Introduction to BlackBerry 10 and Legacy BlackBerry

Overview

This guide is divided into two sections —the first half for BlackBerry 10 and the second half for Legacy BlackBerry devices. Descriptions of what is covered in these sections are as follows:

BlackBerry 10 Overview

BlackBerry has been an icon in the industry of securing corporate data on mobile devices. The release of BlackBerry 10 redesigns their platform by adding new features, such as touch screen and Exchange ActiveSync compatibility. BlackBerry Enterprise Server 10 (BES) was designed to manage all the latest features for BlackBerry 10 devices, however if your enterprise has not implemented a BES 10 server, since BlackBerry 10 devices are compatible with Exchange ActiveSync, it is possible to manage certain functions of BlackBerry 10 devices without having a BES 10 server using AirWatch. This compatibility makes it ideal for companies who do not want to incur the costs of implementing a BES 10 server and find the alternative management capabilities suitable for their deployment.

The first half of the guide explains managing BlackBerry 10 devices. It describes how to integrate, enroll BlackBerry 10 devices with the AirWatch Admin Console, configure devices and outlines the deployment of AirWatch profiles for BlackBerry 10 devices. It also explains functions that the AirWatch Admin Console can control and manage, including wiping devices and pushing a passcode policy using the Exchange ActiveSync protocol and Windows PowerShell commands, integrating with native BlackBerry 10 Application Programming Interfaces (APIs) to track assets, integrating with the Mobile Email Management (MEM) feature to manage email on BlackBerry 10 devices, and the ability to migrate other platforms into the AirWatch solution.

Legacy BlackBerry Overview

The security of the BlackBerry Enterprise Server (BES) and its management of BlackBerry devices has played an important role in securing corporate data. The AirWatch Admin Console integrates with the BES infrastructure allowing you to manage BlackBerry devices along with other mobile devices in a central location. This integration allows you to push profiles to BlackBerry devices, such as telecom usage collection, along with actions such as remotely locking devices. View and track device information in the Device Dashboard. This integration also streamlines the process of migrating to other mobile platforms.

The second half of this guide explains the management of legacy BlackBerry devices. It explains how to integrate with the BES and it describes how to enroll legacy BlackBerry devices with the AirWatch Admin Console. It also discusses the deployment of AirWatch profiles for these devices along with managing these devices in the AirWatch Admin Console.

In this Guide

You will find in this guide the following procedures that were arranged in a logical sequence to guide you from enrolling to managing devices:

- Before You Begin – Details device hardware and software supported, requirements, recommended reading, and things you should know and do before proceeding.
- BES 10 Server Integration – Discusses the process of integrating AirWatch with the BES 10 and use of the AirWatch Cloud Connector (ACC) in a SaaS environment.
- BlackBerry 10 Device Enrollment – Explains the enrollment process needed to establish initial communications with AirWatch.
- AirWatch Applications for BlackBerry 10 Devices –
- Device Profiles for BlackBerry 10 – Explores the AirWatch Admin Console features, such as enabling services for the agent, deploying profiles and credentials, controlling profile time schedules, MEM, etc.
- Legacy BES Server Integration – Describes how AirWatch integrates with BES, rather than replacing it, allowing BES to maintain secure communication between BlackBerry devices and corporate networks.
- AirWatch Agent for Legacy BES Devices– Details the AirWatch Agent for Legacy BES devices including enrollment, configuration, and use.
- Device Profiles for Legacy BES – Explores the AirWatch Admin Console features, such as enabling services for the agent, deploying profiles and credentials, controlling profile time schedules, etc.
- Managing All BlackBerry Devices – Provides AirWatch Admin Console and Self-Service Portal navigation to features needed by administrators to manage devices, as well as information on migrating to other platforms.
- Appendix – BES Configuration – Details the BES Integration Task for on-premise AirWatch deployments and how to adjust synchronization between the BES and AirWatch.

Before You Begin

Overview

This legacy BlackBerry and BlackBerry 10 guide was written for AirWatch administrators and explains the complete process from enrolling to managing those devices in AirWatch. This guide simplifies the entire process by explaining each process step-by-step in a logical sequence. By following procedures in this guide, you can ensure a successful deployment of all BlackBerry devices.

In this Section

You will find in this section all the information you need to know prior to advancing to the procedures in this guide:

- Supported Devices, OS, Agents, Versions, and Browsers—Lists BlackBerry devices and software versions supported by AirWatch.
- Requirements —Details useful and/or required information you need before continuing with this guide.
- Recommended Reading —Provides a list of helpful guides to better your understanding of mobile device management and BlackBerry devices.
- Getting Started —Provides guidance on the steps we recommend you take before using this guide.

Supported Devices, OS, Agents, Versions, and Browsers

Platforms and Devices Supported

BlackBerry 10

AirWatch v7.0 supports the use of the **BlackBerry Z10, Q10, and Q5**.

Legacy BlackBerry

AirWatch v7.0 supports the use of **BlackBerry 5.0, 6.0, 7.0, and 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

- **AirWatch 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 AirWatch Admin Console.
- **Group ID** –This ID associates your device with your corporate role and is defined in the AirWatch 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 AirWatch 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 AirWatch 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 AirWatch 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 AirWatch Admin Console.

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

    - AirWatch **Secure Email Gateway (SEG)/Proxy Model** – This MEM deployment configuration requires the SEG to communicate between your corporate email server, **Exchange 2007/2003, Lotus Notes, or Novell GroupWise** and the AirWatch Admin Console.

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 AirWatch 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 AirWatch Admin Console.

BES Requirements for Legacy BlackBerry

- **BES version 5.0.3** – This version is compatible with the AirWatch solution.
- **BES Admin Account Credentials** – This account allows you to configure the AirWatch Admin Console to access the BES Web Console interface.
- **BES Server information** – Includes the BlackBerry Web Services (BWS) URL, the BWS Utility URL and the location of the BES. This information is needed to configure communication between the AirWatch Admin Console and the BES.
- **Active Directory Integration** – The configuration of Active Directory services at the same Organization Group as the BES lets the Active Directory services and BES interact using the AirWatch Admin Console.

Recommended Reading

AirWatch provides in ASK 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.

Getting Started

Before you begin, we recommend you familiarize yourself with the following documentation and verify the following items have been implemented in order to make for a smooth transition from the first to last procedure in this guide.

- Review the AirWatch Mobile Device Management (MDM) Guide. The MDM guide covers many of the subjects discussed in this guide, such as enrollment, configuration and security profiles, and the AirWatch Dashboard.
- Familiarize yourself with key areas of the AirWatch Admin Console.
- .

BES 10 Server Integration

Overview

AirWatch can integrate with the BES 10 either in an on-premise environment or in a software as a service (SaaS) environment. In a SaaS deployment, BES integration requires the use of the AirWatch Cloud Connector (ACC). Primarily, you can use AirWatch to register BlackBerry 10 devices into the BES 10 infrastructure, and use the integrated environment to provision BES commands to the device. You can use the AirWatch Agent in conjunction with BES 10 in order to manage the device.

