NotifyMDM
Mobile Device Management

User Self-Administrative Web Guide

Table of Contents

The User Self-Administrative Web

The *User Self-Administration Portal* is a resource for *NotifyMDM* users. Its primary benefit is that it provides a quick way to perform time sensitive operations without having to go through an administrator. This means that **if your device is lost or stolen you can issue commands to the device to prevent malicious actions** or unwanted access to sensitive data as soon as you become aware of a threat.

You can access the portal from your desktop computer or from a mobile device. Both the desktop portal and the mobile portal include a way for you to check the location of your device and retrieve a recovery password to unlock your device.

You will also use these portals to upload or install client certificates if access to the server you are interfacing with requires an authentication certificate for security purposes. (See *Client Certificates* below.)

If you have **multiple devices** enrolled against a single *NotifyMDM* user account, you can view and manage all your devices via the Self-Administrative portals. Above the menu options, select the device you wish to view from a drop-down list.

To use the User Self-Administrative portals, you will need to obtain the *NotifyMDM* server address from your administrator. Commit it to memory or note it somewhere.

Accessing the Mobile User Self-Administrative Portal

In a device browser of an Internet enabled device, enter *https://<yourNotifyMDMserveraddress>/mobile*

On-Demand users enter: *https://ondemand.notifymdm.com/mobile*

Login with your *NotifyMDM* user account credentials:

- For users interfacing with an ActiveSync server, use your ActiveSync account ***username***, ***password*** and ***domain***.
- For users not interfacing with an ActiveSync server, use your *NotifyMDM* user account ***username*** and ***password***, and leave the domain field blank.

Sample *User Self-Administrative Portal* view for an Android User

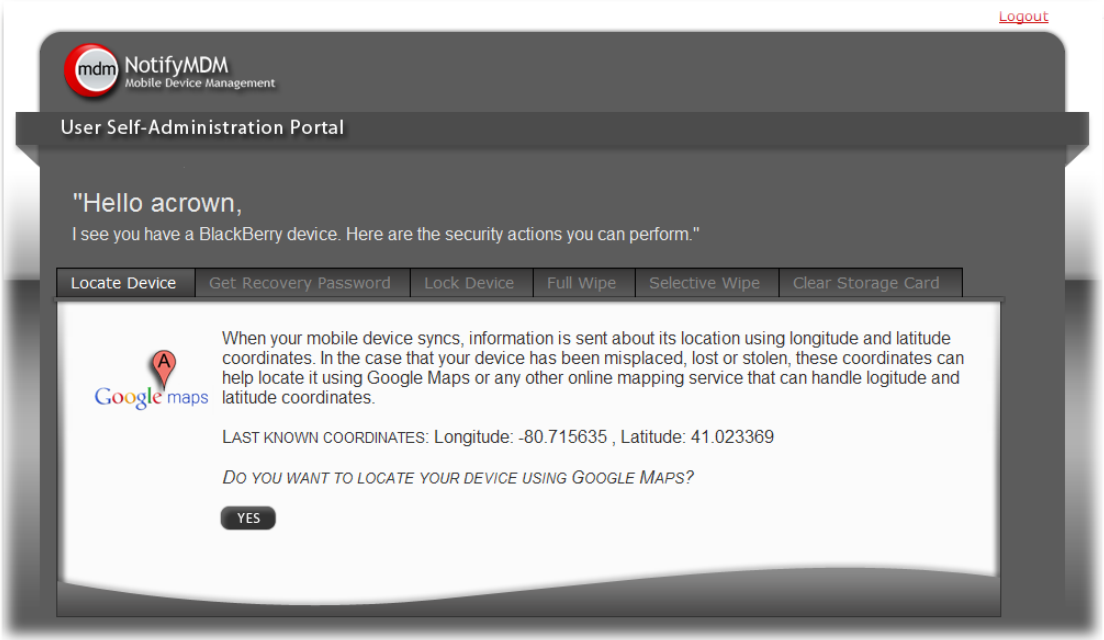
Accessing the Desktop User Self-Administrative Portal

In the web browser of an Internet enabled PC, enter *https://<yourNotifyMDMserveraddress>*

On-Demand users enter: *https://ondemand.notifymdm.com*

Login with your *NotifyMDM* user account credentials:

- For users interfacing with an ActiveSync server, use your ActiveSync account ***username***, ***password*** and ***domain***.
- For users not interfacing with an ActiveSync server, use your *NotifyMDM* user account ***username*** and ***password***, and leave the domain field blank.



