

# 7P MDM Server 6.04

## Release Highlights

### Document information

<b>Author(s)</b>	MDM Team
<b>Date</b>	01.03.2021
<b>Version</b>	1.0
<b>Editing statues</b>	Approved
<b>Approved by</b>	MDM Team
<b>Security classification</b>	public

## 1 General

The following sections provide a brief overview of all new and updated MDM functionalities based on the current 7P MDM release version 6.04.

### 1.1 Removal of the old UI

The old UI has been removed. The URL with the **“/admin”** will lead to a **“404 Not found”** page. Set **“/frontend”** instead of **“/admin”** to navigate to the new UI. The old URL without the **“/admin”** will forward you also to the new UI. Old bookmarks should be updated accordingly.

### 1.2 Apple School Manager is now available on MDM 6

Apple School Manager is now part of MDM 6. For more details, please check chapter 1.10.

### 1.3 New Setup Items for Apple Device Enrollment Program (DEP)

Some new items have been added to the Apple DEP profile. A new DEP profile needs to be created if you would like to use any of the following new items:

- Skip Appearance
- Skip Device To Device Migration
- Skip iCloud Storage
- Skip iMessage And Face Time
- Skip Messaging Activation Using Phone Number
- Skip OnBoarding
- Skip Privacy
- Skip Restore Completed
- Skip Screen Time
- Skip SIM Setup
- Skip Software Update
- Skip Update Completed
- Skip Welcome

The complete list now looks like the following:

#### Define new profile

Department:

Enrollment Profile name:

#### Enrollment

- ☐ Allow pairing
- ☐ Device is supervised
- ☐ MDM profile installation is mandatory
- ☐ MDM profile can be removed
- ☐ Await Device Configured (If checked device does not continue in Setup Assistant)
- ☐ Is multi user (only on newer generation 32+ GB iPads with use on ASM)
- ☐ Use user authentication

**Setup items:**

- ☐ Disable location services
- ☐ Disable restoring from backup
- ☐ Disable Move from Android
- ☐ Disable signing in to Apple ID and iCloud
- ☐ Skip terms and conditions
- ☐ Disable Siri
- ☐ Disable automatically sending diagnostic information
- ☐ Disable Biometrics
- ☐ Disable Payment
- ☐ Disable Zoom
- ☐ Disable DisplayTone
- ☐ Disable FileVault Setup Assistant screen (macOS only)
- ☐ Hides and disables the passcode pane.
- ☐ Skips the Home Button screen in iOS.
- ☐ Skips on-boarding informational screens for user education ("Cover Sheet, Multitasking & Control Center", for example) in iOS.
- ☐ Skips the screen for watch migration in iOS.
- ☐ Skips iCloud Analytics screen in macOS.
- ☐ Disables registration screen in macOS.
- ☐ Skip Appearance
- ☐ Skip Device To Device Migration
- ☐ Skip iCloud Storage
- ☐ Skip iMessage And Face Time
- ☐ Skip Messaging Activation Using Phone Number
- ☐ Skip OnBoarding
  
- ☐ Skip Privacy
- ☐ Skip Restore Completed
- ☐ Skip Screen Time
- ☐ Skip SIM Setup
- ☐ Skip Software Update
- ☐ Skip Update Completed
- ☐ Skip Welcome

## **1.4 Enhancements for Android 11 "Work Profile On Company Owned"**

### **1.4.1 Enrollment type "Work Profile On Company Owned" has been added for Zero Touch**

A Zero Touch device can be now enrolled to the new enrollment type "Work Profile On Company Owned".

