ESET PROTECT

安装、升级和迁移指南

单击此处显示此文档的联机版本

版权所有 ©2023，所有者 ESET, spol. s r.o.

ESET PROTECT 由 ESET, spol. s r.o. 开发

有关详细信息，请访问 https://www.eset.com

保留所有权利。未经作者书面许可，不得以任何形式或任何方式（电子、机械、影印、录制、扫描或其他方式）复制、在检索系统中存储或传输本文档的任何部分。

ESET, spol. s r.o. 保留更改任何所述应用程序软件的权利，恕不另行通知。

技术支持https://support.eset.com

修订日期 2023年m月27日

1 关于帮助 1
2 安装/升级/迁移 1
2.1 ESET PROTECT 10.0 中的新功能 2
2.2 架构 3
2.2 服务器 3
2.2 Web 控制台 4
2.2 ESET BridgeHTTP 代理 – 5
2.2 服务器代理 5
2.2 Rogue Detection Sensor 6
2.2 移动设备连接器 7
2.3 ESET Bridge HTTP 代理、镜像工具和直接连接之间的区别 8
2.3 何时开始使用 ESET Bridge (HTTP 代理) 10
2.3 何时开始使用镜像工具 10
3 系统要求和大小调整 11
3.1 支持的操作系统 11
3.1 Windows 11
3.1 Linux 13
3.1 macOS 13
3.1 移动 14
3.2 支持的桌面设置环境 15
3.3 硬件和基础结构大小调整 16
3.3 部署建议 18
3.3 部署 10,000 个客户端 20
3.4 数据库 21
3.5 受支持的 Apache Tomcat 和 Java 版本 23
3.6 受支持的 Web 浏览器□ESET 安全产品和语言 23
3.7 网络 25
3.7 使用的端口 26
4 安装过程 30
4.1 Windows 上的一体式安装 31
4.1 安装 ESET PROTECT 服务器 31
4.1 安装 ESET PROTECT 移动设备连接器（单机版） 41
4.2 Windows 上的组件安装 47
4.2 服务器安装 - Windows 49
4.2 Microsoft SQL Server 要求 56
4.2 MySQL Server 安装和配置 56
4.2 专用数据库用户帐户 58
4.2 服务器代理安装 - Windows 58
4.2 服务器辅助服务器代理安装 61
4.2 脱机服务器代理安装 62
4.2 ESET Remote Deployment Tool 62
4.2 Web 控制台安装 - Windows 62
4.2 使用一体式安装程序安装 Web 控制台 63
4.2 手动安装 Web 控制台 68
4.2 RD Sensor 安装 - Windows 69
4.2 镜像工具 - Windows 70
4.2 移动设备连接器安装 - Windows 77
4.2 移动设备连接器先决条件 79
4.2 移动设备连接器激活 80
4.2 MDM iOS 许可功能 81

4.2 HTTPS 证书要求 81
4.2 脱机存储库 - Windows 82
4.2 故障转移群集 - Windows 84
4.3 Linux 上的组件安装 85
4.3 在 Linux 上分步安装 ESET PROTECT 85
4.3 MySQL 安装和配置 86
4.3 ODBC 安装和配置 88
4.3 服务器安装 - Linux 90
4.3 服务器先决条件 - Linux 93
4.3 服务器代理安装 - Linux 95
4.3 Web 控制台安装 - Linux 100
4.3 Rogue Detection Sensor 安装 - Linux 101
4.3 移动设备连接器安装 - Linux 102
4.3 移动设备连接器先决条件 - Linux 105
4.3 镜像工具 - Linux 106
4.4 macOS 上的组件安装 113
4.4 服务器代理安装 - macOS 113
4.5 ISO 映像 114
4.6 DNS 服务记录 115
4.7 ESET PROTECT 脱机安装方案 115
5 升级过程 116
5.1 ESET PROTECT组件升级任务 117
5.2 使用 **ESET PROTECT 10.0** 一体式安装程序进行升级 120
5.3 数据库服务器备份/升级 122
5.3 数据库服务器备份和还原 123
5.3 数据库服务器升级 125
5.4 升级故障转移群集中安装的 **ESMC/ESET PROTECT (Windows)** 125
5.5 升级 **Apache Tomcat** 126
5.5 使用一体式安装程序升级 Apache Tomcat (Windows) 126
5.5 手动升级 Apache Tomcat (Windows) 130
5.5 升级 Apache Tomcat 和 Java (Linux) 131
6 迁移和重新安装过程 133
6.1 从一台服务器迁移到另一台服务器 133
6.1 全新安装 – 相同 IP 地址 133
6.1 迁移数据库 – 相同/不同 IP 地址 135
6.2 ESET PROTECT 数据库迁移 136
6.2 MS SQL Server 的迁移过程 136
6.2 MySQL Server 的迁移过程 144
6.2 连接 ESET PROTECT 服务器或 MDM 到数据库 146
6.3 MDM 的迁移 147
6.4 迁移后 **ESET PROTECT 服务器 IP 地址或主机名的更改** 149
7 卸载 ESET PROTECT 服务器及其组件 149
7.1 卸载 **ESET Management 服务器代理** 150
7.2 Windows - 卸载 ESET PROTECT 服务器及其组件 150
7.3 Linux - 升级、重新安装或卸载 ESET PROTECT 组件 152
7.4 macOS - 卸载 ESET Management 服务器代理和 ESET Endpoint 产品 153
7.5 迁移到另一台服务器后，停用旧的 **ESMC/ESET PROTECT/MDM 服务器** 155
8 故障排除 155
8.1 在脱机环境中升级 **ESET PROTECT 组件** 156
8.2 常见安装问题解答 157

8.3 日志文件 159
8.4 诊断工具 160
8.5 升级/迁移 ESET PROTECT 服务器后出现的问题 162
8.6 MSI 日志记录 163
9 ESET PROTECT API 163
10 常见问题解答 163
11 最终用户许可协议 170
12 隐私政策 175

关于帮助

编写此安装指南是为了帮助 ESET PROTECT 的安装和升级并为进程提供说明。

为了保持一致和帮助避免混淆，本指南中使用的术语均基于 ESET PROTECT 参数名称。我们还使用了一组符号来突出显示特定关注内容或重要内容的主题。

注释可以提供有价值的信息，例如特定功能或指向某些相关主题的链接。

这些信息需要您注意，请勿跳过。它通常提供并非关键但很重要的信息。

您应格外注意的关键信息。警告专门用于防止您犯潜在有害的错误。请阅读并了解警告括号中包含的文本，因为它引用了高度敏感的系统设置或有风险的内容。

示例方案描述与其所属主题相关的用例。示例用于解释更复杂的主题。

约定	含义
粗体类型	界面项目的名称，例如框和选项按钮。
斜体类型	您提供的信息的占位符。例如，文件名称或路径表示您键入实际路径或文件名称。
宋体	代码示例或命令。
超链接	支持快速轻松地访问交叉引用的主题或外部 Web 位置。超链接以蓝色突出显示，可能带有下划线。
%ProgramFiles%	可存储 Windows 已安装程序和其他程序的 Windows 系统目录。

- 联机帮助是帮助内容的主要来源。当您有正常的 Internet 连接时，将自动显示联机帮助的最新版本。ESET PROTECT 联机帮助页面在顶部导航标题处包含三个活动的选项卡：安装/升级、管理、VA 部署和 SMB 指南。
- 本指南中的主题分为几个章节和子章节。您可以通过使用顶部的搜索字段来查找相关信息。

从页面顶部的导航栏打开用户指南后，搜索将限制于该指南的内容。例如，如果您打开管理员指南，《安装/升级和 VA 部署指南》中的主题将不包括在搜索结果中。

- ESET 知识库包含对最常见问题的解答以及各种问题的建议解决方案。知识库由 ESET 专业技术人员定期更新，它已成为解决各类问题的最强大工具。
- ESET 论坛可使 ESET 用户轻松获取帮助，并为他人提供帮助。您可以发布任何与您的 ESET 产品相关的问题或难题。

安装/升级/迁移

ESET PROTECT 是一个应用程序，它允许您从一个中心位置的网络环境中管理客户端工作站、服务器和移动设备上的 ESET 产品。借助 ESET PROTECT 的内置任务管理系统，可以在远程计算机上安装 ESET 安全解决方案，并快速响应新的问题和检测。

ESET PROTECT 本身不提供针对恶意代码自身的保护。您的环境保护取决于工作站和移动设备上是否存在 ESET Endpoint Security 等 ESET 安全解决方案，或服务器计算机上是否存在适用于 Microsoft Windows Server 的 ESET Server Security。

ESET PROTECT 围绕两个主要原则构建：

- **集中管理** – 可以从一个位置配置、管理和监视整个网络。
- **可扩展性** – 无论是在小型网络还是大型企业环境中，都可以部署系统ESET PROTECT 专用于使用您的基础架构的增长。

ESET PROTECT 支持新一代 ESET 安全产品，同时也与上一代产品兼容。

ESET PROTECT 帮助页面包含完整的安装和升级指南：

- ESET PROTECT 架构
- 安装过程
- 升级过程
- 迁移过程
- 卸载过程
- 许可证管理
- 部署过程和使用 GPO 或 SCCM 的服务器代理部署
- 安装 ESET PROTECT 后首先执行的步骤
- 管理指南

ESET PROTECT 10.0 中的新功能

增强的 VDI 支持

在设置 VDI 环境时，现在不仅可以通过计算机硬件指纹识别，还可以通过计算机的 FQDN 处理计算机身份（创建新身份和更新现有身份）。了解更多

深色主题

现在，可以尝试使用已添加到 ESET PROTECT 的新深色主题。现在，控制台用户可以在“用户设置”中启用它。了解更多

系统日志的 CEF 格式

现在，可以将日志以通用事件格式发送到系统日志。了解更多

其他改进和可用性更改

可以在变更日志中查找更多详细信息。

架构

ESET PROTECT 是新一代远程管理系统。

若要执行 ESET 安全产品的完整部署，请安装以下组件（Windows 和 Linux 平台）：

- ESET PROTECT 服务器
- ESET PROTECT Web 控制台
- ESET Management 服务器代理

以下支持组件为可选安装，但建议您安装它们，以确保在网络上实现应用程序的最佳性能：

- RD Sensor
- ESET Bridge HTTP 代理
- 移动设备连接器

ESET PROTECT 组件使用证书来与 ESET PROTECT 服务器进行通信。在我们的知识库文章中详细了解 ESET PROTECT 中的证书。

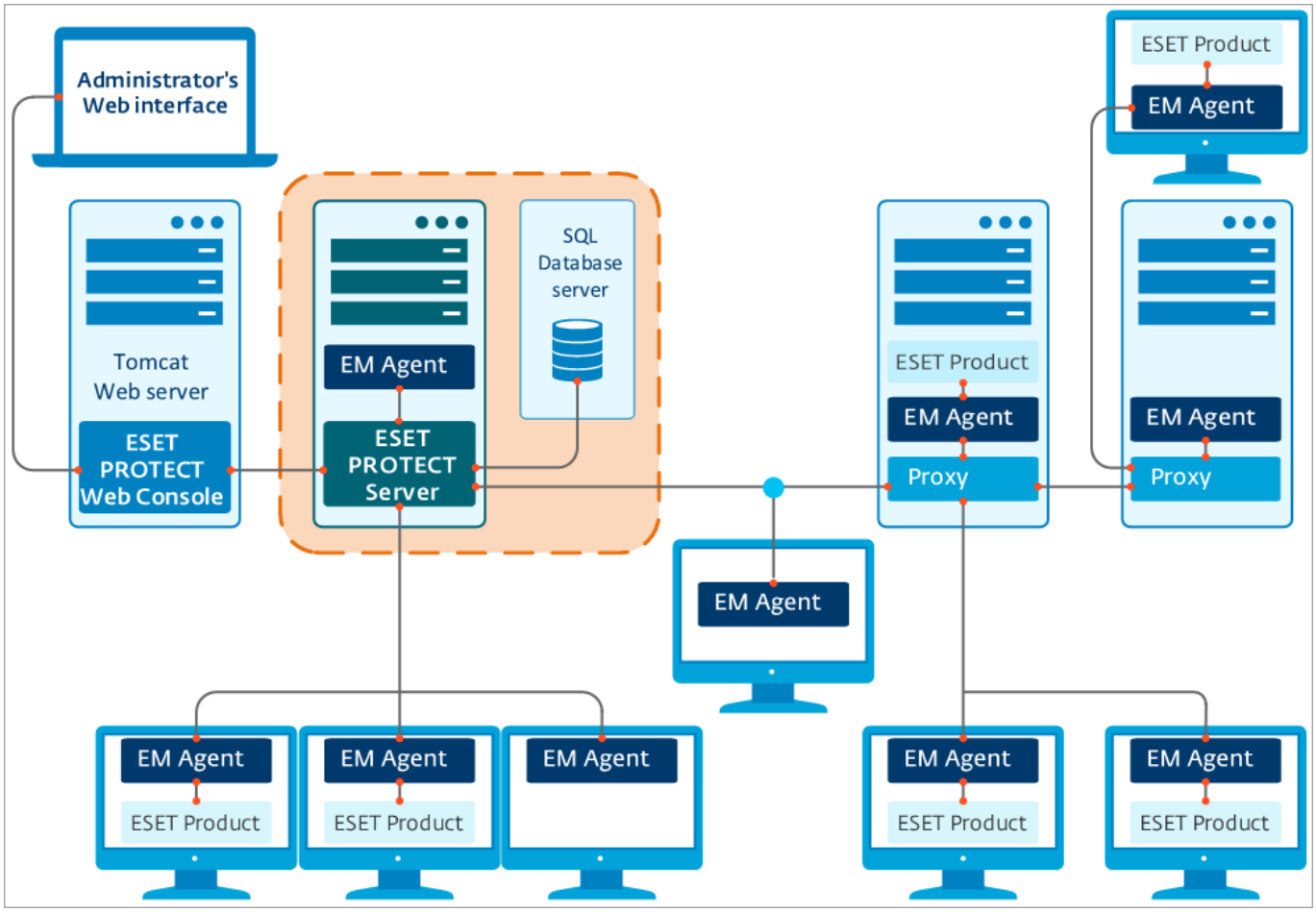
基础架构元素概述

下表中包含 ESET PROTECT 基础架构元素及其功能的概述：

功能	ESET PROTECT 服务器	ESET Management 服务器代理	ESET 安全产品	ESET BridgeHTTP 代理 –	ESET 服务器	移动设备连接器
远程管理 ESET 安全产品（创建策略、任务、报告等）	✔	X	X	X	X	X
在客户端设备上与 ESET PROTECT 服务器通信并管理 ESET 安全产品	X	✔	X	X	X	✔
提供更新、许可证验证	X	X	X	X	✔	X
缓存和转发更新（检测引擎、安装程序、模块）	X	X	✔	✔	X	X
在 ESET Management 服务器代理和 ESET PROTECT 服务器之间转发网络通信	X	X	X	✔	X	X
保护客户端设备	X	X	✔	X	X	X
远程管理移动设备	X	X	X	X	X	✔

服务器

ESET PROTECT 服务器 是可执行应用程序，用于处理从连接到服务器（通过 ESET Management 服务器代理或 HTTP 代理）的客户端接收的所有数据。若要正确地处理数据，服务器需要稳定地连接到存储网络数据的数据库服务器。为了获得更好的性能，我们建议您在另一台计算机上安装数据库服务器。

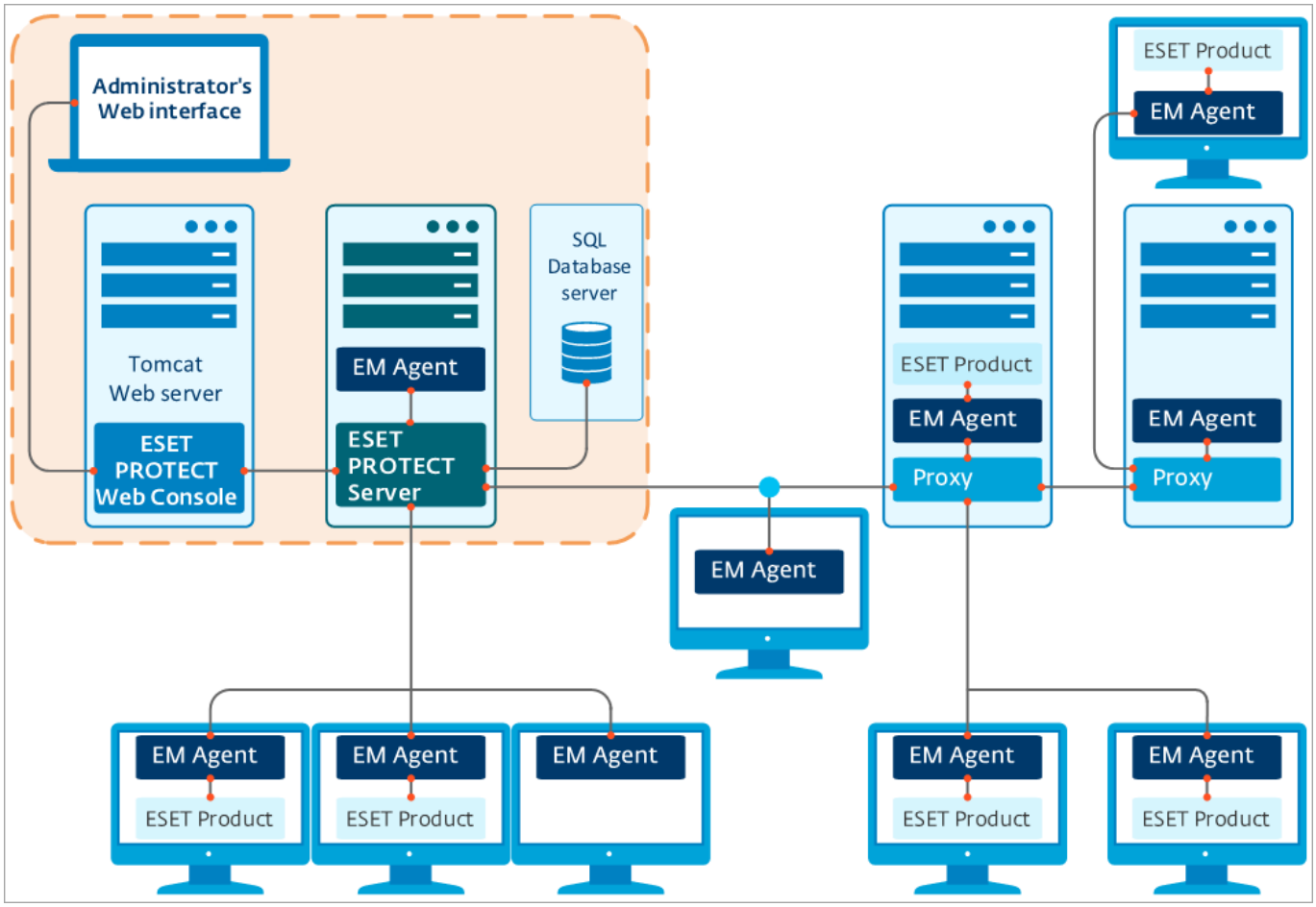


Web 控制台

ESET PROTECT Web 控制台是基于 Web 的用户界面，使您能够在自己的环境中管理 ESET 安全解决方案。它将显示您网络上的客户端状态的概述，并可用于将 ESET 解决方案远程部署到未托管的计算机。可使用您的浏览器来访问 Web 控制台（请参阅支持的 Web 浏览器）。如果您选择使 Web 服务器可通过 Internet 进行访问，则几乎可以从任何地点和设备使用 ESET PROTECT。

Web 控制台将 Apache Tomcat 用作 HTTP Web 服务器。当使用 ESET 安装程序或虚拟设备中捆绑的 Tomcat 时，它仅允许与 Web 控制台建立 TLS 1.2 和 1.3 连接。

可以在未安装 ESET PROTECT 服务器的其他计算机上安装 ESET PROTECT Web 控制台。



ESET BridgeHTTP 代理 –

可以将 ESET Bridge 与 ESET PROTECT 一起用作代理服务以：

- 下载和缓存ESET 模块更新ESET PROTECT 推送的安装和更新包（例如ESET Endpoint Security MSI 安装程序ESET 安全产品更新（组件和产品更新ESET LiveGuard 结果。
- 将与 ESET Management 服务器代理的通信转发到 ESET PROTECT

有关 ESET Bridge 安装和配置的更多详细信息，请阅读 ESET Bridge 联机帮助

Apache HTTP Proxy 用户

从 ESET PROTECT 10.0 开始ESET Bridge 将替代 Apache HTTP Proxy Apache HTTP Proxy 已受有限支持。如果您使用 Apache HTTP Proxy建议您迁移到 ESET Bridge

服务器代理

ESET Management 服务器代理是 ESET PROTECT 的重要组成部分。客户端不会直接与 ESET PROTECT 服务器通信，而是借助服务器代理设施实现此通信。服务器代理从客户端收集信息并将它发送到 ESET PROTECT 服务器。如果 ESET PROTECT 服务器发送了一个客户端任务，该任务将发送到服务器代理，然后由服务器代理将它发送到客户端ESET Management 服务器代理使用的是改进的新通信协议

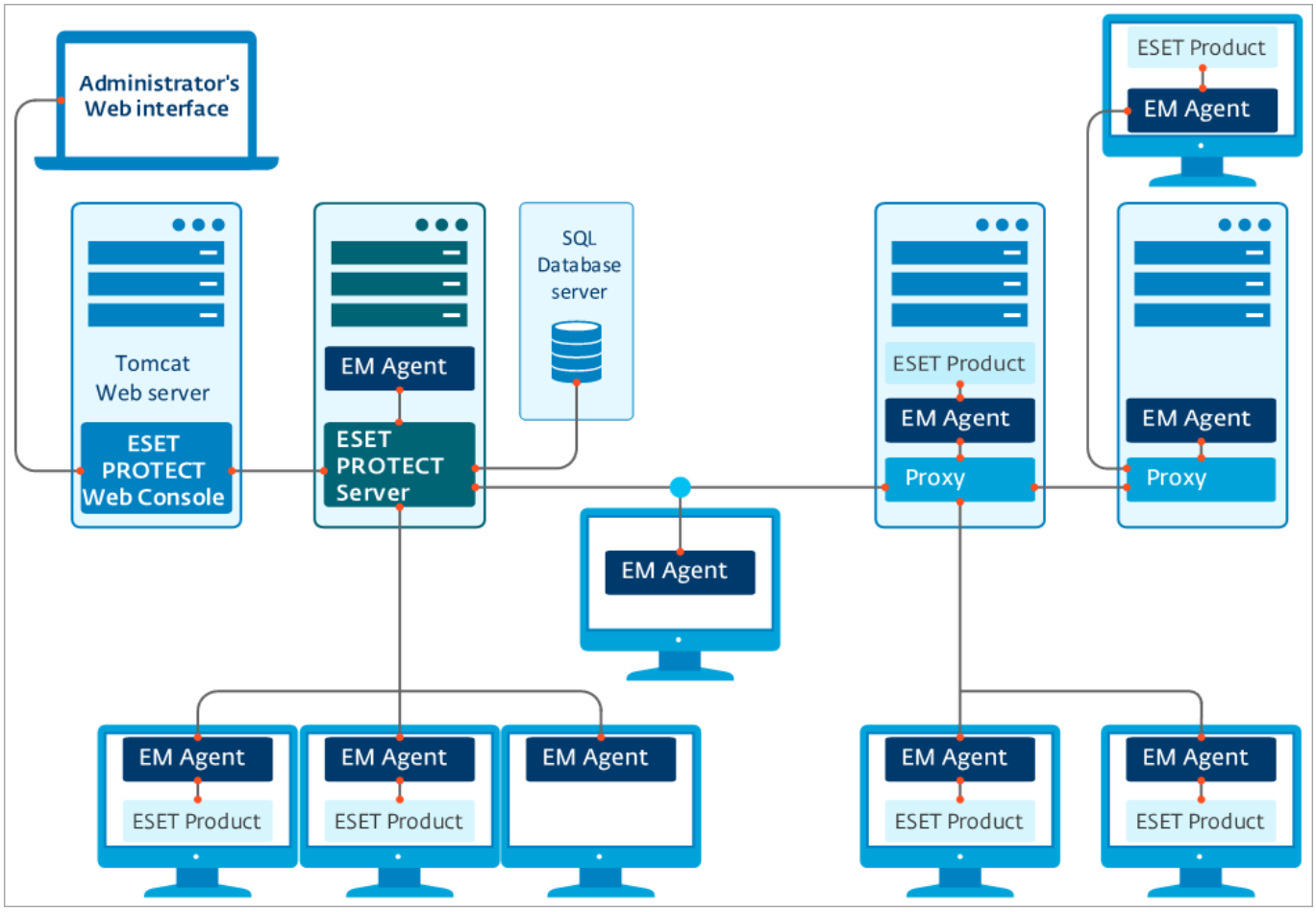
为了简化端点保护的实现，将在 ESET ManagementESET PROTECT 套件中包含独立的 代理。它是一种简单且高度模块化的轻量级服务，涵盖 ESET PROTECT 服务器与任何 ESET 产品或操作系统之间的所有通

信ESET 产品通过服务器代理进行通信，而不是直接与 ESET PROTECT 服务器通信。装有 ESET Management 服务器代理并可以与 ESET PROTECT 服务器通信的客户端计算机被称为“已托管”的计算机。无论是否已安装其他 ESET 软件，您都可以在任何计算机上安装服务器代理。

优点如下：

- 易于设置 – 可以将服务器代理部署为标准企业安装的一部分。
- 即时安全管理 – 由于可将服务器代理配置为存储多种安全方案，因此大大缩短了对检测的反应时间。
- 脱机安全管理 – 即使服务器代理未连接到 ESET PROTECT 服务器，它也可以响应事件。

服务器代理和 ESET PROTECT 服务器之间的通信协议不支持身份验证。任何用于将服务器代理通信转发到需要身份验证的 ESET PROTECT 服务器的代理解决方案将不工作。
如果针对 Web 控制台或服务器代理选择使用非默认端口，可能需要调整防火墙。否则，安装可能会失败。



Rogue Detection Sensor

Rogue Detection Sensor (RD Sensor) 是一个流氓系统检测器工具，用于在您的网络中搜索计算机。该 Sensor 十分方便，因为它可以从 ESET PROTECT 中查找新计算机，您无需手动搜索和添加它们。将立即定位并在预定义的报告中报告所发现的计算机，从而使您可以将它们移动到特定的静态组并继续管理任务。

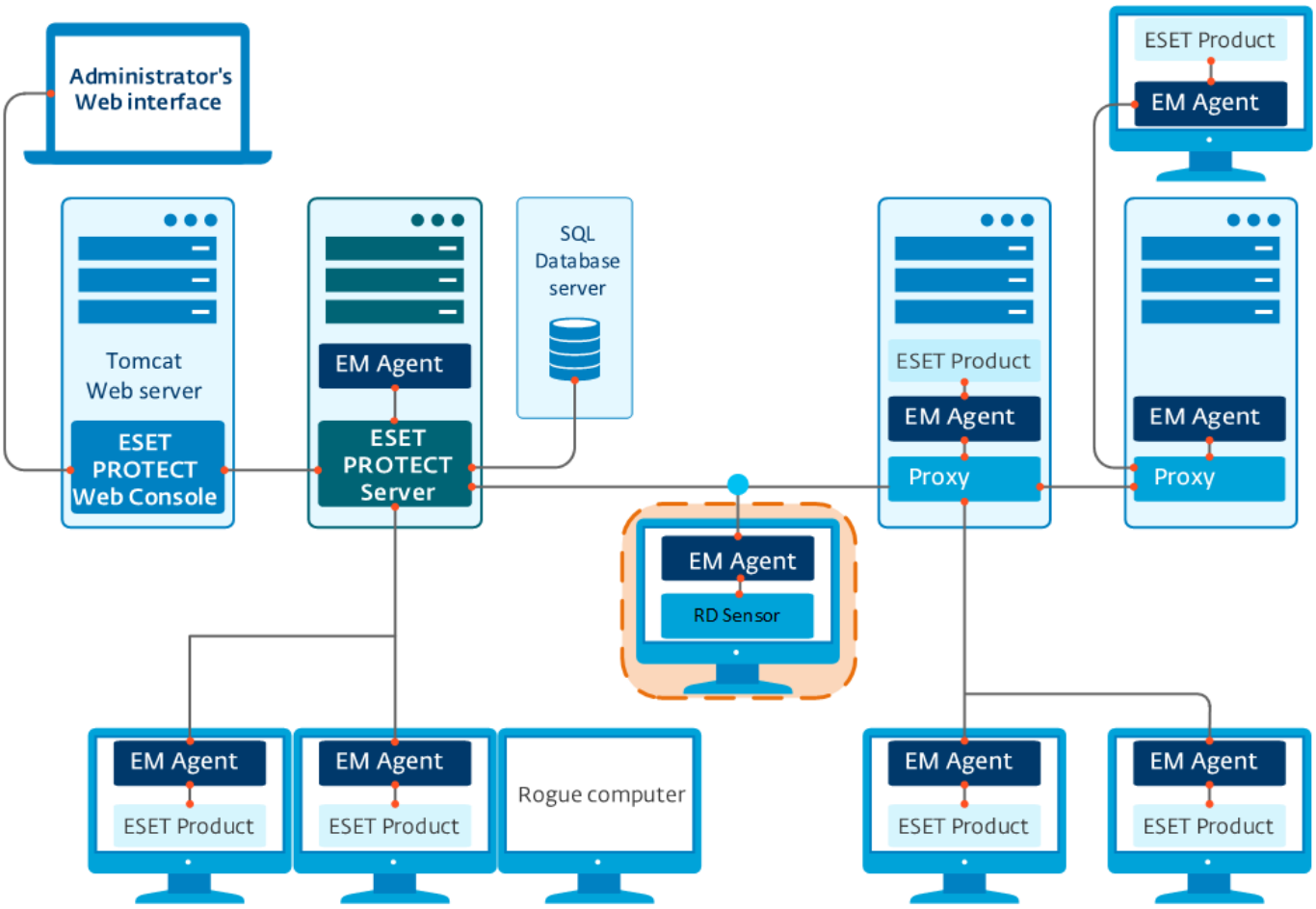
RD Sensor 主动侦听 ARP 广播。当 RD Sensor 检测到新的活动网络组件时RD Sensor 发送 ARP 单播、执行主机指纹验证（使用多个端口）并将有关检测到的计算机的信息发送到 ESET PROTECT 服务器。然后 ESET

PROTECT 服务器将评估在网络上找到的计算机对于 ESET PROTECT 服务器是否处于未知状态，或者是否已被托管。

您无法禁用主机指纹验证，因为它是 RD Sensor 的主要功能。

如果有多个网段，则必须在每个网段上单独安装 Rogue Detection Sensor才能生成整个网络上所有设备的全面列表。

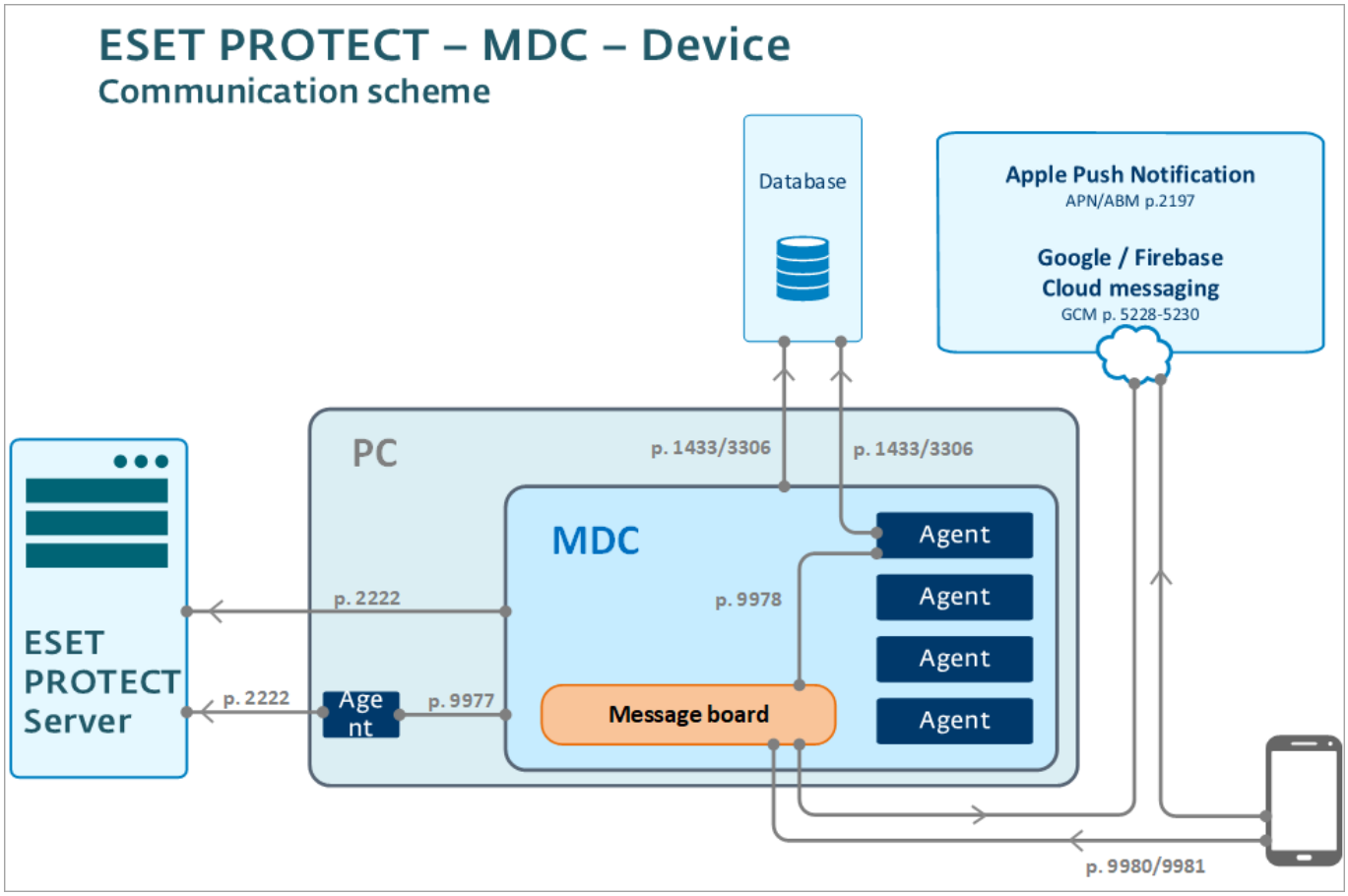
网络结构（域LDAPWindows 网络）中的每台计算机都将通过服务器同步任务自动添加到 ESET PROTECT 服务器的计算机列表中。通过使用 RD Sensor可以很方便地查找不位于域或其他网络结构中的计算机，并将它们添加到 ESET PROTECT 服务器RD Sensor 会记住已发现的计算机，并且不会再次发送相同的信息。



移动设备连接器

ESET PROTECT 移动设备连接器 是一个可用于 ESET PROTECT 的移动设备管理的组件，允许您管理移动设备Android 和 iOS以及管理适用于 Android 的 ESET Endpoint Security

ESET PROTECT 移动设备管理/连接器 (MDM/MDC) 组件（仅限本地）计划结束生命周期。阅读更多建议您迁移到 Cloud MDM



单击此处查看大图

建议您将 MDM 组件部署在独立于托管 ESET PROTECT 服务器的其他主机设备上。

针对约 80 个托管移动设备建议的硬件先决条件为：

硬件	建议配置
处理器	4 个内核2.5 GHz
RAM	4 GB建议）
HDD	100 GB

对于 80 个以上的托管移动设备，硬件要求并不高。从 ESET PROTECT 发送任务与在移动设备上执行任务之间的延迟将随环境中设备的数量成比例地增加。

按照 Windows一体式安装程序或组件安装）或 Linux 的 MDM 安装说明进行操作。

ESET Bridge HTTP 代理、镜像工具和直接连接之间的区别

ESET 产品通信涉及检测引擎和程序模块更新以及 ESET LiveGrid® 数据（参见下表）和许可证信息的交换。

ESET PROTECT 会从存储库中下载最新的产品以分发给客户端计算机。分发结束后，就可以在目标计算机上部署该产品。

安装了 ESET 安全产品之后，必须激活该产品，这意味着产品需要向许可证服务器验证您的许可证信息。激

活后，会定期更新检测引擎和程序模块。

ESET LiveGrid® 预警系统帮助确保 ESET 即时并持续地获得有关新威胁的信息，以便快速保护客户的计算机。该系统允许将新的检测提交给 ESET 研究实验室，以便在此处对这些检测进行分析和处理。

大多数网络通信是由产品模块更新产生的。通常ESET 安全产品每月会下载大约 23.9 MB 的模块更新。

只有 ESET LiveGrid® 数据（约 22.3 MB和更新版本文件（最多 11 KB是无法缓存的分发文件。

更新类型有两种 – 级别更新和微量更新。有关更新类型的详细信息，请参阅我们的知识库文章

在向计算机网络分发更新时，可使用 2 种方法来减少网络负载，即 ESET Bridge HTTP 代理或镜像工具（可用于 Windows 和 Linux

请参阅本知识库文章以设置镜像工具链（配置镜像工具为从其他镜像工具下载更新）。

ESET 通信类型

通信类型	通信频率	网络通信影响	代理–转发通信	代理缓存选项1	镜像选项2	脱机环境选项
服务器代理部署（来自存储库的推送/ Live 安装程序）	一次	大约 每个客户端 50 MB	是	是3	否	是（GPO / SCCM编辑过的 Live 安装程序）3
Endpoint 安装（通过存储库进行软件安装）	一次	大约 每个客户端 100 MB	是	是3	否	是（GPO / SCCM通过程序包 URL 进行安装）4
检测引擎模块/程序模块更新	6 次以上/天	每月 23.9 MB 5	是	是	是	是（脱机 Mirror Tool 和自定义 HTTP 服务器）5
更新版本文件 update.ver	大约 8 次/天	每月 2.6 MB 7	是	否	-	-
激活/许可检查	4 次/天	忽略不计	是	否	否	是（ESET Business Account 上生成的脱机文件）8
ESET LiveGrid® 基于云的信誉	联机	11 MB/月	是	否	否	否

1.有关代理缓存影响/优势，请参见何时开始使用 ESET Bridge HTTP 代理？

2.有关镜像影响，请参见何时开始使用镜像工具？

3.每次安装/升级之后，我们建议一开始只部署一个服务器代理（每个特定版本一个/Endpoint以便缓存该安装程序。

4.若要在大型网络上部署 ESET Management 服务器代理，请参见使用 GPO 和 SCCM 执行服务器代理部署

5.您最初的检测引擎更新可能比平常大，具体取决于安装程序包的年份，因为会下载所有较新的检

测引擎更新和模块更新。我们建议一开始只安装一个客户端，然后让它执行更新，以便缓存所需的检测引擎和程序模块更新。

6.在没有 Internet 连接的情况下，Mirror Tool 无法下载检测引擎更新。您可以使用 Apache Tomcat 作为 HTTP 服务器来将更新下载到镜像工具（可用于 Windows 和 Linux）可用的目录中。

7.当检查检测引擎更新时，总是会下载并分析 *update.ver* 文件。默认情况下，ESET Endpoint 产品的计划程序会每小时查询是否有新的更新。我们假定客户端工作站一天 8 小时都处于打开状态。*update.ver* 文件包含大约 11 kB 的数据。

8.已下载脱机许可证文件 ESET Business Account

您不可以使用 ESET Bridge HTTP 代理缓存适用于版本 4 和版本 5 的更新。要分发适用于这些产品的更新，请使用镜像工具

何时开始使用 ESET Bridge (HTTP 代理)

根据我们的实际测试，如果您网络中至少具有 37 台计算机，我们建议您部署 ESET Bridge HTTP 代理

正确设置 HTTP 代理服务器上的日期和时间对于有效缓存很重要。几分钟的差异也会导致缓存机制无法有效工作以及会下载更多不必要的文件。

在 1.000 台计算机组成的测试网络中执行多次安装和卸载的情况下，分析其中更新单独使用的网络带宽可以得出以下结论：

- 如果一台计算机直接连接到 Internet（不使用 HTTP 代理），更新下载量平均为 23.9 MB/月
- 使用 HTTP 代理，整个网络的下载总量为 900 MB/月

简单比较计算机网络中使用直接 Internet 连接或 HTTP 代理每月下载的更新数据

您公司网络中的电脑数目	25	36	50	100	500	1.000
直接连接到 Internet（MB/月）	375	900	1.250	2.500	12.500	25.000
ESET Bridge HTTP 代理（MB/月）	30	50	60	150	600	900

何时开始使用 Mirror Tool

如果您有脱机环境，这意味着您网络中的计算机很长一段时间（数月或一年）未连接到 Internet，镜像工具（可用于 Windows 和 Linux）是用于分发产品模块更新的唯一方法，因为如果存在可用的新更新，该工具就会根据每个新更新请求下载所有可用的 Level 和 Nano 更新。

请参阅本知识库文章以设置镜像工具链（配置镜像工具为从其他镜像工具下载更新）。

ESET Bridge HTTP 代理和镜像工具之间的主要区别是，ESET Bridge HTTP 代理仅下载缺少的更新（例如，Nano 更新 3），而 Mirror Tool 会下载所有可用的 Level 和 Nano 更新（或者如果指定，仅 Level 更新），无论特定产品模块是否缺少更新都会下载。

使用镜像工具时，流式更新不可用。我们建议，在可能时首选通过 ESET Bridge HTTP 代理进行更新，而不是从镜像更新。即使计算机脱机但可以访问连接到 Internet 并且可以运行 ESET Bridge HTTP 代理以缓存更新文件的另一台计算机，可选择此选项。

在具有 1.000 台计算机的同一网络中，我们使用镜像工具代替 ESET Bridge HTTP 代理进行了测试。分析显示：该月下载更新 5,500 MB向网络中添加更多台计算机并不会增加更新下载的量。相较于客户端直接连接到 Internet 所用的配置，此方法在负载方面下降的幅度较大，但在性能改善方面本质上不如使用 HTTP 代理的时候。

您公司网络中的电脑数目	25	36	50	100	500	1.000
直接连接到 InternetMB/月）	375	900	1.250	2.500	12.500	25.000
镜像工具MB/月）	5.500	5.500	5.500	5.500	5.500	5.500

即使网络中存在 1.000 台以上的计算机，但使用 ESET Bridge HTTP 代理或镜像工具均不会明显增加与更新有关的带宽使用。

系统要求和大小调整

您的系统必须满足一组硬件数据库网络和软件先决条件，才能安装和操作 ESET PROTECT

支持的操作系统

以下部分将介绍适用于 WindowsLinuxmacOS 和移动操作系统版本的 ESET PROTECT 组件支持。

Windows

下表显示了每个 ESET PROTECT 组件支持的 Windows 操作系统：

操作系统	服务器	服务器代理	RD Sensor	MDM
Windows Server 2008 R2 x64 SP1（已安装 KB4493730 和 KB4039648）		✔	✔	
Windows Server 2008 R2 CORE x64（已安装 KB4493730 和 KB4039648）		✔	✔	
Windows Storage Server 2008 R2 x64（已安装 KB4493730 和 KB4039648）		✔	✔	
Microsoft SBS 2011 Standard x64		✔	✔	
Microsoft SBS 2011 Essentials x64		✔	✔	
Windows Server 2012 x64	✔	✔	✔	✔
Windows Server 2012 CORE x64	✔	✔	✔	✔
Windows Server 2012 R2 x64	✔	✔	✔	✔
Windows Server 2012 R2 CORE x64	✔	✔	✔	✔
Windows Storage Server 2012 R2 x64	✔	✔	✔	✔
Windows Server 2016 x64	✔	✔	✔	✔
Windows Storage Server 2016 x64	✔	✔	✔	✔

操作系统	服务器	服务器代理	RD Sensor	MDM
Windows Server 2019 x64	✔	✔	✔	✔
Windows Server 2022 x64	✔	✔	✔	✔

操作系统	服务器	服务器代理	RD Sensor	MDM
Windows 7 x86 SP1（已具有最新 Windows 更新，至少 KB4474419 和 KB4490628）		✔	✔	
Windows 7 x64 SP1（已具有最新 Windows 更新，至少 KB4474419 和 KB4490628）		✔	✔	
Windows 8 x86		✔	✔	
Windows 8 x64		✔	✔	*
Windows 8.1 x86		✔	✔	
Windows 8.1 x64		✔	✔	*
Windows 10 x86		✔	✔	
Windows 10 x64（所有官方版本）	*	✔	✔	*
基于 ARM 的 Windows 10		✔		
- AND	*	✔	✔	*
基于 ARM 的 Windows 11		✔		

ESET PROTECT 移动设备管理/连接器 (MDM/MDC) 组件（仅限本地）计划结束生命周期。阅读更多建议您迁移到 Cloud MDM

* 在客户端操作系统上安装 ESET PROTECT 组件可能违反 Microsoft 许可政策。检查 Microsoft 许可政策或者咨询您的软件提供商以了解详细信息。在 SMB/小型网络环境中，建议您使用 Linux ESET PROTECT 安装或虚拟设备（适用时）。

较旧版本的 Microsoft Windows 系统

- ESET Management 服务器代理 10.x 是支持 Windows 7/8.x 和 Windows Server 2008 R2/Microsoft SBS 2011 的最后一个版本。
- 始终安装最新的服务包，尤其是在较旧的系统上，如 Server 2008 和 Windows 7
- ESET PROTECT 不支持管理运行 Windows 7（无 SP Widows Vista 和 Windows XP 的计算机。
- 从 2020 年 3 月 24 日开始ESET 将不再正式支持以下 Microsoft Windows 操作系统上安装的 ESET PROTECTServer 和 MDM或为其提供技术支持Windows 7Windows Server 2008所有版本）。我们不支持非法或盗版操作系统。

从 2019 年 1 月开始，面向企业、商业或生产用途的 Oracle JAVA SE 8 公开更新将需要商业许可证。如果不购买 JAVA SE 订阅，可以使用本指南来转换为免费替代方案。请参阅 JDK 的受支持版本

您可以在非服务器操作系统上运行 ESET PROTECT而无需 ESXi可以在桌面操作系统上安装 VMware Player，并部署 ESET PROTECT 虚拟设备

Linux

下表显示了每个 ESET PROTECT 组件支持的 Linux 操作系统：

操作系统	服务器	服务器代理	RD Sensor	MDM
Ubuntu 16.04.1 LTS x64 Desktop	✔	✔	✔	*
Ubuntu 16.04.1 LTS x64 Server	✔	✔	✔	*
Ubuntu 18.04.1 LTS x64 Desktop	✔	✔	✔	*
Ubuntu 18.04.1 LTS x64 Server	✔	✔	✔	*
Ubuntu 20.04 LTS x64	✔	✔	✔	*
Ubuntu 22.04 LTS x64		✔	✔	
Linux Mint 20		✔	✔	
RHEL Server 7 x64	✔	✔	✔	*
RHEL Server 8 x64	**	✔		**
RHEL Server 9 x64		✔	✔	
CentOS 7 x64	✔	✔	✔	*
SLED 15 x64		✔	✔	
SLES 12 x64		✔	✔	
SLES 15 x64		✔	✔	
Debian 9 x64		✔	✔	
Debian 10 x64	✔	✔	✔	*
Debian 11 x64		✔	✔	
Oracle Linux 8		✔	✔	
Amazon Linux 2		✔	✔	

*

ESET PROTECT 移动设备管理/连接器 (MDM/MDC) 组件（仅限本地）计划结束生命周期。阅读更多建议您迁移到 Cloud MDM

** Red Hat Entreprise Linux Server 8.x 不支持生成 *.pdf* 报告 – 请参阅 ESET PROTECT 已知问题中的更多详细信息。

macOS

操作系统	服务器代理
macOS Sierra (10.12)	✔
macOS High Sierra (10.13)	✔
macOS Mojave (10.14)	✔
macOS Catalina (10.15)	✔
macOS Big Sur (11.0)	✔
macOS Monterey (12.0)	✔

操作系统	服务器代理
macOS Ventura (13.0)	✔

仅支持 MacOS 作为客户端。适用于 macOS 的 ESET Management 服务器代理和 ESET 产品可以安装在 macOS 上。但 ESET PROTECT 服务器不能安装在 macOS 上。

移动

ESET PROTECT 移动设备管理/连接器 (MDM/MDC) 组件（仅限本地）计划结束生命周期。阅读更多建议您迁移到 Cloud MDM

操作系统	EESA	EESA 设备所有者	MDM iOS	MDM iOS ABM
Android 6.x+	✔			
Android 7.x+	✔	✔		
Android 8.x+	✔	✔		
Android 9.0	✔	✔		
Android 10.0	✔	✔		
Android 11	✔	✔		
Android 12	✔	✔		
Android 13	✔	✔		
iOS 9.x+			✔	*
iOS 10.x+			✔	*
iOS 11.x+			✔	*
iOS 12.0.x			✔	*
iOS 13.x+			✔	✔
iOS 14.x+			✔	✔
iOS 15			✔	✔
iOS 16			✔	✔
iPadOS 13.x+			✔	✔
iPadOS 14.x+			✔	✔
iPadOS 15			✔	✔
iPadOS 16			✔	✔

* iOS DEP 仅在选择国家/地区中可用。

建议您将移动设备的操作系统更新为最新版本，以确保接收就到重要的安全补丁。

iOS 10.3 及更高版本的要求：

自 iOS 10.3 发布以来，作为注册配置文件一部分安装的 CA 可能不会自动受信任。若要解决此问题，请按照以下步骤进行操作：
a)使用受 Apple 信任的证书颁发者发布的证书。
b)在注册之前手动安装证书信任。这意味着您需要在注册之前在移动设备上手动安装根 CA然后为安装的证书启用完全信任

iOS 12 的要求：

请查看 iOS 10.3 及更高版本的要求。

- 连接必须使用 **TLS 1.2 或更高版本**。
- 连接必须使用 **AES-128** 或 **AES-256 对称密码**。协商的 TLS 连接密码套件必须通过 **Elliptic Curved Diffie-Hellman Ephemeral (ECDHE) 密钥交换**支持**完全向前保密 (PFS)**，并且必须为以下情形之一：

```
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
```

- 使用 **RSA 密钥**签名，长度**至少为 2048 位**。证书的哈希算法必须为**摘要长度（有时称为“指纹”）至少为 256 的 SHA-2**（即 **SHA-256 或更大**）。可以在已打开高级安全的 ESET PROTECT 中生成满足这些要求的证书。
- 证书必须包含**整个证书链（包括根 CA**。证书中包含的根 CA 用于建立与设备的信任，并作为 MDM 注册配置文件的一部分安装。

iOS 13 的要求：

- 管理 iOS 13 移动设备需要满足新的 Apple 通信证书 (MDM HTTPS) 要求。在 2019 年 7 月 1 日之前颁发的证书也必须满足这些条件。
- 由 ESMC CA 签名的 HTTPS 证书不满足这些要求。

> 强烈建议您在满足 Apple 通信证书要求之前，不要将移动设备升级到 iOS 13。此类操作将导致您的设备停止连接到 ESET PROTECT MDM。

- 如果您在没有正确证书的情况下已进行升级，并且设备已停止连接到 ESET PROTECT MDM，则需要先将当前用于与 iOS 设备通信的 HTTPS 证书更改为满足 Apple 通信证书 (MDM HTTPS) 要求的证书，然后再重新注册您的 iOS 设备。
- 如果您尚未升级到 iOS 13，请确保当前用于与 iOS 设备通信的 MDM HTTPS 证书满足 Apple 通信证书 (MDM HTTPS) 要求。如果满足，可以继续将 iOS 设备升级到 iOS 13。如果不满足要求，请将当前 MDM HTTPS 证书更改为满足 Apple 通信证书 (MDM HTTPS) 要求的 HTTPS 证书，然后继续将 iOS 设备升级到 iOS 13。

支持的桌面设置环境

桌面设置使设备管理更轻松，并可以更快地将台式计算机交付给最终用户。

已设置的桌面通常为物理或虚拟。有关使用流式操作系统（Citrix 设置服务）的虚拟环境，请参阅支持的虚拟机监控程序列表。

ESET PROTECT 支持:

- 具有非持续磁盘的系统
- VDI 环境
- 识别克隆的计算机

支持的虚拟机监控程序和虚拟机监控程序扩展

虚拟机监控程序	ESET PROTECT	ESET Full Disk Encryption
Citrix XenServer	✔	X
Microsoft Hyper-V	✔	✔（不支持安全启动）
VMware vSphere	✔	✔ (7.0.3.00300)
VMware ESXi	✔	✔ (7.0)
VMware Workstation	✔	✔ (16.2.3)
VMware View	✔	X
Oracle VirtualBox	✔	X
VMware Fusion	X	✔ (12.2.3)
Parallels	X	✔

虚拟机监控程序扩展	ESET PROTECT	ESET Full Disk Encryption
Citrix VDI-in-a-box	✔	X
Citrix XenDesktop	✔	X

工具

（适用于虚拟设备和物理设备）

- Microsoft SCCM
- Windows Server 2012/2016/2019/2022 Server Manager
- Windows Admin Center

硬件和基础结构大小调整

ESET PROTECT 服务器计算机应满足下表中的以下硬件建议。

客户端数	ESET PROTECT 服务器 + SQL 数据库服务器				
	CPU 核心	CPU 时钟速度 (GHz)	RAM (GB)	磁盘驱动器1	磁盘 IOPS2
最多 1, 000	4	2.1	4	单个	500
5.000	8	2.1	8		1.000
10,000 3	4	2.1	16	单独	2.000
20.000	4	2.1	16		4.000
50.000	8	2.1	32		10.000
100.000	16	2.1	64+		20.000

1 单个/单独磁盘驱动器 – 对于具有超过 10, 000 个客户端的系统，建议您将数据库安装在单独的驱动器上。

2 IOPS（每秒 I/O 操作总数）– 最小要求值。

- 建议每个连接的客户端的 IOPS 约为 0.2，但不小于 500。
- 可以使用 diskspd 工具的以下命令检查驱动器的 IOPS

客户端数	命令
最多 5,000 个客户端	`diskspd.exe -c1000M -b4K -d120 -Sh -r -z -w50 C:\testfile.dat`
超过 5,000 个客户端	`diskspd.exe -c10000M -b4K -d600 -Sh -r -z -w50 C:\testfile.dat`

3 查看适用于 10,000 个客户端环境的示例方案

磁盘驱动器建议

磁盘驱动器是影响 ESET PROTECT 性能的关键因素。

- SQL Server 实例可以与 ESET PROTECT 服务器共享资源，以实现利用率的最大化和延迟的最小化。在单台计算机上运行 ESET PROTECT 服务器和数据库服务器可提高 ESET PROTECT 性能。
- 如果将数据库和事务日志文件放置在单独的驱动器上（最好是单独的物理 SSD 驱动器），则 SQL Server 的性能将得到增强。
- 如果您只有一个磁盘驱动器，建议您使用 SSD 驱动器。
- 建议您使用全闪存体系结构。固态磁盘 (SSD) 的速度比标准 HDD 快得多。
- 如果您的 RAM 配置较高，则采用 R5 设置 SAS 就足够了。已测试的配置R5 中的 10 个 1.2TB SAS 磁盘 – 4+1 中的两个奇偶校验组，没有额外缓存。
- 使用企业级 SSD 和高 IOPS 时，性能未提高。
- 100 GB 容量足以满足任何数量的客户端。如果您经常备份数据库，可能需要更高的容量。
- 请勿使用网络驱动器，因为其性能会降低 ESET PROTECT 的速度。
- 如果您现有的多层存储基础架构允许在线存储迁移，则建议您从速度较慢的共享层开始，并监控 ESET PROTECT 的性能。如果您注意到读/写延迟超过 20 毫秒，则可以从存储层无延迟地移至速度更快的层，以使用成本效益最佳的后端。可以在虚拟机监控程序中执行相同操作（如果将 ESET PROTECT 用作虚拟机）。

针对不同客户端数调整大小的建议

可以在下面找到一定量的客户端运行一年的虚拟环境的性能结果。

> 数据库和 ESET PROTECT 正在具有相同硬件配置的单独虚拟机上运行。

CPU 核心	CPU 时钟速度 (GHz)	RAM (GB)	性能		
			10,000 个客户端	20,000 个客户端	40,000 个客户端
8	2.1	64	高	高	正常
8	2.1	32	正常	正常	正常
4	2.1	32	正常	正常	低
2	2.1	16	低	低	不足

CPU 核心	CPU 时钟速度 (GHz)	RAM (GB)	性能		
			10,000 个客户端	20,000 个客户端	40,000 个客户端
2	2.1	8	非常低 (不建议)	非常低 (不建议)	不足

部署建议

部署 ESET PROTECT 的最佳做法

客户端数	最多 1,000	1,000–5,000	5,000–10,000	10,000–50,000	50,000–100,000	100,000+
ESET PROTECT 服务器和数据库服务器在同一台计算机上	✔	✔	✔	X	X	X
使用 Microsoft SQL Express	✔	?*	X	X	X	X
使用 Microsoft SQL	✔	✔	✔	✔	✔	✔
使用 MySQL	✔	✔	✔	X	X	X
使用 ESET PROTECT 虚拟设备	✔	✔	不建议	X	X	X
使用 VM 服务器	✔	✔	✔	可选	X	X
建议的连接间隔（部署阶段）	60 秒	5 分钟	10 分钟	15 分钟	20 分钟	25 分钟
建议的连接间隔（部署之后，标准使用期间）	10 分钟	10 分钟	20 分钟	30 分钟	40 分钟	60 分钟

* 为了避免填充 ESET PROTECT 数据库，如果您也使用 ESET Inspect?我们不推荐此方案。

连接间隔

ESET PROTECT 服务器使用永久连接来连接到 ESET Management 服务器代理。尽管采用永久连接，但数据传输仅在连接间隔期间发生一次。例如，如果将 5,000 个客户端上的复制间隔设置为 8 分钟，则在 480 秒内有 5,000 次传输（每秒 10.4 次）。确保设置适当的客户端连接间隔。即使针对高性能硬件配置，也请确保将“服务器代理 – 服务器”连接总数保持在每秒 1,000 个以下。

如果服务器过载或恶意软件在运行（例如，将 20,000 个客户端连接到每 10 分钟间隔最多可服务 10,000 个客户端的服务器），将忽略部分连接的客户端。未连接的客户端稍后会尝试连接到 ESET PROTECT 服务器。

单个服务器（小型企业）

要管理小型网络（1,000 个客户端或更少），请使用一台安装有 ESET PROTECT 服务器以及所有 ESET PROTECT 组件的计算机。在 SMB/小型网络环境中，建议您使用 Linux ESET PROTECT 安装或虚拟设备（适用时）。

远程分支与代理

如果客户端计算机不能直接看到 ESET PROTECT 服务器，则使用代理转发 ESET 产品通信HTTP代理不会汇总通信，也不会降低复制的通信量。

高可用性（企业）

针对企业环境（超过 10,000 个客户端），请考虑以下事项：

- RD Sensor 有助于搜索网络并发现新计算机。
- 可以在故障转移群集上安装 ESET PROTECT 服务器。
- 为大量客户端配置 HTTP 代理或使用更多代理。

企业解决方案的 Web 控制台配置或低性能系统

默认情况下，通过适用于 Windows 的一体式安装程序安装的 ESET PROTECT Web 控制台会保留 1024 MB 的内存限制用于 Apache Tomcat

可以根据您的基础架构更改默认的 Web 控制台配置：

- 在企业环境中，处理大量对象时，默认 Web 控制台配置可能会不稳定。更改 Tomcat 设置以防止内存不足。在进行这些更改之前，请确保系统具有足够的 RAM16 GB 或更多）。
- 如果您的系统是低性能系统，具有有限的硬件资源，可以减少 Tomcat 内存使用量。

下面提供了建议的内存值。您可以根据硬件资源调整 Tomcat 内存设置。

Windows

1.打开 *tomcat9w.exe* 或运行 `Configure Tomcat` 应用程序。

2.切换到 **Java** 选项卡。

3.更改内存使用量：

a.增加（企业）：将**初始内存池**值更改为 2048 MB并将**最大内存池**更改为 16384 MB

b.减少（低性能系统）：将**初始内存池**值更改为 256 MB并将**最大内存池**更改为 2048 MB

4.重新启动 Tomcat 服务。

LINUX 和 ESET PROTECT 虚拟设备

1.将终端作为根打开或使用 `sudo`

2.打开文件

a.ESET PROTECT 虚拟设备/CentOS`/etc/sysconfig/tomcat`

b.Debian: `/etc/default/tomcat9`

3.将下列行添加到文件：

a.增加内存使用量（企业）：`JAVA_OPTS="-Xms2048m -Xmx16384m"`

b.减少内存使用量（低性能系统）：`JAVA_OPTS="-Xms256m -Xmx2048m"`

4.保存文件并重新启动 Tomcat 服务。

```
service tomcat restart
```

部署 10,000 个客户端

可以在下面找到其中 10,000 个客户端运行一年的虚拟环境的性能结果。

虚拟机监控程序服务器配置

组件	值
VMware	ESXi 6.7 Update 2 及更高版本（VM 版本 15）
虚拟机监控程序	VMware ESXi, 6.7.0
逻辑处理器	112
处理器类型	Intel(R) Xeon(R) Platinum 8176 CPU @ 2.10GHz

专用计算机上运行的测试
数据库和 ESET PROTECT 正在具有相同硬件配置的单独虚拟机上运行。

虚拟机上使用的软件

ESET PROTECT:

- 操作系统：Microsoft Windows Server 2016 Standard (64-bit)

数据库：

- Database server: Microsoft SQL Server 2017 (RTM) Standard Edition (64-bit)
- 操作系统：Microsoft Windows Server 2016 Standard (64-bit)

ESET PROTECT 环境说明

- 10,000 个连接客户端
- 大约 2,000 个动态组和 2,000 个动态组的模板
- 大约 255 个静态组
- 20 个用户
- ESET Management 服务器代理的连接间隔为 15 分钟

• 在环境运行一年后，数据库大小为 15 GB

CPU 数量	RAM (GB)	性能
8	64	高
4	32	正常
2	16	低
2	8	非常低（不建议）

数据库

指定安装 ESET PROTECT 服务器时要使用的数据库服务器和连接器。可以使用环境中运行的现有数据库服务器，但它必须满足以下要求。

默认情况下，ESET PROTECT 10.0 一体式安装程序将安装 Microsoft SQL Server Express 2019。

o如果使用的是旧版 Windows Server 2012 或 SBS 2011，将默认安装 Microsoft SQL Server Express 2014。

o安装程序会自动生成一个用于数据库验证的随机密码（存储在 *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini* 中）。

Microsoft SQL Server Express 的每个关系数据库具有 10 GB 大小限制。不建议使用 Microsoft SQL Server Express。
- 在企业环境或大型网络中。
- 如果要将 ESET PROTECT 与 ESET Inspect 一起使用。

受支持的数据库服务器和数据库连接器

ESET PROTECT 支持两种类型的数据库服务器，Microsoft SQL Server 和 MySQL。

ESET PROTECT 不支持 MariaDB，MariaDB 是大多数当前 Linux 环境中的默认数据库，会在您选择安装 MySQL 时随之一起安装。

受支持的数据库服务器	受支持数据库版本	受支持的数据库连接器
Microsoft SQL Server	• Express 和非 Express 版本 • 2014, 2016, 2017, 2019	• SQL 服务器 • SQL Server Native Client 10.0 • ODBC Driver for SQL Server 11，13，17，18
MySQL	• 5.6* • 5.7 • 8.0	MySQL ODBC 驱动程序版本： • 5.1, 5.2 • 5.3.0-5.3.10 • 8.0.16, 8.0.17 • 8.0.27，8.0.31 仅限 Windows

* MySQL 5.6 在 2021 年 2 月结束生命周期。建议您将 MySQL 数据库服务器升级到版本 5.7 及更高版本。

以下 MySQL ODBC 驱动程序版本不受支持：
- 5.3.11 及更高版本 5.3.x
- 8.0.0-8.0.15
- 8.0.18 及更高版本

数据库服务器硬件要求

请参阅硬件和大小调整说明。

性能建议

为获得最佳性能，建议您使用受支持的最新 Microsoft SQL Server 作为 ESET PROTECT 数据库。虽然 ESET PROTECT 与 MySQL 兼容，但在处理大量数据（包括面板、检测和客户端）时，使用 MySQL 可能对系统性能造成不利影响。相较于使用 MySQL 使用 Microsoft SQL Server 的相同硬件可以显著处理更多客户端。

可以决定是否要在以下位置安装 SQL 数据库服务器：

- 与 ESET PROTECT 服务器所在的同一台计算机。
- 同一台计算机，但在单独的磁盘上。
- 用于安装 SQL 数据库服务器的专用服务器。

如果您希望管理 10,000 个以上的客户端，我们建议您使用具有预留资源的专用计算机。

数据库	SMB 用户	企业用户	客户端限制	Windows	Linux
Microsoft SQL Express	✔	（可选）	5.000	✔	
Microsoft SQL Server	✔	✔	无	✔	
MySQL	✔	✔	10.000	✔	✔

附加信息

ESET PROTECT 服务器不使用集成的备份。我们强烈建议您备份您的数据库服务器，以防止丢失数据。

- 在域控制器（例如 Windows SBS/Essentials 上不要安装 SQL Server。建议您在其他服务器上安装 ESET PROTECT 或者在安装期间不选择 SQL Server Express 组件（这要求您使用现有 SQL 或 MySQL Server 来运行 ESET PROTECT 数据库）。
- 如果您想要使用将仅限访问 ESET PROTECT 数据库的专用数据库用户帐户，必须先创建具有特定权限的用户帐户，然后再开始安装。有关详细信息，请参阅专用数据库用户帐户。此外，还需要创建 ESET PROTECT 要使用的空数据库。
- 请参阅安装和配置 MySQL for Windows 和 MySQL for Linux 的说明，以便正确地与 ESET PROTECT 配合使用。
- Linux 上的 Microsoft SQL Server 不受支持。但可以将 Linux 上的 ESET PROTECT 服务器连接到 Windows 上的 Microsoft SQL Server
- 如果在单独计算机上安装 ESET PROTECT 服务器和 Microsoft SQL Server 则可以启用与数据库的加密

连接

- Windows 环境下数据库的群集设置仅支持用于 Microsoft SQL Server不支持用于 MySQL

受支持的 Apache Tomcat 和 Java 版本

Apache Tomcat

Apache Tomcat 是运行 ESET PROTECT Web Console 所需的必需组件。

ESET PROTECT 仅支持 Apache Tomcat 9.x64 位）。建议您使用最新版本的 Apache Tomcat 9.x

ESET PROTECT 不支持 alpha/beta/RC 版本的 Apache Tomcat

Java

Apache Tomcat 需要 64 位 Java/OpenJDK

如果在系统上安装了多个 Java 版本，建议您卸载较早的 Java 版本并仅保留最新的受支持的 Java 版本。

从 2019 年 1 月开始，面向企业、商业或生产用途的 Oracle JAVA SE 8 公开更新将需要商业许可证。如果不购买 JAVA SE 订阅，可以使用本指南来转换为免费替代方案。请参阅 JDK 的受支持版本