In This Section

- AirWatch Integration Requirements – Defines communication and integration requirements between BES 10 and AirWatch admin console.
- BES Integration Requirements – Defines integration requirements for BES 10.
- Connecting AirWatch to the BES 10 Server – Lists a procedure for connecting the BES 10 server and AirWatch admin console.
- Testing the Connection to the BES 10 Server – Lists a procedure for testing the connection between BlackBerry devices, BES 10 server, and AirWatch admin console.
- Using the MEM Feature for BlackBerry 10 Devices – Learn how to control access to corporate email systems and manage email on devices.

AirWatch Integration Requirements

To configure communication between the BES 10 and the AirWatch Admin Console, you need to set communications using a secure and functional port (e.g., 443) for the following:

- AirWatch MDM Server requires a communication channel to the BES Server over TCP.
- AirWatch MDM Server also requires a communication channel to the Active Directory (AD) Server.
- AirWatch solution uses the admin account that has administrator rights on the BES server. Typically, this admin account is used to access the BES Web Console interface from which BlackBerry devices are managed.

Note: Verify there is connectivity on the port you choose to use.

BES Integration Requirements

- Use a valid BES admin account. You can check this by signing into the BES Web Console using the BES Username, BES Password and Domain.
- Set up AD integration at the AirWatch**Organization Group** where you want to integrate the BES.

- Activate the BES on the SIM card that the BlackBerry device actually uses.

Connecting AirWatch to the BES 10 Server

Use the following procedure to connect the AirWatch Admin Console and the BES 10 server:

1. Navigate to **Groups & Settings ▶All Settings ▶Device & Users ▶BlackBerry 10 ▶BES 10 Settings**.
2. Enter in **BES URL** the URL for the BlackBerry Web Services that contains all the web service APIs used to synchronize the AirWatch solution and the BES 10 server. The URL format is *https://<BES_URL>:38443*.
3. Enter the username and password needed to authenticate with the BES 10 server in the **BES Admin Username** field and the **BES Admin Password** field.
4. Ensure that the **Authentication Method** field is set to **Active Directory** or **BlackBerry Administration Service**.
5. Enter a domain for the BES 10 server in the **Domain** field.
6. If you want to ignore Secure Socket Layer (SSL) certificate errors between AirWatch component and the BES 10 server then select the **Ignore SSL Errors** checkbox.
7. Enter a value in the **BES Sync Batch Size** field for the maximum size of the message to be sent from the BES 10 server through the AirWatch Admin Console to the device.
8. Enter the number of hours in the **Activation Code Expiration** field for the amount of time the end user has to activate their BES 10 server.
9. Select from the **BES Registration Message** dropdown a message the end user receives upon registration.
10. Select either the **Email** or **SMS** radio button to determine the method used to deliver the **BES Registration Message**.

Testing the Connection to the BES 10 Server

Test the connection between AirWatch, the BES and BlackBerry devices. These steps work for on-premise environments. These settings are not visible in the AirWatch Console for SaaS environments unless you also have the AirWatch Cloud Connector (ACC).

1. Go to **Groups & Settings ▶All Settings ▶Device & Users ▶BlackBerry 10 ▶BES 10 Settings**.
2. Click **Test Connection** at the bottom of the screen.

Note: For more information about performing BES integration tasks, see the **Appendix: BES Configuration**.

3. Click **Sync Now** to manually sync all devices and users from the BES 10 server.

Note: If you do not manually sync the devices then it will not occur until the next scheduled service. For more information, see Appendix – BES Configuration.

Using the MEM Feature for BlackBerry 10 Devices

The Mobile Email Management (MEM) feature offers management visibility to your *corporate email traffic* and it controls device access to corporate email systems. The feature requires specific deployment configurations and components. If you have the MEM feature configured and enabled, then after BlackBerry 10 devices enroll with the AirWatch Admin Console, the feature manages the email system on the device.

Note: You must manually configure email on BlackBerry 10 devices so that the MEM feature can manage email on that device.

The AirWatch Admin Console includes BlackBerry 10 devices in the MEM Dashboard by displaying all devices enrolled with AirWatch as managed BlackBerry 10 devices.

The MEM feature uses several configuration models. The two that support the use of BlackBerry 10 devices are the PowerShell model and the SEG/Proxy model.

- The PowerShell model with Exchange 2013/2010 or Office 365 provides management visibility for BlackBerry 10 email traffic, controls device access to email systems, pushes Passcode profiles and issues device wipes.
- The SEG/Proxy model with Exchange 2007/2003, Lotus Notes or Novell GroupWise provides management visibility for BlackBerry 10 email traffic and controls device access to email systems. However, to push Passcode profiles and issue device wipes, your mobile infrastructure must use the PowerShell service, and Exchange 2013/2010 or Office 365.

Note: If you do not have either infrastructure, you can still perform asset tracking and track GPS locations for BlackBerry 10 devices.

For more information about the MEM feature, see the **AirWatch MEM Guide**.

BlackBerry 10 Device Enrollment

Overview

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

In This Section

- Enrolling Using the AirWatch BlackBerry 10 Agent – Defines the steps needed to enroll a device.
- Staging a BlackBerry 10 Device – Explains how to enroll devices using single-user staging.
- Post Enrollment for BlackBerry 10 Devices – Defines the steps taken after a device enrolls in AirWatch.

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 user name and password credentials supplied by your AirWatch admin and then 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 **Groups & Settings ▶All Settings ▶ Devices & Users ▶General ▶Privacy**. For example, you can configure the AirWatch Admin Console to not collect GPS data for employee owned devices.

Staging a BlackBerry 10 Device

You can enroll devices using **Single-User** staging. For more information, see **Enrolling Devices** in the **AirWatch MDM Guide**.

Note: At this time, BlackBerry 10 only supports Single-User, not Multi-User staging.

Post Enrollment for BlackBerry 10 Devices

Once a BlackBerry 10 device completes enrollment with AirWatch using the MDM Agent, AirWatch automatically reaches out to the BES 10 server to verify if the device is already registered in the BES 10 environment. If the device is already registered with BES 10 server then no action is required, otherwise the following steps are taken:

1. AirWatch automatically sends a registration token to BES 10 for the email address of the enrollment user.
2. At the same time, AirWatch also sends a message to the user (either via an email or an SMS) with the registration token and email address to use for registering with BES 10.

Note: Whether you receive the token via email or SMS depends on the configuration in the AirWatch Admin Console under **Configuration ▶System Configuration ▶Devices & Users ▶BlackBerry ▶BlackBerry 10 ▶BES 10 Settings**.

3. The user can then register the device with BlackBerry 10 using the AirWatch provided token.
4. Upon registration, all BES policies that were defined by the BES 10 Admin are downloaded onto the device.

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, 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 AirWatch Admin Console **Groups & Settings ▶All Settings ▶Devices & Users ▶BlackBerry▶BlackBerry 10**.

- **General** – Specify your company's PowerShell information so that the AirWatch Admin Console can use commands to push profiles using the Exchange ActiveSync protocol.
  - **Power-Shell URL** – Specifies the URL where the AirWatch Admin Console can access your PowerShell service.
  - **Username and Password** – Specifies the credentials the AirWatch 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 AirWatch Admin Console:
  - **Heartbeat Interval** – Specify when the AirWatch Agent confirms a connection and synchronizes with the AirWatch 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 AirWatch 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 AirWatch 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.

