DataApex
Clarity™
CHROMATOGRAPHY SOFTWARE

合规环境

Clarity软件 Chinese

版本号/修正：M132-CHS/80D
日期：2020/9/4

电话: +420 251 013 400
传真:+420 251 013 401
clarity@dataapex.com
www.dataapex.com

DataApex Ltd.
Petrzilkova 2583/13
158 00 Prague 5
The Czech Republic

作者：JaKa

目录/内容

本指南中使用不同的字体来区分**合规环境**手册和Clarity色谱工作站内容。不同字体的含义如下：

仪器(蓝色字体)代表了文章中提到的窗口名称。

打开文件(斜体字)代表了菜单栏的选项和Clarity中某些区域的名称，这些区域可以输入一些参数或者窗口或对话框名称(当您当前打开的工作站界面和我们描述相同时)。

WORK1(大写字母)代表了文件或文件夹的名称。

ACTIVE(大写斜体)代表了工作站或者某些部分的当前状态。

加粗的文本有时也用于文本的重要部分和Clarity工作站的名称。此外，有些章节是用普通文本以外的格式编写的。这些部分的格式如下：

注释： 提示读者相关信息。

注意： 警告用户可能有危险或非常重要的信息。

标记问题声明或复杂问题。

描述： 对问题提出更详细的信息，描述其原因等。

*解决方案：*标记对问题的响应，给出一个如何删除它的流程。

1 什么是合规环境

合规环境就是指任何受控制的环境。规则规定了公司必须满足哪些条件才能产生有效的结果或高质量的产品。

注释： 换句话说，遵守合规环境的规定意味着确保任何对数据的操作都可被重现。**Clarity**将下列类型的文档视为数据：色谱图(*.PRM)、校准曲线(*.CAL)和序列(*.SEQ)。因此，在**Clarity**中，这些文件包含了它们自己的审计追踪日志，而且，色谱文件及其历史也会共同被保存。

为工作环境制定的规程可能来自多个方面，例如公司本身、政府机关和机构(如美国FDA)或监管机构以及其他与确保产品标准化相关的团体。当一个公司要为公众生产可信或质量有保证的成果或产品时，它应遵守有关国家当局对这些过程所定的规则。
本手册的目的是帮助**Clarity**软件的用户遵从这些规则，这些规则是针对特定类型的合规环境发布的。

11 良好实验室规范

良好实验室规范(GLP)包括了一套由OECD定义并由国家当局实施的规范，为实验室研究的规划、执行、监测、记录、报告和存档提供了一个框架。进行这些研究是为了产生数据，用以评估药物(仅临床前研究)、农药、化妆品、食品添加剂、饲料添加剂和污染物、新型食品、杀菌剂、洗涤剂等对使用者、消费者及第三方或环境的危害和风险。GLP有助于向监管当局保证，提交的数据真实反映了研究期间获得的结果，因此可以作为风险或安全评估的依据。

12 CFR 21 Part 11

CFR 21 Part 11是由美国食品药品监督管理局(FDA)发布的指令。它规定了当一个组织打算以电子记录的形式而不是传统的纸质形式提交或存储FDA要求的文件时所必须满足的条件。本指令主要关注的是相对纸质文件而言，电子记录可靠性方面的问题。
主要问题有：

- 系统验证
- 仅授权人员才可访问相关记录
- 记录所有对文件的修改(审计追踪)
- 电子签名

只有将软件功能、整体系统设置和组织定义的标准操作程序结合到一起，才能实现对指令的遵从。

2 如何设置Clarity

设置**Clarity**色谱工作站以满足合规环境条件的过程如下：

- 选择正确的的计算机以及安装正确的操作系统——参阅在第**3**页第**"计算机的安装"**节.
- 安装**Clarity**——参阅在第**4**页第**"安装Clarity"**节.
- 在计算机操作层面为各自的用户账号设置适当的权限——参阅在第**11**页第**"计算机用户权限"**节.
- 设置**Clarity**以符合特定的合规环境要求——参阅在第**6**页第**"具体设置"**节.和在第**44**页第**"Clarity中的用户账号"**节.

21 计算机的安装

计算机系统的硬件配置要求随着**Clarity**的不断发展而变化。具体的版本要求可以在**D016-Clarity-Compatibility-Table**数据表中找到(保存在**Clarity** 安装USB盘上)或者在**DataApex网站**上可以找到。
为了能够在合规环境中工作，还需要一个支持基于单个用户帐号的文件访问限制的操作系统。选择系统时请留意，因为有一些操作系统的版本不支持此功能；例如，**Microsoft Windows 7Home**不允许个人的文件访问限制，而**Microsoft Windows 7Professional**允许。**Clarity**里，支持合规环境的操作系统有：

- Microsoft Windows 7 - 专业版、旗舰版*
- Microsoft Windows 8 - 专业版、企业版*
- Microsoft Windows 8.1 - 专业版、企业版*
- Microsoft Windows 10 - 专业版、企业版*

带有星号的系统支持个人的文件访问，但是还没有经过 Clarity**的测试*

注释： 此条注释之后的所有安装过程都适用于**Windows 7 专业版**、**Windows 8.1 专业版**和**Windows 10 专业版**。当使用其他操作系统时，可能需要更改步骤的顺序。

在安装电脑时，请按照以下步骤进行(如可能)：

- 在计算机上安装操作系统。
- 安装操作系统的可用服务包和更新。
- 设置计算机上需要的用户帐号(详细信息请参阅在第**11**页第**"计算机用户权限"**节.)。
- 安装计算机上所需的任何其他软件及其服务包和更新。
- 安装**Clarity**(参见在第**4**页第**"安装Clarity"**节.)。

22 安装Clarity

注释： 如果要更新到新版本，建议首先在电脑上卸载当前版本的**Clarity**。卸载将在新版本安装开始时自动进行。

安装**Clarity**以符合合规环境要求的过程如下：

- 检查**Clarity**软件安装包是否完整，例如，它的内容要与装箱清单相符。

注意： 注意先不要插入任何硬件或者硬件许可！

- 将**Clarity**的安装USB盘插入电脑。在文件资源管理器(例如windows中的“我的电脑”)中搜索可移动磁盘并运行安装位于根目录中的INSTALL.EXE文件。
- 在第一个页面上，选择安装目录(默认情况下是C:\CLARITY)并按下*下一步*按钮。
- 在下一个页面上设置安装的类型(或在底部窗格中选择特定的安装组件)并按下*下一步*按钮。
- 在**Windows***开始*菜单中选择文件夹的名称，其中将放置各种**Clarity**快捷方式。另外，也可以禁止在*开始*菜单中创建文件夹。然后按下*安装*按钮。
- 输入*注册码*。此注册码可以在提供的**安装用USB盘**的塑料卡背面找到，或由**DataApex**通过电子邮件提供。将文件复制到硬盘驱动器，安装将继续进行。

注意： 如果**Clarity**没有提供注册码，它可以在试用模式下运行。在这种情况下，不要在*注册码*字段中输入任何内容。

- 复制完成后，需要安装或更新各种硬件的驱动程序。单击*下一步*按钮。
- 当更新完成后，需要注册所有*.DLL文件。单击*完成*按钮。
- 单击下一对话框中的*下一步*按钮。在以下选项中，勾选*现在执行IQ报告*复选框并按下*完成*按钮。
- IQ报告将被生成。如果它被标记为已通过(报告中第一个表下面的绿色标签)，则意味着**Clarity**已成功安装。如有需要，请打印及签署IQ报告，并储存以供有关当局查核。

注释： 有时IQ报告会失败。这主要发生在旧版本的**Clarity**安装在计算机的其他目录中时。出现这种情况时，我们建议卸载**Clarity**，删除它的安装目录(如果只是重新安装，请注意在删除之前保存数据)，然后再次安装**Clarity**。如果IQ报告再次失败，请将问题反映给您当地的经销商。

- 如果您想插入内部A/D卡，请关闭计算机。否则，只需重新启动它并跳过以下步骤。
- 将内部A/D卡插入计算机。电脑启动后，按照硬件手册中所述的A/D卡安装程序进行安装。
- 将硬件许可插入USB盘插槽，并按照 **Clarity入门指南**手册中描述的安装过程进行操作。

注释： 如果您使用的是串口(打印机端口)硬件许可而不是USB盘硬件许可，请按照所用许可类型的**Clarity 入门指南**中描述的步骤进行操作。

23 具体设置

每个合规环境都有自己一套必须遵守的规则，但在大多数情况下，这些规则与任何其他系统中的规则非常相似。本章罗列了特定合规环境系统的要求，这些要求参考了为符合上述要求所需遵循的标准操作规程(SOP)。

231 21 CFR Part 11——要求

所提到的**21 CFR Part 11**对**Clarity**的要求可在**DataApex**网站上的D019-CLARITY-21CFR11.PDF数据表中找到。对于**21 CFR Part 11**中规定的大多数要求，必须首先在公司层面设定条件。但是，属于**21 CFR Part 11**规定的以下文章列表由**Clarity**提供(有些是完整的，有些只是部分的)，必要的设置在本手册的中有完整的描述。

2.3.1.1 强制要求

- § 11.10 a，§ 11.10 i—— **Clarity**软件必须经过认证。这是由**DataApex**质量保证系统完成的，请参考在**DataApex**网站上的D028ISO9001-DATAAPEX-CERT.PDF数据表，IQ报告提供了软件安装成功的认证，参阅在第**4**页第**"安装Clarity"**节.
- § 11.10 c——您必须确保在整个记录保留期间数据是被存储的，并且能够被调用——参阅在第**49**页第**"数据存档"**节.
- § 11.10 d，§ 11.10 g ——系统访问权限仅限被授权的个人用户——参阅在第**11**页第**"计算机用户权限"**节.和在第**44**页第**"Clarity中的用户账号"**节.
- § 11.10 e ——在**Clarity**系统中执行的任何操作都必须被记录在安全审计追踪中——参阅在第**48**页第**"记录所有变更"**节.
- § 11.50,§ 11.70,§ 11.100 ——在**Clarity**里，必须能够使用个人独有的电子签名签署电子数据，且电子签名不能够被重复使用，或重新分配给其他任何人，也不能够被修改——参阅在第**62**页第**"电子签名"**节.在第**48**页第**"记录所有变更"**节.
- § 11.200 a ——任何访问或签名必须基于两个不同的身份识别组件才能执行——参阅在第**8**页第**"ClarityGLP选项设置"**节.和在第**62**页第**"电子签名"**节.在第**48**页第**"记录所有变更"**节.
- § 11.300 ——任何安全代码/密码必须对单个用户是唯一的。此外，每一个密码都必须定期检查和修改——参阅在第**44**页第**"Clarity中的用户账号"**节.

232 GLP——要求

为了遵从**GLP**，其中一些要求是强制性的，其他要求只有在应满足**Clarity**某些特殊功能或公司的特殊条件时才需要。以下清单中的步骤分为强制和可选两种。每个要求链接到下一章的相应部分，其中包括满足要求的一般性指南和特定的SOP。

2.3.2.1 强制要求

- 安装**Clarity**的计算机必须让每个用户都有相应的设置好的权限——参阅在第**11**页第**"计算机用户权限"**节.
- 在**Clarity**中文件覆盖必须被禁止。由于这个或任何类似原因而造成的数据丢失是不允许的——参阅*注释*一节，在在第**11**页第**"计算机用户权限"**节.
- 每个有权限访问**Clarity**的用户都必须拥有自己的用户账号，并有自己的密码和访问权限来界定他/她可以执行哪些操作——参阅在第**44**页第**"Clarity中的用户账号"**节.
- 数据中的每一项变更都必须被正确的记录——参阅在第**48**页第**"记录所有变更"**节.
  - 变更的原因必须与变更本身一起被记录下来，以便后续可以找到变更的原因——参阅在第**48**页第**"变更原因记录"**节.
- 所有数据必须在相关部门规定的时间内存档——参阅在第**49**页第**"数据存档"**节.

注意： 为了保持良好的数据完整性，运行**Clarity**的工作人员(通常是实验室工作人员)**不得**有任何特权更改运行**Clarity**的计算机上的Windows系统时间。如果不满足此条件，则很容易损害*审计追踪*中时间戳的正确性和完整性，因为它们在执行任何操作时记录的是当前Windows系统时间。

2.3.2.2 可选要求

- 当质量控制/质量评估人员在场时——质量保证人员应该有自己的权限进入**Clarity**工作站，且无权改变任何数据——参阅
- 当使用用户计算时——所有用户必须在用户计算栏中具有相同的设置——参阅在第**52**页第**"共享桌面文件"**节.
- 多工作站环境——当用户(或多个用户)需要在多台计算机上工作时，所有用户的用户帐户(以及存储的密码)在所有地方应该都是一样的——参阅在第**61**页第**"多工作站环境"**节.