受支持的 Web 浏览器ESET 安全产品和语言

以下操作系统受 ESET PROTECT 支持：

- WindowsLinux 和 macOS

ESET PROTECT Web 控制台可以在以下 Web 浏览器中运行：

Web 浏览器
Mozilla Firefox
Microsoft Edge
Google Chrome
Safari
Opera

若要获得使用 ESET PROTECT Web 控制台的最佳体验，建议您将 Web 浏览器保持为最新版本。

可通过 ESET PROTECT10.0 管理的最新版本的 ESET 产品

产品	产品版本
适用于 Windows 的 ESET Endpoint Security	7.3, 8.x, 9.x, 10.x
适用于 Windows 的 ESET Endpoint Antivirus	7.3, 8.x, 9.x, 10.x

产品	产品版本
适用于 macOS 的 ESET Endpoint Security	6.10+
适用于 macOS 的 ESET Endpoint Antivirus	6.10+
适用于 Android 的 ESET Endpoint Security	2.x, 3.x
适用于 Microsoft Windows Server 的 ESET Server Security（以前称为适用于 Microsoft Windows Server 的 ESET File Security	7.3, 8.x, 9.x, 10.x
适用于 Microsoft Exchange Server 的 ESET Mail Security	7.3, 8.x, 9.x, 10.x
ESET Security for Microsoft SharePoint Server	7.3, 8.x, 9.x
适用于 IBM Domino 的 ESET Mail Security	7.3, 8.x, 9.x
适用于 Linux 的 ESET Server Security（以前称为适用于 Linux 的 ESET File Security	7.2, 8.x, 9.x
ESET Endpoint Antivirus 对于 Linux	7.1, 8.x, 9.x
ESET LiveGuard Advanced	
ESET Inspect Connector	1.6+
适用于 Windows 的 ESET Full Disk Encryption	
适用于 macOS 的 ESET Full Disk Encryption	

可通过 ESET PROTECT10.0 管理的最新版本的 ESET 产品

产品	产品版本
适用于 Windows 的 ESET Endpoint Security	6.5
适用于 Windows 的 ESET Endpoint Antivirus	6.5
适用于 Microsoft Windows Server 的 ESET File Security	6.5
适用于 Microsoft Exchange Server 的 ESET Mail Security	6.5
适用于 IBM Domino 的 ESET Mail Security	6.5
ESET Security for Microsoft SharePoint Server	6.5

早于上表中所示的 ESET 安全产品版本不可使用 ESET PROTECT 10 进行管理。有关兼容性的详细信息，请访问 ESET 商业版产品的生命周期结束策略

支持通过订阅许可证激活的产品

ESET 产品	可用的起始版本
ESET Endpoint Antivirus/Security for Windows	7.0
ESET Endpoint Antivirus/Security for macOS	6.8.x
ESET Endpoint Security for Android	2.0.158
ESET Mobile Device Management for Apple iOS	7.0
适用于 Microsoft Windows Server 的 ESET File Security	7.0
ESET Mail Security for Microsoft Exchange	7.0
适用于 Windows Server 的 ESET File Security	7.0
适用于 IBM Domino 的 ESET Mail Security	7.0
ESET Security for Microsoft SharePoint Server	7.0
ESET File Security 对于 Linux	7.0

ESET 产品	可用的起始版本
ESET Endpoint Antivirus 对于 Linux	7.0
ESET Server Security 对于 Windows	8.0
ESET Server Security 对于 Linux	8.1
ESET LiveGuard Advanced	
ESET Inspect 随附适用于 Windows 7.3 及更高版本的 ESET Endpoint	1.5

支持语言

语言	代码
英语（美国）	en-US
阿拉伯语（埃及）	ar-EG
简体中文	zh-CN
繁体中文	zh-TW
克罗地亚语（克罗地亚）	hr-HR
捷克语（捷克共和国）	cs-CZ
法语（法国）	fr-FR
法语（加拿大）	fr-CA
德语（德国）	de-DE
希腊语（希腊）	el-GR
匈牙利语（匈牙利）*	hu-HU
印度尼西亚语（印度尼西亚）*	id-ID
意大利语（意大利）	it-IT
日语（日本）	ja-JP
朝鲜语（韩国）	ko-KR
波兰语（波兰）	pl-PL
葡萄牙语（巴西）	pt-BR
俄语（俄罗斯）	ru-RU
西班牙语（智利）	es-CL
西班牙语（西班牙）	es-ES
斯洛伐克语（斯洛伐克）	sk-SK
土耳其语（土耳其）	tr-TR
乌克兰语（乌克兰）	uk-UA

* 仅该产品以此语言提供，不提供该语言的联机帮助。

网络

ESET PROTECT 服务器和 ESET PROTECT 管理的客户端计算机必须具有可以使用的 Internet 连接，才能够访问 ESET 存储库和激活服务器。如果您不希望将客户端直接与 Internet 进行连接，可以使用代理服务器（与 ESET Bridge HTTP 代理不同）来实现与您的网络和 Internet 进行通信。

ESET PROTECT 管理的计算机应连接到同一 LAN 并且应位于与您的 ESET PROTECT 服务器相同的 *Active Directory* 域中。ESET PROTECT 服务器对于客户端计算机必须是可见的。此外，客户端计算机必须能够与您的 ESET PROTECT 服务器进行通信，才可以使用远程部署和唤醒呼叫功能。

适用于 Windows/Linux 的 ESET PROTECT 与 IPv4 和 IPv6 Internet 协议都兼容。ESET PROTECT 虚拟设备仅与 IPv4 兼容。

使用的端口

如果您的网络使用防火墙，请参阅在基础结构中安装 ESET PROTECT 及其组件时所使用的可能网络通信端口列表。

ESET PROTECT 服务器和 ESET Management 服务器代理通信造成的网络流量影响

客户端计算机上的应用程序不会直接与 ESET PROTECT 服务器通信。ESET Management 服务器代理会帮助实现此通信。此解决方案更易于管理，并且对通过网络传输的数据的要求较低。网络流量取决于客户端连接间隔和客户端执行的任务的类型。即使在客户端上没有要执行的或计划执行的任务，ESET Management 服务器代理也会按每个连接间隔与 ESET PROTECT 服务器通信一次。每次连接都会产生流量。有关流量的示例，请参阅下表：

操作类型	单个连接间隔内的流量
客户端任务：扫描但不清除	4 kB
客户端任务：模块更新	4 kB
客户端任务。SysInspector 日志请求	300 kB
策略病毒防护 – 最大安全性	26 kB

ESET Management 服务器代理复制间隔	空闲 ESET Management 服务器代理产生的每日流量
1 分钟	16 MB
15 分钟	1 MB
30 分钟	0.5 MB
1 小时	144 kB
1 天	12 kB

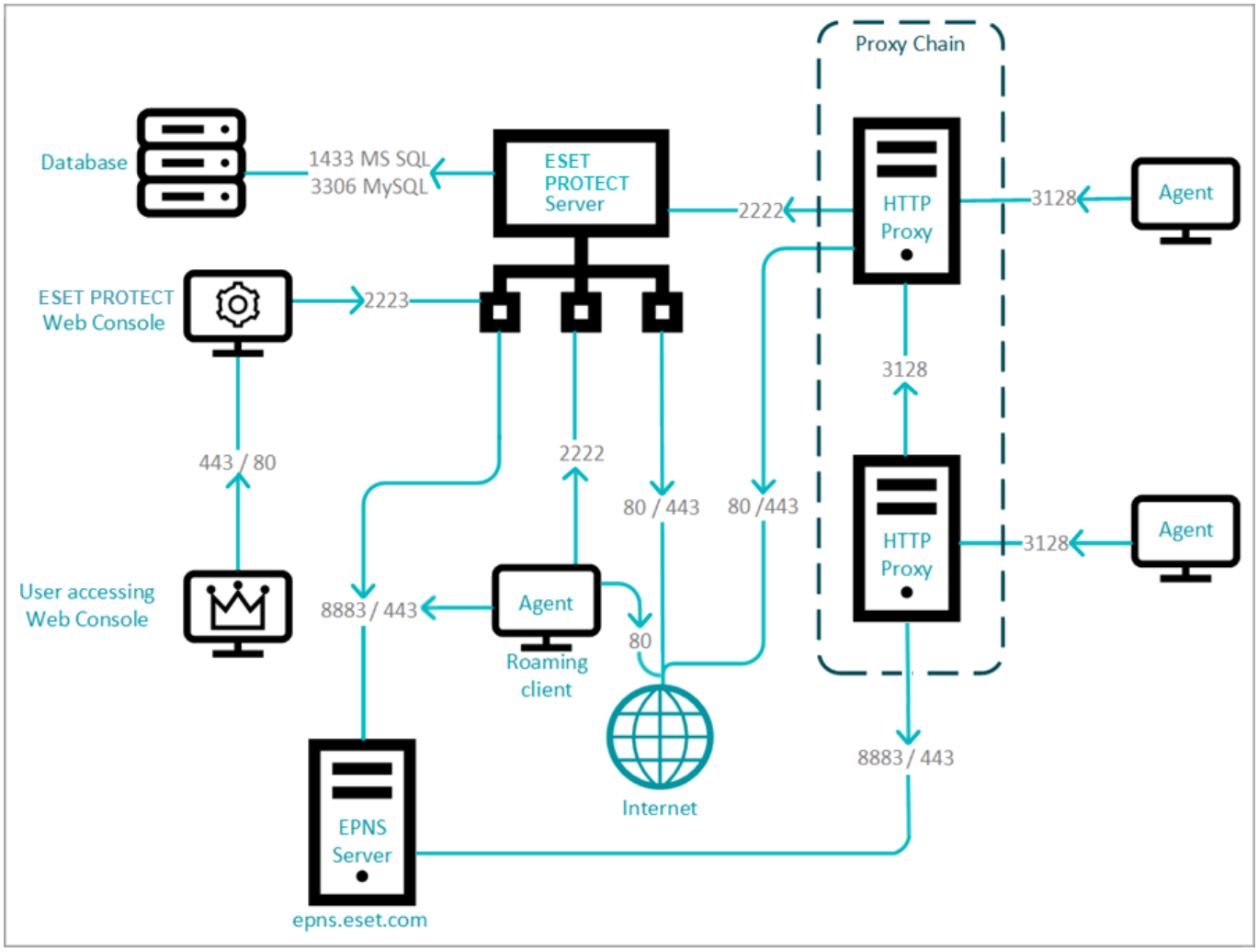
要估算 ESET Management 服务器代理产生的总流量，请使用以下公式：

客户端数量 *（空闲服务器代理产生的每日流量 +（某个任务所需的流量 * 该任务的每日发生次数））

如果使用 ESET Inspect，则 ESET Inspect Connector 每日产生的流量为 2-5 MB。它会因事件的数量而有所不同）。

使用的端口

ESET PROTECT 服务器可以与数据库、ESET PROTECT Web 控制台和 HTTP 代理一起安装在同一台计算机上。下图显示了各个安装及使用的端口（箭头指示网络通信）：



下表列出了在基础架构中安装 ESET PROTECT 及其组件时所使用的所有可能的网络通信端口。其他通信通过本地操作系统进程发生（例如通过 TCP/IP 的 NetBIOS）。

为保证应用程序正常工作 ESET PROTECT 其他应用程序不应使用以下任意端口。请确保将网络中的所有防火墙都配置为允许通过下面列出的端口进行通信。

客户端（ESET Management 服务器代理）或 ESET Bridge HTTP 代理计算机

协议	端口	说明
TCP	2222	ESET Management 服务器代理与 ESET PROTECT 服务器之间的通信
TCP	80	连接到 ESET 存储库
MQTT	8883, 443	ESET 推送通知服务 - ESET PROTECT 服务器与 ESET Management 服务器代理之间的唤醒呼叫，443 是故障转移端口。
TCP	3128	与 ESET Bridge 通信（HTTP 代理）
TCP	443	与 ESET LiveGuard Advanced 通信（仅限代理）

ESET Management 服务器代理 – 用于远程部署到装有 Windows 操作系统的目标计算机的端口

协议	端口	说明
TCP	139	使用共享 ADMIN$
TCP	445	在远程安装期间使用 TCP/IP 直接访问共享资源（TCP 139 的备选项）
UDP	137	远程安装期间的名称解析
UDP	138	在远程安装期间浏览

ESET PROTECT Web 控制台计算机（如果不是同一台 ESET PROTECT 服务器计算机）

协议	端口	说明
TCP	2223	ESET PROTECT Web 控制台与 ESET PROTECT 服务器之间的通信，用于辅助安装
TCP	443/80	Tomcat 广播 Web 控制台。
TCP	443	支持新闻的 RSS 源： • https://era.welivesecurity.com:443 • https://support.eset.com:443/rss/news.xml

ESET PROTECT 服务器计算机

协议	端口	说明
TCP	2222	ESET Management 服务器代理与 ESET PROTECT 服务器之间的通信
TCP	80	连接到 ESET 存储库
MQTT	8883	ESET 推送通知服务 - ESET PROTECT 服务器与 ESET Management 服务器代理之间的唤醒呼叫
TCP	2223	DNS 解析和 MQTT 回退
TCP	3128	与 ESET Bridge 通信（HTTP 代理）
TCP	1433 (Microsoft SQL) 3306 (MySQL)	连接到外部数据库（仅当数据库位于其他计算机上时）
TCP	389	LDAP 同步。在 AD 控制器上也可以打开此端口。
UDP	88	Kerberos 票证（仅适用于 ESET PROTECT 虚拟设备）

Rogue Detection (RD) Sensor

协议	端口	说明
TCP	22, 139	通过 SMB (TCP 139) 和 SSH (TCP 22) 协议的操作系统检测。
UDP	137	通过 NetBIOS 的计算机主机名解析。

ESET PROTECT MDC 计算机

协议	端口	说明
TCP	9977 9978	**内部**通信（在移动设备连接器与 ESET Management 服务器代理之间）
TCP	9980	移动设备注册
TCP	9981	移动设备通信
TCP	2195	发送通知到 Apple 推送通知服务。 (*gateway.push.apple.com*) 最高 ESMC 版本 7.2.11.1
TCP	2196	Apple 反馈服务 (*feedback.push.apple.com*) 最高 ESMC 版本 7.2.11.1
HTTPS	2197	• Apple 推送通知和反馈 (*api.push.apple.com*) ESMC版本 7.2.11.3 及更高版本。
TCP	2222	在 ESET Management 服务器代理□MDC 和 ESET PROTECT 服务器之间通信（复制）
TCP	1433 (Microsoft SQL) 3306 (MySQL)	连接到外部数据库（仅当数据库位于其他计算机上时）

MDM 托管设备

协议	端口	说明
TCP	9980	移动设备注册
TCP	9981	移动设备通信
TCP	5223	与 Apple 推送通知服务外部通信 (iOS)
TCP	443	• 仅针对 Wi-Fi 回退，当设备无法通过端口 5223 访问 APN 时。(iOS) • Android 设备与 GCM 服务器连接。 • 连接到 ESET 许可门户。 • ESET LiveGrid® (Android)□入站：*https://i1.c.eset.com*；出站：*https://i3.c.eset.com*□ • 匿名统计信息发送到 ESET 研究实验室 (Android) (*https://ts.eset.com*) • 设备上安装的应用类别。用于应用程序控制（当已定义阻止某些应用类别时□□(Android) (*http://go.eset.eu*) • 使用“支持请求”功能发送支持请求 (Android) (*https://suppreq.eset.eu*)
TCP	5228 5229 5230	发送通知到 Google Cloud Messaging (Android)* 发送通知到 Firebase Cloud Messaging (Android)*
TCP	80	• 模块更新 (Android) (*http://update.eset.com*) • 仅在 Web 版本中使用。有关最新应用版本更新和下载新版本的信息□(Android) (*http://go.eset.eu*)

* GCM (Google Cloud Messaging) 服务已弃用，并已于 2019 年 4 月 11 日删除。它已替换为 FCM (Firebase Cloud Messaging)□MDM v7 已于该日期将 GCM 服务替换为 FCM 服务，此时只需允许 FCM 服务的通信。

如果需要，可以更改预定义的端口 2222、2223。

安装进程

安装指南包含许多安装 ESET PROTECT 的方法，主要面向企业客户。如果您想要在 Windows 平台上安装 ESET PROTECT 来管理最多 250 个 Windows ESET 端点产品，请参阅适用于中小企业的指南
有关升级现有 ESET PROTECT 安装的说明，请参阅升级过程

可在 ESET 网站的下载 ESET PROTECT 部分获取 ESET PROTECT 安装程序。可选择不同格式以支持不同的安装方法。默认情况下，已选定**一体式安装程序**选项卡。单击相应选项卡以下载 VA 或独立安装程序。提供的下载如下：

- 适用于 Windows 的 ESET PROTECT一体式安装程序包（采用 zip 格式）。
- 包含所有 ESET PROTECT 安装程序的 ISO 映像ESET PROTECT 虚拟设备除外）。
- 虚拟设备OVA 文件）。建议希望在虚拟环境中运行 ESET PROTECT 或偏爱更简单安装的用户部署 ESET PROTECT 虚拟设备。有关分步说明，请参阅完整的 ESET PROTECT 虚拟设备部署指南
- 适用于 Windows 和 Linux 平台的各个组件的单独安装程序。

其他安装方法：

- 分步安装说明（适用于 Linux

自 2022 年 11 月之后，我们不再在 Azure Marketplace 中提供 ESET PROTECT 设备。此外，还可以使用 ESET PROTECT 云，并让 ESET 管理所有必需的基础架构组件。

安装完成后，请勿更改 ESET PROTECT 服务器计算机的计算机名。有关详细信息，请参阅更改 ESET PROTECT 服务器的 IP 地址或主机名

如果要决定适合环境的 ESET PROTECT 安装种类，请参见以下决策表，该表将指导您做出最佳选择：例如：

- 云中的 ESET PROTECT Internet 连接不宜太慢。
- 如果您是 SMB 客户，请选择一体式安装程序。

另请参阅硬件和基础结构大小调整

安装方法	客户类型		迁移		ESET PROTECT 安装环境					Internet 连接		
	SMB	企业	是	否	无服务器	专用服务器	共享服务器	虚拟化平台	云服务器	无	好	差
一体式 Windows Server	✓	✓	✓			✓	✓		✓	✓	✓	✓
一体式 Windows Desktop	✓		✓		✓					✓	✓	✓
虚拟设备	✓		✓					✓		✓	✓	✓
Linux 组件		✓	✓			✓	✓		✓	✓	✓	✓
Windows 组件		✓	✓			✓	✓		✓	✓	✓	✓

Windows 上的一体式安装

可以使用一些不同的方式安装 ESET PROTECT选择最适合您的需求和环境的安装类型。最简单的方法是使用 ESET PROTECT 一体式安装程序。此方法使您可以在单台计算机上安装 ESET PROTECT 及其组件。

组件安装允许您自定义安装，并在单独的计算机上安装每个 ESET PROTECT 组件，只要它满足系统要求。

可以使用以下方式安装 ESET PROTECT

- 一体式程序包安装 ESET PROTECT 服务器ESET Bridge HTTP 代理或移动设备连接器
- ESET PROTECT 组件（组件安装）的独立安装程序

自定义安装方案如下所示：

- 使用自定义证书安装
- 故障转移群集上的安装

许多安装方案都要求您在不同的计算机上安装不同的ESET PROTECT组件，以适应网络架构、符合性能要求，或者出于其他原因这样操作。以下安装程序包可供个别 ESET PROTECT 组件使用：

核心组件安装：

- ESET PROTECT 服务器
- ESET PROTECT Web 控制台 - 可以在未安装 ESET PROTECT 服务器的其他计算机上安装 ESET PROTECT Web 控制台。
- ESET Management 服务器代理（必须安装在客户端计算机上，也可以安装在 ESET PROTECT 服务器上）

可选组件安装：

- RD Sensor
- 移动设备连接器
- ESET Bridge HTTP 代理
- 镜像工具

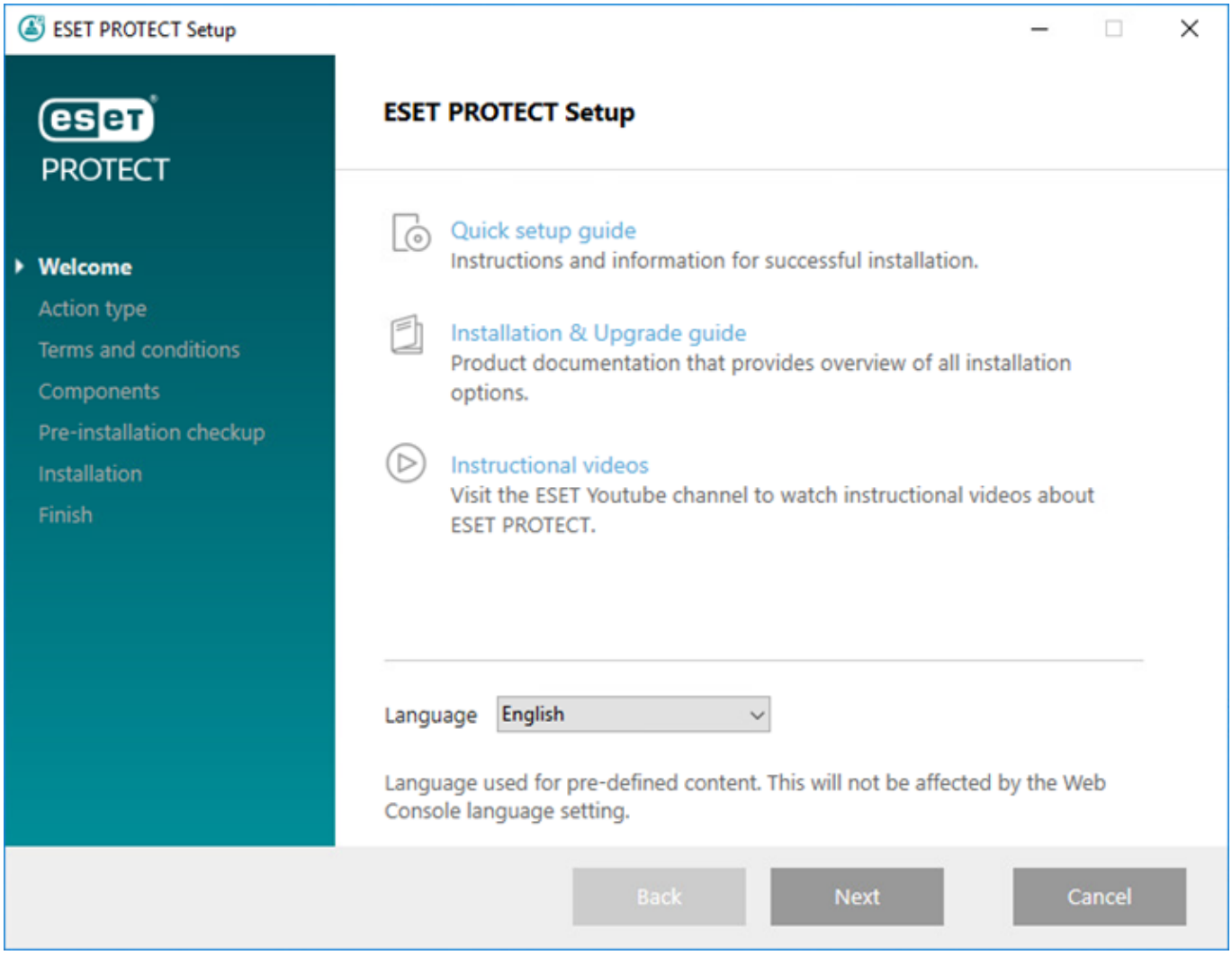
另请参阅 ESET PROTECT 一体式安装

有关将 ESMC 升级到最新 ESET PROTECT 10.0 的说明，请参阅我们的升级过程

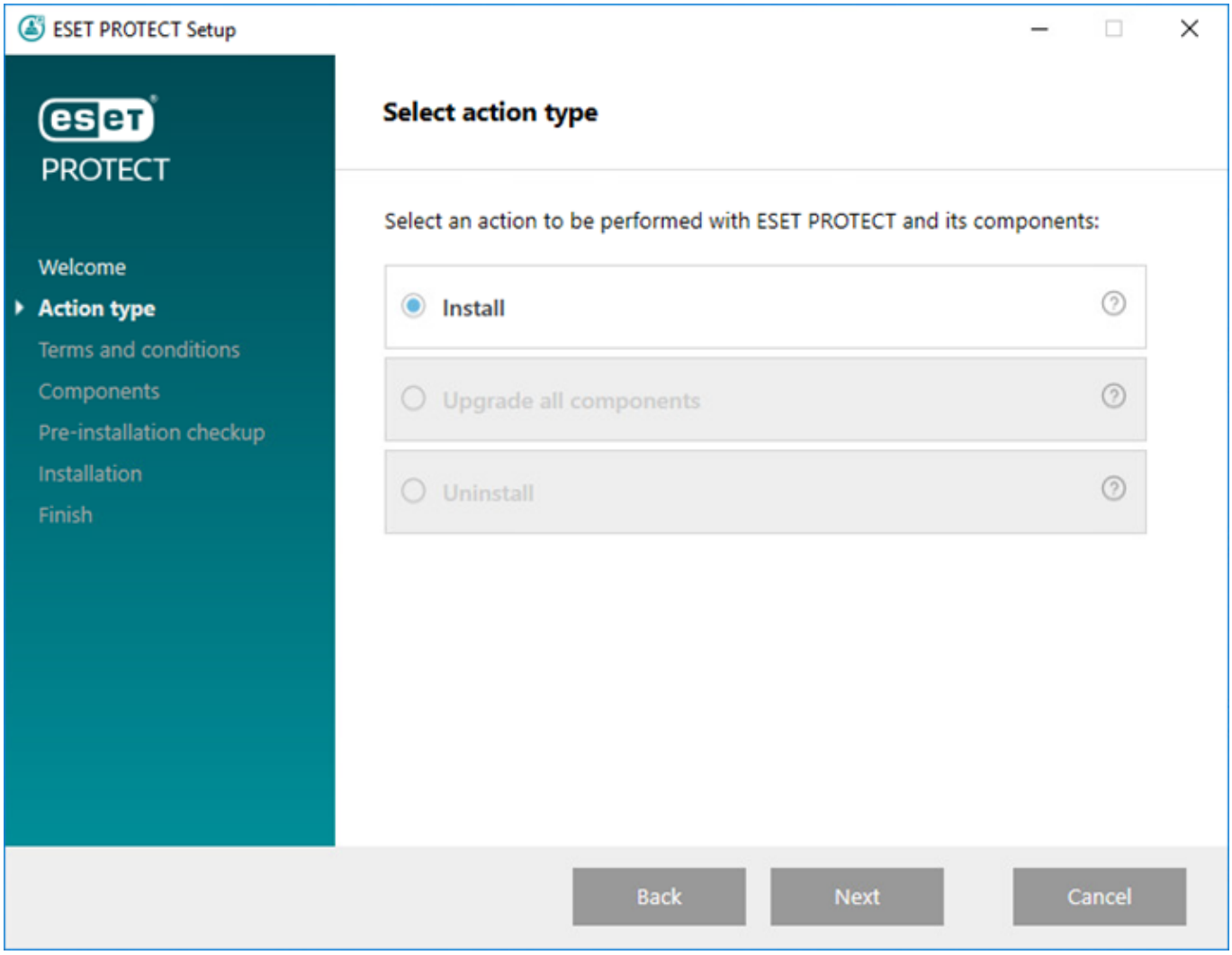
安装 ESET PROTECT 服务器

ESET PROTECT 一体式安装程序仅适用于 Windows 操作系统。一体式安装程序允许您使用 ESET PROTECT 安装向导安装所有 ESET PROTECT 组件。

1. 打开安装包。在欢迎屏幕上，使用**语言**下拉菜单调整语言设置。单击**下一步**以继续。



2. 选择**安装**，然后单击**下一步**。



3. 选中**参与产品改进计划**复选框，以将匿名遥测数据和崩溃报告发送给 ESET（操作系统版本和类型、ESET 产品版本和其他特定于产品的信息）。 接受 EULA 后，单击**下一步**。

4. 选择要安装的适用组件，然后单击**下一步**。

Microsoft SQL Server Express

- 默认情况下，ESET PROTECT 10.0 一体式安装程序将安装 Microsoft SQL Server Express 2019。
  - 如果使用的是旧版 Windows Server 2012 或 SBS 2011，将默认安装 Microsoft SQL Server Express 2014。
  - 安装程序会自动生成一个用于数据库验证的随机密码（存储在 *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini* 中）。

> Microsoft SQL Server Express 的每个关系数据库具有 10 GB 大小限制。不建议使用 Microsoft SQL Server Express：
> - 在企业环境或大型网络中。
> - 如果要将 ESET PROTECT 与 ESET Inspect 一起使用。

- 如果已安装其他受支持版本的 Microsoft SQL Server 或 MySQL，或计划连接到其他 SQL Server，请取消选中 **Microsoft SQL Server Express** 旁边的复选框。
- 在域控制器（例如 Windows SBS/Essentials）上不要安装 SQL Server。建议您在其他服务器上安装 ESET PROTECT，或者在安装期间不选择 SQL Server Express 组件（这要求您使用现有 SQL 或 MySQL Server 来运行 ESET PROTECT 数据库）。

添加用于 Web 控制台的自定义 HTTPS 证书

- 如果要将自定义 HTTPS 证书用于 ESET PROTECT Web 控制台，请选择此选项。
- 如果不选择此选项，则安装程序会自动生成一个新的 Tomcat 密钥库（即自签名的 HTTPS 证书）。

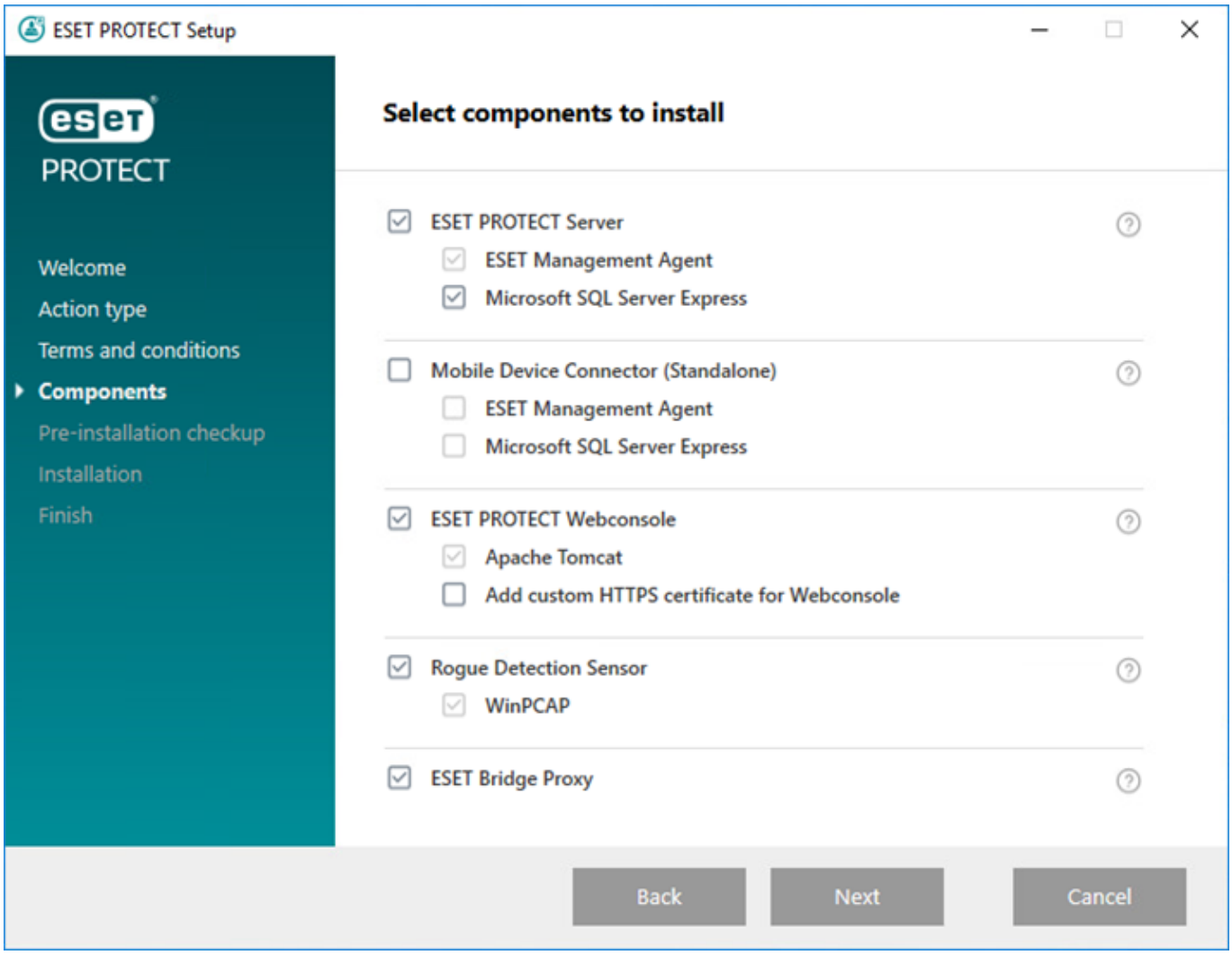
ESET Bridge 代理

ESET Bridge 代理选项仅适用于没有漫游客户端的小型或集中式网络。如果选择此选项，安装程序将客户端配置为通过安装在与 ESET PROTECT 服务器相同的机器上的代理与 ESET 进行隧道通信。如果客户端与 ESET PROTECT 服务器之间没有直接的网络可见性，则此连接将无法工作。

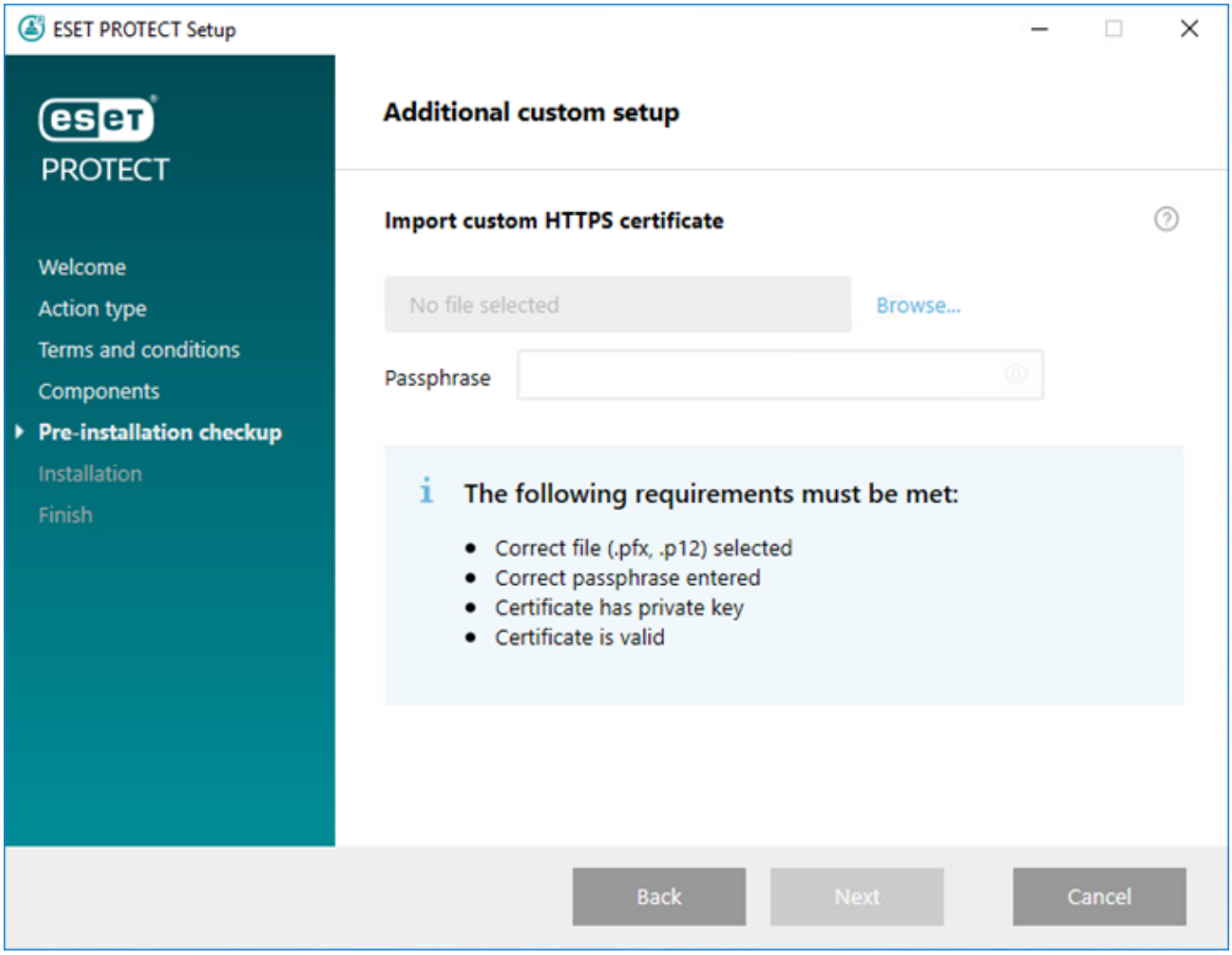
- 使用 HTTP 代理可以大大节省用于从 Internet 下载数据的带宽，并提高产品更新的下载速度。建议您选中 **ESET Bridge 代理**旁边的复选框（如果将从 ESET PROTECT 管理 37 台以上计算机）。还可以选择以后安装 ESET Bridge。
- 有关详细信息，请参阅 ESET Bridge（HTTP 代理）和 ESET Bridge（HTTP 代理）、镜像工具和直接连接之间的差异。

一体式安装程序会为应用于**所有**静态组的 ESET Management 服务器代理和 ESET 安全产品创建默认 **HTTP Proxy 使用**策略。这些策略会自动配置托管计算机上的 ESET Management 服务器代理和 ESET 安全产品，以将 ESET Bridge 用作缓存更新程序包的代理。

HTTP 代理主机是 ESET PROTECT 服务器的本地 IP 地址和端口 3128。身份验证已禁用。可以将这些设置复制到其他策略（如果需要设置其他产品）。



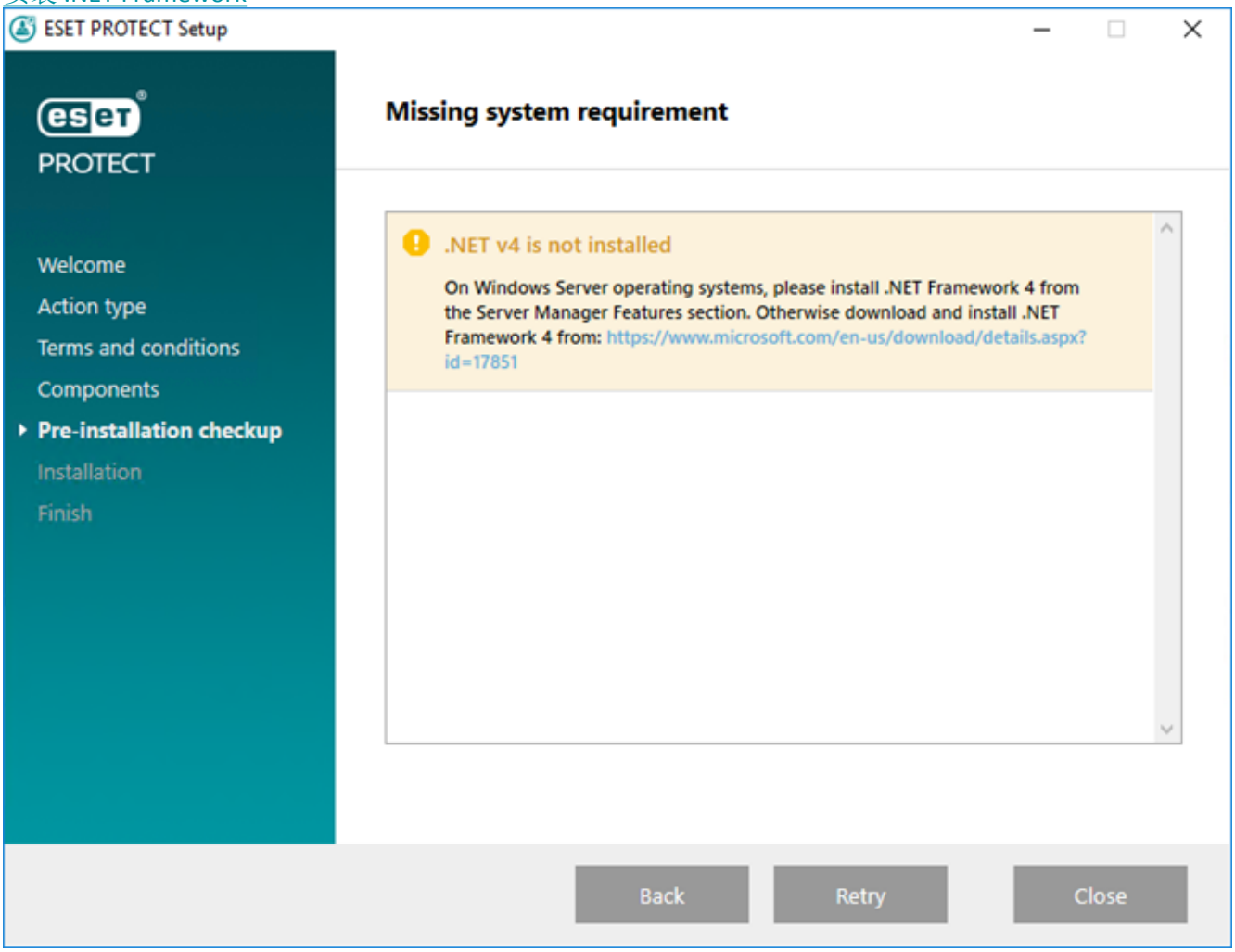
5. 如果已选择**添加用于 Web 控制台的自定义 HTTPS 证书**，则单击**浏览**并选择有效证书（*.pfx* 或 .p12 文件），然后键入其**密码**（如果没有密码，将该字段留空）。安装程序将在您的 Tomcat 服务器上安装用于 Web 控制台访问的证书。单击**下一步**以继续。



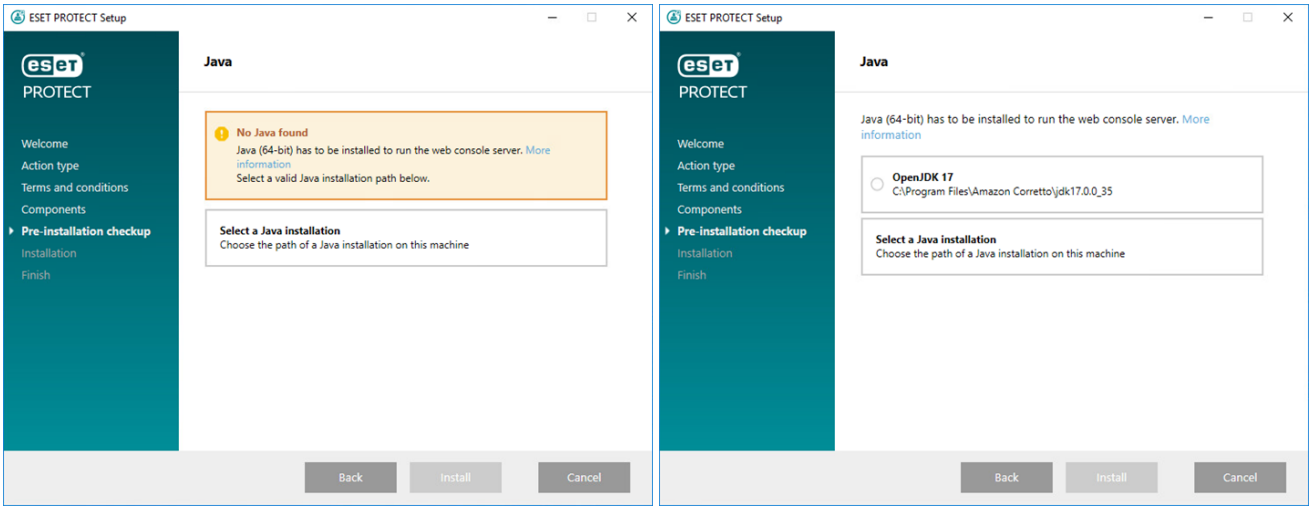
6. 如果在先决条件检查期间发现错误，请相应地解决它们。确保您的系统满足所有先决条件。

.NET v4 未安装

安装 .NET Framework



未找到 Java/检测到 Java（64 位）



如果在系统上安装了多个 Java 版本，建议您卸载较早的 Java 版本并仅保留最新的受支持的 Java 版本。

从 2019 年 1 月开始，面向企业、商业或生产用途的 Oracle JAVA SE 8 公开更新将需要商业许可证。如果不购买 JAVA SE 订阅，可以使用本指南来转换为免费替代方案。请参阅 JDK 的受支持版本

a)要选择已安装的 Java，请单击**选择 Java 安装**，选择安装有 Java 的文件夹（包含子文件夹 *bin*，例如 *C:\Program Files\Amazon Corretto\jdk1.8.0_212*），然后单击**确定**。如果选择的路径无效，安装程序会提示您。

b)单击**安装**以继续，或单击**更改**以更改 Java 安装路径。

系统磁盘上仅 32 MB 可用

- 如果系统没有足够磁盘空间供 ESET PROTECT 安装，安装程序可能会显示此通知。
- 必须至少具有 4,400 MB 可用磁盘空间，才能安装 ESET PROTECT 及其所有组件。

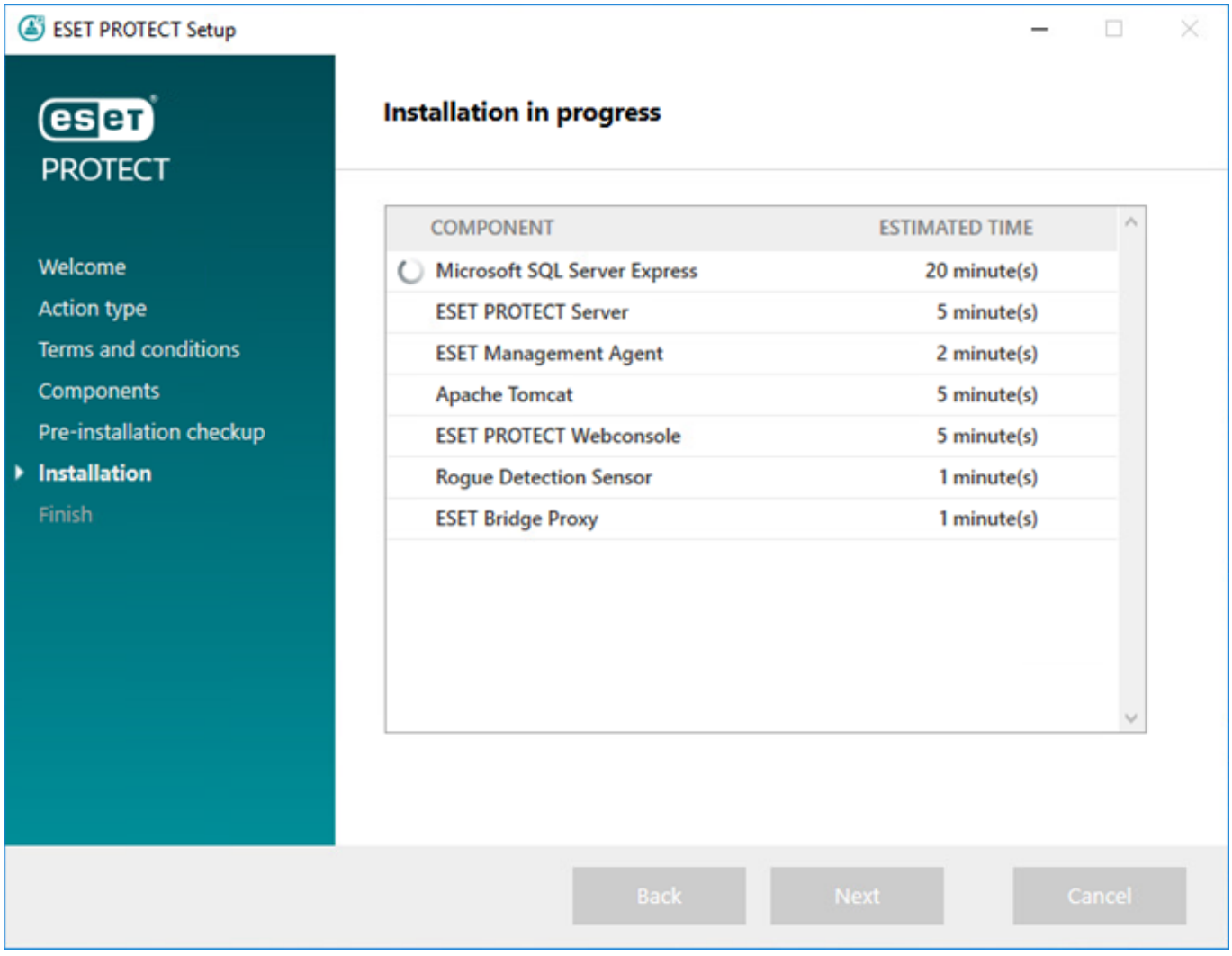
ESET Remote Administrator 5.x 或较早版本安装在阻止安装程序继续的计算机上。

如果您有 ERA 5.x/6.x 或 ESMC 7.0/7.1
- 不支持直接升级到 ESET PROTECT 10.0
- 执行全新安装 ESET PROTECT 10.0

可以从 ESMC 7.2 及更高版本直接升级到 ESET PROTECT 10.0

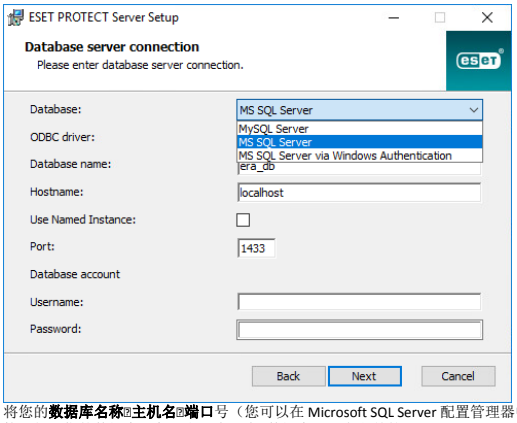
7. 当先决条件检查完成并且环境满足所有要求时，将开始安装。请注意，安装可能需要一个小时以上，具体取决于您的系统和网络配置。

安装正在进行时ESET PROTECT 安装向导不响应。



8. 如果您在步骤 4 中选择安装 **Microsoft SQL Server Express**，安装程序将执行数据库连接检查。如果您具有现有数据库服务器，安装程序将提示您输入数据库连接详细信息：

配置到 SQL/MySQL Server 的连接

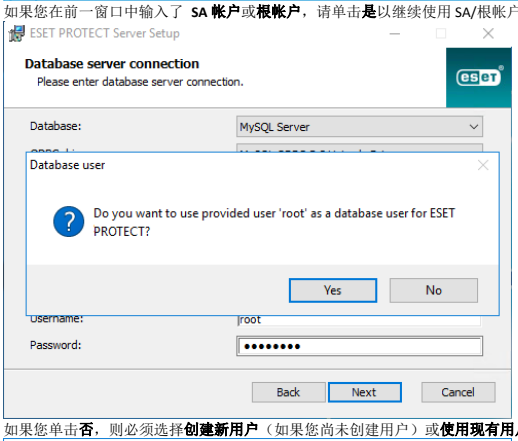


将您的**数据库名称**、**主机名**、**端口**号（您可以在 Microsoft SQL Server 配置管理器中找到此信息）以及**数据库帐户**详细信息（**用户名**和**密码**）输入到相应字段中，然后单击**下一步**。安装程序将验证数据库连接。如果您的数据库服务器上具有现有 数据库（源自之前的 ESMC/ESET PROTECT 安装），将检测到此情况。您可以选择**使用现有的数据库并应用升级**或**删除现有的数据库并安装新版本**。

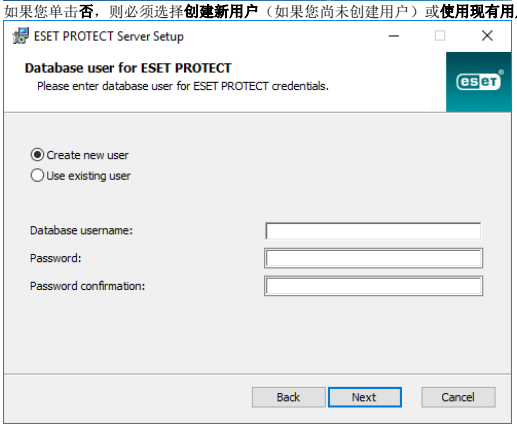
使用命名实例 – 如果您使用的是 Microsoft SQL 数据库，您还可以选中**使用命名实例**复选框以使用自定义数据库实例。您可以在**主机名**字段中使用 *HOSTNAME\DB_INSTANCE* 格式（例如，*192.168.0.10\ESMC7SQL*）设置它。对于群集数据库，仅使用群集名称。如果选中此选项，则无法更改数据库连接端口 – 系统将使用由 Microsoft 确定的默认端口。若要将 ESET PROTECT 服务器连接到故障转移群集中安装的 Microsoft SQL 数据库，请在**主机名**字段中输入群集名称。

输入**数据库帐户**信息时，有两个选项可供选择。您可以使用**专用数据库用户帐户**（将只具有 ESET PROTECT 数据库的访问权限），也可以使用 **SA 帐户** ((Microsoft SQL) 或**根帐户** (MySQL)。如果您决定使用专用用户帐户，需要创建具有特定权限的帐户。有关详细信息，请参阅专用数据库用户帐户。如果您不打算使用专用用户帐户，请输入管理员帐户（SA 或根）。

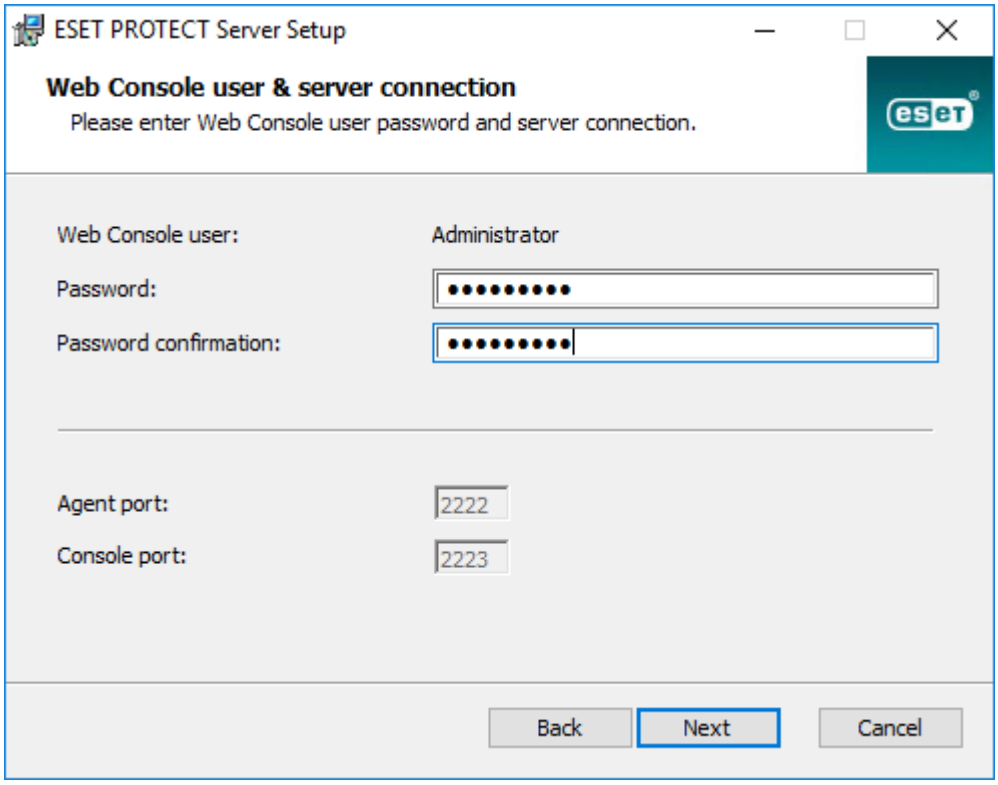
如果您在前一窗口中输入了 **SA 帐户**或**根帐户**，请单击**是**以继续使用 SA/根帐户作为 ESET PROTECT 的数据库用户。



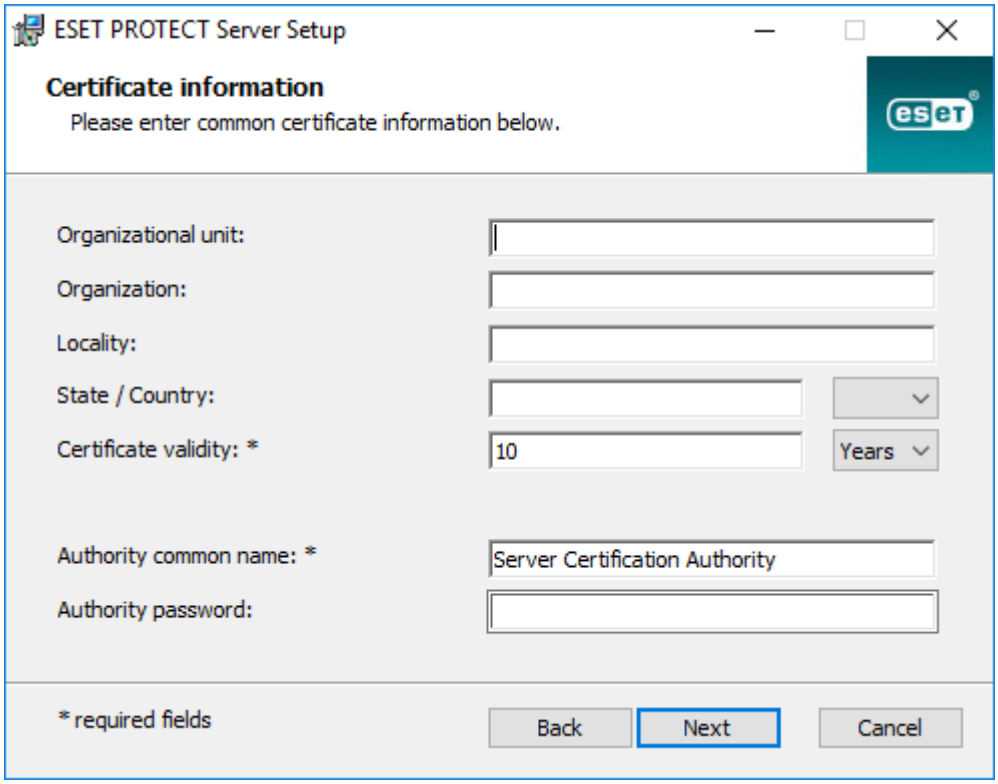
如果您单击**否**，则必须选择**创建新用户**（如果您尚未创建用户）或**使用现有用户**（如果您拥有专用数据库用户帐户）。



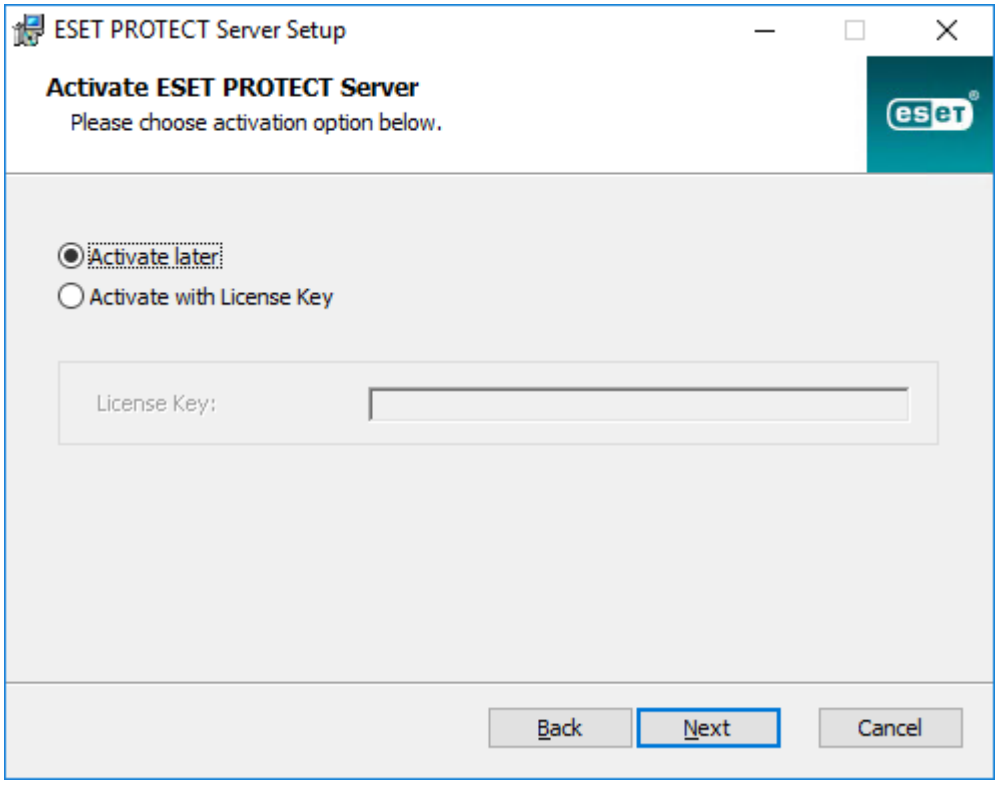
9. 安装程序将提示您输入 Web 控制台管理员帐户的密码。此密码很重要，因为您将使用它登录到 ESET PROTECT Web 控制台。单击**下一步**。



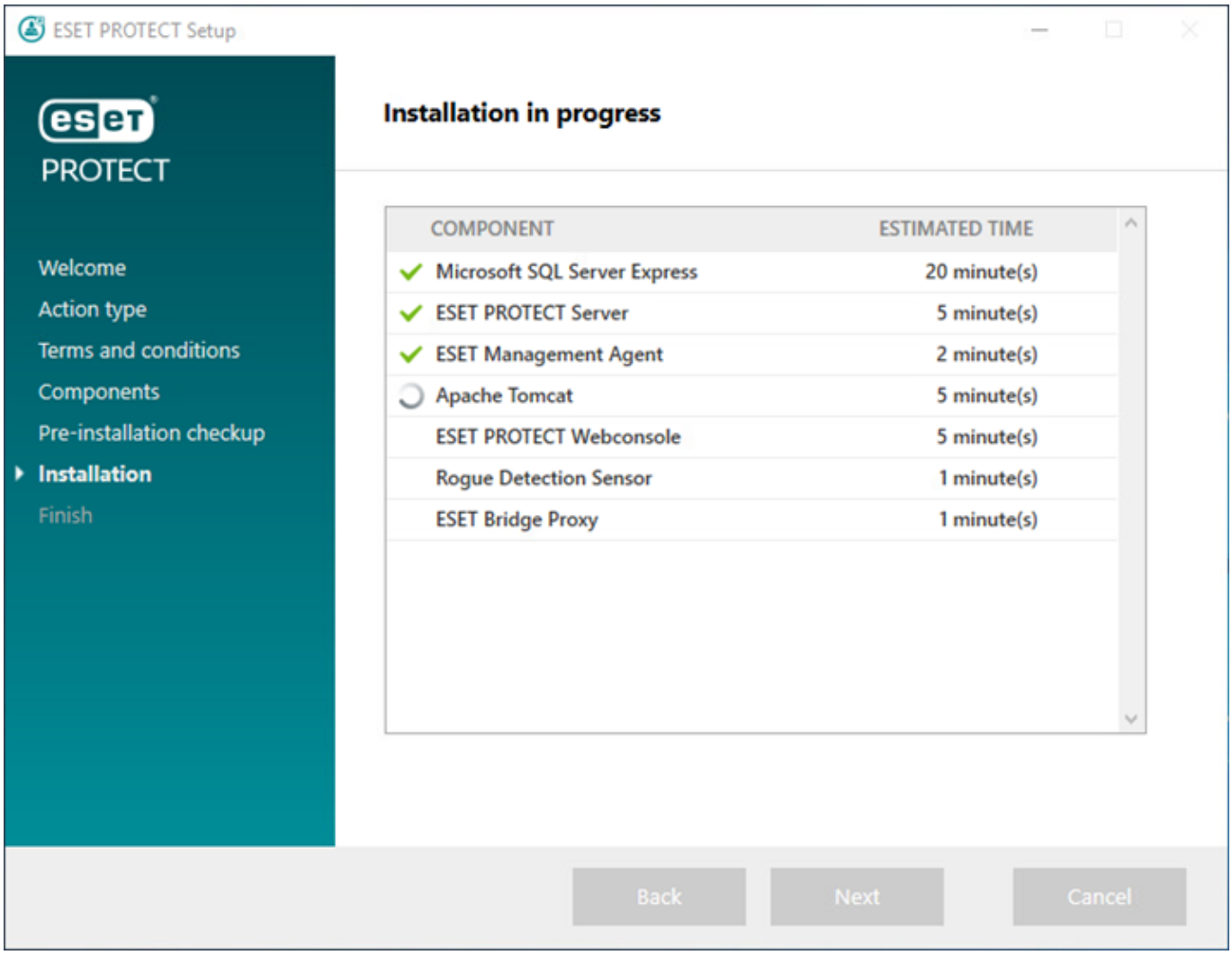
10. 原样保留这些字段，或者键入您公司的信息以在 ESET Management 服务器代理和 ESET PROTECT 服务器证书的详细信息中显示。如果选择在**授权密码**字段中输入密码，请务必记住该密码。单击**下一步**。



11. 输入有效的**许可证密钥**（随附在您从 ESET 收到的全新购买电子邮件中），然后单击**下一步**。如果您使用的是旧许可证凭据（用户名和密码），请将这些凭据转换为许可证密钥。此外，您也可以选择**稍后激活**（有关其他说明，请参阅激活章节）。



