

ArcGIS® Enterprise: Configuring a Base Deployment



ArcGIS[®] Enterprise: Configuring a Base Deployment

STUDENT EDITION

Copyright © 2017–2025 Esri

All rights reserved.

Course version 8.0. Version release date July 2025.

Printed in the United States of America.

The information contained in this document is the exclusive property of Esri. This work is protected under United States copyright law and other international copyright treaties and conventions. No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or by any information storage or retrieval system, except as expressly permitted in writing by Esri. All requests should be sent to Attention: Director, Contracts and Legal, Esri, 380 New York Street, Redlands, CA 92373-8100, USA.

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.

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

Commercial Training Course Agreement Terms: The Training Course and any software, documentation, course materials or data delivered with the Training Course is subject to the terms of the Master Agreement for Products and Services found at the following website: esri.com/TrainingTerms. The license rights in the Master Agreement strictly govern Licensee's use, reproduction, or disclosure of the software, documentation, course materials and data. Training Course students may use the course materials for their personal use and may not copy or redistribute for any purpose. Contractor/Manufacturer is Esri, 380 New York Street, Redlands, CA 92373-8100, USA.

Esri Marks: Esri marks and product names mentioned herein are subject to the terms of use found at the following website: esri.com/EsriMarks.

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

Table of Contents

Esri resources for your organization	vi
--	----

Course introduction

Course introduction	1
Course goals	1
Installing the course data	1
Icons used in this workbook	3

1 ArcGIS Enterprise overview

Lesson introduction	1-1
What is ArcGIS Enterprise?.....	1-2
What can ArcGIS Enterprise do?	1-3
Explain the components of the base ArcGIS Enterprise deployment	1-5
Describe base deployment prerequisites and considerations	1-7
How is a base deployment set up?.....	1-8
How do you automate a base deployment?	1-9
Classroom PC environment.....	1-11
Lesson review	1-12
Answers to lesson 1 questions.....	1-13

2 Configuring a secure environment

Lesson introduction	2-1
Identify component communication	2-2
Using certificates to enable HTTPS encryption.....	2-4
Exercise 2: Enable HTTPS encryption	2-7
Inspect the root certificate	2-8
Bind the certificate to HTTPS.....	2-9
Verify HTTPS communication	2-11
Workflow review	2-12

Answers to lesson 2 questions.....	2-13
------------------------------------	------

3 Setting up an ArcGIS Enterprise portal

Lesson introduction	3-1
Portal for ArcGIS installation overview	3-2
Portal for ArcGIS account.....	3-5
Exercise 3A: Complete a Portal for ArcGIS installation	3-8
Begin the portal configuration	3-9
Use a license file to authorize the portal.....	3-9
Configure the initial portal administrator account	3-10
Identify properties of the Portal for ArcGIS content directory	3-13
Checkpoint	3-14
ArcGIS Web Adaptor.....	3-15
Exercise 3B: Integrate ArcGIS Web Adaptor.....	3-16
Install and configure ArcGIS Web Adaptor	3-17
Validate your Portal for ArcGIS installation	3-19
Import and configure a certificate for your Enterprise portal site	3-20
Workflow review	3-23
Answers to lesson 3 questions.....	3-25

4 Setting up a GIS server

Lesson introduction	4-1
ArcGIS Server installation overview.....	4-2
Explore the ArcGIS Server installation	4-4
Verifying accounts in Active Directory	4-6
ArcGIS Server directories and configuration store.....	4-8
Exercise 4A: Set up your ArcGIS Server site.....	4-11
Create the ArcGIS Server site	4-12
Install the web adaptor	4-13
Configure the web adaptor.....	4-14
Import the web server certificate	4-16
Explore the site	4-18
Checkpoint	4-20
Federation.....	4-21

Exercise 4B: Federate your ArcGIS Server site with your Enterprise portal	4-23
Configure federation	4-24
Explore changes to the implementation	4-27
Migrating from a stand-alone server	4-29
Workflow review	4-33
Answers to lesson 4 questions	4-35

5 Managing GIS resources

Lesson introduction	5-1
ArcGIS Data Store	5-2
Setting up ArcGIS Data Store	5-4
Configuring the hosting server	5-7
Exercise 5A: Set up ArcGIS Data Store	5-8
Install ArcGIS Data Store	5-9
Create relational and object data stores.....	5-10
Import the certificate for ArcGIS Data Store	5-11
Designate the hosting server	5-12
Share a hosted layer	5-14
Defining web layers.....	5-17
Associate web layers with GIS resources.....	5-19
Data registration	5-20
Registering data with ArcGIS Server	5-22
Exercise 5B: Work with registered data	5-23
Register a geodatabase with ArcGIS Server.....	5-24
Share a layer with referenced data	5-26
Inspect the service workspace	5-27
ArcGIS Enterprise account uses.....	5-28
Workflow review	5-29
Answers to lesson 5 questions.....	5-30

6 Securing a base deployment

Lesson introduction	6-1
Understanding identity stores.....	6-2
Configuring portal authentication	6-5
Choosing an authentication method	6-10

Setting up an enterprise identity store	6-12
Exercise 6A: Configure an enterprise identity store and authentication.....	6-13
Configure enterprise logins	6-14
Assign an enterprise portal administrator	6-15
Configure web-tier authentication	6-17
Test the SSO	6-18
Security best practices	6-19
ArcGIS Enterprise security options.....	6-20
Exercise 6B: Evaluate security for a base deployment.....	6-22
Scan your Portal for ArcGIS for security best practices	6-23
Scan your ArcGIS Server for security best practices	6-25
Workflow review	6-27
Answers to lesson 6 questions.....	6-29

7 Managing users and groups

Lesson introduction	7-1
Sharing portal content	7-2
Levels of sharing	7-4
User types	7-6
User roles	7-9
Creating custom roles	7-12
Choosing an appropriate user type and role.....	7-14
Integrating groups from your organization-specific security store	7-15
Exercise 7: Integrate enterprise groups.....	7-18
Configure the portal group store	7-19
Add enterprise members	7-20
Add an enterprise group	7-23
Share content with an enterprise group	7-26
Workflow review	7-28
Answers to lesson 7 questions.....	7-29

Appendices

Appendix A: Data license agreement.....	A-1
Appendix B: Answers to lesson review questions.....	B-1
Appendix C: Additional resources	C-1

Appendix D: Lesson stories.....D-0

Esri resources

Take advantage of these resources to develop ArcGIS® software skills, discover applications of geospatial technology, and tap into the experience and knowledge of the ArcGIS community.

Instructor-led and e-Learning resources

Esri® instructor-led courses and e-Learning resources help you develop and apply ArcGIS skills, recommended workflows, and best practices. View all training options at esri.com/training/catalog/search.

Planning for organizations

Esri training consultants partner with organizations to provide course recommendations for job roles, short-term training plans, and workforce development plans. Contact an Esri training consultant at training@esri.com.

Esri technical certification

The Esri Technical Certification Program recognizes qualified individuals who are proficient in best practices for using Esri software. Esri exams are designed to validate expertise with ArcGIS products, such as ArcGIS Online, ArcGIS Pro and extensions, ArcGIS Enterprise and extensions, and developer technologies. Certifications are offered at three levels: foundation, associate, and professional. Learn more at esri.com/training/certification.

Social media and publications

X (formerly Twitter): [@EsriTraining](https://twitter.com/EsriTraining) and [@Esri](https://twitter.com/Esri)

Esri on LinkedIn: [linkedin.com/company/esri](https://www.linkedin.com/company/esri)

Esri training blog: esri.com/trainingblog

Esri publications: Access online editions of ArcNews, ArcUser, and ArcWatch at esri.com/esri-news/publications

Esri training newsletter: Subscribe at go.esri.com/training-news

Other Esri newsletters: Subscribe to industry-specific newsletters at go.esri.com/subscribe

Esri resources (continued)

Esri Press

Esri Press publishes books on the science and technology of GIS in numerous public and private sectors. esripress.esri.com

GIS bibliography

A comprehensive index of journals, conference proceedings, books, and reports related to GIS, including references and full-text materials. gis.library.esri.com

ArcGIS documentation and tutorials

In-depth information, tutorials, and documentation for ArcGIS products.

ArcGIS Online: arcgis.com

ArcGIS Desktop: desktop.arcgis.com

ArcGIS Enterprise: enterprise.arcgis.com

ArcGIS Pro: pro.arcgis.com

Esri Community

Join the online community of GIS users and experts. community.esri.com

Esri events

Esri conferences and user group meetings offer a great way to network and learn how to achieve results with ArcGIS. esri.com/events

Esri videos

View an extensive collection of videos by Esri leaders, event keynote speakers, and product experts. mediaspace.esri.com

Esri resources (continued)

ArcGIS for Personal Use

Improve your GIS skills at home and use ArcGIS to enhance your personal projects. The ArcGIS for Personal Use program includes a 12-month term license for ArcGIS Pro, extension products, and an ArcGIS Online named user account with 100 service credits. [esri.com/personaluse](https://www.esri.com/personaluse)

GIS Dictionary

This term browser defines and describes thousands of GIS terms. support.esri.com/en-us/gis-dictionary

Course introduction

ArcGIS Enterprise is a full-featured mapping, analytics, and geospatial data management system that enables your organization to discover, use, make, and share maps from any device, anywhere, at any time. ArcGIS Enterprise is designed to be flexibly deployed on your own infrastructure so that your organization can easily collaborate and share geospatial content.

In this course, you will learn to configure and maintain an ArcGIS Enterprise base deployment, which is the minimum configuration and foundation of ArcGIS Enterprise. Each component of an ArcGIS Enterprise base deployment will be covered as you progress through the course toward a fully functioning base deployment.

While several tools are available to help you automate the setup of a base deployment, this course will focus on a manual approach to dive deeper into each component and provide more context and conceptual knowledge of how ArcGIS Enterprise works.

Course goals

After completing this course, you will be able to perform the following tasks:

- Install ArcGIS Server, Portal for ArcGIS, ArcGIS Data Store, and ArcGIS Web Adaptor.
- Configure an ArcGIS Enterprise portal to manage users, groups, and content-sharing privileges.
- Apply HTTPS certificates to support encrypted communication.
- Configure a suitable authentication method for your organization's needs.

Installing the course data

Some exercises in this workbook require data. Depending on the course format, the data is available on a DVD in the back of a printed workbook or as a data download. To use the data, extract it to your C:\EsriTraining folder.



DISCLAIMER: Some courses use sample scripts or applications that are supplied either on the DVD or on the Internet. These samples are provided "AS IS," without warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or noninfringement. Esri and its authorized distributors shall not be liable for any damages under any theory of law related to the licensee's use of these samples, even if Esri and its authorized distributors are advised of the possibility of such damage.

Icons used in this workbook



Estimated times provide guidance on approximately how many minutes an exercise will take to complete.



Notes indicate additional information, exceptions, or special circumstances about specific course topics.



Recommended practices improve efficiency and save time.



Esri Academy resources provide more in-depth training on related topics.



Additional resources provide additional information about related topics.



Warnings indicate potential problems or actions that should be avoided.

1

ArcGIS Enterprise overview

Setting up the base ArcGIS Enterprise deployment is the first step for organizations using ArcGIS Enterprise. This lesson begins with a brief overview of ArcGIS Enterprise and its capabilities. You will then identify the components that make up a base deployment, learning their functions and how to automate the system setup.

Topics covered

- Understanding ArcGIS Enterprise

- Identifying components of a base ArcGIS Enterprise deployment

- Setting up base deployment components

What is ArcGIS Enterprise?

ArcGIS Enterprise provides you with tools to create a modern GIS on infrastructure that you control. ArcGIS Enterprise users can run powerful server-based analysis tools and manage geospatial and location-enabled data at an enterprise scale. Users can also organize their GIS content within a web-based portal. This setup allows for secure and controlled access to authorized members of the organization. In addition to the analytic and data-management capabilities of ArcGIS Enterprise, users can easily create and share web maps and GIS apps without writing a single line of code.

When implementing the software, organizations can choose to deploy ArcGIS Enterprise on premises or in the cloud—connected or disconnected to the open internet. This flexibility opens the door to the benefits of the ArcGIS system to more organizations than ever. It allows organizations to empower teams, businesses, communities, and stakeholders with location-based insights on their own terms.

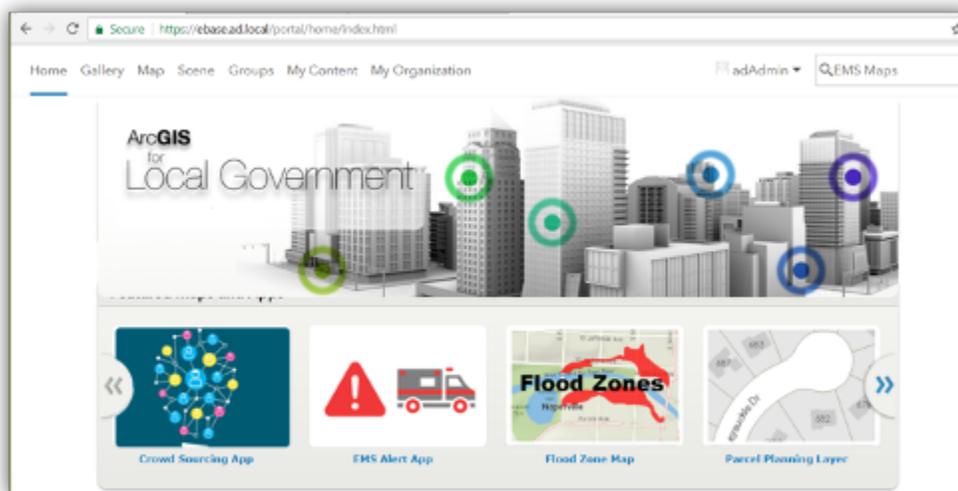


Figure 1.1. This example shows an ArcGIS Enterprise installation for local government.



Esri GIS Products Site: ArcGIS Enterprise Features

What can ArcGIS Enterprise do?

What ArcGIS Enterprise offers your organization can be described with the following categories.

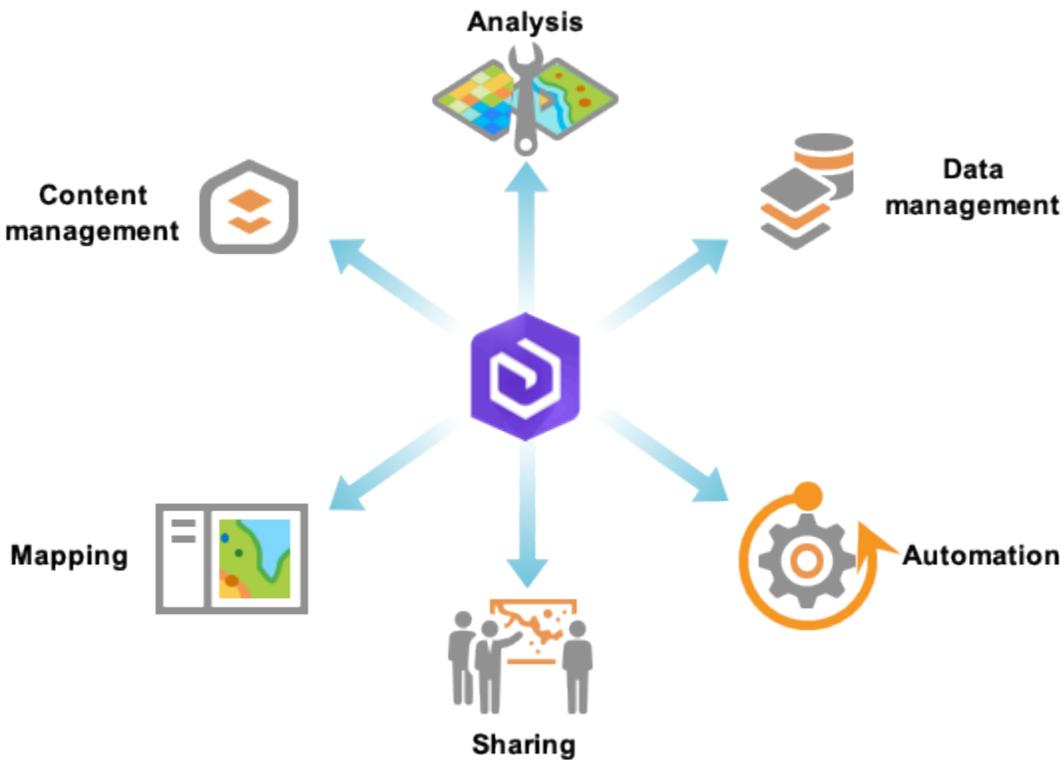


Figure 1.2. ArcGIS Enterprise capabilities are aligned with six functional categories: analysis, data management, automation, sharing, mapping, and content management.

Capability	Description
Analysis	A robust suite of analytical functionality that spans many data types and server distributions.
Data management	Tools to create and manage data according to accepted industry standards.
Automation	Ability to streamline workflows, installation, and configuration, as well as management tasks.

What can ArcGIS Enterprise do? (continued)

(Table continued from previous page)

Capability	Description
Sharing	Sharing GIS information products and services across entire organizations to facilitate the broadest possible collaboration.
Mapping	Ability to visualize and manipulate from 2D and 3D maps and scenes using out-of-the-box map and app templates.
Content management	Use of the ArcGIS Enterprise portal to enable an easy-to-use content management system to store, index, and retrieve an array of GIS information products.



ArcGIS Enterprise Help: ArcGIS GIS Server capabilities and extensions

Explain the components of the base ArcGIS Enterprise deployment

ArcGIS Enterprise workflows and functionality are enabled by four software components. This configuration is the base ArcGIS Enterprise deployment. Each component performs crucial functions that support the minimum requirements of an ArcGIS Enterprise deployment. Each component is installed individually and configured to function as an integrated system working together as ArcGIS Enterprise. The resulting system can be extended in many ways, but the ArcGIS Enterprise base deployment is the foundation that is present in all ArcGIS Enterprise implementations.

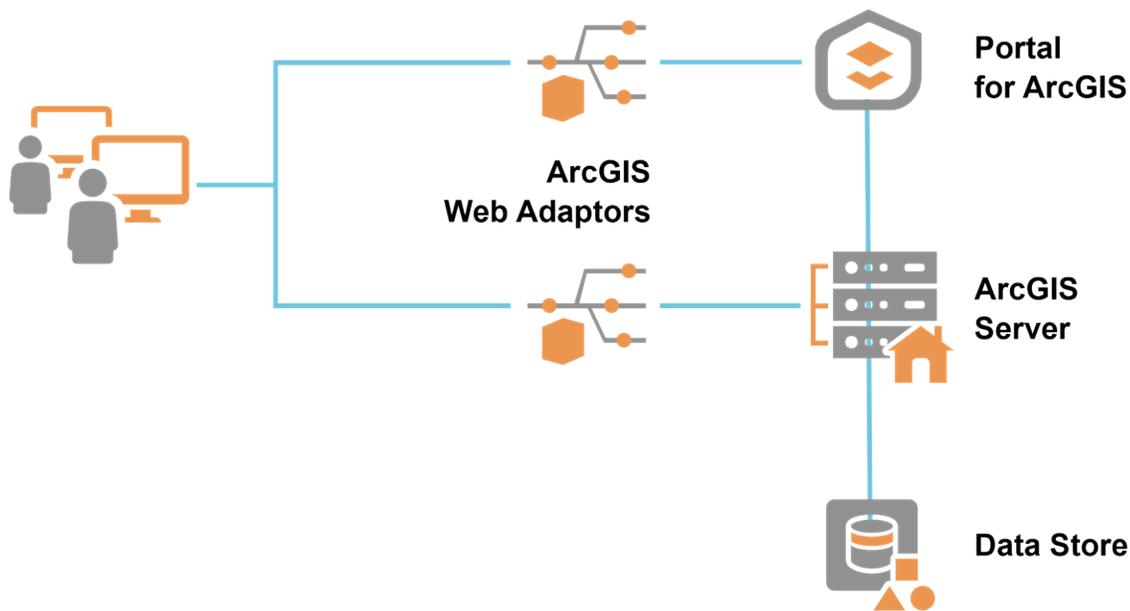


Figure 1.3. This graphic shows the logical architecture of an ArcGIS Enterprise base deployment.

You will investigate each of these components in more depth.

Instructions

- a In a web browser, go to <https://enterprise.arcgis.com>.
- b In the Search ArcGIS Enterprise Site field, type **base arcgis enterprise deployment** and press Enter.
- c Click the Base ArcGIS Enterprise Deployment help page result.

Explain the components of the base ArcGIS Enterprise (continued) deployment

d Review the information provided to answer the following question.



You will need to click links within this page to find the necessary information.

e After you are finished, keep your web browser open for the next activity.

What is the function of each component of the base ArcGIS Enterprise deployment?

ArcGIS Enterprise component	Function
ArcGIS Server	
Portal for ArcGIS	
Data Stores	
ArcGIS Web Adaptor	

Describe base deployment prerequisites and considerations

Before implementing your base ArcGIS Enterprise deployment, it is important to review the installation guides, including system requirements. You will now review these guides at a high level.

Instructions

- a In the top-left corner of the ArcGIS Enterprise Help page, click ArcGIS Enterprise to return to the home page.
- b Search for and open the **ArcGIS Enterprise 11.5 System Requirements** help page.
- c Familiarize yourself with the installation guides and supporting documentation provided for each software component.



Specifically, review the system requirements for the various components of the base deployment.

- d Answer the following question.
- e After you are finished, close the web browser.

1. Which topics are important for your particular implementation?

How is a base deployment set up?

When setting up the base deployment, consider the following points:

- The components are installed individually.
- Each component is implemented in a two-step process:
 1. The software is installed (and licensed, if required).
 2. The component is configured (for example, the creation of an ArcGIS Server site).
- It can be done manually or by using automation tools, which configure the components in a seamless way (automation is preferred).

Base ArcGIS Enterprise setup

Installed component	Configured as	Licensing type (if required)
ArcGIS Web Adaptors	Portal for ArcGIS and ArcGIS Server registered	
Portal for ArcGIS	ArcGIS Enterprise portal	At least one Creator, Professional, or Professional Plus user type
ArcGIS Server	Hosting server	ArcGIS GIS Server
Data Store	Relational and object store	

How do you automate a base deployment?

ArcGIS Enterprise has automation tools, scripts, and templates to speed up and simplify the installation and configuration of a base ArcGIS Enterprise deployment. In addition, these automation methods make for a more repeatable and documentable approach to the installation process. The methods for installing and configuring ArcGIS Enterprise are described in the following table.

Automation option	Description
ArcGIS Enterprise Builder	An easy installation and configuration wizard that allows you to set up an all-in-one base deployment on a single machine in a little less than an hour.
Chef	An IT standard that allows you to use Esri-created cookbooks, which can be downloaded from GitHub (search: Esri ArcGIS Cookbook). The cookbooks contain recipes, which are scripts that you can modify or run directly to install and configure ArcGIS Enterprise. This option is beneficial if you will be doing a lot of repeat deployments. You can run the scripts over and over again, which minimizes human error.
Cloud machine images and templates	<p>When you deploy ArcGIS Enterprise in the cloud, you can use Esri-provided machine images that will specify the infrastructure for you and install and configure ArcGIS Enterprise. You will then have a fully functional system for which you only need to provide the licensing.</p> <p>Esri provides machine images for both the following options:</p> <ul style="list-style-type: none"> • Amazon Web Services (AWS): Using the AWS CloudFormation templates • Microsoft Azure: Using ArcGIS Enterprise Cloud Builder for Microsoft Azure

How do you automate a base deployment? (continued)

(Table continued from previous page)

Automation option	Description
PowerShell DSC (Desired State Configuration)	A Windows-based approach for installing, uninstalling, and upgrading ArcGIS Enterprise deployments on both single and multi-machine sites. Similar in concept to Chef automation, this option is delivered via the PowerShell Gallery . You can adjust the provided samples in the PowerShell for ArcGIS Repository to meet your configuration requirements before using the PowerShell console to install and configure ArcGIS Enterprise.

1. What are four tools available for automation when installing and configuring ArcGIS Enterprise?

2. What tools for installation automation could you use for a multi-machine configuration of ArcGIS Enterprise?



YouTube video: [Esri UC 2017: ArcGIS Enterprise—Improving Installation and Configuration](#)

Classroom PC environment

Your exercises predominantly involve the EBASE virtual machine (VM), both as a client machine and as the machine with the base configuration installed. Although you will not directly interact with the ADSRV2022 and EDATA VMs, these VMs are required to run the Windows domain and the enterprise database, respectively. All three VMs must be kept running throughout the class.

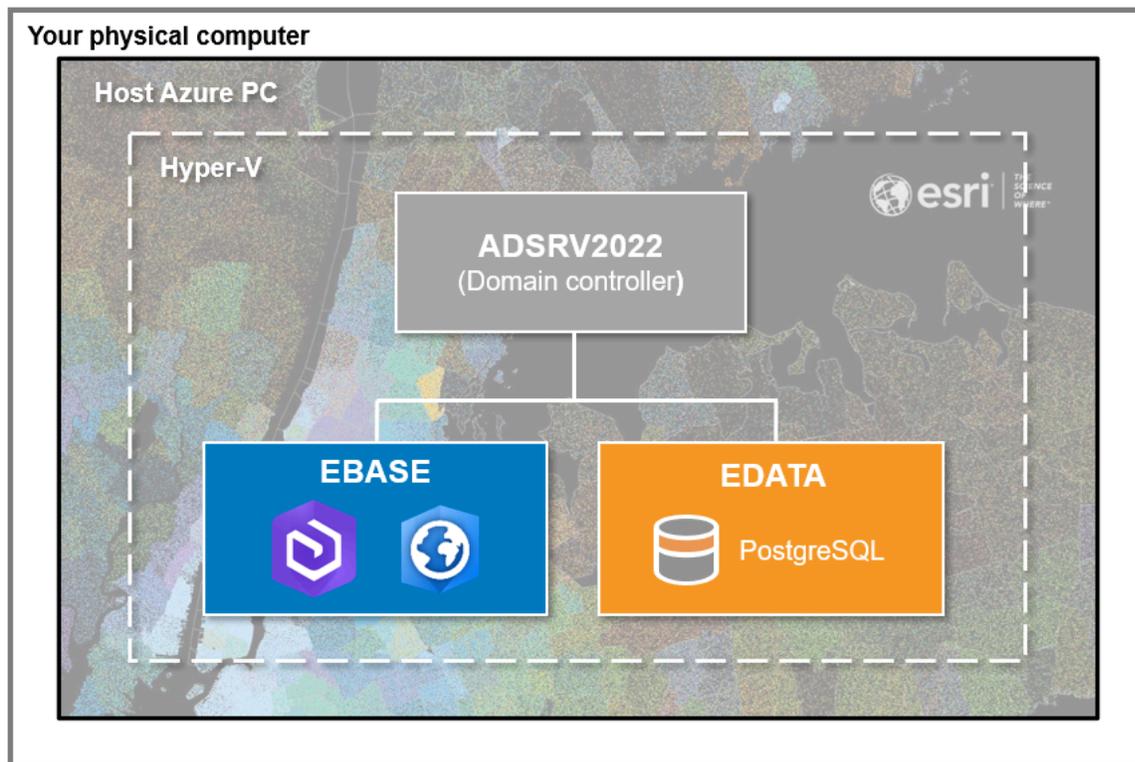


Figure 1.4. Three VMs make up the exercise environment.

Lesson review

1. Which components make up a base ArcGIS Enterprise deployment?

2. Which ArcGIS Enterprise automation tool always installs all the components on one machine?

- a. ArcGIS Enterprise Builder
- b. Chef cookbooks for ArcGIS
- c. ArcGIS Enterprise Cloud Builder for Microsoft Azure
- d. AWS CloudFormation templates

3. What are the two primary steps to implement each component of a base deployment?

Answers to lesson 1 questions

Explain the components of the base ArcGIS Enterprise deployment (page 1-5)

ArcGIS Enterprise component	Function
ArcGIS Server	ArcGIS Server is a server software component of ArcGIS Enterprise that makes your geographic information available to others who have appropriate permissions. Access sharing is accomplished through GIS services that allow a server computer to receive and process requests for information. There are two configuration options for ArcGIS Server: stand-alone site or federation within an ArcGIS Enterprise portal.
Portal for ArcGIS	Portal for ArcGIS is a software component that powers the Enterprise portal. The Enterprise portal provides an intuitive user interface for searching and using or creating GIS content. Users can create customizable or template-based web apps that can be made accessible to any device, anywhere, anytime. The Enterprise portal also facilitates a <i>self-service mapping</i> model that opens GIS to anyone in the organization who is a portal member.
Data Stores	Data Stores act as clearinghouses for content published through the Enterprise portal. A base deployment requires a relational and object data stores. This functionality can be implemented using the ArcGIS Data Store or through a supported cloud service.
ArcGIS Web Adaptor	ArcGIS Web Adaptor enables organizations to configure access to ArcGIS Enterprise through their own web server. The base deployment includes two instances of Web Adaptor, one configured with the portal and one with the hosting server.

Answers to lesson 1 questions (continued)

Describe base deployment prerequisites and considerations (page 1-7)

1. Which topics are important for your particular implementation?

Possible responses include the following topics:

- **Hardware requirements**
- **Software requirements**
- **Domain certificates**
- **Firewall settings/ports use**

How do you automate a base deployment? (page 1-9)

1. What are four tools available for automation when installing and configuring ArcGIS Enterprise?

ArcGIS Enterprise Builder, Chef scripts, cloud image templates, and PowerShell DSC for ArcGIS

2. What tools for installation automation could you use for a multi-machine configuration of ArcGIS Enterprise?

Chef scripts, cloud image templates, and PowerShell DSC for ArcGIS

2

Configuring a secure environment

The software components of the base ArcGIS Enterprise deployment communicate with each other using HTTP.

In this lesson, you will learn how each ArcGIS Enterprise component functions and communicates. You will also enable HTTPS encryption to ensure that all communication is protected.

Topics covered

■ Base deployment component communication

■ HTTPS encryption within a base deployment

Identify component communication

ArcGIS Enterprise components communicate with each other over your network. Each component uses a different set of communication parameters. In this activity, you will determine the network ports used by each base deployment component.

Instructions

- a In a web browser, go to <https://enterprise.arcgis.com>.
- b In the Search ArcGIS Enterprise Site field, type **ports used by base ArcGIS Enterprise components** and press Enter.
- c Review the help topics for each base Enterprise deployment component in the following diagram, then answer the questions that follow.
- d After you are finished, close the web browser.

