绿盟统一身份认证平台

产品白皮书

【绿盟科技】

■ 文档编号	NSF-PROD-UIP-V2.0-产品白皮书-V1.0	■ 密级	完全公开
■ 版本编号	V1.0	■ 日期	2018-09-06
■ 撰写人		■ 批准人	

■ 版权声明

■ 版本变更记录

时间	版本	说明	修改人

目录

一. 前言

1.1 简介

本白皮书的目的在于帮助技术评估小组复查绿盟科技所提供的绿盟科技统一身份认证平台（NSFOCUS Unified Identity Platform）。内容包括产品定位，产品构成，产品性能设计及运行环境配置等。

1.2 适用范围

本文档适用于需要对绿盟统一身份认证平台（NSFOCUS Unified Identity Platform，以下简称“NSFOCUS UIP”）进行全面了解或以前接触过统一身份认证概念并想做进一步了解的用户。如需要了解产品的其他相关信息，请联系绿盟科技的销售工程师，由他们对您提出的问题和疑问集中进行解答。

二. 产品研发背景

2.1 传统身份安全手段落后

身份认证在信息安全体系中主要提供身份鉴别及访问控制作用，是目前网络安全建设的基础与核心之一，他被称作“PKI”公钥基础设施。PKI 技术为信息安全领域提供了身份的不可逆性及防伪造能力，可以帮助政府、金融、企业等客户有效控制业务系统访问人员的身份及权限，但随着信息化建设发展，传统局域网的单一网络环境随着不同行业的需求而快速转变，例如建立在公共网络系统上比如云和移动的计算机网络因为缺乏可信网络，受到的安全

威胁更严重，易受到外来截获和非法攻击的可能性大大增加。这些安全威胁有 70%来自于帐户安全， 比如假冒他人身份、未经授权进行系统越权操作，通过各种手段窃取系统传输过程中或存储的信息数据或用户信息，造成关键数据或用户个人数据泄露等。

在认证手段上应用较为广泛有以下几种:

一是用户名和静态密码。用户名和密码属于早期对称加密技术，容易被截获、盗取，特别在网上用户名和密码非常容易发生安全事故，存在较大安全隐患。

第二种是数字证书认证。政府机构构建权威认证中心(CA)、金融行业的（CFCA）等已经全面覆盖，作为国家信息安全的必要手段，PKI/CA 技术可实现一个专属的数字签名，让伪造、假冒真实用户的非法者无机可乘；另外也能防止在用户与 Web 服务器之间传输敏感、机密信息及数据在互联网上被截取；再者，该技术也能预防对发送信息进行抵赖而引起的不必要的纠纷。然而，我们在看到 PKI/ CA 为身份鉴别提供可靠保障、广受企业欢迎的同时，也会发现该技术目前仅仅只满足了内部的安全需求，而在当下信息化蓬勃发展的大环境下捉襟见肘，无论是昂贵的证书还是设备自身性能瓶颈均无法真正为大众实现服务。

2.2 信息泄露愈演愈烈

在信息化建设高速发展的同时，随之而来面临日趋严重的信息安全问题，账户被盗、数据泄露、身份伪造、资产损失、撞库、脱库、数据截取等安全威胁，由于使用环境脱离内网、终端设备由固定 PC 变为移动终端，使各种攻击手段在传统安全防护措施面前更得心应手、难于防范。

随着各行业信息化发展，逐年增多的应用系统，这些系统建设有先有后，由于建设初期对安全问题认识的局限性及各类系统的安全需求既有共性又有个性，这就直接导致各应用的安全体系结构及安全策略的差异，其安全处理流程错综复杂，主要问题如下：

1) 用户身份认证：公众在政府网上办事、银行资金交易、医院挂号、孩子教育等，其中包含公众个人隐私信息及资金等敏感信息，传统账户/密码认证登录的方式对系统使用人员身份确认无法控制，不能确认登录人员真伪性。
2) 安全信息共享问题：多个具有异构认证机制的业务系统协同完成任务时，认证结果无法传递，重复登录、认证频繁，容易导致认证信息泄露或遗忘等，大多数人员在多业务系统下通常会建立相同账号密码。
3) 数据传输问题：认证登录后，用户终端在与服务器进行数据信息交互过程中，由于网络及数据均为透明传输，无法保证传输过程的安全屏蔽。
4) 数字证书价格昂贵难以实现普及：由于使用对象为公众，不但涉及资金还有大量个人敏感信息，数字证书在信息安全中起到关键作用的同时，昂贵的价格导致其无法普及，现阶段使用对象始终局限于企业、政府等用户类型而无法普及到公众。

我们已经进入到了移动-云计算时代，随之而来的信息安全隐患随处可见，这也是各行业都必须面临的一大难题。脱离传统信息安全防护，应用场景更多元化、面向内部办公、对外提供服务均移动化，传统的帐户密码面临着钓鱼、暴力破解、拖库等众多的风险，并且传统安全设备局限于性能瓶颈，无法满足庞大信息量、众多用户需求。

2.3 账户及权限体系管理的混乱

无论政府、金融、教育、医疗等各行业随着信息化发展、业务系统增多都将面临应用业务系统多元化，涉及开发语言种类繁多；认证源、认证协议各异等问题。由于各业务系统互相独立，账户、权限均独立管理导致业务系统管理、使用均无法统一；用户数量庞大、用户种类多样、应用业务系统日益增加，导致管理任务繁重、难于维护；业务系统使用人员针对每个应用系统使用时均需按照相应的系统认证方式进行登录，需要记录大量账户、密码实现系统登录，给用户带来诸多不便同时也产生大量安全隐患，易受到外来截获和非法攻击的可能性大大增加。

2.4 绿盟统一身份认证平台

针对上述问题，统一认证及单点登录概念应运而生，实现对内对外服务的标准化、精准化、便捷化、平台化和协同化，在已有的安全体系下，构建一套统一、高效、安全的绿盟统一身份认证平台。它需要满足现有业务系统传统 WEB 端及未来移动端、物联网等多领域需求，实现业务系统数字化、网络化、智能化的同时，服务内容规范化、服务便捷化、数据互通化，提升对内、对外网上业务服务能力。在解决现有问题的同时不断发展，以“云大物移”为发展平台，为信息化发展助力、保驾护航。

三. 产品定位及产品特点

3.1 产品定位

1） 加强各区域人员组织机构的管理，加快内部办公信息传递的效率；

2） 紧密联系员工，重视员工的意见，将意见处理流程公开透明；

3） 提高员工办公效率，简化日常工作中员工对各系统操作步骤；

4） 只要通过简单的配置，不需要修改现有的 B/S 和 C/S 应用系统，即可实现集成；

5） 集成结构不受任何条件的限制：支持 Windows 、Linux、Unix(Aix)多种操作系统和 JBoss、WebLogic（Bea）、Apusic (金蝶)等多种应用服务接口；

6） 可满足企业级用户的认证和管理需求，支持集群和负载均衡部署；

7） 激励员工进行日常工作的积极性，保证日常工作的有效性；

8） 利用互联网的快捷和实时性，将一切信息化工作及信息查看都集成入手机。

本产品投入市场后，极大的提升了各行业客户信息化水平，利用信息化提升企业在市场的竞争力。产品实现多领域业务系统、多类型人员、强认证方式等一体化管理解决方案，不

仅确保人员信息唯一性、不可逆性，并且通过对用户、组织机构、角色等多维度应用同步能力，大幅度提升易用性，方便用户统一管理能力，同时通过数字证书加密技术、短时限有效的 Token 进行身份传递，且一次一密，认证作废， 保证访问安全、便捷。通过产品“云大物移”的特点，无论是 B/S 的 WEB 端、H5 应用如 OA，还是针对移动办公的 App 及提供第三方服务的 API,甚至门禁、WIFI、主机等物联网领域应用都能纳入其安全防护的体系下。

3.2 产品特点

- 易用性

实现多组织机构相同人员之间的统一、同步，确保人员信息唯一性、不可逆性，并且通过对用户、组织机构、角色等多维度应用同步能力，大幅度提升易用性，方便用户统一管理能力；

- 安全性

传统的认证方式中，使用用户密码长期未能被更换，仅一次不安全的应用访问即会丢失认证信息。使用绿盟云身份管家后应用系统的认证采用数字证书加密技术、短时限有效的 Token 进行身份传递，且一次一密，认证作废， 保证访问安全、便捷；

- 规范性

使用绿盟统一身份认证平台可以保证用户账号密码的唯一性，更容易遵从安全管理规则，如每隔三个月更改一下密码，因为消除了子帐户密码， 用户只需要更改一下主帐号的密码就可以满足所有应用的审计合规要求。当员工离职后，主身份管理系统中的帐号一经删除，该用户就无法再访问任何企业内的应用和数据。

- 采用最先进的认证技术

目前集中在 2010 年以后的技术，兼容传统认证技术（传统的 Basic/CAS/SAML），覆盖多个行业领域，技术涉及到公/私有云、移动、物联网（智能设备、wifi、门禁、摄像头等）。

为企业移动应用和第三方服务，提供一个基于用户的统一认证平台，无论是 B/S 的 WEB 端、H5 应用如 OA，还是针对移动办公的 App 及提供第三方服务的 API，都能纳入其安全防护的体系下。

- 丰富的应用整合集成经验

集成实施过包括金融行业、大型企业、物流公司、央企在内几十个应用案例，集成整合过各种应用系统超过 400 个。

- 健全的运行安全机制

周密的安全策略管理：基于三权分离理念实现管理员角色管理，支持根据不同的安全需求对认证等级、口令强度、授权粒度等实行安全策略配置，基于 PKI 技术实现对重要数据的加密或数字签名，保证敏感信息的存储和传输安全。

- 灵活的授权管理模式

可控的授权粒度：支持基于 RBAC 的授权模型；支持系统级的粗粒度授权和系统功能级的细粒度用户授权。

- 安全可靠的单点登录

单点登录，多点漫游：支持跨应用域和跨不同认证域的认证和访问控制，并解决了票据在传输过程中被冒用、拦截、篡改、伪造或重放的安全风险。同时，支持 SAML 联邦认证标准。

- 丰富的身份认证方式

支持不同安全等级的用户身份认证，如用户名/口令、手机 APP、二维码、智能 USB Key/智能 IC 卡、生物识别（指纹……）等。

- 即插即用

只要通过简单的配置，不需要修改现有的 B/S 和 C/S 应用系统，即可实现集成。

- 跨平台部署

集成结构不受任何条件的限制：支持 Windows 、Linux、Unix(Aix)多种操作系统和 JBoss、WebLogic（Bea）、Apusic (金蝶)等多种应用服务接口。

