

## Table of Contents

<b>Disclaimer</b> .....	<b>5</b>
<b>What's New?</b> .....	<b>6</b>
<b>Setting Login and Language Preferences</b> .....	<b>7</b>
Saving Login Information .....	7
Setting Your Language Preference .....	7
<b>Navigating the Interface</b> .....	<b>8</b>
Navigation Toolbar .....	8
Sidebar .....	8
Work Area .....	9
Header Bar .....	9
Results Grid .....	9
<b>Customizing Column Layout</b> .....	<b>11</b>
<b>Searching for Information</b> .....	<b>12</b>
<b>Managing Queued Commands and Command History</b> .....	<b>13</b>
<b>About the Self-Service Portal</b> .....	<b>14</b>
Giving Users Access to the Self-Service Portal .....	14
Logging In to the Self-Service Portal .....	14
<b>Working with Computers</b> .....	<b>15</b>
<b>Viewing Computer Details</b> .....	<b>16</b>
<b>Sending Messages to Computers</b> .....	<b>34</b>
<b>Gathering Computer Information</b> .....	<b>35</b>
<b>Working with Mobile Devices</b> .....	<b>36</b>
<b>About Mobile Device Management</b> .....	<b>37</b>
<b>Viewing Device Details</b> .....	<b>38</b>
<b>Locking Devices</b> .....	<b>47</b>
<b>Managing Passcodes on Devices</b> .....	<b>48</b>
<b>Erasing Devices</b> .....	<b>50</b>
<b>Sending Messages to Devices</b> .....	<b>51</b>
<b>Updating Device Information</b> .....	<b>52</b>
<b>Renaming Devices</b> .....	<b>53</b>
<b>Setting Roaming Options for Devices</b> .....	<b>54</b>
<b>Distributing Applications to Devices</b> .....	<b>55</b>

<b>Uninstalling Applications on Devices</b> .....	<b>56</b>
<b>Installing Configuration Profiles on Devices</b> .....	<b>57</b>
<b>Removing Configuration Profiles from Devices</b> .....	<b>58</b>
<b>Installing Provisioning Profiles on Devices</b> .....	<b>59</b>
<b>Removing Provisioning Profiles from Devices</b> .....	<b>60</b>
<b>Setting Device Ownership</b> .....	<b>61</b>
<b>Setting the Enrollment User for Devices</b> .....	<b>62</b>
<b>Setting Organization Information on Devices</b> .....	<b>63</b>
<b>Setting Activation Lock Options</b> .....	<b>64</b>
<b>Setting Custom Field Values</b> .....	<b>65</b>
<b>Retrying Failed Installations</b> .....	<b>66</b>
<b>Adding Devices to Policies</b> .....	<b>67</b>
<b>Working with Policies</b> .....	<b>68</b>
<b>About Policies</b> .....	<b>69</b>
<b>Viewing Policy Details</b> .....	<b>71</b>
<b>Creating Standard Policies</b> .....	<b>72</b>
<b>Creating Smart Policies</b> .....	<b>73</b>
<b>Understanding Filters</b> .....	<b>74</b>
Using the Filter Fields .....	74
Combining Filters .....	74
Removing Filters .....	75
<b>Working with In-House Applications Inside a Policy</b> .....	<b>76</b>
Adding In-House Applications to a Policy .....	76
Removing In-House Applications from a Policy .....	77
<b>Working with Third-Party Applications Inside a Policy</b> .....	<b>78</b>
Adding Third-Party Applications to a Policy .....	78
Removing Third-Party Applications from a Policy .....	79
<b>Working with Configuration Profiles Inside a Policy</b> .....	<b>80</b>
Adding Configuration Profiles to a Policy .....	80
Editing Assignment Rules of Configuration Profiles .....	81
Removing Configuration Profiles from a Policy .....	82
<b>Working with Media Files Inside a Policy</b> .....	<b>84</b>
Adding Media Files to a Policy .....	84

Editing Assignment Rules of Media Files .....	85
Removing Media Files from a Policy .....	86
<b>Working with Actions Inside a Policy .....</b>	<b>87</b>
Adding Actions to a Smart Policy .....	87
Editing Assignment Rules of Actions .....	87
Removing Actions from a Smart Policy .....	88
<b>Editing Policies .....</b>	<b>89</b>
Editing Standard Policies .....	89
Editing Smart Policies .....	90
<b>Deleting Policies .....</b>	<b>92</b>
<b>Working with Assignable Items .....</b>	<b>93</b>
<b>Importing Media Files .....</b>	<b>94</b>
<b>Viewing Media File Details .....</b>	<b>97</b>
<b>Editing Media File Properties .....</b>	<b>99</b>
<b>Deleting Media Files .....</b>	<b>102</b>
<b>Viewing In-House Application Details .....</b>	<b>103</b>
<b>Viewing Third-Party Application Details .....</b>	<b>105</b>
<b>Viewing Electronic Book Details .....</b>	<b>107</b>
<b>Viewing Configuration Profile Details .....</b>	<b>108</b>
<b>Viewing Provisioning Profile Details .....</b>	<b>109</b>
<b>Working with Actions .....</b>	<b>110</b>
<b>Viewing Action Details .....</b>	<b>111</b>
<b>Action: Send Message To Device .....</b>	<b>114</b>
<b>Action: Send Email .....</b>	<b>115</b>
<b>Action: Send SMS .....</b>	<b>116</b>
<b>Action: Set Roaming Options .....</b>	<b>117</b>
<b>Action: Set Activation Lock Options .....</b>	<b>118</b>
<b>Action: Set Wallpaper .....</b>	<b>120</b>
<b>Action: Set Device Name .....</b>	<b>121</b>
<b>Action: Set Custom Field Value .....</b>	<b>122</b>
<b>Action: Update Device Information .....</b>	<b>123</b>
<b>Action: Set Attention Mode .....</b>	<b>124</b>

---

<b>Action: Freeze Device .....</b>	<b>125</b>
<b>Action: Send VPP Invitation .....</b>	<b>126</b>
<b>Action: Register User In VPP .....</b>	<b>128</b>
<b>Action: Retire User From VPP .....</b>	<b>130</b>
<b>Action: Remove Configuration Profile .....</b>	<b>131</b>
<b>Action: Demote To Unmanaged Device .....</b>	<b>132</b>
<b>Editing Actions .....</b>	<b>133</b>
<b>Duplicating Actions .....</b>	<b>134</b>
<b>Deleting Actions .....</b>	<b>135</b>
<b>Working with Custom Fields .....</b>	<b>136</b>
<b>Creating Custom Fields .....</b>	<b>137</b>
<b>Editing Custom Fields .....</b>	<b>138</b>
<b>Duplicating Custom Fields .....</b>	<b>139</b>
<b>Deleting Custom Fields .....</b>	<b>140</b>
<b>Glossary .....</b>	<b>141</b>

## Disclaimer

This documentation, as well as the software described in it, is confidential and contains proprietary information protected by non-disclosure agreements. No part of this documentation may be reproduced in any form or disclosed to any party not bound by a non-disclosure agreement without the express written consent of Absolute® Software Corporation.

Absolute Software Corporation reserves the right to revise this documentation and to periodically make changes in the content hereof without obligation of such revisions or changes unless required to do so by prior agreement.

Information contained herein is believed to be correct, but is provided solely for guidance in product application and not as a warranty of any kind. Absolute Software Corporation assumes no responsibility for use of this information, nor for any infringements of patents or other rights of third parties resulting from the use of this information.

Absolute Software Corporation  
Suite 1600 Four Bentall Centre  
1055 Dunsmuir Street  
PO Box 49211  
Vancouver, British Columbia  
Canada V7X 1K8

©2015 Absolute Software Corporation. All rights reserved. Computrace and Absolute are registered trademarks of Absolute Software Corporation. LoJack is a registered trademark of LoJack Corporation, used under license by Absolute Software Corporation. LoJack Corporation is not responsible for any content herein. All other trademarks are property of their respective owners. For a list of patents issued to Absolute Software Corporation, see [www.absolute.com/patents](http://www.absolute.com/patents).

*Application version: 1.6*

*Last updated (day/month/year): 24/06/2015*

## What's New?

Absolute Manage Web Admin version 1.6 includes the following new and updated functionality:

- A [new area in the application](#) to view computers enrolled on the Absolute Manage Server and access their details
- The ability to [send messages](#) to computers and [collect inventory information](#) from them
- Extension of the [Queued Commands and Command History](#) areas to include commands related to computers
- The introduction of [actions](#), which you can create and assign to smart policies to control what Absolute Manage does with mobile devices when they join a policy
- The ability to create and manage [custom fields](#) for mobile devices, which allow you to extend the predefined list of information items provided by Absolute Manage and build a customized inventory that meets the unique requirements of your organization
- An application programming interface (API) based on the REST architecture, which provides programmatic access to all AM Web Admin functionality (see the API documentation contained in the release package for more information)
- Localization of the Self-Service Portal into Japanese
- Compatibility with Absolute Manage Server version 6.8.1

## Setting Login and Language Preferences

Absolute Manage Web Admin can remember certain preferences you set on the login page, even after you log out of the application and close your browser.

---

**NOTE** If your browser is set to reject cookies, your preferences cannot be saved.

---

### Saving Login Information

To avoid entering your server information and username each time you log in to Absolute Manage Web Admin from the same computer, select the **Remember Me** checkbox on the login page. These details are saved until your browser's cookies are deleted; however, you must still enter your password to log in.

To remove your saved login information, clear the **Remember Me** checkbox before you log in.

### Setting Your Language Preference

When you first visit the login page, Absolute Manage Web Admin is displayed in the default language set for your browser. If Absolute Manage Web Admin does not support your browser's default language, English is used instead.

If you prefer to use a different language than the default, you can easily switch by selecting an available language from the dropdown list on the login page.

## Navigating the Interface





The Absolute Manage Web Admin workspace consists of the following main areas:

- [Navigation Toolbar](#)
- [Sidebar](#)
- [Work Area](#)

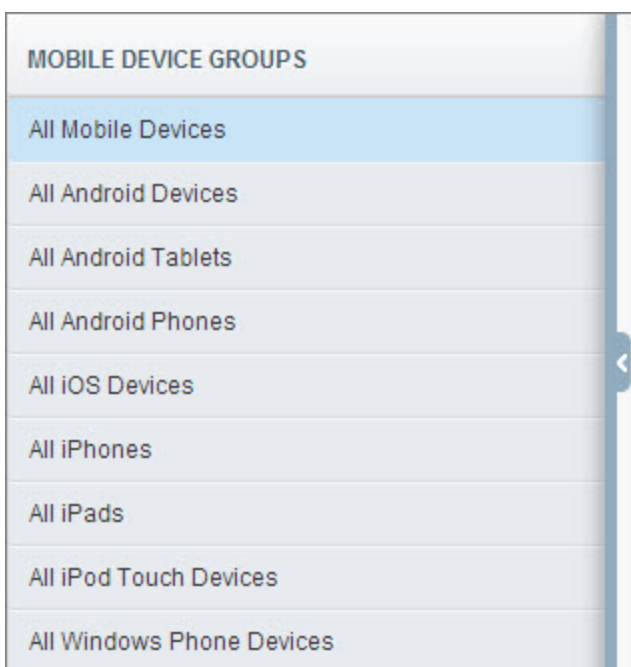
### Navigation Toolbar



All pages in Absolute Manage Web Admin contain a navigation toolbar at the top of the page. This toolbar allows you to quickly move from one area of the application to another. The following table describes the actions you can perform from the toolbar:

Icon	Description
	Click to navigate to the main areas of the application. You can also <a href="#">view your command queue and history</a> from this menu.
	Click to move to the Home page.
	Shows the level of the application you are currently working in. Click to navigate to areas higher in the application hierarchy.
	Click to open product version and login information, or to log out of the application.

### Sidebar

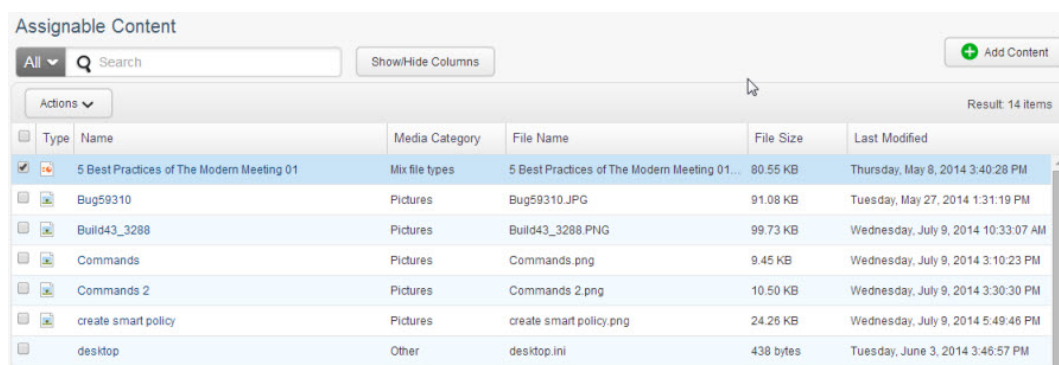




Most pages in Absolute Manage Web Admin contain a sidebar at the left side of the page. The sidebar contains links that let you navigate to items in a particular area. For example, the sidebar in the Mobile Devices area contains links to all of your organization's managed devices, organized by device type. It may also include a search field to let you find a particular item using specific search criteria.

You can hide this sidebar by clicking the tab with the arrow, located on the right edge of the sidebar. To show the sidebar after you have hidden it, click the tab again.

## Work Area



Type	Name	Media Category	File Name	File Size	Last Modified
	5 Best Practices of The Modern Meeting 01	Mix file types	5 Best Practices of The Modern Meeting 01...	80.55 KB	Thursday, May 8, 2014 3:40:28 PM
	Bug59310	Pictures	Bug59310.JPG	91.08 KB	Tuesday, May 27, 2014 1:31:19 PM
	Build43_3288	Pictures	Build43_3288.PNG	99.73 KB	Wednesday, July 9, 2014 10:33:07 AM
	Commands	Pictures	Commands.png	9.45 KB	Wednesday, July 9, 2014 3:10:23 PM
	Commands 2	Pictures	Commands 2.png	10.50 KB	Wednesday, July 9, 2014 3:30:30 PM
	create smart policy	Pictures	create smart policy.png	24.26 KB	Wednesday, July 9, 2014 5:49:46 PM
	desktop	Other	desktop.ini	438 bytes	Tuesday, June 3, 2014 3:46:57 PM

Typically, the work area is where you view items and perform actions on them. The work area encompasses the frame on the right side of the page, including its header bar and results grid.

### Header Bar

The header bar contains the following components:

- Title of the page or item: for example, if you navigate to **Assignable Items > Configuration Profiles**, the name of the page in the header bar is Assignable Configuration Profiles.
- Search field: lets you search for individual items using specific search criteria. For example, in the Mobile Devices area, you can search for all managed devices running a specific version of an operating system.
- Work area toolbar: contains controls specific to the area you are working in. For example, in the Mobile Policies area, you can click the Add Policy button to create a policy or a smart policy.
- Help button: opens the online help. The help is context sensitive, so when you open it, you see information that is relevant to the page or dialog you are currently working in.

### Results Grid

On most pages in Absolute Manage Web Admin, the bottom portion of the work area contains a results grid. The results grid is a table of rows and columns that organizes the information you requested to view. For example, when you view all managed devices in the Mobile Devices area, the devices are presented in the results grid. Depending on the area you are working in, you may be able to perform the following actions on the content in the results grid:

- View the details of an individual item
- Carry out actions on one item or on multiple items simultaneously
- Navigate multiple pages of results
- [Adjust the columns](#)

You can also change how the results within the grid are sorted:


- Results are currently sorted by the column with the icon in its column header.

- To sort the results by another column, click the applicable column header.
- To reverse the sort order, click the column header again. The icon indicates whether the list is sorted in ascending (▲) or descending (▼) order.

## Customizing Column Layout

You can customize the information included in the results grid by showing and hiding columns. You can also change a column's width and position within the results grid. The system remembers your customized layout, even after you log out.


➔ To customize the column layout of the results grid:

1. Navigate to the area where you want to customize the results grid.
2. Click **Show/Hide Columns**.
3. In the Show/Hide Columns dialog, update the columns by performing one or more of the following steps:
  - To add columns to the results grid:
    - i) In the search field under Available Columns, type all or part of the column name you want add. The list of Available Columns updates dynamically as you type. Or, leave this field empty to select from all available columns.
    - ii) Drag the column name from the Available Columns list to the Include Columns list.
  - To remove columns from the results grid, do one of the following:
    - In the Include Columns list, click the  icon next to the column you want to remove.
    - Drag the column name from the Include Columns list to the Available Columns list.
  - To change the column order, in the Include Columns list, do the following:
    - To move a column farther left in the results grid, drag the column toward the top of the list.
    - To move a column farther right in the results grid, drag the column toward the bottom of the list.
4. When you are satisfied with your changes, click **Done**. The Show/Hide Columns dialog closes.
5. To change the width of a column in the results grid, drag the boundary on the right side of the column header until the column reaches your preferred width.

## Searching for Information

Many pages within Absolute Manage Web Admin include a search field that allows you to quickly find information using specific search criteria.

➔ To search for information within the results grid:

1. Navigate to the area you want to search. All available information is included in the results grid by default.
2. To search for specific results, click  next to the search field and select a search criterion from the list.

---

**NOTE** The list of available search criteria depends on the available columns in the area you are working in. Typically, if a column is visible in the results grid, you can use it as a search criterion.

---

3. In the search field, type all or part of the search keyword you want to use to find the information.

Search results are updated dynamically in the results grid as you type.

## Managing Queued Commands and Command History


You can view information about the commands that Absolute Manage Web Admin users have issued to mobile devices and computers within the following areas of the application:

- **Queued Commands:** Contains information related to commands sent from Absolute Manage Web Admin that have not yet been carried out on the target devices and are still pending execution. A command may enter this queue because the target device is unavailable at the time the command is initiated.
- **Command History:** Contains information related to commands sent from Absolute Manage Web Admin that have been completed (successfully or unsuccessfully) on the target devices. If there were any errors during the execution of a command, they show on this page.

You can also delete commands if you no longer want them to be listed on these pages:

- Deleting a command from the command history simply removes it from the results grid.
- Deleting a command from the queue not only removes it from the results grid, but may also prevent it from being carried out on the target device if the system has not yet pushed the command to the device.

➔ To view queued commands or command history:


1. In the top left corner of the screen, click .
2. Click **Queued Commands** or **Command History** from the menu.
3. In the Device Type sidebar, select whether you want to view commands for **Computers** or **Mobile Devices**.
4. To quickly find specific commands within the results grid, you can use the search field to narrow the commands listed by specific criteria. Search results are updated dynamically as you type.

---

**NOTE** You may need to click your browser's refresh button to see updated information in the results grid.

---


➔ To delete queued commands or command history:

1. In the top left corner of the screen, click .
2. Click **Queued Commands** or **Command History** from the menu.
3. In the Device Type sidebar, select whether you want to delete commands for **Computers** or **Mobile Devices**.
4. Select the checkbox of each command you want to delete.

---

**NOTE** Deleting a queued command may prevent it from being carried out on the target device if the system has not yet pushed the command to the device.

---

5. Click .
6. Click **Delete Command**.
7. Click **OK** to close the confirmation message.

## About the Self-Service Portal

Absolute Manage Web Admin is bundled with a Self-Service Portal that allows your device users to remotely manage computers and mobile devices enrolled under their account. Encouraging the use of the Self-Service Portal can empower your users to be more self-sufficient with resolving their own issues, potentially reducing the effort required for IT support.

The management tasks that users can carry out in the Self-Service Portal vary by device platform and include the following:

- Viewing detailed information about their device
- Locking their device to prevent unauthorized access
- Clearing and setting passcodes
- Sending messages to their device
- Erasing their device if it is lost or stolen

## Giving Users Access to the Self-Service Portal

Your device users must be considered "enrollment users" in Absolute Manage to use the Self-Service Portal. For information on importing enrollment users and enrolling their devices in Absolute Manage, see the *Absolute Manage User Guide*.

If you decide you want to give your device users access to the Self-Service Portal, you must communicate the Portal's web address to them. This web address is typically as follows: <https://<address>/mylogin/> (for example, <https://amwebadmin.company.com/mylogin/>). A direct link to the Self-Service Portal is also available at the bottom right of the Absolute Manage Web Admin login page.

You may also want to provide your device users with additional information on how to log in to the Self-Service Portal. After they log in, device users can access the Help to guide them through the steps of each task they can perform.

## Logging In to the Self-Service Portal

➔ To log in to the Self-Service Portal:

1. Enter the web address for the Self-Service Portal in your browser.

---

**NOTE** You can also select the **Self-Service Portal** link at the bottom right of the Absolute Manage Web Admin login page.

---

2. On the Self-Service Portal login page, enter the following information:
  - **Username** – The username associated with your enrollment user account in Absolute Manage
  - **Password** – The password associated with your enrollment user account in Absolute Manage
  - **Domain Name** – The domain associated with your enrollment user account in Absolute Manage
3. To avoid entering your user information each time you log in to the Self-Service Portal from the same computer, select the **Remember Me** checkbox.
4. Click **Log In**.

## Working with Computers

Use the Computers area to view the computers in your IT deployment and perform administrative actions on these devices.

When you first visit this area, computers of all types are listed. If you are only concerned with computers of a specific type, you can filter this list by selecting one of the following device groups from the Computers sidebar:

- All Computers
- PCs
- Macs

You can also [search for individual devices](#) using specific criteria in the Search field, as well as [customize the information](#) included in the results grid.

From the Computers area, you can perform the following tasks:

- [Viewing Computer Details](#)
- [Sending Messages to Computers](#)
- [Gathering Computer Information](#)

## Viewing Computer Details

The Computer Details page lists all available information on a computer, including its hardware profile, installed software, and network adapters.

➔ To view a computer's details:

1. Go to the **Computers > All Computers** page for a list of all your organization's computers.
2. In the results grid, click the computer whose details you want to view.

The Computer Details page opens. The following table provides a summary of device information available on this page:

Field	Description
OS Platform	The type of operating system used on the computer
OS Version	The operating system's version number
Last Heartbeat	The date and time when the last heartbeat signal was received from the agent installed on the computer
Record Creation Date	The date and time when the record for this computer was created on the Absolute Manage Server
Agent Active IP	<p>The computer's IP address, as reported by the agent during the last successful contact and recorded on the Absolute Manage Server</p> <hr/> <p><b>NOTE</b> If the computer has multiple IP addresses, this field will contain "n/a".</p> <hr/>
Agent Version	The version number of the Absolute Manage agent installed on the computer
Agent Build Number	The build number of the Absolute Manage agent installed on the computer
Agent Serial Number	The unique serial number of the Absolute Manage agent installed on the computer
Computer Online	Indicates whether the computer has sent its last scheduled heartbeat signal
SD Server Address	The IP address or DNS name of the software distribution server specified for this computer
LM Server Address	The IP address or DNS name of the license monitoring server specified for this computer
SD Server Check Interval	The interval, in minutes, in which the Absolute Manage agent is set to check the software distribution server for new installation packages
LM Server Check Interval	The interval, in minutes, in which the Absolute Manage agent is set to check for changes to license specifications on the license monitoring server
Included in OS Patch Management	Indicates whether the agent is set to check for operating system and software patches from Apple or Microsoft and install them using Absolute Manage's software distribution feature



Field	Description
Included in Third-Party Patch Management	Indicates whether the agent is set to check for software patches for supported third-party software and install them using Absolute Manage's software distribution feature
Use Only Absolute Manage for OS Updates	Indicates whether the computer receives operating system updates only through Absolute Manage's patch management and not through Software Update (OS X) or Windows Update (Windows)
Absolute Remote Enabled	Indicates whether the screen sharing function of the agent is enabled on this computer
Absolute Remote Port	The port over which the agent accepts screen-sharing connections
Absolute Remote User Confirmation Required	Indicates whether screen-sharing requests must be accepted by the computer's user before the agent establishes the connection
Computer Ownership	The type of owner the computer has: the company, the user, or a guest
Computer Enrollment Date	The date (if any) when this computer was enrolled in MDM through Absolute Manage
Computer Enrolled in MDM	Indicates whether this computer has been enrolled in MDM through Absolute Manage
Computer Enrolled via Enrollment Program	Indicates whether this computer was enrolled in MDM through an enrollment program (as opposed to having been enrolled by other means)
Computer Enrollment Program Registration Date	The date when the computer was registered in the enrollment program (available only for computers enrolled in MDM)
Computer Enrollment Profile Assignment Date	The date when the current enrollment profile was assigned to the computer (available only for computers enrolled in MDM)
Computer Enrollment Profile UUID	The UUID of the enrollment profile assigned to this computer (available only for computers enrolled in MDM)
Computer Enrollment Status	<p>Indicates whether the computer is part of Apple's device enrollment program and provides the status of enrollment. This field can have the following values:</p> <ul style="list-style-type: none"> <li>• <b>not in enrollment program</b> – the device has not been entered into any enrollment program</li> <li>• <b>not assigned</b> – the device is part of an enrollment program, but no enrollment profile is currently assigned to the device</li> <li>• <b>assigned</b> – an enrollment profile has been assigned to the device but the device has not yet been enrolled in MDM</li> <li>• <b>installed</b> – the enrollment profile has been installed on the device; that is, the device has been enrolled in MDM and the profile options have taken effect</li> </ul>

Field	Description
Computer Device Identifier (UDID)	The target identifier (a unique internal ID) of the managed computer (available only for computers enrolled in MDM)
Computer Is Tracked	Indicates whether this computer is currently being monitored through Absolute Manage's computer tracking feature
Client Information 1–10	Information fields for user-definable content. These fields can contain any type of text, as specified by administrators or local users.  <b>NOTE</b> The actual names of these fields may vary.