3 解决方案和SOP

本章列出了一套针对特定合规环境问题的解决方案和标准操作规程(SOP)，以满足特定合规环境平台的要求。SOP应严格执行，并按照在第2页第**"如何设置Clarity"**节.章节中指定平台推荐的顺序执行。

31 ClarityGLP选项设置

此步骤用于在**Clarity**中进行基本的合规环境设置。默认情况下，**Clarity**工作站中所有的合规环境选项都是被禁用的。你可以自行决定是否选择合规，因为一些用户可能不需要整个合规环境，而将工作站设置为合规环境条件只会使他们的工作变得复杂而缓慢。

311 SOP ——GLP选项设置

要将**Clarity**设置成符合合规环境的基本条件，请执行以下步骤:

注释： 如果工作站已经设置为用户账号模式，则只有拥有*管理员*权限的用户才能打开GLP选项对话框。

- 打开**Clarity**工作站。在Clarity主窗口，使用*系统——GLP选项...*命令进入GLP选项对话框。

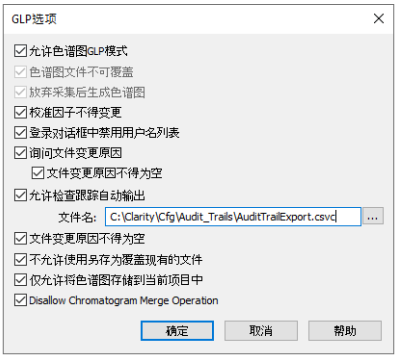


图1 GLP选项

- 为防止从色谱图中丢失任何数据，请勾选*允许色谱图GLP模式*复选框。如果在选定的目录中已经存在同名文件(在新文件的末尾添加一个6位数字)，这将消除覆盖色谱图的可能性；如果由于任何原因分析中止，色谱图将会生成。该功能是**21 CFR Part** 11和**GLP**所要求的，因此必须禁用文件覆盖，并禁用由此或任何类似原因导致的可能的数据丢失。

注释： 如果在Clarity未启用*GLP模式*的情况下，打开在*GLP模式*下创建的色谱图，则该色谱图将始终以只读方式打开。

- 若要防止在校准窗口中手动更改响应，请勾选*校准因子不得变更*复选框。手动更改会在校准审计追踪中被标记出来，但它破坏了校准标样和校准曲线本身之间的链接，并且它在链接到校准文件的色谱图中无法识别。该功能是**21 CFR Part 11**和**GLP**所要求的。
- 要禁止在登录对话框中显示所有可用的**用户名**，请勾选*登录对话框中禁用用户名列表*复选框。然后，用户需要输入两个特有的身份识别组件才能成功登录。该功能是**21 CFR Part 11**所要求的。
- 要将**Clarity**设置为提示用户填写变更原因，请勾选*询问文件变更原因*复选框。保存或修改色谱图、方法、序列、校准或GPC校准文件或其他**Clarity**设置，如(系统配置或用户帐号)，色谱图(方法、序列、...)变更原因，将出现更改对话框。用户可以填写变更的原因。

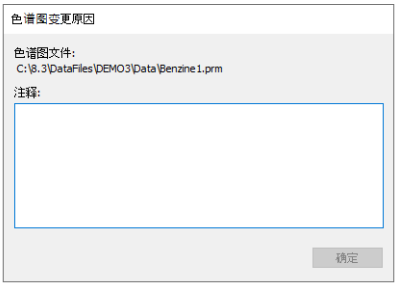


图2 色谱图变更原因

GLP要求为每个变更填写变更的原因。为了确保原因字段不为空，请在GLP选项对话框中勾选*文件变更原因不得为空*复选框。只有在对话框中填写了文本的理由才是有效的。该功能是**21 CFR Part 11**和**GLP**所要求的。

注释： 变更原因显示在**审计追踪**中，并用短划线与"文件已保存"事件分隔。

- 若要自动导出审计追踪，请勾选*允许审计追踪自动输出*复选框。只要**Clarity**是打开的，导出的文件就会被标记为只读。对该导出文件的更改将持续进行。这个功能不是任何合规环境平台要求的，只是它可以帮助QA人员代表检查审计追踪，而不需要让他们访问**Clarity**本身。
- 若要禁用*毛刺峰过滤*和*毛刺峰移除*操作,此操作可能会显著改变信号线，请勾选*禁用毛刺峰过滤和毛刺峰移除*复选框。当然，这些参数的使用会被记录在审计追踪中，也可以从积分表中看到，但是因为这些参数会改变信号(可能会删除色谱图中的峰)，因此最好禁用它们。
- 若要禁止用户覆盖现有文件，请勾选*不允许使用另存为覆盖现有文件*复选框。这个功能适用于任何由**Clarity**创建的文件(方法、校准、色谱图等)。会弹出警告信息，用户必须以不同的文件名保存。
- 选项*仅允许将色谱图存储到当前项目中*是一个工具，它禁止将任何新生成的色谱图存储到当前项目的工作子文件夹(通常是*Data*或*Calib*)之外。此选项禁止将任何新生成的色谱图直接存储到当前项目的根目录

中。它还禁止直接在当前项目的根目录中自动创建新的子文件夹。它将允许在当前项目的一个工作子文件夹(通常是*Data*或*Calib*)中存储新生成的色谱图。此功能旨在支持数据完整性，因为它将禁止在可能不适用的目的地创建数据，在第**11**页第**"计算机用户权限"**节.中有描述。关于该功能的详细描述在GLP选项主题**Clarity**帮助中给出。

32 计算机用户权限

安装**Clarity**的计算机必须让每个用户都有相应设置好的权限。
这些设置只能由系统管理员设置，最好在安装计算机期间设置。该功能是**21 CFR Part 11**和**GLP**要求的。以下是一些有关电脑系统的一般建议：

注释： 这些建议并不是适用于每台计算机的通用SOP，因为计算机系统和一般公司的情况在这一领域中可能有很大的不同。但是，所提供的软件已经在四个选定的计算机操作系统上进行了测试——**Windows 7 专业版**、**Windows 8.1 专业版**以及 **Windows 10 专业版**。

- 将运行**Clarity**的计算机只能使用具有特定权限的用户帐号，这些权限在本章的以下子标题中进行了描述。拥有管理员权限的用户帐号应该留给公司的IT人员，他们不应参与**Clarity**中电子记录的创建。这些特定设置的理由在本节后面的*说明*中进行了描述。
- 每个**Clarity**用户必须在操作系统上有自己的用户帐号。
- **Clarity**的所有用户帐号都必须拥有**Clarity**文件夹中的**Cfg**和**DataFiles**子文件夹设置权限。如果**Clarity**文件夹的子文件夹**DataFiles**的默认名称改变或这个文件夹位于**Clarity**文件夹之外(例如在一个定期备份网盘)，用户权限必须以同样的方式设置为默认的名称或子文件夹的位置。**Clarity**创建的数据将存储在**DataFiles**文件夹，它的位置修改可以通过**Clarity***主窗口*，*系统*菜单，*目录...*中进行设置。
- **Clarity**用户创建的数据不能存储在**Bin**子文件夹中。

注释： 整个过程将确保计算机用户无法在**Clarity**环境之外更改或删除由**Clarity**创建的任何数据。修改数据的唯一方法是在**Clarity**环境中进行，并且所有的操作都将被记录。由于本地IT人员必须拥有管理员权限，因此他们仍然有权在**Clarity**环境之外修改或删除数据，而**Clarity**审计追踪没有任何记录。所以必须建立不同类型的防护措施，以防本地IT人员可能出现的错误和权限的滥用。本地IT部门和其他人事管理部门(如QC、QA等)必须了解这一事实。

321 SOP——在Windows 7中设置用户权限

注释： 本SOP是在安装了**Windows 7 专业版**操作系统(英语本地化)、Service Pack 1和最新升级安装(至2014年7月28日)的计算机上编写和测试的。

本演示中描述的整个流程必须由拥有系统*管理员*权限的人员(例如，公司IT工作者)来执行。默认计算机是新安装的，除了管理员帐号外没有其他用户帐号。**Clarity**已安装好。如果已经存在用户帐号(例如，计算机通过域用户帐号连接到域)，负责本操作的IT工作者需要对已经存在的用户帐号执行以下操作。

- 打开计算机管理窗口，点击*Windows开始*图标，在搜索栏中输入“计算机管理”文本，选择*计算机管理*项。*计算机管理*窗口将打开。导航到*本地用户和组*项目下找到*用户*项。

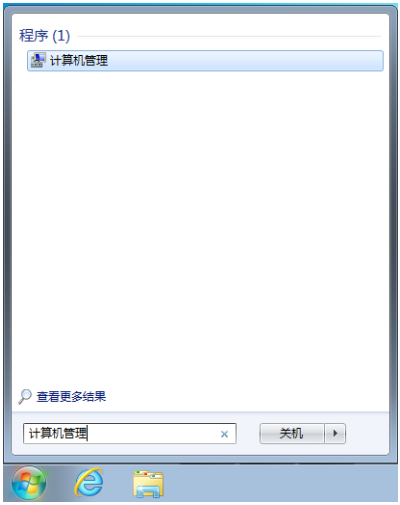
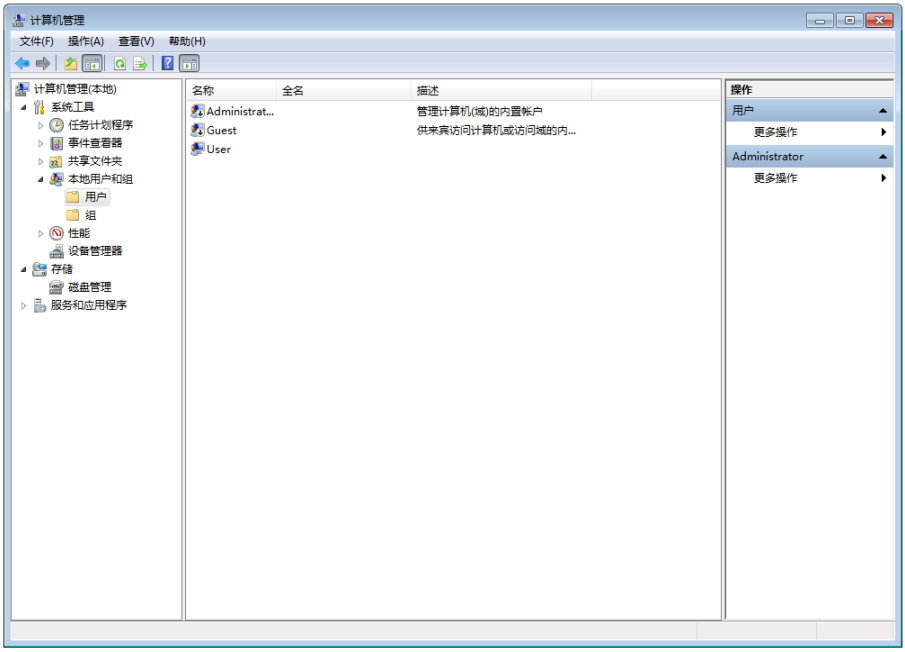


图3 开始——计算机管理



- 创建一个新的计算机用户：
  - 单击*更多操作*命令(或使用鼠标右键调用上下文菜单)并选择*新用户...*。在*新用户*对话框中填写所有空栏并设置密码。它的设置基于安装**Clarity**的机构的政策，单击*创建*按钮。

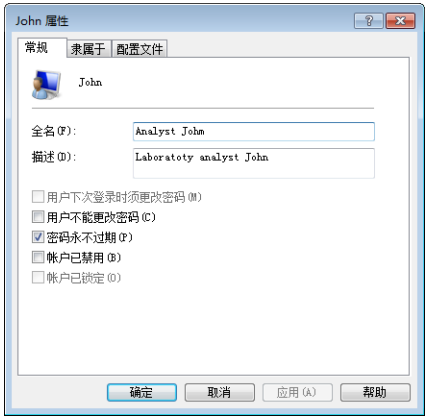


图4 创建新用户

- 对每个要添加的其他用户重复此过程。

- 检查并确保应运行Clarity的用户的所有用户帐号都是*用户*组的成员。为此，单击每个创建的用户并通过鼠标右键调用上下文菜单并选择*属性*，将弹出一个新窗口。然后单击*隶属于*选项卡并检查用户组中相应用户的成员身份。

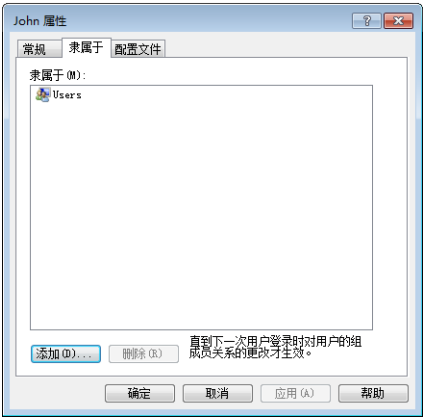


图5 用户组

- 然后，必须先为所有新创建的用户执行首次登录。这个步骤是强制性的，必须在这个阶段执行，不能稍后再执行。延迟登录可能会危及稍后执行的所有设置，并威胁到Clarity创建的所有记录的“电子”安全性。

注释： 在第一次登录时，默认情况下，操作系统会将新创建的用户自动添加到*Authenticated User*组中。为了使Clarity功能在GLP下正常运行，*Authenticated User*必须不能访问**Cfg**和**DataFiles**，因此必须删除该组(原因在下面的步骤中进行了说明)。

- 然后，具有*管理员*权限的本地管理员必须登录操作系统并继续执行以下步骤。
- 使用例如**Windows** 资源管理器等查找**Clarity**的安装目录。
- 更改你之前为子文件夹**Cfg**和**DataFiles**(无论**DataFiles**子文件夹位于何处)添加的用户账号的权限：
  - 右键单击子文件夹**Cfg**并从上下文菜单中选择*属性*命令。
  - 切换到安全选项卡。
  - 选择*高级*，然后*Cfg的高级安全设置窗口*会打开。

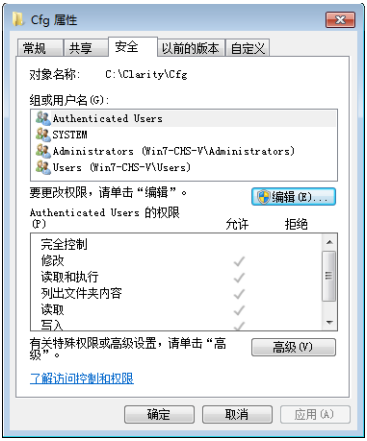


图6 Cfg文件安全属性

图7 高级安全设置——初始状态

- 单击*更改权限*按钮，该按钮将调用权限设置的新窗口。在下一个对话框中取消勾选选项*包括可从该对象的父项继承的权限*，这将调出*Windows 安全*窗口。在这个*Windows 安全*窗口点击*删除*按钮，这将导致在*Cfg的高级安全设置*窗口中的权限条目被消除。请参考下面的两个屏幕截图和清除*Cfg的高级安全设置*窗口的结果。

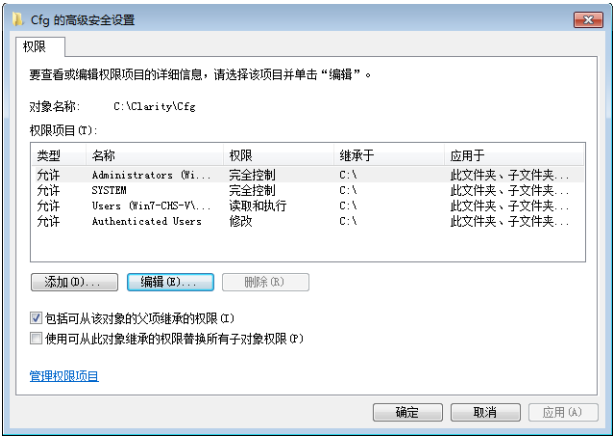


图8 高级安全设置——中间状态

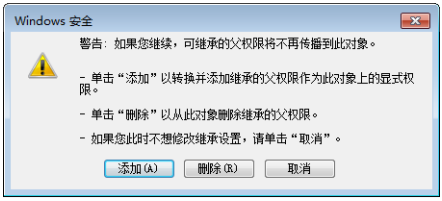


图9 Windows安全

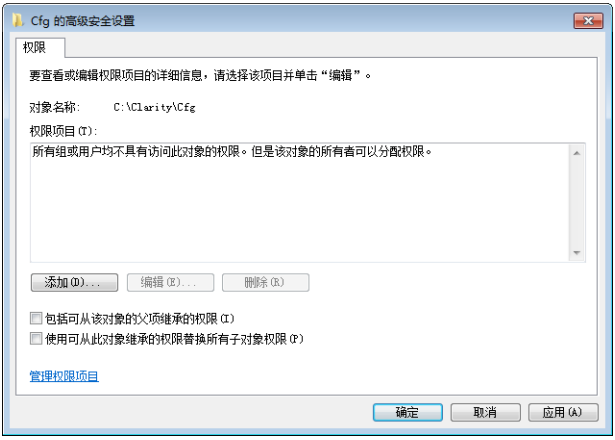


图10 高级安全设置——清除状态

- 单击*添加...*按钮将调用出一个用于选择用户或组的新窗口。单击*高级*按钮，它将调用*选择用户或组*窗口。单击*立即查找*按钮，并选择要运行**Clarity**的用户帐号。

