HongKe 虹科

使用案例指南

如何排除账户锁定故障

目录

1.导言

活动目录审计是确保合规性和 IT 环境安全性的重要组成部分。然而，活动目录管理员面临的一个常见问题是 如何确定账户锁定的来源。如果用户账户因任何原因被锁定，例如他们尝试使用错误的用户名登录，这可能会 导致停机，而查找锁定源并重新启用账户往往是一个耗时且令人沮丧的过程。

在本指南中，我们将探讨账户锁定的一些根本原因，以及简化故障排除过程的方法。

2.账户锁定的常见原因

账户锁定是一种常见现象，发生锁定的原因多种多样，因此查找根本原因可能非常耗时且具有挑战性。以下是一些常见原因：

- 使用旧凭证映射驱动器

  可将映射驱动器配置为使用用户指定的凭证连接到共享资源。之后，用户可以更改密码，而无需更新映射驱动器中的凭据。凭据也可能过期，从而导致账户锁定。

- 使用旧缓存凭证的系统

  有些用户需要在多台计算机上工作。因此，用户可以同时登录多台计算机。这些其他计算机上的应用程序可能正在使用旧的缓存凭据，这可能导致账户被锁定。

- 使用旧凭证的应用程序

  在用户的系统中，可能有多个应用程序会缓存用户的凭据或在配置中明确定义用户的凭据。如果用户的凭据过期且未在应用程序中更新，账户就会被锁定。

- 使用过期凭证的 Windows 服务

  Windows 服务可配置为使用用户指定的账户，即服务账户。这些用户指定账户的凭证可能会过期，ÁWindows 服务将继续使用过期的旧凭证，从而导致账户锁定。

- 计划任务

  无论用户是否登录，Windows 任务调度程序都需要凭据才能运行任务。可以使用用户指定的凭据（可以是域凭据）创建不同的任务。这些用户指定的凭据可能会过期，而 Windows 任务将继续使用旧凭据。

3.如何解决帐户锁定问题

微软提供了账户锁定状态（LockoutStatus.exe）工具来简化确定账户锁定状态的过程。该工具融合了命令行和图形工具，但使用起来比较复杂，而且可能比较耗时。

4.Lepide解决方案

Lepide的账户锁定功能简化了识别账户锁定状态的过程。通过生成账户锁定报告，Lepide 解决方案可确保您轻松识别哪些账户被锁定、锁定发生的时间，并检查账户锁定来自哪台机器。

生成报告后，就可以使用 Lepide Investigator 工具来确定造成锁定的确切原因。利用其内置的远程管理功能，您可以立即解锁账户或重置密码。

整个过程使得管理和维护 Active Directory 中的用户和服务账户状态变得非常容易，尤其是在关键的、时间敏感的情况下。

4.1. 账户锁定报告

如果用户尝试使用错误的用户名登录，则会在域控制器上生成该事件。Lepide 解决方案会从域控制器中读取该事件，并在账户锁定报告中提供锁定的所有详细信息：

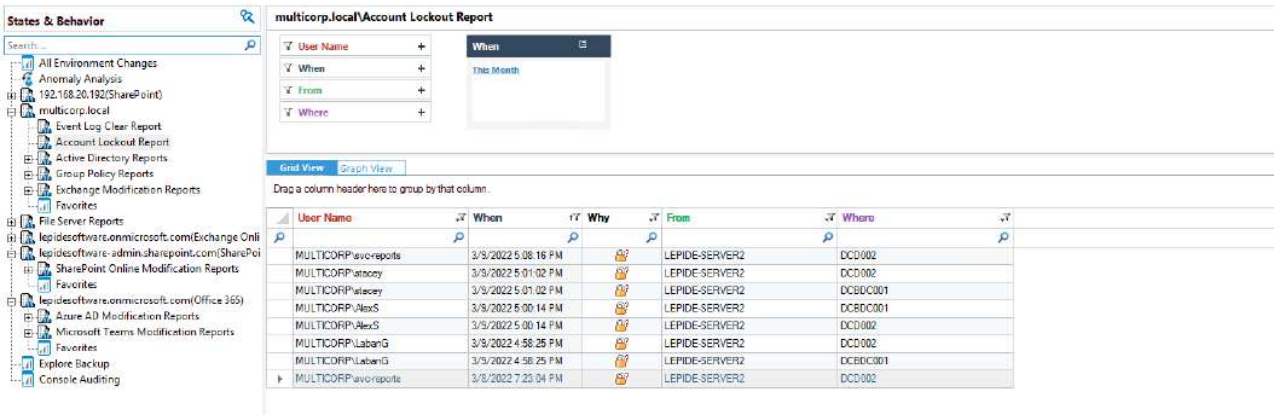

图1: 账户锁定报告

4.2. 账户锁定调查员

Lepide 数据安全平台有一个名为 "账户锁定调查器 "的内置模块，您可以使用该模块找出任何锁定的原因。

Investigator 工具可通知 IT 管理员有关 Active Directory 账户锁定问题。它有助于简化和加快对锁定根本原因的调查， 并提供从工具本身解锁用户账户的功能。

主要功能

- 实时检测账户锁定
- 加快对根本原因的调查
- 通过直观的界面快速解锁账户
- 减轻 IT 服务台的压力
- 证明符合您的 Active Directory锁定策略
- 通过识别锁定的服务账户来实现 SLA

