ADSelfService Plus

Solution Architecture

ManageEngine
ADSelfService Plus

Scope of this document

This document provides a detailed look into the ManageEngine ADSelfService Plus architecture and deployment options. After reading this document, you will have a good idea of the various components that are needed to deploy ADSelfService Plus, the purpose of each component, and how they communicate with each other to enable the various features of ADSelfService Plus.

1. About ADSelfService Plus

ADSelfService Plus is an identity security solution to ensure secure and seamless access to enterprise resources and establish a Zero Trust environment. With capabilities such as adaptive multi-factor authentication, single sign-on, self-service password management, a password policy enhancer, remote work enablement, and workforce self-service, ADSelfService Plus provides your employees with secure, simple access to the resources they need. ADSelfService Plus helps keep identity-based threats out, fast-tracks application onboarding, improves password security, reduces help desk tickets, and empowers remote workforces. For more information about ADSelfService Plus, visit https://www.manageengine.com/products/self-service-password.

2. Components and prerequisites needed to deploy ADSelfService Plus

Server

This is where ADSelfService Plus is installed. The server can be a member server or a domain controller.

In case you are configuring a high availability environment, you will need a primary server and a secondary server. Both servers need to have ADSelfService Plus installed. Refer to the high availability configuration here.

To enable load balancing, a primary server and one or more secondary servers have to be configured. All the servers need to have ADSelfService Plus installed. Learn more about load balancing configuration here.

Learn more about the hardware and software requirements to install ADSelfService Plus.

Database

ADSelfService Plus uses a database to store information like Active Directory (AD) attribute details, audit data, product configuration data, enrollment data, etc. The product comes with a built-in PostgreSQL database. You can also use a standalone MS SQL database or PostgreSQL database. Check out this guide for the steps to migrate from the inbuilt PostgreSQL database to a standalone MS SQL database.

Integration with Active Directory

AD forms the cornerstone of ADSelfService Plus. Scheduled synchronization of data between ADSelfService Plus and AD is necessary to allow the IT administrators to create various self-service policies and apply them to organizational units (OUs) and groups, install the login agent on domain computers, and configure various features and settings from within the product's portal. Synchronization with AD is also necessary for end users to perform the various self-service actions.

ADSelfService Plus web portal

There are two kinds of ADSelfService Plus web portals:

Admin portal: The admin portal lets the IT administrator of the solution configure domain and connection settings (SSL, proxy server, etc.), create and apply various policies, deploy MFA, integrate on-premises and cloud applications with password sync and SSO, and do much more. Click here to learn how to access the admin portal.

User portal: The user portal lets the users enroll themselves in ADSelfService Plus, perform the various self-service actions, search for employees, view the organization chart, etc. The methods to access the user portal are explained in this guide.

Optional components and prerequisites

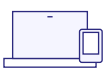
ADSelfService Plus login agent

The ADSelfService Plus login agent is software that, when installed on Windows, macOS, and Linux domain computers, provides users with the option to reset Active Directory passwords and unlock accounts from their login screens. The login agent is also required to enable endpoint MFA for Windows, macOS, and Linux logons; MFA for peripheral processes like UAC prompts and system unlocks; and offline MFA for Windows machines.

The login agent can either be pushed onto the client computers using the admin portal, Active Directory GPOs, Microsoft System Center Configuration Manager (SCCM), third-party endpoint management solutions like ManageEngine Desktop Central, or be installed manually. Refer to the links to know more about the ADSelfService Plus login agent and its installation.

ADSelfService Plus password sync agent

The ADSelfService Plus password sync agent synchronizes native password changes (password changes using the Ctrl+Alt+Del option, and password resets using the Active Directory Users and Computers console) across all the enterprise applications that are integrated with ADSelfService Plus for password synchronization. It is also used to enforce the customized password policy created in ADSelfService Plus during these native password changes. The Password Sync Agent has to be installed on all the domain controllers in a configured domain. Click here to know more about the ADSelfService Plus Password Sync Agent.



ADSelfService Plus mobile application

The ADSelfService Plus mobile app lets domain users perform AD password resets and account unlocks using their mobile device. It enables users to enroll themselves for certain MFA methods. The mobile app is also used to receive push notifications for:

- Notifying users upon successful completion of self-service actions
- Informing users of impending password and account expiration
- Distributing enrollment reminders

With the app, users can also authenticate themselves using a MFA method like time-based one-time-passcode, push notifications, fingerprint-based, and QR codes. The mobile app can be either manually installed by users or pushed to mobile devices by the IT administrator.