3. To view additional computer details, click the **Hardware**, **CPU**, **System Software**, **Memory**, **Volumes**, **Network Adapters**, **Missing Patches**, **Installed Software**, and **Installed Profiles** tabs.

The following table provides a summary of computer information available within these tabs:

Field	Applies To	Description
<b>Hardware</b>		
Computer Serial Number	All computers	The serial number of the computer  <b>NOTE</b> Some Windows-based computers may not have a serial number.
Primary MAC Address	All computers	The MAC address of the computer's current primary network connection
Date & Time	All computers	The date and time of the computer's internal clock, as reported during the last heartbeat signal from the agent  <b>NOTE</b> You can find out the difference between the computer's local clock and the server's clock by comparing this field and the <b>Last Heartbeat</b> field (both display the same point in time measured by the two different clocks).
Boot ROM Information	All computers	The information string from the computer's boot ROM. The exact contents and formatting of this string depend on the ROM's vendor.
Memory Slots	All computers	The number of slots for RAM on the computer's motherboard
Memory Module Count	All computers	The number of RAM modules installed in the computer
Physical Memory	All computers	The amount of actual RAM installed in the computer
Swap Space Total	All computers	The size of the swap space that is currently reserved on the computer's hard disk

Field	Applies To	Description
Swap Space Used	All computers	The current amount of data that has been swapped to disk on the computer
Swap Space Free	All computers	The amount of swap space that has been reserved on the computer's hard disk but is currently unused
Swap Space Encrypted	OS X computers only	Indicates whether encryption for the swap file has been enabled
Volume Count	All computers	The number of volumes that are mounted on the computer
ATA Device Count	All computers	The number of ATA devices that are connected to the computer and powered on
SCSI Device Count	All computers	The number of SCSI devices that are connected to the computer and powered on
FireWire Device Count	All computers	The number of FireWire devices that are connected to the computer and powered on
USB Device Count	All computers	The number of USB devices that are connected to the computer
PCI Device Count	All computers	The number of PCI cards that are installed in the computer
Display Count	All computers	The number of display devices that are connected to and recognized by the computer
BIOS Date	Windows computers only	The creation date of the computer's BIOS, as stored in the BIOS
BIOS Vendor	Windows computers only	The creator of the computer's BIOS
BIOS Version	Windows computers only	The version number of the computer's BIOS
BIOS Type	Windows computers only	The type of BIOS active on the computer: legacy or UEFI
SMBIOS Version	Windows computers only	The version number of the computer's System Management BIOS
Mainboard Manufacturer	Windows computers only	The vendor of the motherboard used in the computer
Mainboard Product Name	Windows computers only	The motherboard's name as specified by its vendor
Mainboard Serial Number	Windows computers only	The motherboard's serial number
Mainboard Type	Windows computers only	The type of the motherboard used in the computer, as specified by its vendor

Field	Applies To	Description
Mainboard Version	Windows computers only	The version number of the motherboard used in the computer
Mainboard Asset Tag	Windows computers only	The asset tag of the computer's motherboard
System Enclosure Manufacturer	Windows computers only	The vendor of the computer's case
System Enclosure Serial Number	Windows computers only	The serial number of the computer's case
System Enclosure Type	Windows computers only	The type of the computer's case
System Enclosure Version	Windows computers only	The version number of the computer's case
System Enclosure Asset Tag	Windows computers only	The asset tag of the computer's case
Computer Manufacturer	Windows computers only	The producer of the computer
Computer Version	Windows computers only	The version number of the computer
Computer Model	Windows computers only	The model name of the computer
Computer Service Tag	Windows computers only	The service tag of the computer
Computer Type	OS X computers only	The exact model of the computer
SMC Version	OS X computers only	The version number of the computer's SMC firmware (Intel-based Macs only)
Computer Age	OS X computers only	The age of the computer; that is, the time that has elapsed since its production
Computer Production Date	OS X computers only	The date when the computer was manufactured
Computer Production Factory	OS X computers only	The site where the computer was manufactured
Apple Product Name	OS X computers only	<p>The official product name Apple uses for this type of computer</p> <hr/> <p><b>NOTE</b> The content of this field is downloaded from an Apple server, based on the computer's serial number. It is therefore available only if the computer had an internet connection at least once after the Absolute Manage agent was installed on it. This field is updated every ten days as long as the computer can contact Apple's server.</p> <hr/>

Field	Applies To	Description
Computer Purchase Date	OS X computers only	<p>The date when the computer was purchased, according to the manufacturer's files</p> <hr/> <p><b>NOTE</b> This information is retrieved from a server of the computer's vendor and is available only if the computer had an internet connection at least once after the Absolute Manage agent was installed on it. In addition, not all vendors provide this information.</p> <hr/>
Computer Warranty Info	All computers	<p>The computer's current warranty status</p> <hr/> <p><b>NOTE</b> This information is retrieved from a server of the computer's vendor and is available only if the computer had an internet connection at least once after the Absolute Manage agent was installed on it. In addition, not all vendors provide this information.</p> <hr/>
Computer Warranty End	All computers	<p>The date when the computer's warranty ends. A value of "n/a" indicates either that no information is available or that the warranty has expired.</p> <hr/> <p><b>NOTE</b> This information is retrieved from a server of the computer's vendor and is available only if the computer had an internet connection at least once after the Absolute Manage agent was installed on it. In addition, not all vendors provide this information.</p> <hr/>
<b>CPU</b>		
OS Platform	All computers	The type of operating system used on the computer
Processor Type	All computers	The main processor's series and version
Processor Vendor	All computers	The main processor's manufacturer
Processor Speed	All computers	The processor's clock rate
Bus Speed	All computers	The clock speed the processor's front-side bus
Physical Cores	All computers	<p>The total number of main processor cores installed in the computer</p> <hr/> <p><b>NOTE</b> With Windows-based machines, physical cores that have been disabled during the boot process or in Task Manager are not reported here.</p> <hr/>

Field	Applies To	Description
Active Cores	All computers	<p>The number of currently enabled main processor cores in the computer. This number may be lower than <b>Physical Cores</b> if individual cores are disabled (for example, to lower power consumption).</p> <p><b>NOTE</b> With Windows-based machines, processors that have been disabled in Task Manager are not reported here.</p>
Cores per Processor	OS X computers only	The number of cores that the main processor has
Processor L1 Data Cache	All computers	The size of the processor's level 1 cache for data
Processor L1 Instruction Cache	All computers	The size of the processor's level 1 cache for instructions
Processor L2 Data Cache	All computers	The size of the processor's level 2 cache for data
Processor L2 Instruction Cache	All computers	The size of the processor's level 2 cache for instructions
Processor L3 Cache	All computers	The size of the processor's level 3 cache
Processor Supports Hyperthreading	All computers	Indicates whether the processor support Intel's Hyper-Threading Technology
Processor Hyperthreading Enabled	All computers	<p>Indicates whether Intel's Hyper-Threading Technology is currently enabled</p> <p><b>NOTE</b> With Windows-based machines, information in this field may not be reliable if processors have been disabled in Task Manager.</p>
Processor Has MMX	Windows computers only	Indicates whether the processor supports Intel's MMX instruction set
Processor Has 3DNow	Windows computers only	Indicates whether the processor supports AMD's 3DNow! instruction set
Processor Has SSE	Windows computers only	Indicates whether the processor supports Intel's SSE instruction set
Processor Has SSE2	Windows computers only	Indicates whether the processor supports Intel's SSE2 instruction set
Processor Has SSE3	Windows computers only	Indicates whether the processor supports Intel's SSE3 instruction set
Processor Family	Windows computers only	The family ID of the main processor, as specified by the manufacturer
Processor Model	Windows computers only	The model ID of the main processor within its family, as specified by the manufacturer

Field	Applies To	Description
Processor Stepping	Windows computers only	The stepping ID of the main processor within its model, as specified by the manufacturer
<b>System Software</b>		
OS Platform	All computers	The type of operating system used on the computer
OS Version	All computers	The operating system's version number
OS Build Number	All computers	The build number of the operating system
OS Language	All computers	<p>The user interface language of the operating system</p> <hr/> <p><b>NOTE</b> For single-language operating systems (such as a standard Windows XP installation), this field contains the installed language. For operating systems that can dynamically change the interface language (such as OS X or Windows 7), this field contains the currently chosen language.</p> <hr/>
Computer Boot Time	All computers	The date and time when the computer was last booted
Computer Uptime	All computers	The time since the computer was last booted, in hours and minutes. This information is current as of the last inventory update.
Current User Name	All computers	The full name of the user who is currently logged in to the computer. If no user is logged in, this field is empty.
Current User Account	All computers	The name of the current user's account under which he or she is logged in
Current User Is Admin	All computers	Indicates whether the currently logged-in user has administrator rights on the computer
Last User Account	All computers	The name of the account under which the current user is logged in to the computer. If no user is logged in, the name of the account of the last user who was logged in is shown.
Last User Name	All computers	The full name of the user who is currently logged in to the computer. If no user is logged in, the name of the user who was last logged in is shown.
AD Computer Organizational Unit	All computers	The name of the Active Directory organizational unit to which the computer belongs

Field	Applies To	Description
AD Computer Organizational Unit Path	All computers	The path of the Active Directory organizational unit to which the computer belongs
AD User Organizational Unit	All computers	The name of the Active Directory organizational unit to which the computer's current user belongs
AD User Organizational Unit Path	All computers	The path of the Active Directory organizational unit to which the computer's current user belongs
Disk Encryption Product	All computers	<p>The name of the disk encryption software used on the computer, if any</p> <hr/> <p><b>NOTE</b> This information is reported for Windows XP and Windows Server 2003 clients only if .NET 2.0 or .NET 3.5 is installed on them.</p> <hr/>
Disk Encryption Version	All computers	<p>The version of the disk encryption software used on the computer</p> <hr/> <p><b>NOTE</b> This information is reported for Windows XP and Windows Server 2003 clients only if .NET 2.0 or .NET 3.5 is installed on them.</p> <hr/>
Disk Encryption Status	All computers	<p>The state of the disk encryption on the computer as reported by the disk encryption software</p> <hr/> <p><b>NOTE</b> This information is reported for Windows XP and Windows Server 2003 clients only if .NET 2.0 or .NET 3.5 is installed on them.</p> <hr/>
Disk Encryption Algorithm	All computers	<p>The encryption algorithm used by the disk encryption software, as reported by the software</p> <hr/> <p><b>NOTE</b> This information is reported for Windows XP and Windows Server 2003 clients only if .NET 2.0 or .NET 3.5 is installed on them.</p> <hr/>
Disk Encryption Key Size	All computers	<p>The length, in bits, of the encryption key used, as reported by the disk encryption software</p> <hr/> <p><b>NOTE</b> This information is reported for Windows XP and Windows Server 2003 clients only if .NET 2.0 or .NET 3.5 is installed on them.</p> <hr/>



Field	Applies To	Description
GMT Delta	All computers	The difference between UTC (Coordinated Universal Time) and the computer's clock
Daylight-Saving Time	All computers	Indicates whether DST (Daylight Saving Time) is in effect on the computer
Fast User Switching Enabled	All computers	Indicates whether fast switching between user accounts (that is, without having to close all applications and logging out before using a different account) is enabled on this computer
Firewall Enabled	All computers	Indicates whether the operating system's built-in firewall is enabled on this computer
Installed Software Count	All computers	<p>The number of installed software items from this computer that are included in the Installed Software table within the Absolute Manage database</p> <hr/> <p><b>NOTE</b> Collecting or updating installed software information is not automatic. You can explicitly trigger an update by using the <a href="#">Gather Inventory</a> command.</p> <hr/>
Missing OS Patches Count	All computers	<p>The number of software patches for the operating system missing from this computer</p> <hr/> <p><b>NOTE</b> Collecting or updating information about patches is not automatic. You can explicitly trigger an update by using the <a href="#">Gather Inventory</a> command.</p> <hr/>
Process Count	All computers	<p>The number of processes running on the computer that are included in the Processes table within the Absolute Manage database</p> <hr/> <p><b>NOTE</b> Collecting or updating process information is not automatic. You can explicitly trigger an update by using the <a href="#">Gather Inventory</a> command.</p> <hr/>

Field	Applies To	Description
File Count	All computers	<p>The number of files located on the computer that are included in the Files table within the Absolute Manage database</p> <hr/> <p><b>NOTE</b> Collecting or updating file information is not automatic. You can explicitly trigger an update by using the <a href="#">Gather Inventory</a> command. Only files recognized by this command are stored in the Absolute Manage database, not all files on the searched computers.</p> <hr/>
Font Count	All computers	<p>The number of fonts installed on the computer that are included in the Fonts table within the Absolute Manage database</p> <hr/> <p><b>NOTE</b> Collecting or updating font information is not automatic. You can explicitly trigger an update by using the <a href="#">Gather Inventory</a> command.</p> <hr/>
Printer Count	All computers	<p>The number of printers defined on the computer that are included in the Printers table within the Absolute Manage database</p> <hr/> <p><b>NOTE</b> Collecting or updating printer information is not automatic. You can explicitly trigger an update by using the <a href="#">Gather Inventory</a> command.</p> <hr/>
Timbuktu Access	All computers	Indicates whether this computer can be remotely controlled using Timbuktu
VNC Access	All computers	Indicates whether this computer can be remotely controlled using Virtual Network Computing (VNC)
Network Adapter Count	All computers	The number of active network adapters currently connected to the computer
Absolute Remote Enabled	All computers	Indicates whether the screen sharing function of the agent is enabled on this computer
Remote Desktop Screen Sharing	All computers	Indicates whether screen sharing through Apple Remote Desktop or Microsoft Remote Desktop is enabled on the computer
OS Service Pack	Windows computers only	The latest operating system service pack installed on the computer

Field	Applies To	Description
OS Installation Date	Windows computers only	The date and time when this copy of the operating system was installed on the computer
OS Activated	Windows computers only	Indicates whether this copy of the operating system has been activated  <b>NOTE</b> This field does not apply to Windows 2000.
OS Activation Grace Period	Windows computers only	The end of the grace period before which the operating system must be activated  <b>NOTE</b> This field does not apply to Windows 2000.
OS Serial Number	Windows computers only	The serial number of this copy of the operating system
OS Product ID	Windows computers only	The serial number of the individual copy of the operating system on this computer. This value is the ID number that is shown in the System area of the Control Panel.
OS Is Volume-Licensed	Windows computers only	Whether this copy of the operating system has been activated as part of a volume license  <b>NOTE</b> This field does not apply to Windows 2000.
Virtual Machine	Windows computers only	The type of virtual machine inside which the agent is running. Absolute Manage can currently identify Parallels, Virtual PC, and VMware. If the agent is not running inside a virtual machine, "native" is reported.
Security Identifier	Windows computers only	The unique ID that Windows generates for use with Active Directory and for other security-related purposes
OS Update Utility Enabled	All computers	Indicates whether the local update utility of the operating system (that is, Software Update on OS X computers and Windows Update on Windows computers) is enabled on this computer
Allow Remote Assistance	Windows computers only	Indicates whether Remote Assistance is enabled on this computer
Allow Remote Control via Assistance	Windows computers only	Indicates whether the ability to control this computer through Remote Assistance is enabled
PC Anywhere Access	Windows computers only	Indicates whether this computer can be remotely controlled using pcAnywhere

Field	Applies To	Description
DameWare Access	Windows computers only	Indicates whether this computer can be remotely controlled using DameWare
Defender Installed	Windows computers only	Indicates whether Windows Defender is installed on this computer
Defender Enabled	Windows computers only	Indicates whether Windows Defender is currently enabled on this computer
Defender Real-Time Protection	Windows computers only	Indicates whether Windows Defender's real-time protection is enabled on this computer
Defender Auto Scan Enabled	Windows computers only	Indicates whether Windows Defender's automatic scanning feature is enabled on this computer
Defender Engine Version	Windows computers only	The version number of Windows Defender installed on the computer
Defender Definition Version	Windows computers only	The version number of the malware definitions used by Windows Defender
Windows Service Count	Windows computers only	<p>The number of services from this computer that are included in the Absolute Manage database</p> <hr/> <p><b>NOTE</b> Collecting or updating service information is not automatic. You can explicitly trigger an update by using the <a href="#">Gather Inventory</a> command.</p> <hr/>
Darwin Version	OS X computers only	The version of Darwin that is part of the operating system
Personal File Sharing	OS X computers only	Indicates whether Personal File Sharing is enabled on the computer
Windows File Sharing	OS X computers only	Indicates whether file sharing for Windows is enabled on the computer
Personal Web Sharing	OS X computers only	Indicates whether Personal Web Sharing is enabled on the computer
Remote Login	OS X computers only	Indicates whether remote login is enabled on the computer
FTP Access	OS X computers only	Indicates whether FTP access is enabled on the computer
Remote Apple Events	OS X computers only	Indicates whether the Remote Apple Events service is enabled on the computer
FileVault Supported	OS X computers only	Indicates whether FileVault is available on this computer
FileVault Enabled	OS X computers only	Indicates whether FileVault is enabled on this computer

Field	Applies To	Description
FileVault Authenticated Restart Supported	OS X computers only	Indicates whether this computer can be restarted remotely without entering a password locally when the FileVault recovery key is presented
FileVault Has Personal Recovery Key	OS X computers only	Indicates whether the computer has a standard, locally generated FileVault recovery key
FileVault Has Institutional Recovery Key	OS X computers only	Indicates whether an institution-wide FileVault recovery key has been set for this computer
FileVault Unlocked Using Recovery Key	OS X computers only	Indicates whether the computer is running and the last restart was performed using the FileVault authenticated restart option
FileVault Recovery Key Stored on Server	OS X computers only	Whether the FileVault recovery key for this computer is stored on the Absolute Manage Server. In addition to “Yes” and “No”, this value can be “Yes, not verified”, which indicates that a recovery key for this computer is stored on the server, but it is unknown whether the key is still valid (for example, the user may have set a different key in the meantime).
Printer Sharing	OS X computers only	Indicates whether Printer Sharing is enabled on the computer
Remote Management	OS X computers only	Indicates whether Apple Remote Desktop remote management access (apart from screen sharing) is enabled
Wake on LAN Enabled	OS X computers only	Indicates whether Wake-on-LAN (turning on or awakening the computer from sleep using administrative network access) is enabled on the computer
Wake on LAN Supported	OS X computers only	Indicates whether the computer supports Wake-on-LAN
Startup Item Count	OS X computers only	<p>The number of start-up items on the computer that are included in the Startup Item table within the Absolute Manage database</p> <hr/> <p><b>NOTE</b> Collecting or updating start-up item information is not automatic. You can explicitly trigger an update by using the <a href="#">Gather Inventory</a> command.</p> <hr/>
<b>Memory</b>		
Memory Slot Name	All computers	The label of the memory slot
Memory Size	All computers	The RAM size of the memory module installed in the slot

Field	Applies To	Description
Memory Speed	All computers	The clock rate at which the memory module is accessed
Memory Type	All computers	The general type of memory installed in the memory slot, such as SDRAM or DDR SDRAM
<b>Volumes</b>		
Volume Name	All computers	The name of the volume  <b>NOTE</b> For Windows computers, this field may be empty.
Size	All computers	The formatted capacity of the volume (total space, whether free or used)
Format	All computers	The file system with which the volume is formatted (for example, NTFS, FAT32, or Mac OS Extended)
Display Name	Windows computers only	The displayed name of the volume
Volume Type	OS X computers only	The general type of volume: hard disk, removable, or server
Free Space	All computers	The unused capacity of the volume in absolute terms
Free Space %	All computers	The unused capacity of the volume as a percentage of the total formatted capacity
Drive Letter	Windows computers only	The drive letter that is currently assigned to the volume
Volume Serial Number	Windows computers only	The serial number of the volume
Object Count	OS X computers only	The total number of objects (files and folders, visible and invisible) on the volume  <b>NOTE</b> This information is not available for server volumes.
Folder Count	OS X computers only	The total number of directories (both visible and invisible) on the volume  <b>NOTE</b> This information is not available for server volumes.
Journaled	OS X computers only	Indicates whether this volume is journaled
Locked by Hardware	OS X computers only	Indicates whether this volume is write-protected through a hardware setting

Field	Applies To	Description
Locked by Software	OS X computers only	Indicates whether this volume is write-protected through a software setting  <b>NOTE</b> Volumes that are write-protected by hardware, such as CD-ROMs, may be shown as being write-protected by software.
Boot Volume	All computers	Indicates whether this is the volume from which the computer has booted
Compressed	All computers	Indicates whether the data on this volume is compressed by the operating system
<b>Network Adapters</b>		
Adapter Name	All computers	The label of the network adapter (for example, Ethernet or AirPort)
Adapter IP Address	All computers	The IP address assigned to the network adapter
Adapter Subnet Mask	All computers	The subnet mask assigned to the network adapter
Adapter MAC Address	All computers	The MAC address of the network adapter
Configuration Type	All computers	The way in which the network adapter has been configured (for example, DHCP or Manual)
Primary Interface	All computers	Indicates whether this is the network adapter currently being used as the main IP interface of the computer
Router Address	All computers	The IP address of the router assigned to the network adapter
DHCP Server Address	All computers	The IP address of the DHCP server, if any, that currently supplies the IP address to the network adapter
DNS Servers	All computers	The IP addresses of all DNS servers that the network adapter is set to contact to resolve names into IP addresses. If multiple DNS servers are specified, their IP addresses are separated by commas.
Search Domains	All computers	The default search domains specified for the network adapter. If multiple domains are specified, they are separated by commas.
TCP Implementation	All computers	The general type of TCP stack in use on the network adapter
Device Name	All computers	The logical name of the network adapter
Link Status	All computers	Indicates whether the network link on this network adapter is active

Field	Applies To	Description
Adapter Speed	All computers	The nominal data rate on this network adapter's current connection
Full Duplex	All computers	Indicates whether the network adapter is currently operating in full duplex mode (as opposed to half duplex)
Adapter Vendor	All computers	The manufacturer of the network adapter
Hardware	All computers	The hardware category of the network adapter
<b>Missing Patches</b>		
Missing Patch Name	All computers	The name of the missing patch
Missing Patch Version	All computers	The version number of the missing patch
Missing Patch Severity	All computers	The rated severity of this patch  <b>NOTE</b> This information is supplied by the source of the patch and may not be present for all patches.
Missing Patch Is Mandatory	Windows computers only	Indicates whether Microsoft has marked this patch as mandatory
Missing Patch Release Date	All computers	The date when this patch was released by the software vendor
Missing Patch Is OS Patch	All computers	Indicates whether this patch is an operating system patch
Missing Patch Action	Windows computers only	Indicates whether this patch includes an install or an uninstall action
Missing Patch Install Deadline	Windows computers only	The date recommended by Microsoft by which this patch should be installed
Missing Patch Language	Windows computers only	The operating system language for which this patch is intended
<b>Installed Software</b>		
Inst. Software Name	All computers	The name of the software
Inst. Software Company	Windows computers only	The name of the company that produced the software
Inst. Software Info	OS X computers only	Additional information from the software's version information file
Inst. Software Version String	All computers	The full version information for the software
Inst. Software Size	All computers	The size of the installed software on the disk
Inst. Software Installation Date	All computers	The date and time when the software was installed on the computer
Uninstallable	Windows computers only	Indicates whether there is an uninstall entry for the software on the client computer



Field	Applies To	Description
Is Hotfix	Windows computers only	Indicates whether this software is marked as a hotfix
Identification Type	All computers	The method by which Absolute Manage found this software on the computer
Install Location	Windows computers only	The path of the software on the computer. This information is not available for software identified by its installer receipt.
Inst. Software Product ID	All computers	For Windows software: the ID noted in the registry For OS X software: the software's bundle identifier
Registered Company	Windows computers only	The company to which this product has been registered
Registered Owner	Windows computers only	The person to which this product has been registered
Installed By	Windows computers only	The name of the user account under which the software was installed
<b><i>Installed Profiles</i></b>		
Installed Profile Name	OS X computers only	The name of the configuration profile
Installed Profile Type	OS X computers only	The type of profile: device profile or user profile. Device profiles contain settings that always apply to the device on which they are installed; user profiles contain settings that apply only when the corresponding user account is used.
Installed Profile Identifier	OS X computers only	The identifying string of the profile
Installed Profile Installation Date	OS X computers only	The date and time when the profile was installed on the computer
Installed Profile Organization	OS X computers only	The optional name of the organization that provided the profile
Installed Profile Allow Removal	OS X computers only	Indicates whether the profile can be removed remotely
Installed Profile For User	OS X computers only	The user for which this profile has been installed. For device profiles, this field contains "n/a".
Installed Profile Verification State	OS X computers only	Indicates whether the signature of the profile, if any, could be verified. Possible values include "unsigned", "verified", "not verified" (which may indicate an unauthorized change), and "unknown".
Installed Profile Description	OS X computers only	The optional description string of the profile

## Sending Messages to Computers

If you need to communicate important information to users of administered computers, you can send a message directly to a computer for the user to read. This command is useful, for example, when you need to advise employees of upcoming administrative actions on their computers.

