ArcGIS Web Adaptor (IIS) 11.4 Installation Guide

THE SCIENCE OF WHERE

Table of Contents

Introduction

Welcome to the ArcGIS Web Adaptor installation guide

ArcGIS Web Adaptor allows you to integrate your existing web server with an ArcGIS Enterprise server site, portal, or ArcGIS Monitor. Use this guide to install and configure the web adaptor. To get started, see Get started with ArcGIS Web Adaptor.

Questions, feedback, and information

Copyright information

Get started with ArcGIS Web Adaptor

You can configure ArcGIS Web Adaptor to work with an ArcGIS Enterprise server site or portal. You may need multiple ArcGIS Web Adaptor instances for your deployment. You cannot configure the same Web Adaptor with multiple components.

Once you decide how you'll be using ArcGIS Web Adaptor, see the sections below to get started.

Use ArcGIS Web Adaptor with a server site

If you'll be using ArcGIS Web Adaptor with a server site, see the following topics to get started:

- Use ArcGIS Web Adaptor with a server site
- Steps to implement ArcGIS Web Adaptor

Use ArcGIS Web Adaptor with Portal for ArcGIS

ArcGIS Web Adaptor is a required component of Portal for ArcGIS. See the following topics to get started:

- Use ArcGIS Web Adaptor with portal
- Steps to implement ArcGIS Web Adaptor

Enable IIS components

Automatically enable IIS components

To install ArcGIS Web Adaptor, certain Microsoft Internet Information Services (IIS) components are required.

⚠ Caution:

You must enable IIS and the required components before proceeding with the ArcGIS Web Adaptor installation.

If you've already enabled IIS but are missing the required IIS components, the installation displays a message indicating that IIS components are missing. You have the option to allow the Web Adaptor installation to automatically enable the required IIS components. You can alternatively enable the components manually. The setup will not proceed if the required IIS components are not enabled.

To automatically enable the missing IIS components, complete the following steps:

1. Review the missing IIS components on the **IIS requirements verification** dialog box. You may find it helpful to record the missing components for your records.
2. Click **I Agree**.

The components are enabled and you can continue with the setup process.

To manually enable the missing IIS components, click **Cancel**. To learn how to manually enable the missing IIS components, see Manually enable IIS components.

Once all required components have been enabled, launch the Web Adaptor installation again by double-clicking **Setup.exe** in the ArcGIS Web Adaptor (IIS) setup folder.

Manually enable IIS components

ArcGIS Web Adaptor requires that IIS and specific IIS components be enabled on supported Windows operating systems. The setup will not proceed if IIS is not detected and specific IIS components are not enabled.

⚠ Caution:
You must enable IIS and the required components before proceeding with the ArcGIS Web Adaptor installation.

If you've already enabled IIS but are missing the required IIS components, the installation displays a message indicating that certain IIS components are missing. You have the option to allow the installation to automatically enable the required IIS components. However, depending on your organization's security policies, it may be necessary to manually enable the required IIS components, as described below.

To enable IIS and the required IIS components on Windows Server 2016, Windows Server 2019, and Windows Server 2022, complete the following steps:

1. Open **Server Manager** and click **Manage** > **Add Roles and Features**. Click **Next**.
2. Select **Role-based or feature-based installation** and click **Next**.
3. Select the appropriate server. The local server is selected by default. Click **Next**.
4. Enable **Web Server (IIS)** and click **Next**.
5. No additional features are necessary to install the Web Adaptor, so click **Next**.
6. On the **Web Server Role (IIS)** dialog box, click **Next**.
7. On the **Select role services** dialog box, verify that the web server components listed in the Required IIS components section are enabled. Click **Next**.
8. Verify that your settings are correct and click **Install**.
9. When the installation completes, click **Close** to close the wizard.

To enable IIS and the required IIS components on Windows 10 and Windows 11, complete the following steps:

1. Open **Control Panel** and click **Programs and Features** > **Turn Windows features on or off**.
2. Enable **Internet Information Services**.
3. Expand the **Internet Information Services** feature and verify that the web server components listed in the Required IIS components section are enabled.
4. Click **OK**.

Required IIS components

The IIS components listed below satisfy the minimum requirements to run the Web Adaptor. If other IIS components are enabled, they do not need to be removed.

- Web Server
  - Common HTTP Features
    - Default Document
    - Static Content

    - Security
        - Request Filtering
        - Windows Authentication
    - Application Development
        - ISAPI Extensions
        - ISAPI Filters
        - WebSocket Protocol
- Management Tools
    - IIS Management Console

Verify system requirements

ArcGIS Web Adaptor 11.4 system requirements

The system and hardware requirements to run ArcGIS Web Adaptor are listed below. For information about earlier versions, see Archives.

Review the deprecation notice to determine whether your hardware and software are still compatible with the current ArcGIS version.

ArcGIS Web Adaptor (IIS)

ArcGIS Web Adaptor (IIS) can be installed on a Microsoft Windows machine and integrated with an Internet Information Server (IIS) web server.

Microsoft IIS required components

Microsoft Internet Information Server (IIS) must be enabled along with specific IIS components. The setup will not proceed if IIS is not detected and specific IIS components enabled.

If you have IIS 10 installed but are missing required IIS components, the setup will display the **IIS requirements verification** dialog box. This gives you the option to allow the installation to automatically enable any missing required IIS components. To do so, click **I agree**.

Note:
If you're going to perform a silent installation of ArcGIS Web Adaptor, all required IIS components must be enabled manually. The setup will not automatically enable missing IIS components when you perform a silent installation.

To learn how to enable IIS on your operating system and optionally enable the missing IIS 10 components manually, see Manually enable IIS and required IIS components.

Caution:
To successfully install and configure ArcGIS Web Adaptor, you must enable IIS and the required components before installing the prerequisites specified in the next section.

Prerequisites

The following prerequisites must be installed on the machine where ArcGIS Web Adaptor (IIS) will be installed:

- Microsoft Web Deploy 4.0
- ASP.NET Core Runtime - Windows Hosting Bundle 8.x

Note:
You must install the ASP.NET Core Runtime - Windows Hosting Bundle, which includes the .NET Runtime and IIS support.

Caution:
If you installed the ASP.NET Core Runtime - Windows Hosting Bundle before enabling IIS and the required components, you must repair the bundle installation using the bundle installer.

Supported web servers

The IIS web server versions available on supported Windows operating systems are supported for use with ArcGIS Web Adaptor (IIS).

Updates on these operating systems and web servers are supported unless otherwise stated. The operating system version and updates must also be supported by the application or web server provider.

Maximum installation instances

The maximum number of instances of ArcGIS Web Adaptor (IIS) you can install on a single machine depends on how you install the first ArcGIS Web Adaptor instance. If you install the first instance using the ArcGIS Web Adaptor setup program, you can install a maximum of 51 instances of the same version of ArcGIS Web Adaptor on a single machine. However, if you install the first instance using ArcGIS Enterprise Builder, you can install a maximum of 50 instances of the same version or ArcGIS Web Adaptor on a single machine. If more instances are required, install them on a separate machine.

If you have earlier versions installed on the machine, you are not required to uninstall them. For example, you can have 5 instances of ArcGIS Web Adaptor at an earlier release and 51 instances of ArcGIS Web Adaptor 11.4 installed on the same machine. The maximum value only applies to instances of the same software version.

Hardware requirements

ArcGIS Web Adaptor (IIS) requires a minimum of 8 GB of memory, with more potentially required depending on the number of ArcGIS Web Adaptor instances installed and the number and size of the requests received.

For hardware considerations when upgrading to ArcGIS Web Adaptor 11.4, see Upgrade ArcGIS Web Adaptor.

Supported Windows operating systems

The following Windows operating systems (OS) are supported for ArcGIS Web Adaptor:

Supported operating system	Latest update or service pack tested
Windows Server 2022 Standard and Datacenter	September 2024 update
Windows Server 2019 Standard and Datacenter	September 2024 update
Windows Server 2016 Standard and Datacenter	September 2024 update

Supported operating system	Latest update or service pack tested
Windows 11 Pro and Enterprise	September 2024 update

Note:

- Prior and future updates or service packs to these OS versions are supported unless otherwise stated. The OS version and updates must also be supported by the OS provider.
- The Desktop Experience option is required on all versions of Windows Server.
- ArcGIS is only supported on 64-bit CPUs with x86-64 architecture.
- Windows 11 is supported for basic testing and application development use only.

Supported web browsers

The Web Adaptor Configuration wizard supports the following web browsers:

- Google Chrome version 122 and later
- Microsoft Edge version 122 and later
- Mozilla Firefox version 125 and later
- Mozilla Firefox version 115 (ESR)
- Safari version 16 and later

Supported virtualization environments and cloud platforms

Virtualization and cloud environment support is the same for all components of a base ArcGIS Enterprise deployment. See ArcGIS Enterprise on cloud platforms and Supported virtualization environments in ArcGIS Enterprise system requirements for details.

Install

Install ArcGIS Web Adaptor

ArcGIS Web Adaptor is provided as a setup program and is run through a utility named `Setup.exe`. You can install ArcGIS Web Adaptor on its own using the steps provided here, or you can install silently using Windows Installer command line parameters.

Installation requirements

- The version of ArcGIS Web Adaptor must match the version of your server site or portal.
- ArcGIS Web Adaptor can be installed side by side with other versions. You are not required to uninstall ArcGIS Web Adaptor unless you are upgrading to a newer version.
- Each ArcGIS Web Adaptor must have its own unique name; you cannot have two Web Adaptors with the same name on a single web server. If a naming conflict is detected during the installation, a warning message appears. You must uninstall the earlier version with the same name to resolve the conflict. Alternatively, you can change the name of one of the Web Adaptors to proceed with the installation.

Before installing ArcGIS Web Adaptor

Before you install ArcGIS Web Adaptor, do the following:

1. Verify that your system meets all system requirements. You can only configure one Web Adaptor with a server site or portal.
2. Automatically or manually enable IIS and the required components.

   Caution:

   To successfully install and configure ArcGIS Web Adaptor, you must enable IIS and the required components before installing the prerequisites specified in the next step.

3. Ensure that the following prerequisites are installed on the machine where ArcGIS Web Adaptor will be installed:
   - Microsoft Web Deploy 4.0
   - ASP.NET Core Runtime - Windows Hosting Bundle 8.x

   Note:

   You must install the ASP.NET Core Runtime - Windows Hosting Bundle, which includes the .NET Runtime and IIS support.

   Caution:

   If you installed the ASP.NET Core Runtime - Windows Hosting Bundle before enabling IIS and the required components, you must repair the bundle installation using the bundle installer.

4. Sign in to the machine on which you're installing ArcGIS Web Adaptor.

   Note:

   You must sign in as a user with administrative privileges.

5. Verify that you have a website running on port 80 and HTTPS is enabled on port 443. This is to accommodate the variety of encrypted and unencrypted calls made to ArcGIS Enterprise. For instructions on how to create a website, consult the IIS product documentation. For more information about setting up and using HTTPS, see Enable HTTPS on your web server.

   Note:
   The use of the default HTTPS port 443 is appropriate for the vast majority of users. In some rare cases, an ArcGIS Web Adaptor instance cannot use port 443 on its web server for organization-specific reasons. If this applies to your organization, see Use nondefault ports for the portal's ArcGIS Web Adaptor, which details additional steps to configure a workaround.

6. Close all applications
7. Browse to the downloaded folder containing the ArcGIS Web Adaptor setup. You can also insert the ArcGIS Server or the Portal for ArcGIS media into the appropriate drive to automatically start the setup.

You are now ready to proceed with the ArcGIS Web Adaptor installation.

Caution:
Attempting to configure ArcGIS Web Adaptor so the URL includes additional levels is not supported and may cause problems with client applications.

How to install ArcGIS Web Adaptor

To install ArcGIS Web Adaptor, complete the following steps:

1. The ArcGIS Web Adaptor setup program should start automatically after the download is complete. If the setup does not start automatically, browse to the location of the downloaded setup files, and double-click **Setup.exe**.
2. Review the terms and conditions of the master agreement. You must agree to the terms to proceed.
3. Choose a website running on port 80 for ArcGIS Web Adaptor. Available websites are listed as **<website name (port)>**. If you don't see the **Select website** dialog box, this means you only have one website. If only one website is found on your machine, ArcGIS Web Adaptor is automatically placed on that website without displaying the **Select website** dialog box.
4. Provide a name for the Web Adaptor. The default value is **arcgis**. This instance name cannot contain spaces.

   Note:
   A message appears if a virtual directory with the same name as the Web Adaptor already exists on the selected website. Click **OK** to close the message, and provide a different name for the Web Adaptor.

5. To complete the installation, follow the directions on the screen.

Note:
Each Web Adaptor installation creates an application pool with the default naming convention of **ArcGISWebAdaptorAppPool<web adaptor name>**.

The Web Adaptor configuration page appears after the installation is complete. You are now ready to configure ArcGIS Web Adaptor for use with a server site or portal. For more information, see the following topics:

- Configure ArcGIS Web Adaptor with a server site
- Configure ArcGIS Web Adaptor with portal

Install ArcGIS Web Adaptor silently

ArcGIS Web Adaptor can be installed by running the setup using Windows Installer command line parameters as described below. Alternatively, you can install from the user interface using `Setup.exe`.

Installation requirements

- The version of ArcGIS Web Adaptor must match the version of your server site or portal.
- ArcGIS Web Adaptor can be installed side by side with other versions. You are not required to uninstall ArcGIS Web Adaptor unless you are upgrading to a newer version.
- Each ArcGIS Web Adaptor must have its own unique name; you cannot have two Web Adaptors with the same name on a single web server. If a naming conflict is detected during the installation, a warning message appears. You must uninstall the earlier version with the same name to resolve the conflict. Alternatively, you can change the name of one of the Web Adaptors to proceed with the installation.
- Manually enable IIS and the required components.

  Caution:

  To successfully install and configure ArcGIS Web Adaptor, you must enable IIS and the required components before installing the prerequisites specified in the next step.

- Install the following prerequisites on the machine where ArcGIS Web Adaptor will be installed:
  - Microsoft Web Deploy 4.0
  - ASP.NET Core Runtime - Windows Hosting Bundle 8.x

  Note:

  You must install the ASP.NET Core Runtime - Windows Hosting Bundle, which includes the .NET Runtime and IIS support.

  Caution:

  If you installed the ASP.NET Core Runtime - Windows Hosting Bundle before enabling IIS and the required components, you must repair the bundle installation using the bundle installer.

Command line parameters for specifying the website and name for ArcGIS Web Adaptor

The following command lines are used for configuring IIS. If these command line parameters are not invoked during a silent installation, the ArcGIS Web Adaptor web application is created under the default website with the default name of `arcgis`.

- ACCEPTEULA=yes
  This property is required to accept the End User License Agreement during a silent installation. Specify yes to agree to the EULA and install the software. Specifying no or omitting this property will result in a failed installation. The download contains a PDF version of the End User License Agreement (EULA). The `EULA.pdf` file is located in the `\Documentation` folder.
- WEBSITE_ID=<numeric value of website>

The WEBSITE_ID parameter is used to specify the website where the ArcGIS Web Adaptor web application will be created. The value for WEBSITE_ID is a number specific to each website on your server and assigned by IIS. The IDs for the websites on your server can be found in IIS Manager. The default website has a website ID of 1. By default, the WEBSITE_ID parameter is set to the default website (even if multiple websites exist). The parameter WEBSITE_ID is case sensitive.

- PORT=<port number>
  Additionally, if you have a website with multiple ports, use the PORT parameter to install to the specified port of the WEBSITE_ID.

  For example, the path is `<path to ArcGIS Web Adaptor (IIS) setup download>\setup.exe /qb VDIRNAME=arcgis_external WEBSITE_ID=4059640 PORT=82`.

- VDIRNAME=<name of ArcGIS Web Adaptor>
  This command line parameter is optional. By default, the VDIRNAME property is set to `arcgis`. If you do not invoke the VDIRNAME parameter in your command line, the Web Adaptor is created as `arcgis`. The VDIRNAME parameter is case sensitive. The Web Adaptor name cannot contain spaces.

  For example, the path is `<path to ArcGIS Web Adaptor (IIS) setup download>\setup.exe /qb ACCEPTEULA=yes VDIRNAME=arcgis_external WEBSITE_ID=4059640`.

- CONFIGUREIIS=TRUE
  This optional parameter will allow the setup program to silently configure and install all missing Microsoft IIS components required by ArcGIS Web Adaptor.

Install multiple ArcGIS Web Adaptor instances

You can install multiple ArcGIS Web Adaptor instances on the same machine at the same time. The installation can also be repeated on separate machines. The workflows below will guide you through the process.

To install multiple Web Adaptors on the same website (port), they must have different names. For example, two Web Adaptors named `arcgis` cannot exist on the same website. If you want multiple Web Adaptors with the same name, you must install them on separate websites (ports).

1. Browse to the downloaded folder containing the ArcGIS Web Adaptor setup, or insert the ArcGIS Server media into the appropriate drive to automatically launch the media front end.
2. Follow the same instructions that you used to install the first Web Adaptor. For details, see Install ArcGIS Web Adaptor.

Note:
The setup detects and prevents any conflicts with the Web Adaptor name. If you see a message indicating that the virtual directory already exists, specify a different name for the Web Adaptor or select a different website.

Note:
To apply a Web Adaptor service pack, the base instance cannot be removed.

Install multiple Web Adaptors silently

You can install multiple Web Adaptors by running the setup using command line parameters. See Install ArcGIS Web Adaptor for full instructions on how to use the command line parameters. No additional command line parameters are necessary to install multiple Web Adaptors.

Configure

Plan your configuration

Steps to implement ArcGIS Web Adaptor

The following is an overview of the steps to implement ArcGIS Web Adaptor with a server site or portal:

1. Plan your configuration based on the type of environment you are setting up.
   - Configure with a server site
   - Configure with a portal
   - Configure with ArcGIS Monitor
2. Verify that your system meets the system requirements.
3. Enable HTTPS on your web server.
4. Install ArcGIS Web Adaptor using the setup or install silently.
5. Configure ArcGIS Web Adaptor for use with one of the following:
   - A server site
   - A portal

Use ArcGIS Web Adaptor with portal

ArcGIS Web Adaptor (IIS) is a component of Portal for ArcGIS that allows you to integrate your portal with your existing web server and your organization's security mechanisms. ArcGIS Web Adaptor is required if you want to use Integrated Windows Authentication with your portal.

The Web Adaptor is an application that runs in your existing website and forwards requests to the machine hosting Portal for ArcGIS. The IIS setup is compatible with IIS in Windows 8.1, 10, 11, Server 2016, 2019, and 2022. This corresponds to IIS versions 8.5 and 10.

Benefits of the Web Adaptor

You can do the following using the Web Adaptor:

- Integrate Portal for ArcGIS with your organization's existing web server. By including a web server in your site, you can host web applications that use your GIS services.
- Use your organization's identity store and security policies at the web-tier level. For example, if you're using IIS, you can use Integrated Windows Authentication to restrict who enters the portal. You can also use public key infrastructure (PKI)-based client certificate authentication or any other identity store for which the web server has built-in or extensible support. This allows you to provide a single sign-on or other custom authentication experience when logging in to use services, web applications, and Portal for ArcGIS.
- Make Portal for ArcGIS available through a site name other than the default: arcgis.
- Make Portal for ArcGIS available through port 80 or 443.

Note:
You can only use the Web Adaptor with port 80 or 443. Using other ports is not supported.

Web Adaptor deployment scenarios

The Web Adaptor version must always match the version of the ArcGIS Enterprise component with which it is configured. If you've configured multiple Web Adaptors on a single web server, you can use different version numbers for all the Web Adaptors.

The Web Adaptor is platform independent of ArcGIS Enterprise; therefore, the Web Adaptor you deploy does not have to match the operating system platform of your portal. For example, if your portal is running on Linux, you can deploy ArcGIS Web Adaptor (IIS) to work with Portal for ArcGIS.

Accessing your portal with the Web Adaptor installed

After installing and configuring the Web Adaptor, the URL that you use to access your portal will be in the format `https://webadaptorhost.domain.com/webadaptorname/home`. For example, if the machine hosting your Web Adaptor is named wa with the domain `myorg.net` and your Web Adaptor is named arcgis, you'll access the portal using the URL `https://wa.myorg.net/arcgis/home`.

If you configured your portal to use HTTPS for all communication, update the installed portal website and help shortcut URLs to use https instead of http; otherwise, you will see failures in your browser when attempting to access the original shortcut URLs.

Web Adaptor setup experience

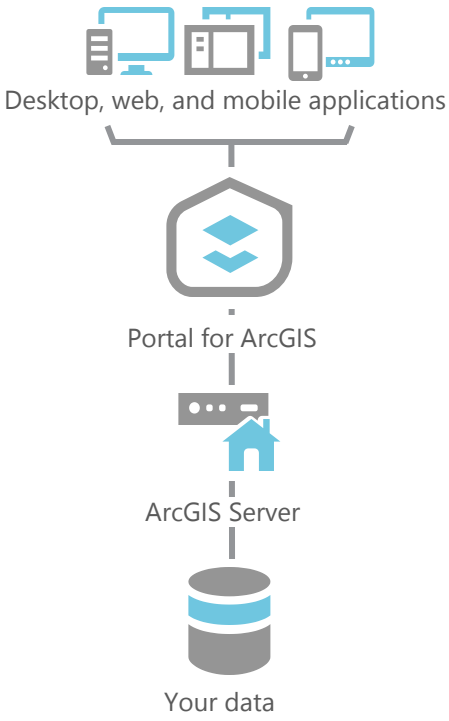
The Web Adaptor has its own setup and installation guide that is separate from the Portal for ArcGIS installation. You must install the Web Adaptor on a machine running a web server. This can be a machine running Portal for ArcGIS or a separate machine.

To learn more about the setup experience, see Steps to implement ArcGIS Web Adaptor.

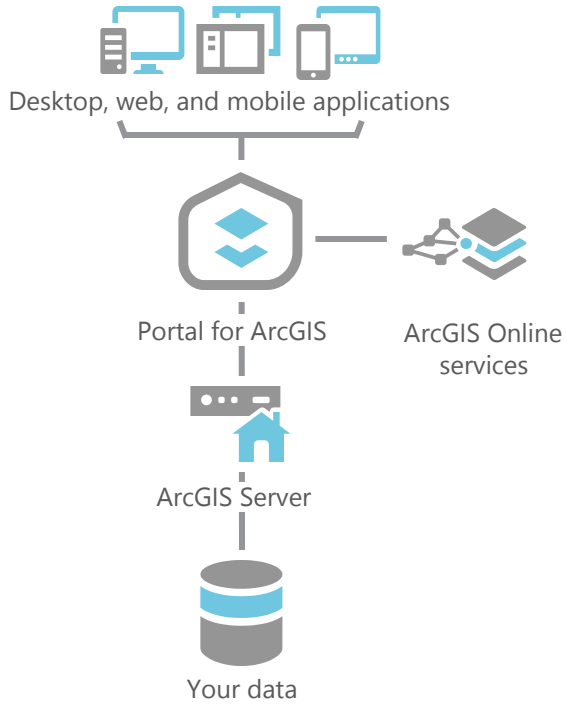
Plan your Portal for ArcGIS configuration

The Portal for ArcGIS component of ArcGIS Enterprise has a central role in organizing and sharing information in your ArcGIS system. The portal provides a user-friendly, searchable repository for your maps and apps. It also helps you create and share maps and apps.

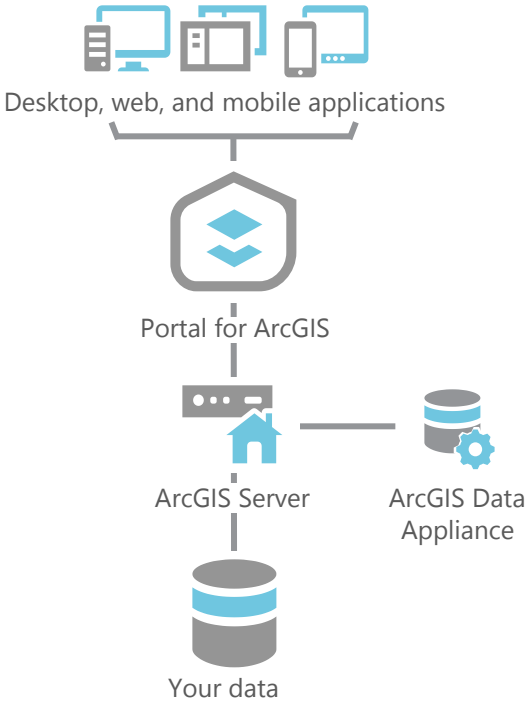
Some of the information in these maps and apps originates from a database in your organization. The GIS content in this database is shared with other devices using web services hosted by ArcGIS Server. The portal helps map and app creators find and use these web services and provides a window into your GIS content without requiring GIS software training.



