安全接入

管理网络设备组

通过以下窗口，您可以配置和管理网络设备组。

网络设备组设置

表 *1:*“网络设备组”*(Network Device Group)*窗口中的字段

字段名称	使用指南
Name	为根网络设备组输入一个名称。对于添加到该根网络设备组的所有后续子网络设备组，请输入这个新建网络设备组的名称。 网络设备组的全称最多可以包含 100 个字符。例如，如果在父组**全球 (Global) > 亚洲 (Asia)** 下创建一个名为**印度 (India)** 的子组，则您创建的网络设备组的全称将为**全球 (Global) > 亚洲 (Asia) > 印度 (India)**。全称不能超过 100 个字符。如果网络设备组的全称超过 100 个字符，则网络设备组创建失败。
Description	为根网络设备组或子网络设备组输入一段说明。
Parent Group	要将所创建的组添加到现有父组，请从下拉列表中选择一个父组。要将此新组添加为根组，请从下拉列表中选择**添加为根组 (Add as root group)**。

字段名称	使用指南
Type	输入根网络设备组 (NDG) 的类型。 所有添加到根网络设备组的子网络设备组都将继承组类型。 如果此网络设备组是根网络设备组，则其类型可作为设备字典中的属性使用。您可以基于此属性定义条件。网络设备组的名称是此属性可以采用的值之一。

相关主题

网络设备组，第 3 页
思科 ISE 在策略评估中使用的网络设备属性，第 4 页
在思科 ISE 中添加网络设备

网络设备组导入设置

表 *2:* 网络设备组导入窗口中的字段

字段名称	使用指南
生成模板 (Generate a Template)	点击此链接下载 CSV 模板文件。 使用相同格式的网络设备组信息更新模板。将模板保存在本地，以便将网络设备组导入任何思科 ISE 部署中。
文件	点击 **浏览**，导航至您要上传的 CSV 文件的位置。该文件可能是新文件，也可能是从另一个思科 ISE 部署中导出的文件。 可以将包含新的和更新后的网络设备组信息的网络设备组从一个思科 ISE 部署导入另一部署。
用新数据覆盖现有数据 (Overwrite Existing Data with New Data)	如果您希望思科 ISE 用您的导入文件中的设备组替换现有网络设备组，请选中此复选框。 如果未选中此复选框，则只会将导入文件中的新网络设备组添加到网络设备组存储库。系统会忽略重复条目。
Stop Import on First Error	选中此复选框，可在导入期间遇到错误的第一个实例时停止导入。 如果未选中此复选框并且遇到错误，思科 ISE 将报告错误，并继续导入剩余设备组。

相关主题

网络设备组，第 3 页
思科 ISE 在策略评估中使用的网络设备属性，第 4 页
将网络设备组导入到思科 ISE，第 4 页

网络设备组

思科 ISE 支持创建分层网路设备组。使用网络设备组根据不同的条件（例如地理位置、设备类型或其在网络中的相对位置 [例如，“接入层”或“数据中心”等]）对网络设备进行逻辑分组。

要查看“网络设备组”(Network Device Group) 窗口，选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备组 (Network Device Groups)**。

例如，要按地理位置组织网络设备，可以按大洲、区域和国家/地区将设备进行分组：

- **非洲** > **南部** > **纳米比亚**
- **非洲** > **南部** > **南非**
- **非洲** > **南部** > **博茨瓦纳**

根据设备类型对网络设备进行分组：

- **非洲** > **南部** > **博茨瓦纳** > **防火墙**
- **非洲** > **南部** > **博茨瓦纳** > **路由器**
- **非洲** > **南部** > **博茨瓦纳** > **交换机**

将网络设备分配给一个或多个分层网络设备组。当思科 ISE 通过已配置的网络设备组的有序列表确定要分配给特定设备的适当组时，它可能会发现同一设备配置文件适用于多个设备组。在这种情况下，思科 ISE 将应用匹配的第一个设备组。

对可创建的网络设备组的最大数量没有限制。对层级的最大数量没有限制。

要在 **网络设备组** 窗口中添加网络设备组，请点击 **添加**。在**父级组 (Parent Group)** 下拉列表中，选择网络设备组必须添加到的父级组，或选择**添加为根组 (Add As Root Group)** 选项将新网络设备组添加为父级组。

注释 如果已向设备组分配了任何设备，则无法删除该设备组。在删除设备组之前，您必须将所有现有设备移动到另一个设备组。

根网络设备组

思科 ISE 包含两个预定义的根网路设备组：**所有设备类型 (All Device Types)** 和**所有位置 (All Locations)**。无法编辑、复制或删除这些预定义的网路设备组，但可以在这些组中添加新设备组。

您可以创建根网络设备组（网络设备组），然后在**网络设备组**窗口中的根组下创建子网络设备组，如前所述。创建新的根网络设备组时，必须提供网络设备组的名称和类型。当在根网络设备组中创建子项时，不需要此信息。

思科 ISE 在策略评估中使用的网络设备属性

创建新网络设备组时，新网络设备属性将添加至**系统字典 (System Dictionaries)** 中的**设备 (Device)** 字典（**策略 (Policy)** > **策略元素 (Policy Elements)** > **词典 (Dictionaries)**）。添加的设备属性随后将在策略定义中使用。

思科 ISE 允许您使用**设备 (Device)** 字典属性（例如设备类型、位置、型号名称或网络设备上运行的软件版本）配置身份验证和授权策略。

将网络设备组导入到思科 ISE

您可以使用逗号分隔值 (CSV) 文件将网络设备组导入到思科 ISE 节点。请注意，您不能同时从两个不同的导入文件导入网络设备组。

从思科 ISE 管理员门户下载 CSV 模板。在模板中输入网络设备组详细信息，并将模板另存为 CSV 文件，然后将编辑的文件导入到思科 ISE。

导入设备组时，您可以创建新记录或更新现有记录。导入设备组时，您还可以定义在思科 ISE 遇到第一个错误时希望思科 ISE 使用新组覆盖现有设备组还是停止导入过程。

步骤 1 选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备组 (Network Device Groups)**。

步骤 2 单击**导入**。

步骤 3 在对话框中，点击**浏览 (Browse)**，从正在运行客户端浏览器的系统中选择 CSV 文件。

要下载用于添加网络设备组的 CSV 模板文件，请点击**生成模板 (Generate a Template)**。

步骤 4 要覆盖现有网络设备组，请选中 **用新数据覆盖现有数据** 复选框。

步骤 5 选中 **Stop Import on First Error** 复选框。

步骤 6 点击**导入 (Import)**。

从思科 ISE 导出网络设备组

您可以用 CSV 文件的形式导出在思科 ISE 中配置的网络设备组。然后，您可以将这些网络设备组导入另一个思科 ISE 节点。

步骤 1 选择 **管理 (Administration)** > **网络资源 (Network Resources)** > **网络设备组 (Network Device Groups)** > **所有组 (All Groups)**。

步骤 2 要导出网络设备组，可以执行以下操作之一：

- 选中您要导出的设备组旁边的复选框，然后选择**导出 (Export)** > **导出选定对象 (Export Selected)**。
- 依次选择 **导出** > **全部导出**，导出已定义的所有网络设备组。

CSV 文件可下载到您的本地硬盘。

管理网络设备组

通过以下窗口，您可以配置和管理网络设备组。

网络设备组设置

表 *3:* “网络设备组” *(Network Device Group)* 窗口中的字段

字段名称	使用指南
Name	为根网络设备组输入一个名称。对于添加到该根网络设备组的所有后续子网络设备组，请输入这个新建网络设备组的名称。 网络设备组的全称最多可以包含 100 个字符。例如，如果在父组**全球 (Global) > 亚洲 (Asia)** 下创建一个名为**印度 (India)** 的子组，则您创建的网络设备组的全称将为**全球 (Global) > 亚洲 (Asia) > 印度 (India)**。全称不能超过 100 个字符。如果网络设备组的全称超过 100 个字符，则网络设备组创建失败。
Description	为根网络设备组或子网络设备组输入一段说明。
Parent Group	要将所创建的组添加到现有父组，请从下拉列表中选择一个父组。要将此新组添加为根组，请从下拉列表中选择**添加为根组 (Add as root group)**。
Type	输入根网络设备组 (NDG) 的类型。 所有添加到根网络设备组的子网络设备组都将继承组类型。 如果此网络设备组是根网络设备组，则其类型可作为设备字典中的属性使用。您可以基于此属性定义条件。网络设备组的名称是此属性可以采用的值之一。

相关主题

网络设备组，第 3 页
思科 ISE 在策略评估中使用的网络设备属性，第 4 页
在思科 ISE 中添加网络设备

网络设备组导入设置

表 *4:* 网络设备组导入窗口中的字段

字段名称	使用指南
生成模板 (Generate a Template)	点击此链接下载 CSV 模板文件。 使用相同格式的网络设备组信息更新模板。将模板保存在本地，以便将网络设备组导入任何思科 ISE 部署中。

字段名称	使用指南
文件	点击 浏览，导航至您要上传的 CSV 文件的位置。该文件可能是新文件，也可能是从另一个思科 ISE 部署中导出的文件。 可以将包含新的和更新后的网络设备组信息的网络设备组从一个思科 ISE 部署导入另一部署。
用新数据覆盖现有数据 (Overwrite Existing Data with New Data)	如果您希望思科 ISE 用您的导入文件中的设备组替换现有网络设备组，请选中此复选框。 如果未选中此复选框，则只会将导入文件中的新网络设备组添加到网络设备组存储库。系统会忽略重复条目。
Stop Import on First Error	选中此复选框，可在导入期间遇到错误的第一个实例时停止导入。 如果未选中此复选框并且遇到错误，思科 ISE 将报告错误，并继续导入剩余设备组。

相关主题

网络设备组，第 3 页
思科 ISE 在策略评估中使用的网络设备属性，第 4 页
将网络设备组导入到思科 ISE，第 4 页

在思科 ISE 中导入模板

思科 ISE 可以让您使用 CSV 文件导入大量网络设备和网络设备组。模板包含用于定义字段格式的标题行。除非添加下表中提到的列，否则不得编辑此标题行。

在网络设备和网络设备组的相关导入流中，可以使用**生成模板 (Generate a Template)** 链接在 Microsoft Office Excel 应用中下载 CSV 文件，并在系统本地保存该文件格式。点击 Generate a Template 链接时，思科 ISE 服务器会显示 Opening template.csv 对话框。通过此对话框，您可以打开 template.csv 文件，并且针对网络设备和网络设备组使用相应的名称将 template.csv 文件以本地方式保存在系统上。如果您选择从对话框打开 template.csv 文件，默认情况下，文件会在 Microsoft Office Excel 应用中打开。

网络设备导入模板格式

下表列出了重要网络设备 CSV 模板文件标题中的字段，并进行了说明。

表 *5:* 网络设备的 *CSV* 模板字段和说明

字段	使用指南
Name:String(32)	输入网络设备的名称。名字必须是一个最多包含 32 个字符的字母数字字符串。

字段	使用指南
Description:String(256)	（可选）输入网络设备的说明，最多 256 个字符。
IP Address:Subnets(a.b.c.d/m|...)	输入网络设备的 IP 地址和子网掩码。您可以输入多个值，使用竖线 “|” 符号分隔这些值。 IPv4 地址是 支持网络设备（TACACS 和 RADIUS）配置以及外部 RADIUS 服务器配置。
Model Name:String(32)	输入网络设备的型号名称，最多 32 个字符。
Software Version:String(32)	输入网络设备的软件版本，最多 32 个字符。
Network Device Groups:String(100)	输入现有网络设备组的名称。如果是子组，必须同时包含由空格分隔的父组和子组。字符串必须是一个最多包含 100 个字符的字符串，例如，*Location#All Location#US*。
Authentication:Protocol:String(6)	输入要使用的身份验证协议。唯一有效的值为 **RADIUS** （不区分大小写）。
Authentication:Shared Secret:String(128)	（如果在 **身份验证：协议：字符串（6）** 字段中输入一个值，则此字段为必填字段）此字段是一个最多为 128 个字符的字符串。
EnableKeyWrap:Boolean(true|false)	KeyWrap 仅在网络设备上支持此字段时才启用。输入 **true** 或 **false**。
EncryptionKey:String(ascii:16|hexa:32)	（如果启用 KeyWrap，则此字段为必填字段）输入用于会话加密的加密密钥。 ASCII 值： 长度为 16 个字符（字节）。 十六进制值 - 长度为 32 个字符（字节）。
AuthenticationKey:String(ascii:20|hexa:40)	（如果启用 KeyWrap，则此字段为必填字段。）输入 RADIUS 消息键控散列消息验证码 (HMAC) 计算的密钥。 ASCII 值： 长度为 20 个字符（字节）。 十六进制值 - 长度为 40 个字符（字节）。
InputFormat:String(32)	输入加密和身份验证密钥输入格式。接受 ASCII 和十六进制值。
SNMP:Version:Enumeration (|2c|3)	输入分析器服务必须使用的 SNMP 协议版本 - 1、2c 或 3。
SNMP:RO Community:String(32)	（如果在 **SNMP:Version:Enumeration (|2c|3)** 字段中输入值，则为必填项）。为只读社区输入最多 32 个字符的字符串
SNMP:RW Community:String(32)	（如果在 **SNMP:Version:Enumeration (|2c|3)** 字段中输入值，则为必填项）。为读写社区输入最多包含 32 个字符的字符串。
SNMP:Username:String(32)	输入一个最多为 32 个字符的字符串。

字段	使用指南
	（如果在 **SNMP:Version:Enumeration (|2c|3)** 字段中输入 SNMP 版本 3，则为必填项）输入 **Auth**、**No Auth** 或 **Priv**。
SNMP:Authentication Protocol:Enumeration(MD5|SHA)	（如果已输入 **Auth** 或 **Priv** 作为 SNMP 安全级别，则此字段为必填字段。）输入 **MD5** 或 **SHA**。
SNMP:Authentication Password:String(32)	（如果已在 **SNMP:Security Level:Enumeration(Auth|No Auth|Priv)** 字段中输入 **Auth**，则为必填项。）输入一个最多为 32 个字符的字符串。
SNMP:Privacy Protocol:Enumeration(DES|AES128|AES192|AES256|3DES)	（如果您在 **SNMP:Security Level:Enumeration(Auth|No Auth|Priv)** 字段中输入了 **Priv**，则为必填项。）输入 **DES**、**AES128**、**AES192**、**AES256** 或 **3DES**。
SNMP:Privacy Password:String(32)	（如果您在 **SNMP:Security Level:Enumeration(Auth|No Auth|Priv)** 字段中输入了 **Priv**，则为必填项。）输入一个最多为 32 个字符的字符串。
SNMP:Polling Interval:Integer:600-86400 seconds	输入 SNMP 轮询间隔（秒）。有效值为介于 600 和 86400 之间的整数。
SNMP:Is Link Trap Query:Boolean(true|false)	通过输入 **true** 或 **false** 来启用或禁用 SNMP 链路陷阱。
SNMP:Is MAC Trap Query:Boolean(true|false)	通过输入 **true** 或 **false**来启用或禁用 SNMP MAC 陷阱。
SNMP:Originating Policy Services Node:String(32)	指示必须用于轮询 SNMP 数据的思科 ISE 服务器。它默认情况下是自动的，但可以通过在此字段中分配不同的值来覆盖该设置。
Trustsec:Device Id:String(32)	输入思科 Trustsec 设备 ID，是最多为 32 个字符的字符串。
Trustsec:Device Password:String(256)	（如果已输入思科 TrustSec 设备 ID，则为必填项。）输入思科 TrustSec 设备密码，该密码是最多包含 256 个字符的字符串。
Trustsec:Environment Data Download Interval:Integer:1-2147040000 seconds	输入思科 TrustSec 环境数据下载时间间隔。有效值为介于 1 和 2147040000 之间的整数。
Trustsec:Peer Authorization Policy Download Interval:Integer:1-2147040000 seconds	输入 TrustSec 对等体授权策略下载时间间隔。有效值为介于 1 和 2147040000 之间的整数。
Trustsec:Reauthentication Interval:Integer:1-2147040000 seconds	输入 TrustSec 重新身份验证时间间隔。有效值为介于 1 和 2147040000 之间的整数。
Trustsec:SGACL List Download Interval:Integer:1-2147040000 seconds	输入思科 TrustSec 安全组 ACL 列表下载间隔。有效值为介于 1 和 2147040000 之间的整数。
Trustsec:Is Other Trustsec Devices Trusted:Boolean(true|false)	通过输入 **true** 或 **false**指示思科 TrustSec 设备是否受信任。
Trustsec:Notify this device about Trustsec configuration changes:String(ENABLE_ALL|DISABLE_ALL)	通过输入 **ENABLE_ALL** 或 **DISABLE_ALL** 通知思科 TrustSec 配置更改到思科TrustSec设备。

字段	使用指南
Trustsec:Include this device when deploying Security Group Tag Mapping Updates:Boolean(true|false)	通过输入 **true** or **false**指示思科 TrustSec 设备是否包含在安全组标签中。
Deployment:Execution Mode Username:String(32)	输入有权编辑设备配置的用户名。这是一个最多为 32 个字符的字符串。
Deployment:Execution Mode Password:String(32)	输入设备密码，该密码是最多包含 32 个字符的字符串。
Deployment:Enable Mode Password:String(32)	输入设备的密码，可以让您编辑设备的配置。这是一个最多为 32 个字符的字符串。
Trustsec:PAC issue date:Date	输入思科 ISE 为思科 TrustSec 设备生成的最后一个思科 Trustsec PAC 的颁发日期。
Trustsec:PAC expiration date:Date	输入思科 ISE 为思科 TrustSec 设备生成的最后一个思科 Trustsec PAC 的到期日期。
Trustsec:PAC issued by:String	输入思科 ISE 为思科 TrustSec 设备生成的最后一个思科 Trustsec PAC 的颁发者（思科 TrustSec 管理员）名称。它必须是一个字符串值。

网络设备组导入模板格式

下表列出模板标题中的字段并提供网络设备组 CSV 文件中的字段描述。

表 *6:* 网络设备组的 *CSV* 模板字段和描述

字段	说明
Name:String(100):	（必填）此字段为网络设备组的名称。它是长度最大为 100 个字符的字符串。NDG 全名的长度最大为 100 个字符。例如，如果在父组“全球”(Global) >“亚洲”(Asia) 下创建一个“印度”(India) 的子组，那么您创建的 NDG 的全称将是 Global#Asia#India。 全称的长度不能超过 100 个字符。如果 NDG 的全名超过 100 个字符，则 NDG 将无法创建。
Description:String(1024)	此字段是可选字段。它是长度不超过 1024 个字符的字符串。
Type:String(64):	（必填）此字段为网络设备组的类型。它是长度最大为 64 个字符的字符串。
Is Root:Boolean(true|false):	（必填）此字段用于确定特定的网络设备组是否为根组。有效值为 true 或 false。

移动设备管理器与思科 ISE 的互操作性

移动设备管理(MDM)服务器保护、监控、管理和支持跨移动运营商、服务提供商和企业部署的移动设备。传统上，MDM 服务器仅支持移动设备。某些 MDM 服务器现在管理网络中的所有类型的设备（移动电话、平板电脑、笔记本电脑和台式机），称为统一终端管理 (UEM) 服务器。MDM 服务器作为策略服务器运行，用于控制移动设备上的某些应用（例如，电子邮件应用）在部署环境中的使用。思科 ISE 向连接的 MDM 服务器查询可用于创建网络授权策略的各种属性的相关信息。

在此示例图中，思科 ISE 是执行点，而 MDM 策略服务器是策略信息点。思科 ISE 从 MDM 服务器获取数据，以提供完整的解决方案。

有关思科 ISE 支持的 MDM 供应商的列表，请参阅支持的 MDM 服务器，第 12 页。

支持的移动设备管理使用情形

思科 ISE 与外部 MDM 服务器联合执行以下功能：

- 管理设备注册：访问网络的未注册终端会重定向到 MDM 服务器上托管的注册页面。设备注册包括用户角色、设备类型等。
- 处理设备补救 ：在补救期间向终端授予有限访问权限。
- 增强终端数据：使用来自 MDM 服务器的信息更新终端数据库，这些信息是无法使用思科 ISE 分析服务收集的。思科 ISE 使用可在**终端 (Endpoints)** 页面中查看的多个设备属性。选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **身份 (Identities)** > **终端 (Endpoints)** 。

  以下是可用设备属性的示例。

  - MDMImei: xx xxxxxx xxxxxx x
  - MDMManufacturer: Apple
  - MDMModel: iPhone
  - MDMOSVersion: iOS 6.0.0
  - MDMPhoneNumber: 5550100
  - MDMSerialNumber: DNPGQZGUDTFx

- 每 4 小时轮询一次 MDM 服务器，获取设备合规性数据。在**外部 MDM 服务器 (External MDM Servers)** 页面中配置轮询间隔。（要查看此页面，选择。
- 通过 MDM 服务器发出设备指示：思科 ISE 通过 MDM 服务器发出针对用户设备的远程操作。通过**终端 (Endpionts)** 页面从思科 ISE 管理门户发起远程操作。要查看此页面，选择**情景可视性 (Context Visibility)** > **终端 (Endpoints)**。选中 MDM 服务器旁的复选框，然后点击 **MDM 操作 (MDM Actions)**。从显示的下拉列表中选择所需的操作。

供应商 MDM 属性

在思科 ISE 中配置 MDM 服务器时，思科 ISE 会查询 MDM 服务器以获取设备属性信息，并将该信息添加到 MDM 系统词典。以下属性用于注册状态，通常受 MDM 供应商支持。

思科 ISE 使用 API 向 MDM 服务器查询所需的设备属性。思科 ISE 版本 3.1 及更高版本支持 MDM API 版本 3。版本 3 API 包括允许思科 ISE 向 MDM 服务器发送查询的 API，以帮助思科 ISE 识别使用 MAC 地址随机化的终端。思科 ISE 向 MDM 服务器查询以下属性：

- GUID：唯一的设备标识符，用于代替 MAC 地址来标识设备。
- MAC 地址：UEM 或 MDM 服务器为特定设备记录的 MAC 地址列表。一台设备最多可共享五个 MAC 地址。

如果 MDM 服务器未提供所需属性的值，思科 ISE 将使用下表中提到的默认值填充属性字段。

表 *7: MDM* 属性和值

属性名称	属性词典	默认值	预期来自 **UEM** 或 **MDM** 服务器的数据	预期来自 **Microsoft SCCM** 服务器的数据
DaysSinceLastCheckin 从 MDM API 版本 3 开始支持	MDM	无	自用户上次签入设备或将设备与 UEM 或 MDM 服务器同步以来的天数。有效范围为 1 至 365 天。	自用户上次签入设备或将设备与 SCCM 服务器同步以来的天数。有效范围为 1 至 365 天。
DeviceCompliantStatus	MDM	不合规	**合规** 或 **非合规**。	**合规** 或 **非合规**。
DeviceRegisterStatus	MDM	已注销	**已注册** 或 **已注销**。	**已注册** 或 **已注销**。
DiskEncryptionStatus	MDM	熄灭	**开启** 或 **关闭**。	**开启** 或 **关闭**。
IMEI	MDM	无	设备的 IMEI 编号。	不适用。
JailBrokenStatus	MDM	不间断	**可访问** 或 **无法访问**。	**可访问** 或 **无法访问**。
MDM 失败原因	MDM	无	设备故障原因。	设备故障原因。
MDMServerName	MDM	无	服务器的名称。	服务器的名称。
MDMServerReachable	MDM	可访问	**可访问** 或 **无法访问**。	**可访问** 或 **无法访问**。
MEID	MDM	无	设备的 MEID 值。	不适用。
Manufacturer	MDM	无	设备制造商的名称。	不适用。
型号	MDM	无	设备型号的名称。	不适用。
OsVersion	MDM	无	设备的操作系统版本。	不适用。
无法	MDM	无	设备的电话号码。	不适用。

属性名称	属性词典	默认值	预期来自 **UEM** 或 **MDM** 服务器的数据	预期来自 **Microsoft SCCM** 服务器的数据
PinLockStatus	MDM	熄灭	**开启** 或 **关闭**。	不适用。
SerialNumber	MDM	无	设备的序列号。	不适用。
服务器类型	MDM	无	移动设备管理器服务器的 **MDM**。 桌面设备管理器服务器的 **DM**。	桌面设备管理器服务器的 **DM**。
UDID	MDM	无	设备的 UDID 编号。	不适用。
UserNotified	MDM	否	**是** 或 **否**	不适用。

如果不支持供应商的唯一属性，可以使用 ERS API 来交换供应商特定属性。请查阅供应商的文档，了解有关支持的 ERS API 的信息。

新 MDM 字典属性可以在授权策略中使用。

当这些 MDM 字典属性用于策略时，无法从思科 ISE 中删除 MDM 服务器配置。要删除 MDM 服务器配置，必须先从策略中删除相关的 MDM 字典属性，然后从思科 ISE 中删除 MDM 服务器。

支持的 MDM 服务器

支持的 MDM 服务器包括来自以下供应商的产品：

- Airwatch, Inc.
- Good Technology
- MobileIron, Inc.
- Zenprise, Inc.
- SAP Afaria
- Fiberlink/IBM MaaS
- Meraki

移动设备管理服务器使用的端口

下表列出思科 ISE 和 MDM 服务器之间要相互通信必须打开的端口。有关必须在 MDM 代理和服务器上打开的端口的列表，请参阅 MDM 供应商的文档。

表 *8: MDM* 服务器使用的端口

MDM 服务器	端口
MobileIron	443
Citrix XenMobile 10.x (On-Prem)	443
Blackberry - Good Secure EMM	19005
VMware Workspace ONE（之前称为 AirWatch）	443
SAP Afaria	443
IBM MaaS360	443
Cisco Meraki	443
Microsoft Intune	80 和 443
Microsoft SCCM	80 和 443

移动设备管理集成流程

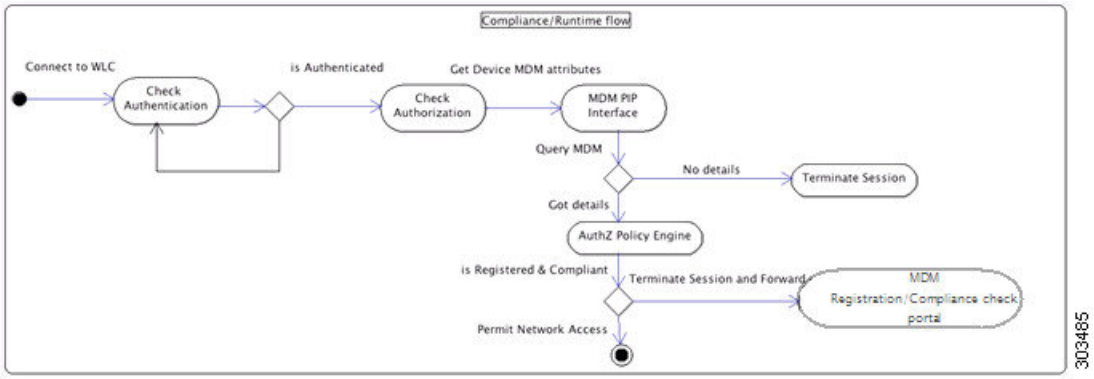
1. 用户将设备与 SSID 关联。
2. ISE 向 MDM 服务器发出 API 调用。
3. 此 API 调用会返回用户的设备列表和这些设备的终端安全评估状态。

注释 输入参数是终端设备的 MAC 地址。对于异地 Apple iOS 设备，输入参数为 UDID。

4. 思科 ISE 使用 MDM 调配设备并向用户显示相应的页面供其注册设备。
5. 用户在 MDM 服务器中注册设备，然后 MDM 服务器通过自动重定向或手动刷新浏览器将此请求重定向至思科 ISE。
6. 思科 ISE 重新查询 MDM 服务器获取安全评估状态。
7. 如果用户的设备不符合 MDM 服务器上配置的终端安全评估（合规性）策略，系统会向用户告知设备不合规。用户必须采取必要的措施来确保设备合规。
8. 用户设备合规后，MDM 服务器会在其内部表中更新设备状态。
9. 如果用户现在刷新浏览器，思科 ISE 将恢复控制。

10. 思科 ISE 每四小时会对 MDM 服务器进行轮询，以获取合规性信息并发出适当的授权更改 (CoA)。您可以配置轮询间隔。思科 ISE 还会每五分钟检查一次 MDM 服务器以确保其可用。

图 *1:* 思科 *ISE* 中的 *MDM* 流程



使用思科 ISE 设置移动设备管理服务器

要使用思科 ISE 设置 MDM 服务器，您必须执行以下高级任务：

步骤 1 将 MDM 服务器证书导入思科 ISE。

步骤 2 创建移动设备管理器定义。

步骤 3 在思科 WLC 上配置 ACL。

步骤 4 配置将非注册设备重定向到 MDM 服务器的授权配置文件。

步骤 5 为 MDM 使用案例配置授权策略规则。

将移动设备管理服务器证书导入思科 ISE

要使思科 ISE 连接 MDM 服务器，您必须将 MDM 服务器证书导入思科 ISE 受信任证书库。如果您的 MDM 服务器有一个 CA 签名的证书，您必须将根证书导入思科 ISE 受信任证书库。

步骤 1 从您的 MDM 服务器导出 MDM 服务器证书并将其保存至您的本地计算机上。

步骤 2 **管理 (Administration)** > **证书 (Certificates)** > **证书库 (Certificate Store)** > **导入 (Import)**。

步骤 3 在**将新证书导入证书库 (Import a new Certificate into the Certificate Store)** 窗口中，点击**浏览 (Browse)**，选择从 MDM 服务器获取的 MDM 服务器证书。

步骤 4 在**友好名称 (Friendly Name)** 字段中，输入证书名称。

步骤 5 点击 **Submit**。

步骤 6 确认**信任证书 (Trust Certificates)** 窗口列出新添加的 MDM 服务器证书。

在思科 ISE 中配置移动设备管理服务器

向思科 ISE 提供终端信息的第一个 MDM 服务器显示在 **情景可视性** > **终端** 窗口中的终端信息中。当终端与其他 MDM 服务器连接时，MDM 服务器信息不会自动更新。您必须从 **情景可视性** 窗口中删除终端，然后终端必须与 MDM 服务器重新连接，以便 **情景可视性** 窗口显示更新的信息。

下图显示了在此任务期间必须使用的思科ISE GUI字段。图中的编号对应于以下任务中的步骤编号。

图 *2:* 在思科 *ISE* 中添加 *MDM* 服务器

步骤 1 选择**管理 (Administration)** > **网络资源 (Network Resources)** > **外部 MDM (External MDM)**。

步骤 2 在 **MDM 服务器** 窗口中，点击 **添加**。

步骤 3 在相应的字段中输入要添加的 MDM 服务器的名称和说明。

步骤 4 从**服务器类型 (Server Type)** 下拉列表中，选择**移动设备管理器 (Mobile Device Manager)**。

步骤 5 从**身份验证类型 (Authentication Type)** 下拉列表中，选择**基础 (Basic)** 或 **OAuth-客户端凭证 (OAuth - Client Credentials)**。

如果选择**基础 (Basic)** 身份验证类型，则会显示以下字段：

- **主机名/IP 地址 (Host Name/IP Address)**：输入 MDM 服务器主机名或 IP 地址。
- **端口**：指定连接至 MDM 服务器时要使用的端口，通常为 443。
- **实例名称 (Instance Name)**：如果此 MDM 服务器有多个实例，应输入要连接到的实例。
- **用户名 (Username)**：输入连接到 MDM 服务器时必须使用的用户名。
- **密码 (Password)**：输入连接到 MDM 服务器所必须使用的密码。

如果您选择 **OAuth-客户端凭证 (OAuth - Client Credentials)** 身份验证类型，则会显示以下字段：

- 从**自动发现 (Auto Discovery)** 下拉列表中，选择**是 (Yes)** 或**否 (No)**。
- **自动发现 URL**：输入 Microsoft Azure 管理门户中的 Microsoft Azure AD 图形 API 终端值。此 URL 是应用可使用图形 API 访问 Microsoft Azure AD 中的目录数据的终端。有关详细信息，请参阅 将 MDM 和 UEM 服务器与思科 ISE 集成。
- **客户端 ID (Client ID)**：应用的唯一标识符。如果应用访问其他应用中的数据，如 Microsoft Azure AD Graph API、Microsoft Intune API 等，则需要使用此属性。
- **颁发令牌的 URL**：输入 Oauth2.0 授权终端值。在该终端上，思科 ISE 可以使用 OAuth2.0 获得访问令牌。
- **令牌受众 (Token Audience)**：令牌面向的接收资源，通常为指向 Microsoft Intune API 的公共知名 **APP ID URL**。

合规性设备重新身份验证查询的时间间隔 (Time Interval For Compliance Device ReAuth Query)：当终端通过身份验证或重新进行身份验证时，思科 ISE 使用缓存获取该终端的 MDM 变量。如果缓存值的期限高于该字段中配置的值，则思科 ISE 会向 MDM 服务器进行设备查询以获取新值。如果合规性状态已变化，则思科 ISE 会触发相应的 CoA。有效范围为 1 到 1440 分钟。默认值为 1 分钟。

轮询间隔：输入思科 ISE 轮询 MDM 服务器以获取合规性检查信息的轮询间隔（以分钟为单位）。此值应与 MDM 服务器上的轮询间隔相同。默认值为 240 分钟。我们建议您在生产环境中将轮询间隔设置为 60 分钟以上，以最大限度地减少因大量不合规终端而可能产生的任何性能影响。

如果将轮询间隔设置为 0，则思科 ISE 会禁用与 MDM 服务器的投票。

注释 如果外部 MDM 服务器收到来自超过 20000 个不合规终端的请求，则外部 MDM 服务器轮询间隔会被自动设置为 0。您还会在思科 ISE 上收到以下警报：

```
MDM 合规性轮询已禁用：原因是定期合规性轮询收到大量不合规设备信息。
```

步骤 6 从 **状态** 下拉列表中，选择 **已启用**。

步骤 7 要验证 MDM 服务器是否已连接到思科 ISE，请点击 **测试连接**。请注意 **测试连接** 并非旨在检查所有使用案例的权限（获取基准、获取设备信息等）。这些在服务器添加到思科 ISE 时进行验证。

步骤 8 点击**保存**。

在思科 ISE 中定义 Microsoft System Center Configuration Manager 服务器

步骤 1 选择**管理 (Administration)** > **网络资源 (Network Resources)** > **外部 MDM (External MDM)** > **MDM 服务器 (MDM Servers)**。

步骤 2 在 **MDM 服务器 (MDM Servers)** 窗口中，单击**添加 (Add)**。

步骤 3 从 **服务器类型 (Server Type)** 下拉列表选择 **桌面设备管理器 (Desktop Device Manager)** 。

步骤 4 在**主机名/ IP 地址 (Host Name / IP Address)** 字段中，输入 Microsoft SCCM 服务器主机名或 IP 地址。

步骤 5 在**实例名称 (Instance Name)** 字段中，如果 Microsoft SCCM 服务器有多个实例，输入要连接到的实例。

步骤 6 在**用户名 (Username)** 字段中，输入连接到 Microsoft SCCM 服务器所必须使用的用户名。

步骤 7 在**密码 (Password)** 字段中，输入连接到 Microsoft SCCM 服务器所必须使用的密码。

步骤 8 在**合规性设备重新身份验证查询的时间间隔 (Time Interval For Compliance Device ReAuth Query)**字段中，输入一个介于 1 和 1440 分钟之间的值。默认值为 1 分钟。合规性设备重新身份验证查询的时间间隔 (Time Interval For Compliance Device ReAuth Query)：当终端通过身份验证或重新进行身份验证时，思科 ISE 使用缓存获取该终端的 MDM 变量。如果缓存值的期限高于该字段中配置的值，则思科 ISE 会向 MDM 服务器进行设备查询以获取新值。如果合规性状态已变化，则思科 ISE 会触发相应的 CoA。

步骤 9 从**状态 (Status)** 下拉列表中选择**已启用 (Enabled)**。

步骤 10 单击**测试连接 (Test Connection)** 以检查思科 ISE 是否可以连接到定义的 Microsoft SCCM 服务器。

步骤 11 点击**保存 (Save)**。

为 WMI 访问开放防火墙端口

Microsoft Active Directory 域控制器上的防火墙软件可能会阻止对 WMI 的访问。您可以关闭防火墙，或者允许在特定 IP 地址（思科 ISE IP 地址）访问以下端口：

- TCP 135：通用 RPC 端口。在执行异步 RPC 呼叫时，侦听此端口的服务告知客户端处理此请求的组件使用哪个端口。
- UDP 138：NetBIOS 数据报服务
- TCP 139：NetBIOS 会话服务
- TCP 445：服务器消息块 (SMB)

注释 思科 ISE 支持 SMB 2.0。

可以动态分配更高的端口，也可以手动进行配置。我们建议您添加 *%SystemRoot%\System32\dllhost.exe* 作为目标。此程序可动态管理端口。

所有防火墙规则均可分配到特定 IP 地址（思科 ISE IP）。

配置用于重定向未注册设备的授权配置文件

开始之前

- 确保您已在思科 ISE 中创建 MDM 服务器定义。只有在成功将思科 ISE 与 MDM 服务器集成后才会填充 MDM 词典。然后，您可以使用 MDM 词典属性来创建授权策略。
- 在思科 WLC 上配置 ACL 以重定向未注册的设备。

步骤 1 选择 **策略 (Policy)** > **策略元素 (Policy Elements)** > **结果 (Results)** > **授权 (Authorization)** > **授权配置文件 (Authorization Profiles)** > **添加 (Add)**。

步骤 2 创建用于重定向不合规或未注册的非注册设备的授权配置文件。

步骤 3 在**名称 (Name)** 字段中，为授权配置文件输入与 MDM 服务器名称匹配的名称。

步骤 4 从**访问类型 (Access Type)** 下拉列表中，选择 **ACCESS_ACCEPT**。

步骤 5 在**常见任务 (Common Tasks)** 部分中，选中 **Web 重定向 (Web Redirection)** 复选框，然后从下拉列表中选择 **MDM 重定向 (MDM Redirect)**。

步骤 6 从 **ACL** 下拉列表中，选择输入您在无线 LAN 控制器上配置的 ACL 的名称。

步骤 7 点击**提交 (Submit)**。

下一步做什么

为 MDM 使用案例配置授权策略规则。

为 MDM 使用案例配置授权策略规则

在思科 ISE 中配置授权策略规则以完成 MDM 配置。

开始之前

- 将 MDM 服务器证书添加到思科 ISE 证书库。
- 确保您已在思科 ISE 中创建了 MDM 服务器定义。只有在成功将思科 ISE 与 MDM 服务器集成之后，才会填充 MDM 字典，您才可以使用 MDM 字典属性创建授权策略。
- 在思科 WLC 上配置 ACL 以重定向未注册或不合规设备。

步骤 1 选择**策略 (Policy)** > **授权 (Authorization)** > **下方插入新规则 (Insert New Rule Below)**。

步骤 2 选择 **策略 (Policy)** > **策略集 (Policy Sets)**，然后展开策略集以查看授权策略规则。

步骤 3 添加以下规则：

- **MDM_Un_Registered_Non_Compliant**：适用于尚未向 MDM 服务器注册或不符合 MDM 策略的设备。当请求与此规则匹配之后，系统会显示思科 ISE MDM 窗口，其中包含有关向 MDM 注册设备的信息。

  注释　请勿在此策略中使用 **MDM.MDMServerName** 条件。使用此条件时，仅当终端注册到 MDM 服务器注册后，才与策略匹配。

- **PERMIT**：如果设备已注册到思科 ISE、MDM，并符合思科 ISE 和 MDM 策略，则系统将根据思科 ISE 中配置的访问控制策略向它授予网络访问权限。

  下图显示了此配置的示例。

  图 *3: MDM* 使用案例的授权策略规则

步骤 4 点击**保存 (Save)**。

在无线控制器上配置 ACL 以实现 MDM 互操作性

在无线控制器上配置 ACL 以用于授权策略，从而重定向未注册的设备和证书调配。ACL 必须采用以下顺序。

步骤 1 允许所有从服务器到客户端的出站流量。

步骤 2 （可选）允许从客户端到服务器的 ICMP 入站流量以进行故障排除。

步骤 3 允许未注册和不合规设备访问 MDM 服务器，以下载 MDM 代理和执行合规检查。

步骤 4 允许从客户端到服务器再到 ISE 的所有入站流量以执行 Web 门户和请求方以及证书调配流程。

步骤 5 允许从客户端到服务器的入站域名系统 (DNS) 流量以进行名称解析。

步骤 6 允许从客户端到服务器的入站 DHCP 流量以获取 IP 地址。

步骤 7 拒绝所有从客户端到服务器再到企业资源的入站流量，以重定向至思科 ISE（根据公司策略）。

步骤 8 （可选）允许其余流量。

示例

以下示例显示的 ACL 用于将未注册的设备重定向至 BYOD 流程。在本例中，思科 ISE IP 地址为 10.35.50.165，内部企业网络 IP 地址为 192.168.0.0 和 172.16.0.0（重定向），MDM 服务器子网为 204.8.168.0。

图 *4:* 用于重定向未注册设备的 *ACL*

General

Access List Name NSP-ACL

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	150720
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Inbound	7227
3	Permit	0.0.0.0 / 0.0.0.0	204.8.168.0 / 255.255.255.0	Any	Any	Any	Any	Any	17626
4	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	7505
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	2864
6	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DHCP Server	Any	Inbound	0
7	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0
8	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	4
9	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	457
10	Deny	0.0.0.0 / 0.0.0.0	173.194.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	1256
11	Deny	0.0.0.0 / 0.0.0.0	171.68.0.0 / 255.252.0.0	Any	Any	Any	Any	Inbound	11310
12	Deny	0.0.0.0 / 0.0.0.0	171.71.181.0 / 255.255.255.0	Any	Any	Any	Any	Any	0
13	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	71819

擦除或锁定设备

思科 ISE 可以让您擦除已丢失的设备或启用其 pin 锁。您可以从**终端 (Endpoints)** 窗口配置此特性。

步骤 1 选择 **管理 (Administration)** > **身份管理 (Identity Management)** > **身份 (Identities)** > **终端 (Endpoints)** 。

步骤 2 选中您想要擦除或锁定的设备旁边的复选框。

步骤 3 从 **MDM 操作(MDM Actions)** 下拉列表中，选择以下选项之一：

- **完全擦除 (Full Wipe)**：此选项会删除公司应用或将设备重置为出厂设置，具体取决于 MDM 供应商。
- **企业擦除 (Corporate Wipe)**：此选项会删除您在 MDM 服务器策略中配置的应用。
- **PIN 锁定**：此选项会锁定设备。

步骤 4 点击 **Yes** 擦除或锁定设备。

查看移动设备管理报告

思科 ISE 记录 MDM 服务器定义的所有添加、更新和删除操作。可以在**更改配置审核 (Change Configuration Audit)** 报告中查看这些事件，该报告显示选定时段内任何系统管理员的全部配置更改。

选择 **操作 (Operations)** > **报告 (Reports)** > **报告 (Reports)** > **审核 (Audit)** > **更改配置审核 (Change Configuration Audit)**。检查您要查看的 MDM 服务器的**对象类型 (Object Type)** 和**对象名称 (Object Name)** 列中的条目，然后点击相应的**事件 (Event)** 值以查看配置事件的详细信息。

查看移动设备管理日志

您可以使用**消息目录 (Message Catalog)** 窗口查看移动设备管理器日志消息。选择**管理 (Administration)** > **系统 (System)** > **日志记录 (Logging)** > **消息目录 (Message Catalog)**。MDM 日志条目的默认报告级别为“INFO”。您可以将报告级别更改为“调试”(DEBUB) 或“跟踪”(TRACE)。

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。