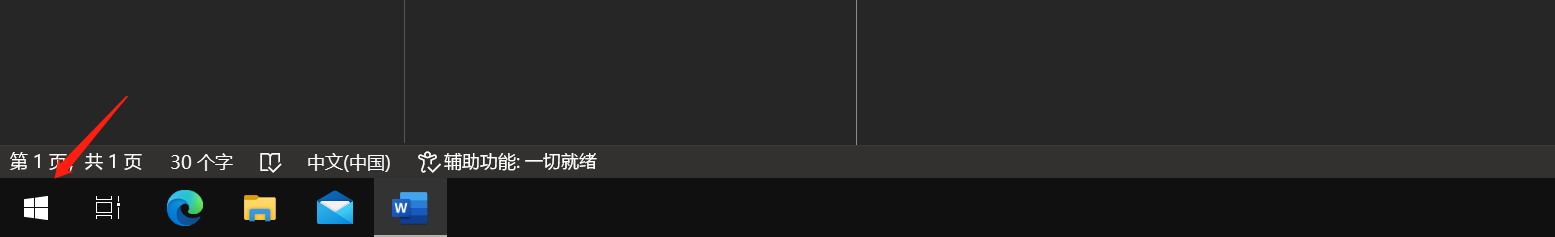
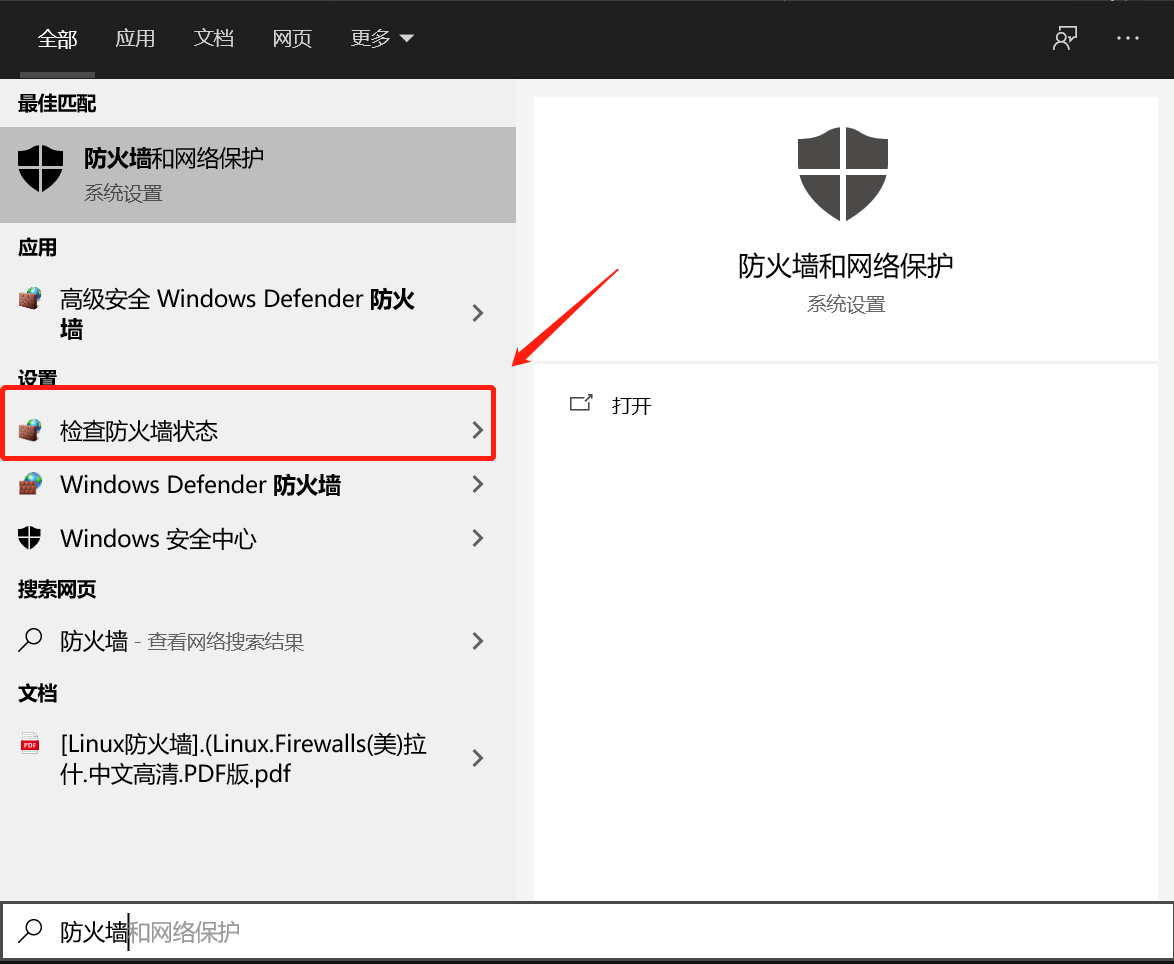
# 终端安全手册

1. 启用防火墙
2. windows10
   * 点击“开始”



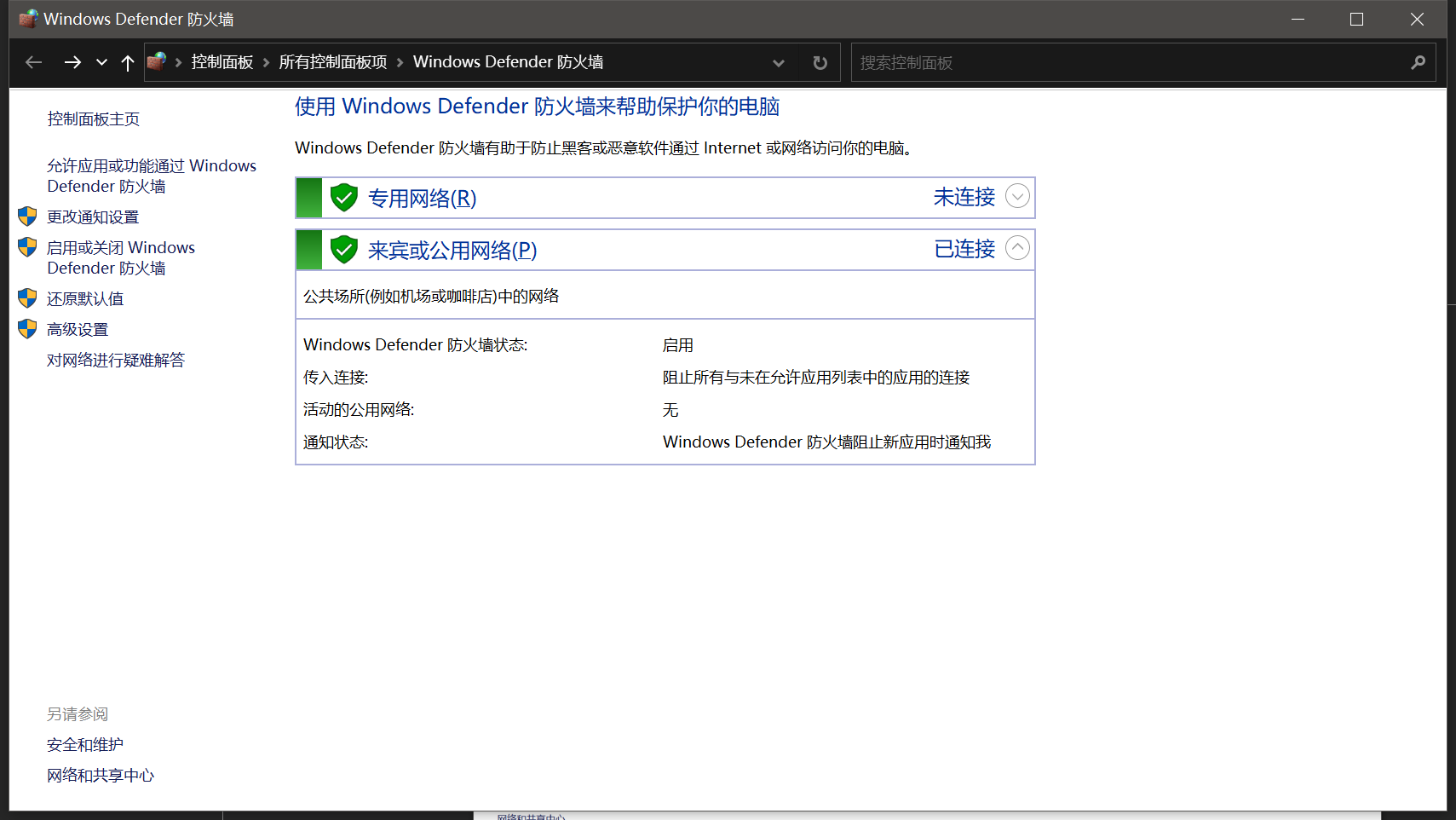
* + 直接输入“防火墙”



