Cisco Secure Firewall 迁移工具使用入门

关于 Cisco Secure Firewall 迁移工具

本指南包含有关如何下载 Cisco Secure Firewall 迁移工具和完成迁移的信息。此外，它还提供故障排除提示，以便帮助您解决可能遇到的迁移问题。

本书中包含的迁移程序示例（迁移示例：FDM 托管设备到 Threat defense 2100）有助于对迁移过程的理解。

Cisco Secure Firewall 迁移工具会将支持的 FDM 托管设备配置转换为支持的 威胁防御 平台。Cisco Secure Firewall 迁移工具允许您将支持的 FDM 托管设备功能和策略自动迁移到 威胁防御。您必须手动迁移所有不支持的功能。

Cisco Secure Firewall 迁移工具收集 FDM 托管设备信息、解析相关信息，最后将它推送到 Cisco Secure Firewall Management Center。在解析阶段中，Cisco Secure Firewall 迁移工具会生成**迁移前报告**，其中会列明以下各项：

- 已完全迁移、部分迁移、迁移不支持和迁移中忽略的 FDM 托管设备配置项目。
- 出错的 FDM 托管设备配置行，列出 Cisco Secure Firewall 迁移工具无法识别的 FDM 托管设备组件；这些配置行会阻止迁移。

控制台

当您启动 Cisco Secure Firewall 迁移工具时，系统将打开控制台。控制台提供有关 Cisco Secure Firewall 迁移工具中各步骤进度的详细信息。控制台的内容也会写入 Cisco Secure Firewall 迁移工具日志文件。

在打开和运行 Cisco Secure Firewall 迁移工具时，控制台必须保持打开状态。

重要事项 当您通过关闭运行 Web 界面的浏览器退出 Cisco Secure Firewall 迁移工具时，控制台会继续在后台运行。要完全退出 Cisco Secure Firewall 迁移工具，请按键盘上的 Command 键 + C 退出控制台。

日志

Cisco Secure Firewall 迁移工具会为每个迁移创建日志。这些日志包含每个迁移步骤中所发生事件的详细信息，如果迁移失败，可以帮助您确定失败的原因。

在以下位置可找到 Cisco Secure Firewall 迁移工具的日志文件：`<migration_tool_folder>\logs`

资源

Cisco Secure Firewall 迁移工具会在 `resources` 文件夹中保存一份**迁移前报告**、**迁移后报告**、 FDM 托管设备配置和日志。

在以下位置可找到 `resources` 文件夹：`<migration_tool_folder>\resources`

未解析文件

在以下位置可找到未解析文件：`<migration_tool_folder>\resources`

Cisco Secure Firewall 迁移工具中的搜索

可以搜索 Cisco Secure Firewall 迁移工具中所显示表格中的项目，例如**优化**、**检查和验证**页面上的项目。

要搜索表格的任何列或行中的项目，请点击表格上方的**搜索**（ ），然后在字段中输入搜索词。Cisco Secure Firewall 迁移工具会筛选表格行，并仅显示包含搜索词的那些项目。

要搜索单列中的项目，请在相应列标题中提供的**搜索**字段中输入搜索词。Cisco Secure Firewall 迁移工具会筛选表格行，并仅显示匹配搜索词的那些项目。

端口

在以下 12 个端口之一上运行时，Cisco Secure Firewall 迁移工具支持遥测：端口 8321-8331 和端口 8888。默认情况下，Cisco Secure Firewall 迁移工具使用端口 8888。要更改端口，请更新 `app_config` 文件中的端口信息。更新后，请确保重新启动 Cisco Secure Firewall 迁移工具，以使端口更改生效。在以下位置可找到 `app_config` 文件：`<migration_tool_folder>\app_config.txt`。

注释 我们建议您使用端口 8321-8331 和端口 8888，因为只有这些端口支持遥测。如果启用思科成功网络，则无法将任何其他端口用于 Cisco Secure Firewall 迁移工具。

