Lepide Web控制台

Lepide Web控制台
- 概述
- 要求和前提条件
- 系统需求
- 如何安装LDSP Web控制台
- 应用程序文件位置
- 从Lepide应用服务器外部访问Web控制台创建Web管理控制台用户
- 主界面
- 添加新用户或组
- 添加组
- 添加用户仪表板和报告
- 仪表板选项
- 显示数据后面的报表运行报告
- 指定日期范围
- 排序报表
- 对报表应用筛选器
- 使用过滤器图标应用过滤器导出报表
- 向我的Lepide添加报告
- 创建自定义报表
- 编辑自定义报表
- 创建自定义文件夹
- 删除、移动或共享报表
- 删除自定义报表移动自定义报表共享报表
- 警报
- 警报状态
- 威胁模型
- 如何启用和配置威胁模型电子邮件设置选项卡
- 如何查看日志
- 如何更改日期和时间格式
- 备份与恢复
- 想要备份和恢复

概述

Lepide Web控制台为Lepide数据安全平台提供了一个可访问和用户友好的界面，提供了一个现代的，逻辑和直观的布局，使其更容易使用自定义过滤器和列查询数据。

要求和前提条件

要使用Lepide Web控制台，您需要安装和配置Lepide数据安全平台，并具有访问Active Directory的适当权限。

系统需求

• 处理器要求

最低双核处理器要求

推荐四核处理器要求

• RAM要求

最低8gb RAM要求

推荐16gb RAM要求

• 磁盘剩余空间要求

最低1gb

推荐2gb

• 以下任意32位或64位Windows操作系统：

Windows Server操作系统:任何2008 R2以上的服务器

• 用于存储审计日志的SQL Server(本地或网络托管)：SQL Server 2005及以上(标准或企业)

• .NET Framework 4.0及以上版本

支持的浏览器：

LDSP Web控制台支持在以下浏览器中运行：— Google Chrome（最新公开发布版本）— Microsoft Edge（最新公开发布版本）— Mozilla Firefox（最新公开发布版本）— Safari（最新公开发布版本）

注意：Internet Explorer不再受支持。

如何安装LDSP Web控制台

• 双击"LDSP Web Console"安装文件"LDSP Web Console.exe"

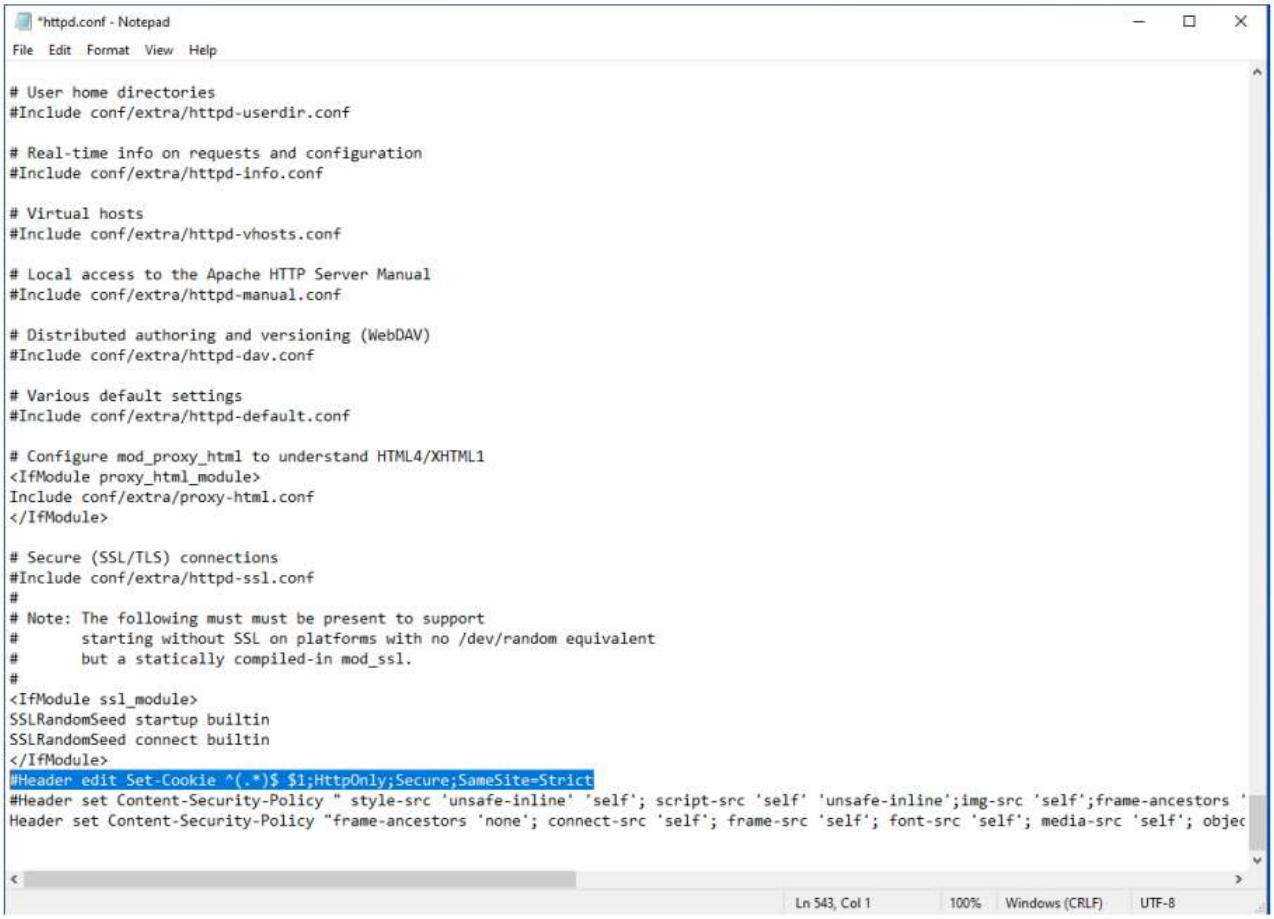
应用程序文件位置

• 如果您通过LepideDSP zip文件夹中的链接下载了解决方案，则.exe文件将位于Web控制台文件夹中。

从Lepide应用服务器外部访问Web控制台

下面的步骤解释了如何配置web控制台，以便您可以从Lepide Application Server外部访问它。

1. 在"Lepide安装目录文件夹/LDSP Web Console/apache/conf"路径下打开"httpd.conf"文件。
2. 转到文件底部，找到以下行，并在开头添加"#":#Header edit Set-Cookie ^(.*)$ $1;HttpOnly;Secure;SameSite=Strict



3. 将更改后的文件保存在同一位置。

4. 重新启动LDSPapache服务。

创建Web管理控制台用户

要使用Web控制台，您需要做的第一件事是指定Web控制台管理用户。一旦设置了这个用户，他们就可以从Web控制台界面中创建所有其他Web控制台用户。

从Lepide数据安全平台：点击设置图标

选择"LDSP Web Console"（树形结构中的最后一个选项）进入"LDSP Web Console"界面。

在对话框中输入用户登录的详细信息，具体操作如下：

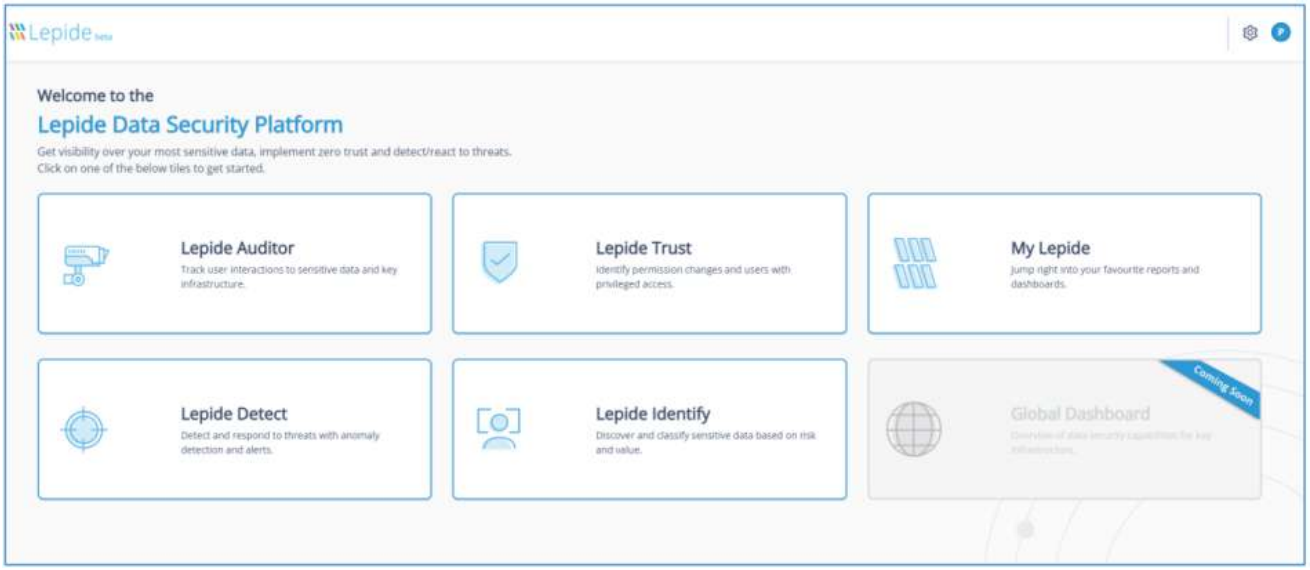
• 输入用户名或单击图标选择用户名。格式应为username@domain.com

