Go-SyncFlow 统一身份同步与管理平台 Unified Identity Sync & Management

Platform

文档版本 v3.0

更新日期 2026-02-09

文档状态 正式发布

本文档为系统自动生成，内容随版本迭代持续更新

目　录

Contents

1 Go-SyncFlow 统一身份同步与管理平台 - 系统使用手册

版本：v3.0 | 更新日期：2026-02-09

1.1 目录

1.2 一、系统登录

1.2.1 1.1 本地账号登录

1. 打开浏览器，访问系统地址（如 http://服务器 IP:8080）
2. 输入用户名和密码
3. 点击「登录」按钮

默认管理员账号：admin / Admin@2024（首次登录建议修改密码）

1.2.2 1.2 SSO 免登

系统支持 IM 平台内免登（钉钉/飞书/企微），在对应工作台中打开应用时自动识别身份登录。SSO 免登需在「上游同步 → IM 平台连接器」中开启对应的 SSO 开关。

> 注意：登录页面不显示第三方登录按钮，SSO 免登仅在 IM 平台内部自动触发。

1.2.3 1.3 忘记密码

1. 在登录页点击「忘记密码」
2. 输入用户名
3. 系统根据消息策略显示可用的验证方式（短信/钉钉等）
4. 选择验证方式，获取验证码
5. 输入验证码和新密码完成重置

1.3 二、个人中心

登录后点击右上角头像进入个人中心，可进行：

- **查看个人信息**：用户名、昵称、邮箱、手机号、所属群组、角色
- **修改密码**：输入当前密码和新密码
- **编辑个人资料**：修改昵称、邮箱、手机号、头像

> 注意：通过 IM 平台同步的用户，部分字段可能为只读状态。

1.4 三、系统首页（仪表盘）

管理员登录后默认进入仪表盘页面，展示：

- **用户统计**：总数、活跃数、禁用数、今日新增
- **同步状态**：上游/下游同步器运行状态
- **最近登录**：最新登录记录
- **系统监控**：CPU、内存、磁盘使用率
- **LDAP 状态**：服务运行状态、Samba 支持状态

1.5 四、用户管理

1.5.1 4.1 用户列表

- 支持按关键词搜索（用户名/昵称/邮箱/手机号）
- 支持按群组/状态/来源筛选
- 支持批量操作：启用/禁用/删除

1.5.2 4.2 新增用户

1. 点击「新增用户」按钮
2. 填写必填字段：用户名、昵称、密码
3. 可选字段：邮箱、手机号、所属群组、角色
4. 点击「确定」保存

> 新建的本地用户默认角色为”普通用户”。

1.5.3 4.3 编辑用户

- 点击用户操作栏的「编辑」按钮
- 修改用户信息后点击「确定」保存
- IM 平台同步的字段会标记为只读

1.5.4 4.4 重置密码

- 管理员可在操作栏点击「重置密码」
- 根据消息策略，新密码可通过短信/钉钉等渠道通知用户
- 密码会自动同步到 LDAP（包括 Samba NT Hash）

1.5.5 4.5 导出用户

- 点击用户列表上方的「导出用户」按钮
- 导出全部本地用户为 Excel 文件（.xlsx）
- 导出字段：ID、用户名、姓名、手机号、邮箱、部门、状态、来源、创建时间
- 需要 `user:export` 权限

1.5.6 4.6 群组管理

- 支持多级树形群组结构
- 顶层群组直接显示在”本地用户”下，无”根部门”概念
- IM 平台同步会自动创建对应的部门群组（钉钉根部门不会创建为本地群组）
- 可手动调整用户所属群组

1.6 五、上游同步

上游同步用于从外部系统拉取用户数据到本地。

1.6.1 5.1 上游连接器

支持的连接器类型

类型	说明
钉钉	需配置 AppKey、AppSecret、AgentID
企业微信	需配置 CorpID、Secret
飞书	需配置 App ID、App Secret
WeLink	需配置 Client ID、Client Secret
LDAP/AD	需配置 Host、Port、Bind DN、BaseDN
MySQL	需配置 Host、Port、用户名、密码、数据库名
PostgreSQL	同上
SQL Server	同上
Oracle	同上
SQLite	需配置数据库文件路径

创建连接器

1. 进入「上游同步」页面
2. 切换到「上游连接器」标签
3. 点击「新增连接器」
4. 选择类型并填写连接参数
5. 点击「测试连接」验证
6. 保存连接器

IM 平台特有配置

- **用户匹配字段**：决定如何匹配已有本地用户（用户名/手机号/邮箱/UserID）
- **用户名生成规则**：新用户的用户名生成方式
  - 中文转拼音（重名加数字）
  - 邮箱前缀

  - 手机号
  - 完整邮箱
  - IM 平台 UserID
- **SSO 免登开关**：启用/禁用该平台的单点登录
- **自动注册**：是否允许免登时自动创建本地账号

