Skip To Content
ArcGIS Enterprise ArcGIS Enterprise
Portal Server Data Stores Cloud

English ⌄
EnglishDeutschEspañolFrançais日本語Русский简体中文

🔍 ✕ Sign In

🔍 ✕

User Avatar
User Avatar
My Profile Sign Out

Installation Guides

OverviewServerPortalWeb AdaptorData StoreGeoEventMore...
Web Adaptor ▾

Enabling SSL on your web server

ArcGIS 10.3 (IIS) Other versions ⌄
10.6IISJava (Windows)Java (Linux)10.5IISJava (Windows)Java (Linux)10.4IISJava (Windows)Java (Linux)10.3IISJava (Windows)Java (Linux)

In this topic

- Creating an SSL certificate
- Binding the certificate to the website
- Testing your site

The SSL protocol is a standard security technology used to establish an encrypted link between a web server and a web client. SSL facilitates secure network communication by identifying and authenticating the server as well as ensuring the privacy and integrity of all transmitted data. Since SSL prevents eavesdropping on or tampering with information sent over the network, it should be used with any login or authentication mechanism and on any network where communication contains confidential or proprietary information.

The use of SSL ensures that names, passwords, and other sensitive information cannot be deciphered as they are sent between the Web Adaptor and the server. When you use SSL, you connect to your web pages and resources using the HTTPS protocol instead of HTTP.

In order to use SSL, you need to obtain an SSL certificate and bind it to the website that hosts the Web Adaptor. Each web server has its own procedure for loading a certificate and binding it to a website.

Creating an SSL certificate

To be able to create an SSL connection between the Web Adaptor and your server, the web server requires an SSL certificate. An SSL certificate is a digital file that contains information about the identity of the web server. It also contains the encryption technique to use when establishing a secure channel between the web server and ArcGIS Server. An SSL

Certificate authority (CA) signed certificates should be used for production systems, particularly if your deployment of ArcGIS Server is going to be accessed from users outside your organization. For example, if your server is not behind your firewall and accessible over the Internet, using a CA-signed certificate assures clients from outside your organization that the identity of the website has been verified.

In addition to being signed by the owner of the website, an SSL certificate may be signed by an independent CA. A CA is usually a trusted third party that can attest to the authenticity of a website. If a website is trustworthy, the CA adds its own digital signature to that website's self-signed SSL certificate. This assures web clients that the website's identity has been verified.

When using an SSL certificate issued by a well-known CA, secure communication between the server and the web client occurs automatically with no special action required by the user. There is no unexpected behavior or warning message displayed in the web browser, since the website has been verified by the CA.

Domain certificates

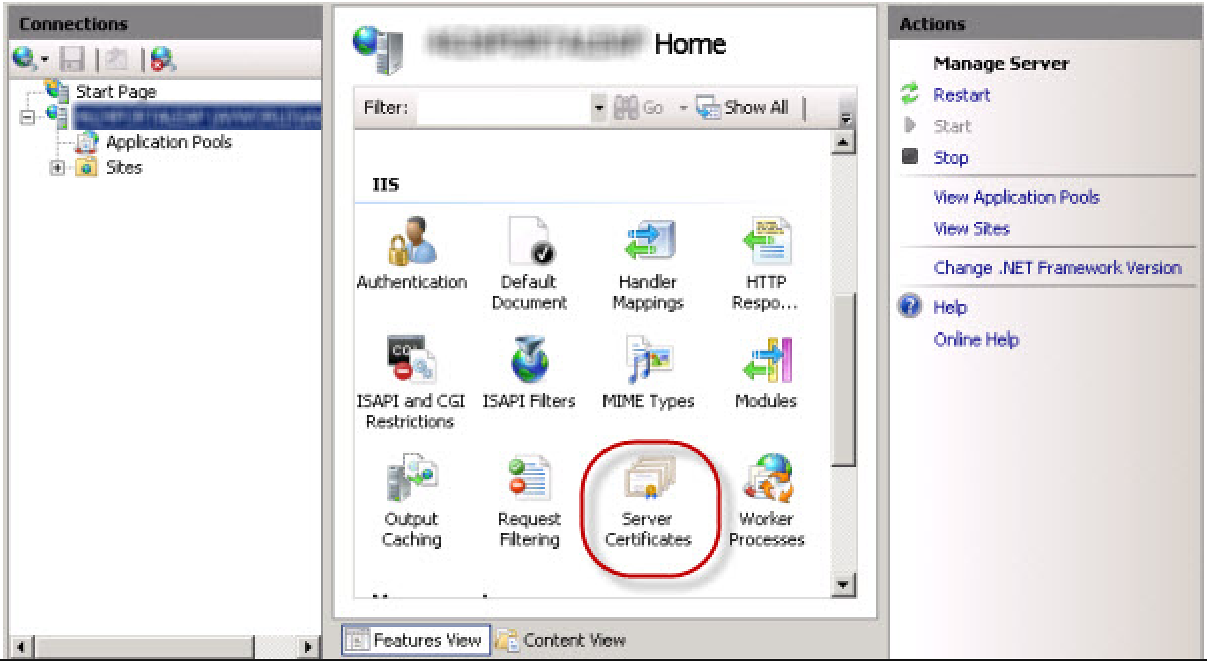
If your server is located behind your firewall and using a CA-signed certificate is not possible, using a domain certificate is an acceptable solution. A domain certificate is an internal certificate signed by your organization's certificate authority. Using a domain certificate helps you reduce the cost of issuing certificates and eases certificate deployment, since certificates can be generated quickly within your organization for trusted internal use.

