Two-Factor / SSO Enforcer

Enforce 2FA, BYOK SAML/OIDC SSO and a login policy (Cyber Essentials)

User Guide · Odoo 18 / 19 Community
Category: Security & Audit
Technical name: gb_two_factor_sso_enforcer
Published by pokutsoft.com · https://pokutsoft.com
support@pokutsoft.com

Table of Contents

1. Overview
2. Installation
3. Configuration
4. Step-by-Step Usage
5. Feature Reference
6. Tips, Troubleshooting & FAQ
7. Support

This guide documents only features implemented in the module. Menu paths, field names and button labels match the application exactly.

1. Overview

Two-Factor / SSO Enforcer hardens Odoo logins. It enforces TOTP two-factor authentication for chosen user groups, connects to your own SAML or OIDC identity provider (BYOK), and applies a login policy covering password strength, ageing, lockout and IP allow-listing — all written to an audit log.

Single sign-on is Enterprise-only, so Community customers cannot meet modern security baselines. This module provides Community-friendly 2FA enforcement, BYOK SSO and policy controls that support frameworks such as UK Cyber Essentials.

Who it is for

- Administrators tightening authentication security.
- Organisations pursuing Cyber Essentials or similar baselines.
- Teams wanting SSO via their own IdP on Community.

UK note

Helps demonstrate the access-control and secure-configuration controls expected by UK Cyber Essentials (multi-factor authentication and password policy).

Key capabilities at a glance

- 2FA enforcement — TOTP enrolment with recovery codes, enforced per group with a grace period.
- Login policy — Password length/strength/ageing, failed-attempt lockout and IP allow-list.
- BYOK SSO — OIDC (discovery parse) and SAML 2.0 (metadata parse) using your own identity provider.
- Account lockout — Tracks failed attempts and locks the account for a configurable period.
- Audit log — Records 2FA, recovery, lockout, policy/IP block, password reject and enrolment events.
- Recovery codes — Hashed emergency codes generated at enrolment.

2. Installation

Install from the Odoo Apps menu with Administrator access; dependencies are pulled in automatically.

1. Open Apps from the main Odoo menu.
2. Click Update Apps List to refresh the catalogue.
3. Search for “Two-Factor / SSO Enforcer”.
4. Click Install on the matching card.
5. The Auth Security menu appears once installation finishes.

Technical name	gb_two_factor_sso_enforcer
Depends on	base, mail
Odoo versions	18.0 and 19.0
Licence	LGPL-3

3. Configuration

Define Login Policies and optional SSO Providers under Auth Security; review the Audit Log for events.

Login policy

- Create a policy and tick enforce 2FA, then select the groups it applies to and a grace period in days.
- Set password rules: minimum length, minimum strength score and maximum age in days.
- Set max failed attempts and a lockout duration, plus an optional IP allow-list.

SSO providers (BYOK)

- Add an OIDC provider with its client ID and discovery URL — Parse Discovery fills the endpoints.
- Or add a SAML 2.0 provider and Parse SAML Metadata to read the entity ID and SSO URL.
- Enable/disable each provider; a validation message confirms the configuration.

4. Step-by-Step Usage

Users enrol in 2FA; the policy then enforces it and the audit log records every event.

Enrol a user in 2FA

1. From the user, Start Enrolment to generate a TOTP secret and recovery codes.
2. Scan the secret in an authenticator app and Confirm Enrolment with a code.
3. Recovery codes are stored hashed for emergency access; 2FA can be disabled by an admin if needed.

Enforce the policy

1. Assign the policy to the relevant groups; users without 2FA are pushed to enrol within the grace period.
2. Failed logins increment the attempt counter; exceeding the limit locks the account for the lockout period.
3. Logins from outside the IP allow-list are blocked.

Audit and review

1. Open the Audit Log to see 2FA successes/failures, recovery-code use, lockouts, policy and IP blocks, rejected passwords and enrolments, each with user, login, IP and detail.
2. Use the log as evidence for security reviews.

5. Feature Reference

Each row corresponds to a real menu, model or wizard in the module.

2FA enforcement	TOTP enrolment with recovery codes, enforced per group with a grace period.
Login policy	Password length/strength/ageing, failed-attempt lockout and IP allow-list.
BYOK SSO	OIDC (discovery parse) and SAML 2.0 (metadata parse) using your own identity provider.
Account lockout	Tracks failed attempts and locks the account for a configurable period.
Audit log	Records 2FA, recovery, lockout, policy/IP block, password reject and enrolment events.
Recovery codes	Hashed emergency codes generated at enrolment.

6. Tips, Troubleshooting & FAQ

Q. Which 2FA method is used?
A. Time-based one-time passwords (TOTP) compatible with standard authenticator apps, with hashed recovery codes.

Q. Can I require 2FA only for admins?
A. Yes. A policy enforces 2FA for the groups you select, with a grace period for enrolment.

Q. Do you host the SSO identity provider?
A. No. It is BYOK — you connect your own OIDC or SAML provider; the module parses your discovery URL or SAML metadata.

Q. What happens after too many failed logins?
A. The account is locked for the configured lockout period and the event is written to the audit log.

Q. Can I restrict logins by IP?
A. Yes, add ranges to the policy's IP allow-list; logins from other addresses are blocked.

Q. Does this help with Cyber Essentials?
A. It supports the MFA and password-policy expectations and provides an audit trail as evidence.

7. Support

We are happy to help with installation, configuration and usage questions.

Email	support@pokutsoft.com
Apps & catalogue	https://pokutsoft.com
Module	Two-Factor / SSO Enforcer (v18.0 / v19.0)

When contacting support, please include your Odoo version, the module version and a short description of the steps that led to the issue.