思科成功网络

思科成功网络是一项用户启用的云服务。启用思科成功网络时，Cisco Secure Firewall 迁移工具与思科云之间会建立安全连接以传输使用情况信息和统计信息。数据流遥测提供一种机制，可从 Cisco Secure Firewall 迁移工具选择感兴趣的数据，并以结构化的格式将其传输至远程管理站，从而获得以下优势：

- 通知您在网络中可用来改进产品效果的未使用功能。
- 通知您适用于您产品的其他技术支持服务和监控。
- 帮助思科改善我们的产品。

Cisco Secure Firewall 迁移工具将建立并维护该安全连接，使您能够注册思科成功网络。您可以通过禁用思科成功网络随时关闭此连接，这样会将设备与思科成功网络云断开。

Cisco Secure Firewall 迁移工具的新功能

版本	支持的功能
4.0.1	Cisco Secure Firewall 迁移工具 4.0.1 包括以下新功能和增强功能： Cisco Secure Firewall 迁移工具现在会根据名称和配置来分析所有对象和对象组，并重新使用具有相同名称和配置的对象。之前只会根据名称和配置对网络对象和网络对象组进行分析。请注意，远程访问 VPN 中的 XML 配置文件仍仅使用其名称进行验证。

版本	支持的功能
4.0	Cisco Secure Firewall 迁移工具 4.0 支持： 如果目标管理中心版本为 7.3 或更高版本且源设备管理器版本为 7.2 或更高版本，则可将 FDM 托管设备迁移到管理中心。 设备管理器的版本必须等于或低于目的管理中心的版本。 以下选项可用于迁移： 1. **迁移 Firepower 设备管理器（仅限共享配置）**：此选项允许您分阶段迁移。在这种情况下，您可以一开始迁移所有共享配置，并等到以后再根据您的要求来迁移设备配置。在迁移过程中，只有共享配置会被迁移到目标管理中心。可以上传从设备管理器获取的配置捆绑包，也可以为工具提供设备管理器凭证以获取配置详细信息。首选方法是自动获取配置详细信息。 2. **迁移 Firepower 设备管理器（包括设备和共享配置）**：此选项允许您将设备和共享配置从设备管理器迁移到目标管理中心。在将源设备及其配置迁移到目标管理中心后，FDM 托管设备就会成为目标管理中心设备。要使工具获取配置详细信息，您必须提供设备管理器凭证。此迁移选项仅允许自动获取配置。 3. **将 Firepower 设备管理器（包括设备和共享配置）迁移到 FTD 设备（新硬件）**：此选项允许您将设备和共享配置迁移到由目标管理中心管理的威胁防御设备。在这种情况下，迁移过程中不会迁移源设备，而只会将设备配置迁移到新的威胁防御设备。可以上传从设备管理器获取的配置捆绑包，也可以为工具提供设备管理器凭证以获取配置详细信息。首选方法是自动获取配置详细信息。

Cisco Secure Firewall 迁移工具的平台要求

Cisco Secure Firewall 迁移工具对基础设施和平台的要求如下：

- 运行 Microsoft Windows 10 64 位操作系统或者 macOS 10.13 或更高版本
- 使用 Google Chrome 作为系统默认浏览器
- (Windows)“电源和睡眠”中的“睡眠”设置配置为“从不让 PC 进入睡眠”，以便在大型迁移推送时系统不会进入睡眠状态
- (macOS) 配置了“节能模式”设置，以便在大型迁移推送时计算机和硬盘不会进入睡眠状态

FDM 托管设备配置文件的要求和前提条件

您可以手动获取 FDM 托管设备配置捆绑包，也可以通过从 Cisco Secure Firewall 迁移工具连接到实时 FDM 托管设备来获取 FDM 托管设备配置捆绑包。仅以下选项支持手动上传：

