常见问题

遵循 21 CFR Part 11 法规的实验室用软件 — Syngistix AA Enhanced Security

21 CFR Part 11 法规（《美国联邦法规》第 21 篇—食品与药品）涵盖了对电子系统合规性的总体要求，包括管理控制、程序管制和技术控制。如果没有其他控制要素的开发和执行，软件本身是无法满足合规性要求的。适用于珀金埃尔默 PinAAcle™ 原子吸收（AA）光谱仪的 Syngistix™ AA Enhanced Security™ 软件提供的功能在与适当的指令和程序相结合时，可满足 21 CFR Part 11 法规中封闭系统电子记录的要求。Syngistix Enhanced Security 软件还可满足与电子签名相关的要素。

21 CFR Part 11 B 部分—电子记录

11.10 封闭系统控制措施

使用封闭系统创建、修改、维护或传输电子记录的人员应当通过程序与控制措施确保电子记录的真实性、完整性和机密性（如有必要），并确保签署人员无法轻易否认已签名记录的真实性。此类程序和控制措施应涉及以下方面：

11.10 a 验证系统以确保系统的准确性、可靠性、持续稳定的预期性能，以及能够识别无效的或被修改的记录。

Q 是否可以在系统上查看记录是否已被修改?

A 如果允许修改，则审计跟踪和文件历史数据库将记录对记录的修改。审计跟踪和文件历史数据库可用于查看或检索已修改的记录信息。

原始数据一旦收入数据文件中，软件就不提供修改原始数据的方法。

为防止未经授权对数据库的修改，Syngistix Enhanced Security 软件对所有文件和数据库记录附加有校验和值。

如果打开在系统外更改过的文件，系统会生成错误消息，并记录在主事件日志中。

开启每个模式时，校验和会在 Syngistix Enhanced Security Tools 实用程序（ES Tools）中自动验证。此外，可以使用数据管理器中的“验证校验和”命令检查结果和方法数据库中的记录。

Q 系统是否可以识别无效记录?

A Syngistix Enhanced Security 软件将校验和附加到所有文件和数据库记录中。尝试打开已在系统外部修改的文件，将在主事件日志中生成错误消息和记录。

开启每个模式时，校验和会在 ES Tools 中自动验证。此外，可以使用数据管理器中的“验证校验和”命令检查结果及方法数据库中的记录。

PerkinElmer®
For the Better

Q 谁负责系统的验证?

A 客户负责验证“系统”(包括政策、程序、硬件、软件和人员)。

初次选择与验证时,客户应进行某种形式的供应商评估,以确定系统软件的开发方式和测试级别。基于风险评估,客户可以确定其验证工作的性质和级别。

Q 供应商在验证中起到什么作用?

A 珀金埃尔默允许客户审核系统的开发,并提供开发过程中的信息。

每个系统都会提供详细说明系统的使用和操作方法的综合文档。Syngistix Enhanced Security 软件版本说明中详细介绍了可能影响软件操作的已知问题。

另外,还提供客户培训课程,深入说明系统的使用和操作方法。

11.10 b 确保系统具备生成准确和完整的、人可读的电子副本的功能,且其电子格式应适合 FDA 检查、审核、拷贝的要求。如对 FDA 审核、拷贝电子记录能力有任何疑问,应及时与 FDA 联系沟通。

Q 系统是否可以生成准确完整,且适合美国 FDA 检查、审核、拷贝要求的电子记录备份?

A 可以。所有文件和数据对象均可使用 Syngistix 应用程序进行读取,使用附带工具进行检查。此外,大多数数据对象可以导出为文本,并使用文本编辑器查看,同时可以打印成纸质文件或 PDF。

安全审计跟踪可以打印或导出 CSV 文件。

方法

“方法”有“保存为文本”选项,由此可创建一个文本文件。ES Tools 允许打印单个方法或整批方法及其相应的状态、签名和时间戳。在 ES Tools 中可以查看和打印各方法与方法版本之间的差异。

样品信息文件(SIF)

样品信息文件始终为文本格式。在 ES Tools 中可以查看和打印各 SIF 文件与文件版本之间的差异。

结果

原始分析数据可利用应用程序导出为逗号分隔的文本文件。方法、IEC 系数和 MSF 文件可以从结果数据库导入应用程序中,并作为单独的文件进行查看、导出或保存。

审计日志

事件日志可利用应用程序进行排序、打印和导出 CSV 文件。如有必要,可将其存档并检索回应用程序进行数据库维护。

Q 系统是否可以生成准确完整,且适合美国 FDA 检查、审核、拷贝要求的纸质记录备份?

