Lepide活动目录高级配置指南

概述

Lepide数据安全平台提供了一种全面的方式来提供跨Active Directory、组策略、Exchange on-premises、Microsoft Office 365、SharePoint、SQL Server、Windows File Server、NetApp Filer以及每个可以提供与syslog和RestAPI集成的平台的可见性。

本指南将带您完成Active Directory的Lepide数据安全平台的高级配置过程。有关安装的信息，请参阅我们的安装和先决条件指南。

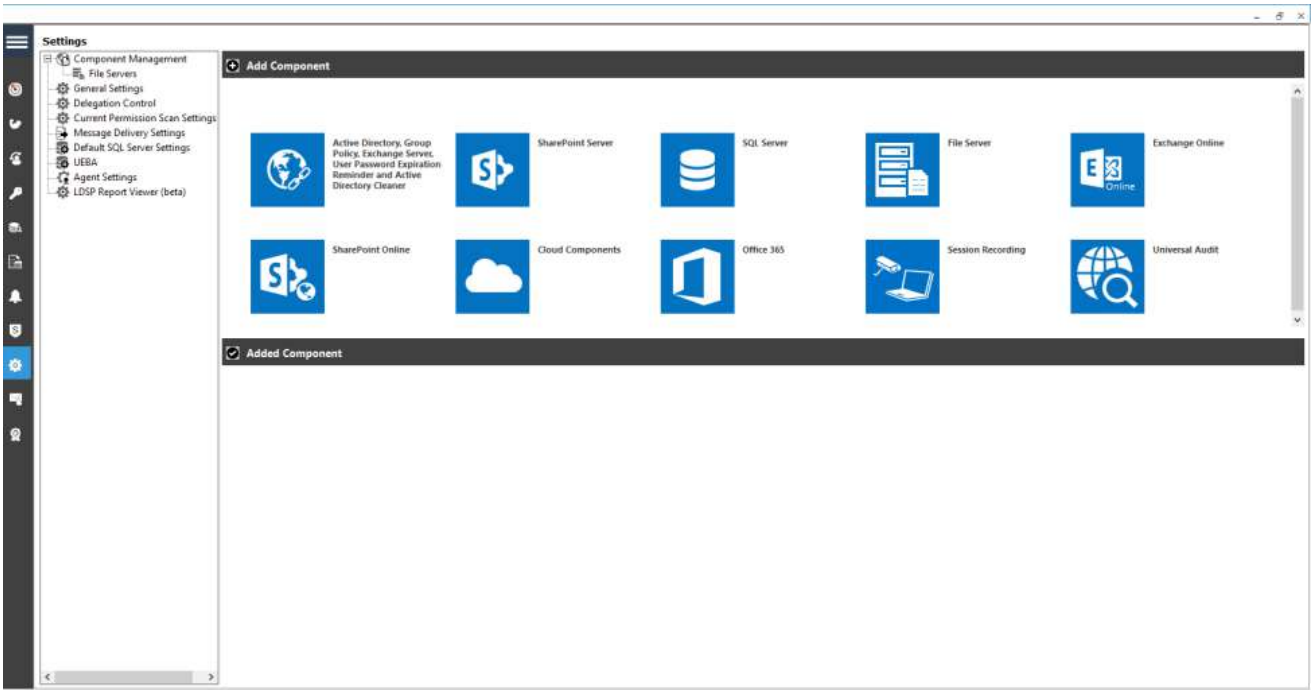
有关标准配置和先决条件的信息，请参阅Active Directory快速入门指南。

如果您在此过程中有任何问题，您可以联系我们的支持团队。联系方式列在本文档的最后。

添加具有高级配置的Active Directory组件

本指南将介绍如何使用高级配置将Active Directory、组策略和Exchange Server组件添加到解决方案。

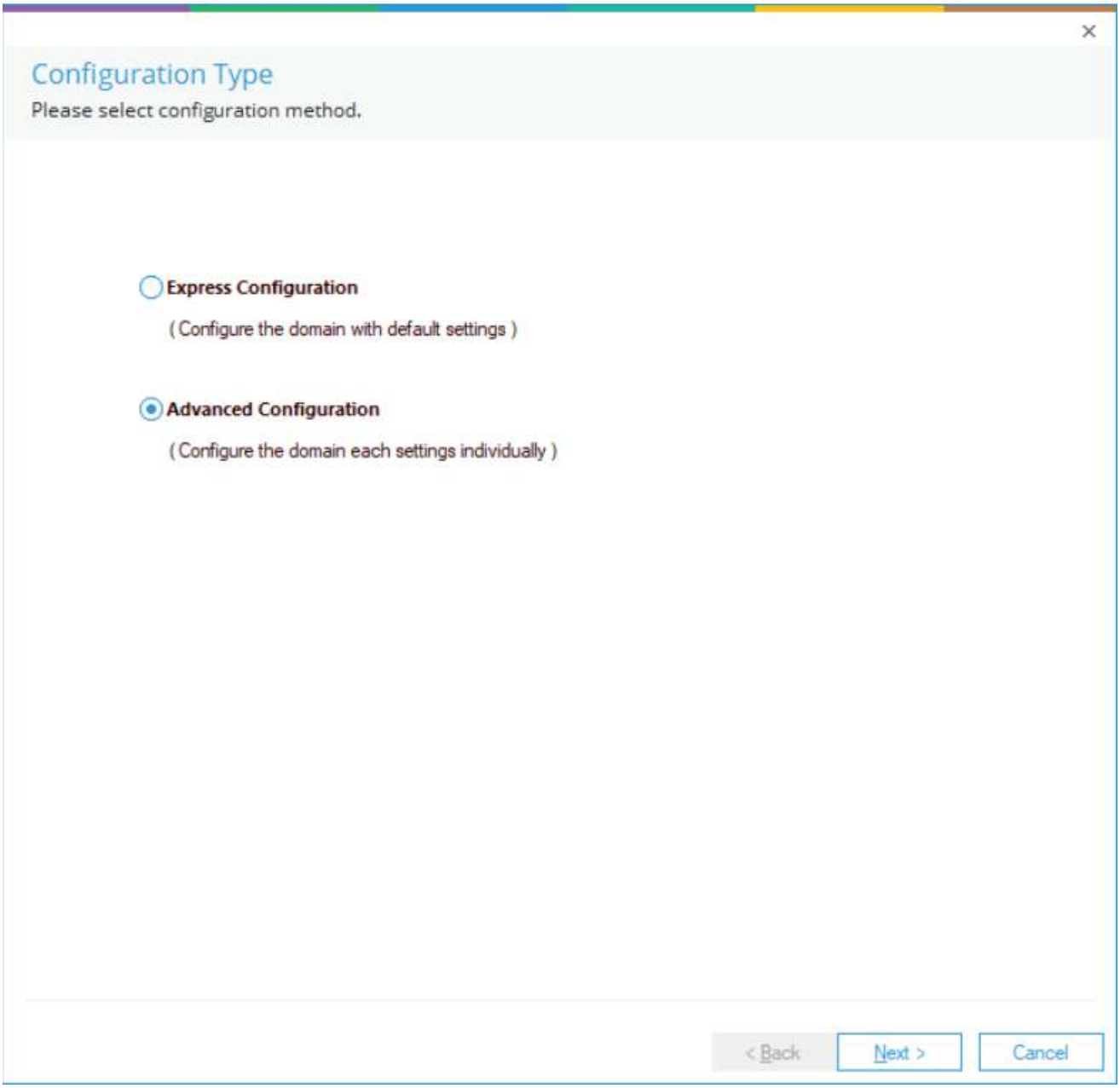
注意：在继续之前，请确保满足审计域的先决条件。



在"组件管理"窗口中，单击"活动目录、组策略和交换"图标，将此组件添加到解决方案中。

向导将从两个可用于添加组件的配置选项开始。它们是：

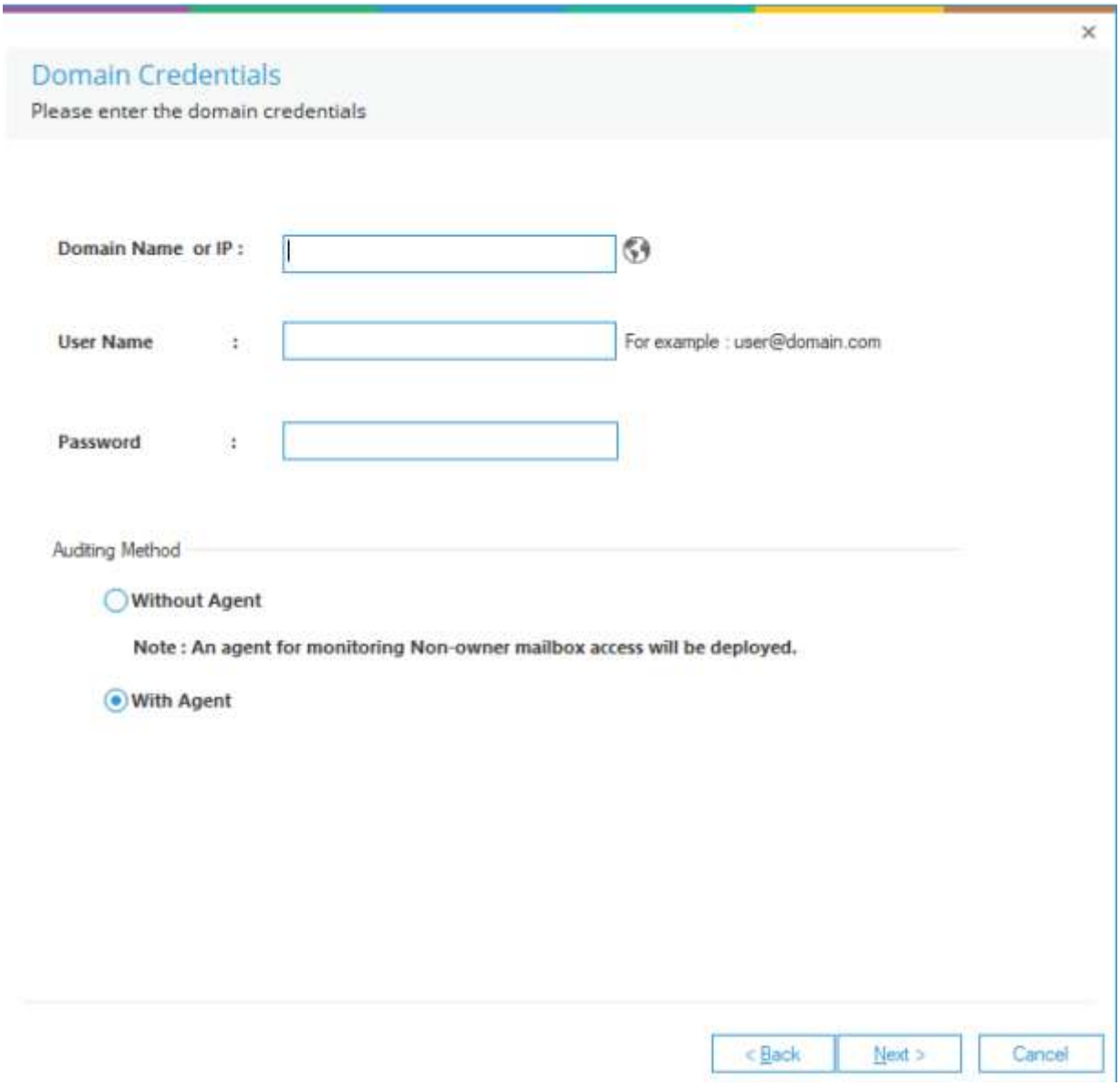
1. Express Configuration：添加具有最小推荐设置的组件。
2. Advanced Configuration：添加具有可定制高级设置的组件。



选择"Advanced Configuration"，单击"Next"。这将使您进入"域凭据"对话框。

域凭据

在本节中，您将提供要添加的组件的详细信息。



1. "Domain Name or IP"：输入域名或IP地址。单击，让解决方案发现安装它的当前域。这将自动填充文本框中的域名。
2. User name：输入用户名，格式为Username@domain.com。确保您提供了完整的用户名和域名。
3. Password：输入所选用户的正确密码。
4. Auditing Method

