

Lepide Active Directory Self Service

Installation and Configuration Guide

Table of Contents

1. Introduction.....	3
2. System Requirements.....	3
2.1 Minimum System Requirements	3
2.2 Supported Platforms	3
2.3 Supported Browsers for Software Access.....	3
2.4 Supported Browsers for TLS.....	4
3. Installing Lepide Active Directory Self Service	4
4. Launching the software	7
5. Admin Login.....	8
6. Add Domain.....	9
6.1 Manage Domain	11
7. User Enrollment	12
7.1 Invite users to Enroll	12
7.2 Bulk Enrollment	14
8. Policy Configuration.....	16
9. Multifactor Authentication	17
9.1 Security Question and Answer Configuration.....	18
9.2 One Time Password Configuration	18
9.3 Authentication Mode.....	19
9.4 Disenrollment.....	20
10. E-mail Server Settings	20
11. SMS Server Settings	22
12. Connection Settings	23
13. Password Synchronization	24
14. Backup/Restore Database.....	26
14.1 Create New Backup	27
14.2 Set Backup Schedule.....	27
14.3 Restore Backup	28
15. GUI Rebranding.....	28
16. Captcha Settings	29
17. Uninstalling the Software.....	30
18. License Activation	33
19. Conclusion.....	37
20. Warranty Disclaimers and Liability Limitation	38
21. Trademarks	38

1. Introduction

Welcome to the Installation and Configuration Guide for Lepide Active Directory Self Service. In this guide, we have covered the steps required for successful installation, uninstallation, license activation, and using Lepide Active Directory Self Service for the first time. A brief overview of policy configuration has also been included in this document.

2. System Requirements

Before you install Lepide Active Directory Self Service, make sure that your computer meets the following requirements:

2.1 Minimum System Requirements

- ☐ Pentium Class Processors
- ☐ 2 GB RAM
- ☐ Disk Space: 400 MB

2.2 Supported Platforms

One of the following Windows operating systems (32/64-bit version):

- ☐ Windows 10 (Both 32-bit and 64-bit)
- ☐ Windows 8.1 (Both 32-bit and 64-bit)
- ☐ Windows 8 (Both 32-bit and 64-bit)
- ☐ Windows 7 (Both 32-bit and 64-bit)
- ☐ Windows Vista (Both 32-bit and 64-bit)
- ☐ Windows XP (Both 32-bit and 64-bit)
- ☐ Windows Server 2012 R2
- ☐ Windows Server 2012 (64-bit)
- ☐ Windows Server 2008 R2
- ☐ Windows Server 2008 (Both 32-bit and 64-bit)

2.3 Supported Browsers for Software Access

- ☐ Internet Explorer 9.0 and above
- ☐ Netscape 7.0 and above
- ☐ Firefox 10.0 and above
- ☐ Google Chrome 17.0 and above

NOTE: Java script must be enabled and preferred screen resolution should be 1024 X 768 pixels or higher

2.4 Supported Browsers for TLS

For Transport Layer Security (https), the following web browser versions are supported:

- Internet Explorer – 9.0 to 11.0 (All Windows OS versions)
- Microsoft Edge (Windows 10)
- Mozilla Firefox and Google Chrome (All Windows OS versions)

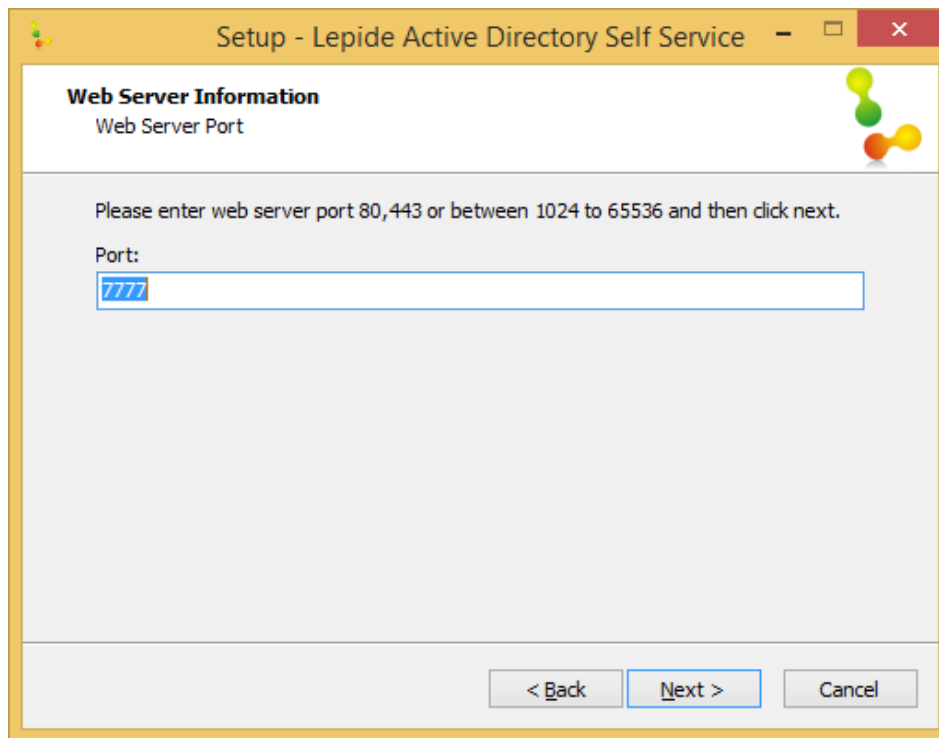
NOTE: For http use, all browser versions are supported.

3. Installing Lepide Active Directory Self Service

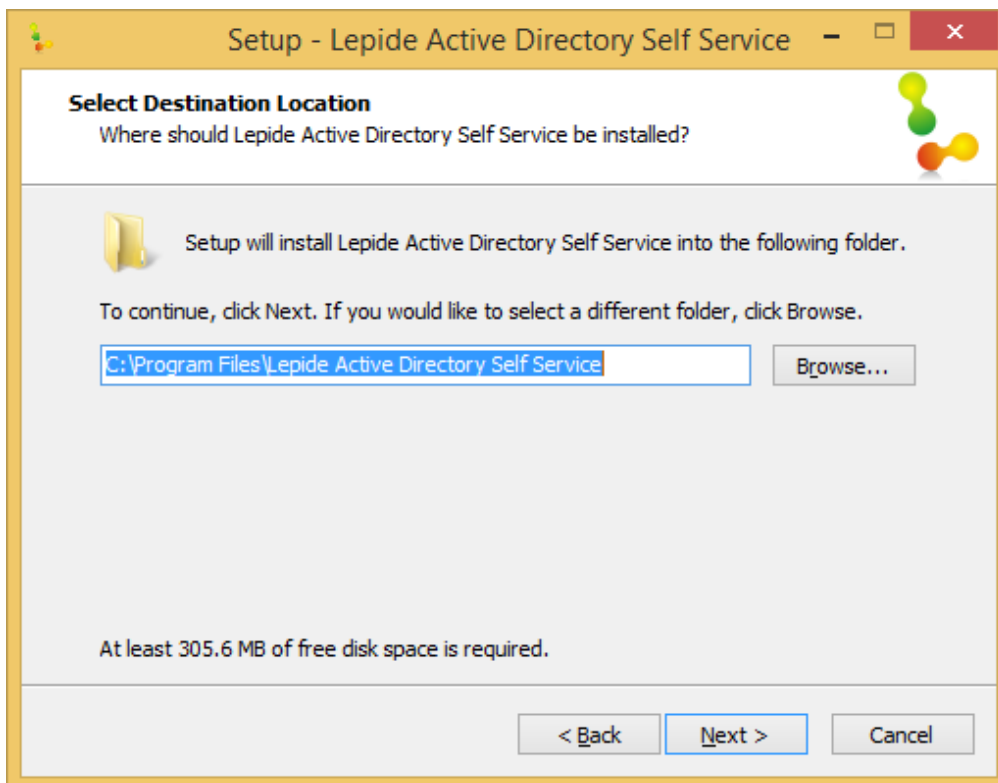
Download the setup file of Lepide Active Directory Self Service from <http://www.lepide.com/active-directory-self-service/download.html> and save it on the disk. Make sure that the host computer meets the entire system requirements and has sufficient memory available.

