ManageEngine
ADSelfService Plus

Setting up a reverse proxy for ADSelfService Plus using AD360

Table of Contents

Document summary

The purpose of this document is to guide you through the process of securely deploying ADSelfService Plus to remote users using ManageEngine AD360 as a reverse proxy server.

Before setting up a reverse proxy

Before you can set up a reverse proxy using AD360, you need to host ADSelfService Plus on the internet so that remote users can access it.

This guide provides step-by-step instructions on how to host ADSelfService Plus on the internet.

What is a reverse proxy and how does it work?

Before jumping into the configuration steps, let's talk about what a reverse proxy is. 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.

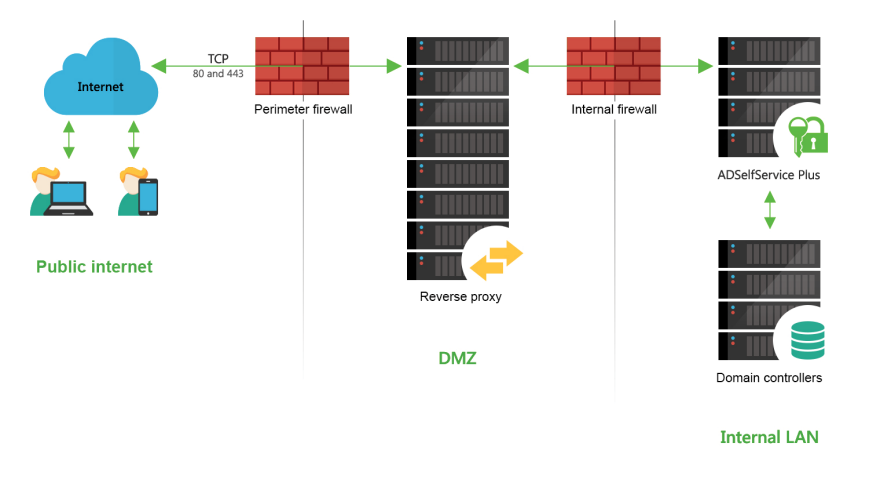


Figure 1. Reverse proxy server in the DMZ and ADSelfService Plus server in the intranet.

As shown in the above figure, ADSelfService Plus works with reverse proxy servers. Requests from clients (users) are received by the reverse proxy server (AD360) in the DMZ. The reverse proxy server then forwards those requests to the ADSelfService Plus server in the LAN (or, if needed, can be placed in the DMZ). External machines never make a direct connection to the ADSelfService Plus server.

Your firewall will only permit the proxy server to access the ADSelfService Plus server and only through the required port.

Important: Once you enable a reverse proxy, please update the Access URL settings in ADSelfService Plus by navigating to **Admin > Product Settings > Connection** and clicking **Configure Access URL.**

Configuring AD360 as a reverse proxy for ADSelfService Plus

AD360 is an integrated identity and access management (IAM) solution for managing user identities, governing access to resources, enforcing security, and ensuring compliance. You can integrate ADSelfService Plus with AD360 to unlock many useful features, including a reverse proxy.

AD360 lets you enable context-based reverse proxies, port-based reverse proxies, or both. We recommend that you apply an SSL certificate and enable HTTPS connection to AD360 to secure communication between clients and the reverse proxy server.

Follow the steps below to set up a reverse proxy server for ADSelfService Plus using ManageEngine AD360.

Prerequisites

- Download and install AD360.
- Choose **Minimal Installation** mode during installation.
- Integrate ADSelfService Plus with AD360.
  - To integrate, log in to the AD360 web console as an administrator.
  - Click the **Admin** tab.
  - Under **Administration**, click **ADSelfService Plus.**
  - Enter the **server name, protocol**, and **port details** of the ADSelfService Plus server, and click **Integrate.**
- We recommend enabling HTTPS connection to AD360 after installation.

- **Host ADSelfService Plus on the internet:** Before you can set up a reverse proxy using AD360, you need to host ADSelfService Plus on the internet so that remote users can access it. This guide provides step-by-step instructions on how to host ADSelfService Plus on the internet.