* + 点击“检查防火墙状态”。
    - 如果防火墙未启用，显示为红色，如下图



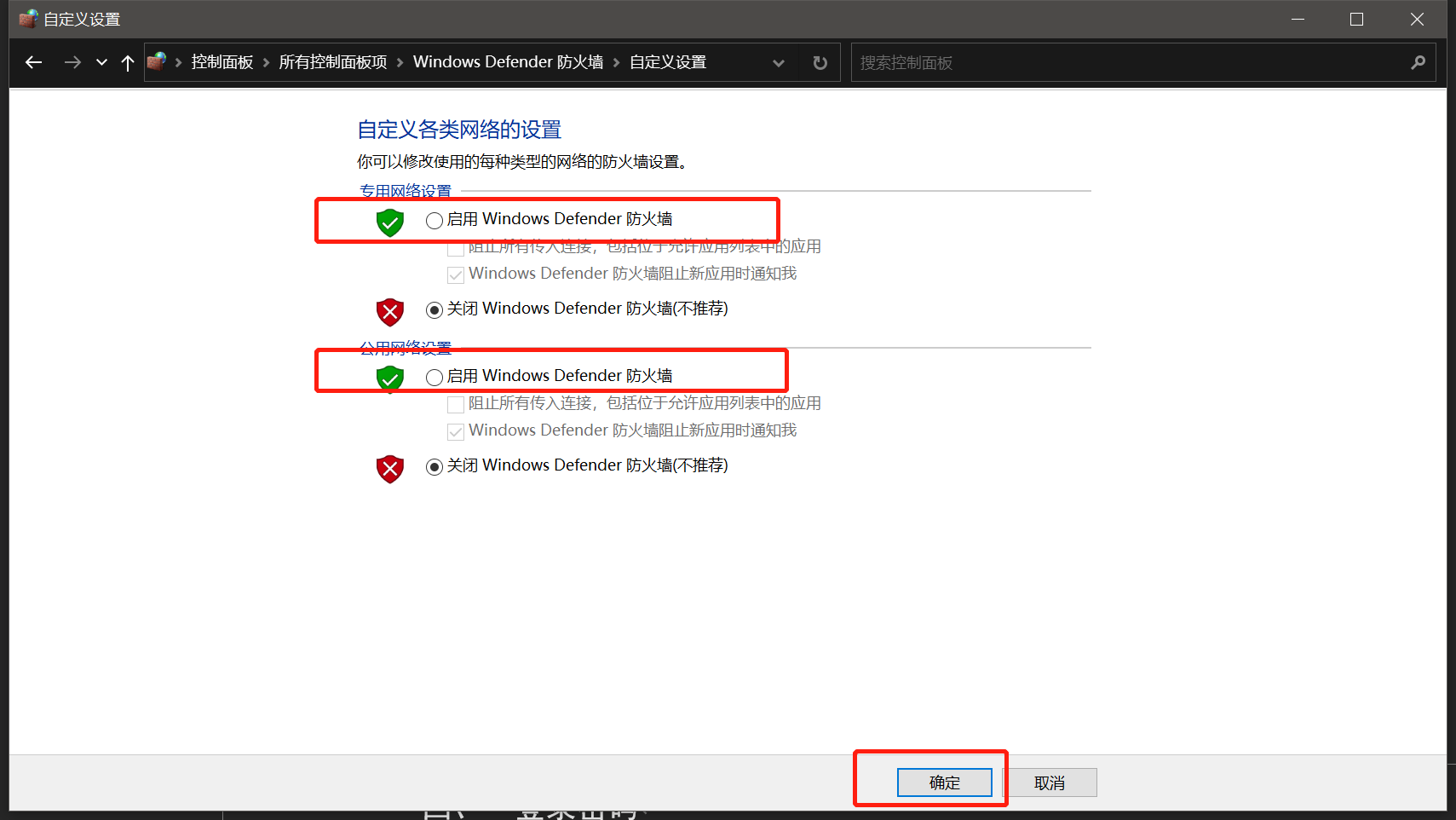
* + - 如果防火墙正常启用，则为绿色，如下图



* + 启用防火墙方法
    - 点击“启用或关闭Windows Defender防火墙”



