User Self-Administration

ZENworks® Mobile Management 3.1.x

March 2015

Novell®

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/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Copyright © 2012-15 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).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (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....7
Security Actions....8
Device Location....8
Applications....9
The Security Commands....11
Client Certificates....13

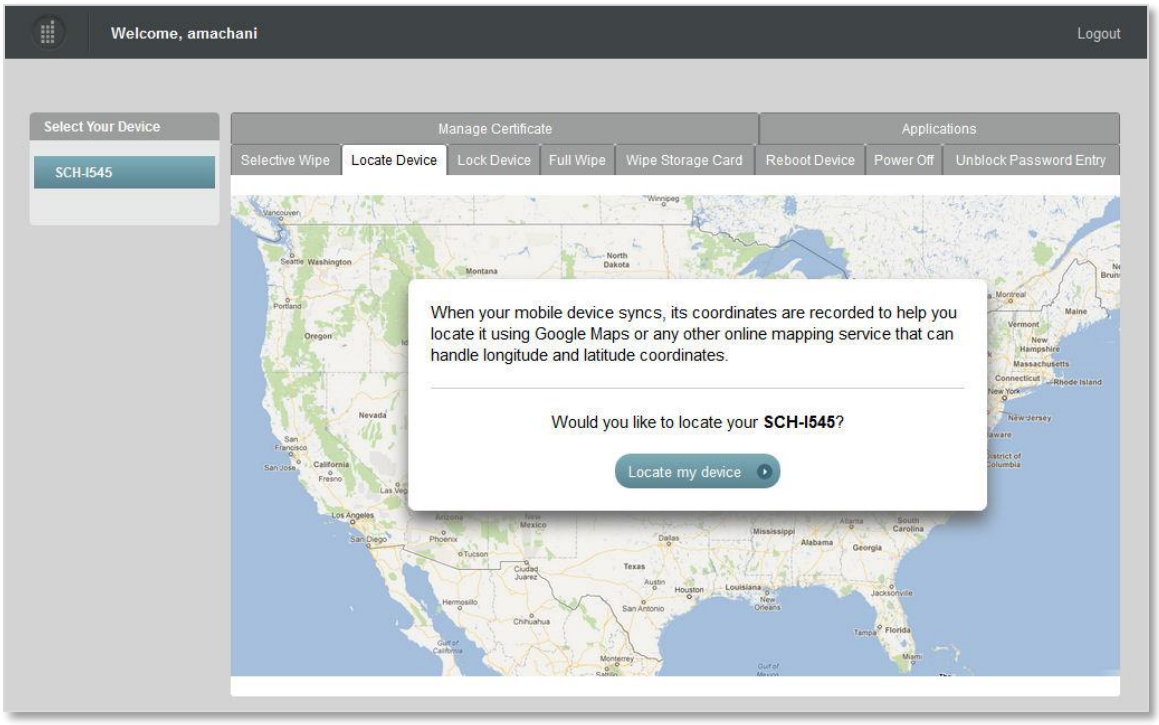
The User Self-Administration Portal

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** and **domain**.
    - Users not interfacing with an ActiveSync server, use your *ZENworks Mobile Management* user account **username**, and leave the domain* field blank.

  * Domain must be supplied (entered as part of a full email address username or in the *Domain* field) if your organization uses an authentication service to identify you as an authorized user.

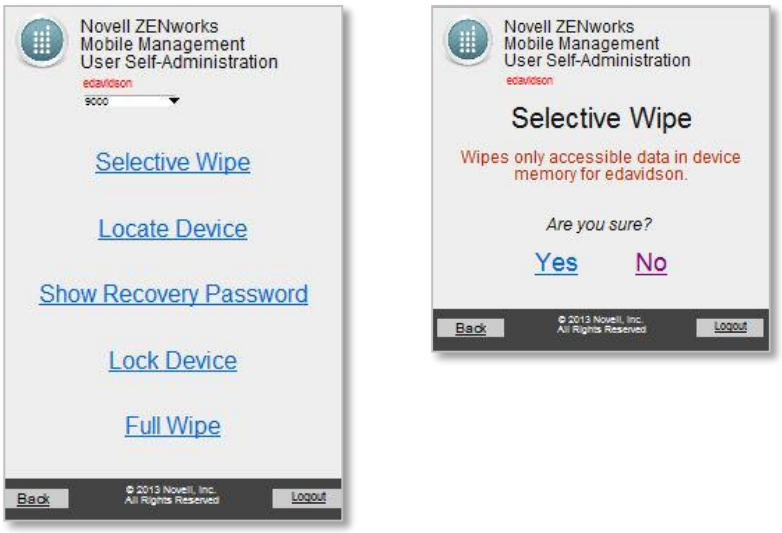
- Select a language to localize the *ZENworks Mobile Management* app. Choose from: English, French, German, Italian, Brazilian Portuguese, Spanish, Swedish, Simplified Chinese, Traditional Chinese, or Japanese.

