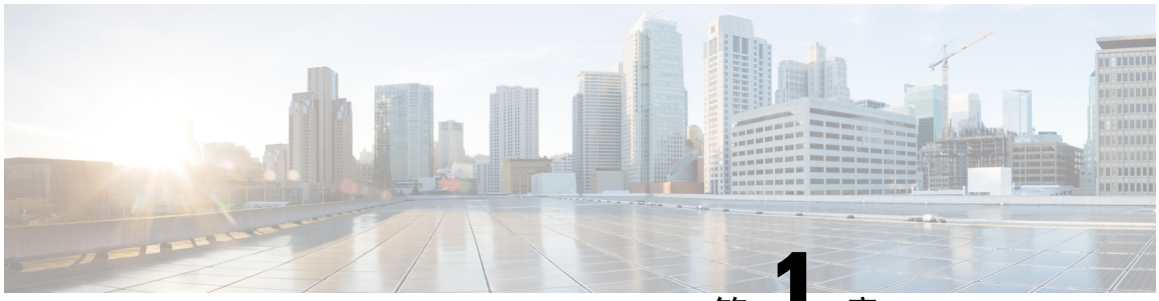
使用 思科安全云控制将 ASA 迁移到 FDM 托管设备

上次修改日期: 2025 年 2 月 27 日

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

目录



第 1 章

使用入门

选择正确的迁移流程

有两种使用 安全云控制 （前称为 Cisco Defense Orchestrator）将自适应安全设备 (ASA) 配置迁移到 FDM 管理 设备的方法：

- 安全云控制 解决方案 - 如果您打算将 ASA 配置迁移到 FDM 管理 设备并使用 安全云控制 和 Firepower 设备管理器进行管理，请使用 安全云控制 中基于云的流程迁移 ASA 配置。
- 本地解决方案（Firepower 设备管理器）- 如果您打算将 ASA 配置迁移到 FDM 管理 设备，请在 安全云控制 中使用基于云的过程来迁移 ASA 配置。然后，您可以使用 Firepower 设备管理器来管理配置。

本指南假定您对 安全云控制 操作有基本的了解。要了解更多信息，请参阅 安全云控制 数据表。

关于 安全云控制 迁移流程

安全云控制 可以帮助您将自适应安全设备 (ASA) 迁移到 FDM 管理 设备。安全云控制 提供 **ASA 到 FDM 迁移**向导，帮助您将 ASA 的运行配置迁移到 FDM 模板。

注释 必须启用 *show-fdm* 和 *enable-asa-to-ftd-migration* 功能标志，才能查看**安全设备**页面上右边窗格的**设备操作**下的**迁移到 FDM** 选项。如果您没有看到 **ASA 到 FDM 的迁移** 选项，请联系 TAC。

您可以使用 **ASA 到 FDM 迁移**向导将 ASA 的以下运行配置元素迁移到 FDM 模板：

- 接口
- 路由
- 访问控制规则 (ACL)
- 网络地址转换 (NAT) 规则
- 网络对象和网络组对象

注释 安全云控制 不支持使用保留关键字的对象名称。通过向其添加后缀“ftdmig”来重命名对象名称。

- 服务对象和服务组对象
- 站点间 VPN

安全云控制 仅迁移引用的对象。访问控制列表中已定义但未引用到访问组的对象不会迁移。安全云控制未能迁移某些元素的常见原因可能是以下一个或多个原因：

- 无 ICMP 代码的 ICMP 访问列表
- 无访问组配置的 TCP/UDP 访问列表
- IP 访问列表未映射到站点间 VPN 配置文件
- 引用到未迁移的访问列表的任何网络对象或组
- 称为关闭的接口

注释 在迁移期间，配置中任何未引用的对象或对象组也将被丢弃并标记为未使用。有关尚未迁移的元素的信息，请参阅**迁移报告**。

将 ASA 运行配置的这些元素迁移到 FTD 模板后，即可将 FDM 模板应用于由 安全云控制管理的新 FDM 管理 设备。FDM 管理 设备采用模板中定义的配置，因此，FDM 管理 现在配置了 ASA 运行配置的某些方面。

使用此过程不会迁移 ASA 运行配置的其他元素。这些其他元素在 FDM 模板中由空值表示。将模板应用于FDM管理设备时，我们会应用迁移到新设备的值并忽略空值。无论新设备具有哪些其他默认值，它都会保留。我们未迁移的 ASA 运行配置的其他元素将需要在迁移过程之外在 FDM 管理 设备上重新创建。

