



应用身份服务 统一认证

文档版本: 20210802



法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。 如果您阅读或使用本文档,您的阅读或使用行为将被视为对本声明全部内容的认可。

- 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档,且仅能用 于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息,您应当严格 遵守保密义务;未经阿里云事先书面同意,您不得向任何第三方披露本手册内容或 提供给任何第三方使用。
- 未经阿里云事先书面许可,任何单位、公司或个人不得擅自摘抄、翻译、复制本文 档内容的部分或全部,不得以任何方式或途径进行传播和宣传。
- 由于产品版本升级、调整或其他原因,本文档内容有可能变更。阿里云保留在没有 任何通知或者提示下对本文档的内容进行修改的权利,并在阿里云授权通道中不时 发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠 道下载、获取最新版的用户文档。
- 4. 本文档仅作为用户使用阿里云产品及服务的参考性指引,阿里云以产品及服务的"现状"、"有缺陷"和"当前功能"的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引,但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的,阿里云不承担任何法律责任。在任何情况下,阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害,包括用户使用或信赖本文档而遭受的利润损失,承担责任(即使阿里云已被告知该等损失的可能性)。
- 5. 阿里云网站上所有内容,包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计,均由阿里云和/或其关联公司依法拥有其知识产权,包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意,任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外,未经阿里云事先书面同意,任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称(包括但不限于单独为或以组合形式包含"阿里云"、"Aliyun"、"万网"等阿里云和/或其关联公司品牌,上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司)。
- 6. 如若发现本文档存在任何错误,请与阿里云取得直接联系。

通用约定

格式	说明	样例
⚠ 危险	该类警示信息将导致系统重大变更甚至故 障,或者导致人身伤害等结果。	⚠ 危险 重置操作将丢失用户配置数据。
⚠ 警告	该类警示信息可能会导致系统重大变更甚 至故障,或者导致人身伤害等结果。	警告 重启操作将导致业务中断,恢复业务 时间约十分钟。
〔〕) 注意	用于警示信息、补充说明等,是用户必须 了解的内容。	大意 权重设置为0,该服务器不会再接受新 请求。
? 说明	用于补充说明、最佳实践、窍门等,不是 用户必须了解的内容。	⑦ 说明您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击设置> 网络> 设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在 结果确认 页面,单击 确定 。
Courier字体	命令或代码。	执行 cd /d C:/window 命令,进入 Windows系统文件夹。
斜体	表示参数、变量。	bae log listinstanceid
[] 或者 [alb]	表示可选项,至多选择一个。	ipconfig [-all -t]
{} 或者 {a b}	表示必选项,至多选择一个。	switch {act ive st and}

目录

1.第三方认证源接入	05
1.1. 微信扫码登录	05
1.2. 支付宝扫码登录	10
1.3. LDAP认证登录	19
1.4. 钉钉扫码登录	27
1.5. 钉钉微应用单点登录	37
1.6. 短信OTP认证登录	46
1.7. 企业微信扫码登录	49
2.移动端扫码登录IDaaS平台	56
3.二次认证	63
4.实人认证	68
5.人脸识别	72
6.添加Radius配置	78

1. 第三方认证源接入

1.1. 微信扫码登录

本文为您介绍如何通过IDaaS认证源管控功能,帮您实现微信扫码登录功能。

背景信息

某些公司将微信作为团队日常办公工具,为了方便使用微信进行扫码登录,现采用微信开放平台扫码登录认 证源来实现该功能。

操作步骤

- 1. 登录微信开放平台
- 2. 点击"创建网站应用"按钮,进行网站应用创建时,授权回调域填写部署的IDaaS地址(需要外网域 名),注意保留申请到的微信开放平台的App key和App Secret。

🏫 微信・开放	牧平台	首页	资源中心	管理中心	数据中心	帐号中心
移动应用 网站应	ī用 公众帧	号/小程序	第三方平台			
创建网站应用	还可创建8~	个网站应用				
应用名称					状态	

备注:(微信回调域默认使用80端口, 需外网域名)

3. IT管理员登录后,依次进行认证、添加认证源、添加微信开放平台扫码登录等操作。

配置属性	配置说明
认证源名称	自定义认证源显示名称
Appld	用户在微信开放平台申请的Appld
AppSecret	用户在微信开放平台申请的AppSecret
授权回调域	由IDP生成,只读不可修改。(用户在微信开放平台设 置的回调域必须完全按照该值填写)

4. 微信扫码登录配置确认保存之后, 启用该认证源。

统一认证·第三方认证源接入

概览 快速入门 应用	^	认证源 ↓证源 ↓ 本平台支持企业使用不同的分	*部认证渡(即允许使用第二方认证方式		使用不同的认证方式。如 DB、LDAF	 (11)扫码等。 	250mfTfTSAid200	istanik lieny X
应用列表 添加应用 账户 机构及组	^	自用认证源后并配置完成后, 投余认证源	平台会允许企业用户登录时使用具体的	3从证源去认证 , Q				
账户管理		认证源名称	认证源 ID	自定义登录	创建时间	状态	操作	
分类管理		短信验证码登录-wl	20200313110953GDMJ2Dy8pesms 2	是	2020-03-20 16:35		详情日志删除	
认证牌		短信验证码登录	20200313110953GDMJ2Dy8pesms 1	是	2020-03-20 15:11	\sim	详情日志删除	
认证源 / 添加	认证源							
← 添加认	证源							
请输入认证源名和				Q				
图标	认证源名	S称	标识		描述			操作
支	支付宝玺	52	alipay		使用支付宝	양국	3	添加认证源
>	钉钉微应	如用登录	ddtalk_micro		使用钉钉微	应用登录	3	泰加认证源
	微信开放	女平台扫码登录	wechat		通过微信开	放平台实现扫码登录	ž	添加认证源
>	钉钉扫码	马登录	ddtalk		使用钉钉扫	周登录	3	家加认证源
LDAP	LDAP		ldap		使用LDAP(!	(IAD城)进行认证	3	翻认证源

* 认证源ID	wceshiwechat6						
	认证源id,由系统生成						
* 认证源名称	微信-draven						
* Appld							
	微信扫码登录开发申请逐	读取的Appld					
* AppSecret							
	微信扫码登录开发申请逐	茨取的AppSecret					
* 微信授权域	idp4.idsmanager.com	idp4.idsmanager.com					
	似信扫的豆 求开及中第1	又直的椒箔投仪墩					
* 前端回调地址	https://idp4.idsmanage	er.com/#wechatCa	allBack				
	IDass服务认业后重定问 示例: http://xxx.xxx.com	I到前頭話的地址, 必 m/#ddtalkCallback	〉须已http或http	DS开头,不能为闪网地址。			
是否显示							
	是否在登录页显示						
	提交取消						
14.11E384				YANIHEJEJAALEJK YANIHALEJK			
↓证源 本平台支持企业使用不同的外部认证簿 启用认证源后并配置充成后,平台会允许	即允许使用第三方认证方式登录账户),可根据公司需要派 企业用户登录时使用具体的认证原去认证。	加并使用不同的认证方式,如 DB、LDAP	、钉钉扫码等。	×			
搜索认证源		Q					
认证源名称 认证源 ID	自定义登录	创建时间	状态	操作			
微信开放平台扫码登录 20200313 hat	110953GDMJ2Dy8pewec 是	2020-04-01 14:55		修改详情。日志删除			

5. 普通用户在登录页,点击微信开放平台认证源

[-]阿	
阿里云IDaaS	服务
draven	
•••••	
请输入验证码	TRUN
	忘记密码
提交	
注册	
第三方认证登	₹

使用移动端微信扫描二维码,并在移动端点击授权登录。



如果用户的微信之前没有绑定过IDaaS的账户,则会弹出一个账户绑定的页面,需要用户在页面上输入 IDaaS的账号密码进行绑定。

绑定成功后,即可登录到IDaaS平台,之后使用微信开放平台扫码登录无需再次绑定。

云盾账户绑定	
请输入IDaaS账户	
请输入密码	
提交	
没有账号? 点击注册	

如果用户希望解除微信与IDaaS的账户绑定关系。在用户登录后,点击 **我的账户 > 三方账户**,选择认 证源点击解除绑定即可。

欢迎・IDaaS		我的账户			
主导航へ		账户安全	个人信息	我的证书	三方账户
首页	ſ				
应用管理		公司已开启并	且用户已绑定的	认证源, 用户可	「在此进行解绑操作。
应用子账户					
设置 ^		-	<u> </u>		
我的账户			-		
二次认证		47 P			
我的消息		用牛肉	ROPAE		
我的日志					

1.2. 支付宝扫码登录

本文为您介绍如何通过IDaaS认证源功能,帮您实现使用支付宝扫码登录IDaaS的功能。

一、支付宝开放平台创建应用

操作步骤

- 1. 登录支付宝开放平台
- 2. 点击进入开发者中心

← → C () open.alipay.com/platform/manageHome.htm		x) 🖯 🕻
🔡 应用 😗 Free IDP Trial - Fr 📒 阿里云 📒 GITLAB 集成单点 📙 新建文件夹		
这 烈旗 开放平台 首页 业务中心 运营中心 开发者中心 账户中心		\$▶2 - 昆2 ⑦ 冬 186*****97[主账号]
战疫情小程序专项现金扶持政策请尽快签约"我要阅读"		
常用功能 边蒙管理 服务订单 账单管理 阿贝A标动应用列表 已经取能力 十 添加功能		13码入群,随时咨询并获取平台业务通知 在我想问题。
您的业务进程 1-应用开发 2-商户拓展 3-业务管理	待办 更多	当前登录: 186*****97[主账号]
 · (南户拓展通过服务市场拓展南户 · (南户拓展)城下拓展,完成南户签约并获得按权 	2个得办任务 【中选编词】备份文件检测… 【中选编词】备份文件检测… 	金 電査 信息未完善 (系統服务向SV)(目研开发者) 〇
业务经营数据	更多	平台公告 更多
交易金额(元) 交易笔数 	动锅商户数 _	战疫情小程序专项现金扶持政策请
日环比-周环比-周环比-	日环比-周环比-	关于疫情期间支付积分有效期延长 new 02/12
		支付宝 IoT 小程序暫停軍核延长 new 02/21 商家风险管理功能上线 new 02/24
ps://openhome.alipay.com/platform/developerIndex.htm		

3. 点击创建应用,选择网页&移动应用标签下的自定义接入

支 熱陰 开发者中心	首页	能力管理	技术支持			Q	⊈ 》2	2	0	(8) 186****	**97[主账 [;]	号]
战疫情小程序专项现金扶持政策请尽	快签约 "查看	计详情"										
我的应用					+ 创建应用	公告					更多〉	
生活号 网页&移动机	应用 🗍	第三方应用			生活号	战疫情小程序	专项现金	扶持政策请	尽快签约	new	02/12	
					网页&移动应用 >	支付接入	吉算服:	务推迟的公	告new		02/13	
					第三方应用 >	自定义接入	「积分	有效期延长	的公告	w	02/12	
						商业消费	茅暂停	审核延长	ew		02/21	_
						i 交通出行	能上线	new			02/24	② 立
			你还没有生活号哦,快来创建吧!			政务民生						即咨
			立即创建			医疗教育	小限	序数据统计	十正式上线	线		询
						支付	宝官方推荐	荐第三方数据	服务平台			
						M	M	战疫	情!			

