Gimmal

Security Model Overview

Gimmal Physical

Contents

Version History

Version	Approved By	Effective Date	Product Version	Description of Change
1	Will Irwin	10/11/2021	3.11	Created for Gimmal Version 3.11
2	Terry Butler	03/014/2022	3.11	Updated screen shots and format
3	Marta Farensbach	12/6/2022	3.12	Minor formatting changes

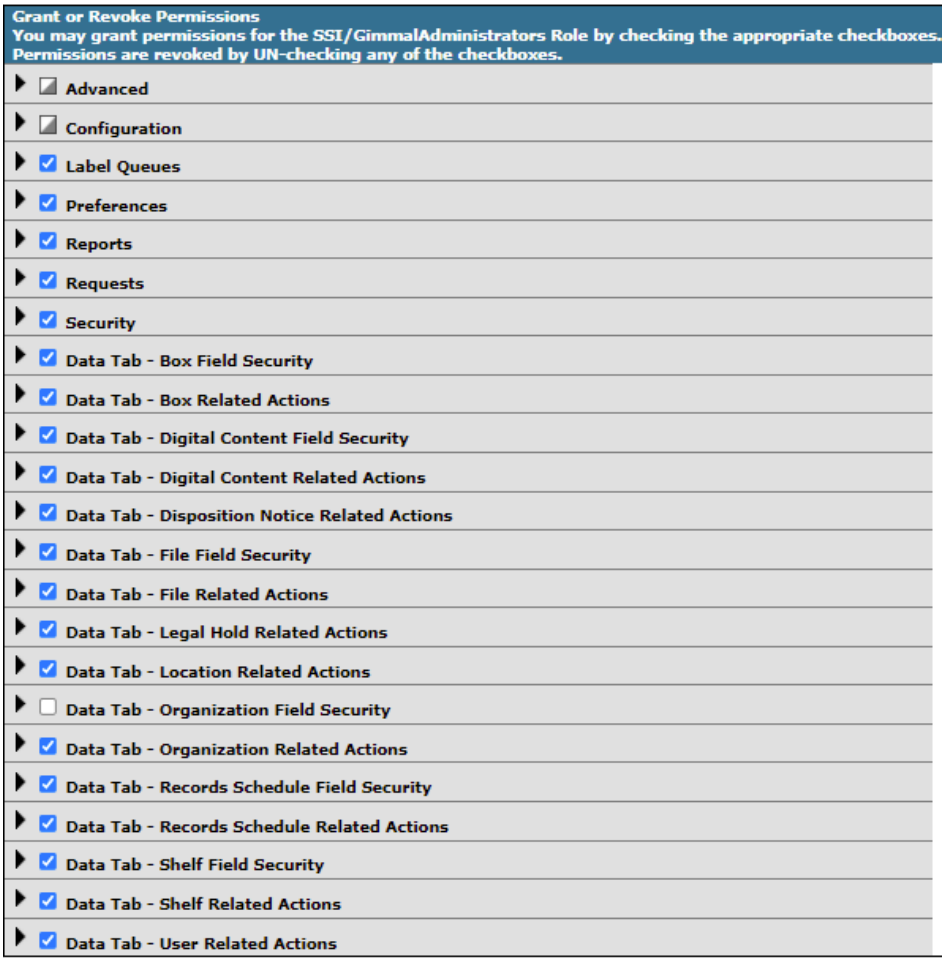
Gimmal

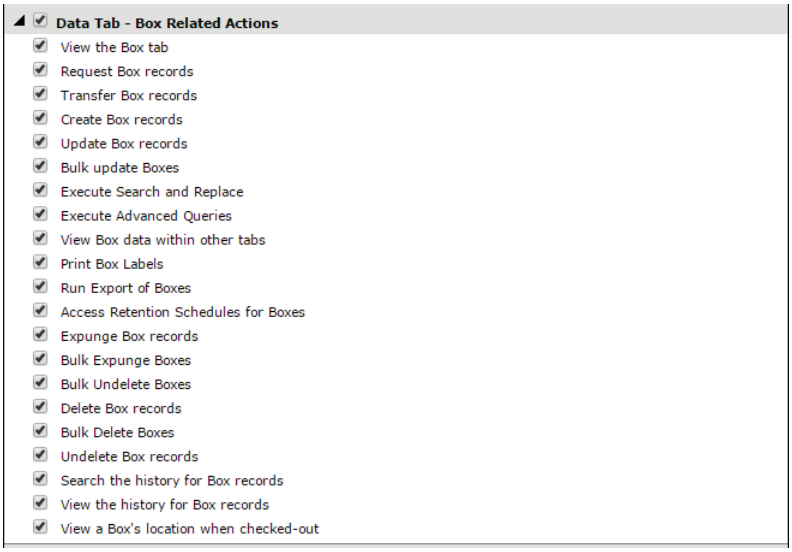
Overview

Gimmal Physical security primarily implements a role-based model supporting either forms or single-sign on authentication like that found within Windows Active Directory or Active Directory Federated Services. An unlimited number of roles are supported.

The model itself consists of two halves, the first restricting data access, and the second is application functionality.

Security roles and their associated privileges are managed from within the Gimmal Physical module, sample screenshots of which are shown below.





Authentication

The Gimmal Physical application may be accessed via either Forms or Single Sign On. Configuration of the authentication mode is managed within the application's corresponding web.config file.