➔ To send a message to computers:

1. Navigate to a page in the Computers area that contains the computers you want to send a message to. For example, you can navigate to **Computers > All Computers**, then [search for specific computers](#).
2. In the results grid, select the checkbox of each applicable computer and click **Commands > Send Message**.

You can also issue the command for a single computer from its Computer Details page:

- a) In the results grid, click the computer you want to send a message to. The computer's Computer Details page opens.
  - b) From the Commands sidebar, click **Send Message**.
3. Enter the message in the field provided.
  4. Click **Send Message**.
  5. Click **OK** to close the confirmation message.

## Gathering Computer Information

You can gather a wide range of information on your administered computers to help you manage your network.

Information about administered computers is regularly collected by the Absolute Manage agent, which sends the information to the Absolute Manage Server. This information is then retrieved by Absolute Manage Web Admin for display within the application. The process of collecting information is mostly automatic; however, certain types of information – such as font, printer, and startup item information – are collected on request only to conserve local processing power and network bandwidth. You can send a command to retrieve information on these specific items, as well as to manually update other computer information when you do not want to wait for the next scheduled update.

➔ To manually gather computer information:

1. Navigate to a page in the Computers area that contains the computers you want to gather information about. For example, you can navigate to **Computers > All Computers**, then [search for specific computers](#).
2. In the results grid, select the checkbox of each applicable computer and click **Commands > Gather Inventory**.

You can also issue the command for a single computer from its Computer Details page:

- a) In the results grid, click the computer you want to gather information about. The computer's Computer Details page opens.
  - b) From the Commands sidebar, click **Gather Inventory**.
3. Computer information that has changed since the last update is always gathered when you perform this command. You can also select options for gathering additional information:
    - **Force full inventory** – Prompts agents on the selected computers to transmit all computer information (that is, not only information that has changed) to the server
    - **Include font information** – Prompts agents on the selected computers to transmit information on installed fonts
    - **Include printer information** – Prompts agents on the selected computers to transmit information on connected printers
    - **Include startup item information (OS X only)** – Prompts agents on selected OS X computers to transmit information on installed startup items
    - **Include service information (Windows only)** – Prompts agents on selected Windows computers to transmit information on running services
  4. Click **Gather Inventory**.
  5. Click **OK** to close the confirmation message.

## Working with Mobile Devices

Use the Mobile Devices area to view the mobile devices in your IT deployment and perform administrative actions on these devices.

When you first visit this area, mobile devices of all types and operating systems are listed. If you are only concerned with devices of a specific type, you can filter this list by selecting one of the following device groups from the Mobile Device Groups sidebar:

- All Android Devices
- All Android Tablets
- All Android Phones
- All iOS Devices
- All iPhones
- All iPads
- All iPod Touch Devices

You can also [search for individual devices](#) using specific criteria in the Search field, as well as [customize the information](#) included in the results grid.

From the Mobile Devices area, you can perform the following tasks:

- [Viewing Device Details](#)
- [Locking Devices](#)
- [Managing Passcodes on Devices](#)
- [Deleting Data on Devices](#)
- [Sending Messages to Devices](#)
- [Updating Device Information](#)
- [Renaming Devices](#)
- [Setting Roaming Options for Devices](#)
- [Distributing Applications to Devices](#)
- [Uninstalling Applications on Devices](#)
- [Installing Configuration Profiles on Devices](#)
- [Removing Configuration Profiles from Devices](#)
- [Installing Provisioning Profiles on Devices](#)
- [Removing Provisioning Profiles from Devices](#)
- [Setting Device Ownership](#)
- [Setting the Enrollment User for Devices](#)
- [Setting Organization Information on Devices](#)
- [Setting Activation Lock Options](#)
- [Retrying Failed Installations](#)

## About Mobile Device Management

Absolute Manage Web Admin allows you to administer mobile devices in your IT deployment that are running the following versions of the iOS, Android, or Windows Phone operating system:

- iOS 4.0 or higher
- Android 2.2 or higher
- Windows Phone 7 or higher

---

**NOTE** The administration commands available to you for a mobile device depend on the operating system the device is running. For information on the operating systems a specific command supports, see the help for that command.

---

The mobile devices in your deployment must be enrolled with Absolute Manage before you can administer them through Absolute Manage Web Admin. For information on how to enroll mobile devices, see "Enrolling mobile devices" in the *Absolute Manage User Guide*.

## Viewing Device Details

The Device Details page lists all available information on a mobile device, including the device's hardware profile, installed software, and user details. You can access this page from several places in the application, including the following:

- The Mobile Devices area
- The Mobile Devices tab of a policy group
- The Mobile Devices tab of a content item

➔ To view a device's details:

1. Navigate to a page where the device is listed. For example, go to the **Mobile Devices > All Mobile Devices** page for a list of all your organization's mobile devices.
2. In the results grid, click the device whose details you want to view.

The Device Details page opens with the device's model and phone number listed at the top. The following table provides a summary of other device information available in the top area of the page:

Field	Applies To	Description
OS Version	All devices	The version of the operating system currently running on the device
Last Contact	All devices	The date and time (displayed in your local time) when the device last received communication from the Absolute Manage Server
Passcode Present	iOS and Android devices only	Indicates whether a passcode is set on the device
Battery Level	iOS and Android devices only	The remaining charge level of the device's battery, expressed as a percentage
Serial Number	iOS and Android devices only	The serial number of the device
Identifier (UDID)	All devices	The unique internal identifier of the device. For iOS devices, this value is the UDID.
OS Build Number	All devices	The build number of the operating system version installed on the device
Ownership	All devices	The type of owner the device has: the company, the user, or a guest. You can change this information by <a href="#">setting device ownership</a> .
Managed	All devices	Indicates whether the device is being managed through the Absolute Manage Mobile Device Management (MDM) system
Jail Broken	iOS devices only	Indicates whether the device has been jail broken; that is, whether the device's firmware has been modified to remove limitations on the operating system

Field	Applies To	Description
Rooted	Android devices only	Indicates whether the device has been rooted; that is, whether the device's firmware has been modified to remove limitations on the operating system
Record Creation Date	All devices	The date and time (displayed in your local time) when the device's record was created in the server
AbsoluteApps Version	iOS and Android devices only	The version number of the AbsoluteApps instance installed on the device
AbsoluteApps Build Number	iOS and Android devices only	The build number of the AbsoluteApps version installed on the device
Supports Persistence	Android devices only	Indicates whether the device supports persistence; that is, whether the Absolute Manage client software is able to remain on the device even after removal attempts and factory resets
MDM Profile Up-to-date	iOS devices only	Indicates whether the MDM access privileges that are set in the MDM profile on the device are the same as those currently set on the server
Production Date	iOS devices only	<p>The date when the device was manufactured</p> <hr/> <p><b>NOTE</b> This information is downloaded from Apple's server, based on the device's serial number. Therefore, the value is available only if the device had a working Internet connection at least once after being enrolled in the MDM system. The value is updated every ten days as long as the device continues to have an Internet connection to the Apple server.</p> <hr/>
Age	iOS devices only	<p>The age of the mobile device; that is, the time that has elapsed since its production</p> <hr/> <p><b>NOTE</b> This information is downloaded from Apple's server, based on the device's serial number. Therefore, the value is available only if the device had a working Internet connection at least once after being enrolled in the MDM system. The value is updated every ten days as long as the device continues to have an Internet connection to the Apple server.</p> <hr/>

Field	Applies To	Description
Warranty Info	iOS devices only	<p>The device's current warranty status</p> <p><b>NOTE</b> This information is downloaded from Apple's server, based on the device's serial number. Therefore, the value is available only if the device had a working Internet connection at least once after being enrolled in the MDM system. The value is updated every ten days as long as the device continues to have an Internet connection to the Apple server.</p>
Warranty End	iOS devices only	<p>The date when the device's warranty ends. A value of <b>n/a</b> indicates that no information is available, or the warranty has expired.</p> <p><b>NOTE</b> This information is downloaded from Apple's server, based on the device's serial number. Therefore, the value is available only if the device had a working Internet connection at least once after being enrolled in the MDM system. The value is updated every ten days as long as the device continues to have an Internet connection to the Apple server.</p>
Passcode Compliant	iOS devices only	Indicates whether the passcode on the device complies with all applicable requirements, including those of Microsoft Exchange Server when applicable
Passcode Compliant with Profiles	iOS devices only	Indicates whether the passcode on the device complies with all active profiles

- To view additional device details, expand the **Storage**, **Networking**, **Hardware**, **Cellular Information**, **Organization Info**, **System Memory**, and **Last Changed Items** sections.

**NOTE** If cookies are enabled in your browser, the system remembers the sections you choose to expand, even if you log out.

The following table provides a summary of device information available in these sections:

Field	Applies To	Description
<b>Storage</b>		
Device Capacity	iOS devices only	The storage capacity of the device, excluding space required by the operating system. This capacity is usually a few gigabytes below the nominal capacity. (For example, a 32 GB iPhone may have a capacity of approximately 29 GB.) This number is the same as the capacity shown in iTunes.



Field	Applies To	Description
Used Capacity	iOS devices only	The amount of used storage on the device
Available Capacity	iOS devices only	The amount of free storage on the device. This number is the same as the free space shown in iTunes.
Internal Storage	Android devices only	<p>The amount of total and available internal storage for application data in the device.</p> <p><b>NOTE</b> Some devices partition their built-in storage and declare some to be USB storage. In this case, the internal storage shown here is much smaller than the actual built-in storage.</p>
SD Card 1 (non-removable)	Android devices only	<p>The amount of total and available storage on the first SD card in the device</p> <p><b>NOTE</b> Some devices partition their built-in storage and declare some to be USB storage. In this case, some of the device's internal storage is shown within SD Card 1.</p>
SD Card 2 (removable)	Android devices only	The amount of total and available storage on the second SD card in the device
<b>Networking</b>		
GPS Capable	iOS and Android devices only	<p>Indicates whether the device can locate itself by GPS signals</p> <p><b>NOTE</b> Devices that are not GPS capable may still be able to locate themselves by other means, such as by known locations of cell towers or Wi-Fi networks in range. However, these location methods are usually less accurate than GPS.</p>
Wi-Fi Network	iOS and Android devices only	The name of the Wi-Fi network (if any) that the device was connected to at the time of its last contact
Home Network	iOS and Android devices only	The standard mobile network of the device
Public IP Address	iOS and Android devices only	The public IPv4 address the device used to communicate with Absolute Manage at the time of its last contact. This value is either the cell IP address or the public address of the NAT router over which the Wi-Fi network is connected to the Internet.
Cell IP Address	iOS and Android devices only	The IP address of the device in the mobile (cellular) network it is currently using (if any)


Field	Applies To	Description
Wi-Fi IP Address	iOS and Android devices only	The IPv4 address of the device in the Wi-Fi network it was using at the time of its last contact (if any)
Wi-Fi MAC Address	iOS and Android devices only	The MAC address of the device's Wi-Fi connection
Bluetooth MAC Address	iOS and Android devices only	The MAC address of the device's Bluetooth connection
<b>Hardware</b>		
Tablet	iOS and Android devices only	Indicates whether the device is a tablet
Manufacturer	All devices	The company that produced the device. This company is not necessarily the same brand name that the device was sold under.
CPU Name	iOS and Android devices only	The type of CPU used in the device
CPU Speed	iOS and Android devices only	The clock rate of the CPU used in the device
Display Resolution	iOS and Android devices only	The screen size of the device, measured in pixels
Board	iOS and Android devices only	The name or type code of the motherboard in the device  <b>NOTE</b> Many motherboards used in mobile devices do not have an accessible name or type code.
Hardware Encryption	iOS and Android devices only	The type of hardware encryption (block level or file level) available on the device
Kernel Version	Android devices only	The version information for the operating system's kernel that is active on the device
Device Info	Android devices only	Additional information about the device as provided by its manufacturer
<b>System Memory</b>		
RAM Total	Android devices only	The total amount of RAM installed in the device
RAM Available	Android devices only	The amount of RAM in the device that is currently free
Cache Total	Android devices only	The total amount of cache memory in the device
Cache Available	Android devices only	The amount of cache memory in the device that is currently free
<b>Cellular information</b>		
Current Carrier Network	All devices	The mobile network that the device was registered on at the time of last contact

Field	Applies To	Description
Cellular Technology	iOS and Android devices only	The basic cellular technology that the device is currently using to communicate, such as GSM or CDMA
Roaming	iOS and Android devices only	Indicates whether the device is currently roaming; that is, if it is connected to a mobile network other than the network of the standard provider
Cellular Data Network Type	Android devices only	The base technology of the cellular network that the device is connected to. Possible values are <b>none</b> , <b>EDGE</b> , <b>GPRS</b> , or <b>UMTS</b> .
IMEI/MEID	All devices	The IMEI (GSM) or MEID (CDMA) telephone identification number of the connected device, if any
SIM ICC Identifier	iOS and Android devices only	The unique international identifier of the SIM present within the device
Current Mobile Country Code	iOS and Android devices only	The mobile country code of the mobile network that the device was registered on at the time of last contact
Current Mobile Network Code	iOS and Android devices only	The mobile network code of the mobile network that the device was registered on at the time of last contact
Home Mobile Country Code	iOS and Android devices only	The mobile country code of the device's standard mobile network
Home Mobile Network Code	iOS and Android devices only	The mobile network code of the device's standard mobile network
Data Roaming Enabled	iOS devices only	Indicates whether the device is set to allow data roaming (exchanging data over mobile networks other than that of the standard provider)
Voice Roaming Enabled	iOS devices only	Indicates whether the device is set to allow voice roaming (initiating or receiving voice calls over mobile networks other than that of the standard provider)
Carrier Settings Version	iOS devices only	The version number of the carrier settings in the device. Carrier settings include the name of the various available networks and other information. These settings are provided by Apple and can be updated independently of the iOS software.
Mobile Device IMEISV	Android devices only	The revision number of the software installed on the device, as noted in the device's IMEI
Modem Firmware Version	iOS and Android devices only	The version number of the modem firmware installed on the device, if any

Field	Applies To	Description
<b>Organization Info</b>		
Name	iOS 7.0 and higher devices only	The name of the organization that is stored on the device
Phone	iOS 7.0 and higher devices only	The phone number of the organization that is stored on the device
E-mail	iOS 7.0 and higher devices only	The e-mail address of the organization that is stored on the device
Address	iOS 7.0 and higher devices only	The postal or street address of the organization that is stored on the device
Custom	iOS 7.0 and higher devices only	Additional information on the organization that is stored on the device
<b>Last Changed Items</b>		
Device Information	All devices	<p>The most recent time (displayed in your local time) when the information stored on the server for the device changed</p> <hr/> <p><b>NOTE</b> This value is not necessarily the time when the corresponding property of the device changed, but only the time when the mobile client software informed the Absolute Manage server of the change. Certain changes that frequently occur are not considered here, such as changes in battery level, free storage, or roaming status.</p> <hr/>
Installed Software	iOS and Android devices only	<p>The most recent time (displayed in your local time) when the information stored on the server for the software installed on the device changed</p> <hr/> <p><b>NOTE</b> This value is not necessarily the time when an application was installed on or deleted from the device, but only the time when the mobile client software informed the Absolute Manage server of the change.</p> <hr/>
Installed Configuration Profiles	iOS and Android devices only	<p>The most recent time (displayed in your local time) when the information stored on the server for the configuration profiles installed on the device changed</p> <hr/> <p><b>NOTE</b> This value is not necessarily the time when a profile was installed on or deleted from the device, but only the time when the mobile client software informed the Absolute Manage server of the change.</p> <hr/>

Field	Applies To	Description
Installed Certificates	iOS devices only	<p>The most recent time (displayed in your local time) when the information stored on the server for the certificates installed on the device changed</p> <hr/> <p><b>NOTE</b> This value is not necessarily the time when a certificate was installed on or deleted from the device, but only the time when the mobile client software informed the Absolute Manage server of the change.</p>
Installed Provisioning Profiles	iOS devices only	<p>The most recent time (displayed in your local time) when the information stored on the server for the provisioning profiles installed on the device changed</p> <hr/> <p><b>NOTE</b> This value is not necessarily the time when a profile was installed on or deleted from the device, just the time when the mobile client software informed the Absolute Manage server of the change.</p>

4. You can click other tabs on this page for further information or to perform certain tasks on the device:


- **Mobile Policies:** Shows all policies that the mobile device belongs to. You can perform the following tasks from this tab:
  - [Add the device to standard policies](#) by clicking the **Add Mobile Device to Policies** button.
  - Remove the device from standard policies by selecting the checkbox of the applicable policies and clicking .
- **Applications:** This tab applies to iOS and Android devices only. It shows applications that are installed on the mobile device.







---

**NOTE** This tab does not show applications that are included with the device firmware, such as Camera or Mail on iOS devices.

---

You can perform the following tasks from this tab:

- [Distribute software to the device](#) by clicking the **Install Application** button.
- [Uninstall applications](#) from the device by selecting the checkbox of the applicable applications and clicking .
- **Certificates:** This tab applies to iOS devices only. It shows certificates that are installed on the mobile device.
- **Configuration Profiles:** Shows the configuration profiles that are installed on the mobile device. You can perform the following tasks from this tab:
  - [Install configuration profiles on the device](#) by clicking the **Install Configuration Profile** button.

- [Remove configuration profiles](#) from the device by selecting the checkbox of the applicable profiles and clicking .
- **Provisioning Profiles:** This tab applies to iOS devices only. It shows provisioning profiles that are installed on the mobile device. You can perform the following tasks from this tab:
  - [Install provisioning profiles on the device](#) by clicking the **Install Provisioning Profile** button.
  - [Remove provisioning profiles](#) from the device by selecting the checkbox of the applicable profiles and clicking .
- **Assigned Items:** Shows the assignable items (in-house and third-party applications, mobile content, and profiles) that are managed through Absolute Manage and present on the mobile device.
- **Custom Fields:** Shows the custom fields available for the mobile device along with the field values, if they have been entered. You can perform the following tasks from this tab:
  - [Enter a custom field value](#) for the mobile device by selecting the checkbox of a custom field and clicking .
  - [Remove a custom field value](#) for the mobile device by selecting the checkbox of a custom field and clicking .
- **Administrators:** Shows the administrators of the mobile device.
- **User:** Shows Active Directory or Open Directory information available for the current user of the mobile device.
- **Performed Actions:** Shows the actions that have been carried out on the mobile device as a result of the device's membership in smart policies. You can perform the following tasks from this tab:
  - Clear actions from the list by selecting the checkbox of the applicable actions and clicking .
  - Re-execute actions on the list by selecting the checkbox of the applicable actions and clicking .

---

**NOTE** After you perform tasks within these tabs, you may need to click your browser's refresh button to see updated information in the results grid.

---

## Locking Devices

You can issue a command to remotely lock mobile devices, rendering them unusable until a passcode is entered locally (unless a passcode has not been set on a device). This command is available for iOS and Android devices only.

After you issue the command, a device is locked as soon as it next contacts the notification server of its OS vendor. If the device is connected to a Wi-Fi or mobile network, this action is usually carried out within a minute; otherwise, it happens when the device reconnects to a network.

With Android devices, you have the option to lock the device using a new passcode that you choose.

➔ To lock mobile devices:

1. Navigate to a page in the Mobile Devices area that contains the devices you want to lock. For example, you can navigate to **Mobile Devices > All Mobile Devices**, then [search for specific devices](#).
2. In the results grid, select the checkbox of the devices you want to lock and click **Commands > Lock Device**.

You can also issue the command for a single device from its Device Details page:

- a) In the results grid, click the device you want to lock. The device's Device Details page opens.
  - b) From the Commands sidebar, click **Device Lock**.
3. If you want to lock an Android device using a new passcode, enter and confirm the passcode in the fields provided (leave these fields empty if you do not want to set a new passcode on the device).

---

**NOTE** If the configuration profile on the device requires a passcode, the user is prompted to create a new passcode if you do not specify one here.

---

4. Click **Lock**.
5. Click **OK** to close the confirmation message.

## Managing Passcodes on Devices

You can issue a command to perform the following actions related to passcodes:

- For iOS devices, remotely remove the passcode from a device
- For Android devices, remotely remove a device's passcode and set a new one

After you issue the command, a device's passcode is removed or updated as soon as it next contacts the notification server of its OS vendor. If the device is connected to a Wi-Fi or mobile network, this action is usually carried out within a minute; otherwise, it happens when the device reconnects to a network.

---

**NOTE** If you remove a passcode from a device without setting a new one, and there is no configuration profile on the device making a passcode mandatory, the device becomes accessible to anyone without requiring a passcode.

---

➔ To remove the passcode on iOS devices:

1. Navigate to a page in the Mobile Devices area that contains the iOS devices whose passcode you want to remove. For example, you can navigate to **Mobile Devices > All iOS Devices**, then [search for specific devices](#).
2. In the results grid, select the checkbox of each applicable iOS device and click **Commands > Clear Passcode**.

You can also issue the command for a single iOS device from its Device Details page:

- a) In the results grid, click the device whose passcode you want to remove. The device's Device Details page opens.
  - b) From the Commands sidebar, click **Clear Passcode**.
3. Click **Clear Passcode**.
  4. Click **OK** to close the confirmation message.

➔ To remove the passcode on Android devices:

1. Navigate to a page in the Mobile Devices area that contains the Android devices whose passcode you want to remove. For example, you can navigate to **Mobile Devices > All Android Devices**, then [search for specific devices](#).
2. In the results grid, select the check box of each applicable Android device and click **Commands > Clear and Set Passcode**.

You can also issue the command for a single Android device from its Device Details page:

- a) In the results grid, click the device whose passcode you want to remove. The device's Device Details page opens.
  - b) From the Commands sidebar, click **Clear and Set Passcode**.
3. Click **Clear Passcode**.

---

**NOTE** If the configuration profile on the device requires a passcode, the user will be prompted to create a new passcode.

---

4. Click **OK** to close the confirmation message.

➔ To set a new passcode on Android devices:



1. Navigate to a page in the Mobile Devices area that contains the Android devices whose passcode you want to set. For example, you can navigate to **Mobile Devices > All Android Devices**, then [search for specific devices](#).

2. In the results grid, select the check box of each applicable Android device and click **Commands > Clear and Set Passcode**.

You can also issue the command for a single Android device from its Device Details page:

- a) In the results grid, click the device whose passcode you want to set. The device's Device Details page opens.
  - b) From the Commands sidebar, click **Clear and Set Passcode**.
3. Select the **Set new passcode** checkbox.
  4. Enter and confirm the new passcode in the provided fields.
  5. Click **Clear and Set Passcode**.
  6. Click **OK** to close the confirmation message.

## Erasing Devices

You can remotely erase all user data on a mobile device as well as all applications the user has installed, effectively resetting the device to its factory condition.

---

**WARNING!** This action is not reversible. You cannot recover the erased information from the mobile device (although recovering the data from a backup system, if one exists within your organization, may be possible). Erasing a device without the consent of the user may expose you to legal liability.

---

After you issue the command, a device is erased as soon as it next contacts the notification server of its OS vendor. If the device is connected to a Wi-Fi or mobile network, this action is usually carried out within a minute; otherwise, it happens when the device reconnects to a network.

After a device is erased, you can no longer administer that device through Absolute Manage until you enroll it again or it has been completely restored from a backup containing the Absolute Manage enrollment profile.

➔ To erase mobile devices:

1. Navigate to a page in the Mobile Devices area that contains the devices you want to erase. For example, you can navigate to **Mobile Devices > All Mobile Devices**, then [search for specific devices](#).
2. In the results grid, select the checkbox of each applicable device and click **Commands > Erase Device**.

You can also issue the command for a single device from its Device Details page:

- a) In the results grid, click the device you want to erase. The device's Device Details page opens.
  - b) From the Commands sidebar, click **Erase Device**.
3. If any of the selected devices have internal SD cards, you are prompted to select one of the following options:
    - **Erase internal storage only**
    - **Erase internal storage and SD card**
  4. Click **Erase Device**.

---

**IMPORTANT** Clicking **Erase Device** issues the command to erase data on the device, which you cannot reverse.

---

5. Click **OK** to close the confirmation message.

## Sending Messages to Devices

If you need to communicate important information to users of mobile devices, you can send a message directly to the devices for users to read. This command is available for iOS and Android devices only.

---

**NOTE** This command requires the AbsoluteApps application to be installed (and launched at least once) on the target devices. Push notifications must also be enabled on the devices.

---

After you issue the command, a device receives the message as soon as it next contacts the notification server of its OS vendor. If the device is connected to a Wi-Fi or mobile network, it usually receives the message within a minute; otherwise, the message is delivered when the device reconnects to a network.

➔ To send a message to mobile devices:

1. Navigate to a page in the Mobile Devices area that contains the devices you want to send a message to. For example, you can navigate to **Mobile Devices > All Mobile Devices**, then [search for specific devices](#).

2. In the results grid, select the checkbox of each applicable device and click **Commands > Send Message**.

You can also issue the command for a single device from its Device Details page:

- a) In the results grid, click the device you want to send a message to. The device's Device Details page opens.
  - b) From the Commands sidebar, click **Send Message**.
3. Enter the message in the field provided.
  4. Click **Send Message**.
  5. Click **OK** to close the confirmation message.

