APPTIX®
Connecting Your Business. Anywhere.

Mobile Device Manager

BlackBerry User Guide (BlackBerry 10 / Legacy)

Document Revision Date: Oct. 21, 2014

Contents

Powered by

Overview

This MDM Blackberry User Guide describes the basic features of the Mobile Device Management Agent for Blackberry devices. This document also guides you through the steps involved to install the agent onto your Blackberry device and enroll the device for management through Mobile Device Manager.

This document covers both the new BlackBerry 10 and Legacy BlackBerry devices.

This user guide describes these features from the perspective of the mobile BlackBerry device user and covers the following topics:

- Enrolling your BlackBerry device using the AirWatch agent
- How to use the agent

Supported Devices

Supported BlackBerry 10 Devices

- BlackBerry Z10,
- BlackBerry Q10
- BlackBerry Q5

Supported Legacy BlackBerry Devices

- BlackBerry 5.0
- BlackBerry 6.0
- BlackBerry 7.0
- BlackBerry 7.1

Agents and Versions Supported

- **BlackBerry 10**
  We recommend always using the latest version of agent posted on BlackBerry AppWorld. AirWatch v7.0 requires a minimum agent version of 1.2.
- **Legacy BlackBerry**
  We recommend always using the latest version of agent posted on BlackBerry AppWorld. AirWatch v7.0 requires a minimum agent version of 1.2.

Requirements

Before reading this guide, perform actions needed to gather and prepare the following requirements:

Enrollment Requirements

All BlackBerry Devices

- **Admin Console Credentials** – These credentials allow access to the AirWatch environment.
- **Enrollment URL** – This is the Host Name URL, is unique to your organization's environment, and is defined in the Admin Console.
- **Group ID** – This ID associates your device with your corporate role and is defined in the Admin Console.

BlackBerry 10 Only

- **BlackBerry ID** – This username and password allow you to download the AirWatch Agent from BlackBerry AppWorld.

Software Requirements for BlackBerry 10 only

- **Windows PowerShell Credentials and URL (Optional)** – The Admin Console needs the location of the Windows PowerShell service and the credentials so that it can use commands to push actions to BlackBerry 10 devices using the Exchange ActiveSync protocol. If your mobile network does not include this service, you can still track assets and GPS locations and have management visibility for email traffic.

NOTES:

If your network does not include a PowerShell service and Exchange 2013/2010 or Office 365, then the Admin Console can only perform asset tracking. In order to push profiles, the network must include a PowerShell service and Exchange 2013/2010 or Office 365.

You must manually configure email on the BlackBerry device so that the device communicates with the PowerShell service and Exchange 2013/2010 or Office 365.

- **MEM Feature Components** – This feature permits or denies email access based on settings in the Admin Console. You must manually configure email on the BlackBerry 10 device for this feature to work.
    - **PowerShell Model** – This MEM deployment configuration requires the PowerShell service to communicate between your corporate email server, Exchange 2013/2010 or Office 365 and the Admin Console.

NOTE: You must manually configure email on the BlackBerry 10 device for this feature to work.

NOTES:

The current MEM design does not support the use of the Google Model for managing email on BlackBerry 10 devices.

If your network does not include a PowerShell service and Exchange 2013/2010 or Office 365, then the Admin Console can only perform asset tracking, track GPS locations, offer management visibility for email traffic, and control access to email systems. In order to push profiles or issue device wipes, the network must include a PowerShell service and Exchange 2013/2010 or Office 365.

- **Active Directory Integration** – The configuration of Active Directory services at the same Organization Group as the BES 10 lets the Active Directory services and BES 10 interact using the Admin Console.

BES Requirements for Legacy BlackBerry

- **BES version 5.0.3** – This version is compatible with the AirWatch solution.

Recommended Reading

AirWatch provides via AirWatch Resources many documents, videos, and webinars on a multitude of related subjects that will give you additional background and knowledge to aid you in the processes explained within this guide. If this is the first time using this guide, you might find the following information helpful:

- **AirWatch BlackBerry Management Solutions** Video – Provides a high-level video of MDM features available for BlackBerry devices. (http://fast.wistia.net/embed/iframe/a5jya7xhwo)
- **AirWatch Mobile Device Management Guide** – Provides additional information regarding the general aspects of MDM and Secure Channel.

BlackBerry 10 Device Enrollment

The Admin Console and BlackBerry 10 devices communicate using the AirWatch Agent. You can download and install the AirWatch MDM Agent from BlackBerry World.

Enrolling Using the AirWatch BlackBerry 10 Agent

1. Open the AirWatch Agent on the device to start the enrollment process using the **Enroll Device** option.
2. Enter the **Enrollment URL** and **Group ID** and click **Next**.
3. Enter your Admin Console user credentials and click **Next**.
4. Select the type of device in the **Device Ownership** drop-down menu.
   Settings include **Corporate-Dedicated**, **Corporate-Shared**, and **Employee-Owned**.
   This setting helps manage devices in a bring-your-own-device (BYOD) deployment.
5. Accept the terms of use to complete the enrollment process.

NOTE: You can configure options and push policies according to the type of device in **Configuration > System Configuration > Devices & Users > General > Privacy**. For example, you can configure the Admin Console to not collect GPS data for employee-owned devices.

BlackBerry 10 AirWatch Agent

Overview

The AirWatch Agent for BlackBerry 10 allows you more control and flexibility for device management. The agent will query your device for data sampling, GPS location, and profile compliance.

Configuring the AirWatch BlackBerry 10 Agent

Configure the AirWatch Agent so that devices can communicate and enroll with it. Find configurations in the Admin Console at **Groups & Settings > All Settings > Devices & Users > BlackBerry > BlackBerry 10**.

- **General** – Specify your company's PowerShell information so that the Admin Console can use commands to push profiles using the Exchange ActiveSync protocol.
    - **Power-Shell URL** – Specifies the URL where the Admin Console can access your PowerShell service.
    - **Username and Password** – Specifies the credentials the Admin Console needs to communicate with the PowerShell service.
- **Agent Settings** – Configure the following options so that the AirWatch Agent transmits the desired data to the Admin Console:
    - **Heartbeat Interval** – Specify when the AirWatch Agent confirms a connection and synchronizes with the Admin Console.
    - **Data Sample Interval** – Specify the intervals at which the AirWatch Agent collects data, as well as GPS location data from the device.
    - **Profile Refresh Interval** – Specify the intervals at which the AirWatch Agent refreshes profiles pushed from the Admin Console.
    - **Administrative Passcode** – Specify the passcode needed to access the **Settings** area of the AirWatch Agent.
    - **Enable GPS** – Select to enable the device to collect GPS data.

