FileAudit

入门指南

4.0

版本

www.isdecisions.com

简介

FileAudit 监测 Microsoft Windows 服务器上对敏感文件及文件夹的访问或访问企图。
FileAudit 允许您主动跟踪、审计和报告针对文件服务器上文件及文件夹的所有访问并给出报警。
由于没有代理且不会造成入侵，您能够远程审计服务器，不用安装任何软件。

FileAudit 入门指南设计用于为主要特性提供每一步安装指南以及配置。目标是快速适应控制台及基本 FileAudit 概念。其它的功能在软件帮助文件中详细描述。

如果在评估、安装或迁移中遇到问题，我们欢迎您联系我们的技术支持团队。
.

目录

1. 安装 FileAudit

在此处提供 FileAudit 安装包（*FileAudit_x86.exe*）。
英语及法语版本一样并且与 32 位及 64 位平台兼容。

FileAudit 支持在以下操作系统上安装审计服务（对于控制台安装）。

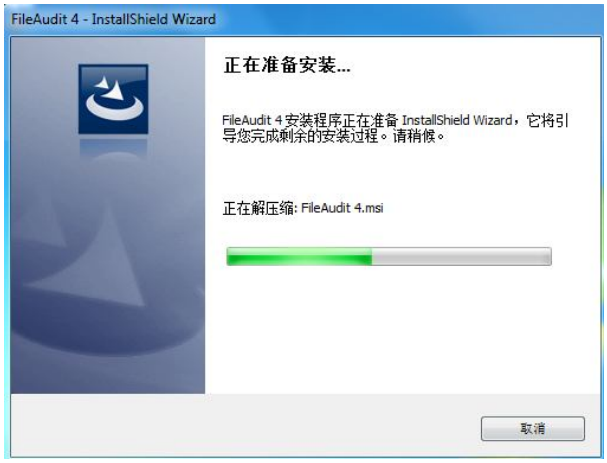
- Windows XP
- Windows 2003 Server
- Windows Vista
- Windows 2008 Server
- Windows 7
- Windows 2008 R2 Server
- Windows 8
- Windows 2012 Server

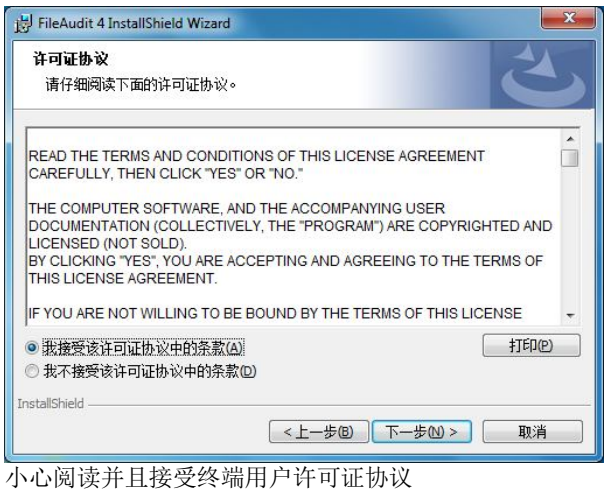
.Net 框架 3.5 SP1 需要从 Microsoft Web 站点下载，并且需要进行安装。
对于 Windows Seven, Windows 8, Windows 2008 R2 及 Windows server 2012 系统，Net Framework 3.5 SP1 能够通过选择‘'Control Panel\Programs\Programs and Features\关闭或打开 Windows features’进行安装。
不强制要求将 FileAudit 安装在将要审计的系统上。任何满足系统需求的机器能够用作 FileAudit 远程主机，并且远程进行审计的系统不需要安装任何软件。

FileAudit 将在数据库中存贮所有检测到的事件。FileAudit 支持以下数据库系统：

- Microsoft Access 数据库文件 (mdb)
- Microsoft SQL Express 2005/2008/2008 R2
- Microsoft SQL Server 2005/2008/2008 R2/2012

