Vulnerability Manager Plus 快速入门手册

ME 产品部

2020-04-01

本文档旨在帮助用户快速熟悉产品的使用方法。

目录

简介

ManageEngine Vulnerability Manager Plus 是一种企业漏洞管理软件，可帮助您扫描，评估，确定优先级并修复网络终结点中的漏洞。 它包括漏洞扫描和漏洞评估，自动补丁管理，安全配置管理，零日漏洞缓解，高风险软件审核和 Web 服务器强化等功能。

Vulnerability Manager Plus 是一种主动式突破管理融合了突破所有功能的解决方案管理-从突破的检测和评估到通过自动修补，从管理中完全消除了它们的网络端点的安全性配置，以强化面向互联网的 Web 服务器到只需一个控制台即可完成所有操作。它可在内部使用，从而使安全管理员和风险承担能力评估团队具备无与伦比的可见性，威胁意识和迅速消除风险的必要手段。Vulnerability Manager Plu 不仅可以保护 Lan 和 Wan 端点，还可以保护不断变化的设备。

Vulnerability Manager Plus 的特点：

- 持续监控并检测系统和服务器的漏洞以及其中的错误配置
- 评估并预测危险系数更高的漏洞
- 缓解 0Day 漏洞
- 为 Windows，Mac，Linux 和更高版本的系统中的 250 多个第三方应用程序自动安装补丁
- 消除默认/不安全的安全设置并合理部署安全配置
- 加固 Web 服务器并保护其免受多重攻击
- 审核端口、许可过期的软件、防病毒软件和防火墙状态
- 检测并删除高风险软件
- 详细评估单个漏洞和不安全的系统
- 利用预定义的，可定制的执行报告来有效地发出风险告警

系统安装

1. 访问以下链接下载安装包

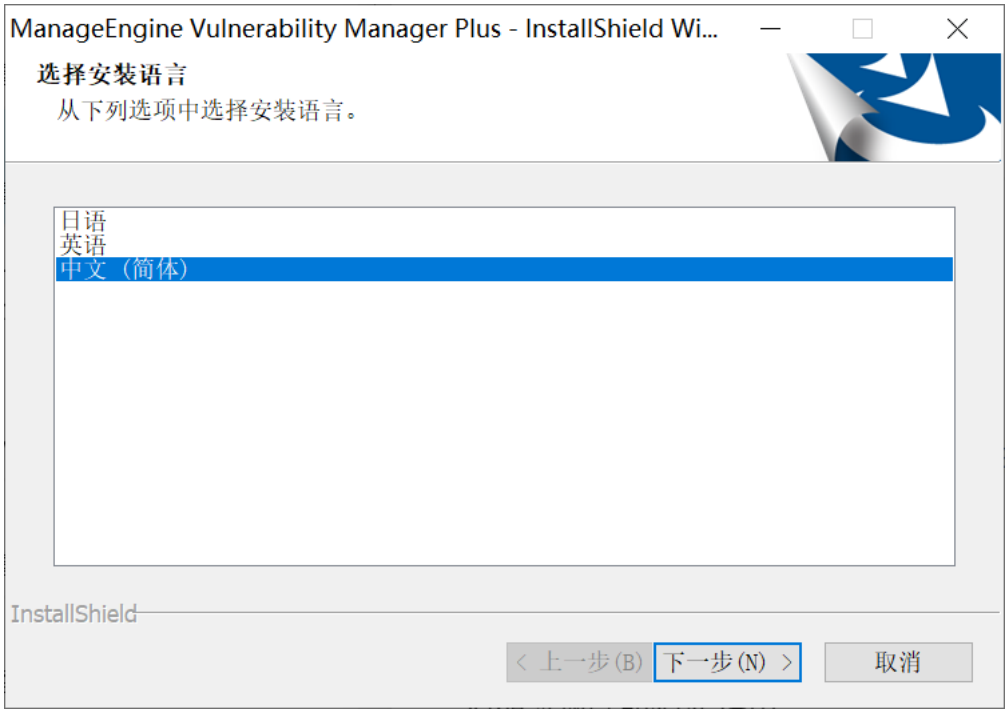
https://www.manageengine.cn/vulnerability-management/download_confirm.html

