

Contents

- Overview 1
- Accessing MDM in the Control Panel..... 2
 - Create the MDM Instance in the Control Panel..... 3
- Adding a New MDM User 4
- Manage MDM Users 6
 - Assign Multiple Tokens to a User with Multiple Devices..... 6
 - Assign (or Unassign) the Admin Role to a User 7
- Manage Domains in MDM 9
 - Add a Domain..... 9
 - Remove a Domain..... 10
- Apple Device Connection 11
- Android Touchdown Client 13

Powered by



Overview

Provisioning Mobile Device Manager (MDM) in the Control Panel is a straightforward process. A few notes about provisioning MDM in the Control Panel:

- When you provision MDM you are doing so for all devices on the account.
- For users with multiple devices – you must specify the number of MDM device licenses the user is granted. A token is granted for each device license.
- Each MDM user must have an Exchange mailbox.
- You must have at least one admin user.

This guide will cover the following topics in provisioning MDM in the Control Panel:

- Accessing MDM in the Control Panel
 - Creating the MDM instance within the Control Panel
- Adding a new MDM user
- Managing MDM users
 - Assigning multiple tokens for a user with multiple devices
 - Assigning an admin user
- Managing domains in MDM
- Apple device connection
- Android *Touchdown* client

Accessing MDM in the Control Panel

1. Login to the Control Panel.

The screenshot shows the APPTIX Control Panel dashboard. The navigation menu at the top includes: Home, Users, Exchange, Microsoft Lync 2010, **Mobile Device Management** (highlighted with a red box), MOZY_ONLINE_BACKUP, Applications, and More Services. The account information at the top right shows: Subscriber Subscription (Account ID: 1024295), Advantage Email - 5GB - 5 Users (zappptixmdm2.collaborationhost.net);1045907, and a Logout button. The dashboard is divided into several sections:

- Service Information:** Subscription (Advantage Email - 5GB - 5 Users), Diskspace (8 KB used of 25 GB), Mailboxes (3 unit used of 5 unit).
- Account:** Outstanding Invoices (\$ 0.00), Need Attention (1 domain(s)), Financial Documents, Admins, Subscriptions, Payment Methods, Change Password.
- Exchange:** This section provides you with managing facilities for your mailboxes, public folders, distribution lists, contacts and mail service general settings. Options: Add New Mailbox, Mailboxes.
- Microsoft Lync 2010:** Microsoft® Lync® is an enterprise-ready unified communications platform. Options: Microsoft Lync 2010, Configuration.
- Mobile Device Management:** Mobile Device Manager (MDM) provides a comprehensive mobile security, device management and application management solution to simplify device activation, configuration, security, application management, end-user support, and full lifecycle management across the enterprise. MDM Users.
- Users:** Create and manage users. Assign services to created users. Options: Users, Create User.
- Store:** Here you can buy additional services, domains and more. Options: Buy More Services, Buy Additional Resources, Register New Domain, Change Service Plan.
- Domains:** Manage your domains and domain names. Options: Registered Domains, Hosted Domains.
- Secure Email Encryption:** Secure Mail. Options: Company Settings, User Settings.

2. Select the **Mobile Device Management** tab (as illustrated above).
The **Mobile Device Management** dashboard displays:

The screenshot shows the Mobile Device Management dashboard. The navigation menu at the top includes: Home >, Mobile Device Management, Screen ID: 2.12.12.05.01, Refresh, and Up Level. The main content area shows: Mobile Device Management - base service. Below this, there is a **Create** button (highlighted with a red box) and a Status section with a radio button labeled "Not activated".

Create the MDM Instance in the Control Panel

When you first access the **Mobile Device Management** dashboard, as above, you must create the service in your Control Panel account in order to give users access to it.

