ManageEngine
AD360

Using AD360 as a reverse proxy server

www.manageengine.com/active-directory-360/

Table of Contents

Document summary

ManageEngine AD360 is an integrated solution comprised of multiple products including ADManager Plus, ADAudit Plus, and ADSelfService Plus.

The purpose of this document is to guide you through the process of using AD360 as a reverse proxy server for the products integrated with it.

What is a reverse proxy?

Before jumping into the configuration steps, let's talk about what a reverse proxy is. A reverse proxy is a server that's used as a strategic point in the network. It enforces web application security by hiding the location and identity of a server when remote users access an application over the internet.

The reverse proxy server receives requests from external clients and forwards them to the target web application servers, which are usually located inside the LAN and are not directly accessible from outside. It also receives the response from the servers and forwards it to the client. Throughout this whole process, the client assumes that the reverse proxy is the web application server.

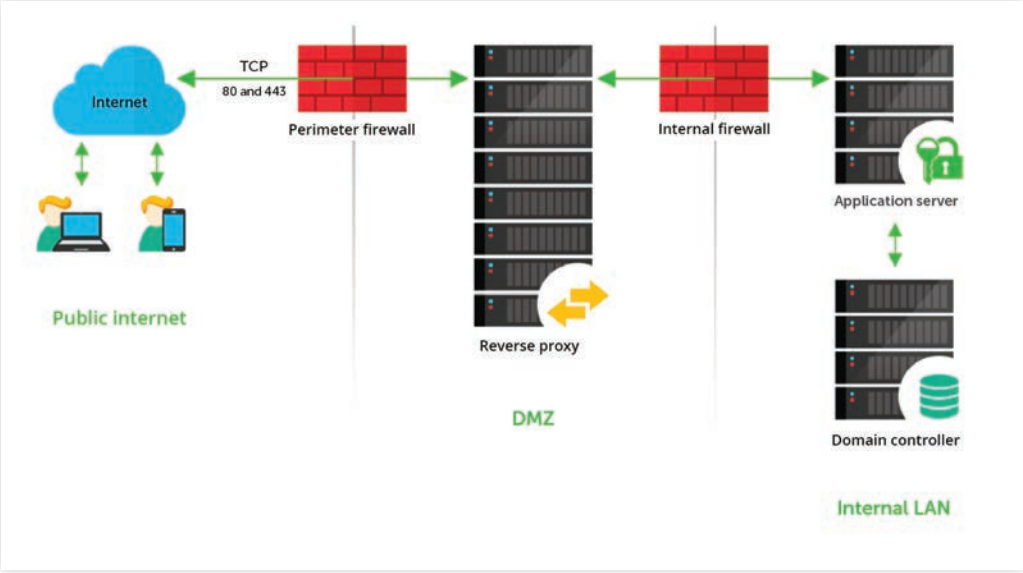


Figure 1. A reverse proxy setup

For example, let's say the reverse proxy server is installed in the DMZ, and the application server is in the LAN, as shown in the figure above. In this case, requests from clients (users) are received by the reverse proxy server in the DMZ. The reverse proxy server then forwards those requests to the application server in the LAN.

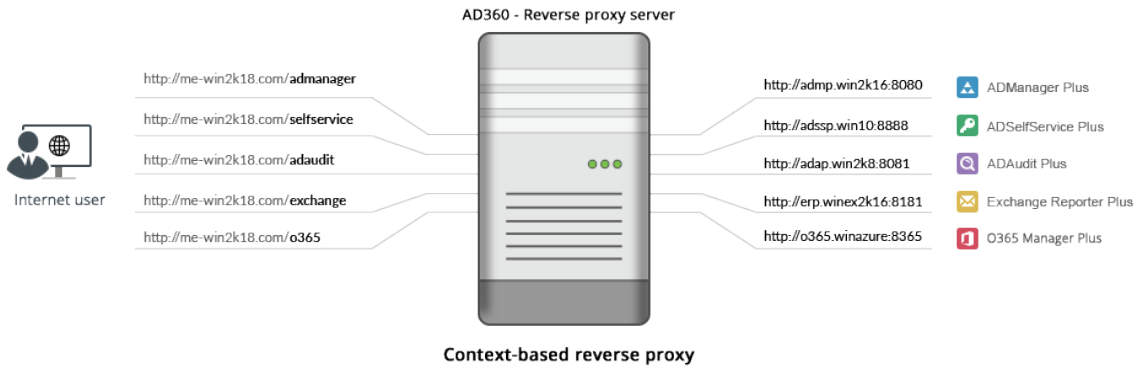
Your firewall will only permit the reverse proxy server to access the application server. External machines never connect directly to the server running the web application.

Configuring AD360 as a reverse proxy

You can use AD360 to act a reverse proxy server for the products that you've integrated with it. AD360 lets you enable a context-based reverse proxy, a port-based reverse proxy, or both.