Integrate with enterprise applications

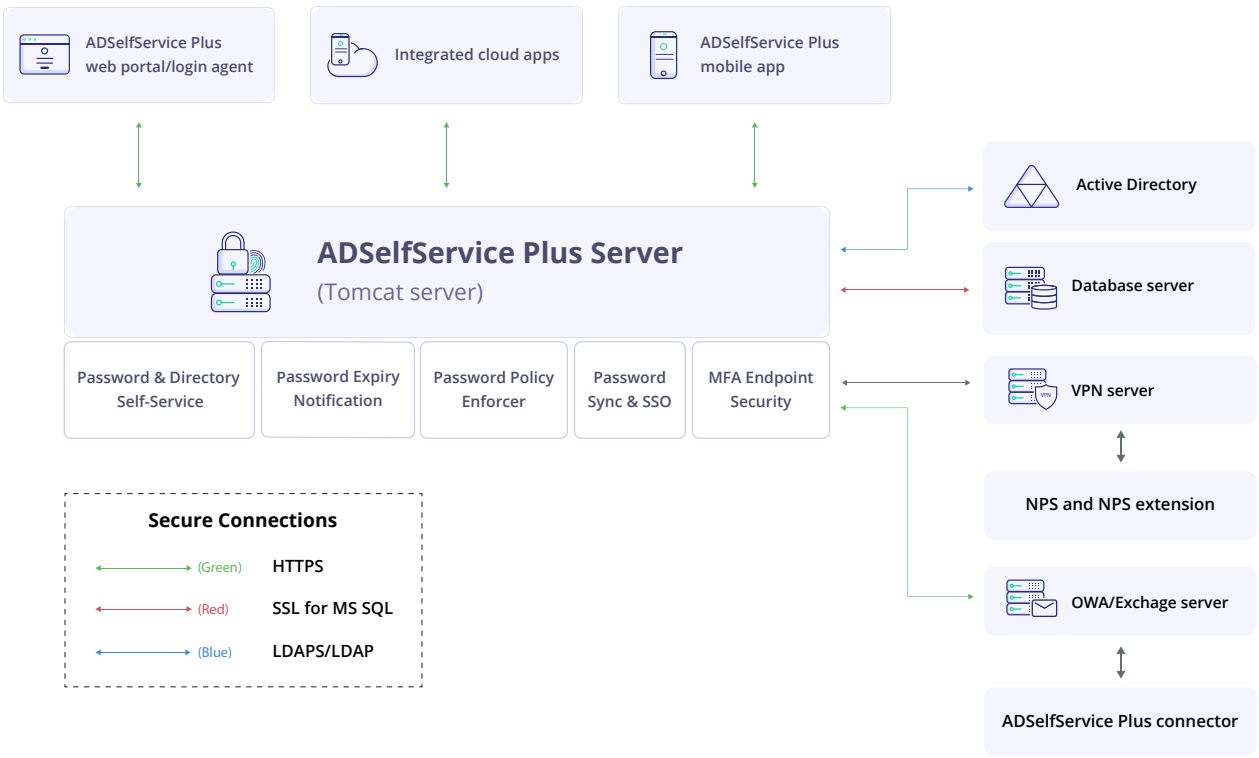
Through password synchronization and single sign-on, ADSelfService Plus integrates with various enterprise applications such as Google Workspace, Salesforce, Microsoft 365 (formerly Office 365), and Dropbox. When password synchronization is enabled, any change to users' domain passwords is synchronized across all the integrated applications, enabling the user to access all of them with a single password. In the case of SSO, if the user has logged into their ADSelfService Plus account, they are automatically logged into these cloud applications without having to furnish their user credentials.

Microsoft Exchange server

To configure ADSelfService Plus' MFA for Outlook Web Access (OWA) and Exchange admin center (EAC) logins, the ADSelfService Plus connector must be installed in the OWA/Exchange server. This connector mediates between OWA or the EAC and ADSelfService Plus to enable MFA during logins.

