

Setting up a reverse proxy for ADSelfService Plus using Internet Information Services (IIS)



Table of Contents

Document summary	1
What is a reverse proxy and how does it work?	1
Configuring IIS as a reverse proxy for ADSelfService Plus	2
How to Install an SSL/TLS certificate	4
About ManageEngine ADSelfService Plus	8

Document summary

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

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.

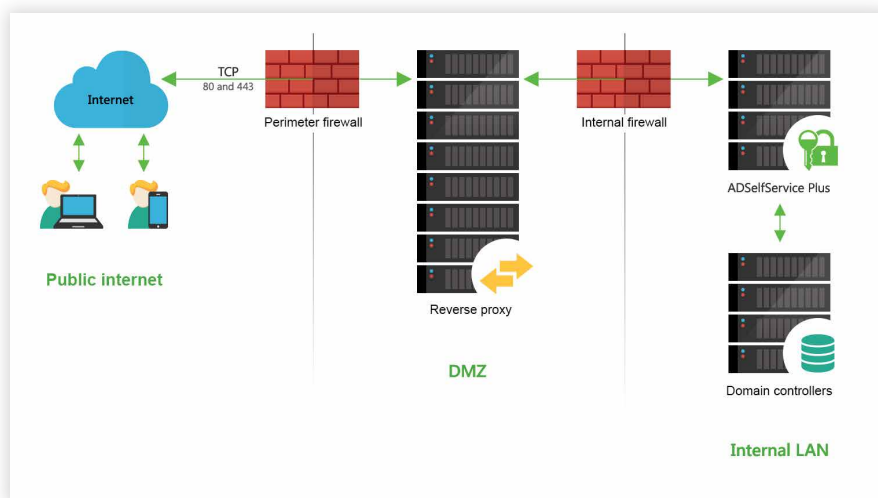


Figure 1: A reverse proxy server in a DMZ, with the ADSelfService Plus server hosted in the intranet.

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 (IIS) 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 be hosted in the DMZ instead. Either way, external machines never connect directly to the ADSelfService Plus server.

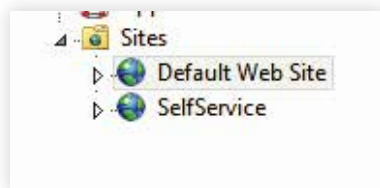
Your firewall will only permit the proxy server to access the ADSelfService Plus server, and only through the required port.

Important: 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**.

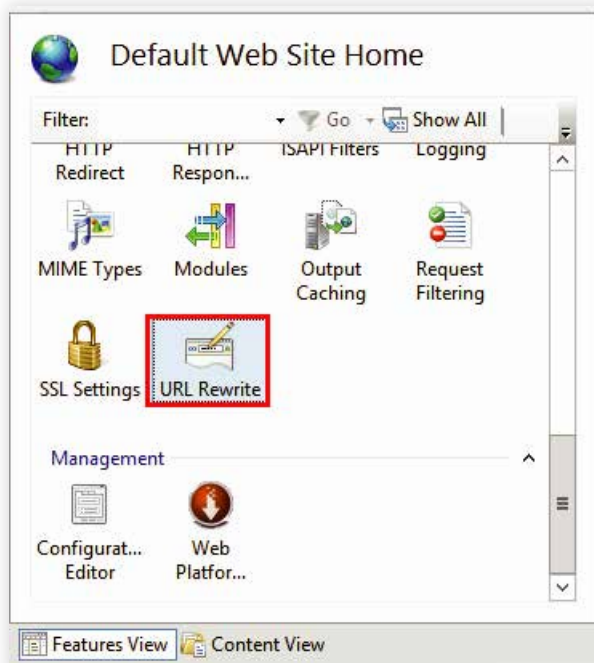
Configuring IIS as a reverse proxy for ADSelfService Plus

You can set up your Microsoft Internet Information Services (IIS) web server as a reverse proxy server for ADSelfService Plus. Follow the steps below to get started.