• 输入密码（这是Active Directory登录密码）

• 输入域控制器IP地址此用户将负责为其他用户分配web接口访问权限。使用这些凭据登录以管理其他用户的角色。

• 单击应用

使用此用户登录Web控制台。请对用户名(Username@domain.com)使用相同的格式。进入Web控制台主界面：



主界面

Lepide Web控制台的主屏幕将显示四种不同的Lepide类别和My Lepide。单击这些按钮中的任何一个都将进入相关选项。

主屏幕选项有：

Lepide Auditor：跟踪敏感数据和关键基础设施的用户交互

Lepide Trust：识别权限更改和具有特权访问权限的用户

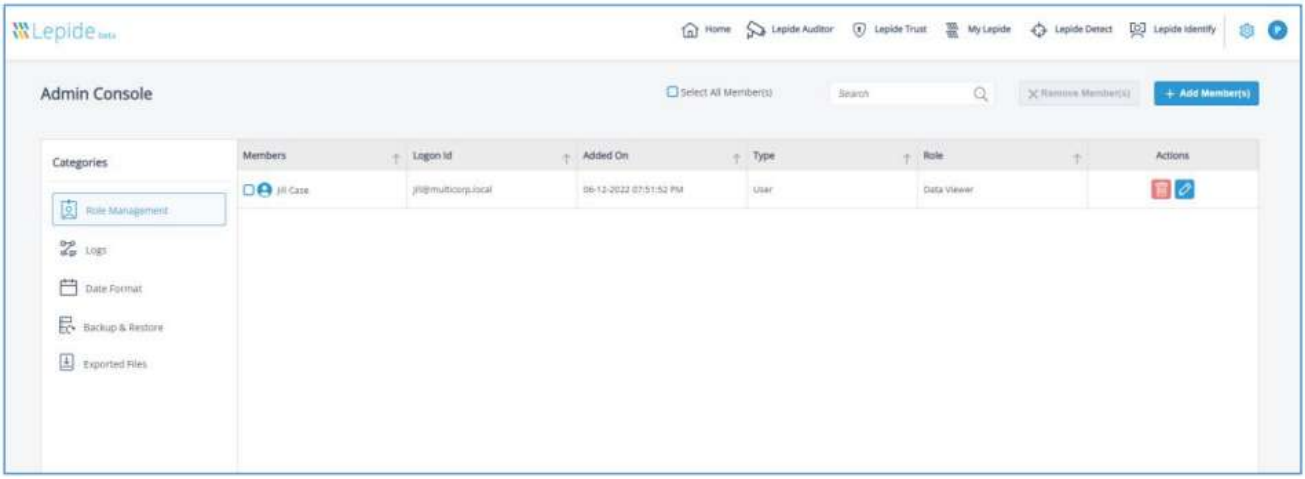
Lepide Detect：通过异常检测和警报检测和响应威胁

Lepide Identify：根据风险和价值发现和分类敏感数据

My Lepide：直接跳转到您最喜欢的报告和仪表板

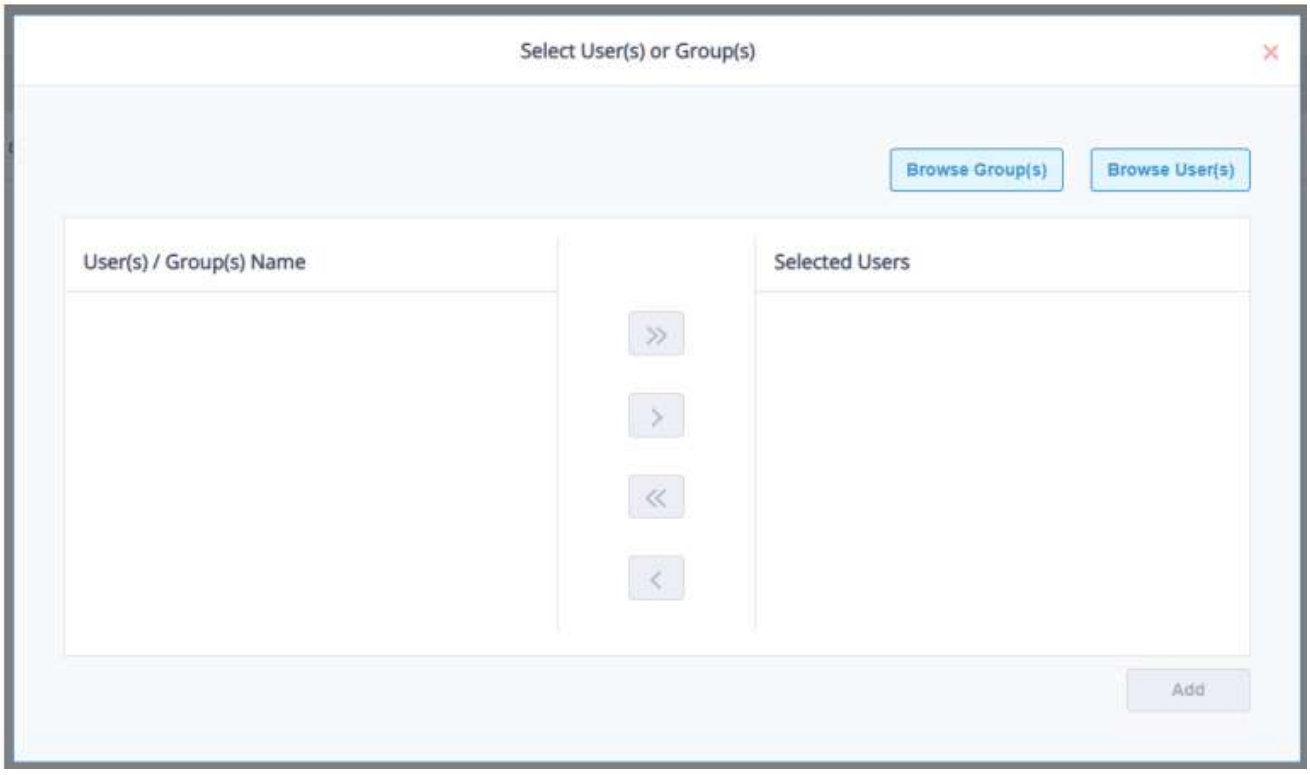
添加新用户或组

在主屏幕上，单击屏幕右上方的设置图标。系统显示"管理控制台"：



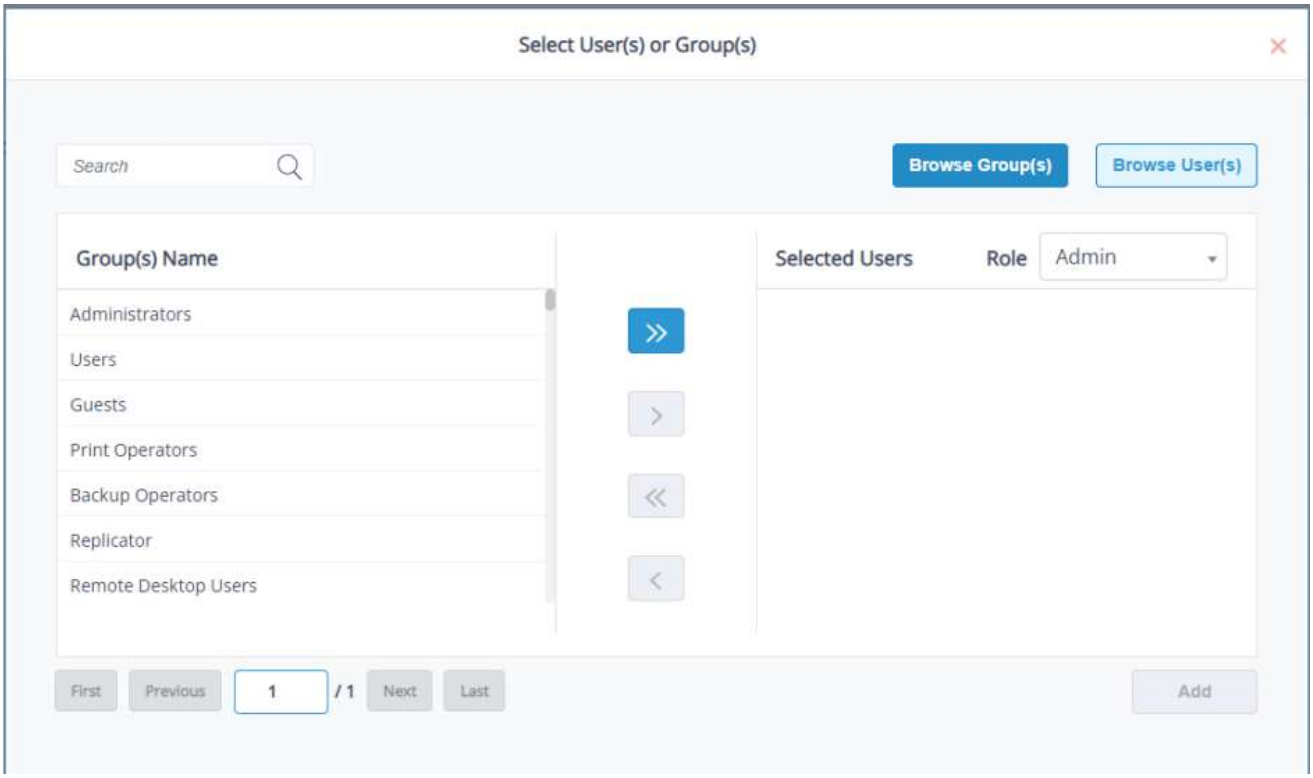
•单击"添加成员"按钮

弹出如下对话框：



添加组

• 点击浏览组按钮



• 组/名区域将填充所有可用的组

• 如果有多个页的组名，使用姓/前面/下/导航按钮进入页面搜索一个特定的组

• 点击对话框的顶部的搜索栏中，输入搜索文本添加所有上市公司。

• 单击按钮添加一个特定群体

• 单击以选中该集团并单击选择按钮将其添加到用户列表中。

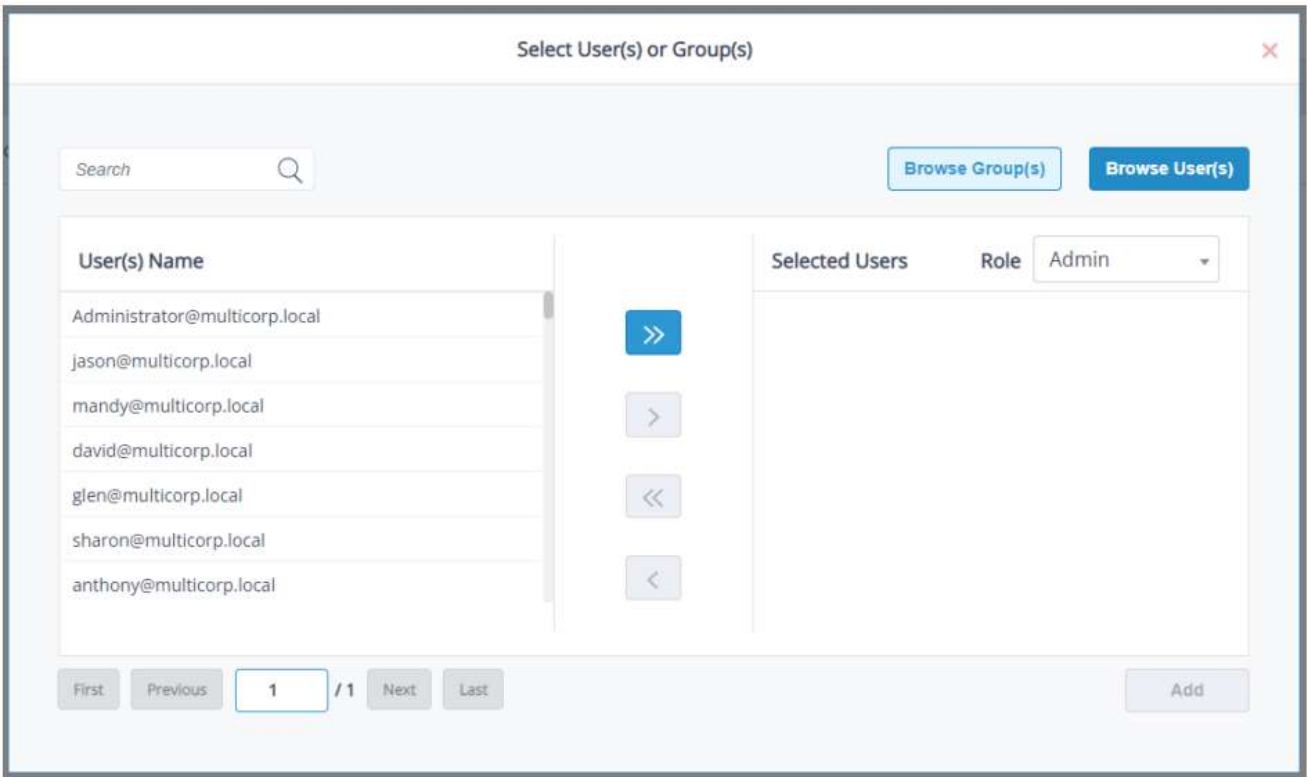
• 选择所需的Admin或Data Viewer角色：

• 单击add按钮添加组

添加用户

• 点击浏览用户按钮

• 用户名称区域将填充所有可用的用户名



• 如果有多个页面的用户名，可以通过"第一页/上一页/下一步/最后一页"导航按钮进行移动。

• 如果要添加所有用户，请单击按钮。

• 如果要添加特定用户，请单击选中用户名，单击按钮将其添加到已选用户列表中。

• 对您想要添加的任何其他用户重复最后一步。

• 选择所需的角色Admin或Data Viewer。

• 单击添加按钮。

仪表板和报告

从主屏幕上，选择一个Lepide类别 - 这可以是Lepide审计，Lepide信任，Lepide检测或Lepide识别。对于本例，我们将查看Lepide Auditor。

仪表板选项

进入"Lepide Auditor Dashboard"界面。这包含基于所选类别（在本例中为Lepide Auditor）的报告的预定义仪表板。有以下选项可用于更改时间段和刷新数据：

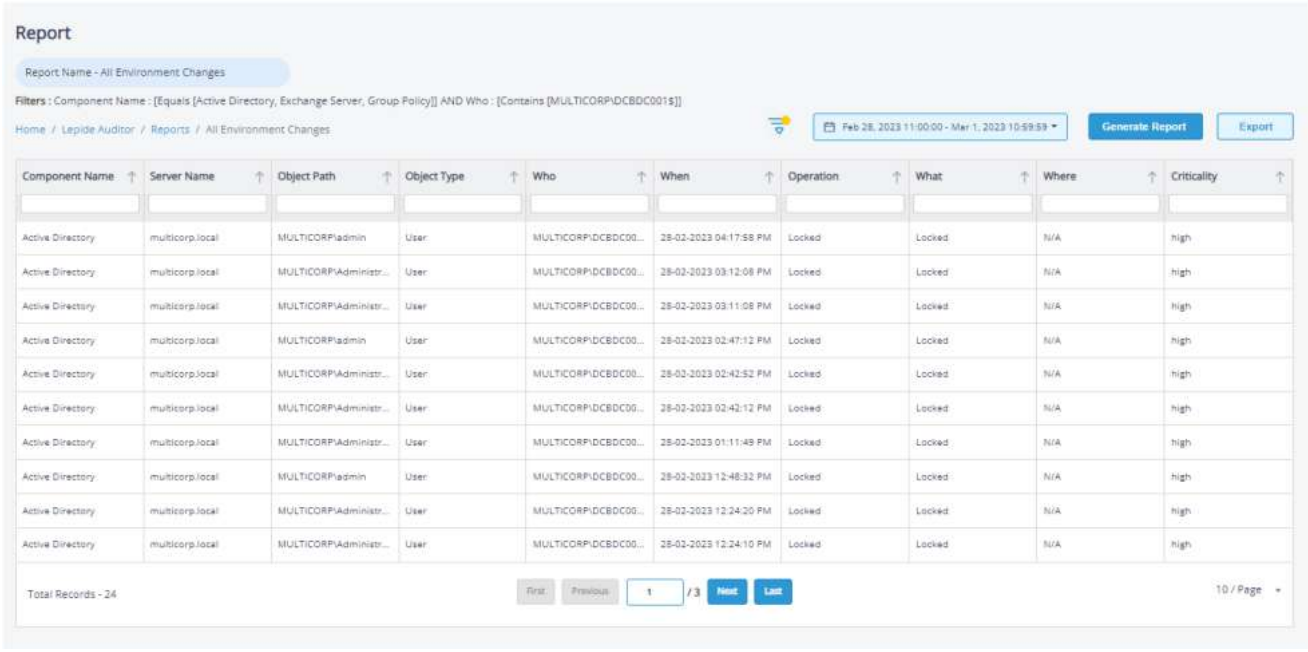
•这些选项是1天前，7天前，31天前和刷新

显示数据后面的报表

• 单击仪表板中的数据区域将显示该数据所基于的报告。

• 在下面的示例中，单击图表中的第一列将显示“所有环境变化报告”，这是该仪表板图表所基于的报告。

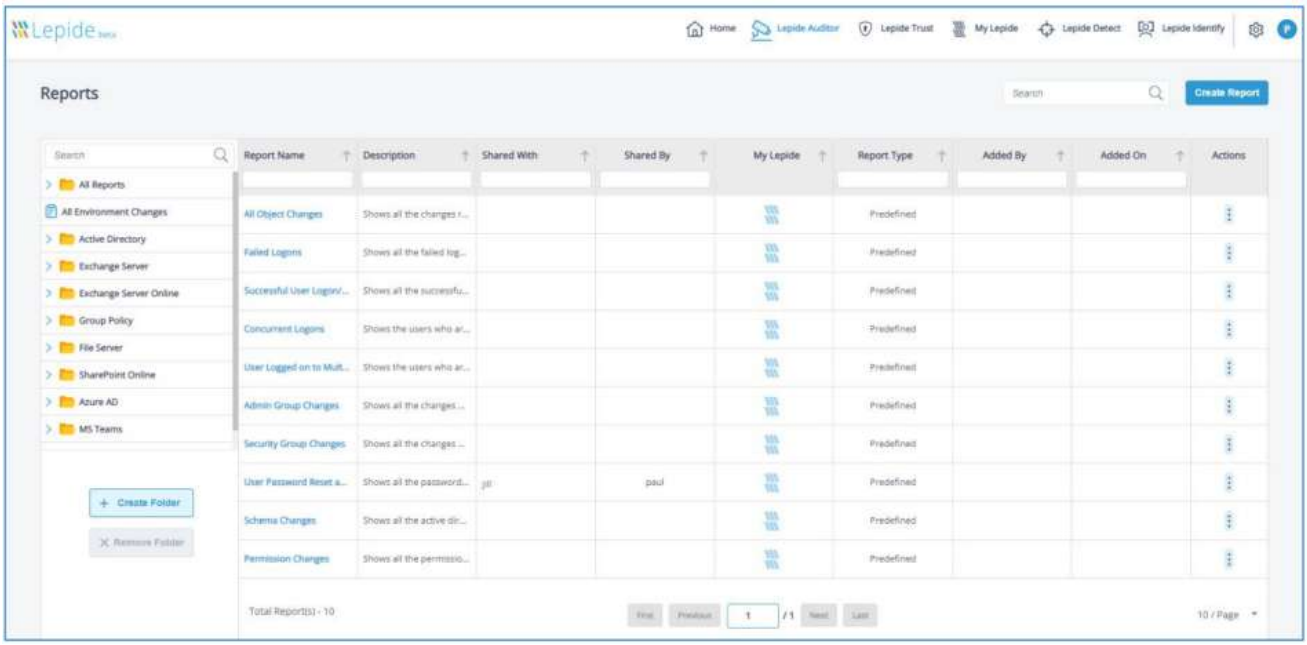
• 单击Generate生成报告：



运行报告

• 从Dashboard屏幕的顶部，单击Lepide Auditor并选择Reports

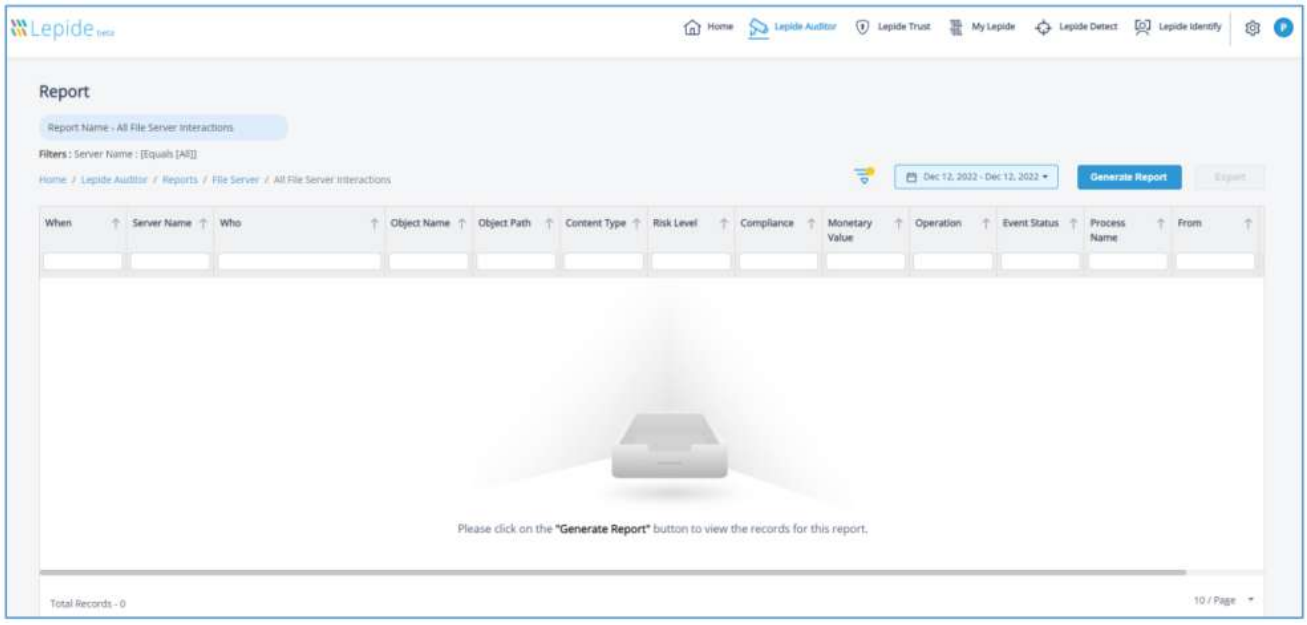
显示报告窗口：



这里显示了Lepide Auditor中可用的所有报告。

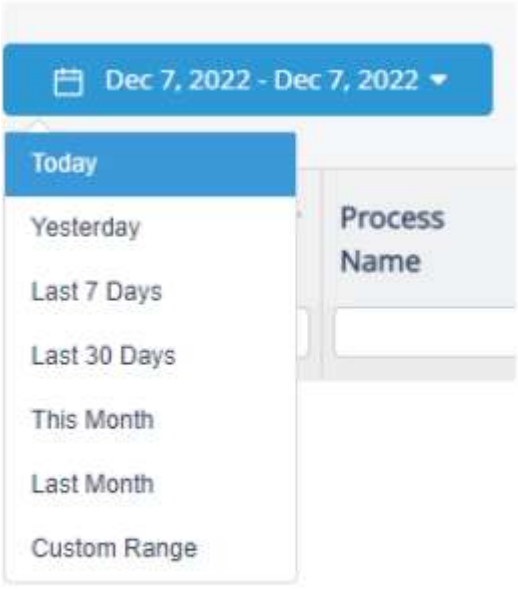
• 若要查看文件夹内的报表，请单击文件夹名称，例如文件服务器

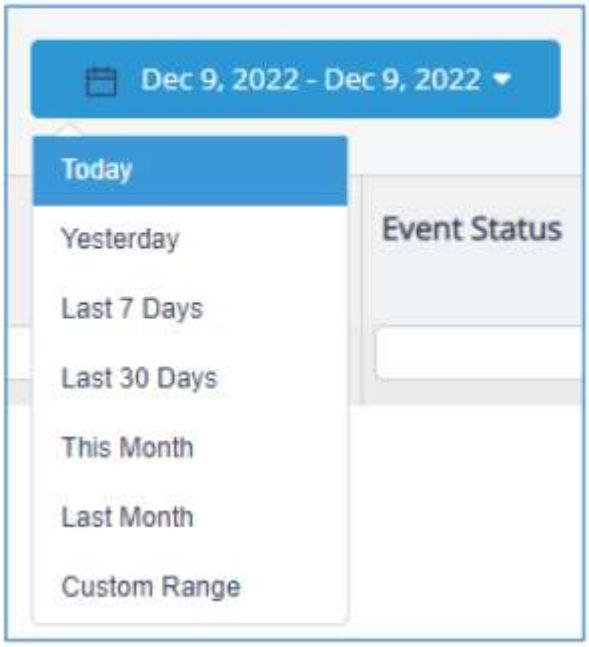
• 若要查看特定报表，请单击报表名称。在这个例子中，所有文件服务器交互报告已经被选中：



指定日期范围

• 在屏幕顶部，单击日期，从列表中选择日期范围

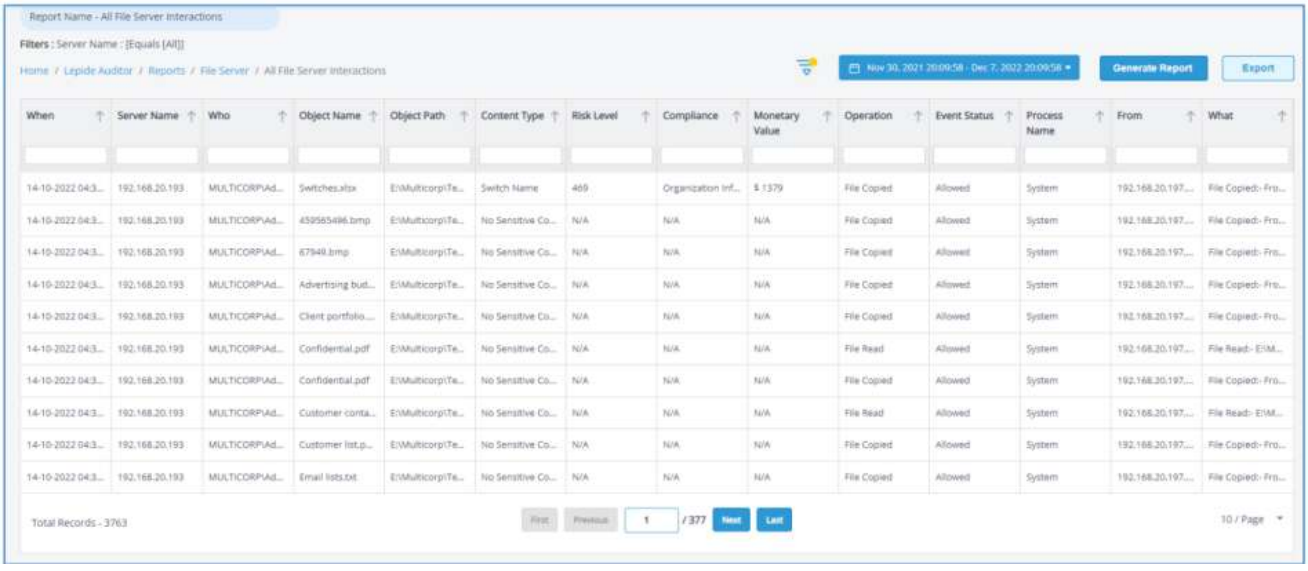




系统弹出如下对话框：

• 从列表中选择日期范围

• 单击"生成报表"按钮，运行指定时间段的报表



排序报表

可以通过单击列标题旁边的箭头对报表进行排序。单击后，箭头变为蓝色并显示排序方向。

这里的Operation已经按Operation升序排序(a-z)：

• 再次点击箭头以降序排序(z-a)