In This Section

- Configuring General Profile Settings – See how to set up a profile's general settings.
- Deploying Passcode Profiles to BlackBerry 10 Devices – Learn how to configure Passcode profiles for use on devices.
- Time Schedules – Details time schedules and how they are created and applied to profiles.

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. 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.
3. Configure **General** settings on the applicable tab. These include:
    - **Name** – Name of the profile to be displayed in the AirWatch Admin Console.
    - **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 assignment type in which the profile integrates with third-party systems to deploy a specific payload to a device.
        - **Compliance** – The profile is deployed when the end user violates a compliance policy applicable to the device.
    - **Minimum Operating System** – The minimum operating system required to receive the profile.
    - **Model** – The type of device to receive the profile.
    - **Ownership** – Determines which ownership category receives the profile:
    - **Allow Removal** – Determines if 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.
        - **Never** – The end user cannot remove the profile from the device.
    - **Managed By** – The Organization Group with administrative access to the profile.
    - **Assigned Organization Groups** – The Organization Groups that receive the profile.
    - **Additional Assignment Criteria** – These check boxes enable additional restrictions for the profile:
        - **Publish only to users in selected User Groups** – Specify one or more User Groups to receive 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. See Time Schedules for more information.

4. Configure a payload for the device platform.

   Note: For step-by-step instructions on configuring a specific payload for a particular platform, please refer to the applicable **Platform Guide**.

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 AirWatch 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** and then select **BlackBerry 10**.
2. Configure General settings for the profile.
3. Select the **Passcode** profile.
4. 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.
5. Select **Save & Publish** when you are finished to push the profile to devices.

Legacy BES Server Integration

Overview

The BES enables secure communication between BlackBerry devices and corporate networks. AirWatch does not replace the BES, but rather works with it to integrate BlackBerry devices with other mobile platforms within your corporate mobile infrastructure. AirWatch supports multiple platforms and can facilitate migration from one platform to another, if desired. AirWatch also gives you the ability to manage mobile multi-tenant environments. For example, create a BlackBerry Administrator to manage just the BlackBerry fleet while still accessing other administrator roles for other mobile platforms within the AirWatch Admin Console.

AirWatch can integrate with the BES either in an on-premise environment or in a software as a service (SaaS) environment.

In This Section

- AirWatch Integration Requirements – Explains configuring communications between the BES and AirWatch Admin Console.
- Connecting AirWatch to the Legacy BES Server – Provides steps needed to connect the BES to the AirWatch Admin Console.
- Testing the Connection to the Legacy BES Server – Provides steps needed to test the connection between AirWatch, the BES, and BlackBerry devices.

AirWatch Integration Requirements

To configure communication between the BES and the AirWatch Admin Console, you need to set communications using a secure and functional port (e.g., 443) for the following:

- AirWatch MDM Server requires a communication channel to the BES Server over TCP.
- AirWatch MDM Server also requires a communication channel to the Active Directory (AD) Server.
- AirWatch solution uses the admin account that has administrator rights on the BES server. Typically, this admin account is used to access the BES Web Console interface from which BlackBerry devices are managed.

Note: Verify there is connectivity on the port you choose to use.

Connecting AirWatch to the Legacy BES Server

Use the following procedure to connect the AirWatch Admin Console and the BES:

1. Go to **Groups & Settings ▶All Settings ▶Device & Users ▶BlackBerry ▶Legacy BlackBerry ▶BES Settings**.
2. Enter the following BES information:

a. **BWS URL** – Enter the URL for the BlackBerry Web Services that contains all the web service APIs used to synchronize the AirWatch solution and the BES. The URL format is *https://<BES_URL>/enterprise/admin/ws*.

b. **BWS Util URL** – Enter the URL for the BlackBerry Web Services Utility that contains helper APIs used to form credentials for connecting to the BWS. The URL format is *https://<BES_URL>/enterprise/admin/util/ws*.

c. **BES Locale** – Enter the country location of the BES. For example, en_US.

3. Ensure that the **Authentication Method** field is set to **Active Directory**.
4. Enter the username and password needed to authenticate with the BES in the **BES Username** field and the **BES Password** field.
5. Enter a domain for the BES in the **Domain** field.
6. Enter the applicable ID associated with the BES in the **Organization ID** field. This entry is typically **0**.
7. Enable **Sync Applications** if you want to pull a list of applications from BlackBerry devices registered with the BES and **Save** the settings.

Testing the Connection to the Legacy BES Server

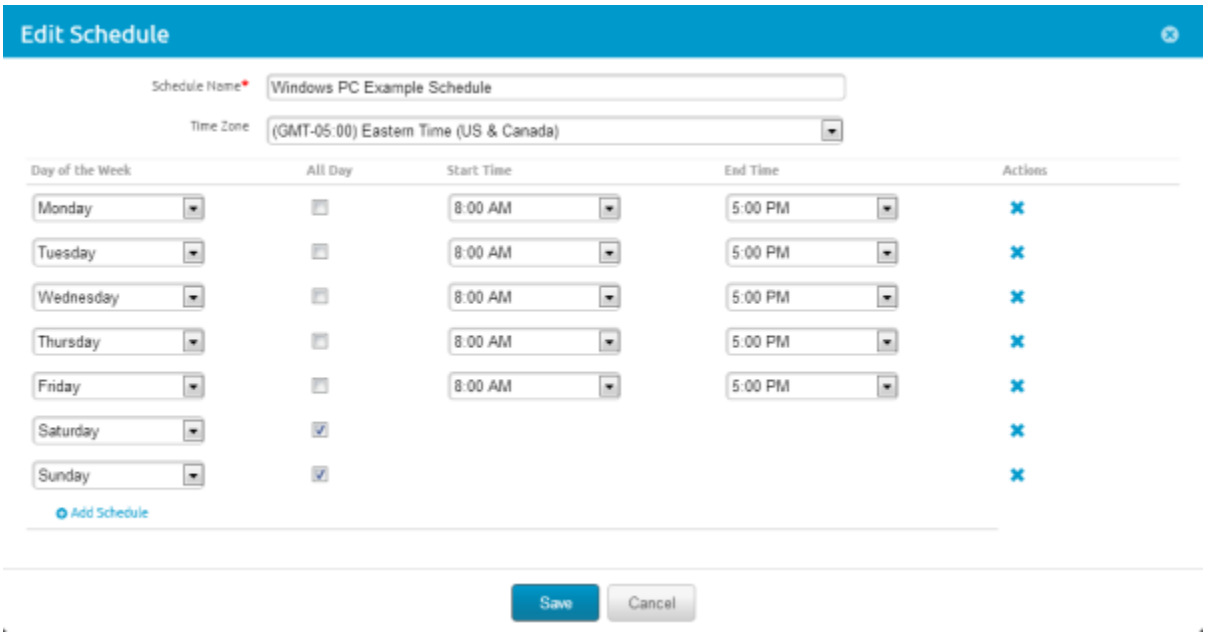
Test the connection between AirWatch, the BES and BlackBerry devices. These steps work for on-premise environments. These settings are not visible in the AirWatch Console for SaaS environments unless you also have the ACC.