Using the AirWatch BlackBerry 10 Agent

The AirWatch Agent for BlackBerry 10 devices uses native BlackBerry APIs to collect asset and GPS tracking data that you can view in the AirWatch Agent. Tracked data includes information about the device, the network, GPS location, applicable services, and support.

The AirWatch Agent for BlackBerry 10 devices includes the following informational areas:

Option	Description
My Device	View current MDM details for the device, including: • **Enrollment** – View the enrollment status of the device. • **Connection Status** – View the connection status between the AirWatch Agent and the Admin Console. • **Location** – View the current GPS location of the device. • **Network** – View the WLAN information. • **Advanced** – View information about system resources, such as battery and memory statistics.
Settings	View information about the AirWatch Agent, including: • **About** – View the version of the AirWatch Agent installed on the device and the version of the AirWatch solution communicating with the AirWatch Agent. • **General** – View services communicating with the device and toggle location services settings.
Support	View and send data for troubleshooting issues on the device, such as **Email Support**.

Device Profiles

Overview

Deploying configurations to BlackBerry 10 devices requires using ActiveSync profiles. Profiles contain a group of payload configurations specific to a system or process. You can push the profile containing the payload configurations to devices over the air. You can set **Passcode** and **Custom Settings** profiles for BlackBerry 10 devices.

CAUTION: The AirWatch Admin needs to be aware that ActiveSync is used to push down profiles to users. If you have multiple users tied to you who are using multiple OSs (for example BlackBerry 10, Android and iOS), all devices will receive the profile you push down --not just BlackBerry devices. This means if a non-BlackBerry device is already being managed by a policy, conflicts could arise if the user is assigned a different mailbox policy in Exchange that contradicts the policy being pushed down. For example, if a passcode requirement was four characters, but the new profile pushed down requires eight characters, the new policy will override the old policy and cause conflicts for users who were set up to use four characters in the past.

Configuring General Profile Settings

The process for creating a profile consists of two parts. First, you must specify the General settings for the profile. The General settings determine how the profile is deployed and who receives it as well as other overall settings. Next, you must specify the Payload for the profile. The payload is the type of restriction or setting applied to the device when the profile is installed. As a best practice, it is recommended that you configure a single Payload per profile.

NOTE: The following profile settings and options apply to most platforms and can be used as a general reference. However, some platforms may offer different selections.

The general settings listed below apply to any profile:

1. Navigate to **Devices > Profiles > List View** and select **Add**.
2. Select the appropriate platform for the profile you wish to deploy.
   Depending on the platform you select, the following settings may vary.
3. Configure **General** settings on the applicable tab. These include:
   - **Name** – Name of the profile to be displayed in the Admin Console.
   - **Version** – Read-only field that reports the current version of the profile as determined by the **Add Version** button.
   - **Description** – A brief description of the profile that indicates its purpose.
   - **Deployment** – Determines if the profile will be automatically removed upon unenrollment:
     - **Managed** – The profile is removed.
     - **Manual** – The profile remains installed until removed by the end user.
   - **Assignment Type** – Determines how the profile is deployed to devices:
     - **Auto** – The profile is deployed to all devices automatically.
     - **Optional** – The end user can optionally install the profile from the Self-Service Portal (SSP) or can be deployed to individual devices at the administrator's discretion.

  - **Interactive** – This is a unique type of profile that is installed by end-users using the Self Service Portal. When installed, these special types of profiles interact with external systems to generate data to send to the device. This option will only be available if enabled in **Groups & Settings > All Settings > Devices & Users > Advanced > Profile Options**.
  - **Compliance** – The profile is deployed when the end user violates a compliance policy applicable to the device.
- **Allow Removal** – Determines whether or not the profile can be removed by the device's end user:
  - **Always** – The end user can manually remove the profile at any time.
  - **With Authorization** – The end user can remove the profile with the authorization of the administrator. Choosing this option adds a required **Password** field.
  - **Never** – The end user cannot remove the profile from the device.
- **Managed By** – The Organization Group with administrative access to the profile.
- **Assigned Smart Group** – The Smart Group to which you want the device profile added. Includes an option to create a new Smart Group which can be configured with specs for minimum OS, device models, ownership categories, organization groups, and more.

NOTE: While Platform is a criterion within a Smart Group, the Platform configured in the device profile or compliance policy will always take precedence over the Smart Group's platform. For instance, if a device profile is created for the iOS platform, the profile will only be assigned to iOS devices even if the Smart Group includes Android devices.

- **Exclusions** – If **Yes** is selected, a new field **Excluded Smart Groups** displays, enabling you to select those Smart Groups you wish to exclude from the assignment of this device profile.
- **View Device Assignment** – After you have made a selection in the **Assigned Smart Group** field, you may select this button to preview a list of all devices to which this profile will be assigned, taking the Smart Group assignments and exclusions into account.
- **Additional Assignment Criteria** – These check boxes enable additional restrictions for the profile:
  - **Enable Scheduling and install only during selected time periods** – Specify a configured time schedule in which devices receive the profile only within that time-frame. Selecting this option adds a required field Assigned Schedules. See *Time Schedules* for more information.
- **Removal Date** – The date the profile will be removed from the device. Must be a future date formatted as M/D/YYYY.

4. Configure a **Payload** for the device platform.
5. Select **Save & Publish**.

Deploying Passcode BlackBerry 10 Payloads

Deploy a Passcode payload for BlackBerry 10 devices to require a passcode on the device. This profile prevents unauthorized users from accessing content on the device. The Admin Console uses PowerShell commands to communicate in the Exchange ActiveSync protocol to push this profile to BlackBerry 10 devices.

To deploy a Passcode profile, following the steps detailed below:

1. Navigate to **Devices > Profiles > List View** and select **Add**.
2. Select **BlackBerry 10**.
3. Configure **General** settings for the profile.

