

|  |  |
| --- | --- |
|  | **icenter.suite** |
|  |  |
|  | Data scopes and permissions |
|  |  |
|  |  |
|  |  |
|  | Technical Document |
|  |  |
|  | Version: 2.2 |
|  | State: Draft |
|  | Classification: Internal use only |
|  | Author: EPT |
|  | Creation date: 2013-09-04 |
|  | Repository: $/Gorba/Main/Center/Common/Documents/TD\_Data scopes and permissions.docx |
|  | Gorba AG  Sandackerstrasse  9245 Oberbüren  Switzerland |

**Table of contents**

[1 Introduction 4](#_Toc430156462)

[1.1 Audience 4](#_Toc430156463)

[2 Overview 4](#_Toc430156464)

[2.1 Authorization 4](#_Toc430156465)

[2.1.1 Null Tenant 4](#_Toc430156466)

[3 Data scopes and permissions 5](#_Toc430156467)

[3.1 Data scopes 5](#_Toc430156468)

[3.2 Permissions 5](#_Toc430156469)

[3.3 Usage in icenter.admin 5](#_Toc430156470)

[3.4 Usage in icenter.media 7](#_Toc430156471)

[3.5 Usage in icenter.suite Portal 8](#_Toc430156472)

[3.6 Usage in icenter.diag 8](#_Toc430156473)

**Modification management**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Date** | **Name** | **Dept.** | **Modifications** | **State** |
| 0.1 | 04.09.2013 | EPT | SW Dev. | Initial document | Draft |
| 0.2 | 06.09.2013 | EPT | SW Dev. | Changes according review | Draft |
| 0.3 | 27.09.2013 | LEF | SW Dev. | Specified the special permissions needed for some operations of the Membership Service (new chapter 3.6) | Draft |
| 1.1 | 19.01.2015 | WES | SW Dev. | Reworked for icenter.suite 2.0, including icenter.admin | Draft |
| 1.2 | 19.01.2015 | EPT | SW Dev. | Added chapter 3.4: Usage in icenter.media | Draft |
| 2.1 | 22.04.2015 | WES | SW Dev. | Added special application specific data scopes for icenter applications. | Draft |
| 2.2 | 16.09.2015 | EPT | SW Dev. | Added permissions for icenter.admin in Meta for BackgroundSystemSettings and FTP servers  Added chapter 3.6 | Draft |

**Review**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Name** | **Dept.** | **Remarks** |
| 0.1 | 06.09.2013 | INB/WES/LEF/EPT |  | Add data scopes Layout and StopPoint  Add chapter 3.5 and 3.6  Replace Update data scope with Interact  Changing some permissions in chapter 3.4 |
|  |  |  |  |  |
| 0.3 | 15.07.2014 | EPT | SW Dev. | Ok. |
|  |  |  |  |  |
| 1.2 | 29.01.2015 | LEF | SW Dev | Ok |

**Release**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Name** | **Dept.** | **Remarks** |
| 1.0 | 15.07.2014 | EPT | SW Dev. | 1st release |
|  |  |  |  |  |
| 2.0 | 29.01.2015 | EPT | SW Dev | 2nd release |
|  |  |  |  |  |

# Introduction

This document describes the data scopes and permissions used in Gorba icenter applications. By now only icenter.admin and icenter.media are described.

## Audience

This document is addressed to developers, product managers and project managers.

# Overview

icenter.BackgroundSystem

Application (icenter.admin, icenter.media)

Service operation:

* Validate the user only
* Throws exception if credentials are wrong

Function

* Only available if the user has the permission

Gorba applications enable functions depending on the data scope and permission of the logged in user. Currently the BackgroundSystem does not validate the permissions for each operation.

## Authorization

To authorize a User to do a specific operation, that User must have the given right for the Tenant for which the operations are executed. Some of the Data Scopes are not tenant-specific (i.e. valid for the entire system), but most data scopes are tenant-specific (i.e. a user can have different rights for different tenants).

A User is never directly given access rights, but through User Roles:

**User**

**User Role**

Association from a User to a User Role for a given Tenant (or the “Null Tenant”)

**Authorization**

\* \*

\* \*

### Null Tenant

If a User should have a certain role for every Tenant in the system (including new Tenants), the role can be assigned to that user with the Tenant set to null. This is called the “Null Tenant”.

The automatically created “admin” user always has all rights for the Null Tenant.

# Data scopes and permissions

## Data scopes

Data scopes define a set of specific operations / UI behaviors. The following table shows all available data scopes:

|  |  |
| --- | --- |
| **Data scope** | **Description** |
| AccessControl\* | Operations related to access control definitions. |
| Tenant\* | Operations related to tenants. |
| User | Operations related to users. |
| ProductType\* | Operations related to product types. |
| Unit | Operations related to units and related data. |
| Resource\* | Operations related to resources. |
| Update | Operations related to unit updates. |
| Software\* | Operations related to software available for installation on units. |
| UnitConfiguration | Operations related to the configuration (config files) of units. |
| MediaConfiguration | Operations related to the presentation files (Infomedia) on units. |
| Meta | Operations related to the structure of the database itself. |
| CenterAdmin | Authorization to download and use icenter.admin |
| CenterDiag | Authorization to download and use icenter.diag |
| CenterMedia | Authorization to download and use icenter.media |

\* The data scopes with an asterisk are not tenant-specific, thus a user has the given permissions for those scopes for the entire database independent for which tenant he was granted the permissions.