After you have downloaded the installer file, execute the following steps to install the software:

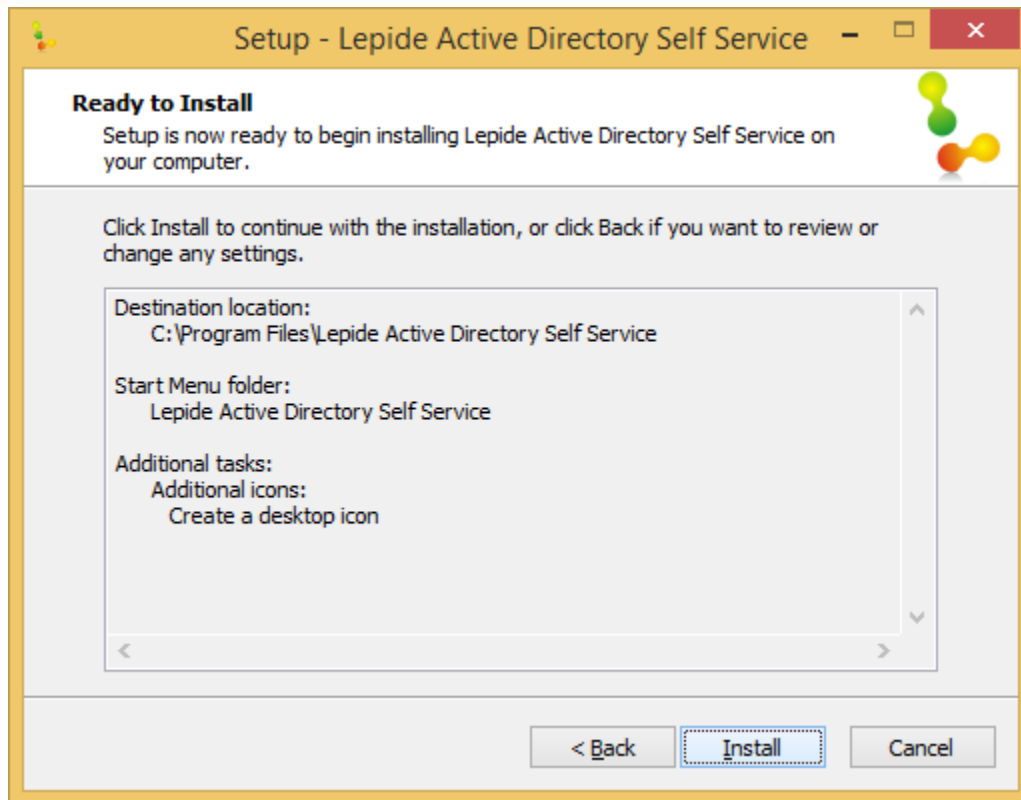
1. Double-click the Lepide Active Directory Self Service's installer file. The LADSS Setup wizard appears; click "Next" to proceed further.
2. Accept the license agreement and click the Next button.
3. Here, the user needs to enter the Web Server Port Number that can vary from 1 to 65535. Here, 7777 is the default port number. After specifying the Port Number, click "Next" to continue.



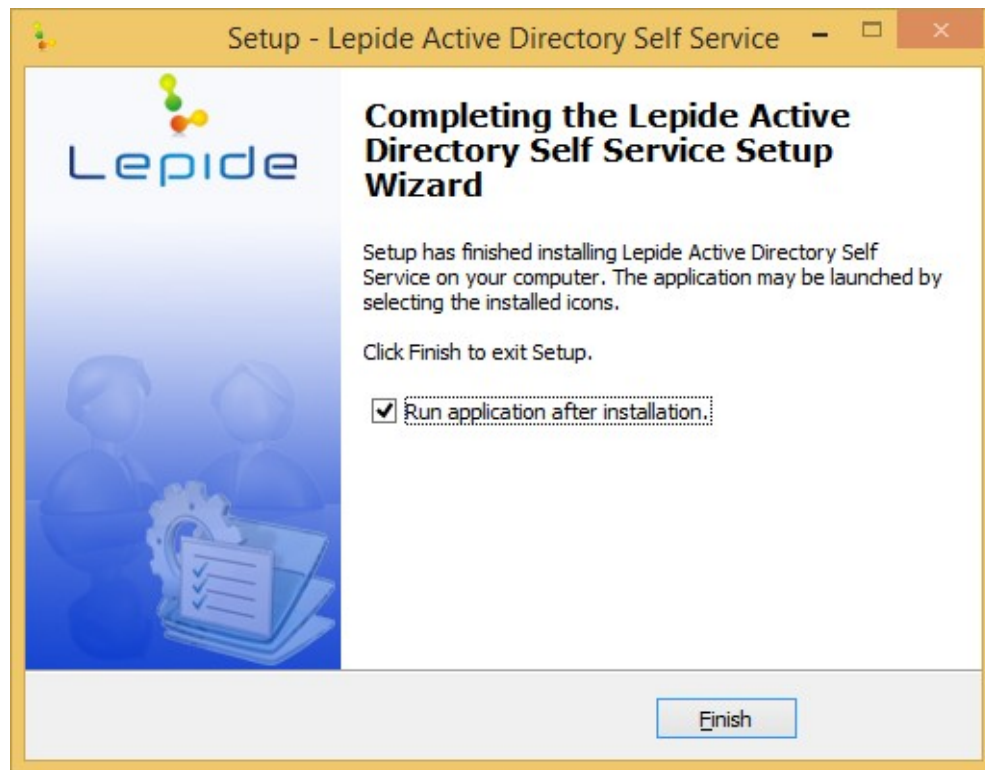
4. Here, the user can change the destination location for installing Lepide Active Directory Self Service software. Click "Next" to proceed.



5. Click "Browse" if you want to change the location of the shortcuts folder in the Start Menu and then click "Next" button.
6. Select the required additional task and click "Next". The setup is now ready to start the installation process:



7. Click "Install" to start the installation process.
8. When the installation process completes, the following message box will appear on the installation wizard. Click the Finish button to complete the installation process and to run the application.



4. Launching the software

Once the solution is installed, it will be added in the system tray. Right-click on the icon and it provides four options to choose from:

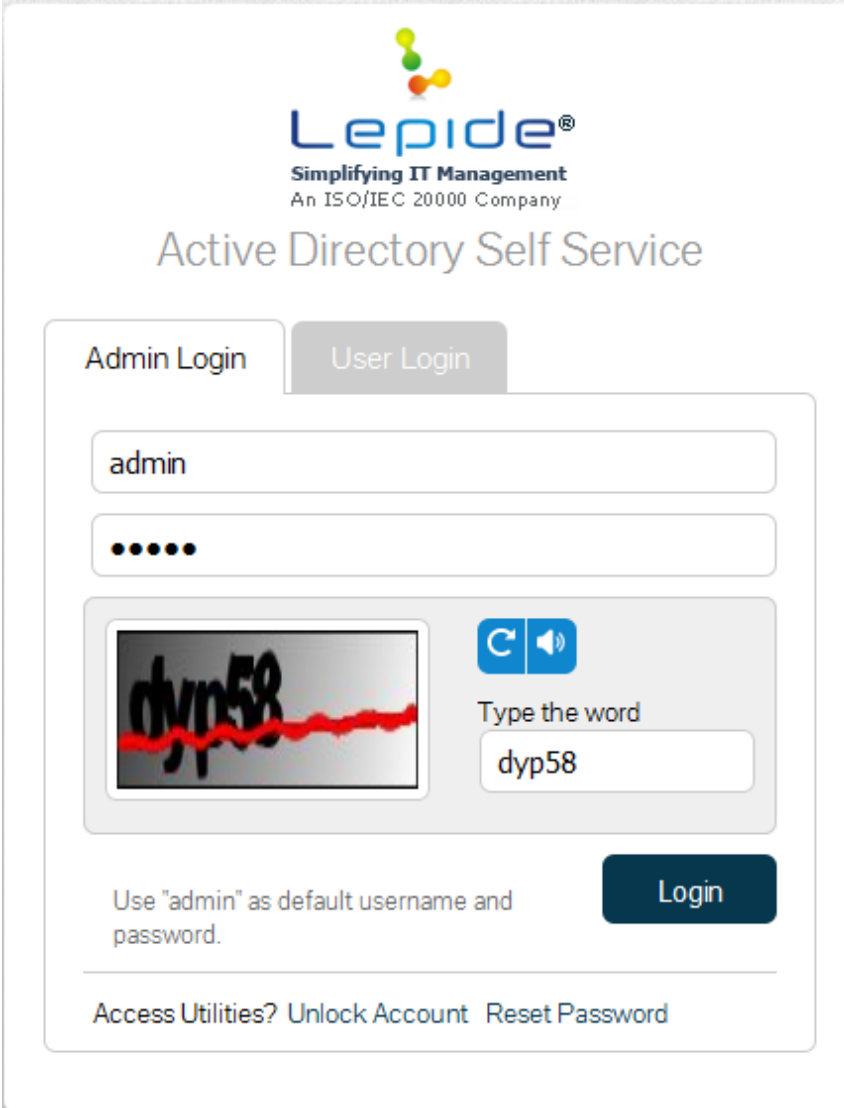
Show Admin Login
Start Server
Stop Server
Exit Tray

- | | |
|-------------------|---|
| Show Admin Login: | This option lets you directly go to the Admin Login section in case you have closed the browser tab where LADSS was running previously. |
| Start Server: | Choosing this option will start the application server. |
| Stop Server: | Choosing this option will stop the application server. |
| Exit Tray: | Choosing this option will remove the application from the system tray. |

NOTE: Admin will need to change the default URL. To change the URL, go to Configuration>>Enrollment Notification>>Add Notification. Here in Mail Content, the default URL will be:
<http://localhost:7777/LADSS/UserLoginAction.do?method=populate>. Change the URL by providing system IP (where the application is installed) in place of "localhost". This URL will be used by users to access the user login section.

