

数字身份管控平台(员工版)

操作指南





【版权声明】

©2013-2024 腾讯云版权所有

本文档(含所有文字、数据、图片等内容)完整的著作权归腾讯云计算(北京)有限责任公司单独所有,未经腾讯云事先明确书面许可,任何主体不得以任何形式复制、修 改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯,腾讯云将依法采取措施追究法律责任。

【商标声明】

🔗 腾讯云

及其它腾讯云服务相关的商标均为腾讯云计算(北京)有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标,依法由权利人所有。未经腾讯云及有关权利人书 面许可,任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为,否则将构成对腾讯云及有关权利人商标权的侵犯,腾讯云将依法采取措施追究法 律责任。

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况,部分产品、服务的内容可能不时有所调整。 您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定,除非双方另有约定,否则,腾讯云对本文档内容不做任何明示或默示的承诺或保

证。

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务,及相应的技术售后服务,任何问题请联系 4009100100或95716。



操作指南

文档目录

概览
用户管理
管理组织机构
管理用户
管理用户组
应用管理
新建应用
配置应用
账号管理
账号组管理
资源管理
授权管理
应用授权
资源级授权
认证管理
审计管理
同步中心
上游同步
新建数据源
配置数据源
删除数据源
下游同步
新建数据源
配置数据源
删除数据源
系统配置
安全设置
短信模板配置
个性化设置
其他管理
注册审批
账号审批
管理员管理
企业微信同步
API 认证与鉴权
概述
步骤1:创建服务
步骤2:创建 API
步骤3:创建 API 网关应用(可选)
步骤4:资源级授权(可选)
步骤5:调用 API



操作指南 概览

最近更新时间: 2022-12-06 17:13:39

数字身份管控平台(员工版)的概览界面作为系统的信息展示处理中心,可以实时展示您的系统用户总数、应用总数、数据源总数、认证源总数、短信用量总数以及用户访 问登录的实时动态,并提供快捷登录入口和快捷功能使用,帮助您更有效率的使用系统。

使用快捷操作

- 1. 登录 数字身份管控平台(员工版)控制台,在左侧导航中,单击概览,进入概览页面。
- 2. 在概览页面底部的快捷操作模块中,提供了快捷登录入口和快捷功能使用,单击"链接"即可快速访问对应的功能页面。

快速操作 快速量示入口	快捷功能使用		
数字身份管控平台 (员工版) 登录 🕖	添加企业微信数据源 ⊙	添加用户 ④	添加应用授权 ⊙
用户门户登录团	添加企业微信扫码登录 ⊙	添加应用 ⊙	查看审计日志 ⊙

配置短信服务提示

如果没有配置腾讯云短信服务,在 <mark>概览页面</mark> 上方,将提供配置腾讯云短信服务入口。单击**立即配置**,跳转到短信模板配置页面,您可以通过短信服务配置指引进行短信模板 配置。



查看系统数据总览

- 1. 在 概览页面 的系统数据总览模块中,可以查看当前系统下用户总数、支持用户总数、应用总数、数据源总数、认证源总数和短信用量总数。
- 2. 单击**立即选购**进入产品选购页面,可以根据您的需要选购产品;单击**计费详情**可以查看产品的计费详情。

				计费注情 🗹
11100 ^个	7 ↑	0 个 影響感激	0 个	0 条
用户总数 支持用户总数()	应用总数①		认证源总数	透信用最总数

查看用户访问统计

在 概览页面 的用户访问统计模块中,可查看近7天、14天、30天的用户成功登录次数和失败登录次数。



查看最近登录用户

在 概览页面 的最近登录用户模块中,可查看最近登录的用户信息和操作详情。

最近登录用户

用户名称	IP	登录时间	操作类型	操作详情
		2021-1	用户登录	月
		2021-1	用户登录	月
		2021-1	用户登录	月
u	7	2021-1	用户登录	月
u	7	2021-1	用户登录	月
		2021-1	用户登录	月
		2021-1	用户登录	月
		2021-1	用户登录	月



用户管理 管理组织机构

最近更新时间: 2022-12-06 17:11:51

本文将为您介绍如何在数字身份管控平台(员工版)控制台中,新增、查看、编辑导出组织机构等。

进入组织机构页面

1. 登录 数字身份管控平台(员工版)控制台,在左侧导航栏,选择用户管理>组织机构管理。

2. 在左侧组织机构树中,定位需要操作的组织机构,单击右侧"···"图标。

数字身份管控平台 (员 工版)	组织机构管理							RELEARING RE	10401
語 概況 え 用P管理 ^	企业组织机构	用户组1							
一组织机构管理	 ■ 株式協会部時代時 ■ ● 根节点 		批量等入 v 用户原款	承执导码	8201916	用户状态 ★	於這本市	清输入用户名称:用户现称:于机号 运作	Q
 用户相管理 2 从证管理 	 ご用が回す ご用や回す 	新婚子組织						線織用户 無除 重重密码 冻结用户	
15 应用管理 	▶ 🛅 A7公司	編編進府 發出初始 時出用/*						10 * 条/页	н

3. 在弹出的操作框,可以进行新增子组织、编辑组织、查看组织详情、导出机构及导出用户操作。

新增子组织

在组织机构树中,可以根据需要增加子组织。

- 1. 在组织机构树弹出的操作框,单击新增子组织。
- 2. 在弹出的对话框,填写子组织信息后,单击确定,即可新增子组织。

上级组织们的		
组织机构名称 *	请输入组织机构名称	
组织机构代码 *	L	φ
	机构代码只能包含0-9,A-Z,a-z和-,长度不超过64位 点击右侧按钮自动生成一个代码不能超过64字符	
组织机构描述	请输入组织机构描述	

查看组织详情

组织机构树中,支持查看所有组织的基本信息。

1. 在组织机构树弹出的操作框,单击**组织详情**。

2. 在组织详情页,可查看该组织的上级组织、组织名称、机构代码及组织描述。



组织机构详情		>
上级组织机构	根节点	
组织机构名称		
组织机构代码		
组织机构描述		

编辑组织

管理员可修改组织属性信息,如组织名称、机构代码及描述。 1. 在 组织机构树弹出的操作框,单击编辑组织。

2. 在弹出的对话框,编辑需要修改的机构属性,如组织名称、机构代码及描述。

导出机构

组织机构管理功能支持导出所选组织机构下的所有组织信息。

- 1. 在 组织机构树弹出的操作框,单击导出机构。
- 2. 在弹出的对话框,确认无误后,单击确定,即可下载导出该组织下的所有机构信息。

导出用户

组织机构管理功能支持导出所选组织机构下的所有用户信息。

- 1. 在组织机构树弹出的操作框,单击导出用户。
- 2. 在弹出的对话框,确认无误后,单击确定,即可导出该组织机构下所有用户信息。



管理用户

最近更新时间: 2022-12-06 17:12:12

本文将为您介绍如何在数字身份管控平台(员工版)控制台中,新建、编辑、删除、重置密码、冻结用户等操作。

进入组织机构页面

- 1. 登录 数字身份管控平台(员工版)控制台,在左侧导航栏,选择**用户管理>组织机构管理**。
- 2. 在左侧组织机构树中,单击需要管理用户的组织机构,在右侧的用户列表,可新建管理用户。

企业组织机构							
清输入组织机构名称或代码	新建用户 删除	批量导入 ▼				请	输入用户名称/用户昵称/手机号 Q
► 10 根节点	用户名称	用户昵称	手机号码	邮箱地址	用户状态 \$	数据来源	操作
					未启用	自建用户	编辑用户 删除 重置密码 冻结用户
· D	c				正常	自建用户	编辑用户 删除 重置密码 冻结用户
› 🖬							

新建用户

- 1. 在 组织机构右侧的用户列表,单击新建用户。
- 2. 在弹出的对话框,填写用户基本信息,包括用户名称、密码、用户昵称、手机号码等,主组织机构默认为新建用户时选中的组织机构,次要组织机构支持多选,单击**确** 定,即可添加成功。

说明 新建用户默认状态为未启用,新用户登录重置密码后,状态将变为正常。



密码 • 用户昵称 • 手机号码 • 邮箱地址	请输入8~12位包含大小写字母、数字、特殊字符密码 请输入用户昵称 中国大陆(+86) ▼ 请输入手机号码	Ø
用户昵称 ◆ 手机号码 ◆ 邮箱地址	请输入用户昵称 中国大陆(+86) ▼ 请输入手机号码	
手机号码 ★ 邮箱地址	中国大陆(+86) ▼ 请输入手机号码	
邮箱地址		
	请输入邮箱地址	
所属主组织机构 *	根节点/用户组1	~
所属次要组织机构	请选择所属次要组织机构	
所属用户组	请选择所属用户组	
过期时间	请选择过期时间	Ö
备注	请输入备注	
	首次登录时重置密码	

查看用户详情

用户添加成功后,可查看用户详情信息,如基本信息、已授权应用、所属用户组等。 1. 在 组织机构右侧的用户列表,单击需要查看详情的用户名称。

新建用户 删除	批量导入 ▼				请编入	用户名称/用户昵称/手机号 Q
用户名称	用戶昵称	手机号码	邮箱地址	用户状态 🕈	数据来源	操作
				未启用	自建用户	编辑用户 删除 重置密码 冻结用户
				正常	自建用户	编辑用户 删除 重置密码 冻结用户

2. 在用户信息详情页,可查看用户信息、已授权应用及所属用户组。



日本		9 用户状态	田用户来源
用户名称	手	1号码	创建时间
是否管理员	由B윢	自地址	过期时间
细细和构日录			
第三方账户绑定			

编辑用户属性

用户添加成功后,可修改用户属性信息,如用户名称、关联邮箱、手机号码等。

- 1. 在 组织机构右侧的用户列表,单击"操作"列的**编辑用户**。
- 2. 在弹出的对话框,编辑用户信息后,单击确定。

编辑用户		×
用户名称 *	Z	
用户昵称★		
手机号码★	中国大陆(+86)	
邮箱地址	请输入邮箱地址	
所属主组织机构 *	根节点	
所属次要组织机构	请选择所属次要组织机构	
所属用户组	请选择所属用户组	
过期时间	请选择过期时间	
备注	清输入备注	
	首次登录时重置密码	
	確定 取消	

删除用户



新建用户 删除	批量导入 ▼					请输入用户名称/用户昵称/手机号	Q
用户名称	用户昵称	手机号码	邮箱地址	用户状态 🕈	数据来源	操作	
				未启用	自建用户	编辑用户删除重置密码	冻结用户
d				正常	自建用户	编辑用户 删除 重置密码	冻结用户

• 方式2:在用户列表,选中一个或多个需要删除的用户,在列表上方,单击**删除**。

重置密码

腾讯云

1. 在 组织机构右侧的用户列表,单击"操作"列的重置密码。

新建用户 删除	批量导入 ▼					请输入用户	名称/用户昵称/手机号	Q
用户名称	用戶昵称	手机号码	邮箱地址	用户状态 🕈	数据来源		操作	
				未启用	自建用户		编辑用户删除重置密码 冻结月	刊户
d				正常	自建用户		编辑用户 删除 重置密码 冻结月	刊户

2. 在弹出的对话框,为该用户生成新的密码。

冻结用户

用户添加成功后,支持冻结用户,使其无法登录数字身份管控平台(员工版)控制台。 1. 在 组织机构右侧的用户列表,单击"操作"列的**冻结用户**。

新建用户 删除	批量导入 🔻					请输入用户名	3称/用户昵称/手机号	Q,
用户名称	用户昵称	手机号码	邮箱地址	用户状态 🛊	数据来源		操作	
				未启用	自建用户		编辑用户删除重置密码 冻结用	户
d				正常	自建用户		编辑用户 删除 重置密码 冻结用	户

2. 在弹出的对话框,单击确定,该用户即可被冻结,无法登录控制台。

批量导入数据

数字身份管控平台(员工版)支持导入组织机构、用户的 CSV 格式数据,支持同步导入企业微信、LDAP/AD 数据。 1. 在 组织机构右侧的用户列表,单击上方的**批量导入**,选择需要导入的方式,如单击**导入机构 CSV**。

北京分公司							
新建用户 删除	批量导入 ▼					请输入用户名称/用户昵称/手机-	, Q
用户名称	导入组织机构CSV 导入用户CSV	手机号码	邮箱地址	用户状态 🕈	数据来源	操作	
	3703 001			未启用	自建用户	编辑用户删除	重置密码 冻结用户
				正常	自建用户	编辑用户 删除	重置密码 冻结用户

2. 在弹出的对话框,下载导入模板,按模板要求填入对应的机构数据,然后上传模板数据。

3. 上传完成后,单击**开始导入**,即可批量导入模板数据。



管理用户组

最近更新时间: 2022-12-06 17:12:35

本文将为您介绍如何在数字身份管控平台(员工版)控制台,新增、编辑用户组,并在用户组中新增或移除用户。

进入用户组页面

管理员登录 数字身份管控平台(员工版)控制台,在左侧导航栏,选择**用户管理 > 用户组管理**。

新建用户组

1. 在用户组管理页面,单击新建用户组。

数字身份管控平台	用户组管理		
器 概変	新建用产档		
・ 组织机构管理	8 测试二组	////////·////////////////////////////	
• 用户组管理	创建时间:2021-04-08 21:17	创建时间:2021-04-08 21:11	
2 认证管理	56(134) (SE) FOR 201201/10/**	 596390 #559X X0201/67**	
	共 2 条		

2. 在弹出的对话框,填入用户组名称及备注信息,单击确定,即可完成用户组的新建。

法意 用户组名称不能 日	能重复。	
新建用户组		×
* 用户组名称	请输入用户组名称	
督注	请输入备注	
	職定	

编辑用户组

新增用户组后,可修改用户组名称及备注信息。

- 1. 在 用户组管理页面,单击用户组下方的编辑。
- 2. 在弹出的对话框,修改用户组名称及备注信息后,单击确定即可。

编辑		×
* 用户组名称	测试用户组	
賀注	请输入备注	
	職定 取消	

删除用户组

新增用户组后,如不再需要已新增的用户组,可删除单个用户组或批量删除用户组。



• 方式1: 在需要删除的用户组下方,单击删除。

新建用户组 删除	
※ ※ ※ ※ ※ ※ ※ ※ ※ ※ ※ ※ ※	

• 方式2: 勾选一个或多个需要删除的用户组,在用户组列表上方,单击删除。

新建用户组 删除		
《 》 测试用户组2	8 测试用户组	
创建时间: 2021-04-19 17:33	创建时间: 2021-03-23 16:54	
编辑 删除 添加用户	编辑 删除 添加用户	

用户组添加用户

新增用户组后,可在用户组中新增用户。

① 说明	
用户与用户组的关系为 N:N,同一个用户可以属于多个用户组。	

方式1

1

1. 在用户组管理页面,单击用户组下方的添加用户。

松 测试用户组2	
创建时间:2021-04-19 17:33 编辑 删除 添加用户	

2. 在弹出的对话框,选择需要添加的用户,单击确定,选中的用户将被加入到该用户组中。

添加用户					×
选择用户(60)			已选择用户 (1)		
请输入用户名称	(С,	用户名称	主键ID	
用户名称	主键ID				0
	01				-
	0				
	0:	+	•		
	0				
	1				
	1				
	40-40440 2-44 405- 5740 50407-400050				
	確	定	取消		

方式2

1. 在 用户组管理页面,选中所需用户组,单击其空白处,进入用户组详情页。



2. 在用户组详情页,单击**添加用户**。

用户组管理			班级管理员				х
新建用户组 删除			创建时间: 2021-09-12 12:09	备注:			
			添加用户移除用户		请输入用户名称/用户昵称/手机号	3	Q,
	·8·		用户名称	用戶昵称	手机号码	操作	
创建时间:2021-09-12 12:09 编辑 删除 添加用户	创建时间:2021-09-12 12:09 编辑 删除 添加用户	创建时间:202				移除用户	

3. 在弹出的对话框,选择需要添加的用户,单击确定,选中的用户将被加入到该用户组中。

用户组移除用户

在用户组中新增用户后,支持将其移除。

方式1

- 1. 在 用户组管理页面,选中所需用户组,单击其空白处,进入用户组详情页。
- 2. 在用户组详情页,单击右侧"操作"列的移除用户,可将该用户从用户组里移除。

用户组管理								Х
新建用户组 翻除			创建时间: 20	021-09-12 12:09	备注:			
			添加用户	移除用户		请输入用户名称/用户昵称/手	机号	Q,
	<u>将</u>		F 用户	2名称	用戶昵称	手机号码	操作	
创建时间: 2021-09-12 12:09	创建时间:2021-09-12 12:09	ŧ	建时间:202				经运用点	
编辑 删除 添加用户	编辑 删除 添加用户	6	辑删除				disk0/40/	

方式2

- 1. 在 用户组管理页面,选中所需用户组,单击其空白处,进入用户组详情页。
- 2. 在用户组详情页,选择一个或多个需要移除的用户,单击上方的**移除用户**,可批量将选中用户从用户组中移除。



应用管理 新建应用

最近更新时间: 2022-12-06 16:55:34

本文将为您介绍如何在数字身份管控平台(员工版),添加公司使用中的应用系统,为其集成单点登录,添加应用并同步账号信息后,账号可以通过控制台单点登录到应用 系统。

方式1: 应用协议新建

- 1. 登录 数字身份管控平台(员工版)控制台,在左侧导航栏,单击应用管理。
- 2. 在应用管理页面,单击**应用协议新建**。

应用协议新建	应用市场新建	批量删除
应用名称		应用ID
共 1 条		

3. 在选择应用协议模板页面,选择需要添加的应用,单击下一步: 配置参数信息。

③ AHGANDARE > ③ RESSIGN > ③ RE
R SAME (Sound America Manage 1998 STOLES, 1822) #7 ML 502, 5885 (America) (SS2598, CHR07) (SR8) X0887 (CR0) 249586668, X887948646890(S2, SAME74864690(S2, SSME74864690(S2, SSME7486490(S2, SSME7486490(S2, SSME7486490(S2, SSME7486490(S2, SSME748690(S2, SSME74890(S2, SSME74890(S2, SSME74890(S2, SSME74890(S2, SSME748690(S2, SSME74890(S2, SSME748690(S2, SSME74890(S2, SSME74890(S2,
CAS ((FRE)) CAS ((CHEST ALTINONICO, 19-4/CLUERS), 18.5.2.0) 20-4/6874/08.000001/09/08/08/09/07/3/S/CLU-4-00, 1992/08/0.
JUT JUT (JOON WID TAME) BERREGERERARGE-HEFTEONEFEREN. ARREBUNTEFORTLANDBAUER (SSO), JUT #ABERFERRENZE, BARR REPUCKUERMENLEDE, MERLEBLEDE, BERBELEBLEDE, BERBELEBLEBE, BERBELEBLEDE, BERBELEBLEDE, BERBELEBLEDE, BERBELEBLEDE, BERBELEBLEDE, BERBELEBLEDE, BERBELEBLEDE, BERBELEBLEDE, BERBELEBLEBERBELEBLEDE, BERBELEBLEDE, BERBELEBLEDE, BERBELEBLEDE, BERBELEBLEDE, BERBELEBLEDE, BERBELEBLEDE, BERBELEBLEDE, BERBELEBLEDE, BERBELEBLEDE, BERBELEBBE
OAunt2 OAunt2 OAunt2 目前空間 OAunt2 目前空間 OAunt2 目前空間 OAunt2 目前空間 OAunt2 目前空間 OAunt2 Import OAunt2
(III) EAF®R REDARG-INTEL, NEAFREREIGENER, NEAFREREIGENER.
Refer References. Alles and a contraction and a contraction of the second and a contraction of
00C 00H0 00H0 0 = -885 0 Am 20 25 26 882 0 Am 20 25 26 882 0 Am 20 25 26 882 0 Am 20 25 26 7 Am 20 26 0 Am 20 26 26 27 0 Tam 20 26 26 26 27 0 Tam 20 26 26 26 26 26 26 26 26 26 26 26 26 26
FADUS RADUE ROBERTADE ENGENERS (NAS, NotAnnes Sover), ((SEPTRANSFORM)HEESTUN75AnansForm, StatussoveRd_118509-86ULBEX/S, REIN-R
U.S. AAMOOD U.A



4. 在配置参数信息页面,根据要求填写相关信息后,单击**下一步:完成**。

✓ 选择应用协议模板	> 2 配置参数信息 > 3 完成	
应用题标 •	还未选择面片 选择图片	
±−−− <i>47 ¥</i> 0.	请上传 Jpg或png 格式文件,大小 1MB 以内	
<u> 立 中 古 称 ・ </u> 安 全 等 级 ・	SAML 请选择安全等级 ▼	
IdP Entity ID *	tencent_idp	
	用于标识SAML IdP的信息,默认为"tencent_idp",管理员可修改。	
SP Entity ID •	请输入SP Entity ID 用于标识SAML SP的信息,由管理员指定。	
SP ACS URL (SSO Location) •	清给入SP ACS URL (SSO Location)	
SP 登出地址 •	请输入SP 登出地址	
Nameld Format *	请选择Nameld Format ▼	
Assertion Attribute	标签键	标签值
	+ 添加	
自定义属性	石华健	标签值
	+ 添加	
企业微信SSO •		
	开启并配置完成后,在企业微信工作台内创建应用并完成配置即可单点登录到各	a应用系统无需再次登录
上一步:选择应用	下一步:完成 取消	

5. 在完成页面,单击**完成**,即可成功添加新应用,新应用默认是启用状态。

方式2: 应用市场新建

- 1. 登录 数字身份管控平台(员工版)控制台,在左侧导航栏,单击**应用管理**。
- 2. 在应用管理页面,单击**应用市场新建**。

应用协议新建	应用市场新建	批量删除
应用名称		应用ID
共 1 条		



腾讯云

1 选择应用 > 2 编辑应用	信息 〉 (3) 完成				
全部应用				请输入应用名称进行搜索	Q
隊 讯企业邮箱	🔗 腾讯云	€-3₩₩₩₩ 阿里云 (用户)	€Э₩₩₩ 阿里云 (角色)	¥为云	AWS
标签 办公协同	标签 云平台	标签 云平台	标签 云平台	标签 云平台	标签 云平台
OpenVPN	GitLab	◎ 数清期待 計 路讯文档	◎ 一般 「「「」」 「「」」 「」 「」 「」 「」 「」 「」 「」 「」 「」 「	(敬请期待) Nextcloud	◎ 金螺云
标签 办公协同	标签 研发工具	标签 办公协同	标签 办公协同	标签 办公协同	标签 云平台
wiji wPS	較清明待 №ccs owe Zohu One	& 读期待 ŸJIRA Jira	敬請期待 Confluence		数清期待 <mark>∉slock</mark> Slack
标签 办公协同	标签 办公协同	标签 研发工具	标签 研发工具	标签 行业应用	标签 研发工具
● Statis Statis	敬清期待 GitHub	歌请期待 Zoom	較清期待 € TAPD	(数清期待) のKee 365	数清期待 注微OA
下一步:编辑应用信息 取消					

4. 在编辑应用信息页面,根据要求填写相关信息后,单击**下一步:完成**。

🗸 选择应用	> 2 编辑应用信息 > ③ 完成
应用图标★	
应用名称 *	腾讯云
安全等级 *	请选择安全等级 ▼
描述	
	仅限128个字符以内
账号ID *	请输入账号ID
身份提供商名称 *	请输入身份提供商名称
角色 *	● 账号 ① ○ 用户组 ○ 自定义
<u>企业</u> 微信SSO *	开启并配置完成后,在企业微信工作台内创建应用并完成配置即可单点登录到各应用系统无需再次登录
上一步:选择质	应用 下一步:完成 取消

5. 在完成页面,单击**完成**,即可成功添加新应用,新应用默认是启用状态。

相关文档

新建完应用后,可以对应用授权进行管理,详情请参见 应用授权 。



配置应用

最近更新时间: 2022-12-06 16:56:02

操作场景

新建应用后,可以通过应用配置对应用属性进行修改。

操作步骤

1. 登录 数字身份管控平台(员工版)控制台,在左侧导航栏,单击应用管理。

2. 在应用管理页面,选择所需应用,单击操作列的**应用配置**。

3. 在应用信息页面,单击右上角的编辑,修改相关参数,单击保存即可修改应用信息。

<	
应用信息 账号	管理 资源管理
应用图标 *	https://e a
	远海图片 删除
	请上传 jpg或png 格式文件,大小 1MB 以内
应用名称 *	
安全等级 *	
Server Names *	http://
	CAS客户端发起认证的URL地址,http或https开头,支持通配符路径恪式,比如:http://www.abc.com/user/**、http://www.abc.com/user/**等。
Target URL *	http://
	本系统支起早示登录时的地址,需要与明具体地址,比如:http://www.abc.com/index
CAS Login URL	https://ter To
CAS Validation URL	https://te
应用登录地址	https://t
企业微信SSO *	开启并配置完成后,在企业微信工作台内创建应用并完成配置即可单点登录到各应用系统无需再次登录
保存取消	Ϋ́



账号管理

最近更新时间: 2022-12-06 16:56:20

新建应用后,可以通过账号管理对应用下的账号进行管理。

新建账号

- 1. 登录 数字身份管控平台 (员工版)控制台,在左侧导航栏,单击**应用管理**。
- 2. 在应用管理页面,单击选择所需应用,单击**应用配置 > 账号管理**。
- 3. 在账号管理页面,单击**新建账号**。



4. 在新建账号弹窗中,配置相关参数,单击确定保存。

	>
请输入账号名称	
请输入账号密码	Ø
密码只能包含英文字母、数字、!"#\$%&'()*+,/;;<=>?@[]^_`{ }~	
请填写简短描述,不超过128字符	
确定取消	
	请输入账号名称 请输入账号密码 密码只能包合英文字母、数字、!"#\$%&'()*+,-,/;;<=>?@[]^_`{}~ 请填写简短描述,不超过128字符 确定

参数说明:

- 账号名称:自定义名称。
- 账号密码:密码只能包含英文字母、数字、!"#\$%&'()*+,-./:;<=>?@[]^_`{]}~。
- 描述:自定义描述,不超过128个字符。

编辑账号

- 1. 在 应用管理页面,单击选择所需应用,单击**应用配置 > 账号管理**。
- 2. 在账号管理页面,选择所需账号,单击**编辑**。

账号管理	账号组管理

新記書を与 一般時 を	谱输入应用际号、用户名称进行搜索	Q
账号名称 用户名称	创建时间 操作	
	2022-01-04 11:46:54 原報 使射管理 删	lê:
	2022-01-04 11:46:34 編編 読射管理 删	l¢:



3. 在编辑账号弹窗中,修改相关参数,单击**确定**保存。

编辑账号		×
账号名称 *		
账号密码	请输入账号密码	,
描述	请填写简短描述,不超过128字符	
	確定取消	

管理映射

通过映射管理,可以将应用账号与用户名称绑定。

 说明 一个账号名称可以映射多个用户名称。 	
1. 在 应用管理页面,单击选择所需应用,单击 应用配置 > 账号管理 。	

2. 在账号管理页面,选择所需账号,单击**映射管理**。

账号管理 账号组管理				
新建账号 删除			请输入应用账号、用户名称进行搜索	Q
账号名称	用户	各称	创建时间	操作
			2022-01-04 11:46:54	编辑 映射管理 删除
			2022-01-04 11:46:34	编辑 映射管理 删除

3. 在映射管理弹窗中,选择映射的用户名称,单击确定即可完成绑定。

映射管理		×
账号名称	test	
用户名称	请选择	Ŧ
	确定取消	

删除账号

- 1. 在 应用管理页面 ,单击选择所需应用,单击**应用配置 > 账号管理**。
- 2. 在账号管理页面,支持单个删除账号,或批量删除账号。
 - 单个:选择所需账号,单击操作列的**删除**,弹出确认删除弹窗。

账号管理	账号组管理			
新建账号	1894		请输入应用账号、用户名称进行搜索	Q
□ 账号名	4	用户名称	创建时间	操作
			2022-01-04 11:46:54	编辑 映射管理 删除
			2022-01-04 11:46:34	编辑 缺射管理 删除

○ 批量:选中一个或多个需要删除的账号,单击删除,弹出确认删除弹窗。





.

账号管理 账号组管理			
新建账号 影除		请编入应用账号、用户名称进行编集	Q
✔ 账号名称	用户名称	创建时间 措	柔作
		2022-01-04 11:46:54	編輯 映射管理 删除
		2022-01-04 11:46:34	編 映射管理 删除

3. 在确认删除弹窗中,单击**删除**,即可删除所选账号。

注意		
删除后,	相应数据将无法恢复,	请谨慎操作。



账号组管理

最近更新时间: 2022-12-06 17:00:33

新建应用后,可以通过账号组管理对应用下的账号组进行管理。

新建账号组

- 1. 登录 数字身份管控平台 (员工版)控制台,在左侧导航栏,单击 应用管理。
- 2. 在应用管理页面,单击选择所需应用,单击**应用配置 > 账号管理 > 账号组管理**。
- 3. 在账号组管理页面,单击**新建账号**。



4. 在新建账号组弹窗中,配置相关参数,单击确定保存。

新建账号组	×
账号组名称 *	请输入账号组名称
描述	请填写简短描述,不超过128字符
	職定取消

参数说明:

- 账号组名称:自定义名称,名称不能重复。
- 描述:自定义描述,不超过128个字符。

编辑账号组

新增账号组后,可修改账号组名称及备注信息。

- 1. 在 应用管理页面,单击选择所需应用,单击**应用配置 > 账号管理 > 账号组管理**。
- 2. 在账号组管理页面,选择所需账号组,单击编辑。

长号管理 账号组管	理		
新建账号组 册	除		
创建时间 :2022-01-04	14:20:29		
編揖 删除	添加账号		



3. 在编辑账号组弹窗中,修改相关参数,单击确定保存。

编辑账号组	×
账号组名称 *	ž
描述	
	職定取消

删除账号组

新增账号组后,如不再需要已新增的账号组,可删除单个账号组或批量删除账号组。

- 1. 在 应用管理页面,单击选择所需应用,单击**应用配置 > 账号管理 > 账号组管理**。
- 2. 在账号组管理页面,支持删除单个账号组,或批量删除账号组。
 - 单个:选择所需账号组,单击操作列的**删除**,弹出确认删除弹窗。

新建账号组 删除		
创建时间 -2022-01-04 14-24-47	AI建时间 ·2022_01_04 14·20·20	
編辑 删除 添加账号	编辑 删除 添加账号	

○ 批量:选中一个或多个需要删除的账号组,单击删除,弹出确认删除弹窗。

号管理 账号组管理 新建账号组 删除		
-		
创建时间 :2022-01-04 14:24:47 编辑	创建时间 :2022-01-04 14:20:29 编辑 删除 添加账号	
5.2 条		

3. 在确认删除弹窗中,单击删除,即可删除所选账号组。

账号组添加账号



新增账号组后,可在账号组中新增账号。

方式1(推荐)

- 1. 在 应用管理页面,单击选择所需应用,单击**应用配置 > 账号管理 > 账号组管理**。
- 2. 在账号组管理页面,选择所需账号组,单击**添加账号**。

新建账号组 删除		
创建时间 :2022-01-04 14:24:47 编辑	创建时间 :2022-01-04 14:20:29 编辑 删除 添加账号	

3. 在添加账号弹窗中,选择需要添加的账号,单击确定,选中的账号将被加入到该账号组中。

添加账号						×
选择用户			已选择 (2)			
请输入账号名称、用户名称搜索	C	2	账号名称		用户名称	
✔ 账号名称	用户名称				0	
						9
						0
			THOMAS			
		Ē	取消			

方式2

1. 在 应用管理页面,单击选择所需应用,单击**应用配置 > 账号管理 > 账号组管理**。



2. 在账号组管理页面,选择所需账号组,鼠标单击"空白处"。

号管理 账号组管理 新建账号组 翻除		
创建时间 :2022-01-04 14:24:47 编辑 删除 添加账号	创建时间 :2022-01-04 14:20:29 编辑	
± 2 条		

3. 在账号组的详情页面,可查看已添加的账号,单击**添加账号**。

		×
创建时间: 2022-01-04 14:24:47	描述:	
添加账号 移除账号		请输入账号名称/用户名称搜索 Q
账号名称	用户名称	操作
		移除

4. 在添加账号弹窗中,选择需要添加的账号,单击**确定**,选中的账号将被加入到该账号组中。

添加账号					×
选择用户			已选择 (2)		
请输入账号名称、用户名称搜索		Q,	账号名称	用户名称	
✔ 账号名称	用户名称				Ø
					0
		+	*		
		确定	取消		

账号组移除账号

在账号组中新增账号后,支持将其移除。

移除后,相应数据将无法恢复,请谨慎操作。

^{1.} 在 应用管理页面,单击选择所需应用,单击**应用配置 > 账号管理 > 账号组管理**。

2. 在账号组管理页面,选择所需账号组,鼠标单击"空白处"。

🔗 腾讯云

创建时间 :2022-01-04 14:24:47 编辑 制除 添加账号	创建时间:2022-01-04 14:20:29 编辑 删除 添加账号

- 3. 在账号组的详情页面,支持移除单个账号,或批量移除账号。
- 单个:选择所需账号,单击操作列的移除,弹出确认移除弹窗。

			×
创建时间: 2022-01-04 14:24:47	描述:		
添加账号 移除账号		请输入账号名称/用户名称搜索	Q
账号名称	用户名称	操作	
		移除]
Ĩ		移除	