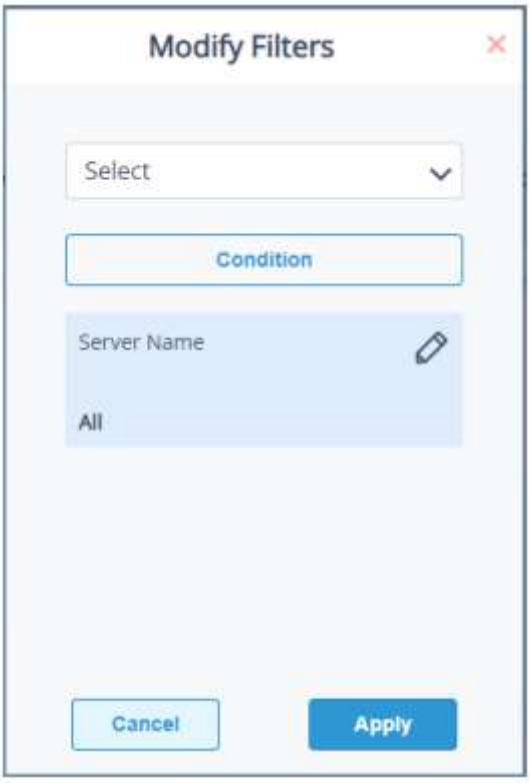
对报表应用筛选器

有两种方法可以使用Lepide Web控制台应用过滤器，下面解释一下：

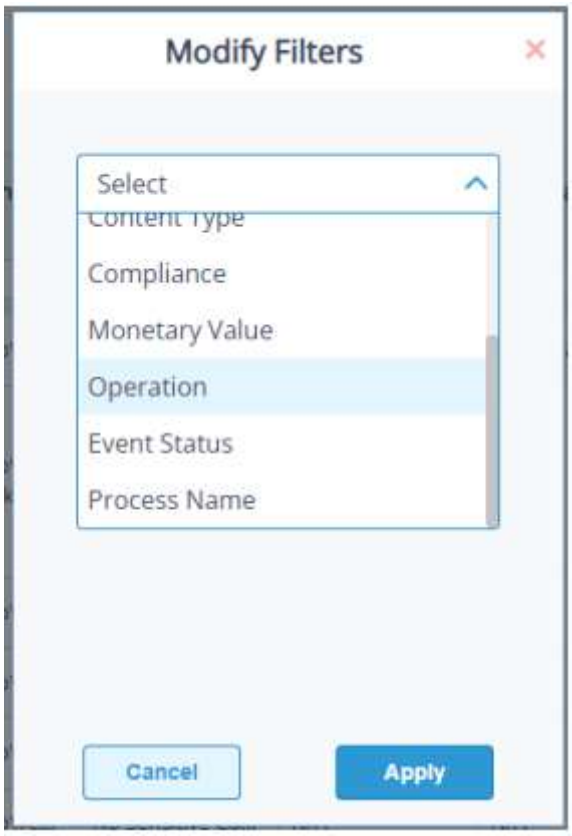
使用过滤器图标应用过滤器

• 要对报表应用过滤器，请单击filter图标。

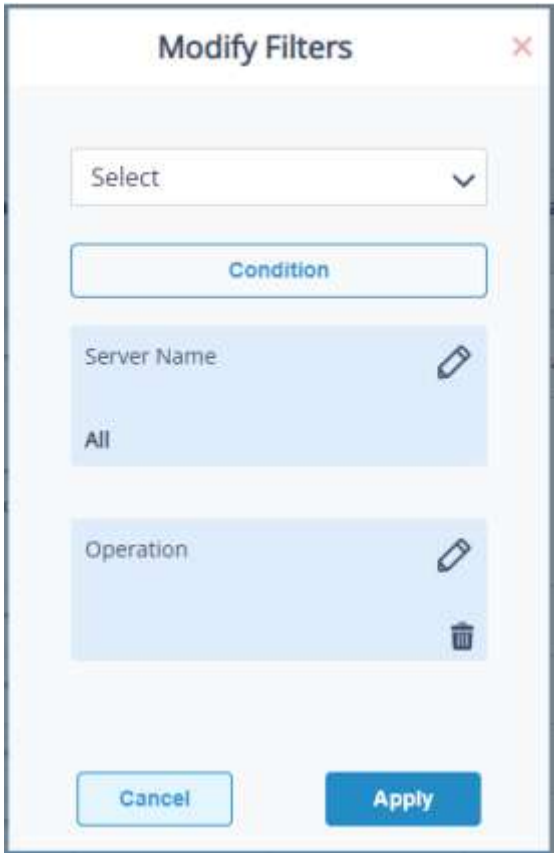
系统弹出"修改过滤器"对话框。



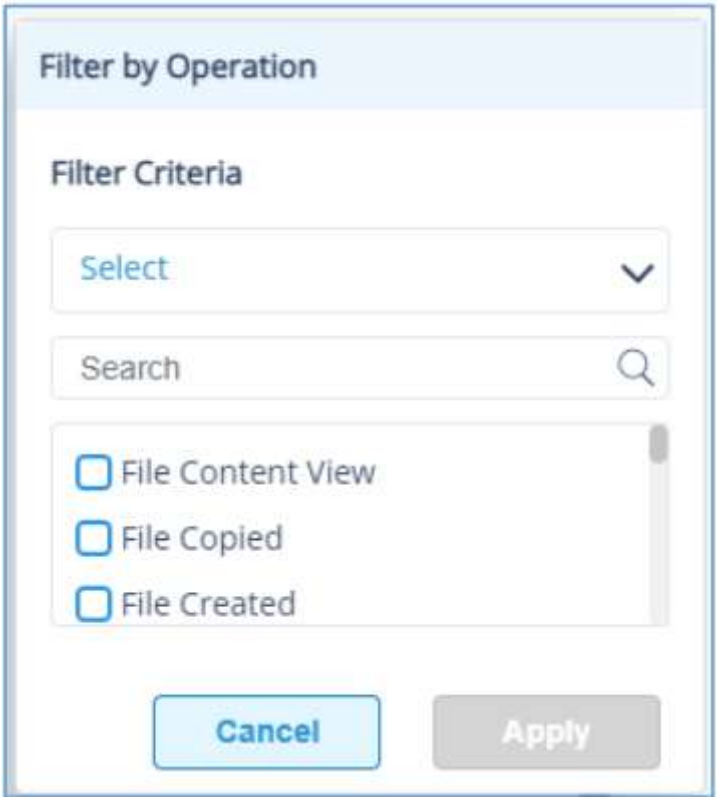
• 单击"选择"下拉列表选择要过滤的列。在本例中，我们将选择



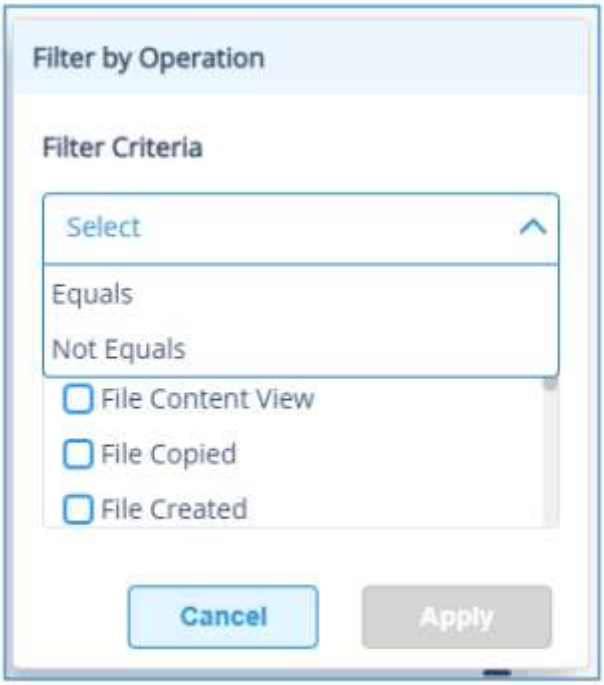
操作现在出现在蓝色高亮的对话框中:

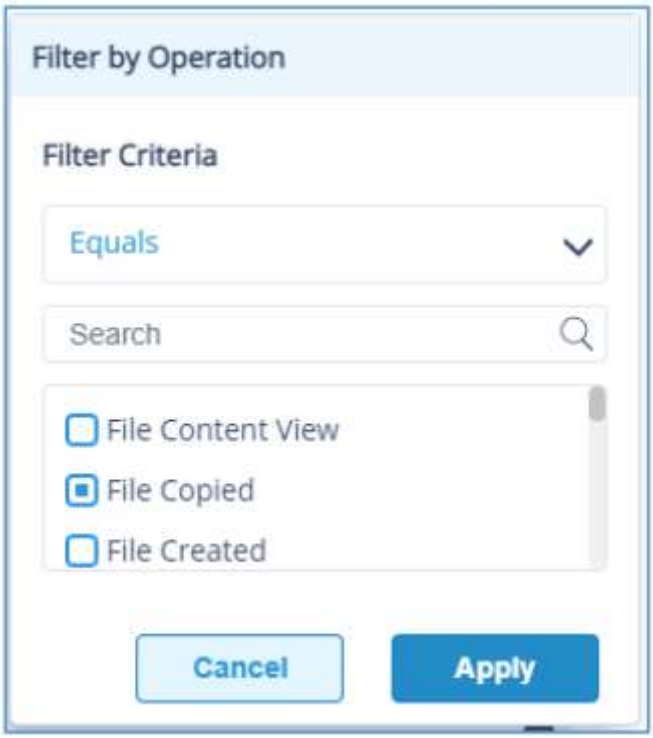


•点击相关列名旁边的编辑过滤器图标（蓝色突出显示）



• 单击Select下拉菜单，从可用的标准选项中进行选择。在本例中，我们通过操作进行过滤，因此可以在Equals或Not Equals之间进行选择：



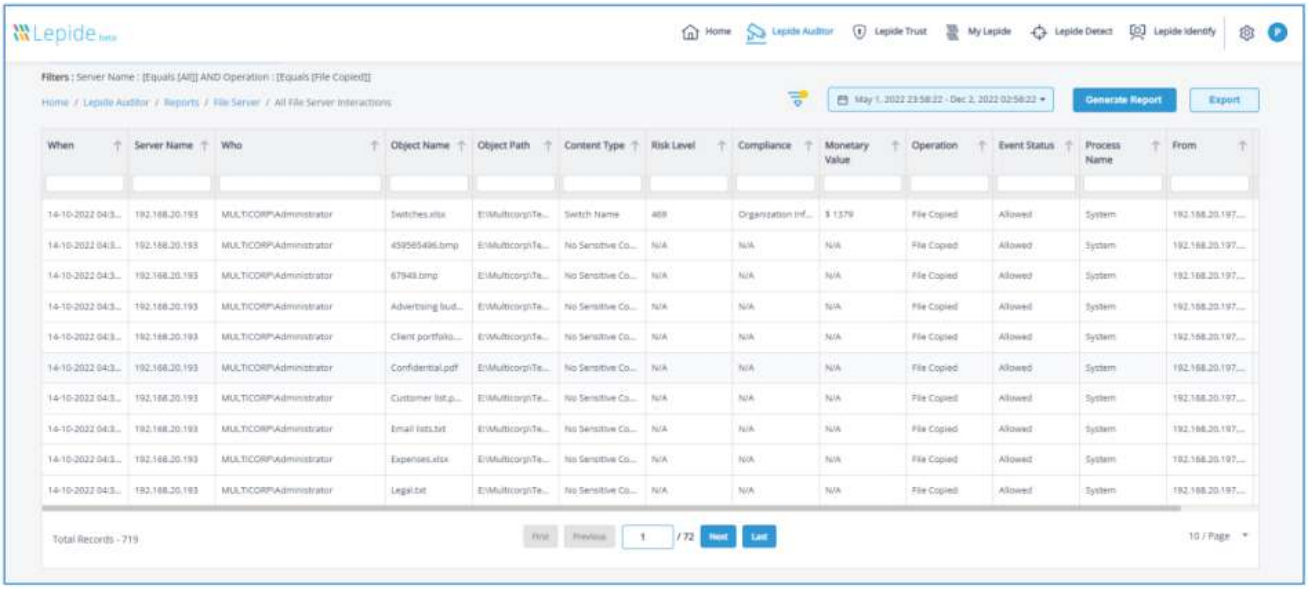


• 选择要过滤的列。在本例中，我们将通过文件复制进行过滤

• 单击应用

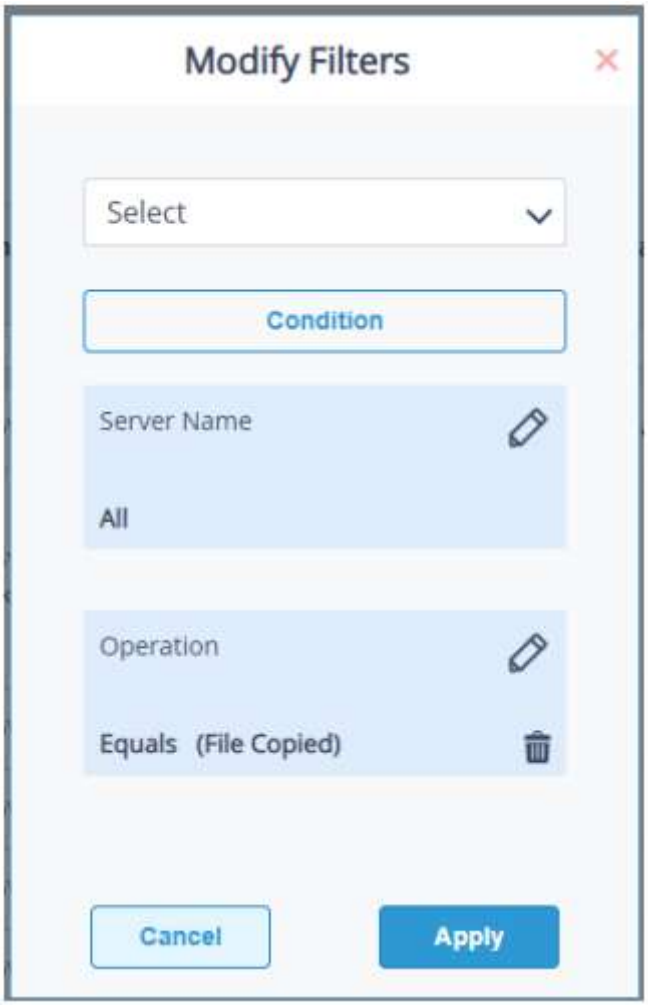
• 单击生成报告

报告将运行并显示过滤后的数据



在上面的例子中，已经应用了File replicated过滤器，并且该过滤器的详细信息显示在屏幕顶部：

• 如果要更改过滤器，请再次单击“过滤器”图标，系统弹出“修改过滤器”对话框。



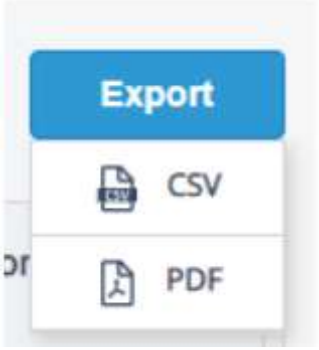
• 根据需要进行更改，然后像以前一样，单击“应用”，然后单击“生成报告”。

• 要删除过滤器，请在“修改过滤器”对话框中单击图标。

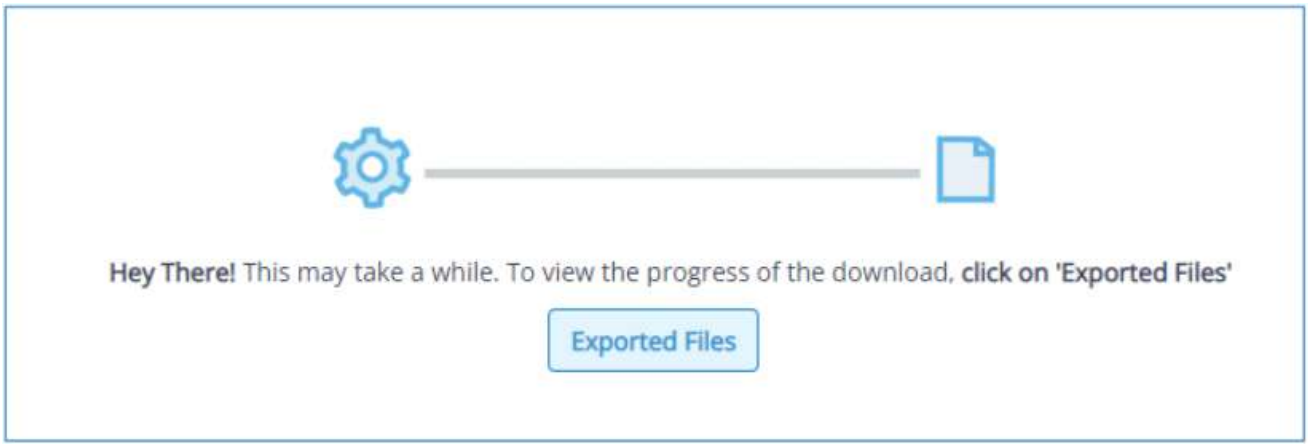
导出报表

报表可以导出为CSV和PDF文件格式。导出到CSV将是即时的，而PDF选项将花费更长的时间，因为它有格式导出。

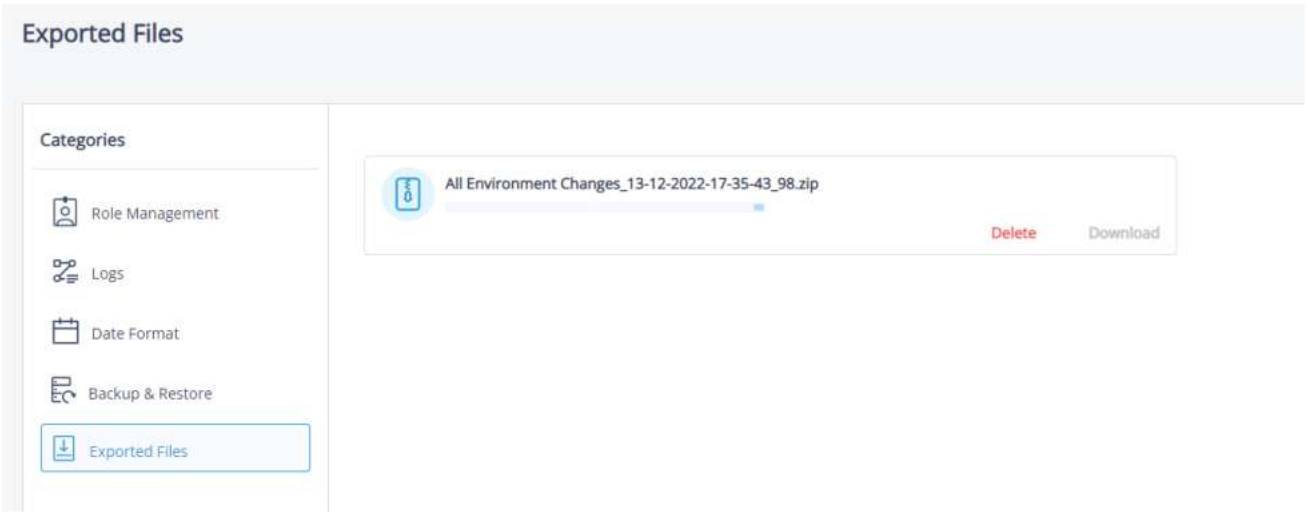
要导出报告：从Reports屏幕中单击export按钮



• 在菜单中选择CSV或PDF格式。
系统弹出如下提示:

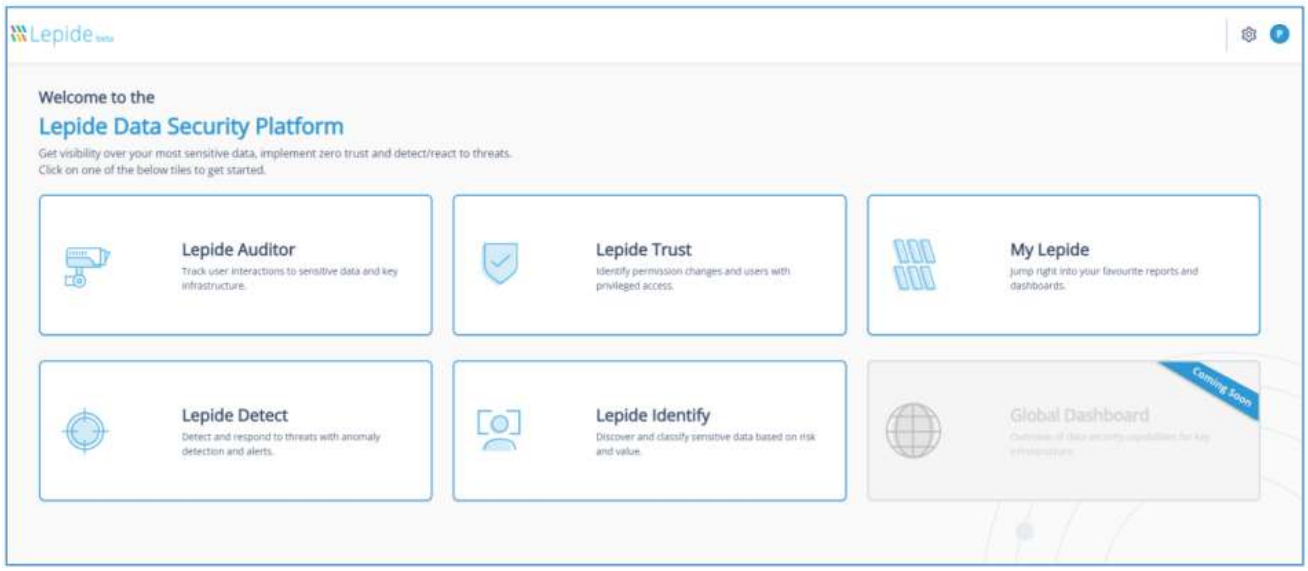


• 点击导出文件按钮查看导出的进度，并在导出过程完成后查看导出的文件



向我的Lepide添加报告

主屏幕上的My Lepide Dashboard列出了您添加到My Lepide的任何报告和仪表板，提供了一种轻松查找和运行您经常使用的报告的方法。任何报表都可以添加到My Lepide，无论是预定义报表还是自定义报表。