FileAudit 包也提供免费的 Microsoft Access 数据库程序。
如果需要启动 FileAudit 安装过程，以管理员帐号运行 FileAudit_x86.exe。



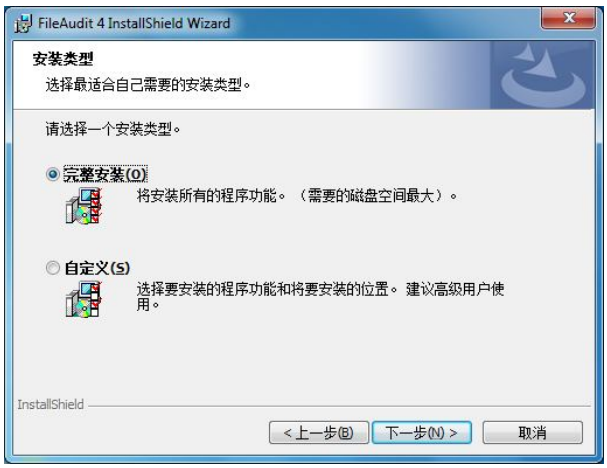


小心阅读并且接受终端用户许可证协议

点击下一步>.

输入您的客户资料并点击下一步

如果需要，可以更改安装文件夹



选中‘完整安装’框并点击下一步

点击‘安装’以开始 FileAudit 安装

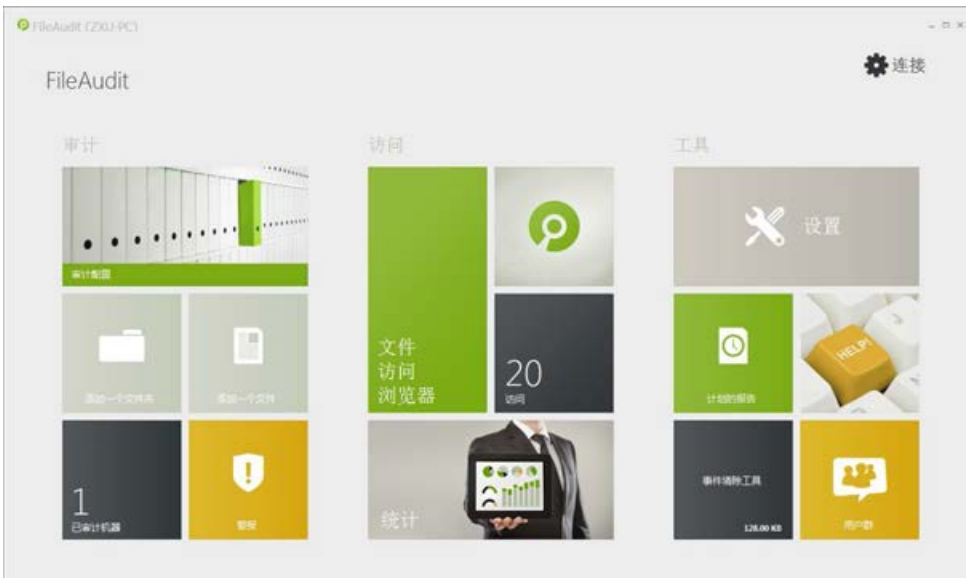
FileAudit 已经成功安装

点击‘完成’。

2. 配置第一个审计路径并且在其上定义一个警报

2.1. 配置第一个审计路径

启动 FileAudit。



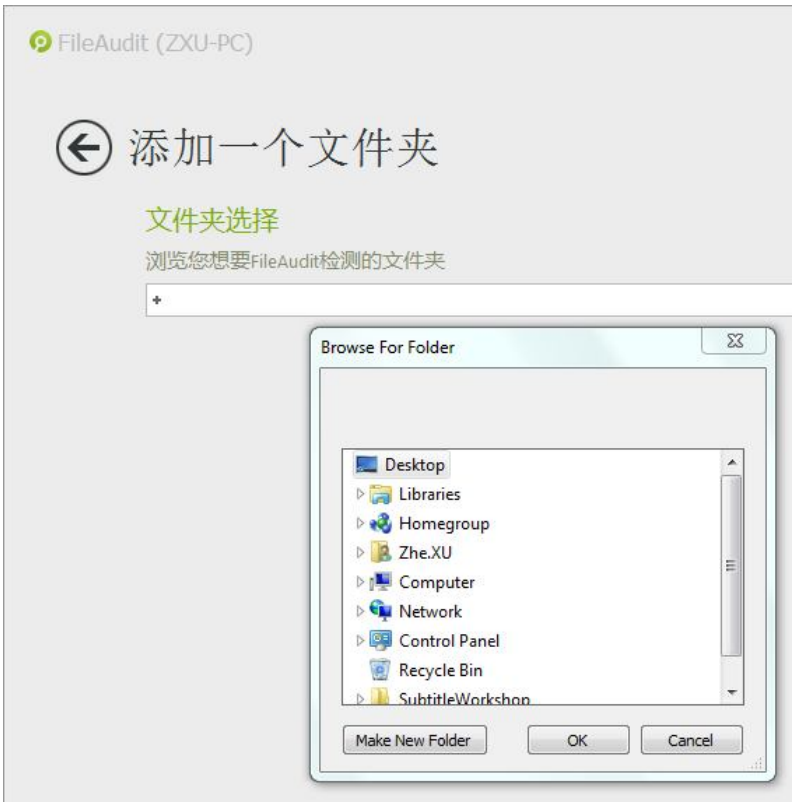
FileAudit 中心

