Apusic 金蝶天燕

生成时间：2026-05-19

操作指南

金蝶Apusic统一身份管理

版权声明

本文档所涉及的软件著作权、版权等知识产权已依法进行了注册，由金蝶天燕云计算股份有限公司合法拥有。受《中华人民共和国著作权法》《计算机软件保护条例》《知识产权保护条例》和相关国际版权条约、法律、法规以及其它知识产权法律和条约的保护。未经授权许可，不得非法使用。

免责声明

本文档包含的版权信息由金蝶天燕云计算股份有限公司合法拥有，受法律的保护，金蝶天燕云计算股份有限公司对本文档可能涉及到的非金蝶天燕云计算股份有限公司的信息不承担任何责任。在法律允许的范围内，您可以查阅并仅能够在《中华人民共和国著作权法》规定的合法范围内复制和打印本文档。任何单位和个人未经金蝶天燕云计算股份有限公司书面授权许可，不得使用、修改、再发布本文档的任何部分和内容，否则将被视为侵权，金蝶天燕云计算股份有限公司有依法追究其责任的权利。

本文档如有更新，不另行通知。对本文档中的问题您可向金蝶天燕云计算股份有限公司告知或查询。未经本公司明确授予的任何权利均予保留。

商标声明

Apusic是深圳市金蝶天燕云计算股份有限公司向中华人民共和国国家商标局申请注册的注册商标，注册商标专用权由金蝶天燕合法拥有，受法律保护。未经金蝶天燕的书面许可，任何单位及个人不得以任何方式或理由对该商标的任何部分进行使用、复制、修改、传播、抄录或与其它产品捆绑使用销售。凡侵犯金蝶天燕商标权的，金蝶天燕将依法追究其法律责任。本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

目录

1 产品概述

产业互联网进行到下半场，企业在数字化转型的大背景下，通过互联网信息技术构建了自己的业务系统。如有面向企业内部沟通的IM系统，有面向企业效率管理的ERP系统，有管理供应链的CRM系统，等等。随着后续国家对数字城市、数字企业的大力支持，可以预见未来的企业数字资产一定是企业的核心竞争力之一。那么作为互联网企业方案提供商，如何保证数字资产的安全性、扩展性、追溯性、灵活性，是互联网下半场的议题。

从现实情况来看，企业面临降本增效的目标。数字化不仅仅是将原有的线下业务搬到线上来，数字化是帮助企业突破自身的生产瓶颈，让企业通过统一标准，统一流程去规范化自己的生产行为，从而实现增效的目标。但是数字化的最大问题就是这些系统的运维成本的增加，如何统一的管理这些系统是企业现在面临的难题。当前企业主要面临以下几个问题：

1. 安全风险：多个系统，多套数据，登录秘钥容易丢失
2. 管理风险：维护成本较高，人员离职后存在僵尸账号
3. 体验风险：多系统，多账号，多密码，用户使用繁琐

2 系统架构

2.1 架构设计

AIDM采用微服务框架，系统采用前后端分离架构，前端使用React进行开发，后端基于开源单点登录认证系统Maxkey进行开发。 idm服务端至上而下分为接口层、业务组件、基础组件等部分。 接口层分为面向第三方调用的身份认证接口，面向管理页面的管理端接口； 业务组件层分为身份认证、第三方验证、网关、协议解析、持久化几个分模块，在每个模块中进行业务代码实现； 基础组件引用了kaptcha进行验证码生成，Quartz处理定时任务，JustAuth、nimbus-jose-jwt、opensaml做oauth、jwt、saml协议的处理，google tink、BouncyCastle提供加解密，caffeine处理缓存。使用mybatis通过配置化的方式去支持不同数据库的切换，如对国产数据库与缓存的支持。

2.2 系统部署

系统组件架构图如下：

AIDM应用采用无状态的的实现方式，应用容器化发布以屏蔽对运行环境的依赖，故可以轻松支持多种部署方式，以下是拟支持的部署方式：

ALL-IN-ONE

以上所有组件均已容器化单实例的方式运行；通过docker-compose+ 的方式打包集成容器镜像，方便的在docker环境中一键部署，在中小微企业项目中可以采用此方式；环境要求 8 cpu+64G内存+512G硬盘。物理机集群上高可用部署：环境要求

