Microworld

eScan Antivirus

Documentation

On

Mobile Device Management

For iOS

Guided By : Raja Sir

Prepared By : Vaibhav Pawar & Sunil Bansode

Index

Summary

eScan MDM simplifies the work of administrators by using a single console to manage iOS mobile devices. eScan MDM can be used to deploy configuration settings, security commands and retrieve asset data over-the-air (OTA).

This Documentation will give you a brief idea about working of eScan Mobile Device Management For iOS.

The basic functionality of this Project is:

- To Add New iOS Device in Managed Devices
- Read and Deploy various policies for selected group or selected devices

Supported Operating System

iOS version 6.0 and above

Supported Devices (iOS)

1. iPhones
2. iPad
3. iPod Touch

Management Operations

1. Enabling Passcode
2. Imposing Restrictions
3. Configuring Emails
4. VPN Settings
5. WiFi Settings
6. Web Clips

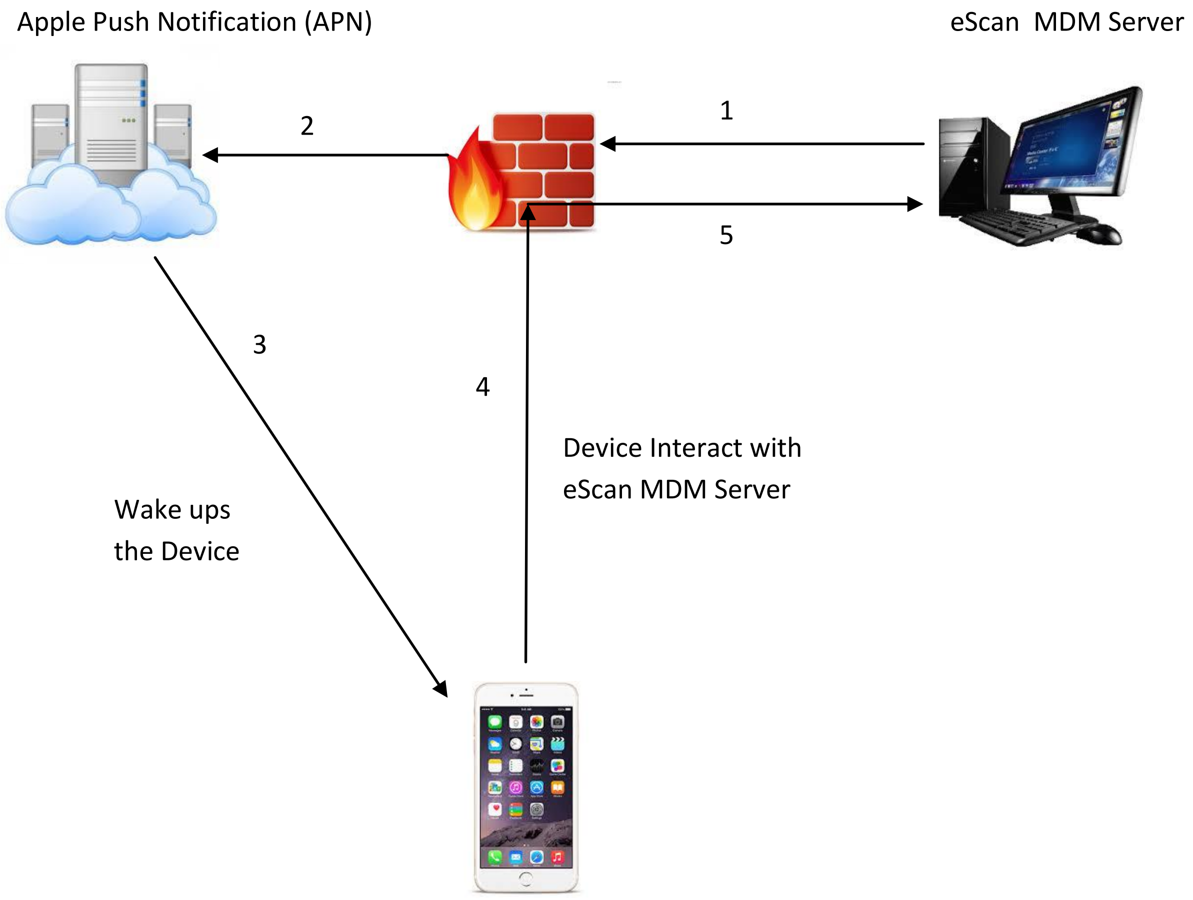
Security Commands

1. Erasing the device data
2. Blocking device
3. Clearing the Passcode

Asset Information

1. Security Details
2. Device Information

MDM Architecture



All Communications from eScan MDM to the managed iOS device will be routed through Apple Push Notification Service (APNs). A live TCP connection is maintained for intermediate service. APNs acts an intermediate wake up service to wake up the device whenever an action is triggered to be performed from the eScan MDM. Managed mobile device communicates with eScan MDM to receive the instructions and report back the status and data.

Requirements

1. Apache should be configured with https
2. Cfgprofiler.dll
3. Latest eserv.exe
4. iOSEnroll.dll
5. Default profile (policy.mobileconfig)
6. Latest mwconsole.dll , htmls & icons

Apache Configuration

- **For Httpd.conf**

Stop eScan-Apache Service using Service Control Window

Modify httpd.conf file located at path
 "c:\program files\common files\microworld\apache2\conf\httpd.conf"
Path for 64Bit
 "c:\program files <x86>\common files\microworld\apache2\conf\httpd.conf"
Note: Take backup of file before Modifying

Add

Listen 10443

Listen 2221

Listen 443

Locate the below mentioned lines in the conf and remove the preceding #

```
#LoadModule ssl_module modules/mod_ssl.so
```

Modify

"c:\program files\common files\microworld\apache2\conf\apache_escan_vhost.conf"

Path for 64Bit

c:\program files <x86>\common files\microworld\apache2\conf\apache_escan_vhost.conf")

Note: Take backup of file before Modifying

Locate the below mentioned lines in the conf and remove the preceding #

```
#SSLPassPhraseDialog  builtin
#SSLSessionCache none
#SSLMutex default
#SSLRandomSeed startup builtin   (In apache_escan_vhost.conf )
#SSLRandomSeed connect builtin  (In apache_escan_vhost.conf )
#SSLEngine on
#SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
#SSLCertificateFile bin/ssl/webconsole.cer
#SSLCertificateKeyFile bin/ssl/webconsole.key
#SSLCACertificateFile bin/ssl/ca.cer
#SSLOptions +StdEnvVars
```

Launch Command prompt with Administrator priviliage and go to directory

"c:\program files\common files\microworld\apache2\bin\SSl"

For 64Bit path

c:\program files <x86>\common files\microworld\bin\SSL

and check if file webconsole.cer, webconsole.key, ca.cer is created or not during installation

If any of the above file is missing you need to regenerate SSL certificate

Execute/run the file ssl_cert.exe to generate self-signed certificates necessary for SSL from directory

"c:\program files\common   files\microworld\apache2\bin"

For 64Bit path "c:\program files <x86>\common files\microworld\bin\SSL”

Note: If ssl_cert.exe file is not present, kindly download from below link
http://www.microworldsystems.com/download/tools/ssl_cert.exe

8. Pause eScan Protection and go to directory "c:\program files\escan" (For 64Bit default path="c:\program files <x86>\eScan")
Open eserv.ini and change the value of UseHTTPs from "0" to "1" in Config Section.

Restart eScan management console service from command prompt using following 2 commands

```
i) killproc eserv.exe,trayeser.exe
ii) net start escan-eserv
```

9. Locate “Insert Virtual Hosts Conf file entry below this line”
Add new line at last
“Include conf/apache_ios_updater.conf”

10. Start escan-Apache Service

11. Browse to https://localhost:10443 or https://ipaddress:10443 and add the Self-Signed certificate to the ssl-store of the browser.

For apache_escan_vhost.conf

Locate <IfModule alias_module> and add following lines,

```
Alias  /setup/ "C:/PROGRA~1/eScan/setup/"
Alias /app/ "C:/PROGRA~1/eScan/App/"
Alias /iOS/ "C:/PROGRA~1/eScan/iOS/"
Alias /config C:/pub/ios/setup

<Directory C:/pub/ios/setup>
    Order allow,deny
    Allow from all
</Directory>
```

For apache_ios_updater.conf

- Save copy of “apache_escan_vhost.conf “ as “apache_ios_updater.conf”
- Locate and do following changes step by steps
- NameVirtualHost *:443
- <VirtualHost *:443>
- ServerName localhost:443
- Delete All the contents from <IfModule alias_module> </ IfModule > tag
- Add following line in <IfModule alias_module> </ IfModule > tag
  - ScriptAliasMatch (?i)^/server "C:/Program Files/escan/iosenroll.dll/server"
  - ScriptAlias /attachments/ "C:/Program Files/Apache Software Foundation/Apache2.2/bin/attachments/"
- Locate tag “<Directory "C:/PROGRA~1/COMMON~1/MICROW~1/Apache2/EMCWebAdmin">” and delete whole tag along with its contents
- Locate tag “<Directory "C:/PROGRA~1/COMMON~1/MICROW~1/Apache2/MDMWebAdmin">” and delete whole tag along with its contents
- Locate tag “<Directory "C:/PROGRA~1/COMMON~1/MICROW~1/Apache2/bin/attachments">” below its ending </Directory> tag add following lines,

```
DefaultType text/plain
<IfModule mime_module>
    TypesConfig conf/mime.types
    AddType application/x-compress .Z
    AddType application/x-gzip .gz .tgz
</IfModule>
```

Cfgprofiler.dll

This dll should be located on Application Path

Functionality

- ➢ Generate Profile
- ➢ Generate Policy
- ➢ Handle Commands

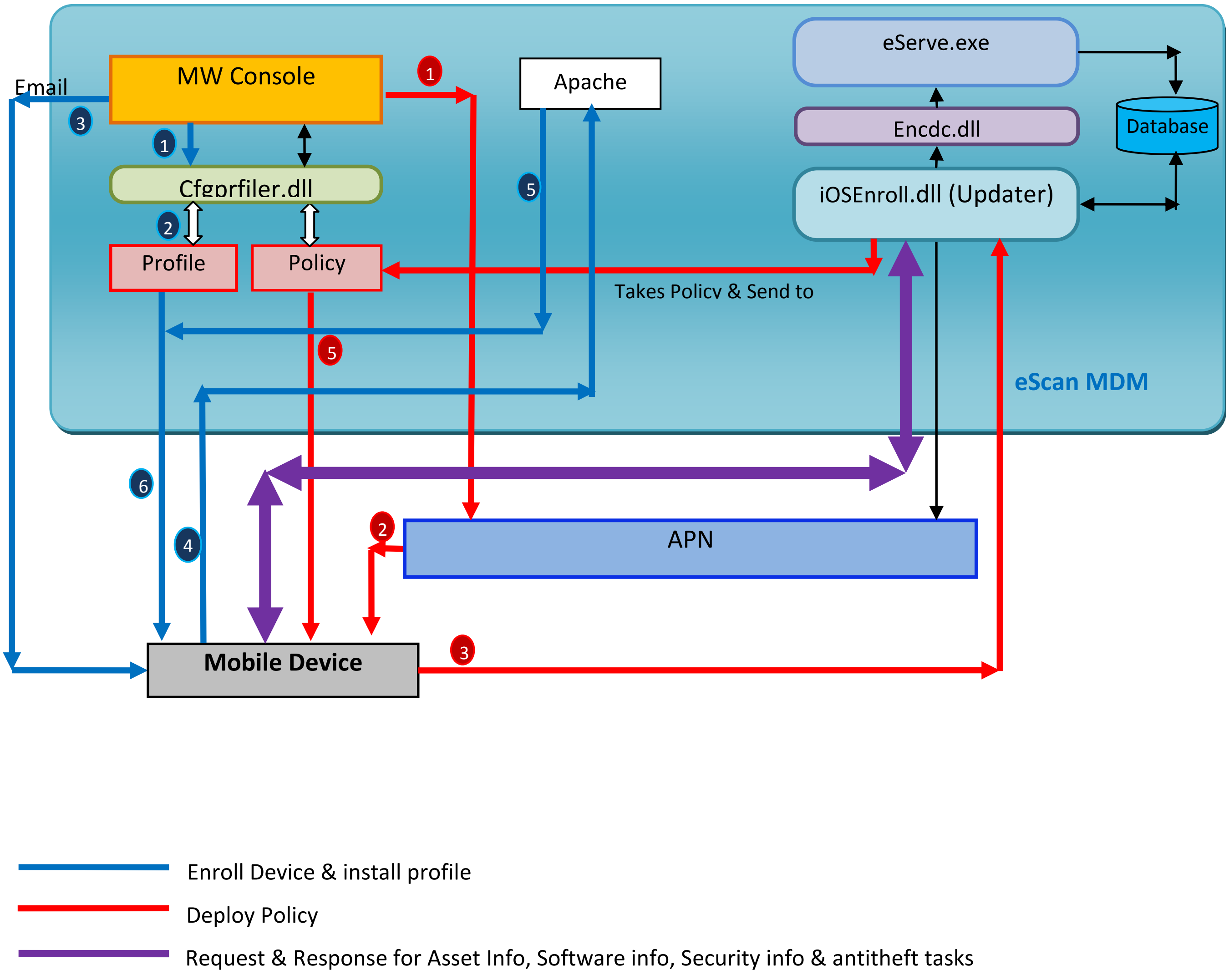
eServ.exe

Version :

This will generate additional columns in database.

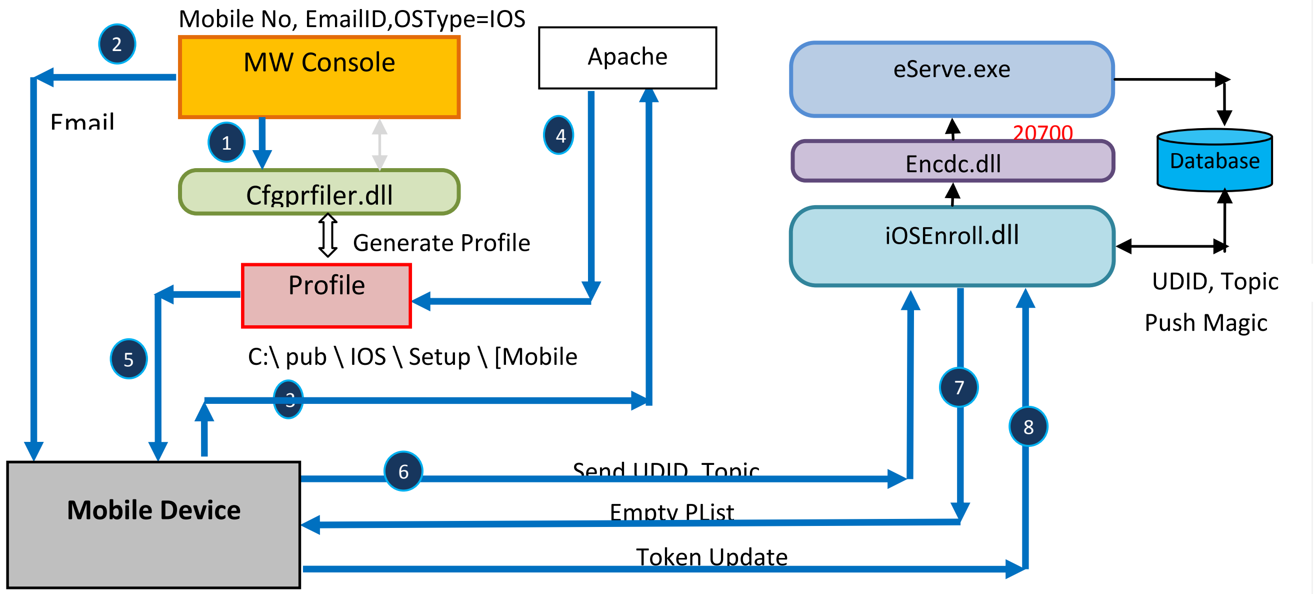
Also fill & update database.

Flow Diagram Of MDM For iOS



Ports	Description	Events ID	Description
443	HTTPS	20700,20702	Enrollment
2225	HTTP	20737	H/W ,Security, Remind H/W Details
2221	iOSEnroll.dll	20800	Software Details
10443	mwconsole	21019	Lock
		21015	Wipe
		21741	Policy
		21017	Scream
		21013	Locate
		21040	Send Message

Enrollment Of Device



Step 1 : Enter Mobile No, Email ID,UserName & OSType=IOS from MWConsole

cfgProfiler.dll will generate Profile at "C:\ pub \ IOS \ Setup \ [Mobile Number] " location

Step 2 : Email with link of profile (htttps://servername:IPAddress:443) send to given email-id.

Step 3 : On Click of profile link in the email, Profile will be downloaded & Saved into Mobile Device.

Step 4,5 : Apache will take profile from location & send it mobile device

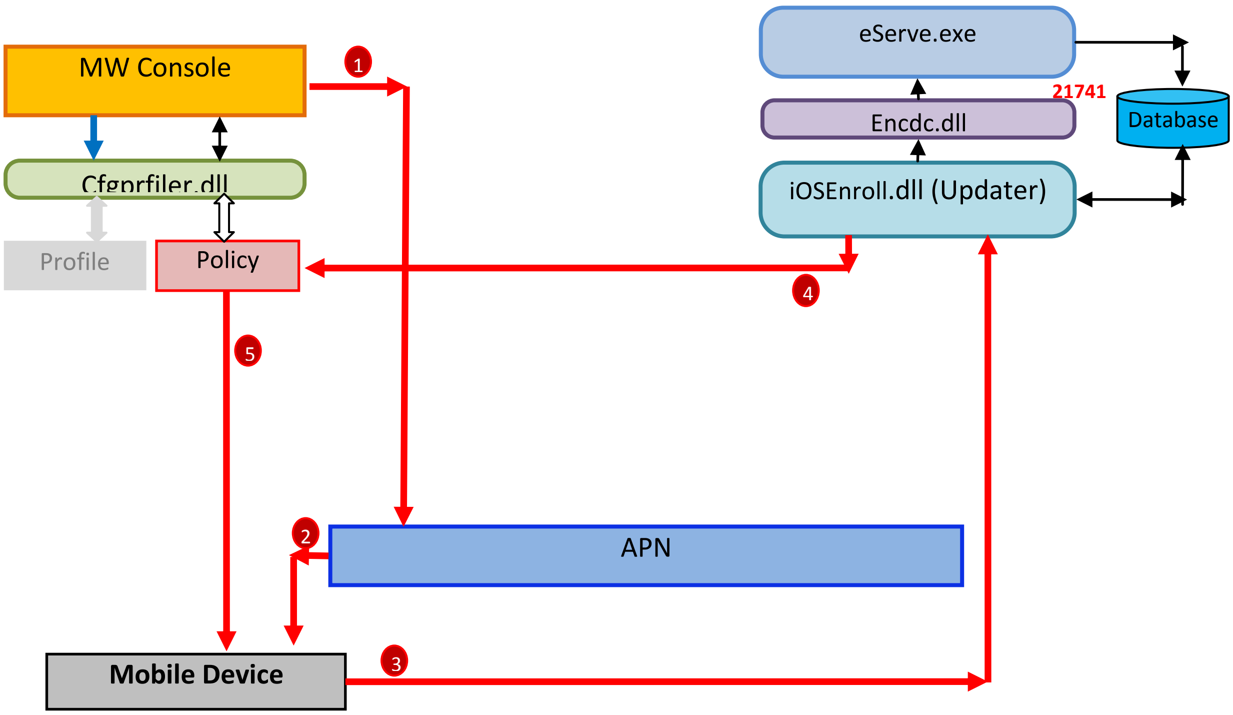
Step 6 : Device will send UDID & Topic to Updater and it will save to database.

Step 7 : IosEnroll will Send Empty PList to the Device.

Step 8 : On Response to Above Device will send Token update to IOSEnroll.dll which will save.

Push Magic & Token to database.

Policy Deployment



Step 1 : Create Policy in MWConsole

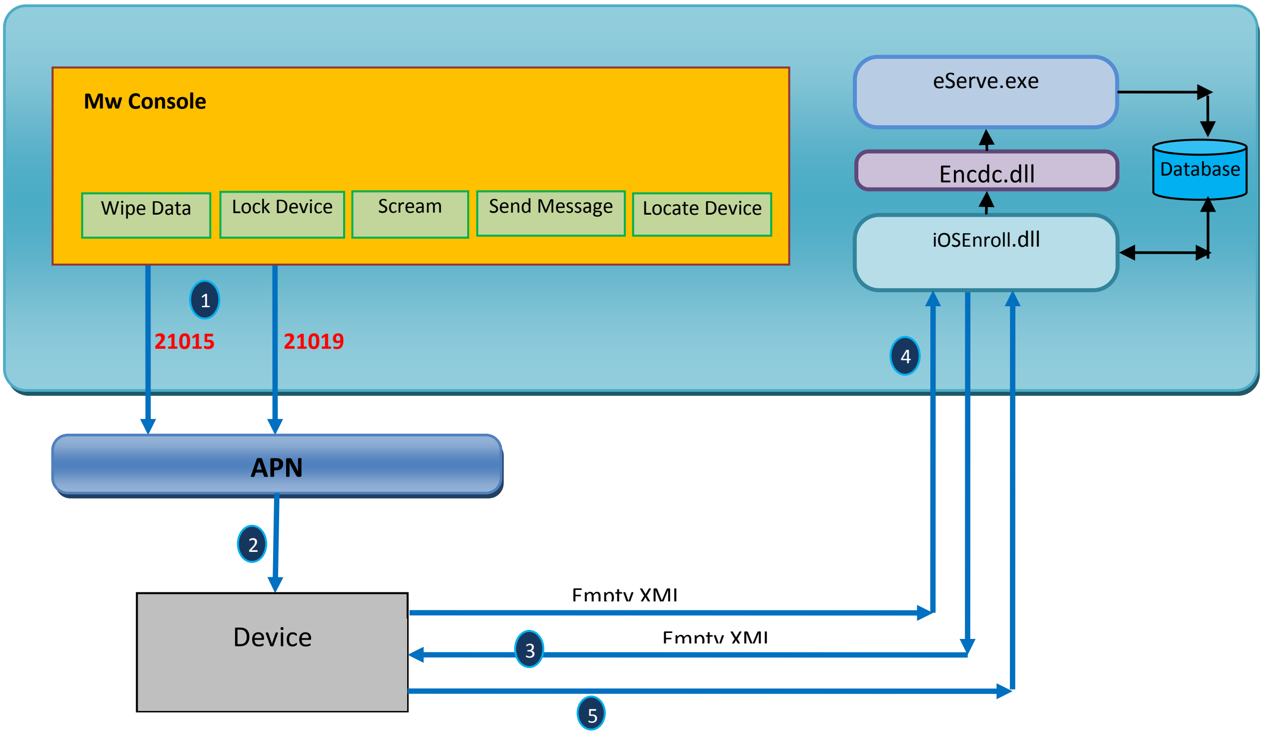
Cfgprofiler will generate policy at location (C:\pub\MDM\policy\Group Policy\)

Step 2 : MWConsole will calls to Mobile through APN

Step 3 : Mobile Device Send Status=Idle to IOSEnroll.dll (Updater)

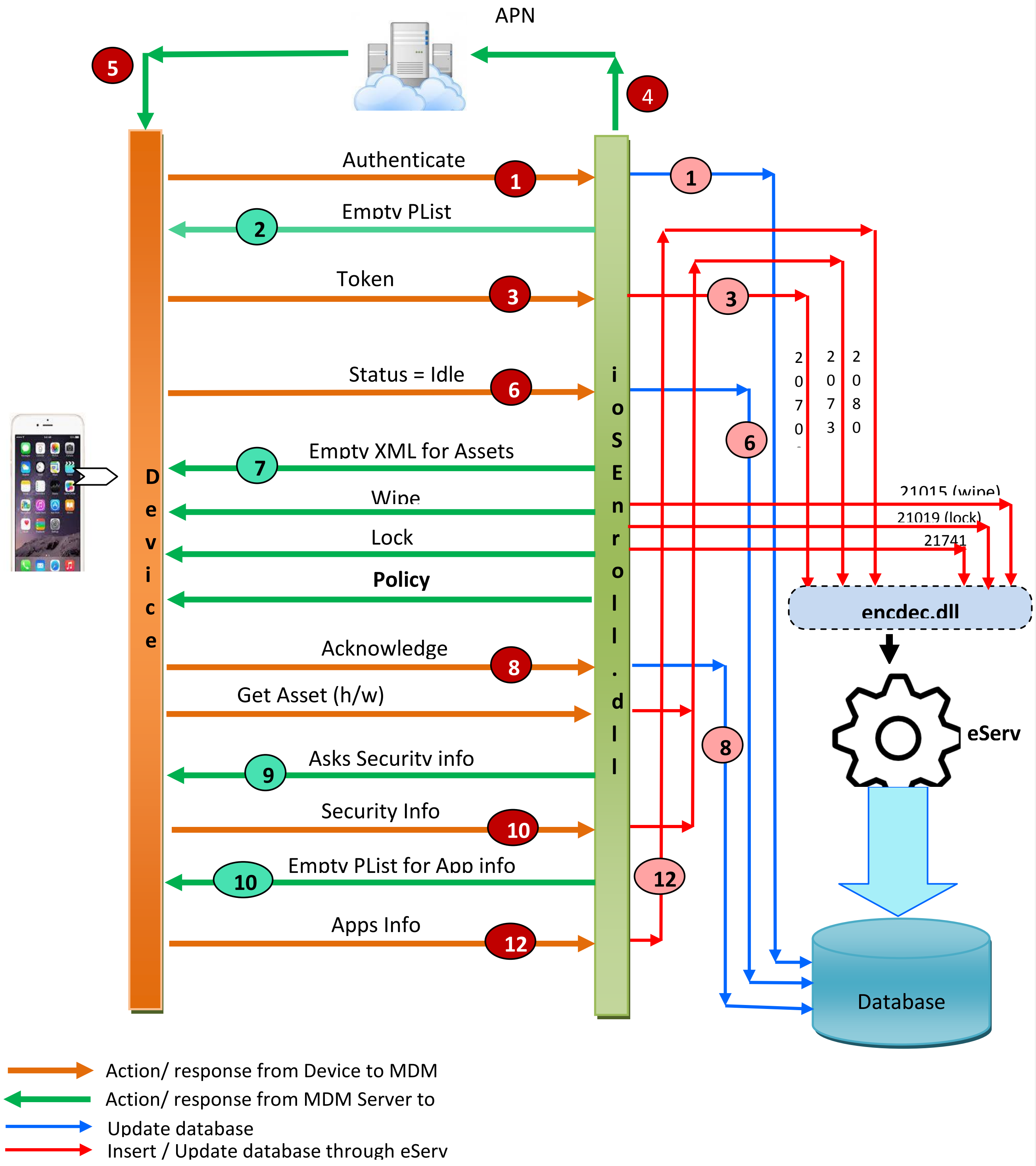
Step 4 : On Response to above iosEnroll.dll will take policy and send to mobile device

Antitheft



Step 1:	Give Wipe Data command from MWConsole it will calls to APN
Step 2:	APN Will calls to Device
Step 3 :	Device will calls to IOSEnroll.dll , it will update to database through eserv.exe by sending event id=21015
Step 4 :	iOSEnroll.dll will send XML file to device
Step 5 :	Device send “Acknowledged” status to iosEnroll.dll

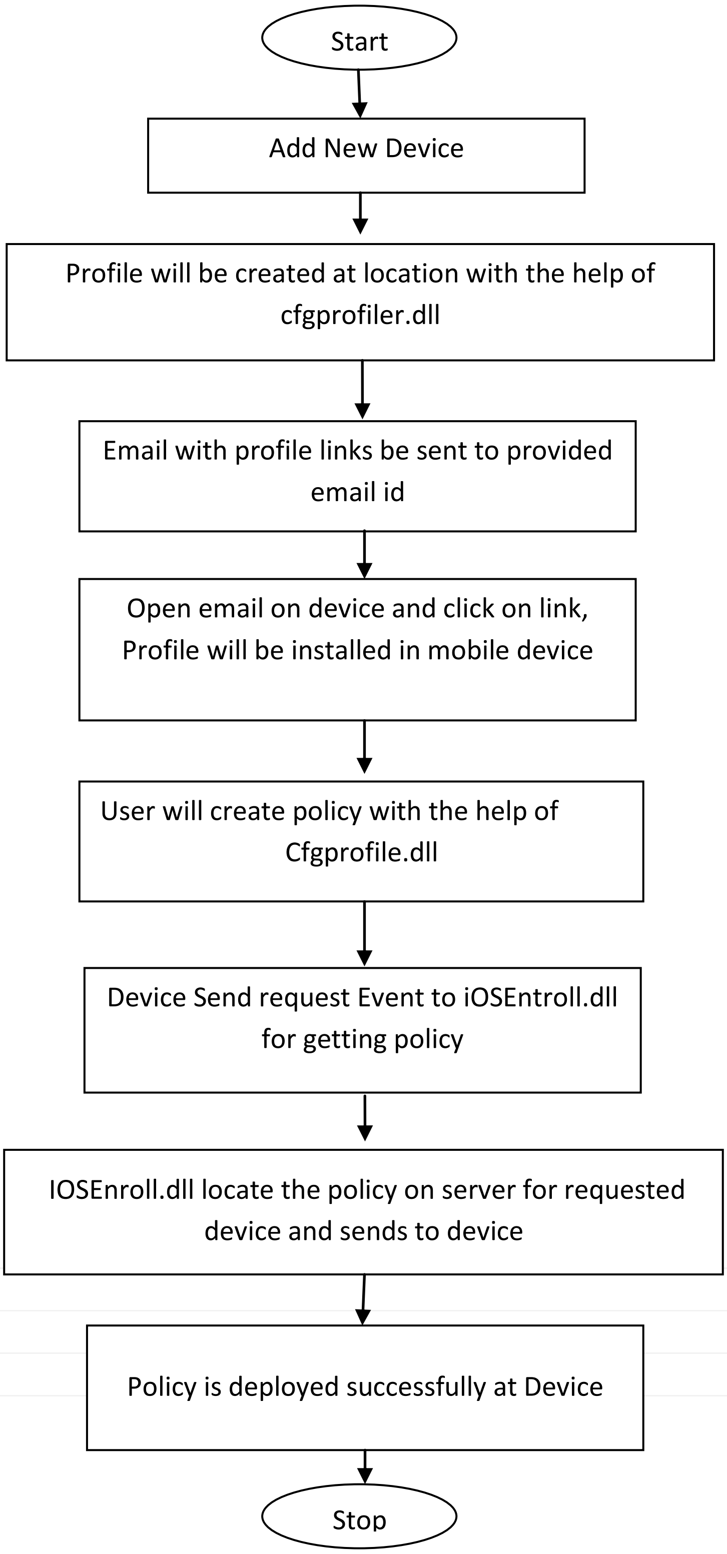
Working flow of iOSEnroll.dll with Device



Step 1	After receiving hit from client by receiving profile sent through mail iosEnroll.dll (Updater) check for MessageType if it is "Authenticate" then iosEnroll.dll (Updater) will save the Topic and UUID in database
Step 2	Empty PList will be send to device
Step 3	Token Update Message will be received from mobile device
Step 4	On response to above, IOSEnroll.dll will send Push Message To the APN
Step 5	APN Will calls to Device
Step 6	Device Will send Status =”Idle”
Step 7	• On Respond to ”Idle” Status iosEnroll.dll (Updater) will check whether hardware detail in database is more than one day then update will send empty XML for Asset Management and save "CommandUUID" to Database. • Send Antitheft (Lock and Wipe) And Policy to the device
Step 8	Device will send the Asset Information to updater, then updater will check for the status "acknowledged" Then goes for fetching the details of asset management to store it into database” mdm_hardwareDetails” table through eserv.exe by sending logline with the help of event id = 20737
Step 9	Updater will asks for Security information by sending Empty PList and Saves “commandUUIDRooted” to database
Step 10	Device will send the Security info updater will save this to database with the help of eServ.exe by sending event= 20737
Step 11	Updater will send empty xml file to the client for getting Installed Application list
Step 12	Updater will check if "commandUUID" is for Application list if then we will save the asset information in the database “mdm_SoftwareDetails” table by sending an event line to the "eServ.exe" with event id= 20800

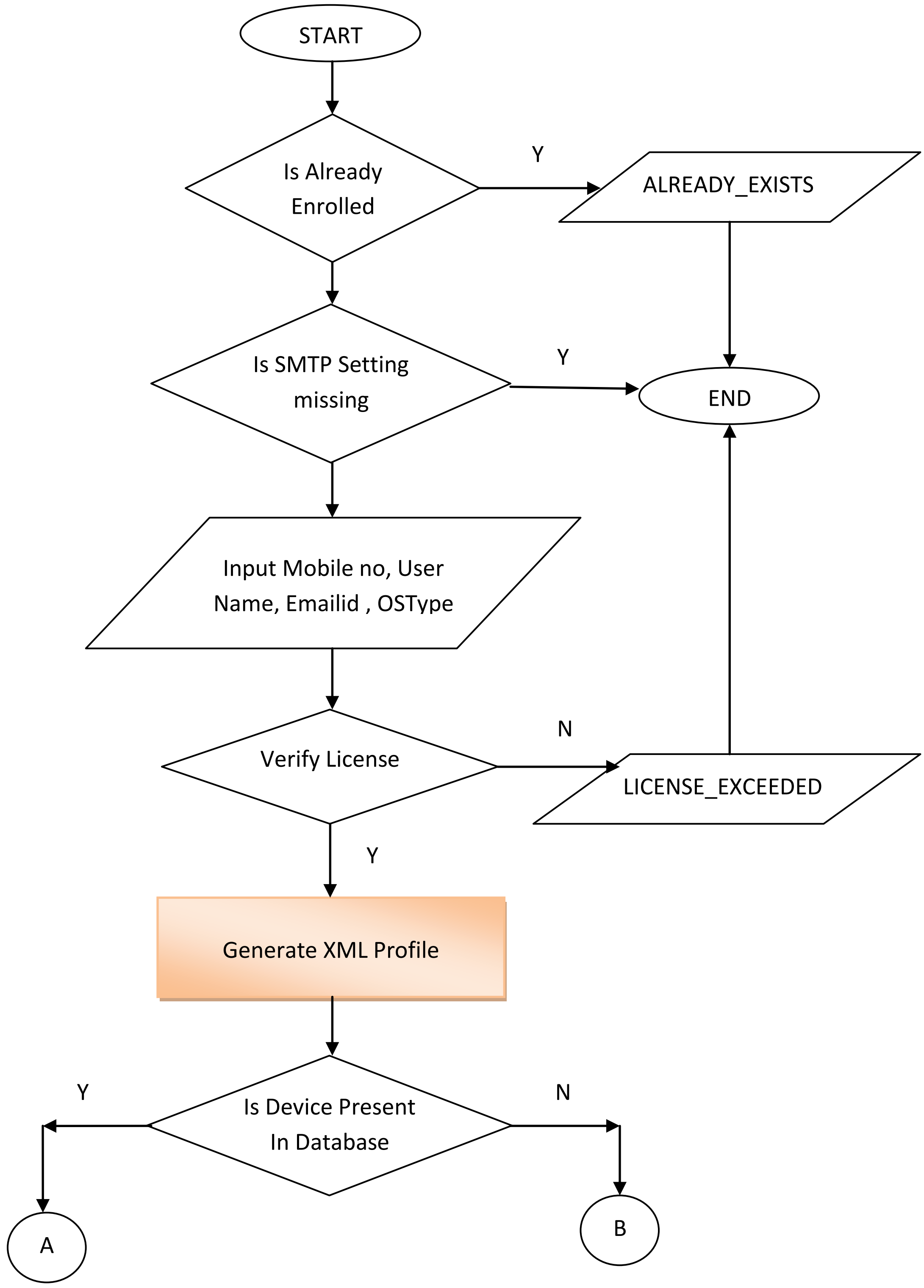
Flowchart

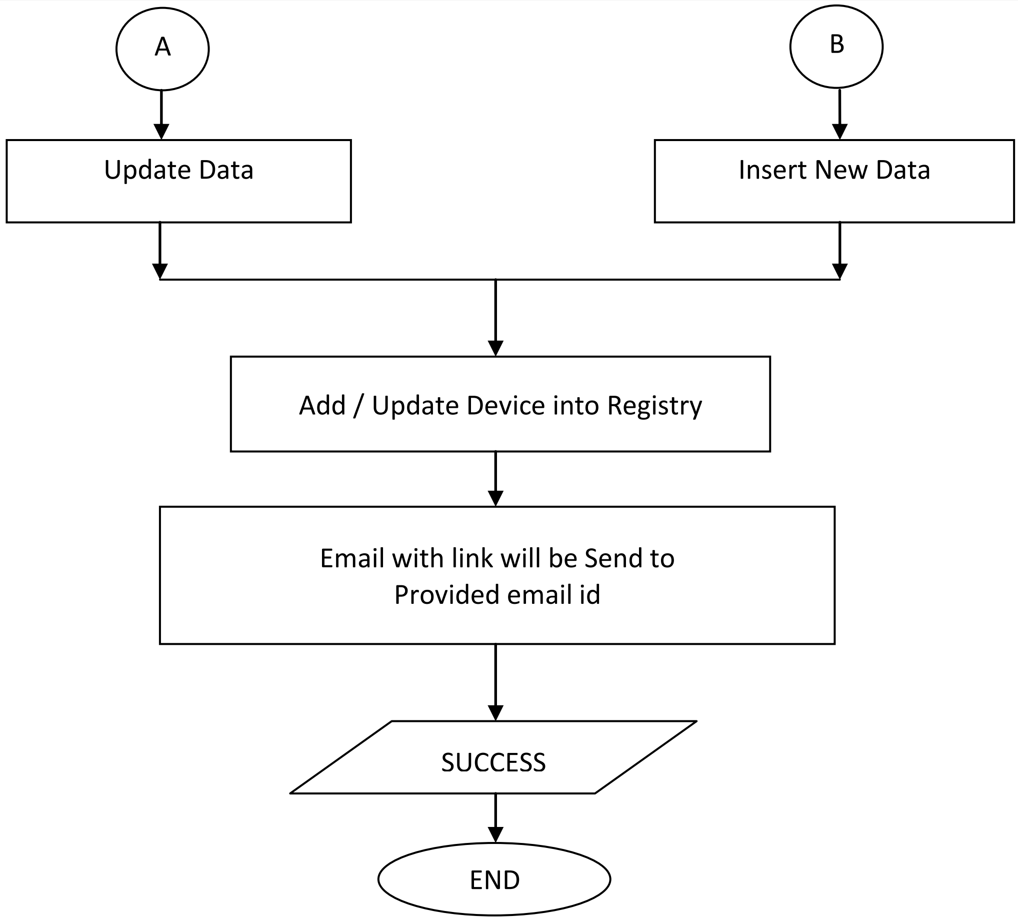
Project's Basic Flow


Start
Add New Device
Profile will be created at location with the help of cfgprofiler.dll
Email with profile links be sent to provided email id
Open email on device and click on link, Profile will be installed in mobile device
User will create policy with the help of Cfgprofile.dll
Device Send request Event to iOSEntroll.dll for getting policy
IOSEnroll.dll locate the policy on server for requested device and sends to device
Policy is deployed successfully at Device
Stop

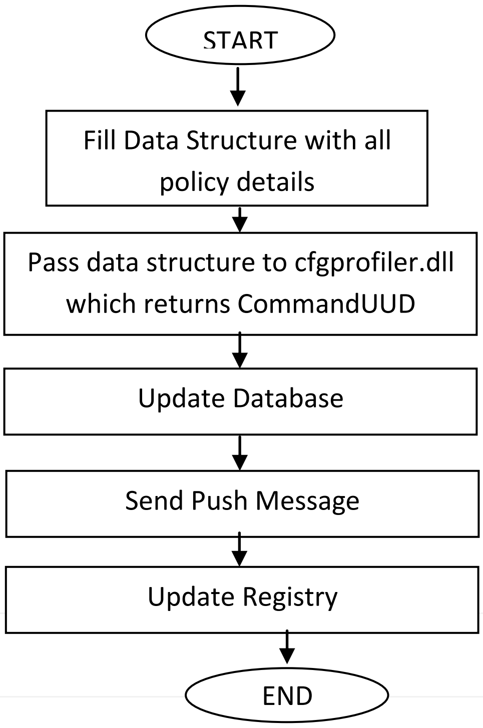
Technical Flowchart

Add New Device

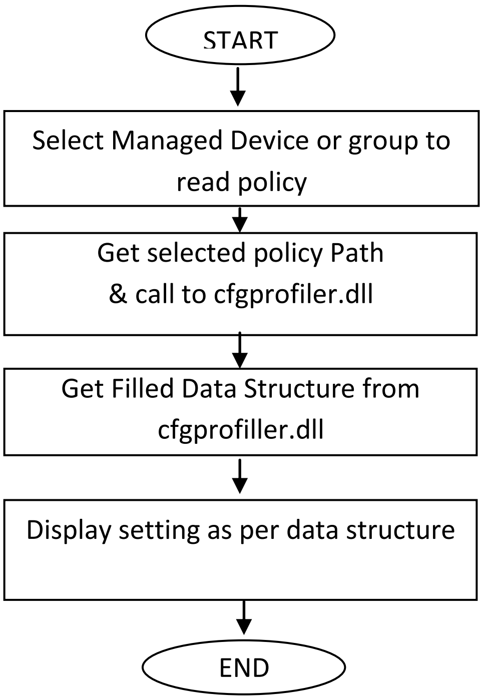



A
B
Update Data
Insert New Data
Add / Update Device into Registry
Email with link will be Send to Provided email id
SUCCESS
END

Save Policy


START
Fill Data Structure with all policy details
Pass data structure to cfgprofiler.dll which returns CommandUUD
Update Database
Send Push Message
Update Registry
END

Read Policy


START
Select Managed Device or group to read policy
Get selected policy Path & call to cfgprofiler.dll
Get Filled Data Structure from cfgprofiller.dll
Display setting as per data structure
END

Policy Details

1. Wi-Fi Settings Policy

You can configure the WiFi settings and configure protocol settings.

Profile Specification	Description
Wi-Fi	
Wireless Network identification	Network identification
Automatically join network	Automatically join the target network
Hidden network	Enable if target network is not broadcasting
Security type	Wireless network encryption while connecting
Password	Password authentication to connect the WiFi.
Configure Protocol	
Protocols Supported	Choose the type of protocol
Use Protected Access Credential	Enabling protected access
provision Protected Access Credential	Enabling protected access
Provision PAC anonymously	Enabling PAC anonymously
User Name	User Name of the device, (%username%)will get the appropriate User Name, mapped to the device
Use per connection Password	User password for initial connection
Credentials for Connection	Credentials like certificates to be uploaded
Externally Visible Identification	Visible identification
Proxy Settings	Manual or Automatic

TOP

2. VPN Policy

You can configure the VPN (Virtual Private Network) and the Proxy settings.

Profile Specification	Description
VPN	
Connection Name	Displays name of the connection
Connection Type	Connection type to be enabled
Server Name / IP Address	Host name or IP address of the server
Account	'User Authentication to access the VPN' (%username%) will get the appropriate user name, mapped to the device
User authentication	Specify user authentication type as password or RSA securID
Shared secret	shared secret for the connection
Send All traffic	Routes all network traffic through VPN connection
Configure Proxy	
Proxy settings	Configure proxy settings for VPN
Server	Proxy server name
Port	Port number to be used
User Name	User name for authentication
Password	user accounts password

TOP

3. Global HTTP Policy

This facility is applicable for only iOS 6 supervised devices only. Global HTTP Proxy settings are

Configured to ensure that all the HTTP network traffic is passed only through it. This ensures

Data security since all the personal and corporate data will be filtered through the Global HTTP proxy.

Profile Specification	Description
Web Clips	
Proxy Settings	You can define the Proxy settings to be manual or automatic.
Server	Proxy server name should be specified here.
Port	Port numbers which needs to be opened can be specified here.
User Name	Specify the 'User Name' for the proxy
Password	Specify the proxy password

TOP

4. Passcode

Profile Settings	Description
Passcode Profile Settings	
Allow simple value	Permit the usage of repeating ascending and descending character sequence.
Require Alphanumeric value	Usage of alphanumeric value
Minimum passcode length	Minimum length allowed as passcode
Minimum number of complex characters	Minimum number of complex characters needed for passcode.
Maximum passcode age	Maximum passcode age from 1 to 730 days
Auto lock the device when it is idle for	Time limit allowed for the device to be idle before the screen locks
Grace period of the device lock	When a device is locked and the user is trying to unlock it, then the time limit allowed for the user to unlock the device without using the passcode If the Grace period is five minutes, users will be allowed to unlock the device without a passcode for the first minutes from the device screen lock.
Maximum number of failed attempts	Maximum number attempts before all data in the device to be erased

Top

5. Restrictions Policy

Profile Settings	Description
Restrictions Profile Settings	
Allow installing Apps	Using this option App store can be disabled and the App store icon will be removed from the home screen. So users will not be able to install or update any Apps using App store of iTunes
Allow removing Apps (iOS 6 and above - Supervised devices only)	Allowing the user to remove the Apps
Allow use of Camera	Cameras are completely disabled and the icons are removed from the home screen. Users cannot take photos, video or use face time
Allow Facetime	Allowing users to receive or make Face Time video calls
Allow AirDrop (iOS 7 and above - Supervised devices	Allowing users to share documents using AirDrop

only)	
Allow iMessage (iOS 6 and above - Supervised devices only)	Allowing the users to use iMessage feature
Allow screen capture	Allowing users to capture the screen shot of the display
Allow automatic sync while roaming	Devices while roaming will sync only when an account is accessed by the user
Allow siri	Allow the usage of siri
Allow siri when device is locked	Permit usage of siri when the device is locked
Force Siri Profanity Filter (iOS 6 and above - Supervised devices only)	Enabling the profanity filter option in Siri
Allow Siri to query from the web (iOS 7 and above - Supervised devices only)	Allowing Siri to query content from the web (Wikipedia, Bing and Twitter)
Allow usage of Touch ID to unlock device (iOS 7 and above)	Allowing user to unlock the device using finger prints
Allow Passbook while device is locked (iOS 6 and above)	Permit the usage of passbook while the device is locked
Allow voice dialing	Permit users to use voice dialing
Show Control Center in lock screen(iOS 7 and above)	Allow users to access control center when the device is locked
Show Notification Center in lock screen (iOS 7 and above)	Display Notifications Center when the device is locked
Show Today view in lock screen (iOS 7 and above)	Display "Today View", of Notifications Center when the device is locked
Allow in App purchase	Enables users to purchase in-App purchases
Force user to enter iTunes store password	Prompt iIunes password for every download.
Allow Game Center (iOS 6 and above - Supervised devices only)	Permit the usage of Game Center

Allow multiplayer gaming	Allow multiple users gaming
Allow adding game center friends	allow users to add game center friends
Applications	
Allow use of you tube	Allow users to use youtube
Allow the usage of iBooks store (iOS 6 and above - Supervised devices only)	Enable iBooks store usage
Allow the user to download erotica media from iBooks store (iOS 6 and above - Supervised devices only)	Enable users to download media which is tagged as erotica
Allow use of iTune music store	Allow users to use iTune store
Allow use of safari	Allow users to use safari
Enable auto fill	Enables the auto fill option
Force fraud warning	Allows force fraud warning
Enable javascript	Allows java script
Allow Pop-ups	Enables pop up
Accept cookies	Accepts cookies
iCloud	
Allow Backup	Enables data backup
Allow Document Sync	Allows document sync
Allow Photo Stream	Enables streaming photos
Allow Shared Stream (iOS 6 and above)	Enable Stream Sharing
Security and Privacy	
Allow Diagnostic data to be sent to Apple (iOS 6 and above)	Enables diagnostic data to be reported to apple
Allow user to accept untrusted TLS certificates	Allows to use untrusted TLS certificates.
Allow automatic updates to certificate trust settings (iOS 7 and above)	Allow trust certificates to be updated automatically
Force Encrypted Backups	Forces to encrypt the data during backup

	process
Force limited ad tracking (iOS 7 and above)	Allows user to restrict Ad tracking and marketing on the device
Allow users to install configuration profiles and certificates interactively (iOS 6 and above - Supervised devices only)	Allow users to install/ modify the configuration and certificates
Allow modifying account settings(iOS 7 and above - Supervised devices only)	Allow users to modify the accounts settings like adding or removing mail accounts, modifying iCloud settings, iMessage settings etc,.
Allow modifying Find my Friends settings (iOS 7 and above - Supervised devices only)	Allow users to modify the settings of "Find my Friends"
Allow paring with non-Configurator hosts (iOS 7 and above - Supervised devices only)	Allow device to be paired with any device, if this is disabled device will be paired only with configurator host
Allow user to change which apps can use cellular data (iOS 7 and above - Supervised devices only)	Allow users to restrict usage of cellular data for specific apps
Allow documents from managed apps in unmanaged apps (iOS 7 and above)	Allow users to share and use the data from a corporate app to a personal app which is not distributed by the corporate.
Allow documents from unmanaged apps in managed apps (iOS 7 and above)	Restrict users to share and use the data from a personal app to a corporate app which is distributed by the corporate
Content Ratings	
Allow Explicit Music & Podcasts	Allows music and podcasts
Ratings by Region	
Enable Ratings by Region	Enables ratings by region
Specify the Region	Allows you to choose the region, so that you can specify the settings accordingly
Ratings for Movies	Allows viewing movies based on the specified ratings
Ratings for TV shows	Allows viewing TV Shows based on the specified ratings
Ratings for Apps	Allows using Apps based on the specified ratings.

TOP

6. Email Policy

Profile Specification	Description
Email	
Account Name	Name of the mail account
Account Type	Account type as IMAP / POP
Path Prefix	Specify the path prefix
User Display Name	User name to be displayed (%username%) will get the appropriate user name, mapped to the device
Email Address	Email address for communication (%email%)will get the appropriate email address, mapped to the device
Allow move	Option to allow move or not
Disable recent mail address sync (iOS 6 and above)	Option to sync the recently used email address in iCloud.
Incoming Mail	
Mail server	Name of the incoming mail server
Port	Port used for incoming mails
User name	User name to be displayed (%username%)will get the appropriate user name, mapped to the device
Authentication Type	Authentication type to be specified
Password	Password for the incoming mail server (If the password field is left empty, password will be prompted once the profile is installed in the device).
Use SSL	Retrieve incoming mail through SSL
Outgoing Mail	
Mail server	Name of the outgoing mail server
Port	Port used for outgoing mails
User name	User name to be displayed (%username%) will get the appropriate user name, mapped to the device
Authentication Type	Authentication type to be specified
Password	Password for the outgoing mail server (If the password field is left empty, password will be prompted once the profile is installed in the device).
Use outgoing password same as incoming	Option to use the same password for both outgoing and incoming mails
Use only in mail	specify whether to be used only in mail
Use SSL	Specify to use SSL
Use S/Mine	Specify to use S/Mine

TOP

7. Web Clip Policy

Profile Specification	Description
Web Clips	
Web Clip Label	The name to be displayed on the web clip
URL to be Linked	The URL to be displayed on selecting the web clip
Removal of Web Clip	Enable to remove the web clip
Icon	The icon used for the web clip
Use Precomposed Icon	This icon will be displayed with no added visual effects
Allow Full Screen	Controls whether the web clip launches as a full screen application

TOP