1. Go to **Groups & Settings ▶All Settings ▶Device & Users ▶BlackBerry ▶Legacy BlackBerry ▶BES Settings**.
2. Click **Test Connection** at the bottom of the screen.

Note: For more information about performing BES integration tasks, see the **Appendix – BES Configuration**.

Time Schedules

In addition to simply assigning applicable profiles, you have the ability to enhance device management further by controlling when each profile assigned to the device is active. Configure and apply time schedules to restrict when profiles are active on the device. Applying time schedules to profiles secures your corporate resources by only allowing employees access during the specific days and time frames. Conversely, applying time schedules can also limit personal content and access during work hours.



In This Section

- Defining Time Schedules – See how to create a time schedule, which allows or denies access to internal content and features based on the day and time.
- Applying a Time Schedule to a Profile – See how to apply a time schedule to a profile, which lets you control when and how a particular profile is activated.

Defining Time Schedules

To create a time schedule:

1. Navigate to **Devices ▶Profiles ▶Settings ▶Time Schedules**.
2. Select **Add Schedule** to launch the **Add Schedule** window.
3. Enter a name for the schedule in the **Schedule Name** field.
4. Select the applicable **Time Zone** using the drop-down menu.
5. Select the **Add Schedule** hyperlink.

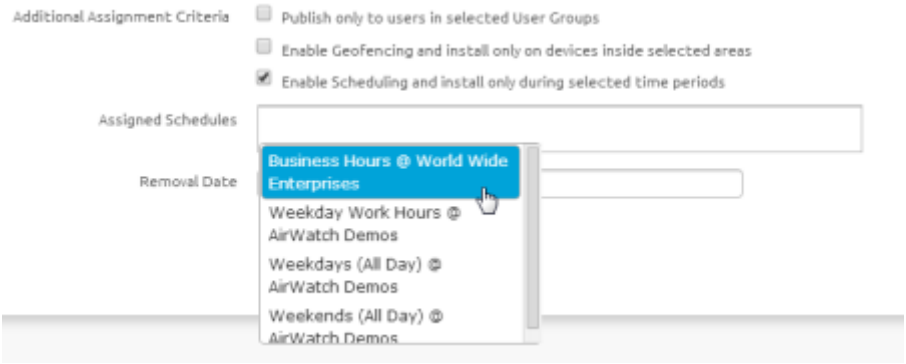
6. Select the **Day of the Week**, **Start Time** and **End Time** using the applicable drop-down menus. You can also select the **All Day** check box to disable start and end times for the schedule.
   To remove a day from the schedule, select the applicable **X** under **Actions**.
7. Repeat steps 5 and 6 as many times as is necessary to add additional days to the schedule.
8. Select **Save**.

Applying a Time Schedule to a Profile

Once you have defined a time schedule, you can apply it to a profile and combine it with other payloads to create more robust profiles. For example, you can define time schedules for the normal work hours of different organization groups and add a Restrictions payload that denies access to the Game Center, multiplayer gaming or YouTube content based on ratings and other settings.

Once activated, the employees of the Organization Group to whom the profile was applied will no longer have access to these functions during the specified times.

1. Navigate to **Devices ▶Profiles ▶List View ▶Add** and select your platform.
2. Select **Enable Scheduling and install only during selected time periods** on the **General** tab. An **Assigned Schedules** box displays.



3. Enter one or multiple Time Schedules to this profile.
4. Configure a payload, such as Passcode, Restrictions or Wi-Fi that you want to apply only while devices are inside the time frames.
5. Select **Save & Publish**.

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 AirWatch Admin Console.

In This Section

- Enrolling Legacy BlackBerry Devices Using the Web – Defines the steps needed to enroll a device.
- Configuring the AirWatch Legacy BlackBerry Agent – Explains how to configure agent settings in order for the AirWatch Admin Console to communicate with devices.
- Using the AirWatch Legacy BlackBerry Agent – Explains how to use the agent and its capabilities.
- Communicating with Legacy BlackBerry through the Secure Channel – Details how to create a secure channel for communication between Legacy BlackBerry devices and AirWatch Admin Console

Enrolling Legacy BlackBerry Devices Using the Web

1. Open the native browser on the BlackBerry device and go to the **Enrollment URL**.
2. Enter your **Group ID** and click **Next**.
3. Enter your AirWatch user credentials and click **Enroll**.
4. Enter your email username and password so that this information appears in the Device Dashboard in the AirWatch Admin Console. This entry is optional.
5. Select the type of device in the **Device Ownership** drop-down menu. Settings include the following options **Corporate-Dedicated**, **Corporate-Shared** and **Employee Owned**. This setting helps manage devices in a bring-your-own-device (BYOD) deployment. This entry is optional.
6. Click **Accept** after reviewing the End User License Agreement (EULA), if applicable.
7. You can enable **Set Application Permissions** if you want to control the permissions of the AirWatch Agent on the BlackBerry device. This entry is optional.
8. Click **Download** and select **Yes** on the **AirWatch Agent Trusted Application status** screen.
9. Click **Save** the permissions, and you can also click **Details** to review the permissions.

Note: You can configure options and push policies according to the type of device in **Groups & Settings ▶All Settings ▶ Devices & Users ▶General ▶Privacy**. For example, you can configure the AirWatch Admin Console not to collect **GPS Data** for employee owned devices.

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 AirWatch 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 AirWatch Admin Console:
    - **Heartbeat Interval** – Specify when the AirWatch Agent confirms a connection and synchronizes with the AirWatch 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 AirWatch Admin Console.
    - **Collect Location Data** – Set the AirWatch Agent to send GPS data to the AirWatch 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.
	  ○ **Location** – See GPS location information from the latest GPS sampling data.
	  ○ **Network** – See network information such as the Wi-Fi IP address.
	  ○ **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.
	  ○ **Transmission Frequency** – Set the transmission interval of data to the AirWatch Admin Console.
	  ○ **Last Heartbeat Attempt** – View the date and time of the last heartbeat sent to the AirWatch Admin Console.
	  ○ **Last Heartbeat Result** – View the success or failure of the last heartbeat sent to the AirWatch Admin Console.
	• **Data Sampling** – Configure and view information about data sampling.
	  ○ **Host Port** – Configure the port number to send data to the AirWatch Admin Console.
	  ○ **Transmission Frequency** – Set the transmission interval to send data samples to the AirWatch Admin Console.
	  ○ **Sample Frequency** – Set the interval for the AirWatch Agent to perform data sampling.
	  ○ **Last Data Sampling Attempt** – View the date and time of the last data sample sent to the AirWatch Admin Console.
	  ○ **Last Data Sampling Result** – View the success or failure of the last data sample sent to the AirWatch Admin Console.
	• **Profile Refresh**, **Profile Refresh Interval** – Set the interval to refresh the profile requests sent to the AirWatch Admin Console.
	• **Logging**, **Log Level** – Send a log request to the AirWatch Admin Console.

About	View the version of the AirWatch Agent.

Communicating with Legacy BlackBerry through the Secure Channel

The Secure Channel certificate enables all the communication such as device status, interrogator, etc. happening between the device and the AirWatch Admin Console to be signed and encrypted. For devices not having the secure channel certificate, you have the option to enable/disable their communication with AirWatch.