## Updating Device Information

You can issue a command that queries devices and updates details about them (such as networking, storage, and hardware information) in the Absolute Manage database. The updated device information is then available in Absolute Manage Web Admin.

After you issue the command, a device is queried as soon as it next contacts the notification server of its OS vendor. If the device is connected to a Wi-Fi or mobile network, this action is usually carried out within a minute; otherwise, it happens when the device reconnects to a network.

➔ To update device information in Absolute Manage:

1. Navigate to a page in the Mobile Devices area that contains the devices that you want to query. For example, you can navigate to **Mobile Devices > All Mobile Devices**, then [search for specific devices](#).
2. In the results grid, select the checkbox of each applicable device and click **Commands > Update Device Info**.

You can also issue the command for a single device from its Device Details page:

- a) In the results grid, click the device you want to query. The device's Device Details page opens.
  - b) From the Commands sidebar, click **Update Device Info**.
3. Click **OK** to close the confirmation message.

---

**NOTE** You may need to click your browser's refresh button to see updated information within the results grid and the Device Details page.

---

## Renaming Devices

You can issue a command to change the name of mobile devices. This command is available only for Android devices and supervised iOS devices running iOS 8 or higher.

After you issue the command, the name change occurs as soon as the device next contacts the notification server of its OS vendor. If the device is connected to a Wi-Fi or mobile network, the name change usually occurs within a minute; otherwise, it occurs when the device reconnects to a network.

➔ To rename a mobile device:

1. Navigate to a page in the Mobile Devices area that contains the device you want to rename. For example, you can navigate to **Mobile Devices > All Mobile Devices**, then [search for a specific device](#).

2. In the results grid, select the checkbox of the device and click **Commands > Set Device Name**.

You can also issue the command for the device from its Device Details page:

- a) In the results grid, click the device you want to rename. The device's Device Details page opens.
  - b) From the Commands sidebar, click **Set Device Name**.
3. Enter a name for the device in the New Name field.

---

**NOTE** The name you give a mobile device must be unique within your Absolute Manage deployment.

---

4. Click **Set Name**.
5. Click **OK** to close the confirmation message.

---

**NOTE** You may need to click your browser's refresh button to see updated information within the results grid and the Device Details page.

---

## Setting Roaming Options for Devices

You can issue a command to activate or deactivate voice and data roaming on mobile devices. This command is available only for iOS devices running iOS 5 or higher.

---

**NOTE** After you set roaming options for a device, the device's user is not prevented from changing these settings.

---

After you issue the command, a device's roaming settings are changed as soon as the device next contacts the notification server of its OS vendor. If the device is connected to a Wi-Fi or mobile network, this action is usually carried out within a minute; otherwise, it happens when the device reconnects to a network.

➔ To set roaming options for mobile devices:

1. Navigate to a page in the Mobile Devices area that contains the devices whose roaming options you want to change. For example, you can navigate to **Mobile Devices > All iOS Devices**, then [search for specific devices](#).
2. In the results grid, select the checkbox of each applicable device and click **Commands > Set Roaming Options**.

You can also issue the command for a single iOS device from its Device Details page:

- a) In the results grid, click the device whose roaming options you want to change. The device's Device Details page opens.
  - b) From the Commands sidebar, click **Set Roaming Options**.
3. Set the roaming options for the devices by selecting or clearing the **Enable voice roaming** and **Enable data roaming** checkboxes.
  4. Click **Set Roaming Options**.
  5. Click **OK** to close the confirmation message.

## Distributing Applications to Devices

You can remotely distribute both in-house applications and third-party applications for installation on mobile devices. This command is available for iOS and Android devices only.

Before you can distribute an application for installation from Absolute Manage Web Admin, you must import the application file as a mobile application package using the Absolute Manage Admin interface. For more information, see "Installing software on mobile devices" in the *Absolute Manage User Guide*.

---

**NOTE** You cannot install an application on an iOS device that already contains an unmanaged version of the same application (unmanaged applications are applications that are installed on a device through means other than Absolute Manage.)

---

After you issue the command to install an application, the device's user is prompted to install the application as soon as the device next contacts the notification server of its OS vendor. If the device is connected to a Wi-Fi or mobile network, the user is usually prompted to install within a minute; otherwise, it happens when the device reconnects to a network. If the device's user declines the installation, the application is not installed on the device.

---

**NOTE** On devices running iOS 4.x, the user is prompted to install the application only when AbsoluteApps comes to the foreground.

---

➔ To distribute software to mobile devices:

1. Navigate to a page in the Mobile Devices area that contains the devices you want to distribute software to. For example, you can navigate to **Mobile Devices > All Mobile Devices**, then [search for specific devices](#).
2. In the results grid, select the checkbox of each applicable device and click **Commands > Install Application**.

---

**NOTE** If you are issuing the command to multiple devices at once, you must select devices of the same OS; that is, select either all iOS devices or all Android devices.

---

You can also issue the command for a single device from its Device Details page:

- a) In the results grid, click the device you want to distribute software to. The device's Device Details page opens.
  - b) From the Commands sidebar, click **Install Application**.
3. From the **In-House Applications** and **Third-Party Applications** lists, select the checkboxes of the applications you want to distribute for installation.  
  
To quickly find specific applications, you can use the search field to narrow the applications listed by specific criteria (for example, by application name or version number).
  4. Click **Install Application**.
  5. Click **OK** to close the confirmation message.

## Uninstalling Applications on Devices

You can send a command to remotely uninstall applications from mobile devices. This command is available only for iOS devices running iOS 5 or higher, and Android devices.

Your ability to uninstall applications varies according to a device's operating system:


- On iOS devices, you can uninstall only managed applications; that is, applications that have been installed through Absolute Manage.
- On Android devices, you can uninstall any application, but the device's user must confirm the application's removal. However, if the device supports persistence, user confirmation is not required.

After you issue the command, the uninstall process begins as soon as the device next contacts the notification server of its OS vendor. If the device is connected to a Wi-Fi or mobile network, this action is usually carried out within a minute; otherwise, it happens when the device reconnects to a network. On Android devices, a confirmation alert is shown before the application is actually removed. If the user does not allow the removal, the application remains on the device.

➔ To uninstall applications on a mobile device:

1. Navigate to a page in the Mobile Devices area that contains the device you want to uninstall applications from. For example, you can navigate to **Mobile Devices > All Mobile Devices**, then [search for a specific device](#).
2. In the results grid, click the device.
3. Click the device's **Applications** tab.
4. Select the checkbox of each application you want to uninstall.

To quickly find specific applications, you can use the search field to narrow the applications listed by specific criteria (for example, by name or version number).

5. Click .
6. Click **Uninstall Applications**.
7. Click **OK** to close the confirmation message.

---

**NOTE** You may need to click your browser's refresh button to see updated information in the results grid.

---



## Installing Configuration Profiles on Devices

You can remotely install existing configuration profiles on mobile devices. A configuration profile is an easy way of distributing common settings (for example, Wi-Fi, VPN, email, or application-specific settings) to the mobile devices in your deployment. Before you can install a configuration profile from Absolute Manage Web Admin, you must import or create the profile using the Absolute Manage Admin interface. For more information, see "Working with configuration profiles" in the *Absolute Manage User Guide*.

After you issue the command, the configuration profile is installed on the device as soon as it next contacts the notification server of its OS vendor. If the device is connected to a Wi-Fi or mobile network, this action is usually carried out within a minute; otherwise, it happens when the device reconnects to a network.

Results of the profile installation vary slightly depending on the device's operating system:

- For iOS and Android devices, the profile is added to the existing profiles installed on the device.
- For Windows Phone devices, the profile replaces the current profile of the mailboxes that the selected devices are synchronized with. Because of the way Exchange ActiveSync works, this action also applies the profile to all other devices that are synchronized with the same Exchange mailboxes. (If such other devices are iOS devices, the installed profile does not replace their current profiles, but the profile's settings may override those of any configuration profiles installed on the devices.)

➔ To install configuration profiles on mobile devices:

1. Navigate to a page in the Mobile Devices area that contains the devices you want to install configuration profiles on. For example, you can navigate to **Mobile Devices > All Windows Phone Devices**, then [search for specific devices](#).
2. In the results grid, select the checkbox of each applicable device and click **Commands > Install Configuration Profile**.

---

**NOTE** If you are issuing the command to multiple devices at once, you must select devices of the same OS; that is, select all iOS devices, all Android devices, or all Windows Phone devices.

---

You can also issue the command for a single device from its Device Details page:

- a) In the results grid, click the device you want to install configuration profiles on. The device's Device Details page opens.
  - b) From the Commands sidebar, click **Install Configuration Profile**.
3. Select the checkboxes of the configuration profiles you want to install.  
To quickly find specific configuration profiles, you can use the search field to narrow the profiles listed by specific criteria (for example, by profile name or description).
  4. Click **Install Profile**.
  5. Click **OK** to close the confirmation message.

## Removing Configuration Profiles from Devices


You can remotely remove configuration profiles from mobile devices. For Windows Phone devices only, the removed profile is replaced with the settings of the default ActiveSync policy specified on the Exchange server.

After you issue the command, the configuration profile is removed from the device as soon as it next contacts the notification server of its OS vendor. If the device is connected to a Wi-Fi or mobile network, this action is usually carried out within a minute; otherwise, it happens when the device reconnects to a network.

➔ To remove configuration profiles from a mobile device:

1. Navigate to a page in the Mobile Devices area that contains the device you want to remove configuration profiles from. For example, you can navigate to **Mobile Devices > All Mobile Devices**, then [search for a specific device](#).
2. In the results grid, click the applicable device.
3. Click the device's **Configuration Profiles** tab.
4. Select the checkbox of each configuration profile you want to remove.

To quickly find specific configuration profiles, you can use the search field to narrow the profiles listed by specific criteria (for example, by profile name or identifier).

5. Click .
6. Click **Uninstall**.
7. Click **OK** to close the confirmation message.

---

**NOTE** You may need to click your browser's refresh button to see updated information in the results grid.

---

## Installing Provisioning Profiles on Devices

You can remotely install existing provisioning profiles on iOS devices. A provisioning profile is a binary file that contains the necessary digital certificate, App ID, and UDIDs to allow an enterprise or beta application to be distributed to an iOS device outside of the App Store. While provisioning profiles are normally automatically installed as part of an application, it may be necessary to manually install them in special situations. Before you can install a provisioning profile from Absolute Manage Web Admin, you must import the profile using the Absolute Manage Admin interface.

After you issue the command, the provisioning profile is installed on the device as soon as it next contacts the notification server of its OS vendor. If the device is connected to a Wi-Fi or mobile network, this action is usually carried out within a minute; otherwise, it happens when the device reconnects to a network.

➔ To install provisioning profiles on iOS devices:

1. Navigate to a page in the Mobile Devices area that contains the iOS devices you want to install provisioning profiles on. For example, you can navigate to **Mobile Devices > All iOS Devices**, then [search for specific devices](#).
2. In the results grid, select the checkbox of each applicable device and click **Commands > Install Provisioning Profile**.

You can also issue the command for a single device from its Device Details page:

- a) In the results grid, click the device you want to install provisioning profiles on. The device's Device Details page opens.
  - b) From the Commands sidebar, click **Install Provisioning Profile**.
3. Select the checkboxes of the provisioning profiles you want to install.  
To quickly find specific provisioning profiles, you can use the search field to narrow the profiles listed by specific criteria (for example, by profile name or UUID).
  4. Click **Install Profile**.
  5. Click **OK** to close the confirmation message.

## Removing Provisioning Profiles from Devices


You can remotely remove provisioning profiles from iOS devices. When you delete a provisioning profile from a device, any applications that rely on that profile for authorization can no longer be used on the device after the next time the device (not the application) is restarted.

After you issue the command, the provisioning profile is removed from the device as soon as it next contacts the notification server of its OS vendor. If the device is connected to a Wi-Fi or mobile network, this action is usually carried out within a minute; otherwise, it happens when the device reconnects to a network.

➔ To remove provisioning profiles from an iOS device:

1. Navigate to a page in the Mobile Devices area that contains the device you want to remove provisioning profiles from. For example, you can navigate to **Mobile Devices > All iOS Devices**, then [search for a specific device](#).
2. In the results grid, click the applicable device.
3. Click the device's **Provisioning Profiles** tab.
4. Select the checkbox of each provisioning profile you want to remove.

To quickly find specific provisioning profiles, you can use the search field to narrow the profiles listed by specific criteria (for example, by profile name or identifier).

5. Click .
6. Click **Uninstall**.
7. Click **OK** to close the confirmation message.

---

**NOTE** You may need to click your browser's refresh button to see updated information in the results grid.

---

## Setting Device Ownership

You can specify the type of owner that mobile devices belong to. Specifying this information is useful if you want to quickly group devices by ownership type during the policy creation process.

➔ To set device ownership:

1. Navigate to a page in the Mobile Devices area that contains the devices whose ownership you want to set. For example, you can navigate to **Mobile Devices > All Mobile Devices**, then [search for specific devices](#).
2. In the results grid, select the checkbox of each applicable device and click **Commands > Set Device Ownership**.

You can also issue the command for a single device from its Device Details page:

- a) In the results grid, click the device whose ownership you want to set. The device's Device Details page opens.
  - b) From the Commands sidebar, click **Set Device Ownership**.
3. Select one of the following options:
    - **Undefined**: No ownership information is specified for the device.
    - **The company**: The device belongs to your organization.
    - **The user (personal device)**: The device belongs to its user.
    - **A guest**: The device belongs to a visitor of your network; that is, a person who is permitted to have access to your network but is not an employee.
  4. Click **Set Ownership**.
  5. Click **OK** to close the confirmation message.

## Setting the Enrollment User for Devices

You can specify the network account of the user that a mobile device belongs to. If you do not specify this information, the device is marked as not belonging to a user but it still remains a managed device.

➔ To set the enrollment user for mobile devices:

1. Navigate to a page in the Mobile Devices area that contains the devices whose enrollment user you want to set. For example, you can navigate to **Mobile Devices > All Mobile Devices**, then [search for specific devices](#).
2. In the results grid, select the checkbox of each applicable device and click **Commands > Set Device Enrollment User**.

You can also issue the command for a single device from its Device Details page:

- a) In the results grid, click the device whose enrollment user you want to set. The device's Device Details page opens.
  - b) From the Commands sidebar, click **Set Device Enrollment User**.
3. In the **Username** field, enter the user name of the Active Directory or Open Directory account you want to associate with the device.
  4. In the **Domain** field, enter the domain that the account belongs to.

---

**NOTE** Domain information is not required for Open Directory accounts.

---

5. Click **Set User**.
6. Click **OK** to close the confirmation message.

## Setting Organization Information on Devices

You can remotely set basic contact information for your organization on mobile devices that run iOS 7 and higher. While these details are stored on the device, they are not visible to the device's user.

➔ To set organization information on devices running iOS 7 and higher:

1. Navigate to a page in the Mobile Devices area that contains the devices you want to set organization information on. For example, you can navigate to **Mobile Devices > All iOS Devices**, then [search for specific devices](#).
2. In the results grid, select the checkbox of each applicable device and click **Commands > Set Organization Info**.

---

**NOTE** If you are issuing the command to multiple devices at once, all selected devices must be running iOS 7 or higher.

---

You can also issue the command for a single device from its Device Details page:

- a) In the results grid, click the device whose organization information you want to set. The device's Device Details page opens.
  - b) From the Commands sidebar, click **Set Organization Info**.
3. Complete the following fields:
    - **Name:** Your organization's name
    - **Phone Number:** Your organization's telephone number
    - **Email:** Your organization's email address
    - **Address:** Your organization's street address
    - **Comments:** Additional information about your organization that you want to store on the selected mobile devices

---

**NOTE** If you want to remove all organization information that is currently stored on a device, clear the text in these fields.

---

4. Click **Set Info**.
5. Click **OK** to close the confirmation message.

## Setting Activation Lock Options

Devices running iOS 7 and higher include the Activation Lock feature, which is part of Apple's Find My iPhone service. The Activation Lock feature requires the input of the device user's Apple ID and password before a device can be reactivated or erased.

By default, the Activation Lock feature is not active on supervised devices when Find My iPhone is turned on. You can choose whether you want the feature to be enabled or disabled on a device when Find My iPhone is turned on.

This command applies only to supervised devices running iOS 7 or higher.

---

**NOTE** You cannot disable the Activation Lock feature using this command if the feature is currently enabled on a device. For information on disabling the Activation Lock feature when it is currently enabled on a device, see "Disabling the activation lock when it is already active" in the *Absolute Manage User Guide*.

---

➔ To set Activation Lock options on supervised devices running iOS 7 and higher:

1. Navigate to a page in the Mobile Devices area that contains the devices you want to set Activation Lock options on. For example, you can navigate to **Mobile Devices > All iOS Devices**, then [search for specific devices](#).
2. In the results grid, select the checkbox of each applicable device and click **Commands > Set Activation Lock Options**.

---

**NOTE** If you are issuing the command to multiple devices at once, all selected devices must be supervised devices running iOS 7 or higher.

---

You can also issue the command for a single device from its Device Details page:


- a) In the results grid, click the device whose Activation Lock options you want to set. The device's Device Details page opens.
  - b) From the Commands sidebar, click **Set Activation Lock Options**.
3. Click one of the following buttons:
    - **Allow Activation:** Whenever Find My iPhone is enabled on the selected devices, the Activation Lock feature will also be enabled. Whenever Find My iPhone is disabled, the Activation Lock feature will also be disabled.
    - **Disallow Activation:** The Activation Lock feature can no longer be enabled on the selected devices. It will remain off regardless of whether Find My iPhone is turned on. However, if the Activation Lock feature is currently enabled on a selected device, it will remain enabled.
  4. Click **OK** to close the confirmation message.




## Setting Custom Field Values

You can manually enter and delete data for custom fields associated with a mobile device. This task describes how to set custom field values for an individual mobile device; to set custom field values on multiple devices, [create a Set Custom Field Value action](#) and [assign it to a smart policy](#).

➔ To enter a custom field value for a mobile device:

1. Navigate to a page where the mobile device is listed. For example, go to the **Mobile Devices** > **All Mobile Devices** page for a list of all your organization's mobile devices.
2. In the results grid, click the mobile device that you want to enter custom field values for.
3. Click the **Custom Fields** tab.
4. In the results grid, select the checkbox of the custom field whose value you want to set.
5. Click .
6. Enter a value for the custom field. The value you can enter is determined by the field's data type:
  - **String** – Any unformatted text
  - **Number** – A number in the display format indicated
  - **Boolean** – A true or false value
  - **Date** – A specific date and time
  - **File Version** – A version number according to the conventions of the target mobile device platform. A valid file version number for iOS consists of up to three integers, separated by periods and optionally followed by one of the letters "a", "b", "d", or "f " and another integer (for example, 1.0, 2.4.1, 6.8d1). A valid file version number for Android and Windows Phone consists of up to four integers, separated by periods (for example, 5.7, 3.0.0.233).
  - **IP Address** – An IPv4 address (for example, 192.168.0.1)
  - **Enumeration** – A value from a predefined list
7. Click **Save**.
8. Click **OK** to close the confirmation message.

➔ To delete custom field values for a mobile device:

1. Navigate to a page where the mobile device is listed. For example, go to the **Mobile Devices** > **All Mobile Devices** page for a list of all your organization's mobile devices.
2. In the results grid, click the mobile device that you want to delete custom field values for.
3. Click the **Custom Fields** tab.
4. In the results grid, select the checkbox of the custom fields whose value you want to delete.
5. Click .
6. Click **Remove**.
7. Click **OK** to close the confirmation message.

## Retrying Failed Installations

You can issue a command to retry the installation of configuration and provisioning profiles or of applications that previously failed on a mobile device. When you issue this command to a device, Absolute Manage attempts to install all profiles or applications that are assigned to any policies the device belongs to and that are not yet present on the device.

➔ To retry failed installations of profiles or applications on mobile devices:

1. Navigate to a page in the Mobile Devices area that contains the devices you want to retry the installation on. For example, you can navigate to **Mobile Devices > All Mobile Devices**, then [search for specific devices](#).
2. In the results grid, select the checkbox of each applicable device and click **Commands > Retry All...**

You can also issue the command for a single device from its Device Details page:

- a) In the results grid, click the device you want to retry the installation on. The device's Device Details page opens.
  - b) From the Commands sidebar, click **Retry All...**
3. Select one of the following options:
    - **Retry All Failed Profiles:** Retries all configuration and provisioning profile installations that have previously failed for the selected devices
    - **Retry All Failed Applications:** Retries all application installations that have previously failed for the selected devices
  4. Click **Retry**.
  5. Click **OK** to close the confirmation message.

## Adding Devices to Policies

You can add a mobile device to existing standard policies. Because devices are dynamically added to smart policies on the fly based on pre-defined criteria, you cannot add a mobile device to this type of policy manually.

➔ To add a mobile device to existing standard policies:

1. Navigate to a page in the **Mobile Devices** area that contains the device you want to add to policies. For example, you can navigate to **Mobile Devices > All Mobile Devices**, then [search for a specific device](#).
2. In the results grid, click the device you want to add to policies.
3. Click the device's **Mobile Policies** tab.
4. Click **Add Mobile Device to Policies**.
5. Select the checkbox of the standard policies you want to add the device to.

To quickly find specific policies, you can use the search field to narrow the items listed by specific criteria (for example, by policy name).

6. Click **Add Policy**.
7. Click **OK** to close the confirmation message.

## Working with Policies

Use the Mobile Policies area to create [standard or smart policies](#) and to manage mobile policies that already exist in the system. Policies can help you automate certain aspects of mobile device administration.

You can [search for individual policies](#) using specific criteria in the Search field.

From the Mobile Policies area, you can perform the following tasks:

- [Viewing Policy Details](#)
- [Creating Standard Policies](#)
- [Creating Smart Policies](#)
- [Editing Policies](#)
- [Deleting Policies](#)

## About Policies

You can automate certain aspects of mobile device administration by using policies. A policy includes a collection of target mobile devices, plus one or more of the following elements:

- Third-party applications, which you can manage in the following ways:
  - Automatically install on devices that are added to the policy and delete from devices that are removed from the policy
  - Automatically install on devices that are added to the policy and leave on devices that are removed from the policy
  - Allow on devices belonging to the policy
  - Allow on devices that are added to the policy and delete from devices that are removed from the policy
- In-house applications, which you can manage in the following ways:
  - Automatically install on devices that are added to the policy and delete from devices that are removed from the policy
  - Automatically install on devices that are added to the policy and leave on devices that are removed from the policy
  - Prohibit on devices belonging to the policy
  - Allow on devices belonging to the policy
  - Allow on devices that are added to the policy and delete from devices that are removed from the policy
- Configuration profiles, which you can manage in the following ways:
  - Make mandatory on devices belonging to the policy
  - Make available to devices belonging to the policy, which users can install at their discretion
  - Automatically install on devices that are added to the policy and delete from devices that are removed from the policy
  - Prohibit on devices belonging to the policy
- Media files, which you can manage in the following ways:
  - Automatically install on devices that are added to the policy and delete from devices that are removed from the policy
  - Automatically install on devices that are added to the policy and leave on devices that are removed from the policy
  - Allow on devices belonging to the policy
  - Allow on devices that are added to the policy and delete from devices that are removed from the policy
- Actions, which allow you to specify what Absolute Manage should do with a mobile device when it joins a smart policy

---

**NOTE** On some mobile operating systems, users may need to confirm the installation or removal of applications.

---

There are two types of policies you can use to automate mobile device administration:





- **Standard policy:** Allows you to manually add and remove specific mobile devices to and from the policy. The list of devices in a standard policy remains the same until you change it.

- [Smart policy](#): Allows you to set filter criteria that determine which mobile devices should be included in the policy. The list of devices in a smart policy is automatically updated on the fly when devices satisfy the filter criteria you have chosen. You cannot manually add or remove specific mobile devices to and from the policy.

## Viewing Policy Details

You can view the details of an existing policy, including the mobile devices, applications, configuration profiles, media files, and actions that make up the policy.

➔ To view the details of a policy:

1. Navigate to the **Mobile Policies** area.
2. In the results grid, click the policy whose details you want to view.
3. Click the following tabs to view specific information or perform certain tasks on the policy:
  - **Mobile Devices:** Lists all mobile devices that are members of the policy. If you are viewing the details of a standard policy, you can [add and remove mobile devices](#) to and from the policy from this tab. If you are viewing the details of a smart policy, you cannot manually edit the list of mobile devices because the policy's filter determines this list.
  - **In-House Applications:** Lists all in-house applications that are part of the policy. You can [add and remove in-house applications](#) to and from the policy from this tab.
  - **Third-Party Applications:** Lists all third-party applications that are part of the policy. You can [add and remove third-party applications](#) to and from the policy from this tab.
  - **Configuration Profiles:** Lists all configuration profiles that are part of the policy. You can perform the following tasks from this tab:
    - [Add and remove configuration profiles](#) to and from the policy.
    - [Edit the policy assignment rules](#) for a configuration profile by selecting its checkbox and clicking .
  - **Content:** Lists all media files that are part of the policy. You can perform the following tasks from this tab:
    - [Add and remove media files](#) to and from the policy.
    - [Edit the policy assignment rules](#) for a media file by selecting its checkbox and clicking .
  - **Actions:** This tab applies to smart policies only. Lists all actions that are part of the policy. You can perform the following tasks from this tab:
    - [Add and remove actions](#) to and from the policy.
    - [Edit the policy assignment rules](#) for an action by selecting its checkbox and clicking .
    - Re-execute actions on the list by selecting the checkbox of the applicable actions and clicking .