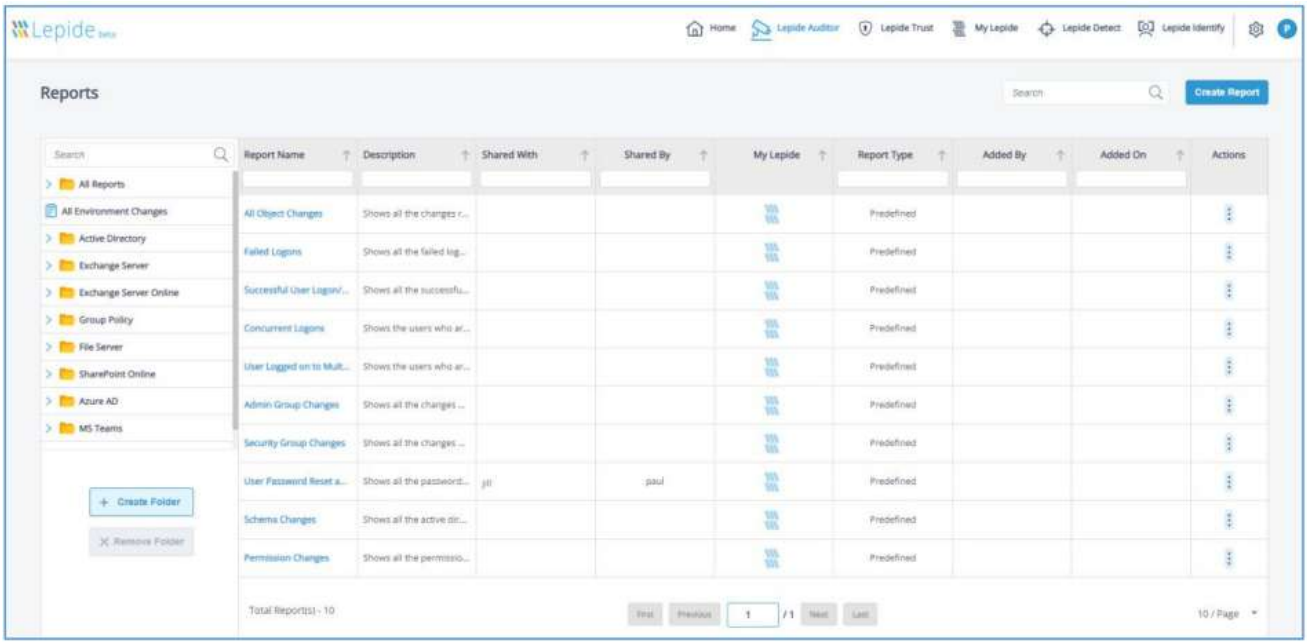


向"我的文件夹"添加报表：

• 在主界面选择一个类别，例如"Lepide Auditor"。

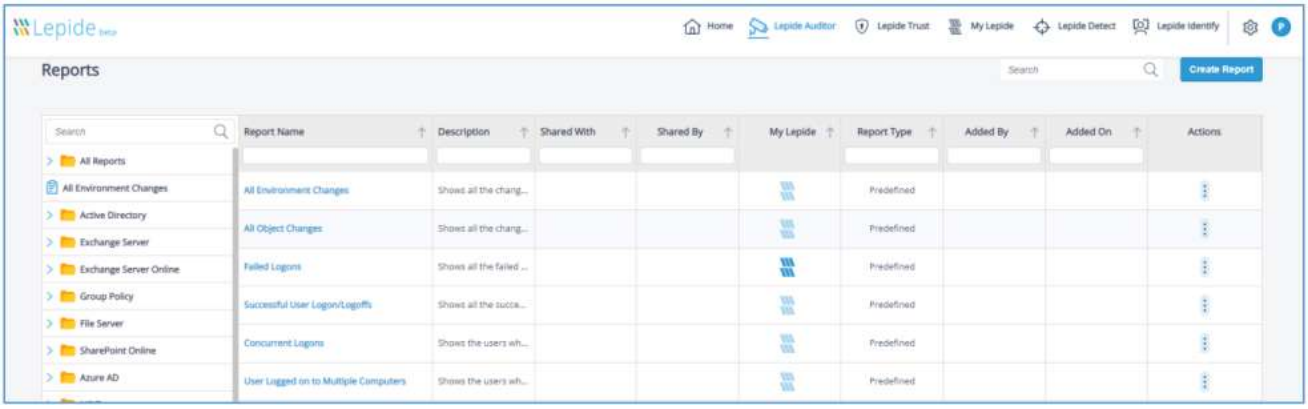
• 进入“Lepide Auditor Dashboard”界面。

• 在界面上方选择一个类别，例如“leide Auditor”，选择“Reports”。



• 找到要保存到My Lepide的报告

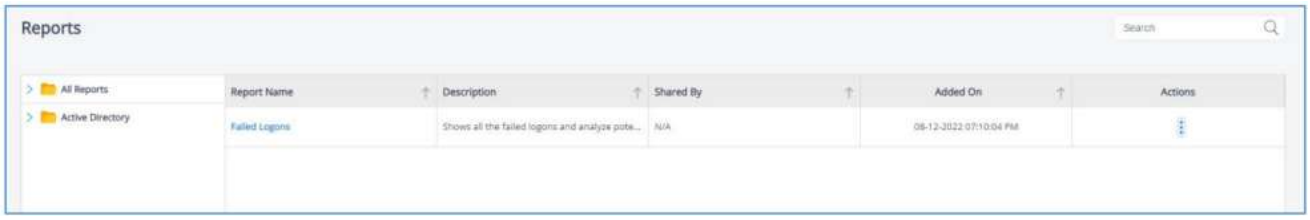
• 单击My Lepide列中的图标，将报告添加到My Lepide Dashboard



在上面的示例中，登录失败报告已添加到My Lepide中。这可以看到图标已经变成了深蓝色。

• 对所有您希望从My Lepide获得的报告重复此操作

现在，当您从报告屏幕顶部的菜单栏或主屏幕上的选项中选择My Lepide时，将显示您的报告。

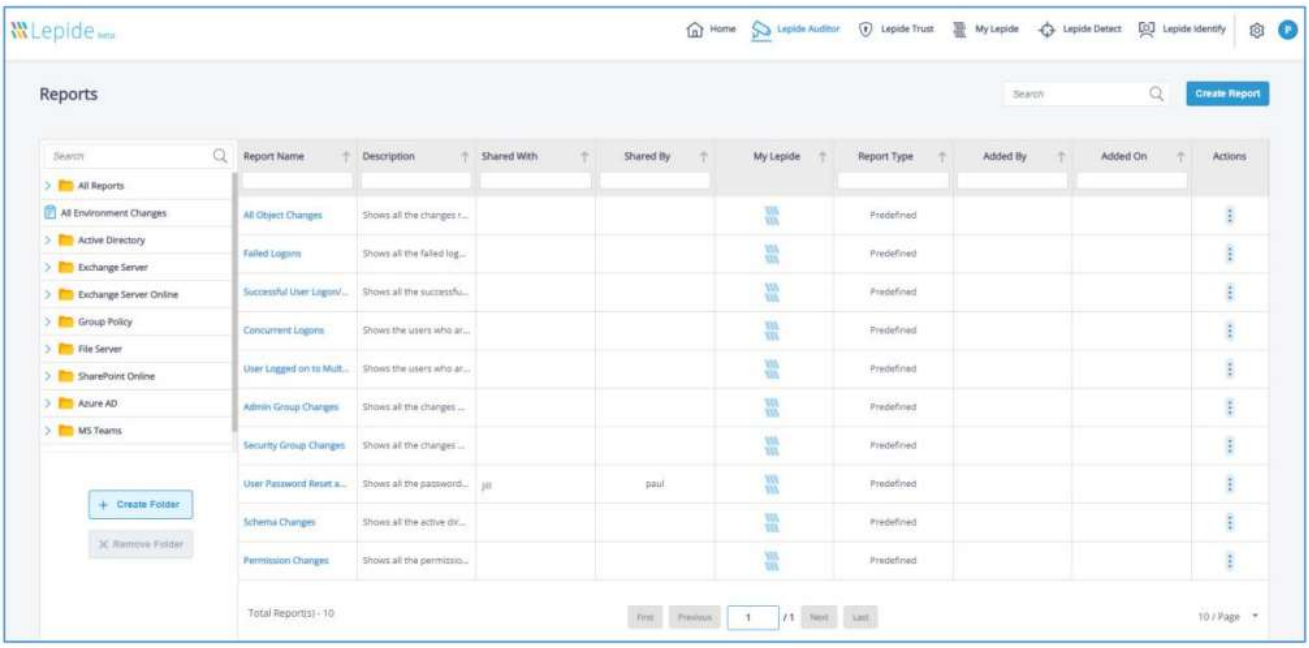


创建自定义报表

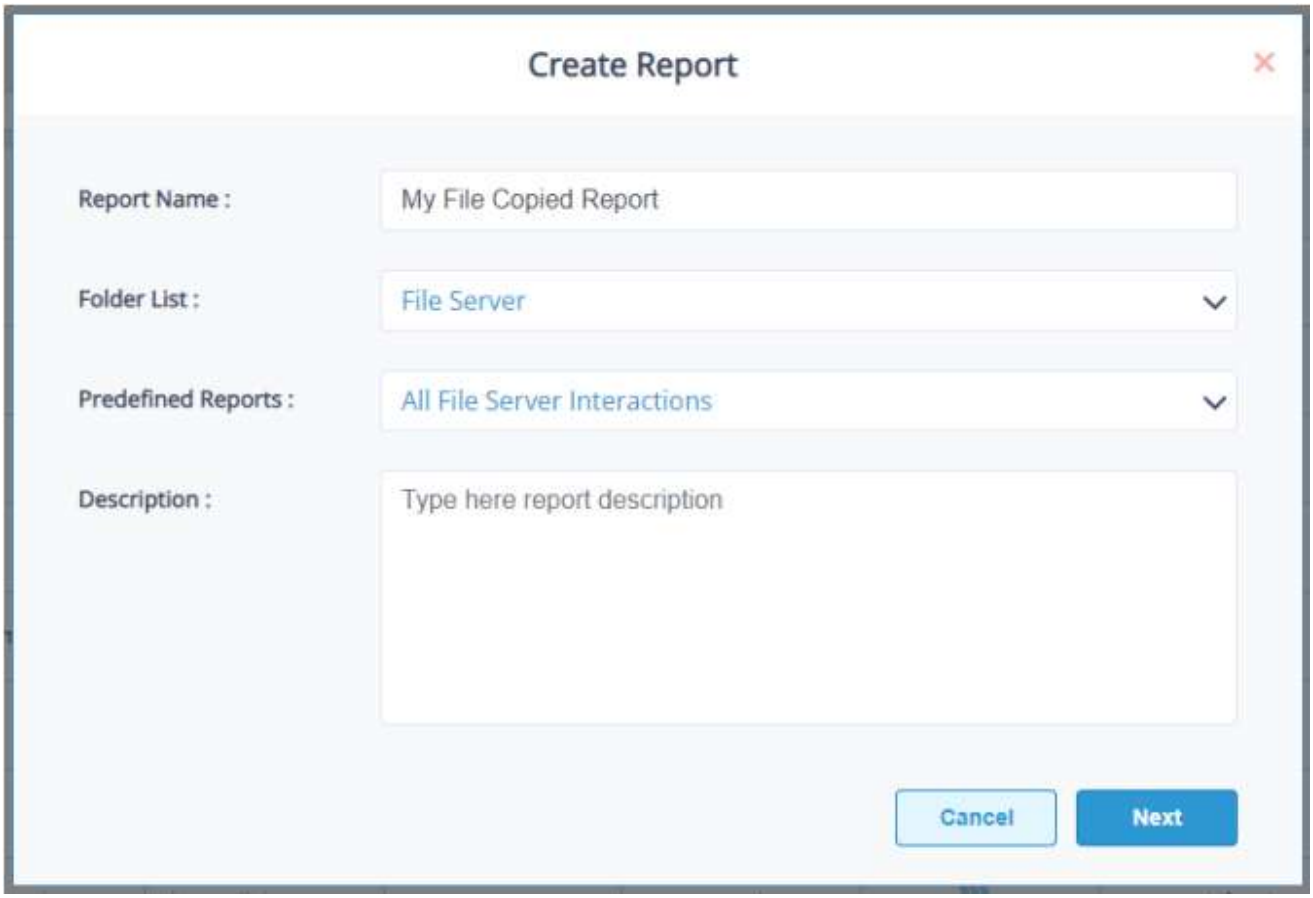
可以创建自定义报表，以便您可以选择想要查看的列和所需的过滤器。创建自定义报表：

• 在主界面中选择一个“Lepide Category”，例如“Lepide Auditor”，进入“Dashboards”界面。

• 在屏幕上方单击一个“Lepide Category”，例如“Lepide Auditor”，选择“Reports”，进入“Reports”窗口。



•单击“创建报表”按钮，系统弹出“创建报表”对话框：



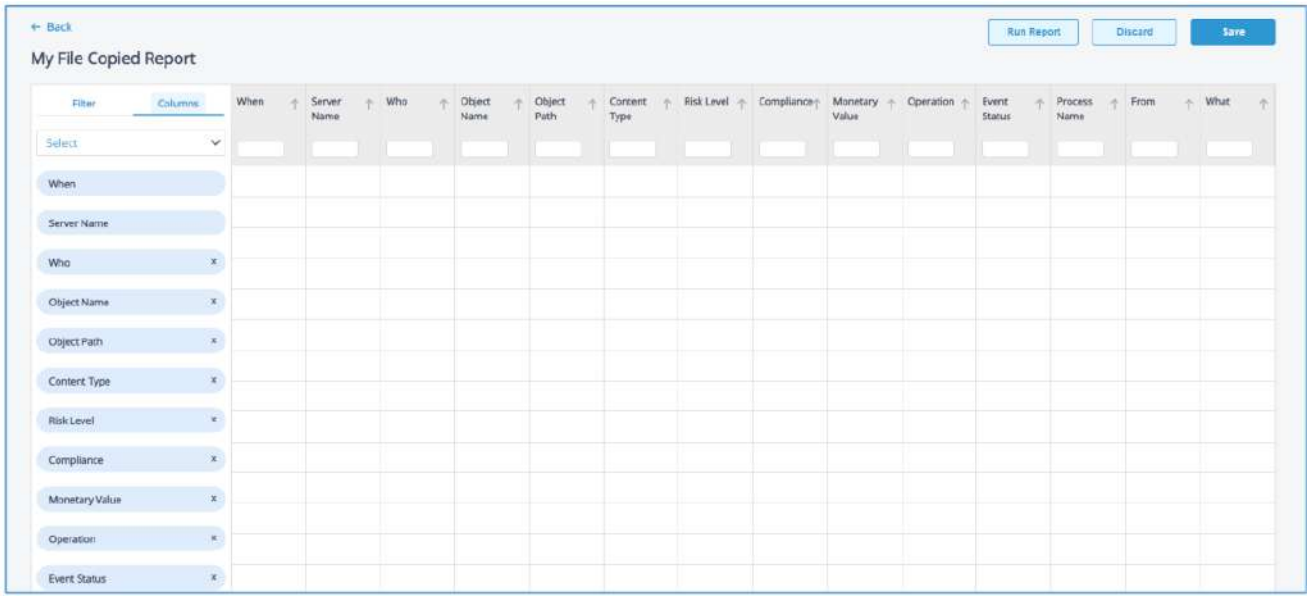
• 输入报表名称

• 在“文件夹列表”中选择需要保存报表的文件夹

• 在“预定义报表”中选择新报表的基础预定义报表

• 添加可选的描述

• 单击“下一步”



将显示Report Editor屏幕，顶部显示报告名称。这些列是预定义报告（之前在Create Report对话框中选择的）中使用的列，此自定义报告将基于这些列。

在屏幕的左上方有两个选项卡：Filter和Columns选中Columns选项卡后，屏幕的顶部和侧面都有列标题。可以使用侧面的列标题通过单击x图标来删除列，并通过将列拖到新位置来更改列的顺序。

在此报表示例中，无法删除"When"和"Server Name"字段，因为它们是报表运行的组成部分。

• 若要恢复先前删除的列名，请单击Select下拉菜单并选择列名。

• 单击Filter选项卡为报表添加过滤器。有关设置过滤器的更多信息，请参考本指南的第10节。

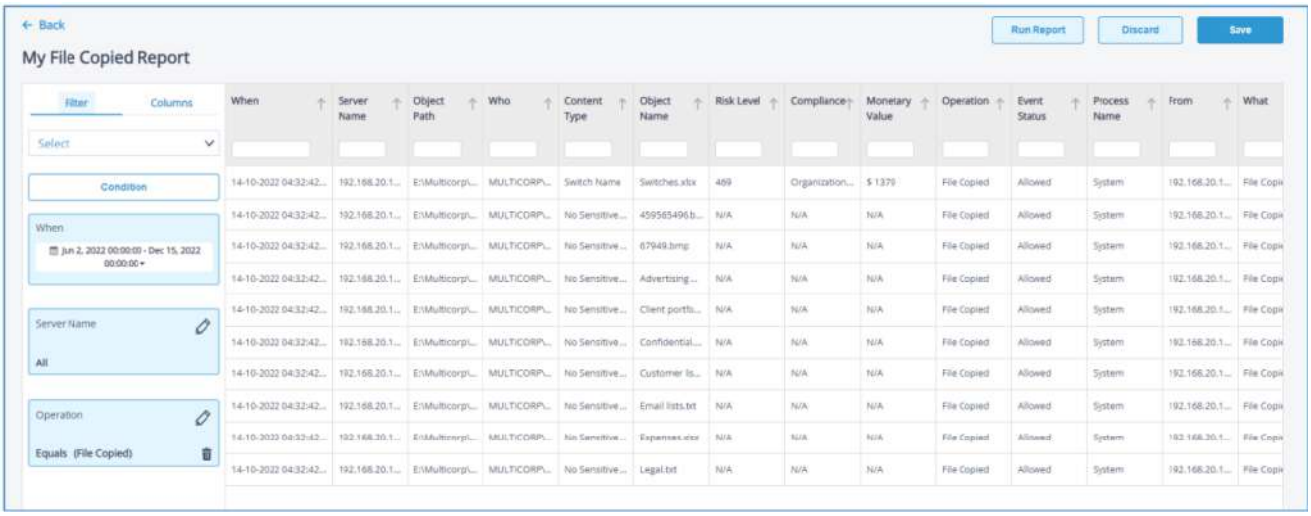
• 完成后，单击保存。这将保存您对列或过滤器所做的任何更改，您将返回Reports屏幕。

• 选择Generate Report以运行报告

报告将存储在您在"创建报告"对话框中指定的文件夹中，并将与您之前选择的所有自定义选项一起保存。

编辑自定义报表

• 要对自定义报告进行更改，请单击自定义报告图标（在过滤器图标旁边），这将带您到报告编辑器屏幕，这将显示您的自定义报告以及您之前指定的列和过滤器



• 根据需要进行更改

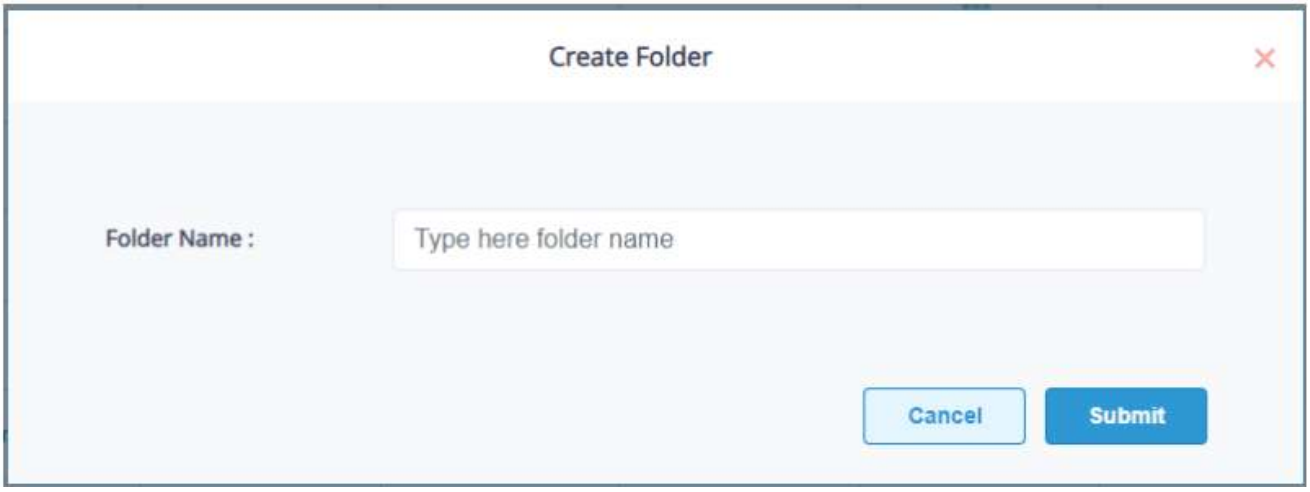
• 完成后单击Save

创建自定义文件夹

可以在Lepide Web控制台中创建自定义文件夹，这提供了一种简单的方法来定位和运行您经常使用的报告。创建自定义文件夹：

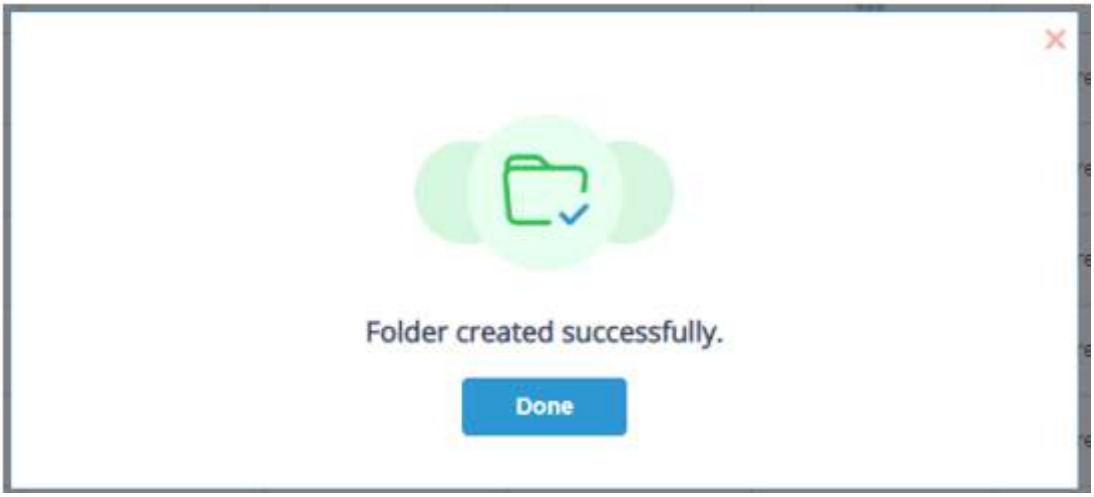
• 从Reports屏幕中选择create folder

系统弹出"创建文件夹"对话框：

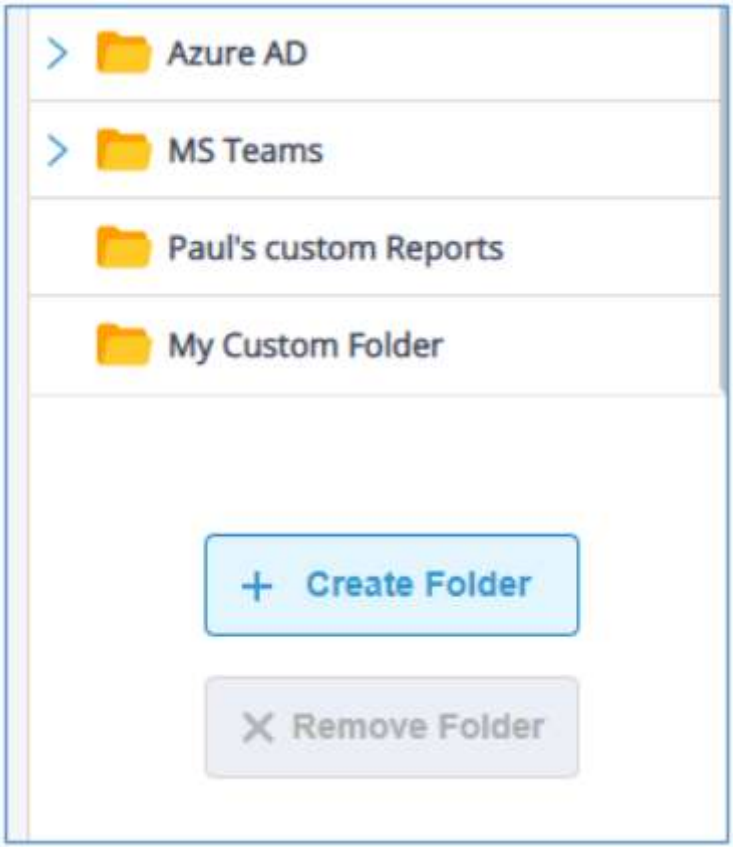


• 输入文件夹名称，单击"提交"。

系统弹出提示框，提示文件夹创建成功：



•单击Done，自定义文件夹将显示在报告屏幕左侧的文件夹列表中：



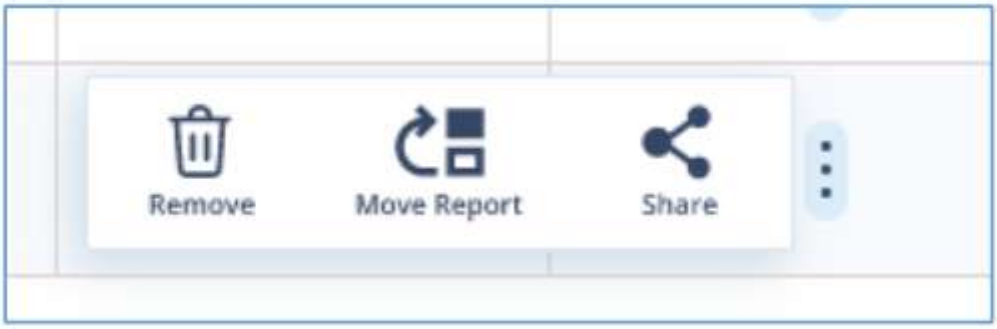
现在，当您创建自定义报告时，您可以将其保存在自定义文件夹中。

删除、移动或共享报表

自定义报表可以删除、移动或共享，而预定义报表可以共享。

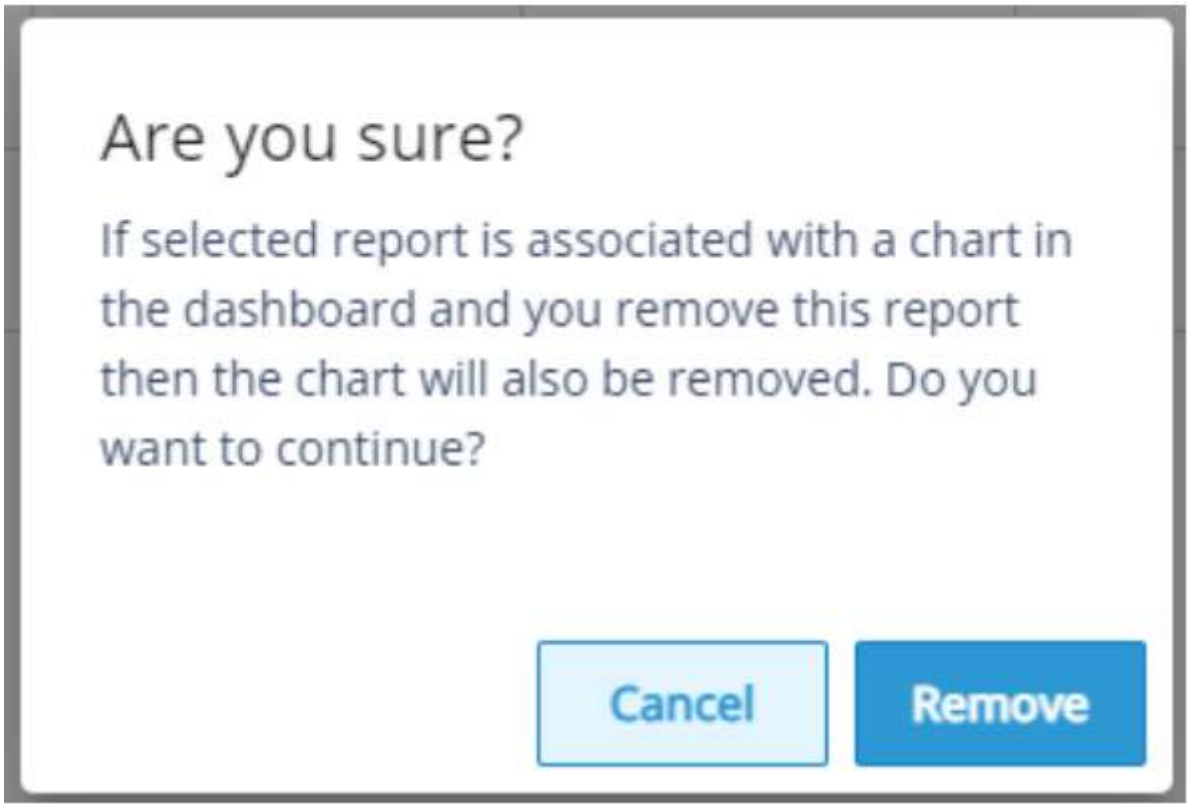
删除自定义报表

在Reports屏幕中，单击要删除的报表旁边的图标。将出现用于删除、移动或共享报表的此菜单选项。



• 选择删除

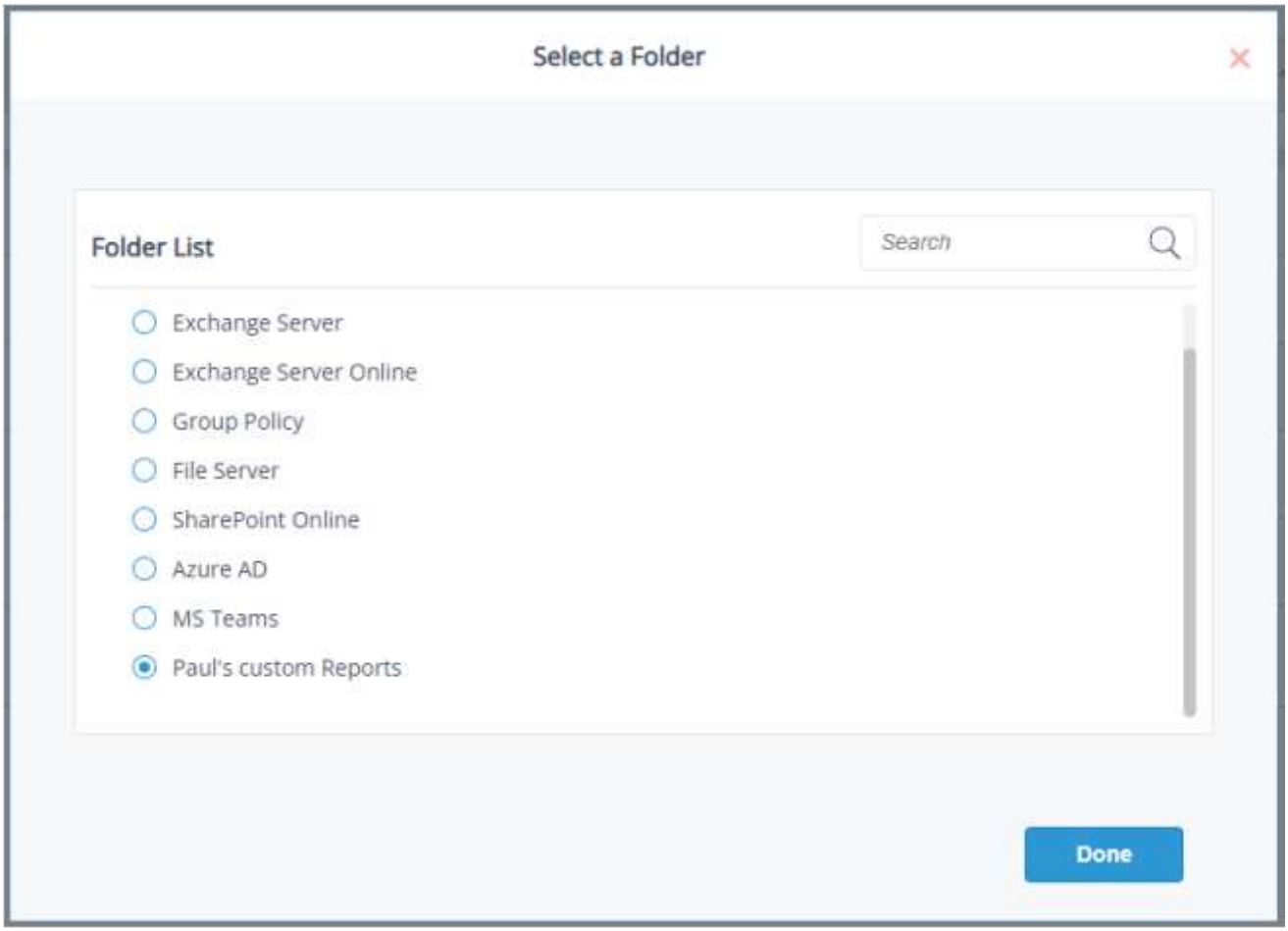
系统弹出如下对话框：



• 单击"移除"，移除报表

移动自定义报表

• 单击图标，选择"移动报告"。系统弹出"选择文件夹"对话框：

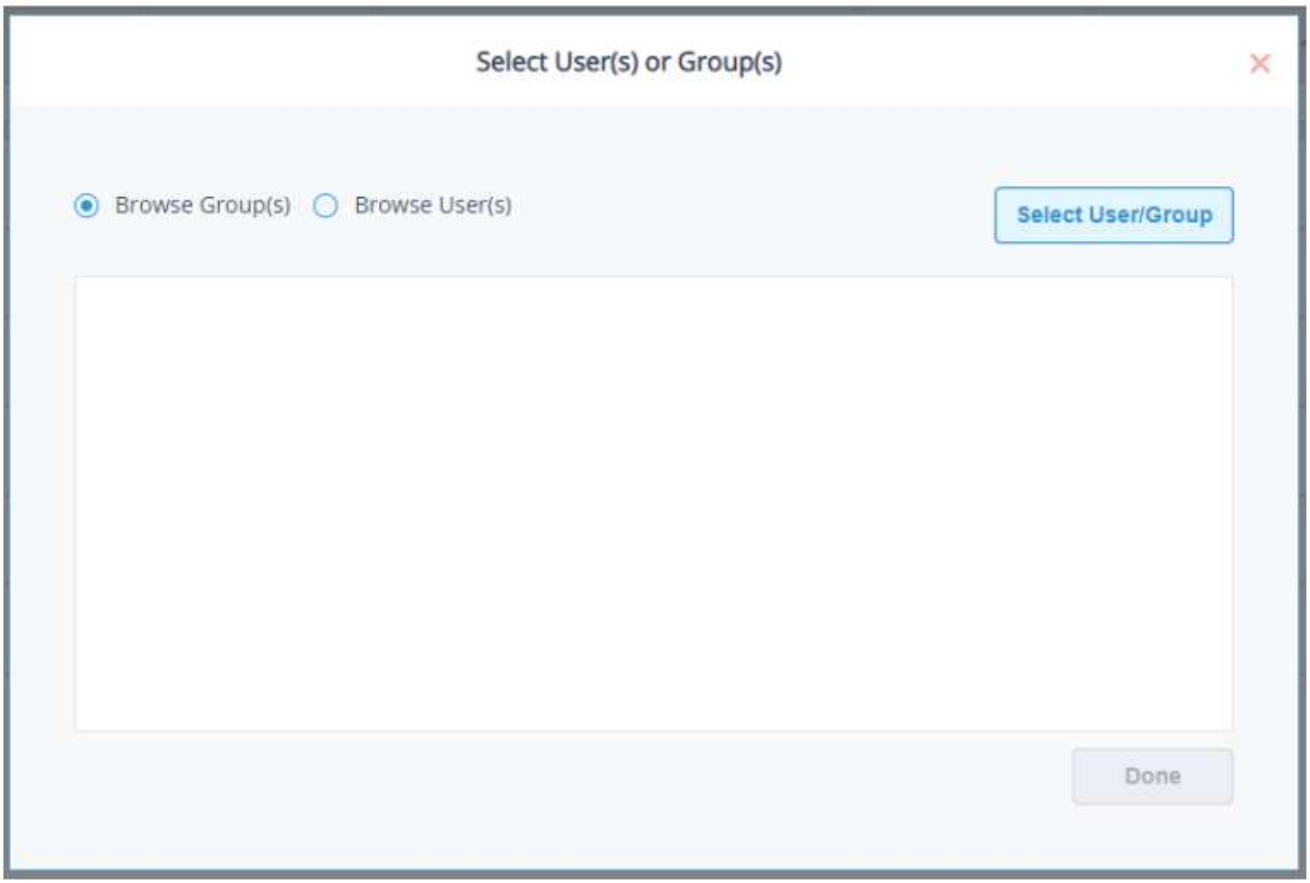


• 选择要移动报表的文件夹

• 单击"完成"

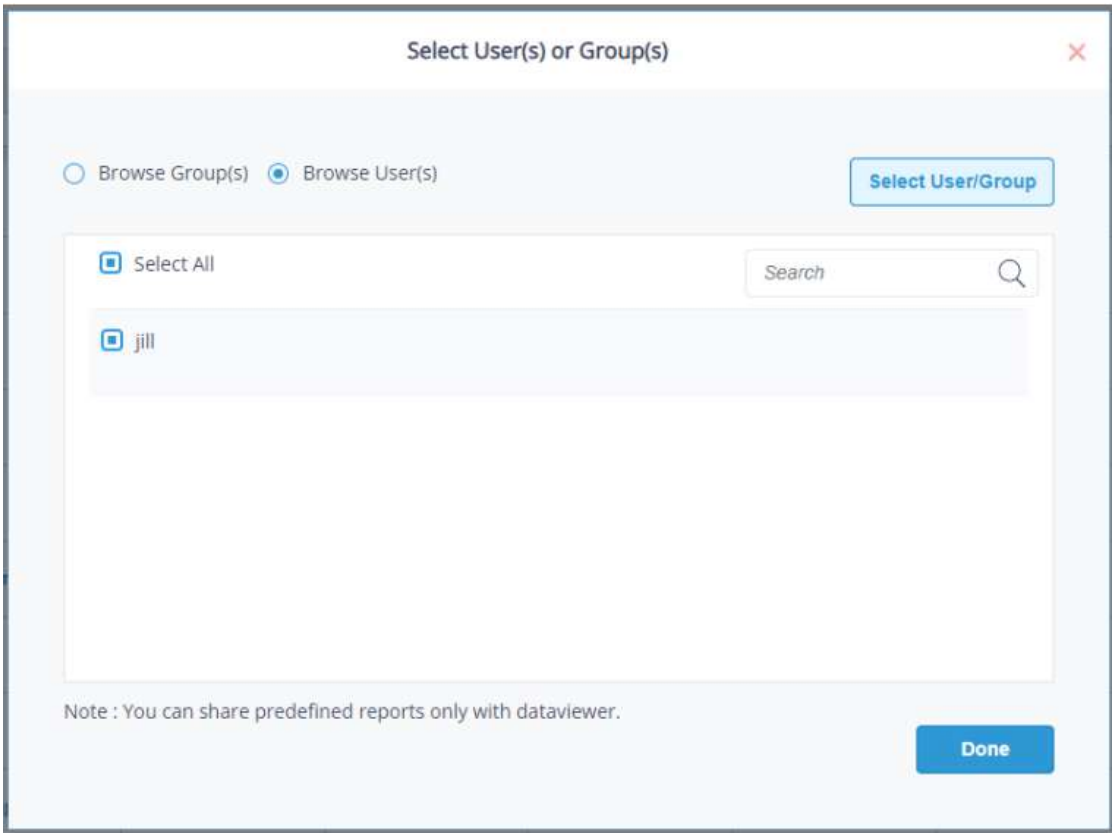
共享报表

• 单击图标，选择"共享报告"。系统弹出"选择用户或组"对话框：



• 选择"浏览组"或"浏览用户"，然后单击"选择用户/组"按钮

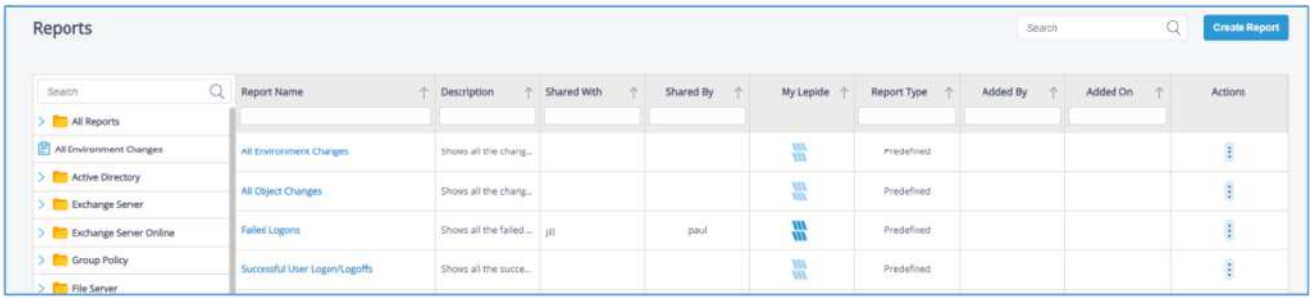
将显示一个用户或组列表：



• 选择要共享报表的用户，单击"完成"。系统弹出"共享成功"提示框。

• 单击Done。

共享信息将显示在Reports屏幕的Shared With和Shared By下。在本例中，Failed Logons报告由Paul与Jill共享。



警报

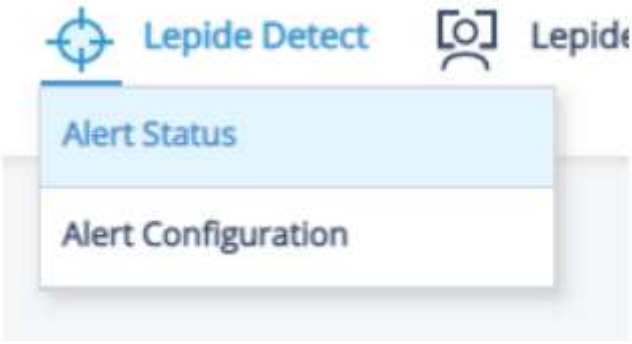
所有重大安全变化的实时警报是使组织能够快速检测和响应潜在威胁的重要工具。所有警报都是实时的，并通过电子邮件或直接到任何iOS或Android移动设备发送给管理员或选定的收件人。

