

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



## Table of Contents

Document summary	1
Prerequisites	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	6
About ManageEngine ADSelfService Plus	9

## 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.

## 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\: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?

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 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**.

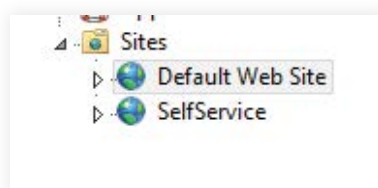
**Note for FIDO passkey users:**

- 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.

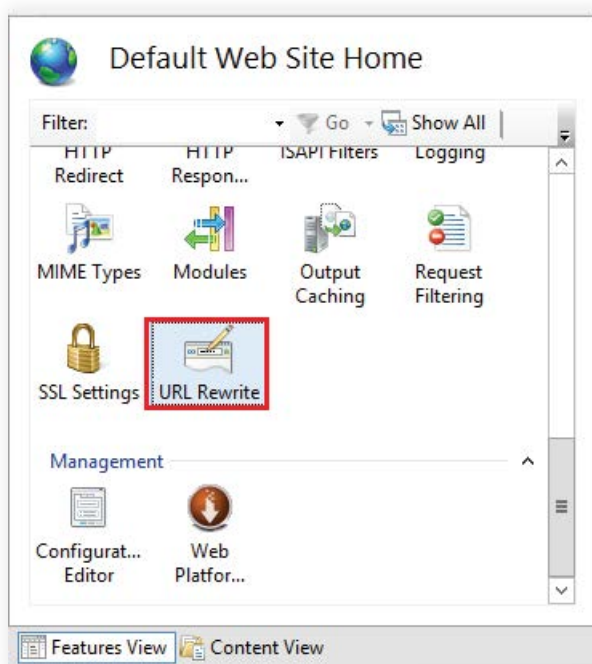
## Configuring IIS as a reverse proxy for ADSelfService Plus

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.

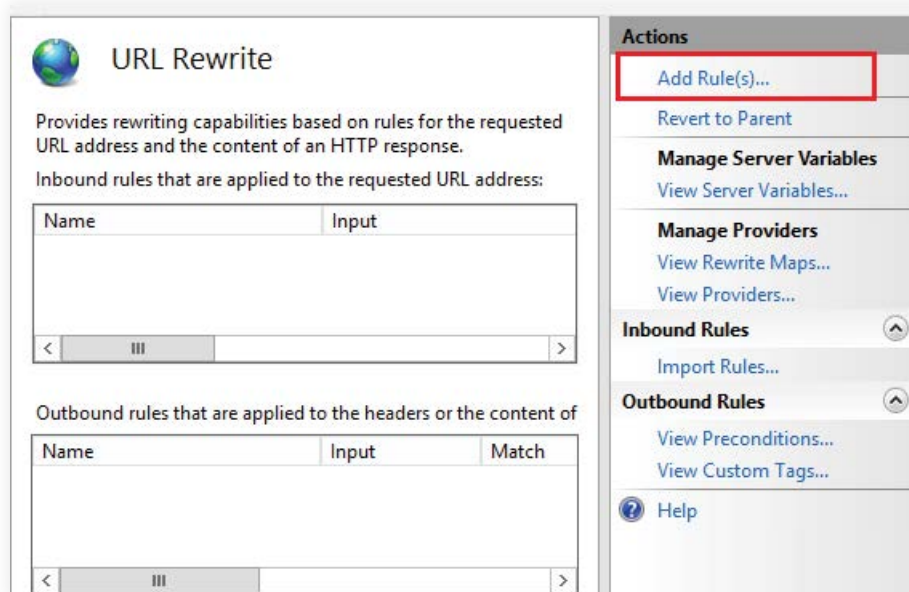
1. **Install the URL Rewrite extension.** You can use the Microsoft Web Platform Installer, or [download the extension directly](#).
2. Open **IIS Manager**.
3. Select **Default Web Site** from the tree view on the left pane.



