深圳市潮流网络技术有限公司.

GDMS 多因子设备认证

用户手册

目录

1. 概述.....4
2. MFA 设备规格.....4
3. 虚拟 MFA 应用程序下载.....5
4. 启用 MFA 设备.....5
4.1. 启用虚拟 MFA 设备.....5
4.2. 启用硬件 MFA 设备.....8
5. 移除 MFA 设备.....10
6. 常见问题.....10
6.1. MFA 设备丢失或无效.....10

图表

图表 1 ： 访问个人信息页面.....6
图表 2 ： 扫描 MFA 二维码.....7
图表 3 ： 输入 MFA 代码.....8
图表 4 ： 硬件 MFA 设备认证.....9
图表 5 ： 硬件 MFA 设备.....9

表格

表格 1 ： MFA 设备规格.....4
表格 2 ：虚拟 MFA 应用程序.....5

1. 概述

GDMS Multi-Factor Authentication (MFA) 是一种非常简便的最佳安全实践方法，它能够在用户名称和密码之外再额外增加一层保护。启用 MFA 后，用户登录 GDMS 平台时，系统将要求他们输入用户名和密码（第一安全要素），以及来自其 MFA 设备的身份验证代码（第二安全要素）。这些多重要素结合起来将为您的 GDMS 账户设置和资源提供更高的安全保护。

您可以自行购买支持的 硬件设备或虚拟 MFA 设备，为您的 GDMS 账号启用 MFA。

- **虚拟 MFA 设备**

一种在手机或其他设备上运行并模拟物理设备的软件应用程序。
该设备将基于进行了时间同步的一次性密码算法生成一个六位数字代码。在登录时，用户必须在键入来自该设备的有效代码。分配给用户的每个虚拟 MFA 设备必须是唯一的。用户无法从另一个用户的虚拟 MFA 设备代码键入代码来进行身份验证。由于虚拟 MFA 可能在不安全的移动设备上运行，因此，它们可能无法提供与硬件 MFA 设备相同的安全级别。

- **硬件 MFA 设备**

一台硬件设备，基于进行了时间同步的一次性密码算法生成一个六位数字代码。在登录时，用户必须键入来自该设备的有效代码。分配给用户的每台 MFA 设备必须是唯一的。用户无法从另一个用户的设备键入代码来进行身份验证。

2. MFA 设备规格

表格 1： MFA 设备规格

	虚拟 MFA 设备	硬件 MFA 设备
设备	见下表	购买
费用	免费	第三方供应商价格
物理设备规格	使用您现有的智能手机或平板电脑，只要它能够运行支持开放 TOTP 标准的应用程序。	由第三方供应商提供的支持开放 TOTP 标准的设备。 推荐 Microcosm 厂商的设备。
功能	在一个设备上支持多个令牌。	许多金融服务机构和企业 IT 组织采用的同一设备类型。

3. 虚拟 MFA 应用程序下载

在您的手机应用程序商店为您的智能手机安装应用程序。下表罗列了一些适合各种智能手机的应用程序。

表格 2：虚拟 MFA 应用程序

Android	Google 身份验证器；Authy 双重身份验证
iPhone	Google 身份验证器；Authy 双重身份验证
Windows Phone	身份验证器