图11 选择用户——初始

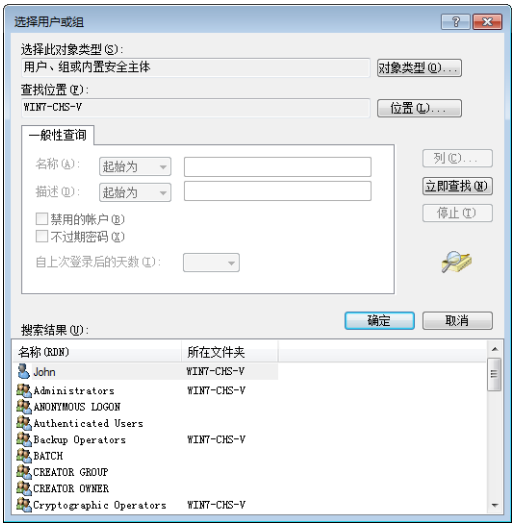


图12 选择用户——中间

图13 选择用户——最终

- 为要运行**Clarity**的用户的用户帐号选择必要的权限，如下所示。在*允许*栏中选中*完全控制*，然后取消选中以下项目：*删除子文件夹及文件*, *删除*, *更改权限* 和 *取得所有权*。*拒绝*栏必须保持全部不勾选。

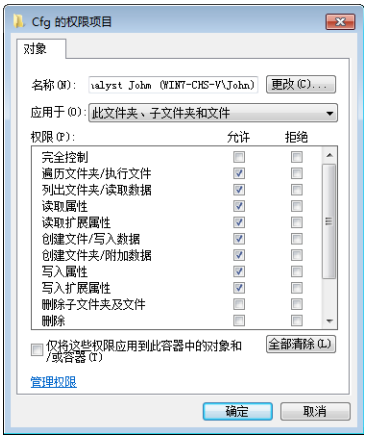


图14 用户的权限项目

- 为要运行**Clarity**的用户的所有用户帐号和本地*管理员*用户帐号，对*Cfg*文件夹重复此过程。*管理员*用户帐号应该具有*允许*栏中列出的所有权限，*拒绝*栏选框必须全部不勾选。

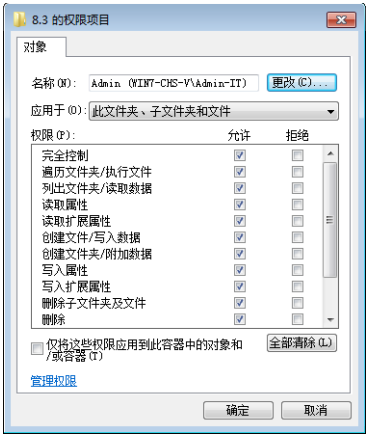


图15 管理员的权限项目

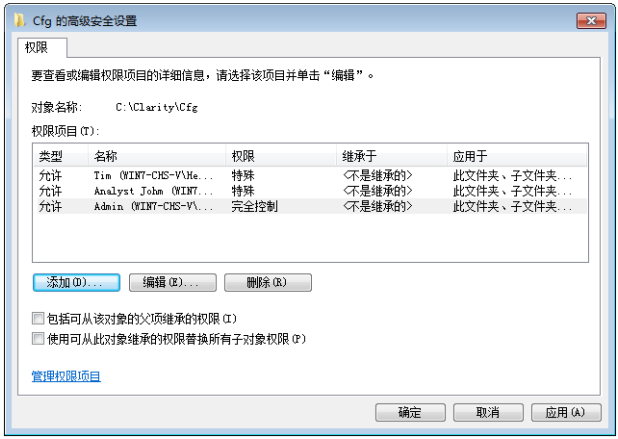


图16 Cfg文件夹的高级安全设置

- 如果需要，可以从*Cfg 属性*窗口的安全选项卡查看相应的用户设置。

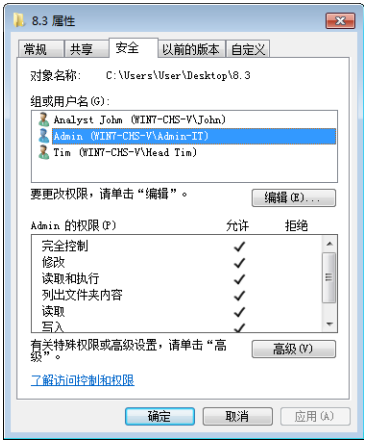


图17 管理员的Cfg文件夹安全属性

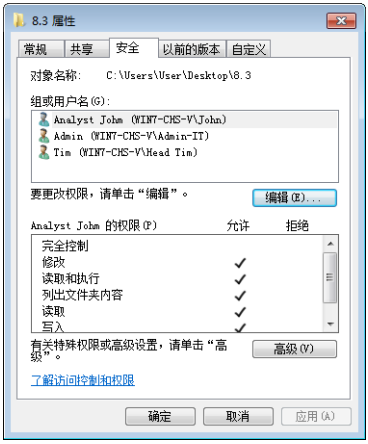


图18 用户的Cfg文件夹安全属性

- 对于要以相同方式运行**Clarity**的所有用户帐号和本地*管理员*用户帐号，对*DataFiles*文件夹重复此过程。

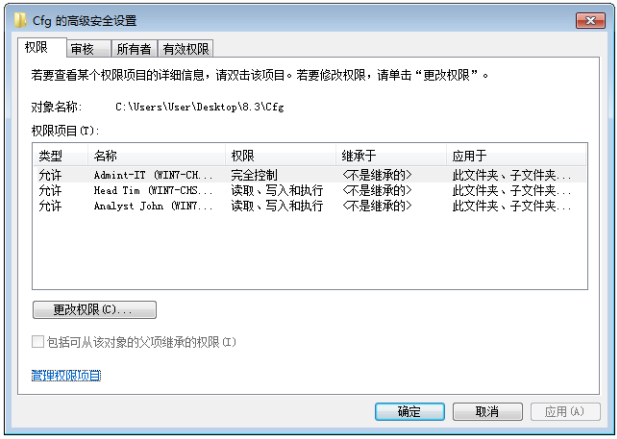


图19 DataFiles 文件夹的高级安全设置

- 运行**Clarity**的用户的所有用户帐号都可以直接从*Windows开始菜单*在各自的*桌面*上创建**Clarity**的快捷方式。

322 SOP ——在Windows 8.1中设置用户权限

注释： 本SOP是在安装了**Windows 8.1 专业版**操作系统(英语本地化)、Service Pack 1和最新升级安装(至2014年7月28日)的计算机上编写和测试的。

本简介中描述的整个流程必须由具有系统*管理员*权限的人员(例如公司IT工作者)来执行。默认计算机是新安装的，除了管理员帐号外没有其他用户帐号。**Clarity**已安装好。如果已经存在用户帐户(例如，计算机通过域用户帐户连接到域)，负责本操作的IT工作者需要对已经存在的用户帐户执行以下操作。

- 打开计算机管理窗口，右键单击*Windows开始*图标调出上下文菜单，选择*计算机管理*项。在计算机管理窗口，导航到*本地用户和组*项目下找到*用户*项。

图20 开始——计算机管理

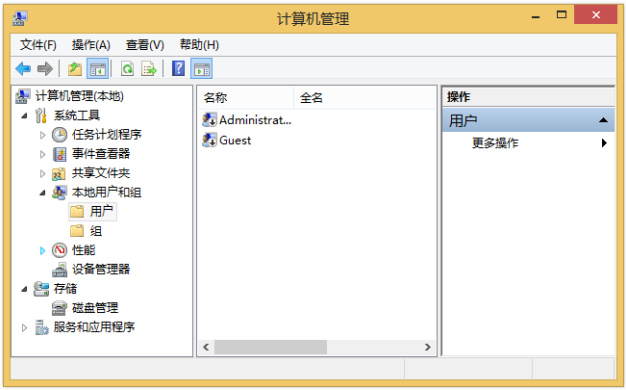


图21 计算机管理

- 创建一个新的计算机用户：
  - 单击*更多操作*命令(或使用鼠标右键调用上下文菜单)并选择*新用户*...。在*新用户*对话框中填写所有的空白栏，根据安装**Clarity**的机构的规定设置密码及其设置，然后单击*创建*按钮。

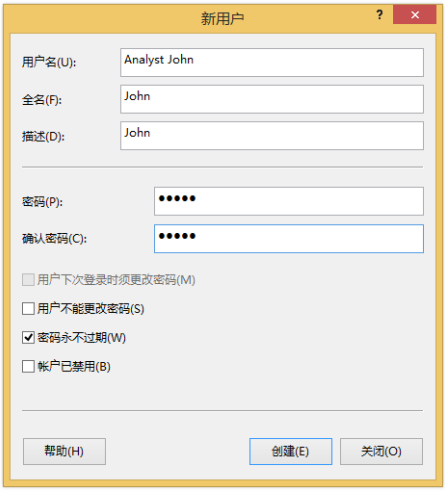


图22 创建新用户

  - 对每个要添加的其他用户重复此过程。
  - 检查并确保应运行Clarity的用户的所有用户帐号都是*用户*组的成员。为此，单击每个创建的用户并通过鼠标右键调用上下文菜单并选择*属性*，将弹出一个新窗口。然后单击*隶属于*选项卡并检查用户组中相应用户的成员身份。

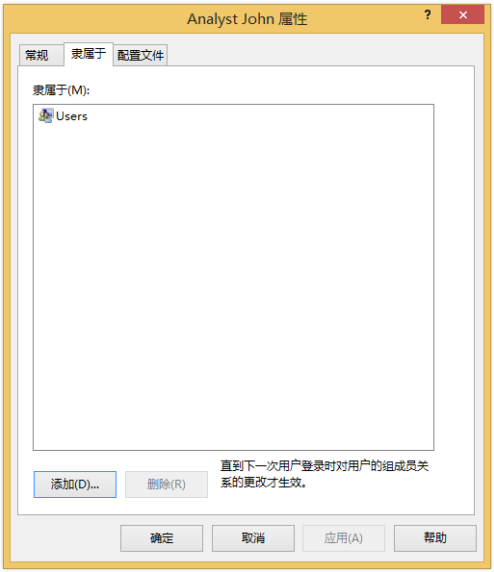


图23 用户组

- 然后，需要先对所有新创建的用户进行首次登录。这个步骤是强制性的，必须在这个阶段执行，不能稍后再执行。延迟执行登录可能会危及稍后执行的所有设置，并威胁到Clarity创建的所有记录的“电子”安全性。

注释： 在第一次登录时，默认情况下，操作系统会将新创建的用户自动添加到已*Authenticated User*组中。为了使Clarity在GLP中功能正常运行，*Authenticated User*必须不能访问**Cfg**和**DataFiles**，因此必须删除该组(原因在下面的步骤中进行了说明)。

- 然后，具有管理员权限的本地*管理员*必须登录操作系统并继续执行以下步骤。
- 使用例如**Windows** 资源管理器等查找**Clarity**的安装目录。
- 更改您先前为子文件夹**Cfg**和**DataFiles**(无论**DataFiles**子文件夹位于何处)添加的用户账号的权限：
  - 右键单击子文件夹**Cfg**并从上下文菜单中选择*属性*命令。
  - 切换到安全选项卡。
  - 点击*高级*选项，然后*Cfg的高级安全设置*窗口会打开。

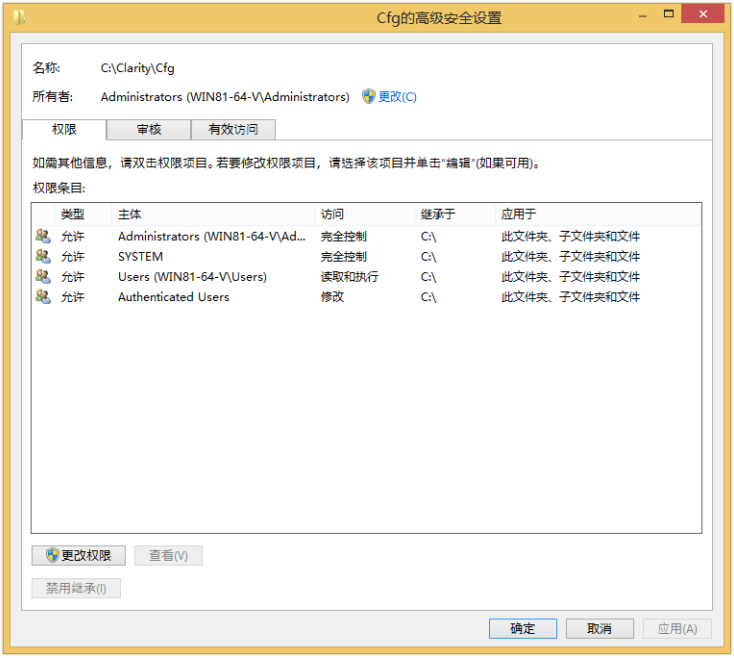


图24 高级安全设置

- 单击*更改权限*按钮，它将调用权限设置的新窗口。在下面的*阻止继承*窗口中，单击*从此对象中删除所有已继承的权限*项。*高级安全设置*窗口中的*权限*选项卡会被清除，不会包含任何权限条目。