Add device

Cancel
Save without enrolling

Choose a platform

Android
iOS
macOS
Windows
Unknown

Enrollment program

Zero Touch

Android enrollment type

Work Profile On Company Owned
Device Owner Mode
Work Profile On Company Owned
Corporate

MDM ID
Device name

ZT-WPOCO

Phone number
Email for enrollment

Comment
Serial number

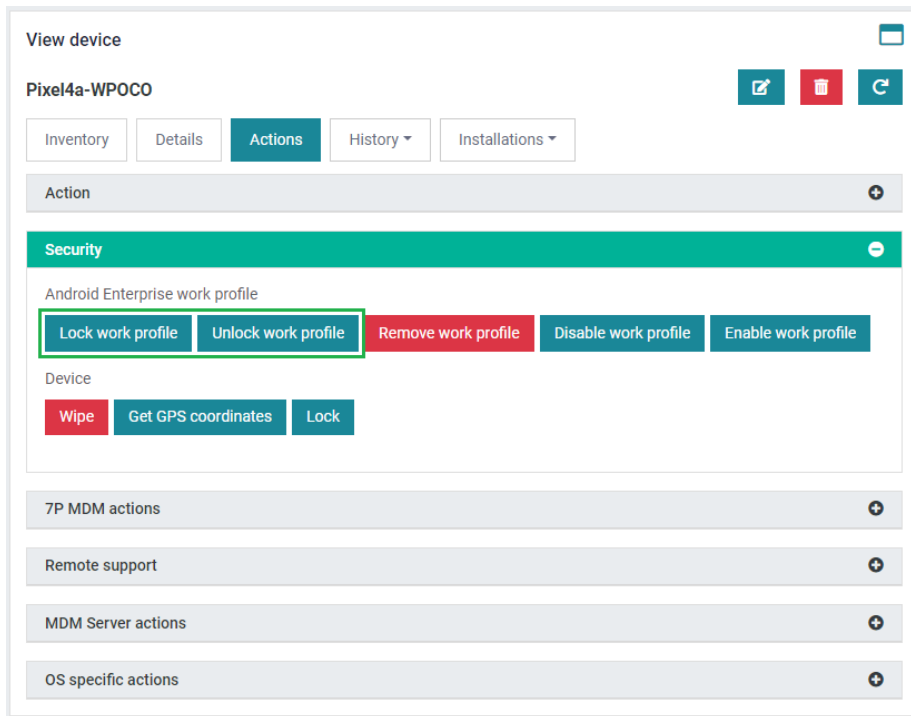
Activation parameters

Download URL
Activation PIN

The enrollment type “Work Profile On Company Owned” is only available for Android 11.

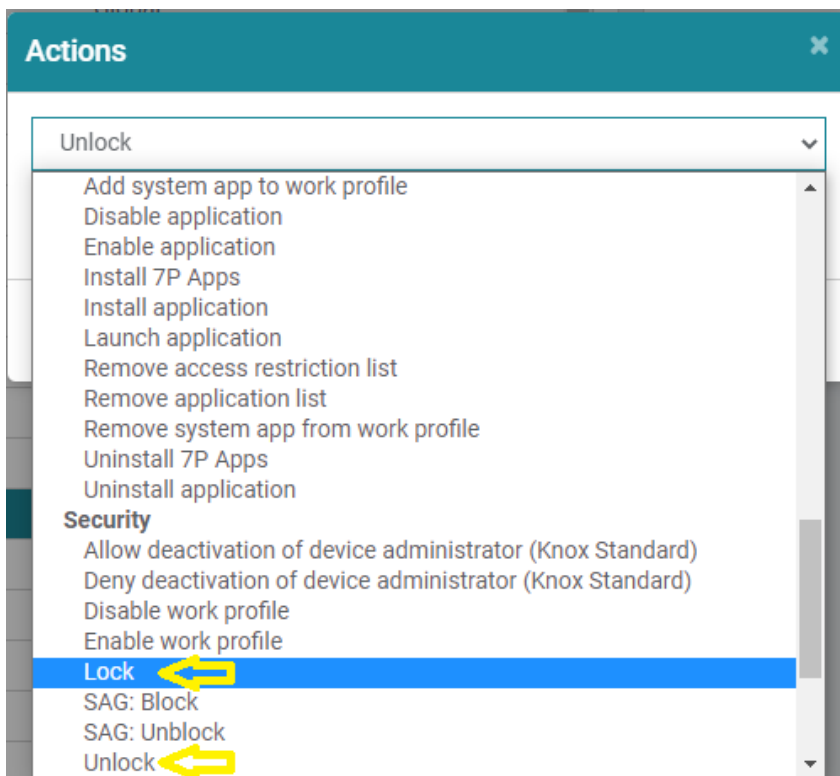
#### 1.4.2 Android “Work Profile On Company Owned” devices can be locked and unlocked from UI

Android 11 devices with enrollment type “Work Profile on company owned” can now be locked and unlocked from UI.



