```

```
keytool -import -trustcacerts -alias essentialSSL -file essentialSSLCA.crt -keystore
<domainName>.keystore
```

```
keytool -import -trustcacerts -alias tomcat -file <domainName>.crt -keystore
<domainName>.keystore
```

- Copy the **<domainName>.keystore** and place it in **<installation directory> \ conf** folder.

Step 4: Associating the Certificate with ADSelfService Plus :

This will configure the ADSelfService Plus server to use the keystore with your SSL certificate.

To configure ADSelfService Plus server to use the keystore with your SSL certificate follow the below steps.

- Edit the **server.xml** in the **<installation directory> \ conf** folder.
- Replace the value of "**keystoreFile**" to "**./conf/<domainName>.keystore**" at the last Connector(End of the page).
- Replace the password for "**keystorePass**" to "**password as given for keystore**"
- Save the **server.xml** file and close it.
- Start ADSelfService Plus and connect to a browser.

If you are able to view the ADSelfService Plus login console without any warning from the browser, you have successfully installed your SSL certificate in ADSelfService Plus!

Server Settings

You can Change Configure ADSelfService Plus startup & log settings.

1. Select the Admin tab.
2. Click the Server settings.
3. Check in the boxes you wish.
4. The default working mode is 'Normal' with minimal debugging information.
5. click on 'Save changes' .

Personalization

- Change Password for ADSelfService Plus
- Change Display Language

Change Password for ADSelfService Plus

Change Password for ADSelfService Plus and Personalize your Admin password.

To change the "admin" login password for ADSelfService Plus Application.

- Click on **Personalize** under "**Admin**" Tab
- Input the Old Password
- Input the new Password
- Confirm Password
- Click on Change

The Admin password can be personalized to a new password.

Display Language

ADSelfService Plus can be Localized to "English" and "Japanese" Languages.

To Localize ADSelfService Plus

- Click on **Personalize** under "**Admin**" Tab
- Choose the Display Language "English" or "Japanese" from the "Pull Down"
- Click on "**Save Changes**" to save the changes.

Domain User Web Portal

From the ADSelfService Plus Domain User Web Portal a domain user will be able to perform the following self service functions.

1. Reset Forgotten Password.
2. Unlock their Locked Out Account.
3. Change their own Password by meeting Policy Requirements.
4. Update their own personal information in the Active Directory.

A Domain User Portal in ADSelfService Plus can be accessed by any domain user for password reset and account unlock in two different ways.

1. From a Web Browser after a User Logon into a Domain Computer
2. Using ADSelfService Plus GINA from the Windows Logon Screen Extension

Any Domain User must Logon into the ADSelfService Plus Domain User Web Portal by providing their proper credentials to change his password or to update their personal information in the Active Directory.

Reset Password / Unlock Account by Logging on into a Domain Computer

A Domain User, must Logon into a Computer, access a web browser and click on "Reset your Password" link on the ADSelfService Plus Web Portal, in-order to reset his password. He or She will need to Logon into a different Domain Computer, click on the "Unlock Your Account" link to Unlock their Locked-out Account.

The screenshot shows the ADSelfService Plus Domain User Web Portal interface. At the top, there are two main buttons: "Forgot Your Password? Reset Your Password" and "Is Your Account Locked? Unlock Your Account". Below these buttons, there is a section titled "Enrolled Users" with the following instructions:

- » Enroll your secret question and answers.
- » Login to change your password.
- » Login to update your information.

To the right of the "Enrolled Users" section is a login form with the following fields:

- User Name:
- Password:
- Log on to:
-

Reset Password / Unlock Account Using ADSelfService Plus GINA from the Windows Logon Screen Extension

The ADSelfService Plus Reset Password portal can also be accessed even without a Logon into a Domain Computer by using the "Ctrl + Alt + Del" Winlogon "Reset Password / Unlock" ADSelfService Plus GINA extension as highlighted in the below figure.



For a Domain user to Access ADSelfService Plus GINA a client software must be installed. Installation of ADSelfService Plus GINA on client machines is facilitated from the Admin portal of ADSelfService Plus.