- 将 Firepower 设备管理器（包括设备和共享配置）迁移到 FTD 设备（新硬件）
- 迁移 Firepower 设备管理器（仅限共享配置）

注释 **迁移 Firepower 设备管理器（包括设备和共享配置）**选项不支持手动上传。

您手动导入到 Cisco Secure Firewall 迁移工具中的 FDM 托管设备配置捆绑包必须满足以下要求：

- 仅包含有效的设备管理器 CLI 配置。
- 包括版本号。
- 配置捆绑包应为 .zip 格式。
- 具有从设备管理器导出的完全导出的配置，请参阅导出 FDM 托管设备配置文件，第 28 页。
- 至少需要一个包含配置的 .txt 文件。
- 应为加密捆绑包提供密钥。对于未加密的捆绑包，加密密钥可以留空。
- 不包含语法错误。
- 尚未手工编码或手动更改。

威胁防御设备的要求和前提条件

当您迁移到管理中心时，它可能已添加目标威胁防御设备，也可能未添加。您可以将共享策略迁移到管理中心，以便将来部署到威胁防御设备。要将设备特定的策略迁移到威胁防御，必须将其添加到管理中心。当您计划将 FDM 托管设备配置迁移到威胁防御时，请考虑以下要求和前提条件：

- 威胁防御硬件必须大于或等于 FDM 托管设备型号。例如，如果源 FDM 托管设备型号为 2100，则目标威胁防御型号可以是 2100、3100、4100 或 9300，而不能是任何低于 2100 的型号。
- 目标威胁防御设备必须向管理中心注册。
- 威胁防御设备可以是独立设备或容器实例。它不能是集群或高可用性配置的一部分。
  - 目标本地威胁防御设备必须至少具有与 FDM 托管设备相同数量的已使用物理数据和端口通道接口（不包括“管理专用”和子接口）；否则，必须在目标威胁防御设备上添加所需类型的接口。子接口由 Cisco Secure Firewall 迁移工具根据物理或端口通道映射创建。

- 如果目标威胁防御设备是容器实例，则必须至少具有与FDM托管设备相同数量的已使用物理接口、物理子接口、端口通道接口和端口通道子接口（不包括“管理专用”接口）；否则，必须在目标威胁防御设备上添加所需类型的接口。

注释
- Cisco Secure Firewall 迁移工具不创建子接口，仅允许接口映射。
- 它允许不同接口类型之间的映射，例如：物理接口可以映射到端口通道接口。

FDM 托管设备配置支持

支持的 FDM 托管设备配置

Cisco Secure Firewall 迁移工具可完整迁移以下 FDM 托管设备配置：

- 网络对象和组
- 服务对象，为源和目的配置的服务对象除外

注释 虽然Cisco Secure Firewall迁移工具不会迁移扩展服务对象（配置了源和目标），参考的 ACL 和 NAT 规则及其所有功能都会被迁移。

- 服务对象组，嵌套服务对象组除外

注释 由于 管理中心 不支持嵌套，因此 Cisco Secure Firewall 迁移工具会扩展引用规则的内容。但是，系统会迁移规则及完整功能。

- IPv4 和 IPv6 FQDN 对象与组
- IPv6 转换支持（接口、静态路由、对象、ACL 和 NAT）
- 访问控制策略
- 自动 NAT 和手动 NAT
- 静态路由、ECMP 路由
- 物理接口
- FDM 托管设备接口上的辅助 VLAN 不会被迁移到 威胁防御。
- 子接口（子接口 ID 在迁移时始终设置为与 VLAN ID 相同的编号）

