M-8000XC Sensor 快速入门手册

修订版 B

McAfee® Network Security Platform

本快速入门手册介绍如何快速安装和激活 McAfee® Network Security Platform M-8000XC Sensor 以通过 McAfee® Network Security Platform XC-240 负载平衡器实现负载平衡。将 Sensor 的 XFP（10 千兆位小型可插拔）监控端口电缆连接到 XC-240 即可使您实现 Sensor 流量负载平衡。

要将现有 M-8000 Sensor 升级到 M-8000XC，请联系 McAfee 技术支持人员。

有关 XC-240 设备的详细信息，请参阅“McAfee Network Security Platform XC-240 负载平衡器设备快速入门手册”。

本快速入门手册所涉及到的所有产品文档都可以在 McAfee ServicePortal 上找到。

Sensor 前面板



1	电源 A（2 - 附带）	**7**	XFP 10 千兆位以太网监控端口 (12)
2	电源 B（2 - 可选，单独出售）	**8**	袖珍闪存端口 (2)
3	RS-232C 控制端口 (2)	**9**	RJ-45 响应端口 (1)
4	RS-232C 辅助端口 (2)	**10**	10/100/1000 管理端口 (1)

5 RJ-11 失效打开控制端口 (14)

6 SFP 1 千兆位以太网监控端口 (16)

11 互连端口 (2)

1 安排 Sensor 的位置

“McAfee Network Security Platform M-8000 Sensor 产品手册”中提供了所有任务的相关详细信息。另请参阅“McAfee Network Security Platform M 系列滑轨装配过程”。

a 松开导轨，用所提供的螺丝紧固（三合一套件中的）内部导轨，从而将其安装到机箱上。



b 将 L 形的外部导轨安装到机架框上。



c 将主 Sensor 安装到机架和安装耳中。您还可以采用中间式安装的方法来安装 Sensor（可选）。





d 安装冗余电源（可选）。



e 将模块安装到 Sensor 的监控端口中。

f 对次 Sensor 重复步骤 a 至步骤 e。



2 连接管理端口和控制台端口电缆

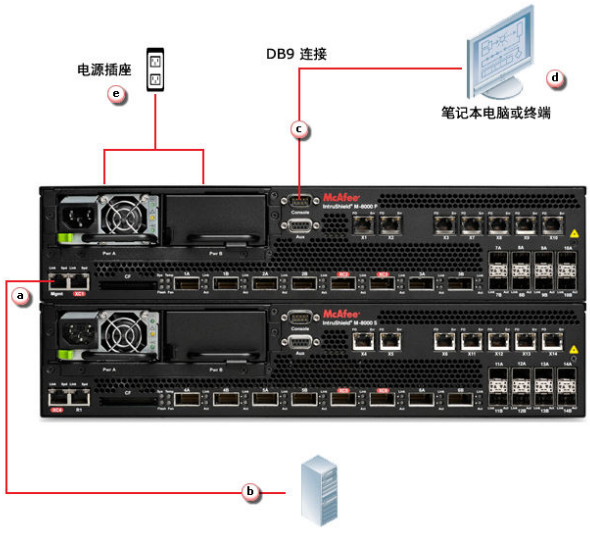
a 将 5e 类以太网电缆插入 M-8000XC P 的管理 (Mgmt) 端口。

b 将此电缆的另一端插入连接到 Manager 服务器的网络设备。

c 将 Sensor 包装箱中随附的 DB9 控制台电缆插入 M-8000XC P 的控制台端口（Sensor 前面板上标有“Console（控制台）”字样的端口）。

> 可以使用次 Sensor M-8000XC S 上的控制台端口来执行闪存恢复过程或进行故障排除。

d 将控制台端口电缆的另一端直接插入用于配置 Sensor 的计算机或终端服务器（例如运行正确配置了 Windows 超级终端软件的计算机）的 COM 端口。最初配置 Sensor 时必须直接连接到控制台；您不能远程配置 Sensor。