1. Click the **[Create]** button.

A list of domains displays:



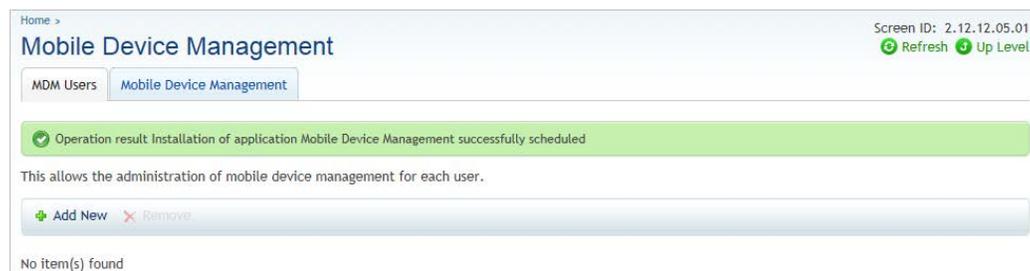
2. Select the domain with which you are going to associate your MDM service and click **[Next]**.
3. Click **[Next]** again.

A summary screen displays:



4. Click **[Finish]** to initialize your MDM service within the Control Panel.

The creation process is complete and you are returned to the **Mobile Device Management** dashboard:



Now that you have created the service in the Control Panel:

From the **Mobile Device Management** dashboard, you can add new users, assign tokens to user accounts, and manage domains for your MDM service.

Adding a New MDM User

To add a new user to your MDM account, you must first add a user to your overall account. The user must have an Exchange mailbox assigned to them. See the *Exchange Admin Guide* for details about adding a service user in the Control Panel.

1. On the **Mobile Device Management** dashboard, on the MDM Users tab (default), click the **[Add New]** button.

The first screen of the **Add New User** wizard displays.

2. Select to add either a **New** (the default) or **Existing Service User**. Since MDM users must have a mailbox, we will select **Existing** user.
3. Click **[Next]**.

The next screen of the wizard displays:

Service User	Login
<input type="radio"/> b	b@zzapptixmdmd2.collaborationhost.net
<input type="radio"/> c	c@zzapptixmdmd2.collaborationhost.net
<input checked="" type="radio"/> new test user	newtestuser@zzapptixmdmd1.collaborationhost.net

4. Select the appropriate user from the list and click **[Next]**.

The next screen of the wizard displays:

Home > Mobile Device Management Screen ID: 2.12.12.07.03
Refresh Up Level

MDM Users Mobile Device Management

Please specify settings for services

MDM User
This allows the administration of mobile device management for each user.

Is Admin

Check if this user should also be an Administrator. Please select at least one user to be the administrator in order to access the MDM Portal.

Number of MDM Device Licenses item
Enter the number of MDM licenses you would like to grant to this user. This initiates the device enrollment process by sending out the activation email with token information for each unique license. Only one device could be enrolled per token. The value should not exceed 9 item.

<< Back Next >> Cancel

5. Select **Is Admin** if this MDM user is to be an admin user.

NOTE: You can have more than one admin in your MDM account.

6. Enter the **Number of MDM Device Licenses** for which this user will be granted tokens.

NOTE: A token initiates the device enrollment process by sending out the activation email with token information for each unique license. Only one device is enrolled per token. The value in this field cannot exceed the number of remaining tokens.

7. Click **[Next]**.

The final wizard screen, the summary screen, displays:

Home > Mobile Device Management Screen ID: 2.12.12.07
Refresh Up Level

MDM Users Mobile Device Management

✔ You are ready to create new MDM User Please confirm creation of MDM User

Service User new test user
Login newtestuser@zzapptixmmdm1.collaborationhost.net

MDM User
This allows the administration of mobile device management for each user.

Is Admin Yes
Check if this user should also be an Administrator. Please select at least one user to be the administrator in order to access the MDM Portal.

Number of MDM Device Licenses item
Enter the number of MDM licenses you would like to grant to this user. This initiates the device enrollment process by sending out the activation email with token information for each unique license. Only one device could be enrolled per token. The value should not exceed 9 item.