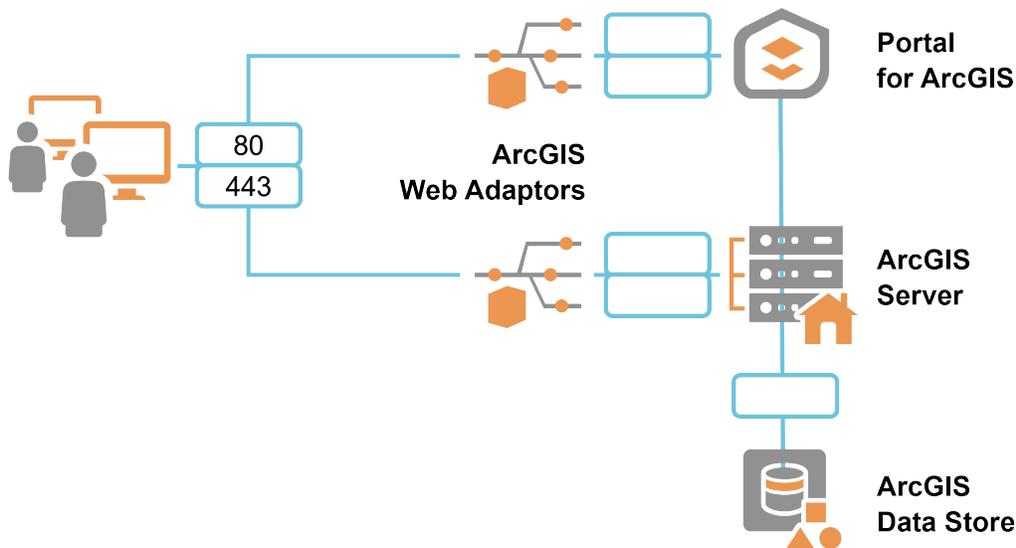


Figure 2.1. This graphic shows the communication between the components that compose the base ArcGIS Enterprise deployment.

Identify component communication (continued)

1. What default ports do the components use for HTTP and HTTPS communication?

2. What could affect component communication on your organization's network?



ArcGIS Enterprise Help: *Ports used by Portal for ArcGIS*

ArcGIS Enterprise Help: *Ports used by ArcGIS Server*

ArcGIS Enterprise Help: *Ports used by ArcGIS Data Store*

Using certificates to enable HTTPS encryption

ArcGIS Enterprise can be configured to use secure HTTPS communication. The HTTPS protocol provides authentication and protection of the privacy and integrity of data exchanged between a user and a website. Web browsers are able to trust HTTPS websites based on certificate authorities (CA).

ArcGIS Enterprise can be used with three types of certificates: self-signed, domain CA-signed, and well-known CA-signed.

Certificate type	Potential uses
Self-signed	As the owner of a website, you can issue self-signed certificates that originate from the local web server. This type of certificate is only recommended for testing and development within your organization's internal network.
Domain CA-signed	If your deployment is behind your organization's firewall, a domain CA-signed certificate can be used for production environments. This type of certificate is signed by your organization's certificate authority for internal use.
Well-known CA-signed	If your deployment is accessible over the Internet, a well-known CA-signed certificate is recommended for production environments. A well-known CA is typically a trusted third party that issues digital signatures to verify that the certificate can be trusted.

Using certificates to enable HTTPS encryption (continued)

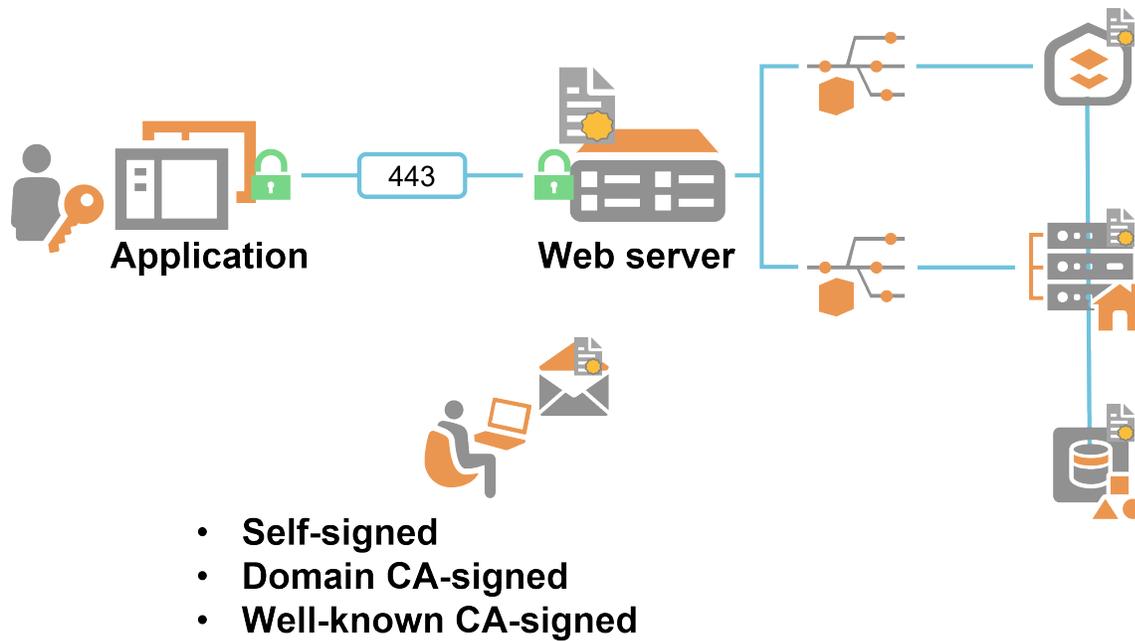


Figure 2.2. Certificates enable secure HTTPS communication at all levels of client/server interaction.

To have a secure ArcGIS Enterprise environment, you need to have a certificate chain that links back to a trusted CA. The root certificate establishes the credibility of the CA signing the certificate by linking it back to a trusted CA.

If you acquired your certificate from a well-known CA, the root certificate is likely already recognized by the ArcGIS component that you are configuring. As a result, the certificate chain is likely already established for you. If you are utilizing any certificate other than a well-known CA-signed certificate, you will need to import the root certificate into the appropriate components to establish the certificate chain back to your CA.

Root certificate

- Establishes the certifying authority's credibility
- Provides validation for all server certificates, as well as any intermediate certificates in the certificate chain
- Must be stored in the trust stores of web clients

Using certificates to enable HTTPS encryption (continued)

Server certificate

- Establishes trust between clients and the server
- Establishes a secure connection between server and client
- Administrator provides the certificate to server applications



ArcGIS Enterprise Help: *Enable HTTPS on your web server - Portal for ArcGIS*

ArcGIS Enterprise Help: *Restrict TLS protocols and cipher suites*

Enable HTTPS encryption

HTTPS communication provides a secure environment for passing credentials and information. To prepare for a secure-base ArcGIS Enterprise deployment, you will set up your web server to support encrypted HTTPS communication.

In this exercise, you will perform the following tasks:

- Inspect the root certificate.
- Bind the certificate to HTTPS.
- Verify HTTPS communication.

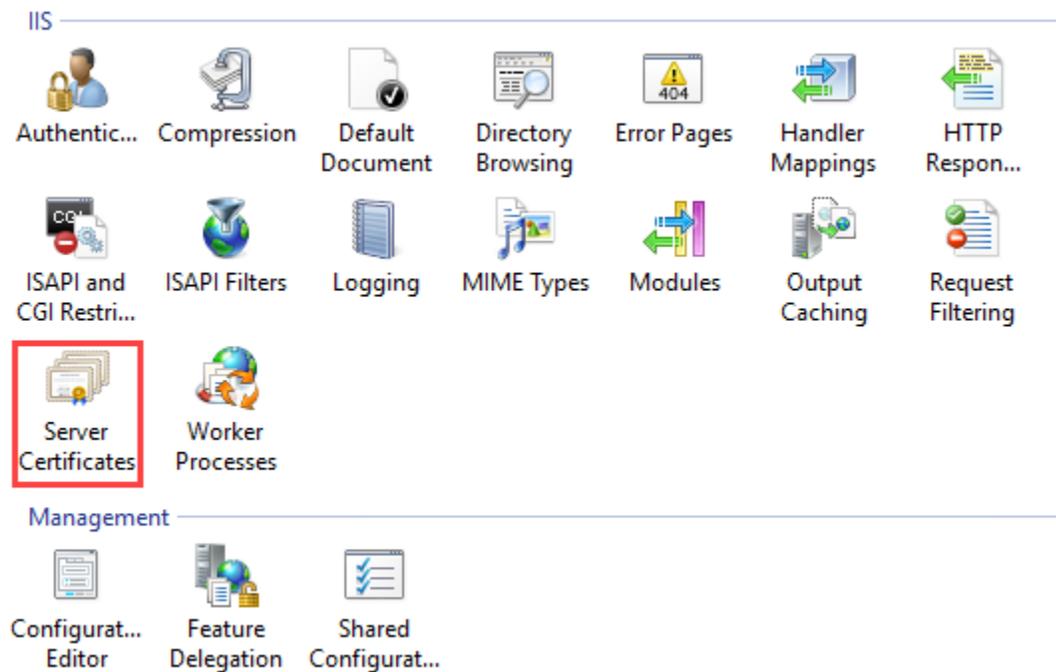
Step 1: Inspect the root certificate

To begin, you will use IIS Manager to inspect the current domain CA-signed certificate that has been created for your web server.

- a On the host PC desktop, double-click the EBASE.rdp shortcut.
- b Enter the account **adAdmin** and password **Esri.4.GIS**, if necessary.
- c The EBASE VM window (blue desktop) appears.
- d Open IIS Manager.

Hint: Click the Start button and type **iis**.

- e In the middle pane, locate and double-click the Server Certificates feature to open it.



Your organization's IT department has created a domain CA-signed certificate for you to use with your base ArcGIS Enterprise deployment. The department has also added the root certificate for the domain CA to the trusted certificate store.

1. What is the name of the certificate and to what machine is it issued?

Next, you will export the certificate for an upcoming configuration step.

- f** Right-click the certificate and choose Export.
- g** In the Export Certificate window, under the Export To parameter, follow these steps to set the export location:
 1. To the right of the text input, click the three dots.
 2. In the File Explorer window, locate the Quick Access icons at left and click `_sw`.
 3. Open the Authorization folder and, for File Name, type **server_cert.pfx**.
 4. Click Open.

The Export To parameter will read `\\BaseVMGen2\Users\student\Desktop_sw\Authorization\server_cert.pfx`.



You will use the `_sw` folder on the host machine (BaseVMGen2 with the map desktop image) periodically throughout the course. This folder has been pinned to the Quick Access pane on the EBASE (blue desktop) machine for easier access.

- h** For the next two parameters, specify the following parameters:
 - Password: **Esri.4.GIS**
 - Confirm Password: **Esri.4.GIS**
- i** Click OK.

You have generated a server certificate that you will use throughout the course to establish HTTPS communication.

Step 2: Bind the certificate to HTTPS

To take advantage of HTTPS encryption, you must first bind your domain CA-signed certificate to HTTPS traffic in IIS Manager.

- a** In the IIS Connections tree, expand Sites and select Default Web Site.

- b** Right-click Default Web Site and choose Edit Bindings.
- c** Click Add.
- d** Change Type to https.
- e** For SSL Certificate, choose ebase.ad.local.

The screenshot shows the 'Add Site Binding' dialog box. The 'Type' dropdown is set to 'https'. The 'IP address' dropdown is set to 'All Unassigned'. The 'Port' text box contains '443'. The 'Host name' text box is empty. There are several unchecked checkboxes: 'Require Server Name Indication', 'Disable TLS 1.3 over TCP', 'Disable QUIC', 'Disable Legacy TLS', 'Disable HTTP/2', 'Disable OCSP Stapling', and 'Negotiate Client Certificate'. The 'SSL certificate' dropdown is set to 'ebase.ad.local'. There are 'Select...' and 'View...' buttons next to the dropdown. At the bottom right, there are 'OK' and 'Cancel' buttons.

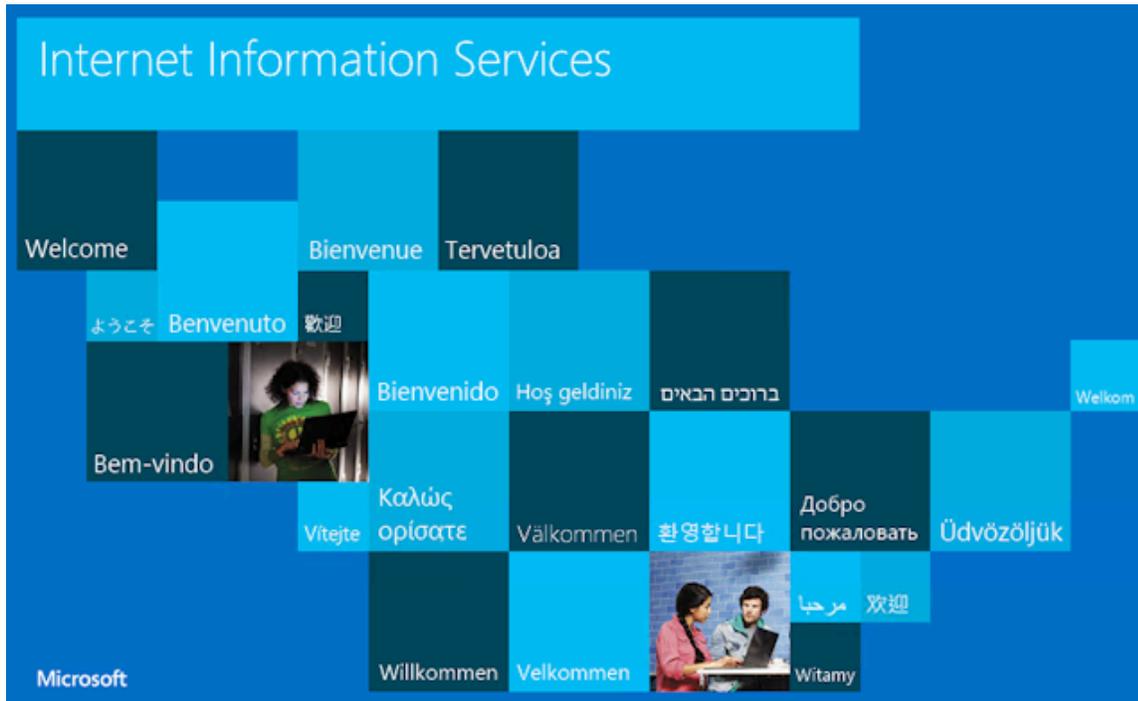
- f** Click OK.
- g** Close the Site Bindings window.

All HTTPS traffic will now be accepted by your web server using the domain CA-signed certificate that you specified. In the next step, you will test that HTTPS communication is working properly.

Step 3: Verify HTTPS communication

To ensure that your domain CA-signed certificate is properly bound to your web server's secure HTTPS port (443), you will now test HTTPS communication.

- a** In a web browser, go to **https://ebase.ad.local**



The default IIS landing page appears.

- b** At the top of the browser, click the View Site Information button .

A padlock icon in the site information is a visual indicator that your HTTPS communication and domain CA-signed certificate are working properly.

2. What kind of HTTPS certificate will you use for your base Enterprise deployment?

- c** Close all open windows in the EBASE VM.

Workflow review

In this lesson, you configured IIS to support HTTPS communication using web certificates. This configuration is the first step of the ArcGIS Enterprise deployment process.

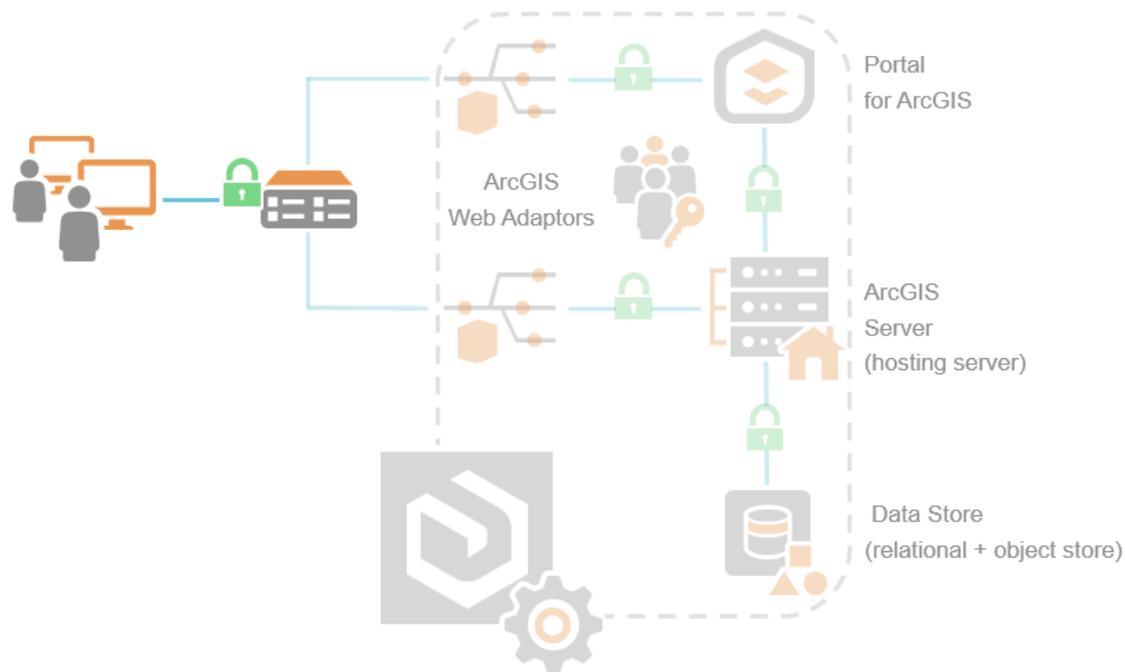


Figure 2.3. A base ArcGIS Enterprise deployment requires that a certificate-based, secure environment has been configured and that the components can communicate with each other over their default network ports.

1. Why might you want to use HTTPS encryption in your ArcGIS Enterprise deployment?

2. Why is it important to know which network ports the ArcGIS Enterprise components use?

Answers to lesson 2 questions

Identify component communication (page 2-2)

1. What default ports do the components use for HTTP and HTTPS communication?

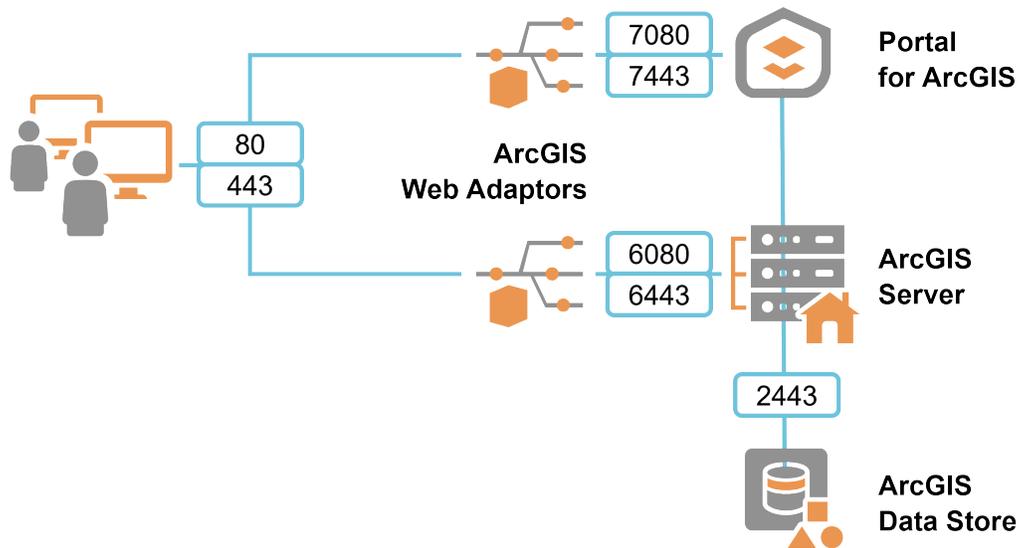


Figure 2.4. This graphic shows the communication between the components that compose the base ArcGIS Enterprise deployment.

Portal for ArcGIS: 7080 and 7443; ArcGIS Server: 6080 and 6443; ArcGIS Data Store: 2443

2. What could affect component communication on your organization's network?
 - Hardware firewall
 - Software firewall
 - Antivirus or security software
 - Existing application using the port

Exercise 2: Enable HTTPS encryption (page 2-7)

1. What is the name of the certificate and to what machine is it issued?

The certificate is named `ebase.ad.local` and is issued to `ebase.ad.local`.

Answers to lesson 2 questions (continued)

2. What kind of HTTPS certificate will you use for your base Enterprise deployment?

Answers will vary based on individual requirements.

Workflow review (page 2-12)

1. Why might you want to use HTTPS encryption in your ArcGIS Enterprise deployment?

Answers will vary but may include:

- **Secures connections between servers and clients**
- **Prevents others from accessing sensitive information**
- **Required by our organization or industry**

2. Why is it important to know which network ports the ArcGIS Enterprise components use?

The appropriate port must be open for components to function.

3

Setting up an ArcGIS Enterprise portal

Once Portal for ArcGIS is installed and configured, it activates the ArcGIS Enterprise portal. The ArcGIS Enterprise portal presents your user with a user-friendly, mapcentric site to search, use, and share content within your organization.

You have already learned that it is a system requirement that each component's network ports are open and available for use. You are now ready to learn about the Portal for ArcGIS install process and its associated ArcGIS Web Adaptor.

Topics covered

- Portal for ArcGIS installation and configuration

- Portal for ArcGIS user account

- ArcGIS Web Adaptor installation and configuration

Portal for ArcGIS installation overview



Before beginning the Portal for ArcGIS installation, verify that your machine meets the minimum system requirements. In addition to ensuring that the default network ports are open, ensure that your machine's hardware and software meet the minimum requirements.

After you have verified your machine's system requirements, there are several important parameters that you must specify during installation that require some planning.

Installation parameters

Parameter	Notes
Installation directory location	<ul style="list-style-type: none"> • Default is C:\Program Files\ArcGIS\Portal
Portal for ArcGIS (root) directory	<ul style="list-style-type: none"> • Default is C:\arcgisportal
Portal for ArcGIS account	<ul style="list-style-type: none"> • Default is a local operating system account named <i>arcgis</i>
License	<ul style="list-style-type: none"> • Must include at least one compatible user type (Creator, Professional, or Professional Plus) to complete configuration • Can be generated at https://my.esri.com
Initial administrator account	<ul style="list-style-type: none"> • Not an operating system account • Compatible user type (Creator, Professional, or Professional Plus) with an Administrator role

Portal for ArcGIS installation overview (continued)

(Table continued from previous page)

Parameter	Notes
Content directory location	<ul style="list-style-type: none"> • Default is C:\arcgisportal\content • Contains an indexed database of your organization's resources and critical system files • Size will grow as your organization adds groups and content

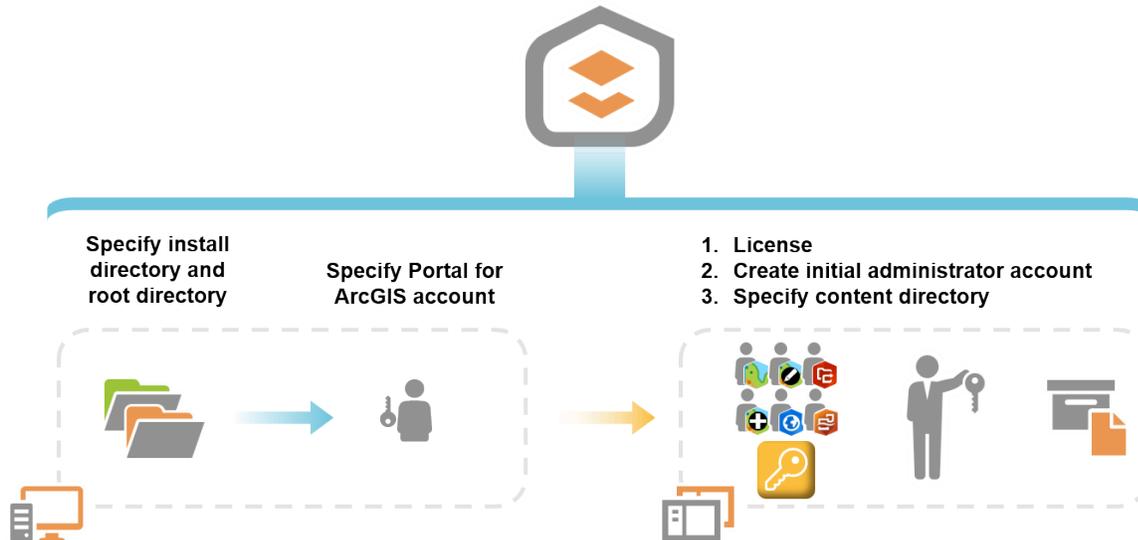


Figure 3.1. The order of operations for Portal for ArcGIS installation are: Specify the install directory and root directory, specify the Portal for ArcGIS account, license Portal for ArcGIS, create the initial administrator account, and specify the content directory.

Licensing members in your Enterprise portal

Each member in your Enterprise portal must be assigned a user type, which describes the privileges and apps that are accessible to the member. There are several available user types, which can be tailored to meet the needs and requirements of each member through roles. The process for obtaining a Portal for ArcGIS license file includes specifying the quantity of each user type required by your organization.

Portal for ArcGIS installation overview (continued)

An initial administrator account is required for the installation and configuration of Portal for ArcGIS. To set up this account the Portal for ArcGIS license must include at least one Creator, Professional, or Professional Plus user type. These user types are compatible with the Administrator role, which provisions full privileges within an Enterprise portal.



You will learn more about the available user types and roles later in the course.



The content directory will grow as your users add content to the Enterprise portal. Consider configuring a location with ample, redundant storage (the location can also be changed after the initial configuration).



ArcGIS Enterprise Help: Portal for ArcGIS system requirements

ArcGIS Enterprise Help: Steps to get Portal for ArcGIS up and running

ArcGIS Enterprise Help: Changing the portal content directory

Portal for ArcGIS account

The Portal for ArcGIS account must be specified during installation. The account's credentials are used to start and run the Portal for ArcGIS service. They are also used to access the Portal for ArcGIS software directory and content store.



The account can be changed or updated at any time after installation using the Portal for ArcGIS `configure-service-account` utility.

Portal for ArcGIS Account types

The Portal for ArcGIS Account can be a local account, a domain account, or a group managed service account (gMSA). By default, a local account named `arcgis` will be created during installation unless you change this parameter. The type of user account can be identified by how it is formatted. Local accounts are notated as `.username`, domain accounts as `domain\username`, and gMSA accounts as `domain\username$`.



Specifying a domain account or group managed service account that conforms to your organization's security policy is recommended for production systems.

If configuring the Portal for ArcGIS account's password to never expire can be aligned with your organization's security policies, consider this option to avoid service downtime. Otherwise, plan this account's password changes accordingly to maintain uninterrupted uptime for the Portal for ArcGIS service.

Portal for ArcGIS account (continued)

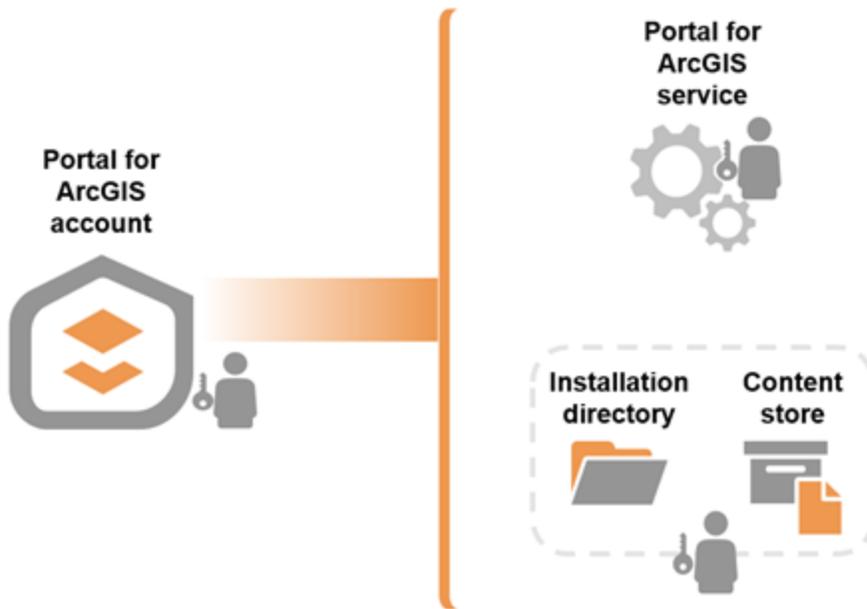


Figure 3.2. The Portal for ArcGIS account is granted specific privileges during installation that control different aspects of the configuration. These include control of the Portal for ArcGIS service, installation directory, and content store.

For each requirement for Portal for ArcGIS, choose the appropriate account that provides the required functionality domain, local, or gMSA account.

Portal for ArcGIS account (continued)

Portal for ArcGIS Need	Account type
Automatic password management from Active Directory	
Simple account management to set up a test machine	
Central management of the Portal for ArcGIS account with a credential known only by domain administrators	
Restrict the account to only a list of predefined servers	
Automatically use the organization's security policies	



ArcGIS Enterprise Help: *Changing the Portal for ArcGIS account*

Complete a Portal for ArcGIS installation

Installing Portal for ArcGIS is the first step to beginning your base deployment implementation. For this exercise, assume that Portal for ArcGIS has already been installed by your IT department but that you still need to license and configure the initial setup of your portal site.

In this exercise, you will perform the following tasks:

- License Portal for ArcGIS.
- Create the initial portal administrator account.
- Complete the initial configuration of your portal.

Step 1: Begin the portal configuration

When you run the Portal for ArcGIS installer your default browser is launched to complete the initial configuration. Portal for ArcGIS has already been installed on the EBASE machine but it has not been configured. In this step, you will configure Portal for ArcGIS.

Because you did not run the installer, you will need to launch the configuration wizard manually.

- a Verify that you are working in the EBASE VM (blue desktop).
- b Click the Start button, and then, to the right of the Pinned section header, click All to open the full application list.
- c Expand the ArcGIS program group.
- d Locate and click the Portal For ArcGIS item.

Your default browser launches and attempts to load the page. You will receive a message that the site is not trusted. By default, the link uses localhost instead of the fully qualified domain name (FQDN).

- e In the URL, replace localhost with the FQDN (**ebase.ad.local**).

The URL should now read `https://ebase.ad.local:7443/arcgis/home`.

- f Press Enter.

When Portal for ArcGIS is installed, it comes with a self-signed certificate. The site's internal self-signed certificate is not trusted.

- g Click Advanced, and then click Proceed To ebase.ad.local (Unsafe).



The Create Or Join A Portal page may take several minutes to load.

If you were implementing a highly available configuration, you could join an existing portal here.

Step 2: Use a license file to authorize the portal

Next, you will begin creating a new portal for your organization, which will require a license.

- a Click Create New Portal.

To get started, choose to either create a new portal or join this machine to an existing portal.



- b For License File, click Choose File.
- c Browse to `\\BaseVMGen2\Users\student\Desktop_sw\Authorization` and open the `115_ENT_Portal_2026.json` file.
- d Click Next.

Now that the license for your portal has been activated, you can finish the portal configuration process.

Step 3: Configure the initial portal administrator account

Portal for ArcGIS requires an internal administrator account with full site privileges. This account is not an operating system account; it only exists within the portal site.

- a Complete the fields using the following values:
 - Username: **portaladmin**
 - Password: **Esri.4.GIS**
 - Confirm Password: **Esri.4.GIS**

Username

Password

Confirm password

User type ⓘ

- b** Click Next.
- c** Complete the remaining details for the initial administrator account with the following information:

- First Name: **portaladmin**
- Last Name: **built-in**
- Email: **portaladmin@ad.local**
- Confirm Email: **portaladmin@ad.local**
- Security Question: What City Were You Born In?
- Answer: **Redlands**

First name

Last name

Email

Confirm email

Security question

Answer

- d** Click Next.