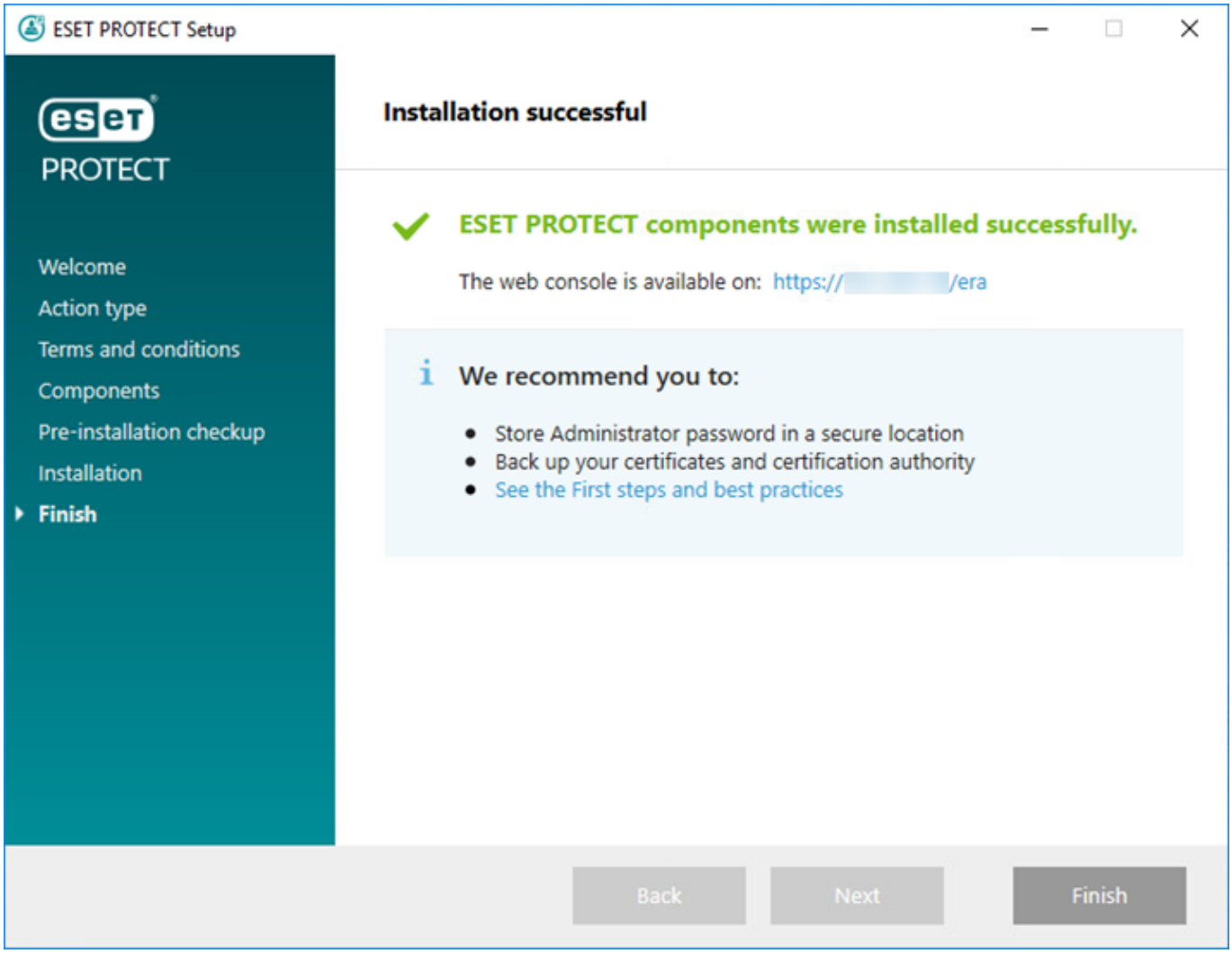
12. 可以看到安装进度。



13. 如果选择安装 **Rogue Detection Sensor**，将会看到 WinPcap 驱动程序的安装窗口。确保选中**在启动**

时自动启动 WinPcap 驱动程序复选框。

14. 安装完成时，将显示“ESET PROTECT 组件已成功安装”以及 ESET PROTECT Web 控制台 URL 地址。单击该 URL 打开 Web 控制台，或者单击**完成**。



如果安装不成功：

- 查看一体式安装包中的安装日志文件。该日志目录与一体式安装程序的目录相同，例如：`C:\Users\Administrator\Downloads\x64\logs\`
- 请参阅疑难解答以获取用于解决您的问题的其他步骤。

安装 ESET PROTECT 移动设备连接器（单机版）

ESET PROTECT 移动设备管理/连接器 (MDM/MDC) 组件（仅限本地）计划结束生命周期。阅读更多建议您迁移到 Cloud MDM。

若要在运行 ESET PROTECT 服务器以外的其他计算机上将移动设备连接器作为独立工具安装，请完成以下步骤。

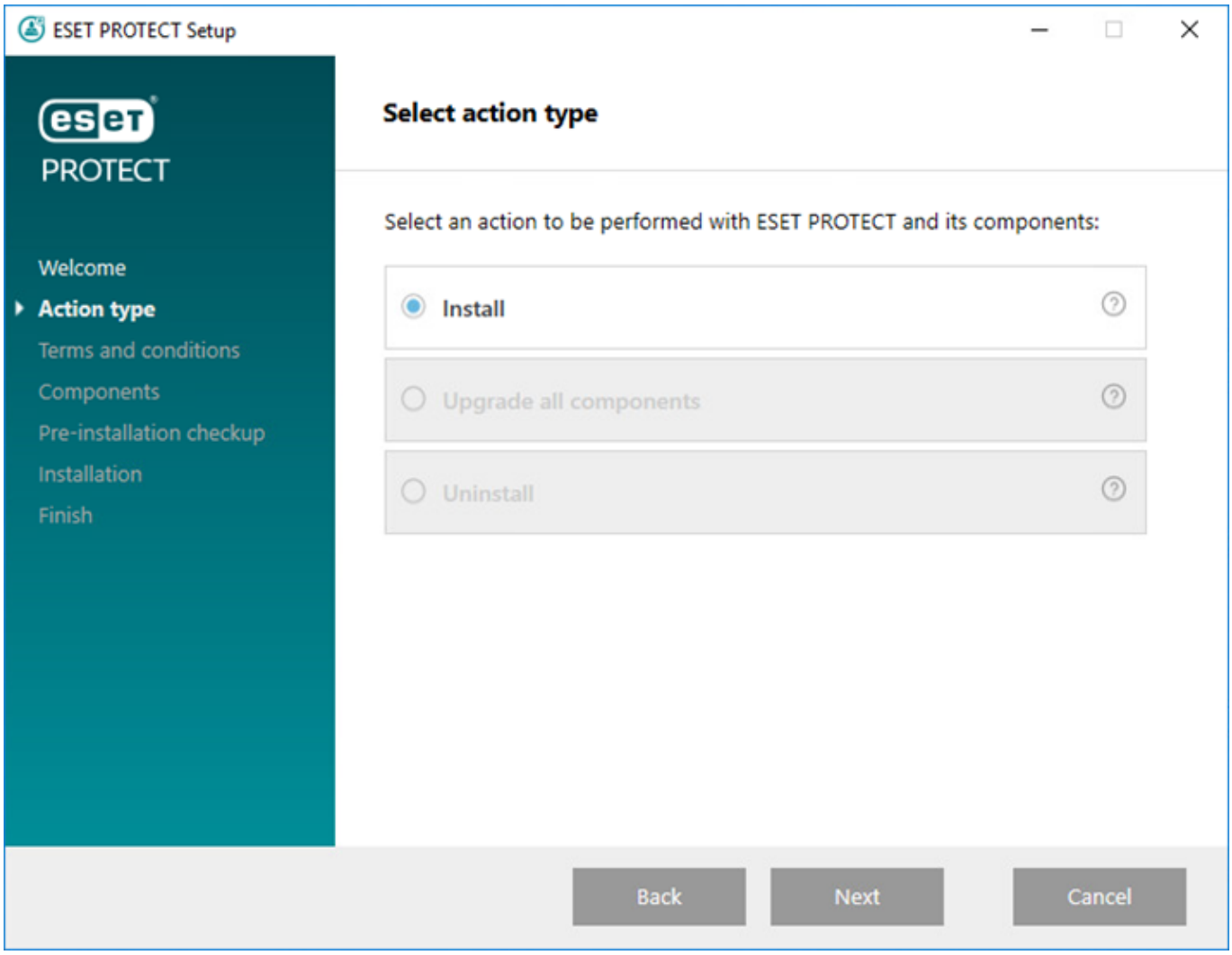
移动设备连接器必须可通过 Internet 进行访问，以便可以随时随地管理该移动设备。

请考虑移动设备会与移动设备连接器通信，这将不可避免地影响移动数据的使用。漫游时尤其如此。

执行以下步骤以在 Windows 上安装移动设备连接器：

1. 请首先阅读先决条件并确保满足所有这些条件。

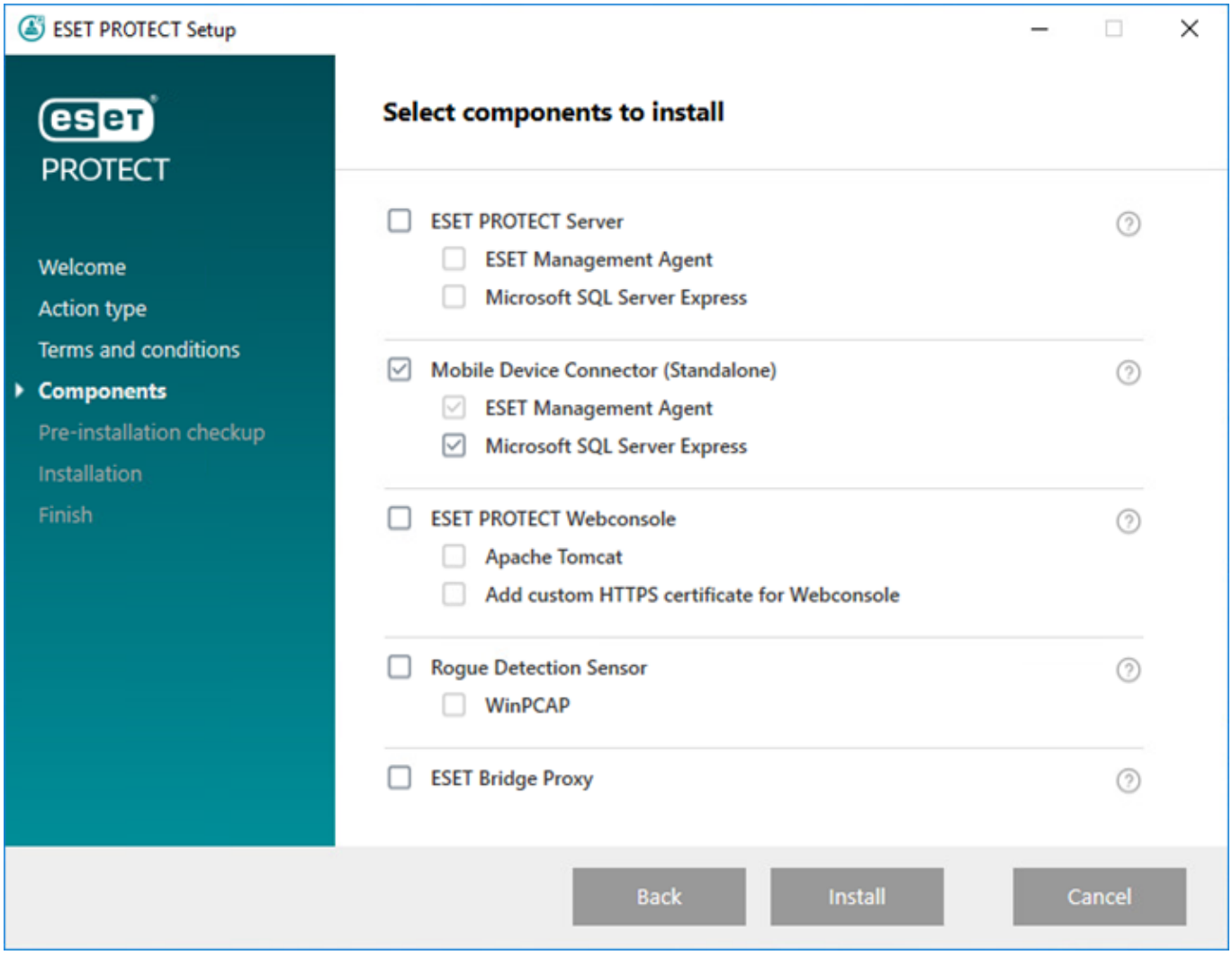
2. 双击安装包以打开它，选择**安装**，然后单击**下一步**。



3. 选中**参与产品改进计划**复选框，以将匿名遥测数据和崩溃报告发送给 ESET（操作系统版本和类型、ESET 产品版本和其他特定于产品的信息）。

4. 接受 EULA 后，单击**下一步**。

5. 仅选中 **Mobile Device Connector (单机版)** 旁边的复选框（ESET PROTECT 移动设备连接器需要**数据库**才能运行。选择 **Microsoft SQL Server Express**（如果要安装数据库），或将复选框保留为空。如果要连接到现有数据库，可在安装期间选择执行此操作。单击**安装**以继续进行安装。



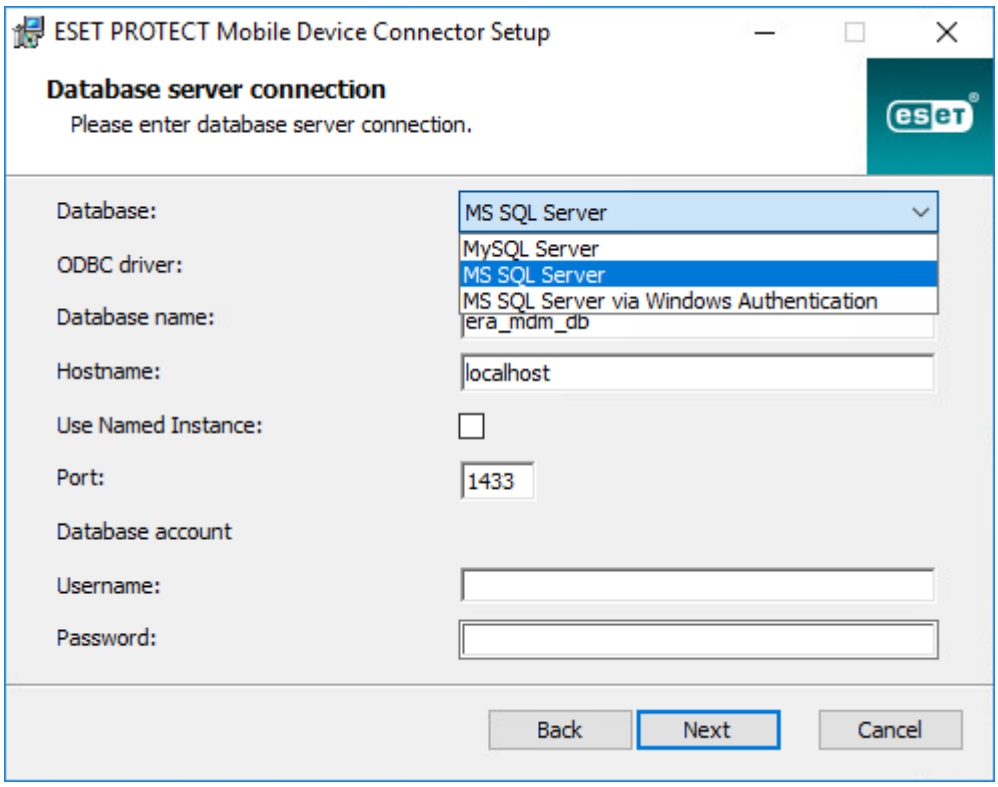
6. 如果已在步骤 5 中作为此安装的一部分安装了数据库，则现在将自动安装该数据库，可以跳到步骤 8。如果在步骤 5 中未选择安装数据库，则系统会提示您将 MDM 组件连接到现有数据库。

> 您可以使用用于 ESET PROTECT 数据库的相同数据库服务器，但如果您计划注册 80 多个移动设备，建议您使用不同的数据库服务器。

7. 安装程序必须连接到供移动设备连接器使用的现有数据库。指定以下连接详细信息：

- **数据库**：MySQL Server/MS SQL Server/通过 Windows 身份验证的 MS SQL Server
- **ODBC 驱动程序**：MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 Unicode Driver/MySQL ODBC 5.3 Unicode Driver/MySQL ODBC 8.0 Unicode Driver/SQL Server/SQL Server Native Client 10.0/ODBC Driver 11 for SQL Server/ODBC Driver 13 for SQL Server/ODBC Driver 17 for SQL Server/ODBC Driver 18 for SQL Server
- **数据库名称**：建议您使用预定义的名称或更改它（如果需要）。
- **主机名**：数据库服务器的主机名或 IP 地址
- **端口**： 用于连接到数据库服务器
- 数据库管理员帐户**用户名/密码**
- **使用命名实例** – 如果您使用的是 Microsoft SQL 数据库，您还可以选中**使用命名实例**复选框以使用自定义数据库实例。您可以在**主机名**字段中使用 *HOSTNAME\DB_INSTANCE* 格式（例

如，*192.168.0.10\ESMC7SQL*）设置它。对于群集数据库，仅使用群集名称。如果选中此选项，则无法更改数据库连接端口 – 系统将使用由 Microsoft 确定的默认端口。若要将 ESET PROTECT 服务器连接到故障转移群集中安装的 Microsoft SQL 数据库，请在**主机名**字段中输入群集名称。

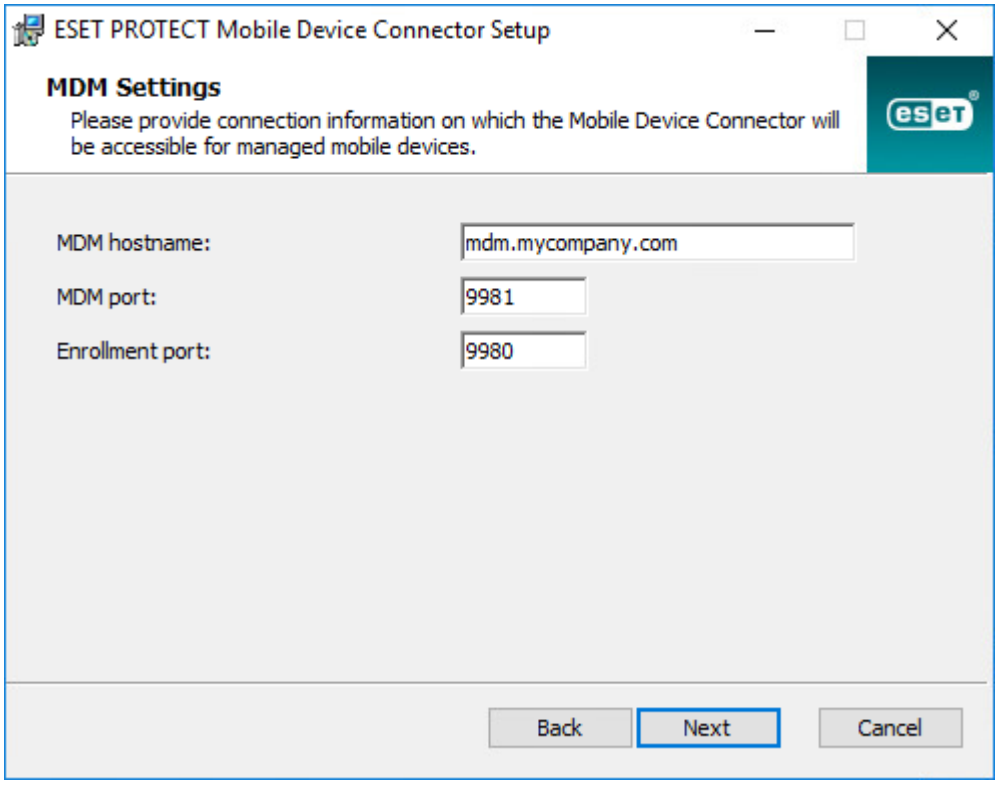


8. 如果连接成功，系统将提示您确认是否要将提供的用户用作 ESET PROTECT MDM 的数据库用户。

9. 在新数据库安装成功或安装程序成功连接到现有数据库后，可以继续进行 MDM 安装。指定 **MDM 主机名**：由于移动设备可以通过 Internet 访问该主机名，因此这是您的 MDM 服务器的公共域或公共 IP 地址。

必须以 **HTTPS 服务器证书**中所示的相同形式输入 MDM 主机名，否则 iOS 移动设备会拒绝安装 MDM 配置文件。例如，如果 HTTPS 证书中存在一个指定的 IP 地址，请将此 IP 地址键入 **MDM 主机名**字段。在已在 HTTPS 证书中指定了 FQDN（例如，`mdm.mycompany.com`）的情况下，请在 **MDM 主机名**字段中输入此 FQDN。此外，如果在 HTTPS 证书中使用了通配符 `*`（例如，`*.mycompany.com`），则可以在 **MDM 主机名**字段中使用 `mdm.mycompany.com`。

在此安装步骤中，填写 **MDM 主机名**字段时请务必小心。如果信息不正确或格式错误，则 MDM 连接器将无法正常工作，修复它的唯一方法是重新安装该组件。



10. 在下一步中，通过单击**下一步**验证与数据库的连接。

11. 将 MDM 连接器连接到 ESET PROTECT 服务器。填写连接到 ESET PROTECT 服务器所需的**服务器主机**和**服务器端口**，然后选择**服务器辅助安装**或**脱机安装**以继续：

• **服务器辅助安装** – 提供 ESET PROTECT Web 控制台管理员凭据，安装程序将自动下载所需证书。还要检查服务器辅助安装所需的权限。

1.输入**服务器主机** – 您的 ESET PROTECT 服务器的名称或 IP 地址和 **Web 控制台端口**（如果不使用自定义端口，则保留使用默认端口 2223）。此外，提供 Web 控制台管理员帐户凭据 – **用户名/密码**。

2.当询问您是否接受证书时，单击**是**。继续进行步骤 11。

• **脱机安装** – 提供代理证书和证书颁发机构（可从 ESET PROTECT 中导出）。此外，可以使用自定义证书和适合的证书颁发机构。

1.单击对等证书旁边的**浏览**，然后导航到**对等证书**（这是从 ESET PROTECT 中导出的代理证书）的位置。使**证书密码**文本字段保留为空，因为此证书不需要密码。

2.为证书颁发机构重复此步骤，然后继续进行步骤 11。

> 如果要使用 ESET PROTECT 的自定义证书（而不是在 ESET PROTECT 安装过程中自动生成的默认证书），则在系统提示您提供代理证书时，应使用这些自定义证书。

12. 指定移动设备连接器的目标文件夹（建议使用默认目标文件夹），依次单击**下一步 > 安装**。

MDM 安装完成后，系统将提示您安装服务器代理。单击**下一步**开始安装，并接受 EULA（如果您同意），然后按照以下步骤操作：

1. 输入**服务器主机**（您的 ESET PROTECT 服务器的主机名或 IP 地址）和**服务器端口**（默认端口为 2222，如果要使用其他端口，请将该默认端口替换为您的自定义端口号）。

请确保**服务器主机**至少与在**服务器证书**的**主机**字段中定义的一个值相匹配（在理想情况下为 FQDN，否则您将收到错误消息“收到错误的服务器证书”。唯一的例外是，服务器证书主机字段中存在一个通配符 (*)，这意味着它适用于所有**服务器主机**。

2. 如果要使用代理，请选中**使用代理**复选框。选中后，安装程序将继续**脱机安装**。

此代理设置仅用于 ESET Management 服务器代理与 ESET PROTECT 服务器之间的（复制），不用于缓存更新。
- **代理主机名**：HTTP 代理计算机的主机名或 IP 地址。
- **代理端口**：默认值为 3128。
- **用户名**和**密码**：如果您的代理使用身份验证，则输入它使用的凭据。

可以稍后在策略中更改代理设置。在可以通过代理配置服务器代理 – 服务器连接之前，必须安装代理。

3. 选择以下安装选项之一，然后执行以下相应部分中的步骤：

服务器辅助安装 – 您将需要提供 ESET PROTECT Web 控制台管理员证书（安装程序将自动下载所需证书）。

脱机安装 – 您将需要提供服务器代理证书和证书颁发机构（均可从 ESET PROTECT 中导出）。此外，您可以使用自定义证书。

- 若要继续进行**服务器辅助服务器代理安装**，请按照以下步骤操作：

1. 在**服务器主机**字段中输入您的 ESET PROTECT Web 控制台的主机名或 IP 地址（与 ESET PROTECT 服务器相同）。如果您不使用自定义端口，请使 **Web 控制台端口**设置保留为默认端口 2223。另外，请在**用户名和密码字段**中输入您的 Web 控制台帐户凭据。若要以域用户登录，请选中**登录到域**旁边的复选框。

- 请确保**服务器主机**至少与在**服务器证书**的**主机**字段中定义的一个值相匹配（在理想情况下为 FQDN，否则您将收到错误消息“收到错误的服务器证书”。唯一的例外是，服务器证书主机字段中存在一个通配符 (*)，这意味着它适用于所有**服务器主机**。
- 无法让使用双重身份验证的用户参与服务器辅助安装。

2. 当询问您是否想要接受证书时，单击**是**。

3. 选择**不创建计算机(在第一次连接期间将自动创建计算机)**或**选择自定义静态组**。如果您单击**选择自定义静态组**，您将能够从 ESET PROTECT 中的现有静态组列表中进行选择。计算机将添加到您已选定的组。

4. 为 ESET Management 服务器代理指定目标文件夹（建议使用默认位置）、单击**下一步**，然后单击**安装**。

- 若要继续进行**脱机服务器代理安装**，请按照以下步骤操作：

1. 如果您在之前的步骤中已选择**使用代理**，则请提供**代理主机名**、**代理端口**（默认端口为 3128）、**用户名**和**密码**，然后单击**下一步**。

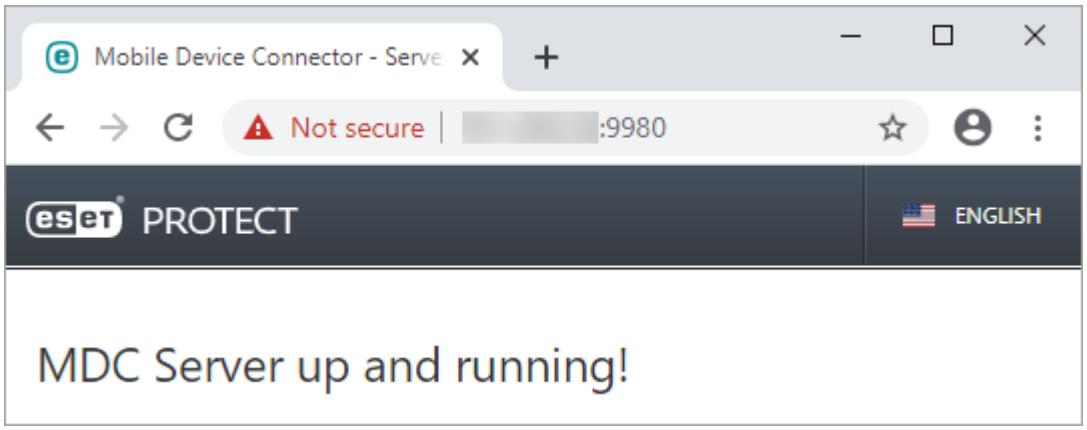
2. 单击**浏览**，然后导航到您的对等证书（这是已从 ESET PROTECT 中导出的服务器代理证书）的位置。使**证书密码**文本字段保留为空，因为此证书不需要密码。您无需浏览找到**证书颁发机构**（使此字段保留为空）。

如果您要使用 ESET PROTECT 的自定义证书（而不是在 ESET PROTECT 安装过程中自动生成的默认证书），请相应地使用您的自定义证书。

证书密码中不得包含以下字符：" \ 这些字符在初始化服务器代理期间会导致严重错误。

3. 单击**下一步**以安装到默认文件夹，或单击**更改**以选择另一个文件夹（建议您使用默认位置）。

安装完成后，通过在 Web 浏览器中或使用移动设备打开 *https://your-mdm-hostname:enrollment-port*（例如 *https://mdm.company.com:9980*）可检查移动设备连接器是否正常运行。如果已成功安装，您将看到以下消息：



现在您可以从 ESET PROTECT 激活 MDM

Windows 上的组件安装

许多安装方案都要求您在不同的计算机上安装不同的ESET PROTECT组件，以适应网络架构、符合性能要求，或者出于其他原因这样操作。以下安装程序包可供个别 ESET PROTECT 组件使用：

核心组件安装：

- ESET PROTECT 服务器
- ESET PROTECT Web 控制台 - 可以在未安装 ESET PROTECT 服务器的其他计算机上安装 ESET PROTECT Web 控制台。
- ESET Management 服务器代理（必须安装在客户端计算机上，也可以安装在 ESET PROTECT 服务器上）

可选组件安装：

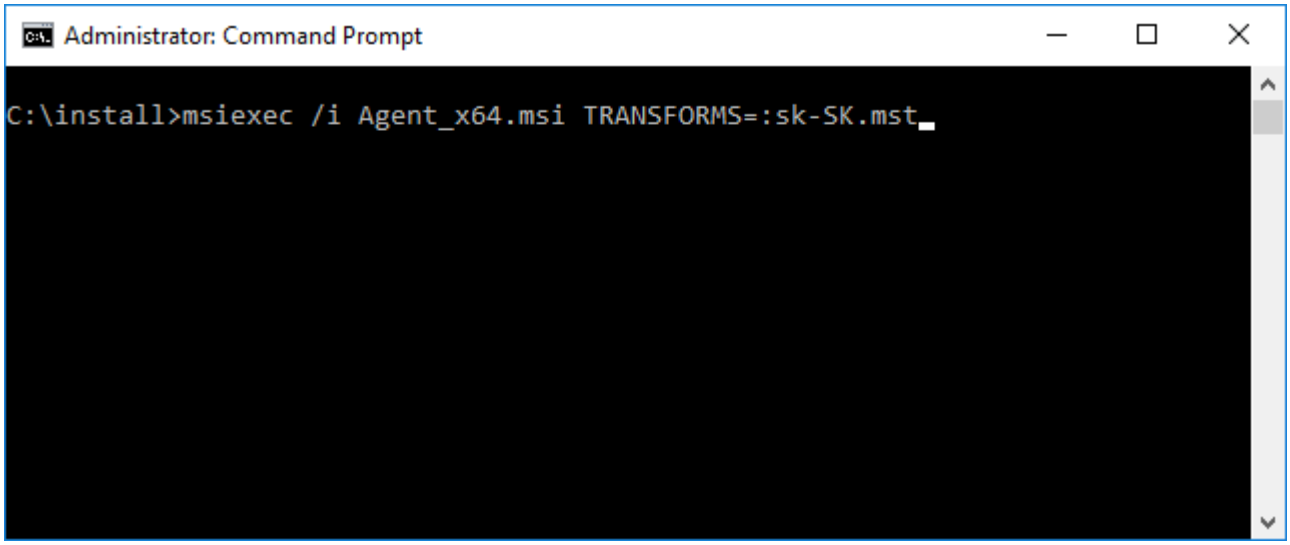
- RD Sensor
- 移动设备连接器
- ESET Bridge HTTP 代理
- 镜像工具

另请参阅 ESET PROTECT 一体式安装

有关将 ESMC 升级到最新 ESET PROTECT 10.0 的说明，请参阅我们的升级过程

如果您希望采用本地语言运行安装，您需要通过命令行启动特定 ESET PROTECT 组件的 MSI 安装程序。

下面是如何采用斯洛伐克语运行安装的示例：



若要选择运行安装程序所希望采用的语言，请依据下表指定相应的 TRANSFORMS 参数：

语言	代码
英语（美国）	en-US
阿拉伯语（埃及）	ar-EG
简体中文	zh-CN
繁体中文	zh-TW
克罗地亚语（克罗地亚）	hr-HR
捷克语（捷克共和国）	cs-CZ
法语（法国）	fr-FR
法语（加拿大）	fr-CA
德语（德国）	de-DE
希腊语（希腊）	el-GR
匈牙利语（匈牙利）*	hu-HU
印度尼西亚语（印度尼西亚）*	id-ID
意大利语（意大利）	it-IT
日语（日本）	ja-JP
朝鲜语（韩国）	ko-KR
波兰语（波兰）	pl-PL
葡萄牙语（巴西）	pt-BR
俄语（俄罗斯）	ru-RU
西班牙语（智利）	es-CL
西班牙语（西班牙）	es-ES

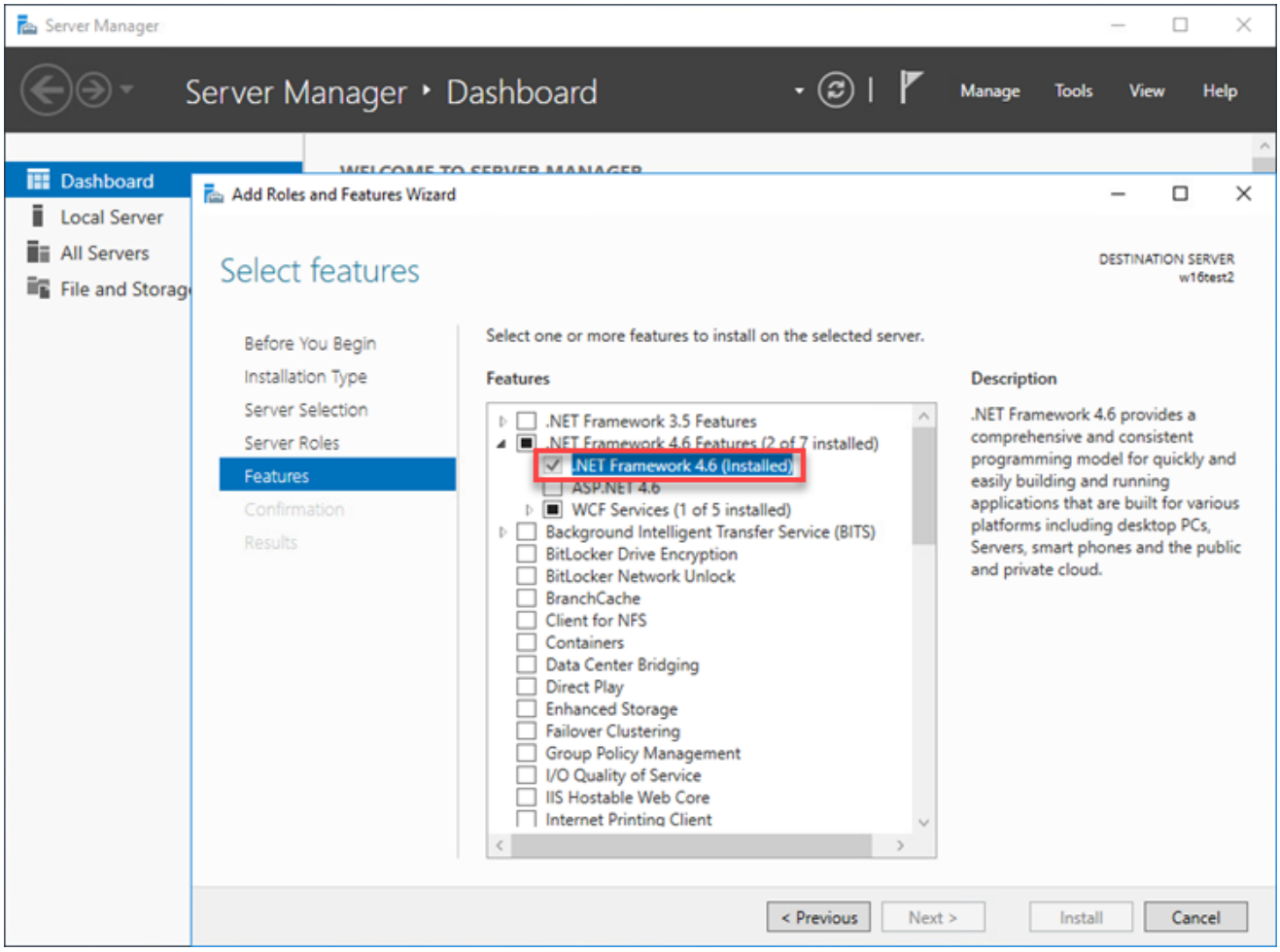
语言	代码
斯洛伐克语（斯洛伐克）	sk-SK
土耳其语（土耳其）	tr-TR
乌克兰语（乌克兰）	uk-UA

* 仅该产品以此语言提供，不提供该语言的联机帮助。

服务器安装 - Windows

先决条件

- 必须具有有效的许可证密钥
- 必须具有受支持的 Windows 操作系统
- 所需端口必须打开且可用 – 请在此处查看端口的完整列表
- 受支持的数据库服务器和连接器Microsoft SQL Server 或 MySQL）已安装并正在运行。建议您查看数据库服务器配置的详细信息（Microsoft SQL Server 或 MySQL），以确保为与 ESET PROTECT 配合使用正确配置了数据库。阅读我们的知识库文章，以为 Microsoft SQL 或 MySQL 设置数据库和数据库用户。
- ESET PROTECT Web 控制台已安装，可用于管理 ESET PROTECT 服务器。
- Microsoft SQL Server Express 安装需要 Microsoft .NET Framework 4您可以使用**添加角色和功能向导**安装它：



安装

按照下面的步骤在 Windows 上安装 ESET PROTECT 服务器组件：

确保满足上面列出的所有安装先决条件。

1. 访问 ESET PROTECT 下载部分，以下载此 ESET PROTECT 组件的独立安装程序（*server_x64.msi*）.

2. 运行 ESET PROTECT 服务器安装程序并接受 EULA（如果同意）。

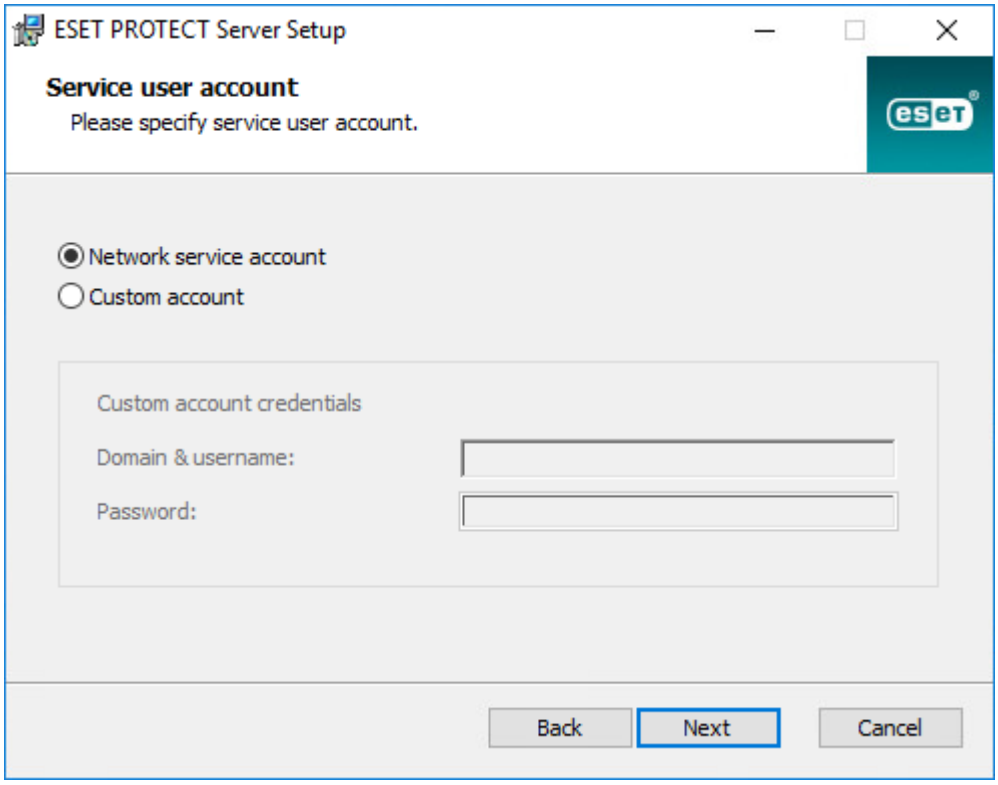
3. 选中**参与产品改进计划**复选框，以将匿名遥测数据和崩溃报告发送给 ESET（操作系统版本和类型、ESET 产品版本和其他特定于产品的信息）。

4. 取消选中**这是群集安装**旁的复选框，然后单击**下一步**。 这是群集安装吗？

如果要在故障转移群集上安装 ESET PROTECT 服务器，请选中**这是群集安装**旁边的复选框。将**自定义应用程序数据路径**指定为指向该群集的共享存储。数据必须存储在一个群集中所有节点都可访问的位置。

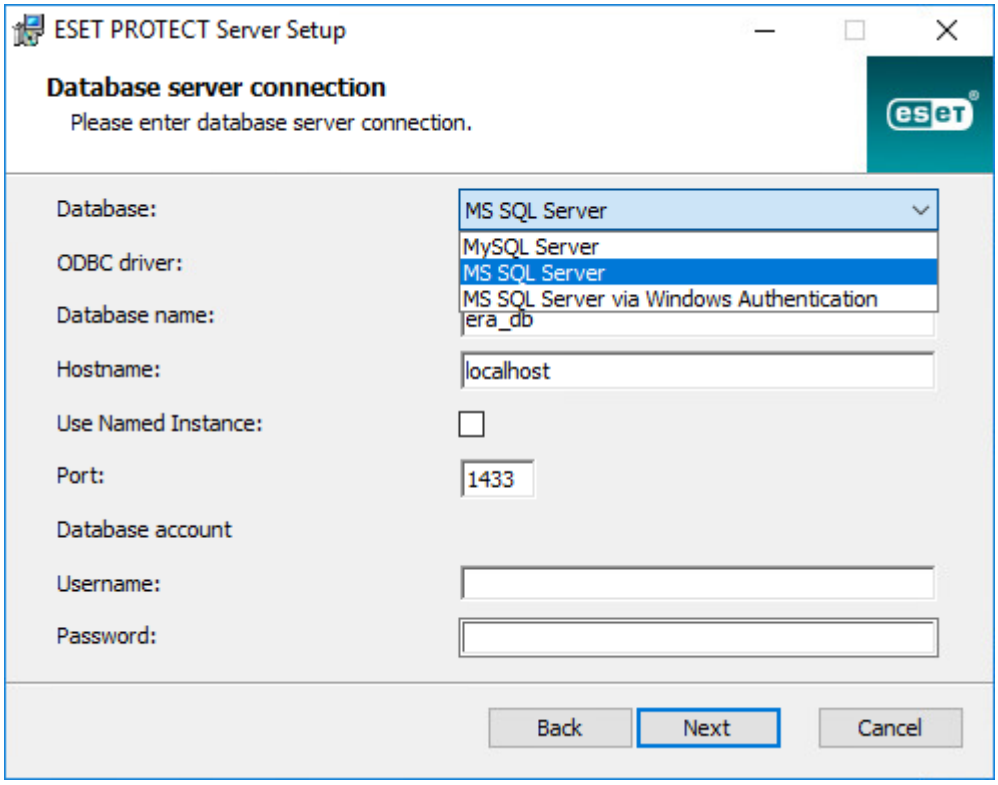
5. 选择一个**服务用户帐户**。此帐户将用于运行 ESET PROTECT 服务器服务。有以下选项可供使用：

- **网络服务帐户** – 如果不使用域，请选择此选项。
- **自定义帐户**：提供域用户凭据：`DOMAIN\USERNAME` 和密码。



6. 连接到数据库。所有数据都存储在此处（ESET PROTECT Web 控制台密码、客户端计算机日志等）：

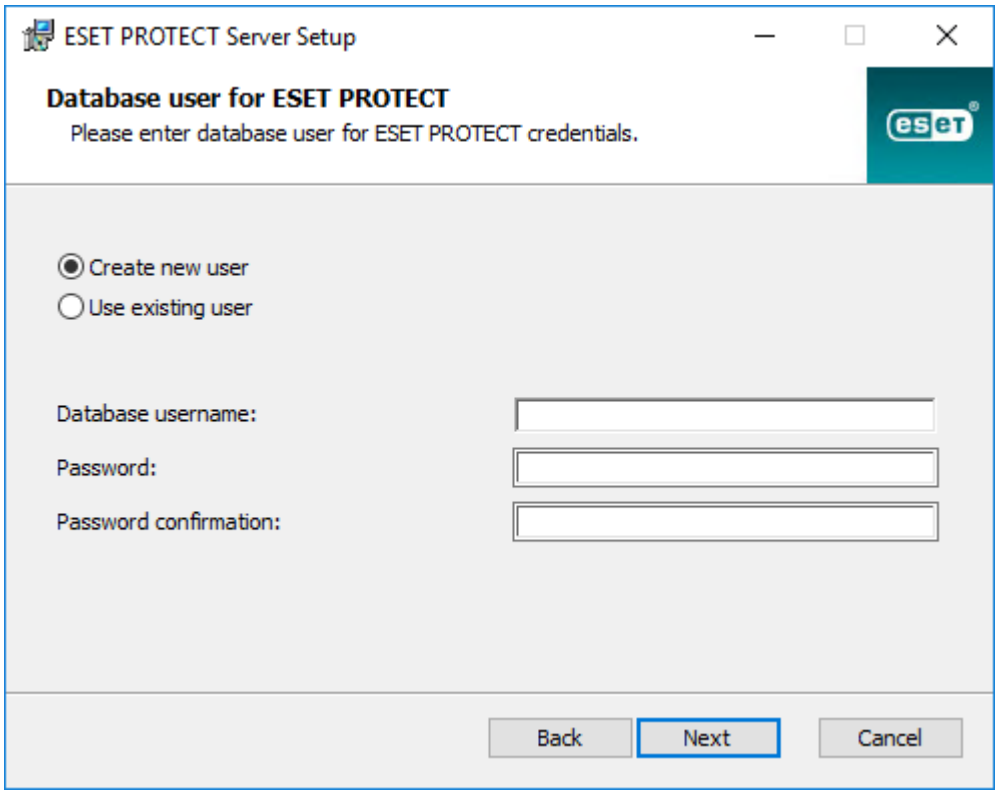
- **数据库**：MySQL Server/MS SQL Server/通过 Windows 身份验证的 MS SQL Server
- **ODBC 驱动程序**：MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 Unicode Driver/MySQL ODBC 5.3 Unicode Driver/MySQL ODBC 8.0 Unicode Driver/SQL Server/SQL Server Native Client 10.0/ODBC Driver 11 for SQL Server/ODBC Driver 13 for SQL Server/ODBC Driver 17 for SQL Server/ODBC Driver 18 for SQL Server
- **数据库名称**：建议您使用预定义的名称或更改它（如果需要）。
- **主机名**：数据库服务器的主机名或 IP 地址
- **端口**： 用于连接到数据库服务器
- 数据库管理员帐户**用户名/密码**
- **使用命名实例** – 如果您使用的是 Microsoft SQL 数据库，您还可以选中**使用命名实例**复选框以使用自定义数据库实例。您可以在**主机名**字段中使用 *HOSTNAME\DB_INSTANCE* 格式（例如，*192.168.0.10\ESMC7SQL*）设置它。对于群集数据库，仅使用群集名称。如果选中此选项，则无法更改数据库连接端口 – 系统将使用由 Microsoft 确定的默认端口。若要将 ESET PROTECT 服务器连接到故障转移群集中安装的 Microsoft SQL 数据库，请在**主机名**字段中输入群集名称。



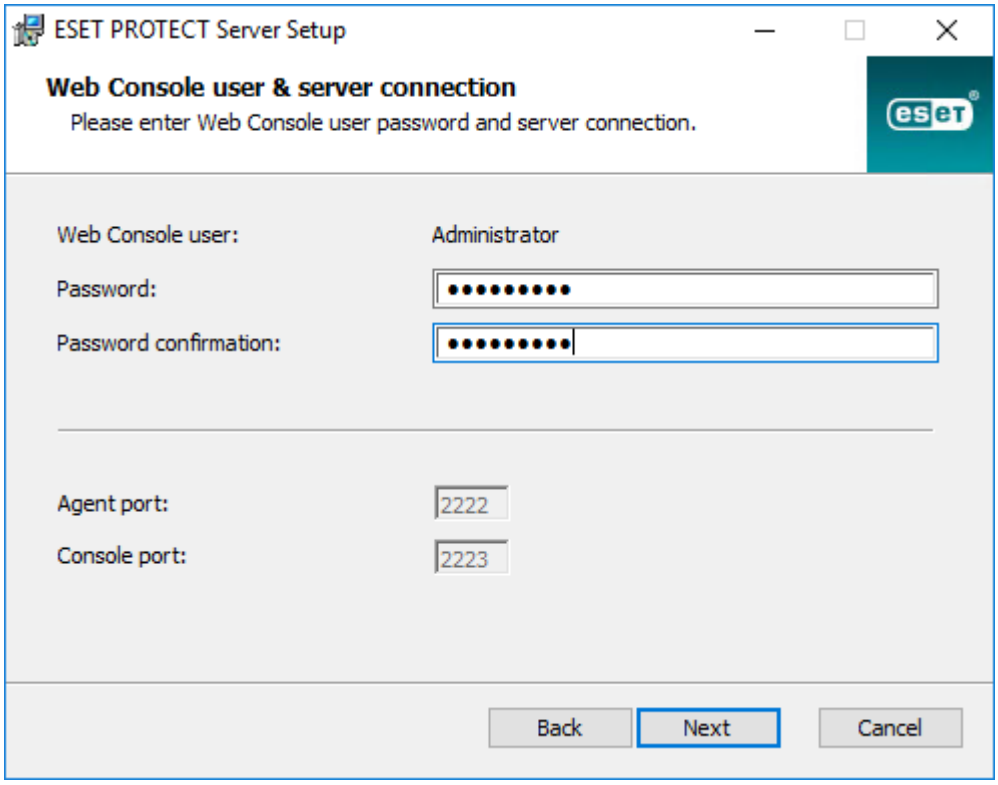
ESET PROTECT 服务器在数据库中存储大数据 blob。因此，要使 ESET PROTECT 能够正常运行，必须将 MySQL 配置为接受大数据包。

此步骤将验证您到数据库的连接。如果连接正常，则继续执行下一个步骤。

7. 为有数据库访问权限的 ESET PROTECT 选择一个用户。您可以使用现有用户，或者安装程序可以为您创建一个用户。

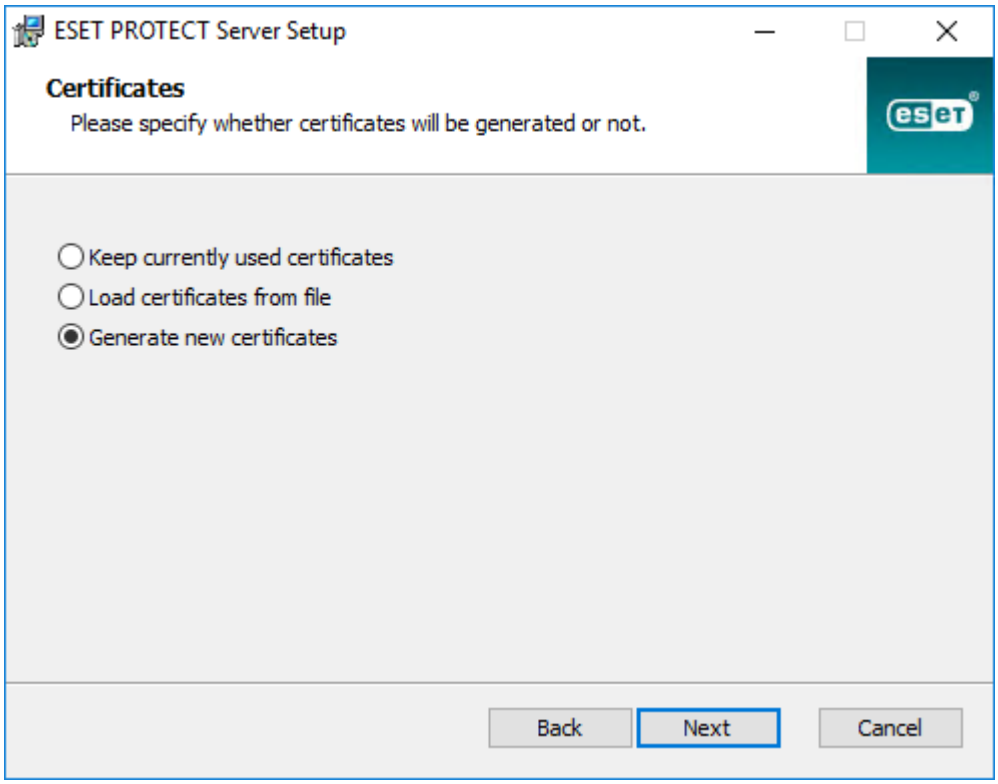


8. 输入 **Web 控制台**访问的密码。



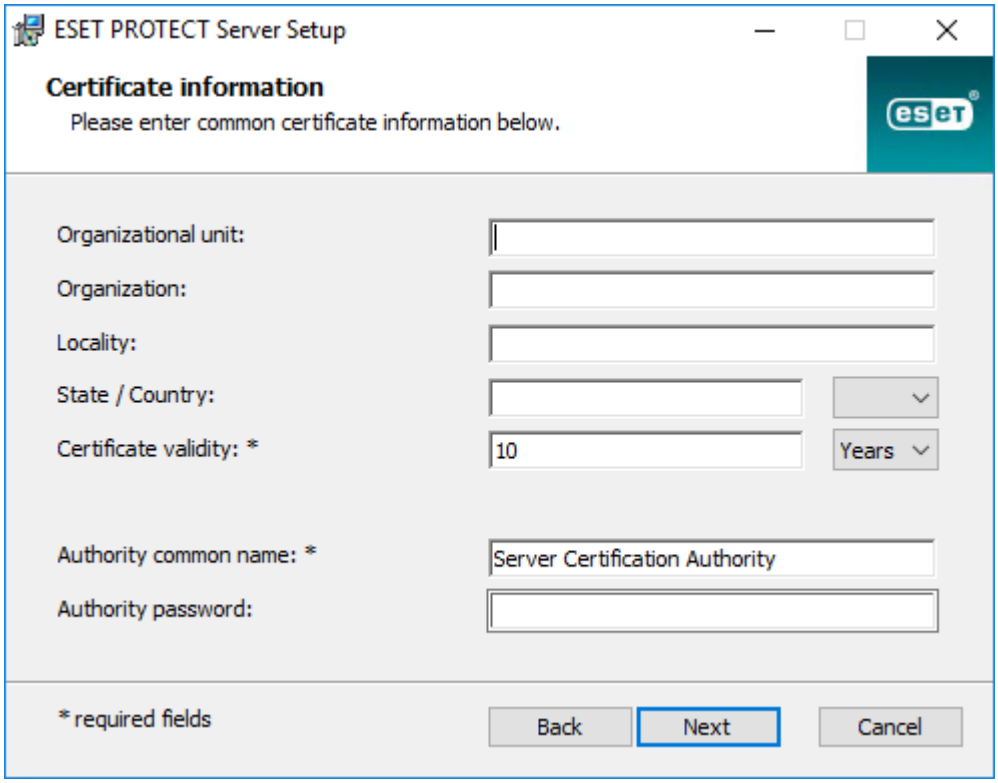
9. ESET PROTECT 将证书用于客户端–服务器通信。选择以下选项之一：

- **保留当前使用的证书** – 仅当以前另一个 ESET PROTECT 服务器已使用数据库时，该选项才可用。
- **从文件加载证书** – 选择现有的服务器证书和证书颁发机构。
- **生成新证书** – 安装程序将生成新的证书。



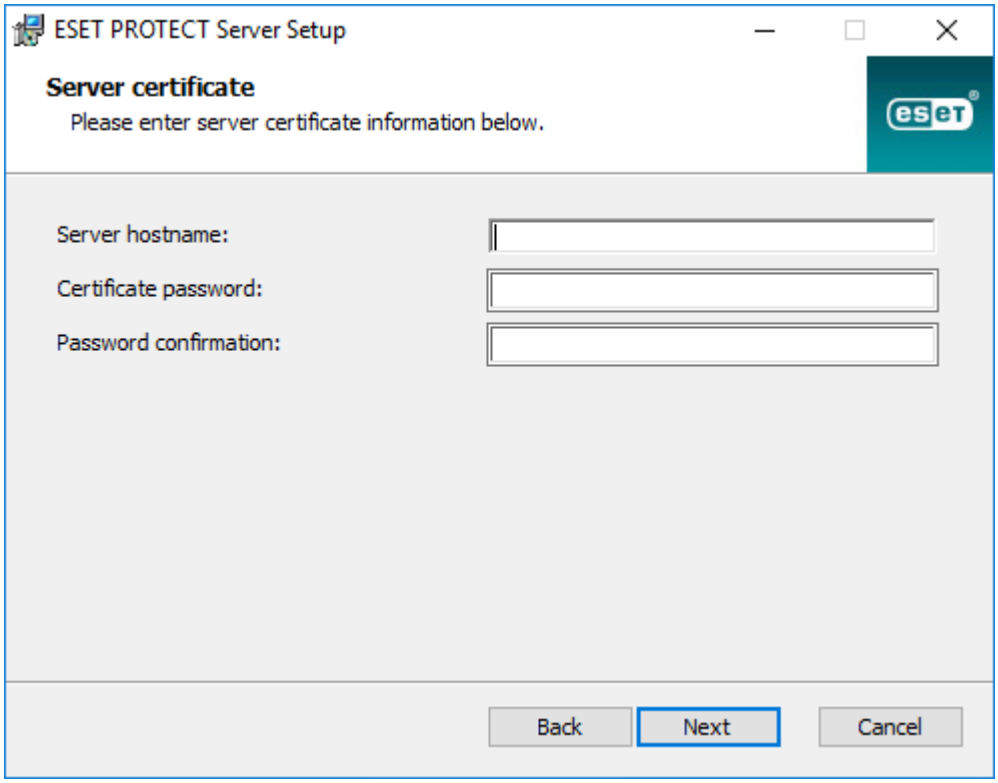
10. 如果已在上一步中选择**生成新证书**选项，请遵循此步骤。

a)指定有关证书的其他信息（可选）。如果键入**颁发机构密码**，请务必记住它。

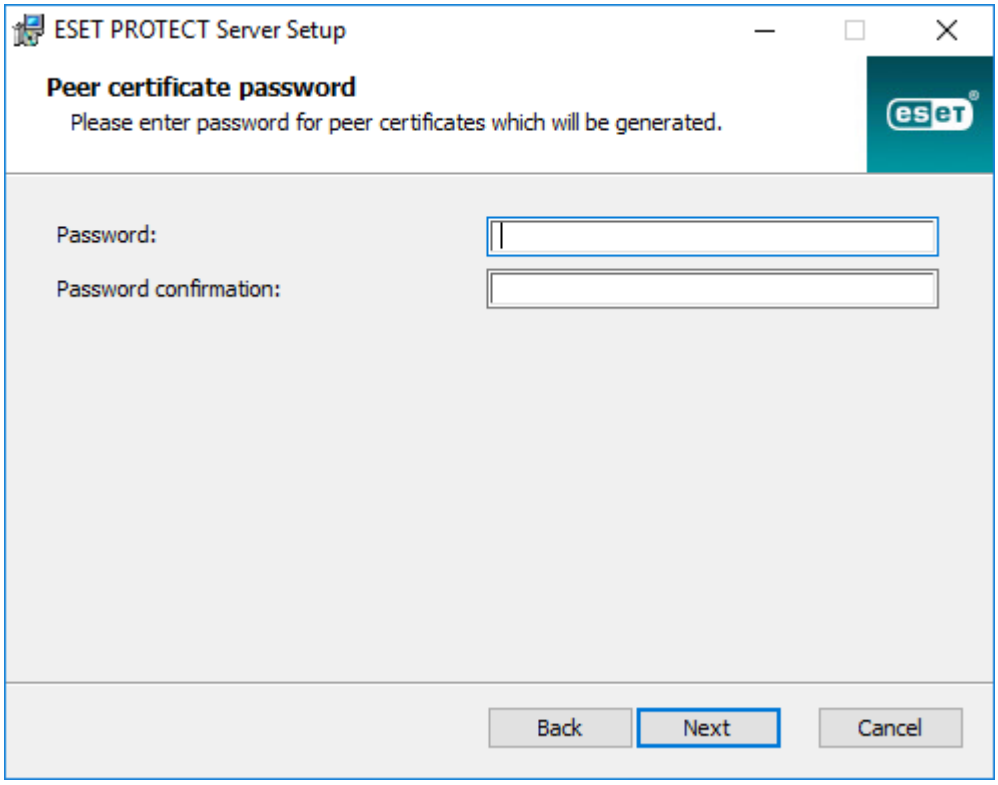


b)在**服务器证书**字段中，键入**服务器主机名**和**证书密码**（可选）。

⚠ 服务器证书中的**服务器主机名**不得包含以下任一关键字：server proxy agent

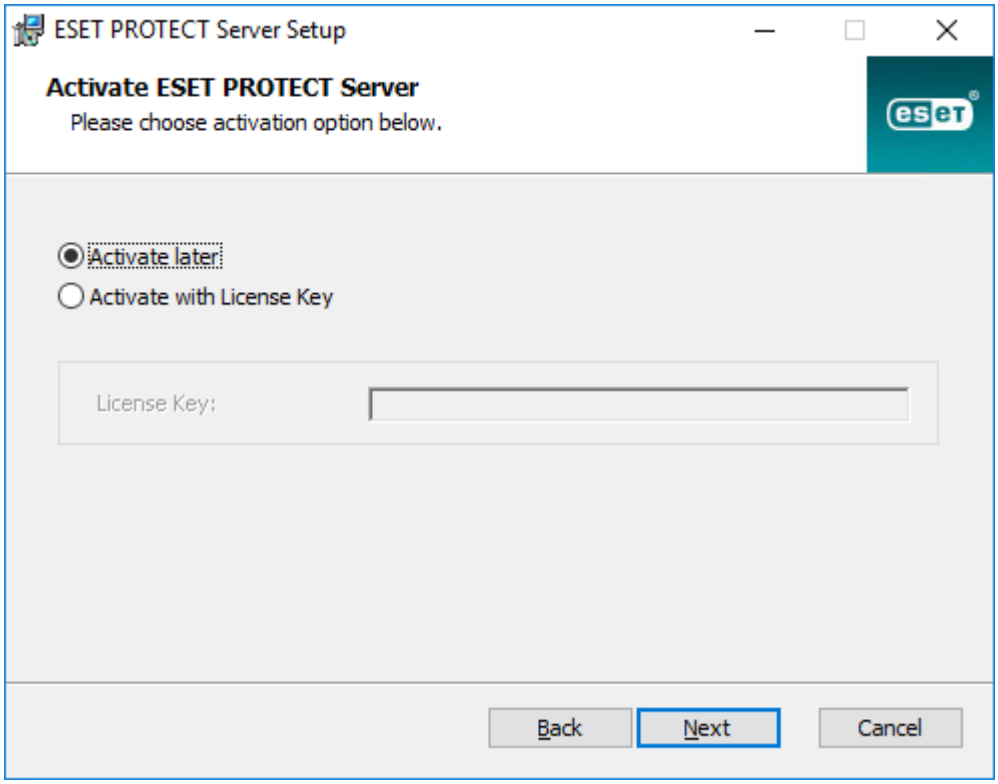


c)在**对等证书密码**字段中，键入服务器代理和代理对等证书的密码。



11. 安装程序可以执行初始静态组同步任务。选择方法（**不同步**、**与 Windows 网络同步**或**与 Active Directory 同步**）并单击**下一步**。

12. 输入有效的许可证密钥，或者选择**以后激活**。



13. 确认或更改服务器的安装文件夹并单击**下一步**。

14. 单击**安装**以安装 ESET PROTECT 服务器。

完成 ESET PROTECT 服务器安装后，可以在同一台计算机上安装 ESET Management 服务器代理（可选），以便能够以与管理客户端计算机相同的方式管理服务器。

Microsoft SQL Server 要求

必须满足 Microsoft SQL Server 的以下要求：

- 安装受支持版本的 Microsoft SQL Server。在安装过程中选择**混合模式**身份验证。
- 如果已安装 Microsoft SQL Server，则将身份验证设置为**混合模式(SQL Server 身份验证和 Windows 身份验证)**。若要执行此操作，请按照此知识库文章中的说明操作。如果要使用 **Windows 身份验证**来登录 Microsoft SQL Server，请按照本知识库文章中的步骤进行操作。
- 允许到 SQL Server 的 TCP/IP 连接。若要执行此操作，请按照此知识库文章（位于 **II.允许到 SQL 数据库的 TCP/IP 连接**部分中）中的说明操作。

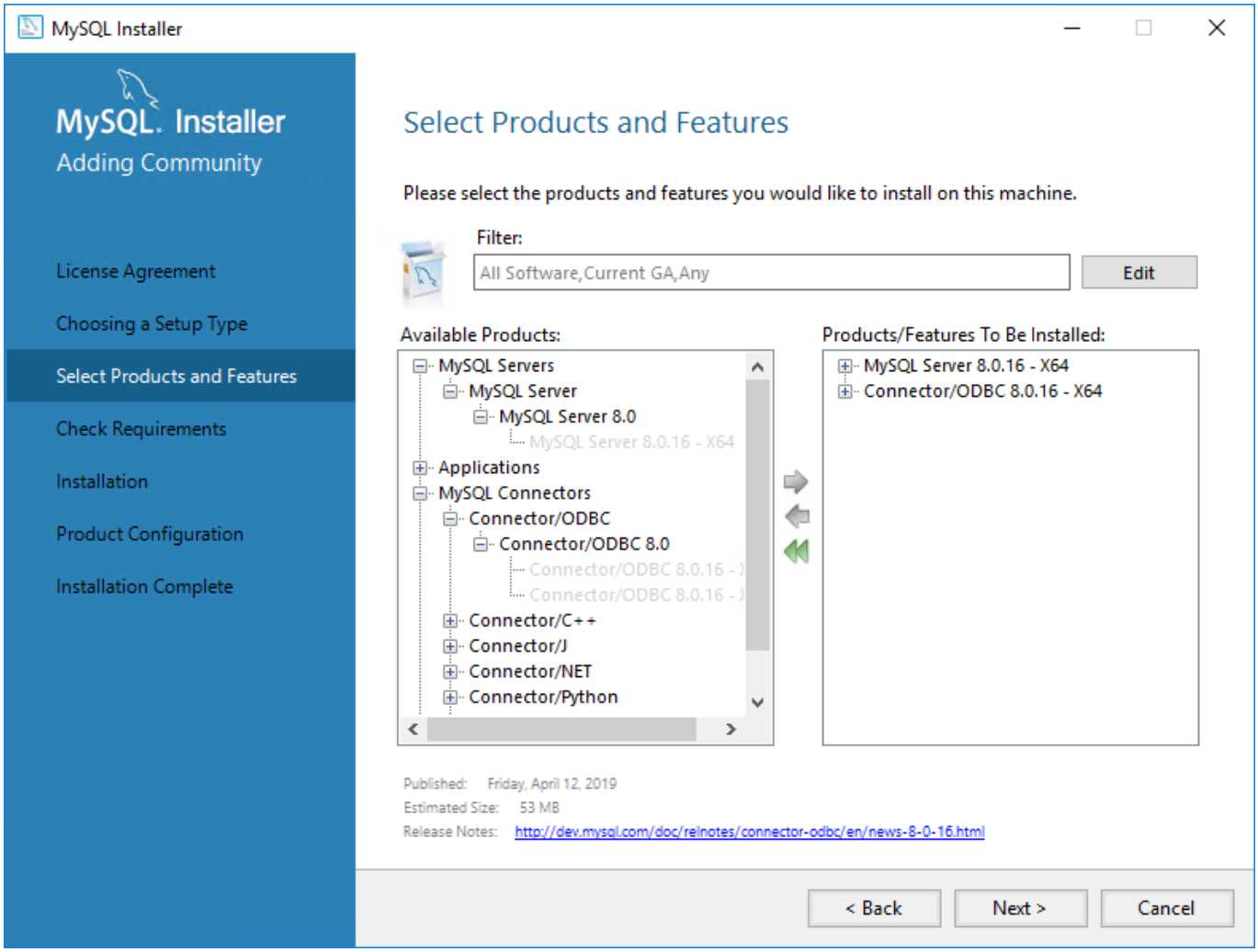
- 若要配置、管理、运行 Microsoft SQL Server 数据库和用户），请下载 SQL Server Management Studio (SSMS)
- 在域控制器（例如 Windows SBS/Essentials 上不要安装 SQL Server。建议您在其他服务器上安装 ESET PROTECT 或者在安装期间不选择 SQL Server Express 组件（这要求您使用现有 SQL 或 MySQL Server 来运行 ESET PROTECT 数据库）。