1+1 部署

数据库和缓存采用主从方式部署。环境要求： 2+ 服务器，服务器配置：8 cpu+64G内存+512G硬盘。

Cluster部署数据库和缓存采用cluster模式部署，环境要求： 3+服务器，服务器配置：8 cpu+64G内存+512G硬盘。

K8S集群内部署

其中Redis，Nacos，Minio采用StatefulSet的方式部署，应用采用deployment的方式实现自动扩缩容。整个项目以helm包的方式提供，实现在云环境中一键部署。

3 核心能力

金蝶天燕统一身份管理系统（Apusic Identity Management，简称AIDM）是一款企业门户产品，通过给企业提供应用认证、资源权限、用户管理、权限分配、审计日志等一系列的功能，构建统一的身份认证平台，帮助企业打通不同系统间的信息孤岛，实现在用户侧、企业侧、运维侧的数据治理。

AIDM统一身份认证管理系统通过提供应用认证、资源权限、用户管理、权限分配、审计日志等一系列的功能，搭建标准的身份管理平台，帮助企业打通不同系统间的信息孤岛，构建统一的身份管理体系。其中：

应用认证：通过提供单点登录（SSO）或第三方认证的功能，优化用户的登录体验，解决一人多户的困扰。

资源管理：统一整理接入系统的资源，通过统一的授权出口，对登录系统进行不同颗粒度的资源管理，包括登录入口等粗颗粒度的管理和页面按钮等细颗粒度的管理。

用户管理：通过对所有系统的使用人员回收，由AIDM统一为用户分配使用权限，解决不同系统间管理混乱、人员变动后需要在多个系统间进行权限回收的问题。

权限分配：通过对回收的系统资源进行统一分配，解决运维人员管理多人多账号成本过高的问题。

审计管理：通过记录用户和管理员的使用操作，监控用户的高危行为，从而实现对用户行为的审计，做到权责分明，安全可溯。

4 功能列表

AIDM的核心功能如下：

核心功能	说明
企业门户	支持打造企业门户中心，集应用访问、通知中心、自助申请、待办事项等多场景办公于一体
单点登录（SSO）	用户仅登录一次即可访问企业内具有访问权限的应用系统，不再需要重新登录验证。
用户管理	支持数据导入、数据同步、API访问，保证多段数据一致。支持多种人员管理方式，角色管理、组织管理、分组管理
应用管理	用户应用可以通过多种主流协议自定义添加，同时也支持集成应用商店一键添加
权限配置	支持入口级别授权和细颗粒度授权，适配多种用户需求
审计管理	支持用户行为监控，包含用户与管理员的操作记录、登录登出记录、应用访问记录。

5 单点登录

在企业的日常管理过程中，通常用户会在多个应用（会话）之间来回操作，比如需要邮件系统来处理企业的内外沟通，CRM系统来管理企业内部的人员流动，信息登记等业务。随着企业的发展，业务系统也逐渐增多，痛点也逐渐显现。如何在单一系统中处理多个应用之间的连接是急需解决的问题，单点登录就是目前较为流行的企业间业务整合的方案。通过提供统一的应用导航界面，简化用户操作。将认证方式置于后台，使得用户可以登录一次就能够便捷访问授信的系统，省去传统用户名+密码的认证手段，提高用户的使用效率，完成企业增效的目标。AIDM系统支持多种认证协议的接入，能兼容主流认证协议，如OAuth认证、SAML认证、OICD认证，以及表单代填的接入方式。

5.1 OAuth2认证

OAuth是一种开放的授权标准，它允许用户在不提供用户名和密码的情况下，授权第三方客户端访问他们存储在另外的服务提供商上的信息。OAuth在“客户端”与“服务提供商”之间，设置了一个授权层（authorization layer）。“客户端”不能直接登录“服务提供商”只能登录授权层，以此将用户与客户端区分开来。“客户端”登录授权层所用的令牌（token），与用户的密码不同。用户可在登录时，指定授权层令牌的权限范围和有效期。“客户端”登录授权层以后，“服务提供商”根据令牌的权限范围和有效期，向“客户端”开放用户储存的资料。