迁移过程的许可证

FDM 管理 设备迁移过程是 安全云控制 的一部分，不需要 安全云控制 许可证以外的任何特定许可证。

准则和限制

注释 在迁移期间，安全云控制 中不支持的配置将被删除为 **不受支持**，并将在 **迁移报告**中进行报告。

功能或函数名称	可以迁移的内容	迁移的限制或限制
防火墙模式	路由防火墙模式	无法迁移透明模式配置。

接口配置	• 物理接口
	• 子接口
		• 设备的物理接口数量必须等于或大于要迁移的 ASA 接口配置。FDM 管理
		• 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）
		• 以下接口配置不会迁移到设备：FDM 管理
		  • ASA 接口上的辅助 VLAN
		  • 冗余接口
		  • 桥接组接口
		  • Virtual Tunnel Interface

功能或函数名称	可以迁移的内容	迁移的限制或限制
EtherChanel	在物理接口上配置的 EtherChannel。 迁移期间会保留映射到 EtherChanel 的成员接口。	• 在迁移配置之前，您必须使用 安全云控制在 FDM 管理 设备上创建等效数量的 EtherChannel。请参阅为 FDM 托管设备添加 EtherChannel 接口。 • 只能迁移到 Firepower 1000 或 2100 系列硬件设备的配置：1010、1120、1140、1150、2110、2120、2130、2140。 • 您可以将 EtherChannel 配置从 ASA 8.4+ 迁移到在软件版本 6.5+ 上运行的设备。FDM 管理 • 迁移前在设备上创建的 EtherChannel 必须与正在迁移的 EtherChannel 的类型相同。FDM 管理 安全云控制 只会将 Etherchannel 迁移到 EtherChannel，并将物理接口迁移到物理接口。 • 在迁移向导的接口映射步骤中，用户将无法使用 FDM 模板中映射到 EtherChannel 的成员接口。但是，它们会保留并迁移到为其分配的 EtherChannel。

路由	静态路由	• 当有多个与目的网络相同的静态路由时，仅迁移一个具有最小度量值的路由，其他路由将被丢弃。
		
		• 以下路由功能不会迁移到设备：FDM 管理
		
		  • 隧道路由
		
		  • Null 0 接口路由
		
		  • 有 SLA 跟踪的静态路由

功能或函数名称	可以迁移的内容	迁移的限制或限制
访问控制规则 (ACL)	• 已启用的访问控制规则 • 源和目标对象 • 安全云控制 支持对 FDM 管理 设备执行“允许”、“信任”和“阻止”等操作。在迁移过程中，系统会处理源 ASA 配置中的允许和拒绝操作，并将其映射到 安全云控制上的FDM管理 设备支持的操作。 • 安全云控制 支持在没有 IP 协议的情况下迁移附加到策略、接口或访问组的 ACL。 • 使用未加密的第3层隧道协议的 ACE	以下 ACL 功能不会迁移到设备：FDM 管理 • 安全云控制 和 Firepower 设备管理器不支持使用 IPv4 和 IPv6 混合协议的 ACL • 记录严重性级别信息 • 非活动或已禁用的规则 • 具有非 TCP、UDP 或 ICMP 协议的服务对象或服务组的 ACE • 具有非 TCP 或 UDP 服务对象的 ACE • ACE 中包含内联对象的非 TCP 或 UDP 协议 • 具有时间范围的 ACE • 访问列表未与访问组映射
网络地址转换 (NAT) 规则	• 网络对象（自动）和两次（手动）NAT 或 PAT • 静态 NAT • 动态 NAT 或 PAT • 身份 NAT • 源端口（服务）转换	以下 NAT 规则功能不会迁移到设备：FDM 管理 • PAT 池 • 单向 • 非活动 • 通过两次NAT，使用目的服务对象进行目的端口（服务）转换（包括同时具有源和目的的服务对象） • 目的端口转换 • NAT46, NAT64 **注释** 安全云控制 不支持具有 0.0.0.0/32 的网络对象。
服务对象和服务组对象	服务对象和嵌套组 有关 安全云控制 支持的服务对象中使用的协议列表，请参阅 安全云控制上支持的 IP 协议。	• 不支持 BCC-RCC-MON 和 BBN-RCC-MON 协议。 • 不支持小于、大于和不等于等运算符。 • 对象组嵌套

功能或函数名称	可以迁移的内容	迁移的限制或限制
网络对象和网络组对象	网络对象和网络组对象	不支持以下网络对象或网络组： • 基于不连续掩码 • IPv4 地址中第一个八位组“0”开头的 IP 地址
ICMP 类型	ICMP 类型	以下 ICMP 类型不受支持： • 具有 INVALID ICMP 类型或/和代码的基于 ICMP 的服务对象条目 • 无 ICMPv4 或 ICMPv6 类型代码的服务类型或 ICMP 类型对象 • 任何未分配的 ICMP 类型（根据 IANA）或无效的 ICMP 类型
其他不受支持的对象	-	不支持以下其他对象： • 基于 SGT 的网络对象组 • 基于用户的网络对象组
站点间 VPN	• IKEv1 和 IKEv2 的第 1 阶段和第 2 阶段提议 • IKEv1 和 IKEv2 的完全前向保密 (PFS) • 带嵌套对象组的加密访问列表 • 具有多个对等 IP 的加密映射 • IKEv1 和 IKEv2 均用于加密映射中的隧道	不支持以下站点间 VPN 功能： • VPN-Filter • vpn-idle-timeout • isakmp keepalive threshold 10 retry 10 • Crypto Map VPNMAP 200 set security-association lifetime seconds 360 • set security-association lifetime千字节无限制 • set security-association lifetime seconds 3600 • 证书身份验证 • 动态加密映射 • 基于路由的 VPN（虚拟隧道接口）