   •无代理:采用这种方法。不需要在域控制器上安装代理。

   通过与域控制器的实时连接，审计将完全无代理地完成。最小权限配置需要使用这种方法，因为不能使用最小权限帐户安装代理。

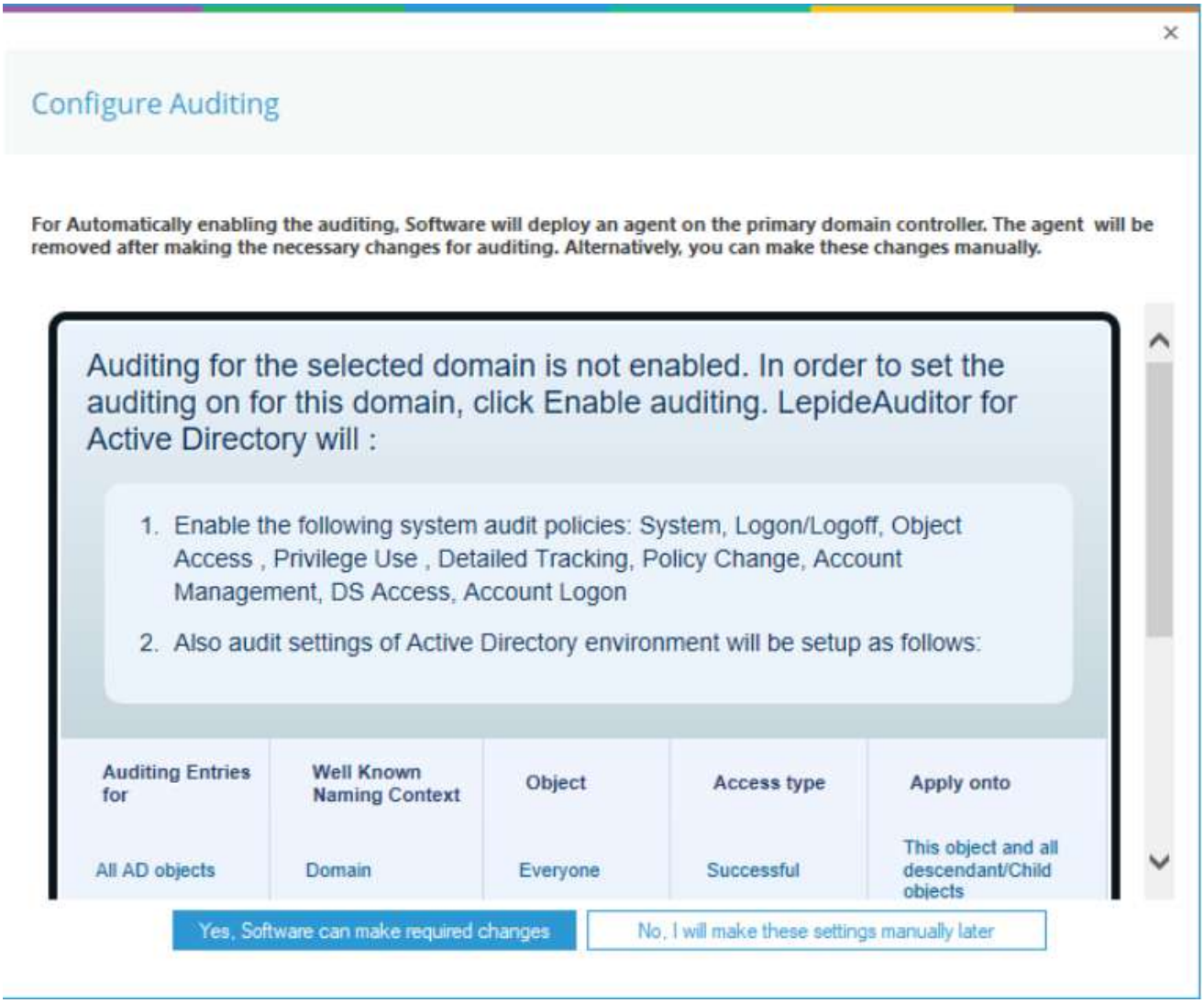
注意：如果您使用最少权限进行配置，请选择无代理。

•With Agent:以下场景推荐使用"With Agent"方式：

域控制器位于不同地理位置，网络连接较慢。
当数据中心的事件日志保留容量小于1GB时。

在提供了域凭据对话框的所有详细信息后，单击Next。

如果默认情况下未在域级别启用本机审计，则会出现以下对话框：

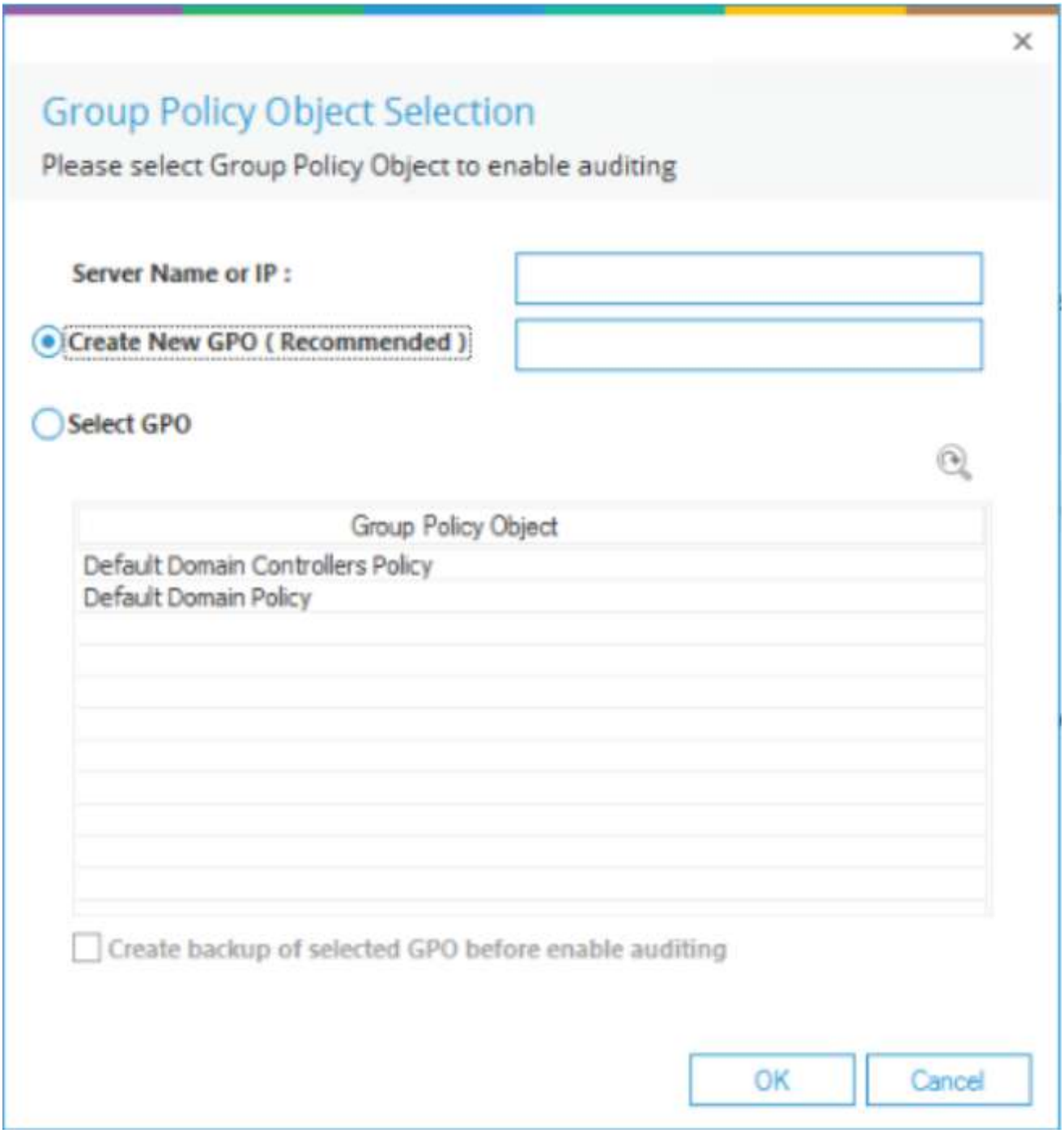


用户帐户至少需要Schema Admin权限才能自动启用审计。您可以暂时将用户帐户的权限提升到Schema Admins，然后单击Yes，以自动启用审计。

或者您也可以单击No，如果您希望稍后在我们的Enable Auditing manually Guide的帮助下手动执行此操作。

单击Yes, Software可以进行所需的更改（仅当用户帐户的权限提升到Schema Admins时）。

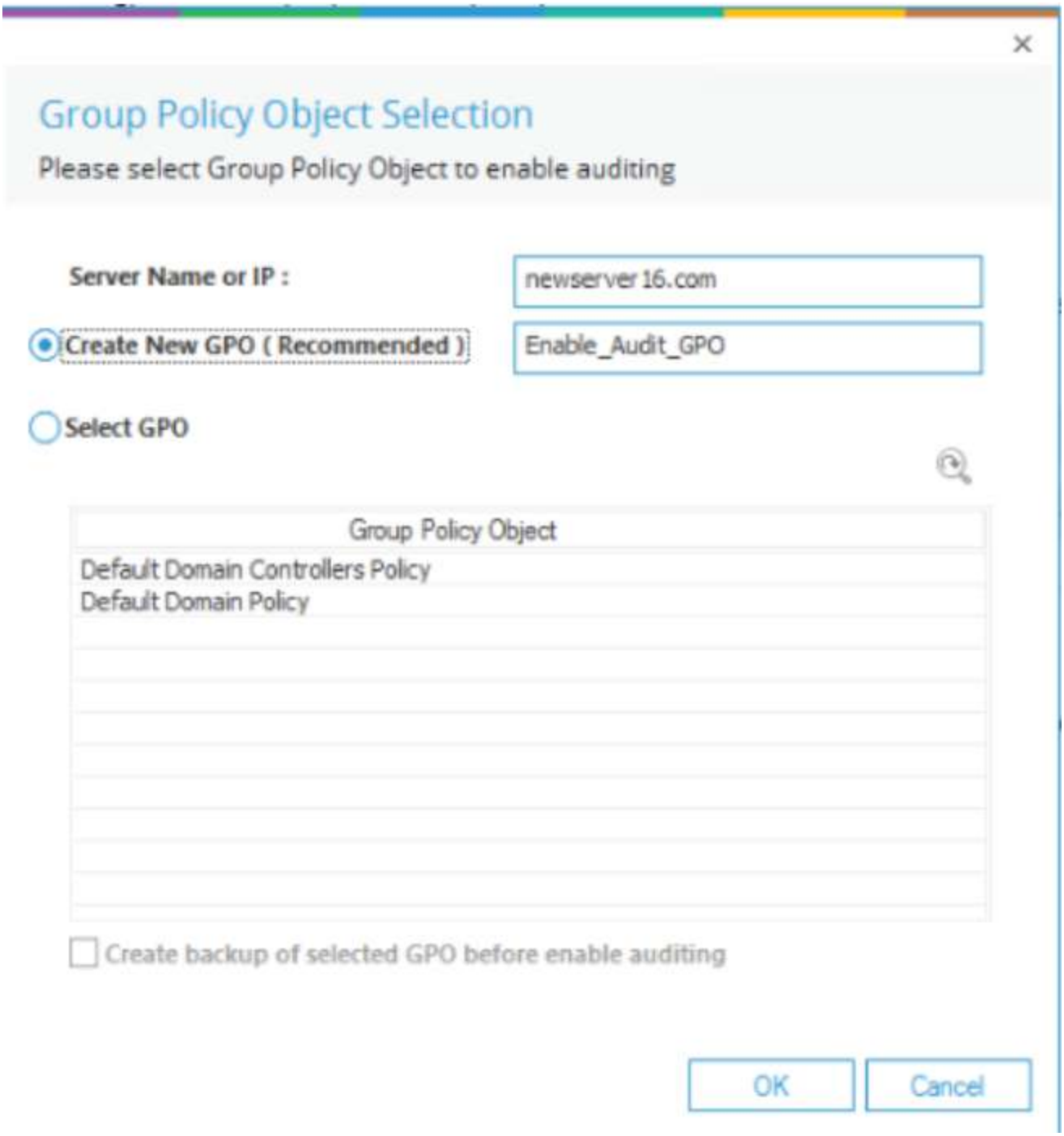
系统弹出如下对话框：

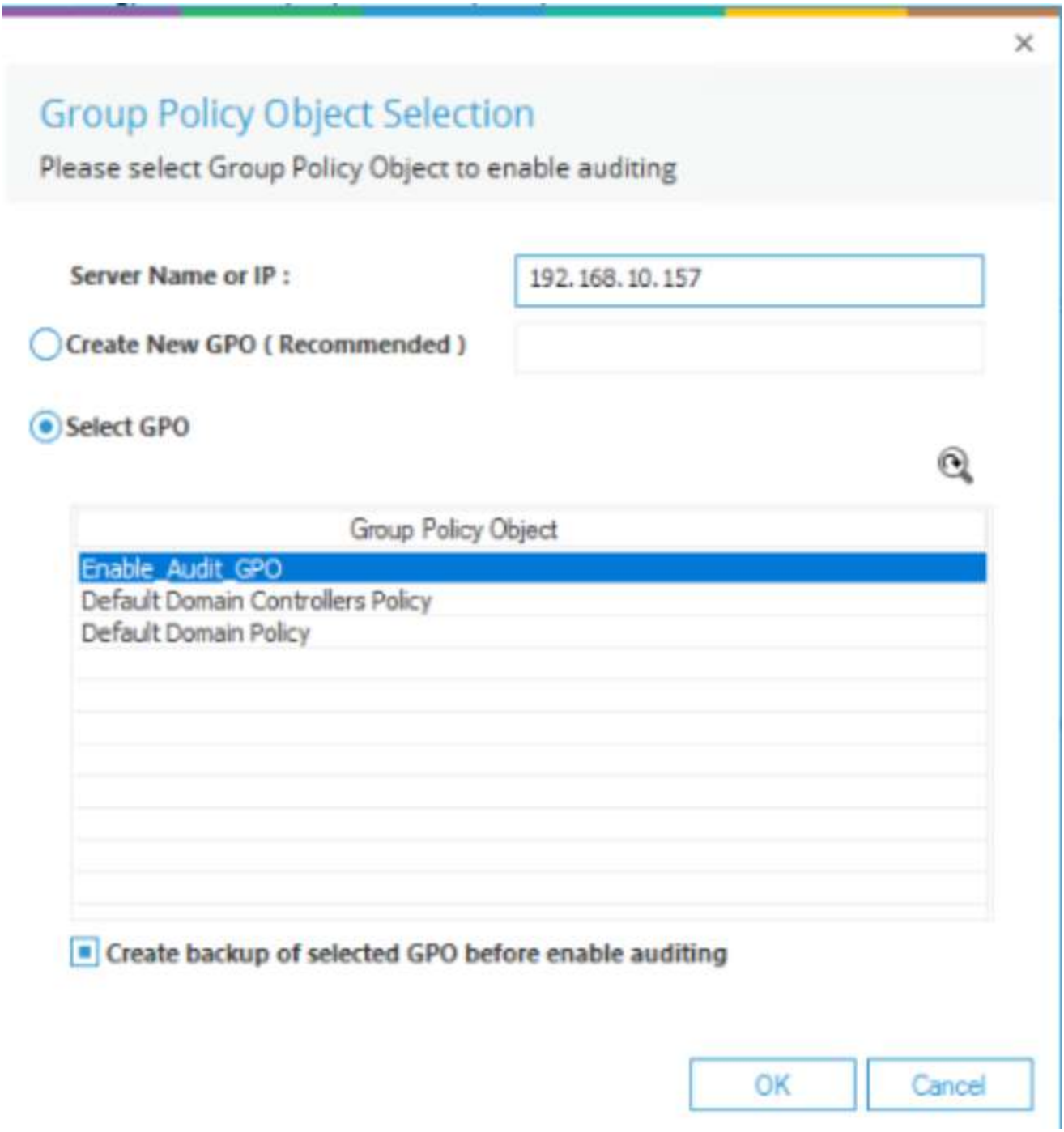


"服务器名称或IP"：输入任意一个域控制器的"IP地址"或"名称"(PDC优先)，然后选择以下任意选项：

• 创建新GPO(推荐)：选择该选项，创建一个新的组策略对象。选中后，您需要提供要创建的新组策略的名称。单击OK，在域中创建新的组策略以启用审计。

• 选择GPO：该选项允许您选择一个组策略对象来启用审计。选择此选项以启用相邻部分。

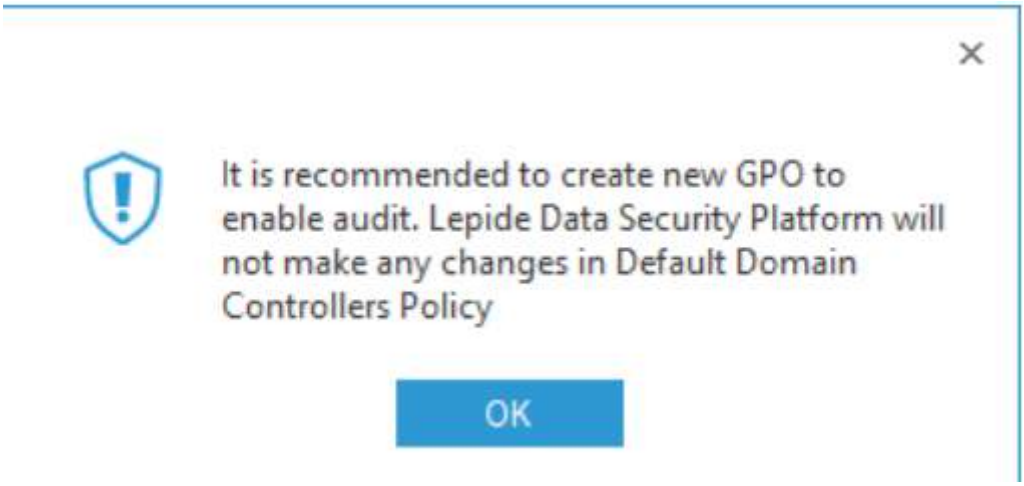

Group Policy Object Selection
Please select Group Policy Object to enable auditing
Server Name or IP :
newserver16.com
Create New GPO (Recommended)
Enable_Audit_GPO
Select GPO
Group Policy Object
Default Domain Controllers Policy
Default Domain Policy
Create backup of selected GPO before enable auditing
OK
Cancel



