

MaxKey 与 Atlassian Jira

单点登录集成指南

1. MaxKey 介绍

MaxKey 社区专注于身份安全管理(IM)、单点登录(SSO)和云身份认证(IDaaS)领域, 将为客户提供企业级的身份管理和认证, 提供全面的 4A 安全管理(指 Account, Authentication, Authorization 和 Audit)。

为企业提供社区版 IAM 产品, 减少企业建设 IAM 的成本; 同时提供企业版的 IAM 咨询和技术支持, 从而提高客户体验和降低企业内部的自开发成本。

MaxKey 单点登录认证系统, 谐音为马克思的钥匙寓意是最大钥匙, 是**业界领先的 IAM 身份管理和认证产品**; 支持 OAuth 2.x/OpenID Connect、SAML 2.0、JWT、CAS、SCIM 等标准协议; 提供简单、标准、安全和开放的用户身份管理(IDM)、身份认证(AM)、单点登录(SSO)、资源管理和权限管理等。

官方网站地址: <https://www.maxkey.top/>

2. Atlassian Jira 介绍

JIRA 是 Atlassian 公司出品的项目与事务跟踪工具, 被广泛应用于缺陷跟踪、客户服务、需求收集、流程审批、任务跟踪、项目跟踪和敏捷管理等工作领域。

JIRA 中配置灵活、功能全面、部署简单、扩展丰富, 其超过 150 项特性得到了全球 115 个国家超过 19,000 家客户的认可。

官方网站地址: <https://www.atlassian.com/software/jira>

3. Jira 安装配置

3.1. Jira 安装

请参照官方文档

<https://confluence.atlassian.com/adminjiraserver0813/installing-jira-applications-1027137422.html>