4. 配置应用的基本信息

 默认新建自运营应用,第三方应用请到第三方应用页面创建 		
	* 应用名称:	不超过32个字符, 查看会会规范
	* 应用图标:	 ・ 「海際 ・ 「「「「「「」」」 ・ 「「」」 ・ 「「」」 ・ 「「」」 ・ 「「」」 ・ 「「」」 ・ 「「」」 ・ 「「」」 ・ 「「」」 ・ 「「」」 ・ ・ ・
	应用类型:	● 网页应用 ○ 移动应用
	网址url:	₩: https://www.example.com/main部Bhttp://www.example.com/main
	应用简介:	
		The second se

5. 为应用添加 获取会员信息的能力

○A 测试OA扫码 ● 开发中	应用类型: 网页应用					
(APPID) 20210	网址url: 暫无					
₩ 概览	应用简介: 智无					
	能力列表					2
	+ 添加能力 總已經添加0项功能					Ŧ
	山能名称	功能介绍	是否需要商户签约	状态	操作	
		● 智元	功能,快去添加吧			
	工会の審					

ì	添加功能						\otimes
1	1. 请谨慎选择 2. 扫码关注前 3. 部分功能存	译需要的功能,过多的功能会 首页右上角二维码"支付宝开 王使用时需要满足准入条件,	影响应用上线审核通过率,以 放平台"及时获取新能力。 请在"文档中心"查看对应的	及使用者的使用门槛 产品说明。	获取		Q
	会员	其他					
		功能名称	描述	行业资质	是否需要商户 签约	操作	*
		获取会员信息 免费 不限	经用户授权,获取用户 个人信息	否	Ϋ́	详细文档	*
	确定	取消					

6. 设置接口加签方式

\leftarrow \rightarrow C $($ openhome.a	alipay.com/platform/appMan	age.htm?#/app/20	21001135670762/overview					প 🖈 🖯 🖸
🔛 应用 🛛 G Free IDP Trial - Fr	📙 阿里云 📒 GITLAB 集成单/	5 , 新建文件共	ž					
支 対焦 开发者中心	首页 能力管理	技术支持			Q	⊲ »2	E2 0	8 186*****97[主账号]
< 返回应用列表	网址url: 暫无	_						
INTERNITY 测试OA扫码	应用简介: 智无	加签管理	1 加签内容配置	2 加亞配置完成	\otimes			
● 开发中 (APPID) 2021001135670762		选择加弦模式:	🔾 公明证书 🔹 公明					
■ 概応 ■ 消息服务	+ 添加協力 總已经	填写公明字符:	 注:资金支出类接口不支持公 支付宝会用SHA256withRsa罰約 器或OpenSSL(第三方工具)生成 	<mark>明的方式进行加落。</mark> 进行接口调用时的验签(不限制密钥长度)。使用 密钥	支付宝密钥生成			
			请输入通过密钥生成器或ope	nssl生成的密钥 (20-2000个字符)				Ø
						・已生效	删除	
	开发设置		保存设置					
		点击设置接	<mark>口加密方式</mark> 环境,查看如何使用:如果需要升	&RSA1到RSA2, 请参考操作指向。				
	接口加签方式: 暂天							
	19白名单: 未设	重 设置						

将工具生成的密钥对和支付宝生成的支付宝公钥保存在本地

加签管理	✓ 加签内容配置	2 加签配置完成	\otimes
应用公钥:		更换应用公制	月复制公钥
MIIBIJANBgk	qhkiG9w0BAQEFAAOCAQ8AMI	IBCgKCAQEAkIVBwZy+joNnlbElADvUu0QV+0OTfDx0	CkyMc8
支付宝公钥:			复制公钥
MIIBIJANBgk	qhkiG9w0BAQEFAAOCAQ8AMI	IBCgKCAQEAqPIQJtHebGqUC1gXGplwCM8w8VOcvll	NI25zEp
查看接入文档			

二、创建支付宝认证源

- 1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
- 2. 点击左侧导航 认证 > 认证源。
- 3. 点击右上角添加认证源,选择支付宝登录,点击添加认证源。

	T I				Q 搜索文档、控制台、API、解决方案	和资源盡用	ΙŴ	备案 🖸	业 支	侍 官阪	Þ_	٥.	Ä	() ()	简体	0
概览		认证源 / 添加	加认证源													
快速入门	_	← 添加i	认证源													
应用 应用列表	Ŷ	调输入认证源	28		Q											
)添加应用 账户	~	图标	认证源名称	\$	示识		描述							操作		
机构及组 账户管理		支	支付宝登录	a	alipay		便用支付宝	登录						漆加认证	瞭	
分类管理			钉钉微应用登录	c	ddtalk_micro		使用钉钉得	应用登录						添加认证	I.	
认证源	Î	9	微信开放平台扫码登录	٧	wechat		通过微信开	放平台实现	扫码登录					添加认证	源	
i征书管理		•	钉钉扫码登录	c	ldtalk		使用钉钉扫	码登录						漆加认证	源	
授权	^		1040		J			60 6 04-00346						100.4440 (2017)	. 7	

4. 将自动生成的RedirectUrl填写到支付宝创建的应用的授权回调地址中

 \times

添加认证源(支付宝登录)

* 认证源名称	支付宝登录
* AppId	请输入获取的AppID
	支付宝扫码登录开发申请获取的AppId,具体请访问:https://open.alipay.com/platfor
	m/home.htm
* appPrivateKey	请输入获取的AppSecret
	本地serve生成的密钥对中的私钥。
* alipayPublicKey	请填写alipayPublicKey
	阿里serve生成的密钥对中的公钥
* ddMappingField	请填写ddMappingField
	从支付宝查询到用户信息后,用支付宝的哪个字段来关联IDP的用户。
* RedirectUrl	https://dexuavjsho.login.aliyunidaas.com/api/public/bff/v1.2/authenticate/alipay/fi
	支付宝扫码后重定向地址, 在申请时填写, 不用修改. 注意: 必须与申请时的一致。
* 前端回调地址	请填写前端回调地址
	IDaaS服务认证后重定向到前端的地址,必须以http或https开头,不能为内网地址。
🖹 metadata.xm	へ 全部显示 ×
🚻 应用 (Free IDP Trial - Fr 📒 阿里	GITLAB 集成单点
支 熟課 开发者中心 首页	能力管理 技术支持 Q 印 2 日 2 ⑦ 8 186******97(主楽号
< 返回应用列表	(法)加定力 学已是:#如1項功器
○ MiloA扫码 ● 开发中	
	• 國際地址: https://dexuavjsho.login.aliyunidaas.com/api/public/bff/v1.2/authenticate/alipay/forw
	使用意可加加的的 安付金汇组回模权数据时,只能返回至该地址。 注: 著于用户内处、支付金汇放平台的第三方专业安全机构,将对台湾写的授权回端地址进行安全 扫描。仿清面,可在"开放中心"安全中心"里着着"另外,输口实、合法、准确读写使双回调 地址、否则所有责任(包括但不限于预维损失)概由应负责。
	单: 未近 只始证地高: 🖬 🔊
	3%关· http
	22. 第五 取用 回地社: 哲元 回面

5. 获取应用的APPID参数保存到本地,并提交审核

```
? 说明
```

使用支付宝扫码登录功能,必须确保支付宝开放平台的应用已通过审核

支熱焦开发者中心	首页							Q	⊈)2	2	?	(8) 186**	****97[主账号	
く 返回应用列表	概货	ā				0	审核未通过, 重新提3	5	- 2 *	师帝审核结果			③ 应用上	线
● 开发中 ◎ 20210		开发中 请先完成	家加功能、进行开发	纹配置,提交审核通过后	后可正式上线							提交审核	删除	
	基础	信息]	
	应用名	S称: 測试OA扫研	3										编	2 文
	应用图	BIR: 0A												即咨询
	应用类	經型: 网页应用												

6. 配置支付宝认证源参数

添加认证源(支付	宝登录)
* 认证源名称	支付宝登录
∗ Appld	2021
	支付宝扫码登录开发申请获取的Appld, 具体请访问:https://open.alipay.com/platfor
	m/home.htm
* appPrivateKey	MIIEvgIBADANBgkqhkiG9
	本地serve生成的密钥对中的私钥。
 alipayPublicKey 	MIIBIjANBgkqhkiG9w0
	阿里serve生成的密钥对中的公钥
* ddMappingField	nickName
	从支付宝查询到用户信息后,用支付宝的哪个字段来关联IDP的用户。
 RedirectUrl 	https://dexuavjsho.login.aliyunidaas.com/api/public/bff/v1.2/authenticate/alipay/fi
	支付宝扫码后重定向地址,在申请时填写,不用修改.注意:必须与申请时的一致。
* 前端回调地址	https://dexuavjsho.login.aliyunidaas.com/frontend/login#alipayCallback

其中:

Appld、appPrivateKey、alipayPublicKey为上述过程中获取的支付宝应用参数

ddMappingField: nickName

前端回调地址: IDaaS域名地址+/frontend/login#alipayCallback

是否显示:勾选之后,会在登录页面展示支付宝认证源

? 说明

IDaaS域名地址可以在云后IDaaS管理控制台获取。

实例列表						云命令行(Cloud Shell) 🗙
实例ID/名称 ,	状态 (全部) ∨	规格授权	创建时间	到期时间	用户访问的Portal的sso地址	用户访问的Portal的api地址
idaas-	运行中	基础版	2019年5月6日	2019年8月7日	ce, gin. aliyunidaas.com	Di.aliyunidaas.com
						く上一页 1

7. 认证源添加完成后,点击启用认证源

概范	认证源					添加认证源						
快速入门												
应用 ^ 应用列表 添加应用	认证源 本平台支持企业使用不 启用认证源后并配置完	同的外部认证源(即允许使用第三方认证为5 成后,平台会允许企业用户登录时使用具体的	13登录账户),可根据公司需要添加 约认证源去认证。	并使用不同的认证方式,如 DB、	LDAP、钉钉扫码等。	×						
账户 ^ 机构及组	搜索认证原	RERUIEM Q										
账户管理	认证源名称	认证源 ID	自定义登录	创建时间	状态	操作						
分类管理 认证 ^	支付宝登录	20200102105351ndfgH9xO0Nalip ay4	是	2020-02-26 18:54		修改详情日志制度						

三、支付宝扫码登录IDaaS

1. 通过浏览器访问云盾IDaaS用户Portal地址。

⑦ 说明

该地址由IT管理员提供。IT管理员可以在云盾IDaaS实例列表中查看用户访问的Port al地址。

(-)	管理控制台				搜索	Q X	肖息14 费用	工单 备案	企业	支持与服务 📐	'Ħ	简体中文	0
	IDaaS	实例列表								云命令行(Clou	d Shell)	× 购买II	DaaS
	实例列表	状态: 全部 🗸 🗸											
		实例ID/名称	状态	規格授权	创建时间	到期时间	用户访问的Po	ortal的sso地址		用户访问的Portal的	lapi地址		操作
		dan kantan di sebuah sebu sebuah sebuah seb	运行中	基础版	2019年4月8日	2019年5月9日	- advection	login.aliyunidaas	.com	api.aliy	unidaas.co	m f	管理
										<.	上一页	12下-	-页 >

2. 点击支付宝认证源图标,并使用移动端打开支付宝扫描页面二维码进行扫码登录



若用户首次使用支付宝扫码认证源,则需要绑定IDaaS账户,在绑定页面中输入IDaaS的用户名和密码

云盾账户绑定	
请输入IDaaS账户	
请输入密码	
提交	
没有账号? 点击注册	

首次绑定后,后续使用都无需再绑定,如果用户想要解绑当前的支付宝账号,需要进入用户界面 **我的账户** > 三方账户,进行解绑

欢迎・IDaaS		我的账户
主导航	^	账户安全 个人信息 我的证书 三方账户
首页 应用管理 应用子账户		公司已开启并且用户已绑定的认证源,用户可在此进行解绑操作。
设置	^	
二次认证 我的消息 我的日志		解除绑定

1.3. LDAP认证登录

本文介绍如何通过LDAP认证源,使用AD域里面的用户登录IDaaS,或者直接登录到应用。

场景

如果客户不希望保存AD用户的密码到阿里,可以使用IDaaS的LDAP认证服务,实现使用AD账户和密码登录 阿里控制台,或者其它应用的目的。



演示动图

统一认证·	第三方认证源接入
-------	----------

⑦ 阿里云IDAAS.认证云IDaaS平台 × +		- 🗆 X
$\leftrightarrow \rightarrow \mathcal{C}$ (\mathbf{A} \mathbf{T} \mathbf	2105351ndfgH9xO0NIdap5&re_sp_login=true	x 🖯 🗘
		•
	阿里云IDAAS	
	当前登录方式为 AD认证原	
	邮箱/手机号/账户名称 I	
	変形	
	博输入验证码 X R.R.K	
	登录	
	第三方账户登录	

配置步骤

1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考IT管理员-登录。

2. 在左侧导航点击 认证 ->认证源 跳转到认证源界面。

3. 点击右上角**添加认证源**,选择LDAP认证源,点击【添加认证源】,即可在弹出的界面中配置LDAP认证 源。

认证源						添加认证源
使用外音 本平台支持近 系统默认方式 启用认证源尼 默认为启用系	部认证 (使用系统数认认证 企业使用不同的外部认证度 (因为许使用第三方认证方式登录用户), , 在成合 Daus 就以支持的两种方式, 使用 Daus 用户名 - 或容器类 和 估种配数地成品、平台会计协全边用户是要对使用具体的认证要并已用成方可开 Edit数认认证。若需要用用外部认证、进行成如认证要并已用成方可开	可療經公司需要添加并使用不同的认适方式,如 DB、 U 明瞭 2018年2月1日發量是。 目 4. 品。	LDAP、专时扫码碑。			
投票认证要	k 21 6736 m	42.00	Q	Shearba	102.25-	
·添加认	证源		٩			
图标	认证题名称	标识		描述		提作
	4万4万物应用登录	ddtalk_micro		使用钉钉微应用登录		添加认证源
*	御信开放平台和四登委	wechat		通过微信开放平台实现扫码登录		添加认证源

使用钉钉扫码登录

LDAP Authenticate

LDAP URL为AD域的IP加端口号;

LDAP Base、LDAP UserDn、LDAP密码为AD的值;

过滤条件填写为如 (UID=\$username\$)。

? 说明

LDAP LDAP

钉钉扫码登录

IDaaS目前只支持公网访问,AD需要提供公网地址,并开启389端口,可以在安全组策略设置只有IDaaS的出口IP可以访问AD,IDaaS出口IP请提工单咨询IDaaS同学获取。

应用身份服务

* 认证源名称	LDAP
* LDAP URL	Idap://
	LDAP URL, 如: Idap://127.0.0.1:389/
* LDAP Base	dc=xxx,dc=com
	LDAP Base, 如: dc=idsmanager,dc=com
* LDAP UserDn	cn=Manager,dc=xxx,dc=com
	LDAP UserDn, such as: cn=Manager,dc=monkeyk,dc=com
* LDAP密码	LDAP密码
	LDAP服务器连接密码
* 过滤条件	查询用户的过滤条件
	过滤条件中使用\$username\$变量替换用户名, 如:(uid=\$username\$)
LDAP加密方式	NONE ~
	LDAP密码加密方式, 若未加密则选择 NONE
userPassword验证	
	在验证密码时是否使用userPassword字段的值进行比较,若选择是,则取该字段的值与登录密码进行比较,若选择
	合,则使用LDAP的用户密码进行验证
更新IDaaS密码	
	包荥经过LDAP认业后,将LDAP的密码更新在IDP中
显示	
	江豆冰风辰小叭证深四你
	提交取消