<< Back Finish Cancel

8. Review and click **[Finish]**.

Manage MDM Users

The ways in which you can manage MDM users in your account:

- assigning multiple tokens for a user with multiple devices
- assigning a user (or multiple users) to the admin role

Assign Multiple Tokens to a User with Multiple Devices

1. On the **Mobile Device Management** dashboard, click the **Service User** name of the user to which you want to assign multiple tokens.

The **User Details** screen for the selected user displays:

Home > Mobile Device Management > MDM User 'newtestuser@zzaptixmdmd1.collaborationhost.net' Screen ID: 2.12.12.06.01
Refresh Up Level

MDM User **Resource Usage**

This allows the administration of mobile device management for each user.

Edit settings Delete

ID	230825
Service User	new test user
Status	Provisioning
Settings	
Is Admin	Yes

Check if this user should also be an Administrator. Please select at least one user to be the administrator in order to access the MDM Portal.

2. Click the **Resource Usage** tab:

Home > Mobile Device Management > MDM User 'newtestuser@zzaptixmdmd1.collaborationhost.net' Screen ID: 2.12.12.06.04
Refresh Up Level

MDM User **Resource Usage**

Edit Update usage information

MDM Device License (100%) 1 of 1 item

3. Click the **[Edit]** button.

The **Resource Usage Edit** screen displays:

Home > Mobile Device Management > MDM User 'newtestuser@zzaptixmdmd1.collaborationhost.net' Screen ID: 2.12.12.06.05
Refresh Up Level

MDM User **Resource Usage**

Resources

Resource	Current usage	Limit
MDM Device License	1 item	9 item

Enter the number of MDM licenses you would like to grant to this user. This initiates the device enrollment process by sending out the activation email with token information for each unique license. Only one device could be enrolled per token. The value should not exceed 9 item.

Submit Cancel

4. Enter the number of devices utilized by the selected user in the **MDM Device License** field and click

[Submit].

The number of devices associated with the selected user is updated and the **Edit** screen closes.

Assign (or Unassign) the Admin Role to a User

1. On the **Mobile Device Management** dashboard, click the **Service User** name of the user to which you want to assign (or unassign) the admin role.

The **User Details** screen for the selected user displays:

Home > Mobile Device Management > MDM User 'newtestuser@zzapptixmdmd1.collaborationhost.net' Screen ID: 2.12.12.06.01
Refresh Up Level

MDM User Resource Usage

This allows the administration of mobile device management for each user.

Edit settings Delete

ID	230825
Service User	new test user
Status	Provisioning
Settings	
Is Admin	Yes

Check if this user should also be an Administrator. Please select at least one user to be the administrator in order to access the MDM Portal.

2. Click the **[Edit settings]** button.

The **Edit Settings** screen displays:

Home > Mobile Device Management > MDM User 'newtestuser@zzapptixmdmd1.collaborationhost.net' > Edit Settings > Screen ID: 2.12.15.05
Refresh Up Level

Edit Settings

Please specify settings for services

MDM User

This allows the administration of mobile device management for each user.

Is Admin

Check if this user should also be an Administrator. Please select at least one user to be the administrator in order to access the MDM Portal.

Next >> Cancel

3. Place a check in the **Is Admin** checkbox to assign this user admin rights.

OR

Remove the check to unassign the admin rights from this user.

4. Click **[Next]**.

The **Edit Settings** summary screen displays:

Home > Mobile Device Management > MDM User 'newtestuser@zzapptixmdm1.collaborationhost.net' >

Screen ID: 2.12.15.07
Refresh Up Level

Edit Settings

MDM User On
This allows the administration of mobile device management for each user.

Is Admin No
Check if this user should also be an Administrator. Please select at least one user to be the administrator in order to access the MDM Portal.

