



User Guide

MCMS[®] - Mobile Device Management



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.



Table of Contents

Introduction	7
Tab and Menu Navigation	7
Breadcrumbs	7
Policy Self Service and Rules Enforcement	7
Administrator Management	7
My Profile	7
Contextual Help	8
Forgotten Password	8
localization.....	8
The MCMS Interface.....	9
Additional Navigation	9
My Profile.....	9
Logout.....	9
Help and Print.....	9
Site Map.....	9
The Home Page.....	9
Reports.....	9
MCMS Application Maintenance Page	11
Role Management and Role-Based Access Control	11
Roles mapping	12
Create Portal Administrator	12
Manage Administrators.....	12
Delete Administrator.....	13
Search for Deleted Administrator accounts	13
Reset User Password.....	13
Reactivate Locked Administrator Accounts	14
MCMS Online Registration.....	15
Step 1: Configure Services	15
Configuring Mobile Device Management for Apple iOS Devices	15
Steps in creating an APNs Certificate	16
System requirements for generating and uploading APNS certificate in MCMS	16
Step 1: Create and Enter Apple ID Credentials.....	16
Step 2: Create Certificate Signing Request (CSR) file.....	16
Step 3: Create Certificate with Apple	17
Step 4: Upload and Generate APNs file.....	17



- Configuring Mobile Device Management for Android..... 17
 - Step 2: Install and Configure Cloud Extender 18
- Installing Visibility Service 18
 - Configuring MCMS Cloud Extender for BlackBerry Enterprise Server 19
 - Configuring MCMS Cloud Extender for Microsoft Exchange ActiveSync 20
 - Installing and Configuring the MCMS Cloud Extender for Lotus Traveler 21
- Visibility Service 23
 - Step 3: Configure Device Enrollment Settings 24
 - Step 4: Enroll a Mobile Device..... 24
- Passcode Authentication 24
- Active Directory Authentication 25
 - Step 5: Configure Mobile Device Policies..... 25
 - iOS policy parameters..... 27
 - Android Policy Parameters 37
 - Exchange ActiveSync (EAS) Policy Parameters 43
 - Manage Policy Files 45
- Reporting 47
 - Mobile Devices Report 47
 - Mobile Device Overview 47
- Device Summary..... 47
- Device Ownership..... 47
- Hardware Details 47
- Network Information 48
 - BlackBerry Reporting..... 49
 - BlackBerry Hardware Overview..... 49
- Device Summary..... 49
- Hardware..... 49
- BlackBerry Policy 49
- Network Information 49
 - BlackBerry Software Overview 49
- Installed Software 49
- Software Details..... 50
 - iOS Device Reports 51
 - iOS Hardware Overview..... 51
- Hardware Details 51
- Network Information 51
 - iOS Software Overview 51
- Installed Software 51



- Software Details.....51
 - Android Device Reports52
 - Android Hardware Overview.....52
- Hardware Details52
- Network Information52
 - Android Software Overview52
- Installed Software52
- Software Details.....52
 - All Devices Reporting53
 - All Devices Inventory Overview53
- Device Summary.....53
- Device Details53
 - All Devices Security Overview53
- All Devices Summary53
- Mobile Device Security Details53
 - Partner Reports54
- Partner Overview54
- Customer Details.....54
- Device Details54
 - My Watch List.....55
 - The Manage Tab.....57
 - Device Management57
- Viewing Android Device Details58
- View iOS Device Details59
- Device Summary.....59
- Perform Mobile Device Actions60
- Viewing BlackBerry Device Details61
- Viewing Details of Devices Registered on the BlackBerry Enterprise Server62
- Viewing Details of Devices Registered on the Exchange ActiveSync Server62
- Viewing Details of Devices Registered on the Lotus Traveler Server63
 - Smart Search.....64
 - Device Groups65
 - Bulk Update (Device Attributes)67
 - Bulk Update Transaction Log.....67
 - Manage Custom Attributes68
 - Manage compliance rule sets.....68
 - Compliance Status Overview.....71
 - Apps for Mobile Distribution72



Manage Apps	72
Apple Store – Volume Purchasing Program	75
Manage App Distributions	76
Distribute Applications	76
Documents for Mobile Devices	77
Manage Documents	77
Distribute Document	78
Manage Document Distributions	79
Manage sharepoint settings.....	80
Mobile Expense Management	80



Introduction

MCMS Mobile Device Management is a cloud-based multi-tenant platform that helps to monitor and manage your smart phones, tablets, and other mobile devices. MCMS is a comprehensive mobile device management solution that supports a variety of mobile device platforms including Apple iOS, Android, BlackBerry, Microsoft Windows and others. Ease of use, security and centralized management are some of the key features of MCMS.

The MCMS system allows you to perform portal administration functions, device management, software distributions, policy self-service and device compliance functions. The MCMS real-time reports include rich intuitive, real-time and interactive graphical reports. Monitor and manage all your tablets, handheld devices, smart phones and mobile devices from a Web-based central system.

TAB AND MENU NAVIGATION

The MCMS user interface provides an easy-to-use tab and menu navigation layout, allowing quicker access to the available applications.

- **Tabs correspond to a related set of applications or tasks available to the portal user.**
- **The menus show the individual workflows, reports, etc. for the portal user. To access the menus, move your mouse-pointer over the tab and the menu will appear. The user only needs to click once to access the item.**

The enhanced User Interface design features layout and color schemes that make it easier to access and read the data presented in the MCMS UI, especially extensive reports. Other features include:

- **Buttons and breadcrumbs that allow you to perform backward navigation.**
- **Consolidated filters to improve the presentation of report results.**
- **Tabs display the suite of related applications available to portal users. The darker color indicates which tab is currently active.**

BREADCRUMBS

Breadcrumbs display your current location in an individual workflow. Navigate to any previous location by clicking on a link in the breadcrumbs.

POLICY SELF SERVICE AND RULES ENFORCEMENT

MCMS MDM solution provides a number of policy self-service and rules management capabilities for managing various Fiberlink mobile device management solutions.

ADMINISTRATOR MANAGEMENT

You can use this workflow to manage your portal administrators. Functionality includes adding an administrator and editing administrator role associations.

MY PROFILE

MCMS provides profile management capabilities through the My Profile workflow. End users can change their passwords and manage the list of their favorite pages.



CONTEXTUAL HELP

MCMS allows you access to extensive help documentation and interactive tutorials. In MCMS click the **Help** icon to view help documentation associated with current page.

FORGOTTEN PASSWORD

MCMS allows you to reset your forgotten MCMS password. To reset your password, click the **Forgot your Password?** link on the MCMS Login screen.

1. Enter your user name in the **Username** box.
2. Enter the displayed Captcha code in the **Enter the Code** box. If you wish to see a new code, then click the **Try a new code** link.
3. Click **Next >>**. The following confirmation message displays.
4. An password reset hyperlink will be sent to your registered email address. Click the hyperlink on the **Reset Portal Administrator Password** screen, if you wish to receive resent the password reset email.
5. Open the **MCMS: Portal Administrator Password Reset** email and click on the hyperlink to view the **Reset Portal Administrator Password** screen.
6. Enter the desired password in **New Password** box. Re-enter the password in the **Confirm Password** box. Ensure your new password conforms with the password rules on the **Reset Portal Administrator Password** screen.
7. Click **Submit**. A confirm message displays. You will receive a **Password Change Confirmation** email in your registered email inbox.

LOCALIZATION

You can choose to view the MCMS portal in different languages. Currently, the MCMS User Interface is available in English and Deutsch languages only.

If you wish to view the MCMS portal in your preferred language, then click on the language tab displayed on the top-right side of the MCMS login screen and click on the language of your choice.

Click on the desired language hyperlink text to view the localized screens. Enter correct credentials and click **Log In**.

After logging in to MaS360, if you wish to change the display language, then select the language tab displayed next to the **My Profile** tab.

Note: there may be a few sections on MCMS portal that still display in the English language



The MCMS Interface

The menu driven navigation used in MCMS ensures an enhanced user experience.

Note: *Some of the features are only available to customers who have purchased them individually from Fiberlink. For more information, contact your Account Manager.*

When you log in to MCMS for the first time and if you wish to manage your iOS, ActiveSync and Android devices, then you must complete the following steps listed in the **Getting Started with MCMS** section.

- Configure Services
- Install and Configure Cloud Extender
- Configure Device Enrollment Settings
- Enroll a mobile device
- Configure Device Policies

On the MCMS Website, click on the **Learn More** link to view the associated help for each step

ADDITIONAL NAVIGATION

Additional navigation provides access to **My Profile**, **English**, **Logout** and the **Search Devices box**, **Help**, and **Print** icons. Clicking the **drop-down** arrow displays the available Device Groups.

MY PROFILE

My Profile lets you view and edit your profile details and change your portal password. Refer to the *Profile Management* section for details.

LOGOUT

Logout lets you exit from MCMS.

HELP AND PRINT

Click the **Help** icon to view help documentation associated with the current page.

Click the **Print** icon to send the displayed page to an installed printer or to obtain a printout of the displayed screen.

SITE MAP

Click the [Site Map](#) link, at the bottom of the MCMS screen, to view all workflows available to you.

THE HOME PAGE

The **Home** page is the first page you see after you log in. The screen features simple navigation and displays a customizable management dashboard depending on your company policies. If you see some feature that is not available to you, you may wish to consult a Fiberlink representative for more information.

REPORTS

MCMS reporting system allows you to use enhanced reporting features and easy navigation between the reports. The enhanced reporting solution also includes filters, which help you generate a variety of real-time reports or narrow down report details based on your filter criteria.





MCMS APPLICATION MAINTENANCE PAGE

During MCMS upgrades and system enhancements, the Fiberlink Administrator can choose to display a maintenance page only for those applications that are being deployed or upgraded.

During the maintenance period, the Administrator can access the other MCMS workflows. However, when there are enhancements or upgrades to the MCMS Login, MCMS Home page, the Registration Portal and the Web fortress applications, a general MCMS maintenance page displays and the other MCMS applications may not be accessible.

ROLE MANAGEMENT AND ROLE-BASED ACCESS CONTROL

Every MCMS user must be associated with one or more roles. A role can be created by selecting one or more access control rights, as described in the following sections. Roles are used to achieve access control for various portal applications and workflows for portal users. When an administrator logs in to MCMS, by clicking the [Site Map](#) link they can view the workflows for which they have access control rights. An administrator account can be created with a role equal to or lesser than that of the administrator logged into the MCMS System, who created the account. Roles-based access control allows the administrator to determine the access rights provided to user categories.

Customer administrators can create and edit new roles, based on their organizational needs with respect to user access rights. Fiberlink provides five basic roles that can be directly assigned, or can be used as models for new roles. You can create and manage roles using the **Portal Administrator Management** workflows on the **Manage** tab. The Portal Administrator Management section includes the **Create Portal Administrator**, **Manage Portal Administrator** and the **Search for Deleted Administrators** workflows.

The **Manage > Create Portal Administrator** menu allows you to create Portal Administrator accounts. The MCMS application provides standard roles as described below.

- **Read-Only: the Read-Only role provides view-only access to all devices, policies, and applications. The Read-Only role also allows the administrator to view reports, My Watch List, devices, policies, and the Action History report in the MCMS System.**
- **Help Desk: the Help Desk role provides the administrator with access rights to perform Help Desk device management actions that include locating an end-user device, sending messages or alerts to the end-user device, lock a device, or reset device passcode. The Help Desk role also allows the administrator to view My Watch List alerts, view policies and reports, manage device enrollments, edit device views, perform remote control and help desk actions.**
- **Administrator: In addition to the access rights of the Read-Only role, the Administrator role provides access rights to perform device management actions on end-user devices. The Administrator role allows you to view My Watch List alerts, view reports and policies and also manage device enrollments, edit device view, perform policy actions, perform remote control, wipe data on a mobile device, send messages to end-user devices and perform device deactivation actions.**
- **Administrator Level 2: the Administrator Level 2 role provides the Administrator with complete device management access rights that include the ability to create and manage policies and applications, The Administrator Level 2 role also allows you to view reports, and My Watch List alerts, manage device enrollments, perform device view bulk updates, define custom attributes, manage MCMS Cloud Extenders, perform group level actions, and view and publish policies in MCMS system.**
- **MCMS Service Administrator: the MCMS Service Administrator role provides the administrator with Master Administrator level access rights that include the ability to configure services and manage administrator accounts. The MCMS Service Administrator role also allows the administrator to view reports and My Watch List alerts, manage device**



enrollments, perform device view bulk updates, define Custom Attributes, manage MCMS Cloud Extenders, perform group level actions, publish policies, and Configure Services.

ROLES MAPPING

The following chart lists the access rights associated with the standard MCMS Roles.

Create Portal Administrator

Customer administrators can create new portal administrators and assign one or more roles.

To create a new portal administrator:

8. Select the **Manage > Create Portal Administrators** menu to view the **Administrator Details** screen.
 9. Enter the user name in the **User Name** field. Make sure the **User Name** has a minimum of six characters.
 10. Enter a valid email address in the **Email Address** field. The password for this user will be automatically generated and sent to this email address.
 11. Click **Next** to view the **Assign Roles** screen.
 12. Click to select one or more roles to assign to the new user. When you click to select a role, the role description appears in the **Role Description** field.
- Note:** A MCMS Portal Administrator can create Administrator accounts only with equal or lesser access rights. For example: Administrator who is assigned the Help Desk role can only create Help Desk accounts, but will be unable to create an account with more access rights such as the Administrator.
13. Click the arrow buttons to move selected options or all options between the fields.
 14. Click **Next** to view the **Review Details** screen.
 15. Review the selected information and click **Save** to save the changes. A message confirms successful creation of **the Administrator** account.

Manage Administrators

Customer administrators can view, edit, or delete a portal administrator's role assignments.

To edit portal administrator role assignments:

16. Select the **Manage > Manage Portal Administrators** menu to view the Search Administrator screen.
17. Enter or select desired search criteria in the **User Name** box, the **Email Address** box, **Role** drop-down list and the **User Administration Group** drop-down list, if required.
18. Click **Search** to view results matching the entered search criteria.
19. Click the **Edit** icon associated with the user to view the **Edit Administrator** screen.
20. Click the arrow buttons to move selected roles or all roles between the fields, as necessary.



21. Click **Save** to save your changes and view the confirmation message.

Delete Administrator

To delete a portal administrator:

22. Select the **Manage > Manage Portal Administrators** menu to view the **Search Administrator** screen.
23. Enter or select desired search criteria in the **User Name** box, the **Email Address** box, **Role** drop-down list and the **User Administration Group** drop-down list, if required.
24. Click **Search** to view results matching the entered search criteria.
25. Click the **Delete** icon to delete the selected portal administrator accounts. A deletion confirmation message displays.
26. Click **Yes** to confirm delete.

Search for Deleted Administrator accounts

As part of the User Management Audit feature, the new **Search for Deleted Administrators** menu item allows you to search and view a list of all deleted portal administrator accounts and the associated audit details.

To view deleted administrator accounts:

27. Click the **Manage > Search for Deleted Administrators** menu to view the **Search Criteria** screen.
28. Enter or select desired search criteria in the **User Name** box, the **Email Address** box and the **Deletion Date** boxes, if required.
29. Click **Search**. Results matching the search criteria display.
30. Click the **Audit History** icon to view the **View Changes History** screen.
31. If required, click the **View Change** link to view the **View Changes** screen.

Note: The changes highlighted in yellow indicate an updated or modified field value; the green text indicates a new value and text with a red strike-through indicate that the value was deleted.

Reset User Password

Customer administrators can use the **Manage Portal Administrators** workflow to reset a user password. You may choose to reset a password when a user has forgotten his password or if a new portal user has requested you to reset and resend password.

To reset a portal administrator password:

32. Select the **Manage > Manage Portal Administrators** menu to view the **Search Administrator** screen.
33. Enter or select desired search criteria in the **User Name** box, the **Email Address** box, **Role** drop-down list and the **User Administration Group** drop-down list, if required.
34. Click **Search**. Results matching the search criteria display.



35. Click the **Reset** icon to reset the selected portal administrator password. The **Reset Password Confirmation** message displays.
36. Click **Confirm** to reset the selected portal administrator's password. A confirmation message displays. The new password will be sent to the portal administrator's email ID.

Reactivate Locked Administrator Accounts

Due to enhanced security features in MCMS, if a user belonging to the MAS Authentication domain enters an incorrect password five times consecutively, then the user account will be locked. If a user account is locked, it can be reactivated through the **Manage Portal Administrators** workflow.

To reactivate a locked administrator account:

37. Select the **Manage > Manage Portal Administrators** menu to view the **Search Portal User** screen.
38. Enter the desired search criteria.
39. Click **Search** to view the results matching the entered criteria.
40. Click the **Reactivate** icon to reactivate the locked user account. The **Reset Password Confirmation** screen displays.
41. Click **Confirm** to reactivate the locked user account. The **Password Reset** screen displays a confirmation message.
42. The user account is reactivated and a new system-generated password is sent to the administrator's email address.



MCMS Online Registration

You can register for a 30 day trial of the MCMS Mobile Device Management solution via the MCMS website at <http://www.MCMS>. The following screen displays.

Clicking on the Start Your Trial link displays the **Mobile Device Management in the Cloud** screen.

In the **Start Your Trial** section, enter appropriate information in the **Email, Password, Confirm Password, Company, First Name, Last Name,** and **Phone** fields. You must select the **I have read and accept the terms of the agreement** checkbox to continue. Click **Start Your Trial** to complete the registration process. The MCMS Home page displays.