Self Service

The Self Service Module allows the end user to perform routine activities associated with his account and account password. This feature from ADSelfService Plus offers users, the flexibility to do these common tasks, without any intervention from the administrator. The tasks included in the Self-Service Module have been listed below:

- Change Password
- Reset Password
- Unlock Account
- Reset Password / Unlock Account using ADSelfService Plus GINA / CP

Change Password

In-order to change password using ADSelfService Plus, the end user must login into the ADSelfService Plus web portal by providing his login credentials.

- Minimum Password Length
 - Minimum Password Age
 - Maximum Password Age
 - Password Complexity
 - Password History
1. Click on the **Change Password** link(top right corner) of the **MyInfo** page. This opens the '**Change Domain Password**' dialog.
 2. Enter the current password in the given text field.
 3. Enter the new password in the text field provided.
 4. Enter the same password in the '**Confirm Password**' field.
 5. Click **OK** to save changes.

Reset Password

Any Enrolled Domain User can self reset his own password from a web browser using ADSelfService Plus application. For a user to self reset his own password the below steps are to be followed.

1. Click on 'Reset Your Password' link under 'Forgot Domain Password?' in the Login Page'. This opens the Reset Your Password wizard.
2. Enter the 'Domain User Name' in the text field provided.
3. Select the Domain from the given list.
4. Click on 'Continue'. This opens the Secret Questions page.
5. Enter the correct answer set for the Secret Question and click 'Continue'.
6. The Reset Password page opens up. Enter the new password and Confirm the same in the text field provided. The new password must confirm to the Domain Password Policy requirements that are listed.
7. In case your Administrator has set for additional Word Verification, Decipher the letters and enter them correctly in the text field provided.
8. Click on 'Change Password' button to update the new password.

Unlock Account


ADSelfService Plus allows an End User to self Unlock his account from a Web Browser when his account is locked out . This is done by validating the secret questionnaire.

1. Click on 'Unlock Your Account' link under 'Is Your Account Locked?' in the Login Page. This opens the Unlock Your Account wizard.
2. Enter the 'Domain User Name' in the text field provided.
3. Select the Domain from the given list.
4. Click on 'Continue'. This opens the Secret Questions page.
5. Enter the correct answer set for the Secret Question and click 'Continue'.
6. The Account page opens up. Click on the 'Unlock' button.
7. In case your Administrator has set for additional Word Verification, Decipher the letters and enter them corectly in the text field provided.

Users Reset Password / Unlock Account using ADSelfService Plus GINA / CP

Any domain user who has enrolled into ADSelfService Plus web console by answering validation questions can use the 'Forgot Password' extension (ADSelfService Plus GINA / CP extension) displayed on the Windows Logon Screen to Reset his password or Unlock his account.

1. An Enrolled Domain user when forgets his/her domain login password or domain account is locked-out can click on the "Ctrl + Alt + Del" button on his Windows machine. This opens the GINA extension or Winlogon extension on the login screen with a 'Reset Password / Unlock' button on the extension.
2. The user in-order to reset his forgotten password to a new password using ADSelfService Plus web console must click on the 'Forgot Password' Button on the Winlogon / GINA extension. The 'Forgot Password' link automatically directs the user to the 'Reset Your Password' Screen of ADSelfService Plus Web Console.
3. The User must enter his domain name and click on continue, this takes the user to the 'Security Questions' screen on the Web Browser.
4. He /She must answer the 'Security Questions' as per his/her enrollment profile and click on 'Continue'
5. The next screen is the 'Reset Password' Screen where the user enters his new password by conforming the password policy requirements that is displayed on the screen.
6. The password is reset to a new password that is set by the user and a successfully reset message appears.
7. The domain user can now use this new password to login into his domain. Kindly check the screen shots below for easy understanding of Password Reset with ADSelfService Plus GINA / CP.

 GINA is installed Windows 2000 and XP Machines only. For Windows Vista Machines a Credential Provider model is installed which requires the same process for resetting the password as GINA tool.