4. 在AD中创建账户。

? 说明

若您的AD中已有账户数据,可以跳过该步骤。AD中账户必须同步IDaaS中,才能实现认证。

5. 在右侧导航中点击机构及组,在机构及组页面 新建LDAP配置,配置完成后,将AD中的账户数据拉取到 IDaaS中。

6. AD中的账户需要同步IDaaS后,才能使用ldap认证源进行登录认证。用户输入AD中的账户和密码时,会 先检验登录的这个账户是否在IDaaS中存在,如果在IDaaS中存在,再传递账户到LDAP中去认证,如果IDaaS 中不存在,不会进行下面的操作。 ? 说明

若已经在机构及组中存在LDAP认证源对应的LDAP配置,则不需要新建LDAP配置。

7. 在<mark>用户登录页面</mark>下侧的第三方认证登录中点击LDAP认证源,跳转到LDAP账户登录界面,使用AD域中的账 户密码进行登录。

◯ 注意

使用LDAP认证源进行登录时,需要使用AD域里面的密码进行登录,不能使用IDaaS里面的密码登录。

ŧ	日码登录更便捷
(-)阿里	<u></u>
阿里云IDaaS服务	
请输入账户 / 邮箱 / 手机号	
请输入密码	
请输入验证码	I EWY
	忘记密码
提交	
注册	
第三方认证登录	
S S C	

LDAP账F	□登录
请输入验证码	₽), 74 7 -
提交	٤
返回	0

通过以上步骤,完成了添加配置LDAP认证源,用户可以直接使用AD中的账户和密码登录IDaaS。

FAQ

1. 是否使用LDAP认证源,一定要同步ldap的账户到IDaaS中。
 是的。只需同步账户,不会同步LDAP中的密码到IDaaS中。
 2. 添加了ldap认证源,但是在登录页面没有显示ldap图标。

请查看下图中的登录页显示,是否进行了勾选。

添加认证源 (LDAP)

	cn=manager,ac=username,ac=com
* LDAP账户密码	LDAP账户密码
	LDAP账户对应的密码
* 过滤条件	查询用户的过滤条件
	LDAP中匹配本系统用户名的筛选条件,如: (sAMAccountName=\$username\$),具体匹配规则可参考L (https://ldap.com/ldap-filters/),举例中的 \$username\$; 数,是固定值。
LDAP加密方式	NONE
	LDAP密码加密方式,若未加密则选择 NONE。
userPassword验证	
	在验证密码时是否使用userPassword字段的值进行比较, 的值与登录密码进行比较,若不勾选则使用LDAP的用户密
更新IDaaS密码	
	登录经过LDAP认证后,将LDAP的密码更新在IDaaS中。
是否显示	
	在登录页展示认证源图标
	提交 取消

3. 是否可以更新LDAP中的密码到IDaaS中。

支持。参考下图设置同步ldap的密码到IDaaS中,当使用LDAP账户和密码登录一次后会自动更新IDaaS中的密码。

添加认证源(LDAP)

	cn=manager,ac=username,ac=com
* LDAP账户密码	LDAP账户密码
	LDAP账户对应的密码
* 过滤条件	查询用户的过滤条件
	LDAP中匹配本系统用户名的筛选条件,如: (sAMAccountName=\$username\$),具体匹配规则可参考LDAF (https://ldap.com/ldap-filters/),举例中的 \$username\$ 为本 数,是固定值。
LDAP加密方式	NONE
	LDAP密码加密方式,若未加密则选择 NONE。
userPassword验证	
	在验证密码时是否使用userPassword字段的值进行比较,若勾的值与登录密码进行比较,若不勾选则使用LDAP的用户密码进
更新IDaaS密码	
	登录经过LDAP认证后,将LDAP的密码更新在IDaaS中。
是否显示	
	在登录页展示认证源图标
	提交取消

4. 通过ldap认证源进行登录,提示账户名和密码不正确。

请检查下面参数和格式是否正确。

添加认证源(LDA	AP)	×			
* 认证源名称	LDAP				
* LDAP URL	Idap://127.0.0.1:389/ 参考该格式				
	LDAP服务器连接地址,如: ldap://127.0.0.1:389/ IPv6 地址主机IP需要放在中括号内,如: ldap://[0000:0000:0000:0000:0000:0000:0001]:389/				
* LDAP Base	dc=xxx,dc=com				
	LDAP中的节点, 会到该节点下认证账户, 如: dc=idsn	nanager,dc=com			
* LDAP账户	cn=Manager,dc=userName,dc=com				
	需要有以上填写的Base的管理权限,如: cn=Manager,dc=userName,dc=com	检查账户密			
* LDAP账户密码	码是否正确				
	LDAP账户对应的密码				
* 过滤条件	(sAMAccountName=\$username\$) 参考	该格式			
	LDAP中匹配本系统用户名的筛选条件,如: (sAMAccountName=\$username\$),具体匹配规则可参 (https://ldap.com/ldap-filters/),举例中的 \$username 数,是固定值。	考LDAP官方文档 \$\$ 为本系统用户名参			
LDAP加密方式	NONE	~			
	I DAP 率码加率方式 若未加率则选择 NONF				

5. 是否可以指定默认的登录方式是ldap认证源

支持。参考下图配置默认的登录方式是ldap认证源。

应用 应用列表 添加应用	^	移动端绑定设置 僵尸账号清理	系统密钥算法	统一二次认证 登录/注册	策略管理 自动同步账户配置 短信配置 邮件配置
账户 机构及组 账户管理 分类管理	^	注册		与用户登录相关的一些配置。 账户部中	
认证	^	应用登录			 开启后用户在登录失败时将被限制失败次数。
认证源 RADIUS 证书管理				显示验证码	✓ 在登录页使用户名密码登录时是否需要输入验证码
授权 权限系统	^			豆水大吸入致亚小亚吐帕	1次 ~ ~ · · · · · · · · · · · · · · · · ·
应用授权	~			时间范围	5 分钟 失败次数的计数时间范围,如:默认为5分钟,则5分钟后重置失
其它管理 [●] 设置	× ^			登录认证方式	LDAP ^
个性化设置 安全设置					他认证方式(第三方外部)。 账户+密码(默认) LDAP

1.4. 钉钉扫码登录

本文为您介绍在 IDaaS 中如何配置钉钉扫码认证源,并使用钉钉扫码登录 IDaaS 平台。

背景信息

云盾IDaaS平台支持公司成员使用多种外部认证源登录。IT管理员可以根据公司需要,添加并启用不同的认证 方式,例如DB、LDAP、钉钉扫码、OTP验证码登录等。

钉钉作为常用的办公软件,以钉钉作为外部认证源,通过钉钉扫码的方式用户可以更加灵活、方便地登录到 IDaaS。

配置钉钉扫码认证源的操作步骤主要分为两步:

- 1. 在钉钉开发者平台添加微应用并配置扫码登录
- 2. 在IDaaS平台添加钉钉扫码认证源

完成以上两步,即可实现使用钉钉扫码登录到IDaaS

在钉钉开发者平台添加微应用并配置扫码登录

- 1. 登录钉钉开发平台, 地址: https://open-dev.dingtalk.com
- 2. 登录成功后,在首页获取Corpld参数

♥ 钉钉开放平台	第四 由用开設 基本信息 开放文档	zhangdh	退出	0
	zhangdh #40288月 Copyed ding62864276000054 工具与党派:设计规源:			
	海島通知			
	同步发送工作通知用意输口下线通知 (mm) 2000/03/19 11:	34		
	开头會講題変領研 (3月) cma 2000/03/16 12: 11T1/NF2年刊学業要素項研 cma 2000/03/16 12:	34 22		

3. 点击应用开发,在左侧导航栏中选择H5微应用,创建一个钉钉微应用

? 说 如果E	⑦ 说明 如果已创建过H5微应用,可以直接使用现有的。									
♥ 钉钉开放平台	≦	<u>应用开发</u> 基本信息 开发文档	zhangdh 退出 💊							
	企业内部开发	企业内部应用 / H5概应用 1								
2	小程序	H5微应用								
	HS微应用	⑦ 如何开发								
	机器人									
	工作台									
	第三方企业应用									

测试

4. 创建完成后,点击应用图标查看应用详情,获取应用的 AppKey 和 AppSecret 参数。

		基础信息	接口权限	稳定性管理	应用发布
应用名称:	测试			修改	
应用类型:	企业内部自主开发-开发应用				
应用logo:	م بند في ال ال ال ا				
应用简介:	测试				
应用首页地址:	https://duhaexkpie.login.aliyunidaas.com/api/public d=303616771&appld= 201910101757083TKqTYyw	c/bff/v1.2/authentica qyjwt2	ate/ddMicro/login?a	agentl	
PC端首页地址:	https://duhaexkpie.login.aliyunidaas.com/api/public d=303616771&appld= 201910101757083TKqTYyw	c/bff/v1.2/authentica qyjwt2	ate/ddMicro/login?a	agentl	
可使用范围:	draven				
AgentId:	303616771				
服务器出口IP:	47.104.68.11,47.105.200.5				
AppKey:	dingjn1ljglz2tcyqtki				
AppSecret:	点击查看				

5. 在左侧导航栏中点击移动应用接入-登录,然后点击创建扫码登录应用授权

首页 应用开发	z 基本信息 开发文	挡						
	1							
企业内部开发	移动应用接入 / 扫码登录							
小程序	扫码登录							
H5微应用	③ 如何开发							
工作台								
第三方企业应用								创建扫码登录应用授权
小程序	名称	描述	授权页面LOGO地址	回调域名	appld	appSecret	权限信息	操作
H5微应用 钉钉云	wang	sdfds	https://mgomerkwuj.login.aliyuni daas.com/api/public/bff/v1.2/aut henticate/ddtalk/forward idaas-c	https://mgomerkwuj.login.aliyuni daas.com/api/public/bff/v1.2/aut henticate/ddtalk/forward_idaas-c	dingoarfhzop0akyft dkfi	gVugzSelfgI3Daqo7TPFimfBbpI7eHB8hgPfYB KZmUcYvZbXfEI0MGz3HEaTU4HW	访问字段: nick	3
上架应用市场			n-v641b5ffj05ddtalk1	n-v641b5ffj05ddtalk1		, ,	dingld	
应用内购	zzd	zzd	https://59.202.52.212:9091/api/p ublic/bff/v1/authenticate/ddtalk/ forward_zzdddtalk	https://59.202.52.212:9091/api/p ublic/bff/v1/authenticate/ddtalk/ forward_zzdddtalk	dingoa6hwaogicfbff bpqv	5UeG8i_uruUahTwnphXNa6Q2Ph1eDPNz1T7 hAtG5TPR8r1Venkfm_R5o-tCsXp8k	访问字段: nick dingld	2
小程序	aliyufa	as	https://skwbptqdqy.login.aliyuni daas.com/api/public/bff/v1.2/aut henticate/ditalk/forward_jdaas-c n-78v180tgr01ddtalk	https://skwbptqdqy.login.aliyuni daas.com/api/public/bff/v1.2/aut henticate/ddtalk/forward_idaas-c n-78v180tgr01ddtalk	dingoaobwznlpbzax jy60h	A95OQ-39nCEvbRynJtsGbWZZ458xAvEMsfFV eRcfwZfFCF9kVxbZafVkQlrumJsz	访问字段: nick dingld	L
分享 登录	2 wangli	ceshi	https://wangli.idp4.idsmanager.c om/api/public/bff/v1.2/authentic ate/ddtalk/forward_wangliddtalk	https://wangli.idp4.idsmanager.c om/api/public/bff/v1.2/authentic ate/ddtalk/forward_wangliddtalk	dingoaoctd2p2iztva xdgf	kellwWcFDdMknVgljjnYSqrWcc1MLKF39CUeb eJS66SK_MHyfTvbE7Rwd1L3pdEe	访问字段: nick dingld	2

6. 创建扫码登录应用授权的必填参数中,名称、描述可以随便填写,授权 logo 地址和回调域名需要填写 IDaaS 里添加钉钉扫码认证源时系统生成的 Redirect Url 的地址。

? 说明

管理员在IDaaS平台新建钉钉扫码认证源时,会自动生成并展示 Redirect Url 参数。直接将页面展示的 Redirect Url 参数复制粘贴到对应位置即可。

