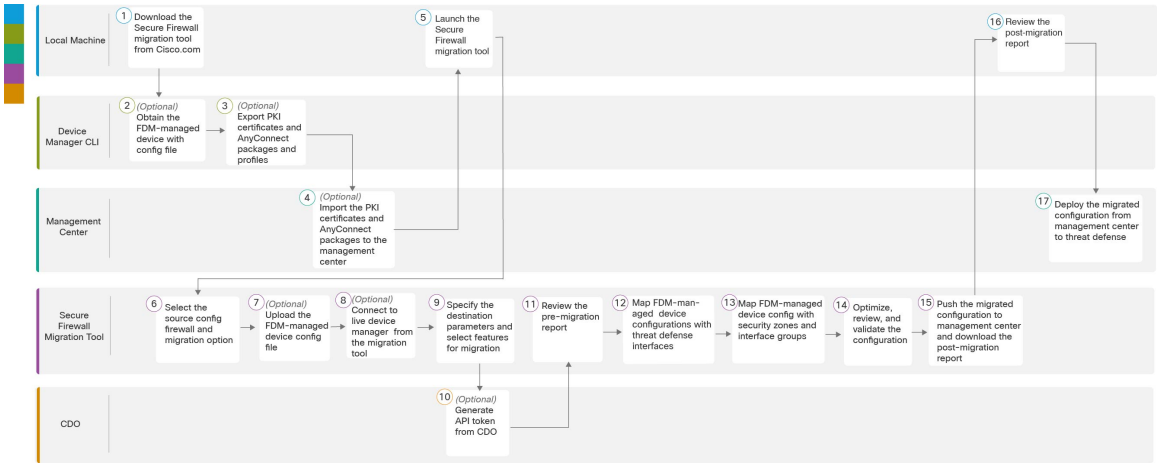
FDM 托管设备到威胁防御工作流程

端到端程序

以下流程图说明了使用 Cisco Secure Firewall 迁移工具将 FDM 托管设备迁移到威胁防御的工作流程。



	工作空间	步骤
1	本地计算机	从 Cisco.com 下载最新版本的 Cisco Secure Firewall 迁移工具。有关详细步骤，请参阅从 Cisco.com 下载 Cisco Secure Firewall 迁移工具。
2	设备管理器 CLI	（可选）获取 FDM 托管设备配置文件：要从设备管理器 CLI 获取 FDM 托管设备配置文件，请参阅获取 FDM 托管设备配置文件。获取 FDM 托管设备配置文件， 第 3 页如果要从 Cisco Secure Firewall 迁移工具连接 FDM 托管设备，请跳至步骤 3。

	工作空间	步骤
3	设备管理器 CLI	（可选）导出 PKI 证书和 AnyConnect 软件包和配置文件：仅当您计划将站点间 VPN 和 RA VPN 功能从 FDM 托管设备迁移到威胁防御时，才需要执行此步骤。要从设备管理器 CLI 导出 PKI 证书，请参阅从设备管理器导出 PKI 证书并导入防火墙管理中心。要从设备管理器 CLI 导出 AnyConnect 软件包和配置文件，请参阅检索 AnyConnect 文件包和配置文件。如果您不打算迁移站点间 VPN 和 RA VPN，请跳至步骤 7。
4	管理中心	（可选）将 PKI 证书和 AnyConnect 软件包导入管理中心：要将 PKI 证书导入管理中心，请参阅从设备管理器导出 PKI 证书并导入防火墙管理中心 和检索 AnyConnect 文件包和配置文件。
5	本地计算机	在本地计算机上启动 Cisco Secure Firewall 迁移工具，请参阅启动 Cisco Secure Firewall 迁移工具。
6	Cisco Secure Firewall 迁移工具	要选择源配置防火墙和迁移选项，请参阅选择源配置和设备管理器迁移选项
7	Cisco Secure Firewall 迁移工具	（可选）上传从设备管理器 CLI 获取的 FDM 托管设备配置文件，请参阅上传 FDM 配置捆绑包。如果您计划连接到实时 FDM 托管设备，请跳至步骤 8。
8	Cisco Secure Firewall 迁移工具	您可以直接从 Cisco Secure Firewall 迁移工具连接到实时设备管理器。有关详细信息，请参阅从 Cisco Secure Firewall 迁移工具连接至 FDM 托管设备。
9	Cisco Secure Firewall 迁移工具	在此步骤中，您可以指定迁移的目标参数。有关详细步骤，请参阅为 Cisco Secure Firewall 迁移工具指定目标参数。
10	CDO	（可选）此步骤为可选，并且仅当您选择云交付的防火墙管理中心作为目标管理中心时才需要。有关详细步骤，请参阅为 Cisco Secure Firewall 迁移工具指定目标参数。
11	Cisco Secure Firewall 迁移工具	导航到下载迁移前报告的位置并查看报告。有关详细步骤，请参阅查看迁移前报告。
12	Cisco Secure Firewall 迁移工具	Cisco Secure Firewall 迁移工具允许您将 FDM 托管设备配置与威胁防御接口进行映射。有关详细步骤，请参阅将 FDM 托管设备配置与 Secure Firewall 设备管理器 威胁防御 接口映射。
13	Cisco Secure Firewall 迁移工具	为确保正确地迁移 FDM 托管设备配置，请将 FDM 托管设备接口映射到相应的威胁防御接口对象、安全区和接口组。有关详细步骤，请参阅将 FDM 托管设备接口映射到安全区。
14	Cisco Secure Firewall 迁移工具	优化并仔细检查配置并验证它是否正确且与您需要的威胁防御设备配置方式匹配。有关详细步骤，请参阅优化、检查和验证要迁移的配置。

	工作空间	步骤
15	Cisco Secure Firewall 迁移工具	迁移过程中的这一步骤会将迁移的配置发送到管理中心，并允许您下载迁移后报告。有关详细步骤，请参阅将迁移的配置推送到管理中心。
16	本地计算机	导航到下载迁移后报告的位置并查看报告。有关详细步骤，请参阅查看迁移后报告并完成迁移。
17	管理中心	将迁移的配置从管理中心部署到威胁防御。有关详细步骤，请参阅查看迁移后报告并完成迁移。

迁移的前提条件

在迁移 FDM 托管设备配置之前，请执行以下活动：

从 Cisco.com 下载 Cisco Secure Firewall 迁移工具

开始之前

您必须拥有 Windows 10 64 位或者 macOS 10.13 或更高版本的计算机，并通过互联网连接至 Cisco.com。

步骤 1 在您的计算机上，为 Cisco Secure Firewall 迁移工具创建一个文件夹。

建议您不要在此文件夹中存储任何其他文件。当 Cisco Secure Firewall 迁移工具启动时，它会将日志、资源和所有其他文件置于此文件夹中。

注释 每当您下载最新版本的 Cisco Secure Firewall 迁移工具时，请确保创建新文件夹，而不使用现有文件夹。

步骤 2 浏览到 https://software.cisco.com/download/home/286306503/type，然后点击**防火墙迁移工具 (Firewall Migration Tool)**。

上面的链接会引导您进入防火墙 NGFW Virtual 下面的 Cisco Secure Firewall 迁移工具。您还可以从 威胁防御 设备下载区域中下载 Cisco Secure Firewall 迁移工具。

步骤 3 将 Cisco Secure Firewall 迁移工具的最新版本下载到您创建的文件夹中。

下载适用于 Windows 或 macOS 计算机的 Cisco Secure Firewall 迁移工具的相应可执行文件。

获取 FDM 托管设备配置文件

您可以使用以下方法之一获取 FDM 托管设备配置文件：

- 导出 FDM 托管设备配置文件，第 4 页
- 从 Cisco Secure Firewall 迁移工具连接至 FDM 托管设备，第 13 页

导出 FDM 托管设备配置文件

仅当您要手动上传 FDM 托管设备配置文件时，才需要执行此任务。可以使用威胁防御 API 从设备管理器导出配置文件。导出配置后，系统会创建 ZIP 文件。可以将 ZIP 文件下载到本地工作站。配置本身表示为在 JSON 格式文本文件中使用属性-值对定义的对象。

导出时，必须指定导出文件中所含的配置。完整导出包括导出 zip 文件中的所有配置。

导出 zip 文件可能包括以下内容：

- 定义各已配置对象的属性-值对。所有可配置项均建模为对象，而不仅仅是设备管理器中称为“对象”的那些对象。
- 远程访问 VPN、AnyConnect 软件包和任何其他引用文件，如客户端配置文件 XML 文件、DAP XML 文件和 Hostscan 软件包。
- 如果已配置自定义文件策略，则参考干净列表或自定义检测列表。

步骤 1 创建用于导出的 JSON 对象正文。

示例：

以下是 JSON 对象的示例。

```
  "diskFileName": "string",
  "encryptionKey": "*********",
  "doNotEncrypt": false,
  "configExportType": "FULL_EXPORT",
  "deployedObjectsOnly": true,
  "entityIds": [
    "string"
  ],
  "jobName": "string",
  "type": "scheduleconfigexport"
}
```

属性包括：

- **diskFileName** -（可选）导出 zip 文件的名称。如果不指定名称，系统会默认生成一个名称。即使指定名称，系统也可能在名称之后附加某些字符以确保唯一性。名称的最大长度为 60 个字符。
- **encryptionKey** - zip 文件的加密密钥。如果不想加密文件，请跳过此字段并改为指定 **doNotEncrypt: true**。如果指定密钥，则在将 zip 文件下载至本地计算机后，可使用该密钥打开 zip 文件。导出的配置文件以明文形式公开密钥、密码和其他敏感数据（否则将无法导入）。在这种情况下，您可能希望应用加密密钥来保护敏感数据。系统使用 AES 256 加密。
- **doNotEncrypt** -（可选）导出文件应该加密 (false) 还是不加密 (true)。默认值为 false，这意味着必须指定非空的加密密钥属性。如果指定 true，则将忽略加密密钥属性。
- **configExportType** - 可以选择以下任何导出类型来导出配置文件：
  - FULL_EXPORT - 在导出文件中包括整个配置。**这是默认选项并应在要迁移时选中**。

- **deployedObjectsOnly** -（可选）是否仅在对象已部署时才将其包含在导出文件中。默认值为 false，表示导出中包含所有待处理更改。指定 true 以排除待处理更改。
- **entityIds** - 一组起始点对象的身份列表，其中对象以逗号分隔并括在 [方括号] 中。PARTIAL_EXPORT 作业需要此列表。列表中的各项均可以是 UUID 值或与 "id=uuid-value"、"type=object-type" 或 "name=object-name" 等模式匹配的属性值对。例如，"type=networkobject"
  - type 可以是叶实体（例如网络对象），也可以是一组叶类型的别名。一些典型的类型别名包括：network（NetworkObject 和 NetworkObjectGroup）、port（所有 TCP/UDP/ICMP 端口、协议和组类型）、url（URL 对象和组）、ikepolicy（IKE V1/V2 策略）、ikeproposal（Ike V1/V2 提议）、identitysource（所有身份源），certificate（所有证书类型）、object（将在“对象”(Objects) 页面上的设备管理器中列出的所有对象/组类型）、interface（所有网络接口）、s2svpn（所有站点间 VPN 相关类型）、ravpn（所有 RA VPN 相关类型）和 vpn（s2svpn 和 ravpn）。
  - 所有对象及其传出引用后代将包含在 PARTIAL_EXPORT 输出文件中。所有不可导出对象都将从输出中排除，即使您指定其身份。使用相应资源类型的 GET 方法获取目标对象的 UUID、类型或名称。

