

Security Model Overview

Gimmel Physical

Contents

Version History	1
Overview	1
Authentication	2
Data Security	4
Table Level Security	4
Column Level Security	4
Row Level Security	5
Functional Security	6

Version History

Version	Approved By	Effective Date	Description of Change
3.11	Will Irwin	10/11/2021	Created for Gimmel Physical v3.11
3.11	Terry Butler	03/25/2022	Updated screen shots and format

Overview

Gimmel 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 application functionality.

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

Grant or Revoke Permissions
 You may grant permissions for the SSI/GimmelAdministrators Role by checking the appropriate checkboxes. Permissions are revoked by UN-checking any of the checkboxes.

<input checked="" type="checkbox"/> Advanced
<input checked="" type="checkbox"/> Configuration
<input checked="" type="checkbox"/> Label Queues
<input checked="" type="checkbox"/> Preferences
<input checked="" type="checkbox"/> Reports
<input checked="" type="checkbox"/> Requests
<input checked="" type="checkbox"/> Security
<input checked="" type="checkbox"/> Data Tab - Box Field Security
<input checked="" type="checkbox"/> Data Tab - Box Related Actions
<input checked="" type="checkbox"/> Data Tab - Digital Content Field Security
<input checked="" type="checkbox"/> Data Tab - Digital Content Related Actions
<input checked="" type="checkbox"/> Data Tab - Disposition Notice Related Actions
<input checked="" type="checkbox"/> Data Tab - File Field Security
<input checked="" type="checkbox"/> Data Tab - File Related Actions
<input checked="" type="checkbox"/> Data Tab - Legal Hold Related Actions
<input checked="" type="checkbox"/> Data Tab - Location Related Actions
<input type="checkbox"/> Data Tab - Organization Field Security
<input checked="" type="checkbox"/> Data Tab - Organization Related Actions
<input checked="" type="checkbox"/> Data Tab - Records Schedule Field Security
<input checked="" type="checkbox"/> Data Tab - Records Schedule Related Actions
<input checked="" type="checkbox"/> Data Tab - Shelf Field Security
<input checked="" type="checkbox"/> Data Tab - Shelf Related Actions
<input checked="" type="checkbox"/> Data Tab - User Related Actions

<input checked="" type="checkbox"/> Data Tab - Box Related Actions
<input checked="" type="checkbox"/> View the Box tab
<input checked="" type="checkbox"/> Request Box records
<input checked="" type="checkbox"/> Transfer Box records
<input checked="" type="checkbox"/> Create Box records
<input checked="" type="checkbox"/> Update Box records
<input checked="" type="checkbox"/> Bulk update Boxes
<input checked="" type="checkbox"/> Execute Search and Replace
<input checked="" type="checkbox"/> Execute Advanced Queries
<input checked="" type="checkbox"/> View Box data within other tabs
<input checked="" type="checkbox"/> Print Box Labels
<input checked="" type="checkbox"/> Run Export of Boxes
<input checked="" type="checkbox"/> Access Retention Schedules for Boxes
<input checked="" type="checkbox"/> Expunge Box records
<input checked="" type="checkbox"/> Bulk Expunge Boxes
<input checked="" type="checkbox"/> Bulk Undelete Boxes
<input checked="" type="checkbox"/> Delete Box records
<input checked="" type="checkbox"/> Bulk Delete Boxes
<input checked="" type="checkbox"/> Undelete Box records
<input checked="" type="checkbox"/> Search the history for Box records
<input checked="" type="checkbox"/> View the history for Box records
<input checked="" type="checkbox"/> View a Box's location when checked-out

Authentication

The Gimmel 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 Gimmel Physical application itself, including Username and Password. Gimmel 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-premise against Active Directory (using Integrated Windows Authentication), each time an Gimmel Physical user attempts to access the Gimmel Physical application via the client-specific url, their network domain-specific User ID is used to query Active Directory to determine which, if any, Gimmel Physical -specific domain groupsthey belong to.

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

1. If no Gimmel Physical -specific domain group memberships are identified, the user is denied access to the application.
2. If an Gimmel Physical -specific domain group membership is identified, Gimmel Physical checks for the existence of an internal Gimmel Physical user record. If one is found, Gimmel Physical updates that record with any changes found from linked Active Directory fields. If one is not found, Gimmel Physical creates the internal Gimmel Physical user record, populating it with any linked Active Directory fields.
3. If more than one Gimmel Physical -specific domain group membership is identified, Gimmel Physical selects the first it finds 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) Gimmel Physical will authenticate the user based on the assertion sent by the IdP. Gimmel Physical can be configured to recognize a specific claim as username information and will find/create the user record in Gimmel Physical based on that information. Gimmel 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.

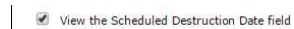
Table Level Security

Table level security corresponds to individual data tab within Gimmal Physical, allowing or preventing access to those screens. 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.

Tab Filters

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

	Tab	Name	Description
<input type="checkbox"/>		Hide Deleted Boxes	Find all Boxes where (Deleted Not Equal To TRUE).
<input type="checkbox"/>		Hide Deleted Digital Content	Find all Digital Content where (Deleted Not Equal To TRUE).
<input type="checkbox"/>		Hide Deleted Disposition Notices	Find all Disposition Notices where (Deleted Not Equal To TRUE).
<input type="checkbox"/>		Hide Deleted Files	Find all Files where (Deleted Not Equal To TRUE).
<input type="checkbox"/>		Hide Deleted Legal Holds	Find all Legal Holds where (Deleted Not Equal To TRUE).
<input type="checkbox"/>		Hide Deleted Locations	Find all Locations where (Deleted Not Equal To TRUE).
<input type="checkbox"/>		Hide Deleted Organizations	Find all Organizations where (Deleted Not Equal To TRUE).
<input type="checkbox"/>		Hide Deleted Records Schedules	Find all Records Schedules where (Deleted Not Equal To TRUE).
<input type="checkbox"/>		Hide Deleted Shelves	Find all Shelves where (Deleted Not Equal To TRUE).
<input type="checkbox"/>		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																		
	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	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Inactive	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Functional Security

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

