Telstra

Mobile Device Management Guide

Apple® iPhone™

https://mdm.telstra.com

Contents

Purpose 3

Overview of Mobile Device Management 3

Getting Help 3

Pre-requisites 3

Customer Admin Login 4

- Web Portal Address 4
- Getting Login Access 4
- First Time Login 5
- Forgotten Password 5
- Password Security 7
- Multiple Customer Logins 8

Searching For Mobile Users 8

Device Enrolment 9

Device Diagnostics 11

Send Configuration Settings 12

Scheduler 17

Lock, Unlock and Wipe 20

- Lock 20
- Wipe 21
- Unlock 22

Reporting 22

FAQs 24

Appendix - Upload Apple Certificate 26

Definitions 27

Purpose

- This user guide is for **IT administrators** who want to remotely manage their fleet of mobile devices via the Telstra Mobile Device Management ("MDM")portal.
- This userguide is not intended to be used by the mobile users.

Overview of Mobile Device Management

Telstra's MDM web portal allows nominated IT administrators to manage a diverse fleet of mobile devices and perform the following activities remotely over the air. The Telstra MDM portal is available to mobile users who have subscribed to Mobile Connect plans on their service.

		Description
Send SMS Messages	☑	SMS messages can be sent to individuals or entire groups
Configuration Settings	☑	Send settings eg ActiveSync, WiFi, VPN, APN etc
Diagnostics	☑	Get information back about the device eg Roaming enabled
Device Security	☑	Lock and unlock. Full wipe
Device Restrictions	☑	Restrict certain applications eg Youtube, App Store etc
Reporting	☑	Run and export standard reports eg list of devices etc
Scheduling	☑	Sending out configuration settings in bulk to a number of mobile users
Deploy Enterprise Software	☒	Coming – Not currently supported
Update Firmware	☒	All iPhones must be upgraded via Apple

Note:
iPhone™ devices do NOT need a client software or any software from the Apple® App store. Telstra MDM is supported natively in iOS 4 and greater.

A mobile user decides whether they will accept company settings on their device and can remove these settings by deleting the enrolment profile. It's up to each customer to ensure they do not allow access to company resources when these settings are manually removed by a mobile user.

Getting Help

Telstra provides assistance during business hours 8am- 6pm, for customers wishing to use Telstra MDM.
All correspondence should be initiated via email to wireless@team.telstra.com and a customer support representative will get back to you.

The customer support representative can only assist you if we have you listed as an authorised representative on the account who has the authority to remotely manage the company's devices.

Pre-requisites

To use Telstra MDM, the following items need to be in place:

- You must have at least one iPhone 3GS (or newer iPhone model) running iOS 4 (or greater) operating system.
- You must have at least one active Telstra SIM and the mobile service MUST be connected with a Telstra Mobile Connect data plan. For more information on Mobile Connect data plans see here www.telstra.com/mobileconnectsolution
- The device MUST always have internet access to https://dm2.mobile.telstra.com/* in order to operate correctly with Telstra MDM.
- The iPhone device(s) must be registered with iTunes and turned on and in a mobile network coverage area
- All mobile devices you want to manage must be grouped under a single Telstra mobile billing account. If unclear about this requirement please contact your Telstra sales person or Telstra service delivery/billing contact and they can discuss implications of grouping mobile services under a single billing account.
- You will require a first time login password to access the Telstra MDM portal.
  - A first time login password can be requested from the Telstra MDM helpdesk via email wireless@team.telstra.com
  - You will need to provide proof that you are an authorised representative of your company and have the authority to remotely manage employee/contractor devices.
- You must also have an existing subscription to the Apple iOS Developer Program (Apple charge an annual fee for this). Under this program you will have received an Apple certificate which you will need to upload into Telstra's MDM portal.

  See the Appendix for details on uploading an Apple certificate to the Telstra MDM Portal for your company.

Customer Admin Login

Web Portal Address

Nominated IT administrators can login to the Telstra MDM portal at https://mdm.telstra.com

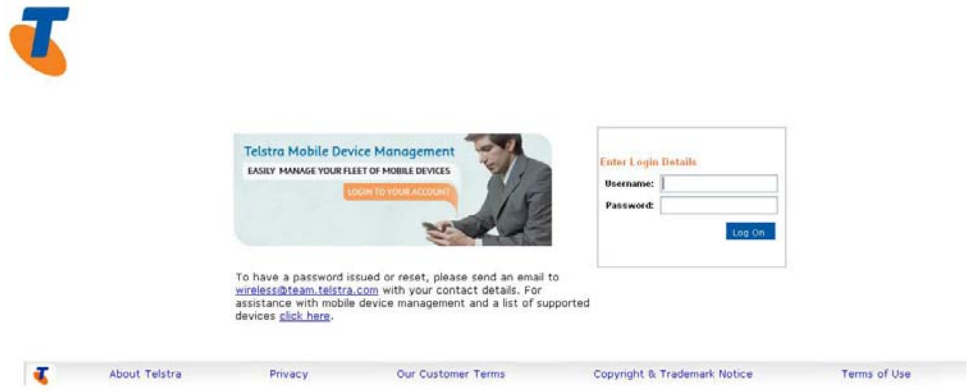
Getting Login Access

The following credentials will be required to gain access

Username	This is your 10 digit Telstra mobile account number under which your mobile users are grouped. If uncertain about your Telstra mobile account number please contact the Telstra MDM helpdesk at wireless@team.telstra.com
Password	This is your unique Telstra MDM password which you will manage. **The very first time you use the Telstra MDM portal, you will be required to request a password from the Telstra MDM helpdesk at wireless@team.telstra.com**

Note:

You will need to provide proof that you are an authorised representative of your company and have the authority to remotely manage employee/contractor devices before Telstra will issue a password.



Telstra Mobile Device Management
EASILY MANAGE YOUR FLEET OF MOBILE DEVICES
LOGIN TO YOUR ACCOUNT
Enter Login Details
Log On
About Telstra
Privacy
Our Customer Terms
Copyright & Trademark Notice
Terms of Use

Username:

Password:

To have a password issued or reset, please send an email to wireless@team.telstra.com with your contact details. For assistance with mobile device management and a list of supported devices click here.

First Time Login

- The very first time you login, you will be required to change your password.
  - Password has to be at least 6 characters
  - Password maximum length is 14 characters
  - Password cannot have 3 consecutive characters or numbers
  - Password must be alphanumeric (no special Characters)
- You should also enter your email address (or a distribution email address) and answer to a secret question as described below so that if you forget your password in future, this can be reset for you online without needing to contact Telstra.

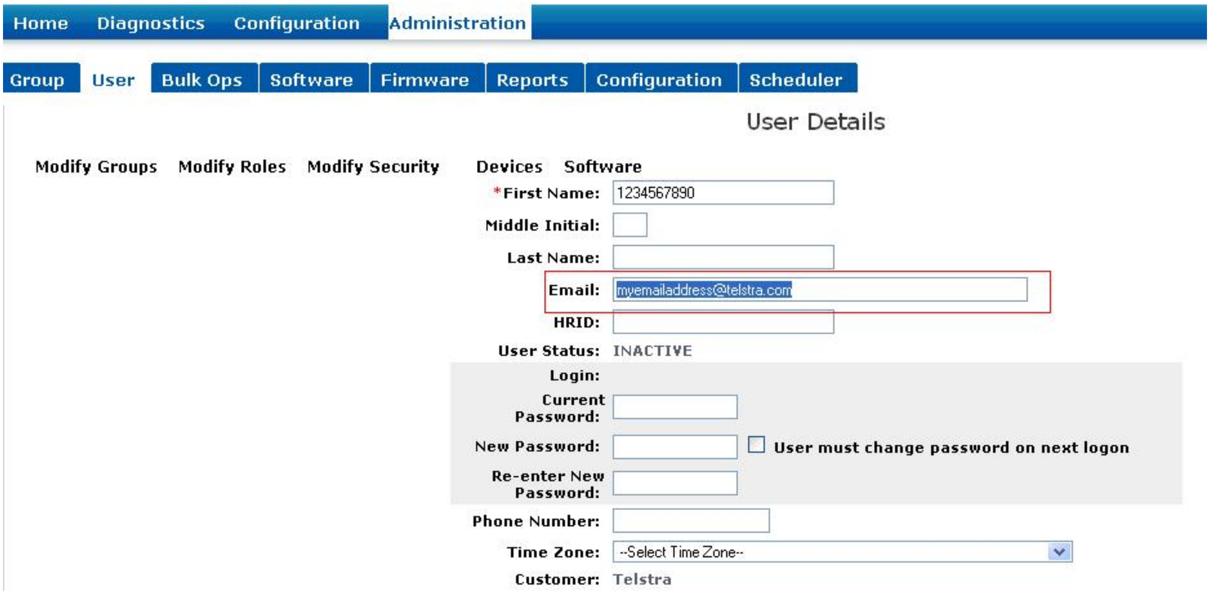
Forgotten Password

If you have forgotten your password, this can be automatically reset and a new password issued online without you needing to contact Telstra.

Alternatively if you get stuck, Telstra's MDM helpdesk can reset the password. Send an email to wireless@team.telstra.com and you will then be asked to verify your details before the password is changed

Pre-requisites:

When you login successfully for the first time you should setup your email address and the answer to a secret question from the administration>user screen. Alternatively click on "My Account" in the top right hand corner to go directly to this page.



User Details

*First Name: 1234567890

Middle Initial:

Last Name:

Email: myemailaddress@telstra.com

HRID:

User Status: INACTIVE

Login:

Current Password:

New Password: □ User must change password on next logon

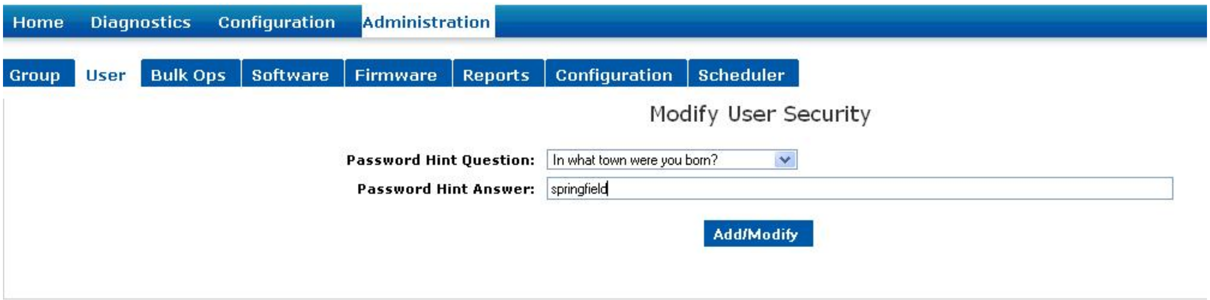
Re-enter New Password:

Phone Number:

Time Zone: --Select Time Zone--

Customer: Telstra

You should also setup an answer to a secret question from the administration>user>modify security screen



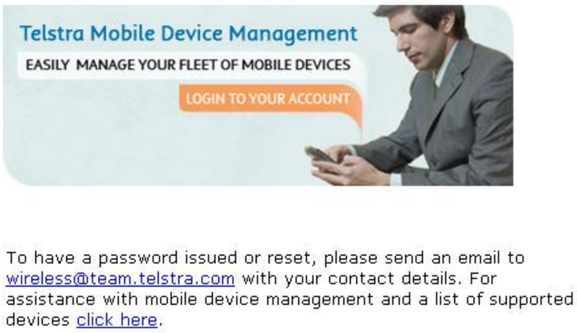
Modify User Security

Password Hint Question: In what town were you born?

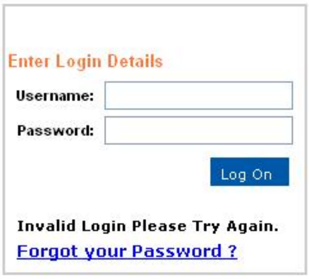
Password Hint Answer: springfield

<u>When you forget your password:</u>

When you enter your username(Telstra 10 digit billing account number) and an incorrect password, you will be asked if you have forgotten your password and given the opportunity to have this reset.


Telstra Mobile Device Management
EASILY MANAGE YOUR FLEET OF MOBILE DEVICES
LOGIN TO YOUR ACCOUNT

To have a password issued or reset, please send an email to wireless@team.telstra.com with your contact details. For assistance with mobile device management and a list of supported devices click here.



Enter Login Details

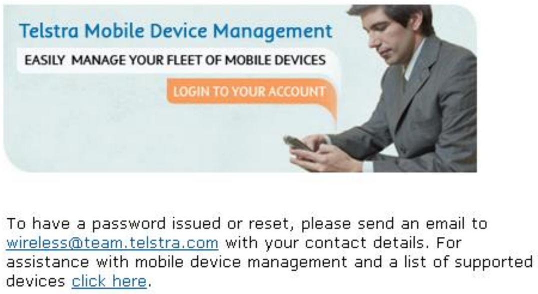
Username:

Password:

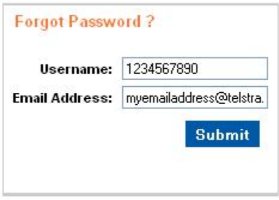
Invalid Login Please Try Again.

Forgot your Password ?

You will then be asked to enter your username and email address

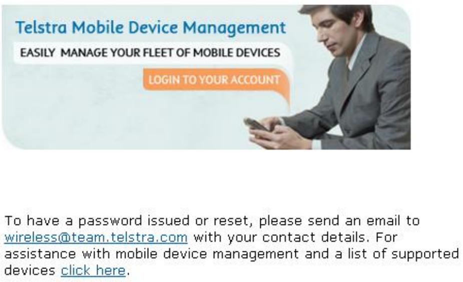

Telstra Mobile Device Management
EASILY MANAGE YOUR FLEET OF MOBILE DEVICES
LOGIN TO YOUR ACCOUNT

To have a password issued or reset, please send an email to wireless@team.telstra.com with your contact details. For assistance with mobile device management and a list of supported devices click here.

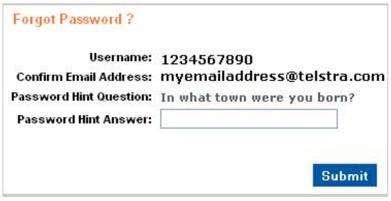


Username: 1234567890
Email Address: myemailaddress@telstra.

You will then be asked for your answer to a secret question


Telstra Mobile Device Management
EASILY MANAGE YOUR FLEET OF MOBILE DEVICES
LOGIN TO YOUR ACCOUNT

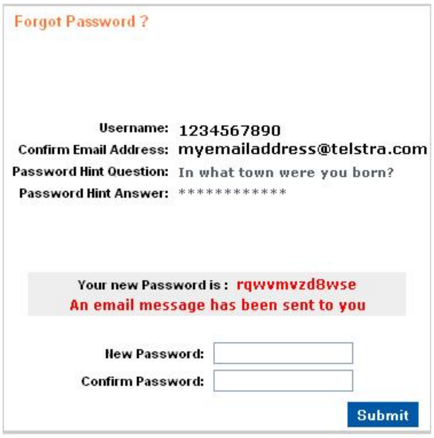
To have a password issued or reset, please send an email to wireless@team.telstra.com with your contact details. For assistance with mobile device management and a list of supported devices click here.



Username: 1234567890
Confirm Email Address: myemailaddress@telstra.com
Password Hint Question: In what town were you born?
Password Hint Answer:

Your password will then be reset and you will be asked to enter a new one. You will also receive a confirmation email that the password was reset

Telstra Mobile Device Management
EASILY MANAGE YOUR FLEET OF MOBILE DEVICES
LOGIN TO YOUR ACCOUNT



Username: 1234567890
Confirm Email Address: myemailaddress@telstra.com
Password Hint Question: In what town were you born?
Password Hint Answer: ************

Your new Password is : rqwvmvzd8wse
An email message has been sent to you

New Password:
Confirm Password:

Password Security

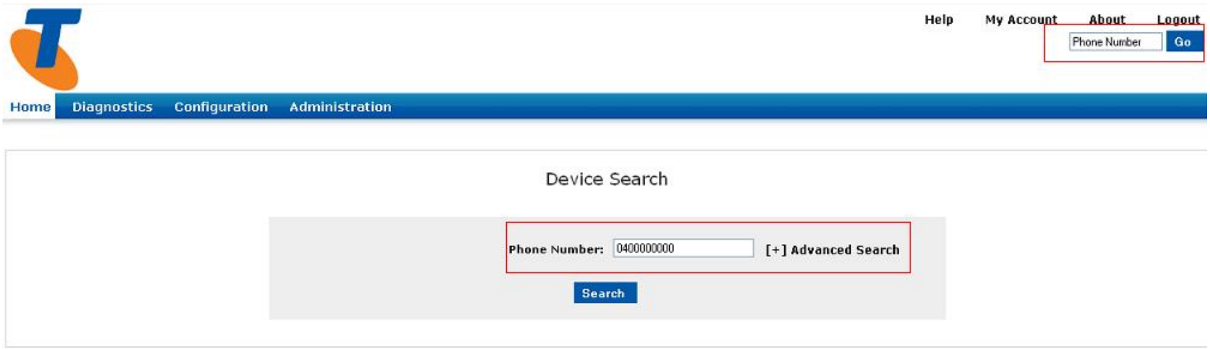
- The Telstra MDM portal will require that you change your password every 60 days
- Your login will timeout after 60 minutes of inactivity and you will be required to login again
- Passwords will be locked out after three incorrect attempts
- Accounts will be locked after 60 days if you have not logged in during that time.
- It is your responsibility to keep your password secret and secure. You should NOT pass these details to any person outside your organisation and should change password details if employees leave the organisation.

Multiple Customer Logins

- Only one person at a time can login using the same username/password. If a second person tries to login using the same username/password the other person's login will timeout.
- Should you require additional logins for your company, please contact the Telstra helpdesk on wireless@team.telstra.com and they can assist.
    - Read only privileges can also be assigned to different logins depending on what roles you want to give different administration groups within your organisation.

Searching For Mobile Users

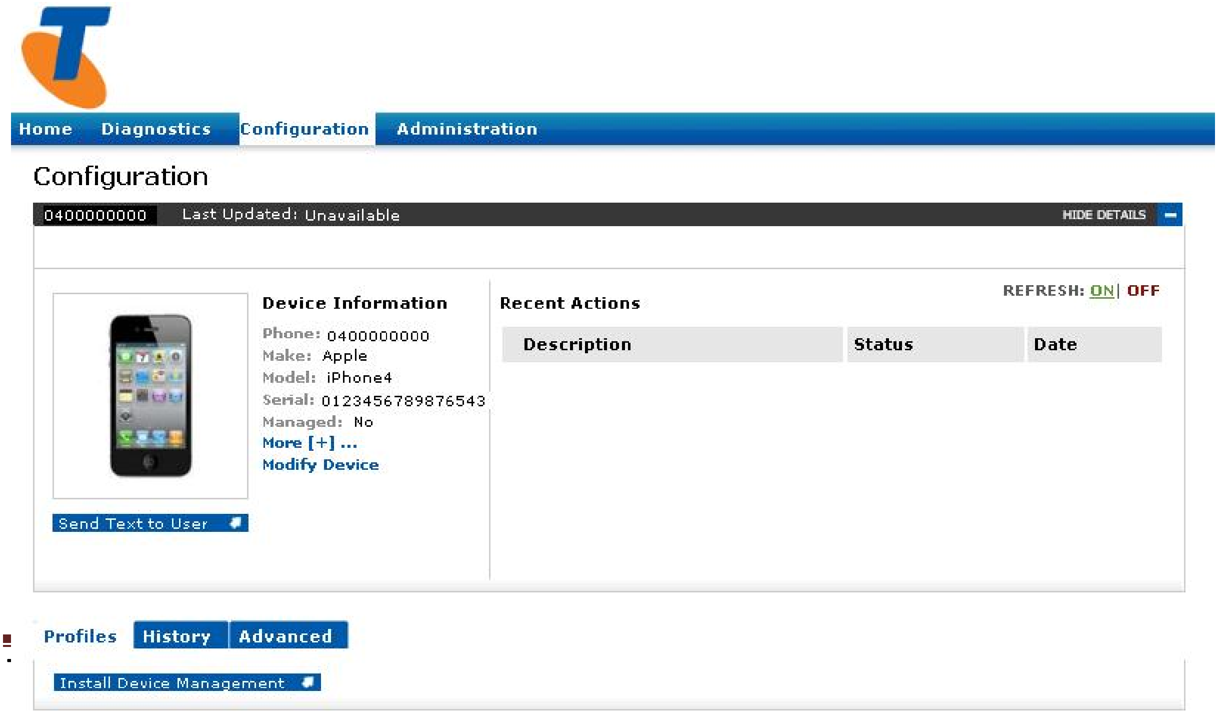
After login you will be presented with the default search screen to make it easy for you to find mobile users. However at any time you can also search for a mobile number by entering this in the top right hand corner.



Device Search

Phone Number: 0400000000

The Telstra MDM portal will then search for the mobile number and display a picture of the handset model associated with that mobile number.



Configuration

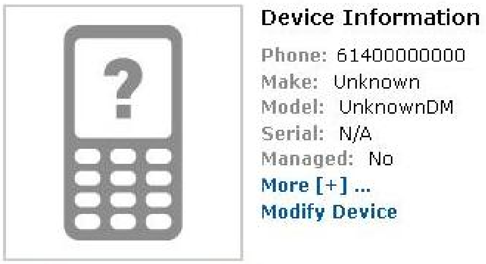
0400000000 Last Updated: Unavailable

Device Information

Phone: 0400000000
Make: Apple
Model: iPhone4
Serial: 0123456789876543
Managed: No

Recent Actions

Description	Status	Date

Search Problem	Resolution
“The device cannot be found”	• Check that the mobile number has a Mobile Connect plan activated • Check that the mobile number belongs to the Telstra billing account number you are using to login. That is, if you logged into Telstra MDM using the mobile billing account number 1234567890, check that the mobile number you are searching for is being billed under that Telstra account number. • Telstra automatically refreshes mobile number information each night, and if a Mobile Connect plan is activated, this mobile number will be displayed the following day.
Device model is shown as unknown  Device Information Phone: 61400000000 Make: Unknown Model: UnknownDM Serial: N/A Managed: No More [+] ... Modify Device	• The device model being used is not supported by the Telstra MDM portal. For a list of supported device models see www.telstra.com/tmcshandsets • Telstra cannot identify the device of the user correctly because the user has swapped devices recently • Telstra automatically refreshes handset information each night and, if the model is supported for Telstra MDM, it will be displayed the following day should the user swap devices.

If you believe the mobile number or handset model is not being displayed correctly please contact the Telstra MDM helpdesk at wireless@team.telstra.com

Device Enrolment

Enrolment is a process of establishing authentication between the device and the Telstra MDM portal. A device MUST be successfully enrolled before the Telstra MDM portal can then send settings and policies to the device. Via a series of pop-up messages the mobile user will be asked to accept the enrolment and install an enrolment profile on their device.

To enrol a device:

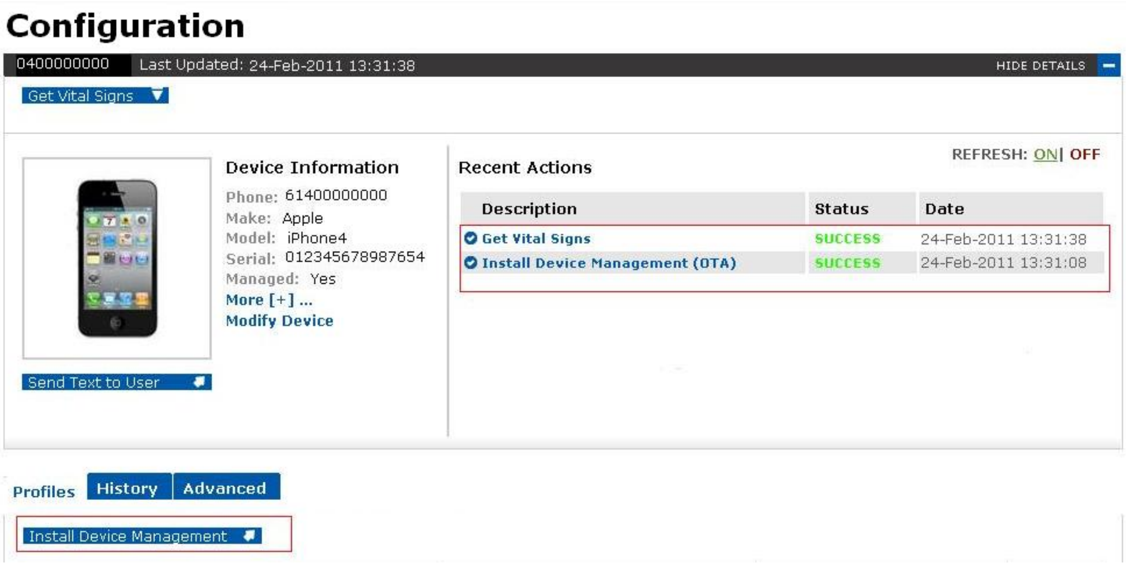
- From the configuration tab, click on the “Install Device Management” button and the server will send an enrolment request to the user and ask them to install an enrolment profile on their device. Note: You will need to advise your users/employees to “accept” the enrolment requests on their mobile devices.
- Under the “Recent Actions” panel the status of you enrolment will be shown. If the enrolment happens successfully you will see status will go from pending>sent>success.

- **The enrolment will only succeed if the user accepts the enrolment message and they install an enrolment profile on the device.**

Recent Actions Status	Meaning
PENDING	• The Telstra MDM server is in the process of sending the message to the device. • If the status remains frozen in "pending" it means that the Telstra MDM server is having trouble sending the message
SENT	• The Telstra MDM server has sent the message to the device and is waiting for a response • If the status remains frozen in "sent" it means the message has not been delivered OR the handset is not responding to the message.
SUCCESS	• The transaction was successful and the device has reported that the setting has been successful
FAILED	• The transaction was unsuccessful either because the handset rejected the message OR the server timed out after 3 minutes

Note:

- This process only needs to be done once for each device (unless the user chooses to wipe the device or manually remove the enrolment profile in the future, in that case the process will need to be repeated for that device).
- The enrolment will not succeed unless the user accepts the popup messages on their phone and installs the enrolment profile.
- Each enrolment SMS sent to the device is unique. If the user clicks on an old expired SMS link the device will not be able to download the enrolment profile from the server.
- The Telstra MDM server will timeout after 3 minutes if it does not receive a successful notification from the device.



Configuration

0400000000 Last Updated: 24-Feb-2011 13:31:38 HIDE DETAILS

Get Vital Signs

Device Information

Phone: 61400000000
Make: Apple
Model: iPhone4
Serial: 012345678987654
Managed: Yes
More [+] ...
Modify Device

Send Text to User

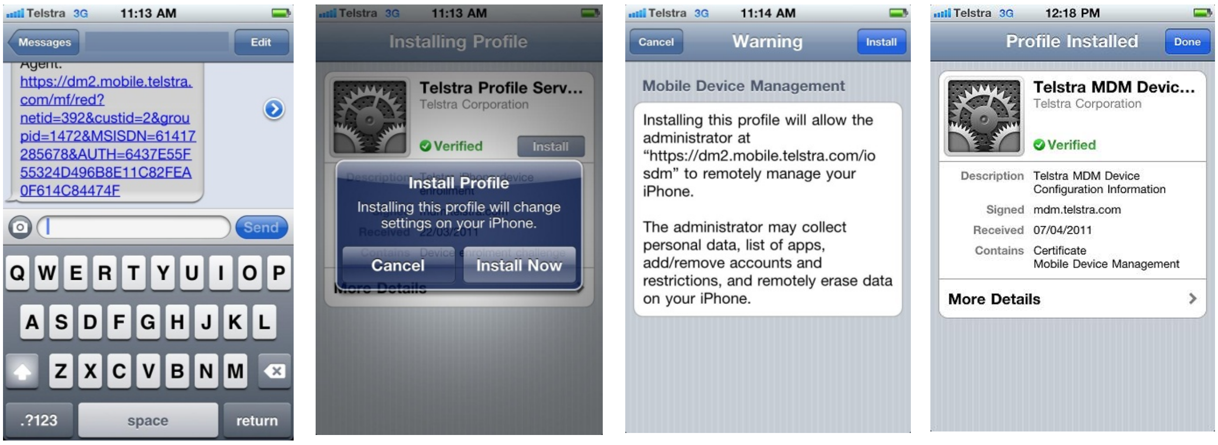
Recent Actions

REFRESH: ON| OFF

Description	Status	Date
Get Vital Signs	SUCCESS	24-Feb-2011 13:31:38
Install Device Management (OTA)	SUCCESS	24-Feb-2011 13:31:08

Profiles History Advanced

Install Device Management



Telstra 3G 11:13 AM

Messages Edit

Agent:
https://dm2.mobile.telstra.com/mf/red?netid=392&custid=2&groupid=1472&MSISDN=61417285678&AUTH=6437E55F55324D496B8E11C82FEA0F614C84474F

Send

Telstra 3G 11:13 AM

Installing Profile

Telstra Profile Serv...
Telstra Corporation
Verified Install

Install Profile
Installing this profile will change settings on your iPhone.

Cancel Install Now

Telstra 3G 11:14 AM

Cancel Warning Install

Mobile Device Management

Installing this profile will allow the administrator at "https://dm2.mobile.telstra.com/iosdm" to remotely manage your iPhone.

The administrator may collect personal data, list of apps, add/remove accounts and restrictions, and remotely erase data on your iPhone.

Telstra 3G 12:18 PM

Profile Installed Done

Telstra MDM Devic...
Telstra Corporation
Verified

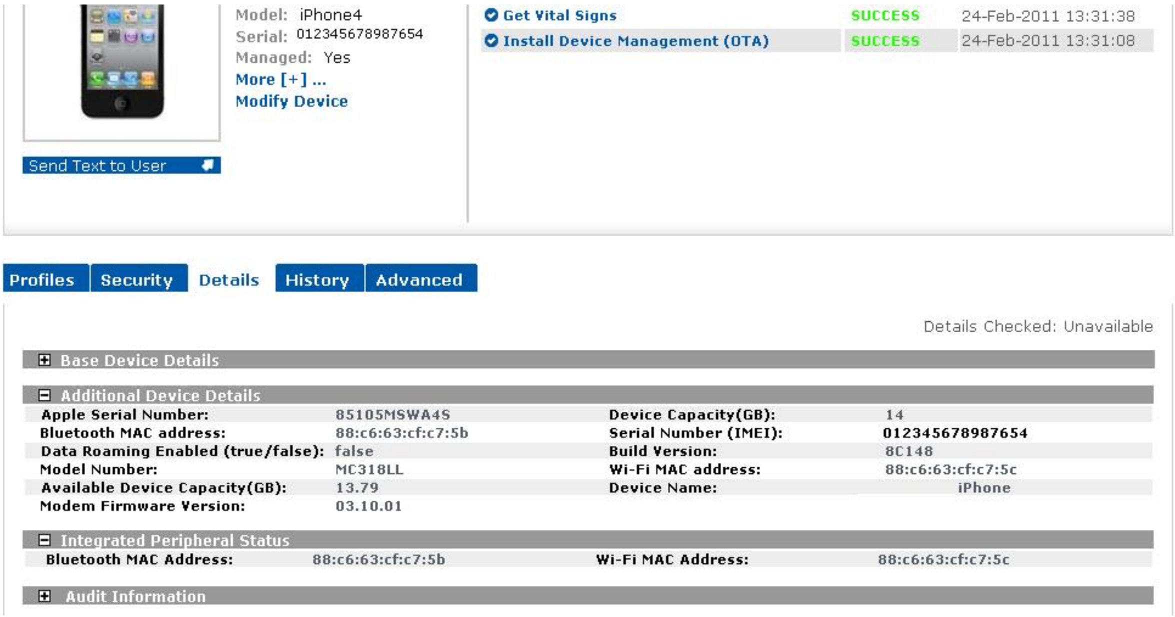
Description Telstra MDM Device Configuration Information
Signed mdm.telstra.com
Received 07/04/2011
Contains Certificate Mobile Device Management

More Details

Device Diagnostics

After a device has been successfully enrolled, the IT administrator can then view information about that particular device eg firmware version, roaming on/off, storage etc.

- Go to the diagnostics>details tab
- A list of device details will be available



Model: iPhone4
Serial: 012345678987654
Managed: Yes
More [+] ...
Modify Device

Get Vital Signs	SUCCESS	24-Feb-2011 13:31:38
Install Device Management (OTA)	SUCCESS	24-Feb-2011 13:31:08

Details Checked: Unavailable

⊞ Base Device Details

⊟ Additional Device Details

Apple Serial Number:	85105MSWA4S	Device Capacity(GB):	14
Bluetooth MAC address:	88:c6:63:cf:c7:5b	Serial Number (IMEI):	012345678987654
Data Roaming Enabled (true/false):	false	Build Version:	8C148
Model Number:	MC318LL	Wi-Fi MAC address:	88:c6:63:cf:c7:5c
Available Device Capacity(GB):	13.79	Device Name:	iPhone
Modem Firmware Version:	03.10.01		

⊟ Integrated Peripheral Status

Bluetooth MAC Address:	88:c6:63:cf:c7:5b	Wi-Fi MAC Address:	88:c6:63:cf:c7:5c

⊞ Audit Information

To refresh the diagnostic information click the “Get Vital Signs” button and the server will request an updated set of values.

Send Configuration Settings

Once a device has been successfully enrolled, the IT administrator can then send and update company settings and policies on the device silently while the user is in mobile network coverage.

Telstra has pre-loaded the following configuration settings that you might find useful

Configuration Setting	Description	IT Admin Prompts	Mobile User Prompts
Restrict YouTube	Prevents the user accessing the native YouTube application. Can be re-enabled by sending down the corresponding enable profile	NA	NA
Restrict iTunes	Prevents the user accessing iTunes. Can be re-enabled by sending down the corresponding enable profile	NA	NA
Restrict App Store	Prevents the user accessing the App Store. Can be re-enabled by sending down the corresponding enable profile	NA	NA
Restrict Explicit Content	Prevents the user accessing explicit content from iTunes. Can be re-enabled by sending down the corresponding enable profile	NA	NA
Restrict Safari Browsers	Turns off the Safari browser. Can be re-enabled by sending down the corresponding enable profile	NA	NA
Restrict Auto Data Roaming	Prevents the device from automatically trying to sync with third party servers when roaming. Can be re-enabled by sending down the corresponding enable profile	NA	NA

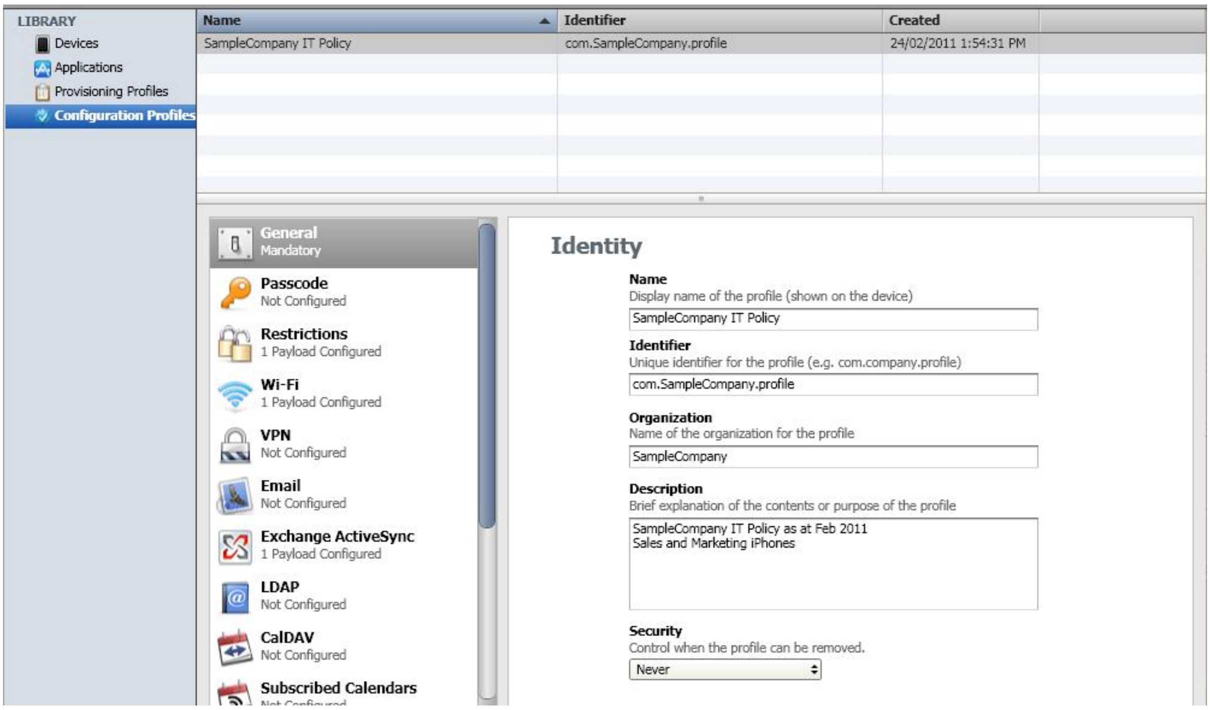
Encrypt data backups	Ensures that data backups are encrypted. Can be re-enabled by sending down the corresponding allow unencrypted profile	NA	NA
Restrict Camera and FaceTime	Turns off the camera. Can be re-enabled by sending down the corresponding enable profile	NA	NA
Restrict Multiplayer gaming	Prevents multiplayer gaming. Can be re-enabled by sending down the corresponding enable profile	NA	NA
Enforce Alpha-numeric Password	• Turns on the device lock and enforces alpha-numeric password entry. • Password can be removed remotely by using unlock under the security tab or sending a disable alpha-numeric password profile to the device.	NA	User prompted for alpha-numeric password
Disable Alpha-numeric Password	Disables the password lock on the device. Note, this does not disable any ActiveSync passwords.	NA	The user will be able to enter their device password and then remove the device password lock.
Windows Live	Configures ActiveSync for Windows Live.	NA	• User receives an SMS and must download profile • User required to enter credentials before profile is installed
Gmail	Configures ActiveSync for Gmail	NA	• User receives an SMS and must download profile • User required to enter credentials before profile is installed

All settings sent to the device are encrypted via SSL. No passwords or company settings are sent over the internet in clear text.

In addition, you can add your own company settings as follows:

Step 1: Define company settings and policies

- On your local PC you will need to download, install and run Apple's iPhone Configuration Utility(iPCU) from http://www.apple.com/support/iphone/enterprise/. Using this tool you can define the settings and policies you want your employees to have.
- Export the configuration file and save it on your local PC (.mobileconfig file).



Name	Identifier	Created
SampleCompany IT Policy	com.SampleCompany.profile	24/02/2011 1:54:31 PM

Identity

Name
Display name of the profile (shown on the device)
SampleCompany IT Policy

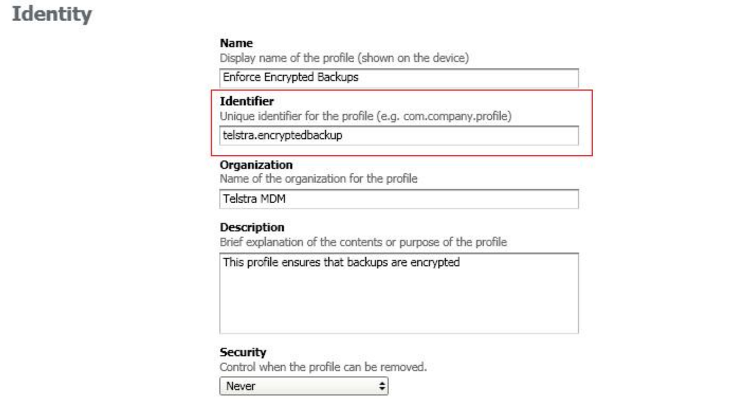
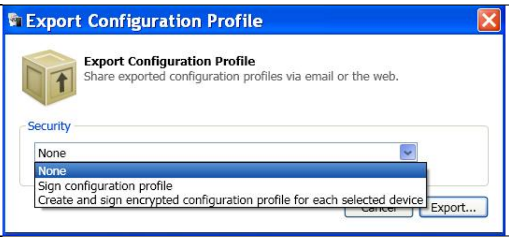
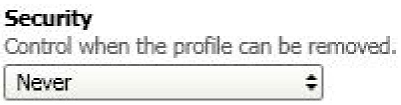
Identifier
Unique identifier for the profile (e.g. com.company.profile)
com.SampleCompany.profile

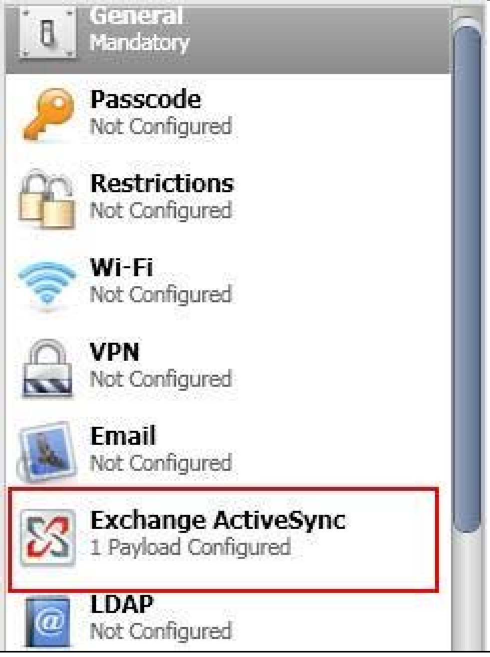
Organization
Name of the organization for the profile
SampleCompany

Description
Brief explanation of the contents or purpose of the profile
SampleCompany IT Policy as at Feb 2011
Sales and Marketing iPhones

Security
Control when the profile can be removed.
Never

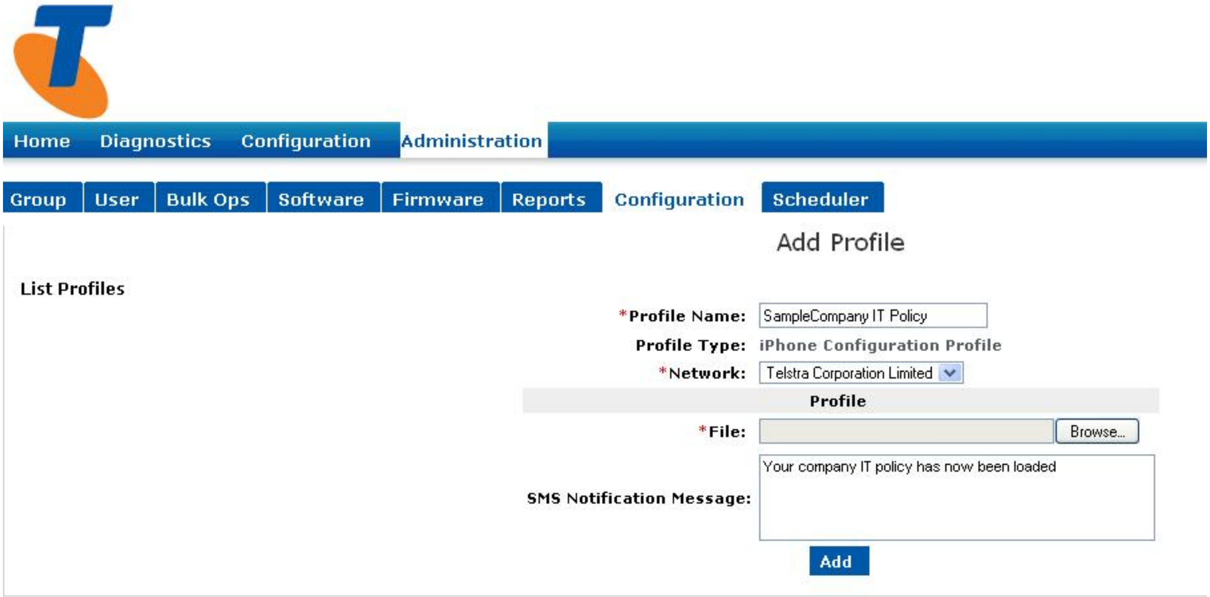
IMPORTANT:

If two profiles share the same identifier, each profile will overwrite the other when sent to the device	 Identity Name Display name of the profile (shown on the device) Enforce Encrypted Backups Identifier Unique identifier for the profile (e.g. com.company.profile) telstra.encryptedbackup Organization Name of the organization for the profile Telstra MDM Description Brief explanation of the contents or purpose of the profile This profile ensures that backups are encrypted Security Control when the profile can be removed. Never
Do NOT sign or encrypt the configuration profiles when they are exported as they will NOT work on the Telstra MDM Portal. The Telstra MDM portal uses it's own certificate and encryption.	 Export Configuration Profile Export Configuration Profile Share exported configuration profiles via email or the web. Security None None Sign configuration profile Create and sign encrypted configuration profile for each selected device Cancel Export...
It is recommended that profiles are defined so that they cannot be removed from the device.	 Security Control when the profile can be removed. Never

ActiveSync settings MUST be created using their own profile without any other payload settings defined. ActiveSync settings are sent to the device in an SMS and therefore need to be created separately. **ActiveSync profiles will not work if they are created with other payload settings**	

Step 2: Upload the settings and policies

- From the Administration>Configuration>Add Profile tab, upload the configuration file into the Telstra MDM portal
- It is up to you how many company profiles you want to upload. It is possible to create and upload one profile per setting or a single profile that has multiple settings.



Add Profile

*Profile Name: SampleCompany IT Policy

Profile Type: iPhone Configuration Profile

*Network: Telstra Corporation Limited

Profile

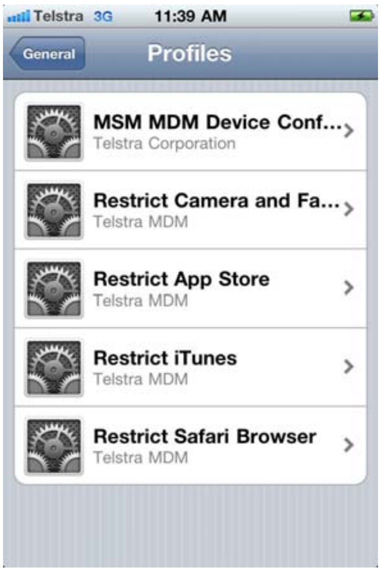
*File:

SMS Notification Message: Your company IT policy has now been loaded

Step 3: Send the settings and policies

- Your new profile will appear in the Diagnostics>Profile tab
- Click send
- Wait until the status is updated to success on the recent actions panel.
- The company policy is updated on the user's device silently.

Recent Actions Status	Meaning
PENDING	• The Telstra MDM server is in the process of sending the message to the device. • If the status remains frozen in "pending" it means that the Telstra MDM server is having trouble sending the message
SENT	• The Telstra MDM server has sent the message to the device and is waiting for a response • If the status remains frozen in "sent" it means the message has not been delivered OR the handset is not responding to the message.
SUCCESS	• The transaction was successful and the device has reported that the setting has been successful
FAILED	• The transaction was unsuccessful either because the handset rejected the message OR the server timed out after 3 minutes



Note:

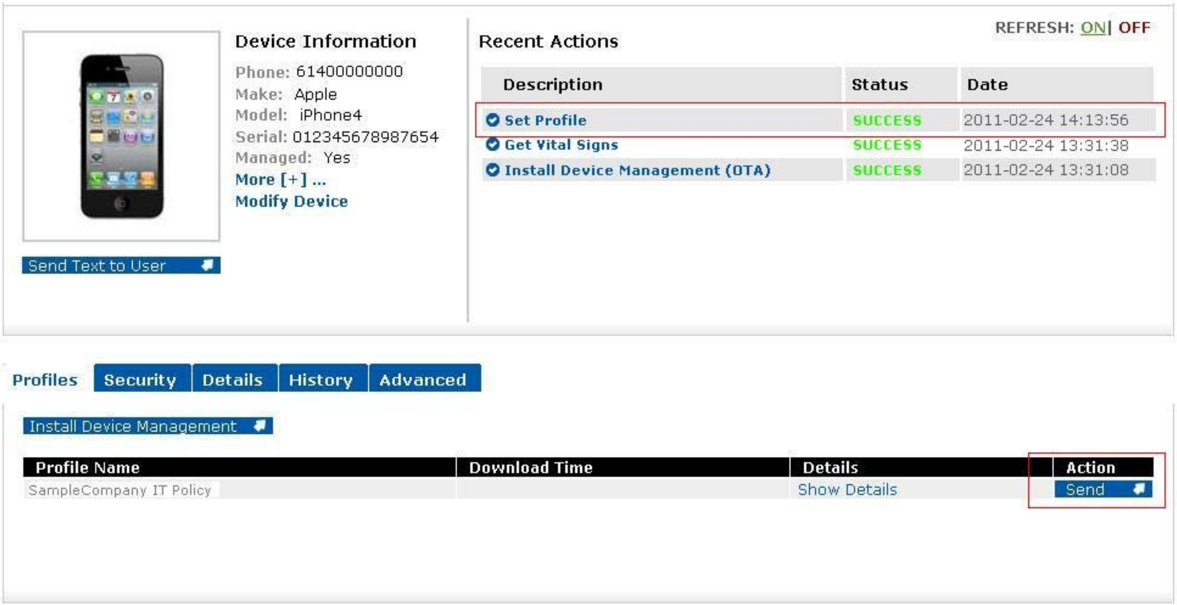
- All configuration profiles are sent to the device silently without user interaction. The only exceptions are the enrolment profile and any profiles containing Exchange ActiveSync settings. These profiles will be sent via SMS to the user.
- Multiple configuration profiles can be sent to the user's device, or an existing profile can be overwritten. Where multiple configuration profiles exist on the device(or an Exchange server has sent ActiveSync policies), the device will use the most secure settings if there is a conflict.
- Should a user manually delete the device enrolment profile, the associated configuration profiles sent from the Telstra MDM portal are also deleted and the device will need to be re-enrolled and the profiles sent again if required. The only exception to this are profiles containing ActiveSync settings. ActiveSync settings are NOT sent via the Telstra MDM protocol and are therefore not deleted when the enrolment profile is deleted.
- The Telstra MDM server does not have any visibility if the end user manually deletes profiles
- The Telstra MDM server will timeout after 3 minutes if it does not receive a successful notification from the device
- The user can also manually side load their own configuration profiles via USB or choose to manually delete profiles on their device(where a profile is able to be deleted).

IMPORTANT:
Before deploying any settings to staff these should be tested to ensure they have the desired result. Sending incorrect APN settings can prevent further Telstra MDM transactions and have charging implications so these advanced settings should be tested carefully.

The device MUST always have internet access to the following URL in order to operate correctly with Telstra MDM https://dm2.mobile.telstra.com/*. If routing via a private APN, this URL MUST be accessible.

You cannot deploy more than one APN profile at a time. Trying to send a second different APN profile (ie with a different identifier) will fail if there is one already loaded on the device. You can however over write an existing APN profile.

Profiles containing ActiveSync settings are currently sent via SMS rather than the Telstra MDM protocol and are therefore are not removed if the enrolment profile is removed. Apple does not currently support prompting the user for credentials if ActiveSync profiles are sent via the Telstra MDM protocol and hence they are sent via SMS. All ActiveSync profiles must be created without any other payload settings.


Device Information
Phone: 61400000000
Make: Apple
Model: iPhone4
Serial: 012345678987654
Managed: Yes
More [+] ...
Modify Device

Recent Actions

REFRESH: ON| OFF

Description	Status	Date
Set Profile	SUCCESS	2011-02-24 14:13:56
Get Vital Signs	SUCCESS	2011-02-24 13:31:38
Install Device Management (OTA)	SUCCESS	2011-02-24 13:31:08

Profile Name	Download Time	Details	Action
SampleCompany IT Policy		Show Details	Send

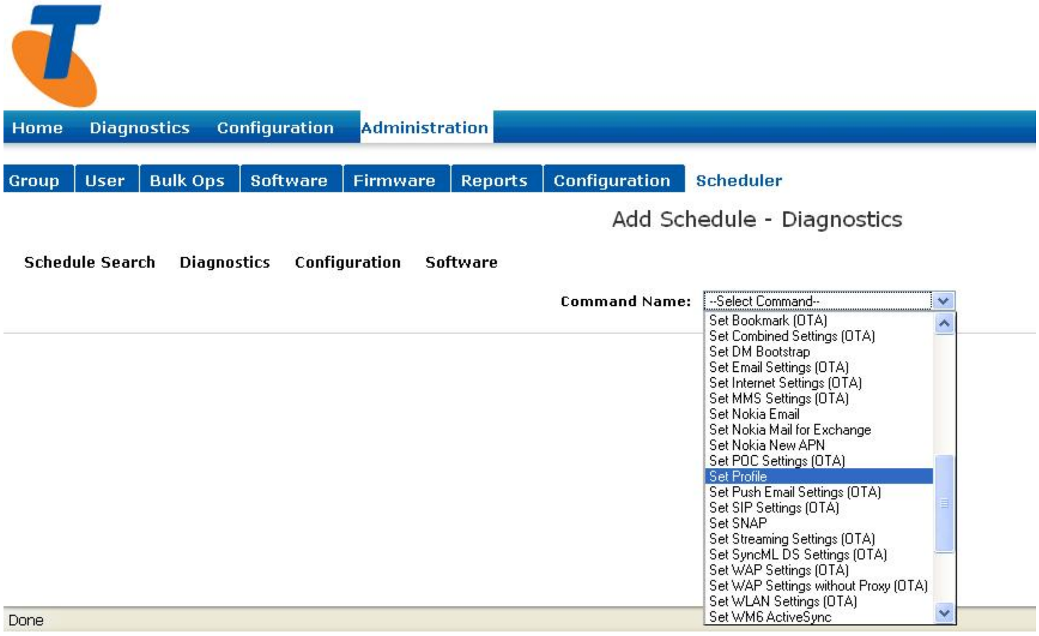
Scheduler

The scheduler function allows for sending settings to multiple devices in bulk rather than one at a time based on a set of criteria you define.

A scheduler will run a batch job based on the following criteria:

- Date and time
- Handset make and model
- Mobile number range ie between 61400000000 and 61411111111
- Customer group

From the administration>scheduler>diagnostics screen select “Set Profile” from the drop down box



Add Schedule - Diagnostics

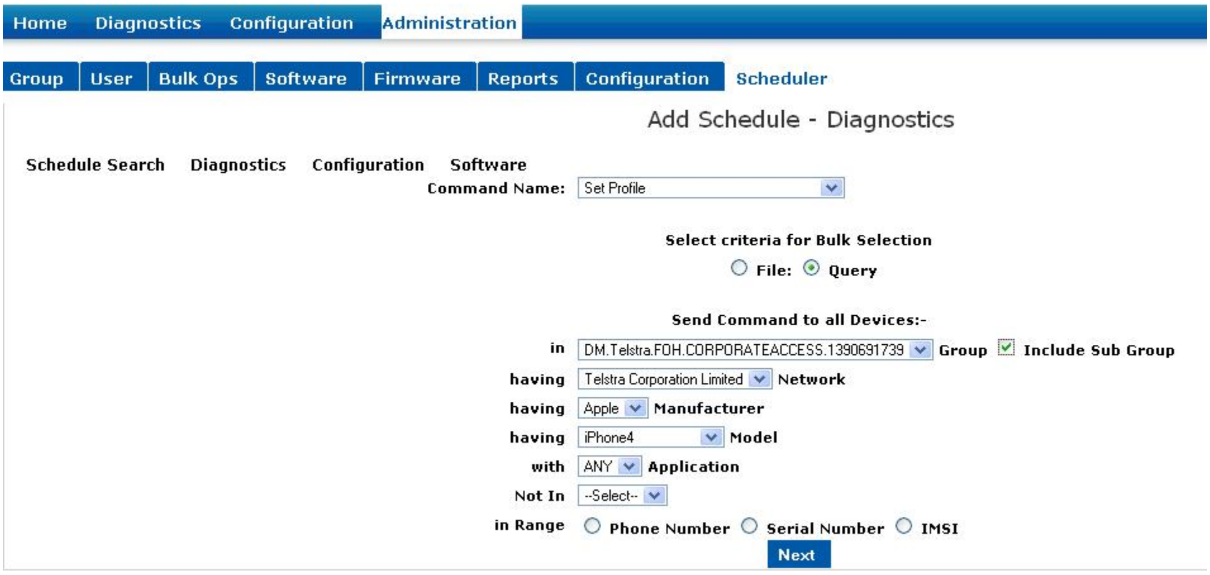
Command Name: --Select Command--

- Select “Query” as the criteria for selection
- Select iPhone as the make/model
- Select the group you want to deliver the settings to
- If you want to limit the scheduled job to a range of mobile numbers select the phone number radio button and enter the mobile number range in the format 614xxxxxxxx to 614yyyyyyyy. Otherwise do not click this radio button to send to all users with the make/model.

NB:
The following commands are available to send to iPhone devices via the scheduler.

Compatible Device	**Command**	**Description**	**Pre-Requisite**
All SMS capable devices	Send Message	Sends an SMS message	NA
iPhone	Get Vital Signs	Queries the device for diagnostics information	This command can only be used if the device has been enrolled first
iPhone	Set Profile	Sends a configuration profile to the device	This command can only be used if the device has been enrolled first
iPhone	Install Device Management (OTA)	Requests the mobile user install an enrolment profile	This command requires to mobile user to accept and install the enrolment profile

- Any other commands are NOT compatible with the iPhone.
- If you try to send these commands to Android, Nokia or Windows devices, the scheduler will try to run but will not be able to send these commands.



Add Schedule - Diagnostics

Command Name: Set Profile

Select criteria for Bulk Selection

○ File: ● Query

Send Command to all Devices:-

in DM.Telstra.FOH.CORPORATEACCESS.1390691739 Group ☑ Include Sub Group

having Telstra Corporation Limited Network

having Apple Manufacturer

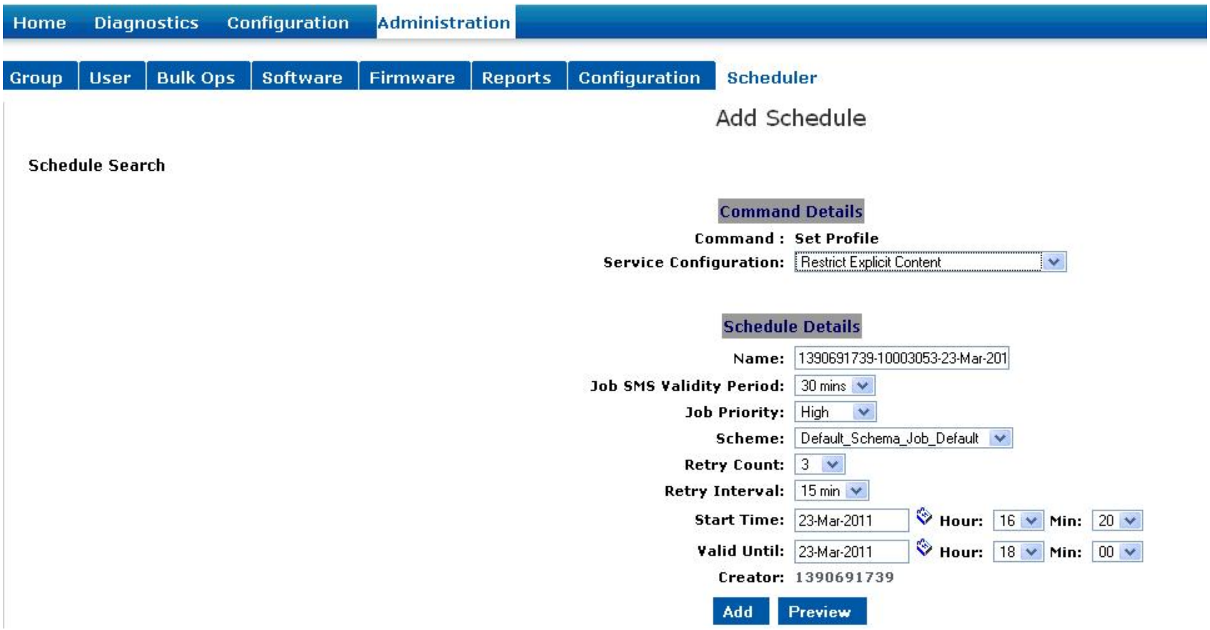
having iPhone4 Model

with ANY Application

Not In --Select--

in Range ○ Phone Number ○ Serial Number ○ IMSI

- Select the iPhone setting you wish to send in the service configuration drop down box
- Select the date time the job is to run
- Select the number of times the job will retry to send a setting if the device is not contactable and how often it retries
- Click the “Preview” button to review how many users will be sent the settings
- If happy with the criteria for the job, click “Add”



Add Schedule

Command Details

Command : Set Profile

Service Configuration: Restrict Explicit Content

Schedule Details

Name: 1390691739-10003053-23-Mar-201

Job SMS Validity Period: 30 mins

Job Priority: High

Scheme: Default_Schema_Job_Default

Retry Count: 3

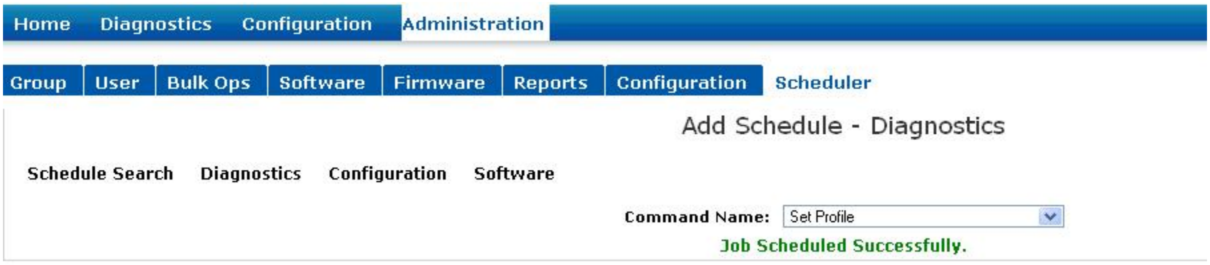
Retry Interval: 15 min

Start Time: 23-Mar-2011 Hour: 16 Min: 20

Valid Until: 23-Mar-2011 Hour: 18 Min: 00

Creator: 1390691739

The job will then be submitted and the Telstra MDM Portal will action the scheduled job based on the criteria selected.

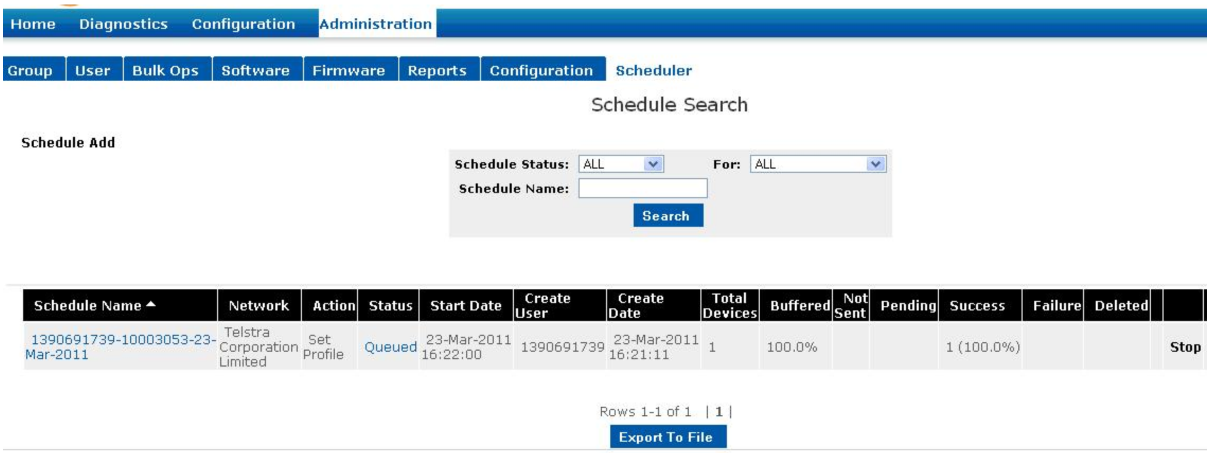


Add Schedule - Diagnostics

Command Name: Set Profile

Job Scheduled Successfully.

To check the progress of a scheduled job go to administration>scheduler>schedule search and click “Search”. The success column will show 100% when completed.



Schedule Search

Schedule Status: ALL For: ALL

Schedule Name:

Schedule Name ▲	Network	Action	Status	Start Date	Create User	Create Date	Total Devices	Buffered	Not Sent	Pending	Success	Failure	Deleted		
1390691739-10003053-23-Mar-2011	Telstra Corporation Limited	Set Profile	Queued	23-Mar-2011 16:22:00	1390691739	23-Mar-2011 16:21:11	1	100.0%			1 (100.0%)				Stop

Rows 1-1 of 1 | 1 |

Lock, Unlock and Wipe

Lock

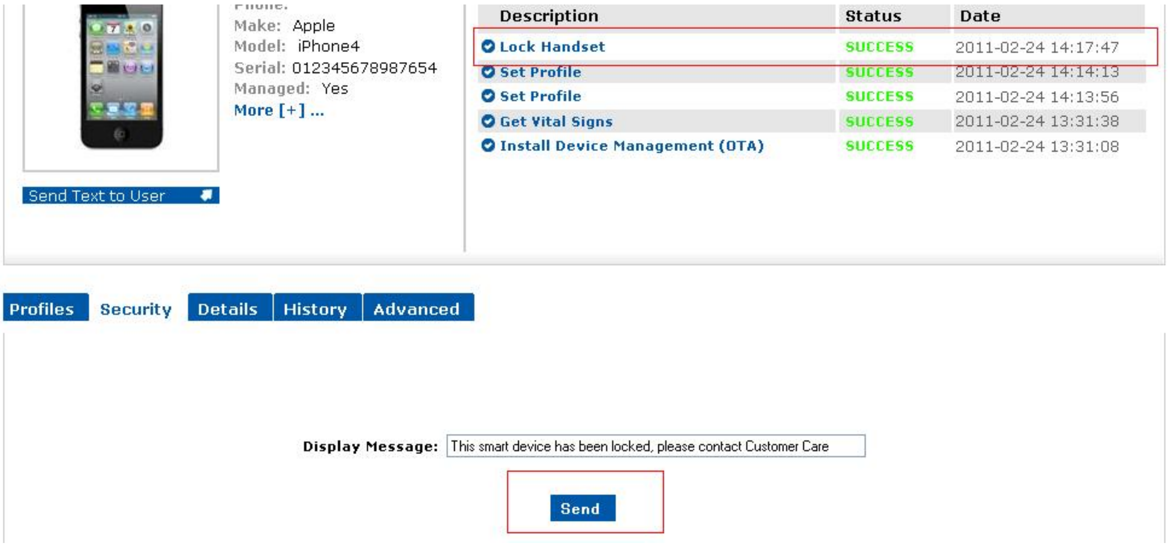
The lock feature will allow an administrator to remotely lock the device and force the user to enter a password if they want to access the device. The device must be in coverage and be enrolled with the Telstra MDM portal.

There are two scenarios where this feature can be used:

1. If the device has a password lock setup either by the Telstra MDM portal or the user, this lock will be activated
2. If the device has an ActiveSync password set, this lock will be activated.

Where a device does not have a password lock or ActiveSync password policy, the lock feature will fail as there is no password on the device to activate.

- Go to Diagnostics>Security tab
- Click “lock device” button



Make: Apple
Model: iPhone4
Serial: 012345678987654
Managed: Yes

Description	Status	Date
Lock Handset	SUCCESS	2011-02-24 14:17:47
Set Profile	SUCCESS	2011-02-24 14:14:13
Set Profile	SUCCESS	2011-02-24 14:13:56
Get Vital Signs	SUCCESS	2011-02-24 13:31:38
Install Device Management (OTA)	SUCCESS	2011-02-24 13:31:08

Display Message: This smart device has been locked, please contact Customer Care

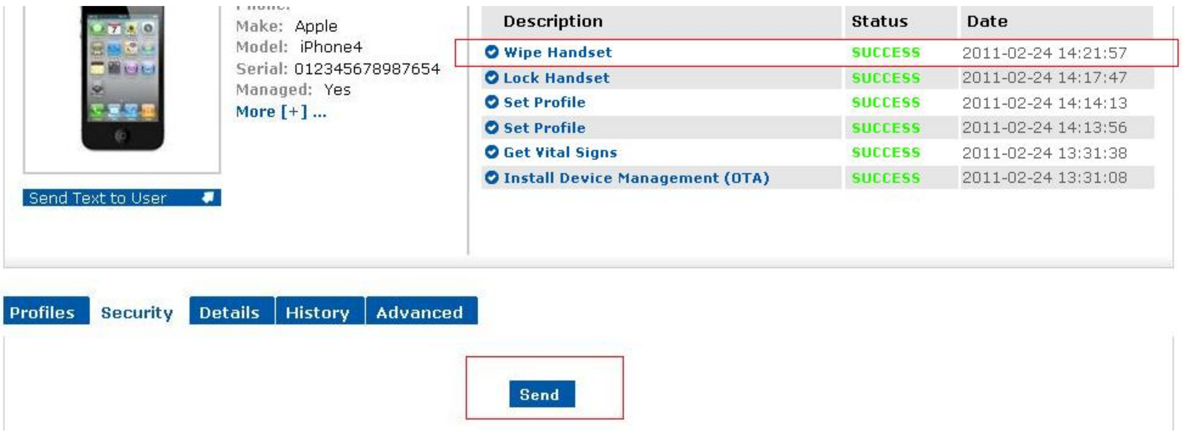
Note:

- The lock setting will fail if the device does not have a password configuration profile installed, the user has not enabled a device password or an ActiveSync password policy is not enabled.
- The Telstra MDM server will timeout after 3 minutes if it does not receive a successful notification from the device

Wipe

Where a device is enrolled, the IT administrator can then remotely wipe this device at any time when the device is in coverage. **THIS WIPES THE ENTIRE DEVICE**.

- Go to Diagnostics>Security tab
- Click “wipe device” button



Make: Apple
Model: iPhone4
Serial: 012345678987654
Managed: Yes
More [+] ...

Description	Status	Date
Wipe Handset	SUCCESS	2011-02-24 14:21:57
Lock Handset	SUCCESS	2011-02-24 14:17:47
Set Profile	SUCCESS	2011-02-24 14:14:13
Set Profile	SUCCESS	2011-02-24 14:13:56
Get Vital Signs	SUCCESS	2011-02-24 13:31:38
Install Device Management (OTA)	SUCCESS	2011-02-24 13:31:08

Note:

- Wiping the device deletes all company and person information from the device. The user will need to restore their personal information via iTunes
- To perform a selective wipe the end user will need to manually remove the enrolment profile and all company settings sent via the Telstra MDM server will be removed.
- The device will need to be re-enrolled if the Telstra MDM portal wants to send further settings.
- The Telstra MDM server will timeout after 3 minutes if it does not receive a successful notification from the device

Unlock

The unlock feature allows you to remove the device password lock.

There are two unlock scenarios:

1. If the device has a password lock setup either by the Telstra MDM portal or the user, this lock will be removed
2. If the device has an ActiveSync password set, the mobile user will be forced to change their ActiveSync password.

- Go to Diagnostics>Security tab
- Click “unlock device” button

Reporting

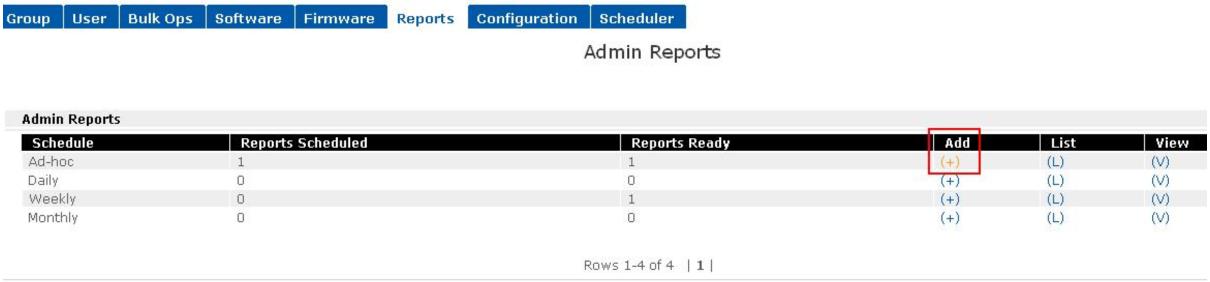
From the Admin Reports screen, standard reports are available.

Once a report has been run, data can be exported to a .csv file for further manipulation.

All reports can be run on an ad-hoc basis(ie as needed). The command history report can also be run on a recurring basis(ie daily, weekly, monthly).

To run an adhoc report:

- Go to Administration>Reports
- Click the add “(+)” link in the Ad-hoc report row
- Select the report you want to run



Admin Reports

Admin Reports

Schedule	Reports Scheduled	Reports Ready	Add	List	View
Ad-hoc	1	1	(+)	(L)	(V)
Daily	0	0	(+)	(L)	(V)
Weekly	0	1	(+)	(L)	(V)
Monthly	0	0	(+)	(L)	(V)

Rows 1-4 of 4 | **1** |

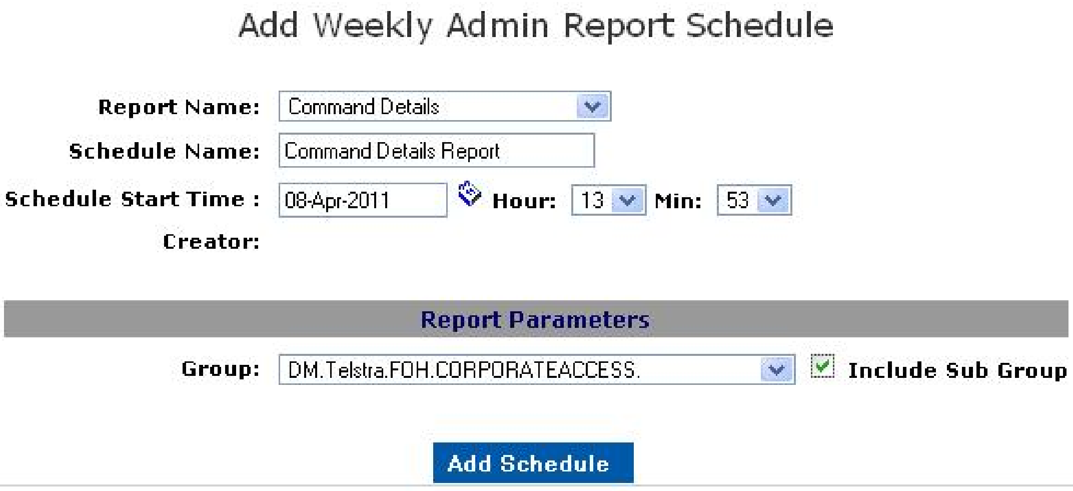
The following standard reports are available on the Telstra MDM portal:

Report Name	**Description**	**Type of Report**
User/Device Inventory	A list of all your mobile numbers, device models and device serial numbers(IMEI)	Can be run on an ad-hoc basis only ie once off as needed
Device Application Inventory	Not available for the iPhone	NA
Device Firmware Summary	Not available for the iPhone	NA
Traffic and Downloads Report	A view of how much data is being transferred between the Telstra MDM Server and each device	Can be run on an ad-hoc basis only ie once off as needed
Command Details Report	List of all the settings that have been sent to the device	Can be run once, daily, weekly or monthly

Recurring reports can be scheduled from a set date/time and will then be run automatically by the Telstra MDM Portal every day, week or month. The Telstra MDM Portal will save these recurring reports for a period of 90 days and then delete them.

To schedule a recurring report

- click the add “(+)” link to create either a daily, weekly or monthly report.
- Select the report you wish to run from the drop down list
- Give the report a name
- Select the date and time you want the report to run from



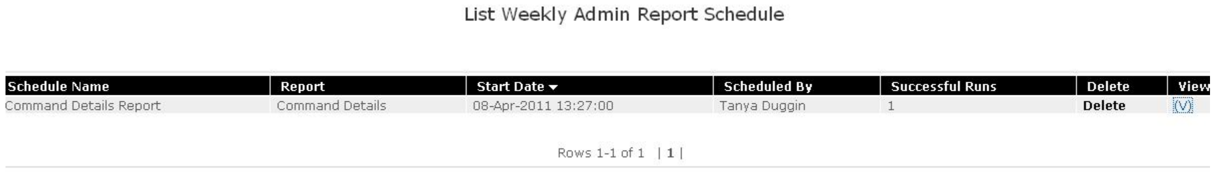
Add Weekly Admin Report Schedule

Report Name:	Command Details
Schedule Name:	Command Details Report
Schedule Start Time :	08-Apr-2011 Hour: 13 Min: 53
Creator:	

Report Parameters

Group: DM.Telstra.FOH.CORPORATEACCESS. ☑ Include Sub Group

The Telstra MDM Portal will then schedule your report to run and a list of scheduled reports and status are listed when you click the listed "(L)" link from the Admin Reports main screen. To delete a recurring report click the delete link.

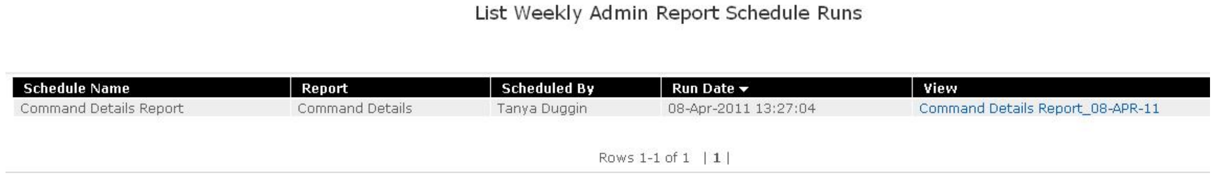


List Weekly Admin Report Schedule

Schedule Name	Report	Start Date ▾	Scheduled By	Successful Runs	Delete	View
Command Details Report	Command Details	08-Apr-2011 13:27:00	Tanya Duggin	1	Delete	(V)

Rows 1-1 of 1 | 1 |

Once a report has been successfully run, the report can be viewed and exported by clicking on the view "(V)" link from the Admin Reports main screen.



List Weekly Admin Report Schedule Runs

Schedule Name	Report	Scheduled By	Run Date ▾	View
Command Details Report	Command Details	Tanya Duggin	08-Apr-2011 13:27:04	Command Details Report_08-APR-11

Rows 1-1 of 1 | 1 |

FAQs

How do I access the Telstra MDM Portal?	https://mdm.telstra.com
How do I get a login?	The first time you login you will need to contact the Telstra MDM helpdesk at wireless@team.telstra.com and get a password
How do I get support?	Send an email to wireless@team.telstra.com
What is enrolment?	A process of setting up authorised authentication between

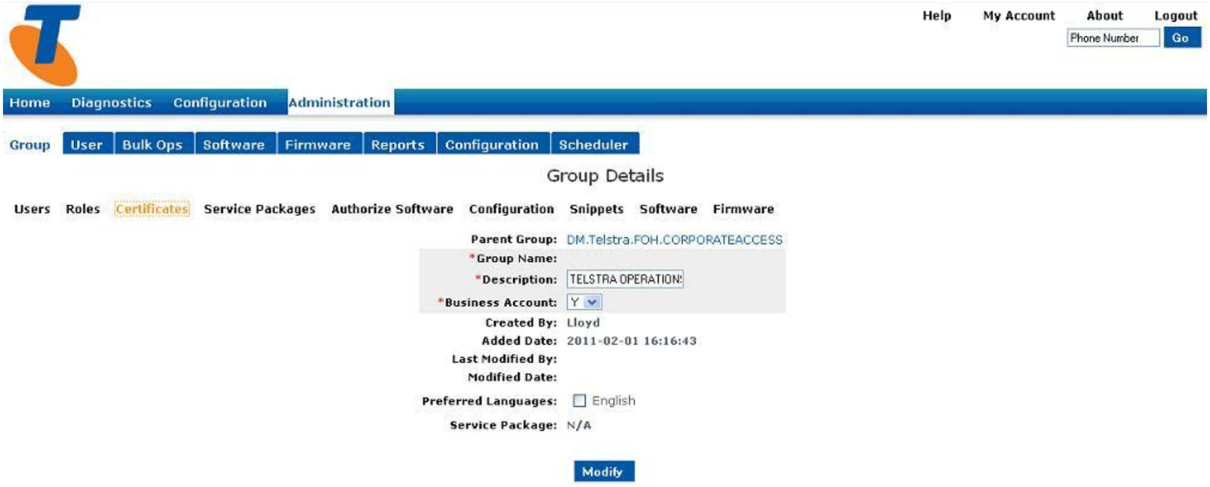
	the device and the Telstra MDM portal. Only needs to be done once per device (unless the user manually deletes it or the device is wiped)
What if an employee leaves the organisation?	• The user can manually remove the enrolment profile and all company settings will be wiped • The device can be wiped remotely and the user will need to restore personal items via iTunes
Can a device be selectively wiped so personal settings remain?	Yes, a user will need to manually delete the enrolment profile and all the Telstra MDM policies and settings will be removed
Will Exchange Server security settings clash with the Telstra MDM settings?	No. The device will use the most secure setting
Can I get Telstra MDM access on standard data plans?	No, each user must have a Telstra Mobile Connect data plan to be eligible
Will Telstra MDM work with other carrier's SIM cards	No
Will Telstra MDM work while the user is roaming internationally	Yes, however international roaming charges apply. It is also only available in countries where Telstra has International Roaming arrangements with carriers. Features and capabilities can differ from network to network & will depend on the devices you are using. Telstra cannot guarantee that services will be available at all times.
Will Telstra MDM work with other carrier's devices	iPhone devices from other carriers may work on Telstra's MDM portal if the device is using a Telstra SIM . However, Telstra cannot guarantee that it will.
Why doesn't the Telstra MDM portal display a picture of the users device?	The device has either been swapped recently or is not supported on the portal. Telstra refreshes device information every night.
How do I know when a setting has been successfully sent to the device.	Under the recent actions panel the status of all settings you send are listed. Note that it can take up to 3 minutes for the Telstra MDM Portal to return a failure as this is how long it takes to timeout
Why do I need to group my mobile users under a single billing account?	This allows you to manage all these users with a single login. You would need to manage multiple logins and passwords otherwise.

Appendix - Upload Apple Certificate

You must have an existing subscription to the Apple iOS Developer Program (Apple charge an annual fee for this). Under this Program you will have received an Apple certificate which you will need to upload into Telstra's MDM portal.

The Apple certificate (.p12 file) and Apple password you received when you subscribed to the Apple iOS Developer Program, can be uploaded into the Telstra MDM portal from the administration tab as follows (this process only needs to be done once for your company).

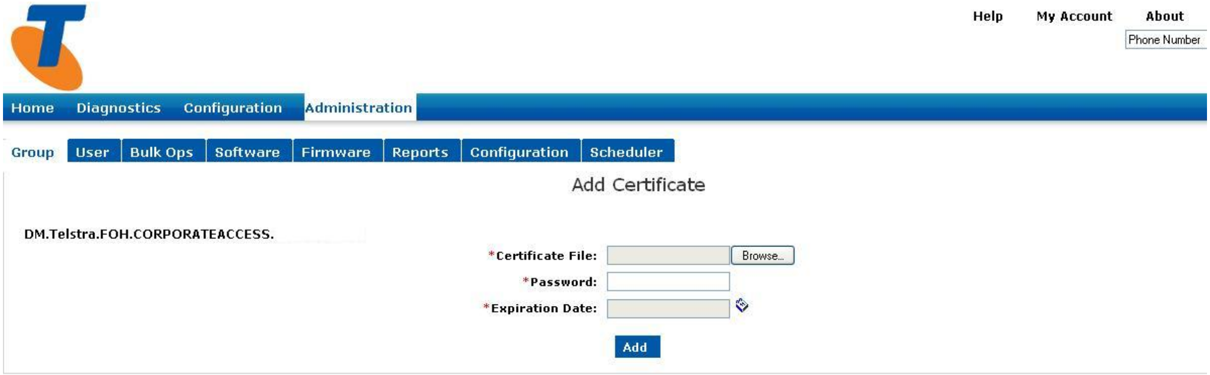
1. Go to the administration tab>groups and enter your 10 digit login number, click search
2. Select you company group and a "Group Details" screen will appear



Group Details

Parent Group: DM.Telstra.FOH.CORPORATEACCESS
*Group Name:
*Description: TELSTRA OPERATION!
*Business Account: Y
Created By: Lloyd
Added Date: 2011-02-01 16:16:43
Last Modified By:
Modified Date:
Preferred Languages: □ English
Service Package: N/A

3. Select the certificate link and then upload your certificate, password and expiration date



Add Certificate

DM.Telstra.FOH.CORPORATEACCESS.

*Certificate File:
*Password:
*Expiration Date:

Important:

- **The Apple certificate needs to be registered using the naming convention "com.apple.mgmt.[your company name]" eg com.apple.mgmt.telstra**
- **Note: as your certificate expires every 12 months, you must register it again if you have renewed your subscription with Apple**

- **Load your certificate at the very top group level for your company ie only ONE certificate for your company is required.**

Definitions

Telstra MDM	Telstra Mobile Device Management
Apple iPhone Configuration Utility (iPCU)	A desktop application from Apple which allows customers to create company policies and settings for us on their iPhones
Enrolment Profile	Process of setting up authentication between the device and the Telstra MDM portal. If successful, an enrolment profile is loaded onto the device and the server can send settings to the device silently
Configuration profile	A list of settings and restrictions that define what a device can and cannot do.
IT administrator	A person or persons nominated by the customer to manage their fleet of devices
iOS	Operating system of Apple iPhone devices
APN	Access Point Name. A connection address used by your device to connect to the internet or private network. Not to be confused with APNS
APNS	Apple Push Notification Service is used to forward notifications from third parties to Apple devices. Not to be confused with APN
Apple Certificate	Required to be uploaded on the Telstra MDM Portal. Each Telstra MDM customer requires their own Apple Certificate which is uploaded into the Telstra MDM Portal.
IMEI	Unique 15 digit serial number of a device
URL	Uniform Resource Locator. Global address of a web page, file or other content on the web.

Apple, iPhone and iTunes are Trade marks of Apple Inc., registered in the U.S. and other countries. iTunes are for legal or rightholder-authorized copying only. Don’t steal music.