您将发现 3 个主要分组：

- 审计：这些标签允许您配置审计及警报。
- 访问：这些标签显示‘文件访问浏览器’及‘统计’视图。
- 工具：这些标签定制 FileAudit 设置、计划自动报表、清除数据库并且访问帮助文件。

点击右上角处的另外‘连接’按钮，您可以远程连接到运行‘FileAudit 服务’的另外系统。

如果需要设置第一个审计路径，点击 FileAudit 中心的‘添加一个文件夹’标签，点击‘＋’按钮并且浏览目标文件夹。

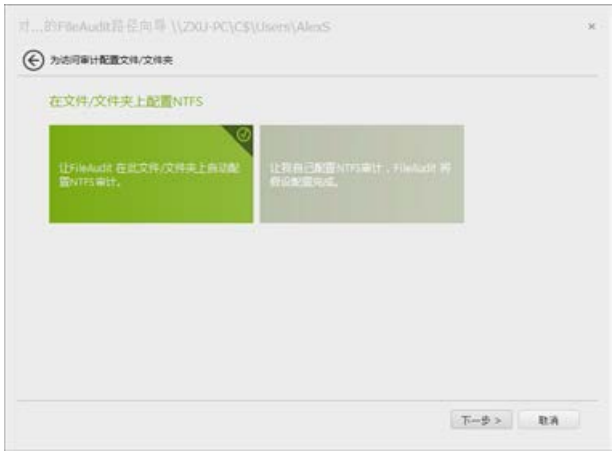


验证完您的选择后，弹出‘FileAudit 路径向导’以指导您如何配置文件夹审计。

此向导将显示选择的文件夹的审计配置状态并且突出显示任何缺少的需求或设置。对于每个必要的动作，您可以选择自动完成（通过向导）或手动完成。我强烈建议对所有审计设置使用 **FileAudit 自动配置。**

