ManageEngine
ADSelfService Plus

A guide to securely hosting ADSelfService Plus on the internet

www.adselfserviceplus.com

Table of Contents

Document summary

This guide will walk you through the process of securely deploying ADSelfService Plus for remote access through the internet.

Before you begin:

Please enable SSL in ADSelfService Plus before hosting the product on the internet.

Hosting ADSelfService Plus on the internet

Scenario 1: ADSelfService Plus is installed in a LAN

Assume ADSelfService Plus is installed inside a local area network (LAN) on a server with *192.168.200.254* as its IP address, *9251* as its port number, and *adselfserviceplus-lan* as its hostname.

For users within the LAN, the URL to access ADSelfService Plus will be *https://adselfserviceplus-lan:9251* or *https://192.168.200.254:9251.*

If ADSelfService Plus has to be accessed over the internet, you need to:

- Register an IP address and a public hostname with your internet service provider. For this example, we'll use the IP address *64.12.13.11* and the public hostname *selfservice.yourdomain.com.*
- Resolve the IP address for *selfservice.yourdomain.com* to *64.12.13.11.* This will be predominantly handled by your internet service provider.
- Configure firewall rules (or access lists in routers) to redirect HTTPS requests for the IP address *64.12.13.11* to the LAN IP address *192.168.200.254.*
- Update the Access URL settings in ADSelfService Plus with the new public IP. Go to **Admin > Product Settings > Connection,** and click **Configure Access URL.**

Please note that all notifications generated by ADSelfService Plus will now be sent with the public URL. The public URL will also be reachable within the LAN.

Note for FIDO passkey users:

- If you have configured FIDO passkey authentication, updating the Access URL will modify the preconfigured FIDO RP ID, resulting in loss of enrollment data and disenrollment of all users.
- If you are planning on configuring FIDO passkey authentication, ensure that the Access URL is updated before configuring FIDO passkey authentication to prevent loss of enrollment data.

Scenario 2: ADSelfService Plus is installed in a DMZ

Assume ADSelfService Plus is installed in a demilitarized zone (DMZ) on a server with *192.168.225.254* as its IP address, *9251* as its port number, and *adselfserviceplus-dmz* as its hostname. We recommend using PostgreSQL bundled with ADSelfService Plus, since using this combination requires no additional configurations.

If you're using an MS SQL database, you'll need to follow the steps below:

- **MS SQL database in a LAN:** You need to configure the firewall's rules so that the application can reach the database server in the LAN through the MS SQL port (default port: *1433*).
- **MS SQL database in a DMZ:** Port *1433* should be reachable from the ADSelfService Plus server in the DMZ.

For PostgreSQL users and MS SQL users that have finished with the database configurations:

- Configure the firewall's rules so that users in the LAN are able to access ADSelfService Plus at *https://adselfserviceplus-dmz:443*. Note that the application is installed on port *9251*, but users have to access it through port *443*. You'll need to redirect HTTPS requests for the IP address *192.168.225.254* on port *443* to port *9251*.
- Register an IP address and a public hostname with your internet service provider. For this example, we'll use the IP address *64.12.13.11* and the public hostname *selfservice.yourdomain.com*.
- Resolve the IP address for *selfservice.yourdomain.com* to *64.12.13.11*. This will be predominantly handled by your internet service provider.
- Configure firewall rules (or access lists in routers) to redirect HTTPS requests for the IP address *64.12.13.11* on port *443* to the LAN IP address *192.168.225.254* on port *9251*.
- Update the Access URL settings in ADSelfService Plus with the new public IP. Go to **Admin > Product Settings > Connection,** and click **Configure Access URL.**

Note for FIDO passkey users:

- If you have configured FIDO passkey authentication, updating the Access URL will modify the preconfigured FIDO RP ID, resulting in loss of enrollment data and disenrollment of all users.
- If you are planning on configuring FIDO passkey authentication, ensure that the Access URL is updated before configuring FIDO passkey authentication to prevent loss of enrollment data.

Please note that all notifications generated by ADSelfService Plus will now be sent with the public URL. The public URL will also be reachable within the LAN.

Remote users should now be able to access ADSelfService Plus over the internet.

Setting up a reverse proxy for improved security

In computer networks, a reverse proxy is a type of proxy server that retrieves resources on behalf of a client (user) from one or more servers (ADSelfService Plus). These resources are then returned to the client as though they originated from the reverse proxy itself. A reverse proxy is used as a strategic point in the network to enforce web application security.

For more information on how to set up a reverse proxy for ADSelfService Plus, refer to:

- Setting up a reverse proxy for ADSelfService Plus using AD360.
- Setting up a reverse proxy for ADSelfService Plus using Apache HTTP Server.
- Setting up a reverse proxy for ADSelfService Plus using Microsoft Internet Information Services (IIS).

Note: To enable a reverse proxy, you need to purchase the Failover and Secure Gateway Services add-on. Buy now.

If you have any questions, please contact support@adselfserviceplus.com. One of our product experts will be happy to help you.