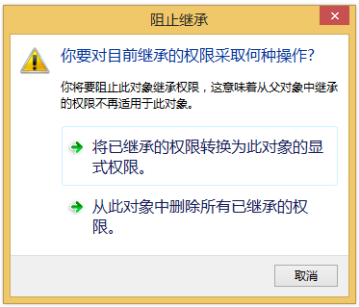


图25 阻止继承

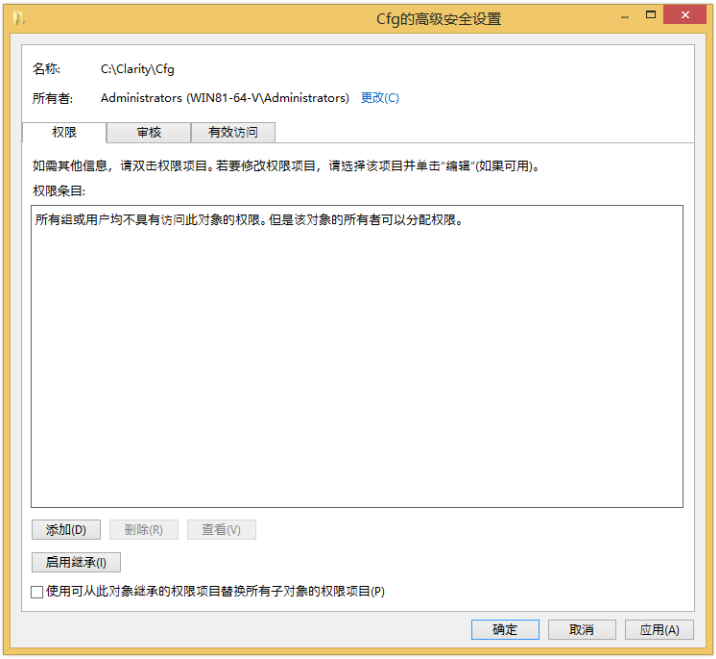
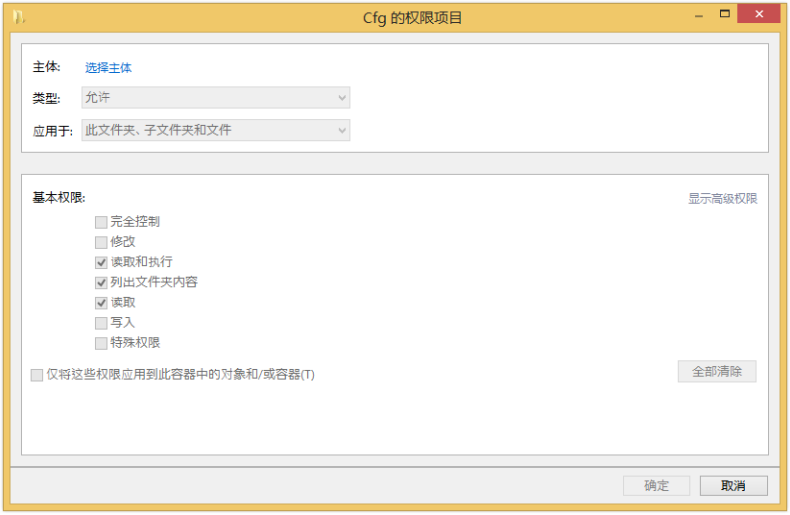


图26 已清除的高级安全设置

- 单击*添加*按钮，它将调用权限设置的新窗口。选择*选择主体*将调出*选择用户或组*窗口。



- 使用高级选择要运行**Clarity**的用户的账号。

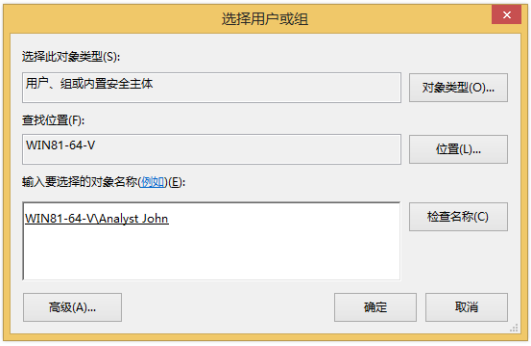


图27 选择用户

- 为**Clarity**的用户帐户选择必要的权限，如下所示。首先，单击*显示高级权限*，勾选*完全控制*，然后取消勾选下列项：*删除子文件夹和文件*、*删除*、*更改权限*和*取得所有权*。仅对窗口上部的*类型*：下拉菜单中的*允许*项执行这些设置。

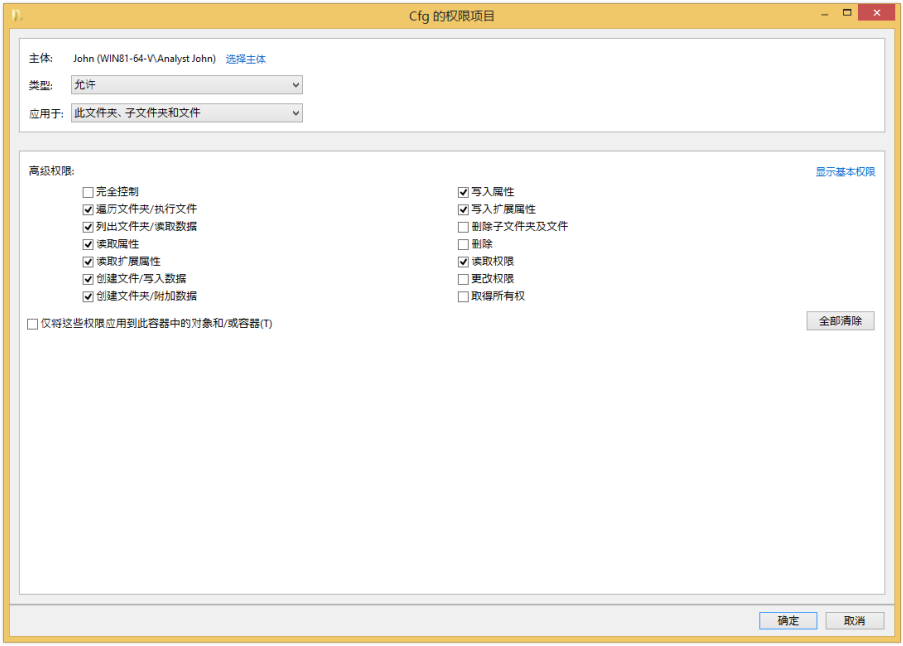


图28 用户权限

- 需要运行**Clarity**的用户的所有用户账号和本地*管理员*用户账号，应对***Cfg***文件夹重复此操作。*管理员*用户帐号应该具有所有权限。

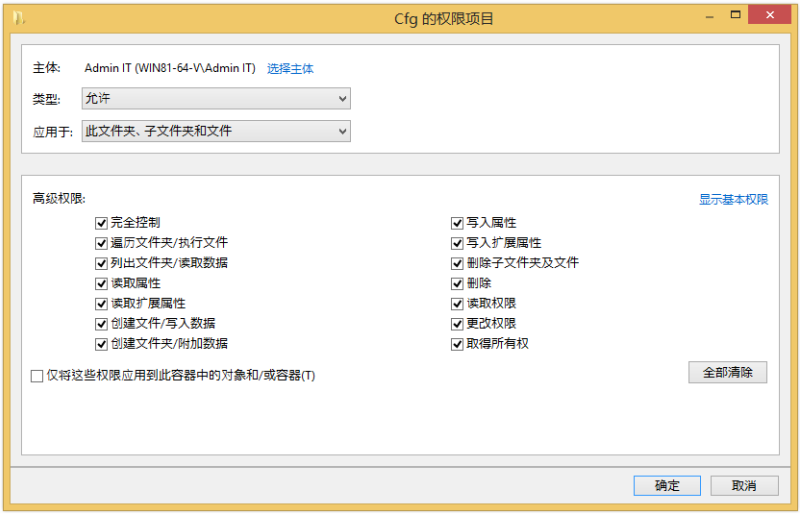


图29 管理员权限

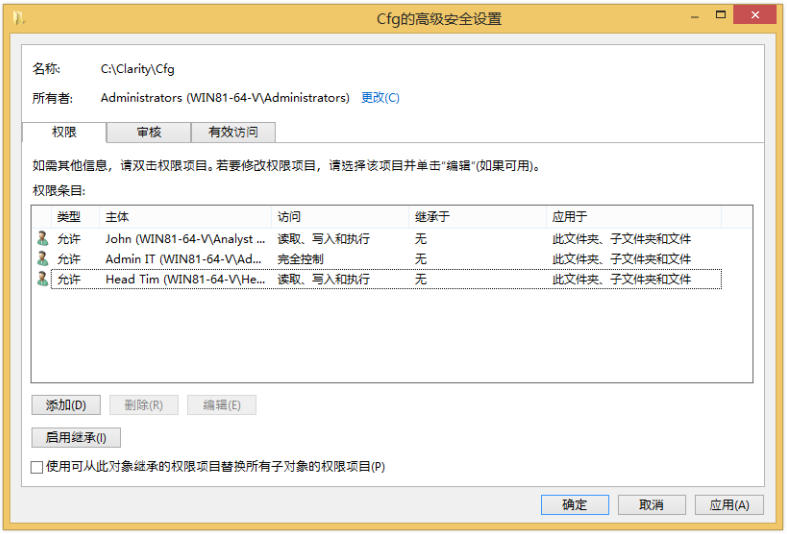


图30 Cfg文件夹的高级安全设置

- 所有**Clarity**的用户账号，包括本地*管理员*账号，都要对*DataFiles*文件夹重复以上的操作进行设置。

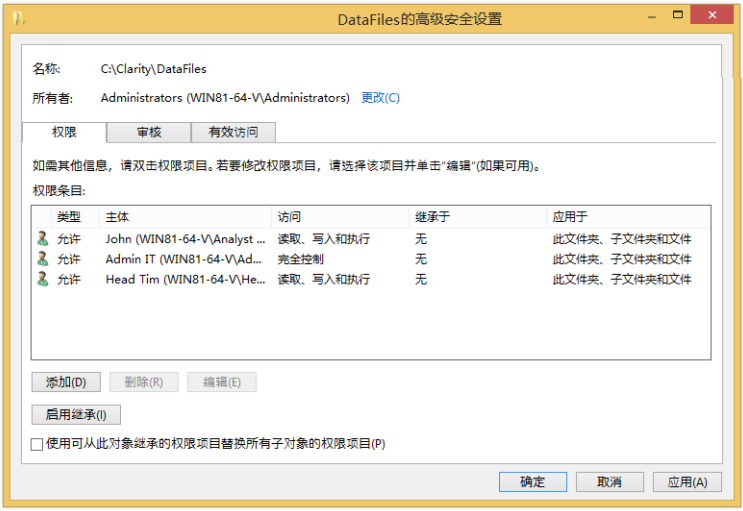


图31 DataFilesr文件夹的高级安全设置

- 所有**Clarity**的用户账号都可以直接从*Windows开始菜单*在各自的*桌面*上创建**Clarity**的快捷方式。

323 SOP——在Windows 10中设置用户权限

注释： 本SOP是在安装了**Windows 10 专业版**操作系统(英语本地化)及所有最新升级安装(至2016年6月22日)的计算机上进行编写和测试的。

本演示中描述的整个流程必须由具有系统*管理员*权限的人员(例如，公司IT工作者)来执行。默认计算机是新安装的，除了管理员账号外没有其他用户账号。**Clarity**已安装好。如果已经存在用户账号(例如计算机以域用户账户连接到域)，负责本操作的IT工作者需要对已经存在的用户帐户执行以下操作。

- 打开计算机管理窗口，将鼠标移动到*Windows开始菜单*的*Windows*图标上，单击鼠标右键调用上下文菜单，选择*计算机管理*项。*计算机管理*窗口将打开。导航到*本地用户和组*项下可用的*用户*。

图32 Windows——计算机管理

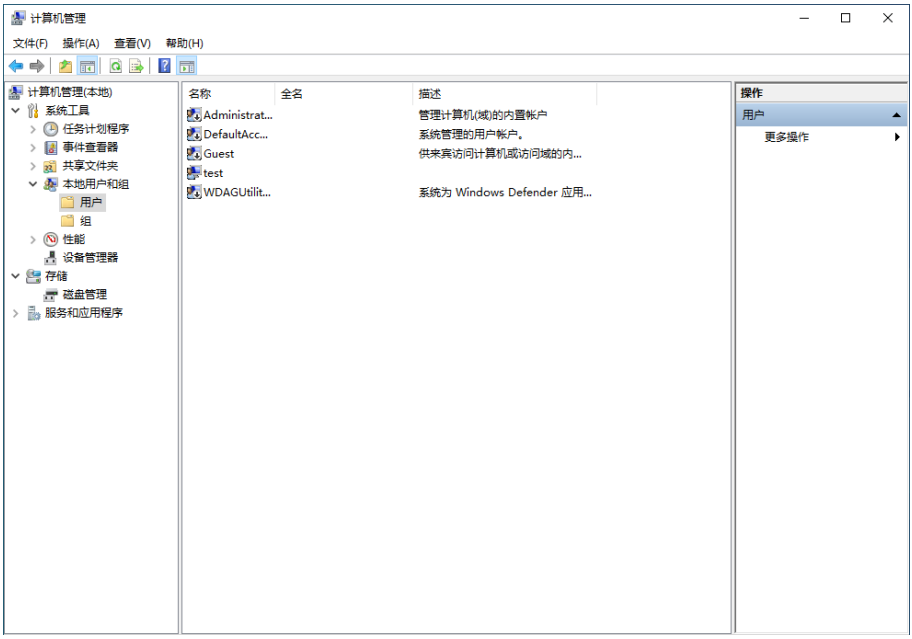


图33 计算机管理

- 创建一个新的计算机用户：
  - 单击*更多操作*命令(或使用鼠标右键调用上下文菜单)并选择*新用户*...。在*新用户*对话框中填写所有的空字段，根据安装**Clarity**的机构的政策设置密码及其他设置，然后单击*创建*按钮。

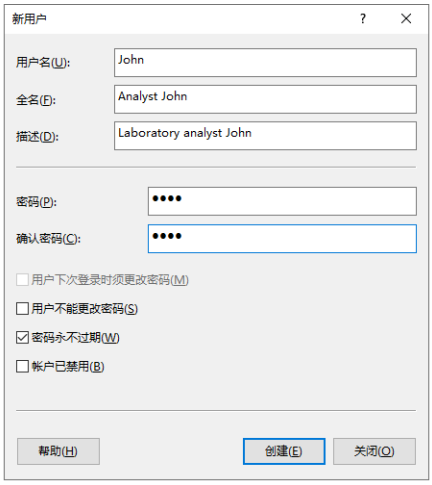


图34 创建新用户

- 重复以上步骤来添加其他你想添加的额外用户。
- 检测并确保Clarity的用户账号都在*用户*组里。要做到这一点，可以右键单击每个已创建的用户打开上下文菜单，选择*属性*项，将弹出一个新的窗口。然后点击*隶属于*选项卡，并检查各个用户组的用户成员。

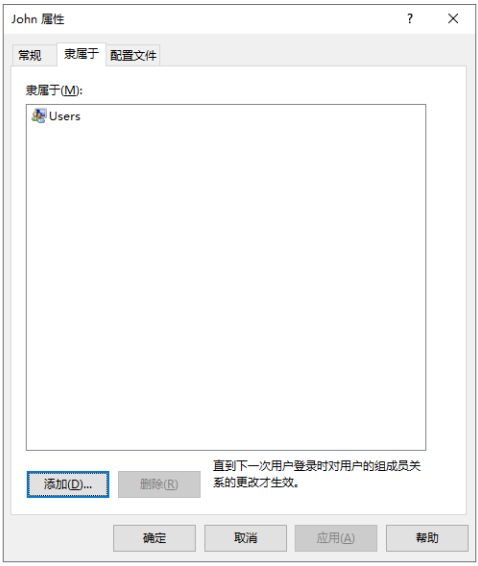


图35 用户组

- 然后，需要先对所有新创建的用户进行首次登录。这个步骤是强制性的，必须在这个阶段执行，不能稍后再执行。延迟登录可能会危及稍后执行的所有设置，并威胁到Clarity创建的所有记录的“电子”安全性。