添加认证源(钉钉	J扫码登录)	\times
	认证源ID,由系统生成	
* 认证源名称	钉钉扫码登录	1
* 扫码AppId	请输入获取的AppID	
	钉钉扫码登录开发申请获取的AppID, 具体请访问:钉钉开放平台	
* 扫码AppSecret	请输入获取的AppSecret	
	钉钉扫码登录开发申请获取的AppSecret, 具体请访问:钉钉开放平台	
* CorpID	请填写CorplD	
	钉钉后台 微应用-> 微应用设置 中获取的 CorpID	
* 应用AppKey	请填写CorpSecret	
	在钉钉开放平台,应用开发 -> 企业内部开发,添加小程序或H5微应用后获取	
∗ 应用AppSecret	请填写应用AppSecret	
	在钉钉开放平台,应用开发 -> 企业内部开发,添加小程序或H5微应用后获取	
* RedirectUrl	https://sbaucspfro.login.aliyunidaas.com/api/public/bff/v1.2/authenticate/ddtalk/fo	
L	钉钉扫码后重定向地址,注意:必须与申请时的一致	
* 前端回调地址	清填写前端回调地址	
	IDaaS服务认证后重定向到前端的地址,必须以http或https开头,不能为内网地址。	

创建扫码登录应用	授权	\times
* 名称:		
* 描述:		
* 授权LOGO地 址:	这个会显示在授权页面的中间页中,以http或 https开头,必填,最多不超过500个字符	
* 回调域名:	微应用回调的URL,以http或https开头,必填, 最多不超过500个字符	
	取消 确	定

7. 添加成功以后,获取扫码登录页面所展示得 appld、appSecret 参数。

企业内部开发	移动应用接入 / 扫码登录							
小程序	扫码登录							
H5微应用	③ 如何开发							
工作台								
第三方企业应用								创建由码登录应用授权
小程序	名称	描述	授权页面LOG0地址	回调域名	appld	appSecret	权限信息	操作
H5微应用 钉钉云 上朝应用肉汤	wangli	测试	e ntic	om ic ic ik		∼g€	访问字段: nick dingld	2
应用内购 第三方个人应用	正式环境	正式环境		8 1 4		w 47	访问字段: nick dingld	2
小程序 移动接入应用	预发环境新	预发环境新		odsus id r con-	c avmw	of www.sHFk8uc' 4Zh	访问字段: nick dingld	2
고주 登录	IDP4wang	IDP4wang				BC	访问字段: nick dingld	2

在IDaaS平台创建钉钉扫码认证源

- 1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
- 2. 在左侧导航栏, 单击认证 > 认证源, 在认证源页面点击右上角的添加钉钉认证源。

三 (-)阿里云	Q 我家文档、控制台、API、新进	決方室和問題 現用 工单 备案 企业 支持 直网 🖸 📮 🕐 简体 🌘
概況	认证到	Sister Statistics and Sister Statistics
快速入门		
应用 ^ 应用列表 添加应用	↓征源 ▲半年支持企业使用不同的外部从证源(即允许使用第三方从证方式登录程户),可根据公司重要添加并使用不同 原用从证源后并配置%或后,平台金允许企业用户登录时使用具体的认证源去认证。	X MNALE955, MDB, LDAP, 1713:H996.
账户 ^ 机构及组	Brauen Q	
账户管理	认证源名称 认证源 ID 自定义登录 创建	建时间 状态 操作
分类管理 认证 ^	短倍验证码登录-wi 20200313110953GDMJ2Dy8pesm 是 2020 s2 2	20.03-20 16 35 译情 日志 删除
认证源	短倍验证码建录 20200313110953GDMJ2Dy8pesm 是 2020	20-03-20 15:11 译情 日志 删除
RADIUS	短倍验证码登录 20200313110953GDMJ2Dy8pesm 是 2020	20-03-20 15:06 译情 日志 删除

3. 在认证源中选择钉钉扫码登录, 点击右侧的添加认证源。

认证源 / 添加认	人证源 ← 返回			
图标	认证源名称	标识	描述	操作
	钉钉扫码登录	ddtalk	使用钉钉扫码登录	添加认证源

4. 配置钉钉扫码认证源

添加认证源(钉钉扫码登录)

 \times

1 不知道怎么	配置? 点击这里
* 认证源ID	20200313110953GDMJ2Dy8peddtalk1
	认证源ID,由系统生成
* 认证源名称	钉钉扫码登录
* 扫码AppId	请输入获取的AppID
	钉钉扫码登录开发申请获取的AppID,具体请访问:钉钉开放平台
* 扫码AppSecret	请输入获取的AppSecret
	钉钉扫码登录开发申请获取的AppSecret,具体请访问: 钉钉开放平台
* CorpID	请填写CorplD
	钉钉后台 微应用-> 微应用设置 中获取的 CorplD
∗ 应用AppKey	请填写CorpSecret
	在钉钉开放平台,应用开发 -> 企业内部开发,添加小程序或H5微应用后获取
* 应用AppSecret	请填写应用AppSecret
	在钉钉开放平台,应用开发 -> 企业内部开发,添加小程序或H5微应用后获取
* RedirectUrl	https://sbaucspfro.login.aliyunidaas.com/api/public/bff/v1.2/authenticate/ddtalk/fc

扫码 Appld 和扫码 AppSecret:上述《在钉钉开发者平台配置》步骤7所获取的 appld、appSecret 参数。

CorpID: 上述在钉钉开发者平台配置步骤2所获取的CorpId参数。

应用 AppKey 和 **应用** AppSecret:上述《在钉钉开发者平台配置》步骤4所获取的H5微应用的 AppKey 和 AppSecret 参数。

前端回调地址:/frontend/login/#/ddtalkCallback(固定值,添加时系统会默认生成)

? 说明								
IDaaS 用户侧的地址 请到 <mark>云盾IDaaS控制台</mark> 页面获取。如下图:								
应用身份管理	实例列表							购买IDaaS
实例列表	实例ID/名称	地域	状态 (全部) ∨	规楷授权	到期时间	用户访问的Portal的sso地址	用户防闭的Portal的api地址	操作
	idaas-cn }	华北2 (北京)	运行中	集成版	2020年3月18日	swtcliegne login aliyunidaas.com	swtcliegne.api.aliyunidaas.com	管理 升级 续器

点击勾选最下方的是否显示

修改认证源(钉钉扫	码)	\times
	אאדשארוא איזאנא איזאנא איזאנא איזאנא איזאנא איזעאנא איזעאנא אוידע אוידע איז אוויעאנא אז אווידע איז א	
* CorpID	1	
	钉钉后台 微应用-> 微应用设置 中获取的 CorpID	
* 应用AppKey	1	
	在钉钉开放平台,应用开发 -> 企业内部开发,添加小程序或H5微应用后获取	
∗ 应用AppSecret	1	
	在钉钉开放平台,应用开发 -> 企业内部开发,添加小程序或H5微应用后获取	
* RedirectUrl	https://sbaucspfro.login.aliyunidaas.com/api/public/bff/v1.2/authenticate/ddtalk/fo	
	钉钉扫码后重定向地址,注意:必须与申请时的一致	
* 前端回调地址	http://xxx.xxx.com/frontend/login#ddtalkCallback	
	IDaaS服务认证后重定向到前端的地址,必须以http或https开头,不能为内网地址。	
	示例: http://xxx.xxx.com/frontend/login#ddtalkCallback	
是否显示		
	在登录页展示认证源图标	
	提交取消	

5. 创建成功后,在认证源列表中启用它

概览		i	人证源	添加性性认证源。添加认证源							
快速入门											
应用 应用列表 添加应用	^		↓证源 本平台武持全业使用不同的分部以证源(即允许使用施三方以证方式登录账户),可根据公司需要添加并使用不同的认正方式,如DB、LDAP、钉钉扫码等。 应用以证源后并配置充成后,平台会允许企业用户登录时使用具体的认证源在认证。								
账户 机构及组	^		搜索认证源								
账户管理			认证源名称	认证源 ID	自定义登录	创建时间	状态	操作			
分类管理	^		们们扫码	20200313110953GDMJ2Dy8peddt alk1	是	2020-03-22 23:44		修改详情。日志删除			

使用钉钉扫码登录到IDaaS

1.在云盾IDaaS控制台复制用户的登录地址进行访问。

实例列表							到买IDaaS
实例ID/名称	状态 (全部) \vee	规格授权	创建时间	到期时间	用户访问的Portal的sso地址	用户访问的Portal的api地址	操作
idaas-cn	运行中	基础版	2019年5月6日	2019年8月7日	cephpmwdoh.login.	cephpmwdoh.api.aliyunidaas.com	管理
						〈上一页 1	下一页 >

2.在用户登录页面可以看到钉钉扫码认证源。

	自码登		
	阿里云IDAAS		
V	请输入账户/邮箱/手机号		
	请输入密码		
	请输入验证码	MWAH '	\sim I
		忘记密码	
	提交		
	第三方认证登录 ——		

3.点击认证源显示扫码页面。



请使用钉钉扫描二维码登录 😳刷新

没有钉钉? 点击使用云盾IDaas平台 账号密码登录。

4.使用钉钉第一次扫码登录时需要绑定IDaaS账户,绑定完成后IDaaS账户会与钉钉账户关联起来,之后登录 无需再次绑定,直接使用钉钉扫码即可登录IDaaS。
	云盾账户绑定	
	请输入账户/邮箱/手机号	
	请输入密码	
	提交	
	没有钉钉?点击使用云盾IDaas平台 <mark>账号密码登录</mark> 。	
-		

完成以上步骤,即可实现钉钉扫码登录的功能。

首次绑定后,后续使用都无需再绑定,如果用户想要解绑当前的钉钉账号,需要进入用户界面 **我的账户 > 三方账户**,进行解绑

欢迎·IDaaS		我的账户
主导航	^	账户安全 个人信息 我的证书 三方账户
首页		
应用管理		公司已开启并且用户已绑定的认证源,用户可在此进行解绑操作。
应用子账户		
设置	^	
我的账户		
二次认证		1921
我的消息		解除绑定
我的日志		

1.5. 钉钉微应用单点登录

通过 IDaaS 微应用认证源能力与钉钉微应用集成,实现在钉钉工作台中单点登录进入应用的效果。

操作流程



准备工作

- 1. 在IDaaS管理员控制台的应用列表中添加想要单点登录的应用。
- 2. 申请注册钉钉组织。如果已有钉钉组织,可跳过该步骤。

创建钉钉微应用

操作步骤

1. 登录钉钉开发者平台

🛇 钉钉开放平台	首页 应用开发	基本信息	开发文档		
	zhangdh 未以证服务商 Corpid: ding6d26f427b000 ③ 技术答疑 ④ 需求違い	05ea35c2f4657eb63 (78f 工具与资源:调试工具; 🗎	设计资源: 🖻	
	消息通知				
	开发者满意度调研(0月) new			
	内购复查通知 new				
	智能工作流全新开放	new			
	关于static.dingtalk.c	om域名IP变更的公告	new		

2. 点击应用开发,选择H5微应用

	首页	应用开发	基本信息	开发文档			
	企业内部开发 小程序 H5微应用	_	企业内部应用 / H5微应用 ⑦ 如何开发	H5微应用			
	工作台 第三方企业应)	₹	+	创建应用			
3. 点击	云创建应用		创建	趁用			
	1 填写	基本信息			2 配置开发	信息	
	* 应用名称:	测试 名称可以由中文、数字	"及英文组成,长度在2-10个	字符, 可修改。点击了触	解更多《基本信息规范》		
	* 应用Logo:	••••• •••••• ••••••••••••••••••••••••	<mark>上 点击上传</mark> 、jpeg、jpg,建议大小为2	00PX*200PX, 可修改			
	* 应用简介:	测试请简要描述应用提供的	〕产品或服务,最多32个字,	可修改		li li	
	* 开发方式:	 企业内部自主开 授权给服务商开 	开发 企业内部开发人员为1 开发 企业内无开发团队,排	全业开发应用 受权给定制服务商为企业3	开发应用		
		下一步					

		创建应用	
1 填写	基本信息		2 配置开发信息
* 开发模式:	● 开发应用 ○ 快捷链接 需要使用开发工具进行功能开发		
* 开发应用类型:	🔵 小程序 🕐 💿 微应用 🕐		
* 应用首页链接:	请输入 请输入http或https开头的网址链接,如	[[https://www.dingtalk.com	
*服务器出口IP:	请输入 调用钉钉服务端API时的合法IP列表,参	多个IP请以","隔开,支持带一个*号	通配符的IP格式
PC端首页地址:	请输入 请输入http或https开头的网址链接,如	ቢhttps://www.dingtalk.com	
管理后台地址:	请输入 请输入http或https开头的网址链接,如	۵. (multips://www.dingtalk.com	
応田首五链接・左ロ	上一步 创建	下面步骤4	
应用首页链接:在ID	aaS上获取,获取方式参考 [·]	下面步骤4	

PC端首页地址:和应用首页链接一致即可

服务器出口IP: IDaaS服务器的出口IP

- 4. 应用首页链接参数的获取方式
 - i. 在IDaaS管理员页面,点击认证源-点击添加钉钉认证源

☰ (-) 阿里云			Q 搜索文档、控制台、	API、解決方靈和资源 费用	工单 备案	企业 支持	官网 🖸	⊒ ∆ '	`₩ (⑦ 简体	
概览	认证源							添加4T4TiJ	LITER OF	添加认证源	
快速入门											
应用 ^ 应用列表 添加应用	↓证源 本平台支持企业使用不同的 局用认证源后并配置完成后	外部认证源(即允许使用第三方认证方式 ,平台会允许企业用户登录时使用具体的	(登录账户) , 可根据公司需要添加并 的认证源去认证。	她用不同的认证方式,如 DB、LDA	2、钉钉扫码等。					×	1
NP ^ 机构及组	搜索认证源		c								
账户管理	认证罪名称	认证源 ID	自定义登录	创建时间	状态		操作				
分类管理	LDAPzbb500	20200102105351ndfgH9xO0Nidap1 0	Ť	2020-03-19 22:57			修改	详情 E	利康 憲際		
ikiEit	支付宝登录-WL	20200102105351ndfgH9xO0Nalipa y6	是	2020-03-19 19:12	×		修改	详情 E	日志 删除		