- 端口通道
- 虚拟隧道接口 (VTI)
- 网桥组（仅限透明模式）
- IP SLA 监控器

  Cisco Secure Firewall 迁移工具创建 IP SLA 对象，映射对象与特定静态路由，并将对象迁移到管理中心。

  IP SLA 监控器定义了受监控 IP 地址的连接策略并跟踪 IP 地址路由的可用性。通过发送 ICMP 回应请求并等待响应，定期检查静态路由的可用性。如果回应请求超时，静态路由将从路由表中删除并使用备份路由来替换。SLA 监控作业在部署后立即开始并持续运行，除非您从设备配置移除 SLA 监控器，即监控器并未过期。IP SLA 监控器对象用在 IPv4 静态路由策略的“路由跟踪”(Route Tracking) 字段中。IPv6 路由无法选择通过路由跟踪使用 SLA 监控器。

- 对象组搜索

  启用对象组搜索可以降低包含网络对象的访问控制策略的内存要求。我们建议您在威胁防御上启用对象组搜索，以通过访问策略提高内存利用率。

注释

- 对象组搜索不适用于 管理中心 或 威胁防御 6.6 之前的版本。
- 共享配置流将不支持对象组搜索，并且会被禁用。
- 基于时间的对象

- 基于时间的对象

  当 Cisco Secure Firewall 迁移工具检测到通过访问规则引用的基于时间的对象时，Cisco Secure Firewall迁移工具会迁移基于时间的对象并映射这些对象与相应的访问规则。根据**检查和验证配置**页面中的规则验证对象。

  基于时间的对象属于允许基于时间段进行网络访问的访问列表类型。如果您必须根据一天中的特定时间或一周中的特定天数限制出站或入站流量，则它非常有用。

注释 您必须将时区配置从源 FDM 托管设备手动迁移到目标 FTD。

- 站点间 VPN 隧道
  - 站点间 VPN - 当 Cisco Secure Firewall 迁移工具检测到源 FDM 托管设备中的加密映射配置时，Cisco Secure Firewall 迁移工具会将加密映射作为点对点拓扑迁移到 管理中心 VPN。
  - FDM 托管设备的基于加密映射（静态/动态）的 VPN
  - 基于路由 (VTI) 的 FDM VPN
  - 源于 FDM 托管设备的基于证书的 VPN 迁移

- FDM 托管设备信任点或证书到 管理中心 的迁移必须手动执行，并且是迁移前活动的一部分。

- 动态路由对象、BGP 和 EIGRP
  - Policy-List
  - Prefix-List
  - 社区列表
  - 自治系统 (AS) 路径
- 远程接入 VPN
  - SSL 和 IKEv2 协议。
  - 身份验证方式 - 仅 AAA、仅客户端证书、SAML、AAA 和客户端证书。
  - AAA - Radius、本地、LDAP 和 AD。
  - 连接配置文件、组策略、动态访问策略、LDAP 属性映射和证书映射。
  - 标准和扩展ACL。
  - 作为迁移前活动的一部分，请执行以下操作：
    - 将 FDM 托管设备信任点作为 PKI 对象手动迁移到 管理中心。
    - 从源 FDM 托管设备检索 AnyConnect 软件包、Hostscan 文件（Dap.xml、Data.xml、Hostscan 软件包）、外部浏览器软件包和 AnyConnect 配置文件。
    - 将所有 AnyConnect 软件包上传到 管理中心。
    - 将 AnyConnect 配置文件直接上传到 管理中心 或从 Cisco Secure Firewall 迁移工具上传。

部分支持的 FDM 托管设备配置

Cisco Secure Firewall 迁移工具部分支持以下 FDM 托管设备配置的迁移。其中一些配置包括含高级选项的规则，这些规则在迁移后失去这些选项。如果 管理中心支持这些高级选项，您可以在迁移完成后手动配置它们。

- 使用高级日志记录设置（例如严重性和时间间隔）配置的访问控制策略规则。
- 配置有跟踪选项的静态路由。
- 基于证书的 VPN 迁移。
- 动态路由对象、EIGRP 和 BGP
  - 路由映射

不支持的 FDM 托管设备配置

Cisco Secure Firewall 迁移工具不支持以下 FDM 托管设备配置的迁移。如果这些配置在 管理中心 中受支持，您可以在迁移完成之后手动配置它们。

