User Impersonation

1. Introduction

The **User Impersonation plugin for Forma LMS** allows authorized administrators to temporarily access the platform as another user.

The plugin is intended for support and debugging activities: an administrator can verify what a specific user sees in the LMS, reproduce access issues, and check course visibility or navigation problems without asking for the user's credentials.

During impersonation, the platform shows a visible banner and prevents learning tracking from being written as the impersonated user.

2. Installation and Activation

1. Go to **Administration > Plugin > Plugin Management**.
2. Locate **User Impersonation** in the plugin list.
3. Click **Install** and then **Activate**.

When activated, the plugin registers:

- the impersonation controller;
- the **Impersonation Log** menu under the management area;
- the permission role used to enable impersonation actions.

3. Plugin Configuration

No external API credentials are required.

After activation, access depends on the administrator level and on the standard Forma LMS visibility rules:

- **Super administrators** can impersonate standard users and administrators, but not other super administrators.

- **Administrators** can impersonate visible standard users only.
- **Administrators** cannot impersonate other administrators or super administrators.
- **Users** cannot impersonate anyone.

The plugin requires Forma LMS **4.2 or later**.

4. User Impersonation from User Management

4.1 Starting an Impersonation Session

Within the user management area:

1. Open **Administration > Users > User Management**.
2. Find the user to verify.
3. Click the **Impersonate** action available on the user row.
4. Confirm the operation.

After confirmation, Forma LMS switches the current session to the selected user and redirects the administrator to the LMS area.

The administrator can then navigate the platform with the same visibility and permissions as the selected user.

5. Active Impersonation Session

While impersonation is active, Forma LMS displays a red banner across the interface.

The banner shows the impersonated user and includes the **Stop Impersonation** action.

During the session, the plugin:

- blocks learning tracking writes, so course progress is not altered;
- bypasses forced password renewal for the impersonated user;
- bypasses concurrent access checks, so the real user's session is not invalidated;
- prevents nested impersonation sessions.

6. Stopping Impersonation

To return to the original administrator session:

1. Click **Stop Impersonation** in the banner.
2. The plugin restores the original administrator user.
3. Forma LMS redirects back to user management.

The stop action is protected by a token and the session ID is regenerated when impersonation starts and stops.

If the session expires while impersonation is active, the plugin writes a timeout entry in the audit log.

7. Reports and History

The plugin provides an **Impersonation Log** page for super administrators.

The log shows:

- date and time of the action;
- administrator username;
- impersonated username;
- action type: start, stop, or timeout;
- IP address.

The log can be filtered by administrator and by impersonated user.

8. Security Notes

The plugin is designed for support and troubleshooting, not for normal user activity.

Main safeguards:

- no impersonation of yourself;
- no impersonation of super administrators;
- no administrator-to-administrator impersonation for standard administrators;
- CSRF-protected stop action;
- session regeneration on start and stop;
- visible banner during the whole session;
- audit log for traceability;

- tracking protection to avoid corrupting learning data.

Revision #3
Created 2026-06-26 07:02:45 UTC by Giuseppe Nucifora
Updated 2026-06-26 09:33:28 UTC by Giuseppe Nucifora