AIDM提供了基于OAuth2协议的身份认证。用户点击单点登录，进入应用单点登录配置界面。点击左侧OAuth2上的“添加”（加号）按钮，即可进入OAuth的配置界面。如下图所示：

用户在协议配置界面可以配置相关字段，如下图所示：

所需配置字段如下：

字段名称	字段说明	是否必填
图标	应用图标	是
应用ID	应用的唯一标识，由系统自动生成	是
应用名称	应用名称	是
Redirect UR	表示重定向URL，由接入应用方生成	是
SP HomePageUR	应用首页地址	否
GrantType	OAuth接入模式，授权码模式和简化模式	是

Access_Token有效期	表示访问令牌有效期	是
Refresh_Token有效期	表示更新令牌有效期	是
应用描述	用来描述应用	是

配置完成后，即可在AIDM中实现接入应用的单点登录。

5.2 FormBased表单代填

基于HTTP+HTML表单的身份验证是一种登录技术，目前是一种简单的基于表单的身份验证。也就是说，网站使用网页表单进行收集，然后进行身份验证。认证凭证信息来自用户代理，通常是Web浏览器。

AIDM提供基于FormBased表单代填协议的应用集成用户点击单点登录，进入应用单点登录配置界面。点击左侧FormBased上的"添加"（加号）按钮，即可进入FormBased的配置界面。如下图所示：

所需配置字段如下

字段名称	字段说明	是否必填
图标	上传jpg或png格式图片，大小1MB以内	是否必填
应用ID	自动生成	是
应用名称	应用名称	是
登录提交UR	AES256登录表单提交完整UR	是
登录名属性名称	Usmename标签name属性	是
登录密码属性名称	Password标签name属性	是
登录其他信息	登录时表单中需要其他信息	否
登录跳转地址	登录成功跳转地址	否
登录提交方式	单选	是
应用描述	备注	否

配置完成后，即可在AIDM中实现接入应用的单点登录。

5.3 其他

AIDM系统也支持SAML和OICD协议的认证接入，能够实现对大多数主流协议的支持。

6 用户管理

AIDM系统作为用户身份管理软件，需要对企业中的各个组织进行管理，如对某一个组织进行授权，某一个部门中的人员的职位变动，因业务需要对不同组织的人进行统一管理等。针对企业中人员管理的需求，AIDM提供了组织管理、用户管理，分组管理来满足各种企业间的不同需求。

6.1 组织管理

管理员登录AIDM系统后，在用户管理-组织管理页面下可以完成组织架构的新增、上下级组织的新增、移动、删除等。同时可以查看不同组织下的用户。组织管理页面主要分为以下两个模块，一是对企业部门的管理，二是对部门中人员的管理。如下图所示：

6.2 部门管理

点击组织架构右侧的“添加”按钮，可以完成企业组织、部门的新增。如下图所示：

点击部门右侧的“更多”按钮，可以完成对该部门下级部门的新增，部门的信息编辑，部门间的移动，部门的删除，如下图所示：

6.3 组织人员管理

组织管理页面右侧展示相关部门中的人员信息，展示字段包括用户名、姓名、手机号、操作。管理员可以针对部门中的人员进行管理。如下图所示：

人员的管理主要是成员入职、人员信息导入、成员添加、部门变更、部门成员移除、人员信息查看、人员离职。

导入

包括组织导入、人员导入，系统内置组织和人员导入模板，管理员在进行多数据导入时可以直接使用该模板。如下图所示：

成员入职

企业初始数据录入完成后，对单个成员的入职可以使用成员入职功能。管理员在该页面通过步骤引导完成成员信息的登记，相关字段如下：用户名、姓名、密码、确认密码、手机号、邮箱、账户过期时间（长期有效、自定义）。第二步完成部门分配后，成员入职流程结束。用户使用用户名和密码即可完成AIDM系统的登录。如下图所示：

添加成员

管理员选取部门后，点击添加成员，可以完成对部门人员的添加。

成员移除

AIDM系统中，人员必须属于某一个部门，因为企业中人员是依托于部门、组织进行工作展开。若某人不属于某一个部门，可以对该成员进行离职处理。当用户隶属于多个部门时，在右侧的用户列表操作栏可以对该人员进行多个部门的移除操作。