* + - 选中两个“启用Windows Defender防火墙”，并确定



1. Windows7

* 点击开始，打开控制面板

电脑萤幕的截图

描述已自动生成

* 选择使用控制面板小图标显示

图形用户界面, 应用程序

描述已自动生成

* 如果防火墙未开启，会如下图所示，显示为红色。需点击“打开或关闭windows防火墙”。

图形用户界面, 文本, 应用程序

描述已自动生成

* 开启防火墙

图形用户界面, 文本, 应用程序

描述已自动生成

* 防火墙开启后如下图所示

图形用户界面, 应用程序

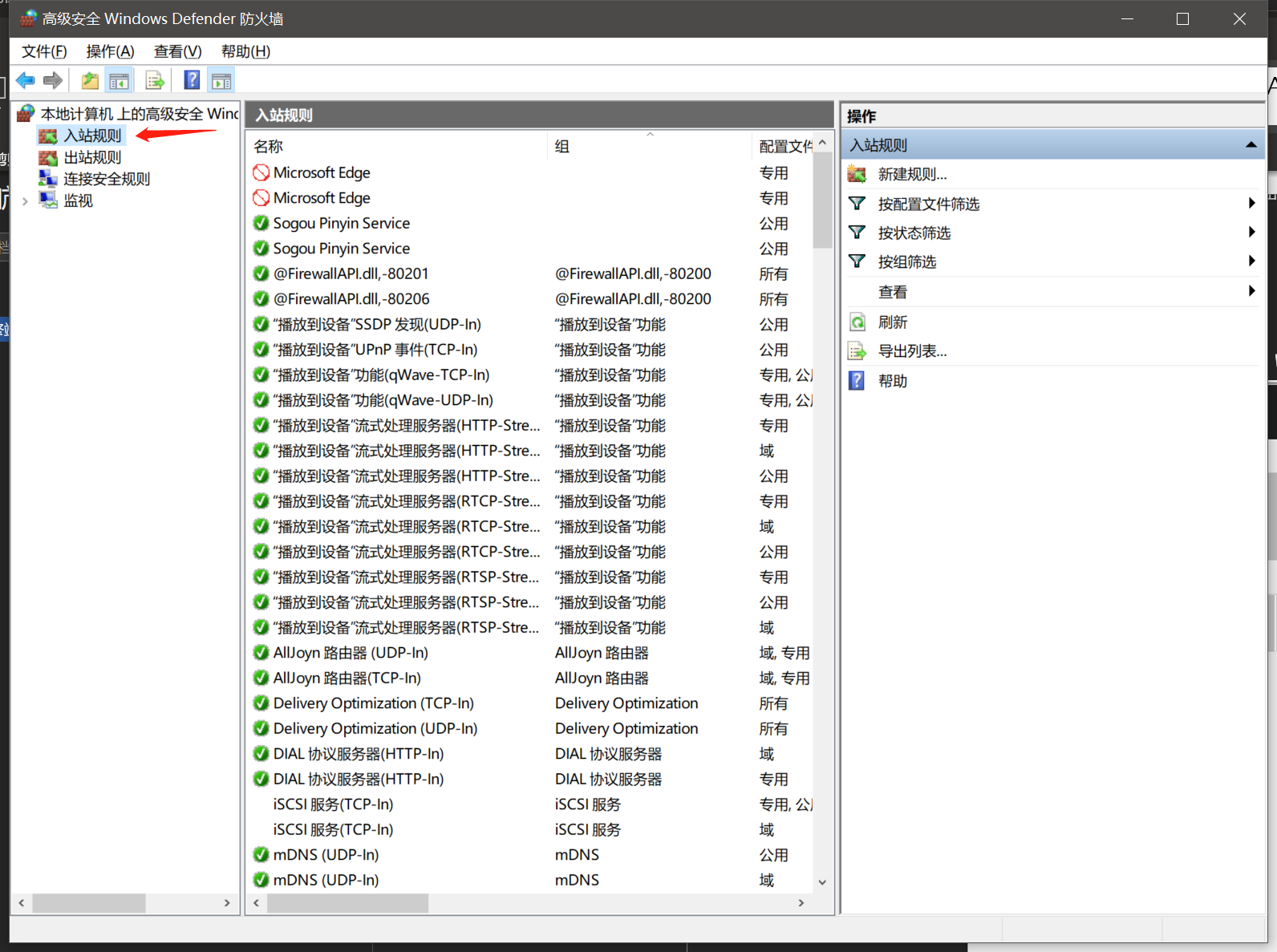
描述已自动生成

1. 封禁高危端口
2. Windows10（手动配置）
   * 在开始菜单搜索“高级安全 Windows Defender 防火墙”，并点击进入。

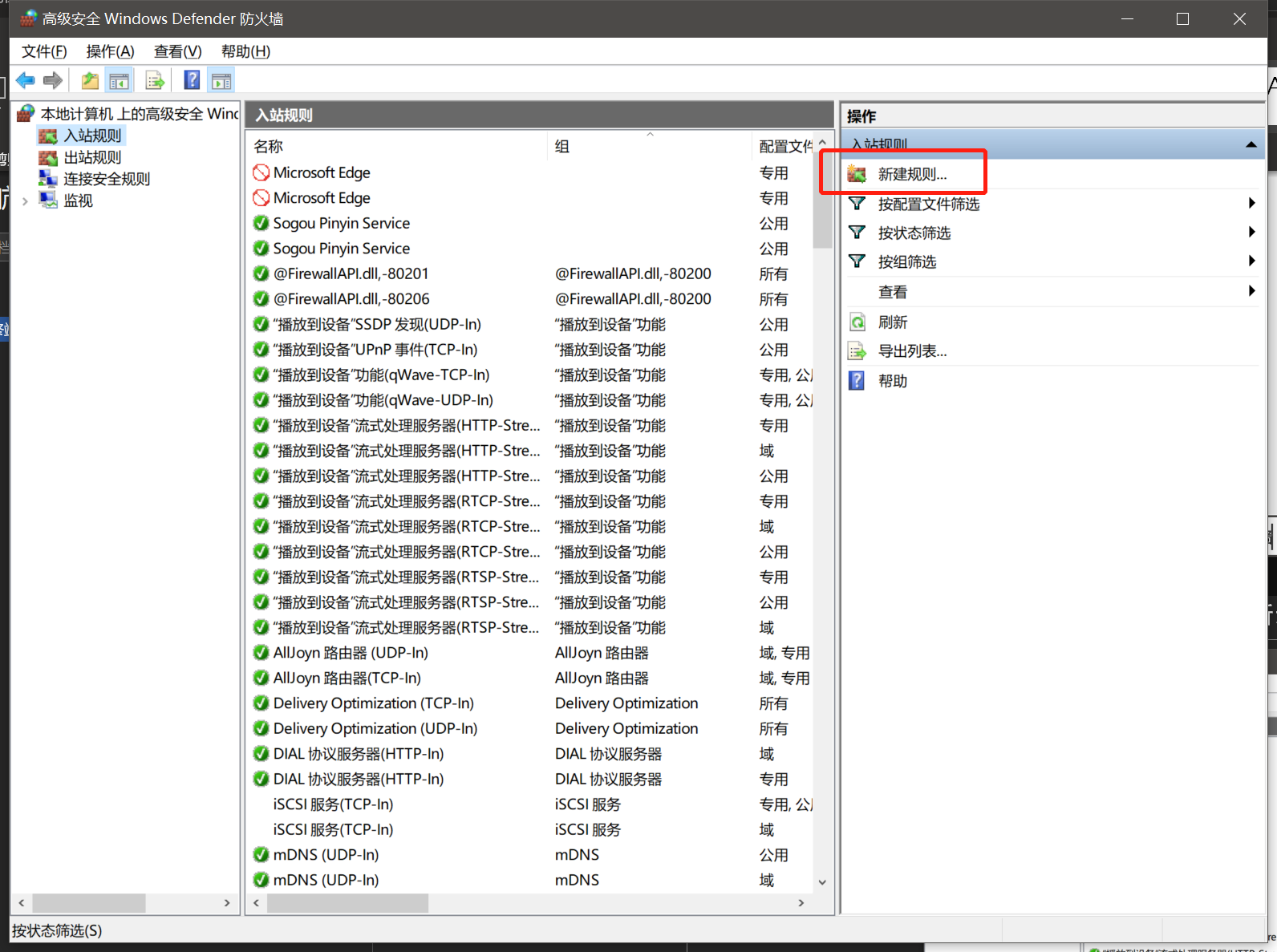
图形用户界面, 文本, 应用程序

描述已自动生成

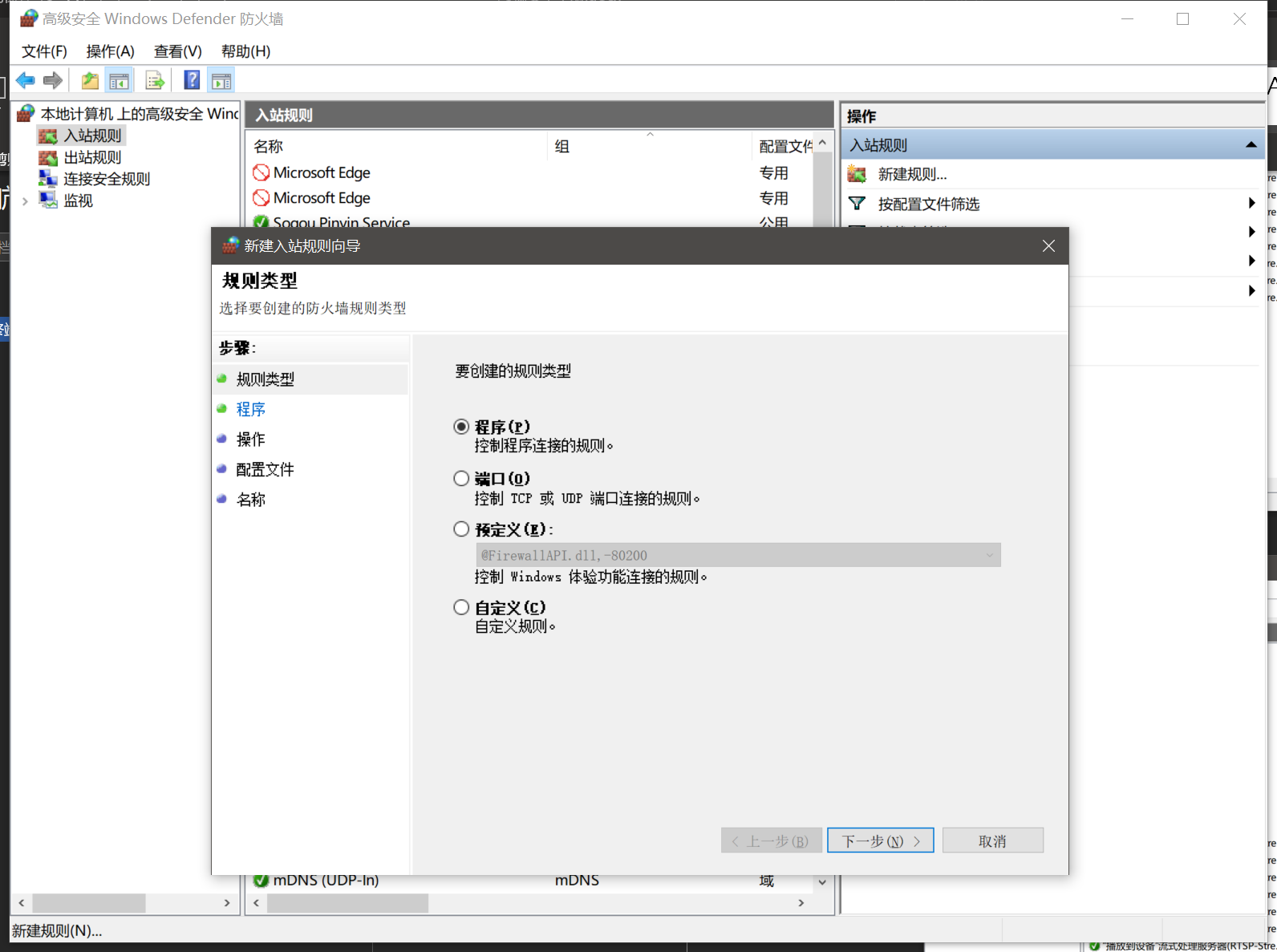
* + 点击“入站规则”，如下图所示：



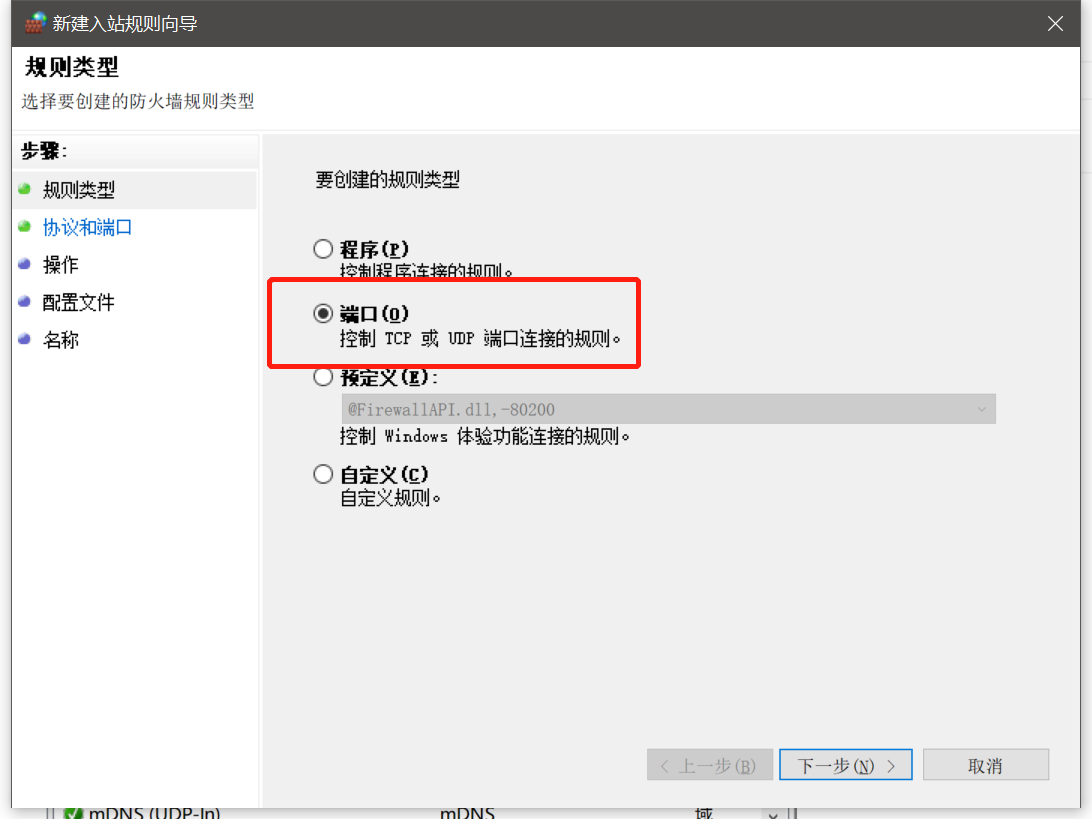
* + 点击“新建规则”



* + 弹出“新建入站规则向导”