5.生成账户锁定报告

5.1. 先决条件

在报告账户锁定并发出警报之前，您需要添加并配置 Active Directory 以启用审计。

配置完成后，您将能够看到所有账户锁定事件，因为 Lepide 数据安全平台提供实时警报和报告。

5.2. 如何运行账户锁定报告

账户锁定报告可确定特定时间段内的任何账户锁定情况。报告生成方式如下：

- 单击用户实体和分析图  显示状态和行为窗口 屏幕左侧以树形结构显示报告列表

- 展开活动目录节点
- 点击账户锁定报告：

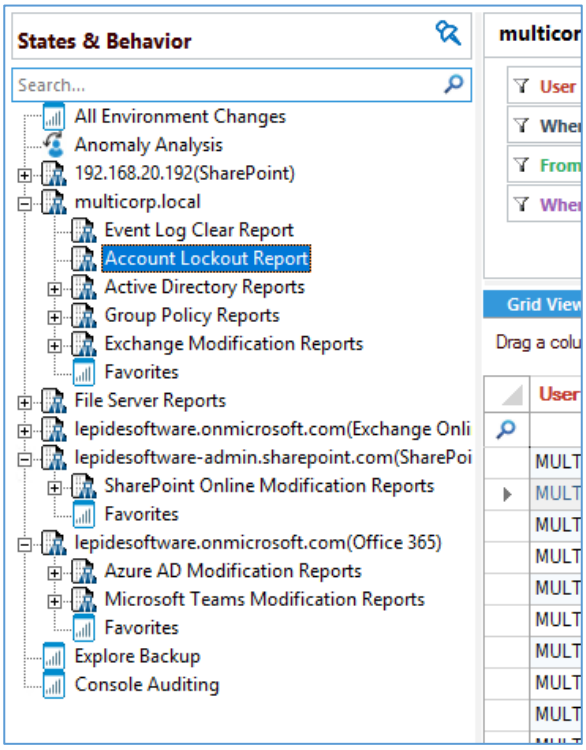

图 2:报告清单

单击何时框并选择报告的日期范围

- 单击＂生成＂运行报告
  账户锁定报告会生成，每一行都会显示有关锁定的完整信息：

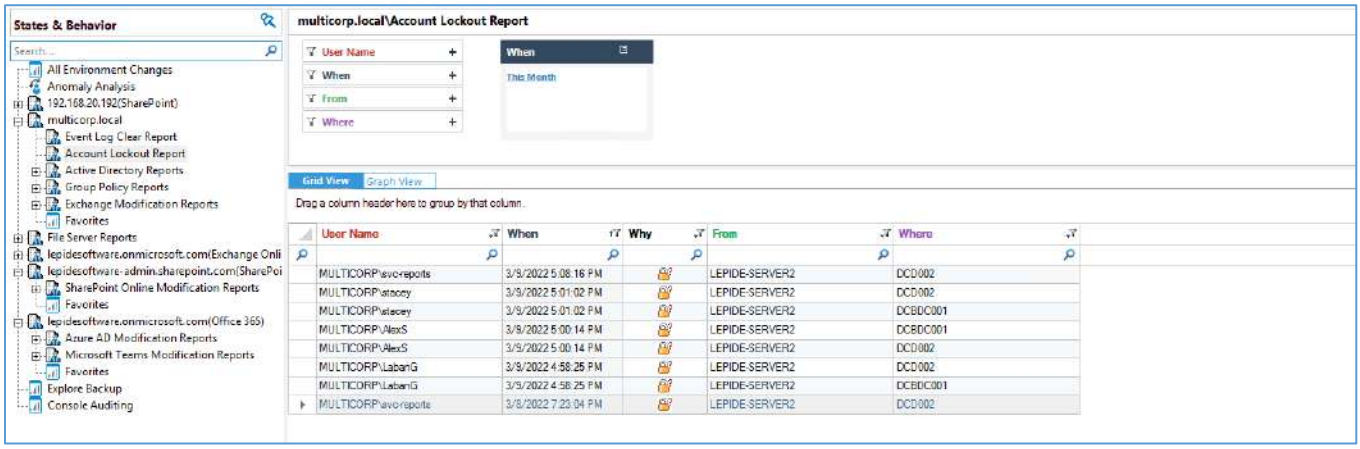

图 3:账户锁定报告

报告包括以下内容

账户被锁定的用户名

锁定发生的日期和时间

锁定发生的原因。单击此栏中的图标可进入调查器，具体说明如下

源计算机，账户在该计算机上进行 Active Directory 身份验证

收到身份验证请求的域控制器地址

5.3. 解锁账户和重置密码

可以在 Lepide 解决方案中解锁账户和重设密码。这可以通过右键菜单完成：

- 右键单击一行可显示与该行相关的上下文菜单。这将为您提供以下选项：解锁、重置密码和调查。

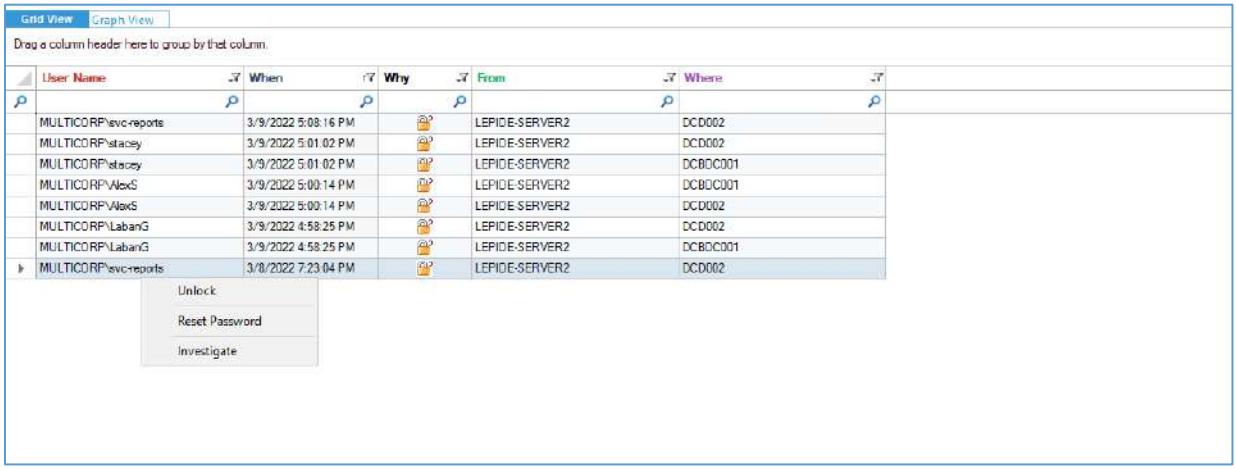

图 4:上下文菜单

解锁账户

- 点击该选项可解锁所选用户账户。解锁后会显示以下信息：

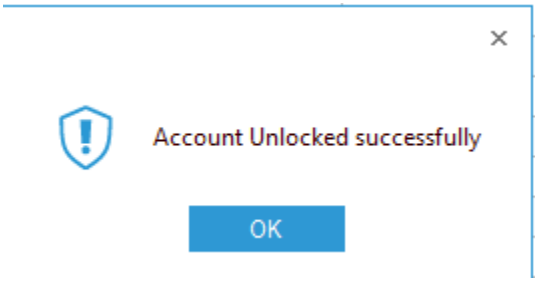

图 5: Account Unlocked Successfully

重置密码

重置用户密码

- 右键单击需要重置密码的用户行。
- 点击右键菜单中的重置密码。
- 输入新密码，然后确认。
- 选择用户必须在下次登录时更改密码选项，强制用户在下次登录时更改密码。