Sample *User Self-Administrative Portal* view for a BlackBerry User

The Security Commands

The security actions you can perform from the portal vary based on the type of device you have. The functionality of the action, in particular the *Full Wipe* command, may also vary slightly, based on what the device platform supports. See the chart that follows for details.

KEY

Anrd	Android devices	**S60**	Symbian S60 3rd edition devices, v9.1
TD/A	*Android devices with TouchDown™*	**WM**	Windows Mobile, v6.1/6.5 devices
NS/BB	*NotifySync™ for BlackBerry*	**wOS**	webOS devices
iOS	iOS devices with multitasking capabilities	**WP7**	Windows Phone 7
iOS Adv MDM	Requires Production Certificate generated with Apple Enterprise Developer account.		

When you login to the *NotifyMDM Self-Administration Portal*, the security actions compatible with your device will be displayed. You may be able to perform some or all of the following actions:

Option	Description	Devices Supported
Full Wipe	Users can issue a full wipe command. Functionality varies by device. *Android w/ native ActiveSync account (requires OS v2.2 or greater)*: Device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased. Does not erase SD card. *Android w/TouchDown (requires OS v2.2 or greater)*: Device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased. Does not erase SD card. *Android w/TouchDown using OS v2.0 or 2.1: Full Wipe* not available – use *Selective Wipe* option. *BlackBerry:* Removes all mail and PIM data associated with the *NotifySync* application and removes the *NotifySync* / *NotifyMDM* accounts. Locks the device if *Require Password* is enabled. Erases *NotifySync* data from the SD card. *iOS:* Device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased. *iOS with (APNs) Enterprise Developers Certificate:* iOS Adv MDM functionality allows for *Full Wipe* to be applied immediately to iOS devices. *Symbian*: Device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased. Some models (N95 and 6120c) wipe only *Mail for Exchange* data. Erases the SD card. *WM*: Device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased. Erases SD card only on *Professional* devices. *webOS, and WP7:* Device returns to factory settings. This entails deleting all data and applications from the device. The device returns to the state it was in when purchased.	**NotifyMDM app:** Anrd, NS/BB, iOS, TD/A, WM, iOSw/Adv MDM, S60 **ActiveSync only:** wOS, WP7

Selective Wipe	Users can issue a selective wipe command. Functionality varies by device. *Android w/ native ActiveSync account (requires OS v2.2 or greater)*: Removes the *NotifyMDM* account information. *Android w/TouchDown (using any supported OS)*: Removes all mail and PIM (calendar, contact, tasks) data associated with the *TouchDown* application and returns *TouchDown* to a pre-registration state. Erases *TouchDown* data from the SD Card. Removes the *NotifyMDM* account information. *BlackBerry:* Removes all mail and PIM data associated with the *NotifySync* application, and locks the device if *Require Password* in enabled. *iOS with (APNs) Enterprise Developers Certificate:* Removes all mail and PIM (calendar and contacts) data controlled by *NotifyMDM*. iOS Adv MDM functionality allows for *Selective Wipe* to be applied immediately* to iOS 4 devices. * *Command is applied immediately, however, device is capable of postponing the action.* *Symbian:* Removes the *NotifyMDM* account information.	**NotifyMDM app:** Anrd, NS/BB, iOSw/Adv MDM, TD/A, S60
Wipe Storage Card	Remotely wipes all data from the device's storage card.	**NotifyMDM app:** Anrd, NS/BB, TD/A, WM
Lock Device	Remotely locks the device, requiring a password to be entered before the device can be used. *Android or Android w/Touchdown:* requires OS 2.2 or greater. *iOS with (APNs) Enterprise Developers Certificate:* iOS Adv MDM functionality allows for *Lock Device* to be applied immediately to iOS devices.	**NotifyMDM app:** Anrd, NS/BB, TD/A, WM, iOSw/Adv MDM
Get Recovery Password	If your device has the capability to issue a request for a temporary recovery password, this is where you can retrieve the temporary unlock password that has been generated for you.	**NotifyMDM app:** NS/BB, TD/A
Locate Device	The GPS or triangulation on the device is used to locate your device. The last known longitudinal and latitudinal coordinates synced from your device display here. You can use this information to help locate the device using Google maps or another online mapping service.	**NotifyMDM app:** Anrd, NS/BB, iOS, TD/A, WM
Clear Passcode	Passcode will be cleared. If passcode is required by the user's policy, the user will be prompted to enter a new passcode. *Available only with advance iOS Adv MDM functionality.*	**NotifyMDM app:** iOS

Client Certificates

If access to the server you interface with requires an authentication certificate for security purposes, you can use the self-administration portals to obtain your certificate.

