实验 - 配置 Windows 本地安全策略

简介

在本实验中，您将配置 Windows 本地安全策略。Windows 本地安全策略用于配置不属于 Active Directory 域的独立计算机的各种安全要求。您将修改密码要求、启用审核、配置某些用户权限，并设置某些安全选项。然后使用事件管理器查看已记录的信息。

建议使用的设备

- 装有 Windows 的计算机。

注意：访问本地安全策略工具的方式因 Windows 版本而异。但是打开之后，本实验中其余步骤的配置是相同的。

第 1 步：查看安全要求。

客户需要根据企业的安全策略，在分支机构配置六个独立 Windows 计算机。这些计算机不属于 Active Directory 域。必须在每台计算机上手动配置策略。

安全策略如下：

- 密码必须至少为 8 个字符。
- 必须每 90 天更改一次密码。
- 用户可以一天更改一次密码。
- 用户必须至少在 8 次密码更改中使用唯一的密码。
- 密码必须包含以下四个要素中的三个要素：
  - 至少一个小写字母字符。
  - 至少一个大写字母字符。
  - 至少一个数字字符。
  - 至少一个符号字符。
- 如果用户尝试 5 次之后未能输入正确的密码，计算机将会锁定。用户必须等待 5 分钟，锁定计时器才能重置。
- 应启用审核策略的每个安全设置。
- 在处于非活动状态 30 分钟后，用户将被自动注销。（仅适用于 Windows 8.1 和 8.0）
- 用户必须先登录，然后再从扩展坞取下笔记本电脑
- 在登录时，用户应该会看到以下标题和文本：
  - 标题：**警告：**
  - 文本：**您的活动将被监控。此电脑仅用于商业用途。**
- 密码过期 7 天前，用户将收到更改密码的提醒。

Windows 本地安全策略工具还提供了许多其他设置，但这些内容不在本课程的讨论范围内。

第 2 步：打开 Windows 本地安全策略工具。

a. 要在 Windows 7 和 Vista 中访问本地安全策略，请使用以下路径：

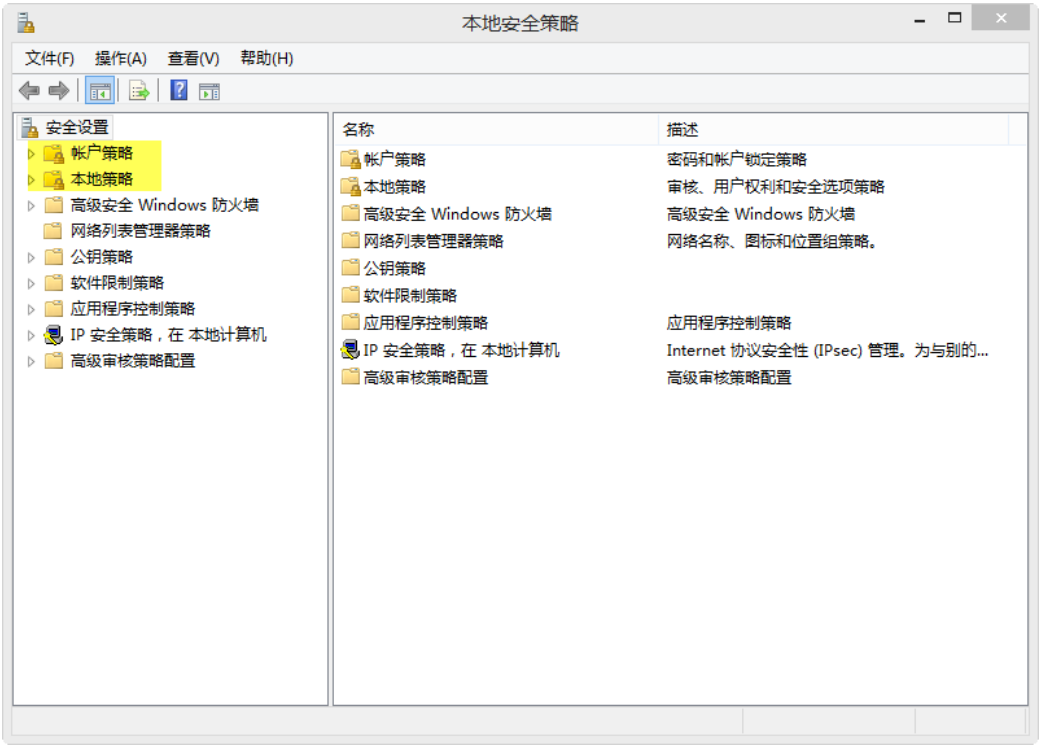
开始>管理工具>本地安全策略

b. 要访问 Windows 8 和 8.1 中的本地安全策略工具，请使用以下路径：

搜索>secpol.msc，然后单击 **secpol**。

c. **“本地安全策略”**窗口打开。本实验将重点介绍**“帐户策略”**和**“本地策略”**，如下图所示。**“安全设置”**的其余内容不在本课程的范围内。

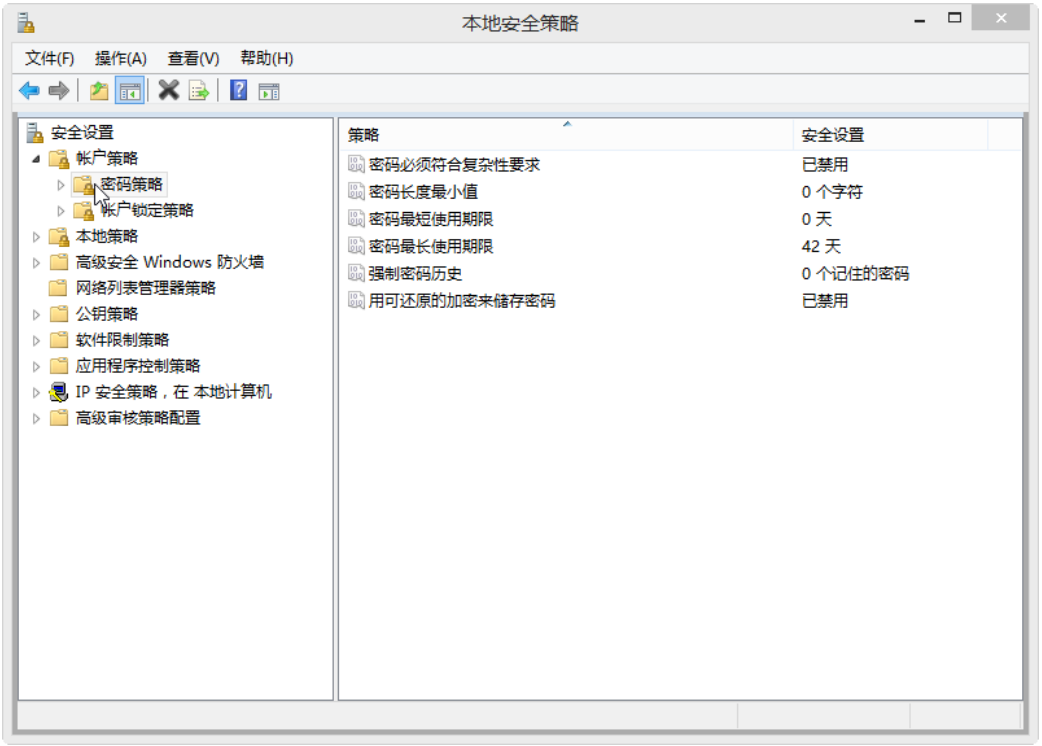
注意：本实验将使用 Windows 8.1 中的截图。



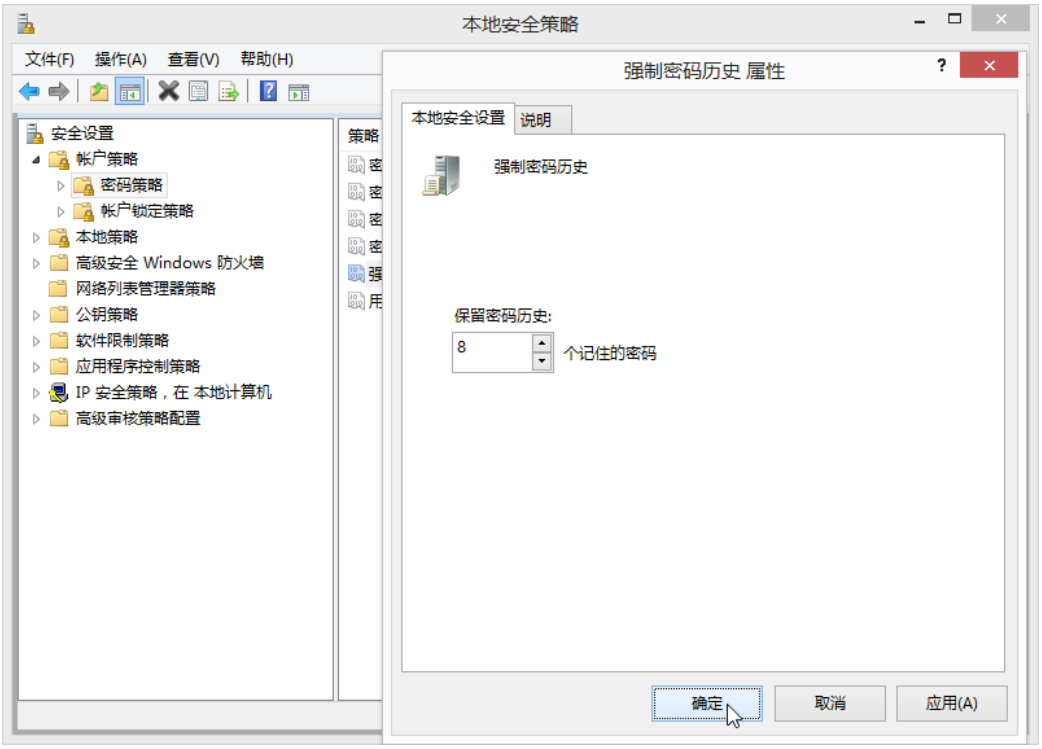
第 3 步：配置“密码策略”安全设置。

公司安全策略的前六个要求在**“本地安全策略”**工具的**“帐户策略”**部分配置。

a. 单击**“帐户策略”**旁边的箭头将其展开，然后单击**“密码策略”**。右侧面板中会显示六个策略及其相关的安全设置。



b. 第一个策略是**“强制密码历史”**，用于设置用户在重新使用某个密码前必须输入的唯一密码的次数。根据第 1 步中的企业安全策略，此策略的安全设置应为 **8**。双击**“强制密码历史”**，打开**“强制密码历史属性”**窗口。将此值设置为 **8**。

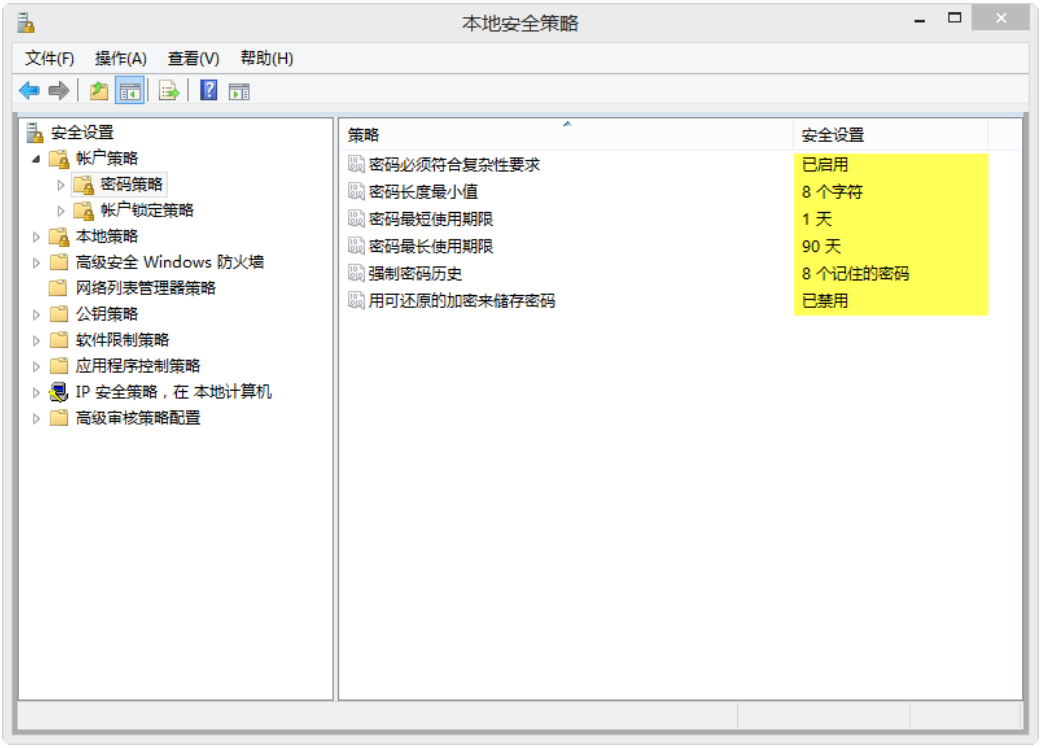


c. 使用第 1 步中的安全策略要求，填写您应为**“本地安全策略”**中的其余**密码策略**安全设置设定的值。

策略	安全设置
强制密码历史	8
密码最长期限	
最短密码期限	
最短密码长度	
密码必须满足复杂性要求	
用可还原的加密来储存密码	已禁用

注意：应始终禁用**“用可还原的加密来储存密码”**安全设置。用可还原的加密来储存密码基本上与储存密码的超文本版本是相同的。因此，除非应用要求比保护密码信息更重要，否则切勿启用此策略。

d. 双击每个策略并根据上表中的条目设置值。完成后，您的配置应如下所示：



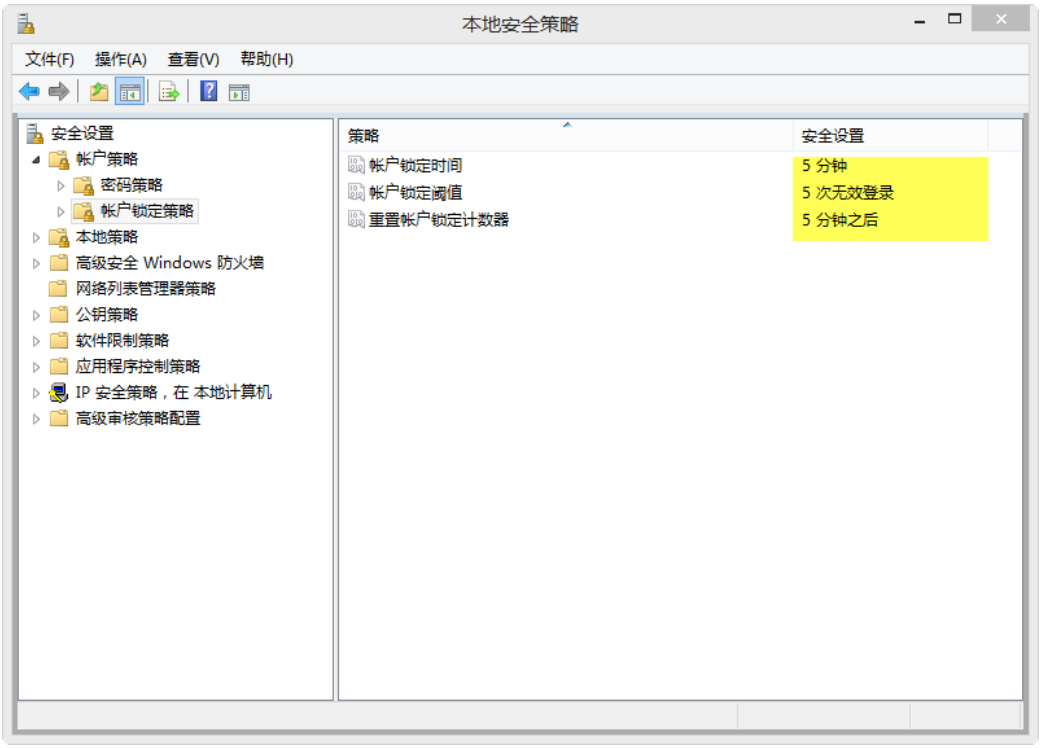
第 4 步：配置“帐户锁定策略”安全设置。

a. 根据第 1 步中的安全策略，用户尝试登录多少次后帐户将会被锁定？

b. 用户必须等待多久后才能再次尝试登录？

c. 使用**“本地安全策略”**中的**“帐户锁定策略”**安全设置来配置策略要求。完成后，您的配置应如下所示：

提示：您需要先配置**“帐户锁定阈值”**。

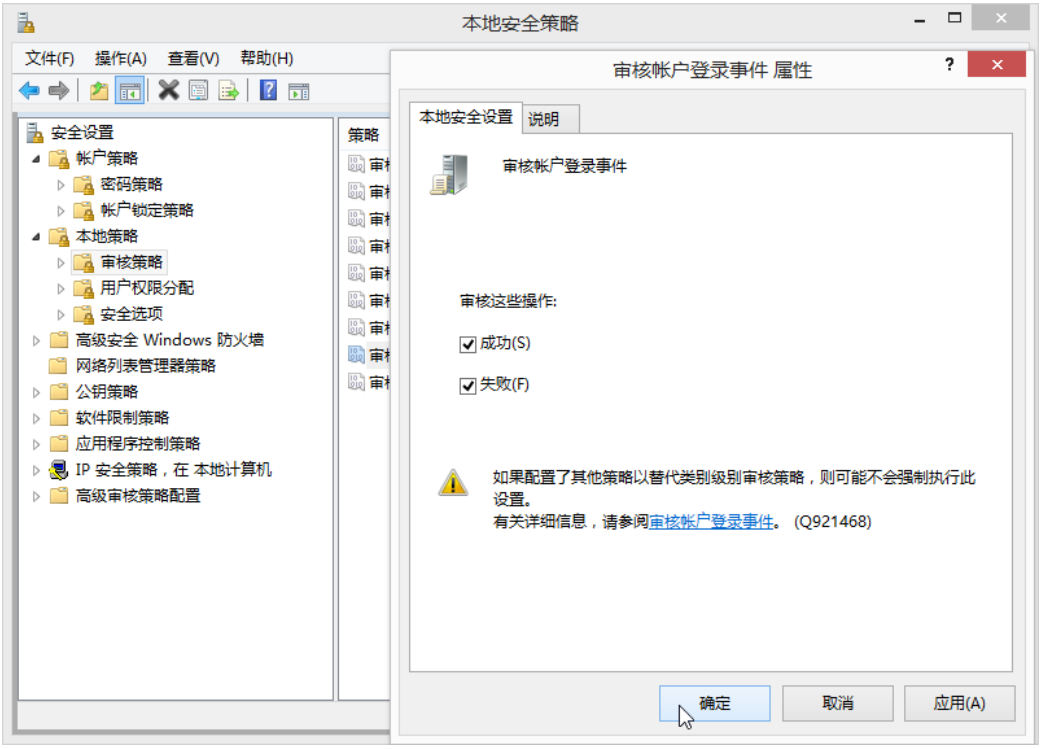


第 5 步：配置“审核策略”安全设置。

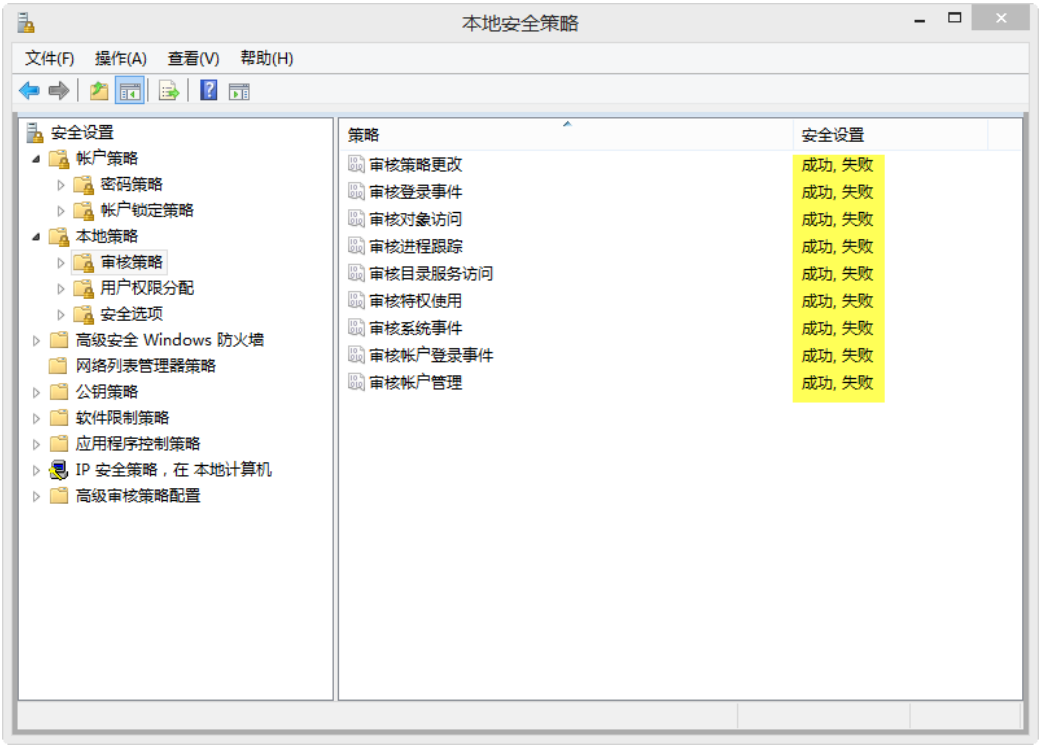
a. 在**“本地安全策略”**中，展开**“本地策略”**菜单，然后单击**“审核策略”**。

b. 双击**“审核帐户登录事件”**，打开**“属性”**窗口。单击**“说明”**选项卡了解此安全设置。

c. 单击**“安全设置”**选项卡，然后单击**“成功”**和**“失败”**复选框。单击**“确定”**关闭**“属性”**窗口并应用安全设置。

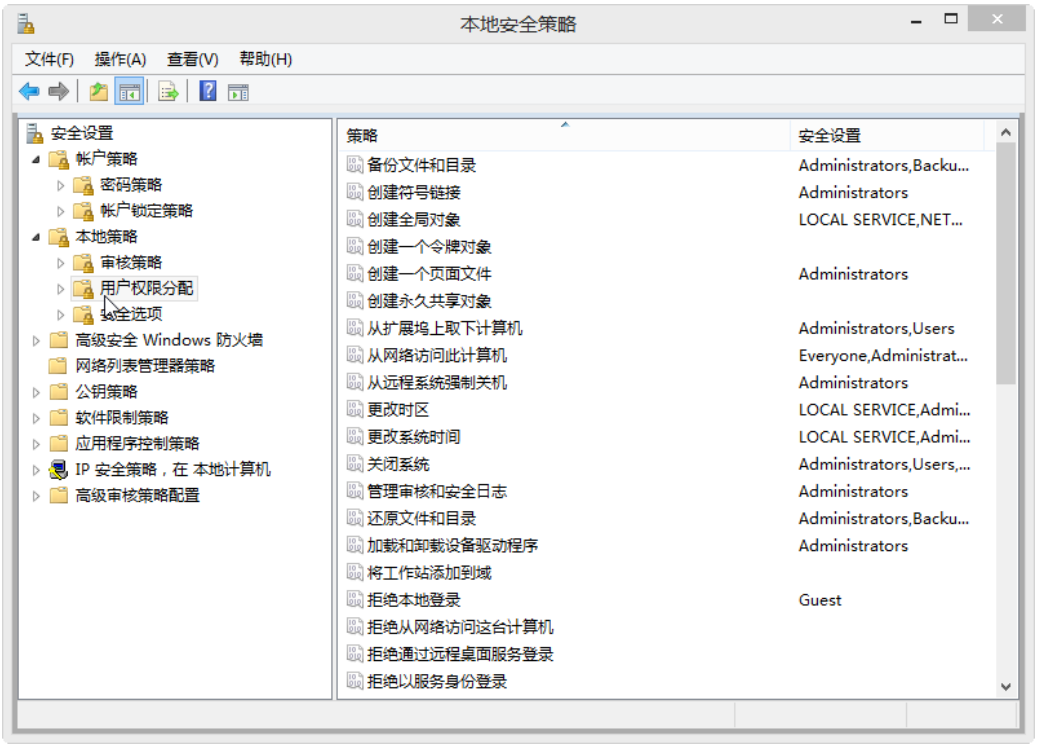


d. 继续修改**“审核策略”**安全设置的其余设置。单击每个设置的**“说明”**选项卡，了解其用途。单击每个**“属性”**窗口中的**“成功”**和**“失败”**复选框。完成后，您的**“审核策略”**配置应如下所示：



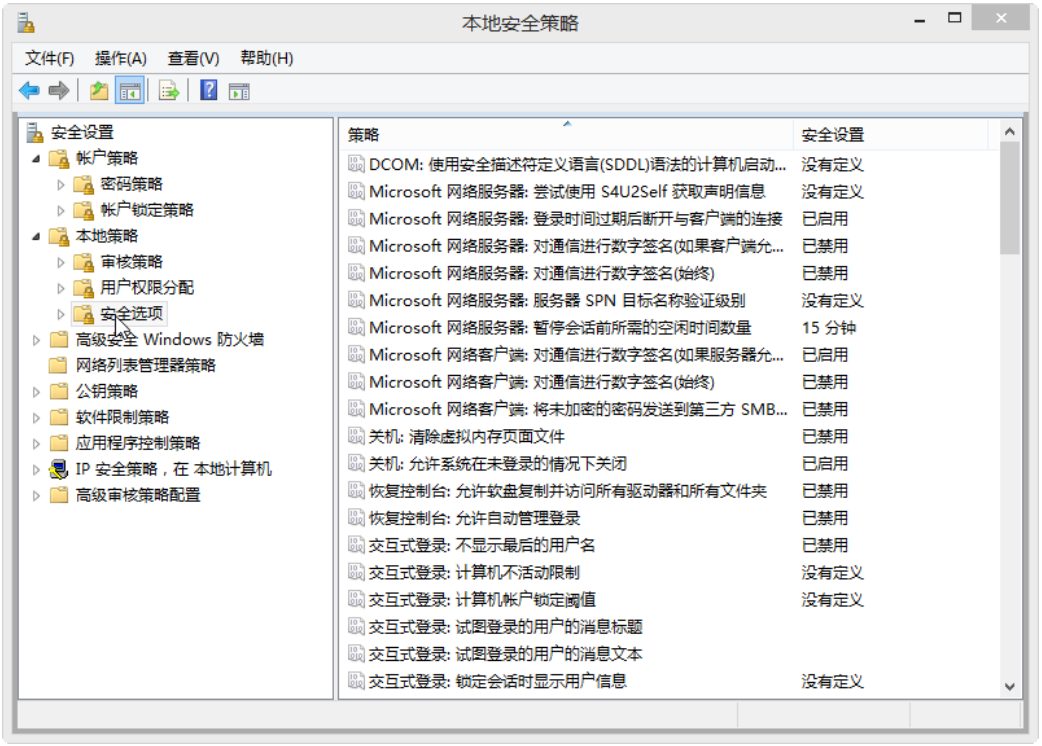
第 6 步: 配置其他本地策略安全设置

a. 在**“本地安全策略”**中，单击**“本地策略”**下的**“用户权限分配”**，查看安全设置。



b. 虽然不需要修改安全设置来满足安全策略要求，但应该花一些时间查看默认设置。您是否会建议更改任何设置？为什么？

c. 在**“本地安全策略”**中，单击**“本地策略”**下的**“安全选项”**，查看安全设置。



d. 使用第 1 步中的其余安全策略要求，在下表中列出您需要在**“安全选项”**中更改的策略和安全设置值。第一项已经为您完成。

策略	安全设置
交互式登录：计算机不活动限制（仅适用于 Windows 8.1 和 8.0）	1800 秒

第 7 步：测试密码策略安全设置。

a. 尝试更改密码，测试您的密码策略安全设置。尝试一个不符合长度或复杂性要求的新密码。

在 Windows 7 和 Vista 中，请使用以下路径：

控制面板>用户帐户>更改您的密码

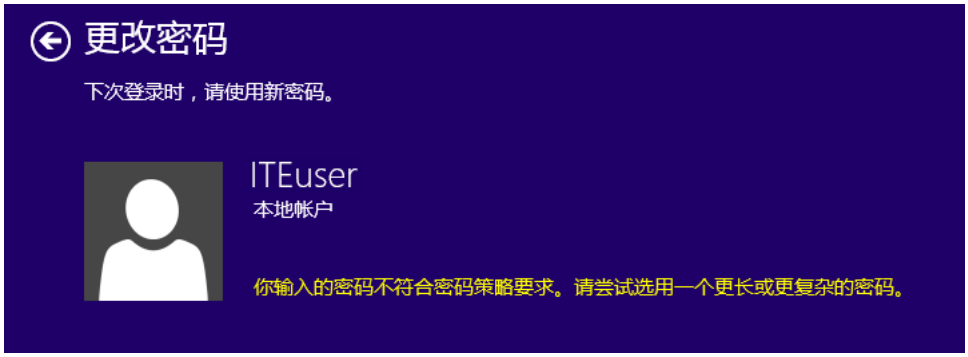
在 Windows 8.1 中，请使用以下路径：

控制面板>用户帐户>在电脑设置中更改我的帐户信息>登录选项，然后单击**“密码”**下方的**“更改”**。

在 Windows 8.0 中，请使用以下路径：

控制面板>用户帐户>在电脑设置中更改我的帐户信息，然后单击**“更改密码”**。

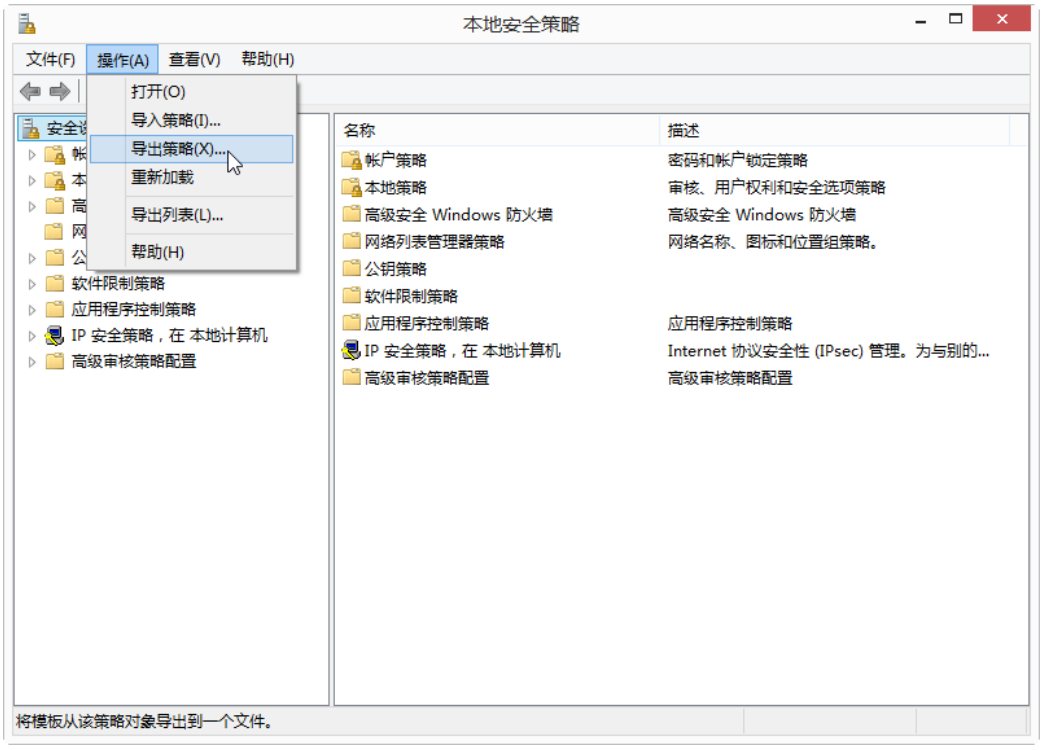
b. 您应该收到一条消息，指示您的新密码不符合密码策略要求，例如 Windows 8.1 中的以下消息：



第 8 步：导出和导入安全策略设置。

客户还有 5 台必须满足相同安全策略要求的独立计算机。客户不需要手动配置每台计算机的设置，只需要导出这台计算机上的设置。

a. 从**“本地安全策略”**菜单栏中，单击**“操作”>“导出策略…”**



b. 为 **.inf** 文件选择一个名称，并保存到您选择的位置。

c. 将安全策略 **.inf** 文件复制到闪存驱动器。将闪存驱动器拿到另一台计算机处。插入闪存驱动器，打开**“本地安全策略”**，然后单击**“操作”>“导入策略…”**找到闪存驱动器上的 **.inf** 文件并打开该文件，对新计算机应用安全策略。