EEforce 26.9 Documentation

Milbitt Software

2026-09-20

Contents

Introduction **7**
Architecture . . . 7
Core Concepts . . . 8
Projects . . . 8
Containers . . . 8
Version Control . . . 8
Access Control . . . 8
Key Features . . . 9
Supported Design Tools . . . 9
What's Next . . . 10

Release Notes - Version 26.9 **10**
Scheduled LDAP Group Sync . . . 10

Server Installation and Configuration **10**
Prerequisites . . . 10
Installation . . . 11
Step 1 - Download and Extract . . . 11
Step 2 - Run the Installer . . . 12
Step 3 - Accept the License Agreement . . . 13
Step 4 - Configure Paths . . . 14
Step 5 - Confirm and Install . . . 15
Step 6 - Complete . . . 16
Starting and Stopping the Server . . . 17
Using IIS Manager (GUI) . . . 17
Using PowerShell . . . 17
Post-Installation Configuration . . . 17
config.json . . . 17
Relocating Storage . . . 18
Setting Folder Permissions . . . 18
SSL/TLS Configuration . . . 19
Troubleshooting . . . 20

Client Installation and Configuration **20**
Prerequisites . . . 20
Installation . . . 20
Step 1 - Download and Extract . . . 20

Step 2 - Run the Installer . . . 21
Step 3 - Welcome Screen . . . 22
Step 4 - License Agreement . . . 23
Step 5 - Choose Installation Folder . . . 24
Step 6 - Confirm and Install . . . 25
Step 7 - Complete . . . 26
First Run . . . 27
Connect to Server . . . 27
Log In . . . 28
Select a License . . . 28
Configuration . . . 30
Server Settings . . . 31
Xpedition Settings . . . 32
PADS Professional Settings . . . 33
BOM Preview Settings . . . 33
Troubleshooting . . . 35

Licensing **35**
How Licensing Works . . . 35
License Dimensions . . . 36
Duration . . . 36
Binding . . . 36
Tool Tier . . . 36
License Upgrades . . . 37
Managing Licenses . . . 37
Troubleshooting . . . 37

Frequently Asked Questions **38**
Compatibility . . . 38
What versions of PADS are supported? . . . 38
What versions of Xpedition are supported? . . . 38
Can I store non-Professional PADS designs (PADS Standard, Logic, etc.)? . . . 38
Can I store other file types (PDFs, specs, mechanical files)? . . . 38
Data and Storage . . . 38
Where is my data stored? . . . 38
How are backups handled? . . . 38
What happens when a design is deleted? . . . 39

Networking and Access . . . 39
Can I access my server over the Internet? . . . 39
What ports does EEforce use? . . . 39
Can multiple users work on the same project simultaneously? . . . 39
Licensing . . . 40
What happens when all license seats are in use? . . . 40
Can I move a node-locked license to a different machine? . . . 40
Troubleshooting . . . 40
The client shows “Cannot connect to server” . . . 40
Check-in is slow or fails on large designs . . . 40
“Design is locked” but no one is editing . . . 40

Project Operations **41**
Project Explorer . . . 41
Filtering Projects . . . 42
Project Status Icons . . . 43
Creating a Project . . . 44
Renaming a Project . . . 45
Managing Project Access . . . 46
Cloning a Project . . . 47
Deleting a Project . . . 48
Batch Project Operations . . . 49

Access Control **49**
Roles . . . 50
How Effective Role Is Calculated . . . 50
Special System Entities . . . 51
Assigning Access . . . 51
From the Desktop Client . . . 51
From the Web Admin Interface . . . 53
Making a Project Public . . . 54
Security Rules . . . 55
Legacy Projects . . . 55
Batch Updates . . . 55

Container Operations **56**
Container Types . . . 56
Accessing Container Operations . . . 57
Importing a Container . . . 57

Renaming a Container . . . 60
Cloning a Container . . . 60
Deleting a Container . . . 60
Moving a Container to Another Project . . . 61
Copying a Container to Another Project . . . 63
Container States . . . 65

Design Operations **65**
Design States . . . 65
Available Operations . . . 66
Opening a Design in Read-Only Mode . . . 67
Checking Out a Design (Start Editing) . . . 67
Checking In a Design (Finish Editing) . . . 67
Cancelling a Check-Out (Discard Changes) . . . 69
Version History . . . 70
Troubleshooting . . . 70

Remote Working **71**
How It Works . . . 71
Exporting a Design for Remote Work . . . 71
Working with the Exported Package . . . 72
Importing a Remotely Updated Design . . . 72
Cancelling a Remote Check-Out . . . 73
Tips for Remote Working . . . 73

Web Administration Interface **73**
Login . . . 74
Dashboard . . . 75
User Management . . . 76
Group Management . . . 77
System Groups . . . 77
Project Management . . . 78
Logs . . . 79
Settings . . . 80
LDAP Configuration . . . 81
SSO Configuration . . . 81
Server Restart . . . 81
Logging Out . . . 83

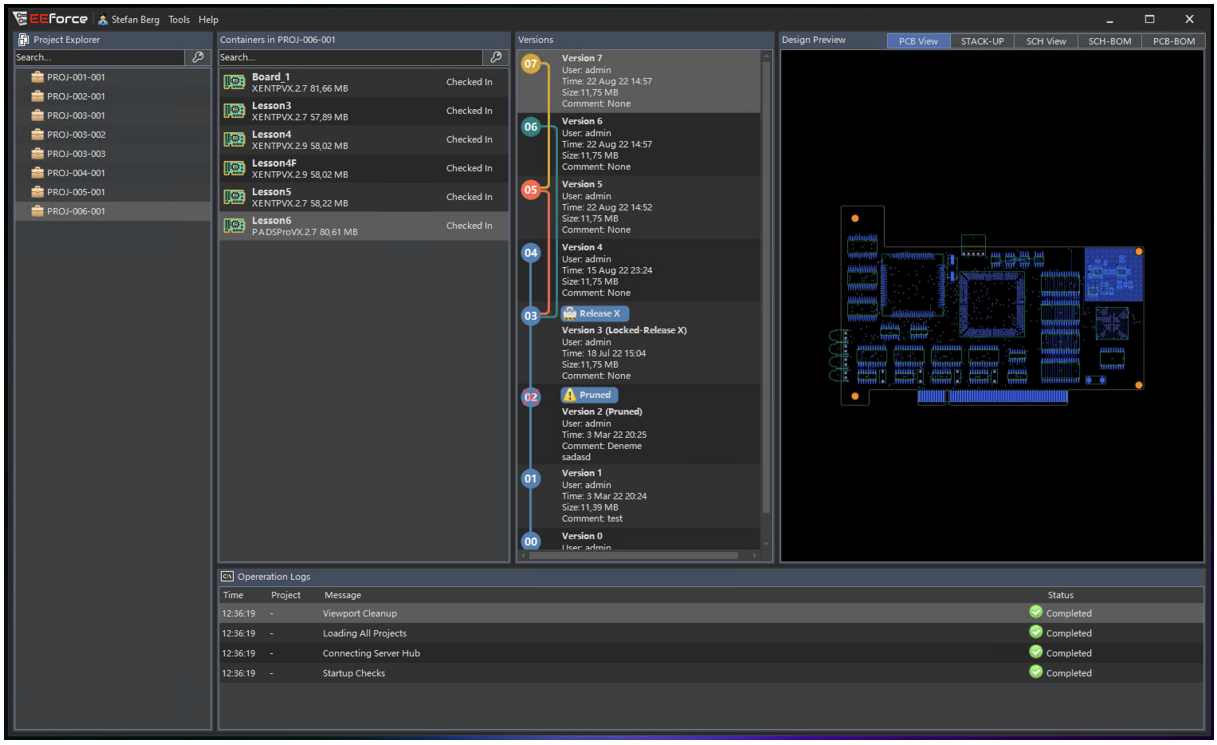
Administration from the Desktop Client **83**
Group Management . . . 84
System Groups . . . 84
User Management . . . 85
LDAP Configuration . . . 86
SSO Configuration . . . 87

LDAP Integration **87**
Overview . . . 87
Configuration . . . 88
From the Web Admin Interface . . . 88
From the Desktop Client . . . 88
Settings Reference . . . 89
Setup Steps . . . 90
1. Create a Service Account in AD . . . 90
2. Configure LDAP in EEforce . . . 90
3. Test the Connection . . . 91
4. Enable Auto-Registration (Optional) . . . 91
Group Synchronization . . . 91
How Group Sync Works . . . 92
Linking a Group . . . 92
Example Configuration . . . 92
User Lifecycle . . . 93
New LDAP User (Auto-Register Enabled) . . . 93
Existing LDAP User . . . 93
User Leaves the Organization . . . 94
SSL/LDAPS . . . 94
Troubleshooting . . . 94

SSO Integration (Single Sign-On) **95**
Overview . . . 95
Authentication Flow . . . 95
Prerequisites . . . 96
Configuration . . . 96
Settings Reference . . . 97
Setup Guide . . . 98
Step 1: Register EEforce in Your Identity Provider . . . 98
Step 2: Configure EEforce . . . 99

Step 3: Test 100
User Provisioning 100
Client Experience 101
Automatic SSO Login 101
Combining SSO with Local and LDAP Authentication 102
Security Considerations 102
Troubleshooting 102

Introduction



EEforce is a design lifecycle management (DLM) platform purpose-built for Siemens EDA tools - Xpedition and PADS Professional. It provides centralized version control, access management, and collaboration for PCB design teams.

Architecture

EEforce uses a client-server architecture:

Component	Role
Server	Stores all design files as versioned objects in an isolated vault. Manages users, groups, licenses, and access control. Runs as an IIS application on Windows Server.

Component	Role
Client	Desktop application (Windows) that provides the UI for browsing projects, checking designs in/out, previewing content, and managing settings.
Web Admin	Browser-based administration panel for managing users, groups, projects, and server settings.

Core Concepts

Projects

Projects are the top-level organizational unit. Each project contains one or more **Containers** (design files). Access permissions are configured at the project level using role-based assignments.

Containers

A container holds a versioned design - typically a PCB board, schematic, or multi-board panel. Containers track full version history and support check-out/check-in workflows.

Version Control

EEforce uses a lock-based version control model:
- **Check out** a design to begin editing (locks it for other users)
- **Check in** to upload changes as a new version
- **Cancel check-out** to discard changes and release the lock

Access Control

Projects use role-based access with three levels:
- **Viewer** - read-only access
- **Contributor** - can check out and check in designs
- **Manager** - full control including member management

See Access Model for complete details.

Key Features

- **Seamless integration** with Xpedition and PADS Professional design tools
- **Built-in previews** for PCB layout, schematics, stack-up, and BOM
- **Role-based access control** with per-project granularity
- **Unlimited version history** for all design files
- **Remote working** support with export/import packages
- **LDAP/Active Directory** integration with group synchronization
- **SSO** support via external identity providers
- **Low resource footprint** - minimal CPU and memory usage
- **Web-based administration** - no need to install tools on the server

Supported Design Tools

Tool	Versions
Siemens Xpedition	All VX versions, 2409, 2504, 2604
Siemens PADS Professional	All versions

> Any file type can be stored using **Folder containers**, but seamless editor integration (open, preview, BOM extraction) is available only for Xpedition and PADS Professional designs.

What's Next

- Server Installation - Set up the EEforce server
- Client Installation - Install and configure the desktop client
- Release Notes - See what's new in this version

Release Notes - Version 26.9

Scheduled LDAP Group Sync

This release introduces a small change over how we sync the LDAP groups.

On every login of an LDAP user, EEforce Server was fetching user's group memberships from the LDAP Server. EEforce Server was also fetching members of a certain group from the LDAP Server manually. We have received information from customers that these two fetches are returning different results and causing some users to be removed from group.

While this can be an isolated configuration issue with LDAP Server, we see an opportunity in it to improve the robustness of our system.

With this patch version, we have changed how the LDAP group sync is working. - We removed login triggered user based fetch is removed. - We added a scheduler to sync all groups (equivalent to clicking Sync LDAP Members) that is possible to set to work on everh 30 minutes, every hour, ever 4 hours and once in a day. - When a LDAP user added, Sync is triggered automatically. - It's also possible to trigger full sync from LDAP Settings page in the Web Administration.

Server Installation and Configuration

Prerequisites

Requirement	Details
OS	Windows Server 2022/2025 (Core, Essentials, Data Center) or Windows 10/11 (LTSC, Pro, Enterprise)

Requirement	Details
CPU	4+ vCPUs recommended
RAM	4 GB free when idle (minimum)
Storage	20 GB+ on local disk; NVMe/SSD recommended
Swap	4 GB recommended
Network	Reliable LAN between server and clients
License	Valid license file prepared for this machine
Backup	Windows shadow copy or equivalent backup solution

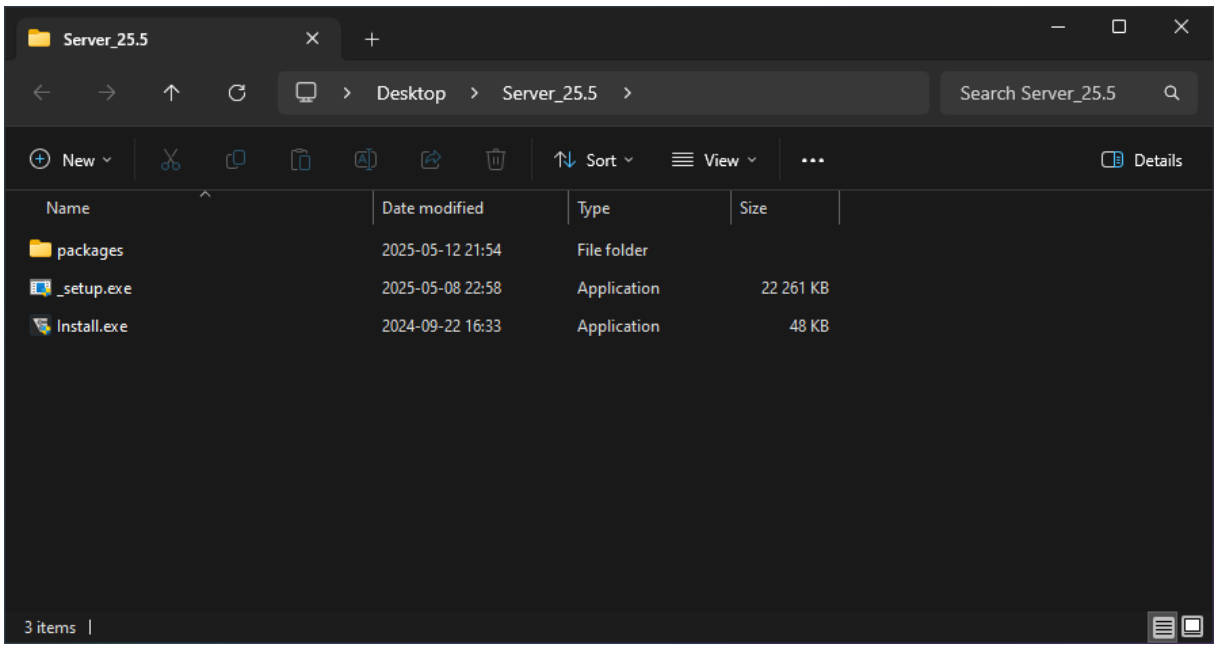
Using network-attached storage for the vault is supported but may reduce check-in/check-out performance. If used, ensure the IIS application pool identity has full read/write permissions on the network path.

Installation

Step 1 - Download and Extract

1. Download the latest server package from the Support Portal. The file is named `Server_XX.X.zip` (version numbers vary).

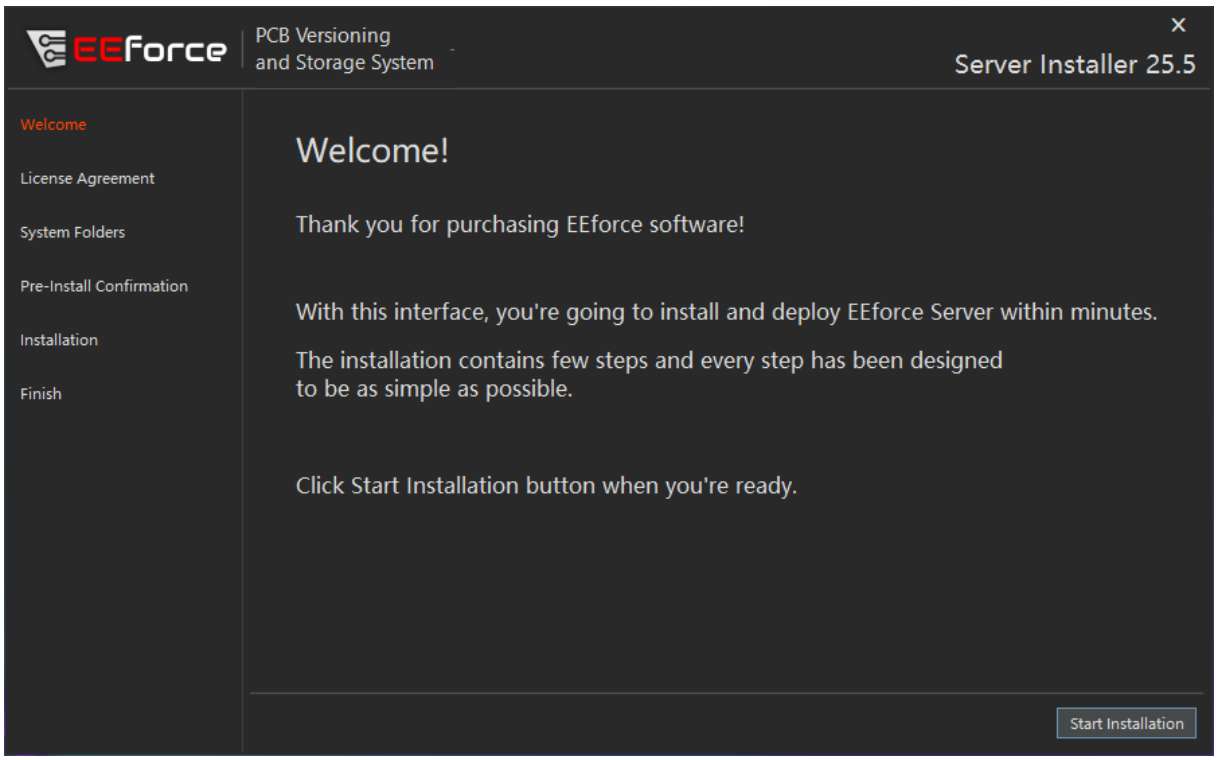
2. Extract the ZIP to a convenient folder.



Step 2 - Run the Installer

1. Run **Install.exe**. Grant administrator permissions if prompted by Windows.

2. The welcome screen appears:



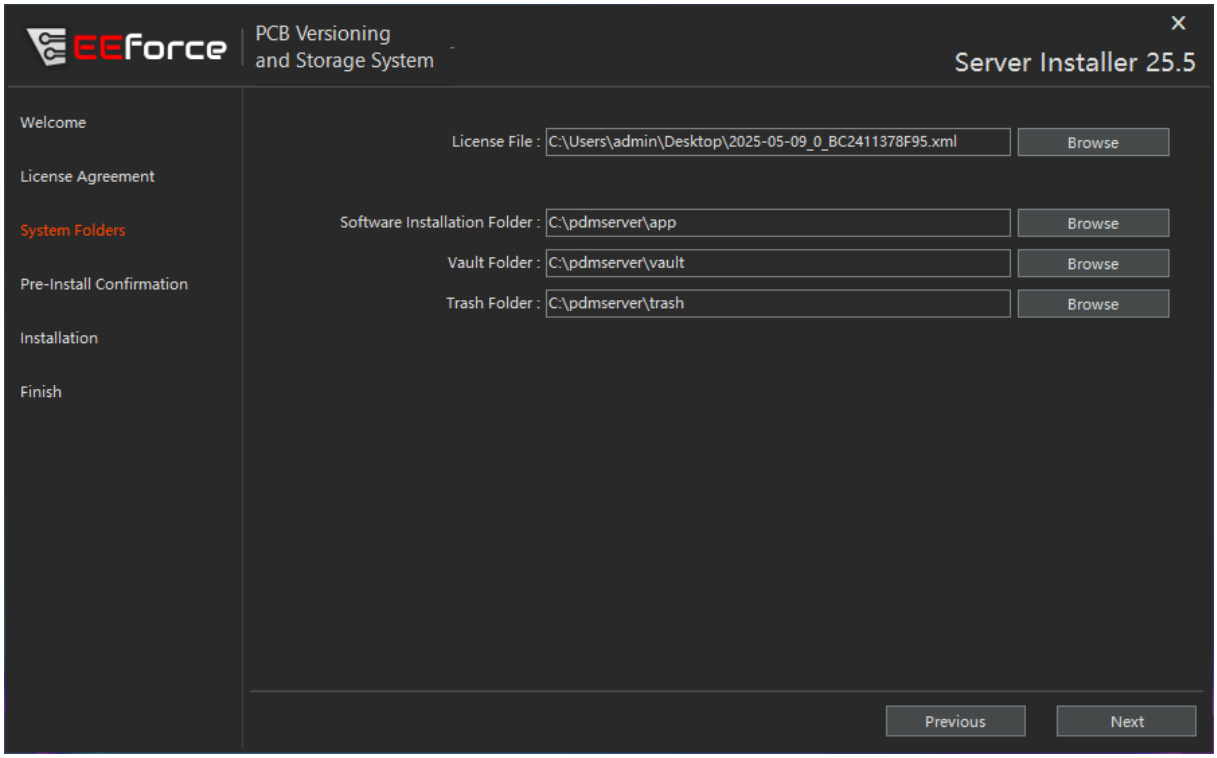
3. Click **Start Installation**.

Step 3 - Accept the License Agreement

Read the End User License Agreement and click **I Agree** to proceed.

Accepting the EULA is a legally binding action.

Step 4 - Configure Paths



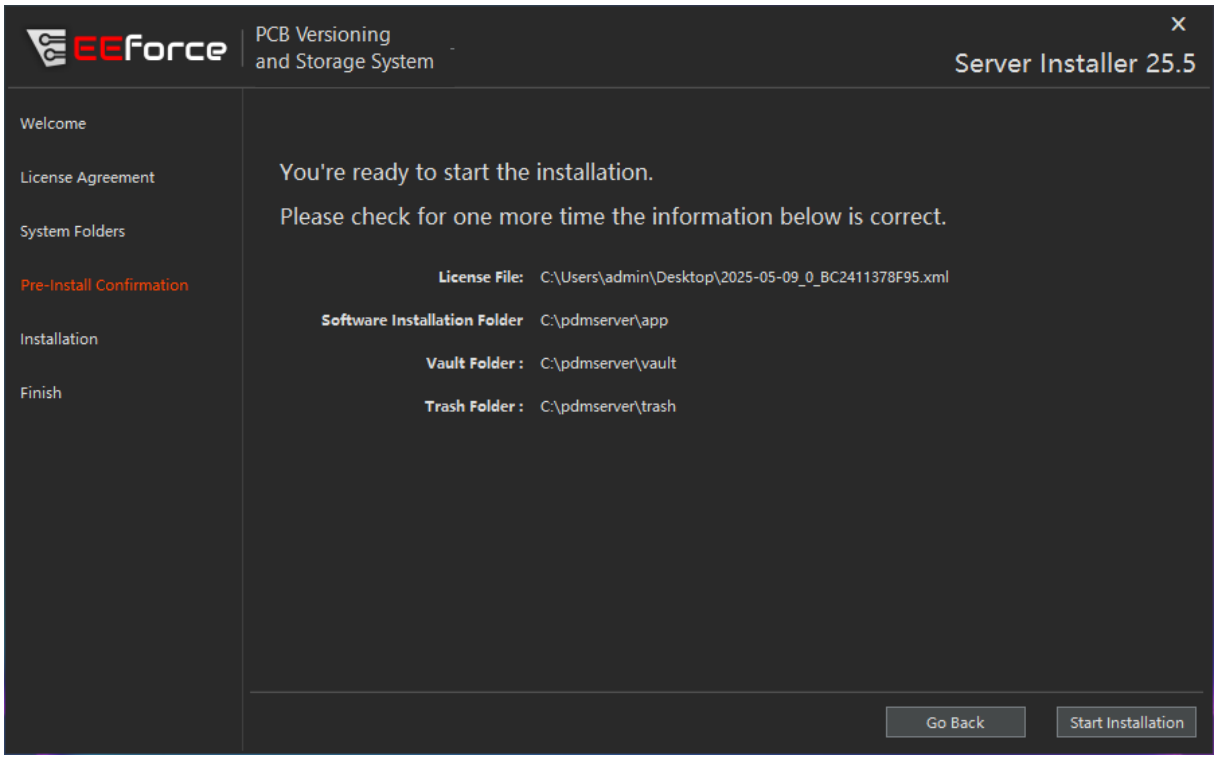
Field	Purpose	Notes
License File	Authorizes the software to run on this machine	Obtain from your reseller
Software Installation Folder	Stores executables	Local drive; ~150 MB required
Vault Folder	Stores design files	20 GB+ minimum; back up regularly
Trash Folder	Holds deleted designs before permanent removal	5 GB+; clean manually as needed

The Trash folder is a safety net - deleted projects are moved here rather than permanently erased. Schedule periodic cleanups to reclaim disk space.

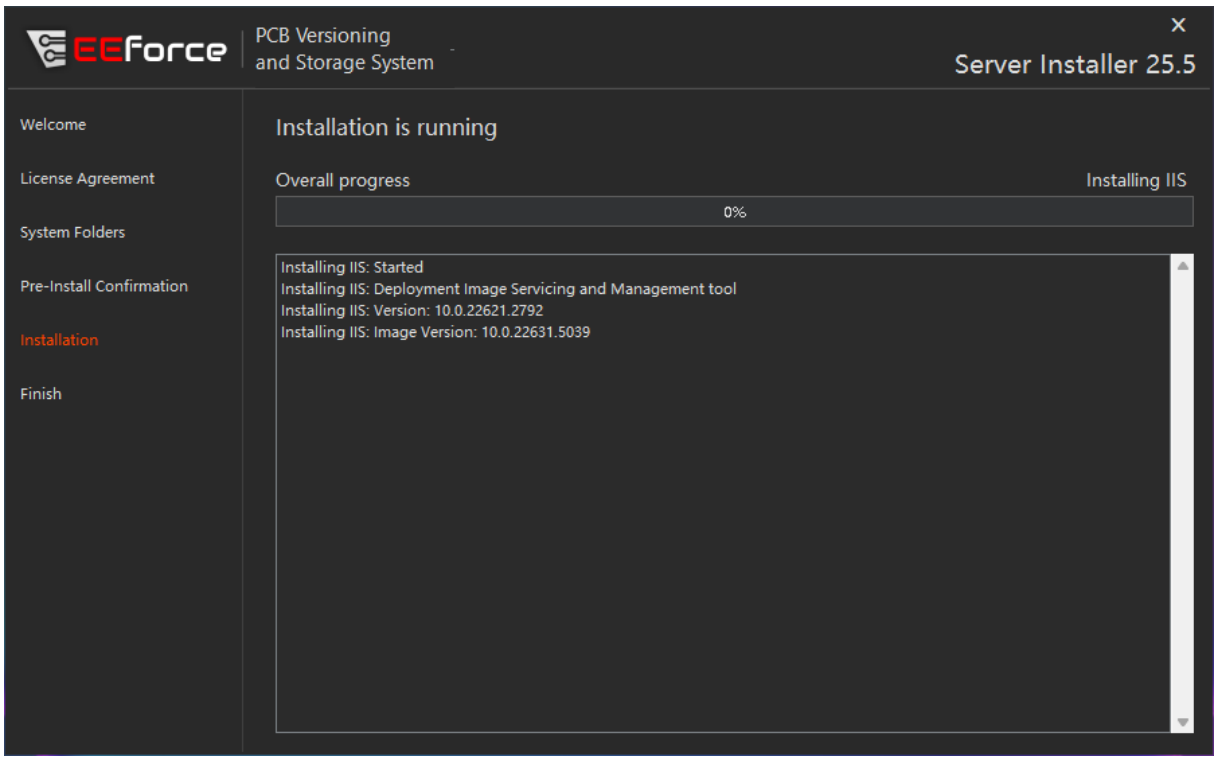
Click **Next** when all fields are filled.

