Worktile 企业版安全白皮书

v1.1

Worktile 团队

2016 年 3 月 28 日

目 录

1. 前言

Worktile 是由北京易成时代科技有限公司出品，为互联网时代的企业打造的协作办公平台，支持企业内部沟通、电话会议、任务管理、日程安排、企业网盘和办公应用，连接企业内外部一切服务。

作为一款企业级 SAAS 产品，Worktile 始终把企业数据安全放在第一位，本白皮书会从数据保护、帐号安全和运维几个方面详细介绍 Worktile 在保护企业数据方面的安全措施。

2. 数据保护

Worktile 通过以下各种方式，全力保护企业数据的保密性，完整性，不会丢失以及不会被第三方应用非法爬取。

2.1 核心数据加密

Worktile 对于企业的数据采用分级保护机制，敏感的、重要的数据采用加密存储方式。对于用户密码的处理，大部分软件的处理方式是只在服务端对密码进行哈希存储，Worktile 进行了两次哈希处理，在用户密码提交到服务端之前，在客户端首先进行一次哈希，在服务端再次进行哈希，好处是用户的密码在所有的环节中始终只是哈希值，密码并不会在网络上明文传输。

2.2 多点灾难备份

Worktile 对于企业数据进行了多点灾难备份，备份分布在不同的网段、不同

的地区，这样即便有不可抗拒力产生的灾难，也能够很快的从其他地区的备份中及时恢复。

2.3 爬虫协议处理

Robots 协议（也称为爬虫协议、机器人协议等）的全称是“网络爬虫排除标准”（Robots Exclusion Protocol），网站通过 Robots 协议告诉搜索引擎哪些页面可以抓取，哪些页面不能抓取。Worktile 中只允许搜索引擎抓取博客上由运营人员产品的文章，用户相关的数据都不允许抓取。采用的 robot.txt 文件内容如图 1 所示：

```
User-agent: *

Disallow: /api/
Disallow: /data/
Disallow: /dist/

Allow: /
Allow: /price
Allow: /blog
```

图 1 robot.txt 内容

2.4 SSL/TLS 全程加密

Worktile 数据传输过程中全程使用 SSL/TLS（Secure Sockets Layer，详情请

参考 RFC5246 及 RFC6176），在不采用 SSL/TLS 前数据存在传输存在以下风险：

1） 窃听风险（eavesdropping）：第三方可以获知通信内容

2） 篡改风险（tampering）：第三方可以修改通信内容

3） 冒充风险（pretending）：第三方可以冒充他人身份参与通信

而采用 SSL/TLS 后，这些风险都可以规避：

1） 所有信息都是加密传播，第三方无法窃听

2） 具有校验机制，一旦被篡改，通信双方会立刻发现

3） 配备身份证书，防止身份被冒充

Worktile 中 SSL/TLS 证书见图 2：

图 2 Worktile SSL 证书信息

3. 帐号保护

Worktile 中采用了非常完善的帐号保护机制，主要包括两步验证、登录日志、手势解锁、强制修改密码和远程会话控制。

3.1 两步验证

大多数互联网用户为了方便记忆，喜欢在不同网站使用相同的帐号密码。这就给不法分子可趁之机，一旦他们通过某个渠道获取了企业成员的帐号密码，就可以窃取所有网站的个人信息。如果启用了两步验证将企业成员的移动设备与 Worktile 帐号绑定。每次登录 Worktile，不仅需要输入帐户密码，还需输入移动设备生成的一次性动态验证码。这样，即使登录密码被恶意攻击者猜测到，攻击者由于没有企业成员的移动设备，仍然无法登录 Worktile，如图 3 所示：

图 3 使用洋葱两步验证

3.2 登录日志

在 Worktile 中提供了两种登录日志，对于企业管理者，可以看到企业所有成员的登录记录，使用什么设备，在什么位置登录，以此判断企业成员的帐号是否有登录异常；对于企业成员，可以看到自己的帐号登录情况，以便发现异常登录，及时修改密码，如图 4 所示：

图 4 员工登录日志

3.3 手势解锁

在 Worktile iPhone 客户端和 Android 客户端中，企业成员可以开启手势密码，在每次进入应用时，都需要输入正确的手势图形才能够进入应用，如图 5 所示：

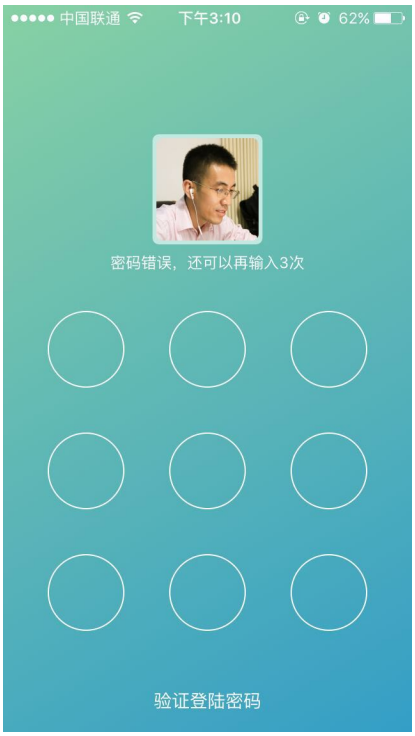

图 5 客户端手势解锁

3.4 远程控制会话

为了防止因为企业成员手机丢失，而导致其他人通过客户端看到企业内部数据；或者是因为在别人电脑上登录了自己的帐号而忘记退出，导致企业内部数据泄漏。Worktile 中提供了远程控制会话功能，员工可以在自己的帐号中退出除了当前浏览器之外的所有会话。这样即便丢失的手机被其他人看到，也无法访问企业内部的数据，如图 6 所示：