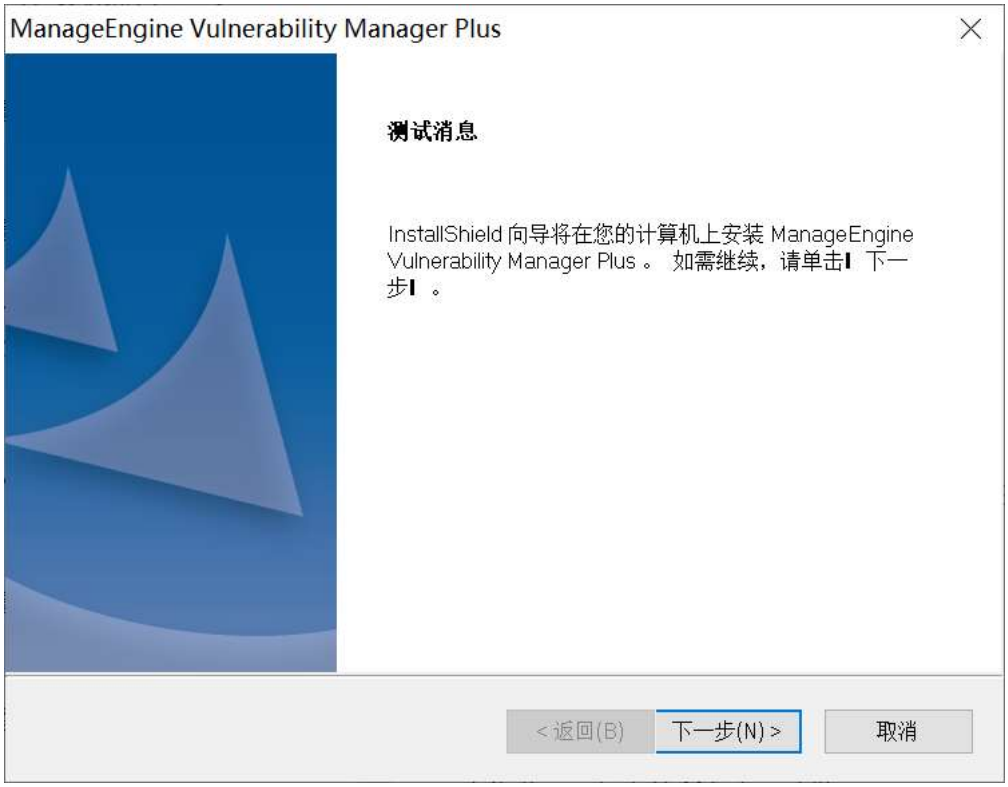
服务器硬件要求：

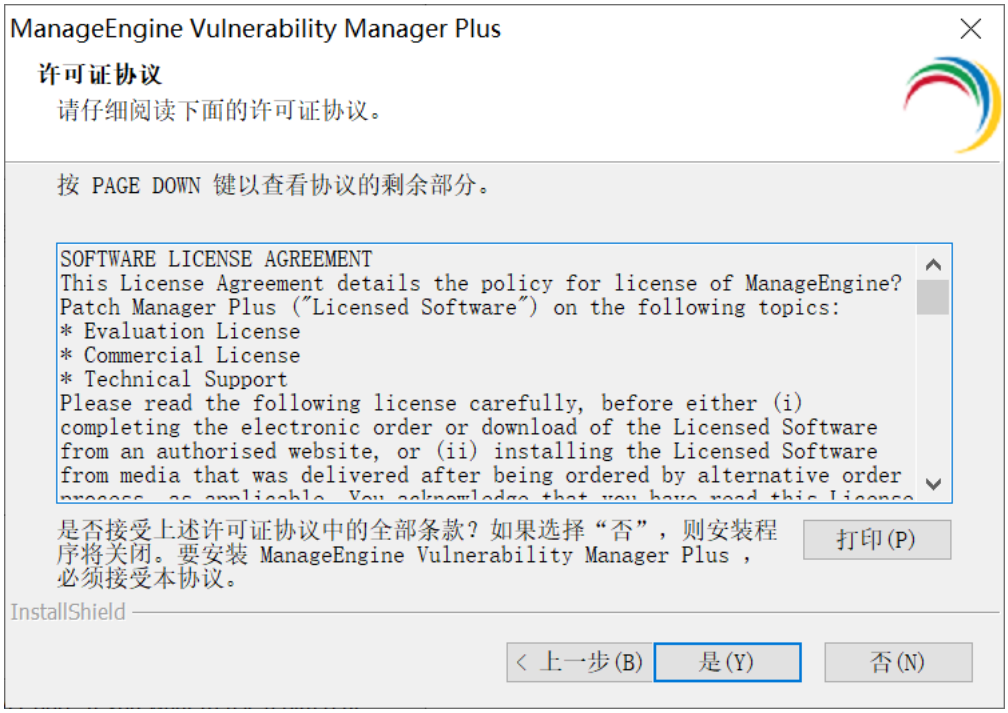
Vulnerability Manager Plus 服务器的硬件要求：

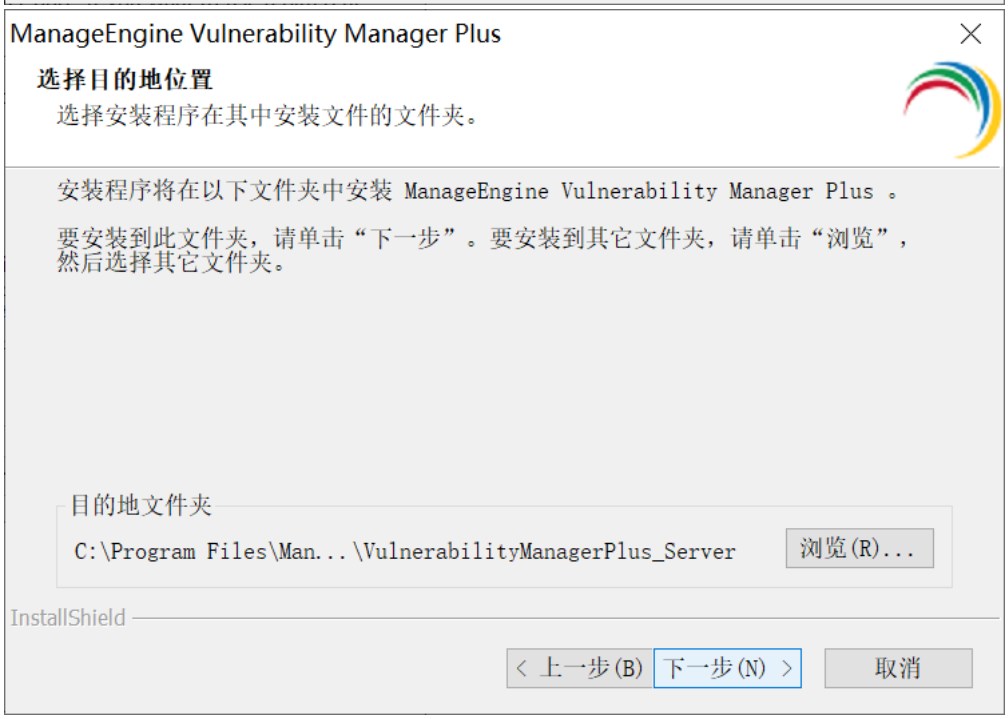
设备数量	服务器	处理器	内存	磁盘空间
1-250	Vulnerability Manager Plus Server	Intel Core i3 (2 core/4 thread) 2.0 Ghz 3 MB cache	2GB	5GB
251-500	Vulnerability Manager Plus Server	Intel Core i3 (2 core/4 thread) 2.4 Ghz 3 MB cache	4GB	10GB
501-1000	Vulnerability Manager Plus Server	Intel Core i3 (2 core/4 thread) 2.9 Ghz 3 MB cache	4GB	20GB
1001-3000	Vulnerability Manager Plus Server	Intel Core i5 (4 core/4 thread) 2.3 GHz. 6 MB cache	8GB	30GB
3001-5000	Vulnerability Manager Plus Server	Intel Core i7 (6 core/12 thread) 3.2 GHz. 12 MB cache	8GB	40GB

2. 在安装包下载完成后，用户可以手动双击安装包进入安装向导，根据向导中的提示进行安装操作。

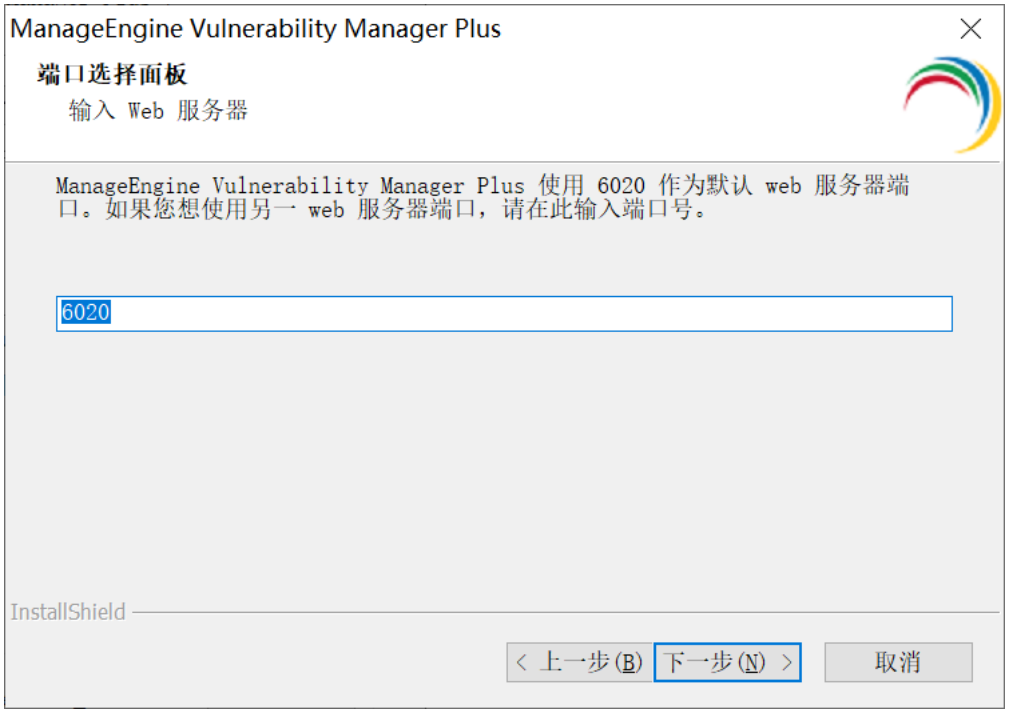

ManageEngine Vulnerability Manager Plus - InstallShield Wi...
选择安装语言
从下列选项中选择安装语言。
日语
英语
中文（简体）
InstallShield
< 上一步(B)
下一步(N) >
取消


ManageEngine Vulnerability Manager Plus
测试消息
InstallShield 向导将在您的计算机上安装 ManageEngine Vulnerability Manager Plus 。 如需继续，请单击"下一步"。
< 返回(B)
下一步(N) >
取消

