Cisco Meraki EMM 与思科身份服务引擎的集成

安全访问操作指南系列

作者：Imran Bashir

日期：2015 年 3 月

目录

移动设备管理 (MDM) 3
概览 3
Cisco Meraki EMM 云集成使用案例概览 4
使用 MDM 集成配置步骤 6
Cisco ISE 和 MDM 集成配置 6
查看 MDM 字典 9
配置 ISE 授权策略 10
附录 A：Meraki EMM 配置 14
Cisco TrustSec 系统： 23
设备配置指南： 23

移动设备管理 (MDM)

概览

Cisco Meraki 企业移动管理 (EMM) 软件可以保护、监控、管理和支持在移动运营商、服务提供商和企业中部署的移动设备。典型的 Cisco Meraki EMM 配置包括基于云的策略服务器和移动设备客户端。但是，通常网络是可以提供终端精细访问的唯一实体（基于 ACL、TrustSec SGT 等）。按照设想，思科身份服务引擎 (ISE) 将用作基于网络的附加实施点，而基于云的 Cisco Meraki EMM 策略服务器则用作策略决策点。ISE 预期接收来自 Cisco Meraki 云 EMM 服务器的特定数据，以提供完整的解决方案。

以下是此解决方案的概要使用案例。

设备注册 - 访问企业内部网络的非注册终端将被重定向至 Cisco Meraki EMM 云上的注册页面，以便根据用户角色、设备类型等进行注册。此外，Meraki 还可以利用 AnyConnect (VPN)、Jabber（协作）等企业应用调配设备，从而使用户可以在设备位于企业外部时安全访问企业资源（依据策略）。

补救 - 不合规的终端将根据合规状态获得受限制的访问权限

定期合规检查 - 定期通过 Cisco Meraki EMM 云服务器检查合规性

ISE 管理员可以通过 Cisco Meraki EMM 云在设备上**发出远程操作**（例如：远程擦除受管设备）

最终用户可利用 ISE My Devices Portal 管理个人设备，例如进行完全擦除、企业级擦除和 PIN 锁。

网络拓扑示例

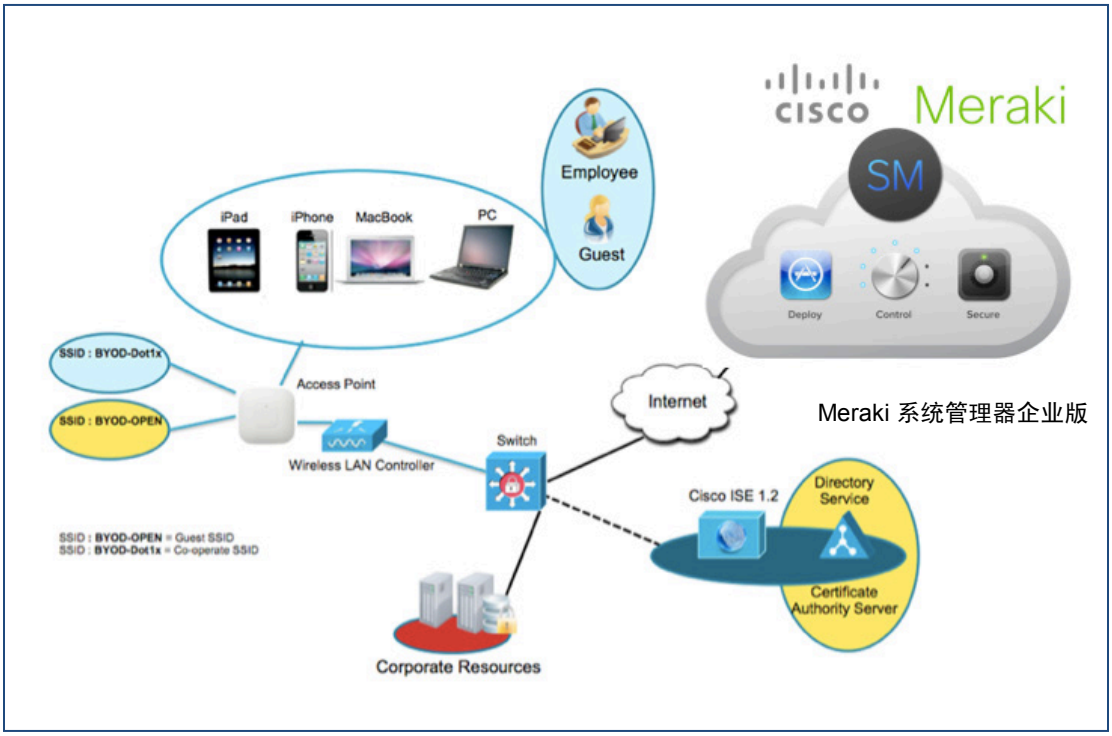


图 1. ISE+EMM 集成拓扑

Cisco Meraki EMM 云集成使用案例概览

1. 用户将设备与 SSID 关联。
2. 如果用户设备尚未注册，用户将完成自带设备自行激活流程，详细信息如附录所示。
3. ISE 向 Cisco Meraki EMM 云请求 API 调用。
4. 此 API 调用返回适用于该用户的设备列表和这些设备的安全状态 - 请注意，我们可以输入参数的形式传递终端设备的 MAC 地址。
5. 如果用户的设备不在此列表中，这意味着该设备未向 Cisco Meraki EMM 云注册。ISE 会向 NAD 发送授权以重定向至 ISE，并会将用户重定向至 Cisco Meraki EMM 云（主页或登录页）。
6. ISE 将获知该设备需要使用 Cisco Meraki EMM 云进行调配，并会向用户显示适当的页面以进行注册。
7. 用户将被转至 Cisco Meraki EMM 云策略引擎，用户将在引擎中完成注册。通过 Cisco Meraki EMM 云服务器的自动重定向或通过用户重新刷新浏览器，控制权将交回给 ISE。
8. ISE 将再次查询 Cisco Meraki EMM 云，以获取安全状态信息。
9. 如果用户设备不符合 Cisco Meraki EMM 云中配置的安全状态（合规性）策略，系统将通知其设备不合规、不合规的原因以及访问网络资源的合规必要性。
10. 用户设备合规之后，Cisco Meraki EMM 云将在其内部表中更新设备状态。
11. 在此阶段，用户可以刷新浏览器，此时控制权将交回给 ISE。
12. ISE 还将定期轮询 Cisco Meraki EMM 云获取合规信息，并相应地发出 COA。

组件

表 1. 本文档中使用的组件 标签

组件	硬件	经过测试的功能	Cisco IOS®软件版本
思科身份服务引擎 (ISE)	支持以下任一硬件：1121/3315、3355、3395、VMware、3415、3495	集成 AAA、策略服务器和服务（访客、分析器和安全状态）	ISE 1.3
EMM 服务器	EMM	云服务	
无线局域网控制器 (WLC)	5500 系列 2500 系列 WLSM-2 虚拟控制器	分析和授权更改 (CoA)	统一无线 7.2
Cisco Meraki 云无线局域网		使用 Cisco Meraki EMM 云的云管理无线 经过测试可替换传统 WLC	不适用
测试设备：例如 Apple iOS、Google Android	Apple 和 Google	不适用	Apple iOS 5.0 及更高版本 Google Android 2.3 及更高版本

注意：在本文档中，我们仅演示了如何配置 Cisco Meraki EMM 云。我们建议您使用我们的操作指南将 ISE 和 WLC/Meraki 配置到建议状态。
操作指南：http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/howto_60_byod_certificates.pdf
有关更多指南，请访问：http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html
https://docs.meraki.com/display/kb/Wireless+LAN

使用 MDM 集成配置步骤

Cisco ISE 和 MDM 集成配置

图 2 显示了配置 MDM 集成的主要步骤。

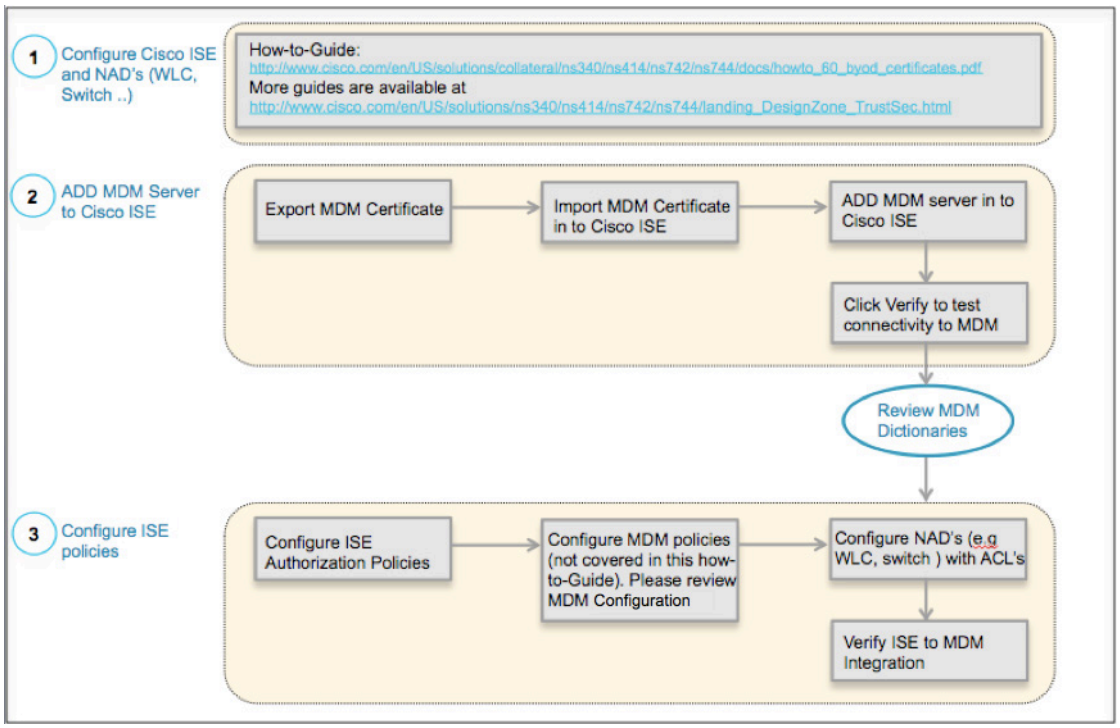


图 2. MDM 配置流程

将外部 MDM 服务器添加至 ISE

Cisco Meraki 的 EMM 服务器可用作云服务；在云上配置了安装、基本设置和合规性检查之后，就可将其添加至 ISE。

导出 MDM 服务器证书

步骤 1 导出 EMM 服务器证书并将其保存在本地计算机上。

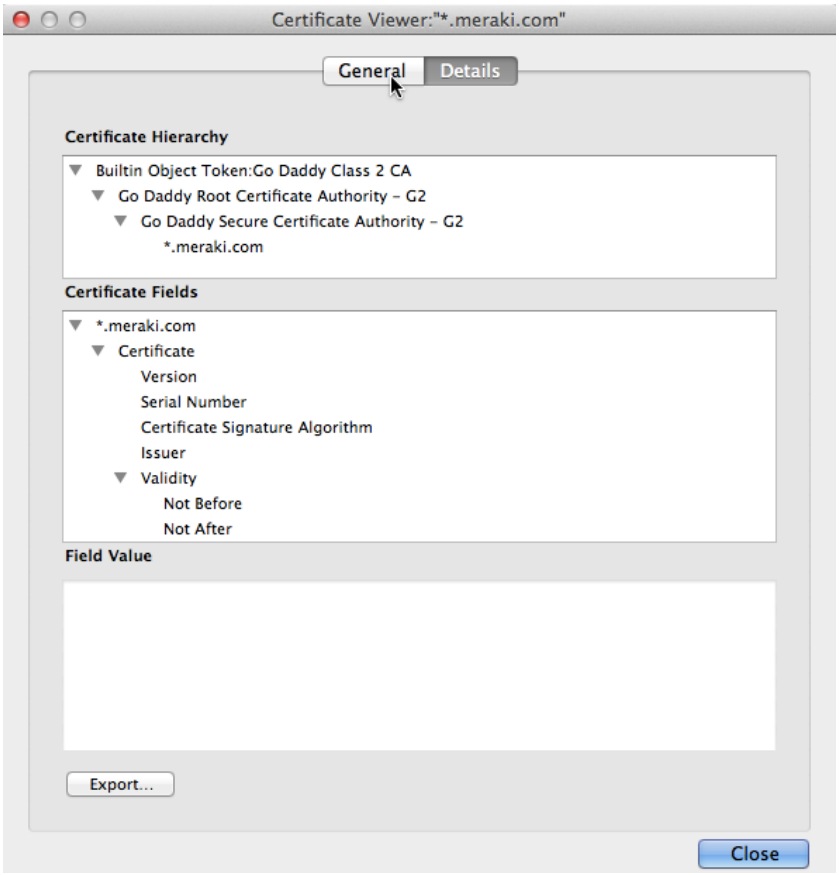


图 3. 导出 MDM 证书

步骤 2 将证书导入 ISE

导航至：**管理 (Administration) -> 证书 (Certificates) -> 证书库 (Certificate Store) -> 导入 (Import)**

在“证书文件”(Certificate File) 上点击“浏览”(Browse)，然后选择“Meraki 证书”(Meraki Certificate)

可选：添加一个容易记住的名称，然后点击“提交”(Submit)

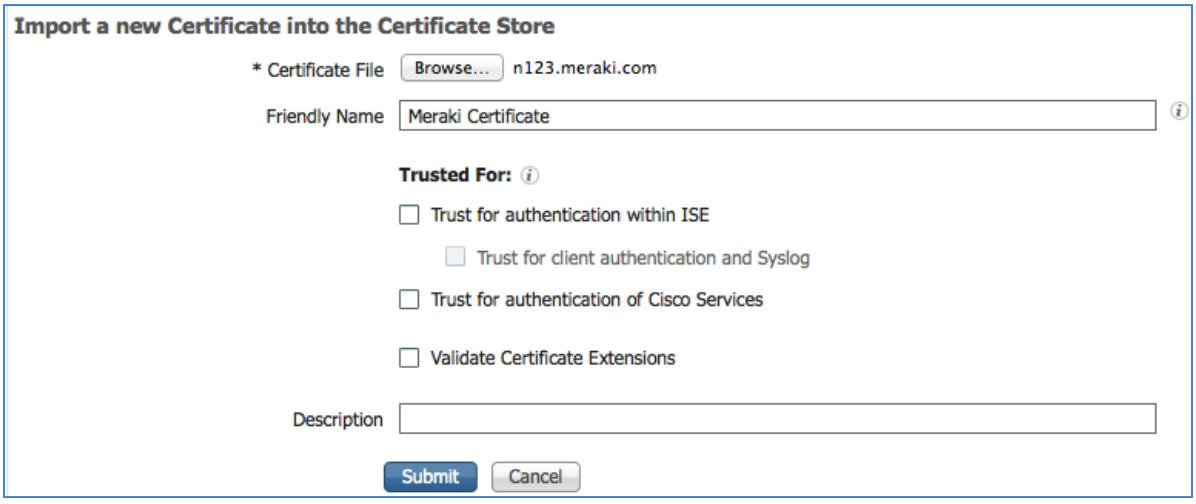


图 4. 将 MDM 证书导入 Cisco ISE

步骤 3 确认证书是否在证书存储区中。

在受信任证书 (Trusted Certificates) 下

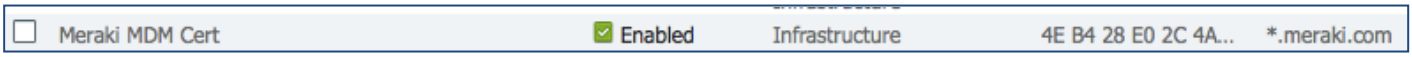


图 5. 确认 MDM 证书是否在 Cisco ISE 中

步骤 4 添加 MDM 服务器。**管理 (Administration) -> MDM**

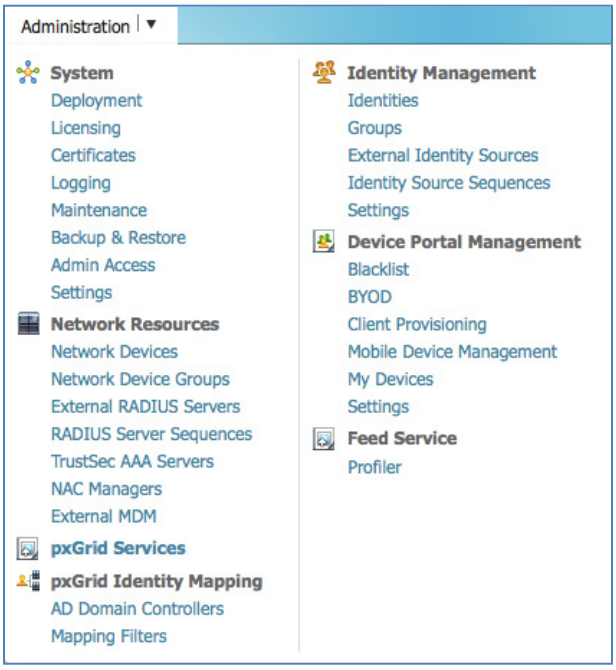


图 6. 在 Cisco ISE 中添加 MDM 服务器

步骤 5 点击“添加”(ADD)，然后输入 MDM 服务器详细信息。

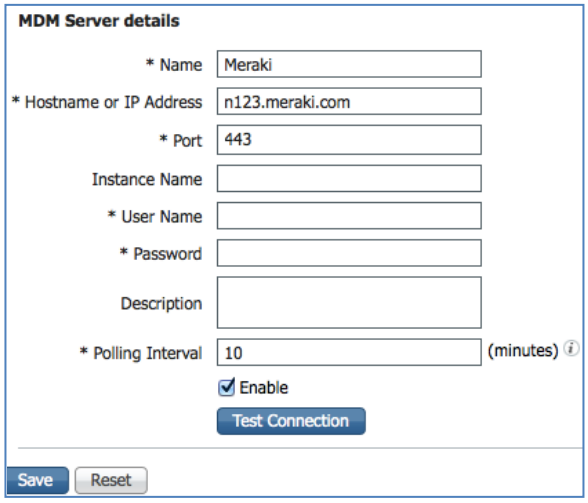


图 7. 在 Cisco ISE 中添加 MDM 服务器

步骤 6 点击**测试连接 (Test Connection）**，ISE 将确认连接是否正常工作。

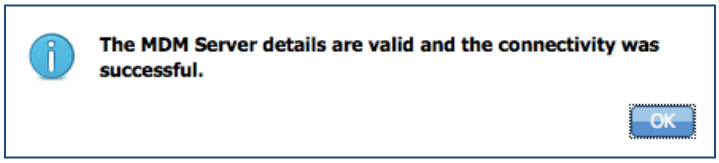


图 8. 在 Cisco ISE 中添加 MDM 服务器

步骤 7 在此弹出窗口上点击“确定”(OK)，然后选择复选框。 

步骤 8 点击“提交”(Submit) 按钮，服务器将成功添加 

，系统将向管理员显示以下成功消息。

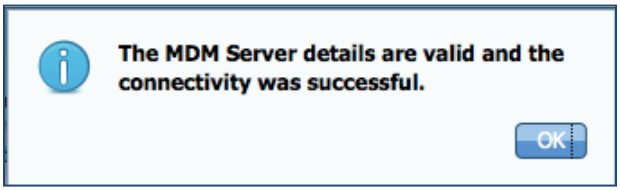


图 9. 在 Cisco ISE 中添加 MDM 服务器

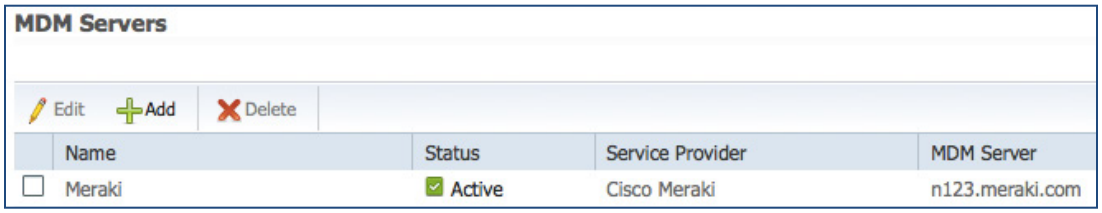


图 10. 已成功添加服务器

查看 MDM 字典

添加 MDM 服务器之后，ISE 中将随即显示支持的字典，稍后可以将这些字典用于 ISE 授权策略。

步骤 1 导航至：**策略 (Policy) -> 策略元素 (Policy Elements) -> 字典 (Dictionaries) -> 系统 (System) -> MDM -> 字典属性 (Dictionary Attribute)**

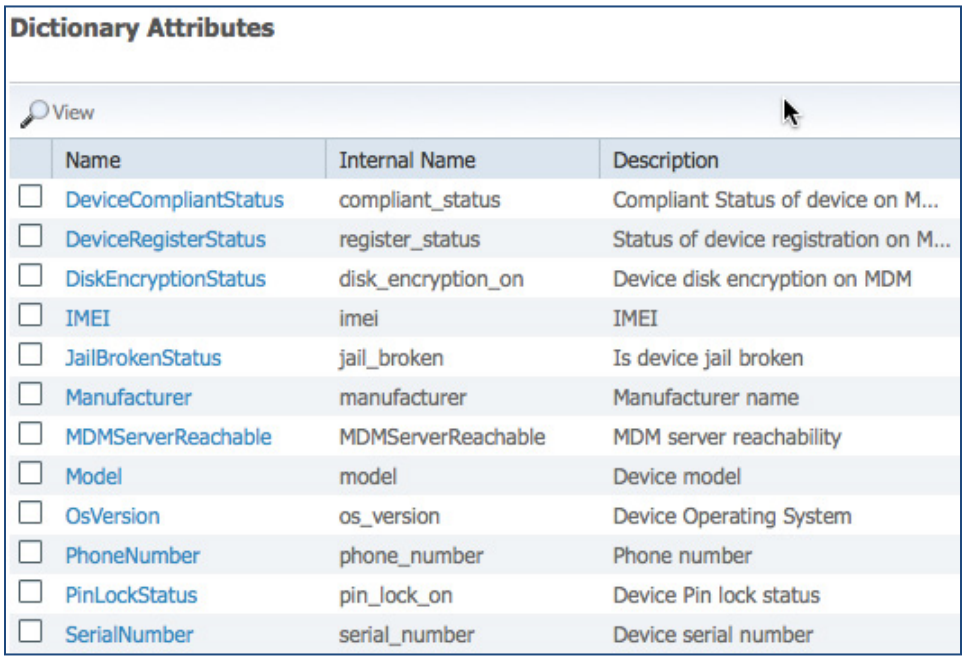


图 11. 查看 Cisco ISE 中的 MDM 字典

配置 ISE 授权策略

MDM 服务器添加到 ISE 中之后，我们就可以在 ISE 中配置授权策略，以利用为 MDM 服务器添加的新字典。

注意：在本文档中，我们演示了如何使用字典属性 **MDM:DeviceRegisterStatus EQUALS UnRegistered** 和 **MDM:DeviceCompliantStatus EQUALS NonCompliant**。另请配置并测试其他属性

步骤 2 在无线局域网控制器中创建一个稍后在策略中使用的名为“NSP-ACL”的 ACL，以重定向为自带设备请求方调配、证书调配和 MDM 隔离选择的客户端。

- 思科身份服务引擎的 IP 地址 = 10.35.50.165
- 公司内部网络 = 192.168.0.0，172.16.0.0（需重定向）
- MDM 服务器子网 = 204.8.168.0

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

图 12. 用于将客户端重定向至自带设备流程的访问控制列表

NSP-ACL 的说明

1. 允许从服务器到客户端的所有“出站”流量
2. 对于故障排除，允许从客户端到服务器的“入站”ICMP 流量，这是可选的
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
4. 允许从客户端到服务器再到 ISE 的所有“入站”流量以执行网络门户和请求方以及证书调配流程
5. 允许从客户端到服务器的“入站”DNS 流量以进行名称解析。
6. 允许从客户端到服务器的“入站”DHCP 流量以获取 IP 地址。
7. 拒绝从客户端到服务器再到用于重定向至 ISE 的企业资源的所有“入站”流量（根据企业策略）。
8. 拒绝从客户端到服务器再到用于重定向至 ISE 的企业资源的所有“入站”流量（根据企业策略）。
9. 拒绝从客户端到服务器再到用于重定向至 ISE 的企业资源的所有“入站”流量（根据企业策略）。
10. 拒绝从客户端到服务器再到用于重定向至 ISE 的企业资源的所有“入站”流量（根据企业策略）。
11. 拒绝从客户端到服务器再到用于重定向至 ISE 的企业资源的所有“入站”流量（根据企业策略）。
12. 拒绝从客户端到服务器再到用于重定向至 ISE 的企业资源的所有“入站”流量（根据企业策略）。
13. 允许其余所有流量（可选）

步骤 3 为不符合 MDM 策略的设备创建名称为“MDM_Quarantine”的授权配置文件。在这种情况下，所有不合规设备都将重定向至 ISE 并显示一条消息。

步骤 4 点击“策略”(Policy) **→策略元素 (Policy Elements) →结果 (Results)，点击授权 (Authorization) →授权配置文件 (Authorization Profiles) →添加 (ADD)。**

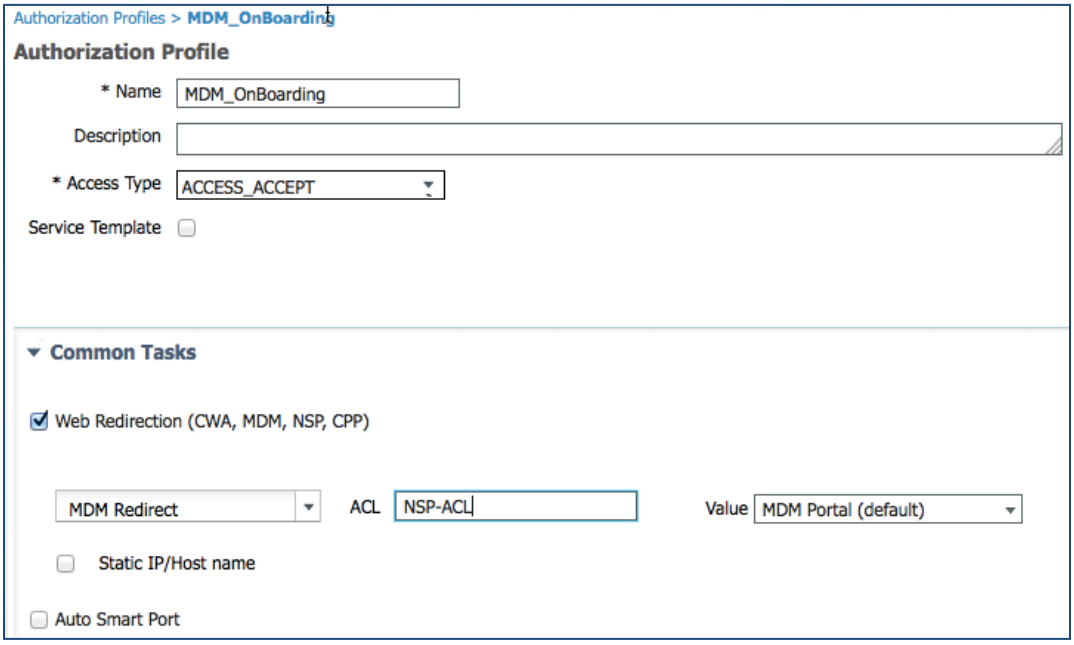


图 13. 授权策略配置

图 14. NSP-ACL

注：需要在无线 LAN 控制器上定义 NSP-ACL。

步骤 5 创建授权策略 (Authorization Policy)。点击“策略”(Policy)**→授权 (Authorization) →授权配置文件 (Authorization Profiles)。**点击**“在下方插入新规则”(Insert New Rule Below)**。

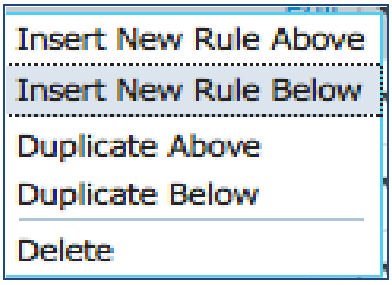


图 15. 插入新规则 (Insert New Rule)

请添加以下授权策略

MDM_OnBoarding = 为尚未向 Cisco Meraki EMM 云注册的设备添加此授权规则。一旦设备符合此规则，则将被转发到 ISE EMM 登录页面，此页面将向用户显示有关向 Cisco Meraki EMM 云注册设备的信息。您将需要为最终用户提供 Cisco Meraki 网络 ID（在“Meraki 控制面板”(Meraki Dashboard) 中在 MDM > “添加设备”(Add devices) 上可提供）：

图 13：在 ISE 中为 Meraki 网络 ID 配置 EMM 门户

图 16. 在 ISE 中为 Meraki 网络 ID 配置 EMM 门户

MDM_OnBoarded = 一旦设备已向 ISE、MDM 注册并且符合 ISE 和 MDM 策略，其将被授予网络访问权限。

默认 (Default) = 如果设备不符合上述策略，例如未向 MDM 注册或不符合 MDM，则符合默认拒绝规则

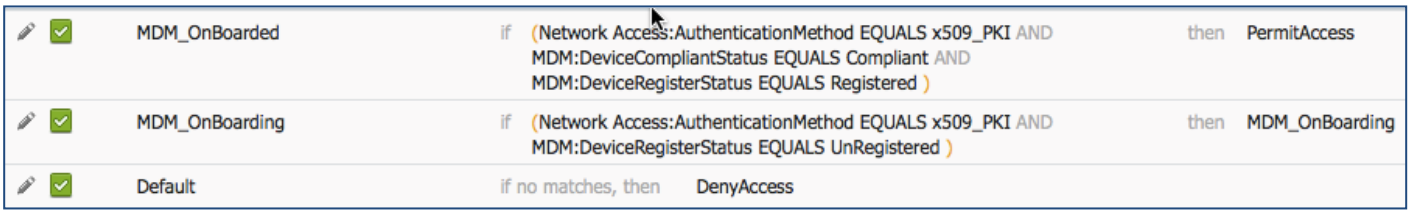
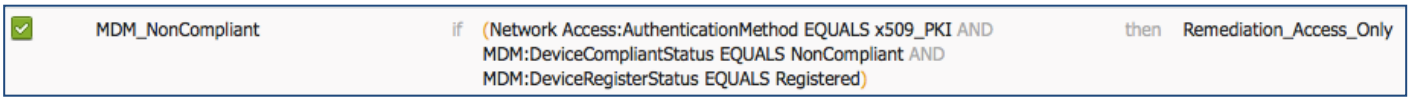


图 17. 授权策略配置视图

您已完成！

注：（可选）您可以添加其他规则，允许对已向 MDM 注册但不合规的设备进行有限访问，例如仅限补救的访问。



有关调配证书以及请求方配置文件的详细信息，请参阅操作指南：**使用差异化访问证书的自带设备**。

注意：也可以在 Cisco ISE 上更详细具体地定义 MDM 策略，例如

演示

如要查看有关自注册 i 设备、Android、Windows 和 MAC OSx 的最终用户体验，请访问以下网站：

http://wwwin.cisco.com/tech/snsbu/prod-sols/ise/#sectionName=4

附录 A： Meraki EMM 配置

在本节我们将回顾一下如何为公司策略配置 Cisco Meraki EMM 云。有关特定于使用案例和您的公司策略的配置，请参阅 Cisco Meraki 文档。本节仅突出介绍实现设置和运行所需完成的简单配置。

本节重点如下：

- 确认必须从 Cisco Meraki EMM 云获取并在 ISE 服务器上配置的 ISE 设置。
- 配置要向终端推送的应用。

步骤 1 访问 Cisco Meraki 管理 Web 界面。

a. 在**管理员** PC 上，启动任意 Web 浏览器。在地址栏中输入 Cisco Meraki URL：

https://dashboard.meraki.com

注意：此处列出的是一个示例 URL。

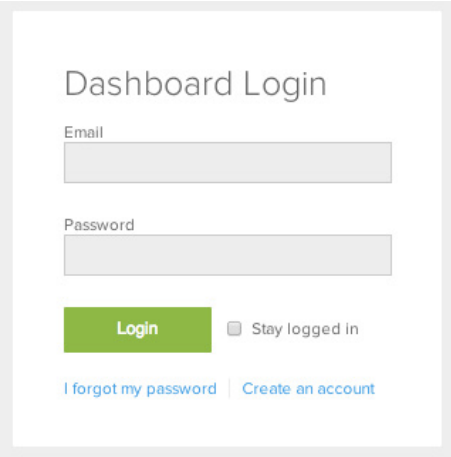


图 18. 登录面板

b. 使用用户名和密码登录。您登录之后，请导航至您的系统管理器网络。

步骤 2 ISE 设置

a. 导航至**组织 (Organization) > MDM 页面。**从那里记下“ISE 设置”(ISE settings) URL、用户名和密码；必须在您的 ISE 服务器上配置这些设置（请参阅上一节中的步骤 4）。

图 19. ISE 设置

步骤 3 Cisco Meraki 服务器上的安全策略。

a. 导航至“配置”(Configure) > “策略”(Policies) 页面。此处，您可以创建和配置安全策略（例如屏幕锁定、磁盘加密、运行列入黑名单的应用等）。

b. 导航至**配置 (Configure) >常规 (General) → ISE 设置 (ISE settings)**。您可以分配向 ISE 报告哪些策略。

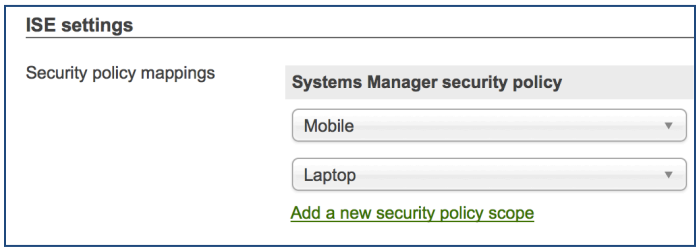


图 20. ISE 设置

在 Meraki 上配置应用

在本节中，我们将为 Cisco AnyConnect 等企业应用配置 Cisco Meraki EMM 云。然后我们将配置随 AnyConnect 应用一起推送的 VPN 配置文件，从而使设备可以在公司外部安全地访问公司数据和应用（通过 VPN）。登录到“Meraki 配置”(Meraki Configuration) 界面后，配置应用。

a. 导航至 **MDM >应用 (Apps)**页面。

b. 在屏幕右侧，点击**新增 (Add New)**图标。

c. 选择 **iOS** 应用。

d. 在搜索框中输入 **AnyConnect**。

e. 点击**添加 (ADD)** 和“保存更改”(Save Changes)。

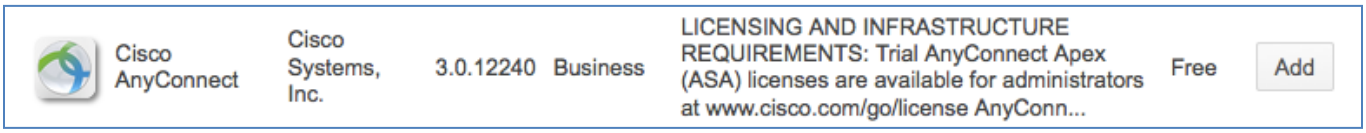


图 21. Cisco AnyConnect

步骤 4 配置 VPN 配置文件。

步骤 5 导航至 **MDM > 设置 (Settings) > VPN 页面 (VPN page)**。

步骤 6 点击“配置 VPN 网络”(Configure a VPN network)。

步骤 7 在 **VPN 服务器地址 (VPN Server address)** 中输入 VPN 服务器地址，作为示例；以下是连接 vpn.cisco.com 的配置。

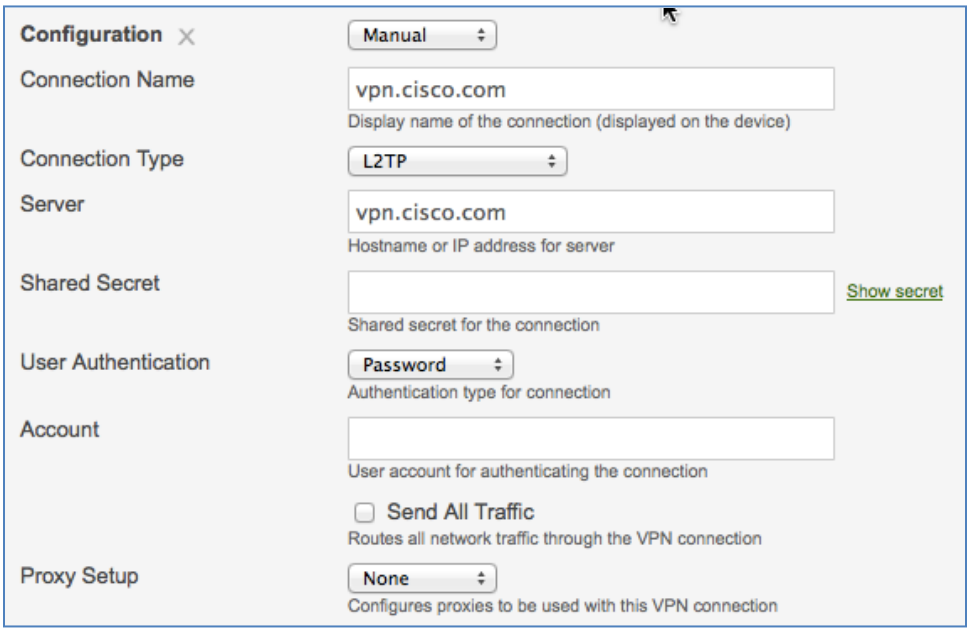


图 22. 示例配置

附录B：Cisco ASA 示例配置

这是 ASA 服务器的示例配置，其中 Meraki MDM 调配的设备应用**Cisco AnyConnect**可以重新连接以建立 VPN 连接。

此设置中使用的 ASA 版本 = ASA 版本 9.3(1)
硬件：ASA5515、8192 MB RAM、CPU Clarkdale 3059 MHz、1 CPU（4 核）

外部接口的 IP 配置、DNS 和 ISE 策略服务节点都已更改，请替换为网络中的 ASA 和 ISE IP 地址。

外部接口 IP 地址 = 1.1.1.100
默认网关 IP 地址 = 1.1.1.1
ISE PSN 节点的 IP 地址 = 2.2.2.2
DNS 服务器的 IP 地址 = 10.10.10.10

```
ASA Version 9.3(1)
!
terminal width 511
hostname VPN
domain-name test.ocm
names
ip local pool user-dhcp-pool 10.42.36.10-10.42.36.254 mask 255.255.254.0
!
interface GigabitEthernet0/0
 speed 1000
 duplex full
 nameif outside
 security-level 0
 ip address 1.1.1.100 255.255.255.248 standby 1.1.1.101
!
interface GigabitEthernet0/1
 speed 1000
 duplex full
 nameif inside
 security-level 100
 ip address 10.42.20.148 255.255.255.248 standby 10.42.20.149
!
!
boot system disk0:/asa931-smp-k8.bin
ftp mode passive
clock timezone PST8PDT -8
clock summer-time PDT recurring10.10.10.10
dns domain-lookup inside
dns server-group DefaultDNS
 name-server 10.10.10.10
domain-name test.ocm
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
object network ocsp.quovadisglobal.com
 fqdn ocsp.quovadisglobal.com
object-group protocol TCPUDP
 protocol-object udp
 protocol-object tcp
access-list pre-posture remark exclude DNS server
access-list pre-posture extended deny ip any host 10.10.10.10
access-list pre-posture extended permit tcp any host 2.2.2.2 eq www
access-list pre-posture remark exclude ISE PSN Servers
access-list pre-posture extended deny ip any host 2.2.2.2
access-list pre-posture remark Permit ALL Traffic
access-list pre-posture extended permit ip any any
access-list pre-posture extended permit ip any object ocsp.quovadisglobal.com log
access-list test extended permit icmp any any
access-list 101 extended permit icmp any any
access-list test101 extended permit ip any4 any4
pager lines 24
mtu outside 1500
mtu inside 1500
icmp unreachable rate-limit 1 burst-size 1
```

```
icmp permit any outside
asdm image disk0:/asdm-731-101.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
route outside 0.0.0.0 0.0.0.0 1.1.1.1 1
route inside 10.19.151.208 255.255.255.240 1.1.1.103 1
route inside 0.0.0.0 0.0.0.0 1.1.1.103 tunneled
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
aaa-server RADIUS-SERVERS protocol radius
accounting-mode simultaneous
 interim-accounting-update
 max-failed-attempts 5
 merge-dacl before-avpair
 dynamic-authorization
aaa-server RADIUS-SERVERS (inside) host 2.2.2.2
 timeout 21
 key *****
 authentication-port 1812
 accounting-port 1813
 radius
-common-pw *****
 acl-netmask-convert auto-detect
acl-netmask-convert auto-detect
aaa-server OTP protocol radius
aaa-server OTP (inside) host 10.35.48.251
 key *****
aaa-server OTP_ETE protocol radius
aaa-server OTP_ETE (inside) host 10.35.50.200
key *****
 radius-common-pw *****
user-identity default-domain LOCAL
aaa authentication http console LOCAL
aaa authentication ssh console MGMT-RBAC LOCAL
http server enable 8443
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
service resetoutside
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec ikev2 ipsec-proposal ESP
 protocol esp encryption aes-gcm-256 aes-gcm-192
 protocol esp integrity sha-256 sha-1
crypto ipsec ikev2 ipsec-proposal AES256
 protocol esp encryption aes-256
protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES192
 protocol esp encryption aes-192
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES
 protocol esp encryption aes
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal 3DES
protocol esp encryption 3des
```

```
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal DES
protocol esp encryption des
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal SAMPG-IKE
 protocol esp encryption aes-256 aes-192 3des
 protocol esp integrity sha-256 sha-1
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map REMOTE-ACCESS 10 set pfs group5
crypto dynamic-map REMOTE-ACCESS 10 set ikev1 transform-set ESP-AES-256-SHA
crypto dynamic-map REMOTE-ACCESS 10 set ikev2 ipsec-proposal AES256 AES192 AES 3DES DES
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set pfs group5
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev1 transform-set ESP-AES-128-SHA ESP-
AES-128-MD5 ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5 ESP-3DES-SHA ESP-3DES-
MD5 ESP-DES-SHA ESP-DES-MD5
crypto dynamic-map SYSTEM_DEFAULT_CRYPTO_MAP 65535 set ikev2 ipsec-proposal AES256 AES192 AES 3DES
DES
crypto map RA-IPSEC-VPN 10 ipsec-isakmp dynamic REMOTE-ACCESS
crypto map RA-IPSEC-VPN interface outside
crypto map inside_map 65535 ipsec-isakmp dynamic SYSTEM_DEFAULT_CRYPTO_MAP
crypto map inside_map interface inside
crypto ca trustpoint ciscoca
 enrollment terminal
 subject-name CN=vpn.test.ocm
 keypair sslvpnkeypair
 crl configure
subject-name CN=10.35.91.252,CN=vpn
 crl configure
crypto ca trustpoint ASDM_TrustPoint0
 enrollment terminal
 fqdn vpn.test.ocm
 subject-name CN=vpn.test.ocm,OU=ISE,O=Cisco,C=US
 crl configure
crypto ca trustpoint ASDM_TrustPoint1
 enrollment terminal
 fqdn vpn.test.ocm
 subject-name CN=vpn.test.ocm,OU=ISE,O=Cisco,C=US
 keypair sslvpnkeypair
 crl configure
crypto ca trustpoint ASDM_Launcher_Access_TrustPoint_23
 enrollment self
 subject-name CN=10.35.91.252,CN=vpn
crl configure
crypto ca trustpoint ASDM_Launcher_Access_TrustPoint_24
 enrollment self
 subject-name CN=10.35.91.252,CN=vpn
crl configure
crl configure
crypto ca trustpool policy
crypto ca certificate chain ciscoca

crypto ikev2 policy 1
 encryption aes-256 aes-192 aes 3des
 integrity sha256 sha md5
group 14 5 2 1
 prf sha256 sha
 lifetime seconds 86400
crypto ikev2 remote-access trustpoint ciscoca
crypto ikev1 enable outside
crypto ikev1 enable inside
crypto ikev1 policy 1
 authentication pre-share
 encryption aes-256
 hash sha
 group 5
 lifetime 86400
crypto ikev1 policy 2
 authentication pre-share
 encryption aes-192
 hash sha
```

```
 group 5
lifetime 86400
crypto ikev1 policy 3
 authentication pre-share
 encryption 3des
 hash sha
 group 5
 lifetime 86400
crypto ikev1 policy 10
 authentication crack
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 20
authentication rsa-sig
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 30
 authentication pre-share
encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 40
 authentication crack
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 50
 authentication rsa-sig
 encryption aes-192
 hash sha
group 2
 lifetime 86400
crypto ikev1 policy 60
 authentication pre-share
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 70
authentication crack
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 80
 authentication rsa-sig
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 90
 authentication pre-share
 encryption aes
hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 100
authentication crack
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 110
 authentication rsa-sig
```

```
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 120
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 130
 authentication crack
 encryption des
hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 140
 authentication rsa-sig
 encryption des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 150
 authentication pre-share
 encryption des
 hash sha
 group 2
 lifetime 86400
telnet timeout 5
no ssh stricthostkeycheck
ssh 0.0.0.0 0.0.0.0 inside
ssh timeout 30
ssh key-exchange group dh-group1-sha1
console timeout 0
management-access inside
!
tls-proxy maximum-session 200
!
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ntp server 171.68.38.65 source inside prefer
ntp server 10.81.254.202 source inside
ssl encryption rc4-sha1 aes128-sha1 aes256-sha1 3des-sha1
ssl trust-point ciscoca outside
ssl trust-point ASDM_Launcher_Access_TrustPoint_28 inside
ssl trust-point ASDM_Launcher_Access_TrustPoint_28 inside vpnlb-ip

group-policy DfltGrpPolicy attributes
 dns-server value 10.10.10.10
 vpn-idle-timeout 1440
 vpn-session-timeout 28800
 vpn-tunnel-protocol ikev1 ikev2 l2tp-ipsec ssl-client
 ipsec-udp enable
 default-domain value test.ocm
 webvpn
  anyconnect ssl rekey time 300
  anyconnect ssl rekey method ssl
  anyconnect profiles value vpnlisting type user
group-policy CISCOVPN internal
group-policy CISCOVPN attributes
dns-server value 10.10.10.10
 dhcp-network-scope none
 vpn-access-hours none
 vpn-simultaneous-logins 2
 vpn-idle-timeout 1440
 vpn-session-timeout none
 vpn-filter none
 vpn-tunnel-protocol ikev1 ikev2 ssl-client
 password-storage disable
```

```
 ip-comp disable
 re-xauth disable
 group-lock none
 pfs disable
 ipsec-udp-port 10000
 split-tunnel-policy tunnelall
 split-tunnel-network-list none
 default-domain value test.ocm
 backup-servers keep-client-config
 webvpn
  anyconnect ssl rekey method ssl
  anyconnect modules value dart,iseposture
  anyconnect profiles value vpnlisting type user
dynamic-access-policy-record DfltAccessPolicy
username sampg password n4q2SM5y13X3ysFc encrypted privilege 15
username admin password ezv7202P8kRjcMXI encrypted privilege 15
tunnel-group npf-sjvpn type remote-access
tunnel-group npf-sjvpn general-attributes
 address-pool user-dhcp-pool
 authentication-server-group RADIUS-SERVERS
 accounting-server-group RADIUS-SERVERS
 default-group-policy CISCOVPN
tunnel-group npf-sjvpn webvpn-attributes
 group-alias SAMPG-IPSEC-VPN disable
group-alias SAMPG-SSL-VPN enable
tunnel-group npf-sjvpn ipsec-attributes
 ikev1 pre-shared-key *****
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
inspect h323 h225
  inspect h323 ras
inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
  inspect icmp
!
service-policy global_policy interface outside
prompt hostname priority state
no call-home reporting anonymous
Cryptochecksum:f75d25311e04e6a83e7e2b0b4d5ce1b1
: end
```

附录 C：参考

Cisco TrustSec 系统：

http://www.cisco.com/go/trustsec

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

设备配置指南：

思科身份服务引擎用户指南：
http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

有关 Cisco IOS 软件、Cisco IOS XE 软件和 Cisco NX-OS 软件版本的更多信息，请参阅以下 URL：

对于 Cisco Catalyst 2900 系列交换机：
http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html

对于 Cisco Catalyst 3000 系列交换机：
http://www.cisco.com/en/US/products/ps7077/products_installation_and_configuration_guides_list.html

对于 Cisco Catalyst 3000-X 系列交换机：
http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html

对于 Cisco Catalyst 4500 系列交换机：
http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html

对于 Cisco Catalyst 6500 系列交换机：
http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html

对于 Cisco ASR 1000 系列路由器：
http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html

对于思科无线局域网控制器：
http://www.cisco.com/en/US/docs/wireless/controller/7.2/configuration/guide/cg.html