To enable this secured communication:

1. Navigate to **Groups & Settings ►All Settings ►System ►Advanced ►Secure Channel Certificate**.
2. Select the **BlackBerry** platform and click **Save.**

Legacy Device Profiles

Overview

The AirWatch Agent links devices to the AirWatch 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, Advanced, and Custom Settings.

In This Section

- Configuring General Profile Settings – See how to set up a profile's general settings.
- Deploying Legacy BlackBerry Device Profiles – Learn how to configure the device profile to control the backlight settings on the device as well as the GPS.
- Deploying Legacy BlackBerry Advanced Payloads– Details how to set the device log including log size and output type.
- Deploying Custom Settings Legacy BlackBerry Payload – Allows you to create your own profile through XML.
- Communicating with Legacy BlackBerry through the Secure Channel – Provides steps needed to configure certificate based signed and encrypted communications between the AirWatch Admin Console and devices.
- Securing Legacy BlackBerry Devices by Time Schedules – Learn how to configure time schedules to set time-based rules to govern profile pushes and when the device user can access corporate data from their device.

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. 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.
3. Configure **General** settings on the applicable tab. These include:
    - **Name** – Name of the profile to be displayed in the AirWatch Admin Console.
    - **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 assignment type in which the profile integrates with third-party systems to deploy a specific payload to a device.
        - **Compliance** – The profile is deployed when the end user violates a compliance policy applicable to the device.
    - **Minimum Operating System** – The minimum operating system required to receive the profile.
    - **Model** – The type of device to receive the profile.
    - **Ownership** – Determines which ownership category receives the profile:
    - **Allow Removal** – Determines if 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.
        - **Never** – The end user cannot remove the profile from the device.
    - **Managed By** – The Organization Group with administrative access to the profile.
    - **Assigned Organization Groups** – The Organization Groups that receive the profile.
    - **Additional Assignment Criteria** – These check boxes enable additional restrictions for the profile:
        - **Publish only to users in selected User Groups** – Specify one or more User Groups to receive 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. See Time Schedules for more information.

4. Configure a payload for the device platform.

   Note: For step-by-step instructions on configuring a specific payload for a particular platform, please refer to the applicable **Platform Guide**.

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** and then select **BlackBerry**.
2. Configure General settings for the profile.
3. Select the **Device** profile.
4. 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 AirWatch Admin Console.
   - **GPS Sample Interval** – Enter the interval at which the AirWatch Agent takes GPS data samples.
5. 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** and then select **BlackBerry**.
2. Configure General settings for the profile.
3. Select the **Advanced** profile.
4. 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 AirWatch 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.

5. 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 AirWatch Admin Console. The AirWatch 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**. The **Dashboard** 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. In addition, 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.

In This Section

- Registration of BlackBerry Devices – Covers registering BlackBerry Devices with the AirWatch Admin Console.
- Using the Device Dashboard – Explains how administrators can locate and manage iOS devices in the AirWatch Admin Console.
- Using List View – Details how to use the Devices List View to search for, filter and perform remote actions on multiple Android devices.
- Using the Device Details Page – Walks through the ways you can manage Android devices from using the Device Details Page in the AirWatch Admin Console.
- Utilizing Reports – Presents reports and collected data within the AirWatch Admin Console featuring detailed information on all aspects of your deployment.
- Using the Hub – Presents the data flow within AirWatch Hub and how to use the data within.
- Using the Self-Service Portal – Explains how users can manage their Android devices from the Self-Service Portal.
- Migration to New Platforms – Explains how you can migrate from BlackBerry devices to a new platform without forcing end users to adapt.

Registration of BlackBerry 10 and Legacy BlackBerry Devices

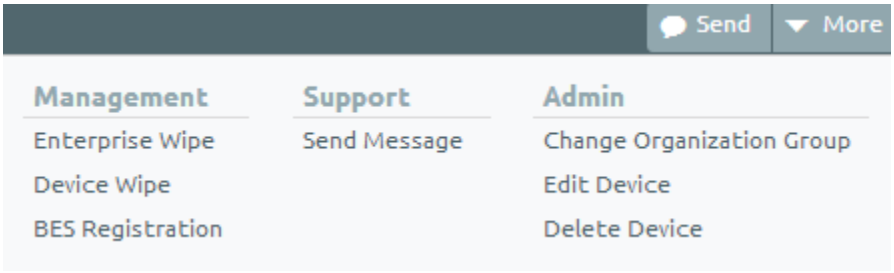
BlackBerry 10 and Legacy BlackBerry devices require AirWatch enrollment in order to receive policies. For BlackBerry 10 devices, AirWatch will automatically initiate registration with BES 10 upon the device being enrolled with the MDM Agent. For Legacy BlackBerry devices, the AirWatch Admin can initiate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

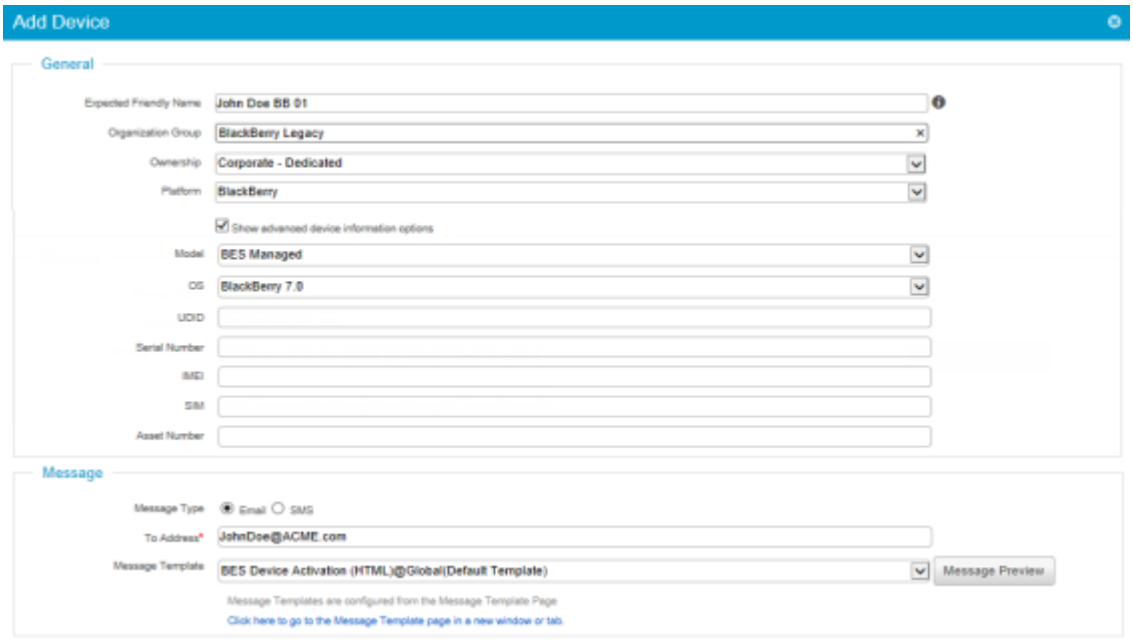
1. Navigate to **Devices ▶List View** in the AirWatch Admin Console

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** dropdown in the upper right.
5. Select **BES Registration** from the dropdown window and follow the prompts.



Registration of Legacy BlackBerry Devices

1. Navigate to **Devices ▶List View ▶ADD DEVICE** in the AirWatch 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 dropdown the owner of the device in **Device Ownership**.
5. Select **BlackBerry** from the **Platform** dropdown menu.
6. Select the **Show advanced device information options** checkbox.
7. Click the **Model** dropdown and select BES Managed.
8. Select from the **OS** dropdown 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 **Email** or **SMS** radio button to determine the method used to send the device user enrollment information.

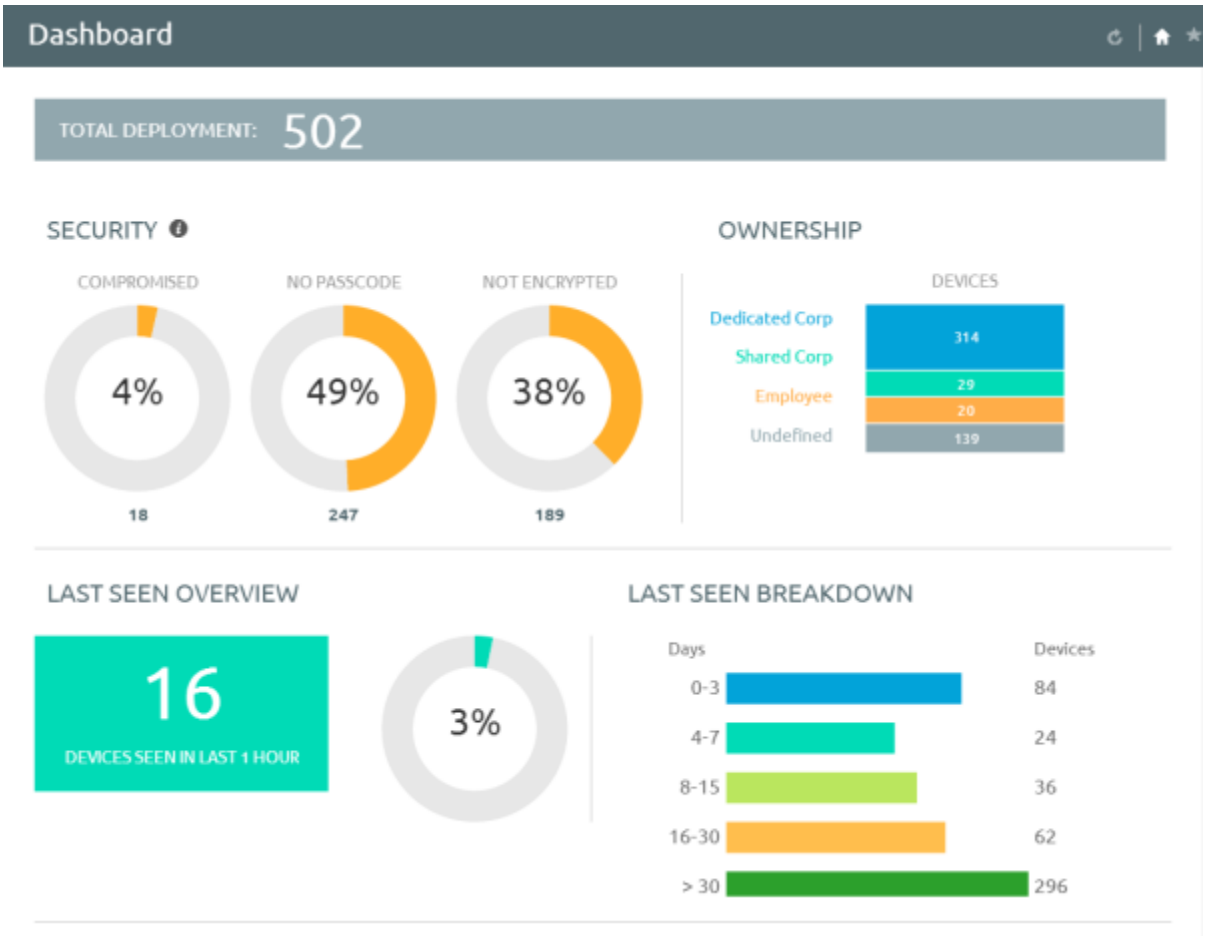
10. Enter the device user's email in the **To Address** field.
11. Select from the **Message Template** dropdown the enrollment template the device user will receive via email or SMS.

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 AirWatch **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 platform breakdown.



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

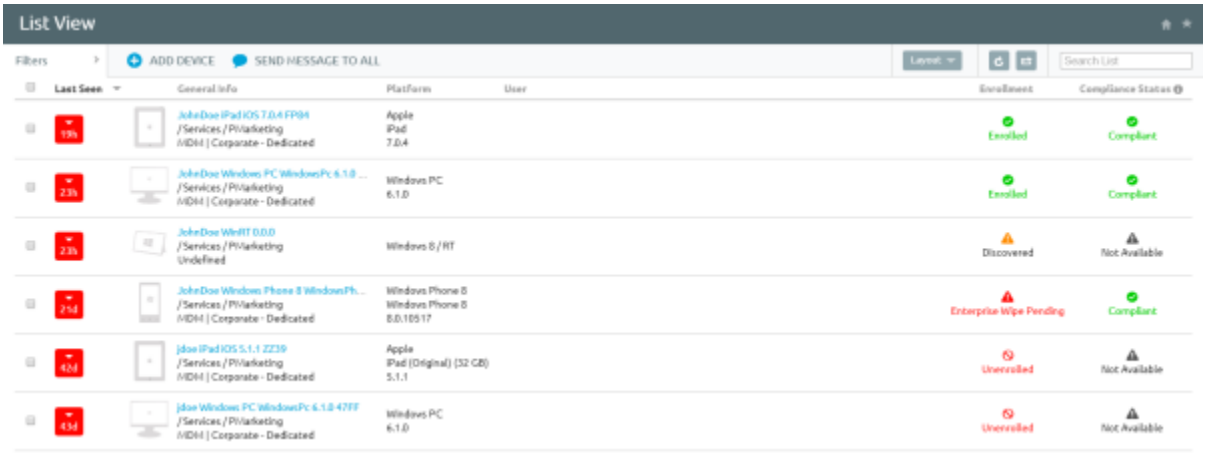
Switch to **List View** (**Devices ▶List View**) at any time to sort and manage devices by filtering the columns and fields available in the **Device Dashboard**, including:

- Last Seen
- Friendly Name
- Ownership
- Username
- Display Name
- Platform/OS/Model

- Corporate - Dedicated
- Corporate - Shared
- Employee-Owned

- Organization Group
- Compliance Status

Select on a device Friendly Name at any time to open up the device details page for that device.



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. Search all devices for a friendly name or user's name to isolate one device or user. Once you have sorted or filtered dashboard information, export, save and send the data for review.

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.

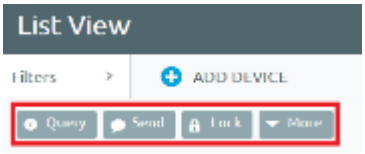
You can also search specific information across all fields associated with devices and users, allowing you to search user name ("John Doe") or device type.

