

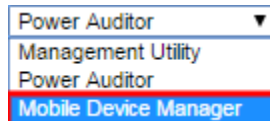


Setting up MDM Server

1. Log into Management Utilities – Select Mobile Device Manager
2. Under Administrator enter MDM Server Configuration
3. Refresh browser – Confirm MDM Server URL Link
4. Create Certificate Request – download certificate request file
5. Log into your Apple Account – Create Certificate
6. Upload certificate request file and download Push certificate
7. Upload Push Certificate and Save
8. Check off MDM profile and press Save
9. Select Administration – Services - Push
10. Choose Poll Device Every (Time interval) from drop down menu and press Update



Log into Management Utilities – Select Mobile Device Manager



MDM Server Settings

Organization

This is the name of your organization; this will appear on the enrollment screen

Host Name

This is the DNS name or Internet facing IP address where the Mobile Devices can communicate to from anywhere in the world.

- You will need to create a firewall rule forwarding the SSL Port # to the server running Management Utilities on your LAN

If you wish to manage mobile devices that are not located on the same network as the server running Management Utilities you can point them to the Internet facing static IP address.

Port # / SSL Port

These are the port numbers that must be available for the mobile devices to be able to access the MDM Server, they are not to be in use by other web server applications and they cannot be the same port number used for browsing to the Management Utilities.

The example below shows how we use port 18066 and the DNS name `mdm.syamsoftware.com` so our mobile devices can be managed anywhere - the router will forward https traffic on port 18066 to the server's IP address on the internal LAN

Enter the MDM Server Information and press Save



Administration

MDM Server Settings

Platform Configuration

Services

About

 The MDM Server is available.
 Basic Authentication
<https://mdm.syamsoftware.com:18066>

Organization

SyAM Software Demo MDM

Host Name

mdm.syamsoftware.com

Port

8080



SSL Port

18066

Save

Delete

Refresh your browser – Click on the MDM Server URL Link to confirm connection

 The MDM Server is available.
 Basic Authentication
<https://mdm.syamsoftware.com:18066>



Quick Reference MDM Server Setup

This will now open up the MDM Server enrolment page – This is the URL you will use to enroll the iOS devices

If you do not see this page please check the network routing for the host name and port number selected on the MDM Server settings



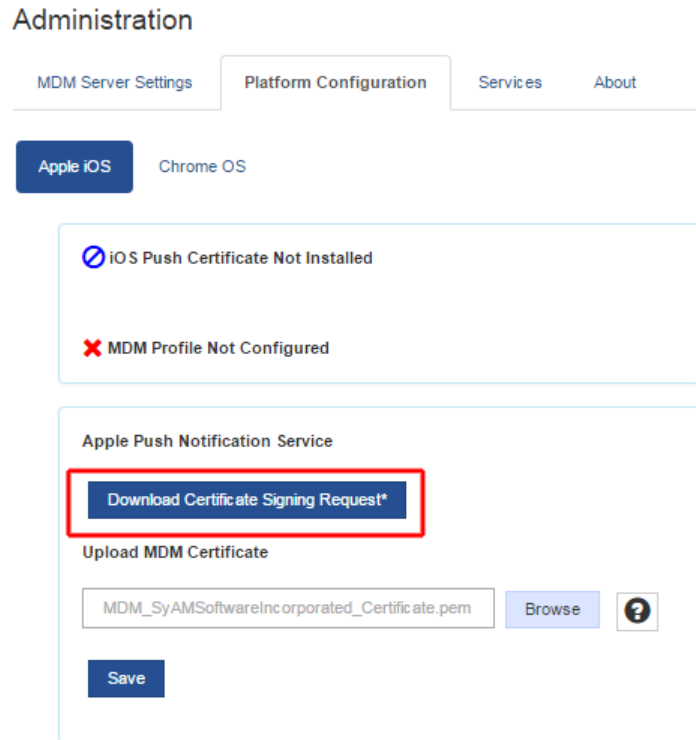
If you had to accept the certificate accessing this page, you should download the **root certificate** and install it so it becomes trusted.

After that, go ahead and **enroll**

Next we need to install the Apple Push certificate that is required for management of iOS devices.

Under Platform Configuration select Apple iOS

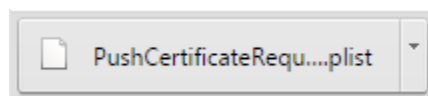
Click on the Download Certificate Signing Request – this will generate the certificate from specific to this installation of the MDM Server.



