Product Manual

MDM On Premise Installation

Version 8.1

Last Updated: 06/07/15

Parallels IP Holdings GmbH
Vordergasse 59
8200 Schaffhausen
Switzerland
Tel: + 41 52 632 0411
Fax: + 41 52 672 2010
www.parallels.com

Version 8.1 – Last updated 6th July 2015

Manual Index

Section 1 - On Premise Edition Requirements and Installation

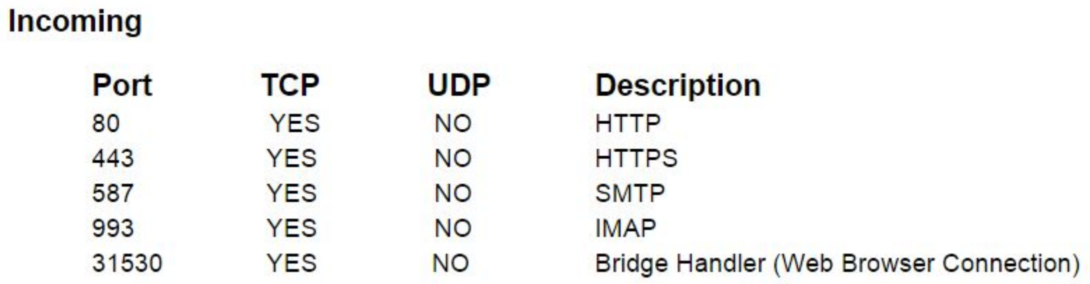
Section 2 - Accounts & BackOffice

Section 3 - The Server User Interface

System Requirements

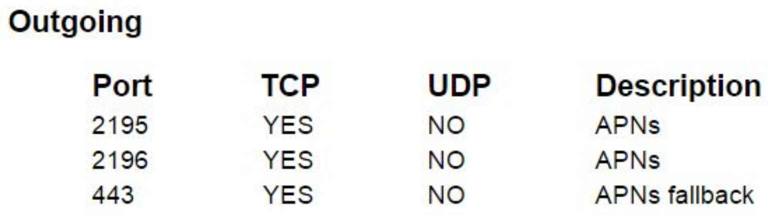
Prerequisites

1. A machine running Windows Server 2008 R2 64-Bit, Windows Server 2012 64-Bit or Windows Server 2012 R2 64-Bit with Microsoft .NET Framework 4.5 and Internet Information Services (IIS) installed.
2. Access to an SMTP server to use to send emails (can be local or remote)
3. **Microsoft SQL Server 2012** - You are required to have a database instance installed either on the same machine running Mobile Device Management or on a different machine within your network. The SA (System Administrator) account needs to be enabled. SQL Server Reporting Services is required to be enabled. If using the Express edition of SQL Server, advanced features are required.
4. A digital certificate valid for the hosting domain signed by a trusted Certificate Authority. A SSL signed certificate from a company which provides digital certificates. This certificate should also support wildcard functionality.
5. **Google Cloud Messaging API** - A Google account with Google Cloud Messaging API enabled is required. For more information on how to enable the GCM service and obtaining the Server API Key, please have a look at the following link: http://developer.android.com/google/gcm/gs.html
6. **SMS Gateway account with CardBoard Fish**. - A HTTPS SMS account with CardBoard Fish is required for the messaging feature to work. More information can be found at the following link: http://www.cardboardfish.com/products/http_sms
7. Make sure that the following firewall ports are open and in the case of the incoming, preferably port forwarded to the MDM server IP as they are vital for communication between your devices and your MDM server:



Incoming

Port	TCP	UDP	Description
80	YES	NO	HTTP
443	YES	NO	HTTPS
587	YES	NO	SMTP
993	YES	NO	IMAP
31530	YES	NO	Bridge Handler (Web Browser Connection)



Outgoing

Port	TCP	UDP	Description
2195	YES	NO	APNs
2196	YES	NO	APNs
443	YES	NO	APNs fallback

Apple Devices Running iOS:

If you have any Apple devices you will also need to make sure that you have in addition to the above:

1. **A Simple Certificate Enrollment Protocol (SCEP)** - A separate server running the SCEP service is required to issue digital certificates to iOS devices. This is vital if you want to manage iOS devices via the MDM portal. The service should also be configured to run using single-password mode. More information can be found at the following link:

http://social.technet.microsoft.com/wiki/contents/articles/9063.network-device-enrollment-service-ndes-in-active-directory-certificate-services-ad-cs.aspx

2. **An Apple Enterprise Account** - An Apple Enterprise Account is required in order to obtain the necessary MDM Vendor Certificate provided by Apple in a .pem format. More information can be found at the following link: https://developer.apple.com/programs/ios/enterprise/

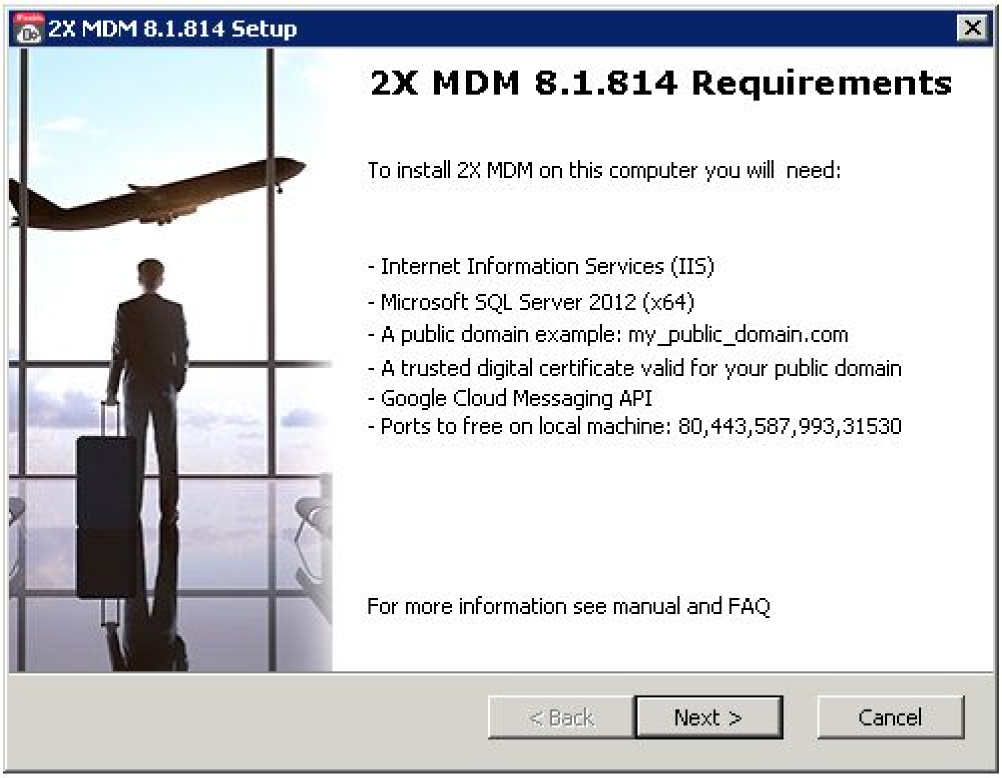
IMPORTANT NOTE: All Certificates should be located in a folder that grants full access at least to the IIS users group (IIS_IUSRS) and SYSTEM. It is also highly recommended that all certificates are saved on a physical drive connected to the MDM Server machine (ex. under the C:\ directory).

Installing Mobile Device Management On Premise Edition

Introduction

Before you can manage your devices using MDM you first have to install and configure the On Premise edition on your server machine. Before doing so, first check whether your machine complies with the minimum hardware specifications (see System Requirements) . Once confirmed, download the Mobile Device Management On Premise edition setup file from here: http://www.2x.com/mdm/downloadlinks/

Setup and File Installation



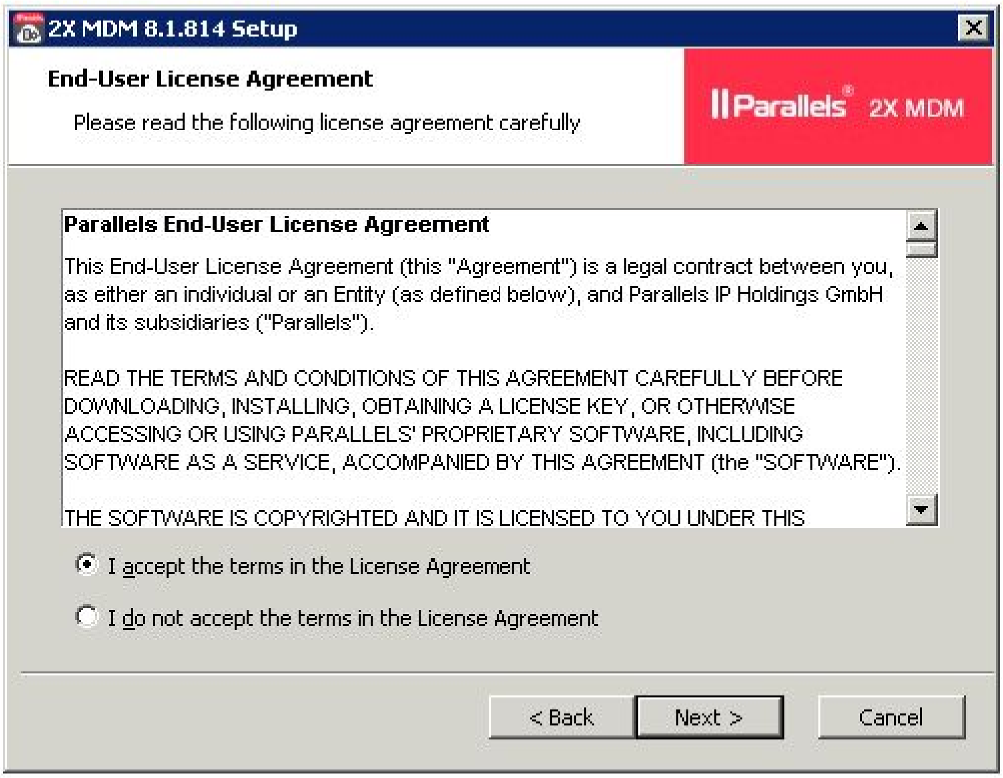
2X MDM 8.1.814 Requirements

To install 2X MDM on this computer you will need:

- Internet Information Services (IIS)
- Microsoft SQL Server 2012 (x64)
- A public domain example: my_public_domain.com
- A trusted digital certificate valid for your public domain
- Google Cloud Messaging API
- Ports to free on local machine: 80,443,587,993,31530

For more information see manual and FAQ

1. Double click the Mobile Device Management setup file to begin the installation. Confirm the machine which Mobile Device Management is going to run on meets the system requirements and click “Next” to continue.



End-User License Agreement

Please read the following license agreement carefully

Parallels End-User License Agreement

This End-User License Agreement (this "Agreement") is a legal contract between you, as either an individual or an Entity (as defined below), and Parallels IP Holdings GmbH and its subsidiaries ("Parallels").

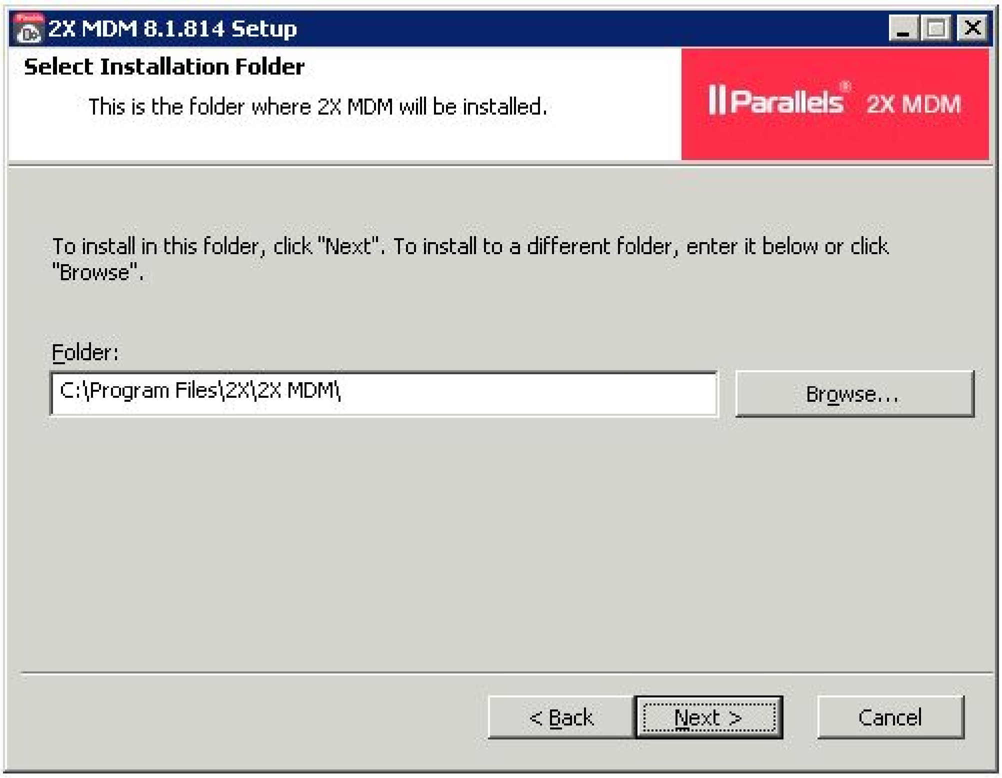
READ THE TERMS AND CONDITIONS OF THIS AGREEMENT CAREFULLY BEFORE DOWNLOADING, INSTALLING, OBTAINING A LICENSE KEY, OR OTHERWISE ACCESSING OR USING PARALLELS' PROPRIETARY SOFTWARE, INCLUDING SOFTWARE AS A SERVICE, ACCOMPANIED BY THIS AGREEMENT (the "SOFTWARE").

THE SOFTWARE IS COPYRIGHTED AND IT IS LICENSED TO YOU UNDER THIS

● I accept the terms in the License Agreement

○ I do not accept the terms in the License Agreement

2. Subsequently, review the End-User License Agreement, and click next to continue. Note that you must accept the terms in order to continue the installation.