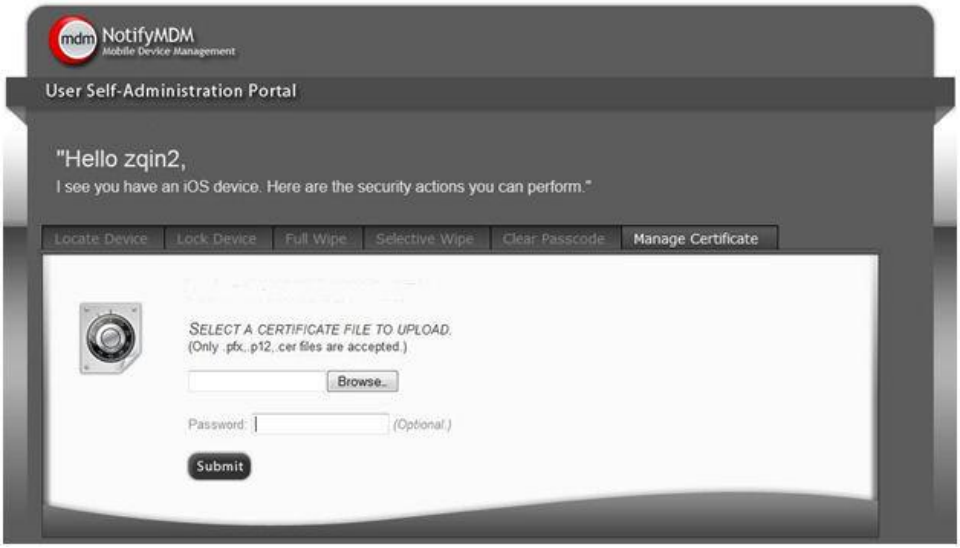
From the Desktop User Self-Administration portal . . .

Your administrator will create and upload a certificate for you on the server or he/she may instruct you to upload the certificate yourself from the Desktop User Self-Administration portal.

If you are uploading the certificate yourself, the administrator will send you the certificate file. There may also be a password associated with the certificate file.

Uploading the Certificate

1. From your PC browser, access the *Desktop User Self-Administration portal* and log in with your user credentials.
2. Select the ***Manage Certificate*** tab.
3. Browse to locate the certificate file your administrator has provided. The file format will be one of the following: .cer, .pfx, or .p12.
4. If your certificate file is protected by a password, enter the ***Password*** and confirm it.
5. Click ***Submit***. The certificate can now be downloaded and installed on your device(s).



Managing the Certificate

When the certificate has been uploaded, you can:

Download the certificate to your device.

- If you are using your mobile device browser, click the certificate file name above to download the certificate to your device.
- Or access the Mobile User Self-Administration portal from your device browser to download the certificate. https://<*yourNotifyMDMserveraddress*>/mobile

Upload a different certificate file. Please note that uploading another certificate will replace the current certificate.

From the Mobile User Self-Administration portal . . .

Once your system administrator has created and uploaded a client certificate for you on the server, you will use the *Mobile User Self-Administration portal* to install the certificate on your device.

1. From your device browser, access the *Mobile User Self-Administration portal* and log in with your user credentials.
2. Select ***Install Certificate***.

   (If you get a message saying there is no available certificate, one has not yet been uploaded to the server for you. Consult your administrator.)

3. Click on the file name that appears to begin the certificate installation. The file format will be one of the following: .cer, .pfx, or .p12.

   Certificate installation is different for each device type. An example of the installation process for your device type is available in Appendix A of every *NotifyMDM* device user guide.

   NotifyMDM for Android

   NotifyMDM for Android with TouchDown

   NotifyMDM for BlackBerry

   NotifyMDM for iOS Devices

   NotifyMDM for Symbian

   NotifyMDM for Windows Mobile