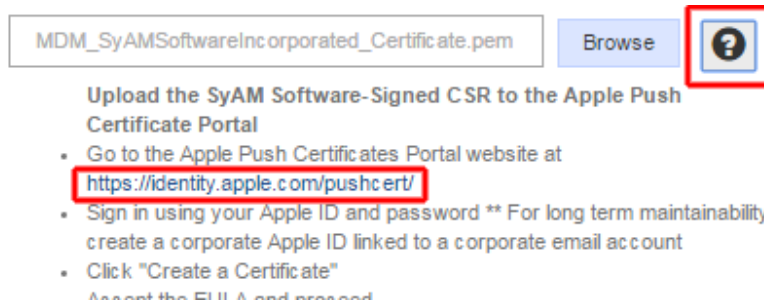
The screenshot shows the Administration interface with the following elements:

- Navigation tabs: MDM Server Settings, Platform Configuration (selected), Services, About
- Platform selection: Apple iOS (selected), Chrome OS
- Status indicators:
 - ⓘ iOS Push Certificate Not Installed
 - ✖ MDM Profile Not Configured
- Section: Apple Push Notification Service
 - Download Certificate Signing Request* (highlighted with a red box)
 - Upload MDM Certificate
 - Text input: MDM_SyAMSoftwareIncorporated_Certificate.pem
 - Buttons: Browse, ?
 - Save button

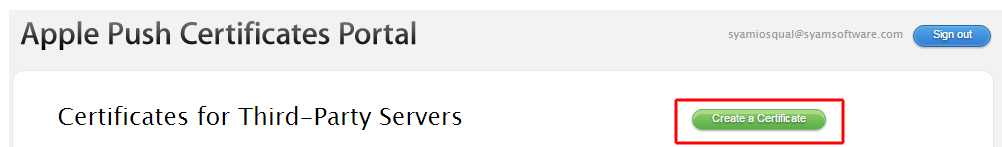
Save this Push Certificate Request file so you have it available to upload to Apple



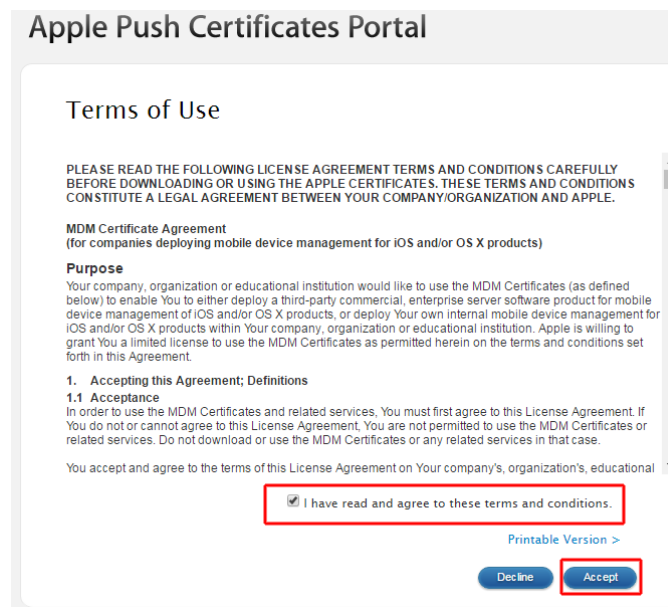
Click on the ? - It will open the help and URL link to the Apple Login



Log into your Apple Account and click on Create a Certificate



Review and accept the Terms of Use



Now Select the Push Certificate Request file that had been generated and Upload

Apple Push Certificates Portal

Create a New Push Certificate

Upload your Certificate Signing Request signed by your third-party server vendor to create a new push certificate.

Notes

SyAM MDM Server

Vendor-Signed Certificate Signing Request

Choose File PushCertific...st (3).plist

Cancel Upload

Now Download the Apple Push Certificate that is has generated

Apple Push Certificates Portal



Confirmation

You have successfully created a new push certificate with the following information:

Service	Mobile Device Management
Vendor	SyAM Software Incorporated
Expiration Date	May 13, 2017

Manage Certificates Download

Save the Push Certificate file so you have it available to upload into the SyAM MDM Server.