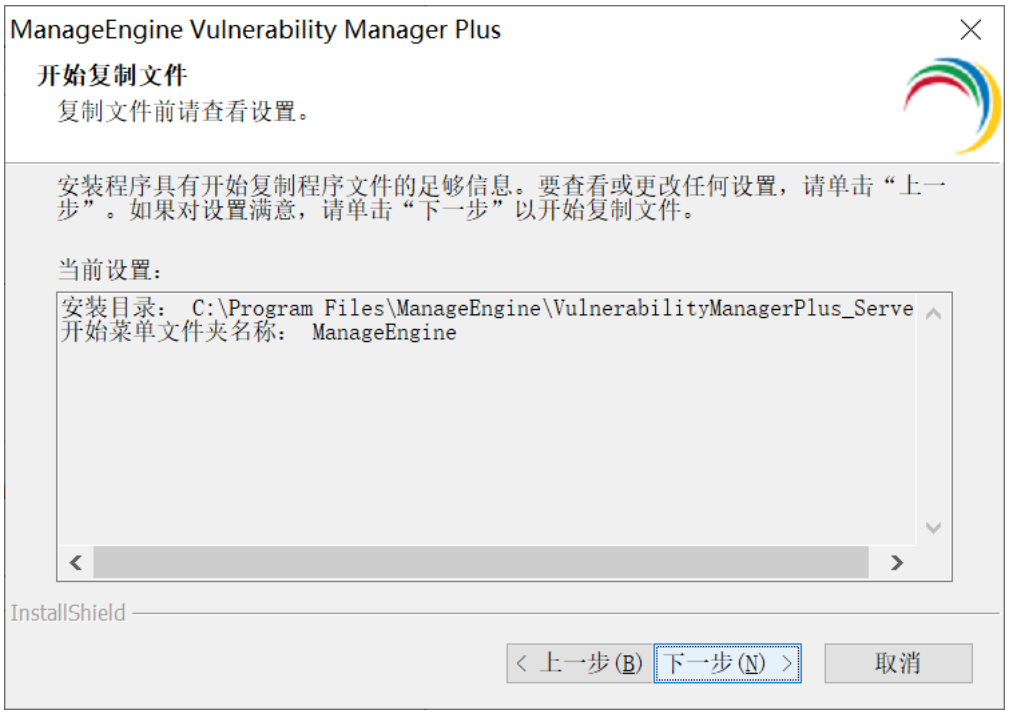

ManageEngine Vulnerability Manager Plus
许可证协议
请仔细阅读下面的许可证协议。
按 PAGE DOWN 键以查看协议的剩余部分。
SOFTWARE LICENSE AGREEMENT
This License Agreement details the policy for license of ManageEngine? Patch Manager Plus ("Licensed Software") on the following topics:
* Evaluation License
* Commercial License
* Technical Support
Please read the following license carefully, before either (i) completing the electronic order or download of the Licensed Software from an authorised website, or (ii) installing the Licensed Software from media that was delivered after being ordered by alternative order
是否接受上述许可证协议中的全部条款？如果选择“否”，则安装程序将关闭。要安装 ManageEngine Vulnerability Manager Plus ，必须接受本协议。
打印(P)
InstallShield
< 上一步(B)
是(Y)
否(N)


ManageEngine Vulnerability Manager Plus
选择目的地位置
选择安装程序在其中安装文件的文件夹。
安装程序将在以下文件夹中安装 ManageEngine Vulnerability Manager Plus 。
要安装到此文件夹，请单击“下一步”。要安装到其它文件夹，请单击“浏览”，然后选择其它文件夹。
目的地文件夹
C:\Program Files\Man...\VulnerabilityManagerPlus_Server
浏览(R)...
InstallShield
< 上一步(B)
下一步(N) >
取消

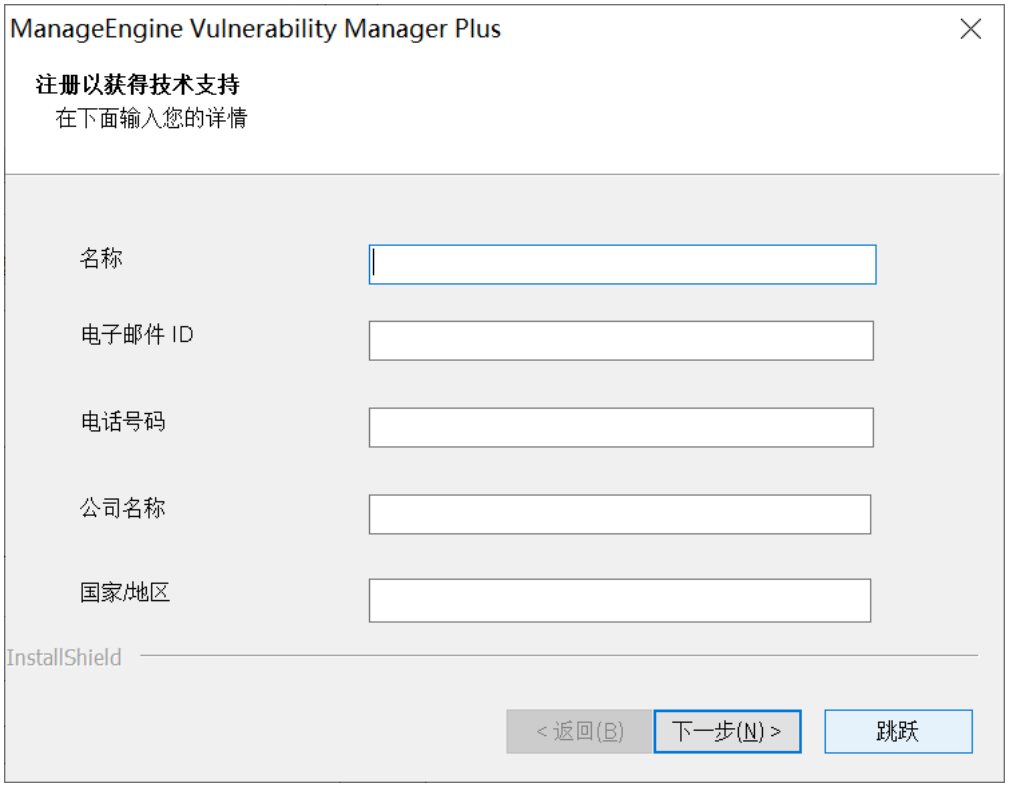
3. 选择访问端口号：



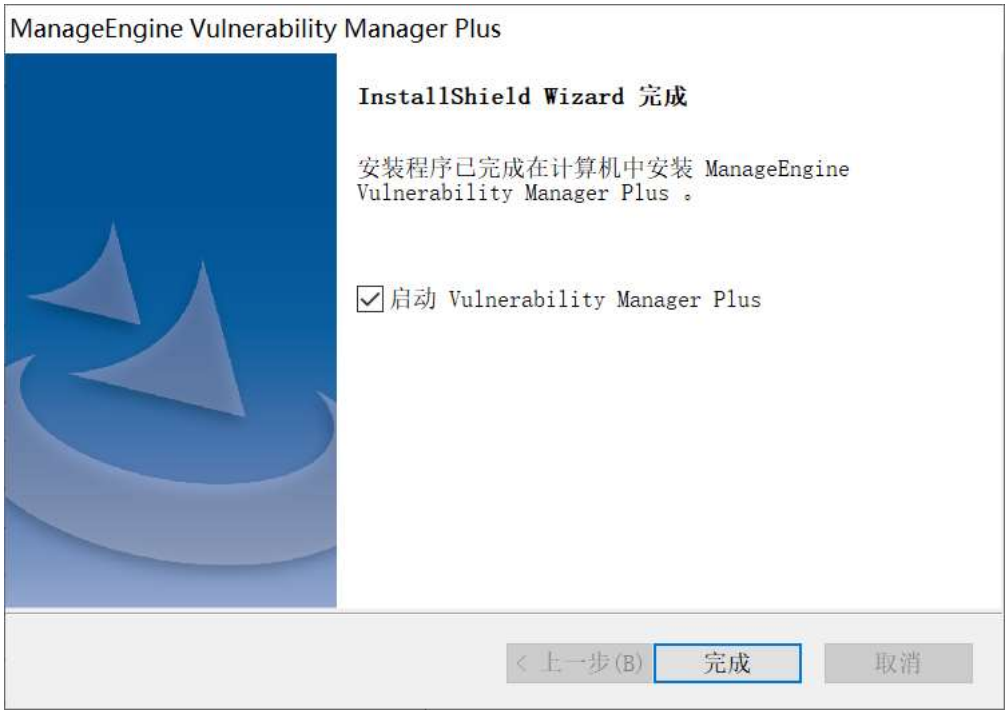
4. 选择安装路径：



5. 跳过填写信息步骤，选择“跳过”（此处翻译有误）



6. 完成以上操作之后，Vulnerability Manager Plus 开始安装。完成后显示：

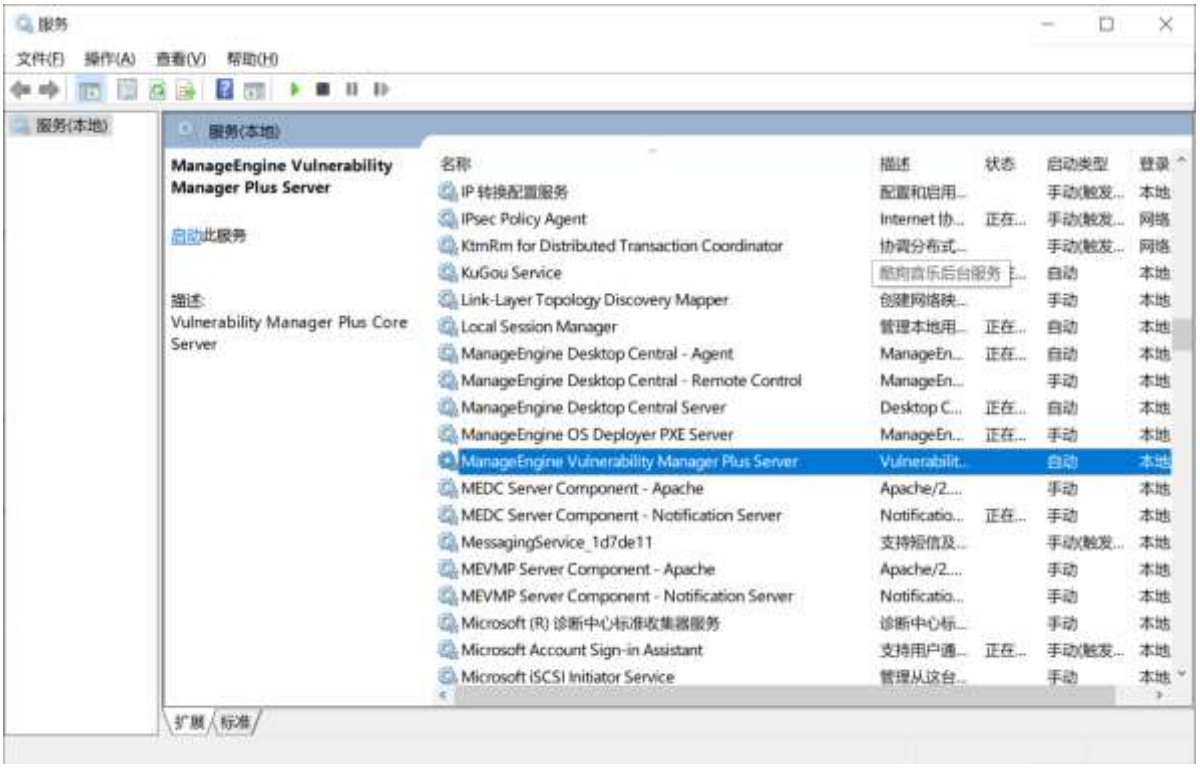


7. 选择“是的，启动 Vulnerability Manager Plus”即可自动启动该系统。点击完成即可结束安装。

启动 Vulnerability Manager Plus

Vulnerability Manager Plus 可以通过如下方式启动：

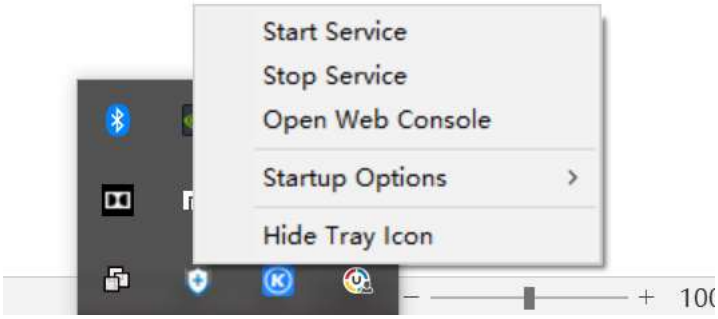
- 方式一：桌面图标启动：双击桌面上的“Start Vulnerability Manager Plus”图标启动；
- 方式二：服务启动：打开 windows 的服务，在服务列表中找到 ManageEngine Vulnerability Manager Plus Server 服务，打开其属性并点击‘启动’；



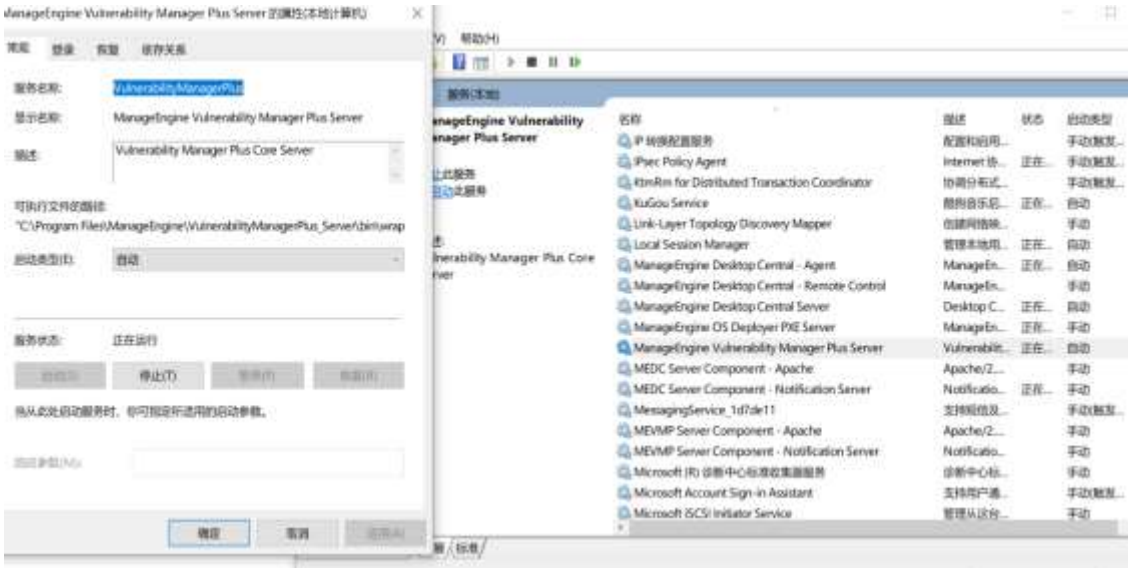
关闭 Vulnerability Manager Plus

Vulnerability Manager Plus 可以通过如下方式关闭：

- 方式一：右击系统托盘中的 Vulnerability Manager Plus 图标，在弹出的选项中选择“Stop Service”



- 方式二：打开 windows 系统的服务列表，关闭 Vulnerability Manager Plus 的服务；



登录 Vulnerability Manager Plus

在启动完成后用户便可以访问客户端登录 Vulnerability Manager Plus。Vulnerability Manager Plus 基于 B/S 架构开发，所以支持基于 WEB 页面的访问，所以用户可以打开浏览器，在地址栏中输入：

http://server:port

来访问 Vulnerability Manager Plus 的客户端，其中链接中的“server”是指 Vulnerability Manager Plus 所安装的服务器的 DNS 名称或者 IP 地址，端口就是在安装的过程中配置的 web 端口，例如 Vulnerability Manager Plus 服务器的 DNS 名称叫 Vulnerability Manager Plus， web 端口使用的是 9030，那么我们可以通过访问

http://192.168.1.12:6020

来访问 Vulnerability Manager Plus 的客户端。当然，如果用户在 Vulnerability Manager Plus 服务器上访问 Vulnerability Manager Plus 的客户端，可以使用:

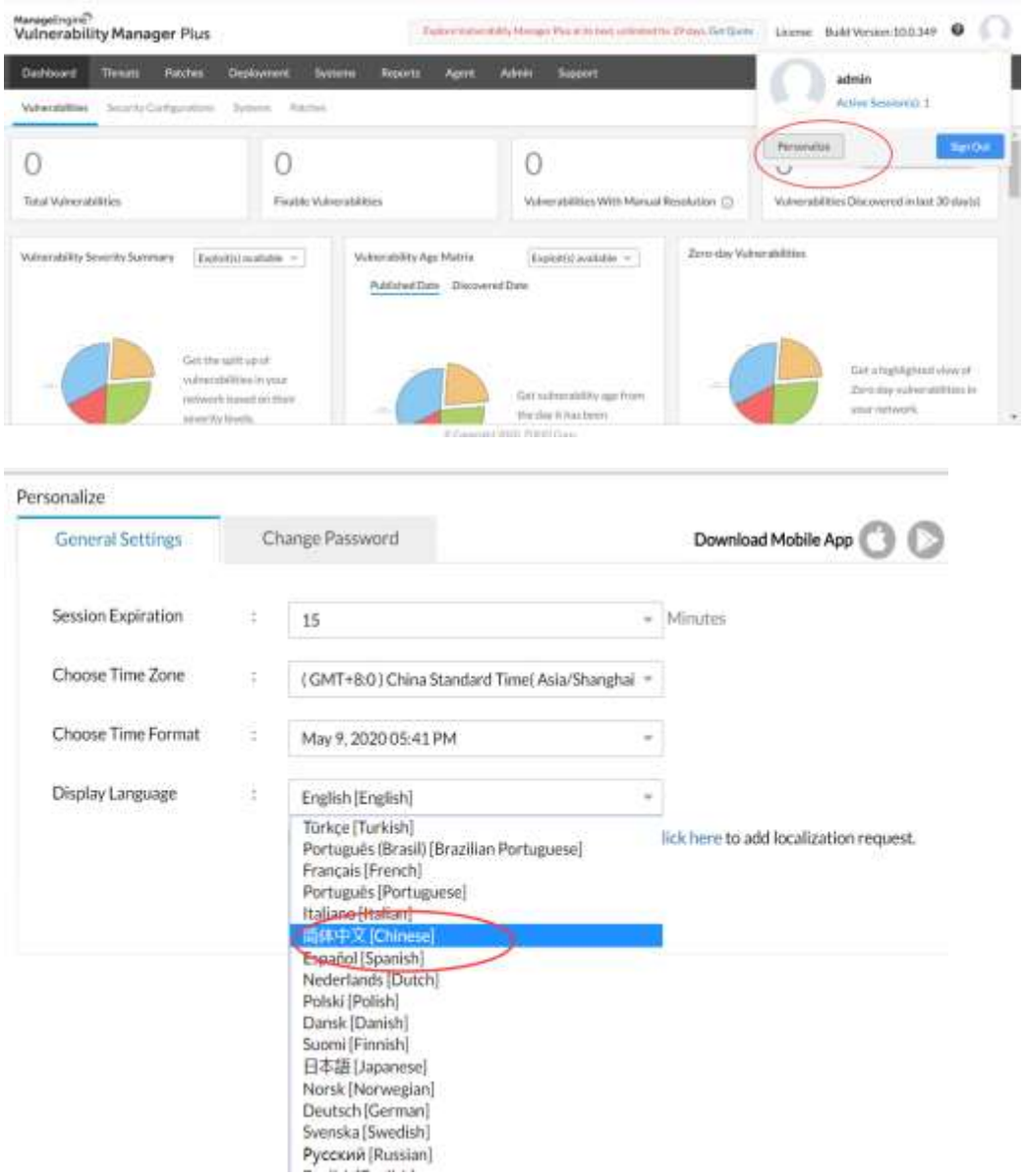
http://localhost:6020

来进行访问。系统默认账号为 admin/admin

添加计算机

Vulnerability Manager Plus 系统通过代理的方式与客户机通信，将计算机添加到系统时，客户机同时安装代理。

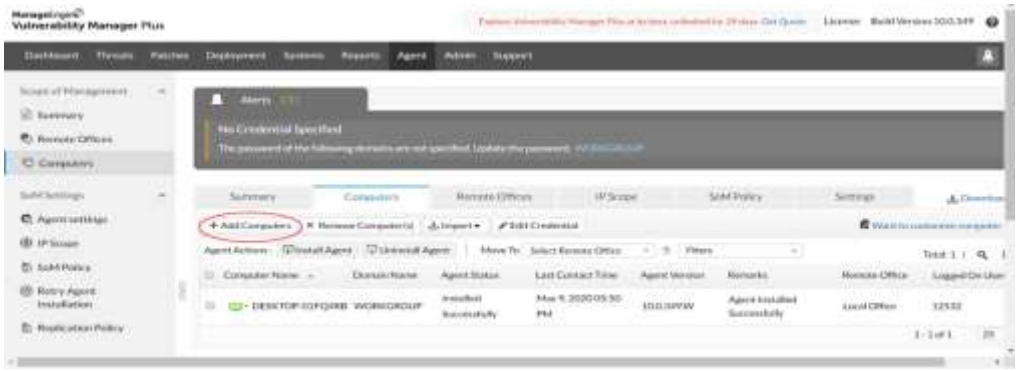
修改界面为中文：Personalize>选择“中文”>“Save”。(建议使用英文界面，截至 10.0.349 版本，中文界面尚未全部完成汉化。)



1. 添加 Windows 计算机

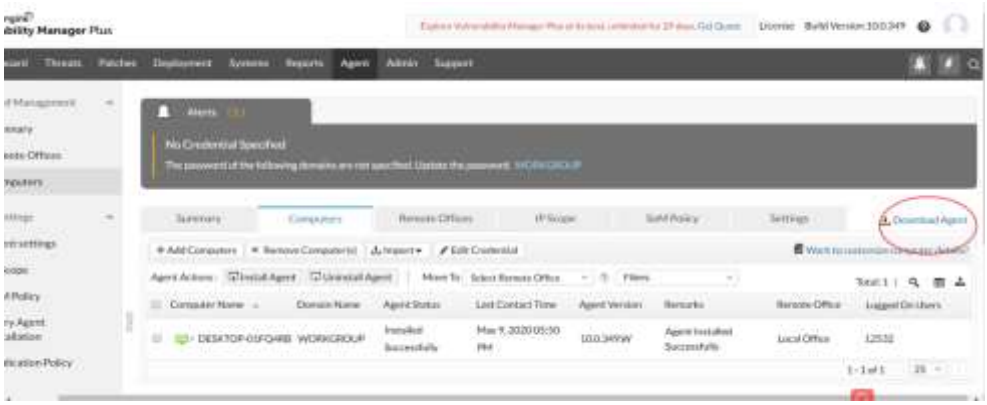
- 有域，直接添加计算机

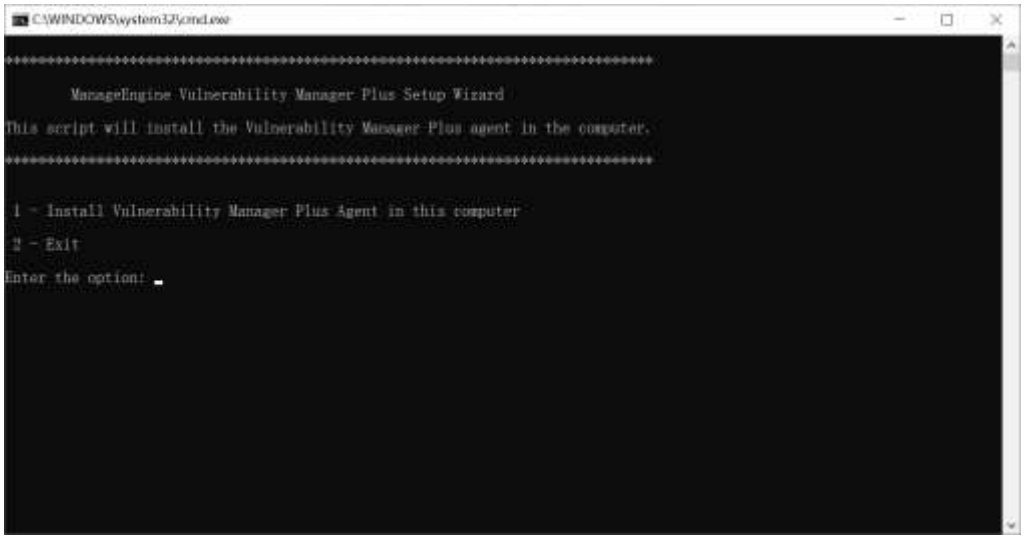
管理员登录系统后，“Admin”-“Scope of Management”，点击“Add Computers”，将客户机添加入系统中，并直接给客户端安装代理。



- 无 AD 域/工作组环境

管理员登录系统后，选择“Agent”-“Computers”，点击“Download Agent”将代理安装压缩文件下载到本地。将代理拷贝到客户机解压，双击 setup.bat 文件安装，输入数字“1”，回车安装完成，任意键退出。

