

User Self-Administration

ZENworks® Mobile Management 2.7.x

June 2013

Legal Notices

Novell, Inc., makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc., makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc., reserves the right to make changes to any and all parts of Novell software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the [Novell International Trade Services Web page \(http://www.novell.com/info/exports/\)](http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2012-13 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.
www.novell.com

Online Documentation: To access the latest online documentation for this and other Novell products, see the [Novell Documentation Web page \(http://www.novell.com/documentation\)](http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see [the Novell Trademark and Service Mark list \(http://www.novell.com/company/legal/trademarks/tmlist.html\)](http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Table of Contents

The User Self-Administration Portal	4
Accessing the Mobile User Self-Administration Portal.....	5
Accessing the Desktop User Self-Administrative Portal	6
The Security Commands	9
Client Certificates	11

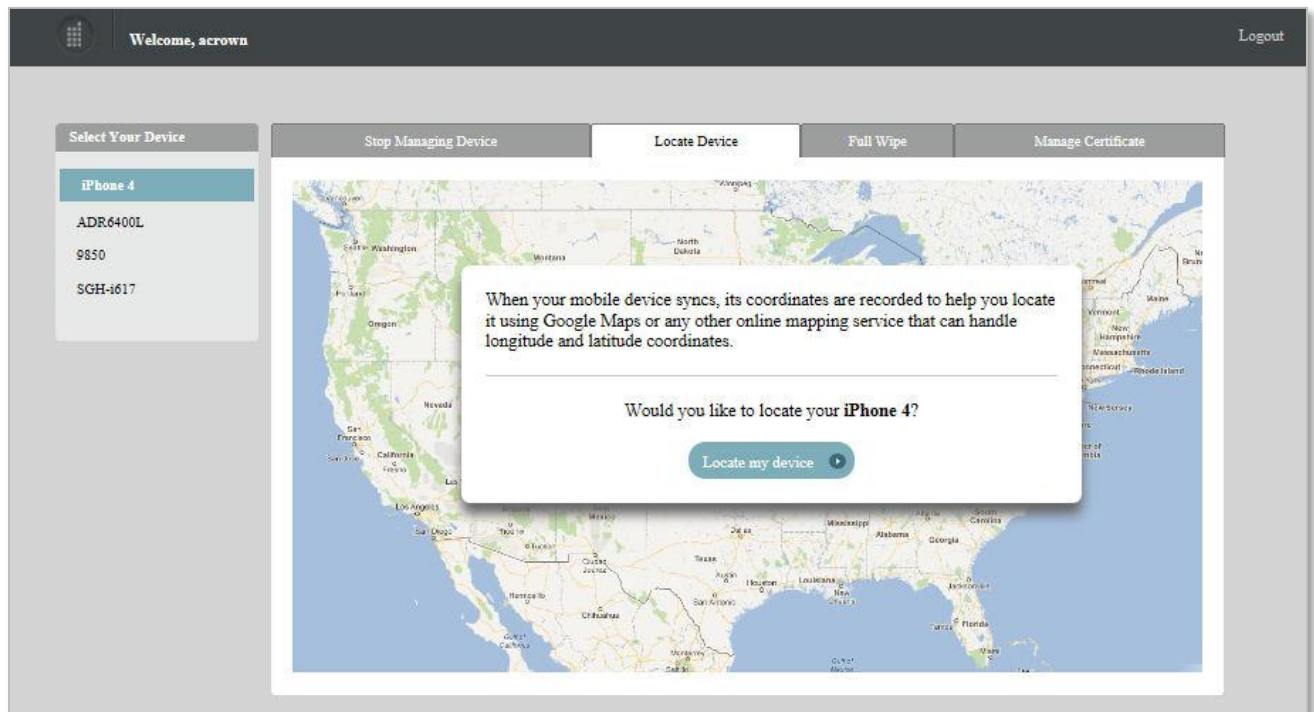
The User Self-Administration Portal

The *User Self-Administration Portal* is a resource for *ZENworks Mobile Management* 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 can 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 later in this document*)

If you have multiple devices enrolled against a single *ZENworks Mobile Management* user account, you can view and manage all your devices via the Self-Administration portals.