既览	认证源 / 添加认证源						
快速入门	← 添加认证源						
添加应用	4]4]	q					
6户 ^	图标 认证源名称	标识	描述	提伯			
机构及组	11打微应用登录	ddtalk_micro	使用钉钉微应用登录	添加认识			
分类管理	1111月時登录	ddtalk	使用钉钉扫码登录	添加认			
۸Æ •							
i A ii E ii R							
添加认证源(银	J钉微应用登录)						
* 认证源ID	201910101757083TKqTYyw	/qyddtalk_micro					
	认证源ID,由系统生成。						
* 认证源名称	钉钉微应用登录						
* AgentID	清輸入获取到的AgentiD						
	钉钉添加微应用获取的AgentII	D.多个AgentID用逗号(.)分隔,具体请;	方问:https://oa.dingtalk.com/				
* CorpID	请填写CorpID						
	钉钉后台 微应用-> 微应用设置	是中获取的 CorpID					
 AppKey 	请输入获取到的Appkey						
	钉钉后台 微应用-> 微应用设置	-> 查看详情中获取的 AppKev					
 AppSecret 	请输入获取的AppSecret						
	红红扫码登录开发由语莽取的	AnnSecret 目休违访问·					
		debe consideration of the second s					
是否在浏览器中	打开						
	"旦"韦云左浏览器由打开应田	"丕"韦云在04丁作会打开应用(仅5	土立て作品が				
			1731 Um255.				
ddConfigUrl	https://duhaexkpie.login.aliv	unidaas.com/api/public/bff/v1.2/authe	enticate/ddlviicro/login?adentid=&apbid=				

iii. 找到ddConfigUrl字段值:

https://duhaexkpie.login.aliyunidaas.com/api/public/bff/v1.2/authenticate/ddMicro/login? agentId=&appId= iv. 点击应用列表, 选择需要单点的应用

■ (-)阿	里云			Q 造業	
概范		应用列表			
快速入门					
应用 应用列表 添加应用	Â	应用	列表 可以在当前页面管理已经添加的所 1完应用后,应该确认应用处于启用	每应用,应用可以实现 单点整要和 用户同步 能力。 长态,并已经免成了张权、在应用评集中,可以看到应用的评喻信息、单点整是地址,子张户配量,同步	記蓋、接权、审计等等信息。
账户	~	JWT			Q
机构及组		应用图标	应用名称	应用ID	设备类型
分类管理		J	JWT	201910101757083TKqTYywqyjwt2	Web应用
认证	^				

该应用ID是上面 url 中的 appld 参数, 拼接成 url 值为:

https://duhaexkpie.login.aliyunidaas.com/api/public/bff/v1.2/authenticate/ddMicro/login? agentId=&appId=201910101757083TKqTYywqyjwt2

- v. 将上述生成的 url 值复制粘贴到应用首页链接和 PC 端首页地址的输入框中,点击保存应用。
- vi. 查看应用的详情,获取应用的AgentId参数

		测证	t		
	基础信息	接口权限	稳定性管理	应用发布	
应用名称:	测试			修改	
应用类型: 应用logo:	企业内部自主开发-开发应	用 ⊘			
应用简介:	测试				
应用首页地址:	https://duhaexkpie.login.a d=&appId= 20191010175	liyunidaas.com/api/p 7083TKqTYywqyjwt2	oublic/bff/v1.2/authen	ticate/ddMicro/login?agentl	
PC端首页地址:	https://duhaexkpie.login.a d=&appId= 20191010175	liyunidaas.com/api/p 7083TKqTYywqyjwt2	oublic/bff/v1.2/authen	ticate/ddMicro/login?agentl	
可使用范围:	全部员工				
AgentId:	303616771				
服务器出口IP:	47.104.68.11,47.105.200.5				
AppKey:	dingjn1ljglz2tcyqtki				
AppSecret:	点击查看				

		测记	<u>.</u> U		
	基础信息	接口权限	稳定性管理	应用发布	
应用名称:	测试				修改
应用类型:	企业内部自主开发-开发应	用 ②			
应用logo:					
应用简介:	测试				
应用首页地址:	https://duhaexkpie.login.al d=8appId= 20191010175	liyunidaas.com/api/p 7083TKqTYywqyjwt2	ublic/bff/v1.2/authent	icate/ddMicro/login?agentl	
PC端首页地址:	https://duhaexkpie.login.al d=xappld= 20191010175	liyunidaas.com/api/p 7083TKqTYywqyjwt2	ublic/bff/v1.2/authent	icate/ddMicro/login?agentl	
可使用范围:	全部员工				
AgentId:	303616771				
服务器出口IP:	47.104.68.11,47.105.200.5				
AppKey:	dingjn1ljglz2tcyqtki				
AppSecret:	点击查看				

vii. 修改应用,把应用详情中的 Agent Id 的值添加到 url 的 agent Id 参数后面

创建钉钉微应用认证源

操作步骤

1. 在IDaaS管理员页面,点击认证源-点击添加钉钉认证源

☰ (-)阿里	Ξ			Q 搜索文档、主	的台、API、解决方案和资源	费用 工单 备案	企业 支持 育	nn d' H	🕐 简体 🌔
概览		认证源						添加时时认证源	添加认证源
快速入门									_
应用 应用列表 添加应用	^	从证源 本平台支持企业使用不 。 向用从证源后并配置完成	司的外部认证源(即允许使用第三方认证方式 成后,平台会允许企业用户登录时使用具体的	《登录账户),可根据公司需要 9认证源去认证。	添加并使用不同的认证方式,如 D	B、LDAP、钉钉扫码等。			×
账户 机构及组	^	搜索认证源			Q				
账户管理		认证源名称	认证源 ID	自定义登录	创建时间	状态		操作	
分类管理		LDAPzbb500	20200102105351ndfgH9xO0Nldap1 0	否	2020-03-19 22:57	()×		修改详情日志 🗒	除
认证源		支付宝登录-WL	20200102105351ndfgH9xO0Nalipa y6	是	2020-03-19 19:12	×		修改详情日志删	Rê

2. 选择钉钉微应用登录-点击添加认证源

概览		认证源 / 添加认证源			
快速入门		← 添加认证源			
应用	^				
应用列表		4 1 4J	٩		
添加应用		图标 认证源名称	标识	描述	操作
账户	^	(11) 数定用登录	ddtalk_micro	使用钉钉微应用登录	添加认证源
账户管理					
分类管理		1111日時登录	ddtalk	使用钉钉扫码登录	添加认证源
认证	^				
认证源					

3. 配置钉钉微应用认证源参数

添加认证源(钉钉微应用登录)

* 认证源ID	201910101757083TKqTYywqyddtalk_micro
	认证源ID,由系统生成。
* 认证源名称	钉钉微应用登录
* AgentID	清输入获取到的AgentID
	钉钉添加微应用获取的AgentID,多个AgentID用逗号(,)分隔,具体请访问:https://oa.dingtalk.com/
* CorpID	请填写CorpID
	钉钉后台 微应用-> 微应用设置 中获取的 CorpID
* АррКеу	请输入获取到的Appkey
	钉钉后台 微应用-> 微应用设置 -> 查看详情中获取的 AppKey
* AppSecret	请输入获取的AppSecret
	钉钉扫码登录开发申请获取的AppSecret,具体请访问:
是否在浏览器中打开	
	"是"表示在浏览器中打开应用,"否"表示在OA工作台打开应用,仅针对PC端免登。
ddConfigUrl	https://duhaexkpie.login.aliyunidaas.com/api/public/bff/v1.2/authenticate/ddMicro/login?agentId=&appId=
	钉钉访问IDaaS的地址,在钉钉后台->微应用设置->查看应用详情->首页地址 查看。
	提交取消

CorpID: 登录钉钉开放平台首页展示的值

♥ 钉钉开放平台	首页	应用开发	基本信息	开发文档			
	zhangdh 末认证服务商 Corpld: ding6d. ⑦ 技术答疑	26f427b0 @ 需求建议	1400-000-08	工具与资源:设计资源: 🖻	调试工具: 🖻	API Explorer: 🔌 ᡞ 🗤	

AgentID、AppKey、AppSecret:钉钉微应用-应用详情中展示的值

送 日	测试
	基础信息 接口权限 稳定性管理 应用发布
应用名称:	: 测试 修改
应用类型:	企业内部自主开发-开发应用 ⑦
应用logo:	ब
应用简介:	· 测试
应用首页地址:	https://duhaexkpie.login.aliyunidaas.com/api/public/bff/v1.2/authenticate/ddMicro/login?agentl d=&appld= 201910101757083TKqTVywqyjwt2
PC端首页地址:	: https://duhaexkpie.login.aliyunidaas.com/api/public/bff/v1.2/authenticate/ddMicro/login?agentl d=&appld= 201910101757083TKqTVywqyjwt2
可使用范围:	全部员工
Agentid:	303616771
服务器出口IP:	47.104.68.11.47.105.200.5
АррКеу	dingjn1ljglz2tcyqtki
AppSecret	点击查看

4. 点击启用钉钉微应用认证源

概览		认证源					添加打打认证源			
快速入门										
应用 应用列表 添加应用	^	₩证源 × *平含支持企业使用不同的外部从证源(間允許使用第三方认证方式登录集中),可根据公司重要添加并使用不同的认证方式,如DB、LDAP、钉钉扫码等。 周用以证源后并配置地成后,平合会允许企业用中登录时使用两体的认证源去认证。								
账户 机构及组	^	授素认证源	ReskA Egg							
账户管理		认证源名称	认证源 ID	自定义登录	创建时间	状态	操作			
分类管理	^	钉钉微应用登录	20200102105351ndfgH9xO0Nddtal k_micro3	是	2020-03-25 18:55		修改详情。日志别除			

5. 在钉钉开放平台中发布应用

首页 应用开发	基本信息 开发文档		zha
企业内部并发	10.100	测试	
小程序		基础信息 接口权限 稳定性管理 应用发布	
H5儆应用			
工作台	应用开发流程		
第三方企业应用	1 应用开发		
小程序	应用编制 已完成		宣晋详情
H5微应用	MPALPHDAHK, MDT, LOGOWARA-1028.		
钉钉云	接口权限 巴弗威 法制服器與开設企业内部応用。必须对服器與進行機权、以便正企业信息完全。		查看详情
上架应用市场			
应用内购	加27122-73 (水弦句) 开发内成后。波布范用。企业全员即可在工作会上重都并使用该应用		查看详情
第三方个人应用			

)旌 [0]	测试				
	基础信息	接口权限	稳定性管理	应用发布	
可使用范围 添加可使用人员,用于开发过程中体验与测试(开发版本最多20人可见) draven ×					
应用发布 发布后,该应用将会出现在钉钉的工作台上,企业组织内部的用户将会看到该应用。					

- 6. 打开钉钉, 打开工作台, 找到应用即可单点成功
 - ⑦ 说明

第一次点击应用进行登录的时候,需要绑定IDaaS的账户。

备注: 若提示 IP 不在白名单内,则需要在钉钉开放平台上对应应用开发管理 > 服务器出口IP 中添加 上对应的IP地址。

1.6. 短信OTP认证登录

通过 IDaaS 认证源能力,配置使用短信接收OTP码进行认证登录 IDaaS 平台。

前提条件

- 1、使用短信验证码登录的账户必须在IDaaS平台填写了手机号
- 2、管理员开启了短信网关 (配置阿里云短信服务)

? 说明

云上 IDaaS 内置了阿里云短信网关,可跳过该步骤。如果您希望使用第三方短信服务提供商的短信网关。也可以在 安全设置-短信配置中进行配置。

添加短信验证码认证源

- 1. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
- 2. 在左侧导航栏中,点击认证 > 认证源。在认证源页面,点击右上角的添加认证源按钮。

= (-) 阿里云				Q、搜索文档、控制台、API	、解決方面和記 義用 工単 醫禽 企	业 支持 首网 🖾 🗘 🗑 🖄 👹				
概范	认证源					添加时形认证题 添加认证题				
快速入门	113700					×				
应用 ^ 应用列表	✓ 本平台支持企业使用不同的外部认证 由用认证源后并配量完成后,平台会分	Winter 本学を支付を比較用不開始が時い注重(加大台市用度三方以近方式動発展が中)、可修成公司業業成品中使用不同的以近方式、和DB、LDAP、1)利日時等。 自用以近面合件経験和成点、平台会大社会业用や重要的使用具体的以近源主以近。								
添加应用										
)) 第一 へ	搜索认证源			<u>्</u>						
形力管理	认证题名称	认证源ID	自定义登录	创建时间	状态	操作				
分與管理	微信开放平台扫码整录	20200313110953GDMJ2Dy8pewechat	뮲	2020-04-01 14:55		停改 洋橋 日志 新除				
WE ^	短信验证码登录-wi	20200313110953GDMJ2Dy8pesms2	뮲	2020-03-20 16:35	\checkmark	洋橋 日志 翻除				
WIER	短信验证码登录	20200313110953/3/DMJ2Dv8nesms1	8	2020-03-20 15:11	\sim					