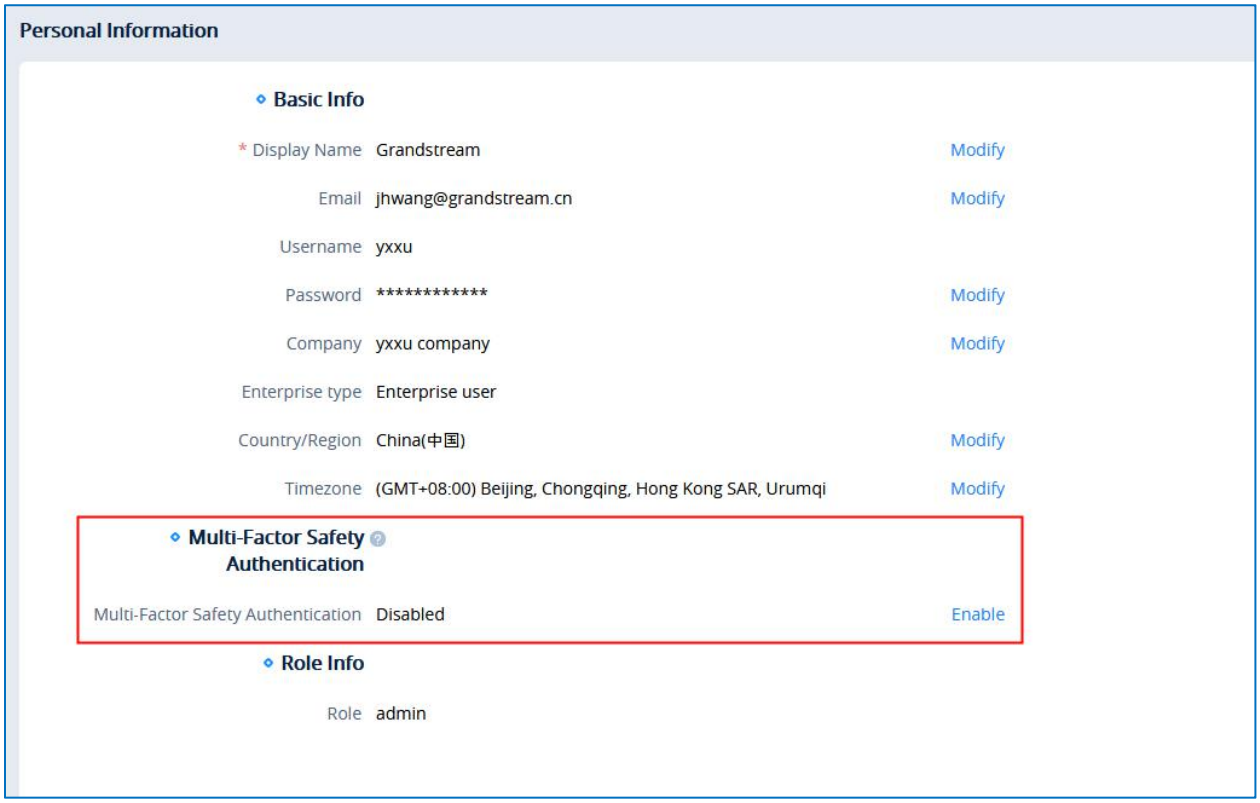
4. 启用 MFA 设备

为增强安全性，我们建议您配置 Multi-Factor Authentication (MFA) 以帮助保护 GDMS 资源。您可以为 GDMS 账号启用 MFA。