Screen shots for better understanding of Password Reset / Unlock Account with ADSelfService Plus GINA / CP

GINA and Credential Provider Extensions for Windows XP and Windows Vista Machines Respectively



Fig.1. ADSelfService Plus GINA Extension For Windows XP

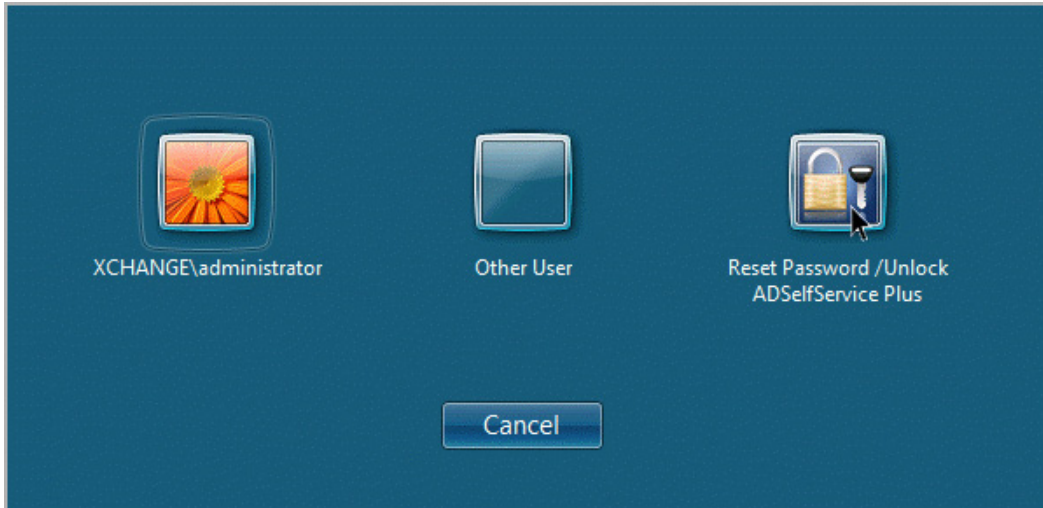


Fig.2. ADSelfService Plus Credential Provider extension for Vista.

Reset Password and Unlock Account Selection in Windows XP and Windows Vista Machines Respectively

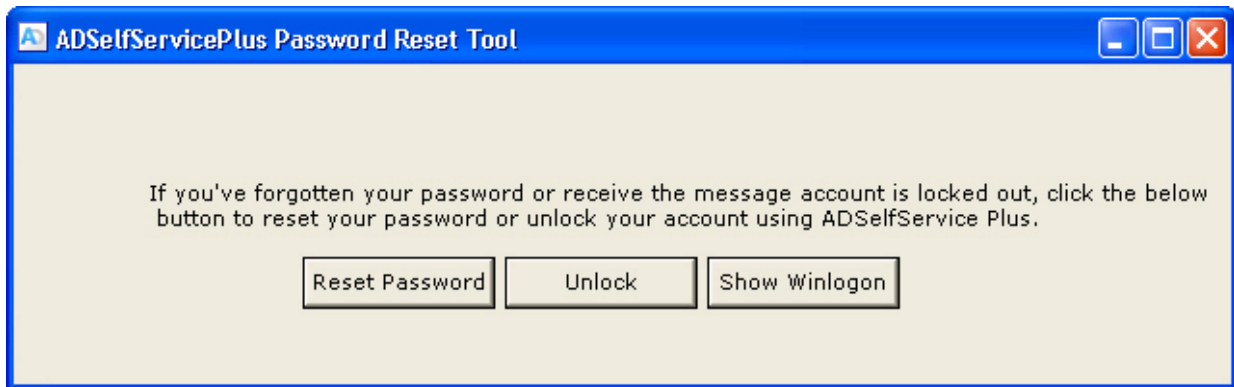


Fig.3. Selection of Reset Password and Unlock Account in Windows XP

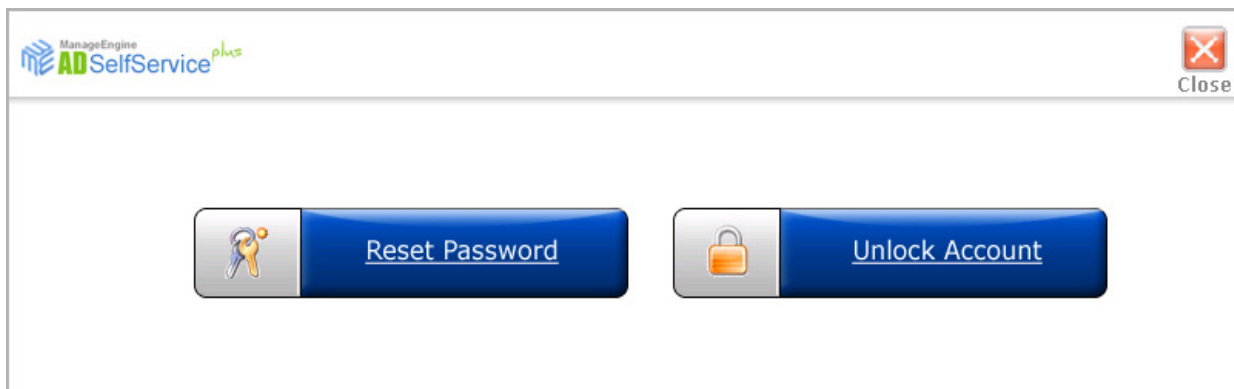


Fig.4. Selection of Reset Password and Unlock Account in Windows Vista

On clicking on the Reset Password / Unlock Account button provided above the user is connected to a Web Browser from where he can provide his Domain Name, Answer the Secret Questionnaire Reset his Password or Unlock his locked out account. Screen Shots are provided below.

Domain User Name Input for Reset Password / Unlock Accounts & Answering Security Questionnaire.

Fig.5. Entering Domain User Name to Reset Password

Fig.6. Entering Domain User Name to Unlock Account

Fig.7. Answering Secret Questions

Reset Password and Account Unlock Screens

ManageEngine
ADSelfService plus

Close

Reset Password
Please enter a new password in the boxes below:

Domain Password Policy Requirements

- ✓ Minimum Password Age : 1
- ✓ Maximum Password Age : 30
- ✓ Minimum Password Length : 7
- ✓ Password History : 3
- ✓ Password Complexity : Enabled

Reset Password

Password :

Confirm Password :