注释： 在第一次登陆时，新建用户都会被系统默认分进*Authenticated User*组。为了使Clarity在GLP下运行正常，*Authenticated User*必须不能访问**Cfg**和**DataFiles**，因此必须删除此组(在下面的步骤中进行了说明)。

- 然后具有管理员特殊权限的本地*管理员*必须登录操作系统，并继续执行以下步骤。
- 使用例如**Windows**资源管理器等查找**Clarity**的安装目录。
- 更改您先前为子文件夹**Cfg**和**DataFiles**(无论**DataFiles**子文件夹位于何处)添加的用户账号的权限：
  - 右键单击**Cfg**子文件夹并从上下文菜单中选择*属性*命令。
  - 切换到安全选项卡。
  - 点击*高级*选项，然后*Cfg的高级安全设置*窗口会打开。

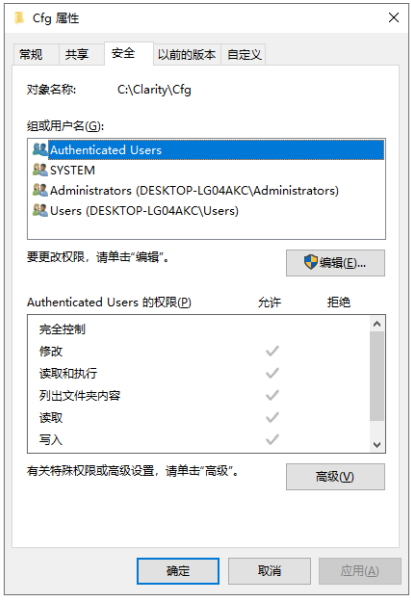


图36 Cfg文件夹安全属性

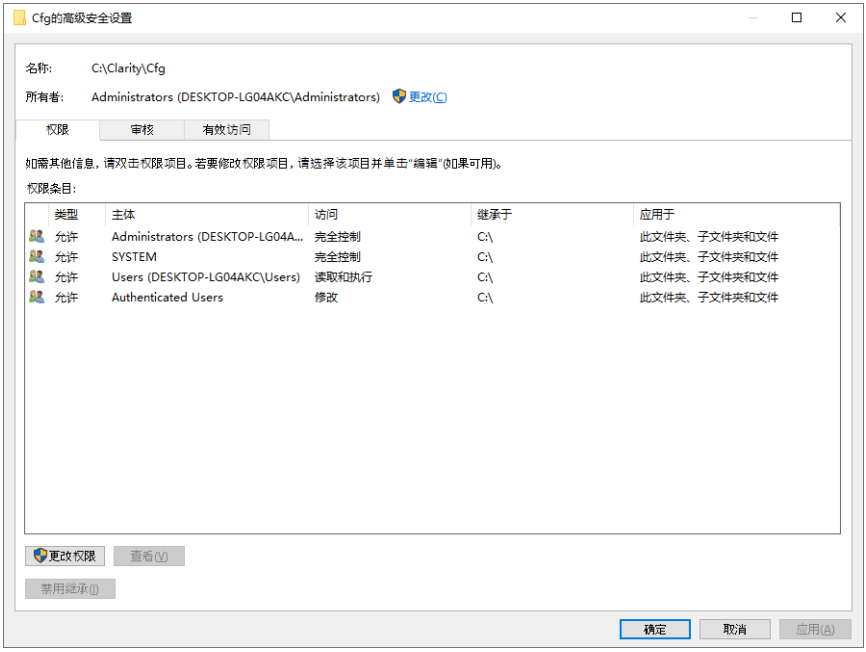


图37 高级安全设置——初始状态

- 单击*更改权限*按钮，它将调用权限设置的新窗口。单击*禁用继承*按钮，将调用新的*阻止继承*窗口。单击*从此对象中删除所有已继承的权限*选项，将清除***Cfg****的高级安全设置*窗口中的权限条目。

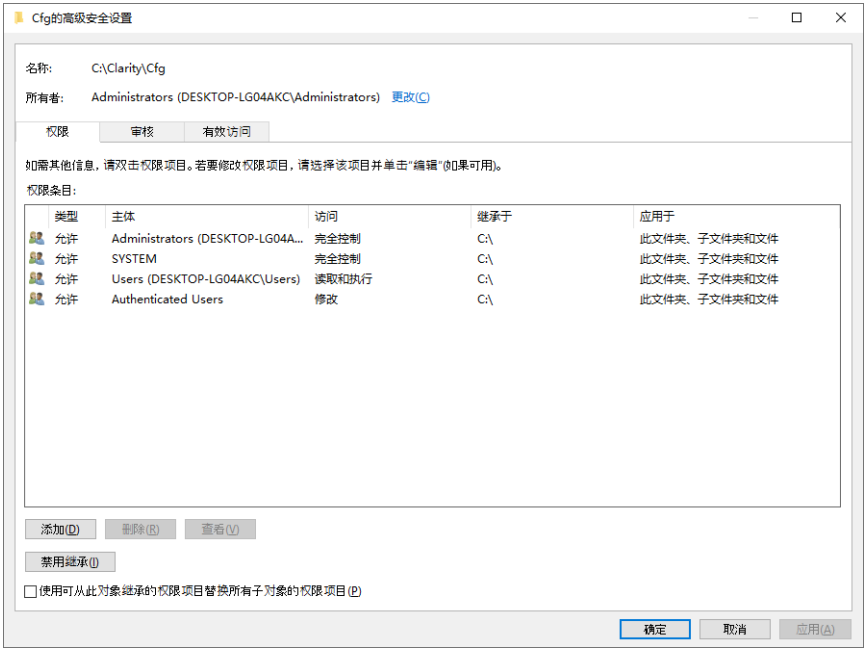


图38 高级安全设置——中间状态

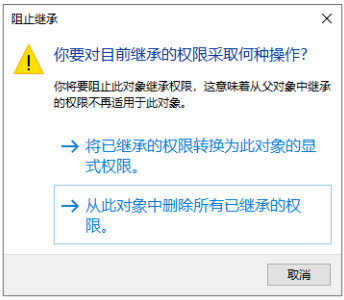


图39 阻止继承

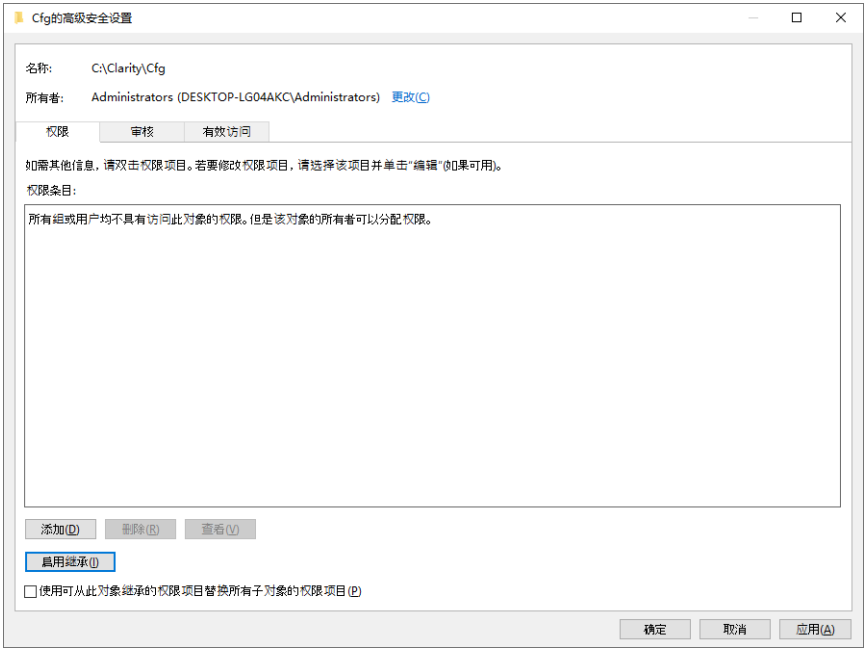
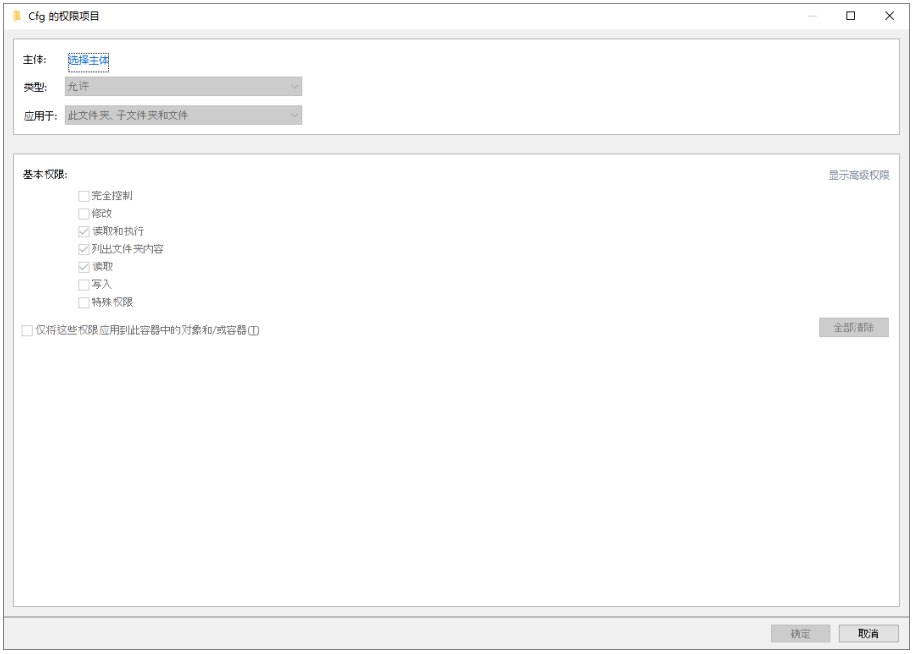


图40 高级安全设置——无项目

- 单击*添加*按钮，它将调用权限设置的新窗口。单击*选择主体*将调用*选择用户或组*的窗口。



- 单击高级...按钮选择应该运行**Clarity**的用户。

图41 权限项目

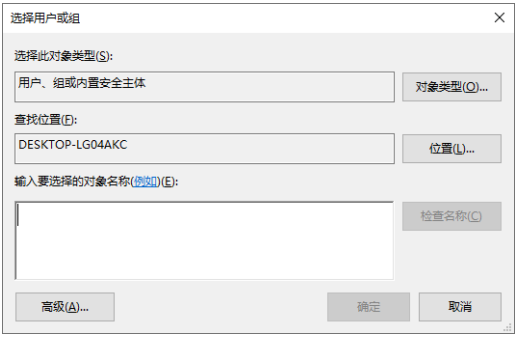


图42 选择用户——初始

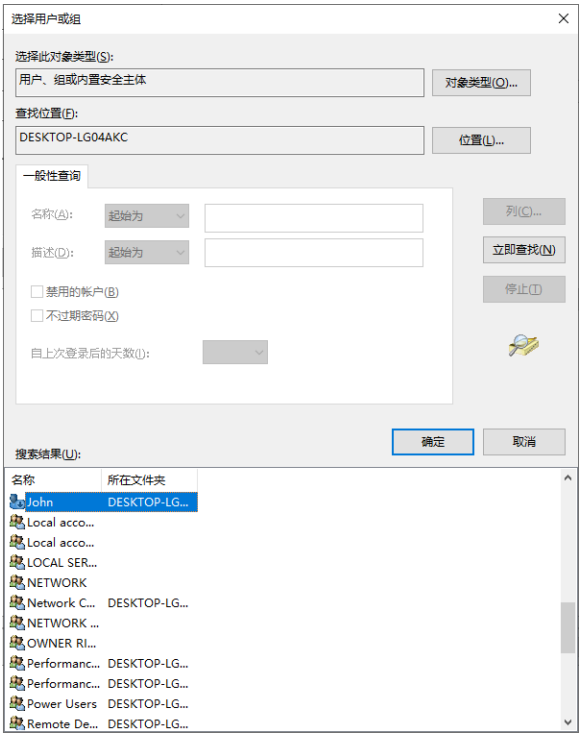


图43 选择用户——中间

图44 选择用户——最终

- 为**Clarity**的用户账号选择必要的权限，如下所示。首先，单击*显示高级权限*，选中*完全控制*项，然后取消下面的选择项目：*删除子文件夹和文件*，*删除*，*更改权限*和*取得所有权*。仅对窗口上部的*类型*：下拉菜单中的*允许*项执行这些设置。