有关准则和限制的详细信息，请参阅 ASA 配置准则和限制以及FDM 管理设备准则和限制。

安全云控制上支持的 IP 协议

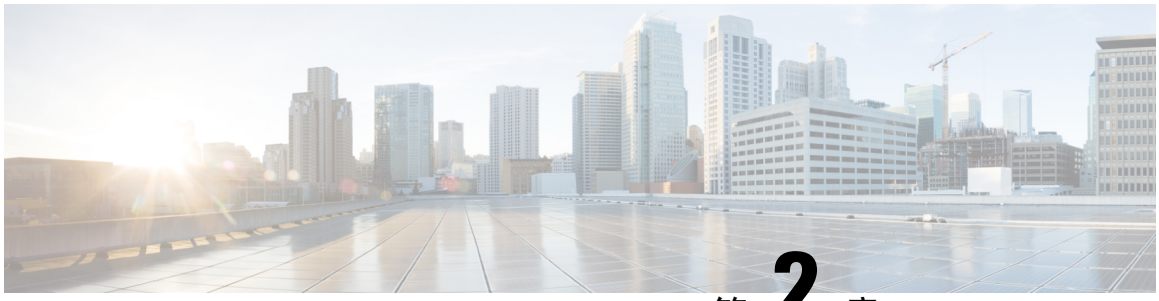
安全云控制 支持的服务对象 IP 协议如下：

服务对象中的 IP 协议			
1= ICMP	34 = THREEPC	73 = CPHB	106= QNX
2 = IGMP	35 = IDPR	74 = WSN	107 = AN
3 = GGP	36 = XTP	75 = PVP	108 = IPCOMP
5 = ST2	37 = DDP	76 = BRSATMON	109= SNP
6 = TCP	38 = IDPRCMTP	78 = WBMON	110 = COMPAQPEER
7 = CBT	39 = TPPLUSPLUS	77 = SUNND	111 = IPXINIP
8 = EGP	40 = IL	79 = WBEXPAK	112 = VRRP
9 = IGP	42 = SDRP	80 = ISOIP	113= PGM
10 = BBNRCCMON	45 = IDRP	81 = VMTP	115 = L2TP
11 = NVP2	46 = RSVP	82 = SECUREVMTP	116 = DDX
12 = PUP	48 = MHRP	83 = VINES	117= IATP
13 = ARGUS	49 = BNA	84 = TTP	118 = ST
14 = EMCON	50 = ESP	85 = NSFNETIGP	119= SRP
15=XNET	51 = AH	86 = DGP	120= UTI
16 = CHAOS	52 = INLSP	87 = TCF	121= SMP
17 = UDP	53 = SWIPE	88 = EIGRP	122= SM
18 = MUX	54 = NARP	89 = OSPFIGP	123= PTP
19 = DCNMEAS	55 = MOBILE	90 = SPRITERPC	124= ISIS
20 = HMP	56 = TLSP	91 = LARP	125 = FIRE
21 = PRM	57 = 跳过	92 = MTP	126 = CRTP
22 = XNSIDP	58= IPv6-ICMP	93 = AX25	127 = CRUDP
23 = TRUNK1	59 = IPv6NONXT	94 = IPIP	128 = SSCOPMCE
24 = TRUNK2	62 = CFTP	95 = MICP	129 = IPLT
25 = LEAF1	64 = SATEXPAK	96 = SCCSP	130 = SPS
26 = LEAF2	65 = KRYPTOLAN	97 = ETHERIP	131= PIPE
27 = RDP	66 = RVD	98 = ENCAP	132 = SCTP
28 = IRTP	67 = IPPC	100 = GMTP	133 = FC
29 = ISOTP4	69 = SATMON	101 = IFMPP	254 = DIVERT
30 = NETBLT	70 = VISA	102= PNNI	
31 = MFENSP	71 = IPCV	103= PIM	
32 = MERITINP	72 = CPNX	104 = ARIS	
33 = SEP		105=SCPS	

最佳实践

使用 安全云控制 将 ASA 配置迁移到 FDM 模板时，请遵循以下最佳实践：

- 确保在模型设备迁移中使用 **show run** 命令从 ASA 设备获取运行配置。
- 查看已跳过、不支持和部分支持的配置的迁移报告。
- 迁移后，请验证 FDM 模板中已迁移的规则和对象，然后再将其部署到FDM 管理设备。
- 在将 ASA 策略迁移到 FDM 模板之前对其进行优化。
- 我们建议您将迁移的 ASA 配置部署到没有现有配置的FDM 管理设备。



第 2 章

将 ASA 迁移到 FDM 托管设备工作流程

如何实施迁移过程

	相应操作
第 1 步	准备迁移， 第 12 页 • 载入 ASA 设备 • 迁移前优化 ASA 策略 • 迁移前将 EtherChannel 配置添加到 FDM 管理的设备， 第 13 页

第 2 步	运行迁移， 第 14 页
	• 选择要迁移的设备
	• （可选）更新迁移名称
	• 解析 ASA 配置
	• 应用迁移
	  • 立即应用迁移
	  • 稍后应用迁移

第 3 步	查看迁移操作
第 4 步	部署配置， 第 22 页

准备迁移

要准备迁移设备，请确保：

- 您有一个 安全云控制 租户，可以登录该租户。有关详细信息，请参阅初始登录。
- 您已将要迁移到设备的 ASA 设备或 ASA 配置文件载入租户。FDM 管理

  您的 ASA 的运行配置文件必须小于 4.5 MB 和 22,000 行。请参阅确认 ASA 运行配置大小。
- 如果要在迁移过程后直接将 ASA 配置迁移到 FDM 管理 设备，或者要将 EtherChannel 配置迁移到设备，则需要将 FDM 管理 设备载入 安全云控制。有关详细信息，请参阅载入 FTD 设备。
- 设备必须处于同步状态。

  这可确保设备上的运行配置与 安全云控制 中存储的运行配置相同。
- 您的 ASA 运行的是 8.4 或更高版本的软件。

要了解有关设备支持摘要、不受支持的设备、硬件和软件详情的更多信息，请参阅 安全云控制支持的软件和硬件。

载入 ASA 设备

点击 **安全设备** 页面中的 (+)。

载入页面显示您可以载入设备的位置。

如何载入 ASA 设备

执行以下操作，使用以下任一选项载入 ASA 设备：

- 载入实时 ASA 设备。
- 导入配置以进行离线管理：
  - 输入**设备名称**，并选择 ASA 作为**设备类型**。
  - 点击**浏览**，选择 ASA 配置文件，即 *.TXT* 或 *.CFG* 文件。
  - 点击**上传 (Upload)**。

迁移前优化 ASA 策略

现在，您已载入所有 ASA，开始使用 安全云控制 识别和纠正网络对象问题，优化现有策略，检查 VPN 连接，并将 ASA 升级到最新版本。

解决网络对象问题

通过解决网络策略对象的问题，开始优化 ASA 上的安全策略。

- 未使用的对象 (Unused objects) -安全云控制 可识别存在于设备配置中存在但未被其他对象、访问列表或 NAT 规则引用的网络策略对象。查找这些未使用的对象并将其删除。

- 重复对象 (Duplicate objects) - 重复对象是指同一设备上具有不同名称但值相同的两个或多个对象。这些对象通常是意外创建的，可用于类似的目的，并供不同的策略使用。寻找机会使名称标准化，同时认识到出于合法原因可能存在一些重复名称。
- 不一致对象 (Inconsistent objects) - 不一致对象是指两台或多台设备上具有相同名称但值不同的对象。有时，用户会在不同的配置中创建具有相同名称和内容的对象，但随着时间的推移，这些对象的值会出现分歧，从而造成不一致。考虑将这些对象中的值标准化或重命名以将其标识为不同的对象。

修复影子规则

现在，您已解决网络对象问题，请查看影子规则的网络策略并进行修复。https://docs.defenseorchestrator.com/Configuration_Guides/Security_Policy_Management/ASA_Policies/Shadowed_Rules影子规则在网络策略页面上用半月形标记进行标记。这是策略中永远不会触发的规则，因为策略中具有较高优先级的规则会在所有数据包到达影子规则之前对其进行操作。如果存在永远不会命中的影子规则，请将其删除，或编辑策略以将该规则“显示出来”。https://docs.defenseorchestrator.com/Configuration_Guides/ASA_Policies/ASA_Network_Policies/0020_Edit_an_ASA_Network_Policy

迁移前将 EtherChannel 配置添加到 FDM 管理的设备

开始之前

回顾此信息：

- 准备迁移，第 12 页
- 用于迁移 EtherChannel。准则和限制，第 3 页

过程

步骤 1 在迁移 EtherChannel 配置之前，必须在从 ASA 迁移的设备上创建相同数量的 EtherChannel。FDM 管理您可以使用 安全云控制 创建 EtherChannel。有关说明，请参阅为 FDM 托管设备添加 EtherChannel 接口。

EtherChannel 的最低配置是一个 EtherChannel ID 和至少一个 EtherChannel 成员。

步骤 2 将更改部署到 FDM 管理 设备。

下一步做什么

请继续运行迁移，第 14 页。

运行迁移

选择要迁移的设备

您可以 选择设备并启动 FDM 迁移向导

选择设备并启动 FDM 迁移向导

过程

步骤 1 登录 安全云控制 租户。

步骤 2 在左侧窗格中，点击 > 。

步骤 3 点击 **设备** 选项卡以找到设备。

步骤 4 点击 **ASA** 选项卡，然后选择要迁移到 FDM 管理 设备的 ASA 设备或型号。

所选 ASA 设备的设备详细信息（例如位置、型号、序列号等）显示在 Device Details 窗格中。

步骤 5 在 **设备操作 (Device Actions)** 窗格中，点击**迁移到 FDM (Migrate to FDM)**。

如果之前有此设备的迁移，您将看到所选设备的迁移结果。

有关过滤的详细信息，请参阅关于迁移过滤器。

如果这是新迁移，请点击**开始新迁移（设备名称）(Start a new migration for [device name])**。

步骤 6 （可选）如果要选择其他 ASA 设备或型号以迁移到 FDM 模板，请参阅关于迁移过滤器。

（可选）更新迁移名称

根据设备名称和时间戳自动生成迁移名称。

过程

步骤 1 在 **FDM 迁移**屏幕中，您还可以更新迁移名称或保留默认名称。安全云控制 允许您使用迁移名称搜索迁移列表。

注释
默认情况下，FDM 模板名称将与迁移名称相同。

步骤 2 点击**下一步**以触发迁移。

（可选）保留运行配置

注释 仅当您从 **安全设备** 页面选择实时 ASA 时，这才适用。

在 **保留运行配置**中，迁移工具允许您将 ASA 的运行配置的 安全云控制副本另存为配置文件。此模型设备配置用于迁移，因此不会影响实时 ASA。

以下选项可用于将 ASA 的运行配置的 安全云控制副本迁移到 FDM 管理 设备：

- 从 ASA 的运行设备的 安全云控制副本创建配置文件

注释 允许您在发起迁移时保留 ASA 配置的快照（模型设备）。当您需要更改配置以进行迁移时，您可以使用配置文件，而不会影响/中断 ASA 运行配置的 安全云控制副本。

- 直接从设备迁移配置

注释 迁移的源配置是 ASA 的运行配置的 安全云控制副本。迁移工具仅考虑迁移开始时的配置。以后对该 安全云控制的 ASA 运行配置副本所做的任何更改都不会反映在生成的迁移中。从已更改的 ASA 运行配置的 安全云控制副本进行的额外迁移尝试可能会导致不同的 FDM 管理 设备配置。

过程

步骤 1 在**模型设备名称 (Model Device Name)** 字段中输入模型设备名称。

步骤 2 执行这些操作之一：

a) 点击**下一步**。

模型设备已创建，并触发该设备的迁移。

b) 点击跳过以在实时 ASA 上触发迁移。

解析 ASA 配置

注释 根据配置文件的大小和其他设备或服务的数量，可能需要一些时间来解析配置。有关详细信息，请参阅确认 ASA 运行配置大小。

迁移的解析将继续，直到成功或失败。迁移过程会收集ASA信息，对其进行解析，创建FDM模板，并启用此FDM模板以应用于 安全云控制中的设备。有关FDM模板的详细信息，请参阅模板。在解析阶段，迁移过程会生成迁移报告和迁移日志，用于识别：

- 已完全迁移、部分迁移、迁移不支持和迁移中忽略的 ASA 配置项目。
- 出错的 ASA 配置行，列出迁移流程无法识别的 ASA CLI；这些配置行会阻止迁移。

注释 与管理接口关联的管理接口和静态路由不会迁移。

修复迁移错误

当出现迁移错误时，您可以在 **FDM 迁移**屏幕中查看**查看迁移报告**和**查看迁移日志**。

从**FDM 迁移**屏幕中选择 **下载报告**和**下载日志**，以下载迁移报告和日志。

报告和日志必须能够打印 ASA 配置中导致解析失败的行。导航到您选择进行迁移的 ASA 设备，更新 ASA 配置，然后重新启动新的迁移。

如果解析成功，但 FDM 模板创建失败，请导航至**模板** > **工作流程**或**迁移** > **工作流程**以识别任何失败并解决问题。

修复迁移错误后重新解析

您可以在修复迁移错误后重新解析 ASA 配置。请执行以下操作：

- 在 **FDM 迁移**屏幕中，点击**转到配置**。
- 转到特定配置并进行导致转换失败的配置更改。
- 更新正确的配置后，请点击**重新解析配置**以根据更改的配置触发迁移。

注释 **重新解析配置**选项仅在您更新配置文件时适用，并且仅适用于存在解析错误的配置。

应用迁移

要应用迁移，您可以选择以下选项之一：

- 立即应用迁移
- 稍后应用迁移

根据 安全云控制 应用模板功能，迁移期间创建的 FDM 模板仅将设备上的更改部署到以下各项：接口、NAT、ACL、对象和路由。

DHCP 和数据 DNS 设置恢复为默认值，因为接口信息在迁移期间会发生更改。

VPN、HA 等其他设置在设备上保持不变。

立即应用迁移

注释 在设备上应用迁移之前，请检查设备是否处于同步状态。

您可以将 FDM 模板应用于任何设备，查看设备模板，然后通过选择设备部署到设备。FDM 管理

过程

步骤 1 选择立即应用迁移。

a) 从选择 FTD 设备下拉列表中，选择要应用 FDM 设备模板的设备。FDM 管理

设备状态必须为“已同步”，连接为“在线”。

b) 点击**选择 (Select)** 以选择 FDM 管理 设备。

步骤 2 点击**下一步**。

步骤 3 在映射接口行中，迁移工具会检索设备上的模板接口和设备接口列表。FDM管理默认情况下，防火墙迁移工具会根据其接口标识符映射 ASA 和 FDM 管理 设备中的接口。点击**继续 (Continue)**。

有关映射 ASA 接口与FDM 管理设备的详细信息，请参阅映射 ASA 接口与防火墙威胁防御接口。

步骤 4 查看要应用于 FDM 管理 设备的 FDM 模板信息，然后点击**应用模板 (Apply Template)**。

步骤 5 在“完成”(Done) 行中，您可以执行以下操作：

您已成功将迁移的配置应用到所选设备。FDM 管理

- 点击**删除用于迁移的设备型号 (Remove model device used for migration)** 复选框。

  选中此复选框将删除从实时 ASA 创建的模型设备。此操作还将删除模型设备，删除迁移日志和与迁移关联的文件。

  注释
  仅当从**安全设备** 页面选择实时 ASA 时，且仅当用户已创建模型设备时，才会显示此复选框。

- 点击**将迁移的配置另存为模板 (Save migrated configuration as a template)** 复选框。

  注释
  此复选框仅在成功应用 FDM 模板时显示，默认情况下处于选中状态。

  如果取消选中该复选框，则不保存 FDM 模板。

  如果您在应用 FDM 模板时遇到任何错误，请导航至设备 > 工作流程以查看错误并解决问题。

  注释
  您可以从设备和服务页面访问这些 FDM 模板。有关 FDM 模板的详细信息，请参阅模板。

  注释
  成功保存 FDM 模板后，您可以执行以下操作：

采取下列操作之一：

- 点击**预览并部署 (Preview and Deploy)** 以部署配置。

  您可以在“预览和部署”页面中验证将要部署的对象列表。

- 点击**转到设备 (Go to Devices)**，为您提供部署配置的选项。

（可选）迁移后任务

- 导航到 FDM 模板以查看迁移结果。
- 使用 安全云控制 功能优化配置。
- 将 FDM 模板部署到设备。

通过管理访问接口迁移支持 *FDM* 受管设备

注释 具有管理访问接口的目标设备不支持应用模板功能。在目标FDM 管理设备上应用 FDM 模板之前，请对其进行手动修改。

在配置了管理访问接口的目标设备上应用任何迁移的FDM模板时，由于映射接口不匹配，应用模板功能会失败。在目标 FDM 管理 设备上，必须保留管理访问接口配置和相应的静态路由，以确保与安全云控制的连接。因此，为避免连接失败，您必须按照以下步骤手动配置管理访问接口以及所需的静态路由，然后应用 FDM 模板。本节提供确保成功迁移所必须遵循的程序。

如果有多个管理访问接口，并且接口配置不正确或未使用，则必须更新目标FDM管理设备以仅保留已配置的相关管理访问接口，以便未使用的接口可用于迁移的配置。

过程

步骤 1 通过修改数据接口的 IP 地址和子网掩码来更新模板中的物理接口，使其与管理访问接口的 IP 地址和子网掩码相同。

注释
目标FDM 管理设备的管理访问接口必须与 FDM 模板中的管理访问接口进行映射。FDM 模板的 IP 地址和子网掩码必须与目标FDM 管理设备的 IP 地址和子网掩码相同。

a) 导航至 页面。
b) 点击**模板 (Template)** 选项卡。
c) 点击**威胁防御**选项卡，然后选择 FDM 设备模板。
d) 从**管理 (Management)** 窗格中选择**接口 (Interface)**。
e) 点击 **Editing Physical Interface** 对话框中的 **Edit**。
f) 输入 **IP 地址**和**子网掩码**。

g) 点击**保存 (Save)**。

步骤 2 在模板设置中将数据接口添加为管理访问接口：

a) 导航至 页面。
b) 点击**模板 (Template)** 选项卡。
c) 点击**威胁防御**选项卡，然后选择 FDM 设备模板。
d) 导航到**管理**窗格右侧的**设置**。
e) 在**数据接口**窗格中，点击 + 将接口添加为管理访问接口。

注释
确保数据接口具有名称、状态和 IP 地址。

f) 点击**保存 (Save)**。

步骤 3 使用设备上关联的接口添加或更新静态路由。将管理访问接口映射到其他接口时，请为所选FDM管理设备设置路由配置。

有关添加或更新静态路由的详细信息，请参阅为威胁设备配置静态路由。

稍后应用迁移

过程

步骤 1 选择稍后应用迁移。

已保存迁移模板。您可以保存创建的模板，稍后将模板应用于 FDM 管理的设备。

注释
您可以从 页面访问 FDM 模板。

成功保存 FDM 模板后，您可以执行以下操作：

- 导航到 FDM 模板以查看迁移结果。
- 使用 安全云控制 功能优化 FDM 模板。
- 导航到目标 FDM 管理的设备，然后选择必须应用的 FDM 模板。
- 将 FDM 模板部署到设备。

步骤 2 点击**完成 (Done)**。

系统将显示 页面，其中包含预选的 FDM 模板。

安全云控制 允许您执行所有与模板相关的操作，例如审核策略、配置等。

步骤 3 当您准备好应用 FDM 模板时：

1. 从 页面中选择目标 FDM 管理的设备。
2. 点击设备操作窗格中的应用模板。

系统将显示**应用设备配置 (Apply Device Configuration)** 屏幕。

3. 选择要在设备上应用的 FDM 模板。
4. 点击 **Apply**。

注释
设备上运行的管理接口 IP 保持不变。

查看迁移操作

迁移表屏幕显示以下内容：

- 迁移名称。默认情况下，安全云控制 会根据设备名称生成迁移名称。您还可以自定义此名称。请参阅（可选）更新迁移名称。
- 上次在设备上执行的迁移活动的时间戳。
- 显示设备的迁移状态。有关迁移状态的详细信息，请参阅迁移状态和说明。
- 允许您执行各种操作，例如重命名、下载日志等。有关操作的详细信息，请参阅操作和说明。

表 *1:* 迁移状态和说明

迁移状态	说明
解析	正在迁移。
解析错误	解析已完成，但存在错误。
转换错误	转换已完成，但有错误。
模板已创建	迁移完成。已成功创建 FDM 模板，但出现验证错误。

有关修复迁移错误的详细信息，请参阅修复迁移错误。

表 *2:* 操作和说明

操作	说明
继续	从迁移过程停止的步骤恢复。 例如，如果迁移完成，则从应用 FDM 模板恢复该过程。
重命名	重命名迁移名称。
工作流程	显示工作流程屏幕。

操作	说明
下载日志	允许您以 TXT 格式下载日志文件。这是解析日志。
下载报告	允许您以 HTML 格式下载报告详细信息。
配置	允许您查看对其执行迁移的 ASA 配置。
删除	删除迁移及其关联的文件，例如日志文件。

关于迁移过滤器：

如果要选择其他 ASA 设备或型号以迁移到 FDM 模板，请使用以下任何选项：

- 按设备过滤
- 按清除选项过滤

按设备过滤

您可以在**迁移 (Migrations)** 页面上使用许多不同的过滤器来查找所需的对象。迁移过滤器允许您按设备、状态和时间范围进行过滤。

表 *3:* 过滤器属性和说明

过滤器属性	说明
按设备过滤	允许您选择要迁移的特定设备。
状态	• 错误 - 显示基于解析错误的迁移列表。 • 完成 - 显示基于成功创建的 FDM 模板的迁移列表。
时间范围	开始、结束 - 根据所选的迁移开始和结束日期显示设备列表。