安装路径 D:\MaxKey\3party\Jira8.13.10

数据路径 D:\MaxKey\3party\Jira8.13.10_data

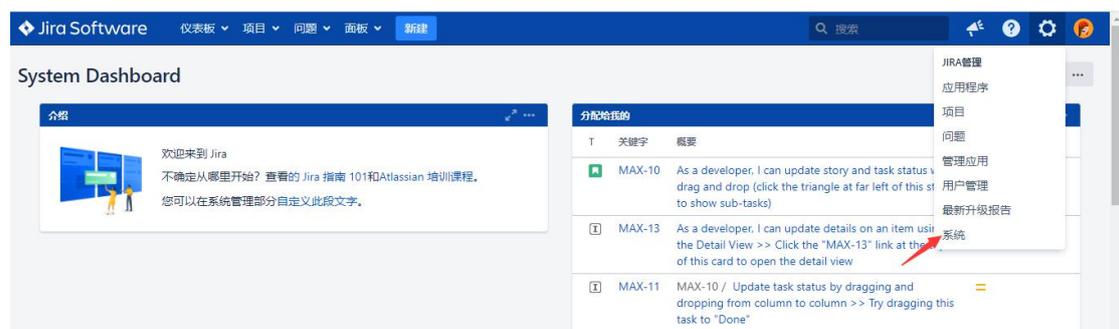
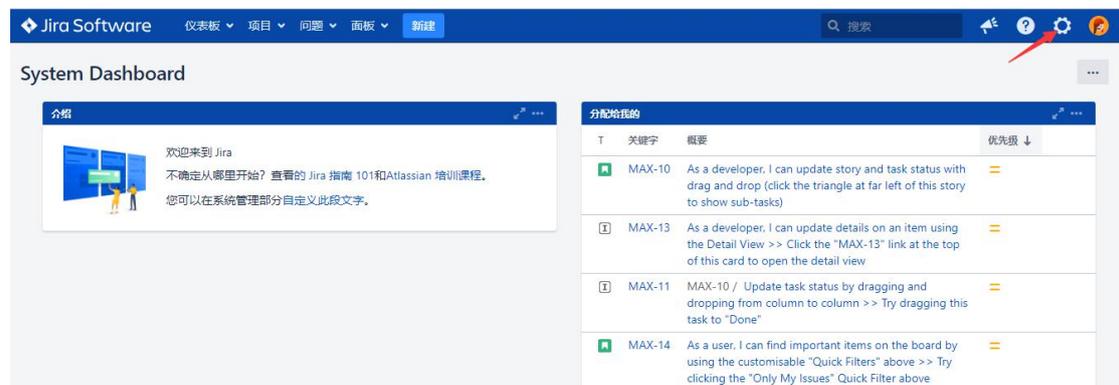
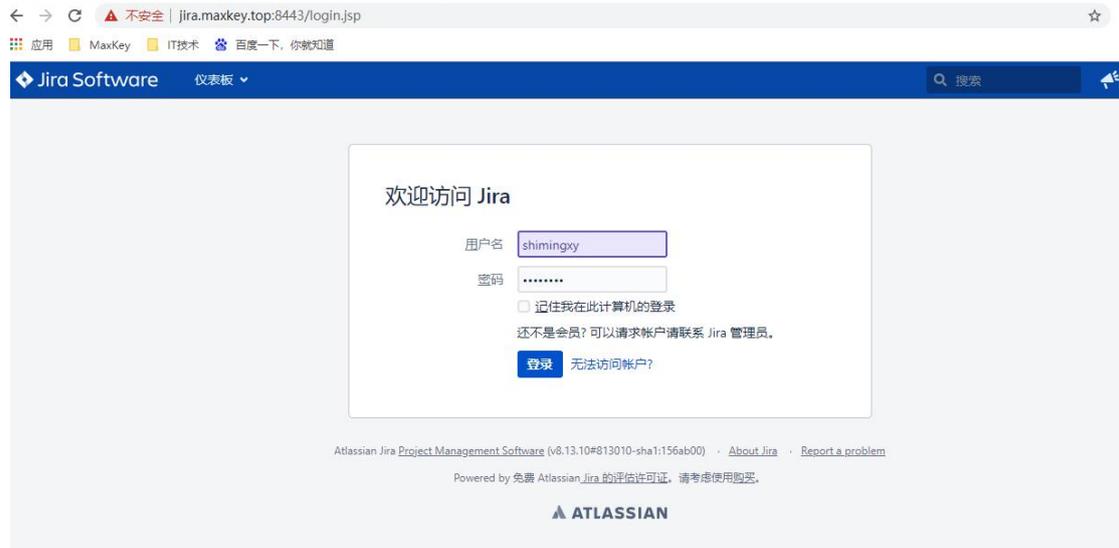
3.2. Jira 启动 https

修改 D:\MaxKey\3party\Jira8.13.10\conf

```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11Protocol"
    maxHttpHeaderSize="8192" SSLEnabled="true"
    maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
    enableLookups="false" disableUploadTimeout="true"
    acceptCount="100" scheme="https" secure="true"
    keystoreFile="D:/MaxKey/3party/Jira8.13.10/conf/maxkeyserver.keystore"
    keystorePass="maxkey"
    clientAuth="false" sslProtocol="TLS" useBodyEncodingForURI="true"/>
```

3.3. 认证配置

配置认证服务，进入 **Jira**，具体配置入下



一般设置

Jira Software 仪表盘 项目 问题 面板 新建

管理 搜索Jira管理功能

应用程序 项目 问题 管理应用 用户管理 最新升级报告 系统

一般配置 高级设置 编辑设置

寻找更多的管理工具
Jira 移动应用

系统支持
系统信息
监测信息
JMX监控
数据库监控
完整性检查程序
日志和分析
调度程序详情
故障诊断和支持工具
审核日志

设置

一般设置

标题	Jira
运行模式	私有
最大尝试验证登录次数	3
登录时需要验证码	关
基本URL	https://jira.maxkey.top:8443
邮件发件人	\$(fullname) (Jira)
介绍	

国际化

基本 URL 更改为 <https://jira.maxkey.top:8443>

SAML 单点登录配置

一般配置

寻找更多的管理工具
Jira 移动应用

系统支持
系统信息
监测信息
JMX监控
数据库监控
完整性检查程序
日志和分析
调度程序详情
故障诊断和支持工具
审核日志
集群
安全
项目角色
全局权限
密码策略
用户会话
SSO 2.0