- 基于 SGT 的访问控制策略规则
- 基于 SGT 的对象
- 基于用户的访问控制策略规则
- 配置有块分配选项的 NAT 规则
- 带有不受支持 ICMP 类型和代码的对象
- 基于隧道协议的访问控制策略规则

注释 支持在 Cisco Secure Firewall 迁移工具和 管理中心 6.5 上使用预过滤器。

- 配置有 SCTP 的 NAT 规则
- 配置有主机“0.0.0.0”的 NAT 规则
- 通过带 SLA 跟踪的 DHCP 或 PPPoE 获取的默认路由
- SLA 监控时间表
- 传输模式 IPsec 转换集
- FDM 托管设备信任点迁移到 管理中心
- 用于 BGP 的透明防火墙模式

FDM 托管设备和威胁防御中的对象

FDM 托管设备配置文件包含您可以迁移到威胁防御的以下对象：

- 网络对象
- 服务对象，在威胁防御中称为端口对象
- IP SLA 对象
- 基于时间的对象
- VPN 对象（IKEv1/IKEv2 策略、IKEv1/IKEv2 IPsec 提议）
- 动态路由对象（策略列表、前缀列表、社区列表、AS 路径、访问列表和路由映射）
- 路由模式下支持 BGP 和 EIGRP
- RA VPN 对象
- 组策略

- AAA 对象（Radius、SAML、本地领域、AD/LDAP/LDAPS 领域）
- 地址池（IPv4 和 IPv6）
- 连接配置文件
- LDAP 属性映射
- IKEv2 策略
- IKEv2 IPsec 提议
- 证书映射
- DAP
- 入侵策略
- 入侵规则

准则和限制

FDM 托管设备迁移准则

以下是使用 Cisco Secure Firewall 迁移工具迁移 FDM 托管设备配置的准则：

- 每个 FDM 托管设备对象具有唯一名称和配置 - Cisco Secure Firewall 迁移工具无需更改即可成功迁移对象。
- FDM 托管设备对象的名称包括一个或多个不受管理中心支持的特殊字符 - Cisco Secure Firewall 迁移工具会使用“_”字符来重命名对象名称中的特殊字符，以便满足管理中心对象命名条件。
- FDM 托管设备对象具有与管理中心中的现有对象相同的名称和配置 - Cisco Secure Firewall 迁移工具会重新使用威胁防御配置的管理中心对象，不迁移 FDM 托管设备对象。
- 多个 FDM 托管设备对象具有相同的名称，但使用不同的大小写 - Cisco Secure Firewall 迁移工具会重命名此类对象，以便满足威胁防御对象命名条件。

重要事项 Cisco Secure Firewall 迁移工具会分析所有对象和对象组的名称和配置。但是，远程访问 VPN 配置中的 XML 配置文件只会使用名称进行分析。

FDM 托管设备配置限制

对源 FDM 托管设备配置的迁移存在以下限制：

- 不受支持的对象和 NAT 规则不会被迁移。
- 不受支持的 ACL 规则将作为禁用的规则迁移到管理中心。

- 所有支持的 FDM 托管设备加密映射 VPN 都将作为管理中心点对点拓扑进行迁移。
- 不受支持或不完整的静态加密映射 VPN 拓扑不会被迁移。
- 您无法迁移某些FDM托管设备配置，例如，将动态路由迁移到威胁防御。手动迁移这些配置。
- 管理中心不支持嵌套服务对象组或端口组。在转换过程中，Cisco Secure Firewall 迁移工具会扩展引用的嵌套对象组或端口组的内容。
- Cisco Secure Firewall 迁移工具将一行中有源端口和目标端口的扩展服务对象或组拆分为跨多行的不同对象。对此类访问控制规则的引用将转换为具有完全相同含义的管理中心规则。
- 如果源 FDM 托管设备配置具有不引用特定隧道协议（例如 GRE、IP-in-IP 和 IPv6-in-IP）的访问控制规则，但这些规则与 FDM 托管设备上的未加密隧道流量匹配，之后在迁移到威胁防御时，相应规则的行为方式将与在FDM托管设备上的行为方式有所不同。我们建议您在威胁防御的预过滤器策略中为它们创建特定的隧道规则。
- 支持的 FDM 托管设备加密映射都将作为点对点拓扑进行迁移。
- 如果在管理中心显示具有相同名称的 AS 路径对象，则迁移将停止，并显示以下错误消息：