VPN server and Network Policy Server

To secure your VPNs using ADSelfService Plus' MFA feature, the VPN server should use a Windows Network Policy Server (NPS) to configure RADIUS authentication, and the ADSelfService Plus NPS extension has to be installed in the NPS. This extension mediates between the NPS and ADSelfService Plus to enable MFA during VPN connections. Here is an illustration of an environment with ADSelfService Plus deployed:

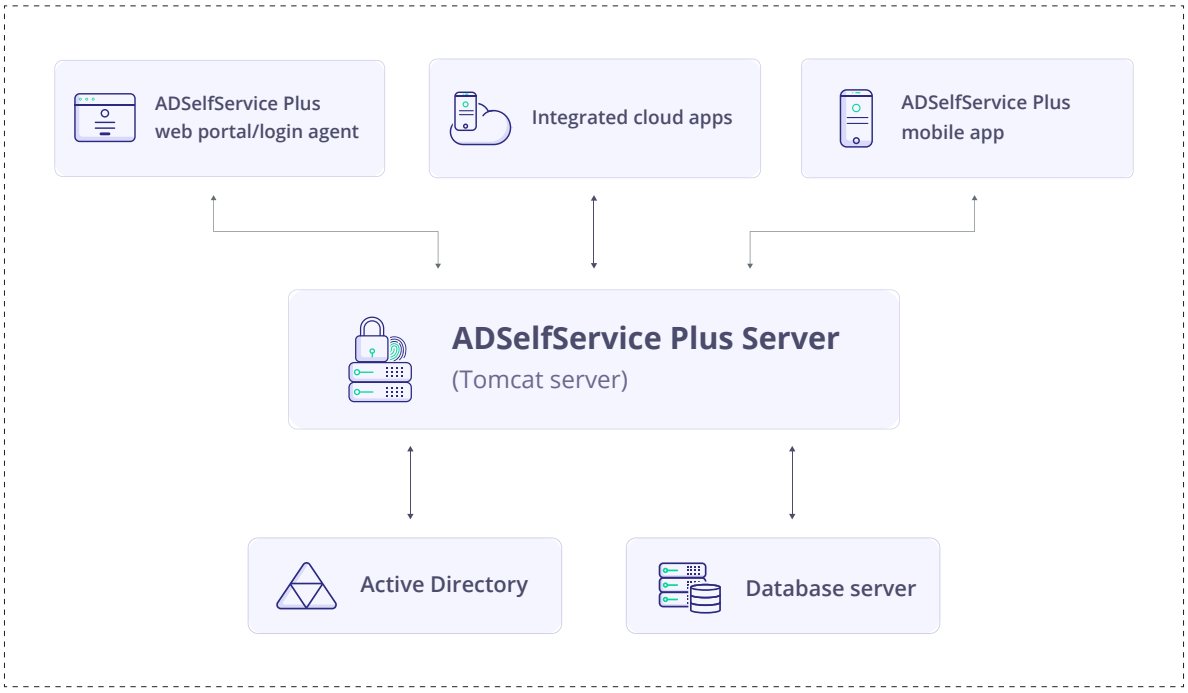


3. Deployment scenarios

Here are five scenarios that illustrate the various methods of ADSelfService Plus deployment:

1. Deploying over an intranet

It is standard to deploy ADSelfService Plus in the intranet of the organization. In this method, the ADSelfService Plus web portal, login agent, and mobile application can only be accessed when the user is connected to the intranet. Below is a depiction of ADSelfService Plus deployment over the intranet:

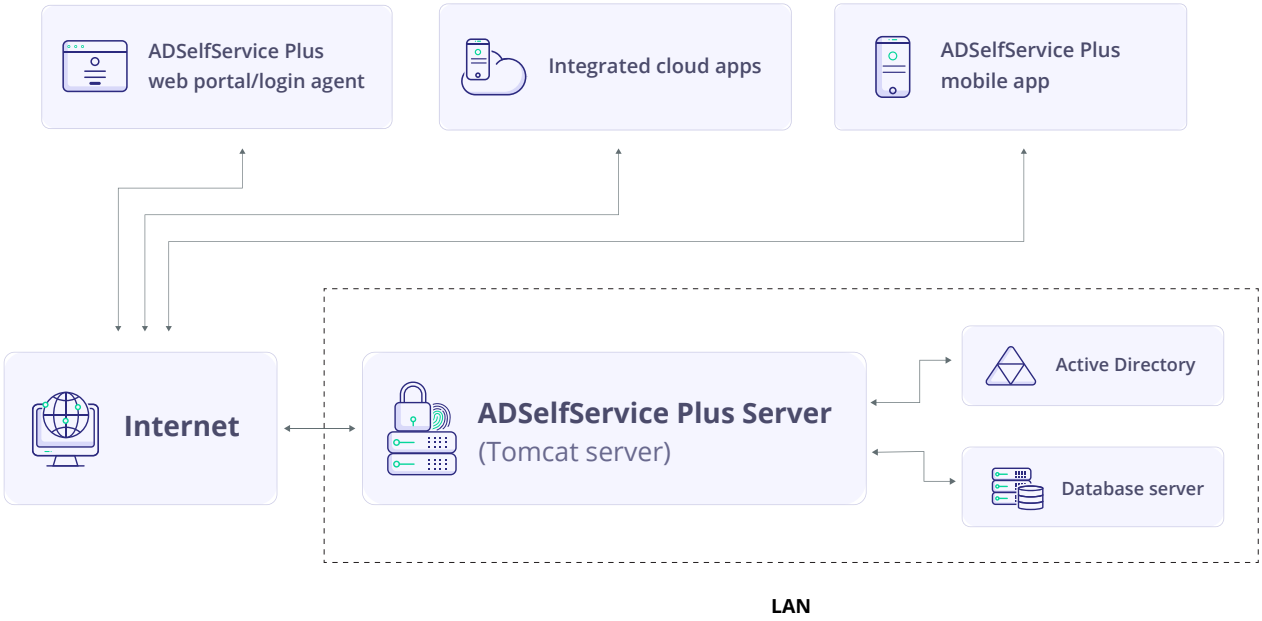


LAN

Learn about installing and starting ADSelfService Plus.

2. Deploying over the internet

When ADSelfService Plus is deployed over the internet, end users can log into the ADSelfService web portal and mobile app through any external network. It is recommended that the internal network with the ADSelfService Plus server, database, and other entities deployed is shielded from client access through the internet using DMZ or reverse proxy. Here is an illustration of ADSelfService Plus deployment over the internet:

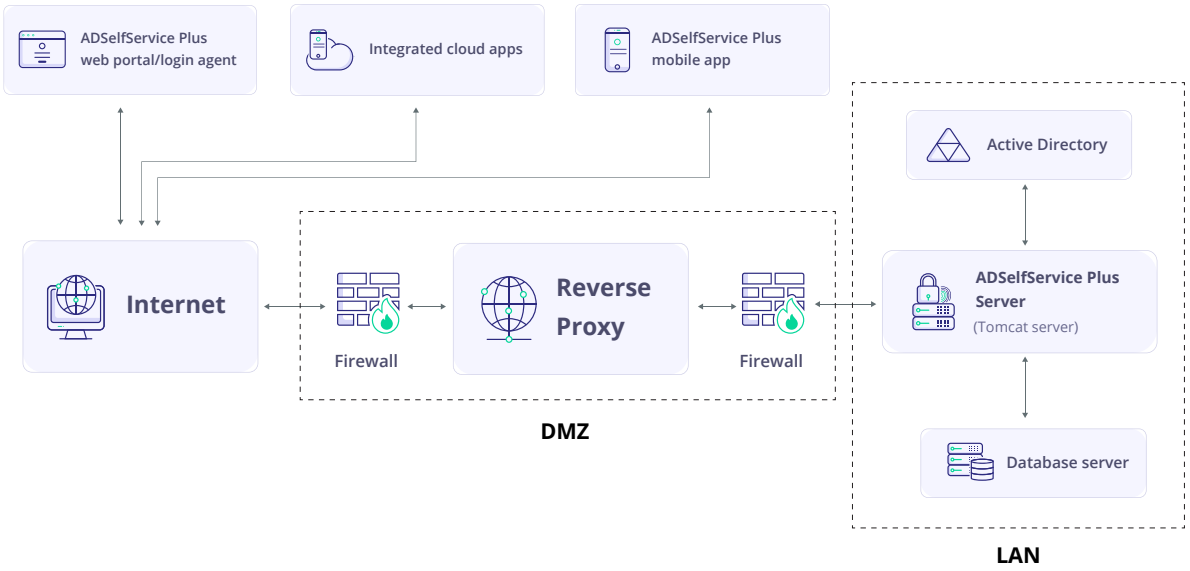


This guide provides the steps for securely hosting ADSelfService Plus over the internet.

a. DMZ setup

A DMZ is a sub-network that prevents clients from directly accessing the server, and therefore, the internal LAN where the server and other components are deployed. The DMZ acts as a barrier between the internet and the internal LAN where the ADSelfService Plus server, database, and AD are located.