The Content Directory parameter is set to C:\arcgisportal\content by default. Remember that the content directory will grow in size as your users add content to the portal. Therefore, choose a location with adequate disk space before exposing the portal to end users.

e Click Next.

f Click Create.



It will take approximately 10 minutes to create the new portal and administrator account. You will leave the portal creation process running in the background.

g Minimize the browser with the creation window for the next activity.

Identify properties of the Portal for ArcGIS content directory

The ArcGIS portal content directory is essential to your portal's functionality. Now that you have installed Portal for ArcGIS, you will examine the ArcGIS portal content directory to understand its contents and properties.

Instructions

- a** Open File Explorer and browse to **C:\arcgisportal**.
- b** Right-click the Content folder and choose Properties.
- c** Use the Content folder properties to answer the following questions.
- d** After you are done, close the Properties window and File Explorer.

1. How big is the Content folder?

2. Why might the Content folder change size as the ArcGIS Enterprise deployment is used?

Checkpoint

1. What is the default Portal for ArcGIS HTTPS port?
 - a. 443
 - b. 7080
 - c. 7443
 - d. 2443

2. Your portal site will automatically use your web server's certificate.
 - a. True
 - b. False

ArcGIS Web Adaptor

ArcGIS Web Adaptor works in concert with your web server to route client and server traffic, acting as a reverse proxy application. Within high-availability contexts, it acts as a load balancer.

In a base deployment, separate ArcGIS Web Adaptors are installed for both Portal for ArcGIS and ArcGIS Server.

ArcGIS Web Adaptor benefits

- It integrates Portal for ArcGIS with your organization's existing web server, allowing you to host web applications that use your GIS services.
- You can use your organization's identity store and security policies at the web tier.
- It allows you to set a different site name than the default of *arcgis* (for example, a name that reflects your organization's identity).
- You can expose the portal through standard ports (80 or 443).



ArcGIS Web Adaptor is available in two different editions: IIS (Windows only) and Java Platform (Windows or Linux). Each edition has its own set of system requirements.

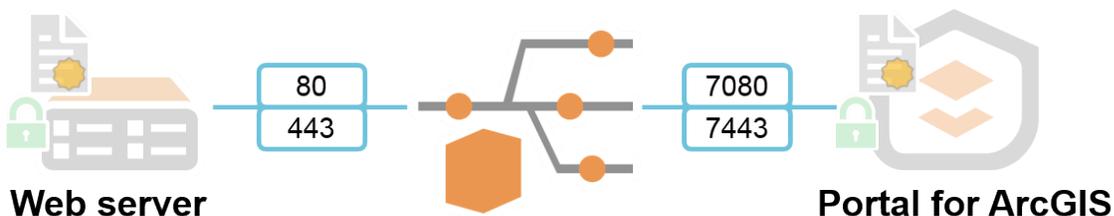


Figure 3.3. ArcGIS Web Adaptor routes and optimizes traffic between your web server and Portal for ArcGIS.



ArcGIS Enterprise Help: [Install ArcGIS Web Adaptor](#)

ArcGIS Enterprise Help: [Import a certificate into the portal](#)

Integrate ArcGIS Web Adaptor

Your portal's site is running with an initial administrator account. You will now integrate your organization's web server with the portal site by installing and configuring ArcGIS Web Adaptor.

In this exercise, you will perform the following tasks:

- Install and configure ArcGIS Web Adaptor.
- Import and configure a certificate for your Enterprise portal site.
- Validate your Portal for ArcGIS installation.

Step 1: Install and configure ArcGIS Web Adaptor

Now, you will complete the initial installation and configuration of ArcGIS Web Adaptor for your portal.

- a Locate the browser tab that shows the portal configuration and ensure that the initial administrator account creation process is complete.

- b Read the information in the Account Created dialog box.



If you do not see the dialog box, keep the browser open and wait until the dialog box appears. After the initial administrator account is created, the portal site restarts.

- c In the Account Created dialog box, click OK.

- d Choose to save the account credentials, if prompted.



It will take several minutes to complete the portal initiation.

- e Close the browser.

- f Open File Explorer and browse to `\\BaseVMGen2\Users\student\Desktop_sw\WebAdaptor\IS`.

- g Double-click Setup.exe to launch the ArcGIS Web Adaptor setup wizard.

- h Continue through the prompts, accepting the Master Agreement, until you get to the Select Web Site For The Web Adaptor dialog.

The installer detects that you have multiple websites configured on your web server. Because you will be implementing HTTPS for your organization, you will install ArcGIS Web Adaptor on that site.

- i Select Default Web Site (443).

Web site (Port):

Default Web Site (80)
 Default Web Site (443)

j Click Next.

A virtual directory will be created on your web server as part of the installation. You can change this value from the default value if desired. The directory name will be included within all ArcGIS Enterprise service URLs.

k Replace the default virtual directory name with **portal**, and then click Next.

l Click Install.

m Click Finish.

The software components are installed before your default browser launches to the Web Adaptor configuration page.

n In the URL, replace localhost with the FQDN and press Enter.

Hint: The FQDN is **ebase.ad.local**.

The page loads successfully using the domain CA-signed certificate on HTTPS.

o Select Portal For ArcGIS, and then click Next.

Which component do you want to configure with your web adaptor?

- GIS, Image, Workflow Manager, or Knowledge Server
- Portal for ArcGIS
- Notebook Server
- Mission Server
- Video Server
- ArcGIS Monitor



This web adaptor is not configured with an ArcGIS Enterprise component.

p For the Portal Name parameter, type **ebase.ad.local**, the FQDN.

q Type the credentials for the initial administrator account that you created previously.

Hint: Username is **portaladmin** and Password is **Esri.4.GIS**.

To configure the Web Adaptor, specify the URL and an administrator account for your Portal.

Portal Name:	<input type="text" value="ebase.ad.local"/>	?
	Example: portal.domain.com	
Administrator Username:	<input type="text" value="portaladmin"/>	?
Administrator Password:	<input type="password" value="●●●●●●●●"/>	?

 A portal is not configured with your Web Adaptor.

r To begin the ArcGIS Web Adaptor configuration process, click Configure.



It will take a few minutes for the configuration to complete.

The registration of the portal Web Adaptor will take several minutes to complete because a full re-indexing of portal items is triggered as a part of this process. When the process completes, a message appears confirming that your portal has been successfully configured with your ArcGIS Web Adaptor.

The following portal is successfully configured with your web adaptor:

- EBASE.AD.LOCAL



Last updated on 7/8/2025 2:38:19 AM

Use the following URL to access your portal application:

<https://ebase.ad.local/portal/home>

Step 2: Validate your Portal for ArcGIS installation

Next, you will load your portal's main home page to verify that it is functioning on a basic level.

a In the browser, open a new tab and click the ArcGIS Enterprise bookmark to go to the portal.

The portal's home page loads using HTTPS with your root certificate.

b Click Sign In.

- c Type the initial administrator account's credentials and click Sign In.

Hint: The username is **portaladmin**, and the password is **Esri.4.GIS**.



If prompted to save your username and password, click Save.

You are automatically taken to the Organization tab. Your initial administrator account is currently the only member.

Your portal's site is now running together with its ArcGIS Web Adaptor and your organization's web server which ensures that clients can connect securely.

Step 3: Import and configure a certificate for your Enterprise portal site

In the previous step, you saw that your web server's domain CA-signed certificate was properly processing HTTPS requests. Your portal site comes with a self-signed certificate. Replacing the self-signed certificate with your domain CA-signed certificate will enhance the security of your deployment, so you will import it now with the Portal Administrator Directory.

- a Open a browser and go to **<https://ebase.ad.local:7443/arcgis/portaladmin>**.

- b If necessary, click Advanced, and then click Proceed To ebase.ad.local.

The Portal Administrator Directory allows you to perform advanced management tasks for your portal. You can use its API to develop management scripts if desired.

- c On the ArcGIS Portal Administrator Site Directory page, click Login.

- d Provide your initial administrator account credentials and click Sign In.

Hint: Username is **portaladmin** and Password is **Esri.4.GIS**.

- e From the Site Root page, click Security and choose SSLCertificates.

Two SSL certificates already exist within your portal's site: *portal* and *samlcert*. The portal certificate is the self-signed certificate that was created automatically when you installed and configured your portal. You will begin by importing the root certificate.

- f Click Import Root Or Intermediate.

You must import the root certificate into the portal to establish the certificate chain with the

certificates provided by other components.

- g For Alias, type **domain_root**.
- h Check the box for the Do Not Restart The Portal After Import option.

The portal will be restarted after you import the certificate in a later step.

- i For File, click Choose File, and open the root certificate at **\\BaseVMGen2\Users\student\Desktop_sw\Authorization\adRoot.cer**.
- j Change the Format parameter to HTML, if necessary.

Alias:

Do not restart the portal after import:

File * adRoot.cer

Format ▼

- k Click Import.

Now that you have established the portal's trust with your certifying authority, you will import the certificate that you exported from your domain earlier.

- l At the bottom of the page, next to Supported Operations, click Import Existing Server Certificate.
- m For Certificate Password, type **Esri.4.GIS**.
- n For Alias, type **server_cert**.
- o For File, click the Choose File button, browse to **.._sw\Authorization**, and then open the server_cert.pfx file.
- p Verify that the Format parameter is set to HTML.
- q Click Import.

Your root certificate now appears in the list at the top of the page. You must still update the

portal's configuration so that it will use this certificate.

- r** At the bottom of the page, click Update.
- s** For Web Server SSL Certificate, type the alias of your server certificate (**server_cert**).
- t** Click Update.

Portal Administrator Directory

[Home](#) > [Security](#) > [SSLCertificates](#)

SSL Certificates

- [domain_root](#)
- [portal](#)
- [samcert](#)
- [server_cert](#)

Web Server SSL Certificate:	server_cert
Web Server SSL Protocols:	TLSv1.2,TLSv1.3
HTTP Strict Transport Security (HSTS) enabled:	false

- u** Wait several minutes for the portal site to fully restart before proceeding.
 - v** In a new tab, go to **https://ebase.ad.local:7443/arcgis/portaladmin**, and notice that the Not Secure icon in the browser's address bar no longer appears.
-  If the Portal Administrator Directory does not load, wait an additional minute, close and reopen browser to the Portal Administrator page.
- w** Close all open windows in the EBASE VM.

The portal site is restarted to commit the certificate update. You are automatically redirected to the previous page. The SSL certificate has been updated to the same one used by your web server. Now all client requests will use the same certificate from the web server to ArcGIS Web Adaptor to Portal for ArcGIS.

Workflow review

You have installed and configured the first two base deployment components: Portal for ArcGIS and its associated ArcGIS Web Adaptor. You have also ensured that your root certificate is used throughout the network path from clients, to the web server, and into your portal.

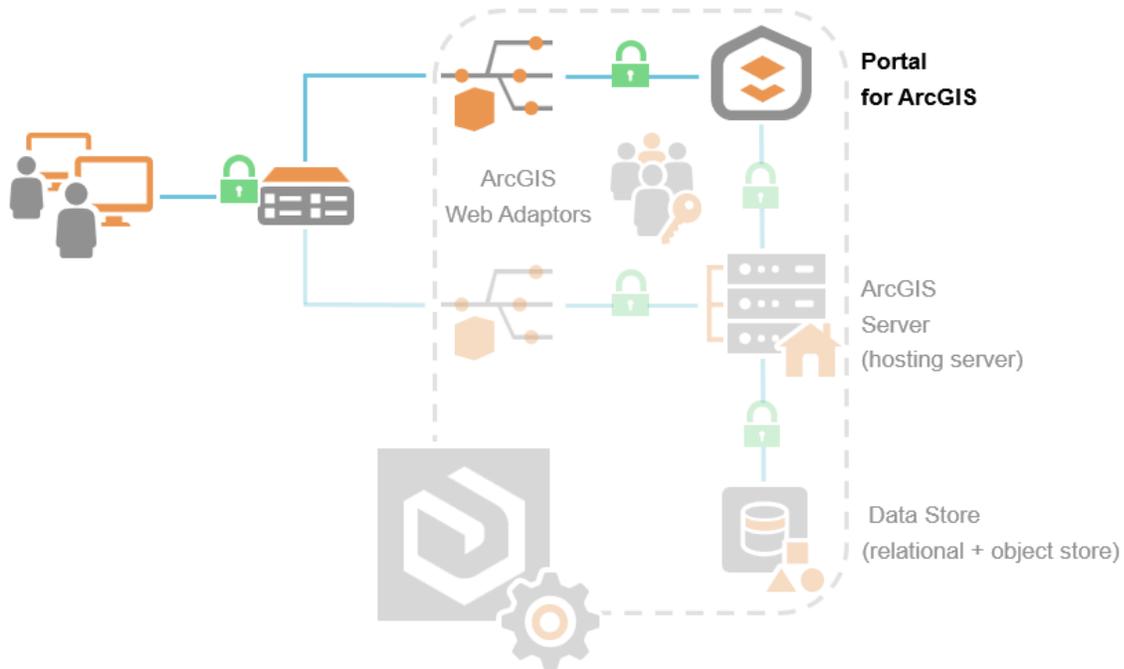


Figure 3.4. The base ArcGIS Enterprise deployment now includes a secure configuration of Portal for ArcGIS.

1. Where will you place your portal content store on your ArcGIS Enterprise configuration?
What are some considerations for where you place it?

Workflow review (continued)

- 2. What are some benefits of configuring ArcGIS Web Adaptor in relation to the portal for your organization?**

Answers to lesson 3 questions

Portal for ArcGIS account (page 3-5)

Portal for ArcGIS Need	Account type
Automatic password management from Active Directory	<ul style="list-style-type: none">• gMSA account
Simple account management to set up a test machine	<ul style="list-style-type: none">• Local account
Central management of the Portal for ArcGIS account with a credential known only by domain administrators	<ul style="list-style-type: none">• Domain account
Restrict the account to only a list of predefined servers	<ul style="list-style-type: none">• gMSA account
Automatically use the organization's security policies	<ul style="list-style-type: none">• Domain account• gMSA account

Identify properties of the Portal for ArcGIS content directory (page 3-13)

1. How big is the Content folder?

If the portal configuration is fully completed, the Content folder will be more than 2 GB.

If it is still configuring, then the file size will be smaller.

2. Why might the Content folder change size as the ArcGIS Enterprise deployment is used?

The directory is created to store content saved and uploaded by users of the portal. As content increases in the portal, the content folder will increase in size as well.

Answers to lesson 3 questions (continued)

Checkpoint (page 3-14)

1. What is the default Portal for ArcGIS HTTPS port?
 - a. 443
 - b. 7080
 - c. 7443
 - d. 2443
2. Your portal site will automatically use your web server's certificate.
 - a. True
 - b. False

(The portal site contains its own web server and self-signed certificate. It is important to understand that the certificates are different during implementation.)

Workflow review (page 3-23)

1. Where will you place your portal content store on your ArcGIS Enterprise configuration? What are some considerations for where you place it?

Answers will vary but may include:

- Place the content store in a location that is large enough for the amount of use that it will get.
- The content store will grow as the use of portal grows.
- Is the content store location available to the portal?

2. What are some benefits of configuring ArcGIS Web Adaptor in relation to the portal for your organization?

Answers will vary but may include:

- Acts as a reverse proxy to your portal server
- Aids in securing the portal connection
- Provides a custom URL for your portal

4

Setting up a GIS server

ArcGIS Server's role in your ArcGIS Enterprise base deployment is to provide core GIS functionality in the form of GIS services. These services are a powerful and flexible way to deliver spatial functionality to your entire organization.

In the base deployment, your users can easily search for, use, and share these services in your portal. To more seamlessly integrate your portal with your GIS server, you will use a process called federation. Federation creates an explicit trust arrangement between both sites, tightly integrating functionality and security.

Topics covered

■ Installation and configuration of ArcGIS Server

■ Federating an ArcGIS Server site with an Enterprise portal

ArcGIS Server installation overview



Before beginning the ArcGIS Server installation, verify that your machine meets the minimum system requirements (including ensuring that its default network ports are open).

Similar to the Portal for ArcGIS installation, the ArcGIS Server installation consists of two phases: installing the software and then creating or joining a site.

An operating system account is required for the ArcGIS Server installation. This account can be the same one that you specified for Portal for ArcGIS, or it can be a separate one.

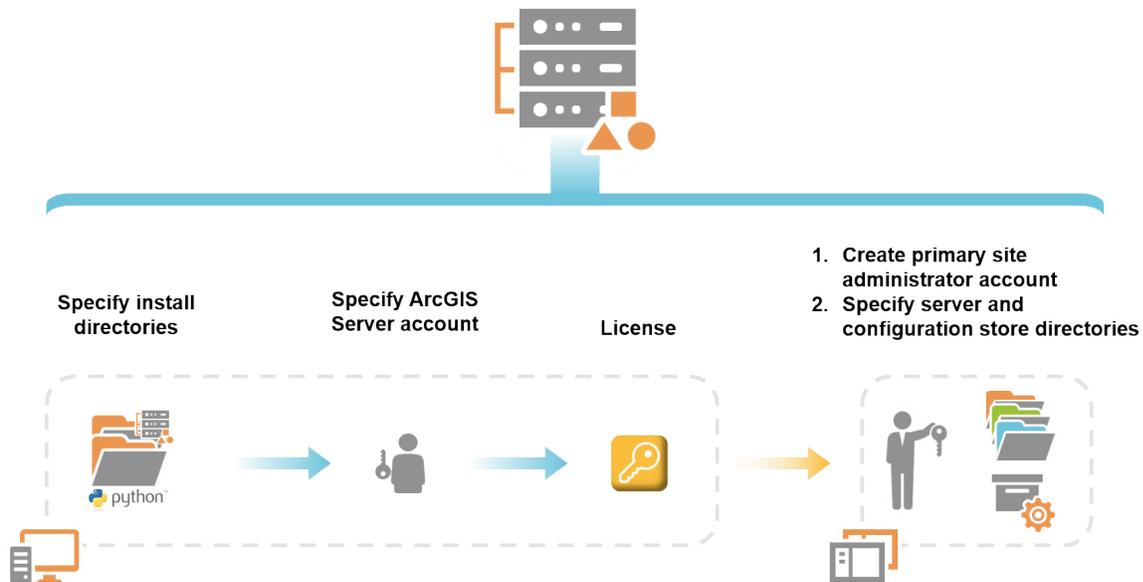


Figure 4.1. The sequence of operations for installing and configuring an ArcGIS Server site are: specify the install directories, specify the ArcGIS Server account, license ArcGIS Server, create the primary site administrator account, and specify the server and configuration store directories.

ArcGIS Server installation overview (continued)

Installation parameters

Parameter	Notes
Installation directory location	<ul style="list-style-type: none"> • Default is C:\Program Files\ArcGIS\Server
Python directory location	<ul style="list-style-type: none"> • Default is C:\Program Files\ArcGIS\Server\framework\runtime\ArcGIS\bin\Python
ArcGIS Server account	<ul style="list-style-type: none"> • Default is a local operating system account named <i>arcgis</i> • If desired, can be the same account specified for Portal for ArcGIS
License	<ul style="list-style-type: none"> • You can generate your license file at https://my.esri.com • Base deployment requires an ArcGIS GIS Server Standard or Advanced license
Primary site administrator account	<ul style="list-style-type: none"> • Account is created within the ArcGIS Server's site • Not an operating system account • Has full privileges to your ArcGIS Server site
Server directories and configuration store locations	<ul style="list-style-type: none"> • Default is C:\arcgisserver\directories and C:\arcgisserver\config-store • Production systems should have the configuration store on a fault-tolerant storage solution



ArcGIS Enterprise Help: *ArcGIS Server system requirements*

ArcGIS Enterprise Help: *Steps to get ArcGIS Server up and running*

Explore the ArcGIS Server installation

To save time, ArcGIS Server has already been installed for you. To fully understand the installation parameters, and to reinforce your knowledge of the ArcGIS Server account, you will spend some time exploring two resources:

1. The Windows service associated with ArcGIS Server
2. ArcGIS Enterprise documentation related to the ArcGIS Server account

Instructions

- a Open your EBASE VM (blue desktop).
 Maximize the window for the EBASE virtual machine, if necessary.
- b Click Start, type **services.msc**, and open the Services application.
- c Locate and open the properties for the ArcGIS Server service.
- d Answer the first question that follows in your workbook.
- e Close the service window and the Services application.
- f Open a web browser and go to **<https://enterprise.arcgis.com>**.
- g In the Search ArcGIS Enterprise Site field, type **arcgis server account** and press Enter.
- h Click the ArcGIS Server Account result.
- i Review the help topic to answer the second question that follows in your workbook.
- j After you are finished, close the web browser.

1. Which type of account has been specified for this service?

Explore the ArcGIS Server installation (continued)

2. How can you change the ArcGIS Server account while preserving its required privileges?



ArcGIS Enterprise Help: *The ArcGIS Server account*

Verifying accounts in Active Directory

When installing ArcGIS Server (and many other components of ArcGIS Enterprise), you must specify an operating system account. This account is used by ArcGIS Server (or other ArcGIS Enterprise components) to perform many necessary administrative tasks on the server machine. The ArcGIS Server account on the operating system is used to perform many tasks including starting and stopping ArcGIS Server services, read and write files to ArcGIS Server directories, and logging messages. Within the course environment, the Group Managed Service Account (gMSA) called `arcgis$` is used as the operating system account.



Within the class's VM configuration, the \$ symbol at the end of the account name indicates that the account is a gMSA account. gMSA accounts frequently use a \$ at the end of the account name to identify the account as a gMSA account.

The `arcgis$` gMSA account is located in the Active Directory of the Domain Controller machine called `ADSRV2022`. Then it can be accessed on the `EBASE` machine and used to install and run ArcGIS Server.



It is best practice to use a Group Managed Service Account (gMSA) created in the Active Directory as the ArcGIS Server operating system because it can manage the service account's password on multiple machines without the need for manual sign ins.

The `ADSRV2022`'s Active Directory also contains other accounts that can be used to provide access to ArcGIS Enterprise. These accounts include the `adPam` and `adPaul` accounts. In lesson

Verifying accounts in Active Directory (continued)

7, you will use the adPam account to publish content to your completed ArcGIS Enterprise base deployment.

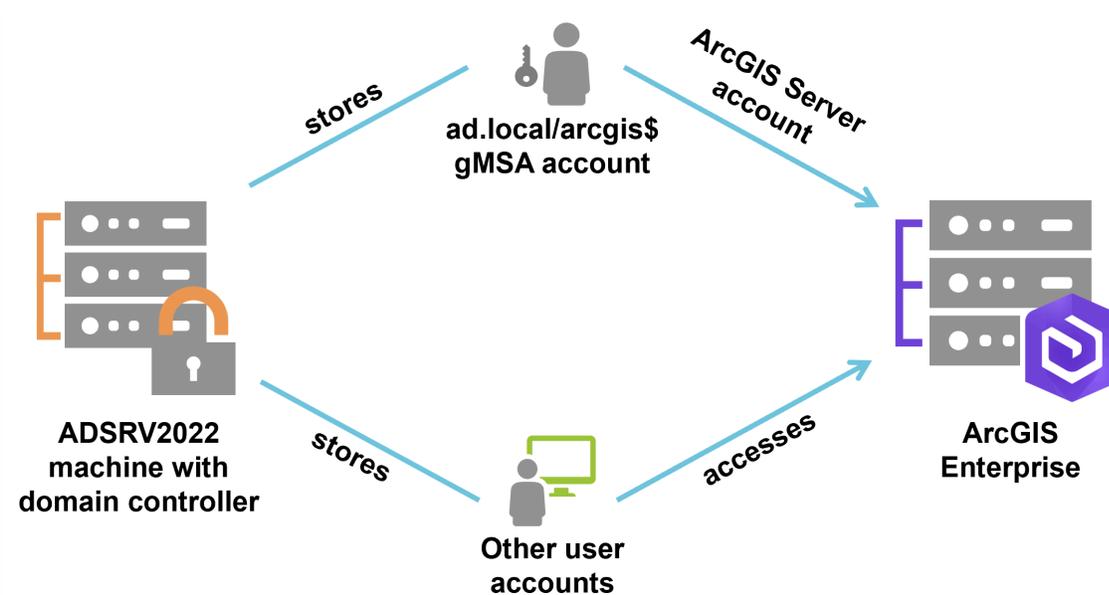


Figure 4.2. Within the course environment, you install your ArcGIS Enterprise base deployment on the EBASE machine. This includes installing ArcGIS Server. There is also a separate ADSRV2022 machine which contains the domain controller which controls the accounts that can be accessed by machines on the network. When installing ArcGIS Server, you use the gMSA account from the ADSRV2022 machine as the ArcGIS Server account. The domain controller also contains several other accounts which can be configured with ArcGIS Enterprise to authenticate users.

ArcGIS Server directories and configuration store

During the creation of your site, you are prompted to select the location of the ArcGIS Server directories and configuration store. You can choose to accept the defaults or customize. Understanding the functions of the directories and store will help you optimize them for your implementation.

ArcGIS Server directories

When ArcGIS Server processes client requests, it uses several physical directories to write, store, and read relevant information. Except for the cache directory, the temporary files in the directories are periodically removed. In addition to the default set of directories (except for the system directory), you can create additional ones to meet your site's requirements.



If you add to or edit the directories, ensure that the ArcGIS Server account has read and write access.

ArcGIS Server directories and configuration store (continued)

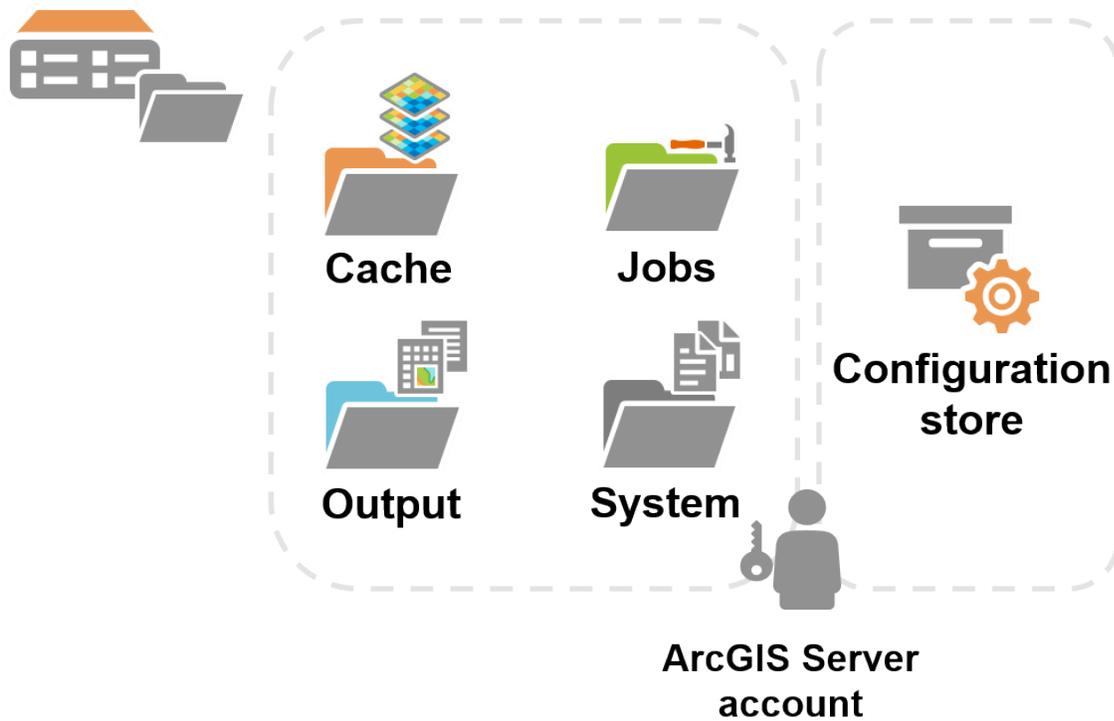


Figure 4.3. ArcGIS Server account controls the site directories including cache, jobs, output, and system. The ArcGIS Server account also controls the configuration store.

ArcGIS Server directories and configuration store (continued)

ArcGIS Server directories

Directory type	Notes
Cache	<ul style="list-style-type: none"> • Stores cached map service tiling data • Can be shared between multiple sites (for example, development and production) to separate the workload of cache creation from your production server
Jobs	<ul style="list-style-type: none"> • Stores temporary files generated while handling geoprocessing service requests
Output	<ul style="list-style-type: none"> • Temporary files related to geoprocessing, geographic data, map image, and web imagery layers are written here
System	<ul style="list-style-type: none"> • Manages information required for maintaining services, servers, and database connections • Each ArcGIS Server site can only have one system directory

ArcGIS Server configuration store

The ArcGIS Server configuration store contains system files that are critical to the functioning and health of the site. For multiple-machine server sites, this directory must be shared with the ArcGIS Server account as a UNC network path.



For mission-critical applications, locate the configuration store on a redundant storage system.



ArcGIS Enterprise Help: Server directories

ArcGIS Enterprise Help: Specify the configuration store location

Set up your ArcGIS Server site

The base ArcGIS Enterprise deployment requires that a GIS hosting server be installed. Your IT staff has already performed the software installation. You will complete the ArcGIS Server configuration by creating a server site, installing a web adaptor for ArcGIS Server, and then importing your domain CA-signed certificate.

In this exercise, you will perform the following tasks:

- Create your ArcGIS Server site.
- Install and configure your web adaptor.
- Import the web server certificate.
- Explore your site.

Step 1: Create the ArcGIS Server site

Because ArcGIS Server has already been installed, your first step will be to create a new ArcGIS Server site.

- a Maximize the EBASE VM (blue desktop) application window, if necessary.
- b Click the Start button, and then click All to open the full application list.
- c Expand the ArcGIS program group.
- d In the ArcGIS program group, click ArcGIS Server Manager.

The URL used by default directs to the internal web server, which uses a self-signed certificate. Your browser warns you that it could be a security risk.

- e Click Advanced, and then click Proceed To Localhost (Unsafe).

The ArcGIS Server Manager application is the administrative web app for configuring and managing ArcGIS Server. You will create a new site.

- f Click Create New Site.

[Help](#)

ArcGIS Server Setup Wizard

This machine does not currently participate in an ArcGIS Server site. You can either create a new site or join an existing site.



The Primary Site Administrator is an ArcGIS Server internal account that has full administrator privileges to the site.

- g Leave the Username as siteadmin, and then type **Esri.4.GIS** twice to confirm.
- h Click Next.

At this time, you will not be configuring a highly available implementation with multiple ArcGIS Server nodes. You will accept the default local paths. If you needed to change these paths later,

you could sign in as an administrator and modify them.



It is important to note that the server directories will be used to store data when the Copy all data option is selected during the publishing process. You should be aware of the system implications of using Copy all data and the option to disable this functionality if desired. For more information, go to ArcGIS Enterprise Help: *Copy data when publishing to ArcGIS Server*.

- i Click Next.
- j In the Configuration Summary window, click Finish to begin site creation.

It will take several minutes to create the site. When it completes, you are directed to the ArcGIS Server Manager web application. Before you sign in to Server Manager, you will install and configure the ArcGIS Server's web adaptor.

Step 2: Install the web adaptor

With your GIS server site created, you are ready to install its web adaptor.

- a Open File Explorer and browse to `\\BaseVMGen2\Users\student\Desktop_sw\WebAdaptorIIS`.
- b Double-click Setup.exe.
- c Advance through the ArcGIS Web Adaptor Setup wizard until you can select the protocol.