Name	D
 MDM_ SyAM Software Incorporated_ Certificate (3).pem	5
 PushCertificateRequest (3).plist	5



Browse to where you saved the Apple Push Certificate and Save

Administration

MDM Server Settings | Platform Configuration | Services | About

Apple iOS | Chrome OS

iOS Push Certificate Not Installed

MDM Profile Not Configured

Apple Push Notification Service

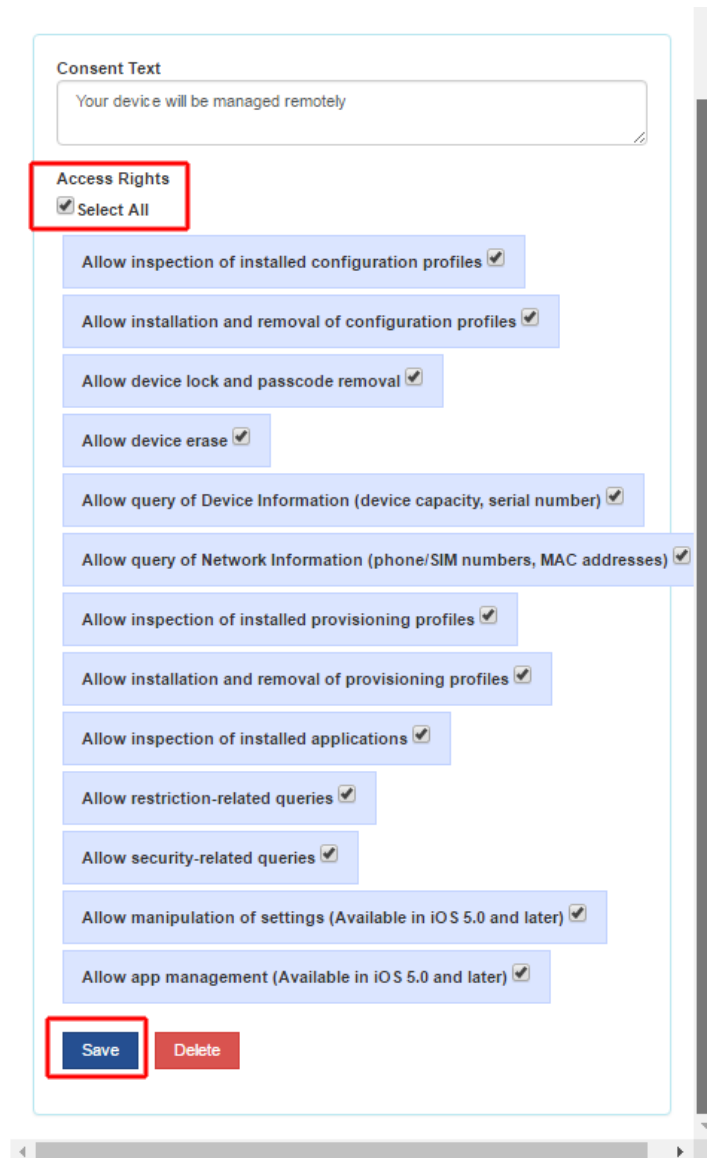
[Download Certificate Signing Request*](#)

Upload MDM Certificate

MDM_SyAM Software Incorporated_Certificate (3) [Browse](#) [?](#)

[Save](#)

Next we Configure the MDM Profile, check off Select All and Press Save



The screenshot shows the MDM Profile configuration interface. At the top, there is a text area for "Consent Text" containing the text "Your device will be managed remotely". Below this is the "Access Rights" section, which is highlighted with a red box. It contains a "Select All" checkbox, which is also checked and highlighted with a red box. Below the "Select All" checkbox are several checkboxes, all of which are checked:

- Allow inspection of installed configuration profiles
- Allow installation and removal of configuration profiles
- Allow device lock and passcode removal
- Allow device erase
- Allow query of Device Information (device capacity, serial number)
- Allow query of Network Information (phone/SIM numbers, MAC addresses)
- Allow inspection of installed provisioning profiles
- Allow installation and removal of provisioning profiles
- Allow inspection of installed applications
- Allow restriction-related queries
- Allow security-related queries
- Allow manipulation of settings (Available in iOS 5.0 and later)
- Allow app management (Available in iOS 5.0 and later)

At the bottom of the "Access Rights" section, there are two buttons: "Save" and "Delete". The "Save" button is highlighted with a red box.



The MDM Server can be set to poll the iOS device every number of hours, to set this polling cycle select Services, PUSH and update the Polling Device Every Time and press Save

Administration

MDM Server Settings

Platform Configuration

Services

About

Site Manager

PUSH

✔ PUSH Service Running

Poll devices every

1 hour

How often should notifications be sent (seconds)?

30

Max # of notifications per Interval?

50

Update Service

Settings Updated