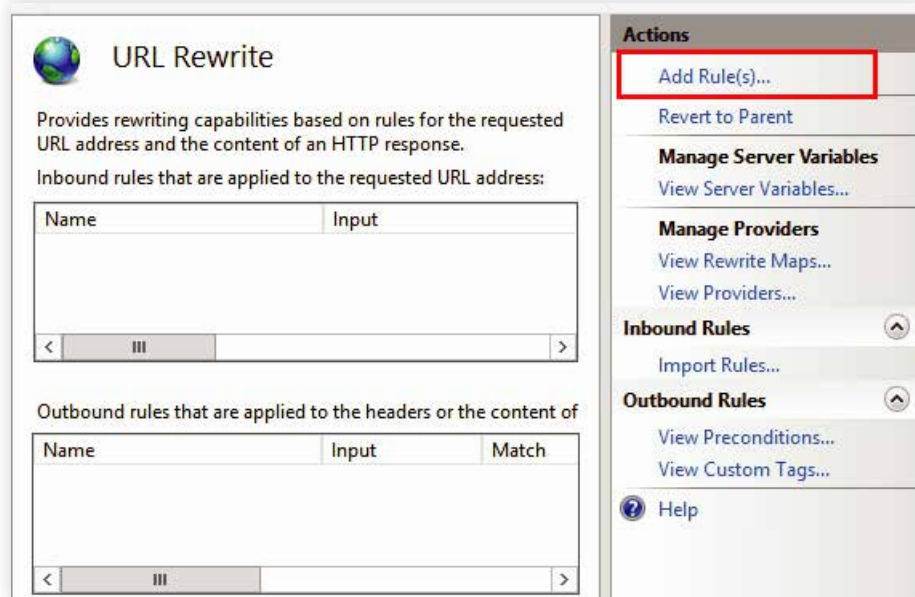
1. Install the URL Rewrite extension. You can use the Microsoft Web Platform Installer, or [download the extension directly](#).
2. Open IIS Manager.
3. Select **Default Web Site** from the tree view on the left pane.



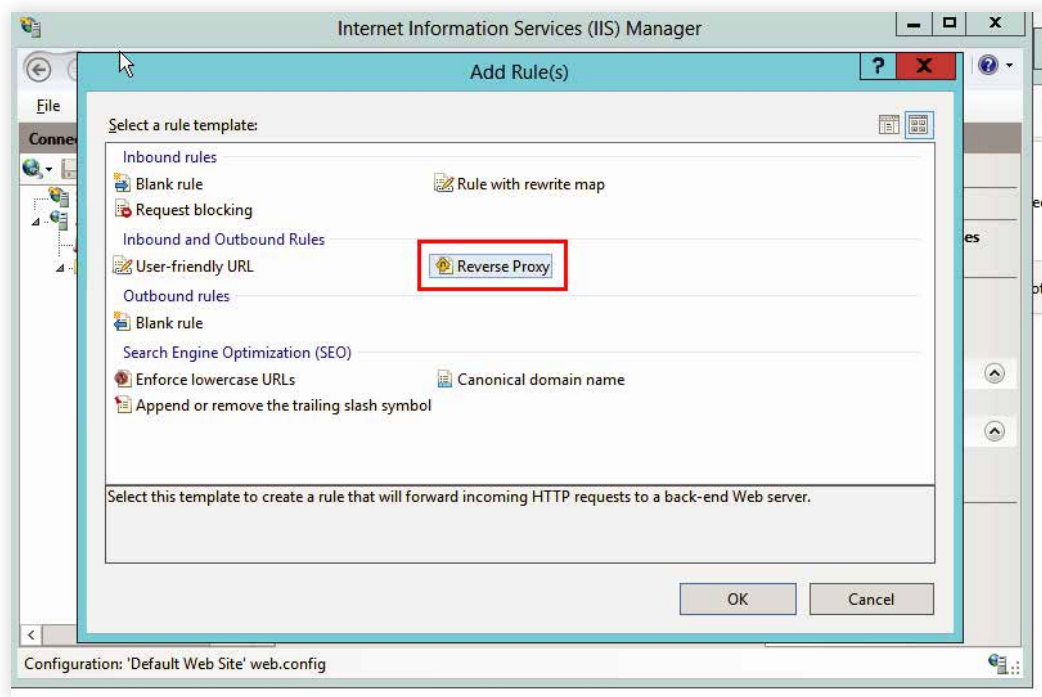
4. Double-click URL Rewrite.