超级终端的必要设置如下：

- 波特率：38400
- 位数：8
- 奇偶校验：无
- 停止位：1
- 数据流控制：无

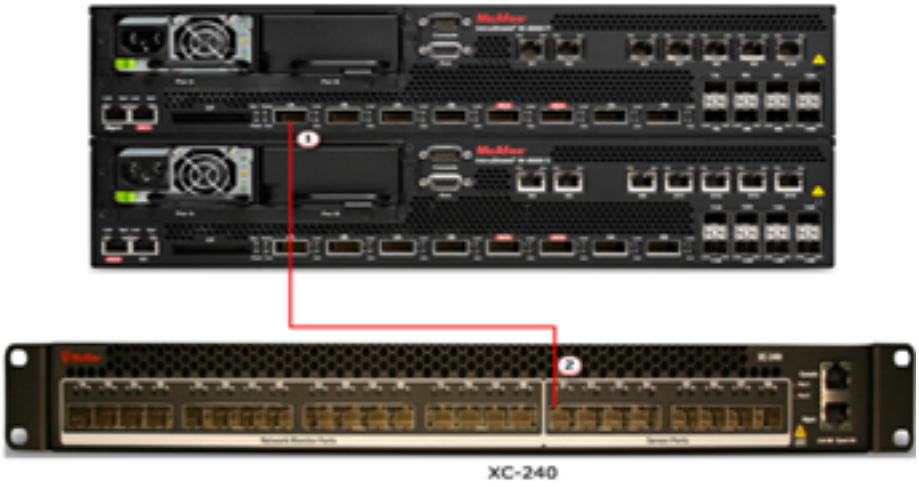
e 将电源线一端有孔的插头插入电源插口，将另一端插入电源插座。Sensor 随附有标准的美式电源和国际通用电缆。

M-8000XC 没有电源开关；只需将电源线插入电源插座即可通电。

3 连接监控端口电缆

以下步骤介绍如何连接 Sensor 电缆，以使其连接到 XC-240 负载平衡器。

a 将您的 XFP 模块适用的电缆插入端口 1A。



McAfee 仅支持通过 McAfee 或向 McAfee 认可的厂商购买的 XFP 模块。

请不要使用 XC 端口。这些端口是为主 Sensor (M-8000XC P) 和次 Sensor (M-8000XC S) 之间的互连保留的。

b 将电缆的另一端连接到 XC-240 负载平衡器上的 Sensor 端口。

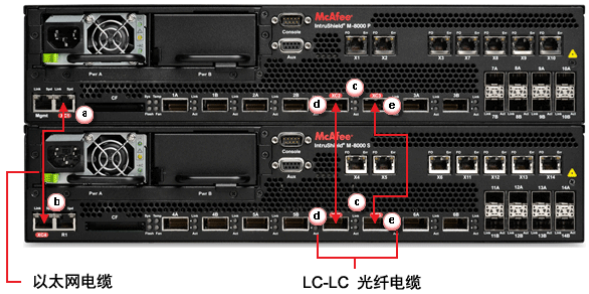
有关如何使用 XC-240 负载平衡器的说明，请参阅“McAfee Network Security Platform XC 群集管理手册”。