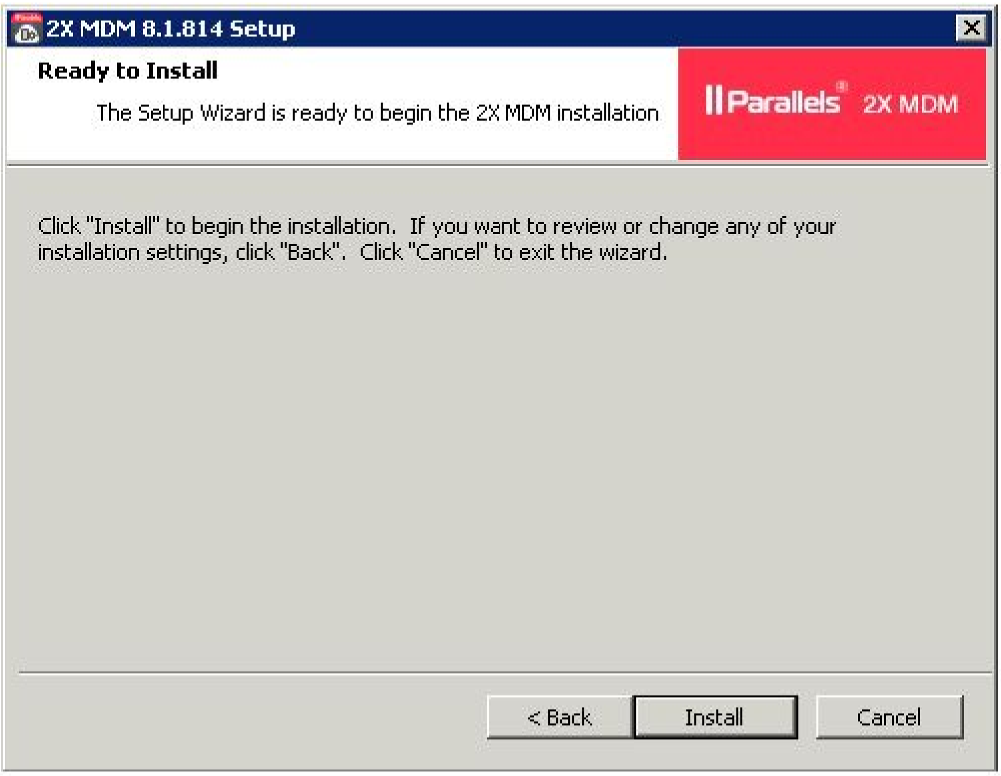
Select Installation Folder

This is the folder where 2X MDM will be installed.

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files\2X\2X MDM\

3. You will then be prompted to define the path where the installation folder will be created. Alternatively, click on the browse button to change the directory if needed.



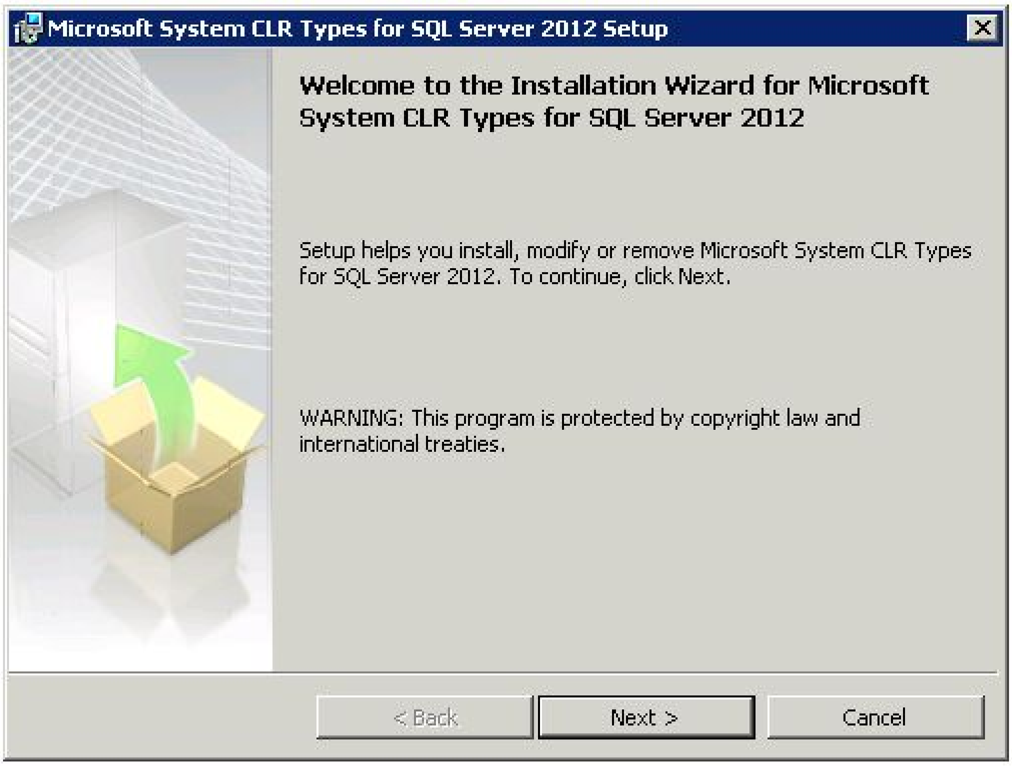
2X MDM 8.1.814 Setup

Ready to Install

The Setup Wizard is ready to begin the 2X MDM installation

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

4. Click 'Install' to confirm the previous steps and start the installation process.



Microsoft System CLR Types for SQL Server 2012 Setup

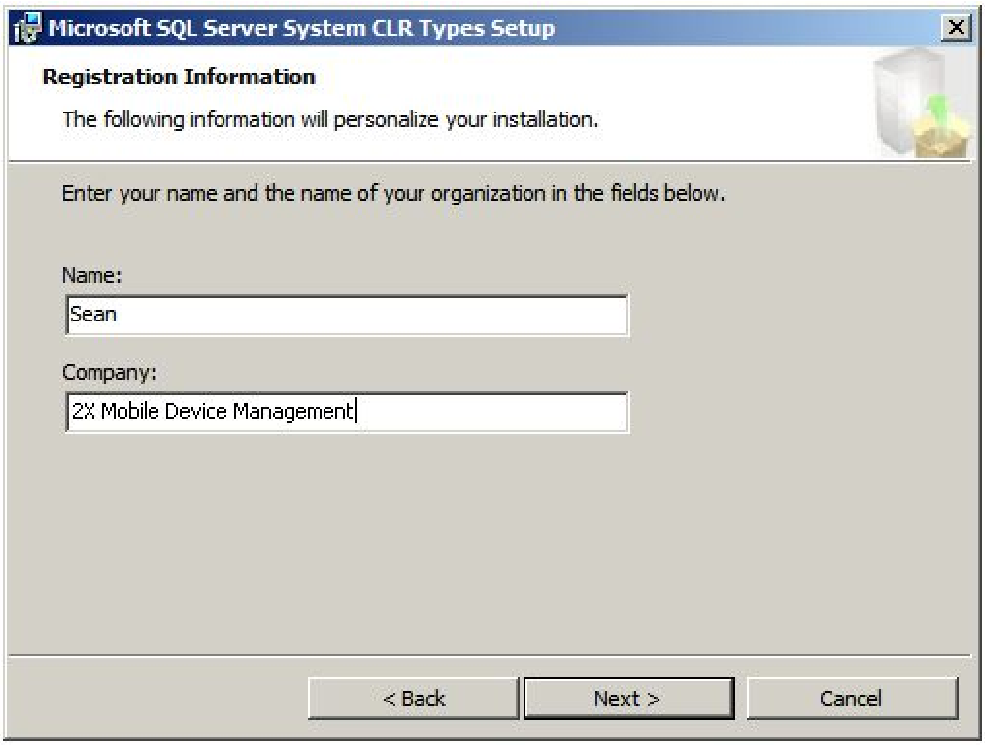
Welcome to the Installation Wizard for Microsoft System CLR Types for SQL Server 2012

Setup helps you install, modify or remove Microsoft System CLR Types for SQL Server 2012. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

5. Once setup starts the file installation process, you shall be prompted to install 'Microsoft SQL Server System CLR Types'. Click on the 'Next' button to proceed. Note that you must accept the terms in order to continue the installation.

Note: You will not be prompted to install this component if it is already available.



Microsoft SQL Server System CLR Types Setup

Registration Information

The following information will personalize your installation.

Enter your name and the name of your organization in the fields below.

Name: Sean

Company: 2X Mobile Device Management

6. Further define the machine administrator and company name, click ‘Next’ and subsequently ‘Install’ to confirm and start the installation process.

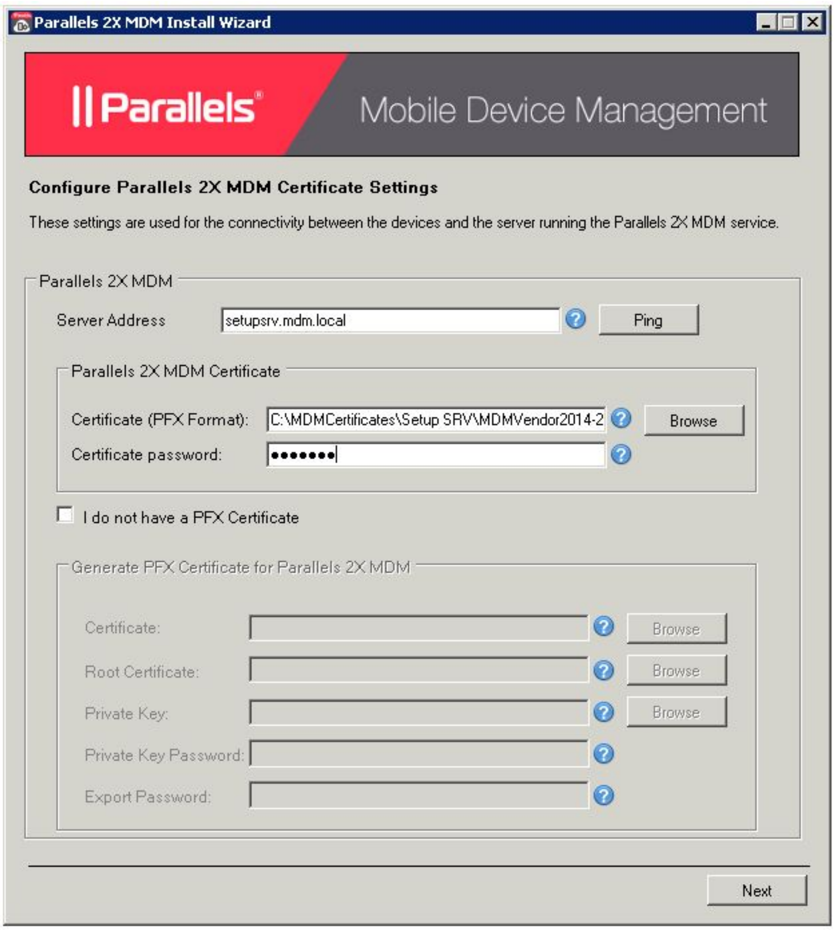
The installation process shall complete and the Mobile Device Management On Premise edition installed on your server machine.

Configuring Mobile Device Management

Introduction

After the file installation is completed, the MDM Install Wizard will start up and guide you through the necessary stages needed to configure your newly installed MDM On Premise edition service. There are a total of 9 settings to be configured.

Certificate Configuration



Parallels 2X MDM Install Wizard

Configure Parallels 2X MDM Certificate Settings

These settings are used for the connectivity between the devices and the server running the Parallels 2X MDM service.

Parallels 2X MDM

Server Address: setupsrv.mdm.local

Parallels 2X MDM Certificate

Certificate (PFX Format): C:\MDMCertificates\Setup SRV\MDMVendor2014-2

Certificate password: •••••••

□ I do not have a PFX Certificate

Generate PFX Certificate for Parallels 2X MDM

Certificate:

Root Certificate:

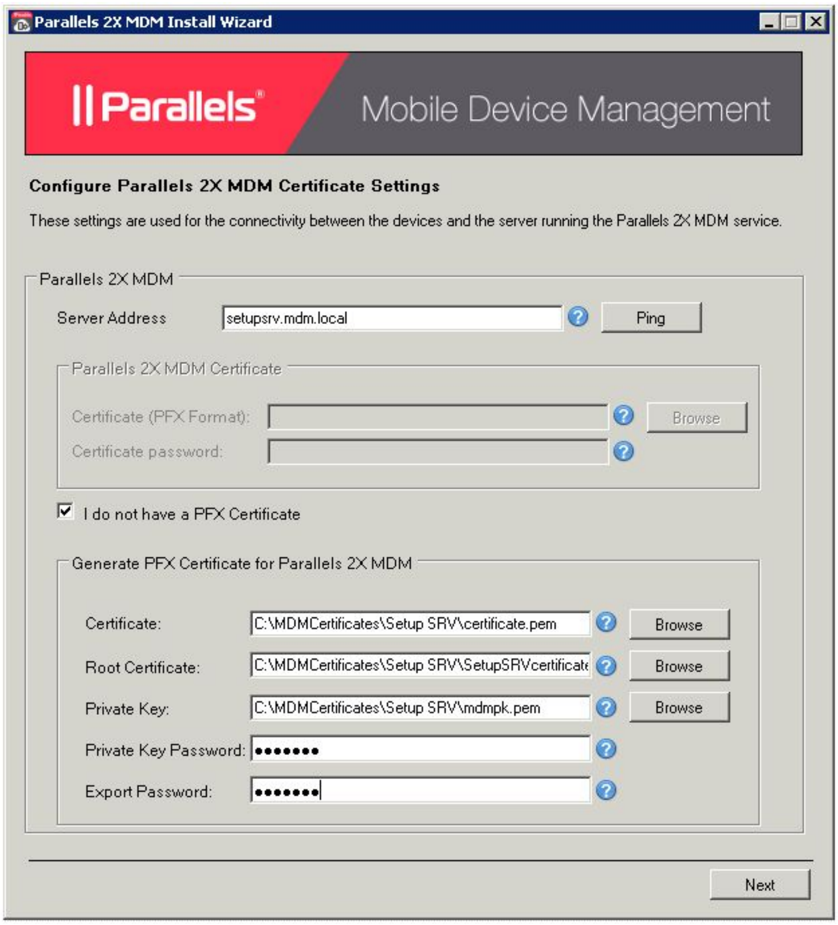
Private Key:

Private Key Password:

Export Password:

1. In this part of the installation and configuration wizard fill in the following fields:
    - **Server Address:** Enter your MDM server FQDN here (Example - mdm.company.com).

   If you already have a PFX certificate available, proceed to configure the below:
    - **Certificate (PFX Format):** Define the path where the PFX file is stored.
    - **Certificate password:** Enter the certificate password.



Parallels 2X MDM Install Wizard

Configure Parallels 2X MDM Certificate Settings

These settings are used for the connectivity between the devices and the server running the Parallels 2X MDM service.