  例如，要导出所有网络对象以及名为 myaccessrule 的访问规则和由 UUID 标识的两个对象，可指定：

  ```
  "entityIds": [
     "type=networkobject",
     "id=bab3e3cd-8c70-11e9-930a-1f12ee87d473",
     "name=myaccessrule",
     "acc2e3cd-8c70-11e9-930a-1f12ee87b286"
     ]",
  ```

- **jobName** -（可选）在检索作业状态时，给出导出作业名称可以更轻松地进行查找。
- **type** - 作业类型，始终为 **scheduleconfigexport**。

步骤 2 发布对象。

示例：

curl 命令会如下所示：

```
  curl -X POST --header 'Content-Type: application/json' --header 'Accept: application/json' -d '{ \
   "configExportType": "FULL_EXPORT", \
   "type": "scheduleconfigexport" \
}' 'https://10.89.5.38/api/fdm/latest/action/configexport'
```

步骤 3 验证响应。

您应获得的响应代码为 200。如果发布了最小的 JSON 对象，则成功的响应正文将类似于以下内容：

```
{
  "version": null,
  "scheduleType": "IMMEDIATE",
  "user": "admin",
  "forceOperation": false,
  "jobHistoryUuid": "c7a8ba61-629a-11e9-8b8d-0fcc3c9d6d0b",
  "ipAddress": "10.24.5.177",
  "diskFileName": "export-config-1",
  "encryptionKey": null,
  "doNotEncrypt": true
  "configExportType": "FULL_EXPORT",
  "deployedObjectsOnly": false,
```

```
  "entityIds": null,
  "jobName": "Config Export",
  "id": "c79be920-629a-11e9-8b8d-85231be77de0",
  "type": "scheduleconfigexport",
  "links": {
    "self": "https://10.89.5.38/api/fdm/latest
/action/configexport/c79be920-629a-11e9-8b8d-85231be77de0"
  }
}
```

步骤 4 检查配置导出的状态。

导出需要一些时间才能完成。配置越大，作业所需的时间就越多。检查作业状态，确保其成功完成，然后再尝试下载文件。

检索状态的最简单方法是使用 **GET /jobs/configexportstatus**。例如，curl 命令会如下所示：

```
curl -X GET --header 'Accept: application/json'
'https://10.89.5.38/api/fdm/latest/jobs/configexportstatus'
```

成功完成的作业会显示以下状态：

```
{
  "version": "hdy62yf5xp3vf",
  "jobName": "Config Export",
  "jobDescription": null,
  "user": "admin",
  "startDateTime": "2019-04-19 13:14:54Z",
  "endDateTime": "2019-04-19 13:14:56Z",
  "status": "SUCCESS",
  "statusMessage": "The configuration was exported successfully",
  "scheduleUuid": "1ef502ad-62a5-11e9-8b8d-074ebc750708",
  "diskFileName": "export-config-1.zip",
  "messages": [],
  "configExportType": "FULL_EXPORT",
  "deployedObjectsOnly": false,
  "entityIds": null,
  "id": "1f0aad8e-62a5-11e9-8b8d-bb1ebb4d1300",
  "type": "configexportjobstatus",
  "links": {
    "self": "https://10.89.5.38/api/fdm/latest
/jobs/configexportstatus/1f0aad8e-62a5-11e9-8b8d-bb1ebb4d1300"
  }
}
```

步骤 5 下载导出文件。

导出作业完成后，系统会将导出文件写入系统磁盘，并将其称为配置文件。可以使用 **GET /action/downloadconfigfile/{objId}** 将此导出文件下载至本地计算机。

要获取可用文件的列表，请使用 GET /action/configfiles 方法。

```
curl -X GET --header 'Accept: application/json'
'https://10.89.5.38/api/fdm/latest/action/configfiles'
```

响应将显示项目列表，每个项目都是一个配置文件。例如，以下列表显示 2 个文件。所有文件的 ID 均为默认值，最佳做法是忽略 ID 并改为使用 diskFileName。

```
{
  "items": [
    {
      "diskFileName": "export-config-2.zip",
      "dateModified": "2019-04-19 13:32:28Z",
```

```
      "sizeBytes": 10182,
      "id": "default",
      "type": "configimportexportfileinfo",
      "links": {
        "self": "https://10.89.5.38/api/fdm/latest/action/configfiles/default"
      }
    },
    {
      "diskFileName": "export-config-1.zip",
      "dateModified": "2019-04-19 13:14:56Z",
      "sizeBytes": 10083,
      "id": "default",
      "type": "configimportexportfileinfo",
      "links": {
        "self": "https://10.89.5.38/api/fdm/latest/action/configfiles/default"
      }
    }
  ],
```


使用 diskFileName 作为对象 ID 下载文件。

```
curl -X GET --header 'Accept: application/octet-stream'
'https://10.89.5.38/api/fdm/latest/action/downloadconfigfile/export-config-2.zip'
```

文件将下载至默认下载文件夹。如果是从 API Explorer 发出 GET 方法，且浏览器配置为提示下载位置，系统会提示您保存文件。

注释 下载成功后会出现 200 返回代码，但无响应正文。

从设备管理器导出 PKI 证书并导入防火墙管理中心

Cisco Secure Firewall 迁移工具支持将基于证书的 VPN 迁移到管理中心。

导入的 FDM 托管设备配置捆绑包包含了证书负载和密钥。这可以在管理中心导入

作为迁移前活动的一部分，在目标管理中心将信任点或VPN证书作为PKI对象手动迁移。必须在使用 Cisco Secure Firewall 迁移工具开始迁移之前执行此活动。

步骤 1 从配置捆绑包中，复制证书负载（值介于 -----BEGIN CERTIFICATE----- 和 -----END CERTIFICATE----- 之间）和密钥（值介于 -----BEGIN RSA PRIVATE KEY----- 和 -----END RSA PRIVATE KEY----- 之间）。

示例：


```
   "type":"identitywrapper",
   "action":"CREATE",
   "data":{
      "version":"girr7veykdjvx",
      "name":"RA_VPN_Cert",
      "cert":"-----BEGIN
[redacted]
CERTIFICATE-----",
      "privateKey":"-----BEGIN RSA PRIVATE
[redacted]
RSA PRIVATE KEY-----",
      "issuerCommonName":"mojave-rsa-root-2048-sha384.cisco.com, CN =
```

```
mojave-rsa-root-2048-sha384.cisco.com",
      "issuerCountry":"US",
      "issuerOrganization":"Cisco",
      "subjectCommonName":"fdm-ra-vpn-cert.cisco.com, CN = 172.16.10.50",
      "subjectCountry":"US",
     "subjectDistinguishedName":" C = US, O = Cisco, CN = fdm-ra-vpn-cert.cisco.com, CN = 172.16.10.50",

      "subjectOrganization":"Cisco",
      "validityStartDate":"Jan  1 12:00:00 2012 GMT",
      "validityEndDate":"Sep  1 12:00:00 2034 GMT",
      "isSystemDefined":false,
      "keyType":"RSA",
      "keySize":2048,
      "allowWeakCert":false,
      "signatureHashType":"SHA1",
      "weakCertificate":true,
      "id":"9d0a8efb-01fa-11ed-8d7b-1f4809c453ac",
      "type":"internalcertificate"
   }
}
```

步骤 2 将 PKI 证书导入管理中心 (**ObjectManagement** > **PKIObjects**)。

有关详细信息，请参阅防火墙管理中心配置指南。

手动创建的 PKI 对象现在可以在 **VPN Tunnels (VPN 隧道)** 部分下的**查看和验证 (Review and Validate)** 页面中的 Cisco Secure Firewall 迁移工具中使用。

检索 AnyConnect 文件包和配置文件

开始之前

AnyConnect 配置文件为可选，并可通过管理中心或 Cisco Secure Firewall 迁移工具进行上传。

- 管理中心上的远程访问 VPN 至少需要一个 AnyConnect 软件包。
- 如果配置包含 Hostscan 和 External Browser 软件包，则必须上传这些软件包。
- 所有软件包都必须作为迁移前活动的一部分添加到管理中心。
- 必须通过 Cisco Secure Firewall 迁移工具来添加 Dap.xml 和 Data.xml。

检查设备管理器上可用的软件包以进行下载。

步骤 1 检查设备管理器上可用的软件包以进行下载。

您可以使用 **GET /object/anyconnectpackagefiles** API 来查看设备上的软件包。

```
curl -X GET --header 'Accept: application/json' '
 https://10.89.5.38/api/fdm/v6/object/anyconnectpackagefiles'
```

此命令可用于检索设备管理器上的可用 AnyConnect 软件包。

```
{
  "items": [
    {
      "version": "gx5yk7xkdsosu",
      "name": "anyconnect-win-4.10.02086-webdeploy-k9.pkg",
      "md5Checksum": "63e4a86fc7c68d7769b6a1b2976ffa73",
      "description": null,
      "diskFileName": "12f0988e-01fb-11ed-8d7b-07ecdd54c7bf.pkg",
      "platformType": "WINDOWS",
      "id": "133f2dbf-01fb-11ed-8d7b-89d64ab04e18",
      "type": "anyconnectpackagefile",
      "links": {
        "self": "
https://10.89.5.38/api/fdm/v6/object/anyconnectpackagefiles/133f2dbf-01fb-11ed-8d7b-89d64ab04e18"
      }
    }
  ],
}
```


响应中的 `diskFilename` 可用于下载 AnyConnect 软件包。

步骤 2 下载 AnyConnect 软件包。

您可以使用 **GET /action/downloaddiskfile/{objId}** 将 AnyConnect 软件包下载到本地工作站。要使用的对象 ID 是 AnyConnect 数据包响应的 diskFileName (12f0988e-01fb-11ed-8d7b-07ecdd54c7bf.pkg)。

```
curl -X GET --header 'Accept: application/octet-stream'
' https://10.89.5.38/api/fdm/v6/action/downloaddiskfile/12f0988e-01fb-11ed-8d7b-07ecdd54c7bf.pkg'
```

步骤 3 检查设备管理器上的可用 AnyConnect 配置文件。

注释 Cisco Secure Firewall 迁移工具会自动从设备管理器中检索 AnyConnect 配置文件。只有当您要手动上传 AnyConnect 配置文件时才需要执行此步骤。

您可以使用 **GET /object/anyconnectclientprofiles** 来检查设备管理器上的可用配置文件。

```
curl -X GET --header 'Accept: application/json'
'https://10.196.155.3:12272/api/fdm/v6/object/anyconnectclientprofiles'
```

系统将显示以下响应：


```
  "items": [

    {
      "version": "jqtwzirf36qke",
      "name": "AnyConnect_VPN_Profile",
      "md5Checksum": "e4ba581f84daec6f24c209f9f7f9e1fb",
      "description": null,
      "diskFileName": "1629395a-0384-11ed-8d7b-ab1a2a5ad583.xml",
      "anyConnectModuleType": "ANY_CONNECT_CLIENT_PROFILE",
      "id": "1754c10b-0384-11ed-8d7b-6b8e36ae1285",
      "type": "anyconnectclientprofile",
    }
  ]
}
```


响应中的 `diskFilename` 可用于下载 AnyConnect 配置文件。

步骤 4 下载 AnyConnect 配置文件。

您可以使用 **GET /action/downloaddiskfile/{objId}** 将 AnyConnect 软件包下载到本地工作站。要使用的 objId 是 AnyConnect 配置文件响应中的 diskFileName (1629395a-0384-11ed-8d7b-ab1a2a5ad583.xml)。

```
curl -X GET --header 'Accept: application/octet-stream'
'https://10.196.155.3:12272/api/fdm/v6/action/downloaddiskfile/1629395a-0384-11ed-8d7b-ab1a2a5ad583.xml'
```

步骤 5 将下载的软件包导入管理中心 (**ObjectManagement >**) > **VPN** > **AnyConnect 文件 (AnyConnect File)**。

1. 必须从**查看和验证 (Review and Validate)** > **远程访问 VPN (Remote Access VPN)** > **AnyConnect 文件 (AnyConnect File)** 部分中的 Cisco Secure Firewall 迁移工具将 Dap.xml 和 Data.xml 上传到管理中心。
2. AnyConnect 配置文件可以直接上传到管理中心，也可以通过**查看和验证 (Review and Validate)** > **远程访问 VPN (Remote Access VPN)** > **AnyConnect 文件 (AnyConnect File)** 部分中的 Cisco Secure Firewall 迁移工具来上传。

现在可以在 Cisco Secure Firewall 迁移工具中使用手动上传的文件

运行迁移

启动 Cisco Secure Firewall 迁移工具

注释 当您启动 Cisco Secure Firewall 迁移工具时，会在单独的窗口中打开控制台。进行迁移时，控制台会显示 Cisco Secure Firewall 迁移工具中的当前步骤的进度。如果控制台未显示在屏幕上，则它最有可能隐藏在 Cisco Secure Firewall 迁移工具后。

开始之前

- 从 Cisco.com 下载 Cisco Secure Firewall 迁移工具
- 查看并验证支持的迁移目标管理中心部分中的要求。
- 确保您的计算机带有最新版本的 Google Chrome 浏览器以运行 Cisco Secure Firewall 迁移工具。有关如何将 Google Chrome 设置为默认浏览器的信息，请参阅将 Chrome 设置为默认 Web 浏览器。
- 如果您计划迁移大型配置文件，请配置睡眠设置，以便在迁移推送时系统不会进入睡眠状态。

步骤 1 在您的计算机上，导航至已在其中下载 Cisco Secure Firewall 迁移工具的文件夹。

步骤 2 执行以下操作之一：

- 在您的 Windows 计算机上，双击 Cisco Secure Firewall 迁移工具可执行文件，在 Google Chrome 浏览器中启动它。

如果出现提示，请点击**是 (Yes)**，以允许 Cisco Secure Firewall 迁移工具对您的系统作出更改。

Cisco Secure Firewall 迁移工具会创建所有相关文件并将文件存储在其驻留的文件夹中，包括日志和资源文件夹。

- 在 Mac 上，将 Cisco Secure Firewall 迁移工具 `*.command` 文件移动到所需文件夹，启动终端应用，浏览到安装防火墙迁移工具的文件夹并运行以下命令：

```
# chmod 750 Firewall_Migration_Tool-version_number.command
# ./Firewall_Migration_Tool-version_number.command
```

Cisco Secure Firewall 迁移工具会创建所有相关文件并将文件存储在其驻留的文件夹中，包括日志和资源文件夹。

提示 当您尝试打开 Cisco Secure Firewall 迁移工具时，因为没有可识别的开发人员在 Apple 中注册 Cisco Secure Firewall 迁移工具，系统会显示警告对话框。有关无法识别的开发人员打开应用的信息，请参阅无法识别的开发人员打开应用。

注释 使用 MAC 终端 zip 方法。

步骤 3 在**最终用户许可协议 (End User License Agreement)** 页面上，如果要与思科共享遥测信息，请点击**我同意与思科成功网络共享数据 (I agree to share data with Cisco Success Network)**，否则请点击**我稍后再执行 (I'll do later)**。

当您同意将统计信息发送到思科成功网络时，系统会提示您使用 Cisco.com 帐户登录。如果您选择不向思科成功网络发送统计信息，则使用本地凭证登录 Cisco Secure Firewall 迁移工具。

步骤 4 在**重置密码**页面上，输入您的旧密码、新密码，然后确认新密码。

新密码必须包含 8 个或更多字符，并且必须包含大写和小写字母、数字和特殊字符。

步骤 5 点击**重置 (Reset)**。

步骤 6 使用新密码登录。

注释 如果忘记了密码，请从 <*migration_tool_folder*> 中删除所有现有数据并重新安装 Cisco Secure Firewall 迁移工具。

步骤 7 查看迁移前核对表并确保您已完成所有列出的项目。

如果您未完成该核对表中的一个或多个项目，请完成所有项目，然后再继续。

步骤 8 点击**新迁移 (New Migration)**。

步骤 9 在**软件更新检查 (Software Update Check)** 屏幕上，如果您不确定自己是否正在运行 Cisco Secure Firewall 迁移工具的最新版本，请点击 Cisco.com 上的链接以验证版本。

步骤 10 点击**继续 (Proceed)**。

下一步做什么

您可以继续执行以下步骤：

- 如果已将 FDM 托管设备配置导出到您的计算机，请继续执行上传 FDM 配置捆绑包。

选择源配置和设备管理器迁移选项

步骤 1 从下拉列表中选择**源防火墙供应商 (Source Firewall Vendor)**，然后点击**开始迁移 (Start Migration)**。

步骤 2 选择要用于迁移 FDM 托管设备的迁移选项。

以下是可用的选项：

- **迁移 Firepower 设备管理器（仅限共享配置）**

  此选项允许将共享配置从设备管理器迁移到目标管理中心。此选项应用于分阶段迁移，以便最初迁移共享配置，并且可以在以后迁移设备配置。此使用案例不涉及停机时间。

- **迁移 Firepower 设备管理器（包括设备和共享配置）**

  此选项允许将共享设备配置迁移到目标管理中心。作为此迁移的一部分，源威胁防御会从设备管理器移至管理中心。成功完成迁移后，管理中心将继续管理威胁防御设备。因此，在此使用案例中，源和目标是同一威胁防御设备。当威胁防御设备被移至管理中心时，此使用案例会涉及停机时间。

  要使用此选项迁移配置，请在迁移前练习中执行以下操作：

  1. 登录设备管理器并导航至**对象 (Objects)** 部分。
  2. 点击**身份源 (Identity Sources)**，然后从**预设过滤器 (Preset filters)** 中选择 **AD 领域 (AD Realm)**。
  3. 在**操作 (Actions)** 下，点击加密类型为 **LDAPS** 或 **STARTTLS** 的特定领域的 **编辑**（✎）。
  4. 在**目录服务器配置 (Directory Server Configuration)** 中，点击服务器名称旁边的**下拉**箭头。
  5. 在**加密 (Encryption)** 部分下，将加密类型更改为**无 (NONE)**，然后点击**确定 (OK)**。
  6. 部署更改。

  注释 将配置迁移到管理中心后，您可以将管理中心中的 AD 领域的加密类型恢复为 LDAPS 或 STARTTLS。有关详细步骤，请参阅查看迁移后报告并完成迁移。

- **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）**

  此选项允许将 FDM 托管设备配置迁移到已向目标管理中心注册的威胁防御。源 FDM 托管设备的配置将被迁移到注册到目标管理中心的用户所选的目标威胁防御。此使用案例不涉及停机时间。

上传 FDM 配置捆绑包

开始之前

将配置文件作为 `.zip` 从源设备管理器导出。

注释 以下两个选项将支持手动上传：

- 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）

步骤 1 在**提取 FDM 信息 (Extract FDM Information)** 屏幕的**手动上传 (Manual Upload)** 部分中，点击**上传 (Upload)** 以上传 FDM 托管配置捆绑包。如果配置捆绑包已加密，请在文本框中输入密钥，以便 Cisco Secure Firewall 迁移工具解密捆绑包。

步骤 2 浏览到 FDM 托管设备配置文件所在的位置，然后点击**打开 (Open)**。

Cisco Secure Firewall 迁移工具会上传配置捆绑包。对于大型配置文件，此步骤需要的时间较长。控制台提供一个逐行的进度日志视图，其中包含正在解析的 FDM 托管设备配置。如果您没有看到控制台，可以在 Cisco Secure Firewall 迁移工具后的单独窗口中找到它

步骤 3 点击**开始解析 (Start Parsing)**。

解析摘要部分显示解析状态。

步骤 4 查看 Cisco Secure Firewall 迁移工具在上传的配置文件中检测和解析的元素的摘要信息。

步骤 5 点击**下一步 (Next)**，选择目标参数。

下一步做什么

为 Cisco Secure Firewall 迁移工具指定目标参数

从 Cisco Secure Firewall 迁移工具连接至 FDM 托管设备

开始之前

Cisco Secure Firewall 迁移工具可以连接到要迁移的 FDM 托管设备，并提取所需的配置信息。所有三个使用案例都支持实时连接到 FDM 托管设备。

- 下载并启动 Cisco Secure Firewall 迁移工具。
- 选择要执行的 FDM 托管设备到管理中心迁移的使用案例。
- 获取管理 IP 地址、设备管理器的管理员凭证。

步骤 1 在**提取 FDM 信息 (ExtractFDM Information)** 屏幕上的**连接 FDM (Connect to FDM)** 部分中，点击**连接 (Connect)** 以连接到要迁移的 FDM 托管设备。

步骤 2 在 **FDM 登录 (FDM Login)** 屏幕中，输入以下信息：

1. 在 **FDM IP 地址/主机名 (FDM IP Address/Hostname)** 字段中，输入 FDM 的管理 IP 地址或主机名。点击**登录 (Login)**。
2. 在**用户名 (Username)**、**密码 (Password)** 字段中，输入相应的管理员登录凭证。
3. 点击**登录 (Login)**。

当 Cisco Secure Firewall 迁移工具连接到 FDM 托管设备时，会在继续迁移之前对 FDM 托管设备执行一系列合规性检查。前提条件和最佳实践部分介绍了这些检查。如果检查成功，迁移将继续执行下一步。

Cisco Secure Firewall 迁移工具连接到 FDM 托管设备，一旦合规性检查成功，该工具就会开始提取配置信息。在提取成功完成后，将显示已解析的摘要页面。

解析摘要部分显示解析状态。

步骤 3 查看 Cisco Secure Firewall 迁移工具从 FDM 托管设备检测和解析的元素的摘要信息。

步骤 4 点击**下一步 (Next)**，选择目标参数。

下一步做什么

为 Cisco Secure Firewall 迁移工具指定目标参数

为 Cisco Secure Firewall 迁移工具指定目标参数

开始之前

如果您使用的是 CDO 上托管的迁移工具的云版本，请跳至步骤 3。

- 获得现场防火墙管理中心的 管理中心 的 IP 地址。
- （可选）如果所选流为**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）**迁移到 管理中心，则将目标威胁防御设备添加到管理中心。请参阅将设备添加到防火墙管理中心
- 如果它要求您在**检查和验证 (Review and Validate)** 页面中将 IPS 或文件策略应用于 ACL，我们强烈建议您在迁移之前在 管理中心 上创建策略。使用相同的策略，因为 Cisco Secure Firewall 迁移工具从连接的管理中心获取策略。创建新策略并将其分配给多个访问控制列表可能会降低性能，也可能导致推送失败。

步骤 1 在**选择目标 (Select Target)** 屏幕的**防火墙管理 (Firewall Management)** 部分中，执行以下操作：

- 要迁移到本地防火墙管理中心，请执行以下操作：

a) 点击**本地 FMC (On-Prem FMC)** 单选按钮。
b) 输入管理中心的 IP 地址或完全限定域名 (FQDN)。
c) 在**域**下拉列表中，选择要迁移到的域。

如果您已选择**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）**，则只能迁移到所选域中可用的威胁防御设备。

d) 点击**连接 (Connect)** 并继续**步骤 2**。

- 要迁移到云交付的防火墙管理中心，请执行以下操作：

a) 点击**云交付的 FMC (Cloud-delivered FMC)** 单选按钮。
b) 选择区域并粘贴 CDO API 令牌。要从 CDO 生成 API 令牌，请执行以下步骤：

1. 登录到 CDO 门户。
2. 导航至**设置 (Settings)** > **常规设置 (General Settings)** 并复制 API 令牌。

c) 点击**连接 (Connect)** 并继续**步骤 2**。

步骤 2 在**防火墙管理中心登录 (Firewall Management Center Login)** 对话框中，输入 Cisco Secure Firewall 迁移工具专用帐户的用户名和密码，然后点击**登录 (Login)**。

Cisco Secure Firewall 迁移工具将登录到 管理中心，并检索由该 管理中心管理的一系列 威胁防御设备。您可以在控制台中查看此步骤的进度。

步骤 3 点击**继续 (Proceed)**。

如果您已选择**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）**，则只能迁移到所选域中可用的威胁防御设备。

如果您已选择**迁移 Firepower 设备管理器（仅限共享配置）**

此工作流程中未填充管理中心的威胁防御部分，而只将共享策略（访问控制列表、NAT 和对象）推送到 FMC。您可以选择包括或跳过需要推送到管理中心的共享策略。

如果您已选择**迁移 Firepower 设备管理器（包括设备和共享配置）**

移至管理中心的威胁防御与设备管理器管理的设备相同。在这种情况下不会填充管理中心的威胁防御部分。

步骤 4 在**选择威胁防御 (Choose Threat Defense)** 部分中，执行以下操作之一：

- 点击**选择防火墙威胁防御设备 (Select Firewall Threat Defense Device)**下拉列表，然后选中您要迁移 FDM 托管设备配置的设备。

  选择的 管理中心 域中的设备将按 **IP 地址**和**名称**列出。

  注释 仅当支持的目标威胁防御平台是具有管理中心版本 6.5 或更高版本的 Firewall 1010 时，FDM 5505 迁移支持才适用于共享策略，而不适用于设备特定策略。当您忽略威胁防御并继续时，Cisco Secure Firewall 迁移工具不会将任何配置或策略推送到威胁防御。因此，作为威胁防御设备特定配置的接口和路由以及站点间 VPN 不会迁移。但是，所有其他受支持的配置（共享策略和对象）将迁移，例如 NAT、ACL 和端口对象。远程访问 VPN 是一种共享策略，即使没有威胁防御也可以迁移。

- 点击**忽略威胁防御并继续 (Proceed without Threat Defense)**，将配置迁移到 管理中心。

  当您忽略 威胁防御 并继续时，Cisco Secure Firewall 迁移工具不会将任何配置或策略推送到 威胁防御。因此，作为 威胁防御 设备特定配置的接口和路由以及站点间 VPN 不会迁移。但是，所有其他受支持的配置

（共享策略和对象）将迁移，例如NAT、ACL 和端口对象。远程访问 VPN 是一种共享策略，即使没有威胁防御也可以迁移。

步骤 5 点击**继续 (Proceed)**。

根据迁移的目标，Cisco Secure Firewall 迁移工具允许您选择要迁移的功能。

步骤 6 点击**选择功能 (Select Features)** 部分以查看并选择要迁移到目标的功能。

- 如果要迁移到目标 威胁防御 设备，Cisco Secure Firewall 迁移工具会自动从**设备配置 (Device Configuration)** 和**共享配置 (Shared Configuration)** 部分的 FDM 托管设备配置中选择可用于迁移的功能。您可以根据需要进一步修改默认选择。
- 如果要迁移到 管理中心，Cisco Secure Firewall 迁移工具会自动从**共享配置 (Shared Configuration)** 部分的 FDM 托管设备配置中选择可用于迁移的功能。您可以根据需要进一步修改默认选择。

  注释 如果您已选择**迁移 Firepower 设备管理器（仅限共享配置）**，则**设备配置 (Device Configuration)** 部分不可用。

- Cisco Secure Firewall 迁移工具在迁移过程中支持以下访问控制功能：
  - 填充目标安全区域 - 在迁移期间启用 ACL 的目标区域映射。

    路由查找逻辑仅限于静态路由和连接路由，而不考虑 PBR、动态路由和 NAT。接口网络配置用于导出连接路由信息。

    根据源和目标网络对象组的性质，此操作可能会导致规则爆炸。

  - 自定义深度检查 - 检查封装的流量并通过快速路径提高性能
    - 提高性能 - 可对从早期处理中受益的其他任何连接使用快速路径或加以阻止。

    Cisco Secure Firewall 迁移工具可识别源配置中的封装隧道流量规则，并将其迁移为预过滤器隧道规则。您可以验证预过滤器策略下迁移的隧道规则。预过滤器策略与 管理中心 上的已迁移访问控制策略相关联。

    迁移为预过滤器隧道规则的协议如下：
    - GRE (47)
    - IPv4 封装 (4)
    - IPv6 封装 (41)
    - Teredo 隧道 (UDP:3544)

    注释 如果不选择预过滤器选项，所有隧道流量规则都将迁移为不受支持的规则。

    FDM 托管设备配置中的 ACL 隧道规则（GRE 和 IPnIP）当前已默认进行双向迁移。您现在可以在访问控制状态选项中将目标的规则方向指定为双向或单向。

- Cisco Secure Firewall 迁移工具支持以下用于 VPN 隧道迁移的接口和对象：
  - 基于策略（加密映射）- 如果目标 管理中心 和 威胁防御 为 6.6 或更高版本。

- 基于路由 (VTI) - 如果目标 管理中心 和 威胁防御 为 6.7 或更高版本。

- 如果目标管理中心是 7.2 或更高版本，Cisco Secure Firewall 迁移工具支持迁移远程访问 VPN。远程访问 VPN 是一种无需威胁防御即可迁移的共享策略。如果选择使用威胁防御进行迁移，则威胁防御版本应为 7.0 或更高版本。
- （可选）在**优化**部分中，选择**仅迁移引用的对象**，以仅迁移访问控制策略和 NAT 策略中引用的对象。

  注释 当您选择此选项时，不会迁移 FDM 托管设备配置中未引用的对象。这可以优化迁移时间并从配置中清除未使用的对象。
- （可选）在**优化**部分中，选择**对象组搜索**以优化 威胁防御 上访问策略的内存利用率。

步骤 7 点击**继续 (Proceed)**。

步骤 8 在**规则转换/流程配置 (Rule Conversion/ Process Config)**部分中，点击**开始转换 (Start Conversion)** 以启动转换。

步骤 9 查看 Cisco Secure Firewall 迁移工具转换的元素的摘要。

要检查配置文件是否已成功上传和解析，请在继续迁移之前下载并验证**迁移前报告**。

步骤 10 点击**下载报告 (Download Report)**，并保存**迁移前报告 (Pre-Migration Report)**。

系统也会在 `Resources` 文件夹中保存**迁移前报告**的一个副本（与 Cisco Secure Firewall 迁移工具处于相同的位置）。

查看迁移前报告

如果您在迁移期间错过下载迁移前报告，请使用以下链接进行下载：

迁移前报告下载终端 — http://localhost:8888/api/downloads/pre_migration_summary_html_format

注释 您只能在 Cisco Secure Firewall 迁移工具正在运行时下载报告。

步骤 1 导航到下载**迁移前报告**的位置。

系统也会在 `Resources` 文件夹中保存**迁移前报告**的一个副本（与 Cisco Secure Firewall 迁移工具处于相同的位置）。

步骤 2 打开**迁移前报告**并仔细检查其内容，以确定可能会导致迁移失败的任何问题。

迁移前报告包括以下信息：

- **总体摘要** - 用于提取 FDM 托管设备配置信息或连接到实时 FDM 托管设备配置的方法。

  可成功迁移到 威胁防御 的受支持 FDM 托管设备配置元素以及为迁移选择的特定 功能的摘要。

  在连接到实时 FDM 托管设备 时，摘要包括命中计数信息（触发 FDM 托管设备规则的次数）及其时间戳信息。

- **出错的配置行** - 因为 Cisco Secure Firewall 迁移工具无法解析而不能成功迁移的 配置元素的详细信息。在 配置上更正这些错误，导出新配置文件，将新配置文件上传到 Cisco Secure Firewall 迁移工具，然后再继续。
- **部分支持的配置** - 仅可部分迁移的 FDM 托管设备配置元素的详细信息。这些配置元素包括含高级选项的规则和对象，其中的规则或对象可在无高级选项的情况下迁移。查看这些行，验证管理中心中是否支持高级选项。如果支持，则计划在使用 Cisco Secure Firewall 迁移工具完成迁移后手动配置这些选项。
- **不支持的配置** - 因 Cisco Secure Firewall 迁移工具不支持迁移这些功能而无法迁移的 FDM 托管设备配置元素的详细信息。查看这些行，验证 管理中心中是否支持每项功能。如果支持，则计划在使用 Cisco Secure Firewall 迁移工具完成迁移后手动配置这些功能。
- **忽略的配置** - 因为不受 管理中心 或 Cisco Secure Firewall 迁移工具支持而被忽略的 FDM 托管设备配置的详细信息。Cisco Secure Firewall 迁移工具不会解析这些行。查看这些行，验证 管理中心中是否支持每项功能。如果支持，则计划手动配置这些功能。

有关 管理中心 和 威胁防御 中受支持功能的更多信息，请参阅管理中心配置指南。

步骤 3 如果**迁移前报告**建议执行纠正操作，请在 接口上完成这些纠正操作，重新导出 FDM 托管设备配置文件，将更新的配置文件上传，然后再继续。

步骤 4 在您的 FDM 托管设备配置文件成功上传和解析之后，返回到 Cisco Secure Firewall 迁移工具，然后点击**下一步 (Next)** 以继续迁移。

下一步做什么

将 FDM 托管设备配置与 Secure Firewall 设备管理器 威胁防御 接口映射

将 FDM 托管设备配置与 Secure Firewall 设备管理器 威胁防御 接口映射

威胁防御 设备必须具有与 FDM 托管设备配置相同或更多的物理接口和端口通道接口。两个设备上的这些接口不需要具有相同的名称。您可以选择所需的接口映射方式。

在**映射威胁防御接口 (Map Threat Defense Interface)** 屏幕上，Cisco Secure Firewall 迁移工具将检索威胁防御 设备上的接口的列表。默认情况下，Cisco Secure Firewall 迁移工具会根据其接口标识符映射 FDM 托管设备和 威胁防御 设备中的接口。例如， FDM 托管设备 接口上的“管理专用”接口会自动映射到 威胁防御 设备上的“管理专用”接口，并且不可更改。

FDM 托管设备接口到 威胁防御 接口的映射因 威胁防御 设备类型而异：

- 如果目标 威胁防御 为本地类型：
  - 威胁防御 必须具有相同或更多数量的已使用 FDM 托管设备接口或端口通道 (PC) 数据接口（FDM托管设备配置中不包括管理专用接口和子接口）。如果其接口数量较少，请在目标 威胁防御 上添加所需类型的接口。
  - 子接口由 Cisco Secure Firewall 迁移工具根据物理接口或端口通道映射创建。
- 如果目标 威胁防御 为容器类型：

- 威胁防御 必须具有相同或更多数量的已使用 FDM 托管设备接口、物理子接口、端口通道或端口通道子接口（FDM托管设备配置中不包括管理专用接口）。如果其接口数量较少，请在目标 威胁防御 上添加所需类型的接口。例如，如果目标 威胁防御 上的物理接口和物理子接口的数量比 FDM 托管设备的接口数量少 100 个，则可以在目标 威胁防御 上创建更多物理接口或物理子接口。
- 子接口不是由 Cisco Secure Firewall 迁移工具创建的。物理接口、端口通道或子接口之间仅允许接口映射。

开始之前

确保您已连接到管理中心 并将目标选择为 威胁防御。有关详细信息，请参阅为 Cisco Secure Firewall 迁移工具指定目标参数 ， 第 14 页。

注释 如果您使用**迁移 Firepower 设备管理器（仅限共享配置）**进行迁移，则此步骤不适用

此步骤仅供参考，适用于**迁移 Firepower 设备管理器（包括设备和共享配置）**。

步骤 1 如果您想要更改接口映射，请点击**威胁防御接口名称 (Threat Defense Interface Name)** 下拉列表，并选择您想要映射到该 接口的接口。

不能更改管理接口的映射。如果 威胁防御 接口已分配到FDM托管设备接口，则您不能从下拉列表中选择该接口。所有已分配的接口将变为灰色且不可用。

您不需要映射子接口。Cisco Secure Firewall 迁移工具会在 威胁防御 设备上为 FDM 托管设备配置中的所有子接口映射子接口。

步骤 2 当您将每个 FDM 托管设备接口映射到 威胁防御 接口时，请点击**下一步 (Next)**。

将 FDM 托管设备接口映射到安全区

注释 如果 FDM 托管设备配置不包括访问列表和 NAT 规则，或者如果您选择不迁移这些策略，则可以跳过此步骤并继续执行 。优化、检查和验证要迁移的配置 ， 第 20 页

为确保正确地迁移FDM托管设备配置，请将FDM托管设备接口映射到相应的 威胁防御 接口对象、安全区。在 FDM 托管设备配置中，访问控制策略和 NAT 策略使用接口名称 (nameif)。在 管理中心 中，这些策略使用接口对象。此外，管理中心策略将按以下项分组接口对象：

- 安全区 - 接口只能属于一个安全区。
- 接口组 - 接口可属于多个接口组。

Cisco Secure Firewall 迁移工具支持接口与安全区和接口组的一对一映射；当安全区或接口组映射到某个接口时，尽管 管理中心 允许，也不可映射到其他接口。有关 管理中心中的安全区和接口组的更多信息，请参阅接口对象：接口组和安全区 。

步骤 1 在**映射安全区和接口组**屏幕上，查看可用接口、安全区和接口组。

步骤 2 要将接口映射到 管理中心 中的安全区和接口组，或映射到在 FDM 托管设备配置文件中作为安全区类型对象并出现在下拉列表中的安全区和接口组，请执行以下操作：

a) 在**安全区**栏中，选择该接口的安全区。

b) 在**接口组**栏中，选择该接口的接口组。

步骤 3 您可以手动映射或自动创建安全区和接口组。

步骤 4 要手动映射安全区和接口组，请执行以下操作：

a) 点击**添加 SZ 和 IG (Add SZ & IG)**。

b) 在**添加 SZ 和 IG (Add SZ & IG)** 对话框中，点击**添加 (Add)** 以添加新的安全区或接口组。

c) 在**安全区**栏中输入安全区名称。允许的最大字符数为 48。同样，您可以添加接口组。

d) 点击**关闭 (Close)**。

要通过自动创建映射安全区和接口组，请执行以下操作：

a) 点击**自动创建 (Auto-Create)**。

b) 在**自动创建**对话框中，选中**接口组**和**区域映射**中的一个或两个。

c) 点击**自动创建 (Auto-Create)**。

Cisco Secure Firewall 迁移工具将为这些安全区提供与 FDM 托管设备接口相同的名称（例如 **outside** 或 **inside**），并在名称后显示“(A)”，以指示它是由 Cisco Secure Firewall 迁移工具创建的。将为接口组添加 `_ig` 后缀，例如 **outside_ig** 或 **inside_ig**。此外，安全区和接口组与 FDM 托管设备接口具有相同的模式。例如，如果 FDM 托管设备逻辑接口是 L3 模式，则为该接口创建的安全区和接口组也是 L3 模式。

步骤 5 在已将所有接口映射到相应的安全区和接口组后，点击**下一步 (Next)**。

优化、检查和验证要迁移的配置

对于FDM托管设备配置，将以不同的方式来验证配置，并将取决于所选的迁移流程。不同选项的配置验证如下：

- **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）**- 在单个流程中查看和验证设备和共享配置。
- **迁移 Firepower 设备管理器（仅限共享配置）**- 仅审核和验证共享配置。
- **迁移 Firepower 设备管理器（包括设备和共享配置）**- 在单独的流程中验证共享和设备配置

优化、检查和验证共享配置

在将迁移的FDM配置推送到管理中心之前，优化并仔细检查配置并验证它是否正确且与您需要的威胁防御设备配置方式匹配。闪烁的选项卡表示您必须执行下一步操作。

注释 如果您在**优化、检查和验证配置 (Optimize, Review and Validate Configuration)** 屏幕上关闭了 Cisco Secure Firewall迁移工具，它会保存进度并允许您在以后恢复迁移。如果在进入此屏幕之前关闭Cisco Secure Firewall迁移工具，则不会保存您的进度。如果解析后出现故障，Cisco Secure Firewall迁移工具继续从**接口映射 (Interface Mapping)** 屏幕重新启动。

此处，Cisco Secure Firewall 迁移工具会获取 管理中心 上已存在的入侵防御系统 (IPS) 策略和文件策略，并允许您将这些策略与要迁移的访问控制规则相关联。

文件策略是作为整体访问控制配置的一部分供系统用于执行网络高级恶意软件防护和文件控制的一组配置。这种关联保证系统在传递流量中与访问控制规则的条件匹配的文件之前，首先检查该文件。

同样，在允许流量继续到达其目标之前，可以使用 IPS 策略作为系统的最后一道防线。入侵策略监管系统如何检测流量是否存在安全违规，并且在内联部署中可以阻止或修改恶意流量。只要系统使用入侵策略来评估流量，它便会使用关联的变量集。变量集中的大多数变量表示入侵规则中常用于识别源和目标IP地址及端口的值。您还可以在入侵策略中使用变量表示规则禁止和动态规则状态中的 IP 地址。

要搜索选项卡中的特定配置项，请在列顶部的字段中输入项目名称。表中的行将筛选，仅显示与搜索术语匹配的项目。

如果您在**优化、检查和验证配置 (Optimize, Review and Validate Configuration)** 屏幕上关闭了 Cisco Secure Firewall迁移工具，它会保存进度并允许您在以后恢复迁移。如果在进入此屏幕之前关闭，则不会保存您的进度。如果解析后出现故障，Cisco Secure Firewall迁移工具继续从**接口映射 (Interface Mapping)** 屏幕重新启动。

Cisco Secure Firewall 迁移工具 ACL 优化概述

Cisco Secure Firewall 迁移工具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，而不会影响网络功能。

ACL 优化支持以下 ACL 类型：

- 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。例如，如果任意两个规则允许同一个网络上的FTP和IP流量，而没有为拒绝访问定义规则，则可以删除第一个规则。
- 影子 ACL - 第一个 ACL 完全镜像第二个 ACL 的配置。如果两个规则具有相似的流量，则第二个规则不会应用于任何流量，因为它稍后会出现在访问列表中。如果两个规则对流量指定了不同的操作，则您可能需要移动阴影规则或编辑两条规则之一，以便实施所需的策略。例如，对于给定的源或目标，基本规则可能会拒绝 IP 流量，而阴影规则可能会允许 FTP 流量。

在比较 ACL 优化规则时，Cisco Secure Firewall 迁移工具会使用以下参数：

注释 优化仅适用于 ACP 规则操作的 FDM 托管设备。

- 在优化过程中不会考虑已禁用的 ACL。
- 源 ACL 将扩展为相应的 ACE（内联值），然后对比以下参数：
  - 源和目标区域
  - 源和目标网络
  - 源和目标端口

对象优化

在迁移过程中会考虑以下对象以进行对象优化：

- 未引用的对象 - 可以选择在迁移开始时不迁移未被引用的对象。
- 重复对象 - 如果对象已存在于 管理中心 上，则不会创建重复对象，而是重复使用策略。

步骤 1 （可选）在 屏幕上，点击**优化 ACL (Optimize ACL)** 以运行优化代码，并执行以下操作：

a) 要下载已识别的 ACL 优化规则，请点击**下载 (Download)**。

b) 选择规则，然后选择**操作 (Actions)** > **作为已禁用迁移 (Migrate as disabled)** 或**不迁移 (Do not migrate)** 并应用其中一项操作。

c) 点击**保存 (Save)**。
迁移操作从**不迁移 (Do not migrate)** 更改为**已禁用 (Disabled)**，反之亦然。

您可以使用以下选项来批量选择规则

- 迁移 - 以默认状态迁移。
- 不迁移 - 忽略 ACL 的迁移。
- 作为已禁用迁移 (Migrate as disabled) - 迁移**状态** ***(State)*** 字段被设为**禁用** ***(Disable)*** 的 ACL。
- 迁移为已启用 (Migrate as enabled) - 迁移**状态** ***(State)*** 字段被设为**启用** ***(Enable)*** 的 ACL。

步骤 2 在优化，**检查和验证配置 (Review and Validate Configuration)** 屏幕上，点击**访问控制规则 (Access Control Rules)**，并执行以下操作：

a) 对于此表中的每个条目，查看映射并验证它们是否正确。

迁移的访问策略规则使用 ACL 名称作为前缀，并在后面附加 ACL 规则编号，以便更轻松地映射回到 FDM 托管设备配置文件。例如，如果 FDM 托管设备 ACL 被命名为“inside_access”，则 ACL 中的第一个规则（或 ACE）行将命名为“inside_access_#1”。如果因为 TCP 或 UDP 组合、扩展的服务对象或一些其他原因而必须扩展规则，则 Cisco Secure Firewall 迁移工具会在名称中添加编号的后缀。例如，如果 allow 规则扩展为两个迁移规则，它们命名为“inside_access _#1-1”和“inside_access_#1-2”。

对于包括不受支持对象的任何规则，Cisco Secure Firewall 迁移工具将“_UNSUPPORTED”后缀附加到名称中。

b) 如果您不想迁移一个或多个访问控制列表策略，请选中相应行的框，选择**操作 (Actions)** > **不迁移 (Do not migrate)**，然后点击**保存 (Save)**。

您选择为不进行迁移的所有规则都会在表中变灰。

c) 如果要将 管理中心 文件策略应用于一个或多个访问控制策略，请选中相应行的复选框，然后选择**操作** > **文件策略**。

在**文件策略 (File Policy)** 对话框中，选择适当的文件策略并将其应用于所选的访问控制策略，然后点击**保存 (Save)**。

d) 如果要将 管理中心 IPS 策略应用于一个或多个访问控制策略，请选中相应行的复选框，然后选择**操作** > **IPS 策略**。

在 **IPS 策略 (IPS Policy)** 对话框中，选择适当的 IPS 策略和对应的变量集并将其应用于所选的访问控制策略，然后点击**保存 (Save)**。

e) 如果要更改已启用日志记录的访问控制规则的日志记录选项，请选中相应行的复选框，然后选择**操作**>**日志**。

在**日志**对话框中，您可以在连接开始和/或结尾时启用日志记录事件。如果启用日志记录，则必须选择将连接事件发送到**事件查看器**和/或**系统日志**。当您选择将连接事件发送到系统日志服务器时，可以从**系统日志**下拉菜单中选择已在 管理中心 上配置的系统日志策略。

f) 如果要更改访问控制表中已迁移的访问控制规则的操作，请选中相应行的复选框，然后选择**操作**>**规则操作**。

在**操作**下拉列表中的**规则操作**对话框中，可以选择 **ACP** 或**预过滤器**选项卡：

- ACP - 每个访问控制规则都具有用于确定系统如何处理和记录匹配流量的操作。您可以对访问控制规则执行允许、信任、监控、阻止或阻止并重置操作。
- 预过滤器 - 规则操作确定系统如何处理和记录匹配的流量。您可以执行快速路径和阻止。

提示 对于“允许”选项除外的所有规则操作，附加到访问控制规则的 IPS 和文件策略将自动删除。

策略容量和限制警告 - Cisco Secure Firewall 迁移工具会将已迁移规则的总 ACE 计数与目标平台上支持的 ACE 限制进行比较。

根据比较结果，如果已迁移的 ACE 的总数超过阈值，或者其接近目标设备支持的限制阈值，则 Cisco Secure Firewall 迁移工具还会显示可见的指示器和警告消息。

如果规则数超过“ACE 计数”列，您可以优化迁移或决定不迁移。您也可以完成迁移，并在部署前在 管理中心 上推送后使用此信息优化规则。

注释 尽管有警告，Cisco Secure Firewall 迁移工具不会阻止任何迁移。

现在，您可以按升序、降序、等于、大于和小于过滤顺序来过滤 ACE 计数。

要清除现有过滤条件并加载新搜索，请点击**清除过滤器 (Clear Filter)**。

注释 基于 ACE 对 ACL 进行排序的顺序仅供查看。ACL 将基于发生的时间顺序推送。

g) **入侵策略 (Intrusion Policy)** 中将显示所有入侵策略和相应的基本策略、存在的自定义/覆盖的规则、入侵模式和 ACP 中的引用。它还会显示 Snort 3 的 Snort 引擎和 NAP 策略。

由于管理中心上的 API 限制，具有覆盖规则的 Snort 2 策略将被忽略。

具有默认设置的入侵策略会在管理中心重复使用。

使用策略名称 _ <FDM Hostname> 为具有 Snort 3 的覆盖规则/自定义规则的入侵策略或 Snort3/Snort2 的入侵模式检测创建新策略

步骤 3 点击以下选项卡并查看配置项：

- **NAT 规则**
- **对象（访问列表对象、网络对象、端口对象、VPN 对象和动态路由对象）**
- **接口**
- **路由**
- **站点间 VPN 隧道**
- **远程接入 VPN**

访问列表对象会显示 BGP、EIGRP 和 RA VPN 中使用的标准和扩展 ACL。

如果您不想迁移一个或多个 NAT 规则或路由接口，请选中相应行的复选框，选择**操作 (Actions)** > **不迁移 (Do not migrate)**，然后点击**保存 (Save)**。

您选择为不进行迁移的所有规则都会在表中变灰。

步骤 4 （可选）在查看配置时，您可以在**网络对象**选项卡或**端口对象**选项卡或 **VPN 对象**中中通过选择**操作** > **重命名**来重命名一个或多个网络或端口对象。

引用重命名对象的访问规则和 NAT 策略也会更新，以使用新的对象名称。

步骤 5 在**远程访问 VPN (Remote Access VPN)** 部分，与远程接入 VPN 对应的所有对象都从 FDM 托管设备迁移到管理中心并显示：

- **Anyconnect 文件** - 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 配置文件应从源 FDM 托管设备检索且必须可用于迁移。

  作为迁移前活动的一部分，将所有 AnyConnect 软件包DOU 上传到管理中心。您可以将 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。

  选择从管理中心检索的现有 Anyconnect、Hostscan 或外部浏览器软件包。您必须至少选择一个 AnyConnect 软件包。您必须选择 Hostscan、dap.xml、data.xml 或外部浏览器（如果在源配置中可用）。AnyConnect 配置文件为可选。

  Dap.xml 必须是从 FDM 托管设备检索到的正确文件。对配置文件中可用的 dap.xml 执行验证。您必须上传并选择所有必需的文件来进行验证。更新失败将被标记为不完整，并且 Cisco Secure Firewall 迁移工具不会继续进行验证。

- **AAA** - 显示 Radius、LDAP、AD、LDAP、SAML 和本地领域类型的身份验证服务器。更新所有 AAA 服务器的密钥。从 Cisco Secure Firewall 迁移工具 3.0 开始，系统会自动检索 Live Connect FDM 托管设备的预共享密钥。您还可以使用 **more system: running-config** 文件来上传包含隐藏密钥的源配置。要以明文格式检索 AAA 身份验证密钥，请执行以下步骤：

  注释 这些步骤应在 Cisco Secure Firewall 迁移工具之外执行。

1. 通过 SSH 控制台连接到 FDM 托管设备。
2. 输入 *more system:running-config* 命令。
3. 转到 **aaa-server and local user** 部分，以明文格式查找所有 AAA 配置和相应的密钥值。

```
ciscoFDM#more system:running-config
!
aaa-server Test-RADIUS (inside) host 2.2.2.2
key <key in clear text> <-----The radius key is now displayed in clear text format. aaa-server
Test-LDAP (inside) host 3.3.3.3
ldap-login-password <Password in clear text> <-----TheLDAP/AD/LDAPS password is now displayed in
 clear text format.
username Test_User password <Password in clear text> <-----The Local user password is shown in
clear text.
```

注释 如果本地用户的密码已加密，您可以在内部检查密码或在Cisco Secure Firewall 迁移工具上配置新密码。

- LDAPS 需要管理中心的域。您必须更新加密类型 LDAPS 的域。
- 在管理中心上，AD 服务器需要唯一的 AD 主域。如果识别出唯一的域，则会将其显示在 Cisco Secure Firewall 迁移工具中。如果发现冲突，必须输入唯一的 AD 主域才能成功推送对象。

  对于加密设置为 LDAPS 的 AAA 服务器，FDM 托管设备支持 IP 和主机名或域，但管理中心仅支持主机名或域。如果FDM托管设备配置包含主机名或域，则会检索并显示这些信息。如果FDM托管设备配置包含LDAPS 的 IP 地址，请在**远程访问 VPN (Remote Access VPN)** 下的 **AAA** 部分输入域。您必须输入可解析为 AAA 服务器 IP 地址的域。

  对于 AD 类型的 AAA 服务器（在 FDM 托管设备配置中，服务器类型为 Microsoft），**AD 主域 (AD Primary Domain)** 是要在管理中心上配置的必填字段。此字段不在 FDM 托管设备上单独配置，而是从 FDM 托管设备上的 LDAP-base-dn 配置中提取。

  如果 `ldap-base-dn` 为：`ou=Test-Ou,dc=gcevpn,dc=com`

  AD 主域是以 dc 开头的字段，其中 dc=gcevpn 和 dc=com 构成主域。AD 主域是 gcevpn.com。

  LDAP-base-dn 示例文件：

  ```
  cn=FDM,OU=ServiceAccounts,OU=abc,dc=abc,dc=com:
  ```

  此处，dc=abc 和 dc=com 将合并为 abc.com 以构成 AD 主域。

  ```
  cn=admin, cn=users, dc=fwsecurity, dc=cisco, dc=com:
  ```

  AD 主域为 fwsecurity.cisco.com。

  AD 主域会自动检索并显示在 Cisco Secure Firewall 迁移工具上。

  注释 每个领域对象的 AD 主域值都必须是唯一的。如果检测到冲突，或者防火墙迁移工具无法在 FDM 托管设备配置中找到该值，则系统会要求您输入特定服务器的 AD 主域。输入 AD 主域以验证配置。

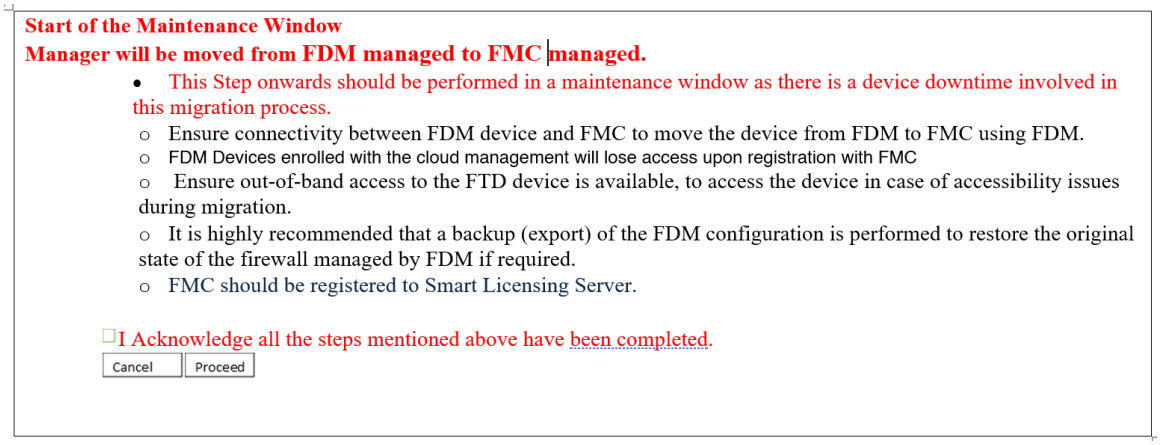
- **地址池 (Address Pool)** - 所有 IPv4 和 IPv6 池都会显示在这里。

- **组策略 (Group-Policy)** - 此部分显示包含客户端配置文件的组策略、管理配置文件、客户端模块以及不包含配置文件的组策略。如果配置文件是在 AnyConnect 文件部分中添加的，则会显示为预选。您可以选择或删除用户配置文件、管理配置文件和客户端模块配置文件。
- **连接配置文件 (Connection Profile)** - 此处显示所有连接配置文件/隧道组。
- **信任点 (Trustpoint)** - 信任点或 PKI 对象从 FDM 托管设备迁移到管理中心是迁移前活动的一部分，并且也是成功迁移 RA VPN 所必不可少的。**映射远程访问接口 (Remote Access Interface)** 部分中的全局 SSL、IKEv2 和接口的信任点，以继续执行后续迁移步骤。如果启用了 LDAPS 协议，则必须使用全局 SSL 和 IKEv2 信任点。如果存在 SAML 对象，则可以在 SAML 部分中映射 SAML IDP 和 SP 的信任点。SP 证书为可选。也可以覆盖特定隧道组的信任点。如果覆盖的 SAML 信任点配置在源 FDM 托管设备中可用，则可以在**覆盖 SAML (Override SAML)** 选项中选择该配置。

  有关从 FDM 托管设备导出 PKI 证书的信息，请参阅导出 FDM 托管设备配置文件。
- **证书映射 (Certificate Maps)** - 此处显示证书映射。

启动维护和移动管理器

一旦推送共享配置，您需要接受弹出窗口才能转到维护窗口。



在**移动管理器 (Move Manager)** 页面中，应提供以下详细信息：

- 在 **FTD 位于 NAT 设备后**、**FMC 位于 NAT 设备后**、**无设备位于 NAT 后**（**默认设置**）之间进行选择
- **管理中心/CDO 主机名或 IP 地址**：将从目标管理器获取所有详细信息。如果需要，您可以修改 IP。

注释 如果 **FMC 位于 NAT 设备后**，则这些字段将被忽略。

- **管理中心/CDO 注册密钥**：需要提供在移动管理器时使用的唯一注册密钥。

- **NAT ID**：（可选。）如果威胁防御或管理中心位于 NAT 设备后，则需要选择此选项。
- **威胁防御 (FTD) 主机名**：从 FDM 托管的设备配置中获取威胁防御 IP/主机名。如果需要，用户可以修改 IP。如果 **FTD 位于 NAT 设备后**，则该字段将被忽略。
- **DNS 服务器组**：用于设备管理器和管理中心之间的连接的 DNS 服务器组。
- **管理中心/CDO 访问接口（数据/管理）**：在数据/管理接口之间进行选择以移动管理器。只有当通过数据接口配置了适当的路由时才支持数据接口。

在选择**移动管理器 (Move Manager)** 后，Cisco Secure Firewall 迁移工具会触发将管理器从设备管理器移动到管理中心。在移动管理器后，将无法从设备管理器访问设备。

优化、检查和验证要迁移的设备配置

步骤 1 选择以下选项卡并查看配置项

- **接口**
- **路由**
- **站点间 VPN 隧道**

在 **Dynamic-Route-Objects** 部分中，将显示所有受支持的迁移对象：

- Policy-List
- Prefix-List
- 路由映射
- 社区列表
- AS 路径
- 访问列表

步骤 2 在**路由 (Routes)** 部分中，显示以下路由：

- 静态 (Static) - 显示所有 IPv4 和 IPv6 静态路由。
- BGP - 显示所有 BGP 路由。
- EIGRP - 显示所有 EIGRP 路由。对于 EIGRP，如果已上传 more system:running 配置且密钥未加密，则会获取身份验证密钥。如果密钥在源配置中已加密，则可以在 EIGRP 的接口部分下手动提供密钥。您可以选择身份验证类型（已加密、未加密、身份验证或无），然后相应地提供密钥

步骤 3 完成检查后，点击**验证 (Validate)**。

在验证期间，Cisco Secure Firewall 迁移工具会连接到管理中心，检查现有对象，然后将这些对象与要迁移的对象列表进行比较。如果管理中心中已存在对象，Cisco Secure Firewall 迁移工具会执行以下操作：

- 如果对象具有相同的名称和配置，Cisco Secure Firewall 迁移工具会重新使用现有对象，而不会在管理中心中创建新对象。
- 如果对象具有相同名称但具有不同的配置，Cisco Secure Firewall 迁移工具会报告对象冲突。

您可以在控制台中查看验证进度。

步骤 4 验证完成后，如果**验证状态**对话框显示一个或多个对象冲突，请执行以下操作：

a) 点击**解决冲突 (Resolve Conflicts)**。

根据报告的对象冲突位置，Cisco Secure Firewall 迁移工具会在**网络对象 (Network Objects)** 和/或**端口对象 (Port Objects)** 选项卡中显示一个警告图标。

b) 点击选项卡，检查对象。

c) 检查存在冲突的每个对象的条目，然后选择**操作 (Actions)** > **解决冲突 (Resolve Conflicts)**。

d) 在**解决冲突**窗口中，完成建议的操作。

例如，系统可能会提示您为对象名称添加后缀，以避免与现有 管理中心对象冲突。您可以接受默认后缀或将其替换为您自己的后缀。

e) 点击**解决 (Resolve)**。

f) 在选项卡上解决所有对象冲突之后，点击**保存 (Save)**。

g) 点击**验证 (Validate)**，重新验证配置，并确认您已解决所有对象冲突。

步骤 5 在验证完成且**验证状态 (Validation Status)** 对话框显示消息**已成功验证 (Successfully Validated)** 时，继续执行将迁移的配置推送到管理中心。

将迁移的配置推送到 管理中心

如果您还未成功验证配置和解决所有对象冲突，则不能将迁移的 FDM 托管设备配置推送到 管理中心。

迁移过程中的此步骤会将迁移的配置发送至管理中心。此步骤不会将配置部署到威胁防御设备。但在此步骤中会擦除 威胁防御上的任何现有配置。

注释 当 Cisco Secure Firewall 迁移工具将迁移的配置发送到 管理中心时，不要更改任何配置或部署到任何设备。

步骤 1 在**验证状态**对话框中，查看验证摘要。

步骤 2 点击**推送配置 (Push Configuration)**，将迁移的 FDM 托管设备配置发送至 管理中心。

通过 Cisco Secure Firewall 迁移工具中的新优化功能，可以使用搜索过滤器快速获取迁移结果。

Cisco Secure Firewall 迁移工具还支持 CSV 下载优化并按页面视图或对所有规则应用操作。

Cisco Secure Firewall 迁移工具会显示迁移进度的摘要信息。您可以在控制台中查看详细的逐行进度信息，了解正在将哪些组件推送至 管理中心。

步骤 3 在迁移完成后，点击**下载报告 (Download Report)**，下载并保存迁移后报告。

系统也会在 `Resources` 文件夹中保存**迁移后报告**的一个副本（与 Cisco Secure Firewall 迁移工具处于相同的位置）。

步骤 4 如果迁移失败，请仔细查看迁移后报告、日志文件和未解析文件，了解是什么原因导致失败。

您也可以联系支持团队进行故障排除。

迁移失败支持

如果迁移不成功，请联系支持部门。

1. 在**完成迁移 (Complete Migration)** 屏幕上，点击**支持 (Support)** 按钮。

   系统将显示“帮助”支持页面。

2. 选中**支持捆绑包**复选框，然后选择要下载的配置文件。

   注释 默认情况下，系统已选择要下载的日志和 dB 文件。

3. 点击**下载 (Download)**。

   支持捆绑包文件以 .zip 格式下载到您的本地路径。解压缩 Zip 文件夹以查看日志文件、DB 和配置文件。

4. 点击**给我们发送邮件 (Email us)**，通过电子邮件将故障详细信息发送给技术团队。

   您还可以将下载的支持文件附加到电子邮件中。

5. 点击**访问 TAC 页面 (Visit TAC page)**，在思科支持页面上创建 TAC 支持请求。

   注释 您可以在迁移过程中随时从支持页面提交 TAC 支持请求。

查看迁移后报告并完成迁移

迁移后报告提供了不同类别下的 ACL 计数、ACL 优化以及对配置文件进行优化的整体视图等详细信息。有关详细信息，请参阅优化、检查和验证要迁移的配置，第 20 页

查看并验证对象：

- **类别**
  - ACL 规则总数（源配置）
  - 考虑优化的 ACL 规则总数。例如，冗余、阴影等。
- 优化的 ACL 计数给出了优化前后计算得出的 ACL 规则总数。

如果您在迁移期间错过下载迁移后报告，请使用以下链接进行下载：

迁移后报告下载终端 — http://localhost:8888/api/downloads/post_migration_summary_html_format

注释 您只能在 Cisco Secure Firewall 迁移工具正在运行时下载报告。

步骤 1 导航至下载了**迁移后报告**的位置。

步骤 2 打开迁移后报告并仔细检查其内容，了解您的 FDM 托管设备配置是如何迁移的：

- **迁移摘要** - 已成功从 FDM 托管设备迁移到 威胁防御 的配置的摘要信息，其中包括有关 FDM 托管设备接口、管理中心 主机名和域、目标 威胁防御 设备（如果适用）和已成功迁移的配置元素的信息。
- **FDM 迁移路径** - 显示在三个迁移流之间选择的选项：
  - **迁移 Firepower 设备管理器（仅限共享配置）**
  - **迁移 Firepower 设备管理器（包括设备和共享配置）**
  - **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）**
- **选择性策略迁移** - 设备配置功能、共享配置功能和优化三个类别中可选择迁移的特定 FDM 托管设备功能的详细信息。
- **FDM 托管设备 接口至 FTD 接口映射** - 已成功迁移的接口的详细信息，以及如何将 FDM 托管设备 配置上的接口映射到 威胁防御 设备上的接口。确认这些映射符合您的预期。

  注释 本部分不适用于没有目标 威胁防御 设备或者**未**选择迁移**接口**的迁移。
- **源接口名称至 FTD 安全区和接口组** - 已成功迁移的 FDM 托管设备 逻辑接口和名称的详细信息，以及如何将它们映射到 威胁防御 中的安全区和接口组。确认这些映射符合您的预期。

  注释 如果**未**选择迁移**访问控制列表**和 **NAT**，则此部分不适用。
- **对象冲突处理** - 已被确定为与 管理中心 中现有对象冲突的 FDM 托管设备对象的详细信息。如果对象具有相同的名称和配置，Cisco Secure Firewall 迁移工具重新使用 管理中心对象。如果对象具有相同名称但具有不同的配置，则重命名这些对象。仔细检查这些对象，并确认已正确解决冲突。
- **您选择不迁移的访问控制规则、NAT 和路由** - 您选择不让 Cisco Secure Firewall 迁移工具迁移的规则的详细信息。查看由 Cisco Secure Firewall 迁移工具禁用且未迁移的这些规则。查看这些行，并验证您选择的所有规则均列在此部分中。如果需要，可以手动配置这些规则。
- **部分迁移的配置** - 仅部分迁移的 FDM 托管设备规则的详细信息，包括带有高级选项的规则，其中，在没有高级选项的情况下也可以迁移规则。查看这些行，验证在 管理中心中是否支持高级选项。如果支持，手动配置这些选项。
- **不支持的配置** - 因 Cisco Secure Firewall 迁移工具不支持迁移这些功能而未被迁移的 FDM 托管设备配置元素的详细信息。查看这些行，验证 威胁防御中是否支持每项功能。如果支持，请在 管理中心中手动配置这些功能。
- **展开访问控制策略规则** - 在迁移期间已从一个 FDM 托管设备 Point 规则扩展到多个 威胁防御 规则的 FDM 托管设备访问控制策略规则的详细信息。

- 对访问控制规则采取的操作
  - **您选择不迁移的访问规则** - 您选择不让 Cisco Secure Firewall 迁移工具迁移的 FDM 托管设备访问控制规则的详细信息。查看这些行，并验证您选择的所有规则均列在此部分中。如果需要，可以手动配置这些规则。
  - **规则操作有更改的访问规则** - 使用 Cisco Secure Firewall 迁移工具更改了“规则操作”的所有访问控制策略规则的详细信息。规则操作值包括允许、信任、监控、阻止、阻止并重置。查看这些行，并验证您选择的所有规则均列在此部分中。如果需要，可以手动配置这些规则。
  - **应用了 IPS 策略和变量集的访问控制规则** - 应用了 IPS 策略的所有 FDM 托管设备访问控制策略规则的详细信息。仔细查看这些规则并确定 威胁防御 是否支持此功能。
  - **应用了文件策略的访问控制规则** - 应用了文件策略的所有 FDM 托管设备访问控制策略规则的详细信息。仔细查看这些规则并确定 威胁防御 是否支持此功能。
  - **规则“日志”设置有更改的访问控制规则** - 使用 Cisco Secure Firewall 迁移工具更改了“日志设置”的 FDM 托管设备访问控制规则的详细信息。日志设置值包括 False、事件查看器、系统日志。查看这些行，并验证您选择的所有规则均列在此部分中。如果需要，可以手动配置这些规则。

注释 未迁移的不受支持的规则可能导致出现问题，使得不必要的流量通过您的防火墙。建议您在 管理中心 中配置一个规则来确保 威胁防御阻止此类流量。

注释 如果它要求您在**检查和验证**页面中将 IPS 或文件策略应用于 ACL，则强烈建议您在迁移之前在管理中心上创建策略。使用相同的策略，因为 Cisco Secure Firewall 迁移工具从连接的管理中心获取策略。创建新策略并将其分配给多个策略可能会降低性能，也可能导致推送失败。

有关 管理中心和 威胁防御中的受支持功能的更多信息，请参阅管理中心配置指南，版本 6.2.3。

步骤 3 打开**迁移前报告**，并记下您必须在 威胁防御 设备上手动迁移的任何 FDM 托管设备配置项目。

步骤 4 在 管理中心中，执行以下操作：

a) 查看 威胁防御设备的迁移配置，确认所有预期规则和其他配置项目（包括以下内容）均已迁移：

- 访问控制列表 (ACL)
- 网络地址转换规则
- 端口和网络对象
- 路由
- 接口
- IP SLA 对象
- 对象组搜索
- 基于时间的对象
- 站点间 VPN 隧道
- 动态路由对象

b) 配置所有未迁移的部分受支持、不受支持、已忽略和已禁用的配置项目和规则。

有关如何配置这些项目和规则的信息，请参阅管理中心配置指南 。以下是需要手动配置的配置项目的示例：

- 平台设置，包括 SSH 和 HTTPS 访问，如威胁防御的平台设置中所述。
- 系统日志设置，如配置系统日志中所述
- 动态路由，如威胁防御路由概述中所述
- 服务策略，如 FlexConfig 策略中所述
- VPN 配置，如威胁防御 VPN 中所述
- 连接日志设置，如连接日志记录中所述

如果您在迁移前更改了 AD 领域的加密，请按照以下步骤将加密类型恢复为 LDAPS 或 STARTTLS：

1. 导航到**集成 (Integration)** 部分，然后点击**其他集成 (Other Integrations)**。
2. 选择**领域 (Realms)**，然后点击特定领域旁边的 **编辑**（ ） 以更改加密类型。
3. 点击**目录 (Directory)** 并将加密类型更改为 **LDAPS** 或 **STARTTLS**。
4. 保存并部署更改。

步骤 5 完成检查之后，将已迁移的配置从 管理中心 部署到 威胁防御 设备。

验证**迁移后报告**中是否正确反映了不支持和部分支持的规则的数据。

Cisco Secure Firewall 迁移工具将策略分配到 威胁防御 设备。验证运行配置中是否反映了更改。为帮助您识别已迁移的策略，这些策略的描述信息中包括 FDM 托管设备配置的主机名。

卸载 Cisco Secure Firewall 迁移工具

所有组件均存储在与 Cisco Secure Firewall 迁移工具相同的文件夹中。

步骤 1 导航至在其中放置 Cisco Secure Firewall 迁移工具的文件夹。

步骤 2 如果要保存日志，请剪切或复制 `log` 文件夹并粘贴到另一个位置。

步骤 3 如果要保存迁移前报告和迁移后报告，请剪切或复制 `resources` 文件夹并粘贴到另一个位置。

步骤 4 删除在其中放置 Cisco Secure Firewall 迁移工具的文件夹。

提示 日志文件与控制台窗口相关联。如果 Cisco Secure Firewall 迁移工具的控制台窗口处于打开状态，就无法删除日志文件和文件夹。

迁移示例： FDM 托管设备到 Threat Defense 2100

注释 创建迁移完成后可在目标设备上运行的测试计划。

- 维护前窗口任务
- 维护窗口任务

维护前窗口任务

开始之前

确保已安装并部署了 管理中心。有关详细信息，请参阅相应的管理中心硬件安装指南和相应的管理中心入门指南。

步骤 1 获取 FDM 托管的配置或连接到 FDM 托管设备以获取配置。

步骤 2 查看 FDM 托管设备配置文件。

步骤 3 在网络中部署 Firepower 2100 系列 设备，连接接口并打开设备电源。

有关详细信息，请参阅《适用于使用管理中心的 2100 系列的思科威胁防御快速入门指南》。

步骤 4 注册 Firepower 2100 系列 设备以接受 管理中心 的管理。

有关详细信息，请参阅将设备添加到管理中心。

步骤 5 （可选）如果源 FDM 托管设备配置具有端口通道，请在目标 Firepower 2100 系列 设备上创建端口通道 (EtherChannel)。

有关详细信息，请参阅配置 EtherChannel 和冗余接口。

步骤 6 从 https://software.cisco.com/download/home/286306503/type 下载并运行最新版本的 Cisco Secure Firewall 迁移工具。

有关详细信息，请参阅从 Cisco.com 下载 Cisco Secure Firewall 迁移工具 ， 第 3 页。

步骤 7 启动 Cisco Secure Firewall 迁移工具并指定目标参数时，请确保选择注册到 管理中心 的 Firepower 2100 系列 设备。

有关详细信息，请参阅为 Cisco Secure Firewall 迁移工具指定目标参数 ， 第 14 页。

步骤 8 将 FDM 托管设备接口与 威胁防御 接口映射。

注释 Cisco Secure Firewall 迁移工具允许您将 FDM 托管设备接口类型映射到 威胁防御 接口类型。

例如，您可以将 FDM 托管设备中的端口通道映射到 威胁防御 中的物理接口。

有关详细信息，请参阅将 FDM 托管设备配置与 Secure Firewall 设备管理器 威胁防御 接口映射。

步骤 9 将逻辑接口映射到安全区时，点击**自动创建 (Auto-Create)** 以允许 Cisco Secure Firewall 迁移工具创建新的安全区。要使用现有安全区，请手动将 FDM 托管设备逻辑接口映射到安全区。

有关详细信息，请参阅将 FDM 托管设备接口映射到安全区。

步骤 10 按照本指南的说明依次检查和验证要迁移的配置，然后将配置推送到 管理中心。

步骤 11 查看迁移后报告，手动设置其他配置并部署到 威胁防御，完成迁移。

有关详细信息，请参阅优化、检查和验证要迁移的配置 ， 第 20 页。

步骤 12 使用您在计划迁移时创建的测试计划测试 Firepower 2100 系列 设备。

维护窗口任务

开始之前

确保您已完成所有必须在维护窗口之前执行的任务。请参阅维护前窗口任务 ， 第 33 页。

步骤 1 通过 SSH 控制台连接到 FDM 托管设备并切换到接口配置模式。

步骤 2 使用 **shutdown** 命令关闭 FDM 托管设备接口。

步骤 3 （可选）访问 管理中心 并配置 Firepower 2100 系列 设备的动态路由。

有关详细信息，请参阅动态路由。

步骤 4 清除周围交换基础设施上的地址解析协议 (ARP) 缓存。

步骤 5 执行从周围交换基础设施到 Firepower 2100 系列 设备接口 IP 地址的基本 ping 测试，确保它们可访问。

步骤 6 执行从需要第 3 层路由的设备到 Firepower 2100 系列 设备接口 IP 地址的基本 ping 测试。

步骤 7 如果要为 Firepower 2100 系列 设备分配新的 IP 地址，而不是重新使用分配给 FDM 托管设备的 IP 地址，请执行以下步骤：

1. 更新指向该 IP 地址的任何静态路由，以使其现在指向 Firepower 2100 系列 设备 IP 地址。
2. 如果使用路由协议，请确保邻居将 Firepower 2100 系列 设备 IP 地址视为预期的下一跳目标。

步骤 8 运行全面的测试计划并监控管理 Firepower 2100 设备的 管理中心。

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。