4. Select the **Passcode** profile.
5. Configure the **Passcode** settings, including:
    - **Allow Simple Value** – Allows users to use a simple passcode.
    - **Minimum Password Length** – Sets the minimum value a passcode can be.
    - **Require Alphanumeric Value** - Requires the use of alphanumeric passwords.
    - **Maximum Number of Failed Attempts** – Reset the device to factory defaults if too many unsuccessful attempts have been made.
    - **Max Inactivity Time Device Lock** – Secure idle devices with short lock times.
    - **Maximum Passcode Age** – Enforce users to renew passcodes at selected intervals.
    - **Passcode History** – Logs past passcodes to prevent their reuse.
6. Select **Save & Publish** when you are finished to push the profile to devices.

AirWatch Agent for BlackBerry Legacy Devices

Overview

Before you enroll Legacy BlackBerry devices, you must prepare the AirWatch Agent for enrollment and download it on to devices. The AirWatch Agent facilitates communication between devices and the Admin Console.

Configuring the AirWatch Legacy BlackBerry Agent

Configure the AirWatch Agent for BlackBerry devices so that devices can communicate and enroll with it. Find configurations in the Admin Console in **Groups & Settings > All Settings > Devices & Users > BlackBerry > Legacy BlackBerry**.

- **Agent Application** – Enter the file path location of the AirWatch Agent in the **Download Path** field. The AirWatch Server finds the AirWatch Agent at this location to install it on the device.
- **Agent Settings** – Configure the following options so that the AirWatch Agent transmits the desired data to the Admin Console:
    - **Heartbeat Interval** – Specify when the AirWatch Agent confirms a connection and synchronizes with the Admin Console.
    - **Data Sample Interval** – Specify the intervals at which the AirWatch Agent collects data from the device.
    - **Profile Refresh Interval** – Specify the intervals at which the AirWatch Agent refreshes profiles pushed from the Admin Console.
    - **Collect Location Data** – Set the AirWatch Agent to send GPS data to the Admin Console.
    - **GPS Sample Interval** – Specifies the intervals at which the AirWatch Agent collects sample GPS data for the device.
    - **Administrative Passcode** – Specify the passcode needed to access the **Settings** area of the AirWatch Agent.
    - **Enable Branding** – Brand the AirWatch Agent with attributes specific to your company. Set the following applicable options:
        - **Login Title Text** – Specify the text users view to log in to the AirWatch Agent.
        - **Toolbar** – Specify the color of the toolbar in the AirWatch Agent.
        - **Background** – Specify the background color of the AirWatch Agent.
        - **Background Image –** Set a specific image for the background of the AirWatch Agent.
        - **Company Logo** – Import your company logo in to the AirWatch Agent.

Using the AirWatch Legacy BlackBerry Agent

The AirWatch Agent for Legacy BlackBerry devices includes information about the device and the user along with other administrative information. It can also send data for troubleshooting purposes. The AirWatch Agent includes the following informational areas:

Option	Description
My Device	View information about the device. • **General** – View information on battery life and available memory. • **Device Details** – View information about location, network, and telecom data. o **Location** – See GPS location information from the latest GPS sampling data. o **Network** – See network information such as the Wi-Fi IP address. o **Telecom** – See information about the number of calls made by the device and the number of text messages sent by the device.
User Info	View information about the user and the device, such as **User Name**, **Full Name**, **Contact Number**, **Email Address**, **Email Username**, and **Group**.
Support	Send data for troubleshooting issues on the device, such as **Send Heartbeat**, **Send Data Sample**, and **Send Profile**.
Settings	Configure and view MDM settings on the device. You must have the Admin passcode to view and configure these options. • **Server** – See the AirWatch Server URL that connects to the device. • **Heartbeat** – Configure and view information about synchronization. o **Transmission Frequency** – Set the transmission interval of data to the Admin Console. o **Last Heartbeat Attempt** – View the date and time of the last heartbeat sent to the Admin Console. o **Last Heartbeat Result** – View the success or failure of the last heartbeat sent to the Admin Console. • **Data Sampling** – Configure and view information about data sampling. o **Host Port** – Configure the port number to send data to the Admin Console. o **Transmission Frequency** – Set the transmission interval to send data samples to the Admin Console. o **Sample Frequency** – Set the interval for the AirWatch Agent to perform data sampling. o **Last Data Sampling Attempt** – View the date and time of the last data sample sent to the Admin Console. o **Last Data Sampling Result** – View the success or failure of the last data sample sent to the Admin Console. • **Profile Refresh, Profile Refresh Interval** – Set the interval to refresh the profile requests sent to the Admin Console. • **Logging, Log Level** – Send a log request to the Admin Console.
About	View the version of the AirWatch Agent.

Legacy Device Profiles

Overview

The AirWatch Agent links devices to the Admin Console and it allows you to push profiles to devices and to query the device for information. Use profiles to deploy configurations to devices over the air. Deploying configurations to legacy BlackBerry devices requires using profiles. Profiles contain a group of payload configurations specific to a system or process. You can push the profile containing the payload configurations to devices over the air. You can set the following profiles for legacy BlackBerry devices: Device, Telecom, Advanced, and Custom Settings.

Configuring General Profile Settings

The process for creating a profile consists of two parts. First, you must specify the General settings for the profile. The General settings determine how the profile is deployed and who receives it as well as other overall settings. Next, you must specify the Payload for the profile. The payload is the type of restriction or setting applied to the device when the profile is installed. As a best practice, it is recommended that you configure a single Payload per profile.

NOTE: The following profile settings and options apply to most platforms and can be used as a general reference. However, some platforms may offer different selections.

The general settings listed below apply to any profile:

1. Navigate to **Devices > Profiles > List View** and select **Add**.
2. Select the appropriate platform for the profile you wish to deploy. Depending on the platform you select, the following settings may vary.
3. Configure **General** settings on the applicable tab. These include:
   - **Name** – Name of the profile to be displayed in the Admin Console.
   - **Version** – Read-only field that reports the current version of the profile as determined by the **Add Version** button.
   - **Description** – A brief description of the profile that indicates its purpose.
   - **Deployment** – Determines if the profile will be automatically removed upon unenrollment:
     - **Managed** – The profile is removed.
     - **Manual** – The profile remains installed until removed by the end user.
   - **Assignment Type** – Determines how the profile is deployed to devices:
     - **Auto** – The profile is deployed to all devices automatically.
     - **Optional** – The end user can optionally install the profile from the Self-Service Portal (SSP) or can be deployed to individual devices at the administrator's discretion.
     - **Interactive** – This is a unique type of profile that is installed by end-users using the Self Service Portal. When installed, these special types of profiles interact with external systems to generate data to send to the device. This option will only be available if enabled in **Groups & Settings > All Settings > Devices & Users > Advanced > Profile Options**.
     - **Compliance** – The profile is deployed when the end user violates a compliance policy applicable to the device.
   - **Allow Removal** – Determines whether or not the profile can be removed by the device's end user:
     - **Always** – The end user can manually remove the profile at any time.