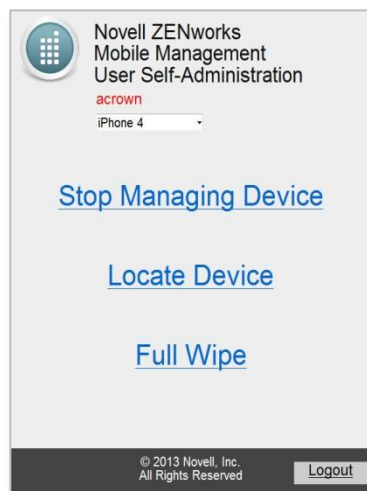
To use the User Self-Administration portals, you will need to obtain the *ZENworks Mobile Management* server address from your administrator. Commit it to memory or note it somewhere.

Accessing the Mobile User Self-Administration Portal

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

Log in with your *ZENworks Mobile Management* 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 *ZENworks Mobile Management* user account **username** and **password**, and leave the domain field blank.



Sample User Self-Administrative Portal views for an iOS User

Accessing the Desktop User Self-Administrative Portal

In the web browser of an Internet-enabled desktop computer, enter `https://<yourZENworksMobileManagementserveraddress>`

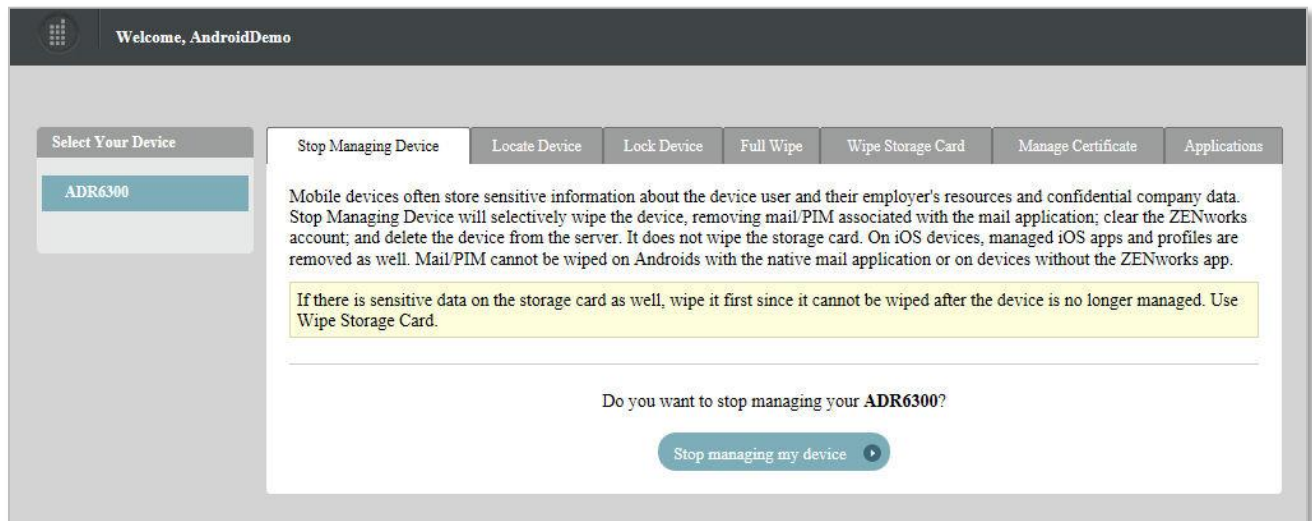
Log in with your *ZENworks Mobile Management* user account credentials:

- 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 *ZENworks Mobile Management* user account **username** and **password**, and leave the domain field blank.

