ManageEngine
ADSelfService Plus

Scaling ADSelfService Plus to meet your specific business requirements

www.adselfserviceplus.com

The Scalability of ADSelfService Plus

ADSelfService Plus is an integrated Active Directory (AD) self-service password management and single sign-on solution fit for enterprises of all sizes. This solution gives users the right amount of autonomy without compromising on security and helps mitigate the time spent on resolving password-related issues by automating password resets and account unlocks.

Scope of this document

This document's purpose is to outline how ADSelfService Plus can scale to any enterprise environment and will be useful to product evaluators and customers looking to upgrade the solution for their expanded network.

Though the scalability requirements of every organization are not the same, we've listed some of the most common requirements and provided solutions for each of them. This document talks about ADSelfService Plus' scalability for:

1. Architecture
2. Features

1. ADSelfService Plus' scalable architecture

A. Server migration

When your organization increases in size, you might move your ADSelfService Plus installation to a new server that facilitates better performance. With ADSelfService Plus' Server Migration capability, you can move your existing installation from one server to another.

Learn more about server migration.

B. Database migration

ADSelfService Plus comes packaged with an open-source PostgreSQL database. If your organization is already using other databases, no problem — ADSelfService Plus supports database migration from PostgreSQL to MS SQL and MySQL.

Moreover, there are two different ways you can migrate databases in ADSelfService Plus: you can either choose to back up ADSelfService Plus' data from the old database and restore it in the new database, or simply create a new database in the new server. Learn more about database migration.

C. High availability

It's common knowledge that downtime on a critical service has a negative impact on efficiency. This spurred the concept of high availability, where ADSelfService Plus' servers are structured so that at least one is available at all times.

ADSelfService Plus utilizes automated failover to support high availability in case of system and product failures. Essentially, what this means is that when the ADSelfService Plus service fails on one machine, another instance of ADSelfService Plus running on another machine automatically takes over.

D. MS SQL Server clustering

To make sure that your organization always has access to its databases, ADSelfService Plus supports MS SQL clustering, meaning data in shared storage can be accessed by different servers.

For instance, consider a single MS SQL Server instance running on the active server of a cluster, and a passive server is available to take over if needed. Now, assume that the active server stops working because of a power outage. The passive server, after a predetermined delay, assumes that the active server has failed and initiates a failover. Due to the failover, the passive server (now the active server) takes control of the data in the shared location (there is one copy of the data, and it does not move).

E. Increased number of domain controllers (DCs)

The number of DCs allocated per domain always depends on the number of users and logins made to that domain. When your organization increases in size, so does the number of DCs. But an increase in the number of DCs in your organization doesn't necessarily translate into reduced replication latency.

If a domain user resets their password through a DC and immediately logs into another DC at a different site, the logon would fail as the other DC wouldn't have the new password. It takes time for changes to be applied across DCs.

ADSelfService Plus' Site Based DC feature ensures changes made by users through the self-service portal are updated in AD without any delay by assigning DCs to organizational units (OUs). When a user performs a self-service operation using ADSelfService Plus, the data is then updated in the DCs assigned to that OU.

F. Increased number of domains

Rapidly growing organizations are bound to have users with multiple accounts in multiple AD domains to effectively manage resources. To prevent unauthorized access to resources, your organization might decide to not establish trust between AD domains. In other words, when users reset their password in one domain, that change won't be reflected in other domains, meaning users have to remember multiple passwords.

Implementing ADSelfService Plus' Password Sync feature helps your organization automatically synchronize password changes between multiple AD domains. That is, users would only have to use a single password to access all their domain accounts.

Moreover, ADSelfService Plus' Technician feature helps effectively manage your AD domains by allowing your administrators to delegate certain or all administrative tasks to end users in a domain.

2. Feature scalability

A. License management

The abstract nature of software assets makes them much more tedious to manage than their hardware counterparts. For businesses that experience fluctuations in their staff throughout the year, effective license management becomes a priority.

How can ADSelfService Plus help with effectively managing its licenses?

You can restrict the licenses of inactive users so they won't be able to access ADSelfService Plus. By doing so, you can repurpose these restricted licenses and give them to new employees. You can also reinstate the restricted users if needed.

To convert ADSelfService Plus' evaluation license to an annual or perpetual subscription without experiencing any outages, contact our support team.

B. Avoid simultaneous logins

As an administrator, you can set a specific number of days after which user passwords expire. ADSelfService Plus' Password Expiration Notifier helps you send emails to users whose passwords are about to expire. Users will be prompted to change their AD passwords by clicking on the access URL sent in the email.

Consider this scenario: You have 5,000 domain users who are notified at the same time that their passwords will expire in five days. Of these 5,000, 1,000 of them simultaneously log in to change their passwords. This activity could negatively impact user performance.

Instead of sending all 5,000 emails at once, configure schedulers to notify different sets of users on specific days along with the number of times you want them to be notified. For instance, you can configure a scheduler to send password expiration notifications to day shift employees (segregated based on group and OU memberships) when there are seven days until password expiration, and again when there are four days until password expiration. Meanwhile, you can configure another scheduler to send notifications to night shift employees when there are eight days until password expiration, and again when there are three days until password expiration. This ensures that users will be notified to change their passwords at different intervals, making it unlikely that users will all attempt this activity at once.

C. Force enrollment of un-enrolled users

With the hectic schedules employees usually have, it's not uncommon for them to forget to enroll for self-service password management. When plain reminder emails fail, you may need a much stronger deployment policy.

With ADSelfService Plus, you can enroll users in bulk without their intervention. Import enrollment data through a CSV file or from an external database to enroll multiple users in a matter of minutes.

Import enrollment data from a CSV file or through an external database.	
Users	**Estimated time to import enrollment data (in minutes)**
1,000	17
5,000	83
10,000	174
20,000	339

D. Generating reports

In-depth reports on various user activities helps you gain control over the various processes in your organization. With this in mind, ADSelfService Plus provides several reports that offer a holistic view the status of users' passwords in all connected domains.

Take a look at the table below to see how quickly ADSelfService Plus can generate reports, even with an increased number of users.

Generating reports in ADSelfService Plus	
Users	**Estimated time taken to generate a report (in seconds)**
1,000	0.3
5,000	0.6
10,000	1.1
20,000	1.9

Hardware and software resources used

The above tests have been performed using the following system resources:

Hardware resources	
Processor	Intel i7
RAM	16GB
Disk space	200GB

Software resources	
Server	Windows 2012 R2
Client	Windows 8

Supported Browsers

- Internet Explorer 7 and above.
- Firefox 4 and above.
- Google Chrome 10 and above.

About ManageEngine ADSelfService Plus

ManageEngine ADSelfService Plus is an integrated self-service password management and multi-factor authentication solution. It offers self-service password reset and account unlock, endpoint multi-factor authentication for machines, VPN, and OWA logins, single sign-on to enterprise applications, Active Directory-based multi-platform password synchronization, password expiration notification, and password policy enforcer. It also provides Android and iOS mobile apps that facilitate self-service for end users anywhere, at any time. ADSelfService Plus helps reduce IT expenses associated with help desk calls, improves the security of user accounts, and spares end users the frustration due to computer downtime. For more information about ADSelfService Plus, visit: https://www.manageengine.com

$ Get Quote Download