MySQL Server 安装和配置

安装

确保安装受支持版本的 MySQL Server 和 ODBC 连接器

1. 从 https://dev.mysql.com/downloads/installer/ 下载并执行 MySQL 8 Windows 安装程序。
2. 选中**我接受许可条款**的复选框，然后单击**下一步**。
3. 安装设置期间，请依次选择**自定义**、**MySQL Server** 和要安装的**连接器/ODBC**。确保 ODBC 连接器与已安装的 MySQL Server 的 x86 或 x64 的位数相匹配：



4. 单击**下一步**和**执行**以安装 MySQL Server 和 ODBC 连接器。

5. 单击**下一步**。在**高可用性**中，选择**独立 MySQL Server/经典 MySQL 复制**，然后单击**下一步**。

6. 在**类型和网络**中，从**配置类型**下拉菜单中选择**服务器计算机**，然后单击**下一步**。

7. 在**验证方法**中，选择建议选项**使用强密码加密进行验证**，然后单击**下一步**。

8. 在**帐户和角色**中，键入 **MySQL 根密码**两次。我们建议您创建专用数据库用户帐户。

9. 在 **Windows 服务**中，保留预选择的值，然后单击**下一步**。

10. 单击**执行**并等待 MySQL 服务器安装完成。单击**完成**。**下一步**和**完成**以关闭安装窗口。

配置

1. 使用文本编辑器打开以下文件：

C:\ProgramData\MySQL\MySQL Server 8.0\my.ini

2. 查找和编辑以下配置或者将该配置附加到 *[mysqld]* 文件的 `my.ini` 部分：

> i
> - 如果文件中不存在 `[mysqld]` 部分，请创建它。
> - 如果该文件中不存在这些参数，请将它们添加到 `[mysqld]` 部分。
> - 要确定 MySQL 版本，请运行命令：`mysql --version`

参数	注释和建议值	MySQL 版本
max_allowed_packet=33M		所有支持的版本
log_bin_trust_function_creators=1	或者，还可以禁用二进制日志记录：log_bin=0	支持的 8.x 版本
innodb_log_file_size=100M innodb_log_files_in_group=2	这两个参数值的乘积必须至少为 **200** innodb_log_files_in_group 的最小值为 **2**，最大值为 **100**；该值还必须为整数。	支持的 8x 版本 5.7 5.6.22（及更高版本 5.6.x)
innodb_log_file_size=200M	将该值设置为至少 **200M**，但不要超过 **3000M**	5.6.20 和 5.6.21

3. 保存并关闭 *my.ini* 文件。

4. 打开命令提示，然后输入以下命令来重新启动 MySQL Server 并应用该配置（进程名称取决于 MySQL 版本8.0 = mysql80 等）：

```
net stop mysql80
net start mysql80
```

5. 在命令提示符下输入以下命令，以检查 MySQL 服务器是否在运行：

```
sc query mysql80
```

专用数据库用户帐户

如果您不希望使用 **SA 帐户** (Microsoft SQL) 或**根帐户** (MySQL)可以创建**专用数据库用户帐户**。此专用用户帐户仅用于访问 ESET PROTECT 数据库。我们建议您先在您的数据库服务器中创建专用数据库用户帐户，然后再开始安装 ESET PROTECT此外，您还需要创建空数据库以供 ESET PROTECT 使用此专用用户帐户进行访问。

必须将一组基本的权限授予专用数据库用户帐户。

- MySQL 用户权限：ALTER, ALTER ROUTINE, CREATE, CREATE ROUTINE, CREATE TEMPORARY TABLES, CREATE VIEW, DELETE, DROP, EXECUTE, INDEX, INSERT, LOCK TABLES, SELECT, UPDATE, TRIGGER。– 有关 MySQL 权限的详细信息，请参阅 http://dev.mysql.com/doc/refman/8.0/en/grant.html

- Microsoft SQL Server 数据库级角色ESET PROTECT 数据库用户必须是 db_owner 数据库角色成员。有关 Microsoft SQL Server 数据库级角色的详细信息，请参阅 https://msdn.microsoft.com/zh-cn/library/ms189121%28v=sql.100%29.aspx

您可以在我们的知识库文章中查找有关如何设置 Microsoft SQL 和 MySQL 的数据库和用户帐户的详细指南。

服务器代理安装 - Windows

可用方法

有各种安装和部署方法可用于在 Windows 工作站上安装 ESET Management 服务器代理：

方法	文档	说明
通过 *.msi* 安装程序基于 GUI 安装	• 本章节 • KB	• **标准**安装方法。 •此方法可以作为服务器辅助安装或脱机安装执行。 • 在 ESET PROTECT 服务器计算机上安装服务器代理时使用此方法。
ESET Remote Deployment Tool	• 联机帮助	• 建议用于通过本地网络的批量部署。 • 可用于部署一体式安装程序（服务器代理 + ESET 安全产品）
一体式服务器代理安装程序	• 创建一体式服务器代理安装程序 • KB	• 该安装程序还可以包含安全产品和嵌入式策略。 • 安装程序大小为数百 MB
服务器代理脚本安装程序	• 创建服务器代理脚本安装程序 • KB	• 该安装程序是可执行脚本。它的大小较小，但需要访问 *.msi* 安装程序的位置。 • 可以编辑该脚本以使用本地安装程序和 HTTP 代理。
SCCM 和 GPO 部署	• SCCM • GPO • KB	• 远程批量部署的高级方法。 • 使用较小 *.ini* 文件。
服务器任务 – 服务器代理部署	• 联机帮助 • KB	• SCCM 和 GPO 的替代方法。 • 通过 HTTP 代理不可行。 • 由 ESET PROTECT 服务器通过 ESET PROTECT Web 控制台执行。

服务器代理和 ESET PROTECT 服务器之间的通信协议不支持身份验证。任何用于将服务器代理通信转发到需要身份验证的 ESET PROTECT 服务器的代理解决方案将不工作。
如果针对 Web 控制台或服务器代理选择使用非默认端口，可能需要调整防火墙。否则，安装可能会失败。

基于 GUI 安装

按照下面的步骤在 Windows 上本地安装 ESET Management 服务器代理组件：

1. 访问 ESET PROTECT 下载部分，以下载此 ESET PROTECT 组件的独立安装程序（*agent_x86.msi*、*agent_x64.msi* 或 *agent_arm64.msi*）。

2. 运行 ESET Management 服务器代理安装程序并接受 EULA（如果同意）。

3. 选中**参与产品改进计划**复选框，以将匿名遥测数据和崩溃报告发送给 ESET（操作系统版本和类型、ESET 产品版本和其他特定于产品的信息）。

4. 输入**服务器主机**（您的 ESET PROTECT 服务器的主机名或 IP 地址）和**服务器端口**（默认端口为 2222，如果要使用其他端口，请将该默认端口替换为您的自定义端口号）。

请确保**服务器主机**至少与在**服务器证书**的**主机**字段中定义的一个值相匹配（理想情况下为 FQDN），否则您将收到错误消息“收到错误的服务器证书”。使用服务器证书主机字段中的通配符 (*) 将允许证书适用于所有**服务器主机**。

5. 如果使用服务器代理的代理 – 服务器连接，请选中**使用代理**旁边的复选框。选中后，安装程序将继续脱机安装。

此代理设置仅用于 ESET Management 服务器代理与 ESET PROTECT 服务器之间的（复制），不用于缓存更新。
- **代理主机名**：HTTP 代理计算机的主机名或 IP 地址。
- **代理端口**：默认值为 3128。
- **用户名**/**密码**：如果您的代理使用身份验证，则输入它使用的凭据。

可以稍后在策略中更改代理设置。在可以通过代理配置服务器代理 – 服务器连接之前，必须安装代理。

6. 选择以下安装选项之一，然后执行以下相应部分中的步骤：

- 服务器辅助安装 – 将需要提供 ESET PROTECT Web 控制台管理员证书。安装程序将自动下载所需证书。

无法让使用双重身份验证的用户参与服务器辅助安装。

- 脱机安装 – 将需要提供服务器代理证书和证书颁发机构。两者皆可从 ESET PROTECT 导出。此外，您可以使用自定义证书。

命令行安装

MSI 安装程序可以本地或远程运行。从 ESET 网站下载 ESET Management 服务器代理。

参数	说明和允许的值
P_HOSTNAME=	ESET PROTECT 服务器的主机名或 IP 地址。
P_PORT=	服务器代理连接的服务器端口（可选；如果未指定，则使用默认端口 2222）。
P_CERT_PATH=	*.txt* 文件中采用 Base64 格式的服务器代理证书的路径（从 ESET PROTECT Web 控制台导出）
P_CERT_AUTH_PATH=	*.txt* 文件中采用 Base64 格式的证书颁发机构的路径（从 ESET PROTECT Web 控制台导出）
P_LOAD_CERTS_FROM_FILE_AS_BASE64=	**YES**；当引用 *.txt* 文件中存储的服务器代理证书和证书颁发机构时使用此参数。
P_CERT_PASSWORD=	使用此参数为服务器代理证书提供密码。
P_CERT_CONTENT=	采用 Base64 格式的服务器代理证书字符串（从 ESET PROTECT Web 控制台导出）
P_CERT_AUTH_CONTENT=	采用 Base64 格式的证书颁发机构字符串（从 ESET PROTECT Web 控制台导出）
PASSWORD=	用于卸载受密码保护的服务器代理的密码。
P_ENABLE_TELEMETRY=	**0** – 禁用（默认选项）；**1** – 启用。将崩溃报告和遥测数据发送至 ESET（可选参数）。
P_INSTALL_MODE_EULA_ONLY=	**1**；将此参数用于半静默 ESET Management 服务器代理安装。可以看到服务器代理安装窗口，并且系统会提示您接受最终用户许可协议并启用/禁用遥测（P_ENABLE_TELEMETRY 在已指定时会忽略）。其他服务器代理安装设置获取自命令行参数。可以看到服务器代理安装过程完成。

参数	说明和允许的值
P_USE_PROXY=	**1**：使用此参数以支持将 HTTP 代理（已安装在网络中）用于 ESET Management 服务器代理和 ESET PROTECT 服务器之间的复制（而非用于缓存更新）。
P_PROXY_HTTP_HOSTNAME=	HTTP 代理的主机名或 IP 地址。
P_PROXY_HTTP_PORT=	用于服务器代理连接的 HTTP 代理端口。

命令行安装示例

如有必要，请替换以下橙色代码。

- 静默安装（/q 参数），其采用默认端口连接、启用遥测以及服务器代理证书和证书颁发机构存储在文件中：

```
Agent_x64.msi /q P_HOSTNAME=10.20.30.40 P_ENABLE_TELEMETRY=1 P_CERT_PATH=C:\Users\Ad
ministrator\Desktop\certificate.txt P_CERT_AUTH_PATH=C:\Users\Administrator\Desktop\
ca.txt P_LOAD_CERTS_FROM_FILE_AS_BASE64=YES
```

- 静默安装，其提供用于服务器代理证书和证书颁发机构的字符串以及服务器代理证书密码和 HTTP 代理参数：

```
Agent_x64.msi /q P_HOSTNAME=protect_server_name P_ENABLE_TELEMETRY=1 P_CERT_CONTENT=
CJfXtf1kZqlZKAl9P48HymBHa3CkW P_CERT_PASSWORD=abcd1234EFGH P_CERT_AUTH_CONTENT=45hvk
pqayzjJZhSY8qswDQYJKoZIhvc P_USE_PROXY=1 P_PROXY_HTTP_HOSTNAME=proxy_server P_PROXY_
HTTP_PORT=3128
```

- 半静默安装：

```
Agent_x64.msi P_INSTALL_MODE_EULA_ONLY=1 P_HOSTNAME=10.20.30.40 P_CERT_PATH=C:\Users
\Administrator\Desktop\certificate.txt P_CERT_AUTH_PATH=C:\Users\Administrator\Deskt
op\ca.txt P_LOAD_CERTS_FROM_FILE_AS_BASE64=YES
```

服务器辅助服务器代理安装

若要继续进行**服务器辅助服务器代理安装**，请按照以下步骤操作：

1. 在**服务器主机**字段中输入您的 ESET PROTECT Web 控制台的主机名或 IP 地址（与 ESET PROTECT 服务器相同）。如果您不使用自定义端口，请使 **Web 控制台端口**设置保留为默认端口 2223。另外，请在**用户名和密码字段**中输入您的 Web 控制台帐户凭据。若要以域用户登录，请选中**登录到域**旁边的复选框。

> - 请确保**服务器主机**至少与在**服务器证书**的**主机**字段中定义的一个值相匹配（在理想情况下为 FQDN。否则您将收到错误消息“收到错误的服务器证书”。唯一的例外是，服务器证书主机字段中存在一个通配符 (*)，这意味着它适用于所有**服务器主机**。
> - 无法让使用双重身份验证的用户参与服务器辅助安装。

2. 当询问您是否想要接受证书时，单击**是**。

3. 选择**不创建计算机（在第一次连接期间将自动创建计算机）**或**选择自定义静态组**。如果您单击**选择自定**

义静态组，您将能够从 ESET PROTECT 中的现有静态组列表中进行选择。计算机将添加到您已选定的组。

4. 为 ESET Management 服务器代理指定目标文件夹（建议使用默认位置）、单击**下一步**，然后单击**安装**。

脱机服务器代理安装

若要继续进行**脱机服务器代理安装**，请按照以下步骤操作：

1. 如果您在之前的步骤中已选择**使用代理**，则请提供**代理主机名**、**代理端口**（默认端口为 3128）、**用户名**和**密码**，然后单击**下一步**。

2. 单击**浏览**，然后导航到您的对等证书（这是已从 ESET PROTECT 中导出的服务器代理证书）的位置。使**证书密码**文本字段保留为空，因为此证书不需要密码。您无需浏览找到**证书颁发机构**（使此字段保留为空）。

> 如果您要使用 ESET PROTECT 的自定义证书（而不是在 ESET PROTECT 安装过程中自动生成的默认证书），请相应地使用您的自定义证书。

> 证书密码中不得包含以下字符：" \ 这些字符在初始化服务器代理期间会导致严重错误。

3. 单击**下一步**以安装到默认文件夹，或单击**更改**以选择另一个文件夹（建议您使用默认位置）。

ESET Remote Deployment Tool

ESET Remote Deployment Tool 是一种通过网络分发由 ESET PROTECT 创建的安装程序包以在计算机上远程部署 ESET Management 服务器代理和 ESET 安全产品的便捷方式。

ESET Remote Deployment Tool 在 ESET 网站上以独立的 ESET PROTECT 组件形式免费提供。该部署工具主要用于小型到中型网络上的部署并在管理员权限下执行。

> ESET Remote Deployment Tool 专用于将 ESET Management 服务器代理部署到仅装有支持的 Microsoft Windows 操作系统的客户端计算机。

有关先决条件和工具用法的更多详细信息，请参阅 ESET Remote Deployment Tool 章节。

Web 控制台安装 - Windows

在 Windows 上，可以通过以下两种方式安装 ESET PROTECT Web 控制台：

- 建议使用一体式安装程序
- 高级用户可以执行手动安装

> 可以在未安装 ESET PROTECT 服务器的其他计算机上安装 ESET PROTECT Web 控制台。

使用一体式安装程序安装 Web 控制台

先决条件

- ESET PROTECT 服务器已安装。

> 可以在未安装 ESET PROTECT 服务器的其他计算机上安装 ESET PROTECT Web 控制台。 该过程需要其他步骤

- Apache Tomcat 是运行 ESET PROTECT Web Console 所需的必需组件。

- Apache Tomcat 需要 64 位 Java/OpenJDK。如果在系统上安装了多个 Java 版本，建议您卸载较早的 Java 版本并仅保留最新的受支持的 Java 版本。

> 从 2019 年 1 月开始，面向企业、商业或生产用途的 Oracle JAVA SE 8 公开更新将需要商业许可证。如果不购买 JAVA SE 订阅，可以使用本指南来转换为免费替代方案。请参阅 JDK 的受支持版本。

安装

要在 Windows 上使用一体式安装程序安装 ESET PROTECT Web 控制台组件，请执行以下操作：

> 确保满足上面列出的所有安装先决条件。

1. 从 ESET 网站下载 ESET PROTECT 一体式安装程序，然后解压缩该下载文件。

2. 如果要安装最新版本的 Apache Tomcat。但一体式安装程序包含较旧版本的 Apache Tomcat。此步骤可选 – 如果不需要最新版本的 Apache Tomcat。请跳到步骤 4）：

   a.打开 *x64* 文件夹，然后导航到 *installers* 文件夹。

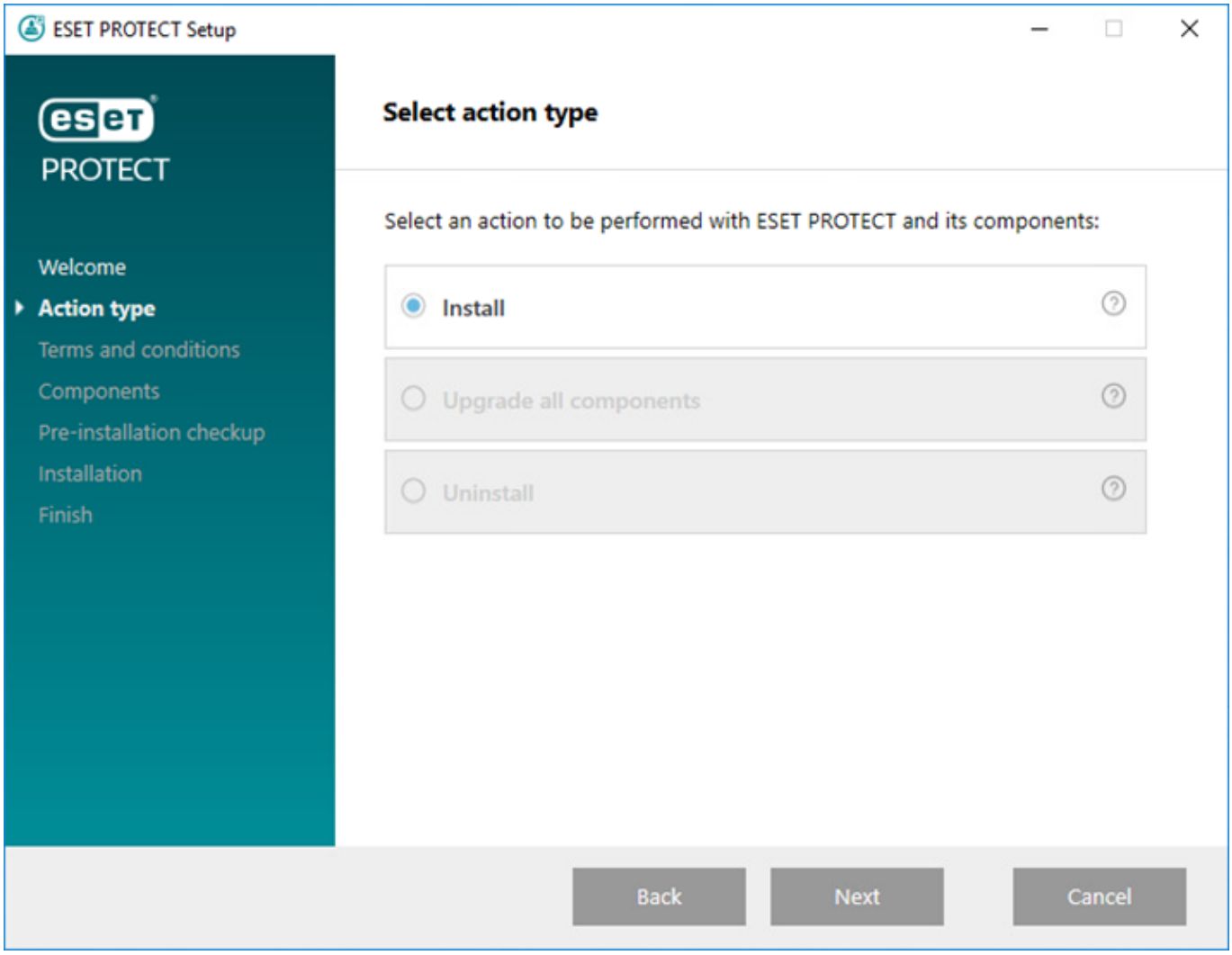
   b.删除位于 *installers* 文件夹中的 *apache-tomcat-9.0.x-windows-x64.zip* 文件.

   c.下载 Apache Tomcat 9 64 位 Windows zip 程序包。

   d.将下载的 zip 程序包移动到 *installers* 文件夹。

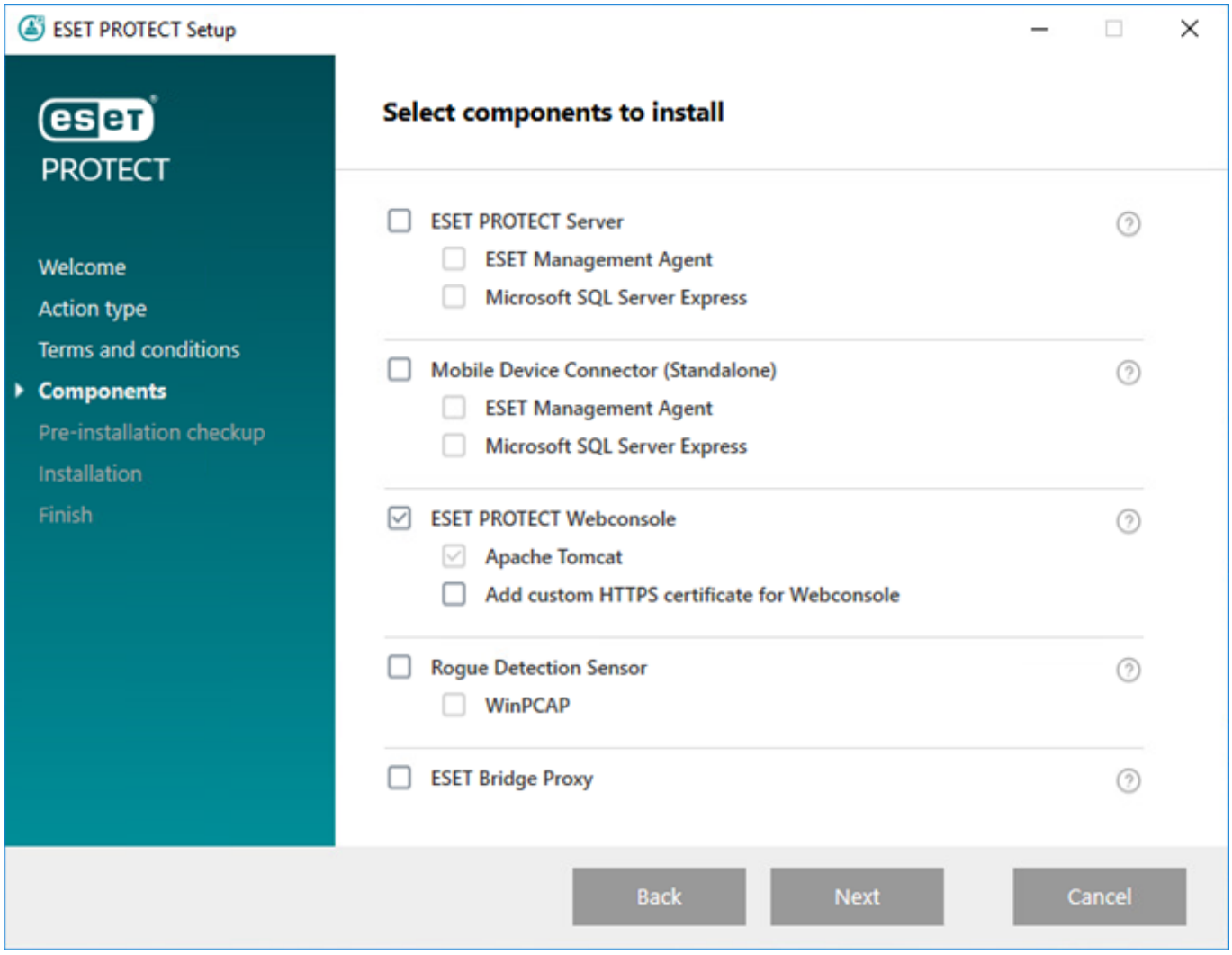
3. 要启动一体式安装程序，请双击 *Setup.exe* 文件，然后在**欢迎**屏幕中单击**下一步**。

4. 选择**安装**，然后单击**下一步**。



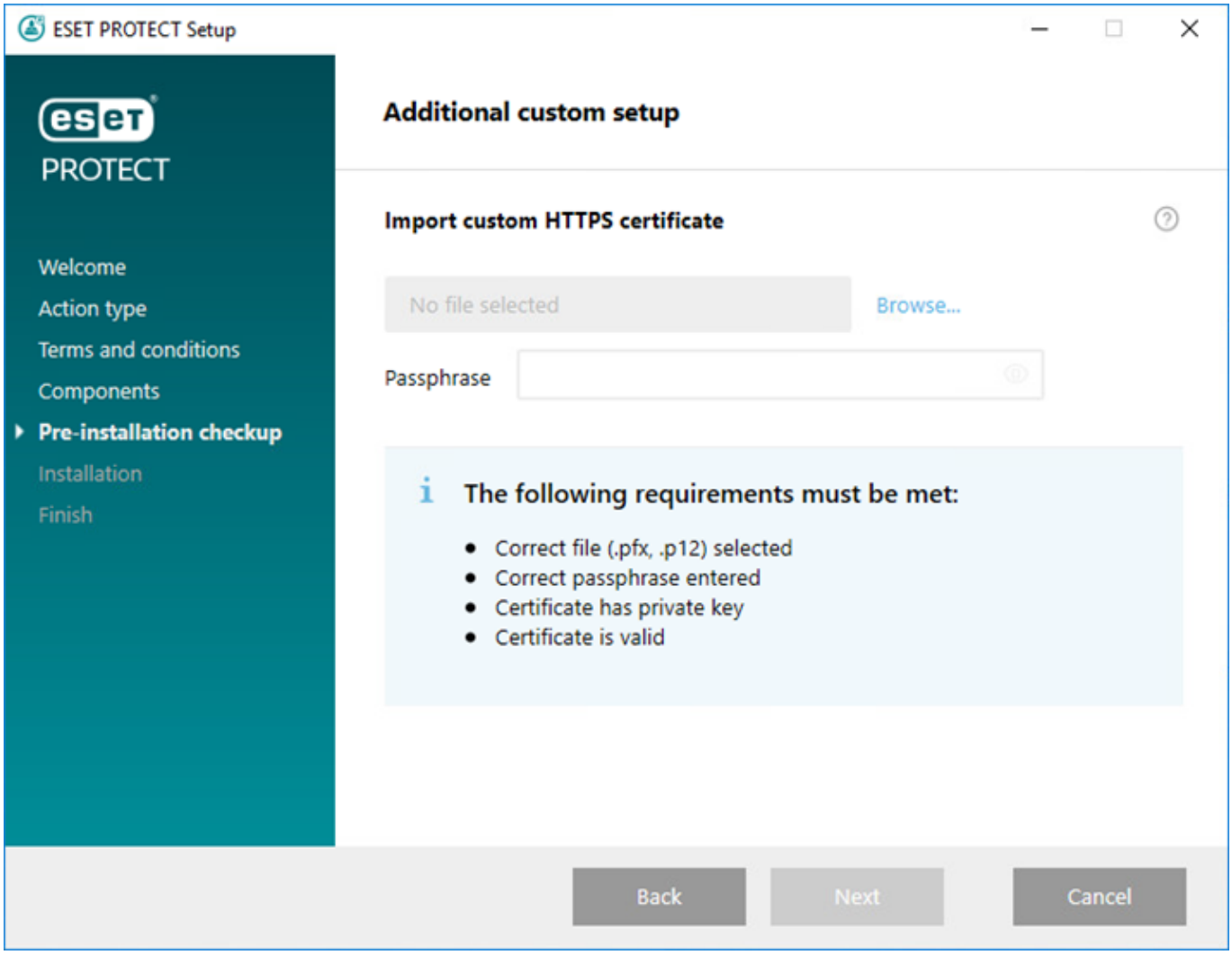
5. 接受 EULA 后，单击**下一步**。

6. 在**选择要安装的组件**中，仅选中 **ESET PROTECT Web 控制台**复选框，然后单击**下一步**。



（可选）选中**添加用于 Web 控制台的自定义 HTTPS 证书**复选框。

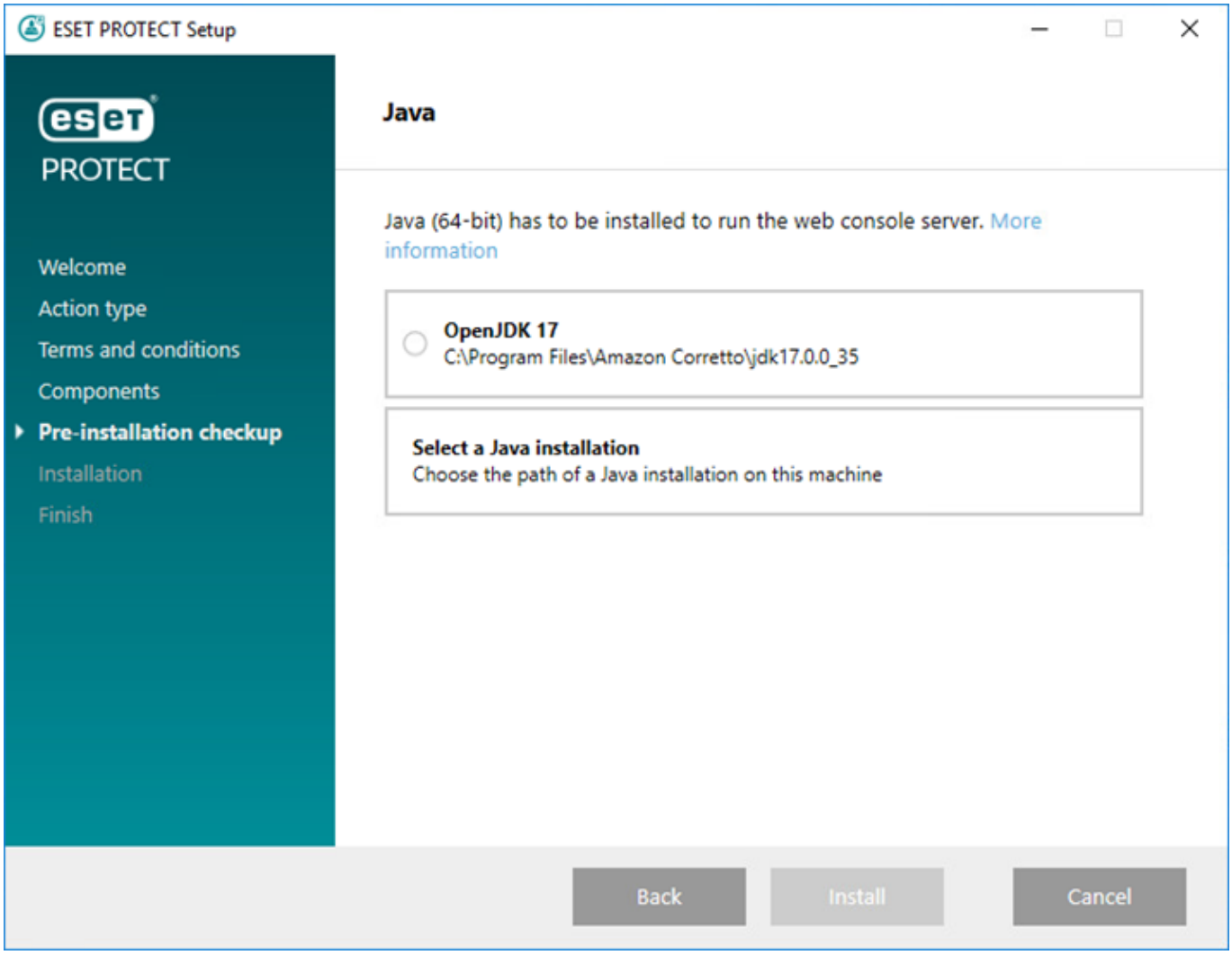
- 如果要将自定义 HTTPS 证书用于 ESET PROTECT Web 控制台，请选择此选项。
- 如果不选择此选项，则安装程序会自动生成一个新的 Tomcat 密钥库（即自签名的 HTTPS 证书）。
- 如果已选择**添加用于 Web 控制台的自定义 HTTPS 证书**，则单击**浏览**并选择有效证书（*.pfx* 或 .p12 文件），然后键入其**密码**（如果没有密码，将该字段留空）。安装程序将在您的 Tomcat 服务器上安装用于 Web 控制台访问的证书。单击**下一步**以继续。



7. 在计算机上选择 Java 安装。确认使用的是最新版本的 Java/OpenJDK。

a)要选择已安装的 Java，请单击**选择 Java 安装**，选择安装有 Java 的文件夹（包含子文件夹 *bin*，例如 *C:\Program Files\Amazon Corretto\jdk1.8.0_212*），然后单击**确定**。如果选择的路径无效，安装程序会提示您。

b)单击**安装**以继续，或单击**更改**以更改 Java 安装路径。



8. 安装完成后，单击**完成**。

如果在 ESET PROTECT 服务器以外的其他计算机上安装了 ESET PROTECT Web 控制台，请执行以下附加步骤以启用 ESET PROTECT Web 控制台与 ESET PROTECT 服务器之间的通信：
a)停用 Apache Tomcat 服务。导航到**启动 > 服务** > 右键单击 Apache Tomcat 服务并选择**停止**。
b)以管理员身份运行“记事本”，然后编辑 *C:\Program Files\Apache Software Foundation\[Tomcat]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties*.
c)查找 `server_address=localhost`。
d)将 `localhost` 替换为您的 ESET PROTECT 服务器的 IP 地址，并保存该文件。
e) 启动 Apache Tomcat 服务：导航到**启动 > 服务** > 右键单击 Apache Tomcat 服务并选择**启动**。

9. 在受支持的 Web 浏览器中打开 ESET PROTECT Web 控制台：将显示一个登录屏幕。

- 从托管 ESET PROTECT Web 控制台的计算机：*https://localhost/era*
- 从可以访问 Internet 的任何计算机访问 ESET PROTECT Web 控制台（将 *IP_ADDRESS_OR_HOSTNAME* 替换为 ESET PROTECT Web 控制台的 IP 地址或主机名）：*https://IP_ADDRESS_OR_HOSTNAME/era*

另请参见企业解决方案的 Web 控制台配置或低性能系统。

手动安装 Web 控制台

手动安装 ESET PROTECT Web 控制台是一个高级步骤。建议您使用一体式安装程序安装 ESET PROTECT Web 控制台。

先决条件

- ESET PROTECT 服务器已安装。

可以在未安装 ESET PROTECT 服务器的其他计算机上安装 ESET PROTECT Web 控制台。 该过程需要其他步骤

- Apache Tomcat 是运行 ESET PROTECT Web Console 所需的必需组件。 安装 Apache Tomcat

  a)从 https://tomcat.apache.org 下载最新支持版本的 Apache Tomcat 安装程序文件（32 位/64 位 Windows Service Installer*apache-tomcat-[版本].exe*

  b)运行该安装程序。

  c)在安装过程中，选择 Java 的路径Java *bin* 和 *lib* 文件夹的父文件夹）并选中 **Run Apache Tomcat** 复选框。

  d)安装完成后，请确保 Apache Tomcat 服务正在运行并且其启动类型设置为**自动**（在 **services.msc** 中）。

- Apache Tomcat 需要 64 位 Java/OpenJDK 如果在系统上安装了多个 Java 版本，建议您卸载较早的 Java 版本并仅保留最新的受支持的 Java 版本。

从 2019 年 1 月开始，面向企业、商业或生产用途的 Oracle JAVA SE 8 公开更新将需要商业许可证。如果不购买 JAVA SE 订阅，可以使用本指南来转换为免费替代方案。请参阅 JDK 的受支持版本

安装

若要在 Windows 上安装 ESET PROTECT Web 控制台组件，请执行以下步骤：

确保满足上面列出的所有安装先决条件。

1. 访问 ESET PROTECT 下载部分，以下载此 ESET PROTECT 组件的独立安装程序 (Web 控制台*era.war*)

2. 将 *era.war* 复制到 Apache Tomcat Web 应用程序文件夹：

C:\Program Files\Apache Software Foundation\[Tomcat 文件夹]\webapps

3. Apache Tomcat 会自动将 *era.war* 文件提取到 *era* 文件夹中，并安装 ESET PROTECT Web 控制台。等待几分钟直到提取完成。如果提取未发生，请遵循故障排除步骤

4. 如果在 ESET PROTECT 服务器所在的同一台计算机上安装了 ESET PROTECT Web 控制台，请重新启动 Apache Tomcat 服务。导航到**启动 > 服务** > 右键单击 Apache Tomcat 服务并选择**停止**。等待 30 秒，然后单击**启动**

如果在 ESET PROTECT 服务器以外的其他计算机上安装了 ESET PROTECT Web 控制台，请执行以下附加步骤以启用 ESET PROTECT Web 控制台与 ESET PROTECT 服务器之间的通信：
a)停用 Apache Tomcat 服务。导航到**启动 > 服务** > 右键单击 Apache Tomcat 服务并选择**停止**。
b)以管理员身份运行“记事本”，然后编辑 *C:\Program Files\Apache Software Foundation\[Tomcat* 文件夹 *]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties.*
c)查找 `server_address=localhost`。
d)将 `localhost` 替换为您的 ESET PROTECT 服务器的 IP 地址，并保存该文件。
e) 启动 Apache Tomcat 服务：导航到**启动 > 服务** > 右键单击 Apache Tomcat 服务并选择**启动**。

5. 在受支持的 Web 浏览器中打开 ESET PROTECT Web 控制台，以访问登录屏幕：

   • 从托管 ESET PROTECT Web 控制台的计算机：*http://localhost:8080/era*

   • 从可以访问 Internet 的任何计算机访问 ESET PROTECT Web 控制台（将 *IP_ADDRESS_OR_HOSTNAME* 替换为 ESET PROTECT Web 控制台的 IP 地址或主机名）：*http://IP_ADDRESS_OR_HOSTNAME:8080/era*

6. 安装完成后配置 Web 控制台：

   • 在 Apache Tomcat 的手动安装过程中，默认 HTTP 端口设置为 8080。 我们建议您设置 Apache Tomcat 的 HTTPS 连接。

   • 另请参见企业解决方案的 Web 控制台配置或低性能系统。

RD Sensor 安装 - Windows

先决条件

- WinPcap – 使用最新的 WinPcap 版本（至少 4.1.0）
- 网络应正确配置（打开相应的端口、防火墙未阻止传入通信等）
- ESET PROTECT 服务器是可访问的。
- ESET Management 服务器代理必须安装在本地计算机上，才能完全支持所有程序功能
- 可以在日志文件中找到 Rogue Detection Sensor 日志文件：*C:\ProgramData\ESET\Rouge Detection Sensor\Logs*

安装

按照下面的步骤在 Windows 上安装 RD Sensor 组件：

确保满足上面列出的所有安装先决条件。

1. 访问 ESET PROTECT 下载部分，以下载此 ESET PROTECT 组件的独立安装程序 （*rdsensor_x86.msi* 或 *rdsensor_x64.msi*）。

2. 双击 RD Sensor 安装程序文件以开始安装。

3. 接受 EULA，然后单击**下一步**。

4. 选中**参与产品改进计划**复选框，以将匿名遥测数据和崩溃报告发送给 ESET。操作系统版本和类型。ESET 产品版本和其他特定于产品的信息）。

5. 选择 RD Sensor 的安装位置，然后依次单击**下一步** > **安装**。

如果有多个网段，则必须在每个网段上单独安装 Rogue Detection Sensor才能生成整个网络上所有设备的全面列表。

镜像工具 - Windows

您是 Linux 用户吗？

镜像工具对脱机检测引擎更新而言不可或缺。如果您的客户端计算机不具有 Internet 连接而需要进行检测引擎更新，您可以使用镜像工具从 ESET 更新服务器下载更新文件，然后将其存储在本地。

镜像工具具有以下功能：
• 模块更新 – 它会下载检测引擎更新和其他程序模块，但不会下载自动更新 (uPCU)。
• 存储库创建 – 它可以创建完整的脱机存储库，包括自动更新 (uPCU)。
镜像工具不会下载 ESET LiveGrid® 数据。

先决条件

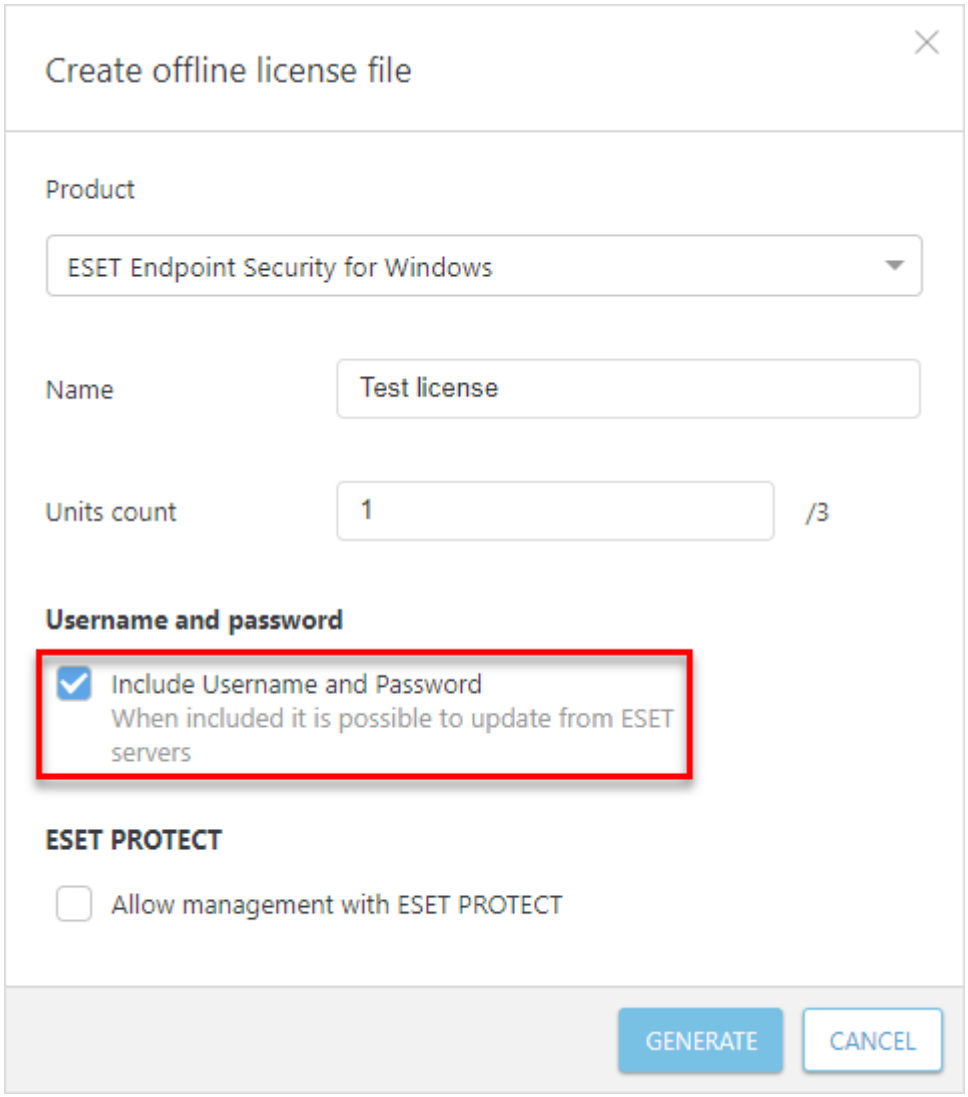
镜像工具不支持 Windows XP 和 Windows Server 2003。

• 目标文件夹必须可供共享（Samba/Windows 或 HTTP/FTP 服务），具体取决于您希望如何访问更新。

o适用于 Windows 的 ESET 安全产品 – 可以使用 HTTP 或共享文件夹远程更新它们。

o适用于 Linux/macOS 的 ESET 安全产品 – 只可以使用 HTTP 远程更新它们。如果使用共享文件夹，该文件夹必须和 ESET 安全产品位于同一计算机上。

• 您必须具有一个包含用户名和密码的有效脱机许可证文件。生成许可证文件时，请务必选中**包括用户名和密码**旁边的复选框。此外，还必须键入许可证**名称**。需要一个脱机许可证文件来激活镜像工具以及生成更新镜像。



- 在运行镜像工具之前，需要安装以下程序包：
- Visual C++ Redistributable for Visual Studio 2010
- Visual C++ 2015 Redistributable x86

如何使用镜像工具

1.从 ESET 下载页（**独立安装程序**部分）下载镜像工具。

2.解压缩下载的压缩文件。

3.打开命令提示，然后导航到内含 *MirrorTool.exe* 文件的文件夹。

4.运行以下命令，以查看镜像工具及其版本的所有可用参数：

```
MirrorTool.exe --help
```

```
C:\Users\                    >MirrorTool.exe --help
Mirror Tool v1.0.1294.0, Copyright (c) ESET, spol. s r.o. 1992-2021. All rights
reserved.
Allowed options:
  --mirrorType arg                      [required for module update]
                                        Type of mirror. Possible values (case
                                        insensitive): regular, pre-release,
                                        delayed.
  --intermediateUpdateDirectory arg     [required for module update]
                                        Files will be downloaded to this
                                        directory to create mirror in output
                                        directory.
  --offlineLicenseFilename arg          [required for module update]
                                        Offline license file.
  --updateServer arg                    [optional]
                                        Update server. (e.g.:
                                        http://update.eset.com/eset_upd/ep6/)
                                        Mirror will be created in output
                                        directory, only specified path in
                                        server will be mirrored.
  --outputDirectory arg                 [required for module update]
                                        Directory where mirror will be created.
  --proxyHost arg                       [optional]
                                        Http proxy address (fqdn or IP).
  --proxyPort arg                       [optional]
                                        Http proxy port.
  --proxyUsername arg                   [optional]
                                        Http proxy username.
  --proxyPassword arg                   [optional]
                                        Http proxy password.
  --networkDriveUsername arg            [optional]
                                        Username used, when output directory is
                                        accessed using smb(e.g:\\hostname).
  --networkDrivePassword arg            [optional]
                                        Password used, when output directory is
                                        accessed using smb(e.g:\\hostname).
  --excludedProducts arg                [optional]
                                        Disable creating mirror for specified
                                        products. Use --listUpdatableProducts
                                        to see possible values.
  --listUpdatableProducts               Show list of all products which modules
                                        are downloaded by default.
  --repositoryServer arg                [required for repository update]
                                        Repository server for repository
                                        creation.
  --intermediateRepositoryDirectory arg [required for repository update]
                                        Files will be downloaded to this
                                        directory to create offline mirror in
                                        output directory.
  --outputRepositoryDirectory arg       [required for repository update]
                                        Directory where offline repository will
                                        be created.
  --trustDownloadedFilesInRepositoryTemp
                                        [optional]
                                        If set, hashes on already downloaded
                                        files are not checked.
  --mirrorOnlyLevelUpdates              [optional]
                                        If set, only level upgrades will be
                                        downloaded (nano/continuous updates
                                        will not be downloaded)
  --mirrorFileFormat arg                [optional]
                                        Specifies which type of update files
                                        will be downloaded. Possible values
                                        (case insensitive): dll, dat.
  --compatibilityVersion arg            [optional]
                                        Version of compatible products.
  --filterFilePath arg                  [optional]
                                        Path to filter file in json format.
                                        Parameter compatibilityVersion has to
                                        be higher than 7.1.0.0 to run program.
  --dryRun arg                          [optional]
                                        Specifies dry run of program with path
                                        to csv file where will be saved list of
                                        products to be downloaded with current
                                        filter configuration.
  --help                                [optional]
                                        Display this help and exit
```

所有过滤器均区分大小写。

可以使用参数来创建存储库镜像或模块镜像：

存储库和模块镜像的参数

--proxyHost
--proxyPort
--proxyUsername
--proxyPassword
--help

存储库特定参数

--repositoryServer
--intermediateRepositoryDirectory
--outputRepositoryDirectory
--compatibilityVersion
--dryRun
--filterFilePath
--trustDownloadedFilesInRepositoryTemp

模块特定参数

--mirrorType
--intermediateUpdateDirectory
--offlineLicenseFilename
--updateServer
--outputDirectory
--networkDriveUsername
--networkDrivePassword
--excludedProducts
--listUpdatableProducts
--mirrorOnlyLevelUpdates
--mirrorFileFormat

参数	说明
--updateServer	Mirror Tool 创建的文件夹结构不同于 Endpoint 镜像创建的文件夹结构。每个文件夹都包含一组产品的更新文件。 必须在使用镜像的产品的更新设置中，指定更新服务器完整链接（即正确文件夹的完整路径）。
--offlineLicenseFilename	您必须指定指向您的脱机许可证文件的路径（如上所述）。

参数	说明
--mirrorOnlyLevelUpdates	不需要参数。如果已设置，则仅下载级别更新（不会下载微量更新）。在我们的知识库文章中阅读有关更新类型的详细信息。
--mirrorFileFormat	⚠ 在使用 --mirrorFileFormat 参数前，确保您的环境不包含更低（6.5 及更低版本）和更高（6.6. 及更高版本）ESET 安全产品版本。此参数的错误使用可能导致 ESET 安全产品的错误更新。 可以指定下载哪种类型的更新文件。可能的值（区分大小写）： • dat – 如果您的环境仅有 ESET 安全产品版本 6.5 及更低版本，则使用此值。 • dll – 如果您的环境仅有 ESET 安全产品版本 6.6 及更高版本，则使用此值。 当创建旧产品（ep4、ep5）的镜像时，忽略此参数。
--compatibilityVersion	此可选参数适用于随 ESET PROTECT 8.1 及更高版本一起分发的镜像工具。镜像工具将下载与您在参数自变量中以格式 x.x 或 x.x.x.x 指定的 ESET PROTECT 存储库版本兼容的更新文件，例如：--compatibilityVersion 10.0 或 --compatibilityVersion 8.1.13.0。 --compatibilityVersion 参数将从镜像中排除自动更新 (uPCU)。如果您需要环境中存在自动更新（uPCU）并希望减小镜像大小，请使用 --filterFilePath 参数。

i 要减少从 ESET 存储库下载的数据量，建议您在随 ESET PROTECT 9 一起分发的镜像工具中使用新参数：--filterFilePath 和 --dryRun。
1.采用 *JSON* 格式创建过滤器（参见下面的 --filterFilePath）。
2.执行使用 --dryRun 参数运行镜像工具的测试（参见下文），并根据需要调整过滤器。
3.使用 --filterFilePath 参数和定义的下载过滤器，以及 --intermediateRepositoryDirectory 和 --outputRepositoryDirectory 参数运行镜像工具。
4.定期运行镜像工具，以始终使用最新的安装程序。

参数	说明

--filterFilePath	使用此可选参数以根据与镜像工具位于同一文件夹中的 *JSON* 格式文本文件过滤 ESET 安全产品，例如：--filterFilePath filter.txt
	过滤器配置说明：
	产品过滤的配置文件格式为 *JSON*，其结构如下所示：
	• 根 *JSON* 对象：
	o use_legacy（布尔值，可选）– 如果为 true 则将包含旧产品。
	o defaults（*JSON* 对象，可选）– 定义将应用于所有产品的过滤器属性。
	■ languages（代码）– 指定要包含语言的 ISO 语言代码，例如法语类型为 "fr_FR"。其他语言代码在下表中。要选择多个语言，请使用逗号和空格分隔它们，例如：(["en_US", "zh_TW", "de_DE"])
	■ platforms（列表）– 要包括的平台 (["x64", "x86", "arm64"])
	⚠ 请谨慎使用 platforms 过滤器。例如，如果镜像工具仅下载 64 位安装程序并且您的基础架构中有 32 位计算机，则 64 位 ESET 安全产品将无法在 32 位计算机上安装。
	■ os_types（列表）– 要包括的操作系统类型（["windows"]["linux"]["mac"]）
	o products（JSON 对象的列表，可选）– 要应用于特定产品的过滤器 – 覆盖特定产品的 defaults。对象具有以下属性：
	■ app_id（字符串）– 如果 name 未指定，则该项为必填项。
	■ name（字符串）– 如果 app_id 未指定，则该项为必填项。
	■ version（字符串）– 指定要包含的版本或版本范围。
	■ languages（列表）– 要包含语言的 ISO 语言代码（参见下表）
	■ platforms（列表）– 要包括的平台 (["x64", "x86", "arm64"])
	■ os_types（列表）– 要包括的操作系统类型（["windows"]["linux"]["mac"]）
	ℹ 要确定各字段的合适值，请在试运行模式下运行镜像工具，并在创建的 CSV 文件中找到相关产品。
	版本字符串格式说明
	所有版本号均由四个以点分隔的数字组成（例如，7.1.0.0）。可以在填写版本过滤器时指定较少数字（例如，7.1），其余数字将为零（7.1 等同于 7.1.0.0）
	版本字符串可以采用以下两种格式之一：
	• [>|<|>=|<=|=]<n>.(<n>.(<n>.(<n>)))
	o 选择大于/小于或等于/小于或等于/等于指定版本的版本。
	• <n>.(<n>.(<n>.(<n>))) - <n>.(<n>.(<n>.(<n>)))
	o 选择大于或等于下限且小于或等于上限的版本。
	从左到右对版本号的每个部分进行数字比较。
	JSON 示例
	{
	"use_legacy": true,
	"defaults": {
	"languages": ["en_US"],
	"platforms": ["x64", "x86"]
	},
	"products": [
	{
	"app_id": "com.eset.apps.business.ees.windows",
	"version": "7.1.0.0–8.0.0.0"
	},
	{
	"app_id": "com.eset.apps.business.eea.windows",
	"version": ">7.1.0.0"
	}
	]
	}
	--filterFilePath 参数将替换较旧镜像工具版本（随 ESET PROTECT 8.x 一起发布）中使用的 --[illegible] 参数。

--dryRun	当使用此可选参数时，镜像工具不会下载任何文件，但它会生成一个 *.csv* 文件（其中列出将要下载的所有程序包）。 可以在不带强制参数 --intermediateRepositoryDirectory 和 --outputRepositoryDirectory 的情况下使用此参数，例如： • Windows：MirrorTool.exe --repositoryServer AUTOSELECT --dryRun test.csv • Linux：sudo ./MirrorTool --repositoryServer AUTOSELECT --dryRun test.csv ℹ 某些 ESET 安装程序是通用于语言的（语言代码为 multilang），即使在 --filterFilePath 中指定了语言，镜像工具也会将它们列在 *.csv* 文件中。 如果使用 --dryRun 参数以及 --intermediateRepositoryDirectory 和 --outputRepositoryDirectory 参数，镜像工具不会清除 *outputRepositoryDirectory*。
--listUpdatableProducts	列出 Mirror Tool 可以为其下载模块更新的所有 ESET 产品（除非使用了 --excludedProducts） 从版本 Mirror Tool 开始提供该参数：1.0.1294.0 (Windows)；1.0.2226.0 (Linux)。

Mirror Tool 文件夹结构

默认情况下，如果不指定 --updateServer 参数，则 Mirror Tool 会在 HTTP 服务器上创建此文件夹结构：

请勿使用仅采用 HTTP 的镜像服务器

确保本地镜像服务器使用 HTTP 和 HTTPS 协议，或仅使用 HTTPS。如果镜像服务器仅使用 HTTP，则无法使用“软件安装”客户端任务，因为无法从 HTTP 服务器检索 ESET 安全产品的最终用户许可协议。

Mirror Tool 默认文件夹	ESET 安全产品	更新服务器（根据 HTTP 服务器根位置）
mirror/eset_upd/era6	*era6* 镜像文件夹对于这些 ESET 远程管理解决方案是通用的：ERA 6、ESMC 7 和 ESET PROTECT。	要从镜像更新 ESET PROTECT 10，请将更新服务器设置为 *http://your_server_address/mirror/eset_upd/era6*
mirror/eset_upd/ep[版本]	适用于 Windows 的 ESET Endpoint Antivirus/Security 版本 6.x（及更高版本）。每个主版本都有其文件夹，例如 *ep10* 对应于版本 10.x。	*http://your_server_address/mirror/eset_upd/ep10*（对应于版本 10.x 的示例）
mirror/eset_upd/v5	适用于 Windows 的 ESET Endpoint Antivirus/Security 版本 5.x	*http://your_server_address/mirror/eset_upd/v5*

ESET 安全产品策略 Linux/macOS

必须指定 `--updateServer` 参数并创建其他文件夹，才能从 HTTP 镜像更新适用于 Linux/macOS 的 ESET 安全产品（见下文）。

--updateServer	其他 Mirror Tool 文件夹	ESET 安全产品	更新服务器（根据 HTTP 服务器根位置）
http://update.eset.com/eset_upd/businesslinux	*mirror/eset_upd/*BusinessLinux	ESET Endpoint Antivirus 对于 Linux	*http://your_server_address/mirror/eset_upd/BusinessLinux*
http://update.eset.com/eset_upd/serverlinux	*mirror/eset_upd/*LinuxServer	ESET Server Security 对于 Linux	*http://your_server_address/mirror/eset_upd/LinuxServer*
http://update.eset.com/eset_upd/businessmac	*mirror/eset_upd/*BusinessMac	适用于 macOS 的 ESET Endpoint Security 版本 7.x+	*http://your_server_address/mirror/eset_upd/BusinessMac*

[语言代码表](#)



```
MirrorTool.exe --mirrorType regular ^
--intermediateUpdateDirectory c:\temp\mirrorTemp ^
--offlineLicenseFilename c:\temp\offline.lf ^
--outputDirectory c:\temp\mirror
```

以下是内含所选产品、语言和已启用旧文件下载功能（在 *filter.txt* 文件中定义）的脱机存储库的更高级配

置示例（请参阅上述 `--filterFilePath` 详细信息中的文件内容示例）：

```
MirrorTool.exe --repositoryServer AUTOSELECT ^
--intermediateRepositoryDirectory c:\temp\repoTemp ^
--outputRepositoryDirectory c:\temp\repository ^
--filterFilePath filter.txt
```

镜像工具和更新设置

- 若要自动下载模块更新，可以创建一个运行镜像工具的计划。若要执行此操作，请打开 Web 控制台并导航至**客户端任务 > 操作系统 > 运行命令。选择要运行的命令行**（包括指向 *MirrorTool.exe* 的路径）和合理的触发器（如每小时都执行 CRON 0 0 * * * ?*您也可以使用 Windows 任务计划程序或 Linux 中的 Cron

- 若要在客户端计算机上配置更新，请创建新策略并将**更新服务器**配置为指向您的镜像地址或共享文件夹。

如果您使用 HTTPS 镜像服务器，则需要将其证书导入到客户端计算机上受信任的根存储中。请参见 Windows 上的安装受信任的根证书

请参阅本知识库文章以设置镜像工具链（配置镜像工具为从其他镜像工具下载更新）。

移动设备连接器安装 - Windows

ESET PROTECT 移动设备管理/连接器 (MDM/MDC) 组件（仅限本地）计划结束生命周期。阅读更多建议您迁移到 Cloud MDM

移动设备连接器必须可通过 Internet 进行访问，以便可以随时随地管理该移动设备。

建议您将 MDM 组件部署在独立于托管 ESET PROTECT 服务器的其他主机设备上。

按照下面的步骤在 Windows 上为 ESET PROTECT 服务器安装 Mobile Device Connector 组件：

确保满足所有安装先决条件

1. 访问 ESET PROTECT 下载部分，以下载此 ESET PROTECT 组件的独立安装程序（*mdmcore_x64.msi*）.

