

# Airwatch 与思科身份服务引擎集成

*安全访问操作指南系列*

作者: Aaron Woland

日期: 2012 年 12 月

# 目录

- 简介 ..... 3
  - 什么是 Cisco TrustSec 系统? ..... 3
  - 关于 TrustSec 操作指南 ..... 3
- 移动设备管理 (MDM) ..... 4
  - 概述 ..... 4
    - MDM 集成使用案例 ..... 4
  - 组件 ..... 5
- 使用 MDM 集成配置步骤 ..... 7
  - 思科 ISE 和 MDM 集成配置 ..... 7
  - 审核 MDM 字典 ..... 11
  - 配置 ISE 授权策略 ..... 12
- 附录 A: Airwatch 配置 ..... 17
- 附录 B: 参考 ..... 19
  - Cisco TrustSec 系统: ..... 19
  - 设备配置指南: ..... 19

# 简介

## 什么是 Cisco TrustSec 系统？

Cisco TrustSec® 是思科 SecureX 架构™ 的核心组件，是一种智能访问控制解决方案。TrustSec 提供对连接整个网络基础设施的用户和设备的全面可视性功能，并对用户和设备能够访问的内容和位置实现卓越控制，从而降低安全风险。

TrustSec 构建于您现有的身份感知接入层基础设施（交换机、无线控制器等）之上。该解决方案及其内部所有组件已作为一个集成系统经过了彻底检查和严格测试。

TrustSec 系统不仅结合了 IEEE 802.1X 与 VLAN 控制等基于标准的身份和实施方式，还包括高级身份和实施方式，如灵活身份验证、可下载访问控制列表 (dACL)、安全组标记 (SGT)、设备分析、安全状态评估等。

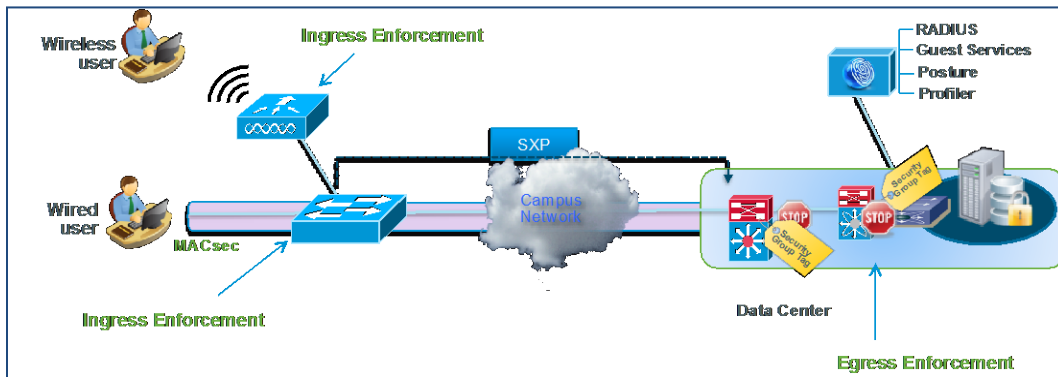


图 1.

## 关于 TrustSec 操作指南

本系列操作指南文档由 TrustSec 团队编制，旨在介绍 TrustSec 部署的最佳实践。本系列文档相辅相成，引导读者成功实施 TrustSec 系统。您可以使用这些文档按照规定的路径完成部署，也可以只选择满足您特定需求的单独的使用案例。

## 移动设备管理 (MDM)

### 概述

移动设备管理 (MDM) 软件保护、监控、管理和支持跨移动运营商、运营商和企业部署的移动设备。典型 MDM 产品包括策略服务器、移动设备客户端和可选内联实施点，该可选内联实施点控制部署环境中移动设备上的某些应用的使用（如邮件）。但是，网络是可以提供终端精细访问的唯一实体（基于 ACL、TrustSec SGT 等）。根据设想，思科身份服务引擎 (ISE) 是一个基于附加网络的实施点，而 MDM 策略服务器则用作策略决策点。ISE 预期接收来自 MDM 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高级使用案例。

- **设备注册** - 访问网络内部的未注册终端将被重定向到 MDM 服务器的注册页面，以根据用户角色、设备类型等进行注册。
- **补救** - 不合规终端将根据合规状态授予受限访问权限。
- **定期合规检查** - 定期向 MDM 服务器检查合规性。
- **ISE 中的管理员通过 MDM 服务器在设备上发出远程操作的能力**（例如远程擦除受管设备）。
- **最终用户利用 ISE My Devices Portal 管理个人设备的能力**，例如完全擦除、公司擦除和 PIN 锁。

### 网络拓扑示例

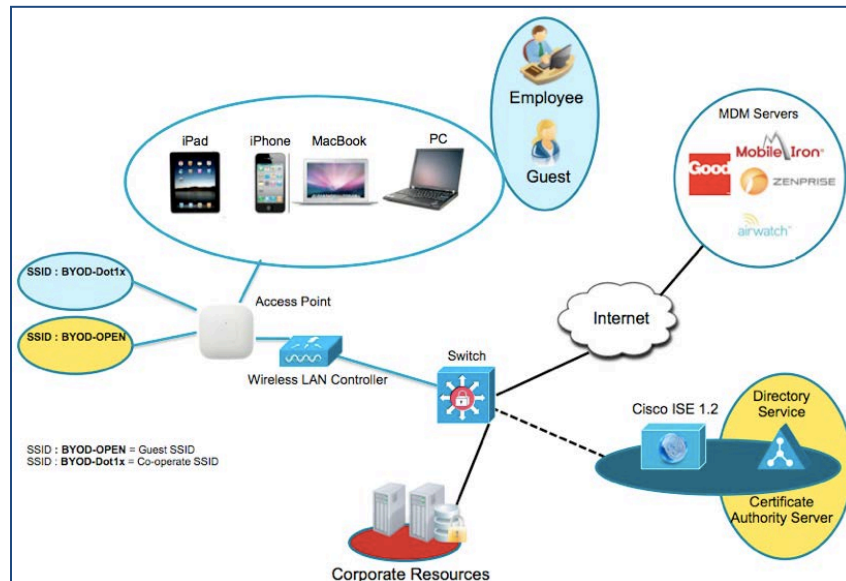


图 2. ISE+MDM 集成拓扑

### MDM 集成使用案例

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注册流程，详细信息如附录所述。
3. ISE 向 MDM 服务器发出 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，我们能够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 MDM 提供商注册。ISE 会向 NAD 发送授权以重定向至 ISE，该 ISE 将把用户重定向至 MDM 服务器（主页或登录页）。
6. ISE 得知该设备需要使用 MDM 进行配置，并将向用户显示适当的页面以执行注册。
7. 用户将被转到 MDM 策略引擎，用户将在此处完成注册。通过 MDM 服务器的自动重定向或通过用户再次刷新浏览器，控制权将交回给 ISE。
8. ISE 将再次查询 MDM，获取安全状态信息。
9. 如果用户设备不符合 MDM 中配置的安全状态（合规性）策略，系统将通知他们设备不合规、不合规的原因以及需要合规才能访问网络资源。
10. 一旦用户设备合规，MDM 服务器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 MDM 服务器获取合规信息，并相应地发出 COA。

## 组件

表 1. 本文中使用的组件

组件	硬件	经过测试的特性	Cisco IOS® 软件版本
思科身份服务引擎 (ISE)	任意：1121/3315、3355、3395、VMWare	集成 AAA、策略服务器和服务（访客、分析器和安全状况）	ISE 1.2
MDM 服务器	MDM		
证书授权服务器（可选）	任意，根据 Microsoft 的规格 (Windows 2008 R2 Enterprise SP2)	SCEP，证书授权服务器	不适用
无线 LAN 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.???
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

在本文档中，我们仅展示了 MDM 配置。我们建议您使用我们的操作指南将 ISE 和 WLC 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](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](http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html)

# 使用 MDM 集成配置步骤

## 思科 ISE 和 MDM 集成配置

图 3 显示了配置 MDM 集成的主要步骤。

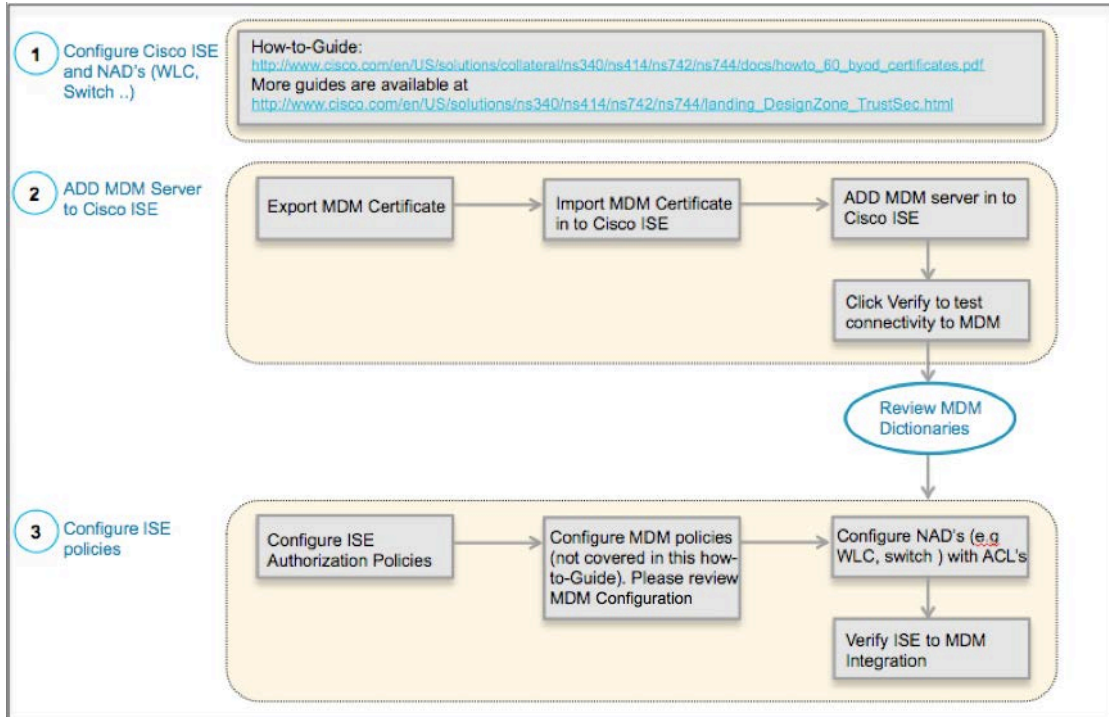


图 3. MDM 配置流程

### 将外部 MDM 服务器添加至 ISE

MDM 服务器可用做云服务或本地内部安装。一旦在 MDM 服务器上配置了安装、基本设置和合规检查，即可将其添加至 ISE。

### 导出 MDM 服务器证书

**步骤 1** 导出 MDM 服务器证书并将其保存在本地计算机上。如果使用的是 FireFox，请访问 Airwatch 服务器，然后单击地址栏中的锁图标，再点击 More Information。



图 4. 导出 MDM 证书

**步骤 2** 点击 View Certificate -> Detail -> Export -> Save，将证书保存至任意所需位置。

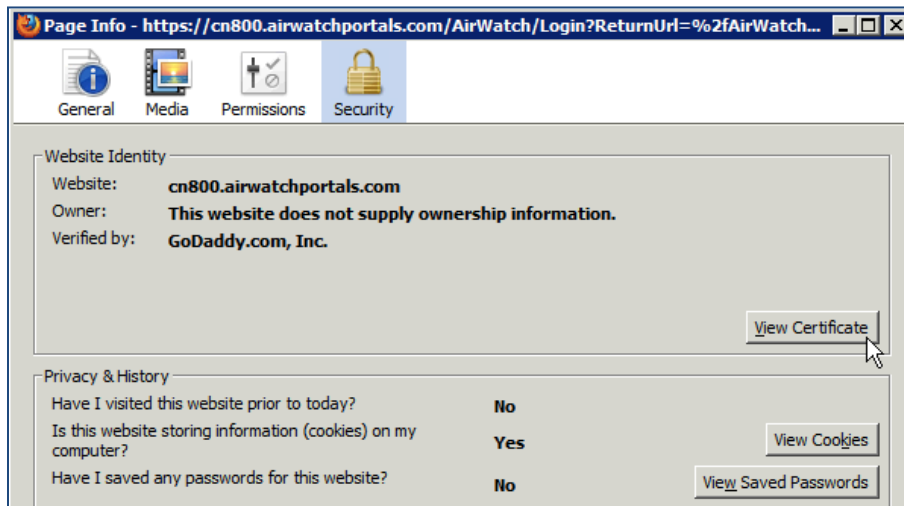


图 5. 将 MDM 证书导入思科 ISE



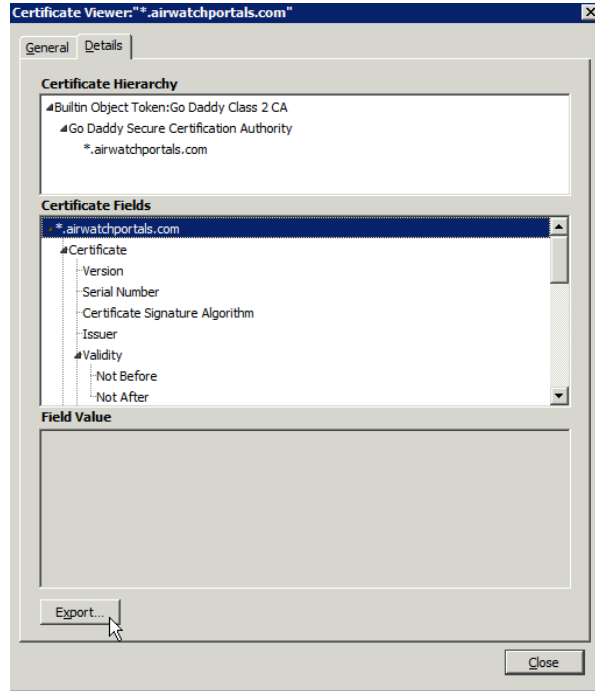


图 6.

步骤 3 将证书导入 ISE。

步骤 4 导航至 **Administration -> Certificates -> Certificate Store -> Import**。

可选：添加一个容易记住的名称，然后点击 Submit。

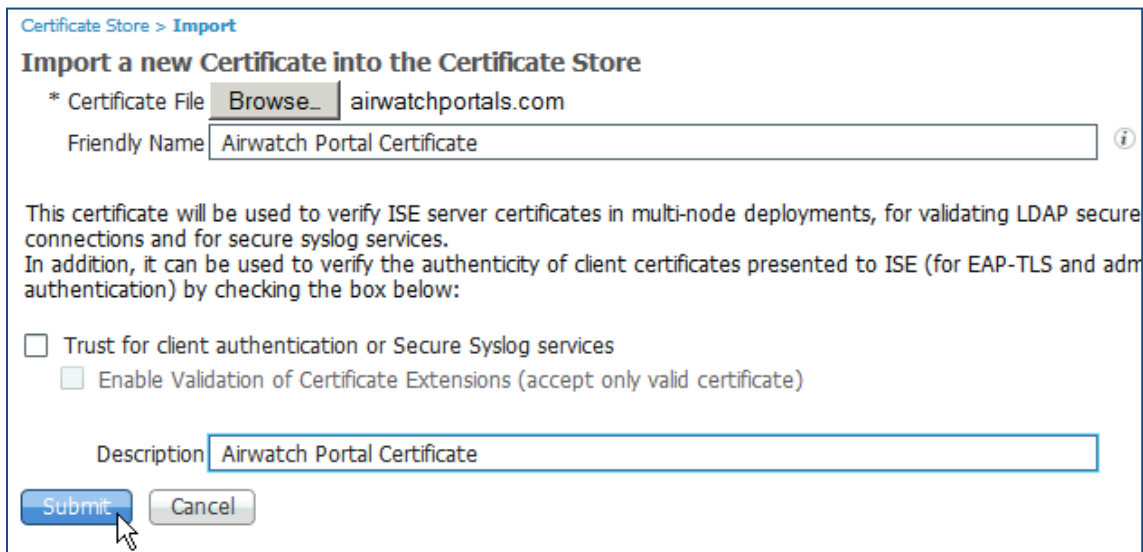


图 7. 验证思科 ISE 中的 MDM 证书

步骤 5 验证该证书已进入 Certificate Store。

Certificate Store				
Selected 0   Total 9				
<span>Edit</span> <span>Import</span> <span>Change Status</span> <span>Export</span> <span>Delete</span> <span>Show</span> All				
<input type="checkbox"/>	Status	Friendly Name	Trust For Client Auth	Issued To
<input type="checkbox"/>	Enabled	Airwatch Portal Certificate	⊖	*.airwatchportals.com
<input type="checkbox"/>	Enabled	Baltimore CyberTrust Root#Baltimore CyberTrust R...	⊖	Baltimore CyberTrust R...
<input type="checkbox"/>	Disabled	Cisco CA Manufacturing	⊖	Cisco Manufacturing C...
<input type="checkbox"/>	Disabled	Cisco Root CA 2048	⊖	Cisco Root CA 2048

图 8.

步骤 6 添加 MDM 服务器。Administration -> MDM。

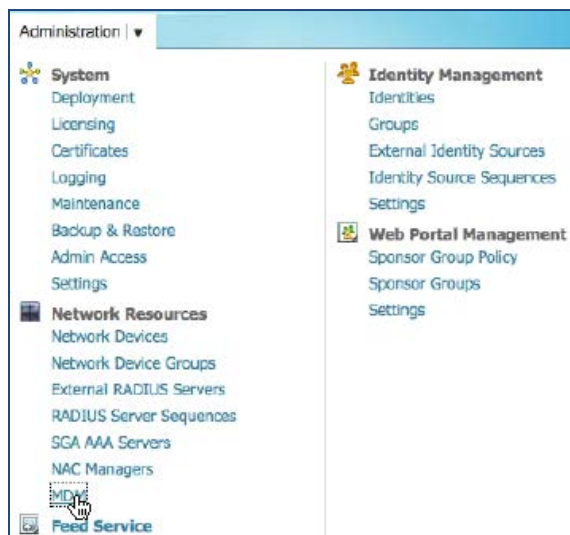


图 9. 在思科 ISE 中添加 MDM 服务器

步骤 7 点击 ADD，然后输入 MDM 服务器详细信息。

MDM Server details	
* Name	<input type="text" value="Airwatch_MDM"/>
* Hostname or IP Address	<input type="text" value="cn800.airwatchportals.com"/>
* Port	<input type="text" value="443"/>
Instance Name	<input type="text"/>
* User Name	<input type="text" value="ISE_API"/>
* Password	<input type="password" value="••••••"/>
Description	<input type="text"/>
* Polling Interval	<input type="text" value="240"/> (minutes) ⓘ
	<input type="checkbox"/> Enable
	<input type="button" value="Test Connection"/>

图 10. 在思科 ISE 中添加 MDM 服务器

步骤 8 点击 **Test Connection**，ISE 将确认连接有效。

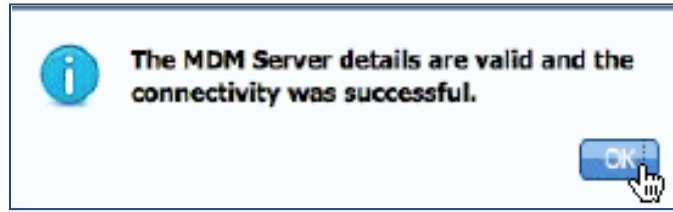


图 11. 在思科 ISE 中添加 MDM 服务器

步骤 9 在此弹出窗口上点击 OK，然后选择复选框。  **Enable**

步骤 10 点击 **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。

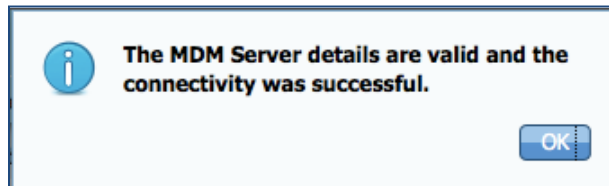


图 12. 在思科 ISE 中添加 MDM 服务器




MDM Servers					
				Show	All
 Edit	 Add	 Delete			
Name	Status	Service Provider	MDM Server	Description	
<input type="checkbox"/> Airwatch_MDM	<input checked="" type="checkbox"/> Active	AirWatch, LLC	cn800.airwatchportals.com		

图 13. Airwatch 服务器添加成功

## 审核 MDM 字典

一旦 MDM 服务器添加成功，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：**Policy -> Policy Elements -> Dictionaries -> MDM -> Dictionary Attribute**。

**Dictionary Management**

Dictionary > **MDM**

Dictionary **Dictionary Attributes**

**Dictionary Attributes**

 View

	Name	Internal Name	Description
<input type="checkbox"/>	DeviceCompliantStatus	compliant_status	Compliant Status of device on MDM
<input type="checkbox"/>	DeviceRegisterStatus	register_status	Status of device registration on MDM
<input type="checkbox"/>	DiskEncryptionStatus	disk_encryption_on	Device disk encryption on MDM
<input type="checkbox"/>	IMEI	imei	IMEI
<input type="checkbox"/>	JailBrokenStatus	jail_broken	Is device jail broken
<input type="checkbox"/>	Manufacturer	manufacturer	Manufacturer name
<input type="checkbox"/>	OsVersion	os_version	OS version
<input type="checkbox"/>	PhoneNumber	phone_number	Phone number
<input type="checkbox"/>	PinLockStatus	pin_lock_on	Device Pin lock status
<input type="checkbox"/>	SerialNumber	serial_number	Device serial number

图 14. 审核思科 ISE 中的 MDM 字典

## 配置 ISE 授权策略

一旦 MDM 服务器被添加到 ISE 中，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：**在本文档中，我们展示了使用字典属性 **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 LAN 控制器中创建一个名为“NSP-ACL”的 ACL，以便稍后在策略中使用，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 IP 地址 = 10.35.50.165
- 公司内部网络 = 192.168.0.0、172.16.0.0（用于重定向）
- 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		
<a href="#">1</a>	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	150720	<input checked="" type="checkbox"/>	
<a href="#">2</a>	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Inbound	7227	<input checked="" type="checkbox"/>	
<a href="#">3</a>	Permit	0.0.0.0 / 0.0.0.0	204.8.168.0 / 255.255.255.0	Any	Any	Any	Any	Any	17626	<input checked="" type="checkbox"/>	
<a href="#">4</a>	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	7505	<input checked="" type="checkbox"/>	
<a href="#">5</a>	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	2864	<input checked="" type="checkbox"/>	
<a href="#">6</a>	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DHCP Server	Any	Inbound	0	<input checked="" type="checkbox"/>	
<a href="#">7</a>	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0	<input checked="" type="checkbox"/>	
<a href="#">8</a>	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	4	<input checked="" type="checkbox"/>	
<a href="#">9</a>	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	457	<input checked="" type="checkbox"/>	
<a href="#">10</a>	Deny	0.0.0.0 / 0.0.0.0	173.194.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	1256	<input checked="" type="checkbox"/>	
<a href="#">11</a>	Deny	0.0.0.0 / 0.0.0.0	171.68.0.0 / 255.252.0.0	Any	Any	Any	Any	Inbound	11310	<input checked="" type="checkbox"/>	
<a href="#">12</a>	Deny	0.0.0.0 / 0.0.0.0	171.71.181.0 / 255.255.255.0	Any	Any	Any	Any	Any	0	<input checked="" type="checkbox"/>	
<a href="#">13</a>	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	71819	<input checked="" type="checkbox"/>	

**图 15.** 用于将客户端重定向至自带设备流程的访问控制列表

图 13 中 NSP-ACL 的解释如下：

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. 允许访问适用于未注册和不合规设备的 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（根据公司策略）。
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（根据公司策略）。
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（根据公司策略）。

- 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（根据公司策略）。
- 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（根据公司策略）。
- 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（根据公司策略）。
- 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，所有不合规设备将重定向至 ISE 并显示一条消息。

**步骤 4** 点击 **Policy** → **Policy Elements** → **Results**，点击 **Authorization** → **Authorization Profiles** → **ADD**。

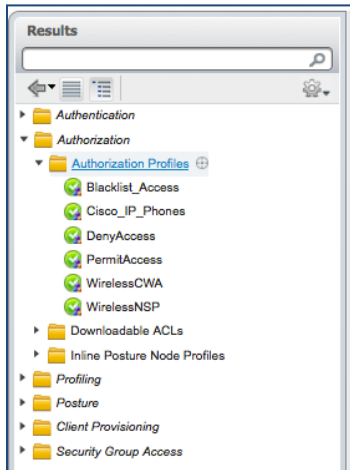


图 16. 授权配置文件导航

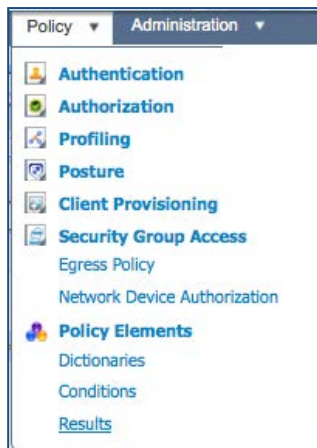
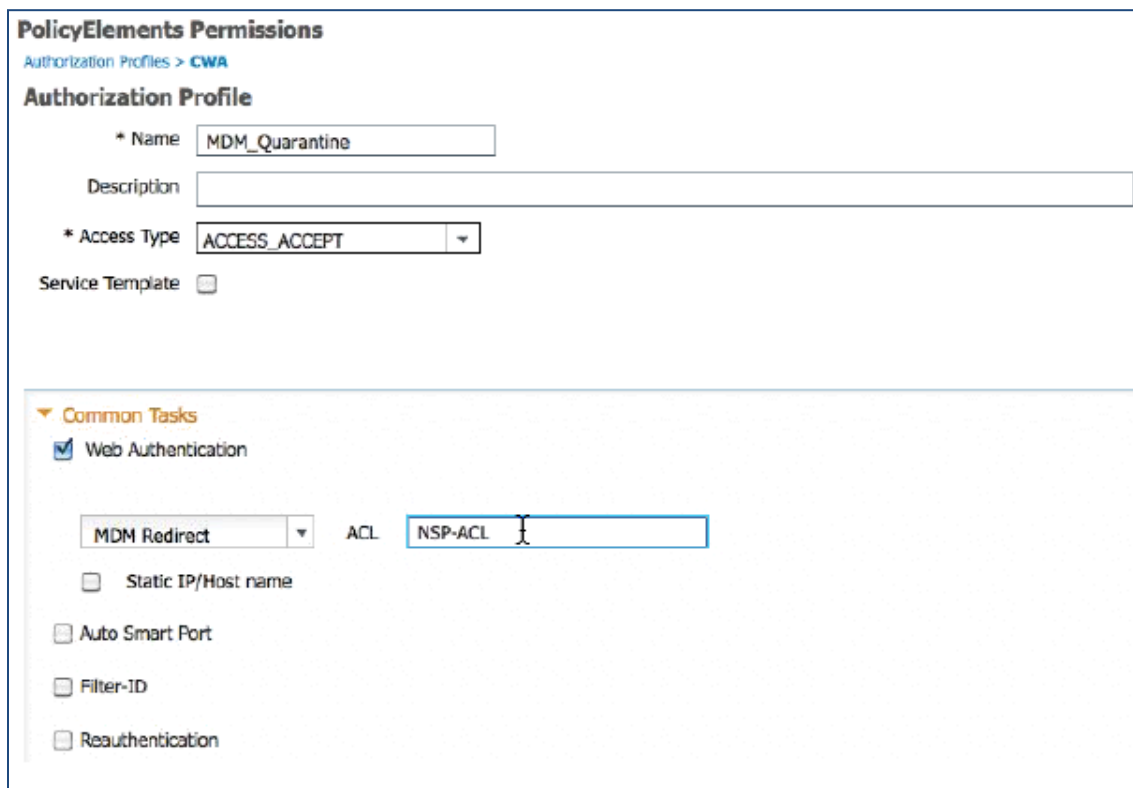


图 17. 授权策略配置



**PolicyElements Permissions**  
 Authorization Profiles > CWA

**Authorization Profile**

\* Name: MDM\_Quarantine

Description: [Empty]

\* Access Type: ACCESS\_ACCEPT

Service Template: [Empty]

**Common Tasks**

Web Authentication

MDM Redirect [Dropdown] ACL: NSP-ACL

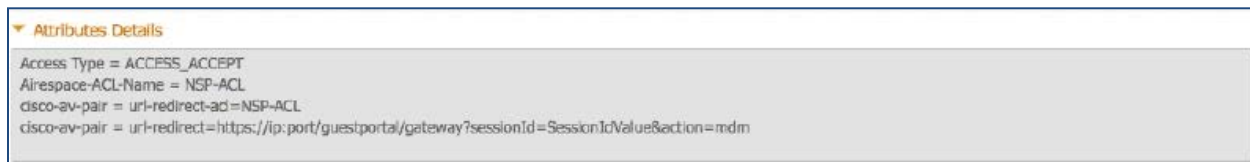
Static IP/Host name

Auto Smart Port

Filter-ID

Reauthentication

图 18. 授权策略配置



**Attributes Details**

Access Type = ACCESS\_ACCEPT  
 Airespace-ACL-Name = NSP-ACL  
 cisco-av-pair = url-redirect-ad=NSP-ACL  
 cisco-av-pair = url-redirect=https://ip:port/guestportal/gateway?sessionId=SessionIdValue&action=mdm

图 19. 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。点击 **Policy** → **Authorization** → **Authorization Profiles**。点击 **Insert New Rule Below**。



Insert New Rule Above

Insert New Rule Below

Duplicate Above

Duplicate Below

Delete

图 20. 插入新规则

### 请添加以下授权策略

**Registered with ISE NOT MDM** = 为已向 ISE 注册（已注册设备组）但尚未向 MDM 服务器注册的设备添加此授权规则。设备符合此规则后，将被转发到 ISE 上的 ISE MDM 登录页，此页面将向用户显示有关向 MDM 注册设备的信息。

**Registered with ISE AND MDM Non\_Compliant** = 为已向 ISE 和 MDM 服务器注册但是不符合 MDM 服务器上配置的策略的设备添加此授权规则。例如，在设备注册期间，一旦 Apple iPad 上的用户点击“Register”按钮，ISE 则将设备转至 APP，以下载 MDM 客户端并继续完成 MDM 注册流程。完成注册后，用户点击“Continue”按钮，然后 ISE 将向控制器发送重新授权 COA。

**Registered with ISE AND MDM Non\_Compliant** = 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。

<input checked="" type="checkbox"/>	Reg with ISE NOT MDM	if <b>RegisteredDevices AND (Wireless_802.1X AND Network Access:EapAuthentication EQUALS EAP-TLS AND CERTIFICATE:Subject Alternative Name EQUALS Radius:Calling-Station-ID AND MDM:DeviceRegisterStatus EQUALS UnRegistered )</b>	then MDM_Quarantine
<input checked="" type="checkbox"/>	Reg with ISE AND MDM non_compliant	if <b>RegisteredDevices AND (Wireless_802.1X AND Network Access:EapAuthentication EQUALS EAP-TLS AND CERTIFICATE:Subject Alternative Name EQUALS Radius:Calling-Station-ID AND MDM:DeviceCompliantStatus EQUALS NonCompliant )</b>	then MDM_Quarantine
<input checked="" type="checkbox"/>	Reg with ISE AND MDM comp	if <b>RegisteredDevices AND (Wireless_802.1X AND Network Access:EapAuthentication EQUALS EAP-TLS AND CERTIFICATE:Subject Alternative Name EQUALS Radius:Calling-Station-ID AND MDM:DeviceCompliantStatus EQUALS Compliant )</b>	then PermitAccess

图 21. 授权策略配置视图



您已完成！

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：**也可以在思科 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: Airwatch 配置

本节我们将回顾一下为企业策略配置 MobileIron 服务器。

本节重点如下：

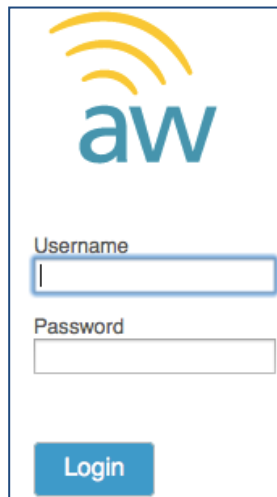
- 为 REST API 验证 **admin** 帐户权限，即 ISE 用于向 MobileIron 服务器发送 REST API 调用的帐户
- 审核默认安全策略
- 审核 iOS APP 安装配置 (AnyConnect)

**步骤 1** 访问 MobileIron 管理网络界面。

- a. 在**管理员 PC** 上，启动 Mozilla Firefox 网络浏览器。在地址栏中输入 MobileIron URL：

<https://mobileiron.demo.local/admin>

**注：**此处列出的 URL 仅为 URL 示例。



**图 22.** Asset Tracking 选项卡

- a. 使用用户名和密码登录。登录后，系统应显示 Asset Tracking 选项卡。

**步骤 2** 导航至 **Menu > Accounts > Administrators**。从这里，点击用户帐户（用于 API 访问），然后点击 **EDIT**。

**步骤 3** 点击 **Roles**，然后点击 **Add Role**。

**步骤 4** 选择 **REST API MDM**，命名 **Role**，添加 **Description**，然后点击 **Save**。

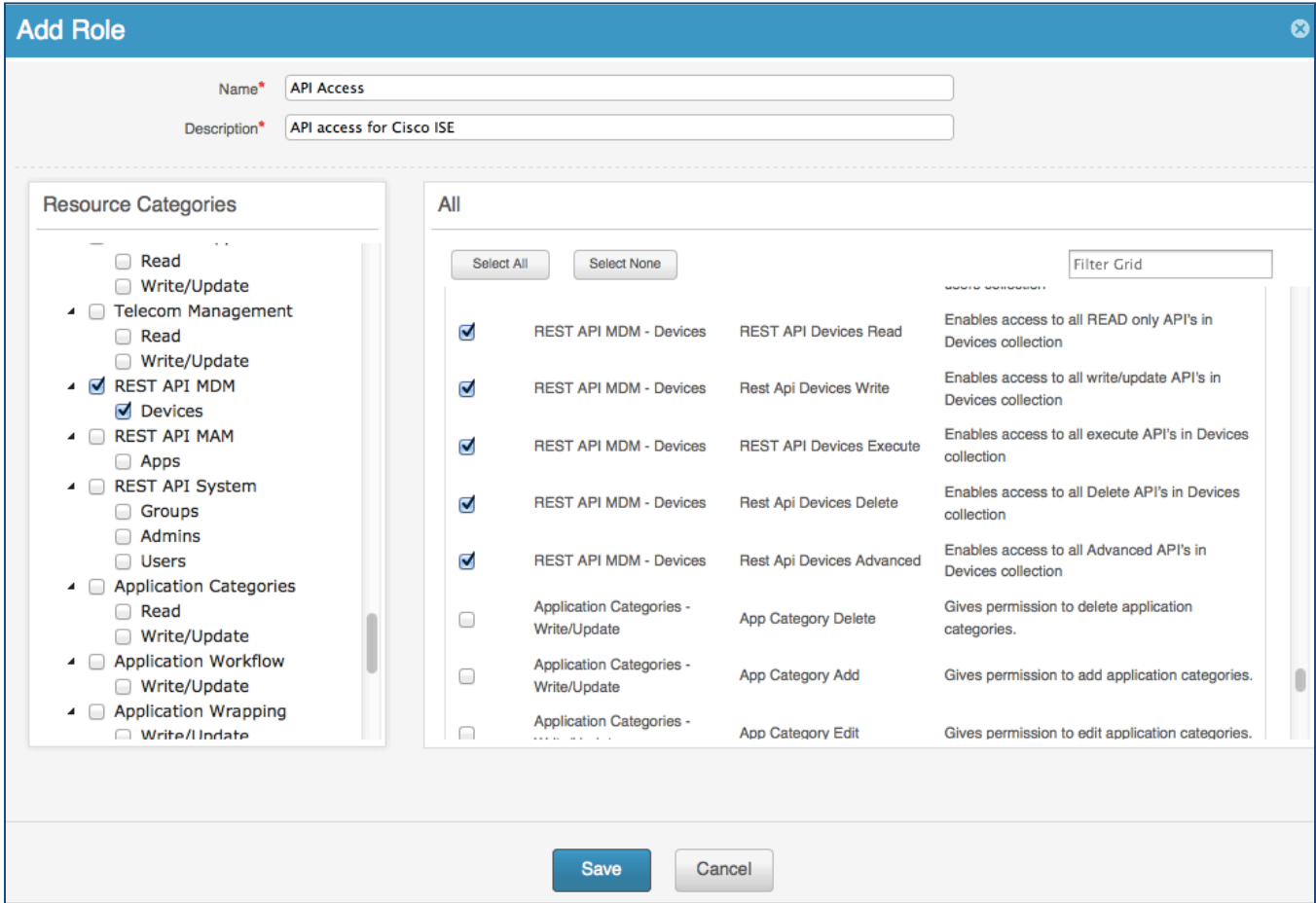


图 23. 添加角色

**步骤 5** 点击 **Admin Accounts**，然后点击 **Add User**。

**步骤 6** 填写基本信息，然后点击 **Roles** 分配创建的角色。

**步骤 7** 点击 **Save**。

**步骤 8** 使用 **Airwatch** 文档，按照公司要求在 **Airwatch** 服务器上配置 **MDM** 策略。有关最佳实践，另请参阅思科验证设计的文档。

[http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns743/ns1050/own\\_device.html](http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns743/ns1050/own_device.html)

## 附录 B：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](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](http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html)

有关思科 IOS 软件、思科 IOS XE 软件和思科 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](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](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](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](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](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](http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html)

对于思科无线 LAN 控制器：

<http://www.cisco.com/en/US/docs/wireless/controller/7.2/configuration/guide/cg.html>