Product Overview

CubeWerx Guardian – Advanced Security for OGC APIs

Authentication, security, and access control for geo-data providers

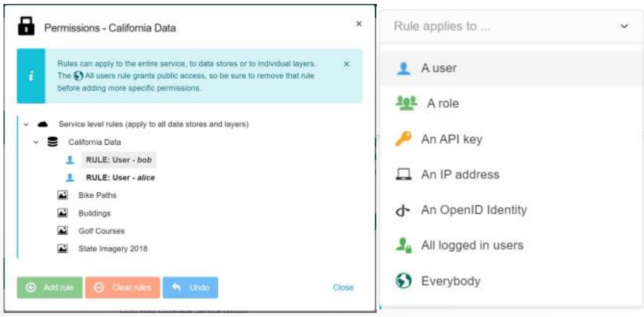
Protecting your investment

As a data provider, securing your geospatial Web services presents distinct challenges, largely unaddressed by current industry standards. Unlike typical web content, spatial data security demands control over access based on factors like location, image resolution, and scale. Traditional access control technologies often fall short in managing these specialized criteria due to the complexity and variety of spatial data requests, which encompass intricate geographic details. Consequently, effective access control solutions for these services must possess a deep understanding of geospatial elements, matching the complexity of the services they safeguard.

CubeWerx Guardian, a component of the Stratos geospatial platform, addresses these challenges.

Role-based access

Stratos Guardian works by assigning a set of rules that apply to all access through a web service's endpoints. A rule groups an identity, a piece of data content and a set of access rights. Every request made through the service APIs is compared to the set of all rules before access is granted. Multiple options are available to identify and authenticate users.

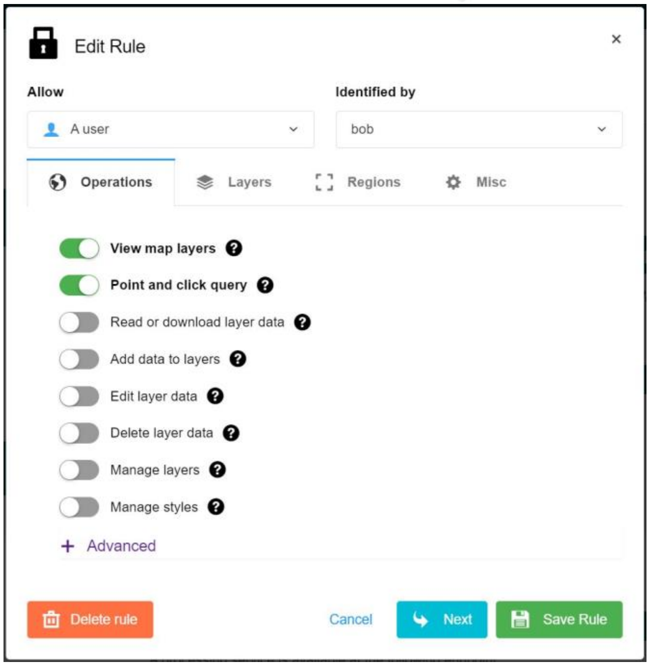


Rules can apply to the entire service, to data stores or to individual layers. The All users rule grants public access, so be sure to remove that rule before adding more specific permissions.

Stratos access control dashboard showing several user-level rules applies across an entire data store. Rules can also be attached to individual map layers in a service.

Fine-grained control

Rules are highly configurable. Each user can have a different set of allowed API operations. The simplified, human-readable operations map to specific sets of API operations in the OGC specifications. Full support for all versions of the OGC standards is built in, including the new, developer-friendly REST APIs.



Allow: A user

Identified by: bob

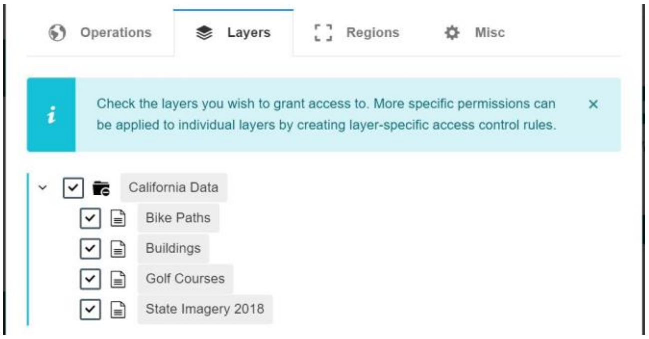
- ☑ View map layers
- ☑ Point and click query
- ☐ Read or download layer data
- ☐ Add data to layers
- ☐ Edit layer data
- ☐ Delete layer data
- ☐ Manage layers
- ☐ Manage styles

The Stratos rule editor provides a vast array of options to customize any web service.

But Guardian can do more than just allow or deny access to content. It can dynamically reconfigure the capabilities and output of any OGC service to provide a custom view on the data, based on user credentials.

Completely customizable service profiles for every user

Each identity can have its own set of layers.

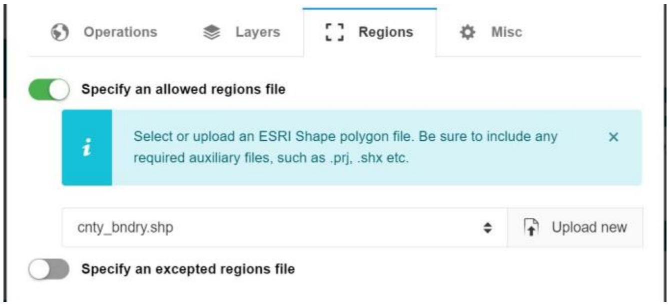


Operations | Layers | Regions | Misc

i Check the layers you wish to grant access to. More specific permissions can be applied to individual layers by creating layer-specific access control rules. ×

- ☑ California Data
  - ☑ Bike Paths
  - ☑ Buildings
  - ☑ Golf Courses
  - ☑ State Imagery 2018

Content can be "geo-fenced" to a restricted set of polygon boundaries. Just upload a shapefile or geojson document.



Operations | Layers | Regions | Misc

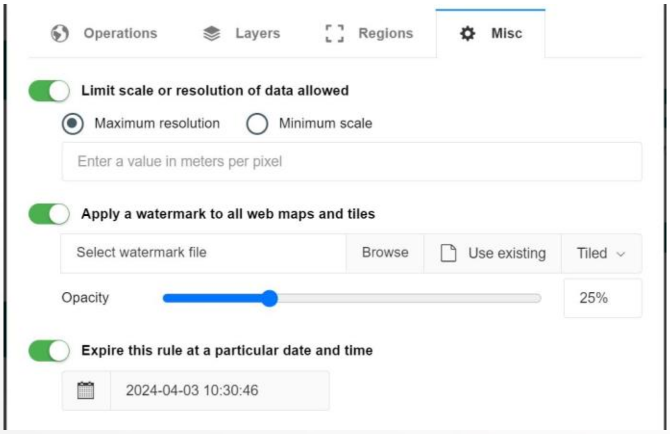
● Specify an allowed regions file

i Select or upload an ESRI Shape polygon file. Be sure to include any required auxiliary files, such as .prj, .shx etc. ×

cnty_bndry.shp | Upload new

○ Specify an excepted regions file

Or several other options, including dynamic resolution filters, i.e. user X may be limited to a resolution of 10m/pixel while user Y has access to the full data resolution. Or watermarks can be applied for free trials etc.



Operations | Layers | Regions | Misc

● Limit scale or resolution of data allowed

● Maximum resolution ○ Minimum scale

Enter a value in meters per pixel

● Apply a watermark to all web maps and tiles

Select watermark file | Browse | Use existing | Tiled

Opacity 25%

● Expire this rule at a particular date and time

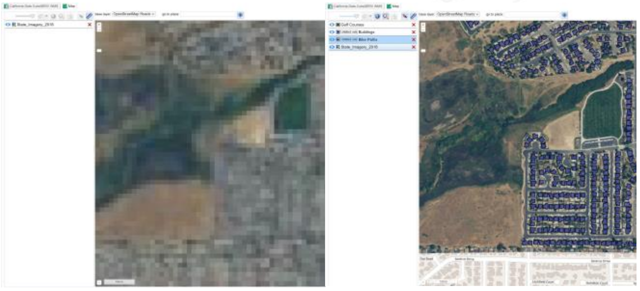
2024-04-03 10:30:46

Proxy downstream services and add security

The web services in the Stratos platform have a "cascading" capability that allows them to connect to any OGC-compliant (or ESRI REST) map server and present their layers as its own. The Guardian technology can then be used to apply access control and authentication to these services, which may have been unsecured.

Ad-hoc web services for every user

Two views on the same data source, with a completely different experience, based on credentials. User X has a limited set of layers and is limited to 10m/pixel. User Y has all layers and full resolution, but is restricted to the (Napa) county boundary polygon.



A simple web mapping application showing two different users accessing the same OGC API service, with completely different results, based on their credentials.

Built for data providers

Data providers need great flexibility in delivering web services if they are to avoid huge cost overruns building custom services for each community of users. Stratos Guardian allows providers to create customized, secure web services with ease, for every unique identity. One service, many views.

Visit https://cubewerx.com/ or email us at info@cubewerx.com today to learn more about our cutting-edge platform.