5. Admin Login

Getting started with Lepide Active Directory Self Service is easy. As soon as you launch the solution, you will be prompted to login. Use 'admin' as default username and password for first time usage.



The screenshot shows the Lepide Active Directory Self Service login interface. At the top, the Lepide logo is displayed with the tagline "Simplifying IT Management" and "An ISO/IEC 20000 Company". Below the logo, the title "Active Directory Self Service" is centered. The login section has two tabs: "Admin Login" (selected) and "User Login". Under the "Admin Login" tab, there is a username field containing "admin" and a password field with masked characters. Below the password field is a CAPTCHA challenge showing a distorted image of the text "dyp58". To the right of the CAPTCHA image are icons for refresh and audio, followed by the text "Type the word" and a text input field containing "dyp58". At the bottom right of the login section is a dark blue "Login" button. Below the login section, there is a note: "Use 'admin' as default username and password." At the very bottom, there are links for "Access Utilities?", "Unlock Account", and "Reset Password".

It is recommended to change the default username and password after first login. To make changes, go to Configuration section and click Configure Admin Account option to make necessary changes.

Configure Admin Account

Change Administrator's Username

Username: max 100 characters

Change Administrator's Password

Old Password: max 40 characters


New Password: max 40 characters

Confirm Password: max 40 characters

6. Add Domain

As you login to the software, you need to add the domain for which self-service actions are to be configured.

Manage Domain



*User must have administrative rights

In order to add a domain, follow the below mentioned steps:

1. Type the domain name in the Domain text field.
2. Type the name of the primary domain controller in the Domain Controller text field. You can also provide the IP Address instead of system name.
3. Type the domain administrator name in the Username text field of that user who has the privilege to reset password, unlock account in the particular domain.
4. Provide the domain admin password in the Password field.
5. Click the Save button.

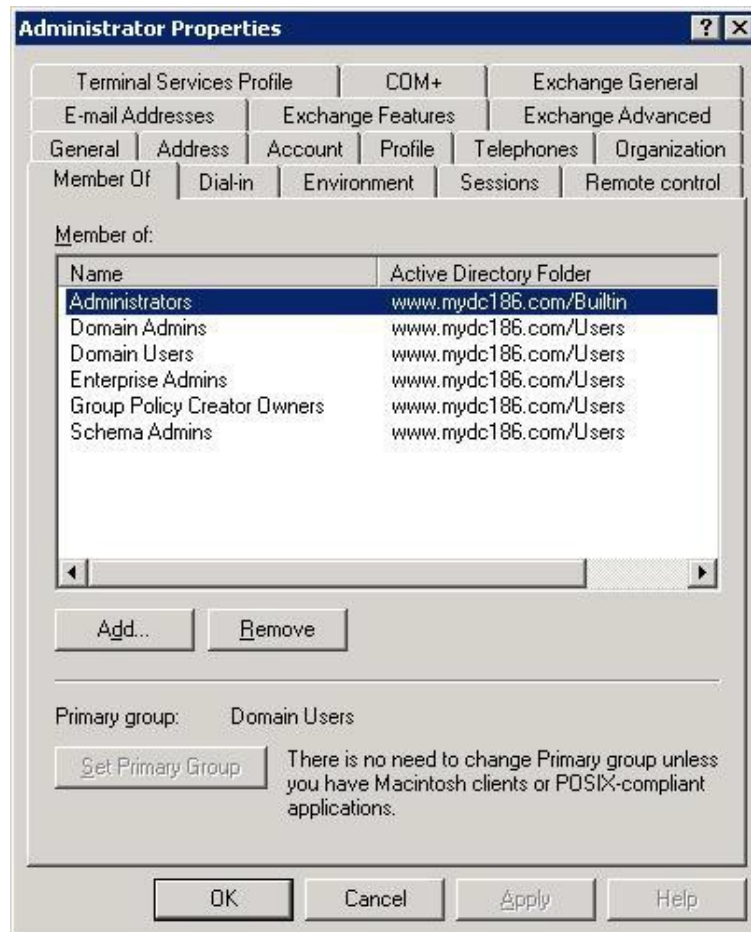
The new domain details will be verified and if correct, the domain will be successfully added. Now, Lepide Active Directory Self Service is ready to be configured as required for self-service activities.

User account privileges

The user account provided here should be a member of the following groups: Administrators, Domain Admins, Enterprise Admins, Schema Admins, Group Policy Creator and Owner.

Follow the below given steps to provide the rights mentioned above:


- 1) Go to Administrative Tools
- 2) Open Active Directory Users and Computers
- 3) Select User Properties
- 4) Click Member Of
- 5) Click Add Group
- 6) Select the following Groups: Administrators, Domain Admins, Enterprise Admins, Schema Admins, Group Policy Creator and Owner
- 7) Click Apply and then click Ok



6.1 Manage Domain

Multiple domains can be added and managed with Lepide Active Directory Self Service. Go to the manage domain section and enter the details for the domain that is to be added. Existing domain details can also be edited and a particular domain can be set as default domain.




Manage Domain



Configure New Domain Settings

*User must have administrative rights

Existing Domains

Action	Default	Domain Name	Domain Controller	User Name
 		mydc186	NDRT-EX3	administrator

7. User Enrollment

This section allows to enroll users with the software. You can send invites to users through email and ask them to enroll with the solution or bulk enroll them using CSV files.

7.1 Invite users to Enroll

You can notify domain users via email to enroll themselves in order to use features like Self Reset Password, Unlock Account, Update Active Directory Attributes, and Automatic Password Reset. You can schedule notifications to be sent at prescribed times to all unenrolled users, as per existing policies.

Schedule New Notification

You can create new notifications for sending notifications to users at scheduled time. Click to Add Notification tab to get started:

1. Provide a name for the schedule.
2. Provide Description.
3. Select the policy which is to be applied on the users who enroll themselves.
4. Select the time interval when notification is to be sent from daily, weekly or monthly options.

5. In the mail setting section, provide the sender's email address.
6. Provide a mail subject for the notification email.
7. Provide mail content that is to be delivered to users. [Edit the URL for accessing LADSS by users. The current URL (<http://localhost:7777/LADSS/UserLoginAction.do?method=populate>) is for demonstration purpose.]
8. Now, click on the 'Save' button to finish.

Enrollment Notification

Schedule Name:

New Schedule

Description:

Enrollment Notification

Select Policy:

ex7sp3 policy

Send Notification:

☐ Daily ☒ Weekly ☐ Monthly

Send notification at:

Monday 10 Hrs

Mail Settings

Send Mail From:

administrator@www.mydc186.com

Mail Subject:

Please Enroll

Mail Content:

Dear <%userName%>,

You have not enrolled yourself with Lepide Active Directory Self Service. To enroll, please visit the following
URL:<http://localhost:1025/LADSS/UserLoginAction.do?method=populate>

For enrollment, please select or write your security questions and answers with which your identity can be verified.

Save

Cancel

7.2 Bulk Enrollment

This section allows you to enroll multiple users at once using a CSV file. You can also send notifications to users who have been newly enrolled. The notification mail generally contains Question and Answer details for the user to authenticate enrollment from their behalf.

To enroll users, follow the below mentioned steps:

1. Select the policy as per which the preselected users are to be enrolled.
2. Click Browse and select the CSV file which contains user data.
3. Select the checkbox 'If already enrolled then skip enrollment' to avoid enrollment of already enrolled users.
4. Select the checkbox 'Automatically disenroll users deleted from AD' to remove enrollment of those users who have been deleted from AD.
5. Select 'Send enrollment status notification to Users' to let respective users know about their enrollment status. If selected:
 - o Provide the admin mail address from whom the notification mail will be sent.
 - o Provide a suitable email subject.
 - o Provide mail content for the body section of the mail.
6. Click Enroll to successfully enroll users in bulk.

Bulk Enrollment

Select Policy:

Import CSV file with Username, Questions and Answers.
Select CSV File:
[Download CSV](#)

☒ If already enrolled, then skip enrollment
☒ Automatically disenroll users deleted from AD
☒ Send Enrollment notification to Users

Email Notification Settings
Send Mail From:
Mail Subject:
Mail Content:

Dear <%userName%>,
Administrator has enrolled you with Lepide Active Directory Self Service with the following set of questions and answers as mentioned below.
Question : <%questions%>
Answer : <%answers%>

Download CSV

Click the 'Download CSV' option to download a blank CSV file with the correct format to enter data. Provide username, question and then answer. For multiple questions, provide question and then answer and then again next question and next answer. Check the sample CSV image below.

NOTE: In case you are working with huge number of entries, it is advised to use multiple CSV files instead of a single large CSV file.

	A	B	C	D	E	F
1	SAM Account Name	Predefined Question1	Predefined Answer1	Predefined Question2	Predefined Answer2	
2						
3						
4						
5						
6						
7						
8						

8. Policy Configuration

Policies help to preconfigure self-service actions that can be performed by domain users. Once a domain is added, a default policy gets automatically created for that particular domain. By default, self-password reset, unlock account, and on behalf actions are included. More settings such as expiry notification schedule, self-update attributes and automatic account unlock actions can be configured. This default policy can be edited or new policies can be created as per requirements.

