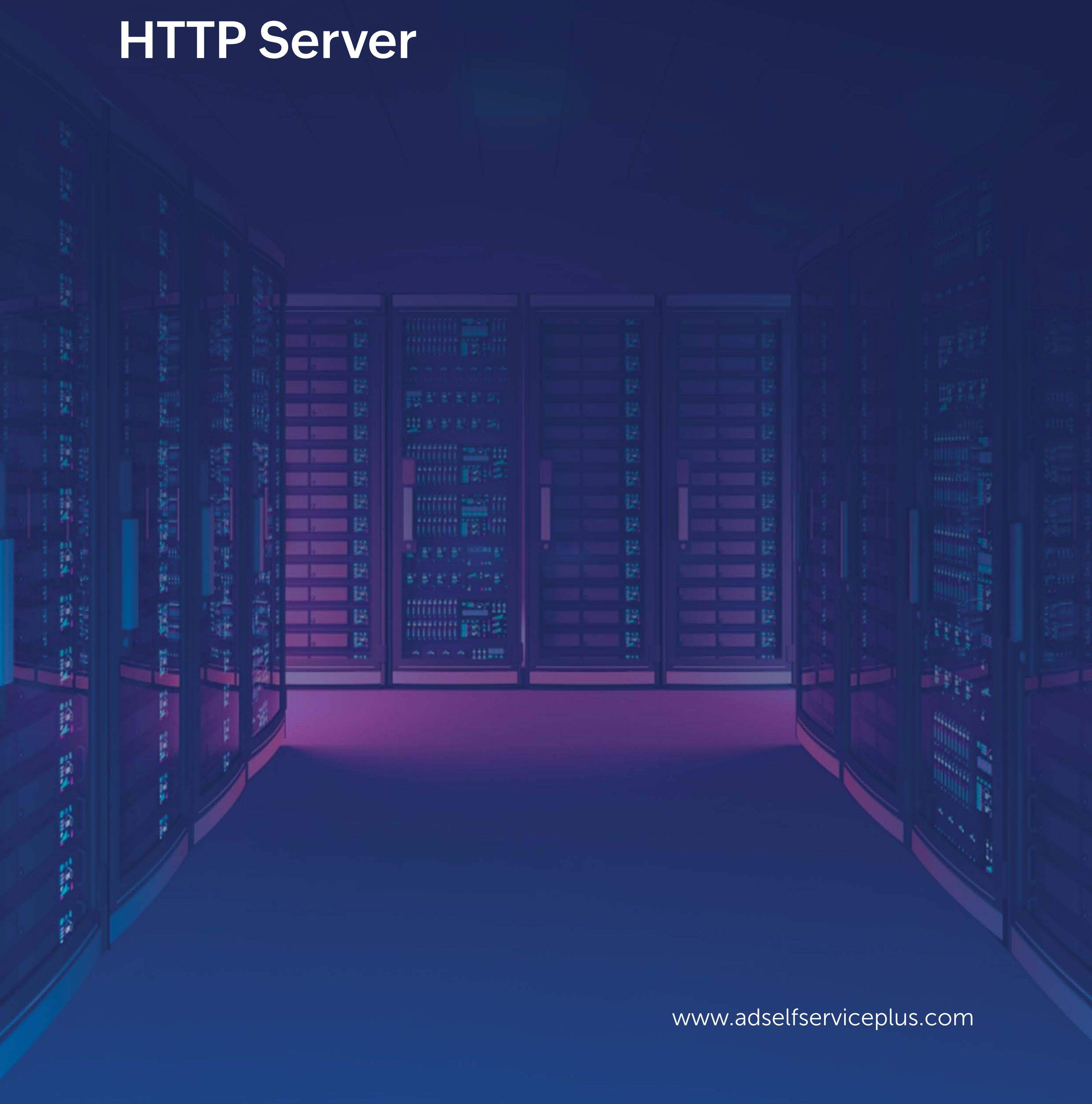
ManageEngine
ADSelfService Plus

Setting up a reverse proxy for ADSelfService Plus using Apache HTTP Server



www.adselfserviceplus.com

Table of Contents

Document summary

This guide will walk you through the process of securely deploying ADSelfService Plus to remote users using Apache HTTP Server as a reverse proxy.