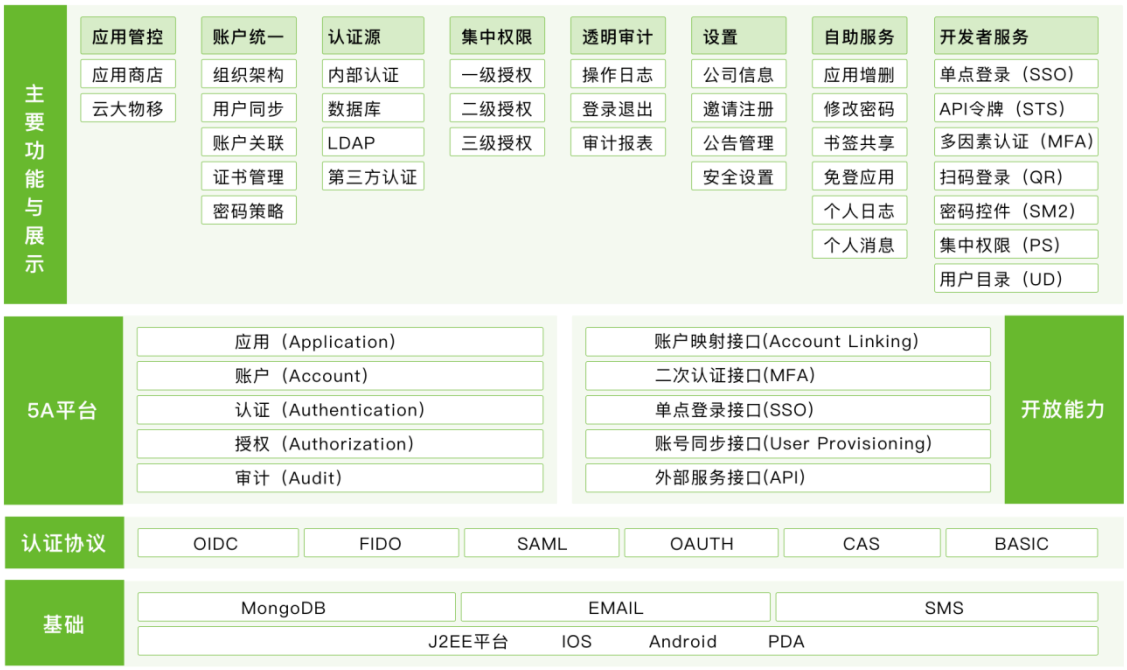
- 性能稳定

支持集群和负载均衡部署：可满足企业级用户的认证和管理需求，支持集群和负载均衡部署。

四. 产品架构及产品功能

4.1 产品架构

产品总体架构采用模块化的方式设计：



如图所示，绿盟统一身份认证平台主要分为：管理员平台，用户 Portal、外部系统认证接口、底层服务、5A 体系、安全认证体系组成，PC 端无客户端插件设计，减轻 PC 端性能损耗，均通过 WEB 界面实现系统访问。

客户端：兼容 PC 端、手机端等访问等多种方式。

统一身份认证的一个重要诉求是一个账户打通覆盖云计算、大数据、物联网、移动互联网所有的应用及资源，并实现结合准入设备对所有终端接入网络资源人员身份进行统一认证。统一身份认证管理平台在认证时利用符合国内、国际标准，基于 PKI 体系的公/私钥证书签名，实现所有用户在使用该身份认证时一次一密，而不是使用长期不变的账户和密码。在解决用户全生命周期的统一身份安全认证中，全程采用支持多种账户同步协议如：SCIM、单点登录 FIDO/OIDC/SAML、跨域访问（身份联邦）、权限控制、审计、应用管控等最佳实践，真正实现用户全生命周期的身份管控。

构建统一身份认证管理平台，通过对用户、组织机构、权限管理和各类应用系统资源的规范化、标准化管理，在与各类已建业务应用系统授权管理功能有效对接的基础上，健全统一、灵活、多维度的门户访问控制机制，对应用访问权限进行全流程监管，推进集中访问业务模式安全有序的开展。

4.2 产品功能

系统由应用、帐户、认证、授权及审计五个模块组成：

- 应用管控（Application）
- 统一账户（Account）
- 统一认证（ Authentication ）
- 集中权限（ Authorization ）
- 透明审计（Audit）

统一身份认证的一个重要诉求是一个账户打通所有的应用和资源。新的 IAM 产品在认证时利用符合国际标准，基于 PKI 体系的公/私钥证书签名，可以实现所有员工在使用该身份认证时一次一密，而不是使用长期不变的账户和密码。在最终针对客户解决不同角色人员全生命周期的统一身份安全认证中，全程采用账户同步 SCIM、单点登录 PKI/OIDC/SAML、权限控制、审计、应用管控等最佳实践，真正实现员工全生命周期的身份管控。

4.2.1 应用管控（Application）

应用管控（Application)：平台设计支持将现有业务系统集中管控的能力，更考虑到未来随着业务拓展而新增加的公有 SAAS、移动、物联网业务系统，以满足客户未来新增业务系统时的自行集成诉求。

系统为所有业务应用按照不同的维度分类呈现，直观地为用户展示出各个领域下的业务应用信息。提供标准的应用集成接口，用户通过简单的系统引导配置便可轻松实现标准业务应用的集成。

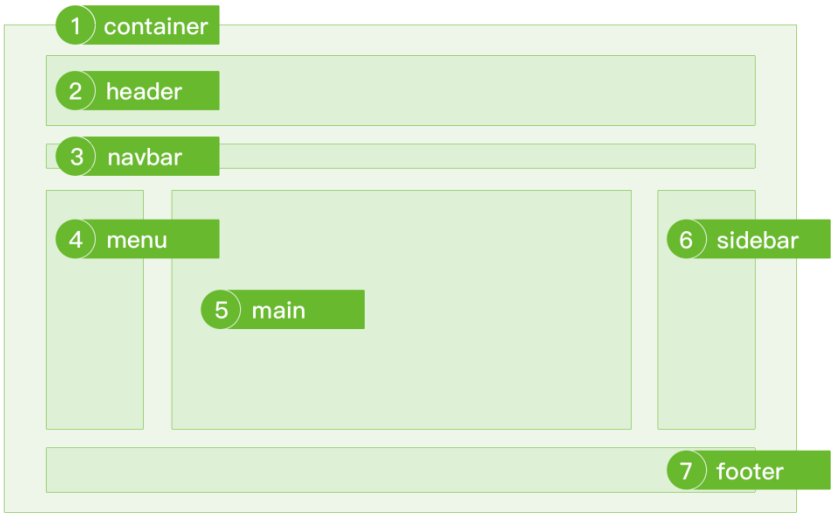
4.2.1.1 门户（End user）

传统门户可将各种应用系统、数据资源和互联网资源集成到一个信息管理平台之上，并以统一的用户界面提供给用户，并建立面向客户、内部员工以及企业对企业的信息通道，使企业能够释放存储在企业内部和外部的各种信息，解决业务系统及信息化办公统一展示能力。

而绿盟统一身份认证平台除满足上述对传统门户的需求外，还提供账号管理、权限管理以及通过强认证及单点登录等几大功能，实现便捷、安全的管理及使用能力。

门户设计的三大原则是：置界面于用户的控制之下、减少用户的记忆负担、保持界面的一致性。

页面基本框架结构：



说明：

container——就是将页面中的所有元素包在一起的部分；

header——是页面的头部区域，一般来讲，它包含网站的 logo 和其他一些元素；

navbar——等同于横向的导航栏，是最典型的页面元素，也可以命名为 nav；

menu——此区域包含一般的链接和菜单，也可以命名为 subNav,links；

main——是网站的主要区域，也可以命名为 content；

sidebar——此区域包含网站的次要内容，例如最近更新内容列表等；

footer——包含一些附加信息，也可以命名为 copyright.

- **分辨率**

所有系统能自适应 1366*768 及以上的测试分辨率，适应 14 英寸笔记本的分辨率（1366*768）。默认窗口设置下，不应该出现水平、垂直滚动条。当界面内容超出显示区域时，以浮动层的形式显示。弹出页面要保证 768 高度的分辨率显示正常，同时能移动查看弹出框内容。弹出框的高度为不超过 450 的分别率，弹出页面内容过多时，使用 tab 页显示。

- **浏览器兼容性**

所有系统后台必须兼容 Chrome 浏览器；前台系统兼容主流的浏览器，如：IE8 及以上、Firefox、Chrome 等。

- **登录框**

所有系统做统一的登录框，当退出系统时，跳转到当前系统的登录页面；登录页面用户名、密码宽度应该上下对齐；鼠标点击登录、重置按钮应该显示手型，而不是箭头；支持按 Tab 键切换用户名/密码输入框；支持按 Enter 键登录系统。

- **必填项**

界面的输入信息标有必填提示的，应以红色*号标识出来，标识在文字前面，如：

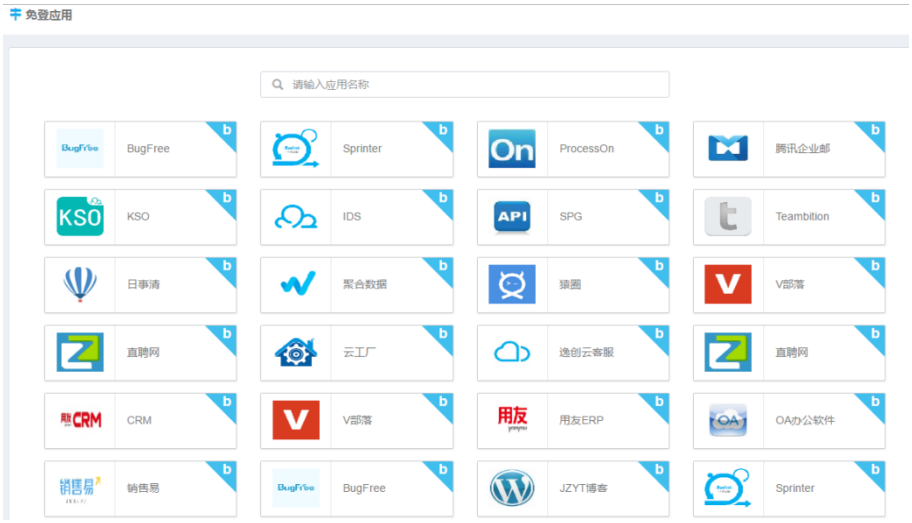
- **防错和出错处理**

对于输入数据进行校验，对于某些情况下不应该使用的菜单项或命令按钮，应将其“失效”或者隐藏执行破坏性操作前，应当获得用户的确认；如：删除记录；如果发生意外或错误，应当及时给予警告信息或错误信息，提醒用户做出正确的处理。当系统某个功能出错或者系统宕机以后，需要给相关人员（系统工程师和项目负责人）发送邮件，前台不能直接显示后台的错误信息。

- **提示语**

提示信息中标点符号统一使用全角符号；功能按钮为图片按钮时，光标停留需给予文字浮动提示信息；按照用户意愿的处理成功提示信息，位置在右下角给予提示信息，如：处理成功，处理成功的提示信息需要能自动消失。请选择需要处理的记录，不同的提示信息中要用不同的颜色标识。重要的提示信息需要弹出确认提示框，如：删除记录、操作失败，指出出错原因并提供解决办法提示。提示框图标，根据内容显示不同，分为：错误、警示、成功。