配置用户登录方式

身份验证方法
SAML单一登录
用户使用SAML身份提供者登录。

SAML SSO 2.0设置

单一登录发行者*
https://sso.maxkey.top/maxkey/saml
您的身份提供程序的实体 ID。例如 https://www.example.com/ab123

身份提供者单一登录URL。*
https://sso.maxkey.top/maxkey/authz/saml20/632279563832918016
您的提供商提供的SAML 2.0 SSO URL。例如: https://www.example.com/abc123/sso

X.509证书*
-----BEGIN CERTIFICATE-----
MIIDfjCCAmagAwIBAgIEXIctizANBgkqhkiG9w0BAQsFADCBgDEgMB4GCSqG
SIb3
DQEJARYRc2hpbWluZ3h5QDE2My5jb20xCzAJBgNVBAYTAmNuMQswCQYD
VQQIDAjz
aDELMakGA1UEBwwCc2gxZDzANBgNVBAoMBm1heGtleTEPMA0GA1UECw
wGbwWF4a2V5
复制并粘贴您从提供商得到的整个的X.509证书。

用户名映射*

SSO 2.0

- 记住我登录
- 白名单

问题收集器

用户界面

- 用户默认选项
- 系统仪表盘
- 外观
- 公告栏

富文本编辑器

导入与导出

- 备份系统
- 恢复系统
- 项目导入
- 导入外部系统

电邮

- 外发邮件
- 接收邮件
- 电邮队列

用户名映射*

\${NameID}

用于将 IdP 属性映射到用户名，例如 \${NameID}

把这些Url发给您身份提供者

认定消费者服务URL

https://jira.maxkey.top:8443/plugins/servlet/samlconsumer

观众URL(实体ID)

https://jira.maxkey.top:8443

JIT 调配

即时用户调配让用户可以在通过 SSO 登录到 Atlassian Data Center 应用时自动创建和更新用户。 [了解更多](#)

在登录应用时创建用户

SAML SSO 2.0行为

记住用户登录

无需重新验证即可保存成功的登录历史记录并自动登录用户。

登录模式*

作为辅助身份验证使用SAML

用户将默认使用登录表单登录，他们可以通过身份提供者程序使用单点登录或使用 [此链接](#)

作为首要身份验证使用SAML

在他们访问应用程序登录表时重定向到浏览器用户到 IDP (仍允许 REST 和其它请求)。 [了解更多](#)

4. MaxKey 配置及登录验证

4.1. 应用配置

进入后台“应用管理”，编辑应用

应用管理 首页 / 应用管理

应用名称: 查询 展开 新增 编辑 删除

<input type="checkbox"/>	图标	应用名称	访问协议	类型	供应商
<input type="checkbox"/>		MaxKey管理系统	JWT	MANAGEMENT	MaxKey
<input type="checkbox"/>		招聘管理系统	OAuth_v2.0	HR	MAXKEY
<input type="checkbox"/>		阿里云用户SSO	SAML_v2.0	SAAS	阿里云
<input type="checkbox"/>		腾讯云	SAML_v2.0	SAAS	腾讯
<input type="checkbox"/>		人力资源管理系统	CAS	HR	MAXKEY
<input checked="" type="checkbox"/>		Jira	SAML_v2.0		
<input type="checkbox"/>		华为云	SAML_v2.0	SAAS	华为
<input type="checkbox"/>		阿里云	SAML_v2.0	SAAS	阿里
<input type="checkbox"/>		GitLab	OAuth_v2.0	DEV	GitLab
<input type="checkbox"/>		Teambition(test)	SAML_v2.0	SAAS	上海汇翼信息科技有限公司

显示第 1 到第 10 条记录, 总共 34 条记录 每页显示 条记录 < 1 2 3 4 >

MaxKey v2.9.0 GA
© Copyright 2021 <https://www.maxkey.top/>
Licensed under the Apache License, Version 2.0