  “在 管理中心 中检测到冲突的 AS 路径对象名称，请在 管理中心 中解决冲突以继续”
- 路由映射对象会使用 Cisco Secure Firewall 迁移工具部分迁移。由于 API 限制，不支持 match 和 set 子句。
- 由于 API 限制，第 7 层策略（例如身份策略、SSL 策略、恶意软件、文件策略、安全智能、SGT、基于用户的规则和平台设置）不会迁移。

RA VPN 迁移的限制

支持远程访问 VPN 迁移，但存在以下限制：

- 由于 API 限制，不支持自定义属性、SSL 设置和 VPN 负载均衡迁移。
- LDAP 服务器已迁移，加密类型为“none”。
- DfltGrpPolicy 不会迁移，因为该策略适用于整个 管理中心。您可以直接在 管理中心 上进行必要的更改。
- 对于 Radius 服务器，如果启用了动态授权，则 AAA 服务器连接应通过接口而不是动态路由。如果发现FDM托管设备配置启用了动态授权的AAA服务器而没有接口，则Cisco Secure Firewall迁移工具将忽略动态授权。在管理中心选择接口后，您必须手动启用动态授权。
- 在 RA VPN 策略下未启用绕过访问控制 sysopt permit-vpn 选项。但如有需要，您可以从管理中心启用它。
- 只有当配置文件被从 Cisco Secure Firewall 迁移工具上传到管理中心时，才能在组策略下更新 AnyConnect 客户端模块和配置文件值。
- 您需要直接在管理中心上映射证书。
- 默认情况下不会迁移 IKEv2 参数。您必须通过管理中心添加它们。

支持的迁移平台

以下 FDM 托管设备和 威胁防御 平台支持通过 Cisco Secure Firewall 迁移工具进行迁移。有关支持的威胁防御平台的更多信息，请参阅 Cisco Secure Firewall 兼容性指南 。

支持的源 FDM 托管设备平台

您可以使用 Cisco Secure Firewall 迁移工具从以下 FDM 托管设备平台迁移配置：

- Firepower 1000 系列
- Firepower 2100 系列
- Secure Firewall 3100 系列
- Firepower 4100 系列
- Firepower 9300 系列
- VMware、AWS、Azure、KVM 上的 FDM 虚拟

支持的目标 威胁防御平台

您可以使用 Cisco Secure Firewall 迁移工具将源 配置迁移到 威胁防御 平台的以下独立实例或容器实例：

- Firepower 1000 系列
- Firepower 2100 系列
- Secure Firewall 3100 系列
- Firepower 4100 系列
- Firepower 9300 系列包括：
  - SM-24
  - SM-36
  - SM-40
  - SM-44
  - SM-48
  - SM-56
- VMware 上的威胁防御，使用 VMware ESXi、VMware vSphere Web 客户端或 vSphere 独立客户端部署
- Microsoft Azure 云或 AWS 云上的 Threat Defense Virtual

注释

- 有关 Azure 中 threat defense virtual 的前提条件和预先配置，请参阅 Cisco Secure Firewall Threat Defense Virtual 和 Azure 入门。
- 有关 AWS 云中 threat defense virtual 的必备条件和预先配置，请参阅 Threat Defense Virtual 前提条件。

对于每一个这些环境，Cisco Secure Firewall 迁移工具在按照要求进行预先配置后，都需要网络连接才能连接到 Microsoft Azure 或 AWS 云中的 管理中心，然后再将配置迁移到云中的 管理中心。