Parallels 2X MDM

Server Address: setupsrv.mdm.local

Parallels 2X MDM Certificate

Certificate (PFX Format):

Certificate password:

☑ I do not have a PFX Certificate

Generate PFX Certificate for Parallels 2X MDM

Certificate: C:\MDMCertificates\Setup SRV\certificate.pem

Root Certificate: C:\MDMCertificates\Setup SRV\SetupSRVcertificate

Private Key: C:\MDMCertificates\Setup SRV\mdmpk.pem

Private Key Password: •••••••

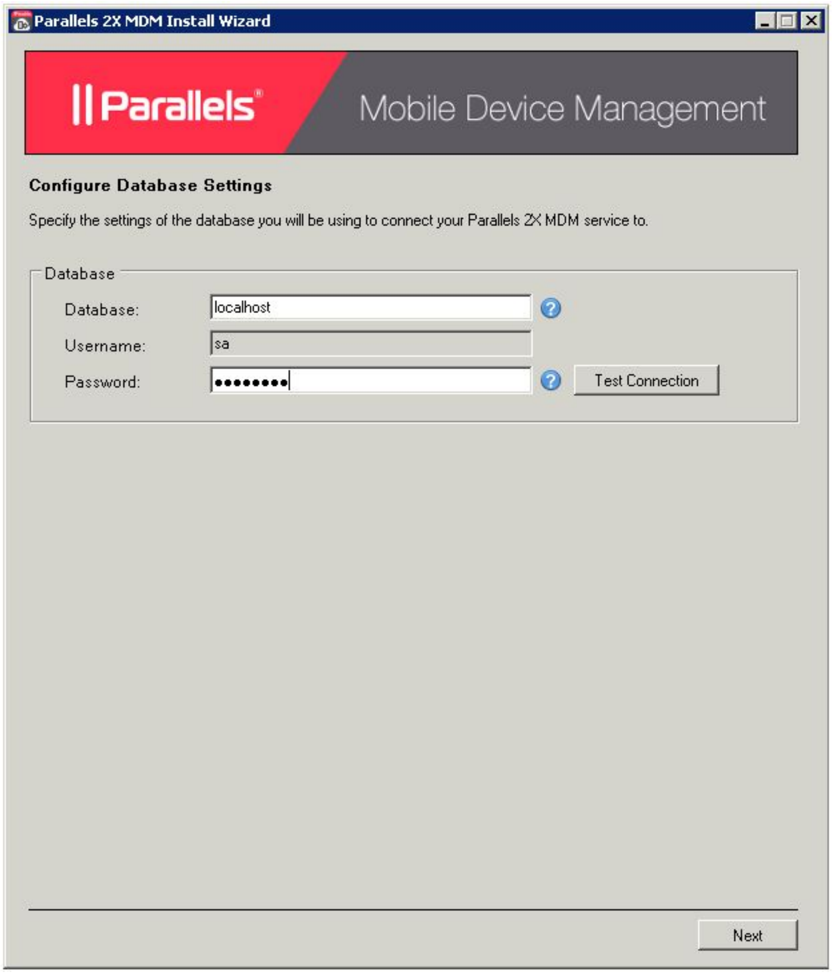
Export Password: •••••••

If you require to generate a PFX certificate from scratch, enable the 'I do not have a PFX Certificate' checkbox and further configure:

- **Certificate:** Select your SSL certificate obtained by a Certificate Authority (CA) company. The file should end with a .pem extension*.
- **Root Certificate:** Select the Root Certificate file obtained by a Certificate Authority (CA) company. The file should end with a .cer extension.
- **Private Key:**Select the Private Key you were provided with by your Certificate Authority (CA) company. The file should end with a .pem extension.
- **Private Key Password:** Insert the password used during the generation of your Private Key.
- **Export Password:** The password to be used for the new PFX file

*** Signed digital certificate must support wildcards.**

Database Configuration



Configure Database Settings

Specify the settings of the database you will be using to connect your Parallels 2X MDM service to.

Database

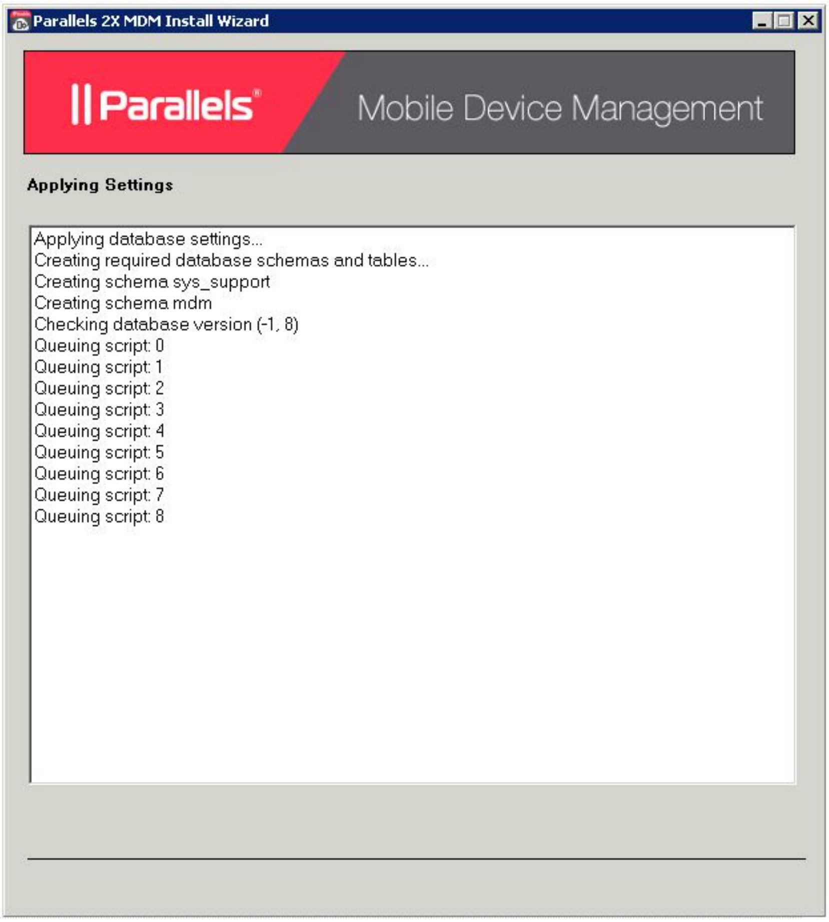
Database: localhost

Username: sa

Password: ••••••••

2. In the Database Settings dialog window, fill in the following:
    - **Location:** Specify the IP address of the machine hosting your SQL database. If the database is located on the same machine you are installing Mobile Device Management, you can also use localhost.
    - **Password:** Fill in the password of your SA database account.

Note: Click ‘Test Connection’ to confirm the MDM server is able to connect to the configured database.

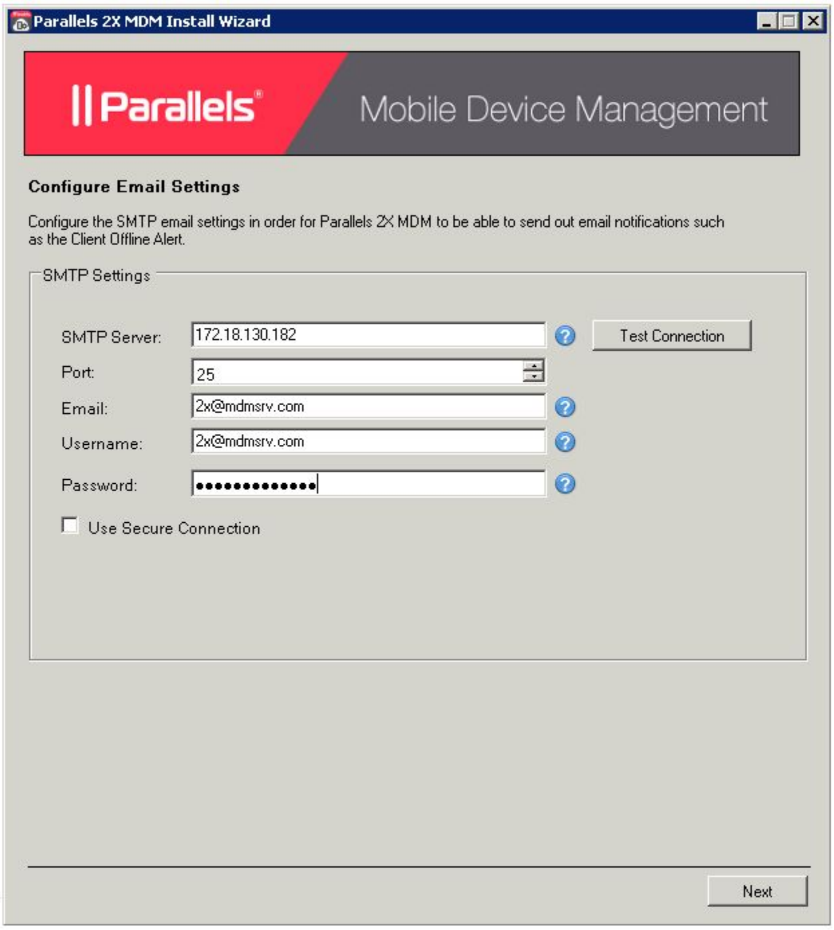


Applying Settings

```
Applying database settings...
Creating required database schemas and tables...
Creating schema sys_support
Creating schema mdm
Checking database version (-1, 8)
Queuing script: 0
Queuing script: 1
Queuing script: 2
Queuing script: 3
Queuing script: 4
Queuing script: 5
Queuing script: 6
Queuing script: 7
Queuing script: 8
```

3. During this process the installer will start performing the following operations:
    - Generate the PFX certificate.
    - Create the database users.

Email Configuration



Parallels 2X MDM Install Wizard

Configure Email Settings

Configure the SMTP email settings in order for Parallels 2X MDM to be able to send out email notifications such as the Client Offline Alert.

SMTP Settings

SMTP Server: 172.18.130.182

Port: 25

Email: 2x@mdmsrv.com

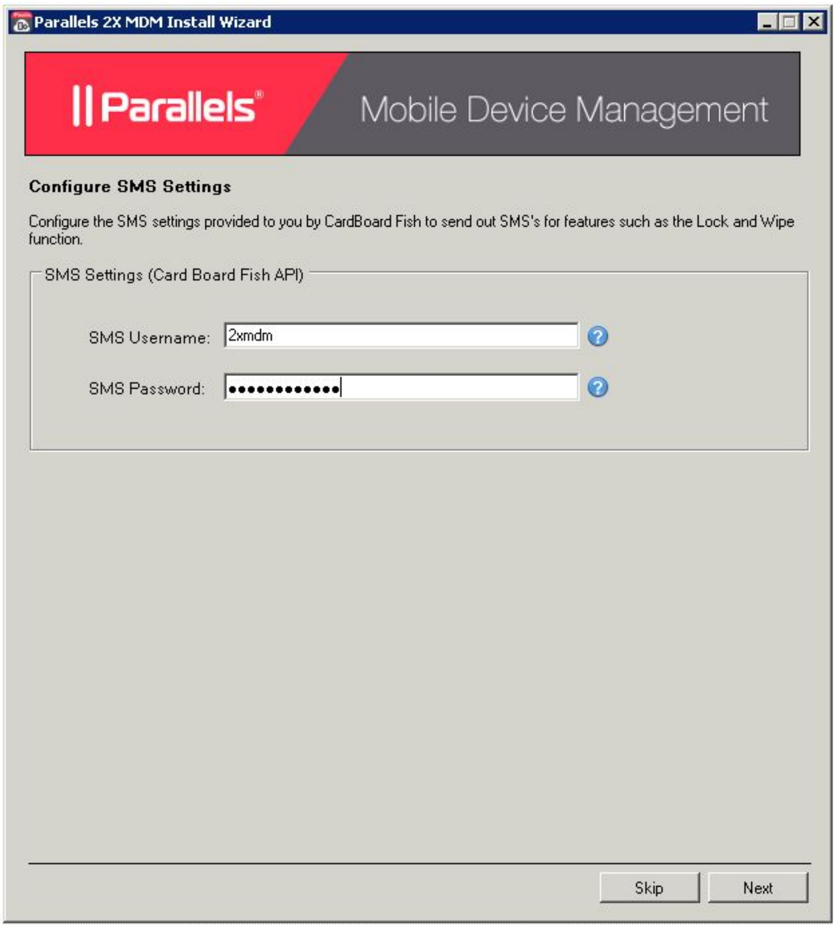
Username: 2x@mdmsrv.com

Password: ••••••••••••••

□ Use Secure Connection

4. Next, you shall be requested to fill in the Email Settings to be used by MDM.
    - **SMTP Server:** Fill in the SMTP server to be used.
    - **Port:** Fill in the port number to be used for sending out emails.
    - **Email:** Fill in the email address that you want to be shown when emails are sent out.
    - **Username:** Fill in the username to be used if the mail server requires authentication.
    - **Password:** Password for the username provided if the mail server requires authentication.
    - **Use Secure Connection:** Tick this box if your SMTP server requires an SSL connection.

SMS Settings Configuration



Configure SMS Settings

Configure the SMS settings provided to you by CardBoard Fish to send out SMS's for features such as the Lock and Wipe function.

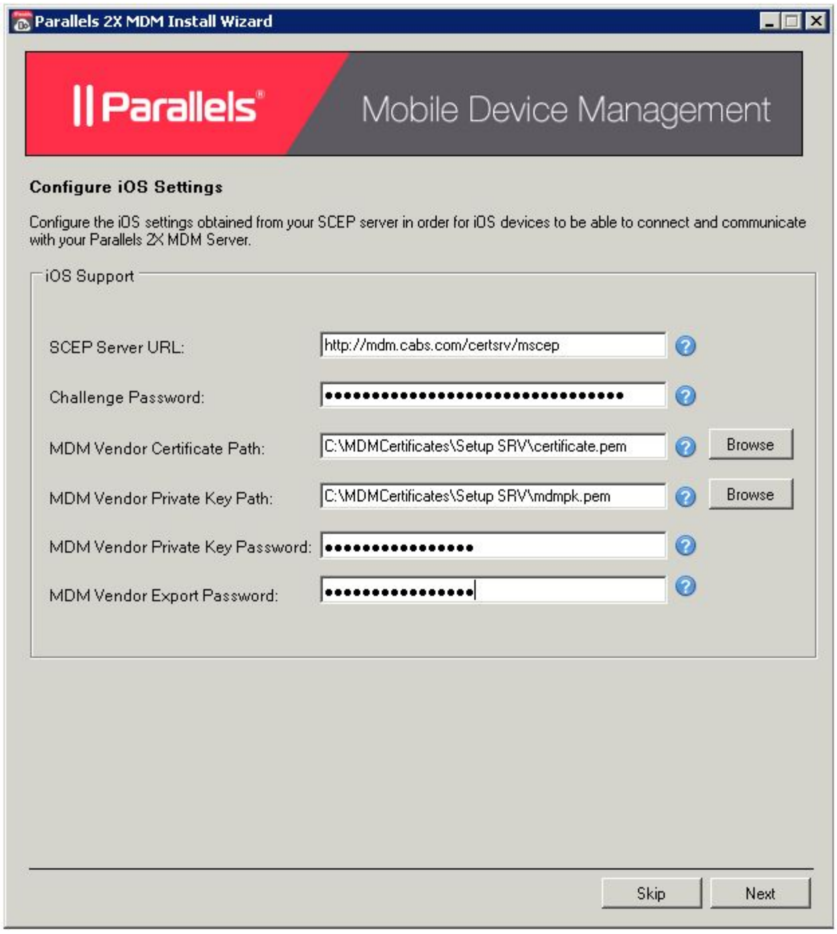
SMS Settings (Card Board Fish API)

SMS Username: 2xmdm

SMS Password: •••••••••••••

5. In the next page you are requested to fill in the SMS Settings provided to you by CardBoard Fish. CardBoardFish is an online service that provides, high quality, reliable, and low cost SMS delivery services. This step is necessary in order to be able to send out SMS's for features such as the Lock & Wipe function:
   - **SMS Username:** Fill in the username obtained from CardBoard Fish.
   - **SMS Password**: Fill in the password for your CardBoard Fish account.

iOS Settings Configuration



Configure iOS Settings

Configure the iOS settings obtained from your SCEP server in order for iOS devices to be able to connect and communicate with your Parallels 2X MDM Server.