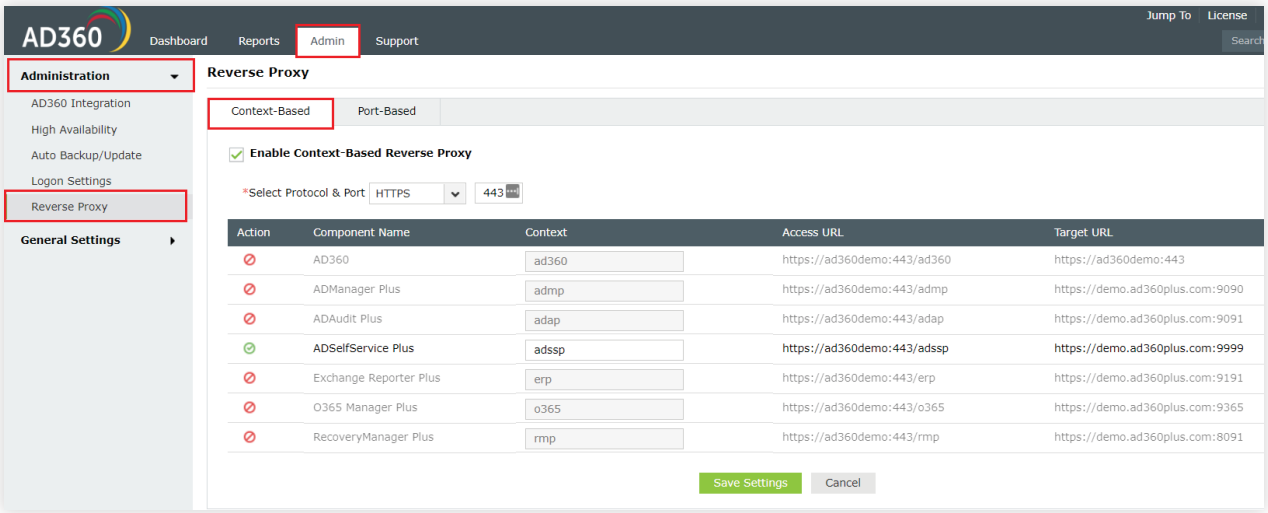
- **Failover and Secure Gateway Services add-on:** To enable a reverse proxy, you need to purchase the Failover and Secure Gateway Services add-on. Buy now.

Enabling a context-based reverse proxy

In a context-based reverse proxy, the URL of ADSelfService Plus is given a unique context path. Whenever a user requests access, it's first forwarded to the AD360 server, which then forwards the request to the ADSelfService Plus server based on the context path in the URL. The end user will not know the details of the ADSelfService Plus server.

Follow the steps given below to enable a context-based reverse proxy:

1. Log in to the **AD360 web console** as an administrator.
2. Navigate to **Admin > Administration > Reverse Proxy.**
3. Click the **Context-based** tab, and check the **Enable Context-based Reverse Proxy** box.



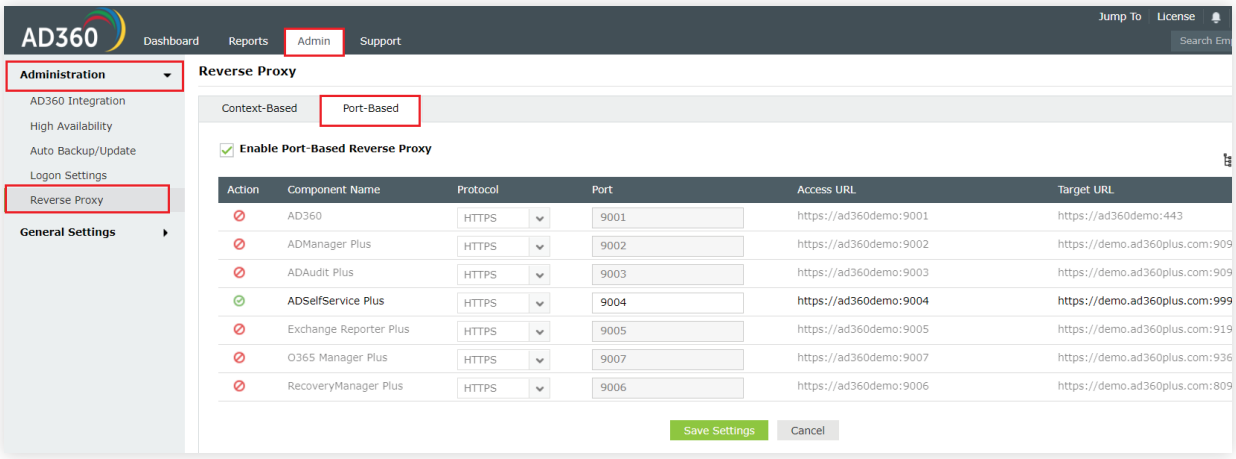
4. Select the **required protocol** and port number from the *Protocol* and *Port* drop-down fields respectively. Please make sure that the port number is not being used by another application.
5. Now, enter a **context path** for ADSelfService Plus under the *Context* column.
6. Write down the **Access URL** for ADSelfService Plus. External users can use this URL to access ADSelfService Plus.
7. Click **Save Settings.**

Enabling a port-based reverse proxy

To enable a port-based reverse proxy, you need to choose a unique port number and protocol for ADSelfService Plus. In this case, a unique port number for the ADSelfService Plus server is mandatory whereas specifying the unique protocol is optional. The hostname remains the same. The AD360 server will forward user requests to the ADSelfService Plus server based on the port number in the URL and the protocol.

Follow the steps given below to enable a port-based reverse proxy:

1. Log in to the **AD360 web console** as an administrator.
2. Navigate to **Admin > Administration > Reverse Proxy.**
3. Click the **Port Based** tab, and check the **Enable Port-Based Reverse Proxy** box.



4. Select a **protocol** for ADSelfService Plus from the *Protocol* drop-down.
5. Enter a **port number** for AD360 and its components in the *Port* field. Please make sure the port number is not being used by another application.
6. Write down the **Access URL** for ADSelfService Plus. External users can use this URL to access ADSelfService Plus.
7. Click **Save Settings.**

The setup for reverse proxy to ADSelfService Plus server using ManageEngine AD360 is now complete.

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

About ManageEngine 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