1.6.2 5.2 同步规则

创建规则

1. 切换到「同步规则」标签
2. 点击「新增规则」
3. 选择关联的连接器
4. 配置触发方式：
   - **手动**：仅通过界面手动触发
   - **定时**：
     - 定点时间：可设置多个每日触发时间（如 10:30、14:00）
     - 固定间隔：每 N 分钟触发一次
5. 保存规则

属性映射

1. 在规则列表中点击「映射」按钮
2. 查看/编辑属性映射表
   - **上游属性（源）**：上游系统的字段名（中文标签下拉选择）
   - **本地属性（目标）**：本地用户的字段名（中文标签下拉选择）
   - **类型**：直接映射 / 转换
   - **转换规则**：中文转拼音、邮箱前缀、手机号等
3. 可添加/删除/恢复默认映射
4. 点击「保存映射」

> 创建新规则时会自动生成默认映射。连接器设置中的”用户名生成规则”与映射中的 username 转换规则是双向同步的。

变更检测（数据库上游） 数据库类型的上游连接器支持变更检测：1. 启用变更检测 2. 配置检测间隔（分钟）3. 指定时间戳字段名（如 `updated_at`）4. 系统定期查询该字段发现变更记录并触发同步

1.6.3 5.3 手动同步

- 在规则列表中点击「同步」按钮触发单条规则
- 同步结果实时展示（成功/失败/跳过数量）

1.7 六、下游同步

下游同步用于将本地用户数据推送到外部目标系统。

1.7.1 6.1 下游连接器

支持类型：LDAP/AD、MySQL、PostgreSQL、SQL Server、Oracle

配置方式与上游连接器类似，但方向为”本地 → 外部”。

1.7.2 6.2 同步规则

- 触发方式：手动 / 事件驱动 / 定时（定点时间或固定间隔）
- 事件驱动：本地用户发生变更时自动触发

1.7.3 6.3 属性映射

下游属性映射将本地字段映射到目标系统字段：

映射方式	说明
直接映射	本地字段值直接写入目标字段
转换	通过转换规则处理后写入
常量	写入固定值
表达式	使用表达式计算结果

常用转换规则：

规则	说明
提取中文姓氏	从姓名中提取姓
提取中文名字	从姓名中提取名
密码转 Unicode（AD）	将密码转为 AD 要求的 Unicode 格式

规则	说明
状态转账户控制（AD）	将启用/禁用状态转为 AD UAC 值
追加域名后缀	在值后面追加 @domain.com
中文转拼音	将中文转为拼音

1.8 七、同步器管理

> 注意：同步器管理为旧版下游同步功能，建议使用新的”下游同步”模块。

同步器支持将本地用户同步到 AD/LDAP 和数据库。操作方式：

1. 配置连接参数
2. 点击「测试连接」
3. 点击「立即同步」执行
4. 在同步日志中查看结果

1.9 八、角色管理

1.9.1 8.1 角色列表

系统内置两个默认角色：- **超级管理员**：拥有所有权限 - **普通用户**：仅限个人中心和基础功能

1.9.2 8.2 创建角色

1. 点击「新增角色」
2. 填写角色名称和编码
3. 勾选权限项
4. （可选）配置角色布局：隐藏特定菜单、设定默认登录页面
5. 保存角色

1.9.3 8.3 权限体系

权限	说明
user:view	查看用户列表
user:create	创建用户
user:edit	编辑用户
user:delete	删除用户
user:reset_password	重置用户密码
user:enable_disable	启用/禁用用户
user:assign_role	分配角色
group:create	创建群组
role:*	角色管理权限
log:*	日志查看权限
settings:*	系统设置权限
sync:*	同步管理权限
notify:*	通知管理权限
security:*	安全管理权限

1.9.4 8.4 多角色合并

当用户拥有多个角色时，系统自动合并所有角色的权限和布局配置：- 权限：取所有角色权限的并集 - 布局：菜单项只要任一角色允许即显示

1.10 九、日志管理

1.10.1 9.1 系统日志

登录日志和操作日志已合并为统一的「系统日志」页面，精简展示：

- **时间**：日志产生时间
- **用户**：操作用户名
- **类型**：登录 / 操作（标签区分）
- **描述**：简要概述，登录日志显示”登录成功/登录失败: 原因”，操作日志显示”模块 - 操作:

目标”
- **状态**：成功/失败
- **IP**：来源 IP 地址

支持按类型（登录/操作）、关键词、日期范围筛选。

1.10.2 9.2 同步日志

记录每次同步执行的详情，支持区分同步方向：

- **方向**：上游同步（IM/LDAP/数据库 → 本地）/ 下游同步（本地 → AD/LDAP/数据库），以标签区分
- **触发方式**：手动/定时/事件
- **事件**：全量同步/用户创建/用户更新/密码修改等
- **状态**：成功/部分成功/失败
- **概要**：同步结果摘要，展开可查看详细信息