按清除选项过滤

1. 点击**清除 (Clear)** 以清除过滤器栏。
2. 点击 (+) 图标。
3. 从列表中选择设备或按名称搜索并选择它。
4. 点击**选择**。

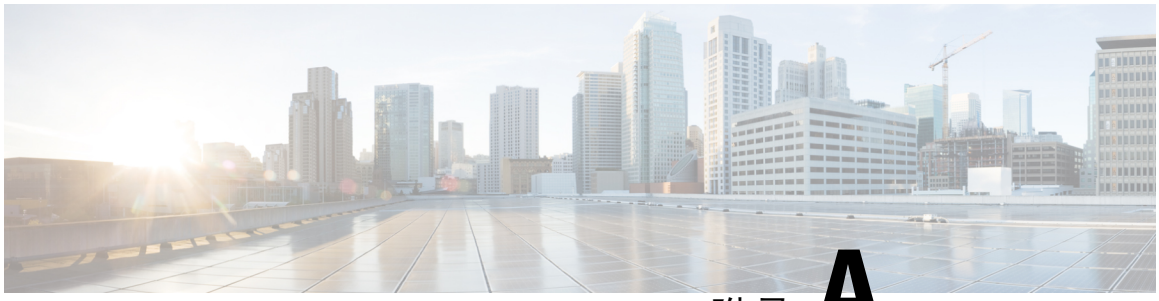
   系统将显示 **FDM 迁移**屏幕。

部署配置

最后一步是部署对设备所做的配置更改。

有关更多信息，请参阅配置设备部署。

请参阅使用 思科安全云控制管理 FDM 设备和使用 思科安全云控制 管理 FMC，了解 安全云控制 如何管理 FDM 托管设备的不同方面及其安全策略。



附录 A

遥测

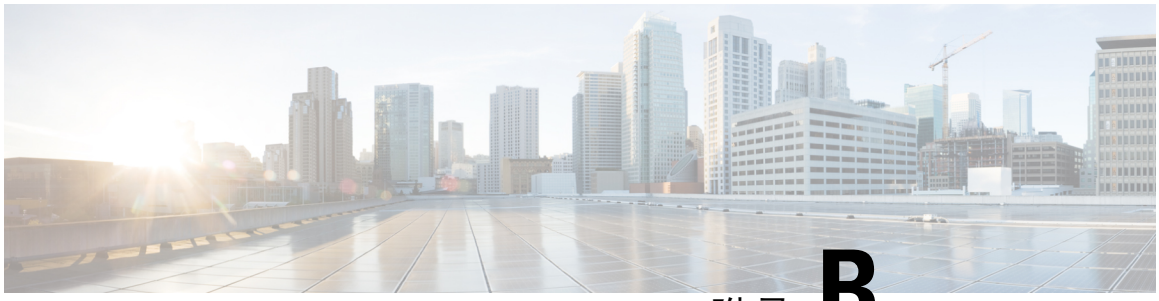
Cisco Success Network

注释 安全云控制 不会管理思科成功网络设置。设备管理器用户界面管理设置并提供遥测信息。

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，设备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。

有关更多信息，请参阅思科成功网络 - 遥测数据。

遥测



附录 B

常见问题解答

故障排除常见问题解答

问: 为什么解析需要更长的时间？

答: 如果 ASA 配置文件很大，则需要更长的时间进行解析。您的 ASA 的运行配置文件必须小于 4.5 MB 和 22,000 行。有关详细信息，请参阅确认 ASA 运行配置大小。

问: 当我在迁移过程中发现解析错误时，我必须怎么做？

答: 有关错误的详细信息，请参阅**查看迁移报告**和**查看迁移日志**。

问: 我在迁移过程中遇到解析错误。如何修复它们？

答: 导航至迁移页面，点击特定设备的下载日志并修复错误。

问: 我在 FDM 模板生成过程中遇到转换错误。我必须怎样做？

答: 导航至“迁移”页面，点击特定设备的工作流程以查看错误。

问: 创建的 FDM 模板出错时该怎么办？

答: 如果创建的 FDM 模板存在验证错误，您可以在**清单 (Inventory)** 页面中搜索 FDM 模板。从设备操作窗格中点击工作流程，您可以在其中查看错误详细信息。

问: 安全云控制 无法写入更改日志。为什么会出现这种情况？

答: 当您将 ASA 载入 安全云控制时，安全云控制 会在其数据库中存储 ASA 的运行配置文件的副本。通常，如果该运行配置文件过大（4.5 MB 或更大），或者包含的行过多（大约 22,000 行），或者单个访问组的访问列表条目过多，则安全云控制 将无法可预测地管理该设备。有关详细信息，请参阅确认 ASA 运行配置大小。

您还可以联系思科客户团队寻求帮助，以在不中断安全策略的情况下安全地减小配置文件的大小。

问: 安全云控制 是否会在迁移前验证 ASA 配置文件的语法？

答: 否。在将 ASA 配置文件迁移到 FDM 模板之前，安全云控制 不会对其进行验证。如果您尝试将已载入的 ASA 型号迁移到 安全云控制，但迁移失败，请查看迁移报告并查看 FDM 迁移屏幕中的迁移日志。您可能需要验证配置文件的语法。

问: 为什么我的某些访问列表和网络对象没有迁移？

答: 安全云控制 仅迁移引用的对象。访问控制列表中已定义但未引用到访问组的对象不会迁移。此外，安全云控制 无法迁移某些元素的一些常见原因可能是以下一个或多个原因：

- 无 ICMP 代码的 ICMP 访问列表
- 无访问组配置的 TCP/UDP 访问列表
- IP 访问列表未映射到站点间 VPN 配置文件
- 引用到未迁移的访问列表的任何网络对象或组
- 称为关闭的接口

有关尚未迁移的元素的详细信息，请参阅**迁移报告**。

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。