



# Cisco Meraki EMM Integration with Cisco Identity Service Engine

*Secure Access How -To Guides Series*

**Author: Imran Bashir**

**Date: March 2015**

## Table of Contents

<b>Mobile Device Management (MDM)</b> .....	<b>3</b>
Overview .....	3
Cisco Meraki EMM cloud integration use-case overview .....	4
<b>Using MDM Integration Configuration Steps</b> .....	<b>6</b>
Cisco ISE and MDM integration configuration .....	6
Review the MDM dictionaries .....	9
Configure ISE Authorization Policies .....	10
<b>Appendix A: Meraki EMM Configuration</b> .....	<b>15</b>
Cisco TrustSec System: .....	25
Device Configuration Guides: .....	25

## Mobile Device Management (MDM)

---

### Overview

Cisco Meraki's Enterprise Mobility Management (EMM) software secures, monitors, manages and supports mobile devices deployed across mobile operators, service providers and enterprises. A typical Cisco Meraki EMM configuration consists of a cloud-based policy server and a mobile device client. However, often times 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 cloud-based Cisco Meraki EMM policy server would serve as the policy decision point. ISE expects specific data from Cisco Meraki cloud EMM 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 Cisco Meraki EMM cloud for registration based on user role, device type, etc. In addition Meraki can also provision the device with corporate application e.g. AnyConnect (VPN), Jabber (Collaboration) etc .. so the user has secure access to corporate resources (per policy) when device is off-premises.

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

**Periodic compliance check** – Periodically check with Cisco Meraki EMM cloud server for compliance

Ability for ISE **administrators to issue remote actions** on the device through the Cisco Meraki EMM cloud (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

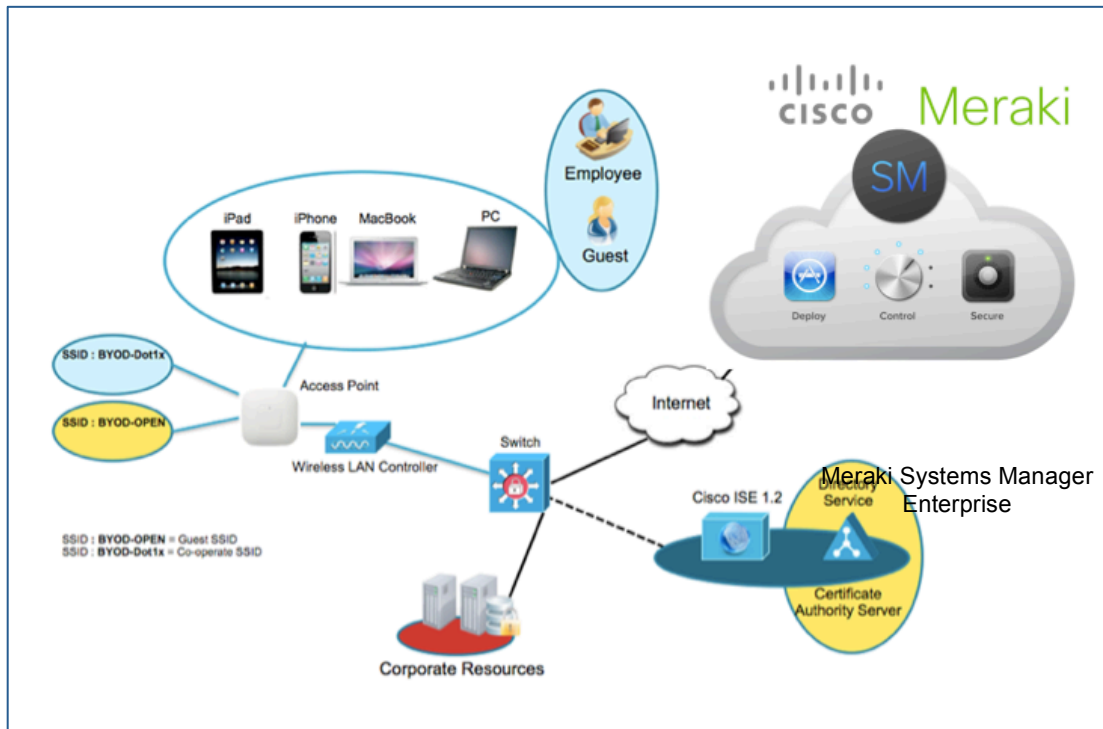


Figure 1. ISE+EMM Integration Topology

## Cisco Meraki EMM cloud 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 Cisco Meraki EMM cloud.
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 Cisco Meraki EMM cloud. ISE will send an authorization to NAD to redirect to ISE, which will re-redirect users to the Cisco Meraki EMM cloud (home page or landing page).
6. ISE will know that this device needs to be provisioned using the Cisco Meraki EMM cloud and will present an appropriate page to user to proceed to registration.
7. User will be transferred to the Cisco Meraki EMM cloud policy engine where the user will complete registration. Control will transfer back to ISE either through automatic redirection by the Cisco Meraki EMM cloud server or by user refreshing their browser again.
8. ISE will query the Cisco Meraki EMM cloud again to gain knowledge of posture status.
9. If the user device is not in compliance to the posture (compliance) policies configured on the Cisco Meraki EMM cloud, 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, the Cisco Meraki EMM cloud 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 Cisco Meraki EMM cloud periodically to get compliance information and issue COA's appropriately.

## Components

Table 1. Components Used in this Document

Tab

Component	Hardware	Features Tested	Cisco IOS® Software Release
The Cisco Identity Services Engine (ISE)	Any: 1121/3315, 3355, 3395, VMware, 3415, 3495	Integrated AAA, policy server, and services (guest, profiler, and posture)	ISE 1.3
EMM Server	EMM	Cloud Service	
Wireless LAN Controller (WLC)	5500-series 2500-series WLSM-2 Virtual Controller	Profiling and Change of Authorization (CoA)	Unified Wireless 7.2
Cisco Meraki Cloud Wireless LAN		Cloud-managed wireless with Cisco Meraki EMM cloud  Tested as replacement to traditional WLC	N/A
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 Cisco Meraki EMM cloud configuration only. We recommend using our How-To-Guide to configure ISE and WLC/Meraki 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](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](http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html)  
<https://docs.meraki.com/display/kb/Wireless+LAN>

# Using MDM Integration Configuration Steps

## Cisco ISE and MDM integration configuration

Figure 2 shows the main steps in configuring MDM Integration.

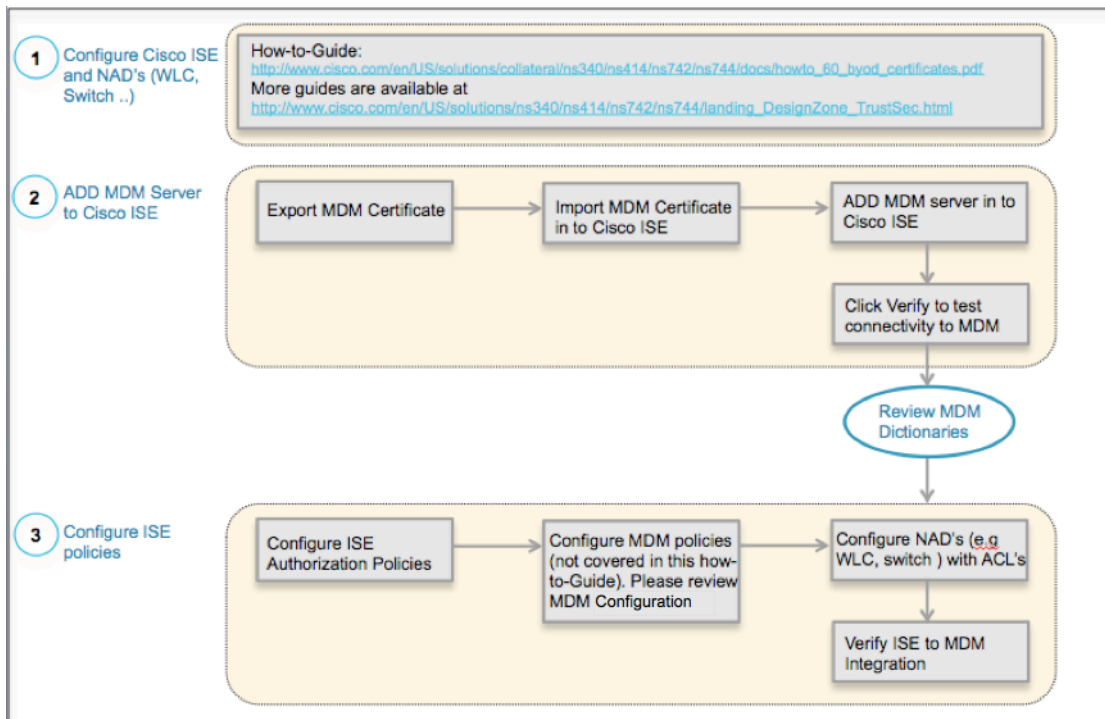


Figure 2. MDM Configuration Flow

### Add External MDM Server to ISE

Cisco Meraki’s EMM Servers can be used as a cloud service; once the installation, basic setup and compliance checks are configured on the cloud, it can then be added to ISE.

### Export MDM Server Certificate

**Step 1** Export EMM Server Certificate and save it on local machine.

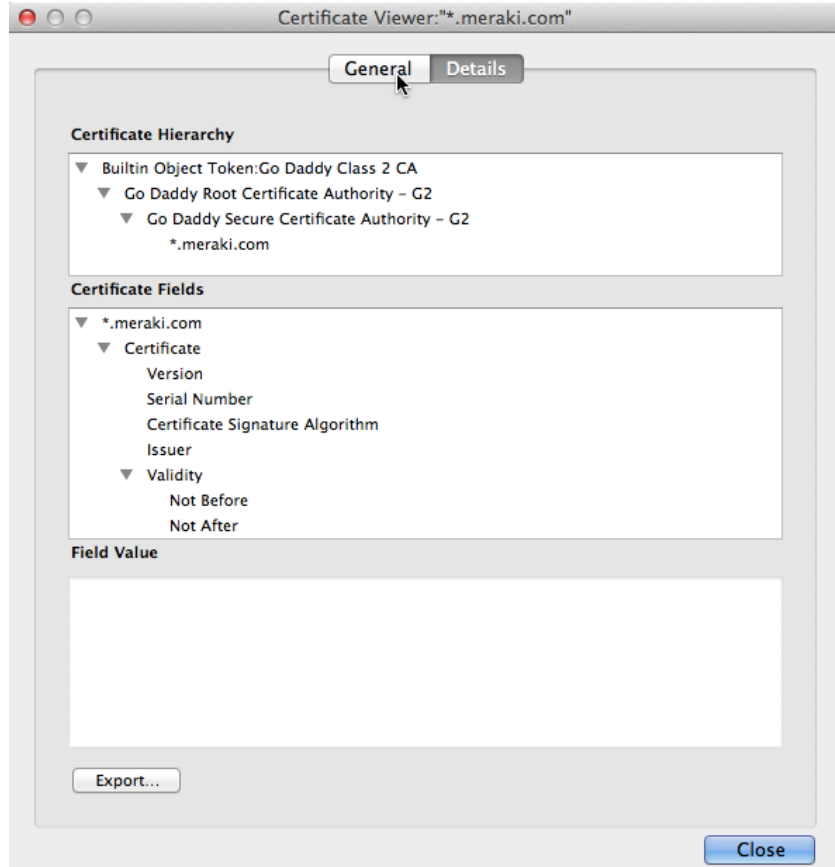


Figure 3. Export MDM Certificate

- Step 2** Import the certificate in to ISE  
 Navigate to: **Administration -> Certificates -> Trusted Certificates -> Import**  
 Click Browse on Certificate File and select the Meraki Certificate  
 Optional: Add a friendly name and then click Submit

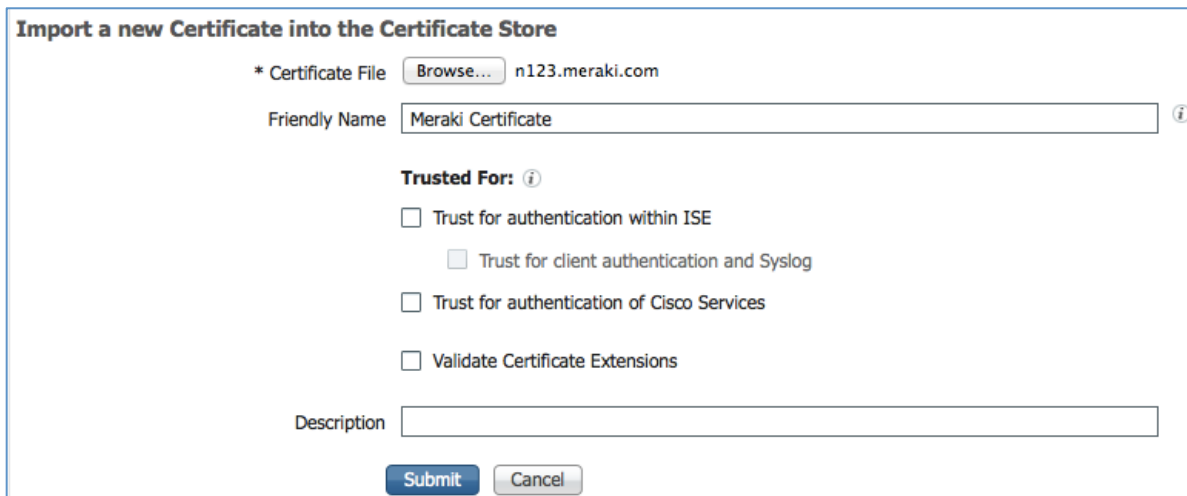
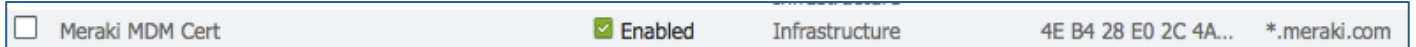


Figure 4. Import MDM Certificate to Cisco ISE

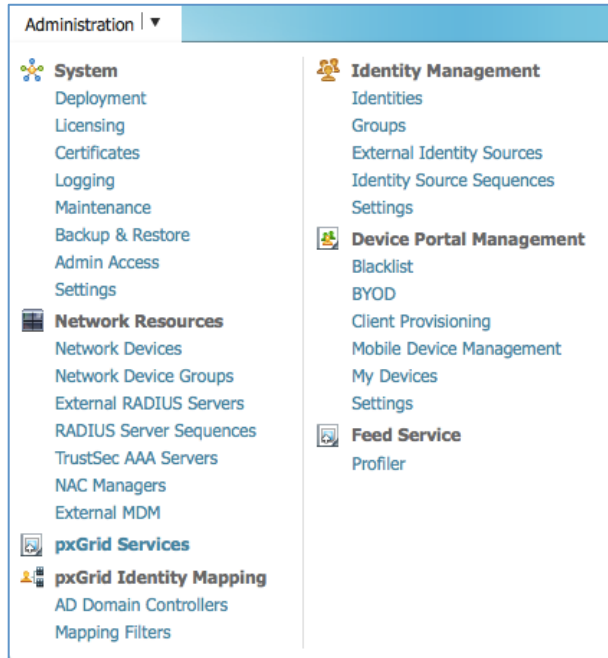
**Step 3** Verify that Certificate is in Certificate Store.

Under Trusted Certificates



**Figure 5.** Verify MDM Certificate in Cisco ISE

**Step 4** Add MDM Server. **Administration -> MDM**



**Figure 6.** ADD MDM Server in Cisco ISE

**Step 5** Click ADD, and then enter MDM Server details.

**MDM Server details**

\* Name

\* Hostname or IP Address

\* Port

Instance Name

\* User Name

\* Password

Description

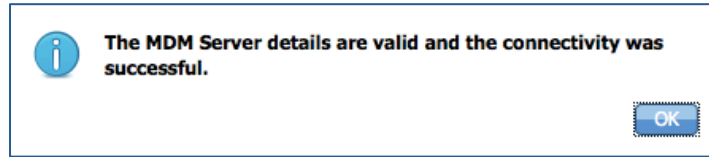
\* Polling Interval  (minutes) ⓘ

Enable

**Figure 7.** ADD MDM Server in Cisco ISE




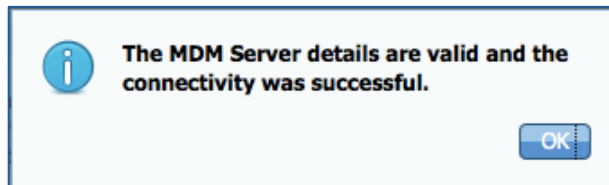
**Step 6** Click **Test Connection**, ISE will confirm that connection is working.



**Figure 8.** ADD MDM Server in Cisco ISE

**Step 7** Click OK on this pop-up and then select the checkbox.  **Enable**

**Step 8** Click the Submit button, the server will be added , the following success message with the presented to the admin.



**Figure 9.** ADD MDM Server in Cisco ISE

MDM Servers			
<span>Edit</span> <span>+ Add</span> <span>X Delete</span>			
Name	Status	Service Provider	MDM Server
<input type="checkbox"/> Meraki	<input checked="" type="checkbox"/> Active	Cisco Meraki	n123.meraki.com

**Figure 10.** Server Added

## 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.

**Step 1** Navigate to: **Policy -> Policy Elements -> Dictionaries -> System -> MDM -> Dictionary Attribute**

Dictionary Attributes			
View			
	Name	Internal Name	Description
<input type="checkbox"/>	DeviceCompliantStatus	compliant_status	Compliant Status of device on M...
<input type="checkbox"/>	DeviceRegisterStatus	register_status	Status of device registration on M...
<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"/>	MDMServerReachable	MDMServerReachable	MDM server reachability
<input type="checkbox"/>	Model	model	Device model
<input type="checkbox"/>	OsVersion	os_version	Device Operating System
<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

Figure 11. 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 demonstrated using dictionary attributes **MDM:DeviceRegisterStatus EQUALS UnRegistered** and **MDM:DeviceCompliantStatus EQUALS NonCompliant**. Please configure and test additional attributes as well

**Step 2** 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

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 /	Any	Any	Any	Any	Outbound	150720	<input checked="" type="checkbox"/>
<a href="#">2</a>	Permit	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 /	204.8.168.0 /	Any	Any	Any	Any	Any	17626	<input checked="" type="checkbox"/>
<a href="#">4</a>	Permit	0.0.0.0 /	10.35.50.165 /	Any	Any	Any	Any	Inbound	7505	<input checked="" type="checkbox"/>
<a href="#">5</a>	Permit	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 /	UDP	Any	DHCP Server	Any	Inbound	0	<input checked="" type="checkbox"/>
<a href="#">7</a>	Deny	0.0.0.0 /	192.168.0.0 /	Any	Any	Any	Any	Inbound	0	<input checked="" type="checkbox"/>
<a href="#">8</a>	Deny	0.0.0.0 /	172.16.0.0 /	Any	Any	Any	Any	Inbound	4	<input checked="" type="checkbox"/>
<a href="#">9</a>	Deny	0.0.0.0 /	10.0.0.0 /	Any	Any	Any	Any	Inbound	457	<input checked="" type="checkbox"/>
<a href="#">10</a>	Deny	0.0.0.0 /	173.194.0.0 /	Any	Any	Any	Any	Inbound	1256	<input checked="" type="checkbox"/>
<a href="#">11</a>	Deny	0.0.0.0 /	171.68.0.0 /	Any	Any	Any	Any	Inbound	11310	<input checked="" type="checkbox"/>
<a href="#">12</a>	Deny	0.0.0.0 /	171.71.181.0 /	Any	Any	Any	Any	Any	0	<input checked="" type="checkbox"/>
<a href="#">13</a>	Permit	0.0.0.0 /	0.0.0.0 /	Any	Any	Any	Any	Any	71819	<input checked="" type="checkbox"/>

**Figure 12.** Access Control List for re-directing client to BYOD flow

## Explanation of the NSP-ACL

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 3** 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.

**Step 4** Click Policy → **Policy Elements** → **Results**, Click **Authorization** → **Authorization Profiles** → **ADD**.

**Figure 13.** Authorization Policy Configuration

**Figure 14.** NSP-ACL

**Note:** NSP-ACL needs to be defined on the Wireless LAN Controller.

**Step 5** Create Authorization Policy. Click Policy → **Authorization** → **Authorization Profiles**. Click “**Insert New Rule Below**”.



Figure 15. Insert New Rule

**Please add the following Authorization Policy**

**MDM\_OnBoarding** = This Authorization Rule is added for devices which are not yet registered with the Cisco Meraki EMM cloud. Once the device hits this rule, it will be forwarded to ISE EMM landing page, which will present user with information on registering the device with the Cisco Meraki EMM cloud. You will need to provide the end user with the Cisco Meraki Network ID (available on the MDM > Add devices page in the Meraki Dashboard):

Figure 13: Configuring EMM portal in ISE for Meraki Network ID



Figure 16. Configuring EMM portal in ISE for Meraki Network ID

**MDM\_OnBoarded** = 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

**Default** = If the device does not hit the above policies, e.g. Not registered with MDM or not Compliant with MDM, then hits the Default Deny Rule

		MDM_OnBoarded	if (Network Access:AuthenticationMethod EQUALS x509_PKI AND MDM:DeviceCompliantStatus EQUALS Compliant AND MDM:DeviceRegisterStatus EQUALS Registered )	then PermitAccess
		MDM_OnBoarding	if (Network Access:AuthenticationMethod EQUALS x509_PKI AND MDM:DeviceRegisterStatus EQUALS UnRegistered )	then MDM_OnBoarding
		Default	if no matches, then	DenyAccess

Figure 17. Authorization Policy Configuration View



You are done!

**Note:** Optionally you could add another rule to allow limited access to devices which are registered with MDM but are not compliance, e.g. Remediation access only

<input checked="" type="checkbox"/>	MDM_NonCompliant	if	(Network Access:AuthenticationMethod EQUALS x509_PKI AND MDM:DeviceCompliantStatus EQUALS NonCompliant AND MDM:DeviceRegisterStatus EQUALS Registered)	then	Remediation_Access_Only
-------------------------------------	------------------	----	--	------	-------------------------

Please see the HowTo guide: **BYOD Using Certificates for Differentiated Access** for more information on 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: Meraki EMM Configuration

In this section we will review configuration of the Cisco Meraki EMM cloud for the corporate policies. Please refer to Cisco Meraki documentation for configuration specific to the use case and your corporate policies. This section only highlights the simple configuration required to get the setup up and running.

This highlight the following:

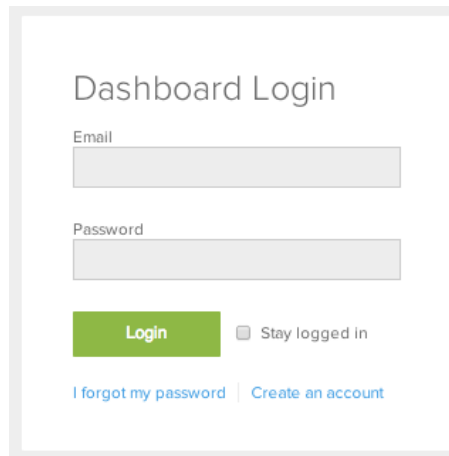
- Verify ISE settings that must be obtained from Cisco Meraki EMM cloud and configured on the ISE server
- Configure Applications to be pushed to End Points.

**Step 1** Access the Cisco Meraki administrative web interface.

- a. On **Admin PC**, launch any standard web browser. Enter Cisco Meraki URL in the address bar:

<https://dashboard.meraki.com>

**Note:** URL listed here is a sample URL



**Figure 18.** Login Panel

- b. Login with username and password. Once you login, navigate to your Systems Manager network.

**Step 2** ISE settings

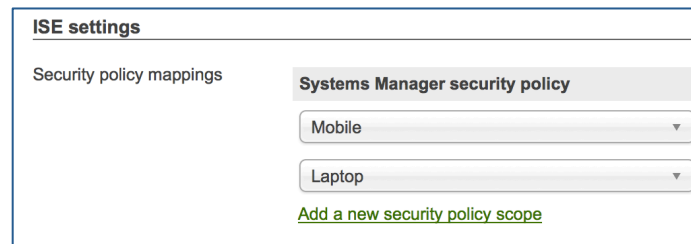
- a. Navigate to **Organization > MDM page**. From there, Note the “ISE settings’ URL, username and password; these settings must be configured on your ISE server (see step #4 in previous section).

ISE settings	
Setup URL	<a href="https://n7.meraki.com/">https://n7.meraki.com/</a>
Username	d35b9672ba56ed95afa77b4620dc74a
Password	f08f039ae4cb114469c73e2652f22d7c

**Figure 19.** ISE Settings

**Step 3** Security Policies on Cisco Meraki Server.

- a. Navigate to the **Configure > Policies** page. Here, you can create and configure your security policies (e.g. screen lock, disk encryption, blacklisted apps running, etc.).
- b. Navigate to **Configure > General → ISE settings**. You can assign which policies will be reported to ISE.

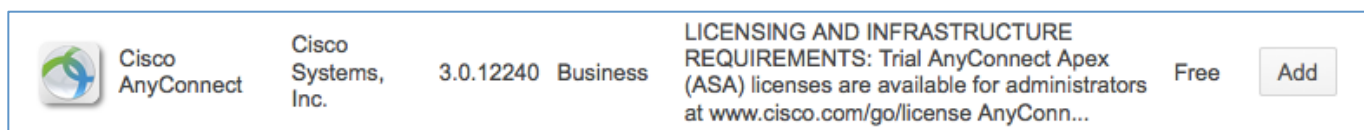


**Figure 20.** ISE Settings

### Configure Applications on Meraki

In this section we will configure the Cisco Meraki EMM cloud for the corporate applications like Cisco AnyConnect. We will then also configure the VPN profile that would be pushed with AnyConnect Applications so the device can access corporate data and applications securely when Off Premises (through a VPN). Once logged in to Meraki Configuration interface, configure applications.

- a. Navigate to **MDM > Apps** page.
- b. Click on **Add New** icon on the right of the screen.
- c. Select **iOS** app.
- d. Type **AnyConnect** in the search.
- e. Click **ADD**, and Save Changes.



**Figure 21.** Cisco AnyConnect

**Step 4** Configure the VPN profile.

**Step 5** Navigate to **MDM > Settings > VPN** page.

**Step 6** Click on **Configure a VPN network**.

**Step 7** Enter your **VPN Server address**, as an example; the following has the configuration to connect to `vpn.cisco.com`.



<b>Configuration</b> ×	Manual ▾
Connection Name	<input type="text" value="vpn.cisco.com"/> Display name of the connection (displayed on the device)
Connection Type	L2TP ▾
Server	<input type="text" value="vpn.cisco.com"/> Hostname or IP address for server
Shared Secret	<input type="text"/> Shared secret for the connection <a href="#">Show secret</a>
User Authentication	Password ▾ Authentication type for connection
Account	<input type="text"/> User account for authenticating the connection
	<input type="checkbox"/> <b>Send All Traffic</b> Routes all network traffic through the VPN connection
Proxy Setup	None ▾ Configures proxies to be used with this VPN connection

**Figure 22.** Example Configuration

## Appendix B: Cisco ASA Sample Configuration

This is a sample configuration of an ASA Server where the Meraki MDM provisioned device application **Cisco AnyConnect** can connect back to establish a VPN connection.

ASA Version used in this Setup = ASA Version 9.3(1)

Hardware: ASA5515, 8192 MB RAM, CPU Clarkdale 3059 MHz, 1 CPU (4 cores)

IP configurations of outside interface, DNS and ISE Policy Services Node are changed, please replace with your ASA and ISE IP address in the network

*IP address of Outside Interface = 1.1.1.100*

*IP address of Default Gateway = 1.1.1.1*

*IP address of ISE PSN Node = 2.2.2.2*

*IP address of DNS Server = 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 recurring 10.10.10.10
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 ojsp.quovadisglobal.com
 fqdn ojsp.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 oosp.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_CRYPTOMAP 65535 set pfs group5
crypto dynamic-map SYSTEM_DEFAULT_CRYPTOMAP 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_CRYPTOMAP 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_CRYPTOMAP
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-shal
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,ise posture
  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
```





## Appendix C: 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](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](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](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](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](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](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](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](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>