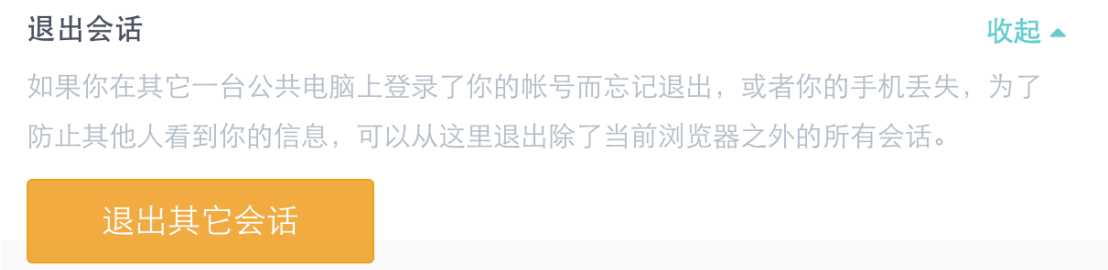

图 6 远程控制会话

4. 运维安全

Worktile 从成立以来一直把运维安全放在最重要的位置，经过几年的改进和完善，在运维管理上已经总结出了一套切实可行的运维流程以及应急灾难处理机制。

4.1 服务器登录授权

Worktile 所有生产环境服务器都采用密钥对登录，无法使用密码登录，密钥对采用公有密钥密码术加密和解密登录信息（基于 2048-bit SSH-2 RSA），只有用户密钥对文件.pem 的人员才可以连接服务器。这种登录授权方式，使得恶意攻击无法通过猜测服务器的用户名和密码来连接服务器。

4.2 分级运维制度

所有能够接触到生产环境服务器的人员，都进行了严格的分级，对于数据中心只有极少数的人员得到授权时才可以访问。Worktile 团队在运维管理上提出了“结对运维”的制度，只要操作生产环境服务器，就需要至少两人同时在场，同时做好每一次操作生产环境服务器的日志。

4.3 网络访问控制

所有生产环境服务器按照逻辑分组之间，使用安全组（防火墙）进行隔离，每个安全组之间的互访都定义了严格的流入和流出规则。所有生产环境服务器都无法通过外部网络直接访问。

服务器软件

4.4 应急灾难处理

Worktile 团队内部组建了一支应急灾难处理分队，由 CTO 直接负责，在遇到问题时，该分队会立即响应，按照灾难应急处理流程及时解决。

5. 安全认证

5.1 可信网站认证

Worktile 已经通过可信网站身份认证，可以在可信网站权威数据库 http://t.knet.cn/index_new.jsp 输入 worktile.com 进行查询。

网站信息 | 安全信息 | 资质荣誉

可信网站 身份验证

可信网站 中网验证

可信网站编码：e160129110108623 50bxmz000000

验证项：

验证深度 ★★★★★

ICP 备案信息 ✓ 域名注册信息 ✓ 工商登记信息 ✓

身份证明信息 ✓ 网站运行监控 ✓ 网站篡改监控 ✓

安全防伪提示：请确认本页面地址以https开头，即应用数据加密传输功能保证信息传输的安全性。
请确认本验证页面水印显示时间为当前访问时间：2016-03-28 11:01
所有可信网站都已收录至 可信网站权威数据库 和 全国网络目录数据库

验证方法说明：该网站已通过中网"可信网站"身份验证，其提交的申请信息经中网（knet.cn）人工审核、权威数据库比对、电话回访等多种方式核验确认。

网站名称：worktile，让工作更简单的协作办公平台。
官网地址：www.worktile.com
ICP备案号：京ICP备13017353号
可信网站有效期：2016-01-29至 2026-01-29

公司名称：北京易成星光科技有限公司
客服电话：400-805-6966
公司注册号：110108015376511
公司注册地址：北京市海淀区北四环中路238号柏彦大厦5层502T
企业类型：有限责任公司(自然人投资或控股)
经营范围：技术开发、技术推广、技术咨询、技术转让、技术服务；计算机技术培训；基础软件服务；应用软件服务；计算机系统服务；数据处理；销售计算机、软件及辅助设备、电子产品、通讯设备；货物进出口、技术进出口、代理进出口。（依法须经批准的项目，经相关部门批准后依批准的内容开展经营活动。）

域名：pro.worktile.com
ICP备案号：京ICP备13017353号

域名：www.worktile.com
ICP备案号：京ICP备13017353号

申请单位经营主体的运营状况、财务状况、信用状况等不在验证范围内。请点击查看验证方法说明。
欢迎公众监督举报，电话：010-58813333、010-96002，邮箱：supervise@knet.cn
如需要更新信息，请登录可信网站验证用户服务平台。

可信网站验证管理机构：北龙中网(北京)科技有限责任公司（KNET）

业务监督机构：中国互联网协会（ISC）
技术支持机构：中国科学院计算机网络信息中心（CNIC）