In order to manage a policy, follow the below mentioned steps:

1. Provide a policy name.
2. Choose the domain for which policy is to be configured from the Select Domain drop-down menu.
3. Select required OU's.
4. The next step is to set permissions for the policy.
 - a) Check self-password reset option if you want domain users to reset their AD account password on their own.
 - b) Check Self Unlock Account option if you want domain users to unlock their account on their own.
 - c) Check Self Update Attributes option if you want domain users to self-update their AD attributes. You can choose which attributes can be edited.
 - d) Check Reset Password on behalf of User option if you want domain users to reset password on behalf of their coworkers.
 - e) Check Unlock Account on behalf of User option if you want domain users to unlock account on behalf of their coworkers.
 - f) Check Set Password Expiry Notification option to preset password expiry reminder.
 - g) Check Automatic User Account Unlock option to allow software to automatically unlock expired AD accounts after a specified time interval.
5. Click 'Save' to finish policy configuration.

Policy Configuration

Policy Name:

Select Domain:

Select OU(s):

Set Permissions

<input checked="" type="checkbox"/> Self Password Reset	<input checked="" type="checkbox"/> Self Unlock Account	<input checked="" type="checkbox"/> Self Update Attributes [Manage self update attributes]
<input checked="" type="checkbox"/> Unlock Account on behalf of User	<input checked="" type="checkbox"/> Reset Password on behalf of User	<input checked="" type="checkbox"/> Set Password Expiry Notification [Create password expiry notification schedule]
<input checked="" type="checkbox"/> Automatic User Account Unlock		

Schedule Automatic User Account Unlock

☐ Daily ☐ Weekly ☒ Monthly

Unlock Account at: Hrs

NOTE: More than one policy cannot be created on a single OU. One OU can be a part of only one policy in a particular Domain. For ex, 'Program data' can be included in only one policy. For assigning any changes concerning 'Program Data', edit the existing policy or delete the existing policy and create a new policy with required OUs.

9. Multifactor Authentication

Lepide Active Directory Self Service allows users to authenticate using multiple options and validate their account for unlock and reset activities. Users can validate through:

1. Security Question and Answer
2. One Time Password

Before performing any configuration, select the policy for which these authentication settings will be applicable. Select the appropriate policy from the list of configured policies provided in the Select Policy drop-down menu.

9.1 Security Question and Answer Configuration

Select Policy:

Security Question & Answer Configuration

☒ Enable Ques & Answer Configuration

Number of Predefined Questions (less than 10 allowed)

Number of User Defined Questions (less than 10 allowed)

Number of Characters in User Defined Question (min: 5 and max: 225)

Number of Characters in an Answer (min: 5 and max: 225)

Question and Answer Settings

Enter the details as given in the table below to perform Q&A settings.

Number of Predefined Questions	Mention the number of predefined questions that you want the domain users to select while enrolling. (Less than 10 allowed)
Number of User Defined Questions	Mention the number of user-defined questions that you want the domain users to create. (Less than 10 allowed)
Number of Characters in User Defined Question	Mention the number of characters that a user defined question can contain. (Minimum 5 characters and maximum 225 characters allowed)
Number of Characters in an Answer	Mention the number of characters that an answer can contain. (Minimum 5 characters and maximum 225 characters allowed)

9.2 One Time Password Configuration


This section allows to configure OTP settings for self-service actions.

You can either enable sending OTP through both SMS and email or any one of them. If needed, the OTP notification text can be edited.

You can also use the SMS and email settings link to perform required settings (if not done previously).

☒ Enable SMS Configuration


text: `Your one time password for <%activity%> is <%OTP%>.`

 SMS Settings

☒ Enable Email Configuration

text: `Dear <%userName%>,

Active Directory Self Service one time password
for <%activity%> is <%OTP%>.`

 E-mail Settings

9.3 Authentication Mode

This option appears when both security questions and OTP have been enabled. You can choose whether users authenticate themselves with both Q&A and OTP or just with any one of them.

Select Authentication Mode

- ☒ Any One (Select this option to allow users authenticate either through OTP or Q&A)
- ☐ Both (Select this option to make users authenticate with both OTP and Q&A)

9.4 Disenrollment

Check this to dis-enroll all currently enrolled users with previous policies. If you have made some changes in the authentication modes or created new policies and you wish users to register as per the new settings, you can select this option to automatically dis-enroll them.

☒ Dis-Enroll Users (All previously enrolled users will be dis-enrolled & a notification will be sent to re-enroll.)

*Send Mail From:

Mail Subject:

*Mail Content:

Dear <\$userName\$>,
There are some changes in the authentication policy so you have to enroll yourself with Active Directory Self Service again as per new authentication level. To enroll, please visit the following URL: <https://192.168.10.178:443>
you complete enrollment, you can-
(a) Reset your forgotten password yourself.
(b) Unlock your account in case you are locked out of your computer.

Users will receive a notification email informing them that they need to re-enroll with LADSS. You can select the mail sender and edit the email subject and content.

NOTE: The 'Send Mail From' option (email sender's profile) is valid for both sending the OTP and email notification.

10. E-mail Server Settings

You need to configure Mail server for sending Scheduled Reports from the software. You can edit the settings later if you want to use another Server as per your mail server. Multiple exchange servers can also be configured for using specific mail servers for different domains.

To perform mail server settings, click E-mail Server Settings option under Configuration tab.

E-Mail Server Settings


Exchange Mail Server:

Port:



☐ Use SSL

☐ Use SMTP Authentication

From Address:

 send test mail

Saved Settings

Actions	Exchange Mail Server	Sender Address	Port	Configured SSL
 	192.168.10.186	administrator@www.mydc186.com	25	No

In order to configure email server settings, follow the below mentioned steps:

1. Exchange Mail Server: Type the Exchange Mail Server Name or IP Address.
2. Port: Enter mail server port number.
3. Use SSL: Enable secure socket layer connection if applicable.
4. SMTP Authentication: Provide SMTP Username and SMTP Password in the given fields.
5. From Address: Provide sender's Email address in the given field. This email address will be used for sending all the scheduled reports.

Click Save to complete adding email server. It is recommended that you use Send Test Email button to test the mail server configuration.

11. SMS Server Settings

In order to send OTP via SMS, you need a GSM modem and a SIM card for communication. Install the modem on the system where the software is installed. SMS data charges will apply as per your service provider.

NOTE: Please use a GSM modem only to successfully send SMS to recipients.


In order to configure SMS server settings, follow the below mentioned steps:

1. The SMS provider is by default selected as GSM Modem.
2. Enter the COM Port number as 3.
3. Enter the number of attempts to be made for sending the OTP.
4. Enter the time-out value until which the software will attempt sending the SMS.
5. Enter the Baud rate value. It is the rate at which information is transferred in your communication channel.
6. Enter a valid recipient mobile number using which the SMS will be sent.

Click Save to complete the SMS settings. It is recommended that you use Send Test SMS button to test the SMS server configuration.

SMS Server Settings

SMS Provider	GSM Modem	
COM Port	<input type="text" value="3"/>	ex: 1/ 2/ 3
No. of Attempt	<input type="text" value="2"/>	
Time-out	<input type="text" value="100"/>	millisecond
Baud Rate	<input type="text" value="115200"/>	from modem settings
Recipient Mobile No.	<input type="text" value="9899113040"/>	

 send test sms

Save

Cancel

12. Connection Settings

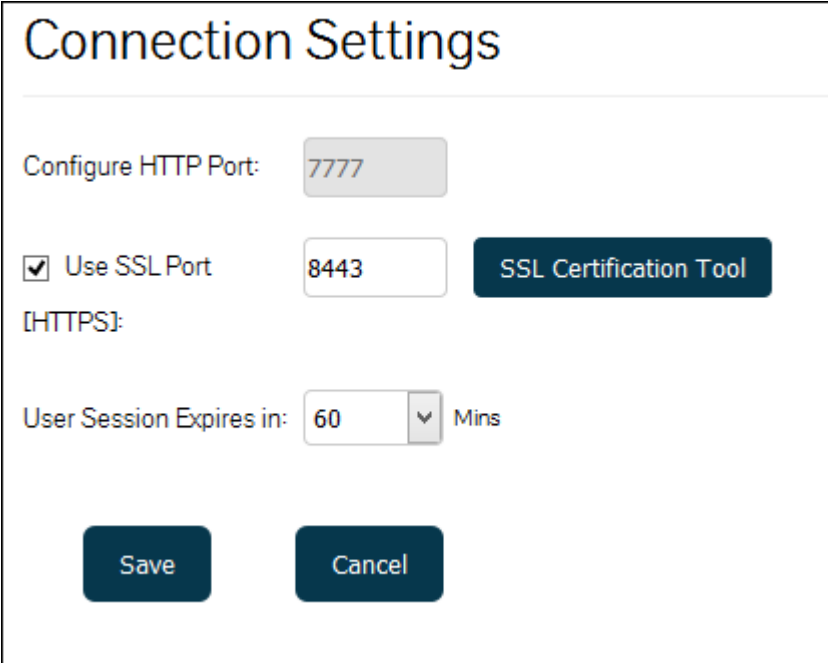
Web Server settings can be updated to change port number. By default, the preconfigured HTTP port number is 7777. The given port number is used to connect with the software from anywhere in the domain.

