账号相关

账号安全

产品文档

腾讯云

文档目录

账号安全
MFA设备
什么是 MFA 设备

最近更新时间：2018-02-08 10:57:01

MFA，Multi-FactorAuthentication，即多因子认证，是一种简单有效的安全认证方法。它能够在用户名和密码之外，再增加一层保护。MFA 设备，又叫动态口令卡或 token 卡，是提供这种安全认证方法的设备。目前腾讯云提供两种 MFA设备： 硬件 MFA 设备和虚拟 MFA 设备 。

硬件 MFA 设备

最近更新时间：2018-09-30 15:53:20

硬件 MFA 设备如下图所示，正面的 6 位数动态安全码 30 秒更新一次，背面有该硬件 MFA 设备的序列号。目前该设备仅开放给内测用户使用。

绑定硬件 MFA 设备

1. 登录腾讯云控制台，进入 安全设置，在 MFA 设备那一栏上，单击【绑定】；
2. 经过敏感操作校验，确认当前操作者身份；
3. 选择硬件设备类型；

4.依照页面指引进行绑定操作；
5.单击提交，完成 MFA 设置。

解绑硬件 MFA 设备

1. 登录腾讯云控制台，进入 安全设置，在 MFA 设备那一栏上，单击【解绑】；
2. 经过敏感操作校验，确认当前操作者身份；
3. 完成解绑。

虚拟 MFA 设备

最近更新时间：2018-09-30 15:53:25

虚拟 MFA 设备是一个产生动态安全码的应用程序，它遵循基于时间的一次性密码 (TOTP) 标准(RFC 6238)，可以将虚拟 MFA 设备安装在不同的移动设备上，如智能手机。因此方便用户使用虚拟 MFA 设备。

绑定虚拟 MFA 设备

1. 登录腾讯云控制台，进入 安全设置，在 MFA 设备那一栏上，单击【绑定】；
2. 经过敏感操作校验，确认当前操作者身份；
3. 依照页面指引进行绑定操作；
4. 单击提交，完成 MFA 设置。

解绑虚拟 MFA 设备

1. 登录腾讯云控制台，进入 安全设置，在 MFA 设备那一栏上，单击【解绑】；
2. 经过敏感操作校验，确认当前操作者身份；
3. 完成解绑。

登录保护

最近更新时间：2018-08-14 15:24:18

登录保护指在您进行登录操作的时候，腾讯云会给您增加一层保护。通常情况下，该保护的措施是，在正确输入账号和密码的前提下，还需要额外输入一种能证明身份的凭证。

开启登录保护后，在登录腾讯云官方网站时需要验证身份。这样即使他人盗取您的密码，也无法登录您的账号，能够最大限度地保证您的账号安全。

开启登录保护

登录腾讯云控制台，进入 安全设置，选择敏感操作中的登录保护部分进行设置。

登录保护类型

登录保护类型	作用
开启 MFA 验证	在登录框中输入账号密码后，要进入 MFA 密码输入页面，输入正确的 MFA 密码即可完成登录。
开启手机验证	在登录框中输入账号密码后，要进入手机验证码输入页面，点击获取手机验证码，输入正确验证码即可完成登录。
不开启	不进行二次认证。

操作保护

最近更新时间：2018-08-14 15:24:26

操作保护是指当您进行敏感操作时，腾讯云会给您增加一层保护。通常情况下，开启操作保护后，在您进行敏感操作前，需要先完成身份验证，以确保是您本人操作。
常见的操作场景为控制台敏感操作，需要输入对应的验证码进行二次确认；

开启操作保护

登录腾讯云控制台，进入 安全设置，选择敏感操作中的操作保护部分进行设置。

操作保护类型

登录保护类型	作用
开启 MFA 验证	在控制台进行相关操作时，进入身份验证页面，需要输入 MFA 密码，如果输入 MFA 密码正确，才能完成此操作，否则不能执行动作。
开启手机验证	在控制台进行相关操作时，进入身份验证页面，需要输入手机验证码，如果输入验证码正确，才能完成此操作，否则不能执行动作。

账号密码

最近更新时间：2018-03-05 18:14:14

账号密码是保证您账号安全性最重要的凭证，请您妥善保管，并在条件允许的情况下定期更换。

密码设置建议

1. 至少每 90 天 变更 一次；
2. 新密码不要使用前 3 次用过的密码。

密码复杂度要求

密码需要包含字母、数字、标点符号（如. / _等，除空格外）中的 3 种，8-20 个字符。

邮箱登录安全性要求

1. 同一账号在一天内，有 3 次尝试输错密码登录的机会；
2. 如果输入密码错误超过 3 次之后，需要输入验证码才可请求登录；
3. 如果输入密码错误超过 10 次之后，锁定 24 小时，锁定的开始时间为当天第一次输错密码的时间。