配置主要明细入下

应用基本信息			
唯一编码:	632279563832918016	应用密钥:	SNm0MDYwOTlwMjExNTM0MjA3NzMyJu 生成
应用名称:	Jira		
登录地址:	http://jira.maxkey.top:8080/plugins/servlet/easysso/saml		
注册地址:		注册方式:	无
访问协议:	SAML_v2.0	类型:	
图标:		排序:	1
供应商:		供应商网址:	
权限范围:	所有用户	扩展属性:	请选择
适配:	禁用	适配器:	请选择
描述:			

SAML V2.0 认证配置			
SP ACS Uri:	https://jira.maxkey.top:8443/plugins/servlet/samlconsumer		
Entity Id:	https://jira.maxkey.top:8443	SAML MetaData	
Issuer:	https://jira.maxkey.top:8443	Audience:	https://jira.maxkey.top:8443
签名算法:	RSAwithSHA1	摘要方法:	SHA1
Nameid Format:	persistent	Nameid Convert:	原始
Binding:	Redirect-Post	有效期:	300
证书类型:	证书	SAML元数据:	Browse... No file selected.
加密:	不加密		
证书颁发者:	duan	证书有效期:	Fri Aug 22 16:21:15 CST 2031
证书主题:	CN=duan, OU=emwiit, O=yunwei, L=shenzhen, ST=guangdong, C=cn		
保存 关闭			

配置对应关系

序号	MaxKey	参数	备注
1	登录地址	https://jira.maxkey.top:8443/	
2	访问协议	SAML	
3	适配	启用	
4	适配器	SAML 默认适配器	
5	SP ACS Url	https://jira.maxkey.top:8443/plugins/servlet/samlconsumer	
6	Entity Id	https://jira.maxkey.top:8443	
7	Issuer	https://jira.maxkey.top:8443	
8	Audience	https://jira.maxkey.top:8443	
9	签名算法	RSAwithSHA1	
10	摘要方法	SHA1	
11	证书文件	选择 SP 的证书文件	

4.2. 应用访问赋权

如果不在该列表内，可以“新增成员”



添加 Jira



成功后状态

- ☰ 首页
- 👤 机构管理
- 👤 用户管理
- 👤 账号管理
- 🔑 应用管理
- 🔑 访问控制管理
- 👤 组管理
- 👤 成员管理
- 👤 访问权限管理
- ⚙️ 角色权限管理
- ⚙️ 配置管理

访问权限管理

首页 / 组管理 / 访问权限管理

用户组: 系统管理员组
请选择
查询
展开
新增成员
删除成员

☐	图标	应用名称	访问协议	类型	供应商
☐		Jenkins	CAS	DEV	Jenkins
☐		GitLab	OAuth_v2.0	DEV	GitLab
☐		泛微OA	CAS	OA	泛微
☐		阿里云	SAML_v2.0	SAAS	阿里
☐		Token_Based_Simple	Token_Based	E-COMMERCE	MaxKey
☐		Teambition(test)	SAML_v2.0	SAAS	上海汇翼信息科技有限公司
☐		有道云笔记	Form_Based	SAAS	网易
☐		腾讯企业邮箱	Extend_API	OA	腾讯
☐		Jira	SAML_v2.0		

显示第 21 到第 29 条记录, 总共 29 条记录 每页显示 10 条记录

< 1 2 3 >

MaxKey v2.9.0 GA
 © Copyright 2021 <https://www.maxkey.top/>
 Licensed under the Apache License, Version 2.0

4.3. 单点登录验证

重新登录 <https://sso.maxkey.top/maxkey>, 点击“Jira”图标单点登录

MaxKey 统一认证系统

欢迎您: 系统管理员 admin

密码修改
管理
退出

我的应用
设置
我的资料
审计

会话
登录日志
访问日志
管理日志

阿里云用户SSO

腾讯云

人力资源管理系统

Jira

华为云

阿里云

GitLab

Teambition(test)

Jenkins

禅道项目管理

JumpServer 堡垒机

泛微OA