



Datasheet

Lepide Active

Directory Self Service

Lepide ADSS

Lepide Active Directory Self Service is a simple web-based solution to allow IT teams to delegate tasks such as password resets and account unlocks.


This solution also provides the ability to authorize co-workers to perform these tasks without having to call IT.

Ultimately this solution makes it easier for the user, easier for the administrator and easier for the whole organization to handle the task of updating Active Directory.

Key Features

- ✓ Gives IT teams the power to delegate Active Directory updates and password resets to the users.
- ✓ Provides the ability for users to unlock accounts either via GINA/CP or any web enabled device.
- ✓ Spot specific trends such as account lockouts, password resets, enrolment data, users not enrolled, overall activity over last seven days and user status with our intuitive dashboard.
- ✓ Sends automated notification reminders to users when their passwords are due to expire.



- 
- ✓ Predefine within the solution whether the user has no access, read only or full control across any of the following Active Directory Attributes – general, contact and address.
 - ✓ Provides authentication through either OTP SMS or challenge/response.
 - ✓ Provides the ability to specify account unlock periods
 - ✓ Provides bulk enrolment – import the relevant enrolment details into a CSV file with the challenge response information into the solution and we will automatically update and notify all the users of their enrolment along with instructions for use.
 - ✓ Provides comprehensive audit and enrolment reports straight to your inbox showing details such as enrolment, self-service actions performed by users, password expiry and lockout details.
 - ✓ Allows end users to perform self-service activities, update their Active Directory details and allows them to delegate certain tasks to other authorized employees.
 - ✓ Allows end users to reset their AD account passwords and enables the synchronization of third-party applications and resetting those particular passwords from the tool itself

Requirements and Supported Systems

Hardware Requirements

- P3 Processor
- 1.0 GHz or later version
- 2 GB of RAM
- 400MB of disk space

Supported Operating Systems

Windows 10 / Windows 8.1 / Windows 8 / Windows 7 / Windows XP / Windows XP Professional x64 Edition / Windows Vista / Windows Server 2008 R2 / Windows Server 2012 / Windows Server 2012 R2 / Windows Server 2016 / Windows Server 2019

GINA/CP Support

- All Windows Server version up to and including Windows Server 2019.
- All Windows versions from Windows XP up until Windows 10.

Supported Web Browsers for TLS

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

- Internet Explorer – 8.0 (installed on Windows XP SP3, Windows 7 and above)
- Internet Explorer – 9.0 to 11.0 (All Windows OS versions)
- Mozilla Firefox and Google Chrome (All Windows OS versions)

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