- **With Authorization** – The end user can remove the profile with the authorization of the administrator.
- Choosing this option adds a required **Password** field.
- **Never** – The end user cannot remove the profile from the device.

- **Managed By** – The Organization Group with administrative access to the profile.
- **Assigned Smart Group** – The Smart Group to which you want the device profile added. Includes an option to create a new Smart Group which can be configured with specs for minimum OS, device models, ownership categories, organization groups, and more.

NOTE: While Platform is a criterion within a Smart Group, the Platform configured in the device profile or compliance policy will always take precedence over the Smart Group's platform. For instance, if a device profile is created for the iOS platform, the profile will only be assigned to iOS devices even if the Smart Group includes Android devices.

- **Exclusions** – If **Yes** is selected, a new field **Excluded Smart Groups** displays, enabling you to select those Smart Groups you wish to exclude from the assignment of this device profile.
- **View Device Assignment** – After you have made a selection in the **Assigned Smart Group** field, you may select this button to preview a list of all devices to which this profile will be assigned, taking the Smart Group assignments and exclusions into account.
- **Additional Assignment Criteria** – These check boxes enable additional restrictions for the profile:
  - **Enable Scheduling and install only during selected time periods** – Specify a configured time schedule in which devices receive the profile only within that time-frame. Selecting this option adds a required field **Assigned Schedules**. See *Time Schedules* for more information.
- **Removal Date** – The date the profile will be removed from the device. Must be a future date formatted as M/D/YYYY.

4. Configure a **Payload** for the device platform.
5. Select **Save & Publish**.

Deploying Legacy BlackBerry Device Payloads

Deploy a Device payload to control the backlight settings to conserve battery power. Also set the GPS sampling feature. GPS sampling is useful for tracking routes and planning schedules. Consider the following options when configuring a **Device** payload:

To deploy a **Device** profile, following the steps detailed below:

1. Navigate to **Devices > Profiles > List View** and select **Add**.
2. Select **BlackBerry**.
3. Configure **General** settings for the profile.
4. Select the **Device** profile.
5. Configure the **Device** settings, including:
   - **Backlight Brightness** – Enter the brightness value you want the device to use.
   - **Backlight Timeout** – Enter the amount of seconds you want the device to wait before timing out the backlight.
   - **GPS Sample Enabled** – Enter the number of GPS data samples the AirWatch Agent takes before sending the information to the Admin Console.

- **GPS Sample Interval** – Enter the interval at which the AirWatch Agent takes GPS data samples.

6. Select **Save & Publish** when you are finished to push the profile to devices.

Deploying Legacy BlackBerry Telecom Payloads

Deploy a Telecom payload to track and research the amount and type of telecom traffic in your BlackBerry mobile environment. You can also control 411 calls to reduce telecom costs. Consider the following options when configuring a **Telecom** payload:

To deploy a **Telecom** payload, follow the steps detailed below:

1. Navigate to **Devices > Profiles > List View** and select **Add**.
2. Select **BlackBerry**.
3. Configure **General** settings for the profile.
4. Select the **Telecom** profile.
5. Configure the **Telecom** settings, including:
   - **Redirect 411** – Define the telephone number the device dials when calling 411 for information.
   - **Sample Enabled** – Select to enable sampling of telecom data.
   - **Track Content Enabled** – Select to enable the tracking of telecom data.
   - **Number of sampled calls** – Enter the number of call samples the AirWatch Agent records and sends to the Admin Console. Consider the battery life of the device when setting this option.
   - **Number of sampled SMS** – Enter the number of text samples the AirWatch Agent records and sends to the Admin Console. Consider the battery life of the device when setting this option.
6. Select **Save & Publish** when you are finished to push the profile to devices.

Deploying Legacy BlackBerry Advanced Payloads

Deploy an Advanced payload to control logging functions for BlackBerry devices. Logging helps with tracking application flows, data and traffic research, and troubleshooting. Consider the following options when configuring an **Advanced** payload:

To deploy an **Advanced** payload, follow the steps detailed below:

1. Navigate to **Devices > Profiles > List View** and select **Add**.
2. Select **BlackBerry**.
3. Configure **General** settings for the profile.
4. Select the **Advanced** profile.
5. Configure the **Advanced** settings, including:
   - **Memory Percentage Remaining** – Defines the percentage of memory that remains before log samples are deleted to save memory.
   - **Sample Count** – Defines the number of log samples that remain based on the entry for **Memory Percentage Remaining**.
   - **Log Level (Verbose, Debug, Info, and Error)** – Defines the level of logging activity.
   - **Log Destination (File and Event Log)** – Creates a log file or an event log for data sampled on the device.
     - The **File** option creates a log file on the device.
     - The **Event Log** option creates a device event in the Admin Console located in **Hub > Reports &**

Analytics > Events > Device Events.

- **Log Size (KB)** – Defines the size of the log file or the event log.
- **Logging Host** – Displays the look up value to find the domain name of the logging server in which the device is enrolled. This lookup value is prepopulated so that you do not need to configure this setting. The look up value is **{InterrogatorURL.Host}**.
- **Logging Path** – Defines the location of the logging application on the AirWatch server.

6. Select **Save & Publish** when you are finished to push the profile to devices.

Deploying Custom Settings Legacy BlackBerry Payloads

Deploy a **Custom Settings** payload to create your own profiles using custom XML. This feature allows you to push code that can perform special functions not already defined in the Admin Console. The Admin Console packages and pushes this custom XML profile to BlackBerry devices.

Managing All BlackBerry Devices

Overview

You can manage all of your deployment's devices from the AirWatch **Dashboard**, which is a searchable, customizable view you can use to filter and find specific devices based on various criteria. This simplifies performing actions and administrative functions on a particular set of devices. You may also generate **Reports** and examine the data flow within the AirWatch **Hub**. Additionally, you can easily identify devices with **Tags**. Lastly, you can set up the Self-Service Portal (SSP) to empower end users to manage their own devices and reduce the strain on Help Desk personnel.