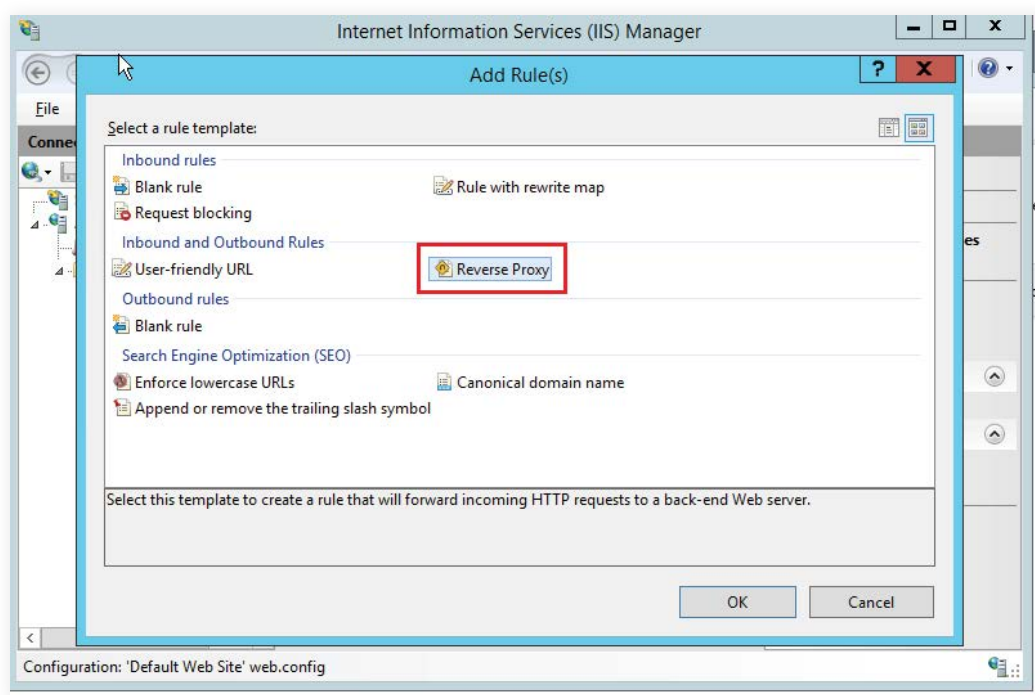
4. Double-click **URL Rewrite**.