- If you are redirected to an authentication service. Enter the **Username** and **Password** by which the service identifies you, then tap **Login**.

  Note: These credentials may be different than your ActiveSync server credentials. Consult your administrator.

- Otherwise, enter your ActiveSync account **Password**.

Only the options supported by or available for your device platform will appear in the portal menu.



Sample Mobile 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>*

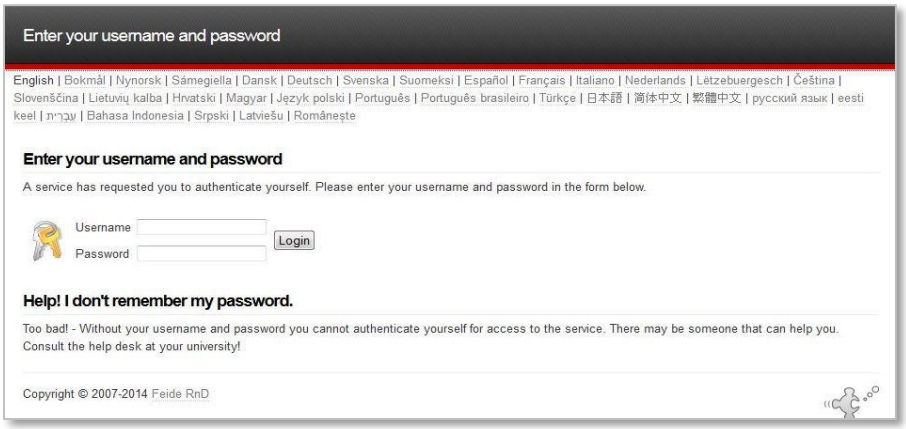
- Log in with your *ZENworks Mobile Management* user account credentials:
  - For users interfacing with an ActiveSync server, use your ActiveSync account **username** and **domain**.
  - Users not interfacing with an ActiveSync server, use your *ZENworks Mobile Management* user account **username** and leave the *domain** field blank.

  * Domain must be supplied (entered as part of a full email address username or in the *Domain* field) if your organization uses an authentication service to identify you as an authorized user.

- Select a language to localize the *ZENworks Mobile Management* app. Choose from: English, French, German, Italian, Brazilian Portuguese, Spanish, Swedish, Simplified Chinese, Traditional Chinese, or Japanese.

- If you are redirected to an authentication service, enter the Username and Password by which the service identifies you, then tap Login.

  Note: These credential may be different than your ActiveSync server credentials. Consult your administrator.



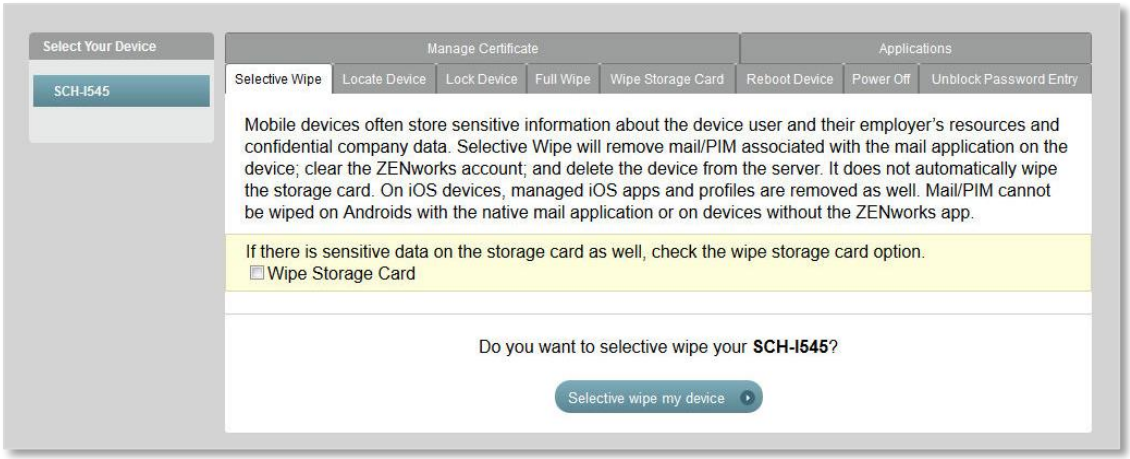
- Otherwise, enter your ActiveSync account **Password**.