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.

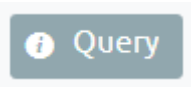
Using the Management Tabs

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:

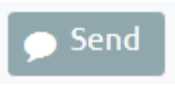
Note: The actions listed below will vary depending on factors such as device platform, AirWatch Admin Console settings, and enrollment status.



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 Send Message menu and compose message to send to selected devices.

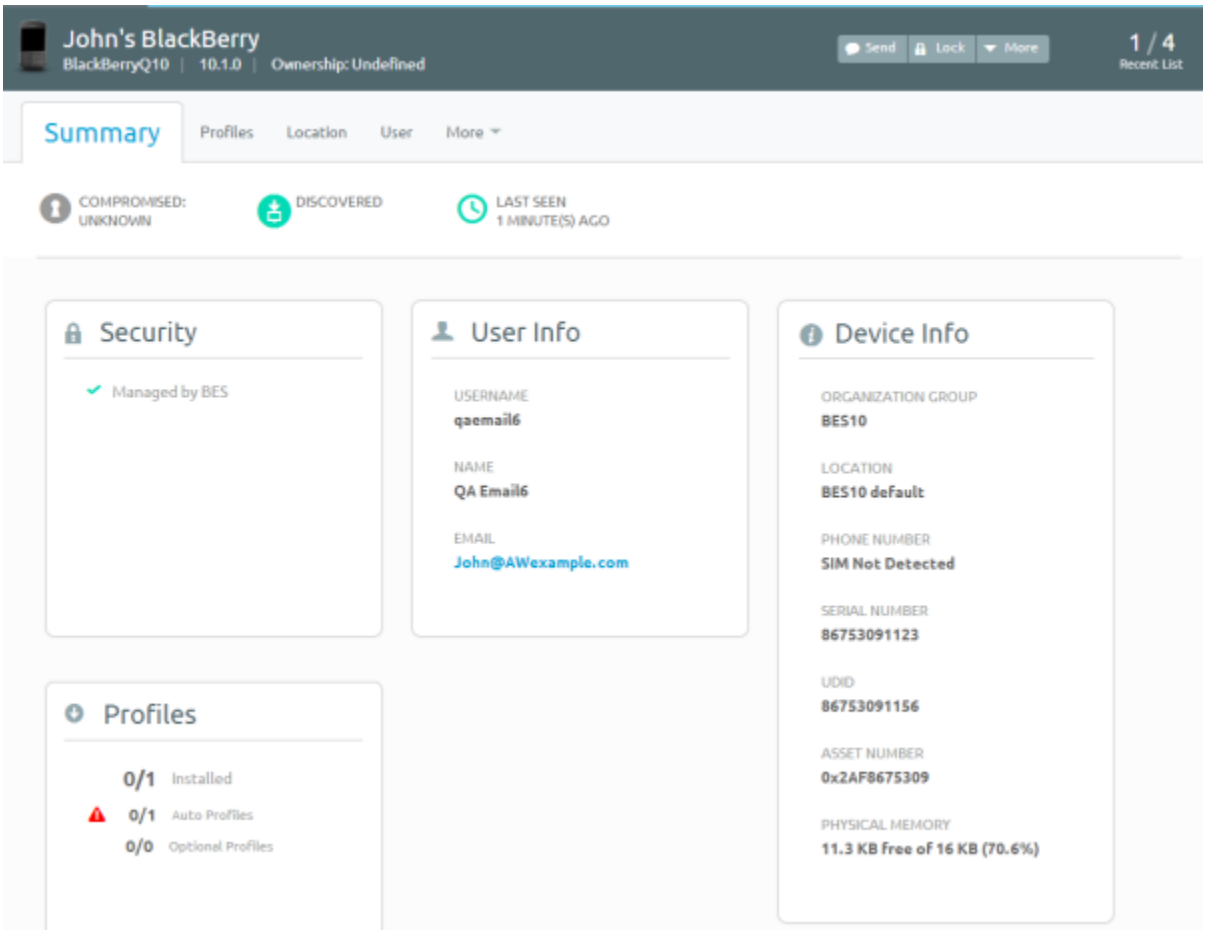
Lock – Lock all selected devices and force users to re-enter device security PIN.

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 AirWatch 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 configuration for selected devices. Select Install Product to install a particular apps to selected devices.

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 either selecting a device's Friendly Name from the Device Search page, from one of the available Dashboards or by using any of the available search tools with the AirWatch Admin Console.

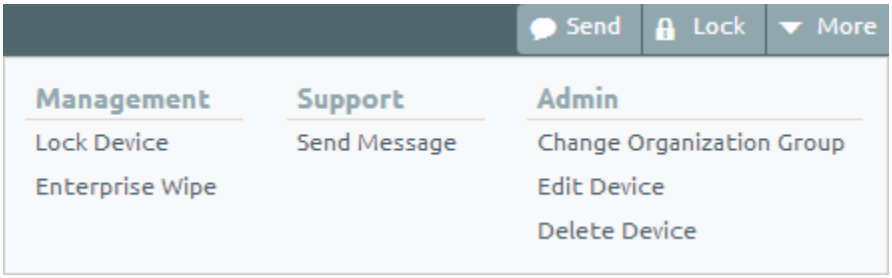


Use the Device Details menu tabs to access specific device information, including:

- **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.
- **User** – Provide information about the device user.
- **Event Log** – Clicking **More** and selecting this from the dropdown 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.



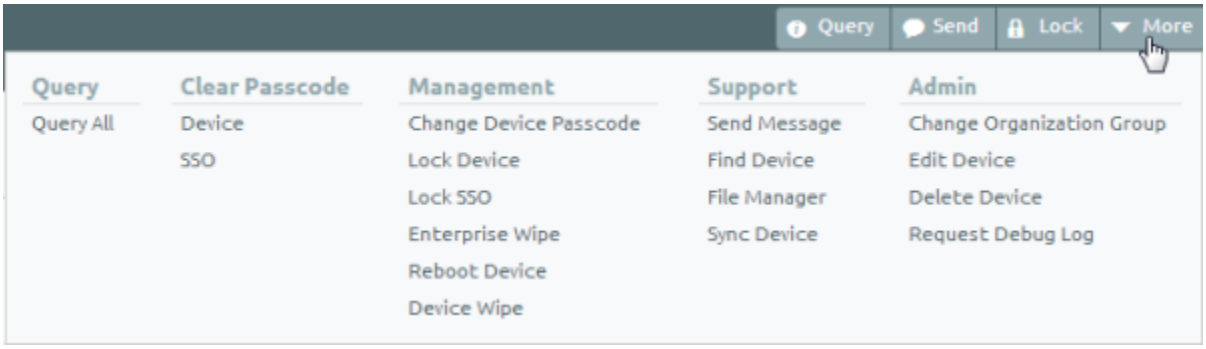
Note: The actions listed below will vary depending on factors such as device platform, AirWatch Admin Console settings, and enrollment status.

- **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 AirWatch 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 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 AirWatch Admin Console settings, including changing Organization 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.

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 will vary depending on factors such as device platform, AirWatch 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 AirWatch 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.

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 AirWatch 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 **AirWatch Mobile Device Management Guide**.