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

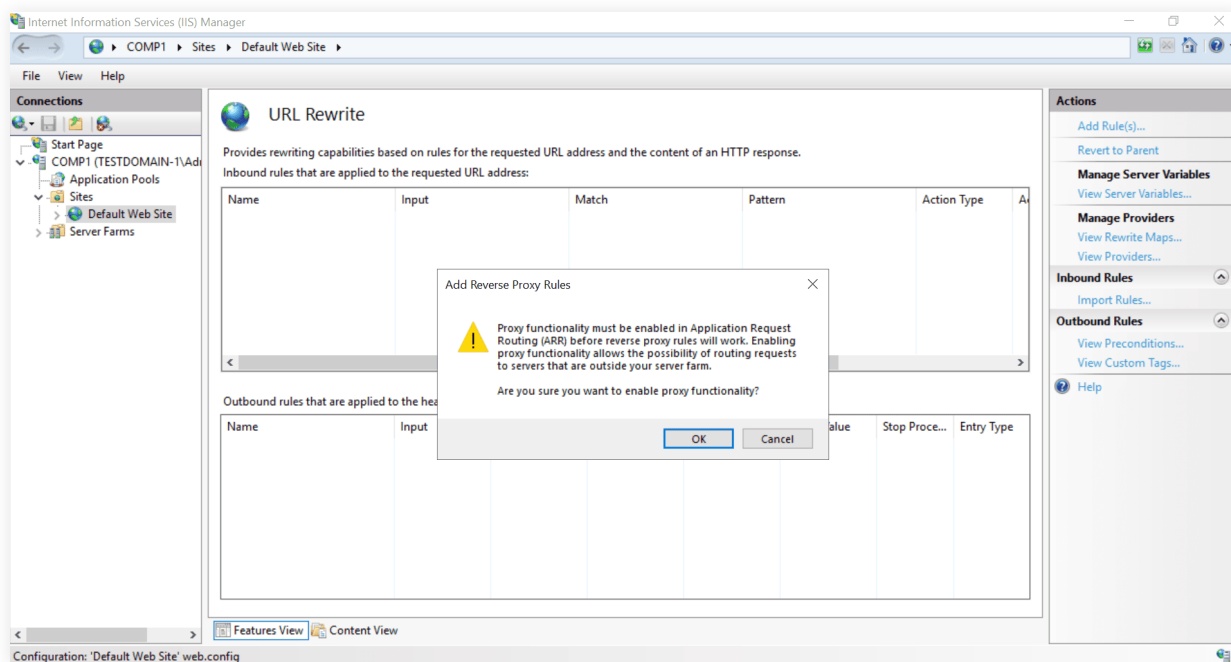


6. In the **Add Rule(s)** window that opens, under **Inbound and Outbound Rules**, click **Reverse Proxy**.

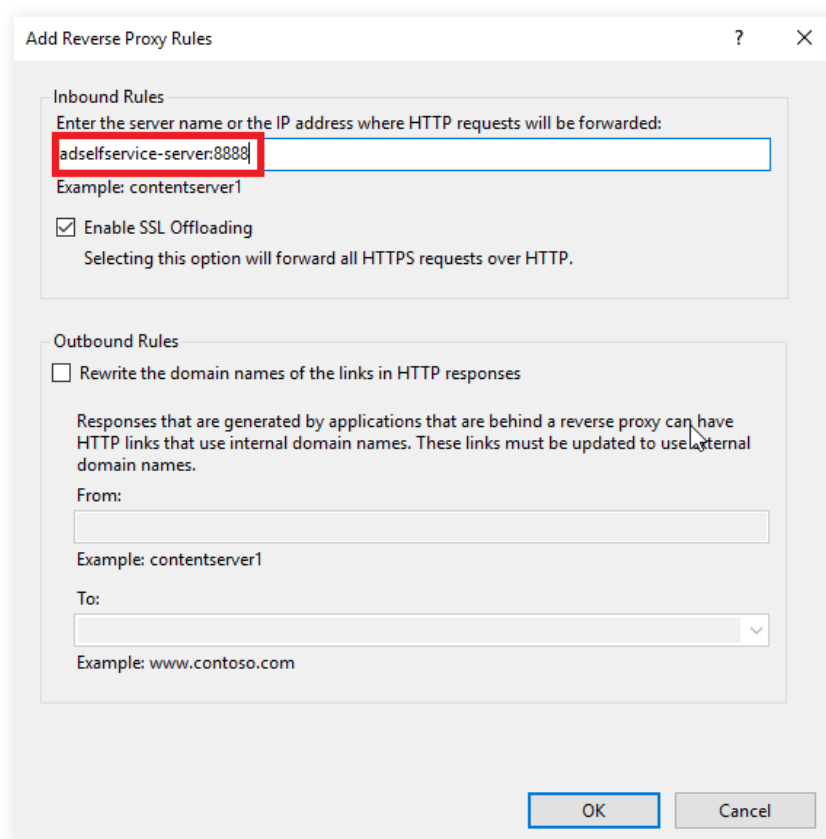


7. The IIS Server may ask the user to install the **Application Request Routing** extension.

This can be installed from [here](#). Following installation, the below warning may also be displayed, click **OK** to proceed.



8. 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

The screenshot shows a dialog box titled "Add Reverse Proxy Rules". It is divided into two main sections: "Inbound Rules" and "Outbound Rules".

**Inbound Rules:**

- Text: "Enter the server name or the IP address where HTTP requests will be forwarded:"
- Text box: "adssp:9251"
- Text: "Example: contentserver1"
- Checkbox:  "Enable SSL Offloading"
- Text: "Selecting this option will forward all HTTPS requests over HTTP."

**Outbound Rules:**

- Checkbox:  "Rewrite the domain names of the links in HTTP responses"
- Text: "Responses that are generated by applications that are behind a reverse proxy can have HTTP links that use internal domain names. These links must be updated to use external domain names."
- Text: "From:"
- Text box: (empty)
- Text: "Example: contentserver1"
- Text: "To:"
- Dropdown menu: (empty)
- Text: "Example: www.contoso.com"

At the bottom right, there are two buttons: "OK" and "Cancel".