5. In the right pane, under the *Actions* section, click **Add Rule(s)...**



6. In the *Add Rule(s)* window that opens, under *Inbound and Outbound Rules*, click **Reverse Proxy**.



7. In the *Add Reverse Proxy Rules* window that opens, under the *Inbound Rules* section, enter the ADSelfService Plus server's **URL** (hostname or IP address, and port number. Format sample: adselfservice-server:8888).

A. When HTTP is used

B. When HTTPS is used.

8. Click OK.

The setup for using IIS server as a reverse proxy for the ADSelfService Plus server is now complete.

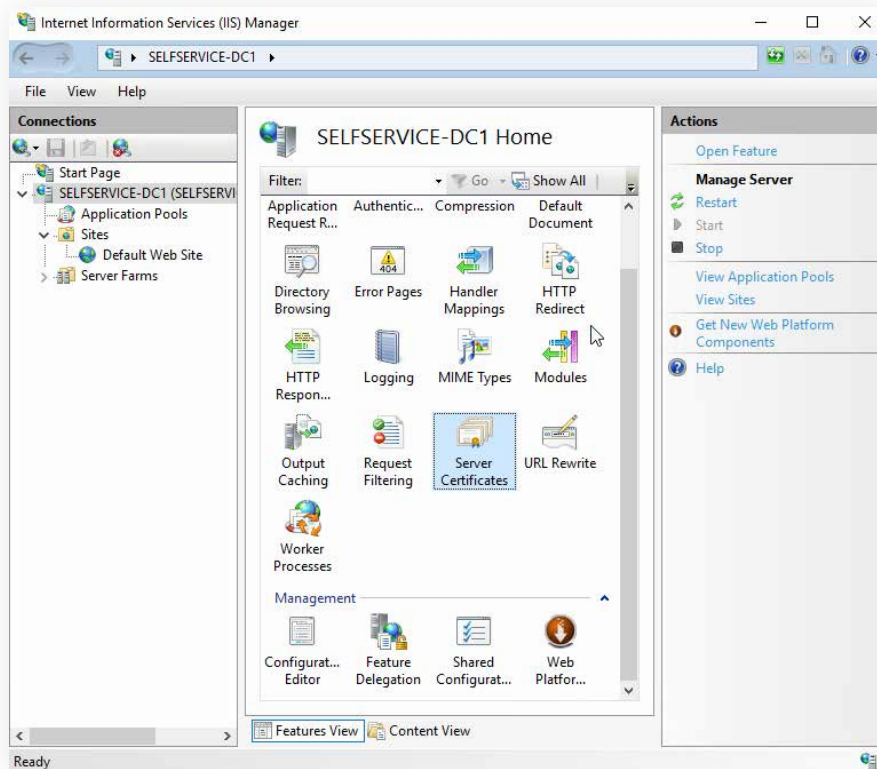
Note: The Enable SSL Offloading checkbox must be unchecked when HTTPS is used.

Steps required to run a proxy server with HTTPS protocol:

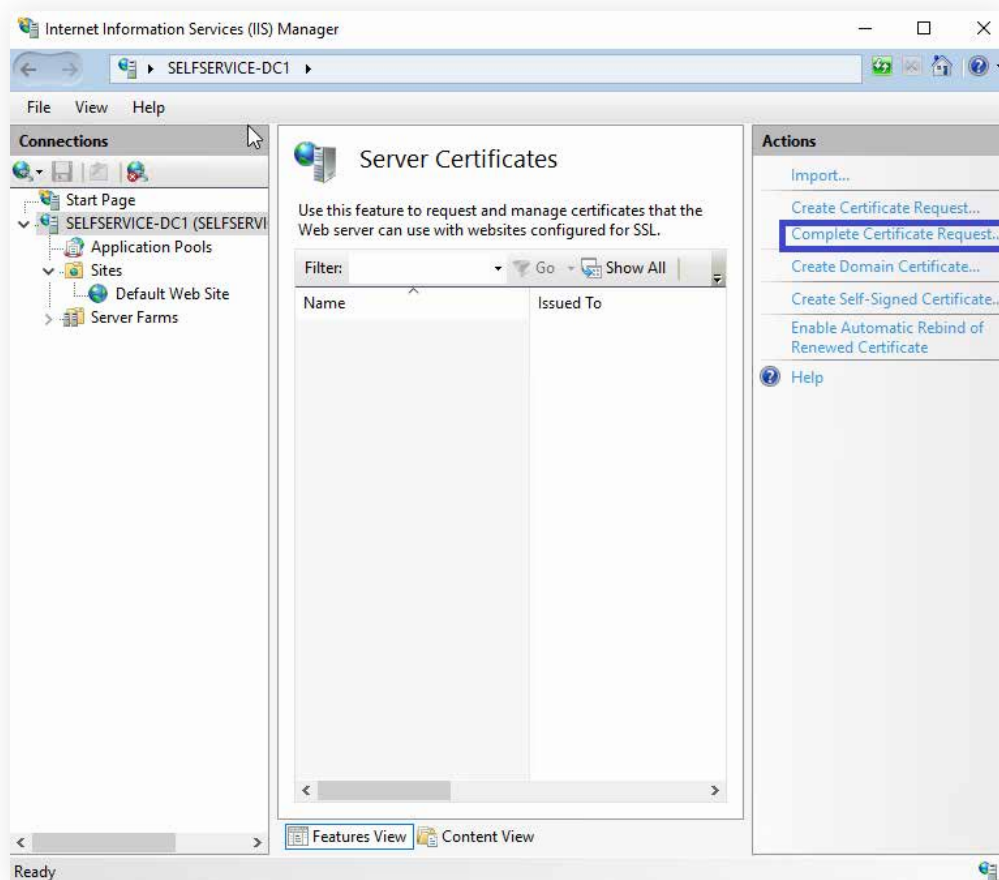
1. To run a proxy server with HTTPS protocol, the SSL certificate has to be [installed](#) in the IIS web server.
2. The HTTPS protocol must be [bound](#) to the IIS web server, where the ADSelfService Plus reverse proxy is configured. This binding must happen so that there is a secure connection between the browser and the ADSelfService Plus server.