You will receive a welcome email containing the Getting Started information, Login URL, User Name, Checklist Information, Account Name, Account Number, Support and Contact details, as shown below.

When you log in to MCMS for the first time and if you wish to manage your iOS, ActiveSync, Android, and other mobile devices, then you must complete the following steps listed in the **Getting Started Checklist** section.

- Step 1 - Configure Services
- Step 2 – Install and Configure Cloud Extender
- Step 3 - Configure Device Enrollment Settings
- Step 4 - Enroll a mobile device
- Step 5 - Configure Device Policies

The additional step of **Installing and Configuring the Cloud Extender** appears when you wish to perform secure enterprise system integration of your email, calendar, and contacts platforms including BlackBerry Enterprise Server, Microsoft Exchange Server, Lotus Notes, Active Directory or Microsoft's Office 365 with the MCMS System.

STEP 1: CONFIGURE SERVICES

On the MCMS Home page, click the **Step 1: Configure Services** link to view the **Configure Services** screen allows you to configure mobile device management settings for Apple iOS, Android devices, BlackBerry devices that connect to a BlackBerry Server, mobile devices that connect to the Corporate Exchange Server using the ActiveSync protocol, and devices that connect to the corporate Lotus Domino Server using ActiveSync protocol or the Traveler client.

Alternatively, click **Manage > Configure Services** menu to configure one or more Services on the **Configure Services** screen.

Configuring Mobile Device Management for Apple iOS Devices

In order to set up MCMS for Mobile Device to work effectively with iOS devices, you need an Apple MDM Certificate also known as the Apple Push Notification service (APNs) certificate. An Apple Push Notification service (APNs) is an MDM certificate provided by Apple to allow MCMS for Mobile Devices (MCMS MDM) to securely communicate and monitor Apple iOS devices Over The Air (OTA). MCMS uses the APNs certificate to identify and send notifications to registered iOS devices. No data is sent through the APNs service, only the notification. Fiberlink link does not provide the APNs certificate.



The section below describes the process of generating and uploading the Apple MDM Certificate.

Steps in creating an APNs Certificate

In MCMS, you can generate an APNs certificate using the following four steps:

Step 1: Create and enter Apple ID credentials

Step 2: Create Certificate Signing Request (CSR) file

Step 3: Create Certificate with Apple using the CSR file

Step 4: Generate and Upload the APNs file

System requirements for generating and uploading APNS certificate in MCMS

- Google Chrome, Mozilla Firefox, or Apple Safari Web browser
- An Apple ID (You can create one from MCMS, if required)

Step 1: Create and Enter Apple ID Credentials

1. To generate an Apple MDM Certificate in MCMS, log into MCMS and click on the **Step 1: Configure Services** checklist item.

Note: Alternately, you can click on the **Manage > Configure Services** menu to view the Configure Services screen.

2. If you do not see the option to generate Apple MDM certificate, then contact Fiberlink to enable this feature. If the Administrator has enabled the Generate APNS feature, then you should be able to generate an Apple MDM certificate from MCMS. The **Configure Services** screen displays as follows:
3. Click on the **Generate one now** button to view the steps involved in generating and uploading an APNS certificate in MCMS.
4. On the **Configure MCMS Service** screen, **enter your Apple ID**. If you do not have an Apple ID, then click the **Create ID?** hyperlink to navigate to the Apple Website and create an Apple ID, as shown below.
5. After entering appropriate details, you must accept the **Apple Terms of Service** and **Apple Customer Privacy Policy** and then click the **Create Apple ID** button to create your Apple ID and password credentials.

Step 2: Create Certificate Signing Request (CSR) file

6. On the **Get Started** tab, enter your Apple ID in the displayed text box.

7. Click **Next**. A **Security Information** pop-up box displays.

***Note:** Ensure the Java Runtime environment and the Java browser plug-ins are installed in your operating system. If Java is not installed on the Operating System and you click Next to navigate to Step 2: Create Certificate Signing Request screen, depending on the web browser, an error message displays. Refer to the **Frequently Asked Questions** section for details.*

8. In MCMS, on the Create Certificate Signing Request tab, click **Next**. If Java and the Java browser plug-ins are installed, then a **Security Information** pop-up box displays.
9. Click **OK** to continue. The **Certificate Signing Request (CSR) file is generated**. You will receive an email with the Certificate Signing Request (CSR) in your registered email inbox.

10. Click the **download** hyperlink to save the CSR file to a file location on your local hard drive.



11. **Save the CSR file** to a desired file location. The downloaded CSR file must be authenticated and signed from Apple. In the next step, you will upload the CSR file to create an Apple Push Certificate file with the **.pem** file extension.

Step 3: Create Certificate with Apple

12. After downloading the generated CSR file to a desired location, click **Next**. The **Create Certificate with Apple** tab displays.
13. Enter your Apple ID and Password credentials.
14. Click **Sign in** to view the **Apple Push Certificates Portal** screen.
15. Click the **Create a Certificate** button. The **Apple Push Certificates Portal Terms of Use** agreement displays. Scroll down to the bottom of the screen. Select the checkbox for accepting the terms and conditions.
16. Click **Accept**. The **Create a New Push Certificate** screen displays.
17. Click **Browse** and select the CSR file that was generated earlier.
18. Click **Upload** to confirm and create the new push certificate.
19. Click **Download** to download the Apple generated **.pem** certificate.
20. Save the **.pem** file to a desired location on your local drive.
21. Click **Next** to upload the Apple Push Certificate to generate the APNs certificate.

Step 4: Upload and Generate APNs file

22. On the **Upload and Generate APNs** tab, click **Browse** to select the **.pem** file that you downloaded from the **Apple Push Certificates Portal**.
23. **Enter Certificate Password** that will be used to encrypt the APNs Certificate. This password will be required, if you use the APNs Certificate in the future.
24. Confirm password in the **Confirm Password** box.
25. Click **Upload** to upload the **.pem** file and generate the APNs certificate.

A confirmation message displays. You will receive an email with the generated APNs certificate.

Configuring Mobile Device Management for Android

By default, MCMS is configured to automatically perform on-device management of Android devices.

Click the hyperlink text if you wish to enable **Enterprise App Store for Android** devices. Enter your MCMS account password in the **Enable Enterprise App Store for Android OS** security check pop-up box. This ensures that only authorized administrators can perform this task. Click **Enable** to enable **Enterprise App Store for Android**.



STEP 2: INSTALL AND CONFIGURE CLOUD EXTENDER

If you wish to perform secure enterprise system integration of your email, calendar, and contacts platforms including BlackBerry Enterprise Server, Microsoft Exchange Server, Lotus Notes, Active Directory or Microsoft's Office 356 with MCMS, then download and install the MCMS Cloud Extender from the **Configure Services** screen.

Alternatively, if you configure Services as described in **Step 1** to enable the BlackBerry Enterprise Manager, ActiveSync Manager, or the Lotus Notes Traveler Manager, the **Download** and install Cloud Extender message displays, as shown below. Click the **Download** link to download the MCMS Cloud Extender application.

Click the **Save File** button to save the Cloud Extender application to a desired file location. Double-click on the Cloud Extender application to complete installation.

Click the associated hyperlink to receive an email containing the license key for completing the Cloud Extender installation.

On the MCMS Home page, under the **Getting Started Checklist**, if the **Step 2: Install and Configure Cloud Extender** is not completed successfully, an exclamation icon is associated with the step, as shown below.

Click the link to view the **Manage MCMS Cloud Extenders** screen. Click **Download Now** to download the Cloud Extender application.

Click **Save File** to save the file to a desired file location. Click **Send License Key** to send an email containing the Cloud Extender license key details to your registered email address, as shown below.

After downloading the MCMS Cloud Extender application and associated license key, you can proceed with the Cloud Extender installation. The MCMS Cloud Extender is an executable, and once installed will automatically launch the **MCMS Cloud Extender Configuration Tool**. This tool can also be executed manually by an administrator after installation by using the Windows Operating System shortcut **All Programs > MCMS > MCMS Cloud Extender Configuration Tool**.

Installing Visibility Service

After downloading the Cloud Extender executable, double-click on the **MCMS_Cloud_Extender.exe** file to begin the MCMS Visibility Service installation, as shown below:

Click **Next** to confirm the MCMS Visibility Service installation.

After the associated files are installed, click **Next** to view the **InstallShield Completed** screen, as shown below.

Click **Finish** to complete installation.

Supported Operating Systems

Make sure that your system meets the system requirements needed to install the MCMS Cloud Extender.

OPERATING SYSTEM	NOTES
Windows XP Professional	



	Supported and tested Requires SP3
English, Simplified Chinese, Traditional Chinese, German, Japanese, French	Windows XP Pro SP3
Windows Vista Enterprise/Business	32-bit version, SP1, SP2
Windows 7 Enterprise/Business	32-bit or 64-bit
Windows Server 2003 R2 **	(32-Bit x86)
Windows Server 2003 **	Service Pack 2
Windows Server 2008 **	

**** Server versions are recommended for the Cloud Extender Modules only.**

Hardware and Software Requirements

MCMS MDM for Lotus Traveler has the following recommended requirements:

- Processor: **Pentium III, 500MHz**
- Ram: **768 MB (1 Gigabyte recommended)**
- Available Hard Disk Space: **100 MB suggested**

CONFIGURING MCMS CLOUD EXTENDER FOR BLACKBERRY ENTERPRISE SERVER

The **Manage > Configure Services** screen allows you to configure MCMS Cloud Extender for BlackBerry Enterprise Server. The MCMS Cloud Extender application allows you to integrate your BlackBerry Email Inbox, Calendar and corporate application installations with the MCMS System.

Click the hyperlink text associated with enable BlackBerry Enterprise Server Manager checkbox. Enter your MCMS account password in the **Enable MCMS BlackBerry Enterprise Server** security check pop-up box. This ensures that only authorized administrators can perform this task. You must download and install the Cloud Extender application for integrating your Black Berry Enterprise Server Manager mailbox, calendars, and contacts with MCMS.

To configure MCMS Cloud Extender for BlackBerry Enterprise Server:

- a. From the Windows Start panel, open the MCMS Cloud Extender Configuration tool.
- b. The **Welcome to Cloud Extender Configuration Setup** screen displays. The **Do not use any proxy** option is selected as the default option. If you wish to specify the proxy settings, then select the **Manually configure proxy settings** option. Enter correct proxy Address and Port information.
- c. Click Next. The Select the Services to be Configured screen displays.



- d. Here you can to select the desired services that you wish to configure. For this example, we have selected the **User Authentication** and the **BlackBerry Enterprise Server Integration Services** options.
- e. Click **Next**. The **Service Account Setup** screen displays.
- f. This step allows you to integrate your account with your corporate Active Directory account. Click **Edit**, if you wish to update your **Username**, **Password** and **Domain** credentials. Click **Next**. The **BES Configuration** screen displays.
- g. Click **Edit**, if you wish to update the **BES Server URL**, **Authentication Type**, **Username**, **Password**, and **Domain** credentials.
- h. Click **Next**. The MCMS Auto Updates Configuration screen displays.
- i. Select the **Enable Automatic Software Updates** checkbox, if you wish to automatically download and install software updates.
- j. Click **Finish** to complete the MCMS Cloud Extender configuration for BlackBerry Enterprise Server. You are now ready to manage and monitor your BlackBerry mobile devices.

CONFIGURING MCMS CLOUD EXTENDER FOR MICROSOFT EXCHANGE ACTIVESYNC

The **Manage > Configure Services** screen allows you to configure MCMS visibility services on mobile devices to connect to your corporate Exchange Server using the ActiveSync protocol.

1. Click the hyperlink text associated with the **enable ActiveSync Manager** to view the **Enable MCMS ActiveSync Manager** pop-up box.
2. Enter your MCMS account password to ensure only authorized administrators configure the ActiveSync settings. From the Mail Servers options displayed, you must choose either **Exchange 2007** or **Exchange 2010**. Click **Enable** to enable the Microsoft ActiveSync Manager.

To configure MCMS Cloud Extender for Exchange ActiveSync Manager:

- a. From the **Windows Start** panel, open the **MCMS Cloud Extender Configuration** tool. The **Welcome to Cloud Extender Configuration Setup** screen displays. The **Do not use any proxy** option is selected as the default option. If you wish to specify the proxy settings, then select the **Manually configure proxy settings** option. Enter correct proxy Address and Port information.
- b. Click **Next**. The Select the Services to be Configured screen displays.
- c. Here you can to select the desired services that you wish to configure. For this example, we have selected the **Exchange ActiveSync Manager** and the **User Visibility** options. Selecting the **Exchange ActiveSync Manager** option displays the associated options, which includes **Exchange 2007**, **Exchange 2010**, and **Office 365**. Select the desired option. Click **Next**. The **Prerequisites Check** screen displays.
- d. The **Service Account Setup** screen displays. This step allows you to integrate your account with your corporate Active Directory account. Click **Edit**, if you wish to update your **Username**, **Password** and **Domain** credentials.

- e. Click **Next**. The **Exchange ActiveSync Integration** screen displays. Here, you can chose to enable Exchange ActiveSync Integration on multiple Cloud Extenders.
- f. The **No** option is selected as the default. If you select **Yes**, from the options box, select the desired mailbox servers that the Cloud Extender will manager. Click **Next**. The **MCMS Auto Updates Configuration** screen displays.
- g. Select the **Enable Automatic Software Updates** checkbox, if you wish to automatically download and install software updates. Click **Finish** to complete the Exchange ActiveSync Integrations with the MCMS system. You are now ready to manage and monitor your mobile devices that are integrated with the Microsoft Exchange Server.
- h. On the **Manage > Configure Services**, the MCMS ActiveSync Manager is enabled message displays.

System Requirements for the MCMS Cloud Extender for Lotus Traveler Module (MCMS for Mobile Devices)

The MCMS Cloud Extender for Lotus Traveler can run on any supported device within the customer environment and does not require any additional hardware and software requirements to run. However, in order for it to function correctly, certain system and network requirements exist.

SYSTEM REQUIREMENTS	NOTES
Traveler 8.5.1, 8.5.2.1	<p>The MCMS Cloud Extender for Traveler provides support for Traveler 8.5.1 and 8.5.2.1.</p> <p>Note: The MCMS Cloud Extender does NOT have to run on the Traveler or Domino Server, but it must run on a device with Notes installed.</p>
Connectivity to the Domino and Traveler Servers	Unrestricted network access to the Domino and Traveler servers is required.
Access to the Internet over port 443 and 80	<p>The MCMS Cloud Extender for Lotus Traveler requires outbound access to the MCMS portal on port 443.</p> <p>Note: The V Agent can accommodate proxy traversal when properly configured.</p>

INSTALLING AND CONFIGURING THE MCMS CLOUD EXTENDER FOR LOTUS TRAVELER

Launch the MCMS Cloud Extender installation package. It can be downloaded from the Getting Started Checklist on the MCMS **Home** tab. The License Key will be provided to you in an email.

As mentioned above, what is being installed is a version of the MCMS Visibility Service which provides the underlying functionality for the Cloud Extender. Once the Visibility Service is installed, the MCMS Cloud Extender Configuration Tool will be launched and will take you through the steps required to configure the Cloud Extender for your environment, and to enable the MCMS Lotus Traveler Manager capabilities. Alternatively, open the **MCMS Cloud Extender Configuration** tool via the Windows Start menu.

System Requirements for the MCMS Cloud Extender for Lotus Traveler Module (MCMS for Mobile Devices)

The MCMS Cloud Extender for Lotus Traveler can run on any supported device within the customer environment and does not require any additional hardware and software requirements to run. However, in order for it to function correctly, certain system and network requirements exist.

SYSTEM REQUIREMENTS	NOTES
Traveler 8.5.1, 8.5.2.1	<p>The MCMS Cloud Extender for Traveler provides support for Traveler 8.5.1 and 8.5.2.1.</p> <p>Note: The MCMS Cloud Extender does NOT have to run on the Traveler or Domino Server, but it must run on a device with Notes installed.</p>
Connectivity to the Domino and Traveler Servers	Unrestricted network access to the Domino and Traveler servers is required.
Access to the Internet over port 443 and 80	<p>The MCMS Cloud Extender for Lotus Traveler requires outbound access to the MCMS portal on port 443.</p> <p>Note: The V Agent can accommodate proxy traversal when properly configured.</p>
Access to the following hosts/IP addresses from the device running the MCMS Cloud Extender	<p><i>https://mpns.MCMS</i> 208.76.128.168</p> <p><i>https://services.fiberlink.com</i> 208.76.128.153 208.76.132.59 208.76.130.187</p> <p><i>http://internettest.fiberlink.com</i> 208.76.128.58 208.76.132.21 208.76.130.58</p>

Best Practices

Fiberlink recommends the following for the installation and running of the MCMS Cloud Extender for Lotus Traveler:

1. Make sure you can access the following URLs. You can test this by entering the following URLs in your browser.
 - *https://services.fiberlink.com*
 - *http://internettest.fiberlink.com*
 - *https://mpns.MCMS*
2. Install the MCMS Cloud Extender for Lotus Traveler on a machine which is on all the time, e.g., a VM machine in your Domino domain.
3. Lotus Notes must be installed prior to the installation of the MCMS Cloud Extender for Lotus Traveler.
4. The Lotus Notes client must have accessed or logged into the Domino server once.
5. Lotus Notes cannot be running during the installation process.



6. The Lotus Notes ID file which is used for configuring the MCMS Cloud Extender for Lotus Traveler must have the following access:
 - Server Remote Admin, Manager with delete access to Traveler.nsf
7. The Lotus Notes client should not be run after the installation.

