Login & Access Audit / Session Monitor

User Guide

Odoo 18 / 19 Community & Enterprise

Security & Audit

pokutsoft.com

support@pokutsoft.com

Table of Contents

1. Overview

2. Installation

3. Configuration

4. Step-by-step Walkthrough

5. Feature Reference

6. Tips, Troubleshooting & FAQ

7. Support

Technical reference

Technical name	gb_login_access_audit_session_monitor
Version	18.0.1.0.0
Odoo series	18.0 and 19.0
Category	Security & Audit
Depends on	base, mail
Licence	LGPL-3
Data models	gb.access.audit.config, gb.ip.geo.range, gb.login.block, gb.login.event, gb.user.session

1. Overview

Give administrators full visibility over who is signing in to your Odoo, from where, and what happens when access fails. Every successful and failed login is recorded with IP, user agent, resolved country and timestamp.

Failed-login throttling flags a source after repeated failures, a live session register lets you force-logout users, and a geo-anomaly detector escalates sign-ins from never-before-seen countries.

Who is it for?

- Administrators and security managers responsible for access control.
- Organisations gathering access-control evidence.
- Anyone who needs to know who is logged in right now.

UK angle

The login event log and lockout register are designed to provide the access-control evidence expected by the UK Cyber Essentials scheme.

2. Installation

The module installs like any standard Odoo app. You need the Administration / Settings access right to install apps.

- Enable developer mode is not required for normal use.
- Open Apps from the main menu.
- Click Update Apps List (top menu) so Odoo re-reads the addons folder.
- Remove the default Apps filter and search for "Login & Access Audit / Se" (technical name **gb_login_access_audit_session_monitor**).
- Click Install. The dependencies (base, mail) are installed automatically.

After installation a new top-level menu becomes available (see Configuration below). On a multi-company database, install once; the records are company-aware where the underlying models are.

3. Configuration

Open Access Audit > Configuration > Settings (gb.access.audit.config) to set the failure threshold, the time window and which managers receive alerts (the Anomaly & Sessions and Notifications options).

Under Configuration > IP → Country Ranges maintain the IP-to-country table (gb.ip.geo.range) used to resolve login locations.

A daily security digest cron summarises failures, new locations and locked sources - no third-party service is contacted.

4. Step-by-step Walkthrough

The flow below uses the real menus, buttons and statuses shipped with the module. Labels are quoted exactly as they appear in the interface.

4.1 Review login activity

1. Open Access Audit > Login Events.
2. Use the Failures, Success and Anomalies filters to focus, and read the Result and Country columns.

4.2 Handle a lockout

1. Open Access Audit > Lockouts to see blocked sources.
2. Investigate the source, then click Unblock when satisfied it is legitimate.

4.3 Monitor and end sessions

1. Open Active Sessions for the live list of authenticated users.
2. Select a session and use Force Logout, or run the Force Logout wizard to end every session of a user.

4.4 Respond to a geo-anomaly

1. Anomalous sign-ins (new or distant countries) are flagged automatically and an alert activity is raised to security managers.
2. Open the flagged event, confirm with the user, and unblock or force-logout as appropriate.

5. Feature Reference

Every feature below is implemented in the module; the model behind each one is named in brackets so administrators can locate it.

Login event log

Every success and failure captured with IP, user agent, country and timestamp (gb.login.event).

Failed-login throttling & lockout

After N failures in a window the source is flagged and an alert is raised; review and Unblock from the lockout register (gb.login.block).

Active session register

Live list of authenticated sessions with last-seen and IP, plus single or all-session force-logout (gb.user.session, gb.force.logout.wizard).

Geo-anomaly detection

Sign-ins from a never-before-used or distant country are marked anomalous and escalated.

IP → country ranges

A configurable IP-range table resolves login locations entirely inside Odoo (gb.ip.geo.range).

Daily security digest

A cron summarises failures, new locations and locked sources for managers.

6. Tips, Troubleshooting & FAQ

Q: Does this contact an external geo-IP service?

A: No. Country resolution uses the configurable IP → Country Ranges table inside Odoo.

Q: How many failures trigger a lockout?

A: It is configurable - set the threshold and window in Configuration > Settings.

Q: Can I log a user out remotely?

A: Yes - select their session and use Force Logout, or end all their sessions with the wizard.

Q: What counts as a geo-anomaly?

A: A sign-in from a country the user has never used, or two distant countries within a short window.

Q: Who gets alerted?

A: The security managers you nominate in the notification settings.

Q: Is this enough for Cyber Essentials?

A: It provides the login and access-control evidence; certification also covers other controls.

7. Support

We are happy to help you get the most out of this app.

Email	support@pokutsoft.com
Catalogue	https://pokutsoft.com
Author	Pokutsoft
Licence	LGPL-3
Supported	Odoo 18.0 and 19.0

When reporting an issue please include your Odoo version, the module version (18.0.1.0.0), the menu/screen you were on and the exact error text. This module performs all processing inside your Odoo instance unless an external connector is explicitly configured by you.