Prerequisites

Enter the reverse proxy server's IP address in the **server.xml** file under the installation directory using these steps:

- Access the **conf** folder in the ADSelfService Plus installation directory (by default, ***C:\Program Files\ManageEngine\conf)***.
- Open the server.xml file in the conf folder.
- Navigate to the below section:

  ```
  <!--Valve className="org.apache.catalina.valves.RemoteIpValve"
  remoteIpHeader="x-forwarded-for" proxiesHeader="x-forwarded-by"
  requestAttributesEnabled="true" internalProxies="127\.0\.0\.1|0\:0\:0\:0\:0\:0\:0\:1"/-->
  ```
- Uncomment the line, and add the <enter server name>* server's IP address as shown:

  ```
  <Valve className="org.apache.catalina.valves.RemoteIpValve"
  remoteIpHeader="x-forwarded-for" proxiesHeader="x-forwarded-by"
  requestAttributesEnabled="true" internalProxies="<IP_address >"/>
  ```

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.

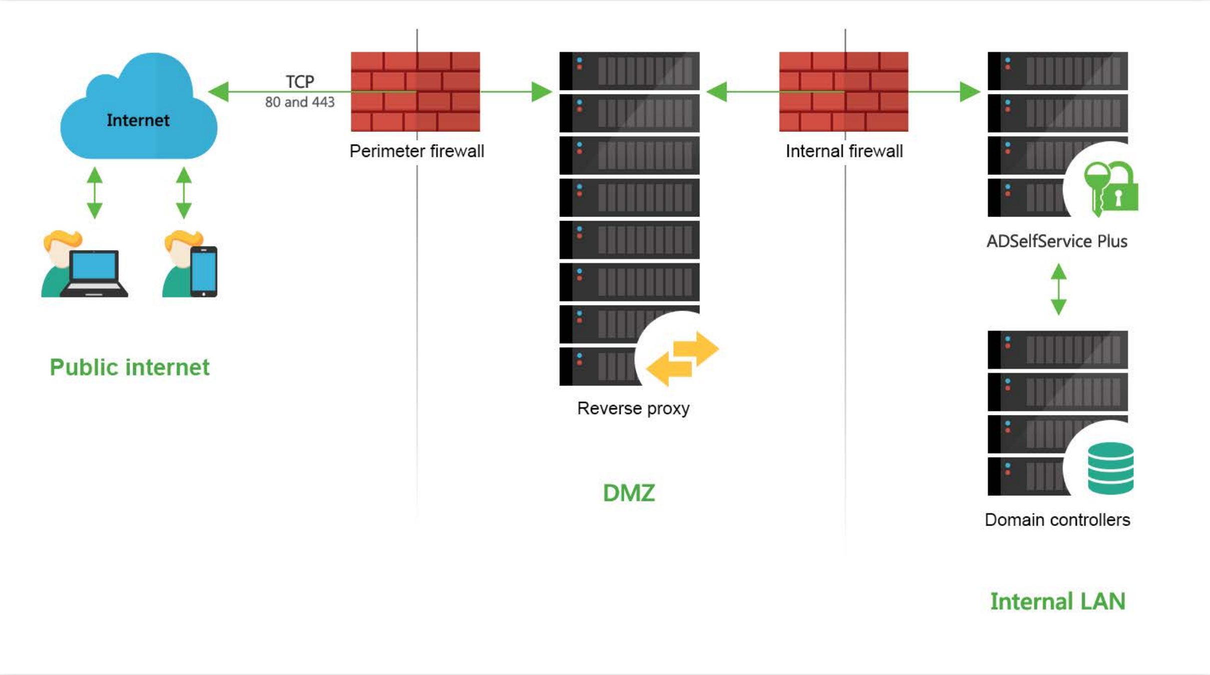


Figure 1: A reverse proxy server in a DMZ, while the ADSelfService Plus server is hosted in the intranet.