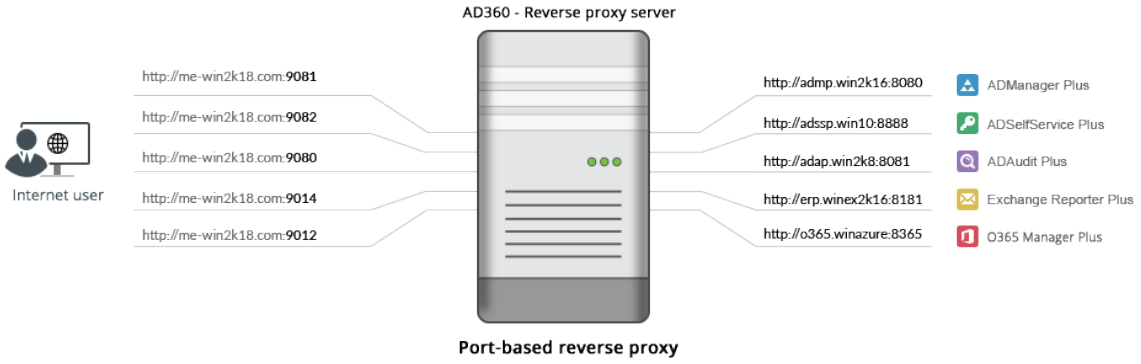
In a context-based reverse proxy, a unique context path is used to redirect requests to the individual products. In this case, a unique context path should be set for each of the integrated products. AD360's hostname will be assigned to the products and you can assign any unused port number—these two details will remain the same for all integrated products.

Whenever a user requests access, the request is forwarded to the respective server based on the context path in the URL. End users will not know the details of the servers from which they are accessing the individual products.



In a port-based reverse proxy, a unique port number and protocol are used to redirect requests to individual products. In this case, you should assign a unique port number for each server; specifying a unique protocol is optional. The hostname of AD360 is assigned to all the individual products.

Whenever a user requests access, the request is forwarded to the respective server based on the port number in the URL.



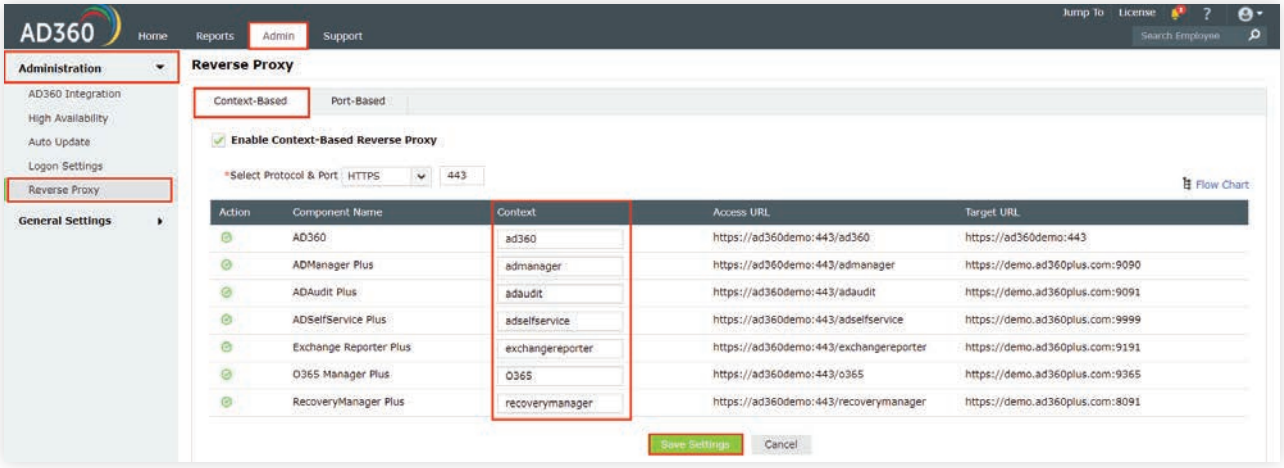
Note: The hostname of the AD360 server will serve as the hostname for the integrated products when a reverse proxy is enabled.

We recommend that you apply an SSL certificate and enable HTTPS connection to AD360 to secure the communication between clients and the reverse proxy server.

Enabling a context-based reverse proxy

Follow the steps 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. Please ensure that the port number is not being used by another application.
5. Enter a **context path** under the *Context* column for AD360 and each of its integrated products. The context path must be unique to each product.



6. Copy the **Target URLs** for AD360 and each of the integrated products.

   Users can utilize these URLs to access the necessary products.

7. Click **Save Settings.**

Enabling a port-based reverse proxy

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

1. Log in to the **AD360 web console** as an administrator.

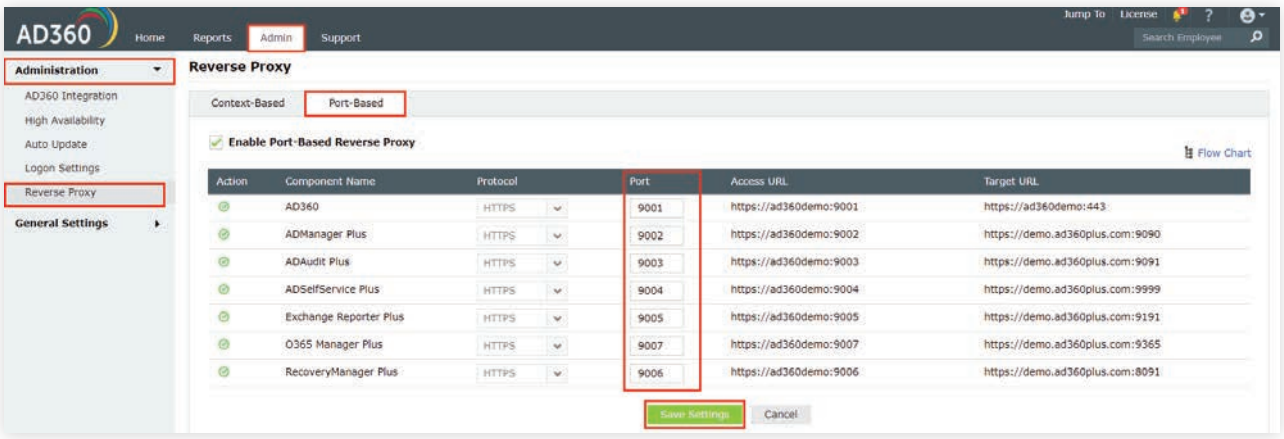
2. Navigate to **Admin > Administration > Reverse Proxy.**

3. Click the **Port-Based** tab, and check the **Enable Port-Based Reverse Proxy** box.

4. Select a **protocol** for AD360 and the integrated products from the *Protocol* drop-down.

5. Enter a **port number** for AD360 and its products in the *Port* field.

   Please ensure the port number is not being used by another application.



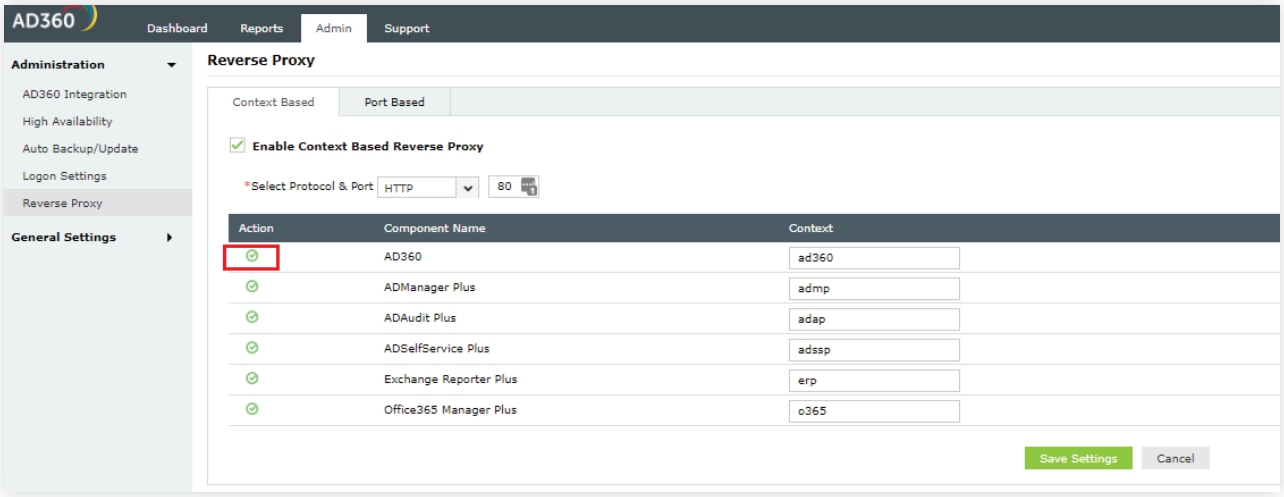
6. Copy the **Target URLs** for AD360 and each of the integrated products.

   Users can utilize these URLs to access the necessary products.

7. Click **Save Settings.**

Disabling reverse proxies

You can disable reverse proxies for certain integrated products if you wish. Under the **Actions** column, click the green check icon [✓] to disable a reverse proxy.



If you have any questions, please contact ad360support@manageengine.com. One of our product experts will be happy to help you.

About ManageEngine AD360

AD360 is an identity and access management (IAM) solution for managing user identities, governing access to resources, enforcing security, and ensuring compliance. AD360 provides all these functionalities for Windows Active Directory, Exchange Server, and Office 365. With AD360, you can choose the modules you need and start addressing IAM challenges across on-premises, cloud, and hybrid environments—all from a single console. For more information about AD360, please visit www.manageengine.com/ad360.

$ Get Quote ⬇ Download