

Cisco MCMS Best Practices Guide

Introduction

This document is a list of best practices that we have accumulated while working with MCMS. The goal is to help you get the most of our MCMS in as short a time as possible, while avoiding the pitfalls we have seen most often.

MCMS is designed to manage your mobile devices by bringing them under centralized control so that you can manage the settings, security, applications, and costs associated with them. Cisco wants to provide administrators with as much or as little control over their devices as possible, which means that you need to really understand what your corporate policies are with regard to:

- Corporate owned devices
- Employee owned devices
- Email
- Web browsing
- Mobile application usage
- Location tracking
- VPN and remote access
- Policy enforcement

Your companies' policies on these issues (and many others obviously) will largely determine how you configure the various settings in MCMS. If you are unsure about any of these, you should probably ensure you have clarity before moving forward incorrectly.

Corporate Owned Devices

Many corporations pay for users mobile phone expenses. These phones are considered company assets, and companies generally exert greater control over these devices than equipment that is personally owned.

Best Practice #1 – Have a Corporate Owned Device policy

Each company's practices will be different, but you should develop a list of items that are important to your company. Often this will be based on the type of business you are, the industry you are in, or the culture of your company.

See the video here:

<https://supportforums.cisco.com/community/netpro/solutions/mcms>

Best Practice #2 – Have an Employee Owned (BYOD) Device policy

When an employee purchases their own device, it is no longer a corporate asset, so enforcing policies can be somewhat more difficult. The tradeoff is often that without proper policies a company will often limit or disable many features that users want (VPN, corporate web browsing, corporate applications). You must find a balance with your users that protect both parties. MCMS provides an easy way to segment employee owned devices.

Manage > Manage Privacy Settings

The screenshot shows the 'Privacy Settings' configuration page in the MCMS interface. It includes a navigation bar with 'Home', 'Manage', and 'Reports' tabs. The main content area has a 'Save' button and a 'View Change History' button. Below these are two sections: 'Restrict Location Information' and 'Restrict App Inventory Information'. Each section has a 'Save' button, a 'View Change History' button, and a 'Select Applicable Ownership Types' section with checkboxes for 'Corporate owned', 'Unknown', and 'Employee owned'. The 'Employee owned' checkbox is checked in both sections. Below the ownership types is a 'Select Applicable Device Group' dropdown menu set to 'All Devices'.

When a device is enrolled it can be listed as “Corporate Owned” or “Employee Owned”, allowing administrators to easily separate devices into large groups. Here under Manage > Manage Privacy Settings we can set “Employee Owned” devices so we do not collect location or application information.

See the video here:

<https://supportforums.cisco.com/community/netpro/solutions/mcms>

Best Practice #3 – Know Industry Regulations

Your industry might have significant regulations that will define many of your MDM policies. Industries like Financial Services and Banking, or Healthcare have government regulations that you will need to adhere to. As much as you can you will want to try and keep your buckets large so that you are not micro managing. Typical buckets are:

1. iOS Devices
2. Android Devices
3. Company Owned
4. Employee Owned

Largely all the devices in a company will need to adhere to the same regulations, so the policies should be the same.

Best Practice #4 – Set PIN and Passcode requirements

Mobile devices are easy to lose, misplace, and steal, so having a passcode enforced is one of the easiest steps to take towards preventing unwanted access to device information.

There are a few options for passcodes:

Name	Description	Example
Simple	Repeating, ascending or descending values	12345 abcde
Numeric	Requires at least one number	1abc 11111
Alphanumeric	Requires at least one number and one letter	1abc abc123
Complex	Requires at least one number, one letter, and one special character	124\$ abc\$ 1abc\$
Pattern	Android only. User draws a pattern across dots	

Passcodes

Can be up to 16 characters, but longer is harder to remember and you might be taking more help desk calls to unlock devices.

Passcode expiration

You can set a time for how often a user is required to set a new passcode.

Passcode history

You can set a policy to prevent users re-using old passcodes.

Manage > Manage Device Policies

The screenshot shows the Cisco MCMS interface for managing device policies. The top navigation bar includes 'Home', 'Manage', and 'Reports'. Below it, the breadcrumb trail is 'Manage Device Policies > View All Policies > Default'. The main content area is titled 'Default' and shows the 'Device Passcode' settings for a policy named 'Default'. The settings are as follows:

Setting	Value
Require Passcode	<input checked="" type="checkbox"/>
Minimum Passcode Length (4-16)	4
Allow Simple Passcode	<input checked="" type="checkbox"/>
Require Alphanumeric in Passcode (at least one letter)	<input type="checkbox"/>
Required Number of Complex Characters (1-4)	1
Allowed Failed Attempts (4 to 16)	8
Number of Unique Passcodes Required Before Reuse Allowed (1-50)	0
Allowed Idle Time Before Auto-Lock (1-60 minutes)	15
Maximum Passcode Age (1-730 days, or blank)	180
Enable Passcode Recovery for Device Unlock	<input type="checkbox"/>

See the video here:

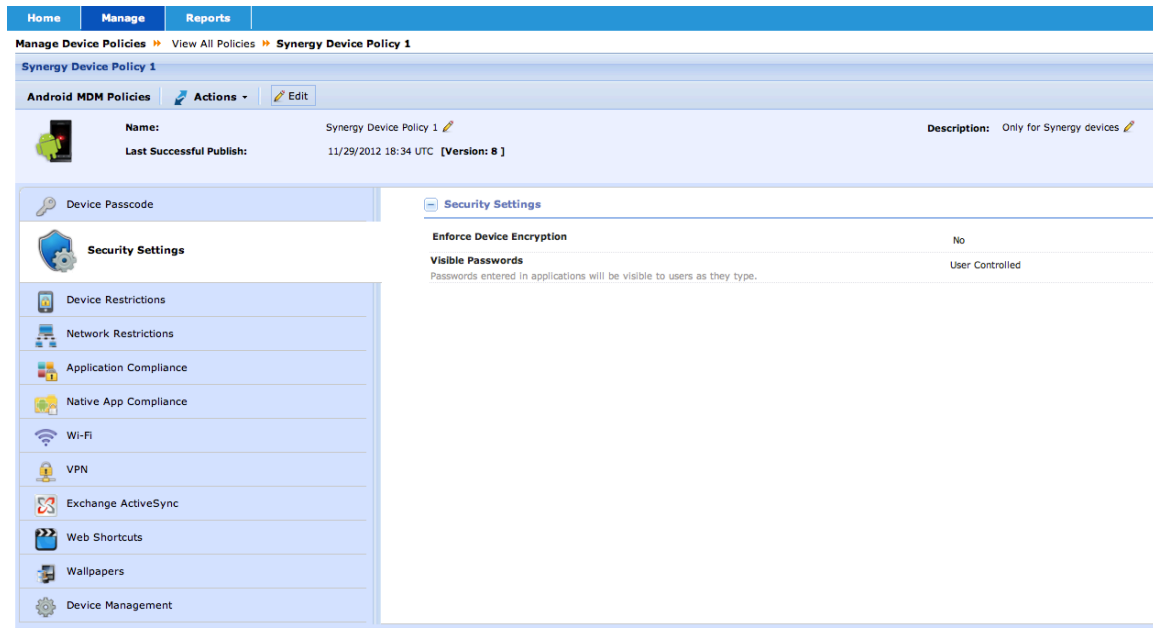
<https://supportforums.cisco.com/community/netpro/solutions/mcms>

Best Practice #5 – Add Encryption

On iOS devices above the 3G, encryption happens when a passcode is enabled. Therefore, when you enforce best practice #2, you also cover this one.

Android devices are much different. There are numerous vendors and software revisions from Google. You will have to make a judgment call if those devices that are unable to perform encryption will be allowed on your network. Our recommendation is to enforce encryption on all devices.

Manage > Manage Device Policies > Security Settings



See the video here:

<https://supportforums.cisco.com/community/netpro/solutions/mcms>

Best Practice #6 – Restrict Device Features

Based on your industry and culture, you can disable features on the device that make sense. For example, disabling the camera may be required for your company due to sensitivity of your products. Backing up documents to iCloud may violate regulations for your industry.

Understand that disabling items like the camera may have a significant impact on device usability, so they should be used only as necessary.

Manage > Manage Device Policies > Device Restrictions

Setting	Control
Enable Background Data Synchronization	User Controlled
Auto-Sync	User Controlled
Allow Installation of Non-Google Play Applications	User Controlled
Camera	Enabled
Bluetooth	User Controlled
Allow USB Mass Storage	User Controlled
Near Field Communication (NFC)	User Controlled
Use Network-provided Date & Time	User Controlled
Location Detection Policies	
Use Wireless Networks / Google's Location Service for Location Detection	User Controlled
Use GPS satellites for Location Detection	User Controlled
Allow Mock Locations	User Controlled

See the video here:

<https://supportforums.cisco.com/community/netpro/solutions/mcms>

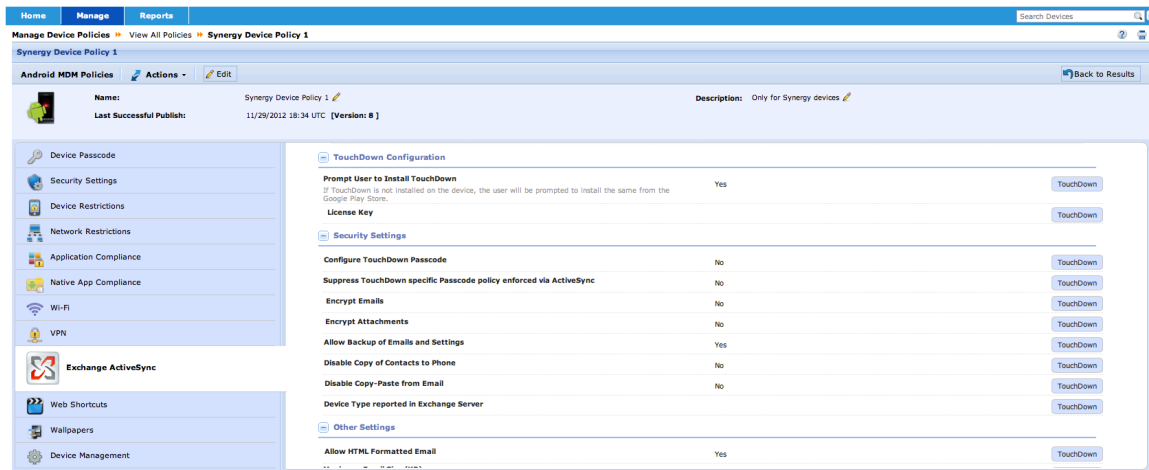
Best Practice #7 – Configuring Email for Users

Email is likely the #1 item that end users want access to, and many companies have found ways to provide access to these users already. However, while using the native email client on iOS devices is relatively straight forward, it is not as easy on Android. Our recommendation is to use NitroDesk's TouchDown client on Android devices. TouchDown allows for several features that the native clients generally do not: encryption, security, and a consistent user experience across devices.

1. Block Native email client
2. Block Gmail
3. Require TouchDown on users devices
4. Encrypt emails
5. Encrypt attachments

TouchDown configuration is actually managed from the ActiveSync settings.

Manage > Manage Device Policies > Exchange ActiveSync



See the video here:

<https://supportforums.cisco.com/community/netpro/solutions/mcms>

Best Practice #8 – Web Browsing

In general, web browsing is considered a must have, but there are a few items to consider:

1. Leave fraud warnings on
2. Block pop-ups
3. Accept cookies only from visited sites

If web browsing is of the highest concern you may disable it all together.

See the video here:

<https://supportforums.cisco.com/community/netpro/solutions/mcms>

Best Practice #9 – Mobile Applications

On mobile devices, applications are king. They are the very reason that mobile devices have exploded in popularity. However, they can also pose a security threat to your organization. You have two main options when it comes to apps.

1. Creating an Application Store or application catalog for your company. This can be suggested applications that are public, or applications that are created in house.
2. Create a list of required apps. When a device is enrolled, these applications will be required to be installed on the device, ensuring a uniform deployment across your company.

You can also create a list of applications that are disallowed.

App	Platform	Target Devices	Status	Date	Distribution Name	Distributed By	Send Email Notification	Action
Metropacme	Device - Rajeev iPhone		Published	10/17/2012 22:35 UTC	Distribute Metropacme to Rajeev iPhone - 10/17/2012 22:35 UTC	rkurana000@y...	No	✖
Anovy Birds	Device - rajekhur-GT-P7510		Published	10/17/2012 22:28 UTC	Distribute Anovy Birds to rajekhur-GT-P7510 - 10/17/2012 22:28 UTC	rkurana000@y...	Yes	✖
Anovy Birds	All Devices		Published	10/15/2012 23:52 UTC	Distribute Anovy Birds to All Devices - 10/15/2012 23:52 UTC	rkurana000@y...	No	✖
Tic Tac Toe Free	Device - mcgiffin-Blaze Tablet		Published	10/15/2012 20:10 UTC	Distribute Tic Tac Toe Free to mcgiffin-Blaze Tablet - 10/15/2012 20:10 UTC	master_rajekhur	Yes	✖
Maas360 for iOS	All Devices		Published	10/09/2012 22:27 UTC	Distribute Maas360 for iOS to All Devices - 10/09/2012 22:27 UTC	rkurana000@y...	No	✖
Cisco AnyConnect	All Devices		Published	10/09/2012 22:26 UTC	Distribute Cisco AnyConnect to All Devices - 10/09/2012 22:26 UTC	rkurana000@y...	No	✖
Samsung AnyConnect	All Devices		Published	09/21/2012 19:38 UTC	Distribute Samsung AnyConnect to All Devices - 09/21/2012 19:38 UTC	master_rajekhur	Yes	✖
Cisco WebEx Meetings	All Devices		Published	09/21/2012 19:36 UTC	Distribute Cisco WebEx Meetings to All Devices - 09/21/2012 19:36 UTC	master_rajekhur	Yes	✖
AppIQ	All Devices		Published	09/21/2012 19:07 UTC	Distribute AppIQ to All Devices - 09/21/2012 19:07 UTC	master_rajekhur	Yes	✖
Cisco WebEx Meetings	All Devices		Published	08/13/2012 21:17 UTC	Distribute Cisco WebEx Meetings to All Devices - 08/13/2012 21:17 UTC	rkurana000@y...	Yes	✖
Metropacme	All Devices		Published	08/13/2012 21:16 UTC	Distribute Metropacme to All Devices - 08/13/2012 21:16 UTC	rkurana000@y...	Yes	✖
Cisco Jabber IM for iPhone	All Devices		Published	08/13/2012 21:14 UTC	Distribute Cisco Jabber IM for iPhone to All Devices - 08/13/2012 21:14 UTC	rkurana000@y...	Yes	✖

See the video here:

<https://supportforums.cisco.com/community/netpro/solutions/mcms>

Best Practice #10 – Distribute Wi-Fi, VPN and Passcode settings

Many corporations use uniform VPN, Wi-Fi and Passcode policies across the business. To simplify the configurations of these, MCMS can push out policies for them to make your deployment much more uniform. If someone leaves the company the policies can later be revoked.

Home	Manage	Reports
Manage Device Policies >> View All Policies >> Synergy Device Policy 1		
Synergy Device Policy 1		
Android MDM Policies Actions Edit		
Name: Synergy Device Policy 1 Last Successful Publish: 11/29/2012 18:34 UTC [Version: 8]		Description: Only for Synergy devices
<ul style="list-style-type: none"> Device Passcode Security Settings Device Restrictions Network Restrictions Application Compliance Native App Compliance Wi-Fi VPN Exchange ActiveSync Web Shortcuts Wallpapers Device Management 	Wi-Fi Profile <hr/> Service Set Identifier (SSID) Non-Broadcast SSID: No Wi-Fi Configuration Type Encryption Key EAP Authentication Protocol Phase 2 Authentication Protocol CA Certificate Upload certificates using the Manage Policy Files workflow and then select the required certificate here. Identity Certificate Authentication Username Use %username% for user's corporate credentials. Authentication Domain Use %domain% for user's corporate credentials. Anonymous Identity Authentication Password Use %password% for user's corporate credentials.	

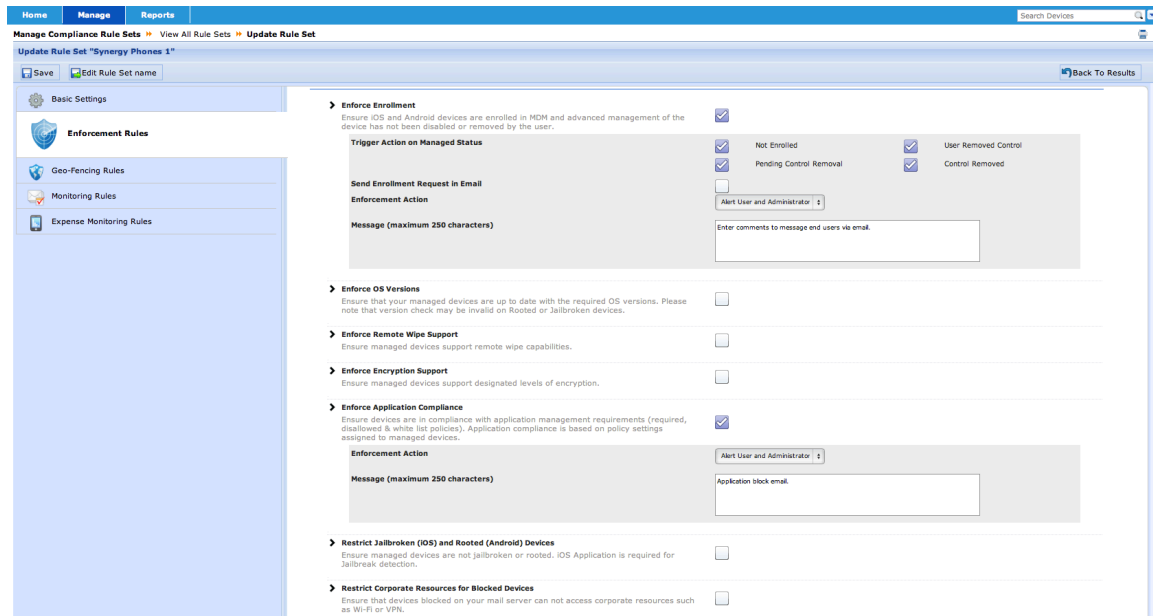
See the video here:

<https://supportforums.cisco.com/community/netpro/solutions/mcms>

Best Practice #11 – Warn Before Revoking

If a user goes out of compliance, you can set tiers of remediation before having to revoke access or wiping a device. In many cases, giving a user some extra time will prevent unwanted support calls.

MCMS has a robust compliance engine that allows you to set many different types of compliance. Choose the one that makes the most sense for you.



See the video here:

<https://supportforums.cisco.com/community/netpro/solutions/mcms>

Best Practice #13 – Test Your Policies

Like any good deployment, you should first test the policies on a subset of devices before applying globally. MCMS allows you to create many different groups of devices and policies to deploy into test groups prior to major rollouts.

See the video here:

<https://supportforums.cisco.com/community/netpro/solutions/mcms>

Best Practice #14 – Cisco Desk Phones

If you are deploying Cisco MCMS to Cisco devices powered by Android, there are a few areas of overlapping features that need to be understood. Cisco desk phones are largely controlled and deployed by Cisco Unified Communications Manager (CUCM), which has some very basic MDM functions native. Those features include:

- Require Screen Lock / PIN
- Screen Lock Timer

- Remote Lock
- Remote Full Wipe
- Application Push
- Allow Applications from Google Play
- WiFi and Bluetooth

These MDM features are pushed via TFTP configuration file to the desk phones, along with other configuration settings. If the device is not connected to the CUCM server (though it may have internet connectivity) the policies will not be pushed, however, there is no requirement that the device is registered to CUCM for MCMS to work.

It is recommended that if you are using MCMS and Cisco Android devices that you:

- 1) Use CUCM to push the least secure settings required for the Cisco devices.
Note: In this scenario you will essentially have two MDM providers (CUCM and MCMS). The most secure policy pushed will take priority. If you set CUCM to the maximum security setting, you will have little room for changes to those devices. Example: the PIN requirement for executives is six digits, and zero for the lobby phones. If you set 6 on the lobby phones from CUCM, and try to push a policy of zero from MCMS, it will have no effect.
(PIN FROM CUCM IS 4 DIGITS)
- 2) Create a separate policy group for Cisco devices
- 3) Enroll the devices into this policy group
- 4) Use MCMS when possible to manage Cisco Android devices – this assumes that desk phones have Google Play access
- 5) Use MCMS to create an application store for Cisco Android devices

Creating policies and enrolling Cisco Android devices is no different than other Android based devices. By using MCMS to manage the Cisco Android devices you will get positive notification that policies have been accepted, that the device is active, and that it is not out of compliance.

Creating MDM Policies from CUCM

These settings are located at:

Within CUCM

Device > Phone

Product Specific Configuration Layout ? Param Override Common Settings

Disable Speakerphone
 Disable Speakerphone and Headset
 Disable USB

SDIO* Disabled

Bluetooth* Enabled

Days Display Not Active Sunday
Monday
Tuesday
Wednesday

Display On Time 07:30

Display On Duration 10:30

Display Idle Timeout 01:00

Display On When Incoming Call* Enabled

Enable Power Save Plus Sunday
Monday
Tuesday
Wednesday

Phone On Time 00:00

Phone Off Time 24:00

Phone Off Idle Timeout* 60

Enable Audible Alert
 EnergyWise Domain
 EnergyWise Endpoint Security Secret
 Allow EnergyWise Overrides

RTCP* Disabled

Advertise G.722 and iSAC Codecs* Use System Default

Video Calling* Enabled

Wifi* Enabled

PC Port* Enabled

Span to PC Port* Disabled

PC Voice VLAN Access* Enabled

PC Port Remote Configuration* Disabled

Switch Port Remote Configuration* Disabled

Detect Unified CM Connection Failure* Normal

Gratuitous ARP* Disabled

Gratuitous ARP*	Disabled	<input type="checkbox"/>
Cisco Discovery Protocol (CDP): Switch Port*	Enabled	<input type="checkbox"/>
Cisco Discovery Protocol (CDP): PC Port*	Enabled	<input type="checkbox"/>
Link Layer Discovery Protocol - Media Endpoint Discover (LLDP-MED): Switch Port*	Enabled	<input type="checkbox"/>
Link Layer Discovery Protocol (LLDP): PC Port*	Enabled	<input type="checkbox"/>
LLDP Asset ID		<input type="checkbox"/>
LLDP Power Priority*	Unknown	<input type="checkbox"/>
Power Negotiation*	Enabled	<input type="checkbox"/>
Automatic Port Synchronization*	Disabled	<input type="checkbox"/>
802.1x Authentication*	User Controlled	<input type="checkbox"/>
<input type="checkbox"/> Always On VPN		<input type="checkbox"/>
<input checked="" type="checkbox"/> Allow User-Defined VPN Profiles		<input type="checkbox"/>
Require Screen Lock*	PIN	<input type="checkbox"/>
Screen Lock Timeout*	900	<input checked="" type="checkbox"/>
Lock Device During Audio Call*	Disabled	<input type="checkbox"/>
Lock Device*	Disabled	<input type="checkbox"/>
Wipe Device*	Disabled	<input type="checkbox"/>
Kerberos Server		<input type="checkbox"/>
Kerberos Realm		<input type="checkbox"/>
Load Server		<input type="checkbox"/>
Peer Firmware Sharing*	Enabled	<input type="checkbox"/>
Log Server		<input type="checkbox"/>
Web Access*	Disabled	<input type="checkbox"/>
SSH Access*	Enabled	<input checked="" type="checkbox"/>
Android Debug Bridge (ADB)*	Enabled	<input checked="" type="checkbox"/>
Multi-User*	Enabled	<input type="checkbox"/>
Allow Applications from Unknown Sources*	Enabled	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Allow Applications from Android Market		<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Allow Applications from Cisco AppHQ		<input checked="" type="checkbox"/>
AppHQ Domain		<input type="checkbox"/>
<input type="checkbox"/> Enable Cisco UCM App Client		<input type="checkbox"/>
Company Photo Directory		<input type="checkbox"/>
Voicemail Server (Primary)	utc-sjcvtg-011.cisco.com	<input checked="" type="checkbox"/>
Voicemail Server (Backup)		<input type="checkbox"/>

Note: If you do NOT enable Allow Applications from Android Market you cannot manage your devices with MCMS.

Creating MDM policies in MCMS

The same set of policy settings are available within MCMS:

Manage > Manage device Policies > Device passcode (Pin, Idle Timer)

Manage > Manage device Policies > Device restrictions (Wi/Fi and Bluetooth)

Manage > Manage device Policies > Native app compliance (Google Play restriction)

Home Manage Reports

Manage Device Policies View All Policies Synergy Device Policy 1

Synergy Device Policy 1

Android MDM Policies Actions Edit

Name: Synergy Device Policy 1 Description: Only for Synergy devices

Last Successful Publish: 11/29/2012 18:34 UTC [Version: 8]

Device Passcode

Configure Passcode Policy Select this option to enforce the use of a Passcode before using the mobile device. Yes

Passcode Settings

Passcode Quality	Numeric
Minimum Passcode Length (4-16 characters)	6
Maximum Passcode Age (in Days)	60
Allowed Idle Time (in minutes) Before Auto-Lock	30 minutes
Passcode history	
Number of Failed Passcode Attempts Before All Data is Erased (4-16)	10

Home Manage Reports

Manage Device Policies View All Policies Synergy Device Policy 1

Synergy Device Policy 1

Android MDM Policies Actions Edit

Name: Synergy Device Policy 1 Description: Only for Synergy devices

Last Successful Publish: 11/29/2012 18:34 UTC [Version: 8]

Device Feature Restrictions

Enable Background Data Synchronization User Controlled

Auto-Sync User Controlled

Allow Installation of Non-Google Play Applications User Controlled

Camera Enabled

Bluetooth User Controlled

Allow USB Mass Storage User Controlled

Near Field Communication (NFC) User Controlled

Use Network-provided Date & Time User Controlled

Location Detection Policies

Use Wireless Networks / Google's Location Service for Location Detection User Controlled

Use GPS satellites for Location Detection User Controlled

Allow Mock Locations User Controlled

Home Manage Reports

Manage Device Policies View All Policies Synergy Device Policy 1

Synergy Device Policy 1

Android MDM Policies Actions Edit

Name: Synergy Device Policy 1 Description: Only for Synergy devices

Last Successful Publish: 11/29/2012 18:34 UTC [Version: 8]

Native App Compliance

Allow Google Play	Yes
Allow Youtube App	Yes
Allow Email	Yes
Allow Browser	Yes
Allow Settings	Yes
Allow Gallery	Yes
Allow Gmail	Yes
Allow Google Maps & Navigation	Yes

See the video here:

<https://supportforums.cisco.com/community/netpro/solutions/mcms>

Best Practice #15 – Pushing MCMS from CUCM Server

CUCM (Cisco Unified Communications Manager) has the capability to push applications to Cisco endpoints, including Android based devices. One of the

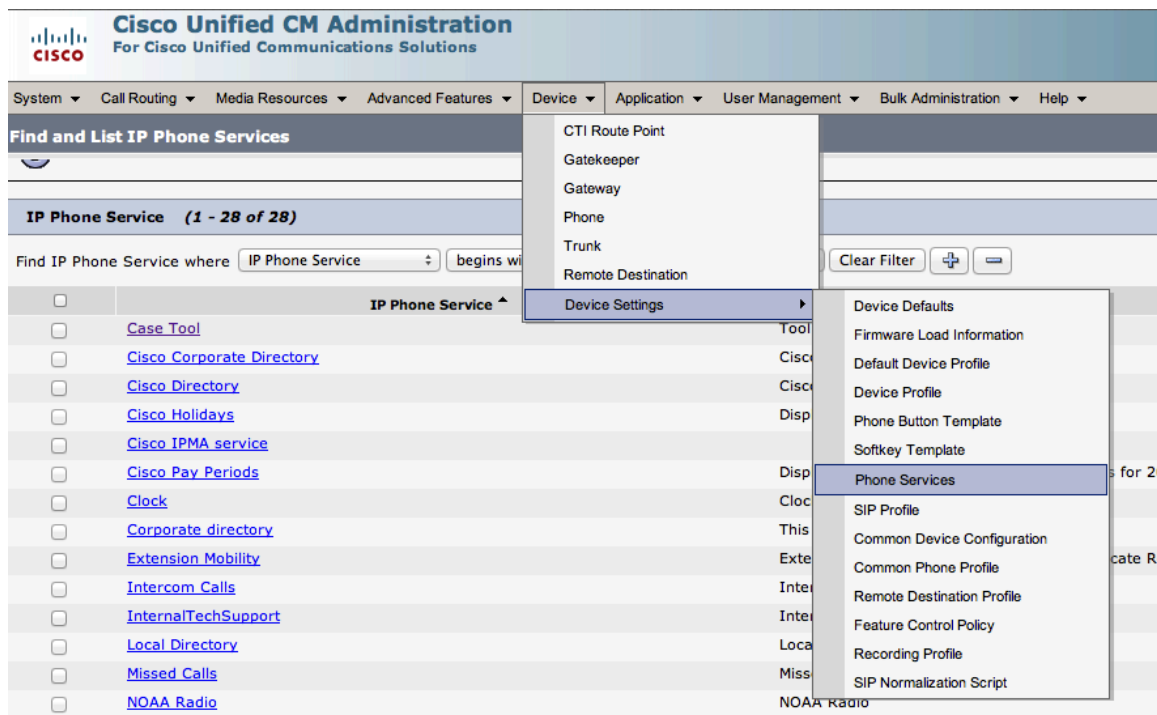
applications that can be pushed is the MCMS application. This is particularly useful if Google Play has been disabled on those devices.

The first step is to load the MCMS Android application onto a web server. You should validate that you can download the file via HTTP from the web server before providing the information to CUCM.

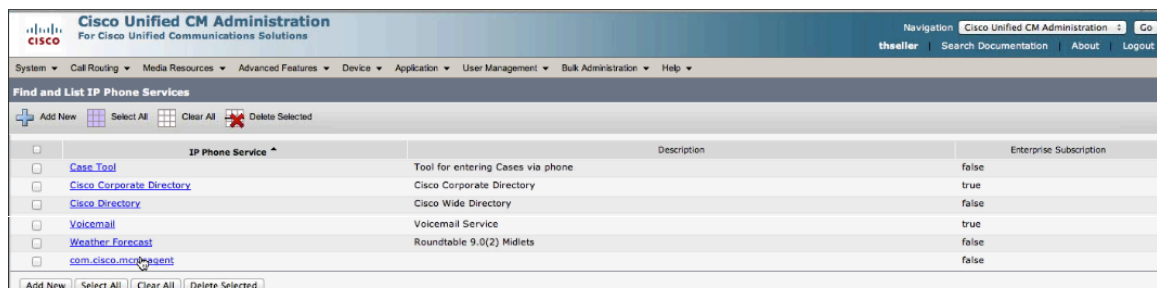
To push an application out to an Android based Cisco phone, you will need to configure the application as a service, from the IP Phone Services Configuration screen. Prior to this you will first need to add a new IP Phone Service.

To add a new IP Phone Service go to:

Device > Device Settings > Phone Services



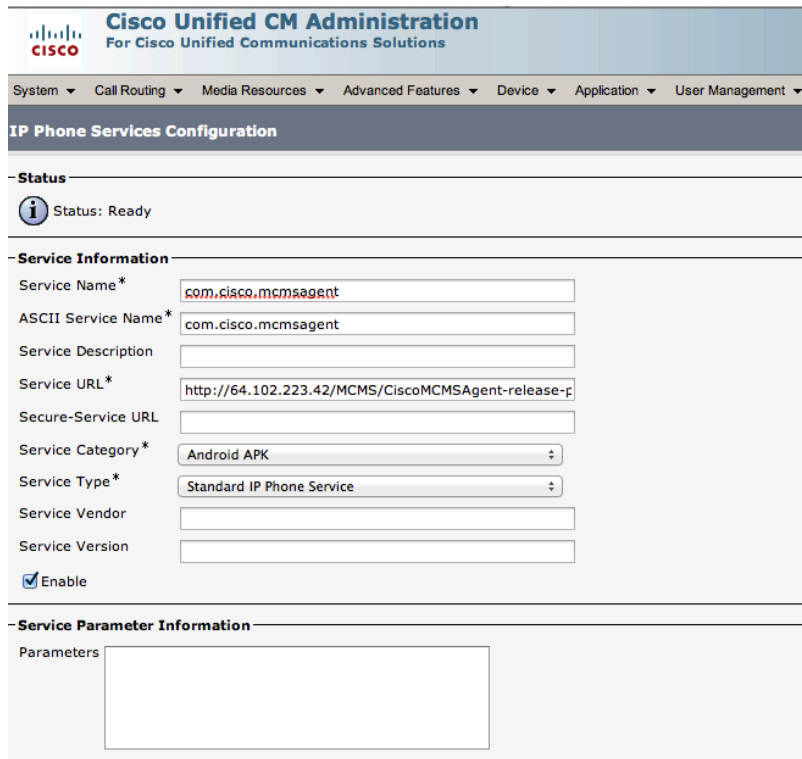
From this screen click “Add New” at the bottom.



Now you can configure the IP Phone Service for the MCMS application. To do so you will need to fill in the following information:

Service Name*: com.cisco.mcmsagent
ASCII Service Name: com.cisco.mcmsagent
Service Description: <blank>
Service URL: <http://<thehttplinktothemcmsapplicationhere>>
Secure-Service URL: <blank>
Service Category: Android APK
Service Type: Standard IP Phone Service
Service Vendor: <blank>
Service Version: <blank>
Enable: Check this box
Parameters: <blank>

As shown in the picture below.



The screenshot shows the Cisco Unified CM Administration interface for IP Phone Services Configuration. The page title is "Cisco Unified CM Administration For Cisco Unified Communications Solutions". The navigation menu includes System, Call Routing, Media Resources, Advanced Features, Device, Application, and User Management. The main heading is "IP Phone Services Configuration".

Status
Status: Ready

Service Information

Service Name*	com.cisco.mcmsagent
ASCII Service Name*	com.cisco.mcmsagent
Service Description	
Service URL*	http://64.102.223.42/MCMS/CiscoMCMSAgent-release-p
Secure-Service URL	
Service Category*	Android APK
Service Type*	Standard IP Phone Service
Service Vendor	
Service Version	

Enable

Service Parameter Information

Parameters

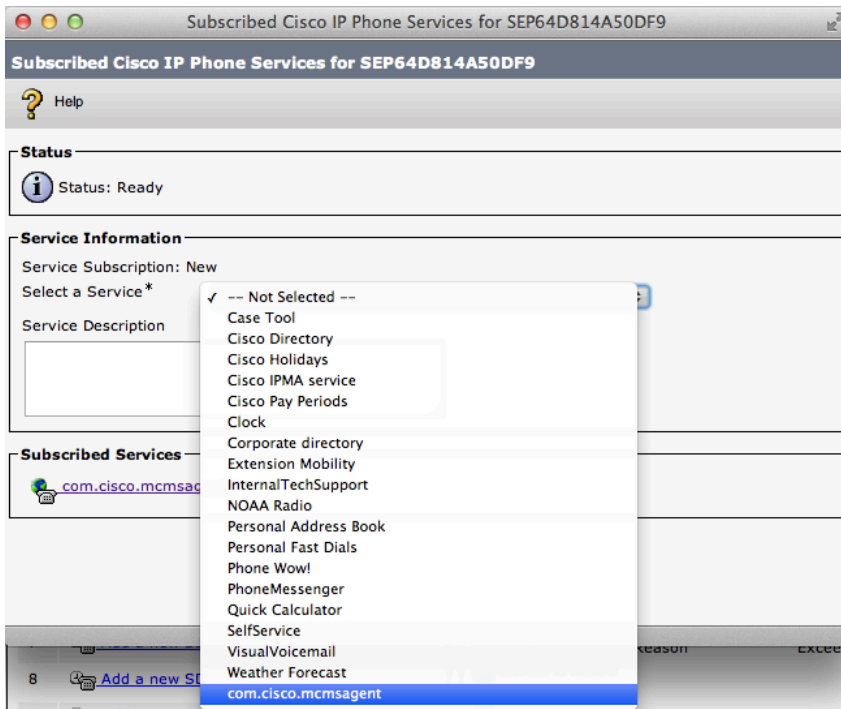
You will now need to add this IP Phone Service to the users device. To access this, go to:

Device > Phone > (search phone here)

Under the Related Links section, scroll down to Subscribe/Unsubscribe Services as shown below.



Find the service from the list under Select a Service.



To force the device to install the application, Reset the phone. This will allow it to get a new TFTP file with the required instructions to install the MCMS application.