可以将Lepide Web控制台配置为在触发警报时执行自定义脚本。脚本可以是以下类型：VB脚本、PowerShell脚本或批处理文件。

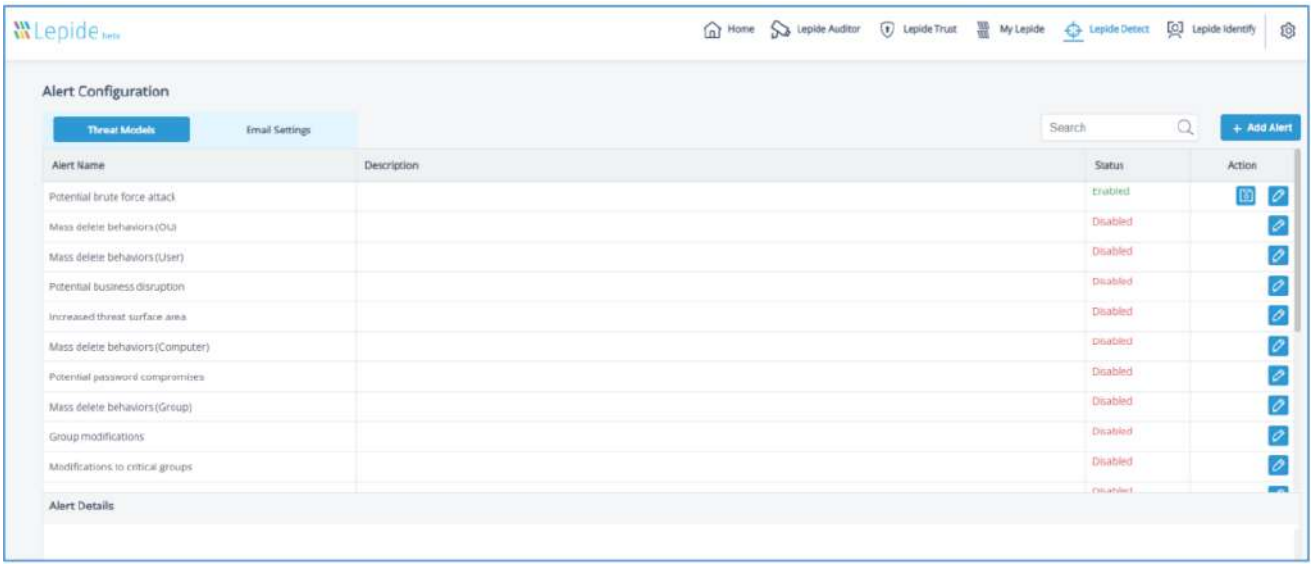
使用自定义脚本执行，您可以关闭用户、服务器并采取其他措施来减轻安全漏洞的影响

警报状态

• 若要查看警报报告列表，请选择警报状态



这将显示警报状态屏幕。这里将显示任何已运行的警报报告。

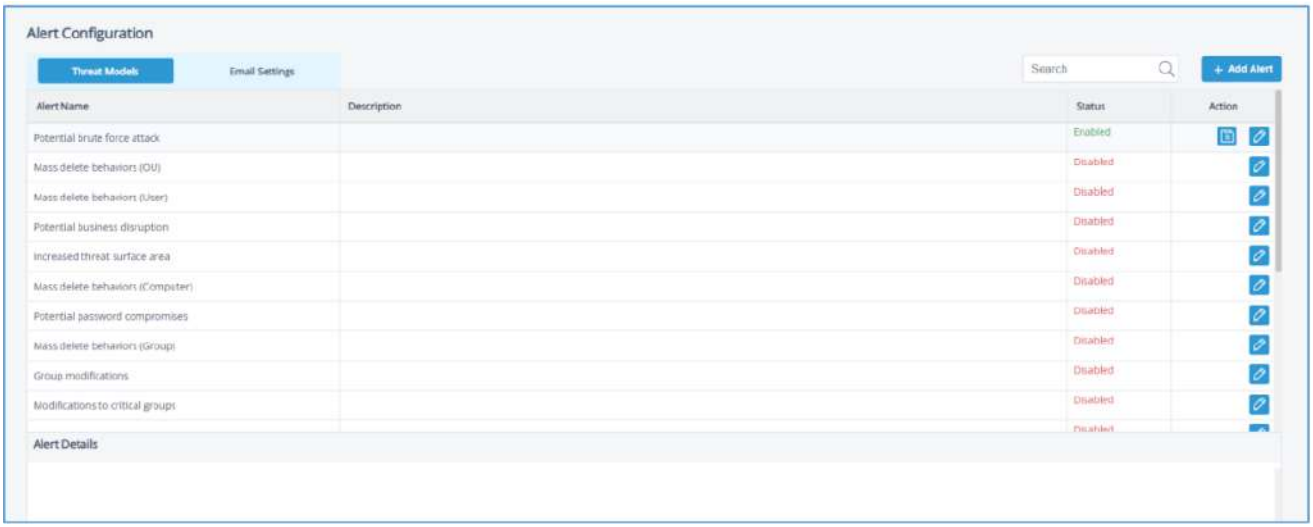


在左边有两个选项卡:威胁模型和电子邮件设置，它们的描述如下:

威胁模型

Lepide Web Console中包含许多威胁模型。威胁模型是针对特定场景的预定义警报，例如场景可能是潜在的勒索软件攻击或文件复制。只要通过启用这些预定义的威胁模型之一检测到潜在威胁，就会生成实时警报。

Lepide Web控制台中可用的所有威胁模型都显示在警报配置屏幕的威胁模型选项卡下:



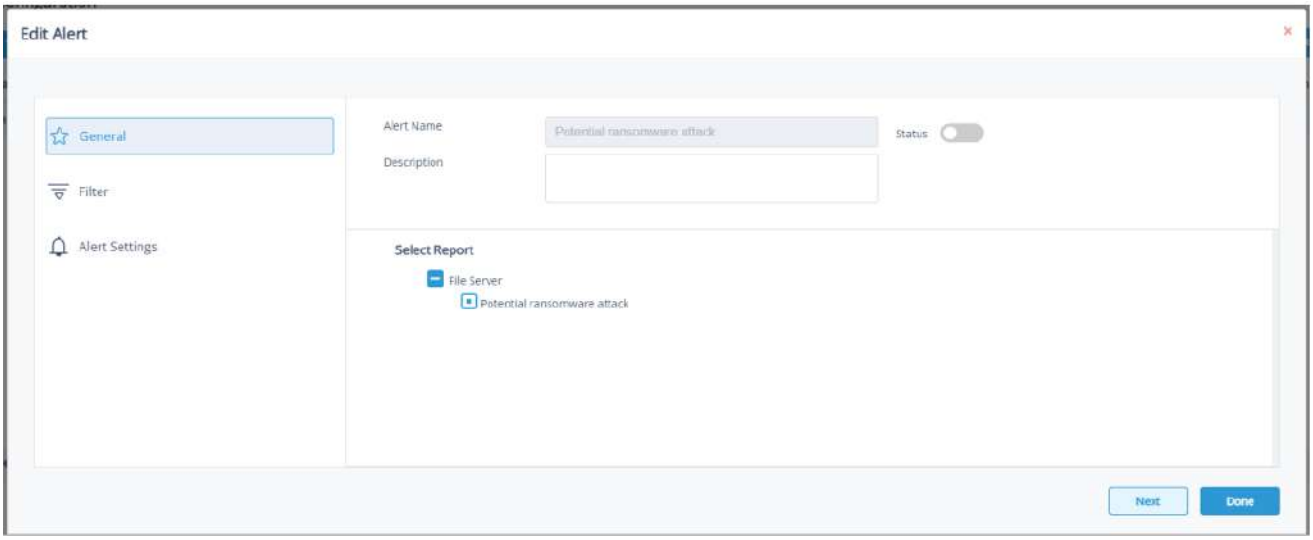
可以根据需要启用威胁模型。然后可以将它们配置为生成警报并对威胁做出响应。下面的示例解释了如何启用潜在勒索软件攻击威胁模型。

如何启用和配置威胁模型

•从警报配置屏幕向下滚动，直到你可以看到你想要启用的威胁模型。您还可以在顶部的搜索栏中键入搜索特定的威胁模型。

•要启用潜在勒索软件攻击威胁模型，请单击编辑图标。

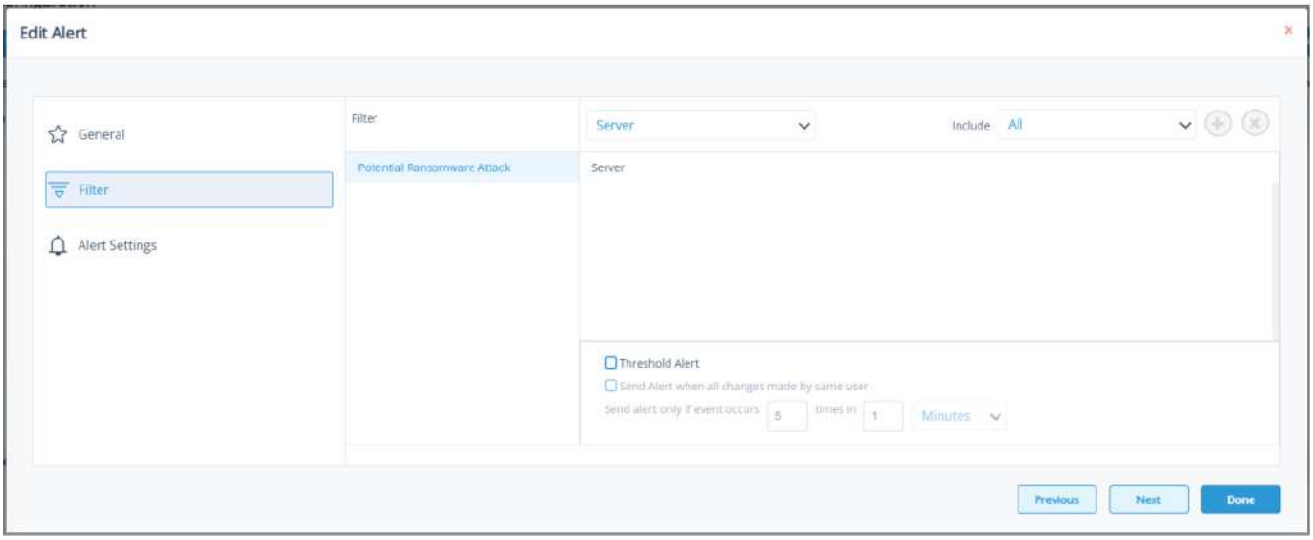
弹出"编辑警报"对话框:



• 向右滑动状态切换按钮以启用威胁模型

• 单击下一步

这将带您到过滤器选项：



• 在对话框的左侧，您可以看到您正在处理的威胁模型，即潜在的勒索软件攻击。

• 单击"服务器"下拉菜单选择选项，以更改服务器、用户、对象名称、对象路径、操作、进程和来源的设置。所有这些选项的默认设置是all。

• 阈值警报选项可自定义如下：

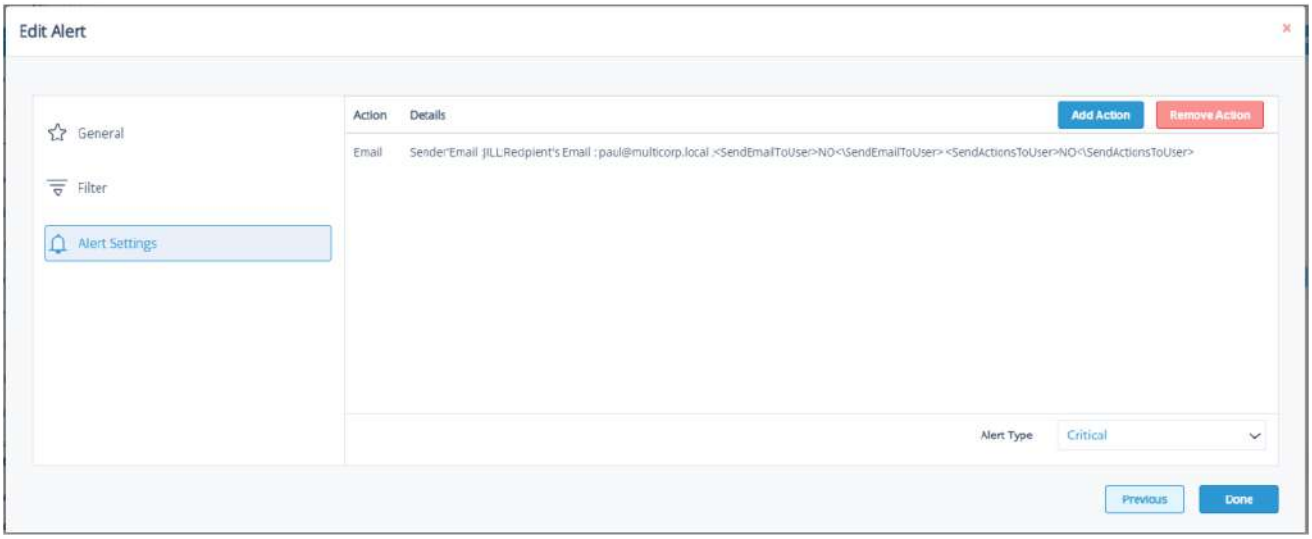
阈值警报：选中此框以开启阈值警报

当同一用户进行所有更改时发送警报：如果您希望在单个用户进行所有更改时发送警报，请勾选此选

项。仅在事件发生时发送警报：更改事件发生的次数，时间值和时间段

• 单击下一步

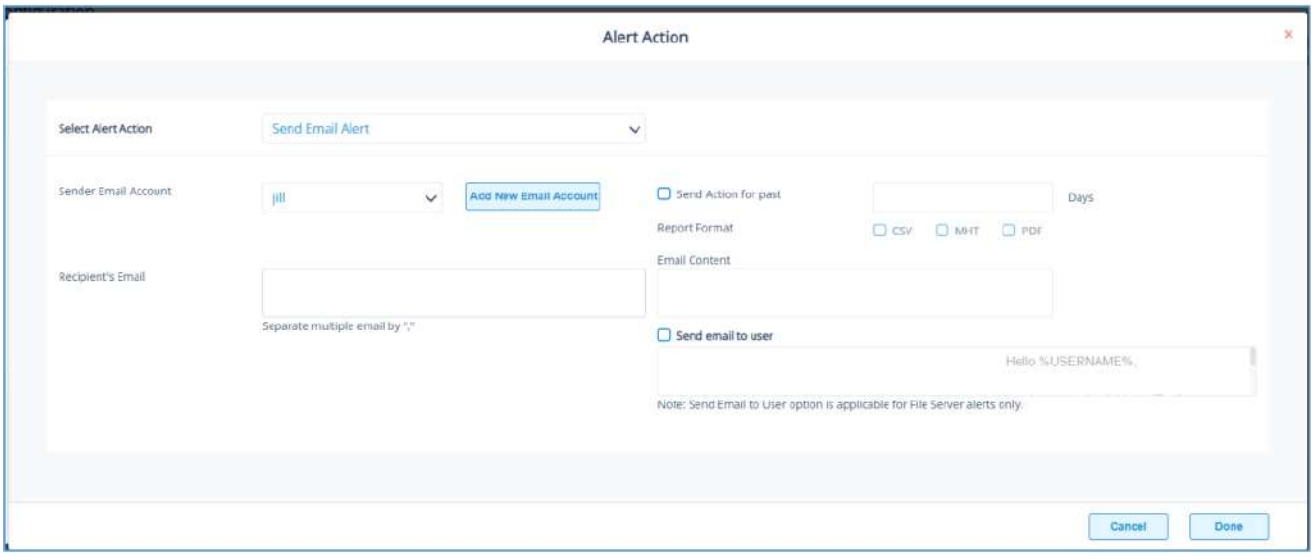
警报设置显示如下：



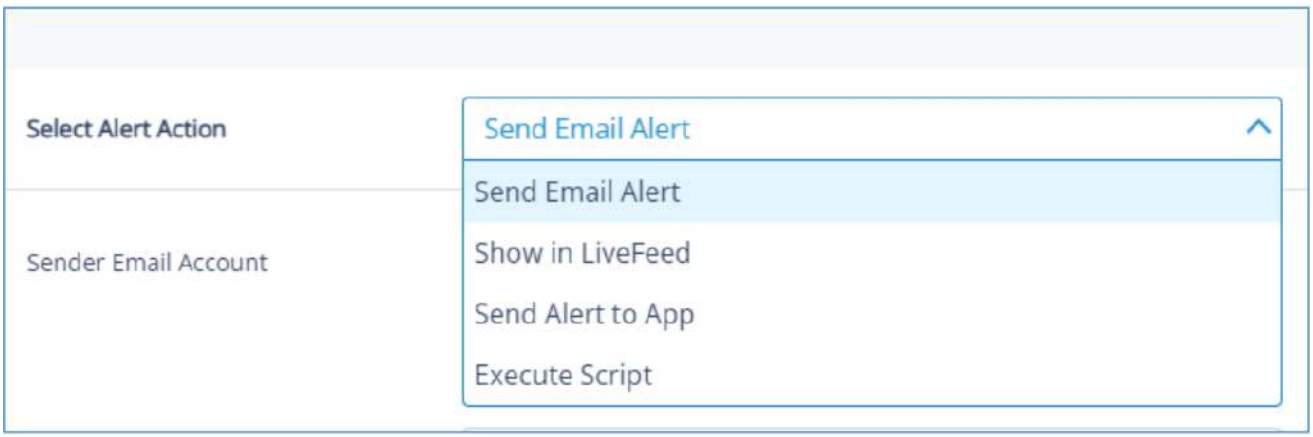
这允许您设置在触发警报时发生的响应，并显示已设置的任何现有响应。您也可以更改警报类型。