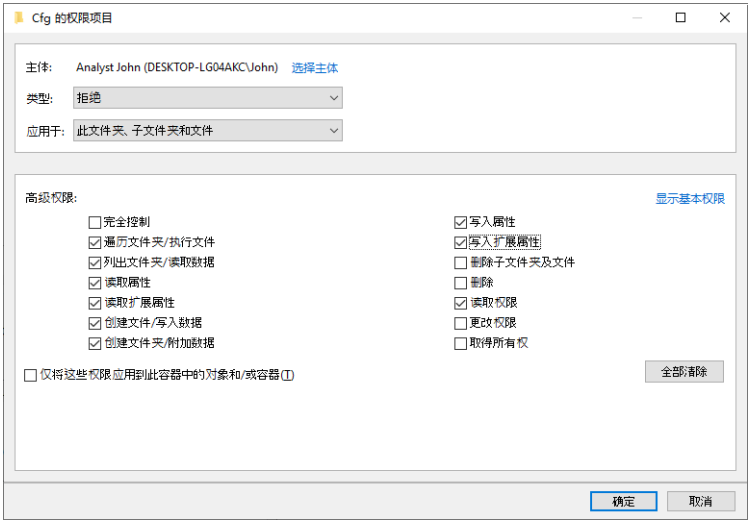


图45 用户权限项目

- 为需要运行**Clarity**的用户的所有用户账号和本地*管理员*用户账号，对*Cfg*文件夹重复此操作。本地*管理员*用户账号应该具有所有权限。

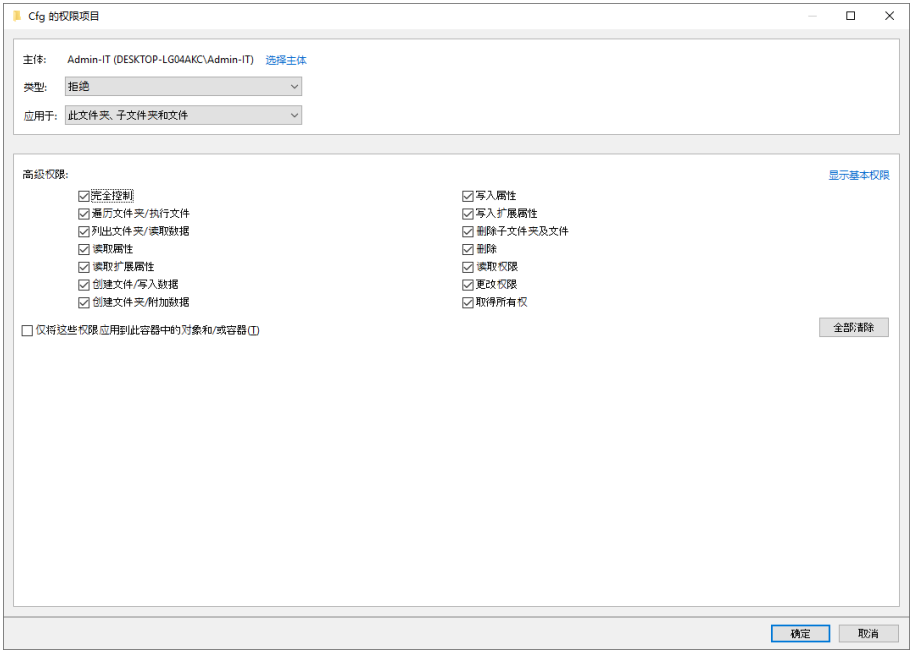

Cfg 的权限项目
主体: Admin-IT (DESKTOP-LG04AKC\Admin-IT) 选择主体
类型: 拒绝
应用于: 此文件夹、子文件夹和文件
高级权限:
显示基本权限
完全控制
遍历文件夹/执行文件
列出文件夹/读取数据
读取属性
读取扩展属性
创建文件/写入数据
创建文件夹/附加数据
写入属性
写入扩展属性
删除子文件夹及文件
删除
读取权限
更改权限
取得所有权
仅将这些权限应用到此容器中的对象和/或容器(T)
全部清除
确定
取消

图46 管理员权限项目

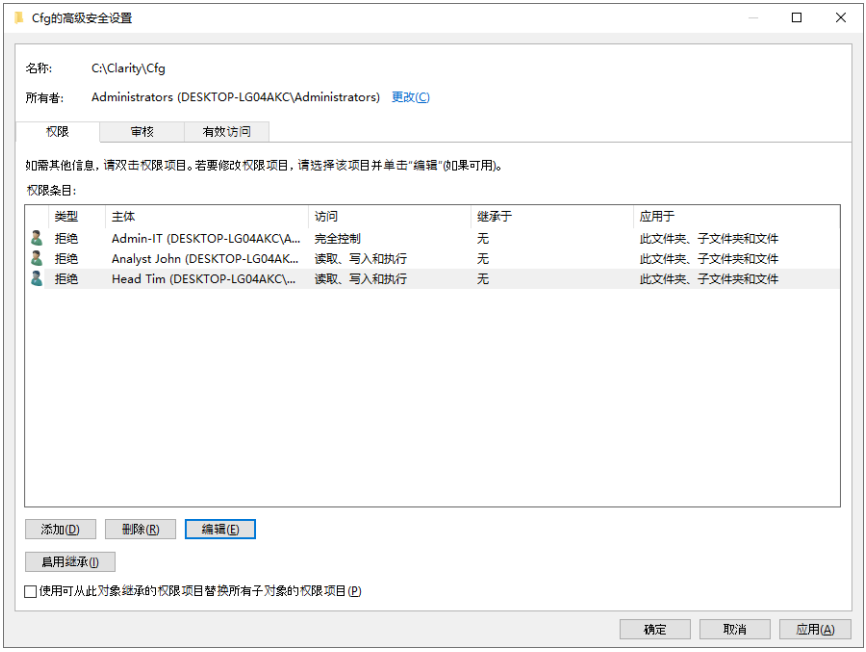


图47 Cfg文件夹的高级安全设置

- 如果需要，可以从*Cfg*属性窗口的安全选项卡查看各个用户的设置。

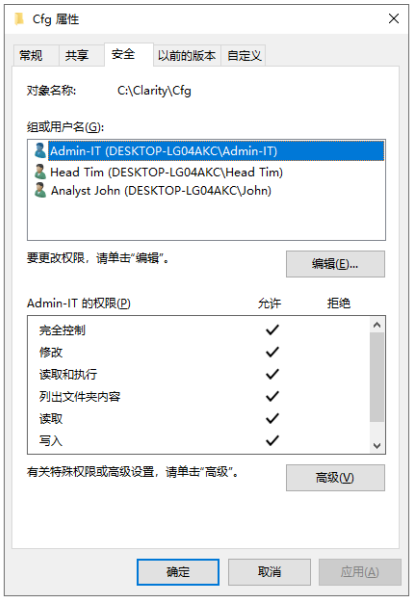


图48 管理员Cfg文件夹的安全属性

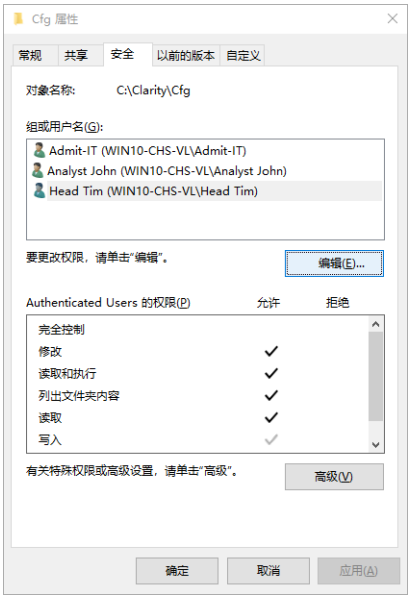


图49 用户Cfg文件夹的安全属性

- 所有要运行**Clarity**的用户和本地*管理员*的用户，其用户账号下的*DataFiles*文件夹都应进行以上完整的操作设置。

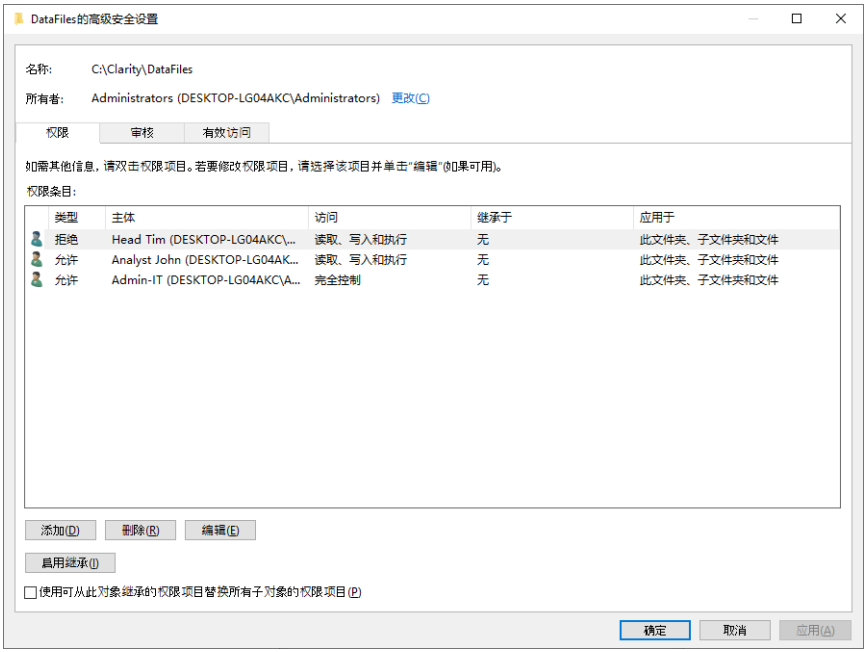


图50 DataFiles文件夹的高级安全设置

- 所有运行**Clarity**的用户，其用户账号都可以直接从*Windows开始菜单*在各自的*桌面*上创建**Clarity**的快捷方式。

33 Clarity中的用户账号

每个有权限访问**Clarity**的用户都必须拥有自己的用户账号，包含自己的密码以及设定好的允许他/她进行某些操作的权限。该功能是**21 CFR Part 11**和**GLP**要求的。

Clarity的其中一个用户应该作为工作站管理员，并拥有**Clarity**工作站的*管理员*权限。

注释： 这些权限可以分配给例如实验室主管。

只有*管理员*才能在**Clarity**中创建新用户账号并更改现有账号的用户权限。请注意，组织内部必须有不止一个知道*管理员*账号登录凭据的人，以便应付一些不可预知情况的出现(例如，本地*管理员*因生病或意外而长期缺勤等)。

331 SOP ——用户账号——设置管理员账号

- 打开**Clarity**工作站。
- 在Clarity主窗口，点击*系统*——*用户账号...*命令来进入用户账号对话框。
- 用*管理者*权限创建用户账号。
  - 点击*新建*按钮。
  - 在*用户名*字段填上您想要的名字。
  - 在*桌面文件*字段填上桌面文件名称，并尽可能在描述字段写上账号的*说明*(例如管理员的描述或需要更改设置时应联系的人的姓名)。

注释： 在*用户名*字段中使用用户的全名。这些名称将显示在审计追踪记录和所有报告中。这将使您更容易识别造成变更的人。

  - 设置*密码限制*(这将适用于所有用户)。密码的最小长度(*最小长度*)必须指定，其他字段是可选的。

注释： 将*最小长度*设置为至少6个字符或根据公司设置的规则。示例设置如第**45**页第**图51**.

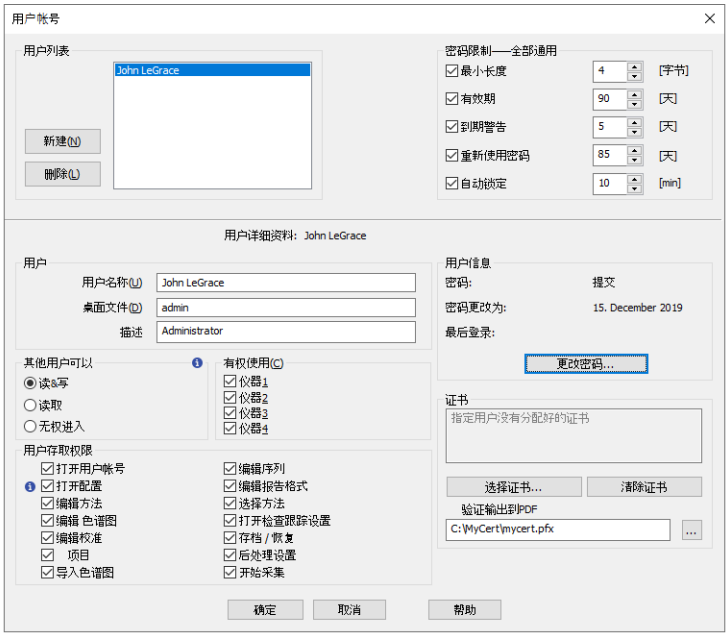


图51 用户账号——设置管理员

- 使用*更改密码*按钮设置*管理员*账号的*用户密码*。密码必须符合前面步骤中设置的*密码限制*。
- 设置*管理员*账号的*用户访问权限*。

注释： *管理员*账号必须具有*打开用户账号*和*打开配置*的权限，才能成功地将**Clarity**工作站设置为合规环境条件。

332 SOP ——用户账号——设置用户账号

- 打开**Clarity**工作站。
- 在Clarity主窗口，有*管理者*权限的用户需点开*系统——用户账号...*的指令进入用户账号对话框。
- 用*用户*权限来创建用户账号。
  - 点击*新建*按钮
  - 填上*用户名*(再一次强调，需要填上全名)，*桌面文件*(如果想要共享用户栏请参阅在第**52**页第**"共享桌面文件"**节.一节)以及*描述*字段
  - 设置用户账号的*用户访问权限*。以下复选框必须取消勾选：
- *打开用户账号*
- *打开配置*
- *打开审计追踪设置*
- *存档/恢复*

注释： *存档/恢复*权限可设置为指定一个用户，由其负责公司数据的存档工作。但是，前面提到的其他选项仍应仅分配给**Clarity***管理员*。我们建议将*存档/恢复*权限留给**Clarity***管理员*和/或*QA*工作人员。

- 请勿更改密码设置，因为用户账号对话框的这一部分，对于给定**Clarity**工作站的所有用户都是通用的。普通用户的用户账号对话框设置如下图所示：

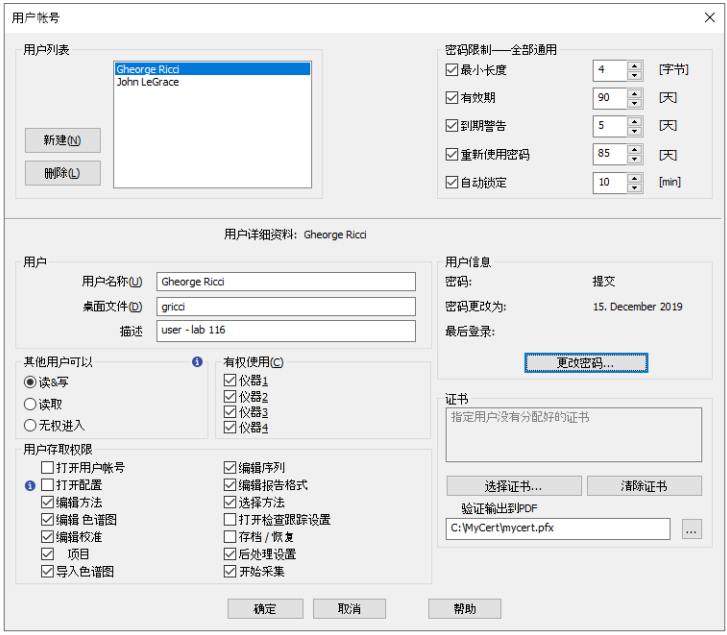


图52 用户账号——设置用户

- 创建另一个用户账号或按下*确定*按钮后关闭用户帐户对话框。

333 SOP ——用户账号——设置QA账号

QA人员必须在**Clarity**工作站里有自己的访问权限，且无权更改任何数据。

在**Clarity**里为QA工作人员创建没有权限更改任何数据的用户账号是必要的。要做到这一点，请遵循以下步骤。

- 打开**Clarity**工作站。
- 在Clarity主窗口，有*管理者*权限的用户须点击*系统——用户账号...*命令来进入用户账号对话框。
- 创建有*QA人员*权限的用户账号。
  - 点击*新建*按钮。