下图展示的是普通用户在 web 端登录界面设计效果：

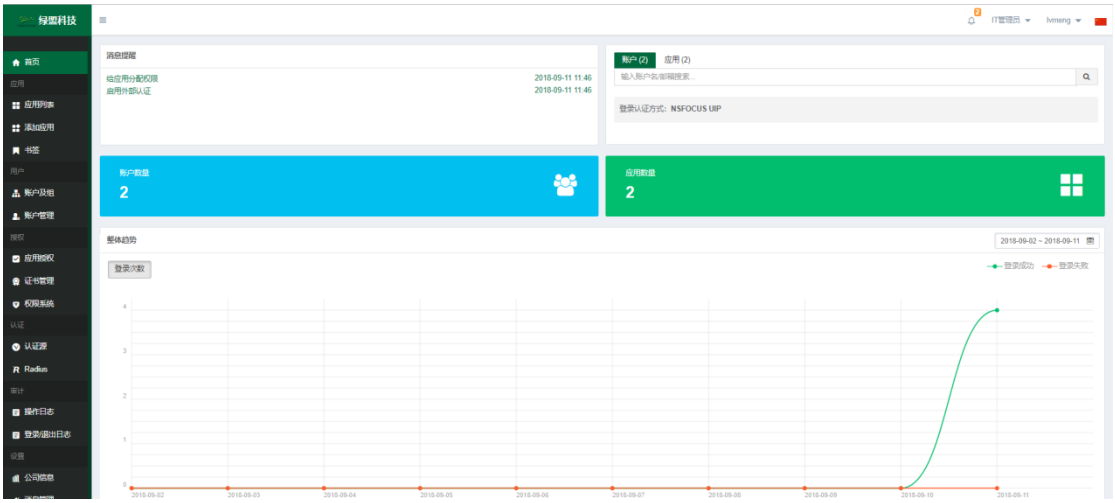


上述界面展示的是当前登录用户授权范围内的所有的业务应用，通过点击界面上的应用图标直接免密码打开对应的业务系统。

- 简易性：界面的简洁是要让用户便于使用、便于了解、并能减少用户发生错误选择的可能性。
- 用户语言：界面中要使用能反应用户本身的语言，而不是设计者的语言。

- 记忆负担最小化：人脑不是电脑，在设计界面时必须要考虑人类大脑处理信息的限度。人类的短期记忆极不稳定、有限，24 小时内存在 25%的遗忘率。所以对用户来说，浏览信息要比记忆更容易。
- 一致性：界面的结构必须清晰且一致，风格必须与内容相一致。
- 安全性：用户能自由的做出选择，且所有选择都是可逆的。在用户做出危险的选择时有信息介入系统的提示。
- 灵活性：简单来说就是要让用户方便的使用，但不同于上述。即互动多重性，不局限于单一的工具(包括鼠标、键盘或手柄)。
- 人性化：高效率和用户满意度是人性化的体现。

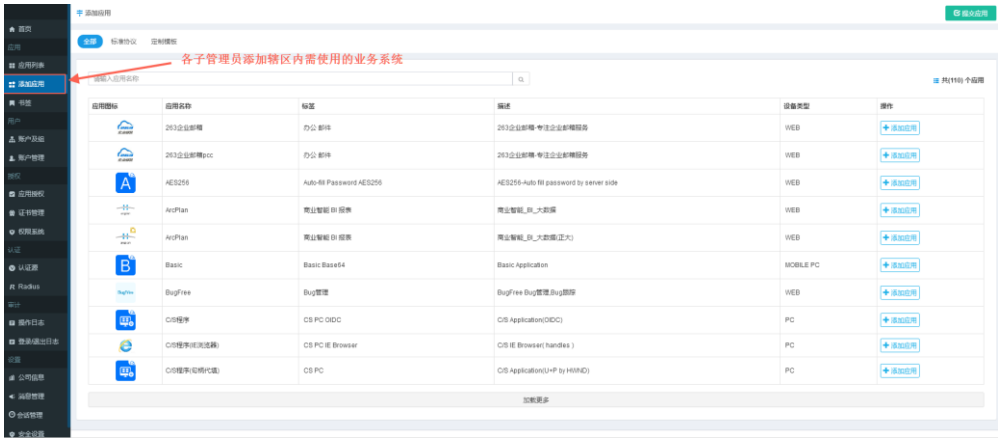
管理员登录后需直观地展示当前单位下的主要相关统计信息，效果图设计如下：



移动端登录后的展示效果：

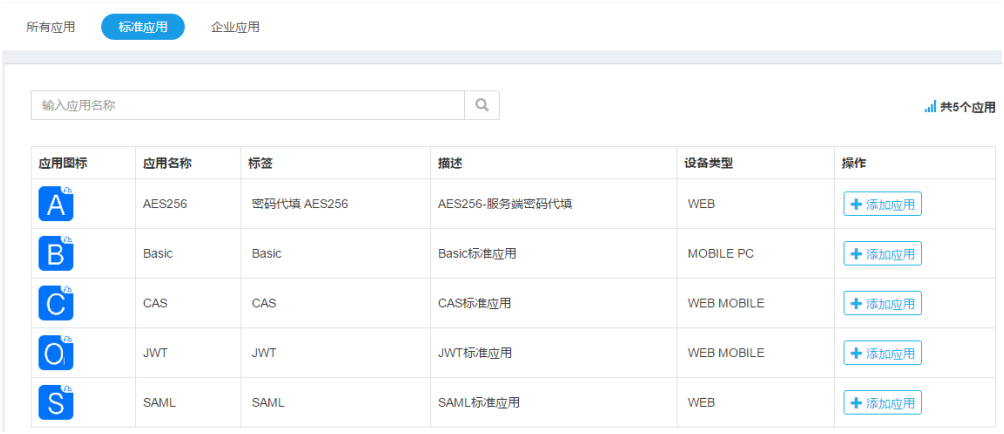
4.2.1.2 应用商店

绿盟统一身份认证平台为不同行业提供除定制化的门户设计外，还为大型企业、集团公司、部委级政府单位等客户提供分级授权管理模式，即平台具备总管理员，而各分支机构、分公司、办事处等子级具备子管理员能力，可以管理辖区内用户及权限能力。针对这部分绿盟统一身份认证平台提供应用商店模式，各子级管理员均可在添加应用界面找到已添加好的应用对辖区内人员进行业务系统访问权限的分配工作，此场景我们称之为“应用商店”。

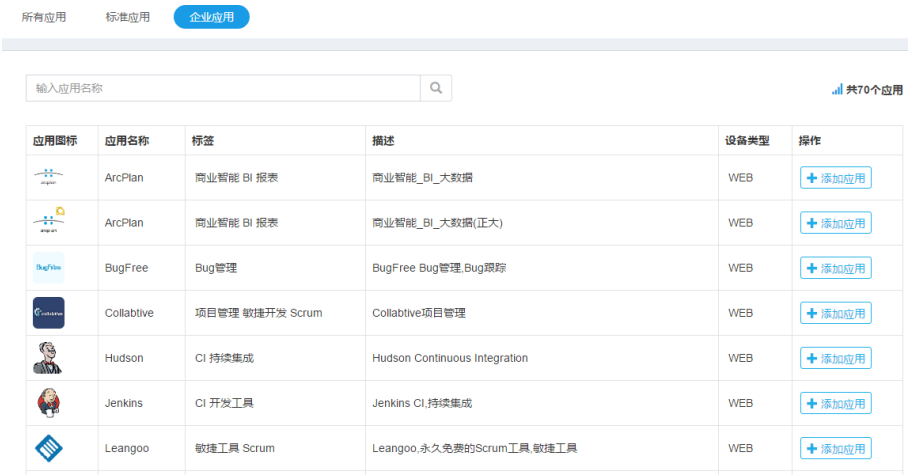


为方便对业务应用的集中管理，系统内预置了多种模板应用；所谓模板应用就是定义了一系列有规则的应用配置模板，当用户需要集成一套业务应用到绿盟统一身份认证平台中时，

只需要选择对应的模板应用，通过界面化最小配置便可完成单点登录的集成，从而到达安全快速管理所有业务应用的目的。

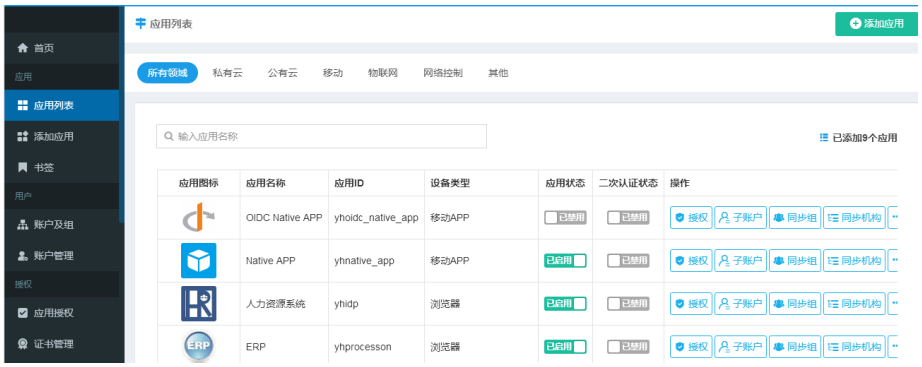


模板应用分为标准模板应用和模板应用（系统自定义模板）两种；标准应用模板是以 AES256、Basic、CAS、JWT、SAML 等标准认证协议为分类依据所提供的应用模板，用户在做业务应用集成时，如果业务应用采用的认证方式是标准应用中的任何一种，都可将业务应用集成到绿盟统一身份认证平台中，最快集成时间达 5 分钟。



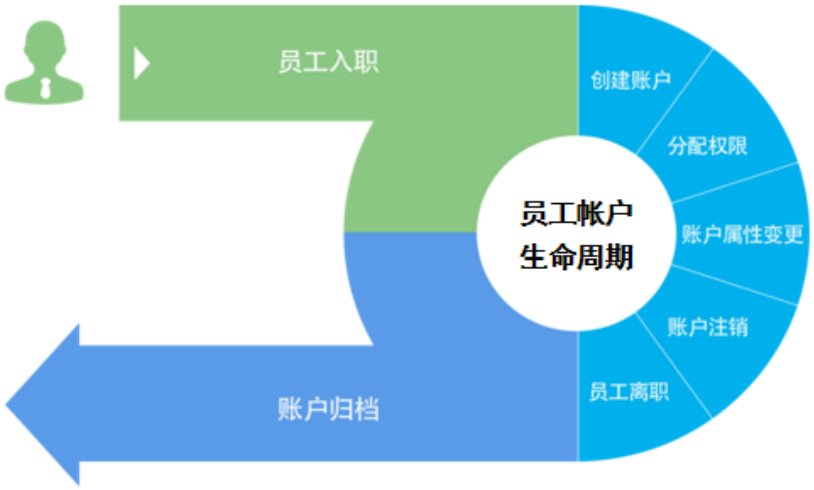
企业模板应用指政府中用到的市场较为流行应用，这些应用通常在内部比较分散，有针对办公的、有移动的、甚至还有物联网相关的应用；系统将这些常用的使用频率较多的应用预置进来，管理员通过对不同用户需要的业务应用进行权限分配，便可实现对所有应用的统一管控。

应用系统均实现列表式展示，针对业务系统可实现添加、删除、挂起等多种状态的操作。



4.2.2 统一账户（Account）

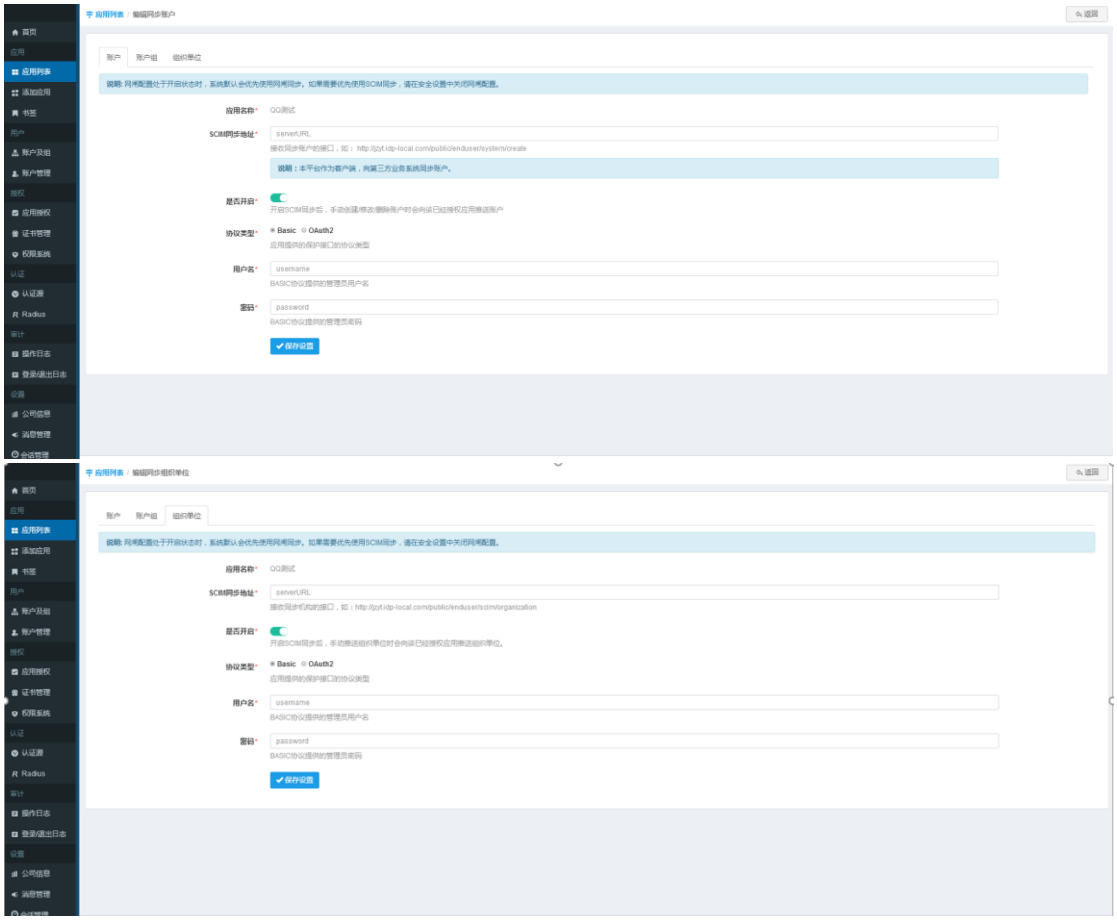
统一账户（Account）：提供统一集中的账号管理，支持管理所有的业务员工账号，支持矩阵式组织架构创建，提供横向、纵向灵活设计，实现被管理资源账号的创建、删除、启用/禁用及同步等流程的自动化管理，实现账号管理生命周期所包含的基本功能并可进行生存周期设定。通过对接入平台的应用系统进行二次开发，实现平台与各接入系统、数据库之间用户信息同步能力，并可实现平台存储所有用户账户信息作为唯一用户账户数据源，下游业务系统均不再存储用户账户信息，确保平台一次操作，命令下达所有应用系统，真正实现用户全生命周期管理能力，如图：



4.2.2.1 数据同步

绿盟统一身份认证平台与应用系统之间以 SCIM/JNDI/LDAP 方式建立通信。数据通过同步引擎、事务机制和 SCIM、JNDI 与 LDAP 协议实现与应用系统之间的同步。同步可以采用不同的协议， 比如 LDAP 协议、SCIM 协议和 JNDI 技术， 以实现与不同类型应用系统（如：HR 系统、账户管理系统）、JDBC 类数据库实现数据同步。支持的 LDAP 包括：ApacheDS、OpenLDAP、SunONE 等，支持的数据库 JNDI 包括：SQL server、Mysql、Oracle 等，另外也包括域控制器（Windows AD、Linux NIS、Unix NFS）。

同步的成功和失败都进行多维度记录，同步的成功信息以报告形式方便于管理人员查看，同步的失败信息通过定时器机制自动完成，直至同步成功。

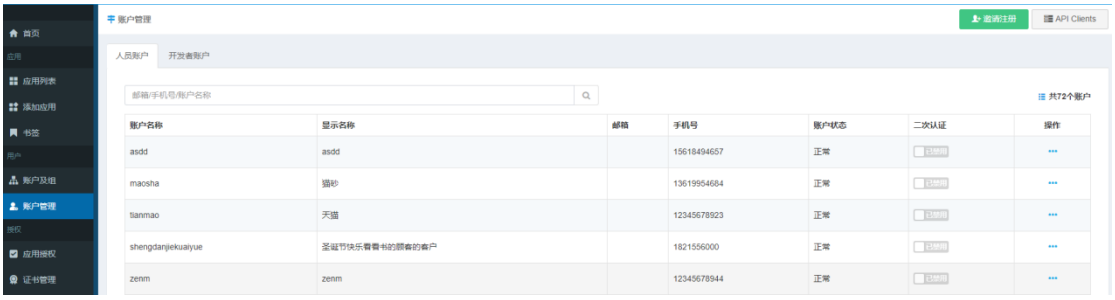


4.2.2.2 账户全生命周期管理

4.2.2.2.1 人员与账号管理

1） 账号管理

在账户管理处，可以对同步后的所有员工进行查看、绑定设备信息，重置密码等操作，所有员工均由员工号或手机号、邮箱等员工唯一值确认该员工信息，确保员工信息唯一性、不可逆性；并可针对用户信息属性实现自定义扩展能力，如下图，外部 ID 可变更为身份证等。



公司管理员可以通过列表的操作功能进行管理和维护：

【删除】可以删除账户；

【禁用】可以禁用账户，账户不再可用；

【属性】可以对用户账户字段属性进行修改或扩展；

【设备】可以查看该账户绑定的设备信息；

【报表】可以生成并查看该账户审计日志报表；

【重置】可以重置账户密码；

2） 单独添加与批量操作

点击某一机构单位，右侧页面显示该组织单位的成员列表，如图：

在任一机构单位的成员列表界面，可以做如下操作：

：可以编辑组织单位的名称、管理者、外部 ID、描述信息；

【新建并添加成员】可以新建机构单位、组、账户，并添加到当前组织单位中；

【添加成员】可以选择现有的组织单位、组、账户，添加到当前组织单位中；

【批量移除】可以批量移除成员；

【修改】可以查看并修改成员信息；

【移除】可以单个移除成员；

【同步到 SP】可以将该账户同步到已被授权的其它业务系统中；

【同步记录】可以记录用户同步操作。

4.2.2.2.2 组织管理

1） 组

组下可以包含：组和账户，下一级组仍可以包含：组，账户；

根据现有人员部门、组信息、类别，进行组织机构建立或同步工作。

组织机构在原则上可以无限进行嵌套，不做限制。

在组织机构下，点击【新建组】编辑相关信息即可新建一个自建组，如图：

点击组名称，进入组属性页面，这里可以分配公司下属某一机构管理员信息，如图：

在组的【常规】标签界面，可以做如下操作：

可以修改组的名称、管理者、外部 ID 和描述信息；

【返回所属组织单位】可以返回到创建该组的组织单位页面。

2） 组织单位树

组织单位树上只显示组织单位，根机构默认是当前下属机构。点击机构时，右侧页面可以查看该公司所有成员列表，包括组织单位、组、账户，如图：

在任一机构上可以新增组织单位、组、账户。点击任一组织单位，右侧页面可以看到该机构下所有成员列表。

在组织单位树中的任一机构下，可以做如下操作：

【新增】可以新建组织单位、组、账户，并添加到当前组织单位中；

当新增组织单位时，会生成一个对应的默认组。

默认组不能编辑、删除、查看；不可添加到其它组织单位下，但可添加到其它组中。

默认组的成员包括该组织单位下所有组织单位、组、账户的集合。

【删除】可以删除当前组织单位；

删除当前组织单位时，同时将其对应的默认组删除掉。

如果当前组织单位下，有除默认组外的其它成员，会提示组织单位非空，不能删除。

【移动】可以将当前组织单位迁移到其它组织单位下；

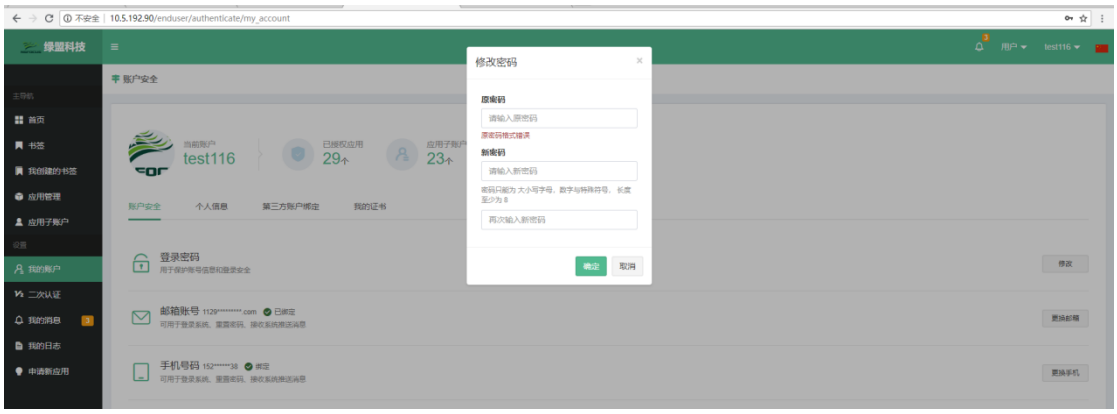
移动后，当前组织单位下的所有成员，将一起移动到新的组织单位下。

【属性】可以查看该组织单位的相关信息；

在属性界面，可以修改该组织单位名称、管理者、外部 ID、描述等信息。

4.2.2.2.3 自助管理服务

系统支持 PC 端、移动端用户自行修改自身属性信息，除账户及姓名外，职务、角色、电话、邮箱等可变更信息均可实现自行修改能力，修改后提交至管理员，需管理员审批确认后方能生效。针对修改内容，系统提供完善的修改记录，及行为信息。



自助式用户注册：系统支持用户自行注册，并由管理员审批后，获得访问平台权限。

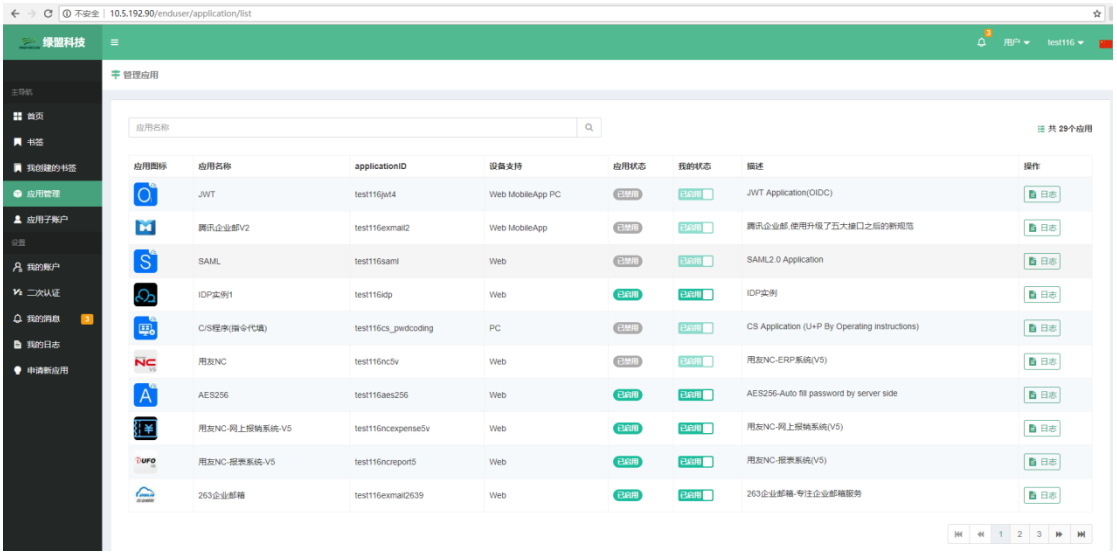
修改密码：系统支持用户自行修改登录密码，密码必须包含英文字母大小写、特殊字符及数字且长度不少于 8 位，密码修改成功后系统自动给用户发送一条密码修改成功的短信或微信。

找回密码：可通过绑定的邮箱、手机号发送邮件、短信进行密码重置；支持通过绑定的微信、QQ 登录后，对密码重置；

修改邮箱：可修改登录邮箱，修改后的邮箱需通过邮箱验证，修改成功后系统用户发送一条密码修改成功的短信或微信。

修改手机号：可修改绑定的手机号，系统给修改后的手机号发送一条附带验证连接的短信，用户需点击进行验证。修改成功后系统用户发送一条密码修改成功的短信或微信。

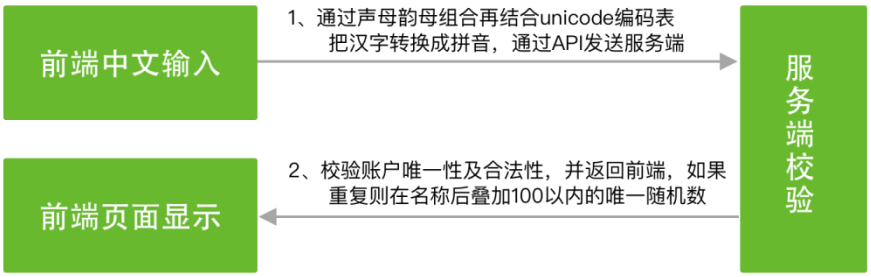
修改微信：可修改绑定的微信，系统后台根据微信接口自动给修改后的微信发送附带验证连接的小程序，用户需点击进行验证。修改成功后系统用户发送一条密码修改成功的短信或微信。



应用管理：用户可自行处理应用的展示，除可控制应用在免登应用列表可现实外，还可查看应用于平台账户关联信息等。

4.2.2.2.4 账户命名规则

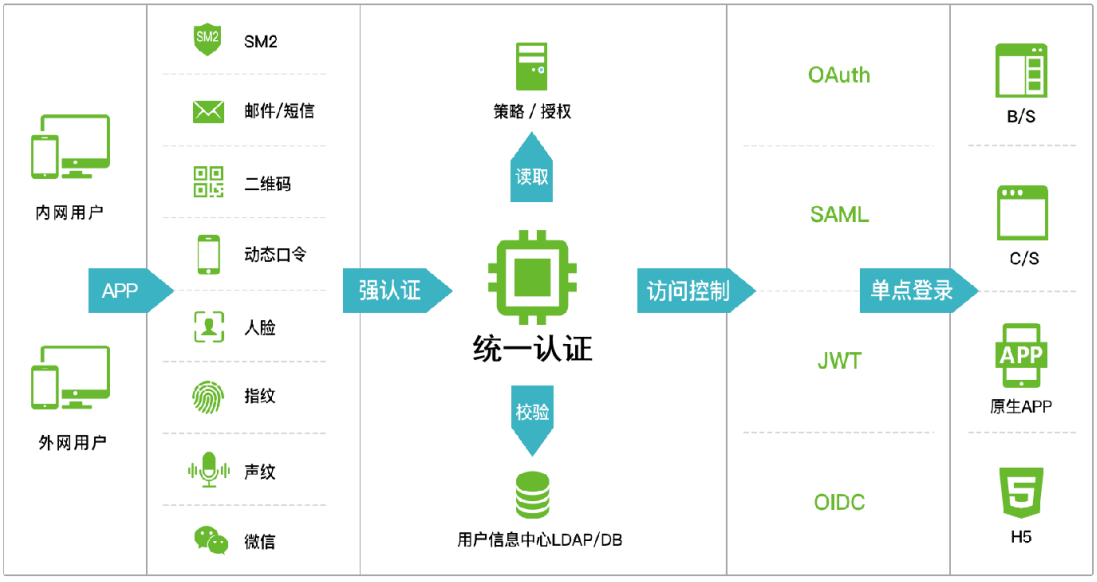
账户可以根据输入的中文姓名自动生成唯一的拼音账户，前端页面通过汉字的声母韵母排列组合及结合 unicode 编码表把汉字转换为拼音，通过 API 发送至服务端，服务端校验拼音账户的唯一性及合法性，如果有重复则在名称后叠加 100 以内唯一性的随机数返回给前端，实现原理图：



示例：

4.2.3 统一认证（ Authentication ）

统一认证（Authentication）：系统能实现用户在各个不同业务应用过程中的单点登录功能。支持不同域下业务应用统一认证集成，通过集中资源服务及授权管理系统提供的集中身份信息和权限信息，消除客户信息系统的业务孤岛和数据孤岛及对员工、合作伙伴、客户登录各个应用系统造成混淆和障碍。结合数字证书身份认证(PKI)体系，剔除传统账号/密码对称秘钥加密认证机制。在用户认证之后，可以在不同业务系统中灵活切换角色和权限信息。从而确保用户只需要认证一次，便可以在访问权限的约束范围内访问不同的应用系统及硬件设备，从而达到“一次认证，安全漫游”的效果。



4.2.3.1 统一认证

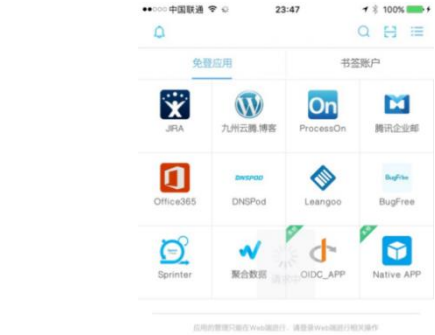
用户在第一次使用时需要先进行注册来绑定信任设备如 PC、手机等。如果需要实名认证，也可以通过上传身份证照片完成用户信息的收集和梳理工作；并且手机 APP 可自动识别身份证信息降低用户使用复杂度提升用户体验；用户提交身份信息与业务系统账号进行绑定，使用户 IT 身份信息与真实身份进行保定；通过认证实现自助账户绑定，而不是由管理员统一进行绑定降低了管理员维护工作量；绿盟统一身份认证平台提供多种认证方式。

PC 端：账户密码、账户密码+验证码、OTP 动态口令；

移动端：比如生物体征、扫描登录、动态令牌、手机“摇一摇”手势认证；

实现效果图如下：

扫描登录过程：通过手机 APP 扫描 PC 端页面提交登录指令即可。



如果继续启用传统的用户名/密码登录，在启用二次认证后，在 PC 上输入用户口令后会向绑定了该账号手机发送摇一摇指令，手机 APP 认证以及手机摇一摇认证确认页面，在用户手机上收到摇一摇指令后，APP 会有提示信息，可通过点击“接受”或者摇动手机实现登录。

当用户手机所处环境无法接入互联网，接收不到推送信息，或希望增强认证手段，实现二次认证时，可在二次认证页面输入 OTP 随机口令，通过手机 APP 上查看即时的随机口令即可登录。该方式可以完全取代短信认证或动态令牌。

4.2.3.2 单点登录（SSO）

- 应用账号传递机制-主从账号映射

用户登录系统后，该系统将其作为用户的主账号。当增加一个单点登录的业务应用时，只需要增加用户唯一 ID（主账号）与该单点登录应用账号（子账号）的一个关联信息即可，不会对应用系统产生任何影响，从而解决登录认证时不同应用系统之间用户交叉、用户账号不同的问题。单点登录过程均通过 TLS 安全通道来保证数据传输的安全。

- 应用账号传递机制-Token

对于可以改造的应用推荐使用 OAuth、CAS 等票据 Token 方式。该部分应用场景，目标应用待开发中或者支持二次开发的方式，目标应用需要配合调用 NSFOCUS UIP 提供的认证协议，根据应用业务系统认证机制确认需要或不需要 API 接口完成，通过数字证书生成的公私钥结合票据（token）、多因子认证，实现非对称密钥加密认证能力，利用具有一次性时效的 PKI 公私钥代替传统账号/密码登录方式，并可对认证信息通过 SM 国密算法进行再加壳，达到双重安全保障效果，可提供对设备终端 IP、MAC、设备配置等信息搜集能力，通过这些信息对用户登录实现管控作用，作为允许/禁止功能的依据。

4.2.3.3 数据互通（STS）

近年来，随着移动办公的盛行，企业需要面临的不仅仅是过去 WEB 的统一认证，更多的带来了对各种 API 接口，或是其它移动应用的访问需求。STS（Security Token Service）支持令牌转换服务，亦即使用一种主身份令牌去换取访问一个服务所需要的另外一种令牌。这样，可以实现接口级别的统一认证。通常，负责验证用户的被称为身份提供方 NSFOCUS UIP 服务提供方被称为 RP (Relying Party)。

绿盟科技的 STS 是实现“云大物移”统一认证的重要一环。也就是说，问多个不同的业务系统，不需要反复登录。这个主要是针对大数据平台提供众多服务的应用场景。比如我们给阿里云 API 网关实现的一个令牌，可以访问后面上百种服务的场景。

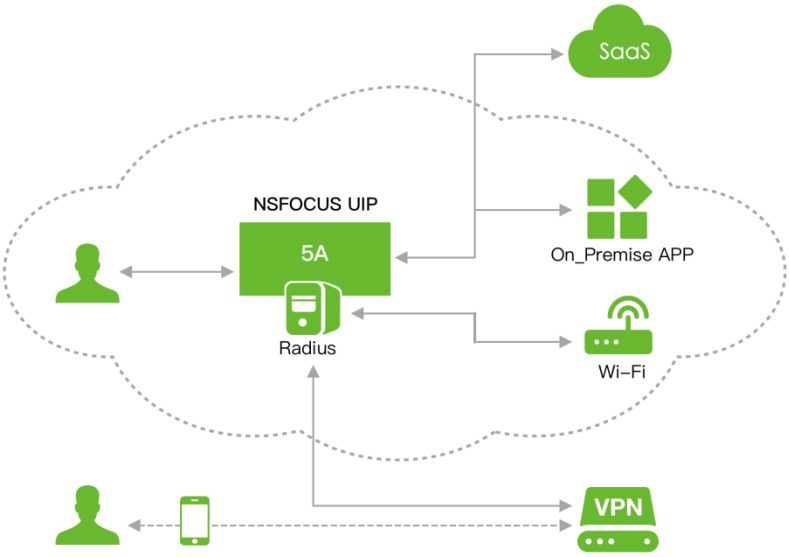
1) 更统一：通过我们的 STS，可以实现一次认证，换取访问各种业务应用 RP 所需要的各种令牌；比如一个证书，一个主账号可以打通所有第三方的 API 服务接口；
2) 更安全：通过 STS，可以通过 OIDC 等非对称密钥协议实现一次一密，从而替代传统的常年不变的密码；即使在网络层被截获，也不能重放/中间人攻击。
3) 更便捷：开发者无需理解复杂的认证协议和流程，只需要注册成为开发者，按照向导一步一步实现即可。

API 令牌 STS 是使用 OIDC 协议（1.0 版本）实现的 API 认证与授权解决方案。OIDC 协议（1.0 版本）是基于 OAuth2.0 授权协议基础上的由 Google，微软，Facebook 等公司于 2014 年发布的最新的认证授权协议（http://openid.net/specs/openid-connect-core-1_0.html），具有更高的安全性，灵活性，并符合未来安全发展的趋势。在该协议中，使用令牌（id_token）替换 OAuth2 的 access_token，id_token 生成时使用私钥进行签名，使用时用公钥进行校验。使用 JSON 数据格式进行传输，并支持各类加密算法（如 RSA）。

NSFOCUS UIP 的 API 令牌 STS 服务主要是提供一个 Token 令牌生成服务。用户通过一种身份认证服务后，获取一个 PT(Primary Token)，可以利用这个 PT 来换取访问各个业务应用的 ST(Secondary Token)。在启用了 OIDC（OpenID Connect），SAML 等身份认证协议以后，不但所有的 PT 会有刷新机制，ST 也可以定期更换，甚至一次一密。从而更好的保证业务认证授权的安全，即使在不安全的网络环境下。

4.2.3.4 其他认证

传统防火墙、VPN 等安全措施已无法完全抵御层出不同的攻击手段，如何防御应用层攻击威胁，与传统安全措施联动，整体提升信息化安全防护，是我们无法回避的问题。NSFOCUS UIP 可以与 VPN 联动，登录 SSL VPN，直接打开应用门户，单点登录到更多应用，这样用户体验更好，WI-FI 也可以达到同样效果，除此之外，像门禁、网络交换设备、主机设备等都能纳入绿盟统一身份认证平台管理体系进行统一管理，针对不同人员分配不同的软、硬件资源。

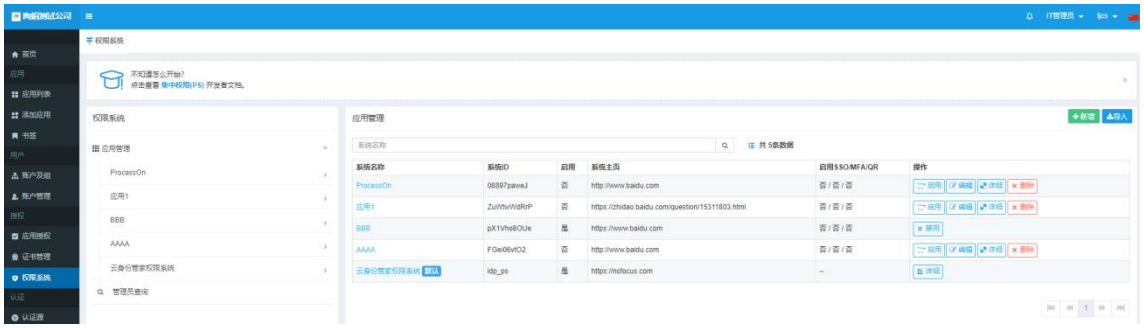


4.2.4 集中权限（ Authorization ）

集中权限（ Authorization ）：在应用资源有效管理的基础上，建立以人为主体、应用为客体的网上在线授权管理体系，控制力度为门户级授权；并建立对人员权限申请、审批和授权的网上流程化管理；实现对网上用户统一的权限控制和管理。

通过集中授权管理，建立统一用户管理和权限视图，当用户职务、岗位等自然属性发生变化时，可以较快地响应变化，根据用户新的属性自动调整其能访问的应用客体对象，进一步降低管理成本，提高工作效率。通过系统创建安全组，将所有的系统用户以组的形式管理起来，通过应用授权给安全组或通过安全组指定应用两种授权机制，已达到管理用户的访问去向。

可以根据用户、组织机构、角色进行灵活授权，并可对下属机构建立的管理员分配该机构所有管理权限，真正实现分级授权管理能力。通过信息同步、建立权限系统，与应用系统权限接口对接实现二级、三级授权能力。



4.2.4.1 一级授权

集中权限，通过默认部门组和自建角色组，对用户权限进行多维度及细颗粒度的划分，实现跨部门、跨地区的分层分级管理。

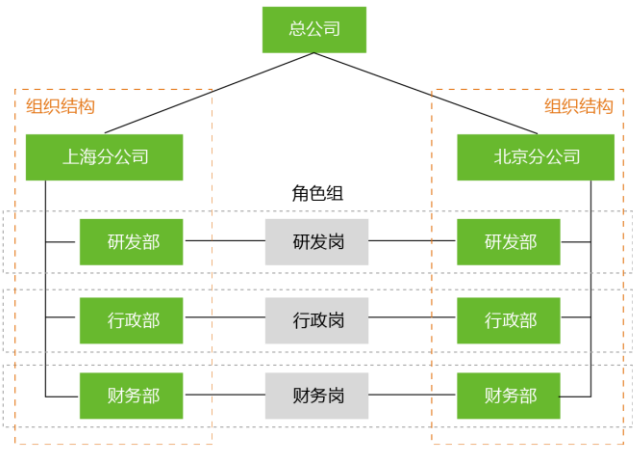
维度除了纵向按照组织架构定义外，还可以横向按岗位角色定义，一横一竖，形成矩阵，实现角色的灵活组合。

1） 纵向管理（HR 发起的公司组织架构树形结构）：

从总公司-分公司-部门-组-岗位的组织架构管理，统一由 HR 系统发起，确保组织架构的唯一性，避免多套系统组织结构冲突形成业务系统数据结构孤岛现象发生。

2） 横向管理：（NSFOCUS UIP 矩阵式结构管理）：

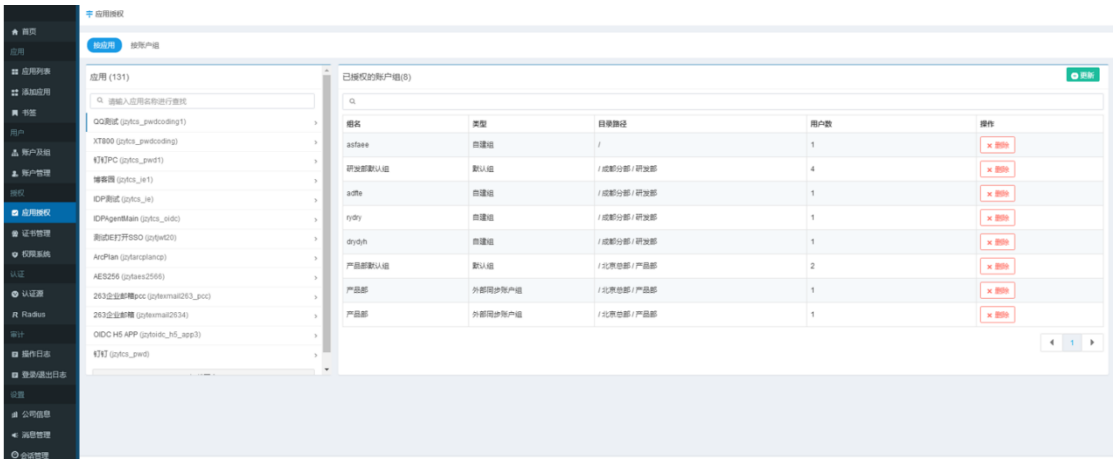
NSFOCUS UIP 管理员通过建立角色组或者项目组等形式，结合公司的树形组织架构创建矩阵式结构管理。



为确保信息资源访问的可控性，防止信息资源被非授权访问，需要在用户身份真实可信的前提下，提供可信的授权管理服务，实现对各类用户的有效管理和访问控制，保护各种信息资源不被非法或越权访问，防止信息泄漏。

NSFOCUS UIP 提供信息资源管理、用户角色定义和划分、权限分配和管理、权限认证等功能。权限管理主要是由管理员进行资源分类配置、用户角色定义及授权等操作；权限认证主要是根据用户身份对其进行权限判断，以决定该用户是否具有访问相应资源的权限。

由于采取分布式的 RBAC 授权管理模型，首先应对用户进行严格的身份认证，保证用户身份的真实性，在此基础之上再综合各个业务系统内部资源，对业务系统进行严格的权限把控，实现各个业务系统内部资源细粒度的授权访问控制。



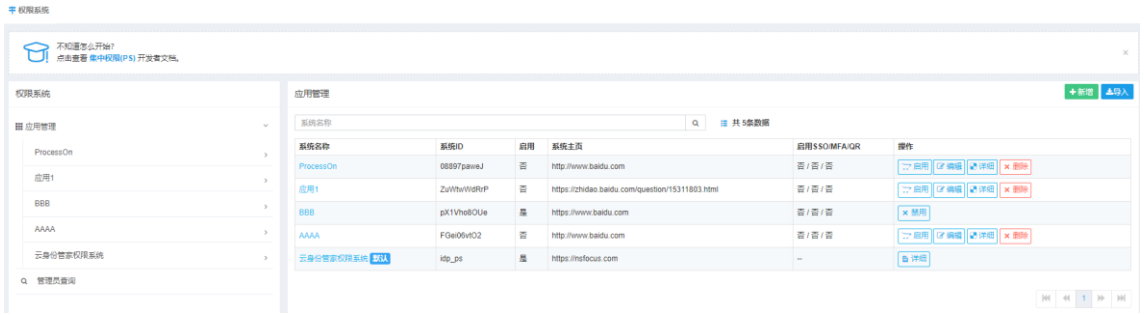
4.2.4.2 二级授权

通过二级授权，可实现平台统一管理平台下所有应用系统内部权限能力，原有业务系统均无需再存储账户信息及权限信息。平台将相当于一个大应用，而平台内所有系统将只提供功能，权限由平台统一管理。

系统提供开发者角色，此角色可实现业务系统对接平台实现二级授权所需进行的配置及操作，平台提供完整详实的操作使用文档，帮助开发人员快速实现权限对接。在实现二级授权前，需先实现系统集成完成 SSO 单点登录 SSO 及账户同步、统一存储功能，在完成前两步工作后，方可实现二级授权的操作配置。

1） 应用管理

应用管理用于管理集成进来的应用系统，如图：



应用管理

在应用管理页面可以做如下操作：

【新增】可以新增应用系统，新增后，应用系统默认是禁用状态；

【启用】/【禁用】可以启用或禁用当前应用系统；

【编辑】可以编辑应用系统相关信息；

【详细】可以查看当前应用系统的详细信息；

【删除】可以在确认操作后删除当前应用系统；

每一个应用系统下又分为角色管理，资源管理，成员管理：

2） 角色管理

角色可以理解为一定数量的权限的集合，权限的载体。

权限系统可以新增、编辑、删除系统角色，并为不同角色赋予不同的权限（即可访问的资源）。

在角色管理处，可以为账户/组赋予角色，通过角色将权限授予用账户/组。

角色与组/账户是多对多的关系。

在角色管理处，可以查看某一个角色下的所有账户/组。

角色管理

在角色管理页面可做如下操作：

【批量删除】可以勾选多个角色，批量删除角色，默认的角色不可被删除；

【编辑】可以修改角色的相关信息；

【删除】可以删除单个角色；

【指定单位或部门】可以为开发者角色指定其可以操作的单位或部门，用于第三方业务系统推送账户至身份管理平台功能；

【新增角色】可以新增一种角色，如图；

新建角色

【关联成员】可以添加账户或组成为其成员，如图：

关联成员

在“关联成员”界面，可做如下操作：

【添加关联】可以添加账户或组成为其成员；

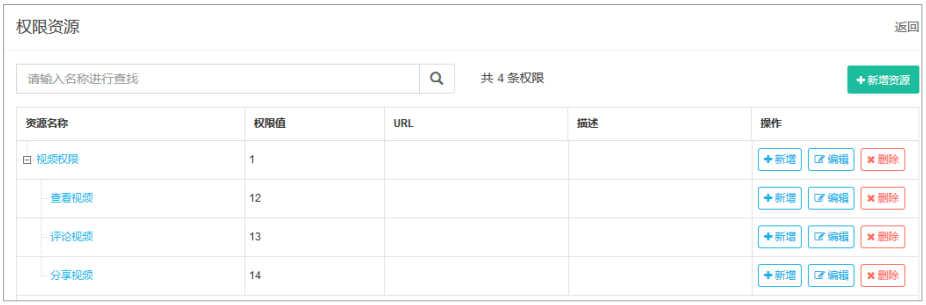
【取消关联】可以取消账户或组与角色的关联；

【批量取消关联】可以勾选多个成员，批量取消账户或组与角色的关联；

【关联权限】可以为角色添加或取消权限，如图：

3） 权限资源

权限资源用于管理相应的权限；并以树的形式显示权限资源，展示权限的等级结构，如图：



权限资源

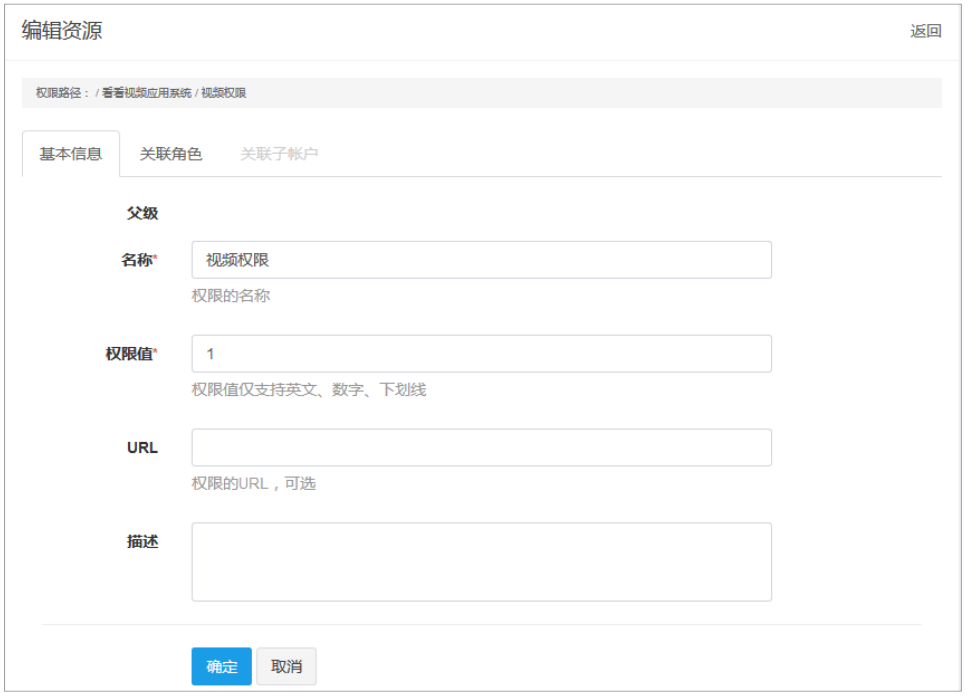
在权限资源页面，可做如下操作：

【新增资源】可以在根目录下创建权限；

【新增】可以在该权限下创建新权限；

【删除】可以删除该权限资源；

【编辑】可以修改该权限的基本信息和进入关联角色界面；



编辑资源

在 “基本信息”页面可以编辑权限名称、权限值、URL 和描述信息；

关联角色

在“关联角色”页面可做如下操作：

【添加关联】可以为权限添加角色关联；

【取消关联】可以单个取消角色关联；

【批量取消关联】可以批量取消角色关联；

4.2.4.3 三级授权

三级权限管理，即对数据访问层面的权限管理，可用于更精细的权限控制，力度更细，更精准。与一级权限，二级权限控制相比，三级在权限设置时会更细致，在指定模块权限的基础上，增加其数据访问的权限（如指定此权限能访问具体的哪几行数据，或哪些字段的数据）。

在系统的权限系统模块中，可实现对三级权限的控制，在权限资源的管理中，增加了对数据访问控制的设置（即三级授权），可按具体的权限按“行”记录范围或“列”字段范围进行数据访问设置（如设置快递人员只能看到分配给自己的订单且看不到金额， 区域经理则能看到下属的所有订单且能看到金额，而客服能看到所有订单， 但是每次只能查询一个但能看到金额） 。为了保证系统的兼容性， 用户可以自定义表达式， 但推荐 Apache Shiro 兼容的方式。规则为：“资源标识符：操作：对象实例 ID” 即对哪个资源的哪个实例可以进行什么操作。


获取角色的所有权限

获取指定角色的所有权限信息

请求URI:

/api/developer/ps/role_permissions/{psId}/{roleUuid} GET REST

Content-Type: application/json

请求参数:

参数名	参数值	备注
psId	{psId}	权限系统ID，URL传递参数
roleUuid	{roleUuid}	角色uuid，URL传递参数
access_token	{access_token}	

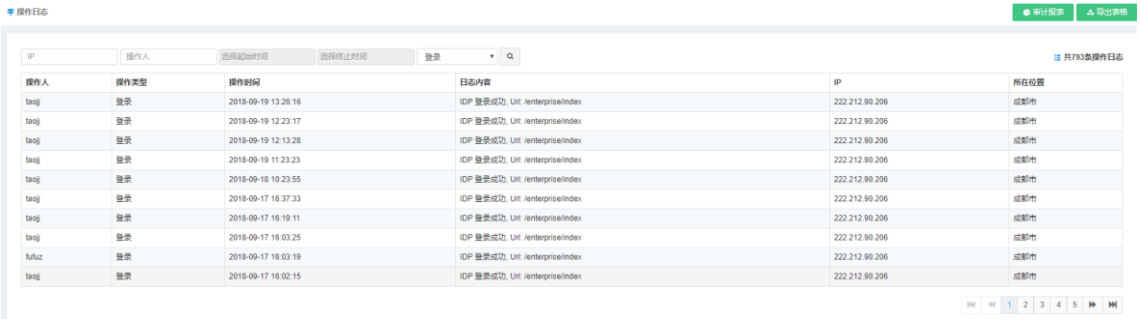
请求示例:

/api/developer/ps/role_permissions/MuJsnHwYAq/93f9d9afe6dd4b5ea40a9264959519f3ocHUD9Kjrka?access_token=9bb3a762-1626-48d3-be29-9b7e5865831c

4.2.5 透明审计

透明审计（Audit）：记录系统范围内的安全和系统审计信息，有效地分析整个系统的日常操作与安全事件数据，通过归类、合并、关联、优化、直观呈现等方法，使管理员轻松识别应用系统环境中潜在的恶意威胁活动，可帮助企业/用户明显地降低受到来自外界和内部的恶意侵袭的风险。在积累了一定的数据后，采用大数据平台，更可以形成一定的规则，直接封 IP、限流量、限时等，并可以在认证的时候实现主动防御，瞬间互动。这样可以有效的防止刷单等操作。

4.2.5.1 管理员审计



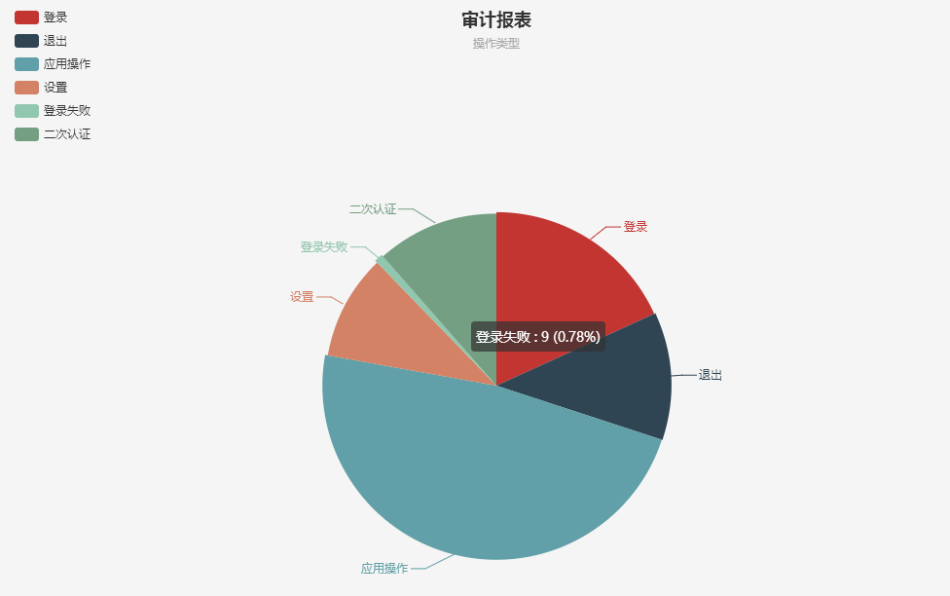
- 日志可以提供查询、备份等管理功能；
- 各单位管理员可查询本机构日志；
- 系统管理员可查询所有日志；
- 安全审计员可以备份、删除日志（只能以时间段备份及删除）；
- 备份/删除日志操作时间有记录，备份/删除的记录不删除；
- 可设置备份提醒，在管理员登陆时提醒。

4.2.5.2 用户账户审计

系统支持检查某个用户一段时间内的使用情况，并且通过一系列安全策略建立起正常使用的模型。这样当系统遭遇撞库等攻击时，能够及时自动做出响应，符合动态防御的原则。

- 检查当前访问网络的用户数量。
- 识别通过远程计算机访问的用户检查所有用户的高峰登录时间。
- 查看上次访问重要资源的用户。
- 发现试图登录不具访问权限的计算机的用户。
- 查看任一个用户登录的全部历史。
- 同一个用户在短时间内从不同地方登陆情况，全面了解用户活动的安全情况。
- 实时预警功能，提供关注重要事件的实时告警。
- 支持计划报表，提供自动发送用户选择的相关报表到管理员邮箱功能。

- 提供自定义报表，要求提供基于用户、计算机、组策略、组织单元等内容定制各种报表。



审计报表

提供自定义活动目录事件数据的保存周期，按周期清理数据库过期事件数据功能。

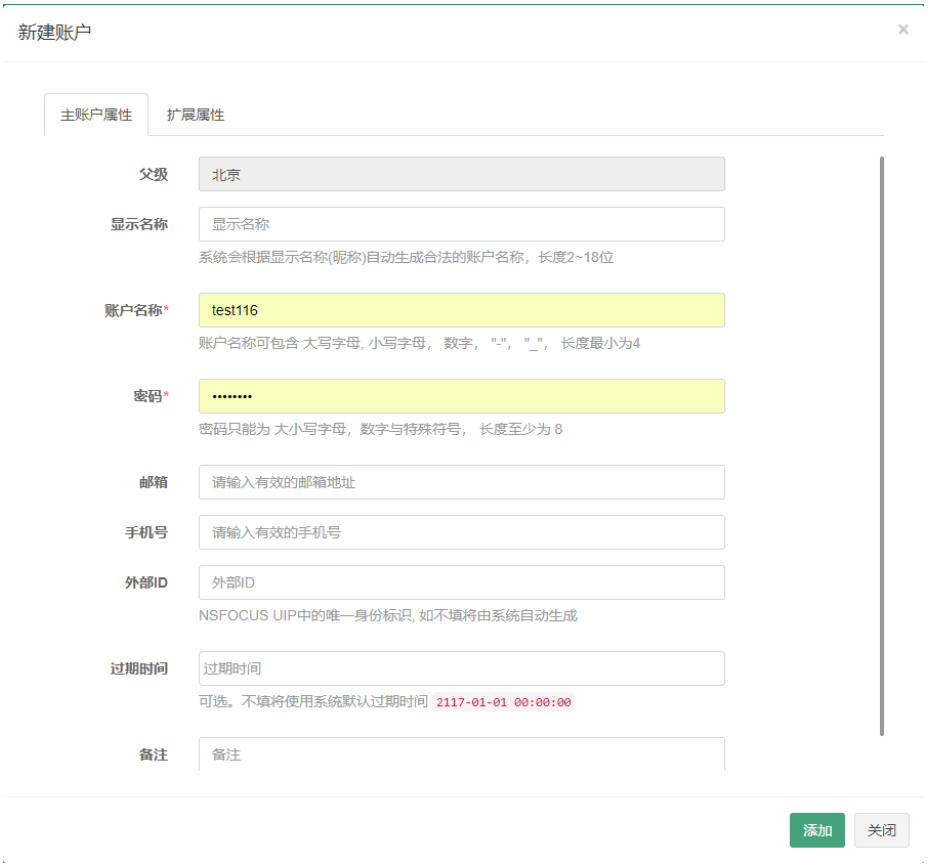
提供日志自动归档功能：即基于用户设定的时间间隔对日志进行自动存档，存于指定目录。