要求的动作列表

选择自动或手动处理



FileAudit 将优化 NTFS 审计设置

文件夹主机将被添加到‘许可服务器’列表中

通过选择选项‘连续监测服务器安全日志’可以启用实时事件监测功能。

您已经选择的文件夹现在由 FileAudit 监测。所有访问事件将存贮在 FileAudit 数据库中，我们建议您保持此视图，我们将从此处讲解下一部分内容。

注意：您可以通过多种方式选择要审计的文件/文件夹。另外，对于您以前使用的方法，您能够：

- 通过直接右击 Windows Explorer 中的文件或文件夹启动控制台，然后在‘上下文菜单’中选择 FileAudit。在这种情况下，忽略以前的步骤，因为文件/文件夹路径直接导入到 FileAudit 控制台中。
- 显示‘文件访问浏览器’并且直接在‘路径’域中输入目标路径。您也能够在‘文件访问浏览器’中发现两个按钮以添加一个文件夹或文件。
- 只需要使用‘审计’部分中的两个标签‘添加一个文件夹’或‘添加一个文件’。

另外，FileAudit 总是检查不同视图中输入的路径审计配置状态及设置，例如：

- ‘文件访问浏览器’
- 计划报表配置
- 警报规则定义

2.2. 为审计的文件夹定义一个警报

一旦 FileAudit 显示目标文件夹的审计配置结果，则您能够为其定义警报。您能从右侧标签找到‘添加一个警报’，然后点击。
FileAudit 将切换到以前设置的特定审计文件夹的‘警报’配置界面。在此示例中，我们将为‘My_Data’文件夹定义一个成功删除事件触发的警报。
第一个‘主‘标签允许您定义触发电子邮件警报的事件。当访问已经授予或拒绝时，FileAudit 能够发送一个警报。在此示例中，仅仅当用户成功删除一个文件时我们才选择接收此警报。在’状态‘域中，检查’授予‘框。

然后选择‘删除‘访问类型，注意此事件因为尝试访问而生成。如果用户试图在监测的文件夹上删除一个文件，您将得到状态为’拒绝‘的’删除‘事件。

最终的参数允许定义一个特定‘用户‘及/或’源‘以触发一个警报。如果您想得到对任何产生一个事件的’用户‘或’源‘的警报，则域’用户‘及’源‘应该保持为空。

注意如果文件/文件夹通过网络进行访问，则‘源‘信息（例如：产生访问尝试的进程名）不可用。

在‘主’标签底部的开关允许启用/禁用此警报。

‘监测的路径’界面已经定义，因为我们在路径上设置审计之后创建了警报。如果任何一个用户在‘My_Data’中成功删除一个文件或文件夹，则此‘警报’将被发送。

现在我们将为此警报定义一个接收方，点击‘接收方’标签。

为了创建一个新的接收方，点击‘添加一个接收方’，这将在屏幕的右侧产生一个面板。直接输入一个接收方名字及有效的电子邮件地址并点击‘验证’，您可以将此联系人添加到‘接收方’列表中。您能够重复此动作以添加几个接收方。

注意：所有以前定义的计划报表或警报都被 FileAudit 存贮为通用参数，允许从列表中选择已有接收方。

电子邮件消息的内容可能通过‘邮件消息’标签进行定制。在方括号‘{ }’中包括动态变量。关于他们的定义，参见帮助文件。

一旦所有配置标签都根据要求进行了定义，则点击‘保存’，此警报将直接激活。
当您添加一个警报时，FileAudit 检查是否定义了要求的电子邮件设置以发送此警报。直到现在，我们没有定义用于邮件发送的电子邮件服务器设置。因此，当您点击‘保存’时会弹出此菜单。

点击‘OK’将使您从 FileAudit ‘设置配置’重新定向到‘电子邮件’界面，输入您的 SMTP 服务器，使用的端口以及电子邮件发送方的地址（要求已有地址）。

通过点击向后箭头按钮，您可以返回 FileAudit 标签以验证配置。
现在可以在‘My_Data’文件夹上设置审计及警报。现在让我们查看为此文件夹生成的访问事件。

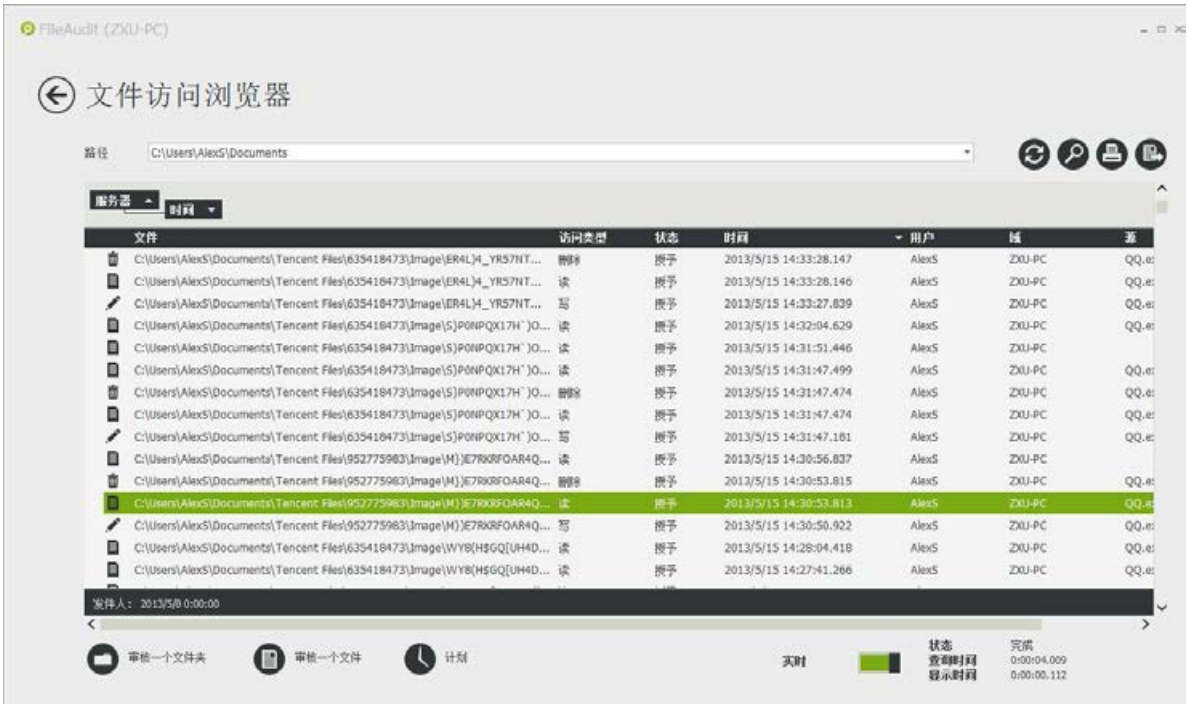
注意：您也能够通过点击‘警报’标签直接从 FileAudit 中心创建一个警报。

3. 显示文件访问事件

‘文件访问浏览器’允许您显示、搜索、计划并打印 FileAudit 上配置的对监测文件/文件夹访问尝试生成的所有报表。使用 FileAudit 中心的中心标签打开‘文件访问浏览器’。
输入文件/文件夹到‘路径’域中以显示相应的文件访问事件。为了验证输入，按下‘回车’或点击刷新按钮。一旦您已经为一个文件夹/文件路径显示事件，FileAudit 将保存在内存中，您能够使用拉列表再次选择。

如前所述，如果 FileAudit 还没有打开，您能够右击 Windows Explorer 中监测的文件夹并且直接从弹出菜单中选择 FileAudit 。这样您可以为此文件夹打开 FileAudit ‘文件访问浏览器’。

您也可以点击屏幕左下角处的‘审计一个文件夹’或‘审计一个文件’按钮。
一旦您已经为一个文件夹/文件路径显示事件，FileAudit 保存在内存中，您能够使用下拉列表再次选择。



事件可以实时检测并且存贮到数据库中。如果您想控制台实时显示事件，启用右下角的‘实时’开关并且点击‘刷新’。
文件访问浏览器数据网格提供几种分组及过滤选项。如果需要按特定列对视图进行分组，将列名拖放到路径域下。

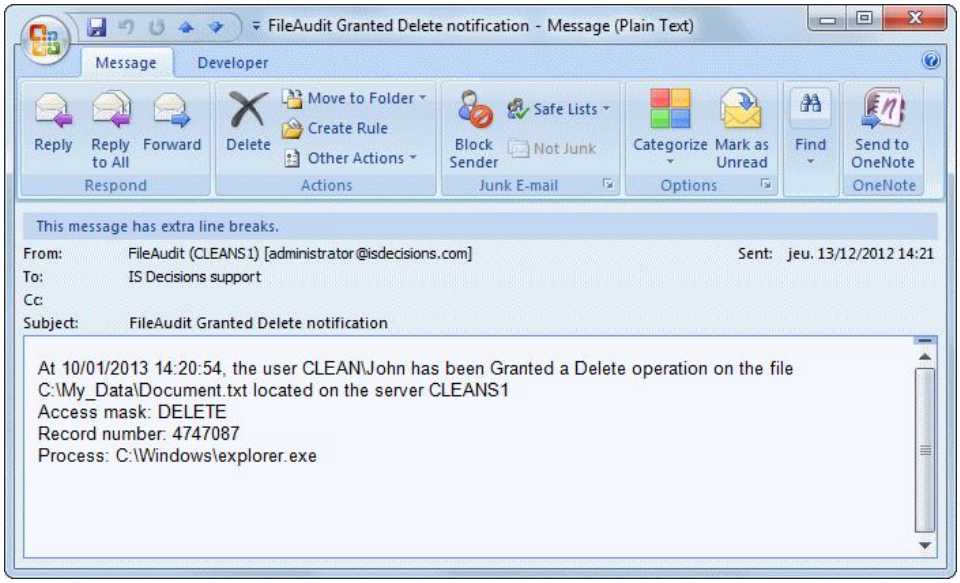
如果需要访问过滤器并执行一次搜索，点击放大镜按钮。在屏幕右侧将弹出过滤器表，选择您的标准并应用过滤器。
通过右击列名行显示弹出菜单，然后您能直接从事件网格中使用过滤器并搜索选项。此菜单允许对数据网格显示进行定制（管理列显示、排序等）并且指示‘过滤器编辑器’位置，您能够启用/禁用‘发现面板’及‘自动过滤器行’。

每个列名提供一个快速搜索功能。当您用鼠标指针滑过列名时，您能够在列名行右上角看到一个漏斗图标。点击此图标，您可以访问搜索选项。

打印按钮使您能够显示文件访问浏览器的可打印版本并且能够直接打印或导出几种文件格式。

注意：事件网格的分组及过滤选项仅仅影响显示的数据。为了对整个事件数据库进行搜索，使用放大镜按钮的过滤器。

同时，当一些用户已经删除文件/文件夹时，电子邮件警报也可以实时发送。



4. 设置一个自动报表

您能够以两种方式设置由电子邮件发送的计划报表。第一种方法是点击 FileAudit 中心的‘计划报表’弹出菜单并且点击‘添加一个计划报表’以创建一个新报表。
同时，此特性能够通过定制您报表中的文件访问浏览器并且点击计划按钮进行启用。您将重新定向到计划报表配置界面。所有以前定义的过滤器设置在前三个标签设置中进行导入（主、监测的路径及时间）。此处我们将使用此方法。

打开‘文件访问浏览器’并且使用过滤器定制视图，例如：如果您想为前天发生的删除文件事件设置一个报表，按以下方式设置过滤器：

- 定义‘发送方’域为‘事件来源’并且设置昨天及早上 8：00。
- 定义‘接收方’域为‘事件接收方’并且设置昨天及下午 6：00 点。
- 设置‘状态’为‘授予’。
- 设置‘删除’为‘访问类型’。
- 点击‘应用’。

‘文件访问浏览器’将根据此过滤器配置刷新显示的事件。点击‘计划’按钮，您将重定向到‘计划报表配置’界面。您为‘文件访问浏览器’定义及应用的以前过滤器设置将在前 3 个设置标签‘主’、‘监测路径’及‘时间’中导入。在‘主’界面，输入此报告的名字。

点击‘接收方’标签以为此报表定义电子邮件接收方。当我们已经为一个警报定义一个接收方，如果合适，我们能够选择接收方电子邮件地址。点击‘添加一个接收方’，则在控制台右侧弹出一个表。

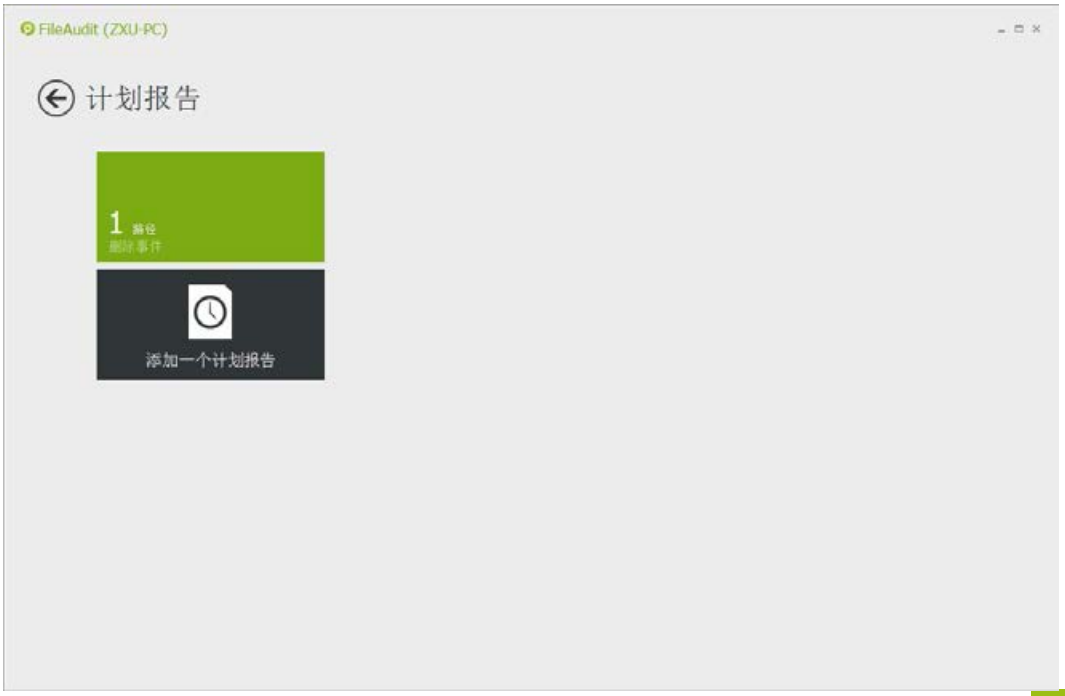
点击‘选择按钮’，在列表中选择接收方并且点击‘OK’。

关于此接收方的所有信息导入到‘添加一个接收方’表，验证接收方，您能够为相同报表添加几个接收方。
‘邮件消息’界面已经用缺省的文字定义，您能够进行定制。

最后的标签‘计划’为报表任务定义了时间触发器。

FileAudit 计划器理解您已经为报表设置的时间周期以定期动态生成报表。此处我们已经选择前天作为监测时间周期。此报告将总是包括执行天前天的事件。此报表将作为电子邮件的 PDF 格式附件。
通过点击‘测试’按钮，您能够测试报表定义。弹出菜单将确认测试已经启动。如果所有操作正常，您们收到一个带报表附件的电子邮件。这使您能够检查是否结果与您的需求一致并且根据需要改变设置。

点击‘保存’以验证您第一次自动报表，您将重定向到‘计划的报表’界面，您能够从此界面修改关于此自动报表的所有设置。



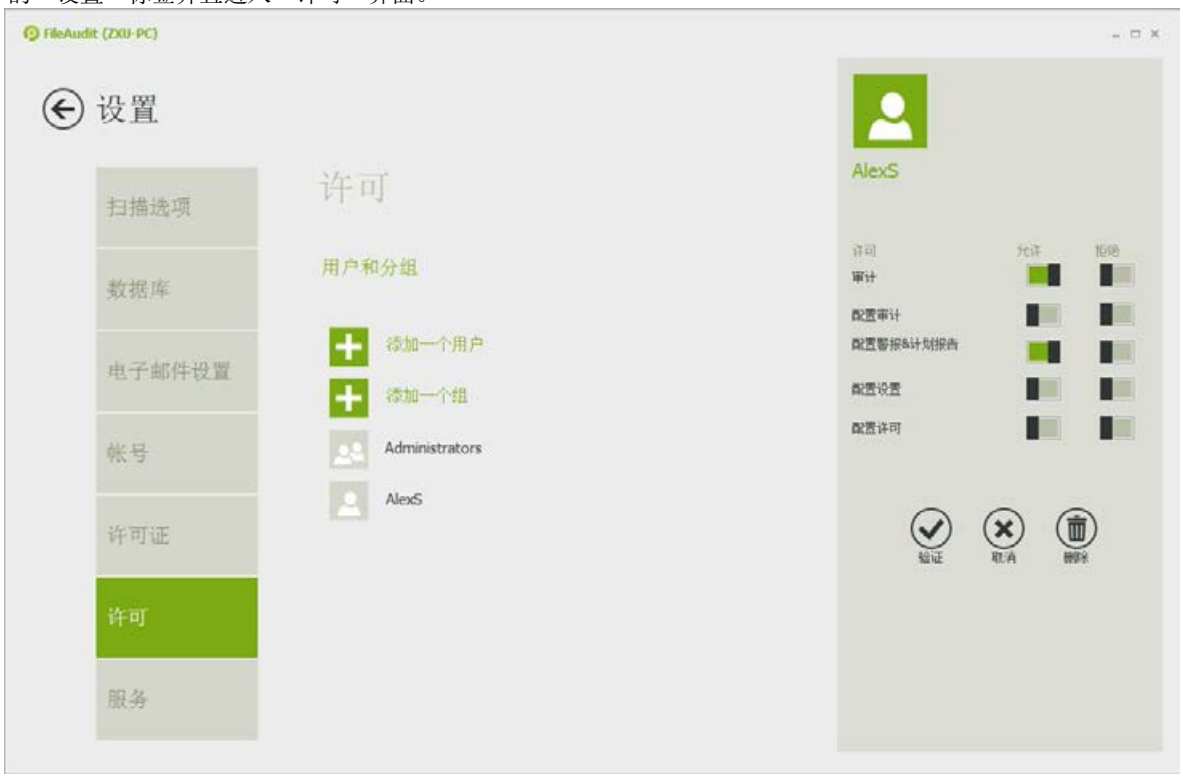
5. 额外设置

5.1. 排除审计中的用户、程序及扩展名

在‘设置配置’中，‘扫描选项’界面能够排除特定用户帐号、可执行文件及扩展名的访问事件。这对由备份软件及病毒等产生的文件访问特别有用。

5.2. 为特定帐号细粒度授权 FileAudit 访问

您能够为没有管理权限的人员设置特定的帐号以及您希望向这些人提供的 FileAudit 功能。如果需要访问此功能，点击工具中的‘设置’标签并且进入‘许可’界面。



然后，您能够允许远程连接到 FileAudit 审计服务，这样可以避免直接访问 FileAudit 所在的系统。

通过仅仅选择控制台部件，可以在非 IT 审计人员机器上执行定制 FileAudit 安装。一旦完成，打开 FileAudit 并且可以使用‘连接’按钮远程连接到审计服务。