#### B. When HTTPS is used

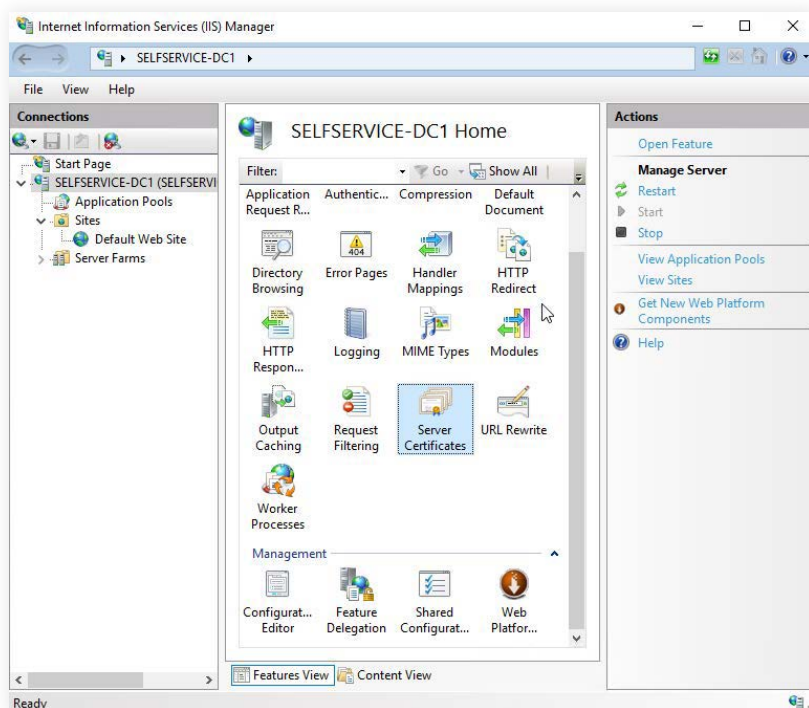
9. Select the **Enable SSL Offloading** checkbox if the ADSelfService Plus server is running under HTTP and IIS server is running HTTPS. If the ADSelfService Plus server is running under HTTPS, this can be left unchecked.

10. Click **OK**.

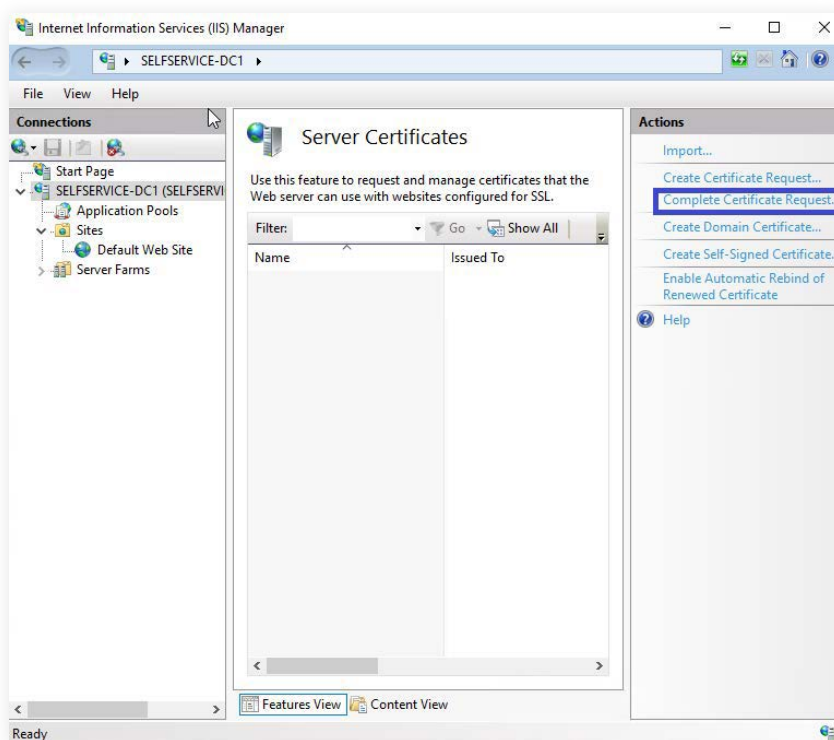
The setup for using IIS server as a reverse proxy for the ADSelfService Plus server is now complete.