Reset Password Cancel

Fig.8. Enter the password to Reset

ManageEngine
ADSelfService plus

Close

Unlock Account
Unlock your locked out account:

Unlock Account Cancel

Fig.9. Unlock Account

ADSelfService Plus Deployment Scenarios

- Enable SSL for Secure Communication over the Internet
- Configuring ADSelfService Plus to Securely Function in a De-militarized Zone (DMZ)
- Open -up selective Firewall Ports to facilitate access over the Internet
- Protocols and Ports Used

Enable SSL for Secure Communication over the Internet:

You will need to enable SSL for enhanced security and secure communication by ADSelfService Plus over the Internet. To enable SSL on ADSelfService Plus kindly follow the below steps

- Logon in to ADSelfService Plus into the "Self-Service Admin Login" by providing proper admin credentials.
- Click on the "Admin" tab ==> "Connection".
- Put a tick on the box provided near "Enable SSL Port [https]"
- Click on the "Save" to save the settings and restart ADSelfService Plus.

This will enable SSL and a secure communication by ADSelfService Plus over the internet is possible. A valid SSL certificate is to be applied for enabling SSL . Steps to [Install a SSL certificate in ADSelfService Plus](#).

Configuring ADSelfService Plus to Securely Function in a De-militarized Zone (DMZ)

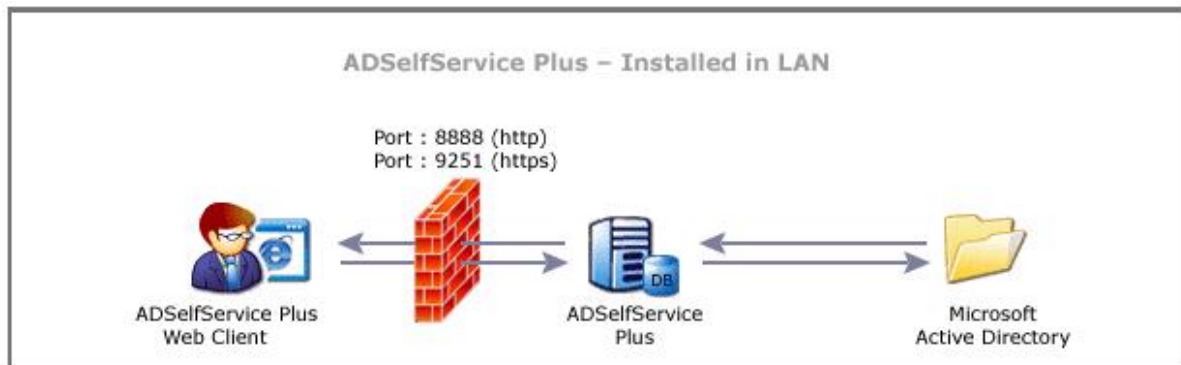
For ADSelfService Plus to be installed in the DMZ (Demilitarized Zone), Port "389" (to communicate with the LDAP Protocol) and Port "135" (to communicate with RPC) are to be opened up in the Firewall along with other dynamic ports.

