(https://sprintr.home.mendix.com)

Buzz (https://sprintr.home.mendix.com/link/home)Apps (https://sprintr.home.mendix.com/link/myprojects)People (https://developer.mendixcloud.com/link/people)

Community (https://developers.mendix.com/) App Store (https://appstore.home.mendix.com)Academy (https://gettingstarted.mendixcloud.com)

Blogs (https://developers.mendix.com/spotlight/)

Forum (https://forum.mendixcloud.com)Docs (https://docs.mendix.com)

Jobs (https://developers.mendix.com/jobs/)

Model Share (https://modelshare.mendix.com/)

MVP Program (https://developer.mendixcloud.com/link/mvp)

Leaderboards (https://developer.mendixcloud.com/link/leaderboards)

Our Partners (https://developer.mendixcloud.com/link/partneroverview)

Mendix Shop (https://shop.mendix.com)

(https://sp home.mendix.com/link/not

Docs (/) / ... / App Modeling (/refguide/modeling) / Menus (/refguide/menus) / View Menu (/refguide/view-menu) / Project Explorer (/refguide/project-explorer)

Search documentation

Security

Last update: Sep 23, 2019

Edit (https://github.com/mendix/docs/blob/development/content/refguide/security.md)

1 Introduction

Security in Mendix has two sides: you want different people to see different parts of your application and you want to prevent unauthorized access. Both of these can be managed from Studio Pro. Access to forms, data and microflows can be limited to authorized users.

> Security in Mendix does not include scanning files that end-users upload or download from your application for viruses and malware. For more information, see the Scanning Uploaded Files for Malicious Content (/howto/security/best-practices-security#scanning-for-malicious-content) section in *How to Implement Best Practices for App Security*.

2 Security Levels

If you want full security, you need to explicitly give access to forms, entities and microflows before someone can access them. By default, no one can access anything. To make it easier to create prototypes and demos there are security levels that require less security settings than are needed for a production system.

See Project Security (project-security) for a description of the security levels.

3 Project vs. Module Security

At the level of a project some global settings can be specified: the security level, the administrator account and whether or not to allow anonymous access.

See Project Security (project-security).

Most of the security settings take place at the module level. This has the advantage that a module can specify its own security and can be distributed and reused in other projects. Access to forms, entities, microflows and datasets can be configured.

See Module Security (module-security).

4 User Roles vs. Module Roles

An end-user in a Mendix application has one or more user roles. These roles can be assigned from within the client when creating or editing a user. User roles are at the level of a project and can be edited in Project Security (project-security).

See User Roles (user-roles).

Each module defines its own set of module roles and you only have to specify security within a module in terms of those module roles. An e-mail module maybe has two module roles, one for normal user and one for an administrator; other modules may have just one or more than two module roles depending on the requirements for those modules.

See Module Role (module-security#module-role).

A user role is a combination of module roles. A user that signs into the system gets the access rights of all of his or her user roles and indirectly to the module roles that are contained by those user roles.

Let us say you have a project with two modules: System and ProjectManagement (PM). The PM module has three module roles: TeamMember, TeamLeader and Administrator. And let us say that in this case, we only need two user roles because we do not need the distinction between team leaders and administrators. You define those two user roles and assign module roles to them. The table below shows which module roles are contained within the user roles. Note that you always need at least the User role in System.

User Role 'TeamMember'	User Role 'TeamLeader'
System.User	System.User
ProjectManagement.TeamMember	ProjectManagement.TeamLeader
	ProjectManagement.Administrator

5 Entity Access vs. Page Access

Per entity you can specify who can read or write what members (attributes and associations) under what circumstances. Using XPath constraints you can express powerful security behavior; e.g. “an employee can only see orders created by the department he is a part of”.

Per page you can specify who can open it from navigation. The menu bar is optimized so that only pages that the user has access to are visible.

A combination of entity access and a page access is necessary because entities can also be accessed from microflows and custom widgets. Furthermore, you can express more advanced security through entity access.

See Entity Access (module-security).

› Release Notes
(/releasenotes/)

Table of contents

Studio Pro 8 Guide
(/refguide/)
General Info
(/refguide/general)
App Modeling
(/refguide/modeling)
Studio Pro Overview
(/refguide/studio-pro-overview)
Menus
(/refguide/menus)
File Menu
(/refguide/file-menu)
Edit Menu
(/refguide/edit-menu)
View Menu
(/refguide/view-menu)
Changes Pane
(/refguide/changes-pane)
Errors Pane
(/refguide/errors-pane)
Project Explorer
(/refguide/project-explorer)
Project
(/refguide/project)
Modules
(/refguide/modules)
Security
(/refguide/security)
Project Security
(/refguide/project-security)
Module Security
(/refguide/module-security)
Model Changes When Security Is Enabled in Studio
(/refguide/studio-security-enabled)
Stories Pane
(/refguide/stories-pane)
Project Menu
(/refguide/project-menu)
Run Menu
(/refguide/run-menu)
Version Control Menu
(/refguide/version-control-menu)

Table of contents

Domain Model
(/refguide/domain-model)
› Pages
(/refguide/pages)
› Application Logic
(/refguide/application-logic)
› Resources
(/refguide/resources)
Data Types
(/refguide/data-types)
Images
(/refguide/images)
Translatable Texts
(/refguide/translatable-texts)
› XPath
(/refguide/xpath)
› Integration
(/refguide/integration)
› Version Control
(/refguide/version-control)
› Mendix Runtime
(/refguide/runtime)
› Mobile
(/refguide/mobile)
› Java Programming
(/refguide/java-programming)
› Studio Pro 8 How-to's
(/howto/)
› Studio 8 Guide
(/studio/)
› Developer Portal Guide
(/developerportal/)
› Strategic Partners Guide
(/partners/)
› APIs & SDK
(/apidocs-mxsdk/)
› Add-on Guides
(/addons/)
› Mendix 7 Reference Guide
(/refguide7/)
› Mendix 7 How-to's
(/howto7/)
› Mendix 7 Studio Guide

(/studio7/)
› Mendix 6 Reference Guide (/refguide6/)
› Mendix 6 How-to's (/howto6/)

Want to contribute to our documentation? Start here! (/developerportal/community-tools/contribute-to-the-mendix-documentation)

Buzz **(https://sprintr.home.mendix.com/link/home)**
Apps (https://sprintr.home.mendix.com/link/myprojects)
People (https://developer.mendixcloud.com/link/people)
App Store (https://appstore.home.mendix.com/)

Community
Blogs (https://developers.mendix.com/spotlight/)
Jobs (https://developers.mendix.com/jobs/)
Model Share (https://modelshare.mendix.com/)
MVP Program (https://developer.mendixcloud.com/link/mvp)
Leaderboards (https://developer.mendixcloud.com/link/leaderboards)
Our Partners (https://developer.mendixcloud.com/link/partneroverview)
Mendix Shop (https://shop.mendix.com)

Academy **(https://gettingstarted.mendixcloud.com)**
Learning Paths (https://gettingstarted.mendixcloud.com/link/path)
Modules (https://gettingstarted.mendixcloud.com/link/module)
Webinars (https://gettingstarted.mendixcloud.com/link/webinar)
Classroom (https://gettingstarted.mendixcloud.com/link/classroom)
Certifications (https://gettingstarted.mendixcloud.com/link/certification)

Forum **(https://forum.mendixcloud.com)**
Forum Questions (https://forum.mendixcloud.com/link/questions)
Forum Ideas (https://forum.mendixcloud.com/link/ideas)

Docs
Refer
(http
How-
(http
Relea
(http
API &
(http
mxsc
Low-
(http
guide