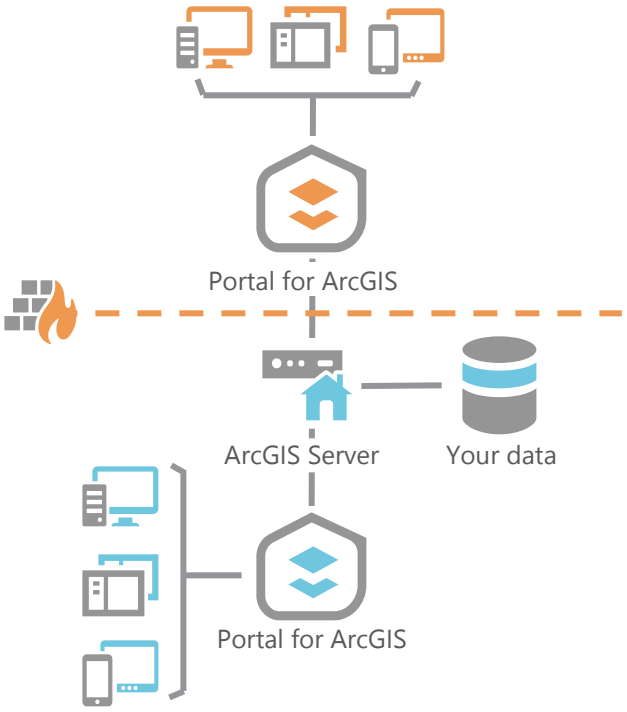
Some organizations publish a full suite of web services that can be used to create a fully in-house app using proprietary data. However, in many cases, you may want to supplement your own services with detailed basemaps, place finders, address finders, and other GIS web services from ArcGIS Online. In this scenario, you combine your own ArcGIS Server services with services that are hosted and continuously updated in the Esri cloud.



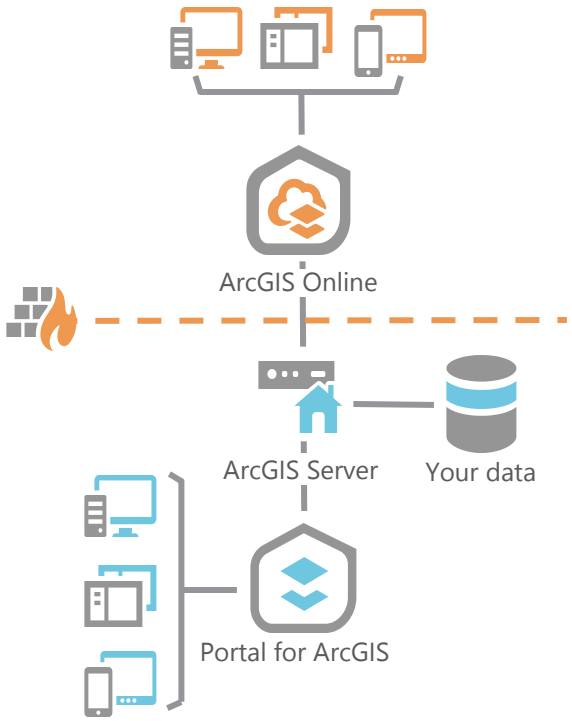
If your organization doesn't have internet access, you can use ArcGIS Data Appliance to access preloaded content that you typically find on ArcGIS Online such as basemaps, address finders, and other web services. You can also download boundary layers from My Esri and configure them in a disconnected environment.



To support a combination of internal and external users, you can deploy two portals: one behind your firewall and one that is exposed to the web. This works well when you want full control over the data location and updates, or if your data is not allowed to be hosted off-site.



Another option for supporting a combination of internal and external users is to use an organizational subscription to ArcGIS Online for your external-facing apps and services.



Use ArcGIS Web Adaptor with a server site

ArcGIS Web Adaptor (IIS) allows ArcGIS Server to integrate with your existing web server. See the system requirements page for more information about supported operating systems for ArcGIS Web Adaptor (IIS).

ArcGIS Web Adaptor is an application that runs in your existing website and forwards requests to your server machines. It polls your site at a regular interval to learn which machines have been added or removed. It then forwards traffic to only the currently participating machines. When you prepare to expose your server site to an external audience, you should install the Web Adaptor or implement comparable request forwarding and security technology.

Benefits of the Web Adaptor

You can do the following using the Web Adaptor:

- Integrate ArcGIS Server with your organization's existing web server. By including a web server in your site, you can host web applications that use your GIS services.
- Provide a single endpoint that distributes incoming requests to the servers in your site.
- Make your ArcGIS Server site available through your organization's standard website and port. Use the Web Adaptor if you don't want users to see the default port, 6080, or the default site name, arcgis.
- Block the ArcGIS Server Administrator Directory and ArcGIS Server Manager from the view of external users.
- Prevent ArcGIS Pro users from establishing administrative or publisher connections to ArcGIS Server.
- Use your organization's identity store and security policies at the web-tier level. For example, if you're using IIS, you can use Integrated Windows Authentication to restrict who enters the portal. You can also use public key infrastructure (PKI)-based client certificate authentication if the web server has built-in or extensible support. This allows you to provide a single sign-on or other custom authentication experience when logging in to use services, web applications, and ArcGIS Server.

Web Adaptor deployment scenarios

The Web Adaptor can be used in various server site configurations. For example, in a site with a single server machine, you can install the Web Adaptor on the same machine as the server machine, or offload it to a dedicated web server. In a multiple-machine deployment, you can have one entry point into your site by installing the Web Adaptor on a single web server, or you can establish redundancy at the web server tier by installing the Web Adaptor on multiple web servers.

The Web Adaptor version must always match the version of its registered server site. If you've configured multiple Web Adaptors on a single web server, you can use different version numbers for all the Web Adaptors.

It's recommended that you use a DNS alias rather than the host name of the machine running ArcGIS Web Adaptor when you register it with ArcGIS Server. If you need to switch the ArcGIS Web Adaptor instance to a new machine in the future, you can remap the DNS alias to that machine. By doing so, you can avoid breaking traffic and interrupting work.

The Web Adaptor is platform independent of ArcGIS Server; therefore, the Web Adaptor you deploy does not have to match the operating system platform of your ArcGIS Server site. For example, if you have a site composed of Linux machines, you can deploy the ArcGIS Web Adaptor (IIS) to work with ArcGIS Server.

For a detailed description of the different ways you can integrate the Web Adaptor into your existing site architecture, see Deployment scenarios.

Accessing your services with the Web Adaptor installed

After installing and configuring the Web Adaptor, the URLs that you use to access your services will change. Examples of URLs that will change after installing a Web Adaptor to use port 443 are shown below.

Services Directory (REST web services)

- Without the Web Adaptor: `https://gisserver.domain.com:6443/arcgis/rest/services`.
- With the Web Adaptor: `https://webadaptorhost.domain.com/webadaptorname/rest/services`. For example, if the machine hosting your Web Adaptor is named wa with the domain `myorg.net` and your Web Adaptor is named arcgis, you'll access the Services Directory using the URL `https://wa.myorg.net/arcgis/rest/services`.

SOAP web services

- Without the Web Adaptor: `https://gisserver.domain.com:6443/arcgis/services`.
- With the Web Adaptor: `https://webadaptorhost.domain.com/webadaptorname/services`. For example, if the machine hosting your Web Adaptor is named wa with the domain `myorg.net` and your Web Adaptor is named arcgis, you'll access SOAP web services using the URL `https://wa.myorg.net/arcgis/services`.

Web Adaptor setup experience

The Web Adaptor has its own setup and installation guide that is separate from the ArcGIS Server installation. You must install the Web Adaptor on a machine running a web server. This can be a machine running an ArcGIS Server site or a separate machine.

To learn more about the setup experience, see Steps to implement ArcGIS Web Adaptor.

Server sites

Inside an ArcGIS Server site

ArcGIS Server, the work center of ArcGIS Enterprise, brings your organization's geographic information, analysis, and products to the web using infrastructure you manage.

Desktop products such as map documents, geoprocessing tools, and address locators are published to ArcGIS Server to become GIS services, available to your organization within its firewall and, optionally, to the greater internet. These services are consumable in web clients, from map viewers to mobile apps, and make it easy to share your resources across clients - even those without specialized GIS software.

This topic explains the structure and functions of ArcGIS Server from an administrator's perspective.

Federated and standalone sites

You can deploy ArcGIS Server as a standalone system to simply provide your users with GIS services, or integrate it with the ArcGIS Enterprise platform as a comprehensive Web GIS deployment in your infrastructure.

This integration is done by **federating** one or more ArcGIS Server sites with an ArcGIS Enterprise portal. In such a deployment, your users can build powerful, appealing products atop ArcGIS Server services and disseminate them easily using the ArcGIS Enterprise portal and native apps.

For example, your GIS professional might create a multilayered map in ArcGIS Pro and share it as a web map—powered by an ArcGIS Server map service—to your ArcGIS Enterprise portal; from there, they might create a web app from a few of the layers and embed it in your website as a public resource. In another case, your GIS department might equip its mobile workers with an Esri mobile app and have them add and update features on a common web map, powered by an ArcGIS Server feature service.

Security and access

When deployed as a standalone system, ArcGIS Server controls its sharing and security models. Administrators can modify settings such as access control, publishing privileges, and web traffic protocols within ArcGIS Server Manager, the browser-based application installed with ArcGIS Server, as well as programmatically through the ArcGIS Server Administrator Directory. Either the built-in ArcGIS Server identity store or your organization's external identity provider can be used to authorize and authenticate users to the standalone site.

When ArcGIS Server is federated with an ArcGIS Enterprise portal, it adopts the sharing and security models of the portal, though some security settings are still configurable from the ArcGIS Server tier.

See Integrate your server with ArcGIS Enterprise to learn more about federation and how federated ArcGIS Server sites operate.

Components of ArcGIS Server

An ArcGIS Server site consists of several components that can optionally be distributed across multiple machines to increase computing power. Each component in the site plays a specific role in the process of managing the resources that are allocated to a set of services.

The components of an ArcGIS Server site can be summarized as follows:

- Web server—Hosts web applications and provides optional security and load balancing benefits to ArcGIS Server.
- ArcGIS Web Adaptor—Integrates ArcGIS Server with your enterprise web server, forwarding incoming requests to your various ArcGIS Server machines.

- ArcGIS Server—Responds to requests issued to the GIS web services. ArcGIS Server can draw maps, run tools, serve imagery, synchronize databases, project geometry, search for data, and perform many other operations offered by ArcGIS.

Web server

The web server hosts web applications and provides optional security and load balancing benefits to the ArcGIS Server site. ArcGIS Server is compatible with many popular web servers, including Internet Information Services (IIS), WebSphere, and WebLogic.

ArcGIS Web Adaptor

ArcGIS Web Adaptor is a web application that forwards requests from your web server to your ArcGIS Server. ArcGIS Web Adaptor keeps track of which machines have been added to (and removed from) your site and forwards transactions to them appropriately. ArcGIS Web Adaptor allows you to set your own name for your site, instead of using the default site name `arcgis`. ArcGIS Web Adaptor also allows you to leverage the native capabilities of your web server for security and can block outside connections to ArcGIS Server Manager and the ArcGIS Server Administrator Directory.

When a web service request is received, ArcGIS Web Adaptor forwards the request to one of the ArcGIS Server machines. If ArcGIS Web Adaptor determines an ArcGIS Server machine is unavailable, it stops forwarding requests to that server.

Other web gateway options

ArcGIS Web Adaptor is not the only way to configure a web gateway, or entry point, to your site. Other web gateway technologies include physical HTTP load balancer and network router devices, or third-party software designed for load balancing purposes. For example, in the Amazon Web Services (AWS) cloud environment, the Amazon Elastic Load Balancer (ELB) can act as a web gateway. If you already have technology in your organization that serves as a web gateway, it can be adapted to work with ArcGIS Server under most circumstances.

It is a security best practice that your users always use a web gateway, whether it be ArcGIS Web Adaptor or a third-party load balancer, to access your ArcGIS Server site. Users should never connect to ArcGIS Server directly using ports 6443 or 6080.

ArcGIS Server

Incoming web service requests for maps, address coordinates, geoprocessing jobs, and so on, are each assigned to an available ArcGIS Server machine in the site. That ArcGIS Server then draws the map, finds the address coordinate, runs the geoprocessing tool, and so on, and returns the result to the client. Essentially, ArcGIS Server machines are the work centers of your site.

You may need to configure your ArcGIS Server site to use multiple ArcGIS Server machines to protect against downtime if one of your machines becomes unavailable. When a machine goes offline (whether planned or unplanned), the Web Adaptor can continue to distribute incoming requests to the remaining ArcGIS Server machines in the site.

The above components of an ArcGIS Server site can reside on the same physical machine for development and testing purposes, or for supporting small deployments. See Deployment scenarios to learn about recommended architectures for small and large sites.

Configuration store

An ArcGIS Server site has a folder designated as the configuration store that contains all the properties of the site and its services. You specify the location for the configuration store when you create the site. In a multiple-machine site, the ArcGIS Server machines access the configuration store through a shared network directory. In a site with multiple ArcGIS Server machines, it's recommended that you keep the configuration store on its own fault-tolerant file server (separate from the ArcGIS Server machines).

Server directories

A server directory represents a physical directory on the network that is specially designated for an ArcGIS Server site to store and write certain kinds of information. There are server directories for storing caches, output, jobs, system files, uploads, input data, KML, and indexes. A set of server directories is created at a location you specify when you create the site. In a multiple-machine site, this must be a shared network directory.

For detailed descriptions of each server directory, see About server directories.

Server roles

ArcGIS Server can be licensed with a number of server roles. These unlock unique server architecture and features that enable specialized analysis and processing tasks. For example, ArcGIS GeoAnalytics Server distributes task processing among multiple server machines to hasten analysis of massive data sets. Server roles require no extra software installation - they are designated in your license files when you authorize ArcGIS Server.

Processes started by ArcGIS Server

You can expect to see the following operating system processes on any ArcGIS Server machine that is started and participating in a site:

- One ArcGISServer.exe process
- One ArcSOC.exe process for each running service instance. An exception is geoprocessing services, which have two ArcSOC.exe processes per running instance. Note that some of these processes are for internal system services, not services your users have published.
- One rmid.exe process
- One javaw.exe process. This provides basic application server functionality and the ability to host web services.
- One conhost.exe process and one cmd.exe process. These are supplementary processes started by Windows to provide console services to ArcGIS Server processes.

You can tell that a javaw.exe process is associated with ArcGIS Server by looking at the Command Line column in Windows Task Manager. If the path includes the ArcGIS installation directory, you know it's a process associated with ArcGIS Server. You can derive further information about each process by examining its full command.

The Windows service **ArcGIS Server** represents ArcGIS Server itself. Stopping this service effectively stops ArcGIS Server on the machine and shuts down any running service instances.

The ArcGIS Server site

An ArcGIS Server site is an assemblage of individual machines configured to work together on equal terms. When first created, a site consists of one machine; using the Join Site or Register Machine operations, additional machines can be added to the site.

Each of a site's machines run all services published to the site, and if assigned a request to any service by the site's Web Adaptor or load balancer, each will be able to handle and process that request. An individual request will be handled entirely by the machine it is assigned to; if that machine is unable to complete the request, the initiative fails rather than passing the unfinished request to another machine in the site.

The exception to the "one request, one machine" pattern is with the ArcGIS GeoAnalytics Server and ArcGIS Image Server roles, which distribute the processing of service requests across multiple machines to tackle large analysis tasks.

Service instances

To process a service request, the assigned ArcGIS Server machine uses an instance of the Esri server process ArcSOC.exe. This process runs the request on the machine. For each machine in your ArcGIS Server site, you can view the instances of ArcSOC.exe currently running by viewing them in Task Manager on a Windows machine or system monitor on a Linux machine.

Note: Geoprocessing services use two ArcSOC.exe processes per running instance. All other service types use one.

ArcSOC service instances are organized by pools, the size of which can be adjusted to accommodate traffic. A service can have its own dedicated pool of instances that will only handle its requests. Beginning at 10.7, the ArcGIS Server site now has a shared pool of instances to which multiple services can be added. The size of an instance pool is governed by two settings—a minimum and a maximum number of instances—that administrators can set in ArcGIS Server Manager. The actual number of instances running at a given time will be within this set range, but it will vary depending on current traffic.

The shared instance pool offers a solution to conserve computer memory usage by ArcGIS Server, by reducing the number of unused ArcSOC instances running on the site's machines. It is intended to be used by services that do not receive constant requests or high numbers of simultaneous requests.

Prior to the introduction of the shared instance pool, the method to reduce unnecessary running instances was to set the minimum number of instances in a dedicated pool to zero. When this is done, a service that has not recently received a request will not have any ArcSOC instances running on the server site's machines, thus conserving memory usage. However, this presents a "cold start" problem—a delay in the response time for the next request to the service while it starts up a new ArcSOC instance. Using the shared instance pool eliminates the "cold start" problem, as there are always ArcSOC instances available for its services to use.

To learn more, see Shared and dedicated instances.

Deployment scenarios

ArcGIS Server is designed to be scalable and to accommodate both small and large deployments. When you first begin building your site, you may start small and install all the components on a single machine. As you deploy your production site, or if your site needs to manage more users, you can add more ArcGIS Server machines to the site. You can also integrate your site into your existing IT infrastructure by using your own enterprise web server (as with ArcGIS Web Adaptor), database, or organization-specific identity providers. ArcGIS Server can also be configured to support critical business operations through the use of high-availability configurations. You can also create multiple ArcGIS Server sites in your ArcGIS Enterprise deployment, with each site serving a different purpose or simply hosting more services.

This section of the ArcGIS Server help describes the different configurations system architects can use to accomplish their organizations' unique needs and goals. These topics provide details on the ArcGIS Server site components of ArcGIS Enterprise, whether the site is federated with a portal or stands alone. The following terms are used when explaining each deployment scenario:

- Site—An ArcGIS Server site consists of one or more ArcGIS Server machines and ArcGIS Web Adaptor. These components can optionally be distributed across multiple machines to increase computing power and redundancy. Each machine in a server site participates on equal terms. For a more detailed description, see Inside an ArcGIS Server site.
- ArcGIS Server—The main component of the site that processes requests issued to its GIS web services. ArcGIS Server can generate maps, run tools, serve imagery, and perform many other operations.
- ArcGIS Web Adaptor—A software component that allows you to configure a web entry point into your site. It integrates with your web server and distributes incoming requests among ArcGIS Server machines. It's recommended that you use ArcGIS Web Adaptor with your server site, unless you are deploying third-party load balancing components and can ensure they will handle each of the Web Adaptor's responsibilities. For more information, see About the ArcGIS Web Adaptor.
- Reverse proxy server—An optional third-party component in your organization that is placed between a client and a server in a network infrastructure. Incoming requests are handled by the proxy, which interacts on behalf of the client with the desired server or service residing on the server. Most organizations set up a proxy server so that the site is not exposed directly to clients. For more information, see Use a reverse proxy server with ArcGIS Server.
- Network load balancer (NLB)—An optional third-party component that uses a distribution algorithm to load balance network traffic across a number of hosts, helping to enhance the scalability and availability of web services. It also typically provides high availability by detecting machine failures and automatically redistributing traffic to available machines.
- Server directories—A set of ArcGIS Server directories containing certain types of files that support your services. These files include map caches, search indexes, and geoprocessing job results. For more information, see server directories.
- Configuration store—A file directory that contains configuration information about the site, such as the list of ArcGIS Server machines participating in the site. The configuration store must be available for your site to function. You are able to specify the configuration store location.
- Data—Data supporting your web services, such as feature classes, tools, imagery, and locators. For more information, see Make your data accessible to ArcGIS Server.

The scenarios outlined in the following topics are presented as deployment guidelines for you to consider as you build your ArcGIS Server site. Although you can configure your site exactly as presented in one of the scenarios, these configurations are flexible and can be adjusted to fit specialized needs and hardware resources.

Single-machine site configurations

- Single machine
- Single machine with reverse proxy server
- Single machine high availability (active-passive)
- Single machine high availability (active-active)

Note:
The single-machine high-availability configurations cannot be federated with the portal. To federate a highly available site with your portal, configure a multiple-machine deployment.

Multiple-machine site configurations

- Multiple machine with ArcGIS Web Adaptor
- Multiple machine with third party load balancer

Single machine site configurations

Single-machine deployment

In its most basic configuration, an ArcGIS Server site can run on a single machine. The deployment scenario described below is straightforward to set up, maintain, and upgrade. It can support a sandbox environment for development and testing, but it is also a valid (and in some cases ideal) configuration for some production environments. The site can either be federated with an ArcGIS Enterprise portal or stand alone.

ArcGIS Server

A single ArcGIS Server machine is configured with the ArcGIS Server account set as a local operating system account on the machine or a domain account. To learn more about the ArcGIS Server account, see Accounts used by ArcGIS Server.

Server directories and configuration store

Since this deployment uses only one machine, the server directories and configuration store location should reside locally on the machine, as opposed to a network share,

Keeping your configuration store and server directories on the local file system typically results in better performance than accessing them over a network share. It also reduces dependencies between the machine running ArcGIS Server and the remote storage device. If you plan to host cached map and image services, using local directories, direct attached, or storage area network volumes (dedicated to the server) are recommended, as this typically yields the highest performance. Cache tile retrieval over a shared network location is a particularly expensive operation.

You can also use cloud storage for some or all of your server directories. However, if your ArcGIS Server site is deployed on physical machines (on-premises), it is recommended that you keep your server directories on-premises as well. The one exception is the cache directory, which can be deployed on cloud infrastructure even if the rest of your site is deployed on-premises. If your ArcGIS Server site is deployed on cloud infrastructure, it's recommended that you use cloud infrastructure for your server directories as well.

There are also particular considerations when using cloud data stores for cache directories.

See Data sources for ArcGIS Server for more information about registering and operating data sources for your site.

ArcGIS Web Adaptor

The server site is configured with ArcGIS Web Adaptor in this example, though it can also be configured with a third-party reverse proxy server. Clients query the services on the site and make administrative and publishing requests using the URL format `https://gisserver.domain.com/server`. The Web Adaptor handles each request and distributes it to one of the machines in the server site using port 6443. If you have not disabled it, direct administrative access to the server site is available through port 6443.

At 10.7 and later, HTTPS communication is enforced by default by ArcGIS Server sites. Though it's recommended that you maintain this setting, you can also enable HTTP communication as well.

If you choose to deploy ArcGIS Server without ArcGIS Web Adaptor or a reverse proxy server, be aware of the following:

Services not available over standard port

Typically, web applications expect HTTPS resources to be accessed over port 443, as opposed to 6443. Access over port 443 requires use of ArcGIS Web Adaptor or a third-party reverse proxy server. ArcGIS Server does not run on

standard ports because it would conflict with third-party web servers that you may already have running in your organization. In some organizations, especially intranet environments, having your applications access services directly over 6443 could be a viable solution.

ArcGIS Server administrative endpoints exposed

ArcGIS Server Manager and the ArcGIS Server Administrator Directory are exposed through the same port (6443) that everyone else uses to access services. This does not imply that anyone can administer your server, because a user must provide administrative credentials to perform administrative operations on the server. However, it is a best practice to block general access to the administrative endpoints, especially if your server is exposed to the internet. If exposing the administrative endpoints is a concern in your deployment environment, overcome this by specifying that only certain IP addresses can access the server. To learn more, see Update Security Configuration in the ArcGIS REST API.

Cannot use web-tier authentication

For example, the basic single-machine deployment without ArcGIS Web Adaptor is inadequate if you're required to enable a single sign-on (SSO) experience for your users.

Data

In this configuration, data in file format (file geodatabases, images, and shapefiles) must be stored locally for optimal performance. If using databases, place them on a dedicated server.

Summary

This is a basic configuration that is straightforward to configure and upgrade. While this configuration represents the typical choice for development and testing environments, it is also valid in some production environments (particularly intranet) with moderate security policies. For higher-security environments, a single-machine configuration with ArcGIS Web Adaptor or a reverse proxy server is recommended.