2. 运行移动设备连接器安装程序并接受 EULA如果您同意）。

3. 单击**浏览**，导航到您的 SSL 证书的位置以通过 HTTPS 进行通信，然后键入此证书的密码。

4. 指定 **MDM 主机名**：由于移动设备可以通过 Internet 访问该主机名，因此这是您的 MDM 服务器的公共域或公共 IP 地址。

必须输入 **HTTPS 服务器证书**中指定的相同形式的 MDM 主机名，否则 iOS 移动设备会拒绝安装 MDM 配置文件。例如，如果 HTTPS 证书中存在一个指定的 IP 地址，请将此 IP 地址键入 **MDM 主机名**字段。在已在 HTTPS 证书中指定了 FQDN例如，`mdm.mycompany.com`）的情况下，请在 **MDM 主机名**字段中输入此 FQDN此外，如果在 HTTPS 证书中使用了通配符 `*`（例如，`*.mycompany.com`），则可以在 **MDM 主机名**字段中使用 `mdm.mycompany.com`

5. 安装程序现在需要连接到供移动设备连接器使用的现有数据库。指定以下连接详细信息：

- **数据库**MySQL Server/MS SQL Server/通过 Windows 身份验证的 MS SQL Server
- **ODBC 驱动程序**MySQL ODBC 5.1 Driver/MySQL ODBC 5.2 Unicode Driver/MySQL ODBC 5.3 Unicode Driver/MySQL ODBC 8.0 Unicode Driver/SQL Server/SQL Server Native Client 10.0/ODBC Driver 11 for SQL Server/ODBC Driver 13 for SQL Server/ODBC Driver 17 for SQL Server/ODBC Driver 18 for SQL Server
- **数据库名称**：建议您使用预定义的名称或更改它（如果需要）。
- **主机名**：数据库服务器的主机名或 IP 地址
- **端口**： 用于连接到数据库服务器
- 数据库管理员帐户**用户名/密码**
- **使用命名实例** – 如果您使用的是 Microsoft SQL 数据库，您还可以选中**使用命名实例**复选框以使用自定义数据库实例。您可以在**主机名**字段中使用 *HOSTNAME\DB_INSTANCE* 格式（例如，*192.168.0.10\ESMC7SQL*）设置它。对于群集数据库，仅使用群集名称。如果选中此选项，则无法更改数据库连接端口 – 系统将使用由 Microsoft 确定的默认端口。若要将 ESET PROTECT 服务器连接到故障转移群集中安装的 Microsoft SQL 数据库，请在**主机名**字段中输入群集名称。

可以使用用于 ESET PROTECT 数据库的相同数据库服务器，但如果您计划注册 80 多个移动设备，建议您使用不同的数据库服务器。

6. 为新创建的移动设备连接器数据库指定用户。您可以**创建新用户**或**使用现有数据库用户**。键入数据库用户的密码。

7. 输入**服务器主机**（您的 ESET PROTECT 的名称或 IP 地址）和**服务器端口**（默认端口为 2222，如果要使用其他端口，则将该默认端口替换为您的自定义端口号）。

8. 将 MDM 连接器连接到 ESET PROTECT 服务器。填写连接到 ESET PROTECT 服务器所需的**服务器主机**和**服务器端口**，然后选择**服务器辅助安装**或**脱机安装**以继续：

- **服务器辅助安装** – 提供 ESET PROTECT Web 控制台管理员凭据，安装程序将自动下载所需证书。还要检查服务器辅助安装所需的权限

  1.输入**服务器主机** – 您的 ESET PROTECT 服务器的名称或 IP 地址和 **Web 控制台端口**（如果不使用自定义端口，则保留使用默认端口 2223）。此外，提供 Web 控制台管理员帐户凭据 – **用户名/密码**

  2.当询问您是否接受证书时，单击**是**。继续进行步骤 10。

- **脱机安装** – 提供**代理证书**和**证书颁发机构**（可从 ESET PROTECT 中导出）。此外，可以使用自定义证书和适合的证书颁发机构。

  1.单击对等证书旁边的**浏览**，然后导航到**对等证书**（这是从 ESET PROTECT 中导出的代理证书）的位置。使**证书密码**文本字段保留为空，因为此证书不需要密码。

2.为证书颁发机构重复此步骤，然后继续进行步骤 10。

如果要使用 ESET PROTECT 的自定义证书（而不是在 ESET PROTECT 安装过程中自动生成的默认证书），则在系统提示您提供代理证书时，应使用这些自定义证书。

9. 指定移动设备连接器的目标文件夹（建议使用默认目标文件夹）、单击**下一步**，然后单击**安装**。

10. 在完成安装后，通过在 Web 浏览器中或从移动设备打开 *https://your-mdm-hostname:enrollment-port*（例如 *https://mdm.company.com:9980*）来检查 Mobile Device Connector 是否正常运行。如果已成功安装，您将看到以下消息：MDM 服务器启动并运行！

11. 现在您可以从 ESET PROTECT 激活 MDM。

移动设备连接器先决条件

如果更改了 MDM 服务器的端口或主机名，则必须重新注册所有移动设备。因此，建议您为 MDM 服务器设置专用主机名，以便在需要更改 MDM 服务器的主机设备时，可以通过在 DNS 设置中将新主机设备的 IP 地址重新分配给 MDM 主机名来实现。

必须满足以下先决条件，才能在 Windows 上安装移动设备连接器：

- 可通过 Internet 访问的公共 IP 地址/主机名或公共域。

如果需要更改 MDM 服务器的主机名，将需要运行 MDC 组件的修复安装。如果更改 MDM 服务器的主机名，需要导入包含此新主机名的新 **HTTPS 服务器证书**，才能使 MDM 继续正常工作。

- 端口已打开并且可用，请在此处查看端口的完整列表。建议使用默认端口号 9981 和 9980，但也可以在 MDM 服务器的配置文件中更改这些端口号（如果需要）。确保移动设备可以通过指定的端口进行连接。更改您的防火墙和/或网络设置（如果适用）以使此操作可行。阅读有关 MDM 体系结构的更多信息。

- 防火墙设置 – 当在非服务器操作系统（例如 Windows 7）上安装移动设备连接器（仅用于评估目的）时，请确保通过创建以下适用防火墙规则允许通信端口：

C:\Program Files\ESET\RemoteAdministrator\MDMCore\ERAMDMCore.exe, TCP port 9980

C:\Program Files\ESET\RemoteAdministrator\MDMCore\ERAMDMCore.exe, TCP port 9981

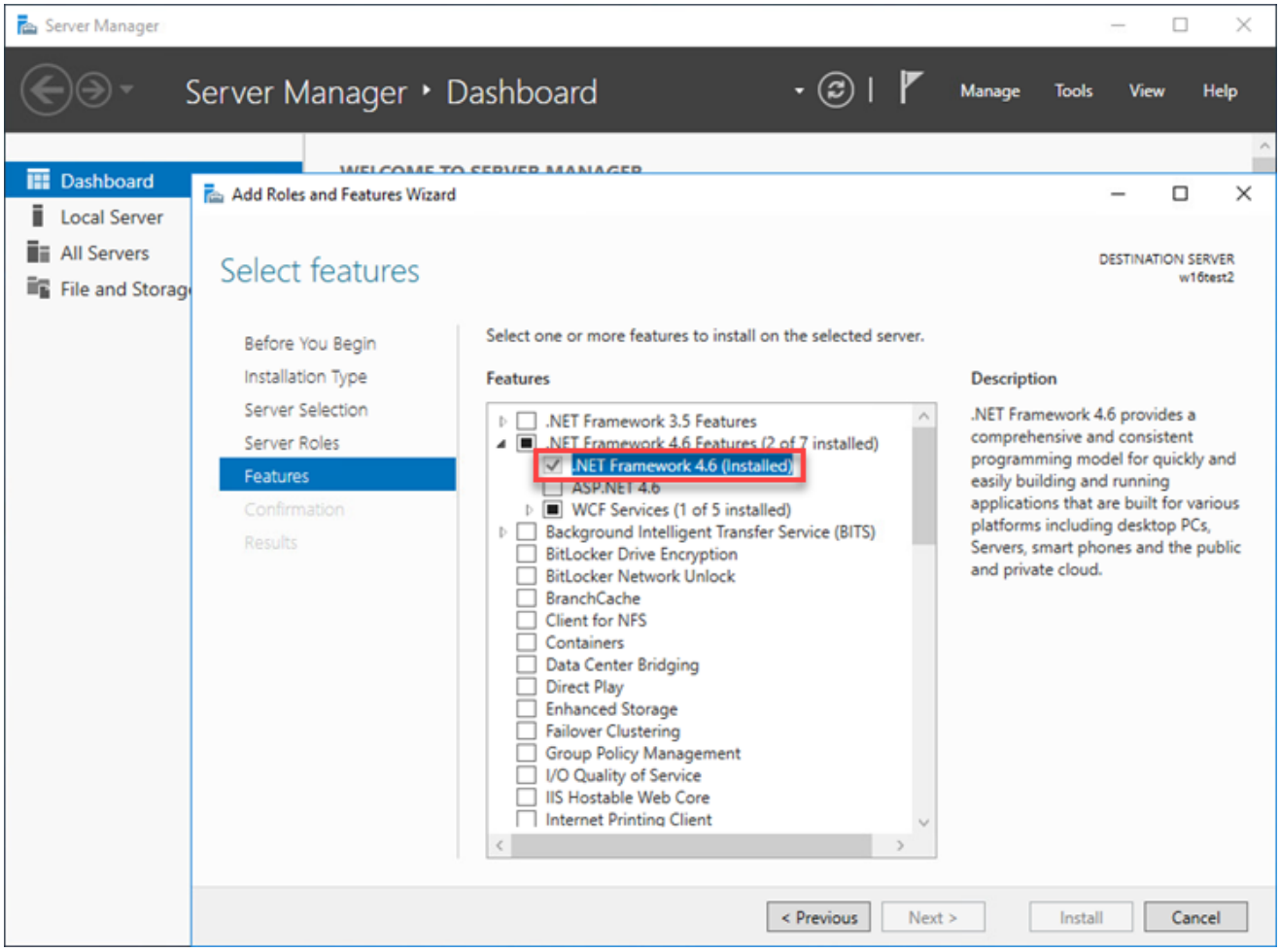
C:\Program Files\ESET\RemoteAdministrator\Server\ERAServer.exe, TCP port 2222

.exe 文件的实际路径可能不同，具体取决于每个 ESET PROTECT 组件在客户端操作系统上的安装位置。

- 数据库服务器已安装并已配置。确保满足 Microsoft SQL 或 MySQL 要求。

- 已针对 MDM 连接器的 RAM 使用进行了优化，以便支持并发运行最多 48 个“ESET PROTECT MDMCore 模块”进程；如果用户连接更多设备，那么这些进程会针对当前需要使用资源的每个设备进行周期改变。

- Microsoft SQL Server Express 安装需要 Microsoft .NET Framework 4。您可以使用**添加角色和功能向导**安装它：



证书要求

• 若要通过 HTTPS 安全地进行通信，需要采用 *.pfx*格式的 **SSL 证书**。建议您使用由第三方证书颁发机构提供的证书。不建议使用自签名证书（包括由 ESET PROTECT CA 签名的证书），因为并非所有移动设备都允许用户接受自签名证书。

• 需要具有 CA 签名的证书和相应私钥，然后利用标准步骤（通常使用 OpenSSL）将上述内容合并到一个 *.pfx* 文件中：

```
openssl pkcs12 -export -in certificate.cer -inkey privateKey.key -out
httpsCredentials.pfx
```

这是适用于大多数使用 SSL 证书的服务器的标准步骤。

• 对于脱机安装，您还需要对等证书（从 ESET PROTECT 中导出的**服务器代理证书**）。此外，您可以使用 ESET PROTECT 的自定义证书。

移动设备连接器激活

在安装移动设备连接器之后，需要使用 ESET 端点、业务或办公室许可证来进行激活：

1.添加 ESET 端点、业务或办公室许可证到 ESET PROTECT 许可证管理。

2.使用产品激活客户端任务激活 Mobile Device Connector。该步骤与在客户端计算机上激活任何 ESET 产品一样 – 在此情况下，移动设备连接器即为客户端计算机。

MDM iOS 许可功能

由于 ESET 未通过 Apple App Store 提供应用程序，因此 ESET 移动设备连接器存储 iOS 设备的许可详细信息。

许可证按设备分配，并且可以使用产品激活任务进行激活（与 Android 一样）。

可以通过以下方式停用 iOS 许可证：

- 通过停止管理任务删除所管理的设备
- 通过**删除数据库**选项卸载 MDC
- 通过其他方式停用ESET PROTECT 或 EBA 停用

因为 MDC 代表 iOS 设备与 ESET 许可服务器进行通信，所以 EBA 门户反映的是 MDC 的状态而不是个别设备的状态。当前设备信息在 ESET PROTECT Web 控制台中始终可用。

未激活的设备或许可证已过期的设备将显示红色防护状态及“产品未激活”消息。这些设备将拒绝处理任务、设置策略和提供非关键日志。

在卸载 MDM 期间，如果选择**不删除数据库**，则不会停用已使用的许可证。如果在此数据库上重新安装 MDM通过 ESET PROTECT 删除或者由 EBA 停用删除，则可以重新使用这些许可证。当迁移到另一台 MDM 服务器时，需要再次执行产品激活任务

HTTPS 证书要求

若要在 ESET 移动设备连接器中注册移动设备，请确保 HTTPS 服务器返回完整证书链。

为使证书正常工作，必须满足以下要求：

- HTTPS 证书pkcs#12/pfx 容器）必须包含完整证书链，包括根 CA
- 该证书必须在需求时间段（有效起始日期/有效截止日期）内有效。
- **CommonName** 或 **subjectAltName** 必须匹配 MDM 主机名。

例如，如果 **MDM 主机名**为 hostname.mdm.domain.com您的证书可以包含如下所示的名称：
- hostname.mdm.domain.com
- *.mdm.domain.com

但不可以包含的名称如下：
- *
- *.com
- *.domain.com

通常，“ * ”不能用于代替“点”。此行为针对 iOS 接受 MDM 证书的方式进行确认。

请注意，某些设备在检查证书有效性时会考虑其当前时区，而其他设备则不会。通过在当前日期之前一两天提供证书有效性，可避免出现潜在问题。

脱机存储库 - Windows

可以使用镜像工具创建脱机存储库（在 Windows 上）。通常，这正是封闭式计算机网络或 Internet 访问受限的网络所需要的。镜像工具可用于在本地文件夹中创建ESET存储库的克隆。之后可以将这一克隆的存储库（例如，外部磁盘上的存储库）移动到封闭式网络中的某个位置。可以将该存储库复制到本地网络中的安全位置，然后通过 HTTP 服务器使其可用。

若要更新脱机存储库，请使用创建脱机存储库所用的相同命令。将使用中间文件夹中的先前数据并仅下载过时的文件。

请注意，存储库的大小不断增长，中间目录具有相同的大小。在开始该过程之前，请确保至少具有 **1.2 TB** 的可用空间。

最佳做法

另请参阅 ESET 知识库文章脱机环境中使用 ESET PROTECT 的最佳实践

适用于 Windows 的示例方案

I. 创建存储库克隆

1. 下载镜像工具。
2. 从已下载的 *.zip* 文件中提取镜像工具。
3. 为以下对象准备（创建）文件夹：
   - 中间文件
   - 最终存储库
4. 打开命令提示符，然后将目录更改为已提取的镜像工具所在的文件夹（`cd` 命令）。
5. 运行以下命令（将中间存储库和输出存储库目录更改为步骤 3 中的文件夹）：

```
MirrorTool.exe --repositoryServer AUTOSELECT ^
--intermediateRepositoryDirectory C:\Intermediary ^
--outputRepositoryDirectory C:\Repository
```

6. 存储库已复制到 `outputRepositoryDirectory` 文件夹后，将该文件夹及其内容移动到可访问您的封闭式网络的另一台计算机。

II. 设置 HTTP 服务器

7. 需要在封闭式网络中的计算机上运行 HTTP 服务器。您可以使用：
   - ESET 下载站点中的 Apache HTTP Proxy此方案）
   - 其他 HTTP 服务器

8. 打开 *apachehttp.zip* 并将文件提取到 *C:\Program Files\Apache HTTP Proxy*

9. 打开管理命令提示符，然后将目录更改为 *C:\Program Files\Apache HTTP Proxy\bin*（`cd` 命令）。

10. 执行以下命令：

```
httpd.exe -k install -n ApacheHttpProxy
```

11. 使用简单文本编辑器打开 *C:\Program Files\Apache HTTP Proxy\conf\httpd.conf* 文件，并在该文件末尾添加以下行：

```
Listen 80
ServerRoot "C:\Program Files\Apache HTTP Proxy"
DocumentRoot "C:\Program Files\Apache HTTP Proxy\htdocs"
<Directory "C:\Program Files\Apache HTTP Proxy\htdocs">
Options Indexes FollowSymLinks
AllowOverride None
Require all granted
</Directory>
CacheRoot "C:\Program Files\Apache HTTP Proxy\cache"
```

12. 使用以下命令启动 **ApacheHttpProxy** 服务：

```
sc start ApacheHttpProxy
```

13. 通过以下方式测试服务是否正在运行：在 Web 浏览器中打开 *http://YourIPaddress:80/index.html*（将 *YourIPaddress* 替换为您计算机的 IP 地址）。

III. 运行脱机存储库

14. 为脱机存储库创建新文件夹，例如 *C:\Repository.*

15. 在 *httpd.conf* 文件中，将以下行

```
DocumentRoot "C:\Program Files\Apache HTTP Proxy\htdocs"
<Directory "C:\Program Files\Apache HTTP Proxy\htdocs">
```

替换为存储库文件夹的地址，如下所示：

```
DocumentRoot "C:\Repository"
<Directory "C:\Repository">
```

16. 将已下载的存储库复制到 *C:\Repository*.

17. 使用以下命令重新启动 **ApacheHttpProxy** 服务：

```
sc restart ApacheHttpProxy
```

18. 现在，您的脱机存储库已在地址 *http://YourIPaddress*（例如，*http://10.1.1.10*）上运行。

19. 使用 ESET PROTECT Web 控制台设置新的存储库地址：

a.ESET PROTECT 服务器 – 依次单击**更多 > 设置 > 高级设置 > 库**，然后在**服务器**字段中输入脱机库地址。

b.ESET Management 服务器代理 – 单击**策略**，再单击服务器代理策略 > **编辑 > 设置 > 高级设置 > 库**，然后在**服务器**字段中输入脱机库地址。

c.ESET Endpoint 产品（适用于 Windows）- 单击**策略**，再单击 **ESET Endpoint for Windows** 策略 > **编辑 > 设置 >更新 > 配置文件 > 更新 > 模块更新**，取消选择**自动选择**，然后在**自定义服务器**字段中输入脱机库地址。

故障转移群集 - Windows

下面是在故障转移群集环境中安装 ESET PROTECT 所需的高级步骤。

有关 ESET PROTECT 服务器的群集安装，另请参阅知识库文章

1. 创建带有共享磁盘的故障转移群集：

- 在 Windows Server 2016 和 2019 中创建故障转移群集的说明
- 在 Windows Server 2012 和 2012 R2 中创建故障转移群集的说明

2. 在**创建群集向导**中输入所需主机名（编写主机名）和 IP 地址。

3. 在 node1 上，在线创建群集的共享磁盘并使用独立安装程序安装 ESET PROTECT 服务器。确保安装期间选择了**这是群集安装**并选择共享磁盘作为应用程序数据存储。编写并输入预先填写的主机名旁的 ESET PROTECT Server 的服务器证书的主机名。记住此主机名，在步骤 6 中（即在群集管理器中创建 ESET PROTECT 服务器角色时）会用到它。

4. 停用 node1 上的 ESET PROTECT Server在 node2 上，在线创建群集的共享磁盘并使用独立安装程序安装 ESET PROTECT 服务器。确保安装期间选择了**这是群集安装**。选择共享磁盘作为应用程序数据存储。原封不动地保留数据库连接和证书信息，因为在 node1 上安装 ESET PROTECT Server 期间会配置它们。

5. 配置防火墙以允许 ESET PROTECT Server 使用的所有端口上的传入连接。

6. 在群集配置管理器中，为 ESET PROTECT 服务器服务创建并启动角色（**配置角色 > 选择角色 > 常规服务**）。从可用服务列表中选择 **ESET PROTECT 服务器**服务。务必为步骤 3 中使用的与服务器证书相关的角色使用同一主机名。

7. 使用独立安装程序在所有群集节点上安装 ESET Management 服务器代理。在**服务器代理配置**和**连接到 ESET PROTECT 服务器**屏幕中，使用您在步骤 6 中所用的主机名。将服务器代理数据存储在本地节点上（而不是群集磁盘上

8. Web 服务器 (Apache Tomcat) 在群集上不受支持，因此需要将它安装在非群集磁盘上或不同计算机上：

a.在单独计算机上安装 Web 控制台，并正确配置为连接到 ESET PROTECT 服务器群集角色。

b.在 Web 控制台安装完成后，在以下位置可以找到其配置文件： *C:\Program Files\Apache Software Foundation\[Tomcat 文件夹]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties*

c.使用“记事本”或任何其他简单文本编辑器打开该文件。在 `server_address=localhost` 行中，将 localhost 替换为 ESET PROTECT 服务器群集角色的 IP 地址或主机名。

Linux 上的组件安装

在大部分安装方案中，您需要在不同的计算机上安装不同的 ESET PROTECT 组件，以适应不同的网络架构、符合性能要求，或者出于其他原因这样操作。

按照分步安装 ESET PROTECT 的说明进行操作。

核心组件安装

- ESET PROTECT 服务器
- ESET PROTECT Web 控制台 - 可以在未安装 ESET PROTECT 服务器的其他计算机上安装 ESET PROTECT Web 控制台。
- ESET Management 服务器代理
- 数据库服务器

可选组件安装

- RD Sensor
- 移动设备连接器
- ESET BridgeHTTP 代理
- 镜像工具

要将 Linux 版的 ESET PROTECT 升级到最新版本，请参阅组件升级任务章节或我们的知识库文章。

在 Linux 上分步安装 ESET PROTECT

在此安装方案中，我们将模拟 ESET PROTECT 服务器和 ESET PROTECT Web 控制台的分步安装。我们将使用 MySQL 模拟安装。

> **所选 Linux 分发版本的安装说明**
> 您可以遵循我们的知识库文章，其中包含特定于分发版本的说明：
> - CentOS 7
> - Debian 10
> - SUSE Linux Enterprise Server (SLES)

安装之前

1. 验证您的网络中是否存在数据库服务器，并确保您有权在本地/远程服务器上访问它。如果未安装数据库服务器，请安装并配置一个新的数据库服务器。

2. 下载 ESET PROTECT Linux 独立组件（服务器代理、服务器Web 控制台）。可以在 ESET 网站上提供的 ESET PROTECT 独立安装程序类别中找到这些安装文件。

安装进程

若要完成安装，您必须能够使用 `sudo` 命令或者在 `root` 特权下进行安装。

1. 为 ESET PROTECT 服务器安装所需的程序包。

2. 配置到 MySQL 服务器的连接，如 MySQL 配置主题中所示。

3. 验证 MySQL ODBC 驱动程序的配置。有关详细信息，请参阅 ODBC 安装和配置。

4. 自定义安装参数并执行 ESET PROTECT 服务器安装。有关详细信息，请参阅服务器安装 - Linux。

5. 安装所需的 Java 和 Tomcat 程序包，然后安装 ESET PROTECT Web 控制台。如果遇到与 ESET PROTECT Web 控制台的 HTTPS 连接有关的问题，请参阅 HTTPS/SSL 连接设置。

6. 在服务器计算机上安装 ESET Management 服务器代理。

> 建议您从命令行历史记录中删除包含敏感数据（例如，密码）的命令：
> 1.运行 `history` 以查看历史记录中所有命令的列表。
> 2.运行 `history -d line_number`（指定命令的行号）。或者，运行 `history -c` 以删除整个命令行历史记录。

MySQL 安装和配置

安装

> ⚠ 确保安装受支持版本的 MySQL Server 和 ODBC 连接器。

如果您已安装并配置了 MySQL，请转到配置继续进行操作。

1. 添加 MySQL 存储库：

Debian, Ubuntu	在终端中运行以下命令：
	`a)wget https://dev.mysql.com/get/mysql-apt-config_0.8.15-1_all.deb`
	`b)sudo dpkg -i mysql-apt-config_0.8.15-1_all.deb`
	可以选择要在程序包安装期间安装的组件版本。建议您选择默认选项。另请参阅 添加 MySQL APT 存储库

CentOS, Red Hat	添加 MySQL Yum 存储库
SUSE Linux Enterprise Server	添加 MySQL SLES 存储库

2. 更新本地存储库缓存：

Debian, Ubuntu	`sudo apt-get update`
CentOS, Red Hat	`sudo yum update`
SUSE Linux Enterprise Server	`sudo zypper update`

3. MySQL 安装会有所不同，具体取决于所使用的 Linux 发行版和版本：

Linux 发行版：	MySQL 服务器安装命令：	MySQL 服务器高级安装：
Debian, Ubuntu	`sudo apt-get install mysql-server`	Installing MySQL from Source with the MySQL APT Repository
CentOS, Red Hat	`sudo yum install mysql-community-server`	Installing MySQL on Linux Using the MySQL Yum Repository
SUSE Linux Enterprise Server	`sudo zypper install mysql-community-server`	Steps for a Fresh Installation of MySQL

下载 MySQL Community Server 以进行手动安装。

配置

1. 在文本编辑器中打开 *my.cnf* 配置文件：

```
sudo nano /etc/my.cnf
```

如果该文件不存在，请尝试使用 `/etc/mysql/my.cnf` 或 `/etc/my.cnf.d/community-mysql-server.cnf` 或 `/etc/mysql/mysql.conf.d/mysqld.cnf`

2. 在 `my.cnf` 文件的 *[mysqld]* 部分中找到以下配置，并修改其值。

> i
> - 如果文件中不存在 `[mysqld]` 部分，请创建它。
> - 如果该文件中不存在这些参数，请将它们添加到 `[mysqld]` 部分。
> - 要确定 MySQL 版本，请运行命令：`mysql --version`

参数	注释和建议值	MySQL 版本
`max_allowed_packet=33M`		所有支持的版本
`log_bin_trust_function_creators=1`	或者，还可以禁用二进制日志记录：`log_bin=0`	支持的 8.x 版本
`innodb_log_file_size=100M` `innodb_log_files_in_group=2`	这两个参数值的乘积必须至少为 **200** `innodb_log_files_in_group` 的最小值为 **2**，最大值为 **100**；该值还必须为整数。	支持的 8x 版本 5.7 5.6.22（及更高版本 5.6.x）
`innodb_log_file_size=200M`	将该值设置为至少 **200M**，但不要超过 **3000M**	5.6.20 和 5.6.21

3. 按 **CTRL + X**，然后键入 **Y** 以保存更改并关闭文件。

4. 重新启动 MySQL 服务器并应用该配置（在某些情况下，服务名称为 `mysqld`

```
sudo systemctl restart mysql
```

5. 设置 MySQL 权限和密码（该步骤是可选的，可能不适用于某些 Linux 发行版）：

a)显示临时 MySQL 密码：`sudo grep 'temporary password' /var/log/mysql/mysqld.log`

b)复制并保存密码。

c)通过以下选项之一设置新密码：

• 运行 `/usr/bin/mysql_secure_installation`，然后键入临时密码。然后，系统会提示您创建新密码。

- 运行 `mysql -u root -p`，然后键入临时密码。运行 `ALTER USER 'root'@'localhost' IDENTIFIED BY 'strong_new_password';` 以更改根密码（将 `strong_new_password` 替换为您的密码），然后键入 `Quit`。

另请参阅 MySQL 参考手册中的改进 MySQL 安装安全性。

6. 验证 MySQL 服务器服务是否正在运行：

```
sudo systemctl status mysql
```

ODBC 安装和配置

⚠ 确保安装受支持版本的 MySQL Server 和 ODBC 连接器。

ℹ 可以安装 Microsoft ODBC 驱动程序（版本 13 及更高版本），以将 Linux 上的 ESET PROTECT 服务器连接到 Windows 上的 Microsoft SQL Server。有关详细信息，请访问本知识库文章。

使用终端安装 MySQL ODBC 驱动程序。按照适用于 Linux 发行版的步骤操作：

- Debian、Ubuntu
- CentOS 7
- 支持的其他 Linux 发行版

Debian, Ubuntu

1. 安装 unixODBC 驱动程序：

```
sudo apt-get install unixodbc
```

2. 下载 ODBC 连接器：

Ubuntu 16	`wget https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-ubuntu16.04-x86-64bit.tar.gz`
Ubuntu 18	`wget https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-ubuntu18.04-x86-64bit.tar.gz`
Ubuntu 20	`wget https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit.tar.gz`
Debian 10	`wget https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-linux-debian10-x86-64bit.tar.gz`

⚠
- 确保选择并安装与 Linux 发行版和版本兼容的相应版本。
- 可以从官方 MySQL 网站下载适用于 MySQL 的 ODBC 连接器。

3. 解压缩 ODBC 驱动程序压缩文件（程序包名称根据所用的链接而发生变化）：

```
gunzip mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit.tar.gz
```

4. 提取 ODBC 驱动程序（程序包名称根据所用的链接而发生变化）：

```
tar xvf mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit.tar
```

5. 导航到 ODBC 驱动程序文件夹（程序包名称根据所用的链接而发生变化）：

```
cd mysql-connector-odbc-8.0.17-linux-ubuntu19.04-x86-64bit
```

6. 复制 ODBC 驱动程序文件：

```
sudo cp bin/* /usr/local/bin
sudo cp lib/* /usr/local/lib
```

7. 注册 ODBC 的驱动程序。

   • 对于新的 Linux 版本（如 Ubuntu 20.x）建议您使用 Unicode 驱动程序：

```
sudo myodbc-installer -a -d -n "MySQL ODBC 8.0 Driver" -t
"Driver=/usr/local/lib/libmyodbc8w.so"
```

   • 对于其他系统，或者当 Unicode 驱动程序不工作时：

```
sudo myodbc-installer -a -d -n "MySQL ODBC 8.0" -t
"Driver=/usr/local/lib/libmyodbc8a.so"
```

8. 列出安装的驱动程序：

```
sudo myodbc-installer -d -l
```

有关详细信息，请参阅：https://dev.mysql.com/doc/connector-odbc/en/connector-odbc-installation-binary-unix-tarball.html

CentOS 7

1. 安装 unixODBC 驱动程序：

```
sudo yum install unixODBC -y
```

2. 下载 ODBC 连接器：

```
wget
https://downloads.mysql.com/archives/get/p/10/file/mysql-connector-odbc-8.0.17-1.e
l7.x86_64.rpm
```

> ⚠
> • 请勿使用 YUM 安装 ODBC 连接器 – 它会安装不兼容的最新版本。
> • 确保选择并安装与 Linux 发行版和版本兼容的相应版本。
> • 可以从官方 MySQL 网站下载适用于 MySQL 的 ODBC 连接器。

3. 安装 ODBC 驱动程序：

```
sudo rpm -ivh mysql-connector-odbc-8.0.17-1.e17.x86_64.rpm --nodeps
```

4. 设置 ODBC 驱动程序：

```
sudo myodbc-installer -a -d -n "MySQL ODBC 8.0.17" -t
"Driver=/usr/lib64/libmyodbc8w.so"
```

5. 列出安装的驱动程序：

```
sudo myodbc-installer -d -l
```

支持的其他 Linux 发行版

- 确保选择并安装与 Linux 发行版和版本兼容的相应版本。
- 可以从官方 MySQL 网站下载适用于 MySQL 的 ODBC 连接器。

1. 按照以下说明安装 ODBC 驱动程序：

   - **SUSE Linux Enterprise Server**: `sudo zypper install unixODBC`. 另请参阅 https://tomcat.apache.org/tomcat-9.0-doc/logging.html
   - 从二进制 Tarball 发行版安装连接器/ODBC

2. 运行以下命令，使用文本编辑器打开 *odbcinst.ini* 文件：

   ```
   sudo nano /etc/odbcinst.ini
   ```

   或 `sudo nano/etc/unixODBC/odbcinst.ini`

3. 将以下配置复制到 *odbcinst.ini* 文件中（确保 **Driver** 和 **Setup** 的路径正确无误），然后保存并关闭该文件：

```
[MySQL]
Description = ODBC for MySQL
Driver = /usr/lib/x86_64-linux-gnu/odbc/libmyodbc.so
Setup = /usr/lib/x86_64-linux-gnu/odbc/libodbcmyS.so
FileUsage = 1
```

某些发行版的驱动程序可能位于其他位置。您可以使用以下命令找到该文件：

```
sudo find /usr -iname "*libmyodbc*"
```

4. 通过运行以下命令，更新用于控制 ODBC 对当前主机上数据库服务器访问权限的配置文件：

   ```
   sudo odbcinst -i -d -f /etc/odbcinst.ini
   ```

   或 `sudo odbcinst -i -d -f /etc/unixODBC/odbcinst.ini`

服务器安装 - Linux

所选 Linux 分发版本的安装说明

您可以遵循我们的知识库文章，其中包含特定于分发版本的说明：

- CentOS 7
- Debian 10
- SUSE Linux Enterprise Server (SLES)

安装

按照下面的步骤使用终端命令在 Linux 上安装 ESET PROTECT 服务器组件：

确保满足所有安装先决条件

1. 下载 ESET PROTECT 服务器组件：

```
wget https://download.eset.com/com/eset/apps/business/era/server/linux/latest/server
-linux-x86_64.sh
```

2. 生成下载的文件的可执行文件：

```
chmod +x server-linux-x86_64.sh
```

3. 您可以准备安装脚本，然后使用 `sudo` 执行它。

根据以下示例运行安装脚本（新行由“\”分隔，以便将整个命令复制到终端）：

```
sudo ./server-linux-x86_64.sh \
--skip-license \
--db-type="MySQL Server" \
--db-driver="MySQL ODBC 8.0 Driver" \
--db-hostname=localhost \
--db-port=3306 \
--db-admin-username=root \
--db-admin-password=password \
--server-root-password=password \
--db-user-username=root \
--db-user-password=password \
--cert-hostname="hostname, IP, FQDN"
```

您可以修改以下属性：

属性	说明	必需
`--uninstall`	卸载产品。	-
`--keep-database`	数据库不会在卸载期间删除。	-
`--locale`	已安装服务器的区域设置标识符 (LCID)默认值为 `en_US`）。有关可用选项，请参阅支持的语言 如果未指定 `--locale`，则 ESET PROTECT 服务器将以英语安装。 在完成 ESET PROTECT 安装后，即可为每个 ESET PROTECT Web 控制台会话设置一种语言。语言变更后，并非 Web 控制台的所有元素都会变更。某些元素（默认面板、策略、任务等）在安装 ESET PROTECT 期间创建，无法更改这些元素的语言。	是
`--skip-license`	安装不会要求用户进行许可协议确认。	-
`--skip-cert`	跳过证书生成（结合使用 `--server-cert-path` 参数）。	-
`--license-key`	ESET 许可证密钥。可以以后提供许可证密钥。	-
`--server-port`	ESET PROTECT 服务器端口（默认值为 `2222`）	-
`--console-port`	ESET PROTECT 控制台端口（默认值为 `2223`）	-
`--server-root-password`	用户“Administrator”的 Web 控制台登录密码，它的长度必须至少为 8 个字符。	是
`--db-type`	将使用的数据库的类型（可能的值：`"MySQL Server"`、`"MS SQL Server"`） Linux 上的 Microsoft SQL Server 不受支持。但可以将 Linux 上的 ESET PROTECT 服务器连接到 Windows 上的 Microsoft SQL Server	-

属性	说明	必需
--db-driver	在 *odbcinst.ini* 文件中指定的用于连接到数据库的 ODBC 驱动程序（命令 odbcinst -q -d 给出可用驱动程序列表，使用以下其中一个驱动程序，例如：--db-driver="MySQL ODBC 8.0 Driver"--db-driver="MySQL ODBC 8.0 Unicode Driver" 或 --db-driver="MySQL ODBC 8.0.17"	是
--db-hostname	数据库服务器的计算机名称或IP地址。命名的数据库实例不受支持。	是
--db-port	数据库服务器的端口（默认值为 3306	是
--db-name	ESET PROTECT 服务器数据库的名称（默认值为 era_db	-
--db-admin-username	数据库管理员用户名（在安装时用于创建和修改数据库）。如果之前创建的数据库用户是通过 --db-user-username 和 --db-user-password 定义的，则您可以省略此参数。	是
--db-admin-password	数据库管理员密码。如果之前创建的数据库用户是由 --db-user-username 和 --db-user-password 定义的，则您可以省略此参数。	是
--db-user-username	数据库 ESET PROTECT 服务器用户用户名（由 ESET PROTECT 服务器用于连接到数据库）；长度不应超过 16 个字符。	是
--db-user-password	数据库 ESET PROTECT 服务器用户密码	是
--cert-hostname	包含 ESET PROTECT 服务器计算机的所有可能名称和/或 IP该值必须与尝试连接到服务器的服务器代理证书中指定的服务器名称相匹配。	是
--server-cert-path	服务器对等证书的路径（如果您还指定了 --skip-cert，请使用此选项）	-
--server-cert-password	服务器对等证书的密码	-
--agent-cert-password	服务器代理对等证书的密码	-
--cert-auth-password	证书颁发机构密码	-
--cert-auth-path	服务器证书颁发机构文件的路径	-
--cert-auth-common-name	证书颁发机构常用名（使用“”	-
--cert-organizational-unit	-	-
--cert-organization	-	-
--cert-locality	-	-
--cert-state	-	-
--cert-country	-	-
--cert-validity	以天或年为单位的证书有效性（在参数 --cert-validity-unit 中指定）	-
--cert-validity-unit	证书有效性的单位，可能的值是“年”或“天”（默认值为 Years	-
--ad-server	Active Directory 服务器	-
--ad-user-name	有权搜索 AD 网络的用户的名称	-
--ad-user-password	Active Directory 用户密码	-
--ad-cdn-include	将进行同步的 Active Directory 树路径；使用空括号 ″″ 可同步整个树	-
--enable-imp-program	打开产品改进计划。	-
--disable-imp-program	关闭产品改进计划。	-

建议您从命令行历史记录中删除包含敏感数据（例如，密码）的命令：
1.运行 `history` 以查看历史记录中所有命令的列表。
2.运行 `history -d line_number`（指定命令的行号）。或者，运行 `history -c` 以删除整个命令行历史记录。

4. 该安装会提示您是否要参与产品改进计划。按 **Y**（如果同意向 ESET 发送崩溃报告和遥测数据），或按 **N**（不同意发送任何数据）。

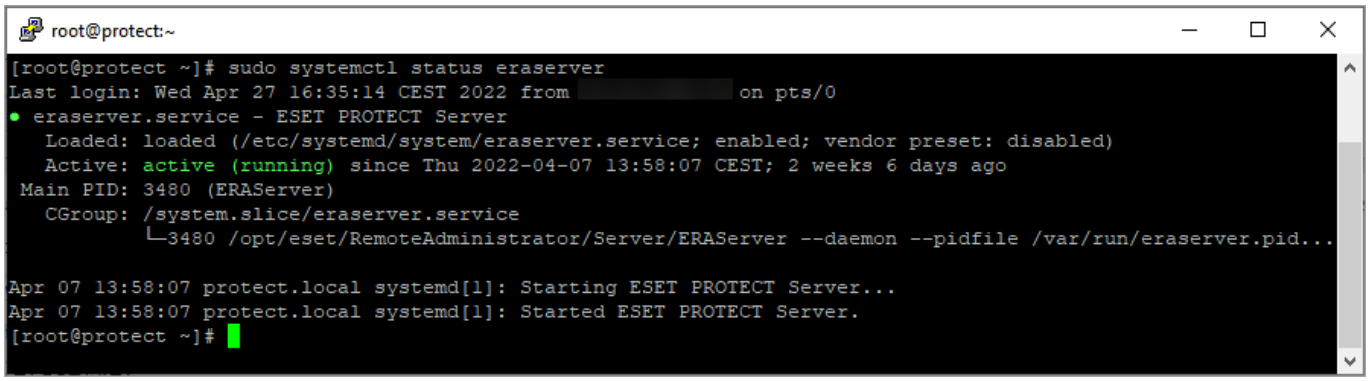
5. ESET PROTECT 服务器和 `eraserver` 服务将安装在以下位置中：

/opt/eset/RemoteAdministrator/Server

安装可能会以 **SELinux policy... failure** 结束。如果不使用 SELinux可以忽略它。

6. 在安装后，使用以下所示命令来验证 ESET PROTECT 服务器服务是否正在运行：

```
sudo systemctl status eraserver
```



安装程序日志

安装程序日志可能有助于排除故障，并且可以在日志文件中找到它。

服务器先决条件 - Linux

确保满足以下先决条件以在 Linux 上安装 ESET PROTECT 服务器：

- 必须具有有效的许可证
- 必须具有受支持的 Linux 操作系统
- 所需端口必须打开且可用 – 请在此处查看端口的完整列表
- 必须使用根帐户来安装和配置数据库服务器。在安装之前，不必先创建用户帐户。安装程序可以创建该帐户。 Linux 上的 Microsoft SQL Server 不受支持。但可以将 Linux 上的 ESET PROTECT 服务器连接到 Windows 上的 Microsoft SQL Server

ESET PROTECT 服务器在数据库中存储大数据 blob要使 ESET PROTECT 正常运行，请将 MySQL 配置为接受较大的数据包大小

- **ODBC 驱动程序** - ODBC 驱动程序用于建立与数据库服务器 (MySQL) 的连接。

- 使用终端命令将服务器安装文件设置为可执行文件：

```
chmod +x server-linux-x86_64.sh
```

- **我们建议您使用最新版本的 OpenSSL1.1.1**。ESET PROTECT 服务器/移动设备管理不支持 OpenSSL 3.x。ESET Management 服务器代理支持 OpenSSL 3.x。适用于 Linux 的 OpenSSL 的受支持最低版本为 openssl-1.0.1e-30。一个系统中可以同时安装有多个版本的 OpenSSL。您的系统中必须存在至少一个受支持的版本。

  - 使用命令 `openssl version` 来显示当前的默认版本。

  - 可以列出您系统上存在的所有版本的 OpenSSL。请查看使用命令 `sudo find / -iname *libcrypto.so*` 列出的文件名结尾

  - 您可以使用以下命令检查您的 Linux 客户端是否兼容：`openssl s_client -connect google.com:443 -tls1_2`

- **Xvfb** – 在没有图形界面的情况下，若要在 Linux Server 系统上正确打印报告（生成报告），需要使用它。

- **Xauth** – 程序包会与 **xvfb** 一起安装。如果不安装 **xvfb**，则需要安装 **xauth**。

- **cifs-utils** – 要将服务器代理正确部署到 Windows 操作系统，需要使用它。

- **Qt4 WebKit 库** – 用于将报告打印为 PDF 和 PS 格式（必须为版本 4.8，而不是版本 5）。所有其他 Qt4 附属组件都将自动进行安装。如果操作系统库中没有可用的程序包，您可以在目标计算机上自行编译它，也可以从第三方库（例如，EPEL 库）中安装它：CentOS 7 说明。Ubuntu 20.04 说明。

- **kinit + klist** - Kerberos 用于在登录和 Active Directory 同步任务时对域用户进行身份验证。确保正确配置 Kerberos (*/etc/krb5.conf*)。ESET PROTECT 10.0 支持与多个域进行同步。

- **ldapsearch** – 用于 AD 同步和授权。

- **snmptrap** – 可选，用于发送 SNMP 陷阱。SNMP 也需要进行配置。

- **SELinux 开发包** – 在产品安装期间用于生成 SELinux 策略模块。这仅在已启用 SELinux 的系统上是必需的。CentOS、RHEL、。SELinux 可能会导致其他应用程序出现问题。对于 ESET PROTECT 服务器，无需使用它。

- **lshw** – – 在客户端/服务器 Linux 计算机上安装 `lshw` 程序包，以使 ESET Management 服务器代理正确报告硬件清单。

下表中包含上述各种 Linux 发行版的每个程序包的相应终端命令（运行如 `sudo` 或 `root` 的命令）：

程序包	Debian 和 Ubuntu 发行版	CentOS 和 Red Hat 发行版
ODBC 驱动程序	请参阅 ODBC 安装和配置。	请参阅 ODBC 安装和配置。
OpenSSL	`apt-get install openssl`	`yum install openssl -y`
xvfb	`apt-get install xvfb`	`yum install xorg-x11-server-Xvfb -y`
cifs-utils	`apt-get install cifs-utils`	`yum install cifs-utils`

程序包	Debian 和 Ubuntu 发行版	CentOS 和 Red Hat 发行版

Qt4 WebKit 库	`apt-get install libqtwebkit4`
	请参阅 Ubuntu 20.04 说明
		Qt4 WebKit 不位于标准 CentOS 存储库中。安装以下程序包：
		`yum install -y epel-release`
		`yum install qtwebkit-devel`
		或者，可以安装 Fedora 存储库中的程序包。

kinit + klist - 可选（Active Directory 服务必须使用它）	`apt-get install krb5-user`	`yum install krb5-workstation`
ldapsearch	`apt-get install ldap-utils libsasl2-modules-gssapi-mit`	`yum install openldap-clients cyrus-sasl-gssapi cyrus-sasl-ldap -y`
snmptrap	`apt-get install snmp`	`yum install net-snmp-utils net-snmp`
SELinux 开发程序包（可选 – 并非 ESET PROTECT 服务器必需；SELinux 可能会导致其他应用程序出现问题。）	`apt-get install selinux-policy-dev`	`yum install policycoreutils-devel`
samba（可选，仅对于远程部署必需）	`apt-get install samba`	`yum install samba samba-winbind-clients`
lshw	`apt-get install -y lshw`	`yum install -y lshw`

服务器代理安装 - Linux

先决条件

- **我们建议您使用最新版本的 OpenSSL1.1.1**。ESET PROTECT 服务器/移动设备管理不支持 OpenSSL 3.x。ESET Management 服务器代理支持 OpenSSL 3.x。适用于 Linux 的 OpenSSL 的受支持最低版本为 openssl-1.0.1e-30。一个系统中可以同时安装有多个版本的 OpenSSL。您的系统中必须存在至少一个受支持的版本。
  - 使用命令 `openssl version` 来显示当前的默认版本。
  - 可以列出您系统上存在的所有版本的 OpenSSL。请查看使用命令 `sudo find / -iname *libcrypto.so*` 列出的文件名结尾
  - 您可以使用以下命令检查您的 Linux 客户端是否兼容：`openssl s_client -connect google.com:443 -tls1_2`
- – 在客户端/服务器 Linux 计算机上安装 `lshw` 程序包，以使 ESET Management 服务器代理正确报告硬件清单。

Linux 发行版	终端命令
Debian, Ubuntu	`sudo apt-get install -y lshw`
Red Hat, CentOS, RHEL	`sudo yum install -y lshw`
OpenSUSE	`sudo zypper install lshw`

- 对于 Linux CentOS建议您安装 `policycoreutils-devel` 程序包。运行命令以安装程序包：

```
yum install policycoreutils-devel
```

- 服务器辅助服务器代理安装：
  - 服务器计算机必须可以通过网络进行访问，并且已安装 ESET PROTECT 服务器和 ESET PROTECT Web 控制台
- 脱机服务器代理安装：
  - 服务器计算机必须可以通过网络进行访问，并且已安装 ESET PROTECT 服务器
  - 服务器代理的证书必须存在。
  - 服务器证书颁发机构公钥文件必须存在。

安装

按照下面的步骤使用终端命令在 Linux 上安装 ESET Management 服务器代理组件：

确保满足上面列出的所有安装先决条件。

1. 下载服务器代理安装脚本：

```
wget https://download.eset.com/com/eset/apps/business/era/agent/latest/agent-linux-x86_64.sh
```

2. 生成该文件的可执行文件：

```
chmod +x agent-linux-x86_64.sh
```

3. 根据以下示例运行安装脚本（新行由“\”分隔，以便将整个命令复制到终端）：

有关更多详细信息，请参阅下面的参数

服务器辅助安装：

```
sudo ./agent-linux-x86_64.sh \
--skip-license \
--hostname=10.1.0.1 \
--port=2222 \
--webconsole-user=Administrator \
--webconsole-password=aB45$45c \
--webconsole-port=2223
```

脱机安装：

```
sudo ./agent-linux-x86_64.sh \
--skip-license \
--cert-path=/home/admin/Desktop/agent.pfx \
--cert-auth-path=/home/admin/Desktop/CA.der \
--cert-password=N3lluI4#2aCC \
--hostname=10.1.179.36 \
--port=2222
```

建议您从命令行历史记录中删除包含敏感数据（例如，密码）的命令：
1.运行 `history` 以查看历史记录中所有命令的列表。
2.运行 `history -d line_number`（指定命令的行号）。或者，运行 `history -c` 以删除整个命令行历史记录。

4. 出现提示时，按 **y** 以接受证书。可以忽略安装程序返回的任何有关 SELinux 的错误。

5. 在安装后，请验证 ESET Management 服务器代理服务是否正在运行：

```
sudo systemctl status eraagent
```

6. 将 **eraagent** 服务设置为系统启动时启动：`sudo systemctl enable eraagent`

安装程序日志
安装程序日志可能有助于故障排除。可以在日志文件中找到它。

参数

使用参数 --hostname 和 --port在提供 SRV 记录时不使用端口）解析 ESET PROTECT 服务器连接。可能的连接格式.

- **主机名**和**端口**
- **IPv4 地址**和**端口**
- **IPv6 地址**和**端口**
- 服务记录SRV 记录） – 若要在 Linux 中配置 DNS 资源记录，计算机必须位于带有运行的 DNS 服务器的域中。请参阅 DNS 资源记录SRV 记录必须以前缀“_NAME._tcp”开头，其中“NAME”表示自定义命名（例如“era”

属性	说明	必需
`--hostname`	要连接的 ESET PROTECT 服务器的主机名或 IP 地址。	是
`--port`	ESET PROTECT () 服务器端口（默认值为 2222	是
`--cert-path`	服务器代理证书文件的本地路径（有关证书的详细信息）。	是（脱机）
`--cert-auth-path`	服务器证书颁发机构文件的路径（有关颁发机构的详细信息）。	是（脱机）
`--cert-password`	服务器代理证书密码。	是（脱机）
`--cert-auth-password`	证书颁发机构密码。	是（如果已使用）
`--skip-license`	安装不会要求用户进行许可协议确认。	否

属性	说明	必需
--cert-content	PKCS12 编码的公钥证书以及私钥的 Base64 编码的内容，用于在服务器和服务器代理之间设置安全通信通道。仅使用 --cert-path 或 --cert-content 选项之一。	否
--cert-auth-content	DER 编码的证书颁发机构私钥证书的 Base64 编码的内容，用于验证远程对等（代理或服务器）。仅使用 --cert-auth-path 或 --cert-auth-content 选项之一。	否
--webconsole-hostname	Web 控制台用于连接到服务器的主机名或 IP 地址（如果保留为空，则安装程序会复制“hostname”中的值）。	否
--webconsole-port	可供 Web 控制台用于连接到服务器的端口（默认值为 2223	否
--webconsole-user	可供 Web 控制台用于连接到服务器的用户名（默认值为 Administrator 无法让使用双重身份验证的用户参与服务器辅助安装。	否
--webconsole-password	可供 Web 控制台用于连接到服务器的密码。	是（服务器辅助）
--proxy-hostname	HTTP 代理主机名。使用此参数以支持将 HTTP 代理（已安装在网络中）用于 ESET Management 服务器代理和 ESET PROTECT 服务器之间的复制（而非用于缓存更新）。	如果使用代理
--proxy-port	用于连接到服务器的 HTTP 代理端口。	如果使用代理
--enable-imp-program	打开产品改进计划。	否
--disable-imp-program	关闭产品改进计划。	否

连接和证书

- 必须提供**到 ESET PROTECT 服务器的连接** --hostname, --port（如果提供服务记录，则不需要端口，默认端口值为 2222

- 为**服务器辅助安装**提供以下连接信息： --webconsole-port, --webconsole-user, --webconsole-password

- 为**脱机安装**提供证书信息：--cert-path, --cert-password。安装参数 --cert-path 和 --cert-auth-path 需要证书文件（*.pfx* 和 *.der*），这些证书文件可以从 ESET PROTECT Web 控制台导出。（参阅如何导出 .pfx 文件和 .der 文件

密码类型参数

密码类型参数可作为环境变量、文件提供，可从 stdin 读取或作为纯文本提供。即：

--password=env:SECRET_PASSWORD，其中 SECRET_PASSWORD 是带有密码的环境变量

--password=file:/opt/secret，其中常规文件 /opt/secret 的第一行包含密码

--password=stdin，指示安装程序从标准输入读取密码

--password="pass:PASSWORD" 等同于 --password="PASSWORD"，并且前者在实际密码是 "stdin"（标准输入） 或者是以 "env:" "file:" 或 "pass:" 开头的字符串时为必填项

⚠ 证书密码中不得包含以下字符：" \ 这些字符在初始化服务器代理期间会导致严重错误。

HTTP 代理连接

如果要将 HTTP 代理用于 ESET Management 服务器代理和 ESET PROTECT 服务器之间的复制（而不是用于缓存更新），可以在 `--proxy-hostname` 和 `--proxy-port` 中指定连接参数。

示例 – 使用 HTTP 代理连接的脱机服务器代理安装

```
./agent-linux-x86_64.sh \
--skip-license \
--cert-path=/home/admin/Desktop/agent.pfx \
--cert-auth-path=/home/admin/Desktop/CA.der \
--cert-password=N3lluI4#2aCC \
--hostname=10.1.179.36 \
--port=2222 \
--proxy-hostname=10.1.180.3 \
--proxy-port=3333 \
```

服务器代理和 ESET PROTECT 服务器之间的通信协议不支持身份验证。任何用于将服务器代理通信转发到需要身份验证的 ESET PROTECT 服务器的代理解决方案将不工作。
如果针对 Web 控制台或服务器代理选择使用非默认端口，可能需要调整防火墙。否则，安装可能会失败。

Linux 上服务器代理的升级和修复安装

如果在已安装服务器代理的系统上手动运行服务器代理安装，则可能出现以下情况：

- **升级** – 运行更高版本的安装程序。
  - 服务器辅助安装 – 应用程序已升级，但它将继续使用以前的证书。
  - 脱机安装 – 应用程序已升级，使用新的证书。
- **修复** – 运行相同版本的安装程序。可以使用此选项将服务器代理迁移到其他 ESET PROTECT 服务器。
  - 服务器辅助安装 – 应用程序已重新安装，并且它将从 ESET PROTECT 服务器获取当前证书（由 `hostname` 参数定义）。
  - 脱机安装 – 应用程序已重新安装，使用新的证书。

如果您手动将服务器代理迁移到其他较新的 ESET PROTECT 服务器，并且您使用服务器辅助安装，则运行安装命令两次。第一次将升级服务器代理，第二次将获取新证书，以便服务器代理可以连接到 ESET PROTECT

服务器。

Web 控制台安装 - Linux

要安装 ESET PROTECT Web 控制台，请遵循以下步骤：

> 可以在未安装 ESET PROTECT 服务器的其他计算机上安装 ESET PROTECT Web 控制台。 该过程需要其他步骤

1. 安装 Apache Tomcat 和 Java 程序包。

> 下面的示例程序包名称可能不同于您的 Linux 发行版存储库程序包。Linux 发行版的默认存储库可能不包含最新支持版本的 Apache Tomcat 和 Java。

Linux 发行版	终端命令
Debian 和 Ubuntu 发行版	`sudo apt-get update` `sudo apt-get install openjdk-17-jdk tomcat9`
CentOS 和 Red Hat 发行版	`yum update` `yum install java-17-openjdk tomcat`
SUSE Linux	`zypper refresh` `sudo zypper install java-17-openjdk tomcat9`

2. 下载 Web 控制台文件（*era.war*）。

```
wget https://download.eset.com/com/eset/apps/business/era/webconsole/latest/era.war
```

3. 将 *era.war* 文件复制到 Tomcat 文件夹：

Debian, Ubuntu	`sudo cp era.war /var/lib/tomcat9/webapps/`
CentOS, Red Hat	`sudo cp era.war /var/lib/tomcat/webapps/`
SUSE Linux Enterprise Server	`sudo cp era.war /usr/share/tomcat/webapps/`

4. 重新启动 Tomcat 服务以部署 *era.war* 文件：

Debian, Ubuntu	`sudo systemctl restart tomcat9`
CentOS, Red Hat	`sudo systemctl restart tomcat`
SUSE Linux Enterprise Server	`sudo systemctl restart tomcat`

5. 验证 *era* 文件夹是否位于 Tomcat 文件夹中：

Debian, Ubuntu	`ls /var/lib/tomcat9/webapps`
CentOS, Red Hat	`ls /var/lib/tomcat/webapps`
SUSE Linux Enterprise Server	`ls /usr/share/tomcat/webapps`

输出应如下所示：`era era.war`

6. 将 Tomcat 服务设置为系统启动时启动：`sudo systemctl enable tomcat`（或基于服务名称的

tomcat9

7. 如果在 ESET PROTECT 服务器以外的其他计算机上安装了 ESET PROTECT Web 控制台，请执行以下附加步骤以启用 ESET PROTECT Web 控制台与 ESET PROTECT 服务器之间的通信：

a)停用 Tomcat 服务：`sudo systemctl stop tomcat`

b)编辑 *EraWebServerConfig.properties* 文件：

```
sudo nano /var/lib/tomcat/webapps/era/WEB-
INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.prop
erties
```

如果 *EraWebServerConfig.properties* 文件不位于上述路径中，可以在您的系统上使用以下命令查找该文件：

```
find / -iname "EraWebServerConfig.properties"
```

c)查找 `server_address=localhost`

d)将 `localhost` 替换为您的 ESET PROTECT 服务器的 IP 地址，并保存该文件。

e)重新启动 Tomcat 服务：`sudo systemctl restart tomcat`（或基于服务名称的 `tomcat9`

f)将 Tomcat 服务设置为系统启动时启动：`sudo systemctl enable tomcat`（或基于服务名称的 `tomcat9`

8. 在受支持的 Web 浏览器中打开 ESET PROTECT Web 控制台，以访问登录屏幕：

- 从托管 ESET PROTECT Web 控制台的计算机：*http://localhost:8080/era*
- 从可以访问 Internet 的任何计算机访问 ESET PROTECT Web 控制台（将 *IP_ADDRESS_OR_HOSTNAME* 替换为 ESET PROTECT Web 控制台的 IP 地址或主机名）：*http://IP_ADDRESS_OR_HOSTNAME:8080/era*

9. 安装完成后配置 Web 控制台：

- 在 Apache Tomcat 的手动安装过程中，默认 HTTP 端口设置为 8080。 我们建议您设置 Apache Tomcat 的 HTTPS 连接
- 另请参见企业解决方案的 Web 控制台配置或低性能系统

Rogue Detection Sensor 安装 - Linux

如果有多个网段，则必须在每个网段上单独安装 Rogue Detection Sensor才能生成整个网络上所有设备的全面列表。

先决条件

- 网络可搜索（端口已打开，防火墙未阻止传入通信等）。
- 服务器计算机是可访问的。
- ESET Management 服务器代理必须安装在本地计算机上，才能完全支持所有程序功能

- 终端已打开。
- 将 RD Sensor 安装文件设置为可执行文件：

```
chmod +x rdsensor-linux-x86_64.sh
```

安装

按照下面的步骤使用终端命令在 Linux 上安装 RD Sensor 组件：

确保满足上面列出的所有安装先决条件。

1. 使用以下命令将安装文件作为 sudo 运行：

```
sudo ./rdsensor-linux-x86_64.sh
```

2. 阅读最终用户许可协议。使用**空格键**前进到 EULA 的下一页。
安装程序将提示您指定是否接受该协议。如果同意，请按键盘上的 **Y**。否则，按 **N**。

3. 按 **Y**（如果同意参与产品改进计划）。否则，按 **N**。

4. ESET Rogue Detection Sensor 将在安装完成后启动。

5. 若要查看安装是否已成功，请通过执行以下命令验证服务是否正在运行：

```
sudo systemctl status rdsensor
```

6. 可以在日志文件中找到 Rogue Detection Sensor 日志文件：

/var/log/eset/RogueDetectionSensor/trace.log

移动设备连接器安装 - Linux

ESET PROTECT 移动设备管理/连接器 (MDM/MDC) 组件（仅限本地）计划结束生命周期。阅读更多建议您迁移到 Cloud MDM。

您可以在其他服务器（而不是运行 ESET PROTECT Server 的服务器）上安装移动设备连接器。例如，您可以使用此安装方案使 Mobile Device Connector 可通过 Internet 访问，以便随时管理用户的移动设备。

按照下面的步骤使用终端命令在 Linux 上安装 Mobile Device Connector 组件：

确保满足所有安装先决条件。

1. 下载 Mobile Device Connector 安装脚本：

```
wget https://download.eset.com/com/eset/apps/business/era/mdm/latest/mdmcore-linux-x86_64.sh
```

2. 根据以下示例运行安装脚本（新行由“\”分隔，以便将整个命令复制到终端）：

```
sudo ./mdmcore-linux-x86_64.sh \
--https-cert-path="full_path/proxycert.pfx" \
--https-cert-password="123456789" \
--port=2222 \
--db-type="MySQL Server" \
--db-driver="MySQL ODBC 8.0 Driver" \
--db-admin-username="root" \
--db-admin-password=123456789 \
--db-user-password=123456789 \
--db-hostname="127.0.0.1" \
--webconsole-password=123456789 \
--hostname=username.LOCAL \
--mdm-hostname=username.LOCAL
```

有关可用参数的完整列表（打印帮助消息），请使用：

```
--help
```

> 建议您从命令行历史记录中删除包含敏感数据（例如，密码）的命令：
> 1.运行 `history` 以查看历史记录中所有命令的列表。
> 2.运行 `history -d line_number`（指定命令的行号）。或者，运行 `history -c` 以删除整个命令行历史记录。

所需的安装命令参数

提供了许多可选安装参数，但其中一些参数是必需的。

- 对等证书 – 可通过两种方法获取 ESET PROTECT 对等证书

  • **服务器辅助安装** – 您将需要提供 ESET PROTECT Web 控制台管理员证书（安装程序将自动下载所需证书）。

  • **脱机安装** – 需要提供对等证书（从 ESET PROTECT 中导出的代理证书）。此外，您可以使用自定义证书

  o对于**服务器辅助安装**，至少包括：

  ```
  --webconsole-password=
  ```

  o对于**脱机安装**，包括：

  ```
  --cert-path=
  --cert-password=
  ```

（在 ESET PROTECT 服务器安装期间创建默认服务器代理证书不需要密码。）

- HTTPS代理）证书：

  o如果您已有 HTTPS 证书：

```
--https-cert-path=
--https-cert-password=
```

o若要生成新的 HTTPS 证书：

```
--https-cert-generate
--mdm-hostname=
```

- 到 ESET PROTECT 服务器的连接（名称或 IP 地址）：

```
--hostname=
```

- 数据库连接：

  o对于 MySQL 数据库，包括：

```
--db-type="MySQL Server"
--db-driver=
--db-admin-username=
--db-admin-password=
--db-user-password=
```

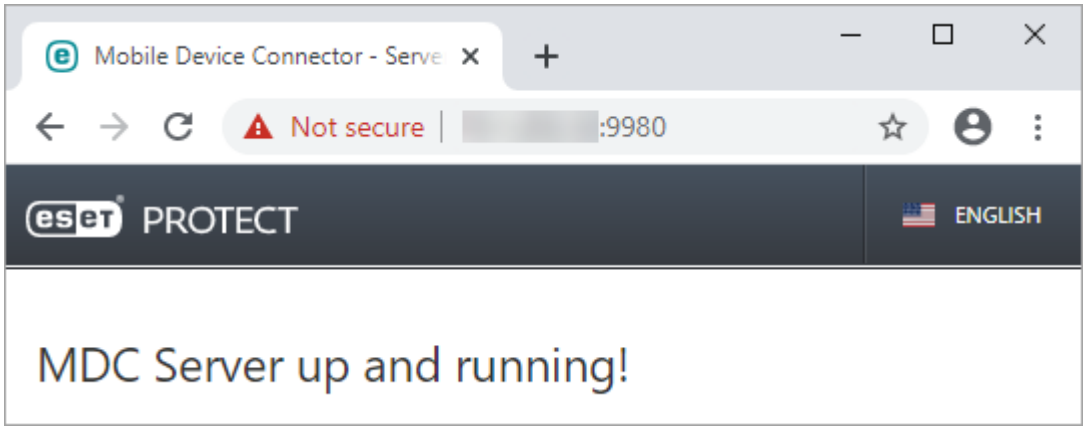
  o对于 Microsoft SQL 数据库，包括：

```
--db-type="Microsoft SQL Server"
--db-driver=
--db-admin-username=
--db-admin-password=
--db-user-password=
```

安装程序日志

安装程序日志可能有助于排除故障，并且可以在日志文件中找到它。

安装完成后，通过在 Web 浏览器中打开 *https://your-mdm-hostname:enrollment-port*（例如 *https://eramdm:9980*）来检查移动设备连接器是否正常运行。如果已成功安装，您将看到以下消息：



通过从移动设备访问移动设备连接器服务器，您还可以使用此 URL 来在 Internet 中检查该服务器的可用性（如果以此方式配置）。如果您无法访问该页面，请检查您的防火墙以及您的网络基础架构的配置。

移动设备连接器先决条件 - Linux

必须满足以下先决条件，才能在 Linux 上安装移动设备连接器：

- 已使用根帐户安装并配置了数据库服务器（无需创建用户帐户即可安装，安装程序可以创建帐户）。
- 用于连接到数据库服务器 (MySQL / Microsoft SQL) 的 ODBC 驱动程序已安装在计算机上。请参阅 ODBC 安装和配置章节。

> 应使用 `unixODBC_23` 程序包（而非默认的 `unixODBC`），以将 MDC连接到 MySQL 数据库，如此便不会产生任何问题。对于 SUSE Linux 来说尤其如此。

> 建议您将 MDM 组件部署在独立于托管 ESET PROTECT 服务器的其他主机设备上。

- MDMCore 安装文件设置为可执行文件。

```
chmod +x mdmcore-linux-x86_64.sh
```

- 在安装后，请验证 MDMCore 服务是否在运行。

```
sudo systemctl status eramdmcore
```

- **我们建议您使用最新版本的 OpenSSL1.1.1**。ESET PROTECT 服务器/移动设备管理不支持 OpenSSL 3.x。ESET Management 服务器代理支持 OpenSSL 3.x。适用于 Linux 的 OpenSSL 的受支持最低版本为 openssl-1.0.1e-30。一个系统中可以同时安装有多个版本的 OpenSSL。您的系统中必须存在至少一个受支持的版本。
  - 使用命令 `openssl version` 来显示当前的默认版本。
  - 可以列出您系统上存在的所有版本的 OpenSSL。请查看使用命令 `sudo find / -iname *libcrypto.so*` 列出的文件名结尾
  - 您可以使用以下命令检查您的 Linux 客户端是否兼容：`openssl s_client -connect google.com:443 -tls1_2`

> 如果 MySQL 上的 MDM 数据库过大（数千个设备），则表明默认的 `innodb_buffer_pool_size` 值过小。有关数据库优化的详细信息，请参阅：http://dev.mysql.com/doc/refman/5.6/en/optimizing-innodb-diskio.html

证书要求

• 若要通过 HTTPS 安全地进行通信，需要采用 *.pfx*格式的 **SSL 证书**。建议您使用由第三方证书颁发机构提供的证书。不建议使用自签名证书（包括由 ESET PROTECT CA 签名的证书），因为并非所有移动设备都允许用户接受自签名证书。

• 需要具有 CA 签名的证书和相应私钥，然后利用标准步骤（通常使用 OpenSSL）将上述内容合并到一个 *.pfx* 文件中：
`openssl pkcs12 -export -in certificate.cer -inkey privateKey.key -out httpsCredentials.pfx`
这是适用于大多数使用 SSL 证书的服务器的标准步骤。

• 对于脱机安装，您还需要对等证书（从 ESET PROTECT 中导出的**服务器代理证书**）。此外，您可以使用 ESET PROTECT 的自定义证书

镜像工具 - Linux

您是 Windows 用户吗？

镜像工具对脱机检测引擎更新而言不可或缺。如果您的客户端计算机不具有 Internet 连接而需要进行检测引擎更新，您可以使用镜像工具从 ESET 更新服务器下载更新文件，然后将其存储在本地。

镜像工具具有以下功能：
• 模块更新 – 它会下载检测引擎更新和其他程序模块，但不会下载自动更新 (uPCU)
• 存储库创建 – 它可以创建完整的脱机存储库，包括自动更新 (uPCU)
镜像工具不会下载 ESET LiveGrid® 数据。

先决条件

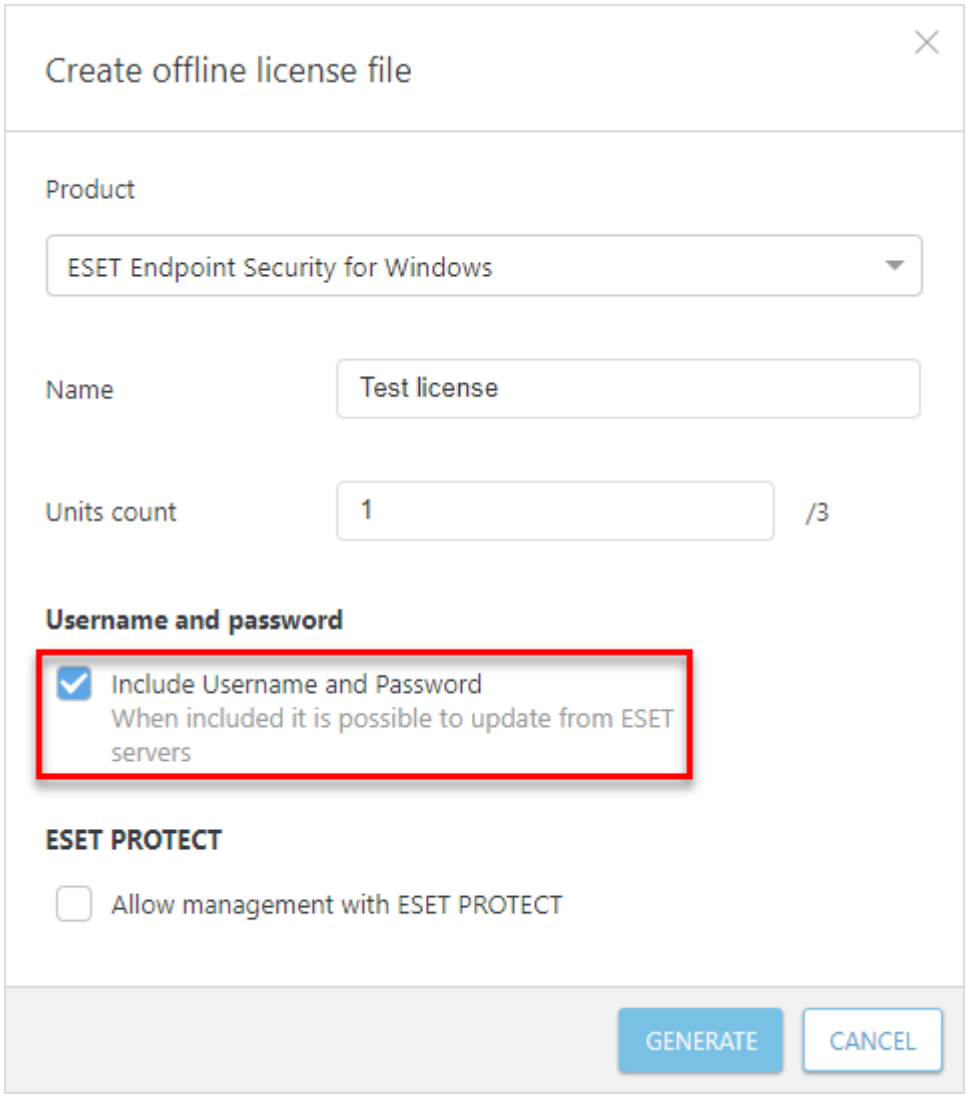
• 对于所有用户，创建镜像的存储库必须有读取和执行权限。以特权用户身份运行以下命令来授权：`chmod 755 mirror/folder/path`（将 `mirror/folder/path` 替换为镜像文件夹路径）。

• 目标文件夹必须可供共享（Samba/Windows 或 HTTP/FTP 服务），具体取决于您希望如何访问更新。

o适用于 Windows 的 ESET 安全产品 – 可以使用 HTTP 或共享文件夹远程更新它们。

o适用于 Linux/macOS 的 ESET 安全产品 – 只可以使用 HTTP 远程更新它们。如果使用共享文件夹，该文件夹必须和 ESET 安全产品位于同一计算机上。

• 您必须具有一个包含用户名和密码的有效脱机许可证文件。生成许可证文件时，请务必选中**包括用户名和密码**旁边的复选框。此外，还必须键入许可证**名称**。需要一个脱机许可证文件来激活镜像工具以及生成更新镜像。