Section: "[Find all Dynamic Ports](#)" highlights the steps for identifying dynamic ports that needs to be opened up in the firewall. We strongly recommend you to run ADSelfService Plus application in Secure Socket Layer (SSL) mode for a DMZ Server Installation. Check the above section on how to [enable SSL](#).

Open -up selective Firewall Ports to facilitate access over the Internet:

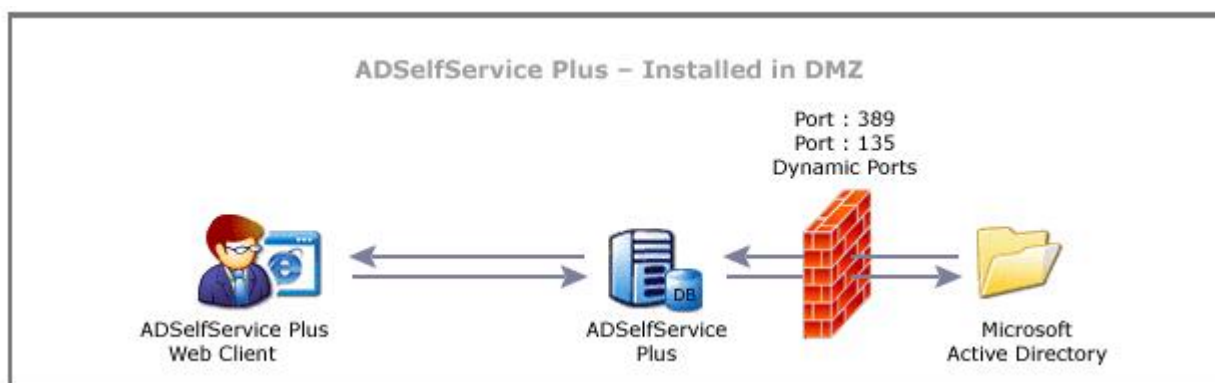
(i) When ADSelfService Plus is installed on your local area network with the url accessible across internet :

Open the port on which ADSelfService Plus is running. By default ADSelfService Plus runs on port 8888 and it is configurable.



(ii) When ADSelfService Plus is installed in the DMZ, open the following ports in the Firewall:

- Port "389" to communicate with the LDAP Protocol.
- Port "135" to communicate with RPC.
- Refer section: "Find Dynamic Ports" for other dynamic ports that needs to be opened in the Firewall. These will be used for communication between AD and ADSelfService Plus.



Protocols and Ports Used

ADSelfService Plus uses Windows ADSI (Active Directory Service Interfaces) to interact with the Active Directory, which in turn uses LDAP (for querying and modifying directory services running over TCP/IP) Protocol on Port 389.

Right now, ADSelfService Plus communicates with the Active Directory using normal LDAP connection. And we have planned to use secured LDAP connections.

Finding / Identifying Dynamic Ports:

ADSelfService Plus uses several other ports which are dynamic. It is required by an administrator to identify all available dynamic ports and open them up in the Firewall. In-order to open-up dynamic firewall ports one can follow the below steps.

Step 1: Open a command prompt in the Domain Controller.

Step 2: Type the following command and execute it in the command prompt.

```
portqry -n "<Your_Domain_Controller_Name>" -e 135 -l resultPorts.txt
```

In case you use different port for RPC, use the Port Number in which your RPC is running by replacing 135 in the above command.