Step 5 - Confirm and Install

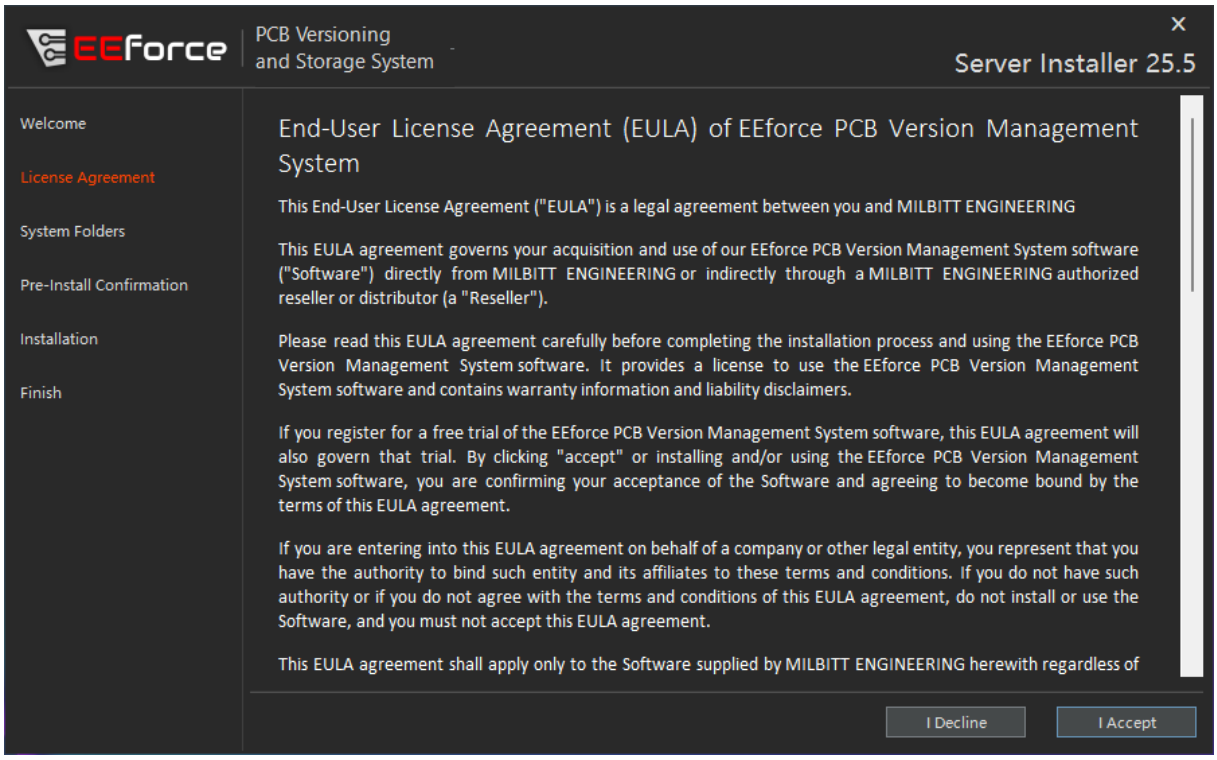
Review the summary screen:



Click **Start Installation**. The installer will: - Create required folders
- Install Windows prerequisites
- Deploy and configure the IIS application



Step 6 - Complete



Note the **server address** shown on the completion screen - you will need it to configure clients.

Starting and Stopping the Server

The EEforce server runs as an IIS (Internet Information Services) application pool.

Using IIS Manager (GUI)

1. Open IIS Manager: press `Win + R`, type `inetmgr`, press Enter.
2. In the left panel, expand your server name -> **Application Pools**.
3. Locate **EEForceApplicationPool**.
4. Right-click -> **Start** or **Stop**.

Using PowerShell

```
# Start the server
Start-WebAppPool -Name "EEForceApplicationPool"

# Stop the server
Stop-WebAppPool -Name "EEForceApplicationPool"
```

Stopping the application pool makes EEforce unavailable to all users until it is started again. Ensure all users have completed their work before stopping.

Post-Installation Configuration

config.json

Server paths are defined in `config\config.json` inside the installation directory:

```
{
  "Configurations": {
    "VaultFolder": "C:\\pdmserver\\vault",
    "TrashFolder": "C:\\pdmserver\\trash"
  }
}
```

Edit this file with any text editor to relocate the vault or trash folder. **Restart the server** after making changes.

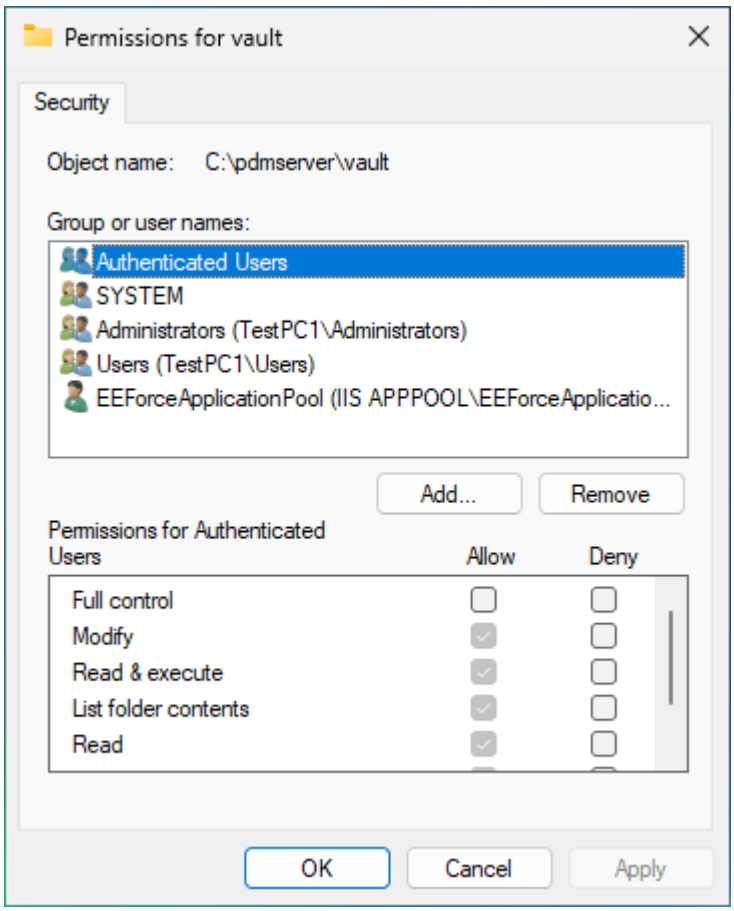
Relocating Storage

1. Stop the EEforce server (see above).
2. Move the vault folder to the new location.
3. Update `config.json` with the new path.
4. Set permissions on the new folder (see below).
5. Start the server.

Setting Folder Permissions

If you use a network drive or relocate storage, grant the IIS application pool identity full control:

- Identity: `IIS_APPPOOL\EEForceApplicationPool`
- Permissions: **Full Control** on vault and trash folders



SSL/TLS Configuration

EEforce does not manage SSL certificates directly. SSL termination is handled by IIS:

1. Obtain a certificate from a trusted CA (or create a self-signed certificate for testing).
2. Import the certificate into the server's certificate store.
3. In IIS Manager, bind the certificate to the EEforce site on port 443.

> If using a self-signed certificate, install it on all client machines to avoid connection errors.

Troubleshooting

Symptom	Possible Cause	Resolution
Clients cannot connect	Firewall blocking port	Open port 8000 (or your configured port) in Windows Firewall
“Access denied” on vault operations	Incorrect folder permissions	Verify IIS_APPPOOL identity has Full Control
Server won’t start after path change	Invalid path in config.json	Check path exists and is accessible
Slow check-in/check-out	Network storage latency	Move vault to local NVMe/SSD or ensure fast network path

Client Installation and Configuration

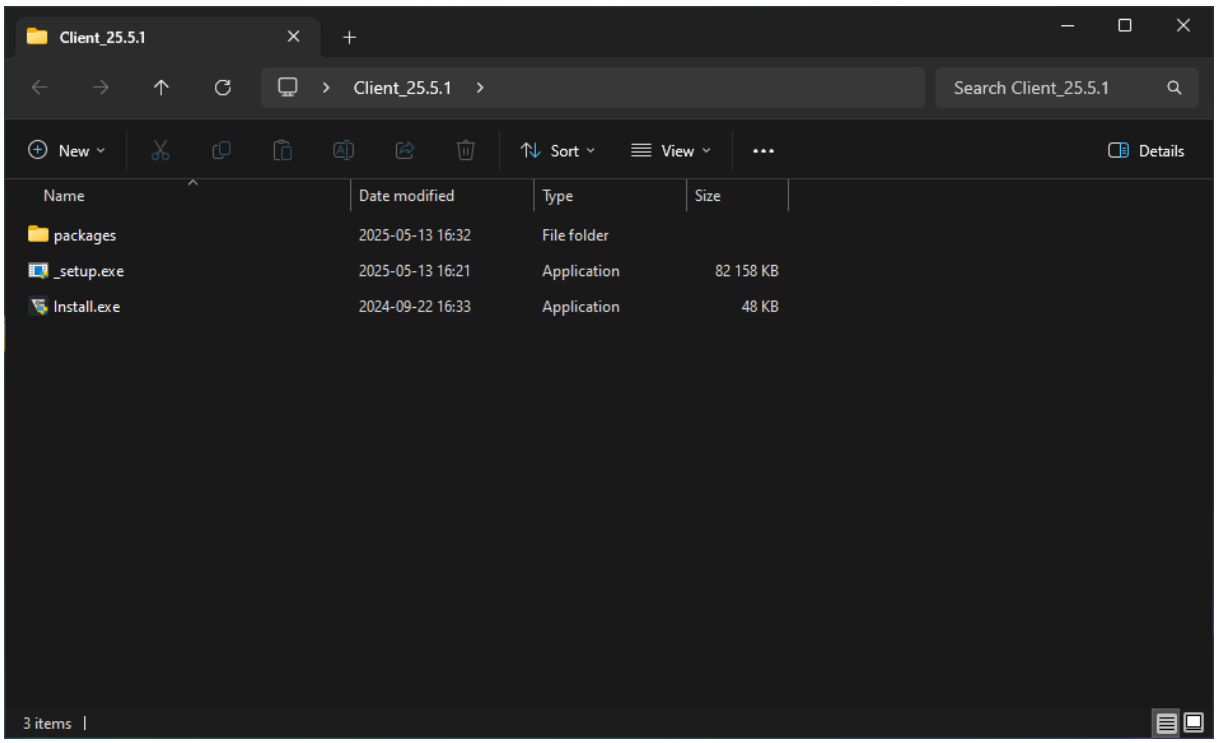
Prerequisites

Requirement	Details
OS	Windows 10 x64 or Windows 11 x64
Privileges	Administrator access (for installation only)
Storage	4 GB+ free disk space; SSD recommended
Network	Stable connection to the EEforce server

Installation

Step 1 - Download and Extract

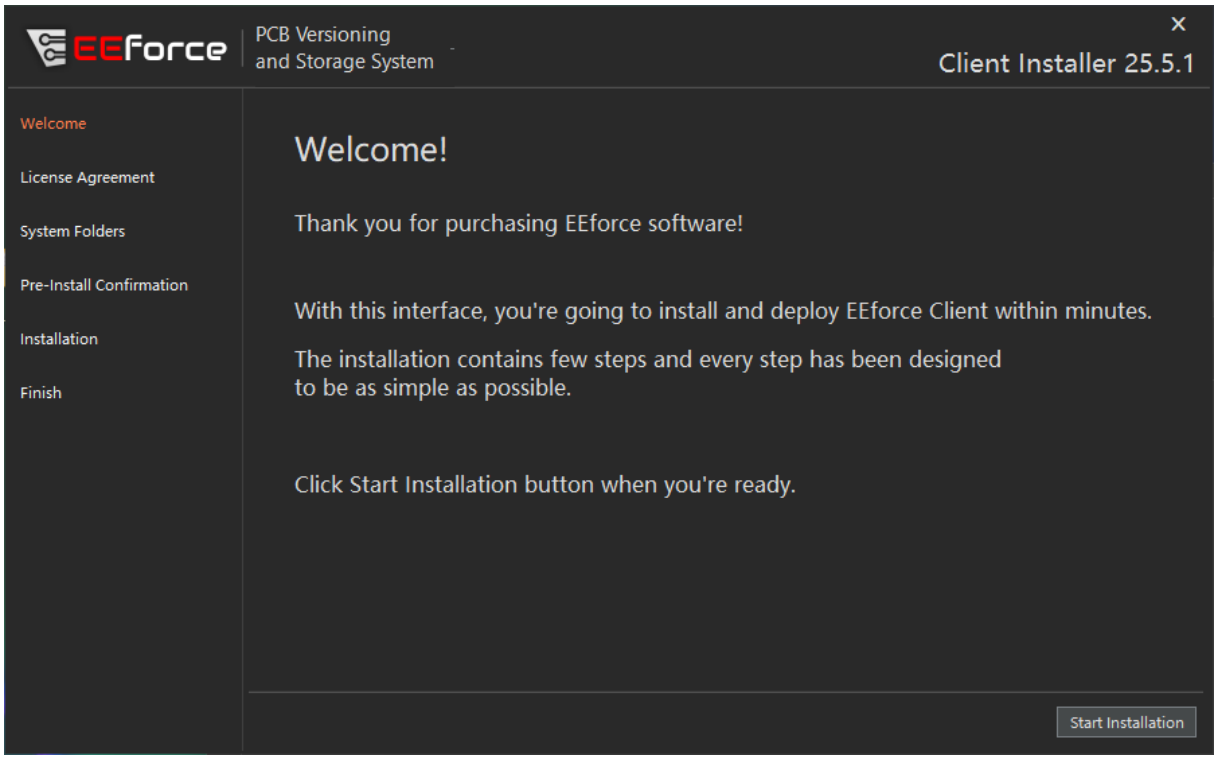
Download the client package from the Support Portal or obtain it from your IT department. Extract the ZIP file.



Step 2 - Run the Installer

Run **Install.exe**. Grant permissions if prompted. The installer checks for required runtimes and installs any that are missing.

Step 3 - Welcome Screen

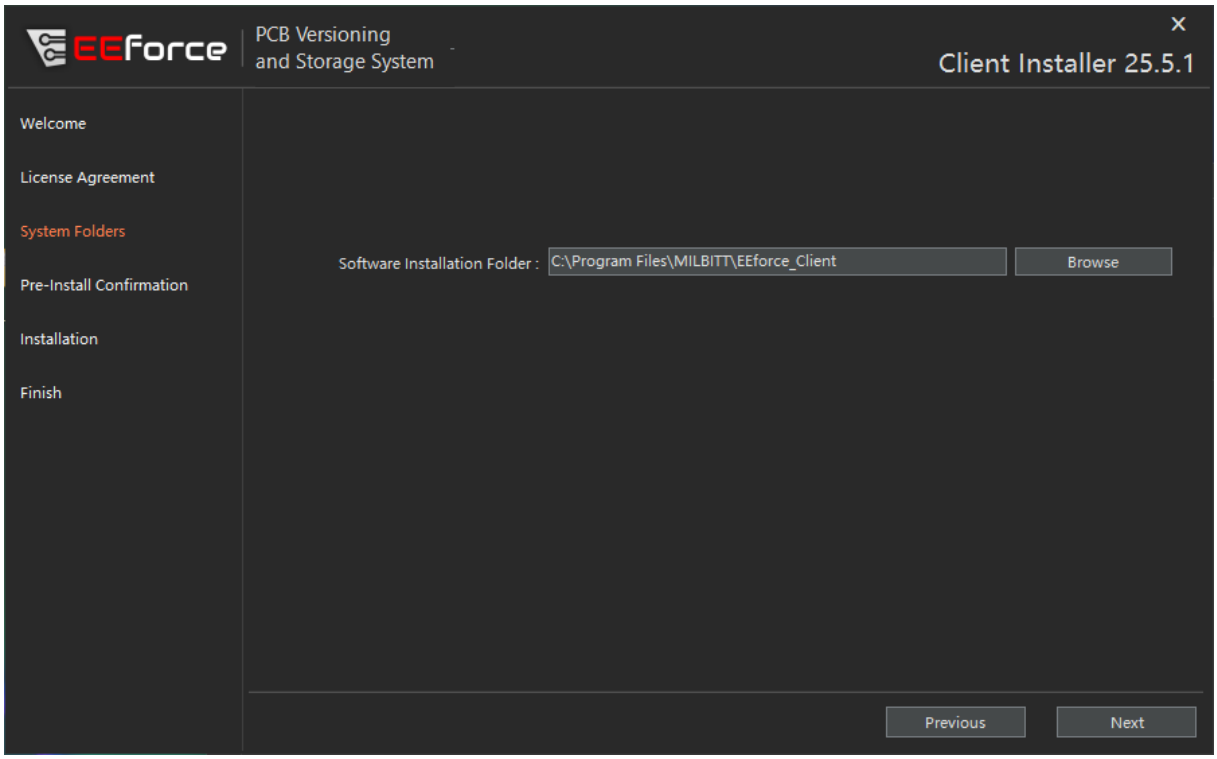


Click **Start Installation**.

Step 4 - License Agreement

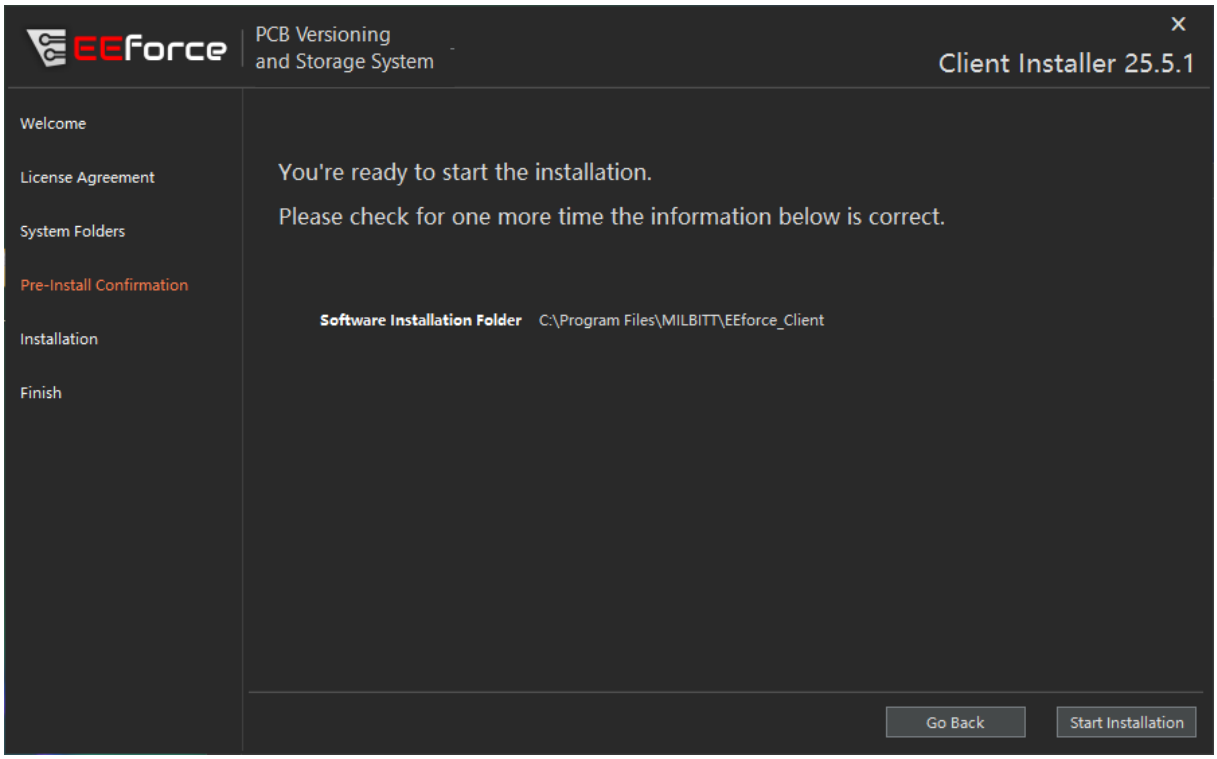
Read the End User License Agreement and click **I Agree**.

Step 5 - Choose Installation Folder

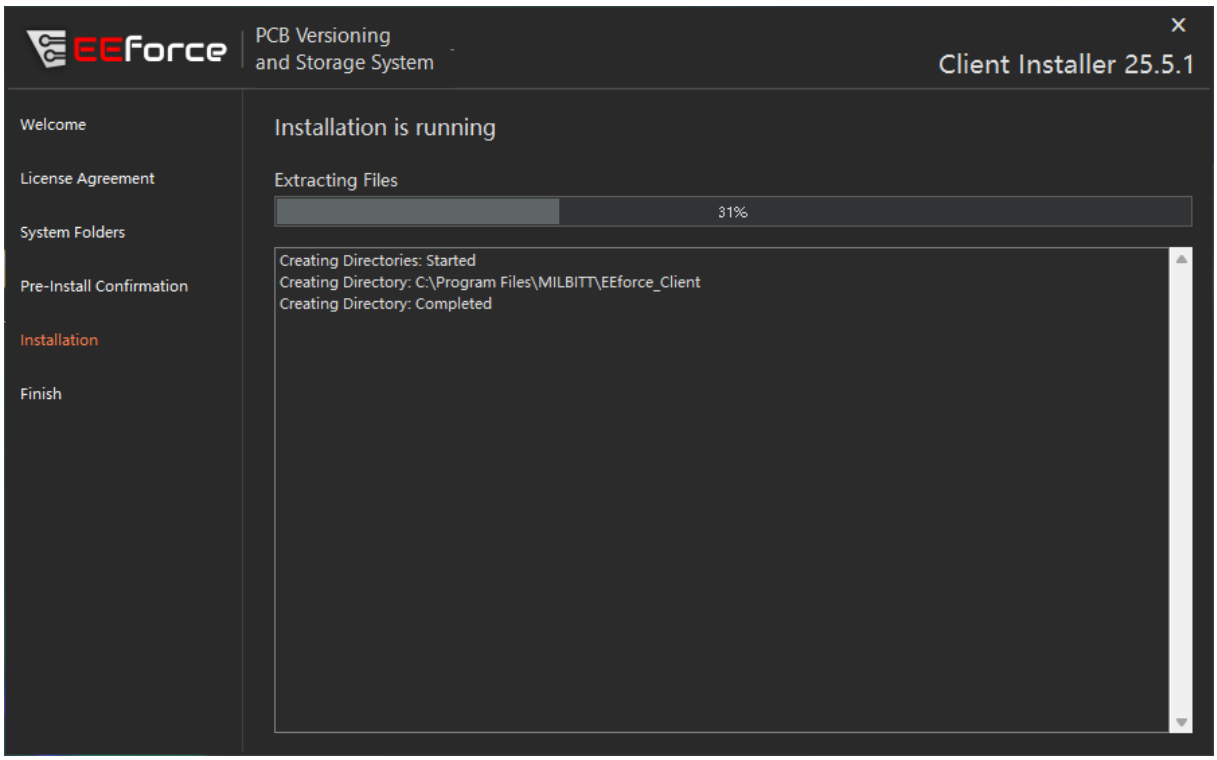


The default location is recommended. Required space is under 50 MB. Click **Next**.

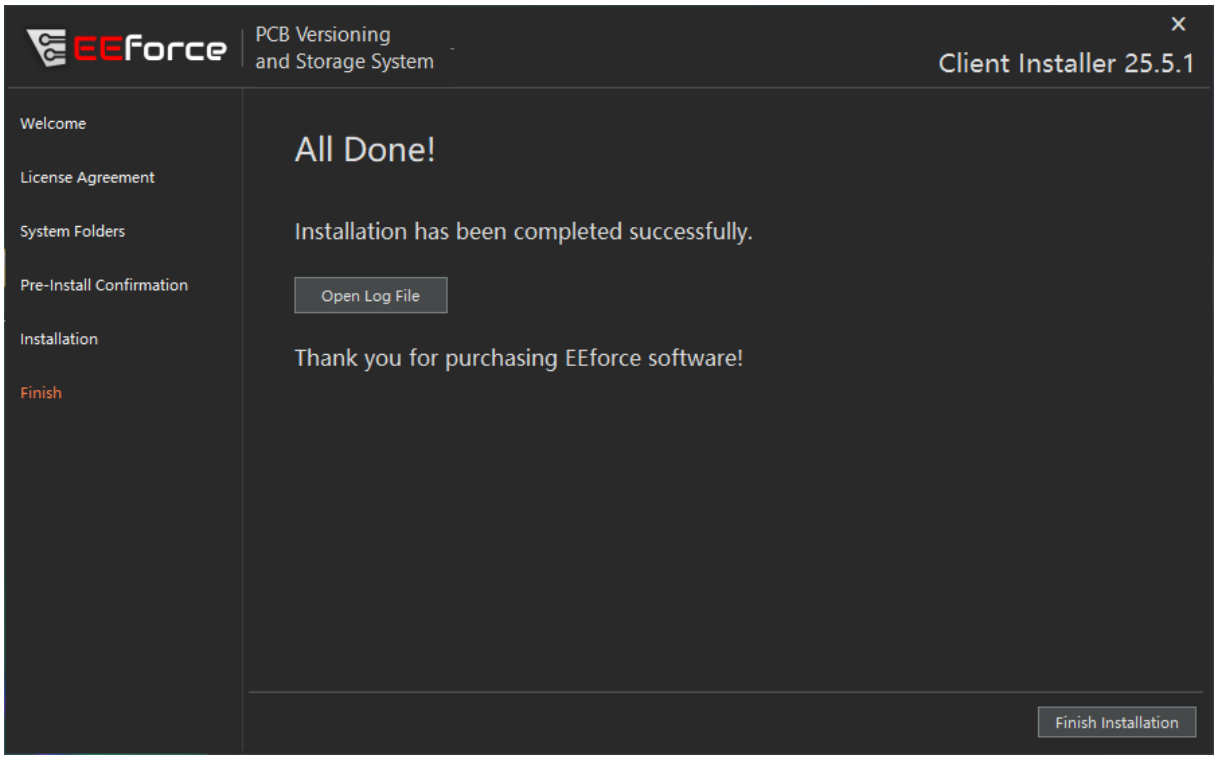
Step 6 - Confirm and Install



Verify the path and click **Start Installation**.