iOS Support

SCEP Server URL: http://mdm.cabs.com/certsrv/mscep

Challenge Password: ••••••••••••••••••••••••••••••••

MDM Vendor Certificate Path: C:\MDMCertificates\Setup SRV\certificate.pem

MDM Vendor Private Key Path: C:\MDMCertificates\Setup SRV\mdmpk.pem

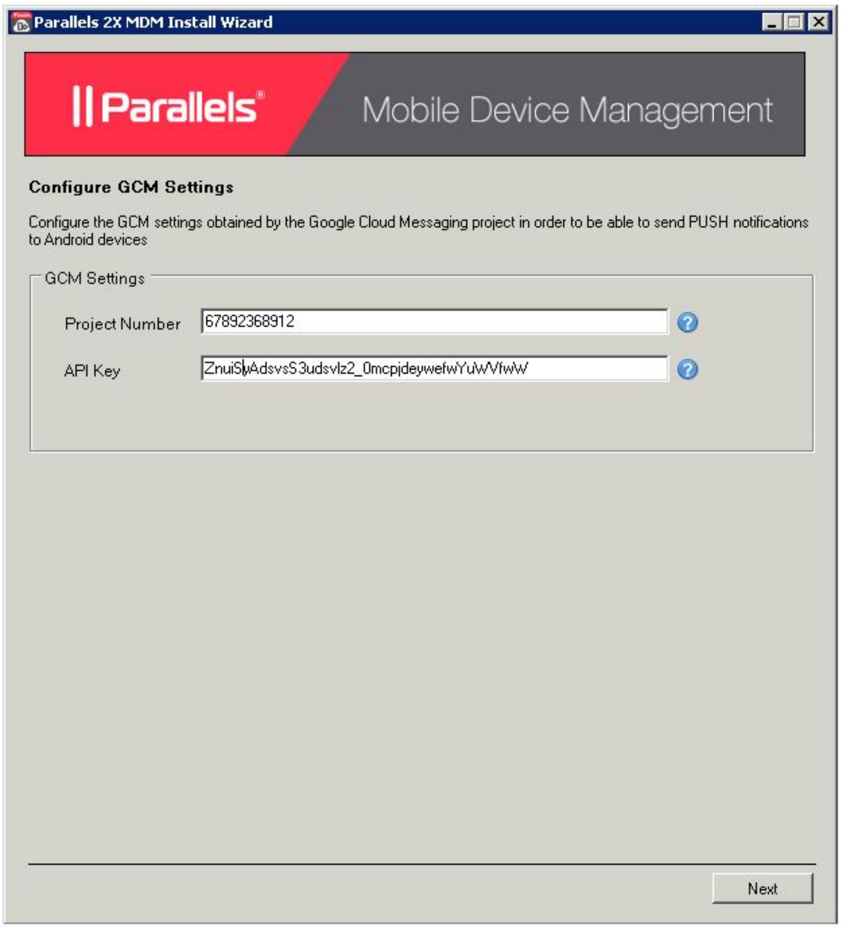
MDM Vendor Private Key Password: ••••••••••••••••

MDM Vendor Export Password: ••••••••••••••••

6. Next, you will be asked to fill in the iOS settings obtained from your SCEP server in order for iOS devices to be able to connect and communicate with your MDM server:
   - **SCEP Server URL:** The URL pointing to your certificate SCEP server.
   - **Challenge Password:** Input the challenge password generated by your certificate SCEP server.
   - **MDM Vendor Certificate Path:** Select the path to the certificate provided to you by Apple.
   - **MDM Vendor Private Key Path:** Select the path to the private key previously generated to obtain the certificate by Apple.
   - **MDM Vendor Private Key Password:** Insert the password of your Private Key.
   - **MDM Vendor Export Password:** Define the password for the Apple certificate which will be generated.

*** Signed digital certificate must support wildcards**

Google Messaging Settings



Configure GCM Settings

Configure the GCM settings obtained by the Google Cloud Messaging project in order to be able to send PUSH notifications to Android devices

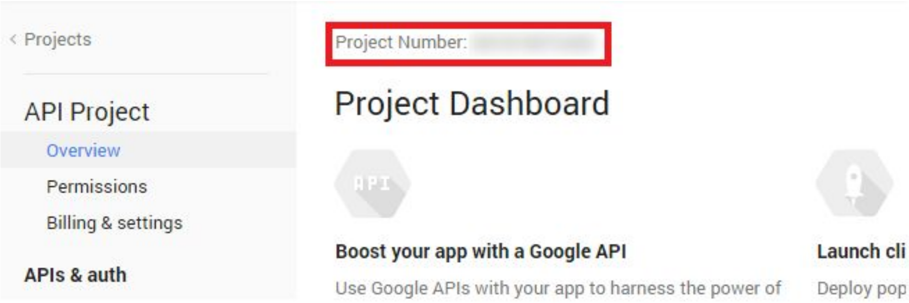
GCM Settings

Project Number: 67892368912

API Key: ZnuiSyAdsvsS3udsvlz2_0mcpjdeywefwYuWVfwW

7. In the next dialog window you are asked to fill in the GCM settings obtained from your Google Cloud Messaging project. This is used to send PUSH notifications to Android devices.
   - **Project Number/ GCM API Key:** Insert the Project Number obtained by the Google Cloud Messaging project.
   - **API Key/ GCM Project Id:** Insert the API Key obtained by the Google Cloud Messaging project.

Note: The **GCM Project Id** is also known as the **Project Number**. Extract this number from the Google Developers Console > API Project > Overview > **Project Number** (Top Left Corner) as shown below.

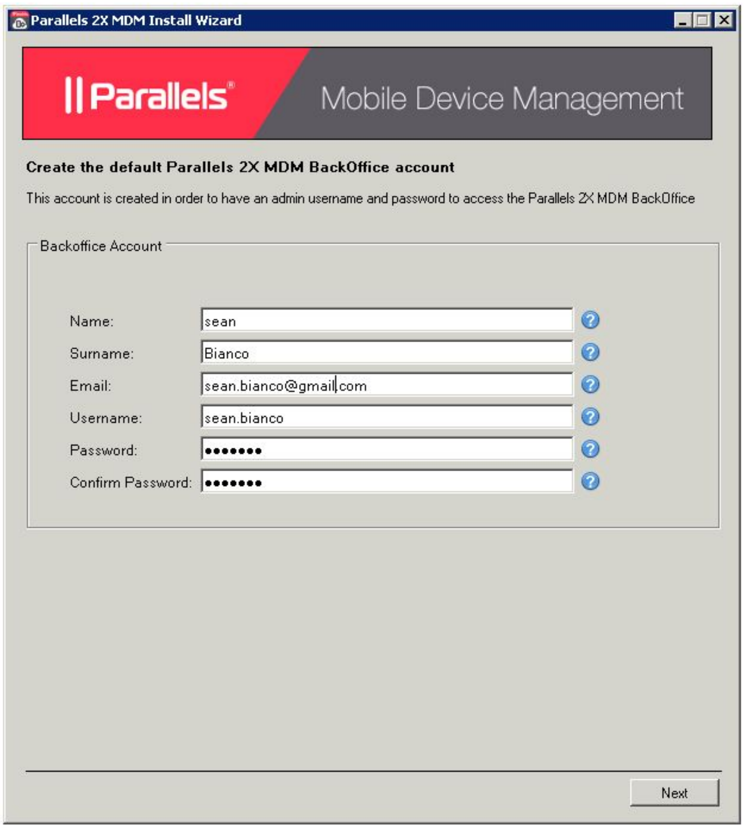


Project Number: [redacted]

Project Dashboard

API
Boost your app with a Google API
Use Google APIs with your app to harness the power of
Launch cli
Deploy pop

BackOffice Account Configuration



Create the default Parallels 2X MDM BackOffice account

This account is created in order to have an admin username and password to access the Parallels 2X MDM BackOffice

Backoffice Account

Name: sean

Surname: Bianco

Email: sean.bianco@gmail.com

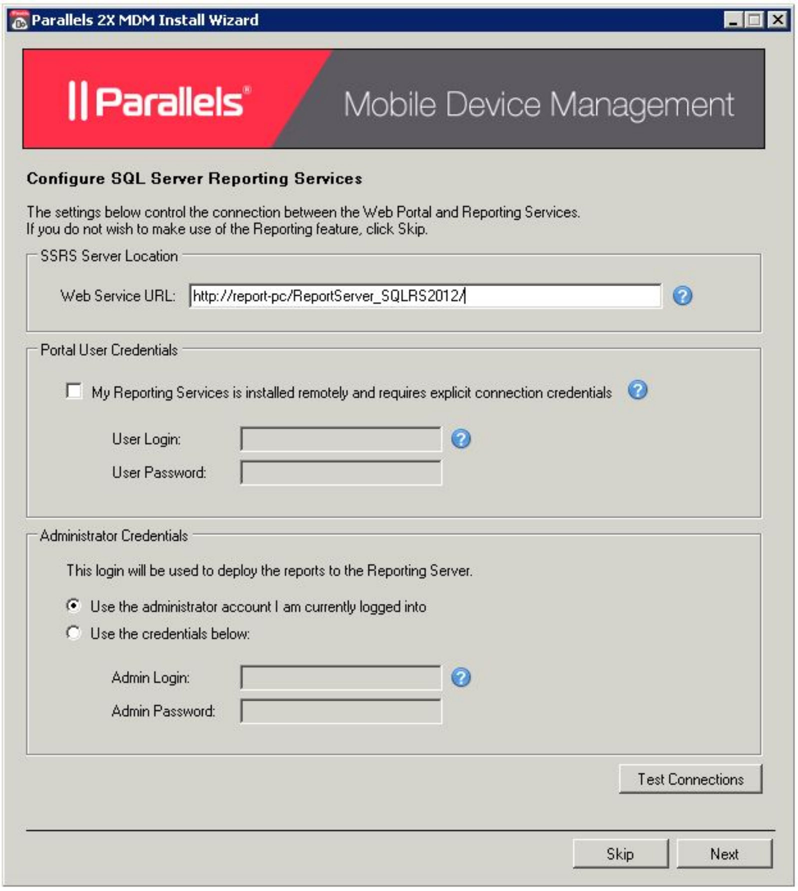
Username: sean.bianco

Password: •••••••

Confirm Password: •••••••

8. After that, you will be asked to fill out the details for the admin account to access the Mobile Device Management BackOffice.
    - **Name, Surname:** Insert the administrator’s name and surname.
    - **Email:** Insert the administrator’s email address.
    - **Username:** The username that will be used by the admin to log into BackOffice.
    - **Password:** The password that will be used by the administrator to log into BackOffice.
    - **Confirm Password:** Re-insert the password to be used by the admin to log into Back Office.

SQL Server Reporting Service Configuration



Configure SQL Server Reporting Services

The settings below control the connection between the Web Portal and Reporting Services.
If you do not wish to make use of the Reporting feature, click Skip.

SSRS Server Location

Web Service URL: http://report-pc/ReportServer_SQLRS2012/

Portal User Credentials

□ My Reporting Services is installed remotely and requires explicit connection credentials

User Login:

User Password:

Administrator Credentials

This login will be used to deploy the reports to the Reporting Server.

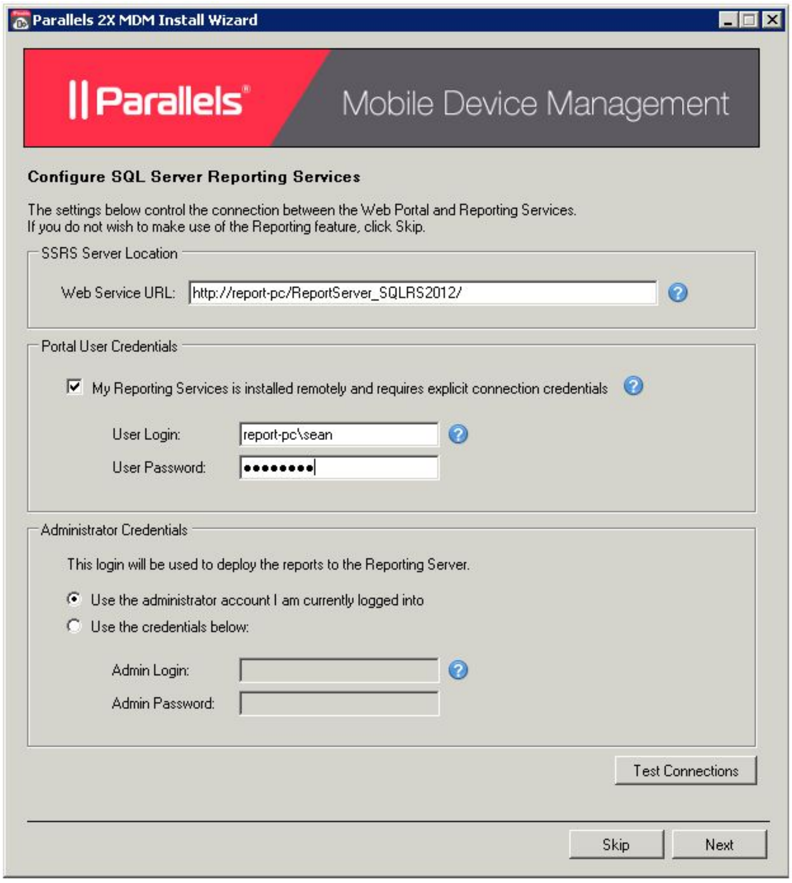
● Use the administrator account I am currently logged into

○ Use the credentials below:

Admin Login:

Admin Password:

9. Next, you will be asked to enter SSRS settings required by setup to deploy SSRS configuration for MDM and also generate reports. Upon completion click ‘Next’ to initialise final setup.
    - **Web Service URL**: The URL pointing toward your Reporting Services end-point.



Configure SQL Server Reporting Services

The settings below control the connection between the Web Portal and Reporting Services.
If you do not wish to make use of the Reporting feature, click Skip.

SSRS Server Location

Web Service URL: http://report-pc/ReportServer_SQLRS2012/

Portal User Credentials

☑ My Reporting Services is installed remotely and requires explicit connection credentials

User Login: report-pc\sean

User Password: ••••••••

Administrator Credentials

This login will be used to deploy the reports to the Reporting Server.