Here is a depiction of ADSelfService Plus deployed using DMZ:

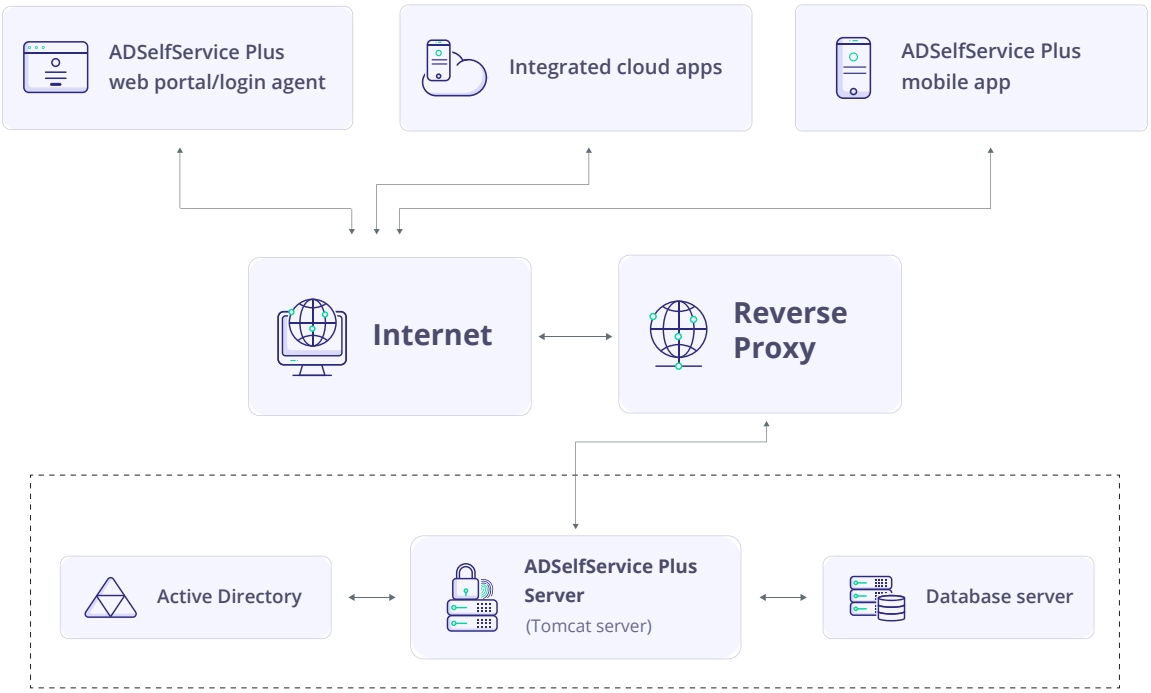


Here, the DMZ setup consists of a reverse proxy that is flanked on both sides by a firewall. The first firewall is configured only to allow traffic from the internet to the reverse proxy, and the second firewall is configured only to receive connections from the organization's LAN to the reverse proxy.

b. Reverse proxy

A reverse proxy is a type of proxy server that retrieves resources on behalf of a client from a server. These resources are then returned to the client, appearing as if they originated from the reverse proxy itself. Thus, the website or service never needs to reveal the IP address of its origin server. Reverse proxy conceals the ADSelfService Plus server, the other components, and the LAN they are located in from third-party attacks.

Here is an example of an ADSelfService Plus deployment with a reverse proxy:

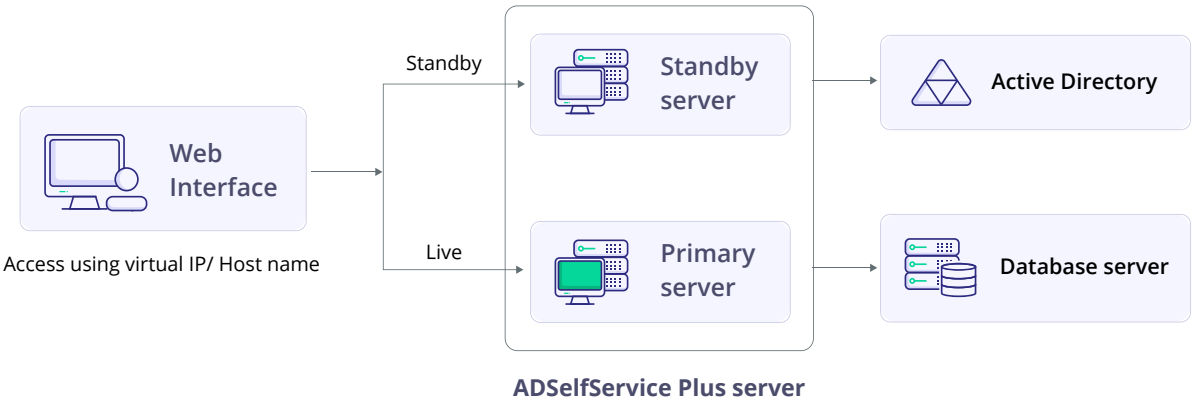


Here, the reverse proxy has been placed behind the firewall that secures the LAN. When an inbound request to the ADSelfService Plus server arrives, the reverse proxy intercepts and sends the request to the server. It then fetches the response and sends it to the client on behalf of the server.

