

前言

[上篇文章](#)以 Ubuntu 为例，介绍了如何给 Linux 服务器添加两步验证，这篇就是来说一下如何给 Windows 服务器远程连接增加两步验证，我也是摸索了很久才成功的，不足之处还请大牛们指教。

由于 Windows 本身的限制，微软官方给出的解决办法是使用自己家的 Azure AD 域控制器，同样配合自家的 Azure MFA，从而启用远程桌面的两步验证。但很明显，必须要使用微软自家的 Azure 云服务上面的域控制器才能达到效果，对于个人来说这条路行不通。

本文将详细介绍如何使用 Microsoft Azure 的网络策略服务器 (NPS) 扩展集成远程桌面网关基础结构与 Azure 多重身份验证 (MFA)。

Azure 网络策略服务 (NPS) 扩展允许客户使用 Azure 基于云的[多重身份验证 \(MFA\)](#) 来保护远程身份验证拨入用户服务 (RADIUS) 客户端身份验证。该解决方案提供双重验证，用于将第二层安全性添加到用户的登录和事务。

本文将逐步说明如何使用 Azure 的 NPS 扩展集成 NPS 基础结构与 Azure MFA。这使得尝试登录到远程桌面网关的用户能够进行安全验证。

① 备注

本文不适用于 MFA 服务器部署，仅适用于 Azure MFA（基于云）部署。

网络策略和访问服务 (NPS) 使组织能够执行以下操作：

- 通过指定执行连接操作的人员、允许连接的时间、连接持续时间，以及客户端必须用于连接的安全级别等来定义网络请求的管理和控制中心位置。这些策略可以集中在一个位置一次性指定，而不是在每个 VPN 或远程桌面 (RD) 网关服务器上进行指定。RADIUS 协议提供集中身份验证、授权和计帐 (AAA)。
- 建立和强制执行网络访问保护 (NAP) 客户端健康策略，可确定是授予设备对网络资源的无限制还是受限制的访问权限。
- 提供一种强制进行身份验证和授权，以访问支持 802.1x 无线访问点和以太网交换机的方式。

通常情况下，组织使用 NPS (RADIUS) 来简化和集中管理 VPN 策略。然而，许多组织也会使用 NPS 简化和集中 RD 桌面连接授权策略 (RD CAP) 的管理。

另外，组织还可以将 NPS 与 Azure MFA 进行集成，以增强安全性并提供高级别的符合性。这将有助于确保用户建立双重验证以登录到远程桌面网关。已授予访问权限的用户，他们必须提供其用户名/密码组合与用户已有的信息。此信息必须受信任且不容易复制，例如手机号码、座机号码、移动设备上的应用程序等等。RDG 目前 2fa 支持电话呼叫和来自 Microsoft 验证器应用方法的推送通知 有关支持的身份验证方法的详细信息，请参阅[决定你的用户可以使用哪些身份验证方法](#)部分。

在为 Azure 提供 NPS 扩展之前，希望对集成的 NPS 和 Azure MFA 环境实施双重验证的客户，必须在本地环境中配置和维护单独的 MFA 服务器，如[使用 RADIUS 的远程桌面网关和 Azure 多重身份验证服务器](#)中所述。

现在提供了 Azure 的 NPS 扩展之后，可使组织选择部署基于内部部署的 MFA 解决方案或基于云的 MFA 解决方案来保护 RADIUS 客户端身份验证。

还好朋友给我推荐了 Duo Security，这是一家提供双重认证服务的商业公司，2018年底被 Cisco 收购，美国很多的大学、企业都在使用他们的方案，而且对于个人来说是免费的。



但是，重要的话说三遍：

不建议使用微软账户登录的用户使用此方法！

不建议使用微软账户登录的用户使用此方法！

不建议使用微软账户登录的用户使用此方法！

-
- 这一点主要是针对 Windows 10 用户，在更新完 1709 后，Duo Security 与 Windows 10 产生了冲突，而官方的规避方法是添加一条注册表项让微软账户绕过两步验证，这很明显不符合我们的要求。他们给出了这个已知问题，有兴趣的可以看一下并规避：[https://support.microsoft.com/en-us/help/4025032/windows-10-duo-security-error](#)
-

开始配置

安装前的要求

- Windows 7 或 Windows Server 2008 R2 及以上的计算机，连接外网
- 必须使用本地账户登录
- 用户必须设置密码，不能空密码

我用一台Windows Server 2019做为例子。

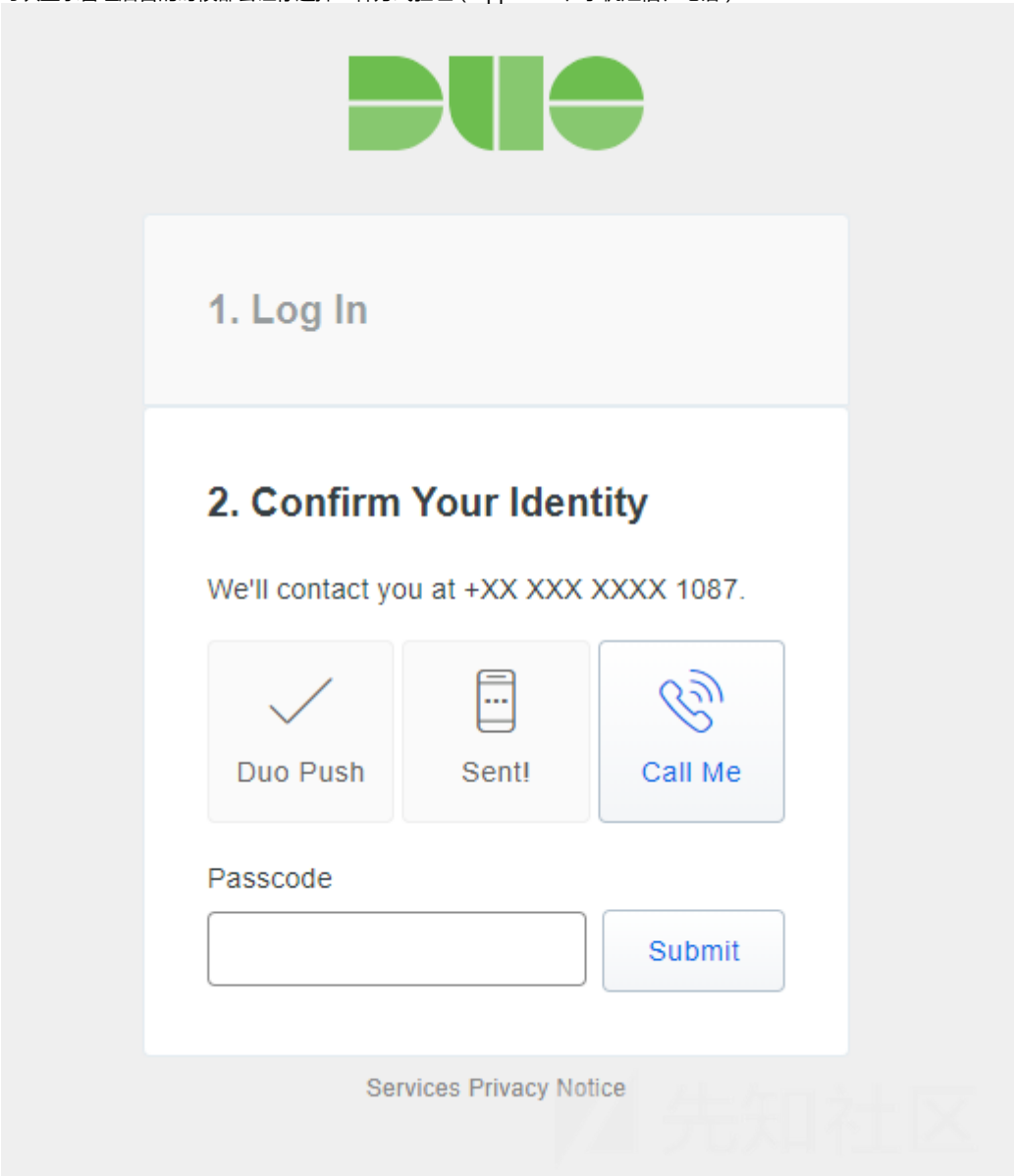
开始创建应用

首先去 <https://duo.com/pricing> 选择免费账号注册，并填写你的手机号

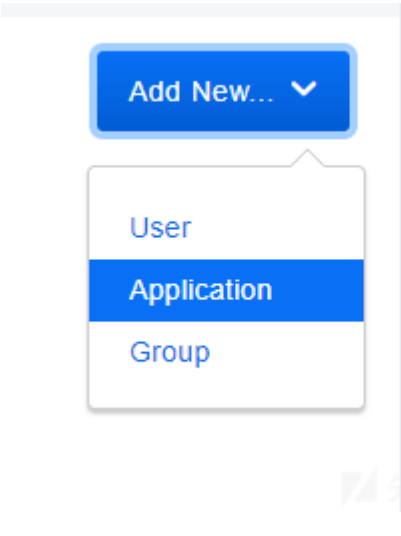
Duo Free Free up to 10 users	Duo MFA \$3 / User / Month	Duo Access \$6 / User / Month Most Popular	Duo Beyond \$9 / User / Month
--	--------------------------------------	---	---


先知社区

每次登录管理后台的时候都会让你选择一种方式验证（App Push、手机短信、电话）



进入管理后台之后，点击首页的Add New-Application，找到Microsoft RDP，点击右边的Protect this Application



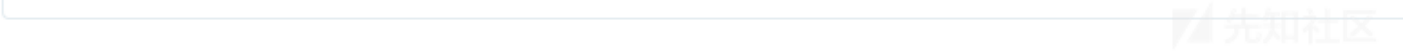
 Microsoft RDP

[Protect this Application](#) | [Read the documentation](#)

一定要妥善保管好Integration key和Secret Key！

Details

Integration key	<div></div>	<div>select</div>
Secret key	<div></div>	<div>select</div>
Don't write down your secret key or share it with anyone.		
API hostname	<div></div>	<div>select</div>



接下来还有一些选项，这里我们先全默认，不过最好勾上Offline Access，防止没有网络了无法登录，点击Save

Offline Access Settings

Offline access	<div><input checked="" type="checkbox"/> Offline login and enrollment is enabled</div>
These settings will take effect the next time the application connects to the internet.	



下载 App 并启用推送

在 [App Store](#) 或者 [Play Store](#) 里面搜索 Duo Mobile 下载安装：



Duo Mobile

4+

Duo Security

★★★★★ 1.0, 4 个评分

免费



Duo Mobile

Duo Security, Inc. 公司

★★★★★ 6,156 人

适合所有人

此应用与您的所有设备都兼容。

已安装

由于我们只有一个用户，所以进入 Duo Security 控制台，找到Users，点击Add User开始创建用户，我这里用户名设置为wb，如果你使用默认的管理员用户，则把用户名设置为 administrator 但不管设置什么，最后要和你服务器登录时候的用户名保持一致！

Add User

Adding Users

Most applications allow users to enroll themselves after they complete primary authentication.

[Learn more about adding users](#) 

Username

Should match the primary authentication username.

Add User

其他可以全默认，然后点Save Changes

接下来拉到下方，点击 Add Phone，输入你的手机号码（中国请改成86），如果你想用平板认证就选择 Tablet，然后点Next

Phones

To use two-factor with a specific phone, type 'push1', 'sms1', 'phone2', 'sms2', etc, as your factor. You may rearrange the phones by dragging and dropping in the table.

Add Phone

This user has no phones. [Add one.](#)

Add Phone

Type



Phone



Tablet

Phone number


 +1 201-555-5555

[Show extension field](#)

Add Phone


在 Setting 选项中，给你的设备取个名字，Platform 选择你手机对应的平台，然后保存设置

Settings

Number	<div> <input type="text" value="139 1234 5678 9010"/></div>	Show extension settings
Device name	<input type="text" value="Work Phone"/> <small>Optional. Examples: "Work phone", "Old iPod touch"</small>	
Type	<div>Mobile ▼</div>	
Platform	<div>Android ▼</div>	
<div>Save Changes</div>		

点击上方的 Active Duo Mobile-Generate Duo Mobile Activation Code

Device Info



Not using Duo Mobile

Activate Duo Mobile

Send Instructions by SMS

or

skip this step

稍等一下之后，手机就会收到短信了：

14:40

【NXSMS】 Welcome to Duo! Please install Duo Mobile from your app store.

【NXSMS】 To activate the app, tap and open this link with Duo Mobile:



刚刚

打开短信中的链接，就会自动激活手机上的 Duo Mobile 客户端并添加验证（前提是要安装）



DUO ADMIN



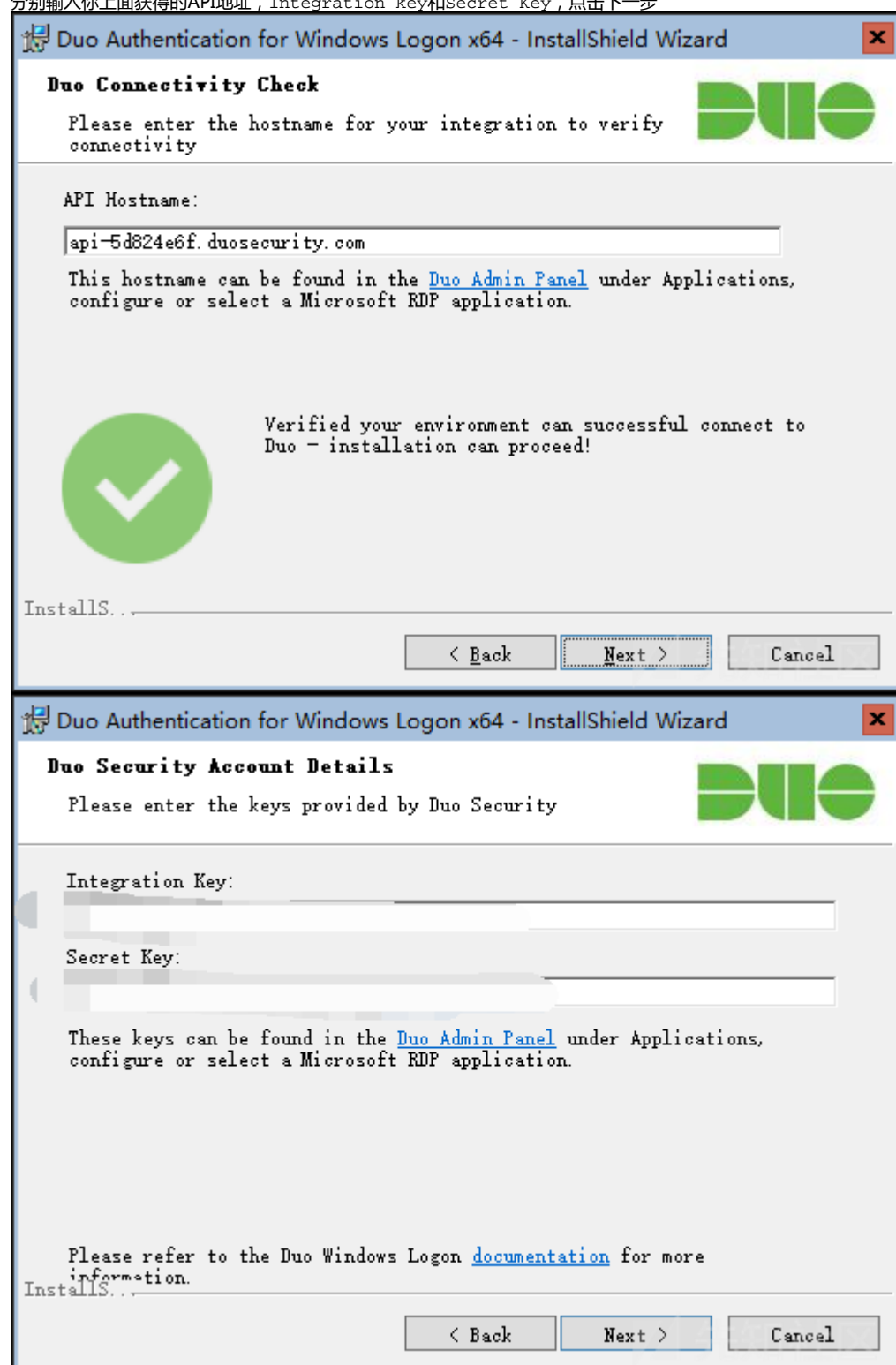
ABOUT PASSCODES

App 配置完成。

在服务器上操作：

首先启用服务器的远程桌面功能，然后下载 Duo Security 认证客户端：<https://dl.duosecurity.com/duo-win-login-latest.exe>，打开安装程序

分别输入你上面获得的API地址，Integration key和Secret Key，点击下一步



Duo Authentication for Windows Logon x64 - InstallShield Wizard

Duo Connectivity Check

Please enter the hostname for your integration to verify connectivity

API Hostname:

api-5d824e6f.duosecurity.com

This hostname can be found in the [Duo Admin Panel](#) under Applications, configure or select a Microsoft RDP application.

Verified your environment can successful connect to Duo - installation can proceed!

InstallS...

< Back Next > Cancel

Duo Authentication for Windows Logon x64 - InstallShield Wizard

Duo Security Account Details

Please enter the keys provided by Duo Security

Integration Key:

Secret Key:

These keys can be found in the [Duo Admin Panel](#) under Applications, configure or select a Microsoft RDP application.

Please refer to the Duo Windows Logon [documentation](#) for more information.

InstallS...

< Back Next > Cancel

关于这三个选项：

Duo integration options



Configure the integration below

☒ **Bypass Duo authentication when offline (FailOpen)**

Enable this option to allow user logon without completing two-factor authentication if the Duo Security cloud service is unreachable. If you plan to enable offline access with MFA consider disabling FailOpen to prevent un-enrolled users from logging in.

☒ **Use auto push to authenticate if available**

Automatically send a Duo Push or phone call authentication request after primary credential validation.

☐ **Only prompt for Duo authentication when logging in via RDP**

Leave this option unchecked to require Duo two-factor authentication for local logon and RDP sessions. If enabled, local logons do not require 2FA approval.

Please refer to the Duo Windows Logon [documentation](#) for more information.

InstallShield

< Back

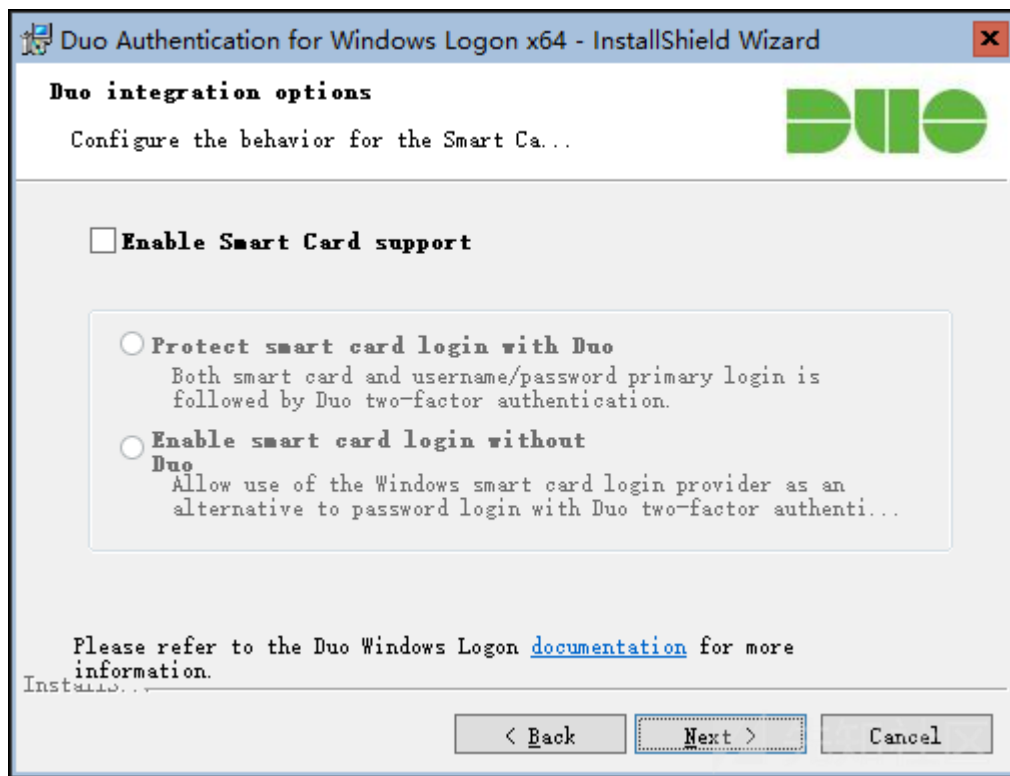
Next >

Cancel

■■■■■■■■■■■■■■■■■■■■Duo■■■■■■■■■■
■■■■■■■■■■■■■■■■■■■■
■■■■RDP■■■■■■■■■■■■■■■■■■■■Duo■■■■■■■■■■

其中前两项默认是选中的，如果第三项选中了，就是只有在远程桌面的时候才会要求Duo身份验证，而直接操作物理服务器的时候就不需要了，这个是否开启取决于个人。

没有智能卡，直接下一步

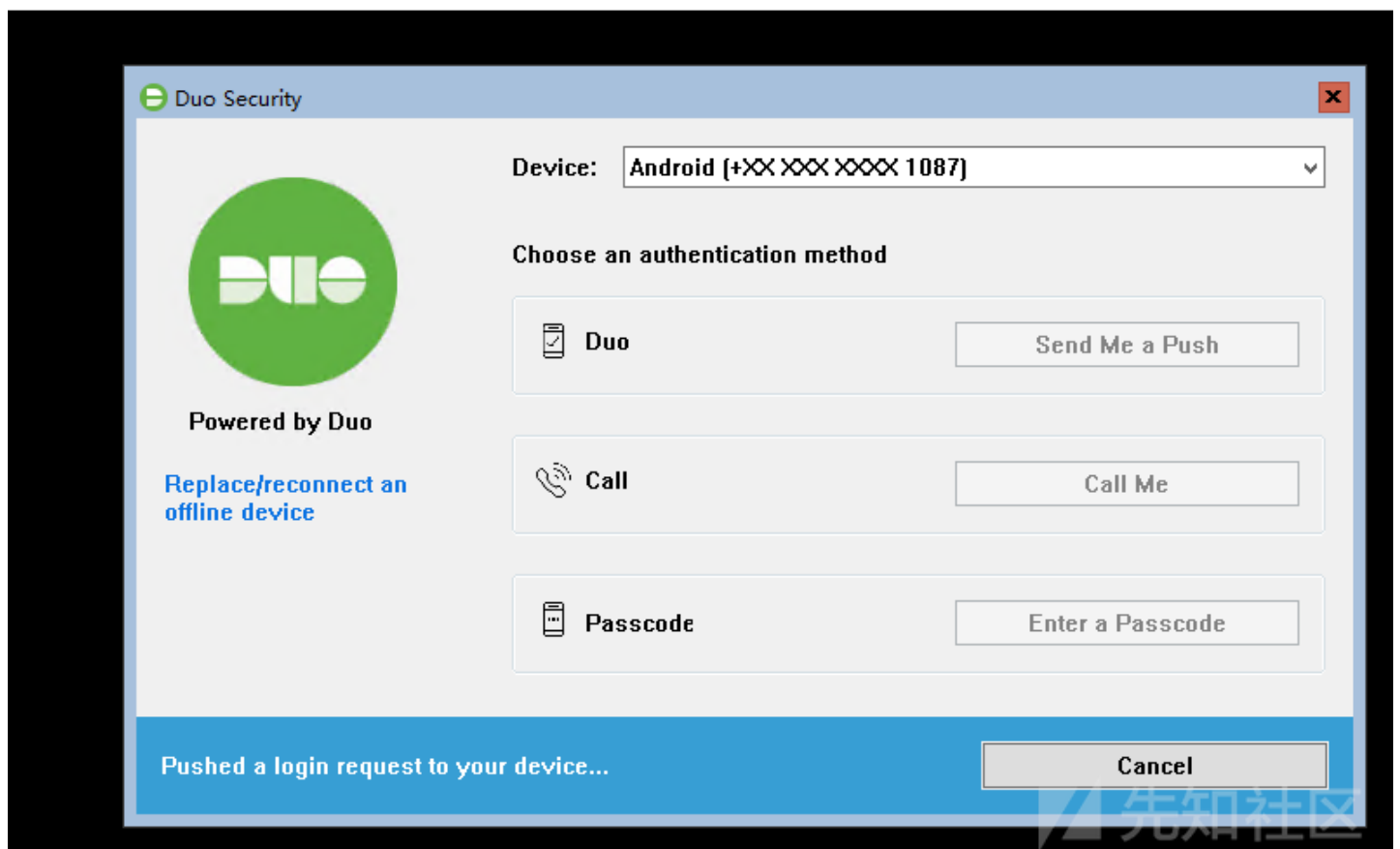


安装完成之后重启电脑

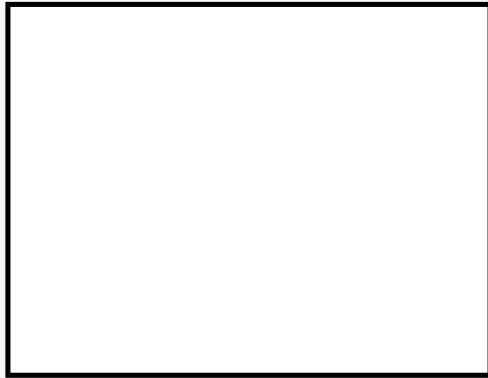
测试

重启服务器之后，尝试使用 RDP 进行远程登陆，输入完用户名和密码之后，如果没有问题的话，就弹出了二次认证页面，同时你的手机也收到了 App Push，点击 Approve 即可完成登录进入桌面

192.168.1.94 - 远程桌面连接



Login Request



192.168.1.175

Unknown



2019年6月3日 14:45


APPROVE


DENY

如果你没法收到通知，可以手动刷新一下App，或者在登录界面选择输入动态码或者手机短信验证码登录。

接下来会提示你如果网络断开了使用什么方式验证，选Mobile Passcode然后点击右下角的按钮（我这个Server没桌面所以字体看起来很差劲）

Duo Security

Login to Windows even when you're offline

Get to work securely even without an internet connection. With Duo Security's new Offline Login, you can count on reliable access to the tools and information you need, anywhere.

Enroll later (May prevent offline login)

What type of authentication method do you want to use login?

☒ Duo Mobile Passcode

☐ Security Key (YubiKey)

用Duo Mobile点击右上角的加号扫码即可。

Duo Security

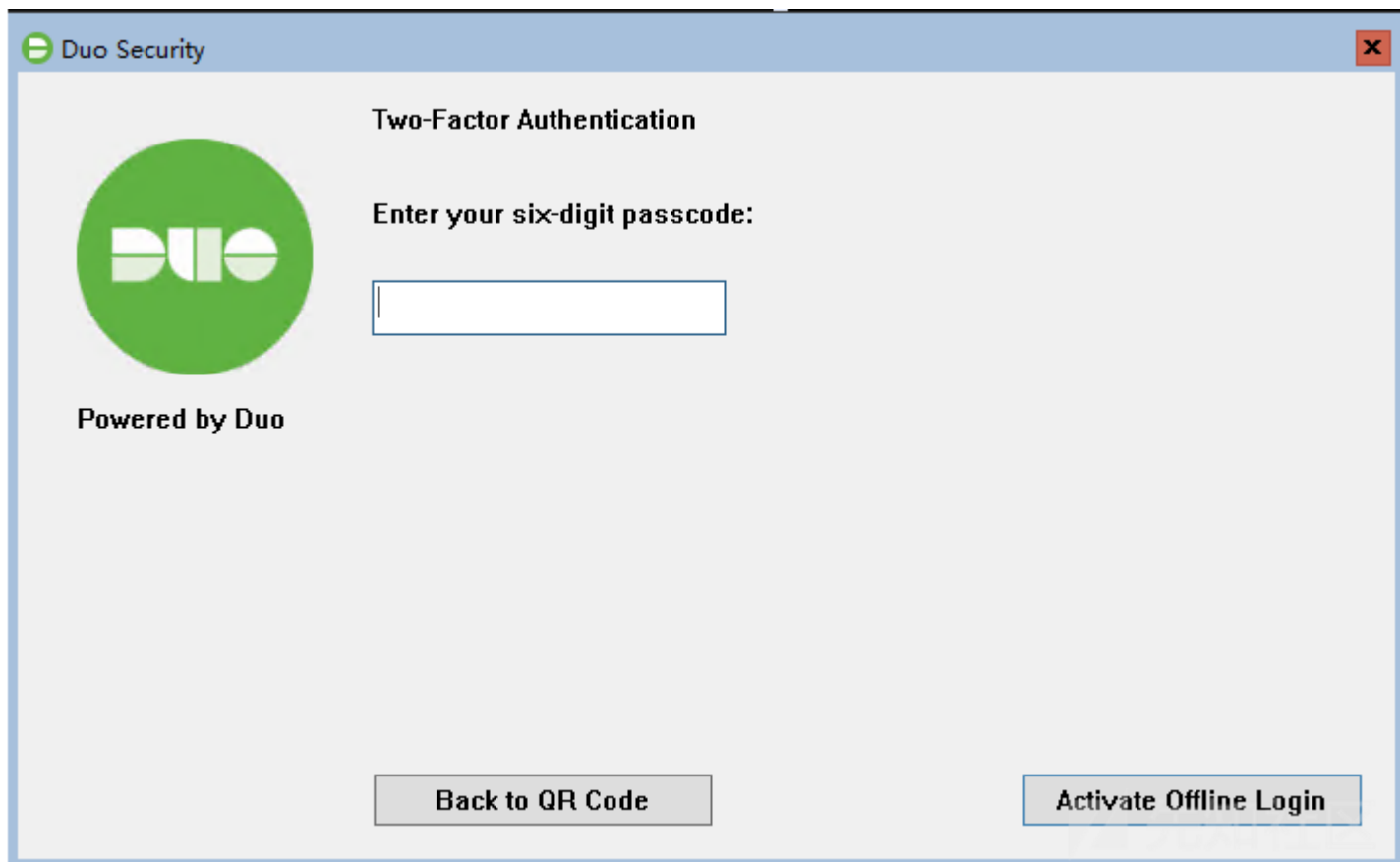
Powered by Duo

Scan the QR Code with Duo Mobile to begin activation:

Open the Duo Mobile app and hit the + icon in the top right. Then, scan the code below and follow the instructions on your mobile device:

Enter Offline Code

然后输入一次刚刚生成的动态码即可。



出了问题没法登录想卸载怎么办？

进入安全模式，先反注册这两个DLL：

```
regsvr32 /u "C:\Program Files\Duo Security\WindowsLogon\DuoCredProv.dll"
regsvr32 /u "C:\Program Files\Duo Security\WindowsLogon\DuoCredFilter.dll"
```

然后重启到正常模式，Duo Mobile就不见了，这个时候在控制面板删除即可。

点击收藏 | 0 关注 | 1

[上一篇：Laravel 5.8 SQL 注...](#) [下一篇：记一次审计小众cms垂直越权](#)

1. 0 条回复

- 动动手指，沙发就是你的了！

[登录](#) 后跟帖

先知社区

[现在登录](#)

热门节点

[技术文章](#)

[社区小黑板](#)

[目录](#)

[RSS](#) [关于社区](#) [友情链接](#) [社区小黑板](#)