3. 选择短信验证码登录认证源, 点击添加认证源

 \times

图标	认证题名称	标识	描述	操作
支	支付宝登录	alipay	使用支付宝登录	添加认证原
>	们们做应用登录	ddtalk_micro	使用们们微应用整录	添加认证源
5	設信开放平台扫码登录	wechat	通过微信开放平台实现扫码登录	添加认证源
>	初初時發展	ddfalk	使用钌钌扫码登录	添加认证原
LDAP	LDAP	Idap	使用LDAP(的ADAW)进行认证	添加认证源
	短信验证码登录	sms	使用坦信验证码登录系统	添加认证源
>-	Connector語行认证	connector_delegate	Connector的托认证	添加认证源

4. 配置短信认证源参数,并点击保存

添加认证源 (短信验证码登录)

* 认证源ID	20200313110953GDMJ2Dy8pesms3
	认证源ID,由系统生成
*认证源名称	短信验证码登录
*短信验证码有效期	2
	短信验证码在认证过程中的有效期,单位分支,默认2分钟。
是否显示	
	在登录页展示认证源图标
	提交 取消

5. 添加完成后,在认证源列表中启用它

认证原					350011111.tit28 35001.tit28
认证原	2度(即允许使用第三方认证方式登录账户), 可根据公司零 5元许企业用户登录时使用具体的认证课去认证。	要添加并使用不同的认证方式,如	DDB, LDAP, \$T\$77H####,		x
搜索认证原			Q		
认证源名称	认证题 ID	自定义登录	创建时间	状态	操作
短信验证码整录	20200313110953GDMJ2Dy8pesms3	2	2020-04-26 09:52		修改洋橋 日志 教験

短信OTP码认证登录

成功添加短信认证源后,在用户登录页会出现短信认证源图标,用户即可使用短信验证码认证登录IDaaS。

1. 通过浏览器访问云盾 IDaaS 用户 Portal 地址(线下产品直接访问登录页)。

? 说明

该地址由IT管理员提供。IT管理员可以在云盾IDaaS实例列表中查看用户访问的Port al地址。

(-)	管理控制台						肖息 ¹¹⁴ 费用	工单	备案	企业	支持与服务		简体中文	()
	IDaaS	实例列表									云命令行	(Cloud Shell)	× 893	EIDaaS
	实例列表	状态: 全部 🗸					_				_			
		实例ID/名称	状态	規格授权	创建时间	到期时间	用户访问的P	ortal的sso	也址		用户访问的Po	rtal的api地址		操作
		Anne a contract, and 1,4004	运行中	基础版	2019年4月8日	2019年5月9日	- advection	login.aliyu	nidaas.cc	m	and a second second second	oi.aliyunidaas.c	om	管理
												< 上一页	127	一页 >

2. 点击短信认证源图标

简体中文	扫码登录更便逮	8
ID		
阿里云		
请输入账户 / 邮箱 / 手机号		
请输入密码		
请输入验证码	~8E9E'	
	忘记密码	
提交		
注册		
第三方认证登	录	
	\mathbf{D}	

3. 输入手机号和图片验证码获取短信验证码,再输入获取到的短信验证码即可登录IDaaS平台。

❷ 短信验证码已发送,说	青注意查收。	
に見ていていた。	t	
166		
0t6t	,०ग्€्т	
请输入手机验证码	59s 后重新获取	
提交		
返回		

1.7. 企业微信扫码登录

本文为您介绍如何在 IDaaS 中添加企业微信认证源,实现企业微信扫码登录 IDaaS。

实现效果

← → C ① 不安全 11.160.136.245/frontend/login#/login	M 阿田永道 🔥 元第记 🎌 医披	aone 🥊 云钉-教主化产品等 🦂 我的印记	ロー☆ 8 8
	商休中文		
	话指输入别约中 / 前结箱 试验输入控约5	iDaas /手机号 · 利ロレー 応記密码 提交	
★ 企业微信登录	# ① 重试	三方以证登录	
saber			
你将登录saber			
确认登录			
取消			

使用流程

- 1) 打开 IDaaS 用户登录页
- 2) 点击选择左下角的【企业微信扫码登录】, 界面显示登录二维码
- 3) 手机移动端打开企业微信,通常和微信一样,默认已登录状态;如未登录,请先登录进入企业微信
- 4) 使用扫一扫功能, 对准屏幕二维码进行扫码登录
- 5) 电脑浏览器显示扫描成功,手机移动端企业微信提示登录信息,点击【确认登录】
- 6) 登录成功,浏览器显示 IDaaS 用户首页

配置流程

实现企业微信扫码登录 IDaaS 功能, 主要有以下 3 个步骤

- 1) 准备工作
- 2) IDaaS 认证源配置
- 3) 企业微信应用配置

准备工作

1.1、IDaaS标准版或专属版

备注说明:免费版不支持该功能,请升级标准版或按需升级至专属版。

1.2、企业微信自建或第三方应用

备注说明:如之前未使用企业微信微应用,则创建新应用即可,具体操作步骤见本文最后 如何创建企业微信 微应用。

1.3、登录 IDaaS IT管理员界面

登录地址: https://yundun.console.aliyun.com 或参考 管理员登录帮助文档

1.4、登录企业微信管理后台

登录地址: https://work.weixin.qq.com/wework_admin/loginpage_wx 可使用微信扫码登录。

IDaaS 认证源配置

2.1、添加认证源

点击导航菜单【认证源】,点击右上角【添加认证源】

统一身份认证	平台						消息 😗	默认管理员 -	切换语言 ~	
概览 快速入门		认证源						添加打打认证源	添加认证源	
应用 应用列表 添加应用	^	↓证源 本平台支持企业使用不同的 启用认证源后并配置完成的	9外部认证源(即允许使用第三方认证方 5,平台会允许企业用户登录时使用具体	式登录账户) , 可根据公司需要添 的认证源去认证。	加并使用不同的认证方式,如 DB、LD	AP、钉钉扫码等。			×	
用户目录 机构及组	^	搜索认证源			Q					
账户管理		认证源名称	认证源 ID	自定义登录	创建时间	状态	操作			
分类管理	^	企业微信扫码登录	testwechat_enterprise	是	2020-08-26 10:55		详惯	日志制除		
认证源	1	钉钉微应用登录	testddtalk_micro	是	2020-08-24 15:47	\checkmark	评價	日志删除		
RADIUS 证书管理		企业微信微应用登录	testwechatenterprise_micro	是	2020-08-20 11:42		修改	(详情)日志制)	余	
授权 权限系统 应用授权	^									
审计	~									
其它管理	~									
设置	~	© 2014-2020 IDaaS 许可证信息							版本:1.7.7-GA	

2.2、添加企业微信扫码登录

找到 企业微信扫码登录 认证源, 点击【添加认证源】

统一认证·第三方认证源接入

应用身份服务

统一身份认证3	平台				消息 🥶 数认管理员	• 切换语言 ~	
概览			Pa Pa Weidar Gaalaan	outent_innero	DUTUES ESTIMATION	A DESIGN OF COMPANY	
快速入门		<u></u>	微信开放平台扫码登录	wechat	通过微信开放平台实现归码登录	添加认证源	
应用 应用列表	^	>	钉钉扫码登录	ddtalk	使用钉钉扫码登录	漆加认证源	
添加应用	^	LDAP	LDAP	ldap	使用LDAP(如AD域)进行认证	添加认证源	
机构及组		BJCA	北京CA数字证书	bjcacert	使用北京CA数字证书认证	添加认证源	
分类管理			短信验证码登录	sms	使用短信验证码登录系统	添加认证源	
认证 认证源	Ŷ	\bigcap	企业微信扫码登录	wechat_enterprise	使用企业微信登录系统	添加认证源	
RADIUS 证书管理		d ™	OIDC 授权码模式	oidc_code	使用 OIDC 授权码模式登录	添加认证源	
授权 权限系统	^	>■	Connector委托认证	connector_delegate	Connector委托认证	漆加认证源	
应用授权 审计	~	4	认证票插件	oidc_code_adapter	使用认证源描件登录	添加认证源	
其它管理	~						
设置	~	© 2014-2020 IDaaS	5 许可证信思			版本:1.7.7-GA	

2.3、填写认证源信息

统一身份认证平台					添加认证源(企业	微信扫码登录)	\times
概范		0	企业微信数应用整要	wechaltenterprise_micro	- 1177510		
快速入门		皮	支付宝登录	alipay	* WEDBID	testwechat_enterprise1 认证题D,由系统生成	
应用			NISZAAD重要	aad	• 认证源名称	企业资信日码整果	
添加应用					▲ 企业ID	清金入CorplD	
用户目录		3	\$7\$7御应用登录	ddtaik_micro		売売値は最適時長〜4000500~55001日合~55000	
形构及组			微信开放平台归码整录	wechat	* AgentID	活動>Agentid 企业做信管理后台→应用管理→自建应用→选择应用→Agentid	
分类管理					· Secret	请输入获取的Secret	
认证	^	3				企业微信管理后台->应用管理->自建应用->选择应用->Secret	
RADIUS		LDAP	LDAP	ldap	• 微信授权城	全业做信管理后台。应用管理。目建应用。选择应用。企业做信度权登录。设置接权回调域	
证书管理		BICS	北京CA数字证书	bjcacert	* 前端回调地址	/frontend/login/#/wechatenterpriseCallback	
授权 权限系统 应用维权		0	NEWINER	sms	是百显示	IDaaS程度认证后重定师到前期的地址,不能为内网地址,示例: http://xxx.xxx.com/trontend/login/WwechatenterpriseCallback或 /frontend/login/WwechatenterpriseCallback	
#st		0	全业微信扫码整要	wechat_enterprise		在登录页展示从证源图标	
其它管理 [●]		ተ	OIDC 授权研编式	oidc_code	账户目动绑定	☑ 开启后,企业簿信成员手机导着在IDeaS中已存在,颜会进行自动关键:不开启,始终进行手动关键	
			ConnectoritifEUUE	connector_delegate		REC NUM	
		4	认证测验件	oidc_code_adapter			
		© 2014-2020 IDaa	aS 许可证信息				

字段说明:

1.认证源 ID: 系统默认生产,不可修改

2.认证源名称:通常填写为,企业微信扫码登录,也可自定义

3.企业ID:企业微信管理后台【我的企业】最下方获取企业ID

4.Agent ID:企业微信管理后台【应用管理】,点击准备好的应用进入,即可看到 Agent ID 信息

○,企业微	信					API文档 联系客服 j
	首页	通讯录	应用管理	客户联系 🎭	管理工具	我的企业
< 返回			sab	er		
		saber < 暂无应用介绍			己居用	
	AgentId Secret 可见范围	JustForTest				编辑
	管理员 应用负责人	2 · · · · · · · · · · · · · · · · · · ·	人,成员即可在企业微信内	管理此应用		
	功能	送消息 III具中的"消息群发"或API发送消	按收消息 操收用户发送的普通》 外部联系人变更回溯	5回以及菜单提作、 导事件信息	令 自动回复 通过检蚊用户的消息,可配置规则进 动问题	世行自

5.Secret: 企业微信管理后台 【应用管理】,点击准备好的应用进入,即可看到 Secret 信息,如上图所示 6.微信授权域:系统默认生成,后续在配置企业微信应用时使用

7.前端回调地址:系统默认生成,无特殊情况,请勿修改

8.是否显示:勾选后会在用户登录页显示企业微信扫码登录 LOGO图标,通常勾选

9.账号自动绑定:勾选后,会将企业微信成员的手机号与 IDaaS 成员的手机号自动关联,不开启则需要手动 绑定,建议勾选

2.4、提交保存

完成企业微信扫码登录认证源的信息填写后,点击【提交按钮】,进行保存。

保存成功后,可在界面看见新添加的企业微信扫码登录认证源

统一身份认证平台	ł						消息 37)	默认管理员 -	切换语言 ~
概览 快週入门		认证源						添加打打认证源	添加认证源
应用 应用列表 添加应用	^	认证源 本平台支持企业使用不同的 启用以证源后并配置完成后,	朴都认证源(即允许使用第三方认证方式 平台会允许企业用户登录时使用具体的	登录账户) , 可根据公司需要添加并使 认证源去认证。	用不同的认证方式,如 DB、LDAP、钉f]扫码等。			×
用户目录 机构及组	^	搜索认证源		٩					
账户管理		认证源名称	认证源 ID	自定义登录	创建时间	状态	操作		
分类管理		企业微信扫码登录	testwechat_enterprise	是	2020-08-26 10:55		详情	日志 删除	
认证源			testddtalk_micro	显	2020-08-24 15:47		详情	日志 删除	
RADIUS 证书管理			testwechatenterprise_micro	是	2020-08-20 11:42	×	修改	详情日志制限	ž.
授权权限系统	^								
应用授权									
审计	~								
其它管理	~								
设置	~	© 2014-2020 IDaaS 许可证信息							版本:1.7.7-GA