You will notice that you can select to install the web adaptor on either the HTTP or HTTPS port of your web server. Your organization's security policies require HTTPS, so you will select the port associated with that protocol.

- d Select Default Web Site (443), and then click Next.
- e For the web adaptor's name, replace the default name with **server** and click Next.
- f Click Install.
- g Click Finish.

When complete, the installation opens the web adaptor configuration page. If you needed to reconfigure a web adaptor, you could return to this page by opening its link in the ArcGIS program group in the Start menu.

Step 3: Configure the web adaptor

You have installed the ArcGIS Web Adaptor and can now direct it to the ArcGIS Server.

- a In the web adaptor configuration tab's URL, replace *localhost* with the fully qualified domain name (FQDN) and press Enter.

Hint: The correct URL is **https://ebase.ad.local/server/webadaptor**.

The page loads successfully using the domain certificate on HTTPS.

- b Verify that the option for GIS, Image, Workflow Manager, Or Knowledge Server is selected, and then click Next.

Which component do you want to configure with your web adaptor?

- GIS, Image, Workflow Manager, or Knowledge Server
- Portal for ArcGIS
- Notebook Server
- Mission Server
- Video Server
- ArcGIS Monitor



This web adaptor is not configured with an ArcGIS Enterprise component.

- c For GIS, Image, Workflow Manager, Or Knowledge Server, type the name of your fully qualified domain name.

Hint: Your fully qualified domain name (FQDN) is **ebase.ad.local**.

- d Type the credentials for the primary site administrator account that you created in the previous exercise.

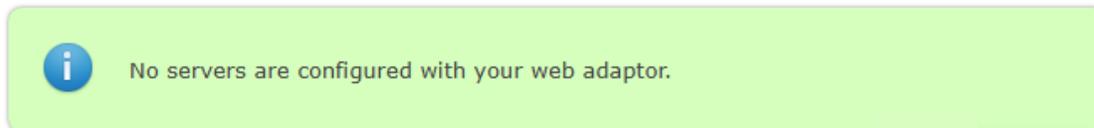
Hint: Username is **siteadmin** and Password is **Esri.4.GIS**.

To configure the web adaptor, specify the fully qualified domain name and an administrator account for your GIS, Image, Workflow Manager, or Knowledge Server.

GIS, Image, Workflow Manager, or Knowledge Server: ?
 Example: server.domain.com

Administrator Username: ?

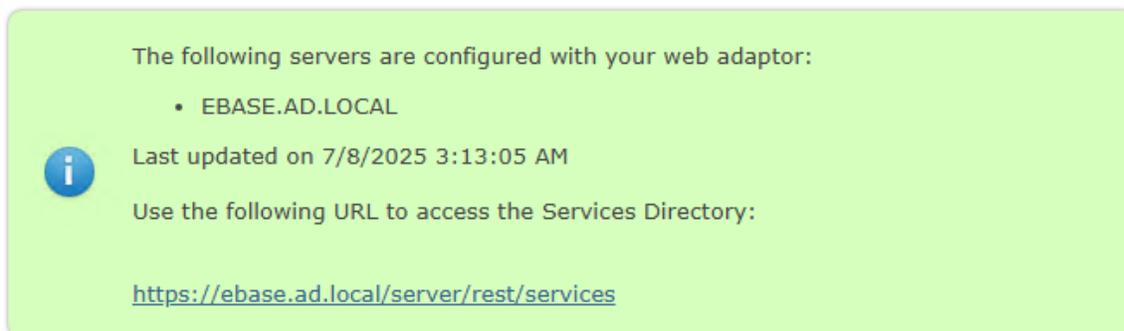
Administrator Password: ?



At ArcGIS Enterprise 11.5, administrative access is enabled by default and cannot be disabled; this was not the case in previous versions. With administrative access enabled, users can access the ArcGIS Server Administrator Directory and ArcGIS Server Manager through the web adaptor from the start. Additionally, because administrative access is enabled, users can create administrative and publisher connections to the server from ArcGIS Pro.

- e** Click Configure to begin the web adaptor configuration process.

When the process completes, a message appears confirming that your ArcGIS Server has been successfully configured with your web adaptor.



- f** To test that the web adaptor is working, click the provided link to the ArcGIS Server Services Directory.

A new tab opens to the service directory. This application is helpful for administrators and developers to perform tests with running services and discovering service capabilities.

Step 4: Import the web server certificate

Previously, you imported your domain certificate into the Portal Administrator Directory. Now you will import the same certificate into the ArcGIS Server Administrator Directory. The process is slightly different, but it will have the same effect on HTTPS communication between clients and your base deployment by using a common certificate.

This process is not required but might be necessary to meet certain business requirements. For example, an organization might have a Service Level Agreement that requires the highest level of trust between all ArcGIS components.

- a In your browser, open a new tab and go to **https://ebase.ad.local:6443/arcgis/admin**.
- b Click Advanced, and then click Proceed To ebase.ad.local (Unsafe).

The ArcGIS Server Administrator Directory allows you to perform advanced management tasks for your server.

- c Provide your site administrator account credentials and click Login.

Hint: Username is **siteadmin** and Password is **Esri.4.GIS**.

- d In the Resources list, click Machines and select EBASE.AD.LOCAL.

1. What is the name of the current SSL certificate?

- e At the bottom of the page, in the Resources list, click sslcertificates.

As you did with your portal configuration, you will begin by importing the domain root certificate.

- f Click ImportRootOrIntermediate.
- g For Alias, type **domain_root**.
- h For Root CA Certificate, click Choose File and open the domain root certificate at **..._sw\Authorization\adRoot.cer**.
- i Click Import.

Now you will import the certificate that you exported from your domain earlier.

- j Click ImportExistingServerCertificate.
- k For Certificate Password, type **Esri.4.GIS**.
- l For Alias, type **server_cert**.
- m For Certificate File, click the Choose File button, browse to `..\sw\Authorization`, and open the `server_cert.pfx` file.
- n Click Submit.

Your domain certificate now appears in the list under SSL Certificates. You must still update the server's configuration so that it will use this certificate.

- o At the top of the page, click the `EBASE.AD.LOCAL` link, as indicated in the following graphic.

ArcGIS Server Administrator Directory

[Home](#) > [machines](#) > **[EBASE.AD.LOCAL](#)** > [sslcertificates](#)

SSL Certificates

- [domain_root](#)
- [selfsignedcertificate](#)
- [server_cert](#)

- p In the Supported Operations list, click Edit.
- q For Web Server SSL Certificate, replace the existing certificate name with **server_cert**, your domain certificate name.
- r At the bottom of the page, click Save Edits and wait until the web page finishes loading before continuing.



It may take several minutes for the site to come back online while your changes are committed. If the web page times out, refresh the page. Copy the URL and close and reopen the web browser as needed.

Your server's site is restarted to commit the certificate change. You are automatically returned to the previous page. You will notice that the SSL certificate has been updated to be the same one

used by your web server.

Server Machine Properties	
Name:	EBASE.AD.LOCAL
Admin URL:	https://EBASE.AD.LOCAL:6443/arcgis/admin
Platform:	Windows 11-amd64-10.0
Server Start Time:	2025-05-26T02:37:35,984
Web server maximum heap size (in MB):	-1
Web server SSL Enabled :	true
Web server SSL Certificate:	server_cert
SOC maximum heap size (in MB):	64
Synchronize:	false
Under Maintenance:	false

Step 5: Explore the site

Your server site has been fully configured, and you have configured your server's web adaptor and internal domain certificate. Next, you will explore your server with ArcGIS Server Manager.

- a** In your browser, open a new tab, and click the bookmark for ArcGIS Server Manager (<https://ebase.ad.local/server/manager/>).
- b** Sign in with your primary site administrator credentials.

Hint: Username is **siteadmin** and Password is **Esri.4.GIS**.

Many administrative and publishing tasks can be conducted with ArcGIS Server Manager. You are taken to the Services tab, where you can publish, edit, stop, start, and restart your GIS services.

- c** Below Site (Root), click the System folder.

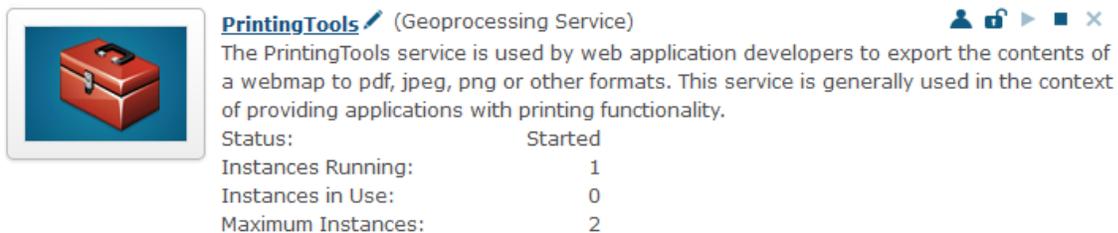
When you created your site, these system services were created. The services are there to keep the site running optimally.

- d Under the System folder link, click the Utilities folder.

Utility services are there for your users to perform certain functions.

You anticipate that some of your users will want to print from their web mapping apps, so you will start the PrintingTools utility service.

- e To start the PrintingTools service, to the right of its name, click the Start button ▶.
- f Ensure that the Status is now listed as Started before continuing.



PrintingTools (Geoprocessing Service) ▶

The PrintingTools service is used by web application developers to export the contents of a webmap to pdf, jpeg, png or other formats. This service is generally used in the context of providing applications with printing functionality.

Status:	Started
Instances Running:	1
Instances in Use:	0
Maximum Instances:	2

You signed in as the primary site administrator, which is an internal administrator account. Next, you will investigate the site's security settings.

- g At the top of the page, click the Security tab.

2. Based on the current configuration settings, which base deployment component is providing security?

ArcGIS Server contains its own security functionality, and you can optionally configure it to use your enterprise's users and roles store (for example, LDAP or a Windows Domain). You will incorporate your server site with your portal in the next exercise.

- h In the EBASE VM, close all open application windows.

Checkpoint

1. Which certificate type enables the ArcGIS Server to trust the certifying authority that issues a certificate?
 - a. Root certificate
 - b. Server certificate
 - c. Domain certificate
 - d. Portal certificate

2. Which certificate is used in HTTPS communication to establish communication between the ArcGIS Server and the client?
 - a. Root certificate
 - b. Server certificate
 - c. Domain certificate
 - d. Portal certificate

Federation

In an ArcGIS Enterprise base deployment, ArcGIS Server provides core, scalable GIS functionality. Federating your ArcGIS Server with your Enterprise portal integrates the ArcGIS Enterprise security and sharing models, as well as providing a user-friendly interface for discovering, using, and sharing content.

Before an ArcGIS Server is federated into an ArcGIS Enterprise deployment, the server uses a role-based security model. The role-based security model grants permission to server users based on their assigned role. This grants certain users more privileges than necessary based on their role alone. It can also make it difficult to determine what permissions to grant roles.

After the ArcGIS Server is federated into an ArcGIS Enterprise deployment, the server's security changes to an item-based security model. The item-based security model allows content owners to share individual items with users, regardless of their role, allowing for more granular control over access privileges. Any existing services, including utility services and user-published services, will be assigned to the Enterprise portal administrator who performed the federation process.

Federation (continued)



Figure 4.4. Federation unites your server and portal under the ArcGIS Enterprise security model.



ArcGIS Enterprise Help: *Federate an ArcGIS Server site with your portal*

ArcGIS Enterprise Help: *The ArcGIS Enterprise security model*

Federate your ArcGIS Server site with your Enterprise portal

Now that your portal and server sites have been installed and configured, you are ready to federate the server with the portal. Federation will allow you to configure a base deployment with a unified security model, simplifying operations for your organization's users.

In this exercise, you will perform the following tasks:

- Configure federation.
- Explore changes to your implementation.

Step 1: Configure federation

You will federate your newly created ArcGIS Server site using the portal administrator account.

- a If necessary, maximize the EBASE VM (blue desktop) application window.
- b Open a web browser, and click the bookmark for ArcGIS Enterprise (<https://ebase.ad.local/portal/home>).
- c At the top of the page, click Sign In.
- d Provide the credentials for the portal administrator account.

Hint: Username is **portaladmin** and Password is **Esri.4.GIS**.

- e On the Organization tab, click Settings on the blue toolbar.
- f On the left side of the page, click the Servers tab.
- g Under Federated Server Sites, click Add Server Site.

The Services URL uses the web adaptor to reference GIS services.

- h For Services URL, type **https://ebase.ad.local/server**.

The Administration URL can point to the ArcGIS Server site directly over port 6443, or through the Web Adaptor, as well as your system design needs.

- i For the Administration URL, type **https://ebase.ad.local:6443/arcgis**.
- j Under Server Credentials, enter the following information:

- Username: **siteadmin**
- Password: **Esri.4.GIS**

Services URL

This is the URL used by external users when accessing the server site.

Example: https://webadaptorhost.domain.com/webadaptorname

Administration URL

This is the URL used for accessing the server site for administrative operations on the internal network.

Example: https://gisserver.domain.com:6443/arcgis ⓘ

Server credentials

These credentials should match the primary site administrator account that was used to initially sign in to and administer the server site.

Username**Password**

- k** Click Next.
- l** Under Configure Server Role, for Hosting Server, click the Requirements Missing link.

Add server site ×

Federate server site Configure server role

Optionally, configure this server site with the following server roles to add functionality to your Enterprise portal.
[Learn more about server roles.](#)

Hosting Server Configure a Hosting Server site to allow members to publish hosted layers and perform analysis in the ArcGIS Enterprise portal.	Requirements missing
GeoAnalytics Server Configure a GeoAnalytics Server site to allow members to perform distributed big data analysis on feature and tabular data.	Requirements missing
Raster Analysis Server Configure a Raster Analysis Server site to allow members to perform distributed raster analytics and image processing.	Requirements missing
Image Hosting Server Configure an Image Hosting Server site to host your image services created from imagery layers and generated by your Raster Analysis Server.	Requirements missing
Notebook Server	Requirements missing

m Read the message and answer the following question.

1. Can this server be designated as your portal's hosting server? Why or why not?

n Click Save Server Role.

The server is added to the list of federated server sites.

Federated server sites

You can add a server site to achieve a single sign-on experience, share items, and optionally host services. A server site that has been added to a portal is called a federated server site. Add one or more server sites to your portal.

Validate server sites
Add server site

<div style="display: flex; justify-content: space-between; align-items: center;"> ▼ ebase.ad.local:6443 ⋮ </div>		
<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%; padding: 2px 5px;">Status</td> <td style="padding: 2px 5px;"> Systems operational, some issues</td> </tr> </table>	Status	Systems operational, some issues
Status	Systems operational, some issues	
<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%; padding: 2px 5px;">Server role</td> <td style="padding: 2px 5px;">Configure server role</td> </tr> </table>	Server role	Configure server role
Server role	Configure server role	
<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%; padding: 2px 5px;">Service URL</td> <td style="padding: 2px 5px;">https://ebase.ad.local/server</td> </tr> </table>	Service URL	https://ebase.ad.local/server
Service URL	https://ebase.ad.local/server	
<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 20%; padding: 2px 5px;">Administration URL</td> <td style="padding: 2px 5px;">https://ebase.ad.local:6443/arcgis</td> </tr> </table>	Administration URL	https://ebase.ad.local:6443/arcgis
Administration URL	https://ebase.ad.local:6443/arcgis	

Your server has been federated with your portal. Next, you will explore both sites to see what has changed.

Step 2: Explore changes to the implementation

Your ArcGIS Server site has been federated with your Enterprise portal. Now you will explore several effects of federation.

a At the top of the portal web page, click Content.

2. What items now appear under My Content?

You will notice that none of these federated services is shared with the organization yet. A portal administrator must explicitly share these items using the portal sharing model.

b Click the PrintingTools geoprocessing service to view the item's details.

3. Who owns this item?

c Scroll down and locate the URL field at the bottom of the page.

d Just above the URL field, click the View link.

A new tab opens to the service's ArcGIS Server Services Directory page.

4. Who is logged in to the Services Directory?

Next, you will sign in to ArcGIS Server Manager to view the changes.

- e Open a new tab and go to <https://ebase.ad.local/server/manager>.

Your portal credentials are still active in the current browser session, so they are automatically passed into Server Manager.

- f At the top of the page, click Security.

5. What security settings changed after federation?

Configuration Settings 	
User Store:	Portal for ArcGIS
Role Store:	Portal for ArcGIS
Authentication Tier:	Portal for ArcGIS
Authentication Mode:	Portal for ArcGIS
Portal URL:	https://ebase.ad.local/portal/home

The ownership of ArcGIS Server's services is automatically transferred to the Enterprise portal administrator that performed the federation process.

The ArcGIS Server site's existing services must now be shared to your organization to be accessible to ArcGIS Enterprise clients.

- g In the EBASE VM, close all open application windows.

Migrating from a stand-alone server

Your organization may have an existing stand-alone ArcGIS Server with content that you wish to make available in your new ArcGIS Enterprise deployment. There are three options to make this content available on ArcGIS Enterprise. Which method you choose will be determined by your available resources, time, and other organizational requirements.

Option 1: Repurpose existing ArcGIS Server site

Upgrade your stand-alone ArcGIS Server site to ArcGIS Enterprise and use it as the hosting server site within your base ArcGIS Enterprise deployment.

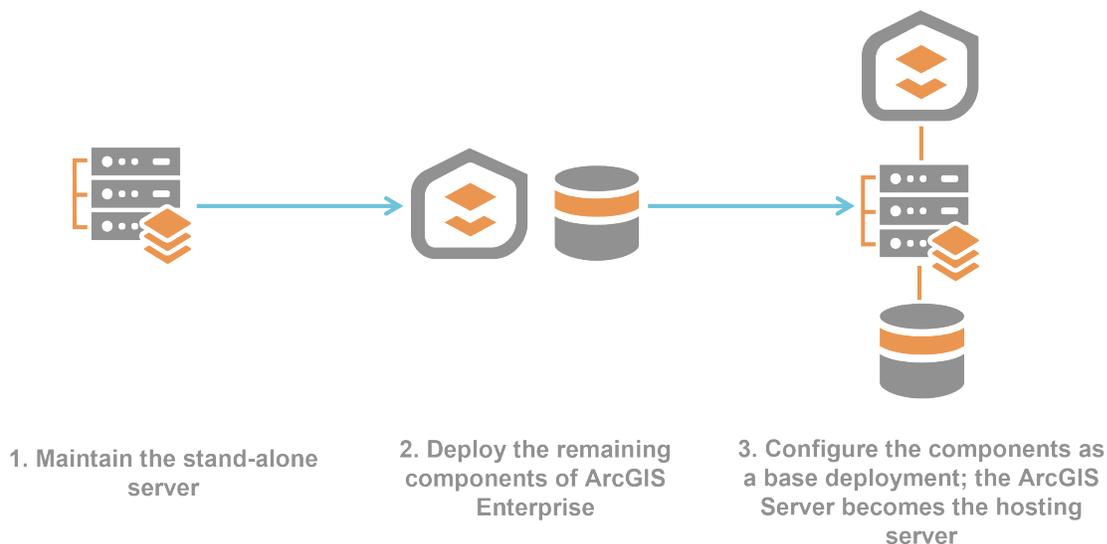


Figure 4.5. With the first option, you federate your existing stand-alone server with the other components of ArcGIS Enterprise to form a base deployment.

Benefits	Considerations
<ul style="list-style-type: none"> • No new infrastructure needed for the GIS server • No need to republish services • Service URLs do not change 	<p>ArcGIS Server site is serving as both a hosting server and a traditional GIS server</p>

Migrating from a stand-alone server (continued)

Option 2: Migrate content to a new base ArcGIS Enterprise deployment

Create a new ArcGIS Enterprise deployment on new infrastructure and migrate services from your stand-alone ArcGIS Server site as needed.

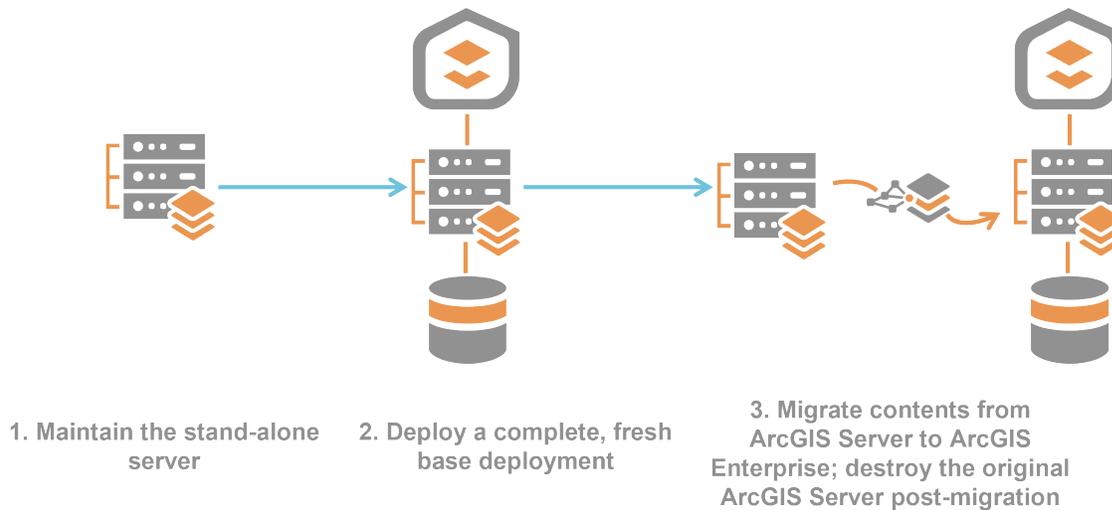


Figure 4.6. With the second option, you deploy a separate base deployment, then migrate all the content and services from the stand-alone server to the new, hosting server of the ArcGIS Enterprise deployment. After, you destroy the stand-alone server.

Benefits	Considerations
<ul style="list-style-type: none"> • Gradual migration • Good choice for custom deployments and multi-machine sites 	<p>Services will need to be republished, and service URLs will change</p>

Migrating from a stand-alone server (continued)

Option 3: Federate the stand-alone server as an additional ArcGIS GIS Server

Create a base ArcGIS Enterprise deployment, separate from your existing ArcGIS Server site, on new infrastructure, and then upgrade and federate your existing ArcGIS Server site to the new ArcGIS Enterprise deployment.

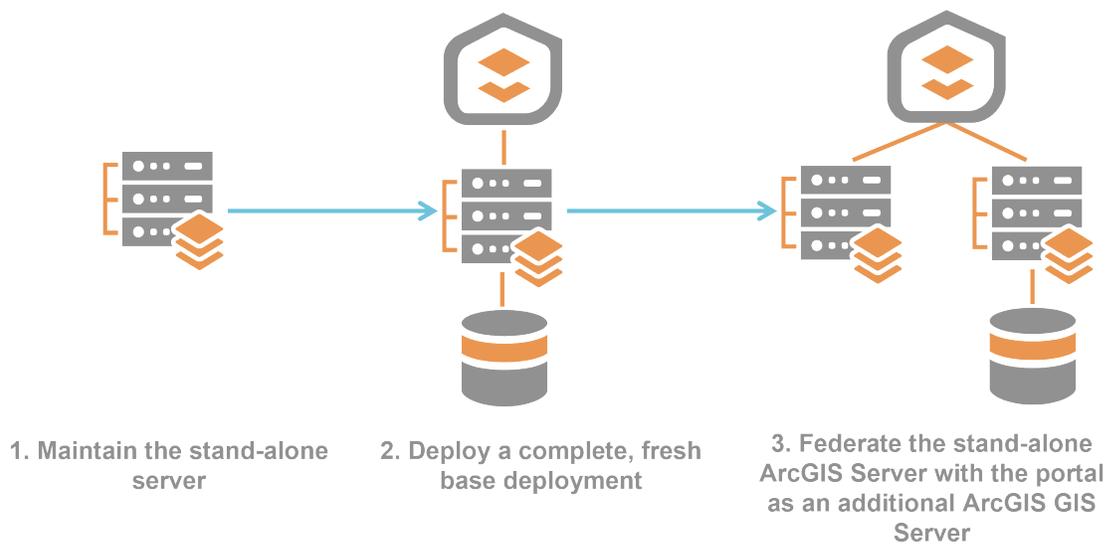


Figure 4.7. For the third option, you will deploy a new base deployment and federate the stand-alone server as an additional ArcGIS GIS Server with the deployment. Both GIS Servers will be maintained simultaneously.

Benefits	Considerations
<ul style="list-style-type: none"> • Provides workload separation • No republishing services • Service URLs do not change 	<ul style="list-style-type: none"> • Must purchase additional cores of ArcGIS Server



This information is from the *Migrating standalone ArcGIS Server to ArcGIS Enterprise* Esri technical paper. A complete copy of this technical paper is available in your student data: **C:\EsriTraining\EBAS\Migration**.

Migrating from a stand-alone server (continued)

1. Which migration option would you choose if you wanted to repurpose your existing infrastructure?

2. Which migration options enable you to use the existing service URLs from your prior stand-alone ArcGIS Server?

Workflow review

In this lesson, you installed and configured the two additional base deployment components: ArcGIS Server and its associated ArcGIS Web Adaptor. You also ensured that your domain certificate is used internally within your server's site and specified secure communication between the ArcGIS server and portal.

Finally, you federated your server with the portal, which allows Portal for ArcGIS to handle the security for your GIS services.

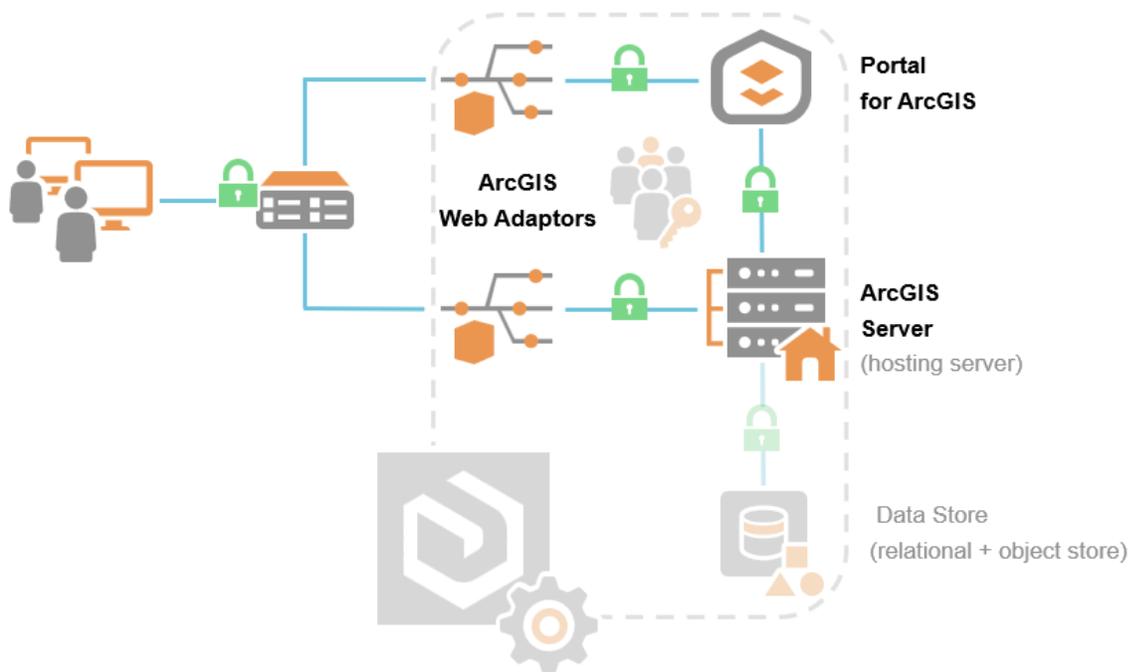


Figure 4.8. The ArcGIS Enterprise now includes a secure hosting server.

1. What are the benefits of federating your ArcGIS Server with ArcGIS Enterprise?

Workflow review (continued)

- 2. Which ArcGIS Server account credentials must be used when federating the server site with the portal?**

Answers to lesson 4 questions

Explore the ArcGIS Server installation (page 4-4)

1. Which type of account has been specified for this service?

A domain account (ad.local\arcgis\$) has been specified.

2. How can you change the ArcGIS Server account while preserving its required privileges?

You can run the Configure ArcGIS Server Account utility, which will ensure that the account specified is granted all required privileges.

Exercise 4A: Set up your ArcGIS Server site (page 4-11)

1. What is the name of the current SSL certificate?

The current certificate is named SelfSignedCertificate.

2. Based on the current configuration settings, which base deployment component is providing security?

ArcGIS Server is providing built-in user and role stores and authentication.

Checkpoint (page 4-20)

1. Which certificate type enables the ArcGIS Server to trust the certifying authority that issues a certificate?

a.

Root certificate

b. Server certificate

c. Domain certificate

d. Portal certificate

Answers to lesson 4 questions (continued)

2. Which certificate is used in HTTPS communication to establish communication between the ArcGIS Server and the client?
 - a. Root certificate
 - b. Server certificate
 - c. Domain certificate
 - d. Portal certificate

Exercise 4B: Federate your ArcGIS Server site with your Enterprise portal (page 4-23)

1. Can this server be designated as your portal's hosting server? Why or why not?

The federated server cannot be designated as a hosting server because a relational data store has not been configured.
2. What items now appear under My Content?

The utility services and a sample map service from your ArcGIS Server appear.
3. Who owns this item?

portaladmin
4. Who is logged in to the Services Directory?

portaladmin
5. What security settings changed after federation?

ArcGIS Server security has changed from its internal security model to ArcGIS Enterprise's security model, that is, Portal for ArcGIS.

Migrating from a stand-alone server (page 4-29)

1. Which migration option would you choose if you wanted to repurpose your existing infrastructure?

Option 1

Answers to lesson 4 questions (continued)

2. Which migration options enable you to use the existing service URLs from your prior stand-alone ArcGIS Server?

Options 1 and 3

Workflow review (page 4-33)

1. What are the benefits of federating your ArcGIS Server with ArcGIS Enterprise?

Answers will vary but may include:

- **Users gain access to the user-friendly portal interface**
- **Content is secured using the ArcGIS Enterprise security model**

2. Which ArcGIS Server account credentials must be used when federating the server site with the portal?

When federating the server site with the portal, the Primary Site Administrator account which was used to sign in and administer the server site must be used. This account has full administrator privileges to the site which is required for federation.

5

Managing GIS resources

Any hosted content shared with your ArcGIS Enterprise base deployment references underlying GIS data and resources. When you share information with others in your organization, other organizations, or the public, you want to be sure that they are viewing the correct data.

In a base ArcGIS Enterprise deployment, your users can share content where the data is ArcGIS-managed (hosted) by ArcGIS Data Store. In addition, you can choose to share content that references user-managed data by registering it with ArcGIS Server.

Topics covered

- ArcGIS Data Store installation and configuration

- Configuration of the ArcGIS Enterprise hosting server

- ArcGIS Data Store functionality

- Registering data with the ArcGIS Server site

ArcGIS Data Store

There are several configurations of the ArcGIS Data Store which determines what types of data and functionality are available to your ArcGIS Enterprise deployment. The two configurations of ArcGIS Data Stores frequently employed in a base deployment are the relational and object data stores. The spatiotemporal big data store and graph configuration options will not be covered in this course.