Step 3: After executing the above command, open the "resultPorts.txt" from where the command is executed.

Step 4: Find for all the "_tcp" in the "resultPorts.txt" (Ex : ncacn_ip_tcp:100.190.1.2[1142])

Step 5 : The value in the Square Brackets[] are the ports which needs to be opened. Make a note of these ports. (Ex: in the above result, 1142 is the port that needs to be opened).

Step 6: Continue with the search until the file ends and open all the identified ports.

Troubleshooting Tips

- Domain Settings
 - Active Directory Self Update
 - Active Directory Reports
-

Domain Settings

1. When I start ADSelfService Plus, none of my domains are discovered. It says "No Domain Configuration available". Why?
2. When I add my domains manually, the Domain Controllers are not resolved. Why?
3. When I add the Domain Controller, I get an error as "The Servers are not operational". What does it mean?
4. When I add the Domain Controller, I get an error as "Unable to get domain DNS / FLAT name". What does it mean?
5. The status column in the domain settings says that the user do not have Admin Privilege?

1. When I start ADSelfService Plus, none of my domains are discovered. It says "No Domain Configuration available". Why?

ADSelfService Plus, upon starting, discovers the domains from the DNS Server associated with the machine running the product. If no domain details are available in the DNS Server, it shows this message.

2. When I add my domains manually, the Domain Controllers are not resolved. Why?

The DNS associated with the machine running ADSelfService Plus might not contain the necessary information and hence you need to add the Domain Controllers manually.

3. When I add a Domain Controller, I get an error "The Servers are not operational". What does it mean?

The Servers are not operational could mean either of the below provided status of the added Domain Controller.

1. The Domain Controller being invalid or
2. The Domain Controller could not be contacted at that point in time due to network unavailability.

4. When I add a Domain Controller, I get an error as "Unable to get domain DNS / FLAT name". What does it mean?

This error could be due to any of the following reasons:

1. When the specified user name or the password is invalid.
2. Anonymous login (when no user name and password is provided)
3. When the "IP Address" of the Domain Controller is inputted instead of its name.

5. The status column in the domain settings says "The user does not have Admin Privilege". Why?

This is a warning message to indicate that the listed user does not have administrator privileges i.e, the user is not a member of Domain Admins Group. Hence permissions applicable to Administrator may not be available to this user.

Active Directory Self Update

1. Error Code - 80070005 / Error Code - 5 : Error In Setting Attributes, Access is denied

Cause : User account does not have enough privileges over the object.

Solution : Make the User privileged by providing "Domain User Name" and "Domain Password". For help on providing privileges to a user [click here](#).

2. While user password reset, I get the following error "Error in setting the Password. The network path not found - Error Code: 80070035"

While setting the password for the user if the target machine could not be contacted, this error is shown. This could happen when the DNS associated with the machine running ADSelfService Plus do not point to the Domain Controller where the user account is being created (possibly both are in different domains).

3. While user password reset, I get the following error "Error in setting the Password. There is a naming violation - Error Code : 80072037"

One possible reason for this error could be that the password contains some special characters that are not allowed.

4. While updating user information using ADSelfService, I get the following error "The server is unwilling to process the request - Error Code : 80072035"

One possible reasons for this error could be: When modifying the SAM Account Name format for multiple users and when more than one user happen to have the same SAM Account Name.

5. While updating user information using ADSelfService Plus, I get the following error " Error In Setting Terminal service Properties. The specified user does not exist - Error Code : 525"

One possible reason could be that the user or the system account as which the product is run do not have an account in the target domain. Terminal Service properties can only be set if the user account or the system account (applies when ADSelfService Plus is run as a service) that runs ADSelfService Plus has an account on the target domain.

6. I have updated the exchange attributes using ADSelfService Plus, but the properties are not updated in the Exchange Server yet.

ADSelfService Plus modifies the exchange properties in the Active Directory. The changes may not immediately reflect in the Exchange Server. It will get updated after some time.

7. I am not able to set the Terminal Services properties for a user?

One possible reason could be that the user or the system as which the product is run do not have an account in that domain.