企业微信应用配置

3.1、打开微应用

登录企业微信管理后台,点击【应用管理】,点击之前准备好的应用,进入应用管理界面。

3.2、进入企业微信授权登录

在界面的最下方,开发者接口一栏中,点击中间的企业微信授权登录的【设置按钮】

从上作EAL版画人的网页 设置成用主页	可佔加用臺品的原語和意識快速操作集團	將並用四周配置到輕大上具在,万便原瓜 在与客户的聊天中直着和使用,提高服务 效率	
同工作台自定义展示 工作台小语本人口展示力预设模板将式, 可通过APU实践更新内容 当新配置: 未配置 进入			
开发者接口			
已 阿页授权及JS-SDK 可信编译:gopsybrga.login.aliyunidaas. com	② 企业微信授权登录 使用企业绩信带号登录已有的Web网页或 移动APP	全 审批接口 使用企业感情率批批力,在非审批应用内 设置消程,发起审批,还能订阅通知消 息,接收审批状态变化情况。	
制脉动用		i κπ	
关于辨讯 用户	P协议 使用規范 隠私政策 更新日志 臀間 © 1998 - 2020 Tencent Inc. All Rights Reserved	护心 中文 *	5 中 🤊 🕑 🍨 🗃 🐇 🕇 👪

3.3、设置回调域

点击第一个 Web 页面的【设置授权回调域按钮】

5	。企业微信					API文档	联系客服 退出
	首页	通讯录	录 应用管理	客户联系	┣ 管理]	具 [●]	的企业
	《返回		:	企业微信授权登录			
		请配置所需的类别				获取帮助	
		Web网页 使用企业微信扫一扫登录	iOS 嵌入登录分享S	iDK,实现一键登录、内容分享	Android 嵌入 登录 分亭SDK,	实现一键登录、内容分享	
	[设置授权回调域 ?	设置 Bundle	ID 💿	设置该应用签名和	抱名 ②	

填写内容为: 在添加 IDaaS 认证源配置时生成的"网页授权可信域"字段,填写完成后点击保存

Q.企业微信					API文档 联系客服 退出
首页	通讯录	应用管理	春户联系 🎭	管理工具	我的企业
~ 350		企业微信	言授权登录		
	请配置所需的类别				获取帮助
	Web网页 使用企业微信扫一扫登录	IOS 嵌入登录分享SDK,实现		Android 嵌入登录分享SDK, 实现一键登录。	内容分享
	援权回调域 ⑦	设置 Bundle ID ⑦		设置该应用签名和包名 💿	
ſ	保存 取消				
	在工作台稳藏此应用 仅使用"企业改信登录",可隐藏在工作台的入口	1			
	关于腾讯 月	月戸协议 使用規范 際	私政策 更新日志 専助中心	中文 *	
		W 1990 - 2020 Tellicen	i ili. Al Nylis Reserved		

配置完成后,在 IDaaS 使用效果参考文档开头的"实现效果"。

2.移动端扫码登录IDaaS平台

本文为您介绍如何获取并绑定IDaaS的移动端应用-云盾IDaaS,并介绍如何通过移动端扫码登录IDaaS平台。

操作步骤

- 1. 使用普通用户账号登录云盾IDaaS控制台。具体操作请参考普通用户指南-登录。
- 2. 点击右上角的手机图标。使用微信或者其他APP在弹出的界面中,扫描第二个二维码进行下载。

IDaaS统一认证身份平台			¥8 🚺	测试4 -		切换语言 ~
欢迎 · IDaaS						
主导航 ^	<u>二次以证</u>					
首页						
应用管理	如果希望当前用户的登录拥有二次认证的保护,请设置以下西观并保存。					
应用子账户	最否开启					
设置	御奈川原大学 With ADD X III					
我的账户	新闻》和ATATATATATATATATATATATATATATATATATATAT					
服的演用						
我的日志	RATE:					
统一认证身份平台		绸定公司				×
欢迎 · IDaaS	RAGR		10-14-010	er		
			(PT/)/WEIDDO	#9.0E		
主 初加 ^ 首页	Web成用	在 云盾 IDaaS 移动调登录前,非 定功能,扫描下方二峰码进行绑切	l要首先使用移动跳 E.	進行扫码绑定操	作。请使用制	影动跳的扫码绑
此985年 成用子茶/中 2025 ~ 投約/茶/中 二次以狂 投約/茶母 找約日志	Elizabether					
	当能会有研究的修动应用。		dent sol			
			移动端下!	R		
		没有移动腾?	PK 或扫描下方二维	弓下戴。 (如果)	有使用 iOS 對	喻的场景,请点

3. APP扫码绑定公司

在用户登录之前,需要扫描绑定登录的公司。之前若没有绑定过公司,应用界面如下图所示,点击"扫码绑定"扫描公司的二维码来绑定公司。





如果之前已经绑定过一个公司,想要登录到另一个公司的用户。可以在登录界面,点击"免密码登录"左下角的"扫描绑定"来重新绑定公司。

	阿里云IDaaS测试服 条	
	MEAIDUU0/MILMIC/J	
draven		
请输入密码		
	登录	
	 	
	光山时显水	
扫码绑定		
JANSHITZ		
	云盾IDaaS V1.0.2	
	- 阿里云IDaaS测试服务 -	

二维码获取来源:

i. 普通用户点击右上角的手机按钮, 扫描弹出的第一个二维码进行扫码绑定。

应用身份服务

- 绑定公司 | 我的应用 欢迎 · IDaaS 移动端扫码绑定 主导航 免登应用 在 云盾 IDaaS 移动講登录前, 需要首先使用移动講进行扫码绑定操作。请使用练动编述行扫码绑定协能。13届下方二值码进行规定 22 M M 设置 移动端下载 没有移动端? 统一认证身份平台 へ 应用 安全设置 应用列表 添加应用 移动端绑定设置 统一二次认证 策略管理 ~ 用户 账户及组 账户管理 ~ 授权 移动端开发密钥 应用授权 公司移动端绑定二维码 权限系统 Key 回爆業者 Σ ~ 认证 Secret 认证源 证书管理 Radius 移动端是否显示证书信息 × 0.2 扫描二维码绑定证书 🔍 🗙 ~ 审计 C 刷新 操作日志 登录/退出日志 ~ 其他 我的消息 消息管理 公司信息 © 2014-2019 IDaaS 安全设置
- ii. 企业管理员可以在安全设置的"移动端绑定设置"中获取公司的二维码。

4. 打开移动端APP, 绑定完公司之后, 输入用户的账户名和密码并点击登录, 成功进入APP表示登录成功。

	[-] 阿里云
	阿里云IDaaS测试服务
draven	
•••••	•••
	登录
	免密码登录
扫码绑定	

成功的登录一次之后, APP会自动把该账户的证书下载到本地, 下次登录则可使用免密码登录, 直接点击 "免密码登录"即可登录成功。

5. PC端扫码登录功能

打开普通用户登录地址并在登录界面点击右上角二维码切换为扫码登录。打开云盾IDaaS应用,使用扫码功能扫描登录界面的二维码即可登录成功。





完成以上操作,即可实现移动端扫码登录功能。

3.二次认证

本文为您介绍IDaaS的二次认证功能。开启IDaaS的二次认证功能,能够在校验账号密码的同时校验app上的 动态口令或者短信验证码,从而确保用户账号的安全性。

用户开启APP二次认证

登录普通用户开启APP二次认证功能(账户需要登录 云盾IDaaS APP)。

- 功能介绍:用户开启二次认证后,后续登录则需要进行二次认证,可使用APP上的动态口令进行二次验证 登录,或摇一摇手机进行登录,或在APP上进行授权登录。
- 操作步骤:
 - i. 使用普通用户账号登录云盾IDaaS控制台。具体操作请参考普通用户指南-登录。
 - ii. 在用户界面点击左侧导航栏设置中的二次认证。点选开启二次认证,并且认证方式选择移动app认证。

统一认证身份3	平台	
欢迎·IDaaS		二次认证
	^	二次认证 设备管理 新设备申请记录
首页		
应用管理		如果希望当前用户的登录拥有二次认证的保护,请设置以下选项并保存。
应用子账户		是否开启 🔽
设置	^	
我的账户		登录认证方式 移动 APP 认证
二次认证		开启二次认证后,账户将会采用移动APP或者短信认证码进行认证
我的消息		
我的日志		保存

用户在开启二次认证之后的登录界面如下图,用户可以通过手机摇一摇或者在APP上进行授权登录。

登录二次认证
请输入移动端APP中的动态口令
设备不在身边?向管理员发送认证码

用户也可以在输入框中输入APP中的动态口令进行登录。



用户开启短信二次认证

登录普通用户开启短信二次认证(该账户必须绑定手机号)。

- 功能介绍: 用户开启短信二次认证后, 使用短信验证码作为二次认证的凭据进行登录。
- 操作步骤:
 - i. 使用普通用户账号登录云盾IDaaS控制台。具体操作请参考普通用户指南-登录。
 - ii. 在用户界面点击左侧导航栏设置中的二次认证。点选开启二次认证,并且认证方式选择短信认证码认
 证。

统一认证身份	平台	
欢迎 · IDaaS		二次认证
主导航 首页	^	
应用管理		如果希望当前用户的登录拥有二次认证的保护,请设置以下选项并保存。
应用子账户		是否开启 🔽
设置	^	
我的账户		登录认证方式 短信认证码认证
二次认证		开启二次认证后,账户将会采用移动APP或者短信认证码进行认证
我的消息		
我的日志		保存

用户在登录IDaaS时, IDaaS会发送短信认证码到用户的手机中, 用户在输入框中输入短信认证码, 完成二次认证, 即可登录。

请输入短信认证码 短信认证码已发送至您的手机,请输入认证码,完成二次认证
未收到短信?重新发送
如有问题请联系管理员

统一二次认证功能

管理员开启或关闭统一二次认证。

- 功能介绍:
 - i. 若管理员开启统一二次认证,则所有的用户登录均需要进行二次认证(APP二次认证或短信二次认证)。若关闭统一二次认证,则所有的用户登录都不需要二次认证。

- ii. 若管理员开启允许用户关闭个人二次认证功能,则用户登录后,可关闭二次认证。若管理员未开启允 许用户关闭个人二次认证功能,则用户登录后,不能关闭二次认证。
- 操作步骤:
 - i. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
 - ii. 管理员在左侧导航栏中点击安全设置,点击统一二次认证。然后通过勾选来开启或关闭统一二次认证 功能和允许用户关闭个人二次认证功能。

统一认证身份平台		
^ 应用	安全设置	
应用列表		
添加应用	移动端绑定设置 统一二次认证	策略管理
~ 用户		
账户及组		
账户管理		
△ 授权	如果希望所有用户的登录都拥有二	二次认证的保护,请设置以下选项并保存。
应用授权	是否开启统一二次认证	
权限系统		
~ 认证	允许用户关闭个人二次认证	
认证源		若不勾选,则用户无法禁用自己处于启用状态的二次认证。
证书管理	登录认证方式	短信认证码认证
Radius		开启二次认证后,账户将会采用移动 APP 或者短信认证码进行认证。
^ 审计		
操作日志		保存设置
登录/退出日志		
^ 其他		
我的消息		
消息管理		
公司信息		
安全设置	© 2014-2019 IDaaS	

如果管理员开启了统一二次认证功能,并且关闭了"允许用户取消个人二次认证"功能,则用户取消 二次认证会失败,并且提示"公司不允许用户关闭二次认证"。

统一认证身份	评台		
欢迎·IDaaS		二次认证	 ▲ 公司不允许用户关闭二次认证
主导航	^		
首页			
应用管理		如果希望当前用户的登录拥有二次认证的保护,请设置以下选项并保存。	
应用子账户		是否开启	
设置	^		
我的账户		登录认证方式 短信认证码认证	
二次认证		开启二次认证后,账户将会采用移动AP	P或者短信认证码进行认证
我的消息			
我的日志		保存	

通过上述步骤,实现了用户登录二次认证功能。

4.实人认证

IDaaS支持接入阿里云实人认证功能,进一步为客户提供平台价值,提高身份验证的安全与便捷。

开启实人认证

- 1. 参考实人认证接入流程-准备工作开通实人认证服务,并配置实人认证场景。
- 2. 在阿里云AK管理平台获取用户的Access Key ID与Access KeySecret。
- 3. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
- 4. 在左侧导航栏, 点击设置 > 安全设置。
- 5. 点击 实人认证 页签, 在页面上进行实人认证的配置。

快速入门	^	安全设置		Â
应用 应用列表	^	移动谱绑定设置 统一二次认证	登录任册 策略管理 自动同步责户配置 短倍配置 邮件配置 风险识别服务配置 <u>实人以是</u> 人能识别 云产品 AD 以正	
添加应用				
账户	^			
机构及组		每个租户只能配置一个实人认证该	<u>分置</u>	
账户管理		实人认证厂商	阿里云	
分类管理				
认证	^	* AccessKey	LTA4F/VBPgC	
认证源			服务编调用阿里云实人认证AP时使用	
RADIUS		* AccessSecret		
证书管理			服务编调用阿里云实人认证AP时使用	
授权	^			
权限系统		 场景标识 	idaas-basic-realname	
应用授权			场關的唯一标识符,后端能入时需要	
审计	~	启用		
其它管理	~			
设置	^		存存进	88

i. 实人认证产商选择阿里云

- ii. 将获取的用户Access Key ID与Access KeySecret填写到对应位置
- iii. 填写场景标识



iv. 启用功能并点击保存设置。

完成上述步骤,即可开启实人认证功能

用户进行实人认证

前提条件

管理员开启并配置了实人认证功能

操作步骤

- 1. 用户登录移动端云盾APP。具体操作请参考用户指南-移动端登录。
- 2. 在我的设置页面, 点击安全中心

내 中国联通 🗢	14:50	72%
	我的设置	
	で に す に の し し し し し し し し し し し し し	
✓ 安全中心		>
〕 关于		>
	退出	
我的应用	東の	全 我的设置