● Use the administrator account I am currently logged into

○ Use the credentials below:

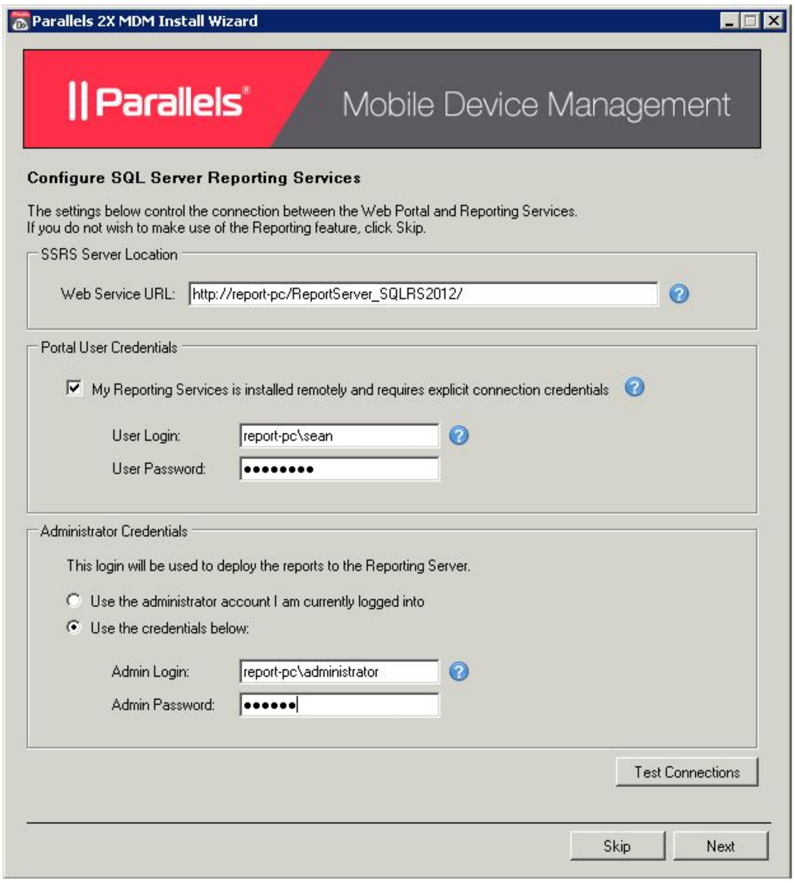
Admin Login:

Admin Password:

Portal User credentials are required to authenticate connections from the MDM portal when generating reports. If the SQL Server Reporting Services (SSRS) is not installed on the same server that MDM setup is running on, enable the “Portal User Credentials” checkbox and configure the below:

- **User Login and Password:** Enter Windows credentials that are configured in SSRS with browser permissions.

Note: If Setup is running on the same machine SSRS will automatically be configured to authenticate credentials from the MDM portal.



Parallels 2X MDM Install Wizard

Configure SQL Server Reporting Services

The settings below control the connection between the Web Portal and Reporting Services.
If you do not wish to make use of the Reporting feature, click Skip.

SSRS Server Location

Web Service URL: http://report-pc/ReportServer_SQLRS2012/

Portal User Credentials

☑ My Reporting Services is installed remotely and requires explicit connection credentials

User Login: report-pc\sean

User Password: ••••••••

Administrator Credentials

This login will be used to deploy the reports to the Reporting Server.

○ Use the administrator account I am currently logged into

● Use the credentials below:

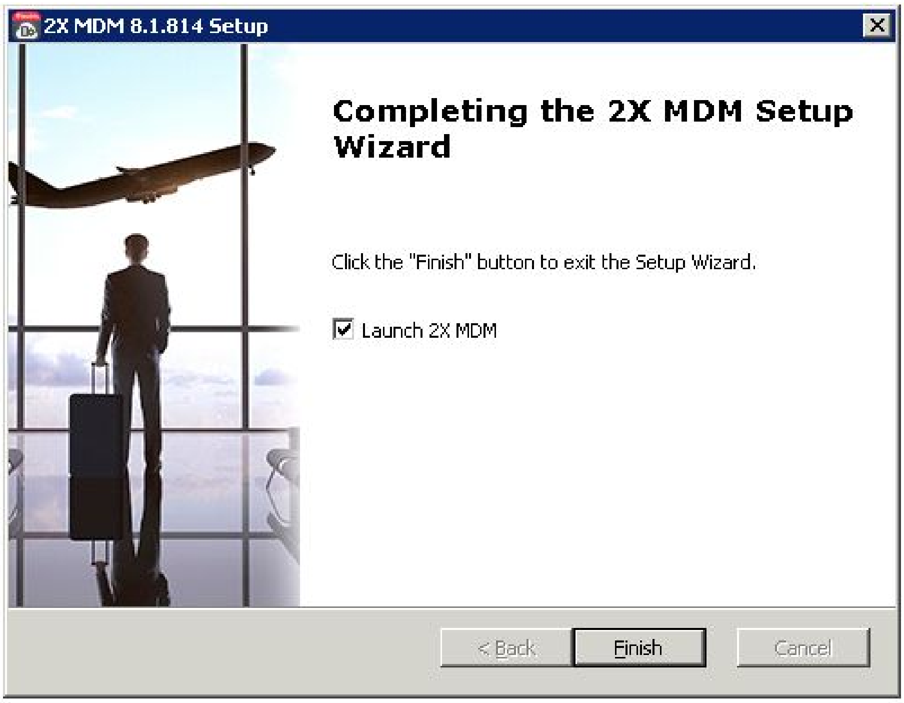
Admin Login: report-pc\administrator

Admin Password: ••••••

Administrator credentials are required to deploy MDM report configuration to SSRS. If the administrator you are currently logged in with does not have administrator privileges and content management rights in SSRS, enable “Use the credentials below”:

- **Administrator Login Name and Password:** Enter Windows account credentials configured with administrator privileges and content management rights in SSRS.

Note: If setup is running on the same machine as SSRS, administrator rights are automatically authenticated.



2X MDM 8.1.814 Setup

Completing the 2X MDM Setup Wizard

Click the "Finish" button to exit the Setup Wizard.

☑ Launch 2X MDM

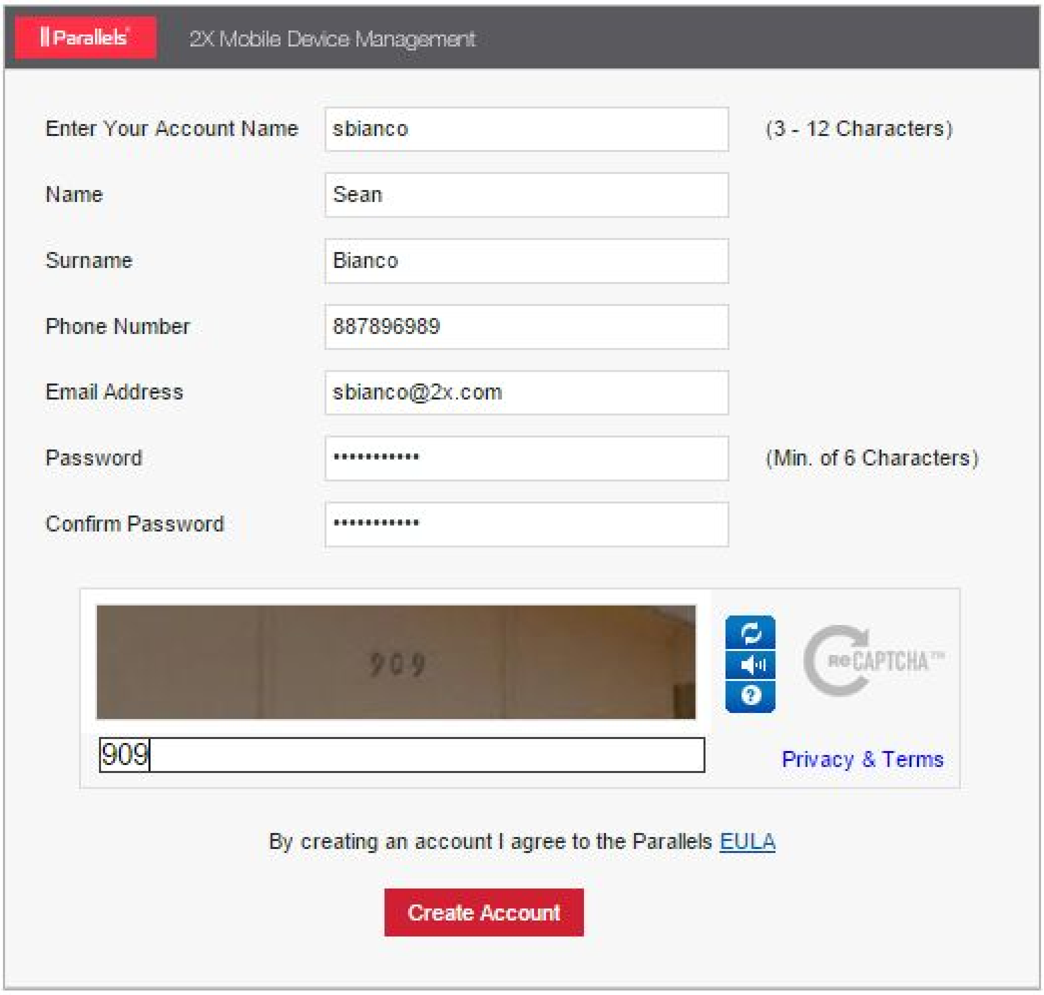
10. Finalise the installation by clicking finish and optionally select to launch Mobile Device Management upon completion.

Creating the MDM Accounts

Introduction

After completing the file and the server configuration you will need to create an account on which your devices will be registered on.

Setting Up Your Account



Enter Your Account Name: sbianco (3 - 12 Characters)

Name: Sean

Surname: Bianco

Phone Number: 887896989

Email Address: sbianco@2x.com

Password: ••••••••••• (Min. of 6 Characters)

Confirm Password: •••••••••••

909

By creating an account I agree to the Parallels EULA

1. You may now set up your Mobile Device Management account:

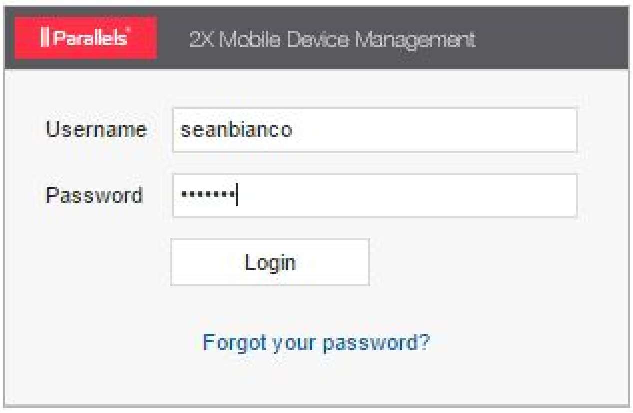
    1. Go to **https://<Your MDM Domain>/signup**
    2. Specify an account name. You will use this account name to enroll mobile devices and to log in to your On Premise MDM portal.
    3. Specify your name and email.
    4. Specify and confirm a password (to login to the account).
    5. Read the Terms of Service document.
    6. Enter the CAPTCHA and click Sign up.
    7. Activate your account by clicking on the link included in the welcome email sent to you.
    8. You can now logon to the portal by specifying your account name, email and password at: **https://<Your MDM Domain>/Admin/Login/LogOnActivate**

2. You are now able to access the Mobile Device Management administration pages through the following URL's:

    - **https://<Your MDM Domain>/signup** - Used to create accounts in order to further assign and manage your devices.
    - **https://<Your MDM Domain>** - Used to log into your account, assign devices and further manage them.
    - **https://<Your MDM Domain>/backoffice** - Used to log into the backend of the system and manage the accounts and change system configuration settings.

Accessing BackOffice

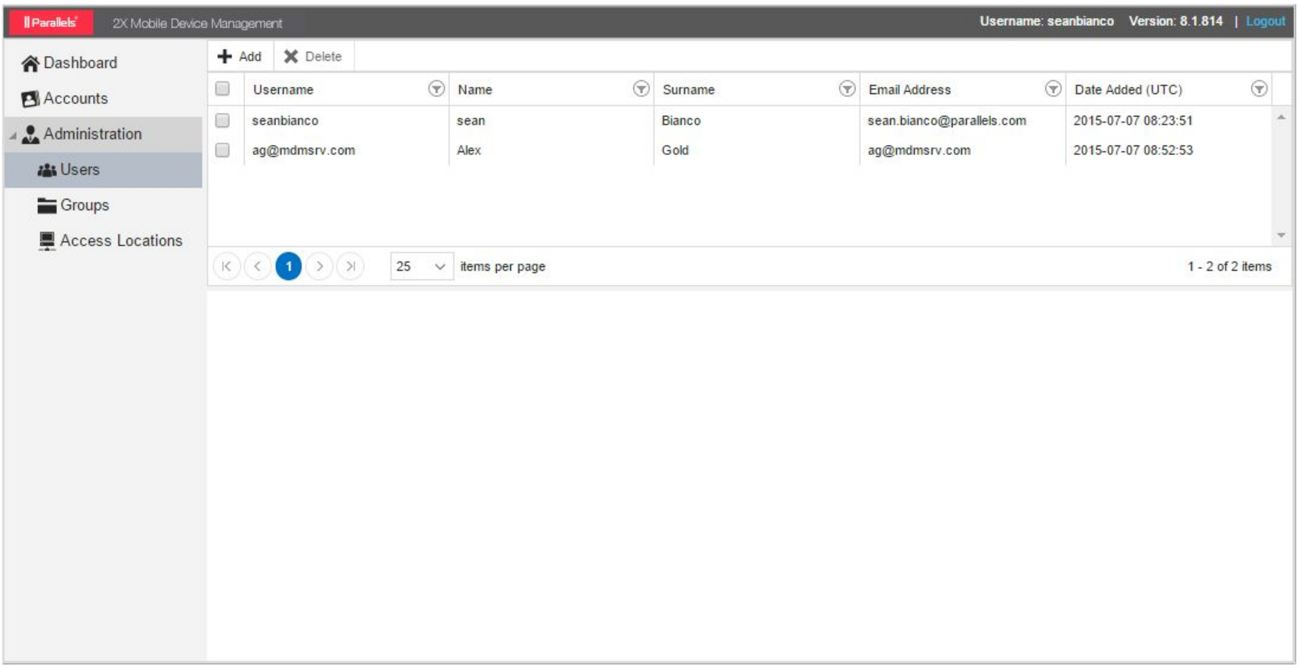
Accessing and Configuring Your BackOffice



Username: seanbianco

Password: •••••••

1. To access the BackOffice of your MDM system, you need to access: **https://<Your MDM Domain>/backoffice**
2. Fill in the Username and Password provided previously in step 8 of chapter 4 (Configuring Mobile Device Manager) to access your BackOffice.



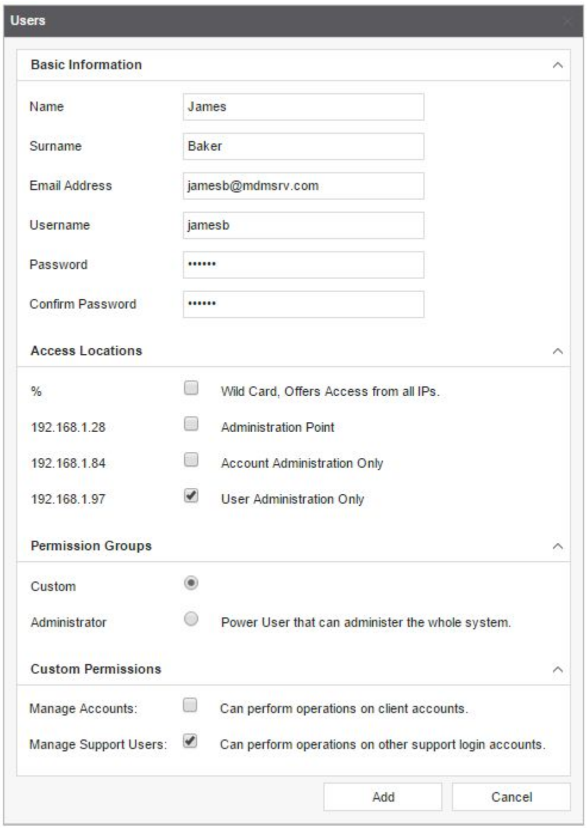
Username: seanbianco Version: 8.1.814

Username	Name	Surname	Email Address	Date Added (UTC)
seanbianco	sean	Bianco	sean.bianco@parallels.com	2015-07-07 08:23:51
ag@mdmsrv.com	Alex	Gold	ag@mdmsrv.com	2015-07-07 08:52:53

25 items per page — 1 - 2 of 2 items

3. From the BackOffice you can add additional users, assign them permissions to perform the actions below and even specify IP's that BackOffice access is allowed from per user:
   - **Account -** You can view, disable, enable, delete or administer existing accounts created through the https://<Your MDM Domain>/signup
   - **Administration -** You can view, add and delete users and groups which can access this Mobile Device Management BackOffice Portal.

Add a BackOffice User



Users

Basic Information

Name	James
Surname	Baker
Email Address	jamesb@mdmsrv.com
Username	jamesb
Password	••••••
Confirm Password	••••••

Access Locations

%	□	Wild Card, Offers Access from all IPs.
192.168.1.28	□	Administration Point
192.168.1.84	□	Account Administration Only
192.168.1.97	☑	User Administration Only

Permission Groups

Custom	●	
Administrator	○	Power User that can administer the whole system.

Custom Permissions

Manage Accounts:	□	Can perform operations on client accounts.
Manage Support Users:	☑	Can perform operations on other support login accounts.

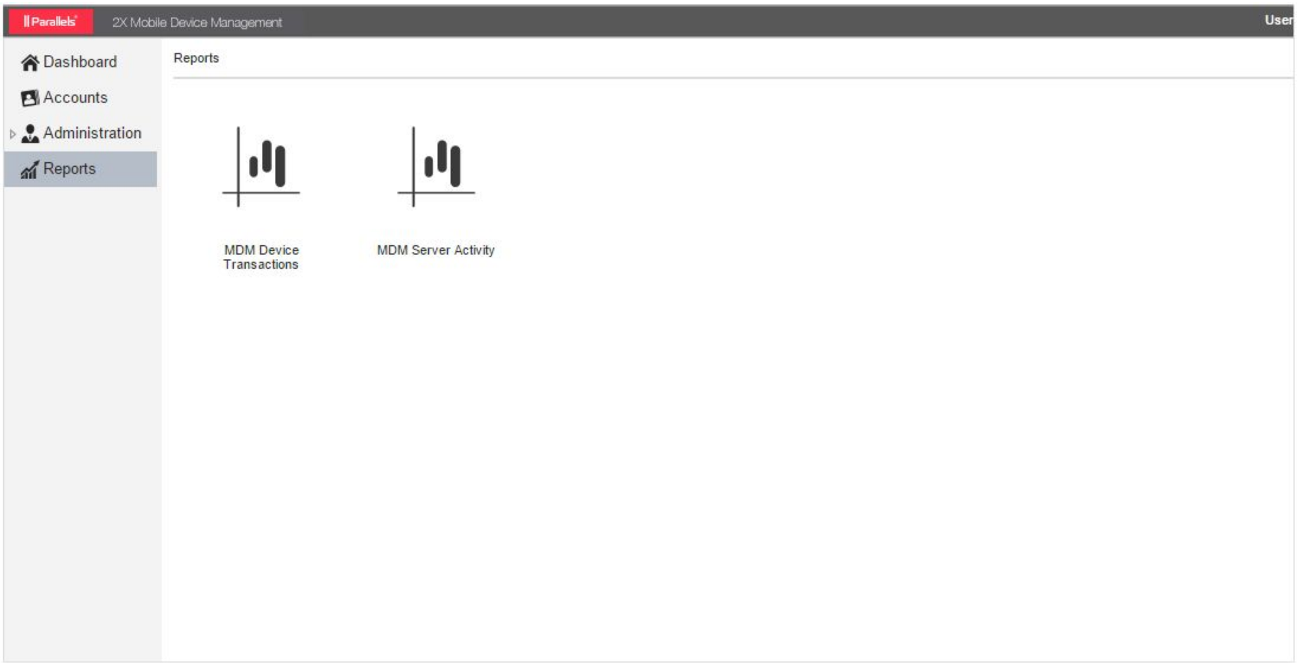
To add a user and assign the permissions discussed in the step 3, click “Add” and configure the below:

- **Basic Information**: Fill in user details such as name, surname, email address and the username and password used to access BackOffice.
- **Access Locations**: Select IP’s (added from ‘Access Locations’) the user is able to access BackOffice from or allow access from all.
- **Permission Groups**: Select the Group (added from the ‘Groups’) this user will inherit permissions from.
- **Custom Permissions**: Enable the Custom permissions below to the user:
  - **Manage Accounts**: User can view, disable, enable, delete or administer existing accounts.
  - **Manage Support Users**: User can view, add and delete users and groups which can access this Mobile Device Management BackOffice Portal and even specify the Access Location IP’s.

In addition, ‘Dashboard’ displays the total number of activated accounts, inactive accounts, devices currently connected and devices currently registered on the system, ‘Groups’ allows you to add new or already existing groups and from ‘Access Locations’, specify IP’s that BackOffice access is allowed from.

Note: Groups and Access Locations specified will show up on new users configuration window.

Reports



The Parallels 2X backoffice provides reports via the reports node:

- **MDM Device Transactions** - this report provides an overview of activity between the MDM server and devices on all accounts including the ID or unique command identifier, the textual description of the command, the amount of these commands sent, the commands which were processed by the device and the overall percentage of pushed vs serviced commands.
- **MDM Server Activity** - presents inventorial data about devices connected to the MDM server from all accounts. Information produced in this report include total active devices by operating system, total active accounts, number of new signups, account signups by source (Play Store, Website etc.), new accounts activity (number of accounts categorized by number of devices enrolled), total active devices by operating system version, total active devices by client version.

Each report can also be exported and downloaded in the following formats: CSV, PDF, MHTML, Excel, Word and TIFF.

Note: The Reporting node requires that SSRS is configured from the Server User Interface > Reports.

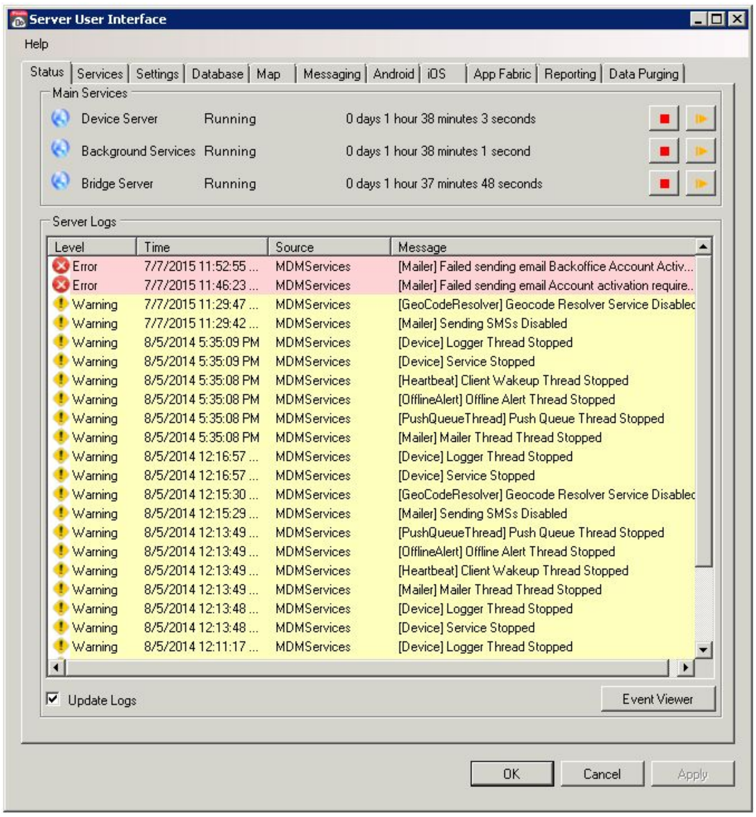
Managing the Server User Interface

The Parallels 2X MDM On Premise Edition installation has successfully completed, MDM accounts created and devices connected.

The backend of Parallels 2X MDM, also known as the 'Server User Interface' consists of 10 tabs used to monitor, maintain and update MDM configuration and processes configured during the installation process including a few additional options.

Access the Server User Interface from the server Parallels 2X MDM is installed on > click the 2X MDM Program Group > click ‘2X MDM Server'.

1. Status Tab



Device Server Running 0 days 1 hour 38 minutes 3 seconds

Background Services Running 0 days 1 hour 38 minutes 1 second

Bridge Server Running 0 days 1 hour 37 minutes 48 seconds

Level	Time	Source	Message
Error	7/7/2015 11:52:55 ...	MDMServices	[Mailer] Failed sending email Backoffice Account Activ...
Error	7/7/2015 11:46:23 ...	MDMServices	[Mailer] Failed sending email Account activation require..
Warning	7/7/2015 11:29:47 ...	MDMServices	[GeoCodeResolver] Geocode Resolver Service Disablec
Warning	7/7/2015 11:29:42 ...	MDMServices	[Mailer] Sending SMSs Disabled
Warning	8/5/2014 5:35:09 PM	MDMServices	[Device] Logger Thread Stopped
Warning	8/5/2014 5:35:09 PM	MDMServices	[Device] Service Stopped
Warning	8/5/2014 5:35:08 PM	MDMServices	[Heartbeat] Client Wakeup Thread Stopped
Warning	8/5/2014 5:35:08 PM	MDMServices	[OfflineAlert] Offline Alert Thread Stopped
Warning	8/5/2014 5:35:08 PM	MDMServices	[PushQueueThread] Push Queue Thread Stopped
Warning	8/5/2014 5:35:08 PM	MDMServices	[Mailer] Mailer Thread Thread Stopped
Warning	8/5/2014 12:16:57 ...	MDMServices	[Device] Logger Thread Stopped
Warning	8/5/2014 12:16:57 ...	MDMServices	[Device] Service Stopped
Warning	8/5/2014 12:15:30 ...	MDMServices	[GeoCodeResolver] Geocode Resolver Service Disablec
Warning	8/5/2014 12:15:29 ...	MDMServices	[Mailer] Sending SMSs Disabled
Warning	8/5/2014 12:13:49 ...	MDMServices	[PushQueueThread] Push Queue Thread Stopped
Warning	8/5/2014 12:13:49 ...	MDMServices	[OfflineAlert] Offline Alert Thread Stopped
Warning	8/5/2014 12:13:49 ...	MDMServices	[Heartbeat] Client Wakeup Thread Stopped
Warning	8/5/2014 12:13:49 ...	MDMServices	[Mailer] Mailer Thread Thread Stopped
Warning	8/5/2014 12:13:48 ...	MDMServices	[Device] Logger Thread Stopped
Warning	8/5/2014 12:13:48 ...	MDMServices	[Device] Service Stopped
Warning	8/5/2014 12:11:17 ...	MDMServices	[Device] Logger Thread Stopped

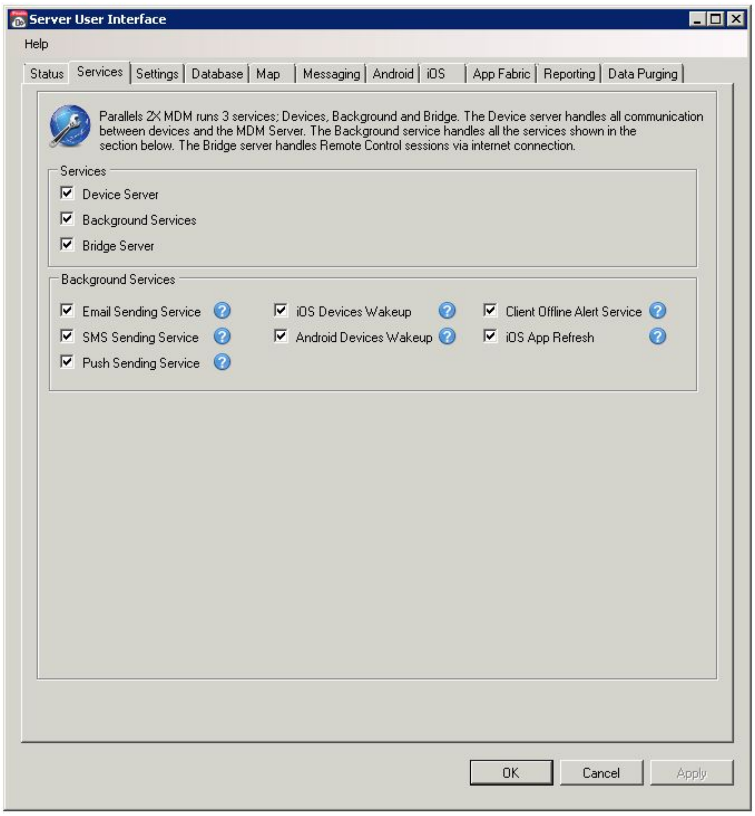
☑ Update Logs

The Status tab lists the Parallels 2X MDM services, how long they have been running for and also allows for each individual service to be stopped and then started again:

- **Device Server:** Handles all communication between devices and the MDM Server.
- **Background Services:** Handles tasks which include email notification, SMS messaging, Push notifications etc.(Review 2. Status Tab for full description)
- **Bridge Server:** Handles Remote Control sessions via internet connection

The server logs listed are extracted from the Windows Event logs and are useful for investigating behavior on the system.

2. Services Tab



Parallels 2X MDM runs 3 services; Devices, Background and Bridge. The Device server handles all communication between devices and the MDM Server. The Background service handles all the services shown in the section below. The Bridge server handles Remote Control sessions via internet connection.

Services

☑ Device Server
☑ Background Services
☑ Bridge Server

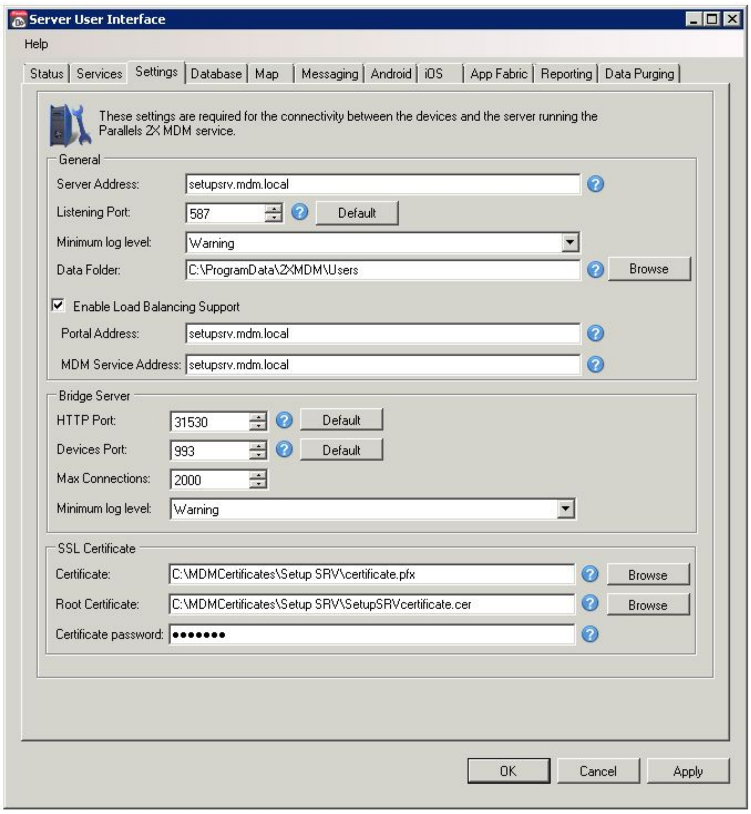
Background Services

☑ Email Sending Service
☑ SMS Sending Service
☑ Push Sending Service
☑ iOS Devices Wakeup
☑ Android Devices Wakeup
☑ Client Offline Alert Service
☑ iOS App Refresh

From this tab, select to disable any of the services described in the “Status Tab”. In addition you can also disable any of the background tasks performed by Parallels 2X MDM Background Services below:

- **Email Sending Service**: Enables the mailer thread that sends out Email notifications
- **SMS Sending Service**: Enables sending of SMS messages to devices
- **Push Sending Service**: Enables sending of Push notifications to devices
- **iOS/ Android Device Wakeup**: Sends push notifications to Android/ iOS devices to recreate a new session when the current session timeout is reached
- **Client Offline Alert Service**: Notifies administrators when a device has reached its offline alert configuration
- **iOS App Refresh**: Performs daily checks of applications iOS devices must install and uninstall since the last check was peformed

3. Settings Tab


Server User Interface
Help
Status | Services | Settings | Database | Map | Messaging | Android | iOS | App Fabric | Reporting | Data Purging
Default
Browse
OK
Cancel
Apply

These settings are required for the connectivity between the devices and the server running the Parallels 2X MDM service.

General
Server Address: setupsrv.mdm.local
Listening Port: 587
Minimum log level: Warning
Data Folder: C:\ProgramData\2XMDM\Users
☑ Enable Load Balancing Support
Portal Address: setupsrv.mdm.local
MDM Service Address: setupsrv.mdm.local

Bridge Server
HTTP Port: 31530
Devices Port: 993
Max Connections: 2000
Minimum log level: Warning

SSL Certificate
Certificate: C:\MDMCertificates\Setup SRV\certificate.pfx
Root Certificate: C:\MDMCertificates\Setup SRV\SetupSRVcertificate.cer
Certificate password: •••••••

The settings tab consists of configuration options required for connectivity between the devices and the server running the Parallels 2X MDM Service. The server address and certificate settings configured during the installation process may also be updated from here.

From the **General** section you can adjust the options below:

- **Server Address**: The MDM server FQDN (Example - mdm.company.com).
- **Listening Port**: The port used for devices to connect to the MDM server
- **Minimum log level**: Set the level of logging displayed on the Status tab
- **Data Folder**: The folder where MDM account data is stored

Optionally **Enable Load Balancing Support** to specify the URL used to access the MDM portal and the Subdomain URL that devices connect to:

- **Portal Address**: The URL pointing toward the server running the Parallels 2X MDM Service
- **MDM Service Address**: The subdomain URL pointing toward the server running the Parallels 2X MDM service

From the **Bridge Server** section, adjust the bridge server options below:

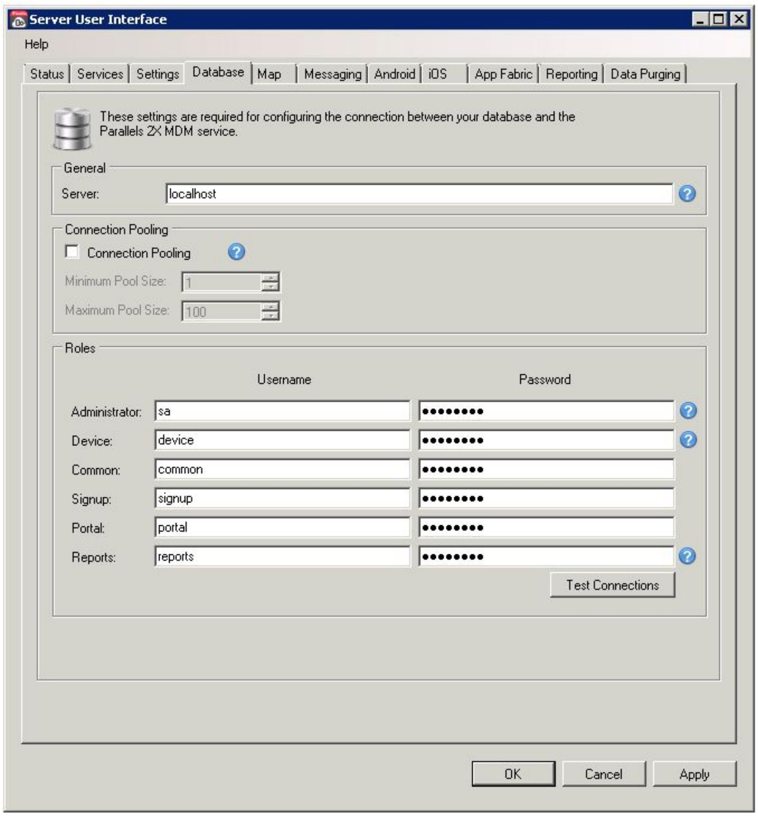
- **HTTP Port**: The port the browser connects through when using Remote Control
- **Devices Port**: The port devices connect through when Remote Control is enabled
- **Max Connections**: The number of Remote Control sessions allowed simultaneously
- **Minimum log level**: Set the level of logging displayed on the Status tab

From the **SSL Certificate** section, you can adjust the certificate settings configured during the installation process:

- **Certificate (PFX Format):** Define the path where the PFX file obtained by a Certificate Authority (CA) is stored

- **Root Certificate:** Select the Root Certificate file obtained by a Certificate Authority (CA) company. The file should end with a .cer extension
- **Certificate password:** Enter the certificate password

4. Database Tab



Server User Interface
Help
Status | Services | Settings | Database | Map | Messaging | Android | iOS | App Fabric | Reporting | Data Purging

These settings are required for configuring the connection between your database and the Parallels 2X MDM service.

General

Server: localhost

Connection Pooling

☐ Connection Pooling

Minimum Pool Size: 1

Maximum Pool Size: 100

Roles

	Username	Password
Administrator:	sa	••••••••
Device:	device	••••••••
Common:	common	••••••••
Signup:	signup	••••••••
Portal:	portal	••••••••
Reports:	reports	••••••••

Test Connections
OK
Cancel
Apply

From here, configure settings required for the connection between your database and Parallels 2X MDM Service.

From the **General** section configure the below:

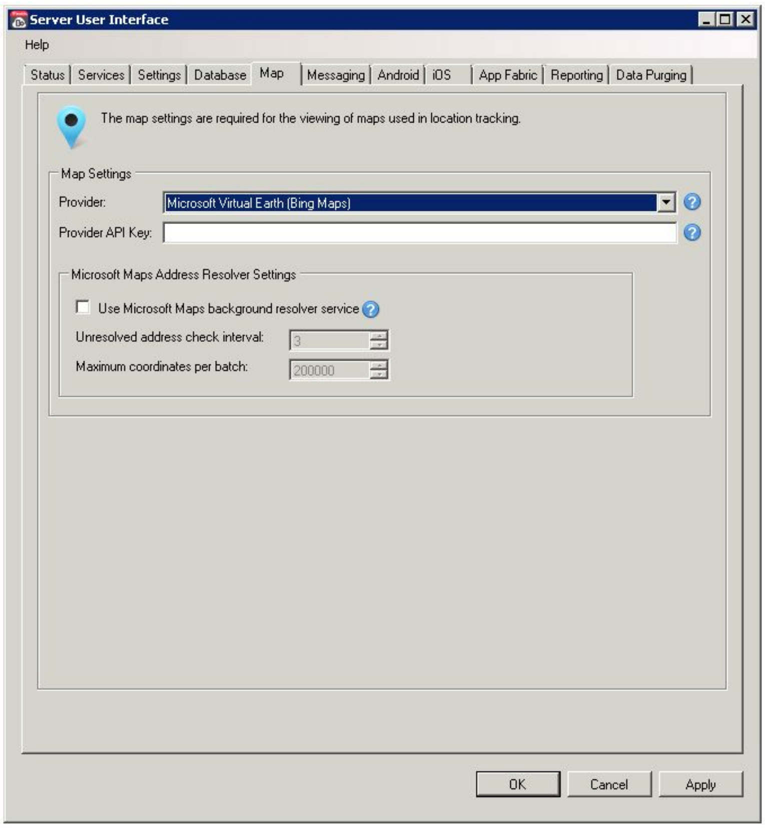
- **Server**: Specify the IP address of the machine hosting your SQL database. If the database is located on the same machine you have installed Mobile Device Management on, you can also use localhost.

Connection Pooling is a cache of database connections maintained so that the connections can be reused when future requests to the database are made. If enabled, you can also adjust both the minimum and maximum connection pool size

The **Roles** section allows you to adjust the below roles configured during setup:

- **Administrator**: Username and Password of administrator account used to connect to the database
- **Device**:Username and Password for users created during setup process
- **Common**:Username and Password that can access and update all of the mdm tables
- **Signup**:Username and Password used to create MDM accounts
- **Portal**:Username and Password used to access the MDM portal
- **Reports**:Username and Password used by the reporting server to connect to the MDM database

5. Map Tab



The map settings are required for the viewing of maps used in location tracking.

Map Settings

Provider: Microsoft Virtual Earth (Bing Maps)

Provider API Key:

Microsoft Maps Address Resolver Settings

□ Use Microsoft Maps background resolver service

Unresolved address check interval: 3

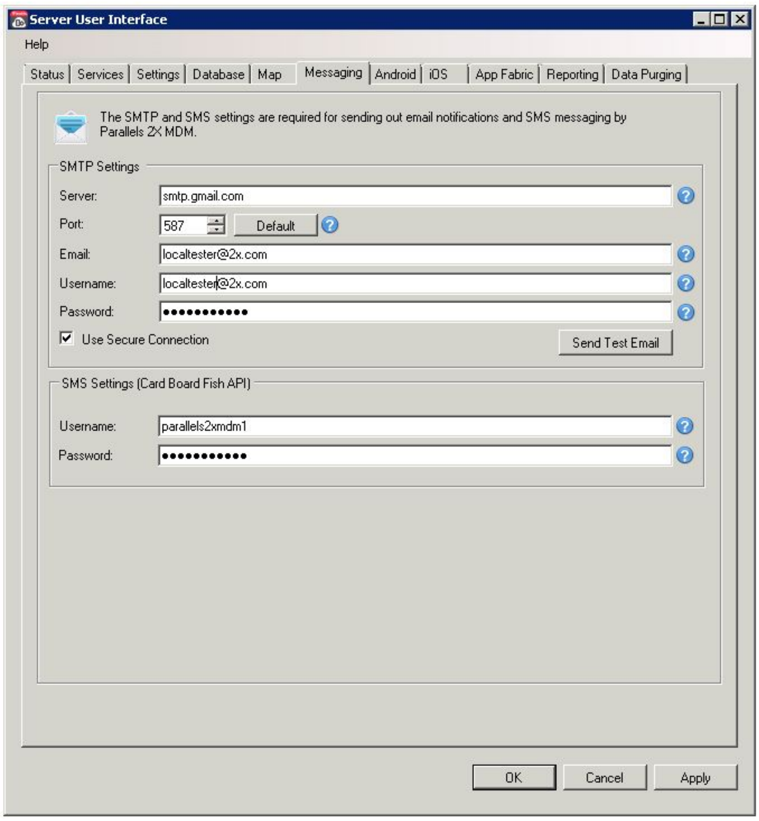
Maximum coordinates per batch: 200000

Next, the Map tab allows you to configure which maps provider location updates will be resolved to and displayed on from the MDM portal.

Select the map provider you have registered with from the **Provider** dropdown and enter the related API key in the **Provider API Key** text field.

If Bing maps is selected, optionally also enable the ‘Use Microsoft Maps Background resolver service’ to resolve location points without an address.

6. Messaging Tab



The SMTP and SMS settings are required for sending out email notifications and SMS messaging by Parallels 2X MDM.

SMTP Settings

Server: smtp.gmail.com

Port: 587

Email: localtester@2x.com

Username: localtester@2x.com

Password: •••••••••••

☑ Use Secure Connection

SMS Settings (Card Board Fish API)

Username: parallels2xmdm1

Password: •••••••••••

This tab consists of settings required for both STMP and SMS message notifications to be sent by Parallels 2X MDM. These settings were configured during setup.

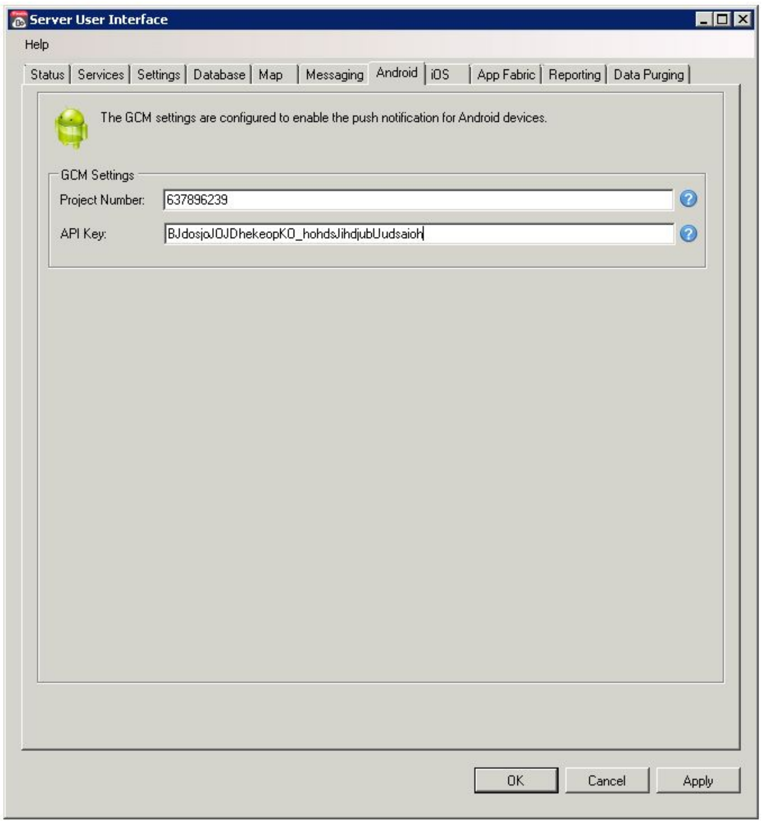
From the **SMTP Settings** section you can adjust the settings below:

- **Server:** The SMTP server IP address or FQDNto be used.
- **Port:** The port number to be used for sending out emails.
- **Email:** The email address that you want to be shown when emails are sent out.
- **Username:** The username to be used if the mail server requires authentication.
- **Password:** Password for the username provided if the mail server requires authentication.
- **Use Secure Connection:** Tick this box if your SMTP server requires an SSL connection.

From the **SMS Settings** section configure the below:

- **Username:** Fill in the username obtained from CardBoard Fish.
- **Password**: Fill in the password for your CardBoard Fish account.

7. Android Tab



The GCM settings are configured to enable the push notification for Android devices.

GCM Settings

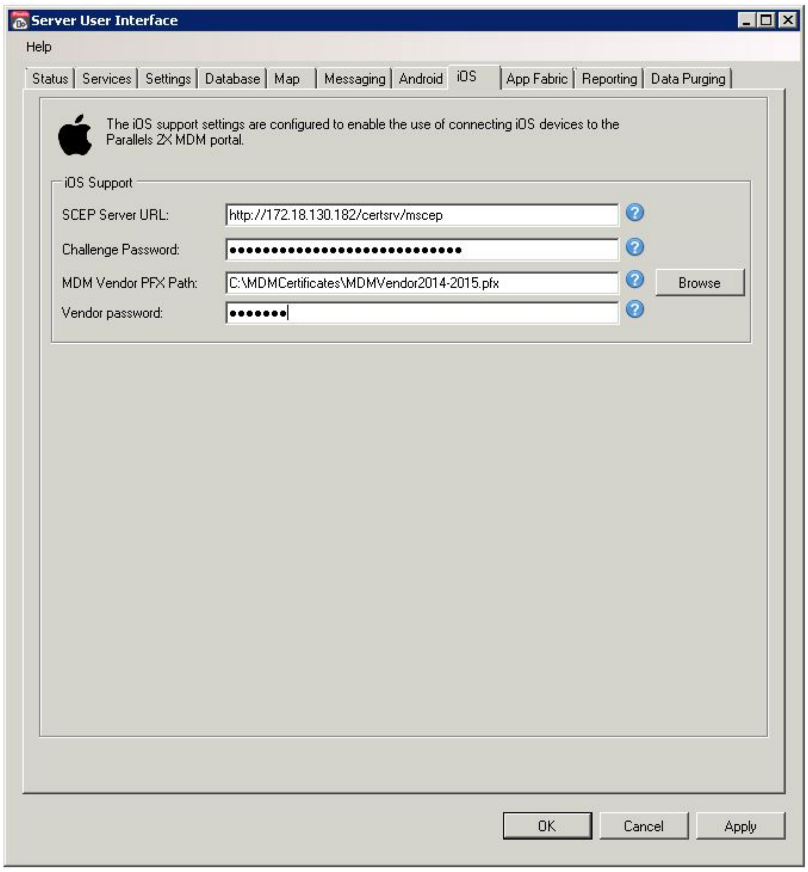
Project Number: 637896239

API Key: BJdosjoJOJDhekeopKO_hohdsJihdjubUudsaioh

For MDM to communicate with GCM and send PUSH notifications to Android devices, configure or update the configuration options below:

- **Project Number:** The project number obtained by the Google Cloud Messaging project.
- **API Key:** The API Key obtained by the Google Cloud Messaging project.

8. iOS Tab



The iOS support settings are configured to enable the use of connecting iOS devices to the Parallels 2X MDM portal.

iOS Support

SCEP Server URL: http://172.18.130.182/certsrv/mscep

Challenge Password: ••••••••••••••••••••••••••••

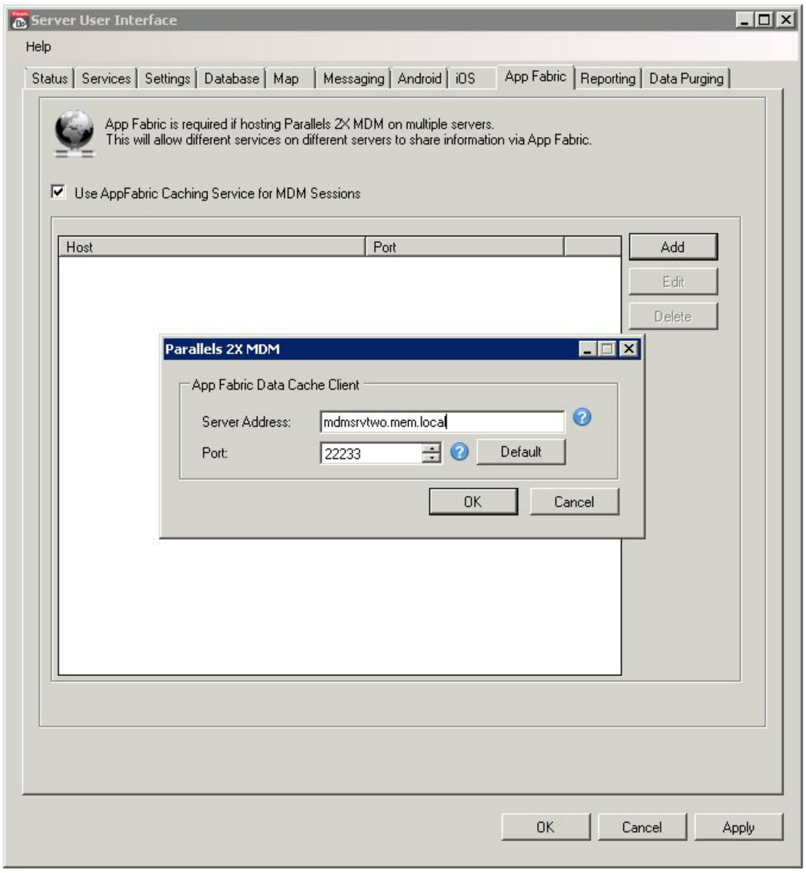
MDM Vendor PFX Path: C:\MDMCertificates\MDMVendor2014-2015.pfx

Vendor password: •••••••

Similarly, for iOS devices to be able to connect and communicate with your MDM server, configure or update the SCEP server configuration options below:

- **SCEP Server URL:** The URL pointing to your certificate SCEP server.
- **Challenge Password:** The challenge password generated by your certificate SCEP server.
- **MDM Vendor PFX Path:** Select the path to the certificate provided to you by Apple.
- **Vendor Password:** The Apple Certificate password

9. AppFabric Tab



App Fabric is required if hosting Parallels 2X MDM on multiple servers.
This will allow different services on different servers to share information via App Fabric.

☑ Use AppFabric Caching Service for MDM Sessions

App Fabric Data Cache Client

Server Address: mdmsrvtwo.mem.local

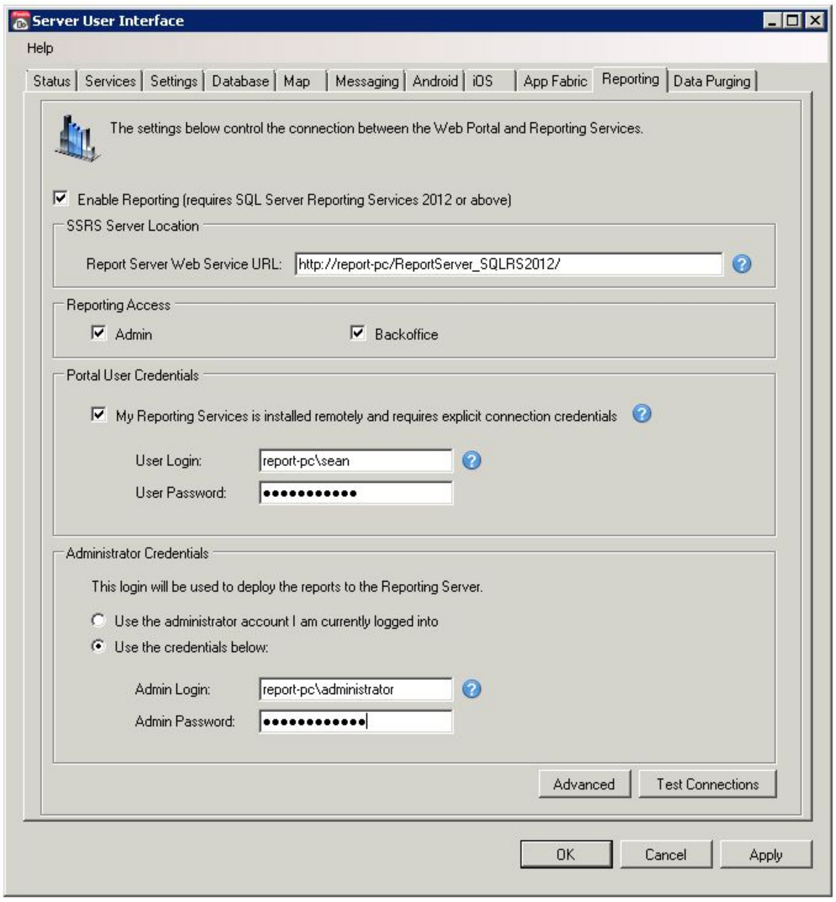
Port: 22233

Parallels 2X MDM uses AppFabric to distribute shared cache to multiple On-Premise installations of MDM. Enable AppFabric if you are hosting MDM on multiple servers. This way you can scale for different services running on different servers to share information via AppFabric.

Enable the ‘Use AppFabric’ checkbox, click ‘Add’ and configure the options below:

- **Server Address**: Server hostname to be used for AppFabric caching to store sessions of the MDM server
- **Port**: The port used to store sessions of the MDM server

10. Reporting Tab



The settings below control the connection between the Web Portal and Reporting Services.

☑ Enable Reporting (requires SQL Server Reporting Services 2012 or above)

SSRS Server Location

Report Server Web Service URL: http://report-pc/ReportServer_SQLRS2012/

Reporting Access

☑ Admin ☑ Backoffice

Portal User Credentials

☑ My Reporting Services is installed remotely and requires explicit connection credentials

User Login: report-pc\sean

User Password: ●●●●●●●●●●●

Administrator Credentials

This login will be used to deploy the reports to the Reporting Server.

○ Use the administrator account I am currently logged into

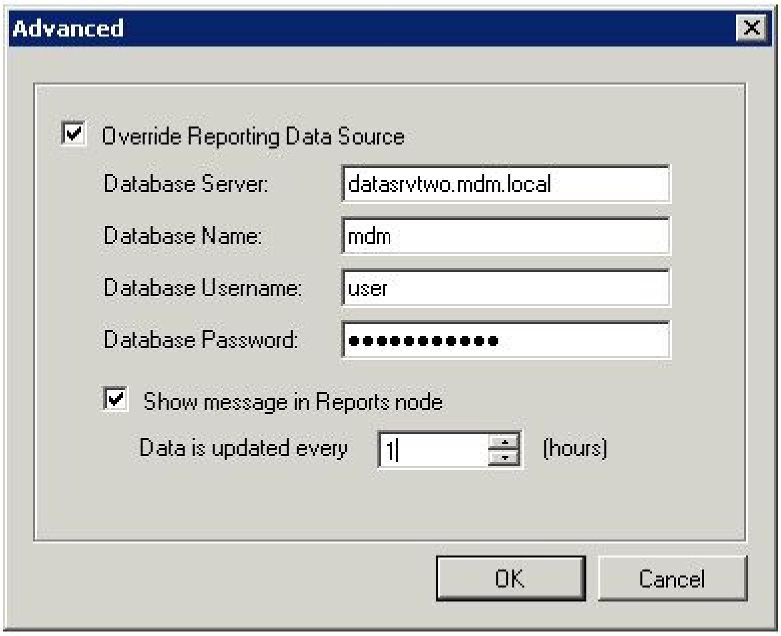
● Use the credentials below:

Admin Login: report-pc\administrator

Admin Password: ●●●●●●●●●●●●●

You can alter the configuration options defined during the setup process used both to deploy and generate reports. The configuration options are listed below:

- **Web Service URL**: The URL pointing toward your Reporting Services end-point.
- **Reporting Access:** Toggle the reporting feature for the back office and admin portal.
- **Portal User Login and Password:** Enter Windows credentials that are configured in SSRS with browser permissions.
- **Administrator Login Name and Password:** Enter Windows credentials configured with administrator privileges and content management rights in SSRS.


Advanced

☑ Override Reporting Data Source

Database Server: datasrvtwo.mdm.local

Database Name: mdm

Database Username: user

Database Password: ●●●●●●●●●●●●

☑ Show message in Reports node

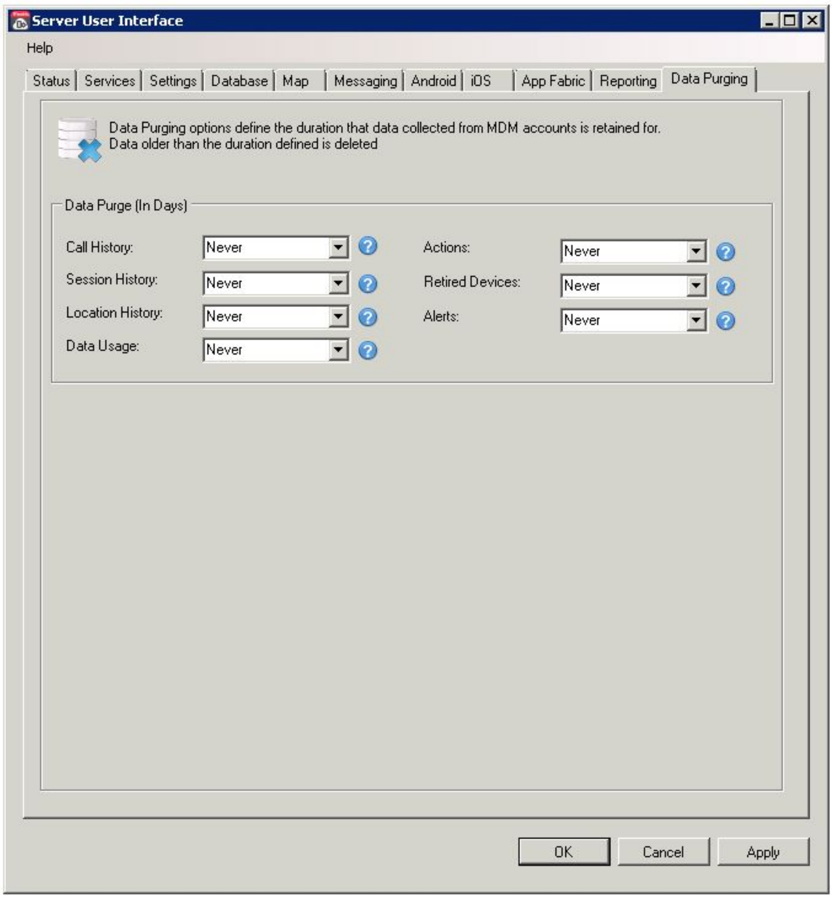
Data is updated every 1 (hours)

The **Advanced** button allows you to define the database that will be used to generate reports. The **Override Reporting Data Source** option is typically enabled when the mdm database that reports will be generated with is mirrored on another server. If required, enable this feature and configure the below:

- **Database Server**: Specify the IP address of the machine hosting the mirrored SQL database
- **Database Name**: Specify the mirrored database name
- **Database Username and Password**: Mirrored Database credentials
- **Show message in reports node**: Set the value in hours equal to the mirrored database update interval used to alert administrators in the portal that report data may be as old as the value set.

Note: Setting the reporting Data Source to a mirrored mdm database takes load off the live database.

11. Data Purging



Data Purging options define the duration that data collected from MDM accounts is retained for.
Data older than the duration defined is deleted

Data Purge (In Days)

Call History:	Never	Actions:	Never
Session History:	Never	Retired Devices:	Never
Location History:	Never	Alerts:	Never
Data Usage:	Never		

Lastly, data purging settings allow you to configure the amount of time data is retained for before being deleted from the MDM Server. You are able to control any data retention period of the data types below:

- Call History
- Session History
- Location History
- Data Usage
- Actions
- Retired Devices
- Alerts