As shown in the figure above, ADSelfService Plus works with reverse proxy servers. In our example above, requests from clients (users) are received by the reverse proxy server (Apache server) in the DMZ. The reverse proxy server then forwards those requests to the ADSelfService Plus server in the LAN. If needed, the ADSelfService Plus server can also be placed in the DMZ. In either case, external machines never connect directly 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 note: Once you enable reverse proxy, please update the **Access URL** settings in ADSelfService Plus by navigating to **Admin > Product Settings > Connection** and clicking **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 modified after enabling reverse proxy before configuring FIDO passkey authentication to prevent loss of enrollment data.

Configuring Apache HTTP Server as a reverse proxy for ADSelfService Plus

Now, let's look at how to configure a reverse proxy for ADSelfService Plus using an Apache server. For this configuration, we're using Apache HTTP Server version 2.2.

Important:

- This configuration assumes that the reverse proxy server is placed in a DMZ, and the ADSelfService Plus server and the domain controllers are in an internal LAN.
- We've used the default values for IP addresses, port numbers, file locations, etc. in the steps provided. If you've changed any default settings in ADSelfService Plus or your Apache server, make sure those changes are reflected in these steps.
- Make sure you have opened the port that will be used in the Apache server configuration for TCP access (80 for HTTP and 443 for HTTPS, by default) in Windows Firewall.

Step 1: Make changes in your Apache server

1. Navigate to **C:\Program Files\Apache Software Foundation\Apache2.2\conf.**
2. Open the **httpd.conf** file in a text editor.
3. Uncomment the following lines:

```
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_ajp_module modules/mod_proxy_ajp.so
LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
LoadModule proxy_connect_module modules/mod_proxy_connect.so
LoadModule proxy_ftp_module modules/mod_proxy_ftp.so
LoadModule proxy_http_module modules/mod_proxy_http.so
LoadModule proxy_scgi_module modules/mod_proxy_scgi.so
Include conf/extra/httpd-vhosts.conf
```

4. Navigate to **C:\Program Files\Apache Software Foundation\Apache2.2\conf\extra.**
5. Open the **http-vhost.conf** file in a text editor.

6. Add the entries below:

   ```
   NameVirtualHost *:443
   <VirtualHost *:443>
   ServerAdmin admin@test.com
   ServerName adselfserviceplus.yourdomain.com
   SSLEngine on
   SSLProxyEngine on
   SSLCertificateFile "C:\Program Files\Apache Software Foundation\Apache2.2\conf\server.crt"
   SSLCertificateKeyFile "C:\Program Files\Apache Software Foundation\Apache2.2\conf\server.key"
   <Location />
   ProxyPass https://192.168.200.254:9251/
   ProxyPassReverse https://192.168.200.254:9251/
   </Location>
   ErrorLog "logs/ADSelfServicePlus.log"
   CustomLog "logs/ADSelfServicePlus.log" common
   </VirtualHost>
   ```

7. **Restart** the **Apache server** to see the changes take effect.

Step 2: Make changes in ADSelfService Plus

Based on whether you've enabled HTTPS or not, the steps for making changes in ADSelfService Plus may vary.

ADSelfService Plus in HTTPS mode

1. Navigate to **<install_dir>\conf.** By default, this folder is listed under **C:\ManageEngine\ADSelfService Plus\conf.**
2. Open the **server.xml** file in a text editor.
3. Search for the connector tag that contains the element *SSLEnabled="true" (i.e. <Connector SSLEnabled="true").*
4. Add the following entry:
   proxyName="<apache-server-ip-address>" proxyPort="443"
5. Save the changes.
6. Restart **ADSelfService Plus** to see the changes take effect.

ADSelfService Plus in HTTP mode

1. Navigate to **<install_dir>\conf.** By default, this folder is listed under **C:\ManageEngine\ADSelfService Plus\conf.**
2. Open the **server.xml** file in a text editor.
3. Search for the connector tag that contains the name="WebServer" element (i.e. <Connector name="WebServer").
4. Add the following entry:

scheme="https" proxyName="<apache-server-ip-address>" proxyPort="443"

5. Save the changes.
6. Restart **ADSelfService Plus** to see the changes take effect.

You have now set up a reverse proxy for ADSelfService Plus using Apache HTTP Server.

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