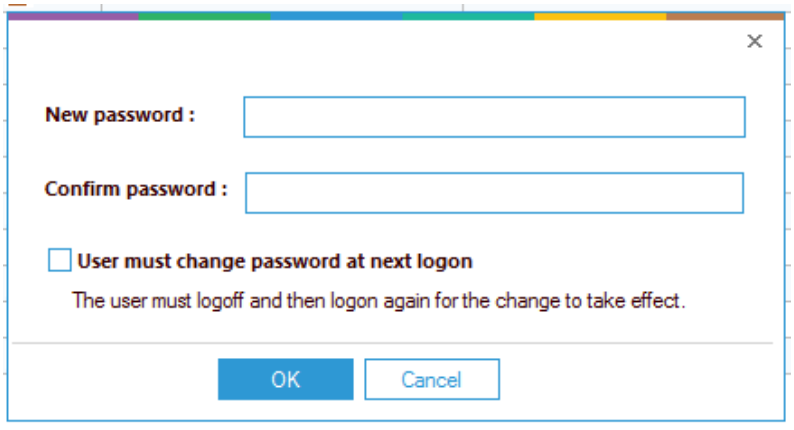

图 6: 重置密码

6.Lepide 账户锁定调查员

账户锁定报告可提供被锁定账户的所有详细信息。但你也可以

想知道账户锁定的原因。为此，您可以使用 Lepide 账户锁定调查器。

6.1. 使用 Lepide 账户锁定调查器

使用调查员工具：

- 从上下文菜单（右键单击一行显示）中选择 "调查显示对话框
- 单击 "生成报告 "生成报告，查看账户锁定的原因：

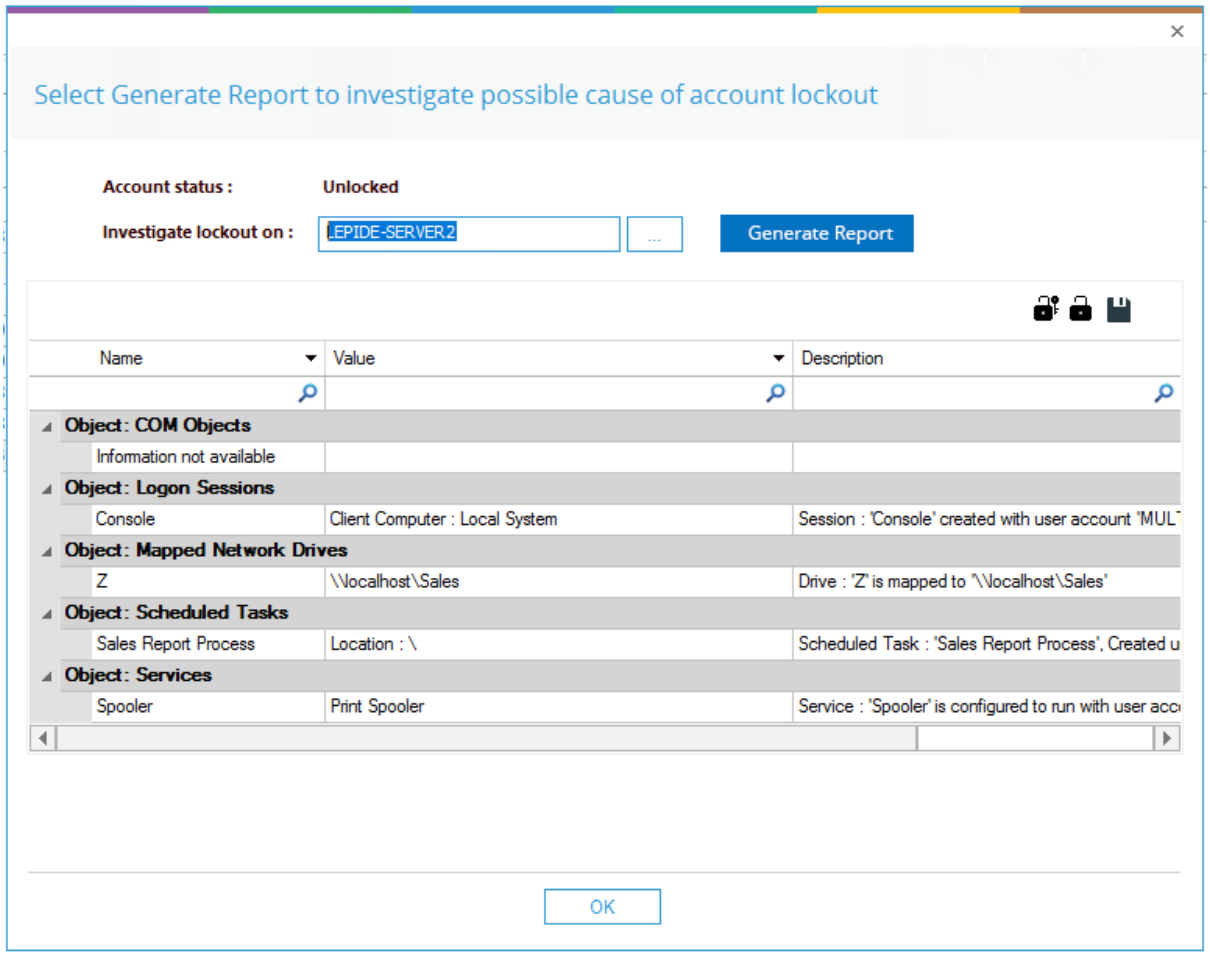

图 7: 锁定调查员

该解决方案将从以下 5 个方面找出账户锁定的原因：

- **计算机对象** 与凭证相关的任何计算机对象
- 映射网络驱动器： 该机器上是否存在该用户账户映射的网络驱动器
- 服务： 使用这些凭据登录的机器上存在的任何服务
- 计划任务： 任何被配置为每天、每周或每月运行的计划任务，这些任务使用这些凭据。可能使用的是旧密码，这将导致帐户锁定

- **登录会话**： 是否有任何使用这些凭证的活动登录会话

在锁定调查器对话框中，可以执行以下操作：

- 单击 " 解锁账户 " 图标解锁账户 
- 单击 " 重置密码 " 图标重置密码 
- 单击 " 保存报告 " 图标保存报告 
  选择该选项后，将显示一个对话框。您可以选择报告的保存位置和文件格式，可以是 .pdf、.csv 和 .mht 。

7.在账户锁定报告中创建警报

如果想在账户被锁定后立即收到通知，可以在账户锁定报告中设置自动警报。

设置警报：

- 单击用户实体和分析图标 
  显示状态和行为窗口 屏幕左侧以树形结构显示报告列表
- 展开活动目录节点
- 右键单击账户锁定报告，显示上下文菜单 显示上下文菜单：

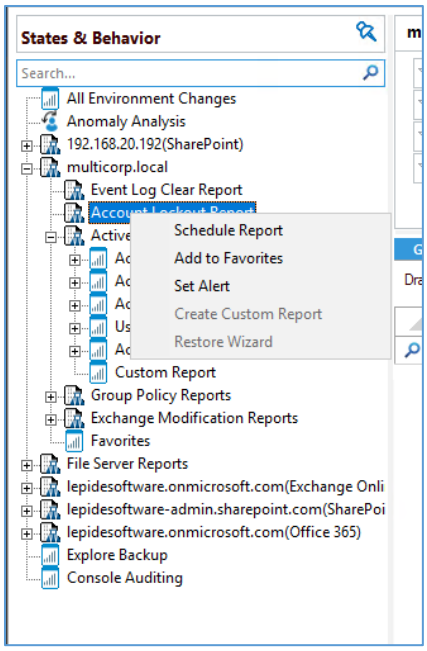

图 8:上下文菜单

- **选择设置警报**

向导将启动，并显示＂选择报告＂对话框：

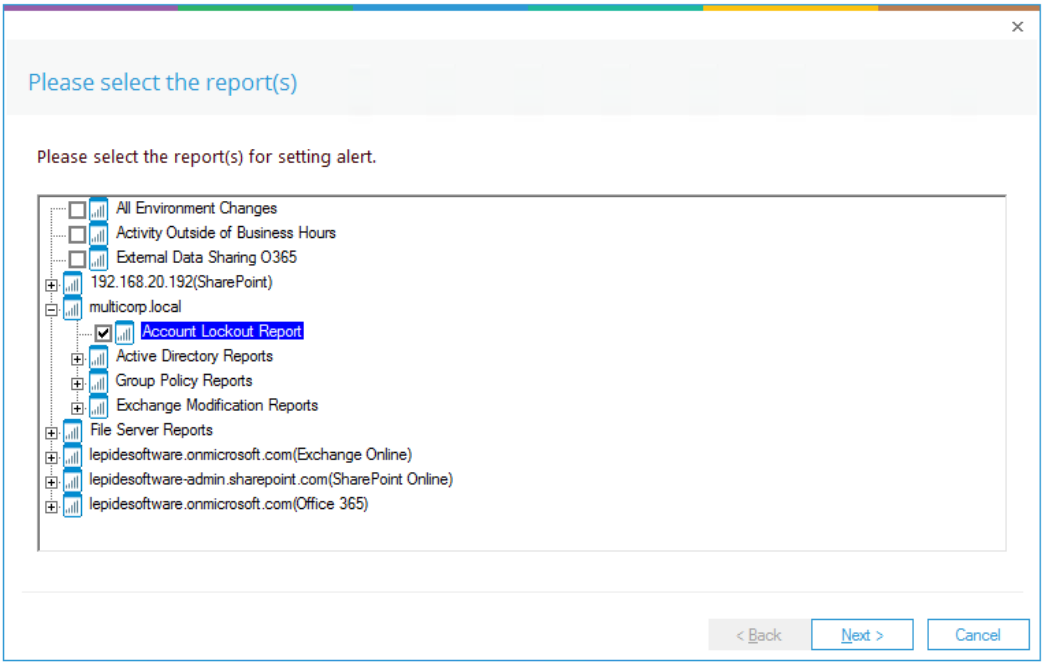

图 9:选择报告

确保要设置警报的报告已被选中。在本例中，就是账户锁定报告。

- **点击下一步**

将显示＂设置筛选器＂对话框：

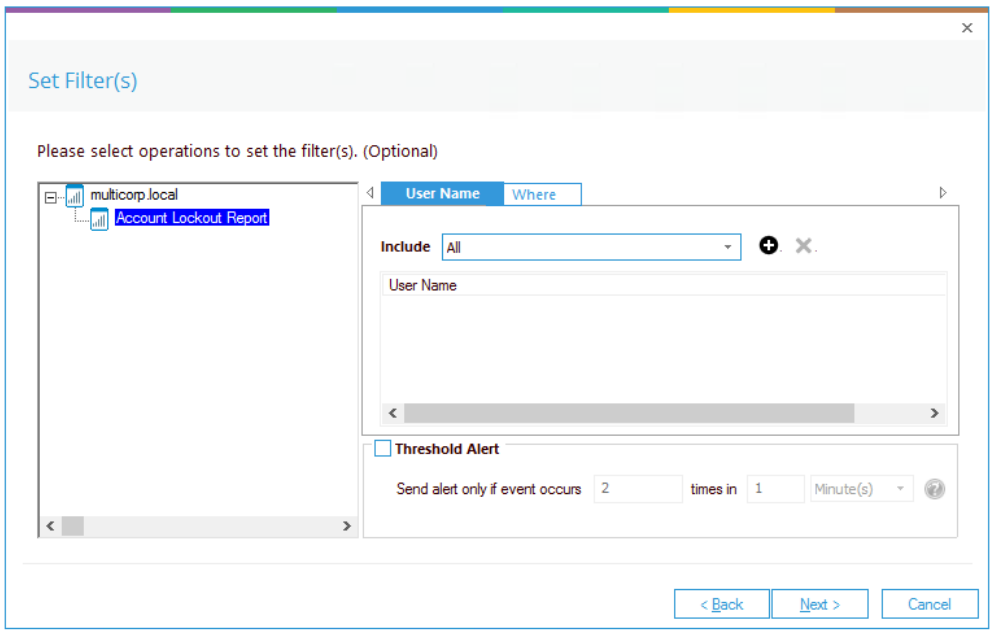

图 10: 设置过滤器

在对话框左侧，你可以看到正在处理的报告，在本例中就是账户锁定。

使用对话框顶部的选项卡可以更改用户名和用户所在位置的设置。这两个选项的默认设置都是全部。

阈值警报选项可自定义如下：

阈值警报： 选中该复选框可打开阈值警报

仅在事件发生时发送警报： 在此输入事件发生的次数、时间值和时间段

- **点击下一步**

警报设置对话框将显示：

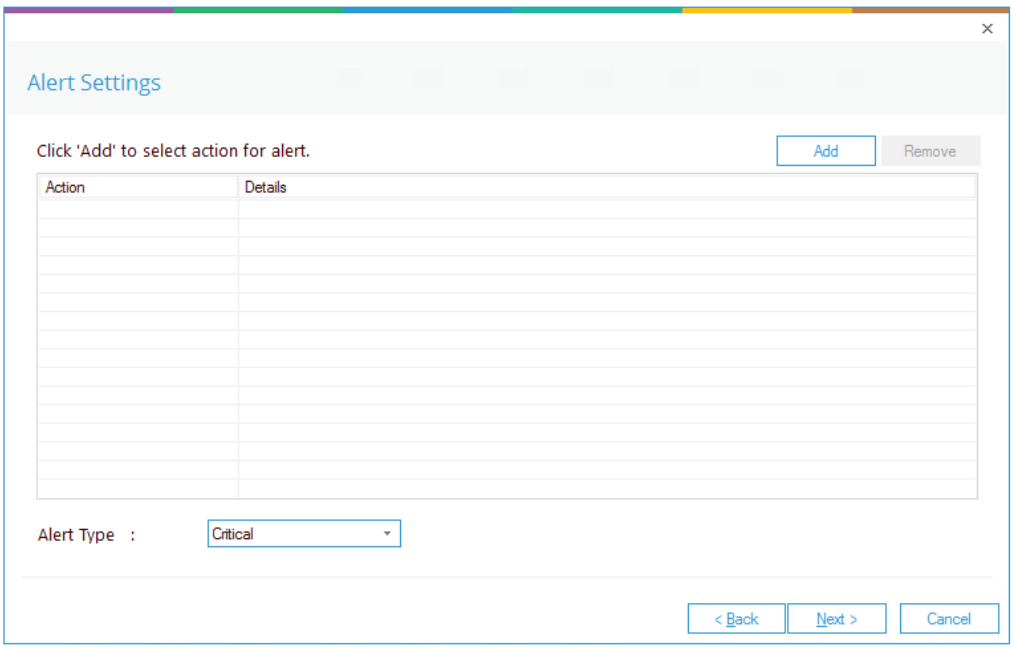

图 11: 警报设置

通过此对话框，您可以设置警报触发后的响应，并显示已设置的任何现有响应。您还可以更改警报类型。

- 要创建新的警报响应，请单击添加按钮。

添加警报操作对话框将显示：

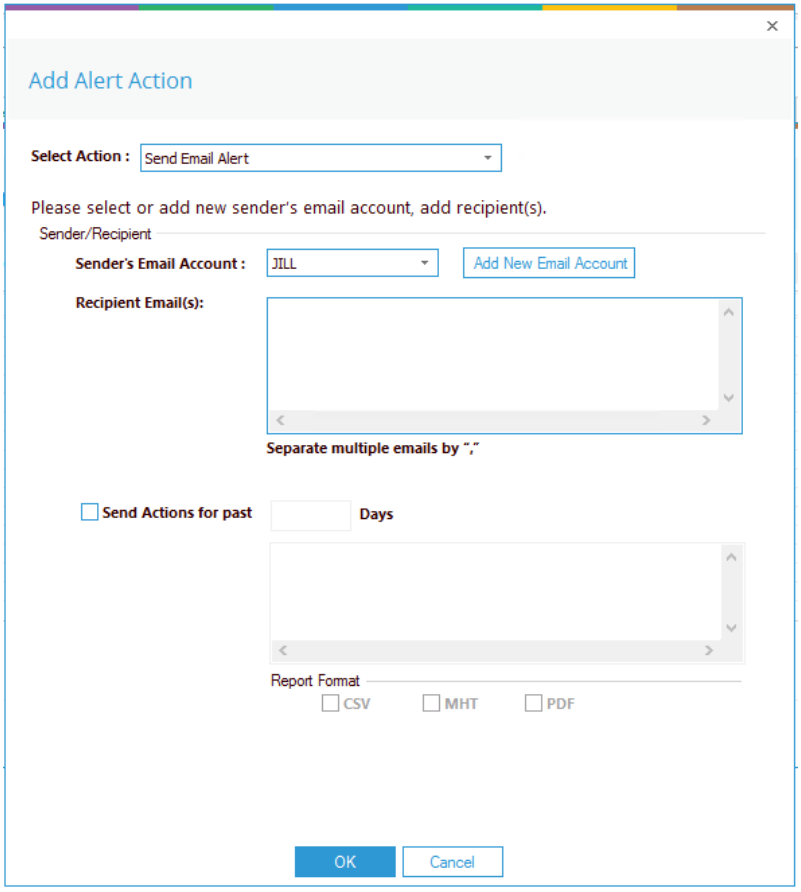

图 12: 添加警报操作

- 单击＂选择操作＂下拉箭头，查看可用操作列表：

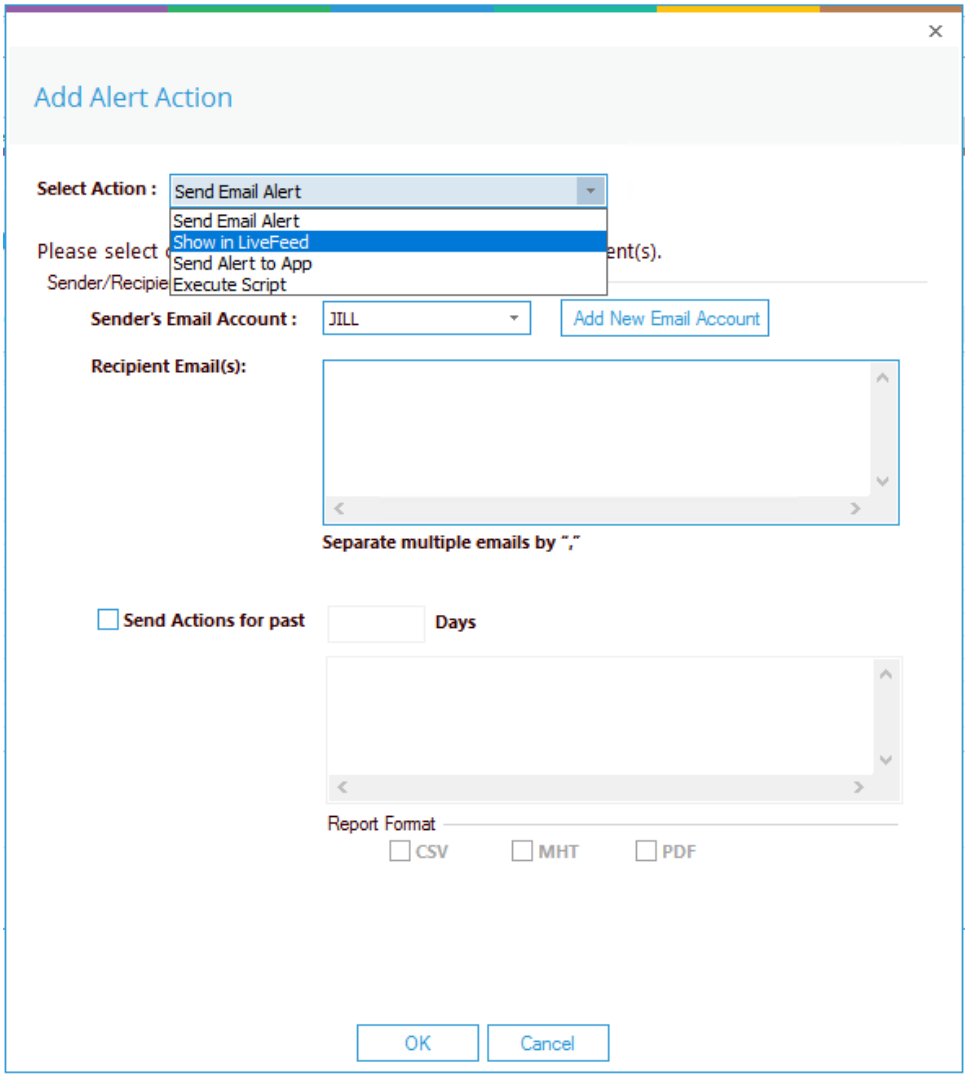

图 13: 添加警报操作选项

警报操作如下：

- 发送电子邮件提醒
- 在 LiveFeed 中显示
- 向应用程序发送警报
- 执行脚本