支持按方向、事件类型、状态、日期范围筛选。

1.10.3 9.3 API 调用日志

记录每次 API 调用：请求方法、路径、调用者、IP、耗时、状态码、请求/响应摘要

1.10.4 9.4 日志设置

在「日志设置」页面配置：- **保留天数**：各类日志的保留时间（如 30 天、90 天）- **清理策略**：每日定时清理过期日志 - **清理时间**：可配置每日清理执行的时间点

1.11 十、通知管理

1.11.1 10.1 通知渠道

支持四种通知渠道：

渠道	配置项
邮件	SMTP 服务器、端口、用户名、密码、TLS 开关
短信	选择服务商、配置 AccessKey/Secret、签名、模板 ID
Webhook	URL、签名方式（HMAC-SHA256/Token）、Header
钉钉工作通知	AppKey、AppSecret、AgentID

1.11.2 10.2 消息模板

消息模板定义各场景通知消息的内容格式。模板存在即生效，删除后对应场景的通知将无法发送。

- **内置模板**：系统预置，不可删除但可编辑内容
- **自定义模板**：用户创建，可自由编辑和删除
- **账号开通通知**：IM 平台同步创建新用户时，自动通过所有已启用的通知渠道发送初始密码，无需额外配置消息策略

支持变量占位符：{{username}}、{{nickname}}、{{password}}、{{code}}、{{department}}、{{time}}、{{app_name}}、{{ip}}

1.11.3 10.3 消息策略

配置”消息类型 → 通知渠道”的映射：

消息类型	说明
密码重置验证码	忘记密码时发送验证码
安全告警	异常登录、暴力破解等告警
账号变更通知	密码修改、账号状态变更
新用户通知	新用户创建时通知初始密码

支持全局策略和群组级策略（群组策略优先级更高）。

1.12 十一、规则与策略

1.12.1 11.1 密码策略

配置密码复杂度要求：- 最小长度 - 必须包含：大写字母、小写字母、数字、特殊字符 - 密码过期天数

1.12.2 11.2 登录策略

- 登录失败锁定次数
- 锁定时长
- IP 锁定策略

1.12.3 11.3 告警规则

配置安全告警触发条件和通知方式。

1.13 十二、系统设置

1.13.1 12.1 界面设置

- 系统名称（显示在页面标题和登录页）
- Logo 自定义
- 版权信息

1.13.2 12.2 功能设置

- 用户注册开关
- 默认角色配置

1.14 十三、LDAP 服务

1.14.1 13.1 基本配置

配置项	说明
启用开关	开启/关闭 LDAP 服务
端口	LDAP 端口（默认 389）
TLS 端口	LDAPS 端口（默认 636）
Base DN	根 DN（如 dc=example,dc=com）
域名	域名标识
管理员 DN/密码	完全访问权限
只读账号 DN/密码	只读查询权限

1.14.2 13.2 Samba 支持

默认启用。启用后：- 用户条目自动包含 sambaSamAccount objectClass - 自动生成 sambaSID、sambaNTPassword 属性 - 自动创建 sambaDomain 条目 - 密码变更自动更新 NT Hash

群晖 NAS 对接

1. 确认 LDAP Samba 已启用

2. 群晖 DSM → 控制面板 → 域/LDAP → LDAP
3. 填写 LDAP 服务器地址和 Base DN
4. 使用管理员或只读账号 Bind
5. 启用 LDAP 服务器的 Samba 架构
6. 映射 LDAP 用户/群组到群晖本地

1.15 十四、安全中心

1.15.1 14.1 IP 管理

- 全局 IP 白名单/黑名单
- 支持单 IP 和 CIDR 网段
- API Key 级别的独立 IP 限制

1.15.2 14.2 会话管理

- 在线用户列表
- 可强制踢出用户会话

1.15.3 14.3 安全事件

- 查看所有安全事件记录
- 支持按类型、严重等级筛选

1.16 十五、API 密钥管理

1.16.1 15.1 创建 API Key

1. 进入「API 密钥管理」页面
2. 点击「创建密钥」
3. 填写名称、备注
4. 可设置 IP 白名单/黑名单
5. 系统自动生成 AppID 和 AppKey
6. **请妥善保存 AppKey，关闭对话框后无法再次查看**

1.16.2 15.2 使用方式

```
# 通过请求头
X-App-ID: your-app-id
X-App-Key: your-app-key
```

```
# 或通过 URL 参数
GET /api/open/users?app_id=xxx&app_key=xxx
```

1.16.3 15.3 管理操作

- 启用/禁用密钥
- 编辑备注和 IP 限制
- 删除密钥

1.17 十六、文档中心

1.17.1 16.1 在线查看

进入管理后台的「文档中心」页面，可在线查看系统文档。

1.17.2 16.2 下载文档

点击文档卡片上的「下载」或「预览」按钮：

文档	说明
技术架构文档	系统功能说明、代码结构、数据库设计
系统使用手册	所有功能模块的操作指南
API 接口文档	完整的 REST API 调用文档

文档格式为 PDF，支持离线查看和打印。