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

Only the options supported by or available for your device platform will appear in the tabs.

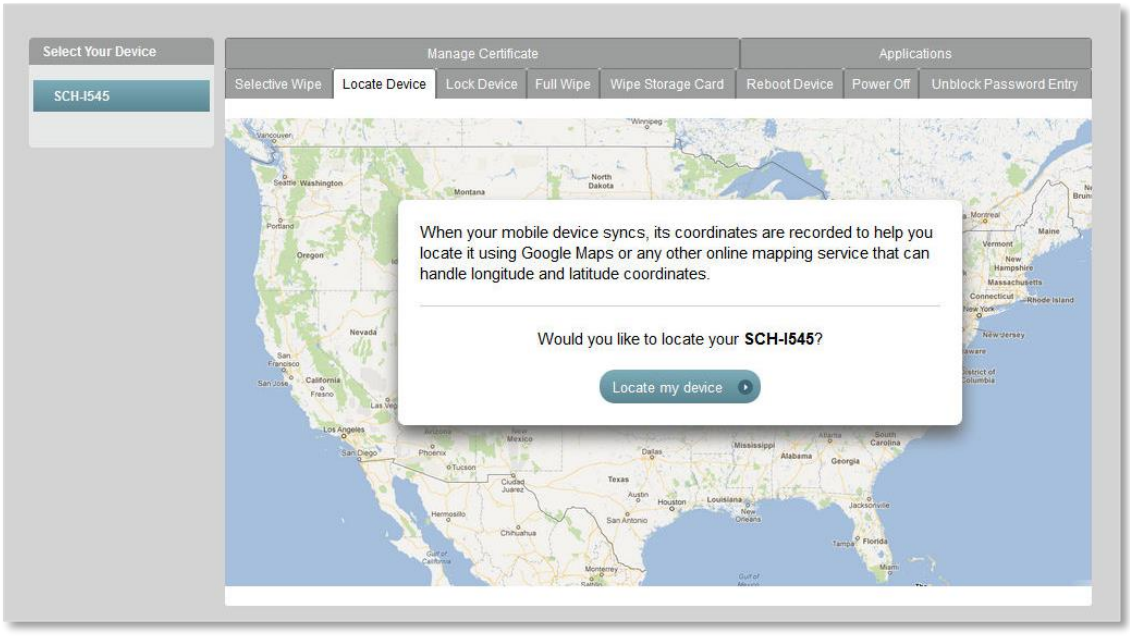
Security Actions

When a device is potentially compromised, you can initiate remote security commands as soon as you become aware of a threat, to prevent malicious actions or unwanted access to sensitive data. See The Security Commands for descriptions of the commands and to determine which device platforms support each command.



Device 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

Managed Apps – Your administrator may compile and make available a list of recommended mobile applications. The *Managed App* option in the User Self-Administration Portal provides one way for iOS device users to access the recommended apps. The list consists of quick links to applications in the App Store or to where in-house enterprise apps are stored, making it convenient to install any one of them on the device. iOS users can also access this page from the *ZENworks Mobile Management* device app using the *Managed Apps* option.

Android and BlackBerry with *NotifySync* users will not see a managed apps list in the User Self-Administration Portal, but can install recommended apps from the *ZENworks Mobile Management* device app using the *Managed Apps* option.

The button beside each app in the list indicates the app's status.

Install indicates the app is available to be installed, but is not required.