You can quickly find specific results on any of these pages by [using the search field](#) at the top of the page to narrow the items listed by specific criteria (for example, by device model or application name). You can also [customize the column layout](#) of these pages to show the information that is most relevant to you.

## Creating Standard Policies

You can create a standard policy to help automate certain aspects of mobile device administration. A standard policy allows you to choose a selection of mobile devices, then apply certain rules to these devices. For more information, see [About Policies](#).

After you create or edit a policy, any changes to an affected device are made as soon as the device contacts the notification server of its OS vendor. If the device is connected to a Wi-Fi or mobile network, this action is usually carried out within a minute; otherwise, it happens when the device reconnects to a network.

➔ To create a standard policy:

1. Navigate to the **Mobile Policies** area.
2. In the work area toolbar, click **Add Policy > New Policy**.
3. Enter a name for the policy and click **Create Policy**.
4. Click **OK** to close the confirmation message.  
Your new policy is added to the Mobile Policies list.
5. In the results grid, click the policy you just created.
6. In the policy's Mobile Devices tab, click **Add Mobile Devices to Policy**.
7. Select the checkbox of the mobile devices you want to add to the policy.

To quickly find specific devices, you can use the search field to narrow the devices listed by specific criteria (for example, by device model or OS type).

8. Click **Add to Policy**.
9. Click **OK** to close the confirmation message.
10. Complete one or more of the following actions:
  - [Add in-house applications to the policy](#)
  - [Add third-party applications to the policy](#)
  - [Add configuration profiles to the policy](#)
  - [Add mobile content to the policy](#)



## Creating Smart Policies

You can create a smart policy to help automate certain aspects of mobile device administration. A smart policy allows you to set filter criteria to determine the mobile devices included in the policy, then apply certain rules to the devices that match your criteria. For more information, see [About Policies](#).

---

**NOTE** The list of mobile devices included in a smart policy is dynamically updated based on devices matching your filter criteria; therefore, you cannot manually add and remove devices to and from a smart policy.

---

After you create or edit a policy, any changes to an affected device are made as soon as the device contacts the notification server of its OS vendor. If the device is connected to a Wi-Fi or mobile network, this action is usually carried out within a minute; otherwise, it happens when the device reconnects to a network.

➔ To create a smart policy:

1. Navigate to the **Mobile Policies** area.
2. In the work area toolbar, click **Add Policy > New Smart Policy**.
3. In the Set Properties dialog page, do the following:
  - a) Enter a name for the smart policy.
  - b) Select the type of criteria you want to use in your smart policy to filter mobile devices:
    - **Mobile Devices:** Lets you create filters based on any combination of device details
    - **Mobile Devices by Installed Applications:** Lets you create filters based on installed or missing applications
    - **Mobile Devices by Added Configuration Profiles:** Lets you create filters based on installed or missing configuration profiles
  - c) Click **Continue**.
4. In the Create Smart Filter dialog page, do the following:
  - a) Add one or more filters. For more information, see [Understanding Filters](#).
  - b) Click **Continue**.
5. In the Verify and Save dialog page, review the filters you have created. If necessary, you can edit the filters by clicking **Back**.
6. If you are satisfied with your filters, click **Save**.
7. Click **OK** to close the confirmation message.

Within the Mobile Devices tab of the smart policy, you can see the list of devices that currently match your filter criteria.

8. Complete one or more of the following actions:
  - [Add in-house applications to the policy](#)
  - [Add third-party applications to the policy](#)
  - [Add configuration profiles to the policy](#)
  - [Add mobile content to the policy](#)
  - [Add actions to the policy](#)

## Understanding Filters

You can use filters in a smart policy to determine the mobile devices that should be part of the policy. For example, you may want to create a policy that installs certain configuration profiles only on mobile devices running iOS 6 and lower. Because you have hundreds of devices in your deployment, you do not want to manually pick and choose the devices to include in your policy; rather, you want the system to automatically create and update the list of included devices on the fly. A smart policy manages the list of included devices for you based on the filters you have set. (See [Creating Smart Policies](#) for more information on creating smart policies.)

### Using the Filter Fields

A filter consists of two or more fields, depending on the filter criterion you use. The following are examples of filters you can specify within a smart policy:

 A filter configuration interface showing three fields: a dropdown menu with 'Mobile Device Managed', a dropdown menu with 'true', and a red minus button to the right.

**Example 1:** This filter isolates mobile devices that are actively managed by Absolute Manage.

 A filter configuration interface showing three fields: a dropdown menu with 'Mobile Device OS Platform', a dropdown menu with 'is', and a dropdown menu with 'iOS', followed by a red minus button.

**Example 2:** This filter isolates mobile devices that are running any version of the iOS operating system.

 A filter configuration interface showing three fields: a dropdown menu with 'Mobile Device OS Version', a dropdown menu with 'is less than or equal to', and a text input field with '6', followed by a red minus button.

**Example 3:** This filter isolates mobile devices that are running version 6 or lower of any operating system.

The fields contained in a filter are defined as follows:

- First field = Filter criteria: A list of available filter criteria (for example, **Mobile Device Managed**)
- Second field = Operator: A list of operators specific to the selected filter criterion (for example, **is less than or equal to**)
- Third field = Value: A text field or list box where you can enter or select a specific value (may or may not be available depending on the filter criterion you selected)
- Fourth field = Value type: A list of possible value types to further define the value you entered in the previous field (may or may not be available depending on the filter criterion you selected)

For example, to isolate all mobile devices whose warranty is expiring in the next 30 days, you can create a filter as follows:

- Filter criteria = **Mobile Device Warranty End**
- Operator = **is in the next**
- Value = **30**
- Value type = **Days**

### Combining Filters


You can combine filters to produce the results you want:

- To refine your results, select **All** from the list above the filter area and click **Add Filter** to specify additional filters. This action places the "AND" operator between each filter and produces only those results that satisfy all filters.

- To expand your results, select **Any** from the list above the filter area and click **Add Filter** to specify additional filters. This action places the "OR" operator between each filter and produces results that satisfy at least one of the filters.

You can add as many filters as required to generate your desired results.

## Removing Filters

You may want to remove one or more filters. To remove an individual filter, click the  icon next to the filter.

## Working with In-House Applications Inside a Policy

For iOS and Android devices, you can use in-house applications within a policy in the following ways:

- Make in-house applications available for on-demand installation by users of mobile devices that belong to the policy
- Automatically install in-house applications on mobile devices that belong to the policy
- Prohibit the installation of in-house applications on mobile devices that belong to the policy

Before you can add an in-house application to a policy from Absolute Manage Web Admin, you must import the application file as a mobile application package using the Absolute Manage Admin interface. For more information, see "Installing software on mobile devices" in the *Absolute Manage User Guide*.

Depending on the operating system of the mobile device, the user may need to confirm the installation or removal of applications:

- Silent installation (the application is installed without user confirmation) is supported on some Samsung Galaxy devices
- Silent removal (the application is removed without user confirmation) is supported on some Samsung Galaxy devices and devices running iOS 5 or higher (only for applications installed through Absolute Manage)

Policy actions take place on any mobile device belonging to the policy as soon as the device contacts the notification server of its OS vendor. If the device is connected to a Wi-Fi or mobile network, this action usually takes place within a minute; otherwise, it happens when the device reconnects to a network. With on-demand installation of applications, you can [send a message](#) to or email the users of the devices to notify them of the availability of a new application.

After you add an in-house application to a policy, you cannot edit the application's assignment properties within the policy. If you want to edit these properties, you must remove the application from the policy and re-add it using the desired properties.

## Adding In-House Applications to a Policy

➔ To add in-house applications to a policy:

1. Navigate to the **Mobile Policies** area.
2. Click the policy that you want to add in-house applications to.
3. Click the **In-house Applications** tab.
4. In the work area toolbar, click **Add In-House Application**.
5. Select the checkbox of each in-house application you want to add to the policy.

To quickly find specific applications, you can use the search field to narrow the applications listed by specific criteria (for example, by application name or version number).

6. From the **Assignment Rule** list, select how you want to manage the selected applications on devices belonging to the policy:
  - **Auto-install**: The application is installed when a device enters the policy. The application remains on the device when it leaves the policy, and the device's user can manually delete the application, if desired.
  - **On-demand**: The application is made available within AbsoluteApps and the device's user can manually install the application. The application remains on the device when it leaves the policy, and the device's user can manually delete the application, if desired.

- **Auto-install, Auto-remove:** The application is installed when the device enters the policy and removed when it leaves.
- **On-demand, Auto-remove:** The application is made available within AbsoluteApps and the device's user can manually install the application. The application is removed when the device leaves the policy.
- **Forbidden:** The application cannot be installed on devices belonging to the policy.

---

**NOTE** For information about on-demand installation on iOS devices, please contact [Absolute Global Support](#).

---

7. If you want the policy to restrict the availability of the selected applications to certain dates or times, select the **Set availability time** checkbox, then choose one of the following options:
  - **Every day between:** The application is available to mobile devices belonging to this policy only during a certain time of the day (for example, during office hours). Specify the start and end times in the available fields.
  - **From:** The application is available to mobile devices belonging to this policy only during a specific time period. Specify the start date and time as well as the end date and time.

---

**NOTE** Use your local time in these fields. Times you enter are converted to and stored in Coordinated Universal Time (UTC) on the Absolute Manage server. As a result, you should take into account any time differences that may exist with your mobile clients. You also must manually compensate for Daylight Saving Time (DST), if desired, because DST does not apply to UTC.


---

8. Click **Add to Policy**.
9. Click **OK** to close the confirmation message.

## Removing In-House Applications from a Policy

When you remove an application from a policy, there is no immediate effect on the mobile devices that belong to the policy. That is, when you remove an application that is set to "auto-install", it is not removed from the policy's devices, and when you remove an application that is set to "forbidden", it is not installed on the policy's devices. However, the restrictions placed on mobile devices with respect to the application are lifted: the user can now remove a previously required application or install a previously prohibited application.

➔ To remove in-house applications from a policy:

1. Navigate to the **Mobile Policies** area.
2. Click the policy that you want to remove in-house applications from.
3. Click the **In-house Applications** tab.
4. Select the checkbox of each application that you want to remove.
5. Click .
6. Click **Remove Applications**.
7. Click **OK** to close the confirmation message.

## Working with Third-Party Applications Inside a Policy

For iOS and Android devices, you can use third-party applications within a policy in the following ways:

- Make third-party applications available for on-demand installation by users of mobile devices that belong to the policy
- Automatically install third-party applications on mobile devices that belong to the policy

Before you can add a third-party application to a policy from Absolute Manage Web Admin, you must import the application file as a mobile application package using the Absolute Manage Admin interface. For more information, see "Installing software on mobile devices" in the *Absolute Manage User Guide*.

Depending on the operating system of the mobile device, the user may need to confirm the installation or removal of applications:

- Silent installation (the application is installed without user confirmation) is supported on some Samsung Galaxy devices
- Silent removal (the application is removed without user confirmation) is supported on some Samsung Galaxy devices and devices running iOS 5 or higher (only for applications installed through Absolute Manage)

Policy actions take place on any mobile device belonging to the policy as soon as the device next contacts the notification server of its OS vendor. If the device is connected to a Wi-Fi or mobile network, this action usually takes place within a minute; otherwise, it happens when the device has reconnected to a network. With on-demand installation of applications, you can [send a message](#) to or email the users of the devices to notify them of the availability of a new application.

After you add a third-party application to a policy, you cannot edit the application's assignment properties within the policy. If you want to edit these properties, you must remove the application from the policy and re-add it using the desired properties.

## Adding Third-Party Applications to a Policy

➔ To add third-party applications to a policy:

1. Navigate to the **Mobile Policies** area.
2. Click the policy that you want to add third-party applications to.
3. Click the **Third-Party Applications** tab.
4. In the work area toolbar, click **Add Third-Party Application**.
5. Select the checkbox of the third-party applications you want to add to the policy.

To quickly find specific applications, you can use the search field to narrow the applications listed by specific criteria (for example, by application name or version number).

6. From the **Assignment Rule** list, select how you want to manage the selected applications on devices belonging to the policy:
  - **Auto-install:** The application is installed when a device enters the policy. The application remains on the device when it leaves the policy, and the device's user can manually delete the application, if desired.
  - **On-demand:** The application is made available within AbsoluteApps and the device's user can manually install the application. The application remains on the device when it leaves the policy, and the device's user can manually delete the application, if desired.

- **Auto-install, Auto-remove:** The application is installed when the device enters the policy and removed when it leaves.
- **On-demand, Auto-remove:** The application is made available within AbsoluteApps and the device's user can manually install the application. The application is removed when the device leaves the policy.

---

**NOTE** For information about on-demand installation on iOS devices, please contact [Absolute Global Support](#).

---

7. If you want the policy to restrict the availability of the selected applications to certain dates or times, select the **Set availability time** checkbox, then choose one of the following options:
  - **Every day between:** The application is available to mobile devices belonging to this policy only during a certain time of the day (for example, during office hours). Specify the start and end times in the available fields.
  - **From:** The application is available to mobile devices belonging to this policy only during a specific time period. Specify the start date and time as well as the end date and time.

---

**NOTE** Use your local time in these fields. Times you enter are converted to and stored in Coordinated Universal Time (UTC) on the Absolute Manage server. As a result, you should take into account any time differences that may exist with your mobile clients. You also must manually compensate for Daylight Saving Time (DST), if desired, because DST does not apply to UTC.


---

8. Click **Add to Policy**.
9. Click **OK** to close the confirmation message.

## Removing Third-Party Applications from a Policy

When you remove an application from a policy, there is no immediate effect on the mobile devices that belong to the policy. That is, when you remove an application that is set to "auto-install", it is not removed from the policy's devices, and when you remove an application that is set to "forbidden", it is not installed on the policy's devices. However, the restrictions placed on mobile devices with respect to the application are lifted: the user can now remove a previously required application or install a previously prohibited application.

➔ To remove third-party applications from a policy:

1. Navigate to the **Mobile Policies** area.
2. Click the policy that you want to remove third-party applications from.
3. Click the **Third-Party Applications** tab.
4. Select the checkbox of the applications that you want to remove.
5. Click .
6. Click **Remove Applications**.
7. Click **OK** to close the confirmation message.

## Working with Configuration Profiles Inside a Policy

You can use configuration profiles within a policy in the following ways:

- Make configuration profiles available for on-demand installation by users of mobile devices that belong to the policy (iOS and Android devices only)
- Automatically install configuration profiles on mobile devices that belong to the policy
- Prohibit the installation of configuration profiles on mobile devices that belong to the policy

Before you can add a configuration profile to a policy from Absolute Manage Web Admin, you must import or create the profile using the Absolute Manage Admin interface. For more information, see "Working with configuration profiles" in the *Absolute Manage User Guide*.

Policy actions take place on any mobile device belonging to the policy as soon as the device contacts the notification server of its OS vendor. If the device is connected to a Wi-Fi or mobile network, this action usually takes place within a minute; otherwise, it happens when the device reconnects to a network.

It is possible to use the same configuration profile inside multiple policies in conflicting ways. For example, a device could belong to one policy where the profile is auto-installed and to another policy where the profile is forbidden. Since there is no way to satisfy both policies' requirements at the same time, Absolute Manage uses the following hierarchy for carrying out profile actions, where higher entries take precedence over lower entries:

- Forbidden
- Auto-install
- On-demand
- Auto-remove

For example, if a configuration profile is auto-installed in one policy that a mobile device belongs to and forbidden in another, the profile is not available on the device because the "forbidden" category has a higher priority than "auto-install".

---

**NOTE** Only one configuration profile (that is, the Exchange ActiveSync policy) can be active on a Windows Phone device at any time. As a result, profiles are not installed on Windows Phone devices when the Absolute Manage policies that the devices belong to specify more than one profile as automatically installed.

---

After you add a configuration profile to a policy, you cannot edit the profile's assignment properties within the policy. If you want to edit these properties, you must remove the configuration profile from the policy and re-add it using the desired properties.

### Adding Configuration Profiles to a Policy

➔ To add configuration profiles to a policy:

1. Navigate to the **Mobile Policies** area.
2. Click the policy that you want to add configuration profiles to.
3. Click the **Configuration Profiles** tab.
4. In the work area toolbar, click **Add Configuration Profile**.
5. Select the checkbox of each configuration file you want to add to the policy.



To quickly find specific configuration profiles, you can use the search field to narrow the profiles listed by specific criteria (for example, by profile name or description).

6. From the **Assignment Rule** list, select how you want to manage the selected profiles on devices belonging to the policy:
  - **Auto-install:** The profile is automatically installed when a device enters the policy. The profile remains on the device when it leaves the policy, and the device's user can manually remove the profile, if desired.
  - **On-demand:** The profile is made available within AbsoluteApps and the device's user can manually install the profile. The profile remains on the device when it leaves the policy, and the device's user can manually remove the profile, if desired.
  - **Auto-install, Auto-remove:** The profile is installed when the device enters the policy and removed when it leaves.
  - **On-demand, Auto-remove:** The profile is made available within AbsoluteApps and the device's user can manually install the profile. The profile is removed when the device leaves the policy.
  - **Forbidden:** The profile cannot be installed on devices belonging to the policy.

---

**NOTE** On-demand profile installation is available on iOS and Android devices only. For information about on-demand profile installation on iOS devices, contact [Absolute Global Support](#).

---

7. To restrict the availability of the selected profiles to certain dates or times, select the **Set availability time** checkbox, then choose one of the following options:
  - **Every day between:** The profile is available to mobile devices belonging to this policy only during a certain time of the day (for example, during office hours). Specify the start and end times in the available fields.
  - **From:** The profile is available to mobile devices belonging to this policy only during a specific time period. Specify the start date and time as well as the end date and time.

---

**NOTE** Use your local time in these fields. Times you enter are converted to and stored in Coordinated Universal Time (UTC) on the Absolute Manage server. As a result, you should take into account any time differences that may exist with your mobile clients. You also must manually compensate for Daylight Saving Time (DST), if desired, because DST does not apply to UTC.


---

8. Click **Add to Policy**.
9. Click **OK** to close the confirmation message.

## Editing Assignment Rules of Configuration Profiles

➔ To edit the assignment rules of configuration profiles inside a policy:

1. Navigate to the **Mobile Policies** area.
2. Click the policy that you want to edit.
3. Click the **Configuration Profiles** tab.
4. Select the checkbox of each configuration profile whose assignment rules you want to change.

5. Click .
6. From the **Assignment Rule** list, select how you want to manage the selected profiles on devices belonging to the policy:
  - **Auto-install**: The profile is automatically installed when a device enters the policy. The profile remains on the device when it leaves the policy, and the device's user can manually remove the profile, if desired.
  - **On-demand**: The profile is made available within AbsoluteApps and the device's user can manually install the profile. The profile remains on the device when it leaves the policy, and the device's user can manually remove the profile, if desired.
  - **Auto-install, Auto-remove**: The profile is installed when the device enters the policy and removed when it leaves.
  - **On-demand, Auto-remove**: The profile is made available within AbsoluteApps and the device's user can manually install the profile. The profile is removed when the device leaves the policy.
  - **Forbidden**: The profile cannot be installed on devices belonging to the policy.
7. To restrict the availability of the selected profiles to certain dates or times, select the **Set availability time** checkbox, then choose one of the following options:
  - **Every day between**: The profile is available to mobile devices belonging to this policy only during a certain time of the day (for example, during office hours). Specify the start and end times in the available fields.
  - **From**: The profile is available to mobile devices belonging to this policy only during a specific time period. Specify the start date and time as well as the end date and time.

---

**NOTE** Use your local time in these fields. Times you enter are converted to and stored in Coordinated Universal Time (UTC) on the Absolute Manage server. As a result, you should take into account any time differences that may exist with your mobile clients. You also must manually compensate for Daylight Saving Time (DST), if desired, because DST does not apply to UTC.

---


8. Click **Save**.
9. Click **Done** to close the confirmation message.

## Removing Configuration Profiles from a Policy

When you remove a configuration profile from a policy, there is no immediate effect on the mobile devices that belong to the policy. That is, when you remove a profile that is set to "auto-install", it is not removed from the policy's devices, and when you remove a profile that is set to "forbidden", it is not installed on the policy's devices. However, the restrictions placed on mobile devices with respect to the configuration profile are lifted: the user can now remove a previously required profile or install a previously prohibited profile.

➔ To remove configuration profiles from a policy:

1. Navigate to the **Mobile Policies** area.
2. Click the policy that you want to remove configuration profiles from.
3. Click the **Configuration Profiles** tab.
4. Select the checkbox of each policy that you want to remove.

5. Click .
6. Click **Remove Profiles**.
7. Click **OK** to close the confirmation message.

## Working with Media Files Inside a Policy

For iOS and Android devices, you can use media files within a policy in the following ways:

- Make media files available for on-demand installation within AbsoluteSafe by users of mobile devices that belong to the policy
- Automatically download media files through AbsoluteSafe to mobile devices that belong to the policy

Mobile devices must have the AbsoluteSafe application installed in order for users to access media files made available to them through policies.

Before you can add media files to a policy, you must [import the files into Absolute Manage](#).

Policy actions take place on any mobile device belonging to the policy as soon as the device contacts the notification server of its OS vendor. If the device is connected to a Wi-Fi or mobile network, this action usually takes place within a minute; otherwise, it happens when the device reconnects to a network. You can [send a message](#) to or email the users of the devices to notify them of the availability of new media files.

### Adding Media Files to a Policy

➔ To add media files to a policy:

1. Navigate to the **Mobile Policies** area.
2. Click the policy that you want to add media files to.
3. Click the **Content** tab.
4. In the work area toolbar, click **Add Content to Policy**.
5. Select the checkbox of each media file you want to add to the policy.

To quickly find specific media files, you can use the search field to narrow the files listed by specific criteria (for example, by file name or media category).

6. From the **Assignment Rule** list, select how you want to manage the selected media files on devices belonging to the policy:
  - **Auto-install**: The media file is downloaded when a device enters the policy. The file remains on the device when it leaves the policy, and the device's user can manually delete the file, if desired.
  - **On-demand**: The media file is made available within AbsoluteSafe and the device's user can manually download the file. The file remains on the device when it leaves the policy, and the device's user can manually delete the file, if desired.
  - **Auto-install, Auto-remove**: The media file is downloaded when the device enters the policy and deleted when it leaves.
  - **On-demand, Auto-remove**: The media file is made available within AbsoluteSafe and the device's user can manually download the file. The file is deleted when the device leaves the policy.
7. If you want the policy to restrict the availability of the selected media files to certain dates or times, select the **Set availability time** checkbox, then choose one of the following options:
  - **Every day between**: The media file is available to mobile devices belonging to this policy only during a certain time of the day (for example, during office hours). Specify the start and end times in the available fields.

- **From:** The media file is available to mobile devices belonging to this policy only during a specific time period. Specify the start date and time as well as the end date and time.

---


**NOTE** Use your local time in these fields. Times you enter are converted to and stored in Coordinated Universal Time (UTC) on the Absolute Manage server. As a result, you should take into account any time differences that may exist with your mobile clients. You also must manually compensate for Daylight Saving Time (DST), if desired, because DST does not apply to UTC.

---

8. Click **Add to Policy**.
9. Click **Done** to close the confirmation message.

## Editing Assignment Rules of Media Files

➔ To edit the assignment rules of media files inside a policy:

1. Navigate to the **Mobile Policies** area.
2. Click the policy that you want to edit.
3. Click the **Content** tab.
4. Select the checkbox of each media file whose assignment rules you want to change.
5. Click .
6. From the **Assignment Rule** list, select how you want to manage the selected media files on devices belonging to the policy:
  - **Auto-install:** The media file is downloaded when a device enters the policy. The file remains on the device when it leaves the policy, and the device's user can manually delete the file, if desired.
  - **On-demand:** The media file is made available within AbsoluteSafe and the device's user can manually download the file. The file remains on the device when it leaves the policy, and the device's user can manually delete the file, if desired.
  - **Auto-install, Auto-remove:** The media file is downloaded when the device enters the policy and deleted when it leaves.
  - **On-demand, Auto-remove:** The media file is made available within AbsoluteSafe and the device's user can manually download the file. The file is deleted when the device leaves the policy.
7. If you want the policy to restrict the availability of the selected media files to certain dates or times, select the **Set availability time** checkbox, then choose one of the following options:
  - **Every day between:** The media file is available to mobile devices belonging to this policy only during a certain time of the day (for example, during office hours). Specify the start and end times in the available fields.
  - **From:** The media file is available to mobile devices belonging to this policy only during a specific time period. Specify the start date and time as well as the end date and time.

---

**NOTE** Use your local time in these fields. Times you enter are converted to and stored in Coordinated Universal Time (UTC) on the Absolute Manage server. As a result, you should take into account any time differences that may exist with your mobile clients. You also must

---

---


manually compensate for Daylight Saving Time (DST), if desired, because DST does not apply to UTC.

