

# User Role Definitions

Anonymous

Authenticated

Device  
Officer

Service  
Desk

BI  
Analyst

Licensing  
Approver

## 1 Anonymous

*Any user that has not authenticated, or logged into the Web or Mobile Storefronts.*

An anonymous user may view the Home, About and App Details pages and request products marked viewable and requestable for the Anonymous Group. Anonymous users will be directed to login to request products not requestable by the Anonymous Group and when they want to rate a product.

## 4 Service Desk

*Allowed access to manage product deployments to machines and users.*

The Service Desk role can manage products for a single user or machine, manage multiple machines, or manage multiple users. Instead of having a user request a product, a Service Desk user may push or revoke products to specific users or machines as necessary. This role can also view deployment and usage information.

## 2 Authenticated

*All users with an account to login to the site are considered 'Authenticated'.*

Any user without additional roles, but can login to GAS is considered Authenticated. All Authenticated users can leverage standard capabilities such as search & request products, view the My Library, provide ratings, etc.

## 5 BI Analyst

*Allowed access to view API documentation and dashboards.*

The Business Intelligence Analyst can view API documentation and the product usage dashboards to produce GAS and product analysis reports.

## 3 Device Officer

*Allowed to submit multiple requests of the same product for offline devices.*

Device Officers are approved to download a product and side load it to multiple devices that may not have a network connection.  
(e.g. Mobile Devices, Thick Client Production Systems)

## 6 Licensing Approver

*Allowed access to approve license requests, restart workflows, duplicate requests and manage exclusion lists.*

The Licensing Approver reviews requests for a software license if a product has reached its license threshold, or if a product is deemed to require Licensing Approval. License Approvers can also view all items that have been manager approved if required, restart workflows, duplicate requests, and manage exclusion lists for excluding specific users requests from needing licensing approval.

More

# User Role Definitions

Manager/  
Supervisor

Department  
Licensing  
Manager

Product  
Team  
Member

Licensing  
Admin

Managed  
App  
Admin

Product  
Admin

## 7 Manager/Supervisor

*Allowed to view, approve or disapprove a product request from all users they manage.*

A user may be identified as a Manager as read from Active Directory, or selected to be a Manager by a Global Admin. The Manager has the authority to approve or disapprove a managed product request from their subordinates before it can be provisioned. A Manager can reject a request and provide justification, or approve a request that is then passed forward to the Licensing Approver.

## 8 Department Licensing Manager

*Allowed to approve or deny product requests ONLY from users within the departments they are assigned to manage.*

Department Licensing Managers are assigned by the Global Admin within each Department profile. The Department Licensing Manager has the authority to approve or deny a request ONLY from a user in a department they manage via the 'Requests' listing page.

## 9 Product Team Member

*Allowed to configure their own products.*

A Product Team Member is any Authenticated user that has submitted a product to be accessed via the GEOINT App Store, or been assigned to an existing product by a Global Admin, or the Product Team Lead. Product Team Members can edit all information for their assigned products.

## 10 Licensing Admin

*Allowed to change product licensing-related details for existing products.*

A Licensing Admin can edit licensing-related information for ALL products. Licensing Administrators are likely a Software Asset Management team that are allowed to view all items on the 'Requests' listing page that have been manager approved if required.

## 11 Managed App Admin

*Allowed to configure provisioning connections and configure managed, non-compensated desktop applications.*

A Managed App Admin is an Authenticated user that can add, edit and delete provisioning connections such as Active Directory, SCCM, and Web Services. They can also add, edit and delete managed, non-compensated desktop products.

## 12 Product Admin

*Allowed to add, edit and configure products.*

The Product Admin can edit all products with the exception of changing the vetting status, or operational level of each app.

# User Role Definitions

Governance  
Admin

IGAPP  
Admin

Global  
Admin

## 13 Governance Admin

*Allowed to upload, approve, reject, edit, and delete product resources regardless of vetting status and view reports and dashboards.*

The Governance Admin can upload, approve, reject, edit and delete governance documents associated with products regardless of the product's current vetting status. There are currently 3 stakeholder organizations within the Applications Services Governance Board (ASGB); Legal, Security, and Testing (OGC, OCIO, VVG) who can approve governance documents.

## 14 IGAPP Admin

*Allowed to change product IGAPP related details for existing products.*

The IGAPP Admin has access to add and edit products tagged as "Compensated" as well as change vetting status from IGAPPTest to IGAPPRecommend or IGAPPRejected.  
(Innovative GEOINT Application Provider Program)

## 15 Global Admin

*Allowed full/global administrative access to entire site.*

The Global Admin is essentially the "super user" role and can perform all the same functions as the other roles. In addition, a Global Admin can manage other users, grant permissions (except to self), manage content, manage messages, access logging, manage configuration of the site and services, view and modify any product in any vetting status, add governance documents, and view the Compensation Dashboard.