## 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.

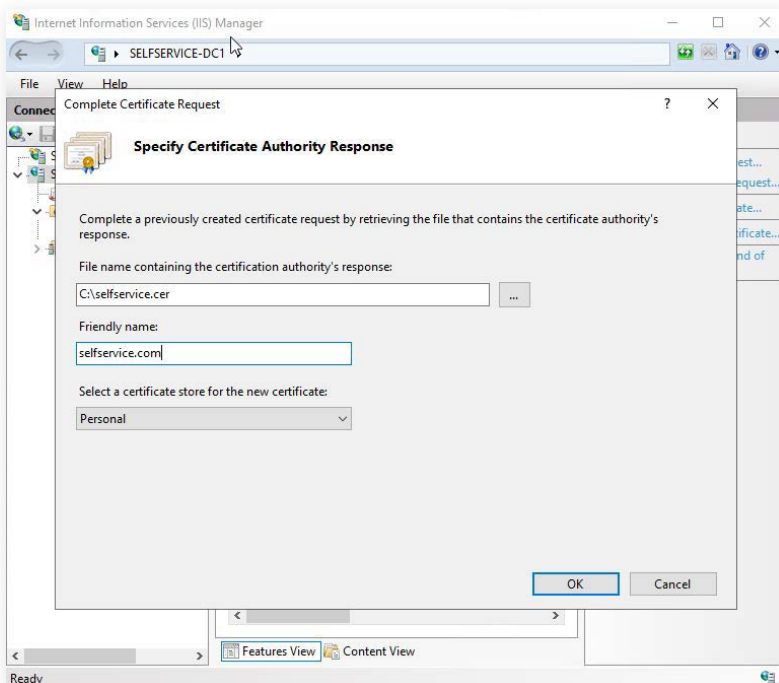


4. In the **Actions** menu on the right pane, click **Complete Certificate Request**.





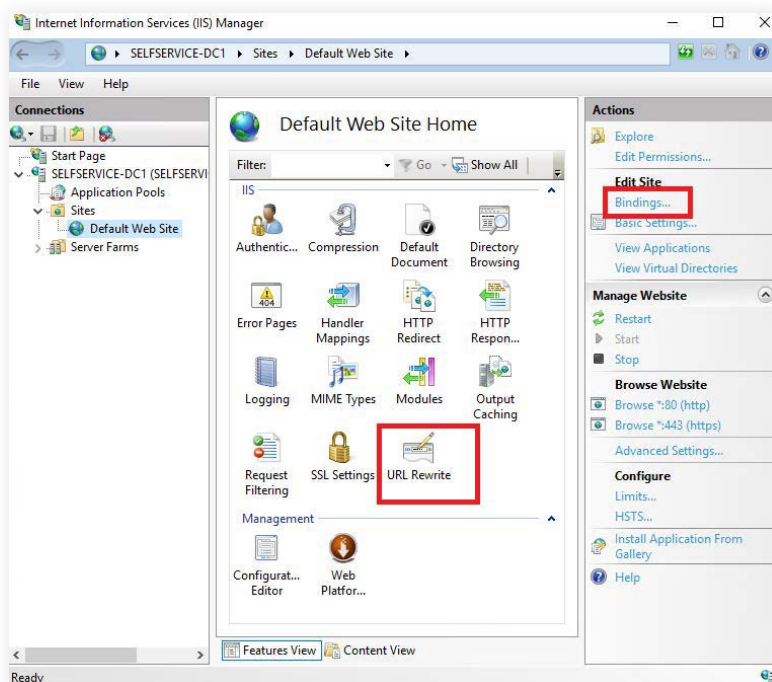
- In the **Complete Certificate Request** wizard, click "..." to browse and select **Your Server Certificate** file.
- Enter a name that will serve as an internal reference name to distinguish the file later. Using the Certificate Authority's name and expiration date can make it easier to find.