Configure HTTP Port: You can change and enter another port number as per your priorities.

Set user session expiry duration: Select the time interval after which user session will automatically expire if no activity has been performed in the selected time.

SSL Port [HTTP]: Select the Use SSL Port [HTTPS] check box if Secure Socket Layer (SSL) is used in your network. LADSS automatically uses a default certificate to populate the HTTPS port field.

To import your own SSL trusted certificate, click on the 'SSL Certification Tool' tab. Enter the required company details and generate a CSR file. Follow the onscreen process to successfully incorporate SSL security.



The screenshot shows a 'Connection Settings' dialog box with the following elements:

- Configure HTTP Port:** A text input field containing the value '7777'.
- Use SSL Port [HTTPS]:** A checked checkbox followed by a text input field containing '8443'.
- SSL Certification Tool:** A dark blue button located to the right of the SSL port input field.
- User Session Expires in:** A text input field containing '60' followed by a dropdown arrow and the text 'Mins'.
- Save:** A dark blue button at the bottom left.
- Cancel:** A dark blue button at the bottom right.

13. Password Synchronization

Password Synchronization enables the synchronization of third party applications and allows you to reset those particular passwords from the solution itself. Currently, password sync is supported for Office 365, IBM AS400 and Google Apps.

Follow the steps below to enable password synchronization:

1. Enter profile name of your choice.
2. Provide a description.
3. Select the policy on which the settings will be applicable.
4. Now select the Application type.

Password Synchronization

Profile Name	<input type="text" value="IBM"/>
Description	<div><div>sync settings for IBM profile.</div><div>30 x 200</div></div>
Select Policy:	<div>3to8 policy x</div>
Application Type	<div>IBM AS400</div>

NOTE: Application type details are different for every application. Below is the step-by-step process for each application.

Application type details for IBM

1. Enter IP Address of your IBM Server.
2. Enter Username of the server account.
3. Enter Password

Application Type Details

IP Address

178.249.3.54

User Name

santosh

Password

••••••••

Test Connection

Application type details for Google Apps

1. Browse and select the P12 Key File. To generate a P12 key file, refer thislink: <https://www.lepide.com/guide/ladss-generate-P12-key.pdf>
2. Enter the service account email address.
3. Enter Domain name
4. Enter Username

Application Type Details

P12 Key File

Browse...

Help

Service Account Email

kali-271@mayur-1229.iam.gserviceaccount.com

Domain Name

exportnotes.co.uk

User Name

sudesh@exportnotes.co.uk

Test Connection

Application type details for Office 365

1. Enter the domain name of your Office 365 account.
2. Enter a valid username
3. Enter password

Application Type Details

Domain Name

lepide.onmicrosoft.com

User Name

administrator@lepide.onmicrosoft.com

Password

••••••••

Test Connection

You can test the connection in every case after entering respective details.

Account Link methods

1. Link AD users automatically: Use this method to link all users within the selected policy automatically.
2. Link as per user's request: Use this method to link accounts when a particular user requests for synchronization.

Account Link Methods

☒ Link AD Users Automatically

☐ Link As Per User's Request

SaveCancel

Click save to finish the password sync settings.

14. Backup/Restore Database

The Backup/Restore Database settings section comprises of three sub-sections:

1. Create New Backup
2. Set Schedule Time
3. Restore Backup

14.1 Create New Backup

In this section you can create a backup of the application's existing database. Running a database backup will create a database export file and store it in your system.

To create a backup you need to click on the 'Backup' button.

Lepide Active Directory Self Service stores the backup in a zipped file format in its system files where the solution was installed. For example: *C:\Program Files\Lepide Active Directory Self Service\tomcat\bin\backup*

Create Backup

Create backup of current settings

Backup

NOTE: If any error message appears during the backup process, do not attempt to restore from that backup.

14.2 Set Backup Schedule

To schedule running a database backup you need to execute the following steps:

1. Select the Daily, Weekly or Monthly option.
2. Select the backup process start time from the dropdown.
3. Click on the Set button to complete the process.

You can enable or disable the automatic backup schedule option by using the given checkbox.

☒ Enable/Disable automatic backup schedule.

Set schedule time:

☐ Daily ☒ Weekly ☐ Monthly

Generate at: Friday 17 Hrs

Set

14.3 Restore Backup

In this section you can use an existing backup to restore the application's database.

Use the Browse button to select a backup file. Click the Restore button to restore the application's database using backup.

Restore

Import Database Backup File to restore previous settings

Select Backup File:

[Click here to import data from older version of LADSS](#)

15. GUI Rebranding

You can customize the application's GUI by using your company's logo and banner image. To rebrand the GUI of the application you need to execute the following steps:

1. Click on the Browse button in the Select Banner Image field and browse a Banner Image file as per your choice. Click on the Set button to upload the image.
2. Click on the Browse button in the Select Login Image field to browse a Login Image file as per your choice. Click on the Set button to upload the image.

GUI Rebranding

(Image size should not exceed 50kb and Dimension should not be more than 105 x 55 pixels)

Select Banner Image:

(Image size should not exceed 50kb and Dimension should not be more than 150 x 95 pixels)

Select Login Image:

16. Captcha Settings

You can enable captcha on the login pages and other self-service activity pages to ensure more authenticity and an added layer of security.

Select the first checkbox to enable captcha on the Admin Login page.

For enabling captcha on rest of the options, first select the respective domain.

1. Select the second checkbox to enable captcha on the User Login page.
2. Select the third checkbox to enable captcha on the Unlock Account operation page.
3. Select the fourth checkbox to enable captcha on the Reset Password operation page.

Captcha Settings

☒ Enable captcha on admin login page

Select Domain

☒ Enable captcha on user login page

☒ Enable captcha on unlock account operation page

☒ Enable captcha on reset password operation page

Save

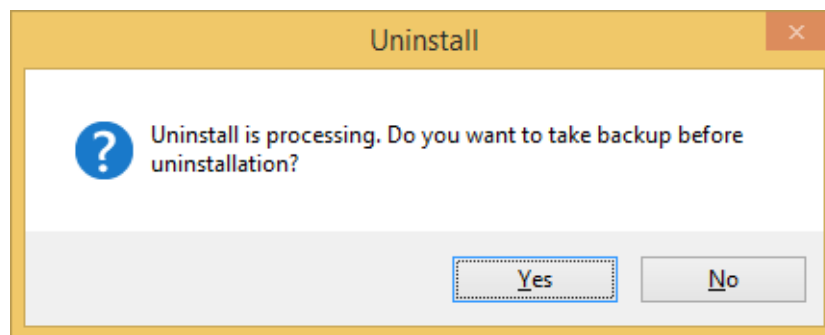
Cancel

17. Uninstalling the Software

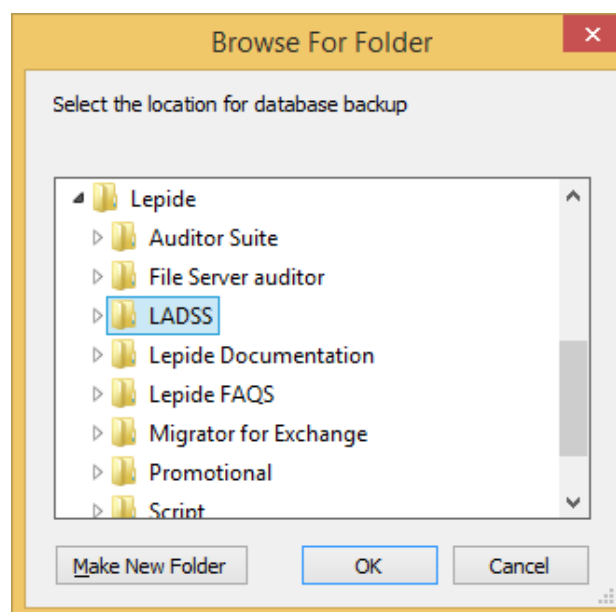
NOTE: Before you start uninstalling the solution, make sure that the software is not running.