Registration of BlackBerry 10 and Legacy BlackBerry Devices

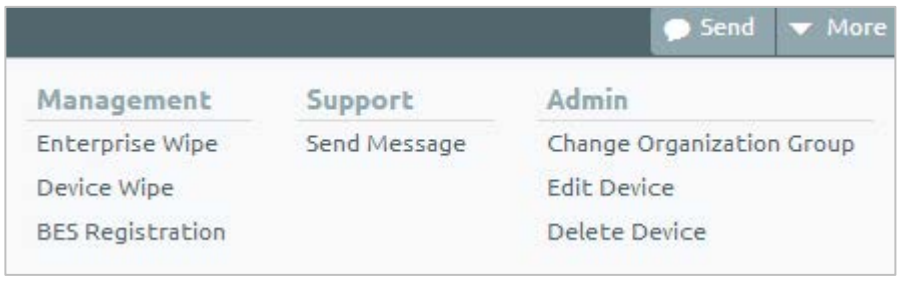
BlackBerry 10 and Legacy BlackBerry devices require AirWatch enrollment in order to receive policies. For BlackBerry 10 devices, AirWatch will automatically initiate registration with BES 10 upon the device being enrolled with the MDM Agent.

For Legacy BlackBerry devices, the AirWatch Admin can initiate BES registration from the Admin Console. In both scenarios, the user will receive an email or a text message with the BES registration token. Using this token, the device user can activate the device with the respective BES server.

Registration of BlackBerry 10 Devices

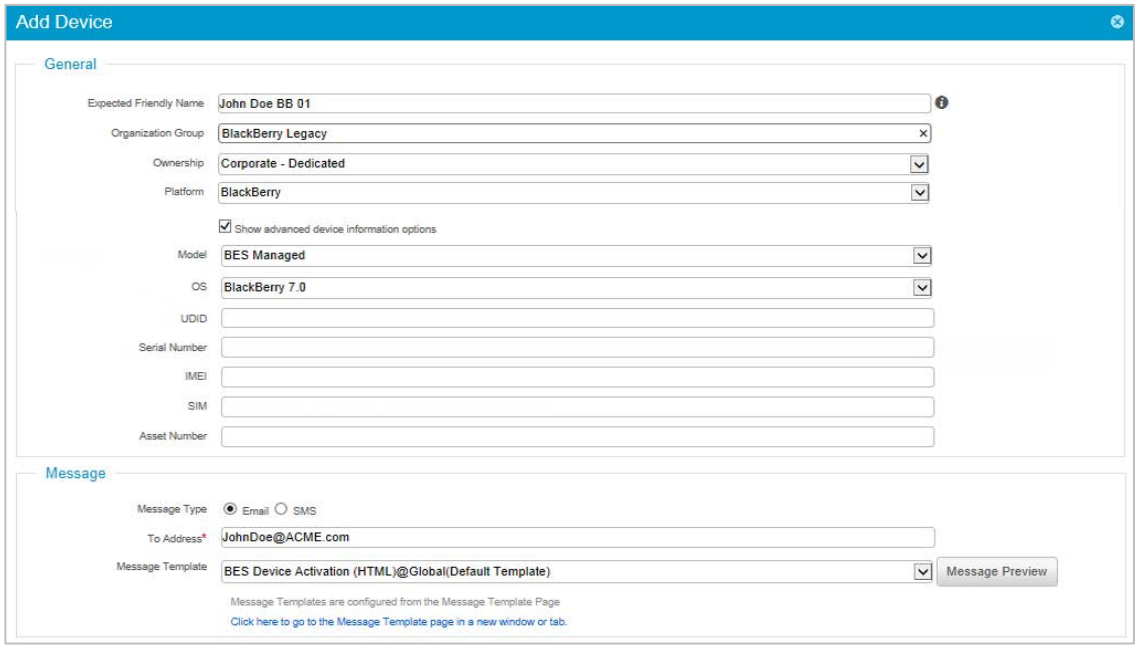
Upon enrollment in AirWatch, BES registration is automatically initiated provided the device is not already registered with BES-10. For BlackBerry 10 devices using BES 10, do the following:

1. Navigate to **Devices > List View** in the Admin Console
2. Search in the **Filter Grid** for BlackBerry devices.
3. Click on the **Friendly Name** of the desired device.
   The details for that device displays.
4. Click the **More** drop-down in the upper right.
5. Select **BES Registration** from the drop-down and follow the prompts.



Registration of Legacy BlackBerry Devices

1. Navigate to **Devices > List View > ADD DEVICE** in the Admin Console.



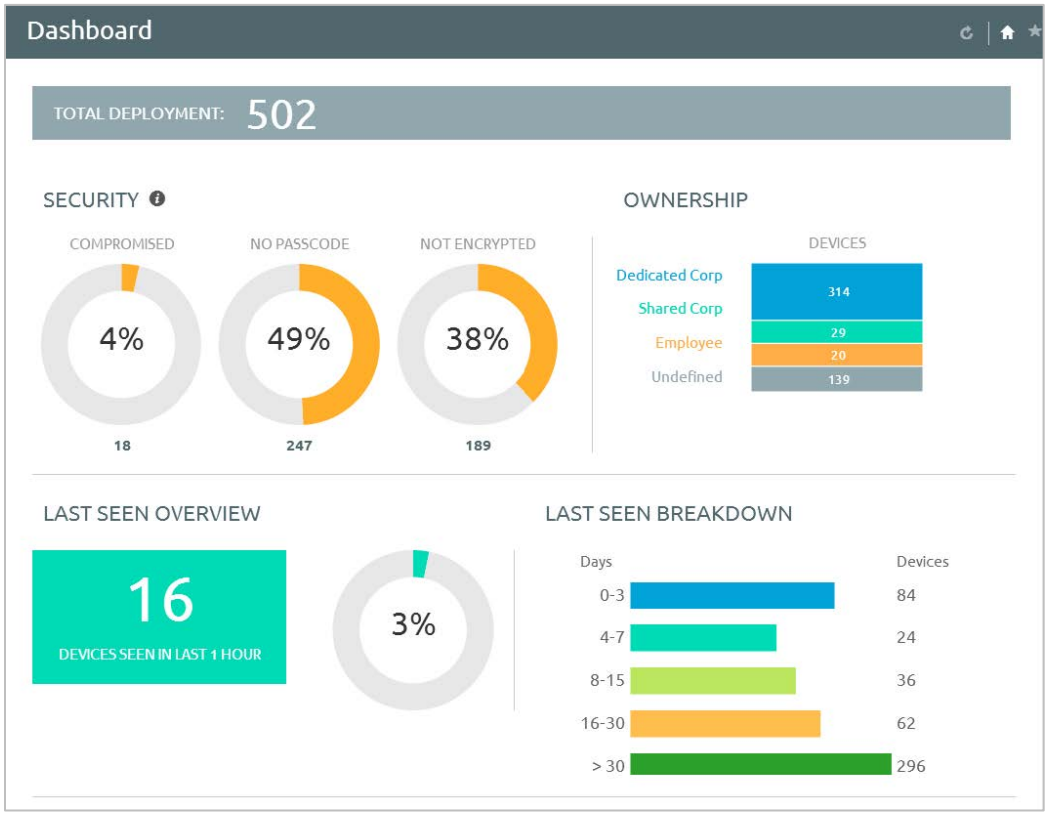
2. Enter a name for the device user in **Expected Friendly Name**.
3. Enter the **Organization Group** in the field.
4. Select from the drop-down the owner of the device in **Device Ownership**.
5. Select BlackBerry from the **Platform** drop-down menu.
6. Select the **Show advanced device information** options checkbox.
7. Click the Model drop-down and select BES Managed.
8. Select from the **OS** drop-down or enter details in the **UDID**, **Serial Number**, **IMEI**, **SIM**, and **Asset Number** fields that allow more granular control, otherwise, continue to the next step.
9. Select either the **Email** or **SMS** radio button to determine the method used to send the device user enrollment information.
10. Enter the device user's email in the **To Address** field.
11. Select from the **Message Template** drop-down the enrollment template the device user will receive via email or SMS.

    NOTE: You can review the message that will be sent to the device user by clicking on the **Message Preview** button.

12. Click **Save**.

Using the Device Dashboard

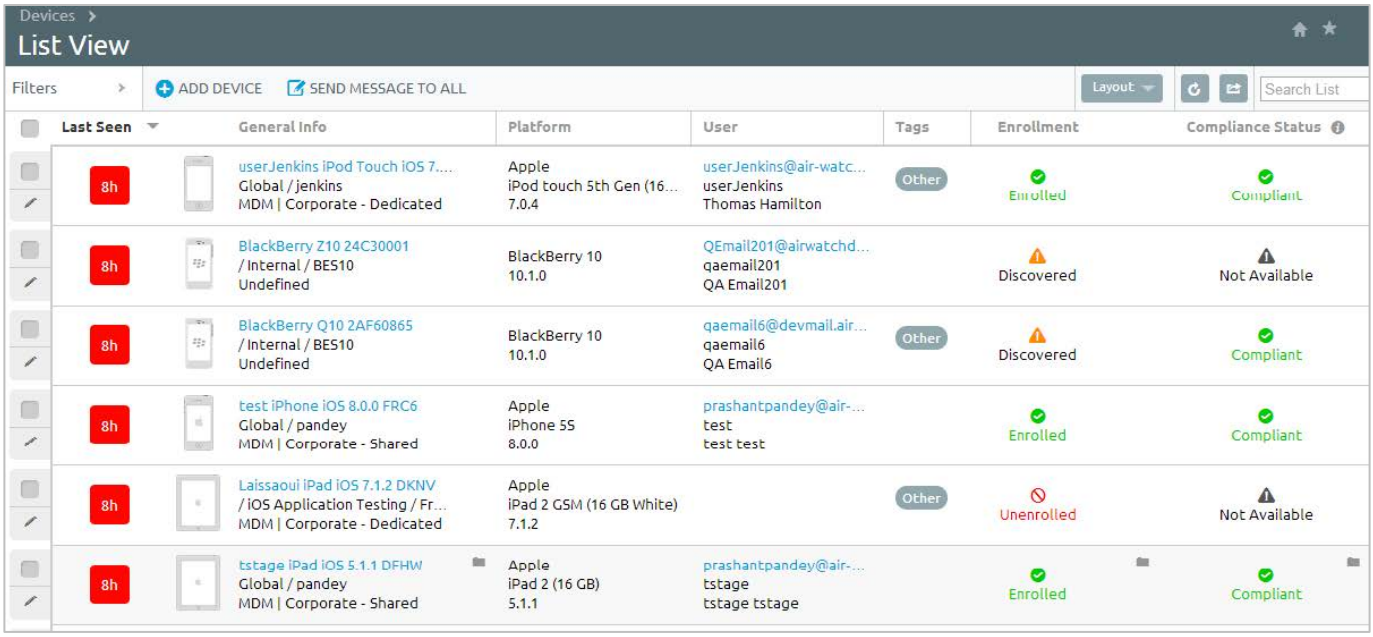
As devices are enrolled, view and manage them from the **Device Dashboard**. The **Device Dashboard** provides a high-level view of your entire fleet of mobile devices while allowing a quick and easy way to drill down to individual devices and take MDM actions. View graphical representations of relevant statistics, including important device information for your fleet, such as device ownership type, compliance statistics, and telecom usage.



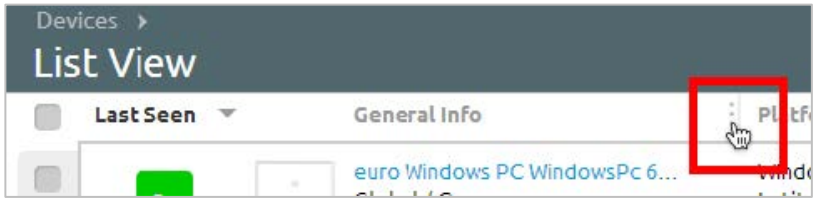
Select any of the available data views from the **Device Dashboard** to quickly access each set of devices in the **List View**. From this List View, take administrative action, including send a message, lock devices, delete devices, and change groups associated with the device.

Using the Device List View

1. Switch to **List View** (**Devices > List View**) at any time to sort and manage devices by filtering the columns and fields available in the **Device Dashboard**, including:
   - **Last Seen**
   - **General Info** (friendly name, display name, ownership, organization group)
   - **Platform/OS/Model**
   - **User**
   - **Tags**
   - **Enrollment Status**
   - **Compliance Status**



2. Select a device **Friendly Name** at any time to open up the device details page for that device.
3. Sort columns and configure information filters to gain insight on device activity based on specific information you are curious about.
   For example, sort the **Compliance Status** column to view only devices that are currently out-of-compliance and take action or message only those specific devices.
4. Search all devices for a friendly name or user's name to isolate one device or user.
   You may also rearrange the order of the columns as they are presented in the listing by dragging and dropping the column headings.