变更部门

当部门中的人员有变更部门需要时，可以通过变更功能实现，用户选择单个或多个成员时，点击变更部门，选择需要变更的部门。需要注意的是，当用户完成部门变更后，原有部门的权限将会取消，会被赋予新部门的权限。

离职

当部门中有人员要离职时，可以对该人员执行离职操作，需要注意的是，离职之后该用户将无法登录AIDM系统应用，授予的所有权限将被回收！

通过对部门成员的管理，即可实现用户从入职到离职全生命周期的权限管理。

6.4 用户管理

除了部门维度，AIDM也提供了企业所有人员的管理，用户点击左侧的用户管理菜单，即可进入。如下图所示：

6.4.1 用户列表

管理员在人员账户列表可以对当前企业中的所有人员进行操作，通过用户名、姓名、手机号搜索可以快速定位用户。同时可以对用户状态进行筛选，用户状态包括启用、停用两种；过期状态包括正常和已过期两种状态。用户信息展示字段包括用户名、姓名、电话、最后登录时间、过期状态、启用状态、操作。如下图所示：

停用

当管理员对公司所有人员执行安全检查时，发现部分账户是过期状态，但是账户仍然是启用状态时，可以通用“停用”按钮进行权限回收。当用户登录次数超过设定次数时，账户也会被停用，此时需要联系管理员进行账号权限的启用。

重置密码

用户在入职时会由管理员登记登录密码，当用户第一次登录AIDM系统时，会强制用户用户修改密码，保证账号密码的安全性。用户进行密码修改后，此时用户个人密码只有用户本人知晓。当用户忘记密码后，需要联系管理员进行密码重置。保证用户登录的唯一性。

离职

当企业中有人员需要离职时，可以通过“离职”按钮对人员进行离职操作，当人员离职后，该人员拥有的所有权限将会被回收，用户将不能登录AIDM系统。

查看

点击用户列表操作一栏中的查看按钮，可以进入用户详情页。如下图所示：

6.4.2 用户详情

进入用户详情页后，通过四个二级tab页面展示用户该用户的所有信息，分别是用户信息、权限信息、访问授权、应用子账号。

用户信息

用户信息页面展示用户的基本信息和扩展信息，基本信息包括用户的基本信息，包含用户名、姓名、手机号、邮箱、组织架构、性别、有效期。当AIDM系统信息字段不足以满足需求时，可以通过扩展字段进行数据扩展，如当第三方系统与AIDM系统进行数据同步时，第三方系统有地址、生日等其他用户信息字段，此时就可以通过扩展信息字段进行扩展。

权限信息

权限信息页面展示用户所属组信息、所属角色信息、当前用户有授权资源列表。如下图所示：

管理员也可以在用户详情页针对用户分组、用户所拥有的角色、所拥有的的资源进行操作。

访问授权

在当前页面，管理员可以查看用户当前可以访问的所有应用，也可进行权限回收，点击右侧的关闭按钮即可回收。

应用子账号

该页面展示与用户相关的所有子账号，展示字段包含应用名称、子账号、关联时间、操作。管理员可以对用户子账号进行删除操作。

6.4.3 离职人员列表

当管理员将人员离职后，离职人员会展示在离职人员列表中，如下图所示：展示字段包含用户名、姓名、手机号、邮箱、离职时间、操作。

6.5 分组管理

分组管理主要是将用户作为一个集合可以进行授权，分组存在的意义就是将用户可以跨组织机构跨角色来建立的一个用户集合，后续系统加入ABAC同时可以把分组作为一个"属性"来获得相应的权限。如下图所示：

6.5.1 分组管理列表

分组管理列表是展示所有分组的预览，是分组管理的主要界面。分组管理主要包含分组名称、备注、组内成员（位）、创建时间、查看、修改、删除、新增操作。

分组管理新增：新增一条分组信息记录，分为3步操作，第一步在弹窗输入分组名称、备注信息进行到第二步选择用户成员将分组下的用户归到此分组。第三步需要选择分组相应的权限这样一个分组算是建好了。

分组管理查看：查看一条分组信息记录，跳转到分组详情二级页面，会显示当前这个分组信息、分组成员、已授权资源信同时可以在里面进行添加成员、移除成员、添加资源、移除资源操作。