Using the Self-Service Portal (SSP) for All BlackBerry Devices

The **AirWatch Self-Service Portal** (SSP) allows end users to remotely monitor and manage their smart devices. The Self-Service Portal lets you view relevant device information for enrolled devices and perform remote actions such as clear passcode, lock device, or device wipe.

Using the SSP

Logging into the SSP

You can access the SSP by logging in through a browser. To do this, navigate to the SSP website using the URL provided to you. It should look similar to this format: **https://mdm.acme.com/mydevice**. Once you launch the SSP, you can log in using the same credentials (**Group ID**, **username** and **password**) you used to enroll in AirWatch. Optionally, if Email Domain registration is configured, you can log in using your corporate email address.

Selecting a Device in the SSP

After logging in to the SSP, a list of all devices tied to your user account displays on the left. Select the device you want to manage. The **Device Details** screen displays.

Viewing Device Information

The following tabs display device-related information:

- **Security** – This tab displays the information specific to security controls currently in place for the device, including: enrollment status, assigned profile status, installed certificate status, certificates nearing expiry and installed applications.
- **Profiles** – This tab shows all of the MDM profiles that have been sent to the devices enrolled under your user account and the status of each profile. From the Profiles view, you can select the install icon ()to install a profile or the delete icon () to remove it from the device.
- **Apps** – This tab displays all applications that have been installed on the selected device and provides basic application information.
- **Location** – This tab displays the coordinates of the selected device, if enabled.
- **Event Log** – This tab contains a comprehensive log of all interactions between the AirWatch Admin Console and the device.
- **Support** – This tab contains detailed device information and contact information for your organization's support representatives.

Perform Remote Actions

The **Remote Actions** enable you to perform remote actions over-the-air to the selected device. See below for detailed information about each remote action.

Note: All remote action permissions are determined by your administrator and therefore you may not be able to perform all listed actions.

- **Send Message –** Sends an Email, SMS (text) or Push Notification over-the-air to the selected device.
- **Lock Device –** Locks the selected device so that an unauthorized user cannot access it. This feature is useful if the device is lost or stolen (In this case, you may also want to use the GPS feature to locate the device.)

- **Enterprise Wipe –** Wipes all corporate data from the selected device and removes the device from AirWatch MDM. All of the enterprise data contained on the device is removed, including MDM profiles, policies and internal applications. The device will return to the state it was in prior to the installation of AirWatch MDM.
- **Device Wipe –** Wipes all data from the selected device, including all data, email, profiles and MDM capabilities and returns the device to factory default settings.

Migrating to New Platforms

The AirWatch solution makes migrating users to other mobile platforms possible.

Preparing for Migration

Preparing to migrate from a BlackBerry to another platform does not alter the end users experience. Rather, consumers can continue to use their BlackBerry smartphones independent of their migration plans. As soon as AirWatch integrates with BES, all existing devices are imported into the AirWatch Admin Console for management. Post-integration you have the capacity to manage centrally all devices in the Console as the Administrator, regardless of platform. The multi-platform structure of the AirWatch Admin Console sets up devices for migration to any device. Furthermore, you can prepare profiles, applications, and content in anticipation of users migrating to other platforms without affecting ongoing BlackBerry support. This is extremely advantageous as all preparatory actions are completely discretionary and can be tailored to fit the unique needs of your company.

Enrolling a New Device

AirWatch's management capabilities vary depending on the platform. However, if the platform is compatible, as soon as an end user decides that they are ready for the new platform, they can go through AirWatch's enrollment process to easily regain all corporate content and get their device up to speed. Enrollment involves simply navigating to a URL on their device and authenticating it with their existing corporate credentials via LDAP. Once enrolled, AirWatch can push down all of the existing corporate configurations and email to that device. Simultaneously, the new device can receive corporate security policies for passcodes and device level encryption. Enrollment of a new device is a simple process that preserves all important corporate content while connecting the new device to key functionality for secure management.

Managing and Monitoring All Devices

Once configured, migration is complete. The new device can start to communicate regularly with the AirWatch Admin Console, and it begins to periodically send asset information back to the AirWatch Admin Console where it is monitored for compliance and threat management. This allows for central management and monitoring of all devices, BlackBerry, as well as other platforms, until retirement. This is how integration with AirWatch sets you up for migration and multi-platform device management.

Appendix – BES Configuration

Overview

This describes how to adjust the how synchronization between the BES and the AirWatch solution and provides examples of user and device privilege screens.

In This Section

- Adjusting the BES Integration Task – Provides steps needed to synchronize the BES and AirWatch Admin Console.
- User and Device Privileges – Provides examples of BES server screens that show user and device privileges.

Adjusting the BES Integration Task

If you have an on-premise AirWatch deployment, you can adjust the synchronization between the BES and the AirWatch solution.

Note: The BES Integration task is pre-configured to a default interval for AirWatch SaaS deployments.

1. Go to **Groups & Settings ▶All Settings ▶Admin ▶Scheduler**.
2. Find the **BES Integration** task and then click **Edit**.

Note: You can *only* edit this task at the Global level.

1. Adjust the interval to an applicable time. If you want to test synchronization, set it to a small value, for example, 5 minutes.
2. Check that the AirWatch Admin Console can pull BES devices and BES users into the **AirWatch Device Dashboard** and into the **Users** section.
3. Set the interval back to an applicable time, for example 12 hours, after testing synchronization.

User and Device Privileges

You can view the following screens on the BES server.

Privileges		
Create a group	No access	
Delete a group	No access	
View a group	Granted	All groups
Edit a group	Granted	All groups
Create a user	Granted	
Delete a user	Granted	
View a user	Granted	All groups
Edit a user	Granted	All groups
View a device	Granted	All groups
Edit a device	Granted	All groups
View device activation settings	Granted	
Edit device activation settings	Granted	
Create an IT policy	No access	
Delete an IT policy	No access	
View an IT policy	No access	
Edit an IT policy	No access	
Import an IT policy	No access	
Export an IT policy	No access	
Create a user-defined IT policy template	No access	
Delete a user-defined IT policy template	No access	
Resend data to devices	Granted	All groups
Edit a user-defined IT policy template	No access	
Import an IT policy template	No access	
Create a software configuration	No access	
View a software configuration	Granted	
Edit a software configuration	No access	
Delete a software configuration	No access	
Create an application	No access	
View an application	Granted	
Edit an application	No access	
Delete an application	Granted	
Create an administrator user	No access	
Add or remove to user configuration	Granted	All groups
Export asset summary data	Granted	All groups
Import or export users	Granted	All groups
Export statistics	Granted	All groups
Import user updates	Granted	All groups
Assign the current device to a user	Granted	All groups
Delete all device data and remove device	Granted	All groups
Delete only the organization data and remove device	Granted	All groups

BlackBerry Enterprise Server privileges		
Specify an activation password	Granted	All groups
Turn off and on external services	No access	
Generate an activation email	Granted	All groups

Synchronization privileges	
Clear synchronization backup data	No access

Email privileges	
Clear user statistics	No access
Reset user field mapping	No access
Turn on redirection	No access
Turn off redirection	No access
Add user from company directory	No access
Import new users	No access
Refresh available user list from company directory	No access
Import or export email message filters for a user	No access