Refer to here for starting ADSelfService Plus in User or System account.

8. When I modify a user, I get the following error " A device attached to the system is not functioning - Error Code : 8007001f "

The possible reasons for this error could be:

1. When modifying an user, if an unacceptable format is chosen for the naming attributes. For example, if the format chosen for the Logon Name is LastName.FirstName.Initials and if the user do not have any one of these attributes specified, this error will occur.

9. Email address for the user not showing up or not set properly?

The possible reason could be:

1. Email could **Not have been set** as per Recipient Policy. Check whether all LDAP Attributes in recipient policy query are set to specific value.
2. Check in the user account properties whether you entered the attribute for email. Ex: xyz@**company.com**. The company should be entered to the users.

10. Error-The server is unwilling to process the request while Password Reset, and does not match with our password complexity requirements?

The possible reason could be:

You have not specified or opted for any options in 'Password Complexity' while creating user account.

Ex: There will be options for password complexity like length of password, Characters that can be used or number of bad login attempts etc. You need to select any degree of complexity, ignoring so will throw above error.

11. Error code: 8007052e

Reason:, The Supplied credentials are invalid.

12. Error code: 80070775

Reason: The referenced account is currently locked out and may not be logged on.

13. Error code: 800708c5

Reason: The password does not meet the password policy requirements. Check the minimum password length, password complexity and password history requirements.

14.No such user matched. Verify the LDAP attribute in search query

Reason: No Users in AD matches with the criteria provided by you.Try choosing the correct matching attributes by checking with the query provided in the "Match criteria for Users in AD",this is obtained by clicking on "Update in AD" button and expanding "Select Attributes" box.

Active Directory Reports


1. When I specify the details and generate the report, it says "No Result available" or incomplete data
2. AD Reports shows an object that do not exist in the Active Directory?

1. When I specify the details and generate the report, it says "No Result available" or incomplete data

It could be because of any of the following reasons:

1. When ADSelfService Plus could not contact the Domain Controller as it is not operational or due to network unavailability.
2. In case of multiple Domain Controllers, when the data is not replicated in all the Domain Controllers.
3. The "LastLogonTime" that is used to determine the inactive users and computers is not replicated in all the Domain Controllers. Hence, you need to specify all the Domain Controllers in the Domain Settings to enable ADSelfService Plus to retrieve the data from all the Domain Controllers.
4. When the password policy is not set (i.e., Max Password Age is set to zero), the Password Expired Users report and Soon to Password Expiry users report will not show any data.

2. AD Reports shows an object that do not exist in the Active Directory?

This mismatch could occur when the data is not synchronized with the Active Directory. The data synchronization with the Active Directory happens everyday at 1:00 hrs. If ADSelfService Plus is not running at that time, you can initiate the data synchronization manually by clicking the  icon of that domain from the Domain Settings.

ADSelfService Plus Frequently Asked Questions

1. How do I configure the ADSelfService Plus server in the DMZ (Demilitarized Zone), and what are the security measures that need to be taken?
2. What are the ports that need to be opened up in the Firewall to publish ADSelfService Plus server over the internet?
3. How do I protect his database?
4. How does ADSelfService Plus communicate with the AD?

1. How do I configure the ADSelfService Plus server to function in a DMZ (Demilitarized Zone)?

To configure the ADSelfService Plus server to function in a DMZ (Demilitarized Zone) one needs to Enable SSL by providing a Secure HTTPS Port Number and Installing a valid SSL Certificate. This is facilitated by the "Connection" settings provided under the "Admin" Tab of ADSelfService Plus. To know more on the Deployment Scenarios, Ports, Portals discussed under the deployment scenarios section.

2. What are the ports that need to be opened up in the firewall to publish ADSelfService Plus server over the internet?

ADSelfService Plus uses HTTP / HTTPS protocols for communication via ports 8888 / 9251 and these ports need to be opened up in the Firewall.

3. How do I protect the database?

A complex password can be set for the MYSQL database this will prevent access to it by other users.

4. How does ADSelfService Plus communicate with the AD?

ADSelfService Plus uses Windows ADSI (Active Directory Services Interface) for interacting with Active Directory.