ArcGIS Data Store type	Description
<p data-bbox="168 793 310 825">Relational</p> 	<p data-bbox="508 793 894 825">Stores hosted feature layers</p>
<p data-bbox="164 1035 380 1066">Spatiotemporal</p> 	<p data-bbox="508 1035 1377 1115">Stores persistent real-time data and enables distributed vector analysis</p>
<p data-bbox="164 1251 253 1283">Graph</p> 	<p data-bbox="508 1251 1349 1283">Stores knowledge graphs that map entities and relationships</p>
<p data-bbox="164 1480 261 1512">Object</p> 	<p data-bbox="508 1480 1195 1512">Caches query responses for hosted feature layers</p>

ArcGIS Data Store (continued)



ArcGIS Enterprise Help: *Introduction to ArcGIS Data Store*

ArcGIS Enterprise Help: *ArcGIS Data Store Vocabulary - Spatiotemporal big data store*

ArcGIS Enterprise Help: *ArcGIS Data Store Vocabulary - Graph store*

Setting up ArcGIS Data Store

ArcGIS Data Store functions as the ArcGIS-managed repository for your organization's GIS data. When ArcGIS Data Store is installed, an account and file directories are specified. You will also need to define the types of data stores that you are configuring and register ArcGIS Data Store with the ArcGIS Server site.

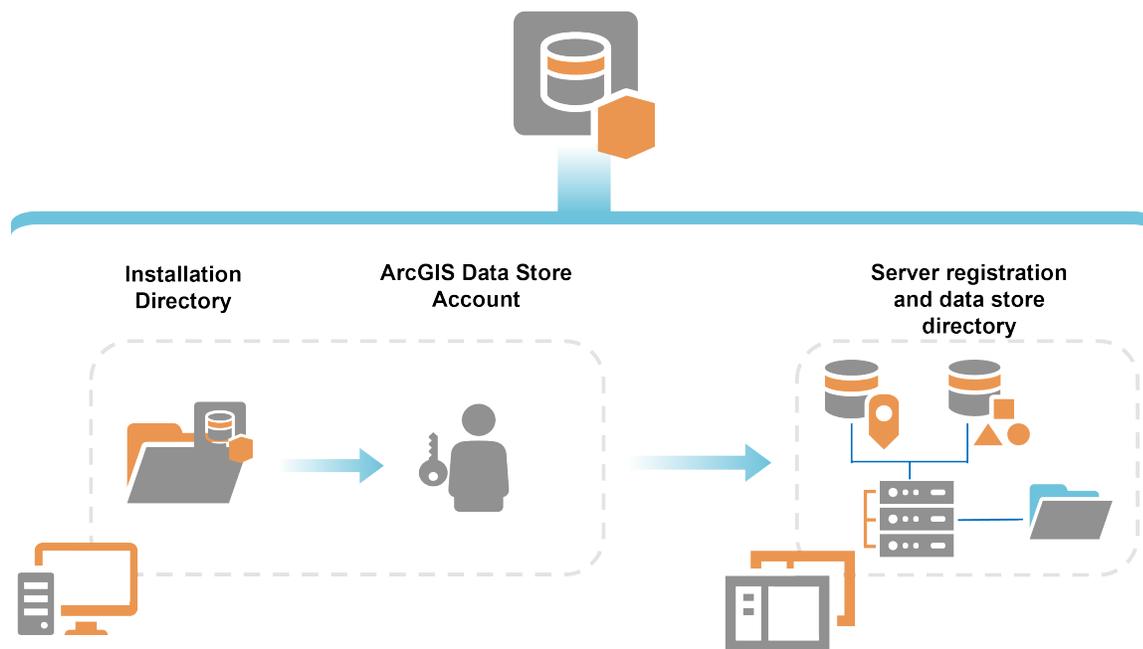


Figure 5.1. This graphic shows the relationship between various installation parameters when setting up ArcGIS Data Store. The ArcGIS Data Store Account and Installation directory are used to install ArcGIS Data store on the server. Then the data store can be registered with the server.

Setting up ArcGIS Data Store (continued)

ArcGIS Data Store Installation Parameters

Installation Parameter	Notes
Install directory location	<ul style="list-style-type: none"> • Default is C:\Program Files\ArcGIS\DataStore
ArcGIS Data Store account	<ul style="list-style-type: none"> • Default is a local operating system account named <i>arcgis</i> • Can be the same account specified for Portal for ArcGIS and ArcGIS Server
ArcGIS Server site URL and credentials	<ul style="list-style-type: none"> • URL of the ArcGIS Server site that you want the data store registered to • ArcGIS Server primary site administrator credentials
Data Store types	<ul style="list-style-type: none"> • Relational and object types required for base deployment
ArcGIS Data Store directory location	<ul style="list-style-type: none"> • Contains data store files and relational data store backup directory • Cannot be a UNC path

For a highly available configuration, you can install ArcGIS Data Store on another machine and register it with the same ArcGIS Server site as the first. See the additional resources at the end of this section for instructions.



Each type of data store should ideally be installed on different machines to avoid resource (CPU, memory, and disk space) contention.

Setting up ArcGIS Data Store (continued)



The relational data store backup directory should be moved to another machine after installation. See the following additional resources for help on tasks to perform after data store creation.



ArcGIS Enterprise Help: *Tasks to perform after you create a data store*

ArcGIS Enterprise Help: *Add a machine to your data store*

ArcGIS Enterprise Help: *ArcGIS Data Store command utility reference*

Configuring the hosting server

Two requirements must be met before a hosting server can be configured for the base deployment:

- An ArcGIS Server site is federated with the Enterprise portal.
- Data Store (with relational and object data stores) is installed and registered with the federated ArcGIS Server site.



Figure 5.2. An ArcGIS Enterprise base deployment uses a data store to host services and functionality. Frequently, this data store is implemented using an ArcGIS Data Store.

If these requirements are met, then ArcGIS Server can be configured with the hosting server role. Users can then share feature layers (relational) and scene layers (object) as hosted services, which automatically copies the data to ArcGIS Data Store.

Set up ArcGIS Data Store

To complete your base deployment, you will install and configure ArcGIS Data Store and set it as your portal's hosting server. To test that it is functioning correctly, you will publish a hosted layer.

In this exercise, you will perform the following tasks:

- Install ArcGIS Data Store.
- Create relational and object data stores.
- Designate the hosting server.
- Share a hosted layer.



ArcGIS Enterprise Help: *An overview of ArcGIS Data Store configuration*

ArcGIS Enterprise Help: *Replace ArcGIS Data Store SSL certificate*

Step 1: Install ArcGIS Data Store

You will install ArcGIS Data Store and register it with your ArcGIS Server to complete your base deployment. After it is set up, you can set your ArcGIS Server as the ArcGIS Enterprise portal's hosting server.

- a If necessary, maximize the EBASE VM (blue desktop) application window.
- b Open File Explorer and browse to `\\BaseVMGen2\Users\student\Desktop_sw\ArcGIS_DataStore`.
- c Double-click Setup.exe to begin the installation.
- d Proceed to the Master Agreement panel, click I Accept The Master Agreement, and then click Next.
- e On the Select Features panel, click Next.

Similar to Portal for ArcGIS and ArcGIS Server, a Windows login that runs the ArcGIS Data Store service on your server must be specified. You will use the same account that you used for the other two component installations.

- f On the Specify ArcGIS Data Store Account panel, check the box for the Managed Service Account option and provide the following information:
 - User name: **ad.local\arcgis\$**
 - Password and Confirm Password parameters: No password should be provided
- g Click Next.
- h On the Export Account Configuration File panel, click Next.
- i Click Install.
- j After installation completes, click Finish.

The installation of the software is complete. Next, you will configure ArcGIS Data Store.

Step 2: Create relational and object data stores

Your default browser launches automatically to the ArcGIS Data Store Configuration Wizard. Because the internal HTTPS certificate is not trusted by the browser, you will receive a warning.

- a** In the browser's address field, replace localhost with **ebase.ad.local**.

Hint: The URL should be **https://ebase.ad.local:2443/arcgis/datastore**.

- b** Press Enter.

- c** Click Advanced, and then click Proceed To ebase.ad.local (Unsafe).

To associate the data store with your ArcGIS Server's site, you must provide the internal URL and an administrator's credentials.

- d** For GIS Server, type **ebase.ad.local**.

- e** For Username and Password, type **siteadmin** and **Esri.4.GIS**, respectively.

GIS Server:
Example: gisserver.domain.com

Username:

Password:

- f** Click Next.

The Content Directory parameter directs ArcGIS Data Store to the location where it should store data, log, and backup files. You will leave the default value for this parameter.

- g** Click Next.

A base deployment requires the relational and object data stores. In a production system, each data store type should be configured on a separate machine. This practice is especially true of the resource-intensive spatiotemporal, object, and graph store configurations. However, for the purposes of this course, you will configure both the Relational and Object stores on the same machine.

- h** Check the Relational and Object data store type boxes, and then click Next.

Select an ArcGIS Data Store type to configure:

- Relational**
- Spatiotemporal**
- Graph**
- Object** (single-machine deployment)
 - single-machine
 - cluster

A summary of the configuration parameters is provided before you commit them.

- i** Click Finish and wait until the configuration completes before proceeding to the next step.

The data stores, log file structure, and backup files are generated and registered with your ArcGIS Server site. When it begins running, you can set ArcGIS Server as the Enterprise portal's hosting server.

Step 3: Import the certificate for ArcGIS Data Store

Next, you will associate the domain certificate that you are using for both the portal and server with ArcGIS Data Store.

- a** Click the Windows Start button and type **cmd**, but do not press Enter.
- b** Right-click the Command Prompt search result and choose Run As Administrator.
- c** In the command window, type **cd \Program Files\ArcGIS\DataStore\tools** and press Enter.
- d** In the command window, type **updateslcertificate** and press Enter.

The parameters for the command are shown. Your certificate file was saved to **\\BaseVMGen2\Users\student\Desktop_sw\Authorization** with a password of Esri.4.GIS. You will set an alias of **server_cert**.

- e** Type the command with the appropriate parameters and press Enter.

Hint: Type **updateslcertificate \\BaseVMGen2\Users\student\Desktop_sw\Authorization\server_cert.pfx Esri.4.GIS server_cert** and press Enter.

- f** Type **Yes** and press Enter.

The internal ArcGIS Data Store web server is restarted. Next, you will test that the domain

certificate is configured correctly by reloading the configuration page.

- g** Restore the web browser.
- h** Open a new tab and go to **<https://ebase.ad.local:2443/arcgis/datastore>**.



If the page does not load without the security warning, wait an additional minute, close and reopen browser.

The page loads without a warning because you have set a trusted domain certificate for the internal site.

Step 4: Designate the hosting server

Your ArcGIS Data Store is fully configured and registered with your ArcGIS Server's site. Next, you will designate the site as your portal's hosting server to fully integrate these components.

- a** In your browser, click the ArcGIS Enterprise bookmark provided (<https://ebase.ad.local/portal/home>).
- b** Sign in as **portaladmin** with the password **Esri.4.GIS**.
- c** From the portal's Organization page, click Settings.
- d** Click the Servers tab.
- e** Under the options for ebase.ad.local:6443, click Configure Server Role.

Servers

Federated server sites

You can add a server site to achieve a single sign-on experience, share items, and optionally host services. A server site that has been added to a portal is called a federated server site. Add one or more server sites to your portal.

[Validate server sites](#)
[Add server site](#)

ebase.ad.local:6443 ...
Status ✔ All systems operational
Server role Configure server role
Service URL https://ebase.ad.local/server
Administration URL https://ebase.ad.local:6443/arcgis

- f** Enable the Hosting Server role.

Configure server role for ebase.ad.local:6443

Optionally, configure this server site with the following server roles to add functionality to your Enterprise portal. [Learn more about server roles.](#)

Hosting Server

Configure a Hosting Server site to allow members to publish hosted layers and perform analysis in the ArcGIS Enterprise portal.

- g** Click Save.
- h** For Server Role, confirm that Hosting Server is listed.

Servers

Federated server sites

You can add a server site to achieve a single sign-on experience, share items, and optionally host services. A server site that has been added to a portal is called a federated server site. Add one or more server sites to your portal.

[Validate server sites](#)[Add server site](#)

▽ ebase.ad.local:6443 ✎

...

Status ✔ All systems operational

Server role [Hosting Server](#)

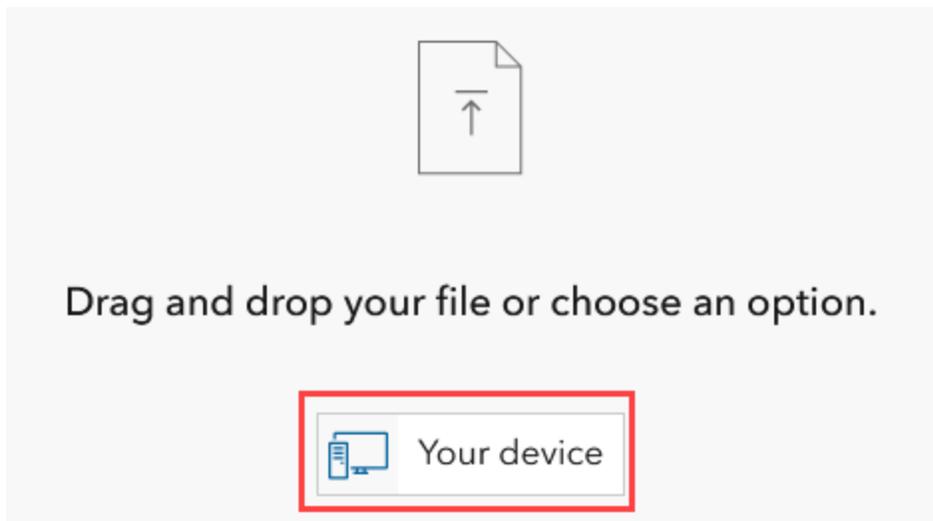
Service URL <https://ebase.ad.local/server>

Administration URL <https://ebase.ad.local:6443/arcgis>

Step 5: Share a hosted layer

Finally, you will test your base deployment's basic functionality by sharing a hosted layer to the portal. The Enterprise portal provides your users with the ability to discover, use, make, and share hosted layers.

- a At the top of the portal page, click Content.
- b Click New Item and choose Your Device.



- c Browse to the course data located at **C:\EsriTraining\EBAS\ManagingResources**, select **Wards.zip**, and press Open.



The GIS data used in exercises is stored on the EBASE (blue desktop) machine in the **C:\EsriTraining** folder.

- d In the New Item window, ensure that File Type is set to Shapefile and that the option to create a hosted feature layer is selected.

File

Wards.zip

File type


Shapefile
 A vector data storage format for storing the location, shape, and attributes of geographic features. A shapefile is stored in a set of related files and contains one feature class.

How would you like to add this file?

Add Wards.zip and create a hosted feature layer
 Add the shapefile and publish as a hosted feature layer that can be added to a map.

- e Click Next.
- f Set or confirm the following parameters:

- Title: **Aurora_CO_Wards**
- Folder: portaladmin
- Tags: **Aurora, Colorado, Wards**

g Click Save.



If you encounter an error when publishing, close the New Item window and add the Wards.zip file again.

The item (compressed shapefile) is added and then published as a hosted feature layer to your portal. After it is published, both items can be shared and managed separately. The shapefile data is not directly linked to the hosted feature layer because the layer's data is now server-managed within your relational data store.

When you registered ArcGIS Data Store with your ArcGIS Server site, it was automatically set to be the site's managed database. This setting allows full integration between ArcGIS Server and ArcGIS Data Store, and it allows the site to be set as the hosting server. Next, you will learn more about ArcGIS Server's data stores for some other approaches to managing GIS resources in ArcGIS Enterprise.

h To verify that the hosted layer is working, click Open In Map Viewer.

i In the EBASE VM, close all open application windows.

Defining web layers

Layers

Layers represent logical collections of geographic information, such as buildings, roads, water bodies, or elevation. Each layer references a dataset, such as 2D or 3D feature classes within a file or enterprise geodatabase. Layers can only represent one type of geometry, such as points, lines, polygons, or rasters.

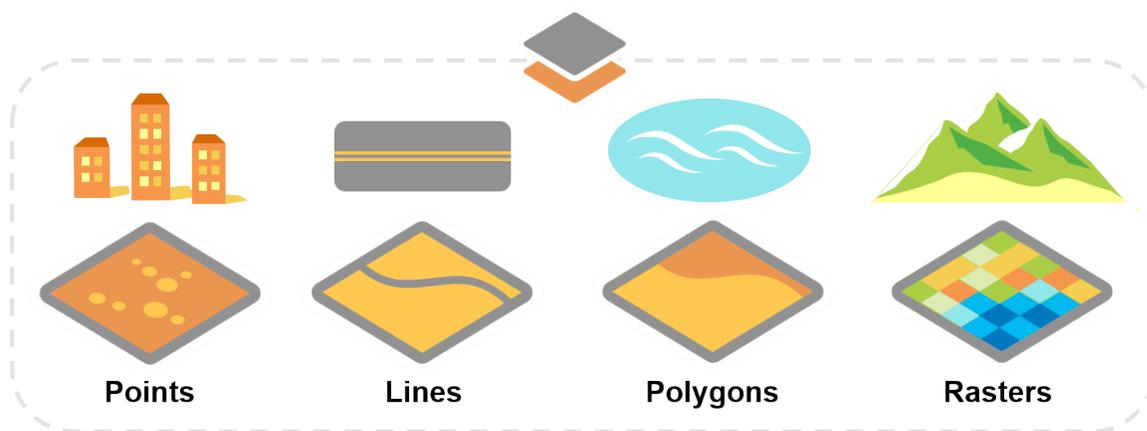


Figure 5.3. Layers represent logical collections of geographic information, such as buildings (points), roads (lines), water bodies (polygons), or elevation (rasters).

Web layers

In ArcGIS Pro, you can share layers to ArcGIS Enterprise as web layers. When a layer is shared to a base deployment, a service is published to the hosting server and exposed through a new item in your Enterprise portal. Depending on the shared layer type and configuration, the published service will point to data in ArcGIS Data Store (hosted service) or another data source that is registered with ArcGIS Server (ArcGIS Server service). There are several web layer types, or services, that can be shared from ArcGIS Pro to ArcGIS Enterprise. Some examples of available web layer types include: feature, tile, vector tile, map image, imagery, scene, and elevation.

Defining web layers (continued)



Figure 5.4. When you share a layer to ArcGIS Enterprise, the resulting web layer corresponds to a service that points to data in ArcGIS Data Store or another registered data source.

 **ArcGIS Enterprise Help:** *Relationships between web services and portal items*

Associate web layers with GIS resources

Web layers can point to data within ArcGIS Data Store (ArcGIS-managed) or another registered data source (user-managed). In this activity, you will compare the ArcGIS Pro options for sharing ArcGIS-managed and user-managed web layers.

Instructions

- a** In a web browser, go to <https://pro.arcgis.com>.
- b** Scroll down to the Documentation section and select the Share topic.
- c** Under the Share Web Layers section, click Learn More About Sharing Web Layers.
- d** On the right side of the page, under In This Topic, click Reference Registered Data Or Copy All Data. Read the information under this topic.
- e** Click Learn More About Reference Registered Data And Copy All Data to read additional information.
- f** Answer the following questions. After you are finished, close your web browser.

1. What are the two web layer sharing options?

2. What happens to a web layer shared with the reference registered data sharing type, when a user updates the data source?

3. When using the copy all data sharing type, how is the shared web layer managed?

Data registration

Your federated ArcGIS Server site can be configured to use registered data sources other than ArcGIS Data Store. Data locations are registered with ArcGIS Server on the ArcGIS Server Manager's data store tab. This internal registry of folders, databases, cloud stores, and raster stores contain geographic data accessible to the ArcGIS Server account. An entry for the ArcGIS Data Store component is automatically created as the default Managed Database during the ArcGIS Data Store configuration.

Administrators can register additional data stores to meet their organizational needs. To register a data store, the ArcGIS Server account must have access to the data locations before you can register them in your ArcGIS Server. The method for granting access depends on the type of data that you need to register.

Depending on your environment, you will connect your enterprise to your data differently. Which connection method you choose will depend on your server setup, the location of your data, and other organizational needs and factors. The GIS server can connect to the data in the same way as the publisher or using alternate connection methods to the same data.

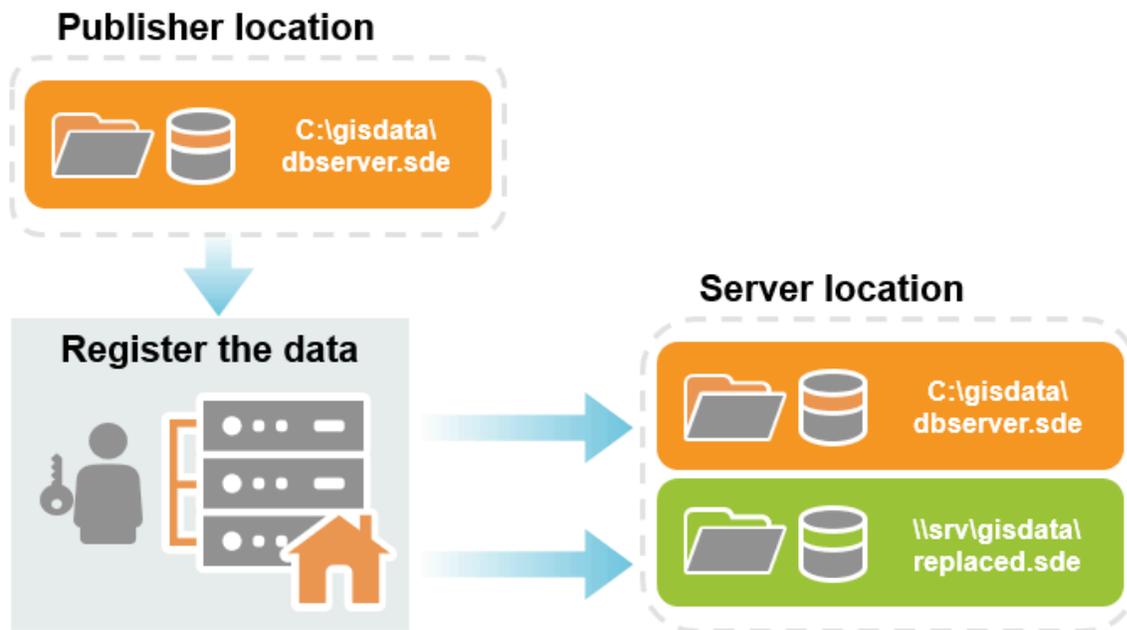


Figure 5.5. You can register your authoritative data with ArcGIS Server by referencing the data directly or by replacing the connection method.

Data registration (continued)



ArcGIS Enterprise Help: *Register your data with ArcGIS Server using Server Manager*

ArcGIS Enterprise Help: *Make your data accessible to ArcGIS Server*

Registering data with ArcGIS Server

Often, your organization's users will want to share layers and allow the underlying data to be hosted and ArcGIS-managed. Your users can optionally specify that shared layers reference your folder, enterprise geodatabase, or cloud-based GIS resources, allowing them additional control and flexibility.

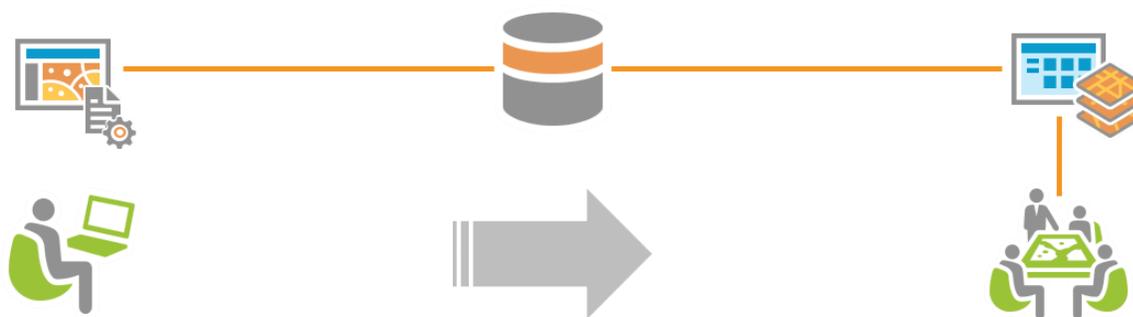


Figure 5.6. Some service types can be configured to reference user-managed data.

Work with registered data

You would like to ensure that a trail and bike network shared layer references your enterprise geodatabase, which represents the most recent data. Before you share this layer with the organization for use in applications, you will test-publish the data and view the service's workspace.

In this exercise, you will perform the following tasks:

- Register a geodatabase with ArcGIS Server.
- Share a layer with referenced data.
- Inspect the service workspace.

Step 1: Register a geodatabase with ArcGIS Server

Registering data directories, databases, and cloud storage locations provides ArcGIS Enterprise with a list of known and approved data locations. Administrators and publishers in an ArcGIS Enterprise portal can register user-managed data stores with federated ArcGIS Server sites. You will begin by registering an enterprise geodatabase using your Enterprise portal.

- a If necessary, maximize the EBASE VM (blue desktop) application window.
- b Open a browser, and then click the ArcGIS Enterprise bookmark provided (<https://ebase.ad.local/portal/home>).
- c Sign in as **portaladmin** with password **Esri.4.GIS**.
- d Click Content.
- e Click New Item and choose Data Store.

Hint: You may need to scroll down through the list of available options.

Many organizations require additional flexibility and control for their layer's data. In your organization's deployment, an enterprise geodatabase is used to store a feature class that is updated regularly. Rather than edit the data in your hosting server, you would prefer to manage it within your database server. You will share a layer that references this geodatabase as a test.

- f For Type, select Database.
- g Click Next.
- h For Type Of Database, select Relational Database.
- i Click Next.

Next, you will provide the appropriate connection file to your enterprise geodatabase.

- j For Publisher Database Connection, click Select File and browse to **C:\EsriTraining\EBAS\ManagingResources**.
- k Select `edata.sde` and click Open.
- l For Server Database Connection, select Same As Publisher Database Connection.

In this case, your database server uses database credentials for geodatabase access. The credentials are saved within your connection file, so it will not be necessary to grant the ArcGIS Server account access to the data. If your geodatabase uses operating system authentication, you must grant the ArcGIS Server account access to the data.

The publisher and server database connections will remain the same for the service that you plan to test. Later, if you decide to create a replica geodatabase to isolate it from your production geodatabase, you can change the Server Database Connection parameter to New Connection.

m Click Next.

You can choose the ArcGIS Server sites to which you want to add your data store. Your hosting server is your only federated server.

n After validation completes and the status is Normal, check the box next to your hosting server to add it to your data store.

o Click Next.

p For Title, type **MyEnterpriseGDB**.

q For Tags, type **Database**.

r Click Create Connection.

If portal members will be publishing data from this database connection in ArcGIS Pro, you would share the data store item with a group that the portal members belong to. Sharing this item allows these portal members to publish data using the same database credentials to the federated server that you specified.

s Open a new browser tab and click the bookmark for ArcGIS Server Manager (<https://ebase.ad.local/server/manager>).

t Click the Site tab.

u On the left side of the page, click Data Stores.

v Click Validate All.

<input type="checkbox"/>	Status	File Name	Type			
<input type="checkbox"/>	✓	ArcGIS_Data_Store	Relational			
<input type="checkbox"/>	✓	MyEnterpriseGDB_ds_bsehtpplkrwkqb0q	Database			
<input type="checkbox"/>	✓	ArcGIS_Data_Store	Managed Object			

1. What is the name of your site's managed database and object?

You can see your site's relational and object data stores, in addition to the enterprise geodatabase that was registered when you added the data store item in the Enterprise portal.

Your new database data store is now registered and validated with your server's site. Registering this database will provide you with additional flexibility for managing some of your layer's data.

Step 2: Share a layer with referenced data

There are many methods to share layers to ArcGIS Enterprise but two of the most common are using ArcGIS Pro and ArcGIS Server Manager. Using the ArcGIS Server Manager, you can publish a service using a service definition file. You will use an existing service definition file to add a service to your ArcGIS Enterprise deployment using the ArcGIS Server Manager.

- a In ArcGIS Server Manager, click the Services tab.
- b Click Publish Service, browse to **C:\EsriTraining\EBAS\ManagingResources**, and open the Trail_and_Bike_Network.sd file.
- c Click Next.
- d Accept the default settings and click Next.

ArcGIS Server services can be configured to support many types of functionality. By default, all map image layers are configured for Mapping support.

- e Click Next.

Because your server is federated with the portal, you can choose to share this layer with your organization.

- f Check the ArcGIS Enterprise box.

g Click Publish, and then wait until the layer finishes publishing.



If the publication does not complete within a minute, refresh your browser.

The service definition is deployed to your server site, and the layer has been shared.



Trail and Bike Network (Map Service)

Trails, bike lanes, and bike routes within Aurora, Colorado.
 Authoring Application: ArcGIS Pro
 Instance Type: Shared
 Status: Started



Step 3: Inspect the service workspace

You will now confirm that the new service references your enterprise geodatabase.

- To the right of the Trail_and_Bike_Network map service, click the Service Workspaces button .
- Click the database entry to review the Workspace Properties below.

Workspace Properties:

Property	Value
Server	EDATA
Instance	sde:postgresql:EDATA
Client	postgresql
Connection Properties	EDATA

All the database properties required to connect to and access the data are shown. After you share the production version of this service, you can be certain that users are viewing the data from your referenced enterprise geodatabase.

- Close your web browser.

ArcGIS Enterprise account uses

Throughout the course exercises, you have created and used a number of accounts for your ArcGIS Enterprise deployment and configuration.

In the following table, connect each account use with the account username needed to complete the task.

Account use	Account username
Sign in to the EBASE machine	
Configure certificates for the portal	
Federate an ArcGIS Server with a portal	
Start and stop GIS services	
Create new ArcGIS Enterprise users	
Acts as the ArcGIS Server account	
Publish content to a portal	

Answers to lesson 5 questions

Associate web layers with GIS resources (page 5-19)

1. What are the two web layer sharing options?

You can reference registered data or copy all data.

2. What happens to a web layer shared with the reference registered data sharing type, when a user updates the data source?

When a user updates the source data for a layer shared using the reference registered data sharing type, the web layer will update to reflect the changes made to the data source.

3. When using the copy all data sharing type, how is the shared web layer managed?

When using the copy all data sharing type, the web layer is managed by ArcGIS.

Exercise 5B: Work with registered data (page 5-23)

1. What is the name of your site's managed database and object?

ArcGIS_Data_Store

ArcGIS Enterprise account uses (page 5-28)

Account use	Account username
Sign in to the EBASE machine	<ul style="list-style-type: none">• adAdmin
Configure certificates for the portal	<ul style="list-style-type: none">• portaladmin
Federate an ArcGIS Server with a portal	<ul style="list-style-type: none">• portaladmin• siteadmin
Start and stop GIS services	<ul style="list-style-type: none">• portaladmin• siteadmin

Answers to lesson 5 questions (continued)

(Table continued from previous page)

Account use	Account username
Create new ArcGIS Enterprise users	• portaladmin
Acts as the ArcGIS Server account	• ad.local\arcgis\$
Publish content to a portal	• portaladmin

Workflow review (page 5-29)

1. When might you want to install and configure additional data stores?

You may want to install and configure additional data stores when you need additional space to store items or when you want to add more types of service storage.