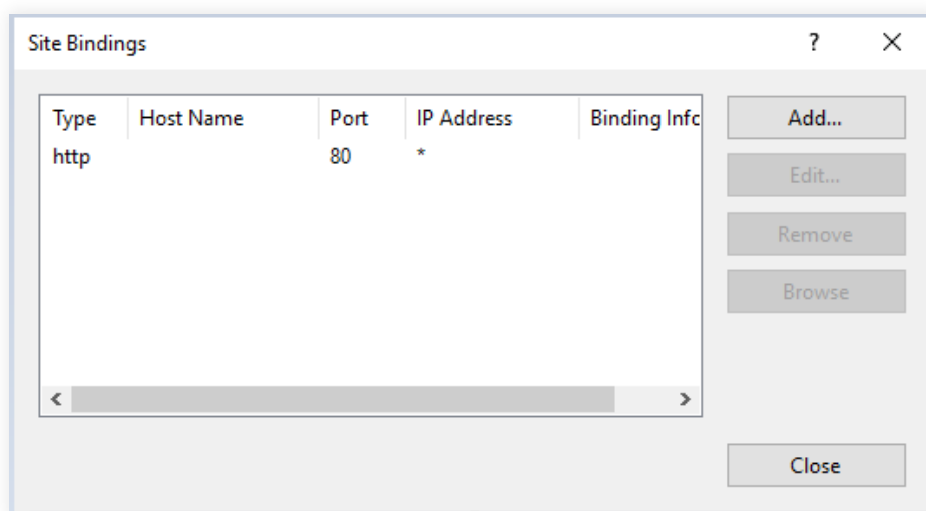
- Click **OK**, and the newly installed certificate should appear in the refreshed Server Certificates List.

### Steps to bind an SSL certificate to the website

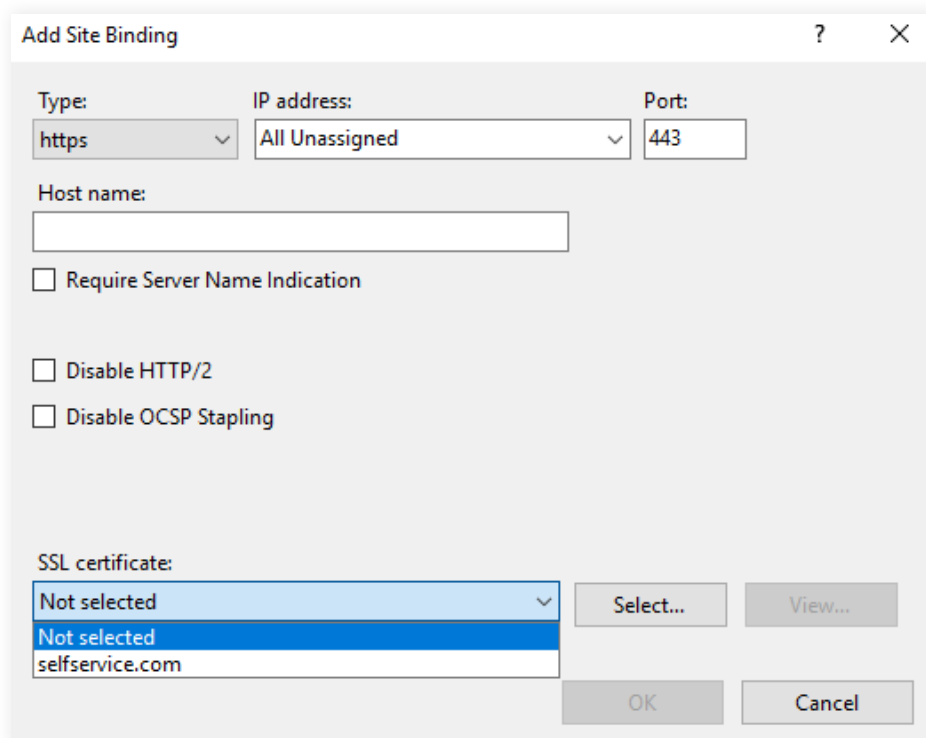
- On the left, expand the **Sites** folder, from the **Connections** column.
- Select **Default Web Site**.
- Select **Bindings**, under the Actions pane on the right.



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](mailto:support@adselfserviceplus.com). One of our product experts will be happy to help you.

## Our Products

AD360 | Log360 | ADManager Plus | ADAudit Plus | RecoveryManager Plus | M365 Manager Plus

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 [www.manageengine.com/products/self-service-password](http://www.manageengine.com/products/self-service-password).

\$ Get Quote

↓ Download