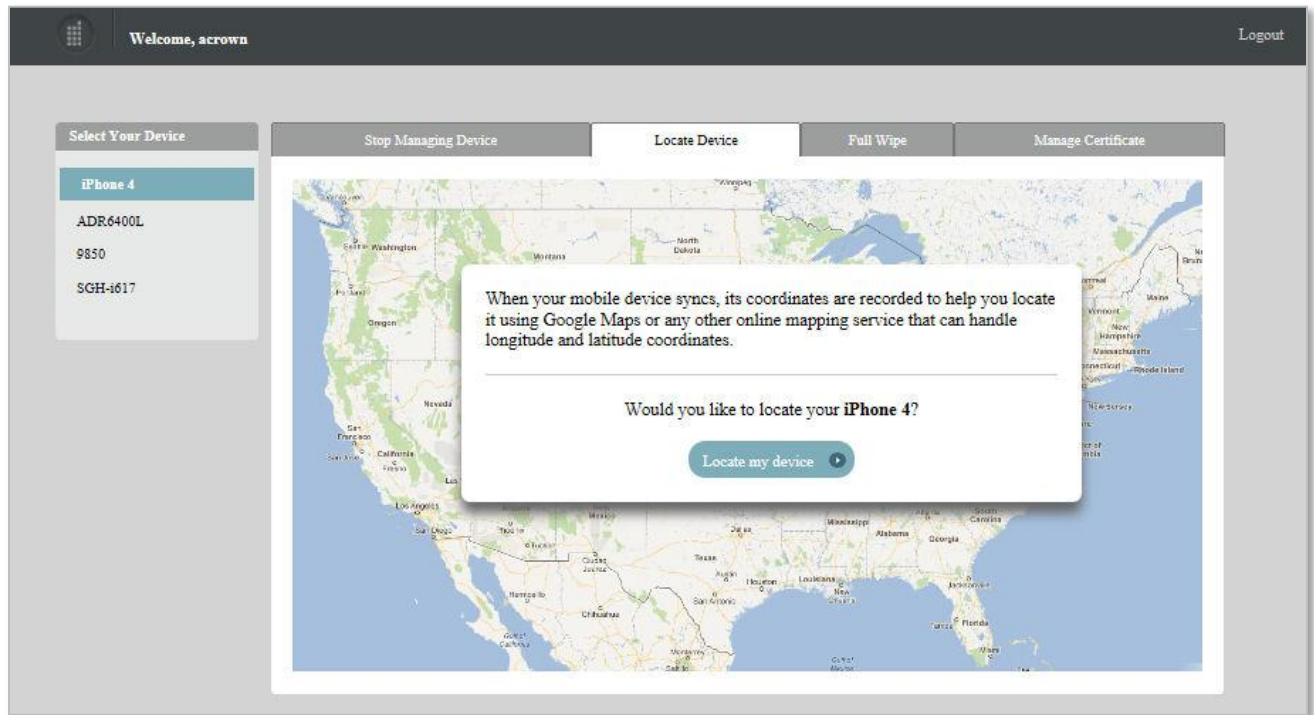


Information about your device is available by selecting the appropriate tab.

Security Actions – Remote security commands you can initiate when a device is potentially compromised, to prevent malicious actions or unwanted access to sensitive data as soon as you become aware of a threat. See [The Security Commands](#) for descriptions of the commands.

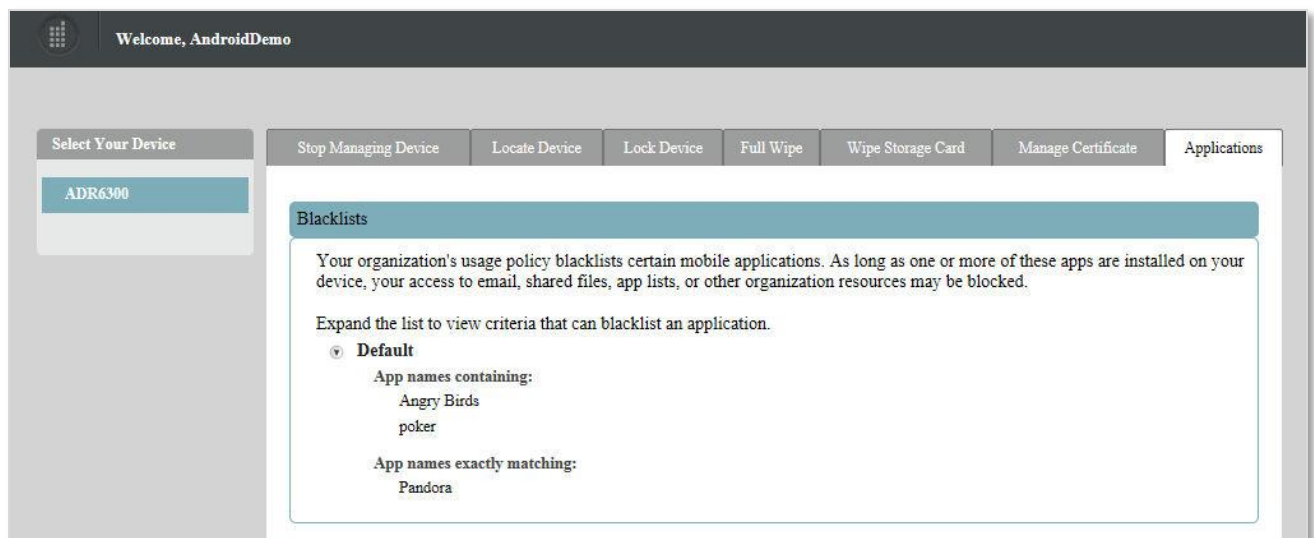


Location – Select the *Locate Device* tab to view the location of the device, reported by the GPS or triangulation on the device. Information is displayed using Google Maps.