Visibility Service

The following screens are representative of what you will see as you step through the Visibility Service installation.

3. Click **Next** to advance to the License Key screen.
4. Enter the license key provided to you in the Welcome email.
5. Click **Next** to advance to the Ready to Install the Program screen.
6. Click **Install** to continue the installation.
7. Click **Next** to continue the installation.
8. When prompted, click **Finish**. The MCMS Cloud Extender Configuration Tool will now launch.

To configure MCMS Cloud Extender for Exchange ActiveSync Manager:

- a. From the Windows Start panel, open the MCMS Cloud Extender Configuration tool. The Welcome to Cloud Extender Configuration Setup screen displays.
- b. The **Do not use any proxy** option is selected as the default option. If you wish to specify the proxy settings, then select the **Manually configure proxy settings** option. Enter correct proxy Address and Port information. Click **Next**. The **Select the Services to be Configured** screen displays.
- c. Here, you can to select the desired services that you wish to configure. For this example, we have selected the **Lotus Traveler Manager** option. Click **Next** to view the **Lotus Traveler Configuration** screen. Click **Edit**, if you wish to update the **Domino Hierarchical Server Name(s)**, **Notes ID Path**, **Password**, **Notes Directory**, and **Notes File Path** credentials.
- d. Click **Next**. The **MCMS Auto Updates Configuration** screen displays.
- e. Select the **Enable Automatic Software Updates** checkbox, if you wish to automatically download and install software updates. Click **Finish** to complete the MCMS Cloud Extender configuration. You are now ready to manage and monitor your mobile devices that are integrated with Lotus Traveler. Clicking the **Manage > Configure Services** menu displays the following screen.



STEP 3: CONFIGURE DEVICE ENROLLMENT SETTINGS

After successfully configuring the desired MCMS services, you must configure the device enrollment settings. On the MCMS Home page, click the **Step 3: Configure Device Enrollment Settings** link to view the **Configure Device Enrollment Settings** screen, which allows you to configure the mobile device enrollment settings.

To configure device enrollment settings in MCMS:

- a. Select **Manage > Configure Device Enrollment Settings** menu item to view the **Configure Device Enrollment Settings** screen.
- b. Enter a suitable name in the Corporate Identifier to be used in your Enrollment box.
 1. From the **Select user authentication mode** for device enrollment section, you can choose to Authenticate using a unique passcode sent to user on your request, Authenticate against the Corporate Active Directory, or the Two-factor Authentication options.
 2. If you choose to perform user authentication using your **Corporate Active Directory**, then you must enter the default domain for user's details. Refer to **Installing and Configuring MCMS Cloud Extender installation guide** for details on how to configure MCMS Cloud Extender for Active Directory.
 3. Select the **Prompt user to accept your corporate usage policy during device enrollment** option and **select the desired Usage Policy** file, if you wish to ensure that your users accept and conform to your corporate usage policy.
 4. **Select the Corporate Support Information** option and enter the correct **Contact Email** address and **Phone Number** information that will be displayed to your end-users.
 5. If required, select the **Alert Administrator when a new device reports to MCMS** option.
 6. Select the desired **Device Types to be considered** option.
 7. In the **Notification Email Address(es)** box, enter the email address of the Administrator that you wish to alert when a new device reports to MCMS.
- c. Click **Save** to save the configuration changes.
- d. Click **Close** if you wish to close the **Configure Device Enrollment Settings** screen and return to the MCMS Home page.

STEP 4: ENROLL A MOBILE DEVICE

After configuring your device enrollment settings, you can enroll your mobile devices in MCMS. Enrolling a device with MCMS is quick and easy.

- a. Click the **Manage > Manage Enrollment Requests** menu.
- b. The **Manage Enrollment Request** screen lists all device enrollment request, along with its status. An enrollment request can be in **New**, **Pending** or **Completed** status.
- c. Click the **Send Enrollment Request** button on the next screen.
- d. The **Add a Device** pop-up box displays.
 - The options displayed on the screen will depend on whether you have opted to use passcode or Active Directory-based authentication.

Passcode Authentication

- If you are using passcode authentication, a pop-up box will be displayed:
- e. Enter the user's **Corporate Username**, **Domain**, **Corporate Email Address** and the **Phone Number** information. Select the desired **Ownership** and **Email Notification** options. Select the **Other** option allows you to include **SMS Notification** to the

user. If required, select the desired **Policy Set**, and **Compliance Rule Set** options. Enter relevant description in the **Comments** box. It is important to note that the information entered in the above fields will also be used to pre-populate any email, Wi-Fi, or VPN profiles that require it.

- f. Click **Send Request** to view the **Enrollment Request Sent** pop-up box, which displays the **URL**, **Corporate Identifier**, and the **Passcode** information.
- g. Enter the displayed details on the mobile device or if you have installed an QR recognition software on your mobile device, then use the mobile device camera to capture the displayed QR code to complete registering the mobile device.

The user will also receive an email (and an SMS message, if you specify it), guiding them through the enrollment process. Once complete, the registration request will be marked as **Complete**. The user's device will now be listed on the **Manage > View All Devices** screen in MCMS.

Active Directory Authentication

Creating an enrollment request is similar. Enter or the select the desired details.

On clicking the **Send Request** button, you will receive the **Device Enrollment Request** email displaying the enrollment details.

This URL will work for any of your devices, and can be published in documentation or linked to for all devices. For your convenience, a QR code containing the link is displayed on this window. If you have QR code reader installed on your mobile device, capturing the QR code using your mobile device camera will automatically open the required web link.

After completing the device enrollment process, the enrolled user device will now be listed on the **Manage > View All Devices** screen.

STEP 5: CONFIGURE MOBILE DEVICE POLICIES

The **Configure Mobile Device Policies** workflow allows the administrator to configure mobile device policies. Alternatively, click the **Manage > Manage Device Policies** menu to view the **Manage Device Policies** screen, which allows you to search and list all mobile device policies.

The **Manage Device Policies** screen displays the Name, Default, Platform, Status, Publish Version, Last Modified, Last Successful Publish, and the Actions information. The **Manage Device Policies** screen also allows you to execute policy actions by selecting the desired option from the **Actions** drop-down menu.

The **Manage Devices Policies** screen includes an enhanced search feature that allows you to dynamically view all entries that contain the text criteria that you enter. The entered search criterion is highlighted in yellow.

The **Manage Device Policies** screen also includes page navigation at the bottom of the screen that allows you to navigate to a desired page.

You can customize the number of policies displayed on your screen by selecting the desired number of entries from the **Show <##> entries** drop-down list.

There may be instances when one or more devices are included in different device groups. When you perform an apply policy action or when an automated action feature is set up for those device groups, then determining the policy set that will be applied to that device may not be possible for the Administrator. In such cases, the **Change Precedence** feature allows



you to set the precedence or the priority for the policies. If a policy precedence is set to 1, it denotes that policy set would be applied to the device even when the same device belongs to different policy groups having different policy settings.

Click the **Change Precedence** button to view the **Change Precedence** dialog box, which lists the available iOS and Android MDM policies.

You can change the policy precedence by dragging a policy box to the desired precedence level. Click **Save** to save changes. Click the **Create New Policy Set** button to view the **Create Policy Set** screen.

Enter the relevant details and click **Continue** to configure the policy settings. Refer to the **Policy Parameter Descriptions** section to view policy categories, policy parameters and the associated description for iOS, Android, and Exchange ActiveSync mobile device policies.

Click **Edit** to edit the current policy settings.

Click **Save** if you wish to save changes. Click **Save And Publish** if you wish to publish the updated policy settings. Clicking on the **Actions** tabs displays the **View Recent Changes**, **View Audit History**, **Publish Policy**, **Mark Inactive** and **Mark as Default** actions.

Click the **View Recent Changes** action to view the recent updates to the policy settings.

Click the **View Audit History** action to view a list of actions that were performed for the selected policy set.

On the **Audit History** screen, you can perform the **View Details** and the **Rollback** actions.

On the **View All Policies**, click the **Publish Policy** action to publish the policy to your registered mobile devices.

The Administrator must enter the log in password to ensure only authorized individuals publish the policy settings. Enter relevant policy description and click **Continue** to publish the policy set.

If required, click the **Mark Inactive** action to deactivate the policy. A confirmation message displays.

Clicking **Yes** sets the policy set status to Inactive.

If you wish to reuse a policy set that is marked Inactive, you must reactivate the Inactive policy by selecting the **Reactivate Policy** action item.

The policy set is active. If required, click the **Mark as Default** action to set the policy as the default policy set.

If required, click the **Mark as Default** action to set the policy as the default policy set. Click **Back To Results** to return to the **View All Policies** screen,



Clicking on an MDM policy displays the associated policy categories. Clicking on a policy category tab on the left panel displays the associated policy parameters on the right. Selecting an iOS policy displays the following screen.

IOS POLICY PARAMETERS

Select the **Manage > Manage Device Policies** option to search and list all mobile device policies. Clicking on a policy name displays the relevant policy categories. Each category contains a set of related policy parameter settings, values, and their associated descriptions.

iOS Policy Parameter Descriptions

When you select an iOS policy, the following policy parameters display.

POLICY CATEGORY	POLICY PARAMETER	PARAMETER DESCRIPTIONS
Device Passcode	Configure Passcode Policy	Configure passcode policy
	Enforce Passcode on Mobile Device	Enforce passcode on mobile device
	Allow Simple Passcode	Passcode values that are ascending, descending or repeating character sequences (e.g. 1111, 123, 654, abc, xyz)
	Require Alphanumeric in Passcode (at least one letter)	Require alphanumeric in passcode (at least one letter)
	Minimum Passcode Length	Minimum passcode Length
	Required Number of Special Characters (1-4)	Required number of special characters (1-4)
	Maximum Passcode Age (1-730 days, or none)	Maximum passcode age (1-730 days, or none)
	Allowed Idle Time (in minutes) Before Auto-lock	Allowed idle time (in minutes) before auto-lock
	Number of Unique Passcodes Required Before Reuse Allowed (1-50, or blank)	Number of unique passcodes required before reuse allowed (1-50, or blank)
	Grace Period for Device Lock	



		Grace period for device lock
	Number of Failed Passcode Attempts Before All Data is Erased (4-16)	Number of failed passcode attempts before all data is erased (4-16)
Device Restrictions	Configure Device Restrictions	Configure device restrictions
	Allow Installing of Applications	When this option is off, users cannot install or update their apps using App Store or iTunes
	Allow Use of Camera	Allow use of camera
	Allow Use of FaceTime	Allow use of FaceTime
	Allow Screen Capture	Allow screen capture
	Allow Automatic Synchronization While Roaming	Allow automatic synchronization while roaming
	Allow Voice Dialing	Allow voice dialing
	Allow In-app Purchase	Allow in-app purchase
	Allow Multiplayer Gaming	Allow multiplayer gaming
	Allow adding Game Center friends	Allow adding Game Center friends
	Enforce Encrypted Device Backups on the Computer	Enforce encrypted device backups on the computer
	Enforce iTunes Password Entry	Enforce iTunes Password Entry
	Allow Untrusted TLS Prompt	Allow untrusted TLS Prompt
	Allow Use of YouTube Application	Allow use of YouTube application
	Allow Use of iTunes for Media Download	Allow use of iTunes for media download
	Allow Use of Safari	



		Allow use of Safari
	Enable Auto-fill in Safari	Enable auto fill in Safari
	Force Fraud Warning	When this option is selected, Safari attempts to prevent users from viewing Websites that are fraudulent or compromised
	Enable Java scripts on the Websites	Enable Java scripts on the websites
	Block Pop-ups on Safari	Block pop-ups on Safari
	Accept Cookies on Safari	Accept cookies on Safari
	Allow Explicit Music and Podcasts purchased from iTunes	Allow explicit music and podcasts purchased from iTunes
	Allow Cloud Back up	Allow Cloud Back up
	Allow Documents Sync	Allow Documents Sync
	Allow Cloud Key Value Sync	Allow Cloud Key Value Sync
	Allow Photo Stream Sync	Allow Photo Stream Sync
	Region for Content Ratings	Region for content ratings
	Maximum Allowed Content Rating for Movies	Maximum allowed content rating for movies
	Maximum Allowed Content Rating for TV Shows	Maximum allowed content rating for TV shows
	Maximum Allowed Content Rating for Applications	Maximum allowed content rating for applications
Application Compliance	Configure Restricted Applications (App Blacklist)	Configure restricted applications (App Blacklist)
	Application Name	



		Application name
	Application Bundle ID	Application Bundle ID
	Configure Allowed Applications (App Whitelist)	Configure allowed applications (App Whitelist)
	Application Name	Application name
	Application Bundle ID	Application Bundle ID
	Configure Required Application	Configure required application
	Application Bundle ID	Application Bundle ID
	Application Name	Application name
Email	Configure for Type	Configure for type
	Protocol for Accessing the Email Account	Protocol for accessing the email account
	Account Description	End users will see the mailbox with this name
	Path Prefix for IMAP Protocol	Path prefix for IMAP protocol
	User Display Name	User display name
	Email Address	Email address
	Mail Server Host Name (for Incoming Mail)	Mail server host name (for incoming mail)
	Mail Server Port Number (for Incoming Mail)	Mail server Port number (for incoming mail)
	Username (for incoming mail)	Username (for incoming mail)
	Authentication Type (for Incoming Mail)	Authentication type (for incoming mail)



	Use SSL (for Incoming Mail)	Use SSL (for incoming mail)
	Mail Server Hostname (for Outgoing Mail)	Mail server hostname (for outgoing mail)
	Mail Server Port number (for Outgoing Mail)	Mail server Port number (for outgoing mail)
	Username (for outgoing mail)	Username (for outgoing mail)
	Authentication Type (for Outgoing Mail)	Authentication type (for outgoing mail)
	Use SSL (for outgoing mail)	Use SSL (for outgoing mail)
	Same Password for Outgoing and Incoming Mail	Same password for outgoing and incoming mail
Exchange ActiveSync	Configure Exchange ActiveSync Settings	Configure Exchange ActiveSync settings
	Account name for the Exchange ActiveSync server	End users will see the mailbox with this name
	Hostname of the Exchange ActiveSync server	Hostname of the Exchange ActiveSync server
	Use SSL	Use SSL
	Domain Name	Domain name
	Account Username	Account Username
	Email Address	Email address
	Synchronize Emails for the Selected Date Range	Synchronize emails for the selected date range
	Identity Certificate	Identity Certificate
	Prevent Moving Mail to Other Accounts	Prevent Moving Mail to other Accounts



	Prevent Third Party Apps from Sending Mail	Prevent Third Party Apps from Sending Mail
CalDAV	Configure CalDAV profile for CalDAV Server Access	Configure CalDAV profile for CalDAV server access
	Display Name of the CalDAV Account	Display name of the CalDAV account
	Hostname of the CalDAV Account	Hostname of the CalDAV account
	Host Port Number of the CalDAV Account	Host port number of the CalDAV account
	Principal URL for the CalDAV Account	Principal URL for the CalDAV account
	CalDAV Account Username	CalDAV account username
	Use SSL to Communicate with CalDAV Servers	Use SSL to communicate with CalDAV servers
CardDAV	Configure CardDAV Profile for CardDAV Server Access	Configure CardDAV profile for CardDAV server access
	Display Name of the CardDAV Account	Display name of the CardDAV account
	Host Name of the CardDAV Account	Host name of the CardDAV account
	Host Port Number of the CardDAV Account	Host port number of the CardDAV account
	Principal URL for the CardDAV Account	Principal URL for the CardDAV account
	CardDAV Account Username	CardDAV account username
	Use SSL to Communicate with CardDAV Servers	Use SSL to communicate with CardDAV servers
Calendar Subscriptions	Configure Calendar Subscriptions to a Device's Calendar App	Configure calendar subscriptions to a device's Calendar app



	Description for the Subscribed Calendar	Description for the subscribed calendar
	URL of the Calendar File*	URL of the calendar file*
	Username for Calendar Subscription	Username for calendar subscription
	Use SSL to View Calendar Subscriptions	Use SSL to view calendar subscriptions
Web Clips	Configure Web Clips for the Device Home Screen	Configure web clips for the device Home screen
	Display Name of the Web Clip	Display name of the web clip
	URL for the Web Clip	URL for the web clip
	Allow Web Clip Removal	Allow web clip removal
	MCMS Web Clip Icon ID	Identifies the location of your certificate or icon file uploaded using the Manage Certificate & Images workflow
	Remove Visual Effects from the Web Clip Icon	Remove visual effects from the web clip icon
	Launch the Web Clip as a Full Screen Application	Launch the web clip as a full screen application
Certificate Credentials	Configure Credentials for Adding Certificates on the Device	Configure credentials for adding certificates on the device
	Credential Name	Credential name
	Credential Identifier	Defines certificate for inclusion on device
Advanced	Configure Advanced Settings	Configure advanced settings
	Name of the Access Point Carrier	Name of the access point carrier
	Access Point User Name	



		Access point user name
	Proxy Server Address	Proxy server address
	Proxy Server Port Number	Proxy server port number
Wi-Fi	Wi-Fi	Wi-Fi
	Configure for type	Configure for type
	Service set identifier (SSID)*	Identification of the wireless network to be connected
	Hidden Network	Hidden network
	Encryption Type	Encryption Type
	Proxy Type	Proxy Type
	Proxy Server Address	Proxy server address
	Proxy Server Port	Proxy server port
	Proxy Server Username	Proxy server username
	Proxy Server Password	Proxy server password
	Proxy PAC URL	Proxy PAC URL
	Password for Authenticating a Wireless Network	Password for authenticating a wireless network
	Accepted EAP types	Accepted EAP types
	Use Protected Access Credential(PAC) (for EAP-FAST)	Protected Access Credential (PAC) configuration allows optimized network authentication
	Use PAC	Use PAC