<< Back Finish Cancel

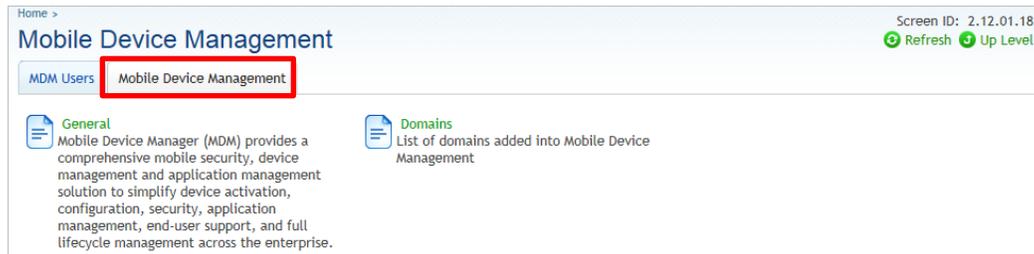
5. Click **[Finish]** to finalize edits.

Manage Domains in MDM

To add a domain to your MDM service, you must first add the domain to your overall account in the Control Panel. See the *Exchange Admin Guide* for details about creating a domain.

Add a Domain

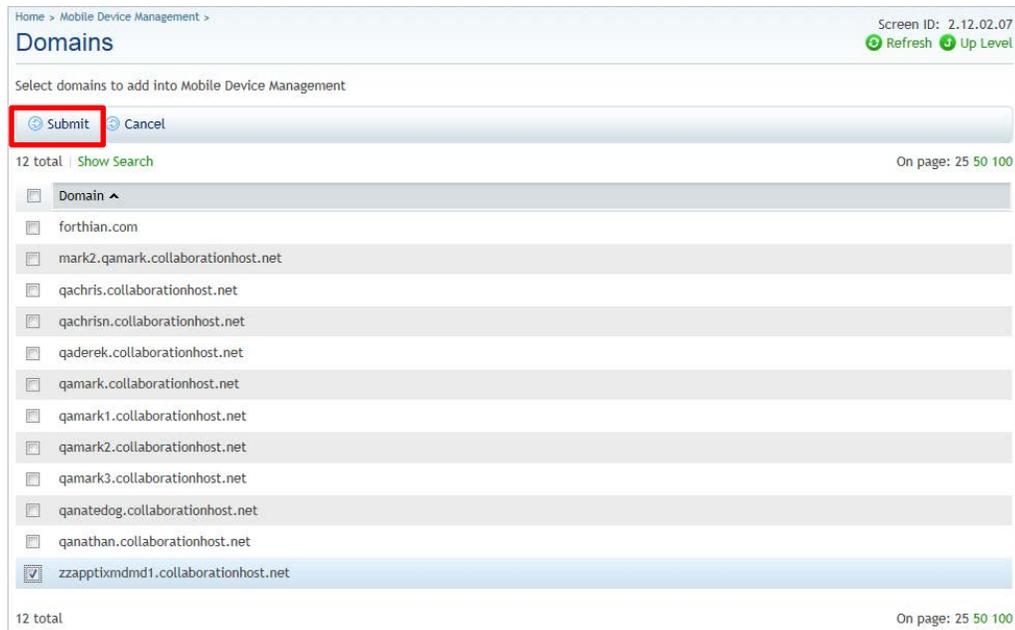
1. On the **Mobile Device Management** dashboard, select the **Mobile Device Management** tab:



2. Select the **Domains** option.
The **Domains** screen displays:



3. Click the **[Add]** button.
A list of available domains displays:



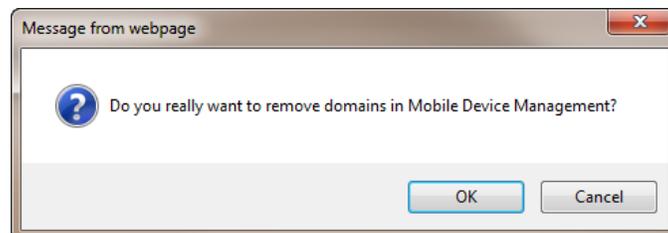
- Place a check mark beside any domains you wish to add to MDM and click **[Submit]**. The **Domains** screen displays again, this time with your added domain in the list.