下文将对每种操作的配置进行说明：

1. 发送电子邮件提醒

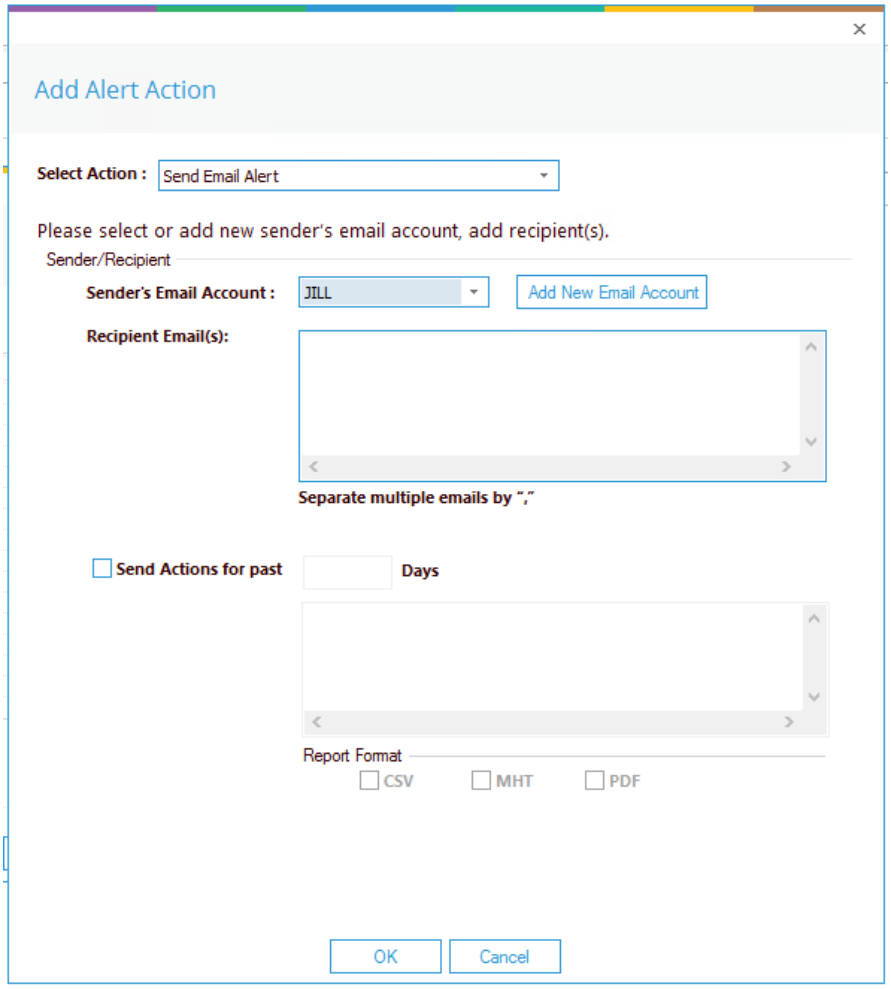

图 14: 添加警报操作 - 发送电子邮件警报

该选项允许您在警报触发后发送电子邮件。对话框的元素如下：

发件人电邮帐户：	发件人的电子邮件帐户将显示在这里，如果它已被选中。单击"添加新电子邮件帐户"以输入新的发件人电子邮件帐户。
收件人电子邮件(s)：	通过在框中键入电子邮件地址来添加收件人电子邮件。如果有多个邮箱地址。用"，"把它们分开
发送过去xx天的操作：	此选项允许您查看该用户在最近指定的天数内所做的所有事情。例如，如果由于帐户被锁定而触发警报，那么您可能希望查看该帐户还发生了什么。选中此框并指定天数，然后将发送一封电子邮件，其中包含一个附件，其中列出了用户所需要的所有内容已在规定的天数内完成。