To remove Lepide Active Directory Self Service, follow the instructions below:

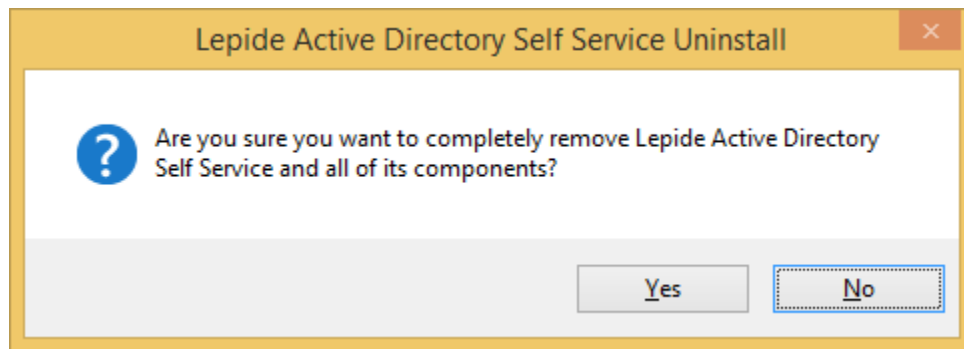
1. Click Start, go to Control Panel/Settings. The Control Panel window appears.
2. Double click the Add or Remove Programs icon or Program and Features option (Windows 8 and above). A list of the programs installed on your computer appears.
3. Select Lepide Active Directory Self Service and click the "Uninstall" button. A backup instruction message appears onscreen before un-installing the software.



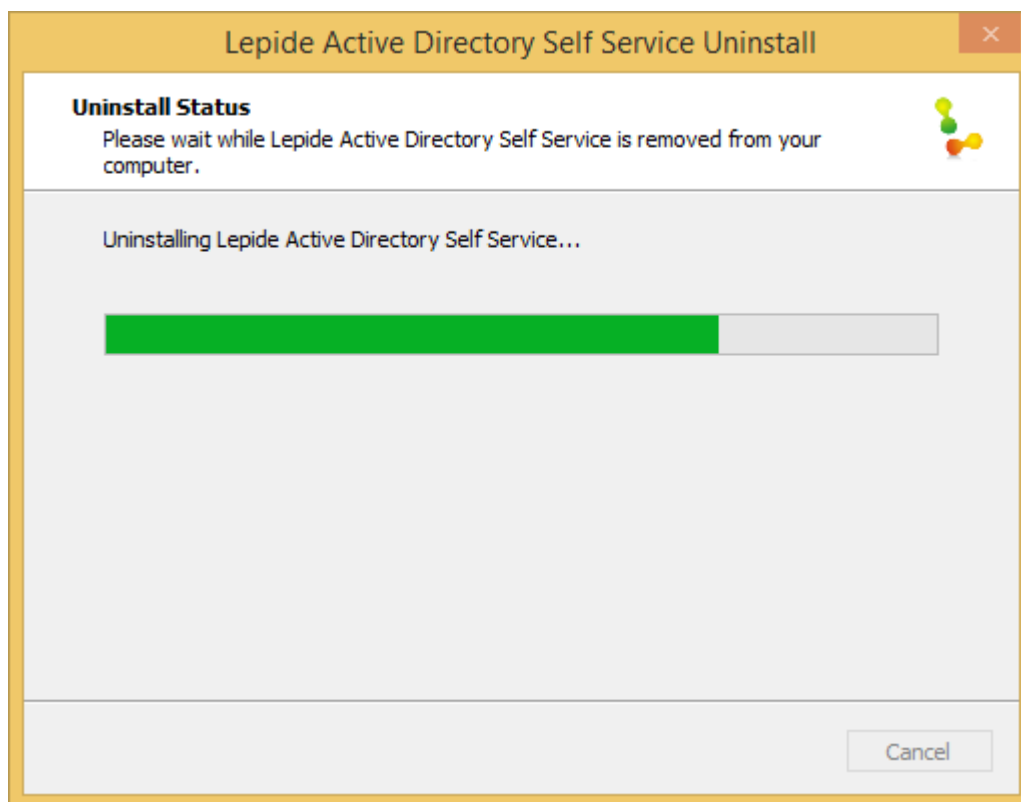
4. Click the Yes button to take a backup at your preferred location and click Ok.



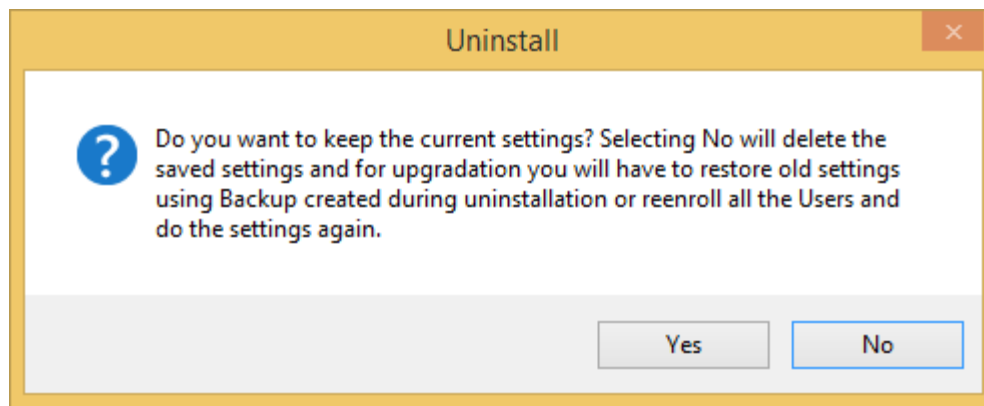
5. Click 'Yes' to start the un-installation process.



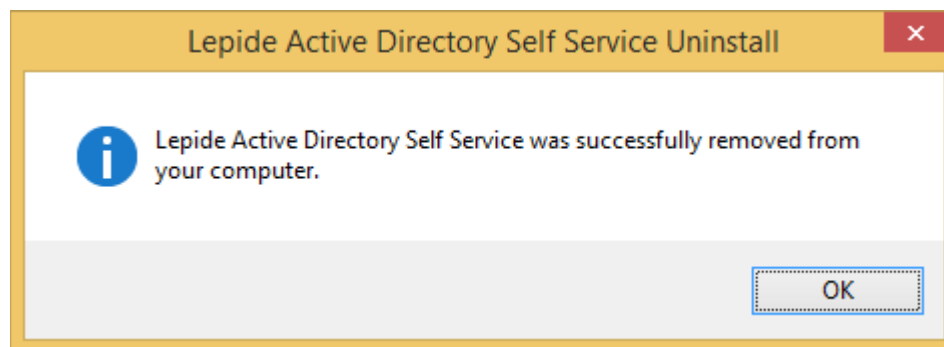
6. The uninstallation process is in progress.



7. The solution confirms whether you wish to keep the current settings or delete them. Click Yes/No as per your preference.



8. Lepide Active Directory Self Service will be successfully uninstalled from your computer system.



To remove the remaining elements, delete its program installation folder manually and then empty the Recycle Bin as well.

After following the above steps, Lepide Active Directory Self Service will be uninstalled successfully from your computer system.

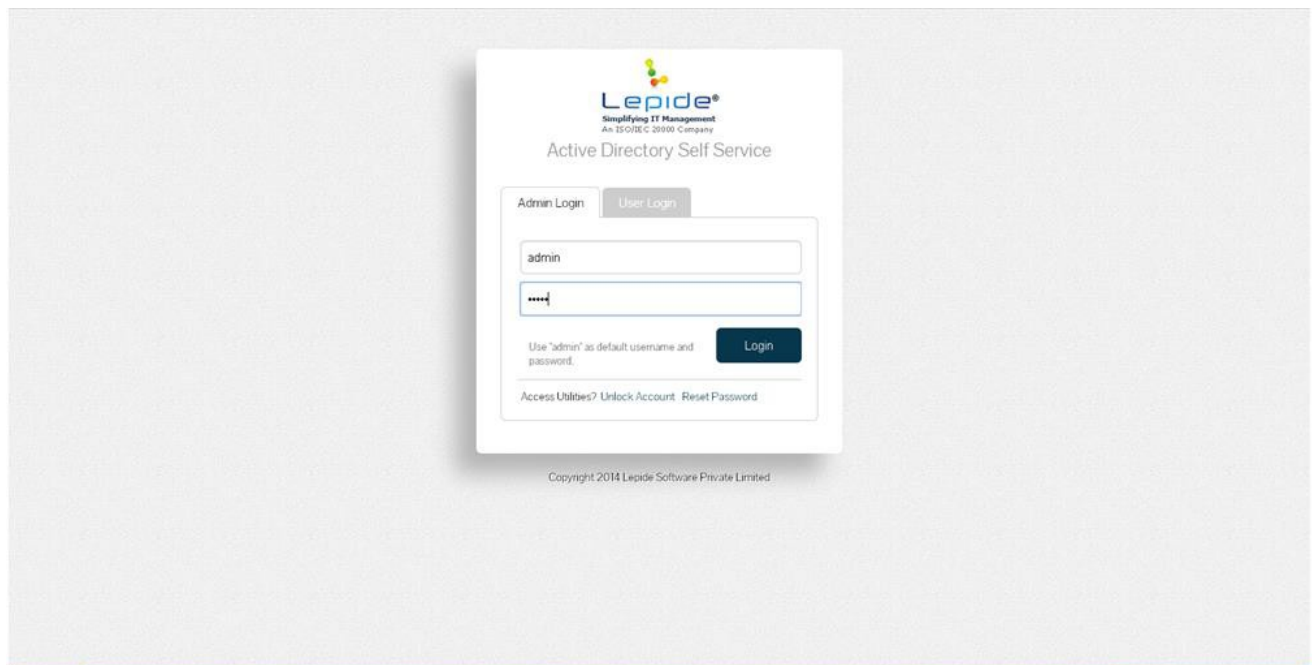
18. License Activation

The free version of Lepide Active Directory Self Service offers a license for 50 Users only. When enrolling more than 50 Users, you will need to purchase additional licenses.

