



导入/导出

以下主题介绍如何使用导入/导出功能：

- [关于配置导入/导出，第 1 页](#)
- [配置导入/导出的要求和必备条件，第 3 页](#)
- [导出配置，第 3 页](#)
- [导入配置，第 4 页](#)

关于配置导入/导出

可以使用导入/导出功能在设备之间复制配置。导入/导出不是备份工具，但可简化将新设备添加到部署的过程。

既可导出单项配置，也可通过单次操作导出一组（相同类型或不同类型的）配置。当您稍后将软件包导入另一台设备时，您可选择要导入软件包中的哪些配置。

导出的数据包包含该配置的版本信息，从而确定是否可以将该配置导入到另一设备上。当设备兼容但数据包包含重复配置时，系统会提供解决方法选项。



注释 导入和导出设备必须运行相同版本的 Firepower 系统。对于访问控制及其子策略（包括入侵策略），入侵规则更新版本也必须匹配。如果版本不匹配，导入将失败。您可以使用导入/导出功能更新入侵规则。相反，请下载并应用最新的规则更新版本。

支持导入/导出的配置

以下配置支持导入/导出：

- 访问控制策略及其调用的策略：预过滤器、网络分析、入侵、SSL、文件、威胁防御服务策略
- 入侵策略，与访问控制无关
- NAT 策略（仅限 Cisco Secure Firewall Threat Defense）

- FlexConfig 策略。但在导出该策略时，将会清除任何密钥变量的内容。在导入使用密钥的 FlexConfig 策略后，必须手动编辑所有密钥的值。
- 平台设置
- 运行状况策略
- 警报响应
- 应用检测器（用户定义的检测器以及那些由思科专业服务提供的检测器）
- 控制面板
- 自定义表
- 自定义工作流程
- 保存的搜索
- 自定义用户角色
- 报告模板
- 第三方产品和漏洞映射
- 用于用户控制的用户和组

配置导入/导出的特殊注意事项

当导出配置时，系统也会导出其他所需的配置。例如，导出访问控制策略也会导出该策略调用的任何子策略、该策略使用的对象和对象组、祖先策略（在多域部署中）等等。又例如，如果导出启用了外部身份验证的平台设置策略，则也会导出身份验证对象。但是，也有一些例外：

- 系统提供的数据库和源 - 系统不会导出 URL 过滤类别和信誉数据、思科情报源数据或地理位置数据库 (GeoDB)。确保部署中的所有设备可从思科获取最新信息。
- 全局安全情报列表 - 系统会导出与导出的配置关联的全局安全情报阻止和 不阻止 名单。（在多域部署中，不管当前域如何，都会发生此情况。系统不导出后代域列表。）导入过程将这些名单转换为用户创建的列表，然后将这些新列表用于导入的配置中。这可确保导入的列表不会与现有全局阻止和 不阻止 名单发生冲突。要在导入 管理中心 时使用全局列表，请将这些列表手动添加到导入的配置中。
- 入侵策略共享层 - 导出过程会中断入侵策略共享层。以前共享的层包含在数据包中，而导入的入侵策略不包含共享层。
- 入侵策略默认变量集 - 导出数据包包含一个默认变量集，此变量集包含自定义变量及带用户定义值的系统提供的变量。导入过程会使用导入的值更新导入 管理中心 上的默认变量集。但是，导入过程不会删除不存在于导出数据包中的自定义变量。对于在导出数据包中未设置的值，导入过程也不会恢复导入 管理中心 上的用户定义值。因此，如果导入 管理中心 具有配置不同的默认变量，则导入的入侵策略的行为可能会与预期大不相同。

- 自定义用户对象 - 如果您在管理中心中创建了自定义用户组或对象，并且此类自定义用户对象是访问控制策略中任何规则的一部分，那么请注意，导出文件(.sfo)不会包含用户对象信息，因此在导入此类策略时，对此类自定义用户对象的任何引用都将被删除，不会导入到目标管理中心。为了避免由于缺少用户组而引起的检测问题，请手动将自定义的用户对象添加到新的管理中心，并在导入后重新配置访问控制策略。

导入对象和对象组时：

- 通常，导入过程将对象和对象组作为新对象和对象组导入，您不能替换现有的对象和对象组。但是，如果采用导入的配置的网络和端口对象或对象组与现有对象或对象组匹配，则导入的配置将重用现有对象/对象组，而不是创建新的对象/对象组。系统通过比较每个网络和端口对象/对象组的名称（不包括任何自动生成的编号）和内容来确定匹配。
- 如果在导入管理中心时导入对象的名称与现有对象匹配，系统会将自动生成的编号附加到导入的对象和对象组的名称，以使其唯一。
- 您必须将导入的配置中使用的任何安全区域和接口组映射到导入管理中心管理的匹配类型区域和组。
- 如果导出使用包含私钥的 PKI 对象的配置，系统会在导出之前解密私钥。导入时，系统会使用随机生成的密钥加密密钥。

配置导入/导出的要求和必备条件

型号支持

Any

支持的域

任意

用户角色

- 管理员

导出配置

导出过程可能需要几分钟，取决于正在导出的配置数量以及这些配置引用的对象数量。



提示

Firepower 系统中的许多列表页面的列表项旁均包括 **YouTube EDU** ()。如果该图标存在，您可将其作为下列导出步骤的快速替代项。

开始之前

- 确认导入和导出设备运行的是同一版本的 Firepower 系统。对于访问控制及其子策略（包括入侵策略），入侵规则更新版本也必须匹配。

过程

步骤 1 选择系统 (⚙️) > 工具 > 导入/导出。

步骤 2 点击 **折叠** (▾) 和 **展开** (▸) 图标以折叠和展开可用配置列表。

步骤 3 选中要导出的配置并点击 **导出 (Export)**。

步骤 4 按照网页浏览器提示将已导出软件包保存至计算机。

导入配置

视乎正在导入的配置数量以及这些配置所引用的对象数量，导入过程可能需要几分钟。



注释 如果您注销系统、如果您更改到其他域，或者点击 **导入** 后用户会话到期，导入过程将在后台继续进行，直到完成为止。我们建议您等待导入过程完成，然后再创建任何新的对象或策略。在导入过程中尝试创建它们可能会导致失败。

开始之前

- 确认导入和导出设备运行的是同一版本的软件系统。对于访问控制及其子策略（包括入侵策略），入侵规则更新版本也必须匹配。

过程

步骤 1 在导入设备上，选择系统 (⚙️) > 工具 > 导入/导出。

步骤 2 点击上传软件包。

步骤 3 输入已导出的软件包的路径或浏览到其位置，然后点击 **上传 (Upload)**。

步骤 4 如果没有版本不匹配情况或其他问题，请选择要导入的配置，然后点击 **导入 (Import)**。
如果无需执行任何冲突解决方案或接口对象映射，则表明导入完成，并会显示成功消息。跳过此程序的其余步骤。

步骤 5 如果提示，请在导入冲突解决方案页面上，将已导入的配置中使用的接口对象映射到具有由导入管理中心管理的匹配接口类型的区域和组。

源和目标接口对象的接口对象类型（安全区域或接口组）以及接口类型（被动，内联，路由等等）必须匹配。有关信息，请参阅 [接口](#)。

如果您正在导入的配置引用尚不存在的安全区域或接口组，则可以将其映射到现有接口对象或创建新接口对象。

注释 对于单个访问控制策略，您可以选择将现有策略替换为导入的策略。但是，对于嵌套访问控制策略，只能将其作为新策略导入。

步骤 6 点击 **Import**。

步骤 7 如果提示，请在“导入解决方案” (Import Resolution) 页面上，展开每项配置并选择相应的选项，如 [解决导入冲突](#)，第 5 页中所述。

步骤 8 点击 **Import**。

步骤 9 更新所有源。

例如，转到 **对象 > 对象管理 > 安全情报**，然后点击 URL、网络和 DNS 列表和源页面上的 **更新源** 按钮。

导入的策略不包括源内容。

步骤 10 等待所有源更新完成，然后再将策略部署到设备。

下一步做什么



注释 如果导入包含 Microsoft Active Directory 用户和组的配置，我们强烈建议您在导入后下载所有用户和组，以避免出现访问控制策略和其他策略 SSL 策略中的问题。（**集成 > 其他集成 > 领域**，然后点击 **↓**（立即下载））。

- 或者，查看总结已导入的配置的报告；请参阅 [查看任务消息](#)。

解决导入冲突

当您尝试导入配置时，系统会确定设备上是否已存在同一名称和类型的配置。在多域部署中，系统还会确定某个配置是在当前域还是在其任何祖先域或后代域中定义的配置的重复。（您无法查看后代域中的配置，但如果后代域中存在具有重复名称的配置，则系统会通知您发生冲突。）当导入包含重复配置时，系统会提供适合于您的部署的解决方法选项，其中包括：

- **保持现有配置 (Keep existing)**

系统不导入该配置。

- **替换现有配置 (Replace existing)**

系统使用选择用于导入的配置覆盖当前配置。

- **保留最新配置 (Keep newest)**

仅在所选配置的时间戳比设备上的当前配置中的时间戳更新时，系统才会导入所选配置。



注释 如果导入包含 Microsoft Active Directory 用户和组的配置 我们强烈建议您 在导入后下载所有用户和组，以避免出现访问控制策略和其他策略 SSL 策略中的问题。（集成 > 其他集成 > 领域，然后点击 （立即下载）。

• 导入为新配置 (Import as new)

系统导入所选重复配置，将系统生成的编号附加到名称以使其唯一。（可以在完成导入过程之前更改此名称。）设备上的原始配置保持不变。

系统提供的解决方法选项取决于部署是否使用域，以及导入的配置是在当前域中定义的配置的重复，还是在当前域的祖先或后代中定义的配置的重复。下表列出系统何时提供或不提供解决方法选项。

解决方法选项	Cisco Secure Firewall Management Center		受管设备
	在当前域中重复	在祖先域或后代域中重复	
保持现有配置 (Keep existing)	兼容	兼容	兼容
替换现有配置 (Replace existing)	是	不兼容	是
保留最新配置 (Keep newest)	是	不兼容	是
导入为新配置 (Import as new)	兼容	兼容	兼容

当导入包含使用干净或自定义检测文件列表的文件策略的访问控制策略，并且文件列表出现重复名称冲突时，系统会提供上表中所述的冲突解决方法选项，但是系统对策略和文件列表执行的操作会有所差异，如下表所述：

解决方法选项	系统操作	
	访问控制策略及其关联的文件策略导入为新策略，并且合并文件列表	现有访问控制策略及其关联的文件策略和文件列表保持不变
保持现有配置 (Keep existing)	不兼容	是
替换现有配置 (Replace existing)	是	否
导入为新配置 (Import as new)	是	否

解决方法选项	系统操作	
		访问控制策略及其关联的文件策略导入为新策略，并且合并文件列表
保持最新配置 (Keep newest)，并且导入的访问控制策略为最新策略	是	否
保持最新配置 (Keep newest)，并且现有访问控制策略为最新策略	不兼容	是

如果修改设备上的已导入配置，然后将该配置重新导入到同一设备，则必须选择要保留的配置版本。

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。