Remove a Domain

- Access the **Domains** screen as we did above:



- Select the domain to remove from the list. The **[Remove]** button above the list activates.
- Click the **[Remove]** button. The system checks to be sure you really want to remove the domain:



- Click **[OK]** to remove. The **Domains** screen displays again, this time with your domain removed from the list.

Apple Device Connection

Before an MDM end-user can enroll his/her iOS device (iPad and iPhone), the MDM administrator must create an Apple Push Notification service (APNs) certificate for their subscription. This is a one-time action that must be performed before any iOS device can be enrolled with MDM.

The MDM admin must obtain a cert for the Apple devices from Apple and then store it in the portal; the portal will then push it to the device after/during the enrollment process.

The admin creates a “request” for a certificate in the portal, and then saves this .plist file on his/her computer.

The admin then accesses the Apple webpage and, using the aforementioned “request,” obtains a certificate. When the certificate (*MDM_AirWatch_Certificate.pem* filename) is received, he/she uploads the certificate to the portal.

Once the certificate is uploaded, the devices on the subscription can be successfully enrolled.

Follow these steps:

1. Login to the MDM portal as an MDM admin.
2. Access **Menu > Profiles and Policies > Certificates > APNs for MDM.**
3. To create a “request” for a certificate in the portal, click the **[Generate new certificate]** button.
4. Click *AirWatchAPNsRequest.plist*.
5. Save the file on your computer's hard drive.
6. Create an Apple ID dedicated to MDM for your company.
7. Click **[Go to Apple]**.
A new window displays the webpage at <https://identity.apple.com/pushcert/>.
8. Use your Apple ID to login.
9. Click **[Create a certificate]**.
10. Accept the agreement terms.
11. Browse to the .plist file you saved on your machine and click **[Upload]**.
A confirmation displays, informing you that the APNs cert has been successfully created:



12. Click **[Download]**.
You are prompted to save the .pem file on your machine.
13. Save the file.
14. Leave this window open and return to the **Certificate Management** window in the MDM portal.
15. Click **[Next]**.
16. Upload the .pem file you saved earlier.
17. Click **[Save]**.
18. Enter the Apple ID and click **[Next]**.
19. Save the APNs on the portal:

APPTIX Mobile Device Manager m3@zzapptix.mdmindirect.collaborationinc

Menu Add My Favorites

Certificates

Certificates

Settings

Certificate Authorities

APNs For MDM

APNs For Applications

Device / iOS / APNs For MDM

Enabled*

Current Setting Inherit Override

Certificate* Certificate Uploaded

Type **Pfx**

Issued to **C=US, CH=APSP:6d0fc0af-5e3e-47d7-bc5b-60faab8427e5, OID.0.9.2342.19200300.100.1.1=com.apple.mgmt.External.6d0fc0af-5e3e-47d7-bc5b-60faab8427e5**

Issued by **CN=Apple Application Integration Certification Authority, OU=Apple Certification Authority, O=Apple Inc., C=US**

Valid From **2/28/2013**

Valid To **2/28/2014**

Thumbprint **50ED185E1FC58A750ADEF2F0D1C5ACC98CF2ECE7**

Apple ID **anand.surada@apptix.com**

Child Permission* Override only Inherit or Override

Android Touchdown Client

The NitroDesk TouchDown application is used to securely configure and access email on your Android device. The TouchDown app is necessary for the following reasons:

- The native device mail client on most Android devices is not encrypted.

NOTE: Touchdown is not necessary on certain devices such as Samsung SAFE devices.

- In addition to being a security risk, the native client does not provide the functionality needed for MDM's over-the-air configuration services.
- MDM integrates with NitroDesk TouchDown to provide a mail client that is securely encrypted, fully functional, and easy to use.

Your administrator configures the Email integration between MDM and NitroDesk Touchdown, but you need to install the TouchDown application. Contact your administrator with any questions about email configuration.