---

8. Click **Edit Content**.
9. Click **Done** to close the confirmation message.

## Removing Media Files from a Policy

➔ To remove media files from a policy:

1. Navigate to the **Mobile Policies** area.
2. Click the policy that you want to remove media files from.
3. Click the **Content** tab.
4. Select the checkbox of each media file you want to remove.
5. Click .
6. Click **Remove Content**.
7. Click **OK** to close the confirmation message.

## Working with Actions Inside a Policy

You can use actions within a smart policy to specify tasks that should be automatically performed on mobile devices when they join the policy. You cannot use actions with standard policies.

Actions must already be available within the [Assignable Items > Actions](#) area before you can add them to a smart policy.

When you add an action to a smart policy, the action is carried out on all mobile devices that are currently a member of the policy as soon as the devices contact the notification server of their OS vendor. If a device is connected to a Wi-Fi or mobile network, this action usually takes place within a minute; otherwise, it happens when the device reconnects to a network. Actions are also carried out on each mobile device that joins the smart policy in the future.

### Adding Actions to a Smart Policy

➔ To add actions to a smart policy:

1. Navigate to the **Mobile Policies** area.
2. Click the smart policy that you want to add actions to.
3. Click the **Actions** tab.
4. In the work area toolbar, click **Add Actions to Policy**.
5. Select the checkbox of each action you want to add to the smart policy.

To quickly find specific actions, you can use the search field to narrow the actions listed by specific criteria (for example, by action name).

6. Specify whether you want to delay or repeat the action:
  - Select **Action start delay** if you do not want the action to be performed immediately when a mobile device joins the smart policy, but only after the interval you specify has elapsed.
  - Select **Action repeat** if you want the action to be repeated on the mobile device after the interval you specify for the number of times you specify.

You can combine both of these options, if desired. For example, you could use both options to send a message to mobile devices two hours after they join the policy and every hour thereafter.

---

**NOTE** Any delays and repetitions you specify apply to both existing and future members of the smart policy. The delay for existing members is calculated from the moment the action is assigned to the smart policy. A delayed or repeated action is not carried out on a mobile device if it is no longer a member of the smart policy.


---

7. Click **Save**.
8. Click **Done** to close the confirmation message.

### Editing Assignment Rules of Actions

➔ To edit the assignment rules of an action inside a smart policy:

1. Navigate to the **Mobile Policies** area.
2. Click the smart policy that you want to edit.
3. Click the **Actions** tab.

4. Select the checkbox of the action whose assignment rules you want to change.
5. Click .
6. Specify whether you want to delay or repeat the action:
  - Select **Action start delay** if you do not want the action to be performed immediately when a mobile device joins the smart policy, but only after the interval you specify has elapsed.
  - Select **Action repeat** if you want the action to be repeated on the mobile device after the interval you specify for the number of times you specify.

You can combine both of these options, if desired. For example, you could use both options to send a message to mobile devices two hours after they join the policy and every hour thereafter.

---

**NOTE** Any delays and repetitions you specify apply to both existing and future members of the smart policy. The delay for existing members is calculated from the moment the action is assigned to the smart policy. A delayed or repeated action is not carried out on a mobile device if it is no longer a member of the smart policy.


---

7. Click **Save**.
8. Click **Done** to close the confirmation message.

## Removing Actions from a Smart Policy

When you remove an action from a smart policy, any remaining repetitions or delayed executions of the action are not carried out. If you want to remove an action from Absolute Manage Web Admin and from all related smart policies, you can [delete the action](#).

➔ To remove actions from a smart policy:

1. Navigate to the **Mobile Policies** area.
2. Click the smart policy that you want to remove actions from.
3. Click the **Actions** tab.
4. Select the checkbox of each action you want to remove.
5. Click .
6. Click **Remove Actions**.
7. Click **OK** to close the confirmation message.



## Editing Policies

You can edit existing policies in the following ways:

- With standard policies, you can change the name of the policy, edit the list of mobile devices belonging to the policy, and move mobile devices from one policy to another.
- With smart policies, you can change the name of the policy and edit the policy's filter criteria.


You can also perform the following tasks on policies:

- [Add or remove in-house applications included in the policy](#)
- [Add or remove third-party applications included in the policy](#)
- [Add or remove configuration profiles included in the policy](#)
- [Add, remove, or change assignment properties of mobile content included in the policy](#)
- For smart policies, [add, remove, or change assignment properties of actions included in the policy](#)


To edit the assignment properties of in-house applications or third-party applications within a policy, you must remove the application from the policy and re-add it using the desired properties.

## Editing Standard Policies

➔ To change the name of a standard policy:

1. Navigate to the **Mobile Policies** area.
2. Select the checkbox of the policy you want to edit.
3. Click .
4. Enter a new name for the policy.
5. Click **Edit Policy**.
6. Click **OK** to close the confirmation message.

➔ To edit the list of mobile devices belonging to a standard policy:

1. Navigate to the **Mobile Policies** area.
2. Click the policy you want to edit.
3. On the Mobile Devices tab, add or remove mobile devices as required:
  - To add mobile devices to the policy:
    - i) Click **Add Mobile Devices to Policy**.
    - ii) Select the checkbox of each mobile device you want to add (to quickly find specific devices, you can use the search field to narrow the devices listed by specific criteria).
    - iii) Click **Add to Policy**.
  - To remove mobile devices from the policy:
    - i) Select the checkbox of each mobile device you want to remove.
    - ii) Click .
    - iii) Click **Remove Devices**.


---

**NOTE** When you remove mobile devices from a policy, any applications, mobile content, or configuration profiles that are set to "auto-remove" are deleted from those devices.

---


4. Click **OK** to close the confirmation message.

→ To move mobile devices from one standard policy to another:

1. Navigate to the **Mobile Policies** area.
2. Click the standard policy that contains the mobile devices you want to move.
3. On the Mobile Devices tab, select the checkbox of each mobile device you want to move.
4. Click .  
A list of available standard policies opens.
5. Select the checkbox of each policy you want to move the mobile devices to.  
To quickly find specific policies, you can use the search field to narrow the policies listed by specific criteria (for example, by policy name).
6. Click **Move Mobile Devices**.
7. Click **OK** to close the confirmation message.

## Editing Smart Policies

→ To change the name or filter criteria of a smart policy:

1. Navigate to the **Mobile Policies** area.
2. Select the checkbox of the smart policy you want to edit.
3. Click .
4. In the Edit Properties dialog page, do the following as required:
  - a) Enter a new name for the smart policy.
  - b) Change the type of criteria you want to use in your smart policy to filter mobile devices:
    - **Mobile Devices:** Lets you create filters based on any combination of device details
    - **Mobile Devices by Installed Applications:** Lets you create filters based on installed or missing applications
    - **Mobile Devices by Added Configuration Profiles:** Lets you create filters based on installed or missing configuration profiles
  - c) Click **Continue**.
5. In the Edit Smart Filter dialog page, do the following as required:
  - a) Edit the policy's filters. For more information, see [Understanding Filters](#).
  - b) Click **Continue**.
6. In the Verify and Save dialog page, review the filters you have edited. To go back to editing the filters, click **Back**.
7. If you are satisfied with your filters, click **Save**.
8. Click **OK** to close the confirmation message.

Within the Mobile Devices tab of the smart policy, you can see the list of devices that currently match your filter criteria.


## Deleting Policies

When you delete a policy, mobile devices that belong to the policy are affected in the following ways:

Policy Contents	Assignment Rule	Effect On Mobile Device After Policy Deletion
In-house applications Third-party applications	Auto-install	Applications remain on device
	On-demand	Applications are no longer available for download within AbsoluteApps Applications already installed remain on device
	Auto-install, Auto-remove	Applications are removed from device
	On-demand, Auto-remove	Applications are no longer available for download within AbsoluteApps Applications already installed are removed from device
Configuration profiles	Auto-install	Profiles remain on device
	On-demand	Profiles are no longer available for installation within AbsoluteApps Profiles already installed remain on device
	Auto-install, Auto-remove	Profiles are removed from device
	On-demand, Auto-remove	Profiles are no longer available for installation within AbsoluteApps Profiles already installed are removed from device
Media files	Auto-install	Files remain accessible within AbsoluteSafe
	On-demand	Files are no longer available for download within AbsoluteSafe Files already downloaded remain in AbsoluteSafe
	Auto-install, Auto-remove	Files are removed from AbsoluteSafe
	On-demand, Auto-remove	Files are no longer available for download within AbsoluteSafe Files already downloaded are removed from AbsoluteSafe

In addition, any restrictions that a policy places on mobile devices (for example, installing forbidden applications) are lifted after you delete the policy.

➔ To delete policies:

1. Navigate to the **Mobile Policies** area.
2. Select the checkbox of each policy you want to delete.
3. Click .
4. Click **Delete Policy**.
5. Click **OK** to close the confirmation message.

## Working with Assignable Items

Use the Assignable Items area to view and manage items (such as media files and applications) that are available for you to assign to mobile devices and policies.

When you first visit this area, only media files are listed. You can see other items by selecting one of the following item types from the Assignable Items sidebar:

- In-House Applications
- Third-Party Applications
- Bookstore Books
- Configuration Profiles
- Provisioning Profiles
- Actions

You can also [search for individual items](#) using specific criteria in the Search field, as well as [customize the information](#) included in the results grid.

Within the Assignable Items area, you can perform the following tasks:

- [Viewing Media File Details](#)
- [Importing Media Files](#)
- [Editing Media File Properties](#)
- [Deleting Media Files](#)
- [Viewing In-House Application Details](#)
- [Viewing Third-Party Application Details](#)
- [Viewing Electronic Book Details](#)
- [Viewing Configuration Profile Details](#)
- [Viewing Provisioning Profile Details](#)
- [Viewing Action Details](#)
- [Creating Actions](#)
- [Duplicating Actions](#)
- [Deleting Actions](#)

## Importing Media Files

You can import media files using Absolute Manage Web Admin and make them available to managed iOS and Android devices through the AbsoluteSafe application.

During the import process, you can distribute media files through existing [policies](#), which give you granular control over who has access to a particular file. Furthermore, you can optionally prevent media files from being taken out of AbsoluteSafe. Files in AbsoluteSafe are stored in an encrypted format on the mobile device and are not part of any device backup to computers (for example, through iTunes).

While you can distribute any type of file to mobile devices, AbsoluteSafe provides support for users to view the following media files directly within the application:


- Web content
  - HTML pages (HTM, HTML)
  - XML
  - XSL
  - Safari web archive (WEBARCHIVE); iOS only
- Documents
  - PDF
  - Word (DOC, DOCX)\*; iOS only
  - Pages (PAGES); iOS only
  - Rich text (RTF)
  - RTF directory (RTFD); iOS only
  - Unformatted text (TXT)
- Presentations
  - PowerPoint (PPT, PPTX)\*; iOS only
  - Keynote (KEY); iOS only
- Spreadsheets
  - Excel (XLS, XLSX)\*; iOS only
  - Numbers (NUMBERS); iOS only
- Images
  - BMP
  - GIF
  - JPG, JPEG
  - PNG
  - TIF, TIFF; iOS only
  - WEBP; Android only
- Audio\*\*
  - AAC audio (M4A/3GP)
  - AAC audio books (M4B/M4P); iOS only
  - AIFF (AIFF, AIF, AIFC, CDDA); iOS only
  - AMR (AMR, 3GP)
  - FLAC; Android only
  - MIDI (IMY, MID, XMF, MXMF, OTA, RTTTL, RTX); Android only
  - MP3 (MP3, SWA)
  - MPEG audio (MPEG, MPG, MP3, SWA)

- Vorbis (OGG, MKV); Android only
- WAVE (WAV, BWF)
- Video and multimedia\*\*
  - 3GP, 3GPP
  - 3GP2, 3G2
  - AVI
  - MPEG-4 (MP4, M4V)
  - QuickTime (MOV, QT, MQV); iOS only
  - VP8 (WEBM, MKV); Android only

\* Microsoft Office 95 or older formats are not supported.

\*\* Support for audio and video formats depends on the container and codec formats of the mobile device. Therefore, some files may not be playable within AbsoluteSafe even though the container and codec are supported. On some devices, AbsoluteSafe may be able to play additional formats not listed here.

➔ To import media files and distribute them to mobile devices through policies:

1. Navigate to the **Assignable Items** area.
2. In the sidebar, click **Content**. (You can also click  in the top left corner of the screen and then click **Mobile Content**.)
3. Click **Add Content**.
4. In the Upload Files dialog page, do the following:
  - a) Drag the files you want to import to the designated area of the page, or click inside the area to browse and select the files to import.
  - b) If needed, edit the names of the files in the text fields.
  - c) Click **Continue**.
5. In the Assign Properties dialog page, do the following:
  - a) Enter a category that best classifies the files you are importing. Default categories (Documents, Pictures, Multimedia, and Other) appear as suggestions as you type.
  - b) Enter a description in the field provided.  
The description you enter here is visible to mobile device users and should give them an indication of the relevance of the files you are importing.
  - c) If you want mobile device users to be able to view or edit the files in applications other than AbsoluteSafe, select the **Files can leave AbsoluteSafe** checkbox.

---

**IMPORTANT** While not enabling this option reliably prevents the actual file from leaving AbsoluteSafe, the same is not necessarily true for the information contained within the file. For example, a user still could take screenshots of the text in a file and send those images to other people.

---

When this option is enabled, you can select the **User can email files** and **User can print files** checkboxes to provide buttons within AbsoluteSafe to let users quickly execute these two tasks.

- d) If the file is large and you do not want users to experience long download times or excessive data charges, select the **Download files only over Wi-Fi** checkbox.

---

**NOTE** This option requires AbsoluteSafe 1.1 or higher. Earlier versions of AbsoluteSafe ignore it.

---

- e) To set a password for the file, enter and confirm the password in the **Passphrase** fields. Users must enter this passphrase every time they open the file in AbsoluteSafe. If you set a passphrase for a file, it cannot leave AbsoluteSafe. Therefore, you can set a passphrase only for file types that are supported by AbsoluteSafe (see above for supported file types). You cannot enable the **Files can leave AbsoluteSafe** option when you set a passphrase.
  - f) Click **Continue**.
6. In the Assign Policy dialog page, do one of the following:
- If you want to import the media files without assigning them to policies at this point, click **Save**.
  - If you want to assign the media files to existing policies now, do the following:
    - i) Select the checkbox of each policy that you want to add the media files to. To quickly find specific policies, you can use the search field to narrow the items listed by specific criteria (for example, by policy name).
    - ii) From the **Assignment Rule** list, select how you want to manage the selected media files on devices belonging to the policy:
      - **Auto-install**: The media file is downloaded when a device enters the policy. The file remains on the device when it leaves the policy, and the device's user can manually delete the file, if desired.
      - **On-demand**: The media file is made available within AbsoluteSafe and the device's user can manually download the file. The file remains on the device when it leaves the policy, and the device's user can manually delete the file, if desired.
      - **Auto-install, Auto-remove**: The media file is downloaded when the device enters the policy and deleted when it leaves.
      - **On-demand, Auto-remove**: The media file is made available within AbsoluteSafe and the device's user can manually download the file. The file is deleted when the device leaves the policy.
    - iii) To restrict the availability of the selected media files to certain dates or times, select the **Set availability time** checkbox, then choose one of the following options:
      - **Every day between**: The media file is available to mobile devices belonging to this policy only during a certain time of the day (for example, during office hours). Specify the start and end times in the available fields.
      - **From**: The media file is available to mobile devices belonging to this policy only during a specific time period. Specify the start date and time as well as the end date and time.
- 
- NOTE** Use your local time in these fields. Times you enter are converted to and stored in Coordinated Universal Time (UTC) on the Absolute Manage server. As a result, you should take into account any time differences that may exist with your mobile clients. You also must manually compensate for Daylight Saving Time (DST), if desired, because DST does not apply to UTC.
- 
- iv) Click **Save**.
7. Click **Done**.





## Viewing Media File Details


You can view the details of media files that have been imported into Absolute Manage, including the properties, policies, and mobile devices that are associated with each file.


➔ To view the details of a media file:

1. Navigate to the **Assignable Items** area.
2. In the results grid, click the media file whose details you want to view.

The Content Details page opens. The following table provides a summary of the file information available on this page:

Field	Description
Leave AbsoluteSafe	Indicates whether mobile device users are permitted to take this file out of AbsoluteSafe (for example, to view it, edit it in another application, or forward it to other devices). In addition, the following icons may be present that represent actions users can perform on the file from AbsoluteSafe:  - Indicates that users can email the file from within AbsoluteSafe  - Indicates that users can print the file from within AbsoluteSafe
Passcode Present	Indicates whether mobile device users are required to enter a passcode (set in the file's properties) to access the file
Wi-Fi Download Only	Indicates whether the media file is downloaded only when the mobile device is connected over Wi-Fi
File name	The name of the media file
File type	The file type of the media file
Category	The content category that the media file has been assigned to
File size	The size of the media file
Last modified	The date and time (displayed in your local time) when the media file was last edited
Description	The description of the media file

3. Click the following tabs to view specific information or to perform certain actions on the media file:
  - **Policies:** Lists all policies that the media file belongs to. You can perform the following tasks from this tab:
    - [Add the media file to policies](#) from this tab by clicking the **Add Content To Policies** button.
    - [Remove the media file from policies](#) by selecting the checkbox of the applicable policies and clicking .

- [Edit the policy assignment rules](#) for the media file by selecting the checkbox of the applicable policies and clicking .
- **Mobile Devices:** Lists all mobile devices that have access to the media file (that is, mobile devices that are members of the policies to which the media file belongs).



You can quickly find specific results on any of these pages by [using the search field](#) at the top of the page to narrow the items listed by specific criteria (for example, by policy or device name). You can also [customize the column layout](#) of these pages to show the information that is most relevant to you.

## Editing Media File Properties


You can edit the properties of media files that have been imported into Absolute Manage. These properties include a file's name, category, description, and permission options.

You can also edit the list of policies that a media file belongs to, as well as the policy assignment rules that are set for the file.

➔ To edit the properties of a media file:

1. Navigate to the **Assignable Items** area.
2. In the sidebar, click **Content**. (You can also click  in the top left corner of the screen and then click **Mobile Content**.)
3. In the results grid, select the checkbox of the media file you want to edit.
4. Click .
5. Edit the file's properties as required. For more information on media file properties, see [Importing Media Files](#).
6. Click **Save**.
7. Click **Done** to close the confirmation message.

➔ To add a media file to policies:

1. Navigate to the **Assignable Items** area.
2. In the sidebar, click **Content**. (You can also click  in the top left corner of the screen and then click **Mobile Content**.)
3. In the results grid, click the media file you want to edit.
4. Click the **Policies** tab.

The results grid lists all policies that the file currently belongs to.

5. Click **Add Content To Policies**.
6. Select the checkbox of each policy you want to add the media file to.

To quickly find specific media files, you can use the search field to narrow the files listed by specific criteria (for example, by file name or media category).
7. From the **Assignment Rule** list, select how you want to manage the media file on devices belonging to the selected policies:
  - **Auto-install**: The media file is downloaded when a device enters the policy. The file remains on the device when it leaves the policy, and the device's user can manually delete the file, if desired.
  - **On-demand**: The media file is made available within AbsoluteSafe and the device's user can manually download the file. The file remains on the device when it leaves the policy, and the device's user can manually delete the file, if desired.
  - **Auto-install, Auto-remove**: The media file is downloaded when the device enters the policy and deleted when it leaves.

- **On-demand, Auto-remove:** The media file is made available within AbsoluteSafe and the device's user can manually download the file. The file is deleted when the device leaves the policy.
8. If you want the selected policies to restrict the availability of the media file to certain dates or times, select the **Set availability time** checkbox, then choose one of the following options:
    - **Every day between:** The media file is available to mobile devices belonging to this policy only during a certain time of the day (for example, during office hours). Specify the start and end times in the available fields.
    - **From:** The media file is available to mobile devices belonging to this policy only during a specific time period. Specify the start date and time as well as the end date and time.


---


**NOTE** Use your local time in these fields. Times you enter are converted to and stored in Coordinated Universal Time (UTC) on the Absolute Manage server. As a result, you should take into account any time differences that may exist with your mobile clients. You also must manually compensate for Daylight Saving Time (DST), if desired, because DST does not apply to UTC.

---


9. Click **Add to Policies**.
10. Click **Done** to close the confirmation message.

➔ To remove a media file from policies:


1. Navigate to the **Assignable Items** area.
2. In the sidebar, click **Content**. (You can also click  in the top left corner of the screen and then click **Mobile Content**.)
3. In the results grid, click the media file you want to edit.
4. Click the **Policies** tab.

The results grid lists all policies that the file currently belongs to.
5. Select the checkbox of each policy you want to remove the media file from.
6. Click .
7. Click **Remove Content**.
8. Click **OK** to close the confirmation message.

➔ To edit the policy assignment rules for a media file:

1. Navigate to the **Assignable Items** area.
2. In the sidebar, click **Content**. (You can also click  in the top left corner of the screen and then click **Mobile Content**.)
3. In the results grid, click the media file you want to edit.
4. Click the **Policies** tab.

The results grid lists all policies that the file currently belongs to.
5. Select the checkbox of each policy whose assignment rule you want to change.

6. Click .
7. From the **Assignment Rule** list, select how you want to manage the media file on devices belonging to the selected policies:
  - **Auto-install:** The media file is downloaded when a device enters the policy. The file remains on the device when it leaves the policy, and the device's user can manually delete the file, if desired.
  - **On-demand:** The media file is made available within AbsoluteSafe and the device's user can manually download the file. The file remains on the device when it leaves the policy, and the device's user can manually delete the file, if desired.
  - **Auto-install, Auto-remove:** The media file is downloaded when the device enters the policy and deleted when it leaves.
  - **On-demand, Auto-remove:** The media file is made available within AbsoluteSafe and the device's user can manually download the file. The file is deleted when the device leaves the policy.
8. If you want the selected policies to restrict the availability of the media file to certain dates or times, select the **Set availability time** checkbox, then choose one of the following options:
  - **Every day between:** The media file is available to mobile devices belonging to the policy only during a certain time of the day (for example, during office hours). Specify the start and end times in the available fields.
  - **From:** The media file is available to mobile devices belonging to the policy only during a specific time period. Specify the start date and time as well as the end date and time.

---

**NOTE** Use your local time in these fields. Times you enter are converted to and stored in Coordinated Universal Time (UTC) on the Absolute Manage server. As a result, you should take into account any time differences that may exist with your mobile clients. You also must manually compensate for Daylight Saving Time (DST), if desired, because DST does not apply to UTC.



---

9. Click **Edit Content**.
10. Click **Done** to close the confirmation message.

## Deleting Media Files

You can delete media files that have been imported into Absolute Manage. When you delete a media file, it is removed from any policies it may belong to and is no longer available to mobile device users through AbsoluteSafe. However, deleting a media file from Absolute Manage Web Admin does not remove any copies of the file that the user may have made (if the file was allowed to leave AbsoluteSafe).

➔ To delete media files that have been imported into Absolute Manage:

1. Navigate to the **Assignable Items** area.
2. In the sidebar, click **Content**. (You can also click  in the top left corner of the screen and then click **Mobile Content**.)
3. In the results grid, select the checkbox of the media files you want to delete and click .  
You can also delete a single media file from its Content Details page:
  - a) In the results grid, click the media file you want to delete. The file's Content Details page opens.
  - b) Click **Delete**.
4. Click **Delete Content**.
5. Click **OK** to close the confirmation message.

## Viewing In-House Application Details


You can view the details of all in-house applications that have been imported into Absolute Manage. These applications are available for distribution to iOS and Android devices.

You can distribute in-house applications to mobile devices in the following two ways:

- On an as-needed basis through [direct installation](#)
- In an automated manner through [policies](#)

Before you can distribute an application for installation from Absolute Manage Web Admin, you must import the application file as a mobile application package using the Absolute Manage Admin interface. For more information, see "Installing software on mobile devices" in the *Absolute Manage User Guide*.

➔ To view the details of in-house applications available within Absolute Manage:

1. Navigate to the **Assignable Items** area.
2. In the sidebar, click **In-House Applications**. (You can also click  in the top left corner of the screen and then click **In-House Applications**.)

A list of available in-house applications shows in the results grid. You can quickly find specific applications by [using the search field](#) at the top of the page to narrow the list by specific criteria (for example, by application name or OS type). You can also [customize the column layout](#) of this page to show the information that is most relevant to you.

The following table provides a summary of application information available on this page:

Field	Applies To	Description
App Name	iOS and Android devices	The name of the application package
OS Type	iOS and Android devices	The operating system supported by the application contained in the package
Version	iOS and Android devices	The version number of the application contained in the package
Build Number	iOS and Android devices	The build number of the application contained in the package
Size	iOS and Android devices	The size the application code requires on the mobile device after installation
Short Description	iOS and Android devices	The short description of the application package
Bundle Identifier	iOS and Android devices	The unique identifier of the application package
Compatibility	iOS and Android devices	The operating system version that is compatible with the application contained in the package
Universal	iOS devices only	Indicates whether the application is optimized for both the iPhone/iPod touch and iPad hardware platforms
Supported Devices	iOS devices only	A comma-separated list of the hardware platforms (iPhone, iPad, iPod touch) that the application runs on

Field	Applies To	Description
iOS Provisioning Profile Name	iOS devices only	The name of the provisioning profile associated with the application
iOS Provisioning Profile Expiry Date	iOS devices only	The date that the provisioning profile associated with the application is valid until



## Viewing Third-Party Application Details


You can view the details of all third-party applications that have been imported into Absolute Manage. These applications are available for distribution to iOS and Android devices.