执行以下步骤选择已存在的组策略。

a. 如果此处未列出组策略，可单击，重新扫描域以获取更新的组策略集。

b. 使用Lepide数据安全平台时，不能选择"默认域控制器组策略"或"默认域组策略"开启审计。如果您尝试这样做，屏幕上将出现以下错误信息：



c. 选择在域级别或域控制器级别创建的需要应用审计设置的自定义组策略。

d. 如果对已存在的组策略启用审计，请确保勾选"在启用审计之前创建所选组策略对象的备份"复选框。如果启用审计后仍然存在任何问题，此备份允许您恢复以前的默认域控制器策略。

e. 为避免此类问题，请创建新的域控制器策略以启用审计。

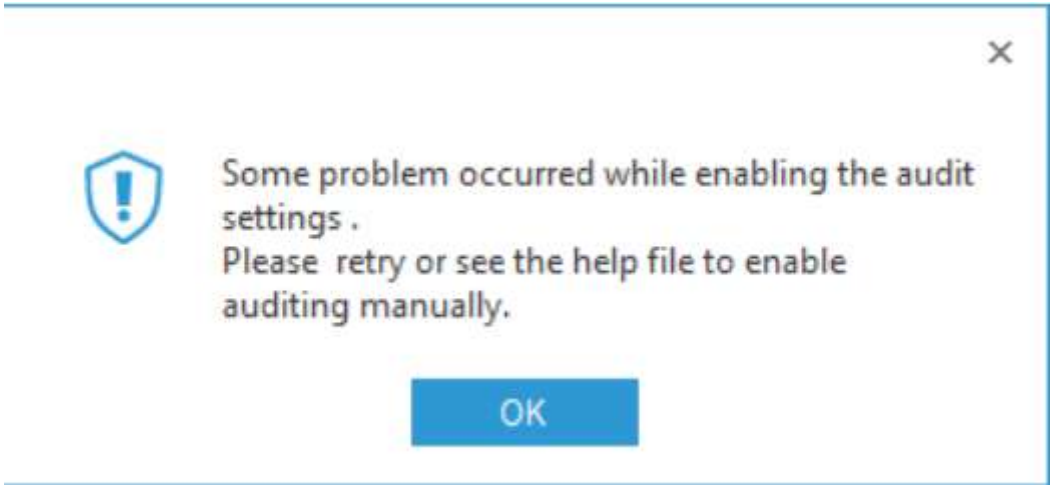
f. 单击"确定"。该软件尝试在服务器上的%systemdrive%\Windows\ Lepide \GPOBKP_24-01-2022 18_13_35\文件夹中启用审计并创建所选组策略的备份。

在这里，24-01-2022将被替换为日期，18_13_35将被替换为单击OK以对所选策略启用审计的时间。

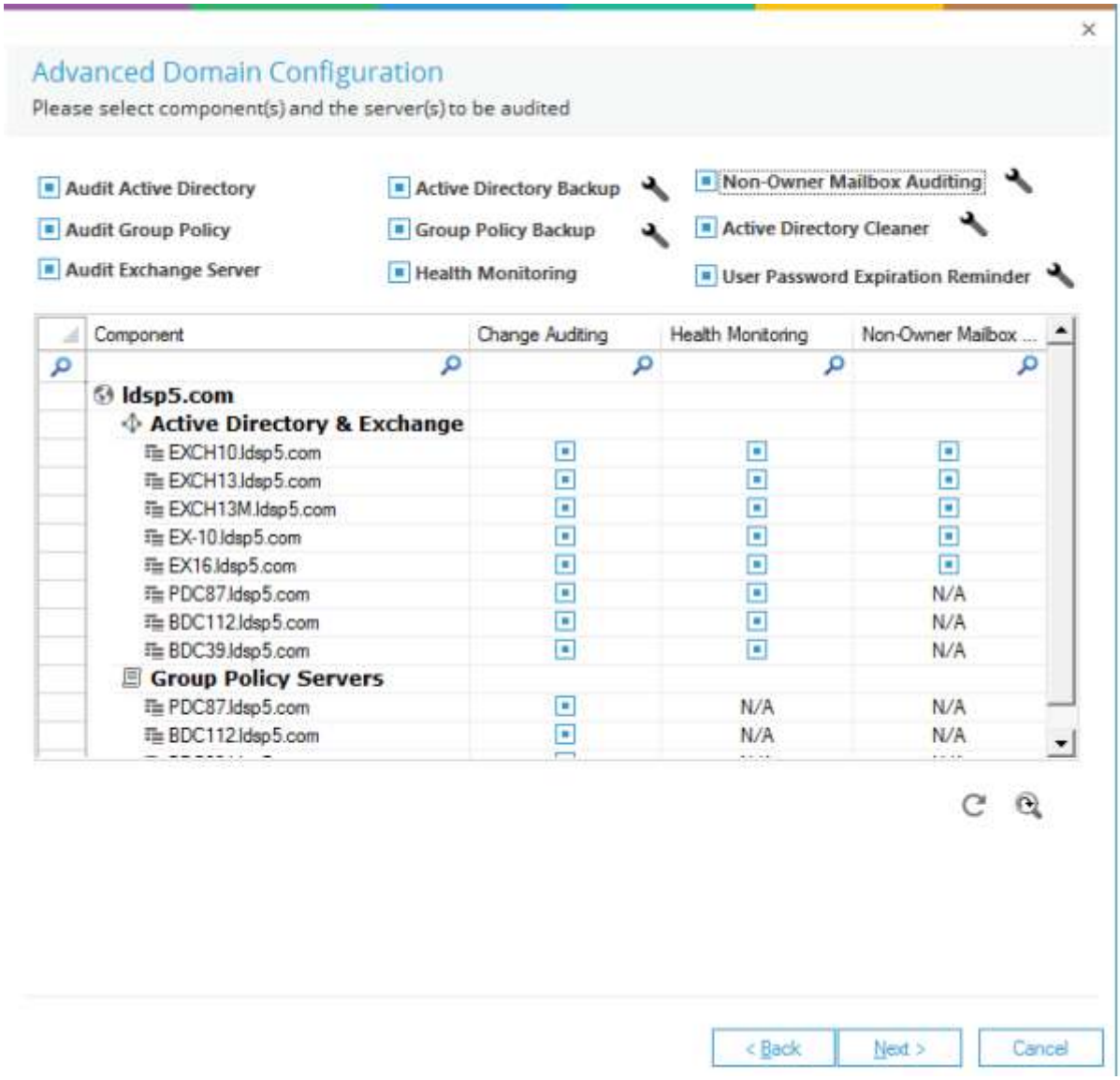
g. 如果将来遇到任何问题，您可以使用此备份将策略恢复到以前的状态。请参考本文档第3.6节恢复组策略。

h. 您需要等待一段时间，直到启用审计。

如果在启用审计时出现问题，您可能会收到以下或其他错误消息：



在出现上述错误或其他问题的情况下，您必须在Windows Server上手动启用审计设置。在这种情况下，请在下一个对话框中选择No，然后继续。有关手动启用审计设置的信息，请参阅"手动启用审计指南"。一旦启用了审计，解决方案将显示配置审计的下一步。



域中的所有域控制器将在此处列出。您可以选择所需的模块：

允许审计

选中或取消选中以下选项以启用或禁用审计、备份快照和运行状况监视。

a. Audit Active Directory:开启/关闭Active Directory审计功能。

b. 审计组策略:开启/关闭对组策略对象的审计。

c. 审计Exchange Server:启用/禁用Exchange On-Premises审计。

d. 非所有者邮箱审计:开启/关闭非所有者、委托用户、管理员和所有者自身的邮箱访问审计。

e. 运行状况监视:启用/禁用Active Directory和Exchange服务器的运行状况监视。

f. Active Directory Backup:启用/关闭备份快照特性，创建Active Directory快照。

g. 组策略备份:启用/关闭备份快照特性，创建组策略对象的快照。

域控制器的选项：

每个域控制器都有以下选项。选中或取消选中这些选项以启用或禁用功能，并为目标域控制器安装或卸载相应的代理。

a. Change Auditing:选中此项，为域控制器启用Change Auditing，并安装相应的代理。在无代理审计模式下不会安装审计代理。

b. 运行状况监视:选中此项以启用Active Directory和Exchange组件的运行状况监视。

c. 非所有者邮箱审计:选中此选项以启用非所有者邮箱访问审计并在所选Exchange服务器上安装代理。

默认情况下，以下选项未选中：

a. Active Directory备份

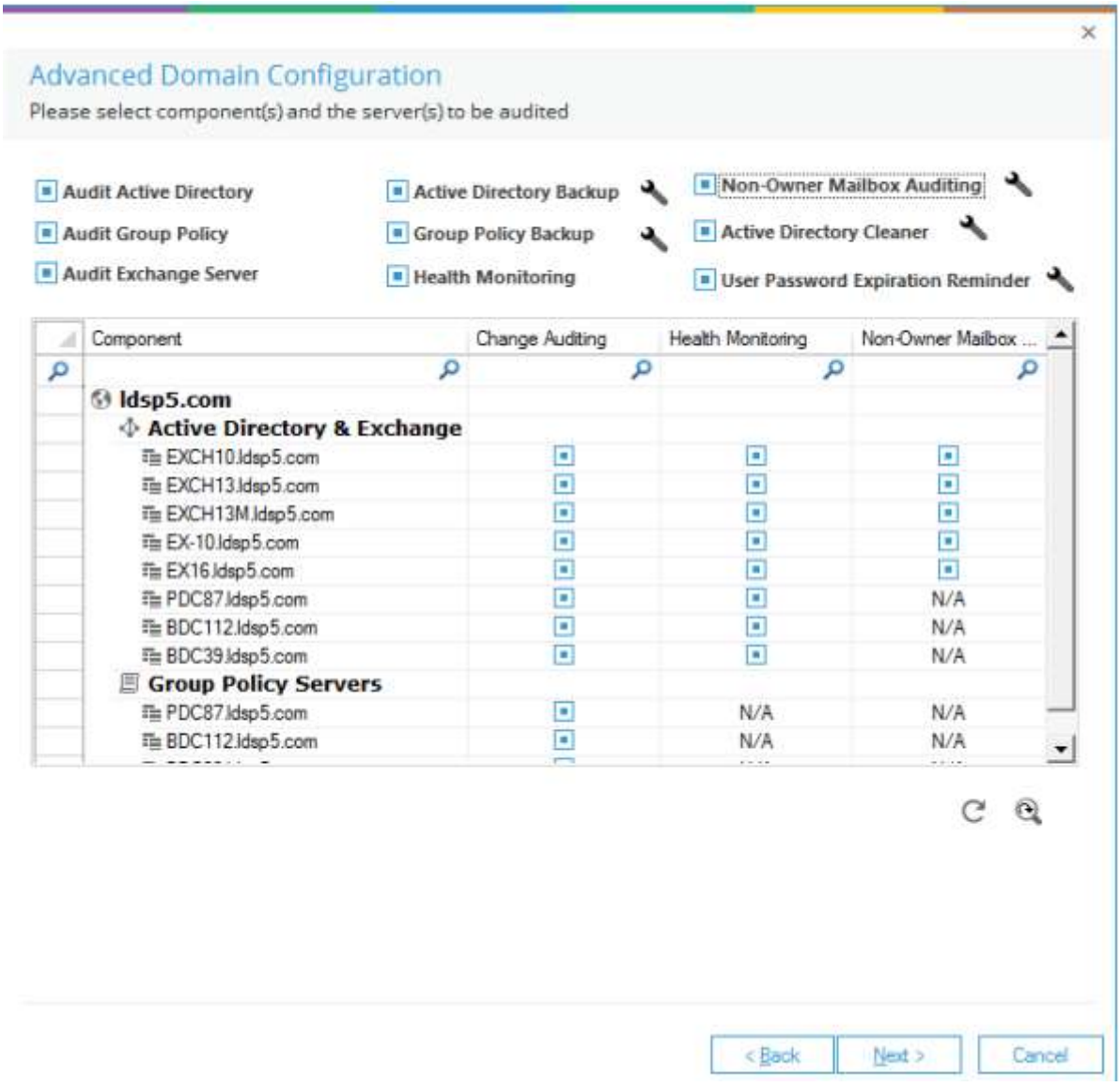
b. 组策略备份

c. 运行状况监控

d. 非所有者邮箱审计

e. Active Directory清洁器

f. 用户密码过期提醒勾选这些选项后才能启用。所有这些选项在这个例子中都被选中了：



其他配置选项：

a. 单击"非所有者邮箱审计"对应的，配置所有者用户和非所有者用户的Exchange邮箱访问审计选项。有关详细信息，请参阅配置邮箱访问审核指南。

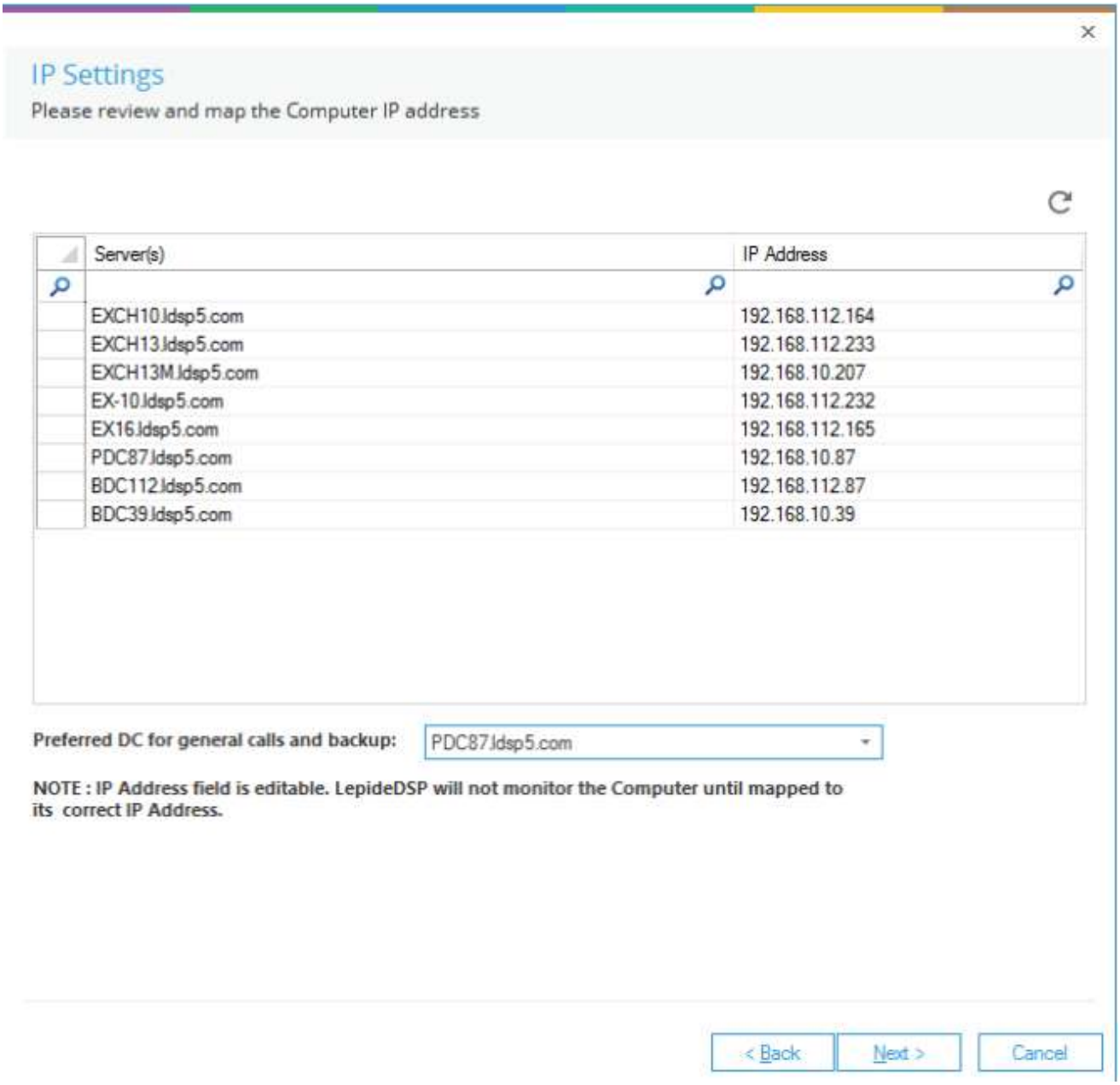
b. 单击"Active Directory Cleaner"对应的，配置其选项。点击查看更多。