4 连接互连端口电缆

以下步骤介绍如何将主 Sensor 连接到次 Sensor。

a

将所提供的以太网电缆插入主 Sensor 的 XC1 端口中。



b 将步骤 a 中所用以太网电缆的另一端插入次 Sensor 的 XC4 端口中。

c 将所提供的 XFP 模块插入主 Sensor 和次 Sensor 上的 XC2、XC3、XC5 和 XC6 端口中。

McAfee 仅支持通过 McAfee 或向 McAfee 认可的厂商购买的 XFP 模块。

d 将 LC-LC 光纤电缆的一端插入主 Sensor 的 XC2 端口中，将另一端连接到次 Sensor 的 XC5 端口中。

e 将 LC-LC 光纤电缆的一端插入主 Sensor 的 XC3 端口中，将另一端连接到次 Sensor 的 XC6 端口中。

5 将 Sensor 添加到 Manager

Manager 会显示“Login ID（登录 ID）”页。

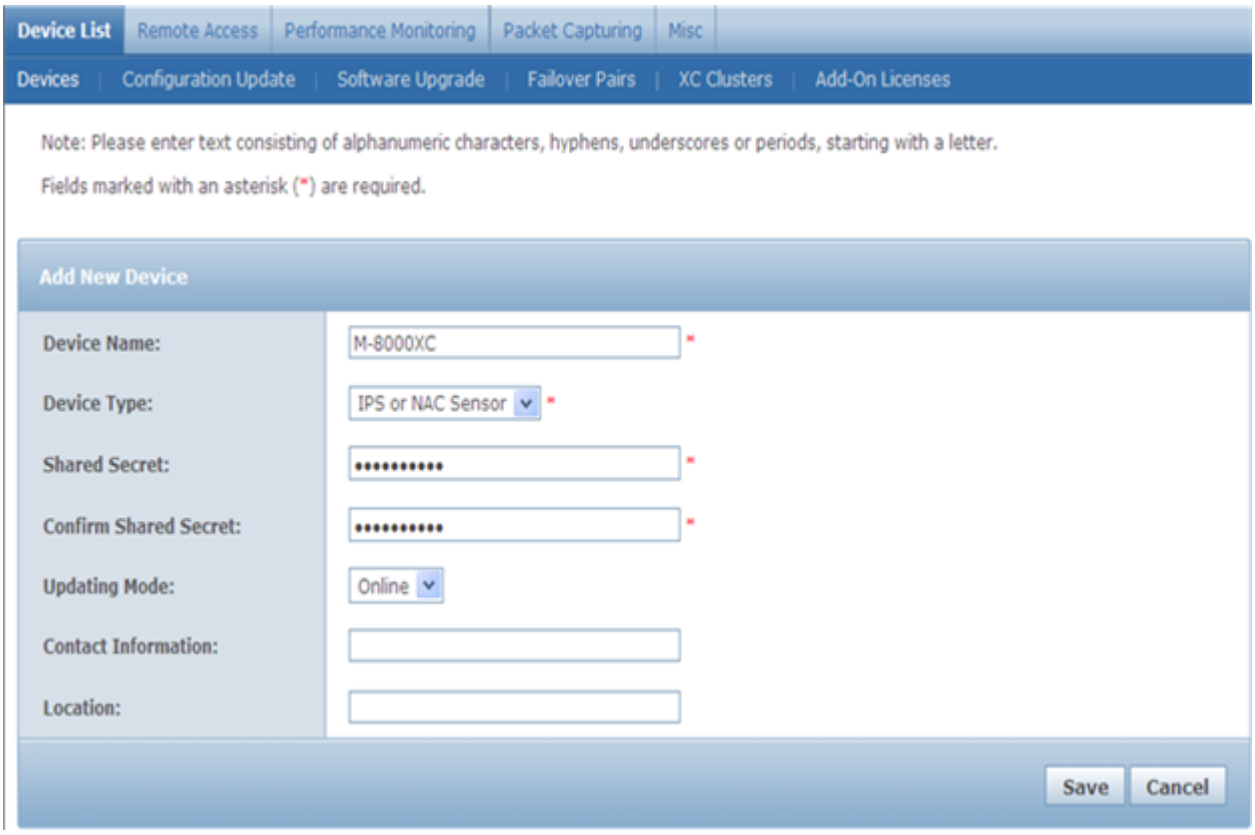
a 登录到 Manager。默认登录 ID 为 admin，默认密码为 admin123。

b 单击“Configure（配置）”。

M-8000XC Sensor 不支持 NAC。无需许可证文件即可在 M-8000XC Sensor 上启用 IPS。

c 要在 Manager 中添加 Sensor，请选择“Device List（设备列表）” | “Devices（设备）”，然后单击“New（新建）”。

此时将显示“Add New Device（添加新设备）”页。



d 在适当的字段中输入信息，然后单击“Save（保存）”。

请记住在此步骤中输入的 **Shared Secret（共享密钥）**值。在配置 Sensor 时，将会用到此值。

有关“Add New Device（添加新设备）”页中各字段的详细信息，请参阅“McAfee Network Security Platform XC 群集管理手册”。

6 配置 Sensor 信息

使用网络信息、名称以及 Sensor 与 Manager 建立安全通信所使用的共享密钥配置 Sensor。使用您在步骤 5d 中设置的名称和密钥值。

首次配置 Sensor 时，务必实际访问 Sensor。

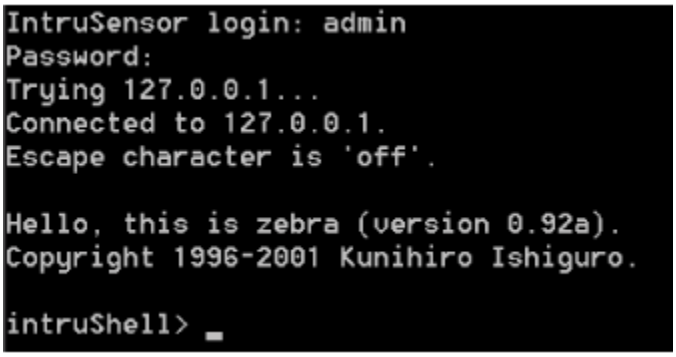
可以使用主 Sensor (M-8000XC P) 的 CLI 来配置 M-8000XC Sensor。

在配置过程中，可以随时键入问号 (?) 查看 Sensor CLI 命令的帮助。要查看所有命令的列表，请键入 commands。

a 通过连接到控制台端口的终端登录到主 Sensor。

b 在提示符处，使用默认的 Sensor 用户名 (admin) 和密码 (admin123) 登录。

c [此步骤是可选的，但建议执行。]更改 Sensor 密码。在提示符处键入：passwd。Sensor 会提示您输入新密码，也会询问旧密码。



密码长度必须介于 8 到 25 个字符之间，且区分大小写，可包括任何字母数字字符或符号。

d 设置 Sensor 的名称：

您可以在提示符处输入 setup 命令，系统将自动提示您输入第 4 项至第 7 项以及第 10 项中所显示的信息。您也可以改用 set 命令。如果你使用 set 命令，您必须手动输入第 4 项至第 7 项以及第 10 项所显示的完整命令语法。