You can distribute third-party applications to mobile devices in the following two ways:

- On an as-needed basis through [direct installation](#)
- In an automated manner through [policies](#)

Before you can distribute an application for installation from Absolute Manage Web Admin, you must import the application file as a mobile application package using the Absolute Manage Admin interface. For more information, see "Installing software on mobile devices" in the *Absolute Manage User Guide*.

➔ To view the details of third-party applications available within Absolute Manage:

1. Navigate to the **Assignable Items** area.
2. In the sidebar, click **Third-Party Applications**. (You can also click  in the top left corner of the screen and then click **Third-Party Applications**.)

A list of available third-party applications shows in the results grid. You can quickly find specific applications by [using the search field](#) at the top of the page to narrow the list by specific criteria (for example, by application name or OS type). You can also [customize the column layout](#) of this page to show the information that is most relevant to you.

The following table provides a summary of application information available on this page:


Field	Applies To	Description
Icon	iOS and Android devices	The icon associated with the application package
App Name	iOS and Android devices	The name of the application package
OS	iOS and Android devices	The operating system that the application contained in the package was written for
Category	iOS and Android devices	The category of the application package, as specified by the administrator
Compatibility	iOS and Android devices	The operating system version that the application contained in the package is compatible with
Universal	iOS devices only	Indicates whether the application is optimized for both the iPhone/iPod touch and iPad hardware platforms
Supported Devices	iOS devices only	A comma-separated list of the hardware platforms (iPhone, iPad, iPod touch) that the application runs on
Short Description	iOS and Android devices	The short description of the application package
Prevent Data Backup	iOS devices only	Indicates whether the application's data on the device is prevented from being included in system backups

Field	Applies To	Description
Remove When MDM Is Removed	iOS devices only	Indicates whether this application is automatically deleted from mobile devices that are no longer enrolled on the Absolute Manage MDM server
VPP Purchased	iOS devices only	The total number of App Store VPP (Volume Purchase Program) managed licenses that have been purchased for this application
VPP Redeemed	iOS devices only	The number of App Store VPP (Volume Purchase Program) codes that have already been used to install a copy of this application on administered mobile devices
VPP Remaining	iOS devices only	The number of App Store VPP (Volume Purchase Program) managed licenses for this application that remain available for assignment

## Viewing Electronic Book Details

You can view the details of all electronic books originating from the iTunes Store that have been imported into Absolute Manage. If you want to distribute these books to iOS devices, you must use the Absolute Manage Admin interface. For more information, see "Distributing iTunes Book Store books to mobile users" in the *Absolute Manage User Guide*.

➔ To view the details of electronic books available within Absolute Manage:

1. Navigate to the **Assignable Items** area.
2. In the sidebar, click **Bookstore Books**. (You can also click  in the top left corner of the screen and then click **Bookstore Books**.)

A list of available electronic books originating from the iTunes Store shows in the results grid. You can quickly find specific books by [using the search field](#) at the top of the page to narrow the list by specific criteria (for example, by book title or description). You can also [customize the column layout](#) of this page to show the information that is most relevant to you.

The following table provides a summary of electronic book information available on this page:

Field	Applies To	Description
Icon	iOS devices only	The icon associated with the book
Title	iOS devices only	The title of the book
Short Description	iOS devices only	A brief description of the book's content
Category	iOS devices only	The genre of the book

## Viewing Configuration Profile Details


You can view the details of all configuration profiles that have been imported or created within Absolute Manage. These configuration profiles are available for install on mobile devices.

You can install the configuration profiles on mobile devices in the following two ways:

- On an as-needed basis through [direct installation](#)
- In an automated manner through [policies](#)

Before you can install a configuration profile from Absolute Manage Web Admin, you must import or create the profile using the Absolute Manage Admin interface. For more information, see "Working with configuration profiles" in the *Absolute Manage User Guide*.

➔ To view the details of configuration profiles available within Absolute Manage:

1. Navigate to the **Assignable Items** area.
2. In the sidebar, click **Configuration Profiles**. (You can also click  in the top left corner of the screen and then click **Configuration Profiles**.)

A list of available configuration profiles shows in the results grid. You can quickly find specific profiles by [using the search field](#) at the top of the page to narrow the list by specific criteria (for example, by profile name or description). You can also [customize the column layout](#) of this page to show the information that is most relevant to you.


The following table provides a summary of configuration profile information available on this page:

Field	Applies To	Description
Profile Name	All devices	The name of the configuration profile
Description	All devices	The optional description of the profile
Issuing Organization	All devices	The optional name of the organization that provided the profile
Profile Type	All devices	The type of profile; for example, device profile or app profile. Device profiles contain settings for the hardware or operating system, while app profiles contain settings for individual applications.
Profile Identifier	All devices	The identifying string of the profile
Profile UUID	All devices	The unique identifier of the profile
Allow Removal	All devices	Indicates whether the profile can be removed remotely
Variables Used	All devices	A comma-separated list of variables that are used in the configuration profile

## Viewing Provisioning Profile Details

You can view the details of all provisioning profiles that are available within Absolute Manage. To manually install these profiles on iOS devices, see [Installing Provisioning Profiles on Devices](#).

➔ To view the details of provisioning profiles available within Absolute Manage:

1. Navigate to the **Assignable Items** area.
2. In the sidebar, click **Provisioning Profiles**. (You can also click  in the top left corner of the screen and then click **Provisioning Profiles**.)

A list of available provisioning profiles shows in the results grid. You can quickly find specific profiles by [using the search field](#) at the top of the page to narrow the list by specific criteria (for example, by profile name or ID). You can also [customize the column layout](#) of this page to show the information that is most relevant to you.

The following table provides a summary of provisioning profile information available on this page:

Field	Applies To	Description
Profile Name	iOS devices only	The name of the provisioning profile
Profile Expiry Date	iOS devices only	The date that the provisioning profile is valid until
UUID	iOS devices only	The unique identifier of the provisioning profile

## Working with Actions

Use the Assignable Actions page to manage actions that you can assign to smart policies. Actions allow you to specify what Absolute Manage should do with a mobile device when it joins a smart policy. For example, you may have a smart policy that identifies mobile devices that have left the country. Using actions, you can decide to send an SMS with roaming instructions to the user when a mobile device is detected to be outside of the country, or you can set the roaming options on the device yourself.

From the Assignable Actions page, you can create the following actions:

- [Send Message To Device](#)
- [Send E-Mail](#)
- [Send SMS](#)
- [Set Roaming Options](#)
- [Set Activation Lock Options](#)
- [Set Wallpaper](#)
- [Set Device Name](#)
- [Set Custom Field Value](#)
- [Update Device Information](#)
- [Set Attention Mode](#)
- [Freeze Device](#)
- [Send VPP Invitation](#)
- [Register User In VPP](#)
- [Retire User From VPP](#)
- [Remove Configuration Profile](#)
- [Demote To Unmanaged Device](#)

With existing actions listed on this page, you can also perform the following tasks:


- [Viewing Action Details](#)
- [Editing Actions](#)
- [Duplicating Actions](#)
- [Deleting Actions](#)

You can also [search for individual items](#) using specific criteria in the Search field, as well as [customize the information](#) included in the results grid.

## Viewing Action Details

You can view the details of actions that have been created within Absolute Manage Web Admin, including the properties and policies that are associated with each action.

➔ To view the details of an action:



1. Navigate to the **Assignable Items > Actions** area. (You can also click  in the top left corner of the screen and then click **Actions**.)
2. In the results grid, click the action whose details you want to view.

The Action Details page opens. The following table provides a summary of the information available on this page:

Field	Description
<b>All actions</b>	
Name	The name under which the action is stored in Absolute Manage
Description	Descriptive text explaining the purpose of the action. This text is shown within Absolute Manage Web Admin and is intended for your own reference and that of other administrators.
Type	The type of action being performed
Target platforms	The mobile device platforms to which the action applies
Last modified	The date and time when the action was last modified
<b>Send Message To Device</b>	
Message text	The text that is sent to mobile devices that trigger the action. This message appears onscreen on the mobile device.
<b>Send E-Mail</b>	
To	The email address to which the e-mail should be sent
CC	The email addresses to which the e-mail should be copied, if any
Subject	The subject of the email
Message text	The body of the email
<b>Send SMS</b>	
Message text	The message to be sent, up to 140 characters in length
Phone number	The telephone numbers to which the SMS text message should be sent
<b>Set Roaming Options</b>	
Voice roaming	The voice roaming option to set on mobile devices entering a smart policy
Data roaming	The data roaming option to set on mobile devices entering a smart policy
<b>Set Activation Lock Options</b>	
Activation lock	Indicates whether the activation lock can be enabled on iOS devices through the “Find My iPhone” or “Find My iPad” setting
<b>Set Wallpaper</b>	

Field	Description
Wallpaper options	Indicates which screens on the mobile device the wallpaper should apply to
Image	A preview of the uploaded wallpaper image
Image dimensions	The dimensions of the uploaded wallpaper image
<b>Set Device Name</b>	
Device name	The new device name the action applies to mobile devices
<b>Set Custom Field Value</b>	
Custom field	The custom field for which the value is being set
Value	The value applied to the custom field on mobile devices on which the action is performed
<b>Set Attention Mode</b>	
Attention mode	Indicates whether the action enables or disables attention mode
Text	The message shown on the screen of mobile devices while attention mode is enabled
<b>Register User In VPP and Send VPP Invitation</b>	
Subject	The subject text for the invitation email
Message text	The text of the invitation message sent using email or AbsoluteApps
SMS text	The text of the invitation message sent through SMS
Send invitation	The channels over which the action sends the VPP registration notice to users
VPP account	The VPP account under which the action registers mobile device users
<b>Retire User From VPP</b>	
VPP account	The VPP account from which the action removes mobile device users
<b>Remove Configuration Profile</b>	
Profile	The configuration profile that the action removes from mobile devices

You can also perform the following tasks from this page:

- [Duplicate the action](#)
  - [Edit the action](#)
  - [Delete the action](#)
3. Click the **Policies** tab to view the smart policies that the action is assigned to. You can also perform the following tasks from this tab:
- [Add the action to smart policies](#) from this tab by clicking the **Add Action To Policies** button.
  - [Remove the action from smart policies](#) by selecting the checkbox of the applicable smart policies and clicking .
  - [Edit the policy assignment rules](#) for the action by selecting the checkbox of the applicable smart policy and clicking .



You can quickly find specific results on any of these pages by [using the search field](#) at the top of the page to narrow the items listed by specific criteria (for example, by policy name). You can also [customize the column layout](#) of these pages to show the information that is most relevant to you.

## Action: Send Message To Device

You can create an action that sends a message to mobile devices when they join smart policies you assign the action to. This action is available for iOS and Android devices only.


After you create actions, you can view and manage them (along with all other actions that exist in your deployment) within the **Assignable Items > Actions** area.

---

**NOTE** If you are editing or duplicating a Send Message To Device action, refer to the table in the following task for a description of the fields available for the action.

---

➔ To create a Send Message To Device action:

1. Navigate to the **Assignable Items > Actions** area. (You can also click  in the top left corner of the screen and then click **Actions**.)
2. In the work area toolbar, click **Add Action > Send Message To Device**.
3. Enter the following information. Required fields are marked with an asterisk (\*).

Field	Description
Action name*	A name for the action
Description	A description explaining the purpose of the action This text is shown within Absolute Manage Web Admin and is intended for your own reference and that of other administrators.
Target platforms	The target platforms of the mobile devices to which this action should apply
Message text*	The text you want to send to mobile devices that trigger the action This message is shown onscreen on the mobile device. You can also use <a href="#">device and user-related variables</a> in your message. The maximum length of the message is 140 characters.

4. Do one of the following:
  - Click **Save** to save the action without immediately assigning it to a smart policy.
  - Click **Save and Assign to Policies** to save and [assign the action to one or more smart policies](#).


## Action: Send Email

You can create an action that sends an email to addresses you specify (for example, those of administrators) when mobile devices join smart policies you assign the action to.

After you create actions, you can view and manage them (along with all other actions that exist in your deployment) within the **Assignable Items > Actions** area.

**NOTE** If you are editing or duplicating a Send Email action, refer to the table in the following task for a description of the fields available for the action.

➔ To create a Send Email action:

1. Navigate to the **Assignable Items > Actions** area. (You can also click  in the top left corner of the screen and then click **Actions**.)
2. In the work area toolbar, click **Add Action > Send Email**.
3. Enter the following information. Required fields are marked with an asterisk (\*).

Field	Description
Action name*	A name for the action
Description	A description explaining the purpose of the action This text is shown within Absolute Manage Web Admin and is intended for your own reference and that of other administrators.
Target platforms	The target platforms of the mobile devices to which this action should apply
Subject*	The subject of the email that the action will prompt
To*	The email addresses of the recipients in the To field Separate multiple addresses in this field with a comma (",").
CC	The email addresses of other people you want to copy on the email Separate multiple addresses in this field with a comma (",").
Message	The body of the email You can also use <a href="#">device and user-related variables</a> in the body.

4. Do one of the following:
  - Click **Save** to save the action without immediately assigning it to a smart policy.
  - Click **Save and Assign to Policies** to save and [assign the action to one or more smart policies](#).


## Action: Send SMS

You can create an action that sends an SMS text message to phone numbers you specify (for example, those of administrators) when mobile devices join smart policies you assign the action to.

After you create actions, you can view and manage them (along with all other actions that exist in your deployment) within the **Assignable Items > Actions** area.

**NOTE** If you are editing or duplicating a Send SMS action, refer to the table in the following task for a description of the fields available for the action.

➔ To create a Send SMS action:

1. Navigate to the **Assignable Items > Actions** area. (You can also click  in the top left corner of the screen and then click **Actions**.)
2. In the work area toolbar, click **Add Action > Send SMS**.
3. Enter the following information. Required fields are marked with an asterisk (\*).

Field	Description
Action name*	A name for the action
Description	A description explaining the purpose of the action This text is shown within Absolute Manage Web Admin and is intended for your own reference and that of other administrators.
Target platforms	The target platforms of the mobile devices to which this action should apply
Phone number*	The phone numbers you want to send the SMS text message to Separate multiple phone numbers in this field with a comma (",").
Message*	The text message you want to send You can also use <a href="#">device and user-related variables</a> in your message. The maximum length of the message is 140 characters.

4. Do one of the following:
  - Click **Save** to save the action without immediately assigning it to a smart policy.
  - Click **Save and Assign to Policies** to save and [assign the action to one or more smart policies](#).

## Action: Set Roaming Options


You can create an action that sets data and voice roaming permissions on mobile devices when they join smart policies you assign the action to. This action is available for iOS devices only.

**NOTE** Users of mobile devices can change the roaming settings on their own device at any time.

After you create actions, you can view and manage them (along with all other actions that exist in your deployment) within the **Assignable Items > Actions** area.

**NOTE** If you are editing or duplicating a Set Roaming Options action, refer to the table in the following task for a description of the fields available for the action.

➔ To create a Set Roaming Options action:

1. Navigate to the **Assignable Items > Actions** area. (You can also click  in the top left corner of the screen and then click **Actions**.)
2. In the work area toolbar, click **Add Action > Set Roaming Options**.
3. Enter the following information. Required fields are marked with an asterisk (\*).

Field	Description
Action name*	A name for the action
Description	A description explaining the purpose of the action This text is shown within Absolute Manage Web Admin and is intended for your own reference and that of other administrators.
Target platforms	The target platforms of the mobile devices to which this action should apply This action is available for iOS devices only.
Voice roaming Data roaming	The voice and data roaming options you want to associate with the action: <ul style="list-style-type: none"> <li>• <b>Leave as is</b> – Leave the current settings on the mobile device unchanged</li> <li>• <b>Off</b> – Disable voice or data roaming on the mobile device</li> <li>• <b>On</b> – Enable voice or data roaming on the mobile device</li> </ul>

4. Do one of the following:
  - Click **Save** to save the action without immediately assigning it to a smart policy.
  - Click **Save and Assign to Policies** to save and [assign the action to one or more smart policies](#).

## Action: Set Activation Lock Options

Devices running iOS 7 and higher include the Activation Lock feature, which is part of Apple's Find My iPhone service. The Activation Lock feature requires the input of the device user's Apple ID and password before a device can be reactivated or erased.


You can create an action that configures the availability of the Activation Lock feature on mobile devices when they join smart policies you assign the action to. This action is available for supervised devices running iOS 7 or higher only.

**NOTE** You cannot disable the Activation Lock feature using this action if the feature is currently enabled on a device. For information on disabling the Activation Lock feature when it is currently enabled on a device, see "Disabling the activation lock when it is already active" in the *Absolute Manage User Guide*.

After you create actions, you can view and manage them (along with all other actions that exist in your deployment) within the **Assignable Items > Actions** area.

**NOTE** If you are editing or duplicating a Set Activation Lock Options action, refer to the table in the following task for a description of the fields available for the action.

➔ To create a Set Activation Lock Options action:

1. Navigate to the **Assignable Items > Actions** area. (You can also click  in the top left corner of the screen and then click **Actions**.)
2. In the work area toolbar, click **Add Action > Set Activation Lock Options**.
3. Enter the following information. Required fields are marked with an asterisk (\*).

Field	Description
Action name*	A name for the action
Description	A description explaining the purpose of the action This text is shown within Absolute Manage Web Admin and is intended for your own reference and that of other administrators.
Target platforms	The target platforms of the mobile devices to which this action should apply This action is available for iOS devices only.
Activation lock	The availability of the Activation Lock feature: <ul style="list-style-type: none"> <li>• <b>Disallow</b> – The Activation Lock feature can no longer be enabled on the mobile device. It will remain off regardless of whether Find My iPhone is turned on. However, if the Activation Lock feature is currently enabled on a mobile device, it will remain enabled.</li> <li>• <b>Allow</b> – Whenever Find My iPhone is enabled on the mobile device, the Activation Lock feature will also be enabled. Whenever Find My iPhone is disabled, the Activation Lock feature will also be disabled.</li> </ul>

4. Do one of the following:
  - Click **Save** to save the action without immediately assigning it to a smart policy.

- Click **Save and Assign to Policies** to save and [assign the action to one or more smart policies](#).

## Action: Set Wallpaper


You can create an action that changes the wallpaper displayed on mobile devices when they join smart policies you assign the action to. This action is available for supervised devices running iOS 7.1 and higher only.

**NOTE** Users of mobile devices can change the wallpaper settings on their own device at any time.

After you create actions, you can view and manage them (along with all other actions that exist in your deployment) within the **Assignable Items > Actions** area.

**NOTE** If you are editing or duplicating a Set Wallpaper action, refer to the table in the following task for a description of the fields available for the action.

➔ To create a Set Wallpaper action:

1. Navigate to the **Assignable Items > Actions** area. (You can also click  in the top left corner of the screen and then click **Actions**.)
2. In the work area toolbar, click **Add Action > Set Wallpaper**.
3. Enter the following information. Required fields are marked with an asterisk (\*).

Field	Description
Action name*	A name for the action
Description	A description explaining the purpose of the action This text is shown within Absolute Manage Web Admin and is intended for your own reference and that of other administrators.
Target platforms	The target platforms of the mobile devices to which this action should apply This action is available for supervised devices running iOS 7.1 and higher only.
Wallpaper options	Where on the mobile device you want to apply the wallpaper: <ul style="list-style-type: none"> <li>• <b>Lock screen</b> – If this option is selected, the mobile device uses the chosen image as the screen background when the device is locked.</li> <li>• <b>Home screen</b> – If this option is selected, the mobile device uses the chosen image as the screen background when the device is unlocked.</li> </ul>

4. Browse for and select the image you want to use as wallpaper.  
The image you select must be in PNG or JPEG format. For resolution guidelines specific to each iOS device model, refer to the tool tip next to the **Select image** button. After you select an image, the preview areas gives you an idea of what the image will look like as wallpaper on a vertical iPhone screen.
5. Do one of the following:
  - Click **Save** to save the action without immediately assigning it to a smart policy.
  - Click **Save and Assign to Policies** to save and [assign the action to one or more smart policies](#).



## Action: Set Device Name

You can create an action that renames mobile devices when they join smart policies you assign the action to. This action is available for Android devices and supervised devices running iOS 8 and higher only.


After you create actions, you can view and manage them (along with all other actions that exist in your deployment) within the **Assignable Items > Actions** area.

---

**NOTE** If you are editing or duplicating a Set Device Name action, refer to the table in the following task for a description of the fields available for the action.

---

➔ To create a Set Device Name action:

1. Navigate to the **Assignable Items > Actions** area. (You can also click  in the top left corner of the screen and then click **Actions**.)
2. In the work area toolbar, click **Add Action > Set Device Name**.
3. Enter the following information. Required fields are marked with an asterisk (\*).

Field	Description
Action name*	A name for the action
Description	A description explaining the purpose of the action This text is shown within Absolute Manage Web Admin and is intended for your own reference and that of other administrators.
Target platforms	The target platforms of the mobile devices to which this action should apply
Device name*	The new device name You can also use <a href="#">device and user-related variables</a> in the name.

4. Do one of the following:
  - Click **Save** to save the action without immediately assigning it to a smart policy.
  - Click **Save and Assign to Policies** to save and [assign the action to one or more smart policies](#).


## Action: Set Custom Field Value

You can create an action that sets the value of a custom field on mobile devices when they join smart policies you assign the action to.

After you create actions, you can view and manage them (along with all other actions that exist in your deployment) within the **Assignable Items > Actions** area.

**NOTE** If you are editing or duplicating a Set Custom Field Value action, refer to the table in the following task for a description of the fields available for the action.

➔ To create a Set Custom Field Value action:

1. Navigate to the **Assignable Items > Actions** area. (You can also click  in the top left corner of the screen and then click **Actions**.)
2. In the work area toolbar, click **Add Action > Set Custom Field Value**.
3. Enter the following information. Required fields are marked with an asterisk (\*).

Field	Description
Action name*	A name for the action
Description	A description explaining the purpose of the action This text is shown within Absolute Manage Web Admin and is intended for your own reference and that of other administrators.
Target platforms	The target platforms of the mobile devices to which this action should apply
Custom field	The custom field whose value you want to set This list contains all custom fields that have been defined in your deployment.
Data type	The data type of the selected custom field
Value*	The value you want to set on mobile devices You can also use <a href="#">device and user-related variables</a> in the value.  <b>NOTE</b> You can clear the information currently set on mobile devices for the custom field by selecting the <b>Remove</b> option instead.

4. Do one of the following:
  - Click **Save** to save the action without immediately assigning it to a smart policy.
  - Click **Save and Assign to Policies** to save and [assign the action to one or more smart policies](#).


## Action: Update Device Information

You can create an action that updates the information stored on the server for mobile devices when they join smart policies you assign the action to.

After you create actions, you can view and manage them (along with all other actions that exist in your deployment) within the **Assignable Items > Actions** area.

**NOTE** If you are editing or duplicating an Update Device Information action, refer to the table in the following task for a description of the fields available for the action.

➔ To create an Update Device Information action:

1. Navigate to the **Assignable Items > Actions** area. (You can also click  in the top left corner of the screen and then click **Actions**.)
2. In the work area toolbar, click **Add Action > Update Device Information**.
3. Enter the following information. Required fields are marked with an asterisk (\*).

Field	Description
Action name*	A name for the action
Description	A description explaining the purpose of the action This text is shown within Absolute Manage Web Admin and is intended for your own reference and that of other administrators.
Target platforms	The target platforms of the mobile devices to which this action should apply

4. Do one of the following:
  - Click **Save** to save the action without immediately assigning it to a smart policy.
  - Click **Save and Assign to Policies** to save and [assign the action to one or more smart policies](#).

## Action: Set Attention Mode

You can create an action that enables or disables attention mode on mobile devices when they join smart policies you assign the action to. When a mobile device is in attention mode, a message is shown on the device's screen and user interaction is not possible until the mode is disabled.


This action is available for the following iOS and Android devices:

- Supervised iOS devices on which AbsoluteApps 1.4.4 or higher is installed
- Samsung for Enterprise (SAFE) devices on which AbsoluteApps 2.0.5 or higher is installed

After you create actions, you can view and manage them (along with all other actions that exist in your deployment) within the **Assignable Items > Actions** area.

**NOTE** If you are editing or duplicating a Set Attention Mode action, refer to the table in the following task for a description of the fields available for the action.

➔ To create a Set Attention Mode action:

1. Navigate to the **Assignable Items > Actions** area. (You can also click  in the top left corner of the screen and then click **Actions**.)
2. In the work area toolbar, click **Add Action > Set Attention Mode**.
3. Enter the following information. Required fields are marked with an asterisk (\*).

Field	Description
Action name*	A name for the action
Description	A description explaining the purpose of the action This text is shown within Absolute Manage Web Admin and is intended for your own reference and that of other administrators.
Target platforms	The target platforms of the mobile devices to which this action should apply
Attention mode	Whether this action should enable or disable attention mode
Attention message*	If you selected <b>Enable</b> , the message that should be shown on the screen of the device while attention mode is enabled

4. Do one of the following:
  - Click **Save** to save the action without immediately assigning it to a smart policy.
  - Click **Save and Assign to Policies** to save and [assign the action to one or more smart policies](#).