如何使用镜像工具

1.从 ESET 下载页（**独立安装程序**部分）下载镜像工具。

2.解压缩下载的压缩文件。

3.在内含 *MirrorTool* 文件的文件夹中打开终端，然后生成该文件的可执行文件：

```
chmod +x MirrorTool
```

4.运行以下命令，以查看镜像工具及其版本的所有可用参数：

```
./MirrorTool --help
```

```
root@ubuntu:/home/user/Desktop/x86_64/x86_64# ./MirrorTool --help
Mirror Tool v1.0.2226.0, Copyright (c) ESET, spol. s r.o. 1992-2021. All rights reserved.
Allowed options:
  --mirrorType arg                      [required for module update]
                                        Type of mirror. Possible values (case
                                        insensitive): regular, pre-release,
                                        delayed.
  --intermediateUpdateDirectory arg     [required for module update]
                                        Files will be downloaded to this
                                        directory to create mirror in output
                                        directory.
  --offlineLicenseFilename arg          [required for module update]
                                        Offline license file.
  --updateServer arg                    [optional]
                                        Update server. (e.g.:
                                        http://update.eset.com/eset_upd/ep6/)
                                        Mirror will be created in output
                                        directory, only specified path in
                                        server will be mirrored.
  --outputDirectory arg                 [required for module update]
                                        Directory where mirror will be created.
  --proxyHost arg                       [optional]
                                        Http proxy address (fqdn or IP).
  --proxyPort arg                       [optional]
                                        Http proxy port.
  --proxyUsername arg                   [optional]
                                        Http proxy username.
  --proxyPassword arg                   [optional]
                                        Http proxy password.
  --networkDriveUsername arg            [optional]
                                        Username used, when output directory is
                                        accessed using smb(e.g:\\hostname).
  --networkDrivePassword arg            [optional]
                                        Password used, when output directory is
                                        accessed using smb(e.g:\\hostname).
  --excludedProducts arg                [optional]
                                        Disable creating mirror for specified
                                        products. Use --listUpdatableProducts
                                        to see possible values.
  --listUpdatableProducts               Show list of all products which modules
                                        are downloaded by default.
  --repositoryServer arg                [required for repository update]
                                        Repository server for repository
                                        creation.
  --intermediateRepositoryDirectory arg [required for repository update]
                                        Files will be downloaded to this
                                        directory to create offline mirror in
                                        output directory.
  --outputRepositoryDirectory arg       [required for repository update]
                                        Directory where offline repository will
                                        be created.
  --trustDownloadedFilesInRepositoryTemp
                                        [optional]
                                        If set, hashes on already downloaded
                                        files are not checked.
  --mirrorOnlyLevelUpdates              [optional]
                                        If set, only level upgrades will be
                                        downloaded (nano/continuous updates
                                        will not be downloaded)
  --mirrorFileFormat arg                [optional]
                                        Specifies which type of update files
                                        will be downloaded. Possible values
                                        (case insensitive): dll, dat.
  --compatibilityVersion arg            [optional]
                                        Version of compatible products.
  --filterFilePath arg                  [optional]
                                        Path to filter file in json format.
                                        Parameter compatibilityVersion has to
                                        be higher than 7.1.0.0 to run program.
  --dryRun arg                          [optional]
                                        Specifies dry run of program with path
                                        to csv file where will be saved list of
                                        products to be downloaded with current
                                        filter configuration.
  --help                                [optional]
                                        Display this help and exit
```

所有过滤器均区分大小写。

可以使用参数来创建存储库镜像或模块镜像：

存储库和模块镜像的参数

--proxyHost
--proxyPort
--proxyUsername
--proxyPassword
--help

存储库特定参数

--repositoryServer
--intermediateRepositoryDirectory
--outputRepositoryDirectory
--compatibilityVersion
--dryRun
--filterFilePath
--trustDownloadedFilesInRepositoryTemp

模块特定参数

--mirrorType
--intermediateUpdateDirectory
--offlineLicenseFilename
--updateServer
--outputDirectory
--networkDriveUsername
--networkDrivePassword
--excludedProducts
--listUpdatableProducts
--mirrorOnlyLevelUpdates
--mirrorFileFormat

参数	说明
--updateServer	Mirror Tool 创建的文件夹结构不同于 Endpoint 镜像创建的文件夹结构。每个文件夹都包含一组产品的更新文件。 必须在使用镜像的产品的更新设置中，指定更新服务器完整链接（即正确文件夹的完整路径）。
--offlineLicenseFilename	您必须指定指向您的脱机许可证文件的路径（如上所述）。
--mirrorOnlyLevelUpdates	不需要参数。如果已设置，则仅下载级别更新（不会下载微量更新）。在我们的知识库文章中阅读有关更新类型的详细信息。

参数	说明
`--mirrorFileFormat`	⚠ 在使用 `--mirrorFileFormat` 参数前，确保您的环境不包含更低（6.5 及更低版本）和更高（6.6. 及更高版本ESET安全产品版本。此参数的错误使用可能导致 ESET 安全产品的错误更新。 可以指定下载哪种类型的更新文件。可能的值（区分大小写）： • `dat` – 如果您的环境仅有 ESET 安全产品版本 6.5 及更低版本，则使用此值。 • `dll` – 如果您的环境仅有 ESET 安全产品版本 6.6 及更高版本，则使用此值。 当创建旧产品（`ep4`ep5）的镜像时，忽略此参数。
`--compatibilityVersion`	此可选参数适用于随 ESET PROTECT 8.1 及更高版本一起分发的镜像工具。镜像工具将下载与您在参数自变量中以格式 `x.x` 或 `x.x.x.x` 指定的 ESET PROTECT 存储库版本兼容的更新文件，例如：`--compatibilityVersion 10.0` 或 `--compatibilityVersion 8.1.13.0` `--compatibilityVersion` 参数将从镜像中排除自动更新 (uPCU)。如果您需要环境中存在自动更新（uPCU）并希望减小镜像大小，请使用 `--filterFilePath` 参数。

i 要减少从 ESET 存储库下载的数据量，建议您在随 ESET PROTECT 9 一起分发的镜像工具中使用新参数：`--filterFilePath` 和 `--dryRun`
1.采用 *JSON* 格式创建过滤器（参见下面的 `--filterFilePath`
2.执行使用 `--dryRun` 参数运行镜像工具的测试（参见下文），并根据需要调整过滤器。
3.使用 `--filterFilePath` 参数和定义的下载过滤器，以及 `--intermediateRepositoryDirectory` 和 `--outputRepositoryDirectory` 参数运行镜像工具。
4.定期运行镜像工具，以始终使用最新的安装程序。

参数	说明

--filterFilePath	使用此可选参数以根据与镜像工具位于同一文件夹中的 *JSON* 格式文本文件过滤 ESET 安全产品，例如：--filterFilePath filter.txt
	过滤器配置说明：
	产品过滤的配置文件格式为 *JSON*，其结构如下所示：
	• 根 *JSON* 对象：
	o use_legacy（布尔值，可选）– 如果为 true 则将包含旧产品。
	o defaults（*JSON* 对象，可选）– 定义将应用于所有产品的过滤器属性。
	■ languages（代码）– 指定要包含语言的 ISO 语言代码，例如法语类型为 "fr_FR"。其他语言代码在下表中。要选择多个语言，请使用逗号和空格分隔它们，例如：(["en_US", "zh_TW", "de_DE"])
	■ platforms（列表）– 要包括的平台 (["x64", "x86", "arm64"])
	⚠ 请谨慎使用 platforms 过滤器。例如，如果镜像工具仅下载 64 位安装程序并且您的基础架构中有 32 位计算机，则 64 位 ESET 安全产品将无法在 32 位计算机上安装。
	■ os_types（列表）– 要包括的操作系统类型（["windows"]["linux"]["mac"]）
	o products（JSON 对象的列表，可选）– 要应用于特定产品的过滤器 – 覆盖特定产品的 defaults。对象具有以下属性：
	■ app_id（字符串）– 如果 name 未指定，则该项为必填项。
	■ name（字符串）– 如果 app_id 未指定，则该项为必填项。
	■ version（字符串）– 指定要包含的版本或版本范围。
	■ languages（列表）– 要包含语言的 ISO 语言代码（参见下表）
	■ platforms（列表）– 要包括的平台 (["x64", "x86", "arm64"])
	■ os_types（列表）– 要包括的操作系统类型（["windows"]["linux"]["mac"]）
	ℹ 要确定各字段的合适值，请在试运行模式下运行镜像工具，并在创建的 CSV 文件中找到相关产品。
	版本字符串格式说明
	所有版本号均由四个以点分隔的数字组成（例如，7.1.0.0）。可以在填写版本过滤器时指定较少数字（例如，7.1），其余数字将为零（7.1 等同于 7.1.0.0）
	版本字符串可以采用以下两种格式之一：
	• [>|<|>=|<=|=]<n>.(<n>.(<n>.(<n>)))
	o 选择大于/小于或等于/小于或等于/等于指定版本的版本。
	• <n>.(<n>.(<n>.(<n>))) - <n>.(<n>.(<n>.(<n>)))
	o 选择大于或等于下限且小于或等于上限的版本。
	从左到右对版本号的每个部分进行数字比较。
	JSON 示例
	{
	"use_legacy": true,
	"defaults": {
	"languages": ["en_US"],
	"platforms": ["x64", "x86"]
	},
	"products": [
	{
	"app_id": "com.eset.apps.business.ees.windows",
	"version": "7.1.0.0–8.0.0.0"
	},
	{
	"app_id": "com.eset.apps.business.eea.windows",
	"version": ">7.1.0.0"
	}
	]
	}
	--filterFilePath 参数将替换较旧镜像工具版本（随 ESET PROTECT 8.x 一起发布）中使用的 --[illegible] 参数。

--dryRun	当使用此可选参数时，镜像工具不会下载任何文件，但它会生成一个 *.csv* 文件（其中列出将要下载的所有程序包）。 可以在不带强制参数 --intermediateRepositoryDirectory 和 --outputRepositoryDirectory 的情况下使用此参数，例如： • Windows：MirrorTool.exe --repositoryServer AUTOSELECT --dryRun test.csv • Linux：sudo ./MirrorTool --repositoryServer AUTOSELECT --dryRun test.csv ℹ 某些 ESET 安装程序是通用于语言的（语言代码为 multilang），即使在 --filterFilePath 中指定了语言，镜像工具也会将它们列在 *.csv* 文件中。 如果使用 --dryRun 参数以及 --intermediateRepositoryDirectory 和 --outputRepositoryDirectory 参数，镜像工具不会清除 *outputRepositoryDirectory*。
--listUpdatableProducts	列出 Mirror Tool 可以为其下载模块更新的所有 ESET 产品（除非使用了 --excludedProducts） 从版本 Mirror Tool 开始提供该参数：1.0.1294.0 (Windows)；1.0.2226.0 (Linux)。

Mirror Tool 文件夹结构

默认情况下，如果不指定 --updateServer 参数，则 Mirror Tool 会在 HTTP 服务器上创建此文件夹结构：

请勿使用仅采用 HTTP 的镜像服务器

确保本地镜像服务器使用 HTTP 和 HTTPS 协议，或仅使用 HTTPS。如果镜像服务器仅使用 HTTP，则无法使用“软件安装”客户端任务，因为无法从 HTTP 服务器检索 ESET 安全产品的最终用户许可协议。

Mirror Tool 默认文件夹	ESET 安全产品	更新服务器（根据 HTTP 服务器根位置）
mirror/eset_upd/era6	*era6* 镜像文件夹对于这些 ESET 远程管理解决方案是通用的：ERA 6、ESMC 7 和 ESET PROTECT。	要从镜像更新 ESET PROTECT 10，请将更新服务器设置为 *http://your_server_address/mirror/eset_upd/era6*
mirror/eset_upd/ep[版本]	适用于 Windows 的 ESET Endpoint Antivirus/Security 版本 6.x（及更高版本）。每个主版本都有其文件夹，例如 *ep10* 对应于版本 10.x。	*http://your_server_address/mirror/eset_upd/ep10*（对应于版本 10.x 的示例）
mirror/eset_upd/v5	适用于 Windows 的 ESET Endpoint Antivirus/Security 版本 5.x	*http://your_server_address/mirror/eset_upd/v5*

ESET 安全产品策略 Linux/macOS

必须指定 `--updateServer` 参数并创建其他文件夹，才能从 HTTP 镜像更新适用于 Linux/macOS 的 ESET 安全产品（见下文）。

--updateServer	其他 Mirror Tool 文件夹	ESET 安全产品	更新服务器（根据 HTTP 服务器根位置）
http://update.eset.com/eset_upd/businesslinux	*mirror/eset_upd/*BusinessLinux	ESET Endpoint Antivirus 对于 Linux	*http://your_server_address/mirror/eset_upd/BusinessLinux*
http://update.eset.com/eset_upd/serverlinux	*mirror/eset_upd/*LinuxServer	ESET Server Security 对于 Linux	*http://your_server_address/mirror/eset_upd/LinuxServer*
http://update.eset.com/eset_upd/businessmac	*mirror/eset_upd/*BusinessMac	适用于 macOS 的 ESET Endpoint Security 版本 7.x+	*http://your_server_address/mirror/eset_upd/BusinessMac*

语言代码表



```
sudo ./MirrorTool --mirrorType regular \
--intermediateUpdateDirectory /tmp/mirrorTool/mirrorTemp \
--offlineLicenseFilename /tmp/mirrorTool/offline.lf \
--outputDirectory /tmp/mirrorTool/mirror
```

以下是内含所选产品、语言和已启用旧文件下载功能（在 *filter.txt* 文件中定义）的脱机存储库的更高级配

置示例（请参阅上述 `--filterFilePath` 详细信息中的文件内容示例）：

```
sudo ./MirrorTool --repositoryServer AUTOSELECT \
--intermediateRepositoryDirectory /tmp/repoTemp \
--outputRepositoryDirectory /var/lib/tomcat9/webapps/mirrorRepo \
--filterFilePath filter.txt
```

> 建议您从命令行历史记录中删除包含敏感数据（例如，密码）的命令：
> 1.运行 `history` 以查看历史记录中所有命令的列表。
> 2.运行 `history -d line_number`（指定命令的行号）。或者，运行 `history -c` 以删除整个命令行历史记录。

镜像工具和更新设置

- 若要自动下载模块更新，可以创建一个运行镜像工具的计划。若要执行此操作，请打开 Web 控制台并导航至**客户端任务 > 操作系统 > 运行命令。选择要运行的命令行**（包括指向 *MirrorTool.exe* 的路径）和合理的触发器（如每小时都执行 CRON 0 0 * * * ?*您也可以使用 Windows 任务计划程序或 Linux 中的 Cron

- 若要在客户端计算机上配置更新，请创建新策略并将**更新服务器**配置为指向您的镜像地址或共享文件夹。

macOS 上的组件安装

在大部分安装方案中，您需要在不同的计算机上安装不同的 ESET PROTECT 组件，以适应不同的网络架构、符合性能要求，或者出于其他原因这样操作。

> 仅支持 MacOS 作为客户端。适用于 macOS 的 ESET Management 服务器代理和 ESET 产品可以安装在 macOS 上。但 ESET PROTECT 服务器不能安装在 macOS 上。

服务器代理安装 - macOS

在 macOS 上，可以通过以下两种方式安装 ESET Management 服务器代理：

- 远程 – 使用服务器任务**服务器代理部署**。若在远程部署 ESET Management 服务器代理时遇到问题（服务器任务**服务器代理部署**以“失败”状态结束），请参阅服务器代理部署故障排除
- 本地 – 请参阅下面的说明。

先决条件

- 已在服务器计算机上安装 ESET PROTECT 服务器和 ESET PROTECT Web 控制台。
- 已在本地驱动器上创建并准备服务器代理证书
- 已在本地驱动器上准备一个证书颁发机构（只有未签名的证书才需要此操作）。

安装

按照下面的步骤在 macOS 上本地安装 ESET Management 服务器代理组件：

确保满足上面列出的所有安装先决条件。

1. 从 ESET 下载站点或系统管理员处获取安装文件（独立服务器代理安装程序 *.dmg*）。
2. 双击 *Agent-MacOSX-x86_64.dmg* 文件，然后双击 *.pkg* 文件以开始安装。
3. 继续进行安装。在要求时，键入**服务器连接**数据：
   - **服务器主机名**：ESET PROTECT 服务器的主机名或 IP 地址
   - **服务器端口**：服务器代理的端口 – 服务器通信，默认端口为 2222。
   - **使用代理**：如果要使用服务器代理的 HTTP 代理 – 服务器连接，请单击此选项。

此代理设置仅用于 ESET Management 服务器代理与 ESET PROTECT 服务器之间的（复制），不用于缓存更新。
- **代理主机名**：HTTP 代理计算机的主机名或 IP 地址。
- **代理端口**：默认值为 3128。
- **用户名**/**密码**：如果您的代理使用身份验证，则输入它使用的凭据。

可以稍后在策略中更改代理设置。在可以通过代理配置服务器代理 – 服务器连接之前，必须安装代理。

4. 选择对等证书以及该证书的密码。或者，您可以添加一个证书颁发机构。

证书密码中不得包含以下字符：" \ 这些字符在初始化服务器代理期间会导致严重错误。

5. 检查安装位置并单击**安装**。服务器代理将安装在您的计算机上。
6. 可在以下位置找到 ESET Management 服务器代理日志文件：

/Library/Application Support/com.eset.remoteadministrator.agent/Logs/
/Users/%user%/Library/Logs/EraAgentInstaller.log

服务器代理和 ESET PROTECT 服务器之间的通信协议不支持身份验证。任何用于将服务器代理通信转发到需要身份验证的 ESET PROTECT 服务器的代理解决方案将不工作。
如果针对 Web 控制台或服务器代理选择使用非默认端口，可能需要调整防火墙。否则，安装可能会失败。

ISO 映像

ISO 映像文件是您在下载（一体式安装程序类别）ESET PROTECT 安装程序时所采用的格式之一。ISO 映像包含以下内容：

- ESET PROTECT 安装程序包
- 用于每个组件的单独安装程序

当您想要将所有 ESET PROTECT 安装程序保留在一个位置中时，ISO 映像很有用。通过该映像，每当您需要

运行安装时，无需再从 ESET 网站中下载安装程序。当您想在虚拟机上安装 ESET PROTECT 时，ISO 映像也很有用。

DNS 服务记录

设置 DNS 资源记录：

1.在您的 DNS 服务器上（在您的域控制器上的 DNS 服务器），导航到**控制面板** > **管理工具**。

2.选择 DNS 值。

3.在 DNS 管理器中，从树形结构中选择 _tcp 并创建新的**服务位置 (SRV)** 记录。

4.根据 DNS 标准规则，在**服务**字段中输入服务名称，在服务名称前键入下划线 (_)（使用您自己的服务名称，例如 **_era**）。

5.按以下格式在**协议**字段中输入 TCP 协议：_tcp。

6.在**端口号**字段中输入端口 2222。

7.在**提供此服务的主机**字段中，输入 ESET PROTECT 服务器完全限定域名 (FQDN)。

8.依次单击**确定** > **完成**保存记录。该记录将显示在列表中。

验证 DNS 记录：

1.登录域中的任何计算机并打开命令提示 (cmd.exe)。

2.在命令提示中键入 `nslookup`，然后按 **Enter**。

3.键入 `set querytype=srv`，然后按 **Enter**。

4.键入 `_era._tcp.domain.name`，然后按 **Enter**。将正确显示服务位置。

> 在其他计算机上安装ESET PROTECT 服务器时，不要忘记将“提供此服务的主机：”值更改为您的新服务器的 FQDN。

ESET PROTECT 脱机安装方案

要在无法访问 Internet 的环境中安装 ESET PROTECT 及其组件，请按照高级安装说明。Windows 上已安装 ESET PROTECT 进行操作。

在已连接 Internet 的计算机上

1. 创建共享网络文件夹。

2. 将以下安装程序下载到共享文件夹：

- ESET PROTECT 一体式安装程序升级
- 支持的 JDK 程序包Web 控制台需要）。
- ESET Management 服务器代理安装程序
- ESET 安全产品安装程序（例如ESET Endpoint Security

在同一本地网络中的脱机 Windows 计算机上

1. 将网络共享文件夹中的安装程序复制到要安装 ESET PROTECT 的脱机 Windows 计算机。
2. 安装 JDK 程序包。
3. 使用一体式安装程序在 Windows 上安装 ESET PROTECT。在安装期间选择**稍后激活**
4. 使用脱机许可证激活 ESET PROTECT
5. 通过服务器代理安装程序脚本将 ESET Management 服务器代理部署到脱机环境中的计算机。修改安装脚本，以使用新的 URL 访问共享网络文件夹中的服务器代理安装包。
6. 使用软件安装任务将 ESET 安全产品部署到工作站。选择**<Choose package>**并从本地存储库中选择用于安装程序包的自定义 URL
7. 使用脱机许可证激活托管端点
8. 禁用 ESET LiveGrid®

强烈建议您使用本地更新库使脱机 ESET 基础架构保持更新。定期更新 ESET 安全产品模块。如果模块未更新，则 ESET PROTECT Web 控制台将计算机标记为**未更新**。若要使此 Web 控制台警告静音，请单击列表中的计算机，然后从右键菜单中选择**静音**

有关升级 ESET PROTECT 的说明，请参阅在脱机环境中升级 ESET PROTECT 组件

升级过程

升级 ESET PROTECT 服务器和其他 ESET PROTECT 组件有不同方法。另请参阅迁移和重新安装过程

在升级到 ESET PROTECT 10.0 之前，请确保您拥有支持的操作系统
如果已安装不受支持的较旧数据库MySQL 5.5 或 Microsoft SQL 2008/2012请升级数据库到兼容的数据库版本，然后再升级 ESET PROTECT 服务器。

升级自 ERA 5.x/6.5 或 ESMC 7.0/7.1

如果您有 ERA 5.x/6.x 或 ESMC 7.0/7.1

- 不支持直接升级到 ESET PROTECT 10.0
- 执行全新安装 ESET PROTECT 10.0

可以从 ESMC 7.2 及更高版本直接升级到 ESET PROTECT 10.0

从 ESMC 7.2 或较早的 ESET PROTECT 版本升级到 ESET PROTECT 10.0

选择其中一个升级过程：

升级过程	操作系统	注释
Web 控制台中的组件升级任务	Windows/Linux	
ESET PROTECT 10.0 一体式安装程序升级	Windows	如果现有安装是通过一体式安装程序（您有 Microsoft SQL 数据库和 Apache Tomcat 的默认安装）执行的，一体式安装程序是建议的升级选项。
基于组件的手动升级	Linux	适用于高级用户的 Linux 说明。
升级 ESET PROTECT 虚拟设备	Linux (虚拟设备)	

若要查看您运行的每个 ESET PROTECT 组件的版本，只需查验您的 ESET PROTECT 服务器版本即可。导航到 ESET PROTECT Web 控制台中的关于页面，然后查看所有 ESET PROTECT 组件版本的列表。

ESET PROTECT组件升级任务

升级之前的建议

建议您使用 ESET PROTECT Web 控制台中提供的ESET PROTECT组件升级任务来升级您的 ESET PROTECT 基础架构。在更新之前，请仔细阅读此处的说明。

如果组件升级在运行 ESET PROTECT 服务器或 Web 控制台的计算机上出现故障，则可能无法远程登录到 Web 控制台。建议您先配置对服务器计算机的物理访问，然后再执行此升级。如果您无法安排对该计算机的物理访问，请确保您能通过远程桌面使用管理权限登录到该计算机。建议您在执行此操作之前，先备份您的 ESET PROTECT 服务器数据库和移动设备连接器数据库。若要备份您的虚拟设备，请创建一个快照或者克隆您的虚拟机。

您是否从 ESMC 虚拟设备升级？

ESET PROTECT 服务器实例是否已安装在故障转移群集上？

如果您的 ESET PROTECT 服务器实例安装在故障转移群集上，您必须手动升级每个群集节点上的 ESET PROTECT 服务器组件。在升级 ESET PROTECT 服务器后，请运行组件升级任务来升级基础架构中的其余组件（例如，客户端计算机上的 ESET Management 服务器代理）。

只可以从 ESMC 版本 7.2 及更高版本升级到 ESET PROTECT 10.0。
当新版本的 ESET PROTECT 服务器可用时，ESET PROTECT 10 会自动通知您。
先备份以下数据，然后再运行升级：
- 所有证书（证书颁发机构、服务器证书和服务器代理证书）
- 将您的证书颁发机构证书从旧的 ESET PROTECT 服务器导出到 *.der* 文件，然后将它保存到外部存储中。
- 从旧的 ESET Management 服务器导出您的对等证书（用于 ESET PROTECT 服务器代理、ESET PROTECT 服务器）和私钥 *.pfx* 文件，然后将它保存到外部存储中。
- 您的 ESMC/ESET PROTECT 数据库。如果已安装不受支持的较旧数据库、MySQL 5.5 或 Microsoft SQL 2008/2012，请升级数据库到兼容的数据库版本，然后再升级 ESET PROTECT 服务器。

在升级到 ESET PROTECT 10.0 之前，请确保您拥有支持的操作系统。
要升级 ESET 安全产品，请使用最新安装程序包运行软件安装任务，以通过现有产品安装最新版本。

建议的升级过程

1. 升级 ESET PROTECT 服务器 – 仅选择使用 ESET PROTECT 服务器作为 **ESET PROTECT 组件升级**任务目标的计算机。

2. 选择一些客户端计算机（作为测试样本 – 每个操作系统和位数至少一个客户端）并在其上运行 **ESET PROTECT 组件升级**。

建议您使用 ESET Bridge HTTP 代理（或任何其他已启用缓存的透明 Web 代理），以限制网络负载。测试客户端计算机将触发安装程序的下载/缓存。再次运行任务时，将直接从缓存将安装程序分发到客户端计算机。

3. 具有已升级 ESET Management 服务器代理的计算机成功连接到 ESET PROTECT 服务器后，继续升级其余的客户端。

要在网络中的所有托管计算机上升级 ESET Management 服务器代理，请选择静态组**全部**作为 **ESET PROTECT 组件升级**任务的目标。该任务将跳过已经运行最新 ESET Management 服务器代理的计算机。ESET PROTECT 10.0 支持在托管计算机上自动升级 ESET Management 服务器代理。

组件已自动升级：

- ESET PROTECT 服务器
- ESET Management 服务器代理
- ESET PROTECT Web 控制台 – 仅当在 Windows 和 Linux 发行版（包括 ESET PROTECT 虚拟设备）中将 Apache Tomcat 安装到其默认安装文件夹（例如：*/var/lib/tomcat8/webapps/*, */var/lib/tomcat7/webapps/*, */var/lib/tomcat/webapps/*）时才适用。

Web 控制台升级限制

- Apache Tomcat 在 ESET PROTECT Web 控制台升级过程中不会通过组件升级任务进行升级。
- 如果 Apache Tomcat 安装在自定义位置，则 ESET PROTECT Web 控制台升级不会工作。
- 如果安装了自定义版本的 Apache Tomcat（非 Tomcat 服务的手动安装），则通过一体式安装程序或通过组件升级任务的后续 ESET PROTECT Web 控制台升级不受支持。

- ESET PROTECT 移动设备连接器

需要手动升级的组件：

ESET 组件

- ESET Rogue Detection Sensor – 使用软件安装任务进行升级。或者，在较早版本上安装最新版本（按照适用于 Windows 或 Linux 的说明操作）。如果通过 ESMC 7.2 及更高版本安装了 RD Sensor，则无需升级它，因为没有新版 RD Sensor。

第三方组件

除了 ESET 组件，ESET PROTECT 还使用需要手动升级的第三方组件。

在 ESET PROTECT Web 控制台中，依次单击**快速链接** > **服务器组件**，以查看更高版本可用的第三方组件。

- 建议您尽快安装最新版本的第三方组件。最新可用版本可能因用于运行 ESET PROTECT 服务器的操作系统而异。
- ESET PROTECT 虚拟设备不会报告第三方组件的可用升级。

ESET PROTECT Web 控制台建议升级低于下列版本的各版本：

第三方组件：	版本：	备注：
Microsoft SQL Server	2019（内部版本 15.0.4261.0）	确定 SQL Server 数据库引擎的版本，然后安装最新的累积更新
MySQL	8.0.0.0	在 ESET PROTECT Web 控制台中，依次单击**帮助** > **关于**以查看已安装的数据库版本。
操作系统	Windows Server 2016	ESET PROTECT 不会报告 Linux 的可用更新。
Apache Tomcat	9.0.65	确定已安装的 Apache Tomcat 版本： • Windows - 导航到 *C:\Program Files\Apache Software Foundation\[Tomcat 文件夹]* 使用文本编辑器打开 *RELEASE-NOTES* 文件以查看版本号。 • Linux - 运行终端命令：`tomcat version`
Java	17.0	确定已安装的 Java 版本： • Windows - 打开命令提示，然后运行以下命令：`java -version` • Linux - 运行终端命令：`java -version`

ESET PROTECT 移动设备管理/连接器 (MDM/MDC) 组件（仅限本地）计划结束生命周期。阅读更多建议您迁移到 Cloud MDM

按照第三方组件的升级说明进行操作：

- 数据库服务器
- 操作系统
- Apache Tomcat
- Java 运行时环境

Apache HTTP Proxy 用户

从 ESET PROTECT 10.0 开始ESET Bridge 将替代 Apache HTTP Proxy Apache HTTP Proxy 已受有限支持。如果您使用 Apache HTTP Proxy建议您迁移到 ESET Bridge

故障排除

- 验证是否可以从已升级的计算机访问 ESET PROTECT 存储库
- 如果至少有一个组件已升级到较新版本，则重新运行 ESET PROTECT 组件升级任务将不起作用。
- 如果 ESET PROTECT Web 控制台不加载或在登录过程中出现错误，请参阅 Web 控制台故障排除
- 如果出现故障的原因尚未弄清楚，可以手动升级组件。请参阅我们的适用于 Windows 或 Linux 的说明。
- 有关解决升级问题的更多建议，请参阅常规故障排除信息

使用 ESET PROTECT 10.0 一体式安装程序进行升级

使用 ESET PROTECT 10.0 一体式安装程序升级 ESMC 7.2 或将较早 ESET PROTECT 版本升级到最新的 ESET PROTECT 10.0。

如果现有安装是通过一体式安装程序（您有 Microsoft SQL 数据库和 Apache Tomcat 的默认安装）执行的，一体式安装程序是建议的升级选项。

默认情况下，ESET PROTECT 10.0 一体式安装程序将安装 Microsoft SQL Server Express 2019。

- 如果使用的是旧版 Windows Server 2012 或 SBS 2011，则将默认安装 Microsoft SQL Server Express 2014。
- 安装程序会自动生成一个用于数据库验证的随机密码（存储在 *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini* 中）。

Microsoft SQL Server Express 的每个关系数据库具有 10 GB 大小限制。不建议使用 Microsoft SQL Server Express。

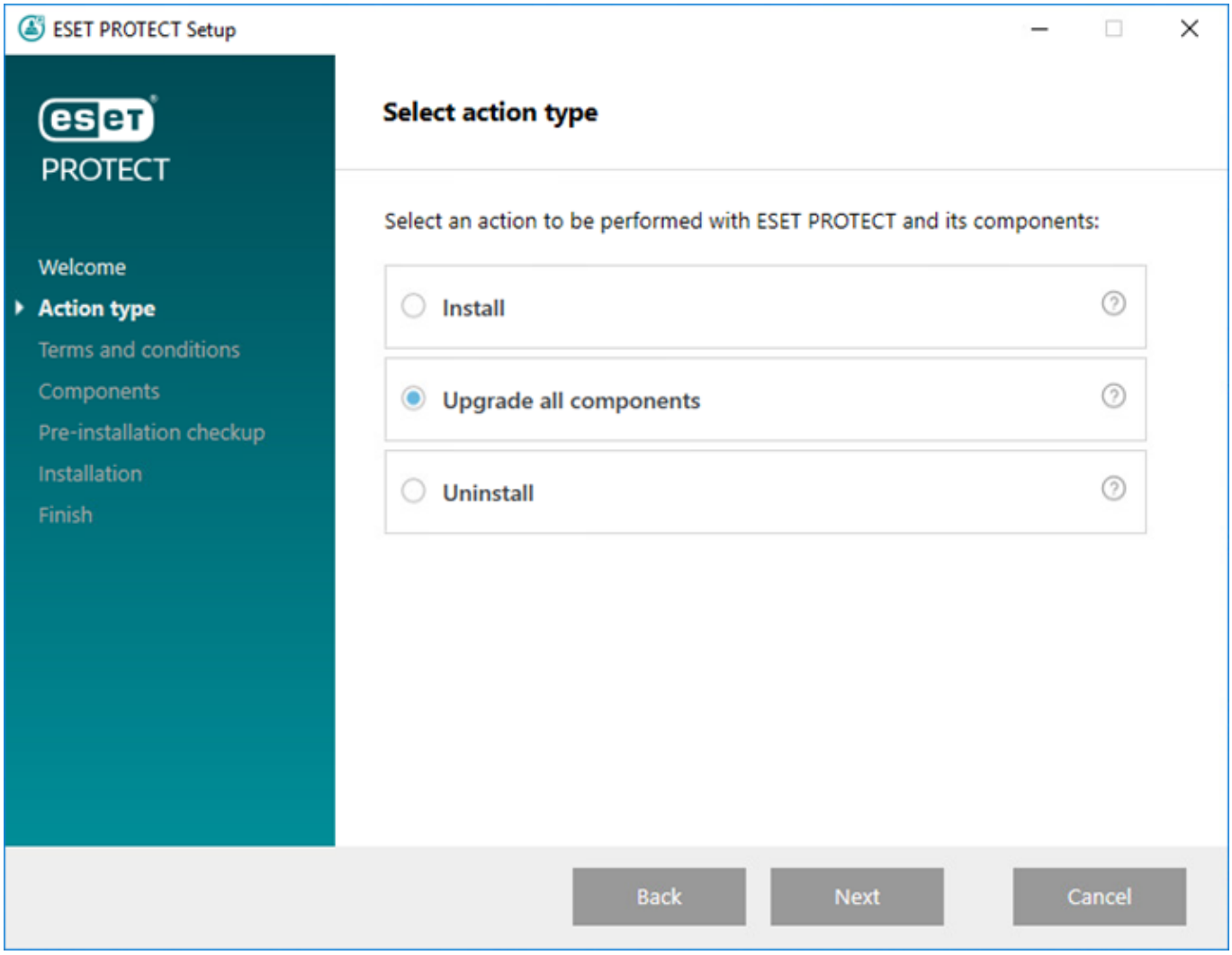
- 在企业环境或大型网络中。
- 如果要将 ESET PROTECT 与 ESET Inspect 一起使用。

只可以从 ESMC 版本 7.2 及更高版本升级到 ESET PROTECT 10.0。
先备份以下数据，然后再运行升级：

- 所有证书（证书颁发机构、服务器证书和服务器代理证书）
- 将您的证书颁发机构证书从旧的 ESET PROTECT 服务器导出到 *.der* 文件，然后将它保存到外部存储中。
- 从旧的 ESET Management 服务器导出您的对等证书（用于 ESET PROTECT 服务器代理、ESET PROTECT 服务器）和私钥 *.pfx* 文件，然后将它保存到外部存储中。
- 您的 ESMC/ESET PROTECT 数据库。 如果已安装不受支持的较旧数据库（MySQL 5.5 或 Microsoft SQL 2008/2012），请升级数据库到兼容的数据库版本，然后再升级 ESET PROTECT 服务器。

在升级到 ESET PROTECT 10.0 之前，请确保您拥有支持的操作系统。

1. 运行 *Setup.exe*。
2. 选择相应语言，然后单击**下一步**。
3. 选择**升级所有组件**，然后单击**下一步**。



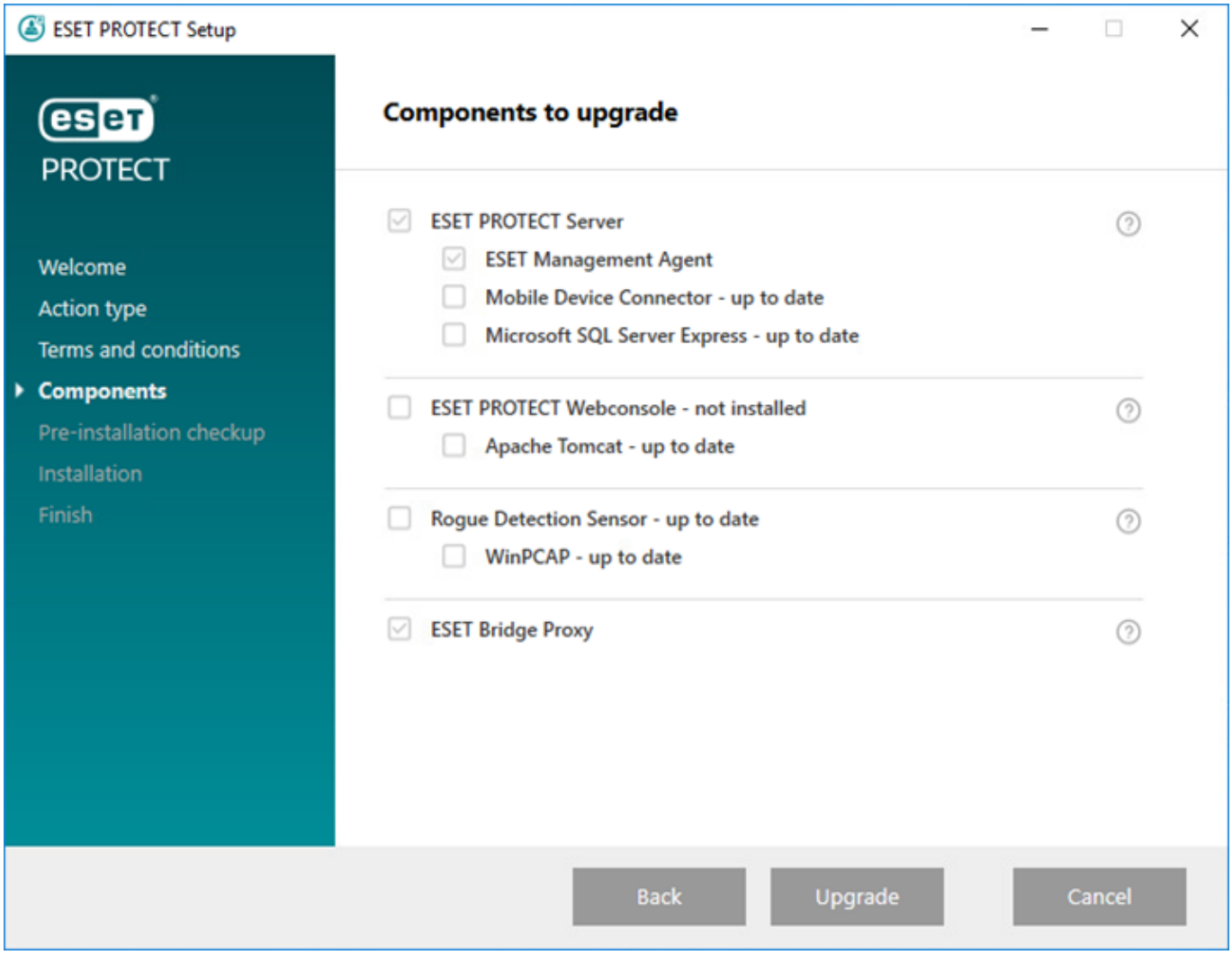
4.阅读**最终用户许可协议**，接受它并单击**下一步**。

5.在**组件**中，查看可以升级的 ESET PROTECT 组件，然后单击**下一步**。

Apache Tomcat 和 Web 控制台升级限制

- 如果安装了自定义版本的 Apache Tomcat（非 ESET PROTECT 服务的手动安装），则通过一体式安装程序或通过组件升级任务的后续 ESET PROTECT Web 控制台升级不受支持。
- Apache Tomcat 升级会删除位于以下位置的 *era* 文件夹：*C:\Program Files\Apache Software Foundation\Tomcat* 文件夹 *]\webapps*. 如果使用 *era* 文件夹存储其他数据，请确保在升级之前先备份相应数据。
- 如果 *C:\Program Files\Apache Software Foundation\Tomcat* 文件夹 *]\webapps* 中包含其他数据（而非 *era* 和 *ROOT* 文件夹），则 Apache Tomcat 升级将不会进行，而仅会升级 Web 控制台。
- Web 控制台和 Apache Tomcat 升级会清除脱机帮助文件。如果使用 ESMC 或较早 ESET PROTECT 版本的脱机帮助，请在升级后为 ESET PROTECT 10.0 重新创建它，以确保您有匹配 ESET PROTECT 版本的最新脱机帮助。

如果在已装有 Apache HTTP Proxy 的 Windows 计算机上运行一体式安装程序，则该安装程序会改为自动卸载 Apache HTTP Proxy 并安装 ESET Bridge。



6.按照**安装前检查**进行操作，以确保您的系统满足所有先决条件。

7.单击**升级**，以开始 ESET PROTECT 升级。升级可能需要一些时间，具体取决于您的系统和网络配置。

8.升级完成后，单击**完成**。

9.升级 ESET PROTECT 后，使用组件升级任务在托管计算机上升级 ESET Management 服务器代理。ESET PROTECT 10.0 支持在托管计算机上自动升级 ESET Management 服务器代理。

数据库服务器备份/升级

ESET PROTECT 使用数据库来存储客户端数据。以下部分详细介绍了 ESET PROTECT 服务器（或 ESMC 服务器）数据库或 MDM 数据库的备份和升级。

- 如果您没有已配置的用于 ESET PROTECT 服务器的数据库，**Microsoft SQL Server Express** 已包含在安装程序中。 默认情况下，ESET PROTECT 10.0 一体式安装程序将安装 Microsoft SQL Server Express 2019。

o如果使用的是旧版 Windows Server 2012 或 SBS 2011，将默认安装 Microsoft SQL Server Express 2014。

o安装程序会自动生成一个用于数据库验证的随机密码（存储在 *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini* 中）。

Microsoft SQL Server Express 的每个关系数据库具有 10 GB 大小限制。不建议使用 Microsoft SQL Server Express
- 在企业环境或大型网络中。
- 如果要将 ESET PROTECT 与 ESET Inspect 一起使用。

- 如果已安装不受支持的较旧数据库MySQL 5.5 或 Microsoft SQL 2008/2012请升级数据库到兼容的数据库版本，然后再升级 ESET PROTECT 服务器。

另请参阅 ESET PROTECT 数据库迁移

必须满足 Microsoft SQL Server 的以下要求：

- 安装受支持版本的 Microsoft SQL Server。在安装过程中选择**混合模式**身份验证。

- 如果已安装 Microsoft SQL Server则将身份验证设置为**混合模式(SQL Server 身份验证和 Windows 身份验证)**。若要执行此操作，请按照此知识库文章中的说明操作。如果要使用 **Windows 身份验证**来登录 Microsoft SQL Server请按照本知识库文章中的步骤进行操作。

- 允许到 SQL Server 的 TCP/IP 连接。若要执行此操作，请按照此知识库文章（位于 **II.允许到 SQL 数据库的 TCP/IP 连接**部分中）中的说明操作。

- 若要配置、管理、运行 Microsoft SQL Server数据库和用户），请下载 SQL Server Management Studio (SSMS)
- 在域控制器（例如Windows SBS/Essentials上不要安装 SQL Server。建议您在其他服务器上安装 ESET PROTECT或者在安装期间不选择 SQL Server Express 组件（这要求您使用现有 SQL 或 MySQL Server 来运行 ESET PROTECT 数据库）。

数据库服务器备份和还原

所有 ESET PROTECT 信息和设置都存储在数据库中。建议您定期备份数据库，以防止数据丢失。以后将 ESET PROTECT 迁移到新服务器时，可以使用该备份。请针对您的数据库参考下面的相应部分：

- 即使产品名称已从 ESET Security Management Center 更改为 ESET PROTECT数据库和日志文件的名称也保持不变。
- 如果使用 ESET PROTECT 虚拟设备，请按照虚拟设备数据库备份说明进行操作。

Microsoft SQL 备份示例

若要将 Microsoft SQL 数据库备份到文件，请按照以下所示的示例进行操作：

这些示例仅适用于使用默认设置的情况（例如，默认的数据库名称和数据库连接设置）。需要自定义您的备份脚本以适配您对默认设置所做的任何更改。
您需要具有足够权限，才能运行以下命令。如果不使用本地管理员用户帐户，则需要更改备份路径，例如更改为 *'C:\USERS\PUBLIC\BACKUPFILE*

一次数据库备份

在 Windows 命令提示符下执行此命令，将备份创建到名为 **BACKUPFILE** 的文件：

```
SQLCMD -S HOST\ERASQL -
Q "BACKUP DATABASE ERA_DB TO DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'"
```

> 在此示例中，**HOST** 代表 IP 地址或主机名，**ERASQL** 代表 Microsoft SQL 服务器实例的名称。您可以（如果使用 Microsoft SQL 数据库）在自定义命名 SQL 实例上安装 ESET PROTECT 服务器。在此情况下相应地修改备份脚本。

使用 SQL 脚本的常规数据库备份

选择以下 SQL 脚本中的其中一个：

a)创建常规备份并基于创建日期存储这些备份：

```
@ECHO OFF

SQLCMD.EXE -S HOST\ERASQL -d ERA_DB -E -
Q "BACKUP DATABASE ERA_DB TO DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'

  WITH NOFORMAT,INIT, NAME = N'ERA_DB', SKIP, NOREWIND, NOUNLOAD, STOP_ON_ERROR, CHE
CKSUM, STATS=10"

REN BACKUPFILE BACKUPFILE-
[%DATE:~10,4%%DATE:~4,2%%DATE:~7,2%_T%TIME:~0,2%%TIME:~3,2%].bac
```

b)将您的备份附加到一个文件：

```
@ECHO OFF

SQLCMD.EXE -S HOST\ERASQL -d ERA_DB -E -
Q "BACKUP DATABASE ERA_DB TO DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'

   WITH NOFORMAT, NOINIT, NAME = N'ERA_DB', SKIP, NOREWIND, NOUNLOAD, STOP_ON_ERROR,
 CHECKSUM, STATS=10"
```

Microsoft SQL 恢复

若要从文件中还原 Microsoft SQL 数据库，请按照以下所示的示例进行操作：

```
SQLCMD.EXE -S HOST\ERASQL -d ERA_DB -E -
Q "RESTORE DATABASE ERA_DB FROM DISK = N'C:\USERS\ADMINISTRATOR\DESKTOP\BACKUPFILE'"
```

MySQL 备份

若要将 MySQL 数据库备份到文件，请按照以下所示的示例进行操作：

```
mysqldump --host HOST --disable-keys --extended-insert --routines -u ROOTLOGIN -
p DBNAME -r BACKUPFILE
```

在此示例中，**HOST** 代表 MySQL 服务器的 IP 地址或主机名、**ROOTLOGIN** 代表 MySQL 服务器的根帐户，**DBNAME** 代表 ESET PROTECT 数据库名称。

MySQL 还原

若要从文件中还原 MySQL 数据库，请按照以下所示的示例进行操作：

```
mysql --host HOST -u ROOTLOGIN -p DBNAME < BACKUPFILE
```

有关 Microsoft SQL Server 备份的详细信息，请访问 Microsoft TechNet 网站。有关 MySQL Server 备份的详细信息，请访问 MySQL 文档网站

数据库服务器升级

按照下面的说明操作，以将现有数据库服务器实例升级为要用于 ESET PROTECT 服务器数据库的更高版本：

1. 停用连接到您将升级的数据库服务器的所有正在运行的 ESMC/ESET PROTECT 服务器或 代理服务。此外，停用可能连接到数据库服务器实例的任何其他应用程序。

2. 在继续操作之前，安全地备份所有相关数据库。

3. 执行数据库服务器升级：

SQL Server Windows

- 按照将 Microsoft SQL Express 数据库升级到最新版本的知识库文章中的说明进行操作。
- 或者，按照数据库供应商的说明进行操作：https://msdn.microsoft.com/en-us/library/bb677622.aspx
- Linux 上的 Microsoft SQL Server 不受支持。但可以将 Linux 上的 ESET PROTECT 服务器连接到 Windows 上的 Microsoft SQL Server

MySQL Server Windows 和 Linux

- 从 MySQL 5.6 升级到版本 5.7
- 从 MySQL 5.7 升级到版本 8

4. 启动 ESET PROTECT 服务器服务，检查跟踪日志以验证数据库连接是否在正常运行。

升级故障转移群集中安装的 ESMC/ESET PROTECT (Windows)

如果在 Windows 的故障转移群集环境中安装了 ESMC/ESET PROTECT 服务器，请按照下面的步骤操作以升级到最新的 ESET PROTECT

确保您拥有支持的操作系统

1. 停用群集管理器中的 ESMC/ESET PROTECT 服务器群集角色。确保所有群集节点上的服务（**ESET**

Security Management Center Server 或 **ESET PROTECT Server**）都已停止。

2. 使群集共享磁盘在 node1 上在线，然后通过执行最新的 *.msi* 安装程序来手动升级服务器组件（就像组件安装一样）。

3. 在安装（升级）完成之后，确保停用 **ESET PROTECT Server** 服务。

4. 使群集共享磁盘在 node2 上在线，然后按照步骤 2 中的相同方法升级服务器组件。

5. 所有群集节点上的 ESET PROTECT 服务器都已更新后，启动群集管理器中的 **ESET PROTECT 服务器角色**。

6. 通过在所有群集节点上执行最新的 *.msi* 安装程序，手动升级 ESET Management 服务器代理。

7. 在 ESET PROTECT Web 控制台中，查看所有节点的代理服务器和服务器版本是否报告已升级到的最新版本。

升级 Apache Tomcat

Apache Tomcat 是运行 ESET PROTECT Web Console 所需的必需组件。

如果您要升级到最新版本的 ESET PROTECT，或者很长一段时间未升级 Apache Tomcator，您应该考虑将 Apache Tomcat 升级到最新版本。将面向公众的服务（包括 Apache Tomcat 及其附属组件）保持为最新状态会降低您环境的安全风险。

若要升级 Apache Tomcat，请按照适合您操作系统的说明进行操作：

- Windows 说明（最新的 ESET PROTECT 一体式安装程序） – 如果现有 Apache Tomcat 安装是通过一体式安装程序执行的，这是建议的升级选项。
- Windows 说明（手动安装） – 如果手动执行现有 Apache Tomcat 安装或者没有最新的 ESET PROTECT 一体式安装程序，则手动升级 Apache Tomcat。
- Linux 说明

使用一体式安装程序升级 Apache Tomcat (Windows)

Apache Tomcat 是运行 ESET PROTECT Web Console 所需的必需组件。 使用此方法来通过使用最新的 ESET PROTECT 10.0 一体式安装程序升级 Apache Tomcat。如果现有 Apache Tomcat 安装是通过一体式安装程序执行的，这是建议的升级选项。 此外，也可以手动升级 Apache Tomcat。

升级之前

备份以下文件：

C:\Program Files\Apache Software Foundation\[Tomcat 文件夹]\.keystore
C:\Program Files\Apache Software Foundation\[Tomcat 文件夹]\conf\server.xml
C:\Program Files\Apache Software Foundation\[Tomcat 文件夹]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties

如果使用的是 *Tomcat* 文件夹中的自定义 SSL 证书存储，也请备份该证书。

Apache Tomcat 和 Web 控制台升级限制

- 如果安装了自定义版本的 Apache Tomcat（Tomcat 服务的手动安装），则通过一体式安装程序或通过组件升级任务的后续 ESET PROTECT Web 控制台升级不受支持。
- Apache Tomcat 升级会删除位于以下位置的 *era* 文件夹： *C:\Program Files\Apache Software Foundation\[Tomcat* 文件夹 *]\webapps*. 如果使用 *era* 文件夹存储其他数据，请确保在升级之前先备份相应数据。
- 如果 *C:\Program Files\Apache Software Foundation\[Tomcat* 文件夹 *]\webapps* 中包含其他数据（而非 *era* 和 *ROOT* 文件夹），则 Apache Tomcat 升级将不会进行，而仅会升级 Web 控制台。
- Web 控制台和 Apache Tomcat 升级会清除脱机帮助文件。如果使用 ESMC 或较早 ESET PROTECT 版本的脱机帮助，请在升级后为 ESET PROTECT 10.0 重新创建它，以确保您有匹配 ESET PROTECT 版本的最新脱机帮助。

升级过程

1. 从 ESET 网站下载 ESET PROTECT 一体式安装程序，然后解压缩该下载文件。

2. 如果要安装最新版本的 Apache Tomcat但一体式安装程序包含较旧版本的 Apache Tomcat此步骤可选 – 如果不需要最新版本的 Apache Tomcat请跳到步骤 4）：

   a.打开 *x64* 文件夹，然后导航到 *installers* 文件夹。

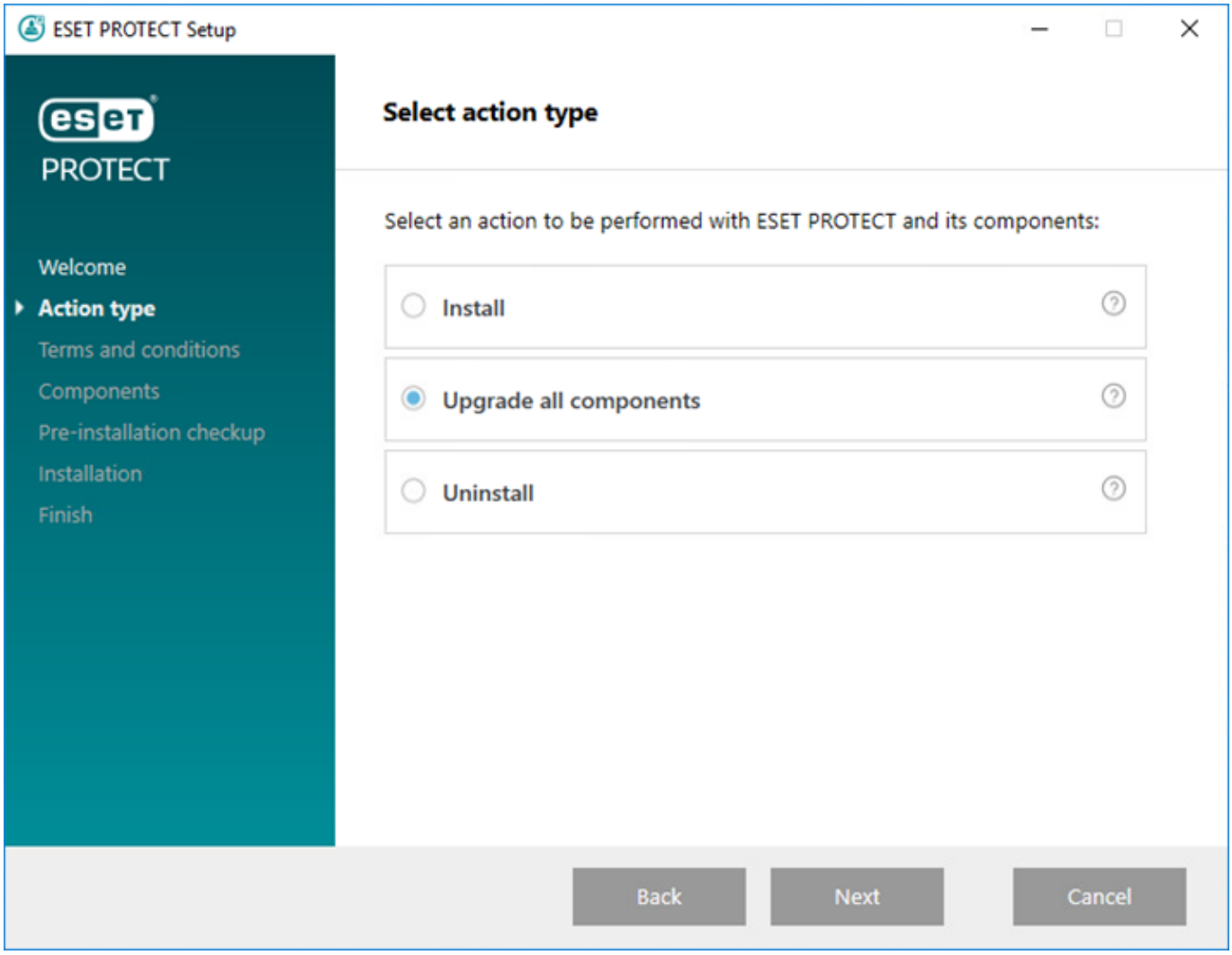
   b.删除位于 *installers* 文件夹中的 *apache-tomcat-9.0.x-windows-x64.zip* 文件.

   c.下载 Apache Tomcat 9 64 位 Windows zip 程序包。

   d.将下载的 zip 程序包移动到 *installers* 文件夹。

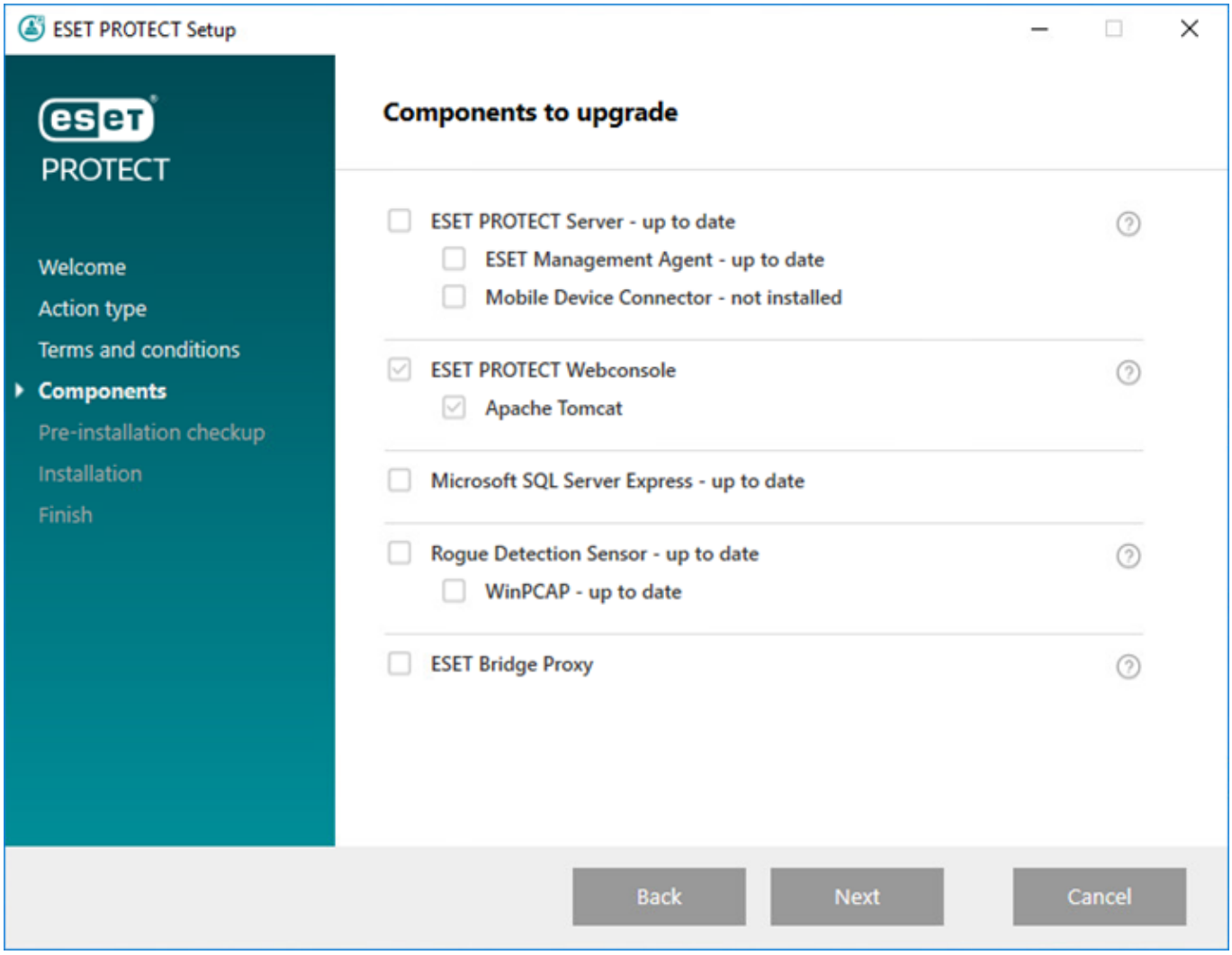
3. 要启动一体式安装程序，请双击 *Setup.exe* 文件，然后在**欢迎**屏幕中单击**下一步**。

4. 选择**升级所有组件**，然后单击**下一步**。



5. 接受 EULA 后，单击**下一步**。

6. 如果升级可用，将自动检测一体式安装程序：在可升级的 ESET PROTECT 组件旁边有复选框。单击**下一步**。



7. 在计算机上选择 Java 安装 Apache Tomcat 需要 64 位 Java/OpenJDK 如果在系统上安装了多个 Java 版本，建议您卸载较早的 Java 版本并仅保留最新的受支持的 Java 版本。

从 2019 年 1 月开始，面向企业、商业或生产用途的 Oracle JAVA SE 8 公开更新将需要商业许可证。如果不购买 JAVA SE 订阅，可以使用本指南来转换为免费替代方案。请参阅 JDK 的受支持版本

8. 单击**升级**以完成该升级，然后单击**完成**

9. 如果在不是 ESET PROTECT 服务器的其他计算机上安装了 Web 控制台：

   a. 停用 Apache Tomcat 服务。导航到**启动 > 服务** > 右键单击 Apache Tomcat 服务并选择**停止**

   b.将 *EraWebServerConfig.properties* 文件（从步骤 1）恢复到其原始位置。

   c. 启动 Apache Tomcat 服务：导航到**启动 > 服务** > 右键单击 Apache Tomcat 服务并选择**启动**

10. 连接到 ESET PROTECT Web 控制台并验证是否正确加载了 Web 控制台。

另请参见企业解决方案的 Web 控制台配置或低性能系统

故障排除

如果升级 Apache Tomcat 失败，请卸载 Apache Tomcat然后重新安装它并应用步骤 1 中的配置。

手动升级 Apache Tomcat (Windows)

Apache Tomcat 是运行 ESET PROTECT Web Console 所需的必需组件。 如果手动执行现有 Apache Tomcat 安装或者没有最新的 ESET PROTECT 一体式安装程序，则手动升级 Apache Tomcat。

如果安装了自定义版本的 Apache Tomcat（Tomcat 服务的手动安装），则通过一体式安装程序或通过组件升级任务的后续 ESET PROTECT Web 控制台升级不受支持。

升级之前

- Apache Tomcat 需要 64 位 Java/OpenJDK。如果在系统上安装了多个 Java 版本，建议您卸载较早的 Java 版本并仅保留最新的受支持的 Java 版本。

从 2019 年 1 月开始，面向企业、商业或生产用途的 Oracle JAVA SE 8 公开更新将需要商业许可证。如果不购买 JAVA SE 订阅，可以使用本指南来转换为免费替代方案。请参阅 JDK 的受支持版本。

- 查看当前使用的是哪一个版本的 Apache Tomcat。

  a.导航到 Apache Tomcat 安装文件夹：
  C:\Program Files\Apache Software Foundation\[Tomcat 文件夹]

  b.使用文本编辑器打开 RELEASE-NOTES 文件，然后检查版本号（例如 9.0.34）。

  c.如果较新支持版本可用，请执行升级。

升级过程

1. 停用 Apache Tomcat 服务。导航到**启动 > 服务** > 右键单击 Apache Tomcat 服务并选择**停止**。

如果 *Tomcat7w.exe* 正在 Windows 通知区域中运行，请关闭它。

2. 备份以下文件：

   C:\Program Files\Apache Software Foundation\[Tomcat 文件夹]\.keystore
   C:\Program Files\Apache Software Foundation\[Tomcat 文件夹]\conf\server.xml
   C:\Program Files\Apache Software Foundation\[Tomcat 文件夹]\webapps\era\WEB-INF\classes\sk\eset\era\g2webconsole\server\modules\config\EraWebServerConfig.properties

如果使用的是 *Tomcat* 文件夹中的自定义 SSL 证书存储，也请备份该证书。

3. 卸载当前版本的 Apache Tomcat。

4. 删除系统上仍存在的以下文件夹：

C:\Program Files\Apache Software Foundation\[Tomcat 文件夹]

5. 从 https://tomcat.apache.org 下载最新支持版本的 Apache Tomcat 安装程序文件（32 位/64 位 Windows Service Installer）`apache-tomcat-[版本].exe`。

6. 安装已下载的较新版本的 Apache Tomcat。

   - 如果已安装更多 Java 版本，请在安装期间选择最新 Java 的路径。

- 安装完成后，请取消选中 **运行 Apache Tomcat** 旁边的复选框。

7. 将 *.keystore*、*server.xml* 和自定义证书恢复到其原始位置。

8. 打开 *server.xml* 文件，并确保 *keystoreFile* 路径正确无误（如果已升级到主版本更高的 Apache Tomcat，则更新该路径）：

keystoreFile="C:\Program Files\Apache Software Foundation\[Tomcat 文件夹]\.keystore"

9. 确保为 ESET PROTECT Web 控制台正确配置了 Apache Tomcat 的 HTTPS 连接。

10. 部署 ESET PROTECT Web控制台（Web 控制台安装 - Windows）。

11. 将 *EraWebServerConfig.properties* 恢复到其原始位置。

12. 运行 Apache Tomcat 并设置正确的 Java VM。

a.导航到文件夹 *C:\Program Files\Apache Software Foundation\[Tomcat 文件夹]\bin*，然后运行 *Tomcat9w.exe*。

b.在**常规**选项卡中，将**启动类型**设置为**自动**，然后按下**启动**。

c.单击 **Java** 选项卡、取消选中**使用默认值**、确保 **Java 虚拟机**包含 *jvm.dll* 文件的路径（参阅所示知识库说明），然后单击**确定**。

13. 连接到 ESET PROTECT Web 控制台并验证是否正确加载了 Web 控制台。

另请参见企业解决方案的 Web 控制台配置或低性能系统。

故障排除

- 如果未成功设置 Apache Tomcat 的 HTTPS 连接，您可以跳过此步骤，暂时使用 HTTP 连接。
- 如果 Apache Tomcat 的升级失败，请安装您的原始版本并应用步骤 2 中的配置。
- Web 控制台和 Apache Tomcat 升级会清除脱机帮助文件。如果使用 ESMC 或较早 ESET PROTECT 版本的脱机帮助，请在升级后为 ESET PROTECT 10.0 重新创建它，以确保您有匹配 ESET PROTECT 版本的最新脱机帮助。

升级 Apache Tomcat 和 Java (Linux)

Apache Tomcat 是运行 ESET PROTECT Web Console 所需的必需组件。

升级之前

1. 执行以下命令以查看安装的 Apache Tomcat 版本（在某些情况下，文件夹名为 `tomcat7` 或 `tomcat8`）：

```
cd /usr/share/tomcat/bin && ./version.sh
```

2. 如果有更高版本：

a.确保更高版本受支持

b.备份 Tomcat 配置文件 */etc/tomcat7/server.xml*

升级过程

1. 运行以下命令以停止 Apache Tomcat 服务（在某些情况下，服务名称为 `tomcat7`）

```
sudo systemctl stop tomcat
```

2. 升级 Apache Tomcat 和 Java

> 下面的示例程序包名称可能不同于您的 Linux 发行版存储库程序包。Linux 发行版的默认存储库可能不包含最新支持版本的 Apache Tomcat 和 Java。

Linux 发行版	终端命令
Debian 和 Ubuntu 发行版	`sudo apt-get update` `sudo apt-get install openjdk-17-jdk tomcat9`
CentOS 和 Red Hat 发行版	`yum update` `yum install java-17-openjdk tomcat`
SUSE Linux	`zypper refresh` `sudo zypper install java-17-openjdk tomcat9`

