How GIS server security works

ArcGIS Server systems allow for two different types of connections: Local and Internet. The way you implement security differs for local and Internet connections. Security for *local* connections is handled by the operating system, which uses the agsusers and agsadmin groups to determine who can connect to and administer the server. Security for Internet connections is administered through the Web server, which can make use of operating system security as well.

Security for local connections

Local connections to a GIS server—and the services running on it—are managed by the operating system of the server object manager (SOM) machine. In much the same way the operating system allows you to create and delete files on your own computer, yet prevents you from doing so on your colleague's computer, the operating system on the SOM grants some users access to the services running on the server machines, while denying access to others. When you log in to your computer, the username and password you specify identifies you as a valid user on your network. Based on your operating system account, you are allowed to perform a certain set of actions—one of which might be to access a GIS server.

Before you can begin to use your GIS server, you need to establish who can access it. Once you've done that, you'll be able to connect to your GIS server and add services to it.

Identifying who can access the server

To whom should you grant access to your GIS server? The answer to this question will depend on what kind of services you run on your server and how you plan to use them. In some cases, the services you place on your server should be made available to everyone. In other cases, you might want to restrict access because a service contains sensitive information that only certain individuals should see.

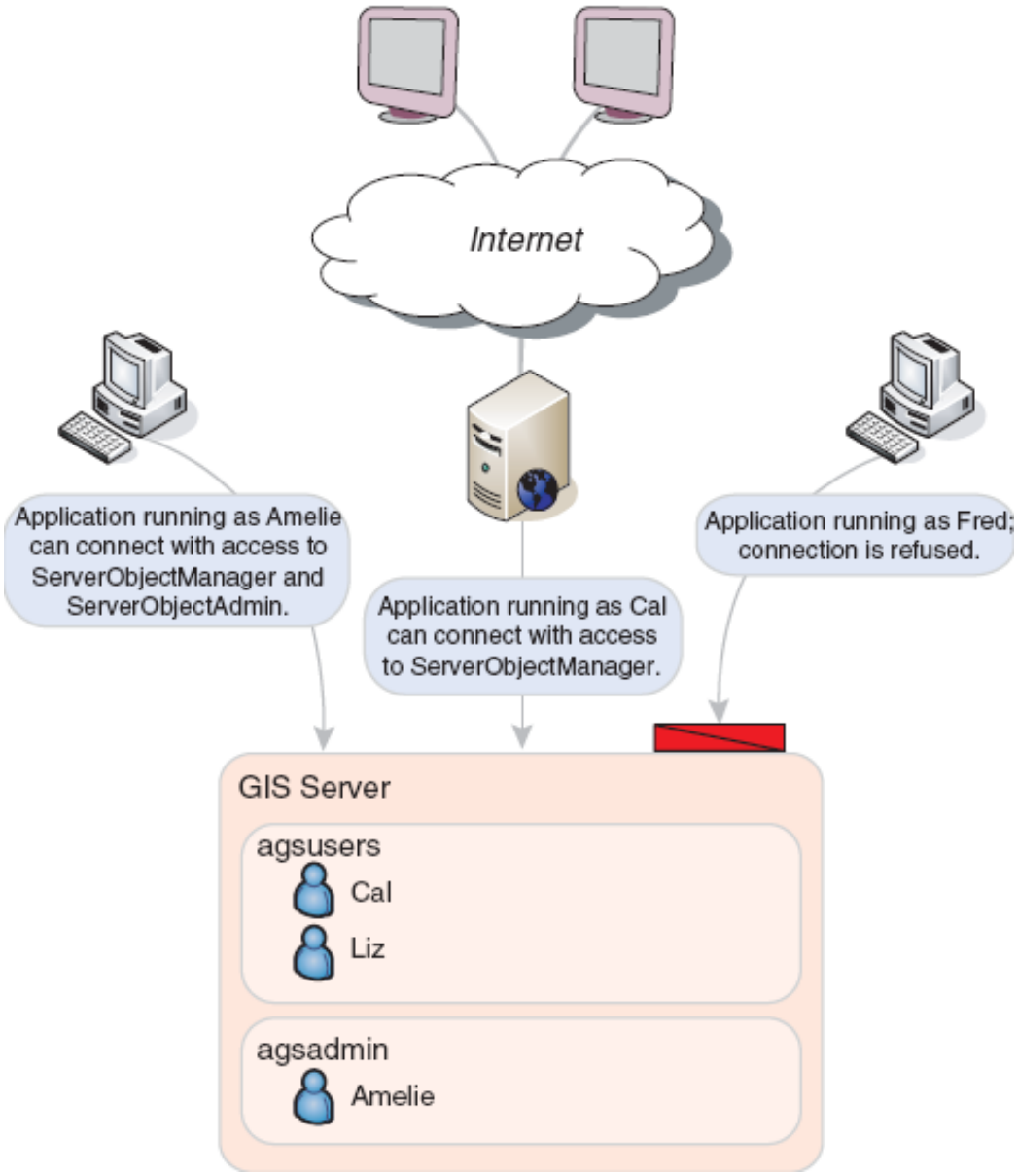
As the administrator of the GIS server, you allow people to access the GIS server by adding their operating system account to the list of users who should have access to the server. In reality, there are actually two lists: a list of users who can use the services running on the server and a list of users who can administer the server itself (that is, add, delete, and modify server services). Because it is the operating system that ultimately controls access to the server, you use two operating system user groups—ArcGIS Server users and ArcGIS Server administrators—to manage the two lists of users. A user group simply defines the set of users who have access to a particular resource, in this case, a GIS server.

In general, the list of accounts you add to the ArcGIS Server users and administrators groups will depend on what clients you anticipate will connect to the server. Each operating system account from which ArcGIS Desktop is run will need to be added to the ArcGIS Server users group if you want that client to access the GIS server. Additionally, each Web application you create can connect to the GIS server through a particular operating system account. Each account your Web applications utilize should be added to the ArcGIS Server users group as well.

You do not need to add the SOM and SOC Accounts to the administrators or users groups. These accounts are only used by the operating system to start and stop processes on the GIS server.

Controlling access to a GIS server

When you install ArcGIS Server, the install program automatically creates the ArcGIS Server users and administrators groups for you. Specifically, the users group is named **agsusers** and the administrators group is named **agsadmin**. These groups are created as local operating system groups on the SOM machine and on each container machine. The ArcGIS Server install program doesn't automatically add any users to these groups for you. Thus, you will need to add users to these groups, depending on the type of access each user should have. Of course, the first account you'll need to add to the administrators group is your own.



When applications make local connections to the GIS server, they are authenticated against the agsusers and agsadmin users groups on the GIS server.

How you choose to add user accounts to these groups depends on how your organization manages users in general. If your organization has a number of user groups already established, you may choose to add particular groups as members of the ArcGIS Server users or administrators groups. By allocating users based on other groups, you can minimize the amount of work you need to do to change access to your GIS server. For example, if a new employee is hired and is added to one of your organization's existing groups, access to your GIS server will automatically be granted because the employee is a member of a group that is a member of the ArcGIS Server users group. Alternatively, you can add individual users to the ArcGIS Server users or administrators groups.

Privileges of users and administrators

Members of the ArcGIS Server users group (agsusers) have consumer-level privileges on the GIS server. Consumers may view and access services; however, they may not perform administrative tasks, such as add, remove, or modify preconfigured services. They also may not modify properties of the server itself, such as adding and removing machines.

Members of the ArcGIS Server administrators group (agsadmin) are granted access and administrator privileges on the GIS server. Connecting as a member of the administrator group allows you to:

- Add or remove container machines
- Add, remove, or modify server directories
- Add, delete, or modify services

- Start, stop, or pause services
- View statistical information

Making a local connection to the server from the ArcGIS Desktop

A desktop client application to ArcGIS Server will run as the user account that started the application. For example, if you are logged into a desktop computer as the domain user ANDY on the domain AVWORLD, and you are running an application such as ArcCatalog, the identity of the application is AVWORLD\ANDY. When you make an ArcGIS Server local connection in that ArcCatalog session, you are connecting as AVWORLD\ANDY. As long as AVWORLD\ANDY is a member of the users group (agsusers) on the SOM, you will be able to connect. If AVWORLD\ANDY is a member of the administrators group (agsadmin), you will have administrator privileges on the server through that connection.

In Windows, you can use the runas command to connect to ArcCatalog with an operating system account other than your current login. See Running ArcCatalog under a different operating system account for more instructions.

Making a local connection to the server from a Web application

When you are using the Web ADF to build Web applications that access local services, you will need to specify an *identity* . The account that you use for the identity must belong to the agsadmin or agsusers group on each local server to which your application will connect. When end users access the application, they will not have to enter a name and password to access the service. Instead, the identity will be used. The encrypted identity information is stored in the application's Web.Config file.

Restricting access to specific services

Restricting access to some services, but not others on the same GIS server is only available through Internet connections. See Securing a service to learn how to implement this.

Security for Internet connections

When you make an Internet connection to an ArcGIS Server, your request first encounters a Web server before it reaches the SOM. It is at the Web server level that ArcGIS Server Internet connections are secured. When you install ArcGIS Server, a directory called "ArcGIS\services" is installed the virtual root directory of your Web server (the name will vary if you chose a different instance name). When you make an Internet connection to a GIS server, you'll notice that the name of this directory determines the URL (for example, http://myServer/ArcGIS/services). You can use Internet Information Services (IIS) to determine who will be able to access the services exposed at this URL.

By default, anonymous access is enabled for the services directory. Anonymous access means that anyone on the Internet can access the URL. If you want users to have to enter a username and password when they make an Internet connection to your server, you need to disable anonymous access for the services directory.

Even when you disable anonymous access, ArcGIS Server Internet connections do not use the agsusers and agsadmin groups to determine who can access the server. Instead, security is based on the authentication method that you have chosen in IIS. This can be either Digest, Basic, or Integrated Windows authentication. The article IIS Authentication from the Microsoft Developer Network provides more detail on anonymous access and the available authentication methods in IIS.

To limit access to certain services, you should do the following:

- Organize your services in folders.
- Organize your users into operating system groups.
- Use the web.config file in the services directory mentioned above to specify which groups will have access to which folders.

To learn how to disable anonymous access and limit access via the web.config file, see Limiting which users can access a service from the topic Securing a Service.

Making an Internet connection to the server from a Web application

When building applications with the Web ADF, you have the option to specify a user name and password for ArcGIS Server Internet services. Your Web application will use this information to access Internet services on the GIS server. You only need to specify a user name and password if your ArcGIS Server administrator has disabled anonymous access to Internet services. The administrator should have granted the user name appropriate access to the GIS server's folders as specified in the section Limiting which users can access a service from the topic Securing a Service.

End users of your application will not have to type a user name and password to access the Internet service. Instead, the Web application uses the name and password that you specified when you built the application. This information is encrypted within the Web application.