This configuration is ideal for production environments where cached map and image services must deliver the maximum throughput possible. In organizations with large ArcGIS Server deployments, a single-machine site is a good choice for hosting all cached services. Other services can be hosted in a parallel site with one or multiple GIS servers. The performance gains of serving cache tiles from a single-machine deployment may overcome the overhead of having to administer a dedicated GIS server for that purpose.

Availability

Since there is only one GIS server, there is a single point of failure. Software or hardware failures can make your services unavailable. Consider other site configurations to eliminate possible downtime.

Scalability

In this configuration, the configuration store and server directories reside locally on the GIS server, as opposed to a network share. It is not possible to add extra GIS servers to the site to increase computing power. Scalability is vertical only and can be increased by adding cores to the GIS server. This configuration can efficiently take advantage of modern hardware with many cores.

Advantages

- Straightforward to install, maintain, and upgrade.

- High performance because local paths are used to access resources; this is ideal for hosting cached map and image services.

Disadvantages

- May not fit your security requirements, since ArcGIS Server Manager and ArcGIS Server Administrator Directory are exposed through the same port (6080) that everyone else uses to access the services. Overcome this by specifying that only certain IP addresses can access the server in the Administrator Directory. This is controlled by the `allowedAdminAccessIPs` property in the server's Security Configuration. To learn how to configure this property to limit access to the server, see the example in Update Security Configuration. To completely isolate administrative access, route inbound traffic through a reverse proxy server or ArcGIS Web Adaptor.
- Nonstandard HTTP ports (6080 and 6443 if using HTTPS) are used to expose services to clients. To overcome this, route inbound traffic through a reverse proxy server or ArcGIS Web Adaptor.
- Web-tier authentication is not available without ArcGIS Web Adaptor. If you need web-tier authentication, include ArcGIS Web Adaptor.
- Not highly available; the GIS server is a single point of failure if it goes offline. Refer to the Single-machine high-availability (active-passive) deployment for details.

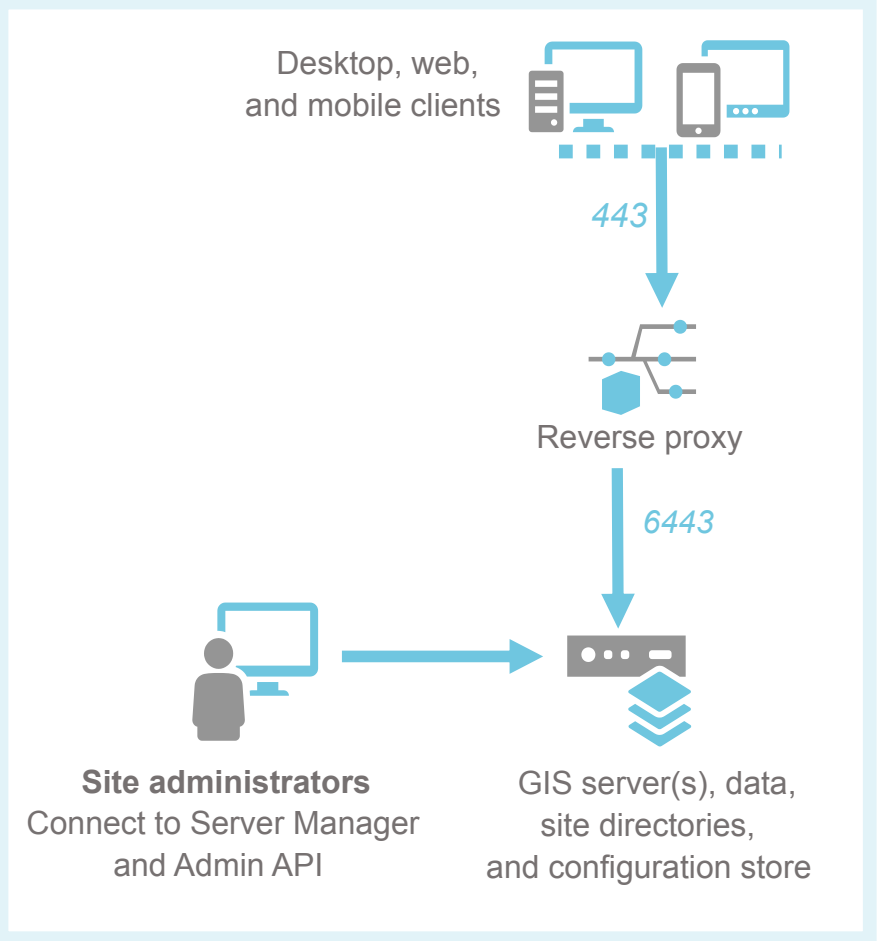
Single-machine deployment with reverse proxy server

A reverse proxy server acts as an intermediary for client requests seeking resources from your ArcGIS Server site, adding extra security features to your site deployment.

ArcGIS Web Adaptor is a software component that you can configure in most common web application servers. Alternatively, you can choose to leverage other third-party reverse proxy web servers.

ArcGIS Web Adaptor or a third-party reverse proxy server is typically configured on a separate web server machine, although it is also possible to co-locate them with your ArcGIS Server.

To client applications, there is no difference between accessing GIS services directly or through the proxy. However, as the ArcGIS Server administrator, you may want to use a reverse proxy server for one or more of the following reasons:



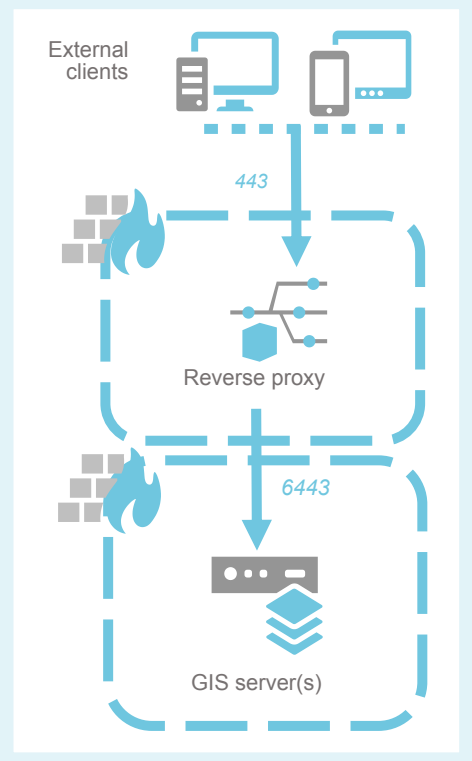
Single-machine site with a third-party reverse proxy installed on a dedicated web server

Access GIS services over standard ports

When not using a reverse proxy server, clients will connect directly to ArcGIS Server through `https://gisserver.domain.com:6443` if you have configured HTTPS. You cannot change the default ports used by ArcGIS Server. If you want client applications to use standard port 443 respectively, you'll need to configure a reverse proxy and direct clients to access services through it. For example, you could configure your reverse proxy at `http://proxy.domain.com/arcgis` or at `http://proxy.domain.com/myGIS`.

Isolate ArcGIS Server behind your organization's firewall

If you want to make your services and applications publicly available on the Internet, it is recommended to use a reverse proxy web server configuration to isolate ArcGIS Server behind your organization's firewall. In this configuration, incoming requests from the Internet pass through a firewall that blocks all ports except 443. Your reverse proxy web server receives the incoming request, passes it to ArcGIS Server through another firewall via port 6443, and sends the response back to the client. The following diagram shows how the reverse proxy server would reside in a perimeter network, helping you control access to your secure internal network.



To learn how to integrate a reverse proxy server with ArcGIS Server, see Using a reverse proxy server with ArcGIS Server.

Block administrative access to your site

A reverse proxy server can be used to block access to specific resources in your site. For example, you can configure your reverse proxy to block access to ArcGIS Server Manager and the ArcGIS Server Administrator Directory. This is a good practice, especially if you expose your ArcGIS Server services to the Internet.

If you are using a third-party reverse proxy server, refer to its specific documentation to block access to all requests that attempt to access ArcGIS Server Manager (`proxy.domain.com/arcgis/manager/`) or the ArcGIS Server Administrator Directory (`proxy.domain.com/arcgis/admin/`).

While administrative access will be blocked when accessing your site through the reverse proxy, administrative access will still be available when accessing your ArcGIS Server directly through its default port (6443). Firewalls should be used appropriately to control where these ports can be accessed.

Leverage features in your own web server

Web servers include many features that you may want to leverage as part of your ArcGIS Server deployment. By sharing your GIS services through your reverse proxy server, you can leverage the logging, caching, and security features of your web server.

- Web tier authentication: By default, ArcGIS Server uses token-based authentication (often referred to as ArcGIS token-based or GIS tier authentication). Alternatively, you can choose to configure ArcGIS Server with web tier authentication. This method enables ArcGIS Server to delegate authentication to your own web server. If you need web tier authentication, you must use ArcGIS Web Adaptor. Web tier authentication is not available through a third-party reverse proxy web server.
- Logging: ArcGIS Server logs include information that is specific to ArcGIS Server services, for example, which operation has been invoked, the execution time of ArcGIS Server calls, as well as warnings and errors triggered in your ArcGIS Server. You can complement this information with logs from your web server, which provide details that may be absent in ArcGIS Server logs, such as the IP address from which the requests were made, the user agent, the referrer, and so on.
- Other features: Most web servers provide you with options to tightly control requests and responses. For example, you can apply filtering rules to incoming requests, block access from specific IP addresses or domain names, and so on.

Summary

ArcGIS Web Adaptor or a third-party reverse proxy server is an excellent complement to single-machine deployments of ArcGIS Server. Both provide additional security features. It is strongly recommended that you use one of them if you plan to expose your GIS services to the Internet, and it may be necessary even for intranet deployments, depending on your security requirements.

Advantages

- Complements the single-machine deployment with an extra level of security.

Disadvantages

- The use of a reverse proxy server can potentially add an overhead to requests to your ArcGIS Server services. This is especially true when leveraging web tier authentication for very large and complex (nested groups or federated) organization-specific identity stores.
- Not highly available; the ArcGIS Server machine and reverse proxy server are single points of failure if either go offline. Refer to the Single-machine high-availability (active-passive) deployment for details.

Use single-machine high-availability (active-passive) deployment

High availability is a technique to ensure system uptime and to minimize or prevent data loss in the event of a machine failure. You can deploy ArcGIS Server, similar to other ArcGIS Enterprise components, in a highly available configuration with a third-party network load balancer.

Active-passive architecture works to clone a single-machine site and place two or more independent instances of it behind a load balancer. While all the sites behind the load balancer are running and ready to service requests, the load balancer only hands over requests to one of the sites, designated as the primary site. If the load balancer detects that the primary site is unavailable, incoming requests are then redirected to a standby site through the failover process.

The failover process is handled completely outside of ArcGIS Server and can be typically configured to be triggered when the ArcGIS Server machine is completely unavailable (network or hardware failure), or in some cases, when a specific service or operation is failing.

Note:
You can request license files from My Esri for your standby sites at no additional cost.

While several machines are used to host ArcGIS Server in this deployment pattern, this configuration cannot be technically described as a multiple-machine site, because the sites behind the load balancer are independent of each other. Each site is composed of a single ArcGIS Server machine and has its own local configuration store and server directories.

The active-passive failover configuration allows you to build a redundant ArcGIS Server tier without incurring additional licensing fees. As the standby servers are not receiving any requests, they can be licensed at no additional cost. However, you must manage each independent server site separately; the sites have their own local configuration store and server directories. This can potentially add significant administration and management overhead if the site's services or data change frequently. In addition, any active requests in the primary site are lost when switching over to the standby site during failover.

ArcGIS Server machine, server directories, and configuration store

Apply the same considerations here as described in the single-machine deployment. Each ArcGIS Server machine has its own local server directories and configuration store. This ensures maximum performance and keeps interdependencies to a minimum.

Data

If using file-based data sources in your GIS services, it is recommended that you store these locally on every ArcGIS Server machine instead of network shares to maximize the performance of your services. In some cases, such as when handling large amounts of imagery, sharing your files over the network may be the only practical choice. If using files in shared resources over the network, it is important that you choose a storage device configured for high availability.

If using databases, you can dedicate a database to each of your sites: one database for your primary site and a separate one for your standby site. To keep the databases in sync, you can leverage database replication, or if needed, geodatabase replication techniques. Alternatively, you can leverage other high-availability techniques from your database provider.

Learn more about data and ArcGIS Server

Reverse proxy server

In this configuration, a third-party load balancer is required. At a minimum, this component is used to handle the load across the sites and failover when necessary. Typically, the load balancer also fulfills the role of the reverse proxy server. In some scenarios, you already may have a reverse proxy server configured independently from the load balancer.

If your network load balancer supports a health check function, you can use the ArcGIS Server site's Health Check endpoint in the REST API to determine if the site is available to receive requests. This is useful to quickly determine if there's a software or hardware failure in the site.

The use of ArcGIS Web Adaptor is optional and typically only necessary for this scenario if you want to leverage web-tier authentication. You can choose to configure it on the same machine as ArcGIS Server or on a dedicated machine. In either case, if using ArcGIS Web Adaptor, you must configure a separate ArcGIS Web Adaptor for every site.

Considerations for active-passive configurations

Keep the following in mind when planning an ArcGIS Server site with a highly available active-passive configuration.

Synchronize services

Unlike a true multiple-machine site, this configuration requires that all of the sites behind the load balancer host exactly the same content and that they follow the same security model. You are responsible for ensuring that all the sites look exactly the same to the load balancer.

There are multiple techniques that can help you keep ArcGIS Server services in sync across the primary and standby sites:

- Scripting—ArcGIS Server includes a REST API to script administrative tasks, such as publishing services and changing their security settings. You can create your own scripts to apply changes to all the ArcGIS Server machines involved in your deployment consistently. Scripting is especially useful when you must make small adjustments, such as changing the security of a service or overwriting it.

  Note:
  Do not use a script to create the initial site. Manually create the first site on a virtual machine image, and script creation of additional sites from this base image. Creating all machines from the same virtual machine image ensures that all machines use the same encryption key.

- Virtualization—If you operate in a virtual environment, you can create and use virtual machine templates to launch new sites. Each template will have a copy of the data needed for GIS services (unless a database is used). The template will also have all services published and configured. If changes are necessary, such as adding or updating existing services, you can create a template to later launch new virtual machines that replace the existing pool of ArcGIS Server machines in use under the load balancer. You can also use virtual machine templates to quickly recover stale ArcGIS Server machines.

The recommended procedure to apply changes to your sites in this deployment pattern is as follows:

1. First make administrative changes against a site that is in standby mode. For example, add a new service and change the security of another in a site that is not actively handling requests.

This ensures that there is no impact to applications using your primary site.

2. Manually configure your load balancer to hand over all requests to the standby site on which the changes have been made.
3. Apply the same changes to the idle site.
4. Revert the load balancer so requests are directed back to the original primary site and leave the standby site in standby mode.

You can manually apply changes to your site in the procedure described above through ArcGIS Server Manager, scripts, or virtual images.

Asynchronous geoprocessing and long-running tasks

When the load balancer switches to the standby site, any active requests in the primary site are lost. For example, if a long-running request such as a geoprocessing task is running when the failover occurs, the task must be reinitiated in the standby site by the client application.

Use token-based security

If using token-based authentication, also referred to as server-tier authentication, it is important that all sites in this configuration use exactly the same shared token key. Otherwise, tokens generated in the primary site do not work when used in the standby site. To duplicate the shared token keys across multiple sites, you can edit token settings in Manager.

Federation

Since there are distinct configuration stores for each site, single-machine active-passive ArcGIS Server deployments cannot be federated with Portal for ArcGIS. To federate a highly available server site with your portal, configure a multiple-machine site.

Single-machine high-availability (active-active) deployment

High availability is a technique to ensure system uptime and to minimize or prevent data loss in the event of a machine failure. ArcGIS Server, like other ArcGIS Enterprise components, can be deployed in a highly available configuration with a third-party network load balancer.

This configuration is a variation of the single-machine high-availability (active-passive) deployment, in which the load balancer is configured to spread the load across all sites at all times. In this configuration, there are no standby sites.

In this architecture, two or more ArcGIS Server sites are configured behind a third-party load balancer to increase the capacity of your ArcGIS Server deployment. You can use this technique to accommodate some of the high-availability limitations described in the single-machine deployment and single-machine deployment with reverse proxy server deployment scenarios, or to scale up by adding more machines.

While you can scale up and achieve high availability by using multiple-machine sites, there are advantages and limitations to active-active deployments, which are discussed below.

The active-active architecture works to clone a single-machine site and place independent instances of it behind a load balancer. Technically, this configuration cannot be described as a multiple-machine site, because each of the sites is independent of each other, composed of a single ArcGIS Server machine, and has its own local configuration store and server directories.

Multiple-machine ArcGIS Server site deployments greatly simplify server administration. However, the active-active architecture can be used in scenarios in which the number and settings of services are well defined and remain static. In these cases, such a configuration can provide significant performance advantages over multiple-machine sites, especially for cached map services.

This architecture can make it easy to replace stale or faulty machines, apply upgrades, or add and remove machines from the site as needed without interrupting services or aborting requests. However, with an active-active architecture, it is your responsibility to keep all sites in sync. This adds an administrative overhead that can make this deployment pattern impractical for cases in which you have many machines or services or caches that change frequently. You or your IT staff must also have a good understanding of third-party load balancers.

ArcGIS Server machines, server directories, and configuration store

Each ArcGIS Server machine must have its own local configuration store and cache, jobs, and system directories. This ensures maximum performance and minimizes interdependency. Conversely, the output directory (or directories) must be shared between each site. For additional details, see other considerations below.

Data

If using file-based data sources in your GIS services, it is recommended that these be stored locally on every ArcGIS Server machine instead of network shares to maximize the performance of your services. In some cases, such as when handling large amounts of imagery, sharing your files over the network may be the only practical choice. If using files in shared resources over the network, it is very important that you choose a storage device configured for high availability.

If using databases, you can dedicate a database to each of your sites: one database for your primary site and a separate one for your standby site. To keep the databases in sync, you can leverage database replication, or if

needed, geodatabase replication techniques. Alternatively, you can leverage other high-availability techniques from your database provider.

Learn more about data and ArcGIS Server

Reverse proxy server

In this configuration, a third-party load balancer is required. At a minimum, this component distributes the load across all the sites. Load balancers have different configurations for distributing the load, such as round robin and least connections. Selecting the correct load distribution depends on the web services you have running on the ArcGIS Server sites, and their patterns of use.

Load balancers also typically leverage different options for handling failures. For example, you may apply rules in your load balancer that prevent it from forwarding requests to a machine that is unavailable due to a hardware or network failure, or to a particular ArcGIS Server service that is not available. If using single-machine sites as in this pattern, requests sent to a particular machine are guaranteed to be managed by that machine.

The use of ArcGIS Web Adaptor is optional and typically only necessary for this scenario if you want to take advantage of web-tier authentication. You can choose to configure it on the same machine as your ArcGIS Server, or on a dedicated machine. In either case, if using ArcGIS Web Adaptor, you must configure a separate ArcGIS Web Adaptor for both sites in the active-active configuration.

Typically, the load balancer itself also fulfills the role of the reverse proxy server. In some scenarios, you may have already configured a reverse proxy server independently of the load balancer.

If your network load balancer supports a health check function, you can use the ArcGIS Server health check endpoint to determine if the site is available to receive requests. This is useful to quickly determine if there's a software or hardware failure in the site. For more information, see Health Check in the ArcGIS REST API.

Considerations for active-active configurations

The following should be kept in mind when planning an ArcGIS Server site with a highly available active-active configuration.

Synchronizing services

Unlike a true multiple-machine site, this configuration requires that all of the sites behind the load balancer host exactly the same content and that they follow the same security model. You are responsible for ensuring that all the sites look exactly the same to the load balancer.

Here are a few techniques that can help you keep ArcGIS Server services in sync across the primary and failover sites:

- Scripting—ArcGIS Server includes a REST API to script administrative tasks, such as publishing services and changing their security settings. You can create your own scripts to apply changes to all the ArcGIS Server machines involved in your deployment consistently. Scripting is especially useful when you need to make small adjustments, such as changing the security of a service or overwriting it.

  Note:
  Each site can be created through scripting. After all sites are created, create a backup from one of the sites and restore the backup to each other site. This ensures that all machines use the same encryption key.

- Virtualization—Create a virtual machine template and use it to launch new sites. As mentioned above, this ensures all machines use the same encryption key. In addition, each template will have a copy of the data needed for GIS services (unless a database is used) and all published and configured services. If changes are necessary, such as adding or updating existing services, create a template to launch subsequent virtual machines that would replace the existing pool of ArcGIS Server machines in use under the load balancer. You can also use virtual machine templates to recover stale ArcGIS Server machines.

The recommended procedure to apply changes to your sites in this deployment pattern is as follows:

1. Make administrative changes against a site that is in standby mode first. For example, add a new service and change the security of another in a site that is not actively handling requests. This ensures there is no impact to applications using your primary site.
2. Manually configure your load balancer to hand over all requests to the standby site on which the changes have been made.
3. Apply the same changes to the idle site.
4. Revert the load balancer so requests are directed back to the original primary site and leave the standby site in standby mode.

Changes to your site in the procedure described above can be applied manually through ArcGIS Server Manager, scripts, or virtual images.

Output directory sharing

Some ArcGIS Server service operations reference resources in one or more output directories. For example, map services can write images to an output directory and reference these images through a URL in the request response. For clients to successfully obtain the image, all sites in your active-active configuration must reference the same output directory. This can be accomplished by placing the output directories on a network resource and sharing them with your sites.

The following is a list of service operations that use output directories:

- Creating a feature service replica (feature service)
- Downloading a raster image (image service)
- Exporting a map image (map service)
- Exporting a schematic diagram (schematics capability in a map service)
- Exporting a web map (geoprocessing service)

Asynchronous execution of geoprocessing services

ArcGIS Server geoprocessing services support two execution modes: synchronous and asynchronous. Synchronous execution follows a stateless request-response pattern and is completely supported in an active-active configuration. Asynchronous execution follows a stateful request-response pattern and is the default. To use asynchronous execution in an active-active configuration, you'll need to consider the following:

- When submitting an asynchronous geoprocessing job, you're returned a job ID that refers to the submitted job and its outputs. Only the ArcGIS Server site that receives the original can recognize this ID. For this reason, the active-active configuration requires you to define affinity in your load balancer (also known as sticky sessions) if you want to use asynchronous execution. This helps provide high availability for asynchronous geoprocessing and

map service outputs. Refer to your load balancer vendor to understand the implications of enabling sticky sessions.

- If your geoprocessing service does not use map services to render outputs and no outputs of type File have been defined, you can select synchronous execution for your geoprocessing services. No sticky sessions in your load balancer are required.

Using token-based security

If using token-based authentication, also referred to as server-tier authentication, it is important that all sites in this configuration use exactly the same shared token key. Otherwise, tokens generated for one machine will not be valid when used against the other machine. To duplicate the shared token keys across multiple sites, you can edit token settings in Manager.

Upgrade approaches

To ensure the least amount of downtime, you can upgrade your ArcGIS Server sites in sequence. When upgrading a site, you can configure your load balancer to prevent it from forwarding requests to the unavailable site and distribute the load across other independent sites in your active-active architecture.

The other approach, upgrading all ArcGIS Server sites in parallel, is practical if your organization can tolerate some amount of downtime and data loss. Since all sites in an active-active architecture are independent of each other, you can upgrade them simultaneously with no interdependency issues.

Federation

Since there are distinct configuration stores for each site, single-machine active-active ArcGIS Server deployments cannot be federated with Portal for ArcGIS. To federate a highly available server site with your portal, configure a multiple-machine site.

Multiple machine site configurations

Multiple-machine deployment with ArcGIS Web Adaptor

ArcGIS Server supports the configuration of multiple-machine sites. In a multiple-machine site, two or more ArcGIS Server machines can be administered and used as a single logical unit, providing ArcGIS Server administrators with great flexibility to easily adjust the computing power of the site by adding or removing ArcGIS Server machines. Multiple-machine sites also simplify the process of publishing and updating services across multiple ArcGIS Server machines.

In a multiple-machine deployment, each ArcGIS Server must be at the same version number for the site to function correctly. Additionally, the exact same license must be applied to each ArcGIS Server that participates in the site.

In its simplest configuration, a multiple-machine site is configured by setting up a pool of two or more ArcGIS Server machines fronted by ArcGIS Web Adaptor running on your own web application server.