Applications – If your organization’s usage policy blacklists or whitelists certain mobile applications, you can see the criteria by which these restrictions are made.

If your organization’s usage policy **blacklists** certain mobile applications, the presence of one or more of these applications on your device may block your access to email, shared files, app lists, or other organization resources.



If your organization's usage policy **whitelists** certain mobile applications, having one or more applications on your device that are not on the list may block your access to email, shared files, app lists, or other organization resources.

The screenshot shows a user interface for mobile device management. At the top, there is a navigation bar with a logo on the left, the text "Welcome, jmartin" in the center, and a "Logout" link on the right. Below the navigation bar is a horizontal menu with several options: "Select Your Device", "Stop Managing Device", "Locate Device", "Lock Device", "Full Wipe", "Wipe Storage Card", "Manage Certificate", and "Applications". The "Applications" option is currently selected. On the left side, there is a sidebar with a "Select Your Device" section containing two items: "Galaxy Nexus" (highlighted) and "SCH-I510". The main content area displays the "Whitelists" section. It features a teal header with the title "Whitelists". Below the header, a text box explains: "Your organization's usage policy permits only selected mobile applications. If apps other than the ones in the whitelist below are installed on your device, your access to email, shared files, app lists, or other organization resources may be blocked." This is followed by the instruction "Expand the list to view apps that are permitted." Below this, there is a section titled "Default" with a dropdown arrow. Under "Default", it lists "App names exactly matching:" followed by a list of applications: "File Manager", "Mileage Expense Log FREE - Mobile Drive Tracker App!", "Skype", and "World Clock".

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, might also vary slightly, based on what the device platform supports. See the chart that follows for details.

KEY:			
Anrd	Android devices	S60	Symbian S60 3 rd 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 multitasking devices	WP	Windows Phone
TD/iOS	iOS multitasking devices with TouchDown	BB10	BlackBerry 10 devices

When you log in to the *ZENworks Mobile Management Self-Administration Portal*, the security actions compatible with your device are displayed. You can perform some or all of the following actions:

Option	Description	Devices Supported
Full Wipe	<p>Users can issue a full wipe command. Functionality varies by device.</p> <p><i>Android w/ native ActiveSync account (requires OS v2.2 or greater):</i> The 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. It does not erase SD card.</p> <p><i>Android w/TouchDown (requires OS v2.2 or greater):</i> The 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. It does not erase SD card.</p> <p><i>Android w/TouchDown using OS v2.0 or 2.1: Full Wipe</i> not available – Use the <i>Selective Wipe</i> option.</p> <p><i>BlackBerry (with NotifySync for BlackBerry):</i> Removes all mail and PIM data associated with the <i>NotifySync</i> application and removes the <i>NotifySync / ZENworks Mobile Management</i> accounts. Locks the device if <i>Require Password</i> is enabled. Erases <i>NotifySync</i> data from the SD card.</p> <p><i>iOS:</i> The 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.</p> <p><i>Symbian:</i> The 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 <i>Mail for Exchange</i> data. Erases the SD card.</p> <p><i>WM:</i> The 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 the SD card only on <i>Professional</i> devices.</p> <p><i>BB10, webOS, and WP:</i> The 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.</p>	<p>ZENworks Mobile Management app: Android, NS/BB, iOS, TD/iOS, TD/A, WM, S60</p> <p>ActiveSync only: BB10, wOS, WP</p>
Stop Managing Device	<p>Un-enrolls the device. Un-enrollment selectively wipes the device, removing mail/PIM associated with the mail application; clears the <i>ZENworks Mobile Management</i> account; and deletes the device from the grid.</p> <p>Android (native): Devices with native mail app only wipe the <i>ZENworks</i></p>	<p>ZENworks Mobile Management app: Anrd, NS/BB, iOS, TD/iOS, TD/A, WM, S60</p>

	<p><i>Mobile Management</i> account. Mail/PIM is not wiped.</p> <p>iOS: Additionally removes managed iOS profiles, thus removing corporate resources and managed apps designated to be removed when the APN profile is removed. (Manually created mail profiles and user-installed apps are not removed.)</p> <p>Devices without <i>ZENworks Mobile Management</i> app: The only action performed is to remove device from the <i>ZENworks Mobile Management</i> server. Mail/PIM is not wiped.</p>	<p>ActiveSync only: BB10, wOS, WP7</p>
Wipe Storage Card	Remotely wipes all data from the device's storage card.	<p>ZENworks Mobile Management app: Android, NS/BB, TD/A, WM</p>
Lock Device	<p>Remotely locks the device, requiring a password to be entered before the device can be used.</p> <p><i>Android or Android w/Touchdown:</i> Requires OS 2.2 or greater.</p>	<p>ZENworks Mobile Management app: Android, NS/BB, TD/A, WM, iOS, TD/iOS</p>
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.	<p>ZENworks Mobile Management app: NS/BB, TD/A, TD/iOS</p>
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.	<p>ZENworks Mobile Management app: Android, NS/BB, iOS, TD/iOS, TD/A, WM</p>
Clear Passcode	The passcode is cleared. If a passcode is required by the user's policy, you are prompted to enter a new passcode.	<p>ZENworks Mobile Management app: iOS, TD/iOS</p>

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.

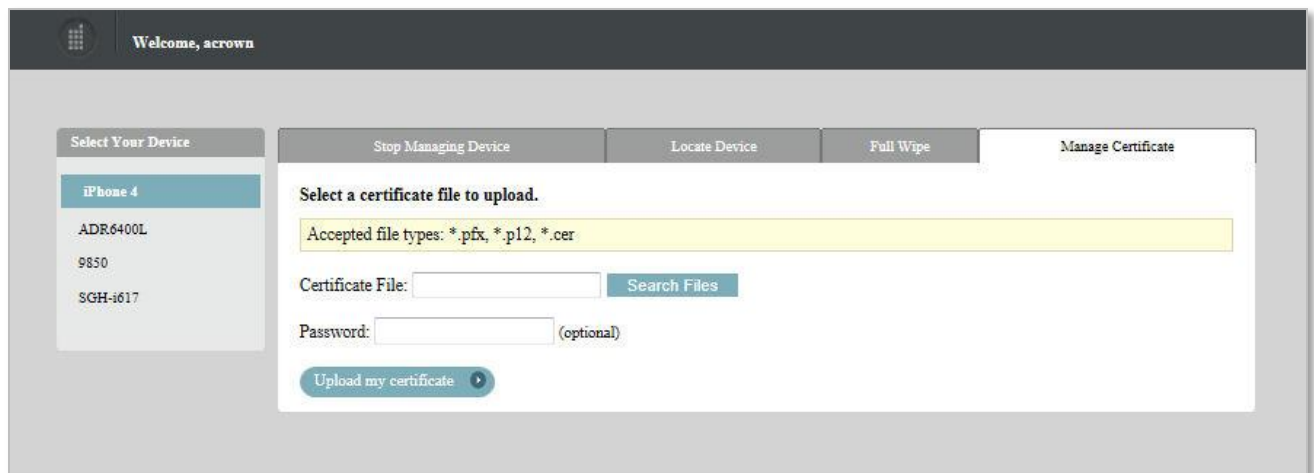
Using the Desktop User Self-Administration Portal

Your administrator will create and upload a certificate for you on the server or 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. A password may be associated with the certificate file.

Uploading the Certificate

1. From your desktop computer 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 .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 devices.



Managing the Certificate

When the certificate has been uploaded, you can download the certificate to your device or you can upload a different certificate file.

Download the certificate to your device.

- If you are using your mobile device browser, click the certificate file name to download the certificate to your device.
- You can also access the Mobile User Self-Administration portal from your device browser to download the certificate: <https://<yourZENworksMobileManagementserveraddress>/mobile>

Upload a different certificate file.

Uploading another certificate replaces the current certificate.

Using the Mobile User Self-Administration Portal

When your system administrator has created and uploaded a client certificate for you on the server, you 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 **User Certificate**.

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



3. Click the file name that appears to begin the certificate installation. The file format will be .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 *ZENworks Mobile Management* device user guide and the *NotifySync for BlackBerry* guide.

[ZENworks Mobile Management for Android](#)

[ZENworks Mobile Management for Android with TouchDown](#)

[ZENworks Mobile Management for iOS Devices](#)

[ZENworks Mobile Management for iOS with TouchDown](#)

[ZENworks Mobile Management for Symbian](#)

[ZENworks Mobile Management for Windows Mobile](#)

[NotifySync for BlackBerry](#)