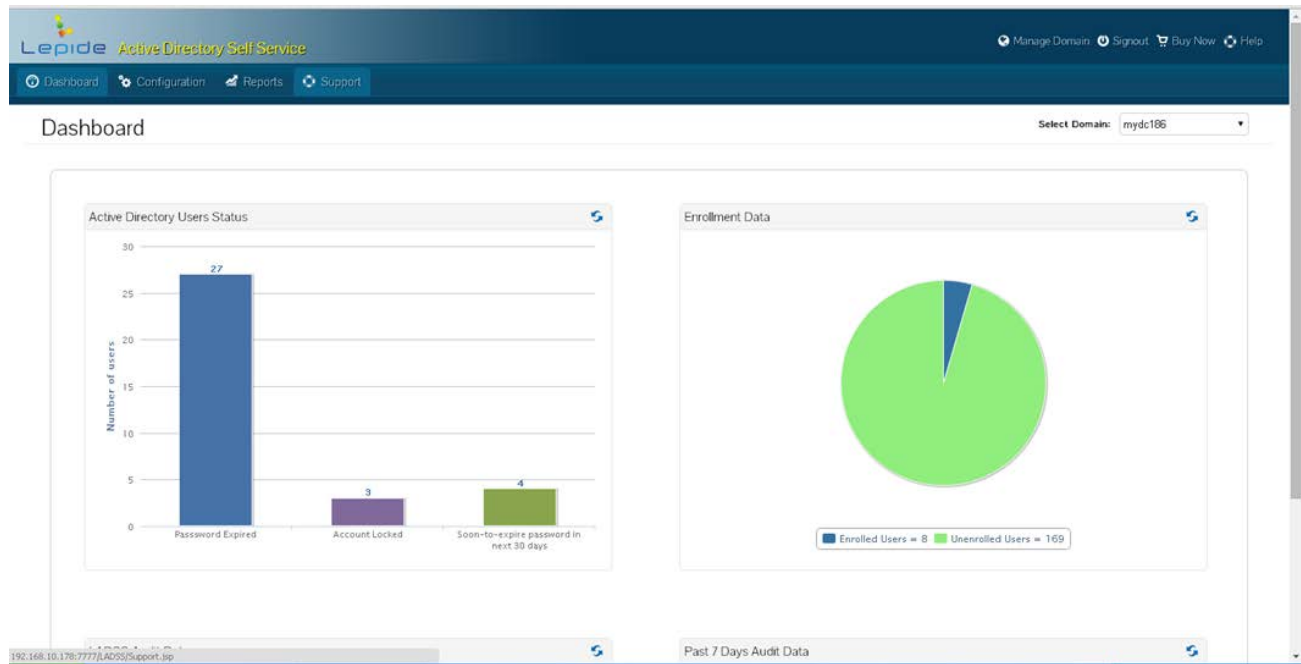
To purchase licenses, contact our sales team at sales@lepidex.com.

If you are using the free version of the product, follow these steps to purchase a license and activate it following these steps:

1. Open the web interface of software and login with administrator credentials.



2. Dashboard is the default screen that opens up.



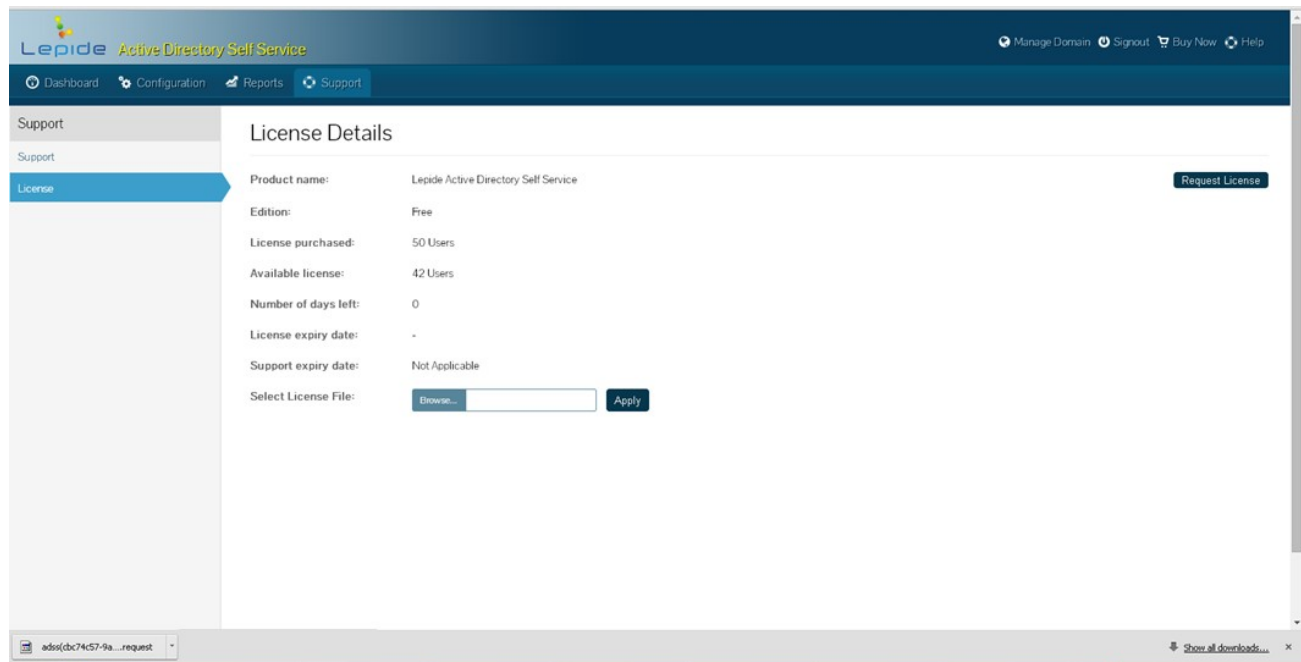
3. Go to the Support tab and click on License in the left pane.

License Details

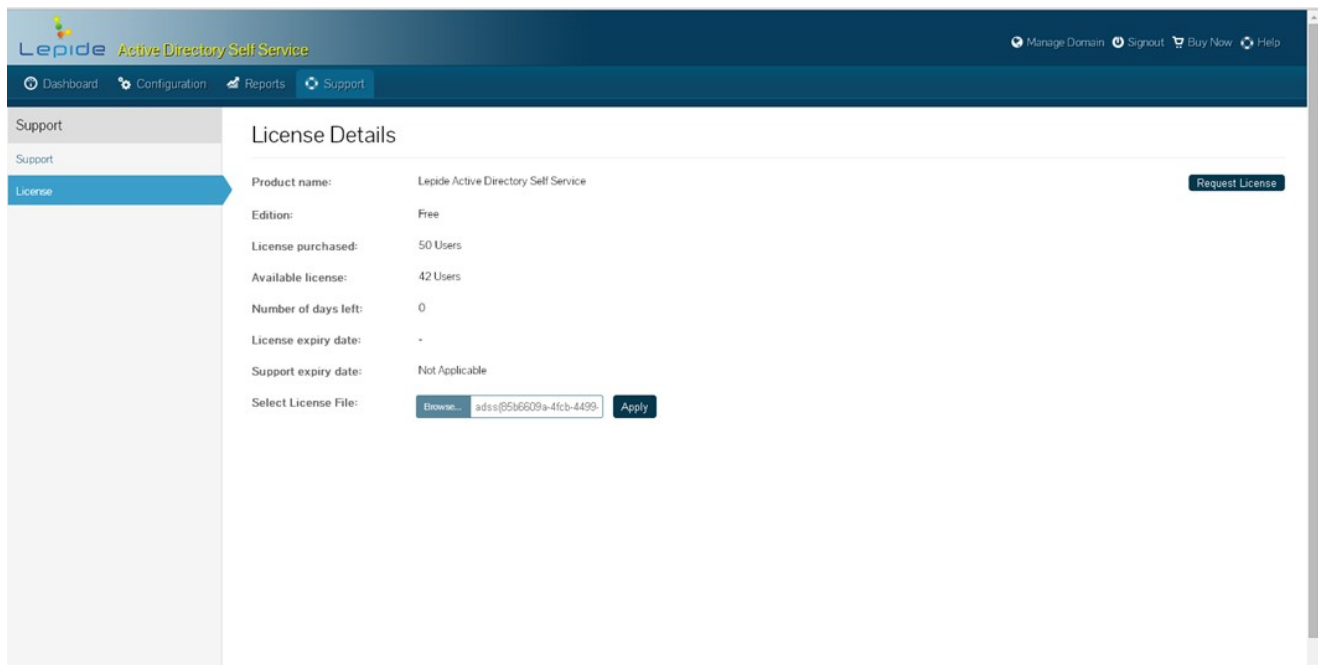
Product name:	Lepide Active Directory Self Service	Request License
Edition:	Free	
License purchased:	50 Users	
Available license:	42 Users	
Number of days left:	0	
License expiry date:	-	
Support expiry date:	Not Applicable	
Select License File:	<input type="text"/> Browse... Apply	