A key aspect of multiple-machine configurations is that all ArcGIS Server machines share the same configuration store and server directories. In this manner, an administrator can log in to any ArcGIS Server using ArcGIS Server Manager and apply changes that will affect all machines within the site. This pattern is also ideal in cases where you want to integrate your site with authentication methods in your organization's web tier.

Server performance can suffer when shared locations are used for multi-machine site directories and data, owing to several factors — network bandwidth and stability, opportunistic locking, and network drive performance among them. Use of server directories and data in shared network locations can also negatively affect performance of services under heavy load.

ArcGIS Server machines, server directories, and configuration store

Because all ArcGIS Server machines in multiple-machine configurations share the same configuration store and server directories, you must select a network location for your server directories and configuration store.

Typically, a domain account is chosen for the ArcGIS Server account, because this simplifies the management of data access permissions to network resources. However, depending on your own security policies, you may choose to use local accounts. The ArcGIS Server account (local or domain) needs to have write access to the network share where the configuration store and server directories are located. For more information, see Accounts used by ArcGIS Server.

Data

As described in other deployment scenarios, when using file-based data, it is highly recommended to use local resources to the ArcGIS Server machine. This has the disadvantage of forcing you to duplicate your data across all ArcGIS Servers, but reduces network traffic and results in higher performance for your services. You should consider this option and use it when applicable. The size of your data and the frequency of updates often dictate if keeping your data local across all machines is practical.

When using databases in this deployment pattern, it is important that you always use dedicated hardware. Keep the database tier independent from the ArcGIS Server tier.

Web Adaptor

In this configuration, ArcGIS Server clients never connect directly to your ArcGIS Servers. Instead, they connect through a Web Adaptor that provides security features and makes your overall site more resilient to failures.

From a security perspective, it's not a recommended practice to access the same channel to use and administer your site. Typically, administrative tasks are only enabled through sections of your network or specific machines that

can access your ArcGIS Server machines directly over port 6443. You can overcome this by specifying that only certain IP addresses can access the server in the Administrator Directory. This is controlled by the `allowedAdminAccessIPs` property in the server's security configuration. To learn how to configure this property to limit access to the server, see the example in Update security configuration.

Requests from client applications are always funneled through ArcGIS Web Adaptor, which can be configured to block the use of any administrative end points.

ArcGIS Web Adaptor also provides the means to integrate ArcGIS Server with standard authentication methods used in your organization. It is a small component that you can install in your own web server acting as a reverse proxy to your ArcGIS Server machines. For a list of supported web servers, see ArcGIS Web Adaptor system requirements. By configuring ArcGIS Server security to use web-tier authentication (as opposed to GIS-tier authentication), ArcGIS Server will delegate authentication into your web server.

Multiple web adaptors can be configured with your site to support multiple authentication methods. To learn more, see Support a mix of public and private services.

ArcGIS Web Adaptor also serves as a load-balancer for the site. ArcGIS Web Adaptor will forward requests to your pool of ArcGIS Server machines following a round-robin, load-balancing algorithm. ArcGIS Web Adaptor will also automatically detect and forward requests to any new ArcGIS Server that is added to your site, or it will stop forwarding requests to machines that are unavailable or dropped from your site.

High availability considerations

A highly available variation of this deployment scenario would add redundancy at the Web Adaptor tier. When configuring multiple Web Adaptors with your site, each Web Adaptor will round-robin requests to all the ArcGIS Server machines in your site.

Consideration should be taken to also eliminate single points of failure at the data, configuration store, and server directories.

Duplicating your file-based datasets across all ArcGIS Server machines can help you, although it may not always be possible due to the frequency of changes in your files or their size. If using a network share for your file-based datasets, ensure that your storage is configured for high availability.

Databases supported by ArcGIS also support different levels of high availability configuration. Refer to the database configuration to cluster your database tier.

In this deployment scenario, your configuration store and server directories must always be stored on a network share. If requiring a high availability configuration, ensure that this tier is set up accordingly.

Multiple-machine deployment with third party load balancer

ArcGIS Server supports the configuration of multiple-machine sites. In a multiple-machine site, two or more servers can be administered and used as a single logical unit, providing ArcGIS Server administrators with great flexibility to easily adjust the computing power of the site by adding or removing machines. Multiple-machine sites also simplify the process of publishing and updating services across multiple ArcGIS Server machines.

In a multiple-machine deployment, each ArcGIS Server machine must be at the same version number for the site to function correctly. Additionally, the exact same license must be applied to each machine that participates in the site.

A common multiple-machine configuration involves a third-party reverse proxy server or network load balancer sitting in front of a pool of ArcGIS Server machines.

A key aspect of multiple-machine configurations is that all ArcGIS Server machines share the same configuration store and server directories. In this manner, an administrator can log in to any machine using ArcGIS Server Manager and apply changes that will affect all machines within the site.

A single ArcGIS Server site provides the means to easily administer ArcGIS Server and its services across a number of machines. However, the use of ArcGIS Server directories and data in shared network locations can negatively affect performance of services under heavy load.

Configuring a third-party load balancer or reverse proxy server grants flexibility to your organization, with greater control over how requests are handled. You cannot configure web-tier authentication with this configuration; to do so, you must configure a multiple-machine deployment with ArcGIS Web Adaptor.

ArcGIS Server machines, server directories, and configuration store

Because all ArcGIS Server machines in multiple-machine configurations share the same configuration store and server directories, you must select a network location for your server directories and configuration store.

Typically, a domain account is chosen for the ArcGIS Server account because this simplifies the management of data access permissions to network resources. However, depending on your own security policies, you may choose to use local accounts. The ArcGIS Server account (local or domain) needs to have write access to the network share where the configuration store and server directories are located. For more information, see Accounts used by ArcGIS Server.

Data

As described in other deployment scenarios, when using file-based data, it is highly recommended to use local resources to the ArcGIS Server machine. This has the disadvantage of forcing you to duplicate your data across all machines, but reduces network traffic and results in higher performance for your services. You should consider this option and use it when it is applicable. The size of your data and the frequency of updates often dictate if keeping your data local across all machines is a practical approach.

When using databases in this deployment pattern, it is important that you always use dedicated hardware. Keep the database tier independent from the ArcGIS Server tier.

Third-party reverse proxy server or network load-balancer

In this configuration, ArcGIS Server clients never connect directly to your ArcGIS Server machines. Instead, they connect through a middle tier that provides security features and makes your overall site more resilient to failures.

From a security perspective, it is not a recommended practice to access the same channel to use and administer your site. Typically, administrative tasks are only enabled through sections of your network or specific machines that can access your ArcGIS Server machines directly over port 6443. You can overcome this by specifying that only certain IP addresses can access the server in the Administrator Directory. This is controlled by the `allowedAdminAccessIPs` property in the server's security configuration. To learn how to configure this property to limit access to the server, see the example in Update security configuration.

Requests from client applications are always funneled through the reverse proxy, which prevents the use of any administrative end points. Most third-party proxies allow you to filter incoming requests that include a particular URL pattern. Blocking incoming requests using resources under the ArcGIS Server Administrator Directory (`https://gisserver.domain.com:6443/arcgis/admin`) or ArcGIS Server Manager (`https://gisserver.domain.com:6443/arcgis/manager`) effectively block any administrative tasks through your reverse proxy.

Your reverse proxy also serves as a load balancer for the site. A simple load-balancing algorithm such as round-robin is adequate for this configuration.

Note:
If you do not use ArcGIS Web Adaptor, be sure that the load balancer context name only goes one level deep. For example, you can have a load balancer URL such as `https://lb.domain.com/enterprise`, but you cannot have a load balancer URL such as `https://lb.domain.com/myorg/enterprise`.

If your network load balancer supports a health check function, you can use the ArcGIS Server site's Health Check endpoint in the REST API to determine if the site is available to receive requests. This is useful to quickly determine if there's a software or hardware failure in the site.

To learn how to integrate a reverse proxy server with ArcGIS Server, see Configure a reverse proxy server with ArcGIS Server.

Configure ArcGIS Web Adaptor with a server site

After you install ArcGIS Web Adaptor, you must configure it to work with a server site. You'll do this from a configuration web page or from a command line utility that was installed with the Web Adaptor. As a security measure, you can only access the configuration page and command line utility from the machine hosting the Web Adaptor.

When you open the configuration page, the current status of the Web Adaptor is displayed. This indicates whether the Web Adaptor has been previously configured. To view the platform type and version number of the Web Adaptor, click **About** on the configuration page.

For full instructions on how to configure the Web Adaptor, see the sections below.

Configuring the Web Adaptor from the configuration web page

To configure the Web Adaptor from the configuration web page that was installed with the software, follow the steps below.

Note:
There are additional considerations for ArcGIS Mission Server, ArcGIS Notebook Server, and ArcGIS Video Server that should be reviewed at this point.

1. Open the Web Adaptor configuration page in a web browser.
   The URL is in the format `https://webadaptorhost.domain.com/webadaptorname/webadaptor`.

   Note:
   If the web server where you installed ArcGIS Web Adaptor is configured to use a forward proxy, disable it while registering the Web Adaptor. Otherwise, you will be unable to access the Web Adaptor configuration page.

2. Select the type of server you want to configure with the Web Adaptor. Click **Next**.
3. Enter the machine name for one of the servers you are registering in your site.
   This machine name will be used to discover all of the machines participating in your server site and register them with the Web Adaptor. The machine name should be in the form `server.domain.com`.
4. Provide a username and password for an account that has administrative privileges to the server site. Typically, you'll use the primary site administrator account username and password you defined when you created the site. If you disabled the primary site administrator account, you'll need to specify an account with administrative access to the site.
5. If you are configuring a server site, you can choose whether users can administer the site through ArcGIS Web Adaptor. By default, administration of the site through ArcGIS Web Adaptor is enabled. The following are considerations for this option:
   - When administration is disabled, external users cannot access ArcGIS Server Manager and the ArcGIS Server Administrator Directory through ArcGIS Web Adaptor. Also, ArcGIS Pro users cannot establish administrative or publisher connections to ArcGIS Server. You can still make user connections from ArcGIS Pro to ArcGIS Server whether this option is enabled or disabled.

- When administrative access through ArcGIS Web Adaptor is disabled, you can access Server Manager and the Administrator Directory and connect to the server in ArcGIS Pro using a direct URL to one of the ArcGIS Server machines in your site as follows:
  - To access Server Manager, use the URL format `https://server.domain.com:6443/arcgis/manager`.
  - To access the Administrator Directory, use the URL format `https://server.domain.com:6443/arcgis/admin`.
  - To create a server connection in ArcGIS Pro, use the URL format `https://server.domain.com:6443/arcgis`.
- If ArcGIS Server is configured with web-tier authentication, you must keep administration enabled through ArcGIS Web Adaptor. This allows users in your organization-specific identity store with publisher and administrator privileges to publish services from ArcGIS Pro. When users in these roles connect to the server in ArcGIS Pro, they must specify the ArcGIS Web Adaptor URL.

6. Click **Configure** to apply your settings to the Web Adaptor.

When the configuration is successful, machines recognized by the Web Adaptor are listed at the bottom of the configuration page (highlighted in green). You can return to this page at any time to see the list of recognized machines and adjust the Web Adaptor settings.

Configuring the Web Adaptor from the command line

You can configure the Web Adaptor using the command line utility (`ConfigureWebAdaptor.exe`) in `C:\Program Files\Common Files\ArcGIS\WebAdaptor\IIS\<current version>\Tools`.

The available parameters are as follows:

`ConfigureWebAdaptor.exe /m <Mode> /w <WebAdaptorURL> /g <MachineName|URL> /u <Username> /p <Password> /a <AdminAccessEnabled>`

- `<Mode>`—The component with which the Web Adaptor will be configured. By default, this parameter is set to `server`, meaning that the Web Adaptor can be configured for use with server site. Below are the parameters you can use to configure other components.
  - Portal for ArcGIS—`portal`
  - ArcGIS Mission Server—`mission`
  - Notebook Server—`notebook`
  - Video Server—`video`
  - ArcGIS Monitor—`monitor`
- `<WebAdaptorURL>`—The URL of the Web Adaptor that you want to configure from the command line. This is the same URL that would be used if you were accessing the Web Adaptor configuration page in a web browser. If the Web Adaptor was installed on a port other than the default of 80, specify the port in the URL.
- `<MachineName|URL>`—The machine name for one of the machines in your server site, for example `server.domain.com`. You can also use the server machine URL instead of the machine name. If you are configuring the Web Adaptor with ArcGIS Server, the machine name or URL will be used to discover all of the machines participating in your site.

- `<Username>`—The username of an account that has administrative privileges to the server site. For ArcGIS Server, this account may be the Primary Site Administrator account entered when the site was first created or an account that has been assigned administrative privileges. For ArcGIS Mission Server, Notebook Server, and Video Server, enter the username for the Primary Site Administrator account used when the site was created.
- `<Password>`—The password of the account that has administrative privileges to the server site.
- `<AdminAccessEnabled>`—The option to enable administrative access only applies to ArcGIS Server. Enabled administrative access (`true`) allows the ArcGIS Server Manager and ArcGIS Server Administrator Directory applications to be accessed through the Web Adaptor. If administrative access is not allowed (`false`), these applications can be accessed using a direct URL to one of the servers in the site. For example, ArcGIS Server Manager can be accessed using `http://machine:6443/arcgis/manager`, and the ArcGIS Server Administrator Directory can be accessed using `http://machine:6443/arcgis/admin`. When configuring Portal for ArcGIS, Notebook Server, and ArcGIS Mission Server, administrative access is required and enabled by default.

See the following example: `ConfigureWebAdaptor.exe /m server /w https://webadaptorhost.domain.com/webadaptorname/webadaptor /g server.domain.com /u siteadmin /p secret /a false`

After configuring the Web Adaptor

Now that the Web Adaptor has been configured for use, consider the items below.

Adding or removing server machines

If you add or remove server machines from your site, it takes the Web Adaptor 1 minute to recognize the changes to your site. If you want the Web Adaptor to immediately recognize the added or removed machines, you can reconfigure it by following the instructions above.

Installing multiple Web Adaptors

You can provide different web entry points into your server site by installing multiple Web Adaptors. Doing so makes your site more highly available to clients, provides support for legacy applications, and allows publishing and administrative access to specific users in a highly secure environment. For more information, see Deployment scenarios.

Multiple Web Adaptors can be installed on the same machine at the same time, or they can be installed on separate machines. To install multiple Web Adaptors on the same website (port), use different names for them. For example, two Web Adaptors named arcgis cannot exist on the same website. If you want multiple Web Adaptors with the same name, you must install them on separate websites (ports).

For full instructions on how to install multiple Web Adaptors, see Installing multiple Web Adaptors.

Configure web-tier authentication with Integrated Windows Authentication

You can configure web-tier authentication for your ArcGIS Server site using Integrated Windows Authentication. This requires users and roles to be managed in an Active Directory server. It can be a convenient approach when you want your users to take advantage of Windows domain accounts they already have on your network.

Note:
If your ArcGIS Server site is federated with a portal, you must secure access through the portal rather than using the steps in this topic. See Use Integrated Windows Authentication with your portal for details.

To use Integrated Windows Authentication, you must use ArcGIS Web Adaptor (IIS) deployed to the Microsoft IIS web server. You cannot use ArcGIS Web Adaptor (Java Platform) to perform Integrated Windows Authentication.

If your login settings deny login rights to the machine where Active Directory is hosted, you'll encounter an error when configuring security. It's not necessary to grant **Log on locally** group policy settings to the user. For more information, see Advanced considerations when using domain accounts.

To configure Integrated Windows Authentication with your server site, follow these steps:

1. Configure ArcGIS Web Adaptor (IIS) to use Windows authentication.
2. Configure ArcGIS Server to use Windows Active Directory users and roles.
3. Review users and roles.
4. Configure Administrator and Publisher privileges for Active Directory users.
5. Set permissions for services.
6. Test access to secured services.

Configure ArcGIS Web Adaptor (IIS) to use Windows authentication

The web adaptor relies on IIS to authenticate the user and provide the web adaptor with the account name of the user. Once it has the account name, it passes that to ArcGIS Server.

1. Install ArcGIS Web Adaptor (IIS), following the instructions in Install ArcGIS Web Adaptor (IIS).
2. Configure ArcGIS Web Adaptor following the instructions in Configure ArcGIS Web Adaptor after installation.

   Note:
   When configuring ArcGIS Web Adaptor, you must enable administration through the web adaptor. This allows users in Windows Active Directory to publish services from ArcGIS Pro. When the users in these roles connect to the server in ArcGIS Pro, they must specify the web adaptor URL.

3. Set the authentication method for the web adaptor using IIS Manager.
   a. To open IIS Manager, click **Start** > **Control Panel** > **Administrative Tools** > **Internet Information Services Manager**.
   b. Under **Sites**, expand the left tree of IIS Manager. Expand **Default Web Site** to find the ArcGIS Web Adaptor (IIS) application. By default, ArcGIS Web Adaptor (IIS) is named **arcgis**.

c. Edit the authentication property for the web adaptor. Deselect **Anonymous** authentication and select **Windows Authentication**.

d. Close IIS Manager.

Configure ArcGIS Server security to use Windows Active Directory users and roles

To support Integrated Windows Authentication, configure ArcGIS Server to retrieve users and roles from a Windows Active Directory server.

1. Open Manager and sign in as the primary site administrator. If you need help with this step, see Log in to Manager.
   You must use the primary site administrator account.
2. Click **Security** > **Settings**.
3. Click the **Edit** button next to **Configuration Settings**.
4. On the **User and Role Management** page, choose the **Users and roles in an existing enterprise system (LDAP or Windows Domain)** option and click **Next**.
5. On the **Enterprise Store Type** page, choose the **Windows Domain** option and click **Next**.
6. On the **Windows Domain Credentials** page, provide the credentials for an account that has permissions to determine the groups in which users reside. Click **Next**.

   Note:
   It is recommended that you specify an account with a password that does not expire. If this is not possible, you'll need to repeat the steps in this section each time the password is changed.

7. On the **Authentication Tier** page, choose **Web Tier**.
8. Review the summary of your selections. Click **Finish** to apply and save the security configuration.

Review users and roles

After configuring a Windows Active Directory domain as the user and role store, review the users and roles to ensure they were retrieved correctly. To add, edit, or delete users and roles, you must use the tools available on the Active Directory server.

1. In Manager, click **Security** > **Users**.
2. Verify users have been retrieved as expected from the Windows domain server.
   If Active Directory has multiple domains, users from the domain that the GIS server machine belongs to are displayed.
3. To view users from other domains, provide the search string `[domain name]\` in the **Find User** field and click the **Search** button .
4. Click **Roles** to review roles retrieved from the Windows domain server.
   If Active Directory has multiple domains, roles from the domain that the GIS server machine belongs to are displayed.
5. To view roles from other domains, provide the search string `[domain name]\` in the **Find Role** field and click the **Search** button .

6. Verify the roles have been retrieved as expected.

Note:
At 10.3.1 and later versions, ArcGIS Web Adaptor (IIS) has properties to configure options related to Active Directory authentication. See Configure ArcGIS Web Adaptor memory cache options in the ArcGIS Web Adaptor (IIS) help for details.

Caching of users and roles

As of 10.5, users and roles from your Active Directory will be cached on the server after a request for users or roles. This optimizes the performance of your secure services. By default, the users and roles will be cached for 30 minutes. You can modify this time period by setting the `minutesToCacheUsersAndRoles` property to another value in the ArcGIS Server Administrator Directory under system properties. You can also disable caching by setting the property to zero.

Configure administrator and publisher privileges for Active Directory users

Out of the box, ArcGIS Server only allows the primary site administrator access to the server. If you'll be using Active Directory users to administer ArcGIS Server or publish services, you must follow the steps below.

1. In ArcGIS Server Manager, click the **Security** tab and open the **Users** page.
2. Using the **Find User** tool, locate the user to whom you want to assign administrator or publisher privileges. Review the roles of which this user is a member and choose the role that will be assigned administrator or publisher privileges.
3. Open the **Roles** page and use the **Find Role** tool to locate the role chosen in the previous step.
4. Click the **Edit** button next to the role.
5. For the **Role Type** parameter, choose either **Publisher** or **Administrator**.
6. Click **Save** to apply your changes.

Set permissions for ArcGIS web services

Once you've configured your security settings and defined users and roles, you can set permissions for services to control who is allowed to access them.

ArcGIS Server controls access to services using a role-based access control model. In a role-based access control model, the permission to access a secured service is controlled by assigning roles to that service. To consume a secured service, a user must be a member of a role that has been assigned permissions to access it.

To change the permissions for a service, see Control access to your services.

Note:
When browsing ArcGIS Server Manager using Integrated Windows Authentication, the **Sign Out** link is no longer visible. This is because the user running the web browser is signed in automatically by the operating system. To run the browser as another user, you can use the Windows **Run as** command option. To do this, locate the program shortcut on the **Start** menu, press the `Shift` key while right-clicking the program, and choose **Run as different user**.

Test access to secured services

To test your setup, identify a Windows domain user account that has access to the root (site) folder containing your services. Sign in to Windows using this user account, open a web browser, and access your ArcGIS Server WSDL:

`https://webadaptorhost.domain.com/webadaptorname/services?wsdl`

Similarly, you can also view the Services Directory to verify access to secured services:

`https://webadaptorhost.domain.com/webadaptorname/rest/services`

Note:
When browsing the Services Directory using Integrated Windows Authentication, the **Logout** link is no longer visible. This is because the user running the web browser is signed in automatically by the operating system. To run the browser as another user, you can use the Windows **Run as** command option. To do this, locate the program shortcut on the **Start** menu, press the `Shift` key while right-clicking the program, and choose **Run as different user**.

To determine which Windows domain users have access to the root folder, do the following:

1. Sign in to Manager and click **Services**.
2. Click the **Lock** button next to the site (root) folder and identify roles that have been given permission to access this folder. If no roles currently have access, grant access to at least one role by clicking **Add Role**.
3. Click **Security** > **Roles** and click the **Edit** button for the role that has access to the root folder.
4. View the list of users who are members of this role.

Configure ArcGIS Web Adaptor memory cache options

When an authenticated user accesses an ArcGIS Server resource and web-tier authentication has been enabled using ArcGIS Web Adaptor (IIS), the Web Adaptor retrieves the user's role membership list from Active Directory. Repeated calls to Active Directory to obtain a user's role list negatively impacts performance of both Active Directory and ArcGIS Server. To optimize performance, the Web Adaptor caches the list of roles that a user is a member of.

In an out-of-the-box installation of ArcGIS Web Adaptor (IIS), a user's roles are cached either in a cookie managed by the web browser or in the primary system memory (RAM) of the web server hosting the Web Adaptor. If the size of a user's role list is less than 4KB, the list is stored as a cookie by the web browser. If the list is 4KB or larger, it is managed in the system memory.

If a user's role list is stored in the web browser cookie cache, it expires in one minute. The ArcGIS Web Adaptor (IIS) system memory cache for a user's role list is configurable and its properties are managed in the `RoleCache` element defined in the `C:\inetpub\wwwroot\{Web Adaptor name}\WebAdaptor.config` file. The following section describes the `RoleCache` element and its properties.

```
<RoleCache>
    <NumberOfUsers>100</NumberOfUsers>
    <Expiration>5</Expiration>
    <Enabled>true</Enabled>
    <CacheAllRolesInMemory>false</CacheAllRolesInMemory>
</RoleCache>
```

Property	Description
`NumberOfUsers`	This property limits the number of users that can have their role membership list stored in the system memory.
`Expiration`	This property defines the amount of time, in minutes, that a user's list is stored in the system memory. The maximum recommended value for this property is one day (or 1,440 minutes).
`Enabled`	This property is used to disable the system memory cache. Disabling the system cache is not recommended.
`CacheAllRolesInMemory`	If this property is set to `true`, the cookie cache is disabled and only the system memory is used to cache the role membership list for all users.

Configure a CA-signed certificate for ArcGIS Server when accessed through ArcGIS Web Adaptor

When ArcGIS Web Adaptor has been configured to forward requests to your ArcGIS Server site, you need to enable HTTPS on the web server hosting ArcGIS Web Adaptor. To get started, follow the steps in the sections below.

1. Create a new self-signed certificate.
2. Request a CA to sign your certificate.
3. Configure ArcGIS Server to use the certificate.
4. Configure each machine in your deployment.
5. Configure HTTPS on ArcGIS Web Adaptor.
6. Access your site.