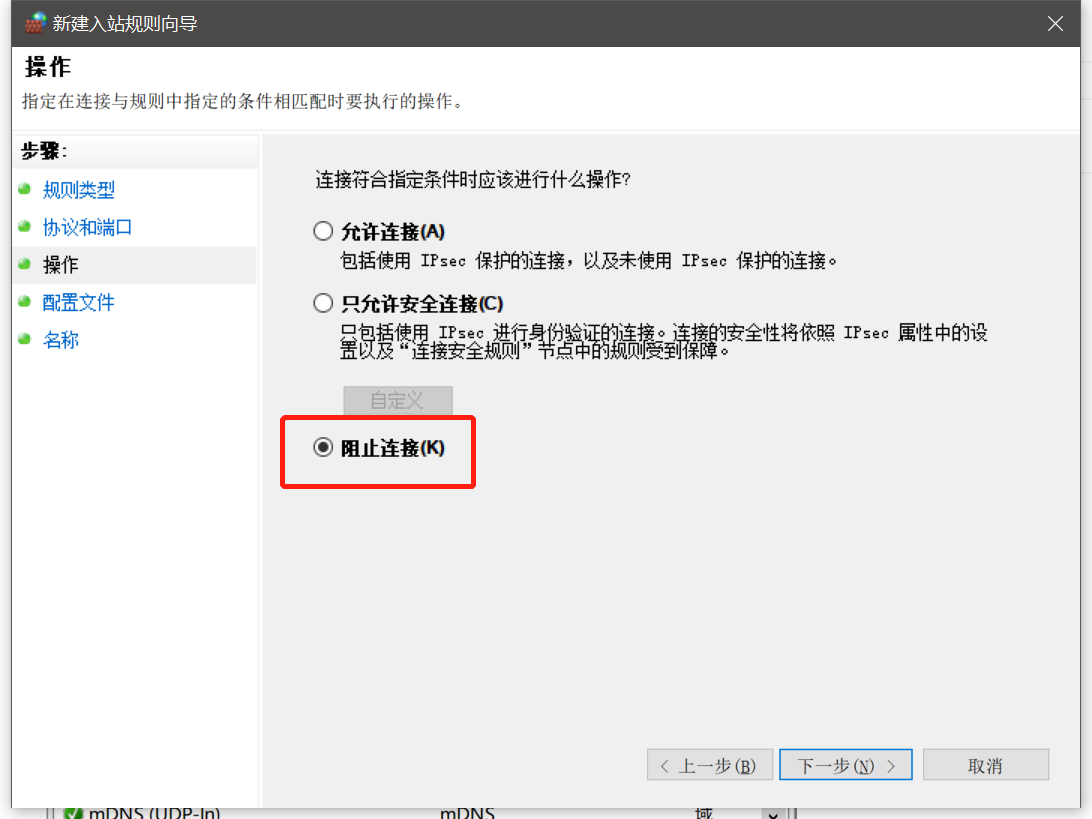
* + 选择端口



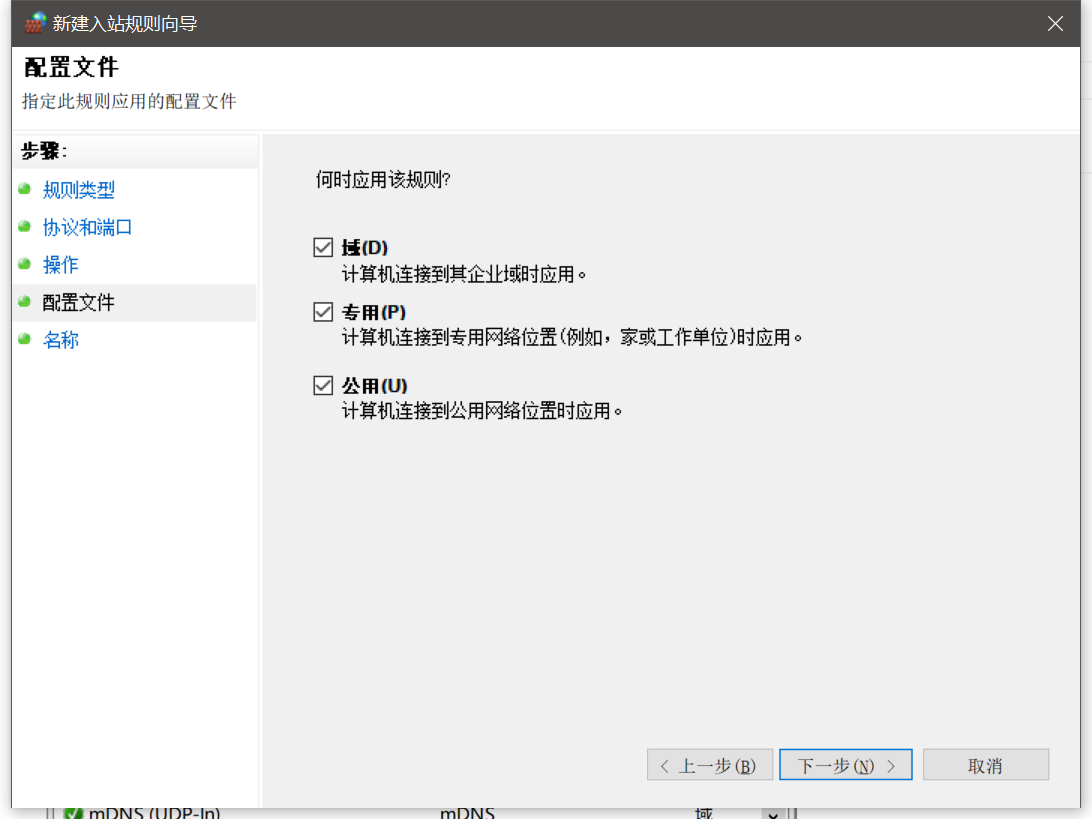
* + 输入指定端口（135,137,138,139,445,3389），点击下一步



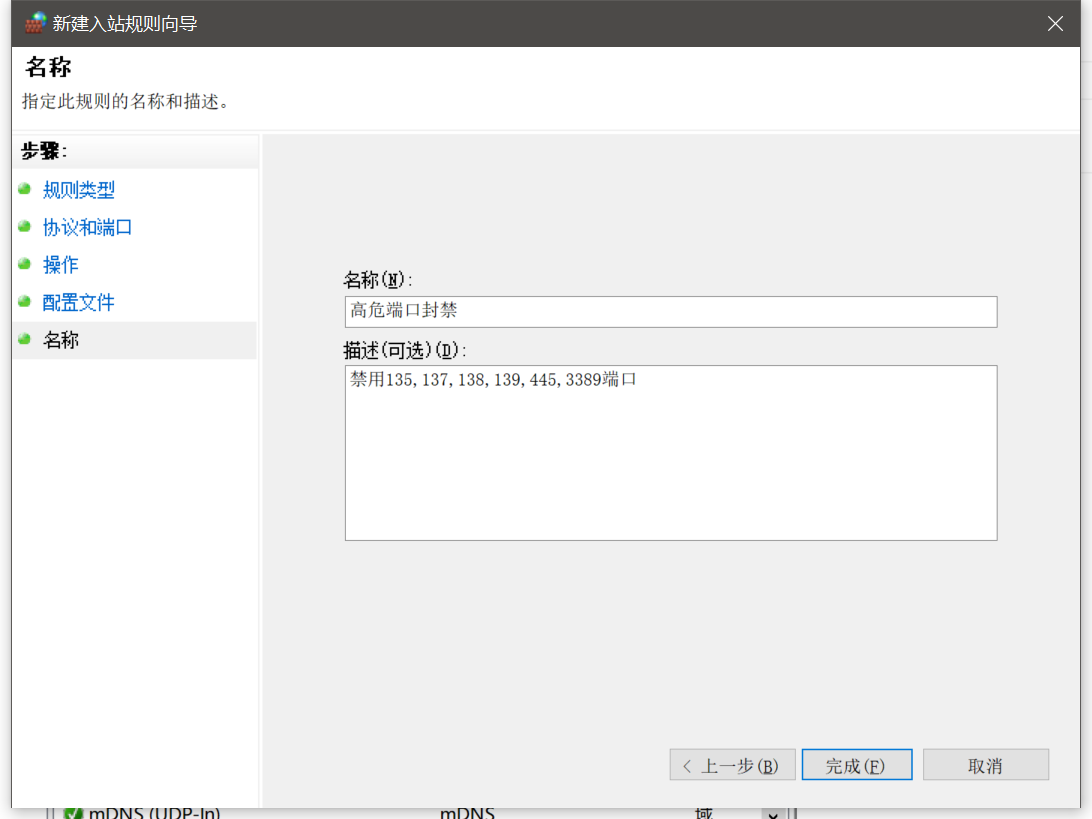
* + 选择阻止连接，点击下一步



* + 全选“域”，“专用网络”，“公用”，点击下一步



* + 填写策略名称和描述，点击完成



1. Windows7
   * 在控制面板打开防火墙配置，点击高级设置

图形用户界面, 文本, 应用程序, 电子邮件

描述已自动生成

* + 点击入站规则

图形用户界面, 应用程序

描述已自动生成

* + 选择端口，下一步

图形用户界面, 应用程序

描述已自动生成

* + 选择特定端口，填写23,135,137-139,445,3389。下一步

图形用户界面, 文本, 应用程序

描述已自动生成

* + 选择阻止连接，下一步

图形用户界面, 文本, 应用程序

描述已自动生成

* + 全选域，下一步

图形用户界面, 文本, 应用程序

描述已自动生成

* + 填写名称，完成

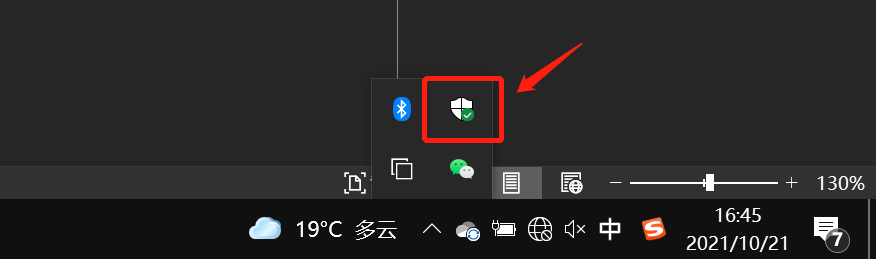
图形用户界面, 应用程序

描述已自动生成

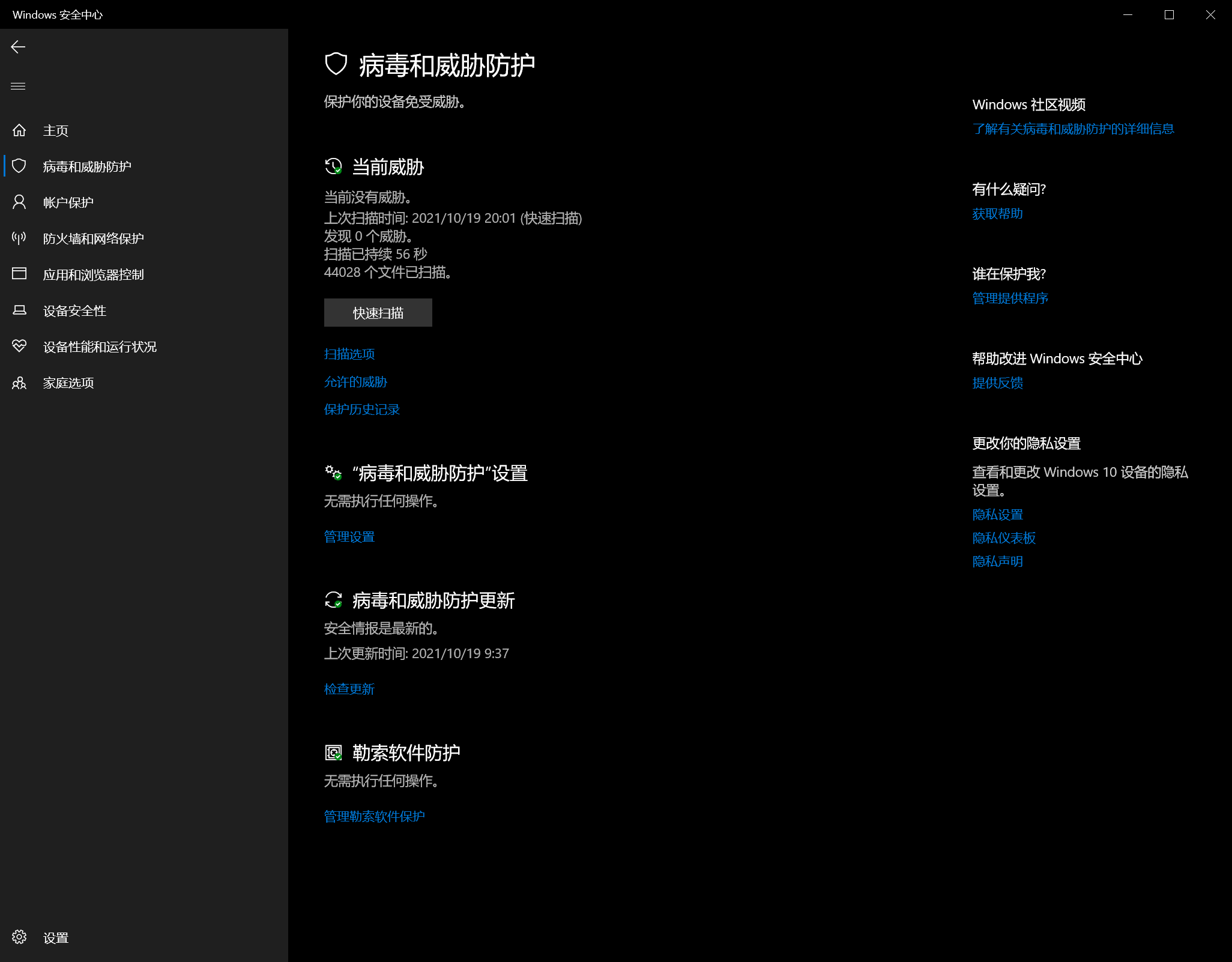
1. Windows7/10（脚本配置）
   * 第一步：右键单机“关闭高危端口.bat”程序
   * 第二步：以管理员身份运行
2. 杀毒软件
3. Windows10
   * 点击小箭头



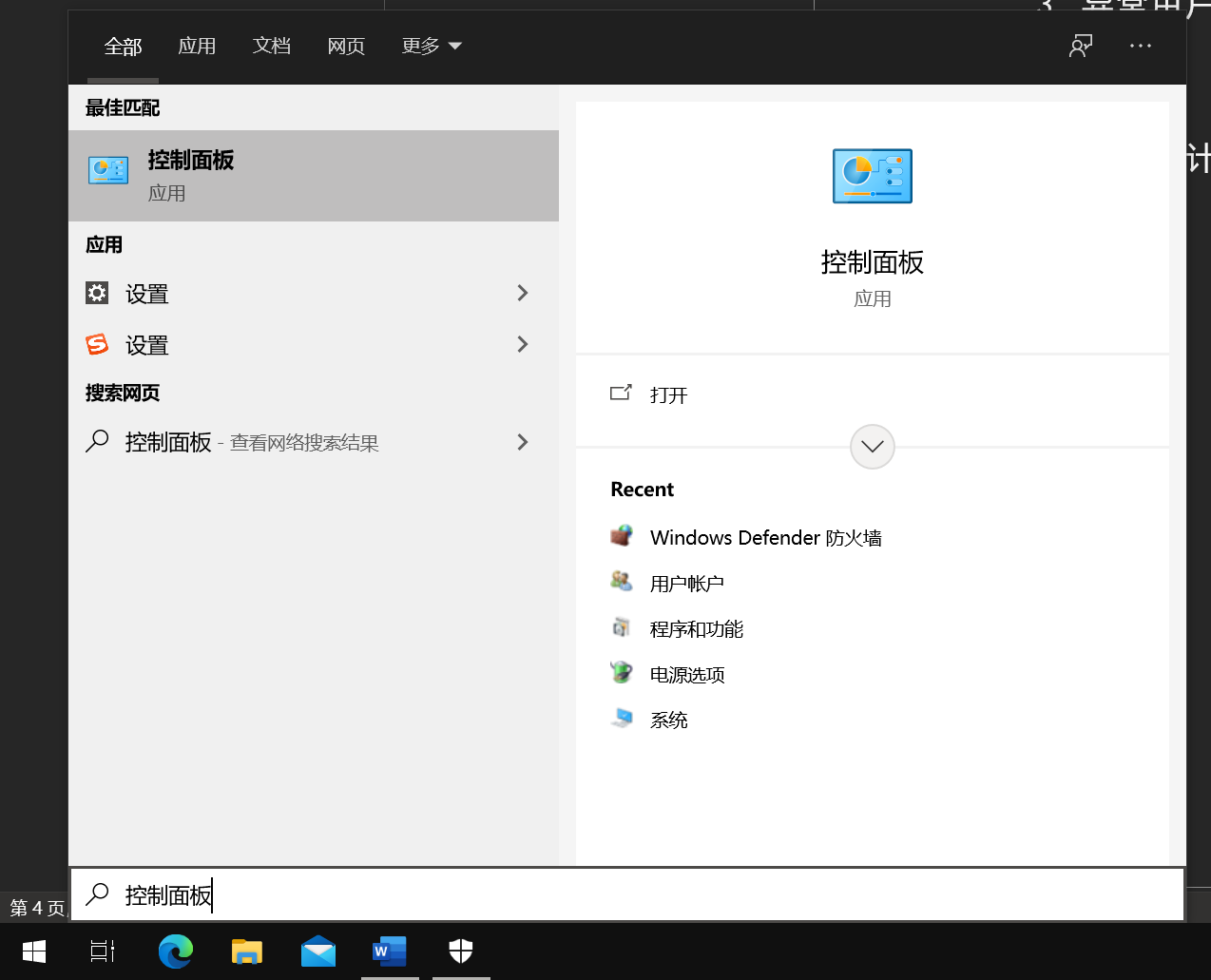
* + 找到一个类似盾牌的小图标（盾牌上有小绿√为杀毒工具正常启用，小红×为存在安全防护问题），点击



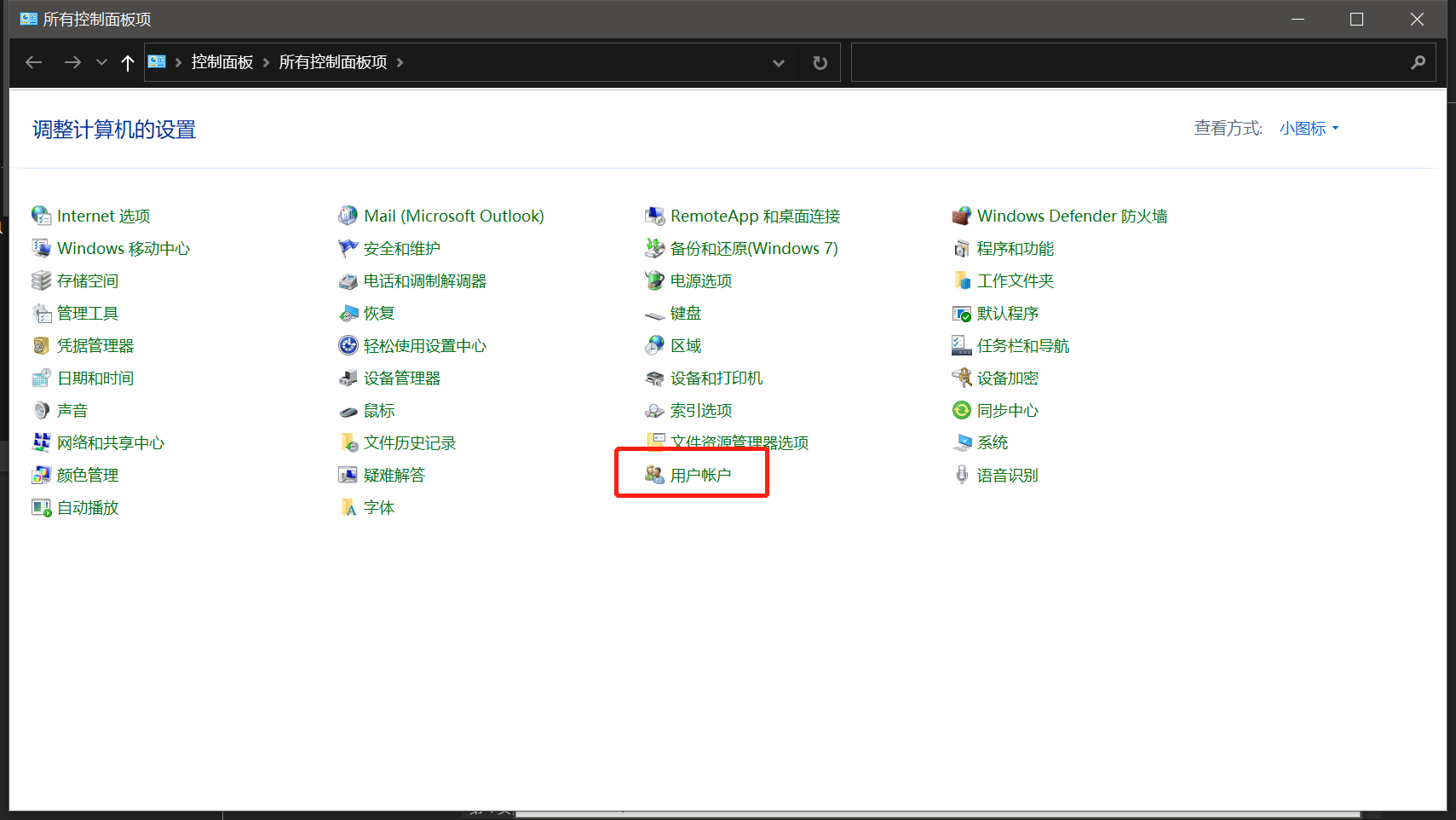
* + 如果未安装第三方杀毒软件，正版windows会启用自带杀毒软件windows defender，只需定期手动或自动更新病毒库，也能实现充分防护。如下图所示：



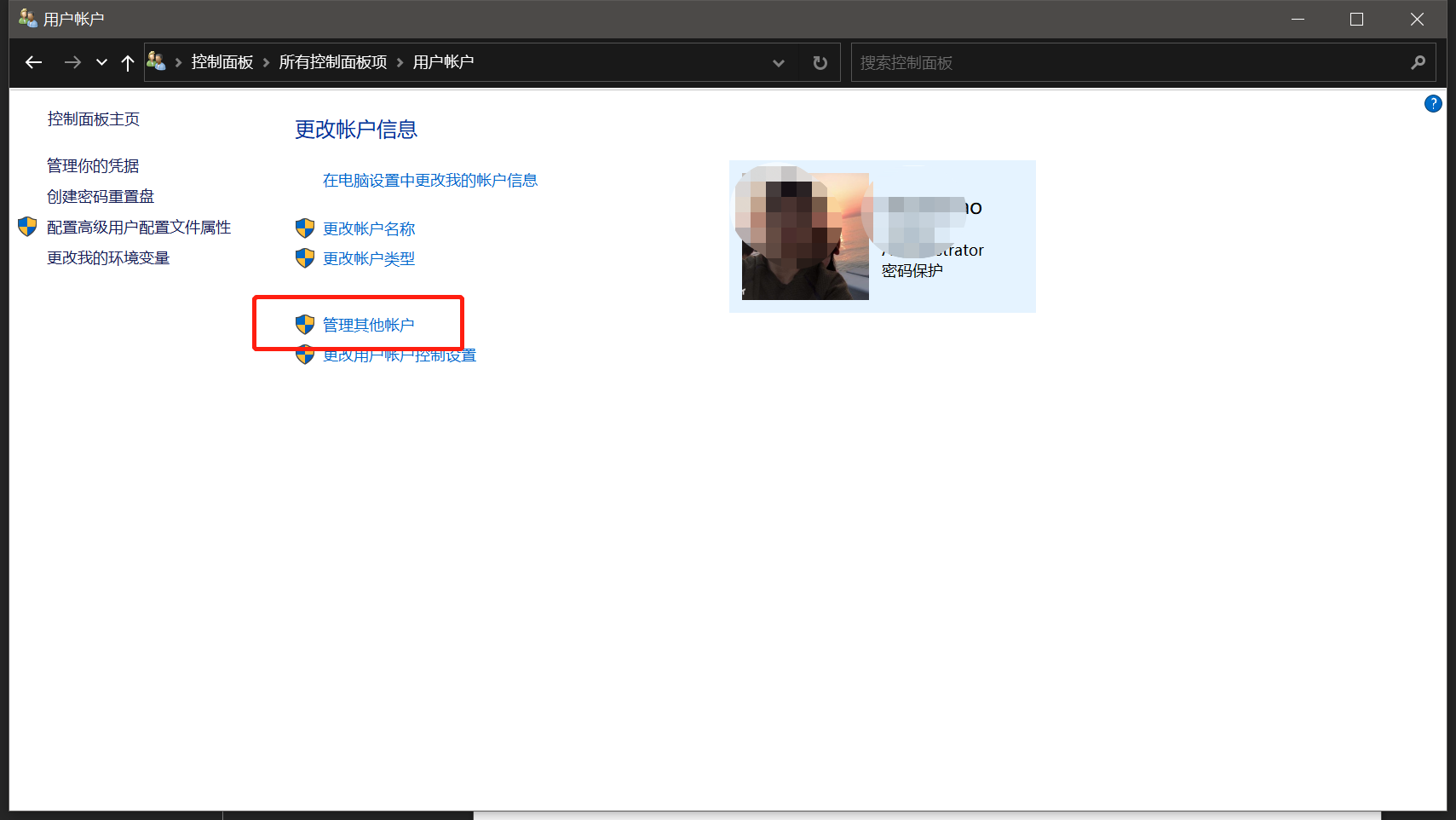
1. 异常用户
2. windows10
   * 在开始菜单中搜索控制面板，并打开



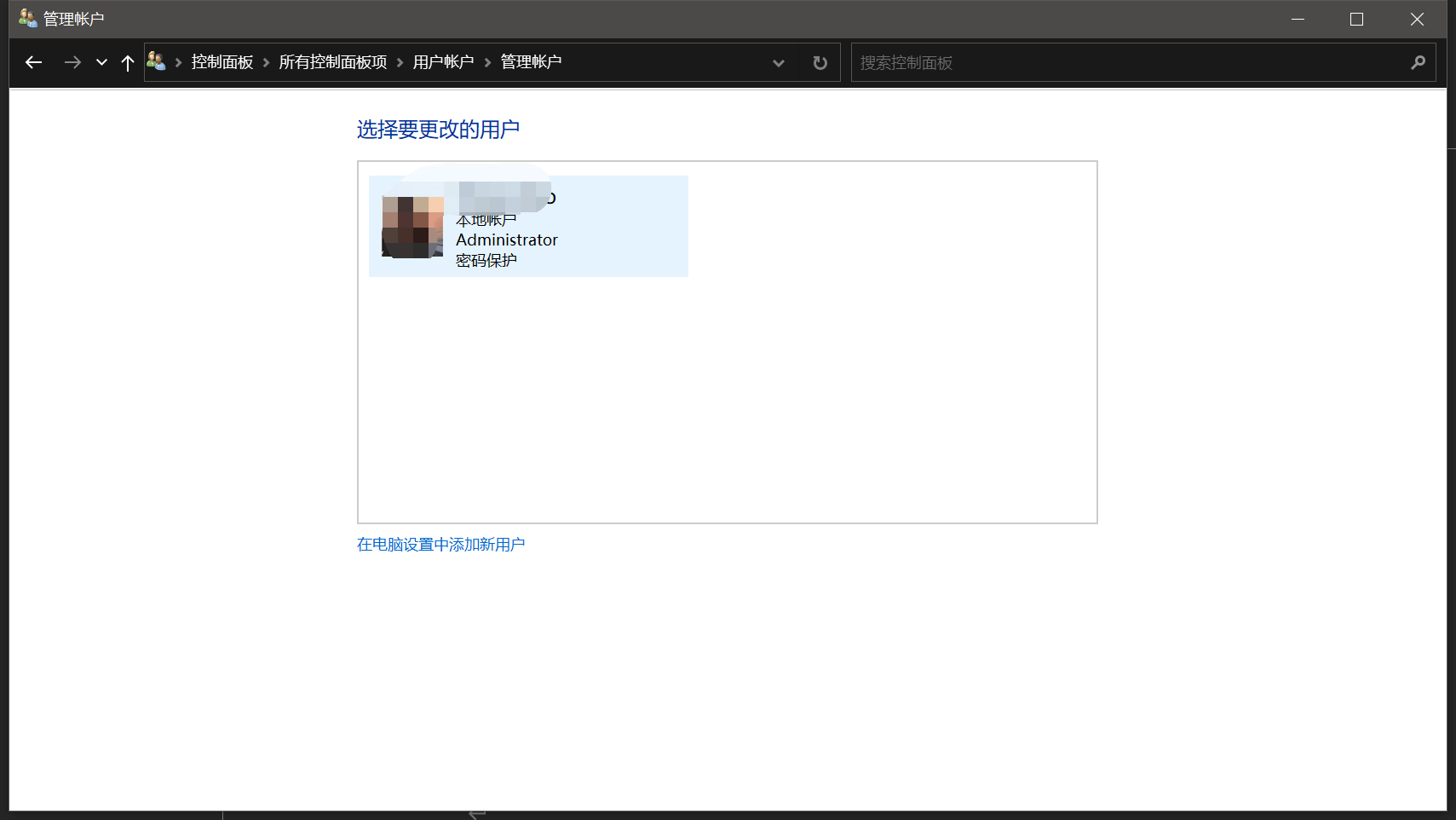
* + 选中“用户账户”



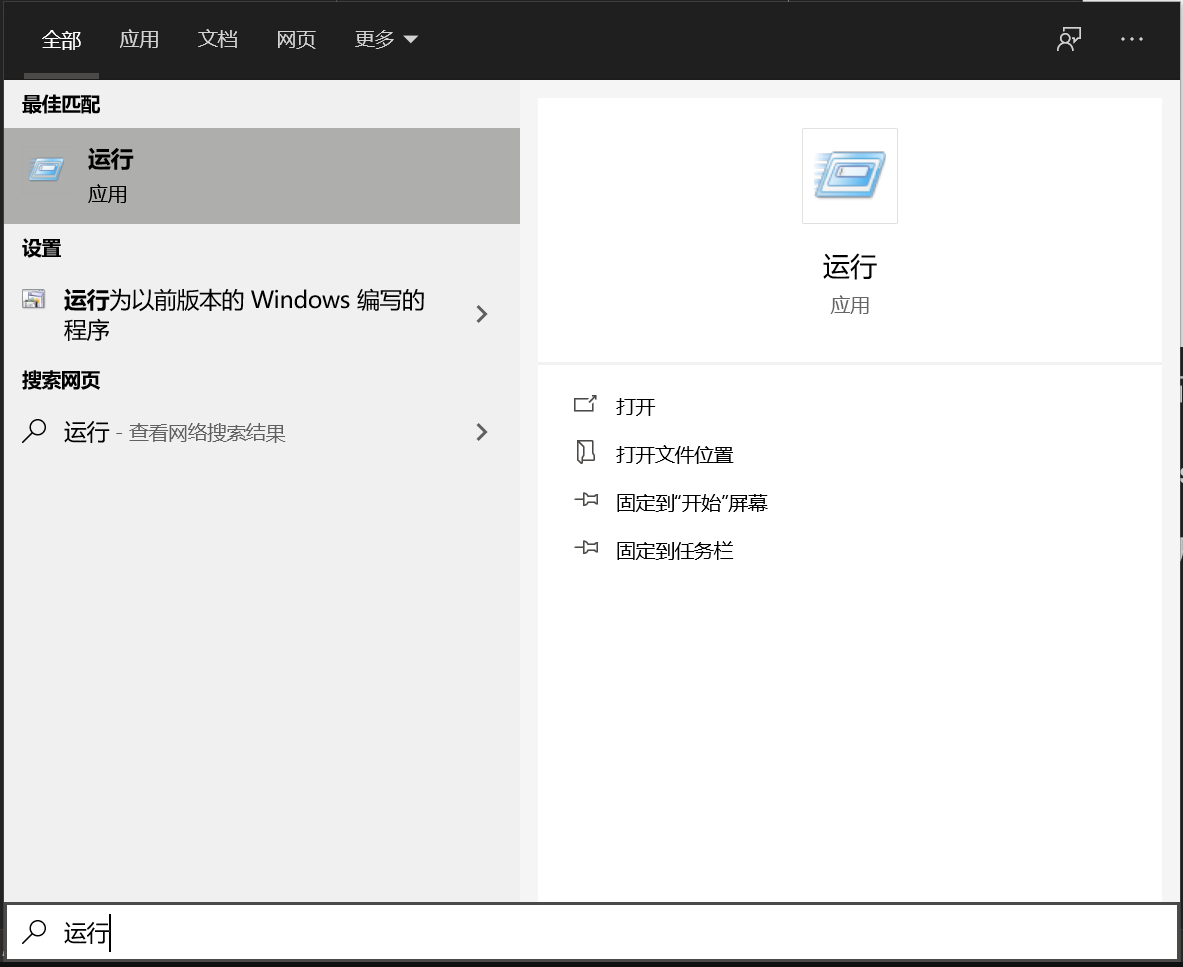
* + 点击“管理其他账户”



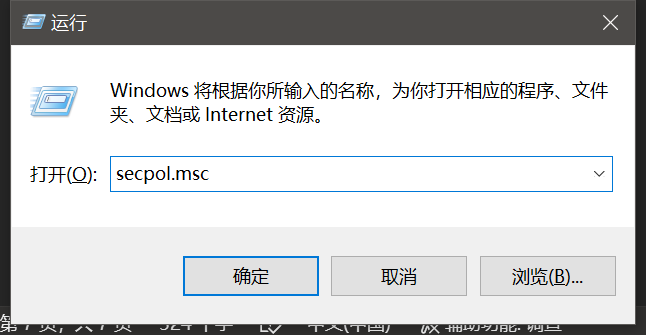
* + 查看是否存在除administrator以外的账户



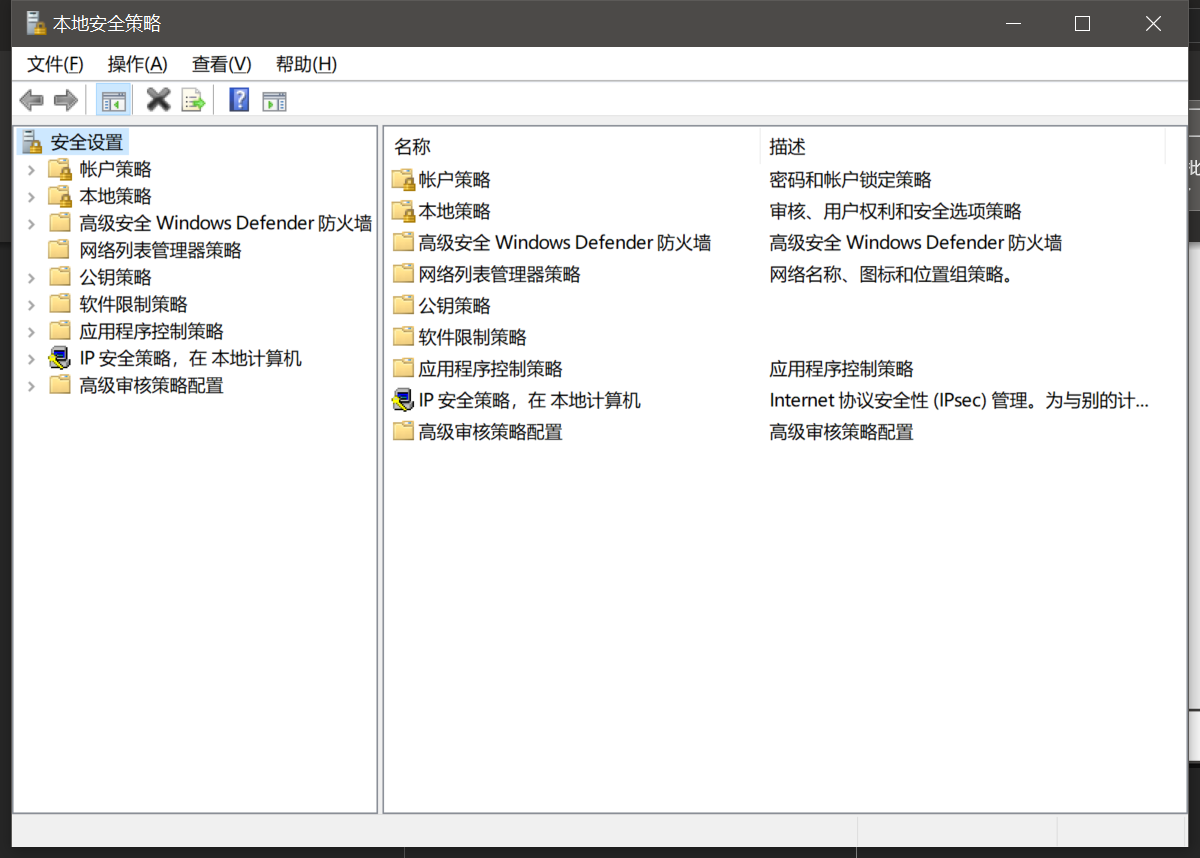
1. 密码审计
2. Windows7/10
3. 非家庭版
   * 在“开始”菜单搜索运行，并点击