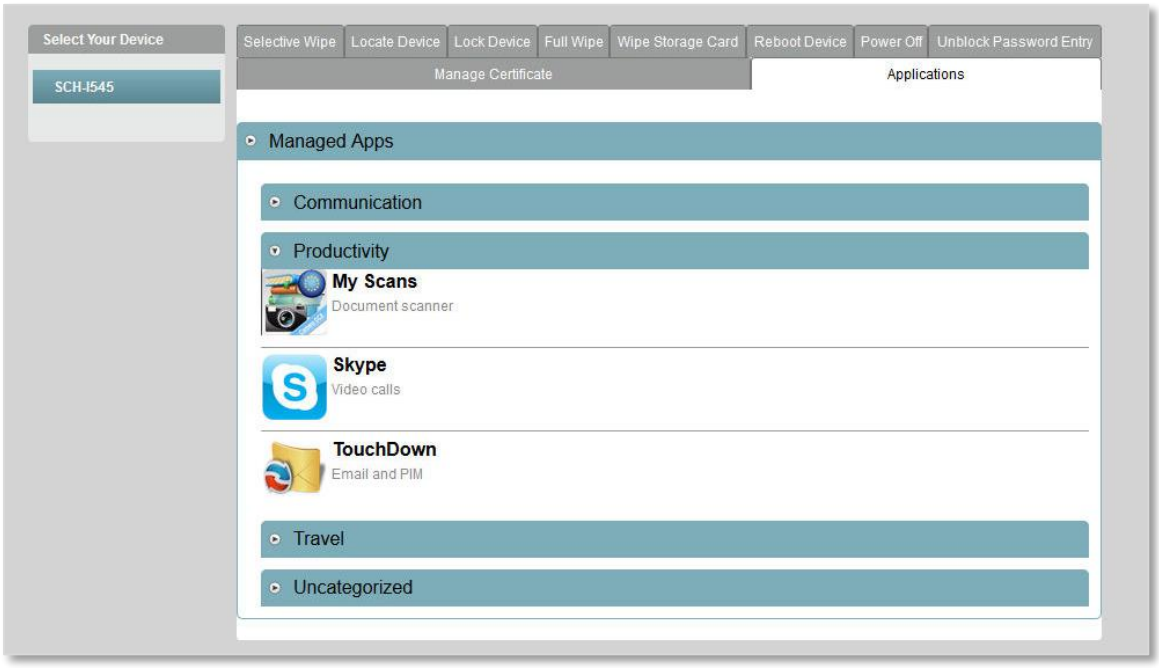
Pending indicates that the app is waiting to be installed. The user must give the server permission from the device.

Installed indicates the app has already been installed.

Required indicates that the app is required by your organization and has automatically prompted you to install the app. A prompt will continue to appear until the app is installed.

Unavailable indicates that the organization has reached its download limit for this application. Contact your organization administrator.

The apps may be listed under categories or may be uncategorized.



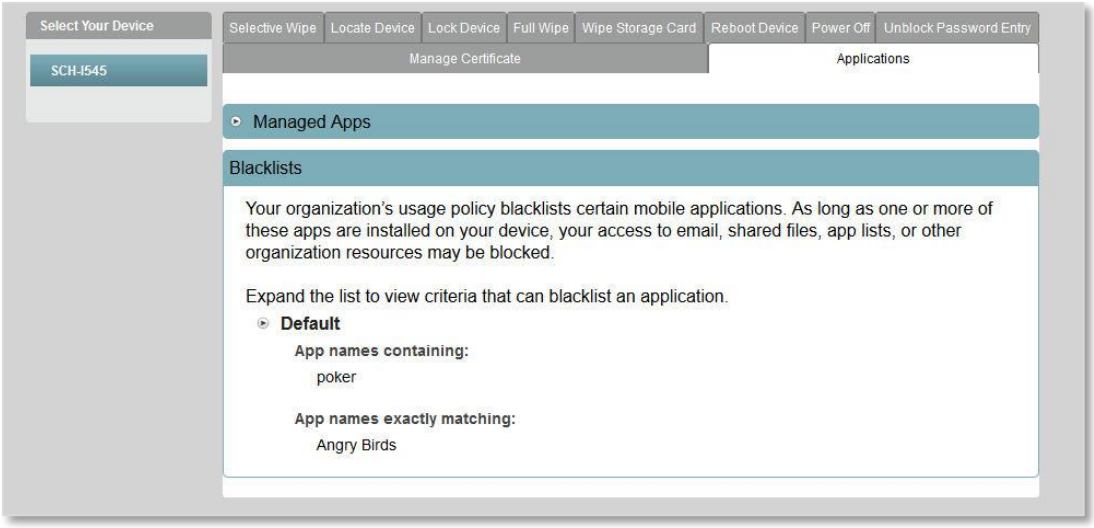
To install an app from the Managed App list:

1. Tap the ***Install*** button beside the app you wish to install. A confirmation pop-up dialog appears. Tap ***OK***.

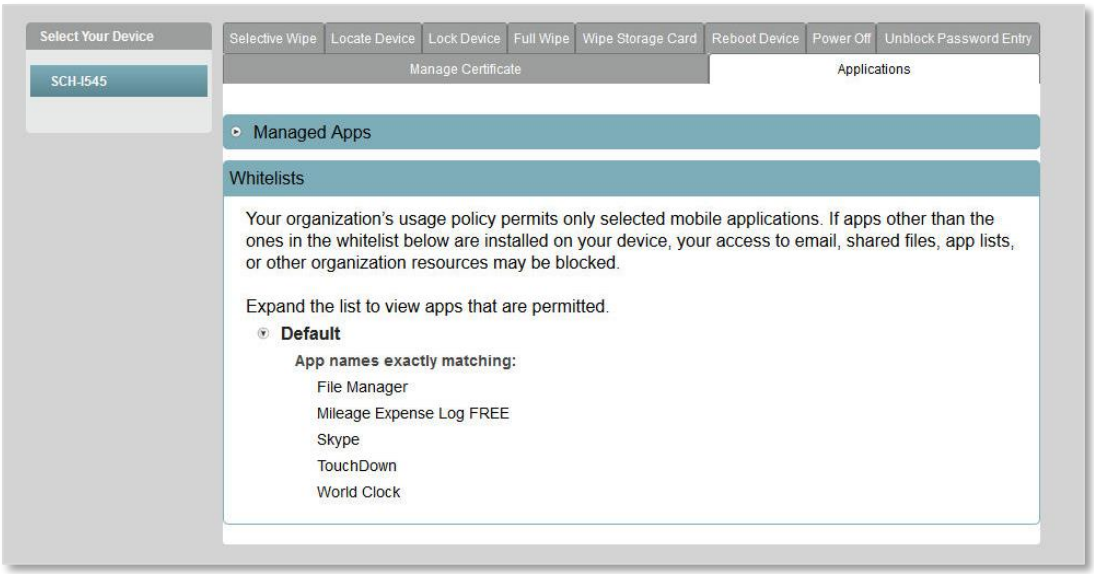
2. On the device, a permissions screen appears. Give the server permission to install the app by tapping ***Install***. You will need to enter your iTunes password as well, unless the app you are installing is an in-house enterprise app.

Blacklists/Whitelists – 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 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	**wOS**	webOS devices
TD/A	Android devices with TouchDown	**WP**	Windows Phone
NS/BB	NotifySync for BlackBerry	**BB10**	BlackBerry 10 devices
iOS	iOS multitasking devices		
TD/iOS	iOS multitasking devices with TouchDown		

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	Users can issue a full wipe command. Functionality varies by device. *Android w/ native ActiveSync account (requires OS v2.2 or greater)*: 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. *Android w/TouchDown (requires OS v2.2 or greater)*: 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. *Android w/TouchDown using OS v2.0 or 2.1: Full Wipe* not available – Use the *Selective Wipe* option. *BlackBerry (with NotifySync for BlackBerry):* Removes all mail and PIM data associated with the *NotifySync* application and removes the *NotifySync* / *ZENworks Mobile Management* accounts. Locks the device if *Require Password* is enabled. Erases *NotifySync* data from the SD card. *iOS:* 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. iOS 7.0.3+ devices enrolled in the Volume Purchase Program : VPP licenses are reclaimed and the user is retired from the program when it is the last iOS 7.0.3+ device associated with the user. *BB10, webOS, and WP:* 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.	**ZENworks Mobile Management app:** Android, NS/BB, iOS, TD/iOS, TD/A **ActiveSync only:** BB10, wOS, WP
Selective Wipe	Un-enrolls the device. Un-enrollment selectively wipes the device, removing mail/PIM associated with the mail application; clears the *ZENworks Mobile Management* account; and deletes the device from the grid. Android (native): Devices with native mail app only wipe the *ZENworks Mobile Management* account. Mail/PIM is not wiped. iOS: Additionally removes managed iOS profiles, thus removing corporate resources and managed apps designated to be removed when the APN	**ZENworks Mobile Management app:** Anrd, NS/BB, iOS, TD/iOS, TD/A