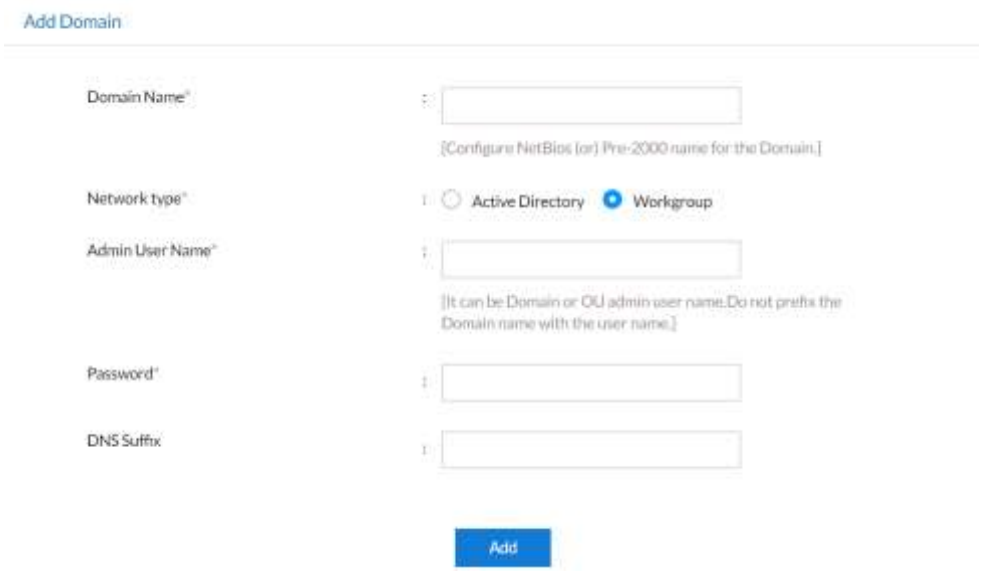




安装成功后，任意键退出安装。

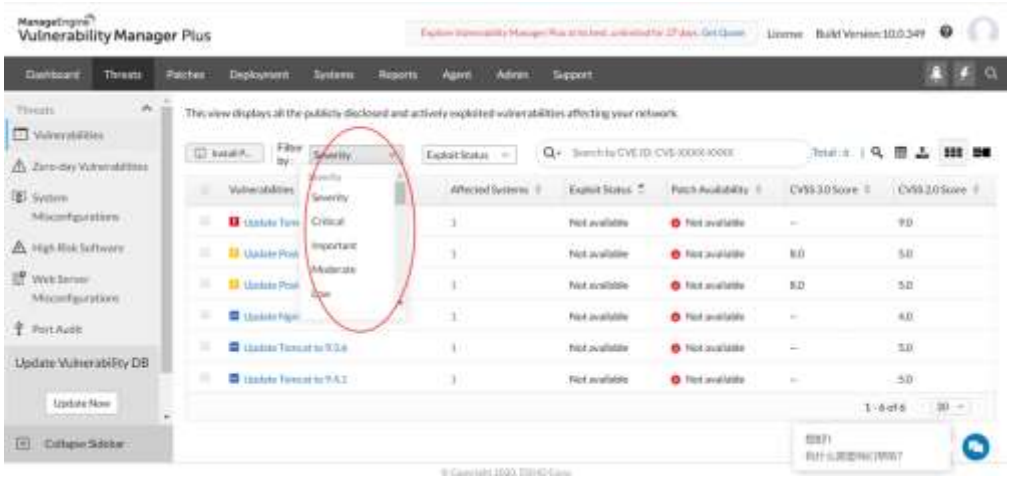
- 添加 AD 域/工作组中的计算机

管理员登录系统后，选择“Agent”-“Active Diretory”，添加工作组，将域/工作组信息填写完成后，点击选择计算机，将客户机添加入系统中，并直接给客户端安装代理。



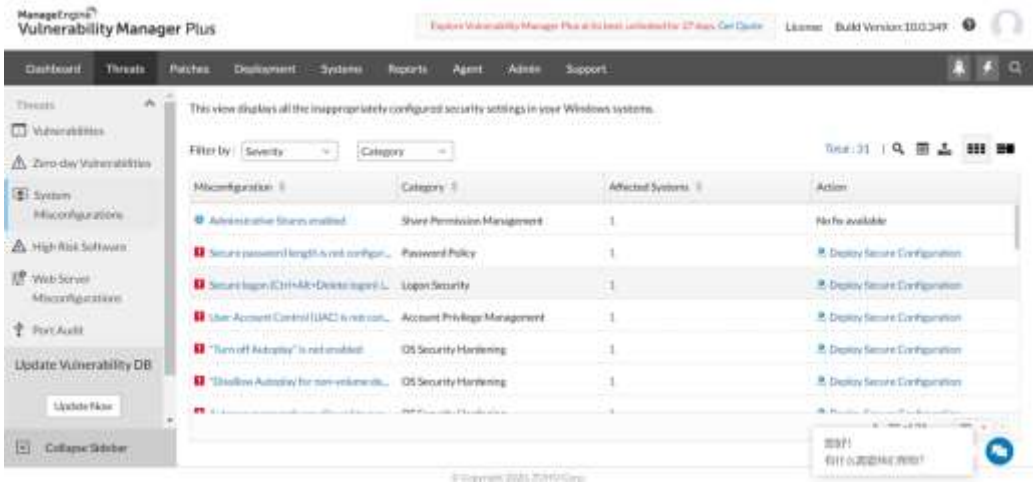
管理

1. Vulnerability Manager Plus 根据可利用性，严重性，寿命，受影响的系统数量以及修复程序的可用性评估并确定漏洞等级。可自行根据漏洞等级进行下载及部署。

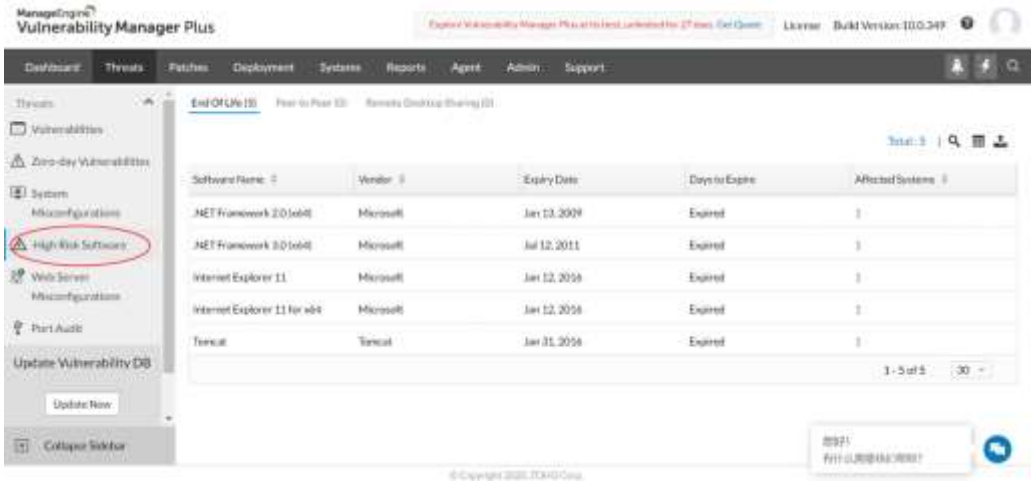


2. Vulnerability Manager Plus 可及时发现 0Day 漏洞。

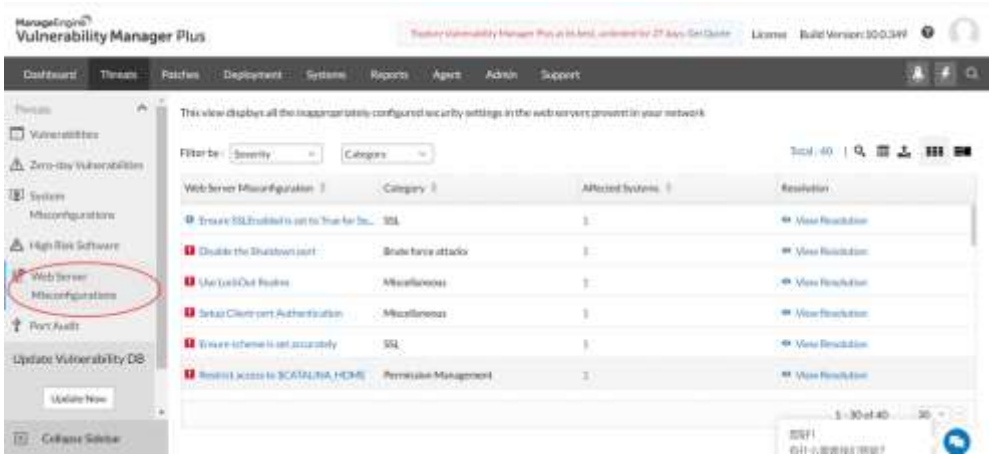
3. Vulnerability Manager Plus 可识别系统配置错误并给出最佳部署策略。



