# 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：Fortinet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 Fortinet 配置转换为支持的 Cisco Secure Firewall Threat Defense 平台。Cisco Secure Firewall 迁移工具允许您将支持的 Fortinet 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 Fortinet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 Fortinet 配置项目
- 出错的 Fortinet 配置行，列出 Cisco Secure Firewall 迁移工具无法识别的 Fortinet CLI；这些配置行会阻止迁移。

如果存在解析错误，您可以纠正问题，重新上传新配置，连接到目标设备，将接口映射到 威胁防御接口，映射应用，映射安全区，然后继续检查和验证您的配置。接下来即可将配置迁移到目标设备。

### 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**、 Fortinet 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

可在以下位置找到未解析文件：

*<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 |
| --- | --- |
| 6.0 | |

| 版本 | 支持的功能 |
| --- | --- |
| | 本版本包含以下新功能和增强功能<br><br>**Cisco Secure Firewall ASA 迁移到 Secure Firewall Threat Defense**<br><br>• 现在，您可以将安全防火墙 ASA 上的 WebVPN 配置迁移到威胁防御设备上的零信任访问策略配置。确保选中 **选择功能** 页面中的 **WebVPN** 复选框，并查看 **优化、查看和验证配置** 页面中的新 **WebVPN** 选项卡。威胁防御设备和目标管理中心必须在 7.4 或更高版本上运行，并且必须将 Snort3 作为检测引擎运行。<br><br>• 现在，您可以将简单网络管理协议 (SNMP) 和动态主机配置协议 (DHCP) 配置迁移到威胁防御设备。确保选中 **选择功能** 页面中的 **SNMP** 和 **DHCP** 复选框。如果您在安全防火墙 ASA 上配置了 DHCP，请注意，也可以选择迁移 DHCP 服务器或中继代理和 DDNS 配置。<br><br>• 现在，您可以在执行多情景 ASA 设备到单实例威胁防御合并情景迁移时迁移等价多路径 (ECMP) 路由配置。已解析摘要中的 **路由** 磁贴现在还包括 ECMP 区域，您可以在 **优化、查看和验证配置** 页面的 **路由** 选项卡下对其进行验证。<br><br>• 现在，您可以将动态隧道从安全防火墙 ASA 的动态虚拟隧道接口 (DVTI) 配置迁移到威胁防御设备。您可以在 **Map ASA Interfaces to Security Zones**、**Interface Groups, and VRFs** 页面中进行映射。确保您的 ASA 版本为 9.19 (x) 及更高版本，此功能才适用。<br><br>**FDM 托管设备迁移到 Cisco Secure Firewall Threat Defense**<br><br>• 现在，您可以将第 7 层安全策略（包括 SNMP 和 HTTP）以及恶意软件和文件策略配置从 FDM 管理的设备迁移到威胁防御设备。确保目标管理中心版本为 7.4 或更高版本，并且选中 **选择功能** 页面中的 **平台设置** 和 **文件和恶意软件策略** 复选框。<br><br>**Check Point 防火墙迁移到 Cisco Secure Firewall Threat Defense**<br><br>• 现在，您可以将 Check Point 防火墙上的站点间 VPN（基于策略）配置迁移到威胁防御设备。请注意，此功能适用于 Check Point R80 或更高版本，以及管理中心和威胁防御版本 6.7 或更高版本。确保在 **选择功能** 页面中选中 **站点间 VPN 隧道** 复选框。请注意，由于这是特定于设备的配置，因此如果您选择 **不使用 FTD 继续**，则迁移工具不会显示这些配置。<br><br>**Fortinet 防火墙迁移到 Cisco Secure Firewall Threat Defense**<br><br>• 现在，您可以在将配置从 Fortinet 防火墙迁移到威胁防御设备时优化应用访问控制列表 (ACL)。使用 **优化、查看和验证配置** 页面中的 **优化 ACL** 按钮查看冗余和影子 ACL 列表，并下载优化报告以查看详细的 ACL 信息。 |

| 版本 | 支持的功能 |
| --- | --- |
| 5.0.1 | 本版本包含以下新功能和增强功能：<br>• Cisco Secure Firewall 迁移工具现在支持将多个透明防火墙模式安全情景从 Cisco Secure Firewall ASA 设备迁移到威胁防御设备。您可以将 Cisco Secure Firewall ASA 设备中的两个或多个透明防火墙模式情景合并到一个透明模式实例，并进行迁移。<br>在一个或多个情景具有 VPN 配置的 VPN 配置的 ASA 部署中，您只能选择一个要将其 VPN 配置迁移到目标威胁防御设备的情景。在未选择的情景中，仅忽略 VPN 配置，并迁移所有其他配置。<br>有关详细信息，请参阅 选择 ASA 安全情景 。<br>• 您现在可以使用 Cisco Secure Firewall 迁移工具将站点间和远程访问 VPN 配置从 Fortinet 和 Palo Alto Networks 防火墙迁移到威胁防御。从 **选择功能** 窗格中，选择要迁移的 VPN 功能。请参阅使用迁移工具将 Palo Alto Networks 防火墙迁移到 Cisco Secure Firewall Threat Defense 和使用迁移工具 将 Fortinet 防火墙迁移到 Cisco Secure Firewall Threat Defense 指南中的指定 Cisco Secure Firewall 迁移工具的目标参数部分。<br>• 现在，您可以从 Cisco Secure Firewall ASA 设备中选择一个或多个路由或透明防火墙模式安全情景，并使用 Cisco Secure Firewall 迁移工具执行单情景或多情景迁移。 |
| 5.0 | • Cisco Secure Firewall 迁移工具现在支持将多个安全情景从 Cisco Secure Firewall ASA 迁移到威胁防御设备。您可以选择从其中一个情景迁移配置，也可以合并所有路由防火墙模式情景中的配置并进行迁移。即将推出对合并多个透明防火墙模式情景的配置的支持。有关详细信息，请参阅选择 ASA 主要安全情景。<br>• 迁移工具现在利用虚拟路由和转发 (VRF) 功能来复制在多情景 ASA 环境中观察到的隔离流量，这将是新合并配置的一部分。您可以在 **已解析摘要** 页面的新 **VRF 磁** 贴中检查迁移工具在新 **情景** 磁贴中检测到的情景数量。此外，迁移工具会在将接口映射 **到安全区域和接口组** 页面中显示这些 VRF 映射到的接口。<br>• 现在，您可以使用 Cisco Secure Firewall 迁移工具中的新演示模式尝试整个迁移工作流程，并直观地了解实际迁移的情况。有关详细信息，请参阅 使用防火墙迁移工具中的演示模式 。<br>• 借助新的增强功能和漏洞修复，Cisco Secure Firewall 迁移工具现在可提供改进、更快的迁移体验，用于将 Palo Alto Networks 防火墙迁移到威胁防御。 |

| 版本 | 支持的功能 |
|---|---|
| 4.0.3 | Cisco Secure Firewall 迁移工具 4.0.3 包括漏洞修补和以下新增强功能：<br>• 迁移工具现在提供增强的 **应用映射** 屏幕，用于将 PAN 配置迁移到威胁防御。有关详细信息，请参阅 使用迁移工具将 *Palo Alto Networks* 防火墙迁移到 *Cisco Secure Firewall Threat Defense* 指南中的映射 配置与应用 。 |
| 4.0.2 | Cisco Secure Firewall 迁移工具 4.0.2 包括以下新功能和增强功能：<br>• 迁移工具现在具有永远在线的遥测功能；但是，您现在可以选择发送有限或广泛的遥测数据。有限的遥测数据包含很少的数据点，而广泛的遥测数据会发送更详细的遥测数据列表。您可以从 **Settings** > **Send Telemetry Data to Cisco?** 。 |
| 3.0.1 | • 对于具有 FirePOWER 服务的 ASA、Check Point、Palo Alto Networks 和 Fortinet，仅支持将 Cisco Secure Firewall 3100 系列作为目标设备。 |
| 3.0 | 如果目标管理中心是 7.2 或更高版本，Cisco Secure Firewall 迁移工具 3.0 支持从 Fortinet 迁移到云交付的防火墙管理中心。 |
| 2.5.2 | Cisco Secure Firewall 迁移工具 2.5.2 支持从防火墙规则库中识别和隔离可优化（禁用或删除）的 ACL，而不会影响 Fortinet 防火墙的网络功能。<br>ACL 优化支持以下 ACL 类型：<br>• 冗余 ACL - 当两个 ACL 具有相同的配置和规则集时，删除非基本 ACL 并不会影响网络。<br>• 影子 ACL - 第一个 ACL 完全镜像第二个 ACL 的配置。<br>**注释** 优化仅适用于 ACP 规则操作的 Fortinet。<br>如果目标 管理中心 是 7.1 或更高版本，则 Cisco Secure Firewall 迁移工具 2.5.2 支持边界网关协议 (BGP) 和动态路由对象迁移。 |

