Mac-Lab/CardioLab 防病毒安装说明 (ZH-CN)

Mac-Lab/CardioLab 软件版本 6.9.6

前言

防病毒软件可协助贵机构遵守隐私规定（例如 HIPAA）。

文档使用

使用此文档来安装适合 Mac-Lab/CardioLab v6.9.6 系统的经过验证的防病毒软件。

修订历史

版本	日期	注释
A	2016 年 2 月 16 日	初次公开发行。
B	2016 年 6 月 9 日	Trend Micro 更新以支持 CO_2。
C	2017 年 5 月 16 日	对 McAfee ePolicy Ochestrator、 Trend Micro 和 Symantec 进行更新。
D	2017 年 7 月 10 日	对 Symantec 12.1.6 MP5、 Trend Micro 11.0 SP1、 McAfee ePO 5.9 和 McAfee VSE 8.8 Patch 9 进行更新。
E	2017 年 8 月 14 日	删除对 McAfee ePolicy Orchestrator 5.9 和 McAfee VirusScan Enterprise 8.8 Patch 9 的引用。增加 6.9.6 R3 UI 语言。
F	2017 年 9 月 25 日	增加 McAfee ePO 5.9 和 McAfee VSE 8.8 Patch 9。更新 Trend Micro 11 和 12 的链接。

入门指南

防病毒要求

警告： **需要安装防病毒软件**

本系统在交付时并未安装防病毒软件。在将系统连入任何网络之前，请先为系统安装经过验证的防病毒软件。不安装经过经过验证的防病毒软件可导致系统不稳定或出故障。

注意以下要求：

- Mac-Lab/CardioLab 系统并未提供防病毒软件，因此客户有责任自行选购、安装和维护防病毒软件。
- 客户负责更新防病毒软件的病毒定义文件。
- 如果发现了病毒，请联系设备系统管理员和 GE 技术支持。
- 仅安装 “ 经过验证的防病毒软件 ” 部分中列出的防病毒软件包。
- 以管理员或管理员组成员的身份登录，以执行此文档中的活动。
- 如有可能，请使用语言版本与操作系统的语言相匹配的有效防病毒软件。如果不具备与操作系统的语言相匹配的有效防病毒软件，则请安装英语版本的防病毒软件。

经过验证的防病毒软件

警告： **系统不稳定性**

切勿安装或使用未经验证的防病毒软件（包括未经验证的版本）。因为这样做可以导致系统不稳定或出故障。只限使用相应语言版本的经验证的防病毒软件。

注意： 如果无法获得特定语言版本的防病毒软件，请安装英语版防病毒软件。

经验证， Mac-Lab/CardioLab v6.9.6 系统可以运行下表中所列出的软件。

支持的防病毒软件	支持的 MLCL 语言	支持的防病毒软件版本
McAfee VirusScan Enterprise	英语、法语、德语、意大利语、西班牙语、瑞典语、挪威语、丹麦语、荷兰语、中文和日语	8.8 Patch 3 8.8 Patch 4 8.8 Patch 8 8.8 Patch 9
McAfee ePolicy Orchestrator（配有 McAfee VirusScan Enterprise）	英语、法语、德语、意大利语、西班牙语、瑞典语、挪威语、丹麦语、荷兰语、中文和日语	v5.0 v5.3.2 v5.9
Symantec EndPoint Protection	英语、法语、德语、意大利语、西班牙语、瑞典语、挪威语、丹麦语、荷兰语、中文和日语	12.1.2、 12.1.6 MP5、14.0 MP1
Trend Micro OfficeScan Client/Server Edition	英语、法语、德语、意大利语、西班牙语、瑞典语、挪威语、丹麦语、荷兰语、中文和日语	10.6 SP2、 11.0 SP1、XG 12.0

受支持的防病毒软件有下表中列出的语言版本。

MLCL 版本	支持的 MLCL 语言
M6.9.6 R1	简体中文
M6.9.6 R2	英语、法语、德语
M6.9.6 R3	英语、法语、德语、意大利语、西班牙语、瑞典语、挪威语、丹麦语、荷兰语、中文和日语

防病毒 Management Console Server 配置

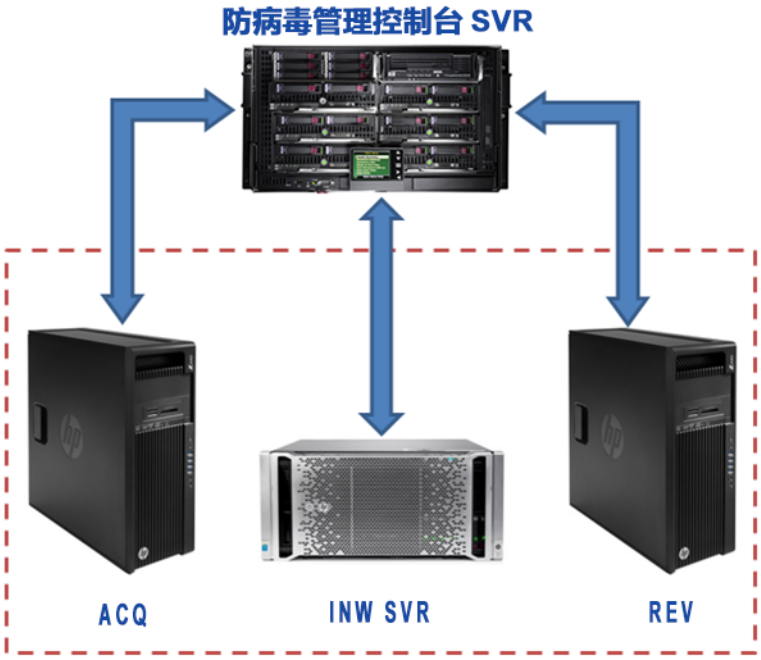
必须在 防病毒 Management Console Server 上安装 防病毒 Management Console。

防病毒 Management Console Server 与 Mac-Lab/CardioLab 设备之间的通信可环境以不同的方式进行：

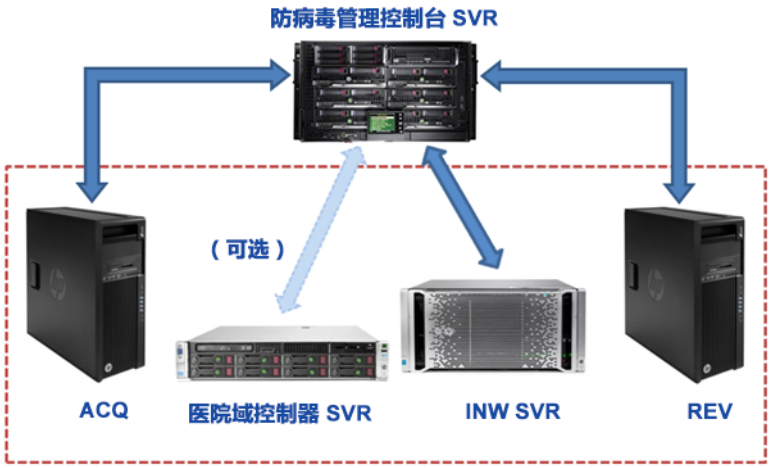
1. INW 域控制器环境 - 防病毒 Management Console SVR 不在 INW Server 域中
   - 通信类型 - 1 < 具有相同子网掩码的相同网络 >
   - 通信类型 - 2 < 具有不同子网掩码的不同网络 >
2. 医院域控制器环境 - 防病毒 Management Console SVR 不在医院域控制器域中
   - 通信类型 - 1 < 具有不同子网掩码的不同网络 >
3. 医院域控制器环境 - 防病毒 Management Console SVR 在医院域控制器域中
   - 通信类型 - 1 < 具有相同子网掩码的相同网络 >

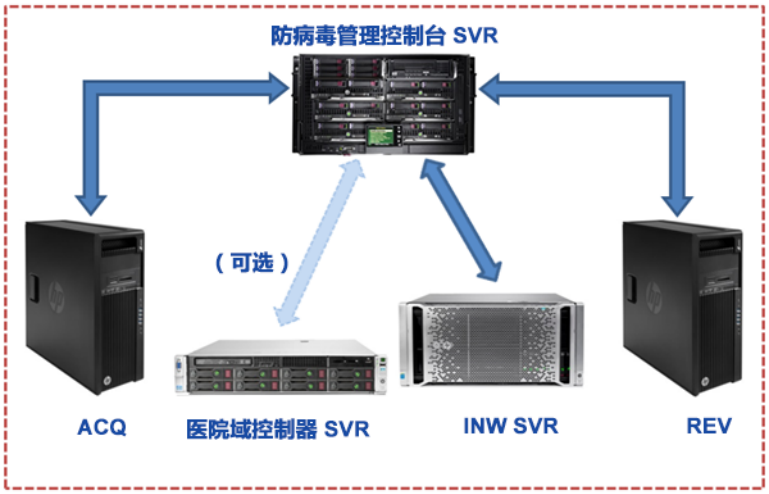
注意： 防病毒 Management Console Server 应该具有两个网络端口。一个网络端口应连接至 Centricity Cardiology INW 网络，另一个应连接至医院网络。

INW 域控制器环境方块图



医院域控制器环境方块图





用户帐户控制

用户帐户控制是一项 Windows 功能，用于防止未经授权更改计算机。在此手册的某些程序中，会显示用户帐户控制消息。

当遵循本手册中的程序操作导致显示此消息时，可以放心地继续。

防病毒软件安装说明

单击您要哪种的防病毒软件：

- Symantec EndPoint Protection（12.1.2、 12.1.6 MP5 或 14.0 MP1）（第 7 页）
- McAfee VirusScan Enterprise（第 15 页）
- McAfee ePolicy Orchestrator（第 19 页）
- Trend Micro OfficeScan Client/Server Edition 10.6 SP2（第 40 页）
- Trend Micro OfficeScan Client/Server Edition 11.0 SP1（第 49 页）
- Trend Micro OfficeScan Client/Server Edition XG 12.0（第 59 页）

防病毒软件通用安装程序

当在防病毒软件安装说明中提到安装程序时，请使用本节中的程序。

禁用环回连接

在连接到 Mac-Lab/CardioLab 环境的采集系统上，禁用环回连接以发现域上具有相同的子网掩码的所有客户端系统。

1. 以**管理员**或管理员组成员的身份登录。
2. 在桌面上右键单击 ***Network***（网络），然后选择 ***Properties***（属性）。
3. 单击***更改适配器设置***。
4. 右键单击 ***Loopback Connection***（环回连接），然后选择 ***Disable***（禁用）。
5. 重新启动采集系统。

注意： 在采集系统上禁用环回连接的目的是发现那些在域中具有相同子网掩码的所有客户端系统。

启用环回连接

在连接到 Mac-Lab/CardioLab 环境的采集系统上，使用下面的步骤启用环回连接。

1. 以**管理员**或管理员组成员的身份登录。
2. 在桌面上右键单击 ***Network***（网络），然后选择 ***Properties***（属性）。
3. 单击***更改适配器设置***。
4. 右键单击 ***Loopback Connection***（环回连接），然后选择 ***Enable***（启用）。
5. 重新启动采集系统。

在安装防病毒软件之前配置 Computer Browser 服务

检查联网的采集和回顾系统上的 Computer Browser 服务设置，确保它已正确配置。

1. 单击 ***Start（开始）> Control Panel （控制面板）> Network and Sharing Center（网络和共享中心）***。

2. 单击 ***Change advanced sharing settings***（更改高级共享设置）。
3. 展开 ***Home or Work***（家庭或工作）。
4. 确保已选中 ***Turn on file and printer sharing***（打开文件和打印机共享）。
5. 单击 ***Save changes***（保存更改）。
6. 单击 ***Start（开始）> Run（运行）***。
7. 输入 **services.msc**，然后按 **Enter** 键。
8. 双击 ***Computer Browser*** 服务。
9. 确保 ***Startup type***（启动类型）设置为 ***Automatic***（自动）。如果此项未设置为 Automatic（自动），请更改，然后单击 ***Start***（启动）。
10. 单击 ***OK***（确定）。
11. 关闭 ***Services***（服务）窗口。

在安装防病毒软件之后配置 Computer Browser 服务

在安装防病毒软件之后，检查联网的采集和回顾系统上的 Computer Browser 服务设置，确保它已正确配置。

1. 单击 ***Start（开始）> Run（运行）***。
2. 输入 **services.msc**，然后按 **Enter** 键。
3. 双击 ***Computer Browser*** 服务。
4. 将 ***Startup type***（启动类型）设置为 ***Manual***（手动）。
5. 单击 ***OK***（确定）。
6. 关闭 ***Services***（服务）窗口。

Symantec EndPoint Protection（12.1.2、 12.1.6 MP5 或 14.0 MP1）

安装概述

仅在联网的 Mac-Lab/CardioLab 环境中安装 Symantec EndPoint Protection。在联网的环境中，一定要先将 Symantec EndPoint Protection 安装在 防病毒 Management Console Server 中，然后再作为客户端部署到 Centricity Cardiology INW Server 和采集 / 回顾工作站。使用下面的说明来安装和配置 ***Symantec EndPoint Protection***。

贵机构有责任升级防病毒软件。定期更新病毒定义，以确保系统上的病毒防护总是处于最新状态。

安装前指南

1. Symantec 防病毒 Management Console 应根据 Symentec 说明安装，并可以正常工作。
2. 在所有客户端系统（采集、回顾和 INW Server）上以**管理员**或管理员组成员的身份登录以安装防病毒软件。

3. 以 ***Run As Administrator***（以管理员身份运行）模式打开命令提示符。
4. 导航到 C:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec。

注意： 要配置 INW Server，请导航到 C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec。

5. 输入 **UpdateRegSymantec.ps1**，然后按 ***Enter*** 键。
6. 确认脚本执行成功。

   如果上述文件夹路径不存在，请针对除 MLCL 6.9.6R1 INW Server 以外的所有 MLCL 系统执行下列步骤（服务器操作系统：Windows Server 2008R2）。

   a. 单击 ***Start***（开始）按钮，然后单击 ***Run***（运行）。
   b. 输入 **Regedit.exe**，然后单击 ***OK***（确定）。
   c. 导航到 ***HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing***。
   d. 找到并双击 ***State*** 注册表项。
   e. 将 ***Base*** 更改为 ***Decimal***。
   f. 将 ***Value data***（值数据）更改为 ***146432***。
   g. 单击 ***OK***（确定）并关闭注册表。
7. 禁用环回连接。有关详细信息，请参阅禁用环回连接（第 6 页）。
8. 配置 Computer Browser 服务。有关详细信息，请参阅在安装防病毒软件之前配置 Computer Browser 服务（第 6 页）。

Symantec EndPoint Protection - 新安装部署步骤（首选推送安装方法）

1. 单击 ***Start（开始）> All Programs（所有程序）> Symantec EndPoint Protection Manager > Symantec Endpoint Protection Manager***。
2. 输入用户名和密码以登录 Symantec Endpoint Protection Manager。（如果出现安全提示，请单击 ***Yes***（是）。）
3. 选中 ***Do not show this Welcome Page again***（不再显示此欢迎页面），然后单击 ***Close***（关闭）以关闭欢迎屏幕。

注意： 对于版本 14.0 MP1, 单击 ***Close***（关闭）以关闭 ***Getting Started on Symantec EndPoint Protection***（Symantec EndPoint Protection 使用入门）屏幕。

4. 在 ***Symantec EndPoint Protection Manager*** 窗口中单击 ***Admin***（管理）。
5. 单击底部窗格中的 ***Install Packages***（安装软件包）。
6. 单击顶部窗格中的 ***Client Install Feature Set***（客户端安装功能集）。
7. 右键单击 ***Client Install Feature Set***（客户端安装功能集）窗口，然后选择 ***Add***（添加）。此时将显示 Add Client Install Feature Set（添加客户端安装功能集）窗口。
8. 输入合适的名称并接下来以备后面需要。

9. 确保 ***Feature set version***（功能集版本）是 ***12.1 RU2 and later***（12.1 RU2 及更高版本）。
10. 只选择下列功能并取消选择其他功能。
    - ***Virus, Spyware, and Basic Download Protection***（病毒、间谍软件和基本下载保护）。
    - ***Advanced Download Protection***（高级下载保护）。
11. 单击消息框中的 ***OK***（确定）。
12. 仅对于版本 12.1.2 和 12.1.6 MP5，单击 ***OK***（确定）以关闭 ***Add Client Install Feature Set***（添加客户端安装功能集）窗口。
13. 在 ***Symantec Endpoint Protection Manager*** 窗口中单击 ***Home***（主页）。
14. 根据软件版本，执行下列其中一项操作：
    - **版本 12.1.2 和 12.1.6 MP5：**从 ***Home***（主页）窗口右上方的 ***Common Tasks***（公共任务）下拉列表中选择 ***Install protection client to computers***（将保护客户端安装到计算机）。此时将显示 Client Deployment Type（客户端部署类型）屏幕。
    - **版本 14.0 MP1：**在 ***Symantec Endpoint Protection Manager*** 窗口中单击 ***Clients***（客户端）。单击 ***Tasks***（任务）下面的 ***Install a client***（安装客户端）。此时将显示 ***Client Deployment wizard***（客户端部署向导）屏幕。
15. 选择 ***New Package Deployment***（新建软件包部署）并单击 ***Next***（下一步）。
16. 选择在步骤 8 中创建的功能集名称。让其他设置保留默认值，然后单击 ***Next***（下一步）。

注意： 对于版本 14.1 Mp1，在 ***Scheduled Scans***（计划扫描）下，取消选中 ***Delay scheduled scans when running on batteries and Allow user-defined scheduled scans to run when scan author is not logged on***（采用电池供电时延迟计划扫描并在扫描作者未登录时允许用户定义的计划扫描运行）。

17. 选择 ***Remote push***（远程推送），然后单击 ***Next***（下一步）。等待 ***Computer selection***（选择计算机）屏幕出现。
18. 展开 ***<Domain>***（示例：INW）。已连接到域的系统会显示在 ***Computer selection***（选择计算机）窗口中。

注意： 如果未能识别所有系统，请单击 ***Search Network***（搜索网络），然后单击 ***Find Computers***（查找计算机）。使用 ***search by IP address***（通过 IP 地址搜索）检测方法来识别客户端（采集、回顾和 INW Server）。

19. 选择已连接到域的所有 Mac-Lab/CardioLab 客户端机器，然后单击 **>>**。此时将显示 ***Login Credentials***（登录凭据）屏幕。
20. 输入用户名、密码和域 / 计算机名称，然后单击 ***OK***（确定）。
21. 确保所有选定的计算机均出现在 ***Install Protection Client***（安装保护客户端）下，然后单击 ***Next***（下一步）。
22. 单击 ***Send***（发送）并等待到 Symantec 防病毒软件在所有客户端系统（采集、回顾和 INW Server）上部署。完成后，将会显示 ***Deployment Summary***（部署摘要）屏幕。
23. 单击 ***Next***（下一步），然后单击 ***Finish***（完成）以完成 Client Deployment Wizard（客户端部署向导）。
24. 等待到 Symantec 图标显示在系统托盘中，然后重新启动所有客户端机器（采集、回顾和 INW Server）。重新启动之后，在所有客户端机器上以管理员或管理员组成员的身份登录。

Symantec EndPoint Protection 服务器控制台的配置

1. 选择 ***Start（开始）> All Programs（所有程序）> Symantec EndPoint Protection Manager > Symantec EndPoint Protection Manager***。此时将打开 Symantec EndPoint Protection Manager 登录窗口。
2. 输入 Symantec Endpoint Protection Manager 控制台密码，然后单击 ***Log On***（登录）。
3. 选择 ***Policies***（策略）选项卡，然后单击 ***Policies***（策略）下面的 ***Virus and Spyware Protection***（病毒和间谍软件保护）。此时将打开 ***Virus and Spyware Protection Policies***（病毒和间谍软件保护策略）窗口。
4. 单击 ***Tasks***（任务）下面的 ***Add a Virus and Spyware Protection***（添加病毒和间谍软件保护）策略。此时将打开 ***Virus and Spyware Protection***（病毒和间谍软件保护）窗口。
5. 在 ***Windows Settings（Windows 设置）> Scheduled Scans（计划扫描）***下，单击 ***Administrator-Defined Scans***（管理员定义的扫描）。
6. 选择 ***Daily Scheduled Scan***（日扫描计划），然后单击 ***Edit***（编辑）。此时将打开 ***Edit Scheduled Scan***（编辑计划扫描）窗口。
7. 将扫描名称和说明分别更改为 ***Weekly Scheduled Scan***（周扫描计划）和 ***Weekly Scan at 00:00***（在 00:00 进行周扫描）。
8. 为 ***Scan type***（扫描类型）选择 ***Full Scan***（完整扫描）。
9. 选择 ***Schedule***（计划）选项卡。
10. 在 ***Scanning Schedule***（扫描计划）下，选择 ***Weekly***（每周）并将时间更改为 ***00:00***。
11. 在 ***Scan Duration***（扫描持续时间）下，取消选中 ***Randomize scan start time within this period (recommended in VMs)***（随机化扫描开始时间在此时间段内（推荐在虚拟机中））并选择 ***Scan until finished (recommended to optimize scan performance)***（扫描直到完成（建议采用以优化性能））。
12. 在 ***Missed scheduled Scans***（错过的计划扫描）下，取消选中 ***Retry scan within***（在以下时间内重试扫描）。
13. 选择 ***Notifications***（通知）选项卡。
14. 取消选中 ***Display a notification message on the infected computer***（在被感染计算机上显示通知消息），然后单击 ***OK***（确定）。
15. 在 ***Administrator-Defined Scans***（管理员定义的扫描）窗口中选择 ***Advanced***（高级）选项卡。
16. 在 ***Scheduled Scans***（计划扫描）下，取消选中 ***Delay scheduled scans when running on batteries***（采用电池供电时延迟计划扫描）、 ***Allow user-defined scheduled scans to run when scan author is not logged on***（在扫描作者未登录时允许用户定义的计划扫描运行）和 ***Display notifications about detections when the user logs on***（在用户登录时显示有关检测项的通知）。

注意： 对于版本 14.0 Mp1，在 ***Scheduled Scans***（计划扫描）下，取消选中 ***Delay scheduled scans when running on batteries and Allow user-defined scheduled scans to run when scan author is not logged on***（采用电池供电时延迟计划扫描并在扫描作者未登录时允许用户定义的计划扫描运行）。

17. 在 ***Startup and Triggered Scans***（启动和触发的扫描）下，取消选中 ***Run an Active Scan when new definitions arrive***（当新定义到达时运行活动的扫描）。

18. 在 ***Windows Settings（Windows 设置）> Protection Technology（保护技术）***下，单击 ***Auto-Protect***（自动保护）。
19. 选择 ***Scan Details***（扫描详细信息）选项卡，然后选择并锁定 ***Enable Auto-Protect***（启用自动保护）。
20. 选择 ***Notifications***（通知）选项卡，然后取消选中并锁定 ***Display a notification message on the infected computer***（在被感染计算机上显示通知消息）和 ***Display the Auto-Protect results dialog on the infected Computer***（在被感染计算机上显示自动保护结果对话框）。
21. 选择 ***Advanced***（高级）选项卡，并在 ***Auto-Protect Reloading and Enablement***（自动保护重新加载和启用）下，锁定 ***When Auto-Protect is disabled， Enable after:***（在禁用自动保护时，经过以下时间后启用：）选项。
22. 在 ***Additional Options***（其他选项）下，单击 ***File Cache***（文件高速缓存）。此时将打开 ***File Cache***（文件高速缓存）窗口。
23. 取消选中 ***Rescan cache when new definitions load***（当加载新定义时重新扫描高速缓存），然后单击 ***OK***（确定）。
24. 在 ***Windows Settings（Windows 设置）> Protection Technology（保护技术）***下，单击 ***Download Protection***（下载保护）。
25. 选择 ***Notifications***（通知）选项卡，然后取消选中并锁定 ***Display a notification message on the infected computer***（在被感染计算机上显示通知消息）。
26. 在 ***Windows Settings（Windows 设置）> Protection Technology（保护技术）***下，单击 ***SONAR***。
27. 选择 ***SONAR Settings***（SONAR 设置）选项卡，然后取消选中并锁定 ***Enable SONAR***（启用 SONAR）。
28. 在 ***Windows Settings（Windows 设置）> Protection Technology（保护技术）***下，单击 ***Early Launch Anti-Malware Driver***（尽早启动防恶意软件驱动程序）。
29. 取消选中并锁定 ***Enable Symantec early lauch anti-malware***（让 Symantec 尽早启动防恶意软件）。
30. 在 ***Windows Settings（Windows 设置）> Email Scans（电子邮件扫描）***下，单击 ***Internet Email Auto-Protect***（Internet 电子邮件自动保护）。
31. 选择 ***Scan Details***（扫描详细信息）选项卡，然后取消选中并锁定 ***Enable Internet Email Auto-Protect***（启用 Internet 电子邮件自动保护）。
32. 选择 ***Notifications***（通知）选项卡，然后取消选中并锁定 ***Display a notification message on the infected computer***（在被感染计算机上显示通知消息）、 ***Display a progress indicator when email is being sent***（当发送电子邮件时显示进度指示器）和 ***Display a notification area icon***（显示通知区域图标）。
33. 在 ***Windows Settings（Windows 设置）> Email Scans（电子邮件扫描）***下，单击 ***Microsoft Outlook Auto-Protect***（Microsoft Outlook 自动保护）。
34. 选择 ***Scan Details***（扫描详细信息）选项卡，然后取消选中并锁定 ***Enable Microsoft Outlook Auto-Protect***（启用 Microsoft Outlook 自动保护）。
35. 选择 ***Notifications***（通知）选项卡，然后取消选中并锁定 ***Display a notification message on the infected computer***（在被感染计算机上显示通知消息）。

36. 在 ***Windows Settings（Windows 设置）> Email Scans（电子邮件扫描）***下，单击 ***Lotus Notes Auto-Protect***（Lotus Notes 自动保护）。

37. 选择 ***Scan Details***（扫描详细信息）选项卡，然后取消选中并锁定 ***Enable Lotus Notes Auto-Protect***（启用 Lotus Notes 自动保护）。

38. 选择 ***Notifications***（通知）选项卡，然后取消选中并锁定 ***Display a notification message on infected computer***（在被感染计算机上显示通知消息）。

39. 在 ***Windows Settings（Windows 设置）> Advanced Options（高级选项）***下，单击 ***Global Scan Options***（全局扫描选项）。

40. 在 ***Bloodhound(™) Detection Settings***（Bloodhound(™) 检测设置）下，取消选中并锁定 ***Enable Bloodhound(™) heuristic virus detection***（启用 Bloodhound(™) 启发式病毒检测）。

41. 在 ***Windows Settings（Windows 设置）> Advanced Options（高级选项）***下，单击 ***Quarantine***（隔离）。

42. 选择 ***General***（常规）选项卡，在 ***When New Virus Definitions Arrive***（当新病毒定义到达时）下，选择 ***Do nothing***（不执行任何操作）。

43. 在 ***Windows Settings（Windows 设置）> Advanced Options（高级选项）***下，单击 ***Miscellaneous***（其他）。

44. 选择 ***Notifications***（通知）选项卡，然后取消选中 ***Display a notification message on the client computer when definitions are outdated***（当定义过时时在客户端计算机上显示通知信息）、 ***Display a notification message on the client computer when Symantec Endpoint Protection is running without virus definitions***（当 Symantec Endpoint Protection 运行时无病毒定义则在客户端计算机上显示通知消息）和 ***Display error messages with a URL to a solution***（显示带解决方案 URL 的错误消息）。

45. 单击 ***OK***（确定）以关闭 ***Virus and Spyware Protection***（病毒和间谍软件保护）策略窗口。

46. 在 ***Assign Policies***（分配策略）消息框中单击 ***Yes***（是）。

47. 选择 ***My Company***（我的公司），然后单击 ***Assign***（分配）。

48. 在消息框中单击 ***Yes***（是）。

49. 在 ***Policies***（策略）下，单击 ***Firewall***（防火墙）。

50. 在 ***Firewall Policies***（防火墙策略）下单击 ***Firewall policy***（防火墙策略），然后在 ***Tasks***（任务）下单击 ***Edit policy***（编辑策略）。

51. 选择 ***Policy Name***（策略名称）选项卡，然后取消选中 ***Enable this policy***（启用此策略）。

52. 单击 ***OK***（确定）。

53. 在 ***Policies***（策略）下，单击 ***Intrusion Prevention***（入侵阻止）。

54. 在 ***Intrusion Prevention Policies***（入侵阻止策略）下单击 ***Intrusion Prevention***（入侵阻止）策略，然后在 ***Tasks***（任务）下单击 ***Edit policy***（编辑策略）。

55. 选择 ***Policy Name***（策略名称）选项卡，然后取消选中 ***Enable this policy***（启用此策略）。

56. 根据软件版本，执行下列其中一项操作：

    - **版本 12.1.2：**从左窗格中单击 ***Settings***（设置）。
    - **版本 12.1.6 MP5 和 14.0 MP1：**从左窗格中单击 ***Intrusion Prevention***（入侵阻止）。

57. 取消选中并锁定 ***Enable Network Intrusion Prevention***（启用网络入侵阻止）和 ***Enable Browser Intrusion Prevention for Windows***（针对 Windows 启用浏览器入侵阻止）。

58. 单击 ***OK***（确定）。

59. 在 ***Policies***（策略）下，单击 ***Application and Device Control***（应用程序和设备控制）。

60. 在 ***Application and Device Control Policies***（应用程序和设备控制策略）下单击 ***Application and Device Control Policy***（应用程序和设备控制策略），然后在 ***Tasks***（任务）下单击 ***Edit policy***（编辑策略）。

61. 选择 ***Policy Name***（策略名称）选项卡，然后取消选中 ***Enable this policy***（启用此策略）。

62. 单击 ***OK***（确定）。

63. 在 ***Policies***（策略）下，单击 ***LiveUpdate***（实时更新）。

64. 选择 ***LiveUpdate Settings policy***（实时更新设置策略），然后在 ***Tasks***（任务）下，单击 ***Edit policy***（编辑策略）。

65. 在 ***Overview（概述）> Windows Settings（Windows 设置）***下，单击 ***Server Settings***（服务器设置）。

66. 在 ***Internal or External LiveUpdate Server***（内部或外部实时更新服务器）下，确保 ***Use default management server***（使用默认管理服务器）处于选中状态，然后取消选中 ***Use a LiveUpdate server***（使用实时更新服务器）。

67. 单击 ***OK***（确定）。

68. 在 ***Policies***（策略）下，单击 ***Exceptions***（例外）。

69. 单击 ***Exceptions policy***（例外策略），然后在 ***Tasks***（任务）下，单击 ***Edit policy***（编辑策略）。

70. 根据软件版本，执行下列其中一项操作：

    - **版本 12.1.2 和 12.1.6 MP5：**单击 ***Exceptions（（例外）> Add（添加）> Windows Exceptions（Windows 例外）> Folder（文件夹）***。
    - **版本 14.0 MP1：**单击 ***Add***（添加）下拉列表并选择 ***Windows Exceptions（Windows 例外）> Folder（文件夹）***。

71. 输入 **C:\Program Files (x86)\GE Healthcare\MLCL**、 **C:\Program Files\GE Healthcare\MLCL**、 **D:\GEData\Studies**、 **E:**、 **G:** 文件路径（一次输入一个）并执行以下操作：

    a. 确保 ***Include subfolders***（包括子文件夹）处于选中状态。

注意： 如果显示 ***Are you sure you want to exclude all subfolders from protection?***（是否确定要排除保护所有子文件夹？）消息框，请单击 ***Yes***（是）。

    b. 从 ***Specify the type of scan that excludes this folder***（指定排除此文件夹的扫描类型）中，选择 ***All***（全部）。

    c. 对于版本 14.0 MP1，单击 ***OK***（确定）以添加例外。

72. 单击 ***OK***（确定）。

73. 在 ***Tasks***（任务）下，单击 ***Assign policy***（分配策略）。

74. 选择 ***My Company***（我的公司），然后单击 ***Assign***（分配）。

75. 单击 ***Yes***（是）。

76. 从左窗格中单击 ***Clients***（客户端），然后选择 ***Policies***（策略）选项卡。

77. 在 ***My Company***（我的公司）下，选择 ***Default Group***（默认组），然后取消选中 ***Inherit policies and settings from parent group "My Company"***（从父组 " 我的公司 " 继承策略和设置），然后在 ***Location-Independent Policies and Settings***（与位置无关的策略和设置）下，单击 ***Communications Settings***（通信设置）。

注意： 如果显示警告消息，请单击 ***OK***（确定），然后再次在 ***Location-Independent Policies and Settings***（与位置无关的策略和设置）下，单击 ***Communications Settings***（通信设置）。

78. 在 ***Download***（下载）下，确保 ***Download policies and content from management server***（从管理服务器下载策略和内容）处于选中状态，然后选中 ***Push mode***（推送模式）。

79. 单击 ***OK***（确定）。

80. 在 ***Location-independent Policies and Settings***（与位置无关的策略和设置）下，单击 ***General Settings***（常规设置）。

81. 选择 ***Tamper Protection***（篡改保护）选项卡，然后取消选中并锁定 ***Protect Symantec security software from being tampered with or shut down***（保护 Symantec 安全软件免被篡改或关闭）。

82. 单击 ***OK***（确定）。

83. 单击 ***Admin***（管理），然后选择 ***Servers***（服务器）。

84. 在 ***Servers***（服务器）下，选择 ***Local Site (My Site)***（本地站点（我的站点））。

85. 在 ***Tasks***（任务）下，选择 ***Edit Site Properties***（编辑站点属性）。此时将打开 ***Site Properties for Locate Site (My Site)***（本地站点（我的站点）的站点属性）窗口。

86. 选择 ***LiveUpdate***（实时更新）选项卡，然后在 ***Download Schedule***（下载计划）下，确保将计划设置为 ***Every 4 hour(s)***（每 4 小时）。

87. 单击 ***OK***（确定）。

88. 单击 ***Log Off***（注销）并关闭 Symantec EndPoint Protection Manager 控制台。确保 Symantec Endpoint Protection Policies（Symantec EndPoint Protection 策略）已在客户端系统中推入。

Symantec EndPoint Protection 安装后指南

1. 启用环回连接。有关详细信息，请参阅启用环回连接（第 6 页）。

2. 配置 Computer Browser 服务。有关详细信息，请参阅在安装防病毒软件之后配置 Computer Browser 服务（第 7 页）。

3. 以 ***Run As Administrator***（以管理员身份运行）模式打开命令提示符。

4. 导航到 C:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec。

注意： 要配置 INW Server，请导航到 C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Symantec。

5. 输入 **RestoreRegSymantec.ps1**，然后按 ***Enter*** 键。

6. 确认脚本执行成功。
   注：您必须先确保 **RestoreRegSymantec.ps1** 脚本已成功执行，然后再继续。

   如果上述文件夹路径不存在，请针对除 MLCL 6.9.6R1 INW Server 以外的所有 MLCL 系统执行下列步骤（服务器操作系统：Windows Server 2008R2）。

   a. 单击 ***Start***（开始）按钮，然后单击 ***Run***（运行）。

   b. 输入 **Regedit.exe**，然后单击 ***OK***（确定）。

   c. 导航到 ***HKEY_USERS\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing***。

   d. 找到并双击 ***State*** 注册表项。

   e. 将 ***Base*** 更改为 ***Decimal***。

   f. 将 ***Value data***（值数据）更改为 ***65536***。

   g. 单击 ***OK***（确定）并关闭注册表。

McAfee VirusScan Enterprise

安装概述

McAfee VirusScan Enterprise 应该安装在独立的 Mac-Lab/CardioLab 系统上，并且它应该单独管理。使用下面的说明来安装和配置 McAfee VirusScan Enterprise。

贵机构有责任升级防病毒软件。定期更新病毒定义，以确保系统上的病毒防护总是处于最新状态。

McAfee VirusScan Enterprise 安装程序

1. 以**管理员**或管理员组成员身份登录。
2. 将 **McAfee VirusScan Enterprise 8.8 Patch 3**、**McAfee VirusScan Enterprise 8.8 Patch 4**、**McAfee VirusScan Enterprise 8.8 Patch 8 CD** 或 **McAfee VirusScan Enterprise 8.8 Patch 9 CD** 放入 CD 驱动器中。
3. 双击 ***SetupVSE.Exe***。此时将显示 Windows Defender 对话框。
4. 单击 ***Yes***（是）。此时将显示 McAfee VirusScan Enterprise Setup（McAfee VirusScan Enterprise 安装）屏幕。
5. 单击 ***Next***（下一步）。此时将显示 McAfee End User License Agreement（McAfee 最终用户许可协议）屏幕。
6. 阅读许可协议并填写任何必填字段，完成后单击 ***OK***（确定）。此时将显示 Select Setup Type（选择安装类型）屏幕。
7. 选择 ***Typical***（典型），然后单击 ***Next***（下一步）。此时将显示 Select Access Protection Level（选择访问保护级别）屏幕。
8. 选择 ***Standard Protection***（标准保护），然后单击 ***Next***（下一步）。此时将显示 Ready to Install（准备安装）屏幕。

9. 单击 ***Install***（安装）并等待安装完成。成功安装 McAfee VirusScan Enterprise 后，将显示 ***McAfee Virus Scan Enterprise Setup has completed successfully***（McAfee Virus Scan Enterprise 安装已成功完成）屏幕。
10. 取消选中 ***Run On-Demand Scan***（运行按需扫描）复选框，然后单击 ***Finish***（完成）。
11. 如果显示 ***Update in Progress***（正在进行更新）窗口，请单击 ***Cancel***（取消）。
12. 如果显示提示重新启动系统的消息框，请单击 ***OK***（确定）。
13. 重新启动系统。
14. 以**管理员**或管理员组成员身份登录。

McAfee VirusScan Enterprise 配置

1. 单击 ***Start（开始）> All Programs（所有程序）> McAfee > VirusScan Console (VirusScan 控制台)***。此时将显示 ***VirusScan Console***（VirusScan 控制台）屏幕。
2. 右键单击 ***Access Protection***（访问保护），然后选择 ***Properties***（属性）。此时将显示 ***Access Protection Properties***（访问保护属性）屏幕。
3. 单击 ***Access Protection***（访问保护）选项卡，然后取消选中 ***Enable access protection***（启用访问保护）和 ***Prevent McAfee services from being stopped***（防止 McAfee 服务停止）。
4. 单击 ***OK***（确定）。
5. 右键单击 ***Buffer Overflow Protection***（缓冲区溢出保护），然后选择 ***Properties***（属性）。此时将显示 ***Buffer Overflow Protection Properties***（缓冲区溢出保护属性）屏幕。
6. 单击 ***Buffer Overflow Protection***（缓冲区溢出保护）选项卡，然后取消选中 ***Show the messages dialog box when a buffer overflow is detected under Buffer overflow settings***（根据缓冲区溢出设置检测到缓冲区溢出时显示消息对话框）。
7. 在 ***Buffer overflow settings***（缓冲区溢出设置）下，取消选中 ***Enable buffer overflow protection***（启用缓冲区溢出保护）。
8. 单击 ***OK***（确定）。
9. 右键单击 ***On-Delivery Email Scanner***（按递送电子邮件扫描程序），然后选择 ***Properties***（属性）。此时将显示 ***On-Delivery Email Scanner Properties***（按递送电子邮件扫描程序属性）屏幕。
10. 单击 ***Scan items***（扫描项目）选项卡，然后在 ***Heuristics***（启发式）下，取消选中以下选项：
    - ***Find unknown program threats and trojans***（查找未知的程序威胁和特洛伊木马病毒）。
    - ***Find unknown macro threats***（查找未知的宏病毒威胁）。
    - ***Find attachments with multiple extensions***（查找含有多个扩展名的附件）。
11. 在 ***Unwanted programs detection***（有害程序检测）下，取消选中 ***Detect unwanted programs***（检测有害程序）。
12. 在 ***Artemis (Heuristic network check for suspicious files)***（Artemis（可疑文件的启发式网络检查））下，为 ***Sensitivity level***（敏感性级别）选择 ***Disabled***（已禁用）。
13. 单击 ***OK***（确定）。

14. 右键单击 ***On-Delivery Email Scanner***（按递送电子邮件扫描程序），然后选择 ***Disable***（禁用）。
15. 右键单击 ***On-Access Scanner***（按访问扫描程序），然后选择 ***Properties***（属性）。此时将显示 ***On-Access Scan Properties***（按访问扫描属性）屏幕。
16. 单击 ***General***（常规）选项卡，然后在 ***Artemis (Heuristic network check for suspicious files)***（Artemis（可疑文件的启发式网络检查））下，为 ***Sensitivity level***（敏感性级别）选择 ***Disabled***（已禁用）。
17. 单击 ***ScriptScan***（脚本扫描）选项，然后取消选中 ***Enable scanning of scripts***（启用脚本扫描）。
18. 单击 ***Blocking***（阻止）选项卡，然后取消选中 ***Block the connection when a threat is detected in a shared folder***（在共享文件夹中检测到威胁时阻止连接）。
19. 单击 ***Messages***（消息）选项卡，然后取消选中 ***Show the messages dialog box when a threat is detected and display the specified text in the message***（检测到威胁时显示消息对话框并在消息中显示规定文本）。
20. 从左侧窗格中单击 ***All Processes***（所有进程）。
21. 单击 ***Scan Items***（扫描项目）选项卡，然后在 Heuristics（启发式）下，取消选中以下选项。
    - ***Find unknown unwanted programs and trojans***（查找未知的有害程序和特洛伊木马病毒）。
    - ***Find unknown macro threats***（查找未知的宏病毒威胁）。
22. 在 ***Unwanted programs detection***（有害程序检测）下，取消选中 ***Detect unwanted programs***（检测有害程序）。
23. 单击 ***Exclusions***（排除项）选项卡，然后单击 ***Exclusions***（排除项）。此时将显示 ***Set Exclusions***（设置排除项）屏幕。
24. 单击 ***Add***（添加）。此时将显示 ***Add Exclusion Item***（添加排除项）屏幕。
25. 选择 ***By name/location***（按名称 / 位置），然后单击 ***Browse***（浏览）。此时将显示 ***Browse for Files or Folders***（浏览选择文件或文件夹）屏幕。
26. 导航到 ***C:\Program Files\GE Healthcare\MLCL***、 ***D:\GEData\Studies***、 ***E:***、 ***G:*** 文件夹（一次一个文件夹），然后选择 ***OK***（确定）。
27. 在 ***Add Exclusion Item***（添加排除项）窗口中选择 ***Also exclude subfolders***（同时排除子文件夹），然后单击 ***OK***（确定）。
28. 确保 C:\Program Files\GE Healthcare\MLCL\、D:\GEData\Studies\、E:\、G:\ 文件夹存在于 Set Exclusions（设置排除项）窗口中。
29. 单击 ***OK***（确定）。
30. 右键单击 ***AutoUpdate***（自动更新），然后选择 ***Properties***（属性）。此时将显示 McAfee AutoUpdate Properties - AutoUpdate（McAfee 自动更新属性 - 自动更新）窗口。
31. 在 ***Update Options***（更新选项）下，取消选中下列选项：
    - ***Get new detection engine and dats if available***（获取新的检测引擎和 DAT（如果可用））。
    - ***Get other available updates (service packs, upgrades, etc.)***（获取其他可用更新（服务包、升级等）。

32. 单击 ***Schedule***（计划）。此时将显示 Schedule Settings（计划设置）屏幕。
33. 在 ***Schedule Settings***（计划设置）下，取消选中 ***Enable (scheduled task runs at specified time)***（启用（在规定时间运行计划任务））。
34. 单击 ***OK***（确定）。
35. 单击 ***OK***（确定）。
36. 右键单击 ***VirusScan Console***（VirusScan 控制台）窗口，然后选择 ***New On-Demand Scan Task***（新建按需扫描任务）。
37. 将新扫描重命名为 ***Weekly Scheduled Scan***（每周计划扫描）。此时将显示 ***On-Demand Scan Properties - Weekly Scheduled Scan***（按需扫面属性 - 每周计划扫描）屏幕。
38. 单击 ***Scan Items***（扫描项目）选项卡，然后在 ***Options***（选项）下，取消选中 ***Detect unwanted programs***（检测有害程序）。
39. 在 ***Heuristics***（启发式）下，取消选中下列选项：
    - ***Find unknown programs threats***（查找未知的程序威胁）。
    - ***Find unknown macro threats***（查找未知的宏病毒威胁）。
40. 单击 ***Exclusions***（排除项）选项卡，然后单击 ***Exclusions***（排除项）。此时将显示 ***Set Exclusions***（设置排除项）屏幕。
41. 单击 ***Add***（添加）。此时将显示 ***Add Exclusion Item***（添加排除项）屏幕。
42. 选择 ***By name/location***（按名称 / 位置），然后单击 ***Browse***（浏览）。此时将显示 ***Browse for Files or Folders***（浏览选择文件或文件夹）屏幕。
43. 导航到 ***C:\Program Files\GE Healthcare\MLCL***、 ***D:\GEData\Studies***、 ***E:***、 ***G:*** 文件夹（一次一个文件夹），然后选择 ***OK***（确定）。
44. 在 ***Add Exclusion Item***（添加排除项）窗口中选择 ***Also exclude subfolders***（同时排除子文件夹），然后单击 ***OK***（确定）。
45. 确保 ***C:\Program Files\GE Healthcare\MLCL***、***D:\GEData\Studies***、***E:***、***G:*** 文件夹存在于 ***Set Exclusions***（设置排除项）窗口中。
46. 单击 ***OK***（确定）。
47. 单击 ***Performance***（性能）选项卡，然后在 ***Artemis (Heuristic network check for suspicious files)***（Artemis（可疑文件的启发式网络检查））下，为 ***Sensitivity level***（敏感性级别）选择 ***Disabled***（已禁用）。
48. 单击 ***Schedule***（计划）。此时将显示 ***Schedule Settings***（计划设置）屏幕。
49. 单击 ***Task***（任务）选项卡，然后在 ***Schedule Settings***（计划设置）下，选择 ***Enable (scheduled task runs at specified time)***（启用（在规定时间运行计划任务））。
50. 单击 ***Schedule***（计划）选项卡，然后选择下列各项：
    a. Run task（运行任务）：Weekly（每周）。
    b. Start Time（开始时间）：12:00 AM
    c. 间隔：1 Weeks, Sunday（1 周，星期天）。
51. 单击 ***OK***（确定）。
52. 单击 ***OK***（确定）。

53. 在 ***VirusScan Console***（VirusScan 控制台）窗口中，单击 ***Tools（工具）> Alerts（警报）***。此时将显示 Alert Properties（警报属性）屏幕。
54. 取消选中 ***On-Access Scan***（按访问扫描）、 ***On-Demand Scan and scheduled scans***（按需扫描和计划扫描）、 ***Email Scan***（电子邮件扫描）和 ***AutoUpdate***（自动更新）复选框。
55. 单击 ***Destination***（目标位置）。此时将显示 ***Alert Manager Client Configuration***（警报管理器客户端配置）屏幕。
56. 选中 ***Disable alerting***（禁用警报）复选框。
57. 单击 ***OK***（确定）。此时将显示 ***Alert Properties***（警报属性）屏幕。
58. 选中 ***Additional Alerting Options***（更多警报选项）选项卡。
59. 从 ***Severity Filter***（严重程度过滤器）下拉列表中，选择 ***Suppress all alerts (severities 0 to 4)***（取消所有警报（严重等级 0-4））选项。
60. 选择 ***Alert Manager Alerts***（警报管理器警报）选项卡。
61. 取消选中 ***Access Protection***（访问保护）复选框。
62. 单击 ***OK***（确定）以关闭 ***Alert Properties***（警报属性）窗口。
63. 关闭 ***VirusScan Console***（VirusScan 控制台）窗口。

McAfee ePolicy Orchestrator

安装概述

仅在联网的 Mac-Lab/CardioLab 环境中安装 McAfee ePolicy Orchestrator。 McAfee ePolicy Orchestrator 必须安装在 防病毒 Management Console Server 上，并且 McAfee VirusScan Enterprise 应该作为客户端部署到 Centricity Cardiology INW Server 和采集 / 回顾工作站中。使用下面的说明来安装和配置 McAfee ePolicy Orchestrator。

下面有关推送和配置 McAfee VirusScan Enterprise 的说明支持 Patch 3、 Patch 4、 Patch 8 和 Patch 9。

贵机构有责任升级防病毒软件。定期更新病毒定义，以确保系统上的病毒防护总是处于最新状态。

安装前指南

1. McAfee 防病毒 Management Console 应根据 McAfee 说明安装，并可以正常工作。
2. 在所有客户端系统（采集、回顾和 INW Server）上以**管理员**或管理员组成员的身份登录以安装防病毒软件。
3. 禁用环回连接。有关详细信息，请参阅禁用环回连接（第 6 页）。
4. 对于部署 McAfee VirusScan Enterprise 8.8 Patch 9，请联系 McAfee 以仅在 INW Server 上安装 UTN-USERFirst-Object 和 VeriSign 通用根证书。在安装证书之后，重新启动系统。

注意： 如果未在 INW Server 上安装 UTN-USERFirst-Object 和 VeriSign 通用根证书，则 McAfee VirusScan Enterprise 8.8 Patch 9 安装将会失败。

5. 对于新安装，将下列代理程序版本添加至 McAfee ePolicy Orchestrator Console 中的 McAfee ePolicy Orchestrator 主存储库：***- McAfee Agent v5.0.5.658***

6. 对于新安装，将下列软件包添加至 McAfee ePolicy Orchestrator Console 中的 McAfee ePolicy Orchestrator 主存储库：

   - McAfee VirusScan Enterprise 8.8 Patch 3：VSE880LMLRP3.ZIP (v8.8.0.1128)。
   - McAfee VirusScan Enterprise 8.8 Patch 4：VSE880LMLRP4.ZIP (v8.8.0.1247)。
   - McAfee VirusScan Enterprise 8.8 Patch 8：VSE880LMLRP8.ZIP (v8.8.0.1599)。
   - McAfee VirusScan Enterprise 8.8 Patch 9：VSE880MLRP9.ZIP (v8.8.0.1804)。

注意： VSE880LMLRP3.zip 包含 Patch 2 和 Patch 3 安装软件包。 Patch 2 适用于 Windows 7 和 Windows Server 2008 操作系统平台，而 Patch 3 适用于 Windows 8 和 Windows Server 2012 操作系统平台。 McAfee 安装程序可通过识别 Windows 操作系统版本安装正确的补丁。

7. 对于新安装，将下列扩展添加至 McAfee ePolicy Orchestrator Console 中的 McAfee ePolicy Orchestrator 扩展表：

   - McAfee VirusScan Enterprise 8.8 Patch 3：VIRUSSCAN8800 v8.8.0.348 和 VIRUSSCANREPORTS v1.2.0.228
   - McAfee VirusScan Enterprise 8.8 Patch 4：VIRUSSCAN8800 v8.8.0.368 和 VIRUSSCANREPORTS v1.2.0.236
   - McAfee VirusScan Enterprise 8.8 Patch 8：VIRUSSCAN8800 v8.8.0.511 和 VIRUSSCANREPORTS v1.2.0.311
   - McAfee VirusScan Enterprise 8.8 Patch 9：VIRUSSCAN8800 v8.8.0.548 和 VIRUSSCANREPORTS v1.2.0.346

注意： VIRUSSCAN8800(348).zip 和 VIRUSSCANREPORTS120(228).zip 可在 McAfee VirusScan Enterprise 8.8 Patch 3 软件包中找到。

VIRUSSCAN8800(368).zip 和 VIRUSSCANREPORTS120(236).zip 可在 McAfee VirusScan Enterprise 8.8 Patch 4 软件包中找到。

VIRUSSCAN8800(511).zip 和 VIRUSSCANREPORTS120(311).zip 可在 McAfee VirusScan Enterprise 8.8 Patch 8 软件包中找到。

VIRUSSCAN8800(548).zip 和 VIRUSSCANREPORTS120(346).zip 可在 McAfee VirusScan Enterprise 8.8 Patch 9 软件包中找到。

McAfee ePolicy Orchestrator 5.0 或 5.3.2 - 新安装部署步骤（首选推送安装方法）

1. 根据软件版本，选择 ***Start（开始）> All Programs（所有程序）> McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.0.0 Console（启动 McAfee ePolicy Orchestrator 5.0.0 控制台）***或 ***Start（开始）> All Programs（所有程序）> McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.3.2 Console（启动 McAfee ePolicy Orchestrator 5.3.2 控制台）***以登录到 ePolicy Orchestrator 控制台。

注意： 如果显示 ***Security Alert***（安全警报）消息框，请单击 ***Continue with this website***（继续此网站）。

2. 输入用户名和密码，然后单击 ***Log On***（登录）。

3. 选择 ***Menu（菜单）> System（系统）> System Tree（系统树）***。此时将打开 System Tree（系统树）窗口。

4. 单击 ***My Organization***（我的组织），然后在焦点在 ***My Organization***（我的组织）上的情况下，从屏幕左下角中单击 ***System Tree Actions（系统树操作）> New Systems（新系统）***。

5. 选择 ***Push agents and add systems to the current group (My Organization)***（推送代理程序并将系统添加至当前组（我的组织）），然后在 Target systems（目标系统）上单击 ***Browse***（浏览）。

6. 输入 **domain/local administrator**（域 / 本地管理员）用户名和密码，然后单击 ***OK***（确定）。

7. 从 ***Domain***（域）下拉列表中选择 ***INW*** 域。

8. 选择已连接到域的客户端机器（采集、回顾和 INW Server），然后单击 ***OK***（确定）。

注意： 如果域名未列出在 ***Domain***（域）下拉列表中，请执行以下操作：

   - 在 ***Browse for Systems***（浏览选择系统）窗口中，单击 ***Cancel***（取消）。
   - 在 ***New Systems***（新系统）窗口中，在 ***Target systems***（目标系统）字段中手动输入客户端机器（采集、回顾和 INW Server）系统名称，然后继续执行以下步骤。

9. 为 ***Agent Version***（代理程序版本）选择 ***McAfee Agent for Windows 4.8.0 (Current)***（McAfee Agent for Windows 4.8.0（当前））或 ***McAfee Agent for Windows 5.0.4 (Current)***（McAfee Agent for Windows 5.0.4（当前））。输入 **domain administrator**（域管理员）用户名和密码，然后单击 ***OK***（确定）。

10. 在客户端机器（采集、回顾和 INW Server）中，确认已正确创建目录，根据补丁版本：

    - 对于 Patch 3 和 Patch 4，验证 ***C:\Program Files\McAfee\Common Framework*** 目录是否存在，并且 McAfee Agent 安装在这个目录中。

注意： 对于 INW Server，确保 ***C:\Program Files (x86)\McAfee\Common Framework*** 目录存在，并且 McAfee Agent 安装在这个目录中。

    - 对于 Patch 8，验证 ***C:\Program Files\McAfee\Agent*** 目录是否存在，并且 McAfee Agent 安装在这个目录中。

注意： 对于 INW Server，确保 ***C:\Program Files (x86)\McAfee\Common Framework*** 目录存在。

11. 重新启动客户端机器（采集、回顾和 INW Server）并以**域管理员**或域管理员成员的身份登录。

12. 根据软件版本，单击 ***Start（开始）> All Programs（所有程序）> McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.0.0 Console（启动 McAfee ePolicy Orchestrator 5.0.0 控制台）***或 ***Start（开始）> All Programs（所有程序）> McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.3.2 Console（启动 McAfee ePolicy Orchestrator 5.3.2 控制台）***。

13. 输入用户名和密码，然后单击 ***Log On***（登录）。

14. 单击 ***Menu（菜单）> Systems（系统）> System Tree（系统树）***。

15. 单击 ***My Organization***（我的组织），然后在焦点在 ***My Organization***（我的组织）上的情况下，单击 ***Assigned Client Tasks***（已分配的客户端任务）选项卡。

16. 单击屏幕底部的 ***Actions（操作）> New Client Task Assignment（新客户端任务分配）***按钮。此时将显示 Client Task Assignment Builder（客户端任务分配构建器）屏幕。

17. 选择以下项目：
    a. **Product（产品）：**McAfee Agent
    b. **Task Type（任务类型）：**Product Deployment（产品部署）
    c. **Task name（任务名称）：**Create New Task（创建新任务）
18. 在 ***Client Task Catalog: New Task- McAfee Agent: Product Deployment***（客户端任务类别：新任务 - McAfee Agent：产品部署）屏幕，按如下所示填写各字段：
    a. **Task Name（任务名称）：**输入合适的任务名称
    b. **Target platforms（目标平台）：**Windows
    c. **Products and components（产品和组件）：**适合 v6.9.6 的 VirusScan Enterprise 版本
    d. **Options（选项）：**如果 ***Options***（选项）可用，则在每次策略强制实施时运行（仅限 Windows）
19. 单击 ***Save***（保存）。
20. 在 ***1 Select Task***（1 选择任务）屏幕上，选择以下项目：
    a. **Product（产品）：**McAfee Agent
    b. **Task Type（任务类型）：**Product Deployment（产品部署）
    c. **Task Name（任务名称）：**新创建的任务名称
21. 单击 ***Next***（下一步）。此时将显示 2 Schedule（2 计划）屏幕。
22. 从 ***Schedule type***（计划类型）下拉列表中选择 ***Run immediately***（立即运行）。
23. 单击 ***Next***（下一步）。此时将显示 3 Summary（3 摘要）屏幕。
24. 单击 ***Save***（保存）。此时将显示 ***System Tree***（系统树）屏幕。
25. 选择 ***Systems***（系统）选项卡，然后选择已连接到域的所有客户端机器（采集、回顾和 INW Server）。
26. 单击窗口底部的 ***Wake up Agents***（唤醒代理程序）。
27. 保留默认设置，然后单击 ***OK***（确定）。
28. 等待到 McAfee 图标显示在系统托盘中，重新启动所有客户端机器（采集、回顾和 INW Server），然后在所有客户端机器上以**管理员**或管理员组成员的身份登录。
29. 单击 ***Log Off***（注销）链接以关闭 McAfee ePolicy Orchestrator Console（McAfee ePolicy Orchestrator 控制台）。

McAfee ePolicy Orchestrator 5.9.0 - 新安装部署步骤（首选推送安装方法）

1. 单击 ***Start（开始）> All Programs（所有程序）> McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.9.0 Console（启动 McAfee ePolicy Orchestrator 5.9.0 控制台）***以登录 ePolicy Orchestrator 控制台。

注意： 如果显示 ***Security Alert***（安全警报）消息框，请单击 ***Continue with this website***（继续此网站）。

2. 输入用户名和密码，然后单击 ***Log On***（登录）。
3. 选择 ***Menu（菜单）> System（系统）> System Tree（系统树）***。此时将打开 ***System Tree***（系统树）窗口。
4. 单击 ***My Organization***（我的组织），然后在焦点在 ***My Organization***（我的组织）上的情况下，从屏幕顶部单击 ***New Systems***（新系统）。
5. 选择 ***Push agents and add systems to the current group (My Organization)***（推送代理程序并将系统添加至当前组（我的组织）），然后在 Target systems（目标系统）上单击 ***Browse***（浏览）。
6. 输入 **domain/local administrator**（域 / 本地管理员）用户名和密码，然后单击 ***OK***（确定）。
7. 从 ***Domain***（域）下拉列表中选择 ***INW*** 域。
8. 选择已连接到域的客户端机器（采集、回顾和 INW Server），然后单击 ***OK***（确定）。

注意： 如果域名未列出在 ***Domain***（域）下拉列表中，请执行以下操作：

- 在 ***Browse for Systems***（浏览选择系统）窗口中，单击 ***Cancel***（取消）。
- 在 ***New Systems***（新系统）窗口中，在 ***Target systems***（目标系统）字段中手动输入客户端机器（采集、回顾和 INW Server）系统名称（以逗号分隔），然后继续执行以下步骤。

9. 为 ***Agent Version***（代理版本）选择 ***McAfee Agent for Windows 5.0.5（当前）***。输入 **domain administrator**（域管理员）用户名和密码，然后单击 ***OK***（确定）。
10. 在客户端机器（采集、回顾和 INW Server）中，确认已正确创建 ***C:\Program Files\McAfee\Agent*** 目录。
11. 重新启动客户端机器（采集、回顾和 INW Server）并以**域管理员**或域管理员成员的身份登录。
12. 单击 ***Start（开始）> All Programs（所有程序）> McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.9.0 Console（启动 McAfee ePolicy Orchestrator 5.9.0 控制台）***以登录 ePolicy Orchestrator 控制台。
13. 输入用户名和密码，然后单击 ***Log On***（登录）。
14. 单击 ***Menu（菜单）> Systems（系统）> System Tree（系统树）***。
15. 单击 ***My Organization***（我的组织），然后在焦点在 ***My Organization***（我的组织）上的情况下，单击 ***Assigned Client Tasks***（已分配的客户端任务）选项卡。
16. 单击屏幕底部的 ***Actions（操作）> New Client Task Assignment（新客户端任务分配）***按钮。此时将显示 ***Client Task Assignment Builder***（客户端任务分配构建器）屏幕。
17. 选择以下项目：
    a. **Product（产品）：**McAfee Agent
    b. **Task Type（任务类型）：**Product Deployment（产品部署）
18. 单击 ***Task Actions（任务操作）> Create New Task（创建新任务）***。此时将显示 ***Create New Task***（创建新任务）屏幕。
19. 在 ***Create New Task***（创建新任务）屏幕上，按如下所示完成各字段：
    a. **Task Name（任务名称）：**输入合适的任务名称

b. **Target platforms（目标平台）：**Windows（取消选中所有其他选项）

c. **Products and components（产品和组件）：**VirusScan Enterprise 8.8.0.1804

20. 单击 ***Save***（保存）。此时将显示 ***Client Task Assignment Builder***（客户端任务分配构建器）屏幕。
21. 在 ***Client Task Assignment Builder***（客户端任务分配构建器）屏幕中，选择以下各项：

    a. **Product（产品）：**McAfee Agent

    b. **Task Type（任务类型）：**Product Deployment（产品部署）

    c. **Task Name（任务名称）：**新创建的任务名称

    d. **Schedule Type（计划类型）：**Run immediately（立即运行）

22. 单击 ***Save***（保存）。此时将显示 ***Assigned Client Tasks***（已分配的客户端任务）屏幕。
23. 选择 ***Systems***（系统）选项卡，然后选择已连接到域的所有客户端机器（采集、回顾和 INW Server）。
24. 单击窗口底部的 ***Wake up Agents***（唤醒代理程序）。
25. 保留默认设置，然后单击 ***OK***（确定）。
26. 等待到 McAfee 图标显示在系统托盘中，重新启动所有客户端机器（采集、回顾和 INW Server），然后在所有客户端机器上以**管理员**或管理员组成员的身份登录。
27. 单击 ***Log Off***（注销）链接以关闭 McAfee ePolicy Orchestrator Console（McAfee ePolicy Orchestrator 控制台）。

McAfee ePolicy Orchestrator 5.0 和 5.3.2 服务器控制台配置

1. 根据软件版本，单击 ***Start（开始）> All Programs（所有程序）> McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.0.0 Console（启动 McAfee ePolicy Orchestrator 5.0.0 控制台）***或 ***Start（开始）> All Programs（所有程序）> McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.3.2 Console（启动 McAfee ePolicy Orchestrator 5.3.2 控制台）***。
2. 输入用户名和密码，然后单击 ***Log On***（登录）。
3. 单击 ***Menu（菜单）> Systems（系统）> System Tree（系统树）***。
4. 单击 ***My Organization***（我的组织），然后在焦点在 My Organization（我的组织）上的情况下，单击 ***Assigned Client Tasks***（已分配的客户端任务）选项卡。
5. 单击屏幕底部的 ***Actions（操作）> New Client Task Assignment（新客户端任务分配）***按钮。此时将显示 ***Client Task Assignment Builder***（客户端任务分配构建器）屏幕。
6. 选择以下项目：

    a. ***Product（产品）：***VirusScan Enterprise 8.8.0

    b. ***Task Type（任务类型）：***按需扫描

    c. ***Task name（任务名称）：***Create New Task（创建新任务）

7. 在 ***Client Task Catalog: New Task - VirusScan Enterprise 8.8.0: On Demand Scan***（客户端任务类别：新任务 - VirusScan Enterprise 8.8.0：按需扫描）屏幕，按如下所示填写各字段：

   a. ***Task Name（任务名称）：*** Weekly Scheduled Scan（每周计划扫描）

   b. ***Description（说明）：*** Weekly Scheduled Scan（每周计划扫描）

8. 单击 ***Scan Items***（扫描项目）选项卡。此时将显示 ***Scan Items***（扫描项目）屏幕。

9. 在 ***Options***（选项）下，取消选中 ***Detect unwanted programs***（检测有害程序）。

10. 在 Heuristics（启发式）下，取消选中下列选项：

    - ***Find unknown program threats（查找未知的程序威胁）。***
    - ***Find unknown macro threats（查找未知的宏病毒威胁）。***

11. 单击 ***Exclusions***（排除项）选项卡。此时将显示 ***Exclusions***（排除项）屏幕。

12. 单击 ***Add***（添加）。此时将显示 ***Add/Edit Exclusion Item***（添加 / 编辑排除项）屏幕。

13. 选择 ***By pattern***（按模式），然后输入 **C:\Program Files\GE Healthcare\MLCL**、**C:\Program Files (x86)\GE Healthcare\MLCL**、 **D:\GEData\Studies**、 **E:**、 **G:** 文件夹（一次输入一个），再选中 Also exclude subfolders（同时排除子文件夹）。单击 ***OK***（确定）。

14. 单击 ***Performance***（性能）选项卡。此时将显示 ***Performance***（性能）屏幕。

15. 从 ***Artemis (Heuristic network check for suspicious files)（Artemis（可疑文件的启发式网络检查））*** 下，选择 ***Disabled***（已禁用）。

16. 单击 ***Save***（保存）。

17. 在 ***1 Select Task***（1 选择任务）屏幕上，选择以下项目：

    - ***Product（产品）：*** VirusScan Enterprise 8.8.0
    - ***Task Type（任务类型）：*** 按需扫描
    - ***Task Name（任务名称）：*** Weekly Scheduled Scan（每周计划扫描）

18. 单击 ***Next***（下一步）。此时将显示 ***2 Schedule***（2 计划）屏幕。

19. 从 ***Scheduled type***（计划类型）下拉列表中选择 ***Weekly***（每周），然后选择 ***Sunday***（星期天）。

20. 将 ***Start time***（开始时间）设置为 ***12:00 AM***，然后选择 ***Run Once at that time***（在该时间运行一次）。

21. 单击 ***Next***（下一步）。此时将显示 ***3 Summary***（3 摘要）屏幕。

22. 单击 ***Save***（保存）。此时将显示 ***System Tree***（系统树）屏幕。

23. 选择 ***Assigned Policies***（已分配策略）选项卡。此时将显示 ***Assigned Policies***（已分配策略）屏幕。

24. 从 ***Product***（产品）下拉列表中，选择 ***VirusScan Enterprise 8.8.0***。

25. 为 ***On-Access General Policies***（按访问常规策略）选择 ***My Default***（我的默认设置）。此时将显示 ***VirusScan Enterprise 8.8.0 > On-Access General Policies（按访问常规策略）> My Default（我的默认设置）*** 屏幕。

26. 从 ***Settings for***（设置对象）下拉列表中选择 ***Workstation***（工作站），然后选择 ***General***（常规）选项卡。此时将显示 ***General***（常规）屏幕。
27. 从 ***Artemis (Heuristic network check for suspicious files)（Artemis（可疑文件的启发式网络检查））***下，选择 ***Disabled***（已禁用）。
28. 单击 ***ScriptScan***（脚本扫描）选项卡。此时将显示 ***Script Scan***（脚本扫描）屏幕。
29. 取消选中 ***Enable scanning of scripts***（启用脚本扫描）。
30. 单击 ***Blocking***（阻止）选项卡。此时将显示 ***Blocking***（阻止）屏幕。
31. 取消选中 ***Block the connection when a threatened file is detected in a shared folder***（在共享文件夹中检测到威胁时阻止连接）。
32. 单击 ***Messages***（消息）选项卡。此时将显示 ***Messages***（消息）屏幕。
33. 取消选中 ***Show the messages dialog box when a threat is detected and display the specified text in the message***（检测到威胁时显示消息对话框并在消息中显示规定文本）。
34. 从 ***Settings for***（设置对象）下拉列表中选择 ***Server***（服务器），然后单击 ***General***（常规）选项卡。此时将显示 ***General***（常规）屏幕。
35. 从 ***Artemis (Heuristic network check for suspicious files)（Artemis（可疑文件的启发式网络检查））***下，选择 ***Disabled***（已禁用）。
36. 单击 ***ScriptScan***（脚本扫描）选项卡。此时将显示 ***Script Scan***（脚本扫描）屏幕。
37. 确保 ***Enable scanning of scripts***（启用脚本扫描）处于取消选中状态。
38. 单击 ***Blocking***（阻止）选项卡。此时将显示 ***Blocking***（阻止）屏幕。
39. 取消选中 ***Block the connection when a threatened file is detected in a shared folder***（在共享文件夹中检测到威胁时阻止连接）。
40. 单击 ***Messages***（消息）选项卡。此时将显示 ***Messages***（消息）屏幕。
41. 取消选中 ***Show the messages dialog box when a threat is detected and display the specified text in the message***（检测到威胁时显示消息对话框并在消息中显示规定文本）。
42. 单击 ***Save***（保存）。
43. 为 ***On-Access Default Processes Policies***（按访问默认进程策略）选择 ***My Default***（我的默认设置）。此时将显示 ***VirusScan Enterprise 8.8.0 > On-Access Default Processes Policies（按访问默认进程策略）> My Default（我的默认设置）***屏幕。
44. 从 ***Settings for***（设置对象）下拉列表中选择 ***Workstation***（工作站）。
45. 单击 ***Scan Items***（扫描项目）选项卡。此时将显示 ***Scan Items***（扫描项目）屏幕。
46. 在 ***Heuristics***（启发式）下，取消选中下列选项：
    - ***Find unknown unwanted programs and trojans（查找未知的有害程序和特洛伊木马病毒）。***
    - ***Find unknown macro threats（查找未知的宏病毒威胁）。***
47. 在 ***Unwanted programs detection***（有害程序检测）下，取消选中 ***Detect unwanted programs***（检测有害程序）。
48. 单击 ***Exclusions***（排除项）选项卡。此时将显示 ***Exclusions***（排除项）屏幕。
49. 单击 ***Add***（添加）。此时将显示 ***Add/Edit Exclusion Item***（添加 / 编辑排除项）屏幕。

50. 选择 ***By pattern***（按模式），然后输入 **C:\Program Files\GE Healthcare\MLCL**、**D:\GEData\Studies**、**E:**、**G:** 文件夹（一次输入一个），再选中 ***Also exclude subfolders***（同时排除子文件夹）。单击 ***OK***（确定）。

51. 从 ***Settings for***（设置对象）下拉列表中选择 ***Server***（服务器），然后单击 ***Scan Items***（扫描项目）选项卡。此时将显示 ***Scan Items***（扫描项目）屏幕。

52. 在 ***Heuristics***（启发式）下，取消选中下列选项：

    - ***Find unknown unwanted programs and trojans（查找未知的有害程序和特洛伊木马病毒）。***
    - ***Find unknown macro threats（查找未知的宏病毒威胁）。***

53. 在 ***Unwanted programs detection***（有害程序检测）下，取消选中 ***Detect unwanted programs***（检测有害程序）。

54. 单击 ***Exclusions***（排除项）选项卡。此时将显示 ***Exclusions***（排除项）屏幕。

55. 单击 ***Add***（添加）。此时将显示 ***Add/Edit Exclusion Item***（添加 / 编辑排除项）屏幕。

56. 选择 ***By pattern***（按模式），然后输入 **C:\Program Files (x86)\GE Healthcare\MLCL**、**D:\GEData\Studies** 文件夹（一次输入一个），再选中 ***Also exclude subfolders***（同时排除子文件夹）。单击 ***OK***（确定）。

57. 单击 ***Save***（保存）。

58. 为 ***On-Access Low-Risk Processes Policies***（按访问低风险进程策略）选择 ***My Default***（我的默认设置）。此时将显示 ***VirusScan Enterprise 8.8.0 > On-Access Low-Risk Processes Policies（按访问低风险进程策略）> My Default（我的默认设置）***屏幕。

59. 从 ***Settings for***（设置对象）下拉列表中选择 ***Workstation***（工作站）。

60. 单击 ***Scan Items***（扫描项目）选项卡。此时将显示 ***Scan Items***（扫描项目）屏幕。

61. 在 ***Heuristics***（启发式）下，取消选中下列选项：

    - ***Find unknown unwanted programs and trojans（查找未知的有害程序和特洛伊木马病毒）。***
    - ***Find unknown macro threats（查找未知的宏病毒威胁）。***

62. 在 ***Unwanted programs detection***（有害程序检测）下，取消选中 ***Detect unwanted programs***（检测有害程序）。

63. 单击 ***Exclusions***（排除项）选项卡。此时将显示 ***Exclusions***（排除项）屏幕。

64. 单击 ***Add***（添加）。此时将显示 ***Add/Edit Exclusion Item***（添加 / 编辑排除项）屏幕。

65. 选择 ***By pattern***（按模式），然后输入 **C:\Program Files\GE Healthcare\MLCL**、**D:\GEData\Studies**、**E:**、**G:** 文件夹（一次输入一个），再选中 ***Also exclude subfolders***（同时排除子文件夹）。单击 ***OK***（确定）。

66. 从 ***Settings for***（设置对象）下拉列表中选择 ***Server***（服务器），然后单击 ***Scan Items***（扫描项目）选项卡。此时将显示 ***Scan Items***（扫描项目）屏幕。

67. 在 ***Heuristics***（启发式）下，取消选中下列选项：

    - ***Find unknown unwanted programs and trojans（查找未知的有害程序和特洛伊木马病毒）。***
    - ***Find unknown macro threats（查找未知的宏病毒威胁）。***

68. 在 ***Unwanted programs detection***（有害程序检测）下，取消选中 ***Detect unwanted programs***（检测有害程序）。

69. 单击 ***Exclusions***（排除项）选项卡。此时将显示 ***Exclusions***（排除项）屏幕。

70. 单击 ***Add***（添加）。此时将显示 ***Add/Edit Exclusion Item***（添加 / 编辑排除项）屏幕。

71. 选择 ***By pattern***（按模式），然后输入 **C:\Program Files (x86)\GE Healthcare\MLCL**、**D:\GEData\Studies** 文件夹（一次输入一个），再选中 ***Also exclude subfolders***（同时排除子文件夹）。单击 ***OK***（确定）。

72. 单击 ***Save***（保存）。

73. 为 ***On-Access High-Risk Processes Policies***（按访问高风险进程策略）选择 ***My Default***（我的默认设置）。此时将显示 ***VirusScan Enterprise 8.8.0 > On-Access High-Risk Processes Policies（按访问高风险进程策略）> My Default 我的默认设置）***屏幕。

74. 从 ***Settings for***（设置对象）下拉列表中选择 ***Workstation***（工作站）。

75. 单击 ***Scan Items***（扫描项目）选项卡。此时将显示 ***Scan Items***（扫描项目）屏幕。

76. 在 ***Heuristics***（启发式）下，取消选中下列选项：

    - ***Find unknown unwanted programs and trojans（查找未知的有害程序和特洛伊木马病毒）。***
    - ***Find unknown macro threats（查找未知的宏病毒威胁）。***

77. 在 ***Unwanted programs detection***（有害程序检测）下，取消选中 ***Detect unwanted programs***（检测有害程序）。

78. 单击 ***Exclusions***（排除项）选项卡。此时将显示 ***Exclusions***（排除项）屏幕。

79. 单击 ***Add***（添加）。此时将显示 ***Add/Edit Exclusion Item***（添加 / 编辑排除项）屏幕。

80. 选择 ***By pattern***（按模式），然后输入 **C:\Program Files\GE Healthcare\MLCL**、**D:\GEData\Studies**、**E:**、**G:** 文件夹（一次输入一个），再选中 ***Also exclude subfolders***（同时排除子文件夹）。单击 ***OK***（确定）。

81. 从 ***Settings for***（设置对象）下拉列表中选择 ***Server***（服务器），然后单击 ***Scan Items***（扫描项目）选项卡。此时将显示 ***Scan Items***（扫描项目）屏幕。

82. 在 ***Heuristics***（启发式）下，取消选中下列选项：

    - ***Find unknown unwanted programs and trojans（查找未知的有害程序和特洛伊木马病毒）。***
    - ***Find unknown macro threats（查找未知的宏病毒威胁）。***

83. 在 ***Unwanted programs detection***（有害程序检测）下，取消选中 ***Detect unwanted programs***（检测有害程序）。

84. 单击 ***Exclusions***（排除项）选项卡。此时将显示 ***Exclusions***（排除项）屏幕。

85. 单击 ***Add***（添加）。此时将显示 ***Add/Edit Exclusion Item***（添加 / 编辑排除项）屏幕。

86. 选择 By pattern（按模式），然后输入 **C:\Program Files (x86)\GE Healthcare\MLCL**、**D:\GEData\Studies** 文件夹（一次输入一个），再选中 ***Also exclude subfolders***（同时排除子文件夹）。单击 ***OK***（确定）。

87. 单击 ***Save***（保存）。

88. 为 ***On Delivery Email Scan Policies***（按递送电子邮件扫描策略）单击 ***My Default***（我的默认设置）。此时将显示 ***VirusScan Enterprise 8.8.0 > On Delivery Email Scan Policies（按递送电子邮件扫描策略）> My Default（我的默认设置）***屏幕。

89. 从 ***Settings for***（设置对象）下拉列表中选择 ***Workstation***（工作站）。

90. 单击 ***Scan Items***（扫描项目）选项卡。此时将显示 ***Scan Items***（扫描项目）屏幕。

91. 在 ***Heuristics***（启发式）下，取消选中下列选项。

    - ***Find unknown program threats and trojans（查找未知的程序威胁和特洛伊木马病毒）。***
    - ***Find unknown macro threats（查找未知的宏病毒威胁）。***
    - ***Find attachments with multiple extensions（查找含有多个扩展名的附件）。***

92. 在 ***Unwanted programs detection***（有害程序检测）下，取消选中 ***Detect unwanted programs***（检测有害程序）。

93. 从 ***Artemis (Heuristic network check for suspicious files)（Artemis（可疑文件的启发式网络检查））***下，选择 ***Disabled***（已禁用）。

94. 在 ***Scanning of email***（扫描电子邮件）下，取消选中 ***Enable on-delivery email scanning***（启用按递送电子邮件扫描）。

95. 从 ***Settings for***（设置对象）下拉列表中选择 ***Server***（服务器）。

96. 单击 ***Scan Items***（扫描项目）选项卡。此时将显示 ***Scan Items***（扫描项目）屏幕。

97. 在 ***Heuristics***（启发式）下，取消选中下列选项：

    - ***Find unknown program threats and trojans（查找未知的程序威胁和特洛伊木马病毒）。***
    - ***Find unknown macro threats（查找未知的宏病毒威胁）。***
    - ***Find attachments with multiple extensions（查找含有多个扩展名的附件）。***

98. 在 ***Unwanted programs detection***（有害程序检测）下，取消选中 ***Detect unwanted programs***（检测有害程序）。

99. 从 ***Artemis (Heuristic network check for suspicious files)（Artemis（可疑文件的启发式网络检查））***下，选择 ***Disabled***（已禁用）。

100. 在 ***Scanning of email***（扫描电子邮件）下，取消选中 ***Enable on-delivery email scanning***（启用按递送电子邮件扫描）。

101. 单击 ***Save***（保存）。

102. 为 ***General Options Policies***（常规选项策略）选择 ***My Default***（我的默认设置）。此时将显示 ***VirusScan Enterprise 8.8.0 > General Options Policies（常规选项策略）> My Default（我的默认设置）***屏幕。

103. 从 ***Settings for***（设置对象）下拉列表中选择 ***Workstation***（工作站）。

104. 单击 ***Display Options***（显示选项）选项卡。此时将显示 ***显示 Options***（显示选项）屏幕。

105. 在 ***Console options***（控制台选项）下，选择以下项目：

    - ***Display managed tasks in the client console（在客户端控制台中显示受管任务）。***
    - ***Disable default AutoUpdate task schedule（禁用默认自动更新任务计划）。***

106. 从 ***Settings for***（设置对象）下拉列表中选择 ***Server***（服务器）。

107. 单击 ***Display Options***（显示选项）选项卡。此时将显示 ***显示 Options***（显示选项）屏幕。

108. 在 ***Console options***（控制台选项）下，选择以下项目：

    - ***Display managed tasks in the client console（在客户端控制台中显示受管任务）。***
    - ***Disable default AutoUpdate task schedule（禁用默认自动更新任务计划）。***

109. 单击 ***Save***（保存）。

110. 为 ***Alert Policies***（警报策略）选择 ***My Default***（我的默认设置）。此时将显示 ***VirusScan Enterprise 8.8.0 > Alter Policies（警报策略）> My Default（我的默认设置）***屏幕。

111. 从 ***Settings for***（设置对象）下拉列表中选择 ***Workstation***（工作站）。

112. 单击 ***Alert Manager Alerts***（警报管理器警报）选项卡。此时将显示 ***Alert Manager Alerts***（警报管理器警报）屏幕。

113. 在 ***Components that generate alerts***（生成警报的组件）下，取消选中 ***On-Access Scan***（按访问扫描）、 ***On-Demand Scan and scheduled scans***（按需扫描和计划扫描）、***Email Scan***（电子邮件扫描）和 ***AutoUpdate***（自动更新）。

114. 在 ***Alert Manager***（警报管理器）选项下，选择 ***Disable alerting***（禁用警告）。

115. 在 ***Components that generate alerts***（生成警报的组件）下，取消选中 ***Access Protection***（访问保护）。

116. 单击 ***Additional Alerting Options***（更多警报选项）。此时将显示 ***Additional Alerting Options***（更多警报选项）屏幕。

117. 从 ***Severity Filters***（严重程度过滤器）下拉菜单中，选择 ***Suppress all alerts (severities 0 to 4)***（取消所有警报（严重等级 0-4））。

118. 从 ***Settings for***（设置对象）下拉列表中选择 ***Server***（服务器），然后选择 ***Alert Manager Alerts***（警报管理器警报）选项卡。此时将显示 ***Alert Manager Alerts***（警报管理器警报）屏幕。

119. 在 ***Components that generate alerts***（生成警报的组件）下，取消选中 ***On-Access Scan***（按访问扫描）、 ***On-Demand Scan and scheduled scans***（按需扫描和计划扫描）、***Email Scan***（电子邮件扫描）和 ***AutoUpdate***（自动更新）。

120. 在 ***Alert Manager***（警报管理器）选项下，选择 ***Disable alerting***（禁用警告）。

121. 在 ***Components that generate alerts***（生成警报的组件）下，取消选中 ***Access Protection***（访问保护）。

122. 单击 ***Additional Alerting Options***（更多警报选项）。此时将显示 Additional Alerting Options（更多警报选项）屏幕。

123. 从 ***Severity Filters***（严重程度过滤器）下拉菜单中，选择 ***Suppress all alerts (severities 0 to 4)***（取消所有警报（严重等级 0-4））。

124. 单击 ***Save***（保存）。

125. 为 ***Access Protection Policies***（访问保护策略）选择 ***My Default***（我的默认设置）。此时将显示 ***VirusScan Enterprise 8.8.0 > Access Protection Policies（访问保护策略）> My Default（我的默认设置）***屏幕。

126. 从 ***Settings for***（设置对象）下拉列表中选择 ***Workstation***（工作站）。

127. 单击 ***Access Protection***（访问保护）选项卡。此时将显示 ***Access Protection***（访问保护）屏幕。

128. 在 ***Access protection settings***（访问保护设置）下，取消选中下列选项：
    - ***Enable access protection（启用访问保护）。***
    - ***Prevent McAfee services from being stopped（防止 McAfee 服务停止）。***
129. 从 ***Settings for***（设置对象）下拉列表中选择 ***Server***（服务器）。
130. 单击 ***Access Protection***（访问保护）选项卡。此时将显示 ***Access Protection***（访问保护）屏幕。
131. 在 ***Access protection settings***（访问保护设置）下，取消选中下列选项：
    - ***Enable access protection（启用访问保护）。***
    - ***Prevent McAfee services from being stopped（防止 McAfee 服务停止）。***
132. 单击 ***Save***（保存）。
133. 为 ***Buffer Overflow Protection Policies***（缓冲区溢出保护策略）选择 ***My Default（我的默认设置）***。此时将显示 ***VirusScan Enterprise 8.8.0 > Buffer Overflow Protection Policies（缓冲区溢出保护策略）> My Default（我的默认设置）***屏幕。
134. 从 ***Settings for***（设置对象）下拉列表中选择 ***Workstation***（工作站）。
135. 单击 ***Buffer Overflow Protection***（缓冲区溢出保护）选项卡。此时将显示 ***Buffer Overflow Protection***（缓冲区溢出保护）屏幕。
136. 在 ***Client system warning***（客户端系统警告）下，取消选中 ***Show the message dialog box when a buffer overflow is detected***（检测到缓冲溢出时显示消息对话框）。
137. 在 ***Buffer overflow settings***（缓冲区溢出设置）下，取消选中 ***Enable buffer overflow protection***（启用缓冲区溢出保护）。
138. 从 ***Settings for***（设置对象）下拉列表中选择 ***Server***（服务器）。
139. 单击 ***Buffer Overflow Protection***（缓冲区溢出保护）选项卡。此时将显示 ***Buffer Overflow Protection***（缓冲区溢出保护）屏幕。
140. 在 ***Client system warning***（客户端系统警告）下，取消选中 ***Show the message dialog box when a buffer overflow is detected***（检测到缓冲溢出时显示消息对话框）。
141. 在 ***Buffer overflow settings***（缓冲区溢出设置）下，取消选中 ***Enable buffer overflow protection***（启用缓冲区溢出保护）。
142. 单击 ***Save***（保存）。
143. 从 ***Product***（产品）下拉菜单中，选择 ***McAfee Agent***。此时将显示 McAfee Agent 的 ***Policies***（策略）窗口。
144. 为 ***Repository***（存储库）选择 ***My Default***（我的默认设置）。此时将显示 ***McAfee Agent > Repository（存储库）> My Default（我的默认设置）***屏幕。
145. 单击 ***Proxy***（代理）选项卡。此时将显示 ***Proxy***（代理）屏幕。
146. 在 ***Proxy settings***（代理设置）下，选择 ***Use Internet Explorer settings (For Windows)/ System Preferences settings (For Mac OSX)***（使用 Internet Explorer 设置（对于 Windows）/ 系统偏好设置（对于 Mac OSX）。
147. 单击 ***Save***（保存）。
148. 单击 ***Systems***（系统）选项卡。

149. 选择将已配置的策略部署至哪些客户端系统（采集、回顾和 Centricity Cardiology INW Server）。

150. 选择 ***Wake Up Agents***（唤醒代理）。此时将显示 ***Wake Up Agent***（唤醒代理）窗口。

151. 单击 ***OK***（确定）。

152. 退出 ePolicy Orchestrator。

McAfee ePolicy Orchestrator 5.9.0 服务器控制台配置

1. 根据软件版本，单击 ***Start（开始）> All Programs（所有程序）> McAfee > ePolicy Orchestrator > Launch McAfee ePolicy Orchestrator 5.9.0 Console（启动 McAfee ePolicy Orchestrator 5.9.0 控制台）***。
2. 输入用户名和密码，然后单击 ***Log On***（登录）。
3. 单击 ***Menu（菜单）> Systems（系统）> System Tree（系统树）***。
4. 单击 ***My Organization***（我的组织），然后在焦点在 My Organization（我的组织）上的情况下，单击 ***Assigned Client Tasks***（已分配的客户端任务）选项卡。
5. 单击屏幕底部的 ***Actions（操作）> New Client Task Assignment（新客户端任务分配）***按钮。此时将显示 ***Client Task Assignment Builder***（客户端任务分配构建器）屏幕。
6. 选择以下项目：
   a. ***Product（产品）：***VirusScan Enterprise 8.8.0
   b. ***Task Type（任务类型）：***按需扫描
7. 在 ***Task Actions***（任务操作）下，单击 ***Create New Task***（创建新任务）。此时将显示 ***Create New Task***（创建新任务）屏幕。
8. 在 ***Create New Task***（创建新任务）屏幕上，按如下所示完成各字段：
   a. ***Task Name（任务名称）：***Weekly Scheduled Scan（每周计划扫描）
   b. ***Description（说明）：***Weekly Scheduled Scan（每周计划扫描）
9. 单击 ***Scan Items***（扫描项目）选项卡。此时将显示 ***Scan Items***（扫描项目）屏幕。
10. 在 ***Options***（选项）下，取消选中 ***Detect unwanted programs***（检测有害程序）。
11. 在 Heuristics（启发式）下，取消选中下列选项：
    - ***Find unknown program threats（查找未知的程序威胁）。***
    - ***Find unknown macro threats（查找未知的宏病毒威胁）。***
12. 单击 ***Exclusions***（排除项）选项卡。此时将显示 ***Exclusions***（排除项）屏幕。
13. 单击 ***Add***（添加）。此时将显示 ***Add/Edit Exclusion Item***（添加 / 编辑排除项）屏幕。
14. 选择 ***By pattern***（按模式），然后输入 **C:\Program Files\GE Healthcare\MLCL**、**C:\Program Files (x86)\GE Healthcare\MLCL**、 **D:\GEData\Studies**、 **E:**、 **G:** 文件夹（一次输入一个），再选中 Also exclude subfolders（同时排除子文件夹）。单击 ***OK***（确定）。
15. 单击 ***Performance***（性能）选项卡。此时将显示 ***Performance***（性能）屏幕。

16. 从 ***Artemis (Heuristic network check for suspicious files)（Artemis（可疑文件的启发式网络检查））*** 下，选择 ***Disabled***（已禁用）。
17. 单击 ***Save***（保存）。此时将显示 ***Client Task Assignment Builder***（客户端任务分配构建器）屏幕。
18. 在 ***Client Task Assignment Builder***（客户端任务分配构建器）屏幕中，选择以下各项：
    - ***Product（产品）：*** VirusScan Enterprise 8.8.0
    - ***Task Type（任务类型）：*** 按需扫描
    - ***Task Name（任务名称）：*** Weekly Scheduled Scan（每周计划扫描）
19. 从 ***Scheduled type***（计划类型）下拉列表中选择 ***Weekly***（每周），然后选择 ***Sunday***（星期天）。
20. 将 ***Start time***（开始时间）设置为 ***12:00 AM***，然后选择 ***Run Once at that time***（在该时间运行一次）。
21. 单击 ***Save***（保存）。此时将显示 ***Assigned Client Tasks***（已分配的客户端任务）屏幕。
22. 选择 ***Assigned Policies***（已分配策略）选项卡。此时将显示 ***Assigned Policies***（已分配策略）屏幕。
23. 从 ***Product***（产品）下拉列表中，选择 ***VirusScan Enterprise 8.8.0***。
24. 为 ***On-Access General Policies***（按访问常规策略）选择 ***My Default***（我的默认设置）。此时将显示 ***VirusScan Enterprise 8.8.0 > On-Access General Policies（按访问常规策略）> My Default（我的默认设置）*** 屏幕。
25. 从 ***Settings for***（设置对象）下拉列表中选择 ***Workstation***（工作站），然后选择 ***General***（常规）选项卡。此时将显示 ***General***（常规）屏幕。
26. 从 ***Artemis (Heuristic network check for suspicious files)（Artemis（可疑文件的启发式网络检查））*** 下，选择 ***Disabled***（已禁用）。
27. 单击 ***ScriptScan***（脚本扫描）选项卡。此时将显示 ***Script Scan***（脚本扫描）屏幕。
28. 取消选中 ***Enable scanning of scripts***（启用脚本扫描）。
29. 单击 ***Blocking***（阻止）选项卡。此时将显示 ***Blocking***（阻止）屏幕。
30. 取消选中 ***Block the connection when a threatened file is detected in a shared folder***（在共享文件夹中检测到威胁时阻止连接）。
31. 单击 ***Messages***（消息）选项卡。此时将显示 ***Messages***（消息）屏幕。
32. 取消选中 ***Show the messages dialog box when a threat is detected and display the specified text in the message***（检测到威胁时显示消息对话框并在消息中显示规定文本）。
33. 从 ***Settings for***（设置对象）下拉列表中选择 ***Server***（服务器），然后单击 ***General***（常规）选项卡。此时将显示 ***General***（常规）屏幕。
34. 从 ***Artemis (Heuristic network check for suspicious files)（Artemis（可疑文件的启发式网络检查））*** 下，选择 ***Disabled***（已禁用）。
35. 单击 ***ScriptScan***（脚本扫描）选项卡。此时将显示 ***Script Scan***（脚本扫描）屏幕。
36. 确保 ***Enable scanning of scripts***（启用脚本扫描）处于取消选中状态。
37. 单击 ***Blocking***（阻止）选项卡。此时将显示 ***Blocking***（阻止）屏幕。

38. 取消选中 ***Block the connection when a threatened file is detected in a shared folder***（在共享文件夹中检测到威胁时阻止连接）。

39. 单击 ***Messages***（消息）选项卡。此时将显示 ***Messages***（消息）屏幕。

40. 取消选中 ***Show the messages dialog box when a threat is detected and display the specified text in the message***（检测到威胁时显示消息对话框并在消息中显示规定文本）。

41. 单击 ***Save***（保存）。此时将显示 Assigned Policies（已分配策略）屏幕。

42. 为 ***On-Access Default Processes Policies***（按访问默认进程策略）选择 ***My Default***（我的默认设置）。此时将显示 ***VirusScan Enterprise 8.8.0 > On-Access Default Processes Policies（按访问默认进程策略）> My Default（我的默认设置）***屏幕。

43. 从 ***Settings for***（设置对象）下拉列表中选择 ***Workstation***（工作站）。

44. 单击 ***Scan Items***（扫描项目）选项卡。此时将显示 ***Scan Items***（扫描项目）屏幕。

45. 在 ***Heuristics***（启发式）下，取消选中下列选项：

    - ***Find unknown unwanted programs and trojans（查找未知的有害程序和特洛伊木马病毒）。***
    - ***Find unknown macro threats（查找未知的宏病毒威胁）。***

46. 在 ***Unwanted programs detection***（有害程序检测）下，取消选中 ***Detect unwanted programs***（检测有害程序）。

47. 单击 ***Exclusions***（排除项）选项卡。此时将显示 ***Exclusions***（排除项）屏幕。

48. 单击 ***Add***（添加）。此时将显示 ***Add/Edit Exclusion Item***（添加 / 编辑排除项）屏幕。

49. 选择 ***By pattern***（按模式），然后输入 **C:\Program Files\GE Healthcare\MLCL**、**D:\GEData\Studies**、**E:**、**G:** 文件夹（一次输入一个），再选中 ***Also exclude subfolders***（同时排除子文件夹）。单击 ***OK***（确定）。

50. 从 ***Settings for***（设置对象）下拉列表中选择 ***Server***（服务器），然后单击 ***Scan Items***（扫描项目）选项卡。此时将显示 ***Scan Items***（扫描项目）屏幕。

51. 在 ***Heuristics***（启发式）下，取消选中下列选项：

    - ***Find unknown unwanted programs and trojans（查找未知的有害程序和特洛伊木马病毒）。***
    - ***Find unknown macro threats（查找未知的宏病毒威胁）。***

52. 在 ***Unwanted programs detection***（有害程序检测）下，取消选中 ***Detect unwanted programs***（检测有害程序）。

53. 单击 ***Exclusions***（排除项）选项卡。此时将显示 ***Exclusions***（排除项）屏幕。

54. 单击 ***Add***（添加）。此时将显示 ***Add/Edit Exclusion Item***（添加 / 编辑排除项）屏幕。

55. 选择 ***By pattern***（按模式），然后输入 **C:\Program Files (x86)\GE Healthcare\MLCL**、**D:\GEData\Studies** 文件夹（一次输入一个），再选中 ***Also exclude subfolders***（同时排除子文件夹）。单击 ***OK***（确定）。

56. 单击 ***Save***（保存）。此时将显示 ***Assigned Policies***（已分配策略）屏幕。

57. 为 ***On-Access Low-Risk Processes Policies***（按访问低风险进程策略）选择 ***My Default***（我的默认设置）。此时将显示 ***VirusScan Enterprise 8.8.0 > On-Access Low-Risk Processes Policies（按访问低风险进程策略）> My Default（我的默认设置）***屏幕。

58. 从 ***Settings for***（设置对象）下拉列表中选择 ***Workstation***（工作站）。
59. 单击 ***Scan Items***（扫描项目）选项卡。此时将显示 ***Scan Items***（扫描项目）屏幕。
60. 在 ***Heuristics***（启发式）下，取消选中下列选项：
    - ***Find unknown unwanted programs and trojans（查找未知的有害程序和特洛伊木马病毒）。***
    - ***Find unknown macro threats（查找未知的宏病毒威胁）。***
61. 在 ***Unwanted programs detection***（有害程序检测）下，取消选中 ***Detect unwanted programs***（检测有害程序）。
62. 单击 ***Exclusions***（排除项）选项卡。此时将显示 ***Exclusions***（排除项）屏幕。
63. 单击 ***Add***（添加）。此时将显示 ***Add/Edit Exclusion Item***（添加 / 编辑排除项）屏幕。
64. 选择 ***By pattern***（按模式），然后输入 **C:\Program Files\GE Healthcare\MLCL**、**D:\GEData\Studies**、**E:**、**G:** 文件夹（一次输入一个），再选中 ***Also exclude subfolders***（同时排除子文件夹）。单击 ***OK***（确定）。
65. 从 ***Settings for***（设置对象）下拉列表中选择 ***Server***（服务器），然后单击 ***Scan Items***（扫描项目）选项卡。此时将显示 ***Scan Items***（扫描项目）屏幕。
66. 在 ***Heuristics***（启发式）下，取消选中下列选项：
    - ***Find unknown unwanted programs and trojans（查找未知的有害程序和特洛伊木马病毒）。***
    - ***Find unknown macro threats（查找未知的宏病毒威胁）。***
67. 在 ***Unwanted programs detection***（有害程序检测）下，取消选中 ***Detect unwanted programs***（检测有害程序）。
68. 单击 ***Exclusions***（排除项）选项卡。此时将显示 ***Exclusions***（排除项）屏幕。
69. 单击 ***Add***（添加）。此时将显示 ***Add/Edit Exclusion Item***（添加 / 编辑排除项）屏幕。
70. 选择 ***By pattern***（按模式），然后输入 **C:\Program Files (x86)\GE Healthcare\MLCL**、**D:\GEData\Studies** 文件夹（一次输入一个），再选中 ***Also exclude subfolders***（同时排除子文件夹）。单击 ***OK***（确定）。
71. 单击 ***Save***（保存）。此时将显示 ***Assigned Policies***（已分配策略）屏幕。
72. 为 ***On-Access High-Risk Processes Policies***（按访问高风险进程策略）选择 ***My Default***（我的默认设置）。此时将显示 ***VirusScan Enterprise 8.8.0 > On-Access High-Risk Processes Policies（按访问高风险进程策略）> My Default 我的默认设置）***屏幕。
73. 从 ***Settings for***（设置对象）下拉列表中选择 ***Workstation***（工作站）。
74. 单击 ***Scan Items***（扫描项目）选项卡。此时将显示 ***Scan Items***（扫描项目）屏幕。
75. 在 ***Heuristics***（启发式）下，取消选中下列选项：
    - ***Find unknown unwanted programs and trojans（查找未知的有害程序和特洛伊木马病毒）。***
    - ***Find unknown macro threats（查找未知的宏病毒威胁）。***
76. 在 ***Unwanted programs detection***（有害程序检测）下，取消选中 ***Detect unwanted programs***（检测有害程序）。
77. 单击 ***Exclusions***（排除项）选项卡。此时将显示 ***Exclusions***（排除项）屏幕。

78. 单击 ***Add***（添加）。此时将显示 ***Add/Edit Exclusion Item***（添加 / 编辑排除项）屏幕。

79. 选择 ***By pattern***（按模式），然后输入 **C:\Program Files\GE Healthcare\MLCL**、**D:\GEData\Studies**、**E:**、**G:** 文件夹（一次输入一个），再选中 ***Also exclude subfolders***（同时排除子文件夹）。单击 ***OK***（确定）。

80. 从 ***Settings for***（设置对象）下拉列表中选择 ***Server***（服务器），然后单击 ***Scan Items***（扫描项目）选项卡。此时将显示 ***Scan Items***（扫描项目）屏幕。

81. 在 ***Heuristics***（启发式）下，取消选中下列选项：

    - ***Find unknown unwanted programs and trojans（查找未知的有害程序和特洛伊木马病毒）。***
    - ***Find unknown macro threats（查找未知的宏病毒威胁）。***

82. 在 ***Unwanted programs detection***（有害程序检测）下，取消选中 ***Detect unwanted programs***（检测有害程序）。

83. 单击 ***Exclusions***（排除项）选项卡。此时将显示 ***Exclusions***（排除项）屏幕。

84. 单击 ***Add***（添加）。此时将显示 ***Add/Edit Exclusion Item***（添加 / 编辑排除项）屏幕。

85. 选择 By pattern（按模式），然后输入 **C:\Program Files (x86)\GE Healthcare\MLCL**、**D:\GEData\Studies** 文件夹（一次输入一个），再选中 ***Also exclude subfolders***（同时排除子文件夹）。单击 ***OK***（确定）。

86. 单击 ***Save***（保存）。此时将显示 ***Assigned Policies***（已分配策略）屏幕。

87. 为 ***On Delivery Email Scan Policies***（按递送电子邮件扫描策略）单击 ***My Default***（我的默认设置）。此时将显示 ***VirusScan Enterprise 8.8.0 > On Delivery Email Scan Policies（按递送电子邮件扫描策略）> My Default（我的默认设置）***屏幕。

88. 从 ***Settings for***（设置对象）下拉列表中选择 ***Workstation***（工作站）。

89. 单击 ***Scan Items***（扫描项目）选项卡。此时将显示 ***Scan Items***（扫描项目）屏幕。

90. 在 ***Heuristics***（启发式）下，取消选中下列选项。

    - ***Find unknown program threats and trojans（查找未知的程序威胁和特洛伊木马病毒）。***
    - ***Find unknown macro threats（查找未知的宏病毒威胁）。***
    - ***Find attachments with multiple extensions（查找含有多个扩展名的附件）。***

91. 在 ***Unwanted programs detection***（有害程序检测）下，取消选中 ***Detect unwanted programs***（检测有害程序）。

92. 从 ***Artemis (Heuristic network check for suspicious files)（Artemis（可疑文件的启发式网络检查））***下，选择 ***Disabled***（已禁用）。

93. 在 ***Scanning of email***（扫描电子邮件）下，取消选中 ***Enable on-delivery email scanning***（启用按递送电子邮件扫描）。

94. 从 ***Settings for***（设置对象）下拉列表中选择 ***Server***（服务器）。

95. 单击 ***Scan Items***（扫描项目）选项卡。此时将显示 ***Scan Items***（扫描项目）屏幕。

96. 在 ***Heuristics***（启发式）下，取消选中下列选项：

    - ***Find unknown program threats and trojans（查找未知的程序威胁和特洛伊木马病毒）。***
    - ***Find unknown macro threats（查找未知的宏病毒威胁）。***

- ***Find attachments with multiple extensions（查找含有多个扩展名的附件）。***

97. 在 ***Unwanted programs detection***（有害程序检测）下，取消选中 ***Detect unwanted programs***（检测有害程序）。
98. 从 ***Artemis (Heuristic network check for suspicious files)（Artemis（可疑文件的启发式网络检查））***下，选择 ***Disabled***（已禁用）。
99. 在 ***Scanning of email***（扫描电子邮件）下，取消选中 ***Enable on-delivery email scanning***（启用按递送电子邮件扫描）。
100. 单击 ***Save***（保存）。此时将显示 ***Assigned Policies***（已分配策略）屏幕。
101. 为 ***General Options Policies***（常规选项策略）选择 ***My Default***（我的默认设置）。此时将显示 ***VirusScan Enterprise 8.8.0 > General Options Policies（常规选项策略）> My Default（我的默认设置）***屏幕。
102. 从 ***Settings for***（设置对象）下拉列表中选择 ***Workstation***（工作站）。
103. 单击 ***Display Options***（显示选项）选项卡。此时将显示 ***显示 Options***（显示选项）屏幕。
104. 在 ***Console options***（控制台选项）下，选择以下项目：
    - ***Display managed tasks in the client console（在客户端控制台中显示受管任务）。***
    - ***Disable default AutoUpdate task schedule（禁用默认自动更新任务计划）。***
105. 从 ***Settings for***（设置对象）下拉列表中选择 ***Server***（服务器）。
106. 单击 ***Display Options***（显示选项）选项卡。此时将显示 ***显示 Options***（显示选项）屏幕。
107. 在 ***Console options***（控制台选项）下，选择以下项目：
    - ***Display managed tasks in the client console（在客户端控制台中显示受管任务）。***
    - ***Disable default AutoUpdate task schedule（禁用默认自动更新任务计划）。***
108. 单击 ***Save***（保存）。此时将显示 ***Assigned Policies***（已分配策略）屏幕。
109. 为 ***Alert Policies***（警报策略）选择 ***My Default***（我的默认设置）。此时将显示 ***VirusScan Enterprise 8.8.0 > Alter Policies（警报策略）> My Default（我的默认设置）***屏幕。
110. 从 ***Settings for***（设置对象）下拉列表中选择 ***Workstation***（工作站）。
111. 单击 ***Alert Manager Alerts***（警报管理器警报）选项卡。此时将显示 ***Alert Manager Alerts***（警报管理器警报）屏幕。
112. 在 ***Components that generate alerts***（生成警报的组件）下，取消选中 ***On-Access Scan***（按访问扫描）、 ***On-Demand Scan and scheduled scans***（按需扫描和计划扫描）、***Email Scan***（电子邮件扫描）和 ***AutoUpdate***（自动更新）。
113. 在 ***Alert Manager***（警报管理器）选项下，选择 ***Disable alerting***（禁用警告）。
114. 在 ***Components that generate alerts***（生成警报的组件）下，取消选中 ***Access Protection***（访问保护）。
115. 单击 ***Additional Alerting Options***（更多警报选项）。此时将显示 ***Additional Alerting Options***（更多警报选项）屏幕。
116. 从 ***Severity Filters***（严重程度过滤器）下拉菜单中，选择 ***Suppress all alerts (severities 0 to 4)***（取消所有警报（严重等级 0-4））。

117. 从 ***Settings for***（设置对象）下拉列表中选择 ***Server***（服务器），然后选择 ***Alert Manager Alerts***（警报管理器警报）选项卡。此时将显示 ***Alert Manager Alerts***（警报管理器警报）屏幕。

118. 在 ***Components that generate alerts***（生成警报的组件）下，取消选中 ***On-Access Scan***（按访问扫描）、 ***On-Demand Scan and scheduled scans***（按需扫描和计划扫描）、***Email Scan***（电子邮件扫描）和 ***AutoUpdate***（自动更新）。

119. 在 ***Alert Manager***（警报管理器）选项下，选择 ***Disable alerting***（禁用警告）。

120. 在 ***Components that generate alerts***（生成警报的组件）下，取消选中 ***Access Protection***（访问保护）。

121. 单击 ***Additional Alerting Options***（更多警报选项）。此时将显示 Additional Alerting Options（更多警报选项）屏幕。

122. 从 ***Severity Filters***（严重程度过滤器）下拉菜单中，选择 ***Suppress all alerts (severities 0 to 4)***（取消所有警报（严重等级 0-4））。

123. 单击 ***Save***（保存）。此时将显示 ***Assigned Policies***（已分配策略）屏幕。

124. 为 ***Access Protection Policies***（访问保护策略）选择 ***My Default***（我的默认设置）。此时将显示 ***VirusScan Enterprise 8.8.0 > Access Protection Policies（访问保护策略）> My Default（我的默认设置）***屏幕。

125. 从 ***Settings for***（设置对象）下拉列表中选择 ***Workstation***（工作站）。

126. 单击 ***Access Protection***（访问保护）选项卡。此时将显示 ***Access Protection***（访问保护）屏幕。

127. 在 ***Access protection settings***（访问保护设置）下，取消选中下列选项：

    - ***Enable access protection（启用访问保护）。***
    - ***Prevent McAfee services from being stopped（防止 McAfee 服务停止）。***
    - ***启用增强型自我保护。***

128. 从 ***Settings for***（设置对象）下拉列表中选择 ***Server***（服务器）。

129. 单击 ***Access Protection***（访问保护）选项卡。此时将显示 ***Access Protection***（访问保护）屏幕。

130. 在 ***Access protection settings***（访问保护设置）下，取消选中下列选项：

    - ***Enable access protection（启用访问保护）。***
    - ***Prevent McAfee services from being stopped（防止 McAfee 服务停止）。***
    - ***启用增强型自我保护。***

131. 单击 ***Save***（保存）。此时将显示 ***Assigned Policies***（已分配策略）屏幕。

132. 为 ***Buffer Overflow Protection Policies***（缓冲区溢出保护策略）选择 ***My Default（我的默认设置）***。此时将显示 ***VirusScan Enterprise 8.8.0 > Buffer Overflow Protection Policies（缓冲区溢出保护策略）> My Default（我的默认设置）***屏幕。

133. 从 ***Settings for***（设置对象）下拉列表中选择 ***Workstation***（工作站）。

134. 单击 ***Buffer Overflow Protection***（缓冲区溢出保护）选项卡。此时将显示 ***Buffer Overflow Protection***（缓冲区溢出保护）屏幕。

135. 在 ***Client system warning***（客户端系统警告）下，取消选中 ***Show the message dialog box when a buffer overflow is detected***（检测到缓冲溢出时显示消息对话框）。

136. 在 ***Buffer overflow settings***（缓冲区溢出设置）下，取消选中 ***Enable buffer overflow protection***（启用缓冲区溢出保护）。
137. 从 ***Settings for***（设置对象）下拉列表中选择 ***Server***（服务器）。
138. 单击 ***Buffer Overflow Protection***（缓冲区溢出保护）选项卡。此时将显示 ***Buffer Overflow Protection***（缓冲区溢出保护）屏幕。
139. 在 ***Client system warning***（客户端系统警告）下，取消选中 ***Show the message dialog box when a buffer overflow is detected***（检测到缓冲溢出时显示消息对话框）。
140. 在 ***Buffer overflow settings***（缓冲区溢出设置）下，取消选中 ***Enable buffer overflow protection***（启用缓冲区溢出保护）。
141. 单击 ***Save***（保存）。此时将显示 ***Assigned Policies***（已分配策略）屏幕。
142. 从 ***Product***（产品）下拉菜单中，选择 ***McAfee Agent***。此时将显示 McAfee Agent 的 ***Policies***（策略）窗口。
143. 为 ***Repository***（存储库）选择 ***My Default***（我的默认设置）。此时将显示 ***McAfee Agent > Repository（存储库）> My Default（我的默认设置）***屏幕。
144. 单击 ***Proxy***（代理）选项卡。此时将显示 ***Proxy***（代理）屏幕。
145. 确保已选中 ***Proxy settings***（代理设置）下的 ***Use Internet Explorer settings (For Windows)/System Preferences settings (For Mac OSX)***（使用 Internet Explorer 设置（对于 Windows）/ 系统偏好设置（对于 Mac OSX）。
146. 单击 ***Save***（保存）。此时将显示 ***Assigned Policies***（已分配策略）屏幕。
147. 单击 ***Systems***（系统）选项卡。
148. 选择将已配置的策略部署至哪些客户端系统（采集、回顾和 Centricity Cardiology INW Server）。
149. 选择 ***Wake Up Agents***（唤醒代理）。此时将显示 ***Wake Up Agent***（唤醒代理）窗口。
150. 单击 ***OK***（确定）。
151. 退出 ePolicy Orchestrator。

McAfee ePolicy Orchestrator 安装后指南

启用环回连接。有关详细信息，请参阅启用环回连接（第 6 页）。

Trend Micro OfficeScan Client/Server Edition 10.6 SP2

安装概述

仅在联网的 Mac-Lab/CardioLab 环境中安装 Trend Micro OfficeScan Client/Server Edition。一定要先将 Trend Micro OfficeScan 安装在 防病毒 Management Console Server 中，然后再作为客户端部署至 Centricity Cardiology INW Server 和采集 / 回顾工作站。使用下面的说明来安装 ***Trend Micro OfficeScan Client/Server Edition***。

贵机构有责任升级防病毒软件。定期更新病毒定义，以确保系统上的病毒防护总是处于最新状态。

安装前指南

1. Trend Micro 防病毒 Management Console 应根据 Trend Micro 说明安装，并可以正常工作。
2. 在安装 Trend Micro OfficeScan 期间，请在 防病毒 Management Console Server 上执行以下操作：
   a. 在 ***防病毒 Feature***（防病毒功能）窗口中，取消选中 ***Enable firewall***（启用防火墙）。
   b. 在 ***Anti-spyware Feature***（防间谍软件功能）窗口中，选择 ***No, Please do not enable assessment mode***（否，不启用评估模式）。
   c. 在 ***Web Reputation Feature***（网络信誉功能）窗口中，取消选中 ***Enable web reputation policy***（启用网络信誉策略）。
3. 当将 CO_2 功能与 Mac-Lab/CardioLab 系统中的 PDM 搭配使用时，建议不要使用 Trend Micro OfficeScan。
4. 如果需要 Trend Micro OfficeScan：
   a. 建议为 Mac-Lab/CardioLab 系统配置一个独立的 Trend Micro 防病毒 Management Console Server。需要对防病毒设置进行全局更改，以便将 CO_2 功能与 Mac-Lab/CardioLab 系统中的 PDM 搭配使用。
   b. 如果不能配置独立的 Trend Micro 防病毒 Management Console Server，则需要在安装后对现有 Trend Micro 防病毒 Management Console Server 进行全局更改。此更改将影响已连接到现有 Trend Micro 防病毒 Management Console Server 的所有客户端系统，应该先通过 IT 人员审查再继续。
5. 在所有客户端系统（采集、回顾和 INW Server）上以**管理员**或管理员组成员的身份登录以安装防病毒软件。
6. 禁用环回连接。有关详细信息，请参阅禁用环回连接（第 6 页）。
7. 配置 Computer Browser 服务。有关详细信息，请参阅在安装防病毒软件之前配置 Computer Browser 服务（第 6 页）。

Trend Micro OfficeScan - 新安装部署步骤（首选推送安装方法）

1. 单击 ***Start（开始）> All Programs（所有程序）> TrendMicro OfficeScan server - <server name> > Office Scan Web Console（Office Scan Web 控制台）***。

注意： 选择 ***Continue to this website (not recommended)***（继续此网站（不推荐）继续。在 Security Alert（安全警报）窗口中，选中 ***In the future, do not show this warning***（以后不再显示此警告），然后单击 ***OK***（确定）。

2. 如果您接收到整数错误，指出网站不可信，请管理您的证书以包括 Trend Micro OfficeScan。
3. 如果系统提示，请安装 ***AtxEnc*** 加载项。此时将显示 Security Warning（安全警告）屏幕。
4. 单击 ***Install***（安装）。
5. 输入用户名和密码，然后单击 ***Log On***（登录）。
6. 如果系统提示，请单击 ***Update Now***（立即更新）以安装新的小组件。等待到新的小组件更新完毕。此时将显示更新已完成屏幕。
7. 单击 ***OK***（确定）。
8. 从左侧菜单栏中，单击 ***Networked Computers（联网的计算机）> Client Installation（客户端安装）> Remote（远程）***。
9. 如果系统提示，请安装 ***AtxConsole*** 加载项。此时将显示 Security Warning（安全警告）屏幕。
10. 单击 ***Install***（安装）。
11. 在 ***Remote Installation***（远程安装）窗口中，双击 ***My Company***（我的公司）。所有域都将列出在 ***My Company***（我的公司）下。
12. 展开列表中的域（示例：INW）。此时将显示已连接到域的所有系统。
13. 如果域或系统未列出在 ***Domain and Computers***（域和计算机）窗口中，请在每个客户端系统（采集、回顾和 INW Server）上执行以下操作：
    a. 在所有客户端计算机上以管理员或管理员组成员的身份登录。
    b. 单击 ***Start（开始）> Run（运行）***。
    c. 输入 ***\\< 防病毒 Management Console_server_IP_address>***，然后按 ***Enter*** 键。系统提示时，输入管理员用户名和密码。
    d. 导航到 ***\\< 防病毒 Management Console_server_IP _address>\ofsscan***，然后双击 ***AutoPcc.exe***。系统提示时，输入管理员用户名和密码。
    e. 安装完成后，重新启动客户端系统。
    f. 在所有客户端计算机上以**管理员**或管理员组成员身份登录，并等待到系统托盘中的 Trend Micro OfficeScan 图标更改为蓝色。
    g. 跳过此程序中的剩余步骤，转到 Trend Micro OfficeScan 服务器控制台配置程序。
14. 选择客户端机器（采集、回顾和 INW Server），然后单击 ***Add***（添加）。
15. 键入 < 域名 >\ 用户名和密码，然后单击 ***Log on***（登录）。
16. 从 ***Selected Computers***（已选择的计算机）窗格中选择客户端机器（采集、回顾和 INW Server），然后单击 ***Install***（安装）。
17. 在确认框中单击 ***Yes***（是）。
18. 在 ***Number of clients to which notifications were sent***（已将通知发送给的客户端数目）消息框中，单击 ***OK***（确定）。

19. 重新启动所有客户端机器（采集、回顾和 INW Server）并在所有客户端计算机上以管理员或管理员组成员身份登录，并等待到系统托盘中的 Trend Micro OfficeScan 图标变成蓝色并显示绿色的勾号。

20. 单击 ***Log Off***（注销）链接以关闭 ***OfficeScan Web Console***（OfficeScan Web 控制台）。

Trend Micro OfficeScan 服务器控制台的配置

1. 依次选择 ***Start（开始）> All Programs（所有程序）> TrendMicro Office Scan server <servername> > Office Scan Web Console（Office Scan Web 控制台）***。此时将显示 ***Trend Micro OfficeScan Login***（Trend Micro OfficeScan 登录）屏幕。

2. 输入用户名和密码，然后单击 ***Login***（登录）。此时将显示 ***Summary***（摘要）屏幕。

3. 在左侧窗格中选择 ***Networked Computers（联网的计算机）> Client Management（客户端管理）***链接。

4. 在右侧窗格中选择 ***OfficeScan Server***。

5. 从 ***Settings***（设置）选项中，选择 ***Scan Settings（扫描设置）> Manual Scan Settings（手动扫描设置）***。此时将显示 ***Manual Scan Settings***（手动扫描设置）屏幕。

6. 单击 ***Target***（目标）选项卡，然后只选择下列选项，取消选中其余的选项：

   - ***Files to Scan（要扫描的文件）> File types scanned by IntelliScan（由 IntelliScan 扫描的文件类型）。***
   - ***Scan Settings（扫描设置）> Scan compressed files（扫描压缩的文件）。***
   - ***Scan Settings（扫描设置）> Scan OLE objects（扫描 OLE 对象）。***
   - ***Virus/Malware Scan Settings Only（仅病毒 / 恶意软件扫描设置）> Scan boot area（扫描启动区）。***
   - ***CPU Usage（CPU 占用率）> Low（低）。***
   - ***Scan Exclusion（扫描排除）> Enable scan exclusion（启用扫描排除）。***
   - ***Scan Exclusion（扫描排除）> Apply scan exclusion settings to all scan types（将扫描排除设置应用到所有扫描类型）。***
   - ***Scan Exclusion List (Directories)（扫描排除列表（目录））> Exclude directories where Trend Micro products are installed and select Add path to client Computers Exclusion list（排除 Trend Micro 产品安装目录并选择将路径添加到客户端计算机排除列表）。***
   - 输入 **C:\Program Files (x86)\GE Healthcare\MLCL**、 **C:\Program Files\GE Healthcare\MLCL**、 **D:\GEData\Studies**、 **E:** 和 **G:** 文件夹（一次一个）并单击 ***Add***（添加）。

7. 单击 ***Apply to All Clients***（应用到所有客户端）。

8. 显示以下消息时，单击 ***OK***（确定）：***The exclusion list on this screen will replace the exclusion list on the clients or domains you selected in the client tree earlier.Do you want to proceed?***（此屏幕上的排除列表将替换您先前在客户端树上选择的代理程序或域上的排除列表。是否要继续？）。

9. 单击 ***Close***（关闭）以关闭 ***Manual Scan Settings***（手动扫描设置）屏幕。

10. 在左侧窗格中选择 ***Networked Computers（联网的计算机）> Client Management（客户端管理）***链接。

11. 在右侧窗格中选择 ***OfficeScan*** Server（OfficeScan 服务器）。

12. 在 ***Settings***（设置）选项中，依次选择 ***Scan Settings（扫描设置）> Real-time Scan Settings（实时扫描设置）***。此时将显示 ***Real-time Scan Settings***（实时扫描设置）屏幕。
13. 单击 ***Target***（目标）选项卡，然后只选择下列选项，取消选中其余的选项：
    - ***Real-Time Scan Settings（实时扫描设置）> Enable virus/malware scan（启用病毒 / 恶意软件扫描）。***
    - ***Real-Time Scan Settings（实时扫描设置）> Enable spyware/grayware scan（启用间谍软件 / 灰色软件扫描）。***
    - ***Files to Scan（要扫描的文件）> File types scanned by IntelliScan（由 IntelliScan 扫描的文件类型）。***
    - ***Scan Settings（扫描设置）> Scan compressed files（扫描压缩的文件）。***
    - ***Scan Settings（扫描设置）> Scan OLE objects（扫描 OLE 对象）。***
    - ***Virus/Malware Scan Settings Only（仅病毒 / 恶意软件扫描设置）> Enable IntelliTrap（启用 IntelliTrap）。***
    - ***Scan Exclusion（扫描排除）> Enable scan exclusion（启用扫描排除）。***
    - ***Scan Exclusion（扫描排除）> Apply scan exclusion settings to all scan types（将扫描排除设置应用到所有扫描类型）。***
    - ***Scan Exclusion List (Directories)（扫描排除列表（目录））> Exclude directories where Trend Micro products are installed（排除 Trend Micro 产品的安装目录）。***
    - 确保 ***C:\Program Files (x86)\GE Healthcare\MLCL***， ***C:\Program Files \GE Healthcare\MLCL***、 ***D:\GEData\Studies***、 ***E:*** 和 ***G:*** 文件夹路径存在于 ***Exclusion List***（排除列表）中。
14. 单击 ***Action***（操作）选项卡。
15. 保留默认设置，然后取消选中以下选项：
    - ***Virus/Malware（病毒 / 恶意软件）> Display a notification message on the client computer when virus/malware is detected（检测到病毒 / 恶意软件时在客户端计算机上显示通知消息）。***
    - ***Spyware/Grayware（间谍软件 / 灰色软件）> Display a notification message on the client computer when spyware/grayware is detected（检测到间谍软件 / 灰色软件时在客户端计算机上显示通知消息）。***
16. 单击 ***Apply to All Clients***（应用到所有客户端）。
17. 单击 ***Close***（关闭）以关闭 ***Real-time Scan Settings***（实时扫描设置）屏幕。
18. 在左侧窗格中选择 ***Networked Computers（联网的计算机）> Client Management（客户端管理）***链接。
19. 在右侧窗格中选择 ***OfficeScan Server***。
20. 从 ***Settings***（设置）选项中，依次选择 ***Scan Settings（扫描设置）> Scheduled Scan Settings（计划扫描设置）***。此时将显示 ***Scheduled Scan Settings***（计划扫描设置）屏幕。
21. 单击 ***Target***（目标）选项卡，然后只选择下列选项，取消选中其余的选项：
    - ***Scheduled Scan Settings（计划扫描设置）> Enable virus/malware scan（启用病毒 / 恶意软件扫描）。***
    - ***Scheduled Scan Settings（计划扫描设置）> Enable virus/malware scan（启用间谍软件 / 灰色软件扫描）。***
    - ***Schedule（计划）> Weekly（每周），每星期天， Start time（开始时间）：00:00 hh:mm。***

- ***Files to Scan（要扫描的文件）> File types scanned by IntelliScan（由 IntelliScan 扫描的文件类型）。***
- ***Scan Settings（扫描设置）> Scan compressed files（扫描压缩的文件）。***
- ***Scan Settings（扫描设置）> Scan OLE objects（扫描 OLE 对象）。***
- ***Virus/Malware Scan Settings Only（仅病毒 / 恶意软件扫描设置）> Scan boot area（扫描启动区）。***
- ***CPU Usage（CPU 占用率）> Low（低）。***
- ***Scan Exclusion（扫描排除）> Enable scan exclusion（启用扫描排除）。***
- ***Scan Exclusion（扫描排除）> Apply scan exclusion settings to all scan types（将扫描排除设置应用到所有扫描类型）。***
- ***Scan Exclusion List (Directories)（扫描排除列表（目录））> Exclude directories where Trend Micro products are installed（排除 Trend Micro 产品的安装目录）。***
- 确保 ***C:\Program Files (x86)\GE Healthcare\MLCL***、 ***C:\Program Files \GE Healthcare\MLCL***、 ***D:\GEData\Studies***、 ***E:*** 和 ***G:*** 文件夹路径存在于 Exclusion List（排除列表）中。

22. 单击 ***Action***（操作）选项卡。
23. 保留默认设置，然后取消选中以下选项：
    - ***Virus/Malware（病毒 / 恶意软件）> Display a notification message on the client computer when virus/malware is detected（检测到病毒 / 恶意软件时在客户端计算机上显示通知消息）。***
    - ***Spyware/Grayware（间谍软件 / 灰色软件）> Display a notification message on the client computer when spyware/grayware is detected（检测到间谍软件 / 灰色软件时在客户端计算机上显示通知消息）。***
24. 单击 ***Apply to All Clients***（应用到所有客户端）。
25. 单击 ***Close***（关闭）以关闭 ***Scheduled Scan Settings***（计划扫描设置）屏幕。
26. 在左侧窗格中选择 ***Networked Computers（联网的计算机）> Client Management（客户端管理）***链接。
27. 在右侧窗格中选择 ***OfficeScan Server***。
28. 从 ***Settings***（设置）选项中，依次选择 ***Scan Settings（扫描设置）> Scan Now Settings（立即扫描设置）***。此时将显示 ***Scan Now Settings***（立即扫描设置）屏幕。
29. 单击 ***Target***（目标）选项卡，然后只选择下列选项，取消选中其余的选项：
    - ***Scan Now Settings（立即扫描设置）> Enable virus/malware scan（启用病毒 / 恶意软件扫描）。***
    - ***Scan Now Settings（立即扫描设置）> Enable virus/malware scan（启用病毒 / 恶意软件扫描）。***
    - ***Files to Scan（要扫描的文件）> File types scanned by IntelliScan（由 IntelliScan 扫描的文件类型）。***
    - ***Scan Settings（扫描设置）> Scan compressed files（扫描压缩的文件）。***
    - ***Scan Settings（扫描设置）> Scan OLE objects（扫描 OLE 对象）。***
    - ***Virus/Malware Scan Settings Only（仅病毒 / 恶意软件扫描设置）> Scan boot area（扫描启动区）。***
    - ***CPU Usage（CPU 占用率）> Low（低）。***
    - ***Scan Exclusion（扫描排除）> Enable scan exclusion（启用扫描排除）。***

- ***Scan Exclusion（扫描排除）> Apply scan exclusion settings to all scan types（将扫描排除设置应用到所有扫描类型）。***
- ***Scan Exclusion List (Directories)（扫描排除列表（目录））> Exclude directories where Trend Micro products are installed（排除 Trend Micro 产品的安装目录）。***
- 确保 ***C:\Program Files (x86)\GE Healthcare\MLCL***、 ***C:\Program Files \GE Healthcare\MLCL***、 ***D:\GEData\Studies***、 ***E:*** 和 ***G:***

30. 单击 ***Apply to All Clients***（应用到所有客户端）。
31. 单击 ***Close***（关闭）以关闭 ***Scan Now Settings***（立即扫描设置）屏幕。
32. 在左侧窗格中选择 ***Networked Computers（联网的计算机）> Client Management（客户端管理）***链接。
33. 在右侧窗格中选择 ***OfficeScan Server***。
34. 从 ***Settings***（设置）选项中选择 ***Web Reputation Settings***（网络信誉设置）。此时将显示 ***Web Reputation Settings***（网络信誉设置）屏幕。
35. 单击 ***External Clients***（外部客户端）选项卡，然后取消选中 ***Enable Web reputation policy on the following operating systems***（在下列操作系统上启用网络信誉策略）（如果在安装期间已选中的话）。
36. 单击 ***Internal Clients***（内部客户端）选项卡，然后取消选中 ***Enable Web reputation policy on the following operating systems***（在下列操作系统上启用网络信誉策略）（如果在安装期间已选中的话）。
37. 单击 ***Apply to All Clients***（应用到所有客户端）。
38. 单击 ***Close***（关闭）以关闭 ***Web Reputation***（网络信誉）屏幕。
39. 在左侧窗格中选择 ***Networked Computers（联网的计算机）> Client Management（客户端管理）***链接。
40. 在右侧窗格中选择 ***OfficeScan Server***。
41. 从 ***Settings***（设置）选项中选择 ***Behavior Monitoring Settings***（行为监控设置）。此时将显示 ***Behavior Monitoring Settings***（行为监控设置）屏幕。
42. 取消选中 ***Enable Malware Behavior Blocking***（启用恶意软件行为组织）和 ***Enable Event Monitoring***（启用事件监控）选项。
43. 单击 ***Apply to All Clients***（应用到所有客户端）。
44. 单击 ***Close***（关闭）以关闭 ***Behavior Monitoring***（行为监控）屏幕。
45. 在左侧窗格中选择 ***Networked Computers（联网的计算机）> Client Management（客户端管理）***链接。
46. 在右侧窗格中选择 ***OfficeScan Server***。
47. 从 ***Settings***（设置）选项中选择 ***Device Control Settings***（设备控制设置）。此时将显示 ***Device Control Settings***（设备控制设置）屏幕。
48. 单击 ***External Clients***（外部客户端）选项卡，然后取消选中以下选项：
    - ***Notification（通知）> Display a notification message on the client computer when OfficeScan detects unauthorized device access（当 OfficeScan 检测到未经授权的设备访问时在客户端计算机上显示通知消息）。***

- ***Block the AutoRun function on USB storage devices（阻止 USB 存储设备上的自动运行功能）。***
- ***Enable Device Control（启用设备控制）。***

49. 单击 ***Internal Clients***（内部客户端）选项卡，然后取消选中以下选项：
    - ***Notification（通知）> Display a notification message on the client computer when OfficeScan detects unauthorized device access（当 OfficeScan 检测到未经授权的设备访问时在客户端计算机上显示通知消息）。***
    - ***Block the AutoRun function on USB storage devices（阻止 USB 存储设备上的自动运行功能）。***
    - ***Enable Device Control（启用设备控制）。***
50. 单击 ***Apply to All Clients***（应用到所有客户端）。
51. 单击 ***Close***（关闭）以关闭 ***Device Control Settings***（设备控制设置）屏幕。
52. 在左侧窗格中选择 ***Networked Computers（联网的计算机）> Client Management（客户端管理）***链接。
53. 在右侧窗格中选择 ***OfficeScan Server***。
54. 从 ***Settings***（设置）选项中选择 ***Privileges and Other Settings***（权限和其他设置）。
55. 单击 ***Privileges***（权限）选项卡，然后只选择下列选项，取消选中其余的选项：
    - ***Scan Privileges（扫描权限）> Configure Manual Scan Settings（配置手动扫描设置）。***
    - ***Scan Privileges（扫描权限）> Configure Real-time Scan Settings（配置实时扫描设置）。***
    - ***Scan Privileges（扫描权限）> Configure Scheduled Scan Settings（配置计划扫描设置）。***
    - ***Proxy Setting Privileges（代理设置权限）> Allow the client user to configure proxy settings（允许客户端用户配置代理设置）。***
    - ***Uninstallation（卸载）> Require a password for the user to uninstall the OfficeScan Client（用户卸载 OfficeScan 客户端需要密码）。***输入合适的密码并确认密码。
    - ***Unloading（卸除）> Require a password for the user to unload the OfficeScan client（用户卸除 OfficeScan 客户端需要密码）。***输入合适的密码并确认密码。
56. 单击 ***Other Settings***（其他设置）选项卡。
57. 选择 ***Client Security Settings（客户端安全设置）> Normal（正常）***，然后取消选中其余选项。

注意： 必须清除以下选项。

- ***Client Self-protection（客户端自我保护）> Protect OfficeScan client services（保护 OfficeScan 客户端服务）。***
- ***Client Self-protection（客户端自我保护）> Protect files in the OfficeScan client installation folder（保护 OfficeScan 客户端安装文件夹中的文件）。***
- ***Client Self-protection（客户端自我保护）> Protect OfficeScan client registry keys（保护 OfficeScan 客户端注册表项）。***
- ***Client Self-protection（客户端自我保护）> Protect OfficeScan client processes（保护 OfficeScan 客户端流程）。***

58. 单击 ***Apply to All Clients***（应用到所有客户端）。

59. 单击 ***Close***（关闭）以关闭 ***Privileges and Other Settings***（权限和其他设置）屏幕。
60. 在左侧窗格中选择 ***Networked Computers（联网的计算机）> Client Management link（客户端管理链接）***。
61. 在右侧窗格中选择 ***OfficeScan Server***。
62. 从 ***Settings***（设置）选项中选择 ***Additional Service Settings***（其他服务设置）。
63. 取消选中 ***Enable service on the following operating systems***（在下列操作系统上启用服务）。
64. 单击 ***Apply to All Clients***（应用到所有客户端）。
65. 单击 ***Close***（关闭）以关闭 ***Additional Service Settings***（其他服务设置）屏幕。
66. 在左侧窗格中选择 ***Networked Computers（联网的计算机）> Global Client Settings link（全球客户端设置）***链接。
67. 仅选择以下选项并取消选中其余选项：
    - ***Scan Settings（扫描设置）> Configure Scan settings for large compressed files（为大型压缩文件配置扫描设置）***。
    - ***Scan Settings（扫描设置）> Do not scan files in the compressed file if the size exceeds 2 MB（不要扫描大小超过 2 MB 的压缩文件）***。
    - ***Scan Settings（扫描设置）> In a compressed file scan only the first 100 files（仅扫描压缩文件中的前 100 个文件）***。
    - ***Scan Settings（扫描设置）> Exclude the OfficeScan server database folder from Real-time Scan（将 OfficeScan 服务器数据库文件夹从实时扫描中排除）***。
    - ***Scan Settings（扫描设置）> Exclude Microsoft Exchange server folders and files from scans.（将 Microsoft Exchange 服务器文件夹从扫描中排除）***。
    - ***Reserved Disk Space（保留的磁盘空间）> Reserve 60 MB of disk space for updates（保留 60 MB 磁盘空间用于更新）***。
    - ***Proxy Configuration（代理配置）> Automatically detect settings（自动检测设置）***。

注意： 如果需要重新启动客户端计算机以加载核心驱动程序时，请务必取消选中 ***Alert Settings（警报设置）> Display a notification message if the client computer needs to restart to load a kernel driver（如果客户端计算机需要重新启动才能加载内核驱动程序则显示通知消息）***选项。

68. 单击 ***Save***（保存）。
69. 从左侧窗格中选择 ***Updates（更新）> Networked Computers（联网的计算机）> Manual Updates（手动更新）***链接。
70. 选择 ***Manually select client***（手动选择客户端），然后单击 ***Select***（选择）。
71. 在 ***OffceScan Server***（OffceScan 服务器）下，单击合适的域名。
72. 选择客户端系统（一次选择一个），然后单击 ***Initiate Component Update***（启动组件更新）。
73. 单击消息框中的 ***OK***（确定）。
74. 单击 ***Log off***（注销）并关闭 OfficeScan Web Console（OfficeScan Web 控制台）。

Trend Micro OfficeScan 安装后指南

1. 在采集系统上，执行下列步骤以配置 Trend Micro：
   a. 单击 ***Start（开始）> Control Panel （控制面板）> Network and Sharing Center（网络和共享中心）***。
   b. 单击***更改适配器设置***。
   c. 右键单击 ***Local Area Connection***（本地连接），然后选择 ***Properties***（属性）。
   d. 选择 ***Internet Protocol Version 4 (TCP/IPv4)***（Internet Protocol 版本 4 (TCP/IPv4)），然后单击 ***Properties***（属性）。
   e. 记录 IP 地址 _____。
   f. 关闭所有打开的窗口。
   g. 单击 ***Start（开始）> Run（运行）***，然后输入 **regedit**。
   h. 导航到 ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion***。
   i. 在右侧面板上，右键单击空白的位置，然后选择 ***New（新建）> String value（字符串值）***。
   j. 输入 **IP Template**（IP 模板）作为名称，然后按 **Enter** 键。
   k. 双击 ***IP Template***（IP 模板）注册表项。
   l. 在 ***Value***（值）数据字段中，输入在步骤 e 中记录的本地连接 IP 地址。
   m. 单击 ***OK***（确定）。
   n. 关闭注册表编辑器。
2. 启用环回连接。有关详细信息，请参阅启用环回连接（第 6 页）。
3. 配置 Computer Browser 服务。有关详细信息，请参阅在安装防病毒软件之后配置 Computer Browser 服务（第 7 页）。

Trend Micro 全局设置配置

注意： 仅当将 CO_2 功能与 Mac-Lab/CardioLab 系统中的 PDM 搭配使用时，才应该使用下面的说明。在继续执行下面的步骤之前，请确保您已与 IT 人员确认。

1. 在 防病毒 Management Console Server 上，导航到 ***C:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV*** 文件夹。
2. 在文本编辑器中打开 ***ofcscan.ini*** 文件。
3. 在 ***Global Setting***（全局设置）部分下，将下列注册表项的值设置为 "**1**"：
   [Global Setting] ***RmvTmTDI=1***
4. 保存并关闭 ofcscan.ini 文件。
5. 单击 ***Start（开始）> All Programs（所有程序）> TrendMicro OfficeScan server - <server name> > Office Scan Web Console（Office Scan Web 控制台）***。
6. 输入用户名和密码，然后单击 ***Log On***（登录）。此时将显示 ***Summary***（摘要）屏幕。

7. 单击 ***Networked Computers（联网的计算机）> Global Client Settings（全局客户端设置）***。
8. 单击 ***Save***（保存）。
9. 从左侧窗格中选择 ***Updates（更新）> Networked Computers（联网的计算机）> Manual Update（手动更新）***链接。
10. 选择 ***Manually select clients***（手动选择客户端），然后单击 ***Select***（选择）。
11. 在 ***OffceScan Server***（OffceScan 服务器）下，单击合适的域名。
12. 选择客户端系统（一次选择一个），然后单击 ***Initiate Component Update***（启动组件更新）。
13. 单击消息框中的 ***OK***（确定）。
14. 在每个采集系统上，执行以下操作：
    a. 打开注册表编辑器。
    b. 导航到 ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\Misc***。
    c. 确保 ***RmvTmTDI*** 注册表值设置为 "**1**"。
    d. 导航到 ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services***。
    e. 如果 ***tmtdi*** 注册表项存在，则将其删除。
    f. 关闭注册表编辑器。
    g. 重新启动客户端系统。
    h. 以管理员或管理员组成员身份登录客户端系统。
    i. 在每个客户端系统上，使用管理员权限打开命令提示符并输入以下命令：***sc query tmtdi***。
    j. 确保显示 ***The specified service does not exist as an installed service***（指定的服务不作为已安装的服务存在）消息。
15. 在 防病毒 Management Console 服务器上，单击 ***Log off***（注销）并关闭 OfficeScan Web Console（OfficeScan Web 控制台）。

Trend Micro OfficeScan Client/Server Edition 11.0 SP1

仅在联网的 Mac-Lab/CardioLab 环境中安装 Trend Micro OfficeScan Client/Server Edition。一定要先将 Trend Micro OfficeScan 安装在 防病毒 Management Console Server 中，然后再作为客户端部署至 Centricity Cardiology INW Server 和采集 / 回顾工作站。使用下面的说明来安装 ***Trend Micro OfficeScan Client/Server Edition 11.0 SP1***。

贵机构有责任升级防病毒软件。定期更新病毒定义，以确保系统上的病毒防护总是处于最新状态。

安装前指南

1. Trend Micro 防病毒 Management Console 应根据 Trend Micro 说明安装，并可以正常工作。

2. 在安装 Trend Micro OfficeScan 期间，请在 防病毒 Management Console Server 上执行以下操作：

   a. 在 ***防病毒 Feature***（防病毒功能）窗口中，取消选中 ***Enable firewall***（启用防火墙）。

   b. 在 ***Anti-spyware Feature***（防间谍软件功能）窗口中，选择 ***No, Please do not enable assessment mode***（否，不启用评估模式）。

   c. 在 ***Web Reputation Feature***（网络信誉功能）窗口中，取消选中 ***Enable web reputation policy***（启用网络信誉策略）。

3. 当将 CO_2 功能与 Mac-Lab/CardioLab 系统中的 PDM 搭配使用时，建议不要使用 Trend Micro OfficeScan。

4. 如果需要 Trend Micro OfficeScan：

   a. 建议为 Mac-Lab/CardioLab 系统配置一个独立的 Trend Micro 防病毒 Management Console Server。需要对防病毒设置进行全局更改，以便将 CO_2 功能与 Mac-Lab/CardioLab 系统中的 PDM 搭配使用。

   b. 如果不能配置独立的 Trend Micro 防病毒 Management Console Server，则需要在安装后对现有 Trend Micro 防病毒 Management Console Server 进行全局更改。此更改将影响已连接到现有 Trend Micro 防病毒 Management Console Server 的所有客户端系统，应该先通过 IT 人员审查再继续。

5. 在所有客户端系统（采集、回顾和 INW Server）上以**管理员**或管理员组成员的身份登录以安装防病毒软件。

6. 禁用环回连接。有关详细信息，请参阅禁用环回连接（第 6 页）。

7. 配置 Computer Browser 服务。有关详细信息，请参阅在安装防病毒软件之前配置 Computer Browser 服务（第 6 页）。

8. 在采集、回顾和 INW 客户端机器上安装需要下列根证书和中间证书：

   - AddTrustExternalCARoot.crt
   - COMODOCodeSigningCA2.crt
   - UTNAddTrustObject_CA.crt
   - UTN-USERFirst-Object.crt
   - UTN-USERFirst-Object_kmod.crt

9. 重复下列子步骤以安装步骤 8 中列出的 5 个必需的根证书和中间级别证书。

   a. 导航至 C***:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro***。
   注意：在 INW 上，导航至 C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro。

   b. 如果上述文件夹路径不存在，请手动获得安装所需的根证书和中间级别证书。

   c. 双击 ***AddTrustExternalCARoot.crt*** 以在 MLCL 系统（采集、回顾和 INW）上安装它。

   d. 打开该证书，然后单击 ***Install Certificate***（安装证书）。

   e. 出现 ***Certificate Import Wizard***（证书导入向导）时，单击 ***Next***（下一步）。

   f. 在 ***Certificate Store***（证书存储）窗口中，选择 ***Place all certificates in following store***（将所有证书放在下面的存储中），然后单击 ***Browse***（浏览）。

g. 选中 ***Show physical stores（显示物理存储）> Trusted Root Certification Authorities（可信的根证书颁发机构）> Local Computer（本地计算机）***，然后单击 ***OK***（确定）。

h. 在 ***Certificate Import Wizard***（证书导入向导）上，单击 ***Next***（下一步）。

i. 单击 ***Finish***（完成）。此时应会显示 ***The import was successful***（导入成功）消息。

j. 对步骤 8 列出的其他证书重复步骤 9。

注意： 每个证书都有一个到期日。证书到期之后，应该续订它们并在 MLCL 系统上更新，以确保 OfficeScan 代理程序按预期正常工作。

Trend Micro OfficeScan - 新安装部署步骤（11.0 SP1 的首选推送安装方法）

1. 单击 ***Start（开始）> All Programs（所有程序）> TrendMicro OfficeScan server - <server name> > Office Scan Web Console（Office Scan Web 控制台）***。

注意： 选择 ***Continue to this website (not recommended)***（继续此网站（不推荐）继续。在 Security Alert（安全警报）窗口中，选中 ***In the future, do not show this warning***（以后不再显示此警告），然后单击 ***OK***（确定）。

2. 如果您接收到整数错误，指出网站不可信，请管理您的证书以包括 Trend Micro OfficeScan。
3. 如果系统提示，请安装 ***AtxEnc*** 加载项。此时将显示 Security Warning（安全警告）屏幕。

   a. 单击 ***Install***（安装）。

4. 输入用户名和密码，然后单击 ***Log On***（登录）。
5. 如果系统提示，请单击 ***Update Now***（立即更新）以安装新的小组件。等待到新的小组件更新完毕。此时将显示更新已完成屏幕。

   a. 单击 ***OK***（确定）。

6. 从顶部菜单中，单击 ***Agents（代理程序）> Agent Installation（代理程序安装）> Remote（远程）***。
7. 如果系统提示，请安装 ***AtxConsole*** 加载项。此时将显示 Security Warning（安全警告）屏幕。

   a. 单击 ***Install***（安装）。

8. 在 ***Remote Installation***（远程安装）窗口中双击 ***OfficeScan Server***（OfficeScan 服务器）。所有域都将列出在 ***OfficeScan Server***（OfficeScan 服务器）下。
9. 双击域（示例：INW）。此时将显示已连接到域的所有系统。

注意： 如果域或系统未列出在 ***Domains and Endpoints***（域和端点）窗口中，请转至 对域和端点窗口中未列出的域或系统进行故障诊断（第 67 页）以手动添加它们，或者直接从客户端机器中运行安装。

10. 选择客户端机器（采集、回顾和 INW Server），然后单击 ***Add***（添加）。
11. 键入 < 域名 >\ 用户名和密码，然后单击 ***Log on***（登录）。
12. 从 ***Selected Endpoints***（已选择的端点）窗格中选择客户端机器（采集、回顾和 INW Server），然后单击 ***Install***（安装）。

13. 在确认窗口中单击 ***OK***（确定）。
14. 在 ***Number of clients to which notifications were sent***（已将通知发送给的客户端数目）消息框中，单击 ***OK***（确定）。
15. 重新启动所有客户端机器（采集、回顾和 INW Server）并在所有客户端计算机上以管理员或管理员组成员身份登录，并等待到系统托盘中的 Trend Micro OfficeScan 图标变成蓝色并显示绿色的勾号。
16. 单击 ***Log Off***（注销）链接以关闭 ***OfficeScan Web Console***（OfficeScan Web 控制台）。

11.0 SP1 的 Trend Micro OfficeScan 服务器控制台配置

1. 依次选择 ***Start（开始）> All Programs（所有程序）> TrendMicro Office Scan server <servername> > Office Scan Web Console（Office Scan Web 控制台）***。此时将显示 ***Trend Micro OfficeScan Login***（Trend Micro OfficeScan 登录）屏幕。
2. 输入用户名和密码，然后单击 ***Login***（登录）。此时将显示 ***Summary***（摘要）屏幕。
3. 从顶部窗格中，选择 ***Agents（代理程序）> Agent Management（代理程序管理）***链接。
4. 在左侧窗格中选择 ***OfficeScan Server***（OfficeScan 服务器）。
5. 从 ***Settings***（设置）选项中，选择 ***Scan Settings（扫描设置）> Manual Scan Settings（手动扫描设置）***。此时将显示 ***Manual Scan Settings***（手动扫描设置）屏幕。
6. 单击 ***Target***（目标）选项卡，然后只选择下列选项，取消选中其余的选项：
   - ***Files to Scan（要扫描的文件）> File types scanned by IntelliScan（由 IntelliScan 扫描的文件类型）。***
   - ***Scan Settings（扫描设置）> Scan compressed files（扫描压缩的文件）。***
   - ***Scan Settings（扫描设置）> Scan OLE objects（扫描 OLE 对象）。***
   - ***Virus/Malware Scan Settings Only（仅病毒 / 恶意软件扫描设置）> Scan boot area（扫描启动区）。***
   - ***CPU Usage（CPU 占用率）> Low（低）。***
7. 单击 Scan Exclusion（扫描排除）选项卡，然后只选择下列选项，取消选中其余的选项：
   - ***Scan Exclusion（扫描排除）> Enable scan exclusion（启用扫描排除）。***
   - ***Scan Exclusion（扫描排除）> Apply scan exclusion settings to all scan types（将扫描排除设置应用到所有扫描类型）。***
   - ***Scan Exclusion List (Directories)（扫描排除列表（目录））> Exclude directories where Trend Micro products are installed（排除 Trend Micro 产品的安装目录）。***
   - 从 ***Saving the officescan agent's exclusion list does the following:***（保存 officescan 代理程序的排除列表会执行以下操作：）下的下拉列表中选择 ***Adds path***（添加路径）。
   - 输入 **C:\Program Files (x86)\GE Healthcare\MLCL**、 **C:\Program Files\GE Healthcare\MLCL**、 **D:\GEData\Studies**、 **E:** 和 **G:** 文件夹（一次一个）并单击 **+**。
8. 单击 ***Apply to All Agents***（应用到所有代理程序）。
9. 显示以下消息时，单击 ***OK***（确定）：***The exclusion list on this screen will replace the exclusion list on the clients or domains you selected in the client tree earlier.Do you want to proceed?***（此屏幕上的排除列表将替换您先前在客户端树上选择的代理程序或域上的排除列表。是否要继续？）。
10. 单击 ***Close***（关闭）以关闭 ***Manual Scan Settings***（手动扫描设置）屏幕。

11. 从顶部窗格中，选择 ***Agent（代理程序）> Agent Management（代理程序管理）*** 链接。
12. 在左侧窗格中选择 ***OfficeScan Server***（OfficeScan 服务器）。
13. 在 ***Settings***（设置）选项中，依次选择 ***Scan Settings（扫描设置）> Real-time Scan Settings（实时扫描设置）***。此时将显示 ***Real-time Scan Settings***（实时扫描设置）屏幕。
14. 单击 ***Target***（目标）选项卡，然后只选择下列选项，取消选中其余的选项：
    - ***Real-Time Scan Settings（实时扫描设置）> Enable virus/malware scan（启用病毒 / 恶意软件扫描）。***
    - ***Real-Time Scan Settings（实时扫描设置）> Enable spyware/grayware scan（启用间谍软件 / 灰色软件扫描）。***
    - ***Files to Scan（要扫描的文件）> File types scanned by IntelliScan（由 IntelliScan 扫描的文件类型）。***
    - ***Scan Settings（扫描设置）> Scan compressed files（扫描压缩的文件）。***
    - ***Scan Settings（扫描设置）> Scan OLE objects（扫描 OLE 对象）。***
    - ***Virus/Malware Scan Settings Only（仅病毒 / 恶意软件扫描设置）> Enable IntelliTrap（启用 IntelliTrap）。***
15. 单击 Scan Exclusion（扫描排除）选项卡，然后只选择下列选项，取消选中其余的选项：
    - ***Scan Exclusion（扫描排除）> Enable scan exclusion（启用扫描排除）。***
    - ***Scan Exclusion（扫描排除）> Apply scan exclusion settings to all scan types（将扫描排除设置应用到所有扫描类型）。***
    - ***Scan Exclusion List (Directories)（扫描排除列表（目录））> Exclude directories where Trend Micro products are installed（排除 Trend Micro 产品的安装目录）。***
    - 确保 ***C:\Program Files (x86)\GE Healthcare\MLCL***， ***C:\Program Files \GE Healthcare\MLCL***、 ***D:\GEData\Studies***、 ***E:*** 和 ***G:*** 文件夹路径存在于 ***Exclusion List***（排除列表）中。
16. 单击 ***Action***（操作）选项卡。
17. 保留默认设置，然后取消选中以下选项：
    - ***Virus/Malware （病毒 / 恶意软件）> Display a notification message on endpoints when virus/malware is detected（检测到病毒 / 恶意软件时在端点上显示通知消息）。***
    - ***Spyware/Grayware（间谍软件 / 灰色软件）> Display a notification message on endpoints when spyware/grayware is detected（检测到间谍软件 / 灰色软件时在端点上显示通知消息）。***
18. 单击 ***Apply to All Agents***（应用到所有代理程序）。
19. 单击 ***Close***（关闭）以关闭 ***Real-time Scan Settings***（实时扫描设置）屏幕。
20. 从顶部窗格中，选择 ***Agents（代理程序）> Agent Management（代理程序管理）*** 链接。
21. 在左侧窗格中选择 ***OfficeScan Server***（OfficeScan 服务器）。
22. 从 ***Settings***（设置）选项中，依次选择 ***Scan Settings（扫描设置）> Scheduled Scan Settings（计划扫描设置）***。此时将显示 ***Scheduled Scan Settings***（计划扫描设置）屏幕。
23. 单击 ***Target***（目标）选项卡，然后只选择下列选项，取消选中其余的选项：
    - ***Scheduled Scan Settings（计划扫描设置）> Enable virus/malware scan（启用病毒 / 恶意软件扫描）。***

- ***Scheduled Scan Settings（计划扫描设置）> Enable virus/malware scan（启用间谍软件 / 灰色软件扫描）。***
- ***Schedule（计划）> Weekly（每周），每星期天， Start time（开始时间）：00:00 hh:mm。***
- ***Files to Scan（要扫描的文件）> File types scanned by IntelliScan（由 IntelliScan 扫描的文件类型）。***
- ***Scan Settings（扫描设置）> Scan compressed files（扫描压缩的文件）。***
- ***Scan Settings（扫描设置）> Scan OLE objects（扫描 OLE 对象）。***
- ***Virus/Malware Scan Settings Only（仅病毒 / 恶意软件扫描设置）> Scan boot area（扫描启动区）。***
- ***CPU Usage（CPU 占用率）> Low（低）。***

24. 单击 ***Scan Exclusion***（扫描排除）选项卡，然后只选择下列选项，取消选中其余的选项：
    - ***Scan Exclusion（扫描排除）> Enable scan exclusion（启用扫描排除）。***
    - ***Scan Exclusion（扫描排除）> Apply scan exclusion settings to all scan types（将扫描排除设置应用到所有扫描类型）。***
    - ***Scan Exclusion List (Directories)（扫描排除列表（目录））> Exclude directories where Trend Micro products are installed（排除 Trend Micro 产品的安装目录）。***
    - 确保 ***C:\Program Files (x86)\GE Healthcare\MLCL***、 ***C:\Program Files \GE Healthcare\MLCL***、 ***D:\GEData\Studies***、 ***E:*** 和 ***G:*** 文件夹路径存在于 Exclusion List（排除列表）中。
25. 单击 ***Action***（操作）选项卡。
26. 保留默认设置，然后取消选中以下选项：
    - ***Virus/Malware（病毒 / 恶意软件）> Display a notification message on the endpoints when virus/malware is detected（检测到病毒 / 恶意软件时在端点上显示通知消息）。***
    - ***Spyware/Grayware（间谍软件 / 灰色软件）> Display a notification message on the endpoints when spyware/grayware is detected（检测到间谍软件 / 灰色软件时在端点上显示通知消息）。***
27. 单击 ***Apply to All Agents***（应用到所有代理程序）。
28. 单击 ***Close***（关闭）以关闭 ***Scheduled Scan Settings***（计划扫描设置）屏幕。
29. 从顶部窗格中，选择 ***Agents（代理程序）> Agent Management（代理程序管理）*** 链接。
30. 在左侧窗格中选择 ***OfficeScan Server***（OfficeScan 服务器）。
31. 从 ***Settings***（设置）选项中，依次选择 ***Scan Settings（扫描设置）> Scan Now Settings（立即扫描设置）***。此时将显示 ***Scan Now Settings***（立即扫描设置）屏幕。
32. 单击 ***Target***（目标）选项卡，然后只选择下列选项，取消选中其余的选项：
    - ***Scan Now Settings（立即扫描设置）> Enable virus/malware scan（启用病毒 / 恶意软件扫描）。***
    - ***Scan Now Settings（立即扫描设置）> Enable virus/malware scan（启用病毒 / 恶意软件扫描）.***
    - ***Files to Scan（要扫描的文件）> File types scanned by IntelliScan（由 IntelliScan 扫描的文件类型）。***
    - ***Scan Settings（扫描设置）> Scan compressed files（扫描压缩的文件）。***
    - ***Scan Settings（扫描设置）> Scan OLE objects（扫描 OLE 对象）。***

- ***Virus/Malware Scan Settings Only（仅病毒 / 恶意软件扫描设置）> Scan boot area（扫描启动区）。***
- ***CPU Usage（CPU 占用率）> Low（低）。***

33. 单击 ***Scan Exclusion***（扫描排除）选项卡，然后只选择下列选项，取消选中其余的选项：
    - ***Scan Exclusion（扫描排除）> Enable scan exclusion（启用扫描排除）。***
    - ***Scan Exclusion（扫描排除）> Apply scan exclusion settings to all scan types（将扫描排除设置应用到所有扫描类型）。***
    - ***Scan Exclusion List (Directories)（扫描排除列表（目录））> Exclude directories where Trend Micro products are installed（排除 Trend Micro 产品的安装目录）。***
    - 确保 ***C:\Program Files (x86)\GE Healthcare\MLCL***、 ***C:\Program Files \GE Healthcare\MLCL***、 ***D:\GEData\Studies***、 ***E:*** 和 ***G:*** 文件夹路径存在于 Exclusion List（排除列表）中。
34. 单击 ***Apply to All Agents***（应用到所有代理程序）。
35. 单击 ***Close***（关闭）以关闭 ***Scan Now Settings***（立即扫描设置）屏幕。
36. 从顶部窗格中，选择 ***Agents（代理程序）> Agent Management（代理程序管理）***链接。
37. 在左侧窗格中选择 ***OfficeScan Server***（OfficeScan 服务器）。
38. 从 ***Settings***（设置）选项中选择 ***Web Reputation Settings***（网络信誉设置）。此时将显示 ***Web Reputation Settings***（网络信誉设置）屏幕。
39. 单击 ***External Agents***（外部代理程序）选项卡，然后取消选中 ***Enable Web reputation policy on the following operating systems***（在下列操作系统上启用网络信誉策略）（如果在安装期间已选中的话）。
40. 单击 ***Internal Agents***（内部代理程序）选项卡，然后取消选中 ***Enable Web reputation policy on the following operating systems***（在下列操作系统上启用网络信誉策略）（如果在安装期间已选中的话）。
41. 单击 ***Apply to All Agents***（应用到所有代理程序）。
42. 单击 ***Close***（关闭）以关闭 ***Web Reputation***（网络信誉）屏幕。
43. 从顶部窗格中，选择 ***Agents（代理程序）> Agent Management（代理程序管理）***链接。
44. 在左侧窗格中选择 ***OfficeScan Server***（OfficeScan 服务器）。
45. 从 ***Settings***（设置）选项中选择 ***Behavior Monitoring Settings***（行为监控设置）。此时将显示 ***Behavior Monitoring Settings***（行为监控设置）屏幕。
46. 取消选中 ***Enable Malware Behavior Blocking for known and potential threats***（针对已知和潜在的威胁启用恶意软件行为阻止）和 ***Enable Event Monitoring***（启用客户端监控）选项。
47. 单击 ***Apply to All Agents***（应用到所有代理程序）。
48. 单击 ***Close***（关闭）以关闭 ***Behavior Monitoring***（行为监控）屏幕。
49. 从顶部窗格中，选择 ***Agents（代理程序）> Agent Management（代理程序管理）***链接。
50. 在左侧窗格中选择 ***OfficeScan Server***（OfficeScan 服务器）。
51. 从 ***Settings***（设置）选项中选择 ***Device Control Settings***（设备控制设置）。此时将显示 ***Device Control Settings***（设备控制设置）屏幕。
52. 单击 ***External Agents***（外部代理程序）选项卡，然后取消选中以下选项：

- ***Notification（通知）> Display a notification message on endpoints when OfficeScan detects unauthorized device access（当 OfficeScan 检测到未经授权的设备访问时在端点上显示通知消息）。***
- ***Block the AutoRun function on USB storage devices（阻止 USB 存储设备上的自动运行功能）。***

53. 单击 ***Internal Agents***（内部代理程序）选项卡，然后取消选中以下选项：
    - ***Notification（通知）> Display a notification message on endpoints when OfficeScan detects unauthorized device access（当 OfficeScan 检测到未经授权的设备访问时在端点上显示通知消息）。***
    - ***Block the AutoRun function on USB storage devices（阻止 USB 存储设备上的自动运行功能）。***
54. 单击 ***Apply to All Agents***（应用到所有代理程序）。
55. 单击 ***Close***（关闭）以关闭 ***Device Control Settings***（设备控制设置）屏幕。
56. 从 ***Settings***（设置）选项中选择 ***Device Control Settings***（设备控制设置）。此时将显示 ***Device Control Settings***（设备控制设置）屏幕。
57. 单击 ***External Agents***（外部代理程序）选项卡，然后取消选中 ***Enable Device Control***（启用设备控制）。
58. 单击 ***Internal Agents***（内部代理程序）选项卡，然后取消选中 ***Enable Device Control***（启用设备控制）。
59. 单击 ***Apply to All Agents***（应用到所有代理程序）。
60. 单击 ***Close***（关闭）以关闭 ***Device Control Settings***（设备控制设置）屏幕。
61. 从顶部窗格中，选择 ***Agents（代理程序）> Agent Management（代理程序管理）***链接。
62. 在左侧窗格中选择 ***OfficeScan Server***（OfficeScan 服务器）。
63. 从 ***Settings***（设置）选项中选择 ***Privileges and Other Settings***（权限和其他设置）。
64. 单击 ***Privileges***（权限）选项卡，然后只选择下列选项，取消选中其余的选项：
    - ***Scans（扫描）> Configure Manual Scan Settings（配置手动扫描设置）。***
    - ***Scan（扫描）> Configure Real-time Scan Settings（配置实时扫描设置）。***
    - ***Scan（扫描）> Configure Scheduled Scan Settings.（配置计划扫描设置）。***
    - ***Proxy Settings（代理设置）> Allow users to configure proxy settings（允许用户配置代理设置）。***
    - ***Uninstallation（卸载）> Requires a password（需要密码）。***输入合适的密码并确认密码。
    - ***Unloading and Unlock（卸载和解锁）> Requires a password（需要密码）。***输入合适的密码并确认密码。
65. 单击 ***Other Settings***（其他设置）选项卡。
66. 选择 ***OfficeScan Agent Security Settings（OfficeScan 代理程序安全设置）> Normal: Allow users to access OfficeScan agent files and registries***（正常：允许用户访问 OfficeScan 代理程序文件和注册表），然后取消选中其余选项。

注意： 必须清除以下选项。

- ***OfficeScan Agent Self-protection（OfficeScan 代理程序自我保护）> Protect OfficeScan agent services.（保护 OfficeScan 代理程序服务）。***

- ***OfficeScan Agent Self-protection（OfficeScan 代理程序自我保护）> Protect files in the OfficeScan agent installation folder（保护 OfficeScan 代理程序安装目录中的文件）。***
- ***OfficeScan Agent Self-protection（OfficeScan 代理程序自我保护）> Protect OfficeScan agent registry keys（保护 OfficeScan 代理程序注册表项）。***
- ***OfficeScan Agent Self-protection（OfficeScan 代理程序自我保护）> Protect OfficeScan agent processes（保护 OfficeScan 代理程序流程）。***

67. 单击 ***Apply to All Agents***（应用到所有代理程序）。
68. 单击 ***Close***（关闭）以关闭 ***Privileges and Other Settings***（权限和其他设置）屏幕。
69. 从顶部窗格中，选择 ***Agents（代理程序）> Agent Management（代理程序管理）***链接。
70. 在左侧窗格中选择 ***OfficeScan Server***（OfficeScan 服务器）。
71. 从 ***Settings***（设置）选项中选择 ***Additional Service Settings***（其他服务设置）。
72. 取消选中 ***Enable service on the following operating systems***（在下列操作系统上启用服务）。
73. 单击 ***Apply to All Agents***（应用到所有代理程序）。
74. 单击 ***Close***（关闭）以关闭 ***Additional Service Settings***（其他服务设置）屏幕。
75. 从顶部窗格中，选择 ***Agent（代理程序）> Global Agent Settings（全局代理程序设置）***链接。
76. 仅选择以下选项并取消选中其余选项：
    - ***Scan Settings for Large Compressed Files（大型压缩文件的扫描设置）> Configure Scan settings for large compressed files（为大型压缩文件配置扫描设置）。***
    - ***Scan Settings for Large Compressed Files（大型压缩文件的扫描设置）> Do not scan files in the compressed file if the size exceeds 2 Mb（如果压缩文件大小超过 2 MB，则不扫描压缩文件中的文件）。***针对 ***Real-Time Scan***（实时扫描）和 ***Manual Scan/Schedule Scan/Scan Now（手动扫描 / 计划扫描 / 立即扫描）***使用本信息。
    - ***Scan Settings for Large Compressed Files（大型压缩文件的扫描设置）> In a compressed file scan only the first 100 files（仅扫描压缩文件中的前 100 个文件）。***针对 ***Real-Time Scan***（实时扫描）和 ***Manual Scan/Schedule Scan/Scan Now（手动扫描 / 计划扫描 / 立即扫描）***使用本信息。
    - ***Scan Settings（扫描设置）> Exclude the OfficeScan server database folder from Real-time Scan（将 OfficeScan 服务器数据库文件夹从实时扫描中排除）。***
    - ***Scan Settings（扫描设置）> Exclude Microsoft Exchange server folders and files from scans.（将 Microsoft Exchange 服务器文件夹从扫描中排除）。***
    - ***Reserved Disk Space（保留的磁盘空间）> Reserve 60 MB of disk space for updates（保留 60 MB 磁盘空间用于更新）。***
    - ***Proxy Configuration（代理配置）> Automatically detect settings（自动检测设置）。***

注意： 如果需要重新启动端点以加载内核模式程序，请务必清除 ***Alert Settings（警报设置）> Display a notification message（显示通知消息）***选项。

77. 单击 ***Save***（保存）。
78. 从顶部窗格中，选择 ***Updates（更新）> Agents（代理程序）> Manual Updates（手动更新）***链接。
79. 选择 ***Manually select agents***（手动选择代理程序），然后单击 ***Select***（选择）。

80. 在 ***OffceScan Server***（OffceScan 服务器）下，双击合适的域名。
81. 选择客户端系统（一次选择一个），然后单击 ***Initiate Update***（启动更新）。
82. 单击消息框中的 ***OK***（确定）。
83. 单击 ***Log off***（注销）并关闭 OfficeScan Web Console（OfficeScan Web 控制台）。

Trend Micro 全局设置配置

注意：仅当将 CO_2 功能与 Mac-Lab/CardioLab 系统中的 PDM 搭配使用时，才应该使用下面的说明。在继续执行下面的步骤之前，请确保您已与 IT 人员确认。

1. 在 防病毒 Management Console Server 上，导航到 ***C:\Program Files (x86)\Trend Micro\OfficeScan\PCCSRV*** 文件夹。
2. 在文本编辑器中打开 ***ofcscan.ini*** 文件。
3. 在 Global Setting（全局设置）部分下，将下列注册表项的值设置为 "**1**"：[Global Setting] ***RmvTmTDI=1***
4. 保存并关闭 ofcscan.ini 文件。
5. 单击 ***Start（开始）> All Programs（所有程序）> TrendMicro OfficeScan server - <server name> > OfficeScan Web Console（OfficeScan 网络控制台）***。
6. 输入相应的用户名和密码，然后单击 ***Log On***（登录）。此时将显示 ***Dashboard***（下载）屏幕。
7. 单击 ***Agents（代理程序）> Global Agent Settings（全局代理程序设置）***。
8. 单击 ***Save（保存）***。
9. 从左侧窗格中选择 ***Updates（更新）> Agents（代理程序）> Manual Update（手动更新）*** 链接。
10. 选择 ***Manually select clients***（手动选择客户端），然后单击 ***Select***（选择）。
11. 在 ***OfficeScan Server***（OffceScan 服务器）下，单击合适的域名。
12. 选择客户端系统（一次选择一个），然后单击 ***Initiate Update***（启动更新）。
13. 单击消息框中的 ***OK***（确定）。
14. 在每个采集系统上，执行以下操作：
    a. 打开注册表编辑器。
    b. 导航至 ***HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PCcillinNTCorp\CurrentVersion\Misc***。
    c. 确保 ***RmvTmTDI*** 注册表值设置为 "***1***"。
    d. 导航到 ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services***。
    e. 如果 ***tmtdi*** 注册表项存在，则将其删除。
    f. 关闭注册表编辑器。
    g. 重新启动客户端系统。

h. 以管理员或管理员组成员身份登录客户端系统。

i. 在每个客户端系统上，使用管理员权限打开命令提示符并输入以下命令：***sc query tmtdi***。

j. 确保显示 ***The specified service does not exist as an installed service***（指定的服务不作为已安装的服务存在）消息。

15. 在 防病毒 Management Console 服务器上，单击 ***Log off***（注销）并关闭 OfficeScan Web Console（OfficeScan Web 控制台）。

Trend Micro OfficeScan 安装后指南

1. 启用环回连接。有关详细信息，请参阅启用环回连接（第 6 页）。
2. 配置 Computer Browser 服务。有关详细信息，请参阅在安装防病毒软件之后配置 Computer Browser 服务（第 7 页）。

Trend Micro OfficeScan Client/Server Edition XG 12.0

安装概述

仅在联网的 Mac-Lab/CardioLab 环境中安装 Trend Micro OfficeScan Client/Server Edition。一定要先将 Trend Micro OfficeScan 安装在 防病毒 Management Console Server 中，然后再作为客户端部署至 Centricity Cardiology INW Server 和采集 / 回顾工作站。使用下面的说明来安装 ***Trend Micro OfficeScan Client/Server Edition XG 12.0***。

贵机构有责任升级防病毒软件。定期更新病毒定义，以确保系统上的病毒防护总是处于最新状态。

安装前指南

注意： Internet Explorer 10 是运行 OfficeScan 管理器的最低要求。

1. Trend Micro 防病毒 Management Console 应根据 Trend Micro 说明安装，并可以正常工作。
2. 在安装 Trend Micro OfficeScan 期间，请在 防病毒 Management Console Server 上执行以下操作：

   a. 在 ***防病毒 Feature***（防病毒功能）窗口中，取消选中 ***Enable firewall***（启用防火墙）。

   b. 在 ***Anti-spyware Feature***（防间谍软件功能）窗口中，选择 ***No, Please do not enable assessment mode***（否，不启用评估模式）。

   c. 在 ***Web Reputation Feature***（网络信誉功能）窗口中，取消选中 ***Enable web reputation policy***（启用网络信誉策略）。

3. 在所有客户端系统（采集、回顾和 INW Server）上以**管理员**或管理员组成员的身份登录以安装防病毒软件。
4. 禁用环回连接。有关详细信息，请参阅禁用环回连接（第 6 页）。
5. 配置 Computer Browser 服务。有关详细信息，请参阅在安装防病毒软件之前配置 Computer Browser 服务（第 6 页）。
6. 在采集、回顾和 INW 客户端机器上安装需要下列根证书和中间证书：

- AddTrustExternalCARoot.crt
- COMODOCodeSigningCA2.crt
- UTNAddTrustObject_CA.crt
- UTN-USERFirst-Object.crt
- UTN-USERFirst-Object_kmod.crt

7. 重复下列子步骤以安装步骤 6 中列出的 5 个必需的根证书和中间级别证书。

   a. 导航至 C***:\Program Files\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro***。
   注意：在 INW 上，导航至 C:\Program Files (x86)\GE Healthcare\MLCL\Special\ThirdPartyUtilities\Trend Micro。

   b. 如果上述文件夹路径不存在，请手动获得安装所需的根证书和中间级别证书。

   c. 双击 ***AddTrustExternalCARoot.crt*** 以在 MLCL 系统（采集、回顾和 INW）上安装它。

   d. 打开该证书，然后单击 ***Install Certificate***（安装证书）。

   e. 出现 ***Certificate Import Wizard***（证书导入向导）时，单击 ***Next***（下一步）。

   f. 在 ***Certificate Store***（证书存储）窗口中，选择 ***Place all certificates in following store***（将所有证书放在下面的存储中），然后单击 ***Browse***（浏览）。

   g. 选中 ***Show physical stores（显示物理存储）> Trusted Root Certification Authorities（可信的根证书颁发机构）> Local Computer（本地计算机）***，然后单击 ***OK***（确定）。

   h. 在 ***Certificate Import Wizard***（证书导入向导）上，单击 ***Next***（下一步）。

   i. 单击 ***Finish***（完成）。此时应会显示 ***The import was successful***（导入成功）消息。

   j. 对步骤 6 列出的其他证书重复步骤 7。

注意： 每个证书都有一个到期日。证书到期之后，应该续订它们并在 MLCL 系统上更新，以确保 OfficeScan 代理程序按预期正常工作。

Trend Micro OfficeScan - 新安装部署步骤（12.0 的首选推送安装方法）

1. 单击 ***Start（开始）> All Programs（所有程序）> TrendMicro OfficeScan server - <server name> > Office Scan Web Console（Office Scan Web 控制台）***。

注意： 选择 ***Continue to this website (not recommended)***（继续此网站（不推荐）继续。在 Security Alert（安全警报）窗口中，选中 ***In the future, do not show this warning***（以后不再显示此警告），然后单击 ***OK***（确定）。

2. 如果您接收到整数错误，指出网站不可信，请管理您的证书以包括 Trend Micro OfficeScan。

3. 如果系统提示，请安装 ***AtxEnc*** 加载项。此时将显示 Security Warning（安全警告）屏幕。

   a. 单击 ***Install***（安装）。

4. 输入用户名和密码，然后单击 ***Log On***（登录）。

5. 如果系统提示，请单击 ***Update Now***（立即更新）以安装新的小组件。等待到新的小组件更新完毕。此时将显示更新已完成屏幕。

a. 单击 ***OK***（确定）。

6. 从顶部菜单中，单击 ***Agents（代理程序）> Agent Installation（代理程序安装）> Remote（远程）***。
7. 如果系统提示，请安装 ***AtxConsole*** 加载项。此时将显示 Security Warning（安全警告）屏幕。

   a. 单击 ***Install***（安装）。

8. 在 ***Remote Installation***（远程安装）窗口中，双击 ***My Company***（我的公司）。所有域都将列出在 ***OfficeScan Server***（OfficeScan 服务器）下。
9. 双击域（示例：INW）。此时将显示已连接到域的所有系统。

注意： 如果域或系统未列出在 ***Domains and Endpoints***（域和端点）窗口中，请转至 对域和端点窗口中未列出的域或系统进行故障诊断（第 67 页）以手动添加它们，或者直接从客户端机器中运行安装。

10. 选择客户端机器（采集、回顾和 INW Server），然后单击 ***Add***（添加）。
11. 键入 < 域名 >\ 用户名和密码，然后单击 ***Log on***（登录）。
12. 从 ***Selected Endpoints***（已选择的端点）窗格中选择客户端机器（采集、回顾和 INW Server），然后单击 ***Install***（安装）。
13. 在确认框中单击 ***Yes***（是）。
14. 在 ***Number of clients to which notifications were sent***（已将通知发送给的端点数目）消息框中，单击 ***OK***（确定）。
15. 重新启动所有客户端机器（采集、回顾和 INW Server）并在所有客户端计算机上以管理员或管理员组成员身份登录，并等待到系统托盘中的 Trend Micro OfficeScan 图标变成蓝色并显示绿色的勾号。
16. 单击 ***Log Off***（注销）链接以关闭 ***OfficeScan Web Console***（OfficeScan Web 控制台）。

12.0 的 Trend Micro OfficeScan 服务器控制台配置

1. 依次选择 ***Start（开始）> All Programs（所有程序）> TrendMicro Office Scan server <servername> > Office Scan Web Console（Office Scan Web 控制台）***。此时将显示 ***Trend Micro OfficeScan Login***（Trend Micro OfficeScan 登录）屏幕。
2. 输入用户名和密码，然后单击 ***Login***（登录）。此时将显示 ***Summary***（摘要）屏幕。
3. 从顶部窗格中，选择 ***Agents（代理程序）> Agent Management（代理程序管理）***链接。
4. 在左侧窗格中选择 ***OfficeScan Server***（OfficeScan 服务器）。
5. 从 ***Settings***（设置）选项中，选择 ***Scan Settings（扫描设置）> Manual Scan Settings（手动扫描设置）***。此时将显示 ***Manual Scan Settings***（手动扫描设置）屏幕。
6. 单击 ***Target***（目标）选项卡，然后只选择下列选项，取消选中其余的选项：
   - ***Files to Scan（要扫描的文件）> File types scanned by IntelliScan（由 IntelliScan 扫描的文件类型）。***
   - ***Scan Settings（扫描设置）> Scan compressed files（扫描压缩的文件）。***
   - ***Scan Settings（扫描设置）> Scan OLE objects（扫描 OLE 对象）。***

- ***Virus/Malware Scan Settings Only（仅病毒 / 恶意软件扫描设置）> Scan boot area（扫描启动区）。***
- ***CPU Usage（CPU 占用率）> Low（低）。***

7. 单击 Scan Exclusion（扫描排除）选项卡，然后只选择下列选项，取消选中其余的选项：
   - ***Scan Exclusion（扫描排除）> Enable scan exclusion（启用扫描排除）。***
   - ***Scan Exclusion（扫描排除）> Apply scan exclusion settings to all scan types（将扫描排除设置应用到所有扫描类型）。***
   - ***Scan Exclusion List (Directories)（扫描排除列表（目录））> Exclude directories where Trend Micro products are installed and select Add path to agent Computers Exclusion list.（排除 Trend Micro 产品安装目录并选择将路径添加到代理程序计算机排除列表）。***
   - 从 ***Saving the officescan agent's exclusion list does the following:***（保存 officescan 代理程序的排除列表会执行以下操作：）下的下拉列表中选择 ***Adds path***（添加路径）。
   - 输入 **C:\Program Files (x86)\GE Healthcare\MLCL**、 **C:\Program Files\GE Healthcare\MLCL**、 **D:\GEData\Studies**、 **E:** 和 **G:** 文件夹（一次一个）并单击 ***Add***（添加）。
8. 单击 ***Apply to All Agents***（应用到所有代理程序）。
9. 显示以下消息时，单击 ***OK***（确定）：***The exclusion list on this screen will replace the exclusion list on the agents or domains you selected in the client tree earlier.Do you want to proceed?***（此屏幕上的排除列表将替换您先前在客户端树上选择的代理程序或域上的排除列表。是否要继续？）。
10. 单击 ***Close***（关闭）以关闭 ***Manual Scan Settings***（手动扫描设置）屏幕。
11. 从顶部窗格中，选择 ***Agent（代理程序）> Agent Management（代理程序管理）***链接。
12. 在左侧窗格中选择 ***OfficeScan Server***（OfficeScan 服务器）。
13. 在 ***Settings***（设置）选项中，依次选择 ***Scan Settings（扫描设置）> Real-time Scan Settings（实时扫描设置）***。此时将显示 ***Real-time Scan Settings***（实时扫描设置）屏幕。
14. 单击 ***Target***（目标）选项卡，然后只选择下列选项，取消选中其余的选项：
    - ***Real-Time Scan Settings（实时扫描设置）> Enable virus/malware scan（启用病毒 / 恶意软件扫描）。***
    - ***Real-Time Scan Settings（实时扫描设置）> Enable spyware/grayware scan（启用间谍软件 / 灰色软件扫描）。***
    - ***Files to Scan（要扫描的文件）> File types scanned by IntelliScan（由 IntelliScan 扫描的文件类型）。***
    - ***Scan Settings（扫描设置）> Scan compressed files（扫描压缩的文件）。***
    - ***Scan Settings（扫描设置）> Scan OLE objects（扫描 OLE 对象）。***
    - ***Virus/Malware Scan Settings Only（仅病毒 / 恶意软件扫描设置）> Enable IntelliTrap（启用 IntelliTrap）。***
15. 单击 Scan Exclusion（扫描排除）选项卡，然后只选择下列选项，取消选中其余的选项：
    - ***Scan Exclusion（扫描排除）> Enable scan exclusion（启用扫描排除）。***
    - ***Scan Exclusion（扫描排除）> Apply scan exclusion settings to all scan types（将扫描排除设置应用到所有扫描类型）。***
    - ***Scan Exclusion List (Directories)（扫描排除列表（目录））> Exclude directories where Trend Micro products are installed（排除 Trend Micro 产品的安装目录）。***

- 确保 ***C:\Program Files (x86)\GE Healthcare\MLCL***， ***C:\Program Files \GE Healthcare\MLCL***、 ***D:\GEData\Studies***、 ***E:*** 和 ***G:*** 文件夹路径存在于 ***Exclusion List***（排除列表）中。

16. 单击 ***Action***（操作）选项卡。
17. 保留默认设置，然后取消选中以下选项：
    - ***Virus/Malware （病毒 / 恶意软件）> Display a notification message on endpoints when virus/malware is detected（检测到病毒 / 恶意软件时在端点上显示通知消息）。***
    - ***Spyware/Grayware（间谍软件 / 灰色软件）> Display a notification message on endpoints when spyware/grayware is detected（检测到间谍软件 / 灰色软件时在端点上显示通知消息）。***
18. 单击 ***Apply to All Agents***（应用到所有代理程序）。
19. 单击 ***Close***（关闭）以关闭 ***Real-time Scan Settings***（实时扫描设置）屏幕。
20. 从顶部窗格中，选择 ***Agents（代理程序）> Agent Management（代理程序管理）***链接。
21. 在左侧窗格中选择 ***OfficeScan Server***（OfficeScan 服务器）。
22. 从 ***Settings***（设置）选项中，依次选择 ***Scan Settings（扫描设置）> Scheduled Scan Settings（计划扫描设置）***。此时将显示 ***Scheduled Scan Settings***（计划扫描设置）屏幕。
23. 单击 ***Target***（目标）选项卡，然后只选择下列选项，取消选中其余的选项：
    - ***Scheduled Scan Settings（计划扫描设置）> Enable virus/malware scan（启用病毒 / 恶意软件扫描）。***
    - ***Scheduled Scan Settings（计划扫描设置）> Enable virus/malware scan（启用间谍软件 / 灰色软件扫描）。***
    - ***Schedule（计划）> Weekly（每周），每星期天， Start time（开始时间）: 00:00 hh:mm。***
    - ***Files to Scan（要扫描的文件）> File types scanned by IntelliScan（由 IntelliScan 扫描的文件类型）。***
    - ***Scan Settings（扫描设置）> Scan compressed files（扫描压缩的文件）。***
    - ***Scan Settings（扫描设置）> Scan OLE objects（扫描 OLE 对象）。***
    - ***Virus/Malware Scan Settings Only（仅病毒 / 恶意软件扫描设置）> Scan boot area（扫描启动区）。***
    - ***CPU Usage（CPU 占用率）> Low（低）。***
24. 单击 Scan Exclusion（扫描排除）选项卡，然后只选择下列选项，取消选中其余的选项：
    - ***Scan Exclusion（扫描排除）> Enable scan exclusion（启用扫描排除）。***
    - ***Scan Exclusion（扫描排除）> Apply scan exclusion settings to all scan types（将扫描排除设置应用到所有扫描类型）。***
    - ***Scan Exclusion List (Directories)（扫描排除列表（目录））> Exclude directories where Trend Micro products are installed（排除 Trend Micro 产品的安装目录）。***
    - 确保 ***C:\Program Files (x86)\GE Healthcare\MLCL***、 ***C:\Program Files \GE Healthcare\MLCL***、 ***D:\GEData\Studies***、 ***E:*** 和 ***G:*** 文件夹路径存在于 Exclusion List（排除列表）中。
25. 单击 ***Action***（操作）选项卡。
26. 保留默认设置，然后取消选中以下选项：

- ***Virus/Malware（病毒 / 恶意软件)> Display a notification message on the endpoints when virus/malware is detected（检测到病毒 / 恶意软件时在端点上显示通知消息)。***
- ***Spyware/Grayware（间谍软件 / 灰色软件 ）> Display a notification message on the endpoints when spyware/grayware is detected（检测到间谍软件 / 灰色软件时在端点上显示通知消息)。***

27. 单击 ***Apply to All Agents***（应用到所有代理程序)。
28. 单击 ***Close***（关闭 ）以关闭 ***Scheduled Scan Settings***（计划扫描设置 ）屏幕。
29. 从顶部窗格中，选择 ***Agents（代理程序 ）> Agent Management（代理程序管理)*** 链接。
30. 在左侧窗格中选择 ***OfficeScan Server***（OfficeScan 服务器)。
31. 从 ***Settings***（设置 ）选项中，依次选择 ***Scan Settings（扫描设置 ）> Scan Now Settings（立即扫描设置)***。此时将显示 ***Scan Now Settings***（立即扫描设置 ）屏幕。
32. 单击 ***Target***（目标 ）选项卡，然后只选择下列选项，取消选中其余的选项：
    - ***Scan Now Settings（立即扫描设置 ）> Enable virus/malware scan（启用病毒 / 恶意软件扫描)。***
    - ***Scan Now Settings（立即扫描设置 ）> Enable virus/malware scan（启用病毒 / 恶意软件扫描 ）.***
    - ***Files to Scan（要扫描的文件 ）> File types scanned by IntelliScan（由 IntelliScan 扫描的文件类型)。***
    - ***Scan Settings（扫描设置 ）> Scan compressed files（扫描压缩的文件)。***
    - ***Scan Settings（扫描设置 ）> Scan OLE objects（扫描 OLE 对象)。***
    - ***Virus/Malware Scan Settings Only（仅病毒 / 恶意软件扫描设置 ）> Scan boot area（扫描启动区)。***
    - ***CPU Usage（CPU 占用率 ）> Low（低)。***
33. 单击 ***Scan Exclusion***（扫描排除 ）选项卡，然后只选择下列选项，取消选中其余的选项：
    - ***Scan Exclusion（扫描排除 ）> Enable scan exclusion（启用扫描排除)。***
    - ***Scan Exclusion（扫描排除 ）> Apply scan exclusion settings to all scan types（将扫描排除设置应用到所有扫描类型)。***
    - ***Scan Exclusion List (Directories)（扫描排除列表（目录 ））> Exclude directories where Trend Micro products are installed（排除 Trend Micro 产品的安装目录)。***
    - 确保 ***C:\Program Files (x86)\GE Healthcare\MLCL***、 ***C:\Program Files \GE Healthcare\MLCL***、 ***D:\GEData\Studies***、 ***E:*** 和 ***G:***
34. 单击 ***Apply to All Agents***（应用到所有代理程序)。
35. 单击 ***Close***（关闭 ）以关闭 ***Scan Now Settings***（立即扫描设置 ）屏幕。
36. 从顶部窗格中，选择 ***Agents（代理程序 ）> Agent Management（代理程序管理)*** 链接。
37. 在左侧窗格中选择 ***OfficeScan Server***（OfficeScan 服务器)。
38. 从 ***Settings***（设置 ）选项中选择 ***Web Reputation Settings***（网络信誉设置)。此时将显示 ***Web Reputation Settings***（网络信誉设置 ）屏幕。
39. 单击 ***External Clients***（外部客户端 ）选项卡，然后取消选中 ***Enable Web reputation policy on the following operating systems***（在下列操作系统上启用网络信誉策略)（如果在安装期间已选中的话)。

40. 单击 ***Internal Agents***（内部代理程序）选项卡，然后取消选中 ***Enable Web reputation policy on the following operating systems***（在下列操作系统上启用网络信誉策略）（如果在安装期间已选中的话）。
41. 单击 ***Apply to All Agents***（应用到所有代理程序）。
42. 单击 ***Close***（关闭）以关闭 ***Web Reputation***（网络信誉）屏幕。
43. 从顶部窗格中，选择 ***Agents（代理程序）> Agent Management（代理程序管理）***链接。
44. 在左侧窗格中选择 ***OfficeScan Server***（OfficeScan 服务器）。
45. 从 ***Settings***（设置）选项中选择 ***Behavior Monitoring Settings***（行为监控设置）。此时将显示 ***Behavior Monitoring Settings***（行为监控设置）屏幕。
46. 取消选中 ***Enable Malware Behavior Blocking***（启用恶意软件行为组织）和 ***Enable Event Monitoring***（启用事件监控）选项。
47. 单击 ***Apply to All Agents***（应用到所有代理程序）。
48. 单击 ***Close***（关闭）以关闭 ***Behavior Monitoring***（行为监控）屏幕。
49. 从顶部窗格中，选择 ***Agents（代理程序）> Agent Management（代理程序管理）***链接。
50. 在左侧窗格中选择 ***OfficeScan Server***（OfficeScan 服务器）。
51. 从 ***Settings***（设置）选项中选择 ***Device Control Settings***（设备控制设置）。此时将显示 ***Device Control Settings***（设备控制设置）屏幕。
52. 单击 ***External Agents***（外部代理程序）选项卡，然后取消选中以下选项：
    - ***Notification（通知）> Display a notification message on endpoints when OfficeScan detects unauthorized device access（当 OfficeScan 检测到未经授权的设备访问时在端点上显示通知消息）。***
    - ***Block the AutoRun function on USB storage devices（阻止 USB 存储设备上的自动运行功能）。***
    - ***Enable Device Control（启用设备控制）。***
53. 单击 ***Internal Agents***（内部代理程序）选项卡，然后取消选中以下选项：
    - ***Notification（通知）> Display a notification message on endpoints when OfficeScan detects unauthorized device access（当 OfficeScan 检测到未经授权的设备访问时在端点上显示通知消息）。***
    - ***Block the AutoRun function on USB storage devices（阻止 USB 存储设备上的自动运行功能）。***
    - ***Enable Device Control（启用设备控制）。***
54. 单击 ***Apply to All Agents***（应用到所有代理程序）。
55. 单击 ***Close***（关闭）以关闭 ***Device Control Settings***（设备控制设置）屏幕。
56. 从 ***Settings***（设置）选项中选择 ***Device Control Settings***（设备控制设置）。此时将显示 ***Device Control Settings***（设备控制设置）屏幕。
57. 单击 ***External Agents***（外部代理程序）选项卡，然后取消选中 ***Enable Device Control***（启用设备控制）。
58. 单击 ***Internal Agents***（内部代理程序）选项卡，然后取消选中 ***Enable Device Control***（启用设备控制）。
59. 单击 ***Apply to All Agents***（应用到所有代理程序）。

60. 单击 ***Close***（关闭）以关闭 ***Device Control Settings***（设备控制设置）屏幕。
61. 在左侧窗格中选择 ***Agents（代理程序）> Agent Management（代理程序管理）***链接。
62. 在左侧窗格中选择 ***OfficeScan Server***（OfficeScan 服务器）。
63. 从 ***Settings***（设置）选项中选择 ***Privileges and Other Settings***（权限和其他设置）。
64. 单击 ***Privileges***（权限）选项卡，然后只选择下列选项，取消选中其余的选项：
    - ***Scan Privileges（扫描权限）> Configure Manual Scan Settings（配置手动扫描设置）。***
    - ***Scan Privileges（扫描权限）> Configure Real-time Scan Settings（配置实时扫描设置）。***
    - ***Scan Privileges（扫描权限）> Configure Scheduled Scan Settings（配置计划扫描设置）。***
    - ***Proxy Setting Privileges（代理设置权限）> Allow the client user to configure proxy settings（允许客户端用户配置代理设置）。***
    - ***Uninstallation（卸载）> Requires a password（需要密码）。***输入合适的密码并确认密码。
    - ***Unload and Unlock（卸载和解锁）> Requires a password（需要密码）。***输入合适的密码并确认密码。
65. 单击 ***Other Settings***（其他设置）选项卡。
66. 取消选中所有选项。

注意： 必须清除以下选项。

- ***OfficeScan Agent Self-protection（OfficeScan 代理程序自我保护）> Protect OfficeScan agent services.（保护 OfficeScan 代理程序服务）。***
- ***OfficeScan Agent Self-protection（OfficeScan 代理程序自我保护）> Protect files in the OfficeScan agent installation folder（保护 OfficeScan 代理程序安装目录中的文件）。***
- ***OfficeScan Agent Self-protection（OfficeScan 代理程序自我保护）> Protect OfficeScan agent registry keys（保护 OfficeScan 代理程序注册表项）。***
- ***OfficeScan Agent Self-protection（OfficeScan 代理程序自我保护）> Protect OfficeScan agent processes（保护 OfficeScan 代理程序流程）。***

67. 单击 ***Apply to All Agents***（应用到所有代理程序）。
68. 单击 ***Close***（关闭）以关闭 ***Privileges and Other Settings***（权限和其他设置）屏幕。
69. 从顶部窗格中，选择 ***Agents（代理程序）> Agent Management（代理程序管理）***链接。
70. 在左侧窗格中选择 ***OfficeScan Server***（OfficeScan 服务器）。
71. 从 ***Settings***（设置）选项中选择 ***Additional Service Settings***（其他服务设置）。
72. 取消选中 ***Enable service on the following operating systems***（在下列操作系统上启用服务）。
73. 单击 ***Apply to All Agents***（应用到所有代理程序）。
74. 单击 ***Close***（关闭）以关闭 ***Additional Service Settings***（其他服务设置）屏幕。
75. 从顶部窗格中，选择 ***Agent（代理程序）> Global Agent Settings（全局代理程序设置）***链接。

76. 仅选择以下选项并取消选中其余选项：
    - ***Scan Settings for Large Compressed Files（大型压缩文件的扫描设置）> Do not scan files in the compressed file if the size exceeds 2 Mb（如果压缩文件大小超过 2 MB，则不扫描压缩文件中的文件）***。针对 ***Real-Time Scan***（实时扫描）和 ***Manual Scan/Schedule Scan/Scan Now（手动扫描 / 计划扫描 / 立即扫描）*** 使用本信息。
    - ***Scan Settings for Large Compressed Files（大型压缩文件的扫描设置）> In a compressed file scan only the first 100 files（仅扫描压缩文件中的前 100 个文件）。*** 针对 ***Real-Time Scan***（实时扫描）和 ***Manual Scan/Schedule Scan/Scan Now（手动扫描 / 计划扫描 / 立即扫描）*** 使用本信息。
    - ***Scan Settings（扫描设置）> Exclude the OfficeScan server database folder from Real-time Scan（将 OfficeScan 服务器数据库文件夹从实时扫描中排除）。***
    - ***Scan Settings（扫描设置）> Exclude Microsoft Exchange server folders and files from scans.（将 Microsoft Exchange 服务器文件夹从扫描中排除）。***
77. 单击 ***Save***（保存）。
78. 从顶部窗格中，选择 ***Updates（更新）> Agents（代理程序）> Manual Updates（手动更新）*** 链接。
79. 选择 ***Manually select agents***（手动选择代理程序），然后单击 ***Select***（选择）。
80. 在 ***OffceScan Server***（OffceScan 服务器）下，双击合适的域名。
81. 选择客户端系统（一次选择一个），然后单击 ***Initiate Update***（启动更新）。
82. 单击消息框中的 ***OK***（确定）。
83. 单击 ***Log off***（注销）并关闭 OfficeScan Web Console（OfficeScan Web 控制台）。

Trend Micro OfficeScan 安装后指南

1. 启用环回连接。有关详细信息，请参阅启用环回连接（第 6 页）。
2. 配置 Computer Browser 服务。有关详细信息，请参阅在安装防病毒软件之后配置 Computer Browser 服务（第 7 页）。

对域和端点窗口中未列出的域或系统进行故障诊断

在执行 Trend Micro OfficeScan Client/Server Edition 11.0 SP1 和 Trend Micro OfficeScan Client/Server Edition XG 12.0 的首选推送安装方法期间，必须列出域和系统以将安装推送到系统。这些步骤提供两个选项供您在客户端（采集、回顾和 INW）上安装防病毒软件。

对于 11.0 SP1，请参阅：Trend Micro OfficeScan - 新安装部署步骤（11.0 SP1 的首选推送安装方法）（第 51 页）。
对于 12.0，请参阅：Trend Micro OfficeScan - 新安装部署步骤（12.0 的首选推送安装方法）（第 60 页）。

1. 使用客户端机器（采集、回顾和 INW）的 IP 地址并执行以下操作：
    a. 在 ***Search for endpoints***（搜索端点）框中输入每个客户端系统的 IP（一次一个），然后按 ***Enter*** 键。
    b. 提供 ***< 域名 >\ 用户名***和密码，然后单击 ***Log on***（登录）。
    c. 根据您的 Trend Micro 版本选择下列其中一个步骤：

i. 对于 11.0 SP1，返回到步骤 10（第 51 页）。

ii. 对于 12.0，返回到步骤 10（第 61 页）。

2. 如果您不知道系统的 IP 地址，或者先前的选项失败，请转到每台客户端机器（采集、回顾和 INW Server）并执行以下操作：

   a. 在所有客户端计算机上以**管理员**或管理员组成员的身份登录。

   b. 单击 ***Start（开始）> Run（运行）***。

   c. 输入 ***\\< 防病毒 Management Console_server_IP_address>***，然后按 ***Enter*** 键。系统提示时，输入管理员用户名和密码。

   d. 导航到 ***\\< 防病毒 Management Console_server_IP _address>\ofsscan***，然后双击 ***AutoPcc.exe***。系统提示时，输入管理员用户名和密码。

   e. 安装完成后，重新启动客户端系统。

   f. 在所有客户端计算机上以**管理员**或管理员组成员身份登录，并等待到系统托盘中的 Trend Micro OfficeScan 图标更改为蓝色。

   g. 根据您的 Trend Micro 版本选择下列其中一个步骤：

      i. 对于 11.0 SP1，请参阅：11.0 SP1 的 Trend Micro OfficeScan 服务器控制台配置（第 52 页）。

      ii. 对于 12.0，请参阅：12.0 的 Trend Micro OfficeScan 服务器控制台配置（第 61 页）。