## Action: Freeze Device


You can create an action that changes the passcode on mobile device and locks them when they join smart policies you assign the action to. This action makes the device inaccessible to the local user and is available for Android devices only.

**NOTE** It may be possible to circumvent this lock by resetting the mobile device to its factory state; however, performing a reset usually deletes all data on the device as well.

After you create actions, you can view and manage them (along with all other actions that exist in your deployment) within the **Assignable Items > Actions** area.

**NOTE** If you are editing or duplicating a Freeze Device action, refer to the table in the following task for a description of the fields available for the action.

➔ To create a Freeze Device action:

1. Navigate to the **Assignable Items > Actions** area. (You can also click  in the top left corner of the screen and then click **Actions**.)
2. In the work area toolbar, click **Add Action > Freeze Device**.
3. Enter the following information. Required fields are marked with an asterisk (\*).

Field	Description
Action name*	A name for the action
Description	A description explaining the purpose of the action This text is shown within Absolute Manage Web Admin and is intended for your own reference and that of other administrators.
Target platforms	The target platforms of the mobile devices to which this action should apply This action is available for Android devices only.
New passcode*	The new passcode This passcode replaces any existing passcode that may already exist on a mobile device.
Verification*	Confirmation of the new passcode

4. Do one of the following:
  - Click **Save** to save the action without immediately assigning it to a smart policy.
  - Click **Save and Assign to Policies** to save and [assign the action to one or more smart policies](#).

## Action: Send VPP Invitation

You can create an action that sends an invitation to users to register in Apple's Volume Purchase Program (VPP) using their personal Apple ID. The invitation is sent to users when their mobile devices join smart policies you assign the action to. This action is available for iOS devices only.

Before sending this invitation to users, ensure they are already registered with your VPP account (for example, by using the [Register User in VPP](#) action).


After you create actions, you can view and manage them (along with all other actions that exist in your deployment) within the **Assignable Items > Actions** area.

---

**NOTE** If you are editing or duplicating a Send VPP Invitation action, refer to the table in the following task for a description of the fields available for the action.

---

➔ To create a Send VPP Invitation action:

1. Navigate to the **Assignable Items > Actions** area. (You can also click  in the top left corner of the screen and then click **Actions**.)
2. In the work area toolbar, click **Add Action > Send VPP Invitation**.
3. Enter the following information. Required fields are marked with an asterisk (\*).

Field	Description
Action name*	A name for the action
Description	A description explaining the purpose of the action This text is shown within Absolute Manage Web Admin and is intended for your own reference and that of other administrators.
Target platforms	The target platforms of the mobile devices to which this action should apply This action is available for iOS devices only.
VPP account	The VPP account in which you want users to register This lists contains all VPP accounts that have been defined in the settings of your Absolute Manage Server.

Field	Description
Send invitation	<p>The VPP invitation options. You can choose one or more of the following notification methods:</p> <ul style="list-style-type: none"> <li>• <b>MDM dialog</b> – Sends an invitation through an MDM dialog displayed on the mobile device. You can use this method with mobile devices running iOS 7.0.3 and higher only.</li> <li>• <b>Web Clip</b> – Sends an invitation using a Web Clip that is placed on the device's home screen</li> <li>• <b>SMS</b> – Sends an invitation through an SMS message. Enter the message in the field provided, up to a maximum of 140 characters. You can also use <a href="#">device and user-related variables</a> in your message.</li> <li>• <b>Email</b> – Sends an invitation through email. Enter the subject and body of the email in the fields provided. You can also use <a href="#">device and user-related variables</a> in the email body.</li> <li>• <b>AbsoluteApps message</b> – Sends an invitation through an AbsoluteApps message. Enter the body of the message in the field provided. You can also use <a href="#">device and user-related variables</a> in your message. You can use this method only with mobile devices on which AbsoluteApps is installed.</li> </ul> <p><b>NOTE</b> In addition to device and user-related variables, you can also use the "MD_VPPInviteURL" variable within the invitation text, which displays a link to the Apple web page where users can enter their Apple ID to register in the VPP.</p>

4. Do one of the following:

- Click **Save** to save the action without immediately assigning it to a smart policy.
- Click **Save and Assign to Policies** to save and [assign the action to one or more smart policies](#).

## Action: Register User In VPP

You can create an action that adds mobile devices to your Volume Purchase Program (VPP) account when they join smart policies you assign the action to. You can also optionally send an invitation to users to register in the program using their personal Apple ID. This action is available for iOS devices only.


After you create actions, you can view and manage them (along with all other actions that exist in your deployment) within the **Assignable Items > Actions** area.

---

**NOTE** If you are editing or duplicating a Register User In VPP action, refer to the table in the following task for a description of the fields available for the action.

---

➔ To create a Register User In VPP action:

1. Navigate to the **Assignable Items > Actions** area. (You can also click  in the top left corner of the screen and then click **Actions**.)
2. In the work area toolbar, click **Add Action > Register User In VPP**.
3. Enter the following information. Required fields are marked with an asterisk (\*).

Field	Description
Action name*	A name for the action
Description	A description explaining the purpose of the action This text is shown within Absolute Manage Web Admin and is intended for your own reference and that of other administrators.
Target platforms	The target platforms of the mobile devices to which this action should apply This action is available for iOS devices only.
VPP account	The VPP account under which you want to register device users This lists contains all VPP accounts that have been defined in the settings of your Absolute Manage Server.



Field	Description
Register options	<p>The VPP registration options:</p> <ul style="list-style-type: none"> <li>• <b>Register users only</b> – If this option is selected, users affected by this action are registered in the selected VPP account, but are not yet invited to link their Apple ID to the account. This invitation must happen at a later time (for example, using the <a href="#">Send VPP Invitation</a> action) before users can download and use apps through VPP. This two-step process is faster on Apple's servers than registering and inviting users at the same time and is therefore recommended if you are registering a large numbers of users.</li> <li>• <b>Register and invite users</b> – If this option is selected, users affected by this action are registered in the selected VPP account and are also invited to link their Apple ID to the account. Select the channels you want to use to send the VPP registration invitation to users. Users must complete the registration themselves by entering their personal Apple ID and password on Apple's VPP website. You can choose one or more of the following notification methods: <ul style="list-style-type: none"> <li>– <b>MDM dialog</b> – Sends an invitation through an MDM dialog displayed on the mobile device. You can use this method with mobile devices running iOS 7.0.3 and higher only.</li> <li>– <b>Web Clip</b> – Sends an invitation using a Web Clip that is placed on the device's home screen</li> <li>– <b>SMS</b> – Sends an invitation through an SMS message. Enter the message in the field provided, up to a maximum of 140 characters. You can also use <a href="#">device and user-related variables</a> in your message.</li> <li>– <b>Email</b> – Sends an invitation through email. Enter the subject and body of the email in the fields provided. You can also use <a href="#">device and user-related variables</a> in the email body.</li> <li>– <b>AbsoluteApps message</b> – Sends an invitation through an AbsoluteApps message. Enter the body of the message in the field provided. You can also use <a href="#">device and user-related variables</a> in your message. You can use this method only with mobile devices on which AbsoluteApps is installed.</li> </ul> </li> </ul> <p><b>NOTE</b> In addition to device and user-related variables, you can also use the "MD_VPPInviteURL" variable within the invitation text, which displays a link to the Apple web page where users can enter their Apple ID to register in the VPP.</p>

4. Do one of the following:

- Click **Save** to save the action without immediately assigning it to a smart policy.
- Click **Save and Assign to Policies** to save and [assign the action to one or more smart policies](#).

## Action: Retire User From VPP

You can create an action that removes mobile devices from Apple's Volume Purchase Program (VPP) when they join smart policies you assign the action to. This action is available for iOS devices only.


After you create actions, you can view and manage them (along with all other actions that exist in your deployment) within the **Assignable Items > Actions** area.

---

**NOTE** If you are editing or duplicating a Retire User From VPP action, refer to the table in the following task for a description of the fields available for the action.

---

➔ To create a Retire User From VPP action:

1. Navigate to the **Assignable Items > Actions** area. (You can also click  in the top left corner of the screen and then click **Actions**.)
2. In the work area toolbar, click **Add Action > Retire User From VPP**.
3. Enter the following information. Required fields are marked with an asterisk (\*).

Field	Description
Action name*	A name for the action
Description	A description explaining the purpose of the action This text is shown within Absolute Manage Web Admin and is intended for your own reference and that of other administrators.
Target platforms	The target platforms of the mobile devices to which this action should apply This action is available for iOS devices only.
VPP account	The VPP account that you want to remove mobile devices from This lists contains all VPP accounts that have been defined in the settings of your Absolute Manage Server.

4. Do one of the following:
  - Click **Save** to save the action without immediately assigning it to a smart policy.
  - Click **Save and Assign to Policies** to save and [assign the action to one or more smart policies](#).

## Action: Remove Configuration Profile

You can create an action that removes a configuration profile from mobile devices when they join smart policies you assign the action to.


After you create actions, you can view and manage them (along with all other actions that exist in your deployment) within the **Assignable Items > Actions** area.

---

**NOTE** If you are editing or duplicating a Remove Configuration Profile action, refer to the table in the following task for a description of the fields available for the action.

---

➔ To create a Remove Configuration Profile action:

1. Navigate to the **Assignable Items > Actions** area. (You can also click  in the top left corner of the screen and then click **Actions**.)
2. In the work area toolbar, click **Add Action > Remove Configuration Profile**.
3. Enter the following information. Required fields are marked with an asterisk (\*).

Field	Description
Action name*	A name for the action
Description	A description explaining the purpose of the action This text is shown within Absolute Manage Web Admin and is intended for your own reference and that of other administrators.
Profile	The configuration profile that you want to remove from mobile devices Configuration profiles in the list are organized by mobile device platform.

4. Do one of the following:
  - Click **Save** to save the action without immediately assigning it to a smart policy.
  - Click **Save and Assign to Policies** to save and [assign the action to one or more smart policies](#).

## Action: Demote To Unmanaged Device


You can create an action that removes MDM control (and the Absolute Manage client software, where applicable) from mobile devices when they join smart policies you assign the action to. After this action is applied to mobile devices, you can no longer manage them through Absolute Manage. This action is available for iOS and Android devices only.

**IMPORTANT** This action cannot be reversed within Absolute Manage. A mobile device that has been removed from management must be re-enrolled if you want to manage it again through Absolute Manage.

After you create actions, you can view and manage them (along with all other actions that exist in your deployment) within the **Assignable Items > Actions** area.

**NOTE** If you are editing or duplicating a Demote To Unmanaged Device action, refer to the table in the following task for a description of the fields available for the action.

➔ To create a Demote To Unmanaged Device action:

1. Navigate to the **Assignable Items > Actions** area. (You can also click  in the top left corner of the screen and then click **Actions**.)
2. In the work area toolbar, click **Add Action > Demote To Unmanaged Device**.
3. Enter the following information. Required fields are marked with an asterisk (\*).



Field	Description
Action name*	A name for the action
Description	A description explaining the purpose of the action This text is shown within Absolute Manage Web Admin and is intended for your own reference and that of other administrators.
Target platforms	The target platforms of the mobile devices to which this action should apply

4. Do one of the following:
  - Click **Save** to save the action without immediately assigning it to a smart policy.
  - Click **Save and Assign to Policies** to save and [assign the action to one or more smart policies](#).

## Editing Actions

When you edit an existing action, your changes are automatically applied to smart policies that the action is currently assigned to.



➔ To edit an action:

1. Navigate to the **Assignable Items > Actions** area. (You can also click  in the top left corner of the screen and then click **Actions**.)
2. In the results grid, select the checkbox of the action you want to edit.
3. Click .
4. Edit the action's properties as required. For more information on the properties of a specific action type, see [Working with Actions](#).
5. Do one of the following:
  - Click **Save** to save the action without immediately assigning it to a smart policy.
  - Click **Save and Assign to Policies** to save and [assign the action to one or more smart policies](#).

## Duplicating Actions

You can make a copy of an existing action and edit it to create another action.



➔ To duplicate an action:

1. Navigate to the **Assignable Items > Actions** area. (You can also click  in the top left corner of the screen and then click **Actions**.)
2. In the results grid, select the checkbox of the action you want to duplicate.
3. Click .
4. Edit the action's properties as required. For more information on the properties of a specific action type, see [Working with Actions](#).
5. Do one of the following:
  - Click **Save** to save the action without immediately assigning it to a smart policy.
  - Click **Save and Assign to Policies** to save and [assign the action to one or more smart policies](#).

## Deleting Actions

When you delete an action, it is also automatically removed from smart policies to which it is assigned.

➔ To delete actions:

1. Navigate to the **Assignable Items > Actions** area. (You can also click  in the top left corner of the screen and then click **Actions**.)
2. In the results grid, select the checkbox of the actions you want to delete.
3. Click .
4. Click **Delete Action**.
5. Click **OK** to close the confirmation message.

## Working with Custom Fields

Use the Mobile Custom Fields page to manage customized information fields for mobile devices. These custom fields allow you extend the amount of information stored about mobile devices in your deployment and help accommodate any special data requirements your organization may have. The data contained in custom fields is stored on the Absolute Manage Server along with standard inventory information.

From the Mobile Custom Fields area, you can perform the following tasks:

- [Creating Custom Fields](#)
- [Editing Custom Fields](#)
- [Duplicating Custom Fields](#)
- [Deleting Custom Fields](#)

You can also [search for individual items](#) using specific criteria in the Search field.




## Creating Custom Fields

You can create a custom field to store any type of information you choose about mobile devices in your deployment. Custom fields allow you to extend the predefined list of information items provided by Absolute Manage and build a customized inventory that meets the unique requirements of your organization.

After you create a custom field, you can set its value on mobile devices in the following ways:

- For an individual mobile device, you can [set custom field values](#) with the Device Details page.
- For multiple mobile devices, you can [create a Set Custom Field Value action](#) and [assign it to a smart policy](#).



➔ To create a custom field:

1. Click  in the top left corner of the screen and then click **Mobile Custom Fields**.
  2. Click **Add Custom Field**.
  3. Enter a name for the custom field.
  4. Enter a description for the custom field.
  5. If you want to use the custom field as a variable so that you can [embed the field's content within certain messages and names](#), enter a variable name.
  6. Select the type of data you want the field to store:
    - **String** – Any unformatted text
    - **Number** – Any number. You can choose from several display formats.
    - **Boolean** – A true or false value
    - **Date** – A specific date and time
    - **File Version** – A version number according to the conventions of the target mobile device platform. A valid file version number for iOS consists of up to three integers, separated by periods and optionally followed by one of the letters "a", "b", "d", or "f " and another integer (for example, 1.0, 2.4.1, 6.8d1). A valid file version number for Android and Windows Phone consists of up to four integers, separated by periods (for example, 5.7, 3.0.0.233).
    - **IP Address** – An IPv4 address (for example, 192.168.0.1)
    - **Enumeration** – A value from a predefined list. Specify the list of possible values, entering one item per line.
- NOTE** All enumeration values are treated as strings.
7. Click **Add Field**.
  8. Click **OK** to close the confirmation message.

## Editing Custom Fields

You can edit any of the properties of an existing custom field, except for the field's data type.



➔ To edit a custom field:

1. Click  in the top left corner of the screen and then click **Mobile Custom Fields**.
2. In the results grid, select the checkbox of the custom field you want to edit.
3. Click .
4. Edit the field's properties as required. You cannot edit the data type of an existing custom field.
5. Click **Save**.
6. Click **OK** to close the confirmation message.

## Duplicating Custom Fields

You can make a copy of an existing custom field and edit it to create another field.



➔ To duplicate a custom field:

1. Click  in the top left corner of the screen and then click **Mobile Custom Fields**.
2. In the results grid, select the checkbox of the custom field you want to duplicate.
3. Click .
4. Edit the field's properties as required. For more information on the properties of a custom field, see [Creating Custom Fields](#).
5. Click **Save**.
6. Click **OK** to close the confirmation message.

## Deleting Custom Fields

When you delete a custom field, you also delete all data associated with that field.

➔ To delete custom fields:

1. Click  in the top left corner of the screen and then click **Mobile Custom Fields**.
2. In the results grid, select the checkbox of the custom fields you want to delete.
3. Click .
4. Click **Delete**.
5. Click **OK** to close the confirmation message.

# Glossary

## A

---

### **Absolute Manage**

Allows organizations to persistently manage and secure all of their endpoints from a single console, including PC, Mac, iOS, Android, and Windows Phone devices. Absolute Manage can be deployed as a complete asset management solution as well as a stand-alone solution for Mobile Device Management (MDM).

### **Absolute Manage Admin**

The software application that administrators can install on their workstations to manage client devices (both computers and mobile devices) through the Absolute Manage system. In contrast, Absolute Manage Web Admin is a web-based application that administrators access through their browser to manage mobile devices only.

### **AbsoluteApps**

The client application installed on mobile devices that acts as a link to Absolute Manage. AbsoluteApps reports on the status of a mobile device and enables administrators to perform remote actions on the device.

### **AbsoluteSafe**

An Absolute Manage client application for iOS and Android devices that allows administrators to securely distribute media to mobile device users.

### **action**

Allows you to specify what Absolute Manage should do when a mobile device enters a smart policy.

### **Active Directory**

A directory service developed by Microsoft for Windows domain networks and included in most Windows Server operating systems as a set of processes and services.

### **ActiveSync**

A protocol that allows mobile devices to synchronize data and policies with a Microsoft Exchange server.

### **agent**

An endpoint software module that allows you to maintain a connection with all of the devices in your deployment. The agent makes regularly scheduled calls to the Absolute Manage Server to report on device status and to allow for remote device management.

### **ATA**

Advanced Technology Attachment. An older interface standard for the connection of storage devices (such as hard disk drives and optical disc drives) in computers.

---

**B**

---

**BIOS**

Basic Input/Output System. Built-in firmware used to start up a computer after it is powered on. BIOS also manages data flow between the computer's operating system and any attached devices.

**Bluetooth**

A technology standard for exchanging data between electronic devices wirelessly over short distances.

---

**C**

---

**cache**

A type of memory that a mobile device can access more quickly than random access memory (RAM). It is used to store instructions that are repeatedly required to run applications, improving overall device speed.

**CDMA**

Code Division Multiple Access. A digital cellular technology that uses spread-spectrum techniques, most common in North America and parts of Asia.

**configuration profile**

An easy way of distributing common settings (for example, Wi-Fi, VPN, email, or application-specific settings) to mobile devices and OS X computers.

**CPU**

Central Processing Unit. The component within a mobile device that interprets and carries out hardware and software instructions.

---

**D**

---

**DHCP**

Dynamic Host Configuration Protocol. A standardized network protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services.

**DNS**

Domain Name System. A hierarchical distributed naming system for computers, services, or any resource connected to the internet or a private network that translates domain and host names into IP addresses.

**DST**

Daylight Saving Time. The practice of advancing clocks during the summer months so that people rise earlier in the morning and experience more daylight in the evening. Typically, clocks

are adjusted forward one hour near the start of spring and are adjusted backward in the autumn. Exact start and end dates for DST vary with location.

---

## E

### EDGE

Enhanced Data GSM Environment. A subsequent version of the GSM standard, designed to enable faster data rates and the delivery of multimedia to mobile devices.

---

## F

### FireWire

A technology that allows high-speed communication and data exchange between digital devices.

### FTP

File Transfer Protocol. A standard network protocol used to transfer files from one computer to another over the internet.

---

## G

### GB

Gigabyte. A multiple of byte, the unit for measuring the size of digital information. One gigabyte equals either 1,000,000,000 or 1,073,741,824 bytes, depending on the measurement standard used.

### GPRS

General Packet Radio Service. A packet-based wireless data standard used on GSM networks that allows mobile devices to maintain a continuous connection to the Internet. GPRS was the first popular data standard for mobile devices and is an evolutionary step toward EDGE and UMTS.

### GPS

Global Positioning System. A global system of navigational satellites that can provide precise location and time information anywhere on or near the Earth where there is an unobstructed line of sight to four or more GPS satellites.

### GSM

Global System for Mobile Communications. The world's most widely used international standard for digital cellular communications.

---

## H

### heartbeat

A regular signal sent by the agent indicating that it is still running on a computer.

---

**I**

---

**ICC Identifier**

Integrated Circuit Card Identifier. A number of up to 22 digits that uniquely identifies each SIM.

**IMEI**

International Mobile Station Equipment Identity. A 15-digit number that uniquely identifies all 3GPP (GSM, UMTS, and LTE) mobile devices.

**IMEISV**

International Mobile Station Equipment Identity Software Version. The two-digit software version number attached to the IMEI that identifies the revision of the software installed on the mobile device.

**in-house applications**

Applications that your organization has developed for use on mobile devices in your IT deployment.

**IPv4 address**

Internet Protocol Version 4 Address. A numerical label assigned to each device in a network using the Internet Protocol Version 4 for communication.

**iTunes**

Apple's mobile device management application that provides an interface for managing files and applications on iOS devices.

**iTunes Store**

An online digital media store operated by Apple that allows users of Apple devices to purchase and download music, video, electronic books, and other media.

---

**K**

---

**kernel**

A fundamental part of a mobile device's operating system that acts as a bridge between the device's software and hardware.

---

**M**

---

**MAC address**

Media Access Control Address. A 12-digit hexadecimal number that hardware devices use to uniquely identify themselves on a network.

**managed device**

A mobile device that is enrolled on the Absolute Manage server and that you can administer through Absolute Manage Web Admin.



**MDM**

Mobile Device Management. The module of Absolute Manage that provides support for administering mobile devices through an MDM server.

**media files**

Files that you can distribute to mobile devices through policies.

**MEID**

Mobile Equipment Identifier. A 14-digit number that uniquely identifies all CDMA mobile devices.

---

**O****Open Directory**

The native directory service for Mac OS X Server.

**OS**

Operating System. The software on mobile devices that manages hardware resources and provides common services for applications.

---

**P****passcode**

A string of alphanumeric characters required to access a mobile device.

**PCI**

Peripheral Component Interconnect. An interconnection system between a computer's micro-processor and any devices attached through expansion slots, such as modem cards and network cards.

**Persistence**

Technology that allows the Absolute Manage client software to remain on a mobile device even after removal attempts or factory resets. Persistence technology is supported on certain Android devices.

**policy**

A tool you can use to automate certain aspects of mobile device administration. A policy includes a collection of target mobile devices, plus one or more of the following elements: third-party applications, in-house applications, configuration profiles, and media files. There are two types of policies you can use: standard policies and smart policies.

**provisioning profile**

Applies to iOS devices only. A binary file that contains the necessary digital certificate, App ID, and UDIDs to allow an enterprise or beta application to be distributed to an iOS device outside of the App Store.

**push notifications**

A technique used by an application to alert mobile device users about content updates, messages, or other events without the need to open the application.

## R

---

### RAM

Random Access Memory. The main type of memory in a mobile device that provides a temporary workspace for quickly carrying out instructions and processing data.

### roaming

When a mobile device moves out of the standard network of its carrier and connects to networks of other carriers to resume voice or data service.

### ROM

Read-Only Memory. A type of storage medium that permanently stores data on a computer, even when turned off. Normally, ROM can only be read and not written to.

## S

---

### SCSI

Small Computer System Interface. A set of parallel interface standards developed by the American National Standards Institute (ANSI) for attaching printers, disk drives, scanners, and other peripheral devices to computers.

### SD

Secure Digital. A memory card format used in portable devices such as smartphones.

### SIM

Subscriber Identification Module. An integrated circuit that securely stores information used to identify and authenticate subscribers on mobile devices. A SIM circuit is embedded into a removable plastic card called a "SIM card".

### smart policy

A policy that allows you to set filter criteria that determine which mobile devices should be included in the policy.

### SMC

System Management Controller. A subsystem of Intel processor-based Mac computers that controls various internal systems.

### standard policy

A policy that allows you to manually add and remove specific mobile devices to and from the policy.

### swap space

The area on a hard disk that temporarily holds inactive memory pages, and along with RAM, makes up a machine's virtual memory. Swap space is used when a machine needs physical memory for active processes and there is insufficient unused physical memory available.

---

## T

---

### TCP

Transmission Control Protocol. A transport layer protocol used by applications that require guaranteed delivery of data.

### third-party applications

Applications for mobile devices that are developed outside of your organization and are generally available through a distribution platform such as Google Play or the App Store.

---

## U

---

### UDID

Unique Device Identifier. A 40-digit sequence of letters and numbers that uniquely identifies every iPhone, iPod touch, and iPad.

### UMTS

Universal Mobile Telecommunications Service. A third generation (3G) mobile broadband system for cellular networks based on the GSM standard that provides high-speed data and multimedia capabilities to mobile users.

### USB

Universal Serial Bus. An industry standard that defines the connection between electronic devices and their peripherals.

### UTC

Coordinated Universal Time. The primary time standard by which the world regulates clocks and time. UTC is closely related to and generally interchangeable with Greenwich Mean Time (GMT).

### UUID

Universally Unique Identifier. A 128-bit number that uniquely identifies Internet objects or data.

---

## V

---

### VPN

Virtual Private Network. A network technology that creates a secure connection to a private network over a public network such as the Internet.

### VPP

Volume Purchase Program. A program offered by Apple that allows organizations to purchase iOS applications in volume and distribute them to mobile device users through the use of activation codes.

**W**

---

**Wi-Fi**

A technology that allows electronic devices to connect to the Internet or communicate with one another wirelessly within a particular area over radio waves.