Copyright 2014 Lepide Software Private Limited

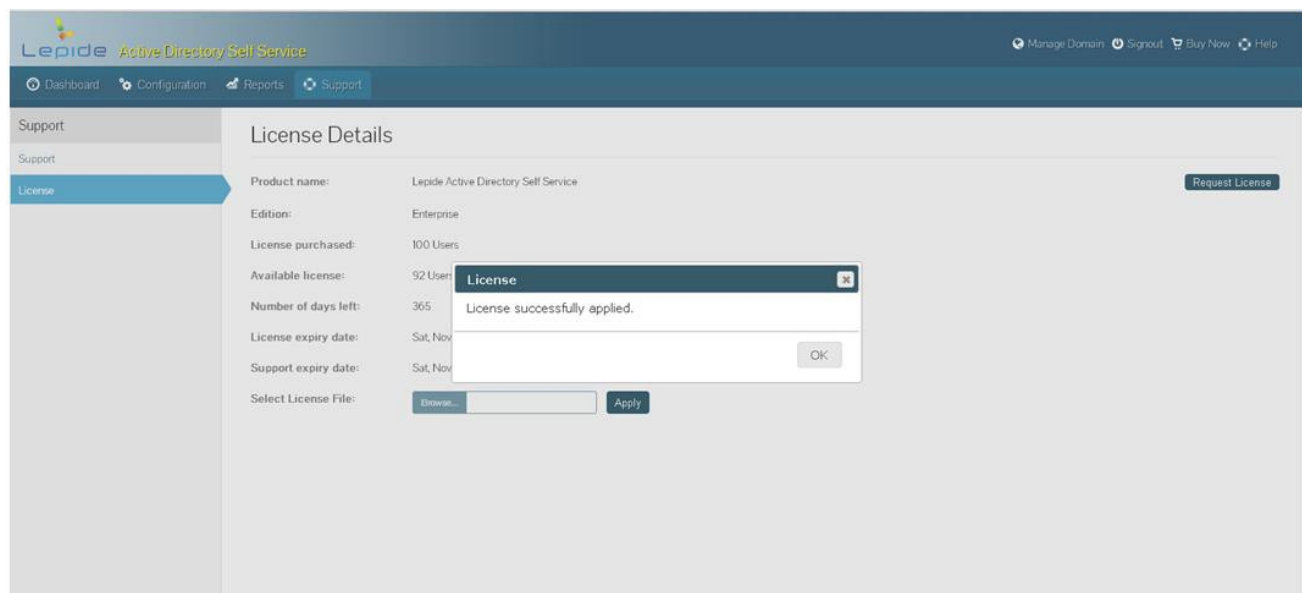
4. Click on the Request License link on the right-top corner. License request file is saved by default on this location: "C:\Documents and Settings\User\My Documents\Downloads" by the name of "adss(alphanumeric code).request".
5. Send this file to the Lepide Software sales team at sales@lepidex.com.
6. Lepide Software will send you a license activation file as per the license purchased.
7. Save that file to the local disk.
8. Open software web-interface and Go to the Support-> License page. And click on Browse button against Select License File field.



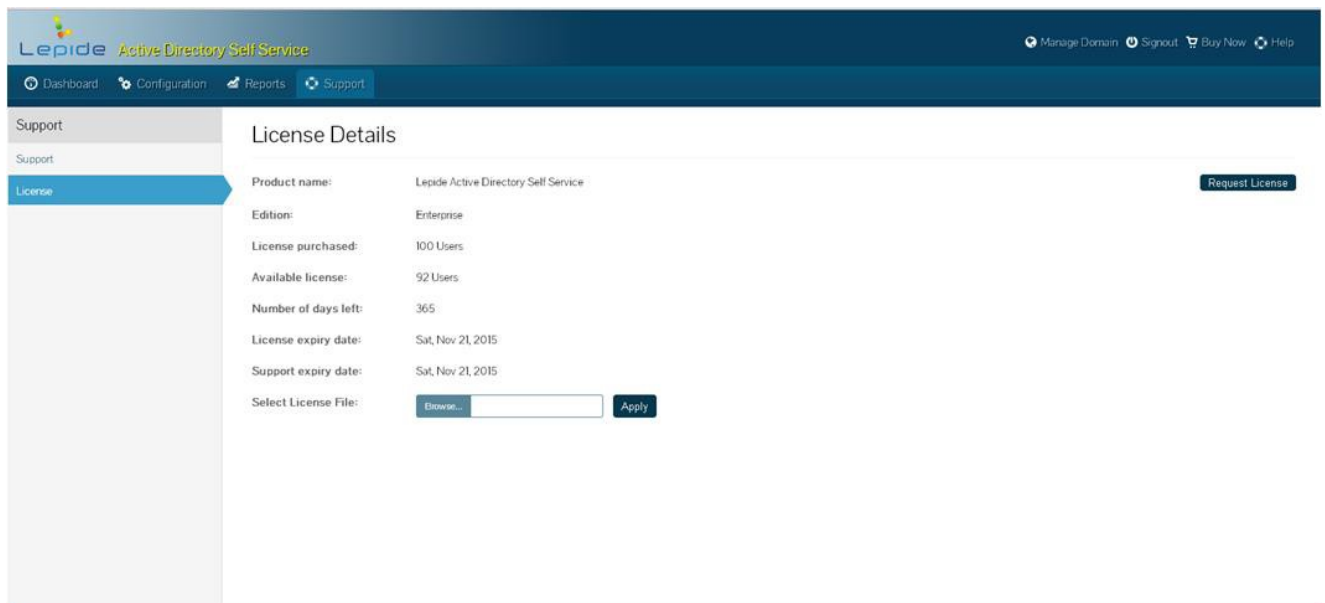
9. Locate and add the license activation file to the path provided.



10. Click on the Apply button to activate the license. The following message appears.



11. Click on Ok and license details will be displayed on the screen:



Thus, you can successfully activate the license for Lepide Active Directory Self Service.

19. Conclusion

By following the steps in this guide, Lepide Active Directory Self Service can be easily configured and used to manage user login and attribute details and allow end users to perform self-service actions on their own.

To read more visit: <http://www.lepide.com/active-directory-self-service/>

For related queries, you can contact us at:

Helpline: +1-800-814-0578

For support or any other queries, drop a mail at:

For General Queries: contact@lepide.com

For Sales: sales@lepide.com

For Technical Support: support@lepide.com

20. Warranty Disclaimers and Liability Limitation

Lepide Active Directory Self Service, and any and all accompanying software, files, data and materials, are distributed and provided AS IS and with no warranties of any kind, whether expressed or implied. In particular, there is no warranty for any harm, destruction, impairment caused to the system where Lepide Active Directory Self Service is installed. You acknowledge that good data processing procedure dictates that any program, including Lepide Active Directory Self Service, must be thoroughly tested with non-critical data before there is any reliance on it, and you hereby assume the entire risk of all use of the copies of Lepide Active Directory Self Service covered by this License. This disclaimer of warranty constitutes an essential part of this License.

In addition, in no event does Lepide Software Private Limited authorize you or anyone else to use Lepide Exchange Recovery Manager in applications or systems where Lepide Exchange Recovery Manager failure to perform can reasonably be expected to result in a significant physical injury, or in loss of life. Any such use is entirely at your own risk, and you agree to hold Lepide Software Private Limited harmless from any and all claims or losses relating to such unauthorized use.

21. Trademarks

Lepide Active Directory Self Service is a copyright work of Lepide Software Private Limited. Windows 95®, Windows 98®, Windows ME®, Windows NT®, Windows XP®, Windows Vista®, Windows 7®, Windows 8®, Windows 8.1®, Windows 10®, Windows 2000 Server®, Windows 2000 Advanced Server®, Windows Server 2008®, Windows Server 2008 R2®, Windows Server 2012®, Windows Server 2012 R2®, Office 365®, Exchange 2000 Server®, Exchange Server 2003®, Exchange Server 2008®, Exchange Server 2010®, Exchange Server 2013®, Microsoft Office®, Microsoft Outlook®, Microsoft Outlook 2000®, Microsoft Outlook 2003®, Microsoft Outlook 2007®, Microsoft Outlook 2010®, Microsoft Outlook 2013®, PST, OST, OWA®, Outlook Web Access®, Microsoft Word®, Exchange Management Tools, Exchange 2010 Management Tools®, Exchange 2013 Management Pack®, .NET®, IIS®, Windows PowerShell®, Microsoft Management Console®, and Windows Management Framework® are registered trademarks of Microsoft Corporation. Intel and Pentium are the registered trademarks of Intel Corporation. All brand names, product names, logos, registered marks, service marks and trademarks appearing in this document are the sole property of their respective owners. These are purely used for informational purposes only. We have compiled a list of such trademarks but it may be possible that few of them are not listed here.