在提示符处键入：set sensor name <WORD>。

示例：set sensor name HR_sensor1

Sensor 名称是一个区分大小写的字符串，最多可包含 25 个字符。此字符串可包括连字符、下划线和点号，但开头必须是字母。

e 如果 Sensor 和 Manager 不在同一个网络上，请设置默认网关地址。在提示符处键入：set sensor gateway <A.B.C.D>

示例：set sensor gateway 192.168.3.68

f 设置 Manager 服务器的 IP 地址。在提示符处键入：set manager ip <A.B.C.D>。

示例：set manager ip 192.168.2.8

g 设置 Sensor 的 IP 地址和子网掩码。在提示符处键入：set sensor ip <A.B.C.D> <E.F.G.H>。

示例：set sensor ip 192.168.2.12 255.255.255.0

指定 IP 地址，该地址由 4 个用点隔开的八位字节组成：X.X.X.X，其中 X 是 0 到 255 之间的一个数字，后接采用同种格式的子网掩码。

h 如果系统提示，则重新启动 Sensor。键入：reboot

Sensor 最多需要 5 分钟才能完成重新启动。

i 从 Sensor ping Manager，以确定到目前为止的配置设置是否已在网络上成功建立 Sensor。在提示符处键入：ping <Manager IP address>。

如果 ping 成功，继续执行以下步骤。如果没有成功，请键入 show 验证配置设置，检查信息是否正确无误。

j 设置 Sensor 的共享密钥值。在提示符处键入：set sensor sharedsecretkey。

然后，Sensor 会提示您输入共享密钥值，并再进行确认。

此值用于在 Sensor 与 Manager 之间建立信任关系。密钥值可以是 8 到 25 个字符之间的任何 ASCII 文本，且区分大小写。确保此值与 Manager 界面中提供的共享密钥值相符。

k 要验证配置信息是否正确，请键入 show。检查所有信息是否都正确无误。

l 要退出会话，请键入 exit。

7 验证安装成功

Sensor 和 Manager 之间开始握手过程。这些设备将需要几秒来建立通信。

执行以下步骤验证 Sensor 与 Manager 之间的通信是否成功。

a 在 Sensor CLI 处键入：status。

将会显示状态报告

b 返回到 Manager。在“Manager Home page（Manager 主页）”的“System Health（系统健康状况）”部分中，查看 Manager 的状态。

Manager 的状态应该是 **up（打开）**，而 Sensor 的状态应该是 **active（活动）**。

c 在“Manager Home page（Manager 主页）”中，单击“Configure（配置）”以打开“Configuration（配置）”页。

d 选择已添加的 Sensor：“Device List（设备列表）” | “Sensor_Name（Sensor 名称）”。此 Sensor 的端口将显示在“Sensor_Name（Sensor 名称）”节点下。

“Device_Name（设备名称）”指示已添加的 Sensor 的名称。

e 选择“Device List（设备列表）” | “Device_Name（设备名称）” | “Port Settings（端口设置）”。

f 单击代表已连接电缆的 Sensor 上的端口的按钮。确保您的端口设置与电缆连接相匹配。

8 Sensor 已启动且正在运行！

您的 Sensor 正在监控已连接的网段并与 Manager 进行通信来执行管理操作。

a 有关系统的概述，请阅读《“McAfee Network Security Platform 快速导览”》。有关详细的使用说明，请参阅《“McAfee Network Security Platform 安装手册”》和《“McAfee Network Security Platform IPS 管理手册”》，或单击 Manager 中每个窗口右上角的 “Detailed Help” (详细帮助) 按钮。

b 从“Home（主页）Threat Analyzer”启动“Threat Analyzer”，以便在检测到攻击时查看警报统计数据。这些统计数据将显示在“Manager Home（Manager 主页）”的“Unacknowledged Alert Summary（未确认的警报摘要）”区域中。

c 遇到问题？有关故障排除信息，请查阅“McAfee Network Security Platform 故障排除手册”。

d 请注意，引发大多数部署问题的原因都在于 Sensor 和它连接到的网络设备之间的配置不符。请检查这两台设备的双工和自动协商设置，以确保它们同步。

如果需要与技术支持联系，请转至 https://mysupport.mcafee.com。

版权所有 © 2017 McAfee, LLC
McAfee 及其徽标是 McAfee, LLC 或其子公司在美国和其他国家/地区的商标或注册商标。 其他商标和品牌可能为其他实体所有。

McAfee
Together is power.