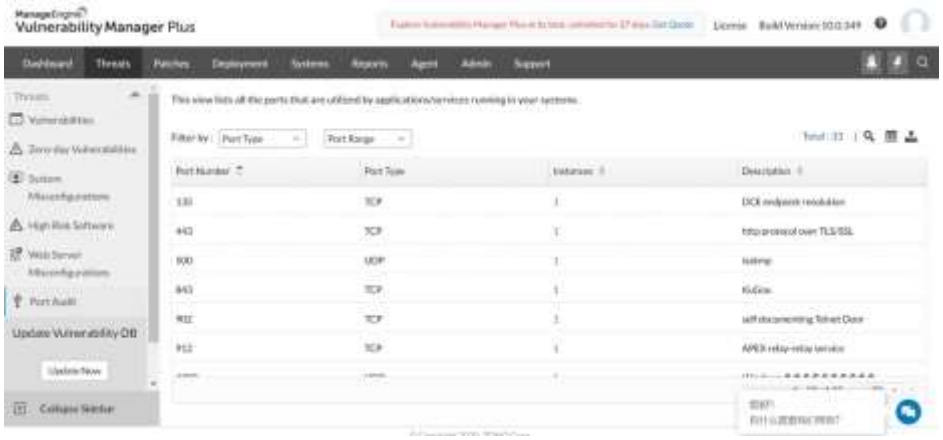
4. Vulnerability Manager Plus 可识别高风险软件，及时发现已终止寿命的软件。



