
# Cisco ISE Integration with Mobile Device Management (MDM)

Imran Bashir
Cisco Technical Marketing

# Table of Contents

# Introduction

Mobile Device Management (MDM) software secures, monitors, manages and supports mobile devices deployed across mobile operators, service providers and enterprises. A typical MDM product consists of a policy server, a mobile device client and an optional inline enforcement point that controls the use of some applications on a mobile device (like email) in the deployed environment. However the network is the only entity that can provide granular access to endpoints (based on ACL's, TrustSec SGT's etc). It is envisaged that Cisco Identity Services Engine (ISE) would be an additional network based enforcement point while the MDM policy server would serve as the policy decision point. ISE expects specific data from MDM servers to provide a complete solution

The following are the high level use cases in this solution.

Device registration- Non registered endpoints accessing the network on-premises will be redirected to registration page on MDM server for registration based on user role, device type, etc

Remediation- Non compliant endpoints will be given restricted access based on compliance state

Periodic compliance check – Periodically check with MDM server for compliance

Ability for ISE administrators to issue remote actions on the device through the MDM server (e.g.: remote wiping of the managed device)

Ability for end user to leverage the ISE My Devices Portal to manage personal devices, e.g. Full Wipe, Corporate Wipe and PIN Lock.

# Sample Network Topology

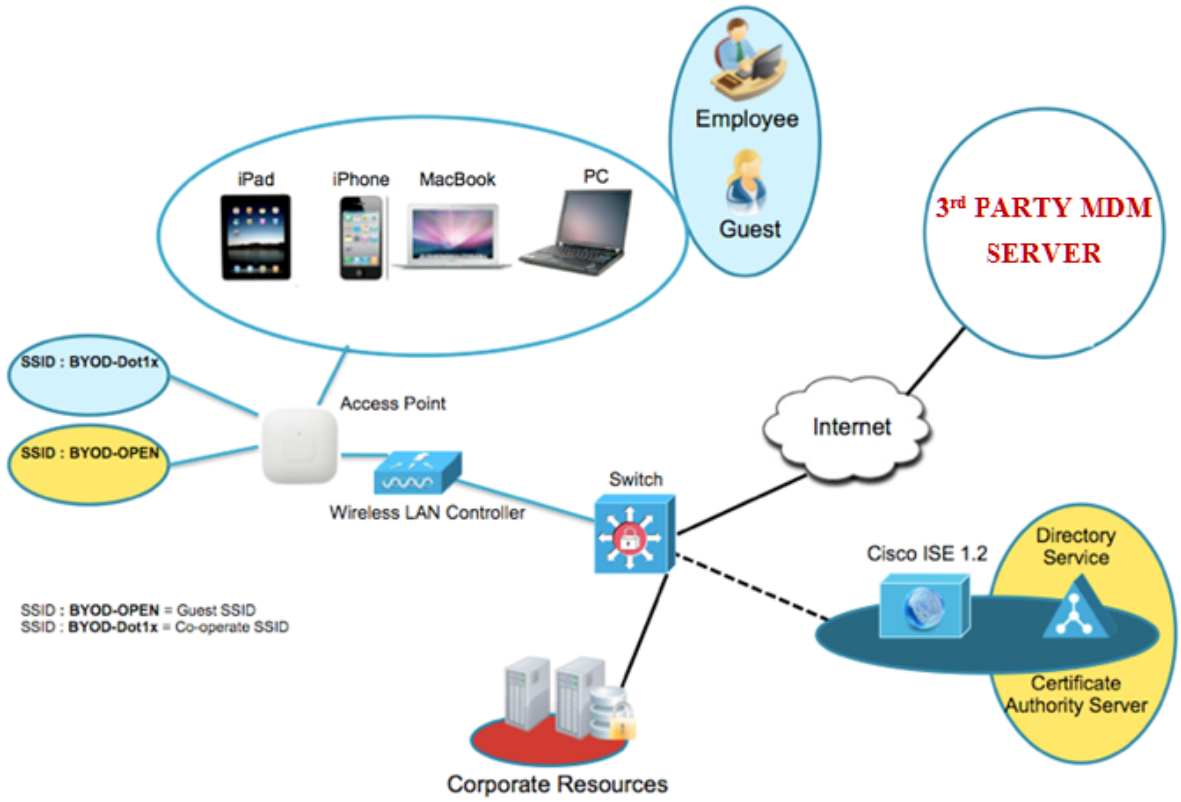



**Figure 1.**

## MDM Integration use-case overview

1. User associates device to SSID
2. If user device is not registered, user goes through the BYOD on-boarding flow, details listed in Appendix
3. ISE makes an API call to MDM server
4. This API call returns list of devices for this user and the posture status for the devices – Please note that we can pass MAC address of endpoint device as input parameter.
5. If user's device is not in this list, it means device is not registered with the MDM provider. ISE will send an authorization to NAD to redirect to ISE, which will re-direct users to the MDM server (home page or landing page)
6. ISE will know that this device needs to be provisioned using MDM and will present an appropriate page to user to proceed to registration.
7. User will be transferred to the MDM policy engine where registration will be completed by the user. Control will transfer back to ISE either through automatic redirection by MDM server or by user refreshing their browser again.
8. ISE will query MDM again to gain knowledge of posture status
9. If the user device is not in compliant to the posture (compliance) policies configured on MDM, they will be notified that the device is out of compliance, reason for non-compliance and the need to be in compliance to access network resources.

10. Once user's device becomes compliant, MDM server will update the device state in its internal tables.
11. At this stage user can refresh the browser at which point control would transfer back to ISE.
12. ISE would also poll the MDM server periodically to get compliance information and issue COA's appropriately.

## Components

Table 1: Components Used in this Document

| Component | Hardware | Features Tested | Cisco IOS® Software Release |
|---|---|---|---|
| The Cisco Identity Services Engine (ISE) | Any: 1121/3315, 3355, 3395, VMware | Integrated AAA, policy server, and services (guest, profiler, and posture) | ISE 1.2 |
| MDM Server | MDM | | |
| Certificate Authority Server (Optional) | Any per specification of Microsoft (Windows 2008 R2 Enterprise SP2) | SCEP, Certificate Authority Server | N/A |
| Wireless LAN Controller (WLC) | 5500-series 2500-series WLSM-2 Virtual Controller | Profiling and Change of Authorization (CoA) | Unified Wireless 7.2 |
| Test Devices: E.g. Apple iOS, Google Android .. | Apple & Google | N/A | Apple iOS 5.0 and higher Google Android 2.3 and higher |

Note: Within this document, we have demonstrated MDM configuration only. We recommend using our How-To-Guide to configure ISE and WLC to a recommended state.

How-to-Guide:
http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns742/ns744/docs/howto_60_byod_certificates.pdf

More guides are available at

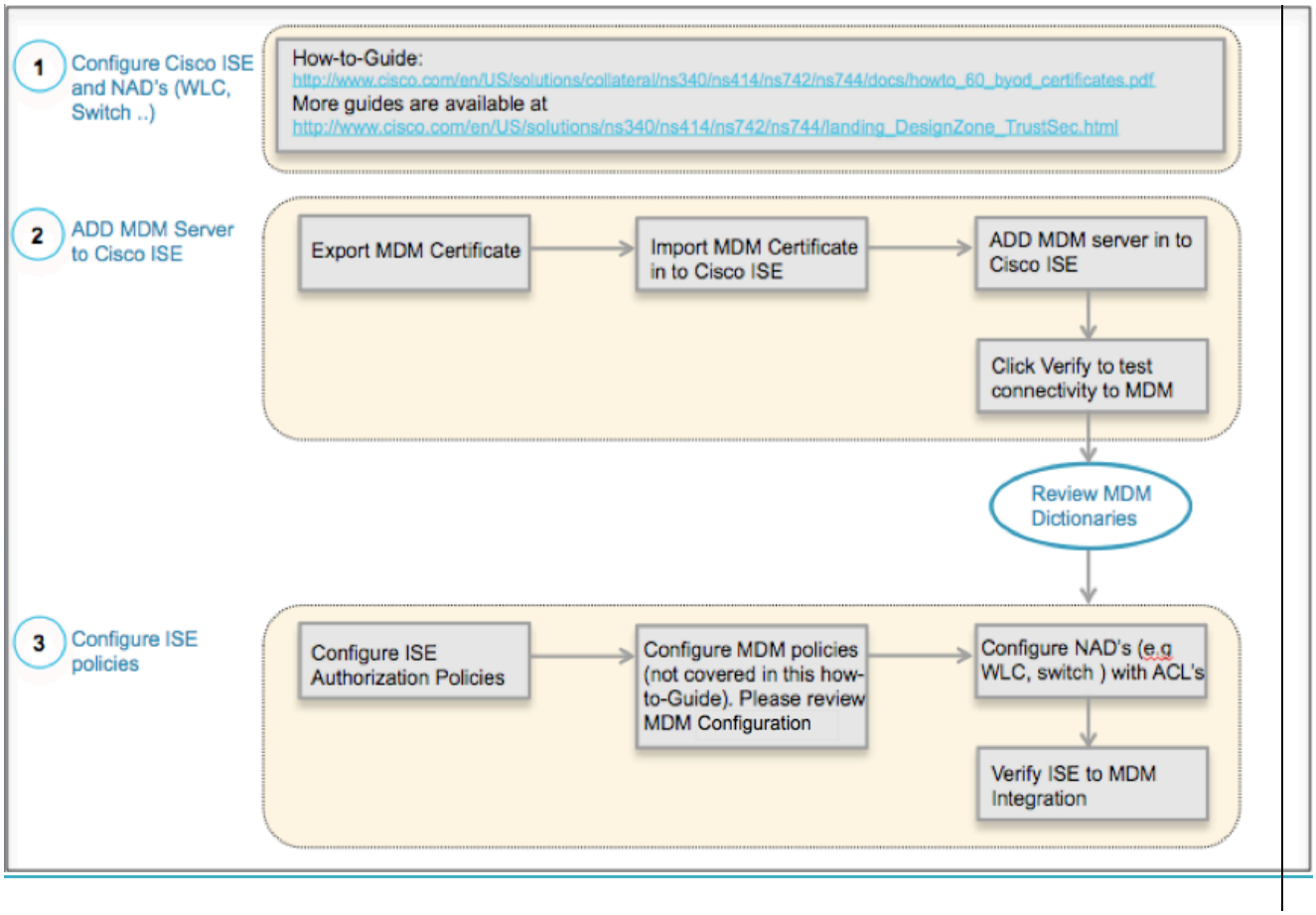
http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

# MDM Integration steps

Cisco ISE and MDM integration configuration.

Figure 3 shows the main steps in configuring MDM Integration.

Figure 4 MDM Configuration Flow



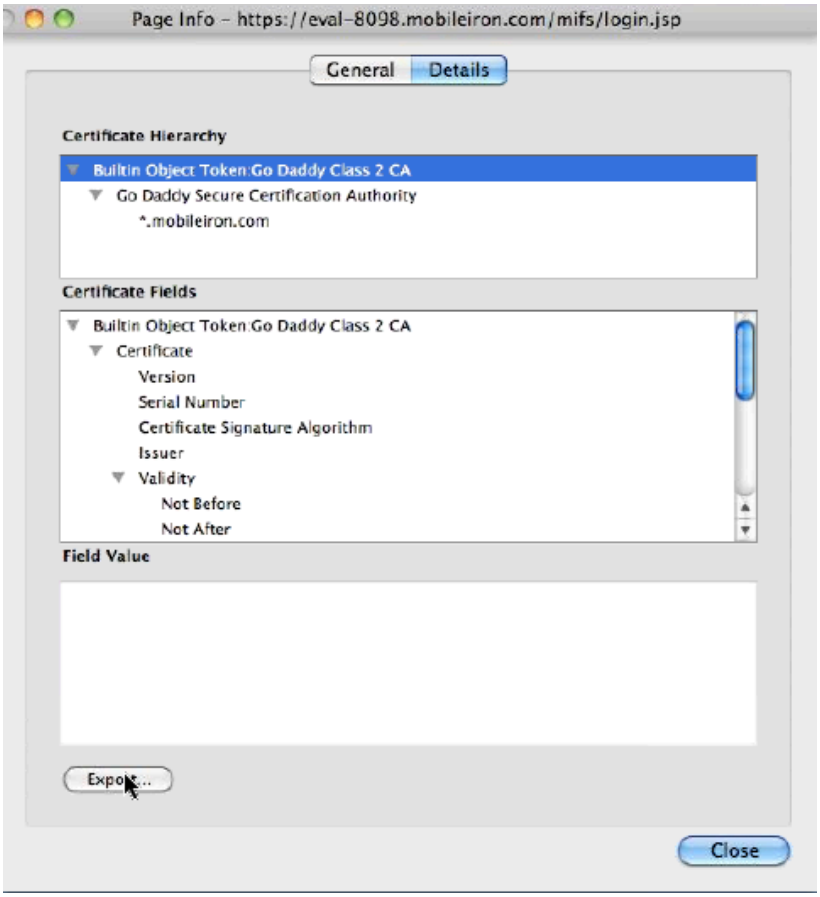

## Add External MDM Server to ISE.

MDM Servers can be used as a cloud service or installed locally on premises. Once the installation, basic setup and compliance checks are configured on the MDM server, it can then be added to ISE

### Step 1 Export MDM Server Certificate

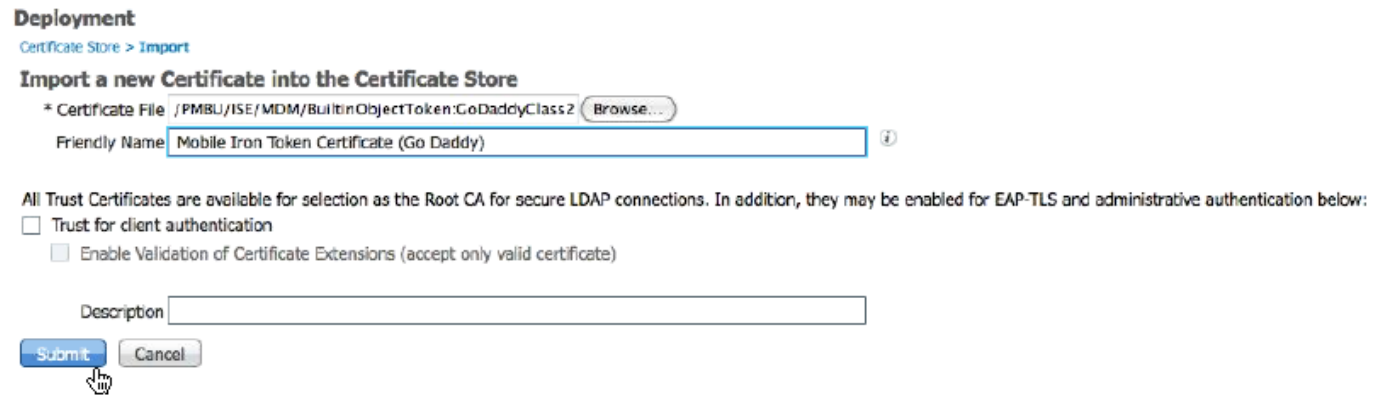
Step 1: Export MDM Server Certificate and save it on local machine

Figure 5 Export MDM Certificate




Step 2: Import the certificate in to ISE
Navigate to: Administration -> Certificates -> Certificate Store -> Import
Optional: Add a friendly name and then click Submit

Figure 6 Import MDM Certificate to Cisco ISE



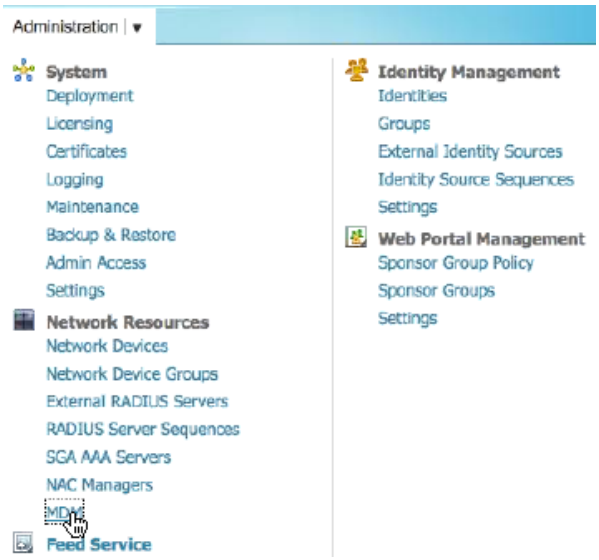

Step 3: Verify that Certificate is in Certificate Store

Figure 7 Verify MDM Certificate in Cisco ISE


Step 4: Add MDM Server. Administration -> MDM

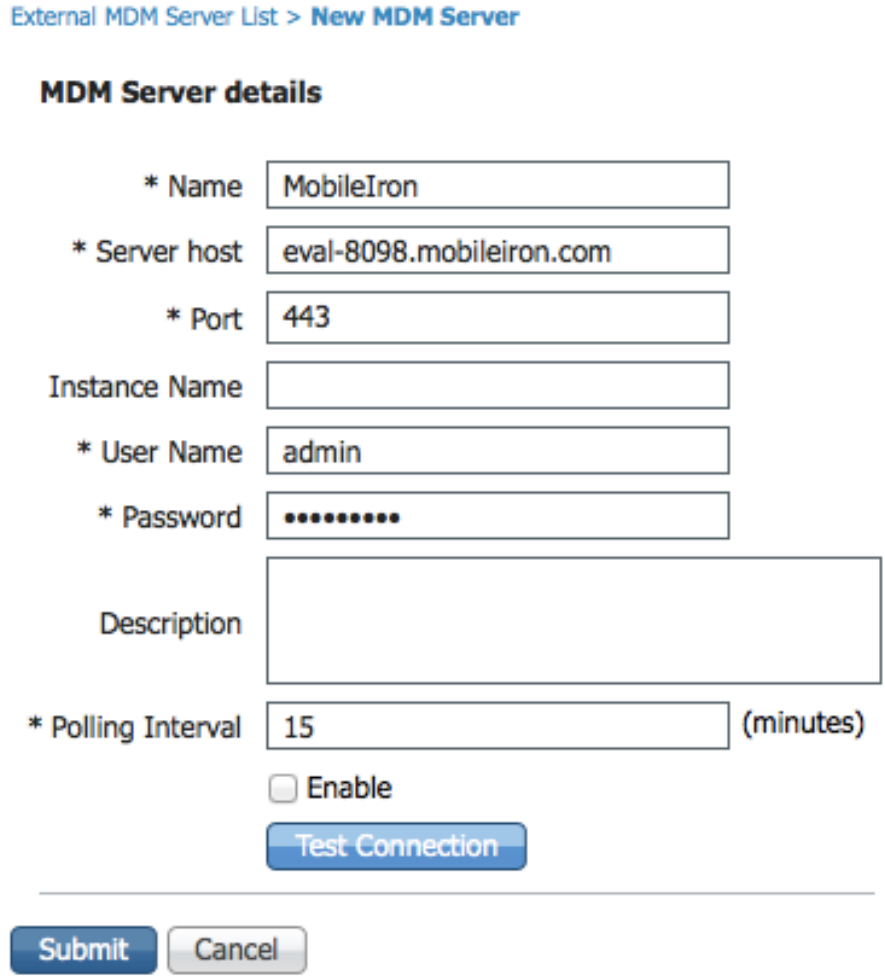
Note: Please review Appendix A to ensure that the account used to connect to Airwatch MDM Server has the API role assigned.

Figure 8.1 ADD MDM Server in Cisco ISE



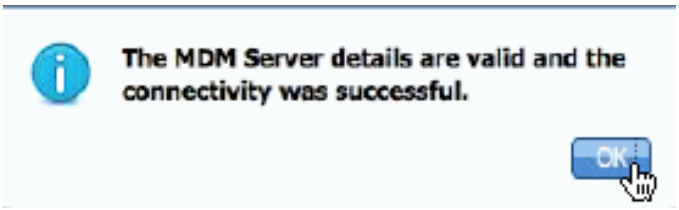

Click ADD, then enter MDM Server details

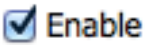
Figure 8.2 ADD MDM Server in Cisco ISE

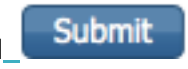



Click Test Connection first, ISE will confirm that connection is working

Figure 8.3 ADD MDM Server in Cisco ISE




Click OK on this pop-up and then select the checkbox 


Click the Submit button, the server will be added 

, the following success message with the presented to the admin

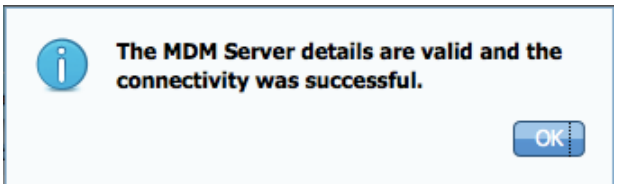


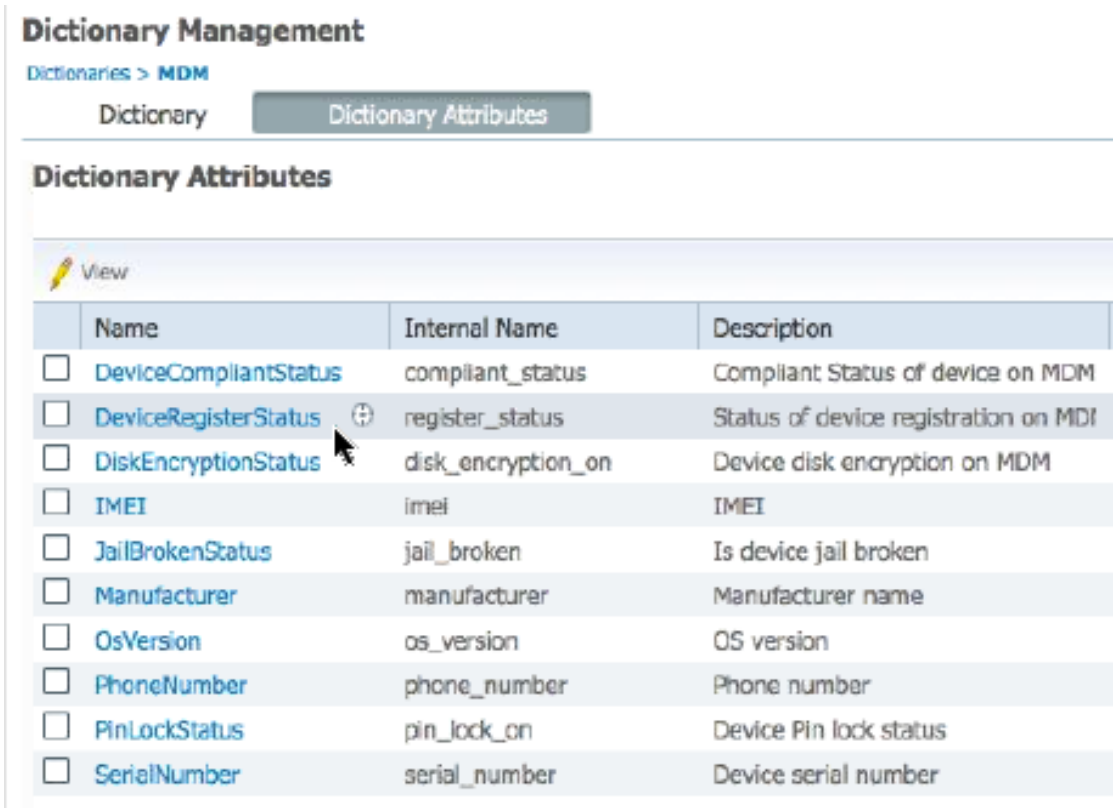
Figure 8.4 ADD MDM Server in Cisco ISE


## Review the MDM dictionaries

Once the MDM server is added, the supported dictionaries now show-up in ISE, which could be later used in to ISE Authorization Policies.

Navigate to: Policy -> Policy Elements -> Dictionaries -> MDM -> Dictionary Attributes

Figure 9 Review MDM Dictionaries in Cisco ISE




## Configure ISE Authorization Policies

Once MDM server is added in to ISE, we can configure authorization polices in ISE to leverage the new dictionaries added for MDM servers.

Note: Within this document, we have demonstrated using dictionary attributes MDM:DeviceRegisterStatus EQUALS UnRegistered and MDM:DeviceCompliantStatus EQUALS NonCompliant. Please configure and test additional attributes as well

Step 1: Create an ACL named “NSP-ACL” in the Wireless LAN Controller, which would be used in the policy later to redirect clients selected for BYOD supplicant provisioning, Certificate provisioning and MDM Quarantine.
The Cisco Identity Services Engine IP address = 10.35.50.165
Internal Corporate Networks = 192.168.0.0, 172.16.0.0 (to redirect)
MDM Server subnet = 204.8.168.0

Figure 10: Access Control List for re-directing client to BYOD flow

**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 |

Explanation of the NSP-ACL in Figure 17 is as follows

1. Allow all traffic “outbound” from Server to Client
2. Allow ICMP traffic “inbound” from Client to Server for trouble shooting, it is optional
3. Allow access to MDM server for un-registered and non-compliant devices to download the MDM agent and proceed with compliance checks
4. Allow all traffic “inbound” from Client to Server to ISE for Web Portal and supplicant and Certificate provisioning flows
5. Allow DNS traffic “inbound” from Client to Server for name resolution.
6. Allow DHCP traffic “inbound” from Client to Server for IP addresses.

7. Deny all traffic “inbound” from Client to Server to corporate resources for redirection to ISE (As per company policy)
8. Deny all traffic “inbound” from Client to Server to corporate resources for redirection to ISE (As per company policy)
9. Deny all traffic “inbound” from Client to Server to corporate resources for redirection to ISE (As per company policy)
10. Deny all traffic “inbound” from Client to Server to corporate resources for redirection to ISE (As per company policy)
11. Deny all traffic “inbound” from Client to Server to corporate resources for redirection to ISE (As per company policy)
12. Deny all traffic “inbound” from Client to Server to corporate resources for redirection to ISE (As per company policy)
13. Permit all the rest of traffic (Optional)

Step 2: Create an Authorization Profile named “MDM_Quarantine” for devices which are not in compliant to MDM polices. In this case all non-compliant devices will be redirected to ISE and presented with a message

Click Policy → Policy Elements → Results, Click Authorization → Authorization Profiles → Click “ADD”

Figure 11: Authorization Profiles Navigation

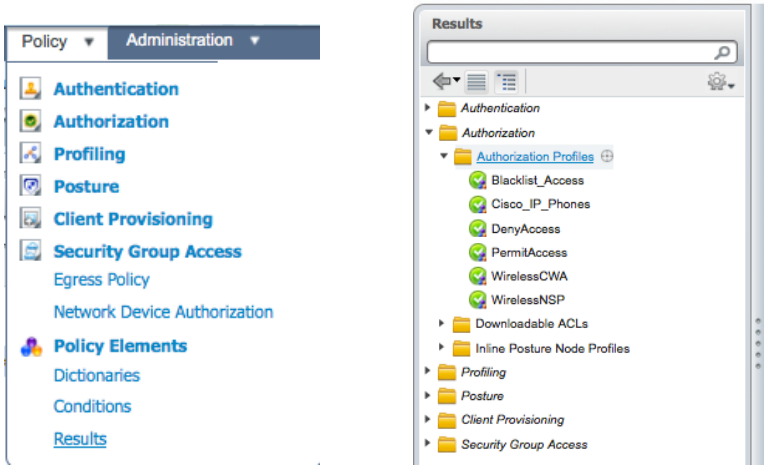



Figure 12.1: Authorization Policy Configuration

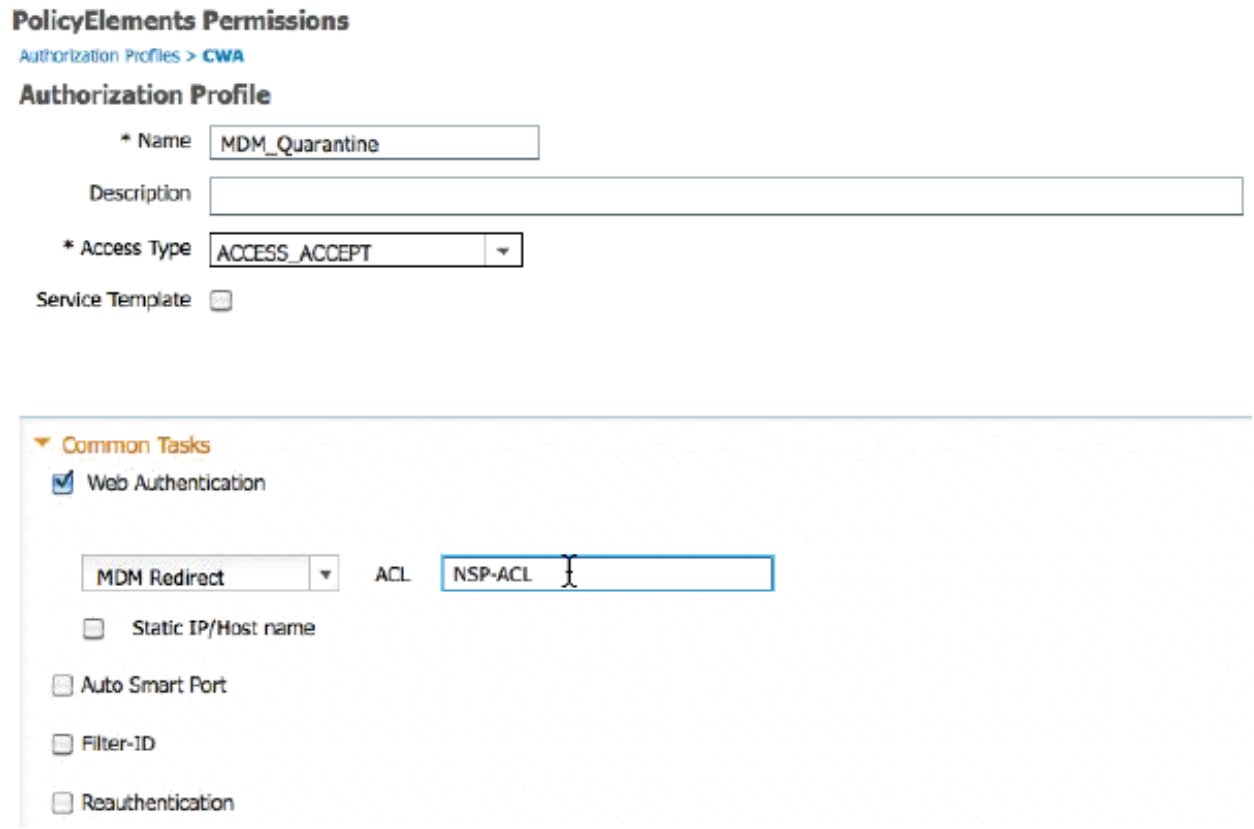
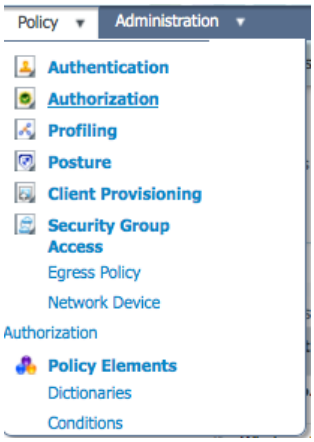


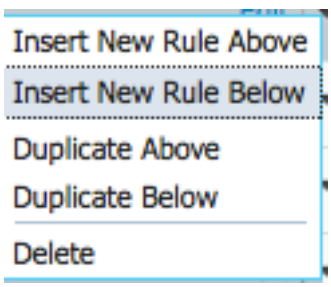

Figure 12.2: Authorization Policy Configuration


Note: NSP-ACL needs to be defined on the Wireless LAN Contoller, sample is attached

Step 3: Create Authorization Policy, Click Policy → Authorization → Authorization Profiles. Click "Insert New Rule Below"

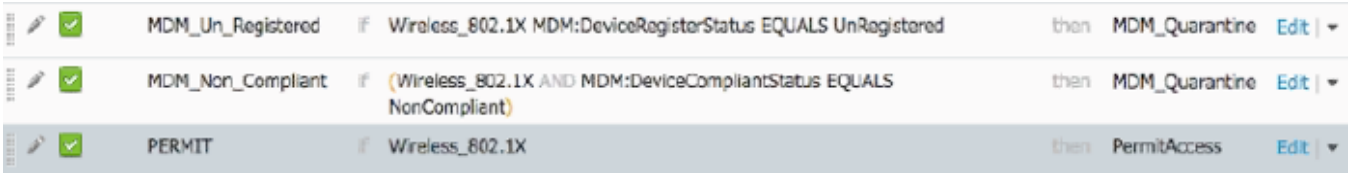
Figure 13: Insert New Rule



Please add the following Authorization Policy
MDM_Un_Registered = This Authorization Rule is added for devices which are not yet registered with an MDM server. Once the device hits this rule, it will be forwarded to ISE MDM landing page, which will present user with information on registering the device with MDM.
MDM_Non_Compliant = This Authorization Rule is added for devices which are not in compliant to MDM policies. Once the Android device hits the "Register" button during device registration, ISE sends a Re-Auth COA to the controller. Once the device hits this rule, it will be forwarded to ISE MDM landing page, which will present user with information on compliance failure.
PERMIT = Once the device is registered with ISE, registered with MDM and is in compliance to ISE and MDM policies it will be granted access to the network.

Figure 14: Authorization Policy Configuration view





You are done!

Please see the how-to-guide "BYOD-Using_Certificates_for_Differentiated_Access" If interested in provisioning Certificates along with the supplicant profile.

Note: MDM policies could also be defined in more granular details on Cisco ISE, e.g.

## Demonstrations.

If interested in looking at the end-user experience for on-boarding i-devices, Android, Windows and MAC OSx, please visit the following website.
http://wwwin.cisco.com/tech/snsbu/prod-sols/ise/#sectionName=4

# Appendix A: Mobile Iron Configuration

In this section we will review configuration of the MobileIron Server for the corporate policies. Please refer MobileIron documentation for configuration specific to the use case and your corporate polcies. This section only highlight simple configuration required to get the setup up and running.

This highlight the following:

- Verify admin account privileges for REST API, i.e. account used by ISE to send a REST API call to MobileIron Server
- Review the Default Security Policies
- Review the iOS APP installation configuration (AnyConnect)

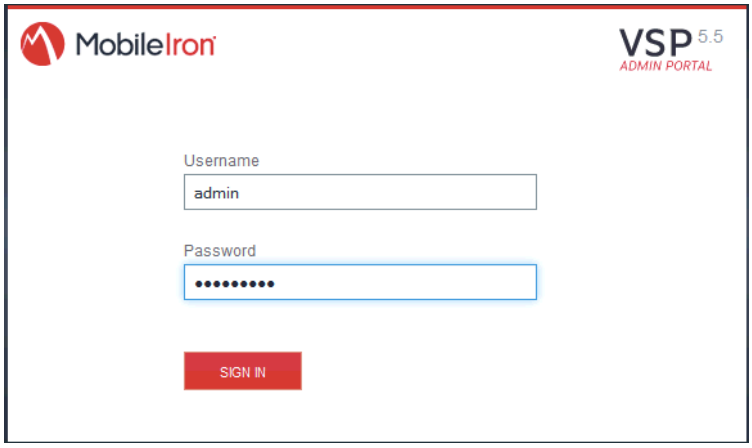
**Step 1** Access the MobileIron administrative web interface.

a. On Admin PC, launch Mozilla Firefox web browser. Enter MobileIron URL in the address bar:

**Step 1** https://FQDN_Name/admin

Note: URL listed here is a sample URL

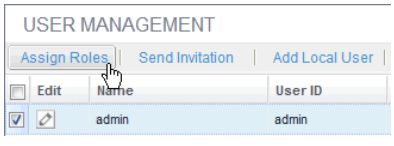
b. Login with username and password. Once you login, the USER & DEVICES tab should display.



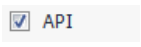

NOTE: Minimally, the account used to sign in here must have User Management privileges i.e. it does not necessarily need to be an admin account.

**Step 2** User Management

a. Navigate to USERS & DEVICES > User Management. From there, click the checkbox before admin user and click on Assign Roles.



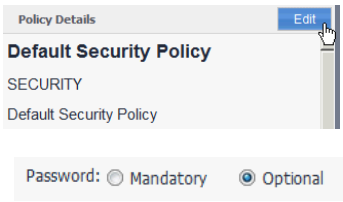

b. Notice that API check box is selected for the user




c. Navigate to USERS & DEVICES > User Management. From there, click the checkbox before employee1 user and click on Assign Roles.

d. Notice that API check box is NOT selected for the user

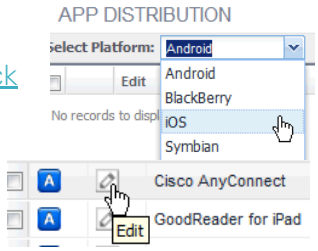
**Step 3** Security Policies on MobileIron Server




a. Navigate to POLICIES > All Policies → Default Security Policy. From there, click the Edit button on the right side of the screen.

b. Review the Policies e.g. Password, Type, Length, Data Encryption etc ..

**Step 4** Application Policies on MobileIron Server

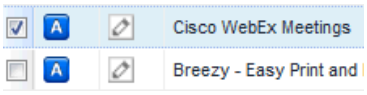



a. Navigate to APPS & CONFIGS > App Distribution. From there, click the dropdown button and select iOS

b. Cisco AnyConnect application has already been uploaded to the MobileIron server from APP store. Click the Edit button to review the details.

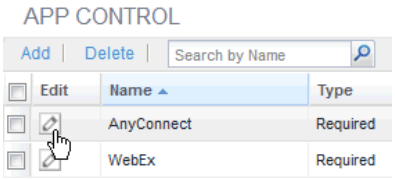
c. Notice the configuration where MobileIron server would send a installation request to the endpoint at the time of registration


d. Cisco WebEx application has already been uploaded to the MobileIron server from APP store. Click the Edit button to review the details.




e. Click on "Yes" where MobileIron server would send an installation request to the endpoint at the time of registration.


**Step 5** Application Control Policies on MobileIron Server




a. Navigate to APPS & CONFIGS > App Control

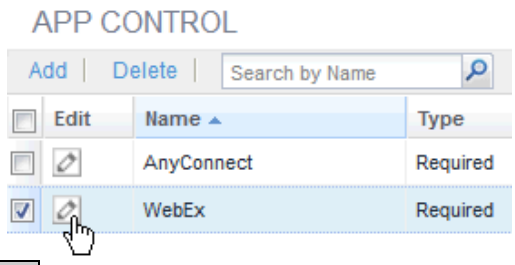
b. Click the Edit button for Anyconnect application

c. Edit the following as per below diagram

| Attribute | Value |
|---|---|
| Name | AnyConnect |
| Type | Required |
| App Name | IS |
| App Search String | AnyConnect |
| Device Platform | ALL |
| Comment | AnyConnect |

d. Click the Edit button for WebEx application

e. Edit the following as per below diagram




| Attribute | Value |
|---|---|
| Name | WebEx |
| Type | Required |
| App Name | IS |
| App Search String | WebEx |
| Device Platform | ALL |
| Comment | WebEx |

# Appendix B: References

Cisco TrustSec System:

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

Device Configuration Guides:

Cisco Identity Services Engine User Guides:
http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

For more information about Cisco IOS Software, Cisco IOS XE Software, and Cisco NX-OS Software releases, please refer to following URLs:

- For Cisco Catalyst 2900 series switches:
http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 3000 series switches:
http://www.cisco.com/en/US/products/ps7077/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 3000-X series switches:
http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 4500 series switches:
http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 6500 series switches:
http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html
- For Cisco ASR 1000 series routers:
http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html

For Cisco Wireless LAN Controllers:
http://www.cisco.com/en/US/docs/wireless/controller/7.2/configuration/guide/cg.html