2. What are some ways that your organization will manage the GIS resources in your ArcGIS Enterprise deployment?

Answers will vary but may include ArcGIS Data Store, registered Enterprise geodatabases, or registered folders.

You now know how to ensure that all network traffic is encrypted between ArcGIS Enterprise components. By default, an internal identity store is configured for the ArcGIS Enterprise portal with the initial administrator account that you specify. While this configuration will allow you to initially test and develop your deployment, you must eventually decide how you will manage access for all your ArcGIS Enterprise member accounts.

ArcGIS Enterprise is designed to flexibly accommodate many different authentication protocols. To effectively limit who can access your Enterprise portal and control which users can administer and publish items and services, you must select an identity store and authentication scheme.

There are other enhancements to security that can be checked for your base deployment. ArcGIS Enterprise provides resources for analyzing your Enterprise portal and ArcGIS Server machines for security vulnerabilities. If any security issues are discovered, information on how to address these issues is provided.

Topics covered

■ Choosing and configuring an identity store

■ Configuring user authentication

■ ArcGIS Enterprise security best practices

Understanding identity stores

An identity store is a location where users and roles are managed. ArcGIS Enterprise supports several different identity stores, allowing you to use the built-in model or integrate external ones in support of your organization's needs.

Built-in identity store

You already learned that federating your ArcGIS Server site with the Enterprise portal resulted in GIS service access being controlled by portal credentials. In a base deployment, your Enterprise portal manages access to services, groups, and other content using its built-in identity store.

The built-in identity store is most useful when you are getting ArcGIS Enterprise up and running and performing development and testing tasks.

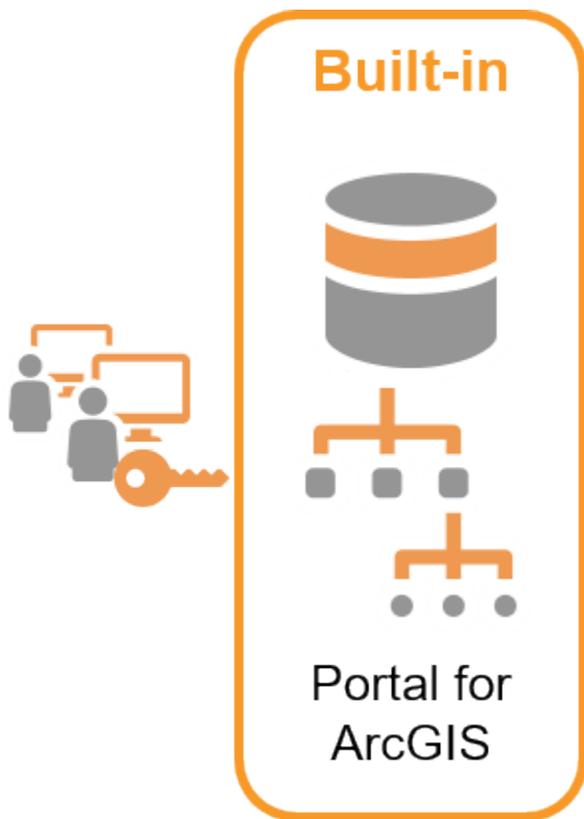


Figure 6.1. The built-in identity store comes with Portal for ArcGIS.

Understanding identity stores (continued)

Organization-specific security store

If your organization manages its own accounts, you can use them to manage or control access to your ArcGIS Enterprise content. After it is configured, your users can provide their enterprise credentials to sign in to ArcGIS Enterprise. An organization-specific security store is most useful when you want to use your organization's security policies (for example, password expiration, complexity requirements, and controlling access using your existing enterprise groups).

The supported organization-specific security store includes the following:

- LDAP (Lightweight Directory Access Protocol) server
- Active Directory server
- Identity providers that support Open ID Connect or SAML (Security Assertion Markup Language) 2.0 Web Single Sign-On

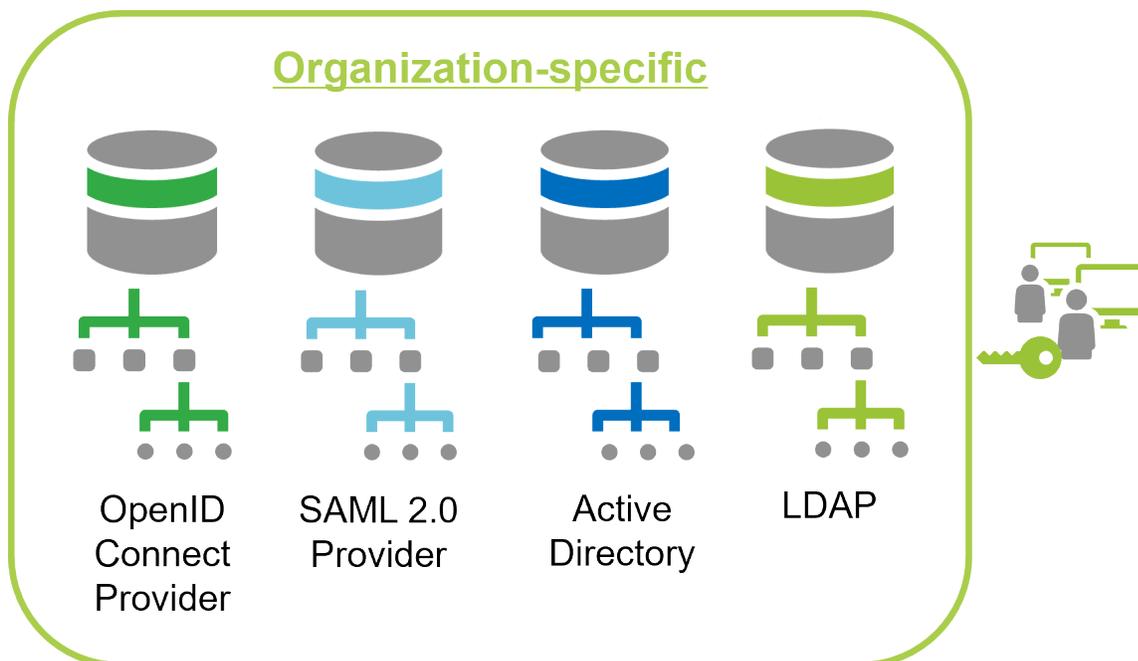


Figure 6.2. Organization-specific security stores can include OpenID Connect, SAML 2.0, Active Directory, and LDAP.

Understanding identity stores (continued)

Multiple identity stores

You can also control access to your deployment with multiple identity stores. Your users can sign in with built-in accounts and from one or more OpenID Connect or SAML identity providers that are configured to trust each other. This type of configuration provides more flexibility for allowing access from both outside and inside your organization.

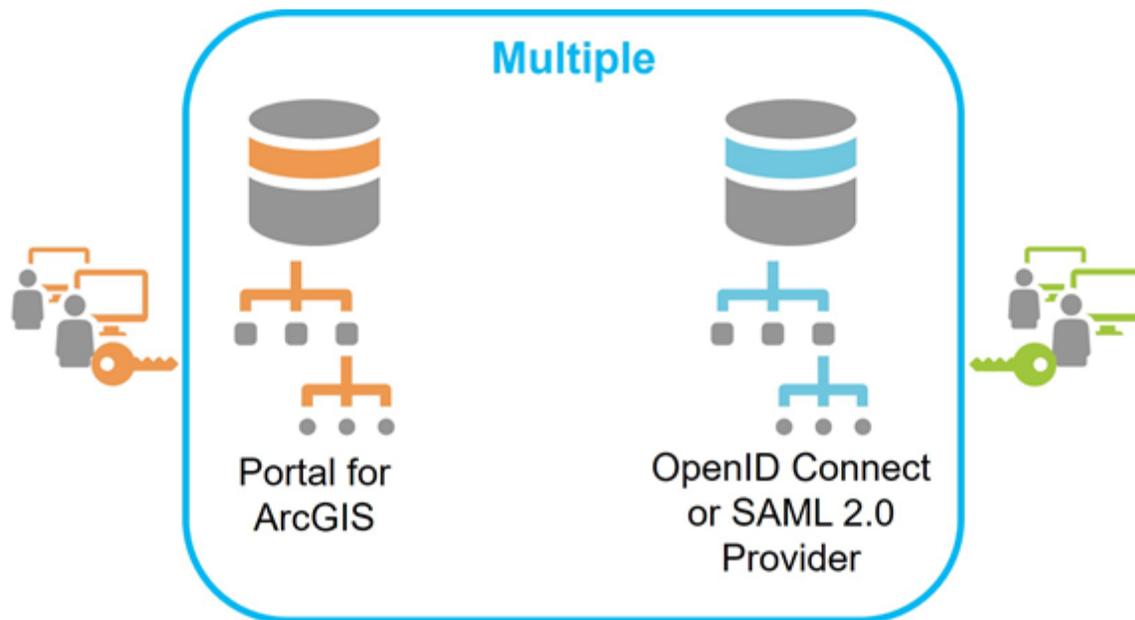


Figure 6.3. Multiple identity stores can be used together.



ArcGIS Enterprise Help:

Configuring a SAML-compliant identity provider with your portal

Configure OpenID Connect logins

Configuring portal authentication

Authentication is the process of controlling access and processing a user's credentials to verify that user's identity. ArcGIS Enterprise provides multiple methods for handling authentication to accommodate different protocols and to provide a flexible framework for identity store and login behavior preferences. Authentication can take place at the portal tier or the web tier, depending on your chosen identity stores and security policies. Login credentials can be grouped into two general categories:

1. Built-in users and groups logins: The Enterprise portal handles all authentication for built-in users and groups internally.
2. Enterprise logins: You can choose between configuring authentication to occur at the web tier (through ArcGIS Web Adaptor) or at the portal tier or externally depending on your organization's needs.

Configuring portal authentication (continued)

Portal tier authentication

Identity store	Web server notes	ArcGIS Web Adaptor edition
Built-in, Active Directory, or LDAP	<ul style="list-style-type: none"> • IIS or Java application server • Anonymous access enabled 	IIS or Java Platform

Additional considerations

- Anonymous access must be enabled on your web server
- Users are required to provide credentials (SSO is not supported)
- Useful method when access from both enterprise and built-in identity stores must be allowed

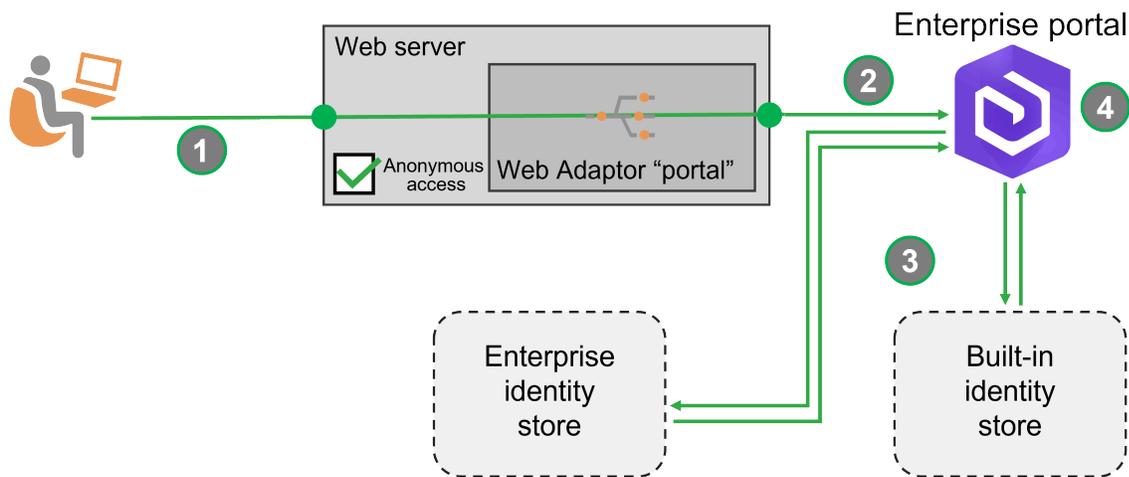


Figure 6.4. In this conceptual diagram of portal tier authentication, the login process begins by browsing to the portal home app (1). The user must provide credentials to sign in (2). The credentials are then authenticated (3). Depending on how ArcGIS Enterprise is configured, the Enterprise portal can use the built-in identity store or an enterprise identity store to authenticate the credentials. The Enterprise portal can then verify member status (4).

Configuring portal authentication (continued)

Web tier authentication

Identity store	Web server notes	ArcGIS Web Adaptor edition
Active Directory	<ul style="list-style-type: none"> • IIS • Integrated Windows Authentication (IWA) enabled • Single sign-on (SSO) supported 	IIS
LDAP	<ul style="list-style-type: none"> • Java application server 	Java Platform

Additional considerations

- Anonymous access is disabled on your web server
- Windows Active Directory and IIS web server environments can take advantage of IWA for an SSO experience
- To use an LDAP directory, ArcGIS Web Adaptor is deployed to a Java application server
- Public key infrastructures (PKIs) are certificate based and can be used with Active Directory (IIS ArcGIS Web Adaptor) or LDAP (Java Platform ArcGIS Web Adaptor); anonymous access is not supported

Configuring portal authentication (continued)

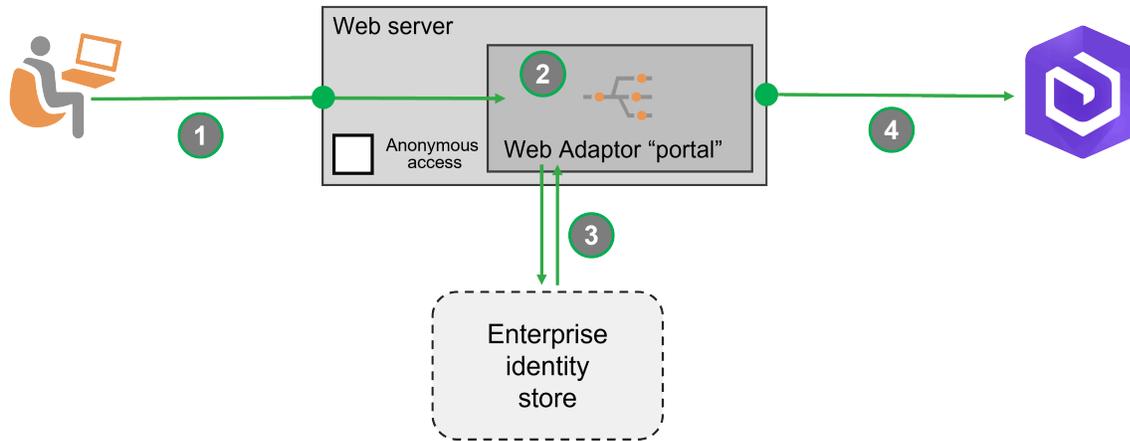


Figure 6.5. With web tier authentication, the login process begins by browsing to the portal home app (1). Anonymous access is disabled on the web server, and the web adaptor is responsible for authenticating the user's credentials (2). An enterprise identity store is used to authenticate the credentials (3). The Enterprise portal can then verify member status (4) to complete the login.

Configuring portal authentication (continued)

External tier authentication

Identity store	Web server notes	ArcGIS Web Adaptor edition
SAML 2.0 or OpenID Connect	<ul style="list-style-type: none"> • IIS or Java application server • SSO supported 	IIS or Java Platform

Additional considerations

- SAML and OpenID Connect (OIDC) are open standards that provide convenience and flexibility for connecting an enterprise identity provider with the Enterprise portal
- Users and groups from the identity provider are both supported
- SSO is supported

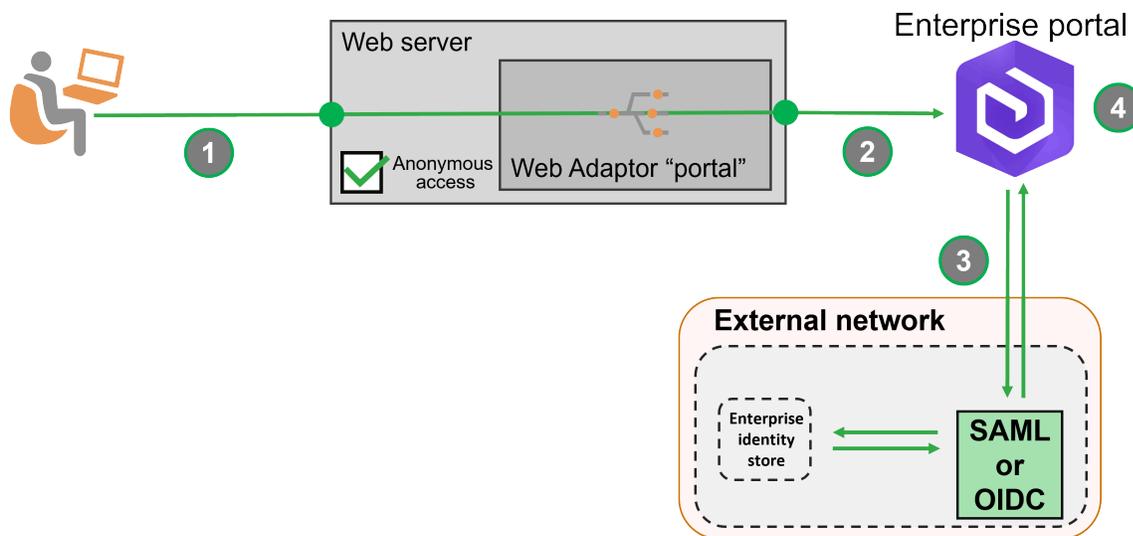


Figure 6.6. In this conceptual diagram of external authentication, the login process begins by browsing to the portal home app (1). The user must provide credentials to sign in (2). The credentials are then authenticated using a SAML-compliant or OpenID Connect-compliant identity provider (3). The Enterprise portal can then verify member status (4).



ArcGIS Enterprise Help: [About configuring portal authentication](#)

ArcGIS Enterprise Help: [Disabling anonymous access](#)

Choosing an authentication method

There are several options for configuring authentication for your base ArcGIS Enterprise deployment.

In the following scenarios, consider the operating systems, web server technology, and identity stores. Choose the best authentication method for each scenario. Be prepared to discuss the reasoning for your answers.

Scenario 1: Linux with LDAP

Your organization plans to implement a base ArcGIS Enterprise deployment in a Linux environment. Your users are maintained in an LDAP identity store, a Java application server with anonymous access disabled, and ArcGIS Web Adaptor for Java Platform.

1. Which kind of authentication will this configuration use?

Scenario 2: Internal and external users

Your organization will be hiring contractors to support a project, and you'll give them access to your portal. You decide to configure your ArcGIS Enterprise to support logins with both a SAML identity store for employees of your organization and a built-in identity store for the contractors.

2. Which kind of authentication will this configuration use?

Scenario 3: Active Directory SSO

Your organization uses an Active Directory identity store for all users. IIS is used for all web servers. You would like to configure an SSO environment for your users that runs the Windows

Choosing an authentication method (continued)

operating system.

3. Which kind of authentication will this configuration use?

Setting up an enterprise identity store

ArcGIS Enterprise is designed to integrate with your organization's enterprise identity stores.



Configure your portal to only allow HTTPS communication before integrating your enterprise identity store.

Portal for ArcGIS



HTTPS



Portal Administrator Directory



```
{
  "type": "WINDOWS",
  "properties": {
    "userPassword": "Esri.4.GIS",
    "isPasswordEncrypted": "false",
    "user": "ad\\arcgisad",
    "userFullnameAttribute": "cn",
    "userEmailAttribute": "mail",
    "userGivenNameAttribute": "givenName",
    "userSurnameAttribute": "sn",
    "caseSensitive": "false"
  }
}
```

Figure 6.7. When setting up an enterprise identity store, you must first confirm that the portal only allows for HTTPS communication. Then, go to the Portal Administrator Directory and modify the security settings in the portal admin directory to connect the portal to the IT-managed identity store.



The password that you provide is encrypted during the update process.



ArcGIS Enterprise Help: *Use Integrated Windows Authentication with your portal*
ArcGIS for Developers Help: *Update Identity Store*

Configure an enterprise identity store and authentication

Your organization already uses Active Directory as its identity store. To make ArcGIS Enterprise as easy as possible to use, you will configure your portal's identity store and web-tier authentication to enable an SSO experience.

In this exercise, you will perform the following tasks:

- Configure enterprise logins.
- Set an Enterprise portal administrator.
- Configure web-tier authentication.
- Test the SSO.

Step 1: Configure enterprise logins

First, you will associate your organization's IT-managed security store with your Enterprise portal. You will perform this step using the Portal Administrator Directory.

- a If necessary, maximize the EBASE VM (blue desktop) application window.
- b Open a web browser and go to the Portal Administrator Directory (<https://ebase.ad.local/portal/portaladmin>).
- c Click Login and sign in as **portaladmin** with the password **Esri.4.GIS**.
- d From the Site Root, click Security.
- e Within Security, click Config.

Security Configuration

```

Properties:           {"disableServicesDirectory":false,"
User store configuration:  {"type": "BUILTIN", "properties":
Group store configuration: {"type": "BUILTIN", "properties":

```

1. What is the current User Store Configuration type?

- f Click Update Identity Store.

The code that you see within the text boxes is JavaScript Object Notation (JSON). You will update the user store configuration to use your organization's enterprise logins by adding a block of code with your organization's details.

- g Open File Explorer and browse to **C:\EsriTraining\EBAS\SecuringBaseDeployment**.
- h Double-click the UserStoreConfig.txt file to open it in Notepad.
- i Select the text in the Step 1 section and copy it to the clipboard.

Hint: Ensure you copy the beginning and ending curly braces ({ }) as well.

- j Return to your browser.

You will now replace the existing text with the text that you copied.

- k For User Store Configuration, select the existing text and paste in the text from the clipboard.



Be sure to remove the existing text—only the updated text should appear in the text box.

- l Click Update Configuration.

Security Configuration

Properties: `{"disableServicesDirectory":false,"en:`

User store configuration: `{ "type": "WINDOWS", "properties":`

Group store configuration: `{ "type": "BUILTIN", "properties": {"i:`

2. What is the User Store Configuration type?

The user account's credentials are now being used to provide access to your organization's Active Directory domain.

Step 2: Assign an enterprise portal administrator

You previously used a built-in portal account to administer the portal. Now that your Active Directory domain is accessible, you will assign an enterprise account as a portal administrator.

- a Open a new browser tab and click the bookmark for ArcGIS Enterprise (<https://ebase.ad.local/portal/home/>).
- b Sign in as **portaladmin** with the password **Esri.4.GIS**, if necessary.
- c If necessary, click Organization.
- d Click Members, and then click Add Members.

- e Select Add Members Based On Existing Active Directory Or LDAP Users.
- f Click Next.
- g Click New Member.
- h For Username, type **adadmin** and click Search For User.

A new window opens with the search results. The portal is using the account specified earlier to access the Active Directory domain and return these results.

- i In the Select User window, click the AD\adAdmin search result to select it.
- j Click Select User.
- k If necessary, in the User Type list, click Creator.
- l For Role, click the down arrow and choose Administrator.

Hint: If a View Saved Logins prompt blocks the Administrator choice, right-click the prompt to clear it, and then choose Administrator.

- m Click Next.
- n On the Compile Member List page, click Next.

You will not add any groups to adAdmin now.

- o On the Set Member Properties page, click Next.
- p Click Add Members.
- q Review the members page and confirm that adAdmin (adAdmin@AD) is listed with Creator user type and Administrator role.



If a role other than Administrator is listed, change the role to Administrator.

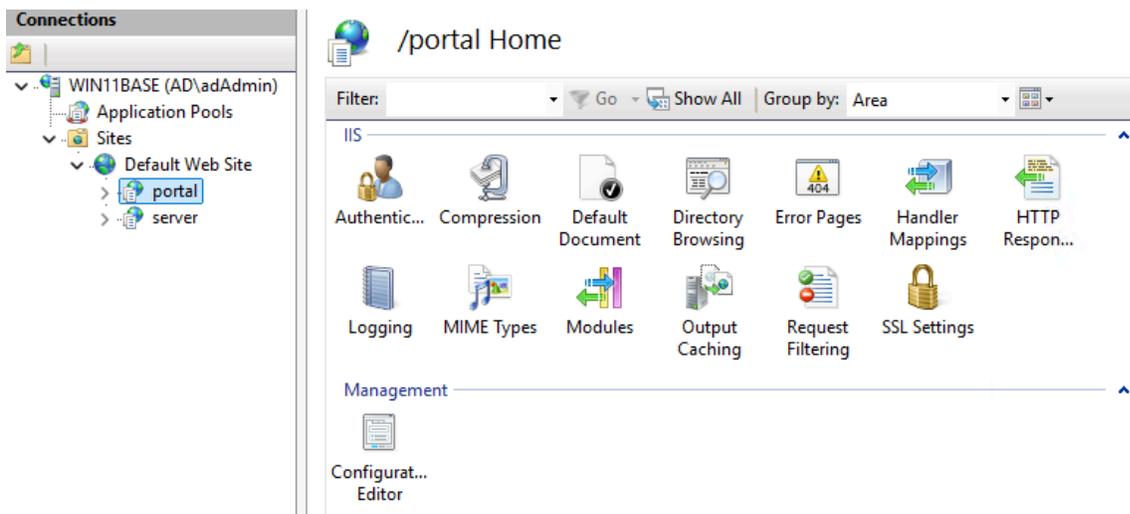
<input type="checkbox"/> Member	Last login	User type	Role
<input type="checkbox"/>  portaladmin built-in portaladmin	Today	Creator	Administrator ▾ ...
<input type="checkbox"/>  adAdmin adAdmin@AD	Never	Creator	Administrator ▾ ...

Your Active Directory enterprise login is now a member of your ArcGIS Enterprise organization.

Step 3: Configure web-tier authentication

To complete the integrated operating system authentication process, you must configure web-tier authentication.

- a Click the Windows Start button, and then type **iis**.
- b In the search results, click Internet Information Services (IIS) Manager.
- c In the Connections pane, expand the WIN11BASE web server object.
- d Under the WIN11BASE web server object, expand the Sites folder.
- e Under the Sites folder, expand the Default Web Site object.
- f Click the portal web adaptor object.



- g On the Features View tab, under the IIS section, double-click Authentication.
- h In the Authentication pane, right-click Anonymous Authentication and choose Disable.
- i Right-click Windows Authentication and choose Enable.
- j Close IIS Manager.

Step 4: Test the SSO

Before you test the SSO experience, you will prepare your system for the change. First, you will clear your browser's cache to remove any previous authentication resources.

- a Restore your browser.
- b Press Shift+Control+Delete.
- c For Time Range, select All Time.
- d Check all options except Browsing History, and then click Delete Data.
- e Close all open applications.

You will restart your Windows session.

- f Click the Windows Start button, and then click the user icon (adAdmin).
- g Click Sign Out.
- h Double-click the EBASE.rdp shortcut on the host, and, if necessary, enter the adAdmin credentials (**adAdmin/Esri.4.GIS**).
- i Open the browser, and then click the ArcGIS Enterprise bookmark.

Your Active Directory enterprise login is passed to the IIS web server, which processes your credentials and authenticates you.



- j Update the browser URL to **https://ebase.ad.local/server/manager** and press Enter.



It might take several minutes as your credentials are processed before the web page loads.

This SSO behavior will be convenient for your organization's users. It will also allow you to continue managing your organization's account management policies separately from ArcGIS Enterprise.

- k Close all open application windows within the EBASE VM.

Security best practices

ArcGIS Enterprise, like any software solution, must be configured in support of your organization's security policies. Practices such as staying up to date with software security patches can ensure enterprise security. Every aspect of your unique environment (networking, hardware, and software) should be considered to be effective in securing your organization's resources.

You will now think about ways in which security could be configured and enhanced for a base ArcGIS Enterprise deployment. As you consider the questions, think about what you have learned so far, and combine that knowledge with what you already know about information technology security concepts from your own experiences.

What IT security policies does your organization currently enforce?



ArcGIS Enterprise Help: Best practices for configuring a secure environment

ArcGIS Trust Center: ArcGIS—Secure and Trustworthy

ArcGIS Enterprise security options

Each organization has a unique set of security needs. Before you can formulate your organization's security strategy, you must understand what options are available for ArcGIS Server and Portal for ArcGIS.

Portal for ArcGIS

- Restrict proxy capability
- Restrict file permissions
- Specify default token expiration
- Configure firewall
- Disable ArcGIS Portal Directory
- Disable anonymous access
- Configure your own server certificate
- Configure HTTPS
- Configure email settings
- Use a group Managed Service Account

ArcGIS Server

- Scan for cross-site scripting attacks
- Secure token transmission

ArcGIS Enterprise security options (continued)

- Use a group managed service account
- Disable PSA account
- Use standardized queries
- Disable Services Directory
- Configure your own server certificate
- Restrict file permissions
- Define a token shared key
- Restrict cross-domain requests



ArcGIS Enterprise Help: *Best practices for configuring a secure environment*

ArcGIS Enterprise Help: *Security best practices*

Evaluate security for a base deployment

Before you open up your base deployment to your organization, you will analyze your systems for security vulnerabilities. You will implement security best practices based on your organization's policies.

In this exercise, you will perform the following tasks:

- Scan Portal for ArcGIS for security best practices.
- Scan ArcGIS Server for security best practices.



ArcGIS Enterprise Help: *Scan your portal for security best practices*

ArcGIS Enterprise Help: *Scan ArcGIS Server for security best practices*

Step 1: Scan your Portal for ArcGIS for security best practices

Portal for ArcGIS can be scanned for security best practices using the existing PortalScan tool included with the portal install or scanned using the included Python script. Now, you will use the PortalScan tool to scan your portal for best practices.

- a Verify that you are working within the EBASE VM (blue desktop).
- b In File Explorer, browse to **C:\Program Files\ArcGIS\Portal\tools\security**.

The Security folder contains the portalScan.py file and the portalScan.bat file. The portalScan.py is a Python script that you can run using the Command Prompt. It also contains portalScan.bat, which provides a guided experience and can be run if you cannot run Python scripts.

- c In File Explorer, double-click portalScan.bat.

The Command Prompt will open, asking for the Portal for ArcGIS hostname. The window will walk you through the tool's parameters.

- d For the Enter Portal for ArcGIS hostname [ebase.ad.local] parameter, type **ebase.ad.local** and press Enter.
- e For the Enter Administrator Username parameter, type **portaladmin** and press Enter.
- f For the Enter Administrator Password parameter, type **Esri.4.GIS** and press Enter.



For security reasons the password will not display in the Command Prompt.

- g For the Enter Output Directory parameter, type **C:\EsriTraining\EBAS\SecuringBaseDeployment** and press Enter.

After you enter the output directory, the Command Prompt will disappear, which indicates that the tool has been run.

- h In File Explorer, browse to **C:\EsriTraining\EBAS\SecuringBaseDeployment**, and then double-click the portalScanReport_ebase_<date>.html file to open it in your default browser.



The <date> portion of the report's file name will be your system's current date.

The report opens in your browser. At this point, you will focus on critical severity items.