c. 单击"用户密码过期提醒"对应的，配置用户密码过期提醒选项。点击查看更多。

d. 单击"Active Directory Backup"对应的，配置Active Directory备份选项。有关进一步信息，请参阅本文档的第3.1节。

e. 单击"下一步"继续。

IP设置



请在此向导中验证解决方案解析的IP地址。

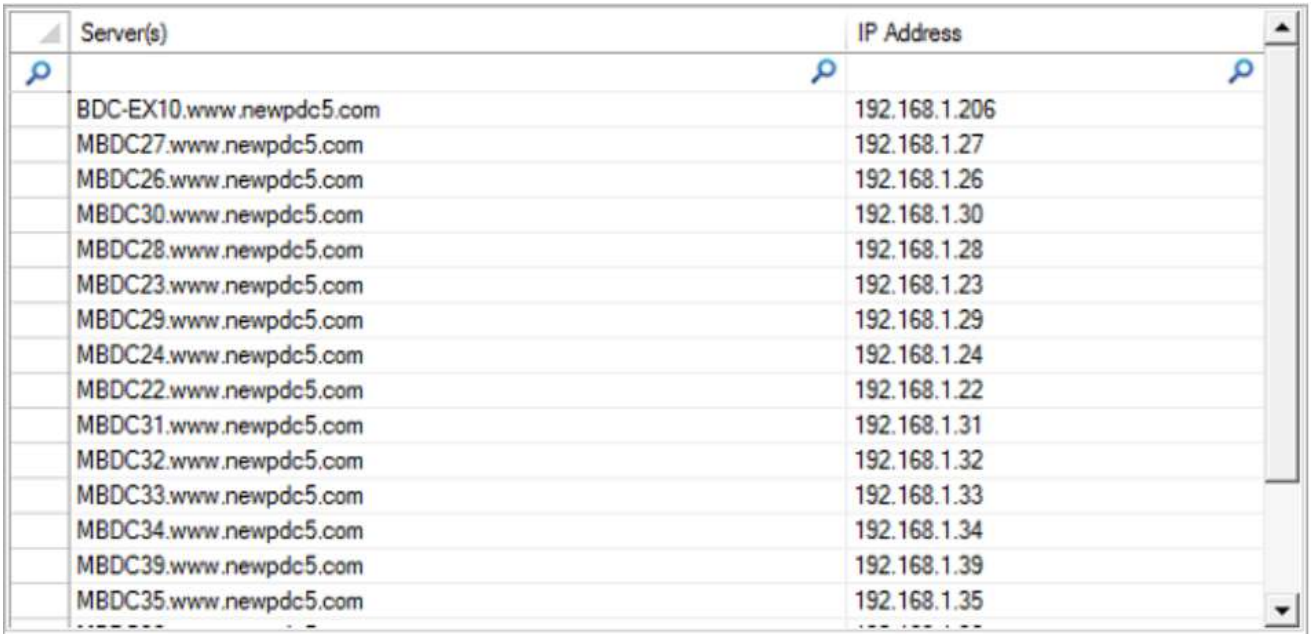
如果该字段为空或IP地址错误，请双击包含IP地址的单元格，使该字段可编辑。输入正确的IP地址，按"Enter"。

您可以单击该图标来恢复此步骤的默认选项。

您还可以选择首选域控制器，备份快照相关的调用将发送到首选域控制器。所选的域控制器应该位于应用程序服务器附近，以便可以首先执行与这些调用相关的操作。您也可以选择相对空闲或负载较小的域控制器。

如果有一个很长的域控制器列表，那么您可以使用顶部过滤行来筛选需要修改的域控制器。

示例如下：

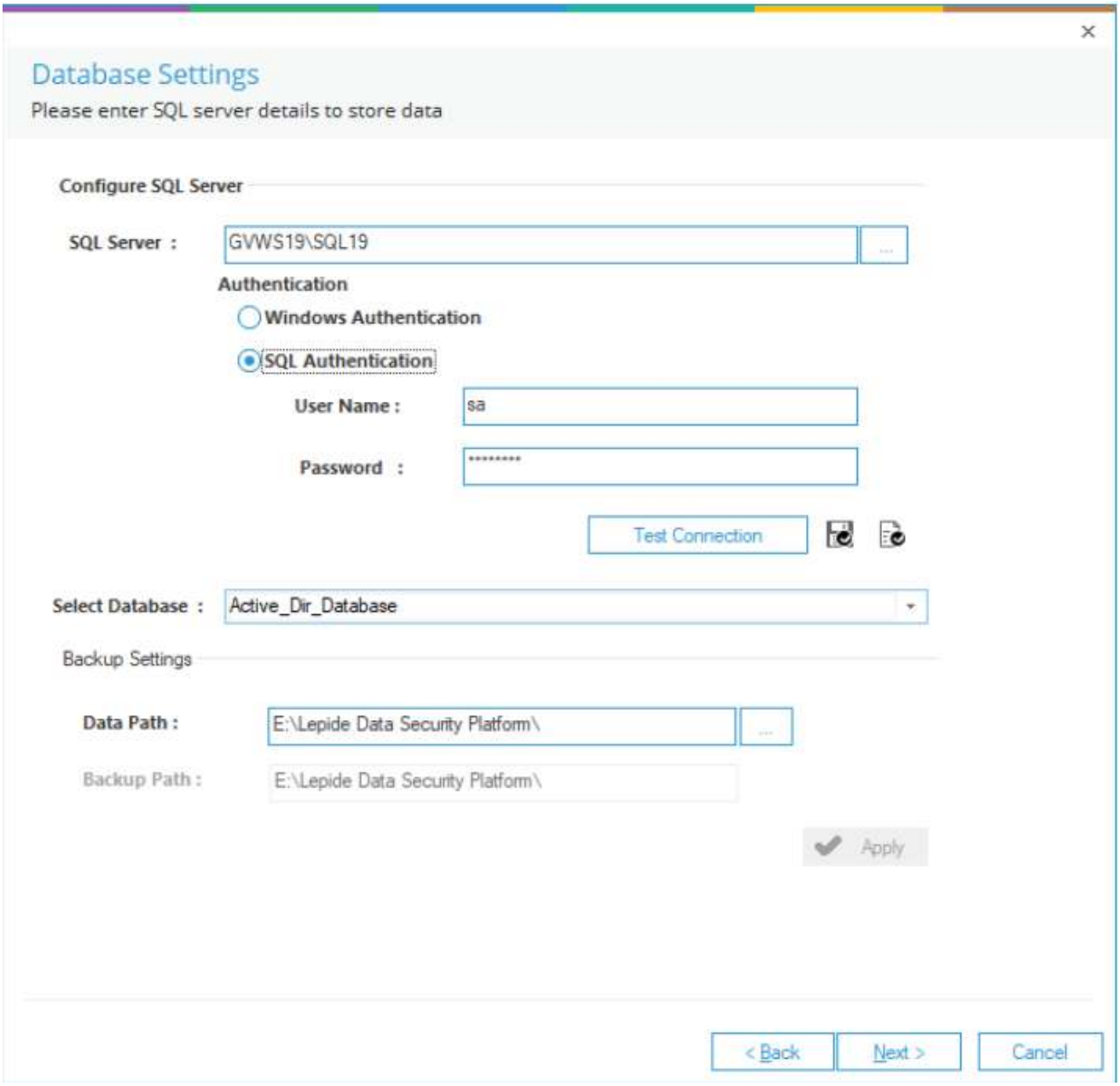


Server(s)	IP Address
BDC-EX10.www.newpdc5.com	192.168.1.206
MBDC27.www.newpdc5.com	192.168.1.27
MBDC26.www.newpdc5.com	192.168.1.26
MBDC30.www.newpdc5.com	192.168.1.30
MBDC28.www.newpdc5.com	192.168.1.28
MBDC23.www.newpdc5.com	192.168.1.23
MBDC29.www.newpdc5.com	192.168.1.29
MBDC24.www.newpdc5.com	192.168.1.24
MBDC22.www.newpdc5.com	192.168.1.22
MBDC31.www.newpdc5.com	192.168.1.31
MBDC32.www.newpdc5.com	192.168.1.32
MBDC33.www.newpdc5.com	192.168.1.33
MBDC34.www.newpdc5.com	192.168.1.34
MBDC39.www.newpdc5.com	192.168.1.39
MBDC35.www.newpdc5.com	192.168.1.35