This will lock / unlock the Work Profile (device). If the device has been locked via this “Lock work profile” button, access to any app in the Work profile section will require the password.

Work profile can be also locked / unlocked via an operation.



## 1.5 Android “Work Profile On Company Owned” device can be locked via a password policy

Android 11 devices enrolled as “Work Profile On Company Owned” can be locked via a password policy. The autolock configuration can be applied to Target = device (work profile) or Target = Parent device. It is also possible to define different password policies, one for the

work profile (device) and one for the parent device by applying two different autolock configurations, one for each target.

The screenshot shows the 'View device' page for a Pixel4a-WPOCO. The 'Actions' tab is selected. Under the 'Action' section, 'Apply configuration' is chosen from the dropdown, and 'Autolock: 11' is selected. The 'Target' dropdown is open, showing 'Device' and 'Parent device' as options. A 'Send' button is located to the right of the target selection. Below this, there are expandable sections for 'Security', '7P MDM actions', 'Remote support', 'MDM Server actions', and 'OS specific actions'.

The autolock password policy can be applied via “Actions” ...

This is a close-up of the 'Actions' dialog box. It contains the same configuration as the previous screenshot: 'Apply configuration' for the action, 'Autolock: 11' for the policy, 'Channel (macOS)' for the channel, and 'Device' for the target. The 'Target' dropdown is open, showing 'Device' and 'Parent device' as options. 'Cancel' and 'OK' buttons are at the bottom right.

... and via operations. Here the “Target” selection is also available.

## 1.6 Improvements on disabling and enabling apps on Android devices

Disabled apps on Android devices will become hidden. This prevents running deactivated apps. To be able to use the apps again, the disabled apps need to be enabled again.

View device  
8655450396958

Inventory Details Actions History Installations

Installations > Applications

☐ Include system applications  
☐ Include deleted applications

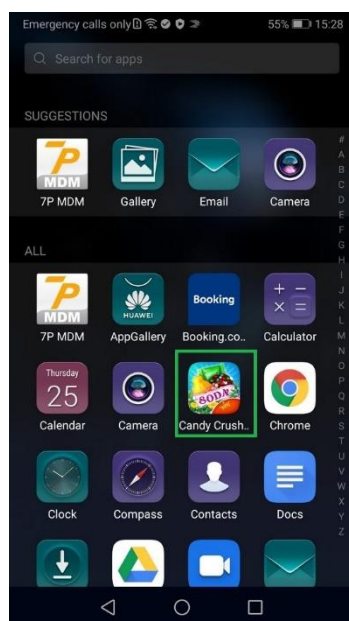
☒ Installed via Google EMM ☒ Installed by MDM server ☐ System App ☐ Deleted app ☐ Other

Program name Identifier

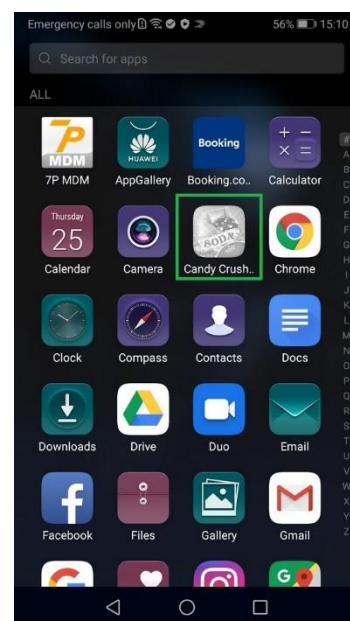
Program name	Identifier	Version	Status	Action
7P MDM	com.sevenprinciples.mdm.android.client	6.03.10	Enabled	-- Send
Booking.com Hotels	com.booking	14.6	Enabled	-- Send
Candy Crush Soda	com.king.candycrushsodasaga	1.136.4	Enabled	Disable applicati... Send
Docs	com.google.android.apps.docs.editors.docs	1.7.232.04.40	Enabled	-- Uninstall application Send
Facebook	com.facebook.katana	stub (35.1.9)	Enabled	Disable application Send
Instagram	com.instagram.android	stub (29.1.0)	Enabled	-- Send
Poweramp	com.maxmpz.audioplayer	v3-build-814-play	Enabled	-- Send
Sheets	com.google.android.apps.docs.editors.sheets	1.7.232.06.40	Enabled	-- Send
Slides	com.google.android.apps.docs.editors.slides	1.7.232.05.40	Enabled	-- Send

7P Apps view

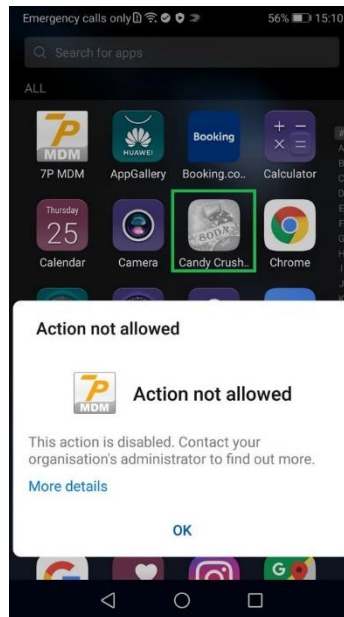
On Huawei devices, disabled apps remain visible but become greyed out.



Enabled application



Disabled application



When trying to run the application, a message will appear, saying that the app has been disabled by the administrator. After enabling the app again, the app will get its colour back and can be used.

## 1.7 Comment field for Apple Push Certificate

A new comment field has been added to Settings > Apple > General options. The field called “Apple Id” can be used to enter the Apple ID that has been used to create the push certificate. It is necessary to use the same Apple ID for renewing the certificate; therefore, this new field will serve as a reminder.

General options

Cancel Save

Cloud Apple MDM Push:

Expires: 24/06/2021 09:54

Choose file

Topic: com.apple.mgmt.7PMobile

Company Apple MDM Push:

Expires: 16/11/2021 09:40

Choose file

Apple id: example.id@apple.com

Topic:

☐ This instance does not use Apple devices and MDM push is not needed

Download CSR

Apple Push Certificates Portal: [identity.apple.com](https://identity.apple.com)



## 1.8 New filter option for movement of devices on Global level

It is now possible to filter tenants when moving a device on Global level.  
When selecting a device either in Organization > Device pool or Organization > Users and devices a new filter can be selected:

The image shows two side-by-side screenshots of a web interface for selecting a user to whom a device will be assigned. The left screenshot shows the 'Users and devices' section with a search bar containing 'example' and a filter icon (a funnel) highlighted with a red box. Below the search bar, there is a table with the header 'Username' and a message 'No data available in table.' The right screenshot shows the same interface but with a 'Filter' overlay. The overlay has a search bar with 'example' and a 'Unselect all' button. Below the search bar, there is a list of tenants: 'Example Tenant' (checked), 'Example group' (checked), and 'Unallocated' (unchecked). At the bottom of the overlay, there is an 'OK' button. Below the overlay, there are 'Cancel' and 'OK' buttons.

By using this filter, you only get the users and devices that exist in the selected tenant(s).

## 1.9 Improvement of certificate related conditions

The conditions “Certificate is installed” as well as “Certificate is not installed” in Operations are now usable on additional Android enrollment types.  
The conditions will now also work on devices enrolled as Device Owner, Work Profile or Work Profile On Company Owned.

The image shows a screenshot of the 'Operation' configuration screen. The 'Name' field is 'Example Operation'. The 'Conditions' section shows '60 matching devices' and a plus button. Below the conditions, there is a list of conditions: 'Certificate is not installed: Identity > Global\_Certificate\_1'. The 'Actions' section shows a plus button. Below the actions, there is a list of actions: 'Install certificate: Identity: Global\_Certificate\_1'. At the bottom, there are four buttons: 'Send', 'Send immediately', 'Cancel', and 'Save'.


## 1.10 Apple School Manager in MDM 6

In server 6.04 we have implemented support for Apple School Manager (ASM), that previously only was available in MDM 5, which is now deprecated.

### Apple School Manager mode activation:

If you want to have Apple School Manager mode activated please contact MDM support, which then will arrange that ASM mode gets activated on the instance.

Hereafter you can inside Global > Settings > Apple and Apple School Manager set the sFTP sync credentials you get from ASM portal as well define how the Shared iPad mode enabled devices should have user profiles configured.

Apple School Manager (all tenants) 

SFTP URL:	upload.appleschoolcontent.com
Username:	[REDACTED]@sftp.apple.com
Password:	*****

Number of resident users by device capacity (Shared iPad)

32 GB:	2
64 GB:	2
128 GB:	4
256 GB:	5
512 GB:	5

**Note:** When activating ASM mode the server changes some logic, UI on user data and enables the Apple School Manager configuration menu inside Infrastructure. Please request special document from MDM support on using ASM mode.

**Warning:** When ASM mode is enabled please do not disable ASM mode again.

### Apple School Manager configuration menu

Inside Global tenant you see this ASM menu:

Apple School Manager	Overview												
<ul style="list-style-type: none"> <li>Overview</li> <li>Locations</li> <li>Courses</li> <li>Classes</li> <li>Students</li> <li>Instructors</li> <li>Download &amp; upload</li> </ul>	<table> <tr> <th>Entity</th><th>Total entries</th></tr> <tr> <td>Locations</td><td>3</td></tr> <tr> <td>Students</td><td>151</td></tr> <tr> <td>Instructors</td><td>71</td></tr> <tr> <td>Courses</td><td>3</td></tr> <tr> <td>Classes</td><td>3</td></tr> </table>	Entity	Total entries	Locations	3	Students	151	Instructors	71	Courses	3	Classes	3
Entity	Total entries												
Locations	3												
Students	151												
Instructors	71												
Courses	3												
Classes	3												

The same ASM menu seen from a tenant look different:

Apple School Manager	Overview
Overview	
Locations	
Courses	
Classes	
Students	
Instructors	

Entity	Total entries
Locations	1
Students	73
Instructors	34
Courses	1
Classes	1

The Global tenant gives you an overview, delete options as well the Download & upload options, where sFTP sync from MDM to ASM is executed, as well the sync back from ASM to MDM is executed.

In tenant you create courses and classes and assigning users to these for the education payload, which is used to configure classes for Student iPads and for configuring the Classroom app for Instructors.

**Note:** The first sFTP sync you execute from MDM to ASM must include certain basic information, which is defined in a special ASM document which you can request from MDM support.

### SFTP sync:

Using sFTP sync from Global tenant > settings > Apple and Apple School manager setting allows the MDM to act as master and sync data from MDM to ASM portal using sFTP sync.

The sFTP sync is executed from the sync buttons inside Global tenant > Infrastructure > Apple School Manager and Download & upload menu

Apple School Manager	Download & upload
Overview	Create and upload zip to ASM SFTP
Locations	Sync data from ASM server (Full sync)
Courses	Sync data from ASM server (Simple sync)
Classes	
Students	
Instructors	
Download & upload	

The data that MDM sends to ASM using sFTP sync are: User data (First name + Last name + Person-ID + Email + Role + Grade + the name of the tenant this user belongs to in MDM)

The data that are synced back from ASM to MDM are users including Managed Apple ID created in ASM portal and confirmation of data like Locations (= tenants in MDM), Courses and Classes.

**Note:** Only users with source = SFTP in ASM will be synced back to MDM. Users that are manually created in ASM are not included to ASM sync to MDM.

**Important:** There must be a DEP token in Global tenant to make DEP sync work as well enable the ASM sync back to MDM option. You can additionally add tenant DEP tokens too.

DEP devices synced to MDM via Global DEP token can move across all tenants, but DEP devices synced to a tenant DEP token will remain in this tenant only.

### User data:

Users created in MDM will at SFTP sync to ASM also be added to ASM portal and via ASM sync synced back to MDM. However, the users can be added in MDM the usual ways like: manually, via CSV import, LDAP sync, AzureAD sync or via webservice APIs.

The user template has changed a bit when ASM mode is activated:

The field User ID from normal MDM mode is now renamed to Person ID and two new fields Role and Grade level have been added.

By default, all users will get the role “student”, unless the user is proactively changed to the role “instructor”. The reason is that students don’t get the Classroom app, which is used by Instructors to manage the iPads of the students.

Grade level is an optional value, but can be used to set a value for users. Grade levels might be used in operations later to install certain applications on specific students’ devices

**Note:** Users added to MDM system (independently of the source) are treated equally in the SFTP sync to ASM.

### User data when doing LDAP sync

When using LDAP sync in a tenant, there are new additional mapping fields for Role and Grade level fields that can be mapped with specific AD attributes.

Furthermore we have added a “translator” for the Role mapping, so that when you Map the Student role field in MDM with an AD attribute in your company AD, then each customer might have an own language/regional wording for what the name is for a student and for an Instructor. In the screenshot below one can see that the Danish words for student (elev) and for instructor (laerer) are mapped accordingly.

Edit mappings

user device attributes

user device parameter:

first name (mandatory)

Last name (mandatory)

Autoassign mobile number

Grade level

Role (mandatory)

Directory attributes:

displayname

distinguishedname

dscorepropagationdata

employeeid

Add

Parameter	attribute	
firstName	givenname	✗
lastName	sn	✗
email	mail	✗
user_name	userprincipalname	✗
asm_grade	description	✗
asm_role	employeeid	✗

Student value:

Elev

Instructor value:

Lærer

### Assign/unassign DEP profiles from individual device via actions:

On the actions tab of the individual devices and Apple Device Enrollment Program menu it is possible to assign a different DEP profile than the one that is assigned to the device or remove DEP profile.

View device

DEP: IPAD WI-FI 128GB SPACE GRAY-HCZ

Inventory

Details

Actions

History

Installations

7P MDM actions

Remote support

MDM Server actions

Apple Device Enrollment Program

Test School Shared ipad

Assign profile

Remove DEP profile

The selectable DEP profiles in this dropdown menu are defined in Global tenant if the device is synced to MDM via DEP token in Global tenant, otherwise it is the selection of tenant DEP profiles if the device is synced to MDM via tenant DEP token.

## Setup new conditions in Operations, when using ASM

In Operations menu there are now some new additional conditions that can be used when ASM mode is enabled.

### ASM role condition:

If you want to filter for the **ASM roles** student or instructor – the following condition can be used.

The left screenshot shows the 'Conditions' dialog box with a list of conditions. The 'ASM role is' condition is highlighted. The right screenshot shows the 'Conditions' dialog box with the 'ASM role is' condition selected and the 'Student' role chosen from the dropdown menu.

### Grade level condition:

In Operations menu there is now also a new condition to filter for certain values defined on users based on the Grade level field, this is named **Belongs to grade (ASM)**

The screenshot shows the 'Conditions' dialog box with the 'Belongs to grade (ASM)' condition selected. Below the condition name is a text input field. At the bottom are 'Cancel' and 'OK' buttons.

First name	Student
Last name	10
Email	Student.10@onlineskole.com
Person ID	student.0010
Role	Student
Grade level	Grade 2008
Managed Apple ID	student.10@onlineskole.com
Tenant	School 1
Groups	Students - Students Students - Grade 2008

It is also possible to use a condition to filter for iPads which **Is Shared iPad** mode enabled:

