Management Center Virtual 初始设置

本章描述部署Management Center Virtual 设备之后，需要执行的初始设置过程。

管理中心 使用 CLI 对 6.5 及更高版本进行初始设置

部署 Management Center Virtual 后，您可以i访问设备控制台进行初始设置。作为使用 Web 界面的替代方法，您可以使用 CLI 执行初始设置。您必须完成初始配置向导来配置新设备，以便在受信任的管理网络上进行通信。向导需要您更改管理员密码并接受最终用户许可协议 (EULA) 并更改管理员密码。

开始之前

- 请确保您拥有 Management Center Virtual 在您的管理网络上通信所需的以下信息：
  - IPv4 管理 IP 地址。

    管理中心 接口已预配置为接受 DHCP 分配的 IP4 地址。要确定您的 DHCP 已配置什么 IP 地址来分配 管理中心 MAC 地址，请咨询您的系统管理员。在 DHCP 不可用的情况下，管理中心 接口使用 IPv4 地址 192.168.45.45。
  - 网络掩码和默认网关（如果不使用 DHCP）。

过程

步骤 1 在设备控制台使用**管理员**帐户（用户名：**admin**，密码：**Admin123**）登录到 Management Center Virtual。注意密码区分大小写。

步骤 2 在出现提示时，按 **Enter** 以显示最终用户许可协议 (EULA)。

步骤 3 审查 the EULA。在出现提示时，输入 **yes**、**YES**，或按 **Enter** 接受 EULA。

重要事项
不接受 EULA 您无法继续。如果您回复 **yes**、 **YES** 或 **Enter** 以外的内容，系统会将您注销。

步骤 4 为了确保系统安全和隐私，您第一次登录 管理中心 时，必须更改 **admin** 密码。当系统提示您设置新密码时，输入符合所示限制的新密码，然后在系统提示确认时再次输入相同的密码。

注释
管理中心 会将您的密码与密码破解词典进行比较，该词典不仅会检查许多英语词典单词，还会检查其他容易被常用密码破解技术破解的字符串。例如，初始配置脚本可能会拒绝 "abcdefg" 或 "passw0rd" 等密码。

注释
完成初始配置过程后，系统会将两个 **admin** 帐户（一个用于 Web 访问，另一个用于 CLI 访问）的密码设置为相同的值，符合您版本的《*Cisco Secure Firewall Management Center* 管理指南》中所述的强密码要求。如果您在此后更改任一 **admin** 帐户的密码，两个密码将不再相同，并且强密码要求可以从 Web 界面 **admin** 帐户中删除。

步骤 5 回答提示以配置网络设置。

按照提示操作时，如遇单选问题，选项会列在括号内，例如 **(y/n)**。默认值会列在方括号内，例如 **[y]**。回复提示时注意以下要点：

- 按 **Enter** 接受默认值。
- 对于主机名，请提供完全限定域名（<主机名>．<域>）或主机名。此栏必填。
- 如果使用 DHCP，则必须使用 DHCP 预留，因此分配的地址不会更改。如果 DHCP 地址更改，设备注册将失败，因为 管理中心 网络配置不同步。要从 DHCP 地址更改中恢复，请连接到 管理中心（使用主机名或新 IP 地址）并导航至**系统 (System)** > **配置 (Configuration)** > **管理接口 (Management Interfaces)**以重置网络。
- 如果您选择手动配置 IPv4 ，系统会提示您设置 IPv4 d地址、网络掩码和默认网关。
- 可以配置DNS服务器；要指定无DNS服务器，输入**none**。否则，指定一个或两个DNS服务器的IPv4地址。如果指定两个地址，请用逗号将它们分隔开来。（如果指定两台以上的DNS服务器，系统将忽略其他条目。）如果 管理中心 不能访问互联网，您将无法使用本地网络之外的 DNS。

  注释
  如果使用的是评估许可证，则这一次指定 DNS 是可选操作，但使用永久许可证进行部署时必须有 DNS。

- 您必须输入至少一个通过您网络可到达的完全限定域名 or IP 地址。（如果未使用 DHCP，则不能指定 NTP 服务器的FQDN。）您可以指定两个服务器（一个主服务器，一个辅助服务器）；用逗号将它们的信息分隔开。（如果指定两台以上的 DNS 服务器，系统将忽略其他条目。）如果 管理中心 不能访问互联网，您将无法使用本地网络之外的 NTP 服务器。

示例：

```
Enter a hostname or fully qualified domain name for this system [firepower]: fmc
Configure IPv4 via DHCP or manually? (dhcp/manual) [DHCP]: manual
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.0.66
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.224
Enter the IPv4 default gateway for the management interface [ ]: 10.10.0.65
Enter a comma-separated list of DNS servers or 'none' [CiscoUmbrella]: 208.67.222.222,208.67.220.220
Enter a comma-separated list of NTP servers [0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org]:
```

步骤 6 系统会显示配置选项的摘要。检查输入的设置。

示例：

```
Hostname:                             fmc
IPv4 configured via:                  manual configuration
Management interface IPv4 address:   10.10.0.66
Management interface IPv4 netmask:   255.255.255.224
Management interface IPv4 gateway:   10.10.0.65
DNS servers:                          208.67.222.222,208.67.220.220
NTP servers:                          0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org
```

步骤 7 最后的提示会让您确认设置。

- 如果设置正确，输入 **y**，然后按 **Enter**键接受设置并继续。
- 如果设置不正确，输入 **n**，然后按 **Enter**键。系统再次提示设置信息，从主机名开始。

示例：

```
Are these settings correct? (y/n) y
If your networking information has changed, you will need to reconnect.

Updated network configuration.
```

步骤 8 在接受设置后，您可以输入 **exit** 退出 管理中心 CLI。

下一步做什么

- 您可以使用刚才配置的网络信息连接到 Management Center Virtual Web 界面。
- 查看初始配置过程中 管理中心 自动配置的每周维护活动。这些活动旨在使系统保持最新状态并备份您的数据。请参阅检查版本6.5 及更高版本的自动初始配置 ， 第 6 页。

在 Web 界面上执行初始设置（6.5 和更高版本）

在部署 Management Center Virtual 后，则可以在设备 Web 界面上使用 HTTPS 执行初始设置。

第一次登录 管理中心 Web 界面时，管理中心 将显示初始配置向导，可让您快速轻松地配置设备的基本设置。此向导包含三个屏幕和一个弹出对话框：

- 第一个屏幕会强制您将 **admin** 用户的密码从默认值 **Admin123** 改为其他密码。
- 第二个屏幕显示最终用户许可协议 (EULA)，必须接受该协议才能使用设备。
- 第三个屏幕允许您更改设备管理接口的网络设置。此页面预先填充了当前设置，您可以更改。
- 向导将对您在此屏幕上输入的值执行验证，以确认以下内容：
  - 语法正确性

- 输入值的兼容性（例如，在使用 FQDN 指定 NTP 服务器时提供的兼容 IP 地址和网关或 DNS）
- Management Center Virtual 与 DNS 和 NTP 服务器之间的网络连接

向导会在屏幕上实时显示这些测试的结果，您可以先更正并测试配置的可行性，再单击屏幕底部的**完成**。NTP 和 DNS 连接测试无阻塞；在向导完成连接测试之前，您可以单击**完成**。如果系统在单击**完成**后报告连接问题，则无法更改向导中的设置，但在完成初始设置后，您可以使用 Web 界面配置这些连接。

如果您输入的配置值会导致 Management Center Virtual 和浏览器之间的现有连接中断，系统不会执行连接测试。在这种情况下，向导不会显示 DNS 或 NTP 的连接状态信息。

- 在三个向导屏幕上完成操作后，系统会弹出一个对话框，您可以快速轻松地在该对话框中设置智能许可。

完成初始配置向导并完成或退出“智能许可”对话框后，系统将显示您的版本对应的《Cisco Secure Firewall Management Center 设备配置指南》的“设备管理”中所述的设备管理页面。

开始之前

- 请确保您拥有 管理中心 在您的管理网络上通信所需的以下信息：
  - IPv4 管理 IP 地址。

    管理中心 接口已预配置为接受 DHCP 分配的 IP4 地址。要确定您的 DHCP 已配置什么 IP 地址来分配 管理中心 MAC 地址，请咨询您的系统管理员。在 DHCP 不可用的情况下，管理中心 接口使用 IPv4 地址 192.168.45.45。
  - 网络掩码和默认网关（如果不使用 DHCP）。
- 如果未使用 DHCP，请使用以下网络设置配置本地计算机：
  - IP 地址：192.168.45.2
  - 子网掩码：255.255.255.0
  - 默认网关：192.168.45.1

  禁用此计算机上的任何其他网络连接。

过程

步骤 1 使用网络浏览器导航到 Management Center Virtual 的 IP 地址：*https://<Management Center-IP>*。

随即显示登录页面。

步骤 2 使用以下管理员帐户登录到 Management Center Virtual：用户名 **admin**，密码 **Admin123**。密码区分大小写。

步骤 3 在**更改密码**屏幕：

a) （可选）选中**显示密码**复选框可在使用此屏幕时查看密码。
b) 单击**生成密码**按钮，让系统为您创建符合所列条件的密码。（生成的密码是非助记密码；如果您选择此选项，请仔细记下密码。）
c) 要设置您选择的密码，在**新密码 (New Password)** 和**确认密码 (Confirm Password)** 文本框中输入新密码。

密码必须符合对话框中列出的条件。

注释
管理中心会将您的密码与密码破解词典进行比较，该词典不仅会检查许多英语词典单词，还会检查其他容易被常用密码破解技术破解的字符串。例如，初始配置脚本可能会拒绝 "abcdefg" 或 "passw0rd" 等密码。

注释
完成初始配置过程后，系统会将两个 **admin** 帐户（一个用于 Web 访问，另一个用于 CLI 访问）的密码设置为相同的值。密码必须符合您的版本对应的《Cisco Secure Firewall Management Center 管理指南》中所述的强密码要求。如果您在此后更改任一 **admin** 帐户的密码，两个密码将不再相同，并且强密码要求可以从 Web 界面 **admin** 帐户中删除。

d) 单击**下一步**。

在**更改密码**屏幕上单击**下一步**后，向导已接受新的 **admin** 密码，即使您未完成剩余的向导活动，该密码也对 Web 界面和 CLI **admin** 帐户有效。

步骤 4 在**用户协议**屏幕阅读 EULA，然后单击**接受**继续。

如果单击**拒绝**，向导会将您从 Management Center Virtual 中注销。

步骤 5 单击**下一步**。

步骤 6 在**更改网络设置**屏幕：

a) 输入**完全限定域名**。如果显示默认值，并且与您的网络配置兼容，则您可以使用该值。否则，输入完全限定域名（语法<主机名>.<域>）或主机名。
b) 选择**配置 IPv4 (Configure IPv4)** 选项的引导协议：**使用 DHCP (Using DHCP)** 或**使用静态/手动 (Using Static/Manual)**。

如果使用 DHCP，则必须使用 DHCP 预留，因此分配的地址不会更改。如果 DHCP 地址更改，设备注册将失败，因为 管理中心 网络配置不同步。要从 DHCP 地址更改中恢复，请连接到 管理中心（使用主机名或新 IP 地址）并导航至**系统 (System)** > **配置 (Configuration)** > **管理接口 (Management Interfaces)**以重置网络。

c) 对于 **IPv4 地址**，接受显示的值（如果显示），或输入新值。使用点分十进制格式（例如 192.168.45.45）。

注释
如果在初始配置期间更改 IP 地址，则需要使用新的网络信息重新连接到 管理中心。

d) 接受显示的**网络掩码**值（如果有显示）或输入新值。使用点分十进制格式（例如 255.255.0.0）。

注释
如果在初始配置期间更改网络掩码，则需要使用新的网络信息重新连接到 管理中心。

e) 您可以接受显示的**网关**值（如果有显示）或输入新的默认网关。使用点分十进制格式（例如 192.168.0.1）。

注释
如果在初始配置期间更改网关地址，则可能需要使用新的网络信息重新连接到 管理中心。

f) （可选）对于**DNS 组**接受默认值 **Cisco Umbrella DNS**。

要更改 DNS 设置，从下拉列表中选择**自定义 DNS 服务器 (Custom DNS Servers)**，然后输入**主 DNS (Primary DNS)** 和**辅助 DNS (Secondary DNS)** 的 IPv4 地址。如果 管理中心 不能访问互联网，您将无法使用本地网络之外的 DNS。从下拉列表中选择**自定义 DNS 服务器 (Custom DNS Servers)**，并将**主 DNS (Primary DNS)** 和**辅助 DNS (Secondary DNS)** 字段留空，不配置 DNS 服务器。

注释
如果使用 FQDN 而不是 IP 地址来指定 NTP 服务器，则必须在此时指定 DNS。如果您使用评估许可证，则 DNS 是可选的，但需要 DNS 才能使用永久许可证进行部署。

g) 对于 **NTP 组服务器**，您可以接受默认值**默认 NTP 服务器**。在这种情况下，系统会将 **0.sourcefire.pool.ntp.org** 用作主 NTP 服务器，将 **1.sourcefire.pool.ntp.org** 用作辅助 NTP 服务器。

要配置其他 NTP 服务器，从下拉列表中选择**自定义 NTP 组 服务器 (Custom NTP Group Servers)**，然后输入一个或两个从您的网络可到达的 FQDN 或 IP 地址。如果 管理中心 不能访问互联网，您将无法使用本地网络之外的 NTP 服务器。

注释
如果在初始配置期间更改网络设置，则需要使用新的网络信息重新连接到 管理中心。

步骤 7 单击**完成**。

向导会对您在此屏幕上输入的值，以确认语法正确性、输入值的兼容性，以及 管理中心 和 DNS 及 NTP 服务器之间的连接性。如果系统在单击**完成**后报告连接问题，则无法更改向导中的设置，但在完成初始设置后，您可以使用 管理中心 Web 界面配置这些连接。

下一步做什么

- 系统会显示弹出对话框，您可以快速、轻松地设置 Smart Licensing。此对话框供选择性使用；如果您的 Management Center Virtual 将管理 威胁防御，并且您熟悉智能许可，请使用此对话框。否则，请关闭此对话框，并参阅您的版本对应的《Cisco Secure Firewall Management Center 管理指南》中的“许可”。
- 查看初始配置过程中 管理中心 自动配置的每周维护活动。这些活动旨在使系统保持最新状态并备份您的数据。请参阅检查版本6.5 及更高版本的自动初始配置，第 6 页。
- 完成初始配置向导并完成或退出“智能许可”对话框后，系统将显示《*Cisco Secure Firewall Management Center* 设备配置指南》中所述的设备管理页面。

检查版本6.5 及更高版本的自动初始配置

在初始化配置期间（无论是通过初始配置向导还是通过 CLI 执行），管理中心 都会自动配置维护任务，使系统保持最新状态并持续备份您的数据。

这些任务计划为 UTC，这意味着在本地发生时，取决于日期和您的特定位置。此外，由于任务是以 UTC 为单位进行计划的，因此它们不会针对夏令时、夏季时间或您在地点可能观察到的任何季节性调整进行调整。如果受影响，则根据当地时间，计划任务会在夏天比冬季“晚”一个小时开始。

注释 我们强烈建议您查看自动安排的配置，确认 管理中心 已成功建立这些配置，并在必要时进行调整。

- 每周 GeoDB 更新

  管理中心 会自动安排每周在同一随机选择的时间进行 GeoDB 更新。您可以使用 Web 界面消息中心观察此更新的状态。您可以在 **系统** > **更新** > **地理位置更新**>**周期性地理位置更新**下看到此自动更新的配置。如果系统无法配置更新，并且您的管理中心有互联网访问权限，我们建议您根据您的版本对应的《Cisco Secure Firewall Management Center 管理指南》中所述，配置常规 GeoDB 更新。

- 每周 管理中心 软件更新

  管理中心会自动安排每周任务，以下载管理中心及其托管设备的最新软件。此任务计划在UTC星期天凌晨 2 点至 3 点之间进行； 根据日期和您的特定位置，这可能在当地时间星期六下午至星期日下午的任何时间发生。您可以使用 Web 界面消息中心观察此任务的状态。您可以在 **系统** > **工具** > **计划** 下的 Web 界面中看到此任务的配置。如果任务计划失败且 管理中心 有互联网访问权限，我们建议您安排一个周期性任务来下载软件更新，如您的版本对应的《Cisco Secure Firewall Management Center 管理指南》中所述。

  此任务仅下载设备当前正在运行的版本的软件修补程序和修补程序更新；您有责任安装此任务下载的所有更新。有关详细信息，请参阅《*Cisco* 管理中心 升级指南》。

- 每周 管理中心 配置备份

  管理中心 会自动安排每周任务，在 UTC 星期一的早上凌晨 2 点执行本地存储的仅配置备份；根据日期和您的具体位置，这可能发生在当地时间星期六下午至星期日下午的任何时间。您可以使用 Web 界面消息中心观察此任务的状态。您可以在 **系统** > **工具** > **计划** 下的 Web 界面中看到此任务的配置。如果任务计划失败，我们建议您安排定期任务来执行备份，如您的版本对应的《Cisco Secure Firewall Management Center 管理指南》中所述。

- 漏洞数据库更新

  在版本 6.6+ 中，管理中心 从 Cisco 支持站点下载并安装最新的漏洞数据库 (VDB) 更新。这是一次性操作。您可以使用 Web 界面消息中心观察此更新的状态。为使您的系统保持最新状态，如果您的 管理中心 已接入互联网，我们建议您安排自动定期下载和安装 VDB 更新的任务，如您的版本对应的《Cisco Secure Firewall Management Center 管理指南》中所述。

- 每日入侵规则更新

  在版本 6.6+ 中，管理中心 从 Cisco 支持站点配置每日自动入侵规则更新。当 管理中心 下一次部署受影响的策略时，将向受影响的受管设备部署自动化入侵规则更新。您可以使用 Web 界面消息中心观察此任务的状态。您可以在 **系统** > **更新** > **规则更新** 下的 Web 界面中看到此任务的配置。如果配置更新失败且管理中心可以访问互联网，我们建议您配置定期入侵规则更新，如您的版本对应的《Cisco Secure Firewall Management Center 管理指南》中所述。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。