完成后，单击Next继续。

数据库设置

在此步骤中，您需要提供将用于存储审计数据的SQL Server和数据库的详细信息。该解决方案允许您连接到本地托管或网络SQL Server。



提供SQL Server用户名和密码，以允许解决方案使用这些凭据访问SQL。

注意：此处选择的用户在SQL Server中应该具有dbcreator角色。

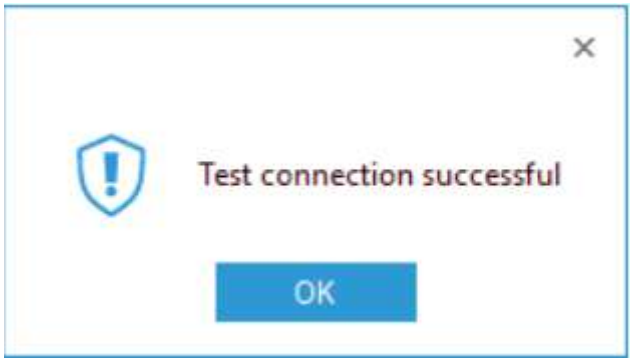
提供数据库名称，leide数据安全平台将在其中存储审计日志。

如果您是第一次使用该解决方案，您可以为解决方案将创建的新数据库提供一个名称。在重新安装的情况下，您可以使用解决方案先前创建的数据库。

必须测试解决方案与所选SQL Server之间的连接。这有助于验证数据库连接。

单击"测试连接"。

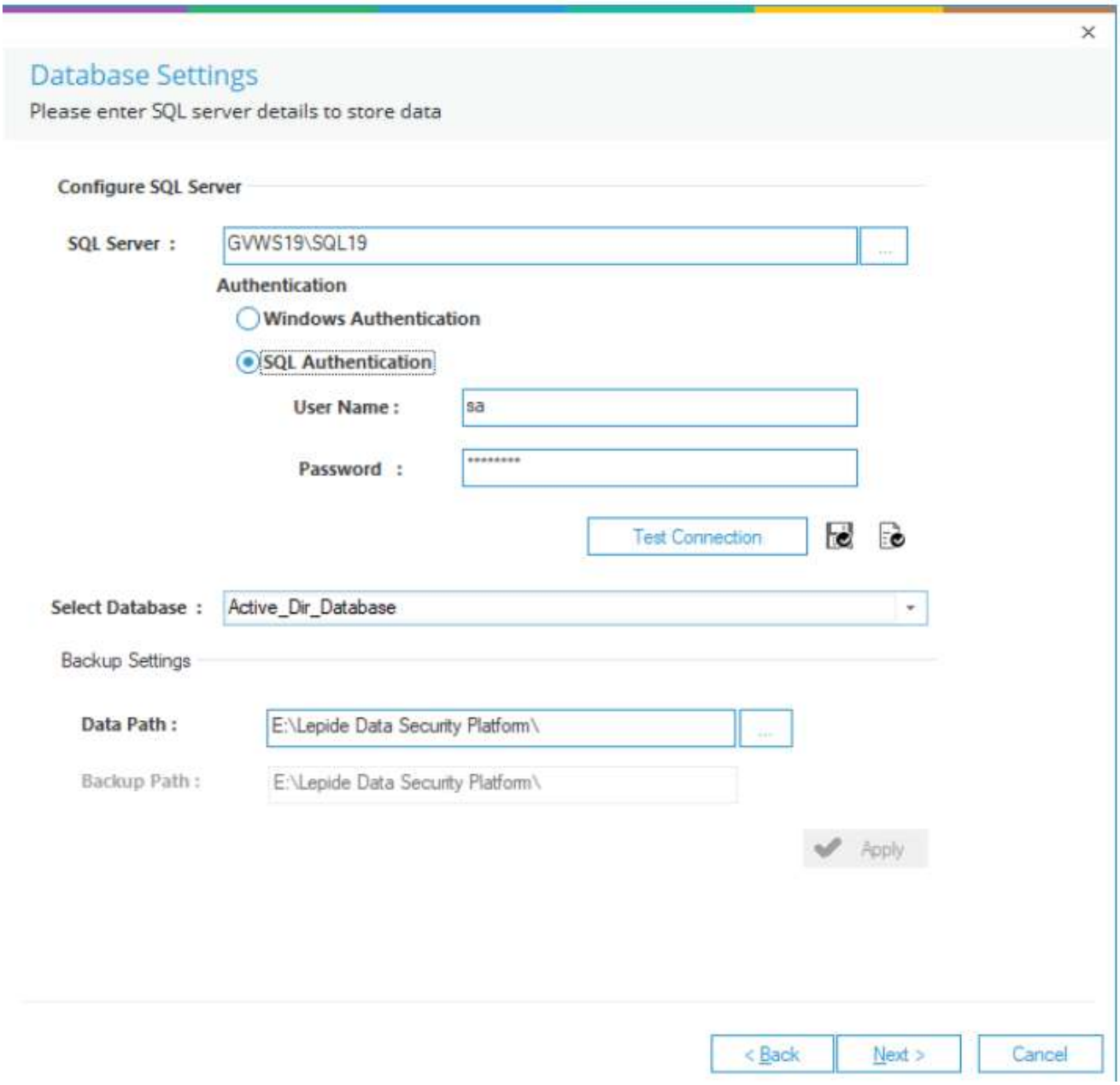
如果连接失败，它将显示一个错误，或者显示以下消息，确认连接成功。



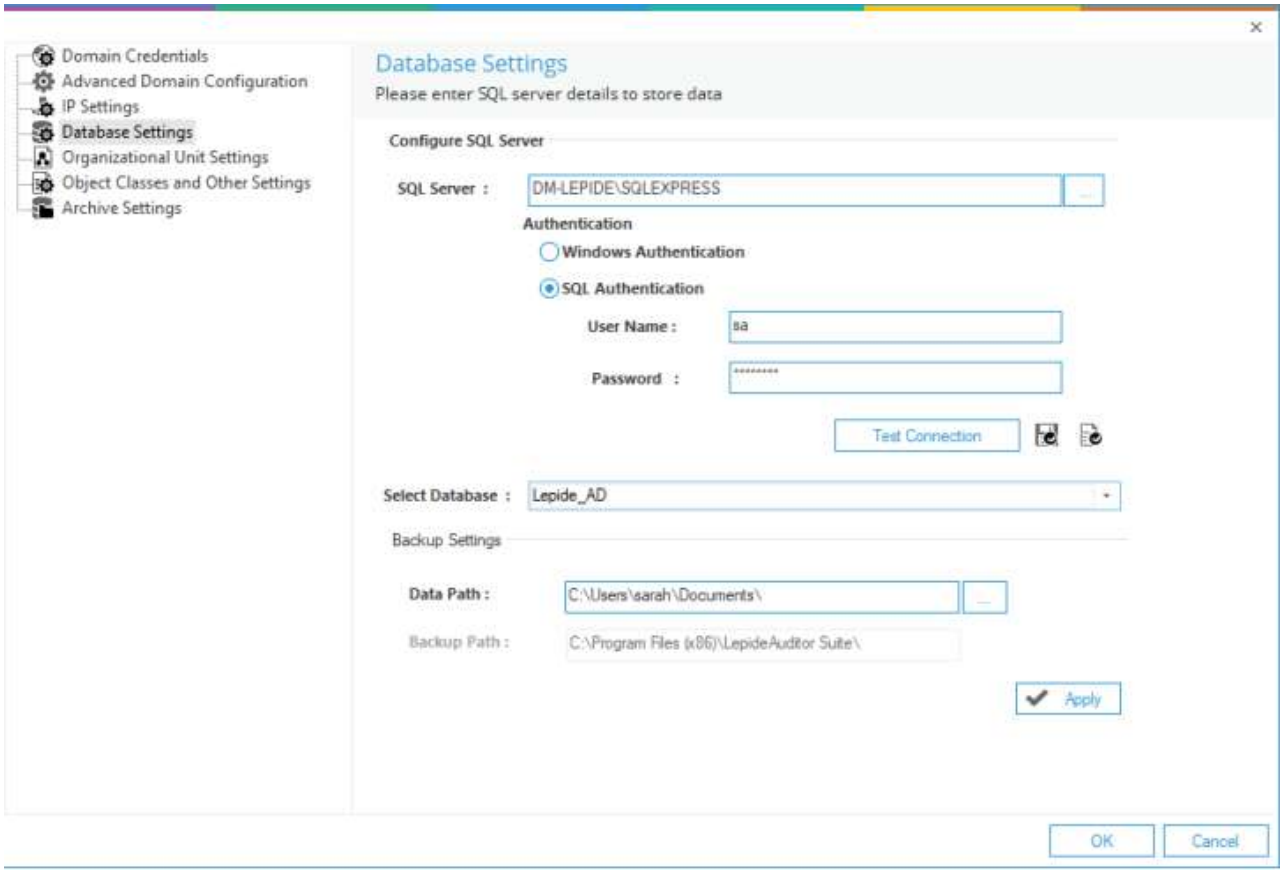
移动备份快照数据

"参考备份"路径和"完全备份"路径都可以修改。如果要修改它们的路径，那么可以使用Move Data实用程序将备份从以前的位置移动到新位置。

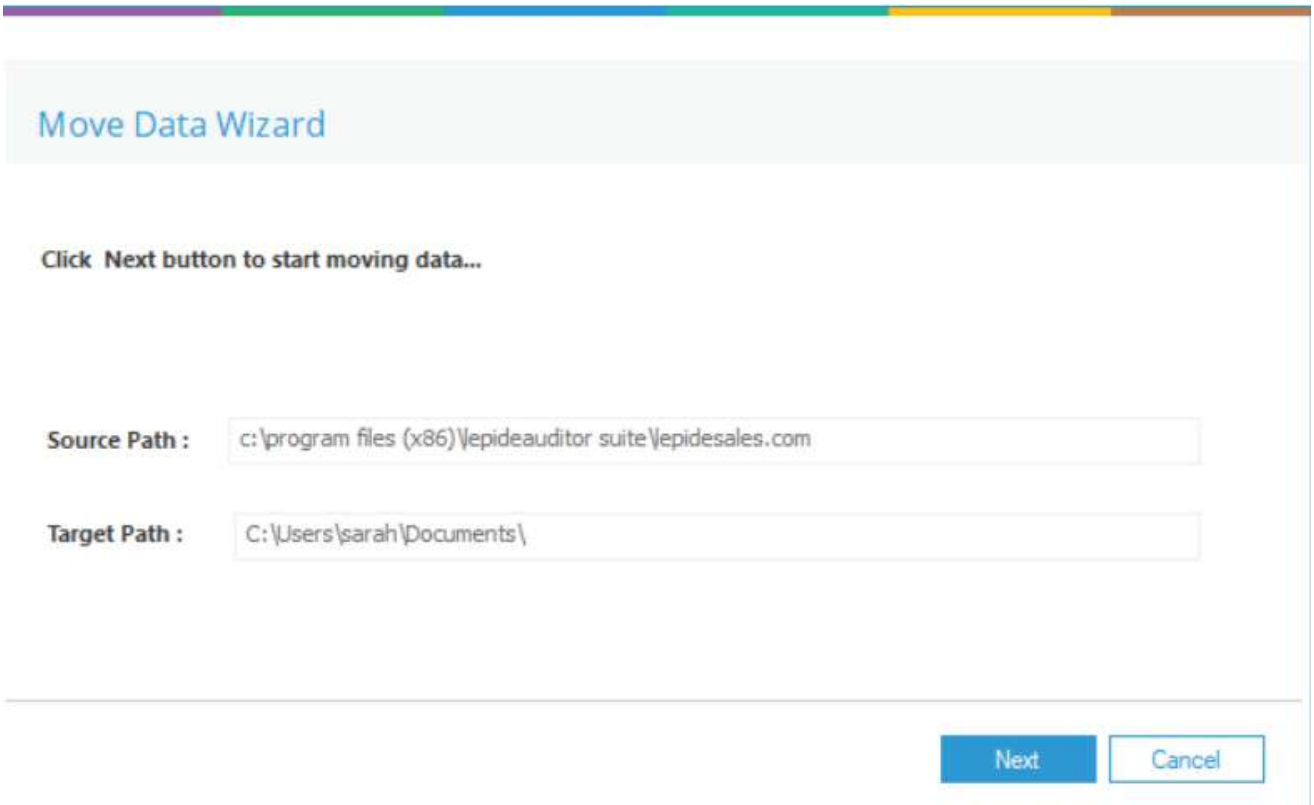
按照以下步骤修改参考备份或完整备份的路径。



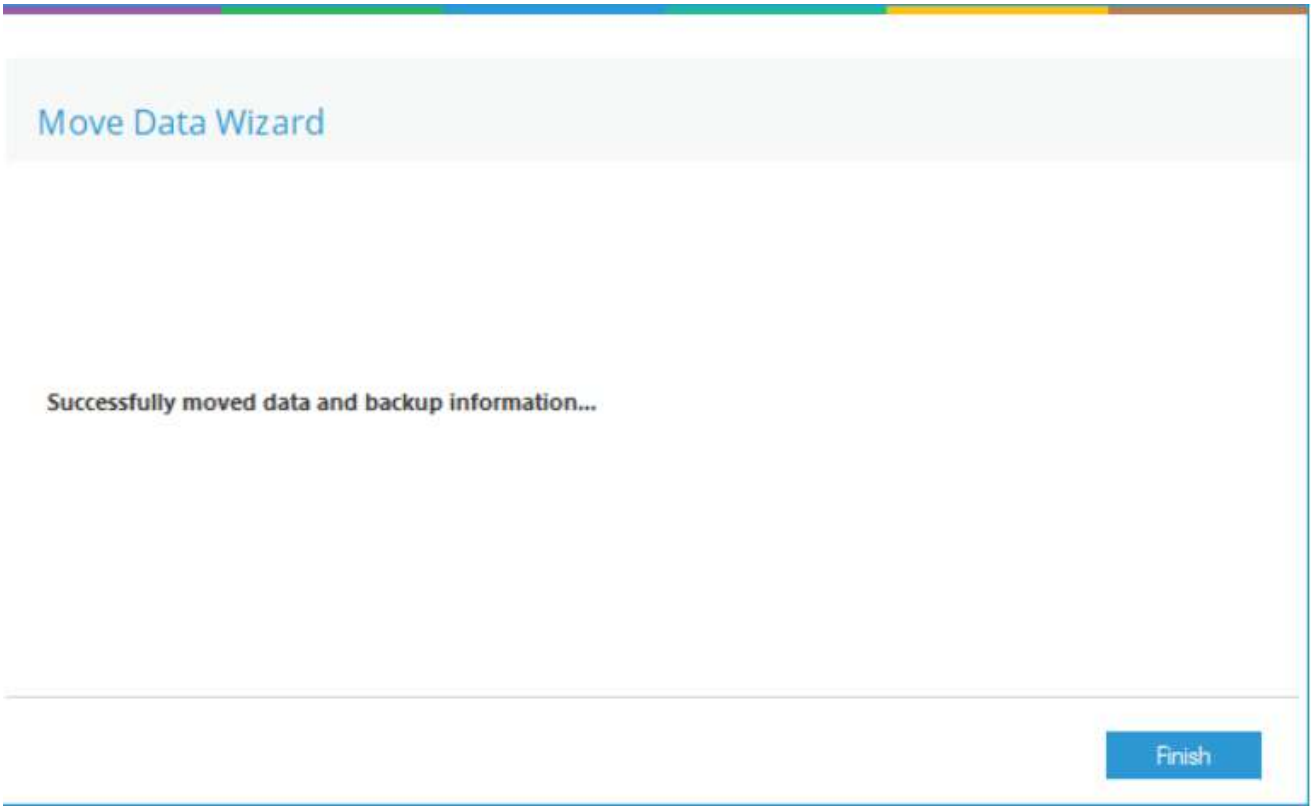
1. 在"数据库设置"对话框中，单击图标（在"备份设置"下）以访问以下对话框，选择用于保存Active Directory或组策略备份的新文件夹；
2. 选择一个文件夹并单击OK。您将返回数据库设置对话框，该对话框现在显示数据路径框中新选择的文件夹。



3. 单击Apply。这将启动移动数据向导，该向导提供将备份数据从旧位置移动到新选择位置的步骤。



4. 单击Next。它开始移动数据。成功移动备份数据后，屏幕上会出现以下消息框：

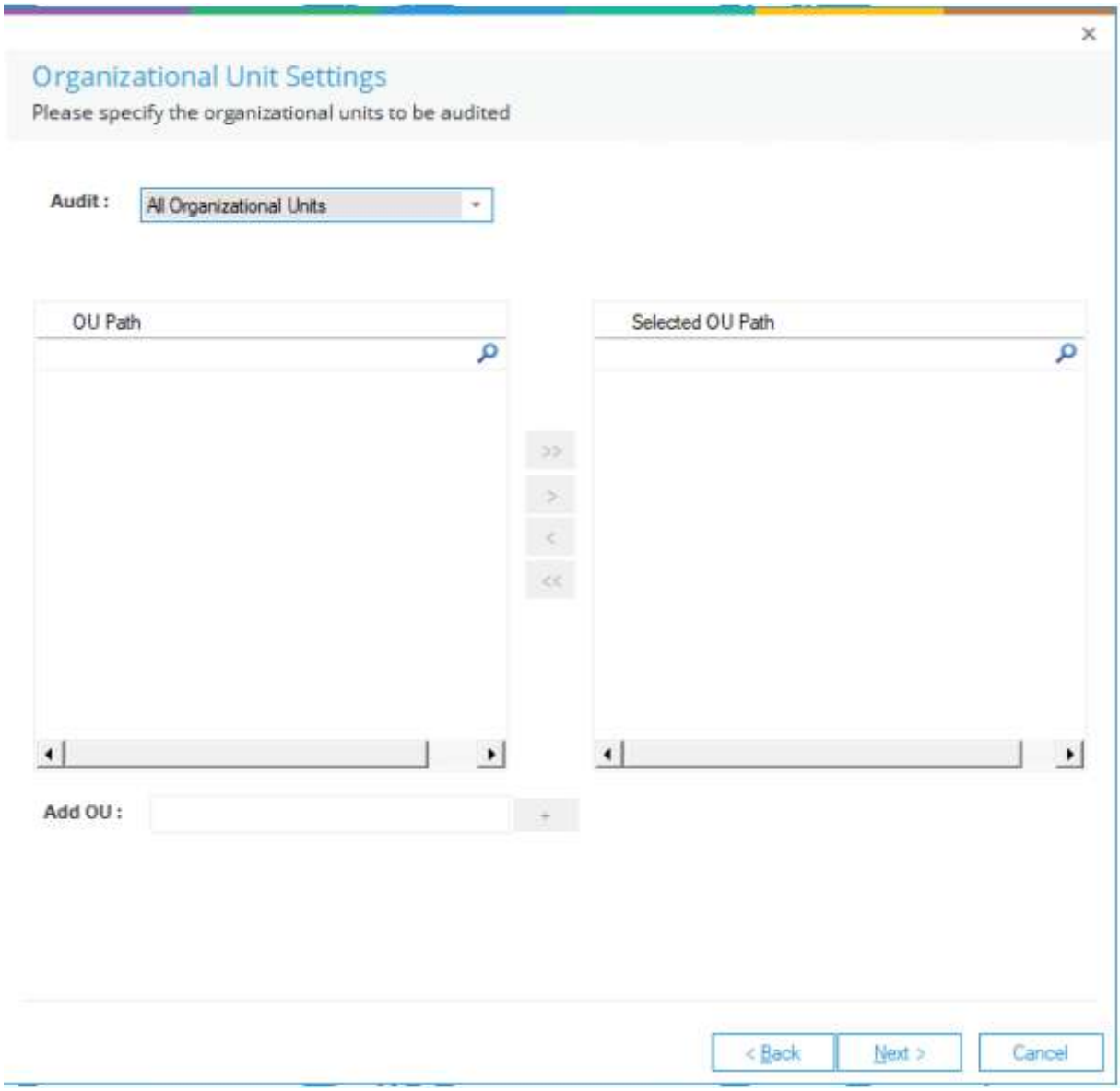


5. 单击Finish关闭向导。它将带您回到"数据库设置"对话框。

6. 单击OK。

组织单位设置

在此步骤中，您可以选择希望审核的组织单位。



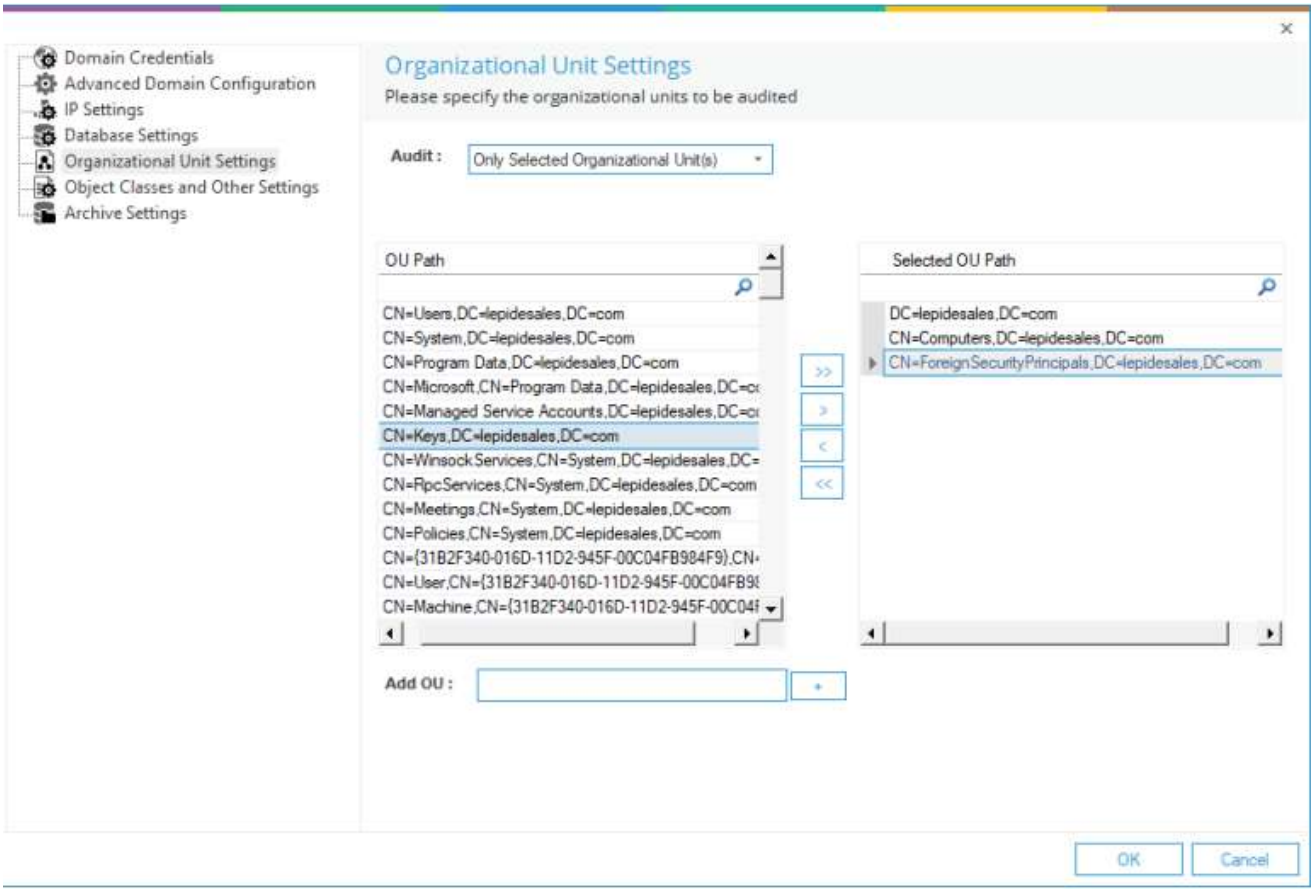
在"审计"下拉菜单中选择以下选项:

• 所有组织单位：选中该选项，对所有组织单位进行审计。默认情况下，选中"审计所有组织单位"选项。如果希望审核所有组织单位，请单击"下一步"继续。

• 仅选定组织单位：选择此选项可使解决方案指向审计特定的组织单位（OU），而不是域中的所有组织单位（OU）。从列表中选择组织单位，然后将它们移动到右侧，然后按Next。

如果需要手动添加组织单位，请在"添加OU"框中输入新建的组织单位名称，单击按钮。

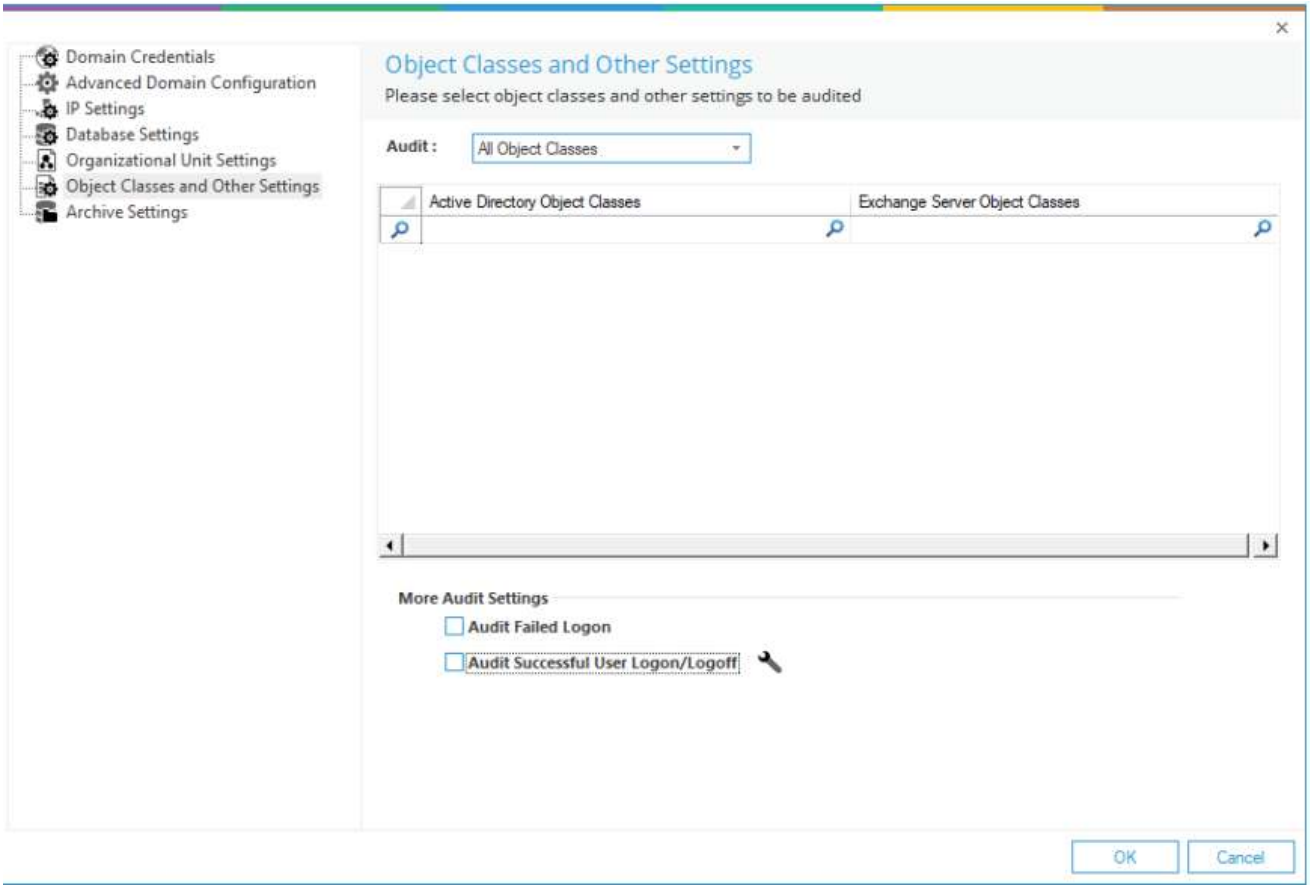
按住"CTRL"键选择多个待添加的组织单位，单击按钮，将组织单位添加到"已选OU路径"列表中。



选中的OU将列在表中。单击Next继续。

对象类和其他设置

在此步骤中，您可以选择希望审计的对象类：



默认情况下，选中"审计所有对象类"选项。如果您想要审计特定的对象类，那么您可以手动选择它们。本节主要分为两部分：

1. 对象类：在本节中，您可以选择以下两种选项中的任何一种：

   a. 所有对象类:选中此选项，审计Active Directory和Exchange Server的所有对象类。

   b. 只选中类:选中此选项，只审计Active Directory和Exchange Server的特定对象类。

   c. 除选定类外的所有类:选中此选项，审计除选定类外的所有Active Directory和Exchange Server对象类。这是添加域时的认选项。这意味着在默认情况下，以下13个对象类仍然被排除在审计之外。您需要取消选中"所有但不包括所选类"中的这些类，或者选择"所有对象类"以启动它们的审计

•CRLDistributionPoint

•CrossRef

•CrossRefContainer

•DnsNode

•InfrastructureUpdate

•LinkTrackOMTEntry

•LinkTrackVolEntry

•MSMQConfiguration

•NTFRSMember

•PrintQueue

•RIDManager

•Secret

•ServiceConnectionPoint

2. 更多审计设置:该部分允许您启用和配置域的登录审计。包括以下选项:

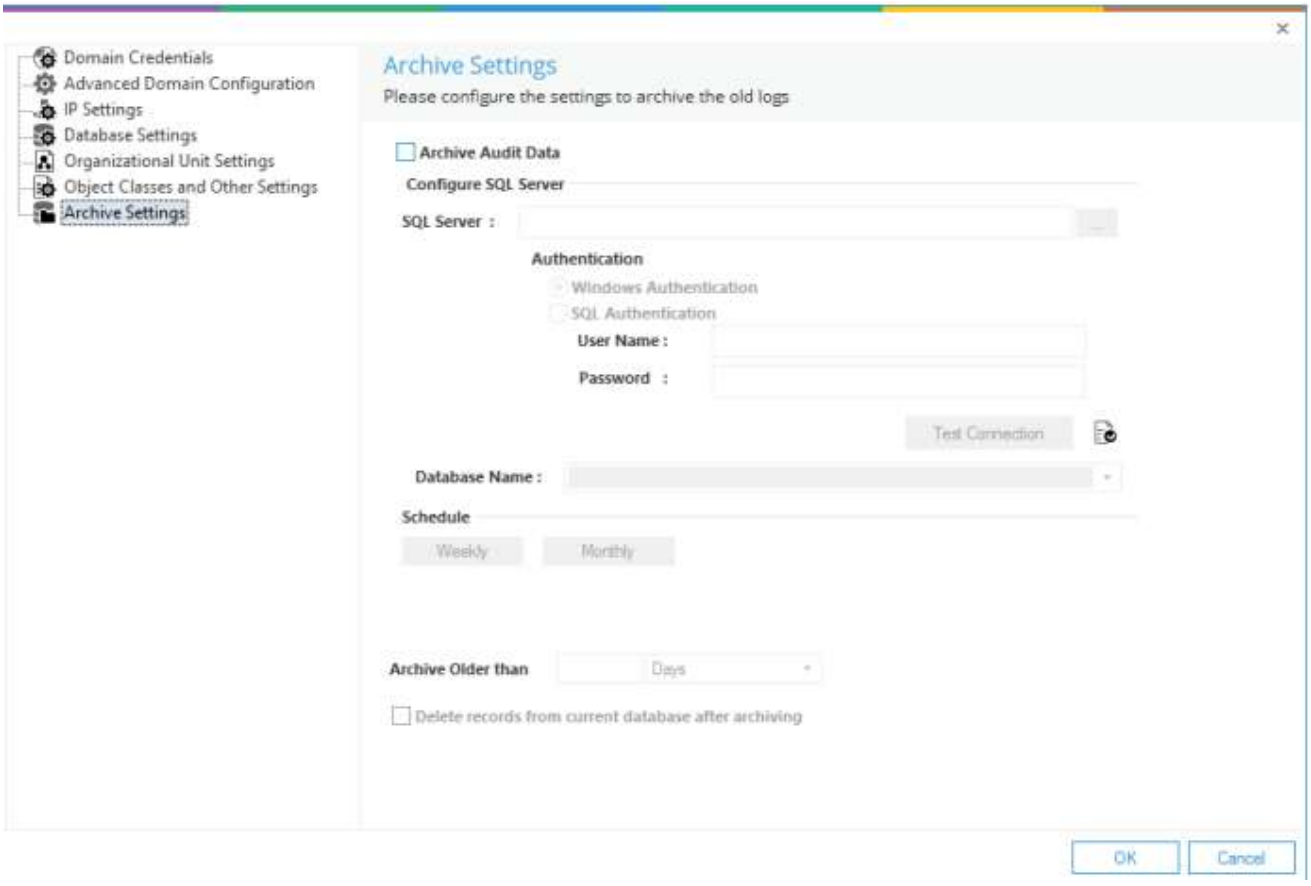
a. 登录失败审计:选中该选项，对所有登录失败的尝试进行审计。

b. 审计成功登录/注销:选中该选项，审计所有登录/注销尝试。在从图标配置此模块之前，这些事件将不会被收集。有关更多信息，请参阅启用登录/注销监视指南。

存档数据库设置

在这里，您可以配置和调度存储在主数据库中的审计日志的自动归档。

还可以在任何时候通过右键单击域并选择Archive Now选项手动执行数据库归档。在这两种情况下，还可以设置为保留或删除主数据库中的归档日志。



要执行存档数据库设置，请遵循以下步骤:

1. 选中Archive Audit Data复选框。

2. 现在通过使用Browse按钮选择SQL Server或手动输入其名称。

3. 选择"Windows身份验证"或"SQL身份验证"。我们建议选择SQL身份验证，并提供SQL用户的用户名和密码。

4. 提供将存储归档日志的数据库的名称。

5. 测试SQL Server连通性。

注意：选择的用户在SQL Server中应该具有dbcreator角色。

注意：单击图标可从默认SQL Server设置中加载数据库设置。

6. 现在选择自动归档的时间表。从以下选项中选择：

   a. 按月：选择归档进程在每月指定的日期运行。

   b. 每周：选择在一周中指定的日期运行存档进程。

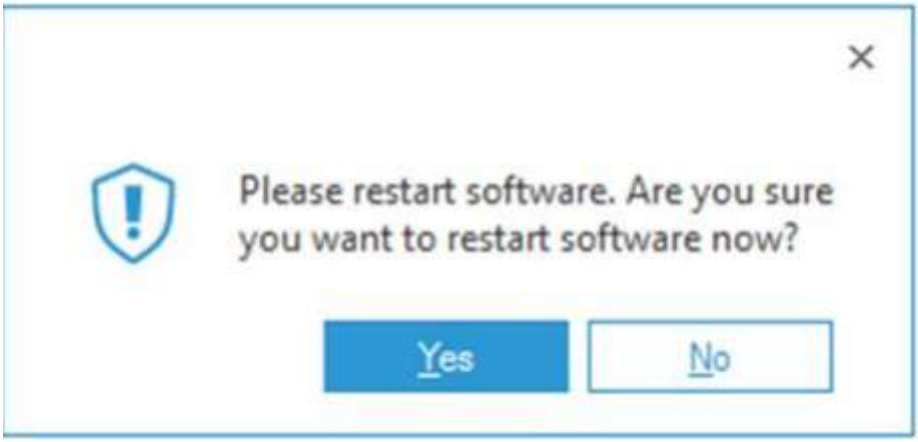
7. 选择存档开始时间。

8. 提供日志的年龄（以天为单位），在此之后，日志将有资格存档。

9. 选中"归档后从生产数据库删除记录"复选框，以在归档后从主数据库中删除归档日志。这有助于限制主数据库的大小

完成通过Advanced Configuration添加组件的所有步骤后，单击Finish。屏幕上将出现一个重新启动解决

方案的消息框



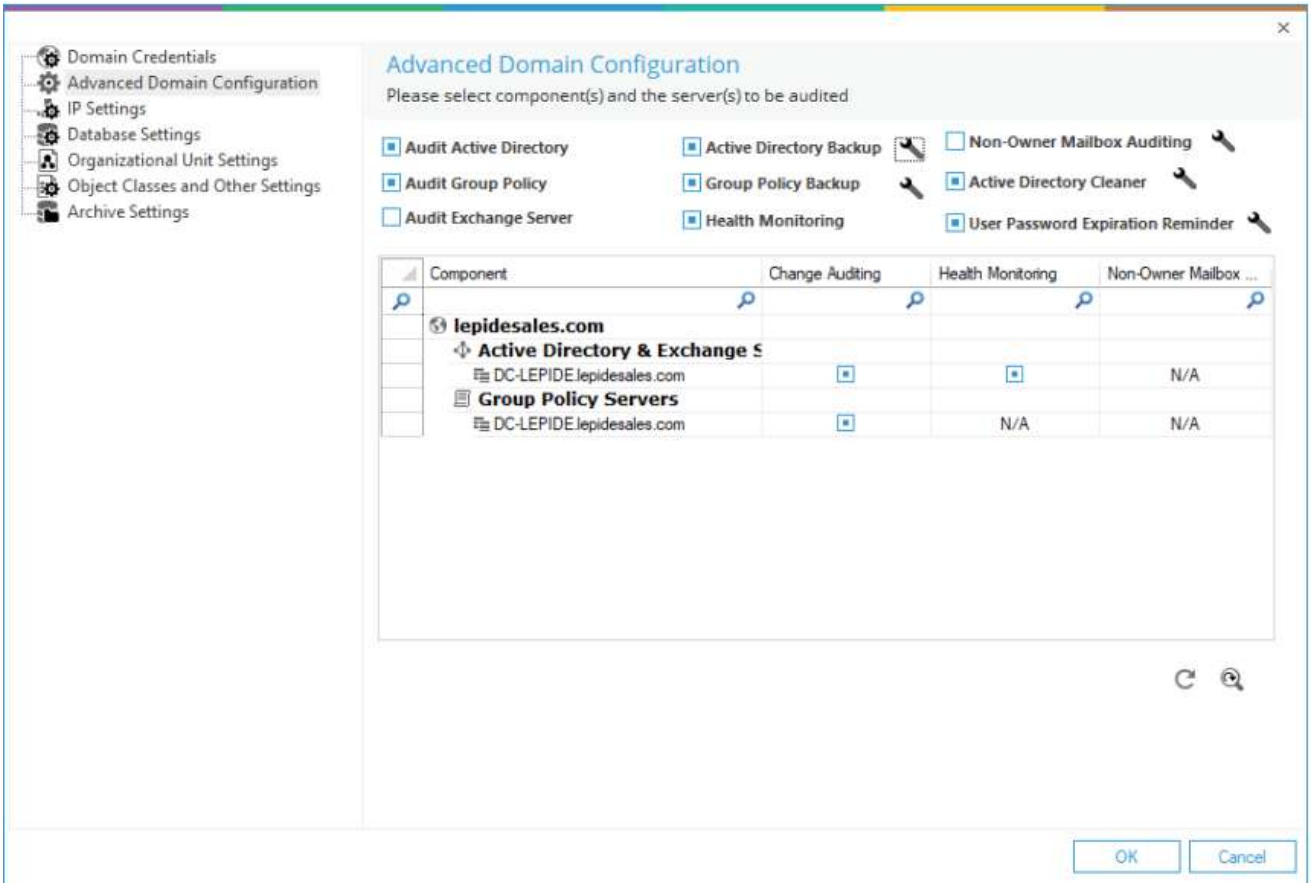
单击Yes重新启动解决方案。

高级域配置选项

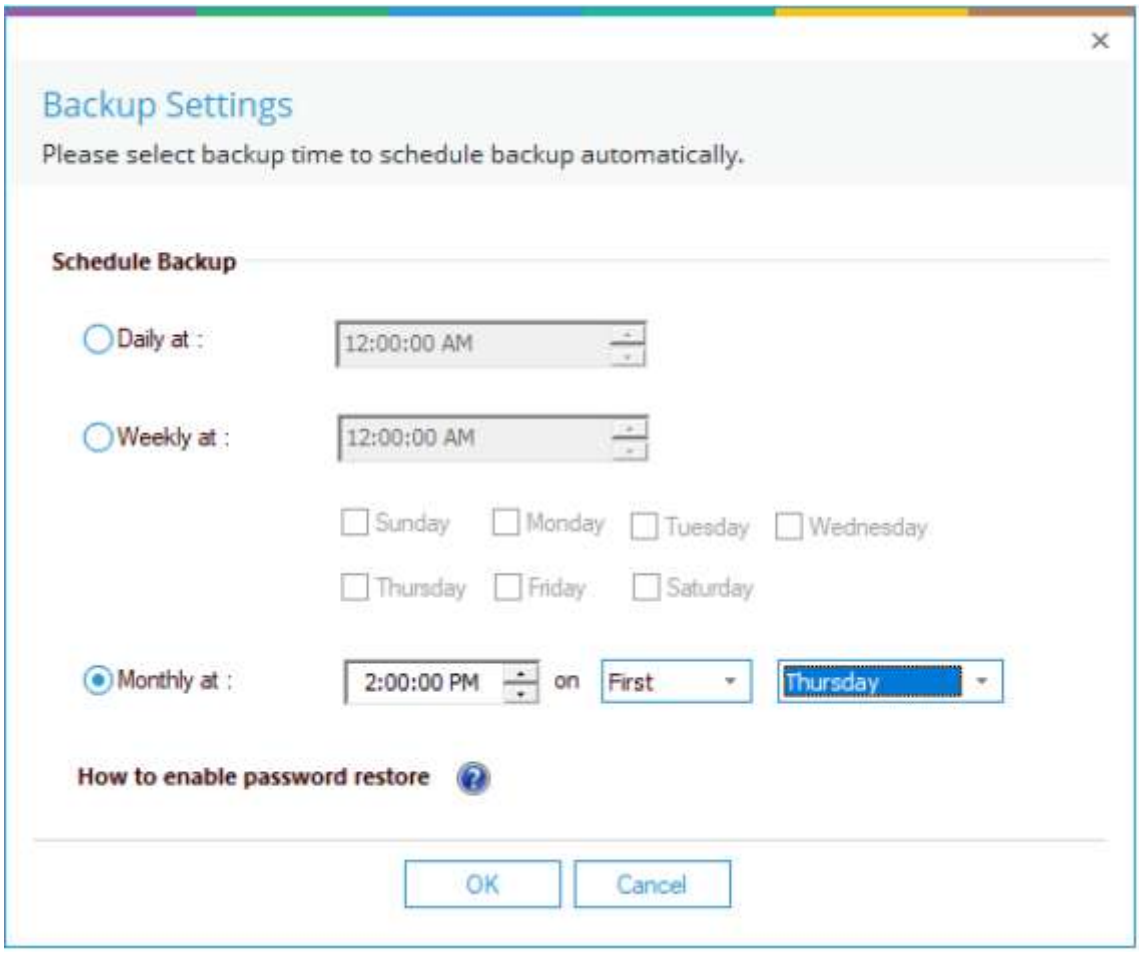
对于高级配置选项，单击相关选项旁边的图标：

Active Directory和组策略对象备份

在添加域或修改已添加的域时，可使用Active Directory备份选项。这可以在高级域配置屏幕中找到：



您需要选中Active Directory Backup选项来启用该特性。启用后，您可以单击相邻的图标来打开其设置。



• 在对话框中选择"每日"、"每周"或"每月"选项。您可以在"每日设置"中自定义时间。选择"每周时间"后，可以指定备份快照在哪天被捕获。

• 如果选择"按月"选项，可以指定时间和日期选项。单击OK应用设置。

同样，单击"组策略备份"图标，并使用上述步骤配置组策略备份。您可以单击图标恢复此步骤的默认选项。

单击图标重新扫描域并加载更新的信息。

健康监测

选中该框以启用运行状况监视。若要查看运行状况监视指示板，请单击该图标。

非所有者邮箱审计

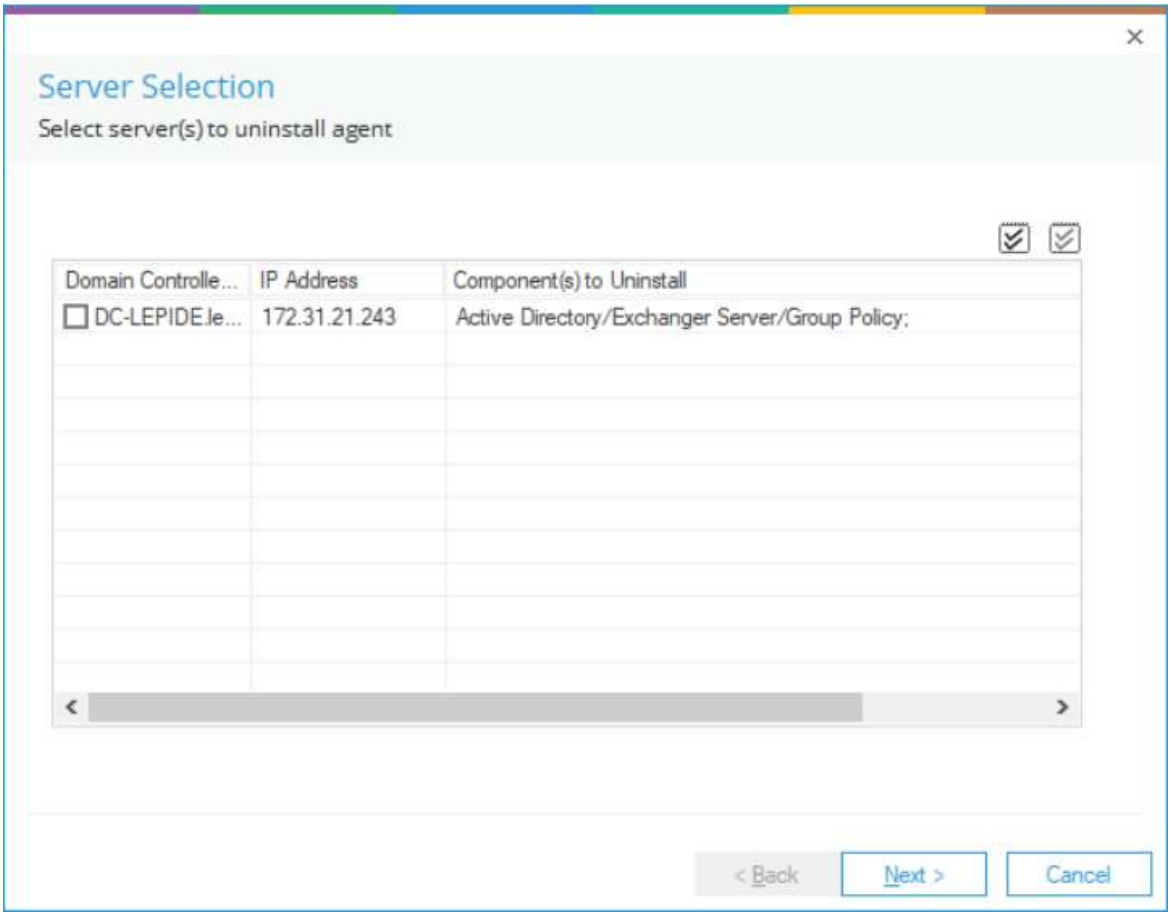
有关如何配置此功能的详细信息，请参阅配置邮箱审核指南。

卸载和移除

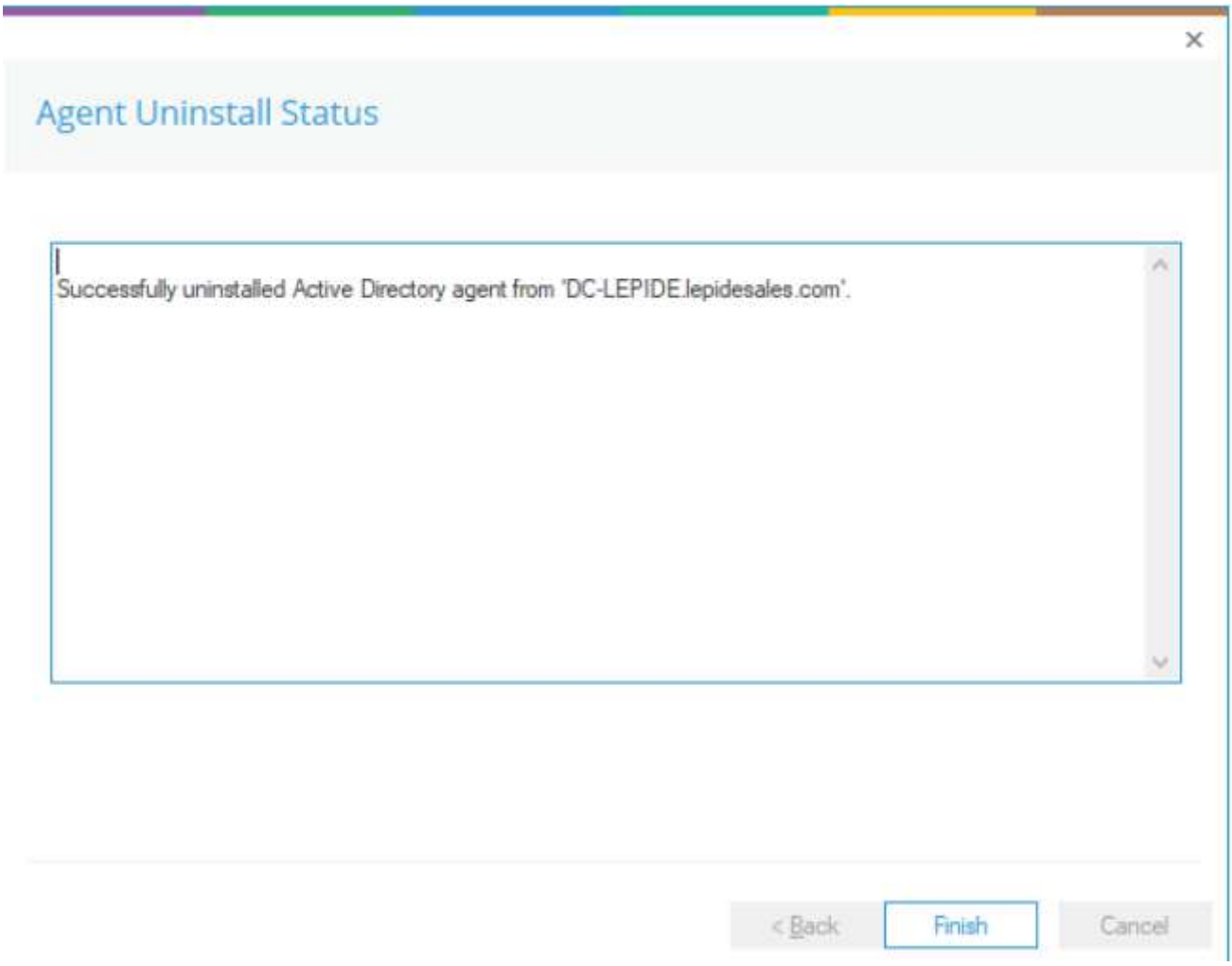
从已添加的域中卸载代理

按照以下步骤从域中卸载代理。

1. 在"设置"界面中右键单击域节点，单击"卸载代理"选项。系统弹出如下对话框：



2. 选择要从其中卸载代理的服务器。单击图标可选择所有列出的域控制器，单击图标可取消选择所有已选项。单击Next。
3. 如果"所选域控制器"的"IP地址"单元格不显示数字或显示错误的"IP地址"，请双击该单元格进入对话框。输入正确的域控制器IP地址，单击"确定"。现在，向导显示输入的IP地址。
4. 单击"下一步"启动卸载代理程序。
5. 卸载代理后，将出现以下消息。