Step 7 - Complete



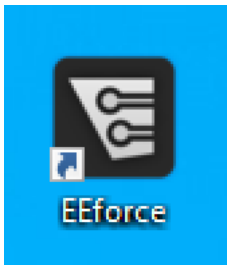
Click **Finish Installation**. The EEforce icon will appear on your desktop.

First Run

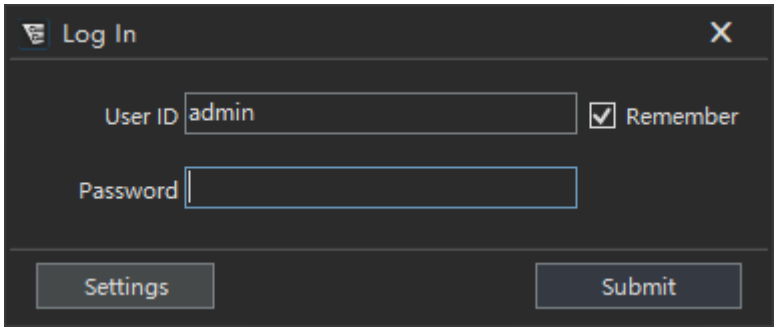
After installation, the client needs to be pointed at your server.

Connect to Server

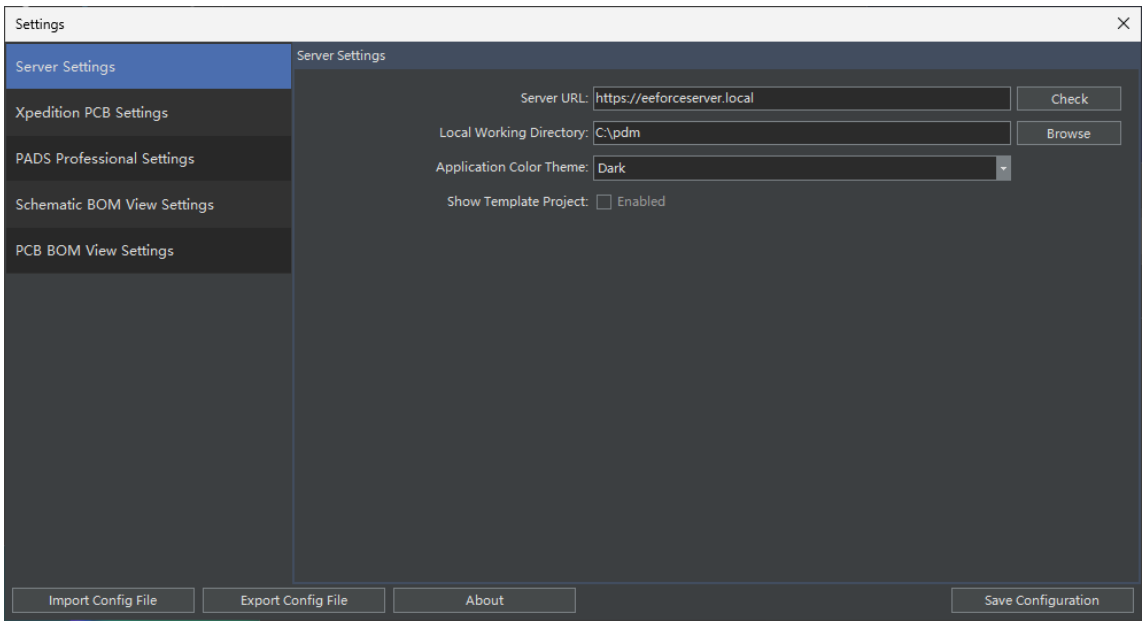
1. Launch EEforce from the desktop icon.



2. The login dialog appears. Click **Settings**.



3. Enter the **Server URL** provided by your administrator and click **Save Configuration**.



::: info Local Testing If the server is installed on your local machine, use `http://localhost:8000` as the Server URL. :::

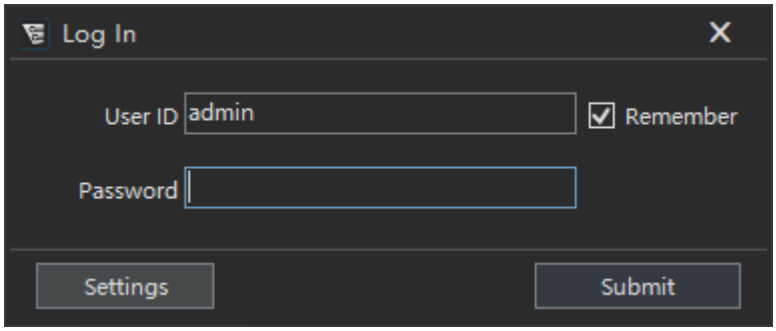
Log In

Return to the login dialog and enter your credentials.

::: details Default Admin Credentials (first-time setup only)

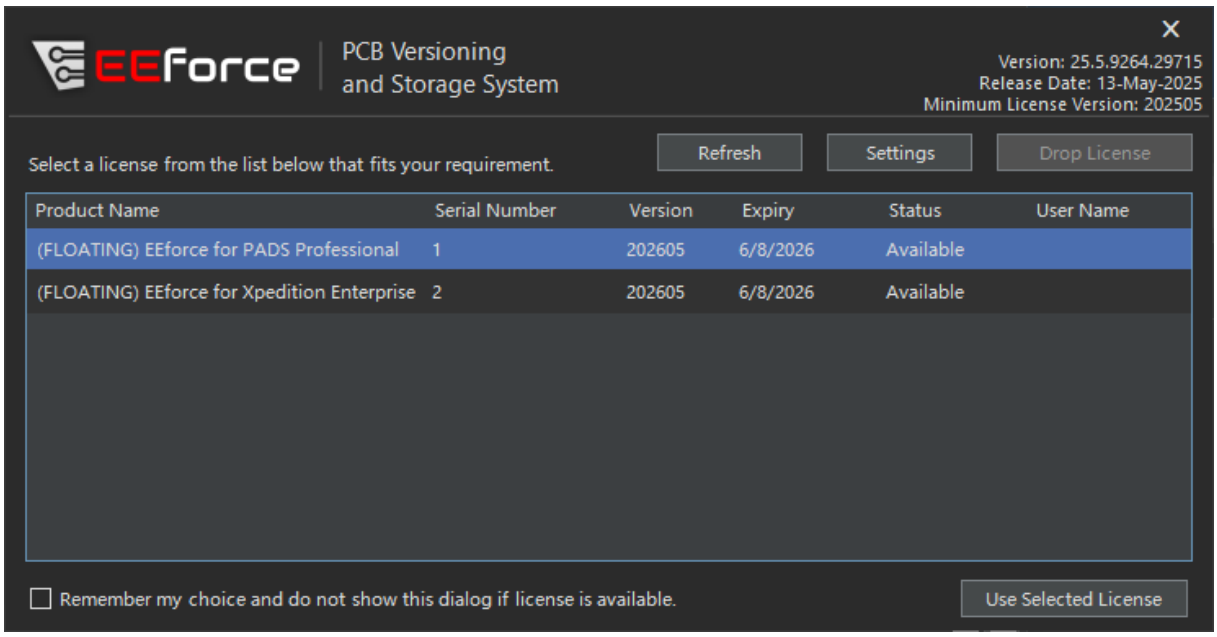
```
User ID:  admin
Password: Passw0rd
```

Change this password immediately after first login. :::

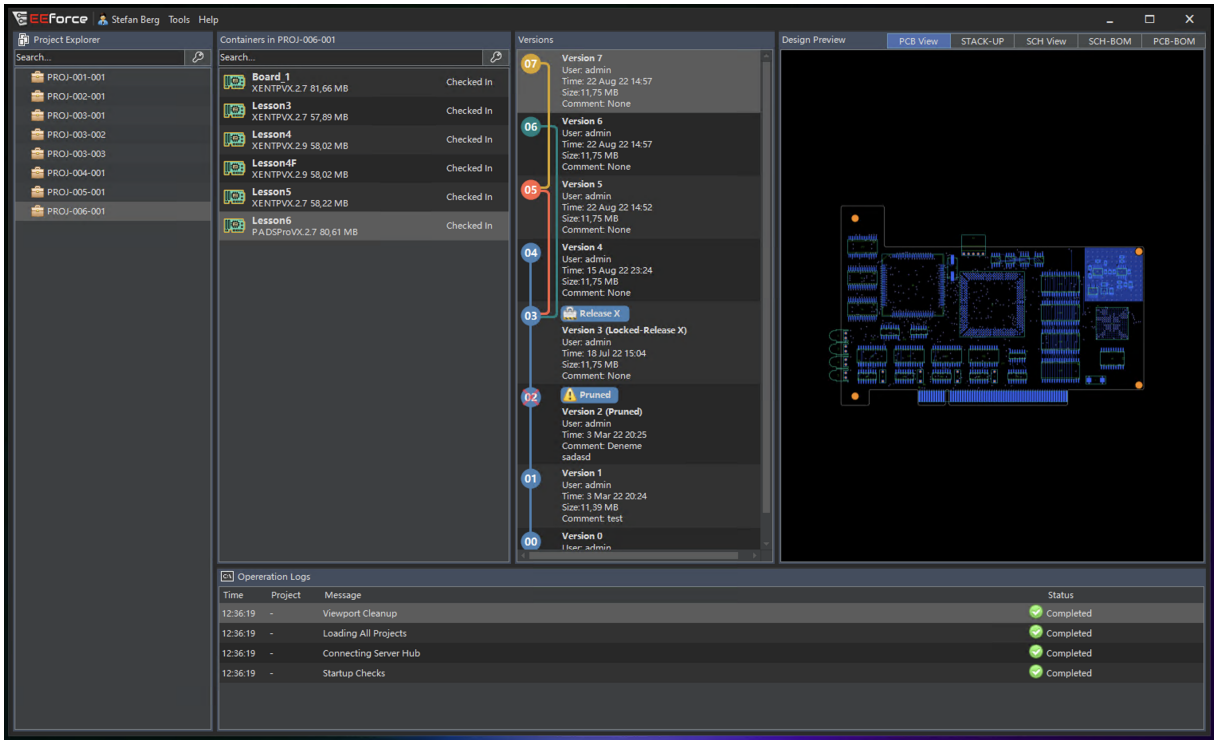


Select a License

After successful login, the license selection window appears:

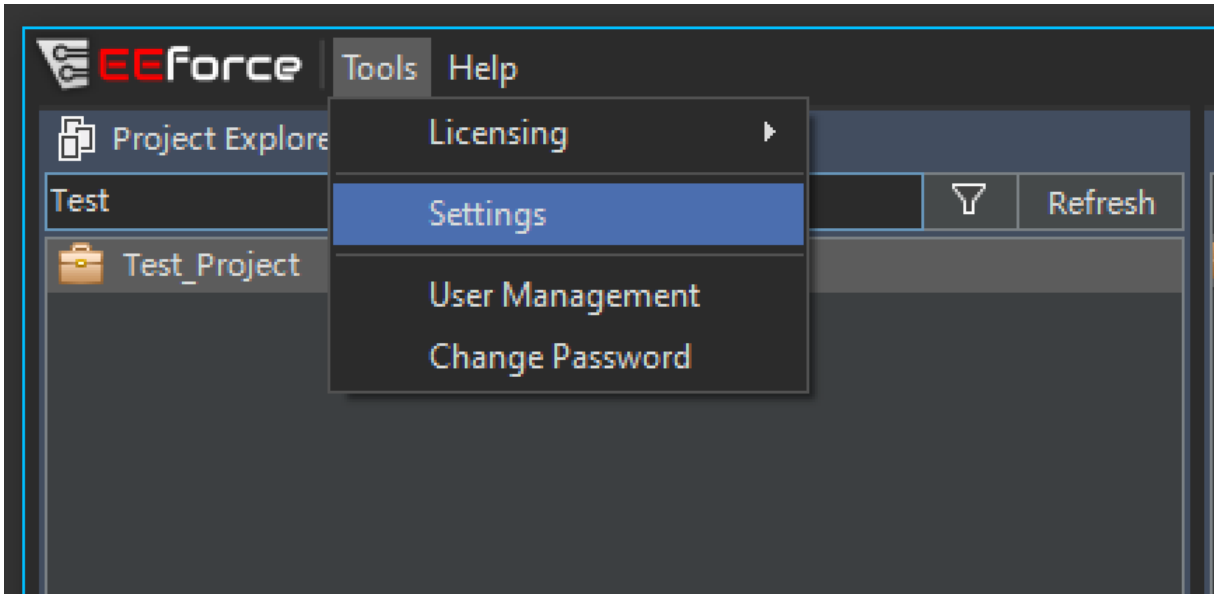


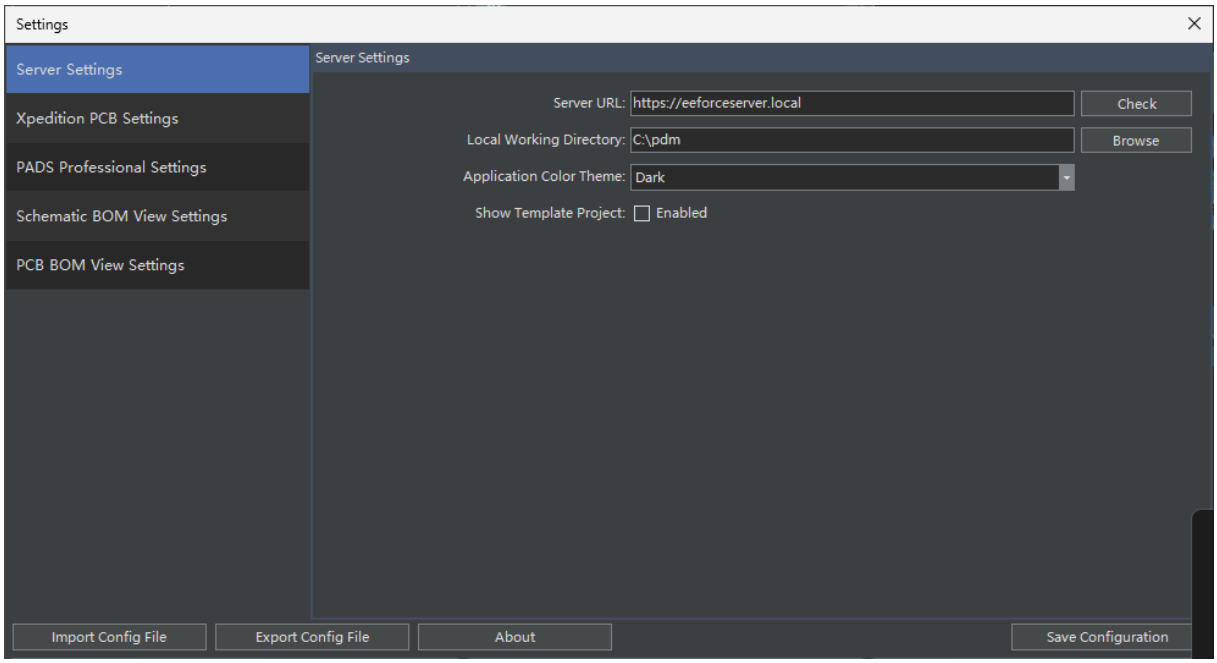
Select an available license and click **Use Selected License**. The main interface loads:



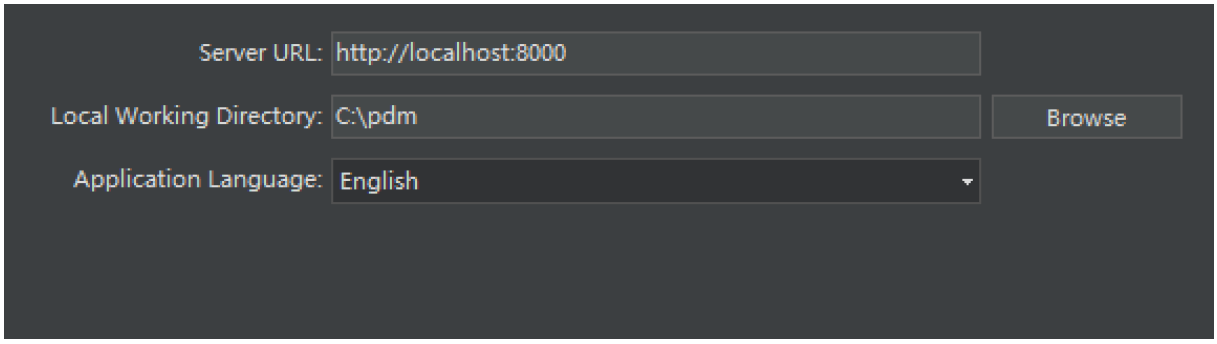
Configuration

Open **Tools -> Settings** to access all configuration pages.



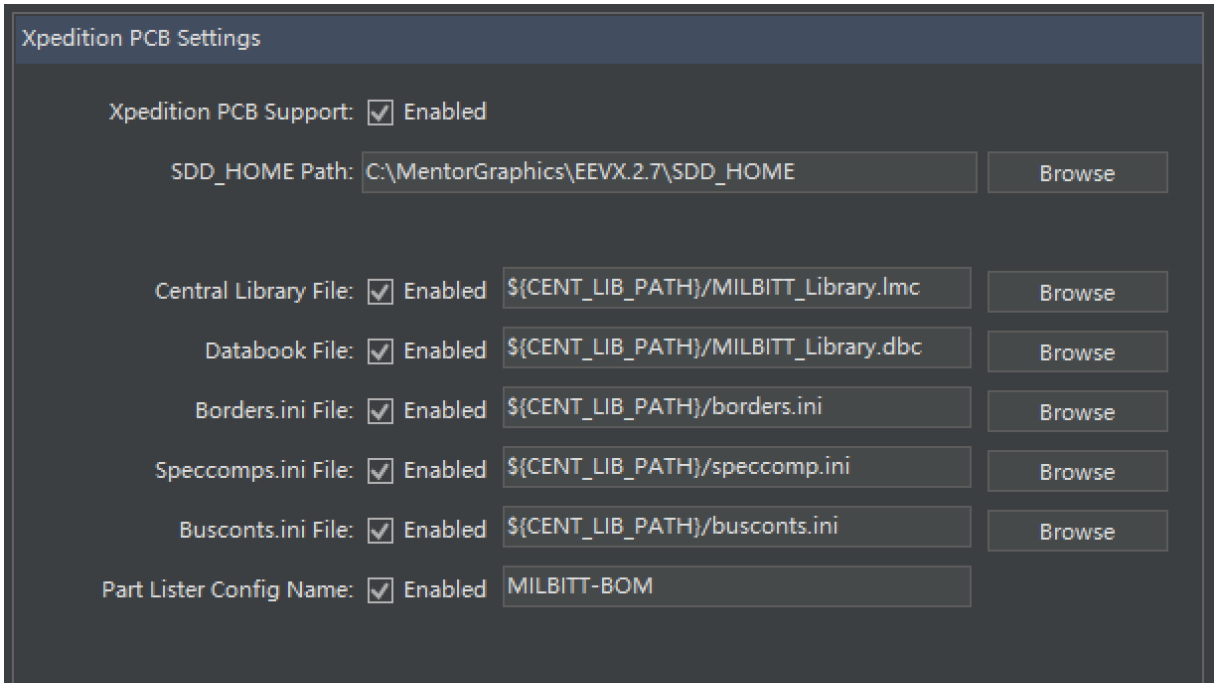


Server Settings



Setting	Purpose
Server URL	Connection address for the EEforce server
Local Working Directory	Root folder for checked-out designs and local caches. Default: `C:\pdm`
Chunked Uploads	Split large uploads into smaller pieces for reliability on slow networks
Application Language	UI language
Application Theme	Dark or Light theme

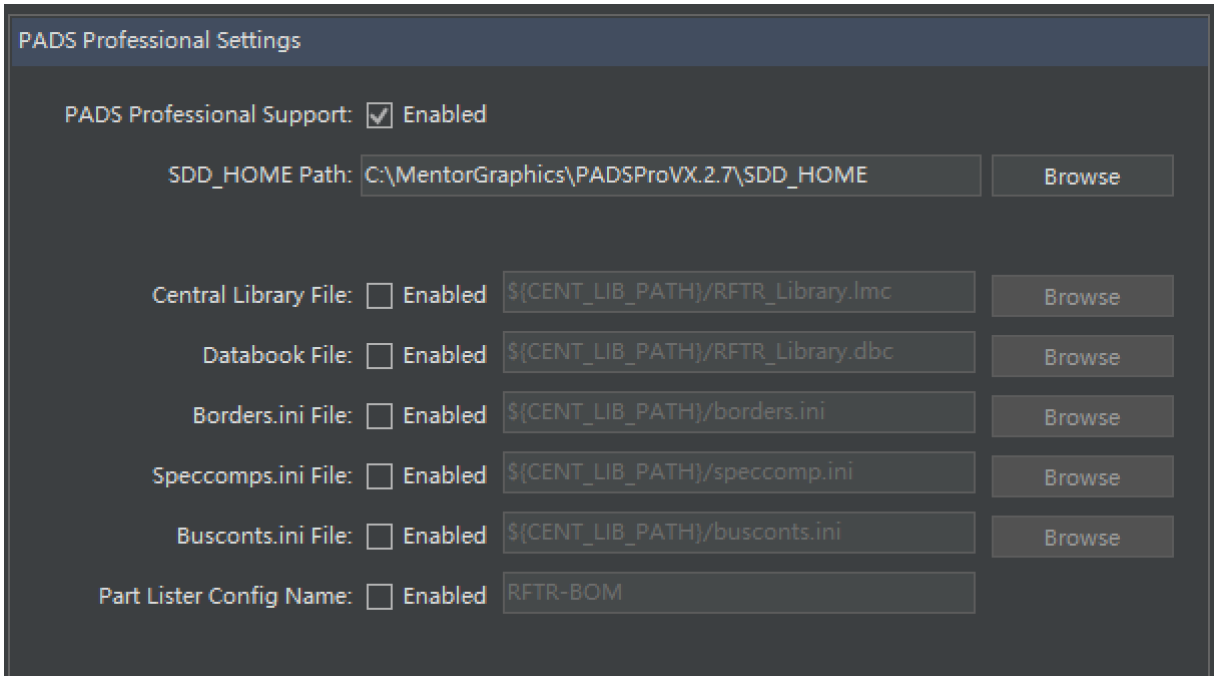
Xpedition Settings



Setting	Purpose
Xpedition PCB Support	Enable/disable Xpedition integration
SDD_HOME Path	Path to your Xpedition installation (SDD_HOME directory)
Central Library File	Override the CL path in PRJ files (optional)
Databook File	Override the Databook path in PRJ files (optional)
Borders.ini File	Override Borders.ini path (optional)
Speccomps.ini File	Override Speccomps.ini path (optional)
Busconts.ini File	Override Busconts.ini path (optional)
Part Lister Config Name	Override Part Lister configuration (optional)

Path overrides support EEforce variables (e.g., `%EXP_CENT_LIB_PATH%/Library.lmc`) for portability across machines.

PADS Professional Settings

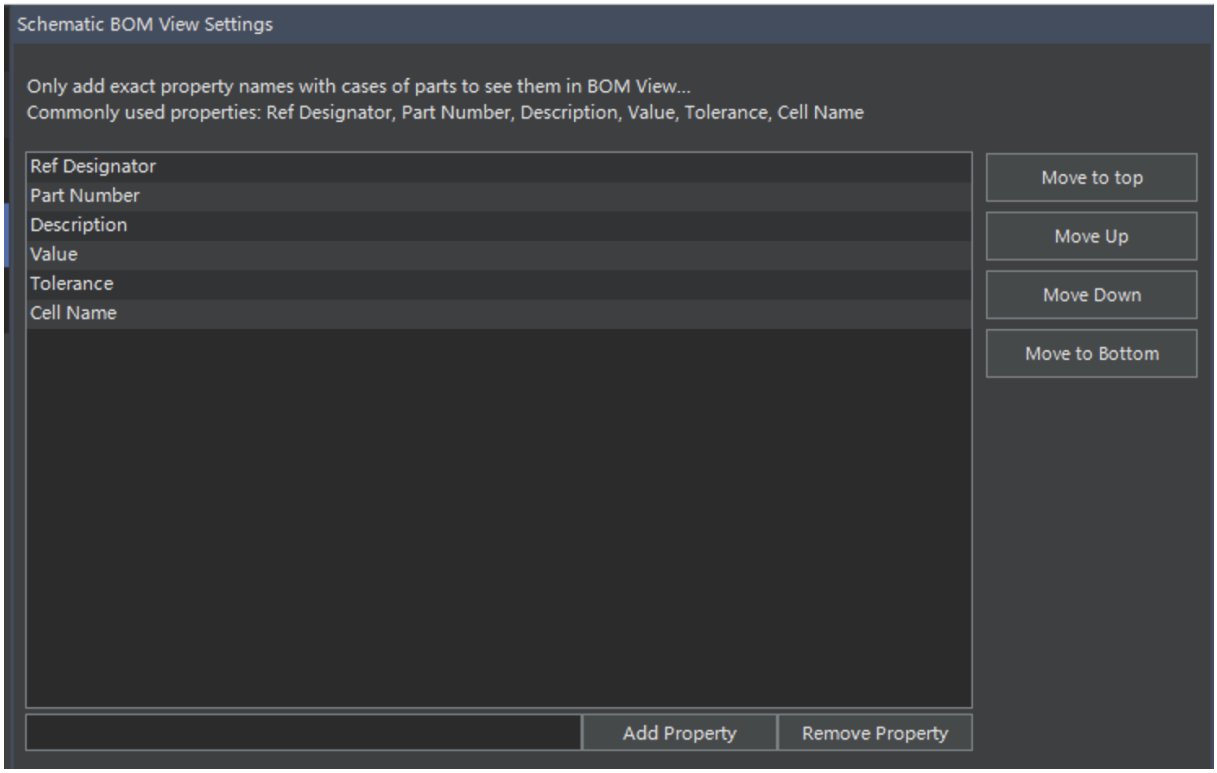


The same override options as Xpedition are available for PADS Professional installations.