	Provision PAC	Provision PAC (Valid only if the Use PAC setting is selected)
	Provision PAC anonymously	Provision PAC anonymously (Valid only if the Provision PAC setting is selected)
	Inner Authentication Protocol (for TTLS)	Inner authentication protocol (for TTLS)
	Authentication Username	Authentication username
	Use per Connection Password	Use per connection password
	Outer Authentication Protocol (for TTLS, PEAP, EAP-FAST)	Outer Authentication Protocol (for TTLS, PEAP, EAP-FAST)
	Trusted certificates	Trusted certificates
	Trusted certificate name	Trusted certificate name
	Allow trust exceptions	Allow trust decisions (via dialog) to be made by the user
	Identity Certificate	Identity certificate
VPN	VPN	VPN
	Configure for Type	Configure for type
	VPN Connection Name	VPN connection name
	Host Name of the VPN Server	Host name of the VPN server
	VPN User Account	VPN user account
	User Authentication Type	User authentication type
	VPN On demand: Always Establish for URLs	VPN On demand: Always establish for URLs
	VPN On demand: Never establish for URLs	VPN On demand: Never establish for URLs



	VPN On demand: Establish if needed for URLs	VPN On demand: Establish if needed for URLs
	Password	Password
	Shared Secret	Shared secret
	Send All Traffic	Send all traffic
	Proxy Server Configuration Mode	Proxy server configuration mode
	Proxy Server Port	Proxy server port
	Proxy Server Username	Proxy server username
	Proxy Server Address	Proxy server address
	Proxy Server URL	Proxy server URL
	Encryption Level	Encryption level
	Machine Authentication Type	Machine authentication type
	Identity Certificate	Identity certificate
	Identity User PIN	Identity user PIN
	Cisco VPN Group name	Cisco VPN Group name
	Shared Secret	Shared secret
	Use Hybrid Authentication	Authenticate using shared secret, group name, and server side certificate
	Prompt for Device Password	Prompt for device password
	Authentication Realm	Authentication realm
		VPN user role



	VPN User Role	
	Cisco VPN Group Name	Cisco VPN group name
Roaming Settings	Configure Roaming Settings	Configure roaming settings
	Enable Data Roaming	Enable data roaming
	Enable Voice Roaming	Enable voice roaming
iPCU Import	Import Settings Created in iPCU	Import settings created in iPCU
	iPCU Settings	iPCU settings

ANDROID POLICY PARAMETERS

Select the **Manage > Manage Device Policies** option to search and list all mobile device policies. On the **Manage > Manage Device Policies** screen, selecting an Android policy displays the associated policy parameters, as shown below.

Android Policy Parameter Descriptions

On the **Manage Device Policies** screen, if you click on an Android policy, the following policy categories and the associated descriptions display.

POLICY CATEGORY	POLICY PARAMETER	PARAMETER DESCRIPTIONS
Device Passcode	Configure Passcode Policy	Configure passcode policy
	Minimum Passcode Length (4-16)	Minimum passcode length (4-16)
	Minimum Number of Complex Characters	Minimum number of complex characters
	Passcode Quality	Passcode quality
	Maximum Passcode Age (in Days)	Maximum passcode age (in Days)
	Allowed Idle time Before Auto-lock	Allowed idle time before auto-lock



	Passcode History	Passcode history
	Number of Failed Passcode Attempts Before All Data is Erased (4-16)	Number of failed passcode attempts before all data is erased (4-16)
Device Restrictions	Enable Background Data synchronization	Allows applications to sync, send or receive data any time
	Auto-Sync	Auto-sync
	Use Data Network	Use data network
	Allow Installation of Non-Market Applications	Allow installation of non-Market applications
	Data Roaming	Data roaming
	Camera	Camera
	USB	USB
	Bluetooth	Bluetooth
	Mobile AP	Mobile Access Point
	Tethering	Tethering
	Near Field Communication (NFC)	Near Field Communication (NFC)
	Use Wireless Networks for Location Detection	Use wireless networks for Location Detection
	Use GPS Satellites for Location Detection	Use GPS satellites for Location Detection
	Use Sensor Aiding for Location Detection	Use sensor aiding for Location Detection
	Allow Mock Locations	Allow mock Locations



Application Restrictions	Disallowed Application Name	Disallowed application name
	Disallowed Application ID	Identifies the location of your certificate or icon file uploaded using the Manage Certificate & Images workflow
Wi-Fi	Wi-Fi	Wi-Fi
	Wi-Fi Configuration Type	Wi-Fi configuration type
	Service Set Identifier (SSID)*	Service set identifier (SSID)*
	Non-Broadcast SSID	Non-broadcast SSID
	Encryption Key	Encryption key
	EAP Authentication Protocols	EAP authentication protocols
	Authentication Username	Use %username% for user's corporate credentials
	Authentication Domain	Use %domain% for user's corporate credentials
	Anonymous Identity	Anonymous identity
	Phase 2 Authentication Protocol	Phase 2 authentication protocol
	Authentication Password	Use %password% for user's corporate credentials
	Server URL	Server URL
	Server Port	Server Port
Device Management	Warning Message After Disabling Device Management	Warning message After Disabling Device Management



	Enforcement Action After Disabling Device Management	Enforcement action when the user disables MCMS Agent as the device administrator
	Defined Inactivity Time Limit Before Device is Out of Compliance (1-15 minutes)	The user response time out limit after which the enforcement action is applied
	Action When Out of Compliance	Action when out of compliance
	Data Collection Frequency (in Minutes)	Reducing this will increase battery usage on the device
	Device Heartbeat Frequency (in Minutes)	Reducing this will increase battery usage on the device
	Usage Data Collection Frequency (in Minutes)	Reducing this will increase battery usage on the device
	Usage Data Upload Frequency (in Minutes)	Reducing this will increase battery usage on the device
Security Settings	Enforce Device Encryption	Enforce device encryption
	Visible Passwords	Passwords entered in applications will be visible to users as they type
	Backup my data	Back up current settings and application data in Google
	Automatic Restore	Restore backed up settings and data when reinstalling an application
Application Compliance	Application Name	Application name
	Application ID	App ID for the application can be found in the Android Software Inventory Overview report.



Native App Compliance	Allow Gallery	Configuring the below settings will increase battery usage on the device.
	Allow Gmail	Allow Gmail
	Allow Email	Allow email
	Allow YouTube App	Allow YouTube App
	Allow Browser	Allow browser
	Allow Google Maps & Navigation	Allow Google maps & navigation
	Allow Android Market	Allow Android Market
VPN	Configure for Type	
	vpnConnectionName	
	hostnameVPN server	
	enableL2TPSecret	
	l2tpSecret	
	dnaSearchDomains	
Exchange ActiveSync	Configure Exchange ActiveSync Account	Configure Exchange ActiveSync account
	Prompt User to Install Exchange by Touchdown	Prompt user to install Exchange by Touchdown
	License Key	License key
	Host Name of the Exchange Server	Host name of the Exchange Server



	Use SSL	Use SSL
	Exchange Account	Exchange account
	Configure Touchdown Passcode	Configure Touchdown passcode
	Encrypt Emails	Encrypt emails
	Encrypt Attachments	Encrypt attachments
	Allow Backup of Emails and Settings	Allow backup of emails and settings
	Disable Copy of Contacts to Phone	Disable copy of contacts to phone
	Disable Copy-Paste from Email	Disable copy-paste from email
	Allow HTML Formatted Email	Allow HTML formatted email
	Maximum Email Size (KB)	Supported values: 0 to 100 or Blank. Messages exceeding the specified limit will be truncated
	Include Past Emails for Selected Date Range	Include past emails for selected date range
	Include Past Calendar Items for Selected Date Range	Include past calendar items for selected date range
	Allow Attachments	Allow attachments
	Maximum Attachment Size (KB)	Maximum attachment size (KB)
	Email Signature	Email signature
	Allow User to change Email Signature	Allow user to change email signature
	Manual Sync when Roaming	Manual sync when roaming



	Enable Touchdown Widgets	Enable Touchdown widgets
--	--------------------------	--------------------------

EXCHANGE ACTIVESYNC (EAS) POLICY PARAMETERS

Clicking the **Manage > Manage Device Policies** screen displays the View All Policies screen.

Clicking on an Exchange ActiveSync policy displays the following screen.

Exchange ActiveSync Policy Parameter Descriptions

An Exchange ActiveSync policy includes the following policy parameters.

POLICY CATEGORY	POLICY PARAMETER	PARAMETER DESCRIPTIONS
Device Passcode	Require password	Enforce passcode policy on mobile device
	Minimum Passcode Length (4-16)	Minimum passcode length (4-16)
	Allow Simple Passcode	Passcode values that are ascending, descending or repeating character sequences (E.g. 1111, 123, 654, abc, xyz)
	Require Alphanumeric in Passcode (at least one letter)	Require alphanumeric in passcode (at least one letter)
	Required Number of Complex Characters (1-4)	Required number of complex characters (1-4)
	Allowed Failed Attempts (4 to 16)	Allowed failed attempts (4 to 16)
	Number of Unique Passcodes Required Before Reuse Allowed (1-50)	Number of unique passcodes required before reuse allowed (1-50)
	Allowed Idle Time Before Auto-lock (1-60 Minutes)	Allowed idle time before auto-lock (1-60 minutes)
	Maximum Passcode Age (1-730 days, or Blank)	Maximum passcode age (1-730 days, or blank)



	Enable Passcode Recovery for Device Unlock	Enable passcode recovery for device unlock
Sync Configurations	Mobile Device Policy Refresh Interval (hours)	Mobile device policy refresh interval (hours)
	Include Past Calendar Items for Selected Date Range	Include past calendar items for selected date range
	Include Past Emails for Selected Date Range	Include past emails for selected date range
	Email Size Limit (KB)	Messages exceeding the maximum email size will truncate
	Enforce Manual Synchronization While Roaming	Enforce manual synchronization while roaming
	Allow HTML Formatted Email	Allow HTML formatted Email
	Allow Attachments to be Downloaded to the Mobile Device	Allow attachments to be downloaded to the mobile device
	Attachment Size (KB)	Attachment size (KB)
Device Restrictions	Allow Camera	Allow camera
	Allow Wi-Fi	Allow Wi-Fi
	Allow Bluetooth	Allow Bluetooth
	Allow Infrared Connections	Allow Infrared connections
	Allow Internet Sharing from Mobile Device	Allow Internet sharing from mobile device
	Allow Remote Desktop Connection from the Mobile Device	Allow remote desktop connection from the mobile device



	Allow Desktop Synchronization	Allow desktop synchronization
	Allow Access to Information Stored on a Storage Card	Allow access to information stored on a storage card
	DISCLAIMER	Your mailbox must have an Exchange Enterprise Client Access License (CAL) to implement the above policy settings on a mobile device.
	Enforce Mobile Device Encryption	Only for mobile devices that support encryption
	Enforce Storage Card Encryption	Only for mobile devices that support storage card encryption
	Allow Non-Provisionable Devices to Connect to the Exchange Server	Allows older devices that may not support application of all policy settings to connect to Exchange server
Application Restrictions	Allow Browser	This policy setting requires an Exchange Enterprise Client Access License
	Allow Consumer Email	This policy setting requires an Exchange Enterprise Client Access License
	Allow Unsigned Applications	This policy setting requires an Exchange Enterprise Client Access License
	Allow Unsigned Application Installations	This policy setting requires an Exchange Enterprise Client Access License
	Allow Access to Windows File Shares	Allow access to Windows File Shares
	Allow Access to Windows SharePoint Services	Allow access to Windows SharePoint Services

MANAGE POLICY FILES

The Policy Manage section allows you to upload mobile device policy files.

1. The **Manage > Manage Policy Files** menu allows the Administrator to upload certificates, images and file containing mobile device settings. Clicking the **Manage Policy Files** menu displays the **Manage Policy Files** screen.



2. Click the **Upload Content** button to view the **Upload Certificate** pop-up box.
3. Enter relevant name in the **Content Name** field. Select the desired **Type**. The available content types that you can upload are **Certificates, Images** and **Device Settings**.
 - **Certificates:** the Certificate type allows you to authenticate and register your mobile devices in the MCMS system.
 - **Images:** the Image type allows you to associate an image or a picture file with your document.
 - **Device Settings:** selecting the Device Settings option allows you to upload a policy file that contains the VPN, EAS and Wi-Fi policy parameters that you wish to apply to all devices that are registered using the certificate.
 1. Select the desired **Sub Type** option.
 2. Click **Browse** to select the content file from your local drive.
 3. Click **Upload Content**. The **Upload Status** box displays.
4. Click **OK**. The uploaded content file link displays in the **Policy Files** section.
5. Click the delete icon under the **Actions** column if you wish to remove an uploaded policy file.

Reporting

MCMS reporting system allows you to use enhanced reporting functions, such as the tabular presentation of reports to group associated graphs and reports, and to provide easy navigation between the reports. The enhanced reporting solution also includes filters, which help you generate a variety of real-time reports or narrow down report details based on your filter criteria.

The two and three-dimensional graphs provide an enhanced representation of the data in summary and detailed reports. The *Print* and *Download* links allow you to print and download the displayed graphs and reports to a variety of file formats.

MOBILE DEVICES REPORT

1. Click the **Reports > Mobile Device Overview** menu under the **Mobile Device Reports** section to view the **Mobile Device Overview** reporting dashboard.

The Mobile Devices Reports section on the Reports tab includes the Mobile Device Overview, iOS Hardware Overview, iOS Software Overview, BlackBerry Hardware Overview, BlackBerry Software Overview, Android Hardware Overview and the Android Software Overview menus.

MOBILE DEVICE OVERVIEW

The Mobile Device Overview menu displays the Device Summary, Device Ownership, Hardware, and the Network Information tabs.

Device Summary

The **Device Summary** tab displays a consolidated dashboard that includes the Devices by Ownership, Devices by Platform, Devices by Approval State, New Devices by Month (6 Months), Agent Managed Mobile Devices by Home Carrier, and Agent Managed Mobile Devices by Home Country (Top 10) graphs.

2. Clicking on a graph section displays the associated report details.

Device Ownership

The **Device Ownership** tab shows the **Device Ownership Details Report** that displays the Device Name, Username, Email Address, Platform, Managed By, Ownership, Installed Date, Approval State, Email Client Device ID, License Status and the Last Reported date details. Enter or select the desired filter criteria and click **Apply Filters** to view results matching the selected criteria.

3. Clicking on a **Device Name** displays the associated device details screen, where you can view reports and perform mobile device management actions.

Hardware Details

The **Hardware Details** tab shows the **Hardware Details Report** that displays the Device Name, Username, Device Type, Platform, Email Client, Manufacturer, Model, Operating System, Approval State, License Status, and the Last Reported date details.

4. Enter or select the desired filter criteria and click **Apply Filters** to view results matching the selected criteria.



Network Information

The **Network Information** tab shows the **Network Information Details Report (Agent Managed Devices)** that displays the Device Name, Username, Phone Number, Platform, Home Carrier, Home Country, Roaming, Current Carrier, Current Country, License Status, and the Last Reported date details.

5. Enter or select the desired filter criteria and click **Apply Filters** to view results matching the selected criteria.
6. Clicking on a **Device Name** displays the associated **View Device Details** screen, where you can view reports and perform mobile device management actions.
7. Click on the **Back To Results** button to return to the previous screen.



BlackBerry Reporting

The **Inventory Management** report for BlackBerry devices allows you to view hardware and software details of selected BlackBerry handheld devices. For this purpose, the **Inventory Management Reports** section includes the **BlackBerry Hardware Overview** and the **BlackBerry Software Overview** menus.

BLACKBERRY HARDWARE OVERVIEW

1. Click the **Reports > BlackBerry Hardware Overview** menu to view the **BlackBerry Hardware Overview** screen. Here, you can perform detailed analysis of BlackBerry Hardware information. The **BlackBerry Hardware Overview** section displays the **Device Summary**, **Hardware**, **BlackBerry Policy**, and the **Network Information** reports.

Device Summary

The Device Summary dashboard displays the Device Summary by Model (Top 10), the Operating System Summary, the Devices by Home Carrier, and the Devices by BlackBerry Policy graphs.

2. Click on the desired sections on the graphs to view associated details.

Hardware

3. Click the **Hardware** tab to view the **Hardware Details Report** that displays the Serial Number (IMEI/ESN), PIN, Phone Number, User, Manufacturer, Model, OS Version, Software Platform Version, Screen Language, Total Memory (MB), Activation Date, and Last Reported information.
4. Enter or select the desired filter criteria and click **Apply Filters** to view matching results.

BlackBerry Policy

5. Click the **BlackBerry Policy** tab to view the **BlackBerry Policy Details Report** that includes the Serial Number (IMEI/ESN), PIN, Phone Number, User, BlackBerry Policy, Security Password, and Last Reported details.
6. Enter or select the desired filter criteria and click **Apply Filters** to view matching results.

Network Information

7. Click the **Network Information** tab to view the **Network Information Details Report** that includes the Serial Number (IMEI/ESN), PIN, Phone Number, User, Home Carrier, Current Carrier, Network Type, Email Address, and the Last Reported details.
8. Enter or select the desired filter criteria and click **Apply Filters** to view matching results.
9. Click **Clear Filters** to reset the entered search criteria.

BLACKBERRY SOFTWARE OVERVIEW

1. Click the **Reports > BlackBerry Software Overview** menu to view the **BlackBerry Software Overview** screen, where you can view and analyze software installation details on the BlackBerry handheld devices. The **BlackBerry Software Overview** section displays the **Installed Software** and the **Software Details** report tabs.

Installed Software

The **Installed Software** tab shows you the **Installed Software Details Report** that includes the Application Vendor, Application Name, Major Versions, and Install Count details.



2. Enter or select the desired filter criteria and click **Apply Filters** to view results matching the selected criteria. Clicking on an Application Name link displays the associated details in the **Software Details** tab.

Software Details

3. Click the **Software Details** tab to view the **Software Details Report** that includes the Device Name, Phone Number, Application Vendor, Application Name, Major Version, Full Version, and Last Reported details.
4. Enter or select the desired filter criteria and click **Apply Filters** to view results matching the selected criteria. Clicking on a Device Name link displays the associated details on the **View Device Details** screen.
5. Clicking on the **Actions** tab displays the available actions that you can perform on the device.
6. Click on the **Back To Results** button to return to the previous screen.



iOS Device Reports

IOS HARDWARE OVERVIEW

1. Click the **Reports > iOS Hardware Overview** menu shows the **iOS Hardware Overview** screen that includes the **Hardware Summary**, **Hardware Details**, and the **Network Information** tabs. The **iOS Hardware Overview** screen displays the Devices by Ownership, Devices by Model, Devices by Operating System, Devices by Free Internal Storage, Devices by Home Carrier, and the Devices by Home Country (Top 10) reporting graphs.
2. Click any section on the bar graph or the pie chart displays the associated report details.

Hardware Details

3. Click on the **Hardware Details** tab to view the **Hardware Details Report** that displays the Device Name, User Name, Phone Number, IMEI/ESN, Apple Serial Number, Ownership, Model, Model ID, Operating System Version, Total Internal Storage (GB), Free Internal Storage (GB), License Status and Last Reported details.
4. Enter or select the desired filter criteria and click **Apply Filters** to view results matching the selected criteria.

Network Information

5. Click on the **Network Information** tab to view the **Network Information Details Report** that displays the Device Name, Username, Phone Number, Home Carrier, Home Country, ICCID, Roaming, Current Carrier, Current Country, License Status, and the Last Reported date details.
6. Enter or select the desired filter criteria and click **Apply Filters** to view results matching the selected criteria.
7. Clicking on a **Device Name** link shows the associated **View Device Details** screen for the selected mobile device.

IOS SOFTWARE OVERVIEW

1. Click the **Reports > iOS Software Overview** menu to view the **Installed Software** and the **Software Details** tabs.

Installed Software

The **Installed Software** tab shows the **Summary by Software Report** that displays the Application Name, Bundle ID, Major Versions and the Install Count details.

2. Click on the **Install Count** link to view the associated **Software Details Report** on the **Software Details** tab.

Software Details

3. Alternatively, click the **Software Details** tab to view the **Software Details Report** that displays the Device Name, Username, Phone Number, Application Name, Bundle ID, Full Version, Application Size (MB), Data Size (MB), License Status, and the Last Reported details.
4. Enter or select the desired filter criteria and click **Apply Filters** to view results matching the selected criteria.
5. Click on a **Device Name** link to display the **View Device Details** screen for the selected mobile device.



Android Device Reports

ANDROID HARDWARE OVERVIEW

1. Select the **Reports > Android Hardware Overview** menu to view the **Android Hardware Overview** screen that includes the **Hardware Summary**, **Hardware Details**, and the **Network Information** tabs.

The **Android Hardware Overview** screen displays the Devices by Ownership, Devices by Manufacturer (Top 10), Devices by Operating System, Devices by Free Storage (Internal Storage + External Storage), Devices by Home Carrier, and the Devices by Home Country (Top 10) reporting graphs.

2. Click any section on the bar graph or the pie chart to view the associated report details.

Hardware Details

3. Click on the **Hardware Details** tab to view the **Hardware Details Report** that displays the Device Name, User Name, Phone Number, Serial Number (IMEI/ESN), Ownership, Manufacturer, Model, Operating System Version, Total Storage (GB), Free Storage (GB), RAM, License Status and Last Reported details.
4. Enter or select the desired filter criteria and click **Apply Filters** to view results matching the selected criteria.
5. If required, click on the **Device Name** link to view the associated details on the **View Device Details** screen.

Network Information

6. Click the **Network Information** tab to view the **Network Information Details Report** that displays the Device Name, Username, Phone Number, Home Carrier, Home Country, IMEI, Roaming, Current Carrier, Current Country, Current Network TYPE, License Status, and the Last Reported date details.
7. Enter or select the desired filter criteria and click **Apply Filters** to view results matching the selected criteria.
8. Click on a **Device Name** link to view the associated **View Device Details** screen for the selected mobile device.

ANDROID SOFTWARE OVERVIEW

1. Click the **Reports > Android Software Overview** menu to view the **Installed Software** and the **Software Details** tabs.

Installed Software

The **Installed Software** tab shows the **Installed Software Report** that displays the Application Name, App ID, Major Versions and the Install Count details.

2. Click on the **Install Count** link to view the associated **Software Details Report** on the **Software Details** tab.

Software Details

3. Click on the **Software Details** tab to view the **Software Details Report** that displays the Device Name, Username, Phone Number, Application Name, App ID, Full Version, Application Size (MB), Data Size (MB), Install Location, License Status, and the Last Reported details.
4. Clicking on a **Device Name** link displays the **View Device Details** screen for the selected mobile device.



All Devices Reporting

The All Devices Reports section displays the All Devices Inventory Overview and the All Devices Security Overview reports menus.

ALL DEVICES INVENTORY OVERVIEW

The **All Devices Inventory Overview** report allows you to view and perform detailed analysis of all your mobile devices. The **All Devices Inventory Overview** section displays the **Device Summary** and the **Device Details** reports.

Device Summary

The Device Summary dashboard displays the Total Managed Devices, the Devices by Platform, and the Devices by Manufacturer (Top 10) graphs.

Click on a graph section to view the associated report details.

Device Details

The **Device Details** tab shows the **Device Details Report** that displays the Device Name, User Name, Phone Number, Platform, Device Type, Manufacturer, Model, Operating System, IMEI/ESN, Install Date, License Status, and the Last Reported information.

ALL DEVICES SECURITY OVERVIEW

The **All Devices Security Overview** report allows you to view and perform security state analysis all your mobile devices. The **All Devices Security Overview** section displays the **All Devices Summary** and the **Mobile Device Security Details** reports.

All Devices Summary

The All Device Summary dashboard displays the Traveler Managed Mobile Devices by Approval State, Traveler Managed Mobile Devices by Vulnerability, BES Managed Mobile Devices by Security State, BES Managed Mobile Devices by Vulnerability, Agent Managed Mobile Devices by Security State, and the Agent Managed Mobile Devices by Vulnerability graphs.

Click on a graph section to view the associated mobile device security details.

Mobile Device Security Details

The **Mobile Device Security Details** tab shows the **Mobile Device Security Details Report** that displays the Device Name, User Name, Phone Number, Platform, Managed By, Device Jailbroken/Rooted, Device Passcode Status, Encryption Status, Model, Remote Wipe Supported, Approval State, License Status, and the Last Reported information.

Clicking on a **Device Name** link displays the associated device details.



Partner Reports

MCMS provides a partner dashboard that is designed especially for MCMS partners and resellers. If you are a Fiberlink Partner or a Reseller, then you can access the partner reports. Partner Reports allow you to view your Customer and Device Details. The Partner Reports section includes a consolidated Overview Dashboard, along with the Customer and Device details reports which allows the Partner to analyze details pertaining to trials, demos, and number of devices using the MCMS Desktop Management and Mobile Device Management solutions.

The **Partner Reports** section allows you to view and perform detailed analysis of all Sales deals to Customers/Prospects and the associated number of mobile device details. Click on the **Manage** tab to view the **Partner Reports** section, which displays the **Partner Overview**, **Customer Details** and the **Device Details** reports.

Partner Overview

The **Partner Overview** dashboard displays the Account by Status, Account by Managed Device Type, Mobile Devices by OS and the Desktop Devices by OS graphs.

Click on a graph section to view the associated report details.

Customer Details

The **Customer Details** tab shows the **Customer Details** report that displays the Billing ID, Customer, Status, Create Date, Trial Expiry, Devices, DTM, MDM, Agent MDM, No of CEs, ActiveSync, Traveler, BlackBerry, and the No of CEs Down information.

Enter/select the desired criteria and click **Apply Filters** to view results matching the selected search criteria.

Device Details

The **Device Details** tab shows the **Device Details** report that displays the Billing ID, Customer, Status, Devices, Mobile Devices, Enrolled, Only CE, iOS, Android, BlackBerry, Windows, Others, Laptops/Desktops, PC, and the MAC information.

Enter/select the desired criteria and click **Apply Filters** to view results matching the selected search criteria.

My Watch List

The **My Watch List** feature allows you to monitor all your devices and view a summary of all device statuses on the MCMS Home page. If you have opted for MCMS Mobile Device Management solutions, the following Home page screen displays.

The **MCMS Home** page displays the **My Watch List** dashboard, which includes various sections. The header section shows the total number of devices that are being monitored, the **My Watch List** section that displays the number of devices that are vulnerable and are out of compliance with the organizational policies, the **MCMS Services** section that allows you to navigate and access the various MCMS features, and the **My Support** section that allows you access MCMS support services.

1. Clicking on the <## devices being managed> hypertext link displays the associated details.
 2. Click the **Manage Watch List** icon to view history of all watch list items that were created and modified.
 3. Alternatively, click the **Manage > Manage Watch List** menu to view the **Manage Watch List** screen.
 - a. The + icon is associated with Watch List metrics that have been modified or deleted. Click the + icon to view an audit history of modifications that were made to the Watch List item.
 - b. Click on the Watch List item to view the associated Watch List criteria and description details.
 - c. Click **Restore** to revert to watch list item criteria and description.
 - d. Click **Back to Home** to return to the Home Page.
 4. Click the **Refresh Watch List** icon to view the most recent watch list.
 5. Click the **Add Watch List** icon to add a watch list item.
 - a. Enter relevant Watch List description. Enter or select the desired Watch List criteria.
 - b. Click **Save** to save the Watch List item.
- The **My Watch List** section lists the real-time device monitoring metrics for the mobile devices. Clicking on a Watch List metric item displays the associated details. You can Edit, Delete, and view an audit report of all changes that were made to watch list item.

6. Click on the **Modify Watch List** icon to view the **Edit**, **Delete**, and **History** icons.
7. Click **Edit** to view the **Edit Watch List** pop-up window. Here, you can edit the Watch List criteria and the Watch List description, as shown below.
 - a. If required, modify the Watch List description and the criteria.
 - b. Click **Save** to save and view the updated Watch List alert.
8. To delete a Watch List item, click on the associated Modify Watch List icon.
9. Clicking the **Delete** icon displays the delete confirmation dialog box. Click **Yes** to delete the Watch List item.



10. Click the Modify Watch List icon.
11. Click the associated **History** icon to view audit history of changes that were made to the Watch List item.
 - a. Click the expand/collapse toggle icon to display or hide the associated Watch List item audit history.
 - b. Click **Restore** if you wish to restore an earlier version of the Watch List criteria.
 - c. Click **Back to Home** to return to the Home page.
12. Clicking on the **My Watch List** item displays the associated metric details.
13. Click on the desired **Device Name** link to **View Device Details** screen for that device.

You can view the various reports available for the selected device by clicking on the drop-down arrow next to the **Summary** menu.

Click on a report menu to view the associated report details. Clicking on the **Actions** drop-down list displays the actions you can perform on the selected device.

On the MCMS **Home** page, the **MCMS Services** section displays links to some of the most popular MCMS applications. Click on the desired link to view the associated details.

The **MCMS Support Center** section on the MCMS Home page allows you to contact and interact with the MCMS support personnel.

The **My Support Center** section also provides information on the upcoming Webinars. Click the **Register Now** button if you wish to enroll for a free MCMS Webinar.



The Manage Tab

This tab contains the workflows for the following:

- **Device Management**
- **Apps for Mobile Devices**
- **Documents**
- **User Management**
- **Policy Management**
- **Portal Administrator Management**
- **Device Enrollment**
- **MDM Services Administration**

DEVICE MANAGEMENT

The **Device Management** module allows you to manage and view consolidated device details that display the various detailed reports for individual devices on your network.

Selecting the **Manage > View All Devices** menu displays **View All Devices** screen.

The **View All Devices** screen lists all devices on your network along with the associated report details. The **Device Details** screen displays the Device Name, Username, Device Type, Manufacturer, Model, Operating System, IMEI/MEID, Installed Date, Last Reported, and the Mailbox Managed details, as shown below.

- **Click the refresh results icon to retrieve and view the most recent results.**
- **You can sort the displayed report in ascending or descending order. Click the drop-down arrow on any column to view the Sort Ascending, Sort Descending, and the Columns menu options.**
- **Clicking the Sort Ascending or the Sort Descending options allow you to sort the displayed column details.**
- **Clicking on the column heading also allows sorting the displayed information.**
- **You can customize the displayed report to show only those columns that you wish to see on the report. Click the drop-down arrow and click the Columns option to select or unselect the desired column headings from the options list, as shown below.**
- **Clicking on the Save Column Preferences button allows you save your column preferences.**
- **Clicking on the Go to Smart Search button displays the Smart Search screen that allows you perform searches using multiple search criteria. For details, refer to the Smart Search section.**
- **To narrow the search results, select the required search option and enter the desired search criteria.**
- **Click Search to view results matching the search criteria.**
- **To export the displayed results to .csv or .xls formats, select the desired file format from the csv drop-down list and click the Export button.**
- **Clicking on a Device Name link displays the associated device summary.**
- **Clicking the Refresh Results icon displays the most recent details.**
- **Clicking the Back To Results button displays the results page.**



The **Summary** screen displays the Username, IMEI/MEID, Last Reported and the Managed Status information, along with the Hardware, Security & Compliance, and the Custom Attributes details.

- **Clicking on the Username link displays the View User Details screen.**
- **Clicking on the Device Name hyperlink displays the View Device Details screen.**

Viewing Android Device Details

1. Click the **Manage > View All Devices** menu to display the **View All Devices** screen.
2. Clicking on an **Android** device displays the associated **View Device Details** screen, as shown below.
3. Click the **Summary** drop-down menu to list the various reports for the selected Android device.

Clicking the **Summary** menu for an Android device lists following device reports:

- Hardware Inventory
 - Operating System
 - Network Information
 - Location Information
 - Security & Compliance
 - Software Installed
 - Running Services
 - App Distributions
 - Documents Accessed
 - Mobile Data Usage
 - MCMS Services
 - Change History
 - Action History
4. Click the **Actions** drop-down menu to list the actions that you can perform a mobile device. The **Actions** drop-down menu for an Android device displays the following actions:
 - **Refresh Device Information:** allows you to refresh and retrieve the most recent data from the mobile device.
 - **Locate Device:** allows you to locate the mobile device location using latitude and longitude coordinate mappings on Bing maps.
 - **Send Message:** allows you to send a notification message to an Android mobile device.
 - **Lock Device:** allows you to send a command that will lock the Android device. This may be helpful especially in cases where a user has misplaced a device and at the same time wishes to restrict any data access on the device.
 - **Reset Device Passcode:** allows you to clear the current passcode on an Android device. This action is helpful especially at times when an end-user had forgotten the device login passcode.
 - **Selective Wipe (Restrict Device):** allows you to wipe the Wi-Fi profile, Exchange ActiveSync profiles, and Web shortcuts configured on the Android device via MCMS policy. The Selective Wipe can be helpful especially when you wish to remove all corporate information from an individual's mobile device.
 - **Wipe Device:** allows you to wipe out all data on an Android mobile device and reset it to the original factory settings. In Android 2.2, the Wipe Device action will reset only the phone memory. However, in Android 2.3, the Wipe Device action will reset both the phone memory and the SD card. The Wipe Device action can be helpful especially when a corporate mobile device is lost or stolen and you wish to ensure access to confidential data on the corporate device is denied.



- **Change Android Policy:** allows you to change or publish updated mobile device management policies on your Android devices. You can create or update the Android policies using the **Create Policy Sets** and the **Manage Policy Sets** menus on the **Manage** tab
 - **Remove Android Control:** allows you to unregister the device from MCMS. For example: an Administrator may use this workflow menu to unregister the mobile device of an employee who has moved out of the organization.
 - **Hide Device Record:** allows you to mark a device as inactive. The **Hide Device Record** action does not remove control on the device.
 - **Change Rule Set:** allows you to apply or update the rule set assigned to a device.
5. On any View Device Details report screen, you can click the **Edit** if you wish to modify or update certain parameter value. On the **Summary** screen, click **Edit** if you wish to modify or update the **Ownership** and the **Phone Number** information.
 6. Make desired changes and click **Save** to save changes.
 7. Click **Back To Results** to return to the **View All Devices** screen.

View iOS Device Details

1. On the **Manage > View All Devices** screen, select an **Apple iOS** mobile device.

The **View Device Details** screen for the selected device displays.

Device Summary

2. Click the **Summary** drop-down menu to list the various reports available for the selected Apple iOS mobile device, as shown below.
3. Clicking the **Summary** drop-down menu displays the **Hardware Inventory, Network & Location, Security & Compliance, Certificates, Software Installed, App Distributions, Documents Downloaded, Change History, Location Information,** and the **Action History** reports.
4. Click the **Hardware Inventory** item to display the **Hardware Inventory** details, as shown below.
5. Click the **Network Information** menu to display the **Network** details, as shown below.
6. Click the **Security & Compliance** item to display the **Security and Compliance, Configuration Profiles,** and **Device Restrictions** details, as shown below
7. Click the **Certificates** item to display the installed **Certificates** details, as shown below.
8. Click the **Software installed** item to display the **Software Installed** and the **Provisioning Profiles** details, as shown below.
9. Click the **App Distributions** item to display the **App Distribution** details, as shown below.
 - a. On the **App Distributions** screen, click on an **App Name** hyperlink to display the associated **Application Details**, as shown below

- b. Click **Back To Results** to return to the **View All Devices** screen.
10. On the **View Device Details** screen, clicking on the **Documents Downloaded** item displays the **Documents Downloaded** details, as shown below.
11. Clicking the Mobile Data Usage item to display the **Plan details**, **Aggregate Mobile Data Usage**, and the **Daily Mobile Data Usage [Current Period]** details, as shown below
12. Clicking the **Change History** item to display the **Change History** details, as shown below
13. Click the **Location Information** report to display the device IP address and the geographic location coordinates on a map, as shown below
14. Click the hyperlink text to enable location history tracking for enrolled devices.
15. Click the **Action History** item to display a list of actions performed on a device, as shown below.

Perform Mobile Device Actions

Click the **Actions** drop-down menu to display a list of actions that you can perform on an **iOS** device. The available options include Refresh Device Information, Lock Device, Reset Device Password, Wipe Device, Change iOS Policy, Distribute App, and the Remove iOS Control actions.

- **Refresh Device Information:** allows you to refresh and retrieve the most recent data from the mobile device.
- **Last Known Location:** allows you to locate the mobile device location using latitude and longitude coordinate mappings on Bing maps.
- **Send Message:** allows you to send a notification message to an iOS mobile device.
- **Lock Device:** allows you to lock an iOS device. This may be helpful especially in cases where a user has misplaced a device and at the same time wishes to restrict any data access on the device.
- **Reset Device Passcode:** allows you to reset and clear the login pass code of an iOS device. This action is helpful especially at times when an end-user had forgotten the device login passcode.
- **Selective Wipe (Restrict Device):** allows you to wipe the Wi-Fi profiles, VPN and Exchange ActiveSync settings configured on the iOS device via MCMS policy. This allows you to delete data folders such as contacts, email Inbox, and other corporate application settings. The Selective Wipe can be helpful especially when you wish to remove all corporate information from an individual's mobile device. Selective Wipe can be helpful especially when you wish to remove all corporate information from an individual's mobile device.
- **Wipe Device:** allows you to wipe out all data on an iOS mobile device and reset it to the original factory settings. The **Wipe Device** action can be helpful especially when a corporate mobile device is lost or stolen and you wish to ensure access to confidential data on the corporate device is denied.
- **Change iOS Policy:** allows you to change or publish updated mobile device management policies on your iOS devices. You can create or update the iOS policies using the **Create Policy Sets** and the **Manage Policy Sets** menus on the **Manage** tab
- **Distribute App:** allows you to distribute application to iPhone devices via iTunes App Store.
- **Remove iOS Control:** allows you to unregister the device from the MCMS. For example: an Administrator may use this workflow menu to unregister the mobile device of an employee who has moved out of the organization.
- **Hide Device Record:** allows you to mark a device as Inactive. The **Hide Device Record** action does not remove control on the device.
- **Change Rule Set:** allows you to apply or update the rule set assigned to a device.



Click **Back To Results** to return to the **View All Devices** screen.

Viewing BlackBerry Device Details

1. Click the **Manage > View All Devices** menu to display the **View All Devices** screen.
2. Clicking on a **BlackBerry** device displays the associated **View Device Details** screen, as shown below.
3. Click the **Summary** drop-down menu to list the various reports for the selected device.

Clicking the **Summary** menu for a BlackBerry device lists following device reports:

- Hardware Inventory
 - Network Information
 - Location Information
 - Software Installed
 - Modules
 - Service Books
 - MCMS Services
 - Change History
 - Action History
4. Click the **Actions** drop-down menu to list the actions that you can perform on the mobile device. The **Actions** drop-down menu for a BlackBerry device displays the following actions:
 - **Refresh Device Information:** allows you to refresh and retrieve the most recent data from the mobile device.
 - **Locate Device:** allows you to locate the mobile device location using latitude and longitude coordinate mappings on Bing maps.
 - **Send Message:** allows you to send a message to a BlackBerry mobile device.
 - **Lock Device:** allows you to lock a BlackBerry device. This may be helpful especially in cases where a user has misplaced a device and at the same time wishes to restrict any data access on the device.
 - **Selective Wipe (Restrict Device):** allows you to wipe the Email profile configured on the BlackBerry device via MCMS policy. This allows you to delete data folders such as contacts, email Inbox, and other corporate application settings. The Selective Wipe can be helpful especially when you wish to remove all corporate information from an individual's mobile device.
 - **Wipe Device:** allows you to wipe out all data on a BlackBerry mobile device and reset it to the original factory settings. The **Wipe Device** action can be helpful especially when a corporate mobile device is lost or stolen and you wish to ensure access to confidential data on the corporate device is denied.
 - **Remove BlackBerry Control:** allows you to unregister the device from MCMS. For example: an Administrator may use this workflow menu to unregister the mobile device of an employee who has moved out of the organization.
 - **Hide Device Record:** allows you to mark a device as inactive. The **Hide Device Record** action does not remove control of the device.
 5. On any **View Device Details** report screen, you can click the **Edit** if you wish to modify or update certain parameter value. On the **Summary** screen, click **Edit** if you wish to modify or update the **Ownership** and the **Phone Number** information.
 6. Make desired changes and click **Save** to save changes.



7. Click **Back To Results** to return to the **View All Devices** screen.

Viewing Details of Devices Registered on the BlackBerry Enterprise Server

1. Click the **Manage > View All Devices** menu to display the **View All Devices** screen.
2. Clicking on a device registered on the **BlackBerry Enterprise Server** displays the associated **View Device Details** screen, as shown below.
3. Click the **Summary** drop-down menu to list the various reports for the selected BlackBerry Enterprise Server device.

Clicking the **Summary** menu lists the following device reports:

- Hardware Inventory
 - Network Information
 - Device Features
 - Messaging History
 - Security & Compliance
 - Software Installed
 - Modules
 - Service Books
 - Change History
 - Action History
4. Click the **Actions** drop-down menu to list the actions that you can perform on the mobile device. The **Actions** drop-down menu for a BlackBerry Enterprise Server device displays the following actions:
 - **Refresh Device Information:** allows you to refresh and retrieve the most recent data from the mobile device.
 - **Send Message:** allows you to send a message to a BlackBerry mobile device. For BlackBerry Enterprise Server devices, you can choose the Message Type option. Click the PIN option if you wish to send an SMS message. Otherwise, select the Email option to send an email notification to the BlackBerry device.
 - **Reset Device Passcode:** allows you to reset the device passcode.
 - **Wipe Device:** allows you to wipe out all data on a BlackBerry mobile device and reset it to the original factory settings. The **Wipe Device** action can be helpful especially when a corporate mobile device is lost or stolen and you wish to ensure access to confidential data on the corporate device is denied.
 - **Change BES Policy:** allows you to change the policy set assigned on the BlackBerry Enterprise Server.
 - **Remove Device from BES:** allows you to unregister a device from the BlackBerry Enterprise Server.
 - **Hide Device Record:** allows you to mark a device as inactive. The **Hide Device Record** action does not remove control on the device.
 5. On any **View Device Details** report screen, you can click the **Edit** if you wish to modify or update certain parameter value. On the **Summary** screen, click **Edit** if you wish to modify or update the **Ownership** and the **Phone Number** information.
 6. Make desired changes and click **Save** to save changes.
 7. Click **Back To Results** to return to the **View All Devices** screen.

Viewing Details of Devices Registered on the Exchange ActiveSync Server

1. Click the **Manage > View All Devices** menu to display the **View All Devices** screen.



2. Clicking on a device registered on the **Exchange ActiveSync Server** displays the associated **View Device Details** screen, as shown below.
3. Click the **Summary** drop-down menu to list the various reports for the selected Exchange ActiveSync Server device.

Clicking the **Summary** menu lists the following device reports:

- Exchange ActiveSync
 - Change History
 - Action History
4. Click the **Actions** drop-down menu to list the actions that you can perform on the mobile device. The **Actions** drop-down menu for a **Exchange ActiveSync Server** device displays the following actions:
 - **Refresh Device Information:** allows you to refresh and retrieve the most recent data from the mobile device.
 - **Wipe Device:** allows you to wipe out all data on an Exchange ActiveSync mobile device and reset it to the original factory settings. The **Wipe Device** action can be helpful especially when a corporate mobile device is lost or stolen and you wish to ensure access to confidential data on the corporate device is denied.
 - **Change ActiveSync Policy:** allows you to change the policy set assigned to an Exchange ActiveSync device.
 - **Remove Device from Exchange Server:** allows you to unregister a device from the Exchange Server.
 - **Change Rule Set:** allows you to apply or update the rule set assigned to a device.
 - **Hide Device Record:** allows you to mark a device as inactive. The **Hide Device Record** action does not remove control on the device and does not remove the device from the Exchange Server.
 5. If an Exchange ActiveSync device is enrolled and merged, then the device view for such devices displays additional reports, as shown below.
 6. For Exchange ActiveSync devices that are enrolled and merged, the actions drop-down for such devices display both EAS and MDM actions, as shown below.
 7. On any **View Device Details** report screen, you can click the **Edit** if you wish to modify or update certain parameter value. On the **Summary** screen, click **Edit** if you wish to modify or update the **Ownership** and the **Phone Number** information.
 8. Make desired changes and click **Save** to save changes.
 9. Click **Back To Results** to return to the **View All Devices** screen.

Viewing Details of Devices Registered on the Lotus Traveler Server

1. Click the **Manage > View All Devices** menu to display the **View All Devices** screen.
2. Clicking on a device registered on the **Lotus Traveler Server** displays the associated **View Device Details** screen, as shown below.
3. Click the **Summary** drop-down menu to list the various reports for the selected Lotus Traveler device.



Clicking the **Summary** menu lists the following device reports:

- Lotus Traveler Summary

- Change History
 - Action History
4. Click the **Actions** drop-down menu to list the actions that you can perform on the mobile device. The **Actions** drop-down menu for a **Lotus Traveler** device displays the following actions:
 - **Block Device:** allows you to block a Lotus Traveler device.
 - **Wipe Device:** allows you to wipe out all data on an Lotus Traveler mobile device and reset it to the original factory settings. The **Wipe Device** action can be helpful especially when a corporate mobile device is lost or stolen and you wish to ensure access to confidential data on the corporate device is denied.
 - **Remove Device from Traveler:** allows you to unregister a device from the Lotus Traveler Server.
 - **Change Rule Set:** allows you to apply or update the rule set assigned to a device.
 - **Hide Device Record:** allows you to mark a device as inactive. The **Hide Device Record** action does not remove control on the device.
 5. If a Lotus Traveler device is enrolled and merged, then the device view for such devices displays additional reports, as shown below.
 6. For Lotus Notes devices that are enrolled and merged, the actions drop-down for such devices display both Lotus Traveler and MDM actions, as shown below.
 7. On any **View Device Details** report screen, you can click the **Edit** if you wish to modify or update certain parameter value. On the **Summary** screen, click **Edit** if you wish to modify or update the **Ownership** and the **Phone Number** information.
 8. Make desired changes and click **Save** to save changes.
 9. Click **Back To Results** to return to the **View All Devices** screen.

SMART SEARCH

The **Smart Search** menu allows you to perform basic and advanced searches for devices. You can perform a quick search for devices by entering the device name or the first few letters of the device in the **Search Devices** box and clicking the **magnifying-glass** icon.

- **To list devices using basic or advanced search options, click the Manage > Smart Search menu to view the Smart Search screen.**
 - You may perform a basic search by selecting the desired **Search for** option, and the **Last Reported** filter option.
 - Select the device types that you wish to search. If you have purchased the MCMS Mobile Device Management solution, apart from **Desktops** and **Laptops**, you also have the choice to select **Smart phones**, **Tablets**, and other mobile devices. Click **Search** to view results matching the selected criteria.
 - a. Alternatively, you may perform an advanced search by selecting multiple options from the **Category**, **Attribute**, and **Criteria** drop-down lists from the **Define Search Conditions** section. You may also enter the desired search criteria in the **search box**.
 - b. Clicking the  icon in the **Smart Search** section allows you to include additional filter options for entering your search conditions. Clicking the  icon allows you to remove a search condition row.
 - c. You can choose to apply the **AND**, **OR**, and **Advanced criteria across the above conditions** options and enter criteria condition in the text box. Hover on the associated help icon to view more details.
 - d. If required, click the **Clear Filter(s)** button to reset the search options.
 - e. Click **Search**. The **Search Results** section displays the results matching the entered search criteria.
 - f. Clicking on a **Device Name** link displays the associated device details.

- g. Click the **Back To Results** button to return to the **Search Results** screen.
- h. If you wish to save the displayed column preference, click the **Save Column Preferences** button.
- i. Click the **Refresh Results** icon to view the most recent results.

- j. Click the **Create Device Group** button to add the listed devices to a device group. The **Device Group Details** pop-up box displays.
- k. Enter the desired **Group Name** and **Description** in the **Device Group Details** pop-up box.
- l. Select **Private** or **Public** options in the **Type** section. Selecting **Private** makes the device group available only to you. However, selecting **Public** will display the device group in the available device groups list.
- m. Click **Save** to save the device group. The **Device Group** pop-up box displays the confirmation message.

- n. Click **OK**.
- o. If **you** wish to edit or modify a device group, then click **Manage > Device Groups** menu to navigate to the **Device Groups** screen, click on a **Group Name** to view the associated devices.

- p. Make desired changes to the selected search criteria and click **Search** to view matching results.

- q. Click on the **Update Device Group** button. If required, enter desired information in the pop-up box and click **Update** to save changes.
- r. On the **Device Groups** screen, click the **Actions** tab to view the available actions that you can perform on the device group

DEVICE GROUPS

The **Device Groups** menu allows you to view, create, and edit device groups. A device group is a collection of devices that have one or more identical attributes. You can search for devices matching specific search criteria and group those devices into a device group.

To list the available Device Groups:

1. Select the **Manage > Device Groups** menu to view the **Device Groups** screen.

2. Clicking a device group link displays the associated devices on the **Smart Search** screen.

3. Click the **Update Device Group** button to view the **Device Group Details** dialog box.

4. If required, edit the **Group Name**, **Description**, and **Type** options information.
5. Click **Update** to save changes. The **Device Group updated successfully** message displays.

6. You can also view the **Device Groups** drop-down window by clicking on the arrow next to the **Search Devices** box.

A device group can be a non-editable default device group, an editable public group, a non-editable public group or a private device group. You can search for devices matching specific search criteria and group those devices into a device group. A device group can be one of the following types:

- **MCMS** –indicates that the device group is visible to all MCMS Administrators. Only Fiberlink Master Administrators can edit or delete such device groups.

- **Public** – indicates that the device group is visible to all Administrators. Such device groups can be edited and deleted by all Administrators. When an device action is applied on a MCMS device group, the device group type is automatically set to public.
 - **Private** - indicates that such device groups are visible only to the Administrator who created the device group. Therefore, it is a private device group and can be edited or deleted by the logged-in Administrator.
7. Click the **Actions** button associated with a device group to view the available actions for the device group. You can also edit a device group by selecting the **Edit Group** action.
 - **The Delete Group action allows you to delete public and private device groups that you have created. If a device group has automated actions associated, then the Delete Group action will not be available, as shown below.**
 - **The Hide Devices action allows you to mark the devices in the group as Inactive. However, the Hide Devices action does not remove control on the devices.**
 - **The Send Message action allows you to send a notification alert to all devices in the device group. This action is applicable only for iOS, Android, and Windows7 mobile devices. The Send Message action for BlackBerry devices includes the additional Message Type option. Select the PIN option to send an SMS message. Otherwise, select the Email option to send the alert notification as Email message.**
 - **The Change MDM Policy action allows you assign a specific policy to devices in the group.**
 - **The Change Rule Set action allows you assign a compliance rule set to all devices in the device group.**
 - **The Change Plan action is available only for devices that have enabled the Mobile Expense Manage module. The Change Plan action allows you to edit and assign a specific plan to devices in the group.**
 - **The Distribute App action allows you distribute applications to devices in the group.**
 - **The Distribute Document action allows you distribute documents to devices in the group.**
 - **The Create Copy of Group action allows you to create a duplicate group that can you can modify, as required.**
 - **The Delete Group action allows you to delete public and private device groups that you have created. The Delete Group action is available for private groups. However, this action is not available for device groups with associated automated actions or to public device groups created by MCMS or other Administrators.**
 - **You can associate automated actions to default MCMS device groups and public device groups.**
 8. Selecting an **Apply Policy** action displays the **Apply Policy** dialog box, as shown below.
 9. Enter relevant details and click the **Setup for Automated Assignments** button.
 10. Enter your MCMS account password in the **Security Check** pop-up box. This ensures that only authorized administrators can assign automated action.
 11. Click **Continue**. A confirmation pop-up box displays.
 12. Click **OK** to view the automated action associated with the device group.
 13. Click the **Show all automated actions** toggle button to view all scheduled action details.
 14. Click the **Hide all automated actions** toggle button to hide the displayed action details.
 15. Click on the desired action item to perform the action.
 16. Click the **Go to Smart Search** button to view **Smart Search** screen.



BULK UPDATE (DEVICE ATTRIBUTES)

The **Bulk Update (Device Attributes)** menu allows you to search for users and edit user properties and associated service plans.

To perform a Bulk Update:

1. Select the **Manage > Bulk Update (Device Attributes)** menu to view the **Bulk Update Device Attributes** screen.
2. In the **Upload File** box, click the **Browse** button and locate the Bulk Update file.

The Bulk Update File must adhere to the following requirements.

- The Bulk Update file must be in either **.txt** or **.csv** formats.
- The file size must be **2 MB** or less.
- The first row in the file must include the attribute titles, which will be displayed as the column headings.
- Every subsequent row must contain attribute values for a single record. The values in each row should be separated by commas.
- **MCMS Device ID**, and **Device Name** values are mandatory for each row and should be the first and second values, respectively. Other details are optional.
- The date attribute must be indicated in the **mm/dd/yyyy** format, where **dd** indicates the day, **mm** indicates the month, and **yyyy** indicates the year.

Note: If required, export the Search Results displayed on the **Manage > Smart Search** screen to **.csv** or **.txt** formats to view a sample Bulk Update file format.

3. After selecting the Bulk Update file, click **Upload** to upload the selected file. The **Active Bulk Update** screen displays status of the **Bulk Update** results.
4. Click the **View Prior Update Logs** button to view the **Bulk Update Transaction Logs**.
5. If required, download the file to view errors that occurred when performing the **Bulk Update** activity.

BULK UPDATE TRANSACTION LOG

The **Bulk Update Transaction Log** menu allows you to view the **Bulk Update Transaction Log** file that is automatically created when you perform a **Bulk Update** activity. This file details the results of a **Bulk Update** activity.

To view the Bulk Update Transaction Log:

1. Select the **Manage > Bulk Update Transaction Log** menu to view the **Bulk Update Transaction Log** screen.
2. If required, click the **Download File** icon to download the **Bulk Update Transaction Log** file.
3. Click **Save** to save the file to a desired location or click **Open** to view the file.
4. On the **Bulk Update Transaction Log** screen, click the **View Errors** icon to view errors that may have occurred during the **Bulk Update (Device Attribute)** activity.
5. Click the **Back to Logs** button to return to the **Bulk Update Transaction Log** screen.



MANAGE CUSTOM ATTRIBUTES

The **Manage Custom Attributes** menu allows you to create Custom Attributes. Every device has a set of unique identifiers or attributes that are standard across devices. For example: Device Name, Operating System, Device ID, Manufacturer, etc. help distinguish one device from the other devices.

Attributes also help in creating device groups that share similar attributes. For example: devices with less than 512 MB of RAM can be formed into a device group, if required. Here, RAM is an attribute of the device.

Apart from the Standard attributes, you can also create Custom Attributes to suit your requirement. For example: if an IT Administrator wishes to group devices based on their location, a Custom Attribute such as Country can help in performing this grouping activity.

Note: When you view device details, the associated Custom Attributes are displayed in the **Custom Attributes** section. To view, create, and manage Custom attributes:

To manage Custom Attributes:

1. Select the **Manage > Manage Custom Attributes** menu to view the **Manage Custom Attributes** screen.
2. Click the **Add Custom Attribute** button to view the **Add Custom Attribute** dialog box.
3. Enter the desired Custom Attribute Name. For this example, **Phone_Color** will be the **Attribute Name**.
4. Select **Text** as **Attribute Type**. The **Attribute Name** will include a **Text** value.
5. Click **Add** to add the Custom Attribute. The **Manage > Manage Custom Attributes** screen displays the added Custom Attribute.
6. To view this Custom Attribute assigned to mobile devices, navigate to the **Manage > View Device Details** screen.
7. Select the **Hardware Inventory** report. The newly added attribute displays under the **Custom Attributes** section.
8. Click **Edit** to edit the Custom Attribute value for the selected device.
9. Click **Save** to save changes

MANAGE COMPLIANCE RULE SETS

MCMS allows you to apply compliance rules on your end-user mobile devices. Compliance Rule sets are conditions that are checked on devices on real-time basis. If a device is not in compliance with the defined rule sets or conditions, then appropriate enforcement actions will be taken on the device. Most mobile device platforms allow users to ignore and override passcode policies and application restrictions. Rules such as the **Enforce MCMS Control** are useful, especially to track users who accidentally or willfully try to remove their organization's device management and control capabilities. Hence, it is necessary to use Compliance Rules to enforce actions, even if you already publish policies to your end-user mobile devices.

To Configure Compliance Rules for your devices:

1. Select the **Manage > Manage Compliance Rule Sets** menu item to view the **Configure Compliance Rules** screen.



- **When you access the Manage > Manage Compliance Rule Sets workflow for the first time, the View All Rule Sets screen displays, as shown below.**
- 2. You must create compliance rule sets by selecting the desired rules settings. Then, you can choose to assign these rule sets to your devices or device groups. Click **Create New Rule Set** if you wish to create a new Rule Set. The **Create New Rule Set** screen displays.
- 3. Enter an appropriate rule set name.
- 4. Click **Continue** to view the **Update Rule Set <rule set name>** screen.
- 5. Compliance Rules are divided into the following five categories, namely: **Basic Settings, Enforcement Rules, Monitoring Rules, Geo Fencing Rules, and Expense Monitoring Rules**. Click on the desired category on the left panel to view and configure the associated rules settings on the right panel. The **Expense Monitoring Rules** and the **Geo Fencing Rules** tabs are available only for select Customers. Contact your MCMS Administrator for details.
- 6. Select the desired rules check boxes. When you select a rule checkbox, the associated rule settings display.
- 7. Click **Save**. The **Update Rule Set** dialog box displays.
- 8. Enter your MCMS account password in the **Update Rule Set** dialog box.
- 9. Click **Continue** to create the rule set.
- 10. If you have already created one or more rule sets, then the View All Rule Sets screen includes **Disable All Rules** and the **Create New Rule Set** buttons.
- 11. Clicking the **Create New Rule Set** button displays the **Create New Rule Set** screen. Notice that when you have already created one or more rule sets, the **Copy From** drop-down menu also displays.
- 12. After entering a Rule Set name, you can choose to copy the rule settings from a predefined rule set by selecting the desired option from the **Copy From** drop-down list.
- 13. Click **Continue** to view the **Update Rule Set** screen.
- 14. Click on the tabs in the left panel to view or set the associated rule settings in the right.

Here you can define the rule criteria and also configure the enforcement action that needs to be taken when a device does not comply with the rule set. Only devices marked as **Important** on the **Manage > View All Devices** screen will be exempt from the automated actions that will occur when a device is out of compliance.

The **Basic Settings, Enforcement Rules, and Monitoring Rules** tab display automatically. The Basic Settings category allows you to set real time compliance for selected Operating Systems, Event Notification Recipients, and Exemptions. The **Enforcement Rules** category allows you to set enforcement actions that will be taken when a device is not in compliance with the device compliance conditions. To ensure security, you can select the **Alert Administrator, Alert User and Administrator, Block, and Wipe** actions, where necessary.

The **Geo Fencing Rules** category is available for select Customers only. If you wish to avail this feature, then contact your Fiberlink Account Administrator. The **Geo Fencing Rules** feature allows you to define geographical coordinates as the boundary for a mobile device. Only devices with iOS and Android platforms that are registered in the MCMS system support the Geo Fencing Rules capability. It is mandatory for iOS devices to have an iOS MDM agent version 1.4 installed, while Android mobile devices must have Android MDM agent version 3.0 installed.

15. Selecting the **Enable Geo-Fencing** checkbox allows you to select an Enforcement Action that should be taken, when a device is taken beyond the specified geographical range. You can specify the geographical boundary via the **Manage > Manage Locations** menu.
16. You can specify **Enforcement Actions** when a device is taken out of the approved locations. You can initiate enforcement actions by alert notifications to the User and the Administrator, enforce policy or take specific actions when the device is checked out of the specified location. For example: if an employee takes a corporate device out of the office premises, then you can choose to enforce the Restrict or Wipe device actions.
17. When a device is taken out of the approved location, you can choose to perform the following actions:
 - **Alert Administrator:** allows you to send an alert message to the Administrator.
 - **Alert User and Administrator:** allows you to send an alert message both to the User and the Administrator.
 - **Restrict Device:** allows you to restrict the device. You can choose to take this action as soon as the device is taken out of the approved location, or after the specified duration in Hours or Days after displaying a warning notification on the device.
 - **Change Policy:** allows you to apply the selected policy when the device is taken out of the approved location.
 - **Wipe:** allows you to wipe out all data on the mobile device and reset it to the original factory settings. In Android 2.2, the Wipe Device action will reset only the phone memory. However, in Android 2.3, the Wipe Device action will reset both the phone memory and the SD card. You can choose to take this action as soon as the device is taken out of the approved location, or after the specified duration in Hours or Days after displaying a warning notification on the device.
18. Click on the **Manage Locations** hyperlink text to view the **Manage Locations** screen. The **Manage Locations** screen displays the Location Name, Location Info, Policy Rules, Last Updated By, Last Updated On, and the Actions information. On the **Manage Locations** screen, you can view, add, and manage the approved locations.
19. Alternatively, click the **Manage > Manage Locations** menu to view the **Manage Locations** screen.
20. Click the page navigation links at the bottom of the screen if you wish to view to the other locations.
21. Click the **Add address based Location** if you wish add a physical location address. The **Add address based Location** dialog box displays.
22. Enter the desired **Location Name, Address** and the **Range (in miles)**.
23. In the **Range (in miles)** field, specify a numeric circumference range for your location.
24. Click **Search** to view the geographical location coordinates displayed on the bing maps.
25. Click the **Here** hyperlink text to select the location. The defined location is added and displays on the Manage Locations screen.
26. Click the **Location Name** hyperlink to edit the specified location.
27. Click the **Actions** drop-down list associated with the **Location Name**. The available actions are **Edit, Assign Policies,** and **Delete**.



28. On the **Manage Locations** screen, you can choose to add Wi-Fi based location. Adding a Wi-Fi location allows you to track and identify devices that are not connected to the specified Wi-Fi hotspot.
29. On the **Add Wi-Fi based Location** pop-up box, enter a desired **Location Name** and **Wi-Fi SSID**.
30. Enter correct access point MAC Address for accuracy.
31. Click **Add** to add and approve the Wi-Fi based location.
32. If you wish to track and view the device location history, then navigate to the **Manage > View All Devices** menu. The **View All Devices** screen displays.
33. Click on the **Device Name** link to view the associated **View Device Details** screen.
34. Click the **Location Information** report menu to view the **Location History** details.

The **Monitoring Rules** category allows you to monitor and alert the User and the Administrator when a device SIM is changed and/or when a device enters a roaming state and/or when the device Operating System settings are changed. You can select the required enforcement actions when the defined monitoring rules are violated.

35. Select the **Expense Monitoring Rules** tab if you wish to specify compliance rules to monitor roaming mobile data usage and In-network mobile data usage. You can specify the Warnings at different threshold levels of data usage.
36. Click **Save** to save changes..
37. Enter your MCMS account password in the **MCMS Password** box. This ensures only authorized Administrators can create and save rule sets.
38. Click **Continue** to confirm adding the rule set.
39. Click **Back To Results** to return to the MCMS Home page.
40. If you wish to exclude a specific device from device compliance actions, then navigate to **Manage > View All Devices** screen.
41. Click on the **Device Name** link to see the associated **View Device Details** screen.
42. Select the **Hardware Inventory** report for the device.
43. Click **Edit**.
44. Under the **Custom Attributes** section, select **Yes** for the **Important Device (Skip Enforcement Action)** attribute.
45. Click **Save** to save changes. Enforcement actions will not be taken on this device. However, the device will receive alerts when it is the out of compliance.

COMPLIANCE STATUS OVERVIEW

The **Compliance Status Overview** report displays a list of all devices that are not in compliance with the configured compliance rules.

To view the Compliance Status Overview report:

1. Select the **Manage > Manage Compliance Status Overview** menu item.

The **Compliance Status Overview** screen displays the Device Name, Username, Active Rule Name, Rule Set Name, Action Configured, Action Status and the Time of Execution details.

2. If required, select the desired search criteria and click **Filter** to narrow the displayed search results.

Depending on the device compliance status, the **Action Status** column will display the **Executed**, **Planned** and the **NA** (Not Available) values. **NA** is displayed only for devices that are configured to receive compliance status alerts.

3. If required, export the displayed list in CSV and Excel formats.
 4. Click on the **Device Name** to see the associated **View Device Details** screen.
 5. Click **Back To Results** to return to the **Compliance Status Overview** screen.
- **When an out of compliance device is remediated and complies with the set rules, then the device name is automatically removed from the Compliance Status Overview list.**

APPS FOR MOBILE DISTRIBUTION

The **Manage > Apps for Mobile Devices** section allows the Administrator to upload applications, distribute applications, and manage application distributions to tablets, smart phones, and mobile devices.

Manage Apps

The **Manage Apps** menu item allows you to search and view all mobile applications available on the upload Server. Clicking the **Add New App** button allows you to upload an application for your mobile device

The **Apps for Mobile Devices** module under the **Manage** tab includes the following menu options:

- Manage Apps
- Manage App Distributions
- Distribute App

To add a new application for mobile devices:

1. Click the **Manage > Manage Apps** menu to view the **Manage Apps** screen. The **Manage Apps** screen displays the App, Name, Platform, Device Support, Category, Type, Latest Version, Active Distribution Count, Installed Count, Pending Upgrade Count, Update Date, Provisioning Profile Expiry, Status and Actions details.
2. Select the desired filter options and click **Search** to view results matching the selected search criteria.
3. If required, click **Clear** to reset the selected filter options.

4. Clicking on an **App** name displays the associated details on the **View App Details** screen.
5. Click **Back To Results** to return to the **Manage Apps** screen.
6. Clicking on an **Install Count** link displays the **Distribution Details by Devices** screen, which lists all mobile devices that have installed the application.
7. Click **Back To Results** to return to the **Manage Apps** screen.
8. On the **Manage Apps** screen, the **Free Space Available** section displays the present space limit that is available on the Upload Server. Hover your mouse-pointer over the displayed value to view the **Total Storage Space** and the **Available Storage Space** information. The size of the application that you wish to upload or distribute to your end user mobile devices must be less than the **Available Storage Space**.
9. Click the **Add New App** button to upload new applications that you wish to distribute and install on iOS, Android, and Windows mobile devices.
10. Select the type of application that you wish to upload. You can add Enterprise Applications for iOS devices, Enterprise Applications for Android mobile devices, Apple iTunes App Store applications, Google Play applications, Marketplace Public Applications and Marketplace Private Applications for Windows mobile devices.
11. Select the desired application type. You can upload the following types of applications.
 - **iTunes App Store App** - allows you to upload applications for Apple iOS devices using the Apple iTunes and the Apple App Store. Enter the first few characters of the iTunes application name in the App Name field. A list of applications matching the entered name displays. Click to select the desired application. The associated application icon displays. Click **Add to MCMS** to view the application on the Manage Apps screen. Click the associated Actions drop-down menu to view a list of actions that you can perform.
 - **Enterprise App for iOS** - allows you to upload Enterprise Applications for iOS devices. Enter appropriate details in the Source, Category, Description, and Upload Screenshots fields. Select the Upload from option and select the desired file. iOS device applications have .ipa file extension. You can also select the Custom URL option, if you wish to upload the .ipa file from a hosted server. Click **Add to MCMS** to view the application on the Manage Apps screen.
 - **Google Play App** - allows you upload Android applications via the Google Play. Open Google Play (<https://play.google.com/store>) and locate the desired Android application. Copy the URL of the selected Android application and paste it in the Google Play URL for App field. Click **Add to MCMS** to view the application on the Manage Apps screen. If required, click on the Name hyperlink to view details on the View App Details screen. Click **Back To Results** to return to the Manage Apps screen. Click on the associated Actions drop-down menu to view a list of actions that you can perform.
 - **Enterprise App for Android** - allows you to upload Enterprise Applications for Android devices. Enter appropriate information in the Source, Category, and Description fields. Click **Browse** to select the desired icons in the Upload Screenshots field. Android application source files have .apk file extension. Click **Add to MCMS** to view the application on the Manage Apps screen.
 - **Marketplace Public App** - allows you to upload applications for Windows mobile devices via the Marketplace Public App. Enter the first few characters of the Windows application name in the App Name field. A list of applications matching the entered name displays. Click to select the desired application. The associated application icon displays. Click **Add to MCMS** to view the application on the Manage Apps screen. Click the associated Actions drop-down menu to view a list of actions that you can perform.

- **Marketplace Private App** - allows you to upload Marketplace Private Application from Microsoft Deep Link applications for Windows Mobile devices. Enter deep link provided by Microsoft, and other appropriate details in the **Category**, **Name**, and **Description** fields. If required, select the desired **App Policies** options. Click **Add to MCMS** to view the application on the **Manage Apps** screen.
12. If you wish to upload an Enterprise App for iOS devices, then select the **Enterprise App for iOS** option. The **Add New App** screen displays.
 13. On the **Upload App** screen, click the **Browse** button next to the **Source** field to select the desired .ipa file or the correct URL if the application resides on a hosted server.
 14. Enter relevant details in the **Category**, and **Description** fields
 15. Click the **Browse** button next to the **Upload Screenshots** field to select the application screens that you wish to display.
 16. Under the **App Policies** section, select the desired policy options.
 17. Click **Add to MCMS** to add the application to MCMS that you can distribute to your end-user devices. The **Uploading App** progress bar displays.

A confirmation message displays on the **Manage Apps** screen.

18. Click the **Audit History** button to view a list of all actions that were performed.
19. On the **Manage Apps** screen, click the **Actions** tab to view the actions that the Administrator can perform on the newly added application.
20. Click the **Actions** tab to view the available actions. The actions displayed on the **Actions** tab vary based on the application type that you have selected.
21. Click the **View App Details** action to view the **View App Details** screen.
22. On the **Manage Apps** screen, selecting the **Upgrade App** action allows you to upgrade an uploaded application to updated version.
23. Enter relevant details and click **Upgrade** to upgrade.
24. Click **Back To Results** to return to the **Manage Apps** screen.
25. Select the **Edit App** action on the **Manage Apps** screen, if you wish to edit the **Category** information, **Description**, or the **Screenshots** for an uploaded application.
26. Make desired changes to the **Category**, **Description**, or the selected screenshots.
27. On the **Manage > Manage Apps** screen, selecting the **Update Provisioning Profile** action allows you to upgrade the provisioning profile for an uploaded application.
28. Click **Back To Results** to return to the **Manage Apps** screen.
29. If you wish to upload an iTunes App Store application, then select the **iTunes App Store App** option from the **Add New App** tab.



30. The Add an iTunes App Store App screen displays.
31. The **Add an iTunes App Store App** screen displays the **App Name** and the **Bundle Identifier** fields. Enter the first few characters of the iTunes App Store application in the **App Name** field. iOS Apps matching the entered criteria display.
32. Click on the desired iTunes application. The associated identifier displays in the **Bundle Identifier** field.
33. Click **Add to MCMS** to add the selected application to MCMS. A confirmation message displays.
34. If required, click on the hyperlink text to view the application details.
35. Click **Back To Results** to return to the **Manage Apps** screen.
36. On the **Manage Apps** screen, click the **Actions** tab to view the actions that the Administrator can perform on the newly added application.

Apple Store – Volume Purchasing Program

The **Apple Store Volume Purchase Program (VPP)** allows educational institutions to buy iOS apps in volume and distribute the apps to their users. The Volume Purchase Program allows developers and organizations to purchase large number of applications at special prices from the Apple Stores.

After receiving the VPP spreadsheet file that contains the buy codes for the apps, the administrator can distribute it to the end users, who can redeem these codes and download apps from the App Stores. Displayed below is a sample VPP Codes file.

1. If you wish to upload and manage your VPP codes, then navigate to the **MCMS Manage > Manage Apps** menu screen.
2. The **Manage Apps** screen displays.
3. Click the **Actions** tab to list the available actions.
4. Click the **Upload VPP File** action to view the **Upload VPP File** screen.
5. Click **Browse** and select the VPP file for the selected iTunes Store application.
6. Click **Add to MCMS** to upload the VPP file to the MCMS system. The VPP codes can now be redeemed against the associated iTunes Store application.
7. If you wish to manage or view the status of VPP codes, then click the **Manage VPP Codes** action
8. The **Manage VPP Codes** screen displays the associated details. If you wish to clear the unused VPP codes, then click the **Clear VPP Codes** button.



9. Alternatively, select the **Clear VPP Codes** action to clear unused VPP codes.
10. In the confirmation box that appears, click **Yes** to confirm clearing the associated VPP codes.

Manage App Distributions

The **Manage App Distributions** menu allows the Administrator to list the uploaded mobile device applications and manage application distributions.

To manage app distributions:

1. Select the **Manage > Manage App Distributions** menu item to view the **Manage App Distributions** screen, which displays the App, Platform, Target Devices, Status, Date, Distribution Name, Distributed By, Send Email Notification and the Action information.
2. Select the desired filter options and click **Search** to view results matching the selected search criteria.
3. If required, click **Clear** to reset the selected filter options.
4. Click an **App** name link to view the associated **View App Details** screen.
5. Click **Back To Results** to return to the **Manage App Distributions** screen.
6. On the **Manage App Distributions** screen, clicking the **Distribution Name** link displays the associated Distribution Details by Devices screen, which shows the Device Name, User Name, Last Reported, Status, and Distributions details.
7. Click **Back To Results** to return to the **Manage App Distributions** screen.
8. The **Action** column displays the **Stop Distribution** icon associated with the uploaded application. Click the **Stop Distribution** icon to stop distributing the selected application, if required. The stopped application is immediately removed from the **Manage App Distributions** screen.
9. If required, select either the CSV or Excel file format option and click **Export** to export the displayed results.
10. Click on the **New Distribution** button to view the **Distribute App** screen that allows you to create a new application distribution.

Distribute Applications

The **Distribute App** module allows the Administrator to distribute software applications to iOS and Android mobile devices on or off the corporate network.

To distribute mobile device applications:

1. Select the **Manage > Distribute App** menu item to view the **Distribute App** screen.
2. Click the **Search App** icon next to the **App** field to view the **Search to Distribute** pop-up window, which lists all uploaded mobile device applications. Alternatively, on the **Distribute App** screen, enter the first few characters of an application name in the **App** field to view a list of applications that include the entered characters.

3. Select the desired **Target Devices** that you wish to distribute the application. If you selected an Android application, then the **Target Devices** section displays All Android Devices, Device Group and Specific Device options. Instead, if you select an iOS application, then all iOS Devices, Device Group and Specific Device options display.
4. If you select the **Device Group** option, then select the desired device group from the associated drop-down list.
5. If you wish to ensure the application is distributed only to members in the current selected group, then check the **Current Group Members Only** option. This will restrict the selected application being distributed to any new members that may be added to the device group in the future.
6. If you wish to distribute the application to a specific device, then select the **Specific Device** option. Click the **Search Device** icon to select the device from the **Search Device** dialog box.
7. Check the box associated with the required device and click **Select Device** to select the device and return to the **Distribute App** screen.
8. The **Distribution Name** field is automatically populated with relevant information. Update the displayed **Distribution Name**, if required.
9. Enter the appropriate description in the **Description** field.
10. In the **Notification Details** section, select the **Send Mail Notifications** checkbox if you wish to receive the App Distribution email notification.
11. Click **Distribute** to perform a security check and then distribute the application to the selected target devices.
12. Click **Continue** to complete the application distribution. The application distribution confirmation message displays on the **Manage App Distributions** screen, which shows the App, Platform, Target Devices, Status, Date, Distribution Name, Distributed By, Send Email Notification, and the Action details.
13. If required, select either the CSV or Excel file format option, and click **Export** to export the displayed results.

DOCUMENTS FOR MOBILE DEVICES

The **Manage > Documents** section allows the Administrator to add new documents, manage and distribute documents, and manage document distributions to smart phones and mobile devices.

The **Documents** module under the **Manage** tab includes the following menu options:

- Manage Documents
- Manage Document Distributions
- Distribute Document

Manage Documents

The **Manage Documents** menu item allows you to search and view all documents available on the upload Server. The **Manage Documents** screen displays the Document, Type, Categories, Active Distributions Count, Downloads, Create Date, Status, Update Date, Status, Restrict Share, and Actions details. Clicking the **Add New Document** button allows you to upload a document that can be downloaded or distributed to your mobile device.

If you wish to add a new document, then navigate to the **Manage > Manage Documents** screen. The **Free Space Available** section displays the present space limit that is available on the Upload Server. Hover your mouse-pointer over the displayed value to view the **Total Storage Space** and the **Available Storage Space** information. The size of the document that you wish to upload or distribute to your end user mobile devices must be less than the **Available Storage Space**.

The **Add New Document** option allows you to upload documents that you wish to distribute to iOS and Android mobile devices.



1. Click the **Add New Document** tab to view the **Upload Document** screen.

The **Total Storage Space** and the **Available Storage Space** information display.

2. Enter relevant details in the **Document Name**, **Document**, and **Description** fields.
 3. Select the **Restrict Share** checkbox, if you wish to restrict sharing the document
 4. The **Categories** option allows you to organize and search your documents in the MCMS system. Enter a category name in the **Categories** text box, if you wish to assign a category for the document. If you have already created few categories, then the list of available categories displays.
5. Click **Upload** to upload the document to MCMS. The **Uploading Package** progress bar displays.

The **Manage Documents** screen displays the uploaded document.

6. Clicking the **Actions** menu displays the actions that you can perform. The available options include **View Document Details**, **Edit Document Details**, **Distribute Document**, **Distribution Details by Devices**, **View All Distributions**, and **Delete Document** actions as shown below.
7. Click on the **Document** name link. The **View Document Details** screen displays.
8. Click on the desired **File Name** to Open or Save the document to a file location.
9. Click **Back To Results** to return to the **Manage Documents** screen.

Distribute Document

The **Manage > Distribute Document** menu allows the Administrator to distribute the uploaded documents to iOS and Android mobile devices.

To distribute a document:

1. Select the **Manage > Distribute Document** menu item to view the **Distribute Document** screen.
2. Click the **Search Document** icon next to the **Document** field to view the **Search to Distribute** pop-up window to list the documents uploaded for mobile devices.
3. Alternatively, on the **Distribute Document** screen, enter the first few characters of a document name in the **Document** field to list documents that include the entered characters.
4. Select the desired **Target Devices** that you wish to distribute the document. **All Devices**, **Device Group** and **Specific Device** are the available Target Devices options.
5. If you select the **Device Group** option, then select the desired device group from the associated drop-down list.
6. Check the **Current Group Members Only** option to ensure the document is distributed only to members in the current selected group. This will restrict the selected document being distributed to any new members who may be added to the device group in the future.



7. If you wish to distribute the document to a specific device, then select the **Specific Device** option. Click the **Search Device** icon to select the device from the **Search Device** dialog box.
8. Check the box associated with the required device and click **Select Device** to select the device and return to the **Distribute Document** screen.
9. The **Distribution Name** field is automatically populated with relevant information. Update the displayed **Distribution Name**, if required.
10. Enter appropriate description in the **Description** field.
11. If required, click the **Calendar** icon to select a document **Expiration Date**.
12. Click **Distribute** to perform a security check and then distribute the document to the selected target devices.
13. Click **Continue** to complete the document distribution. The document distribution confirmation message displays on the **Manage Documents** screen, which shows the Document, Type, Categories, Active Distributions Count, Downloads, Create Date, Update Date, Status, Restrict Share, and the Actions details.

Manage Document Distributions

The **Manage > Manage Document Distributions** menu allows the Administrator to list the uploaded documents and manage document distributions for mobile devices.

To manage document distributions:

1. Select the **Manage > Manage Document Distributions** menu item to view the **Manage Document Distributions** screen, which displays the Document, Type, Target Devices, Status, Date, Expiration Date, Distribution Name, Distributed By, and the Action information.
2. Select the desired filter options and click **Search** to view results matching the selected search criteria.
3. If required, click **Clear** to reset the selected filter options.
4. Click on the **New Distribution** button to create a new document distribution.
5. Enter relevant details in the **Document Name** field.
6. Alternatively, click the **Search Document** icon to view the available document select the document.
7. Select desired options in the Target Devices, and Expiration Date fields.
8. Enter a **Distribution Name** and relevant **Description**.
9. Click **Distribute**. After performing the security check, the document is uploaded to the Server. The **Manage Documents** screen displays.
10. Clicking on an Active Distribution Count or the Downloads link displays the associated details
11. Click **Back To Results** to return to the **Manage Document** screen.
12. Clicking the **Audit History** button displays the **Audit History** screen.
13. If required, select either the CSV or Excel file format option and click **Export** to export the displayed results.

MANAGE SHAREPOINT SETTINGS

The **Manage SharePoint Settings** module allows you to integrate MCMS with your SharePoint Server environment. You can define the Site Display Name, the Browser URL, Site URL, name of the Library or Folder that you wish to share, Group Access Permissions and sharing restrictions. If required, you can configure restriction settings to prevent users from opening document using third party apps or copy and pasting from a document, or emailing the document. You can securely share documents with your end users iOS devices using the MCMS app. Once the desired information is pushed to the MCMS app on the end user's device, the user will be prompted to enter their SharePoint credentials to view and download the content. The downloaded content is stored locally in the app for easy offline access. When you remove the configured site from MCMS, the content will be deleted from the end-user's device.

To distribute information using your SharePoint Server, you must first configure the appropriate settings on the **Manage > Manage SharePoint Settings** screen. The **Manage SharePoint Settings** screen displays the **Site Display Name**, **Site URL**, **Library/Folder** and the **Group Access Permissions** information.

To configure SharePoint Settings:

1. Select the **Manage > Manage SharePoint Settings** menu to view the **Manage SharePoint Settings** screen.
2. Click the **Add New Site** button to view the **Add a Site** pop-up dialog box.
3. Enter appropriate name in the **Site Display Name** box. This will appear both on the MCMS Admin Interface and on the end-user's device.
4. This is optional information where you can enter the Browser URL box. This will be the browser URL where you access the SharePoint folder.
5. Enter the SharePoint site URL in the **Site URL** box.
6. In the **Library/Folder** box, enter the name of the library or folder that wish to share
7. The **Group Access Permissions** drop-down options allow you to set group access permissions and sharing restrictions. Selecting the **View and Share** option will allow users to open document using third party apps, email the document, and/or copy and paste content. Selecting the **Restrict Share** option will restrict the above options.
8. Click **Save** to save the SharePoint settings.
9. If required, click the associated **Edit Site** link to edit the SharePoint settings.
10. Clicking the **Delete** link will delete the SharePoint for the site and remove the associated content from the end-users' device.

MOBILE EXPENSE MANAGEMENT

The **Mobile Expense Management (MEM)** module allows the administrator to enable mobile usage tracking for specific devices. MEM plans can be defined to setup in-network and roaming data usage limits. Alerts can be setup to automatically trigger on reaching or exceeding the specified threshold criteria. You can also specify the action to be taken by the device on exceeding the data usage limit. When devices reach the usage threshold limits, the specified alerts are automatically triggered. For iOS and Android devices, the MEM feature is enabled only if the selected device is associated with an MEM plan. The Mobile Expense Management module allows you to perform only usage-based tracking and not cost-based tracking.

1. Selecting the **Manage > Manage Plans** menu displays the **Manage Plans** screen.
2. Click the **Show All Plans** toggle button to view both published and inactive plans.
3. Click the **Hide Inactive** toggle button if you wish to hide MEM plans that are in the **Inactive** status.



4. Click the **Create New Plan** button if you wish to create a new plan. The **Create Plan** pop-up dialog box displays.
5. Enter appropriate plan name in the **Plan Name** box.
6. Enter relevant description in the **Plan Description** box. Notice the **Continue** button is enabled only on entering the plan name.
7. Click **Continue**. The plan details display.
8. Under the **Plan Details** section, select the desired **First day of the Billing cycle** date.
9. Specify the data usage limit in the **In-Network Mobile Data Usage Limit (MB)** box.
10. Enter the roaming mobile data usage limit in the **Roaming Mobile Data Usage Limit (MB)** box.
11. Click **Save & Publish**. The **Publish Plan** pop-up dialog box displays.
12. If you wish to set this plan as the default plan, then check the **Set as default** checkbox.
13. For authentication purposes, enter your MCMS password in the password box.
14. Enter relevant description in the description box. This will be useful especially during future audits.
15. Click **Continue** to publish the plan. The plan details display.
16. If you wish to edit the **Plan Name** or the **Description**, then click the pencil icon associated with the relevant fields.
17. Make desired changes and click the green tick icon to save changes. If you wish to cancel the changes, then click the red **X** icon.
18. Click **Edit** to make changes to the published plan. After making the desired changes, click **Save & Publish** to publish the updated plan.
19. After publishing an MEM plan, click the **Actions** tab to view the actions that you can perform. You can choose to deactivate the MEM plan, view audit history, or set the plan as the default.
20. Click **Back to Results** to return to the **Manage Plans** screen.
21. Alternatively, click the **Actions** tab associated with an MEM plan to view the actions that you can perform.
22. The **Edit Plan** action allows you to edit a published plan.
23. Click the **Deactivate Plan** action if you wish to deactivate a published plan and set it as Inactive. The **Deactivate Plan** message box displays.



24. Click **Continue** to view the **Security Check** pop-up box.
25. Enter your MCMS account password and click **Continue** to deactivate the selected plan.
26. The deactivated plan is removed from the Manage Plans list. Click the **Show All Plans** button to list the Inactive plans.
27. If you wish to reactivate an Inactive plan, then click the **Show All Plans** button on the **Manage Plans** screen.
28. Click the **Actions** tab associated with an Inactive plan. The **Reactivate Plan** and the **View Audit History** actions display.
29. Click the **Reactivate Plan** action. The **Publish Plan** pop-up dialog box displays.
30. If you wish to set the plan as the default plan, then select the **Set as default** checkbox. Enter your MCMS account password and relevant description in the description box.
31. Click **Continue**. The Inactive plan is reactivated. Notice that the plan status is changed from **Inactive** to **Published**.
32. If you wish to view the list of actions that were performed on the MEM plan, then click the **Actions** tab.
33. Click the **View Audit History** action. The **View Audit History** screen displays the Published Date, Event, Published Version, Published By, and the Comments details.
34. Click **Back to Results** to return to the **Manage Plans** screen.
35. Click the **Set Default** action if you wish to set a plan as the default MEM plan.
36. The **Set as Default** message box displays. Click **Continue**.
37. A green tick under the **Default** column indicates the default plan.
38. If you wish to remove the default setting, then select the **Actions** tab associated with the default and click the **Clear Default** action.
39. The **Clear Default** message box displays. Click **Continue**.
40. Enter your MCMS account password in the **Security Check** pop-up box.
41. Click **Continue**. The MEM plan default setting is removed.