A 可以。当特定编辑器是活动窗口时,可以使用“打印活动窗口”命令打印方法和样品信息文件。以上所有记录均可按整批方法或单个方法打印成纸质文件或 PDF。打印方法时连同其状态、签名和时间戳一并打印。如果需要,可使用第三方屏幕截图实用程序打印 MSF 模型备份。ES Tools 中可以查看和打印各方法和 SIF 文件版本之间的差异。

结果数据库中的许多记录可以使用 Syngistix 主软件中的各种工具打印,也可以通过数据管理器打印出报告。此外,大多数记录可以导出为逗号分隔的文本,然后可以打印。结果可按批样品集,选择样品集或者样品及使用的完整方法,打印成纸质或 PDF 文件。

事件日志和审计跟踪可利用应用程序进行排序、打印和导出 CSV 文件。

11.10 c 保证记录安全,确保记录在保存期内完整准确,易于检索读取。

Q 记录是否在保存期内易于检索读取?

A 记录始终可以通过用于获取记录的 Syngistix Enhanced Security 软件版本读取。并且系统尽可能的设计为在可在新版本的 Syngistix Enhanced Security 软件中检索旧记录。

Data Manager Archive 实用程序是将操作系统上不再需要的数据(即方法或数据集)移至离线存储,以 *.zip 文件存档的选择性过程。此项功能先复制数据,确认复制成功;然后根据要求将原始记录从活动数据库中删除。与待存档的记录相关联的所有“元数据”(例如,签名、评论等)同时存档。数据经过存储后,如用户需要,可以在将来选择性地将记录及其相关元数据恢复至系统。

Data Manager Backup 实用程序是将某一时间点运行中的 Syngistix 系统进行“完整图像”快照备份成压缩文件。此项功能是对最后保存 / 备份的软件版本创建完整的备份（.mdb 文件）。将所有用户的所有文件（结果 / 方法 /ES 数据库、SIF 文件等）都备份到一个 *.zip 文件中。这主要是为了“灾难恢复”。

客户需要针对适用的数据进行记录并实行适当的备份和恢复政策和程序管理。

11.10 d 对授权个人的限制系统访问

Q 系统访问权限是否仅限于获得授权的人员？

A Syngistix Enhanced Security 软件及其运行的推荐计算机 / 操作系统满足 21 CFR Part 11 规定的封闭系统的电子记录要求。

利用专有安全模块或与公司的 Microsoft® Windows® Active Directory 集成，系统访问权限是密码控制的。如果不使用 Windows® 登录选项，则可以使用 Syngistix User Setup 强制定期更改密码和停用识别码 / 密码组合。如果用户已被停用，其活动记录不会删除且可以继续查阅。

用户组创建后分配与其培训相符的不同权限。电子签名和只读访问用于强制执行许可权限。

多个项目或研究可以通过创建特定目录位置进行组织。然后，可以为用户组分配默认的不同文件夹的访问权限。

客户还需要在计算机上正确配置本地 Windows® 安全性。这包括但不限于以下内容：

- 确保本地管理员帐户设置安全
- 禁用访客帐户
- 限制对操作系统文件和控件（如系统时钟）的访问
- 移除安全组对软件目录的删除功能
- 添加 / 配置 Windows® 组并将用户分配入组。

11.10 e 使用计算机生成的安全审计跟踪（带时间戳），独立记录操作者登录和操作的日期和时间，包括电子记录的创建，修改和删除。记录变更不得覆盖以往记录的信息。该审计追踪文件应该与其所归属的记录保存期一致，且支持 FDA 审核和拷贝。

Q 是否有安全的，计算机自动生成的，带时间标记的审计追踪，记录操作者登录和操作的日期和时间，包括电子记录的创建，修改和删除？

A 有，由系统创建的审计跟踪记录操作员执行的每个重要操作。这些操作可能影响写入文件或数据库的分析结果或电子记录。文件历史数据库记录文件名和版本。ES Tools 中可以查看各版本之间的任何差异，包括时间戳和电子签名。