分组管理修改：弹出分组信息的模态框，对分组名称、备注进行编辑修改。

分组管理删除：对任意一条分组信息进行删除操作。

7 应用管理

应用管理主要是管理根据标准协议创建的应用进行一个列表展示，可以根据切换样式变成表格展示全部的应用列表，可对应用进行停用，启用，编辑，删除，配置等操作。以下是应用管理的样例：

7.1 应用管理列表

应用管理列表是所有应用的概览，是应用管理操作应用的主要界面。应用管理列表主要包含应用名称、APP ID、应用类型、应用状态、和配置、启用、停用、编辑、删除、搜索操作。

应用管理配置：主要是查看应用基本信息和应用访问授权和子账号的信息。跳转应用配置信息的界面

应用管理停、启用：对新增的应用状态进行管理，应用停用时用户如果有访问权限在用户门户界面就不好显示该应用，应用启用时用户有访问权限时可以进行单点登录。

应用管理编辑：对应用的详细信息进行编辑操作，要进入编辑界面必须先将应用停用才可以进行修改应用字段。

应用管理删除：对应用进行删除操作，删除前需要将应用状态改为停用才能进行操作。

应用管理搜索：可以对应用名称进行模糊搜索。

7.2 访问授权

访问授权页面是在点击配置时跳转的页面，访问授权列表主要包含授权对象、授权类型、授权作用、取消授权、新增授权操作。

访问授权新增：可以新增用户、角色两种类型，后续会加上分组和组织机构类型，根据选择的类型选择相应的用户，会有两种授权作用拒绝和允许，当给用户是允许的作用时此用户可以在用户门户页面可以看到此应用进行单点登录，拒绝的作用是为了实现日常生活中会出现一种场景，角色的用户集合里面会有一部分人没有此应用的访问授权，这个时候可以给这部分人添加拒绝作用这样这个角色里面的这部分人不用有此应用的单点登录。

访问授权取消授权：可以对已授权作用的这条记录进行取消操作操作。

7.3 子账号

子账号是在点击配置时跳转页面的tab栏上面的子页面，子账号是将AIDM账号和用户应用账号进行绑定，通过账号映射与应用账号建立唯一标识，以AIDM为主账号，其他应用为子账号，通过主账号即可登录用户其他的应用实现单点登

录。子账号页面列表主要包含主账号、子账号、关联时间、新增、删除、搜索、导入等操作。

子账号添加：添加一条应用和AIDM主账号的关联关系需要输入主账号（ps.AIDM账号）、子账号（ps.此应用账号）、如果此应用属于表单代填建立的应用需要输入应用密码。

子账号导入：子账号导入是实现进行批量导入操作，一次可以导入2000条数据。

子账号搜索：可以根据模糊搜索子账号列表进行过滤显示。

子账号删除:对新增的子账号记录进行删除操作。

8 权限配置

权限配置是统一身份管理系统的重要组成部分，它主要是由角色管理、资源管理、授权管理3个部分组成、它采用TAB页的交互来进行显示，通过应用隔离来将各个应用下的角色、资源、授权进行分隔开。目前系统权限模型基于角色的访问控制（RBAC），通过用户、角色这两种对象实现RBAC权限模型的授权。同时为了满足大型系统中的复杂组织架构设计需求，将资源、角色、授权合并在一个应用权限分组中。

8.1 资源管理

资源管理主要是对当前应用的菜单资源、按钮资源、API资源、数据资源进行管理的页面。资源管理主要包括资源列表、创建资源、资源列表、资源名称、上级菜单、类型、描述、创建时间、查看、编辑、删除操作。