3. 将 */etc/tomcat9/server.xml* 文件替换为备份中的 *server.xml* 文件。

4. 打开 *server.xml* 文件，并确保 *keystoreFile* 路径正确无误。

5. 确保正确配置了 Apache Tomcat 的 HTTPS 连接

另请参见企业解决方案的 Web 控制台配置或低性能系统

6. 如果已升级 Java，请按照下面的步骤操作来配置 Apache Tomcat，以使用系统上安装的最新 Java 程序包：

a.导航到 Apache Tomcat 配置文件夹：

```
cd /usr/share/tomcat/conf/
```

b.使用文本编辑器打开 *tomcat.conf* 文件：

```
nano tomcat.conf
```

c.在 `JAVA_HOME` 变量中更新最新安装的 Java 程序包的路径（该路径因在系统中安装的 Java 程序包而异）：

```
JAVA_HOME="/usr/lib/jvm/jre-11-openjdk"
```

d.保存并关闭 文件：按 **CTRL+X**，然后按 **Y** 和 **ENTER**

e.重新启动 **tomcat** 服务：

```
sudo systemctl restart tomcat
```

f.运行以下命令以验证 Apache Tomcat 使用的 Java 程序包：

```
sudo systemctl status tomcat
```

将 Apache Tomcat 升级到更高的主版本（例如Apache Tomcat 版本 7.x 到 9.x
1.重新部署 ESET PROTECT Web 控制台（请参阅 ESET PROTECT Web 控制台安装 - Linux
2.在 ESET PROTECT Web 控制台中再次使用 *%TOMCAT_HOME%/webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties* 以保留任何自定义设置。
Web 控制台和 Apache Tomcat 升级会清除脱机帮助文件。如果使用 ESMC 或较早 ESET PROTECT 版本的脱机帮助，请在升级后为 ESET PROTECT 10.0 重新创建它，以确保您有匹配 ESET PROTECT 版本的最新脱机帮助。

迁移和重新安装过程

迁移和重新安装 ESET PROTECT 服务器和其他 ESET PROTECT 组件有不同方法：

- 从一台服务器到另一台服务器迁移或重新安装 ESET PROTECT 10

如果您打算从一台 ESET PROTECT 服务器迁移到一台新的服务器计算机，则导出或备份所有证书颁发机构和 ESET PROTECT 服务器证书。否则，任何 ESET PROTECT 组件都不能够与您的新 ESET PROTECT 服务器通信。

- ESET PROTECT 数据库迁移
- MDM 的迁移
- 在 ESET PROTECT 服务器上更改 IP 地址或主机名

请参阅升级过程

从一台服务器迁移到另一台服务器

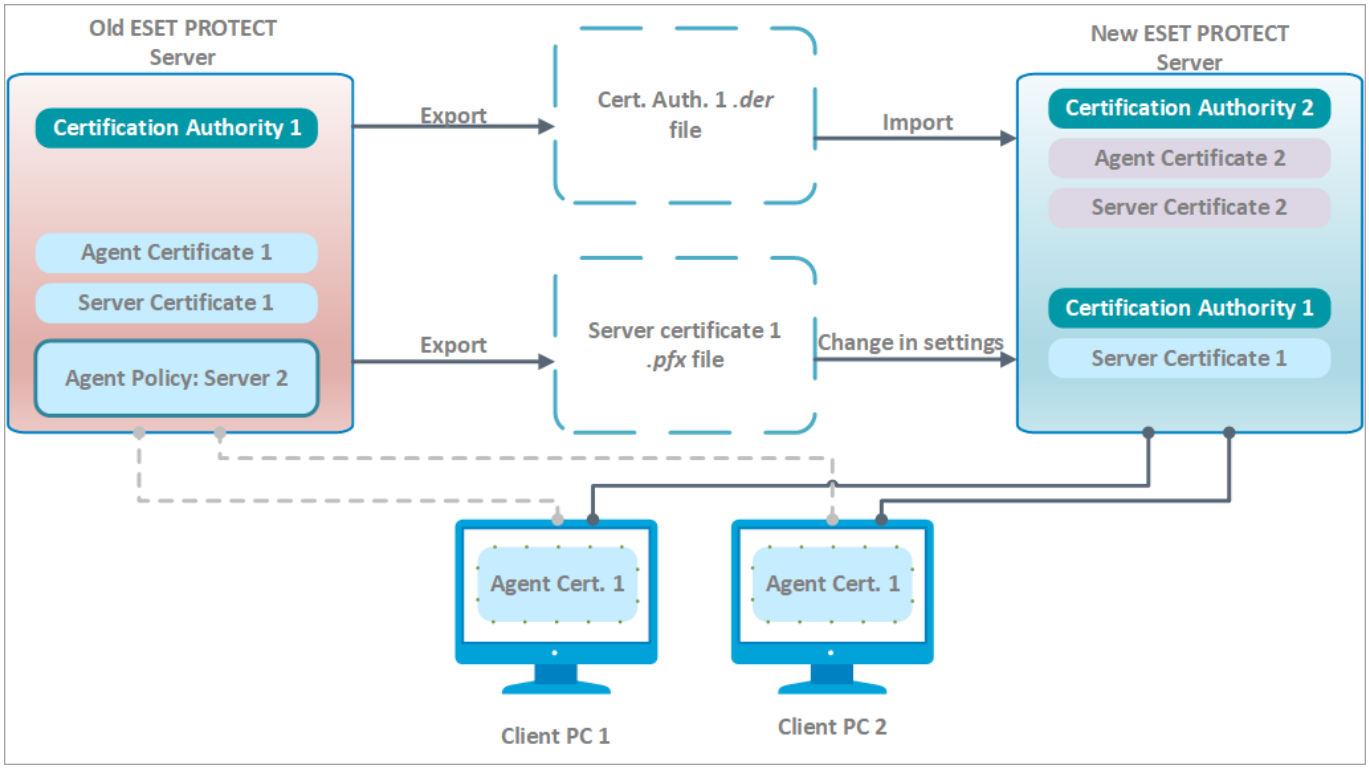
将 ESET PROTECT 从一台服务器迁移到另一台服务器有多种方式可供使用（重新安装 ESET PROTECT 服务器时可以使用这些方案）：

- 全新安装 – 相同 IP 地址 – 此全新安装不使用来自旧 ESET PROTECT 服务器中以前的数据库并保留原始 IP 地址。
- 全新安装 – 不同 IP 地址（知识库文章）– 此全新安装不使用来自旧 ESET PROTECT 服务器中以前的数据库并具有不同 IP 地址。
- 迁移数据库 – 相同/不同 IP 地址 – 数据库迁移只可以在两个相似数据库类型（从 MySQL 到 MySQL 或者从 Microsoft SQL 到 Microsoft SQL和两个相似 ESET PROTECT 版本之间执行。

全新安装 – 相同 IP 地址

此步骤的目标是安装不使用以前数据库的全新 ESET PROTECT 服务器实例，但保留客户端计算机的记录。这一新的 ESET PROTECT 服务器与您以前的服务器具有**相同 IP 地址**，但不会使用旧的 ESET PROTECT 服务器中的数据库。

以下说明要求旧的 ESET PROTECT 服务器正在使用可访问的 Web 控制台运行。如果无法访问旧的 ESET PROTECT 服务器：
1. 使用一体式程序包安装程序安装 ESET PROTECT 服务器/MDM (Windows)或者选择其他安装方式（Windows 手动安装Linux 或虚拟设备）。
2. 连接到 ESET PROTECT Web 控制台。
3. 添加客户端计算机到 ESET PROTECT 基础架构，然后本地或远程部署 ESET Management 服务器代理



单击此处查看大图

❑ **在您的当前（旧ESET PROTECT 服务器上：**

如果管理使用 ESET Full Disk Encryption 加密的设备，请按照以下步骤操作，以避免丢失恢复数据
1.迁移前，导航到**状态概述** > **加密**。您可以在此处**导出**当前 **ESET Full Disk Encryption 恢复数据**
2.迁移后，**导入**新管理控制台上的 **ESET Full Disk Encryption 恢复数据**
如果无法执行这些步骤，则需要在迁移之前解密托管的设备。迁移后，可以从 ESET PROTECT Web 控制台加密受管设备

1. 导出当前 ESET PROTECT 服务器中的服务器证书并将其保存到外部存储。
   - 从 ESET PROTECT 服务器中导出所有证书颁发机构证书并将每个 CA 证书另存为 *.der* 文件。
   - 将 ESET PROTECT 服务器中的 服务器证书导出到 *.pfx* 文件。导出的 *.pfx* 还将包含私钥。
2. 停用 ESET PROTECT 服务器服务。
3. 关闭您的 ESET PROTECT 服务器计算机。

请勿卸载/停用您的旧 ESET PROTECT 服务器。

❑ **在您的新 ESET PROTECT 服务器上：**

要使用 IP 地址相同的新 ESET PROTECT 服务器，请确保新 ESET PROTECT 服务器上的网络配置（**IP 地址**、**FQDN**、**计算机名称**、**DNS SRV 记录**）与旧的 ESET PROTECT 服务器上的网络配置相匹配。

1. 使用一体式程序包安装程序安装 ESET PROTECT 服务器/MDM (Windows)、或者选择其他安装方式（Windows 手动安装、Linux 或虚拟设备）。

2. 连接到 ESET PROTECT Web 控制台。

3. 导入所有 CA（从您的旧 ESET PROTECT 服务器中导出的 CA）。若要执行此操作，请按照导入公钥中的说明操作。

4. 在**更多** > 服务器设置中更改 ESET PROTECT 服务器证书，以便使用来自您的旧 ESET PROTECT 服务器中的服务器证书。

5. 向 ESET PROTECT 导入所有需要的 ESET 许可证。

6. 重新启动 ESET PROTECT 服务器服务，请参阅我们的知识库文章以获取详细信息。

经过一两个服务器代理连接间隔之后，客户端计算机应使用其原始 ESET PROTECT 服务器代理证书（该证书由从旧的 ESET Management 服务器导入的 CA 进行身份验证）连接到新的 ESET PROTECT 服务器。 如果客户端未连接，请参阅升级/迁移 ESET PROTECT 服务器后出现的问题。

添加新的客户端计算机时，使用新的证书颁发机构签署服务器代理证书。执行上述操作的原因是导入的 CA 无法用于签署新的对等证书，只可以对迁移的客户端计算机的 ESET Management 服务器代理执行身份验证。

❑ **旧的 ESET PROTECT 服务器/MDM 卸载：**

当新 ESET PROTECT 服务器上的所有一切都正常运行之后，请按照分步说明操作，小心停用您的旧 ESET PROTECT 服务器/MDM。

迁移数据库 – 相同/不同 IP 地址

此步骤的目标是安装全新的 ESET PROTECT 服务器实例并**保留您的现有 ESET PROTECT 数据库**，包括现有客户端计算机。新的 ESET PROTECT 服务器将具有**相同或不同的 IP 地址**，并且旧 ESET PROTECT 服务器的数据库将会在安装之前导入新的服务器计算机。

- 迁移数据库仅在同一数据库类型之间受支持（从 MySQL 到 MySQL 或从 Microsoft SQL 到 Microsoft SQL）。
- 迁移数据库时，必须在同一版本的 ESET PROTECT 实例之间迁移。请参阅知识库文章以获取用于确定 ESET PROTECT 组件版本的说明。完成数据库迁移之后，您可以执行升级（如有需要）以获取最新版本的 ESET PROTECT。

❑ **在您的当前（旧）ESET PROTECT 服务器上：**

仅建议高级用户迁移到其他 IP 地址。如果新的 ESET PROTECT 服务器具有**不同 IP 地址**，请在当前（旧）ESET PROTECT 服务器上执行以下附加步骤：
a)生成一个新的 ESET PROTECT 服务器证书（内含新的 ESET PROTECT 服务器的连接信息）。在**主机**字段中保留默认值（一个星号）以允许在未关联到特定 DNS 名称或 IP 地址的情况下分发此证书。
b)创建一个用于定义新 ESET PROTECT 服务器 IP 地址的策略并将该策略分配给所有计算机。等待该策略分配给所有客户端计算机（计算机在接收新的服务器信息时会停止报告）。

1. 停用 ESET PROTECT 服务器服务。

2. 导出/备份 ESET PROTECT 数据库。

3. 关闭当前 ESET PROTECT 服务器计算机（如果新的服务器具有不同 IP 地址，则为可选）。

请勿卸载/停用您的旧 ESET PROTECT 服务器。

❑ **在您的新 ESET PROTECT 服务器上：**

要使用 IP 地址相同的新 ESET PROTECT 服务器，请确保新 ESET PROTECT 服务器上的网络配置（**IP 地址**、**FQDN**、**计算机名称**、**DNS SRV 记录**）与旧的 ESET PROTECT 服务器上的网络配置相匹配。

1. 安装/启动一个受支持的 ESET PROTECT 数据库。

2. 导入/恢复来自您的旧 ESET PROTECT 服务器的 ESET PROTECT 数据库。

3. 使用一体式程序包安装程序安装 ESET PROTECT 服务器/MDM (Windows)、或者选择其他安装方式（Windows 手动安装、Linux 或虚拟设备）。 在 ESET PROTECT 服务器安装期间指定您的数据库连接设置。

4. 连接到 ESET PROTECT Web 控制台。

5. 导航到**更多** > **设置** > **连接**。单击**更改证书** > **打开证书列表**，然后选择旧 ESET PROTECT 服务器的**服务器证书**，再单击**确定**两次。

6. 重新启动 ESET PROTECT 服务器服务。

7. 登录到 ESET PROTECT Web 控制台，然后单击**计算机**。

经过一两个服务器代理连接间隔之后，客户端计算机应使用其原始 ESET PROTECT 服务器代理证书连接到新的 ESET Management 服务器。 如果客户端未连接，请参阅升级/迁移 ESET PROTECT 服务器后出现的问题。

❑ **旧的 ESET PROTECT 服务器/MDM 卸载：**

当新 ESET PROTECT 服务器上的所有一切都正常运行之后，请按照分步说明操作，小心停用您的旧 ESET PROTECT 服务器/MDM。

ESET PROTECT 数据库迁移

以下说明适用于不同 SQL Server 实例之间的 ESET PROTECT 数据库（这同样适用于迁移到其他 SQL Server 版本或迁移到在其他计算机上托管的 SQL Server 的情况）：

- Microsoft SQL Server 的迁移过程
- MySQL Server 的迁移过程

Microsoft SQL Server 的迁移过程

本迁移过程同样适用于 **Microsof SQL Server** 和 **Microsoft SQL Server Express**。

有关详细信息，请参阅以下 Microsoft 知识库文章：https://msdn.microsoft.com/en-us/library/ms189624.aspx。

先决条件

- 必须安装源 SQL Server 实例和目标 SQL Server 实例。它们可能托管在不同的计算机上。
- 目标 SQL Server 实例的版本至少应该与源实例相同。**降级不受支持！**
- 必须安装 **SQL Server Management Studio**。如果 SQL Server 实例位于不同的计算机上，则同一计算机上必须有该实例和 SQL Server Management Studio。

使用 SQL Server Management Studio 的迁移

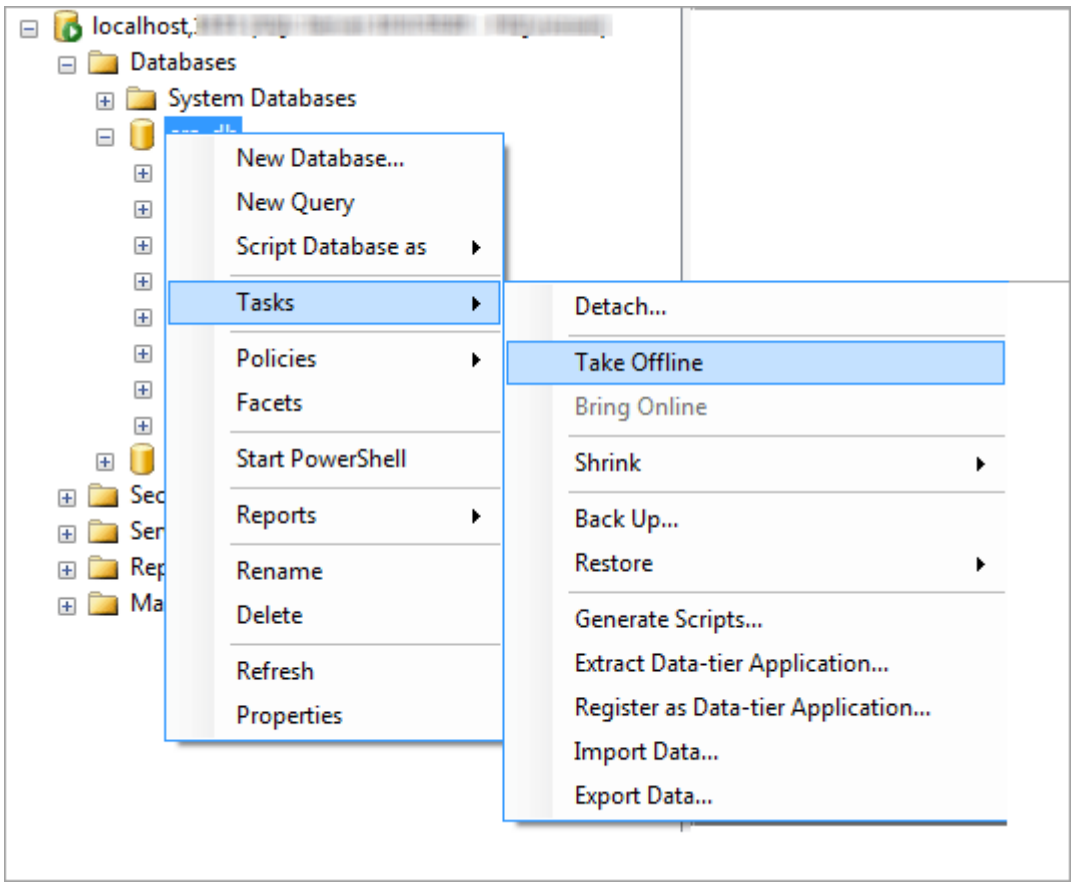
1. 停止 ESET PROTECT 服务器服务（或 ESMC 服务器服务）或 ESET PROTECT MDM 服务。

⚠ 在完成以下所有步骤之前，请勿启动 ESET PROTECT 服务器或 ESET PROTECT MDM。

2. 通过 SQL Server Management Studio 登录到源 SQL Server 实例。

3. 创建一个要迁移数据库的完整数据库备份。我们建议您指定一个新的备份集名称。否则，如果已经使用了备份集，那么新的备份将会附加到原来的备份集中，这将导致生成一个不必要的较大备份文件。

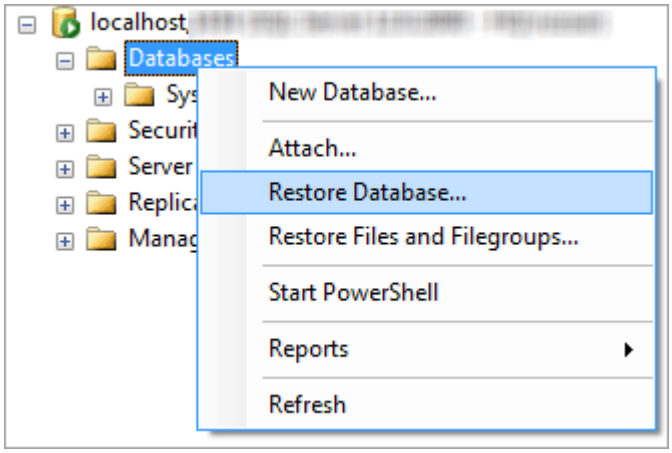
4. 若要将源数据库脱机，请选择**任务 > 脱机**。



5. 将步骤 3 中创建的备份（*.bak*）文件复制到目标 SQL Server 实例能够访问的位置。您可能需要为数据库备份文件编辑访问权限。

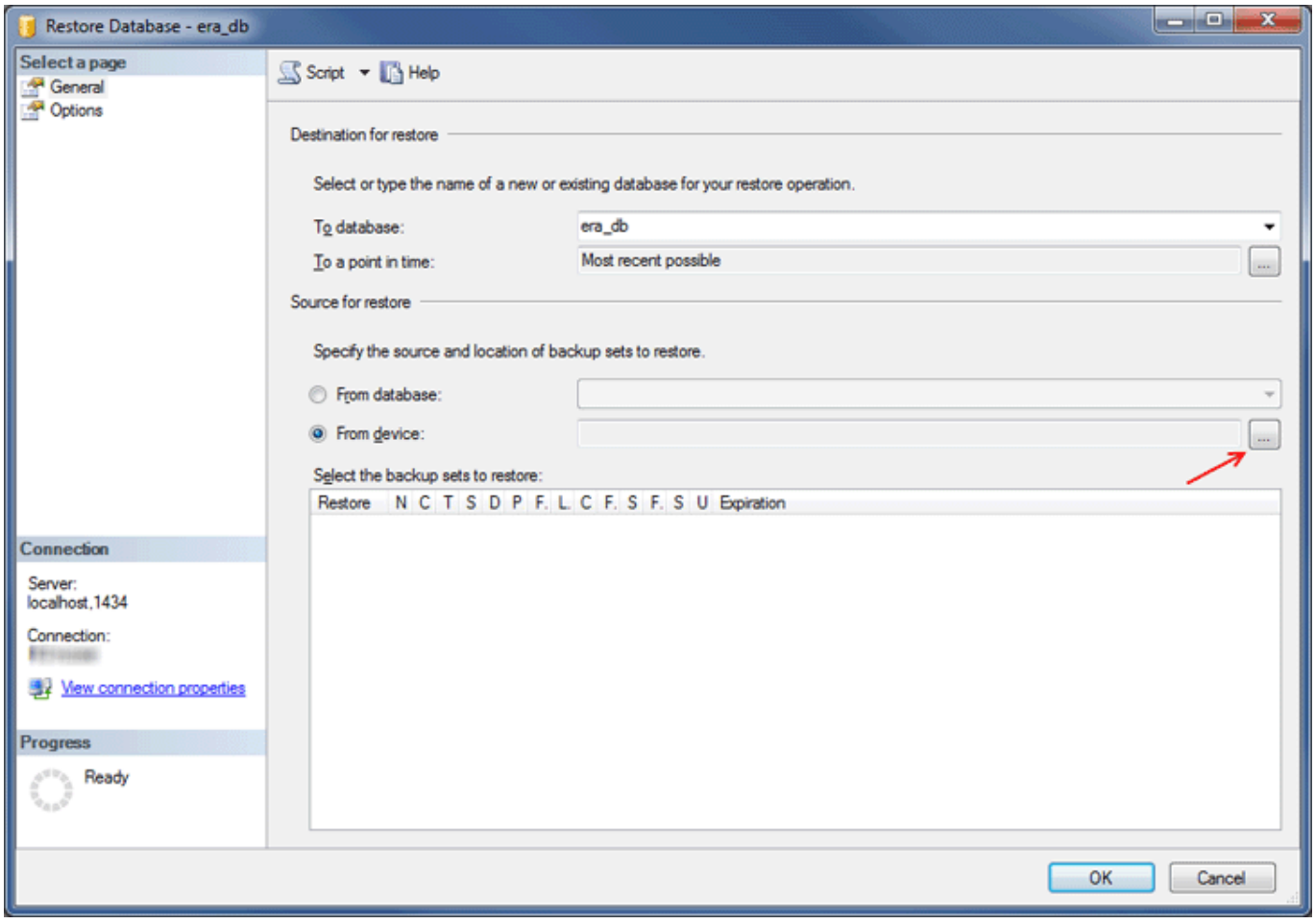
6. 通过 SQL Server Management Studio 登录到目标 SQL Server 实例。

7. 在目标 SQL Server 实例上恢复数据库。



8. 将新数据库名称键入**至数据库**字段中。如果需要，可以使用与旧数据库相同的名称。

9. 选择**指定需要恢复备份集的来源和位置**下的“源设备”，然后单击 ⋯。

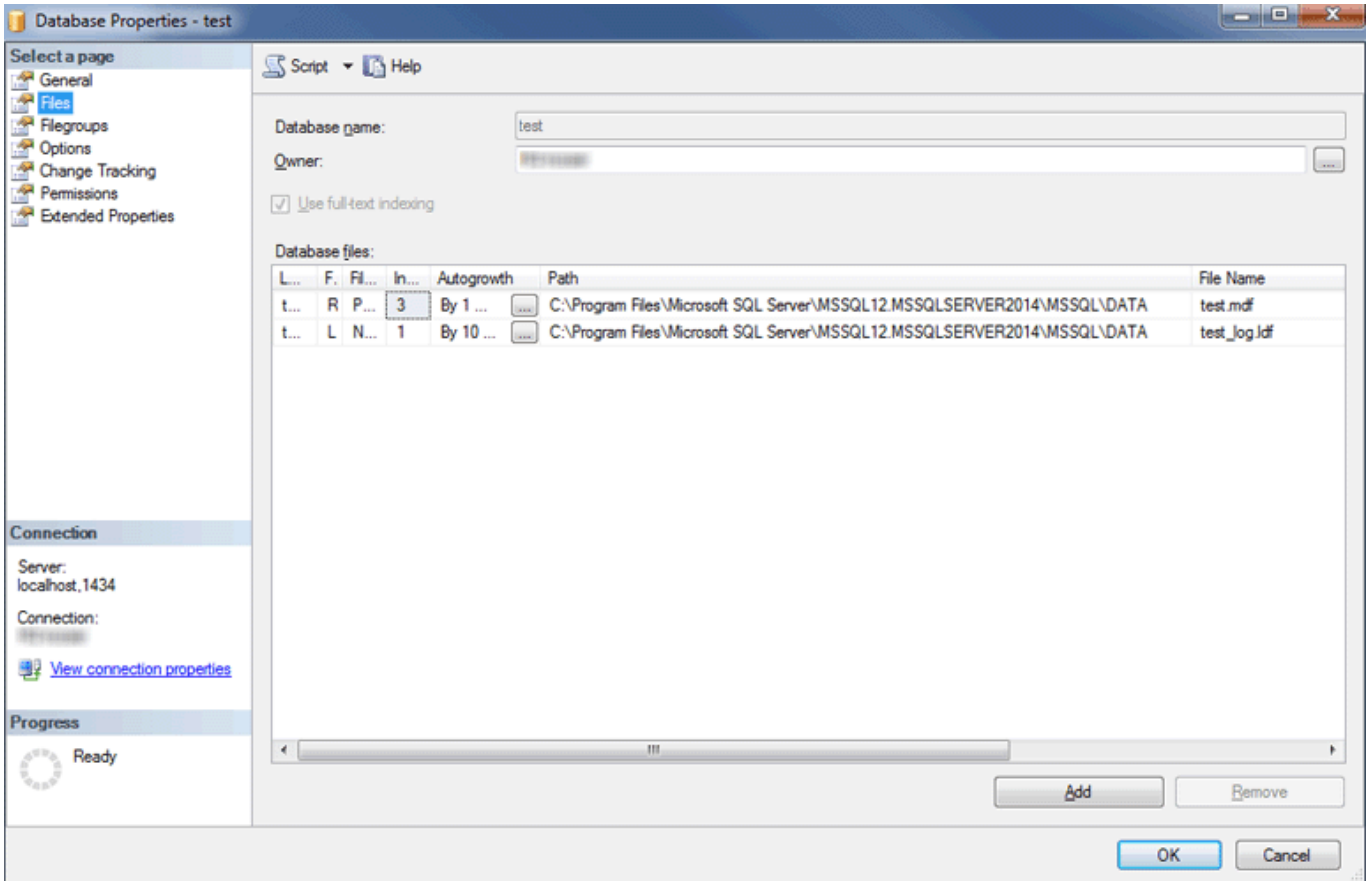


10. 单击**添加，导航到您的备份文件，然后将其打开**。

11. 选择需要恢复的最近的备份（备份集可能包含多个备份）。

12. 单击恢复向导的**选项**页。或者选择**覆盖现有数据库**并确保数据库（*.mdf*）和日志（*.ldf*）的恢复位置都正确。保留默认值不改变将会使用来自源 SQL Server 的路径，因此请检查这些值。

- 如果不确定目标 SQL Server 实例上 DB 文件的存储位置，可以右键单击现有数据库，选择**属性**，然后单击**文件**选项卡。存储数据库的目录会显示在如下所示表格的**路径**列中。

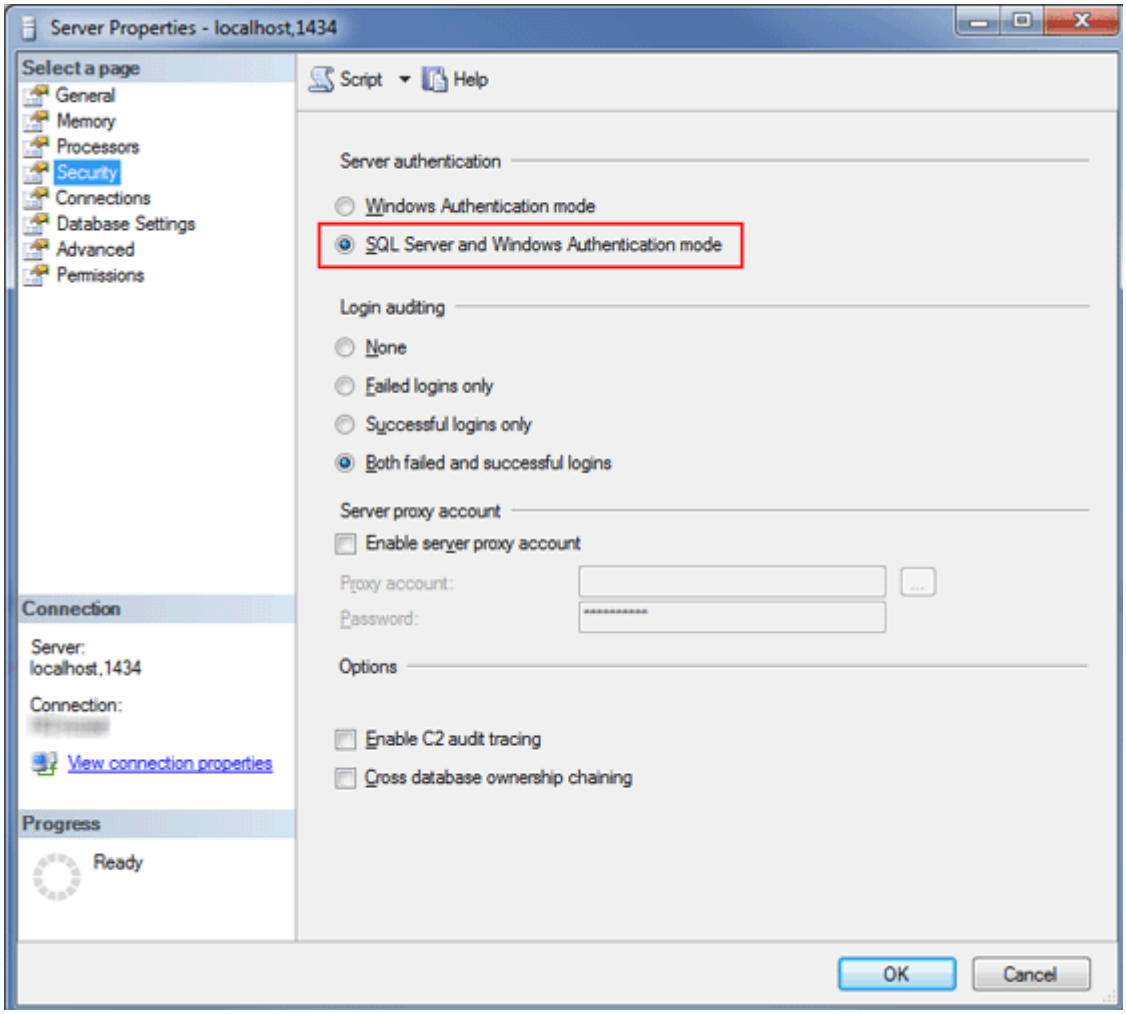


13. 在恢复向导窗口中单击**确定**。

14. 右键单击 **era_db** 数据库，选择**新查询**并运行以下查询以删除 **tbl_authentication_certificate** 表的内容（否则，服务器代理可能无法连接到新服务器）：

```
delete from era_db.dbo.tbl_authentication_certificate where certificate_id = 1;
```

15. 确保新的数据库服务器已经**启用 SQL Server 身份验证**。右键单击服务器，然后单击**属性**。导航到**安全**，然后确认已经选择了 **SQL Server 和 Windows 身份验证模式**。



16. 通过 SQL Server 身份验证在目标 SQL Server 中**创建新的 SQL Server 登录**（适用于 ESET PROTECT 服务器/ESET PROTECT MDM）并将登录映射到已恢复数据库中的用户。

o请勿强制实施密码过期操作！

o建议的用户名字符：

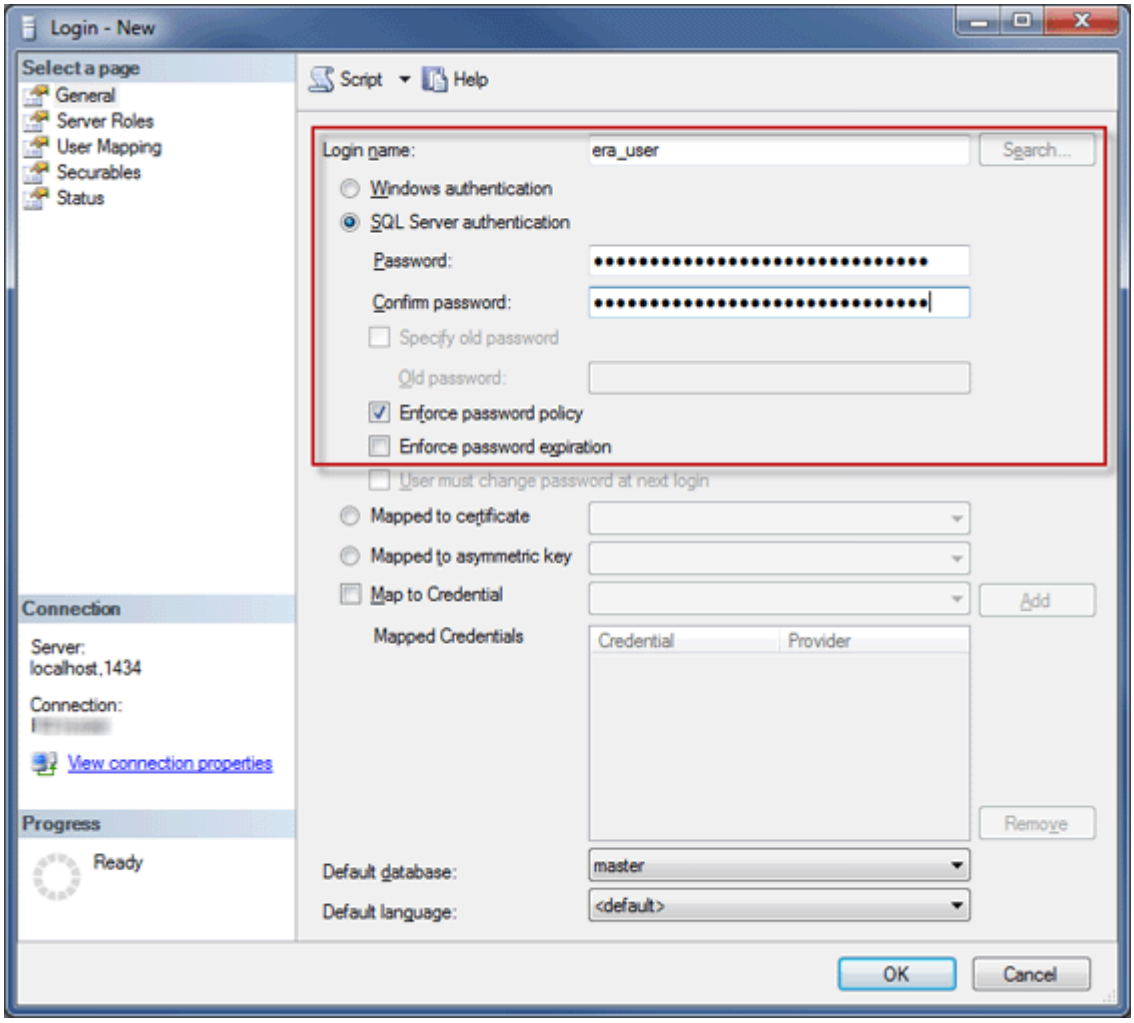
■小写 ASCII 字母、数字和字符下划线“_”

o建议的密码字符：

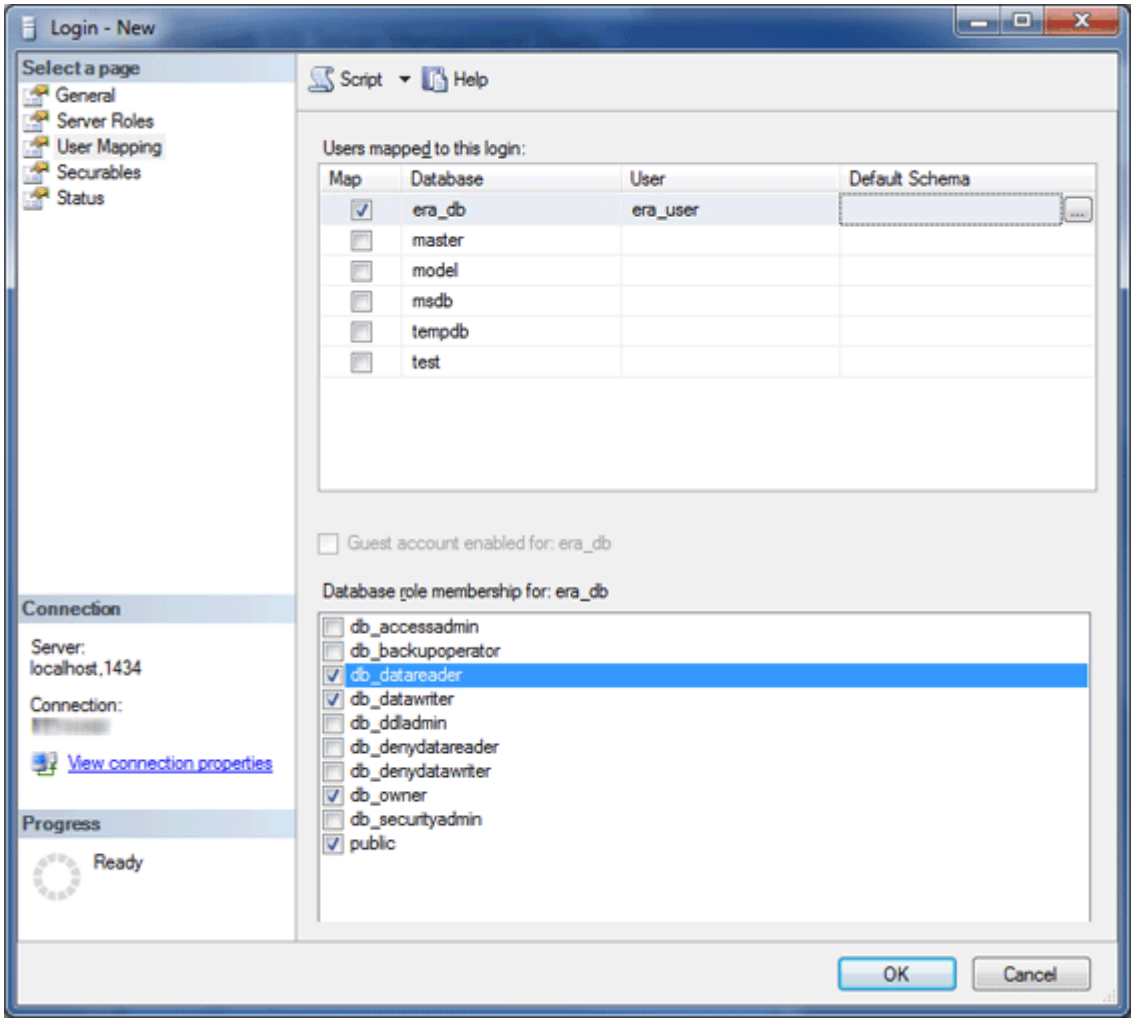
■仅限 ASCII 字符，包括大写和小写 ASCII 字母、数字、空格、特殊字符

o不要使用非 ASCII 字符、大括号 {} 或 @

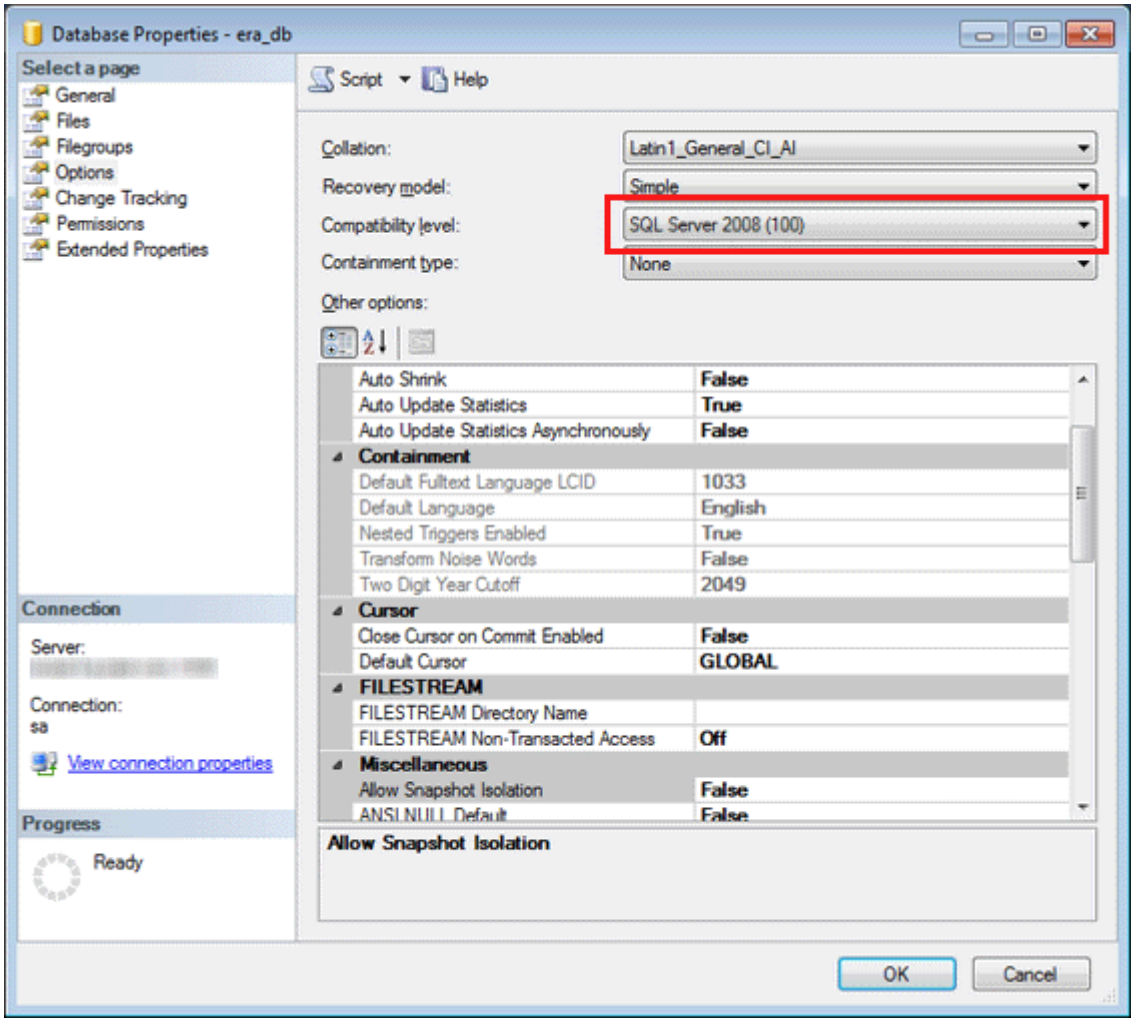
o请注意，如果未使用上述建议的字符，那么可能会遇到数据库的连接出现问题；在数据库连接字符串修改期间的稍后步骤中，需要避免使用特殊字符。本文档中不包含字符转义规则。



17. 将登录映射到目标数据库中的用户。在**用户映射**选项卡中，确保数据库用户具有如下角色：**db_datareader、db_datawriter、db_owner**。

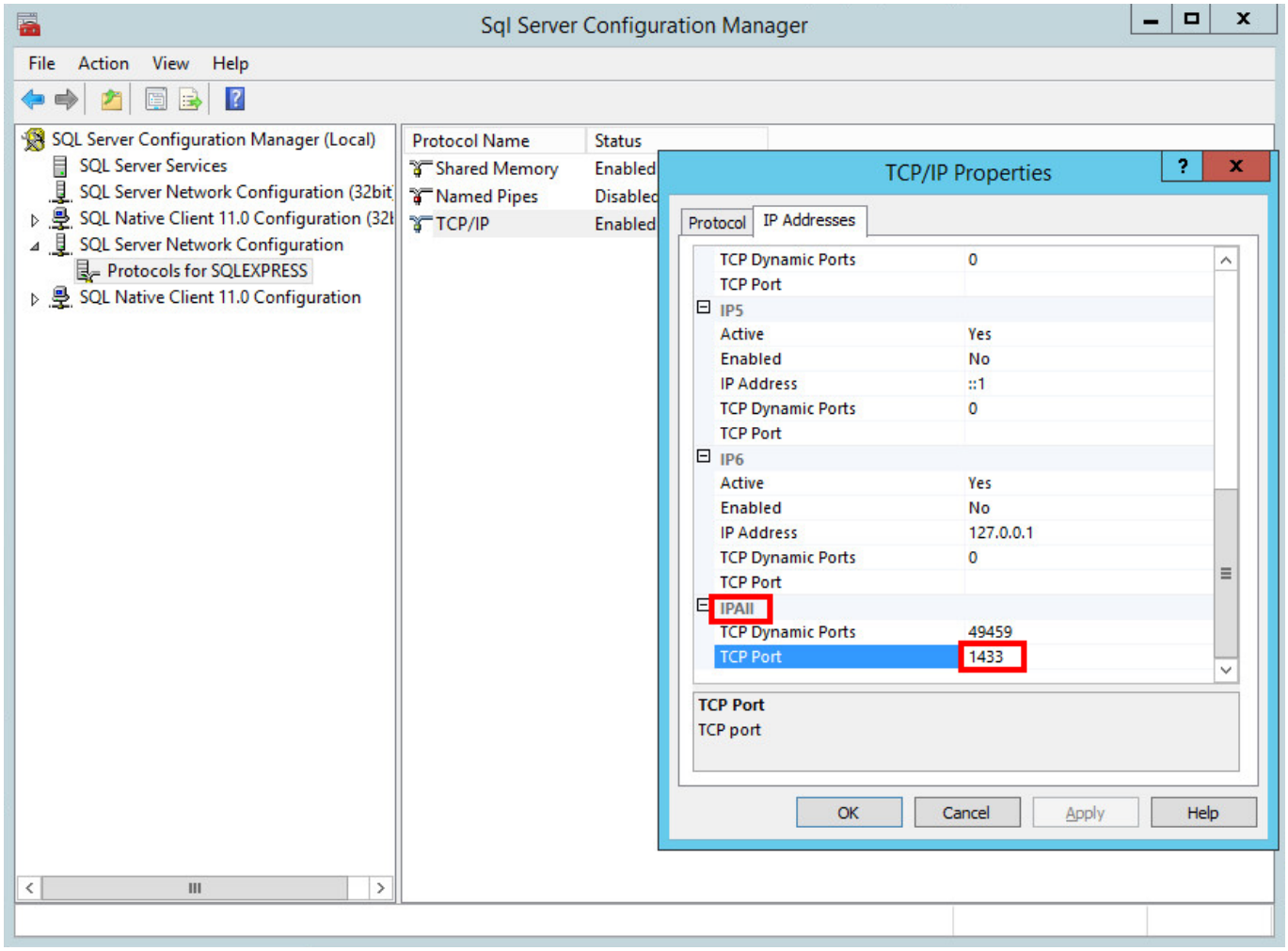


18. 若要启用最新的数据库服务器功能，请将已恢复数据库**兼容级别**更改为最新。右键单击新数据库，然后打开数据库**属性**。



SQL Server Management Studio 无法为高于正在使用的版本定义兼容级别。例如，SQL Server Management Studio 2014 无法为 SQL Server 2019 设置兼容级别。

19. 确保已针对“db_instance_name”（例如 SQLEXPRESS 或 MSSQLSERVER）**启用 TCP/IP** 连接协议，并且 TCP/IP **端口**设置为 **1433**。若要执行此操作，请打开 **SQL Server 配置管理器**，导航到 **SQL Server 网络配置 > db_instance_name 的协议**，右键单击 **TCP/IP**，然后选择**启用**。双击 **TCP/IP**，切换到**协议**选项卡，向下滚动到 **IPAll**，然后在 **TCP 端口**字段中键入 1433。单击**确定**，然后重新启动 **SQL Server** 服务。



20. 将 ESET PROTECT 服务器或 MDM 连接到数据库

MySQL Server 的迁移过程

先决条件

- 必须安装源 SQL Server 实例和目标 SQL Server 实例。它们可能托管在不同的计算机上。
- MySQL 工具必须至少在其中一台计算机（`mysqldump` 和 mysql 客户端）上可用。

有用链接

- https://dev.mysql.com/doc/refman/5.6/en/copying-databases.html
- https://dev.mysql.com/doc/refman/5.6/en/mysqldump.html
- https://dev.mysql.com/doc/refman/5.6/en/mysql.html

迁移过程

在命令（配置文件或下面的 SQL 语句）中，请始终进行以下替换：
- 将 **SRCHOST** 替换为源数据库服务器的地址
- 将 **SRCROOTLOGIN** 替换为源 MySQL 服务器根用户登录
- 将 **SRCDBNAME** 替换为要备份的源 ESET PROTECT 数据库的名称
- 将 **BACKUPFILE** 替换为将用于存储备份的文件的路径
- 将 **TARGETROOTLOGIN** 替换为目标 MySQL 服务器根用户登录
- 将 **TARGETHOST** 替换为目标数据库服务器的地址
- 将 **TARGETDBNAME** 替换为目标 ESET PROTECT 数据库的名称（在迁移后）
- 将 **TARGETLOGIN** 替换为目标数据库服务器上的新 ESET PROTECT 数据库用户的登录名
- 将 **TARGETPASSWD** 替换为目标数据库服务器上的新 ESET PROTECT 数据库用户的密码

不必通过命令行执行以下 SQL 语句。如果存在可用的 GUI 工具，您可以使用您熟悉的应用程序。

1. 停用 ESET PROTECT 服务器/MDM 服务。

2. 创建源 ESET PROTECT 数据库的完整数据库备份（您打算迁移的数据库）：

```
mysqldump --host SRCHOST --disable-keys --extended-insert --routines -
u SRCROOTLOGIN -p SRCDBNAME > BACKUPFILE
```

3. 在目标 MySQL 服务器上准备空数据库：

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--
execute=CREATE DATABASE TARGETDBNAME /*!40100 DEFAULT CHARACTER SET utf8 */;"
```

请在 Linux 系统上使用撇号字符 ’ 而不是双引号 ″。

4. 将目标 MySQL 服务器上的数据库还原为之前准备的空数据库：

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p TARGETDBNAME < BACKUPFILE
```

5. 在目标 MySQL 服务器上创建 ESET PROTECT 数据库用户：

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--
execute=CREATE USER TARGETLOGIN@'%' IDENTIFIED BY 'TARGETPASSWD';"
```

TARGETLOGIN 的建议字符：

- 小写 ASCII 字母、数字和下划线 “_”

TARGETPASSWD 的建议字符：

- 仅限 ASCII 字符，包括大写和小写 ASCII 字母、数字、空格和特殊字符
- 不要使用非 ASCII 字符、大括号 {} 或 @

请注意，如果未使用上述建议的字符，那么可能会遇到数据库的连接出现问题；在数据库连接字符串修改期间的稍后步骤中，需要避免使用特殊字符。本文档中不包含字符转义规则。

6. 为目标 MySQL 服务器上的 ESET PROTECT 数据库用户授予适当的访问权限：

```
mysql --host TARGETHOST -u TARGETROOTLOGIN -p "--
execute=GRANT ALL ON TARGETDBNAME.* TO TARGETLOGIN;"
```

请在 Linux 系统上使用撇号字符 ’ 而不是双引号 ″。

7. 删除 **tbl_authentication_certificate** 表的内容（否则，服务器代理可能无法连接到新服务器）：

```
 mysql --host TARGETHOST -u root -p "--
execute=DELETE FROM era_db.tbl_authentication_certificate where certificate_id = 1;"
```

8. 将 ESET PROTECT 服务器或 MDM 连接到数据库

连接 ESET PROTECT 服务器或 MDM 到数据库

在安装有 ESET PROTECT 服务器或 ESET PROTECT MDM 的计算机上按照以下步骤操作，以将其连接到数据库。

1. 停用 ESET PROTECT 服务器/MDM 服务。
2. 找到 *startupconfiguration.ini*
   - Windows:

服务器：

```
%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configurati
on\startupconfiguration.ini
```

MDMCore

```
%PROGRAMDATA%\ESET\RemoteAdministrator\MDMCore\EraServerApplicationData\Configurat
ion\startupconfiguration.ini
```

   - Linux:

服务器：

```
/etc/opt/eset/RemoteAdministrator/Server/StartupConfiguration.ini
```

MDMCore

```
/etc/opt/eset/RemoteAdministrator/MDMCore/startupconfiguration.ini
```

3. 在 ESET PROTECT 服务器/MDM *startupconfiguration.ini* 中更改数据库连接字符串

   o设置新数据库服务器的地址和端口。

   o在连接字符串中设置新的 ESET PROTECT 用户名和密码。

最终结果应如下所示：

- Microsoft SQL:

```
DatabaseType=MSSQLOdbc

DatabaseConnectionString=Driver=SQL Server;Server=TARGETHOST,1433;Uid=TARGETLOGIN;Pw
d={TARGETPASSWD};CharSet=utf8;Database=TARGETDBNAME;
```

- MySQL

```
DatabaseType=MySqlOdbc
DatabaseConnectionString=Driver=MySQL ODBC 5.3 Unicode Driver;Server=TARGETHOST;Port
=3306;User=TARGETLOGIN;
Password={TARGETPASSWD};CharSet=utf8;Database=TARGETDBNAME;
```

在以上配置中，请始终替换：
- 将 **TARGETHOST** 替换为目标数据库服务器的地址
- 将 **TARGETDBNAME** 替换为目标 ESET PROTECT 数据库的名称（在迁移后）
- 将 **TARGETLOGIN** 替换为目标数据库服务器上的新 ESET PROTECT 数据库用户的登录名
- 将 **TARGETPASSWD** 替换为目标数据库服务器上的新 ESET PROTECT 数据库用户的密码

4. 启动 ESET PROTECT 服务器或 ESET PROTECT MDM 并验证相应服务是否在正确运行。

MDM 的迁移

ESET PROTECT 移动设备管理/连接器 (MDM/MDC) 组件（仅限本地）计划结束生命周期。阅读更多建议您迁移到 Cloud MDM

要将 MDM本地）从一台服务器迁移到另一台服务器，请按照下面的说明进行操作。

MDM 从一台服务器迁移到另一台服务器（本地）

此步骤的目标是迁移现有 ESET PROTECT MDM 实例并**保留您的现有 ESET PROTECT MDM 数据库**，包括注册的移动设备。迁移的 ESET PROTECT MDM 将与旧的 ESET PROTECT MDM 具有**相同 IP 地址/主机名**，并且旧 ESET PROTECT MDM 数据库会在安装之前导入新的 MDM 主机。

- 迁移数据库仅在同一数据库类型之间受支持（从 MySQL 到 MySQL 或从 Microsoft SQL 到 Microsoft SQL
- 迁移数据库时，必须在同一版本的 ESET PROTECT 实例之间迁移。请参阅知识库文章以获取用于确定 ESET PROTECT 组件版本的说明。完成数据库迁移之后，您可以执行升级（如有需要）以获取最新版本的 ESET PROTECT

❑ **在您的当前（旧）ESET PROTECT MDM 服务器上：**

1. 创建 MDM 配置的备份。

a)在**计算机**中，单击 MDM 服务器并选择**详细信息**。

b)单击**配置** > **请求配置**。您可能需要等待一些时间（具体取决于服务器代理连接间隔），直到创建请求的配置。

c)单击 **ESET PROTECT Mobile Device Connector** 并选择**打开配置**。

d)将以下项目从配置导出到外部存储：

- MDM 服务器的准确主机名。
- 对等证书 – 导出的 *.pfx* 文件中将包含私钥。

> 如果在 Linux 上运行 ESET PROTECT MDM 服务器，则需要从 MDM 配置策略中导出 HTTPS 证书：
> I.单击 **HTTPS 证书**旁边的**查看**。
> II.单击 **下载**并下载 PFX 格式的 HTTPS 证书。

e)还将导出以下证书和标记（如果存在）：

- 注册配置文件签名证书
- APNS 证书（同时导出 APNS 证书和 APNS 私钥）。
- Apple 设备注册计划 (DEP) 授权令牌。

2. 停用 ESET PROTECT MDM 服务。

3. 导出/备份 ESET PROTECT MDM 数据库。

4. 关闭当前 ESET PROTECT MDM 计算机。

> 请勿卸载/停用您的旧 ESET PROTECT MDM。

❑ **在新的 ESET PROTECT MDM 服务器上：**

> 请确保您的新 ESET PROTECT MDM 服务器上的网络配置（从您“旧”MDM 服务器导出的主机名）与旧的 ESET PROTECT MDM 上的网络配置相匹配。

1. 安装/启动一个受支持的 ESET PROTECT MDM 数据库。

2. 导入/恢复来自旧的 ESET PROTECT MDM 的 ESET PROTECT MDM 数据库。

3. 使用一体式程序包安装程序安装 ESET PROTECT 服务器/MDM (Windows)或者选择其他安装方式（Windows 手动安装、Linux 或虚拟设备）。 在 ESET PROTECT MDM 安装期间指定您的数据库连接设置。

在 Linux 上安装 ESET PROTECT MDM 时，请使用备份中的 HTTPS 证书。

4. 连接到 ESET PROTECT Web 控制台。

5. 重新启动 ESET PROTECT MDM 服务。

托管移动设备现在应该使用其原始证书连接到新的 ESET PROTECT MDM 服务器。

❑ **旧的 ESET PROTECT 服务器/MDM 卸载：**

当新 ESET PROTECT 服务器上的所有一切都正常运行之后，请按照分步说明操作，小心停用您的旧 ESET PROTECT 服务器/MDM。

迁移后 ESET PROTECT 服务器 IP 地址或主机名的更改

若要更改 ESET PROTECT 服务器的 IP 地址或主机名，请按照以下步骤操作：

1. 如果您的 ESET PROTECT 服务器证书包含特定 IP 地址和/或主机名，请创建新的服务器证书并包含您要切换到的新 IP 地址或主机名。但如果服务器证书的主机字段中存在一个通配符 *，请**跳到步骤 2**。如果不存在通配符，通过添加新的 IP 地址和主机名（由逗号分隔）来创建新的服务器证书，并且还包含以前的 IP 地址和主机名。

2. 使用 ESET PROTECT 服务器证书颁发机构签署新的服务器证书。

3. 创建更改到新 IP 地址或主机名（最好是 IP 地址）的客户端连接策略，但包含到旧 IP 地址或主机名的第二个（备用）连接，以使 ESET Management 服务器代理可以连接到这两台服务器。有关详细信息，请参阅创建用于 ESET Management 服务器代理连接到新 ESET PROTECT 服务器的策略。

4. 将此策略应用到您的客户端计算机并允许 ESET Management 服务器代理进行复制。即使该策略会将客户端重定向到您的新服务器（该服务器不在运行。ESET Management 服务器代理仍将使用备用服务器信息连接到原始 IP 地址。

5. 在“更多”>“设置”中设置新的服务器证书。

6. 重新启动 ESET PROTECT 服务器服务并更改 IP 地址或主机名。

请参阅我们的知识库文章以获取用于更改 ESET PROTECT 服务器地址的图示说明。

卸载 ESET PROTECT 服务器及其组件

选择以下章节之一以卸载 ESET PROTECT 服务器及其组件：

- 卸载 ESET Management 服务器代理
- Windows - 卸载 ESET PROTECT 服务器及其组件
- Linux - 升级、重新安装或卸载 ESET PROTECT 组件
- macOS - 卸载 ESET Management 服务器代理和 ESET Endpoint 产品
- 迁移到另一台服务器后，停用旧的 ESMC/ESET PROTECT/MDM 服务器

卸载 ESET Management 服务器代理

可以采用多种方式卸载 ESET Management 服务器代理。

使用 ESET PROTECT Web 控制台远程卸载

1. 登录到 ESET PROTECT Web 控制台。
2. 从**计算机**窗格中选择您想要删除 ESET Management 服务器代理的计算机，然后单击**新任务**。

   此外，还可以通过选中相应的复选框来选择多台计算机，然后依次单击**计算机** > **任务** > **新任务**。
3. 键入任务的**名称**。
4. 从**任务类别**下拉菜单中选择 **ESET PROTECT**。
5. 从**任务**下拉菜单中选择停止管理（卸载 ESET Management 服务器代理）。

> 在从客户端计算机中卸载 ESET Management 服务器代理后，设备将不再受 ESET PROTECT 管理：
> • 在 ESET Management 服务器代理已卸载后，ESET 安全产品可能会保留一些设置。
> • 如果服务器代理受密码保护，您将无法卸载它。在将设备从管理中删除之前，建议您使用策略将不想要保留的某些设置（例如，密码保护）重置为默认设置。
> • 在服务器代理上运行的所有任务都将弃用。此任务的**正在运行**、**已完成**或**已失败**执行状态可能不会准确地显示在 ESET PROTECT Web 控制台中，具体取决于复制。
> • 在卸载服务器代理后，您可以通过集成的 EGUI 或 eShell 管理安全产品。

6. 查看任务**摘要**并单击“**完成**”。
7. 单击创建触发器以指定此客户端任务应在何时针对哪些**目标**执行。

本地卸载 - Windows

> 另请参阅有关在 Linux 或 macOS 上本地安装 ESET Management 服务器代理的说明。
> 有关服务器代理卸载的故障排除，请参阅 ESET Management 服务器代理卸载故障排除。

1. 连接到您想要删除 ESET Management 服务器代理的端点计算机（例如，通过 RDP）。
2. 导航到**控制面板** > **程序和功能**，然后双击 **ESET Management 服务器代理**。
3. 依次单击**下一步** > **删除**，然后按照卸载说明进行操作。

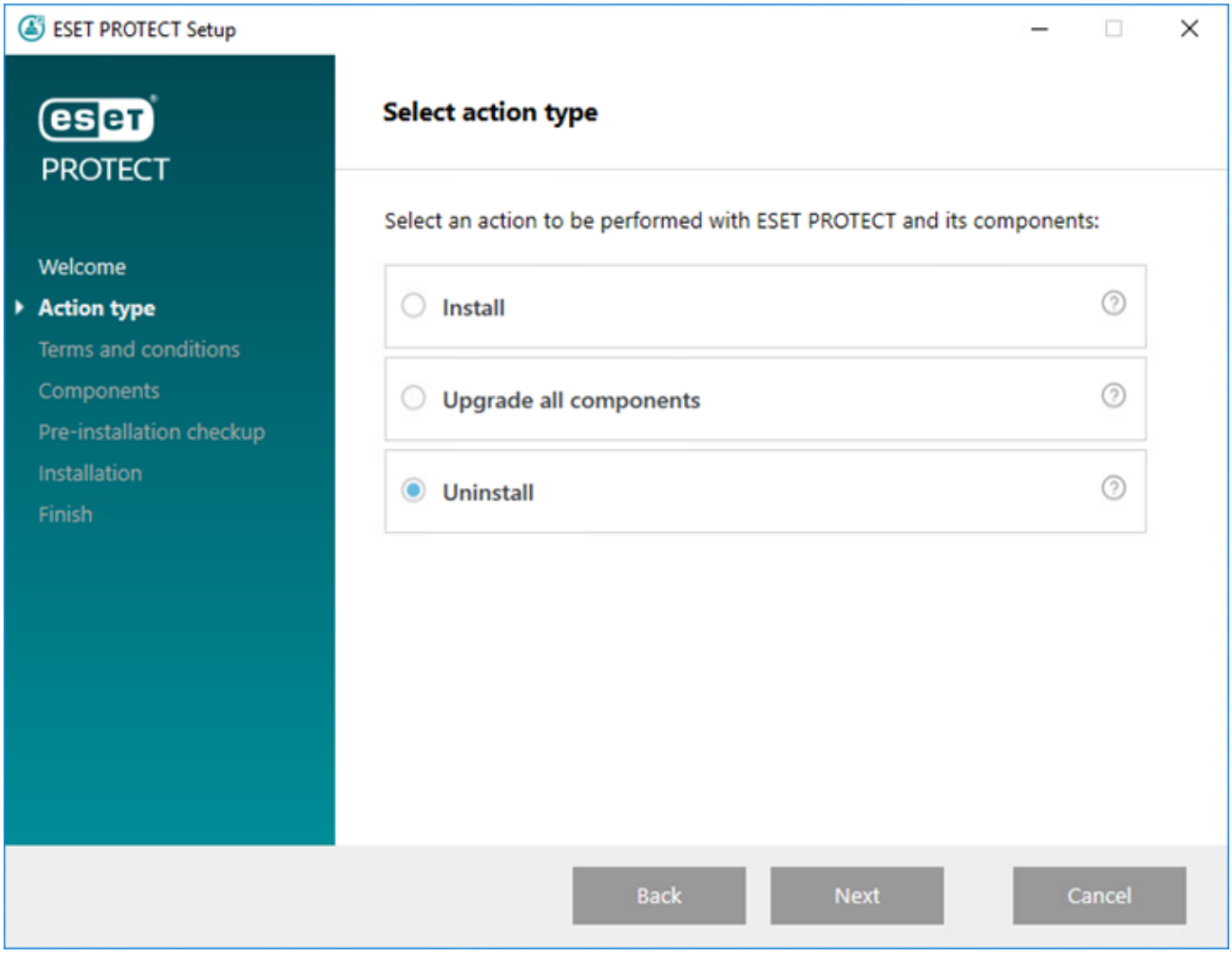
> 如果您使用策略为您的 ESET Management 服务器代理设置了密码，则有以下选项：
> • 在卸载期间，需要键入密码。
> • 在卸载 ESET Management 服务器代理之前，先取消分配策略。
> • 基于受密码保护的现有服务器代理重新部署 ESET Management 服务器代理（知识库文章）。

Windows - 卸载 ESET PROTECT 服务器及其组件

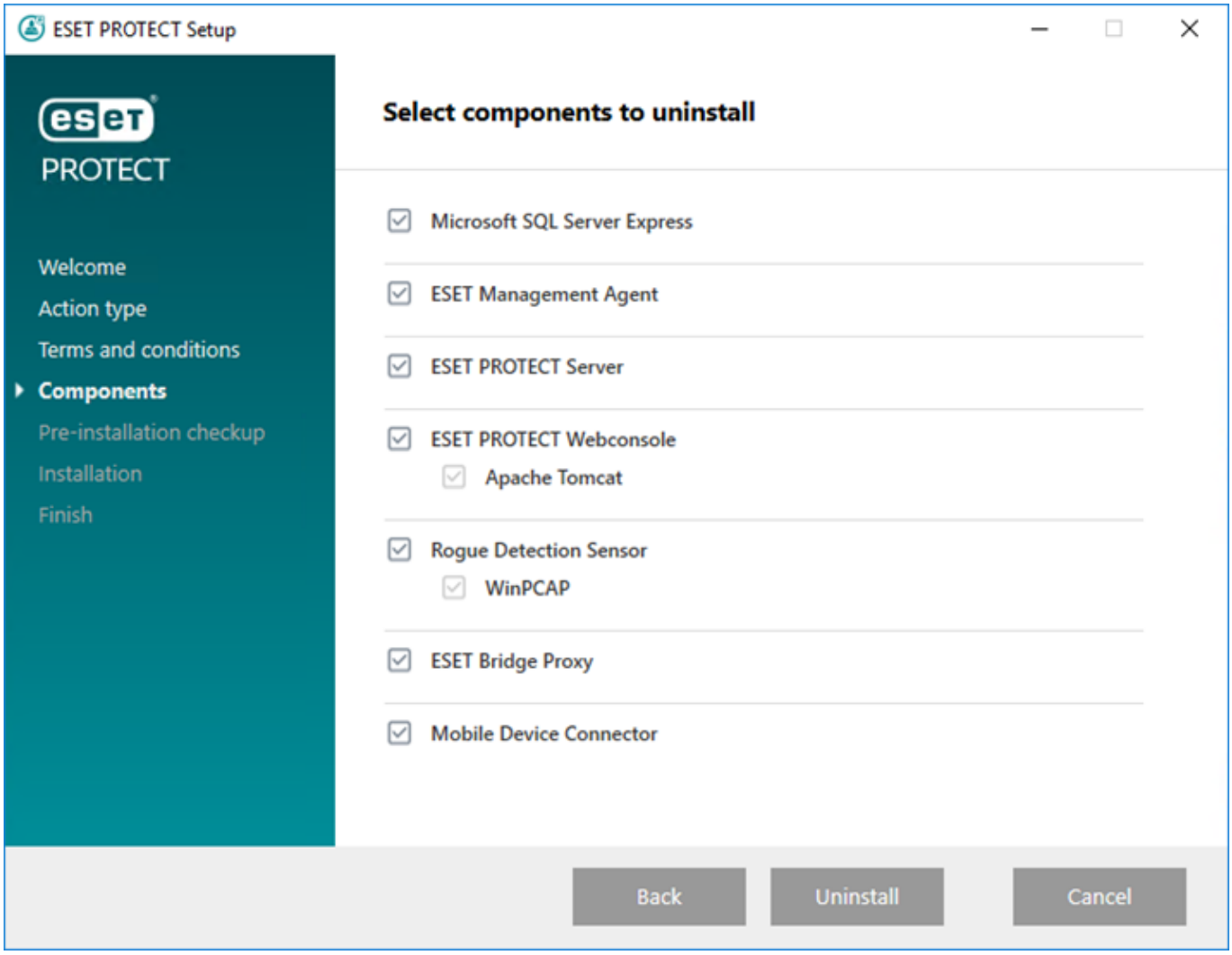
在卸载 ESET PROTECT 之前，请卸载托管计算机上的服务器代理
在卸载移动设备连接器之前，请阅读 MDM iOS 许可功能

若要在 Windows 上卸载 ESET PROTECT 服务器及其组件，请按照以下步骤操作：

1. 下载 ESET PROTECT 一体式安装程序并解压缩程序包。
2. 运行 *Setup.exe*。可以从下拉菜单中选择**语言**。单击**下一步**
3. 选择**卸载**，然后单击**下一步**



4. 接受 EULA然后单击**下一步**
5. 选择要卸载的组件，然后单击**卸载**



6. 为完成特定组件的删除，可能需要重新启动计算机。

另请参见迁移到另一台服务器后，停用旧的 ESMC/ESET PROTECT/MDM 服务器

Linux - 升级、重新安装或卸载 ESET PROTECT 组件

如果您希望重新安装或升级到更新版本，请再次运行安装脚本。

若要卸载组件（在使用 ESET PROTECT 服务器的情况下），请使用以下所示的 `--uninstall` 参数运行安装程序：

```
sudo ./server-linux-x86_64.sh --uninstall --keep-database
```

如果希望卸载其他组件，请在命令中使用相应的程序包名称。例如 ESET Management 服务器代理：

```
sudo ./agent-linux-x86_64.sh --uninstall
```

在卸载期间，将删除配置和数据库文件。若要保留数据库文件，请创建该数据库的 SQL 转储，或使用 `--keep-database` 参数。

卸载完成之后，确认如下内容：

- 将删除服务 `eraserver`
- 文件夹 `/etc/opt/eset/RemoteAdministrator/Server/` 是否已删除。

建议您在执行卸载之前创建数据库转储备份，以防您需要还原数据。
有关重新安装服务器代理的更多信息，请参阅相关章节
有关服务器代理卸载的故障排除，请参阅 ESET Management 服务器代理卸载故障排除

macOS - 卸载 ESET Management 服务器代理和 ESET Endpoint 产品

通过 ESET Management 本地或远程卸载 ESET PROTECT 服务器代理和 ESET Endpoint 产品

可以在我们的知识库文章中查找有关本地安装 ESET Management 服务器代理和 ESET Endpoint 产品的更详细说明。

如果想要远程卸载 ESET Endpoint 产品，请确保在卸载 ESET Management 服务器代理之前执行此操作。

本地卸载 ESET Management 服务器代理

1. 单击**访达**以打开新的**访达**窗口。
2. 单击**应用程序** > 按住 **CTRL** > 单击 **ESET Management 服务器代理** > 从右键菜单中选择**显示程序包内容**
3. 导航到**内容** > **脚本**并双击 **Uninstaller.command** 以运行卸载程序。
4. 如果提示您输入密码，则键入管理员密码并按 **Enter**
5. 当 ESET Management 服务器代理卸载后，您将看到**进程已完成**消息。

通过终端本地卸载 ESET Management 服务器代理

1. 依次打开 **Finder** > **程序应用** > **实用程序** > **终端**
2. 键入以下代码，然后按 **Enter** 键：

```
sudo /Applications/ESET\ Administrator\ Agent.app/Contents/Scripts/Uninstall.command ; exit;
```

3. 如果提示您输入密码，则键入管理员密码并按 **Enter**
4. 当 ESET Management 服务器代理卸载后，您将看到**进程已完成**消息。

通过 ESET Management 远程卸载 ESET PROTECT 服务器代理。

在**计算机**上，单击客户端 macOS 计算机并选择**删除**以卸载 ESET Management 服务器代理并从管理中删除该计算机。

有关服务器代理卸载的故障排除，请参阅 ESET Management 服务器代理卸载故障排除

本地卸载 ESET Endpoint 产品

1. 单击**访达**以打开新的**访达**窗口。
2. 单击**应用程序** > 按住 **CTRL** > 单击 **ESET Endpoint Security** 或 **ESET Endpoint Antivirus** > 从右键菜单中选择**显示程序包内容**
3. 导航到**内容** > **帮助程序**并双击 **Uninstaller.app** 以运行卸载程序。
4. 单击**卸载**
5. 如果提示您输入密码，则键入管理员密码并单击**确定**
6. 当 ESET Endpoint Security 或 ESET Endpoint Antivirus 成功卸载后，您将看到**卸载成功**消息。单击**关闭**

通过终端本地卸载 ESET Endpoint 产品

1. 依次打开 **Finder** > **程序应用** > **实用程序** > **终端**
2. 键入以下代码，然后按 **Enter** 键：
   - 卸载 ESET Endpoint Antivirus:

```
sudo /Applications/ESET\ Endpoint\ Antivirus.app/Contents/Helpers/Uninstaller.app
/Contents/Scripts/uninstall.sh
```

   - 卸载 ESET Endpoint Security:

```
sudo /Applications/ESET\ Endpoint\ Security.app/Contents/Helpers/Uninstaller.app/
Contents/Scripts/uninstall.sh
```

3. 如果提示您输入密码，则键入管理员密码并按 **Enter**
4. 当 ESET Endpoint 产品卸载后，您将看到**处理完成**消息。

通过 ESET PROTECT 远程卸载 ESET Endpoint 产品

要通过 ESET Management 远程卸载 ESET PROTECT 服务器代理，可以使用以下选项之一：

- 在**计算机**中，单击客户端 macOS 计算机，选择**详细信息** > **安装的应用程序** > 选择 **ESET Endpoint Security** 或 **ESET Endpoint Antivirus** 并单击**卸载**按钮。
- 使用**软件卸载**任务

迁移到另一台服务器后，停用旧的 ESMC/ESET PROTECT/MDM 服务器

确保您的新 ESET PROTECT 服务器/MDM 正在运行，并且客户端计算机和移动设备正确连接到新的 ESET PROTECT。

迁移到另一台服务器后，停用您的旧 ESMC/ESET PROTECT 服务器/MDM 时有多个选项可供使用：

I.保留服务器计算机操作系统并重新使用它

1. 停止旧的 ESMC/ESET PROTECT 服务器服务。
2. 删除（DROP DATABASE）旧的 ESMC/ESET PROTECT 服务器数据库实例。Microsoft SQL 或 MySQL。

如果已将数据库迁移到新的 ESET PROTECT 服务器，请确保在卸载之前删除旧的 ESMC/ESET PROTECT 服务器上的数据库，以防止许可证与新的 ESET PROTECT 服务器数据库断开关联（删除）。

3. 卸载旧 /ESET PROTECT/MDM 服务器及其所有组件（包括 ESET Management 服务器代理。Rogue Detection Sensor。MDM 等）：
    - 卸载 ESET PROTECT - Windows
    - 卸载 ESET PROTECT - Linux

如果其他任何软件仍在使用您的数据库，请勿卸载您的数据库。

4. 计划操作系统在卸载后重新启动您的服务器

II.保留服务器计算机

删除 ESMC/ESET PROTECT/MDM 的最便捷方法是格式化其安装磁盘。

该操作会删除磁盘上包括操作系统在内的所有内容。

故障排除

由于ESET PROTECT产品的复杂性（使用多个第三方工具并且支持许多操作系统平台），可能会遇到需要使用“故障排除”解决的问题。

ESET 文档中包括几种 ESET PROTECT 故障排除的方法。请参阅常见安装问题解答以解决使用 ESET PROTECT 时所遇到的某些常见问题。另请参阅 ESET 企业版产品的已知问题。

无法解决问题？

- 每个 ESET PROTECT 组件都有日志文件，可以配置为详细模式，也可以配置简略模式。查看日志以找到可能会解释您所遇到问题的错误。
- 每个组件的日志记录级别都在其以下位置进行设置：策略 > **高级设置** > **日志记录** > **跟踪日志级别** – 设置日志级别以确定收集和记录的信息的级别：从**跟踪**（信息性）到**致命**（最重要的关键信息）。

- ESET Management 服务器代理策略 – 该策略必须应用于设备才能生效。 要在 *trace.log* 文件中启用 ESET Management 服务器代理的完整日志记录，请在 *trace.log* 所在的相同文件夹中创建一个不带扩展名的名为 *traceAll* 的伪文件，然后重新启动计算机（以重新启动 ESET Management 服务器代理服务）。

- ESET PROTECT 服务器设置

- ESET Mobile Device Connector 策略 – 该策略必须应用于设备才能生效。另请参阅 MDM 故障排除

- 如果您无法解决此问题，请访问 ESET 安全论坛并向 ESET 社区请教以了解您可能遇到的问题的信息。

- 联系 ESET 技术支持时，可能会要求您使用 ESET Log Collector 或诊断工具收集日志文件。我们强烈建议您在联系支持人员时提供日志，以便加快客户服务请求的速度。

在脱机环境中升级 ESET PROTECT 组件

遵循以下步骤，升级 ESET PROTECT 组件和 ESET Endpoint 产品，无需访问 Internet

当满足以下条件时，可以将组件升级任务用于脱机环境：
- 有可用的脱机存储库
- ESET Management 服务器代理的存储库位置使用策略配置到一个可访问位置。

升级 ESET PROTECT 服务器和 Web 控制台：

1. 查看服务器上正在运行的 ESET 管理控制台的版本

2. 从 ESET 下载站点下载最新的适用于 Windows 的一体式安装程序或适用于 Linux 的独立 ESET PROTECT 组件安装程序

3. 升级 ESET PROTECT 服务器和 ESET PROTECT Web 控制台：

   - Windows - 使用一体式安装程序升级

   - Linux - 基于组件的手动升级

Web 控制台和 Apache Tomcat 升级会清除脱机帮助文件。如果使用 ESMC 或较早 ESET PROTECT 版本的脱机帮助，请在升级后为 ESET PROTECT 10.0 重新创建它，以确保您有匹配 ESET PROTECT 版本的最新脱机帮助。

继续脱机升级 ESET Endpoint 产品

1. 查看客户端上已经安装的 ESET 产品：打开 ESET PROTECT Web 控制台，依次导航到**面板** > **ESET 应用程序**

2. 确保具有 ESET 端点产品的最新版本

3. 通过 ESET 下载站点将安装程序下载到脱机安装期间配置的本地存储库。

4. 从 ESET PROTECT Web 控制台运行软件安装任务

常见安装问题解答

展开您想要解决的错误消息部分：

ESET PROTECT 服务器

ESET PROTECT 服务器服务不启动：

安装损坏

- 这可能是由于缺少注册表项、缺少文件或文件权限无效造成的。
- ESET 一体式安装程序有其自己的日志文件。手动安装组件时，请使用 MSI 日志记录方法。

侦听端口已使用（很可能是 2222 和 2223）

使用适合您的操作系统的命令：

- Windows:

```
netstat -an | find "2222"
netstat -an | find "2223"
```

- Linux:

```
netstat | grep 2222
netstat | grep 2223
```

数据库不运行/不可访问

- Microsoft SQL Server:验证数据库服务器上的端口 1433 是否可用，或者尝试登录到 SQL Server Management Studio
- MySQL验证数据库服务器上的端口 3306 是否可用，或者尝试登录到您的数据库界面（例如使用 MySQL 命令行界面或 phpmyadmin

数据库损坏

ESET PROTECT 服务器日志文件中会显示多条 SQL 错误。我们建议您从备份中还原您的数据库。如果备份不存在，请重新安装 ESET PROTECT

系统资源RAM磁盘空间）不足

查看运行进程和系统性能：

- Windows 用户：运行“任务管理器”或“事件查看器”并查看信息
- Linux 用户：运行以下命令之一：

`df -h`（用于查看磁盘空间信息）
`cat /proc/meminfo`（用于查看内存空间信息）
`dmesg`（用于查看您的 Linux 系统运行状况）

在 ESET PROTECT 服务器安装期间 ODBC 连接器发生错误

```
Error: (Error 65533) ODBC connector compatibility check failed.
Please install ODBC driver with support for multi-threading.
```

重新安装支持多线程的 ODBC 驱动程序版本，或者重新配置 *odbcinst.ini*（如 ODBC 配置部分所示）。

在 ESET PROTECT 服务器安装期间数据库连接发生错误

安装 ESET PROTECT 服务器结束时，出现以下常见错误消息：

```
The database server is not configured correctly.
Please check the documentation and reconfigure the database server as needed.
```

安装日志中的错误消息：

```
Error: Execution test of long statement failed with exception:
CMysqlCodeTokenExecutor: CheckVariableInnodbLogFileSize:
Server variables innodb_log_file_size*innodb_log_files_in_group
value 100663296 is too low.
```

验证您的数据库驱动程序配置是否与 ODBC 配置部分中所示内容匹配。

ESET Management 服务器代理

ESET Management 服务器代理卸载故障排除

• 请参阅 ESET Management 服务器代理的日志文件。

• 可以采用以下方式卸载 ESET Management 服务器代理：使用 ESET 卸载程序或使用非标准方法（例如删除文件、删除 ESET Management 服务器代理服务和注册表项）。在同一台计算机上装有 ESET Endpoint 产品的情况下，因启用了自我防护，可能无法卸载。
• 在服务器代理卸载期间会显示“数据库无法升级。请先删除产品。”消息 – 修复 ESET Management 服务器代理：
1.依次单击**控制面板** > **程序和功能**，然后双击 **ESET Management 服务器代理**。
2.依次单击**下一步** > **修复**，然后按照说明进行操作。
所有可以卸载 ESET Management 服务器代理的方式在卸载部分中都有介绍。

服务器代理安装期间出现错误代码 1603

当安装程序文件不在本地磁盘上时，会发生此错误。要修复此错误，请将该安装程序文件复制到本地目录，然后重新运行该安装即可。如果这些文件已经存在，或者仍然发生该错误，请按照我们的知识库说明进行操作。

在 Linux 上安装服务器代理期间出现错误消息

错误消息：

```
Checking certificate ... failed
Error checking peer certificate: NOT_REGULAR_FILE
```

此错误的原因可能是安装命令中存在不正确的文件名。控制台区分大小写。例如，`Agent.pfx` 不同于 `agent.pfx`.

从 Linux 到 Windows 8.1（32-位）的远程部署失败

这是由 Microsoft 的 KB3161949 引起的身份验证问题。只能通过从部署失败的主机中删除该更新，才能解决此问题。

ESET Management 服务器代理无法连接到 ESET PROTECT 服务器

请参阅服务器代理连接故障排除和我们的知识库文章。

服务器代理脚本安装程序退出，代码为 30

将服务器代理脚本安装程序与自定义安装程序位置结合使用，但未能正确编辑脚本。查看帮助页面，然后重试。

Web 控制台

ESET BridgeHTTP 代理

ESET Rogue Detector Sensor

为什么以下错误消息持续地记入 ESET Rogue Detector 的 trace.log 中？

```
Information: CPCAPDeviceSniffer [Thread 764]:
CPCAPDeviceSniffer on rpcap://\Device\NPF_
{2BDB8A61-FFDA-42FC-A883-CDAF6D129C6B} throwed error:
Device open failed with error:Error opening adapter:
The system cannot find the device specified. (20)
```

这是 WinPcap 的问题。停用 ESET Rogue Detector Sensor 服务、重新安装最新版 WinPcap（至少为 4.1.0），然后重新启动 ESET Rogue Detector Sensor 服务。

Linux

CentOS Linux 上缺少 libQtWebKit 依赖关系

如果显示以下错误：

```
Error: CReportPrinterModule [Thread 7f5f4c7b8700]:
ReportPrinter: ReportPrinterTool exited with:
/opt/eset/RemoteAdministrator/Server//ReportPrinterTool:
error while loading shared libraries: libQtWebKit.so.4:
cannot open shared object file: No such file or directory [code:127]
```

按照我们的知识库文章中的说明进行操作。

在 CentOS 7 上无法安装 ESET PROTECT 服务器

如果显示以下错误：

```
Error: DbCheckConnection: locale::facet::_S_create_c_locale name not valid
```

该问题可能是因环境/区域设置造成的。在服务器安装程序脚本之前运行以下命令应该会有所帮助：

```
export LC_ALL="en_US.UTF-8"
```

Microsoft SQL Server

在 Microsoft SQL Server 安装期间显示错误代码 -2068052081。

重新启动计算机，然后再次运行安装程序。如果该问题依然存在，请卸载 SQL Server Native Client然后再次运行安装。如果此操作不能解决该问题，请卸载所有 Microsoft SQL Server 产品、重新启动计算机，然后再次运行安装。

在 Microsoft SQL Server 安装期间显示错误代码 -2067922943。

验证您的系统是否满足 ESET PROTECT 数据库要求

在 Microsoft SQL Server 安装期间显示错误代码 -2067922934。

确保具有正确的用户帐户权限

Web 控制台显示“无法加载数据”。

Microsoft SQL Server 尝试让交易记录使用尽可能多的磁盘空间。如果要清理磁盘空间，请访问 Microsoft 官方网站

在 Microsoft SQL Server 安装期间显示错误代码 -2067919934。

确保上述所有步骤都已成功完成。此错误因系统文件配置错误所致。请重新启动计算机，然后再次运行安装。

日志文件

每个 ESET PROTECT 组件都会执行日志记录ESET PROTECT 组件将特定事件的相关信息写入日志文件。日志文件的位置取决于组件。日志文件位置列表如下所示：

Windows

ESET PROTECT组件	日志文件位置
ESET PROTECT 服务器	*C:\ProgramData\ESET\RemoteAdministrator\Server\EraServerApplicationData\Logs*
ESET Management 服务器代理	*C:\ProgramData\ESET\RemoteAdministrator\Agent\EraAgentApplicationData\Logs* 另请参见服务器代理连接故障排除
ESET PROTECT Web 控制台和 Apache Tomcat	*C:\ProgramData\ESET\RemoteAdministrator\Tomcat\Logs* 另请参阅 https://tomcat.apache.org/tomcat-9.0-doc/logging.html
移动设备连接器	*C:\ProgramData\ESET\RemoteAdministrator\MDMCore\Logs* 另请参阅 MDM 故障排除
Rogue Detection Sensor	*C:\ProgramData\ESET\Rogue Detection Sensor\Logs*

ESET PROTECT组件	日志文件位置
ESET BridgeHTTP 代理 –	请参阅 ESET Bridge 联机帮助

C:\ProgramData 默认情况下被隐藏。若要显示该文件夹：
1.导航到**开始 > 控制面板 > 文件夹选项 > 查看**
2.选择**显示隐藏的文件、文件夹和驱动器**，然后单击**确定**

Linux

ESET PROTECT组件	日志文件位置
ESET PROTECT 服务器	*/var/log/eset/RemoteAdministrator/Server/* */var/log/eset/RemoteAdministrator/EraServerInstaller.log*
ESET Management 服务器代理	*/var/log/eset/RemoteAdministrator/Agent/* */var/log/eset/RemoteAdministrator/EraAgentInstaller.log*
移动设备连接器	*/var/log/eset/RemoteAdministrator/MDMCore/* */var/log/eset/RemoteAdministrator/MDMCore/Proxy/* 另请参阅 MDM 故障排除
ESET BridgeHTTP 代理 –	请参阅 ESET Bridge 联机帮助
ESET PROTECT Web 控制台和 Apache Tomcat	*/var/log/tomcat/* 另请参阅 https://tomcat.apache.org/tomcat-9.0-doc/logging.html
ESET RD Sensor	*/var/log/eset/RogueDetectionSensor/*

ESET PROTECT 虚拟设备

ESET PROTECT组件	日志文件位置
ESET PROTECT VA 配置	*/root/appliance-configuration-log.txt*
ESET PROTECT 服务器	*/var/log/eset/RemoteAdministrator/EraServerInstaller.log*
Apache HTTP 代理	*/var/log/httpd*

macOS

/Library/Application Support/com.eset.remoteadministrator.agent/Logs/

/Users/%user%/Library/Logs/EraAgentInstaller.log

诊断工具

诊断工具是所有 ESET PROTECT 组件的一部分。它用于收集和打包日志，这些日志将由技术支持代理人员和开发人员用于解决产品组件的问题。

诊断工具位置

Windows

文件夹 *C:\Program Files\ESET\RemoteAdministrator\<product>***Diagnostic.exe**

Linux

在服务器上的以下目录中：*/opt/eset/RemoteAdministrator/<product>/*，存在一个 **Diagnostic<product>** 可执行文件（一个字词，例如 **DiagnosticServer**、**DiagnosticAgent**）。

用法 (Linux)

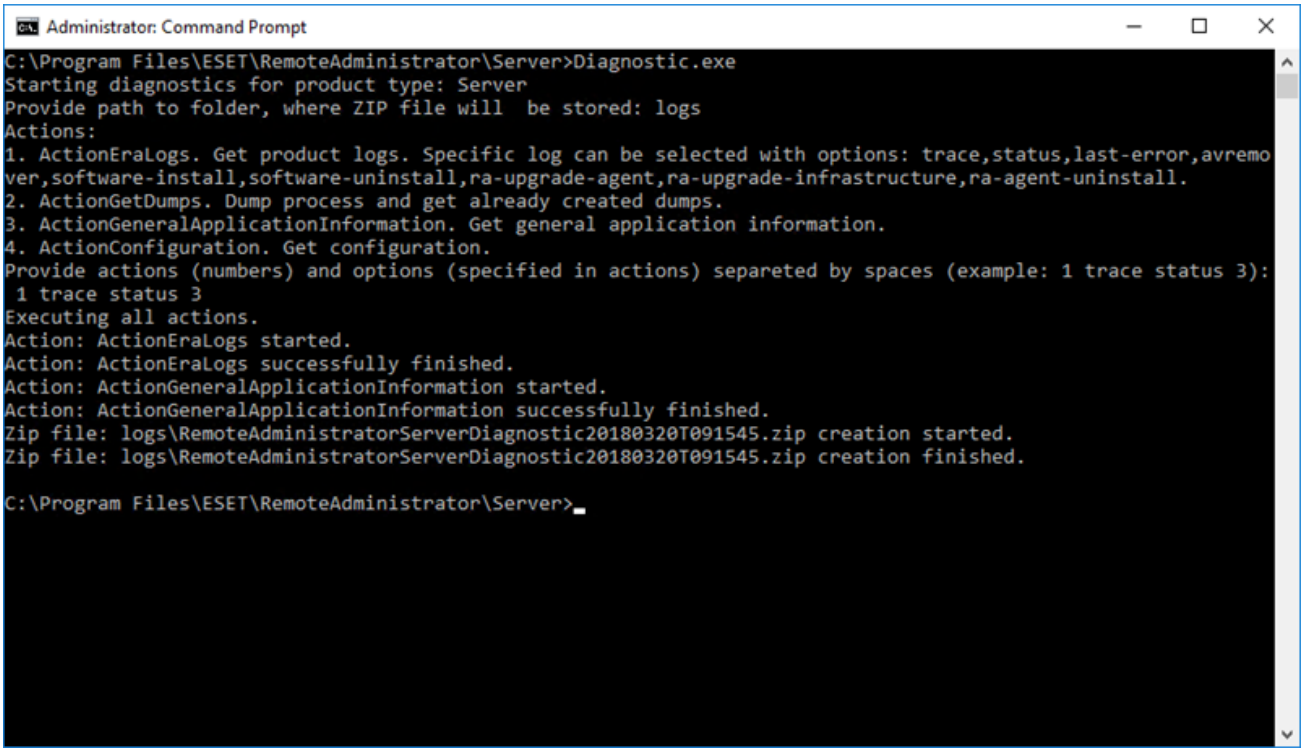
在终端中将诊断可执行文件作为根运行，然后按照屏幕上显示的说明进行操作。

用法 (Windows)

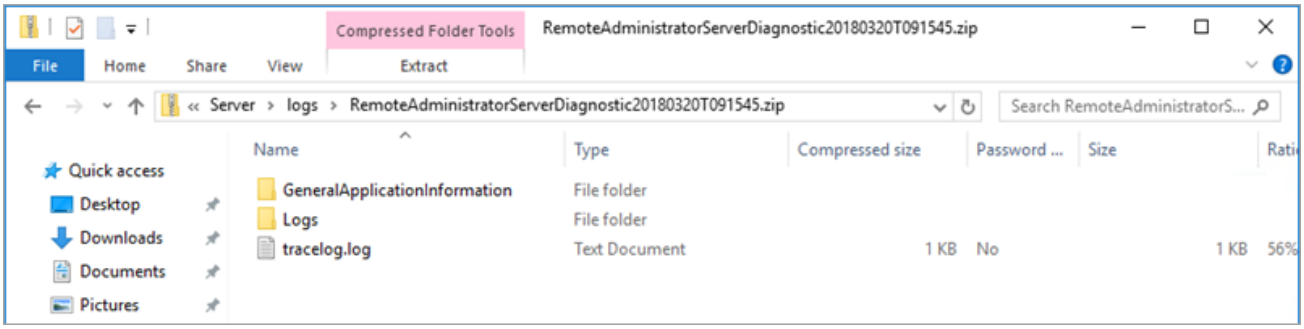
1. 在命令提示符下运行该工具。

2. 输入用于存储日志文件的位置（在我们的示例中为“logs”），然后按 **Enter** 键。

3. 输入您想要收集的信息（在我们的示例中为 `1 trace status 3`）。请参阅以下**操作**以了解详细信息。



4. 操作完成后，可以在诊断工具所在位置的“**logs**”目录中找到压缩为 *.zip* 文件的日志文件。



操作

- **ActionEraLogs** – 将创建日志文件夹，其中会保存所有日志。若要仅指定某些日志，请使用空格分隔每个日志。

- **ActionGetDumps** – 将创建新文件夹。通常在检测到问题的情况下创建进程转储文件。当检测到严重问题时，系统将创建转储文件。若要手动检查它，请转至文件夹 %temp%（在 Windows 中）或者文件夹 /tmp/（在 Linux 中），然后插入一个转储文件。

> 组件服务（Agent、Server、RD Sensor）必须处于运行状态。

- **ActionGeneralApplicationInformation** – 将创建 GeneralApplicationInformation 文件夹，并且在该文件夹中会创建文件 *GeneralApplicationInformation.txt*。此文件包含文本信息，其中包括当前已安装的产品的产品名称和产品版本。

- **ActionConfiguration** – 将创建配置文件夹，其中会保存文件 storage.lua。

升级/迁移 ESET PROTECT 服务器后出现的问题

如果因损坏的安装和未知日志文件错误消息而无法启动 ESET PROTECT 服务器服务，请按照以下所示的步骤进行操作来执行修复：

> 我们建议您在开始修复之前，先执行数据库服务器备份。

1. 导航到**开始 > 控制面板 > 程序和功能**，然后双击 **ESET PROTECT 服务器**。

2. 选择**修复**，然后单击**下一步**。

3. 重新使用现有的数据库连接设置，然后单击**下一步**。**如果系统提示您进行确认，请单击是**。可以在此处找到数据库连接信息：*%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini*

4. 选择**使用已存储在数据库中的管理员密码**，然后单击**下一步**。

5. 选择**保留当前现有的证书**，然后单击**下一步**。

6. 使用有效的许可证密钥激活 ESET PROTECT 服务器，或者选择**以后激活**（有关其他说明，请参阅许可证管理）并单击 **下一步**。

7. 单击**修复**。

8. 重新连接到 Web 控制台并检查一切是否正常。

其他故障排除方案：

ESET PROTECT 服务器不在运行，但存在数据库备份：

1. 恢复数据库备份。

2. 验证新的计算机所使用的 IP 地址或主机名是否与以前的安装相同，以确保服务器代理能够连接。

3. 修复 ESET PROTECT 服务器并使用已恢复的数据库。

ESET PROTECT 服务器不在运行，但具有从中导出的服务器证书和证书颁发机构：

1. 验证新的计算机所使用的 IP 地址或主机名是否与以前的安装相同，以确保服务器代理能够连接。

2. 使用备份证书修复 ESET PROTECT 服务器（修复时，请选择**从文件加载证书**并按照说明操作）。

ESET PROTECT 服务器不在运行，没有数据库备份，也没有 ESET PROTECT 服务器证书和证书颁发机构：

1. 修复 ESET PROTECT 服务器。

2. 使用以下一种方法修复 ESET Management 服务器代理：

   - 服务器代理安装程序脚本
   - 远程部署（这要求您禁用目标计算机上的防火墙）
   - 手动服务器代理组件安装程序

MSI 日志记录

当您无法在 Windows 上正确安装 ESET PROTECT 组件（例如ESET Management 服务器代理）时，这会很有用：

```
msiexec /i C:\Users\Administrator\Downloads\Agent_x64.msi /L*v log.txt
```

ESET PROTECT API

ESET PROTECT ServerApi (*ServerApi.dll*) 是应用程序编程接口，一组用于生成自定义软件应用程序以满足需求和细节的功能和工具。通过使用 ServerApi您的应用程序可以提供您通常通过 ESET PROTECT Web 控制台实现的自定义界面、功能和操作，例如管理 ESET PROTECT生成和接收报告等。

有关详细信息和采用 C 语言的示例以及可用 JSON 消息的列表，请参考以下联机帮助：

ESET PROTECT 10 API

常见问题解答

为什么在服务器上安装 Java此操作不会带来安全风险吗？绝大多数的安全公司和安全框架会建议您从计算机（尤其是服务器）中卸载 Java

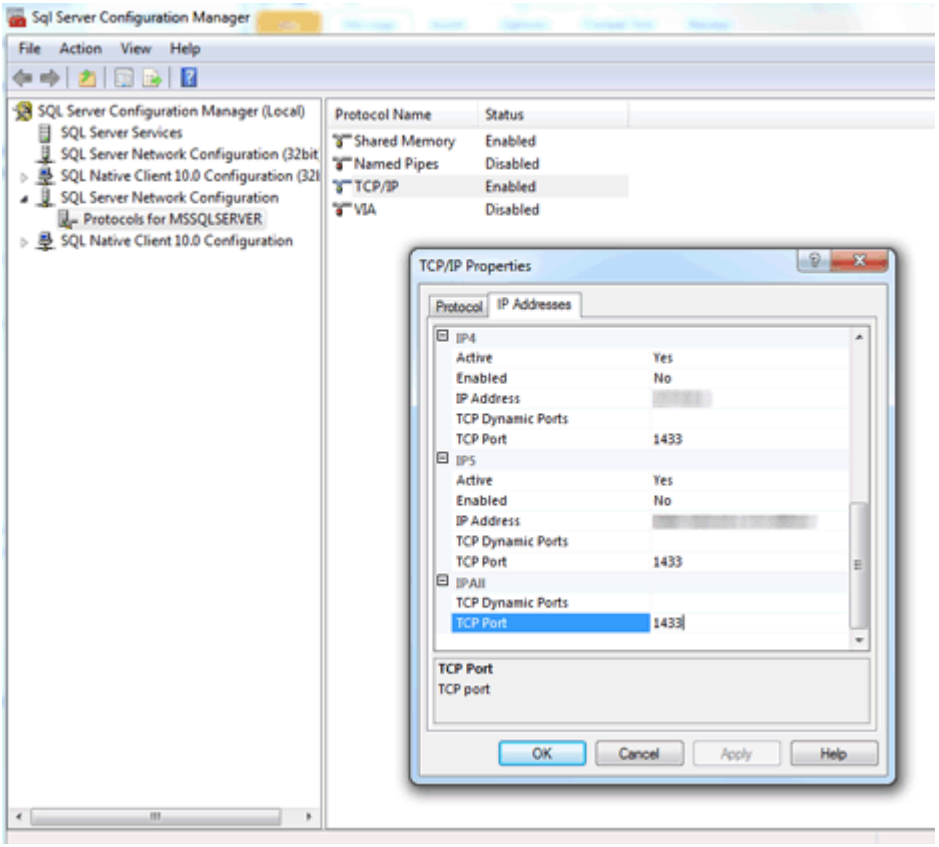
ESET PROTECT Web 控制台需要 Java/OpenJDK 才能运行Java 是基于 Web 的控制台的行业标准，所有主流

Web 控制台都是将 Java 和 Web 服务器 (Apache Tomcat) 用于其操作。需要 Java 才能支持多平台 Web 服务器。出于安全原因，可以在专用计算机上安装 Web 服务器。

从 2019 年 1 月开始，面向企业、商业或生产用途的 Oracle JAVA SE 8 公开更新将需要商业许可证。如果不购买 JAVA SE 订阅，可以使用本指南来转换为免费替代方案。请参阅 JDK 的受支持版本

如何确定 SQL Server 正在使用哪一个端口？

可采用多种方式确定 SQL Server 使用的端口。通过 SQL Server 配置管理器，您可以获取最准确的结果。有关如何在 SQL 配置管理器中找到此信息的示例，请参阅下图：



在 Windows Server 2012 上安装 SQL Server Express（包含在 ESET PROTECT 程序包中）后，它不会显示为在标准 SQL 端口上帧听。它最有可能侦听默认端口 1433 以外的端口。

如何配置 MySQL 以接受较大的数据包？

请参阅 Windows 或 Linux 的 MySQL 安装和配置。

如果我自行安装 SQL，那么如何创建适用于 ESET PROTECT 的数据库？

您不必这样做。数据库是由 *Server.msi* 安装程序创建的，而不是由 ESET PROTECT 安装程序创建的。包含 ESET PROTECT 安装程序的目的在于为您简化步骤，它会安装 SQL Server，然后数据库由 *Server.msi* 安装程序创建。

如果提供给安装程序正确的 Microsoft SQL Server 连接详细信息和凭据，ESET PROTECT 安装程序是否能够在现有 Microsoft SQL Server 安装中为我创建新数据库？如果该安装程序支持不同版本的 SQL Server（2012、2014 等），那么该操作会很方便。

数据库由 *Server.msi* 创建。是的，该安装程序可以在个别已安装的 SQL Server 实例上为您创建 ESET PROTECT 数据库。受支持的 Microsoft SQL Server 版本为 2014 及更高版本。

默认情况下，ESET PROTECT 10.0 一体式安装程序将安装 Microsoft SQL Server Express 2019。

- 如果使用的是旧版 Windows Server 2012 或 SBS 2011，则将默认安装 Microsoft SQL Server Express 2014。
- 安装程序会自动生成一个用于数据库验证的随机密码（存储在 *%PROGRAMDATA%\ESET\RemoteAdministrator\Server\EraServerApplicationData\Configuration\startupconfiguration.ini* 中）。

⚠ Microsoft SQL Server Express 的每个关系数据库具有 10 GB 大小限制。不建议使用 Microsoft SQL Server Express：

- 在企业环境或大型网络中。
- 如果要将 ESET PROTECT 与 ESET Inspect 一起使用。

如果安装在现有 SQL Server 上，SQL Server 应该默认使用内置 Windows 身份验证模式吗？

不是，因为 Windows 身份验证模式可以在 SQL Server 上禁用，而且登录的唯一方式是使用 SQL Server 身份验证（输入用户名和密码）。在安装 ESET PROTECT 服务器过程中，需要进行混合模式身份验证（SQL Server 身份验证和 Windows 身份验证）。在手动安装 SQL Server 时，我们建议您创建根密码（根用户名为“sa”，它代表安全管理的意思），并且将其存储在安全的地方以供将来使用。在升级 ESET PROTECT 服务器时，可能需要根密码。可以在安装 ESET PROTECT 服务器后设置 Windows 身份验证。

我是否可以使用 MariaDB 代替 MySQL？

否，MariaDB 不受支持。 确保安装受支持版本的 MySQL Server 和 ODBC 连接器。 请参阅 MySQL 安装和配置。

我必须按照 ESET PROTECT 安装程序的指示安装 Microsoft .NET Framework 4 (http://www.microsoft.com/en-us/download/details.aspx?id=17851)，但这不适用于附带 SP1 的 Windows Server 2012 R2 的全新安装。

由于 Windows Server 2012 安全策略方面的原因，此安装程序不能在 Windows Server 2012 上使用 Microsoft .NET Framework 必须通过**添加角色和功能向导**进行安装。

很难判断是否正在运行 SQL Server 安装。如果安装所花的时间超过 10 分钟，我如何了解正在发生什么情况？

在极少数情况下，SQL Server 安装可能需要长达 1 小时。安装时间取决于系统性能。

如何为 Web 控制台重置管理员密码（在安装期间输入的密码）？

可以通过运行服务器安装程序和选择**修复**来重置密码。请注意，如果在数据库创建过程中，您没有使用 Windows 身份验证，可能需要密码才能访问 ESET PROTECT 数据库。

- 请务必小心，某些修复选项可能会删除已存储的数据。
- 密码重置会禁用 2FA.

导入包含要添加到 ESET PROTECT 的计算机列表的文件时，文件要求的格式是什么？

该格式为以下几行：

All\Group1\GroupN\Computer1
All\Group1\GroupM\ComputerX

All 是根组的必需名称

是否可以使用 IIS 而不是 Apache Tomcat另一个 HTTP 服务器怎么样？

IIS 是 HTTP 服务器Web 控制台需要 Java 小服务程序容器（如 Apache Tomcat才能运行，而 HTTP 服务器不足以支持控制台运行。现在已有关于如何将 IIS 更改为 Java 小服务程序容器的解决方案，但通常这并不受支持。

我们不使用 Apache HTTP 服务器，我们使用 Apache Tomcat后者是一种不同的产品。

ESET PROTECT 是否具有命令行界面？

是，我们具有 ESET PROTECT ServerApi

能否在域控制器上安装 ESET PROTECT

在域控制器（例如Windows SBS/Essentials上不要安装 SQL Server。建议您在其他服务器上安装 ESET PROTECT或者在安装期间不选择 SQL Server Express 组件（这要求您使用现有 SQL 或 MySQL Server 来运行 ESET PROTECT 数据库）。

如果系统上已安装 SQLESET PROTECT 服务器安装能否检测到？如果检测到，会发生什么？如果是 MySQL 呢？

如果您使用的是安装向导并已选择要安装的 SQL ExpressESET PROTECT 将检查 SQL 是否在系统上运行。如果系统上存在正在运行的 SQL该向导会显示一条卸载现有 SQL 后再次运行该安装的通知，或安装 ESET PROTECT 而不安装 SQL Express 的通知。请参阅适用于 ESET PROTECT 的数据库要求

可以在何处根据 ESET PROTECT 的发行版本找到其相应组件？

请参阅我们的知识库文章

如何执行升级 ESET PROTECT 到最新版本？

请参阅升级过程

如何在没有 Internet 连接的情况下更新系统？

在本地网络上，使用安装在计算机上的可连接到 ESET 更新服务器（更新文件缓存于其中）的 ESET Bridge HTTP 代理，并将 Endpoint 指向该 HTTP 代理。如果您的服务器不具有 Internet 连接，您可以在一台计算机上启用 Endpoint 产品的镜像功能、使用 U 盘将更新文件传递至此计算机，然后配置其他所有脱机计算机以将其用作更新服务器。

有关如何执行脱机安装的详细信息，请按照这些说明操作

如果初始 ESET PROTECT 安装已自动安装现有 SQL Server我如何重新安装 ESET PROTECT 服务器并将其连接到该 SQL Server

如果要使用安装原始 ESET PROTECT Server 时所使用的相同用户帐户（例如，域管理员帐户）安装 ESET PROTECT Server 的新实例，则可以使用**通过 Windows 身份验证的 MS SQL Server**

如何解决 Linux 上的 Active Directory 同步问题？

确认输入的域名使用的全部都是大写字母（`administrator@TEST.LOCAL` 而不是 `administrator@test.local`

是否存在使用我自己的网络资源（如 SMB 共享）而非存储库的方法？

您可以选择提供程序包所在位置的直接 URL。如果要使用文件共享，请使用以下格式指定它。file:// 后跟文件的完整网络路径，例如：

file://\\eraserver\install\ees_nt64_ENU.msi

如何重置或更改我的密码？

理想情况下，管理员帐户应该仅用于为个别管理员创建帐户。在创建管理员帐户后，应保存管理员密码，并且不应使用该管理员帐户。这种做法使管理员帐户仅限用于密码重置/帐户详细信息。

如何为内置 ESET PROTECT 管理员帐户重置密码：

1.打开**程序和功能**（运行 appwiz.cpl），找到 ESET PROTECT 服务器并右键单击它。

2.从右键菜单中选择**更改**。

3.选择**修复**。

4.指定数据库连接详细信息。

5.选择**使用现有数据库并应用升级**。

6.取消选中**使用已存储在数据库中的密码**并输入新密码。

7.使用新密码登录到 ESET PROTECT Web 控制台。

强烈建议您根据所需帐户功能创建具有特定访问权限的其他帐户。

如何更改 ESET PROTECT 服务器和 ESET PROTECT Web 控制台端口？

若要允许 Web 服务器连接到新端口，需要更改 Web 服务器配置中的端口。要执行该操作，请遵循以下步骤：

1.关闭 Web 服务器。
2.修改 Web 服务器配置中的端口。
*a)*打开文件 *webapps/era/WEB-INF/classes/sk/eset/era/g2webconsole/server/modules/config/EraWebServerConfig.properties*
*b)*设置新端口号（例如 `server_port=44591`）

3.再次启动 Web 服务器。

是否可以通过一体式安装程序，将 ERA 5.x/6.x 或 ESMC 7.x 直接升级到 ESET PROTECT 10.0？

如果您有 ERA 5.x/6.x 或 ESMC 7.0/7.1：

- 不支持直接升级到 ESET PROTECT 10.0。
- 执行全新安装 ESET PROTECT 10.0。

可以从 ESMC 7.2 及更高版本直接升级到 ESET PROTECT 10.0。

我收到错误消息或者在使用 ESET PROTECT 时发生问题，我该如何做？

请参阅故障排除常见问题解答。

最终用户许可协议

自 2021 年 10 月 19 日起生效。

重要说明：在下载、安装、复制或使用前，请仔细阅读产品应用程序的以下条款。**下载、安装、复制或使用本软件即表示您同意这些条款和条件并承认隐私政策** 隐私政策。

最终用户许可协议

本最终用户使用许可协议（“协议”）由 ESET, spol. s r. o.(“ESET”或“提供商”）与作为自然人或法人的您（“您”或“最终用户”）签订。ESET 位于 Einsteinova 24, 85101 Bratislava, Slovak Republic，注册地为布拉迪斯拉发第一地区法院商业注册处，企业性质为股份有限公司，注册号 3586/B，BIN 31333532。协议授权您使用此处第 1 条中定义的软件。此处条款 1 中定义的软件可能存储在数据承载工具上、通过电子邮件发送、从 Internet 下载、从提供商的服务器下载或者按照以下指定的条款从其他来源获得。

这不是购买合同，而是关于最终用户权利的协议。无论是此软件的副本，还是经过商业包装的包含此软件的物理介质，亦或根据本协议最终用户有权使用的任何其他副本，所有权均归提供商所有。

在安装、下载、复制或使用软件过程中单击“我接受”或“我接受…”，即表示您同意本协议的条款和条件并确认隐私政策。如果您不同意本协议的任意条款及条件和/或隐私政策，请立刻单击取消选项、取消安装或下载、销毁或退还本软件、安装介质、随附文档和购买发票给提供商或您从中获取软件的渠道。

您同意使用软件表示您已经阅读本协议，您理解并同意遵守本协议的条款。

1.**软件。**本协议中的“软件”是指: (i) 本协议附带的计算机程序及其所有组成部分；(ii) 磁盘、CD-ROM、DVD、电子邮件及任何附件或附带本协议提供的其他介质的所有内容，包括数据承载工具提供、通过电子邮件提供或通过 Internet 下载的对象代码形式的软件；(iii) 任何有关本软件的书面说明材料和任何其他相关文档，包括但不限于所有软件说明、软件规格、软件特点或操作说明、使用软件的操作环境的说明、使用或安装软件的说明，或任何关于如何使用软件的说明（以下称“文档”）；(iv) 软件的副本、软件错误的修复程序、软件的附加程序、软件的扩展、软件的修改版本及软件组件更新（如果有），关于这一点，提供商根据本协议

第 3 条授予您许可。软件将仅以可执行目标代码的形式提供。

2.**安装、计算机和许可证密钥。**数据承载工具上提供、通过电子邮件发送、从 Internet 下载、从提供商服务器下载或从其他来源获得的软件需要安装。文档中指定了安装方式。任何可能对本软件有不利影响的计算机程序或硬件都不能安装在安装本软件的计算机上。计算机是指硬件，包括但不限于个人计算机、笔记本电脑、工作站、掌上电脑、智能电话、手持电子设备或本软件针对其而设计并将于其上安装和/或使用的其他电子设备。任何可能对本软件有不利影响的计算机程序或硬件都不能安装在安装本软件的计算机上。计算机是指硬件，包括但不限于个人计算机、笔记本电脑、工作站、掌上电脑、智能电话、手持电子设备或本软件针对其而设计并将于其上安装和/或使用的其他电子设备。许可证密钥是指唯一的符号、字母、数字或特殊符号的序列，提供给最终用户以允许本软件的合法使用、其特定版本或根据本协议延长许可证的期限。

3.**许可**。如果您同意本条件，同意本协议条款并且遵守此处规定的所有条款，提供商将授予您以下权利(“许可”)：

a) **安装和使用。**您将具有在计算机硬盘或其他永久介质中安装软件以进行数据存储，在计算机系统内存中安装和存储软件，实施、存储和显示软件的非独占、不可转让的权利。

b) **许可数量规定。**软件的使用权利受最终用户数量约束。一位最终用户指(i) 在一个计算机系统上安装软件；或 (ii) 如果许可约束范围为邮箱数量，则单个用户指的是通过邮件用户代理(“MUA”)接收电子邮件的计算机用户。如果 MUA 接受电子邮件，然后将其自动分发到多个用户，则最终用户数量应根据收到电子邮件的实际用户数量确定。如果邮件服务器执行邮件网关的功能，则最终用户数量应等于上述网关所服务的邮件服务器用户数量。如果未指定数量的电子邮件地址（例如通过别名）指向一个用户，用户接受这些地址，并且客户端不自动将邮件分发给大量用户，则需要一台计算机的许可证。您不得同时在多台计算机上使用同一许可。仅当最终用户根据限制（因提供商授予的许可证数量而引起）而有权使用本软件时，最终用户才有权输入本软件的许可证密钥。许可证密钥被视为保密信息，除非本协议或提供商允许，否则您不得与第三方共享许可证或允许第三方使用许可证密钥。如果您的许可证密钥被盗用，请立即通知提供商。

c) **家庭版/商业版。**本软件的家庭版应仅在私人和/或非商业环境中专供家庭和家人使用。必须获得本软件的商业版，才能在商业环境中使用，以及将本软件用于邮件服务器、邮件中继、邮件网关或 Internet 网关。

d) **许可条款。**您使用软件的权利将受时间限制。

e) **OEM 软件。**分类为“OEM”的软件应限于在您获得该软件的计算机上使用。不得转移到其他计算机。

f) **NFR/试用软件。**分类为“非转售性”/NFR 或试用的软件不得用于付费用途，只能用于演示或测试软件功能。

g)**许可终止。**许可将在授予的期限结束时自动终止。如果不遵守本协议的任何条款，提供商有权撤销协议，不影响提供商在此类不测事件下的任何权利或合法补救措施。如果取消许可，您必须立刻删除、销毁本软件及所有备份副本，或自行承担费用将软件及所有备份副本返还至 ESET 或您购买软件的地方。在许可终止后，提供商有权取消最终用户使用本软件功能（这些功能需要连接到提供商的服务器或第三方服务器）的权利。

4.**具有数据收集和 Internet 连接要求的功能。**要正确操作本软件，需要连接到 Internet/并且必须定期连接到提供商服务器或第三方服务器和遵循“隐私政策”的适用的数据收集。要正常使用本软件以及更新和升级本软件，必须连接 Internet 并收集适用数据。提供商有权发布本软件的更新或升级（即“更新”），但没有义务提供更新。此功能在软件标准设置下启用，因此自动安装更新，除非最终用户禁用自动安装更新。为了提供更新，需要进行许可证真实性验证，包括根据“隐私政策”获取其上安装本软件的计算机和/或平台的相关信息。

任何更新的提供可能都要遵循生命周期结束政策（即“EOL 政策”），可通过访问 https://go.eset.com/eol_business 了解该政策。在本软件或其任何功能达到 EOL 政策中定义的生命周期结束日期后，将不会提供任何更新。

就本协议而言，有必要收集、处理和存储数据，使提供商能够根据隐私政策识别您的身份。您特此承认提供商以自有方式检查您是否按照本协议条款使用此软件。您特此承认，就本协议而言，需要通过与提供商计算机系统或作为其分销和支持网络的商业合作伙伴进行软件通信来传输数据，以确保软件功能正常、授权使用软件以及保护提供商的权利。

本协议缔结后，提供商或作为其分销和支持网络的任何商业合作伙伴均有权传输、处理和存储标识您的重要数据，用于计费目的、本协议的履行以及您计算机上通知的传输。

关于隐私、个人数据保护和您作为数据主体所拥有权利的详细信息可以在“隐私政策”（“隐私政策”可在提供商的网站上找到，并可在安装过程中直接访问）中找到。您还可以从软件的帮助部分中访问此信息。

5.**行使最终用户的权利**。您必须亲自或通过员工行使最终用户权利。您只能将软件用于确保操作安全和保护购买了许可证的计算机或计算机系统

6.**权利的限制。**您不得复制、分发、提取组件或创建软件的衍生版本。使用软件时，您必须遵守以下限制：

a) 您可以在永久存储介质上创建一份软件副本作为备份副本，前提是不在任何其他计算机上安装或使用该存档备份副本。创建软件的任何其他副本应视为违反本协议。

b) 您不得以本协议明确提供的方式以外的任何其他方式使用、修改、翻译、复制或转让软件或软件副本的使用权。

c)您不得出售软件、授予从属许可、将软件出租给他人，或从他人租用软件或借出软件用于提供商业服务。

d) 您不得在法律明确禁止此类限制的范围之外以任何其他方式反向工程、反编译、反汇编软件，或试图获得软件的源代码。

e) 您同意使用软件的方式必须符合有关软件使用的相关法律中的所有适用法规，包括但不局限于，符合版权法和其他知识产权中适用的限制。

f) 您同意将只以不会限制其他最终用户获取这些服务的可能性的方式使用该软件及其功能。提供商保留限制向个体最终用户提供的服务范围，以确保最大数量的最终用户能够使用服务的权利。限制服务范围还将意味着完全杜绝在提供商的服务器或与软件的特定功能相关的第三方服务器上使用软件的任何功能和删除数据及信息的可能性。

g) 您同意不从事涉及使用许可证密钥的任何违反本协议条款的活动，或向任何无权使用本软件的人员提供许可证密钥，例如以任何形式转让已使用或未使用的许可证密钥，以及未经授权复制或分发复制或生成的许可证密钥，或从提供商以外的来源获得许可证密钥从而使用本软件。

7.**版权**。软件及所有权利，包括但不局限于所有权和知识产权，归 ESET 和/或其许可提供商所有。它们受国际条约条款以及使用此软件的国家的所有其他适用法律保护。软件的结构、组织和代码均为 ESET 和/或其许可提供商的重要商业机密和保密信息。您不得复制软件，第 6 (a) 款中指定的情况除外。允许按照本协议创建的任何副本必须包含与软件上显示的相同版权和其他所有权声明。如果您反向工程、反编译、反汇编源或试图以违反本协议条款的方式获得软件源代码，则您同意自此类行为开始起获得的任何信息将自动且不可逆地转让给提供商，并全部为提供商所有。

8.**保留权利**。除本协议中未明确授予您作为软件最终用户的权利以外，提供商特此保留所有软件权利。

9.**多个语言版本，双介质软件，多个副本**。如果软件支持多个平台或多种语言，或者如果您获得多个软件副本，则只能将软件用于已购买许可的计算机系统数量和版本。您不得将不使用的软件的任何版本或副本出售、出租、租用、授予从属许可、借出或转让给其他人。

10.**协议开始和终止。**本协议自您同意本协议条款之日起生效。您可以通过永久卸载、销毁或返还（费用自付）软件、所有备份副本以及提供商或其商业合作伙伴提供的所有相关材料来随时终止本协议。您使用软件及其任何功能的权利可能要遵循 EOL 政策。在本软件或其任何功能达到 EOL 政策中定义的生命周期结束

日期后，您使用本软件的权利将终止。不考虑本协议终止方式，第 7、8、11、13、19 和 21 款的条款应保持无限期有效。

11.**最终用户声明**。作为最终用户，您了解软件“按原样”提供，不带任何明示或暗示担保，在适用法律允许的最大范围内。提供商、其许可提供商或分支机构或者版权所有者都不得提供任何明示或暗示的陈述或保证，包括但不限于适销性保证、特定用途适用性保证或对软件不侵犯任何第三方专利、版权、商标或其他权利的保证。提供商或任何其他方均不保证软件包含的功能符合您的要求，或软件操作将顺畅无错为实现预期目的而选择此软件以及安装、使用此软件和软件应用结果的全部责任和风险由您承担。

12.**无其他义务**。除本协议特别列出的义务以外，本协议不对提供商及其许可提供商施加任何其他义务。

13.**责任限制**。在适用法律允许的最大范围内，任何情况下提供商、其员工或许可提供商均不对以下损失负责：在适用法律允许的最大范围内，任何情况下提供商、其员工或许可提供商均不对以下损失负责：以任何形式造成的任何赢利、收入或销售额损失，任何数据损失，为获得备用物品或服务支付的额外费用，财产损失、人身伤害，营业中断，商业信息损失，或任何特殊、直接、间接、意外、经济、涵盖、犯罪、特殊或后继损失。无论这些损失是由合约、故意误操作、疏忽或其他责任理论造成，还是因安装、使用或无法使用本软件导致，提供商、其员工或许可提供商均不负责，即使已经通知提供商或其许可提供商或分支机构此类损失的可能。由于某些国家和某些法律不允许免责，但可能允许责任限制，因此提供商、其员工或许可提供商的责任应限制为您购买许可所支付的价格。

14. 本协议中的任何条款均不影响被法律认可具备消费者权利和地位的一方的权利。

15.**技术支持**ESET 或 ESET 委托的第三方将出于自行考量提供技术支持，不具有任何保证或声明。在本软件或其任何功能达到EOL政策中定义的生命周期结束日期后，将不会提供任何技术支持。提供技术支持前，最终用户需要备份所有现有数据、软件和程序工具ESET 和/或 ESET 委托的第三方不承担因提供技术支持导致的数据、财产、软件或硬件破坏或损失或者利润损失ESET 和/或 ESET 委托的第三方保留决定解决问题是否超出技术支持范围的权利ESET 保留出于自行考量拒绝、暂停或终止提供技术支持的权利。出于提供技术支持的目的，可能需要遵循“隐私政策”的许可证信息、信息和其他数据。

16.**转让许可**。除非违背协议条款，否则软件可以在不同计算机系统之间转移。如果不违背协议条款，最终用户仅有权在提供商同意下，将许可及从本协议产生的所有权利转让给其他最终用户，并受以下条款约束(i) 原始最终用户不得保留软件的任何副本(ii) 权利转让必须从原始最终用户转交给新最终用户(iii) 新最终用户必须承担原始最终用户在本协议条款下承担的所有权利和义务(iv) 原始最终用户必须向新最终用户提供文档，证明第 17 款下指定的软件正版性。

17.**证明软件的正版性。**最终用户可以采用以下任意方式证明软件的使用权(i) 通过提供商或提供商指定的第三方发布的许可证书(ii) 通过书面许可协议，如果已缔结此类协议(iii) 通过提交发送给提供商的包含许可详细信息(用户名和密码)的电子邮件。出于证明软件正版性的目的，可能需要遵循“隐私政策”的许可证信息和最终用户身份数据。

18.**政府当局和美国政府许可**。软件提供给政府当局（包括美国政府）时具有本协议介绍的许可权利和限制。

19.**贸易控制合规性**

a) 您将不得直接或间接地向任何人出口、再出口、转让或以其他方式提供该软件，不得以任何方式使用该软件，也不得涉及任何行为，否则可能导致 ESET 或其控股公司、其子公司及其任何控股公司的子公司以及由其控股公司控制的实体（“关联公司”）违反《贸易管制法》或承担《贸易管制法》所规定的不良后果，包括

i. 美国、新加坡、英国、欧盟或其任何成员国的任何政府、州或监管机构、将履行本协议规定义务的国家/地区、成立或运维 ESET或其任何关联企业的国家/地区颁布或通过的针对出口、再出口或转让商品、软件、技术或服务进行控制、限制或施加许可要求的任何法律，和

ii. 美国、新加坡、英国、欧盟或其任何成员国的任何政府、州或监管机构、将履行本协议规定义务的国家/地区、成立或运维ESET或其任何关联企业的国家/地区实施的任何经济、金融、贸易或其他方式的制裁、

限制、禁运、进出口禁令、禁止转移资金或资产或提供服务或其他等效措施。

（上述“i.”和“ii.”部分中提到的法律行为统称为“《贸易管制法》”）。

b) 如果发生以下情况，ESET 有权立即中止或终止这些条款所规定的义务：

i.ESET 合理认为用户已违反或可能违反了本协议第 19 a) 款的规定；或

ii. 最终用户和/或软件受《贸易管制法》约束，因此 ESET 合理认为继续履行本协议所规定的义务可能会导致 ESET 或其关联公司违反《贸易管制法》，或承担《贸易管制法》所规定的不良后果。

c) 本协议无意，也不应理解或解释为诱导或要求任何一方以不遵循《贸易管制法》、受《贸易管制法》处罚或禁止的方式行事或不作为（或者同意行事或不作为）。

20.**通知**。所有通知、返还的软件和文档必须交付给 ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic，但不影响 ESET 根据本协议的第 22 条有权向您传达对本协议、隐私政策、EOL 政策以及文档所做的任何更改。ESET 可能会通过软件向您发送电子邮件、应用内通知，也可能会在我们的网站上发布通信帖子。您同意接收 ESET 以电子形式发送的法律通信，包括有关条款、特殊条款或隐私政策变更的任何通信、任何合同修改/赞同、要约邀请、通知或其他法律通信。此类电子通信应等同于书面形式接收，除非适用法律明确要求采用其他形式的通信。

21.**适用法律**。本协议受斯洛伐克法律管辖，并按斯洛伐克法律解释。最终用户和提供商同意，法律与联合国国际货物销售合同公约之间的冲突原理不适用。您明确同意，与提供商之间发生的任何索赔或争端，或任何方式的与软件使用相关的索赔或争端，其唯一裁决权属于斯洛伐克布拉迪斯拉发第一地区法院，并且您明确同意上述法院作出的裁决。

22.**通用条款**。如果本协议中的任何条款无效或无法执行，将不影响协议其他条款的有效性，按照此处规定的条款这些条款仍然有效且可执行。本协议已以英文履行。如果出于方便目的或任何其他目的而准备了本协议的任何翻译，或者本协议的各语言版本之间存在差异，则以英文版本为准。

ESET 保留随时更改本软件以及出于以下目的修订本协议的条款、其附件、附录、隐私政策、EOL 政策和文档或其任何部分的权利：(i) 反映对本软件或 ESET 开展业务方式的更改；(ii) 出于法律、法规或安全原因，或 (iii) 防止滥用或损害。将通过电子邮件、应用内通知或其他电子方式通知您本协议的任何修订。如果您不同意对本协议的拟议变更，可以在收到变更通知后的 30 内，根据第 10 条终止履行本协议。除非您在该时限内终止履行本协议，否则拟议变更将视为被接受，并自您收到变更通知之日起开始对您生效。

您与提供商签署的本协议是关于本软件的唯一完整协议，它完全取代任何之前的关于软件的表述、讨论、承诺、沟通或广告。

协议附录

将信息转发给提供商。适用于“将信息转发给提供商”的附加条款如下所示：

本软件包含收集信息的功能，可收集有关安装过程的数据、有关安装本软件的计算机和/或平台的数据、有关本软件的操作和功能的信息以及有关托管设备的信息（以下简称“信息”），然后将它们发送给提供商。信息可能包含涉及托管设备的数据（包括随机或意外获得的个人数据）。如果您启用本软件的上述功能，则“威胁”和“信息”可由提供商按照“隐私政策”和相关法规收集和处理。

软件需要在托管计算机上安装组件，以便在托管计算机和远程管理软件之间传输信息。需要传输的信息包含管理数据，如托管计算机的硬件和软件信息、来自远程管理软件的管理指令。从托管计算机传输的其他数据的内容应由安装在托管计算机上的软件的设置确定。管理软件的指令内容应由远程管理软件的设置确定。

EULAID: EULA-PRODUCT-PROTECT; 3537.0

隐私政策

ESET, spol. s r. o.注册办公室位于斯洛伐克共和国 Einsteinova 24, 851 01 Bratislava在布拉迪斯拉发第一地区法院商业注册处注册，企业性质为股份有限公司，注册号为 3586/B业务识别号：31333532（简称为“ESET”或“我们”ESET 希望在处理个人数据和客户隐私时保持透明。为了达到上述目的，我们发布了此隐私政策，唯一目的是告知我们的客户（“最终用户”或“您”）有关以下主题的信息：

- 个人数据处理、
- 数据机密性、
- 数据主体的权利。

个人数据处理

在我们的产品中实施的由 ESET 提供的服务是根据最终用户许可协议“EULA”提供的，但其中一些可能需要特别注意。我们希望为您提供与服务提供有关的数据收集的更多详细信息。我们提供最终用户许可协议和产品文档中所述的各种服务，例如更新/升级服务ESET LiveGrid®防止数据滥用、支持等。为了正常运行，我们需要收集以下信息：

- 管理 ESET Security 产品需要并会本地存储信息（如席位 ID 和名称、产品名称、许可证信息、激活和过期信息、有关安装有 ESET Security 产品的托管计算机的硬件和软件信息）。将收集并提供有关托管 ESET Security 产品和设备的活动的日志，以便帮助管理和监管功能和服务，而无需自动提交给 ESET
- 有关安装过程的信息（包括安装产品的平台）以及有关产品的操作和功能的信息（如硬件指纹、安装 ID崩溃转储、许可证 IDIP 地址MAC 地址、产品的配置设置，可能还包括托管设备的）。
- 为了计费、许可证真实性验证和服务提供，需要提供许可证信息（如许可证 ID和个人数据（如姓名、地址、电子邮件地址）。
- 支持服务可能需要您的支持请求中包含联系信息和数据。根据您选择与我们联系的渠道，我们可能会收集您的电子邮件地址、电话号码、许可证信息、产品详细信息和支持案例描述。可能会要求您向我们提供其他信息，以便于提供支持服务。
- 在会话期间，有关使用我们的服务的数据完全是匿名的。在会话结束后，不会存储任何个人身份信息。

数据机密

ESET 是一家通过附属实体或合作伙伴（作为我们分销、服务和支持网络的一部分）在全球运营的公司。出于 EULA 的履行（例如，提供服务、支持或计费）考虑，经 ESET 处理的信息可能会在附属实体或合作伙伴之间传输。根据您的位置和选择要使用的服务，欧盟委员会可能会要求我们将您的数据传输到缺乏妥善决策的国家/地区。即使在这种情况下，每一次信息传输都会遵守数据保护法规，并且仅在需要时才会进行传输。必须毫无例外地建立标准合同条款、约束性企业规则或其他适当保护措施。

在根据最终用户许可协议提供服务的同时，我们会尽最大努力防止存储数据超过必要时间。我们的保留期可能长于许可证的有效期，只是让您有时间轻松方便地续订。出于统计目的，可能会进一步处理来自 ESET LiveGrid® 的必要和匿名统计信息和其他数据。

ESET 会实施适当技术和组织措施来确保与潜在风险相称的安全级别。我们会尽最大努力来确保提供处理系统和服务所需的持续机密性、完整性、可用性和灵活性。但当发生导致您的权利和自由遭受威胁的数据泄漏时，我们会随时通知监管机构以及数据主体。作为数据主体，您有权向监管机构提出投诉。

数据主体的权利

ESET 遵守斯洛伐克法律的规定，并且我们受欧盟的数据保护法的约束。在遵守适用数据保护法律规定条件的前提下，您作为数据主体享有以下权利：

- 有权请求访问 ESET 收集的您的个人数据，
- 有权更正可能不准确的个人数据（您也有权补充不完整的个人数据），
- 有权请求清除您的个人数据，
- 有权请求限制处理您的个人数据，
- 有权反对处理
- 还有权提出投诉
- 数据迁移。

如果您希望行使作为数据主体的权利或有疑问，请发送邮件至：

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk