# ArcGIS℠ Online

## Security Overview

ArcGIS℠ Online is a secure, reliable geographic information system (GIS) delivered using the software-as-a-service (SaaS) model. ArcGIS Online services are elastic, available on demand, managed by Esri, and accessed by clients running on a wide range of platforms. They can be shared and utilized by many customers and offer security benefits.

### Built Using Secure Design Principles

Esri's security strategy is based on an industry-standard, defense-in-depth approach that provides security controls at every level, for every user, including the application, network, and facilities. Adherence to these security principles helps ensure that ArcGIS Online provides confidentiality, integrity, and availability of data.

### Certifications and Standards

**Privacy—**The ArcGIS Online Privacy Statement is certified compliant with the highest independent, international, industry-accepted privacy standards, including TRUSTe Certified Privacy Seal and EU Safe Harbor (US Department of Commerce).

**Infrastructure—**ArcGIS Online utilizes cloud infrastructure providers that are ISO 27001, FedRAMP, and SSAE 16 SOC1 Type2 compliant.

**Application—**ArcGIS Online has received Federal Information Security Management Act (FISMA) Low Authorization and Accreditation from the U.S. Department of Agriculture.

**Authentication—**Enterprise logins are supported via SAML 2.0 providing federated identity management. Developers can utilize OAuth 2-based APIs to manage user and app logins.

### Secure Operations

- Background investigations are performed against all employees.
- Access to customer database information is limited to select operation team members.
- Operations/Availability transparency web pages can be seen at **trust.arcgis.com**.

### You Retain Ownership

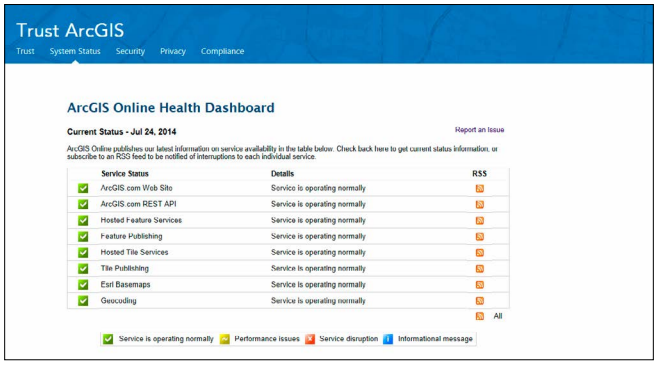
**Ownership—**Customers retain intellectual property rights for data they publish through Esri cloud offerings. Esri and third-party data can be incorporated into web applications using ArcGIS Online, Esri Business Analyst Online℠, and others.

**Multitenancy—**Each data record within multitenant storage is stamped with the ID of the owning subscription to ensure organization data is accessible only by the organization's users.

**Features—**Each organization has its own logically separate database, providing isolation of stored features.

**Extract—**Data publishers can extract and download data to their organization via shapefiles or CSVs. Also, the original publication package can be downloaded to an organization.

**Deletion—**The data owner controls when and what to delete, whether it's removal of features or the publication package. Deleted information is not left in a recycle bin; once the owner deletes it, it's gone.




Get comprehensive information on security, privacy, and compliance at trust.arcgis.com

## Configurable Security

Features engineered by Esri as part of the core ArcGIS platform include:

**Roles—**ArcGIS Online organization roles include User, Publisher, Administrator, and Custom.

- Users can add items, create web maps, share content, and participate in groups.
- Publishers are users that can publish hosted services from feature or tiled map data.
- Administrators utilize a web-based administration interface to manage users, groups, permissions, and organization-wide security features:
  - Easily configure Transport Layer Security (LTS) to enforce confidentiality of all information as it crosses the Internet.
  - Restrict anonymous access to organization data.
- Custom roles add flexibility in assigning privileges to members of an organization that fit the organization's dynamics, workflows, and needs.

**Sharing—**User-added content is only accessible by users and groups that users explicitly share the content with. By default, items are private and only accessible by the user adding content.

**Server—**Secured ArcGIS® 10 Server Service Pack 1 (SP1) and later services can be incorporated into maps.

**Development—**ArcGIS Online utilizes software development coding best practice techniques: the use of static code analysis software, testing/code review, and more.

**Audit—**Data modifications and administrative actions are stored in audit logs.

## Encrypted Communication

- User identity is established through a login process that always takes place over HTTPS to ensure industry-standard encryption of sensitive information.
- Subsequent access requires authentication tokens over HTTP or HTTPS, chosen by the administrator.

## On-Premises Advanced Security Option

Some organizations require segmentation of their solution from the Internet or do not allow distributed multitenant environments such as ArcGIS Online. The on-premises Portal for ArcGIS meets this requirement of high security needs by running inside corporate firewall environments.

## Summary

Moving geospatial services to the cloud requires serious consideration of security issues and technology. Cloud computing is indeed complex; however, by utilizing a secure backbone of both industry-leading cloud providers and geospatial services, ArcGIS Online is able to provide the security organizations need.

For more detail on a specific area, contact the Security Standards and Architecture team at SecureSoftware@esri.com.

For more information on ArcGIS Online security and privacy information, visit **trust.arcgis.com**.

esri
THE SCIENCE OF WHERE™



G92578