Create a new self-signed certificate

1. Sign in to the ArcGIS Server Administrator Directory at `https://gisserver.domain.com:6443/arcgis/admin`.
2. Browse to **machines** > **[machine name]** > **sslcertificates**.
3. Click **generate**.
4. Provide values for the parameters on this page:

Option	Description
Alias	A unique name that easily identifies the certificate.
Key Algorithm	Use RSA (the default) or DSA.
Key Size	Specifies the size in bits to use when generating the cryptographic keys used to create the certificate. The larger the key size, the harder it is to break the encryption; however, the time to decrypt encrypted data increases with key size. For DSA, the key size can be between 512 and 1,024. For RSA, the recommended key size is 2,048 or greater.
Signature Algorithm	Use the default (`SHA1withRSA`). If your organization has specific security restrictions, one of the following algorithms can be used for DSA: `SHA256withRSA`, `SHA384withRSA`, `SHA512withRSA`, `SHA1withDSA`.
Common Name	Use the domain name of your server name as the common name. If your server will be accessed on the Internet through the URL `https://www.gisserver.com:6443/arcgis/`, use `www.gisserver.com` as the common name. If your server will only be accessible on your local area network (LAN) through the URL `https://gisserver.domain.com:6443/arcgis`, use `gisserver.domain.com` as the common name.
Organizational Unit	The name of your organizational unit, for example, GIS Department.
Organization	The name of your organization, for example, Esri.

Option	Description
City or Locality	The name of the city or locality, for example, Redlands.
State or Province	The full name of your state or province, for example, California.
Country Code	The abbreviated code for your country, for example, US.
Validity	The total time in days during which this certificate will be valid, for example, 365.
Subject Alternative Name	The subject alternative name (SAN) is an optional parameter that defines alternatives to the common name (CN) specified in the certificate. There cannot be any spaces in the SAN parameter value. If this parameter is left empty, the fully qualified domain name of the local machine is used as the default value. The SAN field supports multiple values; however, it must include the fully qualified domain name of the website. For example, the URLs `https://www.esri.com`, `https://esri`, and `https://10.60.1.16` can be used to access the same site if the certificate is created using the following SAN parameter value: `DNS:www.esri.com,DNS:esri,IP:10.60.1.16`

5. Click **Generate** to generate the certificate.

Request a CA to sign your certificate

If ArcGIS Web Adaptor will be the only gateway to your site and your organization's IT security policy allows the use of self-signed certificates, you can skip this section. However, if users will occasionally bypass ArcGIS Web Adaptor and access ArcGIS Server directly or your IT policies disallow the use of self-signed certificates, it is recommended to request a CA to sign your certificate by following the steps below.

1. Open the self-signed certificate you created in the previous section and click **generateCSR**. Copy the contents into a file, usually with a `.csr` extension.
2. Submit the CSR to a CA of your choice. You can obtain a Distinguished Encoding Rules (DER) or Base64 encoded certificate. If the CA requests the type of web server the certificate is for, specify **Other\Unknown** or **Java Application Server**. After verifying your identity, the CA will send you a `.crt` or `.cer` file.
3. Save the signed certificate you received from the CA to a location on your computer. In addition to the signed certificate, the CA will also issue a root certificate. Save the CA root certificate to your computer.
4. Sign in to the ArcGIS Server Administrator Directory: `https://gisserver.domain.com:6443/arcgis/admin`.
5. Click **machines > [machine name] > sslcertificates** > **importRootOrIntermediate** to import the root certificate provided by the CA. If the CA issued any additional intermediate certificates, import those as well.
6. Browse to **machines** > **[machine name]** > **sslcertificates**.
7. Click the name of the self-signed certificate that you submitted to the CA.
8. Click **importSignedCertificate** and browse to the location where you saved the signed certificate you received from the CA.
9. Click **Submit**. This replaces the self-signed certificate you created in the previous section with the CA-signed certificate.

Configure ArcGIS Server to use the certificate

To specify the certificate that ArcGIS Server should use, complete the following steps:

1. Sign in to the ArcGIS Server Administrator Directory at `https://gisserver.domain.com:6443/arcgis/admin`.
2. Browse to **machines** > **[machine name]**.
3. Click **edit**.
4. Type the name of the certificate that you want to use in the **Web server SSL Certificate** field.
5. Click **Save Edits** to apply your change. This automatically restarts your ArcGIS Server site.
6. After your site has restarted, verify that you can access the URL `https://gisserver.domain.com:6443/arcgis/admin`. If you do not get a response from this URL, ArcGIS Server was unable to use the specified SSL certificate. Check your SSL certificate and configure ArcGIS Server to use a new or different certificate.
7. On the current page, view the property **Web server SSL Certificate** to verify that the desired certificate will be used for HTTPS.

Configure each machine in your deployment

If you have a multiple-machine deployment of ArcGIS Server, you must configure each machine in your deployment to use the certificate. Repeat the steps in the previous section to configure the certificate with each of your ArcGIS Server machines.

Configure HTTPS on ArcGIS Web Adaptor

Enable HTTPS on the web server that is hosting ArcGIS Web Adaptor. For full instructions, consult the product documentation specific to your web server.

Access your site

You can securely access ArcGIS Server directly though HTTPS using port 6443 or the Web Adaptor URL. If you rename your ArcGIS Server site, you can continue to access ArcGIS Server using HTTPS; however, you must generate a new certificate and configure ArcGIS Server to use it. The URLs are formatted as follows:

ArcGIS Server Manager	Access Manager through the server: `https://gisserver.domain.com:6443/arcgis/manager`. Access Manager through ArcGIS Web Adaptor (only applies if administrative access is enabled): `https://webadaptorhost.domain.com/webadaptorname/manager`.
ArcGIS Server Services Directory	Access Services Directory through the server: `https://gisserver.domain.com:6443/arcgis/rest/services`. Access Services Directory through ArcGIS Web Adaptor: `https://webadaptorhost.domain.com/webadaptorname/rest/services`.

Disable Windows Active Directory groups lookup in ArcGIS Web Adaptor (IIS)

When performing web-tier authentication with ArcGIS Web Adaptor (IIS), the Web Adaptor will look up Windows Active Directory groups for the signed-in user every time a request is sent to your ArcGIS Server site. In organizations with a small number of groups, this lookup will have no impact on performance. However, if your organization has hundreds or thousands of groups, you may see a decrease in performance because of the time it takes to complete the lookup.

If you notice a performance decrease, you can disable Active Directory groups lookup in ArcGIS Web Adaptor (IIS). Disabling this functionality is only applicable if the following criteria are met:

- You've configured web-tier authentication (Integrated Windows Authentication or PKI-based client certificate authentication) in ArcGIS Web Adaptor (IIS).
- You're using the ArcGIS Server built-in groups as the group store for your site. If you're using groups from Windows Active Directory, the lookup must occur to obtain groups.

To disable Active Directory groups lookup in ArcGIS Web Adaptor (IIS), do the following:

1. On the machine hosting ArcGIS Web Adaptor (IIS), browse to and open the WebAdaptor.config file. By default, this file is located in the IIS inetpub folder, for example, `C:\inetpub\wwwroot\<web adaptor name>\WebAdaptor.config`.
2. Locate the `EnableGetRolesForUser` property and change the value to false, for example:

   ```
   <EnableGetRolesForUser>false</EnableGetRolesForUser>
   ```

3. Save and close the file.
4. Restart IIS.
5. Repeat these steps on the remaining Web Adaptors configured with your site.

You can enable lookups at any time by changing the `EnableGetRolesForUser` property to `true`.

Configure ArcGIS Web Adaptor with Portal for ArcGIS

After you install ArcGIS Web Adaptor, you must configure it to work with your ArcGIS Enterprise portal. You'll do this from a configuration web page or from a command line utility that was installed with ArcGIS Web Adaptor. As a security measure, you can only access the configuration page from the machine hosting ArcGIS Web Adaptor.

When you open the configuration page, the current status of ArcGIS Web Adaptor is displayed. This indicates whether ArcGIS Web Adaptor has been previously configured. To view the platform type and version number of ArcGIS Web Adaptor, click **About** on the configuration page.

If you've already configured a Web Adaptor with your ArcGIS Enterprise portal and want to update your portal to use a different Web Adaptor, you must first unregister the current Web Adaptor. You can only do this through the Portal Directory; the unregister functionality is not available from the configuration page or the portal website. For full instructions, see Unregister ArcGIS Web Adaptor with Portal for ArcGIS.

Caution:

Although you can modify a portal's Web Adaptor by registering a new one, doing so may also impact user content in the portal (for example, map notes or other items).

For full instructions on how to configure ArcGIS Web Adaptor, follow the steps below.

Note:

The use of the default HTTPS port 443 is appropriate for the majority of users. In some rare cases, an ArcGIS Web Adaptor instance cannot use port 443 on its web server for organization-specific reasons. If this applies to your organization, see Use nondefault ports for the portal's ArcGIS Web Adaptor, which details additional steps to configure a workaround.

Configure ArcGIS Web Adaptor from the configuration web page

To configure ArcGIS Web Adaptor from the configuration web page that was installed with the software, complete the following steps:

Caution:

To add a DNS alias or reverse proxy after an ArcGIS Server site has been federated with your portal, see Update the organization URL.

1. If you haven't done so already, enable HTTPS on your web server.
2. Open the configuration page in a web browser using an HTTPS URL such as `https://webadaptorhost.domain.com/webadaptorname/webadaptor`. If a DNS alias will be used with the portal, the Web Adaptor should be configured over the DNS alias instead, using a URL such as `https://<dnsalias.domain.com>/<webadaptorname>/webadaptor`.

   Note:

   If you have a forward proxy running on the web server where you've installed ArcGIS Web Adaptor, disable it while registering the Web Adaptor. Otherwise, you will be unable to access the Web Adaptor configuration page.

3. Choose **Portal for ArcGIS** and click **Next**.
4. Enter the name of the machine hosting Portal for ArcGIS. Include the fully qualified domain name, for example, `portal.domain.com`.
5. Supply a username and password for an account that has administrative privileges to Portal for ArcGIS. Typically, you'll use the initial administrator account username and password you defined when you set up your portal. If you demoted or deleted the initial administrator account, you must specify an account with administrative access to the portal website.
6. Click **Configure**.

ArcGIS Web Adaptor is configured for use with the machine hosting Portal for ArcGIS. Now, you'll access your portal through the ArcGIS Web Adaptor URL instead of port 7443. The URL is in the following format: `https://webadaptorhost.domain.com/webadaptorname/home`.

If you configured your portal to use HTTPS for all communication, you should update the installed portal website and help shortcut URLs to use `https` instead of `http`; otherwise, you'll see failures in your browser when attempting to access the original shortcut URLs.

If you'll be configuring Portal for ArcGIS with your organization's reverse proxy server, you must provide some information to your portal about the proxy server. For full instructions, see Integrate your portal with a reverse proxy or load balancer.

Configure ArcGIS Web Adaptor from the command line

You can configure ArcGIS Web Adaptor (IIS) using the command line utility (`ConfigureWebAdaptor.exe`) in `C:\Program Files\Common Files\ArcGIS\WebAdaptor\IIS\<current version>\Tools`.

The available parameters are as follows:

`ConfigureWebAdaptor.exe /m <Mode> /w <WebAdaptorURL> /g <MachineName|URL> /u <Username> /p <Password> -r <ReindexPortal>`

- `<Mode>`—The component with which ArcGIS Web Adaptor will be configured. By default, this parameter is set to `server`, meaning that ArcGIS Web Adaptor will be configured for use with the GIS Server, Image Server, or GeoAnalytics Server. Since you're configuring ArcGIS Web Adaptor for use with Portal for ArcGIS, specify this parameter as `portal`.
- `<WebAdaptorURL>`—The URL of ArcGIS Web Adaptor that you want to configure from the command line. This is the same URL that would be used if you were accessing the configuration page in a web browser. You're required to specify the HTTPS URL of ArcGIS Web Adaptor, for example, `https://webadaptorhost.domain.com/webadaptorname/webadaptor`. If a DNS Alias will be used with the portal, the Web Adaptor should be configured over the DNS Alias instead, using a URL such as `https://<dnsalias.domain.com>/<webadaptorname>/webadaptor`.
- `<MachineName|URL>`—The name of the machine hosting Portal for ArcGIS. Include the fully qualified domain name of the machine, for example, `portal.domain.com`. You can also use the URL of the machine hosting Portal for ArcGIS in place of the machine name.

- `<Username>`—The username of an account that has administrative privileges to Portal for ArcGIS. This account may be the initial administrator account entered when you first set up your portal, or an account that has been assigned administrative privileges.
- `<Password>`—The password of the account that has administrative privileges to Portal for ArcGIS.
- `<ReindexPortal>`—Indicates whether to reindex the default content in the portal when registering the Web Adaptor. This option is useful if you intend to configure your deployment with a reverse proxy or load balancer. Web Adaptor registration takes less time without indexing. Once the `webContextURL` is configured, the built-in content will reference the `webContextURL`.

Example: `ConfigureWebAdaptor.exe /m portal /w https://webadaptorhost.domain.com/webadaptorname/webadaptor /g portal.domain.com /u initialadmin /p secret -r true`

After running the command, ArcGIS Web Adaptor is configured for use with the machine hosting Portal for ArcGIS. Now, you'll access your portal through ArcGIS Web Adaptor URL instead of port 7443. The URL is in the following format: `https://webadaptorhost.domain.com/webadaptorname/home`.

If you'll be configuring Portal for ArcGIS with your organization's proxy server, you must provide some information to your portal about the proxy server. For full instructions, see Integrate your portal with a reverse proxy or load balancer.

Portal

Configure multiple ArcGIS Web Adaptors

Multiple ArcGIS Web Adaptors are required when configuring a highly available portal that uses web-tier authentication. To configure multiple Web Adaptors with Portal for ArcGIS, a single endpoint must be used to access the portal. This URL must be defined in the `WebContextURL` property. Multiple Web Adaptors can then be configured with the portal following the steps below.

1. Configure the first ArcGIS Web Adaptor with your portal.
2. Add Portal for ArcGIS to your reverse proxy server. Set the `WebContextURL` property as follows:
   a. Open a web browser and sign in to the Portal Administrator Directory as an Administrator of your organization.
   The URL is formatted `https://portal.domain.com:7443/arcgis/portaladmin`.
   b. Click **System** > **Properties** > **Update Properties**.
   The Portal for ArcGIS service restarts automatically. Wait for the restart to complete before continuing.
   c. On the **Update System Properties** dialog box, insert the following JSON, substituting your reverse proxy server or DNS alias URL as seen by users outside your organization's firewall:

```
{
   "WebContextURL": "https://reverseproxy.domain.com/myorg"
}
```

   d. Click **Update Properties**.
3. Configure additional Web Adaptors.

All Web Adaptors configured with the portal are listed on the configuration summary page. Users access the portal through the reverse proxy server or DNS alias URL.

Note:
Portal for ArcGIS only supports a single organization URL.

Use Integrated Windows Authentication

You can secure access to your organization using Integrated Windows Authentication (IWA). When you use IWA, logins are managed through Microsoft Windows Active Directory. Users do not sign in and out of the organization; instead, when they open the website, they are signed in using the same accounts they used to sign in to Windows.

To use Integrated Windows Authentication, you must use ArcGIS Web Adaptor (IIS) deployed to Microsoft IIS web server. You cannot use ArcGIS Web Adaptor (Java Platform) to perform Integrated Windows Authentication. If you haven't done so already, install and configure ArcGIS Web Adaptor (IIS) with your portal.

Configure your organization to use Windows Active Directory

By default, ArcGIS Enterprise enforces HTTPS for all communication. If you have previously changed this option to allow both HTTP and HTTPS communication, you must reconfigure the portal to use HTTPS-only communication by following the steps below.

Note:
Using an Active Directory identity store, ArcGIS Enterprise supports authentication from multiple domains with a single forest but does not provide cross-forest authentication. To support organization-specific users from multiple forests, a SAML identity provider is required.

Configure the organization to use HTTPS for all communication

Complete the following steps to configure the organization to use HTTPS:

1. Sign in to the organization website as an administrator.
   The URL is in the format `https://webadaptorhost.domain.com/webadaptorname/home`.
2. Click **Organization** and click the **Settings** tab, and then click **Security** on the left side of the page.
3. Enable **Allow access to the portal through HTTPS only**.

Update your portal's identity store

Next, update your portal's identity store to use Active Directory users and groups.

1. Sign in to the Portal Administrator Directory as an administrator of your organization.
   The URL is in the format `https://webadaptorhost.domain.com/webadaptorname/portaladmin`.
2. Click **Security** > **Config** > **Update Identity Store**.
3. In the **User store configuration (in JSON format)** text box, paste your organization's Windows Active Directory user configuration information (in JSON format).
   Alternatively, you can update the following sample with user information specific to your organization:

```
{
  "type": "WINDOWS",
  "properties": {
    "userPassword": "secret",
    "isPasswordEncrypted": "false",
    "user": "mydomain\\winaccount",
    "userFullnameAttribute": "cn",
    "userEmailAttribute": "mail",
    "userGivenNameAttribute": "givenName",
```

```
    "userSurnameAttribute": "sn",
    "caseSensitive": "false"
  }
}
```

In most cases, you'll only need to alter values for the `userPassword` and `user` parameters. Although you type the password in clear text, it will be encrypted when you click **Update Configuration** (below). The account you specify for the user parameter only needs permissions to look up the email address and full name of Windows accounts on the network. If possible, specify an account whose password does not expire.

In the rare case where your Windows Active Directory is configured to be case sensitive, set the `caseSensitive` parameter to `true`.

4. To create groups in the portal that leverage the existing Active Directory groups in your identity store, paste your organization's Windows Active Directory group configuration information (in JSON format) in the **Group store configuration (in JSON format)** text box as shown below. To use the portal's built-in groups, delete any information in the text box and skip this step.
   Alternatively, you can update the following sample with group information specific to your organization.

```
{
  "type": "WINDOWS",
  "properties": {
    "isPasswordEncrypted": "false",
    "userPassword": "secret",
    "user": "mydomain\\winaccount"
  }
}
```

   In most cases, you'll only need to alter values for the `userPassword` and `user` parameters. Although you type the password in clear text, it will be encrypted when you click **Update Configuration** (below). The account you specify for the user parameter only needs permissions to look up the names of Windows groups on the network. If possible, specify an account whose password does not expire.

5. Click **Update Configuration** to save your changes.
6. If you've configured a highly available portal, restart each portal machine. See Stop and start the portal for full instructions.

Configure additional identity store parameters

Optionally, you can modify additional identity store configuration parameters using the Portal Administrator Directory. These parameters include restricting whether groups are refreshed automatically when an organization-specific user signs in to the organization, setting the membership refresh interval, and defining whether to check for multiple user name formats. See Update Identity Store for details.

Add organization-specific accounts

By default, organization-specific users can access the ArcGIS Enterprise organization. However, they can only view items that have been shared with everyone in the organization. This is because the organization-specific accounts have not been added and granted access privileges.

Add accounts to your organization using one of the following methods:

- Individually or in bulk (one at a time, in bulk from a `.csv` file, or from existing Active Directory groups)
- Command line utility
- Automatically

It's recommended that you designate at least one organization-specific account as an administrator of your portal. You can do this by choosing the Administrator role when adding the account. When you have an alternate portal administrator account, you can assign the initial administrator account to the User role or delete the account. See About the initial administrator account for more information.

Once the accounts have been added and you complete the steps below, users can sign in to the organization and access content.

Configure ArcGIS Web Adaptor to use IWA

To configure ArcGIS Web Adaptor to use IWA, complete the following steps:

1. Open Internet Information Server (IIS) Manager.
2. In the **Connections** panel, locate and expand the website hosting ArcGIS Web Adaptor.
3. Click the name of ArcGIS Web Adaptor.
   The default is `arcgis`.
4. In the **Home** panel, double-click **Authentication**.
5. Select **Anonymous Authentication** and click **Disable**.
6. Select **Windows Authentication** and click **Enable**.
7. Close Internet Information Server (IIS) Manager.

Verify portal access using IWA

To verify you can access the portal using IWA, complete the following steps:

1. Open the portal.
   The URL is in the format `https://organization.example.com/<context>/home`.
2. Verify that you are prompted for your organization-specific account credentials or automatically signed in using your organization-specific account. If you do not see this behavior, confirm that the Windows account you used to sign in to the machine was added to the portal.

Prevent users from creating their own built-in accounts

You can prevent users from creating their own built-in accounts by disabling the ability for users to create built-in accounts in the organization settings.

Use nondefault ports for the portal's ArcGIS Web Adaptor

For the vast majority of ArcGIS Enterprise users, it's appropriate to run ArcGIS Web Adaptor on the default ports 80 and 443. In some rare cases, however, an instance of Web Adaptor cannot use these default ports on the web server that hosts it. For example, the host web server may already have an application running on these ports, or port access may be restricted in a secured organization.

In situations in which you cannot configure the portal's Web Adaptor on ports 80 and 443, you can allow it to run on nondefault ports. When doing so, you must configure a reverse proxy server or load balancer and integrate it with your portal. This will allow users to access the portal through the default ports as required. The use of HTTPS should still be maintained to encrypt communication between ArcGIS Web Adaptor and Portal for ArcGIS.

The ArcGIS Web Adaptor configuration file has a property, **EnableDefaultPortValidation**, which by default enforces the use of default ports 80 and 443 when configuring ArcGIS Web Adaptor with a portal. Changing the value of this property to false bypasses this validation, allowing ArcGIS Web Adaptor to run on nondefault ports.

Configure the portal's ArcGIS Web Adaptor on nondefault ports

If the web server intended to host your portal's ArcGIS Web Adaptor has to run the software on ports other than 80 and 443, you will need to follow additional steps when setting up Web Adaptor using the installation and configuration wizards.

1. Enable HTTPS on the web server that will host the web adaptor. Note the port being used for HTTPS communication, as it will be used to access ArcGIS Web Adaptor during initial configuration with the portal.
2. Install ArcGIS Web Adaptor on the web server, using the Setup.exe installation wizard as a user with administrative privileges.
3. On the machine hosting ArcGIS Web Adaptor, browse to and open the `webadaptor.config` file in a text editor. By default, this is located in the `C:\inetpub\wwwroot\<web adaptor name>` folder.
4. In the `webadaptor.config` file, locate the property `EnableDefaultPortValidation`, which has a default value of true. Change the value to false: `<EnableDefaultPortValidation>false</EnableDefaultPortValidation>`.
5. Restart the web server.
6. Open the ArcGIS Web Adaptor configuration page in an internet browser on the HTTPS port being used by the web server using the URL format `https://webadaptorhost.domain.com:<https_port>/webadaptorname/webadaptor/portal`. If a DNS alias will be used with the portal, Web Adaptor should be configured over the alias instead, using a URL such as `https://dnsalias.domain.com:<https_port>/<webadaptorname>/webadaptor/portal`.
7. For the **Portal URL** property, type the URL of the machine hosting the Portal for ArcGIS software using the fully qualified domain name of the machine in the URL, such as `https://portal.domain.com:7443`.
8. Supply the username and password for an account that has administrative privileges to Portal for ArcGIS. Typically, you'll use the initial administrator account's login as defined when you first set up your portal. If you demoted or deleted the initial administrator account, you'll need to specify a different account with administrative access to the portal website.
9. Click **Configure**.

10. Configure the portal with your organization's reverse proxy server or load balancer so that users access the portal through the default ports. To do this, you need to provide some information to the portal about the reverse proxy or load balancer. For full instructions, see Use a reverse proxy server with Portal for ArcGIS.
11. After you have set up the reverse proxy or load balancer with your portal, refresh the ArcGIS Web Adaptor configuration page to update it.

Note:
When this workflow is complete, the value of the `EnableDefaultPortValidation` property in the `webadaptor.config` file is reset to true. You must change its value to false again and restart the web server for the change to take effect and for the web adaptor to run successfully on the nondefault port.

ArcGIS Web Adaptor is now configured for use with your ArcGIS Enterprise portal. Users will only access the portal and the ArcGIS Portal Administrator Directory through the reverse proxy sever, with the URL format `https://reverseproxy.domain.com/webadaptorname/home`, rather than through port 7443.

Silently configure the portal's ArcGIS Web Adaptor (IIS) on nondefault ports

The installation and configuration of your ArcGIS Web Adaptor (IIS) can also be done from the command line, with additional steps to run on nondefault ports.