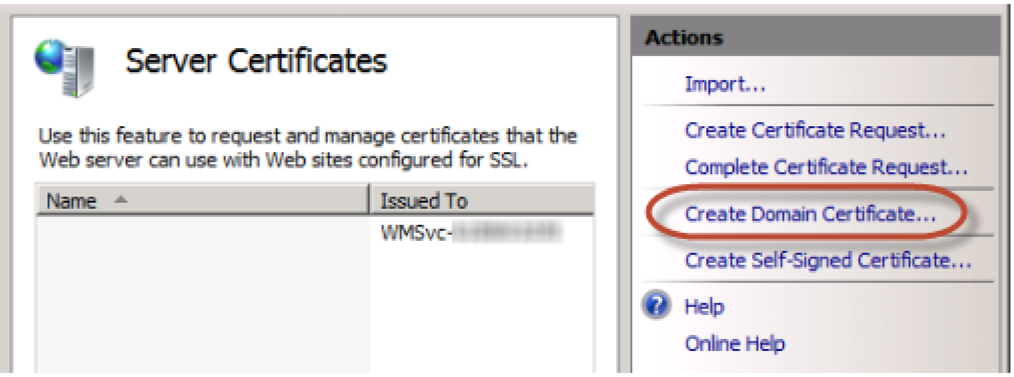
Users within your domain will not experience any of the unexpected behavior or warning messages normally associated with a self-signed certificate, since the website has been verified by the domain certificate. However, domain certificates are not validated by an external CA, which means users visiting your site from outside your domain will not be able verify that your certificate really represents the party it claims to represent. External users will see browser warnings about the site being untrusted which may lead them to think that they are actually communicating with a malicious party and be turned away from your site.

Creating a domain certificate in IIS

In IIS Manager, do the following to create a domain certificate:

1. In the Connections pane, select your server in the tree view and double-click Server Certificates.





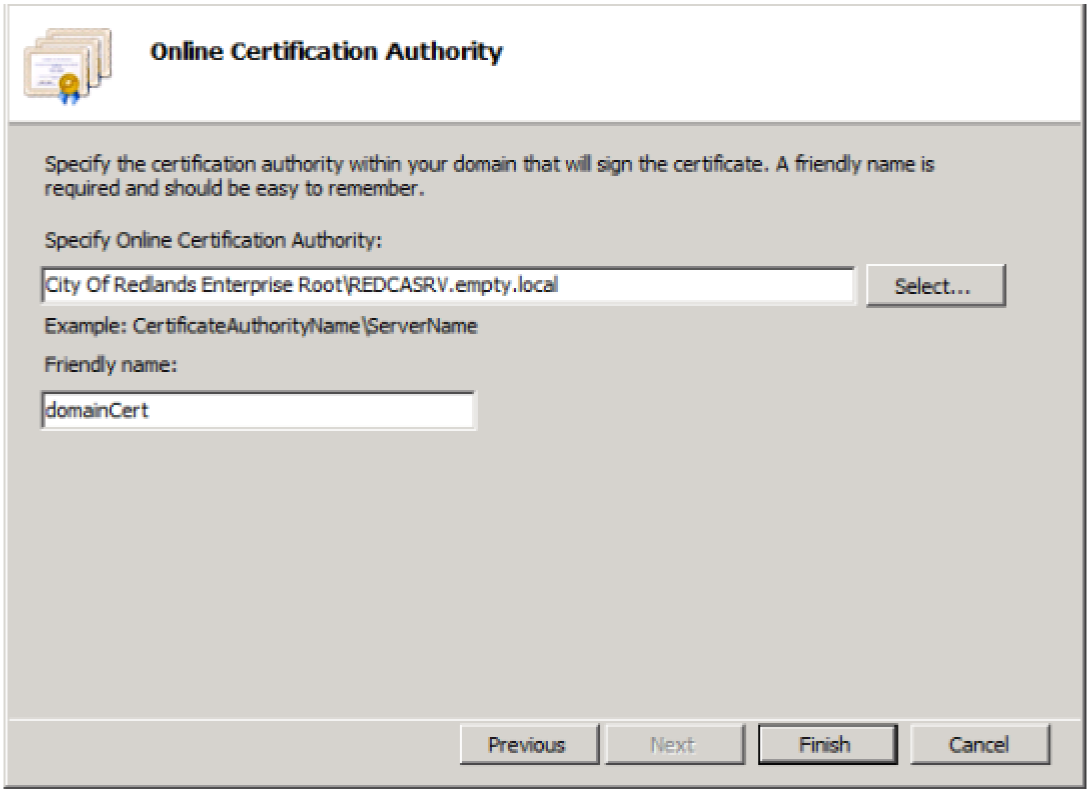
Server Certificates

Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

Name	Issued To
	WMSvc-[redacted]

Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Help
Online Help

3. In the Distinguished Name Properties dialog box, enter the required information for the certificate:
    1. For the Common name, you must enter the fully qualified domain name of the machine, for example, gisserver.domain.com.
    2. For the other properties, enter the information specific for your organization and location.
4. Click Next.
5. In the Online Certification Authority dialog box, click Select and choose the certification authority within your domain that will sign the certificate. If this option is unavailable, enter your domain certification authority in the Specify Online Certification Authority field, for example, City Of Redlands Enterprise Root\REDCASRV.empty.local. If you need help with this step, consult your system administrator.



Online Certification Authority

Specify the certification authority within your domain that will sign the certificate. A friendly name is required and should be easy to remember.

Specify Online Certification Authority:

City Of Redlands Enterprise Root\REDCASRV.empty.local

Example: CertificateAuthorityName\ServerName

Friendly name:

domainCert

6. Enter a user-friendly name for the domain certificate and click Finish.

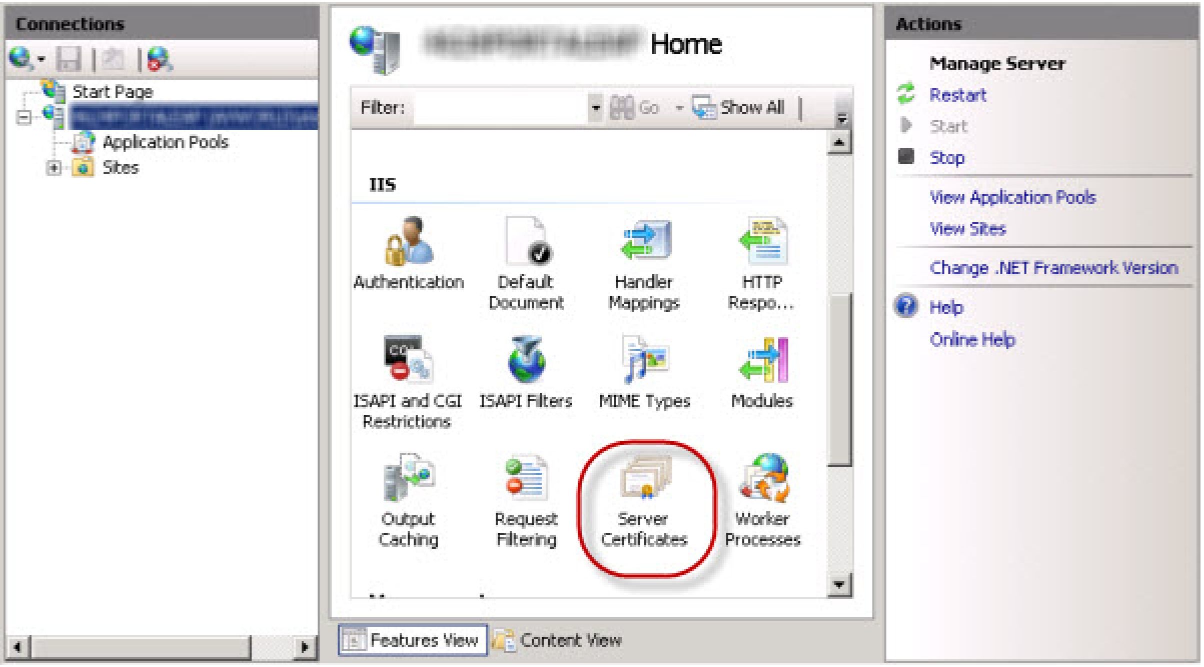
The final step is for you to bind the domain certificate to SSL port 443. See the Binding the certificate to the website below for instructions.

Self-signed certificates

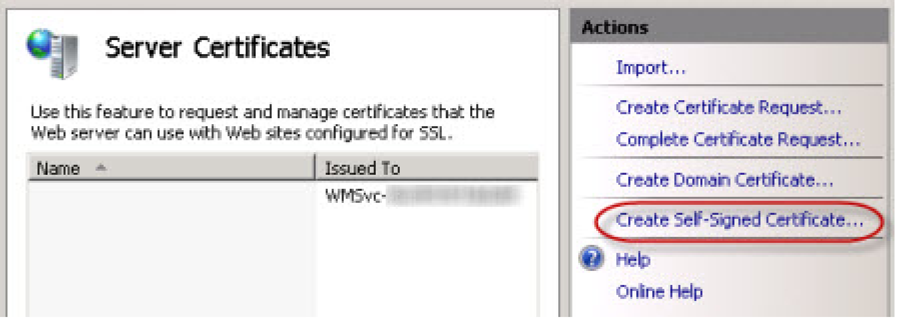
Creating a self-signed certificate in IIS

In IIS Manager, do the following to create a self-signed certificate:

1. In the Connections pane, select your server in the tree view and double-click Server Certificates.



2. In the Actions pane, click Create Self-Signed Certificate.


Server Certificates
Name
Issued To
WMSvc-
Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Help
Online Help

Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

3. Enter a user-friendly name for the new certificate and click OK.

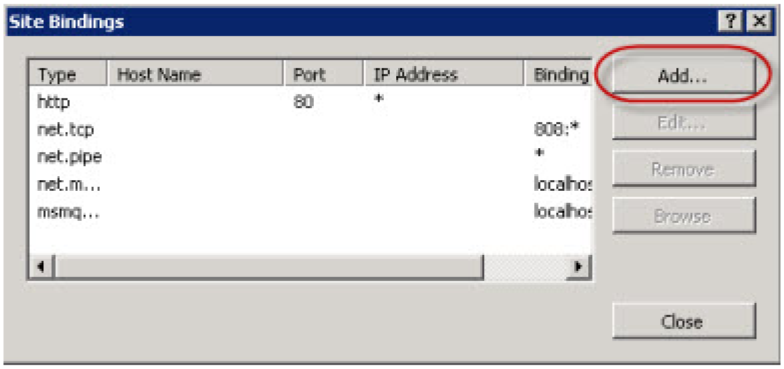
The final step is for you to bind the self-signed certificate to SSL port 443. See Binding the certificate to the website below for instructions.

Binding the certificate to the website

Once you've created an SSL certificate, you'll need to bind it to the website hosting the Web Adaptor. Binding refers to the process of configuring the SSL certificate to use port 443 on the website. The instructions for binding a certificate with the website vary depending on the platform and version of your web server. For instructions, consult your system administrator or your web server's documentation. For example, the steps for binding a certificate in IIS are below.

Binding a certificate to port 443 in IIS

- If port 443 is not available in the Bindings list, click Add. From the Type drop-down list, select https. Leave the port at 443.

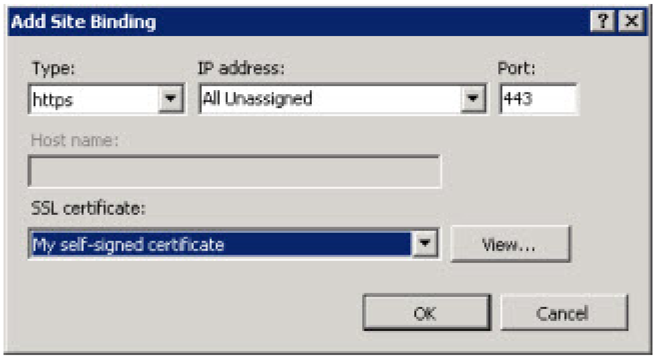


Site Bindings

Type	Host Name	Port	IP Address	Binding
http		80	*	
net.tcp				808:*
net.pipe				*
net.m...				localhos
msmq...				localhos

- If port 443 is listed, select the port from the list and click Edit.

2. From the SSL certificate drop-down list, select your certificate name and click OK.



Add Site Binding

Type: https

IP address: All Unassigned

Port: 443

Host name:

SSL certificate: My self-signed certificate

Testing your site

After binding the certificate to the website, you can configure your Web Adaptor for use with the server. You will need to access the Web Adaptor's configuration page using an HTTPS URL such as https://webadaptor.domain.com/arcgis/webadaptor.

After you've configured your Web Adaptor, you should test that SSL is working properly by making an HTTPS request to ArcGIS Server Manager, for example, https://webadaptor.domain.com/arcgis/manager.

For more detail on testing your site with SSL, see the Microsoft instructions on how to set up SSL on IIS.