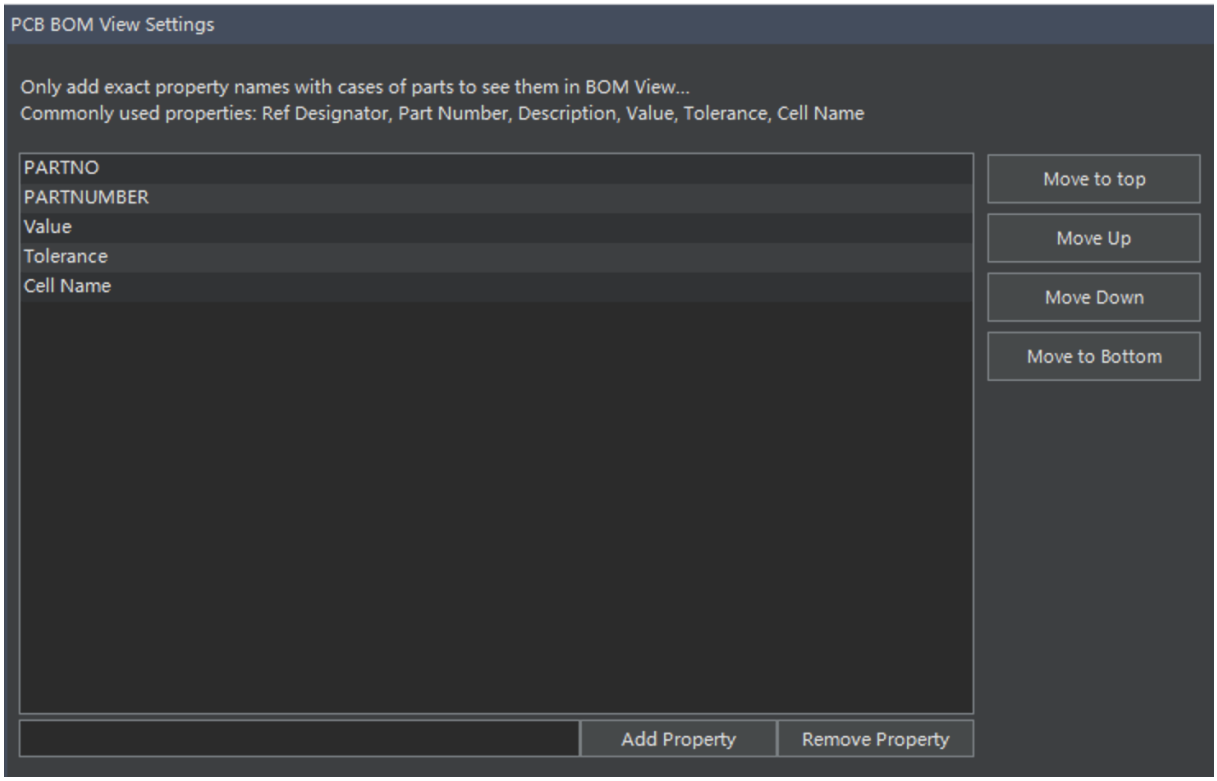
BOM Preview Settings

Configure which parameters appear in the built-in BOM previews:

Schematic BOM:


Schematic BOM View Settings
Only add exact property names with cases of parts to see them in BOM View...
Commonly used properties: Ref Designator, Part Number, Description, Value, Tolerance, Cell Name
Ref Designator
Part Number
Description
Value
Tolerance
Cell Name
Move to top
Move Up
Move Down
Move to Bottom
Add Property
Remove Property

PCB BOM:


PCB BOM View Settings
Only add exact property names with cases of parts to see them in BOM View...
Commonly used properties: Ref Designator, Part Number, Description, Value, Tolerance, Cell Name
PARTNO
PARTNUMBER
Value
Tolerance
Cell Name
Move to top
Move Up
Move Down
Move to Bottom
Add Property
Remove Property

- Add or remove parameter columns
- Drag to reorder columns

Troubleshooting

Symptom	Resolution
“Cannot connect to server”	Verify Server URL in Settings; check network/firewall
No licenses available	Confirm license file is installed on server; check license type matches your tool
Xpedition designs won’t open	Verify SDD_HOME path points to a valid Xpedition installation
Slow file transfers	Enable chunked uploads in Server Settings; check network quality

Licensing

EEforce requires a valid license to operate. Licenses are issued as XML files, stored on the server, and distributed to clients on demand.

How Licensing Works

- Server holds license file.
- User launches Client - requests available licenses.
- Server presents matching, unreserved licenses.
- User selects a license - server locks it for that session.
- User closes Client - license is released for others.

A license is consumed only while the client software is running. Closing the application releases the license immediately.

License Dimensions

Duration

Type	Description
Perpetual	Use the software indefinitely. Includes one year of upgrades and support.
Term (Subscription)	Use the software for a fixed period, typically one year. Includes upgrades and support for the term duration.

Binding

Type	Description
Floating	Can be used on any machine in the network. Shared among users up to the seat count.
Node-Locked	Tied to a specific machine. Only usable on that computer.

Tool Tier

Tier	Covers
PADS Professional	PADS Professional designs only
Xpedition + PADS Professional	Both Xpedition and PADS Professional designs
Xpedition (Standard/Advanced)	Xpedition Standard and Advanced editions

::: tip Choosing a Tier If your team uses only PADS Professional, the PADS-only tier is more economical. If anyone uses Xpedition, select the Xpedition tier - it includes PADS Professional support. :::

License Upgrades

A Perpetual license includes **one year** of upgrades and support from purchase date.

- During the active period: access all new versions released.
- After expiration: continue using the last version released during your active period, but cannot upgrade to newer releases.
- To restore upgrade access: purchase a License Upgrade package for an additional year.

Managing Licenses

Licenses are managed on the server:

1. Place the license XML file on the server (location configured during installation or via `config.json`).
2. Restart the server if adding a license while running.
3. Clients will see available licenses on next login.

Troubleshooting

Issue	Resolution
"No licenses available"	All seats are in use ask other users to close their clients, or purchase additional seats
License not appearing	Verify the XML file is in the correct server directory and the server has been restarted
Wrong tool tier shown	Check that your license file matches your installed design tools
License expired	Contact your reseller to renew or purchase an upgrade package

Frequently Asked Questions

Compatibility

What versions of PADS are supported?

All versions of PADS Professional are supported for seamless integration (check-in/out, preview, BOM extraction).

What versions of Xpedition are supported?

All VX-series versions and newer releases with year/month numbering (e.g., 2409, 2504, 2604).

Can I store non-Professional PADS designs (PADS Standard, Logic, etc.)?

Yes. Use a **Folder container** to store any file type. However, seamless editor integration (one-click open, preview panels) is only available for PADS Professional and Xpedition designs.

Can I store other file types (PDFs, specs, mechanical files)?

Yes. Folder containers accept any file type. They are versioned like design containers but lack tool-specific integration.

Data and Storage

Where is my data stored?

All design data is stored in the **Vault** folder on the server. The vault location is defined during server installation and can be changed in `config.json`.

How are backups handled?

EEforce does not include built-in backup. Use Windows shadow copy, volume snapshots, or a third-party backup solution targeting the vault folder. Schedule daily backups at minimum.

What happens when a design is deleted?

Deleted projects and containers are moved to the **Trash** folder rather than permanently erased. An administrator can recover them by moving files back to the vault, or permanently delete them by clearing the trash.

Networking and Access

Can I access my server over the Internet?

Yes. Two recommended approaches:

1. **VPN** - Connect to your corporate network via VPN, then access the server normally.

2. **Reverse proxy with SSL** - Expose the server through IIS with a valid SSL certificate. Ensure proper firewall rules and authentication.

> Do not expose the server directly to the Internet without SSL and proper access controls.

What ports does EEforce use?

By default, the server listens on port **8000** (HTTP). When configured with SSL in IIS, port **443** is used for HTTPS.

Can multiple users work on the same project simultaneously?

Yes. Multiple users can work on **different containers** within the same project simultaneously. However, a single container can only be checked out by one user at a time (lock-based model).

Licensing

What happens when all license seats are in use?

New users attempting to log in will see “No licenses available.” They must wait for another user to close their client, or the organization can purchase additional seats.

Can I move a node-locked license to a different machine?

Contact your reseller to reissue the license for the new machine.

Troubleshooting

The client shows “Cannot connect to server”

1. Verify the Server URL in **Tools - Settings - Server Settings**.
2. Check that the server is running (IIS application pool is started).
3. Ensure no firewall is blocking the connection port.
4. Try accessing the server URL directly in a browser - you should see the admin login page.

Check-in is slow or fails on large designs

1. Enable **Chunked Uploads** in client settings.
2. Verify network bandwidth between client and server.
3. If using a network-attached vault, consider migrating to local SSD storage.

“Design is locked” but no one is editing

The previous user may have closed their client without checking in. An administrator can force-cancel the check-out from the web admin interface or the client admin menu.

Project Operations

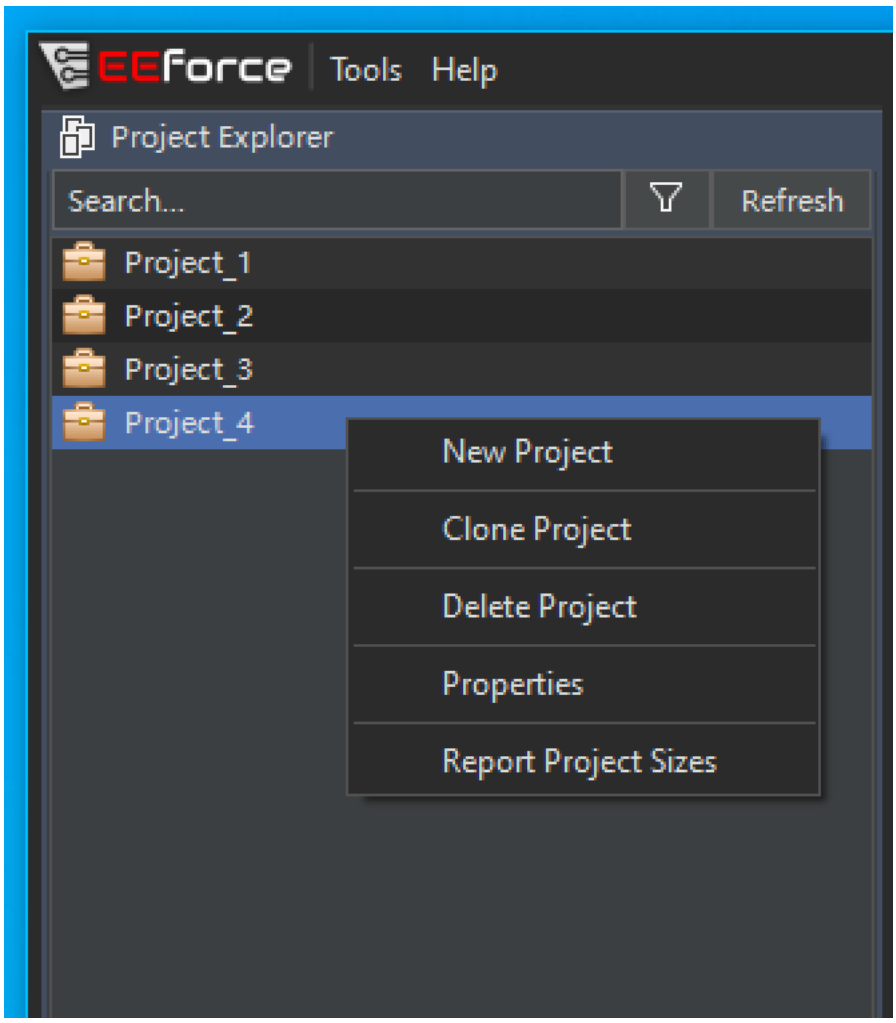
Projects are the top-level organizational unit in EEforce. Each project contains one or more **Containers** (versioned design files) and has its own access control settings.

::: info Naming Rules Project names must follow Windows folder naming conventions: - **Forbidden characters:** < > : " / \ | ? * and control characters (ASCII 031)
- **Reserved names:** CON, PRN, AUX, NUL, COM1``COM9, LPT1``LPT9
- **Cannot** end with a space or period
- Must contain at least one valid character

See Microsoft naming conventions for full details. :::

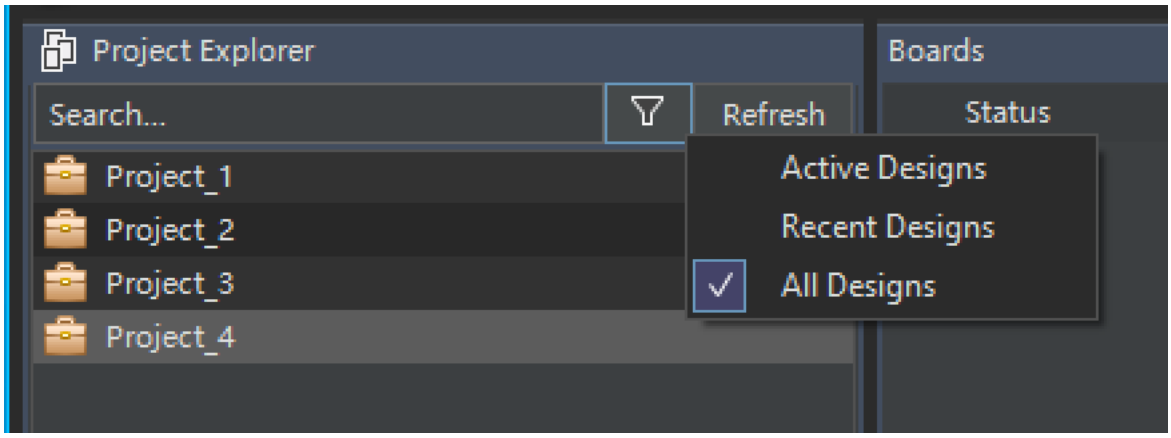
Project Explorer

The Project Explorer panel displays all projects you have access to. It is the starting point for all project operations.



Filtering Projects

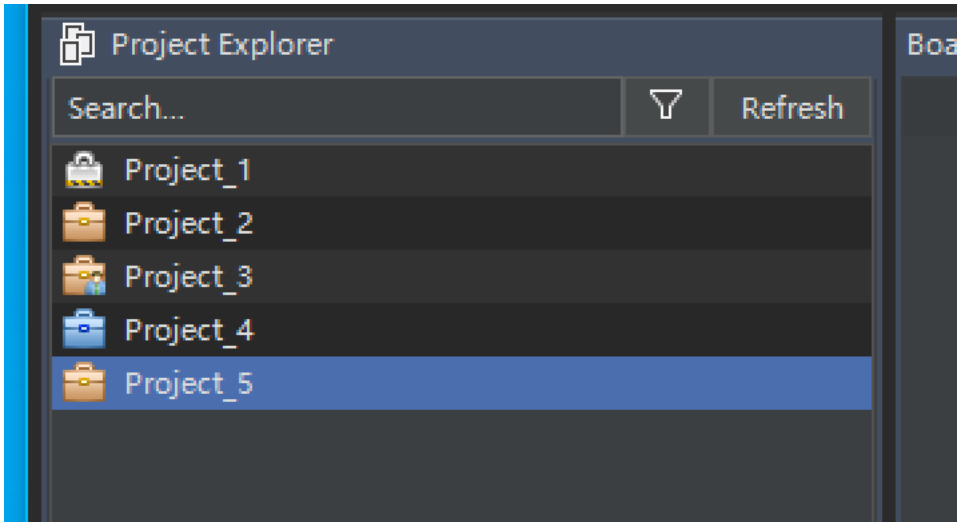
Use the filter bar at the top of the Project Explorer to narrow the displayed list:

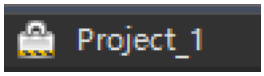
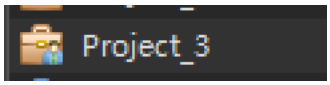


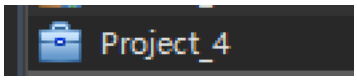
Filter	Shows
Active Designs	Projects with at least one checked-out container (by any user)
Recent Designs	Projects that have a local working folder on your machine (previously downloaded)
All Designs	All projects you have access to

Filter preferences are saved and restored between sessions.

Project Status Icons



Icon	Meaning
	**Read-Only** - You have Viewer access. You can open designs in read-only mode but cannot check out.
	Available - You have edit access and no one is currently working on the project.
	**In Use by Others** - You have edit access but another user has a container checked out.

Icon	Meaning
	**Active** - You have a container checked out in this project.

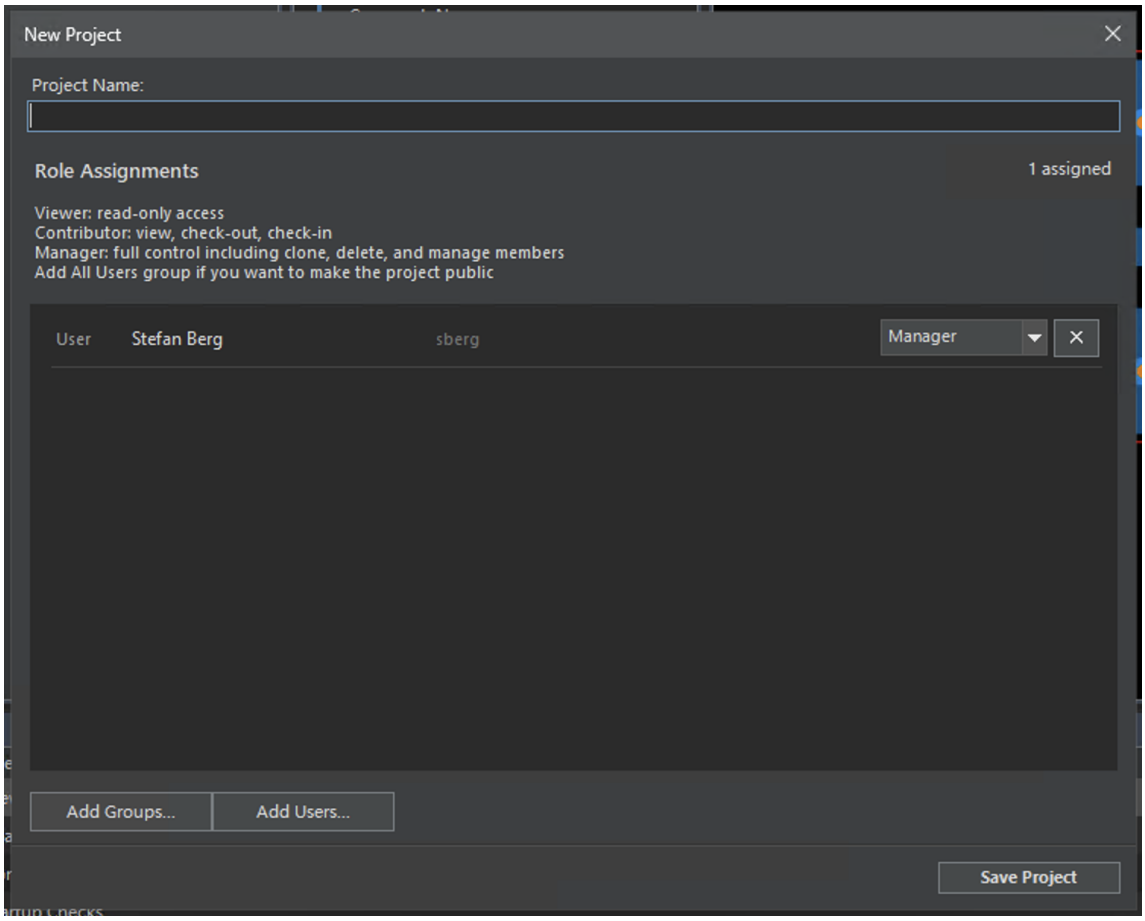
Creating a Project

Requires: Member of the **Project Creators** group or **Project Administrators** group.

1. Right-click anywhere in the Project Explorer.

2. Select **New Project** from the context menu.

3. In the dialog that appears:



- Enter a project name.
- Add users and/or groups to the role assignment list and set their roles.
- Click **Save Project**.

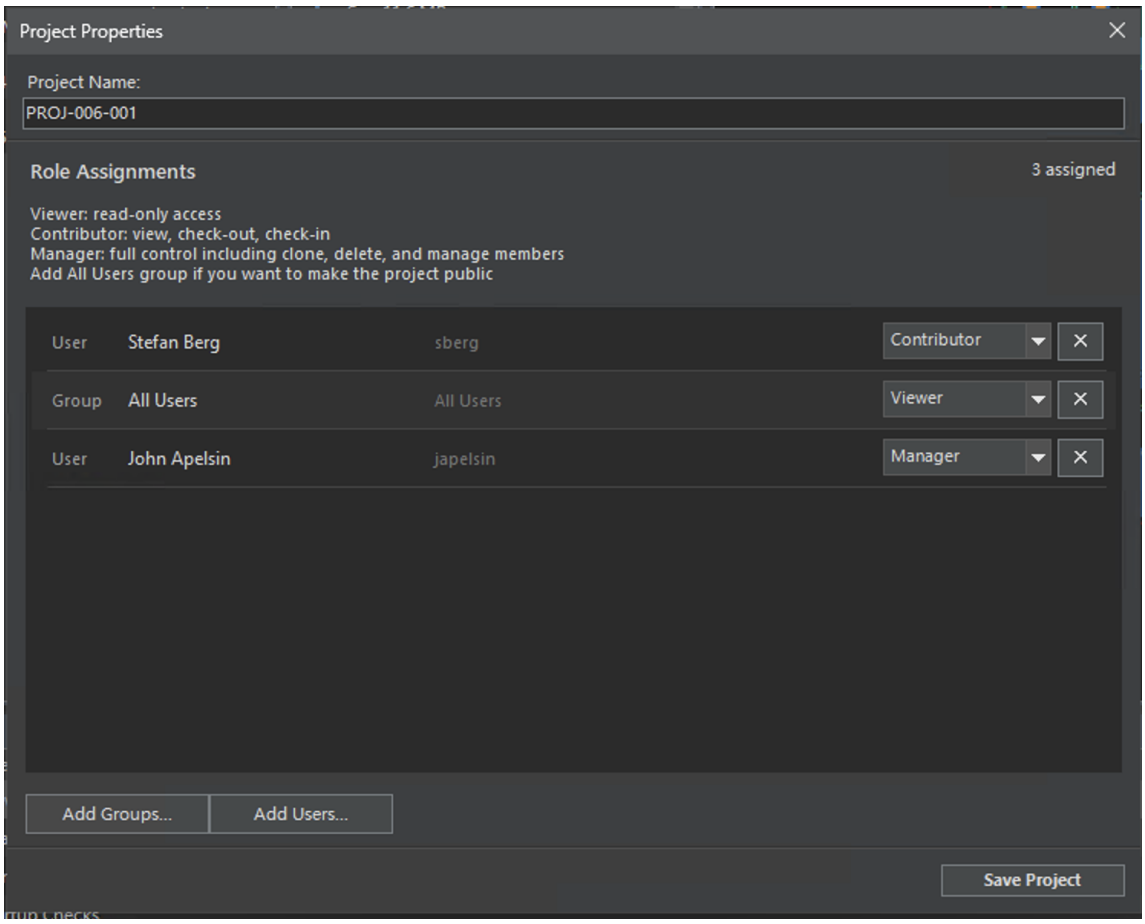
4. The new project appears in the Project Explorer.

> Only you and members of **Project Administrators** can manage the project until you add other users as Managers.

Renaming a Project

Requires: Manager role or Project Administrators membership. No active check-outs.

1. Right-click the project in Project Explorer.
2. Select **Properties**.
3. The Properties dialog appears:



4. Edit the **Project Name** field.

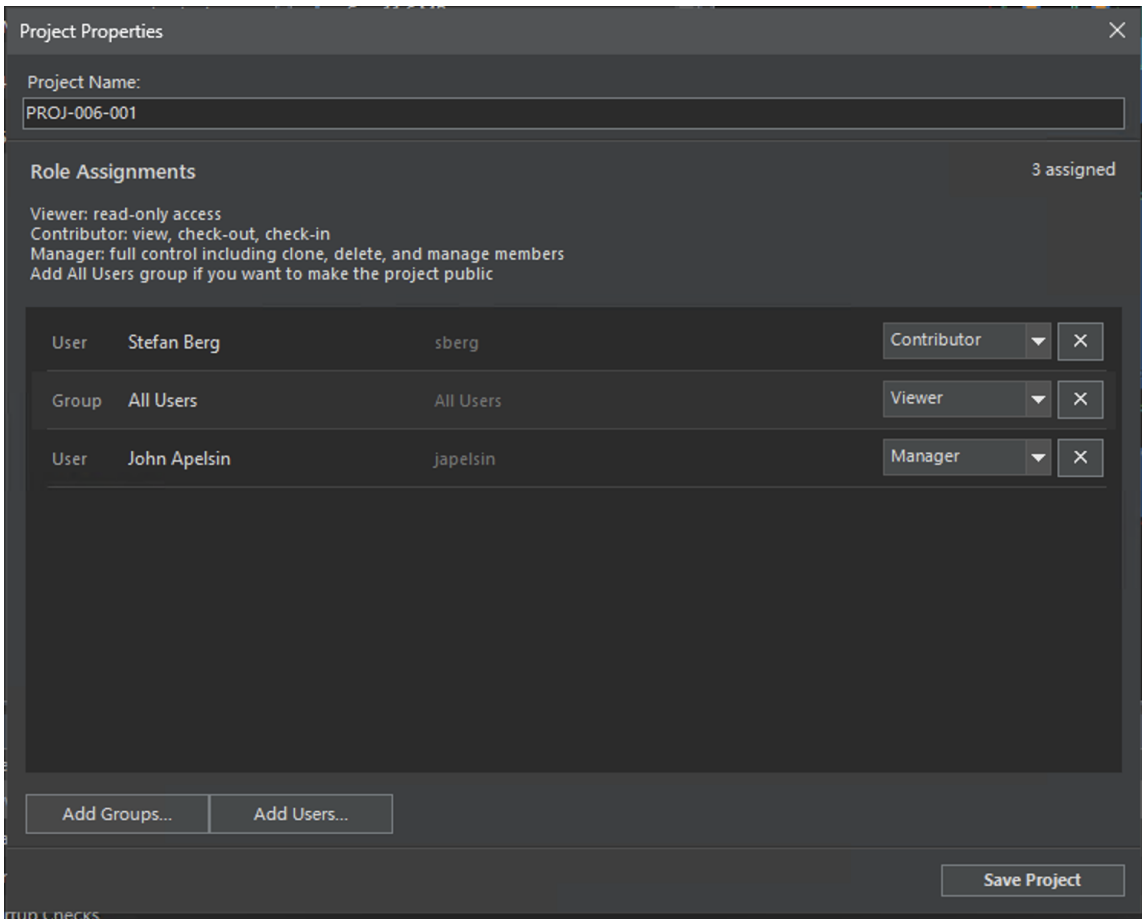
5. Click **Save Properties**.