注释 要成功迁移，必须在使用 Cisco Secure Firewall 迁移工具之前完成 管理中心 或威胁防御虚拟的预先配置前提条件。

支持的迁移目标管理中心

Cisco Secure Firewall 迁移工具支持迁移到管理中心托管的威胁防御设备以及云交付的防火墙管理中心。

管理中心

管理中心是一个功能强大的、基于 Web 的多设备管理器，它在自己的服务器硬件上运行，或者在虚拟机监控程序上作为虚拟设备运行。您可以使用本地和虚拟管理中心作为迁移的目标管理中心。

管理中心应满足以下迁移准则：

- 管理中心软件版本支持迁移，如支持迁移的软件版本，第 14 页中所述。
- 您已获取并安装 威胁防御 的智能许可证，包括您计划从 接口迁移的所有功能，如下所述：
  - Cisco.com 上的思科智能账户“入门指南”部分。
  - 在思科智能软件管理器中注册防火墙管理中心。
  - 许可防火墙系统

云交付的防火墙管理中心

云交付的防火墙管理中心是一个用于威胁防御设备的管理平台，它通过思科防御协调器 (CDO) 交付。云交付的防火墙管理中心提供了许多与管理中心相同的功能。

您可以从 CDO 访问云交付的防火墙管理中心。CDO 通过安全设备连接器 (SDC) 连接到云交付的防火墙管理中心。有关云交付的防火墙管理中心的更多信息，请参阅使用云交付的防火墙管理中心来管理 Cisco Secure Firewall Threat Defense 设备。

Cisco Secure Firewall 迁移工具支持将云交付的防火墙管理中心作为迁移的目标管理中心。要选择将云交付的防火墙管理中心作为迁移的目标管理中心，则需要添加 CDO 区域并从 CDO 门户生成 API 令牌。

CDO 区域

CDO 可用于三个不同的区域中，并且可以使用 URL 扩展名来标识这些区域。

表 *1: CDO* 区域和 *URL*

地区	CDO URL
欧洲地区	https://defenseorchestrator.eu/
美国地区	https://defenseorchestrator.com/
总裁	https://www.apj.cdo.cisco.com/

支持迁移的软件版本

以下是支持迁移的 Cisco Secure Firewall 迁移工具、 FDM 托管设备和 威胁防御 版本：

支持的 Cisco Secure Firewall 迁移版本

software.cisco.com 上发布的版本是我们的工程和支持组织正式支持的版本。我们强烈建议您从 software.cisco.com 下载最新版本的 Cisco Secure Firewall 迁移工具。以下是当前支持的可用版本：

- Cisco Secure Firewall 迁移工具 v 3.0.1
- Cisco Secure Firewall 迁移工具 v 3.0.2

Cisco Secure Firewall 迁移工具版本 3.0.1 目前已停止提供支持，并将从 software.cisco.com 中删除。

支持的 FDM 托管设备版本

Cisco Secure Firewall 迁移工具支持从运行威胁防御版本 7.2 及更高版本的 FDM 托管设备进行迁移。

源 FDM 托管设备配置支持的管理中心版本

对于 FDM 托管的设备，Cisco Secure Firewall 迁移工具支持迁移到由运行 7.2+ 版本的管理中心管理的威胁防御设备。

注释

- 某些功能仅在最新版本的管理中心和威胁防御中支持。
- 为获得最佳迁移时机，我们建议您将管理中心升级为 software.cisco.com/downloads 中提及的建议发行版本。

支持的 威胁防御版本

对于 FDM 托管设备，Cisco Secure Firewall 迁移工具支持迁移到运行威胁防御版本 7.2 及更高版本的设备。

有关思科防火墙软件和硬件兼容性的详细信息（包括 威胁防御的操作系统和托管环境要求），请参阅思科防火墙兼容性指南。

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。