1. Enable HTTPS on the IIS web server that will host Web Adaptor. Note the port being used for HTTPS communication, as it will be used to access ArcGIS Web Adaptor during initial configuration with the portal.
2. Install ArcGIS Web Adaptor (IIS) on the web server using the installation command line utility as a user with administrative privileges.
3. On the machine hosting ArcGIS Web Adaptor, browse to and open the `webadaptor.config` file in a text editor. By default, this is located in the `C:\inetpub\wwwroot\<web adaptor name>` folder.
4. In the `webadaptor.config` file, locate the property `EnableDefaultPortValidation`, which has a default value of true. Change the value to false: `<EnableDefaultPortValidation>false</EnableDefaultPortValidation>`.
5. Restart the IIS web server.
6. Configure ArcGIS Web Adaptor using the command line utility `ConfigureWebAdaptor.exe`, which is located in the `C:\Program Files (x86)\Common Files\ArcGIS\WebAdaptor\IIS\<current version>\Tools` folder. You'll use the syntax `ConfigureWebAdaptor.exe /m <Mode> /w <WebAdaptorURL> /g <Machine Name|URL> /u <Username> /p <Password>`. The parameters to provide are as follows:
   - `<Mode>`—The product mode in which ArcGIS Web Adaptor will be configured. Set this parameter to `portal` for use with Portal for ArcGIS.
   - `<WebAdaptorURL>`—The URL of ArcGIS Web Adaptor that you want to configure from the command line. This is the same URL that would be used if you were accessing the configuration page in a web browser. You're required to specify the HTTPS URL of ArcGIS Web Adaptor—for example, `https://webadaptorhost.domain.com:<https_port>/webadaptorname/webadaptor`. If a DNS alias will be used with the portal, Web Adaptor should be configured over the DNS alias instead, using a URL such as `https://<dnsalias.domain.com>:<https_port>/<webadaptorname>/webadaptor`.

- `<URL>`—The URL of the machine hosting Portal for ArcGIS. Include the fully qualified domain name of the machine in the URL—for example, `https://portal.domain.com:7443`.
- `<Username>`—The username of an account that has administrative privileges to Portal for ArcGIS. Typically, you'll use the initial administrator account you defined when you first set up your portal.
- `<Password>`—The password of an account that has administrative privileges to Portal for ArcGIS. Typically, you'll use the initial administrator account you defined when you first set up your portal.

Example command

```
ConfigureWebAdaptor.exe /m portal /w https://webadaptorhost.domain.com:https_port/
webadaptorname/webadaptor /g portal.domain.com /u initialadmin /p secret123
```

7. Configure the portal with your organization's reverse proxy server or load balancer so that users access the portal through the default ports. To do this, you need to provide some information to the portal about the reverse proxy or load balancer. For full instructions, see Use a reverse proxy server with Portal for ArcGIS.

   Note:
   When this workflow is complete, the value of the `EnableDefaultPortValidation` property in the `webadaptor.config` file is reset to true. You must change its value to false again and restart the web server for the change to take effect and for the web adaptor to run successfully on the nondefault port.

ArcGIS Web Adaptor is now configured for use with your ArcGIS Enterprise portal. Users will only access the portal and the ArcGIS Portal Administrator Directory through the reverse proxy sever, with the URL format `https://reverseproxy.domain.com/webadaptorname/home`, rather than through port 7443.

Integrate your portal with a reverse proxy or load balancer

A reverse proxy server or load balancer is an appliance that is typically deployed within a perimeter network (also known as a demilitarized zone [DMZ] or screened subnet) that handles requests from the internet and forwards them to the machines in your internal network. The forwarding of requests on behalf of the reverse proxy server masks the identity of the machines behind your organization's firewall, thus protecting internal machines from being attacked directly by internet users. Additional security functions can be implemented in the reverse proxy server to further protect your internal network from outside users.

If your reverse proxy server or load balancer supports a health check function, you can use the Portal for ArcGIS heath check endpoint to determine whether the portal is available to receive requests. This is useful to quickly determine whether there's a software or hardware failure in the site. For more information, see Health Check.

⚠ Caution:

The configuration detailed in this topic must be performed before federating any ArcGIS Server site with your portal. To add a DNS alias or reverse proxy after a server site has been federated, see Update the organization URL.

Load balancer types

Reverse proxies are sometimes referred to as load balancers but typically offer more functionality than just distributing incoming messages across back-end targets. Many reverse proxy server implementations can operate in either capacity described below, depending on the configuration.

Load balancing actions are often differentiated by the layer of the Open Systems Interconnection (OSI) model they operate at. When working to integrate an existing load balancer technology, it is important to identify which type is being implemented, as it affects the overall architecture of the deployment.

Layer 3/4 load balancers are sometimes referred to as network or packet-level load balancers. These load balancers typically do not inspect the incoming traffic and instead route the incoming TCP/UDP packets to the back-end targets. Newer implementations allow for SSL termination on the load balancer, but the client SSL session is typically established with the back-end target server or servers.

Layer 7 load balancers are sometimes referred to as an application or application-aware load balancers. These load balancers inspect the incoming messages and can make routing decisions based on several factors, as well as modify the contents of those messages before proxying them to the back-end target or targets. Layer 7 load balancers using HTTPS will terminate the SSL communication with the client and re-encrypt that traffic before proxying the requests to the back-end HTTPS targets.

Prepare a reverse proxy server or load balancer

Before adding Portal for ArcGIS to your organization's reverse proxy server, you must complete the following:

- Configure HTTPS (HTTP and HTTPS or HTTPS-only) on the reverse proxy server. Portal for ArcGIS uses HTTPS for communication by default. Consult the product documentation for your proxy server to learn how to set up HTTPS.

Note:
Portal for ArcGIS does not support SSL offloading through a reverse proxy server/load balancer. Therefore, if your configuration uses a reverse proxy server, it must forward traffic to either the ArcGIS Web Adaptor or directly to Portal for ArcGIS over HTTPS.

Note:
You must ensure that the reverse proxy server's context name only goes one URL level deep. For example, you can have a reverse proxy URL such as `https://proxy.domain.com/enterprise`, but you cannot have a reverse proxy URL such as `https://proxy.domain.com/myorg/enterprise`.

Verify that the proxy server supports `gzip` encoding and is configured to allow the `Accept-Encoding` header. This header allows HTTP 1.1 responses to be compressed using `gzip` encoding. For example, if the header is allowed, a request to load Map Viewer Classic will return a compressed response of approximately 1.4 MB to the browser. If the header is not allowed or ignored, the request will return an uncompressed response of approximately 6.8 MB to the browser. If your network speed is slow, it may take a long time for Map Viewer Classic to load if responses are not compressed. Esri recommends that you allow this header as part of your reverse proxy server configuration.

Layer 3/4 load balancer

The load balancer should listen on the default HTTPS port and pass traffic to either the ArcGIS Web Adaptor or directly to the Portal for ArcGIS machine or machines on port 7443. When terminating client SSL sessions on the Portal for ArcGIS internal web server, ensure that the SSL certificate presented by that web server is valid for both the DNS alias and the FQDN of the machine or machines in the site to avoid certificate trust issues. This can typically be achieved using subject alternative names for the SSL certificate.

Note:
When not using the ArcGIS Web Adaptor, the default context (`/arcgis`) must be used for the site. When integrating multiple Portal for ArcGIS and ArcGIS Server sites on the same layer 3/4 load balancer, a unique DNS record should be used for each site and Server Name Indication (SNI) used to route traffic to the appropriate back-end targets.

Layer 7 load balancer

In the load balancer configuration, an `X-Forwarded-Host` header should be set to the host name of the DNS alias of the site. Portal for ArcGIS expects to see this property set in the header sent by the reverse proxy server and will return requests that match the reverse proxy server's URL. If you aren't using ArcGIS Web Adaptor with your portal, confirm that the `Host` header set by the load balancer matches the host name of the machine where Portal for ArcGIS is installed.

Tip:
You can use the machines endpoint in the Portal Administrator Directory to view the host name of the machine running Portal for ArcGIS.

For example, a request to the ArcGIS Portal Directory (`https://dnsalias.domain.com/arcgis/sharing/rest`) will be returned to the client as the same URL. If the property is not set, Portal for ArcGIS may return the URL of the

internal machine where the request was directed (for example, `https://portal.domain.com/arcgis/sharing/rest` instead of `https://dnsalias.domain.com/arcgis/sharing/rest`). This is problematic, as clients will not be able to access this URL (commonly noted as a browser 404 error). Also, this gives the client access to some information about the internal machine.

Along with the `X-Forwarded-Host` header, your load balancer must be able to direct redirects (HTTP response codes 301 or 302). All `Location` headers should be rewritten on the load balancer to ensure that the fully qualified domain name (FQDN) and context of the response match the portal's `WebContextURL` value.

Add a portal

The following sections describe how to add Portal for ArcGIS to your organization's reverse proxy server.

Layer 3/4 load balancer: Add ArcGIS Web Adaptor or Portal for ArcGIS machines to the load balancer configuration

Since the proxying of traffic to the back-end targets will occur over TCP, the machine or machines for each site should be added to the load balancer configuration. If using the ArcGIS Web Adaptor, the back-end targets should point to the port of the web server or servers (typically 443 or 8443) hosting the web adaptor or adaptors. When proxying traffic directly to Portal for ArcGIS, the back-end targets should point to port 7443 on each machine in the site.

Layer 7 load balancer: Add ArcGIS Web Adaptor or Portal for ArcGIS machines to proxy server directives

After configuring ArcGIS Web Adaptor with Portal for ArcGIS, ArcGIS Web Adaptor can be used with your organization's reverse proxy server by adding the components directly to proxy server directives. For example, if you're using Apache as a reverse proxy, you need to add ArcGIS Web Adaptor to the ProxyPass directives in the Apache web server configuration file `httpd.conf`:

```
ProxyPass /webadaptorname https://webadaptorhost.domain.com/webadaptorname
ProxyPassReverse /webadaptorname https://webadaptorhost.domain.com/webadaptorname
```

The ProxyPass directives must match the name designated for ArcGIS Web Adaptor (`/webadaptorname` in the sample above). When not using the ArcGIS Web Adaptor in front of Portal for ArcGIS, add the following directives where `/context` is the chosen URL top-level path:

```
ProxyPass /context https://portal.domain.com:7443/arcgis
ProxyPassReverse /context https://portal.domain.com:7443/arcgis
```

Configure a portal to use a reverse proxy or load balancer

The following sections describe how to configure your portal to use the reverse proxy server URL and the administrative tasks that must be redone once the URL is configured.

Set the WebContextURL property

The portal's `WebContextURL` property helps it construct the correct URLs on all resources it sends to the end user. Do the following to change the `WebContextURL`:

1. Open a web browser and sign in to the Portal Administrator Directory as a member of the default Administrator role in your organization. The URL is formatted `https://portal.domain.com:7443/arcgis/portaladmin`.
2. Click **System** > **Properties** > **Update Properties**.
3. On the **Update System Properties** dialog box, insert the following JSON, substituting your own reverse proxy server or DNS alias URL as seen by users outside your organization's firewall.

```
{
   "WebContextURL": "https://dnsalias.domain.com/portal"
}
```

Note:
Portal for ArcGIS only supports a single organization URL.

Note:
You cannot use a nonstandard port (that is, a port other than 443) when setting the `WebContextURL` property.

4. Click **Update Properties**.

Redo administrative tasks

Once you've configured the reverse proxy server with your portal, you'll now access your portal through the reverse proxy server URL instead of the ArcGIS Web Adaptor URL. Anything you access in the portal or the Portal Administrator Directory will return the reverse proxy server URL.

The following administrative tasks should be redone using the reverse proxy server URL:

- Federate an ArcGIS Server site with your portal
- Configure utility services

If you've previously added secured services as items in your portal, you'll need to delete the original items and add them again. This is because the original items use the ArcGIS Web Adaptor URL instead of the reverse proxy server URL. For instructions, see Connect to secure services.

After configuring your reverse proxy server with the portal, you may need to adjust its settings. For example, if operations or requests within your deployment fail with an error indicating the connection timed out, the problem may be that your reverse proxy server's time-out value is too short. To fix this error, consider increasing the time-out value to allow long-running requests, such as federating a server, to complete.

Configure the display language for ArcGIS Web Adaptor

The ArcGIS Web Adaptor setup includes prelocalized versions of the Web Adaptor for several languages. These prelocalized languages are as follows:

- Arabic
- Simplified Chinese
- French
- German
- Italian
- Japanese
- Brazilian Portuguese
- Russian
- Spanish
- Turkish

Once the setup completes, the Web Adaptor configuration page opens automatically. If your browser is already configured to display one of the above languages, the Web Adaptor application automatically opens in that language.

To view the Web Adaptor in a different language, you will need to configure your browser to display the language. For instructions, consult your browser's documentation.

Enable HTTPS on your web server

To secure network communication between ArcGIS Web Adaptor and a server or portal, use the HTTPS protocol.

The HTTPS protocol is a standard security technology used to establish an encrypted link between a web server and a web client. HTTPS facilitates secure network communication by identifying and authenticating the server as well as ensuring the privacy and integrity of all transmitted data. Since HTTPS 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.

You must obtain a server certificate and bind it to the website that hosts ArcGIS Web Adaptor. Each web server has its own procedure for loading a certificate and binding it to a website.

Also ensure that your web server is set to ignore client certificates to correctly access secure services over HTTPS.

Create or obtain a server certificate

To create an HTTPS connection between ArcGIS Web Adaptor and a server or portal, the web server requires a server certificate. A 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 the server or portal. A certificate must be created by the owner of the website and digitally signed. There are three types of certificates—CA-signed, domain, and self-signed—which are explained below.

CA-signed certificates

Certificates signed by an independent certificate authority (CA) assure clients that the identity of the website has been verified. A certificate authority is usually a trusted third party that can attest to the authenticity of a website. If a website is trustworthy, the certificate authority adds its own digital signature to that website's self-signed certificate. This assures web clients that the website's identity has been verified.

Use CA-signed certificates for production systems, particularly if your server or portal is going to be accessed from users outside your organization.

When you use a certificate issued by a well-known certificate authority, secure communication between the server and the web client occurs automatically with no special action required by the organization administrator or clients that access it. There is no unexpected behavior or warning message displayed in the web browser, because the website has been verified by the certificate authority.

Domain certificates

If your server or portal is located behind your firewall and you are unable to use a CA-signed certificate, use a domain certificate. 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, because certificates can be generated within your organization for trusted internal use.

Users within your domain will not experience any of the unexpected behavior or warning messages typically associated with a self-signed certificate, because the website has been verified by the domain certificate. However, domain certificates are not validated by an external certificate authority, which means users visiting your site from outside your domain will not be able to 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 they are actually communicating with a malicious party and be turned away from your site.

If you are using IIS and need to create a domain certificate, see Create a domain certificate, which provides a script to run on your machine that will create the appropriate certificate and bind it to HTTPS port 443.

Self-signed certificates

A certificate signed only by the owner of the website is called a self-signed certificate. Self-signed certificates are commonly used on websites that are only available to users on the organization's internal (LAN) network. If you communicate with a website outside your own network that uses a self-signed certificate, you have no way to verify that the site issuing the certificate really represents the party it claims to represent. You could actually be communicating with a malicious party, putting your information at risk.

Creating a self-signed certificate should not be considered a valid option for a production environment, as it will lead to unexpected results and a poor experience for all users of the organization.

When you first set up the organization, you can use a self-signed certificate to do some initial testing to help you quickly verify that your configuration was successful. However, if you use a self-signed certificate, you will experience the following when testing:

- You will receive warnings about the site being untrusted when you access the organization from a web browser or desktop client.
  When a web browser encounters a self-signed certificate, it typically displays a warning and asks you to confirm that you want to proceed to the site. Many browsers display warning icons or a red color in the address bar as long as you use the self-signed certificate. Expect to see these types of warnings if you configure the organization with a self-signed certificate.
- You cannot open a federated service in a map viewer, add a secured service item to the organization, sign in to ArcGIS Server Manager on a federated server, or connect to the organization from ArcGIS for Office.
  To allow you to sign in from ArcGIS for Office, install the self-signed certificate to the **Trusted Root Certification Authorities** certificate store on the machine running ArcGIS for Office.
- You may experience unexpected behavior when printing hosted services and accessing the organization from client applications.

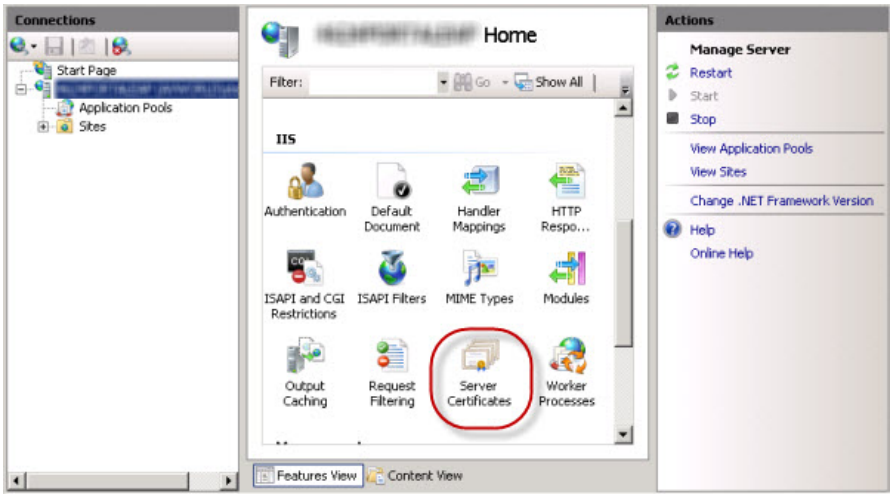
⚠ Caution:

The above list of issues you will experience when using a self-signed certificate is not exhaustive. It is recommended that you use a domain certificate or CA-signed certificate to fully test and deploy an ArcGIS Enterprise organization.

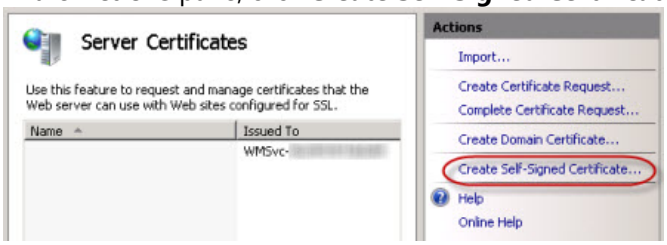
Create a self-signed certificate in IIS

To create a self-signed certificate in IIS Manager, complete the following steps:

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**.



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

The final step is to bind the self-signed certificate to HTTPS port 443.

Bind the certificate to the website

You must bind your certificate to the website hosting ArcGIS Web Adaptor. Binding refers to the process of configuring the certificate to use port 443 on the website.

Note:
The script in the Create a domain certificate topic will bind your certificate for you.

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.

Test your site

After obtaining or creating a certificate that is bound to port 443, configure ArcGIS Web Adaptor for use. You must access the ArcGIS Web Adaptor configuration page using an HTTPS URL such as `https://webadaptorhost.domain.com/webadaptorname/webadaptor`.

Note:
If a host name is specified in the HTTPS site binding, it must match the host name in the URL used to access the ArcGIS Web Adaptor configuration page.

After you configure ArcGIS Web Adaptor, test that HTTPS is working properly by making an HTTPS request to the organization, for example, `https://webadaptorhost.domain.com/webadaptorname/home`, or to ArcGIS Server Manager, for example, `https://webadaptorhost.domain.com/webadaptorname/manager`. If you are testing with a self-signed certificate, dismiss the browser warnings about untrusted connections. This usually involves adding an exception to your browser so that it will allow you to communicate with the site that is using a self-signed certificate.

Unregister

Unregister ArcGIS Web Adaptor

To modify your server site or portal to use a different ArcGIS Web Adaptor, for example, if you want to change the name of the Web Adaptor or the name of the machine hosting ArcGIS Web Adaptor, you first must unregister ArcGIS Web Adaptor with your server site or portal.

Unregister with a server site

You'll use the ArcGIS Server Administrator Directory to unregister ArcGIS Web Adaptor with your server site. You can only unregister through the ArcGIS Server Administrator Directory; the unregister functionality is not available from the ArcGIS Web Adaptor configuration page.

To unregister ArcGIS Web Adaptor, complete the following steps:

1. Open the ArcGIS Server Administrator Directory and sign in as an administrator of your site. The URL is formatted `https://gisserver.domain.com:6443/arcgis/admin`.
2. Click **System** > **Web Adaptors**.
3. On the **Web Adaptors** page, click the string representing ArcGIS Web Adaptor.
4. On the **Web Adaptor** page, ensure that the `URL` listed refers to the Web Adaptor you want to unregister. Click **Unregister**.
5. On the **Unregister Web Adaptor** page, click **Unregister Web Adaptor**. ArcGIS Web Adaptor is unregistered with your ArcGIS Server site.
6. Configure the new ArcGIS Web Adaptor with your ArcGIS Server site. For full instructions, see Configure ArcGIS Web Adaptor with a server site.

Unregister with portal

You'll use the Portal Administrator Directory to unregister ArcGIS Web Adaptor with your portal. You can only unregister through the Portal Administrator Directory; the unregister functionality is not available from the ArcGIS Web Adaptor configuration page or the portal.

⚠ Caution:

Although you can modify a portal's Web Adaptor by registering a new one, be aware that doing so may also impact user content within the portal (for example, map notes or other items).

To unregister ArcGIS Web Adaptor, complete the following steps:

1. Open the Portal Administrator Directory and sign in as an Administrator of your organization. The URL is formatted `https://portal.domain.com:7443/arcgis/portaladmin`.
2. Click **System** and click **Web Adaptors**.
3. On the **Web Adaptors** page, click the name of the machine hosting ArcGIS Web Adaptor.
4. On the **Web Adaptor: <machine name>** page, click **Unregister Web Adaptor**.
5. On the **Unregister Web Adaptor** page, click **Unregister Web Adaptor**. ArcGIS Web Adaptor is unregistered with your portal.

6. Configure the new ArcGIS Web Adaptor with your portal. For full instructions, see Configure ArcGIS Web Adaptor.

Note:
If your intention is to completely remove the previous ArcGIS Web Adaptor from your server site or portal, it is recommended that you uninstall ArcGIS Web Adaptor after following the steps above. Uninstalling deletes all ArcGIS Web Adaptor configuration details from the server site and portal and blocks members and clients from accessing the server site and portal through the unregistered ArcGIS Web Adaptor URL. For full instructions, see Uninstall ArcGIS Web Adaptor.

Uninstall

Uninstall ArcGIS Web Adaptor

When you uninstall ArcGIS Web Adaptor, it is unregistered with your server site and portal, and client applications cannot communicate with them. To reestablish this communication in the future, reinstall ArcGIS Web Adaptor and use the configuration page to reconfigure the Web Adaptor with your server site or portal.

Uninstall the Web Adaptor

To uninstall ArcGIS Web Adaptor, complete the following steps:

If you have multiple Web Adaptors installed, you must uninstall each Web Adaptor individually.

Note:
Each Web Adaptor installation creates an application pool with the default naming convention of `ArcGISWebAdaptorAppPool<web adaptor name>`. When you uninstall a Web Adaptor, its application pool will remain and preserve any advanced settings you configured on it. The pool is left for your convenience if you reinstall or upgrade the Web Adaptor.

Uninstall the Web Adaptor silently

You can uninstall Web Adaptor silently using the following commands depending on the version of Web Adaptor you are running.