| 版本 | 支持的功能 |
| --- | --- |
| 2.3 | • 支持 Fortinet 防火墙操作系统版本 5.0 及更高版本<br>• Cisco Secure Firewall 迁移工具允许将以下 Fortinet 配置元素迁移到 威胁防御：<br>  • 接口<br>  • 区域 (Zones)<br>  • 静态路由<br>  • 网络对象和组<br>  • 服务对象和组<br>  • 访问控制列表<br>  • NAT 从属对象（IP 池、虚拟 IP）<br>  • NAT 规则<br>  • VDOM<br>  • 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。<br>  **注释** 管理中心 版本 6.6 及更高版本支持基于时间的对象。 |

# Cisco Secure Firewall 迁移工具的许可

Cisco Secure Firewall 迁移工具应用是免费的，不需要许可证。但是， 管理中心 必须具有相关 威胁防御 功能所需的许可证，才能成功注册 威胁防御 并向其部署策略。

# 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

# Fortinet 防火墙 配置文件的 的要求和前提条件

您可以手动获取 Fortinet 防火墙配置文件。

您手动导入到 Cisco Secure Firewall 迁移工具中的 Fortinet 防火墙 配置文件必须满足以下要求：

- 具有从 Fortinet 设备导出的运行配置。防火墙迁移工具支持从全局和每 VDOM 导出进行配置备份。有关详细信息，请参阅导出 Fortinet 配置文件。
- 仅包含有效的 Fortinet 防火墙 CLI 配置。
- 不包含语法错误。
- 文件扩展名为 `.cfg` 或 `.txt`。
- 使用 UTF-8 文件编码。
- 尚未手工编码或手动更改。如果您修改了 Fortinet 防火墙 配置，则建议您在 Fortinet 防火墙 设备上测试修改后的配置文件，以确保它是有效的配置。

# 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 Fortinet 防火墙 配置迁移到威胁防御时，请考虑以下要求和先决条件：

- 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。
  - 如果目标威胁防御设备是容器实例，则其使用的物理接口、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”）的数量必须至少与 Fortinet 防火墙数量相同；否则，您必须在目标威胁防御设备上添加所需的接口类型。

**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。

# Fortinet 配置支持

### 支持的 Fortinet 防火墙配置

Cisco Secure Firewall 迁移工具可完整迁移以下 Fortinet 防火墙配置：

- 网络对象和组（通配符 FQDN、通配符掩码、Fortinet 动态对象除外）
- 服务对象
- 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 CiscoSecure 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）
- 访问规则
- NAT 规则
- 未迁移的静态路由、ECMP 路由
- 物理接口
- 子接口（子接口 ID 在迁移时会始终被设为与 VLAN ID 相同的编号）
- 汇聚接口（端口通道）
- Cisco Secure Firewall 迁移工具支持将各个 VDOM 作为单独的威胁防御设备从 Fortinet 防火墙进行迁移。
- 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**优化、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，则此类对象非常有用。

注释
- 您必须将时区配置从源 Fortinet 手动迁移到目标威胁防御。
- 非威胁防御流不支持基于时间的对象，它们将被禁用。
- 管理中心版本 6.6 及更高版本支持基于时间的对象。

### 部分支持的 Fortinet 防火墙配置

Cisco Secure Firewall 迁移工具部分支持以下 Fortinet 防火墙配置的迁移。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。

- 包含不受支持的地址对象的地址组。
- 所含服务对象的协议中包含 TCP 或 UDP 和 SCTP 的服务组。

**注释** SCTP 协议将被删除，服务组将部分迁移。

### 不支持的 Fortinet 防火墙配置

Cisco Secure Firewall 迁移工具不支持以下 Fortinet 防火墙配置的迁移。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。

- 基于用户、基于设备和基于互联网服务 ID 的访问控制策略规则
- 带有不受支持 ICMP 类型和代码的服务对象
- 基于隧道协议的访问控制策略规则
- 配置有块分配选项的 NAT 规则
- 配置有 SCTP 的 NAT 规则
- 配置有主机“0.0.0.0”的 NAT 规则
- 源或目标中包含 FQDN 对象的 NAT 规则
- 以特殊字符开头或包含特殊字符的 FQDN 对象
- 通配符 FQDN
- Fortinet 允许配置结合了 IPv4 和 IPv6 的策略（合并策略）。