• 要创建对警报的新响应，请单击"添加操作"按钮。

• 弹出"警报操作"对话框：



• 单击Select Alert Action下拉箭头以查看可用操作列表：



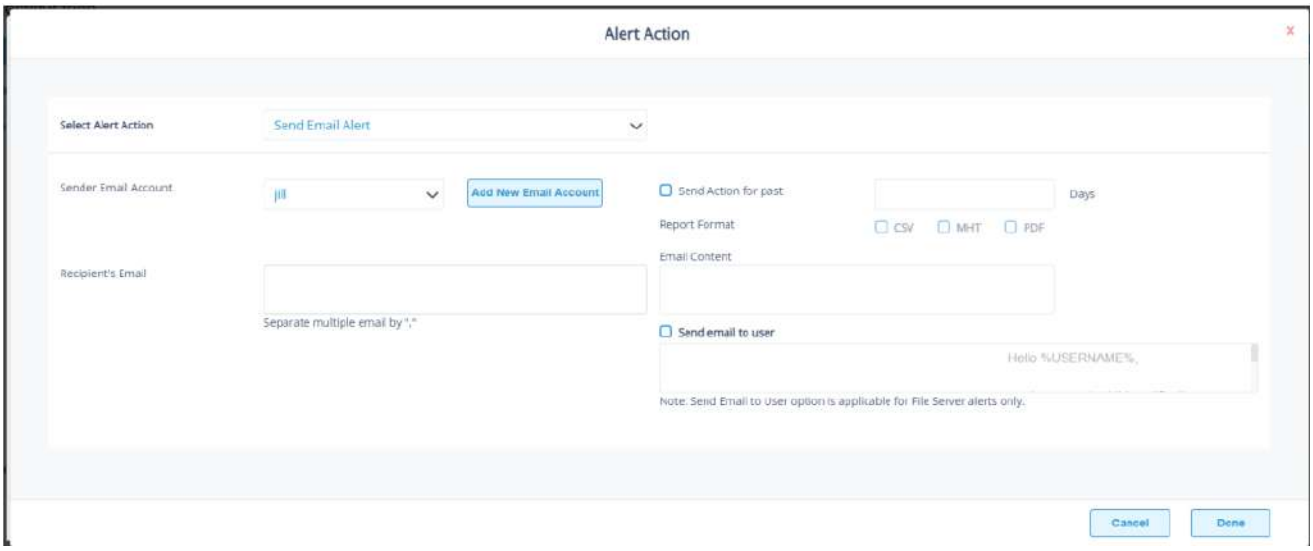
警报动作如下：

- 发送电子邮件警报在LiveFeed中显示发送警报到App

- 执行脚本。

  这些动作的配置解释如下：

1. 发送电子邮件提醒



此选项允许您在触发警报后发送电子邮件。对话框的元素包括：

•发件人电子邮件帐户：如果已选中发件人的电子邮件帐户，此处将显示发件人的电子邮件帐户。

单击"添加新电子邮件帐户"，输入新的发件人电子邮件帐户。有关添加新电子邮件帐户的更多信息，请参阅本指南

的第16.4节。

• 收件人的电子邮件：通过在框中输入电子邮件地址来添加收件人的电子邮件。如果有多个邮箱地址。•发送过去xx天的操作:此选项允许您查看该用户在过去指定天数内所做的所有操作。例如，如果因为他们一直在复制文件而触发警报，那么您可能希望查看他们还做了什么。选中此框并指定天数，将发送一封电子邮件，其中包含一个附件，列出用户在指定天数内所做的所有事情。

• 报告格式：件将包含一份报告，可通过选中相关框指定报告格式。格式为CSV、MHT和PDF。

• 邮件内容：在此处输入要发送的邮件内容。•向用户发送邮件:勾选该复选框，向用户发送邮件。可以在文本框中输入邮件的内容。要在内容中包含用户名，请使用变量%username%。

请注意，此选项仅适用于文件服务器警报。

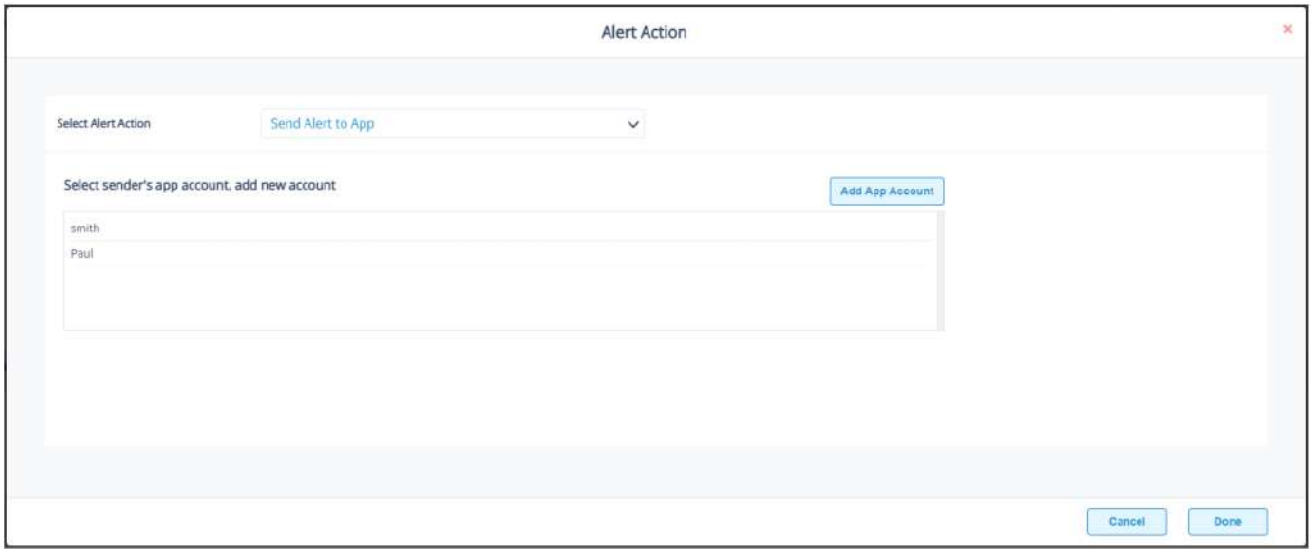
• 单击"完成"保存警报操作。

2. 在LiveFeed中显示

在LiveFeed中显示意味着警报将被发送到LiveFeed仪表板，可以在Lepide检测仪表板屏幕上看到。

• 单击"完成"打开LiveFeed警报。

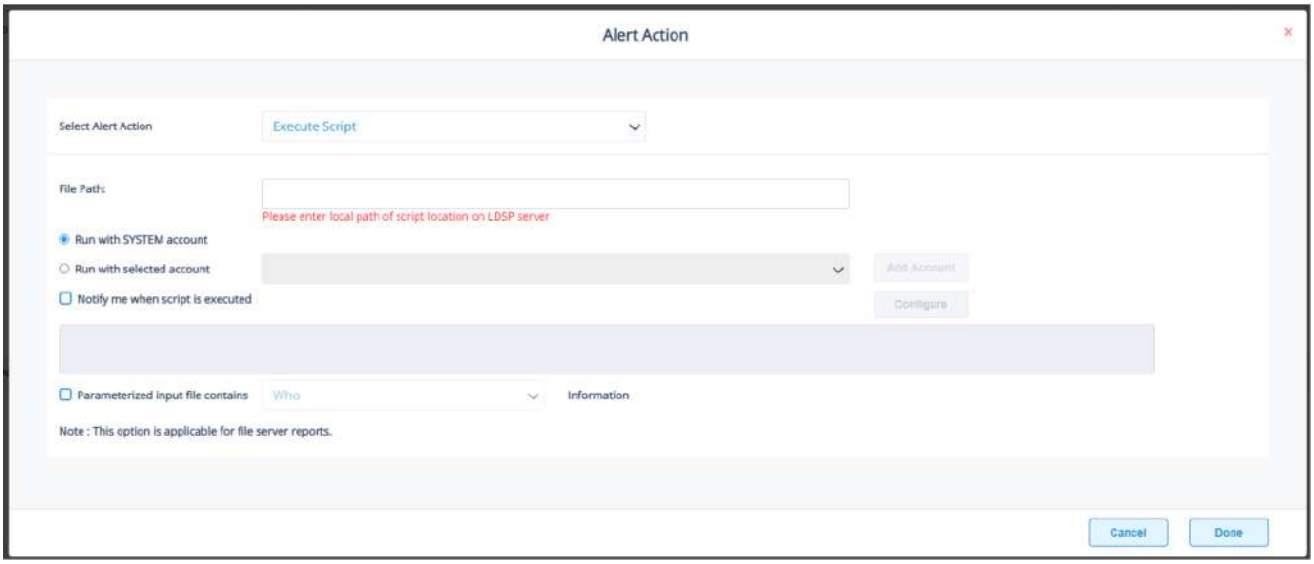
3. 向App发送提醒



• 发送警报到应用程序选项发送警报到移动设备。

• 单击"添加App账号"添加新的手机账号。有关添加新App帐户的更多信息，请参阅本指南的第16.4节。

4. 执行脚本



下拉菜单中的最后一个操作是Execute Script。这将设置在触发警报时执行预定义的PowerShell脚本之一的选项。

对话框各元素如下：

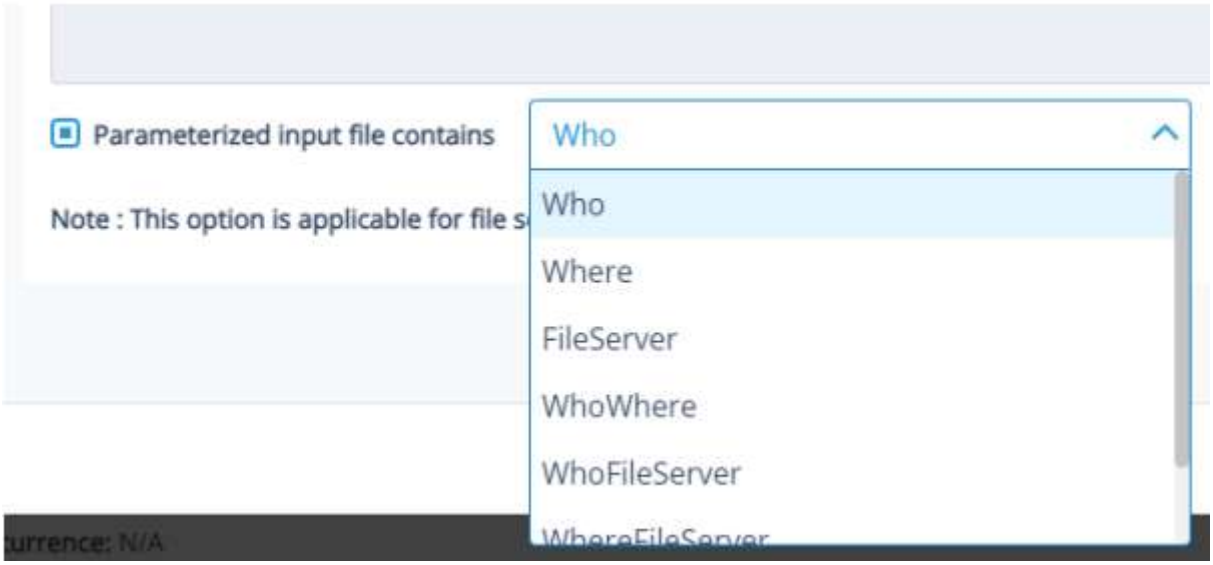
• 文件路径：单击"选择:以SYSTEM帐户运行"或"以选定帐户运行"，选择PowerShell脚本的文件路径。

• 如果选择"带选定账号运行"，可以通过下拉菜单选择账号，也可以单击"添加账号"指定需要使用的账号。

• 选择"脚本执行时通知我"，在脚本执行时发送邮件。

• 选中此选项后，Configure按钮可用。选择"配置"设置发件人的帐户和收件人的电子邮件地址。

• 选择Parameterized input file contains指定脚本中包含的变量。选中此选项后，将出现一个下拉菜单，用于选择变量：



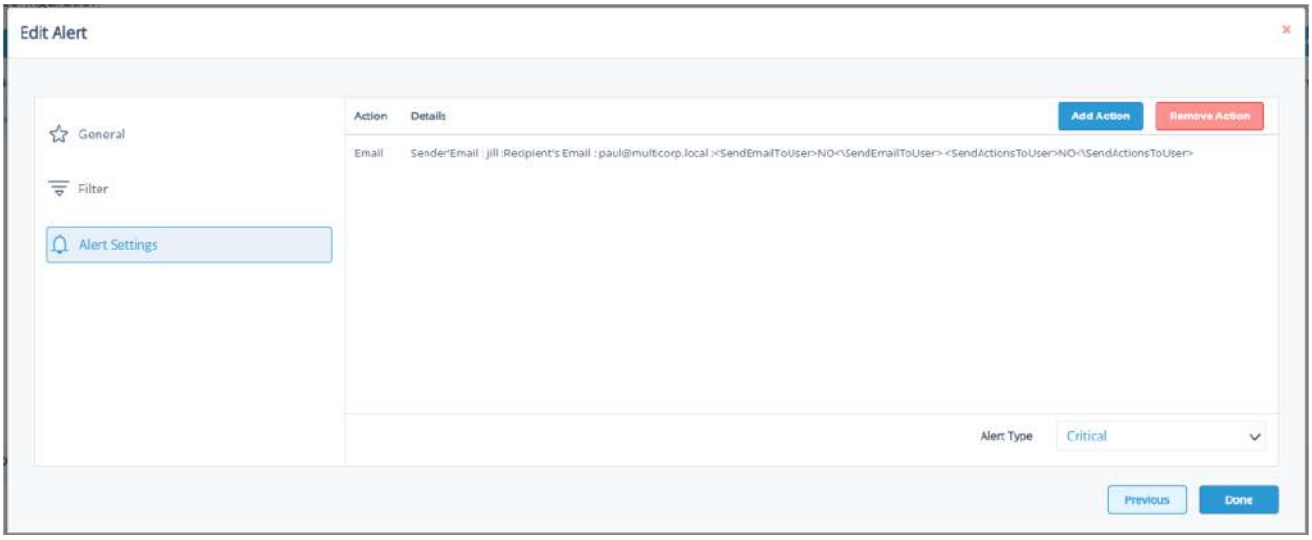
• 单击"完成"返回警报设置

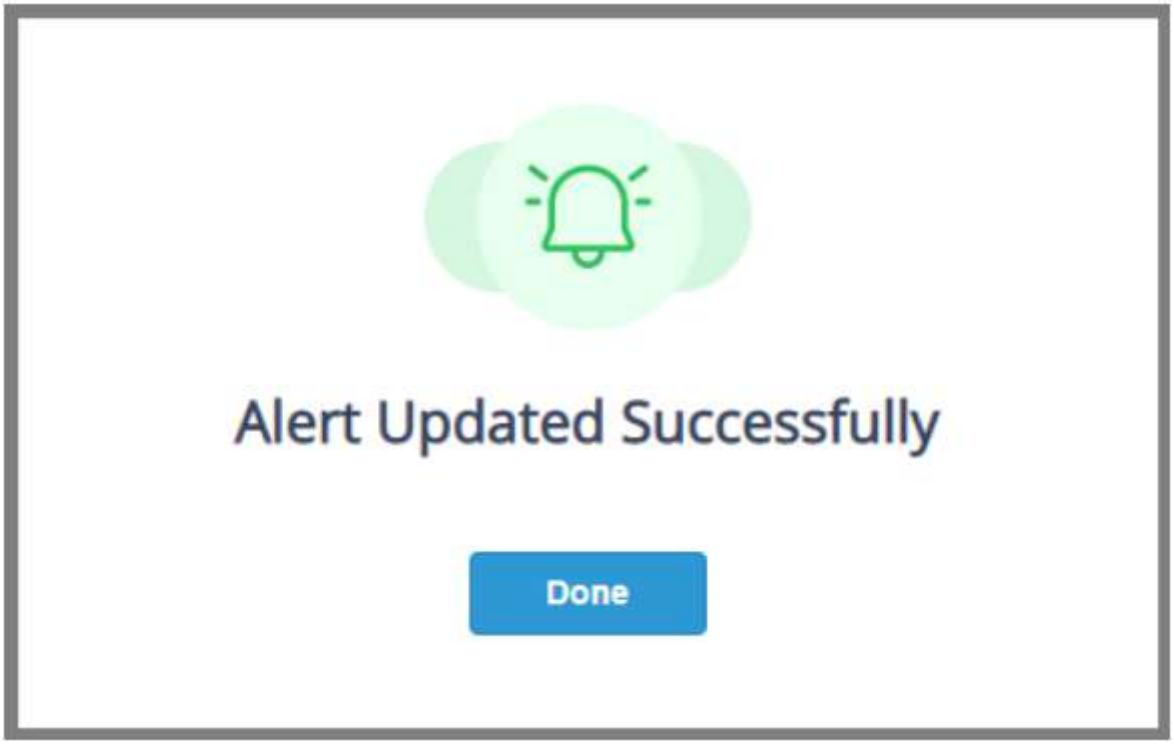
• 现在选择警报类型，可以是紧急，警告或正常

• 单击"下一步"继续

• 弹出确认对话框，显示警报详细信息

• 单击"完成"完成

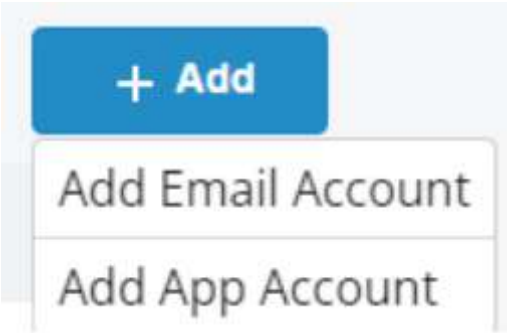




电子邮件设置选项卡

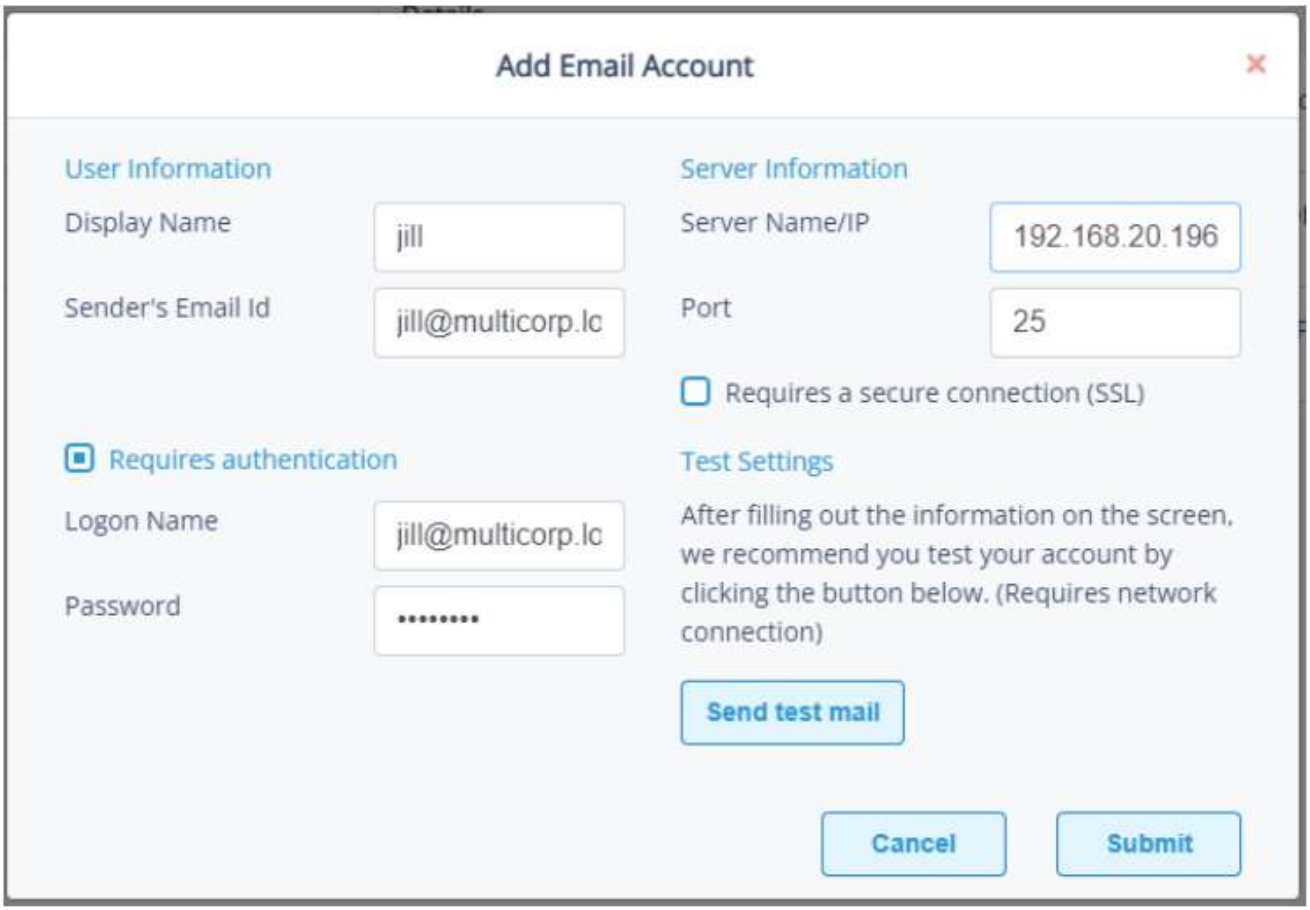
单击电子邮件设置选项卡查看电子邮件设置选项。您可以在这里设置发送警报的电子邮件或应用程序信息。