Uninstall the Web Adaptor from the command line

To uninstall ArcGIS 11.4 Web Adaptor (IIS) silently, run this command from the command line:

```
msiexec /x {A1EEF9DE-E054-461A-BAB8-EE7FF8C8C6E6} /qb
```

To uninstall ArcGIS 11.3 Web Adaptor (IIS) silently, run this command from the command line:

```
msiexec /x {6D1FDF29-5DAB-4816-9CDE-15CF663E3BDD} /qb
```

To uninstall ArcGIS 11.2 Web Adaptor (IIS) silently, run this command from the command line:

```
msiexec /x {3F2DF3A0-0EB7-4DED-BA7F-A33B7B106252} /qb
```

To uninstall ArcGIS 11.1 Web Adaptor (IIS) silently, run this command from the command line:

```
msiexec /x {E2F2DE02-86AC-42EE-B90D-544206717C9E} /qb
```

To uninstall ArcGIS 11.0 Web Adaptor (IIS) silently, run this command from the command line:

```
msiexec /x {FCC01D4A-1159-41FC-BDB4-4B4E05B3436F} /qb
```

To uninstall ArcGIS 10.9.1 Web Adaptor (IIS) silently, run this command from the command line:

```
msiexec /x {BC399DA9-62A6-4978-9B75-32F46D3737F7} /qb
```

To uninstall ArcGIS 10.9 Web Adaptor (IIS) silently, run this command from the command line:

```
msiexec /x {1FD4759C-6858-42AD-A1DC-6DA0C3B1D28C} /qb
```

To uninstall ArcGIS 10.8.1 Web Adaptor (IIS) silently, run this command from the command line:

```
msiexec /x {9695EF78-A2A8-4383-AFBF-627C55FE31DC} /qb
```

To uninstall ArcGIS 10.8 Web Adaptor (IIS) silently, run this command from the command line:

```
msiexec /x {D6059C27-7199-4A94-806B-6C40EFD02828} /qb
```

To uninstall ArcGIS 10.7.1 Web Adaptor (IIS) silently, run this command from the command line:

```
msiexec /x {5ECEF84F-592C-47D1-B7C5-9F3D7E2AB7CE} /qb
```

To uninstall ArcGIS 10.7 Web Adaptor (IIS) silently, run this command from the command line:

```
msiexec /x {F343B520-F769-4D93-86D2-663168AC6975} /qb
```

To uninstall ArcGIS 10.6.1 Web Adaptor (IIS) silently, run this command from the command line:

```
msiexec /x {1B4E7470-72F4-4169-92B9-EF1BDF8AE4AF} /qb
```

To uninstall ArcGIS 10.6 Web Adaptor (IIS) silently, run this command from the command line:

```
msiexec /x {4FB9D475-9A23-478D-B9F7-05EBA2073FC7} /qb
```

To uninstall ArcGIS 10.5.1 Web Adaptor (IIS) silently, run this command from the command line:

```
msiexec /x {0A9DA130-E764-485F-8C1A-AD78B04AA7A4} /qb
```

To uninstall ArcGIS 10.5 Web Adaptor (IIS) silently, run this command from the command line:

```
msiexec /x {87B4BD93-A5E5-469E-9224-8A289C6B2F10} /qb
```

To uninstall ArcGIS 10.4.1 Web Adaptor (IIS) silently, run this command from the command line:

```
msiexec /x {F53FEE2B-54DD-4A6F-8545-6865F4FBF6DC} /qb
```

To uninstall ArcGIS 10.4 Web Adaptor (IIS) silently, run this command from the command line:

```
msiexec /x {B83D9E06-B57C-4B26-BF7A-004BE10AB2D5} /qb
```

To uninstall ArcGIS 10.3.1 Web Adaptor (IIS) silently, run this command from the command line:

```
msiexec /x {10A57135-2051-41AE-B2D3-0B10470CDB9B} /qb
```

To uninstall ArcGIS 10.3 Web Adaptor (IIS) silently, run this command from the command line:

```
msiexec /x {B52143C3-3085-4976-9795-ED134AEA0099} /qb
```

To uninstall ArcGIS 10.2.2 Web Adaptor (IIS) silently, run this command from the command line:

```
msiexec /x {5D50CC1F-63E9-400E-A62C-EEAD948618EC} /qb
```

To uninstall ArcGIS 10.2.1 Web Adaptor (IIS) silently, run this command from the command line:

```
msiexec /x {18C45289-5BB0-448E-813D-34D31DF68104} /qb
```

To uninstall ArcGIS 10.2 Web Adaptor (IIS) silently, run this command from the command line:

```
msiexec /x {1803FE22-6164-4DC4-B14E-EBD4148A8429} /qb
```

To uninstall ArcGIS 10.1 SP1 Web Adaptor (IIS) silently, run this command from the command line:

```
msiexec /x {0EAADB27-2BD7-4ED5-92E2-532F775BCCED} /qb
```

To uninstall ArcGIS 10.1 Web Adaptor (IIS) silently, run this command from the command line:

```
msiexec /x {11CCA428-4679-4D79-ADC0-A13F43290ACF} /qb
```

Uninstall additional Web Adaptors silently

To uninstall additional Web Adaptors silently, replace the above product code with the product code of the Web Adaptor to be uninstalled. Product codes for the Web Adaptor are listed below. The product codes are listed in the same order as the Web Adaptors installed on your system; for example, the first Web Adaptor created is the first product code listed below.

11.4

- {37A3BCC2-9A76-4D87-AC2A-993582ECF891}
- {51D04E2F-9196-43DC-950E-173EED1290D4}
- {5C9B7DA6-01DC-425E-BA94-427DDE199959}
- {D7BDB359-3BCE-4153-A570-7948C6097FF4}
- {6827D461-6440-4C74-9F83-7D7BF9F57F93}
- {47AA6E11-0D24-47C1-99E6-9C0F4B318FFF}
- {BC0F76E2-9583-4E66-8CA6-FD343F329B31}
- {A99CDDFA-B1A0-4924-A659-61E4E1BBCB83}
- {B00814E3-1EBC-41AC-A632-8D0494885AE2}
- {BECA4DB4-7080-4504-96F9-861884FB3FBA}
- {356E98BB-0E15-4FBD-9AAE-81FC15213B7F}
- {51875907-8D8B-46B4-A694-519FDB8F9907}
- {E85450CF-E7A9-4281-9C2A-3CC8CDA952A9}
- {703152AA-069F-46AB-9080-404463A073E4}
- {E514597B-CDE7-460D-9FD1-04B9B786DB23}
- {0ED2A3FD-4B6B-4006-B10C-9F45F1D90CFC}
- {75A1143F-82EC-42D1-9081-30901CF73614}
- {D86A7B19-67FA-4EA3-86EE-A210F618B274}
- {AF997D9E-270C-4CB9-88B5-EFF0FE3F930B}
- {718DE748-4F62-4A16-862D-670564FF79ED}
- {9AD6E83D-DC7B-47FD-AC52-3B3DD1FDA07D}
- {000B3034-FA23-46E6-A5A5-FD13EB302F5F}
- {C79C1A34-2364-4DCB-BA6B-BA6D22A919D9}
- {2479729B-3FFA-41C3-A2C6-4D992782A243}
- {C0FA8EE3-5230-400B-B80E-2F6950D606A4}
- {66FD8F46-B3CF-4C1F-9B04-B5894FD41A75}
- {C87ACC53-FC3D-4527-AB2C-D5FBB41A1F34}
- {8976EB40-82E0-4583-A255-EEB30EC86161}

- {743EDE64-11F6-46BF-85E7-A64ADE4CA7F0}
- {7C841837-FDDE-493E-BCC1-2E8514AFE146}
- {ABFAD895-1F0D-4D50-AFF2-DAD9303FA2A0}
- {CBE7BA7E-0A46-4AEF-AC5D-E7A7C7986701}
- {B61D5494-BD5F-4583-9564-AEA33C2DA6E3}
- {C190AA6A-46A8-4068-840C-125FA21918BB}
- {C5174467-893B-4D38-ABD9-1FA9CB2FB1AD}
- {42C04A4F-7E12-4E37-8143-C8CDBD7E1DE4}
- {22732FD0-C451-4284-B35A-D040B5A16FEC}
- {46FA248B-A29F-42CA-AC41-201F675BD9F3}
- {ACD97940-DA22-4761-8962-8E531EE0EC0A}
- {98671F19-A3DC-4310-970A-E74C8950E3A5}
- {478AABC4-FCD7-4956-9421-F2AE705245DF}
- {E64B3CED-3FFE-4B21-AFD6-CBC400707329}
- {15BAD677-D80E-48A6-84D9-ED1F1C002816}
- {C630E05F-7208-447C-86CE-FEF27E2DDE1C}
- {D721DFD5-9DF9-4F8A-BD45-D61E2D719F91}
- {FCEF4ECC-D7A8-4192-8E47-7A22221A70D2}
- {57244572-CDD1-4079-B5E7-526CB411109D}
- {4A38BCCB-3CBB-47CC-BF03-F4B6178280E6}
- {9608A7E2-D821-4CFF-A8EA-9D9C27A6585C}
- {EB8847FE-9A77-4933-8D0E-874F0F7399C2}

11.3

- {9DA66832-790E-4A08-90D8-3305D2C4F2A2}
- {E3DF9FCC-2078-4816-B195-EE30D1C74086}
- {87C9FEB8-73A7-436A-861E-74C3A3D7805B}
- {3D881639-2227-4E9E-9380-C55991C92D3F}
- {7FB27776-2537-456E-BF4D-6E90B1050E16}
- {013D126B-0E28-4070-B57D-1C7128511E09}
- {F2D44D27-A3EB-4892-A260-7FF8D90AE3ED}
- {AC6ECF31-E1D9-4A08-B7E2-9BF4EA138BFD}
- {D2B275D6-F12D-4AB1-B0E3-7E72E42309F6}
- {8AC70A2E-6E62-47C1-8DAE-63481CF7E570}
- {1C94E9C9-8FE0-4647-B679-1C99721D8E5A}

- {36E80F76-A84A-4C2E-9087-F6B6FC60B8F0}
- {442DAF3B-289D-45AC-855D-CD1AF79AD046}
- {2F5AE3DF-9918-4BB3-ADAC-D6A02681E8C5}
- {B2775E94-5176-42F2-9161-C52EFD7BFFD5}
- {614151D0-B8AE-4D85-83B3-70AFA3961E1A}
- {C9DD2778-546E-4E27-AEC1-C51BCA198172}
- {BF09767E-0CB7-4DAF-9ABE-400EE03CB9D6}
- {72587C29-AB2F-42F4-AB8B-A54325CA7A71}
- {1FA8B39E-07B5-4EAE-BABD-1B121131FEB2}
- {CFE37EEE-9148-4A1D-904C-05EBD63345DA}
- {2C774E47-A888-4F31-8425-781628500874}
- {2F923C43-6CF5-44B7-A21F-AFDE607C417D}
- {112A5C83-2207-4B94-9829-7433E8B82A7E}
- {2EE1C0D5-4631-47B3-B77E-CA5062732BA4}
- {0D125A07-D3FE-4388-870A-0CAC77280683}
- {0155E162-901D-41DF-A260-AA8E6C833D9A}
- {20F7ABC9-CC0F-47DD-B3FB-AA3D70140F1D}
- {407A2E2C-F8D7-4900-9F68-442774F9DD9E}
- {E86311FF-9990-48CD-A04C-B3404FA5B395}
- {2CF5D03B-AD63-4BB4-A3C6-7FD1D595F810}
- {8F2FCF64-7190-45B8-8DC4-4DAB5ED83425}
- {8673E73F-83A3-4C29-8BAB-516394436BC0}
- {3394AAA1-9432-4A9B-B611-A5A9D8B5F789}
- {E953DD69-8BA7-4653-AFEE-622E42B77AE1}
- {457B6C44-9A92-4F31-A071-359E8F000A70}
- {44FE2519-ABD7-4557-BD59-A1717928C539}
- {0B7987AB-85E2-480C-B245-D4BECE95E8EB}
- {D5985070-E78C-4B9A-8075-929EE77AC4B0}
- {F5D192C7-104E-4524-9DE0-36B34216B999}
- {65B4454A-4C0E-4DF0-BC32-18552466B306}
- {8AE7199B-D50C-48AD-BB82-1C289443C4C1}
- {0FDDEF60-6FA8-4DA7-9E05-A8CC4A1C1C9B}
- {033430AD-8978-459F-8CDA-2FD49B67752B}
- {85BD45E5-25CB-4FED-BBAE-2AA34286E556}

- {E46DBEB4-628D-4DC6-BC13-32F42B6EF5F6}
- {D976C4CB-B3B6-43C9-87E9-F27E2BE826AE}
- {91869554-E02E-4AB1-956F-AC1B54AF2158}
- {A88F3595-7DC9-455C-813D-66C6C687A9D1}
- {44CAC131-3CA6-44A1-AFBD-3E083365D5F0}

11.2

- {CAB137C6-98F0-4569-9484-719632E81CF6}
- {899B1E0C-4675-4E52-BFBC-4FFF69DBAF8E}
- {4DE50EC3-6CB8-4EE5-B634-1AE53499F6D4}
- {A0ABE60F-0E01-4D84-A08B-EE34EFF96584}
- {066DEFEE-E71D-42F5-859E-225825268720}
- {53A32CFB-A012-4546-9A7F-09E489442A0A}
- {34AD67CC-2BA2-4EAA-B2A5-777036B0104E}
- {08CF83CB-FC1E-4F7C-8960-96C7D8A0B733}
- {D3803AB3-1C2F-4AD9-80EB-901685912599}
- {6671DEEE-CEE8-4FBD-B2DC-430F268225AF}
- {F92DED6B-B2B4-4E4F-A65B-ACE4973C0A9A}
- {6EDAB5E0-FD24-4427-82BE-134DB0FF9D37}
- {EFA6EC36-1A4B-481D-8A2E-C3B9098179F1}
- {CB1CA2A3-D209-462D-947A-AE5DCAACDC54}
- {D8D5A0CB-3F4F-4863-8EB2-6D24C0D0F093}
- {AE62DBD4-44A1-4E67-BAAC-4A5B2AC8830E}
- {8C323710-4026-4A8C-8DCF-5EFF6EE3F39B}
- {3232DC1F-00C3-4247-B354-FA022F1504C0}
- {3D0E95E1-BDA7-47BF-A967-3E889D3C79D9}
- {151724F6-2228-4A46-B710-88A6BAFEDCB4}
- {42093FF4-084C-4CFF-8771-9FACCFCCC885}
- {B8B8D0E8-C909-4AF3-A6C3-57B65B33DBD5}
- {EFC9E132-8203-4787-B656-35F6DAA8BA83}
- {B66B0665-9A60-4A7D-968F-FFFEEF432D6A}
- {659E9FFE-E066-477E-ACD2-24571B903DB8}
- {9FE56745-E9B0-4A13-A8D3-CD5A6B24549B}
- {33EDE71E-8D2C-4E1D-A9D8-7E7168DE378F}
- {31437F3D-D518-4458-84F2-095496C2B070}

- {8E3AABF7-06D2-41C9-B334-B7DA0D2BCEB6}
- {A93BDC2A-0B66-4C2E-B3FD-084F129DA944}
- {37657603-B344-434F-A199-CC2438DF6E66}
- {62BEE4A7-9A48-497E-B135-1D6C8015EF0F}
- {65CEF052-CA98-4256-9056-B0D773A101DF}
- {3394AAA1-9432-4A9B-B611-A5A9D8B5F789}
- {337A03BB-344D-4E55-A6F1-009707E431A7}
- {6D2B7A3A-B83A-4184-AD06-86124AB7C31E}
- {2BE42936-94CF-4903-9C24-E2D250C4CF29}
- {42DEFD61-19AB-4AEC-AB7F-53B6F8B5C5E5}
- {0C55673B-E0F1-4934-9CA3-5F0518D1D05C}
- {02BEB2CC-577D-4764-ADE7-FB5F26449246}
- {AC39F197-B738-4E66-B7F2-F84E6F018673}
- {2666B636-E834-4CF3-AF87-8CB0233C1E87}
- {EEFABA33-7E3A-4E50-8829-7A4D2DEFF1C4}
- {0E9F50F7-C3BE-47C0-AA6E-661F3166BD11}
- {E248E952-E8F7-43B4-9BE5-5490305A0E21}
- {C7663D45-3D02-43CA-ABA2-CF5888487A8B}
- {EF41B351-9F40-413D-BE90-19B8C52A0E36}
- {38575D5A-2C45-4E66-B008-E227C46BEB71}
- {74ED54F0-9495-441F-9EB8-30047F3E0956}
- {96F6657A-4295-42BD-8751-280AADBA3E84}

11.1

- {A4082192-FA68-4150-8EB7-ACCF12F634C4}
- {7A467DB0-DE13-40A6-9213-7F336C28456E}
- {4C3342AC-45D7-417A-8DFC-54604649A97C}
- {8B8A2734-BEC8-476F-B99D-3E13C9F0BAA8}
- {62FCD139-C853-4944-809C-967835510785}
- {65E3E662-67D0-4608-A522-5C10C59CA2DC}
- {614E9ADA-CE81-44DB-BB04-C2A0E02C6458}
- {83F624D7-ED01-48A1-8E3A-6CEDD4CDEBF2}
- {F2D7F6E9-DB46-4B39-994A-FCA32EA5CF15}
- {4A6C5251-C1E3-4ADD-A442-773C110701E6}
- {E09C05F7-8E85-4402-A1A8-C53B6926D0CD}

- {5E664C01-5D5B-4CAA-A03F-145B69FFF6EA}
- {DC9156D0-13CE-4981-B0EB-3C55B1997632}
- {3A5F0EB2-B721-4E5F-9576-47F02A5F77F6}
- {09AFD321-FD2A-4D22-AEEB-C858E0691386}
- {B14810D6-F62D-4581-BBDB-80B739A504DB}
- {8A2CE94A-6340-4AA4-AE83-62A4FA8C5AC2}
- {90E8E4D4-DDE0-4743-AA83-CBDD1827F307}
- {7C10E922-35BD-4A1B-87B0-6346AF5D1462}
- {1EA1484D-962A-4923-9CD1-BC074031E25F}

11.0

- {920A1EFA-D4DC-4C6D-895A-93FDD1EDE394}
- {258F0D35-985B-4104-BCC4-B8F9A4BB89B4}
- {7B128234-C3D8-4274-917F-BC0BCE90887F}
- {CD160BB2-3AA9-42CE-8BA0-4BFF906E81DE}
- {BBBD3910-2CBB-4418-B5CE-FB349E1E74F0}
- {594D4267-E702-4BA8-9DF4-DB91DCF94B3E}
- {D2538F6E-E852-4BE0-9D20-61730D977410}
- {BAB5BA8A-DE70-4F79-9926-D6849C218BF2}
- {E37D4B50-05EC-4128-AC65-10E299693A3C}
- {2BD1FC31-CFB0-488A-83B3-BEC066423FAA}
- {AA378242-0C2C-4CC2-9E33-B44E0F92577C}
- {F00D0401-C60F-4AB1-BCF2-ADA00DF40AA9}
- {5AE7F499-C7A3-4477-BBED-3D8B21FF6322}
- {5147A262-75C3-4CAE-BCF0-09D9EBBF4A24}
- {7D3F3C7C-A40D-42EC-BA38-E04E6B3CFA16}
- {36305F97-388A-4427-AF76-C4BA8BC2A3DC}
- {BB3F184D-C512-4544-8A7D-76A1F600AEC2}
- {A4CEFD65-D3DF-4992-AC4A-2CED8894F0BF}
- {36B75654-E4C2-4FF3-B9F7-0D202D1ECAC8}
- {0E14FDF9-3D6C-48E4-B362-B248B61FC971}

10.9.1

- {F48C3ABF-AF5F-4326-9876-E748DB244DB7}
- {AC4AD5BF-E0B4-4EE6-838E-93EE66D986EF}

- {F96ECEFD-2015-4275-B15D-363F53407390}
- {21B1638E-47E7-4147-B739-EB341F99986F}
- {78ABEA6E-4832-4087-B7BB-04746D1E83E8}
- {A624163D-A110-4959-BD82-98CB7CE6ECBE}
- {7A6E0537-43A2-4925-8F8A-E19715B21392}
- {4AE1AE3D-2471-4393-B0D9-ECB4D1368EB9}
- {C72DE321-E19C-4737-9513-AE39B1A32953}
- {49F98C43-955D-4BD8-A585-07BA45D72D0A}
- {5DD68937-54F9-4015-A8DA-4602AFCA8986}
- {D3C16E17-DAB1-4025-A029-46C7598DCA4A}
- {A2CBD39F-C2DE-4983-9C70-7F108B52F402}
- {CA174887-E7C6-4DE9-8797-72CBD7FC4B1C}
- {B658575F-82ED-49BE-980C-D4A5089FCA7A}
- {CBEE526A-29B6-46FE-B7F8-B930A785CFF8}
- {76618450-9F2C-4FCC-9CDA-01A61F9E1953}
- {17591EF3-221C-4DD1-B773-6C9617925B5F}
- {566920BF-1EF3-4E62-B2BF-029475E35AAB}
- {4A3B27C6-7CB1-4DE8-BCB1-221B9A23E2E1}

10.9

- {E3CBD7DB-60AE-45F3-B281-F9556781E602}
- {D712233D-C35F-4A04-A7E8-6D3F00A40544}
- {D5EBAE28-7A5C-41E7-A04F-A1AAFF75C8AC}
- {2F798220-41AF-4D8D-B425-98095F3DC287}
- {06B94095-F4F9-4434-8358-2E84965B6301}
- {F2C06411-06A3-4617-8577-7975BD6CC32E}
- {10C21BB5-7E8C-47F6-AB6E-AC62300EA034}
- {B0D3E289-039D-470C-A9DC-1EB9713B2458}
- {35838A3A-D572-4B2B-8C83-4F8A99324F92}
- {CEEC063C-D280-490E-B795-373E7DE6266A}
- {4CB4458D-C08A-4DE8-9D0B-45C4E0B849F9}
- {83605278-1596-4C33-8484-CF2BD4C07587}
- {A2AE04B5-879C-4E0A-B237-D642D8BBE3C7}
- {38E1E357-BA81-4135-A11A-51FBC9C858DC}
- {947676E2-B5A6-49CB-A5AA-DFEB54D8F064}

- {8E838EF7-0B7D-4E2A-AF21-4639AC6E5492}
- {37913C5B-A6BA-4F1D-B12F-AD505B91D05A}
- {1C9C9C3C-CE4D-4F42-8A3B-78ECA6C57B8E}
- {0C000BEA-E770-4138-A707-CCB02E64469A}
- {D5CEFB24-D0FD-4C73-8685-205222E08C12}

10.8.1

- {56F26E70-2C61-45BC-A624-E100175086F7}
- {996B7BC1-3AF4-4633-AF5F-F7BE67448F51}
- {0FB565D2-7C0E-4723-B086-C67443ADE5FD}
- {246A7BFA-BE78-4031-A36D-F7BB95FFC5E2}
- {7D3E447C-3DB7-488D-AB11-C84A02476FF5}
- {1B5B7A25-F639-44F8-987B-6CD8F88967BE}
- {4242D730-262E-45E0-8E1F-9060F03452C3}
- {7CF4D730-F1D6-4D01-B750-D1BA7E55C3CC}
- {179DB6A6-DFE4-4AF1-92D5-2FDDD831A783}
- {0F67B656-1ED6-4C87-9DB3-DA51ABEE40C0}
- {86F8D877-87EA-4296-9D48-64D7AE94330B}
- {80FEB406-8086-42FE-B14B-C45A96B36894}
- {5990ACD0-4A80-4115-BFAE-F8DEB498A7C0}
- {12E78447-5AD7-41DB-82E5-BEDAAE7242C0}
- {25A1ECD8-4FAA-4271-9586-6FD94549365D}
- {221CCAE0-DA79-4C5E-ABCA-396E827334B1}
- {508FBAA8-FD44-4998-B797-1666BD41D804}
- {23EB5093-17EE-45A0-AE9F-C96B6456C15F}
- {BEB8559D-6843-4EED-A2ED-7BA9325EF482}
- {A12D63AE-3DE9-45A0-8799-F2BFF29A1665}

10.8

- {E77ED9CA-7DC8-45FC-A8BB-57AD2096EF8A}
- {068CA630-558A-4C4A-983F-ECF5F8183FC9}
- {F168EBD1-CEDA-469B-89E4-E79C85253CB6}
- {96229607-EC9D-4805-AF94-E1AC47676586}
- {D89375FD-6CAC-4204-8761-22F51B39E6A1}
- {BABA485F-681E-4B5D-95EF-54CC738F4A0C}

- {AEFE7DEE-1EEE-4F99-BCA7-2193B86C7058}
- {FC4B3333-7AEB-46C6-AD90-E071A18D653F}
- {119C0DB0-02B8-442C-B3F5-999D99C9D42F}
- {89946E15-3E27-4F13-946F-30205F18D34B}
- {5B21D9CD-DDC8-4768-88F6-3C0633E7B97E}
- {C0752042-FAAC-4A94-B5A4-918BE46B7595}
- {751ED05E-63BF-407C-9039-C72F33CC73D4}
- {720EDDD5-B0FD-4E53-8F80-0F328EA8ABE0}
- {5FBFC270-1AEE-4E41-B7A2-47F7C742EF95}
- {A46D3ECC-39D2-459C-9BC3-1C780CA5BCF1}
- {CAE80A6F-8046-47CE-B3F6-D2ACEDDDA99A}
- {0B5C6775-B1D2-4D41-B233-FC2CDC913FEE}
- {278663A9-7CA3-40D5-84EA-CA7A9CABACB6}
- {9452D085-0F4F-4869-B8B4-D660B4DD8692}