- 填上*用户名*(再一次强调，须填全名)，*桌面文件*(如果您需要共享用户栏，请参阅在第**52**页第**"共享桌面文件"**节.)和*描述*字段。
- 设置用户账号的*用户访问权限*。大多数复选框必须取消勾选，只有*项目*复选框应该启用。根据公司本身的存取权限和规则，还可以启用其他一些复选框。这专门针对*后处理设置*和*存档/恢复*选项。
- 请勿更改密码设置，因为用户账号对话框的这一部分对于给定**Clarity**工作站的所有用户都是通用的。普通用户的用户账号对话框的设置可以在第**47**页第**图53**.中看到：

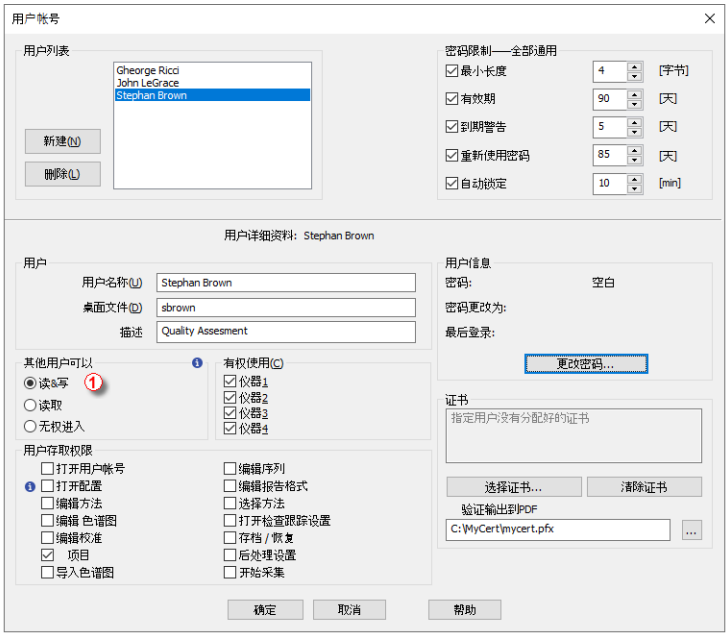


图53 用户帐户——设置QA工作人员

- 确保所有其他用户没有*其他用户可以*部分①切换到*无权进入*的选项。
- 按下*确定*按钮关闭用户帐号对话框。

34 记录所有变更

所有数据的变更以及变更的理由都必须被正确记录，以便以后可以找到变更的原因。该功能是**21 CFR Part 11**和**GLP**要求的。
总的来说，确保每个重要的变更都被记录下来的最佳方法是记录**Clarity**执行的每个操作。这是**Clarity** 2.7及更高版本的默认设置。要确认这种情况，或设置此功能，具有*管理员*权限的**Clarity**用户应执行以下步骤：

341 SOP ——在审计追踪中设置记录

- 在Clarity主窗口中使用*系统*——*审计追踪*命令来打开审计追踪窗口。
- 在审计追踪窗口中使用*视图*——*属性*...命令访问审计追踪设置对话框。

注释： 您将会被要求填入正确的**Clarity***用户名*和密码。

- 勾选所有选项卡上的所有复选框，并确认它们都已启用；如果其中一些没有启用，则勾选它们。
- 点击*确定*按钮退出对话框。

35 变更原因记录

变更的原因必须与变更本身一起被记录下来，以便后续可以找到变更的原因。
这个问题可以通过GLP选项对话框与其他问题一起解决。有关详细信息，请参阅在第**8**页第**"SOP ——GLP选项设置"**节.

36 数据存档

所有数据保存的时长必须符合相关部门所作的规定。该功能是**21 CFR Part 11**和**GLP**要求的。

注释： **FDA**(美国)版本的**GLP**已经包含了§58.195中的最短数据保留时间的要求。

这一要求可以由仪器窗口的*保存...*和*恢复...*命令来实现(从**Clarity**的角度来看)。一些外部存档软件也可能是合适的。

注释： 数据的存档和恢复应由具有管理员账号的人员操作。

361 SOP ——数据存档

数据保存时为了节省空间，可以使用整个项目的压缩存档。按如下操作：

- 拥有*存档/恢复*权限的人(**Clarity***管理员*或*QA*工作者)必须打开**Clarity**和给定的仪器。
- 使用*文件*——*存档...*命令打开备份对话框。

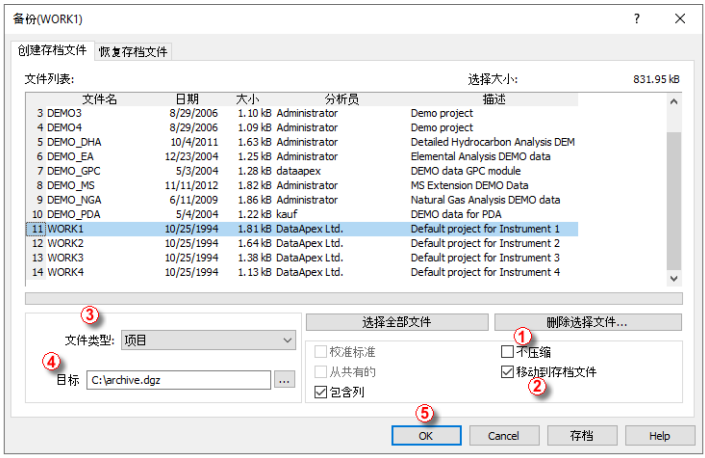


图54 备份

- 取消勾选*不压缩*复选框①。
- 勾选*移动到存档文件*复选框②。

注释： 如果您只想保档文件，且不想删掉源文件，则不要勾选*移动到存档文件*复选框

注意： 如果您想存档文件并删除源文件(如色谱图，序列等)，选择②*移动到存档文件*选项。注意，若*DataFiles*文件夹的*安全设置*是根据在第**11**页第**"计算机用户权限"**节.一章来设定的，那么移动到存档文件(等于删除源文件)这个操作只能由拥有*DataFiles*文件夹的*完全控制*权限的人来完成，一般是本地的IT工作人员。

- 从*文件类型*字段③的下拉菜单中选择*项目*。可用项目的列表将出现在*文件列表*中。在那里选择要存档的项目。
- 在*目标*选项④中选择存档文件的路径和名称(*.DGZ扩展名)。

注释： 请注意，不允许将文件保存到操作系统的根文件夹中(通常为"C:\")，这通常是因为*Windows 7*和更新版本中通常预定义的*UAC——用户帐户控制*设置。在这种情况下，需要选择用于存储生成的*.DGZ存档的其他位置，不能是*Windows*根文件夹。通常在*Windows*根文件夹中创建其他文件夹即可。

注意： 可以禁用删除或更改已创建的*.DGZ存档的功能。*目标*选项④中所述文件夹的*安全设置*必须与在第**11**页第**"计算机用户权限"**节.一章中所述完全相同。在根据使用的*windows*版本的情况下，有必要遵循在第**11**页第**"计算机用户权限"**节.一章相应分章中给出的指导。

- 按下*确定*按钮⑤存档项目并关闭备份对话框。在不离开对话框的情况下，可以使用*存档*按钮进行存档。
- 为了数据完整有效，必须存档另外两种文件类型——审计追踪和配置文件。存档审计追踪文件：

注释： 由**Clarity**生成的每个数据文件都有自己的审计追踪日志，但这些单独的日志并不包含有关全局事件的信息，例如在**Clarity**中打开仪器、更改方法文件等等。所有这些事件都记录在工作站的审计追踪中。

  - 在已打开的备份对话框中取消勾选*不压缩*的复选框①。与整个项目的存档不同,*移动到存档文件*复选框②应保持不勾选。

注释： 每日的工作站审计追踪对整个**Clarity**工作站来说是常见的。因此，如果用户可以使用多台仪器，那么删除审计追踪文件也可能会从其他**Clarity**项目中删除日志数据。

  - 在*文件类型*选项③中选择*审计追踪文件*选项，在*文件列表*中选择有效的文件。
  - 在*目标*选项④中选择要存档的文件的路径和名称(*.DGZ扩展名)。注意不要覆盖已备份的项目。
  - 按下*确定*按钮⑤来存档项目并关闭备份对话框。在不离开对话框的情况下，可以使用*存档*按钮进行存档。
- 要存档配置文件，请执行以下步骤：

注释： 无法在**Clarity**环境中执行**Clarity**配置文件的存档过程。进一步的文件记录不需要配置文件，它只是为了实现测量的重复性而需要保存一个必要部分。

- 在计算机上具有*管理员*权限的人(不在**Clarity**中，通常是公司IT工作人员或实验室主管)必须在**Clarity**关闭时打开文件管理器，并进入**Clarity**安装目录(C:\CLARITY \BIN，默认情况下)。
- 此*管理员*应找到CLARITY.CFG文件(C:\CLARITY\CFG默认情况下)，并将其复制到与其他存档文件一起的位置。

37 共享桌面文件

所有用户在用户计算栏中必须具有相同的设置。
这些设置是在用户桌面中定义的，默认情况下，并不是所有用户都使用这些设置，因为桌面文件还保存了最后打开的文档、用户设置等数据。当所有用户都必须使用表格中的用户计算功能或其他保存在用户设置中的功能时，必须确保所有用户使用相同的桌面文件，并且桌面文件不可修改。如需设置，请执行以下步骤：

371 SOP——共享桌面文件

- 准备好桌面文件，使其符合你的设置要求。
- 用*管理者*权限的账号进入用户账号对话框。
- 一次一个，选择在*用户列表*中需要用同一个桌面的用户。对于每一位选中的用户，在数据选项中将*桌面文件*的名字改成想要的名字。

注释： 所需桌面的文件名是为准备桌面的账号设置的。如果*桌面文件*选项为空，则使用与给定用户名相同的默认桌面文件名。

- 通过按下*确定*按钮来关闭用户账号对话框。
- 关闭**Clarity**。
- 在您电脑上的文件管理程序中找到桌面文件。该文件将位于**Clarity**主目录(默认情况下为C:\CLARITY \CFG) 中，并具有给定的文件名和*.DSK扩展名。
- 将文件的属性更改为只读。只有具有*管理员*权限的*Windows*用户账号才可以通过与在第**11**页第**"计算机用户权限"**节.所述相同的方式进行设置。此设置应适用于使用此选定共享桌面文件的**Clarity**用户的所有*Windows*用户账号。
- 将安全属性更改为选定的共享桌面文件时，请确保*Cfg*文件夹的安全设置与在第**11**页第**"计算机用户权限"**节.中所述的完全相同。
- 注意，用户可以在**Clarity**中修改*当前共享桌面文件，但无法存储修改内容，因为关闭仪器窗口时将显示一条错误消息桌面文件写入错误。*

- ***Windows 7***：

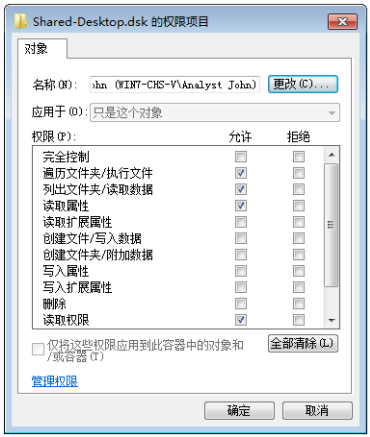


图55共享桌面的安全设置——用户权限项目

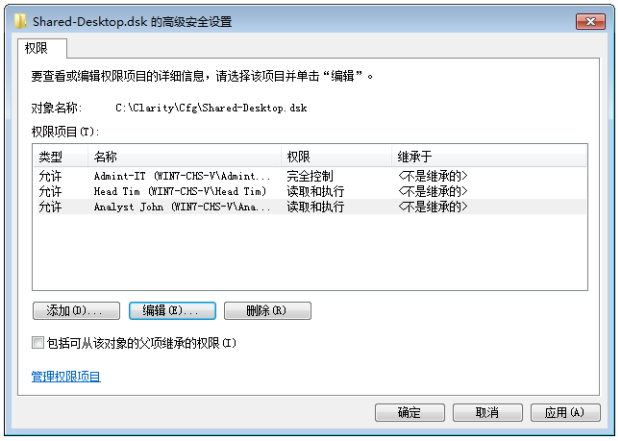


图56共享桌面的安全设置——高级设置——1

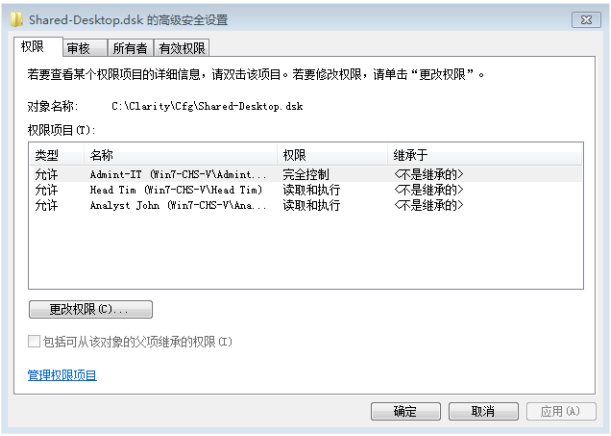


图57 共享桌面的安全设置——高级设置——2

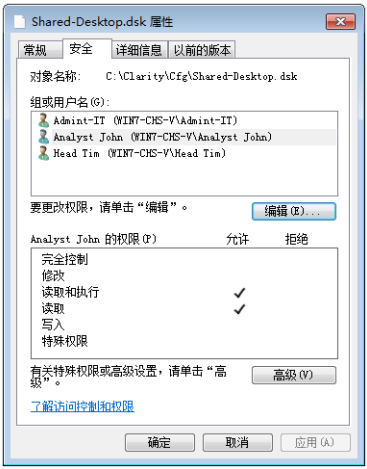


图58 共享桌面的安全设置——安全概述

- ***Windows 8.1***：

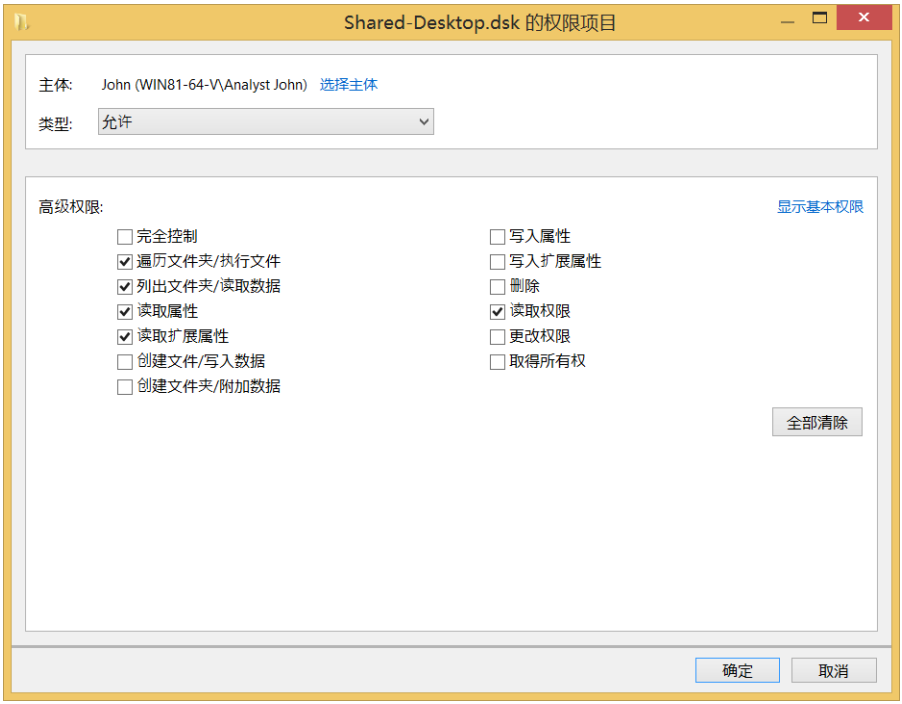


图59 共享桌面的安全设置——用户权限项目

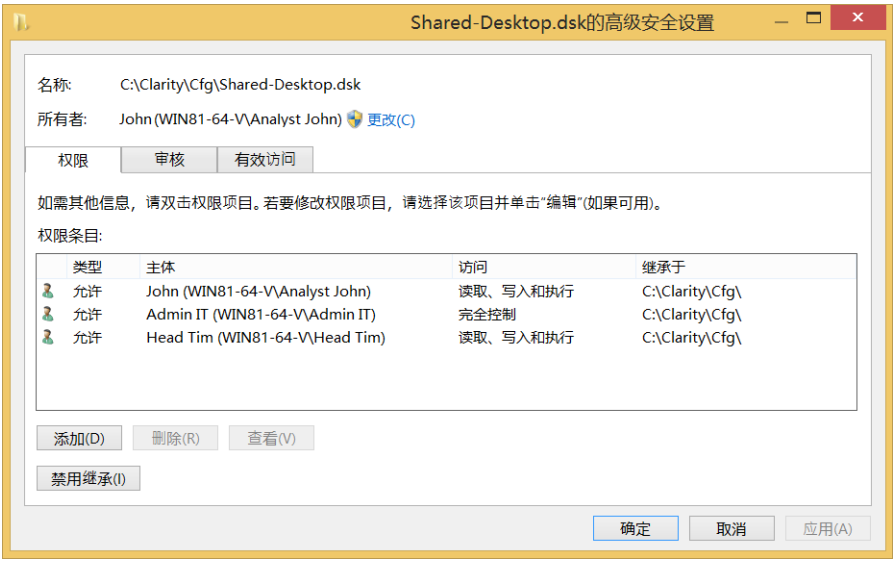


图60 共享桌面的安全设置——高级设置

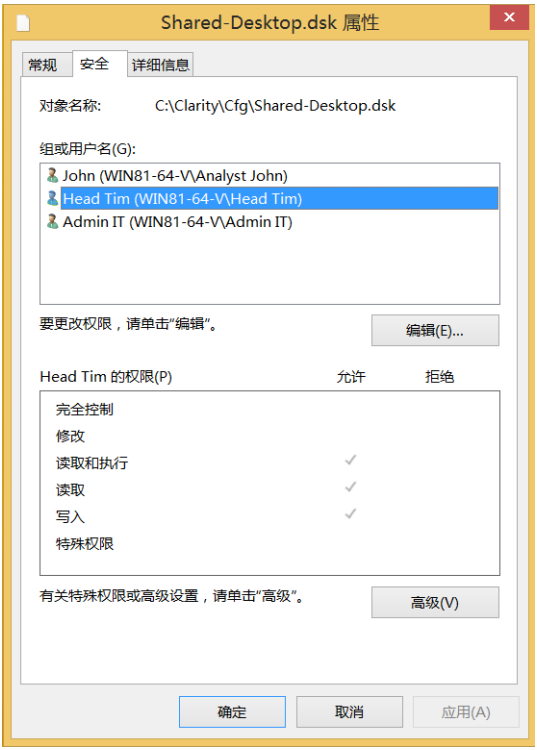


图61 共享桌面的安全设置——安全概述

- ***Windows 10***：

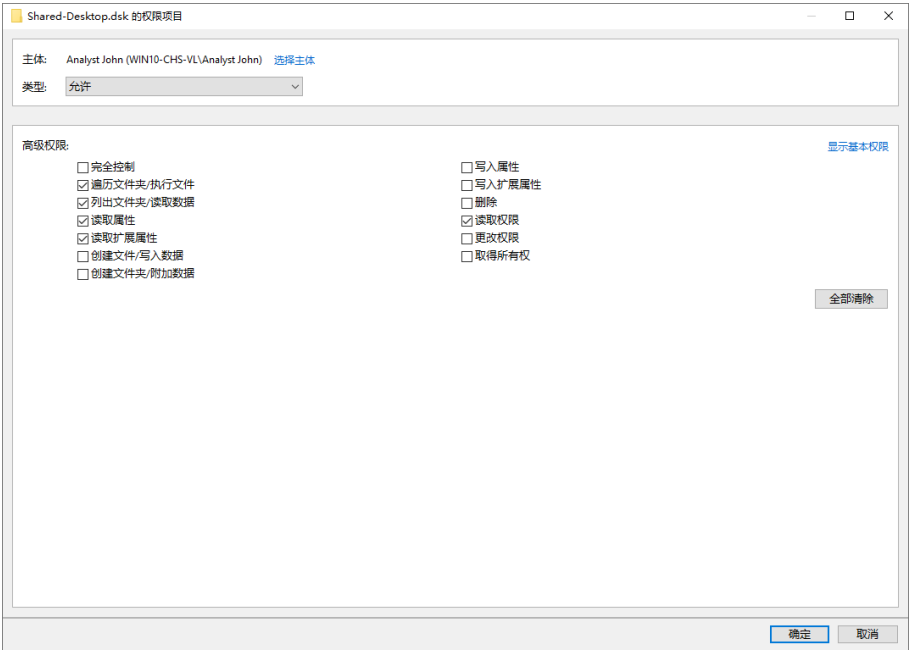


图62 共享桌面安全设置——用户项目

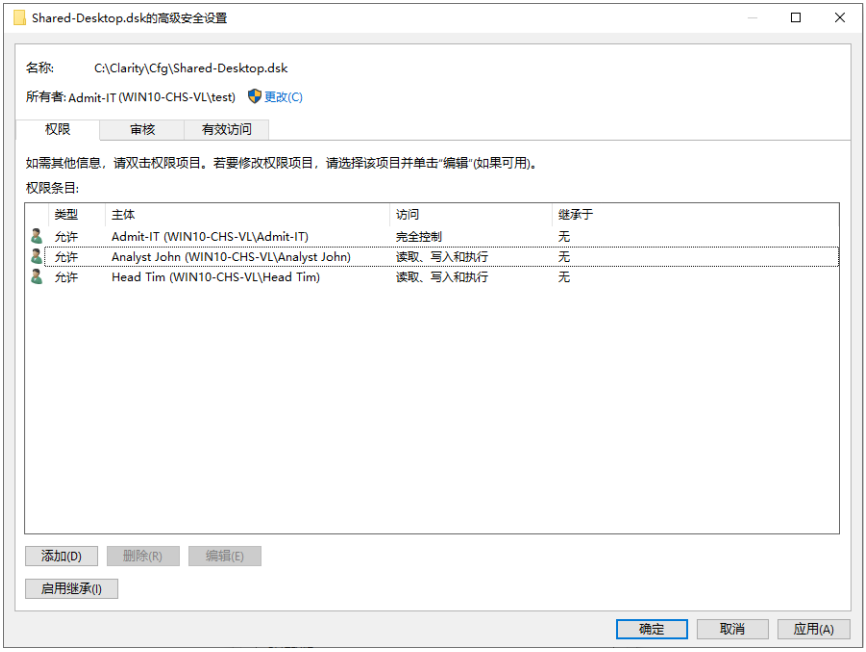


图63 共享桌面的安全设置——高级设置

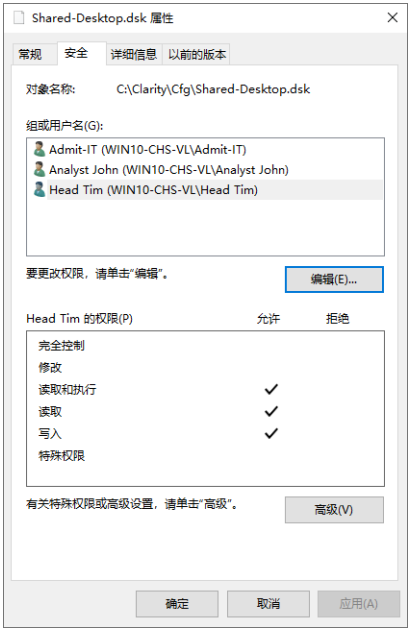


图64 共享桌面的安全设置——安全概述

38 多工作站环境

当用户(或多个用户)需要在多台计算机上工作时，所有用户的用户账号(以及存储的密码)都应该是相同的。在所有计算机的**Clarity** 工作站的CFG目录(默认路径 C:\ CLARITY \CFG)中创建相同的CLARITY.PSW文件即可实现以上功能。

CLARITY.PSW文件只在两种情况下发生改变——当一个新用户添加到用户列表时，或者当前用户更改他/她的密码时。

注意： 只需确保所有计算机上使用的用户账号是相同的，换句话说，只有在用户账号对话框更改后(添加用户、修改用户权限...)才需要去做这个检查。确保密码更改后文件是相同的会让使用者更放心，但不是必须的。

由于普通用户不被允许访问**Clarity**的整个安装目录，所以应由系统*管理员*将这个CLARITY.PSW文件复制到装有**Clarity**多工作站环境的所有电脑上。

注释： CLARITY.PSW文件在**Clarity**工作站关闭时会被保存和修改。因此，需要在不运行**Clarity**时将文件复制到根目录中。

39 电子签名

在**Clarity**里，必须能够使用个人独有的电子签名签署电子数据，电子签名是每个人独有的，且电子签名不能够被重复使用，或重新分配给其他任何人，也不能够被修改。该功能是**21 CFR Part 11**要求的。

注释： 用于电子签名的证书不属于**Clarity**安装的一部分，此类证书应由认证机构提供。DataApex不颁发任何电子签名证书。

要与**Clarity**一起使用的证书必须包含密钥部分，其中的密码只有特定用户知道，并在每次使用时都需要被输入。要将证书设置给特定用户，请执行以下步骤：

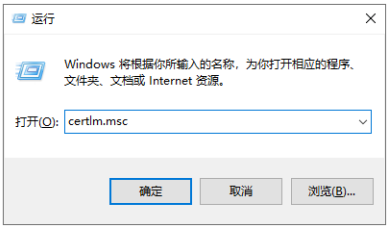
注意 需要注意的是，在使用第三方证书签署色谱图时，操作Clarity的计算机上必须有每个Windows用户账号的证书，并且这些证书相应安装在每个用户的个人存储中。如果要在单个Windows用户账号下安装多个证书给多个用户账号，那么很容易会出现不同的Clarity用户(通过用户账号对话框定义)可以使用其他人的证书签署色谱图的情况。出现这种情况的原因是，在Windows环境中，Windows用户仅在账号登录期间首次使用证书时，才会被要求输入其证书的密码。使用已经用过的证书对色谱图进行签名时，系统不会要求你重新输入密码。这时候，你可以选择当前登录的Windows账户下任意一个可用的证书对色谱图进行签名。在使用第三方证书的情况下，为了避免这种情况的发生，有必要为每个Clarity用户账号分别设置具有唯一凭据的Windows账号，并在此账号的专用存储中安装第三方证书。在合规环境中部署Clarity时，必须满足以上条件，并应有第三方认证机构颁发的使用证书。避免这种情况出现的另外一种方式是，通过在签名对话框中的选项*作为当前用户签名*为每个Clarity用户定义凭据来签名色谱图。

391 设置证书

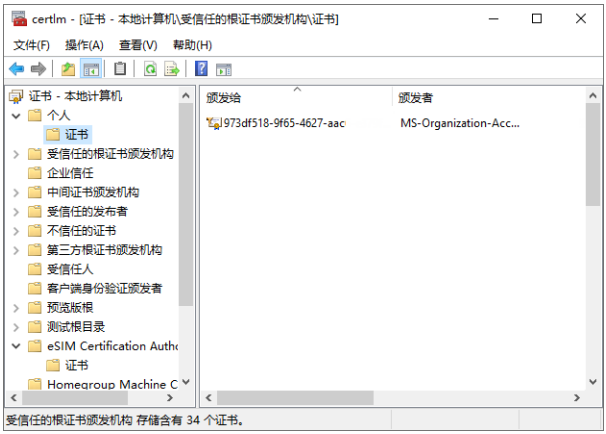
任何官方颁发的证书都是一个可以安装在指定计算机上的文件。安装的步骤应该由发出证书的核证机构详细解释并说明。

检查已安装的证书：

- 应该由系统*管理员*运行证书文件，并按照发证机构描述的流程进行安装。它的安装可能在不同的操作系统中有所不同，但是文件应该安装到个人证书存储中。
- 在微软窗口里同时按下键盘上的windows键和“R”键来调出运行对话框。在输入栏输入“certmgr. msc”并单击*确定*按钮。



- 在下面的窗口中，导航到*个人*文件夹。此类文件夹包含以**Clarity**方式显示的证书，可以在用户账号窗口的选择证书对话框中进行选择。



设置色谱图的签署证书：

- **Clarity***管理员*应该运行**Clarity**并打开用户账号对话框(通过使用*系统——用户账号...*命令)。
- 在对话框左上角的*用户列表*部分中选择特定的用户名。
- 按下对话框右下角的*选择证书*按钮。将出现选择证书对话框。
- 从对话框中的可用证书列表中选择证书并按下*确定*按钮。选中的证书将被添加到用户的用户账号中。
- 如果需要，可以通过重复上述步骤为其他用户设置其他证书。
- 按下*确认*按钮关闭用户账号对话框。

设置PDF文件的签署证书：

- **Clarity***管理员*应该运行**Clarity**并打开用户账号对话框(通过使用*系统——用户账号...*命令)。
- 单击...按钮以调用*打开*对话框并选择PKCS#12类型证书。

- 如果需要，可以通过重复上述步骤为其他用户设置其他证书。
- 按下*确定*按钮关闭用户帐号对话框。