For more information, take a look at the guides on setting up a reverse proxy for ADSelfService plus using AD360, Apache HTTP server, and Microsoft IIS.

3. High availability

High availability is configured in ADSelfService Plus to provide failover in the case of system or application failures. High availability is achieved through automatic failover, that is, when the service running on one server fails, another instance of the service running on another server will take over. This illustration shows the architecture of the ADSelfService Plus environment when high availability is configured:

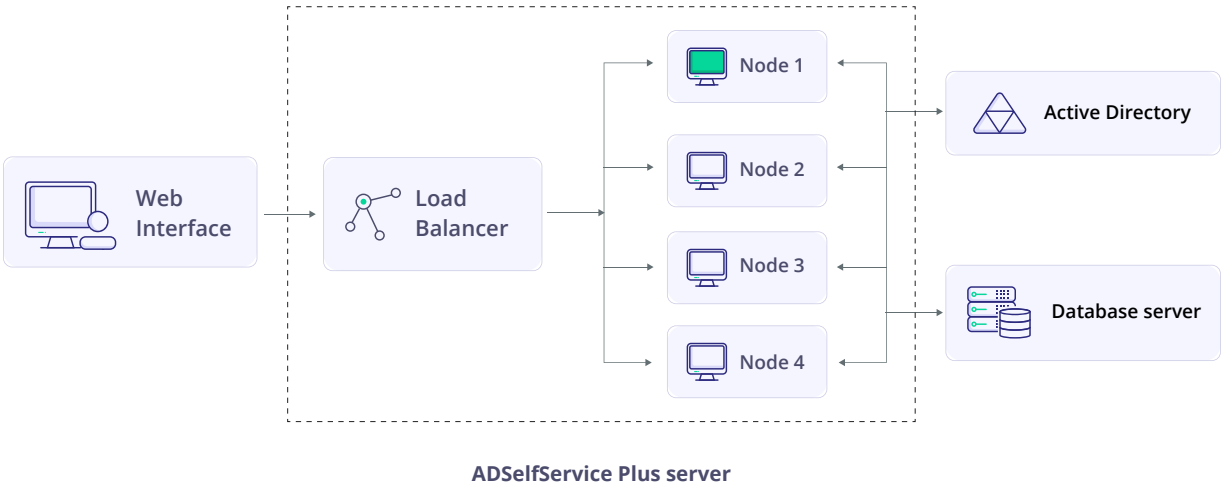


When the primary server fails to function, the instance running in the secondary server takes over. Since the data in the primary server is cloned to the secondary server during configuration, the switchover is automatic and free of problems. High availability helps the IT administrators and end users have continued access to ADSelfService Plus.

Here is a detailed guide on configuring high availability in ADSelfService Plus.

4. Load balancing

With load balancing, the incoming requests to ADSelfService Plus are split among multiple server nodes. To enable load balancing in ADSelfService Plus, a primary node and multiple secondary nodes have to be configured. Here is how the primary node and secondary nodes are placed in the ADSelfService Plus architecture:



When requests are made to ADSelfService Plus, the primary node directs splits the requests among the secondary nodes using the round-robin method. Load balancing helps alleviate performance degradation due to heavy traffic and improves user experience.

These scenarios explain various ways that ADSelfService Plus can be deployed in a network. If you need help deploying ADSelfService Plus, contact us at support@adselfserviceplus.com.

About ADSelfService Plus

ADSelfService Plus is an identity security solution to ensure secure and seamless access to enterprise resources and establish a Zero Trust environment. With capabilities such as adaptive multi-factor authentication, single sign-on, self-service password management, a password policy enhancer, remote work enablement and workforce self-service, ADSelfService Plus provides your employees with secure, simple access to the resources they need. ADSelfService Plus helps keep identity-based threats out, fast-tracks application onboarding, improves password security, reduces help desk tickets and empowers remote workforces.

For more information about ADSelfService Plus,visit
https://www.manageengine.com/products/self-service-password.

$ Get Quote Download