5. Vulnerability Manager Plus 持续监控 Web 服务器和不安全的配置并分析 Web 服务器的错误配置获得修复的详细信息。

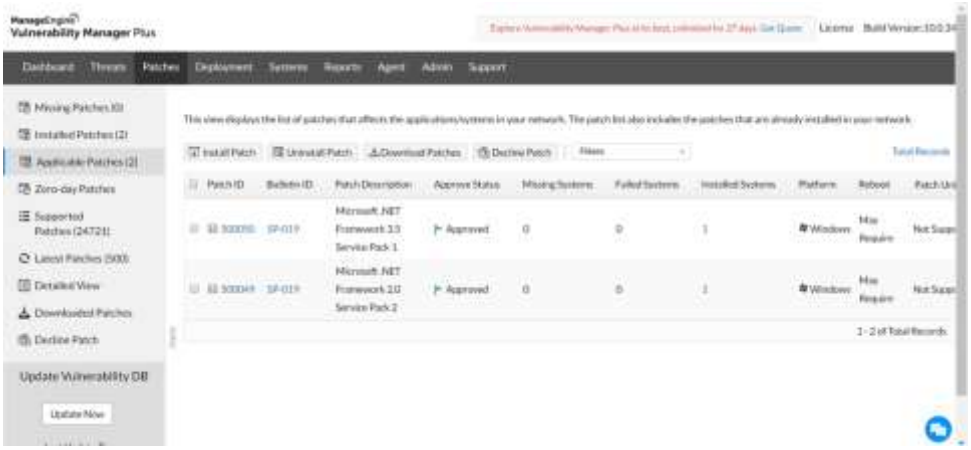


6. Vulnerability Manager Plus 端口审计可识别端口类型（TCP 还是 UDP），可查看端口对应的计算机，进程，进程路径，进程描述等。



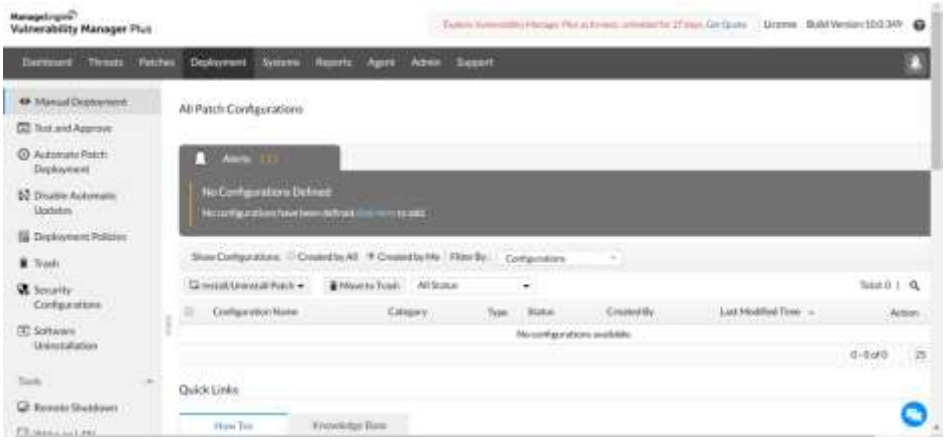
补丁管理

1. Vulnerability Manager Plus 补丁管理中，补丁可分为遗漏的补丁、已安装的补丁、适用的补丁、支持的补丁及 0Day 补丁。“Latest Patches”中的补丁是直接从系统及第三方软件官网抓取的最新的补丁。

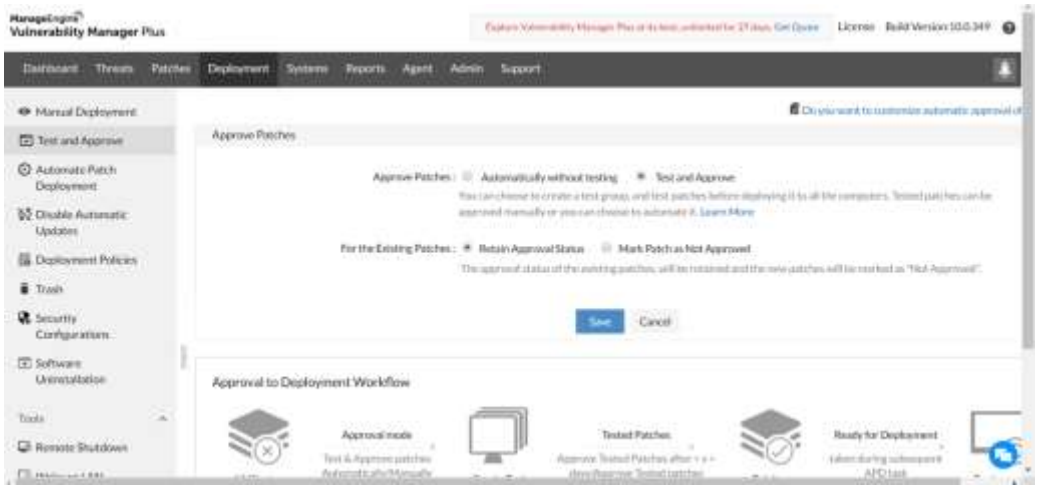


部署策略

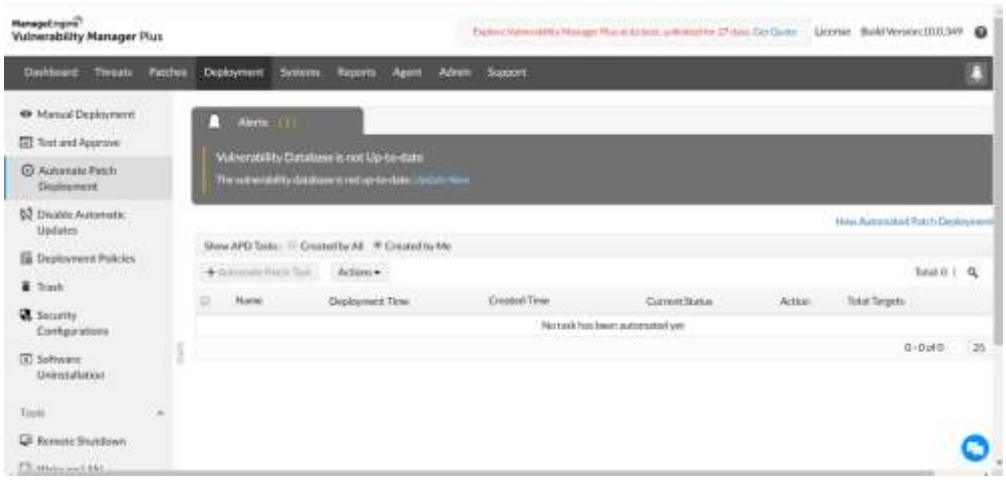
1. 部署策略分为普通部署：可以选择受手动安装/卸载补丁。



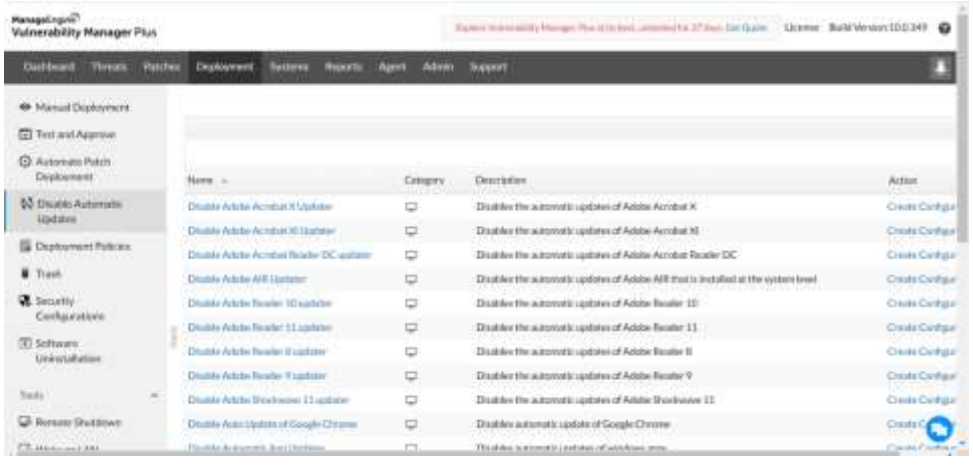
2. 测试及批准：将特定补丁推送给一个测试组，测试完成后批准此补丁推送到所有计算机，确保补丁不会影响计算机的使用。



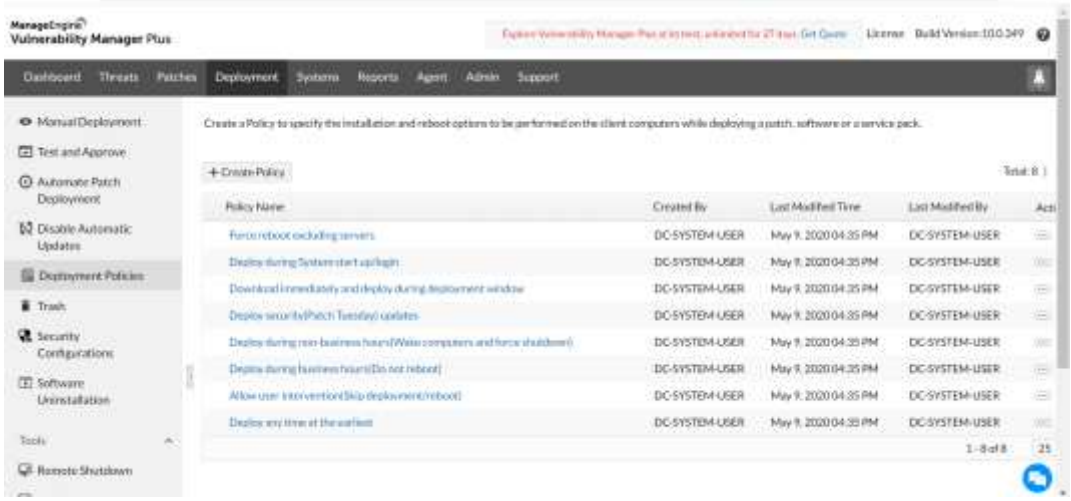
3. 自动部署策略：自定义补丁自动安装部署



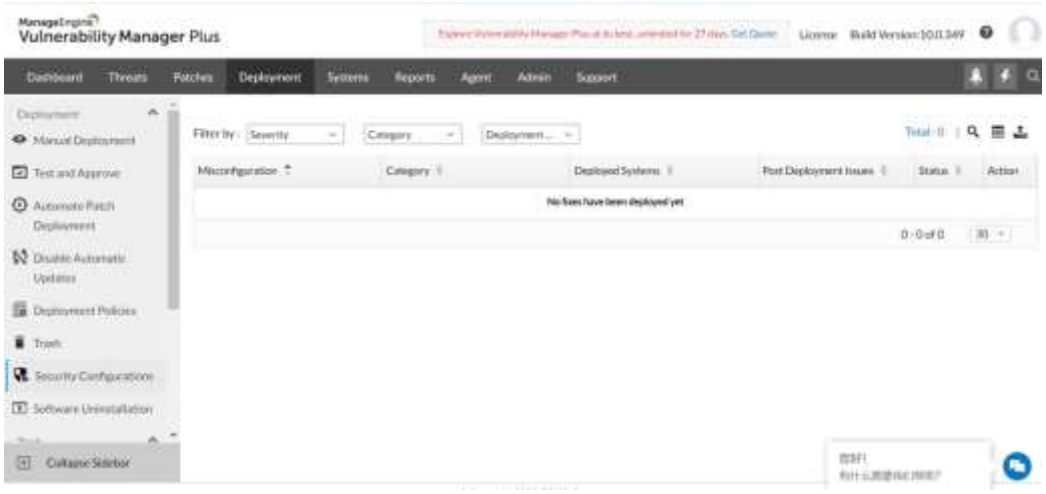
4. 禁止自动更新：禁止特定软件自动更新，比如 Adobe/Java 等。



5. 部署策略:VMP 提供八种部署模板，也可以自定义创建部署策略。

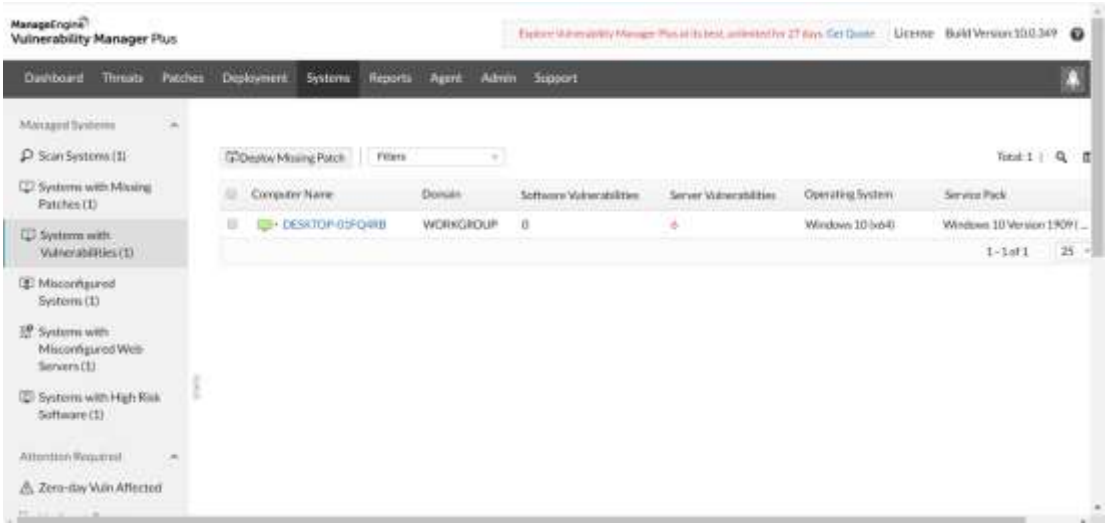


6. 安全配置：审计防火墙策略，禁止向未授权的用户打开共享、弱密码、遗留系统协议和其他错误的安全配置。



系统安全

此项中详细展示系统中检测到的漏洞及补丁，高风险软件、配置错误的网络，并给出有效的安全策略。


ManageEngine
Vulnerability Manager Plus
License
Build Version 10.0.349
Dashboard
Threats
Patches
Deployment
Systems
Reports
Agent
Admin
Support
Managed Systems
Scan Systems (1)
Systems with Missing Patches (1)
Systems with Vulnerabilities (1)
Misconfigured Systems (1)
Systems with Misconfigured Web Servers (1)
Systems with High Risk Software (1)
Attention Required
Zero-day Vuln Affected
Deploy Missing Patch
Filters
Total: 1
Computer Name
Domain
Software Vulnerabilities
Server Vulnerabilities
Operating System
Service Pack
DESKTOP-01FQ4RB
WORKGROUP
0
0
Windows 10 (x64)
Windows 10 Version 1909 (...
1 - 1 of 1
25

产品文档

关于更详细的说明可参见产品官网：

https://www.manageengine.cn/vulnerability-management/help.html

在线演示： https://www.manageengine.cn/vulnerability-management/request-demo.html

联系电话：4006608680

技术支持：support@manageengine.cn