• 批量:选中一个或多个需要移除的账号,单击**移除账号**,弹出确认移除弹窗。

		×
描述:		
	请输入账号名称/用户名称搜索	Q,
用户名称	操作	
	移除	
	移除	
	描述: 用户名称	描述: 请输入账号名称/用户名称搜索 用户名称 操作 修除

4. 在确认移除弹窗中,单击**移除**,可将选中账号从账号组里移除。



资源管理

最近更新时间: 2022-12-06 17:01:06

新建应用后,资源管理可以管理应用下属资源,包括功能、菜单、按钮、API、数据等类型。完成资源的注册后即可进行资源级授权。

新建资源

- 1. 登录 数字身份管控平台(员工版)控制台,在左侧导航栏,单击应用管理。
- 2. 在应用管理页面,单击选择所需应用,单击**应用配置 > 账号管理 > 资源管理**。
- 3. 在资源管理页面,单击**新建资源**。

应用個	謥	账号管理	资源管理						
0	资源管理	用来管理应用下属	资源,包括功能、	菜单、	按钮、	API,	数据等类型。	完成资源的注册后即可进行资源级授权。	
新建	资源	删除							

4. 在新建资源弹窗中,配置相关参数,单击确定保存。

新建资源	×	
资源名称★	请输入资源名称	
资源标识★	请输入资源标识	
描述	请填写简短描述,不超过128字符	
	确定取消	

参数说明:

- 资源名称:自定义名称。
- 资源标识:自定义标识。
- 描述: 自定义描述,不超过128个字符。

编辑资源

资源新建成功后,可编辑资源详细信息。

1. 在 应用管理页面,单击选择所需应用,单击**应用配置 > 账号管理 > 资源管理**。

2. 在资源管理页面,选择所需资源,单击**编辑**。

资源名称	资源标识	描述	操作
			编辑删除
			编辑删除

3. 在编辑资源弹窗中,修改相关参数,单击确定保存。

腾讯云

编辑资源	×
资源名称 *	-
资源标识*	•
描述	请埴写简短描述,不超过128字符
	确定取消

删除资源

资源新建成功后,如不再需要已新增的资源,可删除单个资源或批量删除资源。

⊿	<mark>注意</mark> 删除后,所有数据将清除且无法恢复,所有授权关系将解除,请谨慎操作。
1. 在 2. 在	<mark>应用管理页面</mark> ,单击选择所需应用,单击 应用配置 > 账号管理 > 资源管理 。 资源管理页面,选择所需资源,支持删除单个资源,或批量删除资源。 〕 单个:选择所需资源,单击操作列的 删除 ,弹出确认删除弹窗。
	账号管理 账号组管理

创建时间:2022-01-04 14:24:47	创建时间 :2022-01-04 14:20:29	
编辑 删除 添加账号	编辑 删除 添加账号	

○ 批量:选中一个或多个需要删除的资源,单击删除,弹出确认删除弹窗。

新建资源			请输入资源名称/资源标识进
✓ 资源名称	资源标识	描述	操作
			编辑 删除

3. 在确认删除弹窗中,单击删除,即可删除所选资源。

相关文档

新建完资源后,可以对资源授权进行管理,详情请参见 资源级授权。



授权管理

应用授权

最近更新时间:2022-12-06 17:01:32

本文将为您介绍如何在数字身份管控平台(员工版)控制台,根据组织架构、用户组及用户统一对应用进行授权。

前提条件

- •已新建应用。
- 已新建组织机构。
- 已新建用户组。
- •已新建用户。

授权组织架构

- 1. 登录 数字身份管控平台(员工版)控制台,在左侧导航栏,选择**授权管理 > 应用授权**。
- 2. 在组织架构授权页面,单击**新增授权**。

应用授权			
组织架构授权	用户组授权	用户授权	
新増授权			
应用名称			

3. 在选择应用页面,勾选要授权的应用,单击**下一步**。

3 选择应用 > ② 选择组织机构 > ③ 完成						
选择应用(1)			已造择应用 (1)		
请输入应	用各称或应用ID		Q	应用各称	应用ID	
	应用名称	应用ID		云API网关		0
	云API网关					
				•		
下一步	取り用					

4. 在选择组织机构页面,选择需要授权应用访问权限的组织机构,单击**保存**,即可完成组织架构授权。

✓ 选择应用 > 2 选择组织机构 > ③ 完成			
选择组织机构	已选择暗积机构 (1)		
请输入组织机构名称或代码 Q	机构名称	机构代码	
 D 県节点 	测试公司一	123	0
 調査公司一 調査公司二 			
1-0 8 0 EM			

授权用户组

1. 登录 数字身份管控平台(员工版),在左侧导航栏,选择**授权管理 > 应用授权**。



2. 在应用授权页面,选择**用户组授权 > 新增授权**。

组织架构授权	用户组授权	用户授权
新增授权		
应用名称		

3. 在选择应用页面,勾选要授权的应用,单击**下一步**。

1 选择	3 湖洋協用 > ② 選擇用户組 > ③ 完成						
选择应用(1)				已选择应用 (1)			
清蛎入应用	用各称或应用ID	Q		应用各称	应用ID		
<u>~</u>	应用各称	应用ID		ZAPI网关		0	
	云API网关						
			\leftrightarrow				
T _#	Rect						

4. 在选择用户组页面,选择需要授权应用访问权限的用户组,单击**保存**,即可完成用户组授权。

✓ 送降血用 > 2 送降用户組 > 3 完成						
选择用户组	(2)			已选择用户组 (1)		
请输入用	户语名称	Q		用户组名称	留注	
	用户组名称	畲注		测试用户组	-	0
	测试用户组					-
	测试用户组2					
			\leftrightarrow			
#	6247 2008					

授权用户

- 1. 登录 数字身份管控平台(员工版),在左侧导航栏,选择**授权管理 > 应用授权**。
- 2. 在应用授权页面,选择**用户组授权 > 新增授权**。

组织架构授权	用户组授权	用户授权	
新増授权			
应用名称			应用ID
			-
共1条			



3. 在选择应用页面,勾选要授权的应用,单击**下一步**。

1 迷	→ 選择 通用 > (2) 通貨 用户 > (3) 完成						
选择应用(1)			己选择应用 (1)			
请输入应	用名称或应用ID	Q		应用各称	应用ID		
	应用名称	应用ID		云API网关		0	
	云API网关						
			\leftrightarrow				
下一步	取消						

4. 在选择用户页面,选择需要授权应用访问权限的用户,单击保存,即可完成用户授权。

迷 😒) 送降面用 → 2 送降用户 → 3 完成							
选择用户(3	1			己选择用户 (2)				
请输入用	中名称或用户昵称	Q		用户省称	用户昵称			
	用户省称	用户昵称				0		
						·		
						٥		
上一步	保存 取消							





资源级授权

最近更新时间: 2024-11-14 14:50:32

本文将为您介绍如何在数字身份管控平台(员工版)控制台,根据组织架构、用户组及用户统一对资源进行授权。

前提条件

- •已新建应用。
- 已新建资源。
- 已新建组织机构。
- 已新建用户组。
- 已新建用户。

授权组织架构

- 1. 登录 数字身份管控平台(员工版)控制台,在左侧导航栏,选择**授权管理>资源级授权>组织机构授权**。
- 2. 在组织机构授权页面,选择需要进行授权的应用,单击**新增授权**。

资源级授权	c))	• (j	
组织机构授权	用户组授权	用户授权			
新增授权	取消授权				
名称/ID				授权组织机构	

3. 在选择资源页面,勾选要授权的资源,单击**下一步**。

1 选择资源 > 2	1 选择资源 > 2 选择组织机构 > 3 完成						
请选择资源			已选择 (1)				
请输入资源名称/标识搜索		Q,	资源名称	资源标识			
- 资源名称	资源标识				0		
		↔					
下一步取消							

4. 在选择组织机构页面,选择需要授权资源访问权限的组织机构,单击**下一步**。

送择资源 > 2 选择	✓ 选择资源 〉 2 选择组织机构 〉 ③ 完成							
请选择组织机构			已选择 (1)					
请输入组织机构名称或代码		Q,	组织机构名称	组织机构代码				
✓ 组织机构名称	组织机构代码		根节占	root	0			
✓ 根节点	root				9			
上一步下一步取消								



5. 单击**完成**,即可完成组织架构授权。

授权用户组

- 1. 登录 数字身份管控平台(员工版)控制台,在左侧导航栏,选择**授权管理 > 资源级授权 > 用户组授权**。
- 2. 在用户组授权页面,选择需要进行授权的应用,单击**新增授权**。

资源级授权			• (i)
组织机构授权	用户组授权	用户授权	
新增授权	取消授权		

3. 在选择资源页面,勾选要授权的资源,单击**下一步**。

〕 选择资源 > ② 选择组织机构 > ③ 完成						
请选择资源			в	选择 (1)		
请输入资源名称/标识搜索		Q		资源名称	资源标识	
<mark>一</mark> 资源名称	资源标识					c
		•	↔			
下一步取消						

4. 在选择用户组页面,选择需要授权资源访问权限的用户组,单击下一步。

✓ 选择资源 〉 2 选择用户组	> 选择资源 > 2 选择用户组 > ③ 完成						
请选择用户组			已选择 (1)				
请输入用户组名称或代码		Q	用户组名称	用卢组代码			
✓ 用户组名称	用户组代码				0		
		\leftrightarrow					
上ーサ 下一步 取消							

5. 单击**完成**,即可完成用户组授权。

授权用户

- 1. 登录 数字身份管控平台(员工版)控制台,在左侧导航栏,选择**授权管理 > 资源级授权 > 用户授权**。
- 2. 在用户授权页面,选择需要进行授权的应用,单击**新增授权**。

资源级授权	СА		Ŧ	(i)
组织机构授权	用户组授权	用户授权		
新增授权	取消授权			
名称/ID				授



3. 在选择应用页面,勾选要授权的应用,单击**下一步**。

遇 🚺	海路への用いた「「「「」」」、「「」」、「」、「」、「」、「」、「」、「」、「」、「」、「」、						
选择应用(1)			已选择应用 (1)			
请输入应	用名称或应用iD	Q		应用各称	应用ID		
×	应用各称	应用ID		ZAPIMĚ		0	
	云API网关					•	
			↔				
下#	20H						

4. 在选择用户页面,选择需要授权资源访问权限的用户,击**下一步**。

✓ 选择资源 〉 2 选择	● > ③ 完成						
请选择用户			i	已选择 (1)			
请输入用户名称或代码			Q,	用户名称	用户昵称	用户代码	
✓ 用户名称	用戶昵称	用户代码			root		0
	root						
			\leftrightarrow				
上一步 下一步 取消							•

5. 单击**完成**,即可完成用户授权。



认证管理

最近更新时间:2022-12-06 16:21:00

本文将为您介绍如何在数字身份管控平台(员工版)控制台,新建认证源、启用/禁用认证源。 数字身份管控平台(员工版)支持配置多种外部认证源登录。管理员可以根据需要,添加并启用不同的认证方式。启用认证源并完成配置后,平台会在公司用户登录时使用 具体的认证源去认证用户身份,并通过外部 ID 与平台的用户进行关联。

前提条件

管理员必须先添加并启用一个认证源,才能开启外部认证。支持添加并启用多个外部认证源。目前支持配置的认证源包括:

- LDAP
- 企业微信扫码登录
- 短信验证码登录
- AD

新建认证源

- 1. 登录 数字身份管控平台 (员工版)控制台,在左侧导航栏,单击认证管理。
- 2. 在认证管理页面,单击**新建认证源**。

认证管理				
新建认证规	#8			
	认证源名称/认证源ID	描述	认证源状态	操作
	284 ⁴⁴⁴⁴ 284	使用短信验证码整录系统		编辑 测试赔偿 删除
共1条				10 - 条/页

3. 在选择认证源模板页面,选择要添加的认证源,单击**下一步**。

- 新建认证源
 3 选择以证源模板 > ② 编辑认证源信息 > ③ 完成
2. 地位输送研会录 他用地位给证明金录系统
企业委任用股票 建筑信用股票 取用企业研究性事系统
LDAP BIRLDAP2ETULE
BS AD ARABINE
T9 201

4. 在编辑认证源信息页面,完成相关配置,单击确定。

说明 要添加的认证源不同,管理员需要完成的配置也不相同,请以具体认证源的配置要求为准。



🕑 选择认证源模板	t > 2 编辑认证源信息 > ③ 完成	
▲ 认证源名称	AD	
* AD URL	请给,\AD URL	
	AD服务器连接地址。如: ldap://127.0.0.1:389/	
* AD Base	请能入AD Base	
	AD中的节点,会到该节点下以证账户,如: dc=idsmanager,dc=com	
* AD账号	错能JAD服务	
	需要有以上调写的Base的管理权用	
* AD账号密码	請協入走利	
	AD服号对应密码	
描述	使用AD域进行认证	
* 过滤条件	调输入过速条件	
	AD中匹配用户名的得选条件,如:(sAMAccountName=\$username\$)	
上一步 取	消化	

启用/禁用认证源

已添加的认证源,管理可以开启和禁用。支持同时启用多个外部认证源,用户在登录时,可以从中选择一种方式进行登录。 1. 在 认证管理 页面,定位到要操作的认证源,单击认证源状态按钮开关,蓝色按钮表示开启。

新建认证源	8.8			
	认证源名称/认证源ID	描述	认证源状态	绿作
	28- 28-	使用现估验证码整录系统		an Nates Bits

2. 在弹出的对话框,单击确定。


审计管理

最近更新时间: 2022-12-06 16:20:45

本文将为您介绍如何在数字身份管控平台(员工版)控制台,查看用户操作日志、系统操作日志。 审计日志详细地记录了用户在平台上进行的关键操作。管理员可以随时对某条记录进行查看,对某次操作进行复盘,对高危行为进行统计。

查看用户操作日志

主要查看用户的登录、应用单点登录等日志信息。

- 1. 登录 数字身份管控平台(员工版)控制台,在左侧导航栏,单击**日志审计**。
- 2. 在用户操作日志页面,可以选择今天、昨天、近7天、近30天的日期进行日志查看,也可以通过搜索框查询操作人或者操作类型进行日志搜索。

审计管理				
用户操作日志 系统操作日志				
<u>今天</u> 昨天 近7天 近30天	2021-04-11 00:00:00 ~ 2021-04-11 23:59:59			領職入操作人種作类型理素 Q
操作时间	操作人	操作类型	操作评估	IP地址

查看系统操作日志

主要查看系统相关的操作日志信息,如用户自动同步、定时任务等日志信息。

- 1. 在 日志审计 页面,单击**系统作日志**。
- 2. 在系统操作日志页面,可以选择今天、昨天、近7天、近30天的日期进行日志查看,也可以通过搜索框查询操作人或者操作类型。



同步中心 上游同步 新建数据源

最近更新时间: 2024-11-14 14:50:32

上游同步是指从外部数据源同步组织机构、用户数据到平台用户目录。支持主流的 LDAP/AD 导入、按照标准协议 SCIM 协议导入。本文将介绍如何新建不同类型的上游 同步数据源。

新建 SCIM 数据源

- 1. 登录 数字身份管控平台(员工版)控制台,在左侧导航中,单击**同步中心 > 上游同步**。
- 2. 在上游同步页面,单击**新建上游同步**,选择 SCIM 协议。

数字身份管控平台 (员 工版)	上游同步
器 概 览	
泉 用户管理 · ·	 上游同步是指从外部数据源同步组织机构、用户数据到半台用户目录
<u> 今</u> 认证管理	新建上游同步
品 应用管理	同步名称ID
授权管理 ·	
目 审计管理	
口。同步中心 ^	
上游同步	

3. 在配置基本信息页面,输入数据源名称和描述,单击下一步。

1 配置基	本信息 > 2 配置参数信息 > 3 完成
数据源名称 *	请输入数据源名称
描述	请填写简短描述,限128字内
下一步:	配置参数信息 取消



4. 在配置参数信息页面,配置相关参数后,单击下一步:完成。

✔ 配置基本信息 〉 2 配置参数信息 〉 3 完成		
获取方式 访 *	○ 数据源推送 ○ 平台拉取 获取方式在创建后不可修改	
Client ID *	请输入Client ID	
Client Secret *	请输入Client Secret	
Token *	请输入Token	
User URL *	请输入User URL	
Org URL *	请输入Org URL	
上一步: 配置基本信息 下一步: 完成 取消		

参数说明:

- 获取方式:根据实际需求选择数据源推送或平台拉取,获取方式在创建后不可修改。
- Client ID:客户端 id,在 应用管理页面,选定指定应用,单击操作列的应用配置,查看 Client ld 值。

应用管理					
① 支持持创建标准协议应用,包括CAS、SCIN	1、JWT、OAuth2、泰单代旗、云API网关应用;支持在应用市场选择预集成应用	快速接入。		不再揭醒 ×	
应用协议新建 应用市场新建 提出	2.059		请输入应用名称/应用ID搜索	Q	
应用名称	应用ID	应用状态	操作		
			应用配置。翻除		
			应用配置 影除		
			应用配置。部除		

- Client Secret:客户端 Secret,在应用管理页面,选定指定应用,单击操作列的应用配置,查看 Client Secret 值。含有特殊字符,需要做 URLEncode。
- Token:根据 Client ID 和 Client Secret 返回的 access_token。详情请参见 SCIM 数据源对接─调用方式。
- User URL: 用户 id,详情请参见 SCIM 数据源对接-用户 API。
- Org URL: 组织机构 id,详情请参见 SCIM 数据源对接-组织机构 API。
- 5. 在完成页面,单击**完成**返回数据源列表。



新建 AD 数据源

1. 在 上游同步页面,单击**新建上游同步**,选择 AD。



2. 在配置基本信息页面,输入数据源名称和描述,单击**下一步**。

1 配置基	本信息 > 2 配置参数信息 > 3 完成
数据源名称 *	清输入数据源名称
描述	请填写简短描述,限128字内
下一步:	配置参数信息

- 3. 在配置服务器连接页面,根据同步的 AD 的安装位置,选择是否启用代理开关。
 - 如果同步的 AD 安装在外网,则关闭使用代理开关,根据要求填写相关信息后,单击下一步。

🗸 基本信息	息 > 2 配置服务器连接 > 3 字段匹配规则 > 4 完成
agent下载	AD Agent:将内网AD与本系统进行连接 大小: 25MB 点击下载
使用代理 *	如果同步的LDAP安装在内网环境,需要先下载LDAP Agent并根据配置指引进行代理配置,再打开"使用代理"开关
服务器地址 *	请输入服务器地址
端□号★	请输入端口号
Base DN *	请输入Base DN,如:dc=XXX,dc=XXX
	为确保数据同步成功,Based DN保存后不可更改,如果Base DN发生变化会使双方组织机构无法对应而导致数据同步失败
SSL连接方式 *	一 开启后,服务器采用SSL连接方式
管理员DN *	请输入管理员DN
	若进行同步操作后修改管理员DN,需重新进行数据同步
管理员密码 *	请输入管理员DN所对应的密码
同步默认密码★	请输入同步默认密码
	数据同步后,用户登录EIAM的默认密码
上一步	下一步 取消 测试连接

参数名称	描述	示例值
服务器地址	连接的外网 AD 服务器地址	116.62.207.52
端口号	连接服务器地址的端口号	389
Base DN	在 AD 服务器上 AD 域控的 DN	DC=moonxy,DC=com
管理员 DN	管理员的全名,也就是 AD 服务器上管理员账号的 distinguishedName 属性值	CN=Administrator,CN=Users,DC=ebg,DC=gtac,D C=com
管理员密码	所填 AD 服务器管理员账号的密码	Aa123456



	同步默认密码	数据同步后,用户登录 EIAM 的默认密码	Aa123456
0	如果同步的 AD 5	安装在内网环境,需要先下载 AD Agent 并根据配置指引进行代理配置,再打	开使用代理开关,根据要求填写相关信息后,单击 下一步 。
	✔ 基本信	息 〉 2 配置服务器连接 〉 ③ 字段匹配规则 〉	4 完成
	agent下载	AD Agent:将内网AD与本系统进行连接 大小:25MB 点击下载	
	使用代理★	如果同步的LDAP安装在内网环境,需要先下载LDAP Agent并根据配置指引进行代理图	2置,再打开 "使用代理" 开关
	agent地址 *	请填写agent地址	
	同步默认密码 *	请输入同步默认密码	
		数据同步后,用户登录EIAM的默认密码	
	client_id	‡k Г	
	client_secrent	1 6	
	上一步	下一步 取消 测试连接	

参数名称	描述	示例值
agent 地址	连接的内网 AD 服务器地址	http://116.25.75.22: 8080
同步默认密码	数据同步后,用户登录 EIAM 的默认密码	Aa123456
client_id	用于配置 agent 的参数	f5k58wfdc7jcc87jz74k
client_secret	用于配置 agent 的参数	fvjazuorj5f1



4. 在字段匹配规则页面,根据要求填写相关信息后,单击**下一步**。

🗸 🛃	な信息 〉 💙 配置服务器连接 〉 3 字段匹配规则 〉 4 完成
用户名 ★	请输入用户名对应的字段名
	若为Windows AD,则字段名为: sAMAccountName
用户昵称★	请输入用户昵称
	通常为displayName
手机号码★	请输入手机号码对应的字段名
	通常为telephoneNumber
邮箱地址 *	请输入邮箱地址对应的字段名
	通常为mail
域名名称	请输入域名名称
	若域名为elam.tencent.com,用户名为joy,则Windows AD登录名为Joy@elam.tencent.com
上一步	下一步 取消

参数说明:

参数名称	描述	示例值
用户名	用户名对应的字段名	sAMAccountName
用户昵称	通常为 displayName	displayName
手机号码	通常为 telephoneNumber	telephoneNumber
邮箱地址	通常为 mail	mail
域名名称	AD 域名名称	eiam.tencent.com

5. 在完成页面,单击**完成**返回数据源列表。



新建 LDAP 数据源

1. 在 上游同步页面,单击**新建上游同步**,选择 LDAP。



2. 在配置基本信息页面,输入数据源名称和描述,单击**下一步**。

1 配置基	本信息 > 2 配置參数信息 > 3 完成
数据源名称 *	请输入数据源名称
描述	请填写简短描述,限128字内
下一步:	配置参数信息

3. 在配置服务器连接页面,根据同步的 LDAP 的安装位置,选择是否启用代理开关。

○ 如果同步的 LDAP 安装在外网,关闭使用代理开关,根据要求填写相关信息后,单击**下一步**。

✔ 基本信	息 〉 2 配置服务器连接 〉 3 字段匹配规则 〉 4 完成
agent下载	LDAP Agent:将内网LDAP与本系统进行连接 大小: 25MB 点击下载
使用代理★	如果同步的LDAP安装在内网环境,需要先下载LDAP Agent并根据配置指引进行代理配置,再打开 "使用代理" 开关
服务器地址★	请输入服务器地址
端口号★	请输入端口号
Base DN *	请输入Base DN, 如: dc=XXX,dc=XXX
	为确保数据同步成功,Based DN保存后不可更改,如果Base DN发生变化会使双方组织机构无法对应而导致数据同步失败
SSL连接方式 *	● 开启后,服务器采用SSL连接方式
管理员DN *	请输入管理员DN
	若进行同步操作后修改管理员DN,需重新进行数据同步
管理员密码 *	请输入管理员DN所对应的密码
同步默认密码 *	请输入同步默认密码 💋
	数据同步后,用户登录EIAM的默认密码

参数名称	描述	示例值
服务器地址	连接的外网 LDAP 服务器地址	116.62.207.52
端口号	连接服务器地址的端口号	80
Base DN	在 LDAP 服务器上 LDAP 域控的 DN	DC=moonxy,DC=com
管理员DN	管理员的全名,即 LDAP 服务器上管理员账号的 distinguishedName 属性值	CN=Administrator,CN=Users,DC=ebg,DC=gtac,DC =com
管理员密码	所填 LDAP 服务器管理员账号的密码	Aa123456
同步默认密码	数据同步后,用户登录 EIAM 的默认密码	Aa123456



○ 如果同步的 LDAP 安装在内网环境,需要先下载 LDAP Agent 并根据配置指引进行代理配置,再打开使用代理开关,根据要求填写相关信息后,单击下一步。

🗸 基本信	記 〉 2 配置服务器连接 〉 3 字段匹配规则 〉 4 完成
agent下载	LDAP Agent: 将内网LDAP与本系统进行连接 大小: 25MB 点击下载
使用代理 *	
	如果同步的LDAP安装在内网场境,需要先下载LDAP Agent开根据配置指引进行代理配置,再打开"使用代理"开关
agent地址 *	请填写agent地址
同步默认密码	• 请输入同步默认密码
	数据同步后,用户登录EIAM的默认密码
client_id	· rī
client_secrent	
上一步	下一步 取消 测试连接

参数说明:

参数名称	描述	示例值
agent 地址	连接的内网 LDAP 服务器地址	116.62.207.52
同步默认密码	数据同步后,用户登录 EIAM 的默认密码	Aa123456
client_id	用于配置 agent 的参数	f5k58wfdc7jcc87jz74k
client_secret	用于配置 agent 的参数	fvjazuorj5f1

4. 在字段匹配规则页面,根据要求填写相关信息后,单击**下一步**。

🗸 基本	「信息 〉 💙 配置服务器连接 〉 3 字段匹配规则	> 4 完成
用户名 *	请输入用户名对应的字段名	
	LDAP目录,字段名为:uld	
用户昵称 *	请输入用户昵称	
	通常为displayName	
手机号码 *	请输入手机号码对应的字段名	
	通常为telephoneNumber	
邮箱地址 *	请输入邮箱地址对应的字段名	
	通常为mail	
上一步	下一步取消	
参数说明:		
参数名称	描述	示例值



用户名	用户名对应的字段名	uid
用户昵称	通常为 displayName	јоу
手机号码	通常为 telephoneNumber	13xxxx5xxx6
邮箱地址	通常为 mail	1xxxxxx9@qq.com

5. 在完成页面,单击**完成**返回数据源列表。





配置数据源

最近更新时间: 2023-06-05 17:46:53

新建数据源后,可以通过配置数据源对数据源属性进行修改。

配置 SCIM 数据源

- 1. 登录 数字身份管控平台(员工版)控制台,在左侧导航中,单击**同步中心 > 上游同步**。
- 1. 在上游同步页面,选择 SCIM 数据源,单击操作列的基础配置。

数据源名称/ID	描述	数据源类型 ▼	启用状态 🚯	创建时间 🕈	同步状态 ▼	操作
		SCIM		2022-01-28 10:48:23	未同步	基础配置删除
	-	SCIM		2021-08-18 16:11:44	未同步	基础配置删除

2. 在该应用源的基本信息页面,单击基本配置或参数配置右上角的**编辑**。

① 说明 当获取方式为 平台拉取 时,支持修改参数配置中的参数。	
基本信息 增量同步	
基本配置	编辑
数据源名称	
数据图D 6 FD	
参数配置	馬嶺
Rindsi Limet	
Cient ID	
Client Secret	
Token	
User URL	
Org URL	

3. 在基本配置弹窗中,修改相关参数,单击确定,即可修改数据源信息。

基本配置		×
数据源名称 *		
描述	请填写简短描述,限128字内	
	确定取消	

4. 单击增量同步,可以查看增量同步的数据同步情况。

D 2002年8月人(新生) P 第7022年8日人(新生) 第802年8日人(新生) 第802年9日人(新生) 第802年9日人(新生)	基本信息							
R/1987 R/2 R/2018 R							清输入异维原因搜索	Q
	同步时间	同步来源	同步目标	腔弧类型	网步结束	异常原因	股級非常	

5. 如果数据获取是平台拉取,当数据源启用时,还可以在手动同步页面中单击**手动同步**,进行数据的手动同步。

基本信息	手动同步 增量同步日志					
手动同步						请输入任务批次ID进行搜索
任务批次ID		同步时间	同步来源	同步目标	同步状态	撮作
			本系统目录服务	12	等待同步	停止同步



6. 在手动同步页面中,单击**查看日志**,可以查看数据的同步明细。

日志明细			×
		请输入异常原因搜索	Q
数据类型	同步结果	异常原因	数据详情
共 1 条		10)▼条/页 🛛 ◀ 1 /1页 ▶ №

配置 AD 数据源

1. 在 上游同步页面,选择 AD 数据源,单击操作列的基础配置。

kat brite							
数据源名称/ID	掘述	数据源类型 ▼	启用状态 ①	创建时间 \$	同步状态 T	操作	
		AD		2022-01-24 15:58:15	未同步	新設配置 同步配置 删除	
Succession of the local division of the loca	1	AD		2022-01-22 18:31:22	未同步	基础配置 同步配置 删除	

- 2. 在该应用源的基本信息页面,单击右上角的**编辑**,修改相关参数,单击确定即可修改数据源信息。
- 3. 在 AD 数据源信息页面,选择手动同步,查看手动同步的数据同步情况。数据源启用时,单击一键同步可以进行手动同步。

基本信息 同步配置					
任务批次ID	四位 时(6)	同步来源	同步目标	同步状态 ▼	操作

4. 选择需要同步的 AD 数据源节点和平台节点,单击确定同步,即可将数据节点下的组织机构和用户数据同步至平台节点下。

一键同步				×
同步重置	■置			
同步范围				
序号	数据源节点	平台节点	操作	
1	请选择 ▼	请选择 ▼	新增删除	
	确	定同步 取消		

配置 LDAP 数据源

1. 在 上游同步页面,选择 LDAP 数据源,单击操作列的基础配置。

MR L2014-							
数据源名称/ID	描述	数据源类型 ▼	启用状态 ①	创建时间 \$	同步状态 ▼	操作	
		AD		2022-01-24 15:58:15	未同步	基础配置 同步配置 删除	
-	1	AD		2022-01-22 18:31:22	未同步	基础配置 同步配置 删除	



2. 在数据源信息页面,单击基本配置、配置服务器链接或字段匹配规则右上角的编辑。

基本信息	同步就置	
基本配置		编辑
数据源名称		
数据源ID	3/7 c /2	
描述		
		_
配置服务器	· 接	编辑
使用代理		
服务器地址		
端口号		
Base DN		
使福島DN		
管理员密码	· · · · · · · · · · · · · · · · · · ·	
同步默认密研		
字段匹配规	I	编辑
用户名		9
用户昵称		C
手机号码		=
邮箱地址		-

3. 在对应弹窗中,修改相关参数,单击确定即可修改数据源信息。

4. 在 LDAP 数据源信息页面,选择手动同步,查看手动同步的数据同步情况。数据源启用时,单击一键同步可以进行手动同步。

基本信息 同步配置					
任务批次ID	同步时间	同步来源	同步目标	同步状态 T	操作

5. 选择需要同步的 LDAP 数据源节点和平台节点,单击确定同步,即可将数据节点下的组织机构和用户数据同步至平台节点下。

一键同步			×
同步重置	重置	择范围后进行同步	
同步范围			
序号	数据源节点	平台节点	操作
1	请选择 ▼	请选择 ▼	新增 删除
		确定同步取消	



删除数据源

最近更新时间: 2022-12-06 17:04:45

新增数据源后,如不再需要数据源,支持删除单个数据源或批量删除数据源。

```
    注意
    删除后,相应的权限将会取消且无法恢复,请谨慎操作。
```

删除单个数据源

1. 在 上游同步页面,选择未启用的数据源,单击操作列的删除,弹出确认删除弹窗。

新建上游同步 删除						
数据源名称/ID	描述	数据源类型 ▼	启用状态 ()	创建时间 \$	同步状态 下	操作
	-	SCIM		2022-01-28 10:48:23	未同步	基础配置 删除
	-	SCIM		2021-08-18 16:11:44	未同步	基础配置删除
	-	LDAP		2021-08-04 15:04:26	未同步	基础配置 同步配置 删除

2. 在确认删除弹窗中,单击确定,即可删除所选账号。

确定删除所选择的数据源?		×
当前数据源 测 谨慎操作。)删除后,相应的权限将会取消且无法恢复,	请
	論定 关闭	

批量删除数据源

1. 在 上游同步页面,选择一个或多个未启用的数据源,单击左上角的删除,弹出确认删除弹窗。

新建上游同步 劃除						
✓ 数据源名称/ID	描述	数据源类型 ▼	启用状态 🛈	创建时间 🕈	同步状态 ▼	操作
	-	SCIM		2022-01-28 10:48:23	未同步	基础配置册除
	-	SCIM		2021-08-18 16:11:44	未同步	基础配置删除
C 4	-	LDAP		2021-08-04 15:04:26	未同步	基础配置 同步配置 删除

2. 在确认删除弹窗中,单击确定,即可删除所选账号。

确定删除所选择的数据源?	×
您已选择2条数据源, 查看详情 ▶ 删除后,相应的权限将会取消且无法恢复,请谨慎操作。	
确定 关闭	



下游同步

新建数据源

最近更新时间: 2024-11-14 14:50:32

下游同步是指从平台同步组织机构、用户数据到外部数据源或下游应用、LDAP/AD。

新建 SCIM 数据源

- 1. 登录 数字身份管控平台(员工版)控制台,在左侧导航中,单击**同步中心 > 下游同步**。
- 2. 在下游同步页面,单击**新建下游同步**,选择 SCIM 协议。

数字身份管控平台 (员 工版)	下游同步
器 概 览	
ஜ 用户管理 ∽	下游同步是指从平台同步组织机构、用户数据到外部数据源或下游应用、
鸟 认证管理	新建下游同步
品 应用管理	同步名称/ID
授权管理 · · · ·	
目 审计管理	6
「「同步中心 ^	共 1 条
• 上游同步	
• 下游同步	

3. 在配置基本信息页面,输入数据源名称和描述,单击**下一步**。

1 配置基	本信息 > 2 配置参数信息 > 3 完成
数据源名称 *	请输入数据源名称
描述	请输入简单描述,不超过128字个字符
下一步	取消



4. 在配置参数信息页面,配置相关参数后,单击**下一步**。

✔ 配置基本信息 〉 2 配置参数信息 〉 3 完成		
获取方式 🛈 *	○平台推送 ○数据源拉取 获取方式在创建后不可修改	
Client ID *	请输入Client ID	
Client Secret *	请输入Client Secret	
Token *	请输入Token	
User URL *	请输入User URL	
Org URL *	请输入Org URL	
上一步	下—步 取消	

参数说明:

- 获取方式:根据实际需求选择数据源推送或平台拉取,获取方式在创建后不可修改。
- Client ID: 客户端 id,在 应用管理页面,选定指定应用,单击操作列的应用配置,查看 Client ld 值。

应用管理				
① 支持特创建标准协议应用,包括CAS、SCIM、JW	T、OAuth2、表单代填、云API网关应用;支持在应用市场选择预集成应用t	共速接入。		不再提醒 X
应用协议新建 应用市场新建 能是那种			请输入应用名称应用ID搜索	Q
应用名称	应用ID	应用状态	操作	
			应用配置 删除	
			应用配置 删除	
			应用配置 选择	

○ Client Secret:客户端 Secret,在应用管理页面,选定指定应用,单击操作列的应用配置,查看 Client Secret 值。含有特殊字符,需要做 URLEncode。

- Token: 根据 Client ID 和 Client Secret 返回的 access_token。详情请参见 SCIM 数据源对接─调用方式。
- User URL: 用户 id,详情请参见 SCIM 数据源对接-用户 API。
- Org URL: 组织机构 id,详情请参见 SCIM 数据源对接-组织机构 API。
- 5. 在完成页面,单击**完成**返回数据源列表。



新建 AD 数据源

1. 在 下游同步页面,单击**新建下游同步**,选择 AD。



2. 在配置基本信息页面,输入数据源名称和描述,单击**下一步**。

1 配置基	本信息 〉 ② 配置参数信息 〉 ③ 完成
数据源名称★	清输入数据源名称
描述	请输入简单描述,不超过128字个字符
下一步	取消

3. 在配置服务器连接页面,根据同步的 AD 的安装位置,选择是否启用代理开关。

○ 如果同步的 AD 安装在外网,则关闭使用代理开关,根据要求填写相关信息后,单击**下一步**。

✔ 基本信	息 〉 2 配置服务器连接 〉 3 字段匹配规则 〉 4 完成
agent下载	AD Agent: 将内网AD与本系统进行连接 大小: 25MB 点击下载
使用代理 *	の 如果同步的LDAP安装在内网环境,需要先下载LDAP Agent并根据配置指引进行代理配置,再打开 "使用代理" 开关
服务器地址★	请输入服务器地址
端口号*	清缅入端口号
Base DN *	请输入Base DN,如:dc=XXX,dc=XXX
	为确保数据同步成功,Based DN保存后不可更改,如果Base DN发生变化会使双方组织机构无法对应而导致数据同步失败
SSL连接方式 *	一 开启后,服务器采用SSL连接方式
管理员DN *	请输入管理员DN
	若进行同步操作后修改管理员DN,需重新进行数据同步
管理员密码*	请输入管理员DN所对应的密码 💋
同步默认密码 *	请输入同步默认密码 💋
	数据同步后,用户登录EIAM的默认密码
密码加密方式 *	请选择密码加密方式 ▼
上一步	下一步 取消 测试连接

参数名称	描述	示例值
服务器地址	连接的外网 AD 服务器地址	116.62.207.52
端口号	连接服务器地址的端口号	389
Base DN	在 AD 服务器上 AD 域控的 DN	DC=moonxy,DC=com



管理员 DN	管理员的全名,也就是 AD 服务器上管理员账号的 distinguishedName 属性值	CN=Administrator,CN=Users,DC=ebg,DC=gtac,D C=com
管理员密码	所填 AD 服务器管理员账号的密码	Aa123456
同步默认密码	数据同步后,用户登录 EIAM 的默认密码	Aa123456

○ 如果同步的 AD 安装在内网环境,需要先下载 AD Agent 并根据配置指引进行代理配置,再打开使用代理开关,根据要求填写相关信息后,单击下一步。

✔ 基本信題	息 > 2 配置服务器连接 > 3 字段匹配规则 > 4 完成
agent下载	AD Agent: 将内网AD与本系统进行连接 大小: 25MB 点击下载
使用代理 *	
	如果同步的LDAP安装在内网环境,需要先下载LDAP Agent并根据配置指引进行代理配置,再打开 "使用代理" 开关
agent地址 *	请填写agent地址
同步默认密码 *	请输入同步默认密码
	数据同步后,用户登录EIAM的默认密码
密码加密方式 *	请选择密码加密方式 ▼
client_id	w z 17
client_secrent	oi E
上一步	下一步 取消 测试连接

参数名称	描述	示例值
agent 地址	连接的内网 AD 服务器地址	http://116.25.75.22
同步默认密码	数据同步后,用户登录 EIAM 的默认密码	Aa123456
client_id	用于配置 agent 的参数	f5k58wfdc7jcc87jz74k
client_secret	用于配置 agent 的参数	fvjazuorj5f1



4. 在字段匹配规则页面,根据要求填写相关信息后,单击**下一步**。

🗸 🛃	「信息 〉 🗸 配置服务器连接 〉 3 字段匹配规则 〉 👍 完
用户名 *	请输入用户名对应的字段名
	若为Windows AD,则字段名为: sAMAccountName
用户昵称 *	请输入用户昵称
	通常为displayName
手机号码 *	请输入手机号码对应的字段名
	通常为telephoneNumber
邮箱地址*	请输入邮箱地址对应的字段名
	通常为mail
域名名称	请输入域名名称
	若域名为eiam.tencent.com,用户名为joy,则Windows AD登录名为Joy@eiam.tencent.com
上一步	下一步取消

参数说明:

参数名称	描述	示例值
用户名	用户名对应的字段名	sAMAccountName
用户昵称	通常为 displayName	displayName
手机号码	通常为 telephoneNumber	telephoneNumber
邮箱地址	通常为 mail	mail
域名名称	AD 域名名称	eiam.tencent.com

5. 在完成页面,单击**完成**返回数据源列表。



新建 LDAP 数据源

1. 在 下游同步页面,单击**新建下游同步**,选择 LDAP。



2. 在配置基本信息页面,输入数据源名称和描述,单击**下一步**。

数据源名称 *	请输入数据源名称	
描述	请输入简单描述,不超过128字个字符	

3. 在配置服务器连接页面,根据同步的 LDAP 的安装位置,选择是否启用代理开关。

○ 如果同步的 LDAP 安装在外网,关闭使用代理开关,根据要求填写相关信息后,单击**下一步**。

🗸 基本信息	息 > 2 配置服务器连接 > ③ 字段匹配规则	> ④ 完成
agent下载	LDAP Agent: 将内网LDAP与本系统进行连接 大小: 25MB 点击下载	
使用代理 *	如果同步的LDAP安装在内网环境,需要先下载LDAP Agent并根据配置指引进行	代理配置,再打开 "使用代理" 开关
服务器地址 *	请输入服务器地址	
端口号*	清堬入满口号	
Base DN *	请输入Base DN,如:dc=XXX,dc=XXX	
	为确保数据同步成功,Based DN保存后不可更改,如果Base DN发生变化会使)	双方组织机构无法对应而导致数据同步失败
SSL连接方式 *	一 开启后,服务器采用SSL连接方式	
管理员DN *	请输入管理员DN	
	若进行同步操作后修改管理员DN,需重新进行数据同步	
管理员密码 *	请输入管理员DN所对应的密码	
同步默认密码 *	请输入同步默认密码	
	数据同步后,用户登录EIAM的默认密码	
密码加密方式 *	请选择密码加密方式 ▼	
上一步	下一步 取消 测试连接	

参数名称	描述	示例值
服务器地址	连接的外网 LDAP 服务器地址	116.62.207.52
端口号	连接服务器地址的端口号	80
Base DN	在 LDAP 服务器上 LDAP 域控的 DN	DC=moonxy,DC=com



管理员DN	管理员的全名,即 LDAP 服务器上管理员账号的 distinguishedName 属性值	CN=Administrator,CN=Users,DC=ebg,DC=gtac,DC =com
管理员密码	所填 LDAP 服务器管理员账号的密码	Aa123456
同步默认密码	数据同步后,用户登录 EIAM 的默认密码	Aa123456

○ 如果同步的 LDAP 安装在内网环境,需要先下载 LDAP Agent 并根据配置指引进行代理配置,再打开使用代理开关,根据要求填写相关信息后,单击下一步。

✓ 基本信息 〉 2 配置服务器连接 〉 3 字段匹配规则 〉 4 完成
agent下载 LDAP Agent: 將內网LDAP与本系统进行连接 大小: 25MB 点击下载
使用代理 •
agent地址 * 请填写agent地址
同步默认密码 请输入同步默认密码
数据同步后,用户登录EIAM的默认密码
密码加密方式★ 请选择密码加密方式 ▼
client_id t
client_secrent r
上一步 取消 測试 差接

参数名称	描述	示例值
agent 地址	连接的内网 LDAP 服务器地址	116.62.207.52
同步默认密码	数据同步后,用户登录 EIAM 的默认密码	Aa123456
client_id	用于配置 agent 的参数	f5k58wfdc7jcc87jz74k
client_secret	用于配置 agent 的参数	fvjazuorj5f1



4. 在字段匹配规则页面,根据要求填写相关信息后,单击**下一步**。

°目录,字段名为:uid					
<u></u> 輸入用户昵称					
为displayName					
	字段名				
为telephoneNumber					
	字段名				
101 101 101 101 101 101	输入用户昵称 为displayName 输入手机号码对应的 ³³ 为telephoneNumber 输入邮箱地址对应的 ³⁴	輸入用户昵称 为displayName 输入手机号码对应的字段名 为telephoneNumber 输入邮箱地址对应的字段名	輸入用户昵称 为displayName 输入手机号码对应的字段名 为telephoneNumber 输入邮箱批址对应的字段名	輸入用户昵称 为displayName 输入手机号码对应的字段名 为telephoneNumber 输入邮箱地址对应的字段名	輸入用户昵称 为displayName 输入手机号码对应的字段名 为telephoneNumber 输入邮箱地址对应的字段名

参数说明:

参数名称	描述	示例值
用户名	用户名对应的字段名	uid
用户昵称	通常为 displayName	јоу
手机号码	通常为 telephoneNumber	13xxxx5xxx6
邮箱地址	通常为 mail	1xxxxxx9@qq.com

5. 在完成页面,单击**完成**返回数据源列表。





配置数据源

最近更新时间: 2022-12-06 17:11:05

新建数据源后,可以通过配置数据源对数据源属性进行修改。

配置 SCIM 数据源

- 1. 登录 数字身份管控平台(员工版)控制台,在左侧导航中,单击**同步中心 > 下游同步**。
- 1. 在下游同步页面,选择 SCIM 数据源,单击操作列的基础配置。

BRE FEIRIG							
數据源名称/ID	描述	数据源关型 ▼	启用状态 ①	合[1批日](II] 中	同步状态 ▼	操作	
1. 6		SCIM		2022-01-24 17:07:03	未同步	基础配置 手动同步 删除	
61		SCIM		2022-01-24 17:05:16	末間步	基础配置 手动同步 删除	

2. 在该应用源的基本信息页面,单击基本配置或参数配置右上角的编辑。

① 说明 当获取方式为 平台拉取 时,支持修改参数配置中的参数。						
基本配置	编辑					
設造課名称						
政策用D b 15						
無送						
参数配置	编辑					
积和方式 下 剧推送						
Client ID						
Client Secret						
Token						
Uig UKL						

3. 在基本配置弹窗中,修改相关参数,单击确定,即可修改数据源信息。

	基本配置		×
	数据源名称★		
	描述	请填写简短描述,限128字内	
		确定 取消	
4.	单击 增量同步 ,	可以查看增量同步的数据同步情况。	

基本信息 增量同步							
						请输入异常原因被索	Q
同步时间	同步来源	同步目标	15% 类型	同步结束	异常原因	823804 (II	

5. 如果数据获取是平台拉取,当数据源启用时,还可以在手动同步页面中单击**手动同步**,进行数据的手动同步。

基本信息 手动同步 增量同步日志					
手动同步					请输入任务批次ID进行搜索
任務批次ID	同步时间	同步来源	同步目标	同步状态	操作
		本系統目录服务	12	等待同步	停止同步



6. 在手动同步页面中,单击**查看日志**,可以查看数据的同步明细。

日志明细			×
		请输入异常原因搜索	Q
数据类型	同步结果	异常原因	数据详情
共 1 条		10 •	▼条/页 I /1页 ▶ M

配置 AD 数据源

1. 在 下游同步页面,选择 AD 数据源,单击操作列的基础配置。

数据源名称/ID	描述	数据源类型 ▼	启用状态 ①	创建时间 🕈	同步状态 ▼	操作
		AD		2022-01-28 15:38:28	未同步	基础配置同步配置 删除
☐ <u>ă</u> 6	-	SCIM		2022-01-28 11:50:50	未同步	基础配置删除

2. 在数据源信息页面,单击右上角的编辑,修改相关参数,单击确定即可修改数据源信息。

基本信息	
基本配置	编辑
教委等各位	-
数编制D 238 m	
描述	
配置聯旁器链接	编辑
服务器地址	
第四号	
Base DN	
SSL连接方式 🕐 已开启, 超另闢將采用SSL连接方式	
管理员DN C	
管理児素詞 → ••••• ◎	
室园加定方式 不 加 查	
学得死能接触	
用户规定	•
手机导码	E
新職地址	E
城高客僚	
E AD 数据源信息页面,选择手动同步,查看手动同步的数据同步情况。数据源启用时,单击 一键同步 可以进行手动同步。	

3. 7	在 AD 数据源信息页面,	选择手动同步,	查看手动同步的数据同步	青况。数据源启用时,单击	一键同步可以进行手动同步。	0	
	基本信息 同步配置 增量同步						
	一個同步						
	任务批次ID	网络银银	四步來源	同步目标	同步状态 ▼	操作	

4. 选择需要同步的 AD 数据源节点和平台节点,单击**确定同步**,即可将数据节点下的组织机构和用户数据同步至平台节点下。可选择开启增量同步,开启后,将自动执行增 量同步。



数据源节点	3	平台节点		操作
请选择 ▼		请选择	•	新增删除
▶ 开启后,将自动执行增量同步, 7	可在增量同步页面查看记录	L c		
	数据源节点 请选择 ▼ 开启后,将自动执行增量同步,	数据源节点 3 请选择 ▼ 【 】 开启后,将自动执行增量同步,可在增量同步页面查看记录	数据源节点 平台节点 请选择	数据源节点 平台节点 请选择 ▼ 「请选择 ▼ → 开启后,将自动执行增量同步,可在增量同步页面查看记录

5. 在增量同步页面,支持开启/关闭增量同步并查看增量同步记录。

基本信息 同步音	2 增量同步						
増量同步 🔵	已关闭 最近同步时间 -					请输入异常原因搜索	Q
同步时间	同步来源	同步目标	設掘类型	同步结束	异龙原因	胶掘洋销	

配置 LDAP 数据源

1. 在 下游同步页面,选择 LDAP 数据源,单击操作列的基础配置。

60E120F0/ 803							
数据源名称/ID	描述	数据源类型 ▼	息用状态 ①	8)](能时)(印) \$	同步状态 下	揮作	
		LDAP		2022-01-24 16:41:01	未阅步	基础起源 同步配置 删除	

2. 在数据源信息页面,单击右上角的编辑,修改相关参数,单击确定即可修改数据源信息。

基本配置		
如据源名称 1		
対展源ID 8	8 7a 1 <mark>0</mark>	
彭述		
己置服务器链	<u>接</u>	
电用代理		
务器地址	1	
10 9	8	
ase DN	d	
SL连接方式	● 已开启, 服务器将采用SSL连接方式	
理员DN	c i i i i i i i i i i i i i i i i i i i	
理员密码		
步默认密码		
網加密方式	不加密	
段匹配规则		

基本信息 同步配置					
任务批次ID	同步时间	同步来源	同步目标	同步状态 T	操作

选择需要同步的 LDAP 数据源节点和平台节点,单击确定同步,即可将数据节点下的组织机构和用户数据同步至平台节点下。可选择开启增量同步,开启后,将自动执行增量同步。



一键同步			×				
同步重置	重置	围后进行同步					
同步范围							
序号	数据源节点	平台节点	操作				
1	请选择 ▼	请选择 ▼	新增 删除				
确定同步取消							



删除数据源

最近更新时间: 2022-12-06 17:05:09

新增数据源后,如不再需要数据源,支持删除单个数据源或批量删除数据源。

▲ 注意

删除后,相应的权限将会取消且无法恢复,请谨慎操作。

删除单个数据源

1. 在 下游同步页面,选择未启用的数据源,单击操作列的删除,弹出确认删除弹窗。

数据源名称/ID	描述	数据源类型 ▼	启用状态 ①	创建时间 \$	同步状态 ▼	操作
		LDAP		2022-02-09 16:36:04	未同步	基础配置同步配置删除
e e		SCIM		2022-01-11 16:08:35	未同步	基础配置删除

2. 在确认删除弹窗中,单击确定,即可删除所选账号。

确定删除所选择的数据源?	:	×
当前数据源 测 谨慎操作。) 删除后,相应的权限将会取消且无法恢复,谨	土口
	義定关闭	

批量删除数据源

1. 在 下游同步页面,选择一个或多个未启用的数据源,单击左上角的删除,弹出确认删除弹窗。

新建下游同步 删除								
✓ 数据源名称/ID		描述	数据源类型 ▼	启用状态 ()	ŧ	则建时间 \$	同步状态 ▼	操作
₹3	э	-	LDAP		2	022-02-09 16:36:04	未同步	基础配置同步配置 删除
₩		-	SCIM		2	022-01-11 16:08:35	未同步	基础配置删除
11 61		-	SCIM		2	021-12-07 16:59:26	已同步	基础配置手动同步删除

2. 在确认删除弹窗中,单击确定,即可删除所选账号。

确定删除所选择的数据源?	×
您已选择2条数据源, 查看详情 ▶ 删除后,相应的权限将会取消且无法恢复,请谨慎操作。	
确定 关闭	



系统配置 安全设置

最近更新时间: 2022-12-06 16:10:44

本文将为您介绍如何在数字身份管控平台(员工版)控制台,配置二次认证、密码策略等。

二次认证

启用二次认证后,所有用户在登录时需强制二次认证,认证方式主要包含短信验证码认证。 1. 登录 数字身份管控平台(员工版)控制台,在左侧导航栏,选择**系统配置 > 安全设置**。

2. 在二次认证页面,勾选开启登录二次认证,根据需求选择二次认证方式后,单击确定,即可开启登录二次认证。

安全设置				
二次认证	密码策略	登录配置	注册配置	安全域 (CORS)
开启登	录二次认证	<mark>✓ 开启登录</mark> 勾选后,所有	二次认证 「用户在登录时需	强制二次认证。取消勾选,关闭所有用户的二次认证。
* 二次认	证方式	短信验证码;	认证	•
		选择二次认证	方式。	
		确定		

密码策略

新建用户以及用户注册中的密码,管理员可以通过密码策略来进行设置。

- 1. 登录 数字身份管控平台(员工版)控制台,在左侧导航栏,选择**系统配置 > 安全设置**。
- 2. 在密码策略页面,根据需求选择密码强度,调整密码最大长度与最小长度后,单击**确定**,将按新的密码策略进行校验。

安全设置					
二次认证	密码策略	登录配置	注册配置	安全域(CORS)	
* 密码碑	÷	数字+大写号	字母+小写字母+粽	殊字符	.
* 最大长	÷	- 12	+ 位		
* 最小长	÷.	- 8	+ 位		
		确定			

登录配置

- 1. 登录 数字身份管控平台(员工版)控制台,在左侧导航栏,选择**系统配置 > 安全设置**。
- 2. 在登录配置页面,进行相关配置后,单击**确定**。

()	说明	
	勾选 锁定设置 ,	将启用户登录失败锁定规则



安全设置	
二次认证 密码策略	登录配置 注册配置 安全域 (CORS)
锁定设置	▼
* 密码错误锁定次数	 − 5 + 密码输入错误穴数超过设定范围,账户将被锁定,在解锁前都不能再次登录。
* 密码尝试时间范围	 — 3600 +< 单位: 秒。
* 解锁时间	30分钟 ▼ 登录时密码错误次数过多被锁定后的自动解锁时间
验证码	✓ 验证码 开启后用户在登录失败超过限定次数时,会自动开启验证码验证。
* 密码错误次数	- 1 + 密码输入错误次数超过设定范围,即开启验证码登录验证。
* 验证码尝试时间范围	- 1 + 单位: 秒。
	确定

注册配置

- 1. 登录 数字身份管控平台(员工版)控制台,在左侧导航栏,选择**系统配置 > 安全设置**。
- 2. 在注册配置页面,进行相关配置后,单击确定。

安全设置				
二次认证	密码策略	登录配置	注册配置	安全域 (CORS)
允许注册	Ð	● 开启后,允许用F	户通过自助注册	8.
注册审批	比	注册审批 开启注册审批后,	,用户注册后言	暑要管理员进行审批,通过后才能激活用户。
默认所属	属主组织机构	请选择		
		注册用户所属机构	构,若不选择,	则注册用户将属于组织机构根节点下。
默认所属	國用户组	请选择		·
		注册用户所属用户	户组, 若不选持	译,则注册用户将不属于任何用户组。
		确定		

参数说明:

- 允许注册:开启后,将允许用户自助注册。
- 注册审批:开启注册审批后,用户注册后需要管理员进行审批,通过后才能激活用户。
- 默认所属主组织机构:注册用户所属机构,若不选择,则注册用户将属于组织机构根节点下。
- 默认所属用户组:注册用户所属用户组,若不选择,则注册用户将不属于任何用户组。

安全域 CORS

如果需要采用 SDK 方式调用平台 API,必须要填写信任的安全域(CORS)范围才能成功调用,最多可设置10个安全域。 1. 登录 数字身份管控平台(员工版)控制台,在左侧导航栏,选择**系统配置 > 安全设置**。



2. 在安全域(CORS)页面,填写信任的安全域(CORS)范围后,单击确定。

安全设置		
二次认证 密码策略	登录配置 注册配置 安全域 (CORS)	
安全域 (CORS)	请填写信任的安全域(CORS)范围,多个请用换行符分割,如: https://example.com https://*.example.com	
	如果需要采用SDK方式调用平台API,必须要填写信任的安全域(CORS)范围才能成功调用,最多可设置10个安全域。安全域的校验规则如下: (1) 应以https://或http://开头(2) 格式应为协议+域名+鳞口,不支持携带请求路径(3)域名部分只允许包含小写字母、数字、中文、半角、半角*、半角+(4)域名的每一段中,*-*不能作为开头或结尾(5)域名的第 一段,允许为*,但不允许包含*,其他段不允许为*或包含*	
	離定	安全地

校验规则如下:

- 应以 https:// 或 http:// 开头。
- 格式应为协议+域名+端口,不支持携带请求路径。
- 域名部分只允许包含小写字母、数字、中文、半角.、半角*、半角-。
- 域名的每一段中, 不能作为开头或结尾。
- 域名的第一段,允许为 * ,但不允许包含 * ,其他段不允许为 * 或包含 * 。



短信模板配置

最近更新时间: 2022-12-06 16:10:58

操作场景

本文将为您介绍如何在数字身份管控平台(员工版)控制台,配置短信服务网关和短信模板的信息。

操作步骤

1. 登录 数字身份管控平台(员工版)控制台,在左侧导航栏,选择**系统配置 > 模板设置**,进入模板设置页面。

2. 在模板设置页面,在未设置任何短信模板的情况下,系统默认显示以下空白模板信息,短信服务测试功能暂时无法使用。

 说明 平台默认提供50条免费短信,超额后平台提供的短信服务将无法使用。 	
模板设置	
短信影务配置	编辑
超压器务 -	
短信模板配置 ①	
地震い症 ③・ ・	
修改手机号码 ①*	
短续服务测试 《中立大学》:"在学校》	

- 3. 在模板设置页面,单击界面右上角的编辑,进入短信模板编辑页面。
- 4. 在编辑页面,分别设置短信服务配置、短信模板配置的相关参数,并测试短信服务。

0	说明			
	不同的短信服务配置的参数不同,	平台目前 仅支持腾讯云短信服务 ,	后续会陆续支持其他短信服务的配置。	以下为配置腾讯云短信服务所需要的相关参数。

• 短信服务配置

短信服务选择腾讯云短信服务,并输入 SDK AppID、SecretId 和 SecretKey 参数, 相应参数获取方法如下:

短信服务配置		
短信服务	腾讯云短信服务	*
SDK AppID *	请输入SDK AppID	
SecretId *	请输入SecretId	
SecretKey *	请输入SecretKey	

获取 SDK AppID

4.1.1 登录 腾讯云短信控制台,在左侧导航栏,选择**应用管理 > 应用列表**,进入应用列表页面。



4.1.2 在应用列表页面,单击创建应用,输入应用名称和简介,单击创建,即可完成创建应用。

创建应用		×
应用名称*		
应用简介	请输入应用简介	
	0 / 300 不超过300字	
	创建取消	

4.1.3 在应用列表页面,选择所需应用,单击口获取该应用的 SDK AppID。

•	E	
SDRAppID: 1	1221	1
停用		

○ 获取 SecretId 和 SecretKey

4.1.1 登录 访问管理控制台,在左侧导航栏,选择用户 > 用户列表,进入用户列表页面。

4.1.2在用户列表页面,选择所需子账号,单击**用户名称**,进入用户详情页面。

用户名称	用户类型	账号ID	创建时间	关联信息	操作
>	是账号			65	授权更多操作 ▼
· [子用户			L. 🖾	授权 更多操作 ▼

4.1.3在用户详情页面,单击 API 密钥,选择所需密钥,单击 口获取该子账号的 SecretId;单击显示,身份校验成功后,即可获取该子账号的 SecretKey。

权限 服务 组(0) 安全 ① API 案钥 」	程序			
 密钥最近访问时间为此密钥最近一次被调用的时间。 				
新建密钥				
邀钥	创建时间	最近访问时间	状态	操作
SecretId: Al Fi SecretKey: ******显示	2	2021-06-15	已启用	禁用

• 短信模板配置

为了确保业务的正常使用,管理员需要通过模板设置页面的短信模板功能,配置短信服务网关和短信模板,后续短信服务将通过该配置的短信服务网关和短信模板进行发 送。

4.1 腾讯云短信服务需要分别设置 短信签名 和 短信模板 ID,并针对短信认证(包括短信验证码登录和短信二次认证)、修改手机号码等短信发送场景分别设置对应的 模板。





4.2 如果用户已经设置了短信模板,通过模板设置页面可以查看已设置的短信模板信息。

短信服务配置		
短信服务	腾讯云短信服务	
SDK AppID •		
SecretId •		
SecretKey ·		
短信模板配置 🛈		
短信认证 🛈 •	80	6
修改王和昌和 ①•	10	9

• 测试短信服务

用户可对短信服务的有效性和正确性进行测试,测试过程如下所示。

4.1 单击**点击立即测试短信服务**链接,则会弹出测试窗口。

短信模板		
短信服务配置		
短信服务	腾讯云短信服务	
SDK AppID •		
SecretId .		
SecretKey .		
短信模板配置 🛈		
短信认证 🛈 •	推 电 1	9
修改手机号码 🛈 •	腾讯	91
短信服务测试	点击立刻测试短信服务	

4.2 在短信服务测试窗口中,输入手机号码并选择测试模板,单击**发送**,即可通过输入的手机号码是否接收到测试短信、短信签名,来确认短信服务的配置是否正确。

短信服务测	山试		×
手机号码 *	+86	•	
测试模板 *	○ 短信登录	○ 修改手机号码	
		发送	



个性化设置

最近更新时间: 2022-12-06 16:12:31

本文将为您介绍如何在数字身份管控平台(员工版)控制台,设置门户信息、自定义门户域名。

门户设置

- 1. 登录 数字身份管控平台 (员工版)控制台,在左侧导航栏,选择**系统配置 > 个性化设置**。
- 2. 在门户设置页面,选择图片设置公司图标,通过公司名称设置修改门户展示名称,单击**保存**。

① 中途面 ② 切園都	 说明 单击予 	项览 ,可以提前预览配置后的门户信息。
E 主义項名 Correct Data Correct Correct Data Correct Data Correct Da	个性化设置	Niko (
公司商息 * 公司商标 正式 通貨商片 通貨商片 通上传 jogillang 格式文件、大小 1MB 0/约	I IP WE BE	246
C 公司图标 E 決违計準片 通片間片 通上传 (pg)E gg E	公司信息	
張上传 jagiliping 結式文件、大小 1MB 以内 *公司名称	*公司图标	送未進件進片 "血血 通時照片
* 公司各称		请上传 jpg用png 相比文件。大小 1MB 30均
	*公司名称	
2017 税定	保存	預定

自定义域名

- 1. 登录 数字身份管控平台 (员工版)控制台,在左侧导航栏,选择**系统配置 > 个性化设置**。
- 2. 在自定义域名页面,通过自定义域名设置,更改访问的门户的域名地址,单击**保存**。

门户	92 1	自定义域名			
	_				
	① 支持	通过配置自定义域名使用自有域名登录。如果	1.不配置,则采用默认城名。		
0	域名前缀	○ 自有域名			
,	https:// to	N .portal.te	com		
	保存				



其他管理

注册审批

最近更新时间: 2022-12-06 16:22:08

本文将为您介绍如何在数字身份管控平台(员工版)控制台,审批用户注册申请的系统账号。

操作步骤

1. 登录 数字身份管控平台(员工版)控制台,在左侧导航栏,选择**其他管理 > 注册审批**。

2. 在注册审批页面,定位到要操作的申请记录,单击操作列的**通过**或拒绝。

通过 担绝					请输入用户名称或ID
用户名称	手机号码	郎箱	申请时间	审批状态 ▼	操作
1	+86-1		2022/01/18 18:30:08	⊘ 已通过	查看详情
	+86-1	1 d.	2022/01/18 14:59:00	() 待审批	通过 拒绝

3. 在弹出的对话框,单击确定,即可完成注册账号的审批。

4. 在注册审批页面,单击操作列下的**查看详情**,可以查看具体的应用账号申请信息。

通过担急					请输入用户名称或ID
用户名称	手机号码	邮箱	申请胜任问	审批状态 ▼	操作
	+86-	14 1	4 2022/01/18 18:30:08	⊘ 已通过	查看详情
1	+86-1	14	d 2022/01/18 14:59:00	() 待审批	通过 拒绝



账号审批

最近更新时间: 2022-12-06 16:22:17

本文将为您介绍如何在数字身份管控平台(员工版)控制台,审批用户申请的应用账号。

操作步骤

1. 登录 数字身份管控平台(员工版)控制台,在左侧导航栏,选择**其他管理 > 账号审批**。

2. 在账号审批页面,定位到要操作的申请记录,单击操作列的**同意**或**拒绝**。

F	拒绝							请输入用户
	用户名称	账号名称	应用名称	账号组	叩请时间	审批状态 ▼	操作	
			OAUTH2		2021-12-31 17:30:45	已通过	详情	
		100 C	OAUTH2		2021-12-31 17:30:34	① 已拒绝	详情	
			JWT		2021-12-31 11:27:19	③待审批	同意	拒绝 详情
			SAMLtengxunyun		2021-12-31 11:27:13	⑥ 待审批	同意	拒绝 详情

3. 在弹出的对话框,单击确定,即可完成用户账号的审批。

4. 在账号审批页面,单击操作列下的**详情**,可以查看具体的应用账号申请信息。

同意	拒绝						请输入用户
	用户名称	账号名称	应用名称	账号组	申请时间	审批状态 ▼	操作
			OAUTH2		2021-12-31 17:30:45	❷ 已通过	详情
			OAUTH2		2021-12-31 17:30:34	① 已拒绝	详情
			JWT		2021-12-31 11:27:19	③ 待审批	同意 拒绝 详情
			SAMLtengxunyun		2021-12-31 11:27:13	() 待审批	同意拒绝详情



管理员管理

最近更新时间: 2022-12-06 16:27:30

本文将为您介绍如何在数字身份管控平台(员工版),新建、编辑、删除管理员等操作。

管理员权限说明

- 支持将用户设置为不同管理员角色和管理范围,如用户/组织机构管理员、应用管理员、权限管理员、审计管理员、注册审批管理员、账号审批管理员等角色。
- 同一个用户支持配置多个不同管理员角色。
- 同一个用户只能分配一个用户/组织机构管理员、应用管理员、权限管理员、审批管理员、审计管理员角色,即一个人一个角色类型只能建立一个。
- 设置后,不同管理员角色能够访问的菜单不同,如应用管理员,则仅能访问应用管理菜单。
- 不同管理角色的权限和管理范围具体如下图所示:

管理员角色	菜单查看权限	管理范围
超级管理员	全部	全部
用户/组织机构管理员	用户管理	 对指定的组织机构、用户组具备增删改查的管理权限管理员 具备对自己创建的资源(组织机构、用户组、用户)的能力
应用管理员	应用管理	 对指定的应用范围,具备增删改查的能力管理员 具备对自己创建的资源(应用)的管理能力
权限管理员	授权管理	对指定的组织机构、用户组和指定的应用具有授权和取消授权的能力
账号审批管理员	其它管理−审批管理−账 号审批	对指定的应用具有账号审批的能力
注册审批管理员	其它管理−审批管理−注 册审批	对指定的组织机构、用户组具有账号注册审批的能力
审计管理员	概览、审计管理	可审计全部范围内的操作日志

新建管理员

- 1. 登录 数字身份管控平台(员工版)控制台,在左侧导航栏,选择**其他管理 > 管理员管理**。
- 2. 在管理员管理页面,单击**新建管理员**,根据实际需求选择管理员类型。

营理员管理				功能使用说明
功能使用说明 1. 支持将用户设置为不同管理员角色和管理范围。如 2. 同一个用户支持数置多个不同管理员角色 3. 同一个用户和财务一个用户组织时期管理员,应 4. 设置后,不同管理员角色能够访问的第单不同。如	用小编码机构管理员,应用管理员,权限管理员,审计管理员,注册审批 用管理员,权限管理员,审批管理员,审计管理员角色,即一个人一个角柱 进用管理员,别仅能访问应用管理某单	普達氏 殊号审批管理员等角色 管理员权限投资 给供型只能建立一个		Ø 時間
新建管理员 👻 潮除			请输入用户名称/ID搜索	Q
新達用户/组织初构管理员 新建应用管理员	用户ID	管理员角色 ▼	操作	
新建权限管理员	4f1	☞ 应用管理员	编辑 删除	
新建注册审批管理员 新建张号审批管理员 邮建审计等符员			10 ▼ 釜/页	1 /1页 ト H

3. 在弹窗中,不同类型管理员,所需要配置的参数有所不同,具体如下所示:
○ 用户/组织机构管理员:选择用户、用户管理的组织机构、用户组和应用范围,单击确定保存。

分 腾讯云

选择用户 *	1000				
组织机构范围ㆍ	○ 全部组织机构 ○ 指定组织机构				
	请选择组织机构			已选择 (2)	
	请输入组织机构名称或代码	Q		组织机构名称	
	- 组织机构名称			根节点/A子公司	8
	✓ 根节点/A子公司				
	✓ 根节点/A子公司/产品部/产品一部			根节点/A子公司/产品部/产品一部	8
	根节点/A子公司/产品部		↔		
	根节点				
	根节点/用户组1				
	根节点/用户组1				
	#共占/∧Z/\∋)/治 生				

○ 应用管理员:选择用户、用户管理的应用范围,单击确定保存。

±z⊡ċ.	建进程田台		_		
≇用广•			*		
H)UQ *				已选择 (2)	
	请输入应用名称或应用ID	Q		应用名称/ID	
	■ 应用名称/ID S 7			S 7: 华 47	0
			\leftrightarrow		
	a				
	□ 腾 eC				
	华				



🔗 腾讯云

○ 权限管理员:选择用户、用户管理的组织机构、用户组和应用范围,单击确定保存。

疑用户★	请选择	▼	
识机构范围 •	○ 全部组织机构 🔹 指定组织机构		
□组范围★	○ 全部用户组 ○ 指定用户组		
	请选择用户组	已选择 (1)	
	请输入用户组名称或代码	Q, 用户组名称	
	用户组名称	⇒	8
	✓ ⇒		
	□ ±	\leftrightarrow	
	BR		

○ 注册审批管理员:选择用户、用户管理的组织机构和用户组范围,单击确定保存。

			נוניברי נין	A A LUNCE CAR	
选择用户 *	请选择用户		,	7	
l织机构范围★	○ 全部组织机构 ○ 指定组织机构				
	请选择组织机构			已选择 (0)	
	请输入组织机构名称或代码	Q		组织机构名称	
	组织机构名称				
	eiam根节点/I				
	eiam根节点/l				
	eiam根节点/l		\leftrightarrow		
	eiam根节点/				
	elam根节点/l				
	elam根节点/l				
	eiam超共占/A				



○ 账号审批管理员:选择用户、用户管理的应用范围,单击确定保存。

新增账号审批	管理员				>
 通过; 	没置账号审批管理员, 让该管理员具备对指定应用范围执行账号审排	比的权限	₹		
选择用户*	请选择用户		•		
应用范围★ ○	全部应用 🔘 指定应用				
选	择应用			已选择 (2)	
	请输入应用名称或应用ID	Q		应用名称/ID	
	一 应用名称/ID			SA	
	✓ 5 7		75	75	
				华: 47 区	
	✓ ⁴ / ₄	*	↦		
	8				
	a				
	<u>B</u>				
	e				
	1 1 2				
		_			
	确定		取消	ă	

○ 审计管理员:选择用户,单击确定保存。

新增审计管	管理员	×
① 通	<u>时设置审计管理员,让该管理员具备审计全部操作日志的权限</u>	
选择用户 🕇	请选择用户 ▼	
审计范围★	○ 全部范围 审计管理员可以审计全部范围内的操作日志	
	職定取消	

编辑管理员

新建管理员后,可修改用户管理的组织机构、用户组、应用范围。 1. 在 管理员管理页面,选择需要编辑的管理员,单击**编辑**。

新建	新建論電気 × 1000						
	用户名称	用户ID	管理员角色 ▼	操作			
			② 用户/组织机构管理员	编辑 删除			
			2. 权限管理员	编辑 删除			
	-		⑦ 审计管理员	编辑 删除			
			▶ 账号审批管理员	编辑 删除			
			☆ 应用管理员	编辑 删除			
			其册审批管理员	编辑 删除			



2. 在编辑管理员弹窗中,修改相关参数,单击确定保存。

 通过设置应用管理员,让该管理员具备对指定范围的应用进行 	增删改查的权限		
284 A.	-		
	· ·		
选择应用	已选择 (1)		
请输入应用名称或应用ID	Q, 应用名称	D	
■ 应用名称/ID	0		8
C f	f1		
	\leftrightarrow		
F			
00374e04-0020-408e-abes-old007.000 tse			

删除管理员

新建管理员后,如不再需要已新建的管理员,可删除单个管理员或批量删除管理员。

- 1. 在 管理员管理页面,支持删除单个或批量删除管理员,具体操作如下所示:
 - 单个:选择需要删除的管理员,单击操作列的**删除**,弹出确认删除弹窗。

新建管理员 副除			请输入用户名称ID搜索	Q
用户名称	用户ID	營理员角色 ▼	操作	
12	41	⋳ 应用管理员	编辑	

○ 批量:选中一个或多个需要删除的用户,单击删除,弹出确认删除弹窗。

6988 · 1998				講輸入用户名称の理察	Q
■ 用户名称	口refi的 D	管理员角色 Y	1013		
		⊗ 用 [→] /编码机构管理员	4040 ANIA		
		A 和田前田田	编辑 删除		
=		⊘ 新計管理员	1010 1010		

2. 在确认删除弹窗中,单击**删除**,即可删除所选账号组。

▲ 注意

- 批量删除会删除所选用户下的所有管理员角色。
- 删除后,相应数据将无法恢复,请谨慎操作。





企业微信同步

最近更新时间: 2022-12-06 16:13:37

操作场景

通过配置企业微信导入,可以把企业微信当中的用户信息导入到数字身份管控平台(员工版)(简称为:EIAM)。企业微信当中的账号对应 EIAM 的用户名,以姓名映射 为昵称,企业微信导入到 EIAM 的用户可以通过用户名密码登录到 用户门户端 。

操作步骤

1. 登录 数字身份管控平台(员工版)控制台,在左侧导航栏,单击**用户管理 > 组织机构管理**,并单击页面右上角处的**配置企业微信**,进入配置企业微信页面。

组织机构管理								配置LDAP/AD 配置企业微信
企业组织机构		根节点						
请输入组织机构名称或代码	Q,	新建用户 删除	批量导入 ▼					请输入用户名称/用户昵称/手机号 Q
口 恨节点		用户名称	用户昵称	组织机构路径	手机号码	邮箱地址	用户状态 🍸	款搭用进 操作

2. 在配置企业微信页面,单击**新建企业微信**,进入新建企业微信配置页面。

数字身份管控平台 (员 工版)	← 配置企业微信
ぷ 用户管理 へ	 通过企业微信配置可以将组织机构/用户信息导入到本半台,
• 组织机构管理	新建企业微信配置
• 用户组管理	

3. 在新建企业微信配置页面,根据页面提示设置相关参数,单击确定,将企业微信导入 EIAM。

配置名称	请输入配置名称
	请输入配置名称
CorpID	请输入企业D
	可前往企业微信管理后台->我的企业获取企业ID
通讯录Secret	请编入通讯员secret
	可前往企业微信管理后台->管理工具->遭讯录同步开启API 接口同步后获取Secret
CallbackURL	https://calli
	可前往企业微信管理后台->管理工具->通讯录同步->已设置接收事件服务器(编辑)->URL设置该回调地址
Token	FX
	可前往企业微信管理后台->管理工具->通讯录同步->已设置接收事件服务器(编辑)->Token设置该token
EncodingAESKey	zA. To
	可前往企业微信管理后台->管理工具->通讯录同步->已设置接收事件服务器(编辑)->EncodingAESKey设置该EncodingAESKey
导入本系统默认密码	· 请输入密码
状态	
状态 开启自动同步到本系统	
状态 开启自动同步到本系统 开启自动同步到企业微.	
状态 开启自动同步到本系统 开启自动同步到企业微。 所属节点	
状态 开启自动同步到本系统 开启自动同步到企业微 所履节点	 → →

- 配置名称:数据源配置名,唯一。
- CorpID:企业微信 ID,可前往企业微信管理后台 >我的企业页面,在企业信息中获取企业 ID。



● 通讯录 Secret:企业微信当中的通讯录 Secret。可前往企业微信管理后台 > 管理工具 > 通讯录同步页面,开启 API 接口同步后,单击查看获取 Secret。

首	页	通讯录	应用管理	客户联系	管理工具	我的企业
<>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>			通讯	录同步		
	٤	通讯录同步 ^{可通过API接口或第三方,}	立用同步通讯录			
	同步方式	API接□				
	权限	API编辑通讯录(已开启 除通过API编辑通讯录,智	手动编辑) 編辑 1理员可同时手动编辑通讯录,成の	员也可在客户满修改字段。 查看成	员可修改字段	
	Secret	查看 重新获取				
	已设置接收	事件服务器 编辑				
	关闭API接[口同步				

- CallbackURL、Token、EncodingAESKey:
- 3.1 开启自动同步到本系统后,需要将配置企业微信页面生成的3个链接,复制到企业微信管理后台 > 管理工具 > 设置接收事件服务器页面。

CallbackURL	https://) 🖬	
	可前往企业微信管理后台->管理工具->通讯录同步->已设置接收事件服务器(编辑)->URL设置该回调地址		
Token	6		
	可前往企业微信管理后台->管理工具->通讯录同步->已设置接收事件服务器(编辑)->Token设置该token		
EncodingAESKey	ZAJ ♪ Tī		
	可前往企业微信管理后台->管理工具->通讯录同步->已设置接收事件服务器(编辑)->EncodingAESKey设置该EncodingAESKey		
* 导入本系统默认密码	请输入密码		Ø
状态			
开启自动同步到本系统			

3.2 单击保存,完成企业微信回调地址配置;配置完成后企业微信修改、新增、删除用户和组织机构时会自动同步到 EIAM。

○,企业微信					服务商后台	API文档	联系客服 退
首页	通讯录	应用管理	客户联系	管理工具		我的	企业
《返回		设置接收	事件服务器				
	URL @ 获 https://c Token N EncodingAEI D3u	取帮助 SKey 取消	· · · · · · · · · · · · · · · · · · ·	1 随机获取 随机获取			

- 导入本系统默认密码:企业微信当中的用户导入 EIAM 时,默认的密码。
- 所属节点:企业微信当中的组织机构导入到 EIAM 的指定节点下。
- 状态:整个配置是否开启,当状态未关闭时,开启自动同步到本系统和开启自动同步到企业微信无论是否开启都无效。
- 开启自动同步到本系统:开启时,在 EIAM 导入的所属节点下的新增、修改、删除用户或组织机构等操作,会自动同步到企业微信。
- 开启自动同步到企业微信:开启时,企业微信的新增、修改、删除用户或组织机构等操作,会自动同步到 EIAM。



API 认证与鉴权

概述

最近更新时间: 2022-12-06 16:15:25

- 数字身份管控平台(员工版)(以下简称为 EIAM)用于管理企业内员工的账号、权限、身份认证规则、应用访问控制规则。
- 支持对用户身份的集中管理、用户认证、应用集成、SSO、授权管理、审计管理等能力;
- 支持 SAML、CAS、JWT、OIDC、OAuth2.0 等多种协议;
- 支持多种基于角色的访问控制(RBAC)模型。

采用 EIAM 为API 网关提供认证和鉴权能力,可以为 API 调用提供更为安全和简便的方式。

功能优势

通过 EIAM 为 API 网关提供防护的能力,具有以下优势:

- 使用标准 OAuth2.0 协议;
- 可一键创建授权 API 和业务 API, 轻配置;
- EIAM 维护用户目录,免自建认证服务器;
- 在认证能力基础上支持鉴权功能,保护 API 安全;
- EIAM 内置多种 RBAC 模型,免自建鉴权服务器和授权模型;
- 内置缓存机制,更快的访问速度。

操作步骤

通过 EIAM 为 API 网关提供防护能力需进行以下操作:

- 步骤1: 创建服务
- 步骤2: 创建 API
- 步骤3: 创建 API 网关应用 (可选)
- 步骤4:资源级授权(可选)
- 步骤5:调用 API



步骤1: 创建服务

最近更新时间: 2022-12-06 16:16:57

前提条件

已经开通腾讯云 API 网关服务 和 数字身份管控平台(员工版)服务。

操作步骤

1. 登录 API 网关控制台,在左侧导航栏中,单击 服务 > 基本信息,进入服务基本信息页面。

	API 网关	HOT Se	erverless Wordpre	ss 动态	网站建站	新体验, 毎月	月免费赠送	鍵站所需资	额和代金券,	立即体验 >> (查看	活动规则)	
	器 概 览	服务	⑤广州(40) ▼									
	♀ 实例	基本信	息数据统	sit								
	开放 API			Û	用户之	声: 欢迎您想	較API网	关产品的功能	能/体验/文档等	\$65面的需求和建议。	期待您的声音!	点击提3
	● 服务			Ŭ								
	弐 插件			新建		导入 API	Ş	出 API	删除			
2. 7	在服务基本信息页面,单击 新建 ,	弹出新建制	服务弹窗。									

3. 在新建服务弹窗中,根据页面提示填写或选择所需内容。

① 说明	
● 前端类型:建议为"HTTP"或"HTTPS";	
● 访问方式:固定为"公网";	
• 其他项根据实际填写或选择即可。	



新建服务		×
() E	目前IPv6功能正在广州、上海地域内测,您可以提交 <u>测试申</u> 遣 🗹	
所属地域	广州	
服务名		
前端类型	HTTP&HTTPS HTTP HTTPS	
计费模式	按量计费	
访问方式	□ 内网VPC □ 公网 当选择内网VPC时,所生成的内网VPC域名可在与服务同地域的VPC网络内	
实例	访问 共享型 专享型 专享实例底层资源独享,可提供超高性能和SLA保证, 立即选购 [2	
标签	标签键 ▼ 标签值 ▼ X	
备注	+ 添加 请输入备注	
费用	调用费: (按阶梯计费) 流量费:	
	提交关闭	

4. 单击**提交**,即可完成服务创建。



步骤2: 创建 API

最近更新时间: 2022-12-06 16:16:49

前提条件

已经开通腾讯云 API 网关服务 和 数字身份管控平台(员工版)服务。

操作步骤

1. 登录 API 网关控制台,在左侧导航栏中,单击 服务 > 基本信息,进入服务基本信息页面。

API 网关	HOT Serverless Wordpress 动态网站建站新体验,每月免费赠送建站所需资源和代金券,立即体验 >> (查看活动规则)
器 概 览	服务 ⑤ 广州(40) ▼
♀ 实例	
开放 API	() 用户之声: 欢迎您提交API网关产品的功能/体验/文档等方面的需求和建议,期待您的声音! 点击
② 服务	
弐 插件	新建 导入 API 导出 API 删除

2. 在服务基本信息页面,选择之前所创建的服务,单击"服务名",进入该服务的 API 管理界面。

服务。广州	T							○ API网关用户交流群	3月 扫码关注公众号	专享实例专家	分享 🗹 🗄
基本信息数据	充计										
	 用户之声: 欢迎您提交A 	API网关产品的功能/体验	2/文档等方	面的需求和建议,期待您的;	声音! <u>点击提交</u> 12						
	新建 导入 API	导出 API	UR\$				请选择您要进行	冠海的标签		Q	φ φ
	服务名	服务状态	监控	网络类型	已发布环境	实例	标签	创建时间	备注	操作	
		⊘ 运行中	di	公网	发布	共享型		2021-07-28 17:41:24		发布编辑	置管理
		⊘ 运行中	di	公网	发布	共享型		2021-07-28 16:20:57		发布编辑	遭管理

3. 在 API 管理界面,单击新建,进入新建 API 页面。

(1000												
管理API	基础配置	使用计划	自定义域名	服务日志	监控信息	数据统计	策略配置	发布管理					
		通用API (1) 🤅	〕 微服务AF	이 ()									
		新建	导入 API 措	制除复制	Ð							多个过滤标签用回车键分	Q Ø
		ID/名称		监控	路径				方法	标签	创建时间	操作	
				di	T				ANY		2021-07-28 17:4	1:27 编辑 导出 配置管	理 更多 ▼

4. 在新建 API 页面,根据页面提示配置所需内容。

4.1 前端配置:根据页面提示填写或选择所需内容,单击下一步。

① 说明
● 前端类型:建议为"HTTP"或"HTTPS"。
● 鉴权类型:请选择"EIAM 认证"。
◎ 接入方式:
○ 如选择"新建 EIAM 应用",会在 EIAM 侧同步创建"云 API 网关"类型的应用。
○ 如选择"选择已有 EIAM 应用",下方会出现"选择 EIAM 应用"下拉选择框,需在下拉选择框中选择指定的应用。
◎ 认证与鉴权:
○ 如选"只认证不鉴权",则 API 调用时不检验 API 调用权限。
○ 如选" <mark>既认证又鉴权</mark> ",则 API 调用时需检验 API 调用权限。
● EIAM 应用类型:
● 如选择"非 Web 客户端",则同步创建对应的"授权 API"。



- 如选择"Web 客户端",则通过 Web 客户端首次访问该 API 时,会自动重定向到 EIAM 进行身份认证。
- Token 有效期,id_token 的有效时间,单位为秒,默认为600,最小值为10,最大值为86400。
- 其他项根据实际填写或选择即可。

> 腾讯云

4.2 后端配置:选择合适的后端类型后,填写相关信息,单击**下一步**。

	公 网 URI 后端服务)	L/IP 通过公网对外闭	干放	VPC内资源 通过内网CLB 容器资源	对接VPC内主机	云。	函数SCF R云提供的无服务器计算服务	Mock 模拟响应数据以便测试	事件总线 EventBridge API网关作为事件集入口	
域名(http:// 👻									
	http或https开 共享实例只到	干头,包含don 支持填写公网站	nain内容,格 或名,不支持	试结尾无需"/" 埴写内网域名;	专享实例支持填	写公网域名和	和实例所属VPC下的内网IP			
路径(1)										
	1、支持"/"开 2、前端参数 3、Path类型	手头,大小写字 (中的"="与"^~' 题的请求参数必	母、数字、利 为前端路径料 须以{}包裹,	'Q\$+!*'(),/%等(青确度匹配符,局 作为独立部分包	符合URL规则的符 5端路径不继承 1含在路径中(示	符号 例: /{parar	m}/)			
求方法	GET	POST	PUT	DELETE	HEAD	ANY				
	15		秒							
满超时()										
满超时①	时间范围: 1	1-1800秒								
歯超时 ④ 量参数	时间范围: 1	1-1800₱少		参数位	置 ()		参数值	备注		
≒超时 ③ 量参数	时间范围: 1 参数名 新増常量。	▶数(0/30)		参数位	置 ()		参数值	备注		

5. 发布服务:无需填写响应结果内容,单击**完成**,选择发布环境和输入备注信息,单击发布服务或稍后自行发布。

()服务	↓ 服务发布后,API配置方能生效									
发布环境	✔ 发布 🕢 预发布	测试								
备注	\$									
	发布服务	稍后自行发布								



步骤3: 创建 API 网关应用(可选)

最近更新时间: 2022-12-06 16:16:38

背景信息

创建 API 时,如选择"选择已有 EIAM 应用",则需要数字身份管控平台(员工版)创建"云 API 网关"类型的应用,才能在下拉选择框中选择应用。

前提条件

已经开通腾讯云 API 网关服务 和 数字身份管控平台(员工版)服务。

操作步骤

- 1. 登录 数字身份管控平台(员工版)控制台,在左侧导航栏中,单击**应用管理**,进入应用管理页面。
- 2. 在应用管理页面,单击新建应用,进入新建应用页面,选择"云 API 网关",单击下一步。

÷	新建应用
	1 选择应用协议模板 > ② 集组应用信息 > ③ 完成
	29 JWT JWT (JSON Web Token) 是在网络应用环境声明的一种器子JSON的开放标准。本系统使用JWT进行分布式站击的单点整要(SSO),JWT 单点整要器子非对称加密,由本系统 将用户状态和信息使用机停加密。传递检应用后,应用使用公明解率并进行检证、使用场看非常 广泛、集成演单。
	OAuth2 OAuth2是一个开放的资源接权协议,应用可以通过OAuth2获取到今禅access_token,并携带今禅来服务装谱求用户资源,应用可以使用OAuth2应用模板来实现统一身份管理。
	CAS (存准) CAS (Central Authentication Service,集中式认证服务,版本 2.0) 是一种基于挑战。应管的开源单点登录协议。在集成客户随和服务施之间网络遗畅的情况下广泛在企业中使用,有集成流便,扩展性强的优点。
	OIDC OIDC (OpenID Connect, OIDC=(Identity, Authentication) + OAuth2.0。它在OAuth2上物達了一个身份层,是一个基于OAuth2协议的身份认证标准协议。在OAuth2基础上提供了ID Token未解决第三方案户牌标识用户身份认证的问题。
	あな代類 表現代項の以機以用や在登表気輸入用や各和密码、再通过表準備交釣一份登录方式。应用的称号密码在本系统中使用AES256加密算法本地加密存储。很多旧系统、不支持标准认证协议的系统或不支持改造的系统可以使用表単代填实现统一身份管理。表単中有面片验证码、 CSRF loken、 动态参数的场景不适用。
	RPI 采用GAuth2+JWT方式,对云API网关接入应用进行鉴权,为云API党得提供安全保健。
	FADIUS 联合radus-server力网络访问服务器(NAS)提供统一身份认证解决方案。实现以统一身份登录VPN、连接Wi-FI等功能。
	SAML SAML (Security Assertion Markup Language, 安全新音标记语言, 版本 2.0) 基于 XML 协议,使用包含新言 (Assertion) 的安全令牌, 在接权方 (本系统) 和谐器方 (应用) 之间传递身份信息, 实现基于网络跨域的单点登录, SAML协议最成熟的认证协议, 在国内外的公 有云何政务云中有非常广泛的运用,
h	下

3. 在应用管理页面,根据页面提示,一次上传应用图标、输入应用名称、Access_token 有效期,单击保存。

💛 选择应用协议模构	仮 〉 2 編辑应用信息 〉 3 完成	
* 应用图标	文件大小: 445K 上传日期: - 重新上传 删除	Ø
* 应用名称	请上传png或jpg文件,图片大小不超过1MB	
★ Access_token有效期	← 600 + 秒 Access_token的有效时长(单位:秒),默认为600(10分钟)。	
上一步取消	保存	

4. 在应用管理页面,单击完成,即可创建 API 网关应用。

步骤4:资源级授权(可选)

最近更新时间: 2022-12-06 16:17:56

背景信息

创建API时,如选择"既认证又鉴权",则需要数字身份管控平台(员工版)对 API 进行授权。

前提条件

已经开通腾讯云 API 网关服务 和 数字身份管控平台(员工版)服务。

操作步骤

- 1. 登录 数字身份管控平台(员工版)控制台,在左侧导航栏中,单击 **授权管理 > 资源级授权 > 组织机构授权**,进入组织机构授权页面。
 - 🕛 说明
 - 可根据实际需求,按"组织机构"、"用户组"、"用户"三种维度进行 API 授权。
 - 本文以"组织机构"维度为例,如需从"用户组"或"用户"维度进行 API 授权,可单击**用户组授权**或**用户授权**切换至相应页面,进行以下操作即可。
- 2. 在组织机构授权页面,在资源级授权下拉框中选择所需应用。
- 3. 在组织机构授权页面,单击**新增授权**,进入新增授权页面。

资源级授权		· (j
组织机构授权	用户组授权	用户授权
 資源级授 	又为用户提供细粒度权阿	艮管理能力,支持用户为应用定义的服务、接口等资源进行授权。
新增授权	取消授权	

4. 在新增授权页面,选择区域和 API 接口后,单击下一步:选择组织机构。

1 选择	3 选择服务/API > ② 选择组织机构 > ③ 完成										
应用											
区域	-										
API接口	请选择资源				已选择 (1)						
	请输入资源名称或ID			Q,	资源ID	资源名称	描述				
	✓ 资源ID	资源名称	描述			1		0			
		1									
				\leftrightarrow							
上一步	下一步:选择组织机构取消										



5. 在新增授权页面,请选择组织机构后,单击**下一步:完成**。

✓ 选择服务(API > 2 选择组织机构 > 3 完成											
请选择组织机构		已选择 (1)									
唐辅入组织机构名称或代码		Q 组织机构名称	组织机构代码								
✔ 组织机构名称	组织机构代码			0							
	-										
		**									
上 一步 下一步:完成 取消											

6. 在新增授权页面,单击**完成**,即可授权添加成功。



步骤5:调用 API

最近更新时间: 2023-12-28 11:36:22

前提条件

已经开通腾讯云 API 网关服务 和 数字身份管控平台(员工版)服务。

操作步骤

Web 客户端调用 API

- 1. 登录 API 网关控制台,在左侧导航栏中,单击**服务 > 基本信息**,进入服务基本信息页面。
- 2. 在服务基本信息页面,选择之前所创建的服务,单击"服务名",进入该服务的 API 管理界面。

	•							○ API网关用户交流群	3月 扫码关注公众号	专享实例专家	分享 🖸 🗄
基本信息数据	统计										
	 ・ 用户之声: 欢迎您提交A 	PI网关产品的功能/体验	/文档等方	面的需求和建议,期待您的;	声音! <u>点击提交</u> 🖸						
	新建 导入 API	导出 API #	97 0				请选择您要进行	記述簿的标签		Q	¢φ
	服务名	服务状态	监控	网络类型	已发布环境	实例	标签	创建时间	备注	操作	
		⊘ 运行中	di.	公网	发布	共享型		2021-07-28 17:41:24		发布 编辑 【	證管理
		⊘ 运行中	di	公网	发布	共享型		2021-07-28 16:20:57		发布编辑	超管理

3. 在 API 管理界面,选择所需的ID,单击"ID/名称",进入该 ID 的基本信息页面。

÷													
管理API	基础配置	使用计划	自定义域名	服务日志	监控信息	数据统计	策略配置	发布管理					
		通用API (3) (i) 微服务AP	1 (0) 🚯									
		新建 导入 API 删除 复制到			ĒIJ							多个过滤标签用回车键分 Q 🗘	
		ID/名称		监控	路径				方法	标签	创建时间	操作	
				di	1.0				POST		2021-08-11 11:1	6:59 编辑 导出 配置管理	昰 更多 ▼

4. 在基本信息页面,取 API 访问地址,如下:

← 基本信息 基础配	置 插件管理		
	基本信息	日志监控调试编辑	默认访问地址
	路径 方法 Apild 创建时间 2021-08-11 11:16:59		公司成名 http:// https:///////////////////////////////////
	韵靖配置 前满方法 HTTP		您可按照"协议"/公园城名或内网VPC城名已发布环境协同播栏的推式用提API的默认访问地址 访问内内VPC城名构造的地址封必规模有满口号,否则将访问不通



5. 通过浏览器发起访问 API,自动跳转到 EIAM 认证门户登录页面输入账号和密码,单击登录,成功登录后会返回 API 输出信息。

	密码登录	
账号	2	\odot
密码	A]⊘
	登 录	
← →	C servi	ork ork
web wo	rk	

非 Web 客户端调用 API

- 1. 登录 API 网关控制台,在左侧导航栏中,单击**服务 > 基本信息**,进入服务基本信息页面。
- 2. 在服务基本信息页面,选择之前所创建的服务,单击"服务名",进入该服务的 API 管理界面。

服务。广州	T							API网关用户交流群	3月 扫码关注公众号	专享实例专家	分享 🛛 🗄
基本信息数据	充计										
	 用户之声: 欢迎您提交A 	PI网关产品的功能/体验	》文档等方	面的需求和建议,期待您的)	書音! <u>点击提交</u> 12						
	新建 导入 API	导出 API		请选择您要进行过考的标签			Q	¢¢.			
	服务名	服务状态	监控	网络类型	已发布环境	实例	标签	创建时间	备注	操作	
	□		di.	公网	发布	共享型		2021-07-28 17:41:24		发布编辑配置管理	
		⊘ 运行中	di	公网	发布	共享型		2021-07-28 16:20:57		发布编辑	置管理

3. 在 API 管理界面,选择所需的ID,单击"ID/名称",进入该 ID 的基本信息页面。

÷														
管理API	基础配置	使用计划	自定义域名	服务日志	监控信息	数据统计	策略配置	发布管理						
	通用API (3) ① 微服务API (0) ①													
		新建 导入 API 删除 复制到			N							多个过滤标签用回车键分 Q 🗘		
		ID/名称		监控	路径				方法	标签	创建时间	操作		
				di					POST		2021-08-11 11:16;	59 编辑 导出 配置管理	理 更多 ▼	



4. 在基本信息页面,取 API 访问地址,如下:

← ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■ ■							
	基本信息	日志 监控 调试 编辑	默认访问地址				
	路径 方法 Apild		公网络名 http://https: 已发布环境 访问路径				
	 ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・		请求方法 POST 您可按照"协议"心例域名或内网VPC域名/已发布环境/5时路径"的格式拼接API的默认访问地址 说问内网VPC域名构造的地址封必须携带施口号,否则将访问不遵				

5. 通过后端程序、postman 等方式,携带 username、password 参数发起访问授权 API,获取返回的 JWT 格式的 id_token,如下:

POST ▼ → http://servis		password# , `	Send •	Save	¥
Parames Authorization Headers (7) Body Pre-request Script Tests Settings Cookes Query Parames					
KEY	VALUE	DESCRIPTION		Bul	(Ed)
≡ √ username					
password					
Key	Value	Description			
Body Cookies Headers (10) Test Results Save Response Body Save Response Save Response Save Response Save Response					
Pretty Raw Preview Visualize Text * 🛱					
1 eyJhbGci0iJSUZIINiIsIm eyJqdC Qi0iJz OVISIC	rp2C161	MURIE AND CONTRACTORS		XRycr	dW
Jya96c @IxdXI				18MDhe	hD

6. 通过后端程序、postman 等方式,在 HTTP 头部 Authorization 域携带 id_token 参数,以及其他业务参数,访问业务API,如下:

GET • http://service-30etw6/m-1/Lencentcs.com/80/none_web_wark					
Params Authorization Headers (7) Body Pre-request Script Tests Settings					
Hea	nders 🐵 6 hidden				
	KEY	VALUE	DESCRIPTION *** Buik Edit Presets ¥		
~	Authorization	Bearer id_token="ey hbGciOiJSU ZFMkQzNkY2QUQ1In0.ey qdGkiOiJ			
	Key	Value	Description		
Body	Cookies Headers (11) Test Results		Status: 200 OK Time: 75 ms Size: 397 B Save Response •		
Pr	etty Raw Preview Visualize	JSON 👻 🚍	🖷 Q.		
	1 none_web_work 2				