How to Install an SSL/TLS certificate

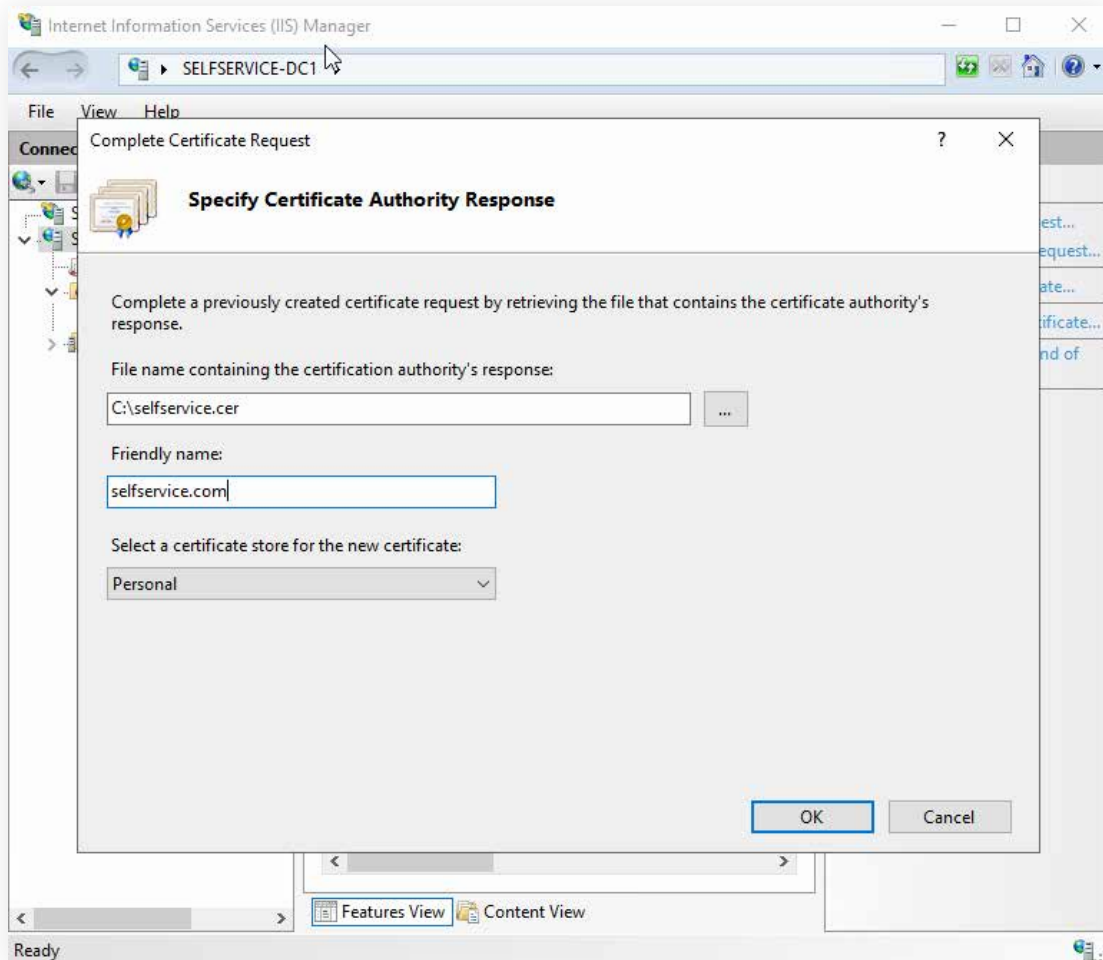
1. Go to **Start > Control Panel > Administrative Tools > Internet Information Services (IIS) Manager**.
2. In the **Connections** menu on the left, select the **server name** (host) where you want to install the certificate.
3. In the middle pane, click the **Server Certificates** icon under the Security section.



4. In the *Actions* menu on the right pane, click **Complete Certificate Request**.



5. In the **Complete Certificate Request** wizard, click "..."/>

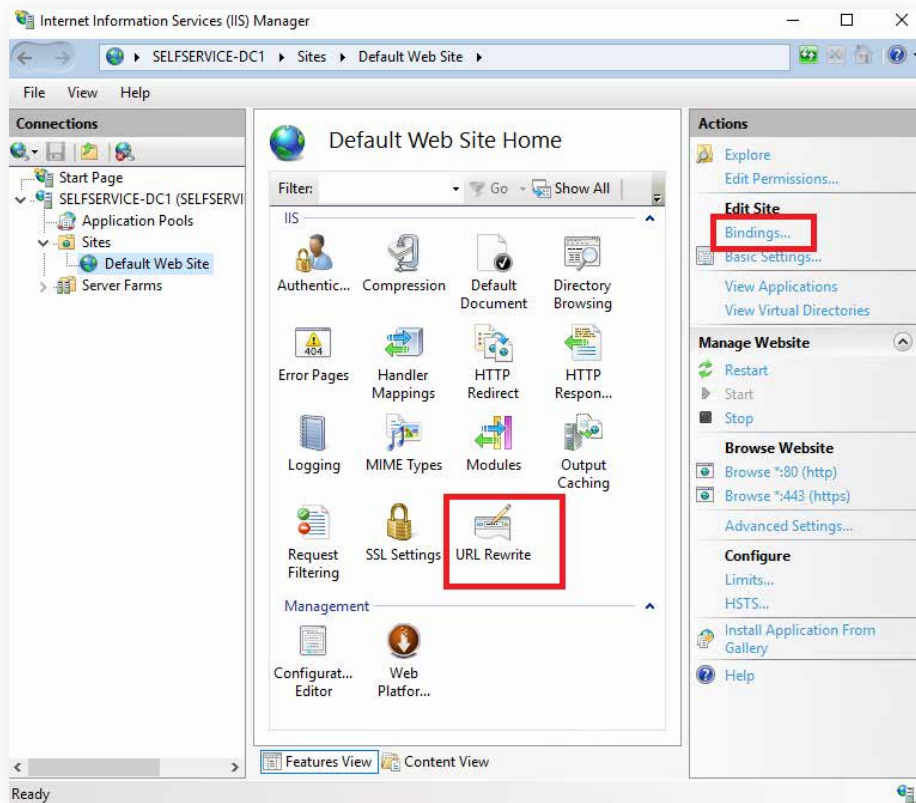


7. Click **OK**, and the newly installed certificate should appear in the refreshed Server Certificates List.

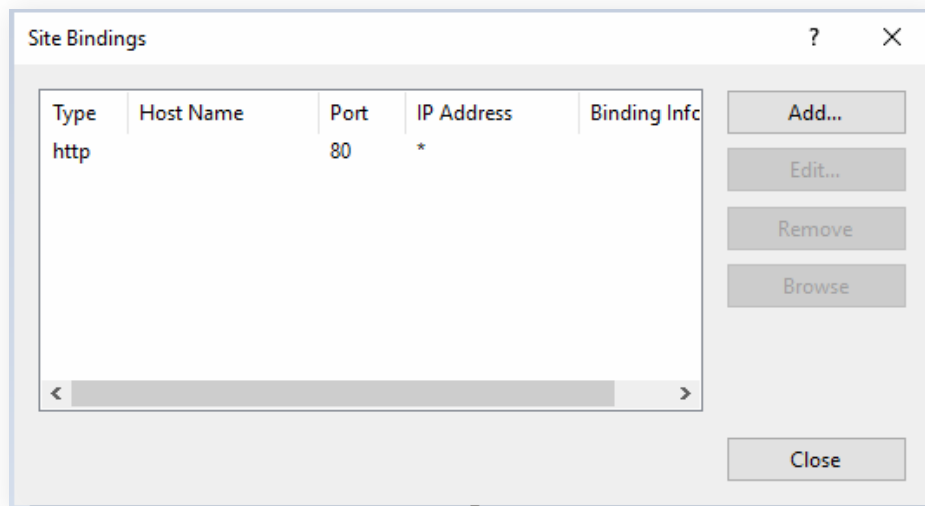
Note: If a self-signed certificate has been used in the ADSelfService Plus server to configure SSL, the IIS web server must be configured to trust the self-signed SSL certificate to enable communication between the servers.

Steps to bind an SSL certificate to the website

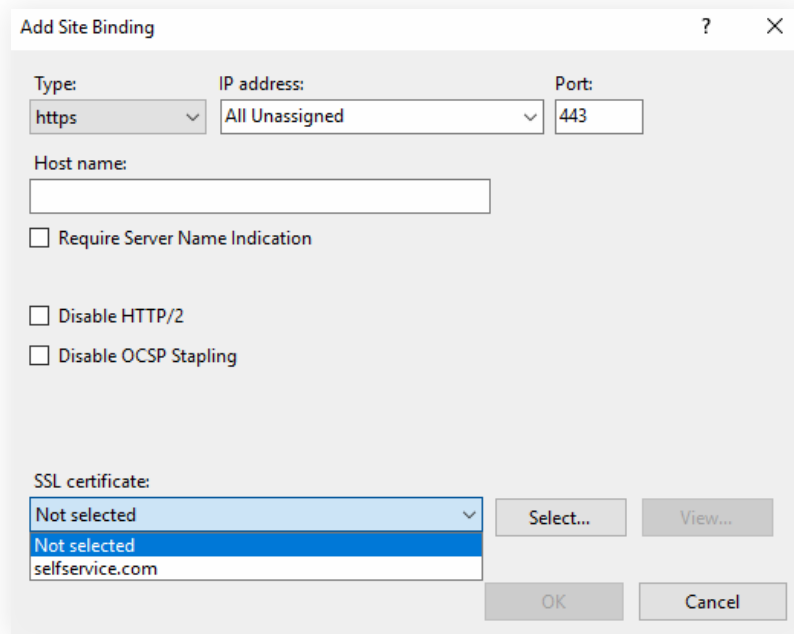
1. On the left pane, expand the **Sites** folder, from the **Connections** column.
2. Select **Default Web Site**.
3. Select **Bindings**, under the Actions pane on the right.



4. In the **Site Bindings** window that appears, select the **https** binding and select **Edit**. If there is **no https** binding link in the Site Bindings window, choose **Add**, and change the **Type** from **HTTP** to **HTTPS**.



5. From the **SSL certificate** drop-down in the **Add Site Binding** window, select a certificate that you want to bind to the website. In case of multiple certificates in this drop-down list, select the **View** button beside the **SSL certificate** drop-down to see information about each certificate, and choose the one that you want to add.



6. Click **OK**.

Notes: You may need to stop and restart the machine where the IIS is installed for changes to take effect. In some cases, a mere restart of the IIS services is not sufficient for the changes to get implemented. A reboot is required.

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