• 要添加新的电子邮件或应用程序帐户，请单击添加



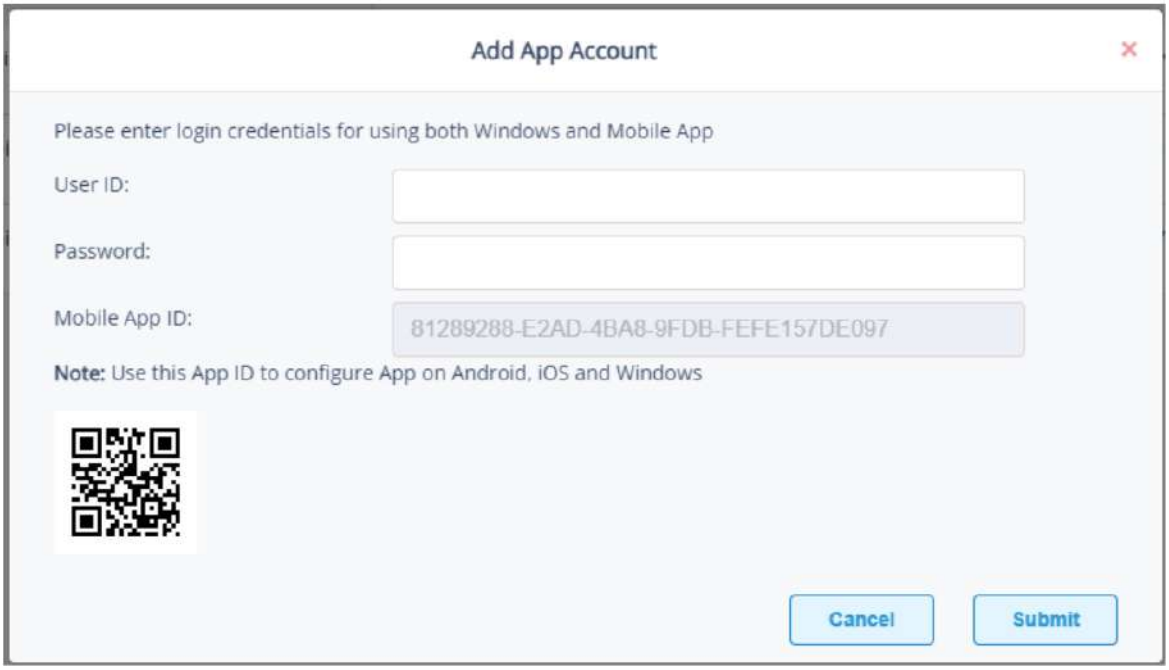
• 选择"添加邮件账号"，添加邮件账号的详细信息

• 输入电子邮件帐户信息，单击“提交”



• 电子邮件帐户的详细信息将在警报配置屏幕中列出：

• 选择“添加应用帐号”，添加应用帐号的详细信息



• 输入"用户名"和"密码"

• 输入"移动App ID"，该ID是通过移动设备扫描对话框底部显示的二维码生成的。

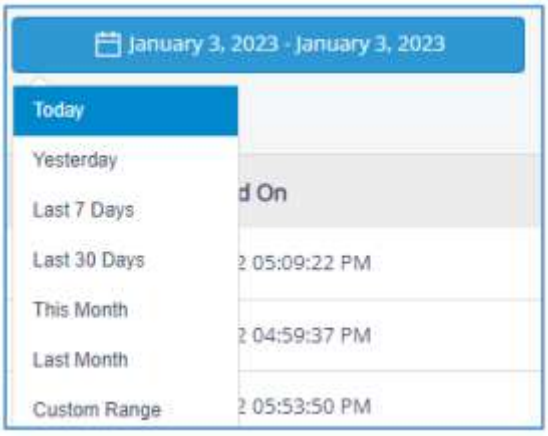
• 单击"确定"

如何查看日志

活动日志可以从管理控制台中查看：

• 添加搜索条件，单击"生成日志"，根据搜索结果查看日志：

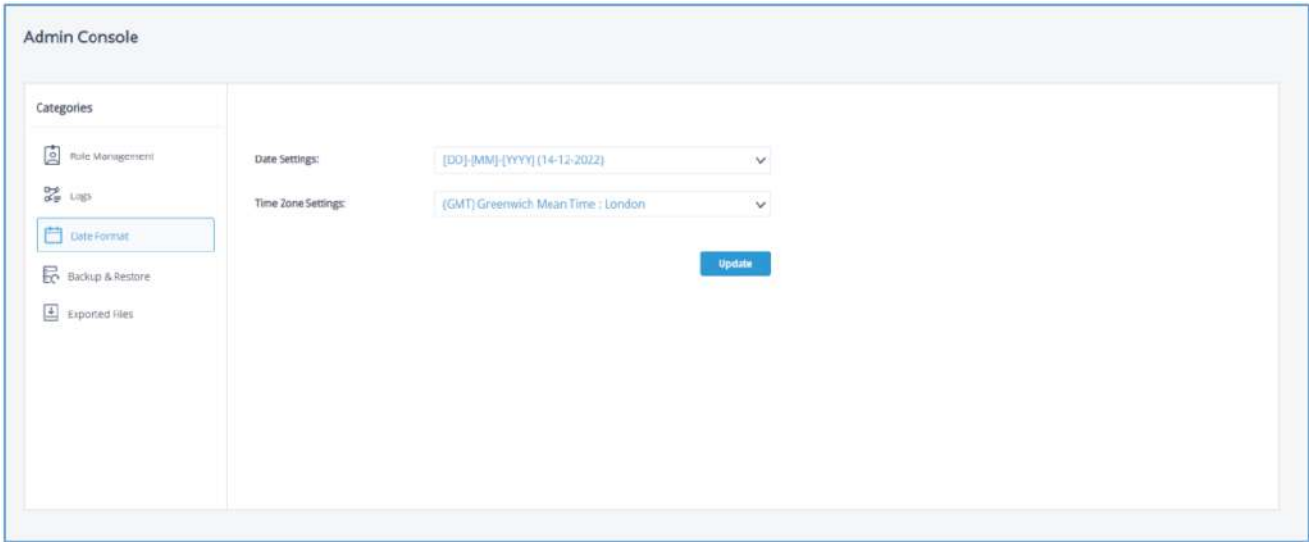
• 选择日期并单击生成日志以查看该日期/时间段的活动



• 通过单击Export按钮将活动日志导出为CSV或PDF

如何更改日期和时间格式

可以在管理控制台中更改Date和Time格式



• 在主界面单击屏幕右上角的"设置"图标

• 选择日期格式

• 单击"日期设置"，选择所需的日期设置

• 单击"时区设置"，选择所需的时区

备份与恢复

可以在管理控制台中设置备份和还原选项。

这些选项允许您导出和导入数据库，其中包含您在Web控制台中选择的所有配置选项，包括自定义报告和文件夹。您可能希望使用备份和恢复特性的示例包括：

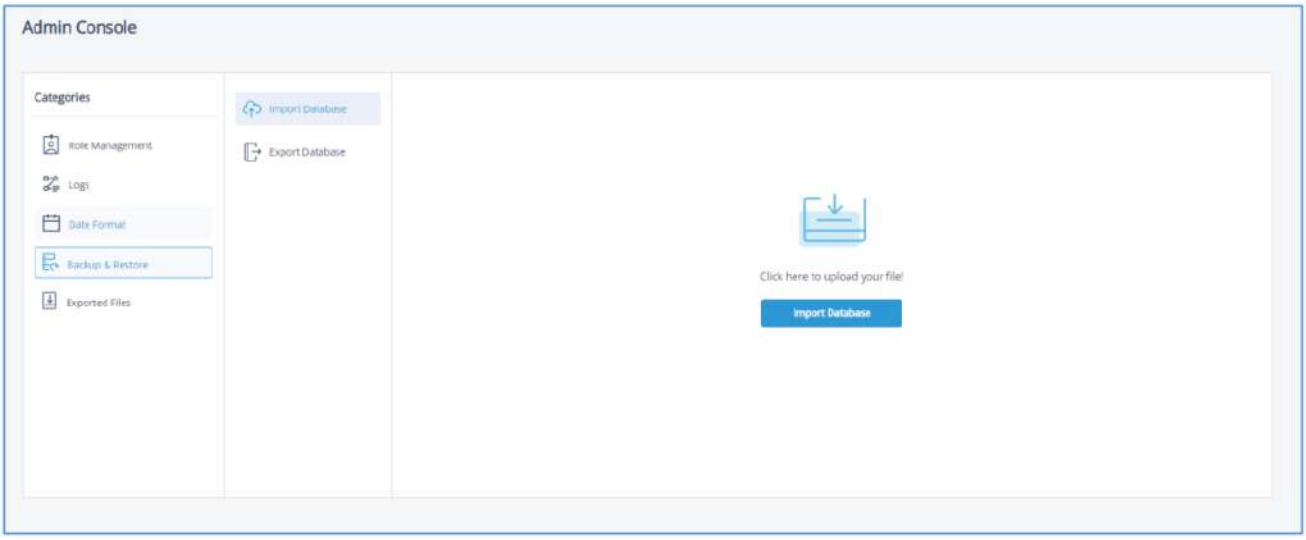
• 进行常规备份的最佳实践方法

• 在希望将Web控制台迁移到其他服务器的情况下

想要备份和恢复

• 从主界面，单击屏幕右上角的设置图标

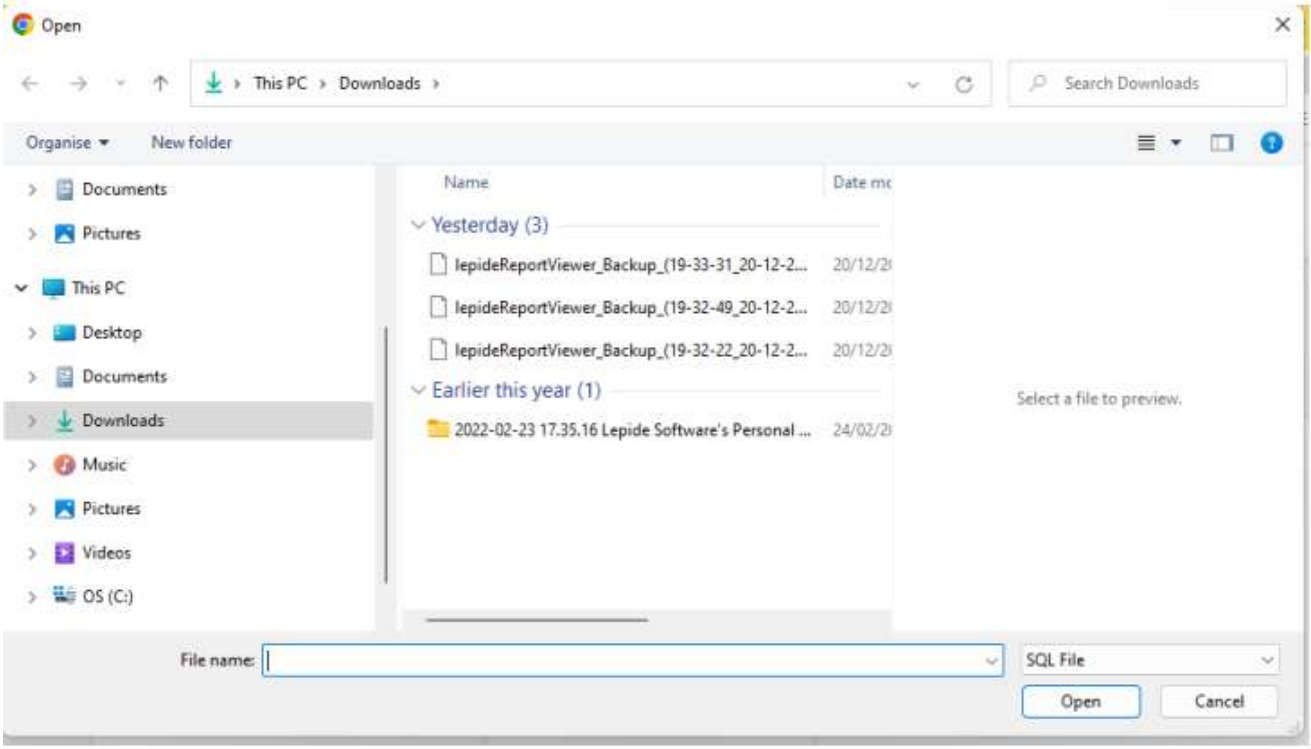
• 从管理控制台屏幕，选择备份和恢复：



• 选择"导入数据库"

• 单击"导入数据库"按钮

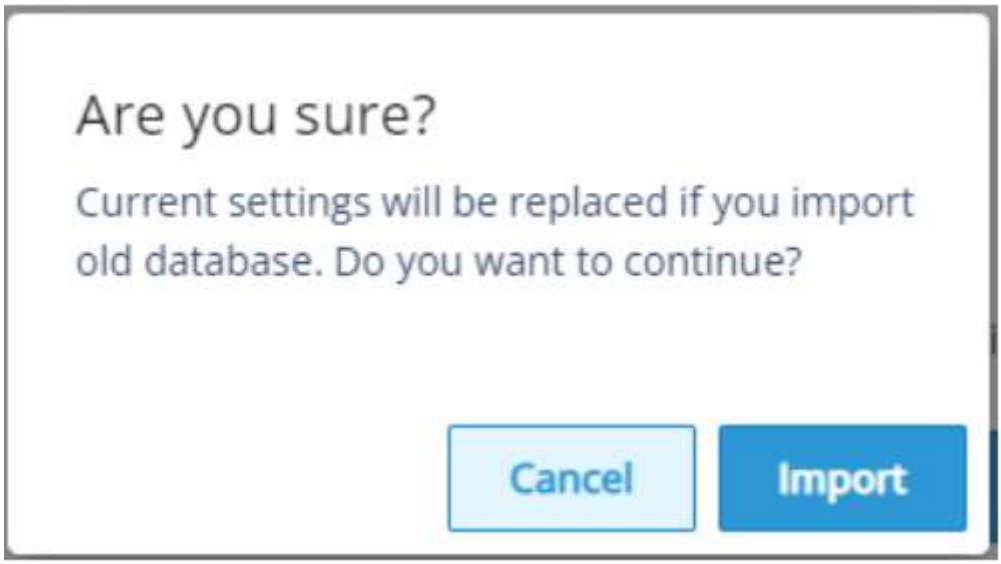
• 出现"下载"文件夹中的文件列表:



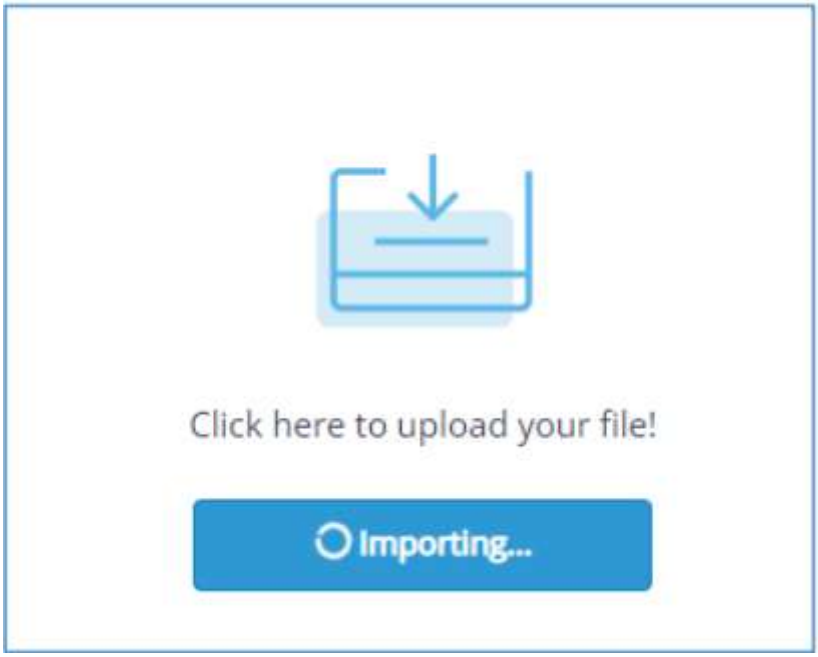
• 选择待导入的数据库文件

• 单击"打开"

• 弹出提示框:



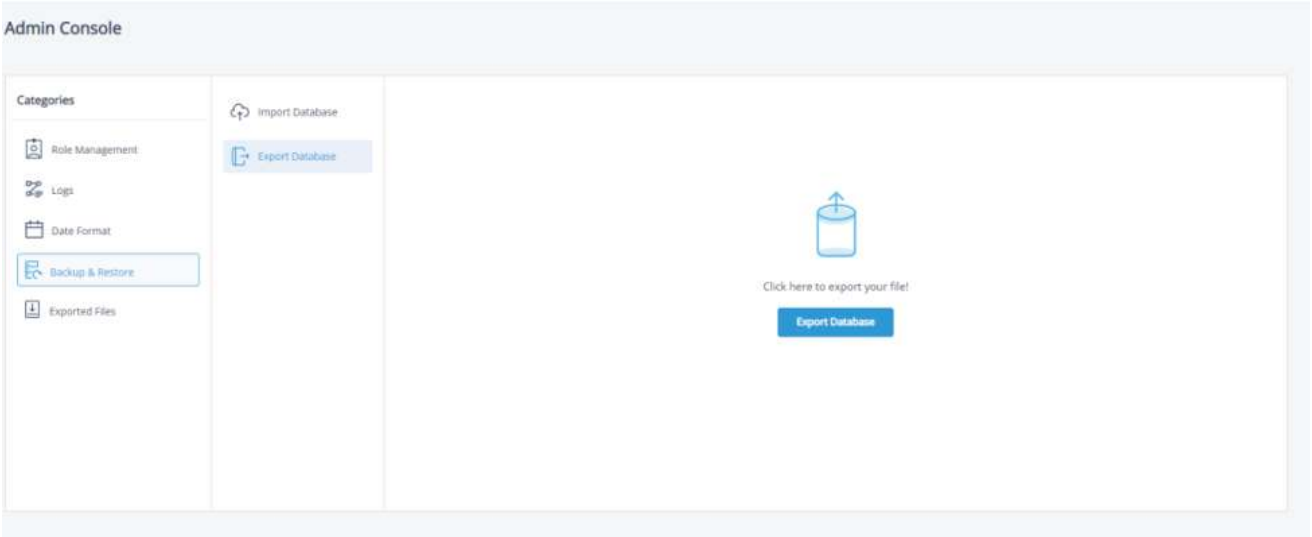
单击"导入"，界面显示如下：



• 导入可能需要一些时间来进行

导出数据库：

• 从管理控制台屏幕，选择导出数据库：



• 单击Export Database按钮

• 屏幕顶部将显示Loading•导出可能需要一些时间。

• 当它完成后，您将在下载文件夹中看到一个SQL文件。这将以' lepideReportViewer_Backup '开始，并将是一个SQL文件类型。

例如：lepideReportViewer_Backup_(19-00-02_21-12-2022)

• 导入数据库时可选择该文件

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 - 23/09/10

联系我们　获取更多资料　haocst.com