<u>Id</u>	<u>Severity</u>	<u>Property Tested</u>	<u>Scan Results</u>
PS01	Critical	Proxy restrictions	The portal proxy capability is unrestricted. This should be limited to trusted web addresses. More information
PS14	Important	Default print service status	The default print service distributed with your portal is currently enabled. Since the portal is already configured to use a print service from ArcGIS Server, it is recommended to disable the default print service. More information
PS03	Important	Portal services directory	The portal services directory is accessible through a web browser. This should be disabled to reduce the chances that your portal items, services, web maps, groups, and other resources can be browsed, found in a web search, or queried through HTML forms. More information
PS06	Recommended	Anonymous access	To prevent any user from accessing the Home application without first providing credentials to the portal, it is recommended that you configure your portal to disable anonymous access. More information
PS09	Recommended	Cross-domain requests	Cross-domain (CORS) requests are unrestricted. To reduce the possibility of an unknown application accessing a shared portal item, it is recommended to restrict cross-domain requests to applications hosted only in domains that you trust. More information
PS17	Recommended	KML service status	The KML service is used by the portal to communicate with KML endpoints. If no KML endpoints will be accessed through any web maps on the portal, it is recommended to disable this service. More information
PS16	Recommended	RSS service status	The RSS service is used by the portal to communicate with GeoRSS feeds. If no GeoRSS feeds will be accessed through any web maps on the portal, it is recommended to disable this service. More information

i To the right of the first critical severity item with an Id of PS01, click More Information.

The relevant help topic in the Portal for ArcGIS documentation opens for a full explanation of the item.

The sharing proxy is used in situations where a remote server hosted on a different domain does not support Cross-Origin Resource Sharing (CORS), or in cases where web service credentials are saved with the portal item. This warning informs you that the Portal's sharing proxy is allowed to make requests to any site, which could potentially be used to launch a Server-Side Request Forgery (SSRF) attack. An SSRF may potentially result in information disclosure issues or a denial-of-service condition. It is recommended that you restrict the proxy to only access preapproved, validated hosts. If you have federated ArcGIS Server with your portal, the list must contain the addresses of all machines in the site, as well as any resource that is shared as an item in the portal.

- j** In your web browser, open a new tab and go to **https://ebase.ad.local/portal/portaladmin**.
- k** In the Portal Administrator Directory, click Security, click Config, and then click Update Security Configuration.
- l** Open File Explorer, browse to **C:\EsriTraining\EBAS\SecuringBaseDeployment**, and open the BestPracticeCommands.txt file.
- m** Under the Step 1 section, copy the line that reads , *"allowedProxyHosts": "ebase.ad.local"*.



Be sure to copy the comma at the beginning of the line.

- n In the Update Security Configuration text box, insert your cursor right before the ending curly bracket.
- o Paste the line that you copied.

Home > Security > Config > Update Security Configuration

Update Security Configuration

```
{"disableServicesDirectory":false,"enableAutomaticAccountCreation":false,"webgisServerTrustKey": "NbsTbLNaU+2itH+7qPJDg+QICcmgwUH8y5P4yNuEMI=", "allowedProxyHosts": "ibase.ad.local"}
```

- p Click Update Configuration.

This critical severity security item has been addressed.

- q Close the web browser but keep the text file windows open for the next step.

Step 2: Scan your ArcGIS Server for security best practices

ArcGIS Server does not have a .bat tool, but script is provided with ArcGIS Server to scan your site for security best practices. This script can be run using the Command Prompt if your machine is configured to run Python scripts in the Command Prompt.

- a Click the Windows Start button and type **cmd**, but do not press Enter.
- b Right-click the Command Prompt search result and choose Run As Administrator.
- c In File Explorer, from the BestPracticeCommands text file, copy the command under Step 2 section that reads `cd \Program Files\ArcGIS\Server\tools\admin`, paste it into the command window, and press Enter.

Hint: Right-clicking to paste the command also works.

- d Copy and execute the next line that reads `python serverScan.py -h`.

The parameters for the serverScan script are identical to those parameters for the portalScan tool. However, you must provide the ArcGIS Server primary site administrator credentials for this

script instead of your Portal for ArcGIS credentials.

e Copy and execute the next line that reads

```
python serverScan.py -n ebase.ad.local -u siteadmin -p Esri.4.GIS -o \EsriTraining\EBAS\SecuringBaseDeployment.
```

f In File Explorer, browse to **..\EsriTraining\EBAS\SecuringBaseDeployment**, and then double-click the `serverScanReport_ebase_<date>.html` file to open it in your default browser.

<u>ID</u>	<u>Severity</u>	<u>Property Tested</u>	<u>Scan Results</u>
SS08	Important	Cross-domain requests	Cross-domain requests for REST endpoints are unrestricted. To reduce the possibility of an unknown application sending malicious requests to your web services, it is recommended to restrict the use of your services to applications hosted only in domains that you trust. More information
SS08	Important	Cross-domain requests	Cross-domain requests for SOAP endpoints are unrestricted; this applies to OGC endpoints (WMS, WFS, etc.) that are exposed as well. To reduce the possibility of an unknown application sending malicious requests to your web services, it is recommended to restrict the use of your services to applications hosted only in domains that you trust. More information
SS07	Important	Rest services directory	The Rest services directory is accessible through a web browser. Unless being actively used to search for and find services by users, this should be disabled to reduce the chance that your services can be browsed, found in a web search, or queried through HTML forms. This also provides further protection against cross-site scripting (XSS) attacks. More information
SS11	Recommended	PSA account status	The primary site administrator account is enabled. It is recommended that you disable this account to ensure that there is not another way to administer ArcGIS Server other than the group or role that has been specified in your configuration. More information

The report details several security issues in a similar format as the portal scan results. These reports provide you with the information to maintain your deployment configured in support of your organization's security policies. You should consider running these scripts periodically.

g Close all open application windows within the EBASE VM.

Workflow review

Your base deployment now has an identity store and an authentication scheme in place. You have reviewed your deployment's security and can now confidently begin managing your users, groups, and content with your organization.

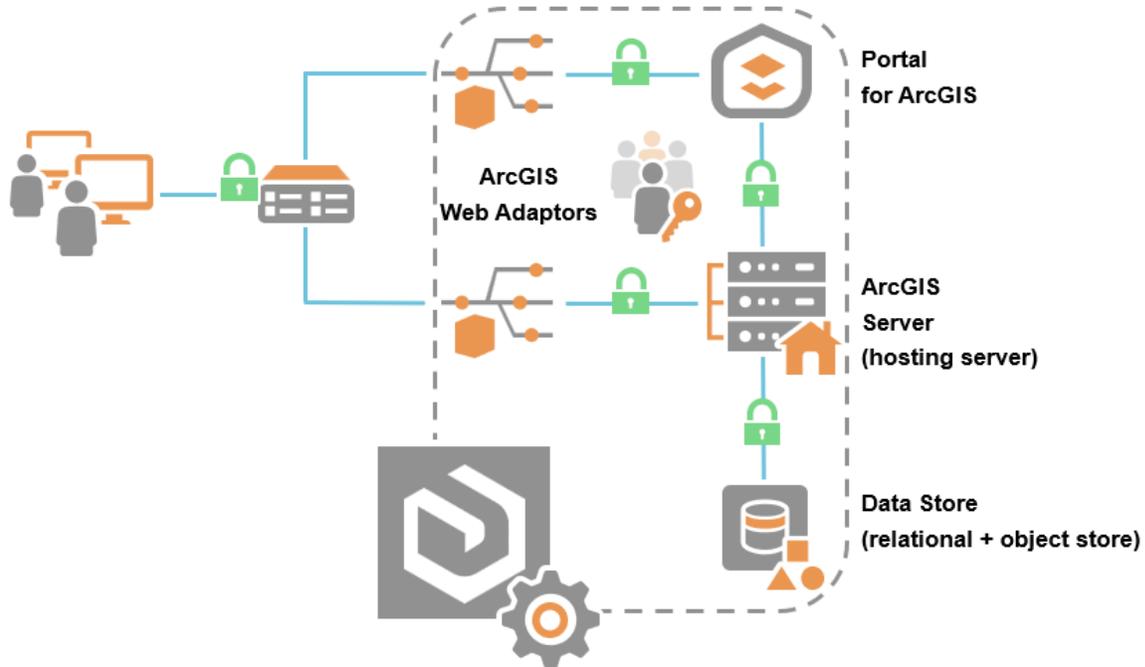


Figure 6.8. The base ArcGIS Enterprise deployment now includes integrated enterprise authentication.

1. What are some login methods for managing members in your portal?

Workflow review (continued)

2. What security best practices do you plan on implementing?

Answers to lesson 6 questions

Choosing an authentication method (page 6-10)

Scenario 1: Linux with LDAP

1. Which kind of authentication will this configuration use?

Web-tier authentication will be used because anonymous access is being disabled.

Scenario 2: Internal and external users

2. Which kind of authentication will this configuration use?

Portal-tier for internal use for built-in identity store and external for external use through SAML will be used because two types of logins must be: built-in identity store and SAML identity store.

Scenario 3: Active Directory SSO

3. Which kind of authentication will this configuration use?

Web-tier authentication will be used because the authentication must use SSO. SSO authentication excludes portal-tier from being utilized, and the use of Active Directory indicates that web-tier should be used instead of external.

Exercise 6A: Configure an enterprise identity store and authentication

(page 6-13)

1. What is the current User Store Configuration type?

BUILTIN

2. What is the User Store Configuration type?

WINDOWS

Answers to lesson 6 questions (continued)

Workflow review (page 6-27)

1. What are some login methods for managing members in your portal?

Answers may include: built-in portal accounts, organization-specific logins, active directory, or Lightweight Directory Access Protocol

2. What security best practices do you plan on implementing?

Answers may include: restrict proxy capability, restrict file permissions, disable anonymous access, configure your own server certificate, specify default token expiration, configure firewall, disable ArcGIS Portal Directory, configure HTTPS, scan for cross-site scripting attacks, secure token transmission, use a group managed service account, disable PSA account, use standardized queries, disable Services Directory, restrict file permissions, define a token shared key, restrict cross-domain requests.

As you prepare your base ArcGIS Enterprise deployment for your organization's use, you will need to consider all your users' needs. Users perform different workflows, from everyday departmental responsibilities to working on occasional special projects. The ArcGIS Enterprise portal allows you to customize your users' access and privileges, ensuring that they can be productive while still protecting sensitive information.

Each member of your Enterprise portal can be assigned to default roles. These roles are preconfigured with privileges that are appropriate to their particular needs, or custom privileges can be configured.

The Enterprise portal is populated with members who can be further organized into groups. These groups are a powerful way to manage access to shared items and functionality. As the portal administrator, you can choose to integrate your existing organization-specific security store groups with the Enterprise portal's groups.

Topics covered

Sharing content using the ArcGIS Enterprise portal

Sharing levels and user types and roles

Integrating groups to manage portal members

Sharing portal content

The Enterprise portal is an organized collection of items optimized to allow members to discover, use, make, and share content. Groups make it simple to share items with teams of users.

Membership in your Enterprise portal allows your organization's members to own content and participate in groups.

Members

Members have the following abilities:

- Create, own, and manage content.
- Create, join, and manage groups.

Items

Items are the supported content units of the portal. Some examples include the following:

- Services published to federated ArcGIS Server sites
- Hosted services
- Applications
- Supported files

Tags

Tags are an important element of your Enterprise portal. Tags provide a keyword index for fast searching of your organization's items and groups.

Three key relationships exist between members, groups, items, and tags:

- Members can own items and groups.
- Groups organize and control access to items.

Sharing portal content (continued)

- Tags integrate both items and groups to make the content organized and simpler to locate quickly.

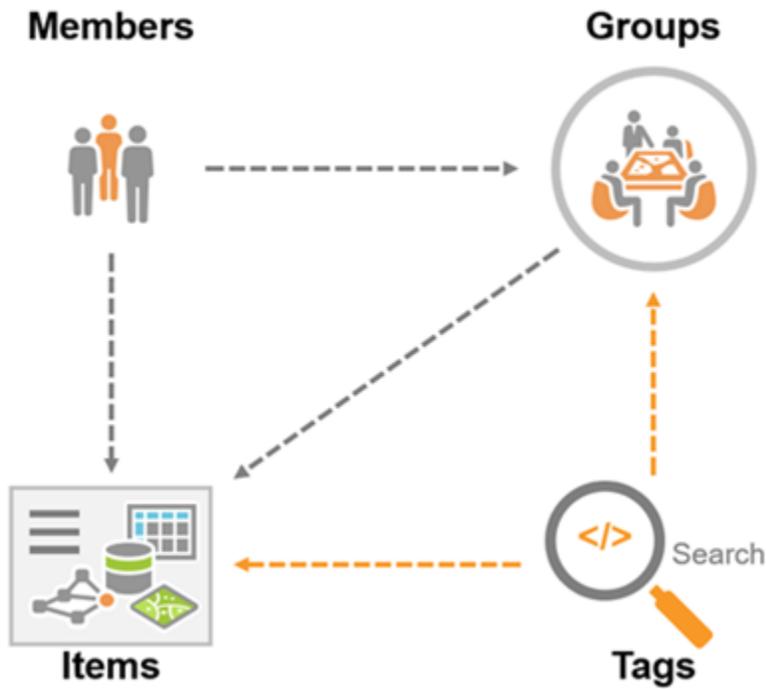


Figure 7.1. Portal provides the framework for an intuitive, productive workspace for sharing content with your organization.

Levels of sharing

When items are shared within ArcGIS Enterprise, there are several levels of sharing to consider.

Unshared



By default, all new content will be private. This setting is most appropriate for projects where no collaboration is needed. Any unshared items will only be accessible by the owner and all administrator-role members.

Group



Sharing items with a group makes the items accessible to all members of the group. Administrator-role members can also access all group content.

Organization (your portal)



When items are shared to your organization, all Enterprise portal members within your organization can access them.

Everyone



If anonymous access is enabled, anyone with network access to your Enterprise portal can access items that have been shared with everyone. If this option is available to members, they can also combine it with other sharing levels. For example, if items are shared with the Featured Maps and Apps group and the organization, then only Enterprise portal members will be able to access those items within that group. If items are shared with the Featured Maps and Apps group and everyone, then both Enterprise portal members and anonymous access users will be able to access those items within that group.

Levels of sharing (continued)

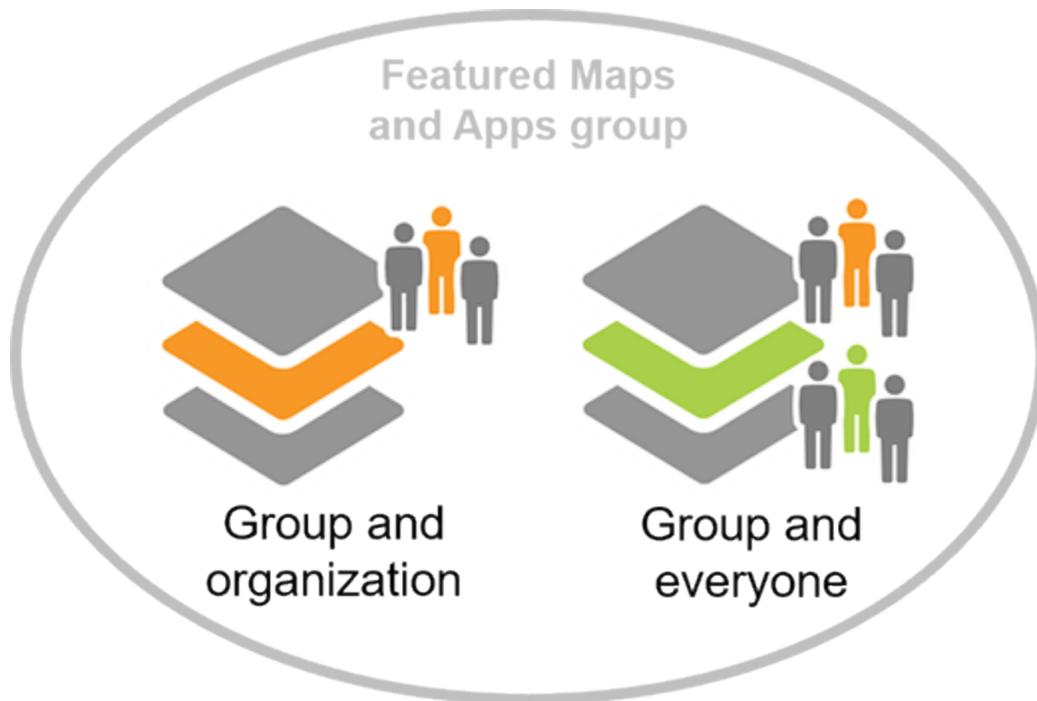


Figure 7.2. Sharing to a group and the organization or a group and everyone are two ways that sharing levels can be combined.



In many cases, it is recommended that you disable anonymous access to your Enterprise portal, especially if it is exposed to the internet.



ArcGIS Enterprise Help: Share items

User types

When you purchase ArcGIS Enterprise, it is licensed with various user types to fit your organizational needs. You can decide how to assign these user types to the members in your organization based on their individual needs and requirements. A user type determines the apps available to the member by default as well as the privileges the user has in the organization through the user's role. As necessary, an organization can also assign apps and provision add-on licenses.

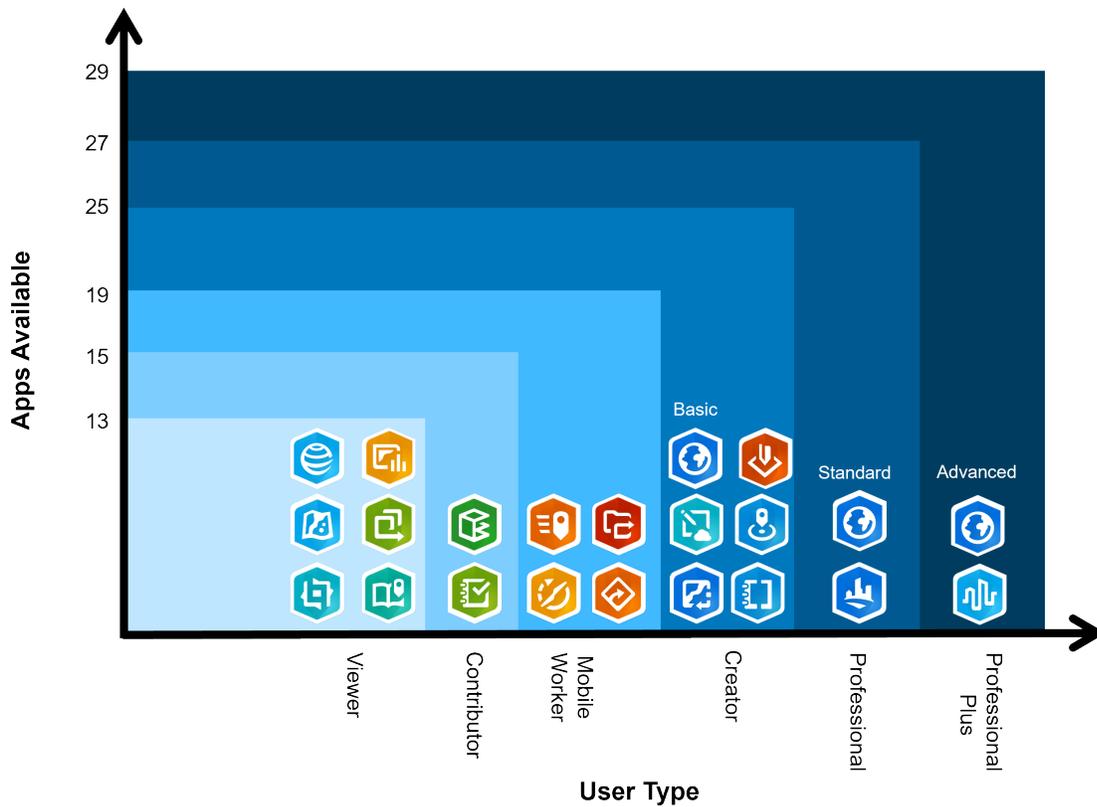


Figure 7.3. Six user types are available in ArcGIS Enterprise. These user types are Viewer, Contributor, Mobile Worker, Creator, Professional, and Professional Plus. Each user type includes access to specific apps. As the user type changes from Viewer to Professional Plus, a user gains access to more applications.

User types (continued)

User type	Description
Viewer	Has access to the following apps: <ul style="list-style-type: none"> • ArcGIS for AutoCAD • ArcGIS Dashboards • ArcGIS Earth • ArcGIS Experience Builder • ArcGIS Field Maps • ArcGIS Instant Apps • ArcGIS Living Atlas of the World • ArcGIS Maps for Adobe Creative Cloud • ArcGIS for Microsoft 365 • ArcGIS for PowerBI • ArcGIS StoryMaps • ArcGIS Map Viewer • ArcGIS Scene Viewer
Contributor	Has all the apps of the Viewer, plus: <ul style="list-style-type: none"> • ArcGIS Survey123 • ArcGIS GeoBIM
Mobile Worker	Has all the apps of the Contributor, plus: <ul style="list-style-type: none"> • ArcGIS Flight • ArcGIS Navigator • ArcGIS QuickCapture • ArcGIS Workforce
Creator	Has all the apps of the Mobile Worker, plus: <ul style="list-style-type: none"> • ArcGIS Pro Basic • ArcGIS Connectors for Power Automate • ArcGIS Excalibur • ArcGIS Notebooks • ArcGIS Web Editor • ArcGIS Business Analyst Web App Standard

User types (continued)

(Table continued from previous page)

User type	Description
Professional	Has all the apps of the Creator, plus: <ul style="list-style-type: none">• ArcGIS Pro Standard• ArcGIS CityEngine
Professional Plus	Has all the apps of the Professional, plus: <ul style="list-style-type: none">• ArcGIS Pro Advanced• ArcGIS Urban

*What a user is capable of doing with these apps is determined by the user's role.



ArcGIS Enterprise Help: User types, roles, and privileges

User roles

User types allow administrators to control the scope of privileges that can be assigned to members in their organization through roles. Depending on member needs, a default or custom role can be assigned.

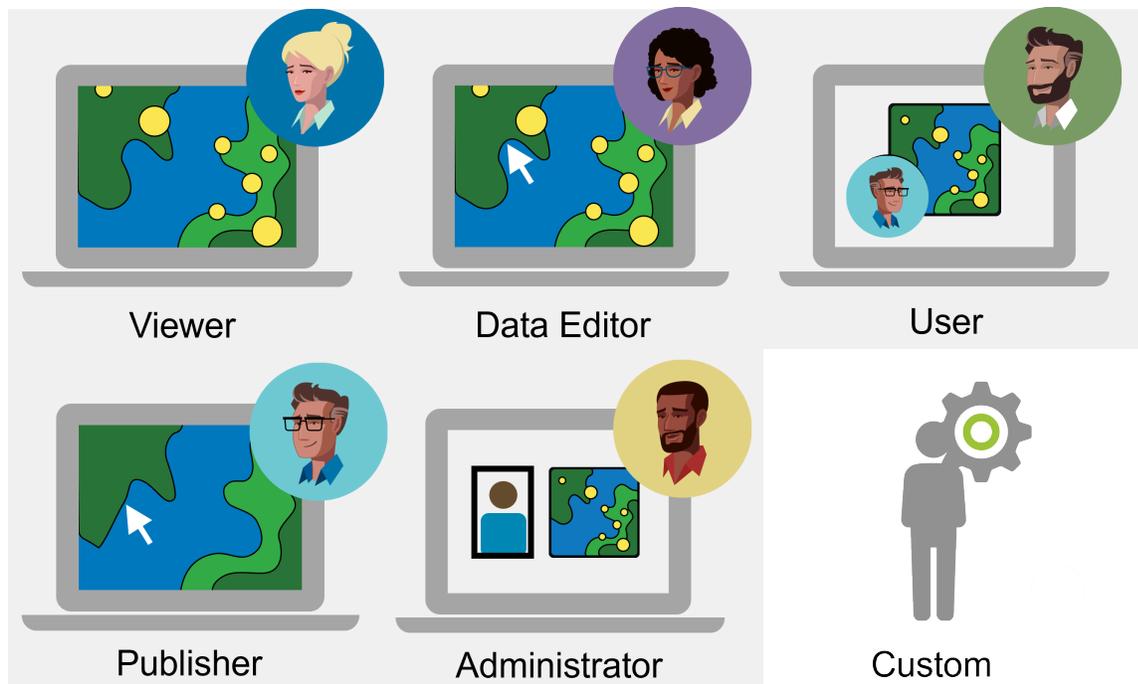


Figure 7.4. There are five built-in user roles: viewer, data editor, user, publisher, and administrator. You can also create a custom role.

Roles

Five default roles can be applied to compatible user types. An organization must have at least one administrator. To minimize security issues, the administrator role should only be assigned to members who require the privileges.

In addition to the five default roles, a custom role can also be applied. Administrator members can create a custom role to apply fine-grained privileges when necessary.

User roles (continued)

Role	Privileges	Compatible user types
Viewer	<ul style="list-style-type: none"> • View items (maps, apps, and so on) • Join groups • Geocoding, geosearch, network analysis 	All user types
Data Editor	<ul style="list-style-type: none"> • Viewer privileges plus: <ul style="list-style-type: none"> • Edit features 	All user types, except Viewer
User	<ul style="list-style-type: none"> • Data Editor privileges plus: <ul style="list-style-type: none"> • Use layers and tools • Create maps and apps • Add items • Share content • Create groups 	Creator, Professional, Professional Plus
Publisher	<ul style="list-style-type: none"> • User privileges plus: <ul style="list-style-type: none"> • Publish hosted feature layers, ArcGIS Server layers • Register data stores and publish data store items • Perform feature and raster analysis 	Creator, Professional, Professional Plus
Administrator*	<ul style="list-style-type: none"> • Publisher privileges plus: <ul style="list-style-type: none"> • Configuration of all portal settings • Manage organization and other users 	Creator, Professional, Professional Plus
Custom	<ul style="list-style-type: none"> • Customized privileges set by an Administrator • Privileges cannot exceed those of the member's user type 	All user types

*The default Administrator role allows the member to configure all the Enterprise portal settings. This privilege cannot be granted through a custom role. While custom roles can include certain administrative-type privileges, the default role is required for Administrators in an Enterprise portal.

User roles (continued)



Some portal workflows require a specific combination of privileges. Refer to the following additional resource for a recommended workflow for configuring a custom role.



ArcGIS Enterprise Help: *Configure roles*

Creating custom roles

An organization's existing roles may not have privileges that are compatible with a member's workflows. By creating a custom role, the organization can set a more fine-grained combination of privileges according to business needs.

Administrator members configure custom roles. The administrator can use an existing role or predefined template to import initial privilege settings, then disable or enable additional privileges as necessary for the organization's needs, as shown in the table below which compares the default and a customized version of the publisher role.

Role Privileges	Default Publisher Role	Custom Publisher Role
View items	✓	✓
Edit features	✓	✗
Create maps and apps	✓	✓
Publish hosted feature layers	✓	✓
Register data stores	✓	✗

Creating custom roles (continued)

(Table continued from previous page)

Role Privileges	Default Publisher Role	Custom Publisher Role
Perform feature and raster analysis		

A default publisher role has several privileges associated with it. If the member requires publisher role privileges but will not be expected to perform editing workflows or register data stores, the administrator might create a custom publisher role that disables those specific privileges.

Choosing an appropriate user type and role

Individual organization members will require different privileges depending on the different ways that they need to access and work with content.

Consider each scenario provided and match it with the required user type and role.

Scenario 1: Creating redundancies

You and another member of your organization are responsible for adding, updating, and managing Enterprise portal members as needed. When one of you is not available, you would like to ensure that the other can manage members and configure the portal's settings. In addition to these responsibilities, the other member uses ArcGIS Pro regularly.

- 1. Which user type and role should you assign to the other member?**
-

Scenario 2: Project with analysis

One of your members is currently a Viewer user type with the default Viewer role. This member is working on a project that requires use of the portal's Map Viewer to perform standard feature analysis. You do not want the member to have the ability to create or edit features.

- 2. How should you set this member's user type and role so they have enough privileges to use an app for standard feature analysis, but are prevented from creating or editing features?**
-

Scenario 3: Limiting privileges

A member with the default Viewer role has requested the ability to edit features.

- 3. How could you configure the member's user type and role to meet these requirements?**
-

Integrating groups from your organization-specific security store

You previously learned how to integrate existing enterprise users with your Enterprise portal. You can also integrate your existing organization-specific groups (for example, groups in your Windows Active Directory security store) to more efficiently manage your Enterprise portal members.

ArcGIS Enterprise can use organization-specific groups in two ways:

1. To add new members to the portal
2. To create a portal group whose members mirror the enterprise users in an organization-specific group

Add members from a Windows group

Rather than add each member one at a time, you can add a set of members at the same time from an existing organization-specific group. In the following diagram, the Enterprise portal member accounts for adPam and adPaul were created because they are active directory users that belong to the existing gisPubs Windows group and were added in a single operation.

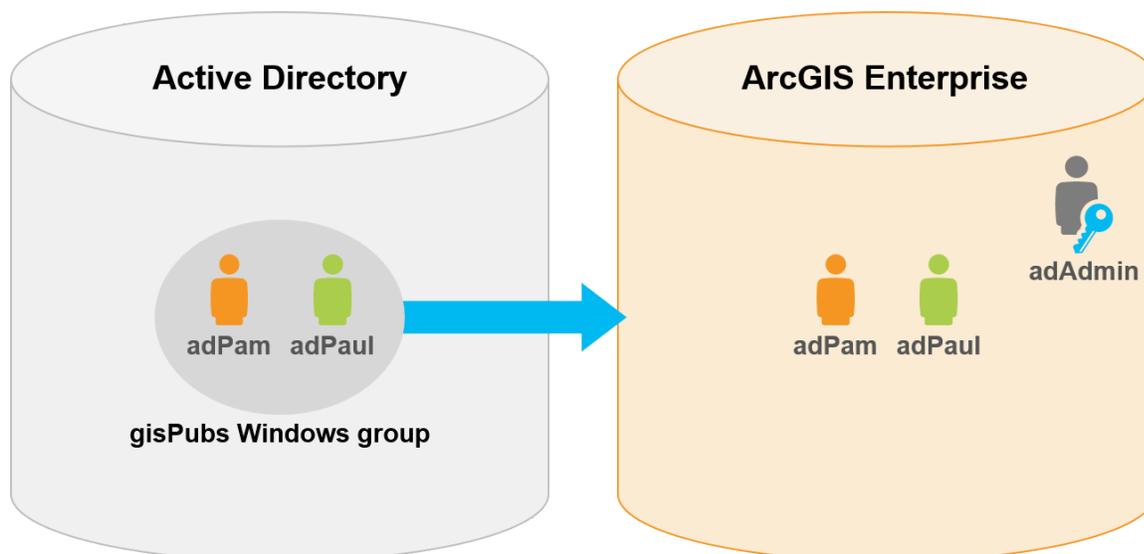


Figure 7.5. Members can be added to your Enterprise portal in bulk from existing organization-specific security store groups.

Integrating groups from your organization-specific security store (continued)

Create an Enterprise portal group from an existing organization-specific group

Another way that you can use your existing organization-specific groups is to create portal groups whose membership is linked to them. For example, if the Enterprise portal group `grpEntProj` is interactively linked to the existing Windows Active Directory (AD) group `gisWinProject`, then the following is true:

- Any members of the Enterprise portal who also belong to the AD `gisWinProject` group are members of the portal group `grpEntProj`. Creation of the linked portal group does not automatically add new members to the portal. The portal group membership can only be populated from existing portal members.
- If an existing AD user belonging to the `gisWinProject` AD group is later added to the Enterprise portal as a member, this member will automatically be added to the `grpEntProj` portal group.

