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 brining 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.

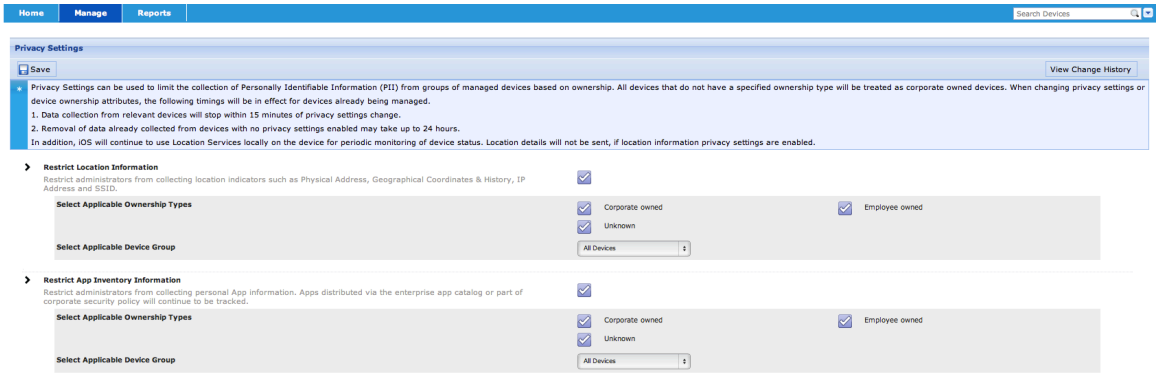
Best Practice #1 – Have a Corporate Owned Device policy

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



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:

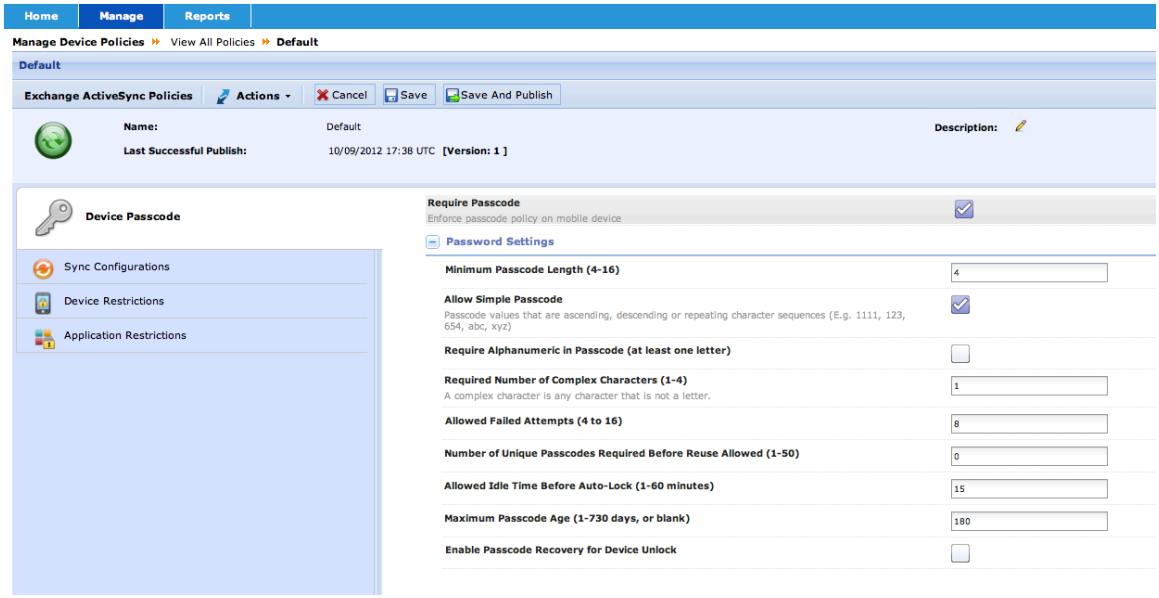
Name	Description	Example
Simple	Repeating, ascending or descending values	12345 abcde
Numeric	Requires at least one number	1abc 11111
Alphanumeric	Requires at least one number and one letter	1abc abc123
Complex	Requires at least one number, one letter, and one special character	124$ abc$ 1abc$
Pattern	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



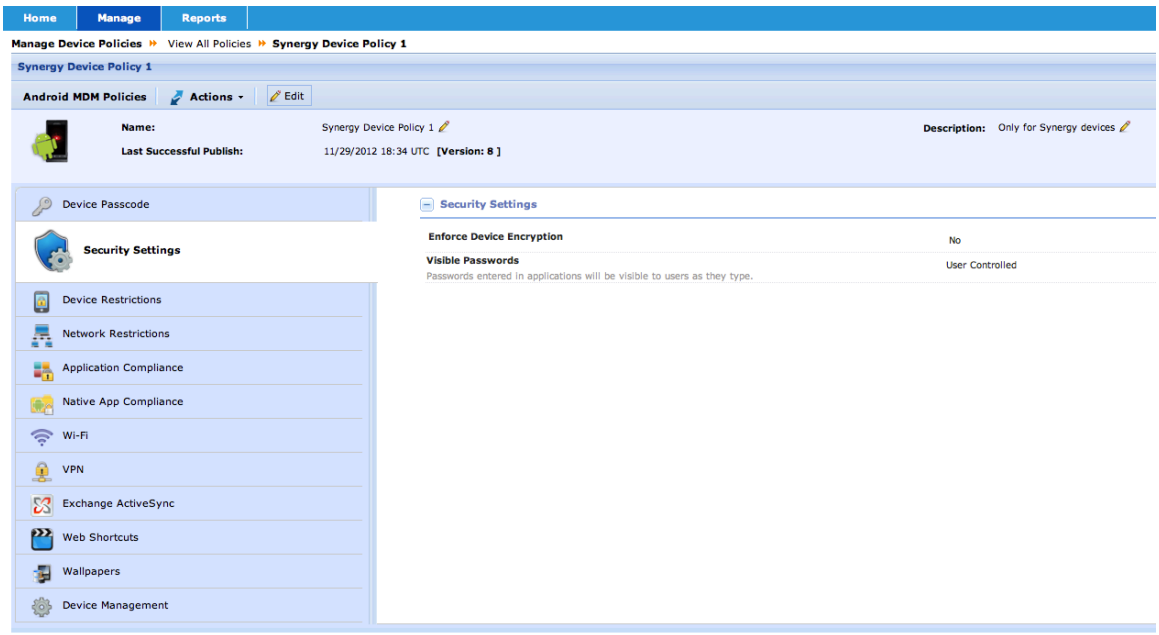
See the video here:
https://supportforums.cisco.com/community/netpro/solutions/mcms

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



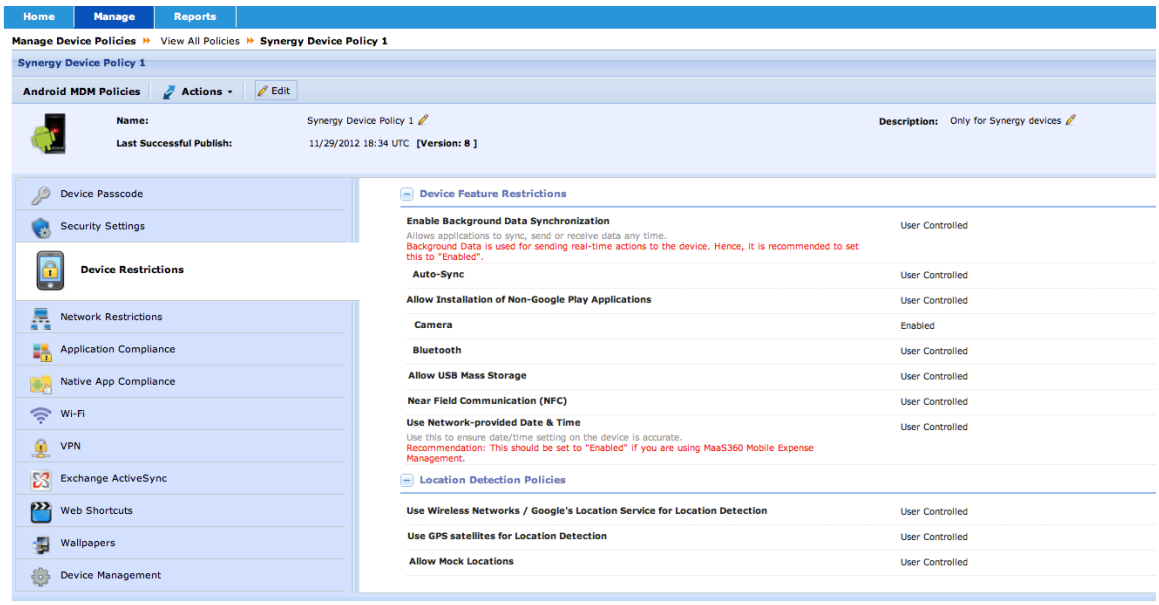
See the video here:
https://supportforums.cisco.com/community/netpro/solutions/mcms

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



See the video here:
https://supportforums.cisco.com/community/netpro/solutions/mcms

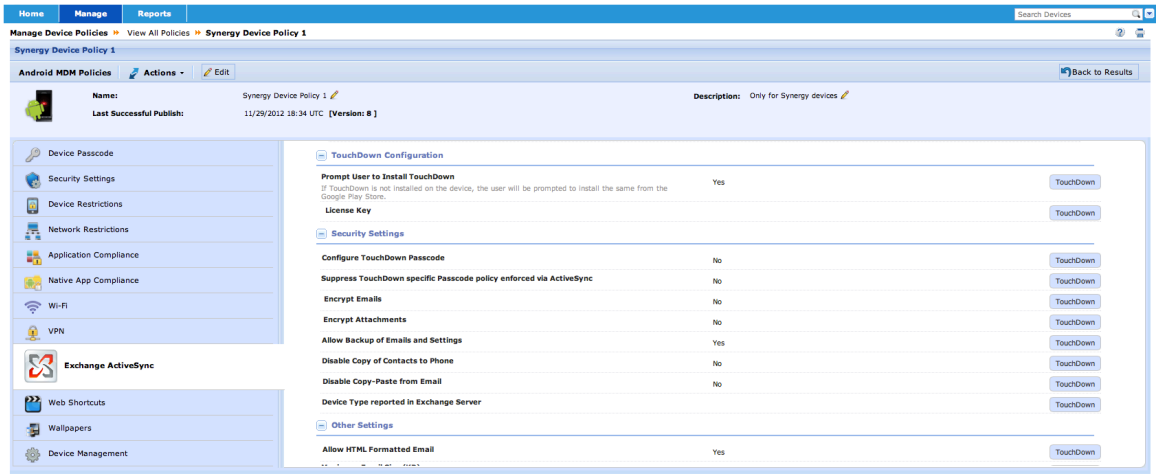
Best Practice #7 – Configuring Email for Users

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.

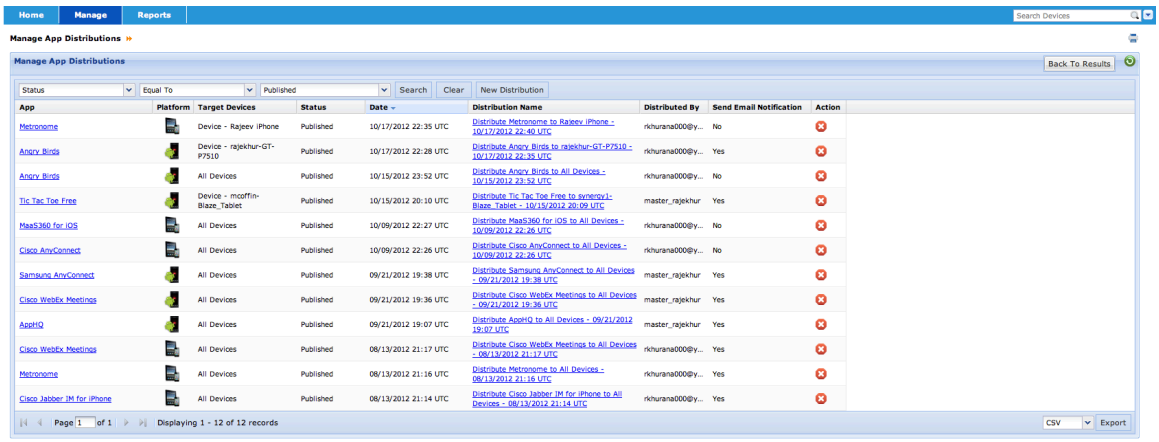
See the video here:
https://supportforums.cisco.com/community/netpro/solutions/mcms

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.

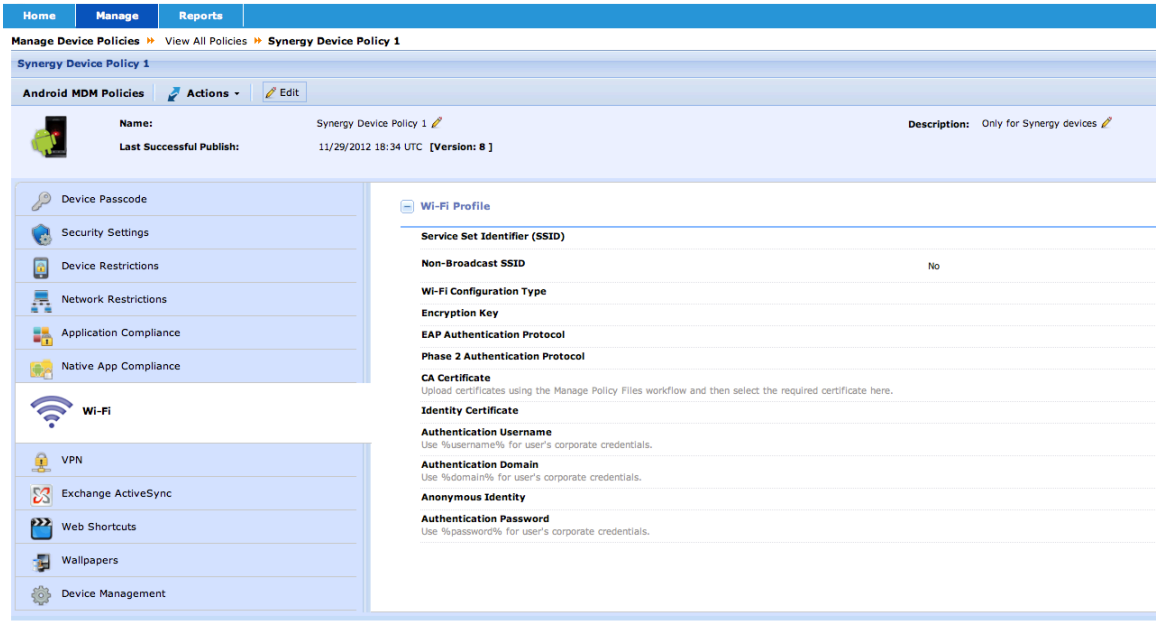
You can also create a list of applications that are disallowed.



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.

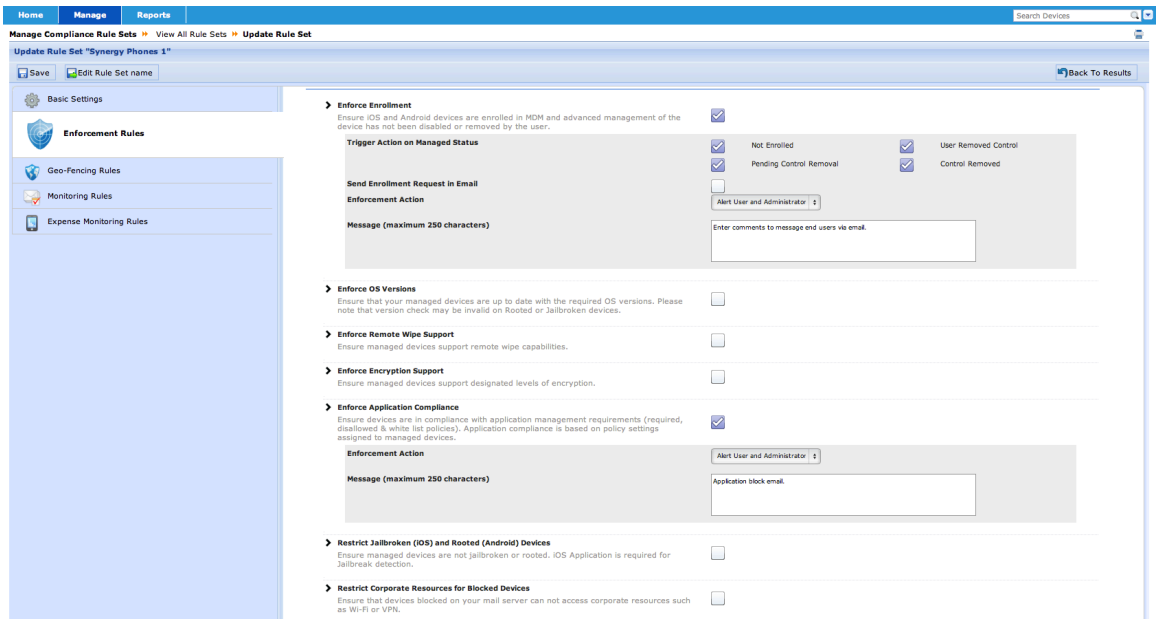


See the video here:
https://supportforums.cisco.com/community/netpro/solutions/mcms

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:

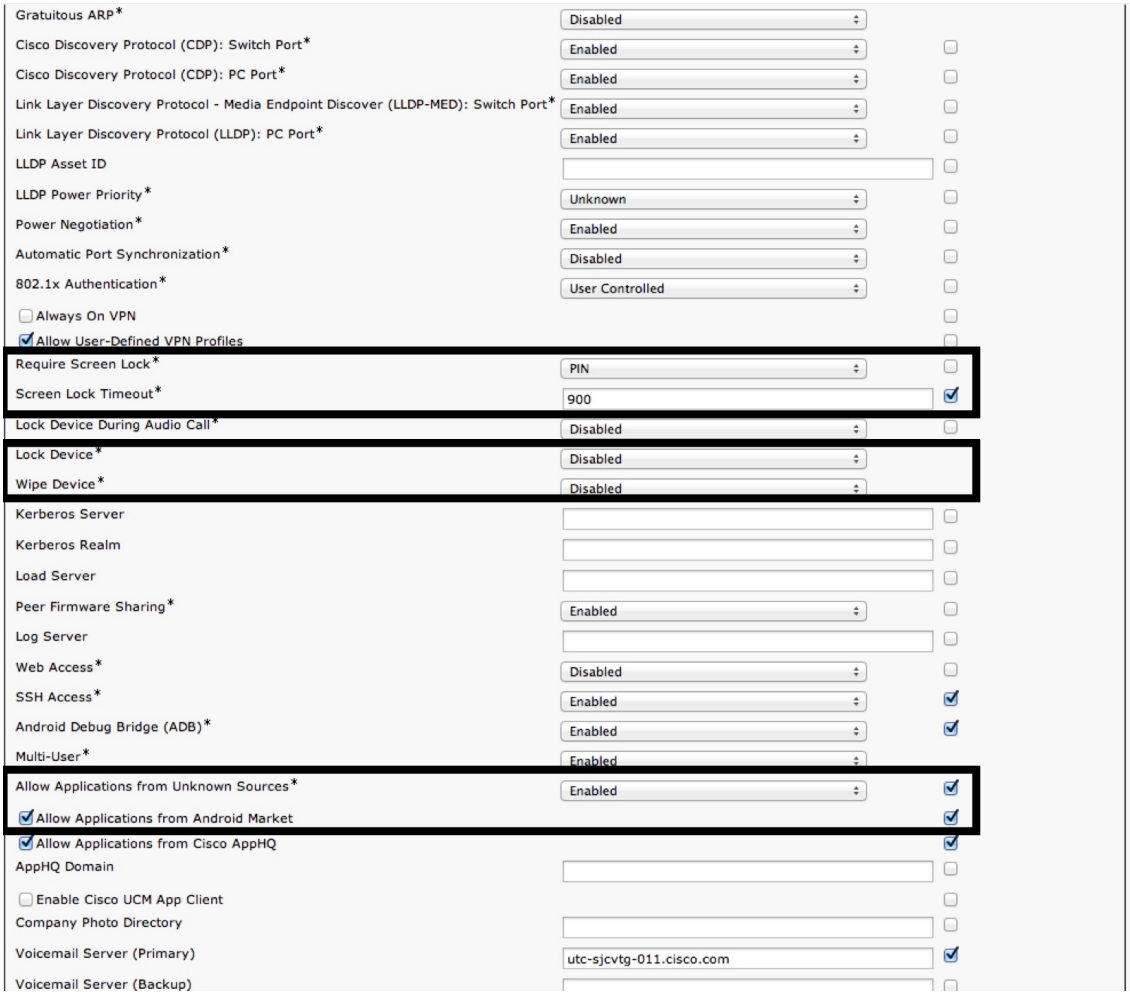
1) Use CUCM to push the least secure settings required for the Cisco devices. Note: In this scenario you will essentially have two MDM providers (CUCM and MCMS). The most secure policy pushed will take priority. If you set CUCM to the maximum security setting, you will have little room for changes to 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

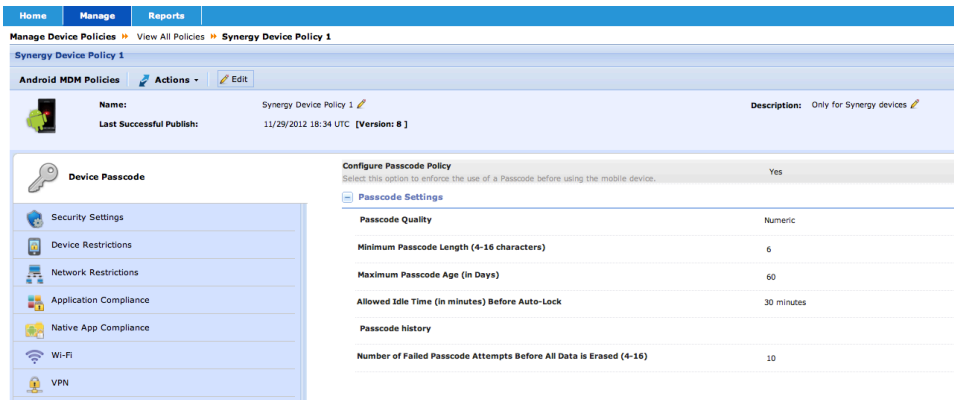
	Param	Override Common Settings
Disable Speakerphone		
Disable Speakerphone and Headset		
Disable USB		
SDIO*	Disabled	
Bluetooth*	Enabled	
Days Display Not Active	Sunday Monday Tuesday Wednesday	
Display On Time	07:30	
Display On Duration	10:30	
Display Idle Timeout	01:00	
Display On When Incoming Call*	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	

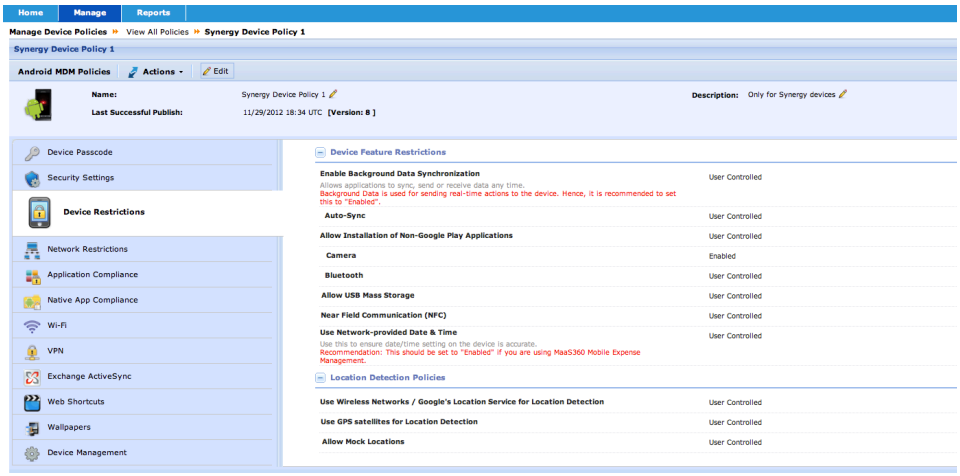


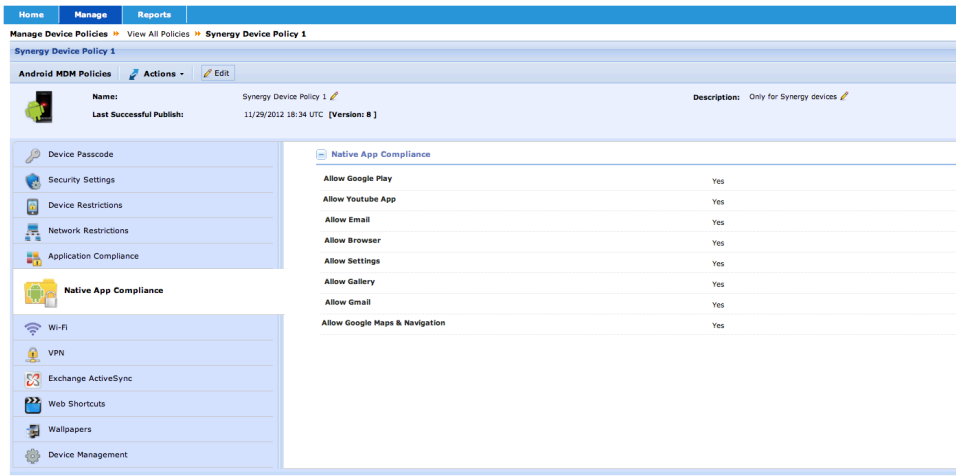
Note: If you do NOT enable Allow Applications from Android Market you cannot manage your devices with MCMS.

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)







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

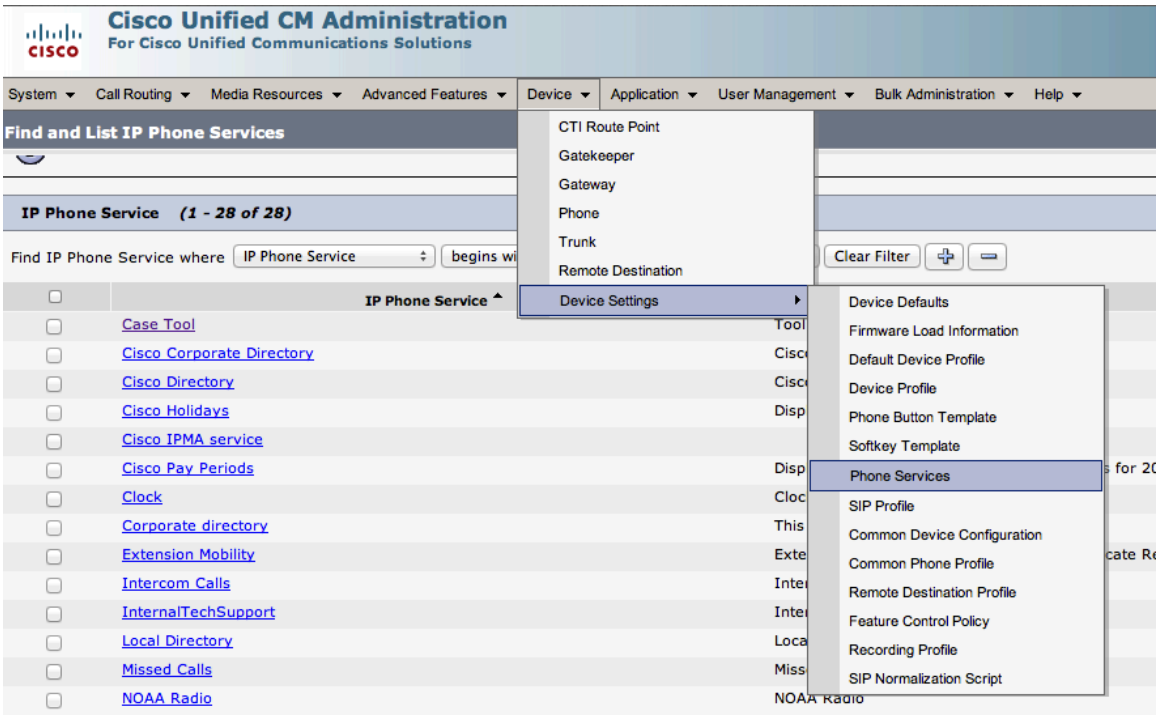
applications that can be pushed is the MCMS application. This is particularly useful if Google Play has been disabled on those devices.

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.

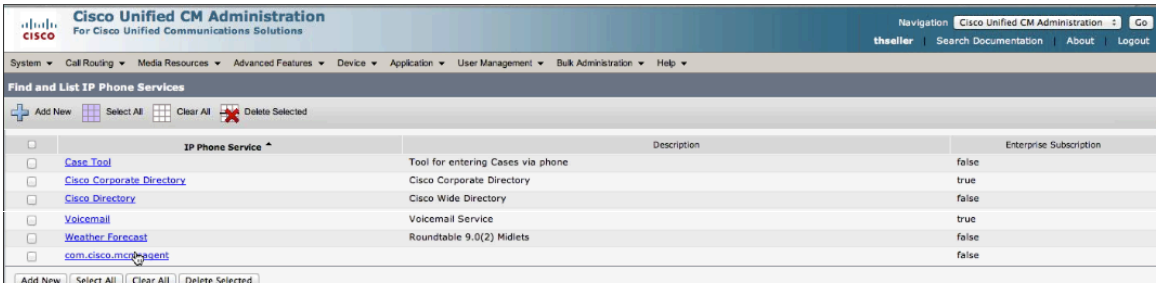
To push an application out to an Android based Cisco phone, you will need to configure the application as a service, from the IP Phone Services Configuration screen. Prior to this you will first need to add a new IP Phone Service.

To add a new IP Phone Service go to:

Device > Device Settings > Phone Services



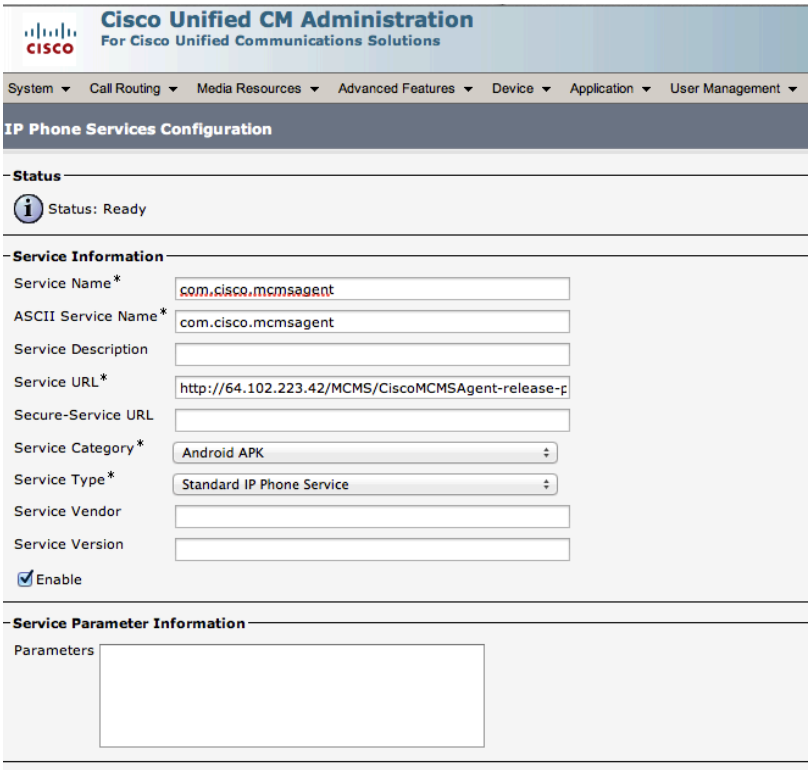
From this screen click “Add New” at the bottom.



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.

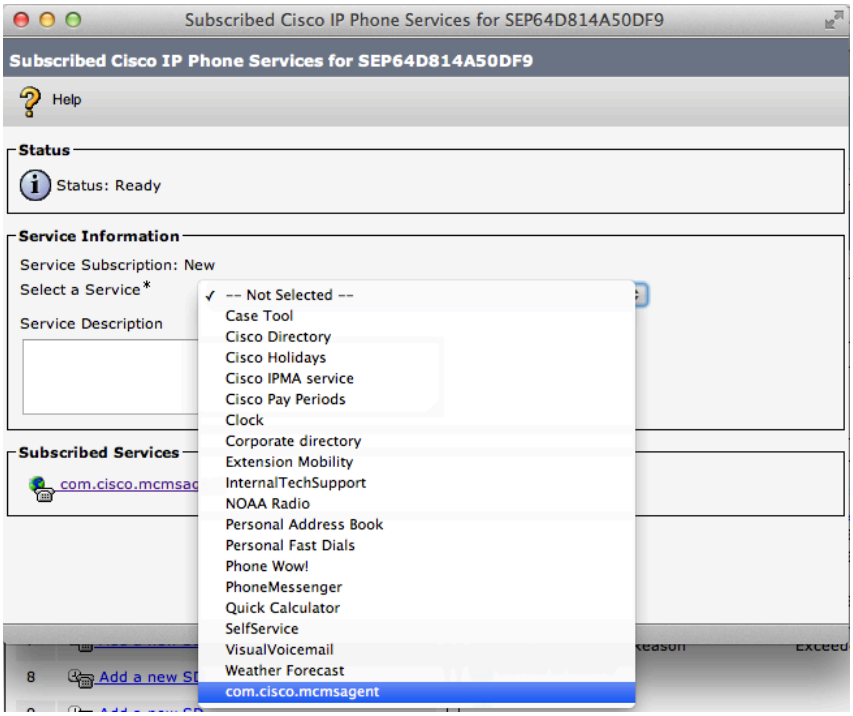


You will now need to add this IP Phone Service to the users device. To access this, go to:

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.