附件将包含一份报告，可以通过选中相关框来指定格式。格式为CSV、MHT和PDF。

- 单击＂确定＂保存警报操作。

2. 在 LiveFeed 中显示

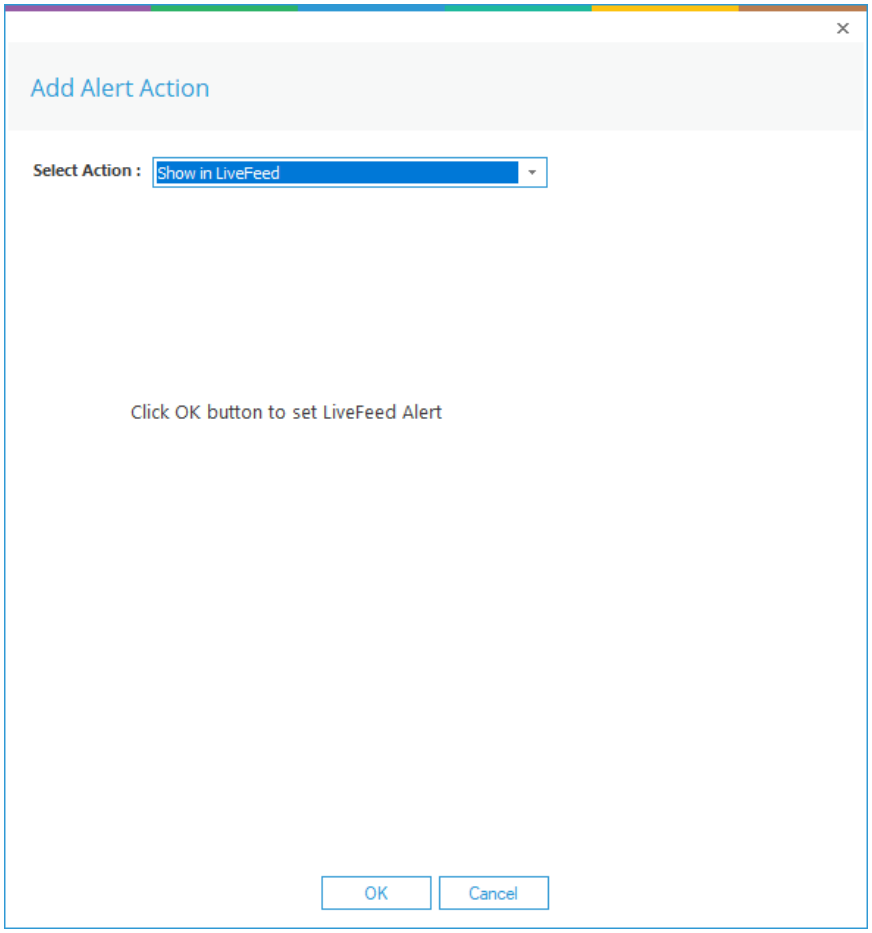

图 15: 添加警报操作 - 在 LiveFeed 中显示

显示在 LiveFeed 中表示警报将发送到 Lepide 面板。

- 单击＂确定＂打开 LiveFeed 提示。

3. 向应用程序发送警报

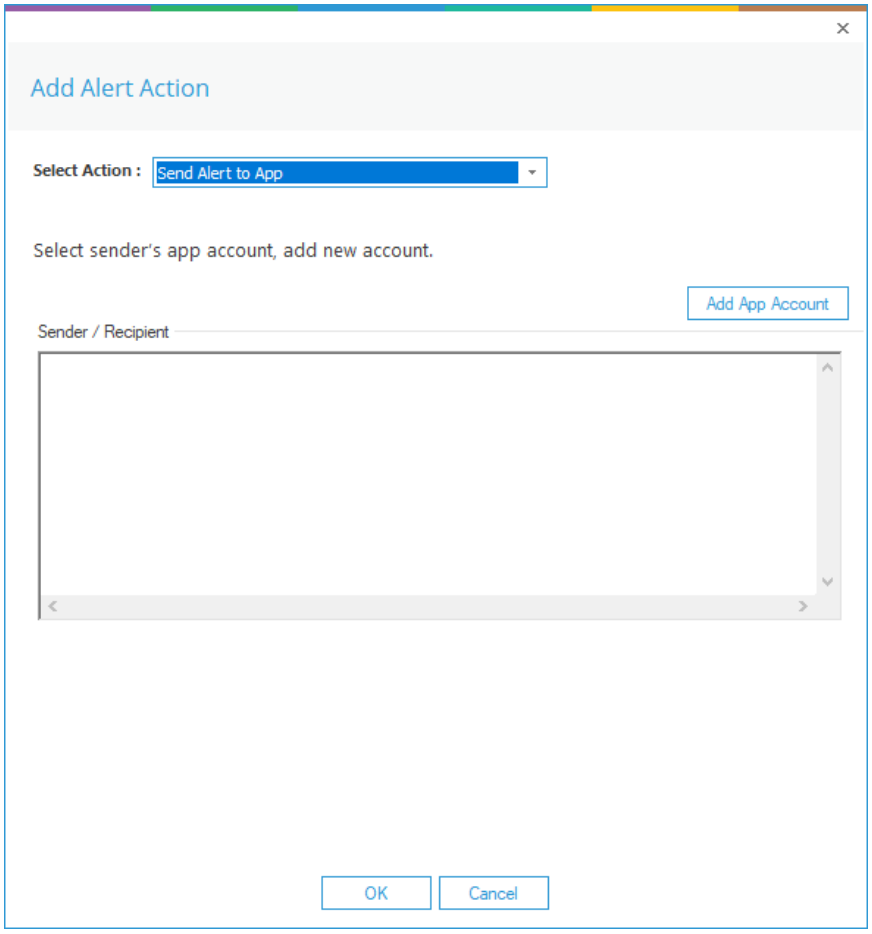

图 16: 添加警报操作 - 向应用程序发送警报

发送警报到应用程序选项可将警报发送到移动设备。

- 单击添加应用程序帐户以添加新的手机帐户。将显示以下对话框：

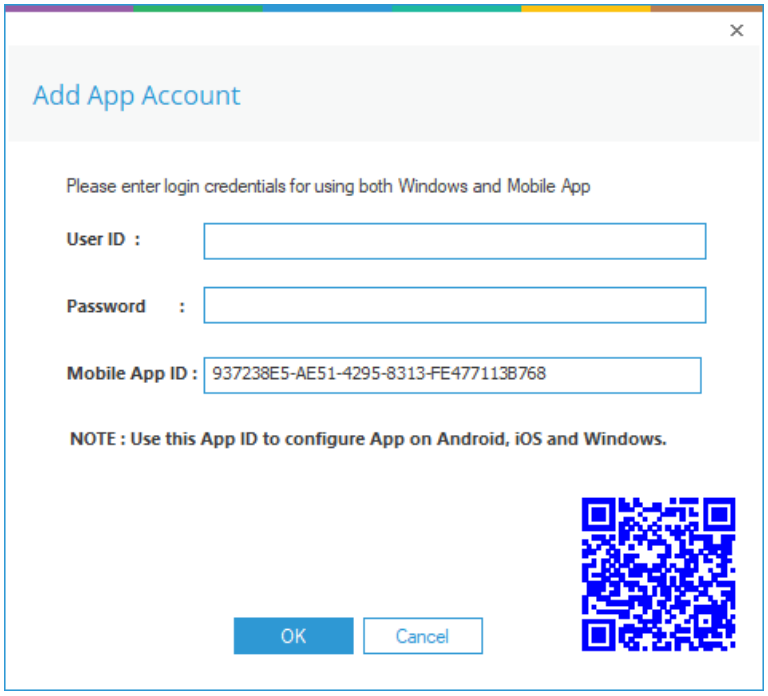

图 17: 添加应用程序帐户

- 输入用户 ID 和密码
- 输入移动应用程序 ID，该 ID 是使用移动设备扫描对话框底部显示的二维码生成的。
- 点击确定

4. 执行脚本

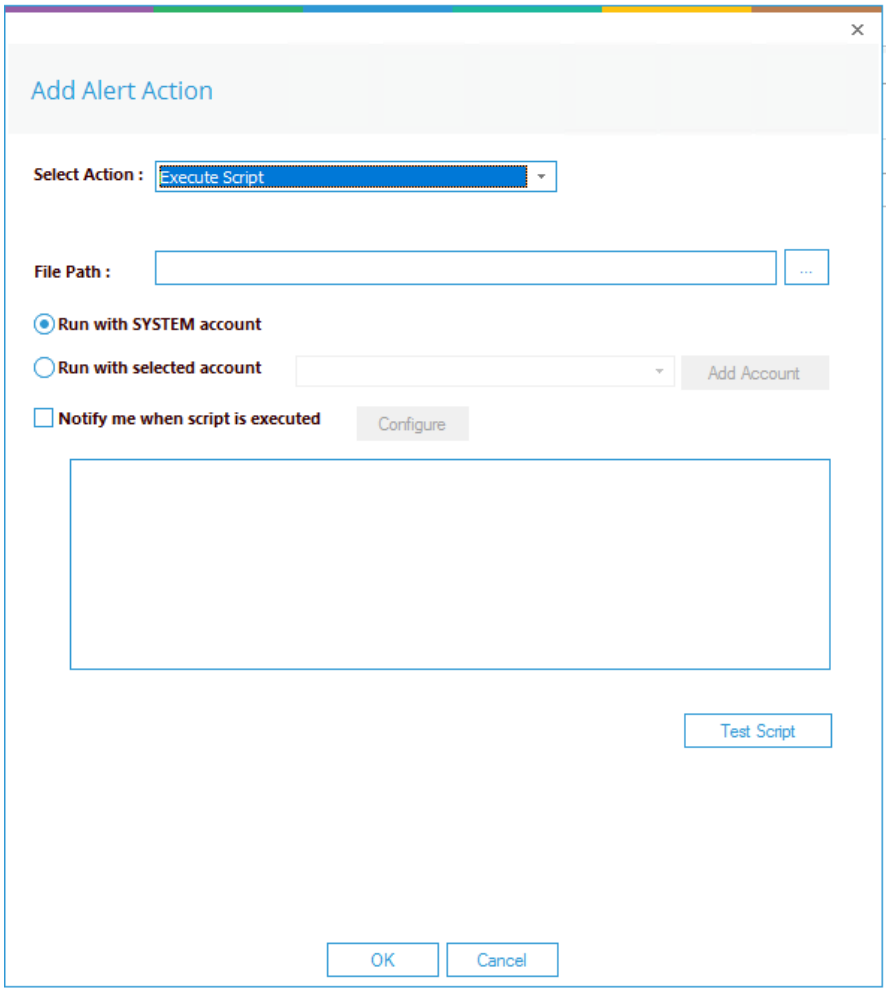

图 18: 添加警报操作 - 执行脚本

下拉菜单中的最后一个操作是执行脚本

这将设置在触发警报时执行一个预定义 PowerShell 脚本的选项。对话框的元素如下：

文件路径： 点击 "浏览"，选择 PowerShell 脚本的文件路径。 使用系统帐户运行或使用选定账户运行。

如果选择＂使用选定账户运行＂，则可使用下拉菜单选择账户，或单击＂添加账户＂指定要使用的账户。

选择脚本执行时通知我，以在脚本执行时发送电子邮件。

选中该选项后，"配置"按钮就可用了。选择"配置"可设置发件人账户和收件人电子邮件地址。

- 单击"测试脚本"测试指定脚本是否运行无误。
- 单击"确定"返回"警报设置"对话框。

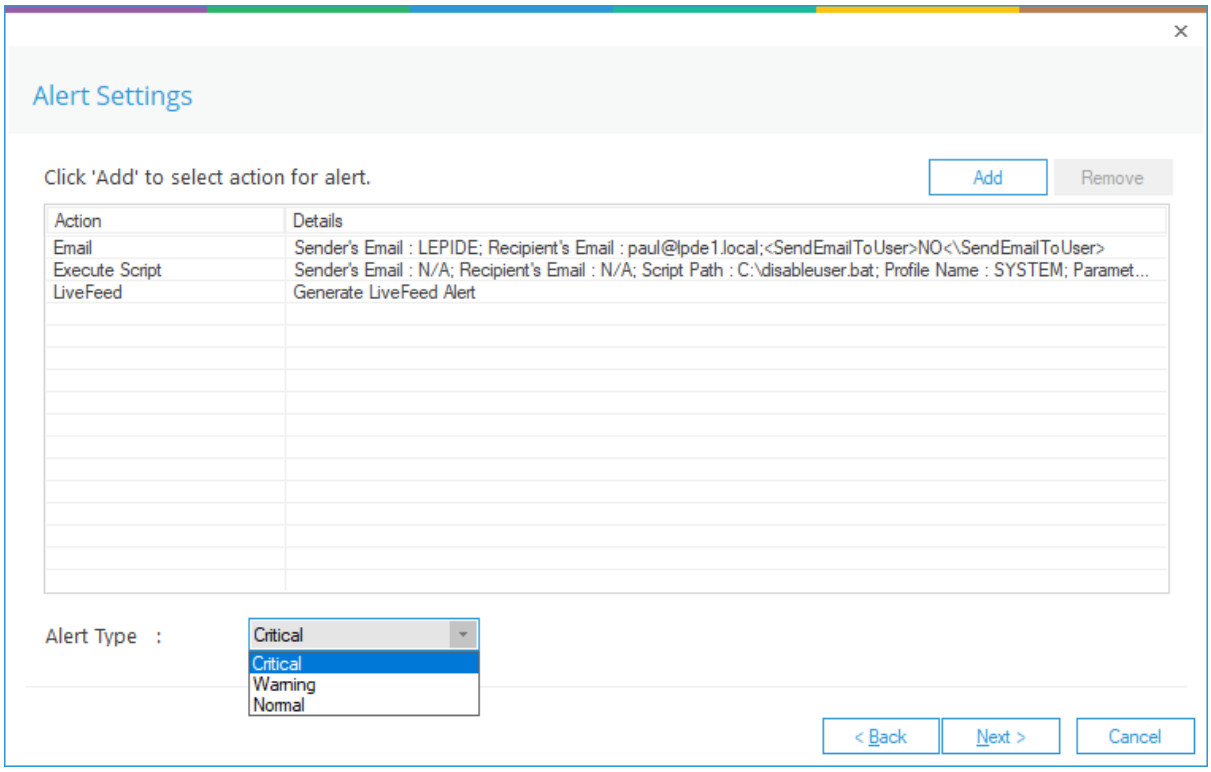

图 19: 警报设置 - 警报类型选项

- 现在选择警报类型，可以是"危急"、"警告"或"正常"。
- 点击下一步继续
- 确认对话框将显示警报详情。
- 单击"完成"返回"状态和行为"页面。

HongKe 虹科

虹科电子科技有限公司

www.haocst.com
network@hkaco.com

广州市黄埔区开泰大道30号佳都PCI科技园6号楼1-7层

T (+86) 400 - 999 - 3848
M (+86) 135 3349 1614

各分部：广州 | 成都 | 上海 | 苏州 | 西安 | 北京 |
台湾 | 香港 | 日本 | 韩国 | 美国硅谷

版本：V1.0 - 23/09/11

联系我们

获取更多资料

haocst.com