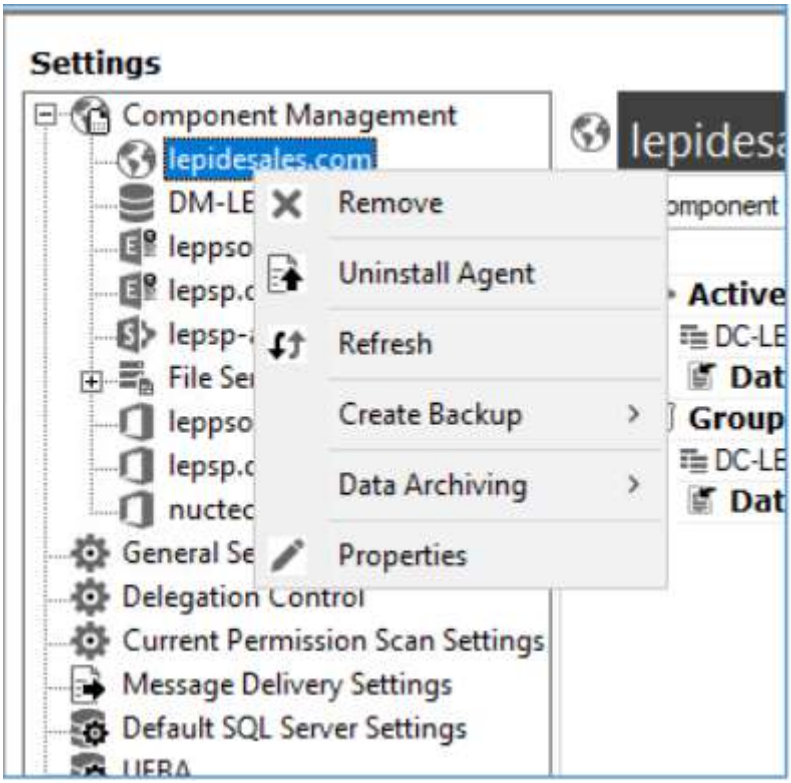


6. 单击Finish完成该过程。

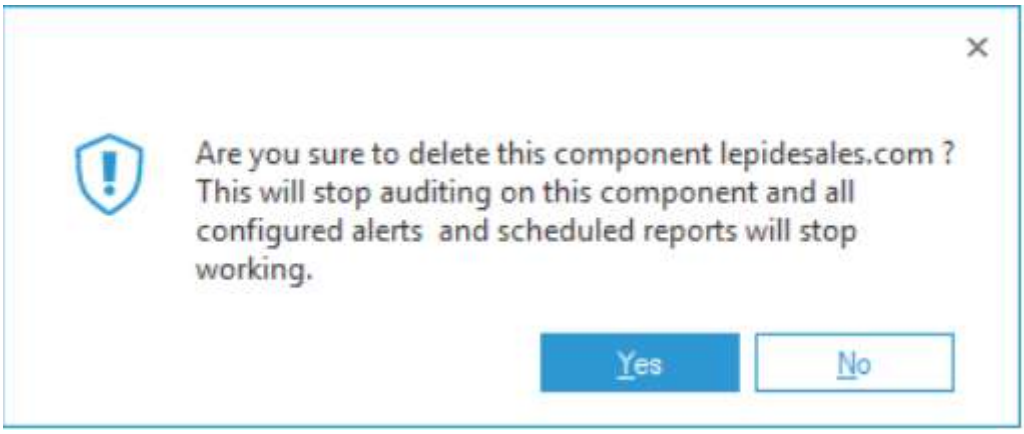
删除域名列表

从审计列表中删除已添加的域，请执行以下步骤。

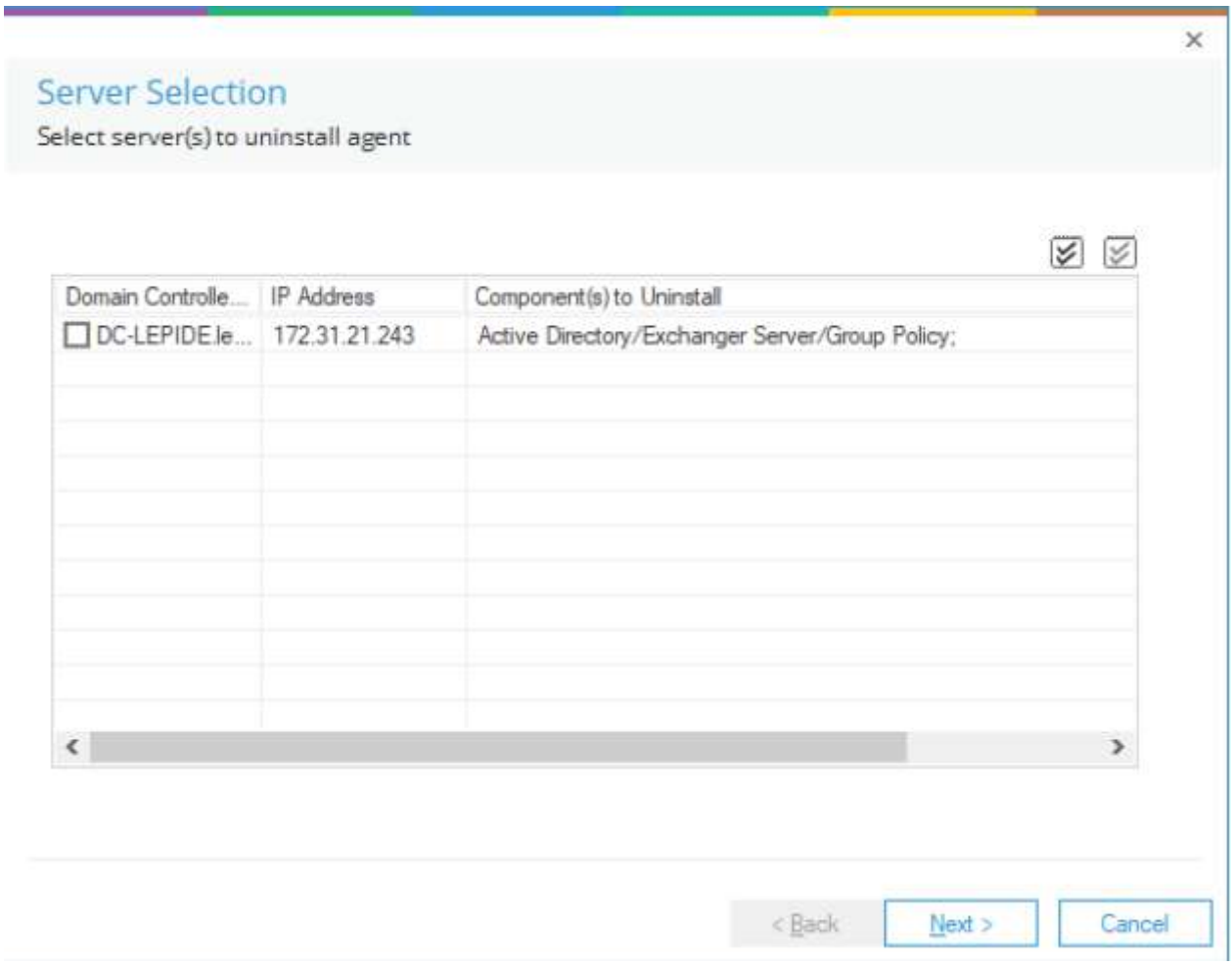
1. 右键单击Component Management下的域节点，然后单击Remove option。



2. 系统显示如下警告信息：



3. 单击Yes。弹出“卸载代理”对话框：

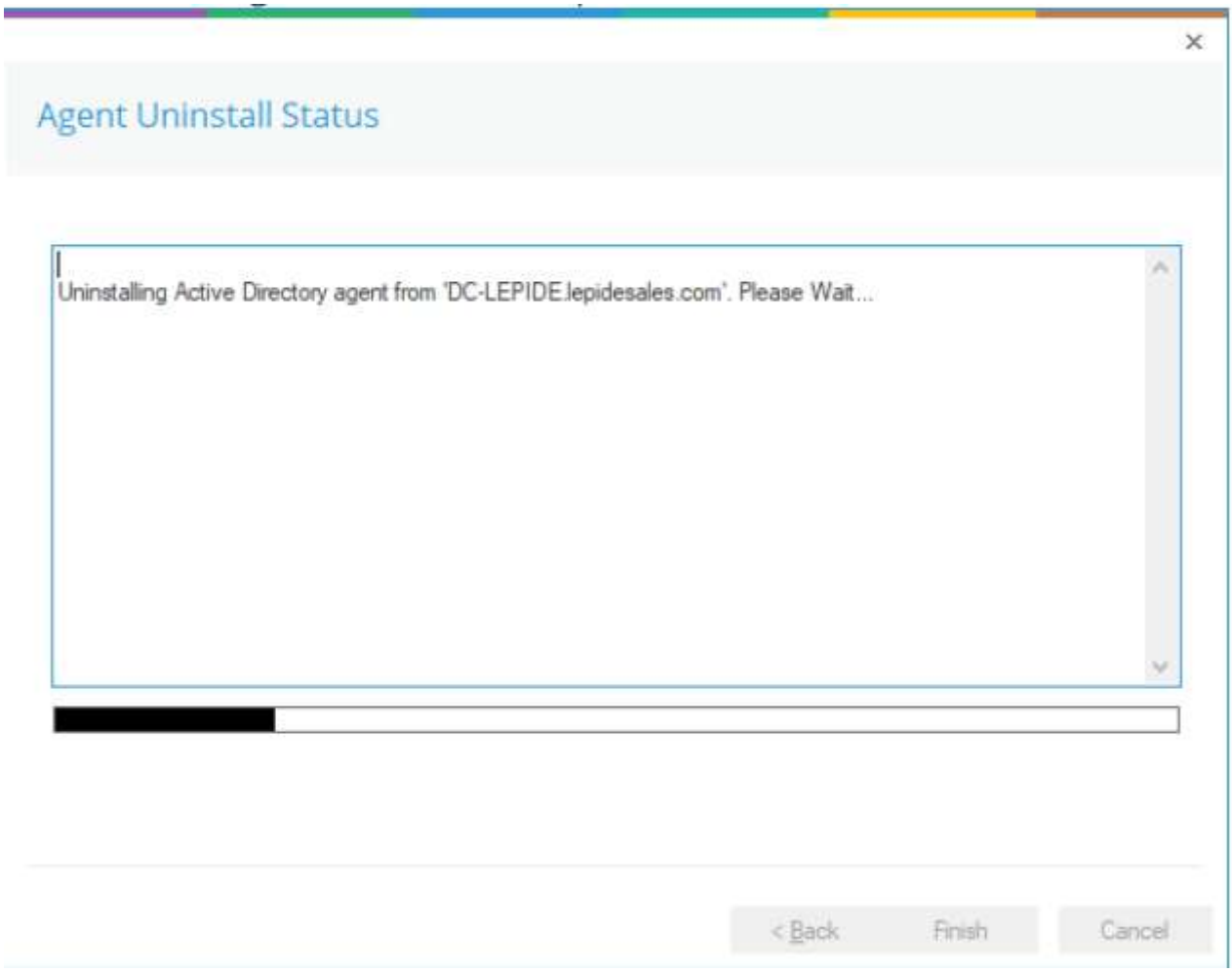


4. 如果不想再次添加域，则需要卸载代理。

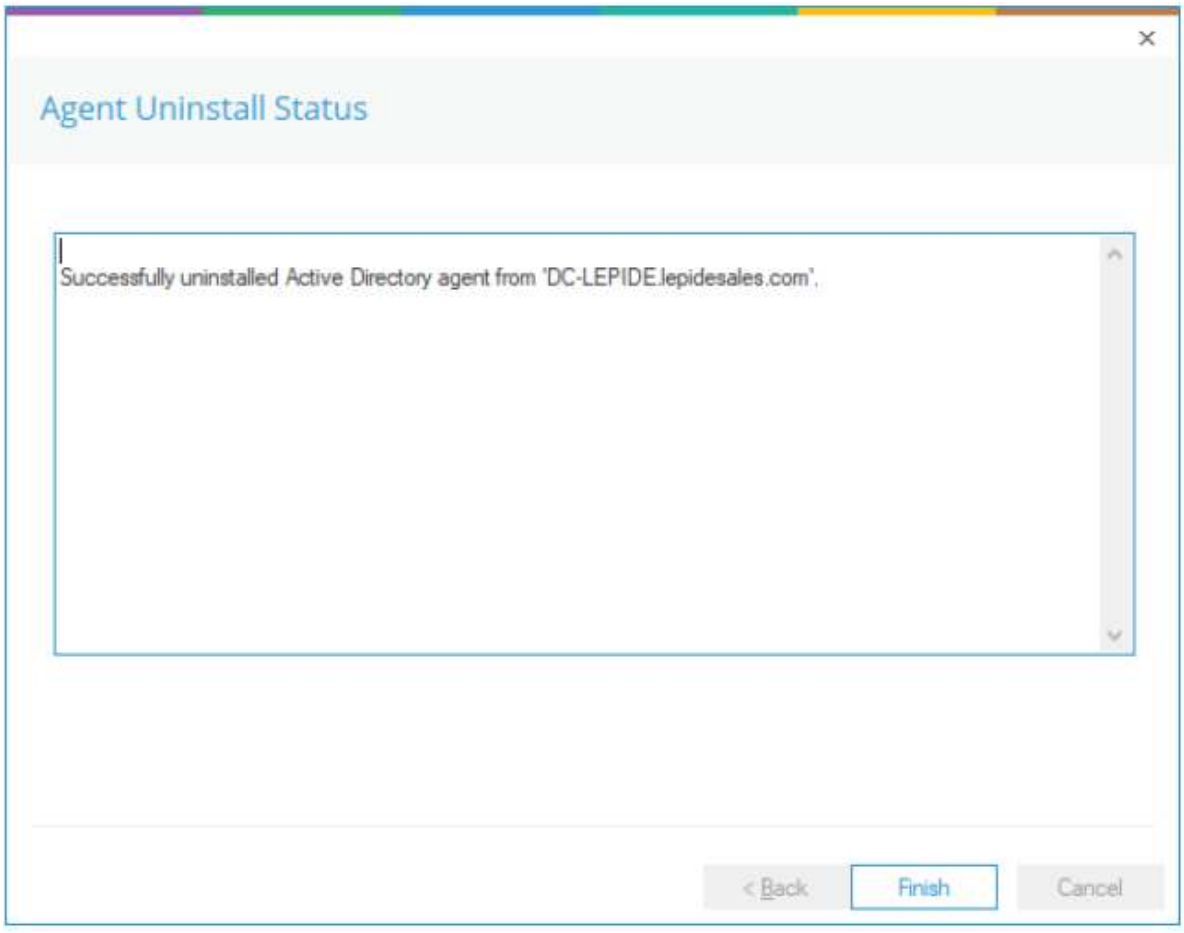
5. 选中要从中卸载代理的域控制器复选框。单击图标可选择列表中的所有域控制器，单击图标可取消选中所有域控制器。

注意：在某些情况下，被删除域的域控制器仍在被监视，因此我们建议您在从审计列表中删除域的同时卸载代理。

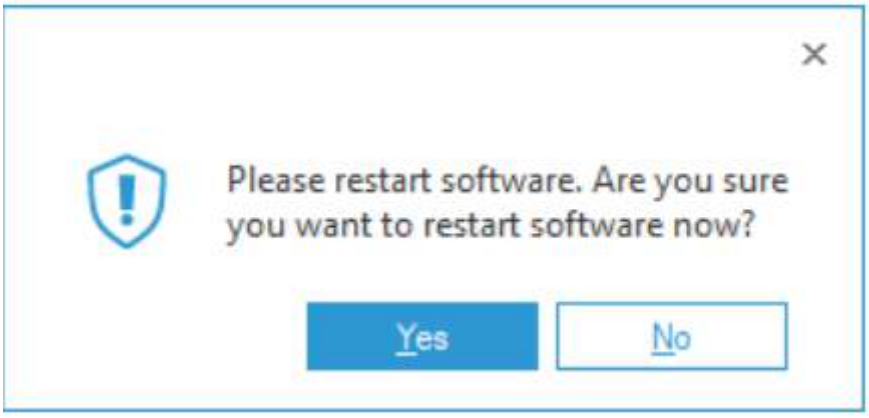
6. 单击Next启动代理卸载过程。



7. 代理卸载成功完成后，向导将进行确认。



8. 单击Finish完成向导。将显示一条消息：



9. 单击Yes重新启动解决方案。

卸载Lepide数据安全平台

在某些情况下，您可能需要卸载莱德数据安全平台。请确保在卸载解决方案之前关闭它。按照下面的步骤卸载它。

1. 有两种方式可以开始卸载。

   a. 进入"开始→所有程序→leide数据安全平台"，单击"卸载Lepide数据安全平台"。

   b. 单击"开始→控制面板"。窗口出现了。启动程序和功能。选择"莱德数据安全平台"，单击"卸载"。

2. 以上任何一种方法都会显示一条警告消息。

3. 单击Yes开始卸载过程。

4. 卸载后，屏幕上出现确认成功卸载的消息框。

5. 单击OK以完成该过程。

在执行上述步骤后，从您的计算机上成功卸载了leide数据安全平台。

解决方案默认配置在程序安装文件夹中保留license文件、服务器审计、备份快照数据等设置。要删除剩余的元素，请手动删除其程序安装文件夹，然后清空回收站。

如果您希望保留license文件或必须重新安装相同/升级版本的解决方案，请勿删除此文件夹。

%ProgramFiles%\ leide Data Security Platform - for 32位操作系统%ProgramFiles(x86)%\ leide Data Security Platform - for 64位操作系统如果删除上述文件夹，解决方案捕获的快照数据也将被删除(如果您没有提供其他存储快照的路径)，并且无法恢复它们。因此，如果您希望保留应用程序日志、license文件、备份快照和其他设置，请不要删除安装文件夹。