每条审计跟踪记录包括日期、时间、用户 ID、用户名、执行的操作、操作详情、电子签名信息以及操作原因（如适用）。Syngistix Enhanced Security 管理员可以自定义默认的原因列表。如果操作原因必填，用户可以从默认列表中选择，从默认列表中选择并注释，或提供其他原因。

审计跟踪记录保存在密码加密的数据库中。

Q 电子记录一旦更改后，之前的记录信息是否仍然可用（即修改后未被覆盖）？

A 在保存每份文件的新版本之前，将其旧版本复制到密码加密的文件历史数据库。文件的版本号递增，表明已创建修改的版本。ES Tools 中可以查看各版本之间的任何差异，包括时间戳和电子签名。

一旦获得分析数据，无法对原始数据进行任何修改。重新处理数据将会创建数据的复制备份，所有重新处理的数据都会带此标记。

Q 电子记录的审计跟踪是否可以在记录保存期内易于检索读取？

A 审计跟踪和文件历史记录可以通过用于创建记录的 Syngistix Enhanced Security 软件版本随时检索。

审计跟踪和文件历史记录可以存档。恢复后，审计跟踪和文件历史记录可以通过用于创建记录的 Syngistix Enhanced Security 软件版本随时检索。

所有日志和审计跟踪也都可以打印为 PDF 或导出为逗号分隔文件，然后使用文本编辑器或电子表格程序查看。

客户负责制定对存档数据的存档和后续检索读取的安全政策和程序控制。

Q 审计跟踪是否可供美国 FDA 审核和拷贝?

A 审计跟踪和安全审计跟踪可以使用 Syngistix Enhanced Security 软件打印，以供审核。

11.10 f 使用操作系统检查，酌情按照批准的顺序执行各项步骤和事件。

Q 如果系统步骤或事件的顺序重要，系统是否会强制执行（例如，像过程控制系统一样）?

A Syngistix Enhanced Security 软件可执行大量方法和分析检查，以确保在执行分析任务之前所有设置均有效。方法只能由 Syngistix 系统管理员分配了相应权限的操作员创建和修改。

利用电子签名点确保经授权的用户才能执行相应操作。其他分析问题使用弹出或警告消息标记。

在开始分析之前，用户必须提供其登录凭据才能保存用于生成数据记录的所有文件。

11.10 g 使用权限检查，确保只有经过授权的人员方可使用系统、以电子方式签署记录、使用操作功能或访问计算机系统输入或输出设备、更改记录，或执行其它操作。

Q 系统是否可以确保仅有经过授权的人员方可使用系统、以电子方式签署记录、使用操作功能或访问计算机输入或输出设备、更改记录，或执行其他操作?

A Syngistix Enhanced Security 软件及其运行的推荐计算机 / 操作系统满足 21 CFR Part 11 规定的封闭系统的电子记录要求。

利用专有安全模块或与公司的 Windows® Active Directory 集成，软件访问权限是密码控制的。如果不使用 Windows® 登录选项，则可以使用 Syngistix User Setup 强制定期更改密码和停用识别码 / 密码组合。如果用户已被停用，其活动记录不会删除且可以继续查阅。

用户组创建后分配与其培训相符的不同权限。客户负责制定关于数据系统培训和用户角色的 SOP。

电子签名和只读访问用于强制执行许可权限并应用于所有相关操作。

多个项目或研究可以通过创建特定目录位置进行组织。然后，可以为用户组分配默认的不同文件夹的访问权限。

11.10h 适当时，使用设备（例如，终端）核查以确定数据输入或操作指令来源的有效性。

Q 如果系统要求输入的数据或指令只能来自于特定的输入设备（例如，终端），系统是否能检查所接收的任何数据或指令的来源的有效性?

（注：这适用于数据或指令来自于多个设备的情况，因此系统必须验证其来源（例如称重设备或远程无线电控制终端的网络）的完整性。）

A Syngistix Enhanced Security 软件总是针对单个光谱仪适配，在任何给定时间只能有一个用户登录系统。创建者的用户名和用户凭据以及仪器序列号将作为保存的数据的一部分进行记录，并记入在 ES Tools 的样品报告中。用户输入只能来自于已登录用户或在发起数据采集时提供登录凭据的用户。

从仪器收到的信息采用专有格式，有设备轮询健康状态，以确认光谱仪是否已连接且可操作。

输入文件（方法和样本）经校验和，如果在系统外部被篡改，将会被标记。文件内容始终参照其密码加密版本进行验证。

11.10 i 确定开发、维护或使用电子记录 / 电子签名系统的人员都具备相应的教育，培训，经验，来完成被分配的任务。

Q 供应商是否有质量管理体系?

A 珀金埃尔默已通过 ISO 9001 认证，并根据 ISO 指南开发所有产品。

Q 供应商是否提供开发人员 21 CFR Part 11 知识培训?

A 负责实现 Syngistix Enhanced Security 软件功能的开发团队接受有关 21 CFR Part 11 的含义和指示的培训。21 CFR Part 11 知识培训和随后理解确保系统的开发符合法规要求。

Q 对最终用户有什么意义?

A 最终用户负责提供员工 21 CFR Part 11 知识培训，并负责提供支持 21 CFR Part 11 的系统的程序和政策及预期用途的培训。

11.10 j 制定并遵守书面政策，要求人员对其电子签名确认发起的各项操作负责，从而避免记录和签名伪造的情况。

Q 是否制定政策要求个人对记录和签名伪造负责?

A 客户负责实施描述正确使用电子签名的义务和责任的政策。

如果客户打算使用电子签名，则有责任通知美国 FDA，且需要有政策和标准操作程序以及不可否认电子签名的培训。

11.10 k 对系统文档采取适当的控制措施，包括：

1. 对系统操作和维护文档的分发、访问和使用采取适当的控制措施。
2. 要有一套修订和变更控制程序，以维护记录系统文档按时间顺序开发和修订的审计跟踪。

Q 系统文档的分发、访问和使用是否采取控制措施?

A 配有 Syngistix Enhanced Security 软件的电子文档存在于软件媒体上，用户无法修改。该媒体带有部件编号，用于识别存在的文档版本。

客户需要有关系统文档版本控制发布和维护的 SOP。这可能包括供应商提供的用户手册和维修手册，以及客户建立的有关系统软硬件操作和使用的 SOP。

客户需要维护和系统配置管理 SOP 和记录，包括仪器维护日志。

11.30 开放系统控制措施

使用开放系统创建、修改、维护或传输电子记录的人员应当通过程序与控制措施确保电子记录的真实性与完整性，并在必要时确保电子记录从创建之时至交付之时的机密性。这些程序和控制应包括第 11.10 章节介绍的控制措施，适当时使用额外的方法，如文档加密，合适的电子签名标准，在必要时来确保记录的真实性、完整性和机密性。

Q 数据传输是否加密? 电子签名是否适用?

A Syngistix Enhanced Security 软件是一个封闭系统。

11.50 签名表现形式

11.50 a 已签署的电子记录应包含签名的相关信息，明确表明以下所有内容：

1. 签名者的印刷体姓名；
2. 签名的日期和时间；及
3. 签名相关的含义（如审查、批准、责任或署名）。

Q 已签署的电子记录是否包含以下相关信息?

- 签名者的印刷体姓名；
- 签名的日期和时间；及
- 签名的含义（如批准、审查、责任）

A Syngistix Enhanced Security 软件能够应用电子签名。Syngistix Enhanced Security 软件中的审计跟踪保存所有记录时连同用户名、签名日期 / 时间和签名的含义一并保存。

11.50 b 本节 (a)(1)、(a)(2) 和 (a)(3) 中确定的项目应受到电子记录同等程度的管控，并被纳入可读版本的电子记录（如电子显示或打印输出）之中。

Q 在 [11.50(a)] 中确定的项目是否显示在电子记录的显示和打印副本上? 在 [11.50(a)] 中确定的项目是否受到其他电子记录同等程度的管控?

A Syngistix Enhanced Security 软件在软件内以及在审计跟踪的打印副本中显示此信息。

所有受控活动都需要具有该活动有效系统权限的用户的双成分签名。

11.70 签名 / 记录关联

电子签名和手写签名应与相应的电子记录相互关联，以确保他人无法通过普通方式删除、复制或以其他方式转移签名以伪造电子记录。

Q 签名是否与相应的电子记录相关联，以确保他人无法通过普通方式删除、复制或以其他方式转移签名进行伪造?

A Syngistix Enhanced Security 软件使用安全数据库关联所有签名并跟踪所有相关联的签名。任何用户都无法访问或修改此数据库。

21 CFR Part 11 C 部分—电子签名

11.100 通用要求

11.100 a 每个电子签名应对应唯一的用户，不得由任何其他人重复使用或重新分配给任何其他人。

Q 可以有多个人使用相同的登录信息吗?

A Syngistix Enhanced Security 软件提供实用程序以使用电子签名，但用户访问控制应由公司协议建立。

11.100 b 当组织创建、分配、认证或批准一个用户的电子签名或者电子签名的任何组成要素前，应先核实用户的身份。

Q 用户的身份是否经过核实?

A Syngistix Enhanced Security 软件提供实用程序以使用电子签名，但用户访问控制应由公司协议建立。

11.200 电子签名的组成及控制措施

11.200 a1 不基于生物识别技术的电子签名应:

至少使用两种不同的识别组成部分，例如识别码和密码。

i. 当一个用户在单个持续的受控系统访问期内执行一系列的签名操作时，第一个签名应该使用所有电子签名的组成部分，后续的签名应至少使用一种电子签名组成部分，且该组成部分只能由用户个人执行及使用。

ii. 当一个用户不在单个持续的受控系统访问期内执行一个或多个签名操作时，每个签名都应使用所有电子签名的组成部分。

Q 签名要求是否有管控? 特别是要执行一系列签名操作时?

A Syngistix Enhanced Security 软件每次都需要一个唯一的用户名和密码才能使用电子签名功能。

所有受控的操作都需要具有相应操作权限用户的双组份签名。

11.200 a2 不基于生物识别技术的电子签名应:

仅供其真正的拥有者使用。

Q 以电子方式签署数据 / 文件有哪些要求?

A Syngistix Enhanced Security 软件需要一个唯一的用户名和密码才能使用电子签名功能。需要公司政策和用户培训，以确保不会出现凭据共享。

11.200 a3 不基于生物识别技术的电子签名应:

经过适当的管理和执行，确保非真正拥有者在尝试使用电子签名时，需要两个或两个以上人员协作。

Q 是否任何人都可以另一个用户身份登录?

A Syngistix Enhanced Security 软件需要一个唯一的用户名和密码才能使用电子签名功能。

Syngistix Enhanced Security 软件提供实用程序以使用电子签名，但用户访问控制应由公司协议建立。

11.200 b 基于生物识别技术的电子签名应经过设计确保非真正拥有者无法使用。

Q 生物识别是否可以确保真实?

A Syngistix Enhanced Security 软件不使用生物识别访问系统。

11.300 识别码 / 密码的控制措施

当基于识别码和密码组合的验证方式使用电子签名时，使用者应采取控制措施以确保电子签名的安全性和完整性。所述控制措施应包括：

11.300 a 维护每一对识别码和密码组合的唯一性，保证其他人不具有相同的识别码和密码组合。

Q 系统是否可以确保不会存在两个相同的帐户？

A Syngistix Enhanced Security 软件需要一个唯一的用户名和密码才能使用电子签名功能。

11.300 b 识别码和密码的发放应定期进行审查，回收失去授权的识别码和密码，或对其进行修改（例如，预防密码过期等情况）。

Q 系统是否会强制定期更改密码，以及停用识别码 / 密码组合同时不丢失其历史使用记录？

A Syngistix Enhanced Security 软件通过用户 ID/ 密码双组分验证限制应用程序访问。如果使用珀金埃尔默登录，则可以使用 Syngistix User Setup 强制定期更改密码和停用识别码 / 密码组合。创建新用户，应使用预过期密码，确保只有用户才知道账户密码。

如果用户已被停用，其活动记录不会删除且可以继续查阅。

11.300 d 利用事务处理安防措施，防止未经授权使用密码和 / 或识别码，并侦测任何此类企图，并立即向系统安全部门及组织管理层（视情况而定）紧急报告。

Q 系统是否会提示未经授权的访问尝试并采取预防措施（例如，经过指定次数的失败尝试后锁定终端、吞卡）？

A Syngistix Enhanced Security 软件会侦测到未经授权的访问，并通过任何登录失败或密码重置的电子邮件或短信提供通知。所有登录（成功或失败）都记录在安全审计跟踪中。

若使用珀金埃尔默登录，管理员设置帐户在指定登录失败次数后锁定及锁定持续时间（定时或永久）。

珀金埃尔默企业管理（上海）有限公司
地址：上海 张江高科技园区 张衡路 1670 号
邮编：201203
电话：021-60645888
传真：021-60645999
www.perkinelmer.com.cn

PerkinElmer®

014656_CHN_01 PKI