资源管理创建资源：创建资源是添加一条应用资源信息，弹出创建资源框，需要输入资源名称、选择菜单类型、选择上级菜单、输入资源描述。资源名称在当前应用下不允许重复。

资源管理编辑：对资源信息进行重新编辑，弹出编辑框，内容与资源创建时页面一样只是对当前资源信息进行一个反显，并可以进行编辑操作。

资源管理查看：资源列表支持对资源进行查看操作，对资源信息进行反显不能编辑。

资源管理删除：对当前应用下的资源任意一条可以进行删除，如果当前资源没有下级资源则会删除成功，有下级资源需要先删除下级资源才可删除。

8.2 角色管理

角色管理是对应用下所有角色的预览。角色管理主要包括角色列表、角色名称、用户数量（位）、创建时间、状态、查看、编辑、删除、新增操作。

角色管理创建：创建一条角色信息，弹出新增角色框，需要输入角色名称、备注、状态信息。角色名称在相同应用下是不允许重复的。

角色管理删除：对任意一条角色记录进行删除操作，但是删除之前需要先将角色进行停用操作和将角色下的用户进行移除才能删除成功。

角色管理编辑：可以对角色列表的角色信息进行编辑操作，弹出当前角色信息进行一个反显并可以对角色名称、备注、状态编辑。

角色管理查看：对当前角色信息进行查看，跳转到角色详情页面。角色详情页面主要是由角色基本信息和角色下已授权用户列表、已授权组织机构列表、已授权资源列表组成。同时可以对当前角色进行添加用户、组织机构、资源等操作

8.3 授权管理

授权管理是用户对角色、用户两种对象授权资源的权限操作的功能。授权管理主要包括创建授权、授权列表、被授权主体、主体类型、查看详情、删除操作

授权管理创建：创建资源是添加一条授权信息，弹出创建资源框，创建资源框主要是分为两步操作。第一步需要先选择授权的主体类型目前系统有用户和角色两种类型，后续会有分组和组织机构类型，选择类型穿梭框会显示相应类型授权对象，选择授权对象才能进行到下一步。第二步需要选择资源类型，资源类型会有菜单、API、按钮、数据4种类型，授权资源穿梭框会显示类型的资源。

授权管理查看：对授权列表授权信息进行查看操作，可以查看当前授权信息、授权对象、已授权资源列表。

授权管理删除：对任意一条授权信息进行删除操作。

9 审计日志

审计日志主要是将全部的AIDM系统账户操作日志集中记录管理和分析帮助用户对账户行为进行监控并且通过集中的审计数据进行数据挖掘，以便于事后的安全事故责任认定，所有操作行为都可以通过审计日志归档。审计日志主要是分为管理员操作日志、用户操作日志。

9.1 管理员操作日志

管理员操作日志主要是监控管理员的操作行为，通过管理员操作日志审计可以防止管理员权限过大跟踪不到痕迹都可以在整理找到痕迹以对某次改变提供充分的溯源数据。管理员操作日志主要是可以通过筛选某个时间段或者操作类型、操作人组合搜索日志列表数据，日志列表由操作人、操作类型、日志内容、IP、操作时间组成。

9.2 用户操作日志

用户操作日志主要是监控普通用户操作日志，对于普通用户的登录、登出、应用单点登录、个人中心操作进行记录。可以获取用户的操作记录从而进行审计分析。用户操作日志主要是可以通过筛选某个时间段或者操作类型、操作人组合搜索日志列表数据，日志列表由操作人、操作类型、日志内容、IP、操作时间组成。

10 密码安全设置

密码安全设置主要是满足用户对密码强度、密码策略进行自定义的需求，当客户公司对安全要求比较严格的时候密码强度可以设置严格同时对密码长度进行限制。可以限制密码周期当达到对应时间，会强制用户修改密码，还可以进行设置首次登录强制修改密码。可以对密码进行一个邮箱短信的通知。还可以开启密码锁定功能当在一定时间内错误多少次就会锁定一定时间。

全国统一服务热线

4008-555-800

金蝶天燕云计算股份有限公司(简称“金蝶天燕云”)成立于2000年，前身为“金蝶中间件公司”，是金蝶集团旗下新一代软件基础云平台服务商，云计算国家标准制定企业，国家信创产业核心软件企业。金蝶天燕是国家863重点研发计划与核高基重大专项承接企业，也是“两网一站四库十二金”国家重点工程的基础平台提供商，产品广泛应用于政府、军工、金融、能源等关键行业，累计服务客户总数超过10万家。

Apusic 金蝶天燕

云计算国家标准制定企业

金蝶集团旗下基础软件企业

信息技术应用创新核心企业

官网：www.apusic.com