4.1. 启用虚拟 MFA 设备

前提：首先在您的智能手机或电脑上安装虚拟 MFA 应用程序（参考【虚拟 MFA 应用程序下载】章节）

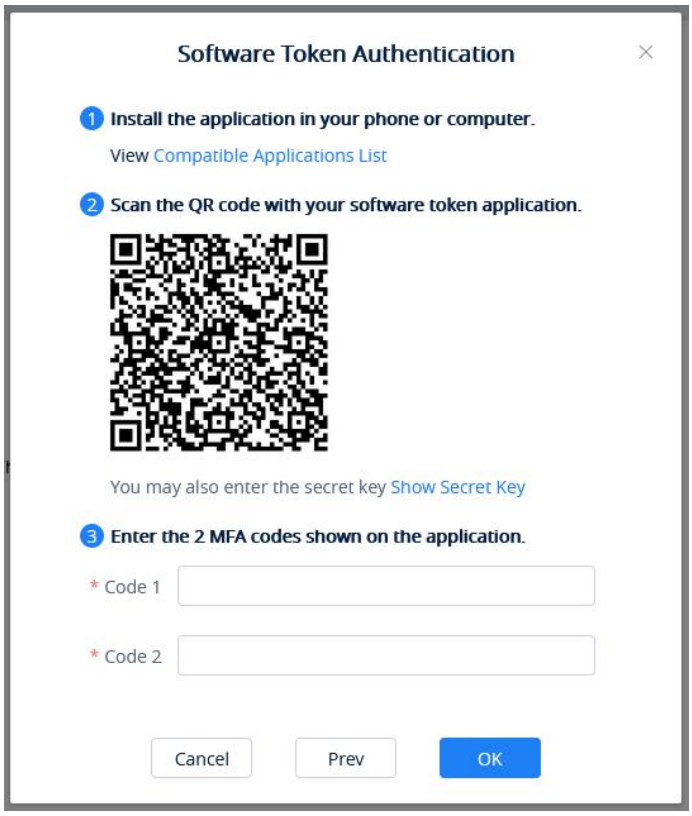
1. 使用您的账号登录到 GDMS 平台，点击右上角的姓名，进入个人信息页面：



图表 1：访问个人信息页面

2. 点击“开启”多因子认证，并且在弹窗中选择使用“虚拟 MFA 设备”，然后点击“下一步”。

3. 此时界面上将生成并显示虚拟 MFA 设备的配置信息，包括 QR 代码图形。此图形是秘密配置密钥的表示形式，适用于不支持 QR 代码的设备上的手动输入。



图表 2：扫描 MFA 二维码

4. 打开您的虚拟 MFA 应用程序。确定 MFA 应用程序是否支持 QR 代码，然后执行以下操作之一：

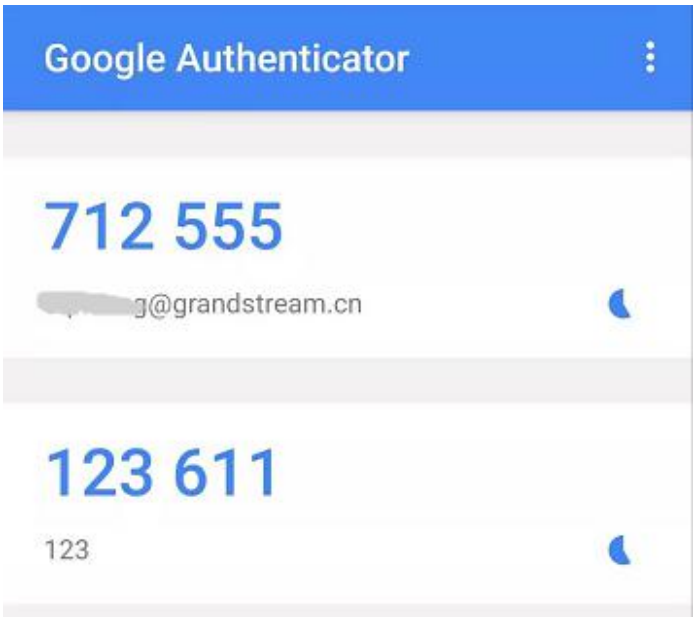
(1) 如果您的 MFA 应用程序支持 QR 代码，可以使用该应用程序扫描 QR 代码。例如，您可选择摄像头图标或选择类似于 Scan code 的选项，然后使用设备的摄像头扫描此代码。

(2) 如果不支持 QR 代码，点击显示秘钥，然后在您的 MFA 应用程序中键入私有密钥。

注意：如果虚拟 MFA 应用程序支持多个虚拟 MFA 设备或账户，请选择相应的选项以创建新的虚拟 MFA 设备或账户。

5. 完成操作后，您的虚拟 MFA 设备会开始生成一次性密码。

(1) 在 MFA 代码 1 框中，输入虚拟 MFA 设备上当前显示的一次性密码。请等候 30 秒，以便设备生成新的一次性密码。然后在 MFA 代码 2 框中输入第二个一次性密码。



图表 3：输入 MFA 代码

6. 点击“开启认证”按钮，验证通过后，您的账号和此虚拟 MFA 设备已绑定成功。以后登录必须输入 MFA 设备代码才可成功登录。

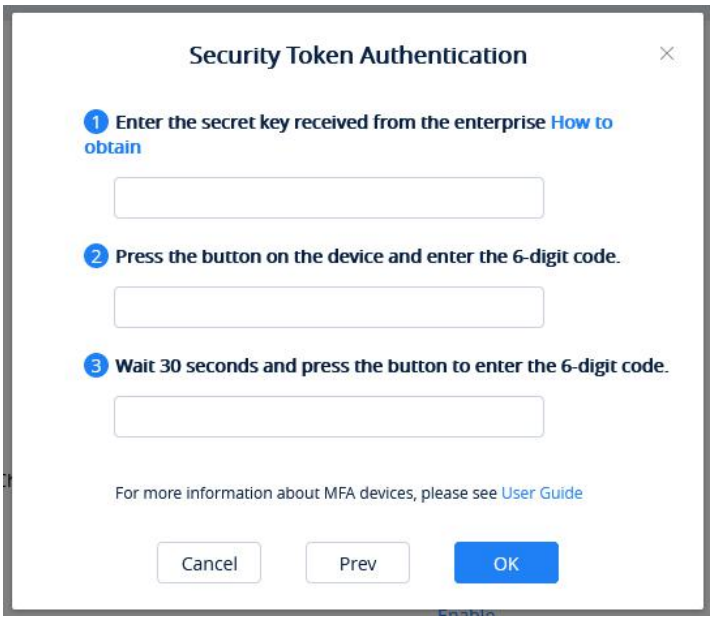
重要：
1. 生成代码之后立即提交您的请求。如果生成代码后等待很长时间才提交请求，一次性密码（TOTP）很快会过期。这种情况下，您可以重新启用设备。
2. 一个用户只能绑定一个 MFA 设备。

4.2. 启用硬件 MFA 设备

前提：您已购买硬件 MFA 设备（参考【MFA 设备规格】章节）。

1. 使用您的账号登录到 GDMS 平台，点击右上角的姓名，进入个人信息页面。
2. 点击“开启”多因子认证，并且在弹窗中选择使用“硬件 MFA 设备”，然后点击“下一步”。

3. 此时进入到绑定硬件 MFA 设备界面：



图表 4：硬件 MFA 设备认证

4. 键入设备的秘钥，请联系厂商获取秘钥。
注意：秘钥格式要求是 Default hex seeds（seeds.txt）或者是 base32 seeds。
例子：
HEX SEED: B12345CCE6DA79B23456FE025E425D286A116826A63C84ACCFE21C8FE53FDB22
BASE32 SEED: WNKYUTRG3KE3FFTZ7UIO4QS5FBVBC2HJKY6IJLCP4QOH7ZJ12YUI====

5. 在 MFA code 1（MFA 代码 1） 框中，输入 MFA 设备显示的六位数编码。您需要按设备正面的按钮来显示编码。在设备刷新期间等候 30 秒，然后在 MFA code 2（MFA 代码 2） 框中键入第二个六位数编码。您需要再次按设备正面的按钮来显示第二个编码。

图表 5：硬件 MFA 设备

6. 点击“开启认证”按钮，验证通过后，您的账号和此虚拟 MFA 设备已绑定成功。以后登录必须输入 MFA 设备代码才可成功登录。

重要：
1. 生成代码之后立即提交您的请求。如果生成代码后等待很长时间才提交请求，一次性密码（TOTP）很快会过期。这种情况下，您可以重新启用设备。
2. 一个用户只能绑定一个 MFA 设备。

5. 移除 MFA 设备

如果您不需要 MFA 认证，您可以移除 MFA 设备，恢复普通的登录认证。

1. 使用您的账号登录到 GDMS 平台，点击右上角的姓名，进入个人信息页面。
2. 点击“移除”多因子认证，即可移除。

6. 常见问题

6.1. MFA 设备丢失或无效

如果您的 MFA 设备丢失或无法正常工作，您可以使用以下方式先移除 MFA 设备，然后再重新启用新的 MFA 设备。

- **方式 1：**

如果您是子级账号， 您可以联系 GDMS 的主账号在用户管理页面移除您的多因子认证。移除后，您即可使用密码登录 GDMS 平台，然后重新启用新的 MFA 设备。

- **方式 2：**

如果您是 GDMS 的主账号，无法登录 GDMS 平台，您可以联系我们的 Support，提供您的相关材料给 Support，然后协助您移除多因子认证（仅发送移除邮件给用户，由用户输入账号密码并确认移除）。