Managing Project Access

Requires: Manager role or Project Administrators membership. No active check-outs.

1. Right-click the project -> **Properties**.

2. In the Properties dialog:



- Click **Add Groups...** to assign groups with a role.
- Click **Add Users...** to assign individual users with a role.
- Use the role dropdown on each row to change assignments.
- Set a row to **No Access** to remove the assignment.

3. Click **Save Properties**.

For details on roles and how access is determined, see Access Model.

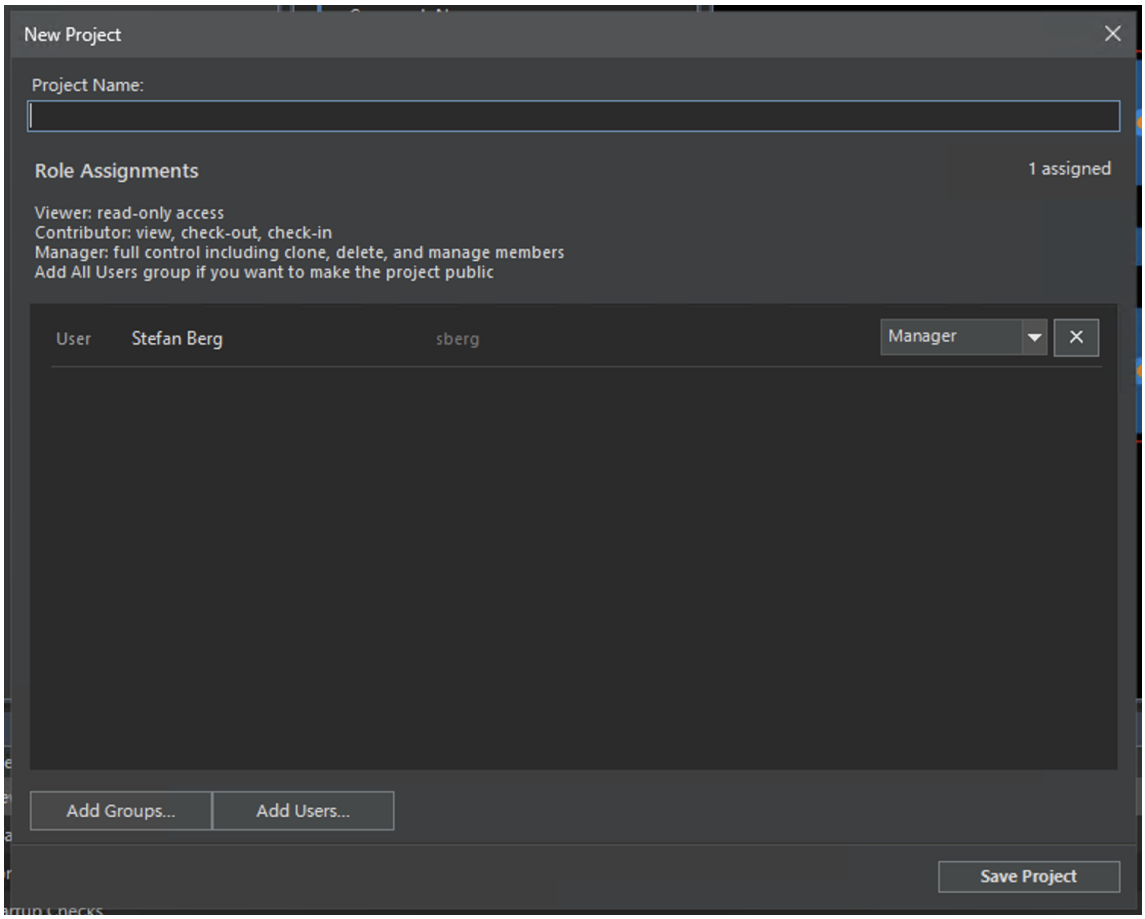
Cloning a Project

Requires: Manager role or Project Administrators membership. No active check-outs.

Cloning creates a complete copy of the project including all containers and their latest versions.

1. Right-click the project -> **Clone Project**.

2. Enter a name for the new project.



3. Click **OK**.

4. The cloned project appears in the Project Explorer.

Cloning copies design files but does not copy version history. The new project starts with version 1 of each container.

Deleting a Project

Requires: Manager role or Project Administrators membership. No active check-outs.

> Deleting a project removes **all containers and their entire version history**. The data is moved to the server's Trash folder and can be recovered by an administrator if needed.

1. Right-click the project -> **Delete Project**.
2. Confirm in the dialog that appears.
3. The project is removed from the Project Explorer.

Batch Project Operations

For managing access across multiple projects at once, use the **Batch Project Updater**:

1. Open **Tools -> Batch Project Updater** (available to Project Administrators).
2. Select target projects.
3. Configure the user and group assignments to apply.
4. Check **Override role assignments** to replace existing assignments on the selected projects.
5. Click **Apply**.

> Override replaces **all** existing role assignments on the selected projects with the new set. There is no undo.

See Access Model - Batch Updates for details.

Access Control

Starting with version 26.6, EEforce uses a role-based access control (RBAC) system. Each project independently defines who can access it and what they can do.

Roles

Every user or group assigned to a project receives exactly one role:

Role	Level	Permissions
Viewer	1	Browse projects, open designs in read-only mode, view previews and BOM
Contributor	2	Everything in Viewer, plus check-out and check-in designs
Manager	3	Everything in Contributor, plus clone/delete projects, manage members

A user who is **not assigned** to a project (and not in an assigned group) has **No Access** - the project is hidden from them entirely.

There is no explicit “Admin” role at the project level. System-wide administration is handled through the **Project Administrators** group (see below).

How Effective Role Is Calculated

When a user accesses a project, the system determines their effective role:

1. If the user has a **direct assignment** -> that role applies.
2. If the user belongs to one or more **assigned groups** -> the highest group role applies.
3. The effective role is the **maximum** of the direct assignment and all group assignments.
4. If no assignment matches -> **No Access**.

```
Effective Role = max(direct user role, highest matching group role)
```

Example: A user has Viewer assigned directly, but belongs to a group assigned as Contributor. Their effective role is **Contributor**.

Special System Entities

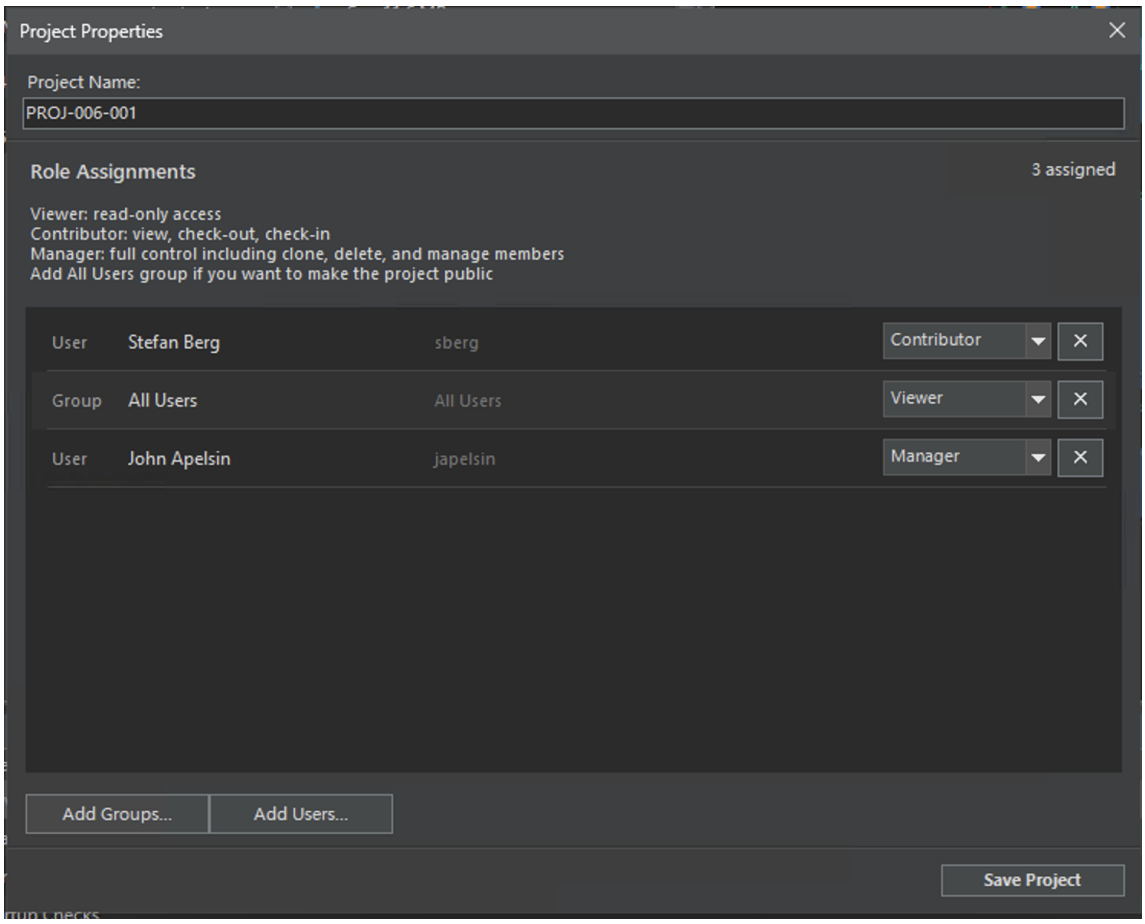
Entity	Behavior
`admin`	Built-in administrator. Always has full access to everything.
Project Administrators	Members have full unrestricted access to all projects, regardless of per-project assignments.
Project Creators	Members can create new projects. Does not grant access to existing projects.

Assigning Access

From the Desktop Client

1. Right-click a project -> **Properties**.

2. The role assignment panel shows current assignments:

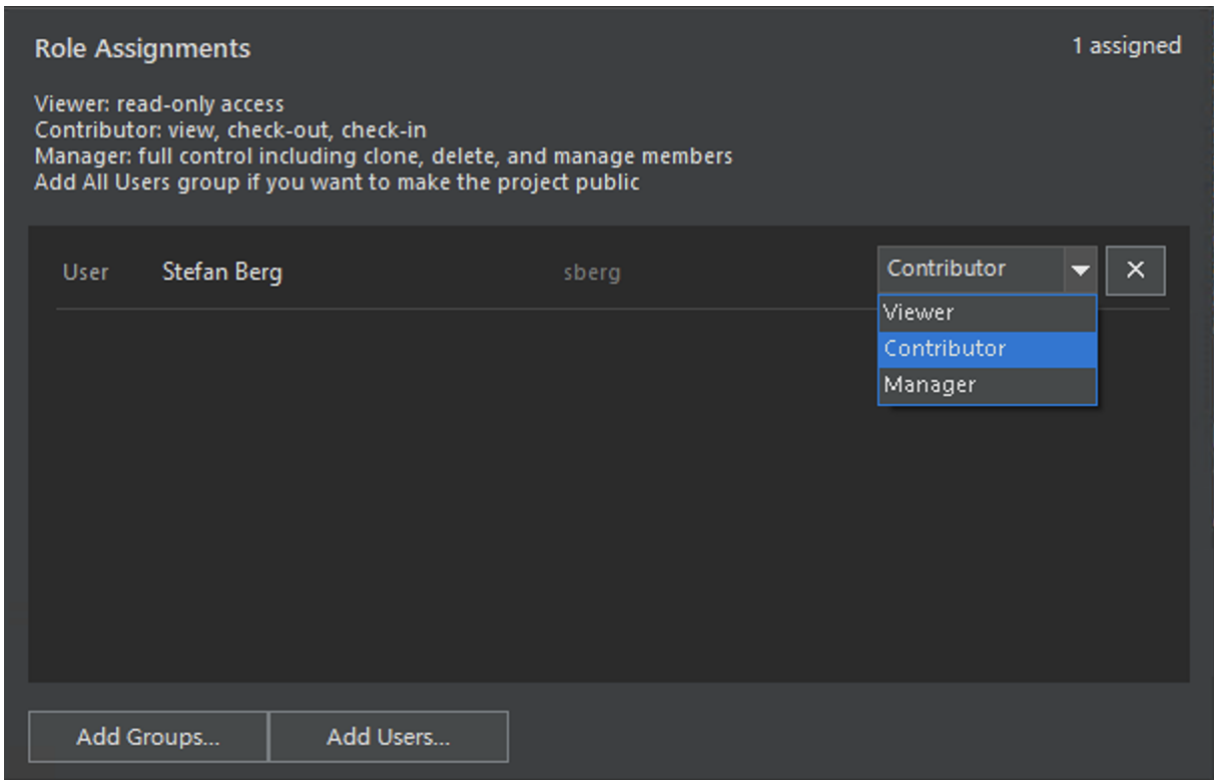


3. Click **Add Groups...** or **Add Users...** to add new entries.

4. Set the role dropdown for each entry.

5. To remove access: set the role to **No Access**.

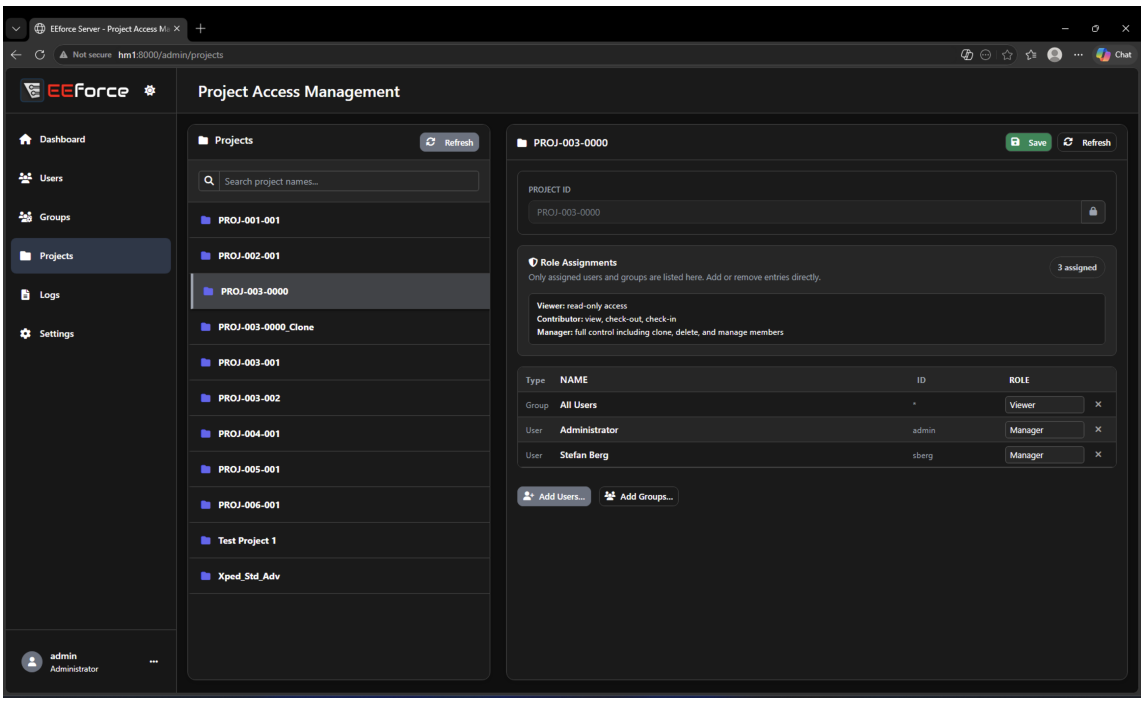
6. Click **Save Properties**.



From the Web Admin Interface

1. Navigate to **Admin -> Project Management**.

2. Select a project from the list.



3. Modify role assignments in the detail panel.

4. Click **Save**.

Making a Project Public

To make a project accessible to all authenticated users, assign the **All Users** group:

Goal	Configuration
Everyone can view	All Users -> **Viewer**
Everyone can edit	All Users -> **Contributor**
Private project	Do not assign “All Users”

Individual and group assignments **override** the All Users role when they grant a higher level. For example, if All Users is Viewer but a specific user is assigned Manager, that user has Manager access.

Security Rules

- Only **Managers** (or Project Administrators) can modify a project's access list.
- The **SuperUser** role (level 4) is assigned internally to members of Project Administrators and the built-in `admin` account.

Legacy Projects

Projects created before version 26.6 used a simpler access model (binary allowed/not-allowed). These projects are handled as follows:

Old State	New Behavior
User/group was in the access list	Shown with **Manager** role (preserves full access)
Project was "visible to all" (public)	Shown with **All Users -> Viewer** (read-only indicator)

> Legacy assignments are display-only until you explicitly edit and save. Once saved, the project fully adopts the new role model.

To migrate a legacy project: 1. Open Project Properties.
2. Review the auto-assigned roles.
3. Adjust roles as needed.
4. Click **Save Properties** - the project now uses the new model exclusively.

Batch Updates

The **Batch Project Updater** applies role changes across multiple projects simultaneously.

1. Open the Batch Project Updater (Project Administrators only).
2. Select target projects from the list.

3. Configure the role assignments you want to apply.

4. Check **Override role assignments** to replace all existing assignments on the selected projects with the new set.

5. Click **Apply**.

> Override mode removes **all** existing role assignments on the selected projects and replaces them with the assignments you configured. This cannot be undone.

Container Operations

Containers are versioned items within a project. Each container holds a design - typically a PCB layout, schematic, multi-board panel, or a generic folder of files. EEforce tracks full version history for every container.

::: info Naming Rules Container names must follow these rules: - **Forbidden characters:** < > \ : " /
- **Length:** 3 to 40 characters
- **Must be unique** within the project

Spaces, dots, hyphens, and underscores are all allowed.

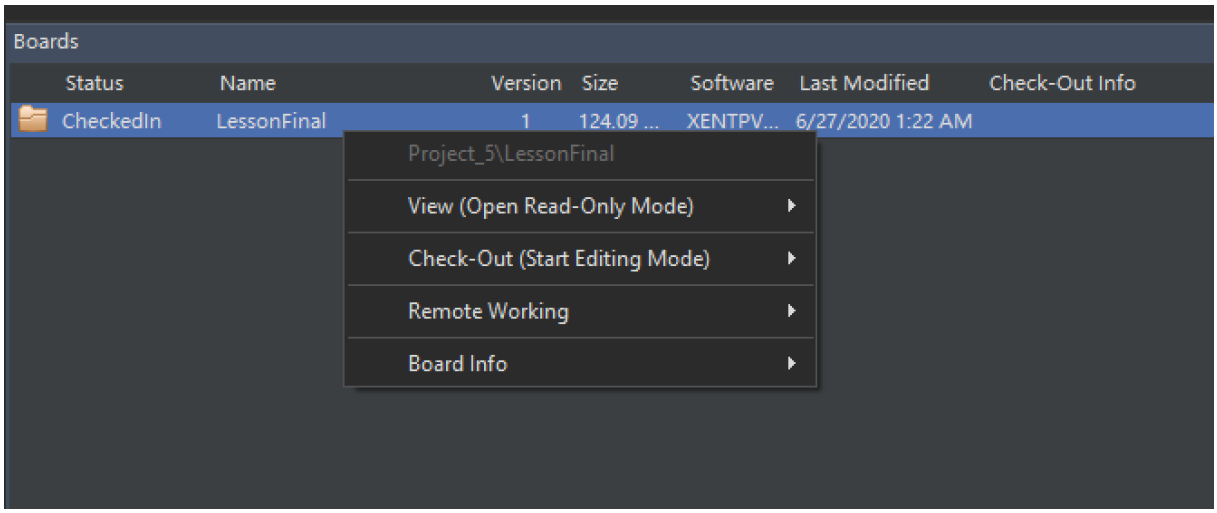
Valid: `Main_Board_01`, `My Board Rev-2`, `Project.v3` **Invalid:** `Bo` (too short), `Design/Main` (contains /), `AB` (under 3 chars) :::

Container Types

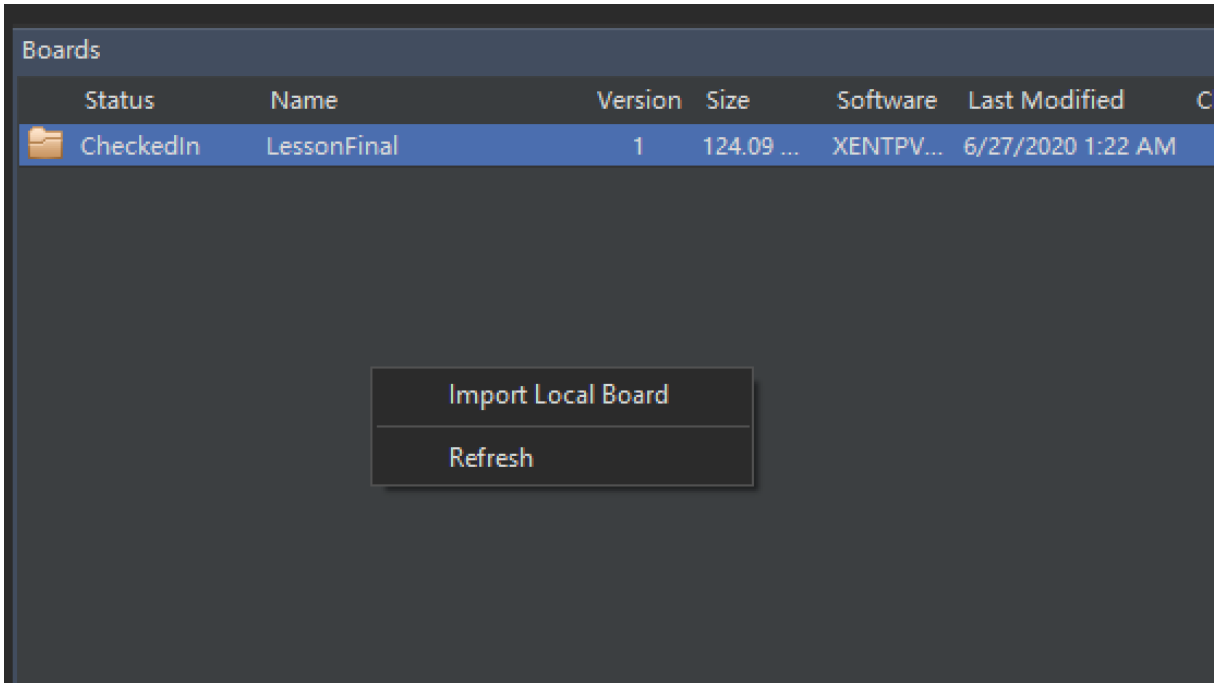
Type	Description
Board	PCB/Schematic design (Xpedition or PADS Professional). Supports full preview, BOM extraction, and editor integration.
Multi-Board Panel	Panel design containing multiple board instances.
Folder	Generic container for any file type. Versioned but without editor integration or preview.

Accessing Container Operations

Right-click a container in the **Containers** panel to access all operations:



Right-click an empty area in the Containers panel for project-level operations (import):



Importing a Container

Requires: Contributor or Manager role.

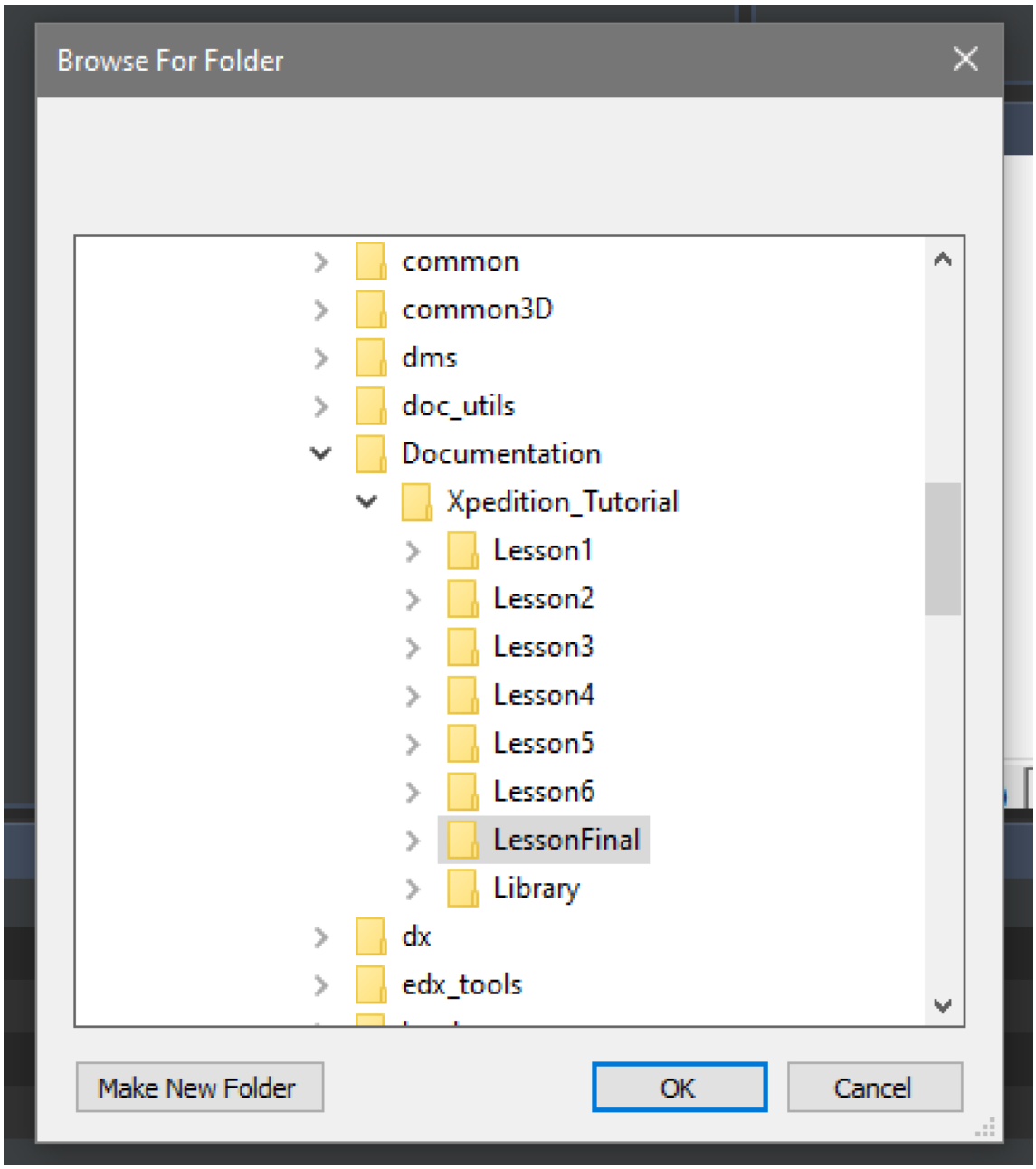
Import brings an external design into the project as a new container.

