teambition

最好用的团队协作工具

Teambition 企业版安全白皮书

V1.0

目录

1.前言

Teambition 是国内最领先的团队协作工具，通过帮助团队轻松共享和讨论工作中的任务、文件、分享、日程等内容，让团队协作焕发无限可能。

Teambition 在网页、桌面、移动环境都打造了体验出众的应用，所以你随时随地都可以和团队协作，其 iPhone 应用还被苹果公司评为 2015 年度最佳应用。

作为一款企业级 SAAS 产品，Teambition 始终坚信企业数据安全是重中之重，本白皮书将会从数据安全，账号安全和运维安全几方面详细介绍 Teambition 是如何保护企业数据安全的。

2.数据安全

Teambition 一直在通过以下的各种方式，保护着企业数据的安全性，保密性。

2.1 数据高可用

Teambition 的数据库架构为高可用架构，无单点问题。且还有对应各个延时节点，以保障用户的数据的安全性，保密性。

2.2 异地多机房数据备份

Teambition 对于企业数据进行了多点灾难备份，备份会分布在不同的服务器，不同的地区，不同的机房。这样可以在不可抗力产生的灾难出现时，依旧保障用户数据的安全性，并及时从备份中恢复出来。

2.3 SSL/TLS 全程加密

Teambition 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

Teambition 的 SSL/TLS 证书见图 1：

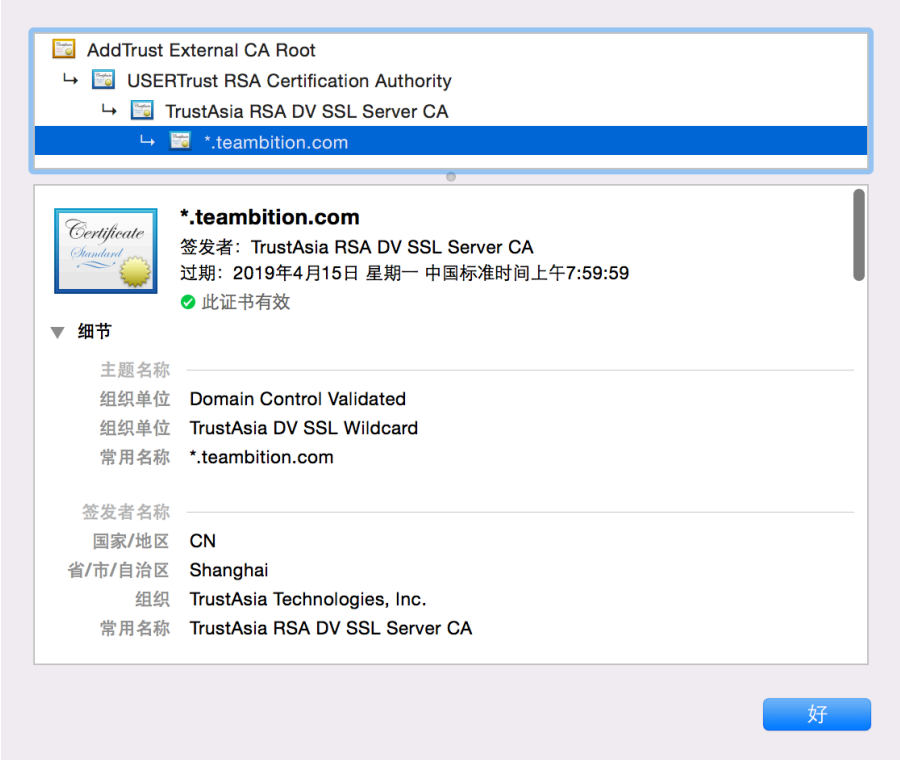

图 1 Teambition SSL 证书信息

3.账号安全

3.1 账号加密算法

Teambition 使用了自研的加密算法，对我们用户的密码进行加密，用户的密码信息存在 Teambition 数据库中的将不是明文的而是通过自研算法加密过后的数据，用户的密码信息将不会遭到泄露。

3.2 两步验证

在互联网时代，非常多的用户为了方便自己使用与记忆，常常在不同网站不同服务上使用相同的账号密码。这类行为非常容易给不法分子可趁之机，现在互联网上非常多的社工库，一旦他们通过某类手段获得了启用成员的用户密

码信息，那么就可以获取到所有网站的个人信息以及有关的企业信息。

如果启用了 Teambition 的两步验证，企业成员的账号将与移动设备进行绑定。每次登录 Teambition 的时候用户不仅需要输入用户密码，还需要输入移动设备生产的一次性动态验证码。这样即使登录密码被恶意攻击者获取，也无法登录 Teambition。如图 2 所示

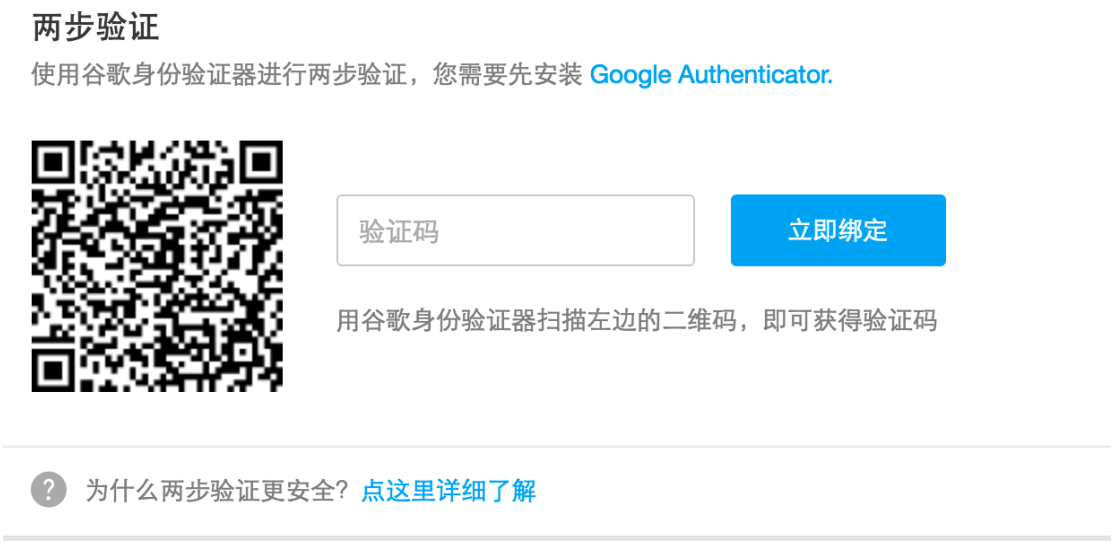

图 2 两步验证

3.3 密码解锁

在 Teambition 的 iPhone 客户端中（Andorid 客户端该功能即将上线），启用成员可以开启登录密码，在每次进入应用的时候，都需要输入正确的密码才能进入应用，如图 4 所示

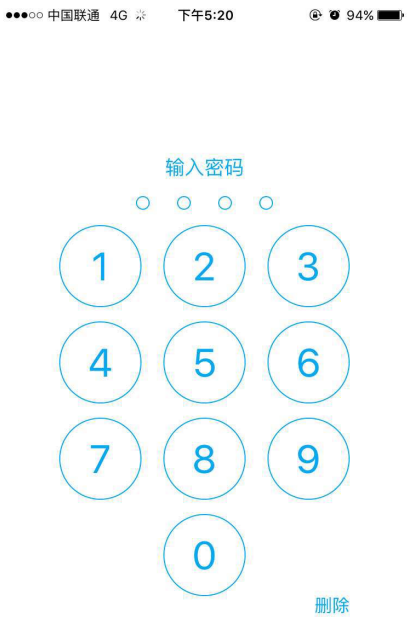

图 4 客户端密码解锁

3.4 远程一键登出

为了防止因为企业成员手机丢失导致他人通过移动客户端看到 Teambition 内关于该企业的内部数据。Teambition 提供了远程登出对应设备的功能，员工可以在自己的账号中登出各个手机端的回话。这样即便手机丢失了，也不会造成企业内部数据丢失，如图 5 所示：

图 5 远程一键登出

4.运维安全

Teambition 一直都对于运维安全十分的重视，在不断的完善与改进中，Teambition 在不断的加强运维安全体系。

4.1 服务器登录限制

Teambition 所有的生产服务器均做了严格的登录与各端口访问限制，在除了我们所指定的 ip 来源以外，其他任何来源的登录都将在最外层的网络层面进行拒绝。使得服务器远离恶意攻击者的暴力破解（猜测服务器用户名密码不断尝试登录）。并且只允许通过 key 登录。

4.2 严格的运维权限控制

Teambition 的生产服务器的访问权限，都进行了非常严格的分级，对于数

据中心来说只有极少数的人员在得到授权时才可访问。各类人员的权限以及对于职责也做了很严格的分级确保服务器环境的安全。

4.3 应急制度

Teambition 内部有一支应急处理小组，直属于 CTO，在遇到问题的时候，我们的应急处理小组将会立刻响应并处理。

与此同时我们会定期进行应急演练，以保持应急状态。应急演练包含如下内容：

1. 精确到每条任务与状态的应急处理
2. 数据多级别备份恢复以及异地备份恢复
3. 灾后应急响应