4.2.6 开发者服务

NSFOCUS UIP 自身便提供统一标准规范，平台自带开发者服务功能模块，此模块不但提供应用系统账户、认证、授权、审计、应用的集成能力，并提供针对所有功能实现的标准规范，满足未来客户新业务系统实现统一规范化集成集成、管理，形成标准化流程操作，确保对信息化需求的满足。如下图：

1） 账户规范

可以使用手机号、员工 ID 以及邮箱等方式进行登陆系统，并可以根据用户和用户密码提供可配置的管理策略，用户名注册的策略、密码长度的策略及用户登陆策略、用户访问策略以及用户的行为策略。



2） 认证规范

提供多种的标准身份认证协议，不同的应用场景选择不同的技术，灵活可控。

- SAML：金融级的跨域身份认证标准，适用于云计算
- OIDC： API 认证授权标准，适用于大数据接口
- FIDO： 2C 的去密码化身份认证标准，适用于物联网
- NAPPS：移动应用的统一认证标准，适用于移动 APP 的统一认证

3） 集成规范

针对 PHP，JAVA，.NET，Python 等常见的开发语言，提供业务应用集成的开发者服务及样本代码。业务应用开发者可根据我们提供的规范进行应用的开发，快速集成到绿盟统一身份认证平台。

4） 数据规范

严格定义 API 接口中参数数据规范，业务系统需要根据我们提供的字段标准来开发接口。

Request URI: /api/application/scim/organization PUT REST

Content-Type: application/json

业务系统需要根据我们提供的字段标准来开发接口，如下所示:

参数说明:

参数名	参数值	备注
organization	{organization}	组织机构的名称
parentUuid	{parentUuid}	所属父级组织机构的uuid或外部ID
rootNode	{rootNode}	是否是根节点
organization...	{organizationU...	本组织机构的uuid或外部ID
manager	{manager}	组织机构的管理者,value是管理者账户的外部ID,display是用户名,管理者可为空
regionId	{regionId}	组织机构所属的区域id,type为SELF_OU(自建组织机构)时有可能会有值,可为空,type为DEPARTMENT("自建部门")不会出现值
type	{manager}	SELF_OU(自建组织机构)或DEPARTMENT("自建部门")

5) 管理规范

- 基于角色访问控制（ RBAC ）设计，对角色、组及账户进行不同的授权，从不同维度、颗粒度集中分配权限，防止越权操作。
- 提供二级授权模块，使业务应用开发人员可以专注在业务逻辑上，不需要对应用内的权限模型进行再次开发

五. 产品价值

- **员工的价值**

从员工角度来看，NSFOCUS UIP 解决了他们记忆多个用户名、密码的烦恼，解除了使用多个应用系统必须进行多次认证的重复劳动，提高工作效率使员工更多精力投身到业务工作当中，减少了因员工密码泄露而带来的企业安全风险，弥补传统信息安全无法提供的安全防护；

从系统管理员来看，NSFOCUS UIP 可以使他们从繁琐的账号密码管理工作中解脱出来，不必每天为员工在多个不同业务系统后台重置密码而苦恼，使信息化工作人员可以将精力投入到更多有意义的 IT 建设工作中，提升企业信息化整体水平。

- **企业管理者的价值**

NSFOCUS UIP 可全面提升企业核心竞争力，由原有各业务系统单兵作战转为集群化作业，消除企业内部信息流通不畅、交互困难问题，促进企业内部人员有效沟通，提高员工合作意识，增强企业凝聚力，实现全球化竞争实力；

实现革新企业管理模式，信息化协助企业人为管理，而 NSFOCUS UIP 可减少管理中矛盾、问题的产生，有效监管工作人员的工作情况，实现实时工作任务的监督与催办；明确工作岗位与工作职责，增强人员的责任感，减少工作中的推托、扯皮等现象，从根本提高企业管理自动化水平，提升企业经济效益；

通过 NSFOCUS UIP 整合企业管理、生产、服务、经营、决策能力，实现资源整合、提高资源综合利用水平，加强企业生存力及竞争环境下快速应变能力，协助企业在市场竞争中争分夺秒立于不败之地；

NSFOCUS UIP 可实现“云大物移”多领域各应用系统统一集成，在改善现有信息化管理模式同时，展望、着眼未来发展，采用超前意识及高新技术，实现一次性采购，长期受益，在为企业信息化能力带来提升的同时，降低采购成本，达到“一劳永逸”的效果。

- **企业 IT 化建设升级**

多个应用系统，员工可自由切换，实现单点登录，多地漫游，真正提高办公效率；

采用模板化、轻开发实现单点登录，降低实施成本、缩短实施周期、减少实施风险；

实现集中的用户管理，便捷的单点登录，细粒度的权限控制和全方位的审计分析，达到事前审批、事中控制和事后审计的全方位安全管理，并

形成大数据分析，提升对危险、危害的态势感知能力及风险预判能力；

整体降低安全风险，提高企业内部核心数据安全防护，提升对外信誉和形象；

- **商业数据的安全价值**

信息安全本身包括的范围很大。大到国家军事政治等机密安全，小到如防范商业企业机密泄露、防范个人信息的泄露等。网络环境下的信息安全体系是保证信息安全的关键，包括计算机安全操作系统、各种安全协议、安全机制（数字签名、信息认证、数据加密等），其中任何一个安全漏洞便可以威胁全局安全。信息安全服务至少应该包括支持信息网络安全服务的基本理论，以及基于新一代信息网络体系结构的网络安全服务体系结构。

信息作为一种资源，它的普遍性、共享性、增值性、可处理性和多效用性，使其对于企业具有特别重要的意义。信息安全的实质就是要保护信息系统或信息网络中的信息资源免受各种类型的威胁、干扰和破坏，即保证信息的安全性。根据国际标准化组织的定义，信息安全性的含义主要是指信息的完整性、可用性、保密性和可靠性。但是，对于不同的企业和行业来说，其对信息安全的要求和重点却是有区别的。最重要的问题是不能在对非法（非授权）获取（访问）不加防范的条件下传输信息。

2015 年，世界上发生了多起大数据泄露事件。携程信用卡信息泄露事件，“心脏出血”漏洞事件……这些服务器证书隐私等敏感数据泄露的事件，让人们对数据安全感到忧虑。

阿里巴巴无线安全首席架构师潘爱民透露，我国全网已泄露个人账号超过 21 亿条，覆盖全网账号的 40%以上。

目前，世界各国都比较重视大数据的发展。2015 年 8 月，中国出台了关于促进大数据发展的行动纲要，中国“十三五”规划也明确指出拓展网络经济空间，推进数据资源开放共享，实现国家大数据战略，超前布局下一代互联网。

综上所有叙述，数据安全是现在面临的一大挑战，NSFOCUS UIP 就是用来规范保护用户账号信息的关键技术环节，也是未来边界安全新定义。通过单点登录一次一密的会话机制，使用户的账号信息从根源上防范不被窃取，从而保护用户数据信息的安全。

六. 产品性能设计及运行环境配置

6.1 性能设计

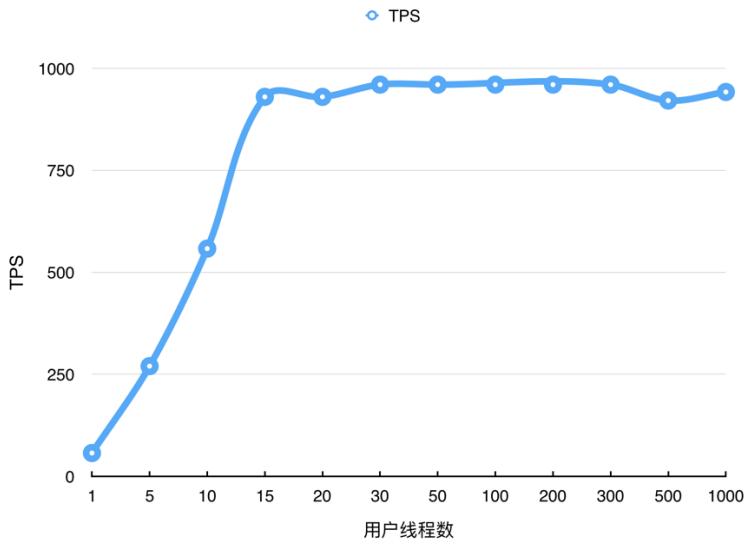
NSFOCUS UIP 支持水平扩展，通过负载均衡实现微服务调度。首先，可根据业务需要优化微服务设计提高单节点性能，确保系统运行稳定；其次，系统设计可支持集群部署，考虑到集群中主机数量到达一定程度后会有 80%的衰减，通过负载均衡、LB 等手段，可以满足项目的性能要求。并支持分布式部署确保验证过程最短路径。

针对单机性能指标如下：

1) 统一身份认证可满足服务 1,000,000 以上用户量；

2) 支持最大服务并发访问量不小于 3000 个，在系统达到最大峰值时表现稳定；

3) 支持最大处理登录请求（TPS）≥1000/秒；



如上图所示，当并发逐渐增加时，系统的处理能力将达到一定峰值，依据业务场景，可达到 1000Tps。

6.2 运行环境配置

软硬件**最低**要求：

硬件环境	应用服务器	数据库服务器	客户端
硬件配置	CPU ： Intel(R) Celeron(R) CPU 2.40GHz stepping 01 内存：4G 硬盘：500G	CPU ： Intel(R) Celeron(R) CPU 2.40GHz stepping 01 内存：4G 硬盘：500G	无
软件配置	OS ： windows server 、Linux Jre 版本：1.8 Web 服务器：tomcat8+	OS：windows server 数据库：mongodb2.6.6	浏览器：360、chrome、IE7 以上、火狐、Safari 等浏览器

以上是系统运行的最低配置，系统基于 J2EE 架构设计，软硬件兼容性良好，系统运行环境的配置原则及支持情况如下：

硬件环境：

CPU：Intel 四核 @ 2.50GHz 或以上(CPU 越高越好，运行越流畅)；

硬盘：400G 以上；

内存：16G 以上；

显示器：分辨率 1024*768 或以上；

外设：USB 接口，键盘鼠标；

网络带宽：要求 10M 带宽；建议 20M 以上；

软件环境：

数据库：支持 NoSQL（默认是 MongoDB）、Oracle；

Web 应用服务器：支持 Tomcat7.0、WebLogic 等；

JDK：支持 JDK1.8 及以上的版本；

浏览器：兼容 360、Chrome、IE7 以上、火狐、Safari 等浏览器；

操作系统：支持 Windows 系列、Linux 系列、中标系统，包括 32 位和 64 位版本。HA 双机：支持双机备援，防止设备故障造成网络瘫痪，提升整个网络的可靠性；负载：支持用 Nginx、HA-Proxy、Apache 等服务器做负载均衡，来提高系统的高可用性。

服务器：支持联想、IBM、浪潮、华为、曙光等多种服务器部署。