## Permissions

Permissions can be set for each data scope per user role. The following table shows all available permissions:

|  |  |
| --- | --- |
| **Permission** | **Description** |
| Create | Allows the user to create new entities in the given data scope |
| Read | Allows the user read-only access to entities in the given data scope. |
| Write | Allows the user read and write access to entities in the given data scope |
| Delete | Allows the user to delete existing entities in the given data scope |
| Interact | Allows the user to interact with an entity in the given data scope |
| Abort | Allows the user to abort operations related to an entity in the given data scope |

## Usage in icenter.admin

Only used permissions are listed.

|  |  |  |
| --- | --- | --- |
| **Data scope** | **Permission** | **Usage** |
| AccessControl | Create | * Create Authorizations * Create User Roles |
|  | Read | * See the Authorizations Entity Stage * See the User Roles Entity Stage * Can change access to the “null tenant” (any current and future tenant in the system) for any user |
|  | Write | * Change Authorization properties * Change User Role properties |
|  | Delete | * Delete Authorizations * Delete User Roles |
| Tenant | Create | * Create Tenants |
|  | Read | * See the Tenants Entity Stage |
|  | Write | * Change Tenant properties |
|  | Delete | * Delete Tenants |
| User | Create | * Create Users * Assign Users to User Roles for a certain Tenant |
|  | Read | * See the Users Entity Stage * See the Users to User Role Entity Stage |
|  | Write | * Change User properties * Change associations between Users and User Roles |
|  | Delete | * Delete Users * Delete associations between Users and User Roles |
| ProductType | Create | * Create Product Types |
|  | Read | * See the Product Types Entity Stage |
|  | Write | * Change Product Type properties |
|  | Delete | * Delete Product Types |
| Unit | Create | * Add Units to the database |
|  | Read | * See the Units Entity Stage |
|  | Write | * Change Unit properties |
|  | Delete | * Delete Units from the database |
| Resources | Create | * none |
|  | Read | * See the Resources Entity Stage |
|  | Write | * none |
|  | Delete | * Delete Resources |
| Update | Create | * Create Update Groups * Create Update Parts * Create Update Commands * Create Update Feedbacks |
|  | Read | * See the Update Groups Entity Stage * See the Update Parts Entity Stage * See the Update Commands Entity Stage * See the Update Feedbacks Entity Stage |
|  | Write | * Change Update Group properties * Change Update Part properties * Change Update Command properties * Change Update Feedback properties |
|  | Delete | * Delete Update Groups * Delete Update Parts * Delete Update Commands * Delete Update Feedbacks |
| Software | Create | * Create Software Packages * Create Software Package Versions |
|  | Read | * See the Software Packages Entity Stage * See the Software Package Versions Entity Stage |
|  | Write | * Change Software Package properties * Change Software Package Version properties |
|  | Delete | * Delete Software Packages * Delete Software Package Versions |
| UnitConfiguration | Create | * Create Unit Configurations |
|  | Read | * See the Unit Configurations Entity Stage * See the Documents Entity Stage * See the Document Versions Entity Stage |
|  | Write | * Change Unit Configuration properties * Change Document properties * Change Document Version properties |
|  | Delete | * Delete Unit Configurations * Delete Documents * Delete Document Versions |
| MediaConfiguration | Create | * none |
|  | Read | * See the Media Configurations Entity Stage * See the Documents Entity Stage * See the Document Versions Entity Stage |
|  | Write | * Change Media Configuration properties * Change Document properties * Change Document Version properties |
|  | Delete | * Delete Documents * Delete Document Versions |
| Meta | Create | * Create User Defined Properties * Create FTP servers |
|  | Read | * See the User Defined Properties Entity Stage * See the BackgroundSystemSettings Stage * See the FtpServers Stage |
|  | Write | * Change User Defined Property properties * Change FTP servers * Change BackgroundSystem settings |
|  | Delete | * Delete User Defined Properties * Delete FTP servers |
| CenterAdmin | Interact | * Use icenter.admin for this tenant |

Remark: Despite some data scopes not being tenant-specific, the visibility of the Entity Stages is still done depending on the currently selected Tenant. If you can’t see a certain “non-tenant-specific” Stage, try switching the Tenant.

## Usage in icenter.media

Only used permissions are listed.

|  |  |  |
| --- | --- | --- |
| **Data scope** | **Permission** | **Usage** |
| MediaConfiguration | Create | * Create new media projects * Import projects * Check-in as project |
|  | Read | * Open projects * Navigate within projects |
|  | Write | * Change projects (layouts, cycles, sections, physical screens, media (resources), text replacements) * Check-in projects * Export projects * Rename projects |
|  | Delete | * Delete projects |
| CenterMedia | Interact | * Use icenter.media for this tenant |

Remark: If a project is opened with Read rights, the user can still edit the existing content, but he can’t save it.

## Usage in icenter.suite Portal

Only used permissions are listed.

|  |  |  |
| --- | --- | --- |
| **Data scope** | **Permission** | **Usage** |
| CenterAdmin | Interact | * Download icenter.admin |
| CenterDiag | Interact | * Download icenter.diag |
| CenterMedia | Interact | * Download icenter.media |

Remark: Only the link to the download of an application is hidden, the download itself is not secured with a password. If the user knows the path to the download, he can still download the application. But in any case he won’t be able to log in.

## Usage in icenter.diag

Only used permissions are listed and these are only valid in Online mode.

|  |  |  |
| --- | --- | --- |
| **Data scope** | **Permission** | **Usage** |
| Unit | Interact | * Restart unit * Restart/Exit applications on a unit |
| CenterDiag | Interact | * Use icenter.diag for this tenant |