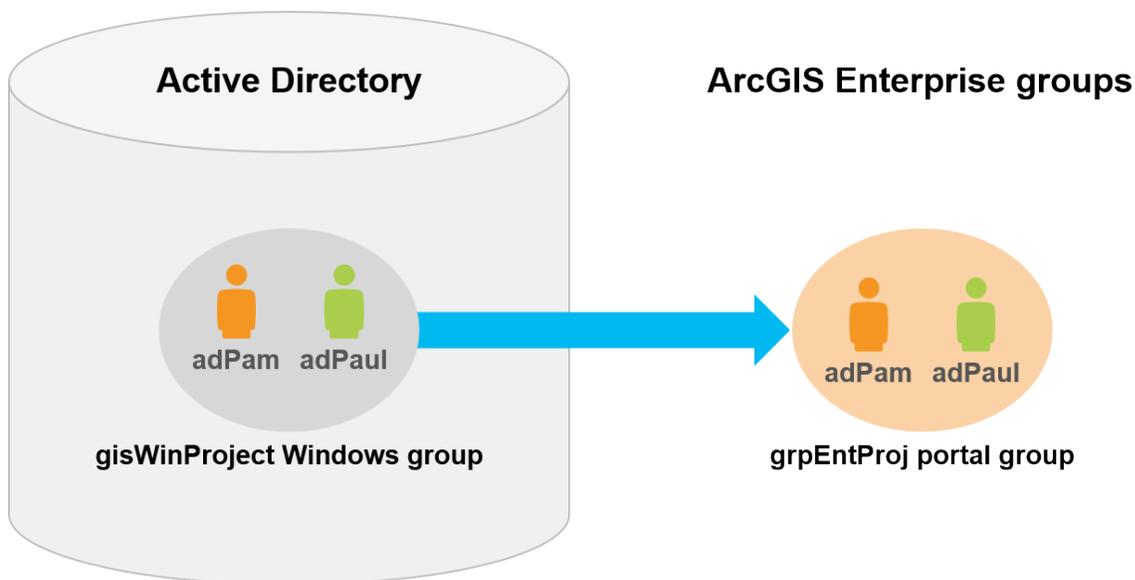


Figure 7.6. You can create Enterprise portal groups from your existing organization-specific security store groups.



By default, the Enterprise portal automatically refreshes your external identity store once every 24 hours (at midnight) or when a new member logs in.

Integrating groups from your organization-specific security store (continued)



ArcGIS Enterprise Help: *Create groups*

ArcGIS Enterprise Help: *Add members to your portal*

Integrate enterprise groups

You have already integrated your organization's user store, allowing you to add your organization's user accounts into the Enterprise portal as members. In this exercise, you will integrate your organization's existing group store. Your existing groups can then be used to add new members and create linked portal groups, which can simplify portal administration.

In this exercise, you will perform the following tasks:

- Configure the portal group store.
- Add enterprise members.
- Add an enterprise group.

Step 1: Configure the portal group store

You will integrate your organization's Windows Active Directory group identity store with your Enterprise portal by updating the portal's group store configuration.

- a Maximize the EBASE VM (blue desktop) application window.
- b Open a web browser and go to the Portal Administrator Directory (<https://ebase.ad.local/portal/portaladmin>).

You are automatically signed in as adadmin.

- c From the Site Root, click Security.
- d Within the Security endpoint, click Config.

Security Configuration

Properties:	<code>{"disableServicesDirectory":false,"enableAutomaticAccountCreati</code>
User store configuration:	<code>{ "type": "WINDOWS", "properties": { "userPassword": "54gbIX", "userFullNameAttribute": "cn", "isPasswordEncrypted": "true" } }</code>
Group store configuration:	<code>{ "type": "BUILTIN", "properties": {"isPasswordEncrypted": "true"</code>

1. What is the current Group Store Configuration type?

- e Within the Config endpoint, click Update Identity Store.

You will update the Group Store Configuration to use your organization's enterprise groups by adding an updated block of JSON code containing your organization's credentials.

- f Open File Explorer and browse to **C:\EsriTraining\EBAS\ManagingUsersGroups**.
- g Double-click the GroupStoreConfig.txt file to open it in Notepad.
- h Select the text in the Step 1 section and copy it to the clipboard.

Hint: Be sure to copy the beginning and ending curly braces ({}) as well.

- i Return to your browser.
- j For Group Store Configuration, select the existing text and paste the the text that you copied.



Be sure to remove the existing text so that only the updated text appears in the text box.

- k Click Update Configuration.

Security Configuration

Properties: {"disableServicesDirectory":false,"enableAutomaticAccountCrea

User store configuration: {"type": "WINDOWS", "properties": { "userPassword": "54gbI
"userEmailAttribute": "mail", "user": "ad\\arccgisad", "userFullna

Group store configuration: {"type": "WINDOWS" "properties": { "userPassword": "54gbI

2. What is the Group Store Configuration type now?

The user account's credentials are now being used to provide access to your organization's Active Directory identity store. In this case, you used the same credentials that you used to install the ArcGIS Enterprise components because the account password is set to not expire.

Now that both your enterprise users and groups have been integrated, you can begin setting up your Enterprise portal groups.

Step 2: Add enterprise members

After modifying your Enterprise portal's group store configuration, you can add two Active Directory users, Pam and Paul, as members to your portal by using an Active Directory group that they belong to.

- a In your browser, click the bookmark for ArcGIS Enterprise (<https://ebase.ad.local/portal/home>).

- b** Click Organization.
- c** Click the Members tab, and then click Add Members.
- d** Select Add Members Based On Existing Active Directory Or LDAP Users and click Next.
- e** Click New Members From An Enterprise Group.
- f** For Enterprise Group, type **gis** and click Search For Group.

The enterprise group to which Pam and Paul belong is named gisPubs.

- g** Click AD\gisPubs, and then click Select Group.
- h** If necessary, for User Type, choose Creator.
- i** For Role, choose Publisher.

Add members from an enterprise group

Enterprise group

AD\gisPubs

User type

Creator
3 available

Role

Publisher

- j** Click Add.

<input type="checkbox"/>	 adPaul adPaul@AD · adPaul@ad.local	Creator	Publisher	
<input type="checkbox"/>	 adPam adPam@AD · adPam@ad.local	Creator	Publisher	

k Click Next, click Next again, and then click Add Members.

<input type="checkbox"/>	 adAdmin adAdmin@AD	Today	Creator	Administrator	▼
<input type="checkbox"/>	 portaladmin built-in portaladmin	Today	Creator	Administrator	▼
<input type="checkbox"/>	 adPam adPam@AD	Never	Creator	Publisher	▼
<input type="checkbox"/>	 adPaul adPaul@AD	Never	Creator	Publisher	▼

Both adPam and adPaul have been added as Creator user types with the Publisher role.

3. How would this functionality facilitate more efficient member management for your portal?

Next, you will test that the adPam member can sign in to your Enterprise portal.

l Close any open application windows.

m Sign out of the EBASE VM.

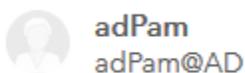
Hint: Windows Search button > click the person icon > click Sign Out

n Double-click the adPam.rdp shortcut.

You are signed in to the EBASE VM as adPam\Esri.4.GIS.

o Open a browser and click the ArcGIS Enterprise bookmark.

You will notice that adPam is automatically signed in to the portal.



p Click Groups.

4. Is Pam a member of any ArcGIS Enterprise groups?

- q Close the browser.
- r Sign out of the EBASE VM.

In this step, you added some ArcGIS Enterprise members by specifying an existing organization-specific group.

Step 3: Add an enterprise group

You have already used your existing AD groups to add members in bulk to the Enterprise portal. In this step, you will use an existing AD group to create a portal group and link them together.

- a Double-click the EBASE.rdp shortcut.
- b Open a browser and click the bookmark for ArcGIS Enterprise (<https://ebase.ad.local/portal/home>).
- c Click Groups.
- d Click Create Group.
- e Under Group Overview, complete the following information:
 - Name: **grpEntProj**
 - Summary: **Project folder**
 - Tags: **Active Directory**

Group overview

Name

grpEntProj

Summary

Project folder

 We will truncate the summary when it is longer than 250 characters.

Tags

Active Directory × Add tags

- f** Under Group Membership, for How Can People Join This Group, select Being A Member Of An Active Directory Group.



You may need to scroll down to see all options.

- g** For Group Name, type **gis**.
- h** From the list of results, select AD\gisWinProject.

Group membership

Who can view this group?

- Only group members
- All organization members
- Everyone (public)

How can people join this group?

- By invitation
- By request
- Being a member of an Active Directory group

Group name

- By adding themselves

i Keep the default settings for the remaining group options.

j Click Save.

Now, adPam can test the new enterprise group.

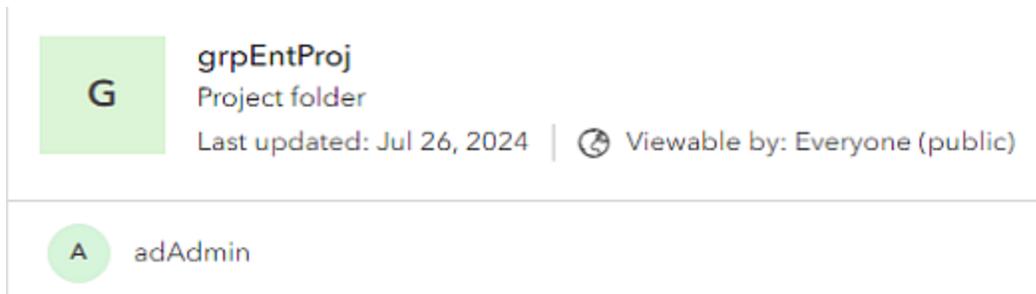
k Close the browser.

l Sign out of the EBASE VM.

m Double-click the adPam.rdp shortcut.

n Open a browser and click the ArcGIS Enterprise bookmark.

o Click the Groups tab.



Although adPam was never explicitly added to grpEntProj, the user is clearly a member of that group and can access it now.



adPaul is also a member of the Windows Active Directory group AD\gisWinProject, so adPaul will also have access to this group.

In this step, you created an ArcGIS Enterprise group with adPam as a member.

Step 4: Share content with an enterprise group

Now that you have created an enterprise group, you will test that Pam can publish content to the new group.

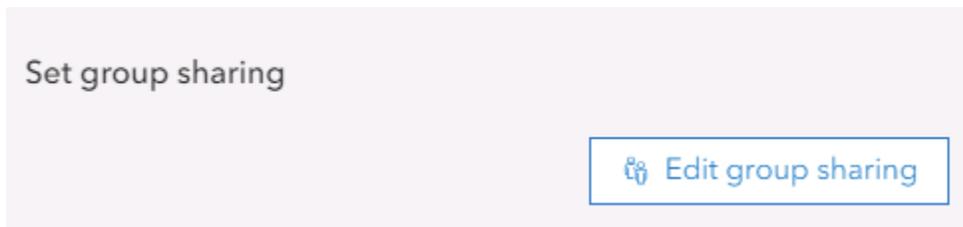
- a At the top of the Enterprise portal page, click Content.
- b Click New Item and choose Your Device.
- c Browse to **C:\EsriTraining\EBAS\ManagingResources** and open Wards.zip.
- d In the New Item window, ensure that File Type is set to Shapefile and the option to create a hosted feature layer is selected.
- e Click Next.
- f Set or confirm the following parameters:
 - Title: **Aurora_CO_Wards_Pam**
 - Folder: adPam@AD
 - Tags: **EBAS**
- g Click Save.

- h Wait for the Creating Service animation on the item page to stop before proceeding.

5. Who is the item shared with currently?

Hint: View the Details section.

- i To the right of the Share header, click Edit.
- j In the Share dialog box, click Edit Group Sharing.



- k Check the box for grpEntProj and click OK.
- l In the Share dialog box, click Save.
- m At the top of the page, click Groups.
- n For the grpEntProj group, click Preview.
- o At the bottom of the Preview pane, click View Details.

Your enterprise group has been successfully configured with your Enterprise portal. Going forward, changes to your AD group will automatically be reflected in the Enterprise portal group for users who are members of the portal.

- p Close all open windows, and then sign adPam out of the EBASE VM.

In this exercise, you created an ArcGIS Enterprise group with adPam as a member.

Workflow review

Your base deployment now has full integration with your existing user and group stores. You have reviewed the portal information model, membership management, and sharing procedures. You are ready to begin exploring primary workflows in ArcGIS Enterprise to suit your organization's needs.

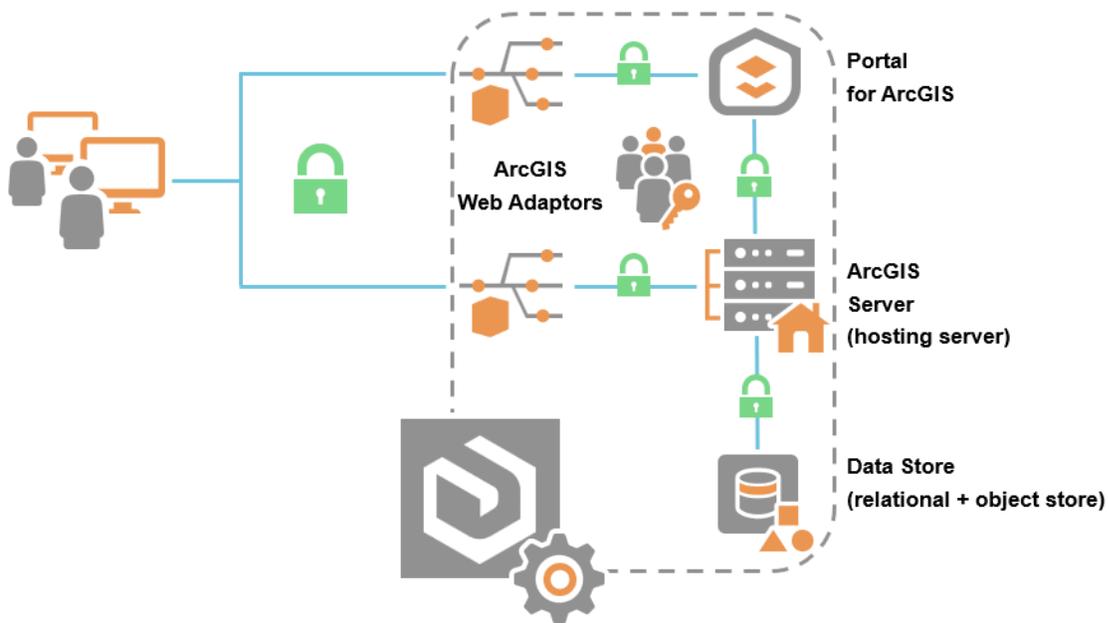


Figure 7.7. The base ArcGIS Enterprise deployment is now fully configured.

1. Who will be using your ArcGIS Enterprise deployment? What user types will you need?

2. Why should you control the scope of privileges for your ArcGIS Enterprise users?

Answers to lesson 7 questions

Choosing an appropriate user type and role (page 7-14)

Scenario 1: Creating redundancies

1. Which user type and role should you assign to the other member?

Creator, Professional or Professional Plus user types, Administrator role

Scenario 2: Project with analysis

2. How should you set this member's user type and role so they have enough privileges to use an app for standard feature analysis, but are prevented from creating or editing features?

Creator user type, custom Publisher role

Scenario 3: Limiting privileges

3. How could you configure the member's user type and role to meet these requirements?

Contributor user type, Data Editor role

Exercise 7: Integrate enterprise groups (page 7-18)

1. What is the current Group Store Configuration type?

BUILTIN

2. What is the Group Store Configuration type now?

WINDOWS

3. How would this functionality facilitate more efficient member management for your portal?

If you already have an existing organization-specific identity store, it saves time because you do not have to add each account separately.

Answers to lesson 7 questions (continued)

4. Is Pam a member of any ArcGIS Enterprise groups?

No. You can confirm this fact by clicking Groups while signed in as adPam.

5. Who is the item shared with currently?

The item is not shared.

Workflow review (page 7-28)

1. Who will be using your ArcGIS Enterprise deployment? What user types will you need?

Answers will vary. Some user types that they could use are viewer, contributor, mobile worker, creator, professional, or professional plus.

2. Why should you control the scope of privileges for your ArcGIS Enterprise users?

Controlling the scope of privileges for your users protects your ArcGIS Enterprise deployments and your content by limiting users to only the privileges that they need for their work.

Appendix A

Data license agreement

ENVIRONMENTAL SYSTEMS RESEARCH INSTITUTE, INC. ("ESRI"), IS WILLING TO LICENSE THE ENCLOSED ELECTRONIC VERSION OF THE TRAINING MATERIALS TO THE STUDENT ("YOU") ONLY UPON THE CONDITION THAT YOU ACCEPT ALL TERMS AND CONDITIONS CONTAINED IN THIS ESRI DATA LICENSE AGREEMENT ("AGREEMENT"). PLEASE READ THE TERMS AND CONDITIONS CAREFULLY. BY CLICKING, "I ACCEPT", YOU ARE INDICATING YOUR ACCEPTANCE OF THE ESRI DATA LICENSE AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS AS STATED, ESRI IS UNWILLING TO LICENSE THE TRAINING MATERIALS TO YOU.

Training Materials Reservation of Ownership. This Agreement gives You certain limited rights to use electronic and tangible versions of the digital or printed content required to complete a course, which may include, but are not limited to, workbooks, data, concepts, exercises, and exams ("Training Materials"). Esri and its licensor(s) retain exclusive rights, title, and ownership to the copy of Training Materials, software, data, and documentation licensed under this Agreement. Training Materials are protected by United States copyright laws and applicable international copyright treaties and/or conventions. All rights not specifically granted in this Agreement are reserved to Esri and its licensor(s).

Grant of License. Esri grants to You a personal, nonexclusive, nontransferable license to use Training Materials for Your own training purposes. You may run and install one (1) copy of Training Materials and reproduce one (1) copy of Training Materials. You may make one (1) additional copy of the original Training Materials for archive purposes only, unless Esri grants in writing the right to make additional copies.

Training Materials are intended solely for the use of the training of the individual who registered and attended a specific training course. You may not (i) separate the component parts of the Training Materials for use on multiple systems or in the cloud, use in conjunction with any other software package, and/or merge and compile into a separate database(s) or documents for other analytical uses; (ii) make any attempt to circumvent the technological measure(s) (e.g., software or hardware key) that effectively controls access to Training Materials; (iii) remove or obscure any copyright, trademark, and/or proprietary rights notices of Esri or its licensor(s); or (iv) use audio and/or video recording equipment during a training course.

Appendix A

Data license agreement (continued)

Term. The license granted by this Agreement will commence upon Your receipt of the Training Materials and continue until such time that (1) You elect to discontinue use of the Training Materials or (2) Esri terminates this Agreement for Your material breach of this Agreement. This Agreement will be terminated automatically without notice if You fail to comply with any provision of this Agreement. Upon termination of this Agreement in either instance, You will return to Esri or destroy all copies of the Training Materials, including any whole or partial copies in any form, and deliver evidence of such destruction to Esri, and which evidence will be in a form acceptable to Esri in its sole discretion. The parties hereby agree that all provisions that operate to protect the rights of Esri and its licensor(s) will remain in force should breach occur.

Limited Warranty. Esri warrants that the media on which Training Materials is provided will be free from defects in materials and workmanship under normal use and service for a period of ninety (90) days from the date of receipt.

Disclaimer of Warranties. EXCEPT FOR THE LIMITED WARRANTY SET FORTH ABOVE, THE TRAINING AND TRAINING MATERIALS CONTAINED THEREIN ARE PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT. ESRI DOES NOT WARRANT THAT THE TRAINING OR TRAINING MATERIALS WILL MEET YOUR NEEDS OR EXPECTATIONS; THAT THE USE OF TRAINING MATERIALS WILL BE UNINTERRUPTED; OR THAT ALL NONCONFORMITIES, DEFECTS, OR ERRORS CAN OR WILL BE CORRECTED. THE TRAINING DATABASE HAS BEEN OBTAINED FROM SOURCES BELIEVED TO BE RELIABLE, BUT ITS ACCURACY AND COMPLETENESS, AND THE OPINIONS BASED THEREON, ARE NOT GUARANTEED. THE TRAINING DATABASE MAY CONTAIN SOME NONCONFORMITIES, DEFECTS, ERRORS, AND/OR OMISSIONS. ESRI AND ITS LICENSOR(S) DO NOT WARRANT THAT THE TRAINING DATABASE WILL MEET YOUR NEEDS OR EXPECTATIONS, THAT THE USE OF THE TRAINING DATABASE WILL BE UNINTERRUPTED, OR THAT ALL NONCONFORMITIES CAN OR WILL BE CORRECTED. ESRI AND ITS LICENSOR(S) ARE NOT INVITING RELIANCE ON THIS TRAINING DATABASE, AND YOU SHOULD ALWAYS VERIFY ACTUAL DATA, SUCH AS MAP, SPATIAL, RASTER, OR TABULAR INFORMATION. THE DATA CONTAINED IN THIS PACKAGE IS SUBJECT TO CHANGE WITHOUT NOTICE. IN ADDITION TO AND WITHOUT LIMITING THE PRECEDING PARAGRAPH, ESRI DOES NOT WARRANT IN ANY WAY TRAINING DATA. TRAINING DATA MAY

Appendix A

Data license agreement (continued)

NOT BE FREE OF NONCONFORMITIES, DEFECTS, ERRORS, OR OMISSIONS; BE AVAILABLE WITHOUT INTERRUPTION; BE CORRECTED IF ERRORS ARE DISCOVERED; OR MEET YOUR NEEDS OR EXPECTATIONS. YOU SHOULD NOT RELY ON ANY TRAINING DATA UNLESS YOU HAVE VERIFIED TRAINING DATA AGAINST ACTUAL DATA FROM DOCUMENTS OF RECORD, FIELD MEASUREMENT, OR OBSERVATION.

Exclusive Remedy. Your exclusive remedy and Esri's entire liability for breach of the limited warranties set forth above will be limited, at Esri's sole discretion, to (i) replacement of any defective Training Materials; (ii) repair, correction, or a workaround for Training Materials; or (iii) return of the fees paid by You for Training Material that do not meet Esri's limited warranty, provided that You uninstall, remove, and destroy all copies of the Training Materials and execute and deliver evidence of such actions to Esri.

IN NO EVENT WILL ESRI BE LIABLE TO YOU FOR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR TRAINING; LOST PROFITS; LOST SALES; BUSINESS EXPENDITURES; INVESTMENTS; BUSINESS COMMITMENTS; LOSS OF ANY GOODWILL; OR ANY INDIRECT, SPECIAL, EXEMPLARY, CONSEQUENTIAL, OR INCIDENTAL DAMAGES ARISING OUT OF OR RELATED TO THIS AGREEMENT, HOWEVER CAUSED OR UNDER ANY THEORY OF LIABILITY, EVEN IF ESRI HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ESRI'S TOTAL CUMULATIVE LIABILITY HEREUNDER, FROM ALL CAUSES OF ACTION OF ANY KIND, WILL IN NO EVENT EXCEED THE AMOUNT ACTUALLY PAID BY YOU FOR THE PORTION OF THE TRAINING UNDER THIS AGREEMENT. THESE LIMITATIONS WILL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY.

Export Regulation. You must comply with all applicable laws and regulations of the United States including, without limitation, its export control laws. You expressly acknowledge and agree not to export, reexport, transfer, or release Esri-provided Training Materials, in whole or in part, to (i) any US embargoed country (including to a resident of any US embargoed country); (ii) any person or entity on the US Treasury Department Specially Designated Nationals List; (iii) any person or entity on the US Commerce Department Lists of Parties of Concern; or (iv) any person or entity where such export, reexport, or provision violates any US export control laws or regulations including, but not limited to, the terms of any export license or licensing provision and any amendments and supplemental additions to US export laws.

Appendix A

Data license agreement (continued)

Governing Law. This Agreement is governed by and construed in accordance with the laws of the state in which training is being held or, in the case of training provided over the Internet, the laws of the State of California, without reference to its conflict of laws principles.

Appendix B

Answers to lesson review questions

Answers to lesson 1 review questions

1. Which components make up a base ArcGIS Enterprise deployment?
 - **ArcGIS Web Adaptor**
 - **Portal for ArcGIS**
 - **ArcGIS Server**
 - **Data store**

2. Which ArcGIS Enterprise automation tool always installs all the components on one machine?
 - a. **ArcGIS Enterprise Builder**

3. What are the two primary steps to implement each component of a base deployment?
Software installation/licensing and component configuration

Appendix C

Additional resources

Lesson 1	Resources
What is ArcGIS Enterprise?	<ul style="list-style-type: none">• Esri GIS Products Site: <i>ArcGIS Enterprise Features</i>
What can ArcGIS Enterprise do?	<ul style="list-style-type: none">• ArcGIS Enterprise Help: <i>ArcGIS GIS Server capabilities and extensions</i>
How do you automate a base deployment?	<ul style="list-style-type: none">• YouTube video: <u>Esri UC 2017: ArcGIS Enterprise–Improving Installation and Configuration</u>

Lesson 2	Resources
Identify component communication	<ul style="list-style-type: none">• ArcGIS Enterprise Help: <i>Ports used by Portal for ArcGIS</i>• ArcGIS Enterprise Help: <i>Ports used by ArcGIS Server</i>• ArcGIS Enterprise Help: <i>Ports used by ArcGIS Data Store</i>
Using certificates to enable HTTPS encryption	<ul style="list-style-type: none">• ArcGIS Enterprise Help: <i>Enable HTTPS on your web server - Portal for ArcGIS</i>• ArcGIS Enterprise Help: <i>Restrict TLS protocols and cipher suites</i>

Appendix C

Additional resources (continued)

Lesson 3	Resources
Portal for ArcGIS installation overview	<ul style="list-style-type: none">• ArcGIS Enterprise Help: <i>Portal for ArcGIS system requirements</i>• ArcGIS Enterprise Help: <i>Steps to get Portal for ArcGIS up and running</i>• ArcGIS Enterprise Help: <i>Changing the portal content directory</i>
Portal for ArcGIS account	<ul style="list-style-type: none">• ArcGIS Enterprise Help: <i>Changing the Portal for ArcGIS account</i>
ArcGIS Web Adaptor	<ul style="list-style-type: none">• ArcGIS Enterprise Help: <i>Install ArcGIS Web Adaptor</i>• ArcGIS Enterprise Help: <i>Import a certificate into the portal</i>

Lesson 4	Resources
ArcGIS Server installation overview	<ul style="list-style-type: none">• ArcGIS Enterprise Help: <i>ArcGIS Server system requirements</i>• ArcGIS Enterprise Help: <i>Steps to get ArcGIS Server up and running</i>
Explore the ArcGIS Server installation	<ul style="list-style-type: none">• ArcGIS Enterprise Help: <i>The ArcGIS Server account</i>

Appendix C

Additional resources (continued)

Lesson 4	Resources
ArcGIS Server directories and configuration store	<ul style="list-style-type: none">• ArcGIS Enterprise Help: <i>Server directories</i>• ArcGIS Enterprise Help: <i>Specify the configuration store location</i>
Federation	<ul style="list-style-type: none">• ArcGIS Enterprise Help: <i>Federate an ArcGIS Server site with your portal</i>• ArcGIS Enterprise Help: <i>The ArcGIS Enterprise security model</i>

Lesson 5	Resources
ArcGIS Data Store	<ul style="list-style-type: none">• ArcGIS Enterprise Help: <i>Introduction to ArcGIS Data Store</i>• ArcGIS Enterprise Help: <i>ArcGIS Data Store Vocabulary - Spatiotemporal big data store</i>• ArcGIS Enterprise Help: <i>ArcGIS Data Store Vocabulary - Graph store</i>
Setting up ArcGIS Data Store	<ul style="list-style-type: none">• ArcGIS Enterprise Help: <i>Tasks to perform after you create a data store</i>• ArcGIS Enterprise Help: <i>Add a machine to your data store</i>• ArcGIS Enterprise Help: <i>ArcGIS Data Store command utility reference</i>

Appendix C

Additional resources (continued)

Lesson 5	Resources
Set up ArcGIS Data Store	<ul style="list-style-type: none">• ArcGIS Enterprise Help: <i>An overview of ArcGIS Data Store configuration</i>• ArcGIS Enterprise Help: <i>Replace ArcGIS Data Store SSL certificate</i>
Defining web layers	<ul style="list-style-type: none">• ArcGIS Enterprise Help: <i>Relationships between web services and portal items</i>
Data registration	<ul style="list-style-type: none">• ArcGIS Enterprise Help: <i>Register your data with ArcGIS Server using Server Manager</i>• ArcGIS Enterprise Help: <i>Make your data accessible to ArcGIS Server</i>

Lesson 6	Resources
Understanding identity stores	<ul style="list-style-type: none">• ArcGIS Enterprise Help:• <i>Configuring a SAML-compliant identity provider with your portal</i>• <i>Configure OpenID Connect logins</i>

Appendix C

Additional resources (continued)

Lesson 6	Resources
Configuring portal authentication	<ul style="list-style-type: none">• <i>ArcGIS Enterprise Help: About configuring portal authentication</i>• <i>ArcGIS Enterprise Help: Disabling anonymous access</i>
Setting up an enterprise identity store	<ul style="list-style-type: none">• <i>ArcGIS Enterprise Help: Use Integrated Windows Authentication with your portal</i>• <i>ArcGIS for Developers Help: Update Identity Store</i>
Security best practices	<ul style="list-style-type: none">• <i>ArcGIS Enterprise Help: Best practices for configuring a secure environment</i>• <i>ArcGIS Trust Center: ArcGIS–Secure and Trustworthy</i>
ArcGIS Enterprise security options	<ul style="list-style-type: none">• <i>ArcGIS Enterprise Help: Best practices for configuring a secure environment</i>• <i>ArcGIS Enterprise Help: Security best practices</i>
Evaluate security for a base deployment	<ul style="list-style-type: none">• <i>ArcGIS Enterprise Help: Scan your portal for security best practices</i>• <i>ArcGIS Enterprise Help: Scan ArcGIS Server for security best practices</i>

Appendix C

Additional resources (continued)

Lesson 7	Resources
Levels of sharing	<ul style="list-style-type: none"><li data-bbox="592 449 1118 483">• ArcGIS Enterprise Help: <i>Share items</i>
User types	<ul style="list-style-type: none"><li data-bbox="592 617 1398 651">• ArcGIS Enterprise Help: <i>User types, roles, and privileges</i>
User roles	<ul style="list-style-type: none"><li data-bbox="592 785 1170 819">• ArcGIS Enterprise Help: <i>Configure roles</i>
Integrating groups from your organization-specific security store	<ul style="list-style-type: none"><li data-bbox="592 953 1154 987">• ArcGIS Enterprise Help: <i>Create groups</i><li data-bbox="592 1008 1349 1041">• ArcGIS Enterprise Help: <i>Add members to your portal</i>

Contact Esri Training Services

T 909 793 2853 x1585

F 909 793 5953

esri.com/training

380 New York Street

Redlands, California 92373-8100 USA



esri[®]

THE
SCIENCE
OF
WHERE[®]