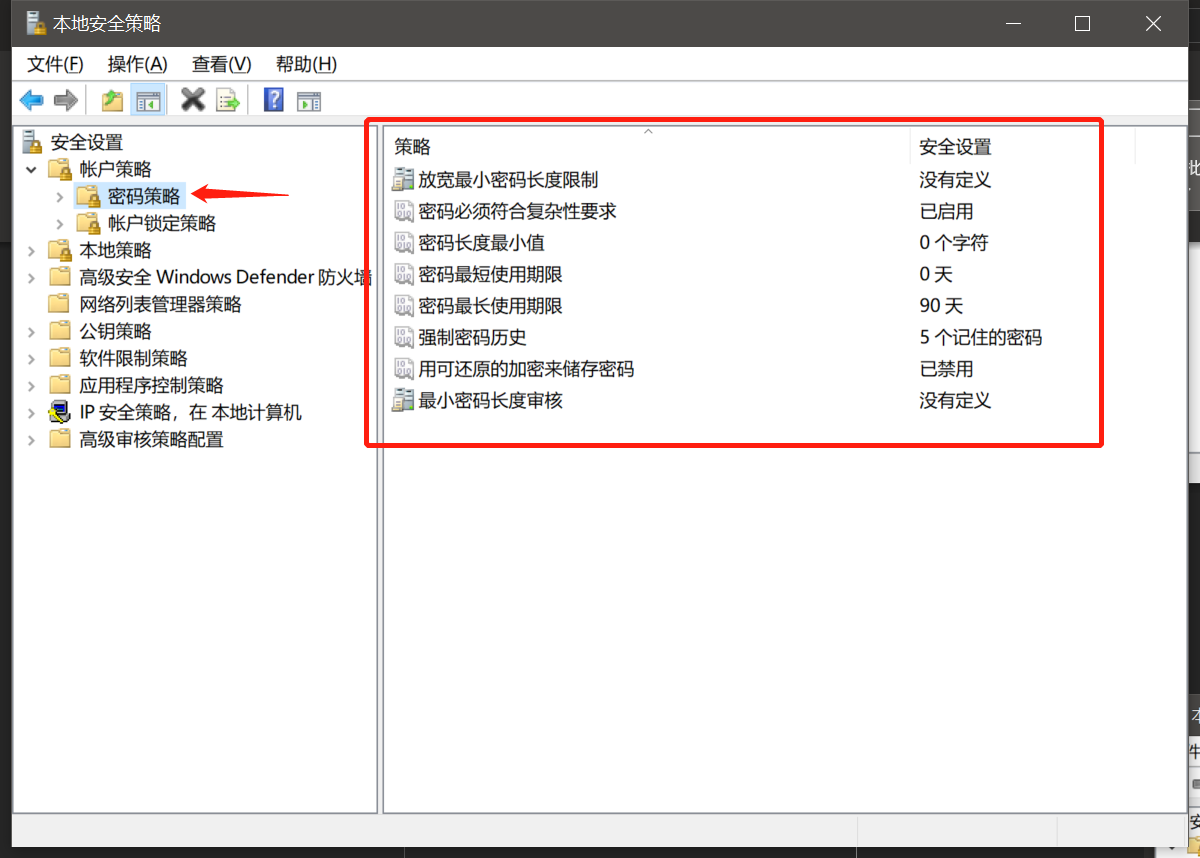
* + 在输入框输入secpol.msc，并确定



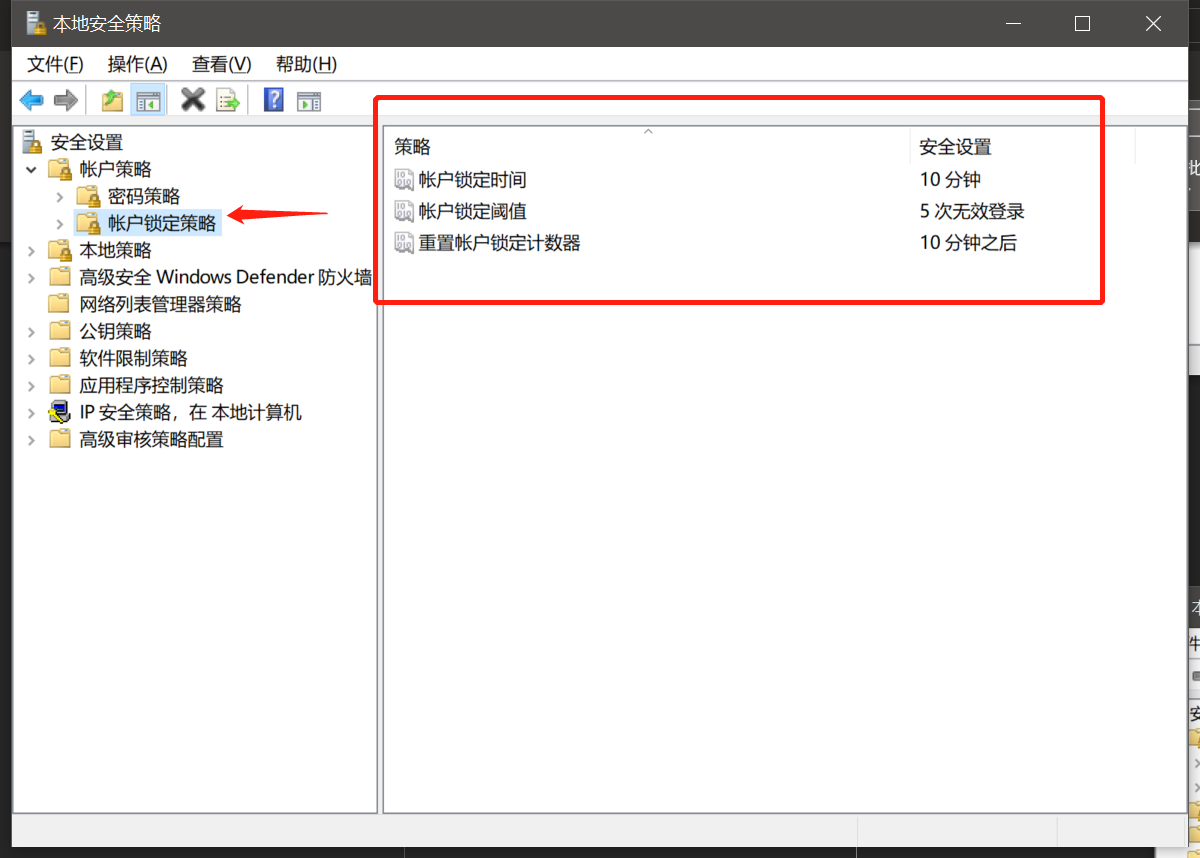
* + 显示如下窗口



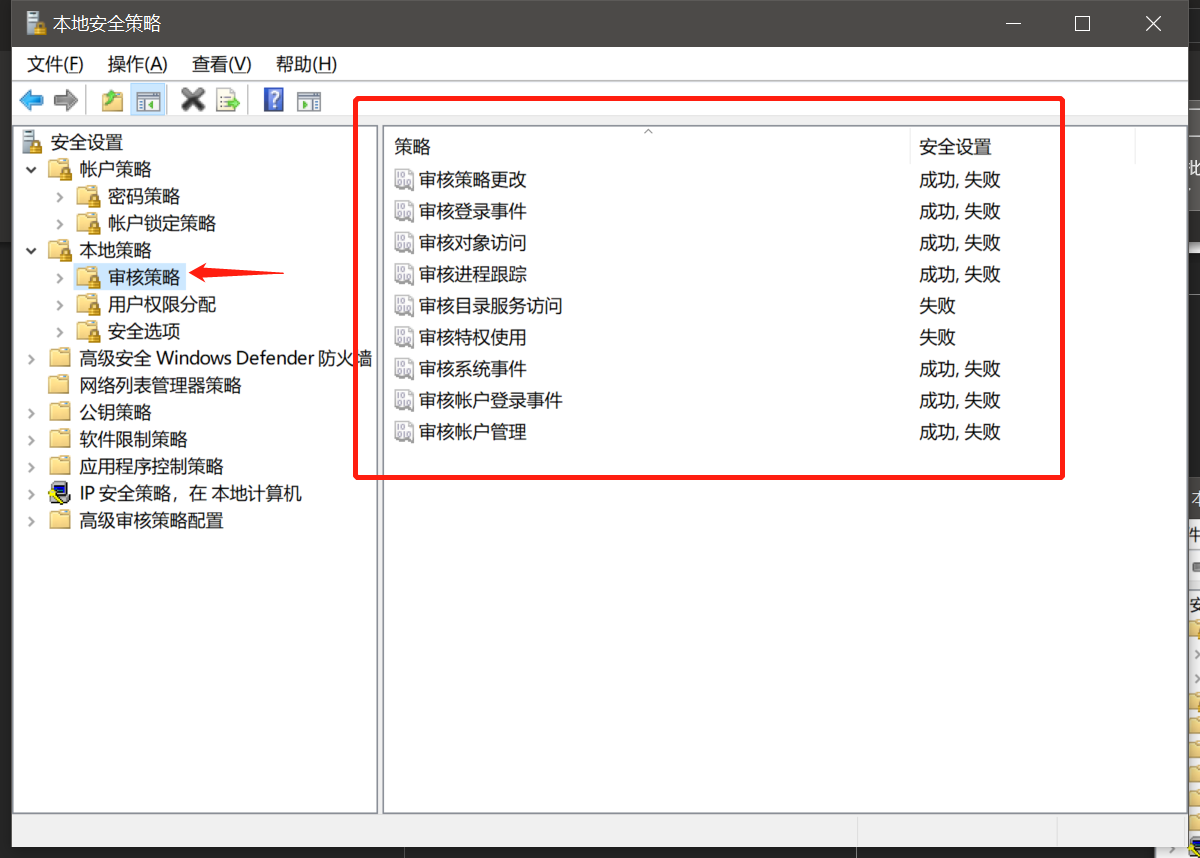
* + 修改策略：安全设置 -> 账户策略 -> 密码策略。如下图所示：



* + 修改策略：安全设置 -> 账户策略 -> 账户锁定策略。如下图所示：



* + - 注意：需要先修改“账户锁定阈值”，才能对其余项进行修改
  + 修改策略：安全设置 -> 本地策略 -> 审核策略。如下图所示：



1. 家庭版

Windows10家庭版默认没有本地安全策略，需要通过脚本开启。

第一步：右键单击“开启本地安全策略.bat”脚本；

第二步：以管理员身份运行；

第三版：等待运行结束后，按照“非家庭版步骤执行”；