1. Select the target project in the Project Explorer.

2. Right-click an **empty area** in the Containers panel.

3. Click **Import Local Container**.

4. In the folder browser, select the root folder of your design:



Select the folder that contains the project/schematic file (e.g., the `.prj` file), not a parent folder.

5. Monitor progress in the **Operation Logs** panel.

Renaming a Container

Requires: Contributor or Manager role. Container must be **checked in**.

1. Right-click the container.
2. Go to **Container Info -> Rename**.
3. Enter the new name and click **OK**.

Cloning a Container

Requires: Contributor or Manager role. Container must be **checked in**.

Creates a copy of the container (latest version only) within the same project.

1. Right-click the container.
2. Go to **Container Info -> Clone**.
3. Enter a name for the copy and click **OK**.

Deleting a Container

Requires: Manager role. Container must be **checked in**.

> Deleting removes the container and all its version history. The data is moved to the server Trash folder.

1. Right-click the container.
2. Go to **Container Info -> Delete**.
3. Confirm the deletion.

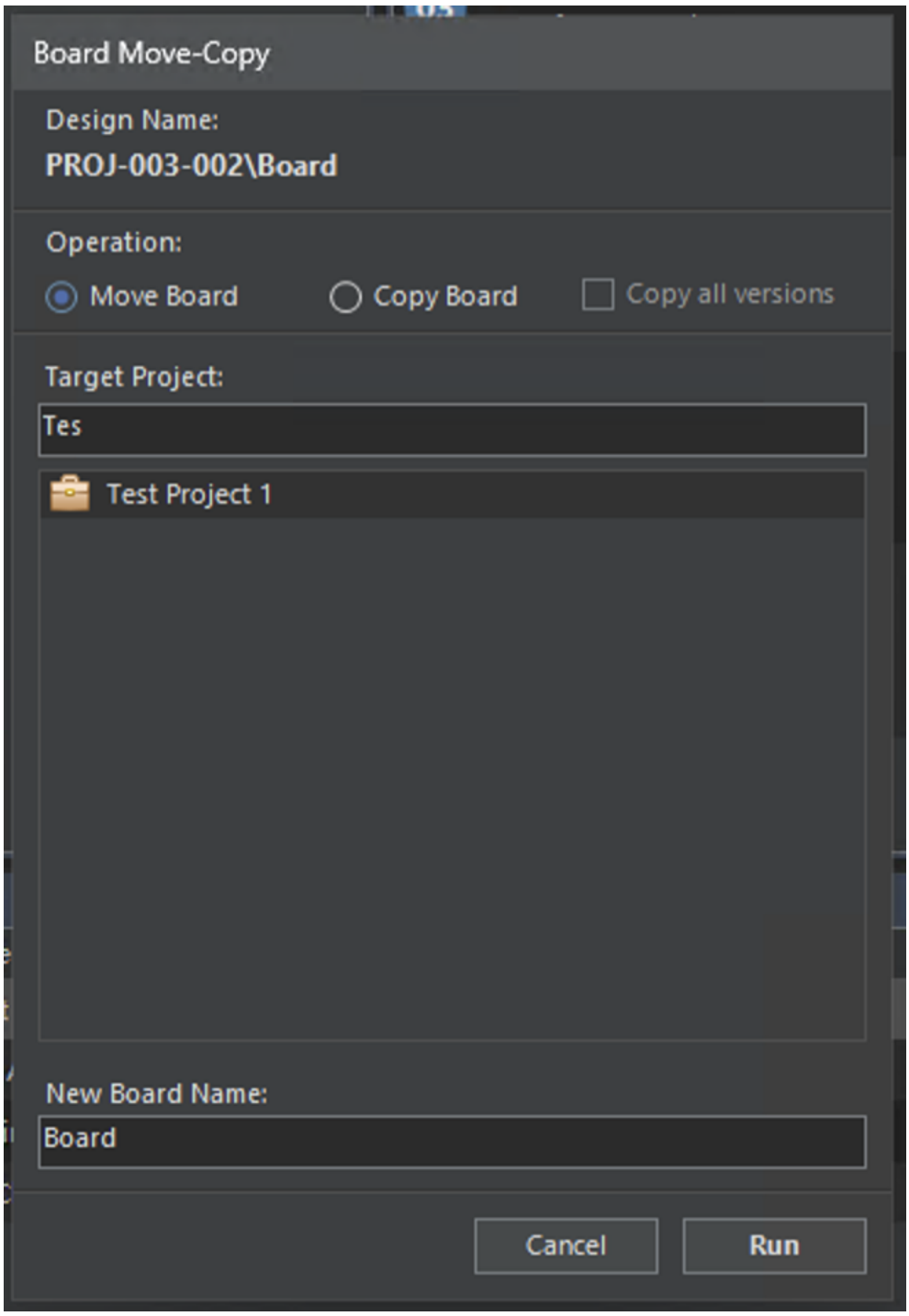
Moving a Container to Another Project

Requires: Manager role in both source and destination projects. Container must be **checked in**.

1. Right-click the container.

2. Go to **Container Info -> Move/Copy to Another Project**.

3. In the dialog:



4. Select **Move Container** under Operation.

5. Select the destination project.

6. Optionally rename the container.

7. Click **OK**.

The container is removed from the source project and appears in the destination.

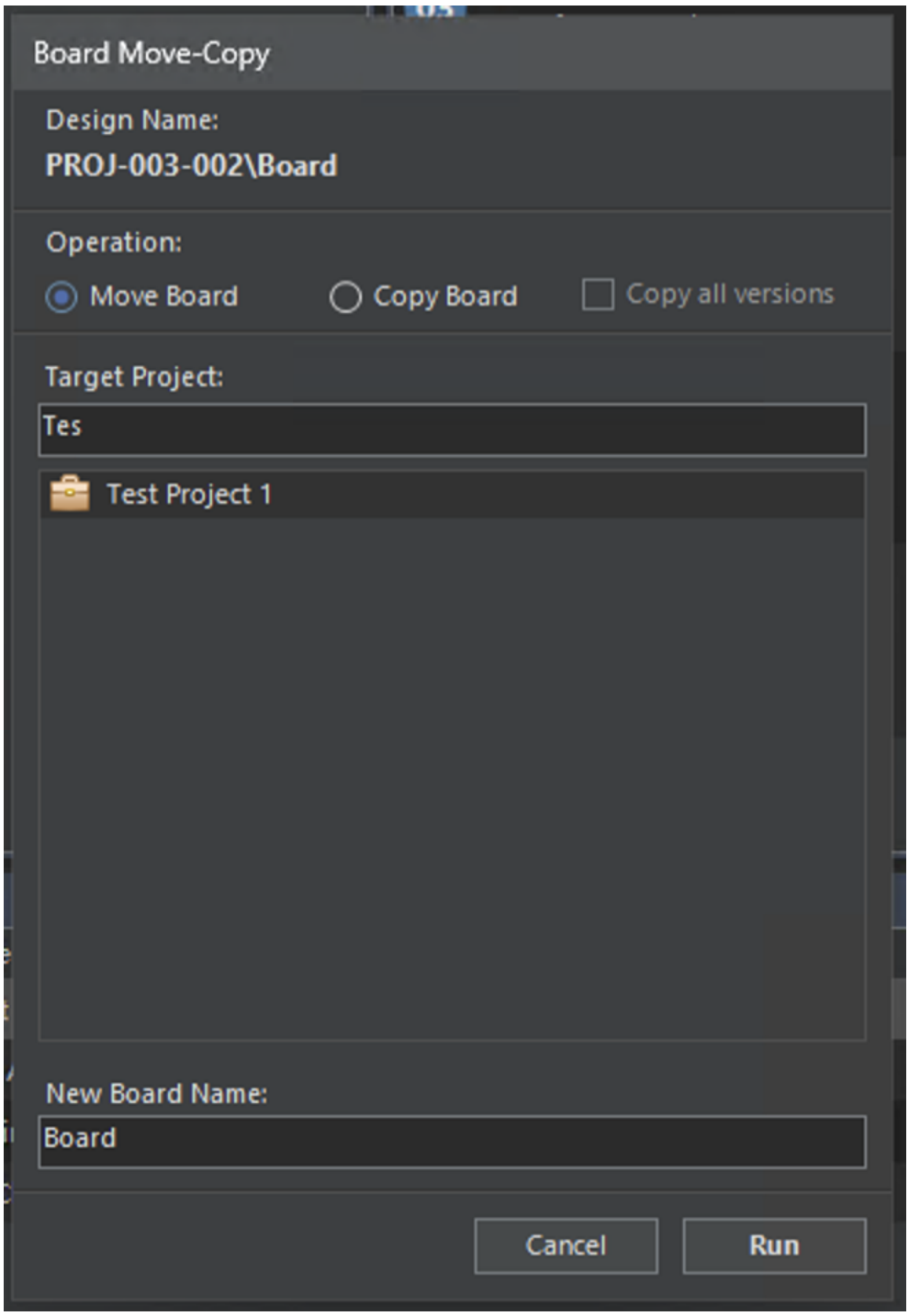
Copying a Container to Another Project

Requires: Contributor or Manager role in the destination project. Container must be **checked in**.

1. Right-click the container.

2. Go to **Container Info -> Move/Copy to Another Project**.

3. In the dialog:



4. Select **Copy Container** under Operation.

5. Optionally check **Copy all versions** to include full history (otherwise only the latest version is copied).

6. Select the destination project.
7. Optionally rename the container.
8. Click **OK**.

Container States

Containers follow a state machine:

State	Meaning
Checked In	Stored on server. Available for check-out. All operations (rename, clone, delete, move, copy) require this state.
Checked Out	A user is actively editing. Locked to that user until check-in or cancel.

Only the user who checked out a container can check it back in or cancel the check-out. Administrators can force-cancel from the web admin interface.

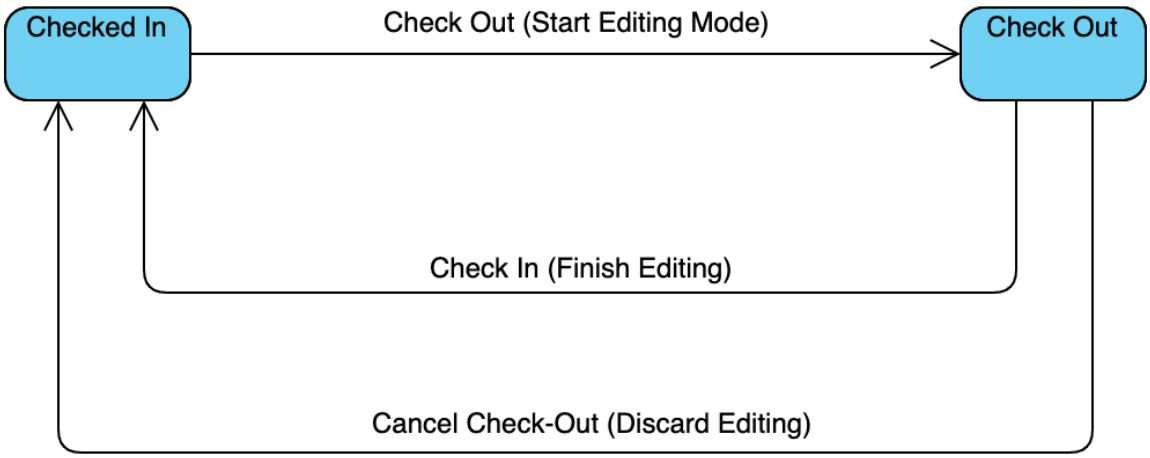
See Design Operations for check-in/check-out procedures.

Design Operations

Design operations manage the lifecycle of design files within containers. EEforce uses a **lock-based** version control model where a design can only be edited by one user at a time.

Design States

State	Description
Checked In	Design is stored in the vault. No one is editing it. Available for check-out.
Checked Out	A copy has been downloaded for editing. The container is locked to the user who checked it out.



Available Operations

Operation	When Available	What It Does
Check Out	Checked-in state	Downloads the design to your local machine; locks the container
Check In	You have it checked out	Uploads your changes as a new version; unlocks the container
Cancel Check-Out	You have it checked out	Discards local changes; unlocks without creating a new version
View (Read-Only)	Any state	Downloads a read-only copy without locking

Opening a Design in Read-Only Mode

Requires: Viewer, Contributor, or Manager role.

Read-only mode downloads a copy of the design without locking it. You can view and inspect but not save changes back.

1. Right-click the container or a specific version.

2. Under **View (Open Read-Only Mode)**, select the desired action (e.g., Open in Xpedition, Open PCB, Open Schematic).

Read-only mode does not affect other users. Multiple users can view simultaneously.

Checking Out a Design (Start Editing)

Requires: Contributor or Manager role. Container must be checked in.

1. Right-click the container (or a specific version to check out an older version).

2. Under **Check Out (Start Editing Mode)**, select the desired action.

3. The design files are downloaded to your local working directory.

4. The container status changes to **Checked Out** and is locked to you.

> While you have a design checked out, no other user can edit it. Check in or cancel promptly when done.

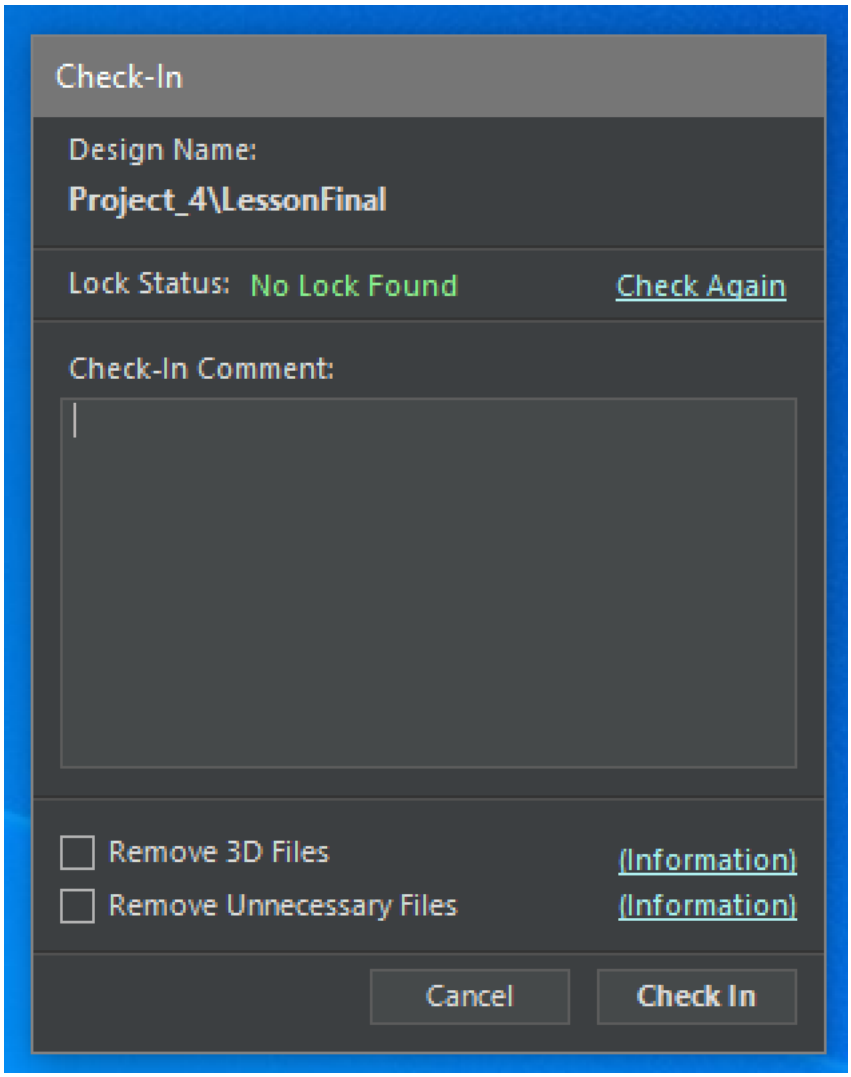
Checking In a Design (Finish Editing)

Requires: You must have the container checked out.

1. Right-click the checked-out container.

2. Click **Check In (Finish Editing)**.

3. The Check-In dialog appears:



4. Review the following:

Field	Purpose
Lock Status	Shows if any program still has design files open. Must show “Unlocked” to proceed.
Check-In Comment	Optional description of what changed. Displayed in version history.

Field	Purpose
Remove 3D Files	Strips 3D data to save vault space (use if you made no 3D changes).
Remove Unnecessary Files	Removes log files and old CCZ files that don't need versioning.

5. Click **Check-In**.

6. Monitor upload progress in the **Operation Logs** panel.

If the Lock Status shows "LOCKED", close all editor windows (Xpedition, PADS) and click **Check Again**.

Cancelling a Check-Out (Discard Changes)

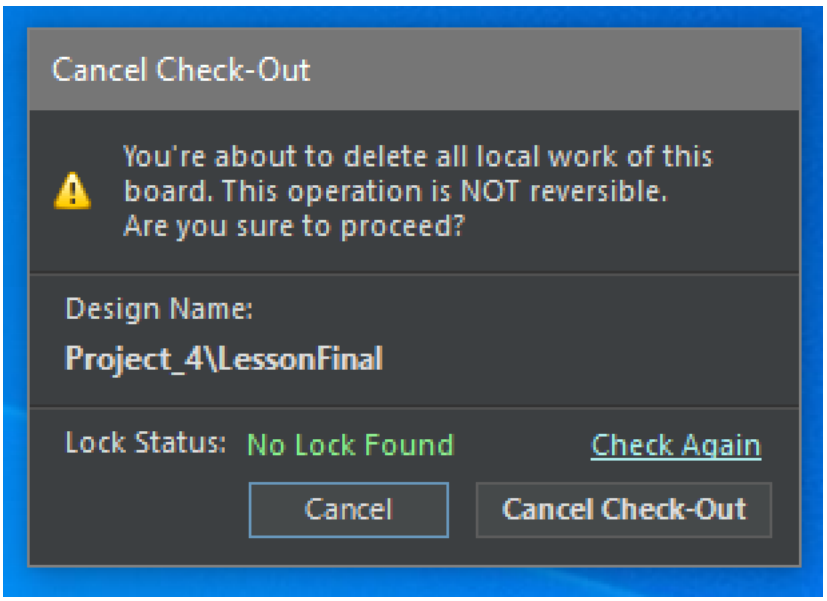
Requires: You must have the container checked out.

This permanently discards all local changes made since check-out. The design reverts to its last checked-in version.

1. Right-click the checked-out container.

2. Click **Cancel Check-Out (Discard Editing)**.

3. The confirmation dialog appears:



4. If Lock Status shows “LOCKED”, close editor windows and click **Check Again**.

5. Click **Cancel Check-Out** to confirm.

Version History

Each check-in creates a new version. You can:

- **View any previous version** in read-only mode by right-clicking the version number.
- **Check out a specific version** to create a new version based on an older one (effectively reverting).
- **See check-in comments** for each version in the version list.

Troubleshooting

Issue	Resolution
“Design is locked” but you need to edit	Contact the user who has it checked out, or ask an admin to force-cancel
Lock Status stuck on “LOCKED”	Close all Xpedition/PADS windows. Check Task Manager for lingering processes.
Check-in fails midway	Check network connection. Enable chunked uploads in Settings for large designs.
Local files missing after cancel	Expected behavior - cancel removes all local copies of the design.

Remote Working

EEforce supports offline workflows for users who need to work outside the network - remote sites, travel, or environments without reliable server connectivity.

How It Works

```
1. Export a design as a ZIP package (checks it out on the server)
2. Work offline using the ZIP contents
3. Import the updated package back (creates a new version)
```

The design remains **locked** on the server while you have it exported. Other users can view it in read-only mode but cannot edit until you import or cancel.

Exporting a Design for Remote Work

Requires: Contributor or Manager role. Container must be checked in.

1. Select the project in the **Project Explorer**.

2. Select the container in the **Containers** panel.

3. Right-click the container -> **Remote Working -> Export Package**.

4. In the file dialog, choose a save location and filename for the ZIP package.

5. Click **Save**.

The ZIP file contains all design files for the latest version. The container is now marked as **Checked Out** on the server.

The exported ZIP is a self-contained package. You can copy it to a USB drive, email it, or transfer it by any means.

Working with the Exported Package

1. Extract the ZIP to a local folder.

2. Open and edit the design files using your normal tools (Xpedition, PADS Professional).

3. When done, keep all modified files in the same folder structure.

> Do not rename or restructure the folder layout inside the package. EEforce expects the same structure when importing back.

Importing a Remotely Updated Design

Requires: You must have the container checked out (via the export step).

1. Select the project in the **Project Explorer**.

2. Select the checked-out container in the **Containers** panel.

3. Right-click the container -> **Remote Working -> Import Package**.

4. In the folder browser, select the folder containing your updated design files.

5. Wait for the upload to complete. Monitor progress in the **Operation Logs** panel.

The import creates a **new version** of the container and releases the lock (checks it in).

Cancelling a Remote Check-Out

If you decide not to import your changes:

1. Right-click the checked-out container.
2. Click **Cancel Check-Out (Discard Editing)**.
3. Confirm the cancellation.

The lock is released and no new version is created.

Tips for Remote Working

Scenario	Recommendation
Slow upload connection	Enable chunked uploads in Settings before importing
Multiple designers need to work remotely	Export different containers to different people never the same container
Long-term remote work	Communicate with your team so they know the container is locked
Lost or corrupted export ZIP	Cancel the check-out on the server and re-export

Web Administration Interface

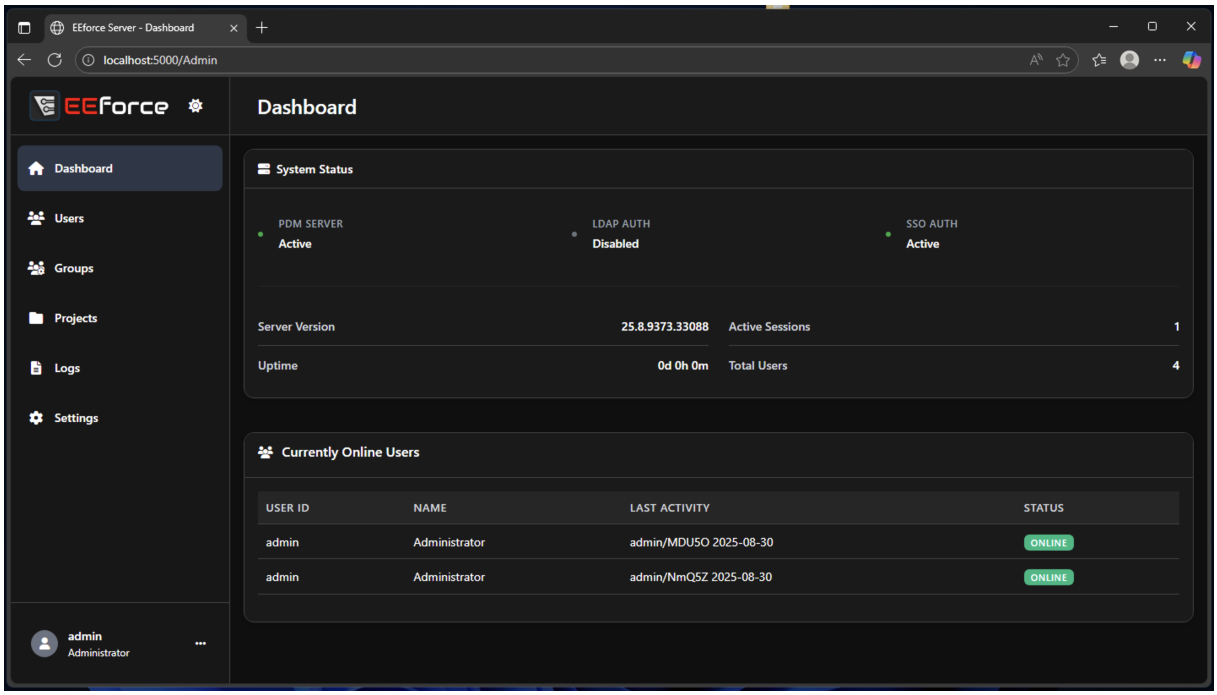
The EEforce Web Admin provides a browser-based interface for system administration. It is designed for IT administrators and does not require any software installation beyond a modern web browser.

::: info Access URL Navigate to `http://<SERVER-ADDRESS>/Admin` in your browser. :::

Login

Enter the administrator password to access the interface. The web admin is restricted to users with administrator privileges.

Dashboard

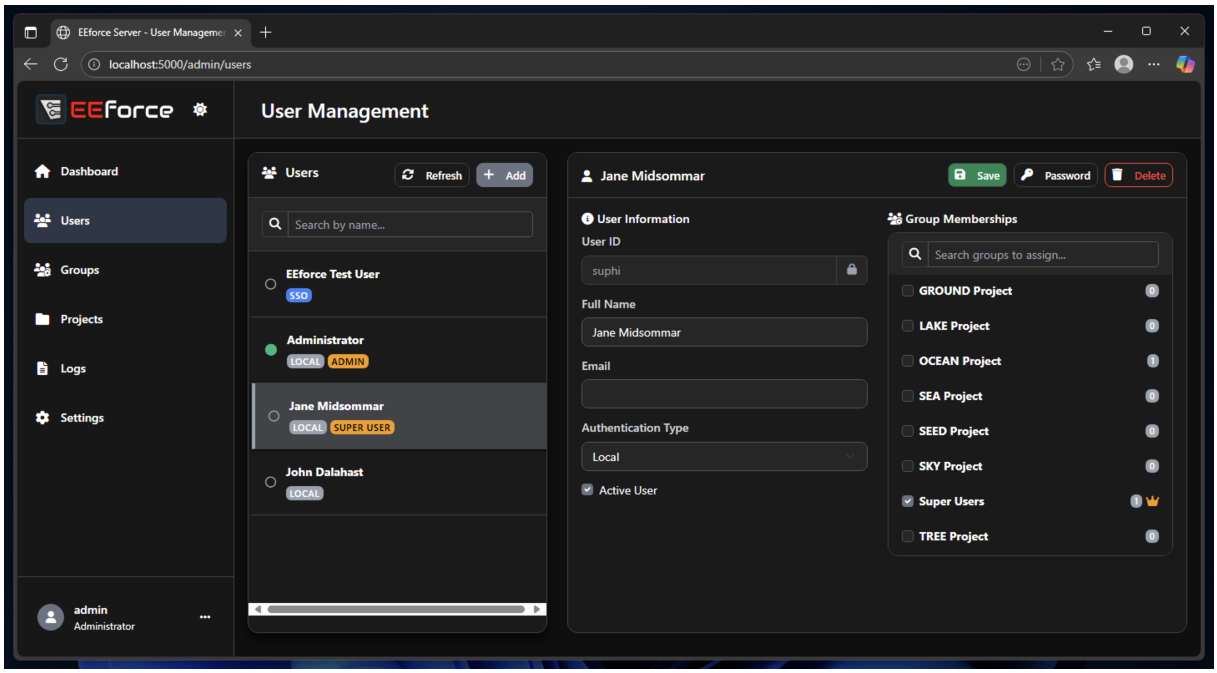


The Dashboard provides a real-time overview of server status:

- **System Status** - server version, uptime, and service indicators (PDM Server, LDAP Auth, SSO Auth)
- **Active Sessions** - number of currently active user sessions
- **Currently Online Users** - table showing logged-in users with their last activity

---

User Management

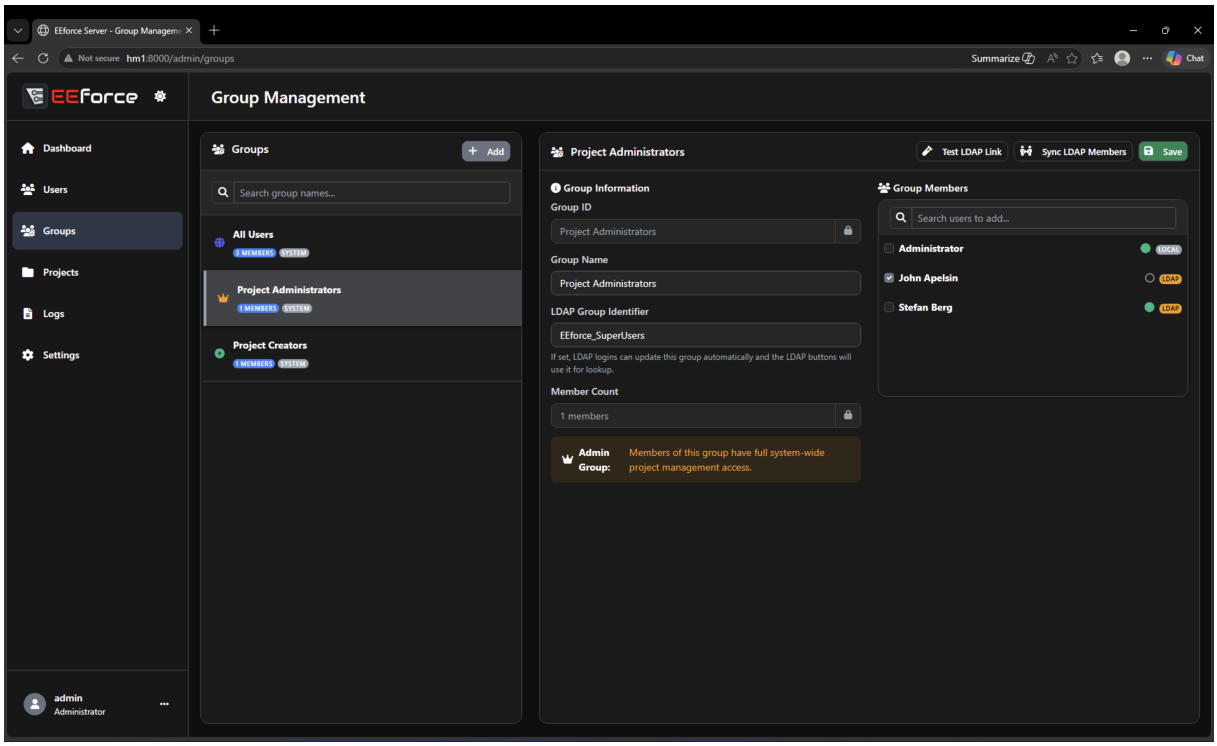


Manage user accounts from this page:

Action	How
Create a user	Click the “Add” button, fill in user ID, name, and password
Edit a user	Select from the list, modify name or group memberships
Delete a user	Select from the list, click delete
Reset password	Select the user, enter a new password

::: info SSO Users Users provisioned through SSO or LDAP cannot have their credentials modified here - they are managed by the external identity provider. :::

Group Management



Manage groups and their memberships:

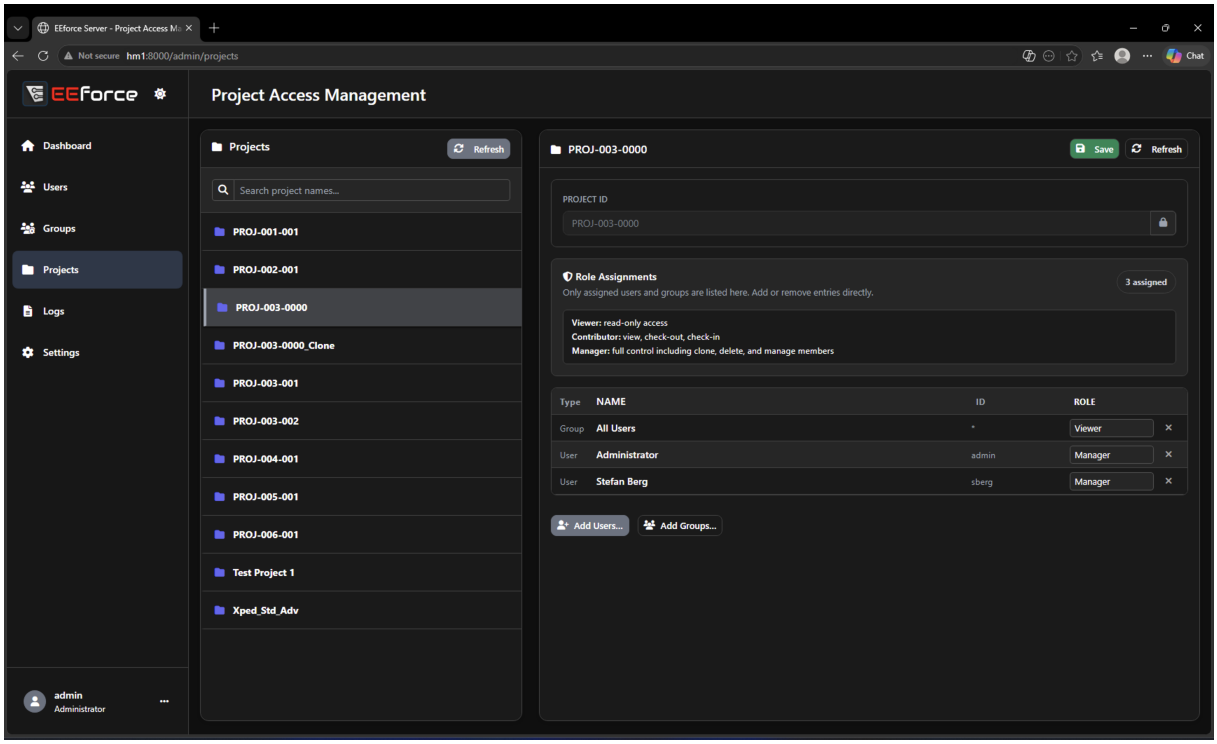
Action	How
Create a group	Click “Add”, enter group name
Add members	Select a group, add users from the member panel
Remove members	Select a group, remove users from the member list
Delete a group	Select from the list, click delete

System Groups

These groups have special meaning and cannot be deleted:

Group	Purpose
Project Administrators	Members have Manager access to all projects
Project Creators	Members can create new projects

Project Management



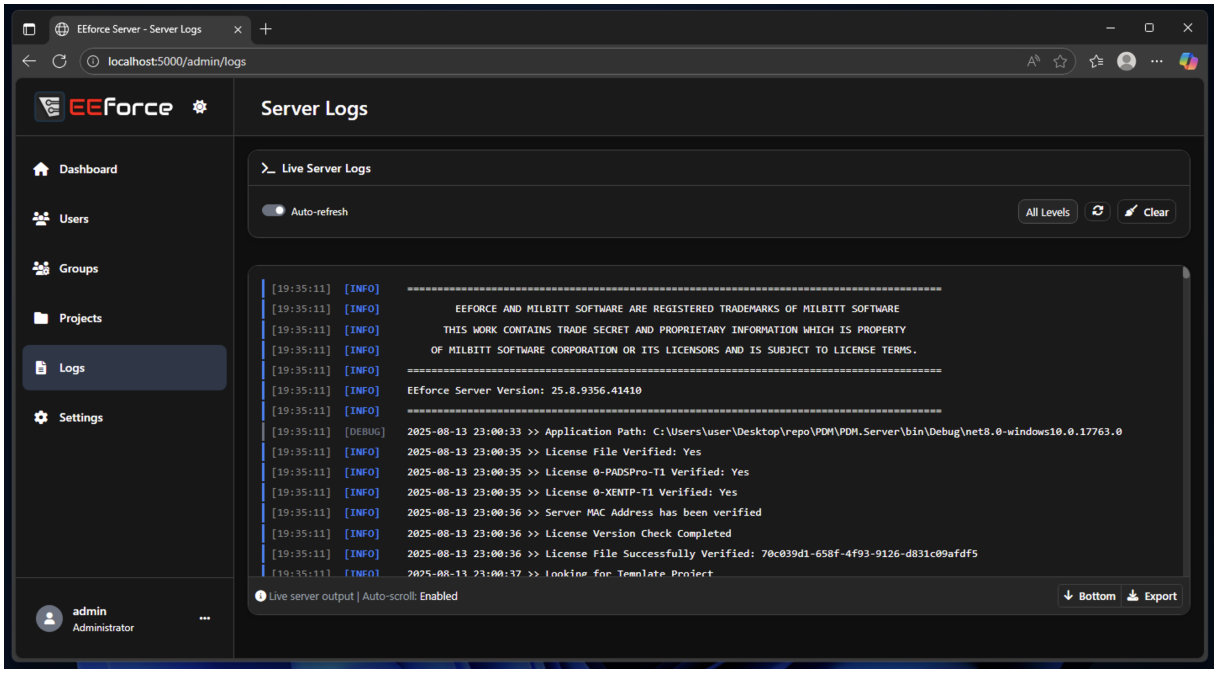
View and manage role assignments for existing projects:

Action	How
View assignments	Select a project to see its current role assignments
Add user/group	Add entries with a specific role (Viewer, Contributor, Manager)

Action	How
Change role	Modify the role dropdown for existing assignments
Remove assignment	Set role to No Access or remove the entry
Save changes	Click Save to persist modifications

::: warning Limitations Creating, deleting, and renaming projects is only available from the desktop client. These operations involve vault filesystem changes that require the controlled environment of the client application. :::

Logs



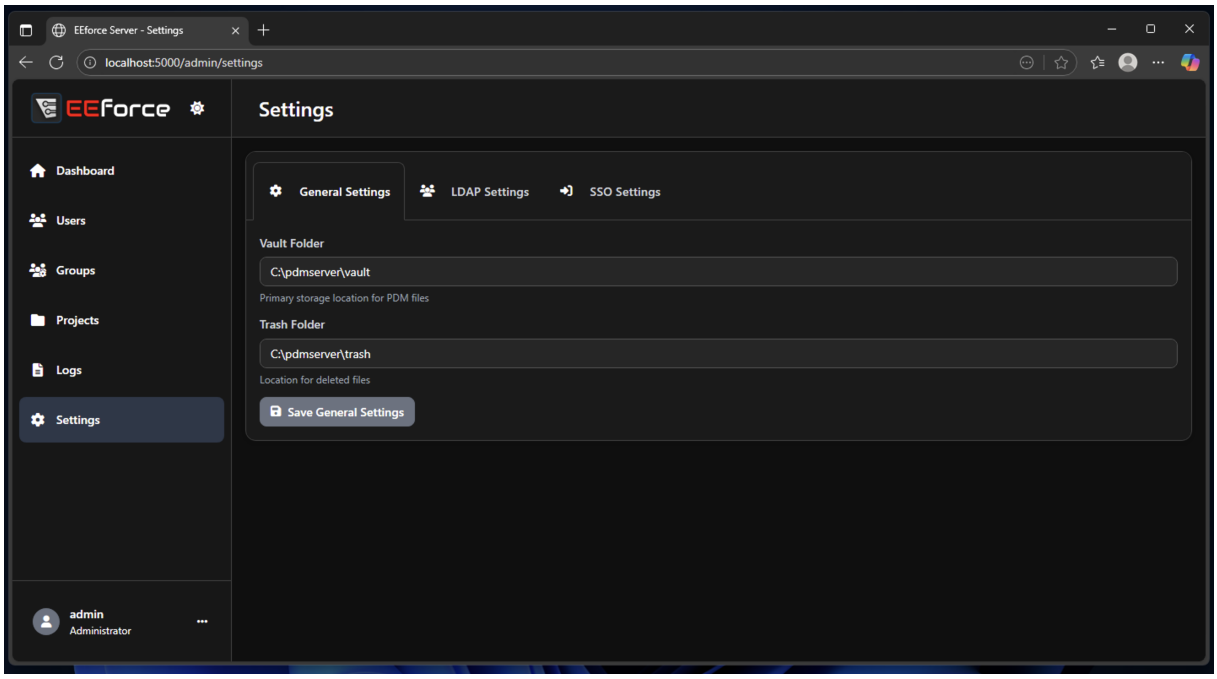
The Logs page displays server-side activity in real time:

- User login/logout events

- Check-in/check-out operations
- Administrative actions
- Error messages and warnings

Use the log view for: - **Troubleshooting** connection or permission issues
- **Auditing** who accessed or modified what
- **Debugging** unexpected behavior

Settings



Configure server-wide settings:

Setting	Notes
Vault / Trash folders	Storage paths for design files and deleted items
LDAP configuration	Domain, service account, auto-provisioning

Setting	Notes
SSO configuration	Identity provider settings, callback URLs

LDAP Configuration

Configure Active Directory integration:

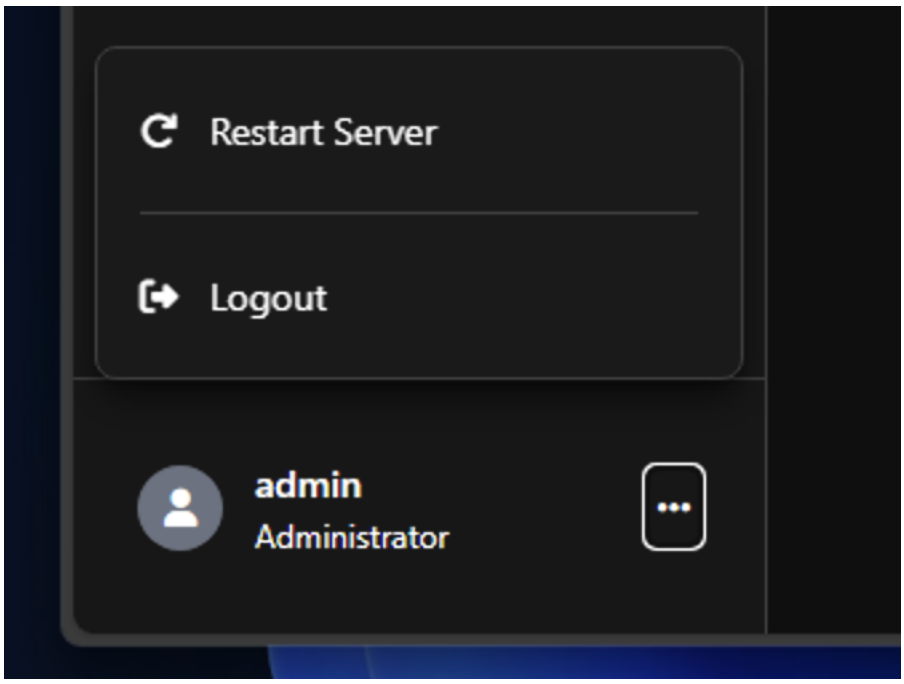
- **Domain** - the AD domain to authenticate against (e.g., `corp.example.com`)
- **Use Secure Socket Layer (SSL)** - connect via LDAPS (port 636) instead of plain LDAP
- **Service Account UID / Password** - credentials used to query the directory
- **Auto-register LDAP users on first login** - automatically create EEforce accounts on first successful authentication
- **Test LDAP Connection** - built-in test panel to verify configuration

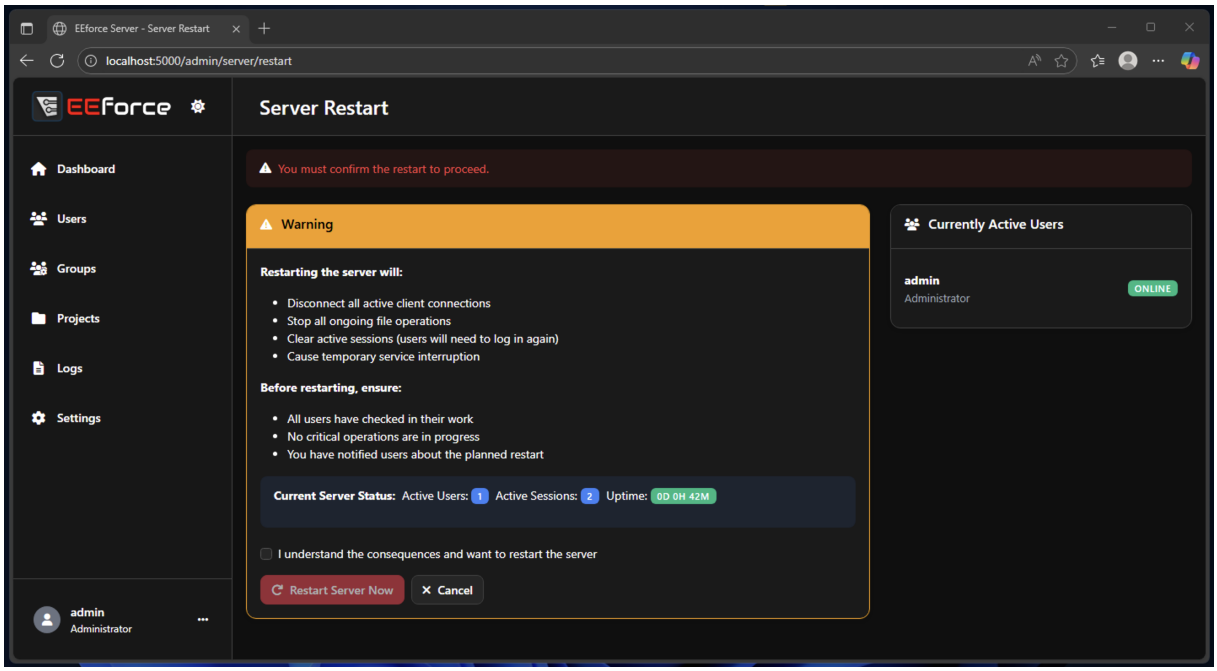
SSO Configuration

Configure OpenID Connect (OIDC) identity provider integration. See SSO Integration for detailed setup instructions.

Server Restart

Click the three-dot menu in the bottom-left corner -> **Restart Server**.



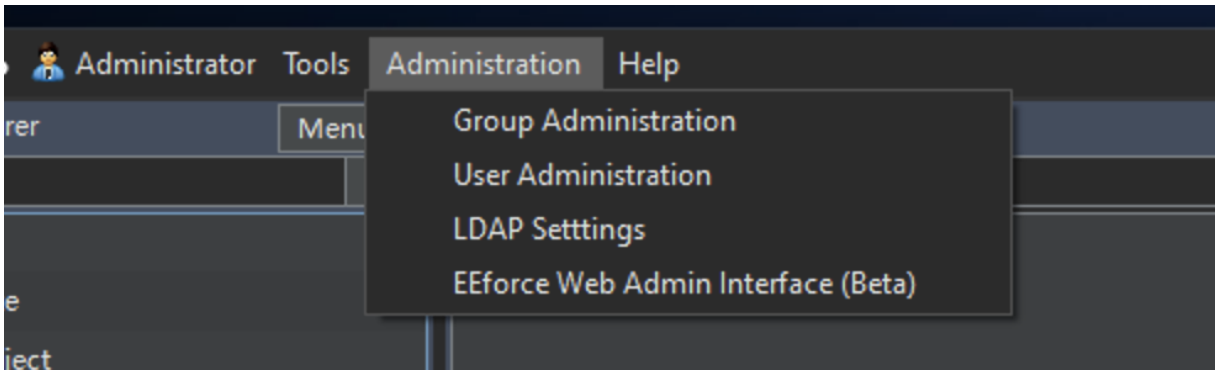


Restarting the server disconnects all active users. Ensure all users have completed their work (no active check-ins in progress) before restarting.

Logging Out

Click the three-dot menu in the bottom-left corner -> **Logout**.

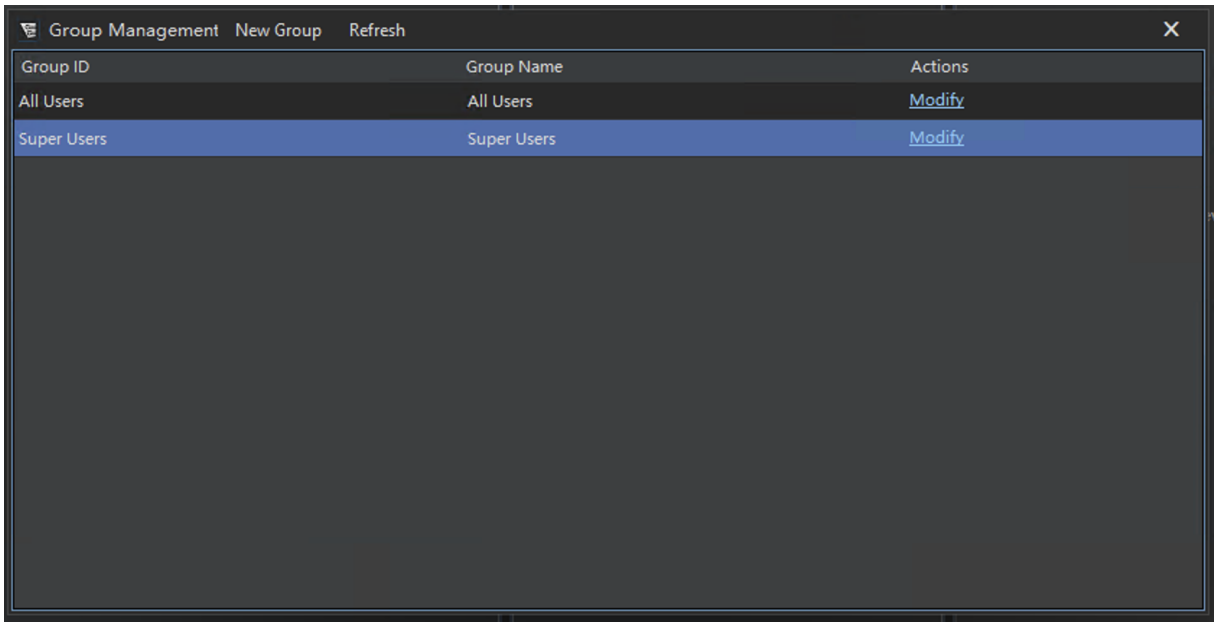
Administration from the Desktop Client



The EEforce desktop client provides administration features for users with administrator privileges. These are accessible from the **Admin** menu in the top menu bar.

::: info Web Interface Recommended The same administration tasks are available in the Web Admin Interface, which offers a more modern experience. The client-based admin panels are maintained for convenience but may be retired in future versions. :::

Group Management



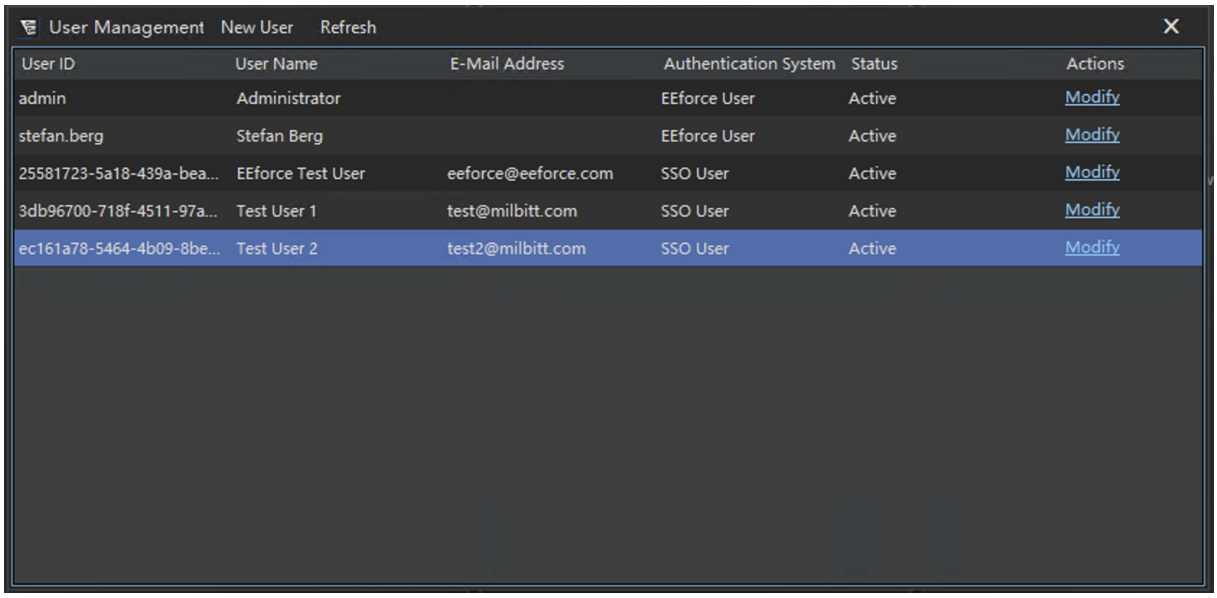
Manage user groups from the desktop client:

- **Create groups** - define organizational or functional groups
- **Delete groups** - remove groups that are no longer needed
- **Add/remove members** - assign users to groups or remove them
- **View membership** - see which users belong to a group

System Groups

Group	Cannot Be Deleted	Purpose
Project Administrators	Yes	Members have Manager access to all projects
Project Creators	Yes	Members can create new projects

User Management

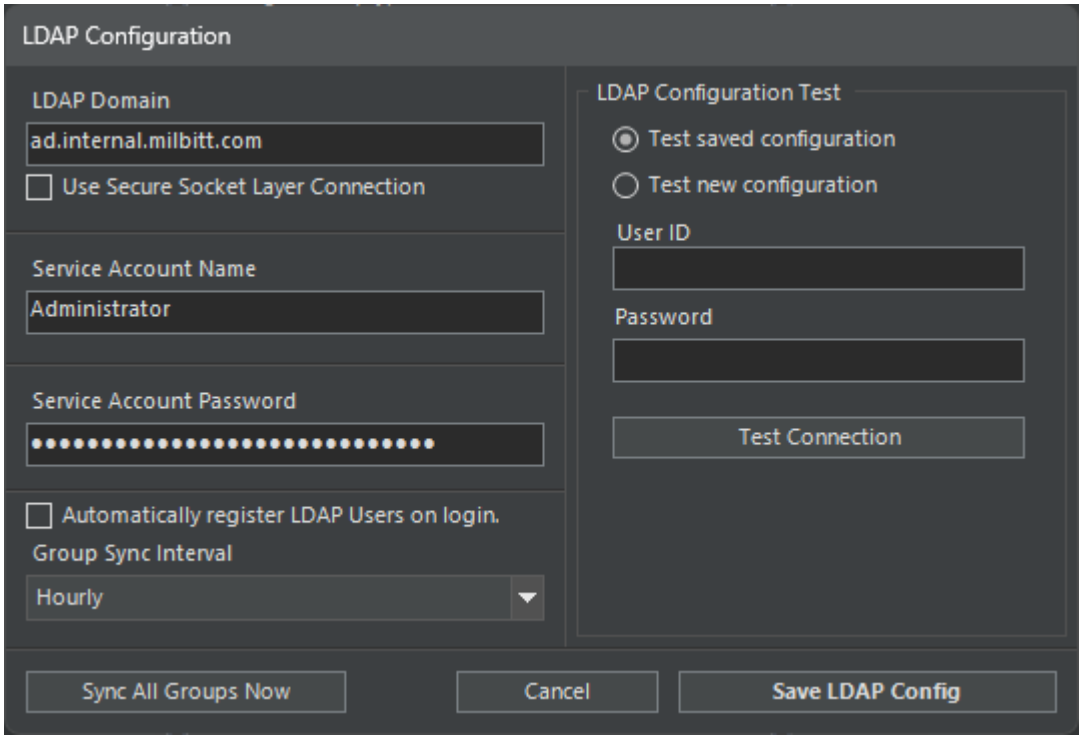


Manage user accounts:

- **Create users** - add new user accounts with a username, display name, and password
- **Modify users** - update display name, reset password, change group memberships
- **Disable/delete users** - remove access for users who have left

::: info SSO/LDAP Users Users authenticated through SSO or LDAP have their identity managed externally. You can modify their group memberships in EEforce but cannot change their credentials. :::

LDAP Configuration



Configure Active Directory / LDAP integration:

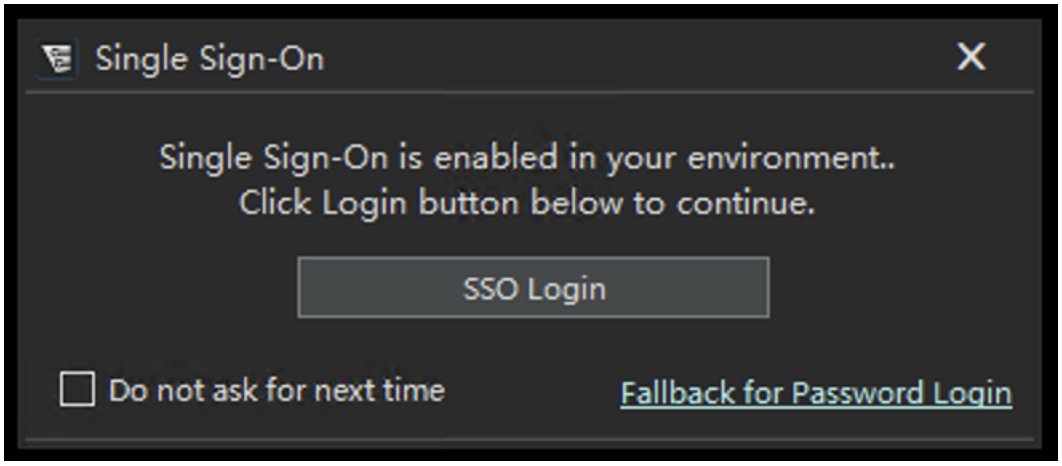
Setting	Description
LDAP Domain	The Active Directory domain to connect to
Service Account	Credentials used to query the directory
Auto-Register on Login	Automatically create EEforce accounts for LDAP users when they first log in
Group Linking	Link EEforce groups to AD groups for automatic membership sync

Use the **Test Connection** button to verify your LDAP configuration before saving.

> When auto-registration is enabled, new users can log in with their AD credentials without any manual account creation. Their EEforce account is created automatically on first successful authentication.

SSO Configuration

Single Sign-On configuration is only available from the Web Admin Interface. The desktop client does not support SSO setup.



Once SSO is configured on the server, the client login screen will show an SSO option alongside traditional username/password authentication.

LDAP Integration

EEforce integrates with Active Directory (AD) and other LDAP-compatible directories for user authentication and group synchronization. This allows your team to log in with their existing corporate credentials.

Overview

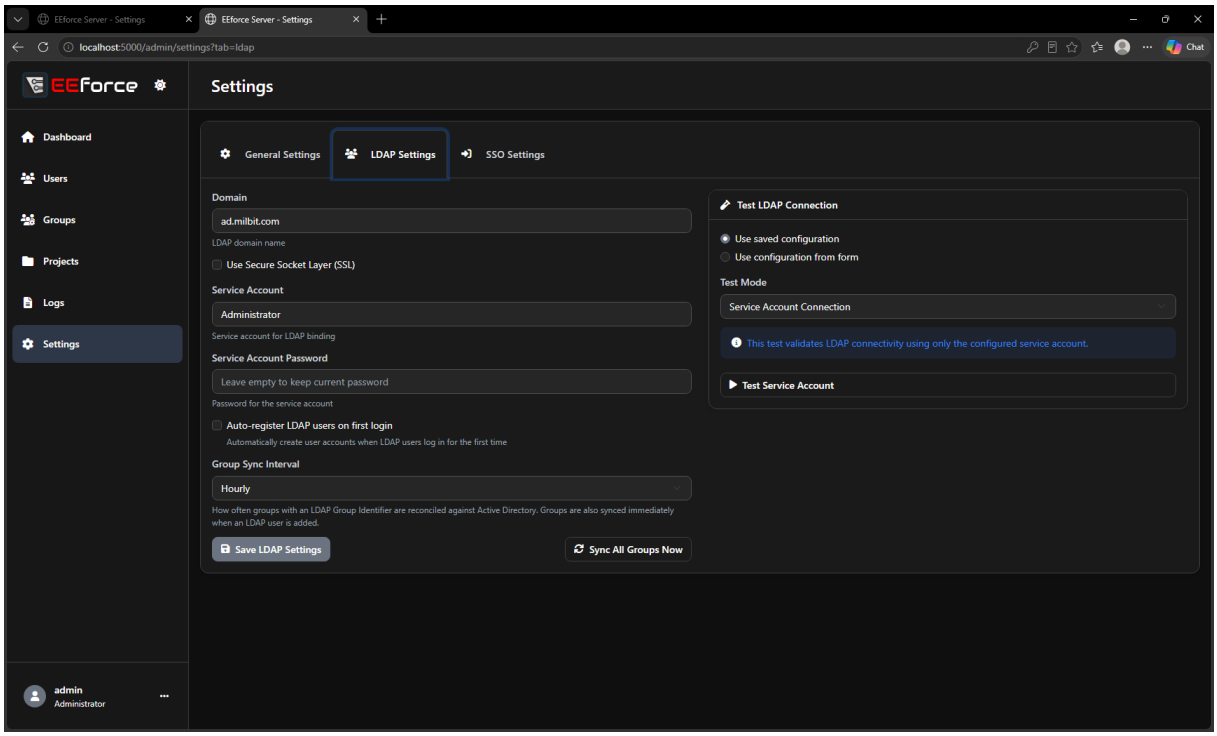
LDAP integration provides:

- **Authentication** - Users log in with their AD username and password
- **Auto-provisioning** - New user accounts are created automatically on first login (Optional)
- **Group synchronization** - EEforce groups can be linked to AD groups for automatic membership updates
- **SSL support** - Secure LDAP (LDAPS) connections

Configuration

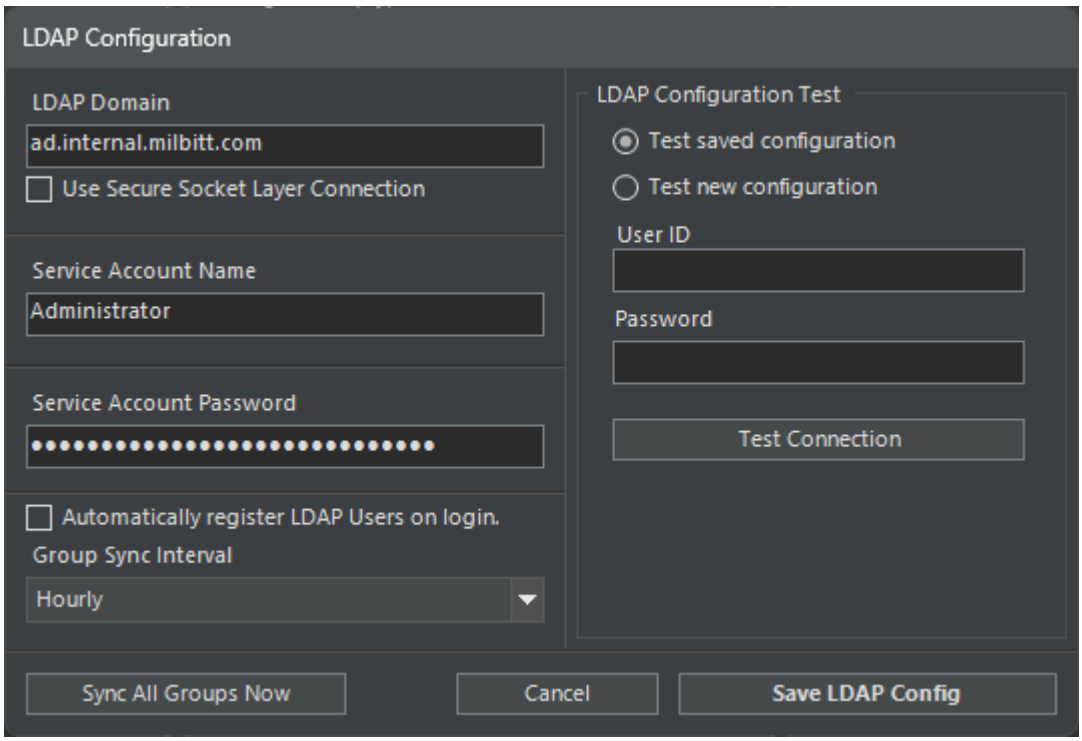
From the Web Admin Interface

Navigate to **Admin -> Settings -> LDAP Settings** tab.



From the Desktop Client

Open **Admin -> LDAP Configuration** from the menu bar.



Settings Reference

Setting	Description	Example
Domain	The LDAP/AD domain to authenticate against	`corp.example.com`
Service Account	Username of the account used to query the directory	`svc_eeforce`
Service Account Password	Password for the service account	*(stored encrypted)*
Use Secure Socket Layer (SSL)	Connect via LDAPS (port 636) instead of plain LDAP (port 389)	Enabled/Disabled
Auto-register LDAP users on first login	Automatically create an EEforce account when an unknown LDAP user logs in successfully	Enabled/Disabled

Setting	Description	Example
Group Sync Interval	The interval that will be used to automatically sync groups with LDAP server.	Hourly

::: warning Service Account Requirements The service account needs **read access** to user and group objects in Active Directory. It does not need write permissions. Use a dedicated service account with minimal privileges. :::

Setup Steps

1. Create a Service Account in AD

Create a service account in Active Directory with read permissions: - No special admin rights needed
- Set password to never expire (or manage rotation)
- Example: `svc_eeforce@corp.example.com`

2. Configure LDAP in EEforce

1. Open the web admin: `http://<server>/Admin`
2. Go to **Settings -> LDAP Settings**
3. Fill in:
   - **Domain:** Your AD domain (e.g., `corp.example.com`)
   - **Service Account:** The service account username
   - **Service Account Password:** The service account password
4. Enable **Use Secure Socket Layer** if your domain controller supports LDAPS

5. Enable **Auto-register LDAP users on first login** (recommended)

6. Click **Save LDAP Settings**

3. Test the Connection

Use the built-in test panel (available in web admin) to verify the configuration:

Test Mode	What It Checks
Service Account Connection	Validates that the service account can bind to the directory
User Lookup	Finds a specific user in AD and retrieves their display name
Group Lookup	Resolves a group identifier (DN, sAMAccountName, or CN)
List User Groups	Shows all AD groups a specific user belongs to
User Login	Performs a full authentication test with a user's credentials

> Always test with **Service Account Connection** first. If that fails, check the domain name, service account credentials, and network connectivity to the domain controller.

4. Enable Auto-Registration (Optional)

When enabled, any user who successfully authenticates against AD will automatically get an EEforce account created. This eliminates the need to manually create accounts for each team member.

If disabled, an administrator must manually create accounts and mark them as LDAP-authenticated before users can log in.

Group Synchronization

EEforce groups can be linked to AD groups. When linked, group membership is automatically synchronized based on AD membership.

How Group Sync Works

1. An administrator links an EEforce group to an AD group by setting the **LDAP Group Identifier**.
2. They can click Sync LDAP Members or wait for scheduled sync.
3. For each linked EEforce group:
    - If the user is in the corresponding AD group -> they are added to the EEforce group
    - If the user is NOT in the AD group -> they are removed from the EEforce group
4. Changes are applied immediately on login.

Linking a Group

From the Web Admin: 1. Go to **Groups** management page
2. Select or create a group
3. Set the **LDAP Group Identifier** field to one of:
- Distinguished Name: `CN=Engineering,OU=Groups,DC=corp,DC=local`
- sAMAccountName: `Engineering`
- Common Name: `Engineering`

From the Desktop Client: 1. Open **Admin -> Group Management**
2. Select a group
3. Set the LDAP Group Identifier field

The LDAP Group Identifier is matched flexibly - you can use the full Distinguished Name (DN), the sAMAccountName, or the CN. The system will try to resolve it.

Example Configuration

EEforce Group	LDAP Group Identifier	Effect
Hardware Team	`CN=HW-Engineers,OU=Teams,DC=corp,DC=local`	All AD members of HW-Engineers are added to Hardware Team

EEforce Group	LDAP Group Identifier	Effect
Project Administrators	`EEforce-Admins`	AD members of EEforce-Admins get Manager access to all projects
Project Creators	`EEforce-Creators`	AD members can create new projects

User Lifecycle

New LDAP User (Auto-Register Enabled)

1. User opens EEforce Client and enters AD credentials
2. Server authenticates against AD -> success
3. Server creates an EEforce account with:
    - User ID = AD username (sAMAccountName)
    - Display Name = AD display name
    - Marked as LDAP-authenticated
4. Group sync runs -> user is added to appropriate linked groups
5. User is logged in

Existing LDAP User

1. User enters credentials

2. Server authenticates against AD

3. User is logged in

User Leaves the Organization

When an AD account is disabled or deleted: - The user cannot authenticate anymore (login fails)
- Their EEforce account remains but is inaccessible
- An administrator can manually delete or deactivate the account

> Consider periodically reviewing user accounts in the web admin to clean up accounts for departed employees.

SSL/LDAPS

For secure connections:

1. Ensure your domain controller has a valid SSL certificate (port 636)

2. Enable **Use Secure Socket Layer** in EEforce LDAP settings

3. If using a self-signed CA, install the CA certificate on the EEforce server machine

> Plain LDAP (port 389) transmits credentials in clear text on the network. Always use LDAPS in production environments.

Troubleshooting

Issue	Possible Cause	Resolution
Service account test fails	Wrong credentials or domain	Verify domain, username, and password. Try `domain\username` format.
User lookup returns nothing	User not in expected OU	The search covers the entire domain tree; check the username spelling
Group sync not updating	LDAP Group Identifier not set	Verify the group has a valid identifier in group management
SSL connection fails	Certificate not trusted	Install the AD CA certificate on the server machine
Auto-register not working	Setting is disabled	Enable `Auto-register LDAP users on first login` in settings
Login slow	DNS resolution issues	Ensure the server can resolve the AD domain name quickly

SSO Integration (Single Sign-On)

EEforce supports Single Sign-On using the **OpenID Connect (OIDC)** protocol. This allows users to authenticate through an external Identity Provider (IdP) such as Keycloak, Azure AD (Entra ID), Okta, or any OIDC-compliant provider.

Overview

With SSO enabled: - Users click **Sign in with SSO** on the login screen
- A browser window opens to the identity provider's login page
- After successful authentication, the user is automatically logged into EEforce
- User accounts are provisioned automatically on first SSO login

---

Authentication Flow

```
1. User clicks "Sign in with SSO" in EEforce Client
2. Browser opens to Identity Provider login page
3. User authenticates with IdP (username/password, MFA, etc.)
4. IdP redirects back to EEforce with an authorization code
5. EEforce exchanges code for tokens (ID token + access token)
6. EEforce extracts user identity from the token
7. If user is new -> account is created automatically
8. User is logged in
```

::: info Protocol EEforce uses the **Authorization Code** flow (OAuth 2.0 / OIDC). The client application starts a local HTTP listener to receive the redirect callback. :::

Prerequisites

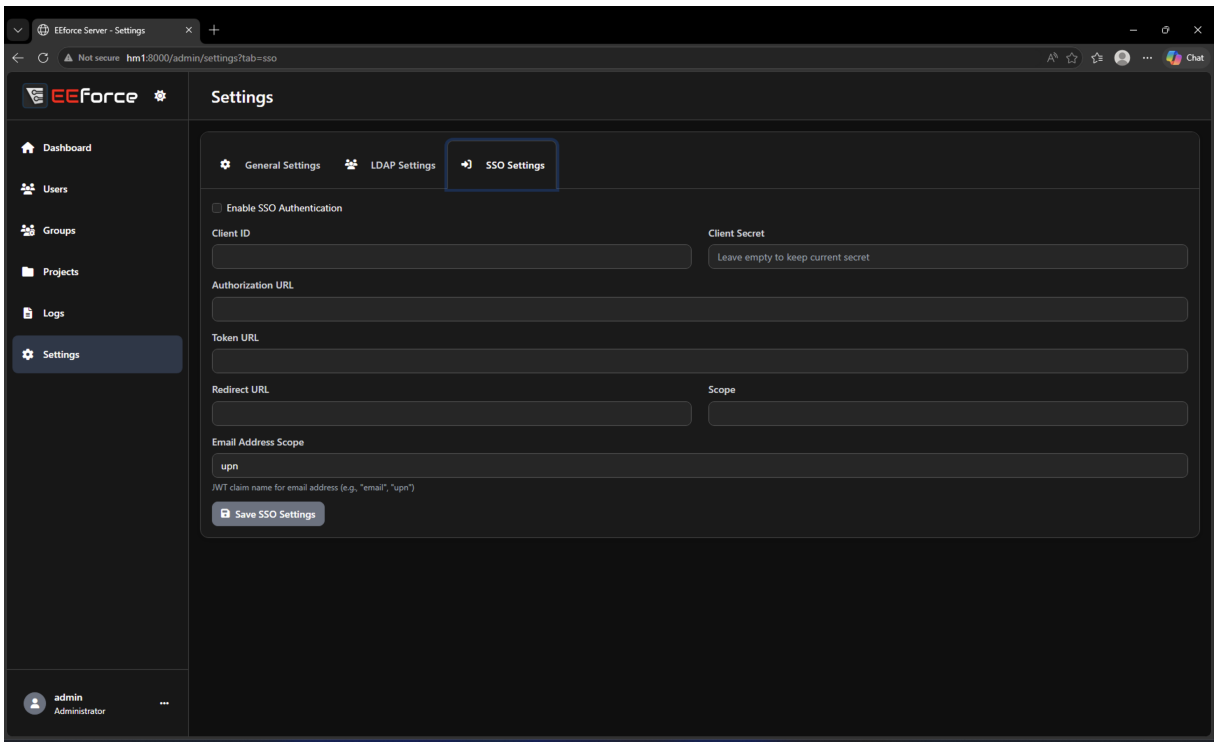
Before configuring SSO in EEforce, you need:

1. An OIDC-compliant Identity Provider (Keycloak, Azure AD, Okta, Auth0, etc.)
2. A **client application** registered in your IdP with:
   - Client ID and Client Secret
   - Redirect URI set to `http://localhost:8001/` (for desktop client callback)
   - Authorization Code grant type enabled
   - Required scopes: `openid`, `profile`, `email`

Configuration

SSO is configured exclusively from the **Web Admin Interface**.

1. Navigate to `http://<server>/Admin`
2. Go to **Settings -> SSO Settings** tab



Settings Reference

Setting	Description	Example
Enable SSO Authentication	Master switch for SSO functionality	Checked/Unchecked
Client ID	The OAuth client ID registered with your IdP	`eeforce_production`
Client Secret	The OAuth client secret	*(stored securely)*
Authorization URL	IdP's authorization endpoint	`https://idp.example.com/auth`
Token URL	IdP's token endpoint	`https://idp.example.com/token`
Redirect URL	Callback URL (must match IdP configuration)	`http://localhost:8001/`

Setting	Description	Example
Scope	OIDC scopes to request	`openid profile email`
Email Address Scope	JWT claim name for the user's email/identifier	`upn` or `email`

Setup Guide

Step 1: Register EEforce in Your Identity Provider

Keycloak Example

1. Open Keycloak Admin Console
2. Select your realm
3. Go to **Clients -> Create Client**
4. Set:
   - Client ID: `eeforce`
   - Client Protocol: `openid-connect`
   - Access Type: `confidential`
   - Valid Redirect URIs: `http://localhost:8001/*`
5. Save and note the **Client Secret** from the Credentials tab

Azure AD (Entra ID) Example

1. Open Azure Portal -> Azure Active Directory -> App registrations

2. Click **New registration**

3. Set:

   - Name: `EEforce`

   - Redirect URI: `http://localhost:8001/` (type: Public client/native)

4. After creation, go to **Certificates & secrets** and create a new client secret

5. Note the **Application (client) ID** and **Client Secret**

6. Find your endpoints under **Endpoints**:

   - Authorization URL: `https://login.microsoftonline.com/{tenant-id}/oauth2/v2.0/authorize`

   - Token URL: `https://login.microsoftonline.com/{tenant-id}/oauth2/v2.0/token`

Okta Example

1. Open Okta Admin -> Applications -> Create App Integration

2. Select **OIDC - OpenID Connect** and **Native Application**

3. Set:

   - Sign-in redirect URI: `http://localhost:8001/`

   - Grant type: Authorization Code

4. Note the Client ID and Client Secret

Step 2: Configure EEforce

1. Open Web Admin -> **Settings -> SSO Settings**

2. Check **Enable SSO Authentication**

3. Fill in:

    - **Client ID** and **Client Secret** from your IdP
    - **Authorization URL** - the IdP's `/authorize` endpoint
    - **Token URL** - the IdP's `/token` endpoint
    - **Redirect URL:** `http://localhost:8001/`
    - **Scope:** `openid profile email`
    - **Email Address Scope:** `email` (or `upn` for Azure AD)

4. Click **Save SSO Settings**

Step 3: Test

1. Open the EEforce Client
2. On the login screen, click **Sign in with SSO**
3. A browser window should open to your IdP's login page
4. Log in with valid credentials
5. The browser should show "You are logged in" and close automatically
6. The EEforce Client should now be authenticated

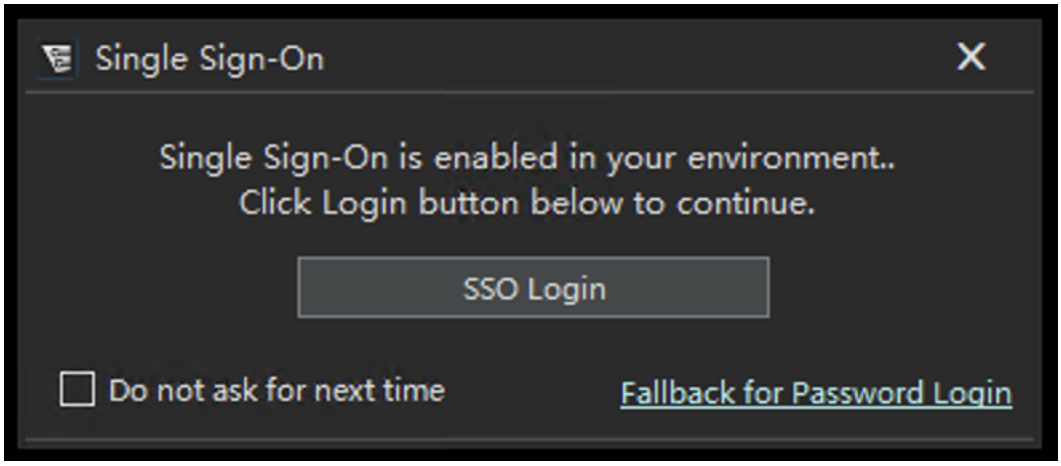
User Provisioning

When a user authenticates via SSO for the first time:

1. EEforce creates a new user account using information from the ID token:
   - **User ID** -> Subject claim (`sub`)
   - **Display Name** -> Name claim (`name`)
   - **Email** -> Claim specified by Email Address Scope setting
2. The account is marked as SSO-authenticated
3. The user is added to the system and can be assigned to groups/projects normally

SSO users cannot change their password in EEforce - authentication is always delegated to the Identity Provider.

Client Experience



The login screen shows an SSO button when SSO is enabled on the server. Users can also check **Remember me** to enable automatic SSO login on subsequent launches (skips the login dialog).

Automatic SSO Login

When enabled (via the “Remember” checkbox), the client will: 1. Skip the login dialog on next launch
2. Automatically open the browser for SSO authentication
3. Complete login without user interaction (if IdP session is still valid)

Combining SSO with Local and LDAP Authentication

SSO, LDAP, and local authentication can coexist:

User Type	How They Log In
Local users	Username + password in login dialog
LDAP users	AD credentials in login dialog
SSO users	Click “Sign in with SSO” button

A single EEforce instance can have a mix of all three user types.

Security Considerations

Aspect	Recommendation
Client Secret	Store securely; never share in plain text
Redirect URI	Use `http://localhost:8001/` (local loopback only)
Token validation	EEforce validates the JWT signature and expiration
HTTPS	Use HTTPS for all IdP endpoints
Session duration	Controlled by EEforce’s token expiry, independent of IdP session

---

Troubleshooting

Issue	Possible Cause	Resolution
Browser opens but login fails	Incorrect Authorization URL	Verify the URL matches your IdP's OIDC discovery document
" "Authorization code is missing" "	Redirect URI mismatch	Ensure the redirect URI in EEforce matches exactly what's configured in the IdP
User created with wrong ID	Wrong claim mapped	Check Email Address Scope setting (try `email`, `upn`, or `preferred_username`)
" "Error: invalid_client" "	Wrong Client ID or Secret	Verify credentials match the IdP's client configuration
Browser shows error from IdP	Grant type not allowed	Ensure Authorization Code flow is enabled for the client in the IdP
SSO button not showing	SSO not enabled on server	Enable SSO in Web Admin -> Settings -> SSO Settings
Auto-login not working	Remember not checked; or IdP session expired	Re-check remember option; re-authenticate with IdP