4. 实名认证成功后,可在管理员页面查看对应账户的实名认证信息。

ļ	账户管理 / 账户详情					
	← 账户详情 ()				
	账户信息 已授权应	如用 应用子账户 隶属于组织机构	设备 报表	实名认证信息		
实	名认证信息					
	姓名	林	性别	男	民族	汉
	身份证号	3501811	地址		签发机构	
	证件有效开始时间	20151225	证件有效结束时间	20251225		

5.人脸识别

IDaaS支持接入阿里云实人认证服务的活体人脸验证功能,进一步为客户提供平台价值,提高身份验证的安全与便捷。用户通过实人认证后,可以扫脸免密登录到移动端,也可以使用扫脸完成PC端登录的二次认证。

启用人脸识别

操作步骤

- 1. 根据文档,开启并进行实人认证。
- 2. 参考活体人脸验证接入流程-准备工作, 配置活体人脸验证场景。
- 3. 在阿里云AK管理平台获取用户的Access Key ID与Access KeySecret。
- 4. 以IT管理员账号登录云盾IDaaS管理平台。具体操作请参考 IT管理员指南-登录。
- 5. 在左侧导航栏, 点击设置 > 安全设置。
- 6. 点击 人脸识别 页签, 在页面进行人脸识别的配置

快速入门	安全	殳置											
应用 应用列表	^ 移动道	端绑定设置	统一二次认证	登录/注册	策略管理	自动同步账户配置	短信配置	邮件配置	风险识别服务配置	实人认证	人脸识别	云产品 AD 认证	
添加应用													
账户	^												
机构及组	N	脸识别厂商		阿里云									
账户管理													
分类管理	* Ac	cessKey		LTAI4FrVBPg									
认证	~			版夯實调用的里	云头入认业APII	19102.AB							
认证源	* Ac	cessSecret		•••••	•••••	•••••							
RADIUS				服务端调用阿里	云实人认证APIB	付使用							
证书管理	* 场:	景标识		FvBioOnly									
4FE #7				场景的唯一标识	符,后端接入时	需要							
初期系统		次认证											
र्वेग्रसम्बद्धाः				开启此功能,用	户登录PC端时常	\$P\$要使用人脸识别进行二;	欠认证						
MANUTA													
审计	* 启	用											
其它管理	~			肉方沙平									
设置	^			林井城山									

- i. 人脸识别厂商选择阿里云
- ii. 将获取的用户Access Key ID与Access KeySecret填写到对应位置
- iii. 填写场景标识

? 说明 均	汤景标识为用户在 <mark>实人认证控制台</mark> ,新增活体人脸验证场景时填写的场景标识
云盾·实人认证	接入及设置
数据统计	实人认证 活体人脸验证 人脸比对
接入及设置	
实人认证查询	IDaaS活体人胎验证 IDaaS人胎验证 FvBioOnly IDaaS-FVBioOnly
通用设置	认证方案: FVBioOnly 详细说明 最后编辑: 2020-03-25 16:10:14
	此认证场景需上传要集成服务的应用,然后下载生成的认证SDK 获取认证SDK 帮助文档
iv. 根据需求开启或关闭二次认证

⑦ 说明 开启人脸识别-二次认证功能后。如果用户开启了APP二次认证,在登录PC端时需 要进行扫脸

v. 启用功能并点击保存设置

通过人脸识别免密登录到移动端

操作步骤

- 1. 用户登录移动端云盾APP。具体操作请参考用户指南-移动端登录。
- 使用移动端进行实人认证,操作步骤可参考用户进行实人认证。如果已完成实人认证,可以跳过该步骤。
- 3. 在安全中心开启证书免密登录。

⑦ 说明 用户账户首次登录移动端时会自动下载移动端证书,并开启证书免密登录功能。如果没有下载成功,可以在PC端管理员页面认证>证书管理页面重置账号证书,然后手动在安全中心开启证书免密登录。



4. 点击人脸识别,开启人脸识别功能



完成上述步骤后,用户可以在app登录页点击免密码登录,使用人脸识别免密登录到移动端。



阿里云 IDAAS

请输入邮箱/手机号/账户名称

请输入密码

登录

免密码登录

扫码绑定

云盾IDaaS V1.6.2 - 阿里云 IDAAS - 人脸识别

点击图标开启人脸验证

使用人脸识别进行二次认证

操作步骤

- 1. 用户登录移动端云盾APP。具体操作请参考用户指南-移动端登录。
- 使用移动端进行实人认证,操作步骤可参考用户进行实人认证。如果已完成实人认证,可以跳过该步骤。
- 3. 在移动端开启人脸识别功能。
- 4. 开启用户开启APP二次认证,可以参考APP二次认证。

完成上述步骤后,用户登录pc端登录进行二次认证时,需要在移动端进行人脸识别的安全验证。验证通过 后,才可以登录PC端。

6.添加Radius配置

本文介绍IT管理员如何在云盾IDaaS控制台添加Radius配置。

背景信息

RADIUS(Remote Authentication Dial In User Service,远程用户拨号认证系统)是一种用于在需要认证其 链接的网络访问服务器(NAS)和共享认证服务器之间进行认证、授权和记帐信息的文档协议。

RADIUS 服务器负责接收用户的连接请求、认证用户,然后返回客户机所有必要的配置信息以将服务发送到用户。

IT管理员可以在云盾IDaaS中添加Radius,实现OTP登录VPN、连接WI-FI等。

操作步骤

- 1. 以IT管理员账号登录云盾IDaaS控制台。
- 2. 在左侧导航栏,单击认证 > Radius。
- 3. 在Radius页面, 单击新建 Radius。
- 4. 在添加Radius页面,完成以下配置:

② 说明 配置好Radius各属性值,下载Radius config配置文件,并将其与Radius服务器一起使用,可实现OTP登录VPN,连接Wi-Fi等。

配置	描述
Radius名称	为Radius命名,该名称必须保持唯一。
Radius认证端口	Radius认证端口,默认为1812。
Radius计费端口	Radius的计费端口,默认为1813。
Radius SharedSecret	Raduis的共享密钥,10位及以上字符串组合。
Radius连接超时时间	Radius连接超时时间,单位为毫秒(ms)。默认值为 10,000,即10秒。

配置	描述		
	Radius 服务器 在当前系统进行认证的方式,可选值: 账号 OT P 账号 密码 账号 (密码 OT P) 账号 密码 (LDAP或其它数据库)。 		
	⑦ 说明 若选择该方式,需要在IDaaS中添加 对应的认证源并开启。		
Radius认证方式	其他짜罟·		
	 All E L L 6 启用Radius计费功能:是否启用Radius计费功能。 Radius 服务器默认作为认证服务器使用,不启用 Radius计费功能。 		
	 • 授权公司所有账户:是否授权公司所有账户登录该 Radius。若不授权,可通过分配组来进行细粒度授 权。 • 支持账户硬件OTP:若勾选,如果账户有硬件 OTP,则允许其使用。 		
硬件 OTP 允许误差	支持硬件OTP时,配置硬件OTP的时间误差周期。取值 范围:0-10。默认是2,即前后两周期范围内OTP码都 允许。		
IDaaS平台服务器地址	公司所在的 IDaaS 平台服务器地址。		
Radius Vendor	选择Radius供应商,可选值: 未知 华为 思科 WISPr 		
备注	备注信息。		

5. 单击**新建RADIUS**,填写radius名称,点击确定即可。

\times

新建 RADIUS

说明:配置好 R 接 Wi-Fi 等。	ADIUS 各属性值,下载 RADIUS 配置文件 并将其与 RADIUS Server 一起使用,可实现 OTP 登录 VPN,连		
*RADIUS 名称			
	RADIUS名称,需唯一		
*RADIUS 认证端	1812		
	认证端口, 默认 1812		
*计费端口	1813		
	计费端口, 默认 1813		
*RADIUS	8cFWnxOEngNxPVHH		
SharedSecret	RADIUS SharedSecret, 长度至少 10 位		
*连接超时时间 10000			
	RADIUS 连接超时时间,单位: 毫秒 (ms), 默认 10000 毫秒		
*认证方式	账号+OTP ~		
	RADIUS 服务器 在当前系统进行认证的方式。若选择「账号+密码(LDAP或其它数据库)」,需要在系统中添加 对应的认证源并开启。		
启用 RADIUS 计 费功能	□ RADIUS 服务器 默认作为认证服务器使用,不启用 RADIUS 计费功能		
立刻授权所有账 户	■ 是否授权公司所有账户登录该 RADIUS,若不授权,可通过分配组来进行细粒度授权		
支持账户硬件 OTP	☑ 支持账户硬件 OTP		
硬件 OTP 允许误 差	1 硬件OTP的时间误差周期, 默认 2 (范围: 0-10)		
*IDaaS 平台服务	https://iefcgwocbr.login.aliyunidaas.com/		
譜地址	公司所在的 IDaaS 平台服务器地址		
RADIUS 服务提	和 ~ ~		
供問	请选择 RADIUS Vendor,若不关心则使用默认即可		
备注	内容		
	备注 "		
	新建RADIUS		

6. linux服务器上部署RADIUS Server。

- 在IDaaS页面下载 RADIUS Server 安装包
- 安装包中有安全部署文档说明,直接使用/run.sh 命令启动, 不需要编译

					• • • •	
RADIUS						
RADIUS 使用 RADI 请 点击这	(远程用户拨号认证系线 US (Remote Authenticatio 里 → 載 IDaaS RADIUS S	充) nn Dial In User Service,远转 erver 安装包,并配合列表中	程用户拨号认证系统)可以实现x RADIUS 可下载的配置文件使用	功防火墙、堡垒机、Wi-Fi 引。	等设备的统一认证。	
搜索 RADIUS					Q	
RADIUS 名称	认证端口:	计费端口	连接超时时间	认证方式	RADIUS 服务提供商	启用
					暂无数据	

FAQ

1. 使用radius认证提示 Invalid username

请排查 sharedsecret 参数是否添加正确。

2.显示下图报错内容

java.lang.IllegalStateException: aesDecrypt error
at com.idsmanager.oidc.OIDCUtils.aesDecrypt(OIDCUtils.java:156)
at com.idsmanager.oidc.OIDCUtils.aesDecrypt(OIDCUtils.java:129)
at com.idsmanager.oidc.OIDCUtils.aesDecrypt(OIDCUtils.java:168)
at com.idsmanager.radius.infrastructure.IDPOTPCodeRetriever.parseToResult(IDPOTPCodeRetriever.java:118)
at com.idsmanager.radius.infrastructure.IDPOTPCodeRetriever.lambda\$retrieve\$0(IDPOTPCodeRetriever.java:90)
at com.idsmanager.commons.utils.httpclient.HttpClientExecutor.executeWithException(HttpClientExecutor.java:11
7)
at com.idsmanager.radius.infrastructure.IDPOTPCodeRetriever.retrieve(IDPOTPCodeRetriever.java:86)
at com.idsmanager.radius.IDaaSRadiusServer.accessRequestReceived(IDaaSRadiusServer.java:109)
at org.tinyradius.util.RadiusServer.handlePacket(RadiusServer.java:477)
at org.tinyradius.util.RadiusServer.processRequest(RadiusServer.java:432)
at org.tinyradius.util.RadiusServer.listen(RadiusServer.java:377)
at org.tinyradius.util.RadiusServer.listenAuth(RadiusServer.java:334)
at org.tinyradius.util.RadiusServer\$1.run(RadiusServer.java:137)
Caused by: org.jose4j.lang.InvalidAlgorithmException: A256KW is an unknown, unsupported or unavailable alg algorithm
(not one of [RSA1_5, RSA-0AEP, RSA-0AEP-256, dir, A128KW, ECDH-ES, ECDH-ES+A128KW, PBES2-HS256+A128KW, A128GCMKW]).
at org.jose4j.jwa.AlgorithmFactory.getAlgorithm(AlgorithmFactory.java:52)
at org.jose4j.jwe.JsonWebEncryption.getKeyManagementModeAlgorithm(JsonWebEncryption.java:151)
at org.jose4j.jwe.JsonWebEncryption.decrypt(JsonWebEncryption.java:181)
at org.jose4j.jwe.JsonWebEncryption.getPlaintextBytes(JsonWebEncryption.java:79)
at org.jose4j.jwe.JsonWebEncryption.getPlaintextString(JsonWebEncryption.java:72)
at org.jose4j.jwe.JsonWebEncryption.getPayload(JsonWebEncryption.java:87)
at com.idsmanager.oidc.OIDCUtils.aesDecrypt(OIDCUtils.java:154)
10 metro

是因为使用的算法 Java不支持,需要更新JDK或 JRE下的jce 配置。

3. Radius 服务器部署在内网,但是可以访问到公网的IDaaS,是否可以这样部署。

可以。Radius通过调用IDaaS API实现认证。