Verizon MDM – UEM
Unified Endpoint Management

Version: 1.0
Last Updated: 3/29/18
# Table of Contents

Overview  .................................................................................................................................................. 4
Account Dashboard ................................................................................................................................. 4

Unified Endpoint Management (UEM) Quick Start .............................................................................. 6
  Apple Push Certificate ............................................................................................................................ 6
  Security Policy ........................................................................................................................................ 8
  Add Users ............................................................................................................................................ 9
  Email Setup ....................................................................................................................................... 10
  Add Applications ................................................................................................................................ 11

Devices & Groups .................................................................................................................................. 14
  Groups .............................................................................................................................................. 14
  Devices ........................................................................................................................................... 15
  Users ............................................................................................................................................... 18

Policy ..................................................................................................................................................... 20
  Policies ............................................................................................................................................ 20
  Policy Assignments ............................................................................................................................ 22

Events & Actions .................................................................................................................................. 22

Reports Tab .......................................................................................................................................... 24
  Reports ............................................................................................................................................ 24

Admin Tab ............................................................................................................................................. 25
  Account Settings ............................................................................................................................... 26
    Account Options .............................................................................................................................. 26
    Android For Work ........................................................................................................................... 27
    Application Ranking ....................................................................................................................... 28
    Apple Push Certificate ................................................................................................................... 29
    Bulk Import .................................................................................................................................. 30
    Certificates .................................................................................................................................... 31
    Device Search Columns ................................................................................................................ 32
    Domains ......................................................................................................................................... 33
    Google Cloud Messaging ................................................................................................................ 34
    Group Ranking ............................................................................................................................... 35
    Pre-Approved Devices .................................................................................................................. 36
Overview

Verizon's Unified Endpoint Management provides a unique strategic solution which enables customers to overcome the challenges of deploying and managing mobility services through a unified, user-based solution.

Through the Verizon MDM Portal, customers can select which features of the service are deployed to each user; fine-tuning the service and removing the need to deploy unnecessary functionality to all users. As a result, Verizon MDM enables all the front end functionality of mobility management, without any the back-end difficulties associated with such a feature-rich service.

Account Dashboard

The account dashboard shows a comprehensive display of company information. The Widgets show pertinent information.

- The Quick Start Menu widget provides shortcuts to Quick start menus for Unified Endpoint Management (UEM) and Broadband Hotspot Management (BBHM).
- Alerts include 5 default alerts (newly enrolled devices, devices out of compliance, jailbroken devices, roaming devices (does not include Jetpacks), Apple Push Notification Certificate (expiration less than 60 days).
- Clicking on an alert navigates to the details of the alert for an administrator to take action.
- Clicking on any dashboard widget navigates to the page with the underlying data.
- The gear icon in the upper right corner allows users to add/remove ‘Dashboard’ widgets.
Unified Endpoint Management (UEM) Quick Start

Consolidated page with the basic features for getting started with UEM.

Apple Push Certificate

The Apple Push Certificate is used to communicate securely to the iOS devices. The process to obtain the certificate has been automated in the portal to make it as simple as possible for the administrator. Please follow the 3 simple steps to obtain and install the Apple push certificate.

1. From the Quick Start menu choose **Apple Push Certificate** and then select configure.
2. Click on the Download CSR button. The Certificate Signing Request (CSR) page will now display. After filling out the form, press the Download CSR button to save the CSR file to your local machine.

3. After the signed CSR is downloaded, click the link in the next step (2) and sign into the Apple website with any Apple ID.

4. After logging into the Apple website, click the Create a Certificate Button.

5. After accepting terms, you will be brought to a page where you can upload the CSR created in Step 1. Click the Browse button to locate the CSR and upload to the Apple site. Follow the prompts to download the new certificate from Apple and save to your local machine.

6. The final step is to upload the certificate from Step 5 to the Unified Endpoint Management portal. Click the Browse button to locate the certificate downloaded in Step 5, then click Upload Certificate to install the certificate to the portal.

7. After the certificate is successfully installed, the Apple Push Certificates page will state that the Apple Push Certificate was uploaded and will indicate the date it will remain active until.
Security Policy

Select one of the 3 security policies and then save to confirm your selection.

Security Levels:
- **High**: Storage encryption on, jailbreak/root detection on, 8 digit password (number, upper case character, special character), new password every 60 days, last 5 passwords cannot be re-used
- **Medium**: Storage encryption on, jailbreak/root detection on, 6 digit alphanumeric password, new password every 120 days, last 2 passwords cannot be re-used
- **Low**: 4 digit pin code + jailbreak/root detection, Storage encryption on
Add Users

Click on the **Add New User** button and you will be taken to the Add New User form which you can fill out and then click the **Save** button. You also have the ability to link to the Search Users screen by selecting the link.
Email Setup

Select an email provider by click on a logo and confirm your selection by clicking the Save button.
Add Applications

Here you have the option to add new applications or select from existing ones. Click on the **Add New Application** button. On the next screen you will be presented with four sections you must fill out from but are these are dynamic based on the platform you choose.
Unified Endpoint Management (UEM)

**Android:**

- Platform: Android
- Source: App Store
- Search Store
- Google Play URL

**iOS:**

- Platform: iOS
- Source: App Store
- Search Store
- App Store ID
- Prevent App Data Backup: No
- Sync Store Version: No

**Windows Desktop:**
Unified Endpoint Management (UEM)

Windows Phone:

Platform
Source
Display Name
Version
Upload Application Library
More Info Pop Up
More Information
Files In Cab To Run
Command Line
Key File Path
Key File Registry Key
Key File Version
Key File Date And Time
Package Checksum
Related Software
Class ID
Install For New Users
Run As Administrator
Reboot After Install
Restart And Resume
Required Operating Systems
Devices & Groups

The Devices & Group menu enables Administrators to manage all their Devices, Users and Groups. A specific Dashboard provides additional details on all of these.

Clicking on “Devices” or “Users” will toggle the chart to show further details of these. Different tabs are available to access the Group, Device or User functionality.

Groups

The Groups tab lists all the existing groups, showing the number of users and devices in each group (note: a device and user can belong to multiple groups). The list can be sorted by clicking on each column header. Clicking on a group name will navigate to the group page information, which displays the same information as the Mobility Services Dashboard page, just specific to the selected group.

Clicking the “Create Group” button opens the page to create a new group.
Unified Endpoint Management (UEM)

Create Group

- **Group Name** – Create a group name. Each group must have a unique name.
- **Add New Devices/Users to Group** – Check the boxes if all new Device and/or Users are to be subsequently and automatically added to the group.
- **Add Existing Devices (Optional)** – Add existing devices to the new group by MDN. After the group is created memberships can be managed from the Devices tab.

Devices

The Devices tab lists all available devices which can be ranked by clicking on a column header.
The devices list can be filtered by clicking on the filter icon ( ).

The details of the filtered devices can be exported to a tab separated file by clicking on the export icon.

Clicking on a Device name will open the profile page of that device:
The Device profile page provides an overview of the device status:

- **Device** – Make & Model of the device
- **Associated user** – a user the device may be assigned to in the Verizon MDM system
- **Ownership** – corporate, personal or unknown (can be changed by clicking on the edit icon). Note: Only “corporate” ownership is currently supported.
- **Status** – Active, not activated, archived
- **Platform** – device type
- **Last check-in** – time elapsed since the device last checked in.
- **Associate device** – click on the associate device icon to associate it to a specific user.

The Device profile also has eleven collapsible trays with additional information on the device:

- **GENERAL**
  - Network
  - Hardware
  - Security
- **Group Memberships**
  - List of assigned groups
- **Location**
  - Map showing location of device
- **Applications**
  - List of installed applications
- **Installed Policies**
  - List of installed policies
- **Assigned Policies**
  - List of assigned policies
- **Client Logs**
  - List of uploaded client logs
- **Command History**
  - List of commands issued to device
- **Check-in History**
  - List of check-ins recorded for this device.
- **Certificates**
  - List of installed certificates
- **Reports**
  - List of reports
Users
The Users tab lists all available users which can be ranked by clicking on a column header. New users can be created by clicking on the “Add New User” button.

The User list can be filtered by clicking on the filter icon ( filtro ).
The details of the filtered users can be exported to a tab separated file by clicking on the export icon.

Clicking on a User name will open the profile page of that user:

![User profile page](image)

The User profile provides an overview of the User status:

- **User** – Name of User
- **User ID**: Verizon MDM ID of User
- **Status**: Active, Inactive
- **Registered** – registration status

The User Profile also has three collapsible trays with additional information on the user:

- **Devices** – list of devices assigned to the user. Clicking on a device will navigate to the Device Profile page
- **Group Memberships** – lists group membership of the user
- **Profile** – displays information about the user (name, e-mail, etc.), password reset and user deactivation.
Policy
The Policy menu enables Administrators to manage all the device policies. The Policy Dashboard displays the number of policies created and assigned to devices. Different tabs are available to access the Policies and Policy Assignment.

Policies

The Policy tab lists all policies which have been created. Policies can be ranked by clicking on a column header as well as filtered by clicking on the filter button (▁▁▁▁)

The Policy tab lists all policies which have been created. Policies can be ranked by clicking on a column header as well as filtered by clicking on the filter button (▁▁▁▁).

The Policy tab lists all policies which have been created. Policies can be ranked by clicking on a column header as well as filtered by clicking on the filter button (▁▁▁▁).
The Policy Assignments tab lists all policies which assigned by group, policy type, Assigned Item (Policy Name) date and assignee. The group name, assigned name and assigned by fields can be clicked on to navigate to their respective pages.

The “Add Policy” button opens up the policy creation page. The policy types displayed can be searched or filtered by policy type or device platform.

Click on the desired policy type to open its configuration page.
After a policy has been created it can be assigned to a group or groups through the Edit Policy page of each group (see above).

Policy Assignments

Events & Actions

An Events & Actions policy allows an administrator to define custom and/or dynamic events to trigger actions. This allows the automation of notifications, group assignments, device commands and more.

- creation of alerts (e.g. device out of compliance)
- automatic group assignments (e.g. based on AD attributes returned to Verizon MDM)
- automatic device commands
- user notifications
- user management

<table>
<thead>
<tr>
<th>Event Types</th>
<th>Action Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigned Applications</td>
<td>De-Activate User</td>
</tr>
<tr>
<td>Customer Status</td>
<td>Group Assignment</td>
</tr>
<tr>
<td>Device Property Value</td>
<td>Issue Device Command</td>
</tr>
<tr>
<td>Installed Application</td>
<td>Notification</td>
</tr>
<tr>
<td>LDAP Group Membership</td>
<td>Set Device Ownership</td>
</tr>
<tr>
<td>Radius</td>
<td></td>
</tr>
<tr>
<td>User Property Value</td>
<td></td>
</tr>
</tbody>
</table>

Each action is triggered by an event, such as a device reporting usage information, a device not checking-in within a certain time-frame, the user belonging to a new group. Based on a single event, multiple actions can be triggered in succession.
Add Events & Actions

Define custom, dynamic events to trigger actions. This allows the automation of notifications, group assignments, device commands and more.

**Details**

**Events**
- Assigned Application
- Customer Status
- Device Property Value
- Installed Application
- LDAP Group Membership
- RADIUS Attribute Value
- User Property Value

Add a new Event

**Actions**

Add a new Action
Reports Tab
User based reports that are assigned to the user will be listed under this tab.

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Check-In Summary: Internet Devices</td>
<td>Device Check-in Summary for the specified number of days exclusively for Internet Devices. Contains breakdowns by model.</td>
</tr>
<tr>
<td>Device Count With No Recent Check-in</td>
<td>Shows the number of devices without a check-in since the specified number of days. Defaults to 7 days.</td>
</tr>
<tr>
<td>Device Platforms</td>
<td>Shows a count of devices grouped by platform.</td>
</tr>
<tr>
<td>Events</td>
<td>Shows a list of Events and the number of executed actions.</td>
</tr>
<tr>
<td>User and Device Counts By Group</td>
<td>Shows the number of users and devices by group, including current statuses.</td>
</tr>
<tr>
<td>Verizon MDM Billing</td>
<td>Shows the total number of purchased licenses and the number of licenses currently in use.</td>
</tr>
</tbody>
</table>

Reports

- Device Check-in Summary: Internet Devices: Device Check-in Summary for the specified number of days exclusively for Internet Devices. Contains breakdowns by model.
- Device Count With No Recent Check-in: Shows the number of devices without a check-in since the specified number of days. Defaults to 7 days.
- Device Platforms: Shows a count of devices grouped by platform.
- Events: Shows a list of Events and the number of executed actions.
- User and Device Counts By Group: Shows the number of users and devices by group, including current statuses.
- Verizon MDM Billing: Shows the total number of purchased licenses and the number of licenses currently in use.
Admin Tab

The Administration tab consists of 4 subcategories:

- Accounts Settings
- Apple DEP
- Apple VPP
- Servers

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Options</td>
<td>Global account settings.</td>
</tr>
<tr>
<td>Android For Work</td>
<td>Link your Google For Work account to deploy and configure Android For Work.</td>
</tr>
<tr>
<td>Application Ranking</td>
<td>Rank applications to specify an installation order.</td>
</tr>
<tr>
<td>Apple Push Certificate</td>
<td>Configure an Apple Push Certificate to allow Apple device enrollment.</td>
</tr>
<tr>
<td>Bulk Import</td>
<td>Bulk import users, devices, settings and more.</td>
</tr>
<tr>
<td>Certificates</td>
<td>Configure certificates which can be used in Wi-Fi, VPN and Exchange configurations.</td>
</tr>
<tr>
<td>Device Search Columns</td>
<td>Customize the displayed device search result columns.</td>
</tr>
<tr>
<td>Domains</td>
<td>Configure domains for portal user accounts.</td>
</tr>
<tr>
<td>Google Cloud Messaging</td>
<td>Configure Google Cloud Messaging to enable over-the-air Android device administration.</td>
</tr>
<tr>
<td>Group Ranking</td>
<td>Rank groups to specify a priority order. The highest ranked group will take precedence in the case of any duplicate assignments.</td>
</tr>
<tr>
<td>Pre-Approved Devices</td>
<td>Manage a pre-approved device list to restrict which devices are allowed to enroll by specific properties such as phone number or IMEI.</td>
</tr>
<tr>
<td>User Properties</td>
<td>Customize portal user properties.</td>
</tr>
<tr>
<td>User Search Columns</td>
<td>Customize the displayed user search result columns.</td>
</tr>
</tbody>
</table>
Unified Endpoint Management (UEM)

Account Settings

Account Options

- Global account settings.
Android For Work

- Link your Google for Work account to deploy and configure Android For Work.

Choose EMM Managed to set up Android For work when you do not have a managed Google Domain.
Application Ranking
- Rank applications to specify an installation order.
Apple Push Certificate

- Configure an Apple Push Certificate to allow Apple device enrollment

The Apple Push Certificate is used to communicate securely to the iOS devices. The process to obtain the certificate has been automated in the portal to make it as simple as possible for the administrator. Please follow the 3 simple steps to obtain and install the Apple push certificate.

1. From the Quick Start menu choose **Apple Push Certificate** and then select configure.

2. Click on the **Download CSR** button. The Certificate Signing Request (CSR) page will now display. After filling out the form, press the **Download CSR** button to save the CSR file to your local machine.

3. After the signed CSR is downloaded, click the link in the next step (2) and sign into the Apple website with any Apple ID.

4. After logging into the Apple website, click the **Create a Certificate** Button.

5. After accepting terms, you will be brought to a page where you can upload the CSR created in Step 1. Click the **Browse** button to locate the CSR and upload to the Apple
site. Follow the prompts to download the new certificate from Apple and save to your local machine.

6. The final step is to upload the certificate from Step 5 to the Unified Endpoint Management portal. Click the Browse button to locate the certificate downloaded in Step 5, then click Upload Certificate to install the certificate to the portal.

7. After the certificate is successfully installed, the Apple Push Certificates page will state that the Apple Push Certificate was uploaded and will indicate the date it will remain active until.

Bulk Import
- Bulk import users, devices, settings and more

Bulk Import History

There are no items available.

Bulk Import

Use this page to bulk load data from a tab delimited text file. The input file must be in the same format as the listed samples.

Import Type
- Bulk Import Users

Select a file to import

Sample Files
- Download a sample User Bulk Import file
- View available countries and ISO-3 codes

Upload and Import  Cancel
Certificates
Configure certificates which can be used in Wi-Fi, VPN and Exchange configurations.

**All Certificates**
Upload certificates which can be used for authentication in Wi-Fi, VPN Gateway and Exchange Mail settings.

There are no items available.

**Add Certificate**
Upload certificates which can be used for authentication in Wi-Fi, VPN Gateway and Exchange Mail settings.

- Type
- Select File
- Certificate Password

Provision

Browse...

Create  Cancel
Device Search Columns

- Customize the displayed device search result columns.

Device Search Result Columns

Use this list to control which Device Property values are shown in the device search result list. Drag an item to re-order.

Add Search Result Display Column +

- Display Name
- Phone Number
- Platform
- User ID
- Last Check-In
- Device Status
Domains

- Configure domains for portal user accounts.

Users can self-register by entering an email address from an approved domain from the portal logon screen. The portal will send the user an email with a secure link to register the user, and download the client software. Follow these steps to setup the approved email domains.

1. From the portal, choose **Administration > Domains**.

2. Choose **User Self-Registration Email Domain** from the drop-down list, enter the email domain suffix, and click Save.
Google Cloud Messaging

- Configure Google Cloud Messaging to enable over-the-air Android device administration.

Each customer in the Mobile Workforce portal must create a Google API Project and enable Google Cloud Messaging (GCM) for the project. An existing Google API Project may also be used. This process will generate a Project ID and an API Key which must be entered into the portal.

1. From the portal, choose Provisioning > Google Cloud Messaging to display the following page. Click the link under Step 1 to follow the instructions from Google to create the API Project.

2. After creating your Project ID and API Key, enter them in the form shown above and click Save. Your company is now enabled for Google Cloud Messaging.
Group Ranking

- Rank groups to specify a priority order. The highest ranked group will take precedence in the case of any duplicate assignments.

**Group Ranking**

Click and drag Groups to change their ranking. Group rankings will be used to determine which policies will be applied to devices in the case where policies are assigned to multiple groups.

<table>
<thead>
<tr>
<th>GROUP NAME</th>
<th>ACTIVE USERS</th>
<th>DEVICES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrators</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Craig Test</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Standard</td>
<td>2</td>
<td>8/167</td>
</tr>
<tr>
<td>All Devices &amp; Users</td>
<td>2</td>
<td>8/167</td>
</tr>
</tbody>
</table>

**Create Group**

GROUP NAME

- [ ] ADD NEW USERS TO GROUP
- [ ] ADD NEW DEVICES TO GROUP

ADD EXISTING DEVICES (OPTIONAL)

Add existing devices to the new group by MDN. After the group is created, memberships can be managed from the Devices tab.

MDN
Pre-Approved Devices

- Manage a pre-approved device list to restrict which devices are allowed to enroll by specific properties such as phone number or IMEI.

Pre-Approved Devices

Use this feature to create and manage an approved device whitelist. Add allowed device property values to restrict enrollment in conjunction with the Approved Devices feature. These values can also be imported via a Bulk Import.

Add a Pre-Approved Device

Device Property

ESN

Allowed Value

Ownership Type

Any

User ID

Default Group Membership

-- None --
User Properties

- Customize portal user properties.

### All User Properties

<table>
<thead>
<tr>
<th>Label</th>
<th>Enabled</th>
<th>Visible</th>
<th>Required Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Last Name</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Add a User Property

- Label
- Property ID
- Control Type: Textbox
- Regular Expression
- Invalid Submission Message
- Maximum Input Length
- Required Field: No
- Visible: Yes
- Display Name: No
- List Item Set

[Create] [Cancel]
User Search Columns

- Customize the displayed user search result columns.

User Search Result Columns

Use this list to control which User Property values are shown in the user search result list. Drag an item to re-order.

There are no items assigned. Defaults will be used.
Unified Endpoint Management (UEM)

Apple DEP

Settings
- Configure a token to manage Apple Device Enrollment Program devices.

Configuration Profiles
- Manage profiles to control Apple Device Enrollment Program device setup options.

Please upload a valid Apple DEP Token prior to managing profiles.
Unified Endpoint Management (UEM)

Devices

- View and manage Apple Device Enrollment Program devices.

Apple Device Enrollment Program Devices

List Devices that are DEP enabled. To assign a different DEP Profile, hover over an item and press the assign button to the right.

Apple VPP

Settings

- Configure settings to deploy and manage Apple Volume Purchase Plan application licenses.
Purchased Apps

- View purchased Apple VPP application licenses and usage.

Apple VPP Managed Distribution

Please upload a valid Apple VPP Token prior to managing assets.

Servers

IMAP Servers

- Configure IMAP servers which can be used for portal authentication.

All IMAP Servers

There are no items available.
SCEP Servers

- Configure SCEP servers which can be used to deploy device certificates in Wi-Fi, VPN and Exchange configurations.
Android Devices - Quick Start Guide

Introduction
This section describes how to enroll in Verizon MDM with an Android device. Your company’s Verizon MDM administrator will let you know when your account is available for enrollment.

Open the Play Store
Tap on the Play Store icon, enter your Google account, search for and install Verizon MDM

Figure 1 Play Store
Unified Endpoint Management (UEM)

Figure 2 Google Account ID

Figure 3 Google ID Password
Unified Endpoint Management (UEM)

Figure 4 Accept Terms

Figure 5 Google auto-backup (optional)
Figure 6 Search and Choose Verizon MDM

Figure 7 Install from Google Play
**Figure 8** Verizon MDM App Installed

Launch Verizon MDM
Accept all app permissions

**Figure 9** Allow Access to Location
Unified Endpoint Management (UEM)

Figure 10 Allow Dialing

Figure 11 Allow File Access
Login to Verizon MDM app

Figure 12 Enter Credentials
Accept Phone Administrator and/or Samsung KNOX Security

**Figure 13 Allow Phone Administrator**

**Figure 14 Allow KNOX Security**
Verizon MDM App Completes Registration

![Figure 15 Verizon MDM Completes Registration](image)

Verizon MDM App Completes Registration

![Figure 16 Status Tab - Policies Complete](image)
Figure 17 Connect Tab - Session Summary

Figure 18 App Tab - Required or Optional apps, if any provided by you administrator
Unified Endpoint Management (UEM)

Figure 19 Settings Tab - Basic settings and tap to update

Figure 20 Verizon MDM Shortcut
iOS Devices - Quick Start Guide

Introduction
This section describes how to enroll in Verizon MDM with an iOS device. Your company’s Verizon MDM administrator will let you know when your account is available for enrollment.

Open the App Store
Tap on the App Store icon, enter your Apple account, search for and install Verizon MDM
Unified Endpoint Management (UEM)

Figure 22 Install Verizon MDM app
Launch Verizon MDM
Accept all app permissions

Figure 23 Chose to Allow Location Reporting
Figure 24 Choose to Allow Sending Notifications
Login to Verizon MDM app

Figure 25 Enter Verizon MDM Portal Credentials
Figure 26 Processing Installation
Unified Endpoint Management (UEM)

Continue to MDM Enrollment

**Figure 27 Continue to MDM Enrollment**

![Continue to MDM Enrollment](image)

**Verizon MDM**
Your device must complete MDM registration, clicking Continue will segue out of the app. Please follow the prompts to install MDM. Then return to this app.

Continue

**Figure 28 Allow Verizon MDM to Open Settings (Requirement for iOS 10)**

![Allow Verizon MDM to Open Settings](image)

This website is trying to open Settings to show you a configuration profile. Do you want to allow this?

Ignore  Allow
Figure 29 Install MDM Profile
Figure 30 MDM Enrollment Continues
Figure 31 Complete MDM Profile Installation

Installing this profile will allow the administrator at "https://verizonmdm.vzw.com/emm/mdm/apple/checkin" to remotely manage your iPad.

The administrator may collect personal data, add/remove accounts and restrictions, list, install, and manage apps, and remotely erase data on your iPad.
Figure 32 Allow Remote Management via ‘Trust’
Figure 33 Dismiss Profile Installation Dialog
Verizon MDM Installed

Figure 34 Verizon MDM Installed