Once you have sorted or filtered dashboard information, export, save, and send the data for review.

Hover-Over Pop-up

Each device in the **General Info** column features a tooltip icon in the upper-right corner. When this icon is tapped (mobile touch device) or hovered-over with a mouse cursor (PC or Mac), it will display a Hover-Over Pop-up containing information such as the device's **Friendly Name**, **Organization Group**, **Group ID**, **Management**, and **Ownership**.

Similar tooltip icons are found in the **Enrollment** and **Compliance Status** columns in the **Device List** view, featuring Hover-Over Pop-ups displaying **Enrollment Date** and **Compliance Violations** respectively.

Using the Search List, Filters, and Bulk Messaging

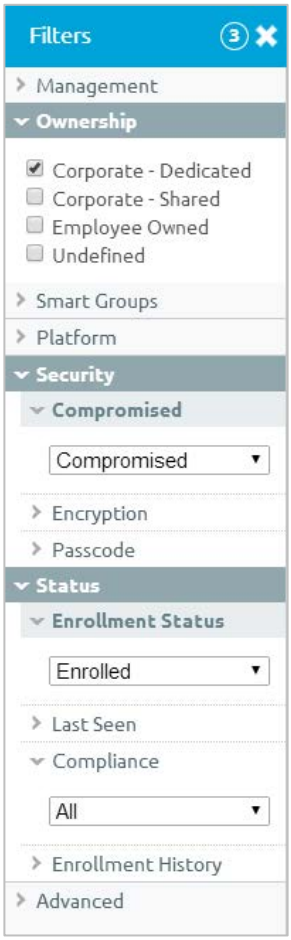
At times, you will need to search for a single device for quick access to its information and take remote action on the device. For example, search for a specific device, platform or user.

Navigate to **Devices > List View > Search List** and search for all devices within the current Organization Group and all child groups.

You can also drill down to specific sets of devices by filtering device criteria, including by **Platform**, **Ownership Type**, **Passcode**, **Last Seen**, **Enrollment**, **Encryption**, and **Compromised** status.

You can also search specific information across all fields associated with devices and users, allowing you to search user name ("John Doe") or device type.

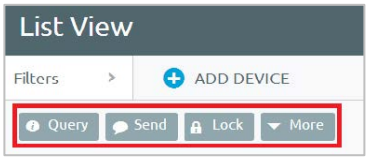
Once you have applied a filter to show a specific set of devices, perform bulk actions to multiple, selected devices by clicking the check box for those devices and selecting an action from the **Management** tabs.



Using the Management Tabs

With the categorized devices displayed, take bulk action on specific devices by selecting the check box next to each device and using the top Control Panel to:

NOTE: The actions listed below will vary depending on factors such as device platform, Admin Console settings, and enrollment status.



With the categorized devices displayed, take bulk action on specific devices by selecting the check box next to each device and using the top Control Panel to:

Query – Query all selected devices for current device info, including last seen, OS, model, and compliance status.

Send – Access the **Send Message** menu and compose message to send to selected devices.

Lock – Lock all selected devices and force users to re-enter device security PIN.

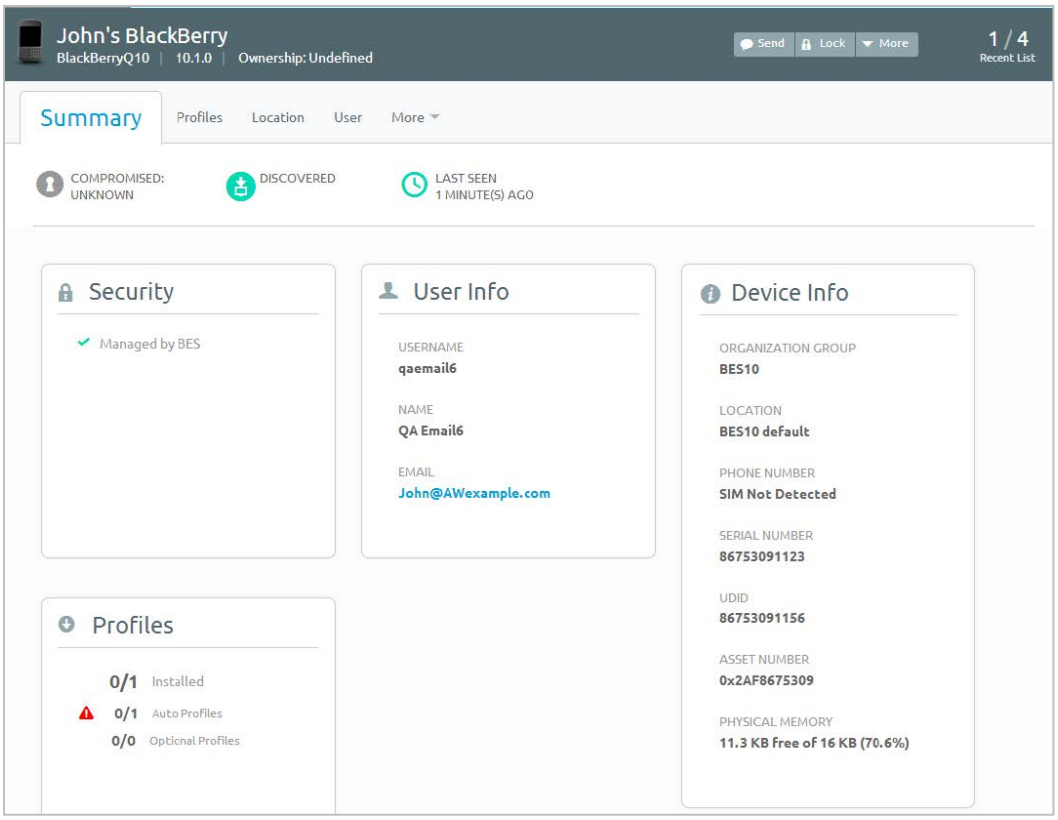
More – View commands that you can perform on all selected devices. For example:

- **Management** – Query, lock or perform Enterprise Wipe on all selected devices.
- **Support** – Send a message to a device with instructions or communication to end user. Locate current GPS location of all selected devices.
- **Admin** – Change Admin Console settings, including changing Organization Group, Ownership type, or device group of selected devices or deleting devices from AirWatch MDM.
- **Advanced** – Perform a warm boot on devices to remotely reboot those devices.
  Select **Provision Now** to perform a number of configurations for selected devices.
  Select **Install Product** to install particular apps to selected devices.

You can perform additional remote actions to individual devices from the **Device Details** page.

Using the Device Details Page

Use the **Device Details** page to track detailed device information and quickly access user and device management actions. You can access the **Device Details** page by selecting a device's **Friendly Name** from the **List View** page or from one of the available Dashboards, or by using any of the available search tools within the Admin Console.

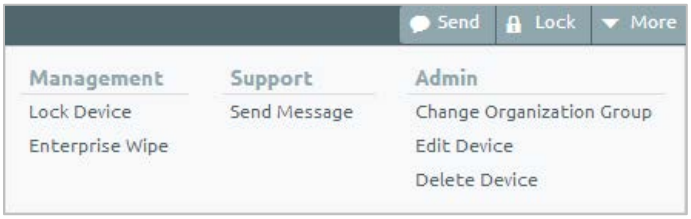


Use the **Device Details** menu tabs to access specific device information, including:

- **Summary** – Displays a snapshot of the status of the device including its security status, if it has a passcode, its network information and the number of profiles and applications installed on the device.
- **Profiles** – Lists the AirWatch profiles that are currently on the device.
- **Apps** – Lists the applications that are currently on the BlackBerry device.
- **Location** – Locates the device using GPS and displays the location on a map.
- **User** – Provide information about the device user.
- **Event Log** – Clicking **More** and selecting this from the drop-down lists the events triggered on the device.

Performing Remote Actions

The **More** drop-down on the Device Details page enables you to perform remote actions over-the-air to the selected device. See below for detailed information about each remote action.

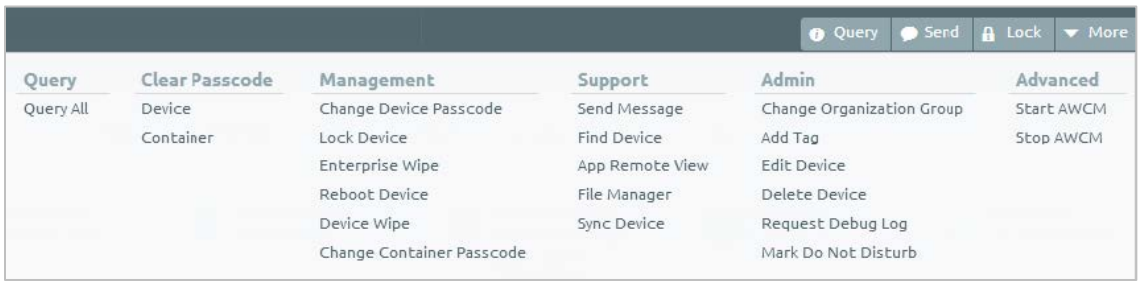


NOTE: The actions listed below vary depending on factors such as device platform, Admin Console settings, and enrollment status.

- **Enterprise Wipe** – Removes AirWatch profiles and applications. For BlackBerry 10 devices, this command blocks devices from accessing email.
- **Device Wipe –** Returns all BlackBerry devices to factory defaults. For BlackBerry 10 devices, the AirWatch solution uses PowerShell integration with your EAS platform to push the wipe.
- **Send Message –** Sends text messages to all BlackBerry devices from the Admin Console.
- **Lock Device** – Locks legacy BlackBerry devices. This option is *not* available for BlackBerry 10 devices.
- **BES Registration –** Allows the AirWatch Admin to register *only* BlackBerry 10 devices with the BES 10 server. This option is not available for legacy BlackBerry devices. For instructions on how to register legacy BlackBerry devices, see *Registration of Legacy BlackBerry Devices*.
- **Management** – Lock or perform an Enterprise Wipe on all selected devices.
  When you lock a SAFE 4 device, you can configure a customized lockscreen. Set the **Message Template** to **Custom Message**. Then, in the **Message** field, provide your text and provide a **Phone Number**.
- **Support** – Send a message to email AirWatch Technical Support regarding selected device. Also, locate the device according to its current GPS location.
- **Admin** – Change Admin Console settings, including changing Organization Group and editing/deleting devices from AirWatch MDM.
- **Advanced** – Perform a warm boot on devices to remotely reboot those devices. Select **Provision Now** to perform a number of configurations for selected devices.

Performing Remote Actions

The **More** drop-down on the Device Details page enables you to perform remote actions over-the-air to the selected device. See below for detailed information about each remote action.



NOTE: The actions listed below vary depending on factors such as device platform, Admin Console settings, and enrollment status.

- **Query** – Query the device for all information.
- **Clear Passcode** – Clear either the device-level passcode or the SSO Passcode.
- **Management** – Lock the device or SSO session, reboot the device, or perform an enterprise or device wipe.
- **Support** – Perform support actions such as sending the device a message, finding the device by playing an audible tone, or syncing the device.
- **Admin** – Change Admin Console settings, including changing Organization Group, and editing/deleting devices from AirWatch MDM.

Utilizing Reports

AirWatch has extensive reporting capabilities that provide administrators with actionable, result-driven statistics about their device fleets. IT administrators can leverage these pre-defined reports or create custom reports based on specific devices, User Groups, date ranges or file preferences.

In addition, the administrator can schedule any of these reports for automated distribution to a group of users and recipients on either a defined schedule or a recurring basis. For example, you can run reports to see the number of compromised devices, how many devices there are for a specific make or model, or the total amount of devices running a particular version of an operating system.

For more information about generating custom reports, compiling a list of personalized bookmarked reports, and creating report subscriptions, refer to the *AirWatch Reporting Analytics Guide*.

Using the Hub

Utilize the AirWatch Hub as your central portal for fast access to critical information. Quickly identify important issues or devices and take action from a single location in the Admin Console. Select any metric to open the **Device List View** for that specific set of devices, where you can perform actions such as sending a message to those devices.

For more information about using the Hub to filter and view specific information, refer to the *Managing Devices* section of the *Mobile Device Management Guide*.