	profile is removed. (Manually created mail profiles and user-installed apps are not removed.) iOS 7.0.3+ devices enrolled in the Volume Purchase Program : VPP licenses are reclaimed and the user is retired from the program when it is the last iOS 7.0.3+ device associated with the user.	
Wipe Storage Card	Remotely wipes all data from the device's storage card.	**ZENworks Mobile Management app:** Android, NS/BB, TD/A
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.	**ZENworks Mobile Management app:** Android, NS/BB, TD/A, iOS, TD/iOS
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.	**ZENworks Mobile Management app:** NS/BB, TD/A, TD/iOS
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.	**ZENworks Mobile Management app:** Android, NS/BB, iOS, TD/iOS, TD/A
Clear Passcode	The passcode is cleared. If a passcode is required by the user's policy, you are prompted to enter a new passcode.	**ZENworks Mobile Management app:** iOS, TD/iOS
Reboot Device	Rebooting a device is a troubleshooting measure that will power off your device and restart it. In the process it returns device software to a known state and often corrects what is causing the issue.	**ZENworks Mobile Management app:** Anrd & TD/A Samsung KNOX devices only
Power Off	Power off your device to conserve its charge.	**ZENworks Mobile Management app:** Anrd & TD/A Samsung KNOX devices only
Unblock Password Entry	If the password entry field to unlock your device has been blocked due to a password violation, you can remove the block by sending this command. This does not reset the password.	**ZENworks Mobile Management app:** Anrd & TD/A Samsung KNOX devices only

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.

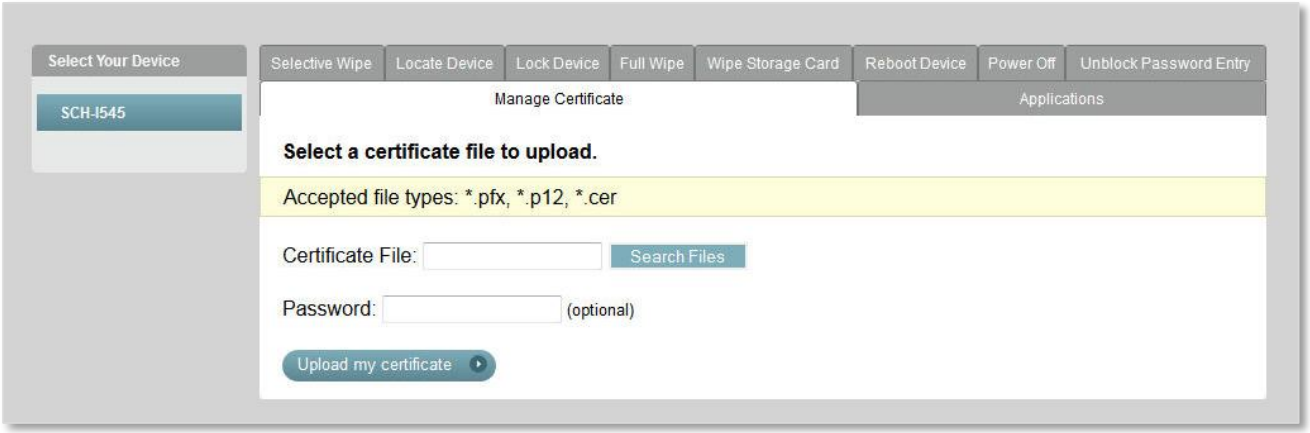
Using the Desktop User Self-Administration Portal

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.

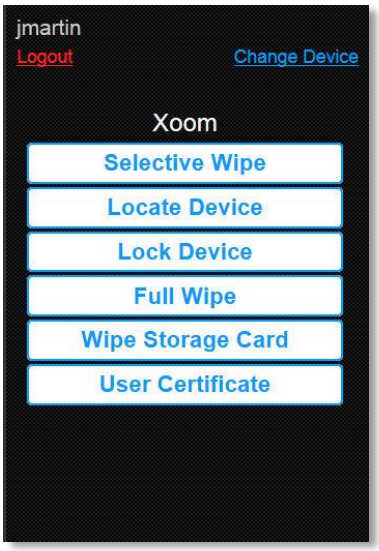
Uploading another certificate replaces the current certificate.

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.



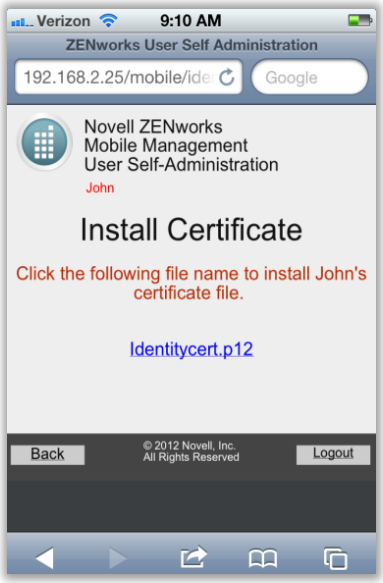
3. Click the file name that appears to begin the certificate installation. The file format will be .cer, .pfx, or .p12.

   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

   NotifySync for BlackBerry