When under Forms authentication, all security credentials are managed within the Gimmal Physical application itself,including Username and Password. Gimmal Physical supports the standard suite of password complexity rules including password length, types of characters required, lifespan, and number of failures until lockout.

When running on-premises against Active Directory (using Integrated Windows Authentication), each time a Gimmal Physical user attempts to access the Gimmal Physical application via the client-specific url, their network domain- specific User ID is used to query Active Directory to determine which, if any, Gimmal Physical -specific domain groupsthey belong to.

Gimmal Physical makes this determination based upon a textual comparison of Gimmal Physical roles defined within the Gimmal Physical application compared to role names defined with the network domain (e.g. 'Gimmal -administrator'or 'Gimmal Physical -Records Officer'). Outcomes include:

1. If no Gimmal Physical -specific domain group memberships are identified, the user is denied access to theapplication.

2. If an Gimmal Physical -specific domain group membership is identified, Gimmal Physical checks for the existence of aninternal Gimmal Physical user record. If one is found, Gimmal Physical updates that record with any changes found from linked Active Directory fields. If one is not found, Gimmal Physical creates the internal Gimmal Physical user record, populating it with any linked Active Directory fields.

3. If more than one Gimmal Physical -specific domain group membership is identified, Gimmal Physical selects the first itfinds and processes authentication via #2 above.

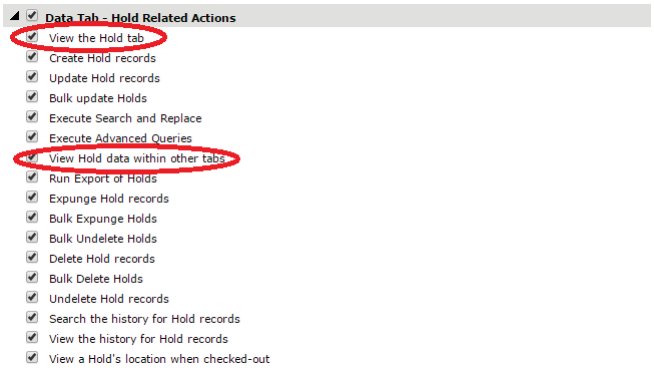
When using Single Sign On against an Identity Provider which can utilize SAMLv2, (such as OKTA, ADFS, or AAD) Gimmal Physical will authenticate the user based on the assertion sent by the IdP. Gimmal Physical can be configured to recognize a specific claim as username information and will find/create the user record inGimmal Physical based on that information. Gimmal Physical can also assign the user to a role and configure other metadata based on the claims sent in the assertion.

Data Security

Gimmal Physical data security may be configured at table, row, or column levels.

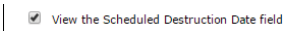
Table Level Security

Table level security corresponds to individual data tab within Gimmal Physical, allowing or preventing access to thosescreens. Table level security is managed via simple checkbox driven logic within the security module as shown below. A common example is granting or denying access to the Holds tab.



Column Level Security

Column level security provides the ability to hide individual data elements. Column level security is managed via simple checkbox driven logic within the security module as shown below. A common example might be to hide the Scheduled Destruction Date for boxes or files.



Row Level Security

Row level security provides the ability to restrict users to those data records specific to them. Row level security may be implemented via Tab Filters, Secured Lists, or User-level meta-data, an example of each shown below.

Gimmal

Tab Filters

You may apply filters to the SSI/GimmalAdministrators Role by checking the appropriate checkboxes.
Filters are removed by UN-checking any of the checkboxes.

	Tab	Name	Description
☐		Hide Deleted Boxes	Find all Boxes where (**Deleted** Not Equal To **TRUE**).
☐		Hide Deleted Digital Content	Find all Digital Content where (**Deleted** Not Equal To **TRUE**).
☐		Hide Deleted Disposition Notices	Find all Disposition Notices where (**Deleted** Not Equal To **TRUE**).
☐		Hide Deleted Files	Find all Files where (**Deleted** Not Equal To **TRUE**).
☐		Hide Deleted Legal Holds	Find all Legal Holds where (**Deleted** Not Equal To **TRUE**).
☐		Hide Deleted Locations	Find all Locations where (**Deleted** Not Equal To **TRUE**).
☐		Hide Deleted Organizations	Find all Organizations where (**Deleted** Not Equal To **TRUE**).
☐		Hide Deleted Records Schedules	Find all Records Schedules where (**Deleted** Not Equal To **TRUE**).
☐		Hide Deleted Shelves	Find all Shelves where (**Deleted** Not Equal To **TRUE**).
☐		Hide Deleted Users	Find all Users where (**Deleted** Not Equal To **TRUE**).

Modify List Security

Select Tab: Legal Hold

Checked fields are rights that have been granted for items with the specified list value.

List: Hold Status

Select All Unselect All

	Bulk Delete	Bulk Expunge	Bulk Undelete	Bulk Update	Create	Data Sheet	Delete	Export	Expunge	History	Print Labels	Request	Retention	Search & Replace	Transfer	UnDelete	Update	View
Active	☐	☐	☐	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Inactive	☐	☐	☐	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

Functional Security

Gimmal Physical functional security provides the ability to grant or deny access to virtually every functionalcapability within the software, corresponding to the application ribbon and action menus displayed below.