

Security statement: eSpatial OnDemand GIS™

This document provides information on the security and reliability of eSpatial OnDemand GIS, including the cloud deployment environment, data storage and additional measures.

Cloud deployment environment: Amazon EC2

eSpatial OnDemand GIS is deployed on Amazon Elastic Cloud Computing (EC2) / Amazon Web Services (AWS) environment. This cloud computing platform has high availability and reliability, and is used by a wide range of organisations. In addition, eSpatial have taken various measures to further improve security and reliability of the service we deliver from this environment.

ISO 27001 certification

ISO 27001/27002 is a widely-adopted global security standard set by the International Organization for Standards (ISO). Achieving ISO 27001 certification requires the company to demonstrate a systematic and ongoing approach to managing information security risks that affect the confidentiality, integrity, and availability of company and customer information.

AWS has achieved ISO 27001 certification of its Information Security Management System (ISMS) covering infrastructure, data centres, and services including Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Simple Storage Service (Amazon S3). AWS' ISO 27001 certification includes all its data centres in all in-scope regions worldwide. AWS has established a formal program to maintain the certification.

SAS70

SAS70 certifies that a service organisation has had an in-depth audit of its controls (including control objectives and control activities). In the case of AWS, the audit relates to operational performance and security to safeguard customer data. AWS holds a Statement on Auditing Standards No. 70 (SAS70) Type II Audit, and has obtained a favorable unbiased opinion from its independent auditors. AWS has established a formal program to maintain the certification.

Federal Information Security Management Act (FISMA)

FISMA is a United States federal law that assigns specific responsibilities to bodies in the US to strengthen information system security. Information systems that achieve compliance with FISMA may be used by US government agencies.

AWS has been awarded an approval to operate at the FISMA-Low level. It has also completed the control implementation and successfully passed the independent security testing and evaluation required to operate at the FISMA-Moderate level. AWS is currently pursuing an approval to operate at the FISMA-Moderate level from government agencies.

eSpatial Inc.

2325 Dulles Corner Boulevard, Suite 500, Herndon, VA, USA – 20171
Ph: +1 877 365 1456

eSpatial Solutions EMEA

Block A1, East Point Business Park, Fairview, Dublin 3, Ireland.
Ph: +353 1 870 8800 | Fax: +353 1 870 8899 | UK: +44 (0) 800 169 0451

Restricted access to data centres

Physical access to AWS data centres is strictly controlled both at the perimeter and at building ingress points by professional security staff utilising video surveillance, intrusion detection systems, and other electronic means. Authorised staff must pass two-factor authentication a minimum of two times to access datacentre floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorised staff.

Amazon only provides data centre access and information to employees who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or AWS. All physical and electronic access to data centres by Amazon employees is logged and audited routinely.

Amazon Machine Instances (AMIs)

Different instances running on the same physical machine are isolated from each other utilising the Xen hypervisor.

Firewalls

Amazon EC2 provides a complete firewall solution. The mandatory inbound firewall is configured in a “default deny” mode, requiring the Amazon EC2 customer to explicitly open any ports to allow inbound traffic. The traffic may be restricted by protocol, by service port, as well as by source IP address (individual IP or CIDR block).

Amazon have implemented specific measures against the following threats:

- Distributed Denial Of Service (DDoS) attacks.
- Man In the Middle (MITM) attacks.
- IP spoofing.
- Port scanning.
- Packet sniffing by other tenants.

At eSpatial, we disable password-based access to the Amazon hosts that we use, and utilise cryptographically strong key-based authentication to control access to these.

We utilise Amazon Secret Access Keys to control access to the Amazon APIs and API calls are encrypted in transit using SSL-protected API endpoints. At eSpatial, we also enforce strict management of Amazon security groups.

For further details on security in the Amazon cloud environment, please visit:

<http://aws.amazon.com/security>

eSpatial OnDemand GIS data storage

eSpatial OnDemand GIS uses the tried-and-trusted, enterprise grade Oracle database management software.

The eSpatial OnDemand GIS database is stored on Amazon Elastic Block Storage (EBS) – a more robust data store facility than that in Amazon Machine Instances (AMIs). Standard enterprise-grade Oracle database management system mechanisms are used for continuous database log archiving and for regular database backups.

Database archives and backups are made to Amazon Simple Storage Services (S3). Data stored in Amazon S3 or Amazon EBS is redundantly stored in multiple physical locations. Amazon S3 provides object durability by storing objects multiple times across multiple Availability Zones on the initial write and then actively performing further replication in the event of device unavailability or detected bit-rot.

The AWS disk virtualisation layer automatically wipes every block of storage used by the customer, and guarantees that one customer's data is never exposed to another.

eSpatial OnDemand GIS keeps the database tablespaces, log archives and backups all in separate storage volumes.

eSpatial OnDemand GIS assures high availability through a standby database for additional protection of data, which utilises separate volumes to the main database.

Additional measures taken by eSpatial

In addition to utilising best-of-breed, enterprise-grade technology and suppliers, we have taken additional measures to further improve the security and reliability of the service we deliver from this environment.

eSpatial OnDemand GIS:

- Employs a multi-tenant isolation mechanism to keep customer organisations' data separate from each other.
- Authenticates users and enforces role-based access restriction to data and functions.
- Doesn't allow users to directly access the database. Furthermore, application-user credentials cannot be used as database access credentials.
- Uses standard mechanisms to authenticate users (HTTP authorisation).

eSpatial Inc.

2325 Dulles Corner Boulevard, Suite 500, Herndon, VA, USA – 20171
Ph: +1 877 365 1456

eSpatial Solutions EMEA

Block A1, East Point Business Park, Fairview, Dublin 3, Ireland.
Ph: +353 1 870 8800 | Fax: +353 1 870 8899 | UK: +44 (0) 800 169 0451

- Follows enterprise best practice of using an LDAP Directory Server to manage a secure directory of users, passwords, roles and permissions.
- Stores all passwords in an encrypted format.
- Enforces role-based access restriction to data sets (map layers), user objects (maps, queries, reports, print layouts, etc.) and functions (and associated screens and screen components).
- Provides administrators within each customer organisation with a web-based user administration interface to manage users and user groups, and to control access entitlements and permissions.
- Maintains an audit log of all data edits.

The architecture of eSpatial OnDemand GIS, combined with the multi-location backup strategy, is designed to deliver enhanced levels of reliability and security. For example, while issues were reported with Amazon EC2 in April 2011, eSpatial OnDemand GIS did not experience any loss of availability.

We engage respected third party security consultants to audit the security of eSpatial OnDemand GIS, and conduct penetration tests.

eSpatial Inc.

2325 Dulles Corner Boulevard, Suite 500, Herndon, VA, USA – 20171
Ph: +1 877 365 1456

eSpatial Solutions EMEA

Block A1, East Point Business Park, Fairview, Dublin 3, Ireland.
Ph: +353 1 870 8800 | Fax: +353 1 870 8899 | UK: +44 (0) 800 169 0451

About eSpatial OnDemand GIS™

eSpatial OnDemand GIS combines the latest innovations in software delivery and usability with the traditional performance of in-house GIS, over the web.

eSpatial OnDemand GIS is an affordable, predictable, and scalable web GIS offering which provides an ideal enterprise grade hosted services delivery platform for geospatial applications.



About eSpatial

eSpatial is a leading provider of Geographic Information Systems (GIS), and a pioneer in the provision of location intelligence delivered via Software-as-a-Service (SaaS).

Our flagship product, eSpatial OnDemand GIS, is the world's first full-function available via SaaS delivery. It combines the latest innovations in software delivery and usability with the traditional performance of in-house GIS, over the web.

We are proud to work with leading technology partners such as Oracle, NAVTEQ and Digital Globe; and to count many leading organisations amongst our global customer base.

eSpatial is headquartered in Dublin, Ireland.

Email: info@espatial.com

Website: www.espatial.com

eSpatial Inc.

2325 Dulles Corner Boulevard, Suite 500, Herndon, VA, USA – 20171
Ph: +1 877 365 1456

eSpatial Solutions EMEA

Block A1, East Point Business Park, Fairview, Dublin 3, Ireland.
Ph: +353 1 870 8800 | Fax: +353 1 870 8899 | UK: +44 (0) 800 169 0451