**注释** Cisco Secure Firewall 迁移工具不支持此策略。

# 适用于 Fortinet 防火墙配置的准则和限制

在转换期间，Cisco Secure Firewall 迁移工具会为所有支持的对象和规则创建一对一映射，而无论它们是否用于规则或策略。Cisco Secure Firewall 迁移工具提供优化功能，允许您在迁移中排除未使用的对象（任何 ACL 和 NAT 中未引用的对象）。

Cisco Secure Firewall 迁移工具处理如下不受支持的对象和规则：

- 不受支持的接口、对象、NAT 规则和路由不会被迁移。
- 不受支持的 ACL 规则将作为禁用的规则迁移到管理中心。

### Fortinet 防火墙配置限制

源 Fortinet 防火墙配置的迁移存在以下限制：

- 系统配置未迁移。
- Cisco Secure Firewall 迁移工具不支持迁移被应用于 50 个或更多接口的单个 ACL 策略。您必须手动迁移已应用于超过 50 个或更多接口的 ACL 策略。
- 不支持类型为虚拟线路、冗余接口、隧道接口、vdom-link 和 SDwan 接口或区域的 Fortinet 防火墙接口，它们不会被迁移。

  Fortinet 硬件或软件交换机逻辑接口将作为威胁防御 L3 接口进行迁移。硬件或软件交换机成员接口不会使用 Cisco Secure Firewall 迁移工具来进行迁移。
- 不支持迁移通配符 FQDN、通配符 IP、动态对象和排除组等对象。
- 无法迁移处于透明模式或透明 VDOM 的 Fortinet 防火墙设备。
- 管理中心不支持嵌套服务对象组和端口组。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。

### Fortinet 防火墙迁移指南

Cisco Secure Firewall 迁移工具会对威胁防御配置使用最佳实践。

ACL 日志迁移选项遵循对应于威胁防御的最佳实践。根据源 Fortinet 防火墙配置启用或禁用规则的日志选项。对于使用 **拒绝**操作的规则，Cisco Secure Firewall 迁移工具会在连接开始时配置日志记录。如果操作是 **允许**，则 Cisco Secure Firewall 迁移工具会在连接结束时配置日志记录。

### 适用于威胁防御设备的准则和限制

当您计划将配置迁移到威胁防御时，请考虑以下准则和限制：

- 如果威胁防御上有任何现有的设备特定配置（例如路由、接口等），则在推送迁移期间，Cisco Secure Firewall 迁移工具会自动清除设备并从配置执行覆盖。

**注释** 为防止设备（目标威胁防御）配置数据意外丢失，我们建议您在迁移之前手动清理设备。

- Fortinet 硬件或软件交换机逻辑接口将作为威胁防御 L3 接口进行迁移。硬件或软件交换机成员接口不会使用 Cisco Secure Firewall 迁移工具来进行迁移。

在迁移期间，Cisco Secure Firewall 迁移工具会重置接口配置。如果在策略中使用这些接口，则 Cisco Secure Firewall 迁移工具无法重置它们，因此迁移会失败

# 支持的迁移平台

以下 Fortinet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
- Cisco Secure Firewall 4200 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 15 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 Fortinet 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
  - 您已为 REST API 启用 管理中心。

    在 管理中心 web 接口，导航至 **系统** > **配置** > **Rest API 首选项** > **启用 Rest API** 并选中 **启用 Rest API** 复选框。

重要事项 您需要在 管理中心 中拥有管理员用户角色，才能启用 REST API。有关管理中心用户角色的详细信息，请参阅 用户角色。

### 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、 Fortinet和 威胁防御 版本：

### 支持的 Cisco Secure Firewall 迁移工具版本

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。

### 支持的 Fortinet 防火墙版本

Cisco Secure Firewall 迁移工具支持迁移到运行 Fortinet 防火墙操作系统版本 5.0 及更高版本的 威胁防御。

### 源 Fortinet 防火墙配置支持的 管理中心 版本

对于 Fortinet 防火墙，Cisco Secure Firewall 迁移工具支持迁移到运行 6.2.3.3 或更高版本的 管理中心 所管理的 威胁防御 设备。

注释 当前不支持迁移到 6.7 威胁防御 设备。因此，如果设备配置了用于 管理中心 访问的数据接口，则迁移可能会失败。

### 支持的 威胁防御版本

Cisco Secure Firewall 迁移工具建议迁移到正在运行 威胁防御 版本 6.5 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。