10.7.1

- {5F1D01EA-296E-4226-A704-6A90E2916782}
- {7368D3C8-F13B-4786-AE38-B51952F43867}
- {2C838C64-DF81-4A64-8618-072AD30D51C1}
- {D4054E1B-C75C-4F69-BBB7-DBE77250F345}
- {C2C75F23-3E15-43E4-A902-673569F3F0DF}
- {F633A04F-D08B-4EBF-B746-00ADA0334CE3}
- {7D13D8C5-751F-44B1-BEAE-C9EB8E13FDF8}
- {ACAA0479-B7C5-44A1-B5FD-34A018EA2137}
- {E0343824-0C94-4A6C-96F7-AA5E1D8F8437}
- {8D108926-DC71-493D-B2C9-8BAE04DD9047}
- {A19DF635-25F0-4371-AC42-A4EECAF8BD75}
- {78F54FC8-C530-4D7E-91CC-48B9BC364535}
- {CEFB5C80-707B-471A-B8BF-5EC333F1A8B2}
- {BE892BB6-842B-4A18-A0B7-E89C5AAAD1A3}
- {A11006D2-3C1A-4D56-917D-4417D3341ADD}
- {763E3951-E827-492B-8E86-F526F251083E}
- {57C506AE-3BB7-4936-9154-7A2744735456}
- {4E2BA3D3-EFD2-4FCE-91C0-1D15457F8F08}
- {1BBB3C99-8EF5-4225-B5DD-799E50582BF7}

- {F6E99E06-B303-4965-9566-2F21EE7FD130}

10.7

- {58A76431-E1A9-4D11-BB89-0D12C6E77C78}
- {E7B9D4A3-4E55-49F8-B34C-CA8745FFD894}
- {D89709DB-8B6D-431A-95D4-FFEB69C474D5}
- {858283F5-B9E9-4688-BF3C-BD3F3FD169D8}
- {DE2BA579-D2F0-4068-9C52-8AC24022F13D}
- {48405A7D-CFA4-4F6F-BB8C-B36A22E99B07}
- {BEC99E10-7AB1-4B90-9C81-D2CBFCAD4239}
- {C0C178B9-EBC6-46C5-B009-186661E9AEA3}
- {0D5F9D8E-B221-4C74-87C3-13050F906A94}
- {52EC0A7A-9BBA-4F47-9C52-2E1D1D09D9B4}
- {6CF9C794-AEC2-45EF-A11A-83938F01A1E9}
- {F36AF2F5-2E37-409B-9E71-D2D2B1D4A22F}
- {4F54A93E-2F0F-4515-99AA-83BF88961D5F}
- {A04ACEF7-4E22-4F4F-8608-9FD335572C6F}
- {0D562427-2AB5-46C6-998E-4C33D642DE10}
- {8C15E459-D24F-46E0-B945-CD4812A040AC}
- {24821676-BD09-49CA-95B4-591BBE86118A}
- {3C4D06FD-8194-4062-AB04-E87003CBE908}
- {71044157-41F9-4AEC-B6B1-834FBA256135}
- {C4ECCD46-EC43-4C44-8147-916649A2BA1B}

10.6.1

- {3FA8B44E-E0E3-4245-A662-6B81E1E75048}
- {8D6EE2C0-A393-49CD-A048-1D9FD435D7B8}
- {6C05375F-78A5-4DF7-A157-C2A6E0D7BAD2}
- {1F1EEC9F-80D5-48DD-B8BC-EB3D0404D9AD}
- {2CA5FC7F-1165-4870-9C16-004ACC848435}
- {E23D8BB8-0FEB-4316-8E09-80772FD1B5E0}
- {C67E73AB-8278-49C9-9CA8-A714E20B8124}
- {E527C0BD-E026-46D8-9461-2A7EEFBDA35A}
- {D5DF4279-E3FF-4261-AB85-93F8BDE90D8D}
- {8D439456-493A-4B48-A542-492AABD9CF7D}

- {D61CE1AE-2DB8-4D46-AC7F-3BEAB7C29A59}
- {9B07A4CE-58C6-4689-B37B-EFF565712CF2}
- {C97C2CEF-F939-496E-8CB7-8756856CBBC6}
- {59079961-A0BA-48DD-9B07-45437FCBC42A}
- {5372DAF1-7EB6-4822-843E-0B2F7A7B052B}
- {D807F4E9-0F87-4B3C-8F93-456251226187}
- {7BEB71AD-3958-41FB-8EC3-64DBE4775760}
- {286D4CB5-777E-4AA1-B2EB-D6A3A4212107}
- {37F3B528-915F-4528-949B-F199E4B3B4AA}
- {6FEB4C76-14AC-4A70-BE45-6CBAED529CAF}

10.6

- {38DBD944-7F0E-48EB-9DCB-98A0567FB062}
- {8214B9D8-49D9-43DB-8632-AE2BAD4B21E9}
- {B3FD1FE3-4851-4657-9754-73876D4CB265}
- {88CDE5E9-23B8-4077-9E69-9CD3715BE805}
- {E7630CBC-96DE-4665-9C2A-D682CFFD5B0E}
- {E2601F84-D2E5-4DD4-B0EC-6AED75CB77D9}
- {75FB755F-AF36-484E-98A8-FADA56574D25}
- {AA32D01D-27CD-4842-90CF-F22C1BD6309B}
- {CF126207-4C89-44AA-8783-9BAA2BA5F106}
- {9F8694BE-613F-4195-AA42-B849E84D059A}
- {2C3BE00F-57BE-4D0B-81BC-3378D823CF0E}
- {EAC54B65-D6BC-41DC-8C82-5E99D7FD4271}
- {76C17CB6-106C-41F8-89BA-41C086E69238}
- {4493EB64-CAE0-439F-8FA6-897677D5A6C8}
- {0C59A27D-B4B6-4A23-8873-897B870F6E2B}
- {B46B6E63-D8E1-4EA4-9A9B-D98DFAA6644D}
- {89E6330E-6139-4F4B-BA9F-ACD59065230D}
- {238E647E-53DF-4B8B-B436-ADA5004065DE}
- {30EF8944-904A-45D3-96D4-7DF3B0FE01D5}
- {06012CC0-5C12-4499-B5CC-99E9D547A2FD}

10.5.1

- {B8A6A873-ED78-47CE-A9B4-AB3192C47604}

- {7DEAE915-5FAC-4534-853D-B4FC968DBDEB}
- {AC10F3CF-A5C1-44B0-8271-27F26D323D14}
- {5F748B0C-3FB6-42FF-A82D-C1573D3C1469}
- {428DE39D-BF23-42B5-A70E-F5DD5DD21C2C}
- {98B1DE9B-0ECF-4CAA-A29A-B89B2E8F38F1}
- {4876508B-31CF-4328-BE11-FFF1B07A3923}
- {D803A89F-4762-4EFD-8219-55F4C3047EDE}
- {4A5F404B-391F-4D13-9EE4-5B9AC434FD5A}
- {99FFFA13-2A40-4AA4-AAC1-9891F2515DB1}
- {2B04DE60-3E79-4B44-9A93-40CAC72DE2FB}
- {D595C9E2-BBA0-4708-A871-1166CD0CFB61}
- {50825C57-5040-436D-B64C-A53FFB897E9D}
- {5D750A11-BC80-45CE-B0DD-33BA8A5D8224}
- {60390703-9077-4DDE-8BB1-A025AB0FE75B}
- {BF75DC6C-F1A5-4A3C-A6A6-76BCB5DB5881}
- {96B29B2F-888A-4C2B-B8C3-97E9A7849F2F}
- {7FDD9158-2E93-4E12-A249-CD9D5445C527}
- {A868CBAC-D9A2-41A7-8A5B-069AB63FEC7B}
- {83462AE4-27BB-4B63-9E3E-F435BD03BB12}

10.5

- {604CF558-B7E1-4271-8543-75E260080DFA}
- {9666ABD8-8485-4383-B3DD-4D1598F582A3}
- {58264BBA-5F61-41D9-839A-00B6C2C66A63}
- {5988C905-772F-4F62-8339-1796C38674B7}
- {ADD5FF4F-EB57-4460-BD33-D55562AE6FA7}
- {3294151B-CA4C-4A89-BBC7-DCE521D8A327}
- {EF65064A-96C8-4EA1-B76D-B9BCC97EF76A}
- {6B2FA0A8-6F2C-4359-B7A4-D2F9FD63EE97}
- {ACF59C57-A613-44CC-A927-1D8C2B280516}
- {2E5E4CDE-9964-4B40-A1F1-843C62AC789E}
- {2901A5D3-C16D-4993-A306-86261B0430B1}
- {AC910B51-6077-4055-B042-D72CA0D23D69}
- {8F36D583-35F0-43F2-8F8F-5B696F87183A}
- {37C2CAE2-4A81-4289-B318-93D63C63AA47}

- {CC345B69-1E26-4C56-B640-92BCBADBDF06}
- {F0FAE80D-0C51-4D9D-A79B-057396A2456D}
- {5BA355D1-D9B6-4CA0-B1C6-694377084464}
- {25118D44-AD2D-423F-85F0-5D730A2691B7}
- {D4855344-CEE0-47A3-BD50-D7E2A674D04E}
- {9CD66AA3-F0DA-46CC-A5DD-0BB5B23499AD}

10.4.1

- {475ACDE5-D140-4F10-9006-C804CA93D2EF}
- {0547D7D8-7188-4103-9387-A99FE15215AF}
- {25DFAFFF-07CE-42A2-B157-541D7980A3DA}
- {771998A8-A440-4F5F-B55A-0FE2C594208B}
- {C120DC32-DBEA-4CB1-94E4-F50A7EE09F5C}
- {3294151B-CA4C-4A89-BBC7-DCE521D8A327}
- {E04FB941-248D-4806-9871-04DB306EEA91}
- {66CD667D-440D-4CF1-9ECB-C6C77A7A0520}
- {7938463B-E744-4332-8617-39E91B10FC15}
- {C22C2AF5-D58E-4A4D-85DF-E3A38C83F37A}
- {9AF62D15-755B-43DE-878A-DBA23D33B28A}
- {D4F22207-C5FA-49B0-9466-9E4D37435882}
- {C8ADE9B2-3BC8-4417-97D0-785BA0CD86D9}
- {C85A40C5-00B9-4CDE-9299-397BFD5A2EAF}
- {E0BD73FB-4028-4A5D-9A24-9FA0BD614D4B}
- {83CF76EC-F959-46B3-9067-F59B2A846D2F}
- {F7D6BD55-8D07-4A57-8284-ADACE0F567D8}
- {C56A0E47-D4E1-4762-9BAF-07A19A154EE6}
- {09AC608B-7CE4-4280-9F4E-F2988A58428D}
- {5695B2B6-A25E-4013-B5F8-30686FDDFE0D}

10.4

- {E2C783F3-6F85-4B49-BFCD-6D6A57A2CFCE}
- {901578F9-BC82-498D-A008-EC3F53F6C943}
- {E3849BEC-6CAF-463F-8EFA-169116A32554}
- {EE889E4F-85C7-4B8A-9DAA-5103C9E14FD6}
- {89D96D88-CC2F-4E9B-84DD-5C976A4741EE}

- {0913DB77-F27B-4FDE-9F51-01BB97BBEBB9}
- {99B6A03C-D208-4E2E-B374-BA7972334396}
- {A0F3D072-0CD1-43D7-AFDA-8F47B15C217C}
- {0FE26871-21C3-4561-B52E-A8FED5C8E821}
- {1D1F3C15-F368-44AF-9728-6CF031D478AF}
- {CE5EC52D-B54D-4381-9F6E-2C08F7721620}
- {E71AEC5B-25F0-47E5-B52C-847A1B779E48}
- {5DA1F056-A3F1-46D5-8F2E-74E72F85B51B}
- {1EB3D37A-902A-43E2-9EAA-1B43BA10C369}
- {839FFEB7-76B5-4CBB-A05E-E2276FC3421D}
- {594E1C33-1C6D-49B4-A83F-2A780193B75F}
- {34330B0C-34CD-4DCF-A68D-FDE7A1834659}
- {42A96EC7-7CA9-4F68-B946-E9BF84713605}
- {A1A8DAE4-B6F9-446F-8F6A-487F1E07A434}
- {3BF277C6-6A88-4F72-A08C-54F1E45F44E5}

10.3.1

- {2350F5B2-44A2-413E-804C-445DB177152B}
- {7729802B-A3BB-49E5-8BCC-8413C4F852F1}
- {6494393C-0657-4D5D-9A51-E54831E48CC4}
- {140F583D-4EB9-4A3A-8B60-2DA3A72234D1}
- {794D05F0-522C-42E7-AF0D-5A7FDECD7FB2}
- {D4CFB367-FF83-4632-AA26-F7138001C071}
- {096A7FDD-9548-44BE-B04D-1F82669850E3}
- {95DB352A-B1A4-49DD-9D16-5AD8870203D0}
- {D3C84839-B233-4951-8F9B-962D4CD81DB7}
- {2C858B42-0479-4F5B-9B3B-2489EDF9639F}
- {395889EC-8AB3-4570-AC77-11C2EEDB9A61}
- {BE5D14D7-5433-4F04-8E3A-6A6DB7032C28}
- {FD8D58CC-B361-4198-B83C-41DEF9AA9C81}
- {553CDCDB-5559-43B7-A61C-8838529634CA}
- {F569182C-6726-4BD3-B4C5-57982598761A}
- {89E4E8EC-4594-428F-AEAD-0936A7EC21A4}
- {F313D6A5-1057-4A09-B512-DB20D5D801D4}
- {7A22729E-048C-493B-8766-6FDF7155E134}

- {36FEEE30-C19C-416D-A19D-38D277F45620}
- {A1C899A0-8582-4C38-8A4B-DFAEC55681F0}

10.3

- {0E139F65-5170-4F6D-A27C-873C61DA98F6}
- {45CD1727-42C8-4986-90B0-5E16C58EBFC7}
- {D6447963-213B-4E7F-A133-02E995C6F948}
- {CB34AB51-E1EF-42C5-A0DF-C37C5C5F3160}
- {EDA2D3D2-733F-4B63-89BB-48AA5AD65A17}
- {8445558D-7ECF-4C2B-95AA-8C85E41140E8}
- {34072E47-BF27-4D33-A52B-B33BEDB667DA}
- {FD629592-E642-415F-B048-C53D8AD68866}
- {0BAD8A19-1D69-461E-817A-E4B1F7F26639}
- {556DAC0C-C01E-4D5E-B470-077A60BC5F28}

10.2.2

- {B4F6E64E-FC38-4743-92F0-F934EEFE683B}
- {1879DA6F-9FBE-406C-970A-E4E7D1D588F9}
- {058D6AC8-5E5D-42CE-B02D-1F93EA0CA2FD}
- {16990EFC-29DE-4973-AC57-FE4ED65CF149}
- {28832100-4AF5-4CE6-B397-EA209892A466}
- {9253CEB5-4FFD-4E2D-B6CC-8636D38C8776}
- {07C61E8A-EEB0-4E3A-BA98-BD1B6D2E996F}
- {5F3600B0-3421-4734-9240-D69A65398E36}
- {F73700E5-E5E3-4B35-AFC3-182EC445D23F}
- {1636DF85-7289-4E4D-960F-D695167B7006}

10.2.1

- {345B5297-EB09-42E3-9AC4-726D2D3953AE}
- {EFB3F701-9AF6-4577-AE0A-0C0B09BCA5C8}
- {F3C325DE-3F65-4D60-AC47-0DD9D9E35B16}
- {4B9BF032-BF90-4B71-87D1-CAFC65FA67A7}
- {52D5974A-753E-419A-B5FE-3B01326B0F69}
- {A59DCF22-BEAE-484B-9997-4EC8426054A3}
- {94DD2DB1-C250-4BFD-A189-74774814DF5E}
- {2F3A4E46-FFA9-4359-A0E1-AEA0A38352FA}

- {8DE09037-50A3-4E3A-8F94-86DF0A116E22}
- {7A5BC91C-B3C0-465B-9670-643F88DAF793}

10.2

- {2A79BF0A-248E-45A1-B283-5EC0CFA07537}
- {EF39D7A8-94B9-4042-A480-8BB5F4CD04D6}
- {E045E259-E3FA-4C5B-9F85-8FB1A40FA1BB}
- {8C5ECECE-8FA3-4E6A-8219-62276CD40617}
- {DB03FAC4-6F6E-4A20-AA79-4D31A6C3E8C1}
- {9ADB734F-294E-4E03-808B-8BAECE9493E8}
- {2D9BF186-23BA-4DBB-8360-315AF8A345AF}
- {66C75B2A-B5AC-441E-9286-09DF7E0D75F2}
- {AA60D73D-F69B-42E3-9A57-150F5D3D3916}
- {FB4D8549-9627-45DA-9D94-FC0FCA6263FA}

10.1 SP1

- {D52794EA-CFED-4A35-AD48-D7B70362872E}
- {FC0598F8-DFF8-4324-9E88-8EABB2D9B855}
- {53D94675-CA80-4333-9FFF-BA9DF7AAAB01}
- {1B4C6478-0E9B-4781-AADE-EECE7923BE02}
- {2FAC39EB-E9F1-478F-BB9A-46D77920FE90}
- {9892BC97-25CC-47F8-BA52-AE616DF07393}
- {B34156D4-6941-4DCD-BF16-BA9FA11673FD}
- {4512A442-2FB4-48E7-927A-49874DB5C57B}
- {CF5D211A-6637-4B65-8E0A-B152888A4ECB}
- {8353ED1D-4DFC-4FCE-B3B8-2668009D653A}

10.1

- {F2D4A6C5-E11F-4FEF-A240-5F2BA22F6418}
- {DF32A6BA-A260-4BCD-B59A-4CEB4173B2D8}
- {0CF52969-7F17-4F85-82FF-C658F3DC5F6E}
- {8E4D5C3B-B54C-4CC5-9A5F-3EC0C6BF64F0}
- {0329B7AD-D457-42F2-B97E-BBAE26D54329}
- {38A627D7-01C7-4E3F-945D-3CD4CDF14BE5}
- {635C3AE6-F3F1-434D-B1E7-B12CE91AD83F}
- {39BE94C5-8146-4560-A54E-859979624ACF}

- {1506767A-988E-44EB-A733-E5B8BFFBE81E}
- {BFA02DB7-9E55-4179-88AC-D2C1B9802096}

Upgrade

Upgrade ArcGIS Web Adaptor

To upgrade ArcGIS Web Adaptor to 11.4, you must uninstall the earlier version, and install the 11.4 setup. During the 11.4 installation, you'll specify the same name as your earlier Web Adaptor. This guarantees your Web Adaptor URL will remain identical to the earlier version.

If a naming conflict is detected during the 11.4 installation, a warning message appears. You must uninstall the earlier version with the same name to perform the upgrade.

Note that if you are upgrading from version 11.0 and earlier and have multiple instances of Web Adaptor installed, you will see an increase in memory usage. This is because each Web Adaptor instance now requires its own application pool to provide enhanced availability and resiliency.

After installing 11.4, you must configure ArcGIS Web Adaptor with its corresponding server site or portal. For more information, see the following topics:

- Configure ArcGIS Web Adaptor with a server site
- Configure ArcGIS Web Adaptor with portal

Note:
If no administrative account credentials are available to re-register the Web Adaptor with the server site or portal, you can use command line tools to create a temporary administrator account or re-enable the primary site administrator account.

Reference

Questions, feedback, and information

There are a number of options for you to provide feedback or obtain further information.

My Esri

My Esri is a website where you can interact with Esri to find answers to questions, post feedback, and obtain information. The website also contains frequently asked questions, how-to instructions, software downloads, troubleshooting tips, and so on. Sign in to the website with your Esri account. Alternatively, you can contact Customer Service or your local distributor.

Web help

Visit the ArcGIS Pro, ArcGIS Enterprise, Esri Documentation and Esri Developer websites for up-to-date information about ArcGIS software and services. These resources can help you increase your understanding of GIS technology.

Installation help

Downloads include the `Install.htm` help file. You can find what you need by searching the table of contents or finding the number of times a term appears in a section.

Copyright Information

The information contained in this document is subject to change without notice.

You may have received Products or Services that include Graph Editor Toolkit, Copyright © 1992-1999 Tom Sawyer Software, Berkeley, California, All Rights Reserved, and Tom Sawyer Visualization, Ver. 8.0 Copyright © 1992-2009 Tom Sawyer Software, Berkeley, California, All Rights Reserved.

Portions of this computer program are Copyright © 1995-2016 Celartem, Inc., dba Extensis. All rights reserved.

This application supports the ECW data format and ECWP compression protocols. Portions of this computer program are copyright © 2007-2015 Intergraph Corporation. All rights reserved. Creating compressed files using ECW technology is protected by one or more of U.S. Patent No. 6,201,897, No. 6,442,298, and No. 6,633,688.

PANTONE® Colors displayed in the software application or in the user documentation may not match PANTONE-identified standards. Consult current PANTONE Color Publications for accurate color. PANTONE® and other Pantone trademarks are the property of Pantone LLC. © Pantone LLC, 2022. Pantone is the copyright owner of color data and/or software which are licensed to Esri to distribute for use only in combination with the ArcGIS family of Products. PANTONE Color Data and/or Software shall not be copied onto another disk or into memory unless as part of the execution of the ArcGIS family of Products.

This product includes software developed by the JDOM Project.

Note:
The jdom.org site has gone offline as of July 22, 2024. An alternative site may be https://github.com/hunterhacker/jdom#introduction-to-the-jdom-project.

This product includes software developed by the Indiana University Extreme! Lab (https://www.extreme.indiana.edu).

Note:
As of August 2024, the webite now states: "This site has been deprecated. You can access an archive of this site at https://web.archive.org/web/20210225153105/https://www.extreme.indiana.edu/".

ArcGIS consists of many programs and services—some of which may have been developed using Altova® XMLSpy® and includes libraries owned by Altova GmbH, Copyright © 2007-2023 Altova GmbH (www.altova.com).

Third-Party OSS-FOSS Acknowledgement Documents

Esri's use of open source software libraries is disclosed in the Third-Party OSS-FOSS Acknowledgement Documents found at the link below.

Open Source Acknowledgements (https://links.esri.com/open-source-acknowledgments)

ArcGIS Notebooks makes use of The FreeType Project, following The FreeType Project License (https://git.savannah.gnu.org/cgit/freetype/freetype2.git/tree/docs/FTL.TXT).

EXPORT NOTICE

Use of these Materials is subject to U.S. export control laws and regulations, including the U.S. Department of Commerce Export Administration Regulations (EAR). Diversion of these Materials contrary to U.S. law is prohibited.

US GOVERNMENT CUSTOMER

The Products are commercial items, developed at private expense, provided to Customer under this Master Agreement. If Customer is a US government entity or US government contractor, Esri licenses or provides subscriptions to Customer in accordance with this Master Agreement under FAR Subparts 12.211/12.212 or DFARS Subpart 227.7202. Esri Data and Online Services are licensed or subscribed under the same DFARS Subpart 227.7202 policy as commercial computer software for acquisitions made under DFARS. Products are subject to restrictions, and this Master Agreement strictly governs Customer's use, modification, performance, reproduction, release, display, or disclosure of Products. Agreement provisions that are inconsistent with federal law regulation will not apply. A US government Customer may transfer Software to any of its facilities to which it transfers the computer(s) on which it has installed such Software. If any court, arbitrator, or board holds that a US government Customer has greater rights to any portion of the Products under applicable public procurement law, such rights will extend only to the portions affected. Online Services are FedRAMP Tailored-Low authorized but do not meet higher security requirements, including those found in DFARS 252.239-7010.

Esri Trademarks

Esri Products or Services referenced in this work are trademarks, service marks, or registered marks of Esri in the United States, the European Community, or certain other jurisdictions. To learn more about Esri marks, go to the Esri Product Naming Guide (https://links.esri.com/product-naming-guide).

Licensed Trademarks

Other companies and products or services mentioned herein may be trademarks, service marks, or registered marks of their respective mark owners.

The Kubernetes ship's wheel logo is a registered trademark of the Linux Foundation.

Trademark Images

Logos of licensed trademarks include the following: